eSSL®
Security at Fingertips

MANUAL

AIFACE JUPITER

Table of Contents

1 INSTRUCTION FOR USE 4

1.1 FINGER POSITIONING 4
1.2 STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE 4
1.3 FACE REGISTRATION 5
1.4 STANDBY INTERFACE 6
1.5 VIRTUAL KEYBOARD 8
1.6 VERIFICATION MODE 9
1.6.1 FINGERPRINT VERIFICATION 9
1.6.2 CARD VERIFICATION 12
1.6.3 FACIAL VERIFICATION 15
1.6.4 PASSWORD VERIFICATION 18
1.6.5 COMBINED VERIFICATION 20

2 MAIN MENU 22

3 USER MANAGEMENT 24

3.1 USER REGISTRATION 24
3.1.1 REGISTER A USER ID AND NAME 24
3.1.2 SETTING THE USER ROLE 25
3.1.3 REGISTER FINGERPRINT 26
3.1.4 REGISTER FACE 27
3.1.5 REGISTER CARD NUMBER 28
3.1.6 REGISTER PASSWORD 28
3.1.7 REGISTER USER PHOTO 29
3.1.8 ACCESS CONTROL ROLE 29
3.2 SEARCH USER 31
3.3 EDIT USER 32
3.4 DELETING USER 32
3.5 DISPLAY STYLE 33

4 USER ROLE 34

5 COMMUNICATION SETTINGS 36

5.1 NETWORK SETTINGS 36
5.2 SERIAL COMM★ 37
5.3 PC CONNECTION 38
5.4 WIRELESS NETWORK 39
5.5 CLOUD SERVER SETTING 41
5.6 WIEGAND SETUP 42
5.6.1 WIEGAND INPUT 42
5.6.2 WIEGAND OUTPUT 44
5.7 NETWORK DIAGNOSIS 45

6 SYSTEM SETTINGS 46

6.1 DATE AND TIME 46
6.2 ACCESS LOGS SETTING 48

6.3 FACE PARAMETERS 49
6.4 FINGERPRINT PARAMETERS 51
6.5 SECURITY SETTINGS 52
6.6 FACTORY RESET 54
6.7 DETECTION MANAGEMENT★ 55

7 PERSONALIZE SETTINGS 56

7.1 INTERFACE SETTINGS 56
7.2 VOICE SETTINGS 57
7.3 BELL SCHEDULES 58
7.4 PUNCH STATES OPTIONS 59
7.5 SHORTCUT KEYS MAPPINGS 60

8 DATA MANAGEMENT 61

8.1 DELETE DATA 61

9 ACCESS CONTROL 63

9.1 ACCESS CONTROL OPTIONS 64
9.2 TIME SCHEDULE 65
9.3 HOLIDAYS 67
9.4 COMBINED VERIFICATION 68
9.5 ANTI-PASSBACK SETUP 69
9.6 DURESS OPTIONS SETTINGS 70

10 ATTENDANCE SEARCH 71

11 AUTOTEST 73

12 SYSTEM INFORMATION 74

APPENDIX 1 75

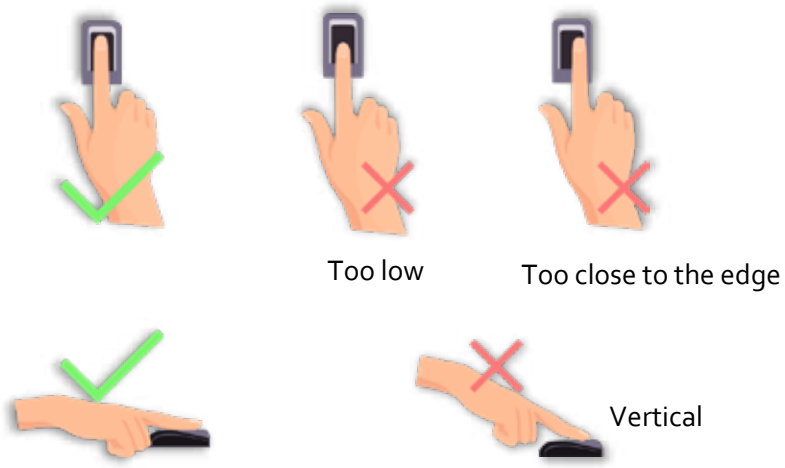
REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE TEMPLATES 75
REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE TEMPLATE DATA 76

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

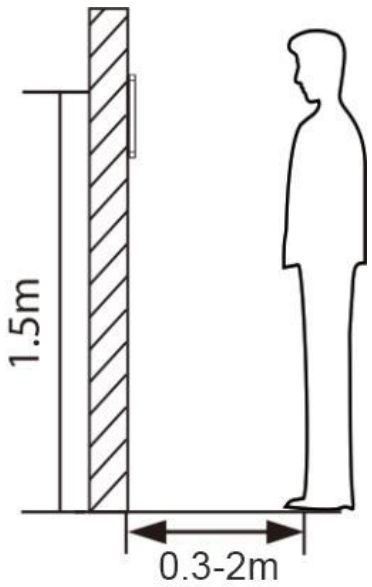
Recommended fingers: Index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.



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.

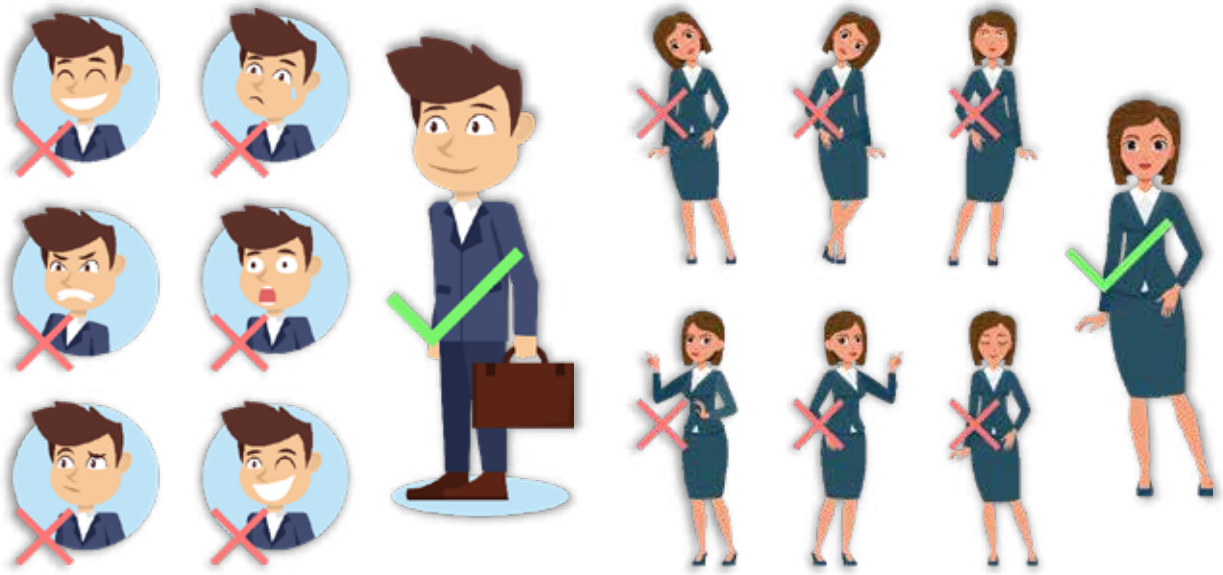
1.2 Standing Position, Facial Expression and Standing Posture

- **The Recommended Distance**



The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the character of facial images captured.

- **Recommended Standing Posture and Facial Expression**



Facial Expression **Standing Posture**

Note: Please keep your facial expression and standing posture natural while enrolment or verification.

1.3 Face Registration

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

- **Correct Face Registration and Authentication Method**

Recommendation for Registering a Face

- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful to keep your facial expression natural and not to change. (smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses or eyeglasses.
- Be careful not to display two faces on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

Recommendation for Authenticating a Face

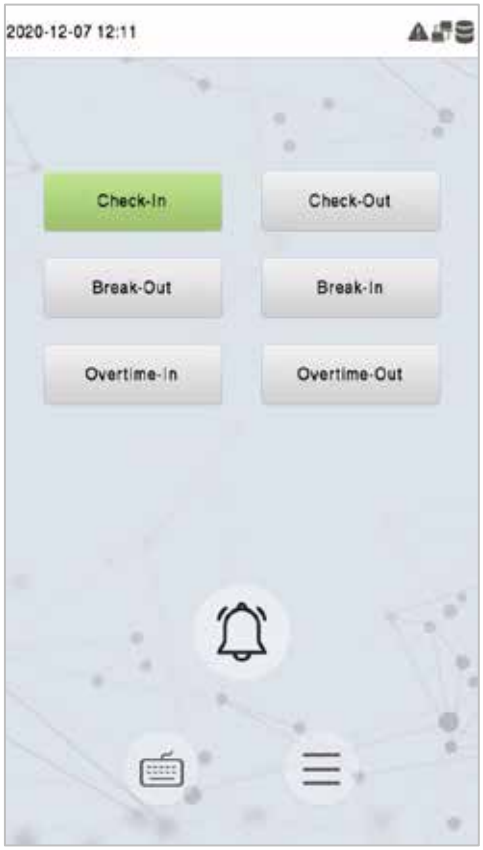
- Ensure that the face appears inside the guideline displayed on the screen of the device.
- Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

1.4 Standby Interface

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

- Tap to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.

  Note: For the security of the device, it is recommended to register a super administrator the first time you use the device.
- The punch state options can also be displayed and used directly on the standby interface. Tap 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. Please refer to "Shortcut Key Mappings" for the specific operation method.

  Note: The punch state options are off by default and need to select other mode options in the "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.

