eSSL®
Security at Fingertips

MANUAL

AIFACE ERIS

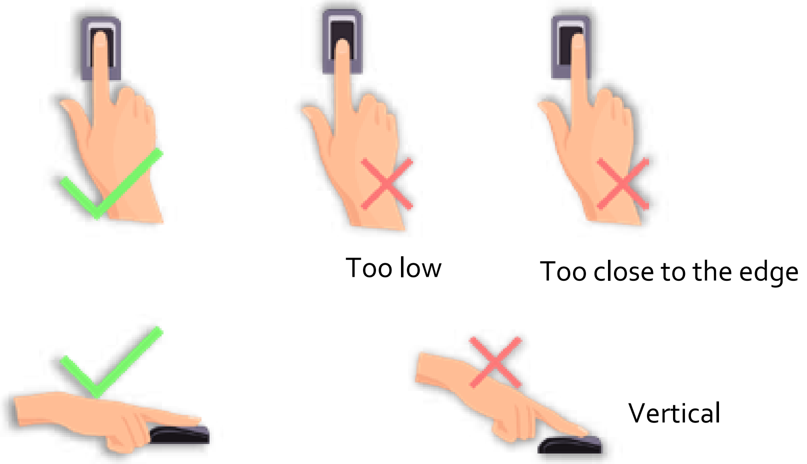
TABLE OF CONTENTS

1 Instruction for Use

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

1.1 Finger Positioning

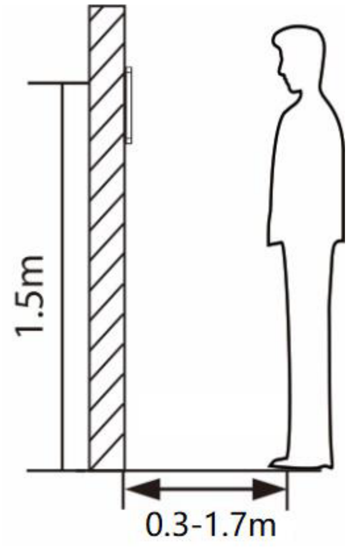
Recommended fingers: The index, middle, or ring fingers are recommended fingers to use, and avoid using the thumb or pinky, as they are difficult to position correctly onto the fingerprint reader.



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

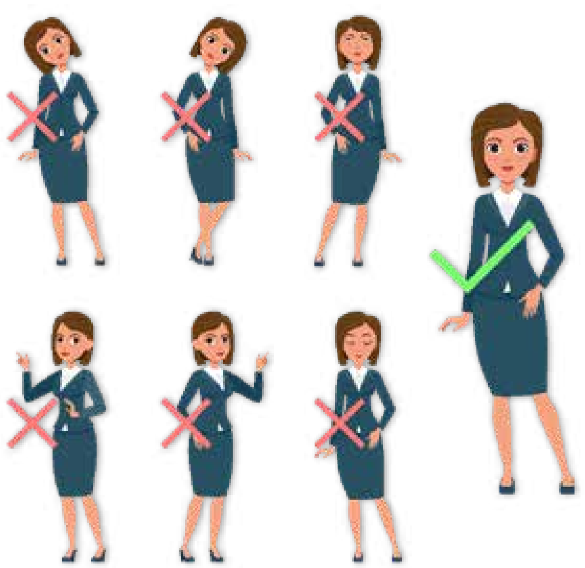
1.2 Standing Position, Posture and Facial Expression

- **The recommended distance**



The distance between the device and a user whose height is in a range of 1.55 m to 1.85 m is recommended to be 0.3 m to 1.7 m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended standing posture and facial expression:**



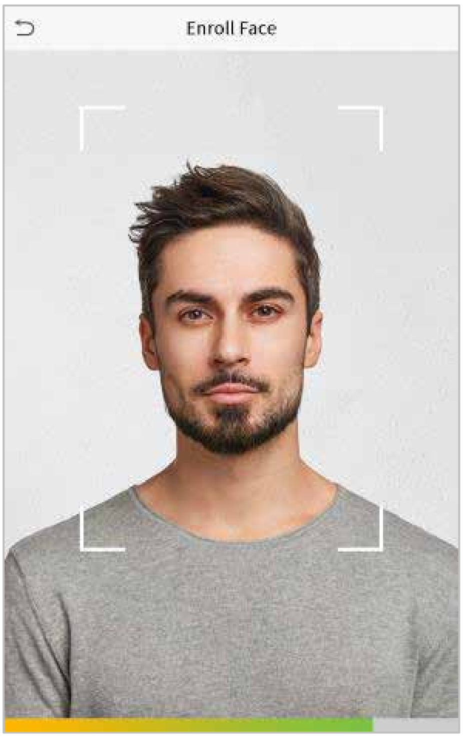
Standing Posture

Facial Expression

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

1.3 Face Template Registration

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

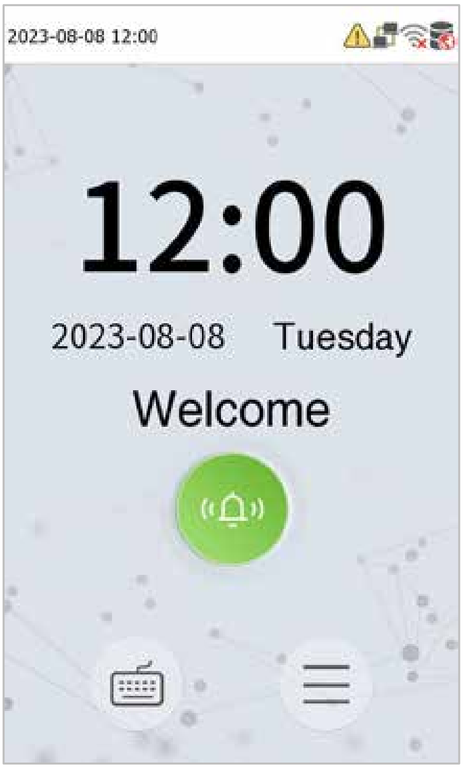


Correct face template registration and authentication method

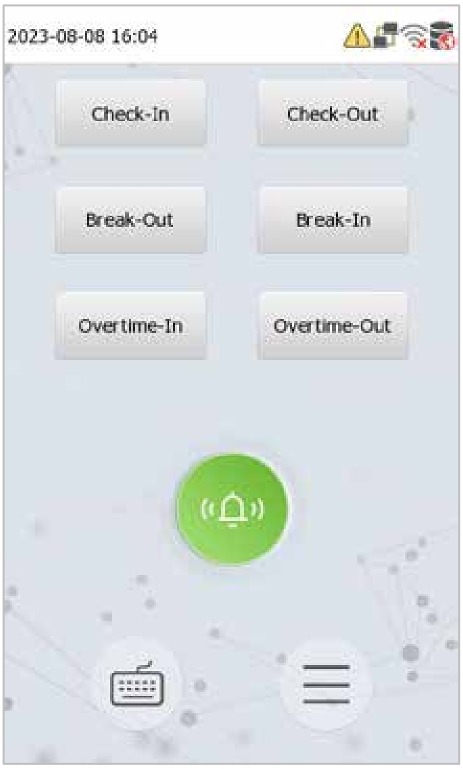
- **Recommendation for Registering a Face Template**
  - When registering a face template, maintain a distance of 40 cm to 80 cm space between the device and the face template.
  - Be careful not to change your facial expression. (Smiling face template, drawn face template, wink, etc.)
  - If you do not follow the instructions on the screen, the face template registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two face templates on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both face templates with and without glasses.
- **Recommendation for Authenticating a Face Template**
  - Ensure that the face template appears inside the guideline displayed on the screen of the device.
  - If the glasses have been changed, authentication may fail. If the face template without glasses has been registered, authenticate the face template without glasses further. If the face template with glasses has been registered, authenticate the face template with the previously worn glasses.
  - If a part of the face template is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face template, allow the device to recognize both the eyebrows and the face template.

1.4 Standby Interface

After connecting the power supply, the following standby interface template is displayed:



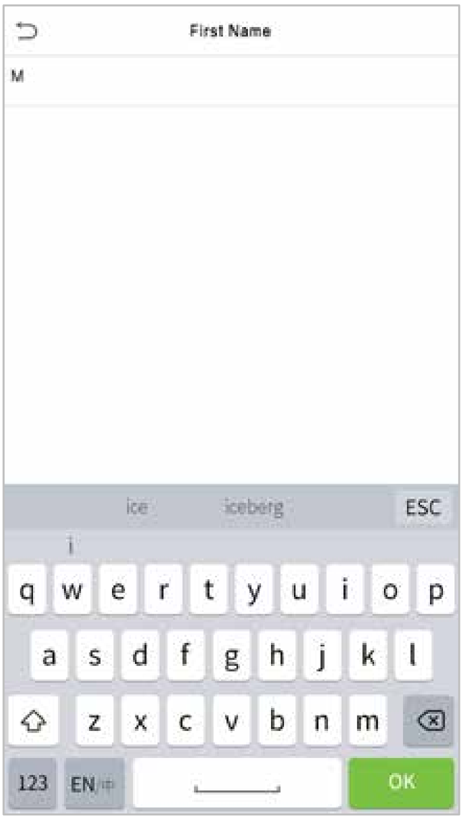
- Click ⌨ icon to enter the User ID input interface template.
- When there is no Super Administrator set in the device, tap ☰ con to go to the menu.
- After setting the Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.
- **Note**: For the security of the device, it is recommended to register super administrator the first time you use the device.
- On the standby interface template, the punch state options can also be shown and used directly. Click anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green.

Note: The punch state options are off by default and need to be changed to other option in the "7.4 Punch States Options" to get the punch state options on the standby screen.

1.5 Virtual Keyboard



Note:

The device supports the input in Chinese language, English language, numbers, and symbols.

- Click **En** to switch to the English keyboard.
- Press **123** to switch to the numeric and symbolic keyboard.
- Click **ABC** to return to the alphabetic keyboard.
- Click the input box, virtual keyboard appears.
- Click **ESC** to exit the virtual keyboard.

1.6 Verification Mode

1.6.1 Fingerprint Verification

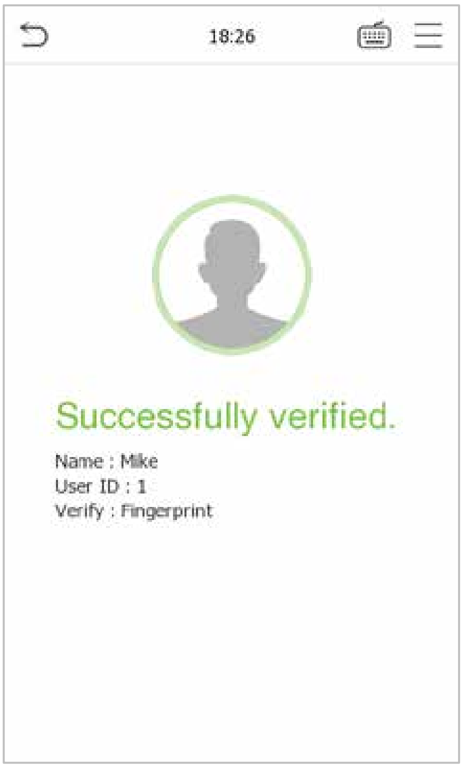
- **1: N Fingerprint Verification Mode**

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

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

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

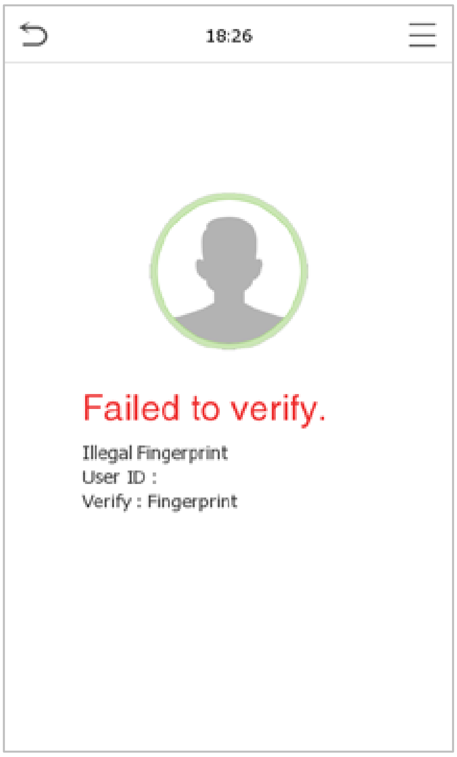
Verification is successful:



Successfully verified.

Name : Mike
User ID : 1
Verify : Fingerprint

Verification is failed:



Failed to verify.

Illegal Fingerprint
User ID :
Verify : Fingerprint

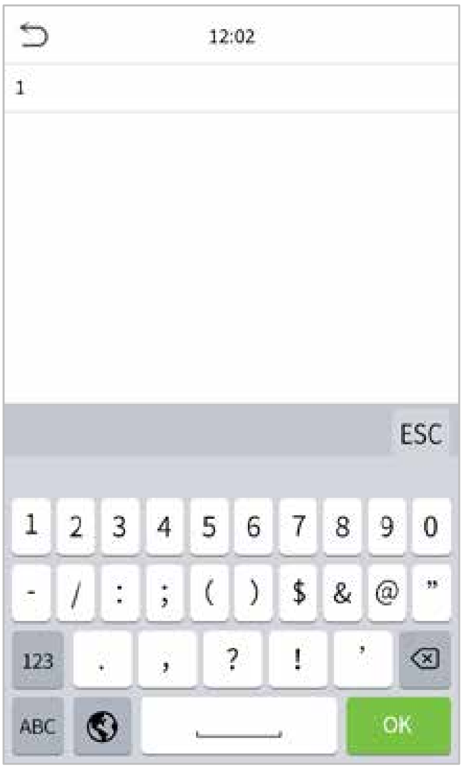
- **1: 1 Fingerprint Verification Mode**

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

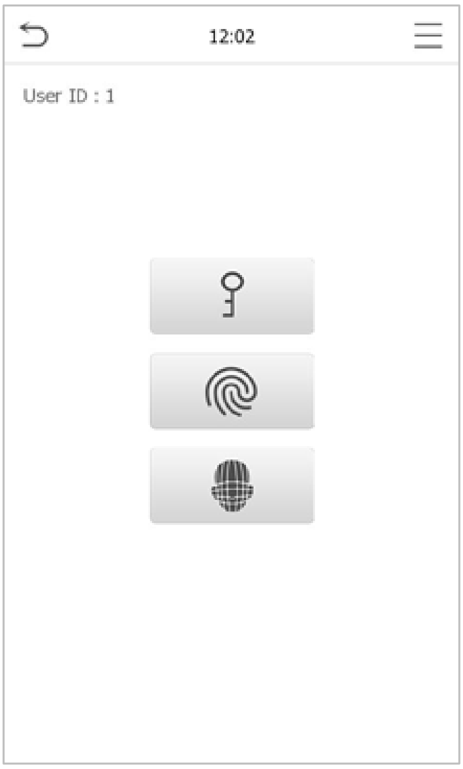
In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

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

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



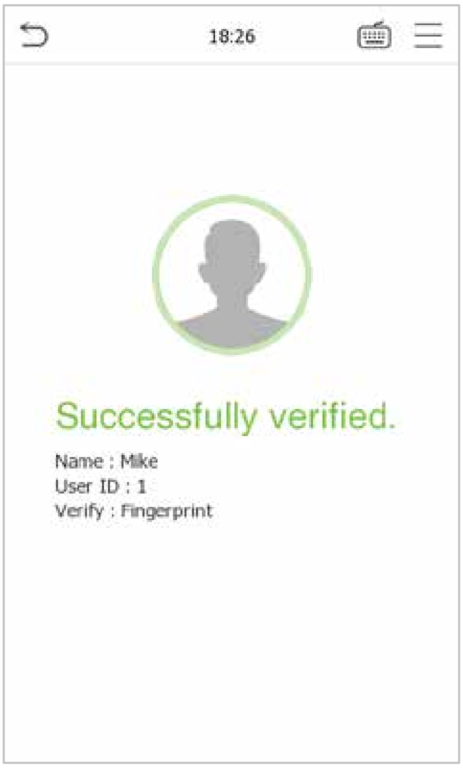
If the user has registered face template and password in addition to his/her fingerprints and the verification method is set to password/fingerprint/face template verification, the following screen will appear. Select the fingerprint icon to enter fingerprint verification mode.



User ID : 1

Press the fingerprint to verify.

Verification is successful:

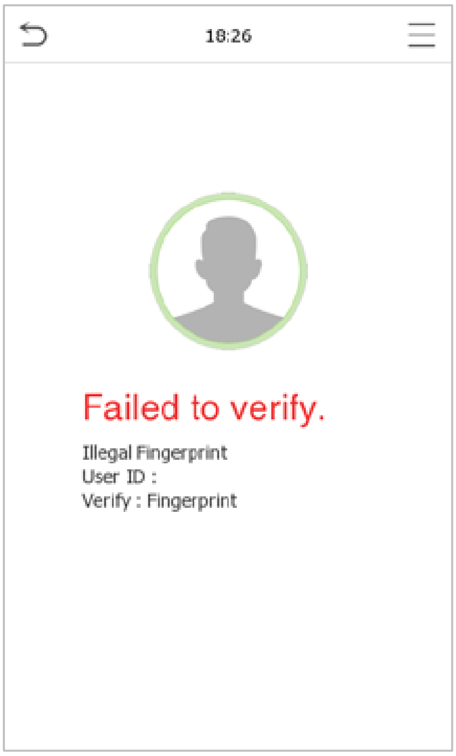


18:26

Successfully verified.

Name : Mike
User ID : 1
Verify : Fingerprint

Verification is failed:



18:26

Failed to verify.

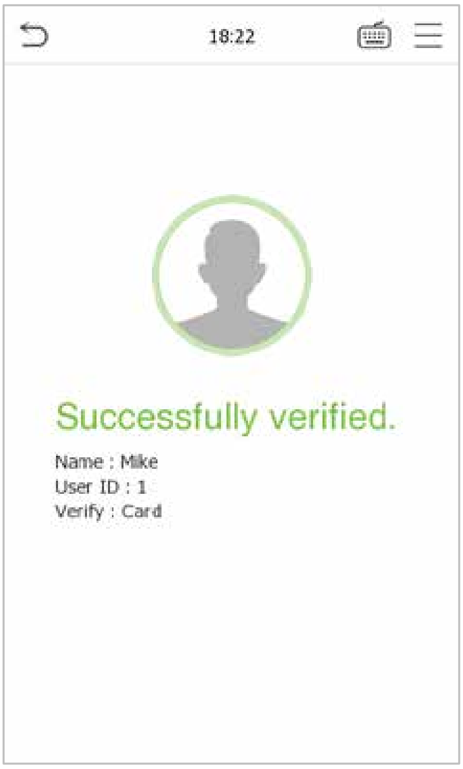
Illegal Fingerprint
User ID :
Verify : Fingerprint

1.6.2 Card Verification★

Card verification can be set up as both card and QR code verification methods.

- **1:N card verification**

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



Successfully verified.

Name : Mike

User ID : 1

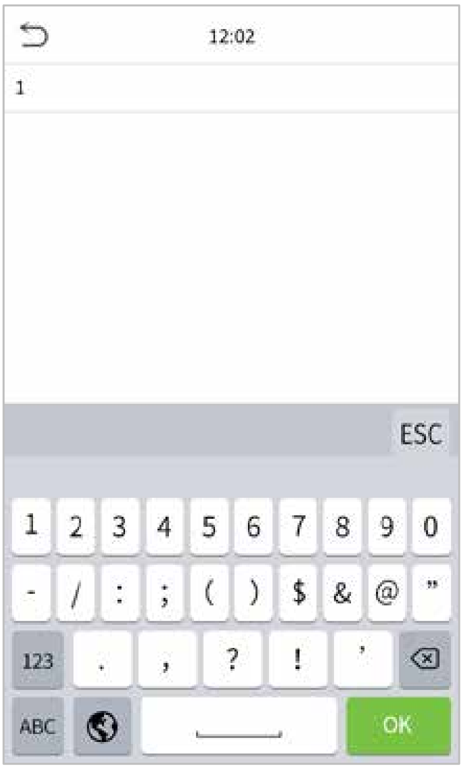
Verify : Card

- **1:1 card verification**

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

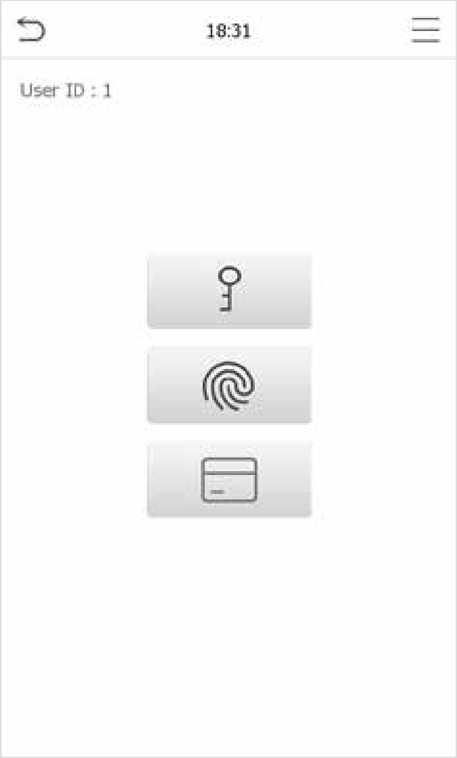
Press ⌨ in the main interface template to open the 1:1 card verification mode.

