

User Manual

MiniTA

Date: July 2023

Doc Version: 2.0

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.in.

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

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

Trademark

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

Disclaimer

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

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

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

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

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

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

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating

to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

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

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

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

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

ZKTeco India Global R&D Centre

Address J P Pride, Survey # 55, Khata # 503/499/5,
Puttapa Industrial estate, Mahadevapura,
Bangalore-560048, Karnataka.

Phone 080 68281342

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

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

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 **MiniTA**.

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






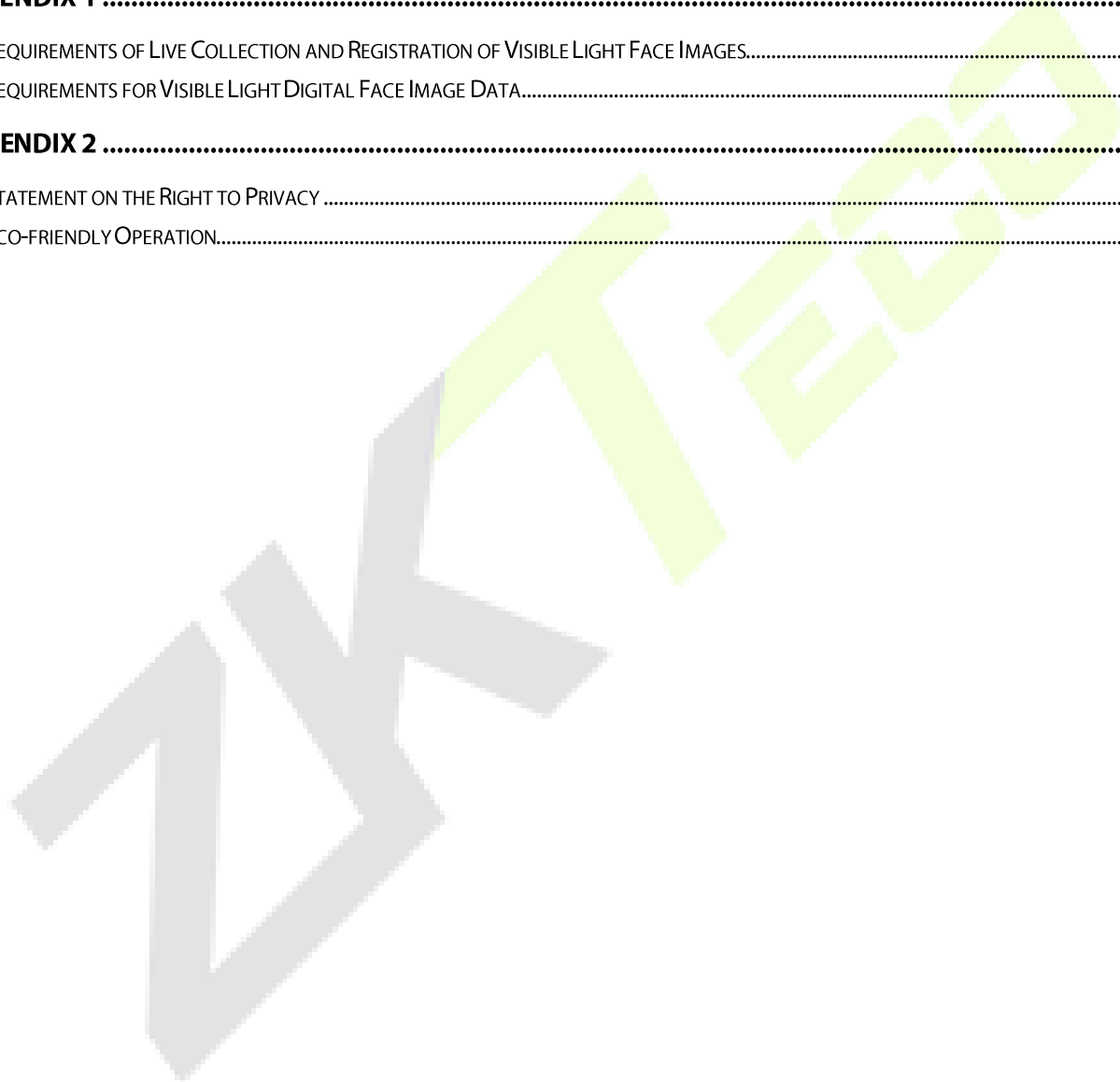
Convention	Description
	This implies about the notice or pays attention to, in the manual
	The general information which helps in performing the operations faster
	The information which is significant
	Care taken to avoid danger or mistakes
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1	INSTRUCTION FOR USE	7
1.1	STANDING POSITION, FACIAL EXPRESSION AND STANDIN POSTURE.....	7
1.2	FACE REGISTRATION.....	8
1.3	STANDBY INTERFACE.....	9
1.4	VIRTUAL KEYBOARD	10
1.5	VERIFICATION MODE.....	10
1.5.1	FACIAL VERIFICATION	10
1.5.2	PASSWORD VERIFICATION.....	12
2	MAIN MENU	14
3	USER MANAGEMENT	15
3.1	NEW USER REGISTRATION	15
3.2	ALL USERS.....	18
3.3	DISPLAY STYLE	19
4	USER ROLE	20
5	COMMUNICATION SETTINGS.....	22
5.1	ETHERNET.....	22
5.2	PC CONNECTION.....	23
5.3	WI-FI SETTINGS	24
5.3.1	ADDING WI-FI NETWORK.....	25
5.3.2	ADVANCED OPTIONS	25
5.4	CLOUD SERVER SETTING.....	26
5.5	NETWORK DIAGNOSIS.....	26
6	SYSTEM	28
6.1	DATE AND TIME.....	28
6.2	ATTENDANCE PARAMETERS.....	29
6.3	FACE.....	29
6.4	RESET.....	31
6.5	SECURITY SETTING.....	32
7	PERSONALIZE SETTINGS.....	33
7.1	USER INTERFACE SETTINGS.....	33
7.2	VOICE SETTINGS.....	34
7.3	BELL SCHEDULES.....	34
7.4	PUNCH STATE OPTIONS.....	35
7.5	SHORTCUT KEYS MAPPINGS.....	36
8	DATA MANAGEMENT	38
8.1	DELETE DATA	38
9	ACCESS CONTROL	40

- 9.1 ACCESS CONTROL OPTIONS.....40
- 10 ATTENDANCE SEARCH 42**
- 11 AUTOTEST 43**
- 12 SYSTEM INFORMATION..... 44**
- 13 CONNECT TO EASYTIMEPRO SOFTWARE..... 45**
 - 13.1 SET THE COMMUNICATION ADDRESS.....45
 - 13.2 ADD PERSON ON THE SOFTWARE47
- APPENDIX 1 50**
 - REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES.....50
 - REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA.....51
- APPENDIX 2 52**
 - STATEMENT ON THE RIGHT TO PRIVACY52
 - ECO-FRIENDLY OPERATION.....53

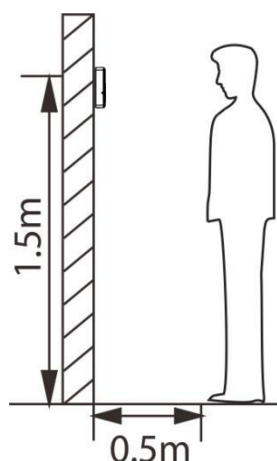


1 Instruction for Use

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

1.1 Standing Position, Facial Expression and Standin Posture

- **The recommended distance**



The distance between the device and a user whose height is within 1.55m to 1.85m is recommended to be 1.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

- **Facial expression and standing posture:**

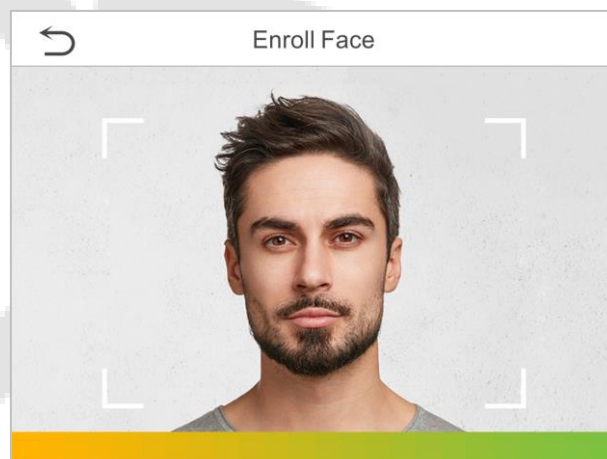




Note: During enrolment and verification, please remain natural facial expression and standing posture.

1.2 Face Registration

Try to keep the face in the centre of the screen during registration. Please face the camera and stay still during face registration. The page looks like this:



Correct face registration and authentication method

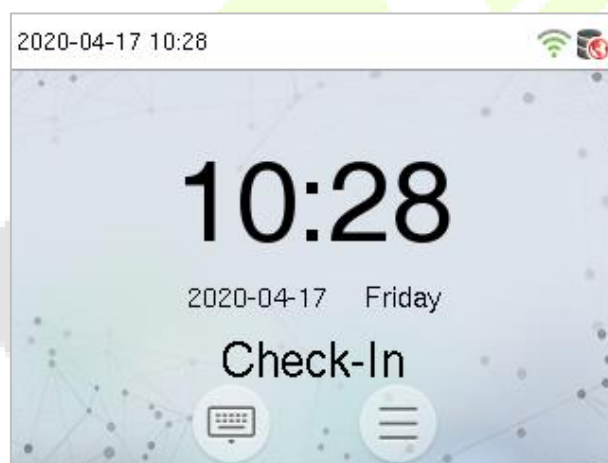
● Cautions for registering a face:

- ❖ When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- ❖ 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.
- ❖ Be careful not to cover the eyes or eyebrows.
- ❖ Do not wear hats, masks, sunglasses, or eyeglasses.
- ❖ Be careful not to display two faces on the screen. Register one person at a time.
- ❖ It is recommended for a user wearing glasses to register both faces with and without glasses.
- **Cautions for authenticating a face:**
 - ❖ Ensure that the face appears inside the guideline displayed on the screen of the device.
 - ❖ If glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
 - ❖ If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

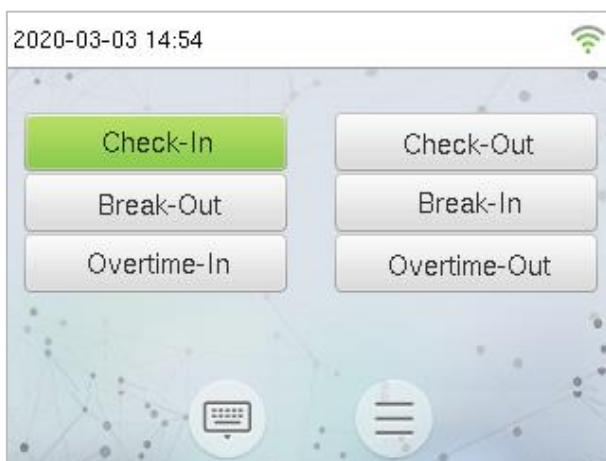
1.3 Standby Interface

After connecting the power supply, enter the following standby interface:



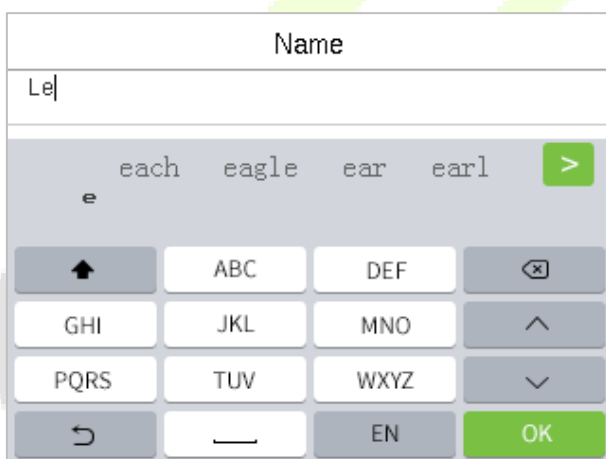
Notes:

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



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

1.4 Virtual Keyboard



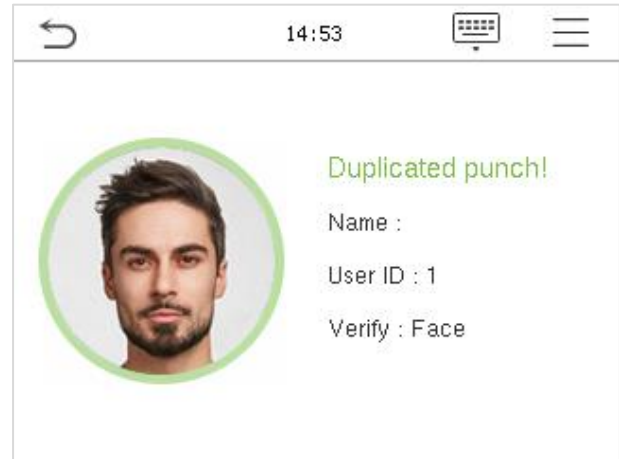
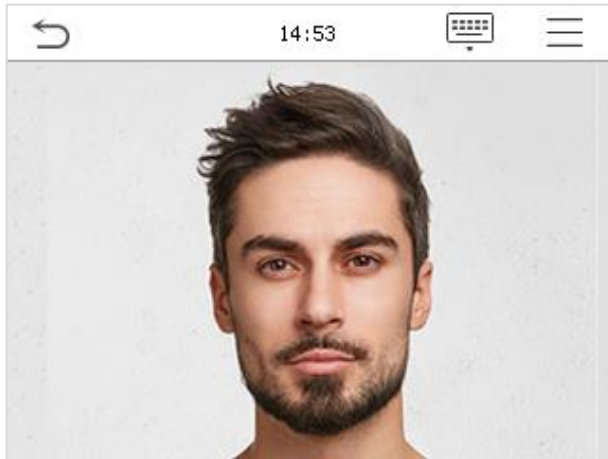
Note: The device supports the input of English, numbers, and symbols. Click [En] to switch to English keyboard. Press [123] to switch to the numeric and symbolic keyboard and click [ABC] to return to the alphabetic keyboard. Click the input box, virtual keyboard appears. Click [ESC] to exit the input.

1.5 Verification Mode

1.5.1 Facial Verification


- **1: N Facial Verification**

Compare the acquired facial images with all face data registered in the device. The following is the pop-up prompt box of comparison result.



● 1:1 Facial Verification


Compare the face captured by the camera with the facial template related to the entered user ID.

Press  on the main interface and enter the 1:1 facial verification mode.

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



If an employee registers palm and password in addition to face, the following screen will appear. Select the

 icon to enter face verification mode.



After successful verification, the prompt box "successfully verified" will appear.



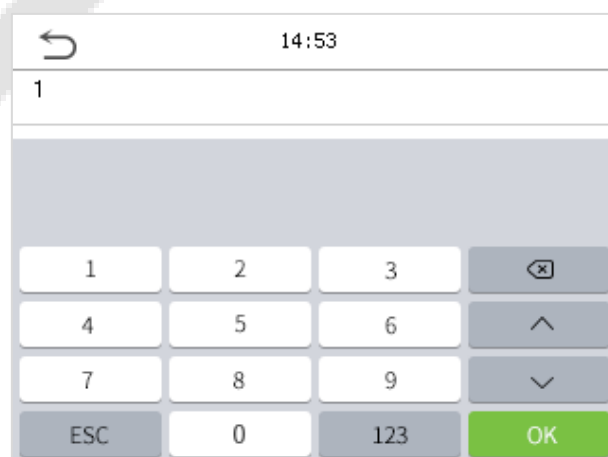
If the verification is failed, it will prompt as "Please adjust your position!".

1.5.2 Password Verification

Compare the entered password with the registered User ID and password.

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

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



If an employee registers palm and face in addition to password, the following screen will appear. Select the

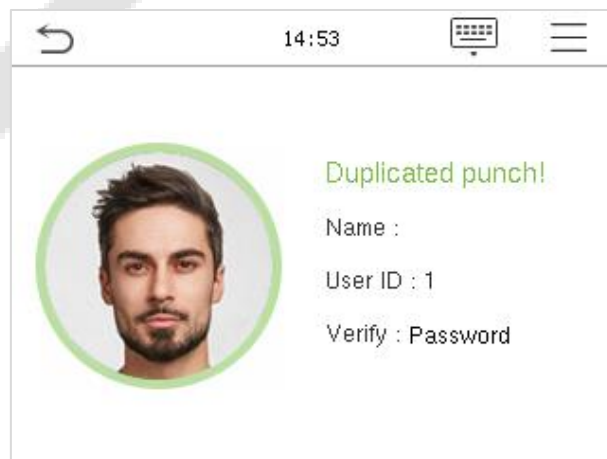
 icon to enter password verification mode.




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

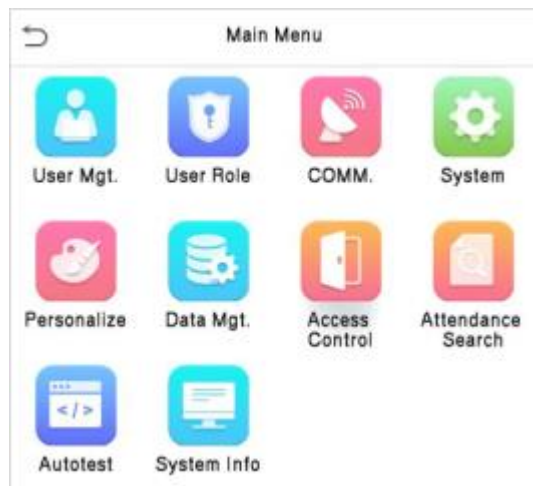


Verification is successful:



2 Main Menu

Press  on the initial interface to enter the main menu, as shown below:

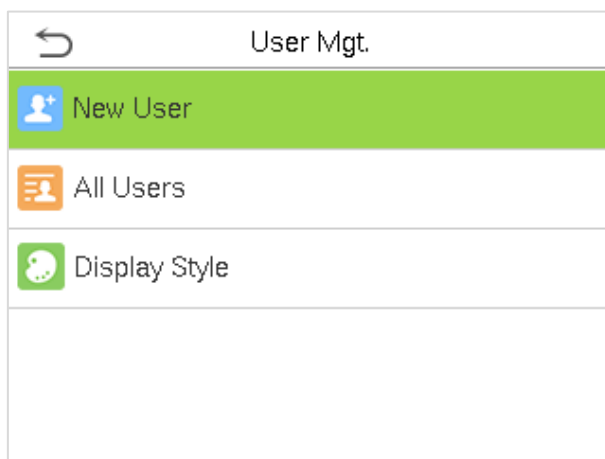


Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of PC connection and wireless network.
System	To set parameters related to the system, including date & time, attendance, face and resetting to factory settings.
Personalize	This includes user Interface, voice, bell, punch state options and shortcut key mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	To provide access and to set the duration of time (seconds) to Door Lock Delay, Door Sensor Delay, Door Sensor Type and Auxiliary Input Configuration.
Attendance Search	Query the specified access record, check attendance photos and blacklist photos.
Autotest	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 of the current device.

3 User Management

3.1 New User Registration

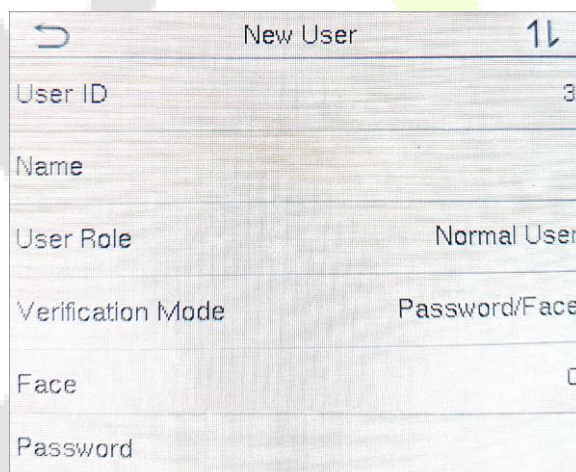
Tap **User Mgt.** on the main menu.



Tap **New User.**

- **Register a User ID and Name**

Enter the user ID and name.



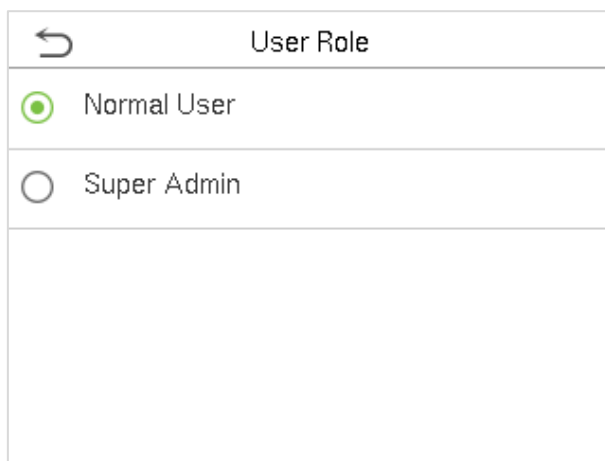
Notes:

- 1) A username contains 34 characters.
- 2) The user ID contain 1-9 digits by default.
- 3) During the initial registration, you can modify your ID, which cannot be modified after registration.
- 4) If the message "Duplicated ID" pops up, you must choose another ID.

- **Setting the User Role**

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

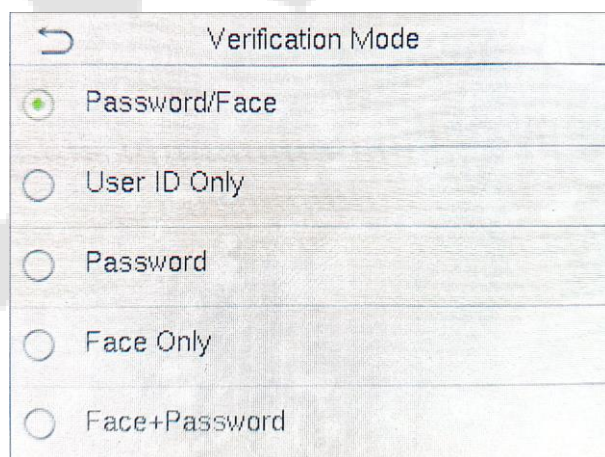
Click **User Role** to select Normal User or Super Admin.



Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to [1.5 Verification Mode](#).

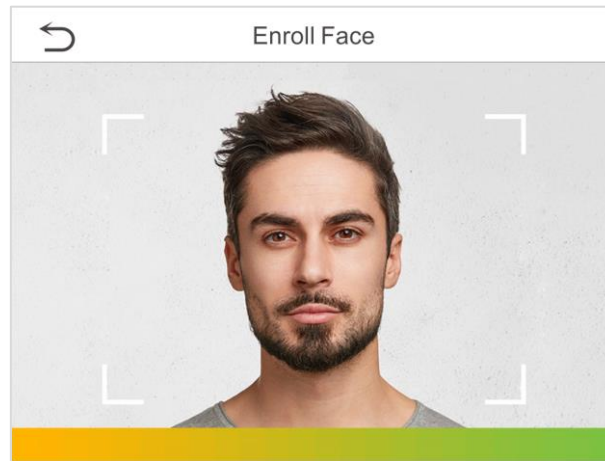
- **Verification Mode**

Set the mode of verification to access as **Password/Face, User ID Only, Password, Face Only, and Face+Password**.