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

1.6 Verification Mode

1.6.1 Fingerprint Verification

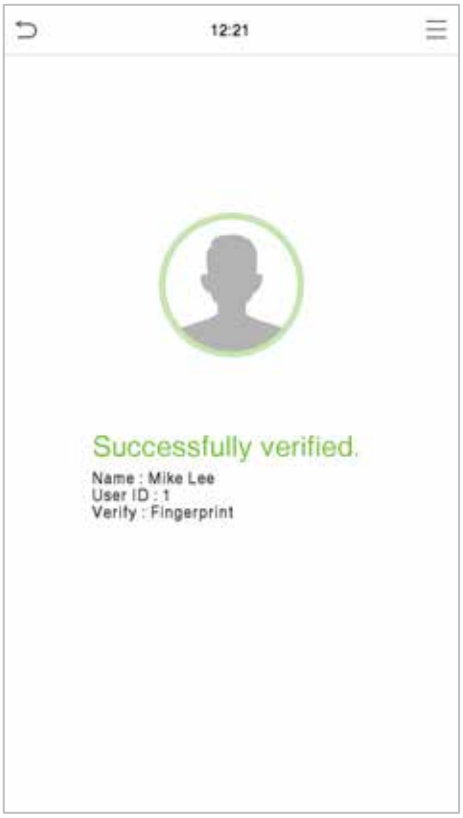
- **1: N Fingerprint Verification Mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

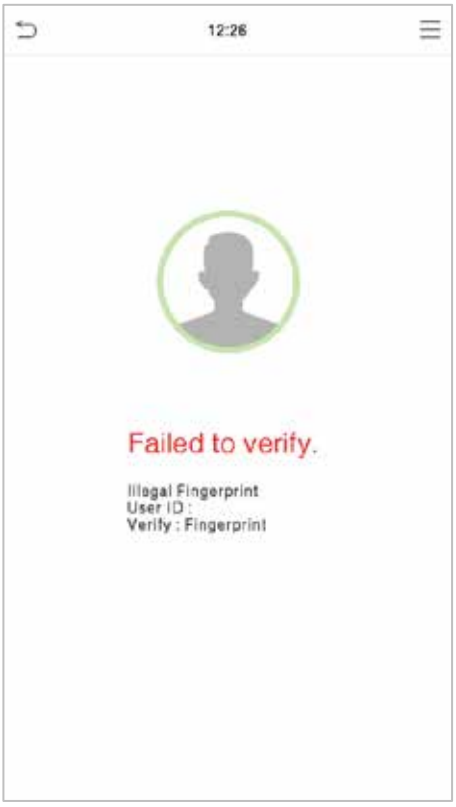
The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

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

Verification is successful:



Verification is failed:



- **1: 1 Fingerprint Verification Mode**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

Users may verify their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

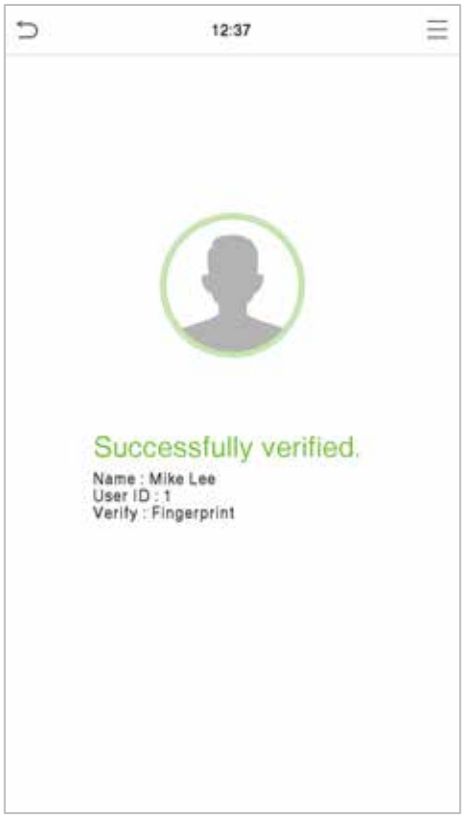
Click the button on the main screen to enter 1:1 fingerprint verification mode.

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

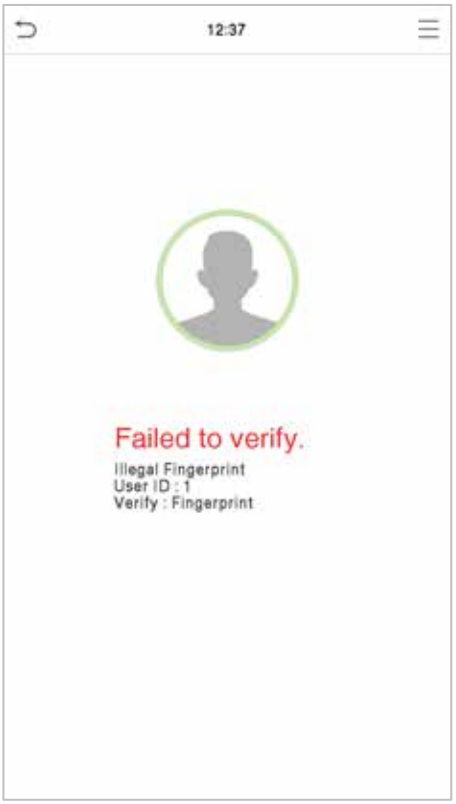
If the user has registered face and password in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Face verification, the following screen will appear. Select the fingerprint icon to  enter fingerprint verification mode.

Press the fingerprint to verify.

Verification is successful:



Verification is failed:



1.6.2 Card Verification

- **1:N Card Verification**

It compares the acquired card information with all card data registered in the device. The following is the pop-up prompt box of comparison results.

- **1:1 Card Verification**

Compares the card that is being put onto the card reader with the card data that related to the entered user ID.

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

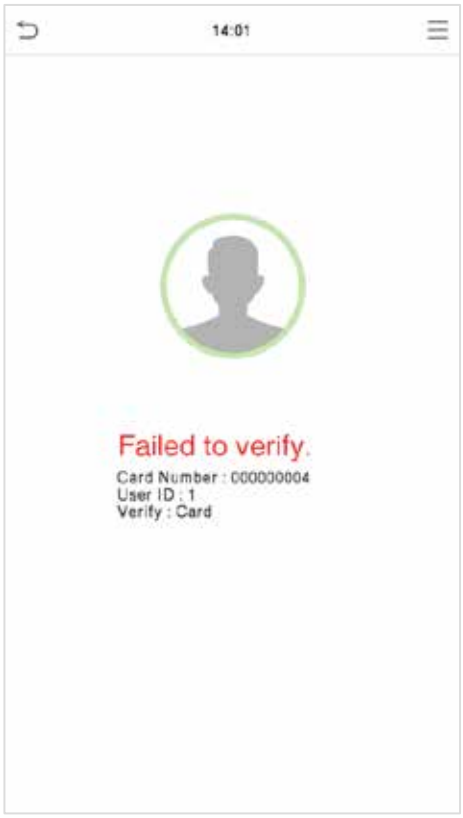
Enter the user ID and click **OK**.

If an employee registers a fingerprint in addition to the card, the following screen will appear. Select the  icon to enter card verification mode.

Following are the display screen after putting a correct card and a wrong card respectively.

Verification is successful:

Verification is failed:

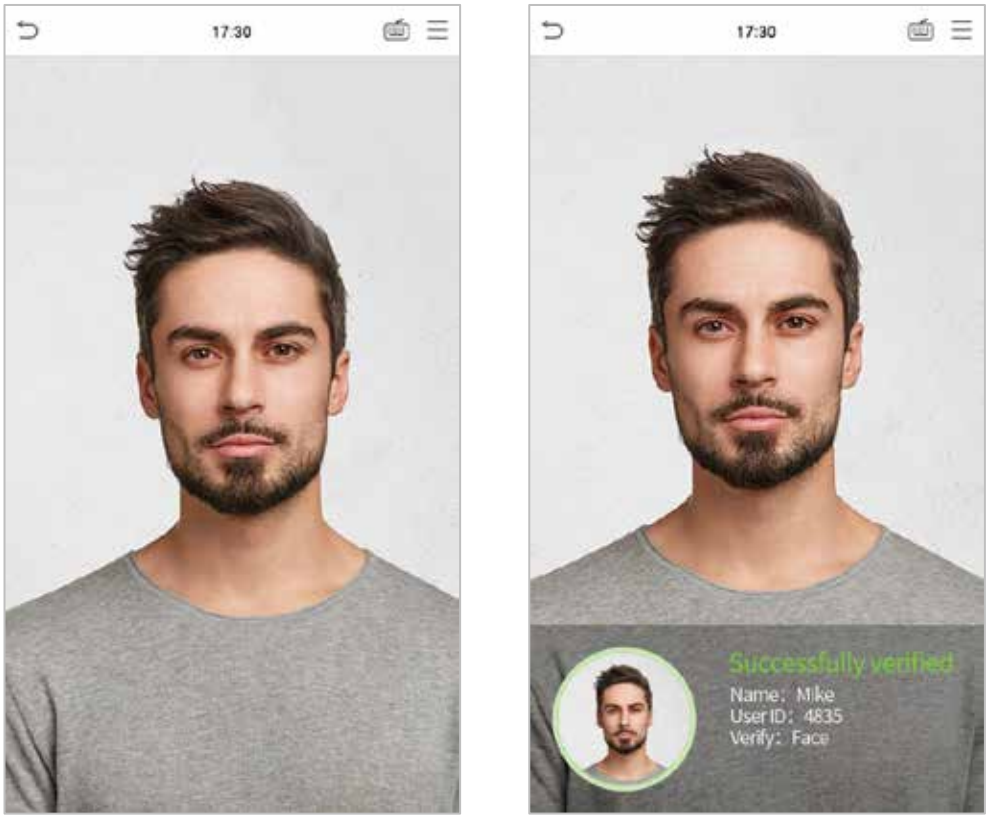


1.6.3 Facial Verification

- **1:N Facial Verification**

Conventional Verification

In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



- **1:1 Facial Verification**

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

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

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

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

Select the  icon to enter face verification mode.

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

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 of the given User ID.

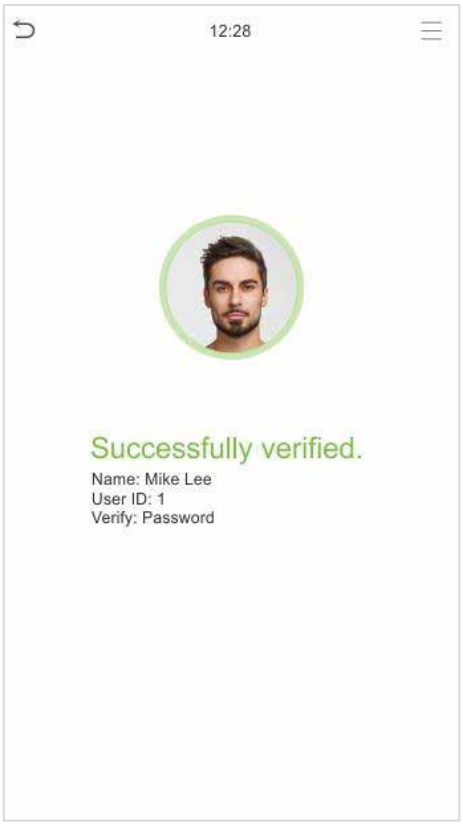
Tap the button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press **OK**.