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



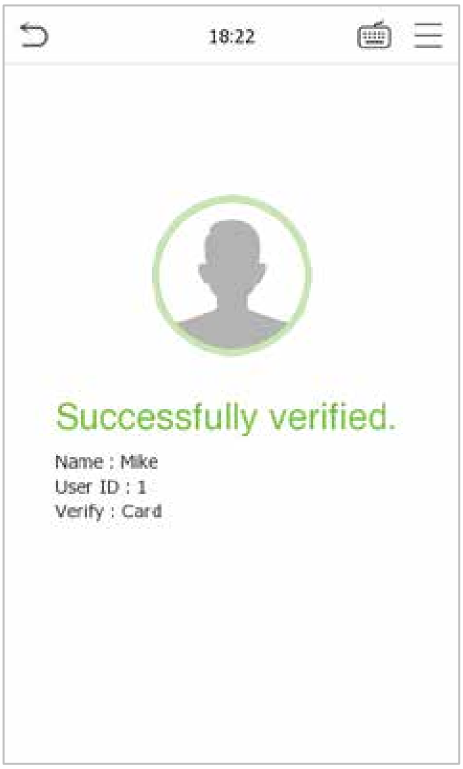
1

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



User ID : 1

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



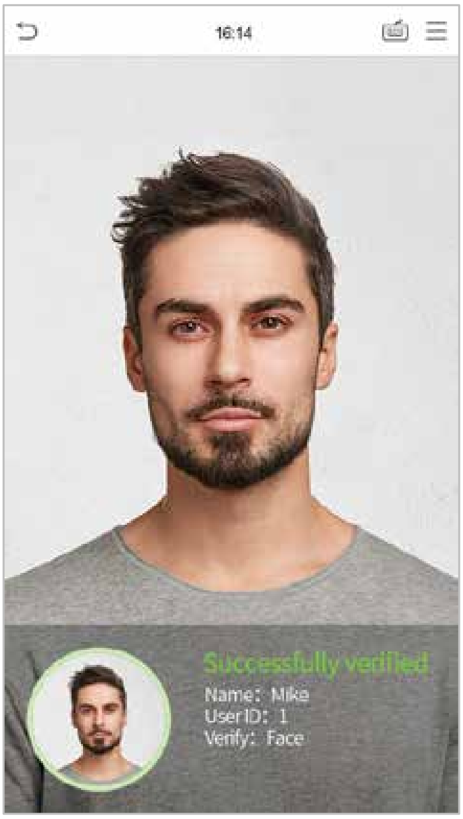
Successfully verified.

Name : Mike
User ID : 1
Verify : Card

1.6.3 Facial Verification

- **1:N Facial Verification**

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

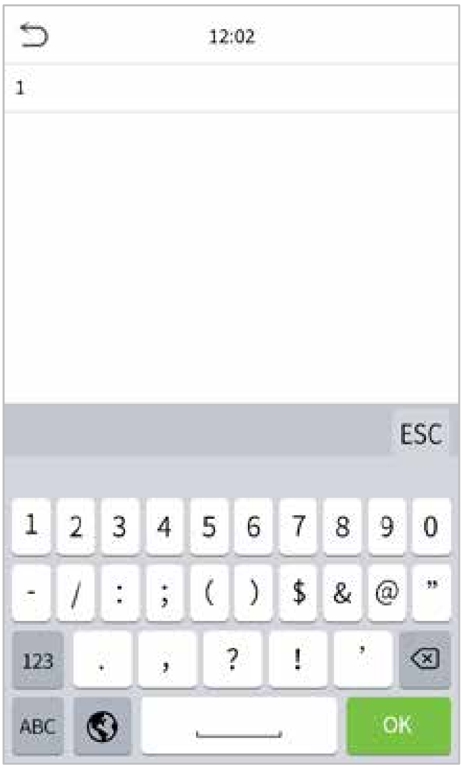


Successfully verified

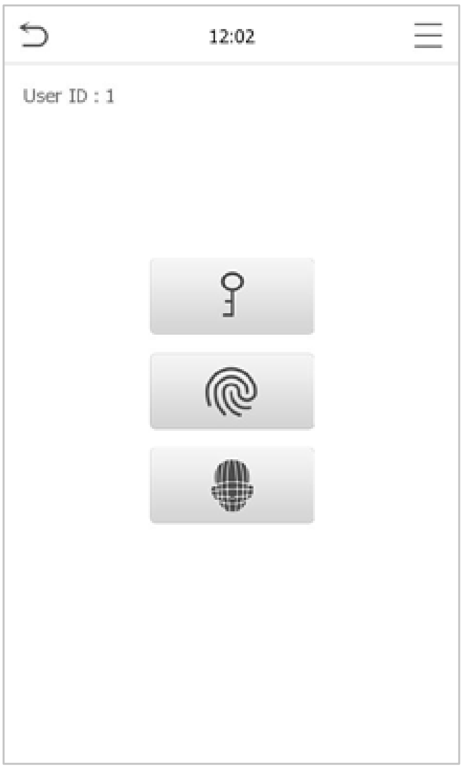
Name: Mike
UserID: 1
Verify: Face

- **1:1 Facial Verification**

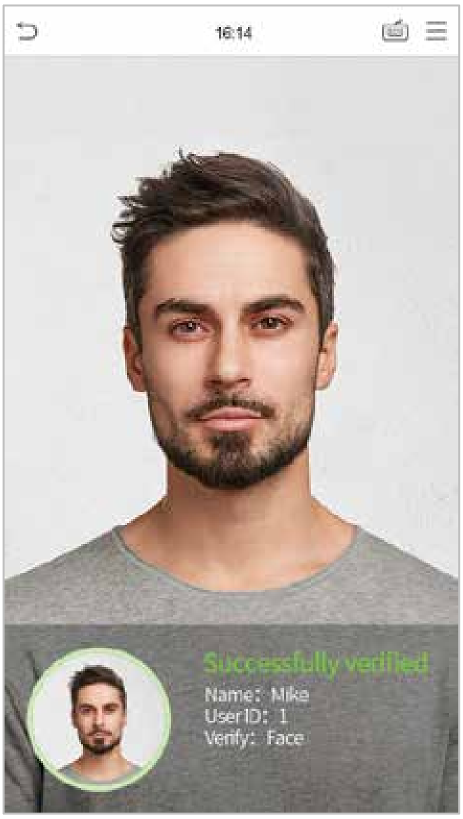
In this verification mode, the device compares the face template captured by the camera with the facial template related to the entered user ID. Press icon in the main interface template and enter the 1:1 facial verification mode and enter the user ID and click **OK**.



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



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



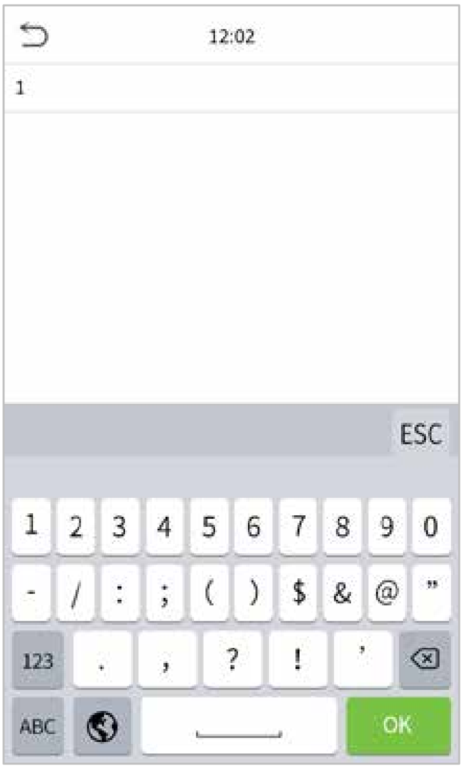
Successfully verified
Name: Mike
UserID: 1
Verify: Face

If the verification is failed, it prompts “**Please adjust your position!**”.

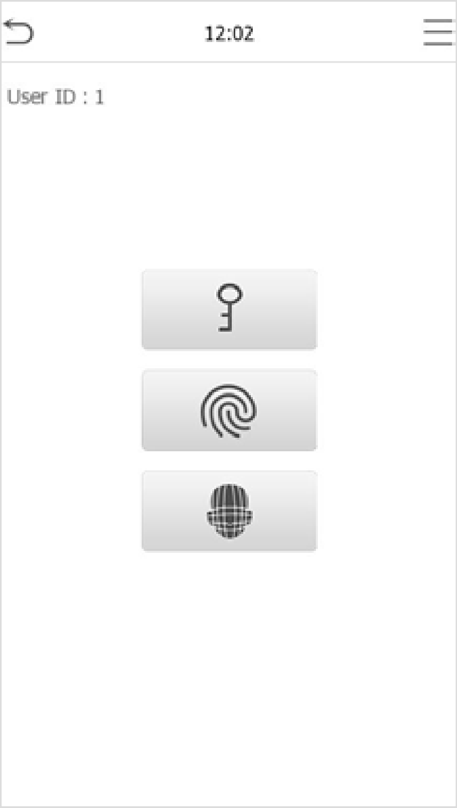
1.6.4 Password Verification

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

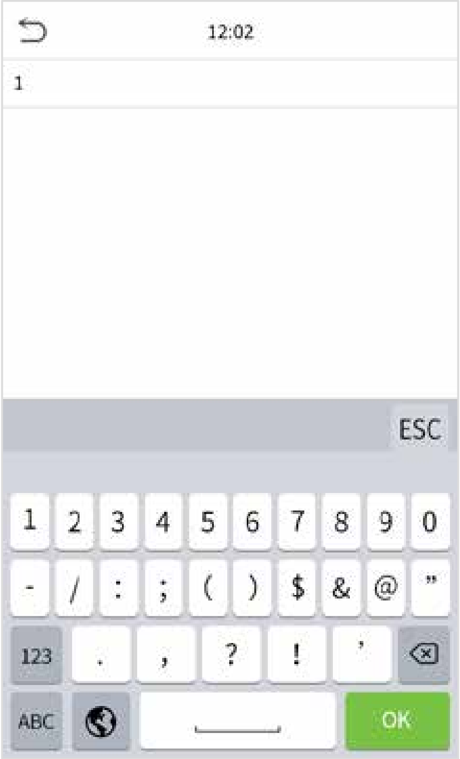
Click the ⌨ button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press **OK**.



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

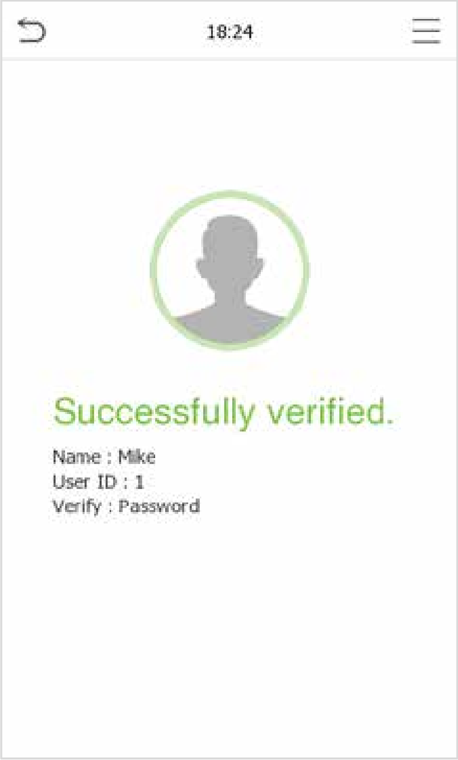


Input the password and press **OK**.



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

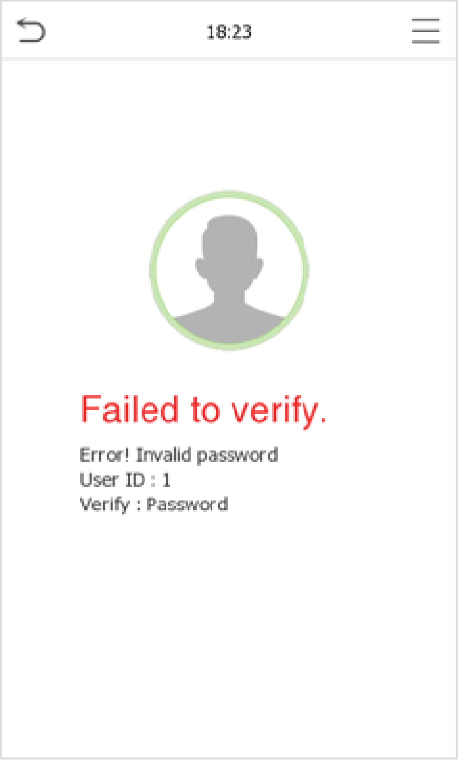
Verification is successful:



Successfully verified.

Name : Mike
User ID : 1
Verify : Password

Verification is failed:



Failed to verify.

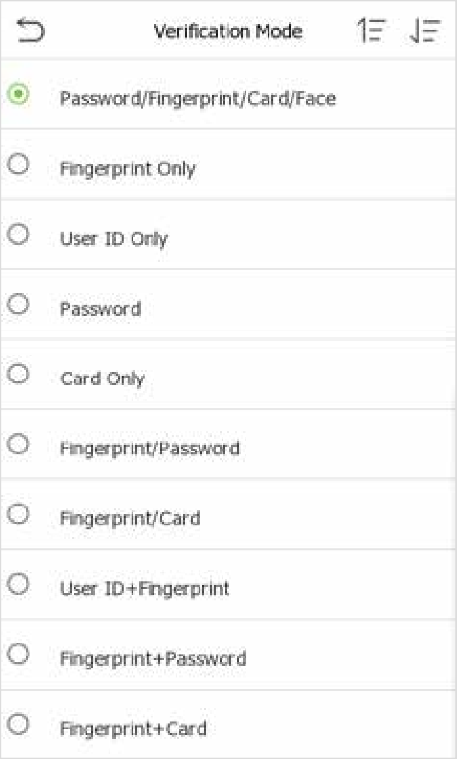
Error! Invalid password
User ID : 1
Verify : Password

1.6.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 12 different verification combinations can be used, as shown below:

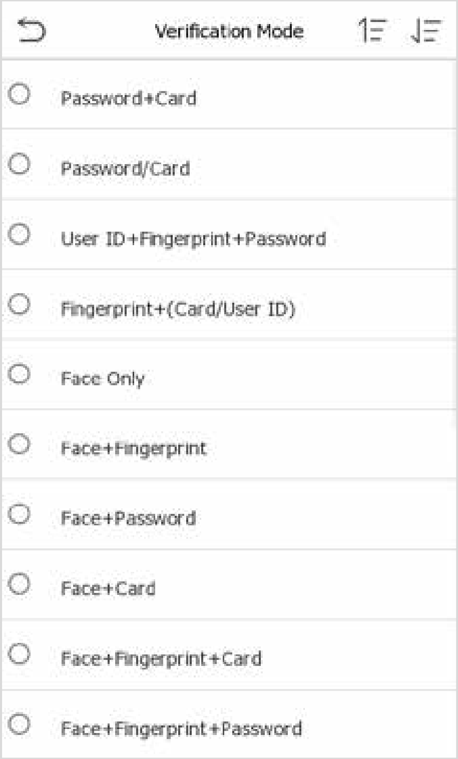
Combined Verification Symbol Definition:

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



Verification Mode

● Password/Fingerprint/Card/Face
○ Fingerprint Only
○ User ID Only
○ Password
○ Card Only
○ Fingerprint/Password
○ Fingerprint/Card
○ User ID+Fingerprint
○ Fingerprint+Password
○ Fingerprint+Card



Verification Mode

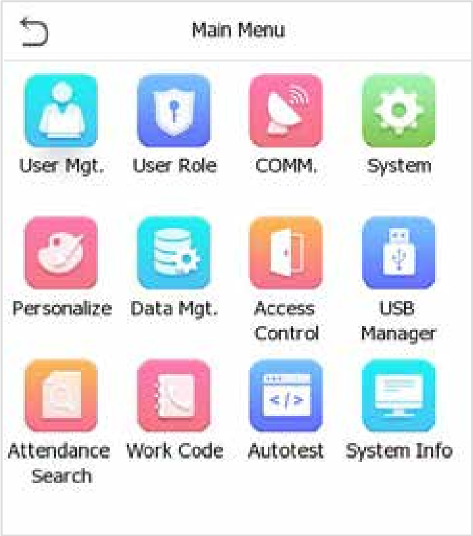
○ Password+Card
○ Password/Card
○ User ID+Fingerprint+Password
○ Fingerprint+(Card/User ID)
○ Face Only
○ Face+Fingerprint
○ Face+Password
○ Face+Card
○ Face+Fingerprint+Card
○ Face+Fingerprint+Password

Procedure to set for Combined Verification Mode:

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

2 Main Menu

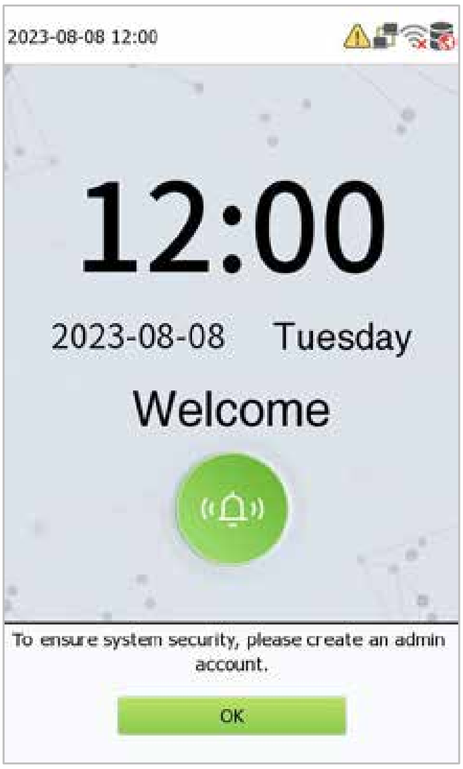
Press ☰ on the Standby interface to enter the **Main Menu**, the following screen will be displayed:



Function Description

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

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

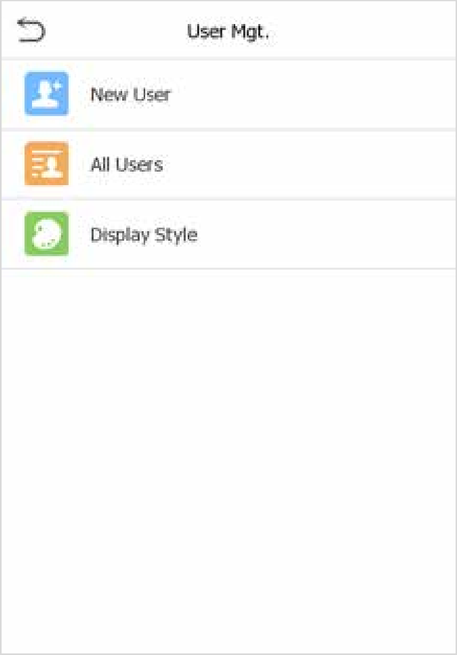


To ensure system security, please create an admin account.

3 User Management

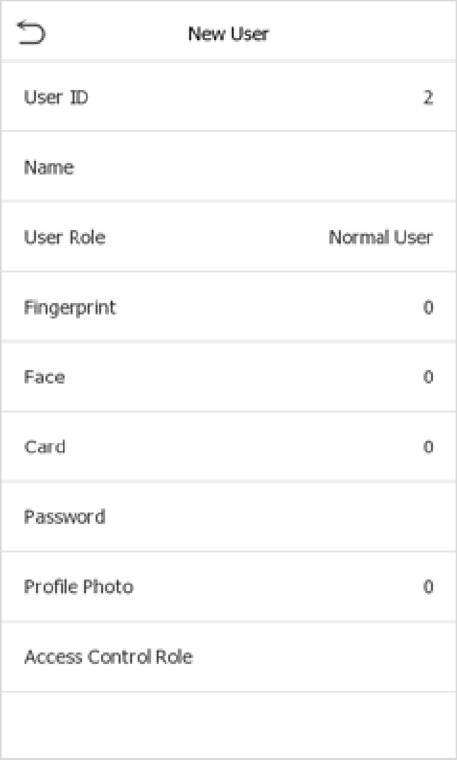
3.1 User Registration

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



3.1.1 User ID and Name

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



New User

User ID	2
Name	
User Role	Normal User
Fingerprint	0
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	

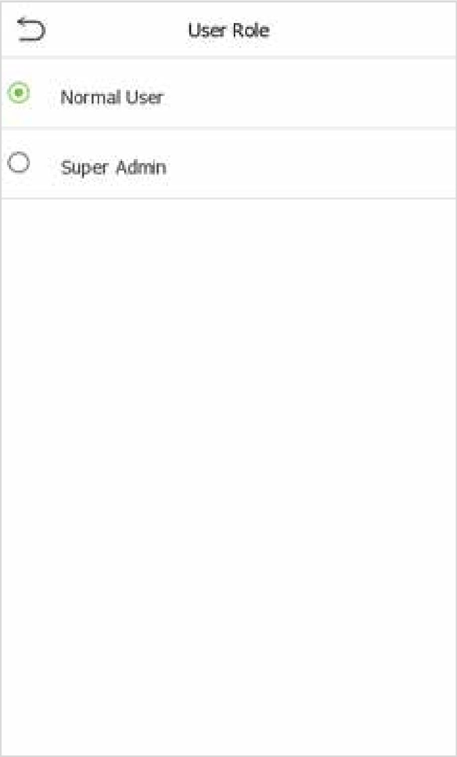
Notes:

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

3.1.2 User Role

On the New User interface, tap on **User Role** to set the role for the user as either **Normal User** or **Super Admin**.

