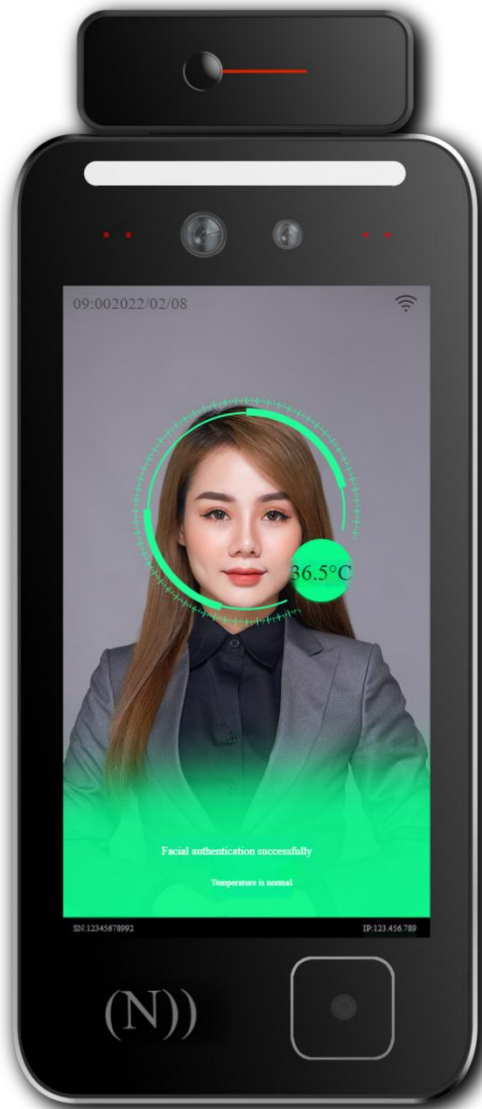


FCV4914

Product User Manual



Documentation describe

This document mainly consists of the following parts.

Chapters 1-4: Product Overview, including product features, appearance, parameters, interface leads, and installation methods.

Chapters 5 and 6: Introduce the ways to log in to the device backend and several working modes of the device, facilitating users to fully understand the device authentication process.

Chapter 7: Due to the relatively large number of backend settings, this chapter lists several common scenario settings to facilitate users in quickly setting up the device after receiving it.

Chapter 8: Detailed introduction to the configuration options and operation instructions of the facial device backend.

Users can quickly learn how to use the device according to the instructions.

目录

1. FOREWORD	5
1.1. Product Introduction	5
1.2. Product Characteristics	5
2. Product Appearance	7
2.1. Non temperature measurement version	7
2.2. Dimension	8
2.3. Schematic diagram of reading area	9
2.4. Installation Method	10
2.5. Interface Definition	12
Port Description	12
3. Scene application and wiring	14
3.1. Independent Use	14
3.2. Cooperate with the security module	15
4. Technical Parameters	16
5. Equipment usage instructions	18
5.1. Equipment Setting Process Description	18
5.2. Equipment networking configuration	18
5.3. Login to the facial device backend	19
6. Equipment authentication mode description	22
6.1. Setting method	22
6.2. Transparent transmission mode	23
6.3. Protocol Mode	23
6.4. Development Mode	24
6.5. Local Whitelist Mode	24
7. Quick Settings	25
7.1. Scenario 1	25
Scenario description	25
Set up process	25
7.2. Scenario 2	26
Scenario description	26
Set up process	27
7.3. Scenario Three	28
Scenario description	28
Set up process	28
8. Background Description	29
8.1. Basic Settings	29
Basic configuration	29
Configuration related to traffic records	30
Voice and output related configurations	30
Alarm related settings	32
Equipment anti dismantling setting	33
Related settings for fill lights	33
Facial related configurations	34

Card swiping related configurations	35
Scan code related configurations	36
Channel related configurations	37
Authentication mode	38
network configuration	39
MQTT related configurations	40
Camera calibration	40
Set device time	40
Disable Enable	40
Password modification	40
Device restart	41
8.2. Whitelist Setting	42
8.3. Firmware Information	43
Firmware update	43
Reset device	43
8.4. Personnel Configuration	44
Add personnel	44
8.5. Traffic Records	44
9. matters needing attention	45
Facial registration photo requirements	45
Facial recognition registration requirements	45

1. FOREWORD

Thank you for using the FCV4914 all-in-one device for facial recognition, temperature measurement, QR code scanning, and card swiping. Carefully reading this document can help you understand the functions, features, and quickly grasp the usage and installation methods of this device.