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

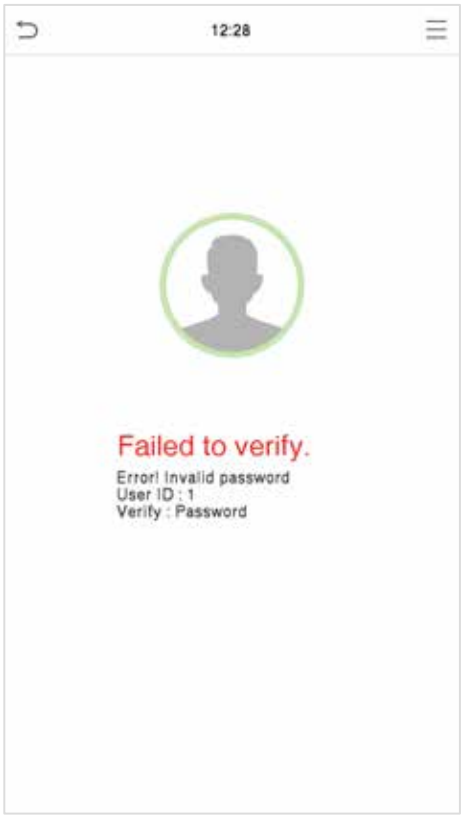
Input the password and press **OK**.

Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful:

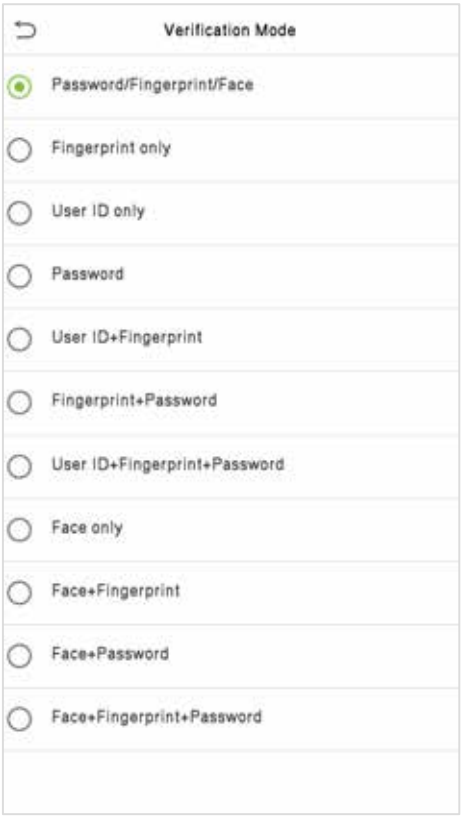


Verification is failed:



1.6.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods.



Procedure to Set for Combined Verification Mode

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

But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays "**Verification Failed**".

Note:

- "**/**" means "**or**", and "**+**" means "**and**".
- You must register the required verification information before using the combination verification mode, otherwise the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

2 Main Menu

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

Function Description

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete 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 parameters related to the system, including Date & Time, Access Logs Setting, Face, card, password and Fingerprint parameters, Video Intercom parameters, security settings and resetting to factory settings.
Personalize	To customize settings of 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 schedule, Holiday Settings, Combine verification, Anti-passback Setup, and Duress Option Settings.
Attendance Search	To query the specified Event logs, check Attendance Photos and Blocklist attendance photos.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Fingerprint sensor, Camera, 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.

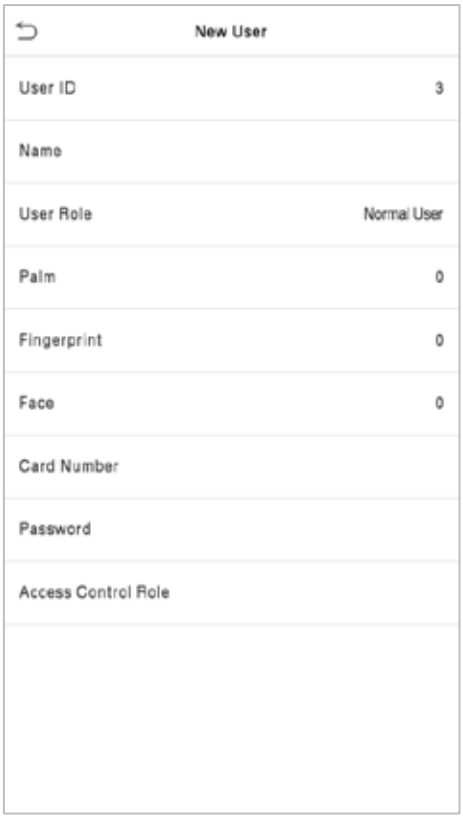
3 User Management

3.1 User Registration

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

3.1.1 Register a User ID and Name

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



Note:

- A name can take up to 17 characters.
- The user ID may contain 1-9 digits by default.
- You can modify your ID during the initial registration but not after registration.
- If a message "**Duplicated!**" pops up, you must choose another ID as the entered User ID already exists.

3.1.2 Setting the User Role

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

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

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

3.1.3 Register Fingerprint

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

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

3.1.4 Register Face

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

3.1.5 Register Card Number

- **Enroll 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:

3.1.6 Register Password

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

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

3.1.7 Register User Photo

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

Click **User Photo**, click the camera icon to take a photo. The system will return to the **New User** interface after taking a photo.

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

3.1.8 Access Control Role

User access control sets the door unlocking rights of each person, including the group and the time period that the user belongs to.

Click **Access Control Role** > **Access Group**, 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.

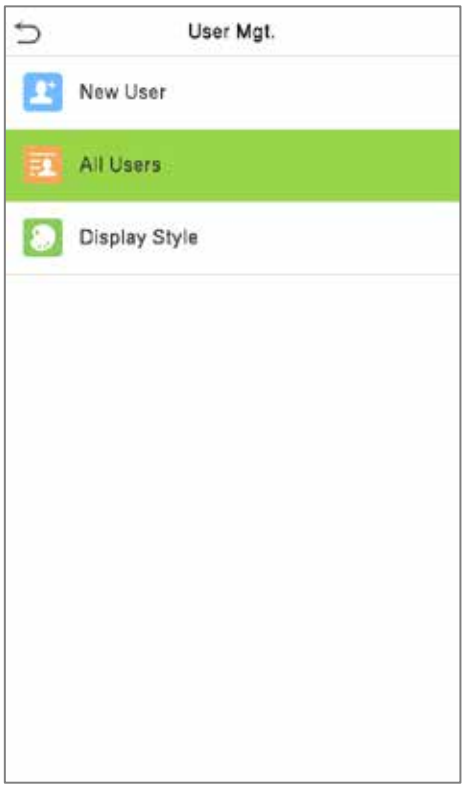
Click **Time Period**, select the time period to use.


Access Control
Access Group
Disabled
Time Period
Duress Fingerprint
1

3.2 Search User

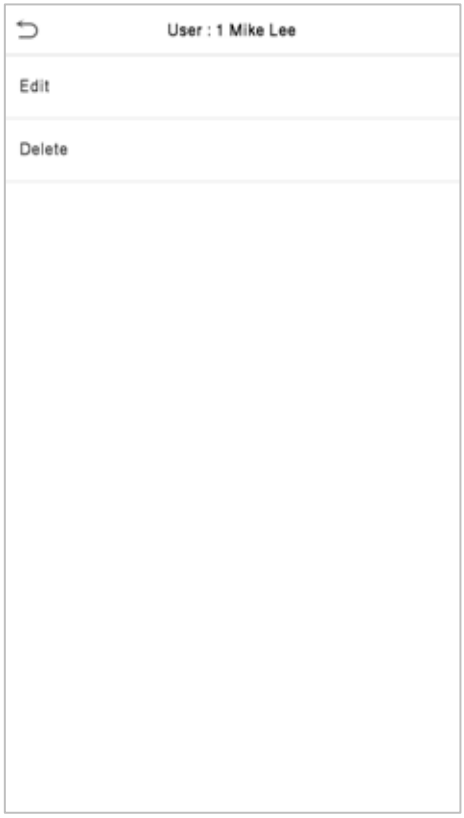
On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search a User.

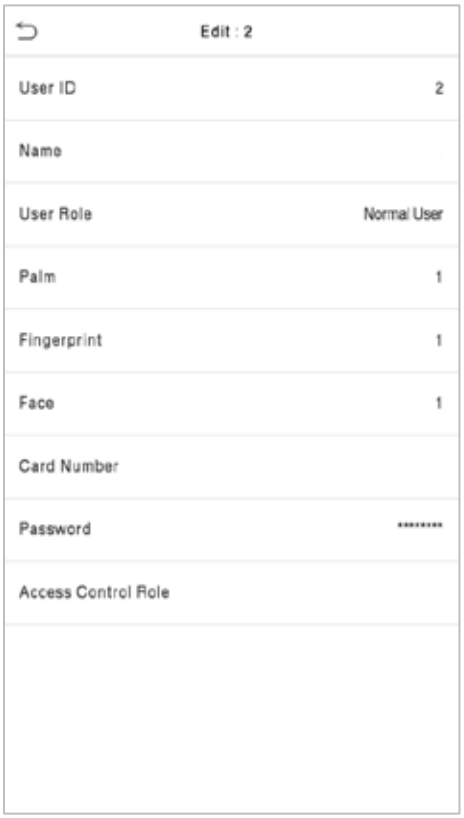
On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.



3.3 Edit User

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





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

3.4 Deleting User

On the **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or 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: Deletes all the user information (deletes the selected User as a whole) from the Device.