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



User Role

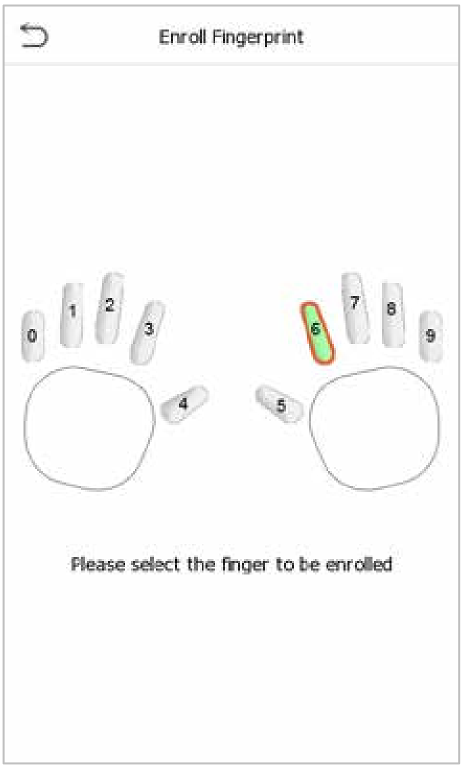
● Normal User

○ 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. Please refer to 1.5 Verification Mode.

3.1.3 Fingerprint

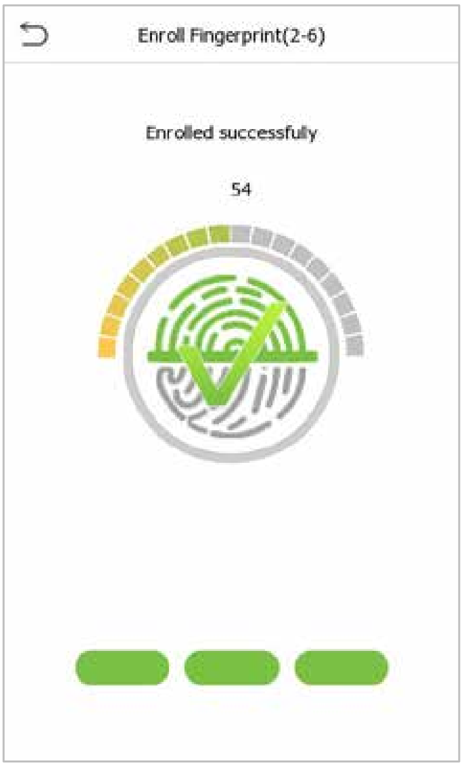
Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.



Enroll Fingerprint

Please select the finger to be enrolled

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



Enroll Fingerprint(2-6)

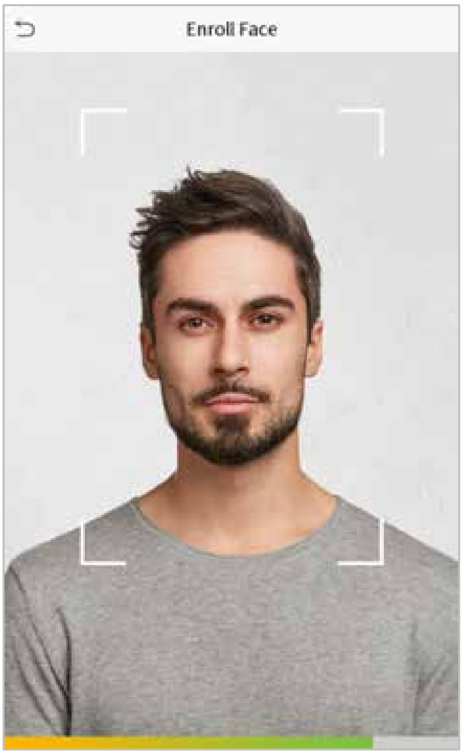
Enrolled successfully

54

3.1.4 Face Template

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

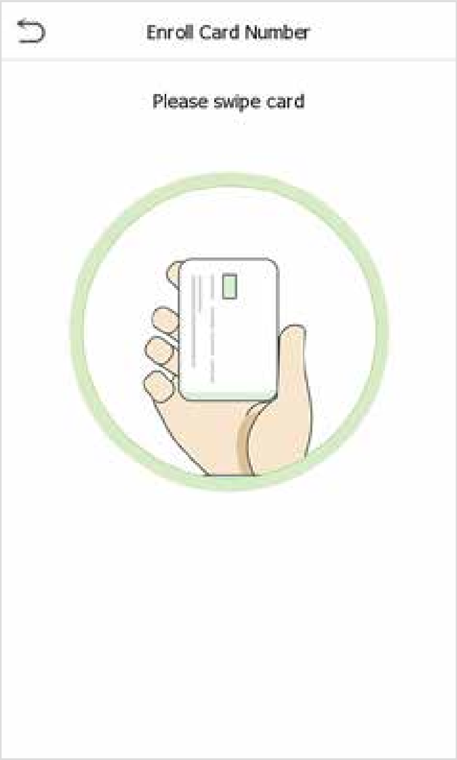
- Please face towards the camera and position your face template inside the white guiding box and stay still during face template registration.
- A progress bar shows up while registering the face template and a **"Enrolled Successfully"** is displayed as the progress bar completes.
- If the face template is registered already then, the **"Duplicate Face"** message shows up. The registration interface is as follows:



3.1.5 Card★

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

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



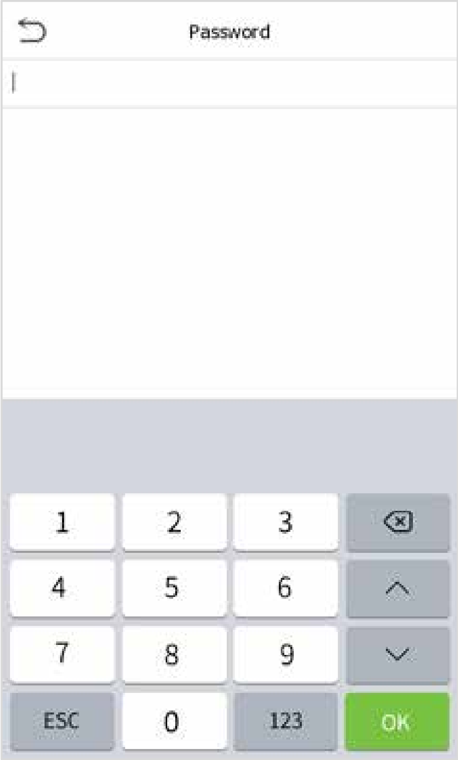
Enroll Card Number

Please swipe card

3.1.6 Password

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

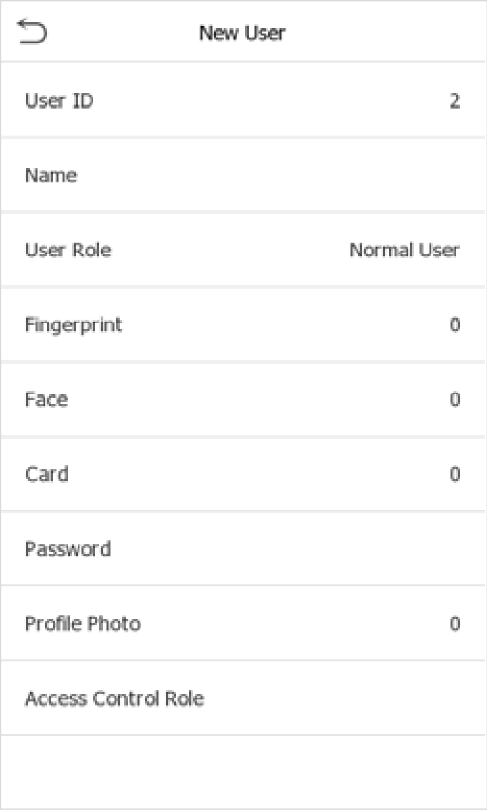
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.



Note: The password may contain 6 to 8 digits by default.

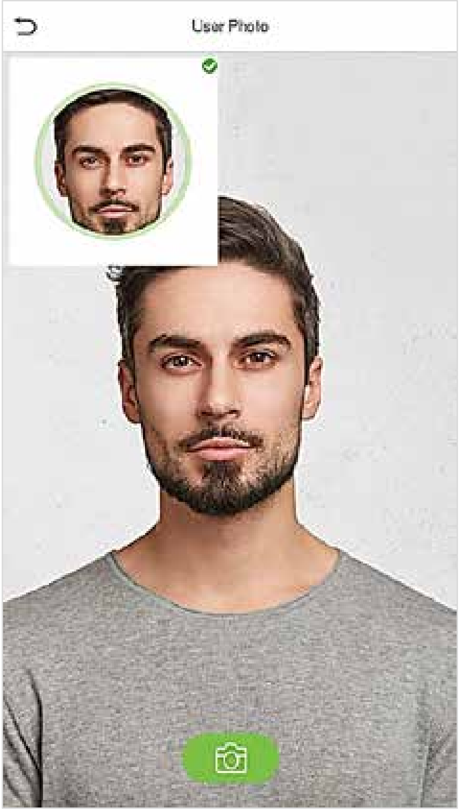
3.1.7 Profile Photo

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



New User

User ID	2
Name	
User Role	Normal User
Fingerprint	0
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	



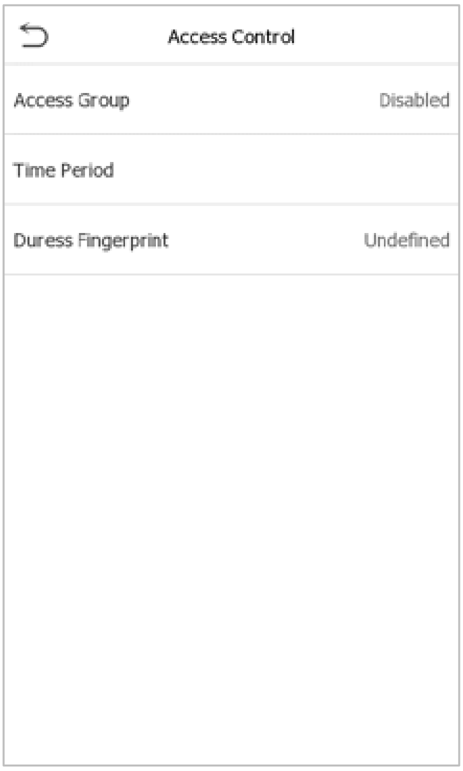
- When a user registered with a photo passes the authentication, the registered photo will be displayed.
- Tap **Profile Photo**, the device's camera will open, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens again to take a new photo, after taking the initial photo.

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

3.1.8 Access Control Role

The **Access Control Role** sets the door access privilege for each user. This includes the access group, duress fingerprint and facilitates to set the group access time-period.

- Tap **Access Control Role** > **Access Group**, to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Tap **Time Period**, to select the time period to use.



Access Control

Access Group Disabled

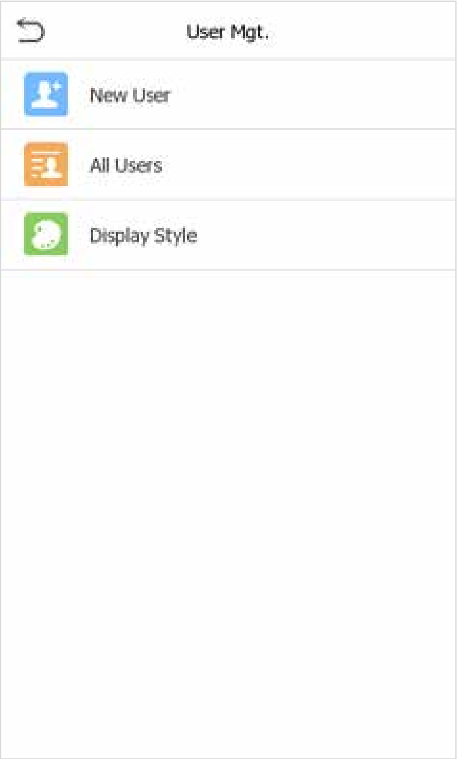
Time Period

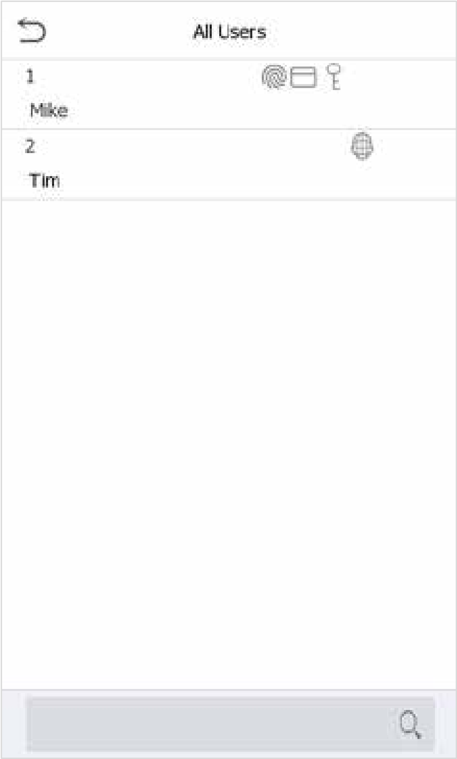
Duress Fingerprint Undefined

3.2 Search for Users

On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search for a User.

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



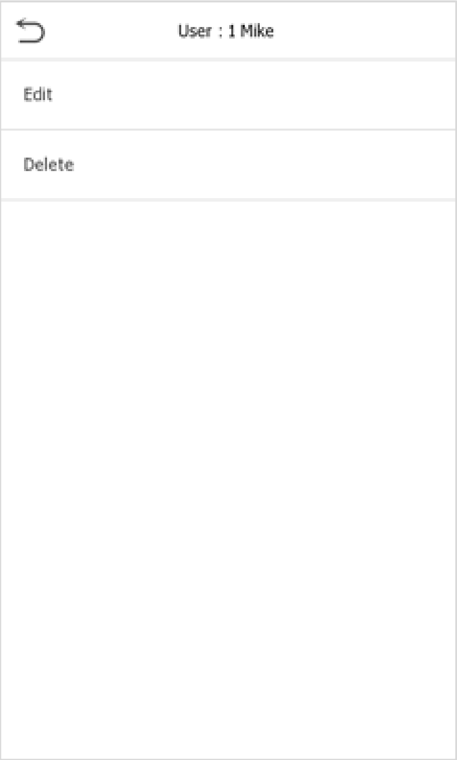


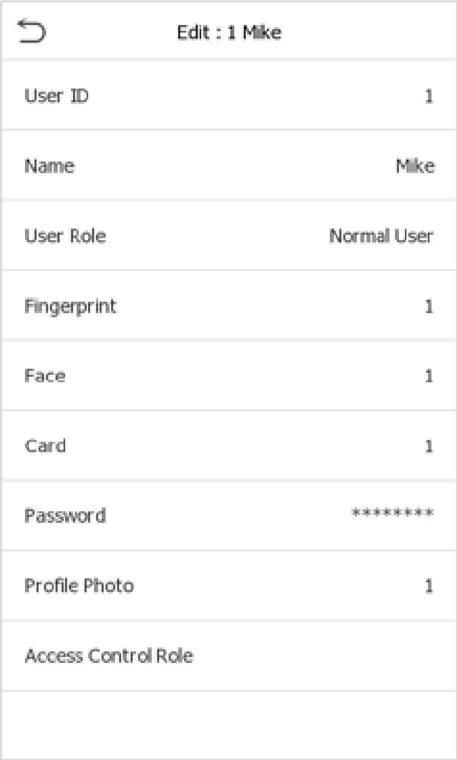
1 Mike

2 Tim

3.3 Edit User

On **All Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.





User ID 1

Name Mike

User Role Normal User

Fingerprint 1

Face 1

Card 1

Password ********

Profile Photo 1

Access Control Role

Note: The process of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user’s detail. The process in detail refers to "3. User Management".

3.4 Delete User

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

- **Delete operations:**

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

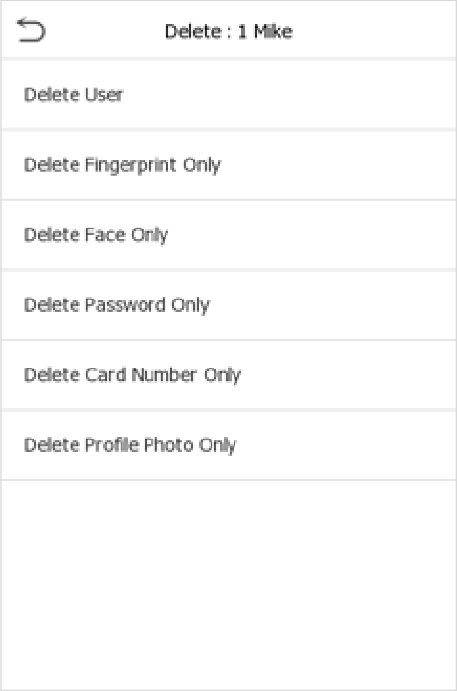
Delete Fingerprint Only: Deletes the fingerprint information of the selected user.

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

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

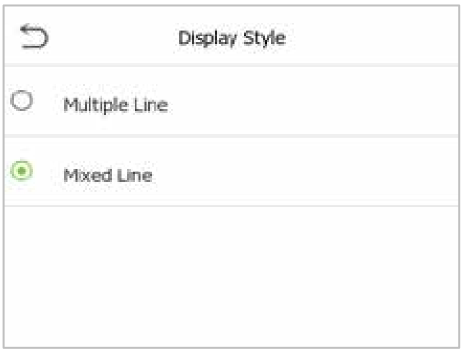
Delete Card Number Only: Deletes the card information of the selected user.

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



3.5 Display Style

Tap on **User Mgt.** > **Display Style** to choose the style of **All Users** interface's list.

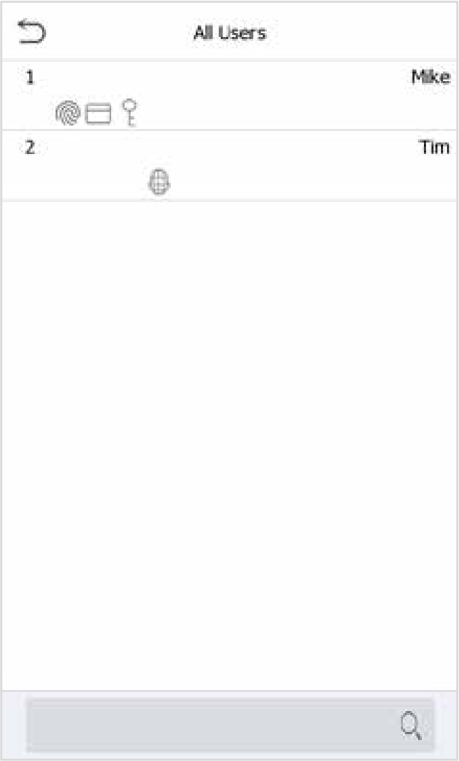

Display Style

○ Multiple Line

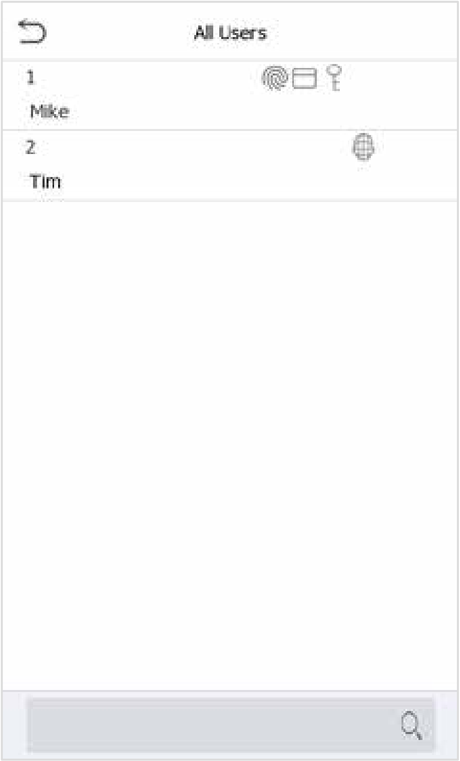
● Mixed Line

Different display styles are shown as below:

Multiple Line:



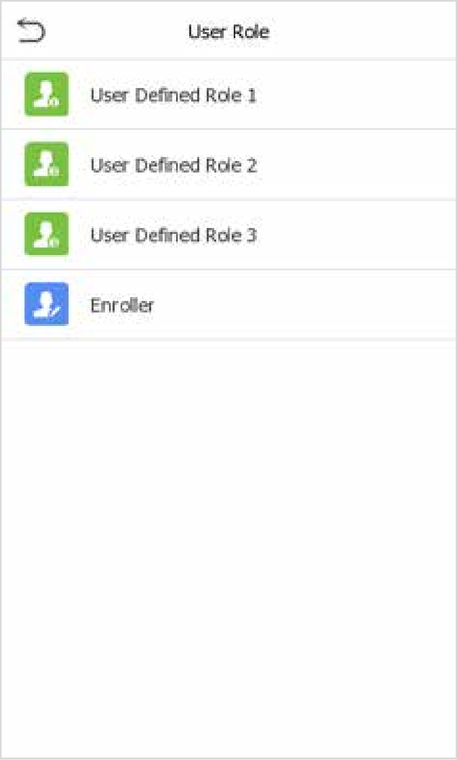
Mixed Line:



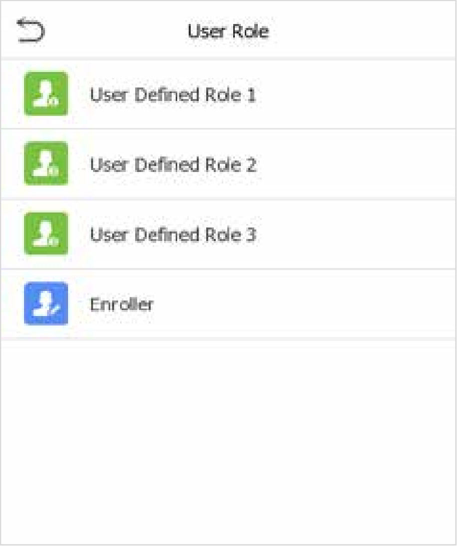
4 User Role

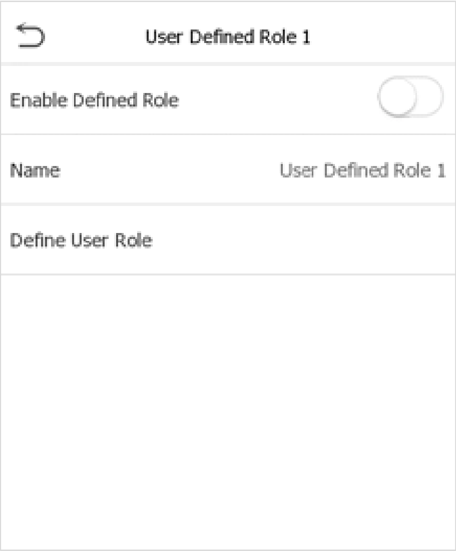
User Role facilitates to assign some specific permissions to specific users, based on the requirement.

- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up to 3 roles, that is, the custom operating scope of the menu functions of the user.



- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



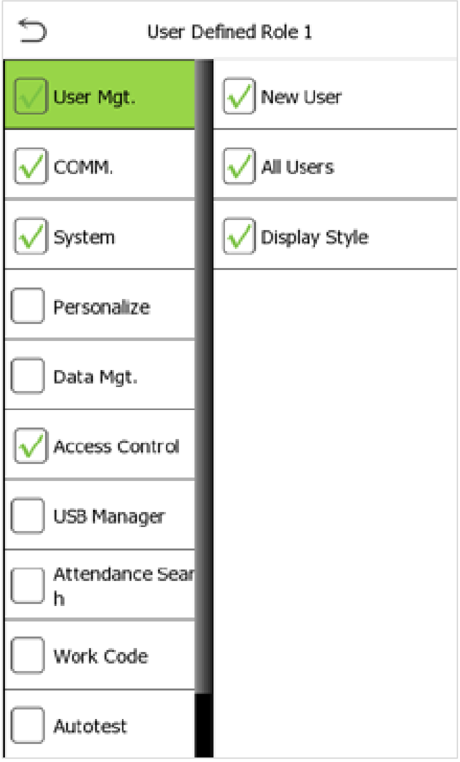

User Defined Role 1

Enable Defined Role

Name User Defined Role 1

Define User Role

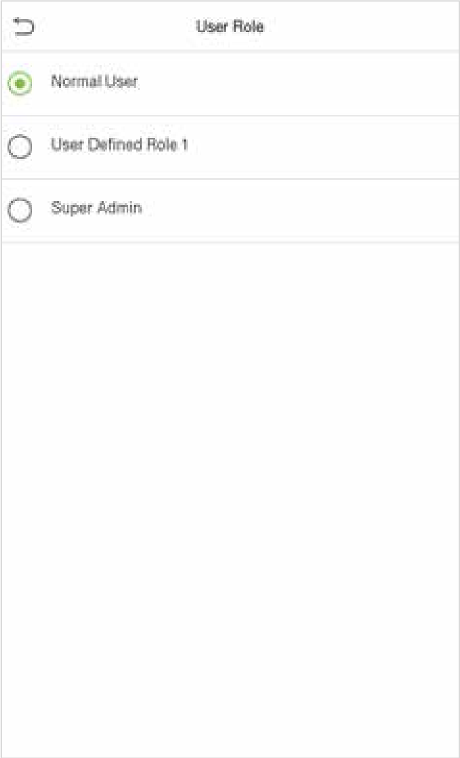
- Then, tap on **User Defined Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on its right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



User Defined Role 1

☑ User Mgt.
☑ COMM.
☑ System
□ Personalize
□ Data Mgt.
☑ Access Control
□ USB Manager
□ Attendance Search
□ Work Code
□ Autotest

☑ New User
☑ All Users
☑ Display Style



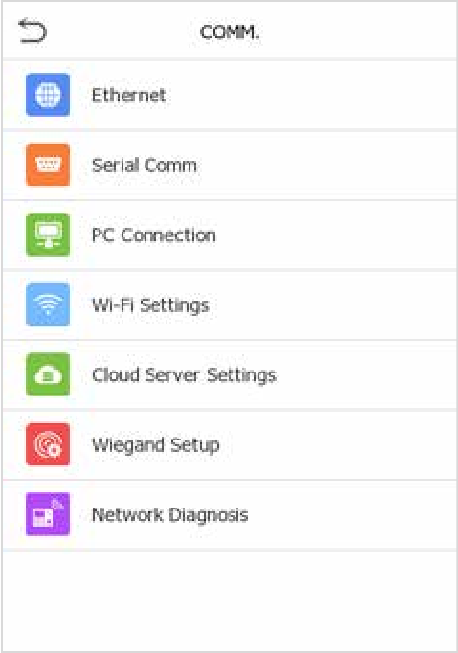
User Role

● Normal User
○ User Defined Role 1
○ Super Admin

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

5 Communication Settings

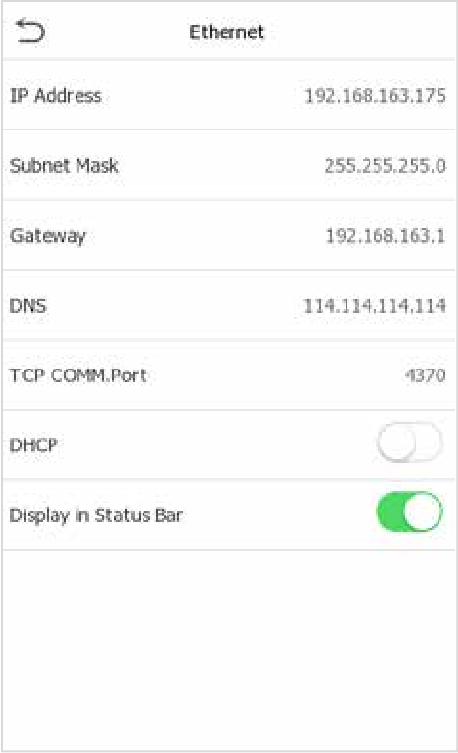
Tap **COMM.** on the **Main Menu** to set the relevant parameters of Network, Serial Comm, PC Connection, Wireless Network, Cloud Server, Wiegand and Network Diagnosis.



5.1 Network Settings

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

Tap **Ethernet** on the **Comm**. Settings interface to configure the settings.



Ethernet

IP Address 192.168.163.175

Subnet Mask 255.255.255.0

Gateway 192.168.163.1

DNS 114.114.114.114

TCP COMM.Port 4370

DHCP ○

Display in Status Bar ●

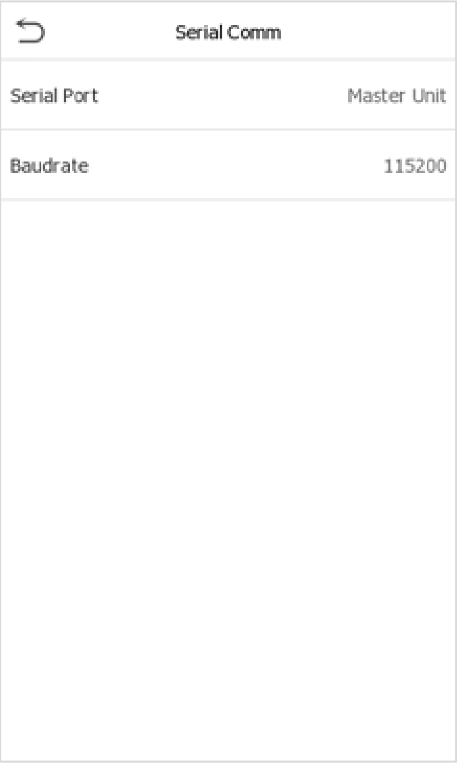
Function Description

Function Name	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 is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

5.2 Serial Comm

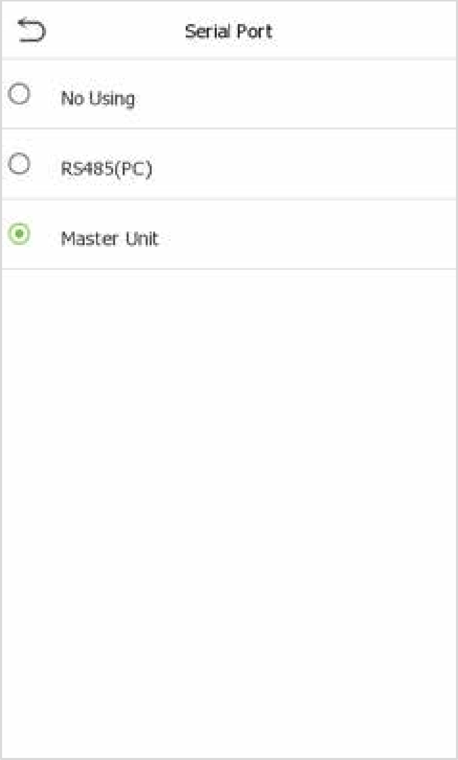
Serial Comm function facilitates to establish communication with the device through a serial port (RS485/ Master Unit).

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



Serial Comm

Serial Port	Master Unit
Baudrate	115200



Serial Port

○ No Using

○ RS485(PC)

● Master Unit

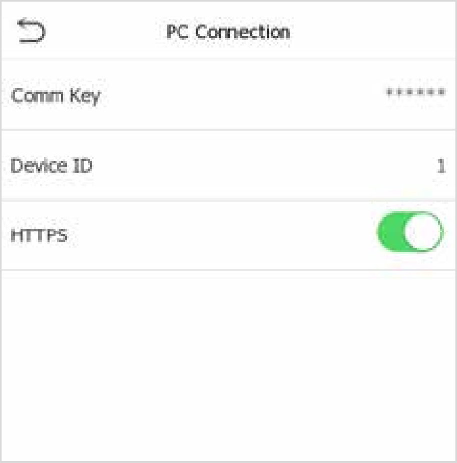
Function Description

Function Name	Descriptions
Serial Port	**no using:** Do not communicate with the device through the serial port. **RS485(PC):** Communicates with the device through RS485 serial port. **Master Unit:** When RS485 is used as the function of "**Master unit**", the device will act as a master unit, and it can be connected to RS485 card reader.
Baud Rate	The rate at which the data is communicated with PC, there are 4 options of baud rate: 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 would be 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.

Tap **PC Connection** on the **Comm.** Settings interface to configure the communication settings.



Comm Key ******

Device ID 1

HTTPS

Function Description

Function Name	Descriptions
Comm Key	The default password is 0 and can be changed. The Comm Key must be 6 digits.
Device ID	Identity 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.
HTTPS	To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of

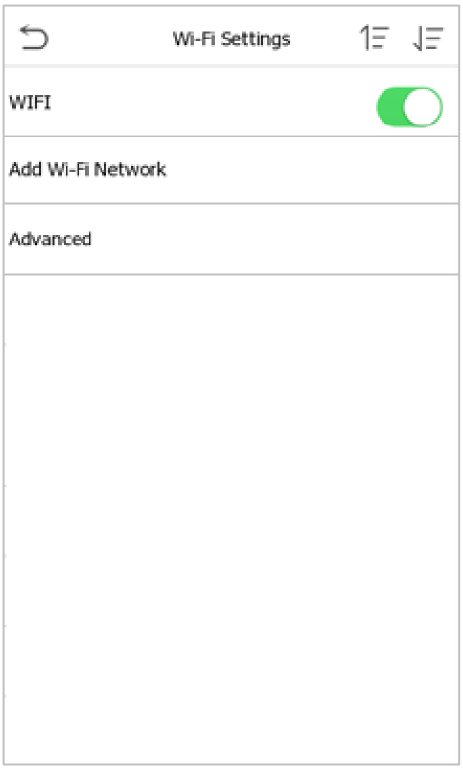
	sent data through identity authentication and encrypted communication. This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation.

5.4 Wireless Network★

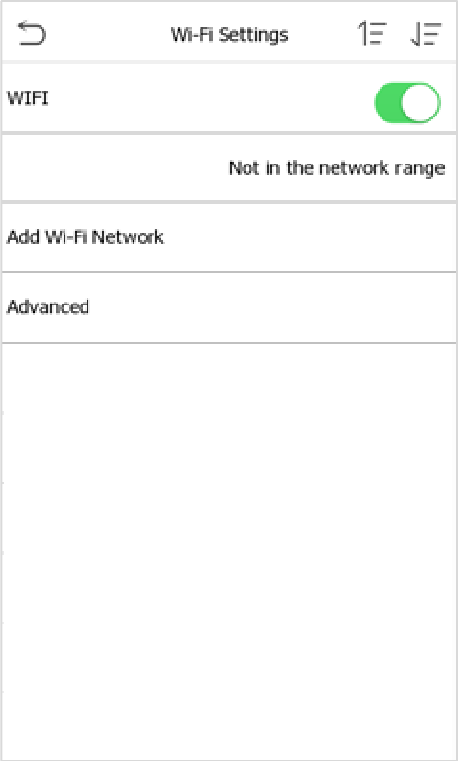
The device provides a Wi-Fi module, which can be built-in within the device mould or can be externally connected.

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

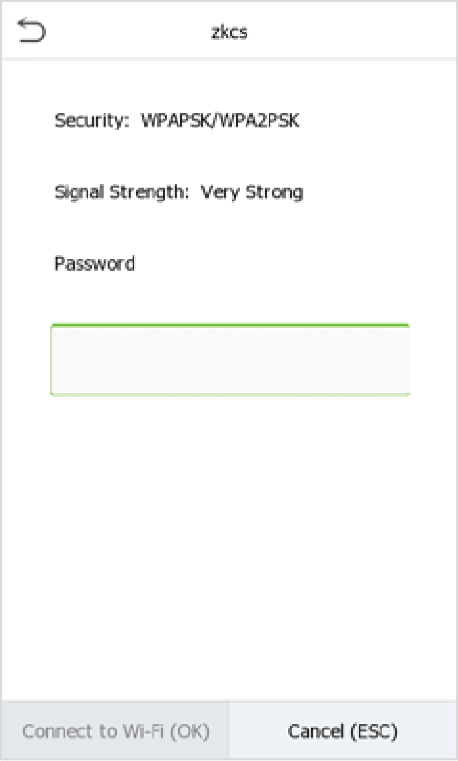
Tap **Wireless Network** on the **Comm.** Settings interface to configure the WiFi settings.



- **Search the WIFI Network**
  - WIFI is enabled in the Device by default. Toggle on button to enable or disable WIFI.
  - Once the Wi-Fi is turned on, the device will search for the available WIFI within the network range.
  - Choose the appropriate WiFi name from the available list, and input the correct password in the password interface, and then tap **Connect to WIFI (OK)**.



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



Security: WPAPSK/WPA2PSK

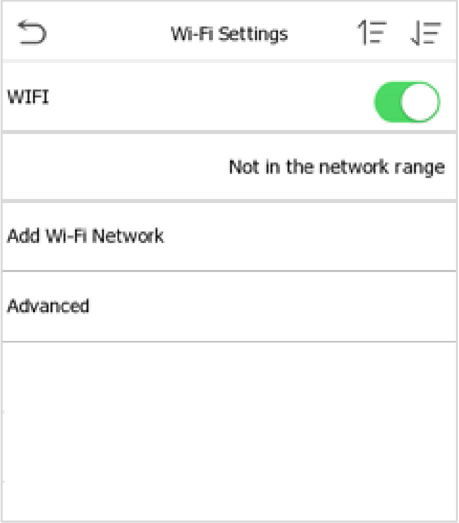
Signal Strength: Very Strong

Tap on the password field to enter the password, and then tap on **Connect to WIFI (OK).**

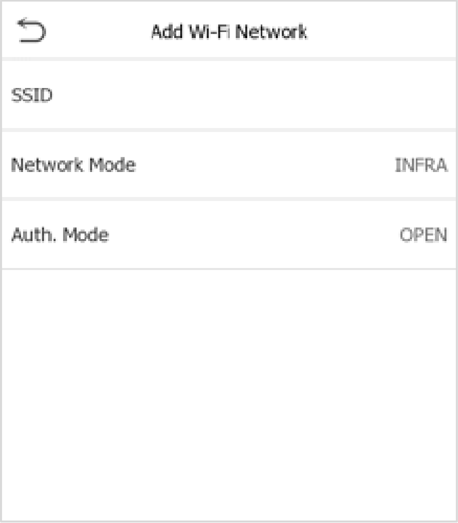
- When the WIFI is connected successfully, the initial interface will display the Wi-Fi logo.

- **Add WIFI Network Manually**

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



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



Network Mode INFRA

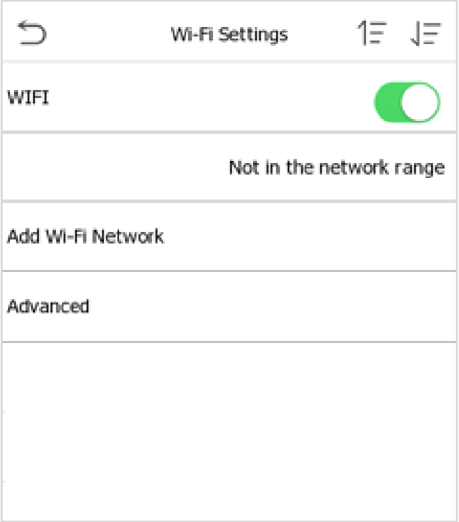
Auth. Mode OPEN

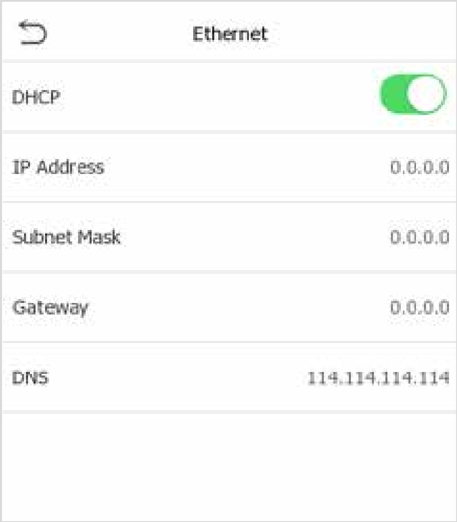
On this interface template, enter the WIFI network parameters. (The added network must exist.)

Note: After successfully adding the WIFI manually, follow the same process to search for the added WIFI name. Click here to view the process to search the WIFI network.

- **Advanced Setting**

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





Ethernet

DHCP

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Gateway 0.0.0.0

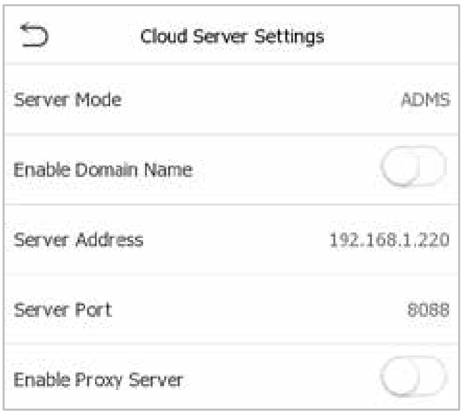
DNS 114.114.114.114

Function Description

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

5.5 Cloud Server Setting

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



Cloud Server Settings

Server Mode ADMS

Enable Domain Name ○

Server Address 192.168.1.220

Server Port 8088

Enable Proxy Server ○

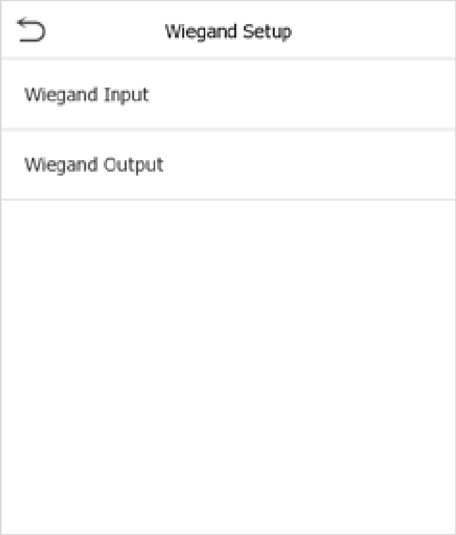
Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once 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.