1.1. Product Introduction

FCV4914 facial intelligent terminal integrates facial recognition, IC card, QR code, cloud ID card, infrared temperature measurement, and TTS voice library functions. Supports TCP, HTTP, MQTT protocols, can work in transparent mode, protocol mode, and offline access control mode, with IP66 protection level, can adapt to epidemic prevention scenarios, face temperature measurement, mask detection, ID health information authentication, and health code authentication.

Suitable for office areas, hotels, access gates, office buildings, banks, hospitals, schools, shopping malls, shops, communities, public services, and management projects that require facial access control.

1.2. Product Characteristics

- Dynamic facial recognition, integrating QR codes and card swiping.

- 6-inch high brightness LCD screen, human voice prompts, integrated TTS voice library.

- Over 97% recognition accuracy and millisecond level recognition rate.

- The recognition distance is 0.3m-1.5m, supporting a maximum of 5000 face databases and 20000 QR codes/card whitelists.

- Personnel wearing masks, glasses, and hats can be effectively identified and support mask detection.

- Built in silent liveness detection can effectively block photo, video, and mask attacks.

- Multiple working modes: transparent transmission mode, protocol mode, whitelist mode.

- Supports TCP, MQTT, and HTTP protocols.

- Support scanning configuration and scanning registration.

- External alarm input, door magnetic status input, and exit switch input.

- RS485、Weigen outputs the facial ID number, QR code content, or card ID number.

- Built in high-precision clock chip and RTC battery, can save time when powered off.

- Electrostatic protection contact 8KV, air 8KV.

- Built in Hall switch anti disassembly detection.

Waterproof and dustproof rating: IP66.

Support logo customization, protocol customization, and OEM support.

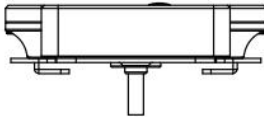
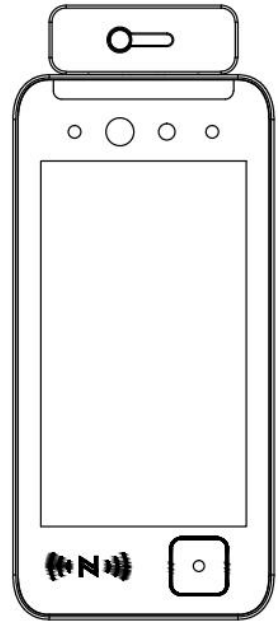
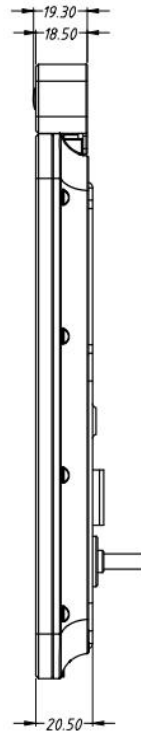
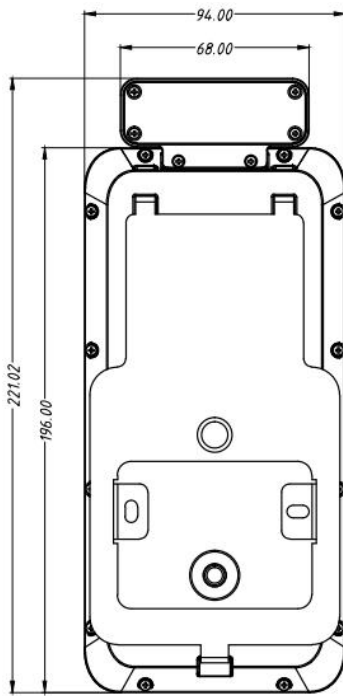
Support the installation of turnstiles, 86 boxes, flat walls, and columns.