- **Face Registration**

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



- **Password Registration**

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

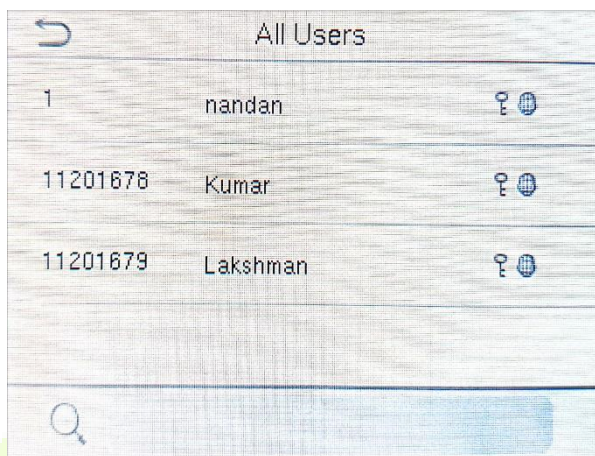
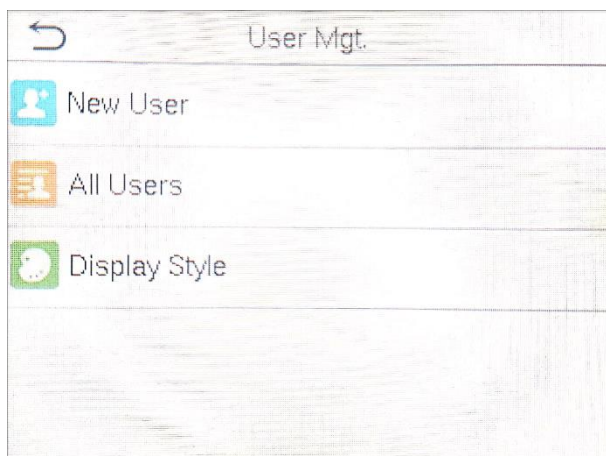
The image shows a mobile application interface titled "Password". It features a text input field at the top with a vertical cursor. Below the input field is a numeric keypad with buttons for digits 1-9, 0, and function keys: ESC, 123, a delete key (X), an up arrow (^), and a down arrow (v). A green "OK" button is located at the bottom right of the keypad.

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

3.2 All Users

All users option helps you to Search, Edit, and Delete the users. In **User Management** module, select **All Users** to access given function.

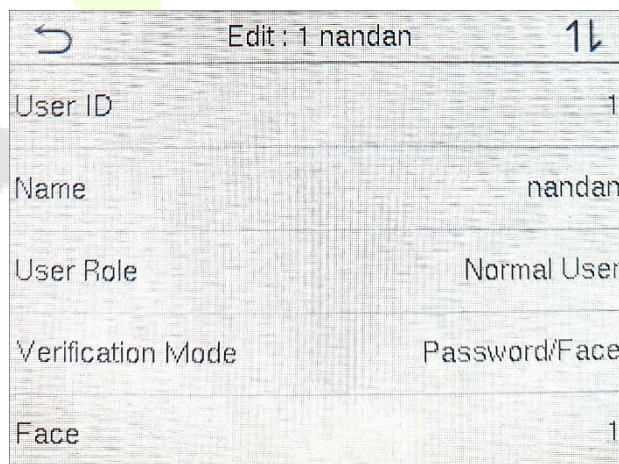
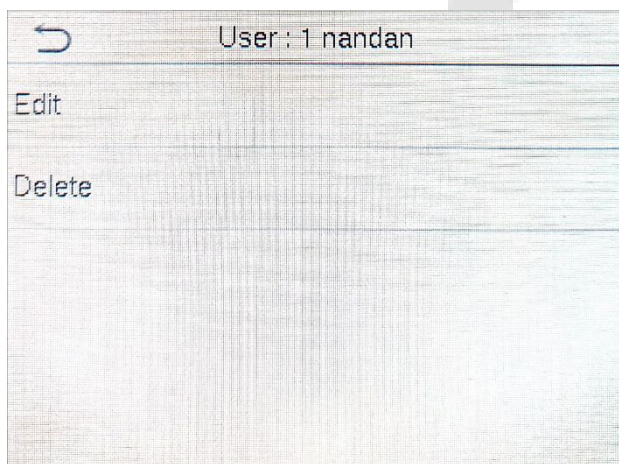
- **Search Users**



In All User interface, Search bar is found below. Click on search bar and provide username to search.

- **Edit Users**

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



Note: The operation of editing a user is as same as of adding a user, except that the user ID cannot be modified when editing a user. Operation method refers to "[3.1 Adding users](#)".

- **Deleting Users**

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

↶	User : 1 Mick
Edit	
Delete	

↶	Delete : 1 Mick
Delete User	
Delete Face Only	
Delete Password Only	

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

3.3 Display Style

User can set the displaying style for options and functions as Single line, Multiple Line, and Mixed Line.

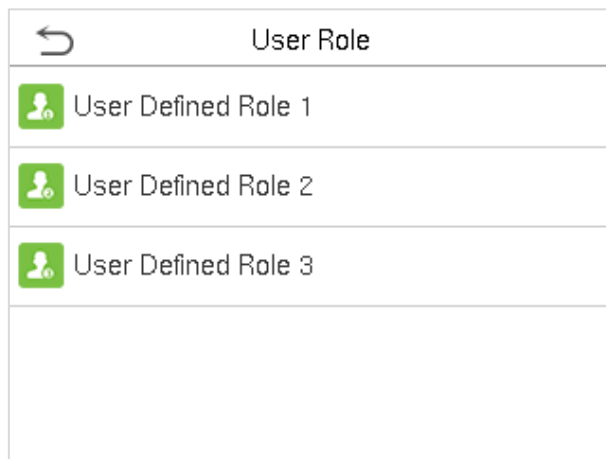
↶	Display Style
<input checked="" type="radio"/>	Single Line
<input type="radio"/>	Multiple Line
<input type="radio"/>	Mixed Line

4 User Role

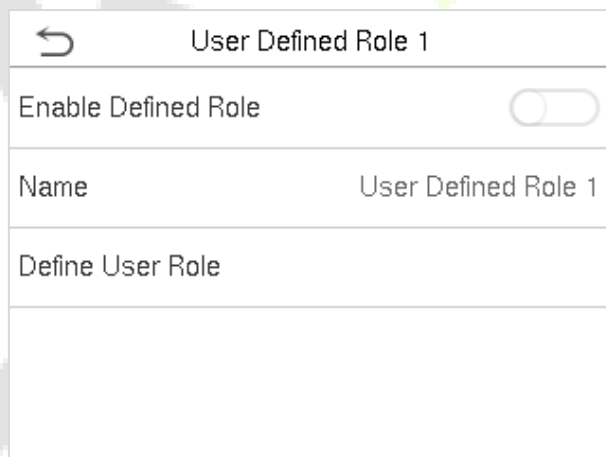
If you need to assign some specific permissions to certain users, you can edit the “User Defined Role” under the **User Role** menu.

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

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



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



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

User Defined Role 1	
<input checked="" type="checkbox"/> User Mgt.	<input checked="" type="checkbox"/> New User
<input checked="" type="checkbox"/> Comm.	<input checked="" type="checkbox"/> All Users
<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Display Style
<input type="checkbox"/> Personalize	
<input type="checkbox"/> Data Mgt.	

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

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

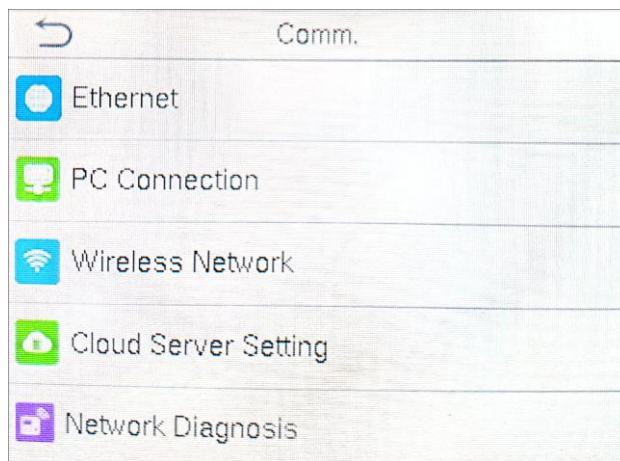
If no super administrator is registered, the device will prompt "Please enroll super admin first." after clicking the enable bar.

User Defined Role 1	
Enable Defined Role	<input type="checkbox"/>
Name	User Defined Role 1
Define User Role	
Please enroll super admin first.	
<input type="button" value="OK"/>	

5 Communication Settings

Set the relevant parameters of PC Connection, Ethernet, Cloud Server Setting and network Diagnosis.

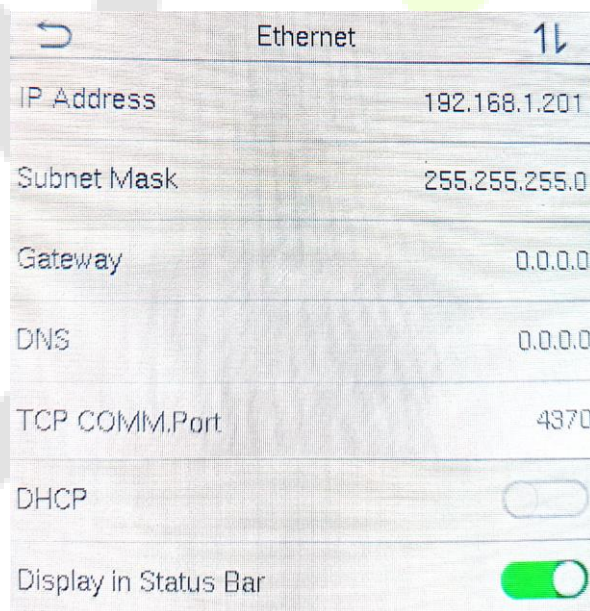
Tap **COMM.** on the main menu.



5.1 Ethernet

When the device needs to communicate with a PC over the Ethernet, you need to configure network setting and make sure that the device and the PC connect to the same network segment.

Tap **Ethernet** on the **comm.** Setting interface to configure the settings.



Item	Descriptions
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.

Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM.Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via sever.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

5.2 PC Connection

Comm Key helps to improve the security of the data by setting up the communication between the device and the PC.

If a Comm Key is set, a password is required to connect the device to the PC software.


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

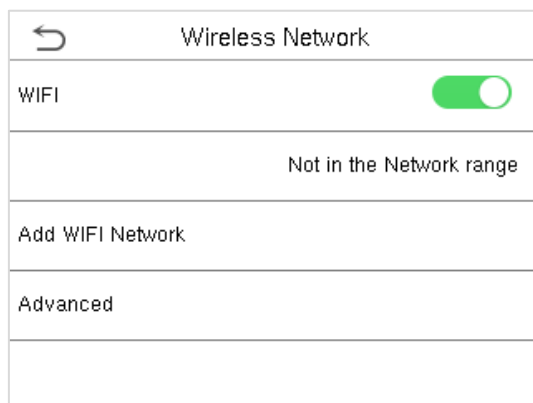
PC Connection	
Comm Key	0
Device ID	1

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

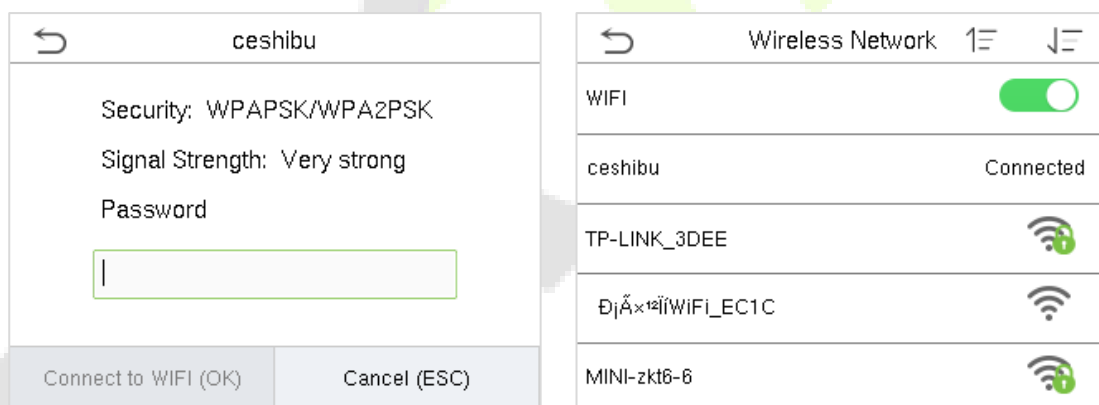
5.3 Wi-Fi Settings

Wi-Fi is short for Wireless Fidelity. The device provides a Wi-Fi module, which can be built in the device mould or externally connected, to enable data transmission via Wi-Fi and establish a wireless network environment.