5.6 Wiegand Setup

To set the Wiegand input and output parameters.

Tap **Wiegand Setup** on the **Comm.** Settings interface to set the Wiegand input and output parameters.

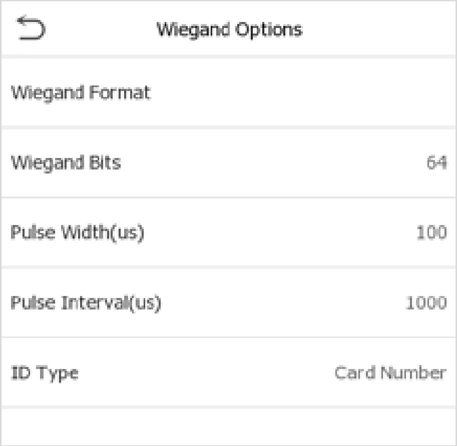


Wiegand Setup

Wiegand Input

Wiegand Output

5.6.1 Wiegand Input



Wiegand Options

Wiegand Format	
Wiegand Bits	64
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	Card Number

Function Description

Function Name	Descriptions
Wiegand Format	Values range from 26 Bits, 32 Bits, 34 Bits, 36 Bits, 37 Bits, 50 Bits and 64Bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between User ID and card number.

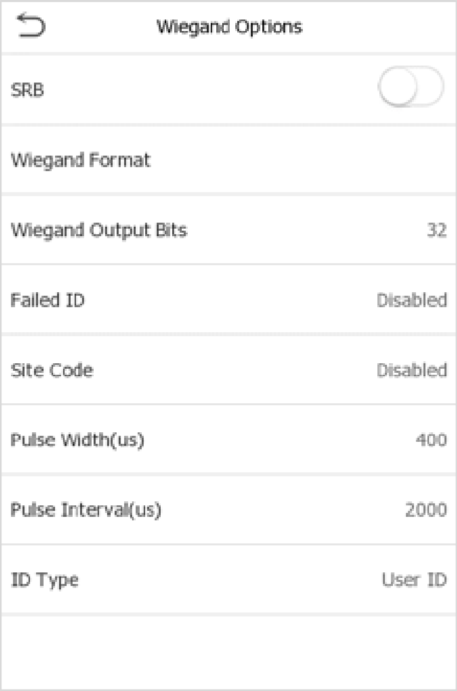
Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers.

Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers.

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

5.6.2 Wiegand Output



Wiegand Options

SRB ○

Wiegand Format

Wiegand Output Bits 32

Failed ID Disabled

Site Code Disabled

Pulse Width(us) 400

Pulse Interval(us) 2000

ID Type User ID

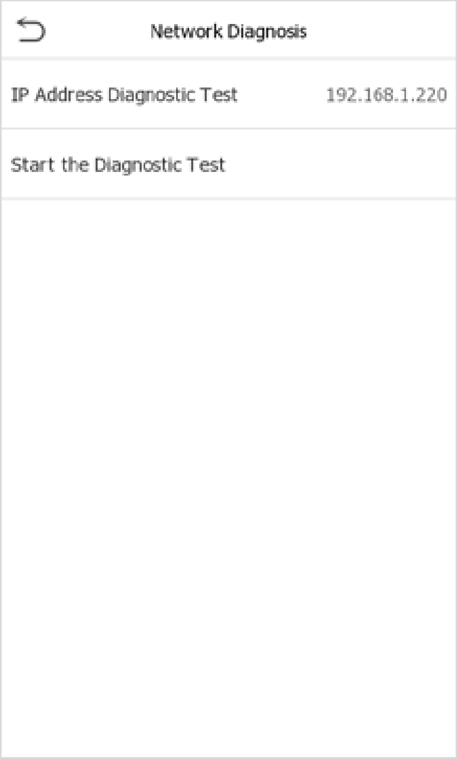
Function Description

Function Name	Descriptions
SRB★	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 32 Bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits of the Wiegand format.
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

5.7 Network Diagnosis

To set the network diagnosis parameters.

Tap **Network Diagnosis** on the **Comm.** Settings interface to set the IP address diagnostic and start the diagnostic parameters.



Network Diagnosis

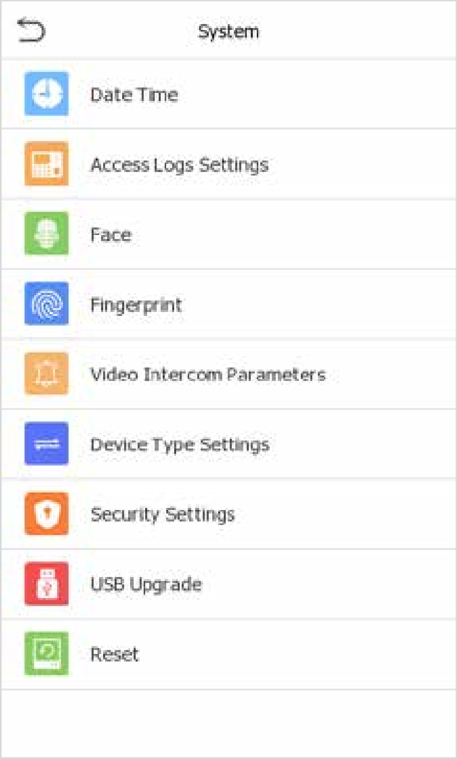
IP Address Diagnostic Test 192.168.1.220

Start the Diagnostic Test

6 System Settings

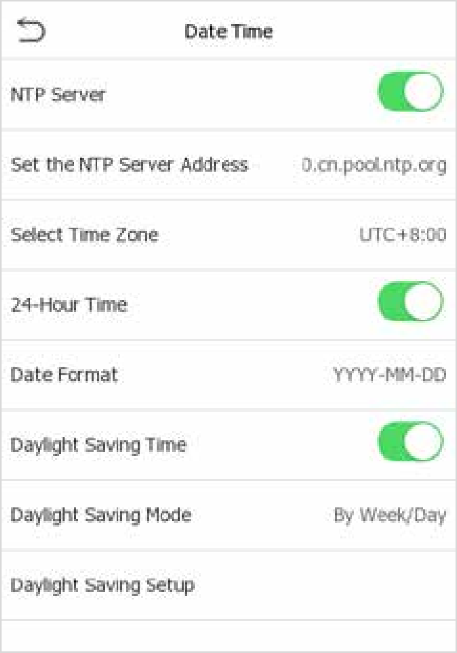
Set related system parameters to optimize the performance of the device.

Tap **System** on the **Main Menu** interface to set the related system parameters to optimize the performance of the device.



6.1 Date and Time

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



NTP Server

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

Select Time Zone UTC+8:00

24-Hour Time

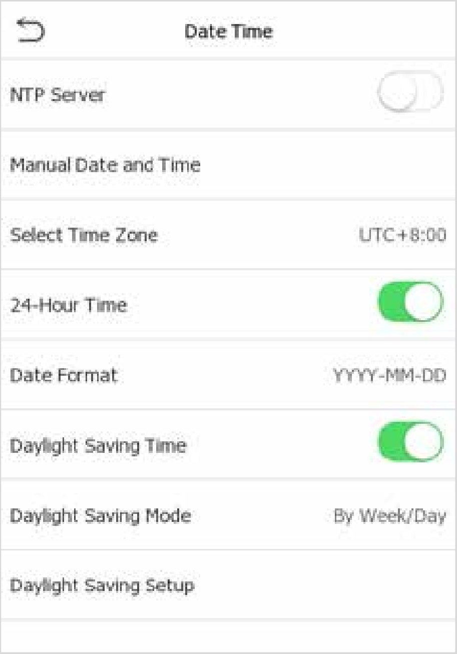
Date Format YYYY-MM-DD

Daylight Saving Time

Daylight Saving Mode By Week/Day

Daylight Saving Setup

- The product supports the NTP synchronization time system by default. This function takes effect after **NTP Server** is enabled and the corresponding NTP server address link is set.
- If users need to set date and time manually, disable **NTP Server** first, and then tap **Manual Data and Time** to set date and time and tap **Confirm** to save.

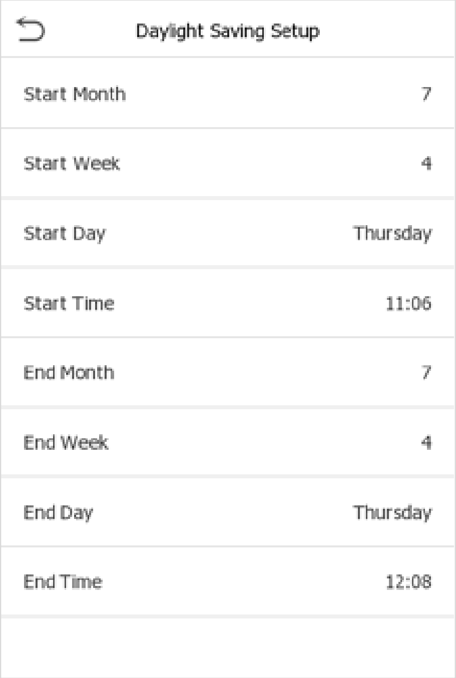


Date Time

NTP Server	○
Manual Date and Time	
Select Time Zone	UTC+8:00
24-Hour Time	●
Date Format	YYYY-MM-DD
Daylight Saving Time	●
Daylight Saving Mode	By Week/Day
Daylight Saving Setup	

- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.

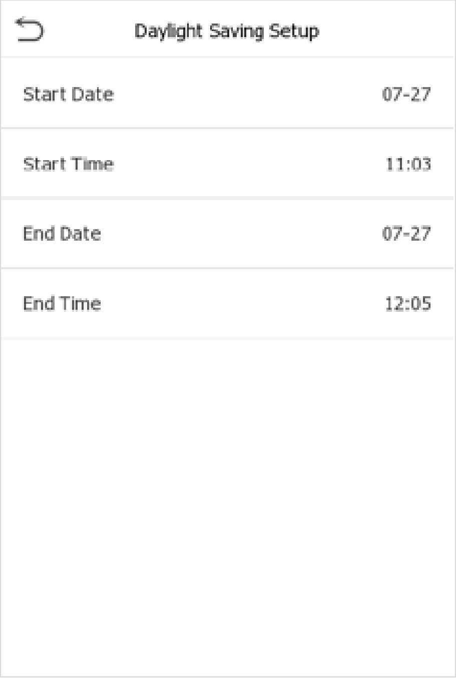
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.



Daylight Saving Setup

Start Month	7
Start Week	4
Start Day	Thursday
Start Time	11:06
End Month	7
End Week	4
End Day	Thursday
End Time	12:08

Week mode



Daylight Saving Setup

Start Date	07-27
Start Time	11:03
End Date	07-27
End Time	12:05

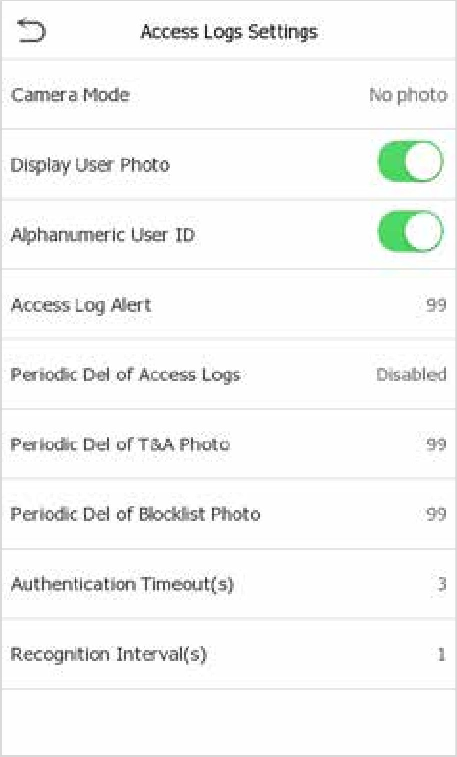
Date mode

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

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

6.2 Access Logs Settings

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



Access Logs Settings

Camera Mode: No photo

Display User Photo: ON

Alphanumeric User ID: ON

Access Log Alert: 99

Periodic Del of Access Logs: Disabled

Periodic Del of T&A Photo: 99

Periodic Del of Blocklist Photo: 99

Authentication Timeout(s): 3

Recognition Interval(s): 1

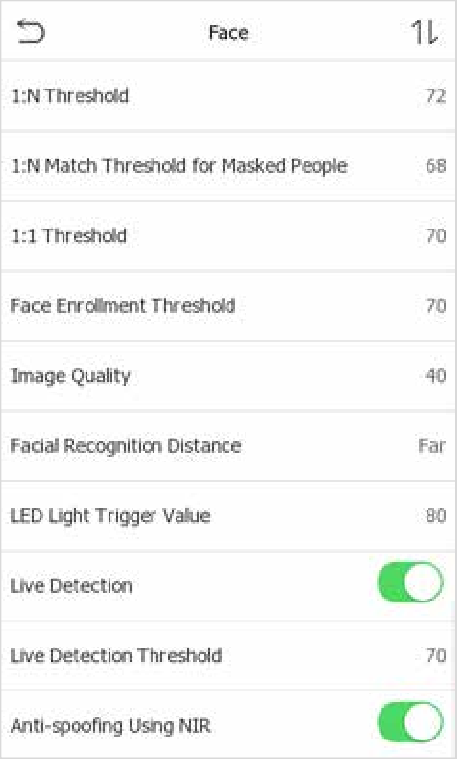
Function Description

Function Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo will be taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, there will be a security prompt.
Alphanumeric User ID	Decides whether to support letters in a User ID.

Access Logs Alert	When the record space of the attendance access reaches the maximum threshold value, the device will automatically display the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access records have reached full capacity, the device will automatically delete a set of old access records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of T&A Photo	When attendance photos have reached full capacity, the device will automatically delete 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 have reached full capacity, the device will automatically delete 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 length of the message of successful verification displays. Valid value: 1~9 seconds.
Recognition Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

6.3 Face Template Parameters

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



Face

1:N Threshold 72

1:N Match Threshold for Masked People 68

1:1 Threshold 70

Face Enrollment Threshold 70

Image Quality 40

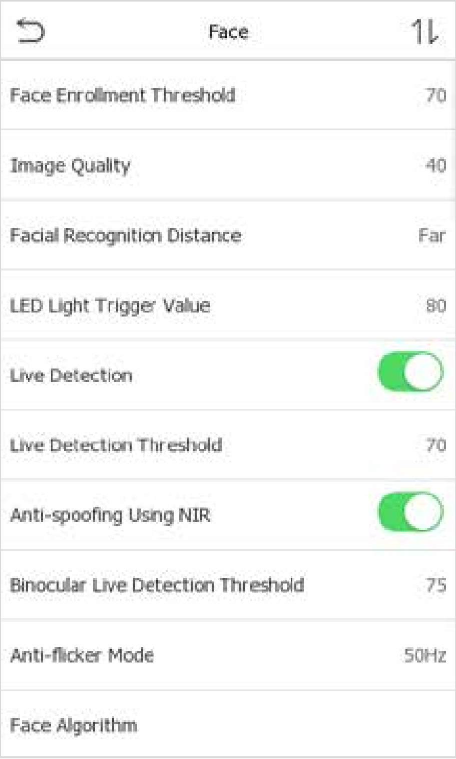
Facial Recognition Distance Far

LED Light Trigger Value 80

Live Detection

Live Detection Threshold 70

Anti-spoofing Using NIR



Face

Face Enrollment Threshold 70

Image Quality 40

Facial Recognition Distance Far

LED Light Trigger Value 80

Live Detection

Live Detection Threshold 70

Anti-spoofing Using NIR

Binocular Live Detection Threshold 75

Anti-flicker Mode 50Hz

Face Algorithm

FRR	FAR	Recommended Matching Thresholds

High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

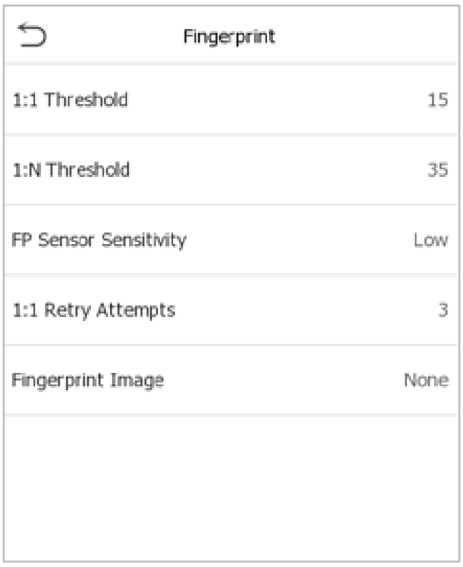
Function Description

Function Name	Description
1:N Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
1:N Match Threshold for Masked People	Under 1:N verification mode, the device will perform similarity matching between the face template currently wearing the mask and the registered face template template in the device. When the similarity is greater than this value, it means the matching is successful, otherwise it means the matching fails. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 68.
1:1 Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
Face Enrollment Threshold	During face template enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face template has already been registered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Facial Recognition Distance	Face template recognition of the maximum distance, greater than this value will be filtered. The parameter value can be understood as the face template size required for registration and comparison. The farther the distance from people, the smaller the face template pixels obtained by the algorithm. When the value is 0, it means that the face template comparison distance is not limited.
LED Light Triggered Value	This value controls the on and off the LED light. The larger the value, the more frequently the LED light will be turned on.
Live Detection	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person (a live human being) or false representation.
Live Detection Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.

Anti-spoofing using NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4 Fingerprint Parameters

Click **Fingerprint** on the System interface.


Fingerprint

1:1 Threshold 15

1:N Threshold 35

FP Sensor Sensitivity Low

1:1 Retry Attempts 3

Fingerprint Image None

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

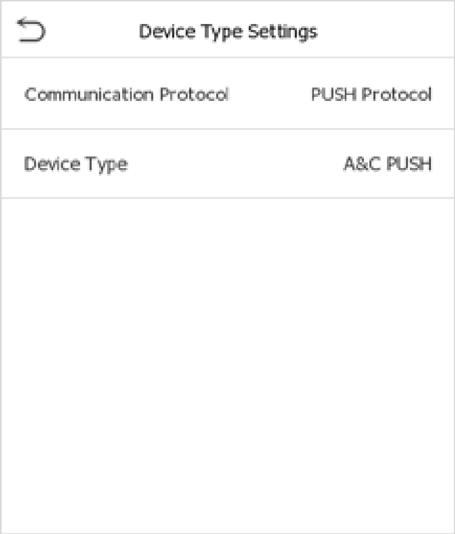
Function Description

Function Name	Descriptions
1:1 Match Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Match Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".

1:1 Retry Times	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available: **Show for enroll**: to display the fingerprint image on the screen only during enrollment. **Show for match**: to display the fingerprint image on the screen only during verification. **Always show**: to display the fingerprint image on screen during enrollment and verification. **None**: not to display the fingerprint image.

6.5 Device Type Setting

Tap **Device Type Setting** on the System interface.



Device Type Settings

Communication Protocol PUSH Protocol

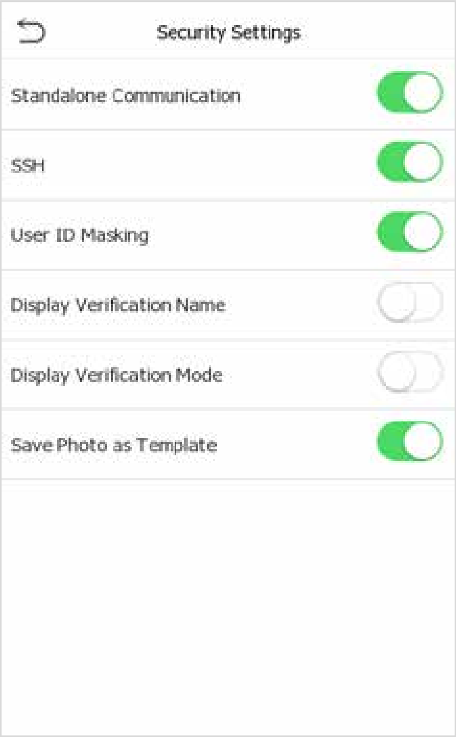
Device Type A&C PUSH

Function Description

Function Name	Description
Communication Protocol	Set the device communication protocol.
Device Type	Set the device as time attendance terminal (T&A PUSH) or access control terminal (A&C PUSH).

6.6 Security Setting

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



Security Settings

Standalone Communication ●

SSH ●

User ID Masking ●

Display Verification Name ○

Display Verification Mode ○

Save Photo as Template ●

Function Description

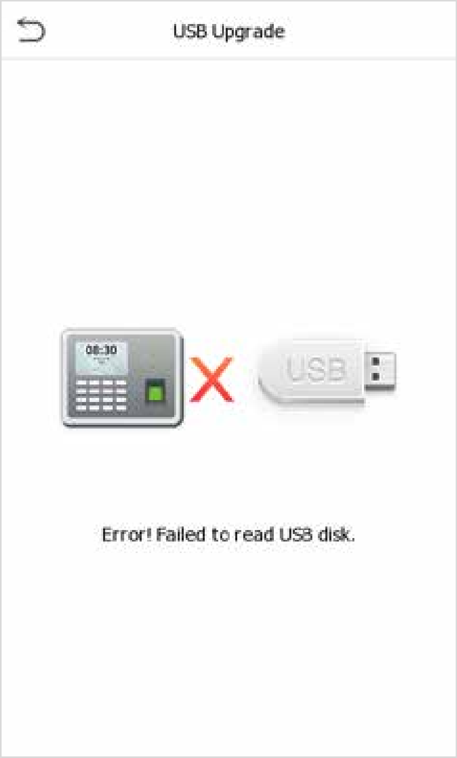
Function Name	Description
Standalone Communication	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
SSH	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
User ID Masking	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
Display Verification Name	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.
Display Verification Mode	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.
Save Photo as Template	After disabling this function, face template re-registration is required after an algorithm upgrade.