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

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

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

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

3.5 Display Style

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

Different display styles are shown as below:

Multiple Line:

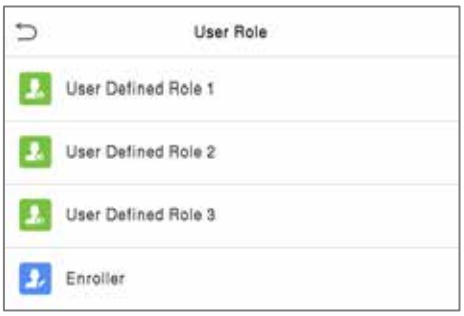
Mixed Line:

4 User Role

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

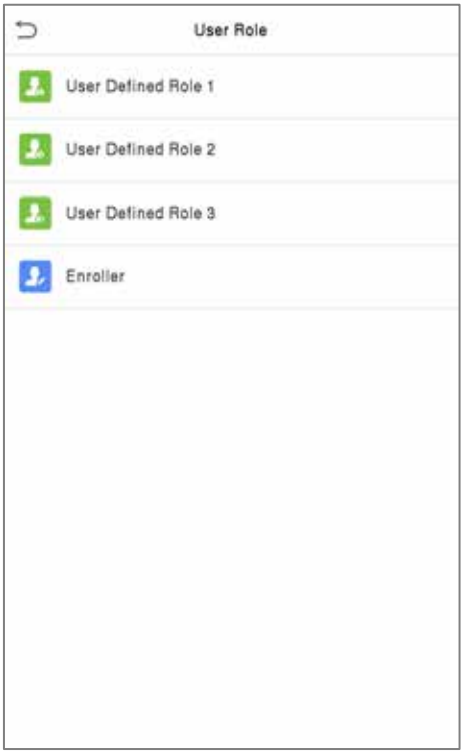
You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

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



On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user-defined role.

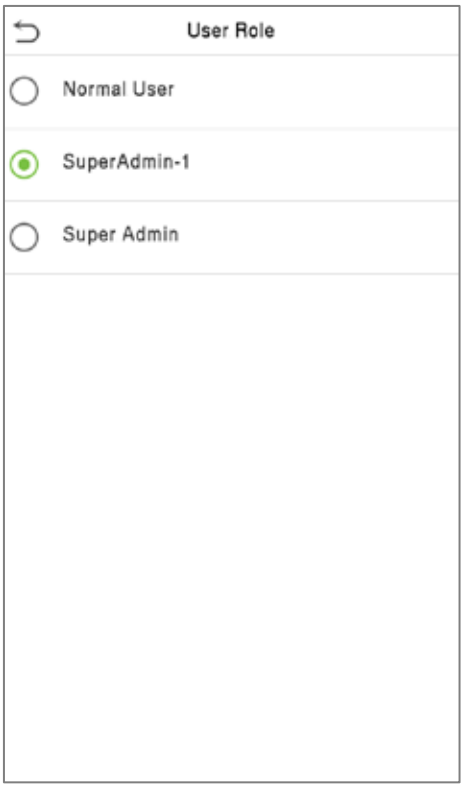
Tap on **Name** and enter the custom name of the role.



Then, tap on **Define User 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.

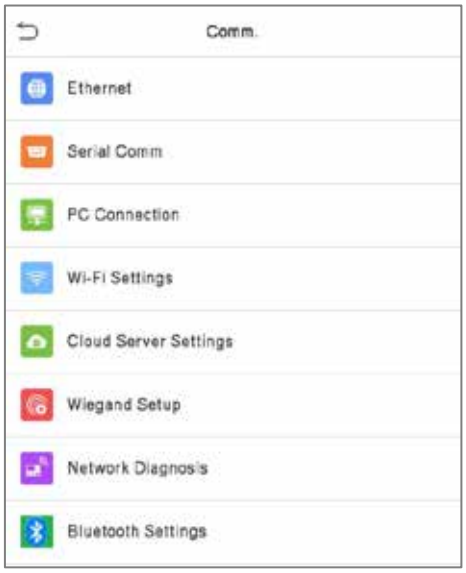
First, tap on the required **Main Menu** functions, and then select its required sub-menus from the list which the user can access.



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 Ethernet PC connection, Cloud Server setting, 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 connect to the same network segment.

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

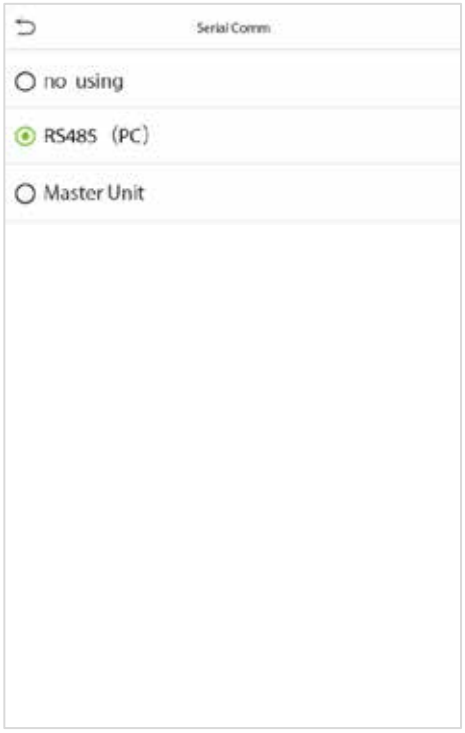
Function Description

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 dynamically allocates 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.



Function Description

Function Name	Descriptions
Serial Port	**Disable:** 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 fingerprint & 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

Comm Key facilitates to improve the security of data by setting the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

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

Function Description

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

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

Wi-Fi is enabled in the Device by default. Toggle on button to enable or disable Wi-Fi.

Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.

Tap on the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.

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

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

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

- **Add Wi-Fi Network Manually**

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

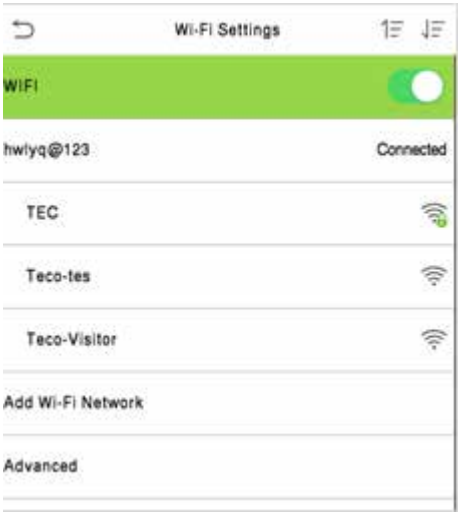
Tap on **Add WIFI Network** to add the Wi-Fi manually.

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

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

- **Advanced Setting**

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

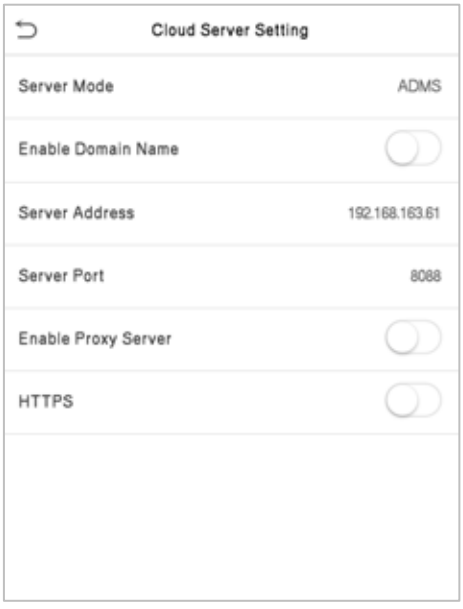


Function Description

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 Wi-Fi network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the Wi-Fi network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. Can be modified according to the network availability.

5.5 Cloud Server Setting

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



Function Description

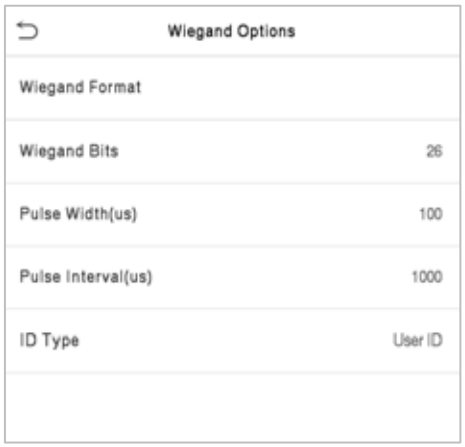
Function Name		Description
Enable Domain Name	**Server Address**	Once this mode is turned **ON**, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.
HTTPS		To increase the security of browser 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.

5.6 Wiegand Setup

It is used to set the Wiegand input and output parameters.

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

5.6.1 Wiegand Input



Function Description

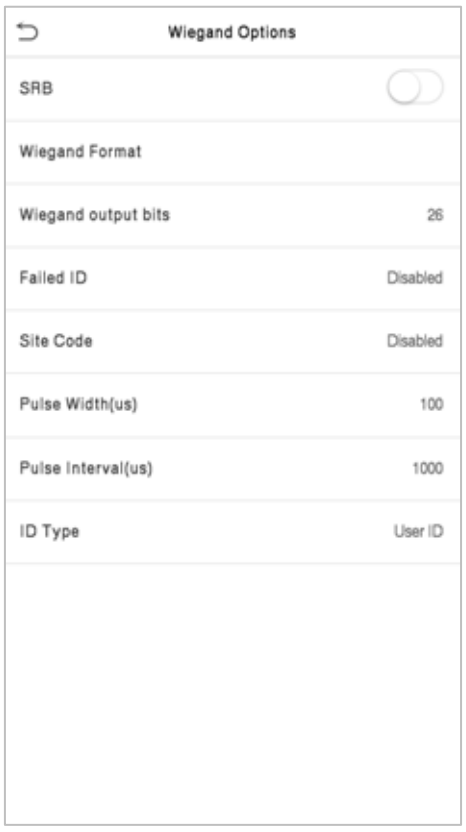
Function Name	Descriptions
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width (us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to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

Various Common Wiegand Format Description

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO It 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	ESSSSSSSSCCCCCCCCCCCCCCCO It 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 It 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 It 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	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME It 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	EFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO It 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	OMMMMSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE It 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	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO It 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	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It 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



Function Description

Function Name	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from opening due to device removal.
Wiegand Format	Its value can be 26 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 fails, 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 on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes in 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

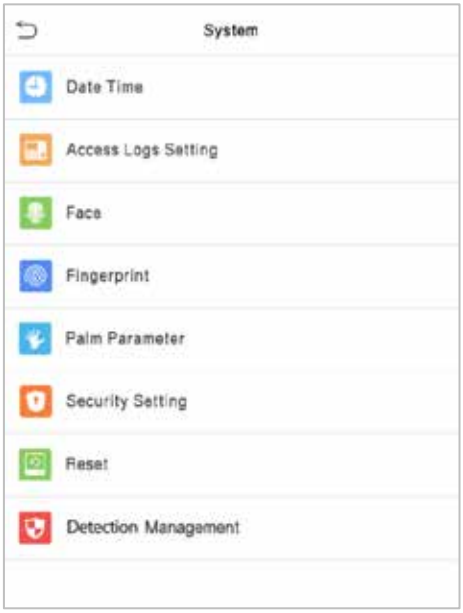
To set the network diagnosis parameters.