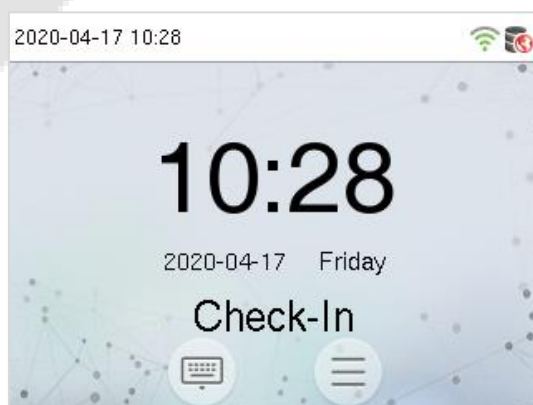
Wi-Fi is enabled in the system by default. If the Wi-Fi network does not need to be used, you can tap the  button to disable Wi-Fi.



When Wi-Fi is enabled, tap the searched network. Tap password entry text box to enter the password, and tap **Connect to Wi-Fi (OK)**.



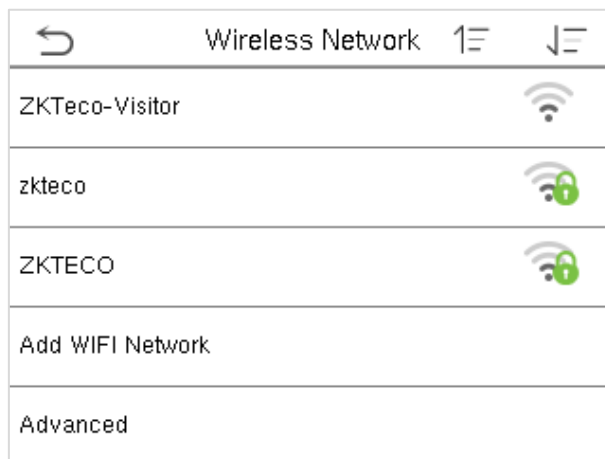
The connection succeeds, with status displayed on the icon bar.



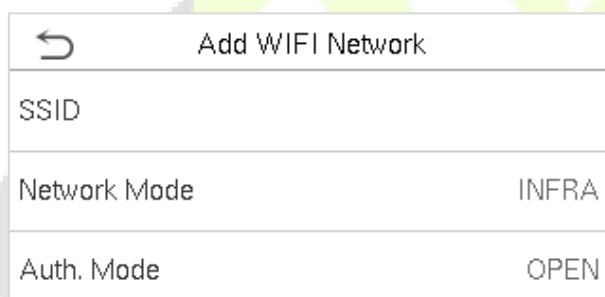
5.3.1 Adding Wi-Fi Network

If the desired Wi-Fi network is not in the list, you can add the Wi-Fi network manually.

Tap **Page Down** and **Add Wi-Fi Network**.



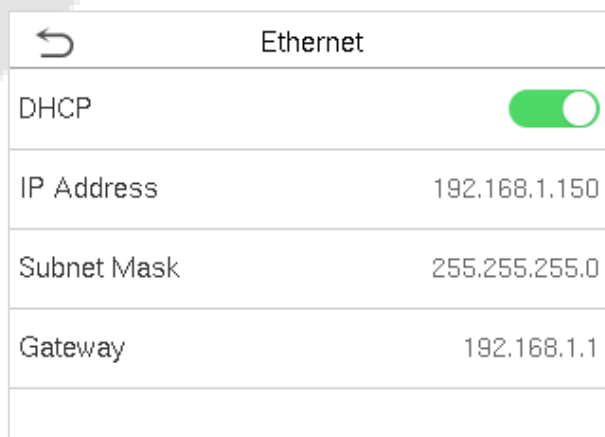
Enter the parameters of Wi-Fi network. (The added network must exist.)



After adding, find the added Wi-Fi network in list and connect to the network in the above way.

5.3.2 Advanced Options

This is used to set Wi-Fi network parameters.

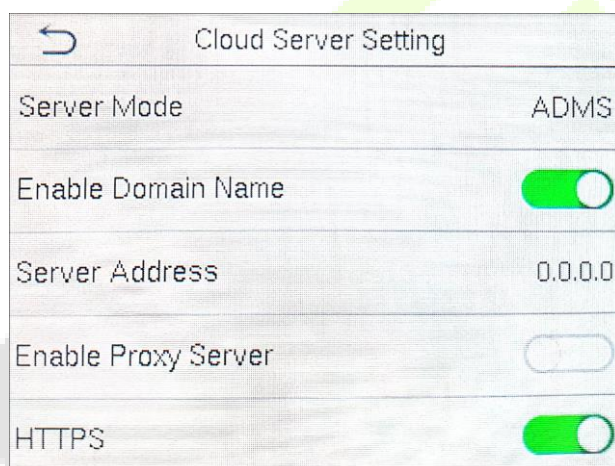


Menu Item	Description
DHCP	Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.

5.4 Cloud Server Setting

This represents settings used for connecting with the ADMS server.

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

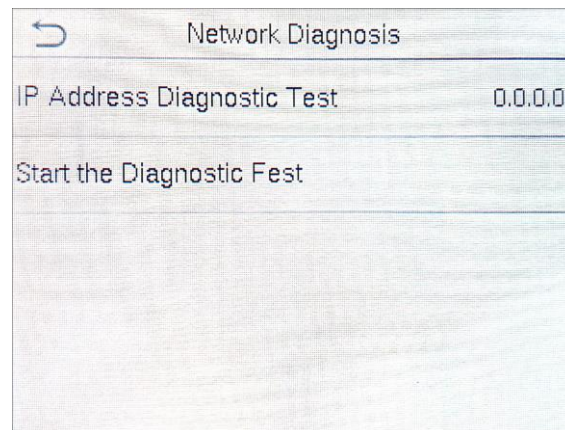


Item	Description
Enable Domain Name	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	Server Address IP address of the ADMS server.
	Server Port Port used by the ADMS server.
Enable Proxy Server	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.
HTTPS	Enable or disable HTTPS.

5.5 Network Diagnosis

To set the network diagnosis parameters.

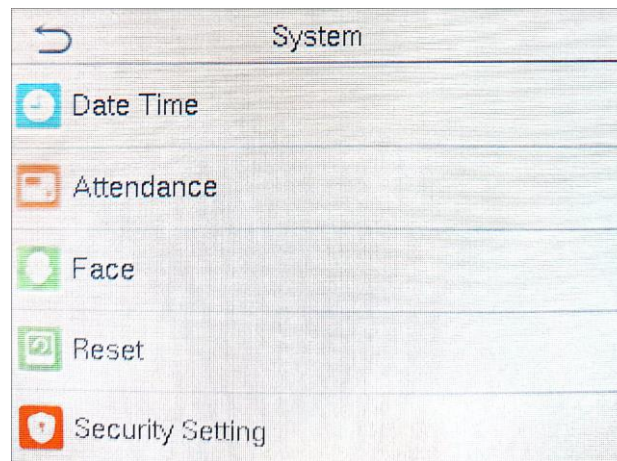
Click **Network Diagnosis** on the **Comm. Settings** interface. Enter the IP address that needs to be diagnosed and click **Start the Diagnostic Test** to check whether the network can connect to the device.



6 System

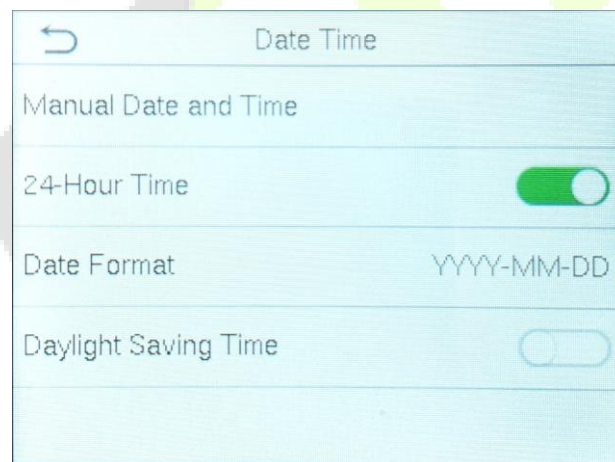
Set related system parameters to optimize the performance of the device.

Click **System** on the **Main Menu** interface to get into its menu options.



6.1 Date and Time

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



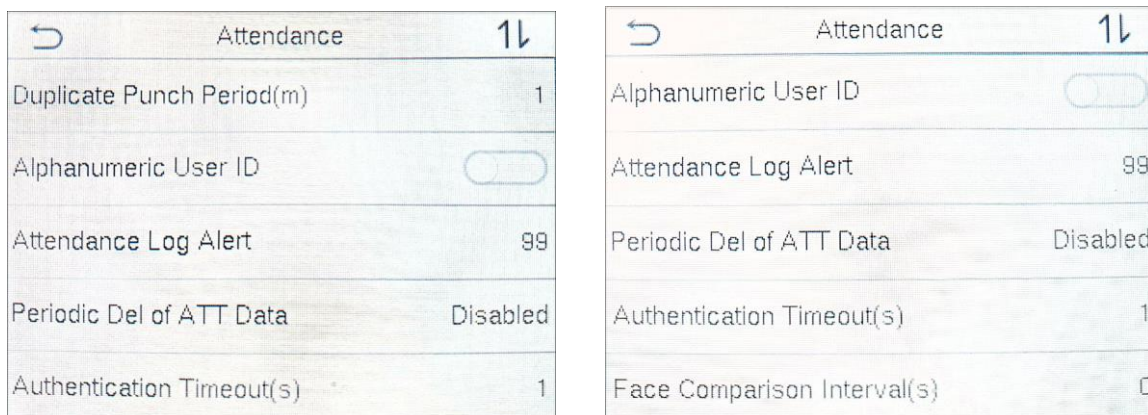
1. You can manually set date and time and click Confirm to save.
2. Tap the toggle **24-Hour Time** to enable or disable this format and select the date format.
3. Tap on toggle to enable or disable **Daylight Saving Time**. If enabled, select a daylight-saving mode and set the switch time like By Date/Time and By Week/Day.

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

Note: For example, the user sets the time of the device (18:35 on March 15, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

6.2 Attendance Parameters

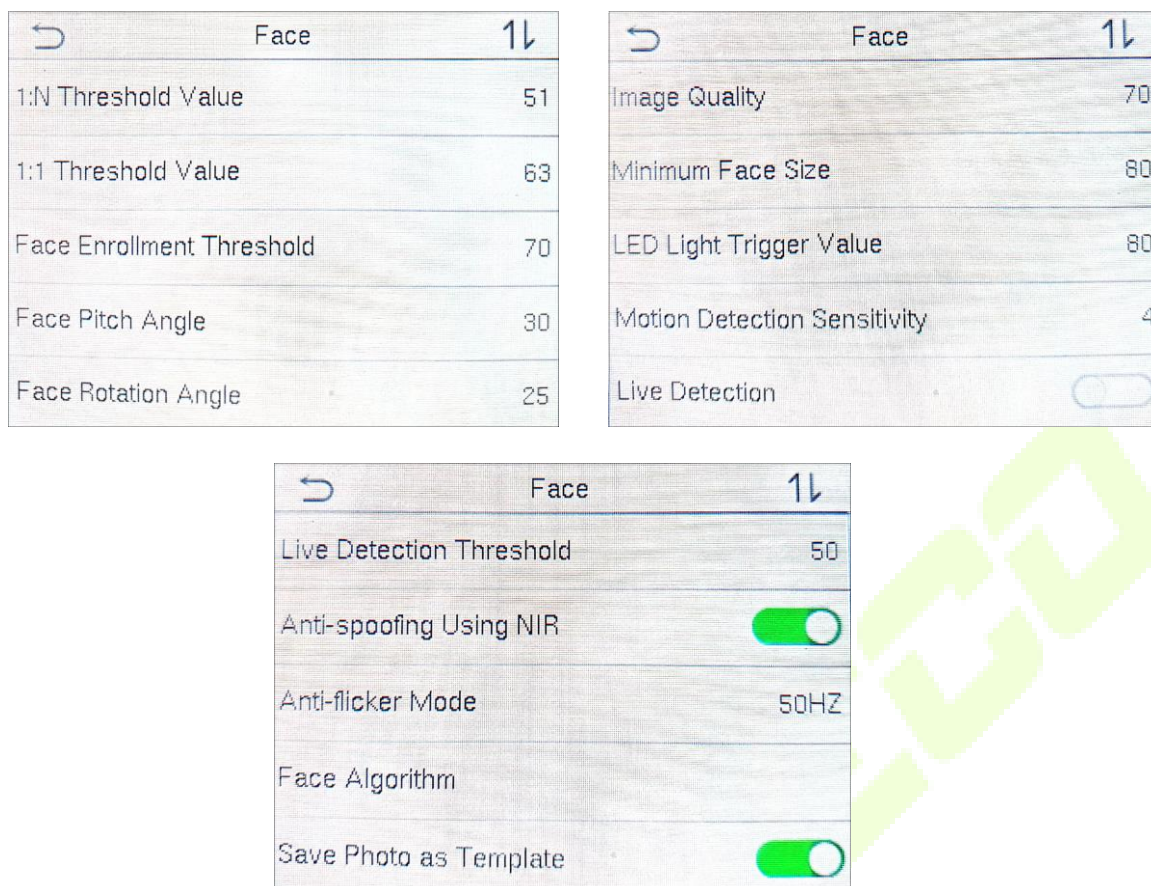
Click **Attendance** on the System interface.