6.7 USB Upgrade

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

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

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



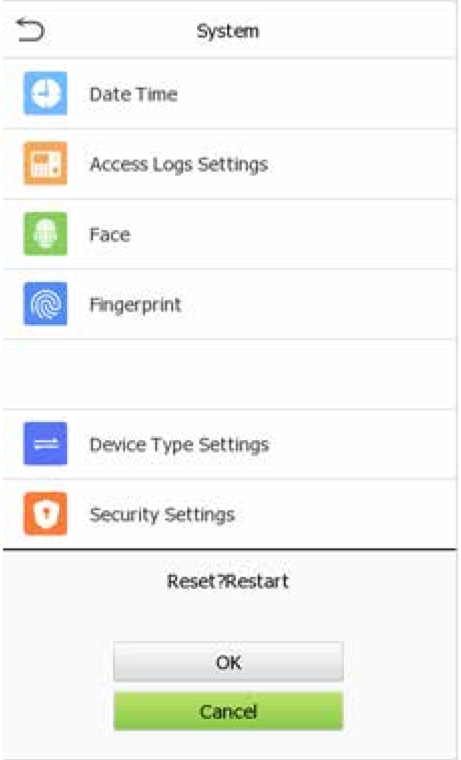
Error! Failed to read USB disk.

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

6.8 Factory Reset

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

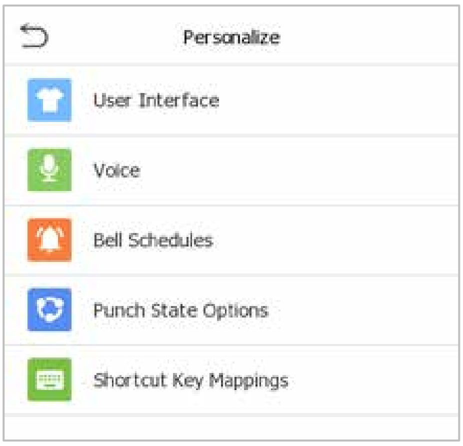
Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



Reset?Restart

7 Personalize Settings

Tap **Personalize** on the **Main Menu** interface to customize interface settings, voice, bell, punch state options and shortcut key mappings.



Personalize

User Interface

Voice

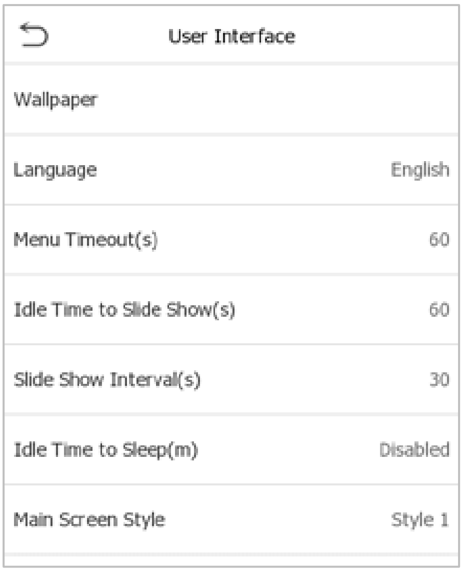
Bell Schedules

Punch State Options

Shortcut Key Mappings

7.1 User Interface Settings

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



User Interface

Wallpaper

Language English

Menu Timeout(s) 60

Idle Time to Slide Show(s) 60

Slide Show Interval(s) 30

Idle Time to Sleep(m) Disabled

Main Screen Style Style 1

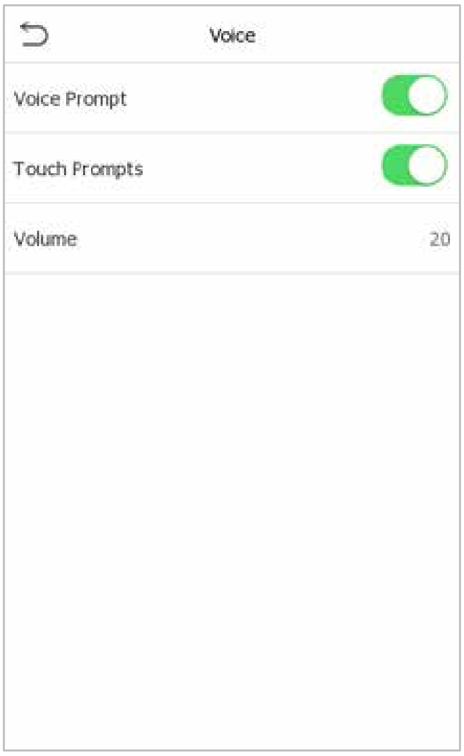
Function Description

Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	Select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. The function either can be disabled or set the required value between 60 and 99999 seconds.
Idle Time to Slide	When there is no operation, and the time exceeds the set value, a slide show will be played. The function can be disabled, or you may set the value between

Show (s)	3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show photos. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. Tap the screen anywhere to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

7.2 Voice Settings

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



Voice

Voice Prompt

Touch Prompts

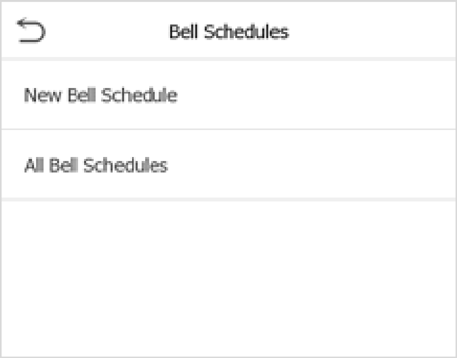
Volume 20

Function Description

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

7.3 Bell Schedules

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



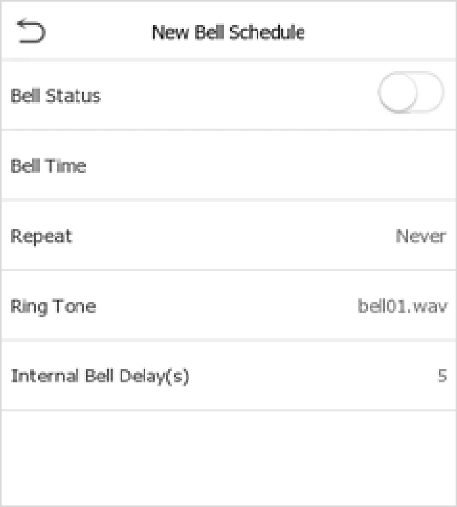
Bell Schedules

New Bell Schedule

All Bell Schedules

- **New bell schedule**

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



New Bell Schedule

Bell Status ○

Bell Time

Repeat Never

Ring Tone bell01.wav

Internal Bell Delay(s) 5

Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device will automatically trigger to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ring tone.
Internal Bell Delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

- **All bell schedules:**

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

- **Edit the scheduled bell:**

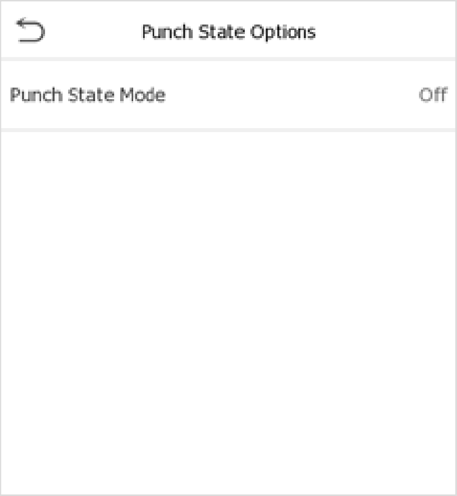
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **Delete a bell:**

On the **All Bell Schedules** interface, tap the required bell schedule, and tap **Delete**, and then tap **Yes** to delete the selected bell.

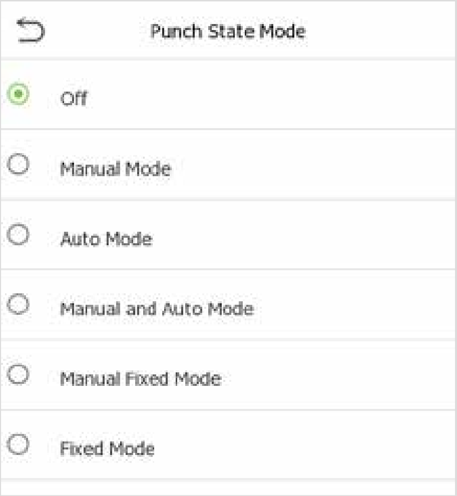
7.4 Punch States Options★

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



Punch State Options

Punch State Mode: Off



Punch State Mode

● Off

○ Manual Mode

○ Auto Mode

○ Manual and Auto Mode

○ Manual Fixed Mode

○ Fixed Mode

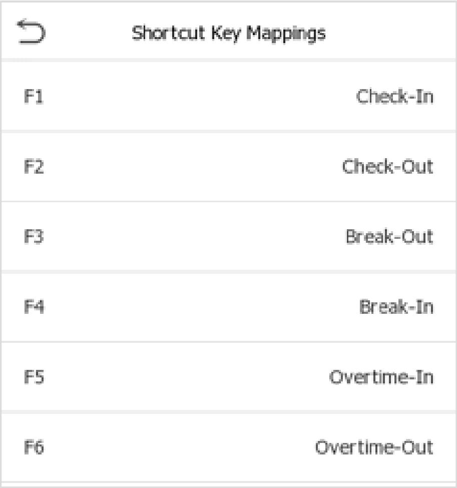
Function Description

Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.

7.5 Shortcut Key Mappings★

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

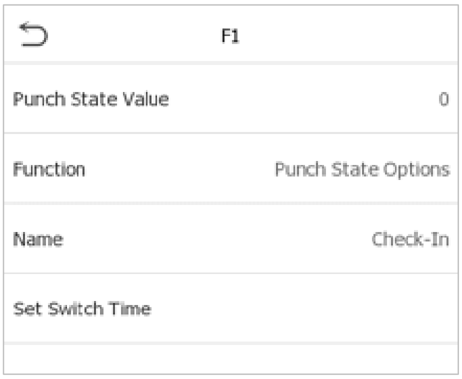
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.



Shortcut Key Mappings

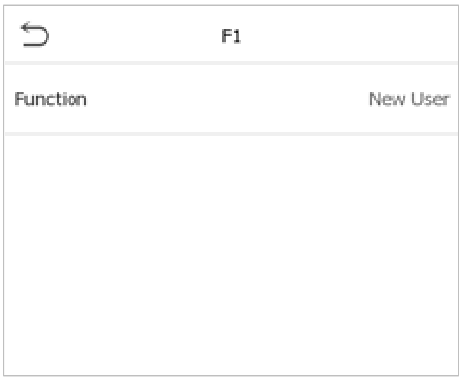
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (**that is "F1"**)** interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.



F1

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



F1

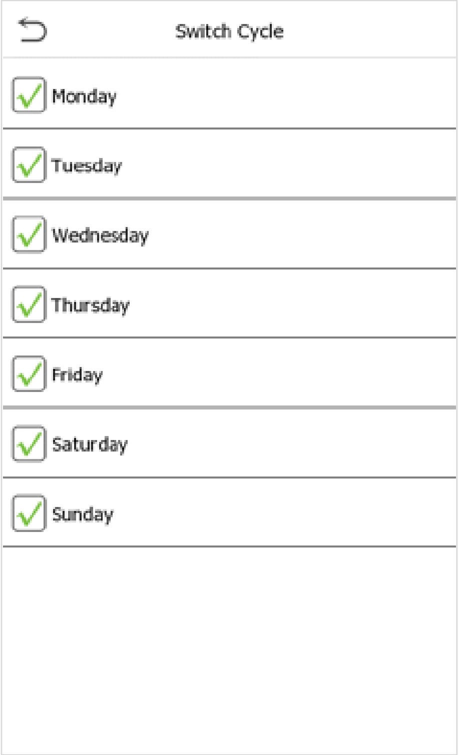
Function	New User

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

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

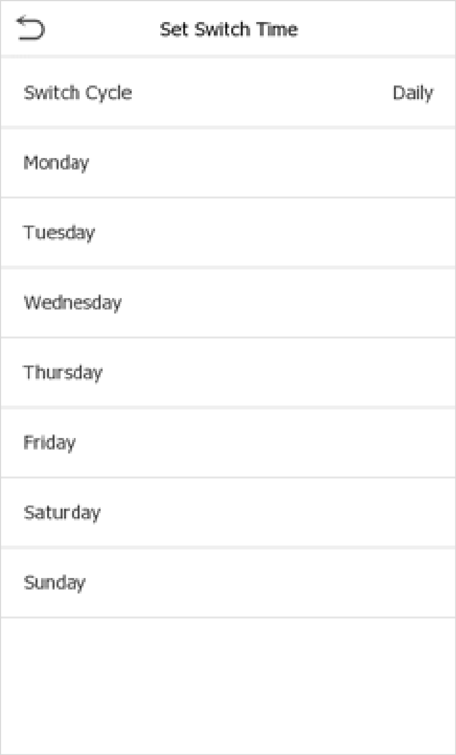
- **Set the Switch Time★**
  - The switch time is set in accordance with the punch state options.
  - When the **punch state mode** is set to **auto mode**, the switch time should be set.

- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday etc.) as shown in the image below.



Switch Cycle

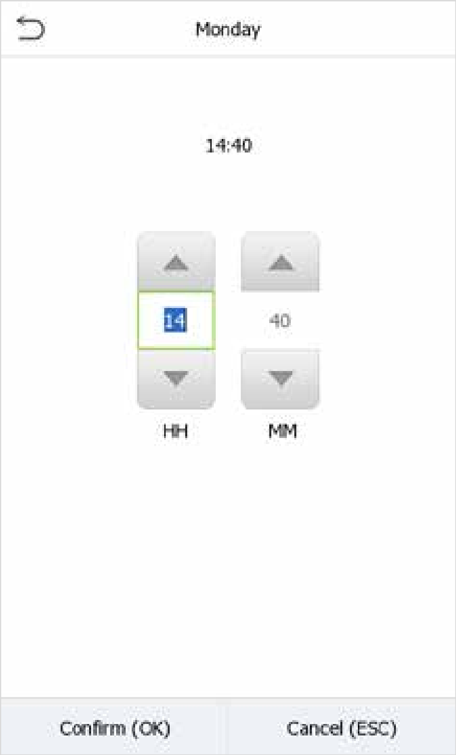
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday



Set Switch Time

Switch Cycle	Daily
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	
Saturday	
Sunday	

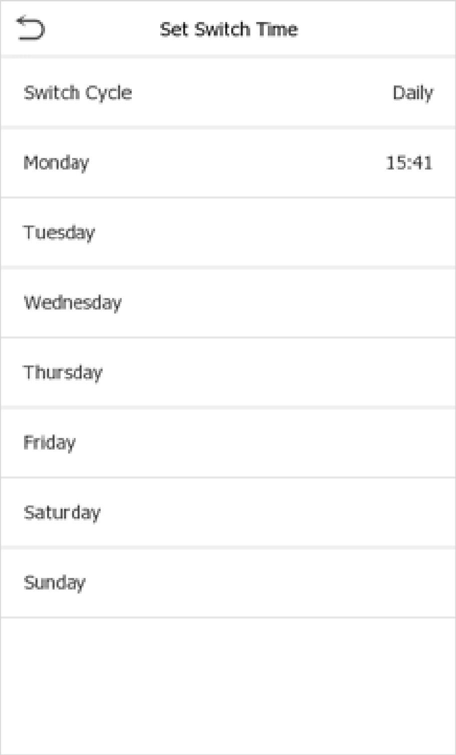
- Once the Switch cycle is selected, set the switch time for each day and tap **OK** to confirm, as shown in the image below.



Monday

14:40

HH: 14
MM: 40

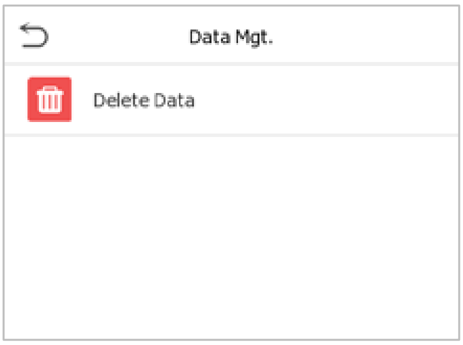


Set Switch Time

Switch Cycle	Daily
Monday	15:41
Tuesday	
Wednesday	
Thursday	
Friday	
Saturday	
Sunday	

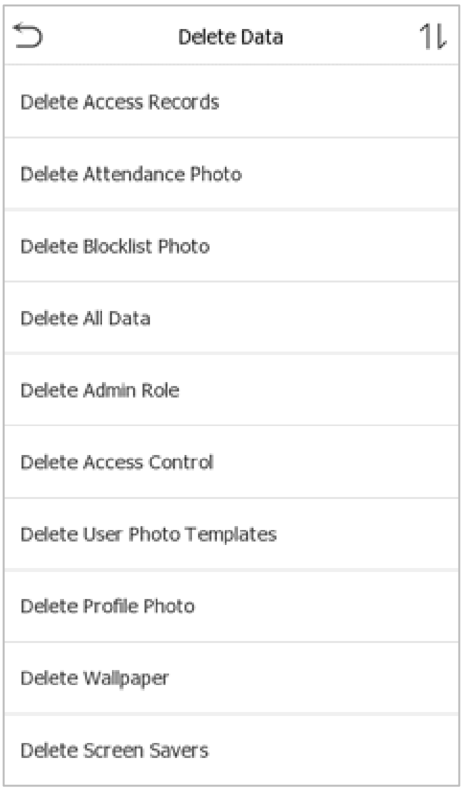
8 Data Management

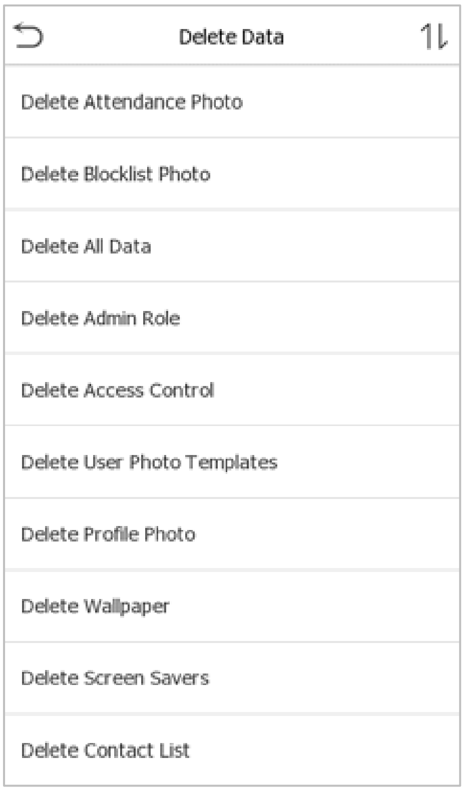
On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



8.1 Delete Data

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



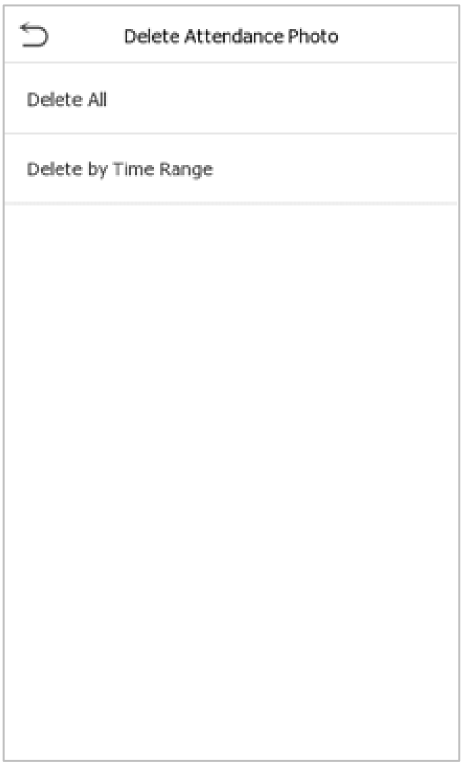


Function Description

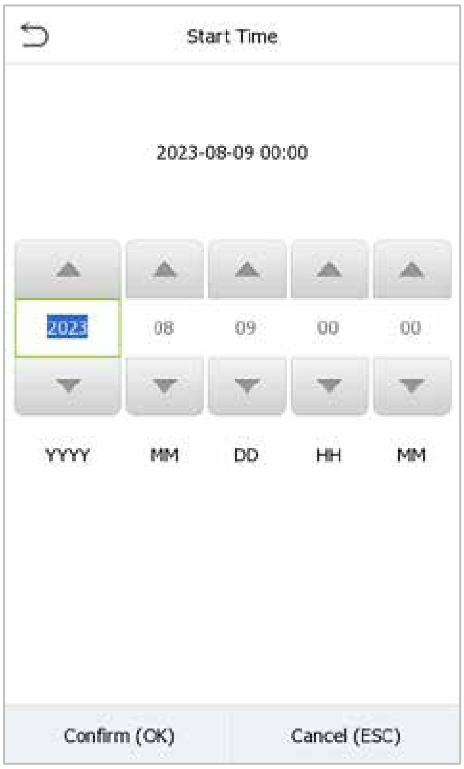
Function Name	Description
Delete Access Records	To delete access records conditionally.
Delete Attendance Data★	To delete attendance data conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all

	registered users.
Delete Admin Role	To remove all administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"
Delete Profile Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.
Delete Contact List	To delete all contact list of video intercom in the device.