2. Product Appearance

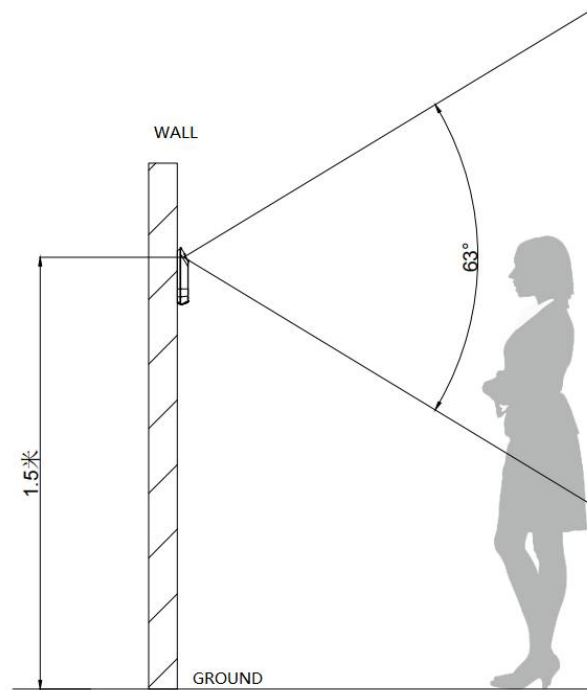
2.1. Non temperature measurement version



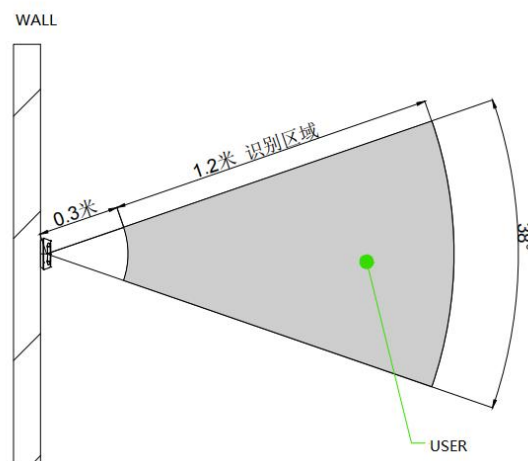
2.2. Dimension



2.3. Schematic diagram of reading area



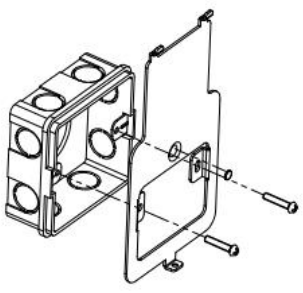
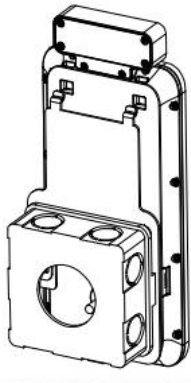
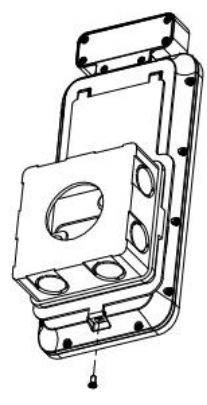
side view



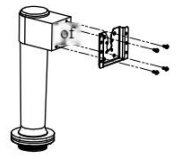
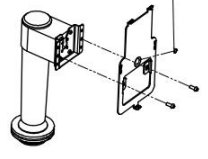
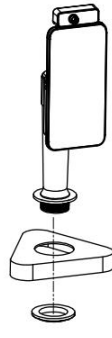
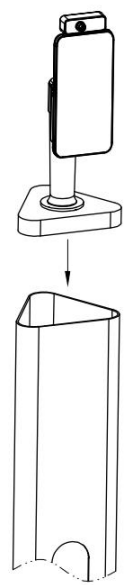
vertical view