Menu Item	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).
Alphanumeric User ID	Alphanumeric User ID can be enabled or disabled as required.
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 ATT Data	When attendance records reach its maximum storage capacity, the device automatically deleted a set of old attendance records. Users can disable the function or set a valid value between 1 to 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
Face Comparison Interval (s)	To set the face comparison interval as required, within the range of 0-9 s.

6.3 Face

Click **Face** on the System interface.



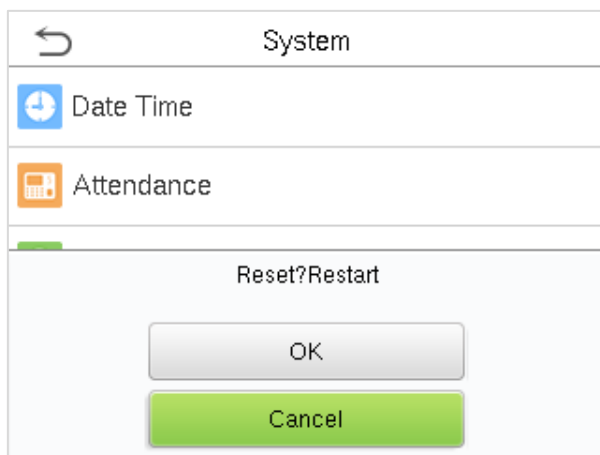
Item	Description
1: N Threshold Value	Under 1: N verification method, the verification will only be successful when the similarity between the acquired face data enrolled in the device is greater the set value. Value range is 0 to 100.
1:1 Threshold Value	The verification will only be successful when the similarity between the acquired face data enrolled in the device is greater the set value. Value range is 0 to 100.
Face Enrollment Threshold	During face enrollment, 1: N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison. If a face’s pitch angle exceeds this set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face’s rotation angle exceeds this set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.

Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Minimum Face Size	Required for facial registration and comparison. If an object's size is smaller than this set value, the object will be filtered and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Trigger Value	This value controls the ON and OFF of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitivity	A measurement of the amount of change in a camera's field of view that qualifies as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface is much easier and frequently triggered.
Live Detection	Detecting a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation using visible light images.
Live Detection Threshold	Helping to judge whether the visible image comes from an alive body. The larger the value, the better the visible light anti-spoofing performance.
Anti-Spoofing Using NIR	Enable or disable Anti-spoofing using NIR by tapping on toggle as required.
Anti-flicker Mode	Set an Anti-Flicker mode for 50HZ or 60HZ.
Face Algorithm	Set a Face Algorithm as Major Ver-3.5, Minor Ver-4 or select Pause Facial Template Update to stop from current face template usage.
Save Photo as Template	Enable or disable the function Save photo as template.

6.4 Reset

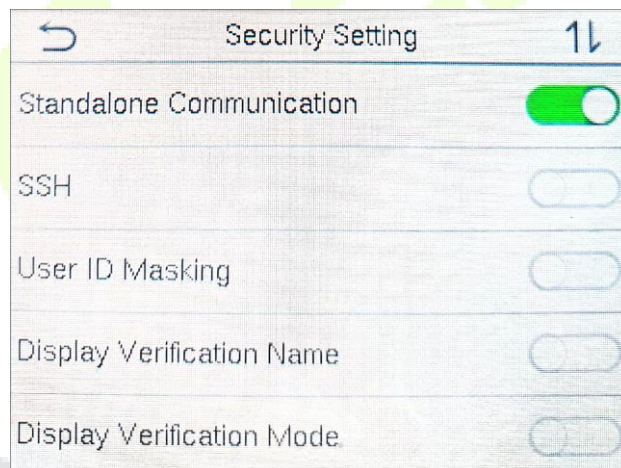
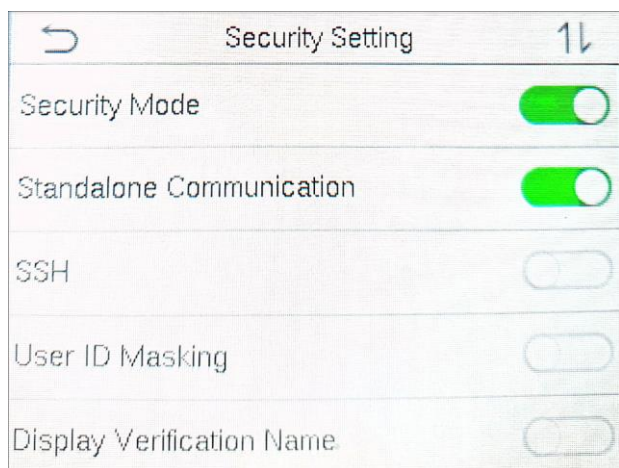
Restore the device, such as communication settings and system settings, to factory settings (Do not clear registered user data).

Click **Reset** on the System interface.



Click **OK** to reset.

6.5 Security Setting

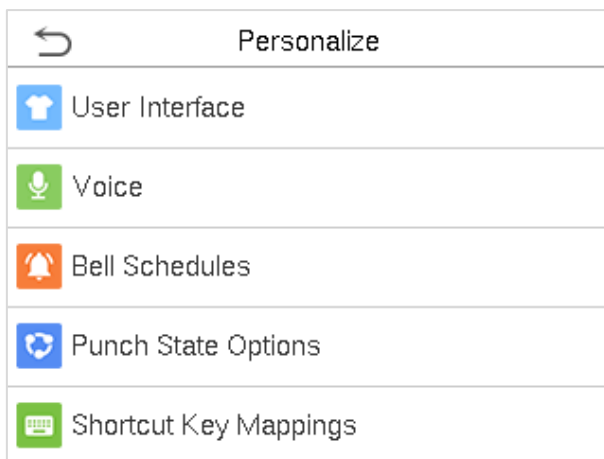


Item	Description
Security Mode	Select whether to enable the security mode to protect the device and the user’s personal information. You can set the device to work offline and hide he user’s personal information to prevent leakage during user verification.
Standalone Communication	TO avoid being unable to use when the device is offline, you can download the C/S software on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified the User ID in the displayed verification result will be replaced to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.

7 Personalize Settings

You may customize interface settings, audio, and bell.

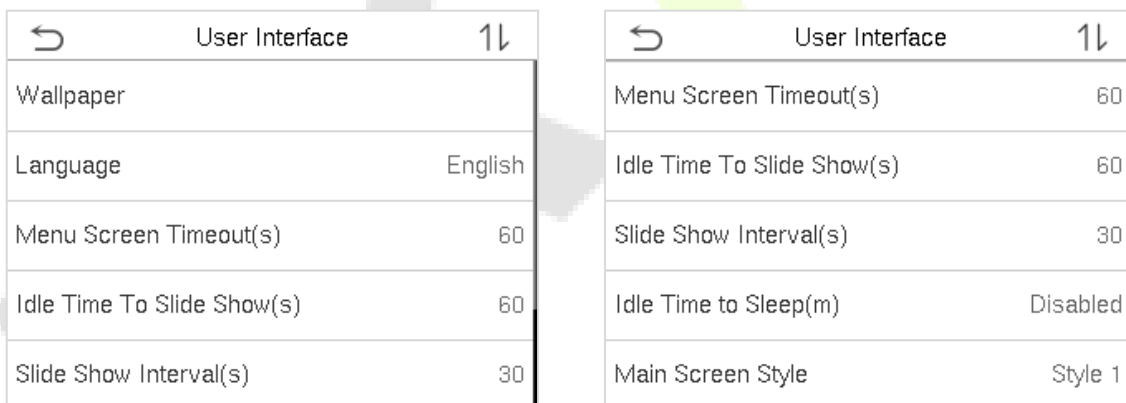
Click **Personalize** on the main menu interface.



7.1 User Interface Settings

You can customize the display style of the main interface.

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

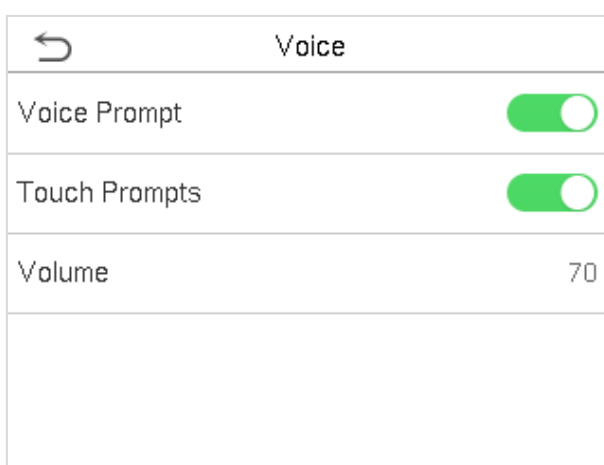


Item	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.

Slide Show Interval (s)	This refers to the time interval switching different 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 you have activated the sleep mode, when there is no operation, the device will enter 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 Settings

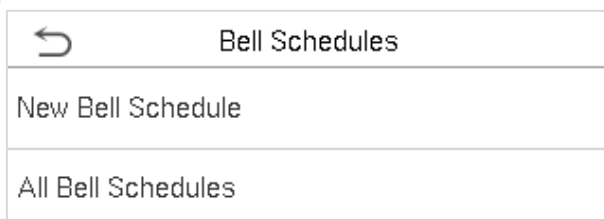
Click **Voice** on the Personalize interface.



Item	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

7.3 Bell Schedules

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



- **Add a bell:**

1. Click **New Bell Schedule** to enter the adding interface:

New Bell Schedule	
Bell Status	<input checked="" type="checkbox"/>
Bell Time	
Repeat	Never
Ring Tone	bell01.wav
Internal bell delay(s)	5

Item	Description
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

2. Return to the Bell Schedules interface, and click on All **Bell Schedules** to view the newly added bell.

- **Edit a bell:**

On the All-Bell Schedules interface, tap the bell to be edited.

Click **Edit**, the editing method is the same as the operations of adding a bell.

- **Delete a bell:**

On the All-Bell Schedules interface, tap the bell to be deleted.

Tap **Delete** and select **Yes** to delete the bell.