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



Select **Delete by Time Range**.



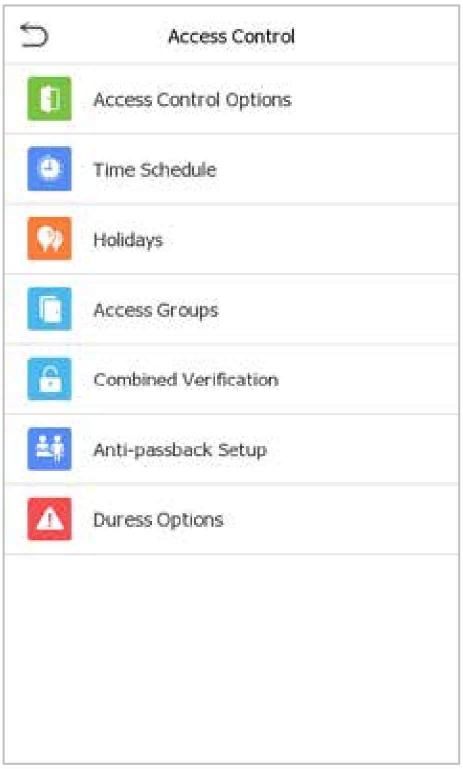
2023-08-09 00:00

2023 08 09 00 00

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

9 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of door opening, locks control and to configure other parameters settings related to access control.



Access Control

Access Control Options

Time Schedule

Holidays

Access Groups

Combined Verification

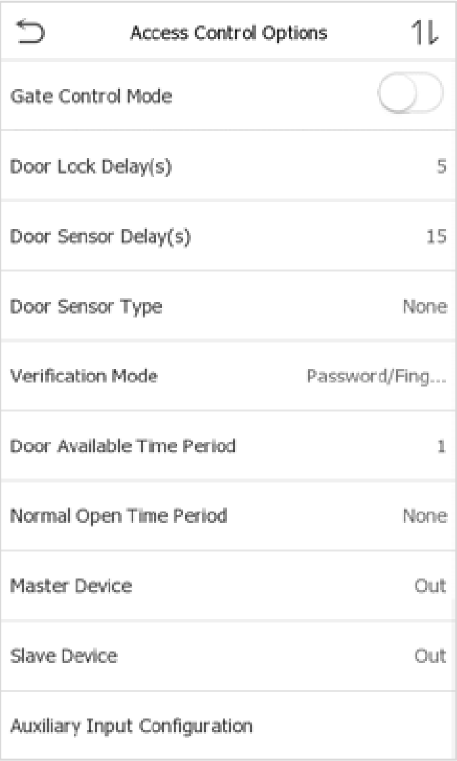
Anti-passback Setup

Duress Options

- **To gain access, the registered user must meet the following conditions:**
  - The relevant door's current unlock time should be within any valid time zone of the user time period.
  - The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members are also required to unlock the door).
  - In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

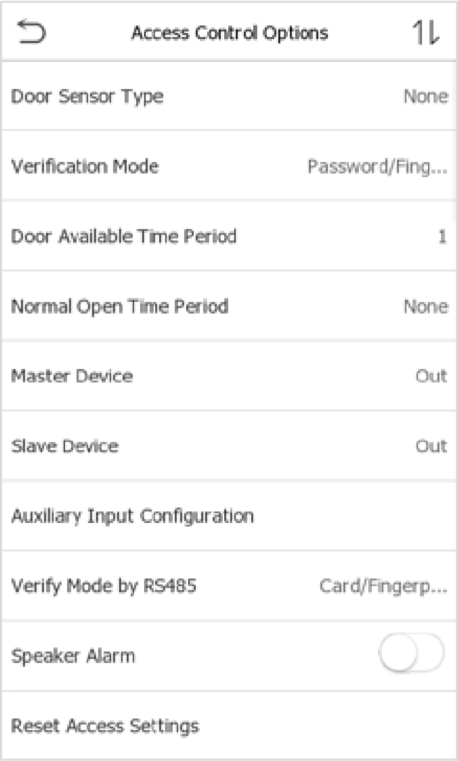
9.1 Access Control Options

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



Access Control Options

Gate Control Mode	○
Door Lock Delay(s)	5
Door Sensor Delay(s)	15
Door Sensor Type	None
Verification Mode	Password/Fing...
Door Available Time Period	1
Normal Open Time Period	None
Master Device	Out
Slave Device	Out
Auxiliary Input Configuration	



Access Control Options

Door Sensor Type	None
Verification Mode	Password/Fing...
Door Available Time Period	1
Normal Open Time Period	None
Master Device	Out
Slave Device	Out
Auxiliary Input Configuration	
Verify Mode by RS485	Card/Fingerp...
Speaker Alarm	○
Reset Access Settings	

Function Description

Function Name	Description
Gate Control Mode	Toggle between ON or OFF switch to get into gate control mode or not. When set to **ON**, on this interface will remove Door lock relay, Door sensor relay and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open** and **Normal Closed**. **None:** It means door sensor is not in use. **Normal Open:** It means the door is always left opened when electric power is on. **Normal Closed:** It means the door is always left closed when electric power is on.
Door Alarm Delay(s)★	When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specified time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds. 0 means immediate alarm.
Retry Times to Alarm★	When the number of failed verifications reach a set value, which ranges from 1 to 9 times, an alarm will be triggered. If the set value is "None", the alarm will never be triggered due to failed verifications.

Verification Mode	The supported verification mode includes Card/Fingerprint, Fingerprint Only, Card Only, Fingerprint + Password, Card + Password, Card + Fingerprint and Card + Fingerprint + Password.
Door Available Time Period	To set time period for door, so that the door is available only during that period.
Normal Close Time Period★	Scheduled time period for "Normal Close" mode, so that the door is always close during this period.
Normal Open Time Period	Scheduled time period for "Normal Open" mode, so that the door is always left open during this period.
Master Device	When setting up the master, the status of the master can be set to exit on enter. **Out:** The record verified on the host is the exit record. **In:** The record verified on the host is the entry record.
Slave Device	When setting up the slave, the status of the slave can be set to exit on enter. **Out:** The record verified on the host is the exit record. **In:** The record verified on the host is the entry record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card Only and Card + Password.
Valid Holidays★	To set if Normal Close Period or Normal Open Period settings are valid in set holiday time period. Choose ON to enable the functions during holiday.
Speaker Alarm	Transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.
Reset Access Settings	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

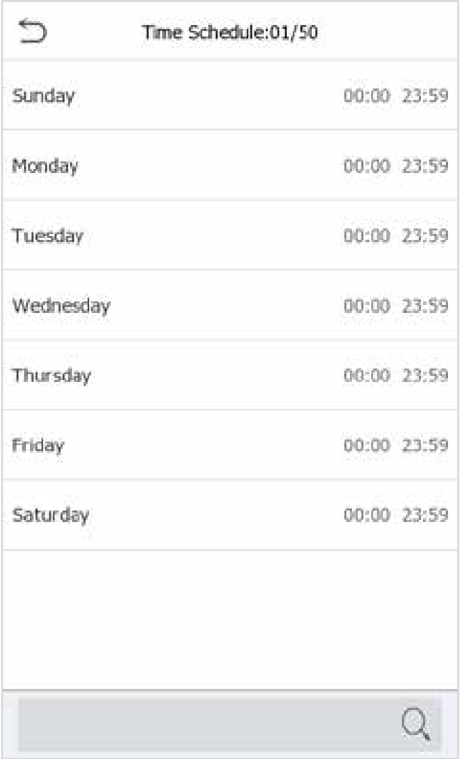
9.2 Time Rule Setting

Tap **Time Rule Setting** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.

- Each Time Period represents **10** Time Zones, i.e. **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time periods is "**OR**". Thus, when the verification time falls in any one of these time periods, the verification is valid.
- The Time Zone format of each Time Period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

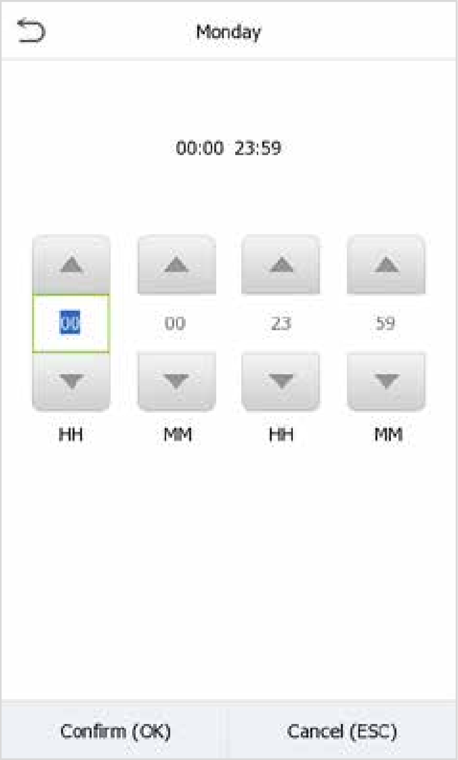
Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum: up to 50 zones).



Time Schedule:01/50

Sunday	00:00 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59
Wednesday	00:00 23:59
Thursday	00:00 23:59
Friday	00:00 23:59
Saturday	00:00 23:59

On the selected Time Zone number interface, tap on the required day (that is Monday, Tuesday etc.) to set the time.



Specify the start and the end time, and then tap **OK**.

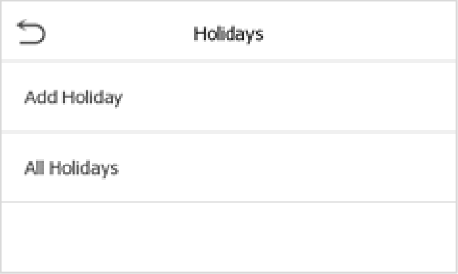
Notes:

- When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.
- When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.
- The effective Time Period to keep the Door Unlock or open all day is (00:00~23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00~23:59).
- The default Time Zone 1 indicates that door is open all day long.

9.3 Holidays

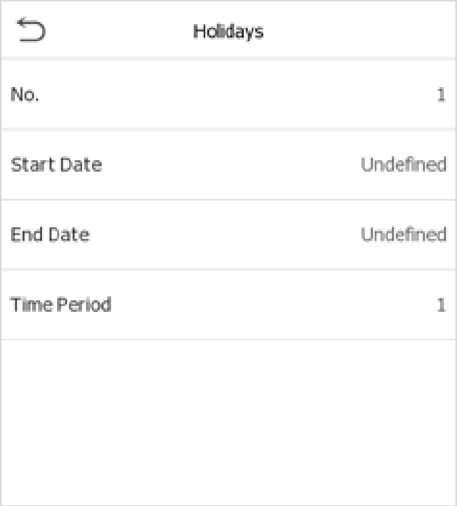
Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which is applicable to all employees, and the user will be able to open the door during the holidays.

Tap **Holidays** on the **Access Control** interface to set the Holiday access.



- **Add a new holiday:**

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



Holidays

No.	1
Start Date	Undefined
End Date	Undefined
Time Period	1

- **Edit a holiday:**

On the **Holidays** interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

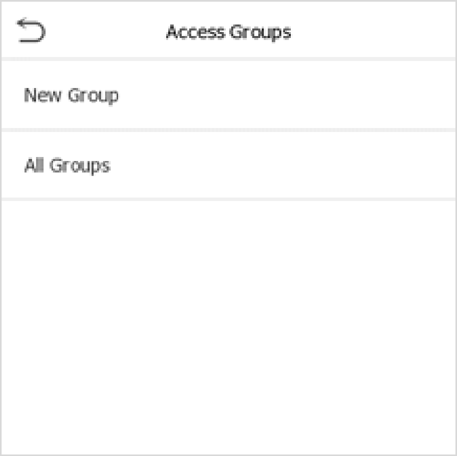
- **Delete a Holiday:**

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

9.4 Access Groups

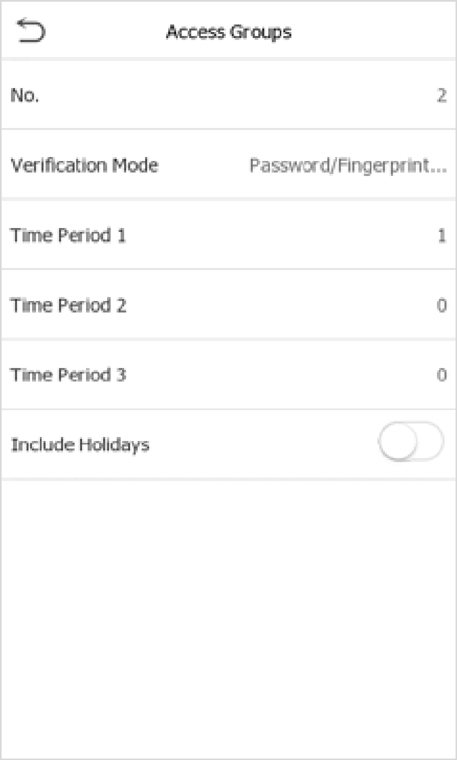
This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication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

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



- **Add a New Group**

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



Access Groups

No. 2

Verification Mode Password/Fingerprint...

Time Period 1 1

Time Period 2 0

Time Period 3 0

Include Holidays

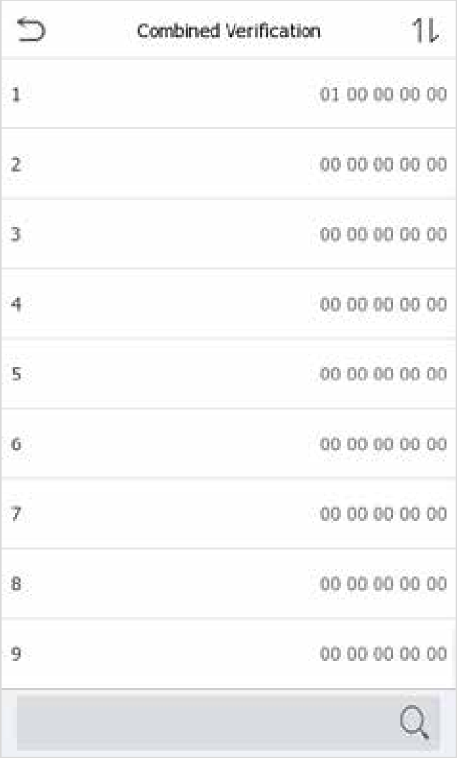
Notes:

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

9.5 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen the security. In a door-unlocking combination, the range of the combined number N is: 0 ≤ N ≤ 5, and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification** on the **Access Control** interface to configure the combined verification setting.



Combined Verification

1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00

On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then press **OK**.

For Example:

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group** 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.
- The **Door-unlock combination 2** is set as **(02 02 04 04 07)**, indicating that the unlock combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlock combination 3** is set as **(09 09 09 09 09)**, indicating that there are 5 people in this combination; all of which are from AC group 9.
- The **Door-unlock combination 4** is set as **(03 05 08 00 00)**, indicating that the unlock combination 4 consists of only three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

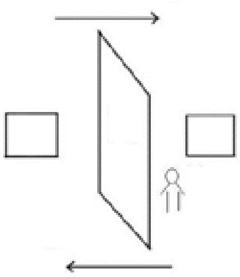
- **Delete a Door-unlocking Combination:**

Set all Door-unlock combinations to 0 if you want to delete door-unlock combinations.

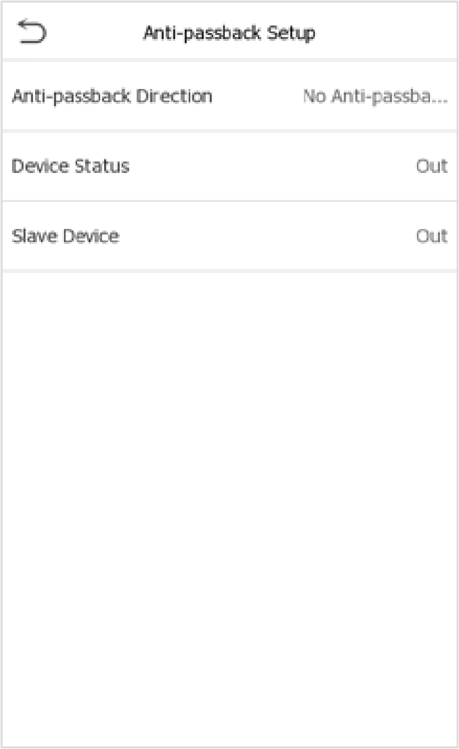
9.6 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), and the other one is installed outside the door (slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap **Anti-passback Setup** on the **Access Control** interface.



Anti-passback Setup

Anti-passback Direction: No Anti-passba...

Device Status: Out

Slave Device: Out

Function Description

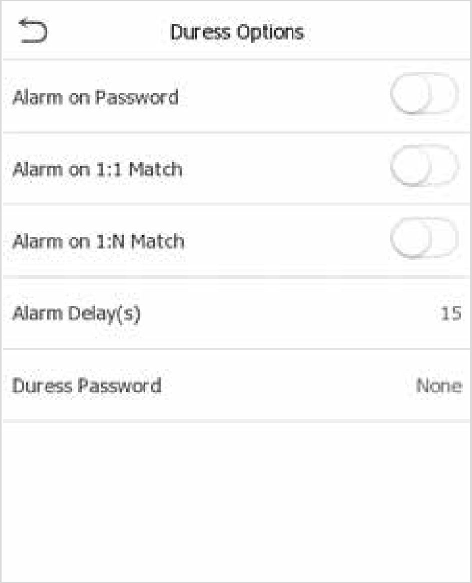
Function Name	Description

Anti-passback Direction	**No Anti-passback:** Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely. **In Anti-passback:** After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely. **In/Out Anti-passback:** After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.
Device Status★	Set the state of the device as **Out** or **In**. **Out**: A record of verification on the device is a check-out record. **In**: A record of verification on the device is a check-in record.
Slave Device★	While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**. **Out**: A record of verification on the slave device is a check-out record. **In**: A record of verification on the slave device is a check-in record.

9.7 Duress Options

Once a user activates the duress verification function with specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device will unlock the door as usual, but at the same time, a signal will be sent to trigger the alarm.

On **Access Control** interface, tap **Duress Options** to configure the duress settings.



Duress Options

Alarm on Password ○

Alarm on 1:1 Match ○

Alarm on 1:N Match ○

Alarm Delay(s) 15

Duress Password None

Function Description

Function Name	Description

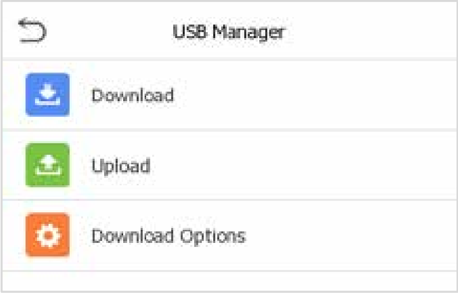
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated, otherwise there will be no alarm signal.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

10 USB Manager

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

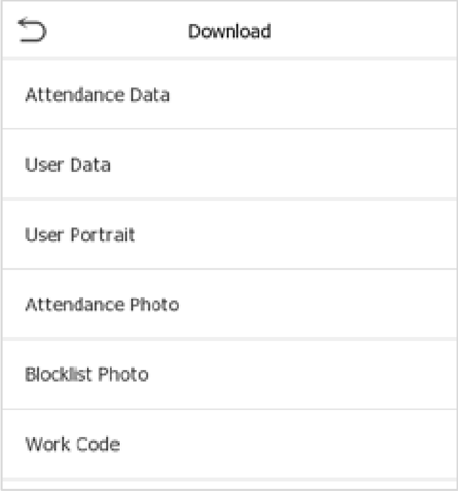
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

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



10.1 USB Download

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

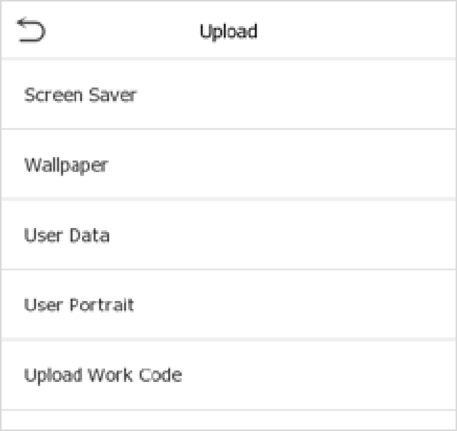


Function Description

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

10.2 USB Upload

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



Upload

Screen Saver

Wallpaper

User Data

User Portrait

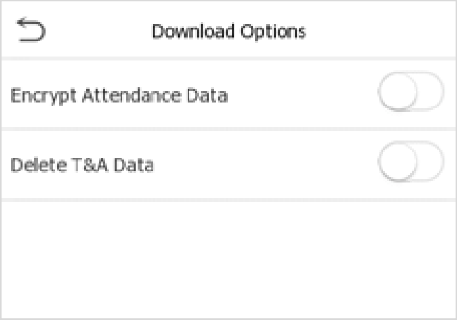
Upload Work Code

Function Description

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

10.3 Download Options★

It is used to encrypt attendance data in the USB disk or delete attendance data. On the **USB Manager** interface, click **Download Options**.