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

6 System Settings

It helps to set related system parameters to optimize the accessibility of the device.

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

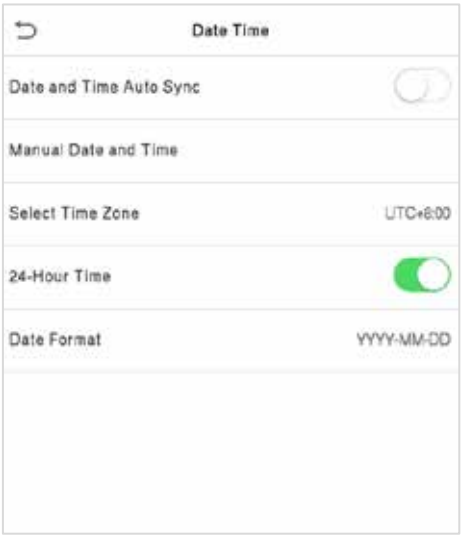


6.1 Date and Time

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

The product supports the NTP synchronization time system by default. This function takes effect after **Date and Time Auto Sync** is enabled and the corresponding NTP server address link is set.

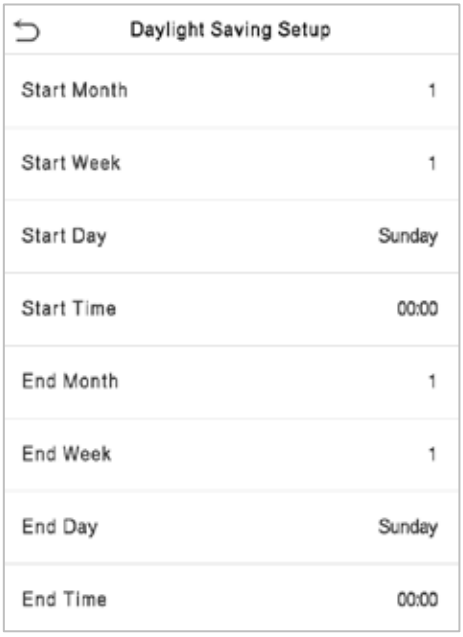
If users need to set date and time manually, disable **Date and Time Auto Sync** first, and then tap **Manual Time Setting** to set date and time and tap Confirm to save.



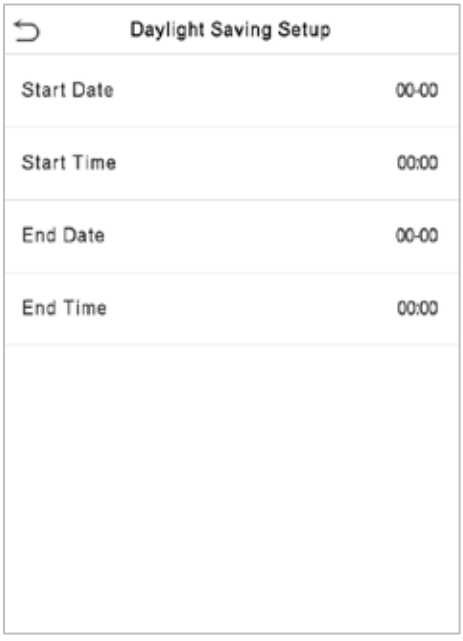
Tap **Select Time Zone** to select a time zone then tap the return button to save and exit.

Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format i.e., the way date should be displayed on the device.

★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.



Week Mode



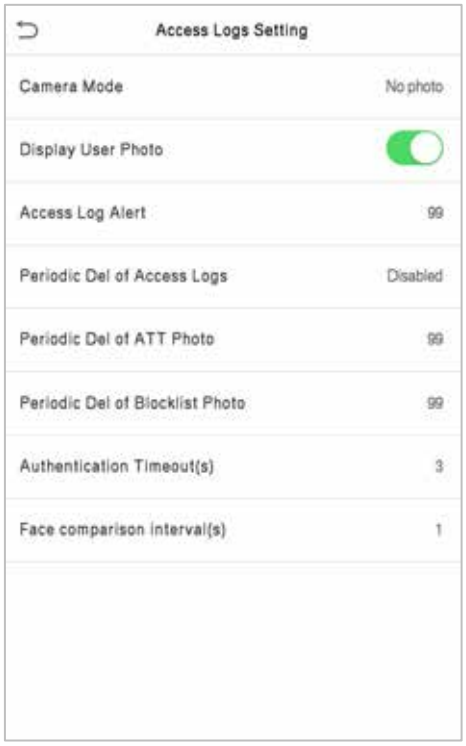
Date Mode

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

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

6.2 Access Logs Setting

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



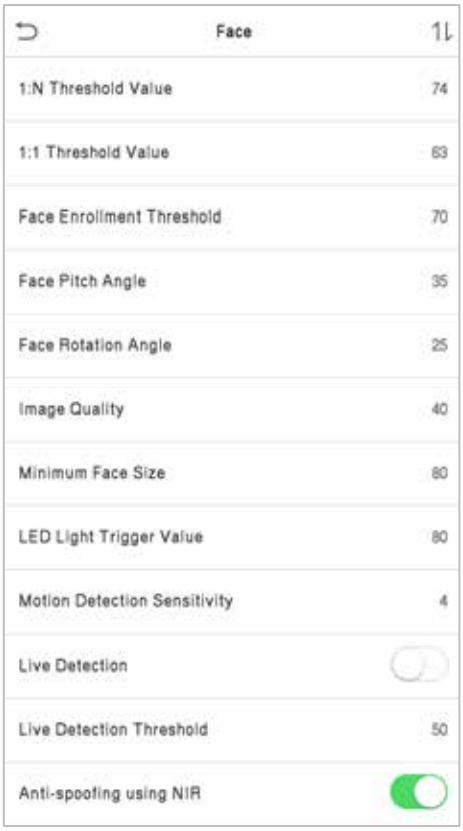
Function Description

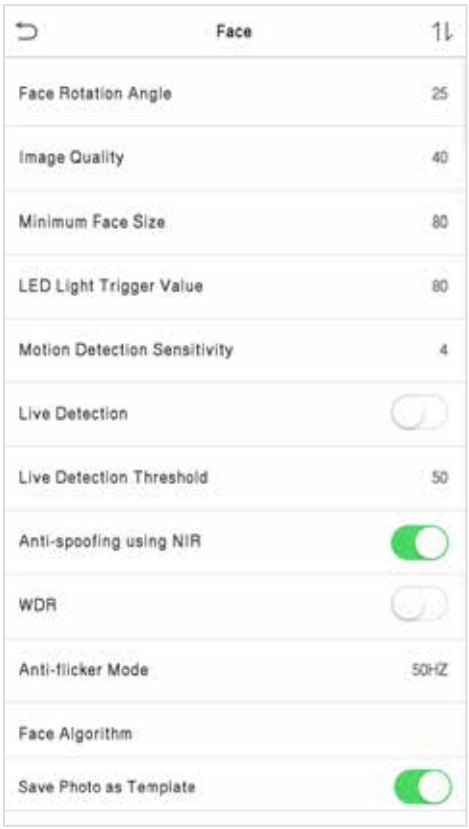
Function Name	Description
Camera Mode	This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but not saved during verification. **Take photo and save:** All the photos taken during verification is saved. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	This function is disabled by default. When enabled, a security prompt will pop-up.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of ATT	When attendance photos reach its maximum capacity, the device

Photo	automatically deletes a set of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout (s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Face Comparison Interval (s)	The amount of time required to compare facial templates. Valid value: 0~9 seconds.

6.3 Face Parameters

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





Function Description

Function Name	Description
1:N Match 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 65 to 120. 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 75.
1:1 Match 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 55 to 120. 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 63.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.
Face Pitch Angle	It is the pitch angle tolerance of a face for facial template registration and comparison. If a face's pitch angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
Face Rotation Angle	It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Minimum Face Size	It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Trigger Threshold	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Motion Detection Sensitivity	It sets the value for the amount of change in a camera's field of view known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface activates with much ease, and the motion detection is frequently triggered.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-counterfeiting	Using near-infrared spectra imaging to identify and prevent fake photos and

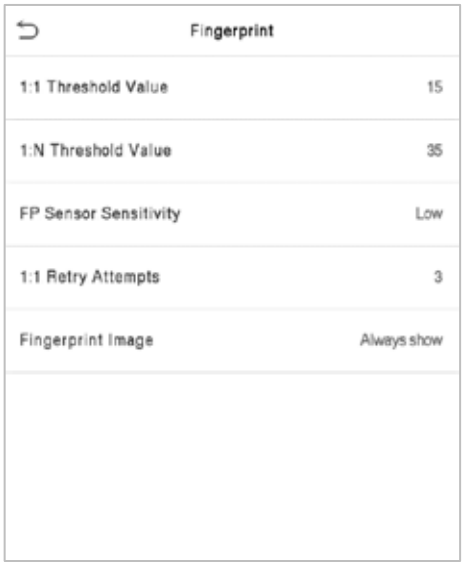
with NIR	videos attack.
WDR	Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	It has facial algorithm related information and pause facial template update.
Save Photo as Template	This function is enabled by default, and the menu interface supports enabling or disabling this function, and there is a security prompt when switching. When this function is disabled, it will indicate that there is a risk reminder: "**Face re-registration is required after an algorithm upgrade.**"

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

- **Process to modify the Face Recognition Accuracy**
- On the **System** interface, tap on **Face** and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > Test Face** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.
- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

6.4 Fingerprint Parameters

Click **Fingerprint** on the System interface.



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 Security Settings

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

Function Description

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

Mode	mode. The verification result will not show the verification mode after you disable it.