7.4 Punch State Options

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

Punch State Options	
Punch State Mode	Manual and Auto Mode
Punch State Timeout(s)	10
Punch State Required	<input type="checkbox"/>

Item	Description
Punch State Mode	<p>Select a punch state mode, which can be:</p> <p>Off: To disable the punch state key function. The punch state key set under Shortcut Key Mappings menu will become invalid.</p> <p>Manual Mode: To switch the punch state key manually, and the punch state key will disappear after Punch State Timeout.</p> <p>Auto Mode: After this mode is chosen, set the switching time of punch state key in Shortcut Key Mappings; when the switching time is reached, the set punch state key will be switched automatically.</p> <p>Manal and Auto Mode: Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After timeout, the manually switching punch state key will become auto-switching punch state key.</p> <p>Manual Fixed Mode: After punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time.</p> <p>Fixed Mode: Only the fixed punch state key will be shown, and it cannot be switched.</p>
Punch State Timeout (s)	The time of one punch state displays. The punch state will disappear or switch to other punch states as the time is out. The value is 5~999 seconds.
Punch State Required	Set whether to select punch state during verification.

7.5 Shortcut Keys Mappings

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

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

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

F1	
Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	

Item	Description
Punch State Value	Set punch state value for the limit. Valid value:0 to 250.
Function	Function can be set to an option like Undefined, Punch State Options, New User, All Users, and Ethernet.
Name	Set name to either User Defined or Check-In.

2. If the key is defined as a function key, the setting is completed; If set to a punch state key, set the punch state

value (valid value 0~250), the name and switch time.

How to set the switch time?

The switch time is used in conjunction with the punch state options. When the punch state mode is set to auto

mode, the switch time should be set. Select the switch period and set the switch time every day, as shown in the

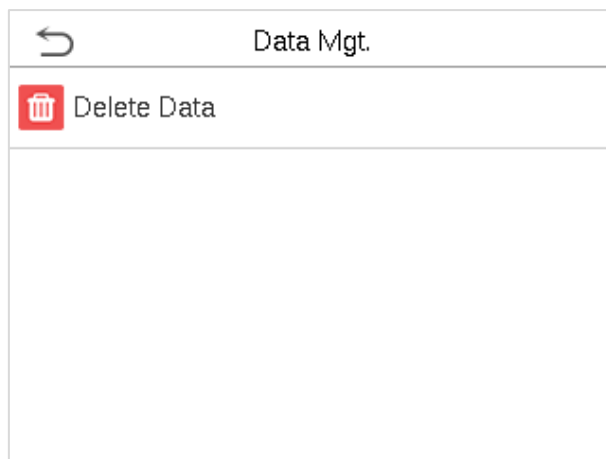
figure below:

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

8 Data Management

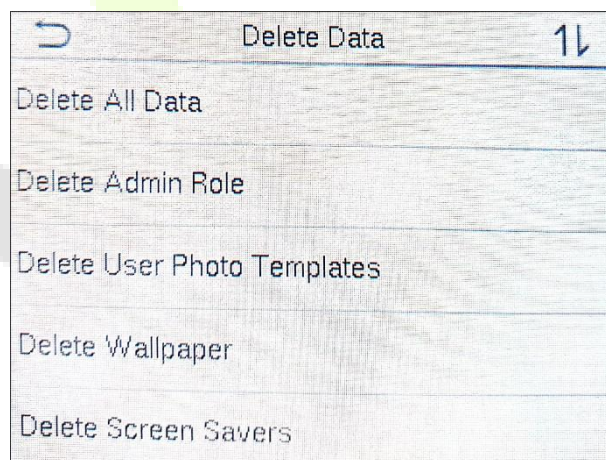
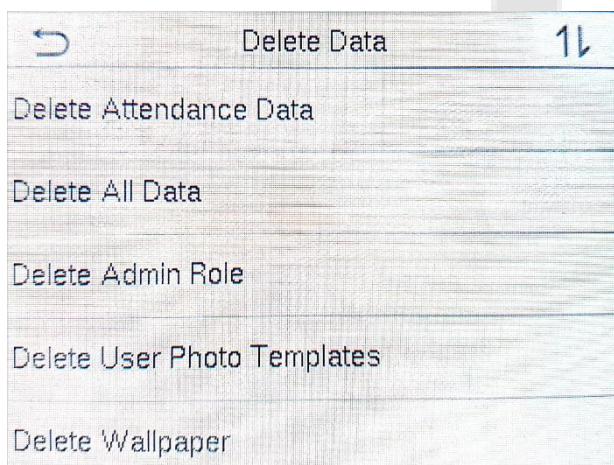
To delete the relevant data in the device.

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



8.1 Delete Data

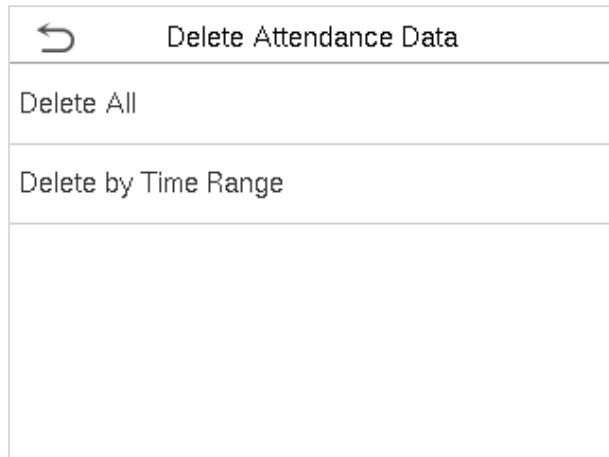
Click **Delete Data** on the Data Mgt. interface.



Menu Item	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete All Data	To delete all user information, fingerprints, and attendance logs etc.
Delete Admin Role	To make all Administrators become Normal Users.
Delete User Photo Templates	To delete all user photo templates in the device.
Delete Wallpaper	To delete all wallpapers in the device.

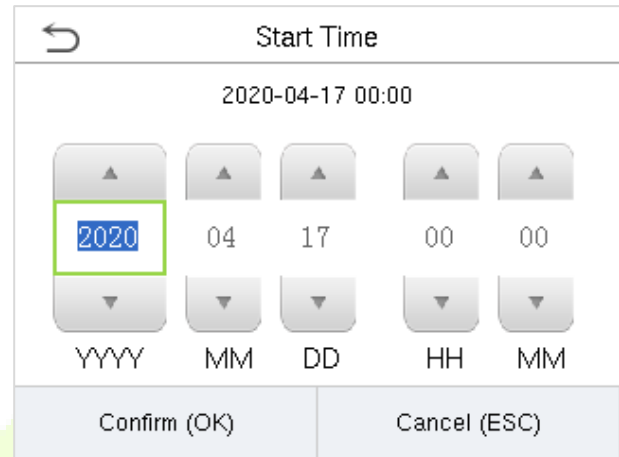
Delete Screen Savers	To delete all screen savers in the device.
-----------------------------	--

Note: When deleting 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.



← Delete Attendance Data
Delete All
Delete by Time Range

Select Delete by Time Range.

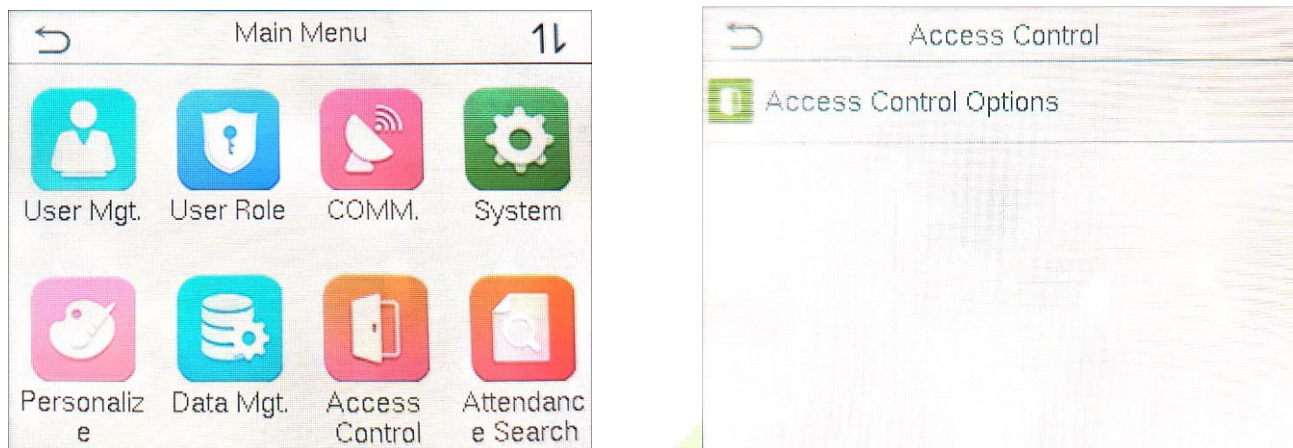


← Start Time				
2020-04-17 00:00				
▲	▲	▲	▲	▲
2020	04	17	00	00
▼	▼	▼	▼	▼
YYYY	MM	DD	HH	MM
Confirm (OK)		Cancel (ESC)		

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

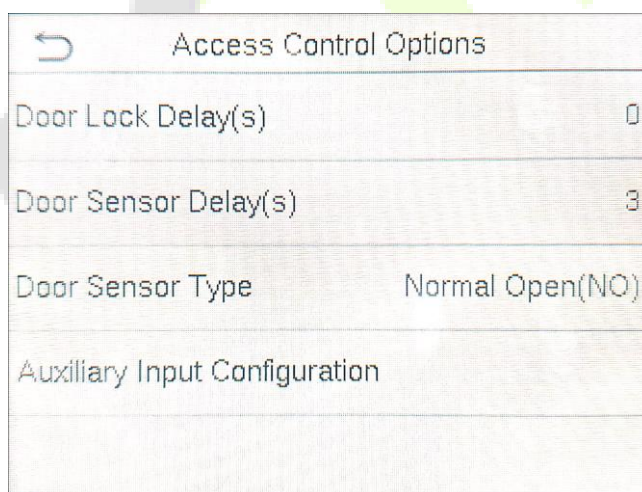
9 Access Control

In the **Main Menu**, tap on **Access Control** to set the parameters of the door locks and the relevant access control options.



9.1 Access Control Options

Tap on **Access Control Options** in the **Access Control** interface to set the parameters like Door Lock Delay(s), Door Sensor Delay(s), Door Sensor Type, and Auxiliary Input Configuration.



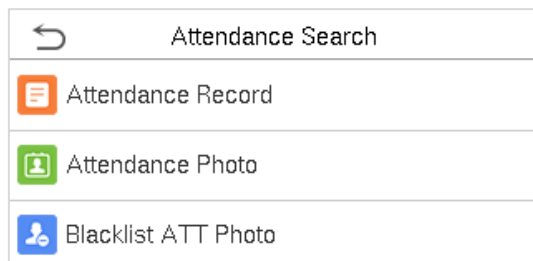
Item	Description
Door Lock Delay(s)	To set the duration of time (seconds) that the device controls the electric lock to be in unlock state. Valid Value Range: 1 to 10 seconds.
Door Sensor Delay(s)	If the door is not locked and is left open even after a standard time duration to lock, an alarm will be triggered. Valid Value Range: 1 to 255 seconds.
Door Sensor Type	There are three Sensor Types: Normal Open (NO), Normal Close (NC), and None.

	<p>Normal Open (NO): This sensor type is to set the door to be always open when electric power is on.</p> <p>Normal Close (NC): This sensor type is to set the door to be always closed when electric power is on.</p> <p>None: This sensor type is to set when the door is not in use.</p>
Auxiliary Input Configuration	<p>There are two options to set up Auxiliary Input Configuration:</p> <p>Aux Output/Lock Open Time(s): To set the time in seconds for Lock open or Aux output.</p> <p>Valid Value Range: 1 to 255 seconds.</p> <p>Aux Output Type Settings: To set the type of Aux output as either None or Trigger Door Open.</p>

10 Attendance Search

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

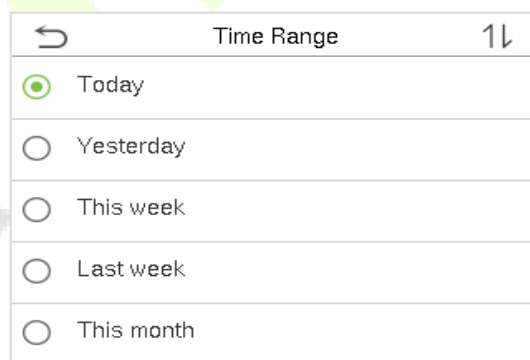
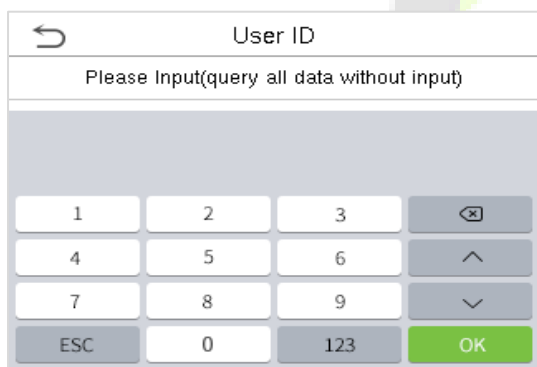
Click **Attendance Search** on the main menu interface.