Download Options

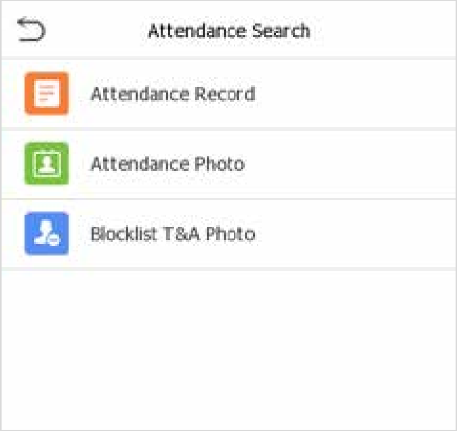
Encrypt Attendance Data ○

Delete T&A Data ○

11 Attendance Search

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

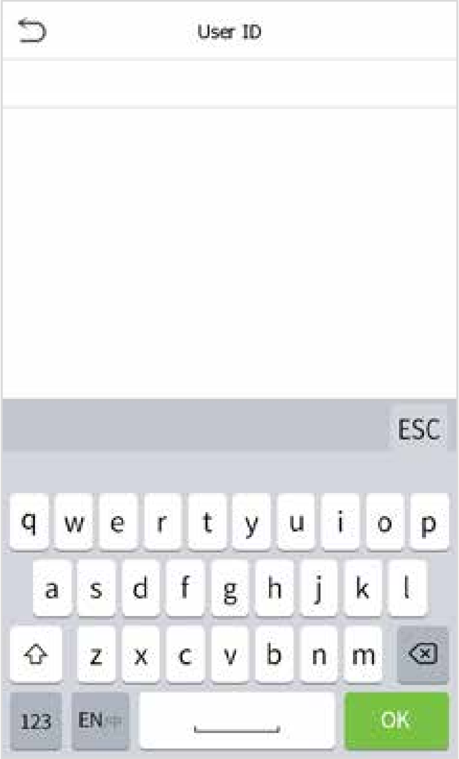
Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



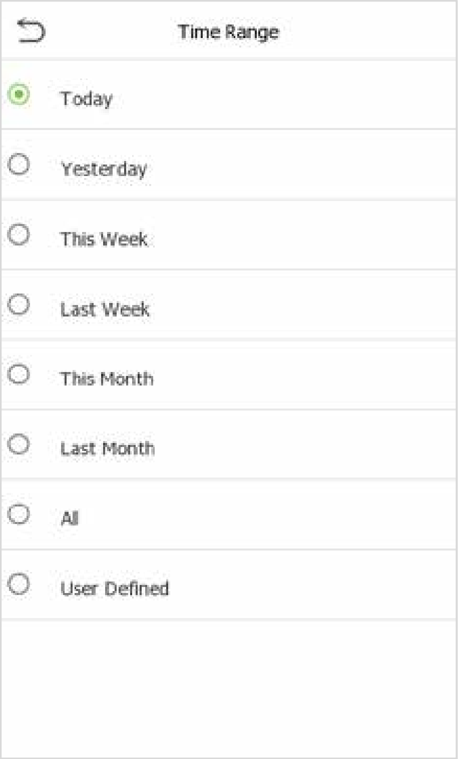
The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

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



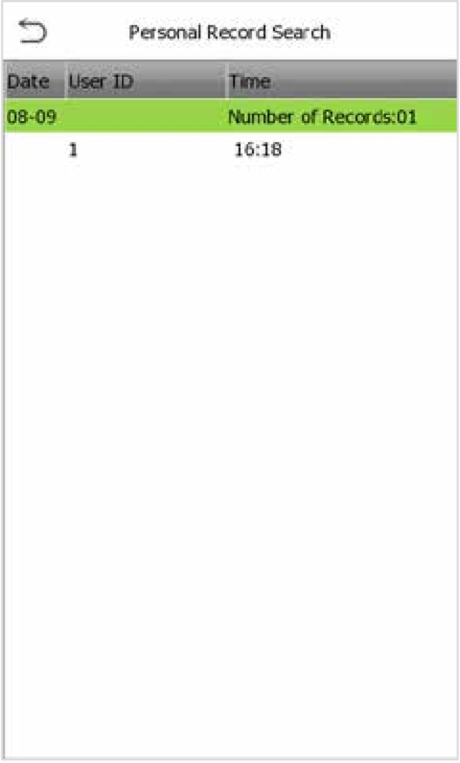
2. Select the time range in which the logs need to be searched.



3. Once the log search succeeds. Tap the login

4. The below figure shows the details of the

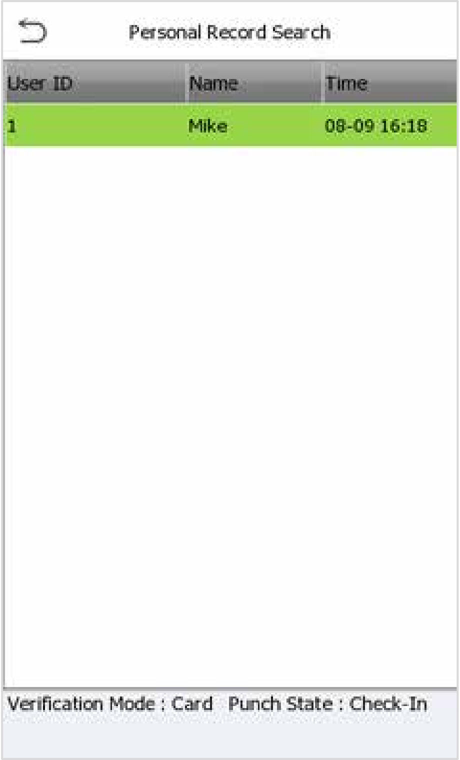
highlighted in green to view its details.



Personal Record Search

Date	User ID	Time
08-09		Number of Records:01
	1	16:18

selected log.



Personal Record Search

User ID	Name	Time
1	Mike	08-09 16:18

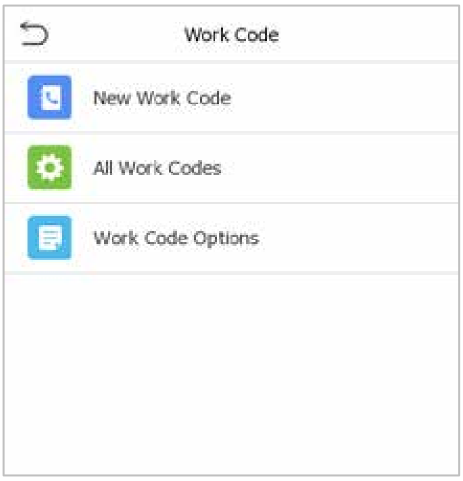
Verification Mode : Card   Punch State : Check-In

12 Work Code★

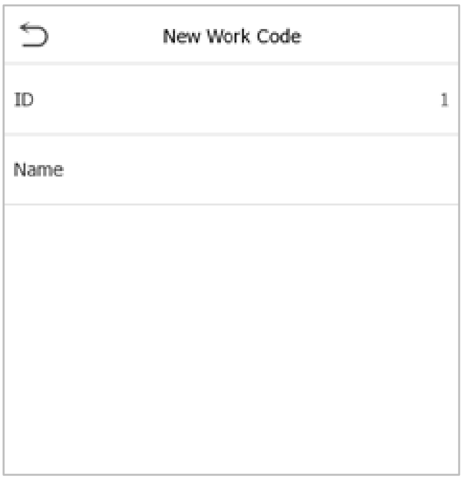
Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate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

Note: Only can use in the T&A PUSH, please refer to 6.5 Device Type Setting.

Tap **Work Code** on the **Main Menu** interface.



12.1 Add a Work Code


New Work Code

ID 1

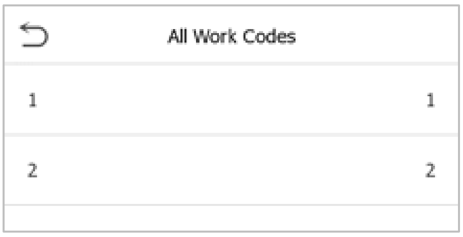
Name

Function Description

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

12.2 All Work Codes

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

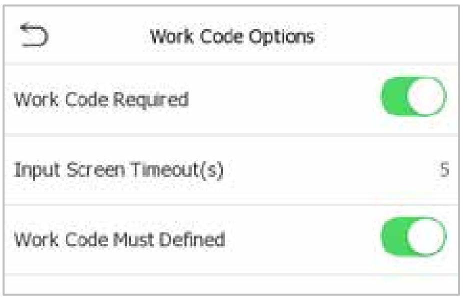


All Work Codes

1	1
2	2

12.3 Work Code Options

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



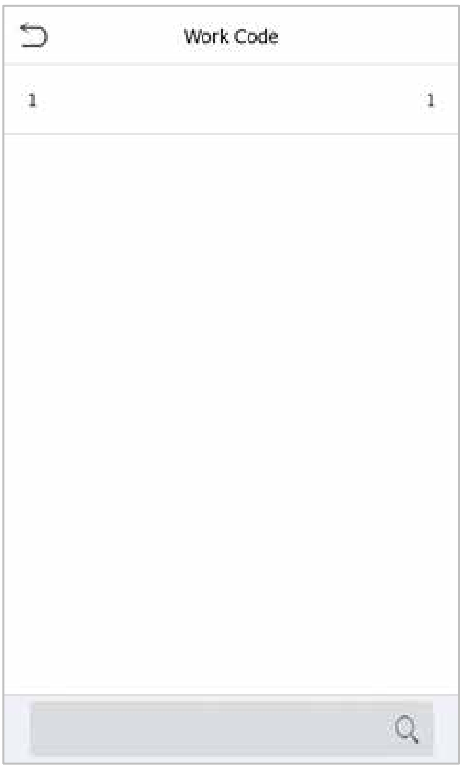
Work Code Options

Work Code Required: on

Input Screen Timeout(s): 5

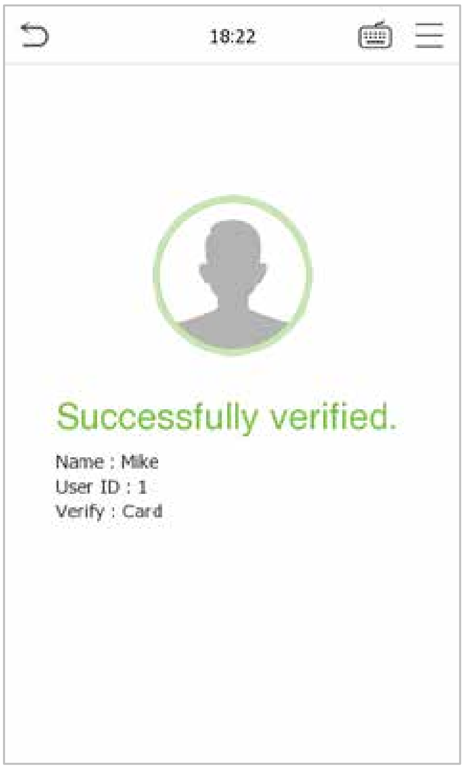
Work Code Must Defined: on

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



Work Code

1	1



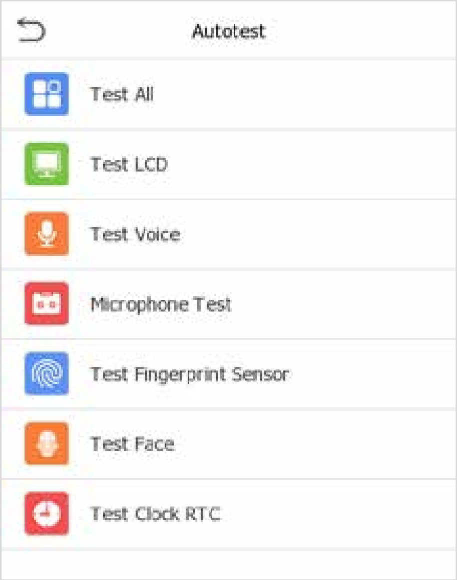
18:22

Successfully verified.

Name : Mike
User ID : 1
Verify : Card

13 Autotest

On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, Voice, Camera and Real-Time Clock (RTC).


Autotest

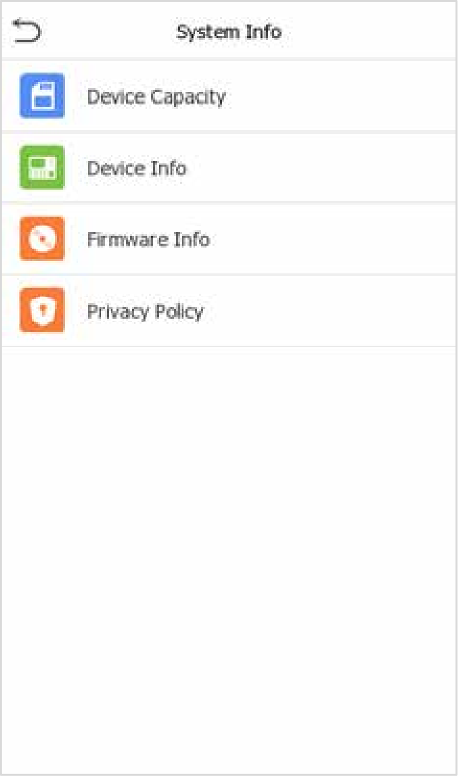
- Test All
- Test LCD
- Test Voice
- Microphone Test
- Test Fingerprint Sensor
- Test Face
- Test Clock RTC

Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Audio, Camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Microphone Test	Check whether the microphone is working by speaking to microphone and playing the microphone recording.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Face	To test if the camera functions properly by checking the photos taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

14 System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, and firmware information.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, password, face template and card storage, administrators, access records, attendance and blocklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face template algorithm, version information, platform information, and manufacturer and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After clicking "**I have read it**," the customer can use the product regularly. Click **System Info > Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in Simplified Chinese/ English. However, translation of other multi-language content is underway, with more iterations.

Appendix 1

Requirements of Live Collection and Registration of Visible Light Face Templates

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.

2) Do not place the device towards outdoor light sources like door or window or other harsh light sources.

3) Dark-color apparels, different from the background color is recommended for registration.

4) Please expose your face template and forehead properly and do not cover your face template and eyebrows with your hair.

5) It is recommended to show a plain facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).

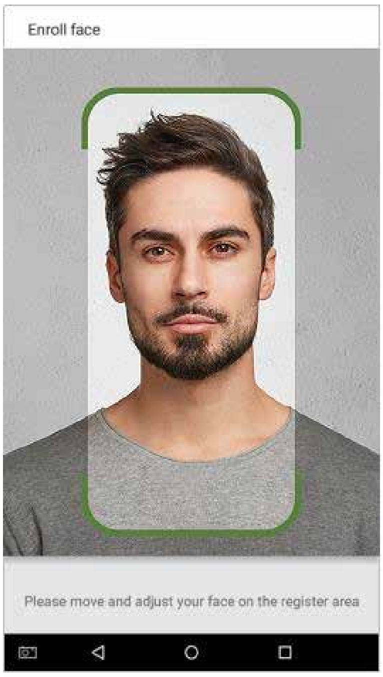
6) Two templates are required for a person with eyeglasses, one template with eyeglasses and the other without the eyeglasses.

7) Do not wear accessories like a scarf or mask that may cover your mouth or chin.

8) Please face template right towards the capturing device, and locate your face template in the template capturing area as shown in the template below.

9) Do not include more than one face template in the capturing area.

10) A distance of 50cm to 80cm is recommended for capturing the template. (The distance is adjustable, subject to body height).



Enroll face

Please move and adjust your face on the register area

Requirements for Visible Light Digital Face Template Data

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

- **Eye distance**

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

- **Facial expression**

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

- **Gesture and angel**

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

- **Accessories**

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

- **Face template**

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

- **Template format**

Should be in BMP, JPG or JPEG.

- **Data requirement**

Should comply with the following requirements:

1）White background with dark-colored apparel.

2）24bit true color mode.

3）JPG format compressed template with not more than 20kb size.

4）Resolution should be between 358 x 441 to 1080 x 1920.

5）The vertical scale of head and body should be in a ratio of 2:1.

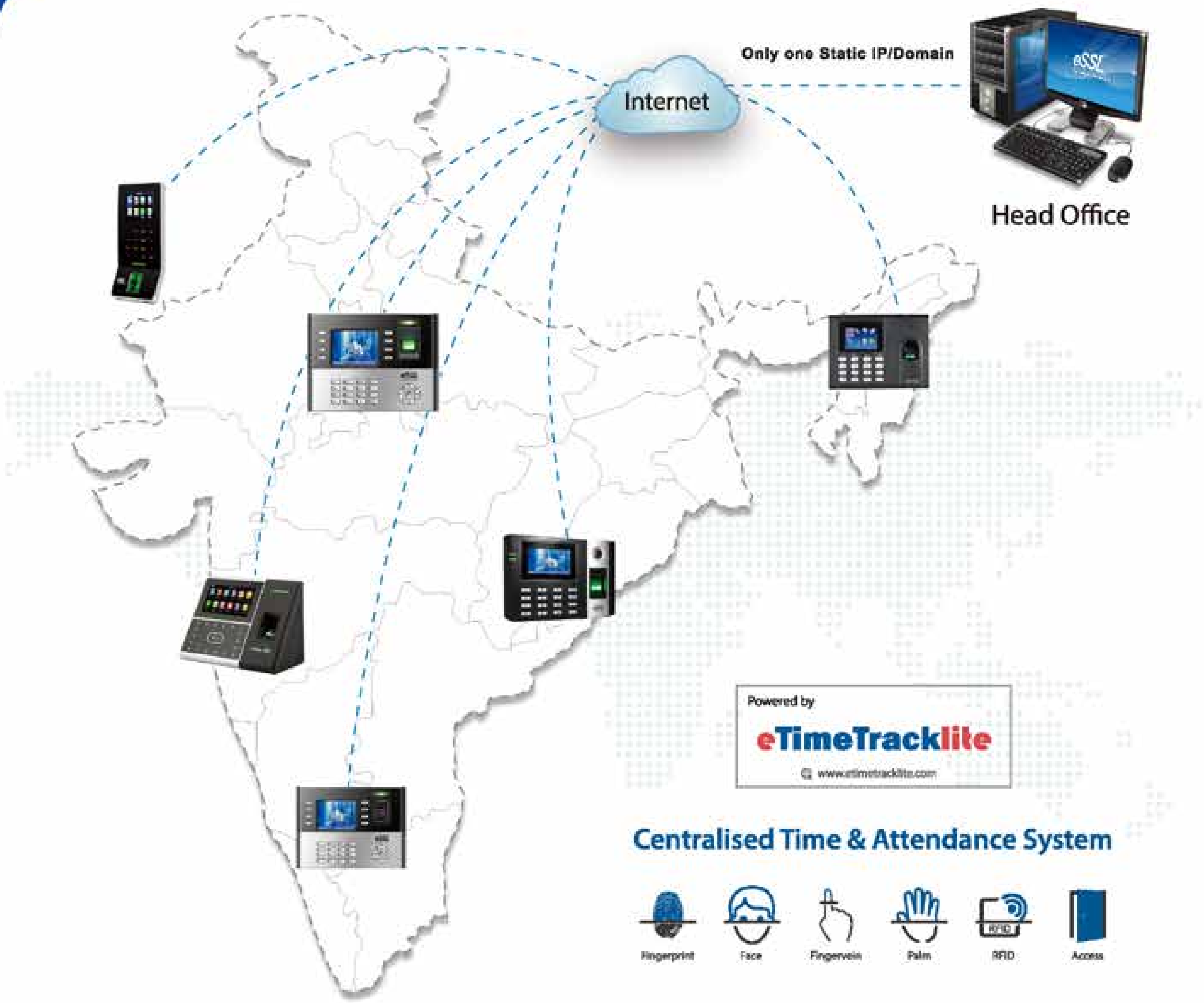
6）The photo should include the captured person's shoulders at the same horizontal level.

7）The captured person's eyes should be open and with clearly seen iris.

8）Neutral face template or smile is preferred, showing teeth is not preferred.

9）The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face template or background. The contrast and lightness level should be appropriate.

Manage Time & Attendance for all your Branches from Head Office



Disclaimer : Specifications can be changed without prior notice.

1. Buying and Selling eSSL products online is prohibited and is termed as illegal
2. Installation / Technical support / Training to end user is the responsibility of the installer or dealer
3. eSSL do not support end user directly, if they want support charges will be applicable

Enterprise Software Solutions Lab Pvt. Ltd. (Corporate-Office)
#24, 23rd main, Shambhavi Building, J P nagar 2nd phase, Bengaluru - 560078
www.esslsecurity.com | sales@esslsecurity.com | Ph : 91-8026090500