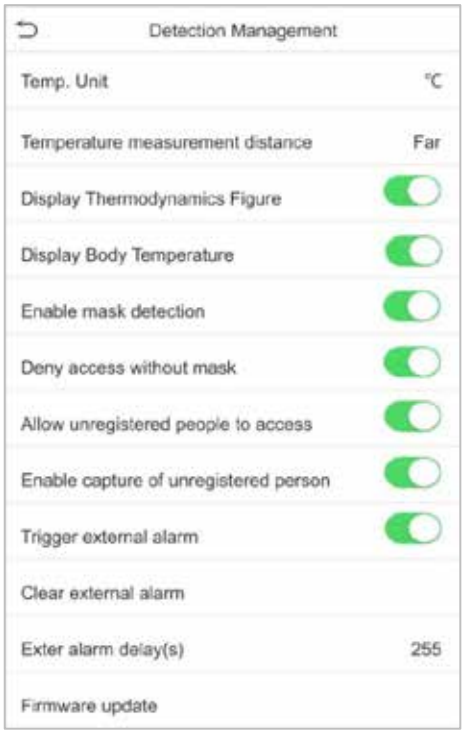
6.6 Factory Reset

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.

6.7 Detection Management★

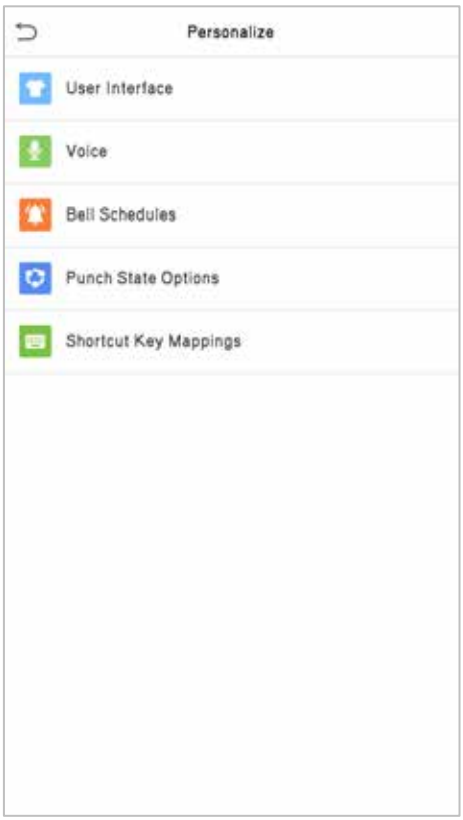
Click **Detection Management** on the System interface.



Function Name	Description
Allow Unregistered People to Access	To enable or disable the unregistered people to access function. When enabled, as long as the person who passes the detection, the device allows the personnel to enter without registration.
Enable Capture of Unregistered Person	To enable or disable the capture of unregistered person function. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow Unregistered People to Access**.
Trigger External Alarm★	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.
Clear External Alarm ★	It clears the triggered alarm records of the device.
External Alarm Delay(s)★	The delay (s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.
Firmware Update★	Choose whether to update the thermal imaging temperature detection module software version.

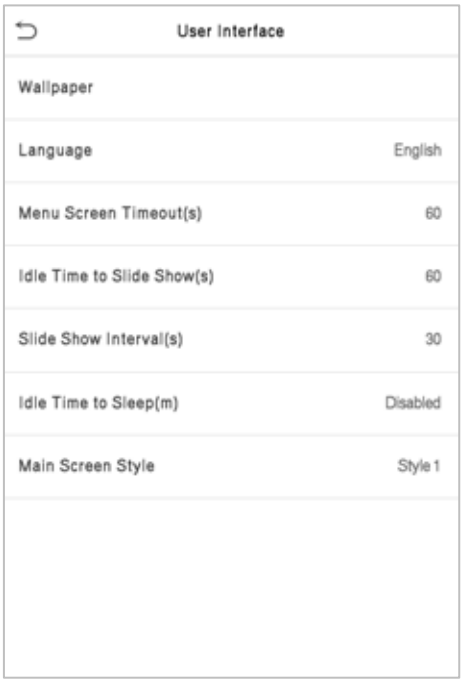
7 Personalize Settings

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



7.1 Interface Settings

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

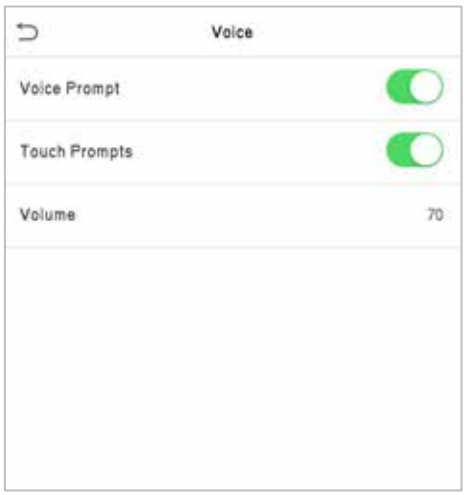


Function Description

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

7.2 Voice Settings

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



Function Description

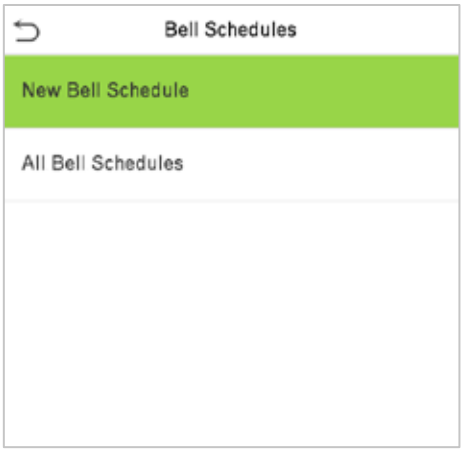
Function Name	Description
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

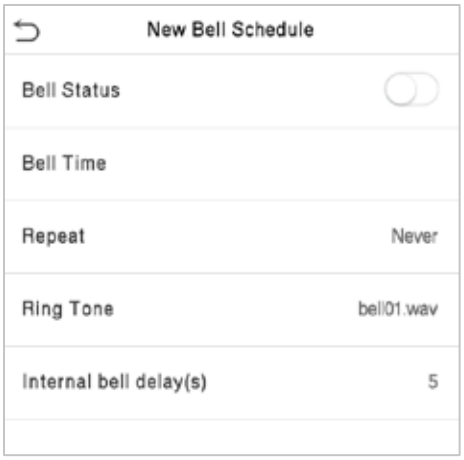
7.3 Bell Schedules

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

- **New Bell Schedule**

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





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 automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
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**

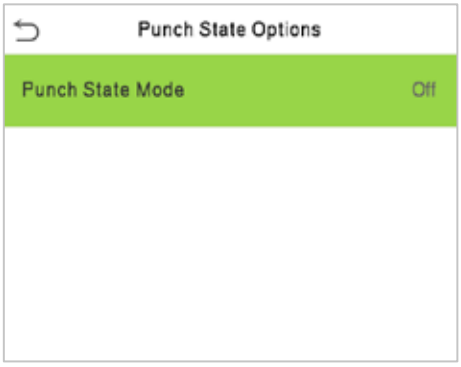
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

- **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.



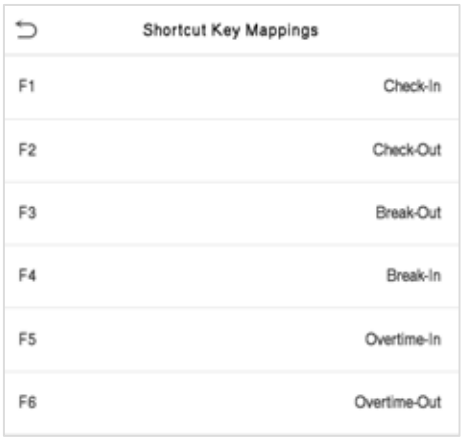
Function Description

Function Name	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** It disables the punch state function. And the punch state key set under the **Shortcut Key Mappings** menu becomes 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 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 an alternative that is the manual attendance status. After the timeout, the manual switching punch state key will become an 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 manually switched again. **Fixed Mode:** Only the manually fixed punch state key is shown. Users cannot change the status by pressing any other keys.
Punch State Timeout (s)	It is the amount of time for which the punch state is displayed. The value ranges from 5~999 seconds.
Punch State Required	To choose whether an attendance state needs to be selected during verification.

7.5 Shortcut Keys Mappings

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

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



- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** ("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 done as shown in the image below.

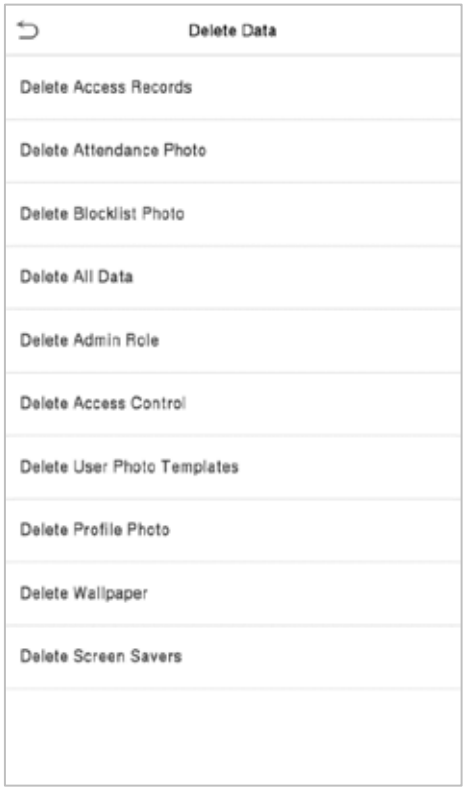
- If the Shortcut key is set as a punch state key (such as check-in, check-out, etc.), then it is required to set the punch state value (valid value 0~250), name, and switch time.

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.