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

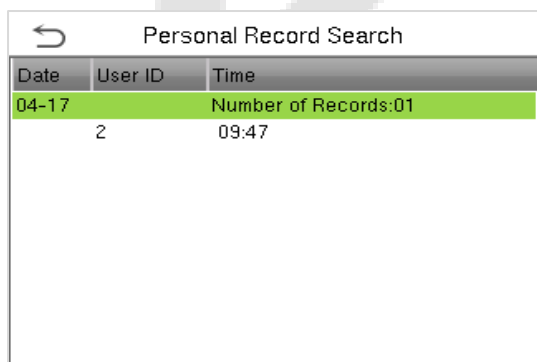
On the Attendance Search interface, click **Access Records**.

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



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

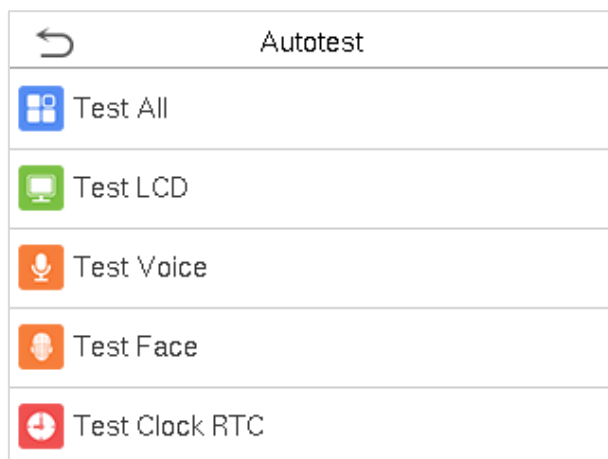
4. The below figure shows the details of the selected record.



11 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, audio, camera, and real-time clock (RTC).

Click **Auto test** on the main menu interface.

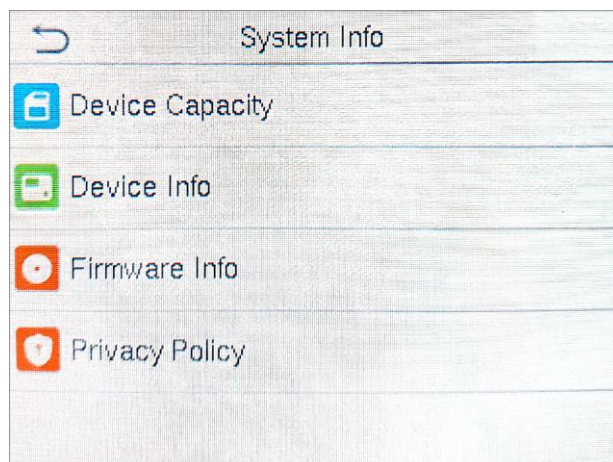


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays color normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Face	To test if the camera lens and camera functions properly by checking the photos taken are clear for use.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

12 System Information

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

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



Item	Description
Device Capacity	Displays the current device's user storage, palm, password and face storage, administrators, access records, attendance and blacklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm version information, platform information, and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy policy	Displays the Privacy policy of product and service.

13 Connect to easyTimepro Software

13.1 Set the Communication Address

- **Device Side:**

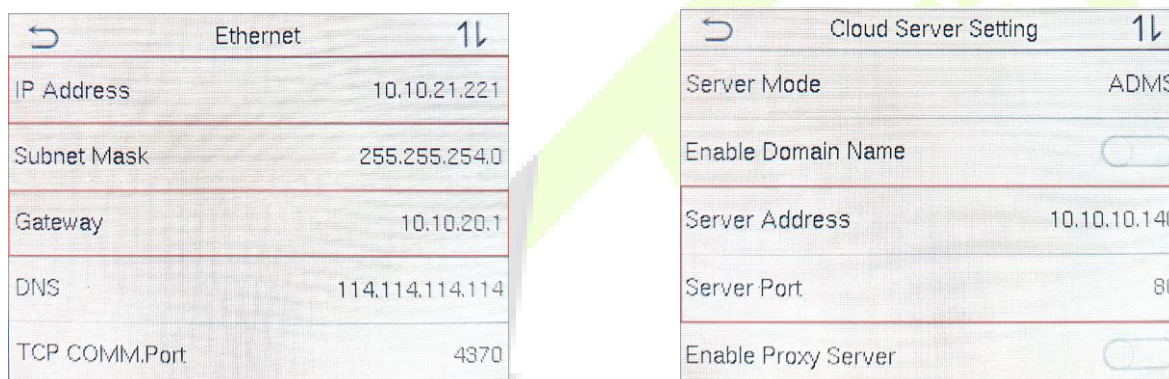
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

(Note: The IP address should be able to communicate with the easyTimePro 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 easyTimePro server.

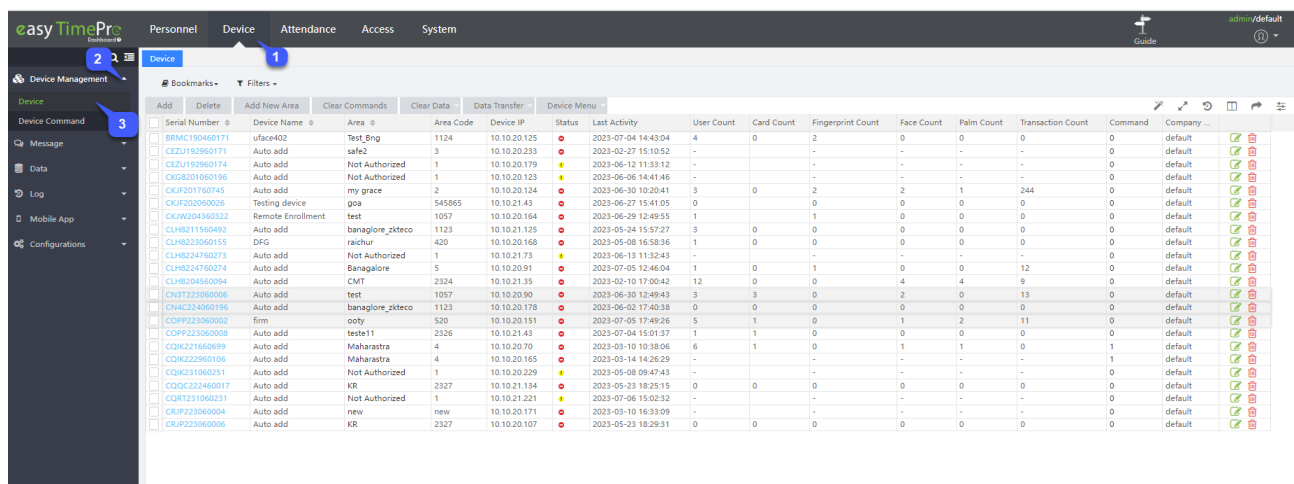
Server port: Set the server port as of easyTimePro (The default is 80).



Serial Number	Device Name	Area	Area Code	Device IP	Status	Last Activity	User Count	Card Count	Fingerprint Count	Face Count	Palm Count	Transaction Count	Command	Company
BRMC190460171	uface402	Test_Bng	1124	10.10.20.125	●	2023-07-04 14:43:04	4	0	2	0	0	0	0	default
CEZU192960171	Auto add	safe2	3	10.10.20.233	●	2023-02-27 15:10:52	-	-	-	-	-	0	0	default
CEZU192960174	Auto add	Not Authorized	1	10.10.20.179	●	2023-06-12 11:33:12	-	-	-	-	-	0	0	default
CKG6201080198	Auto add	Not Authorized	1	10.10.20.123	●	2023-06-06 14:41:46	-	-	-	-	-	0	0	default
CKG201160195	Auto add	my grace	2	10.10.20.124	●	2023-06-30 10:20:41	3	0	2	2	1	244	0	default
CKG202060026	Testing device	goa	545865	10.10.21.43	●	2023-06-27 15:41:05	0	0	0	0	0	0	0	default
CKW204360322	Remote Enrollment	test	1057	10.10.20.164	●	2023-06-29 12:49:55	1	0	1	0	0	0	0	default
CLH8211560492	Auto add	banaglore_ziteco	1123	10.10.21.125	●	2023-05-24 15:57:27	3	0	0	0	0	0	0	default
CLH8223060155	DFG	rachur	420	10.10.20.168	●	2023-05-08 16:58:36	1	0	0	0	0	0	0	default
CLH8230160273	Auto add	Not Authorized	1	10.10.21.175	●	2023-06-13 11:32:43	-	-	-	-	-	0	0	default
CLH8224760274	Auto add	Banagalore	5	10.10.20.91	●	2023-07-05 12:46:04	1	0	1	0	0	12	0	default
CLH8204560094	Auto add	CMT	2324	10.10.21.35	●	2023-02-10 17:00:42	12	0	0	4	4	9	0	default
CN3T223060006	Auto add	test	1057	10.10.20.90	●	2023-06-30 12:49:43	3	3	0	2	0	13	0	default
CN4C224060198	Auto add	banaglore_ziteco	1123	10.10.20.178	●	2023-06-02 17:40:38	0	0	0	0	0	0	0	default
COP9223060002	Firm	cofy	520	10.10.20.151	●	2023-07-05 17:49:26	5	1	0	1	2	11	0	default
COP9223060008	Auto add	test+1	2326	10.10.21.43	●	2023-07-04 15:01:37	1	1	0	0	0	0	0	default
CQK2231060099	Auto add	Maharashtra	4	10.10.20.70	●	2023-03-10 10:38:06	6	1	0	1	1	0	1	default
CQK222960106	Auto add	Maharashtra	4	10.10.20.165	●	2023-03-14 14:26:29	-	-	-	-	-	-	-	1
CQK231060251	Auto add	Not Authorized	1	10.10.20.229	●	2023-05-08 09:47:43	-	-	-	-	-	-	-	0
CQK2230480017	Auto add	KB	2327	10.10.21.154	●	2023-05-23 18:23:15	0	0	0	0	0	0	0	default
CQK231060031	Auto add	Not Authorized	3	10.10.21.321	●	2023-07-06 15:02:32	-	-	-	-	-	-	-	0
CRP223060004	Auto add	new	new	10.10.20.171	●	2023-05-10 16:33:09	-	-	-	-	-	-	-	0
CRP223060006	Auto add	KR	2327	10.10.20.107	●	2023-05-23 18:29:31	0	0	0	0	0	0	0	default

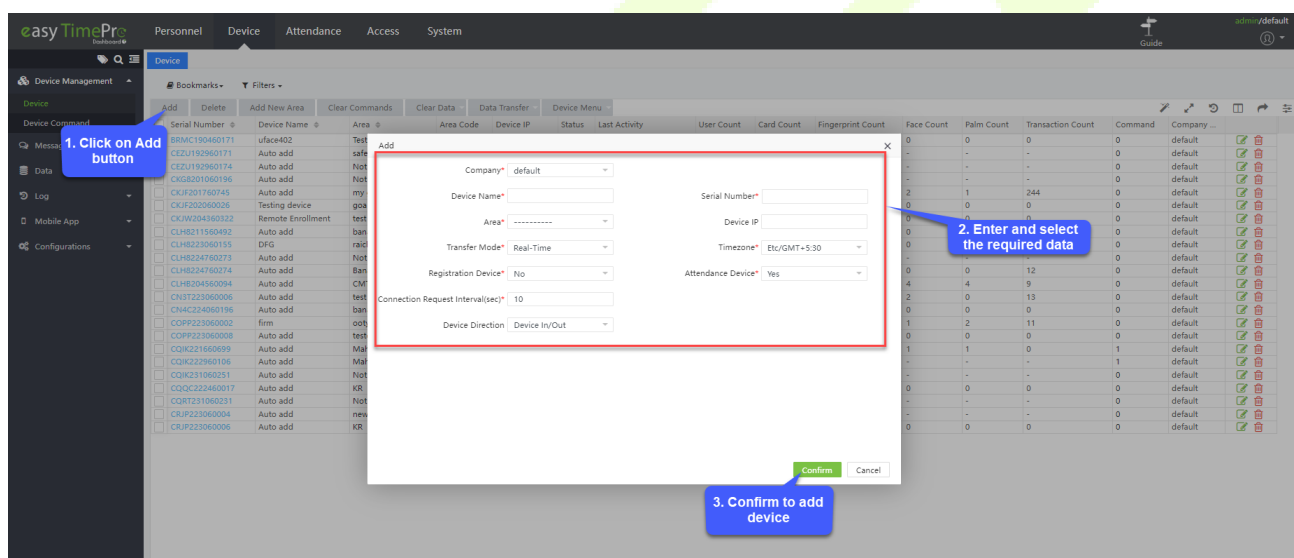
- **Software side**

Login to easyTimePro software, click **Device** > **Device Management** > **Device** to add Device on the Software.