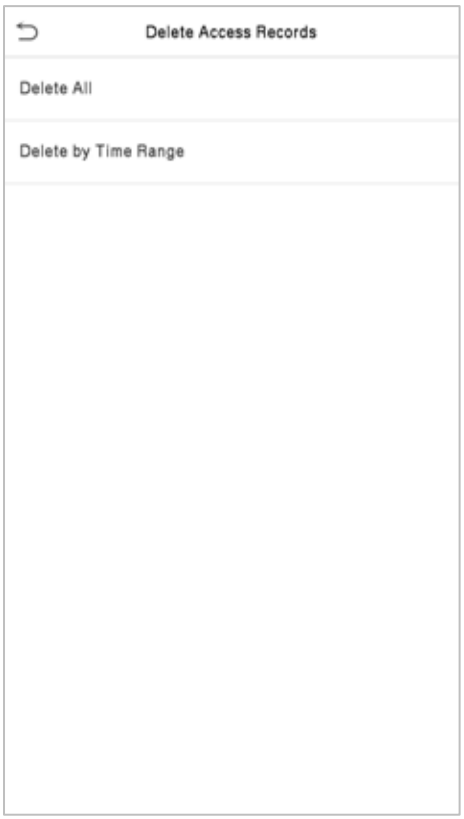


Function Description

Function Name	Description
Delete Access Records	To delete attendance data/access records 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.

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.

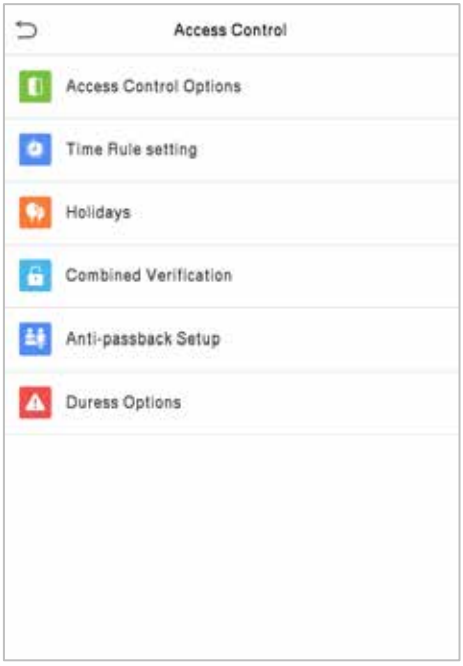


Select Delete by Time Range

Set the time range and click **OK**

9 Access Control

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

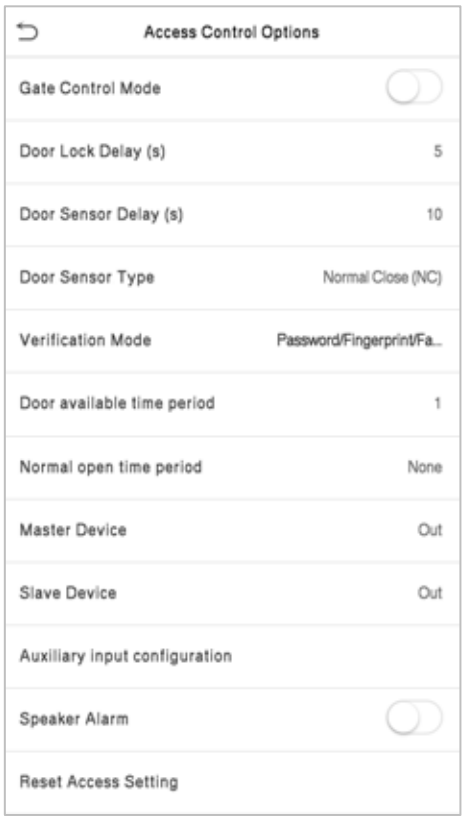


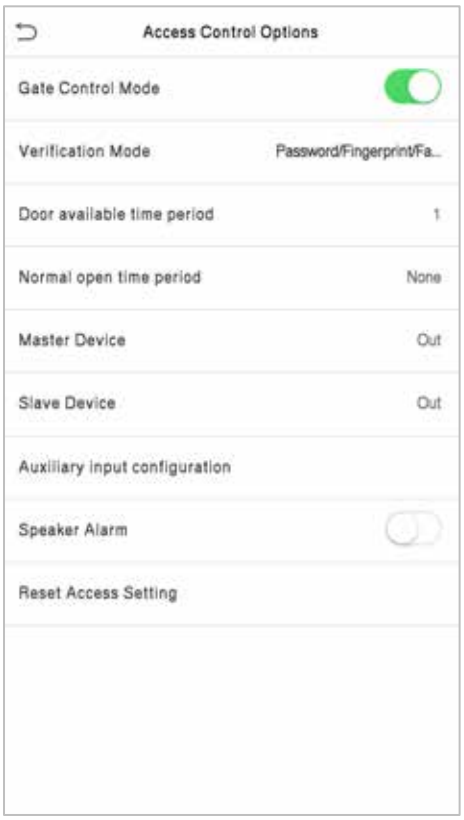
To gain access, the registered user must meet the following conditions:

- The relevant door's current unlock time should be within any valid time zone of the user's 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 is 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.





Function Description

Function Name	Description
Gate Control Mode	It toggles between **ON** or **OFF** switch to get into gate control mode or not. When set to **ON**, the interface removes the 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 seconds represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open,** and **Normal Closed**. **None:** It means the door sensor is not in use. **Normally Open:** It means the door is always left open when electric power is on. **Normally Closed:** It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Fingerprint/Face, Fingerprint only, User ID only, Password, User ID + Fingerprint, Fingerprint + Password, User ID + Fingerprint + Password, Face only, Face + Fingerprint,

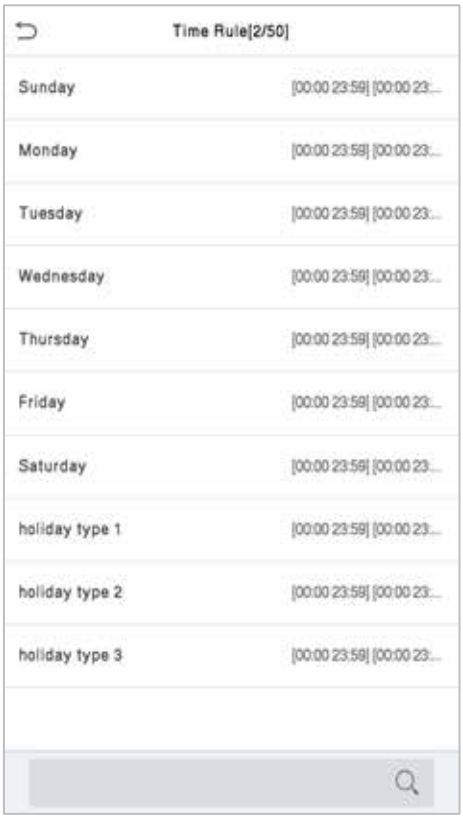
	Face + Password, Face + Fingerprint + Password.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Master Device	While configuring the master and slave devices, you may set the state of the master as **Out** or **In**. **Out**: A record of verification on the master device is a check-out record. **In**: A record of verification on the master 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.
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.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	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 Schedule

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 is **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).



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**.

Note:

- The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).
- It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).
- The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).
- The default Time Zone 1 indicates that the door is open all day long.

9.3 Holidays

Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies 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.

- **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 the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

9.4 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen 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.

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:

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates 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.
- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates 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.

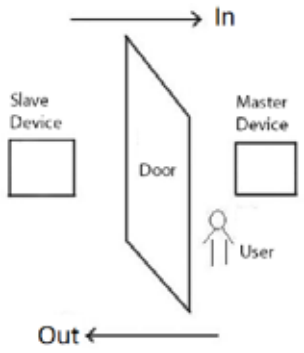
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

9.5 Anti-passback Setup

A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

This function requires two devices to work together:

One device is installed on the indoor side of the door (master device), and the other one is installed on the outdoor side of the door (the 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.

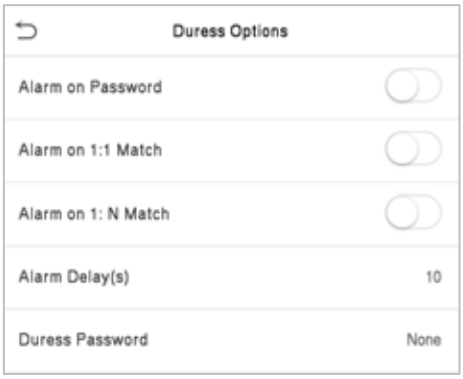
Function Description

Function Name	Description
Anti-passback Direction	**No Anti-Passback:** The 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:** The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely. **In Anti-Passback:** The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely. **In/Out Anti-Passback:** In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.

9.6 Duress Options Settings

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

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



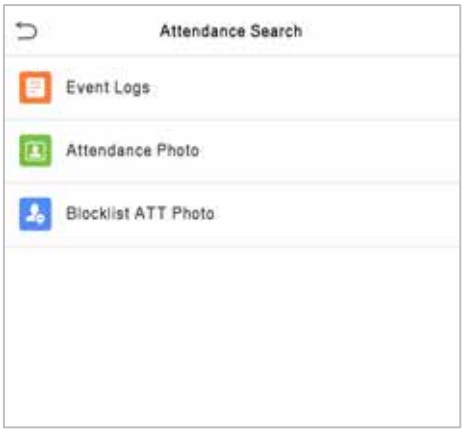
Function Description

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 the 1:1 verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses the 1:N verification method, 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 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

Select **Attendance Search** on the **Main Menu** interface to search for the required event Logs.

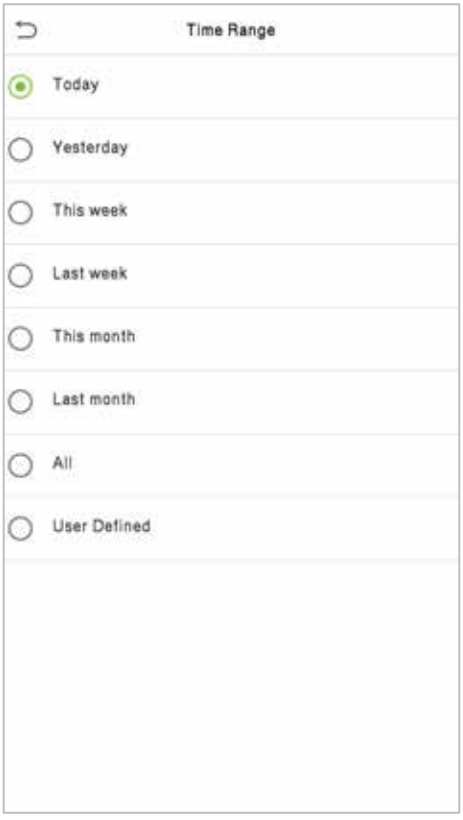


The process of searching for attendance and blocklist photos is similar to that of searching for event logs. The following is an example of searching for event logs.

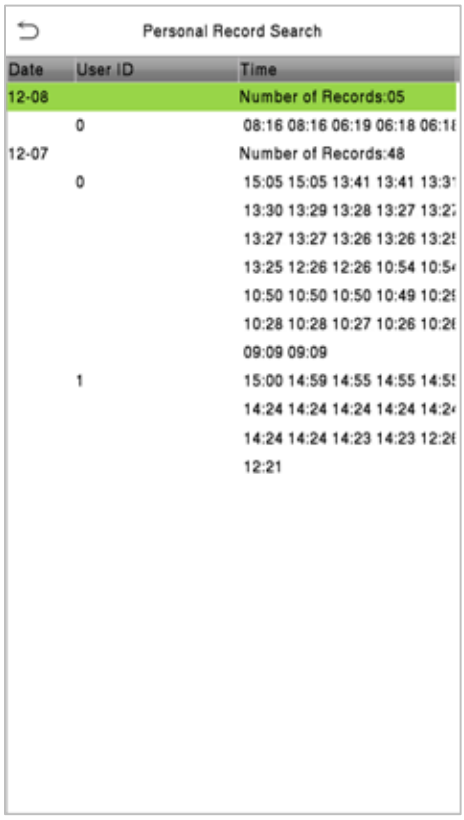
On the **Attendance Search** interface, tap **Event Logs** to search for the required record.

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

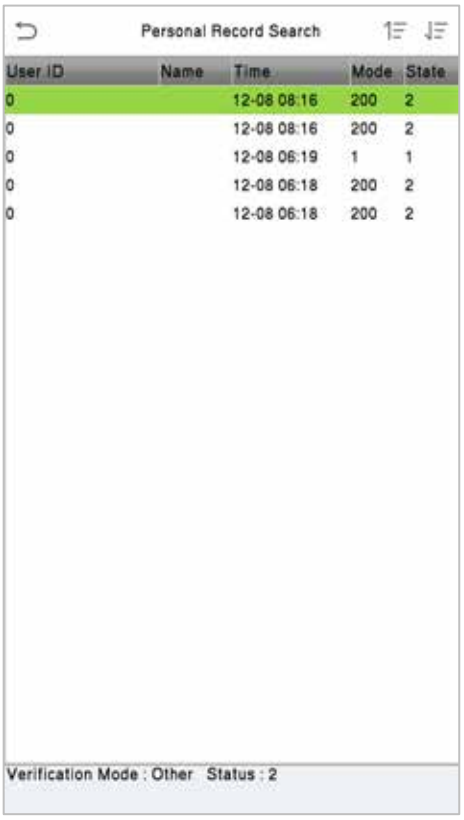
2. Select the time range in which the records need to be searched.



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

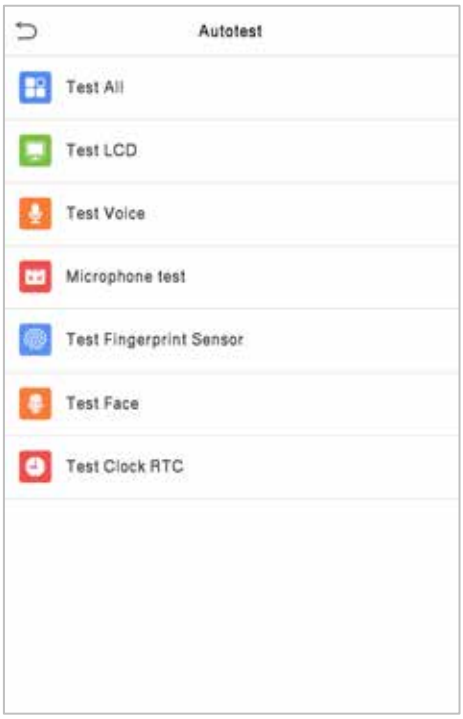


4. The below figure shows the details of the selected record.



11 Autotest

Select **Main Menu**, tap **Autotest.** It enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Camera, and Real-Time Clock (RTC).

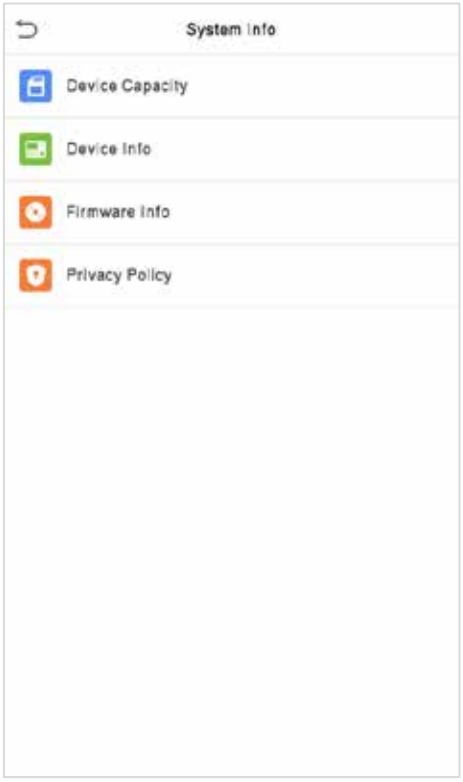


Function Description

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	To test if the microphone is working properly by speaking into the microphone.
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 pictures 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. Touch the screen to start counting and press it again to stop counting.

12 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, and face storage, administrators, access records, attendance and blocklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm, 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 on the face.
2) Do not place the device towards outdoor light sources like door or window or other harsh light sources.
3) Dark-color apparels other than the background color are recommended for registration.
4) Expose your face and forehead properly and do not cover your face and eyebrows with your hair.
5) It is recommended to show a normal facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).
6) Two images are required for persons with eyeglasses, one image with eyeglasses and one other without them.
7) Do not wear accessories like scarf or mask that may cover your mouth or chin.
8) Please face right towards the capturing device and locate your face in the image capturing area as shown in the image below.
9) Do not include more than one face in the capturing area.
10) A distance of 50cm to 80cm is recommended for capturing the image. (the distance is adjustable, subject to body height).

Requirements for Visible Light Digital Face Template Data

The digital photo should be straight-edged, coloured, 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 photos captured.

- **Eye Distance**

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

- **Facial Expression**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

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

- **Accessories**

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

- **Face**

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

- **Image Format**

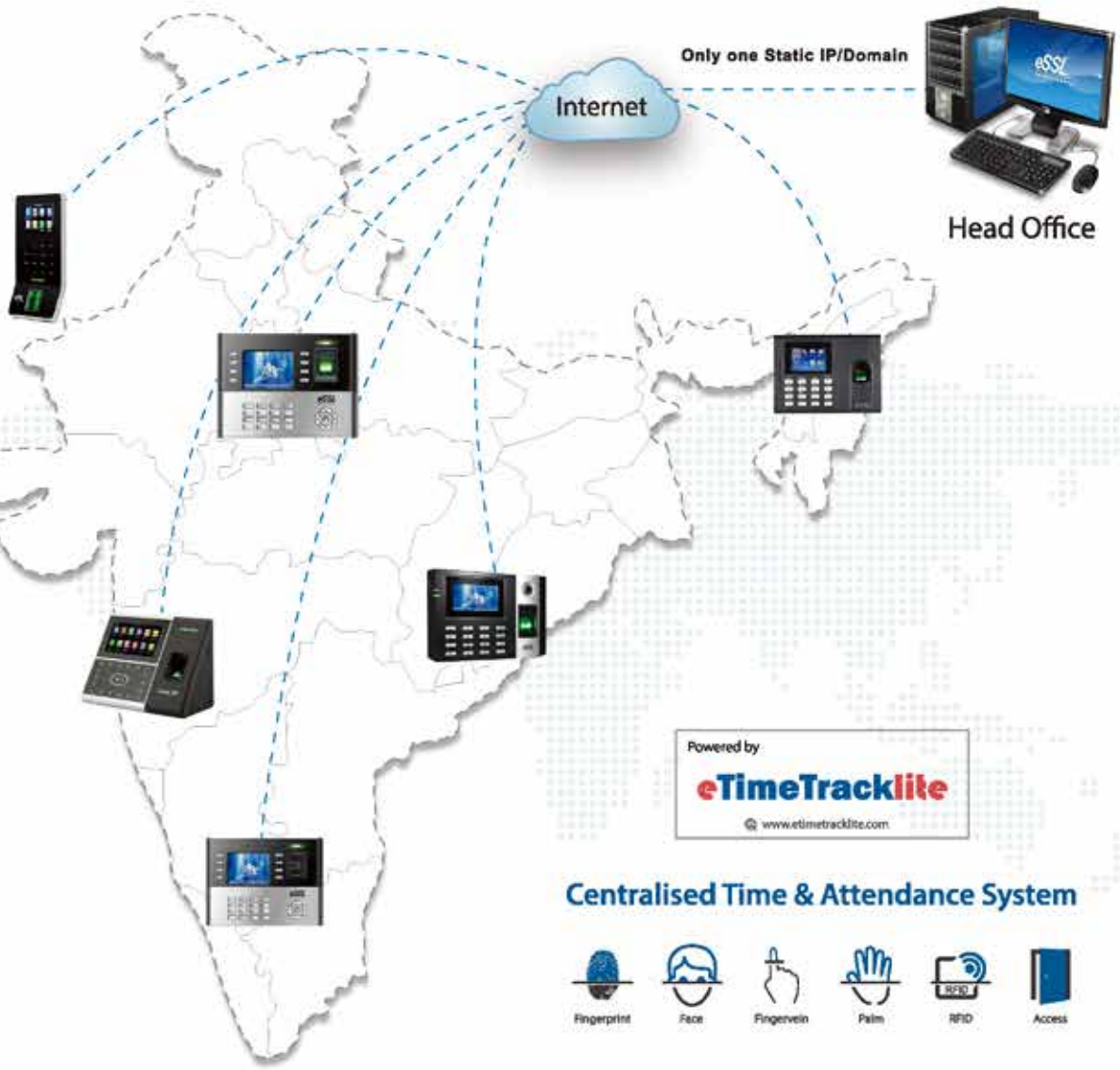
Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

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