● Add device Manually in the Software:

1. Click **Add** button to enter the **Add Device** interface.



Set the parameters as required. The parameter with *, means cannot be empty.

Company: Select the company name that device belongs to from the drop-down list. By default, the company name will get. It displayed as default when there is no Company added.

Device Name: Enter the unique Device Name.

Serial Number: Enter the Device Serial Number.

Device IP: Enter the Device IP specified in the Device, under Network Settings.

Area: Select the mounted Area name of the Device from the drop-down list.

Time zone: Select the common standard time of the specified Area from the drop-down list.

Registration Device: Select from the drop-down list whether the Device is for User Registration or not.

Attendance Device: Select from the drop-down list whether the Device is for tracking Attendance or not.

Connection Request Interval: Enter the time-interval for the Device's pulse oscillation.

Transfer mode: Select from the drop-down list whether to transfer the Device data in real-time or to be sent at the predefined time.

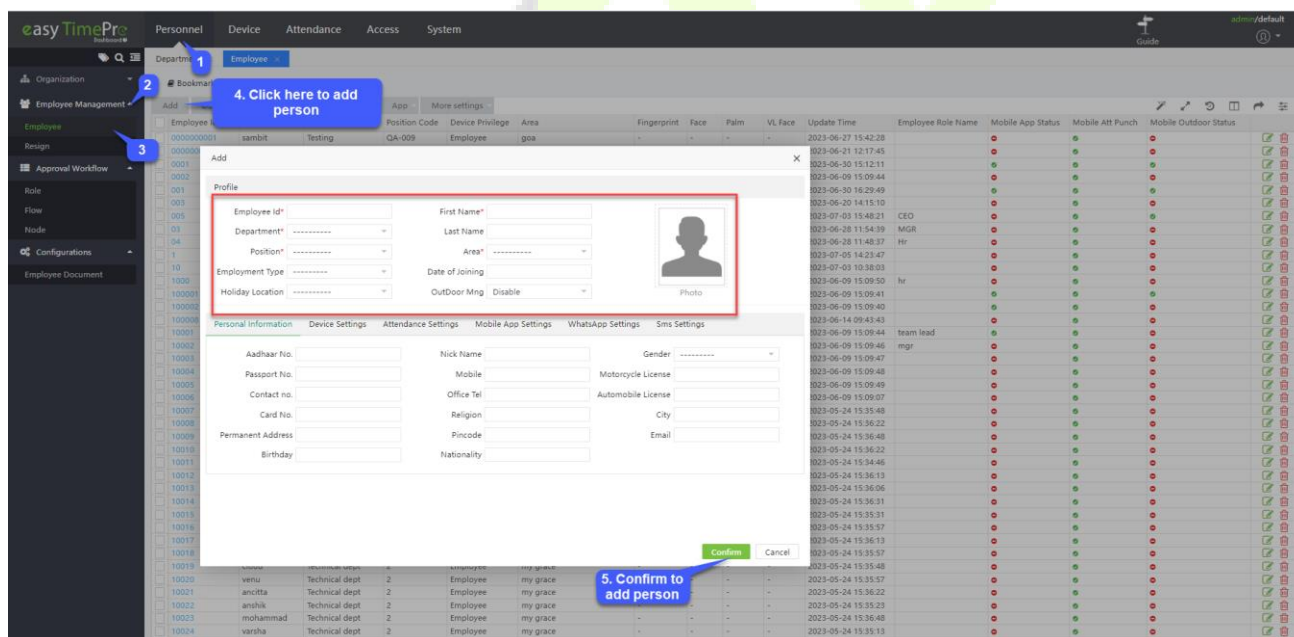
Device Direction: Select an option to direct a device as Device In/Out, In Device, and Out Device.

Click Confirm to save the newly mounted Device to the software.

13.2 Add Person on the Software

Add personal info and issue card as required. The specific operation is shown below:

1. Click **Add** button to enter the **Add Employee** interface.



Note: The parameter with * cannot be empty.

Employee ID: Enter unique employee ID, (Not repeatable).

First Name, Last Name, Email: Enter the employee's first name, last name and email address as required.

Department: Click ▼ button and select the subordinate department in the drop-down department list.


Position: Select the Organization Position or the designation of the Employee from the drop-down list.


Employment Type: Select the required Employment Type Permanent or Temporary for the Employee, based on the Employment discussion.


Date of joining: Choose the date of joining or the joined date of the Employee from the calendar.

Photo: Click on the photo to upload the image of the Employee.

Supports two kinds of method to add photo info for the employee:

Method 1: Click  icon, double-click and select file in the pop-up window, add a photo for the employee.

(**Tips:** The size of the employee photo must be in the scope of 200*200. You can click  icon to delete the added employee photo.)

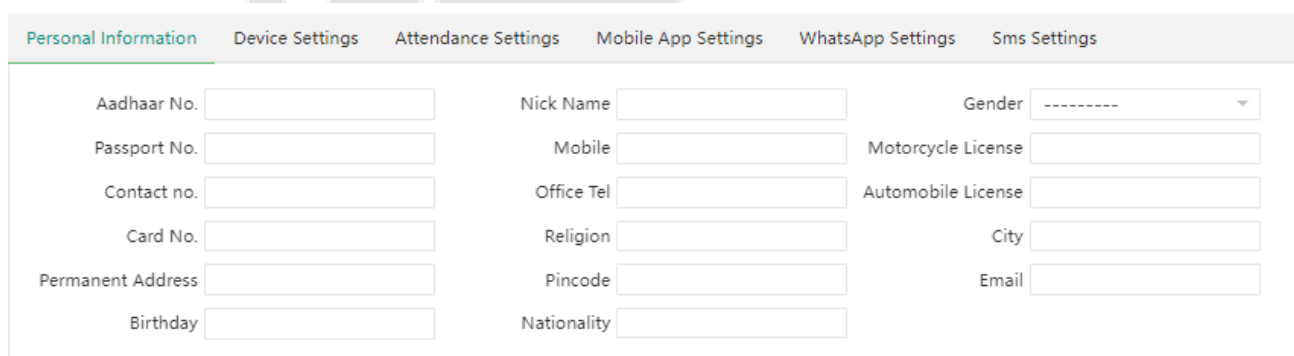
Method 2: If the computer is connected with a video camera, you can click  icon, and add a photo for the employee via camera photograph.

Holiday Location: Location of the employee where he is working.

Outdoor Management: This function is for the employees who visit the client's place for business/service purposes. It tracks the attendance and location of the employees who have been to the client's location. It is primarily used by sales, support, service teams when comparing to other teams.

● **Personal Information**

Click **Personal Detail** tag to enter the **Personal Detail** setting interface.



Aadhaar No: Enter the Employee's 12-digit unique identification Aadhaar number issued by the government.

Gender: Select the sociocultural expression of the Employee from the drop-down list.

Passport No.: Enter the Employee's official travel document number issued by the government.

Motorcycle License: Enter the Employee's driving authorization number issued by the government.

Automobile License: Enter the Employee's driving authorization number issued by the government.

Contact No.: Enter the personal or official contact number of the Employee.

Mobile: Enter the alternative or the wireless cellular phone number of the Employee.

Nationality: Enter the legal Nation or the Country name of the Employee.

City: Enter the Employee's city name.

Permanent Address: Enter the Employee's permanent address.

Email: Enter the Employee's official Email ID.

Birthday: Enter the Employee's birth date. User can generate the Birthday report in Attendance Module.

Office Tel: Enter the Employee's Office desk contact number.

Religion: Enter the religious practice of the Employee.

Pin Code: Enter the postal code number of the Employee.

Card No: Enter the given card number.

2. Fill in all the required fields and click **[OK]** to register a new user.
3. Click **Device > Device Management > Device > Data Transfer > Synchronize Data to Devices** to synchronize all the data to the device including the new users.

Appendix 1

Requirements of Live Collection and Registration of Visible

Light Face Images

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



Image1 Face Capture Area

Requirements for Visible Light Digital Face Image Data

Digital photo should be straightly edged, coloured, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

- **Eye Distance**

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

- **Facial Expression**

Plain face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

Horizontal rotating angle should not exceed $\pm 10^\circ$, elevation should not exceed $\pm 10^\circ$, and depression angle should not exceed $\pm 10^\circ$.

- **Accessories**

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

- **Face**

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

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

- 1) White background with dark-coloured apparel.
- 2) 24bit true color mode.
- 3) JPG format compressed image with not more than 20kb size.
- 4) Definition rate between 358 x 441 to 1080 x 1920.
- 5) The vertical scale of head and body should be 2:1.
- 6) The photo should include the captured person's shoulders at the same horizontal level.
- 7) The captured person should be eyes-open and with clearly seen iris.
- 8) Plain face or smile is preferred, showing teeth is not preferred.
- 9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

Appendix 2

Statement on the Right to Privacy

Dear Customers:

Thank you for choosing this hybrid biometric recognition product, which was designed and manufactured by ZKTeco. As a world-renowned provider of core biometric recognition technologies, we are constantly developing and researching new products, and strive to follow the privacy laws of each country in which our products are sold.

We Declare That:

1. All of our civilian fingerprint recognition devices capture only characteristics, not fingerprint images, and do not involve privacy protection.
2. None of the fingerprint characteristics that we capture can be used to reconstruct an image of the original fingerprint and does not involve privacy protection.
3. As the provider of this device, we will assume no direct or indirect responsibility for any consequences that may result from your use of this device.
4. If you would like to dispute human rights or privacy issues concerning your use of our product, please directly contact your dealer.

Our other law-enforcement fingerprint devices or development tools can capture the original images of citizen's fingerprints. As to whether this constitutes an infringement of your rights, please contact your government or the final supplier of the device. As the manufacturer of the device, we will assume no legal liability.

Note:

The Indian law includes the following provisions on the personal freedom of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons.
2. Personal dignity is related to personal freedom and shall not be infringed upon.
3. A citizen's house may not be infringed upon.
4. A citizen's right to communication and the confidentiality of that communication is protected by the law.

As a final point, we would like to further emphasize that biometric recognition is an advanced technology that will be certainly used in E-commerce, banking, insurance, judicial, and other sectors in the future. Every year the world is subjected to major losses due to the insecure nature of passwords. The Biometric products serve to protect your identity in high-security environments.

Eco-friendly Operation



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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

Zkteco India Global R&D Centre

J P Pride, Survey #55. **Khata** #503/499/5,

Puttapa Industrial estate, Mahadevapura,

Bangalore-560048, Karnataka.

Phone:080 68281342

www.zkteco.in

Copyright © 2023 ZKTECO CO., LTD. All Rights Reserved.