2.4. Installation Method

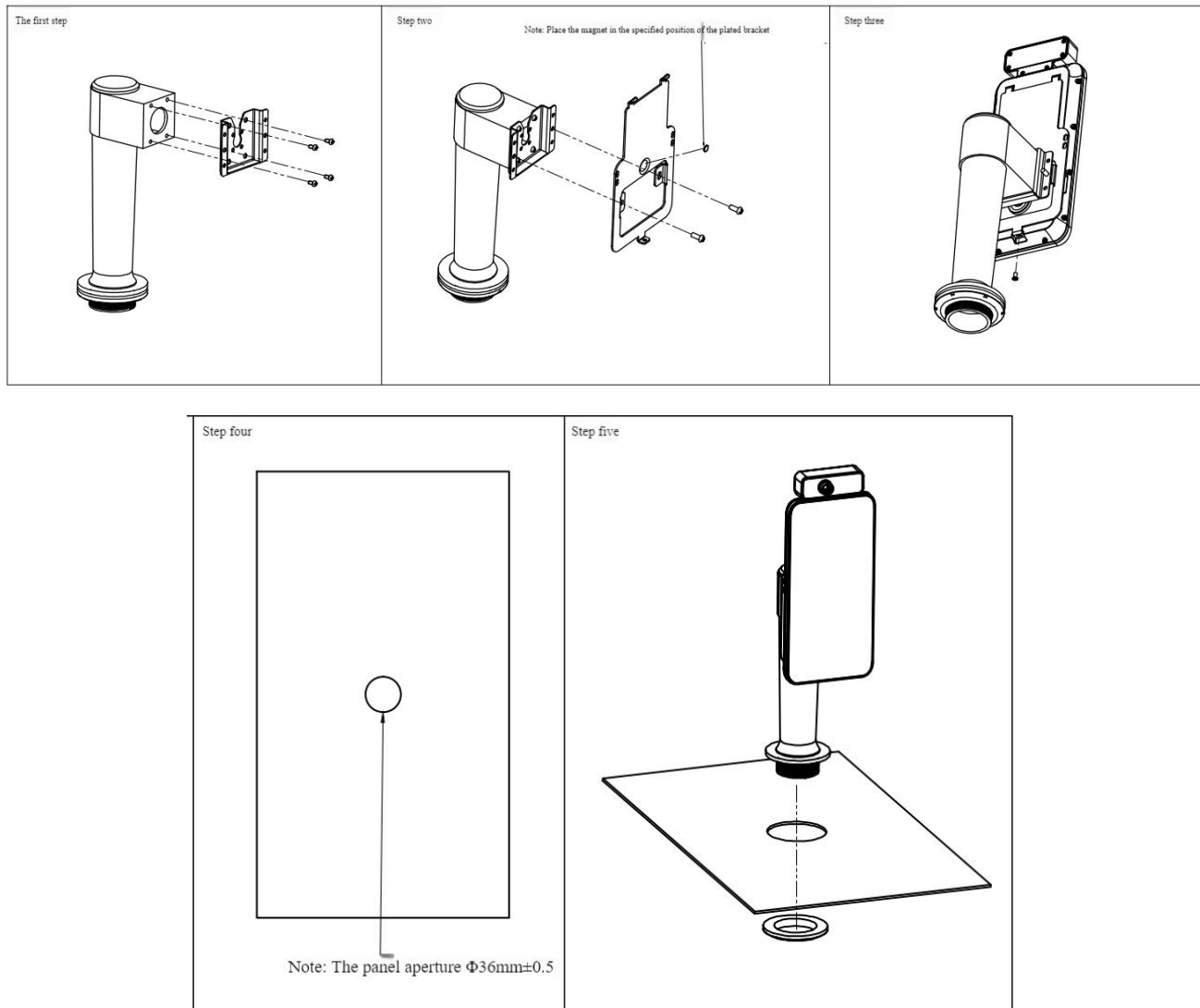
86 box installation

 Step 1: Fix the metal bracket on the 86 box or install panel and lock the screw, putting the magnet into the round hole of the bracket to the middle.	 Step 2: Install the device on a metal support. Note: first insert the card button on top of the metal bracket to the hole in the back of the device.	 Step three: lock the screw.
--	---	--

Column Installation

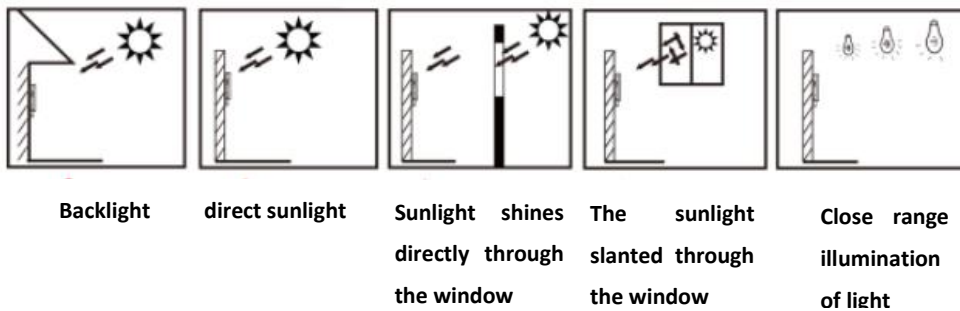
 Step one	 Step two Note: Place the magnet in the specified position of the plated bracket	 Step three	 Step four	 Step five
---	--	---	---	--

Gate Installation



Installation Precautions:

Avoid backlighting, direct sunlight, direct sunlight through windows, oblique sunlight through windows, and close range lighting.

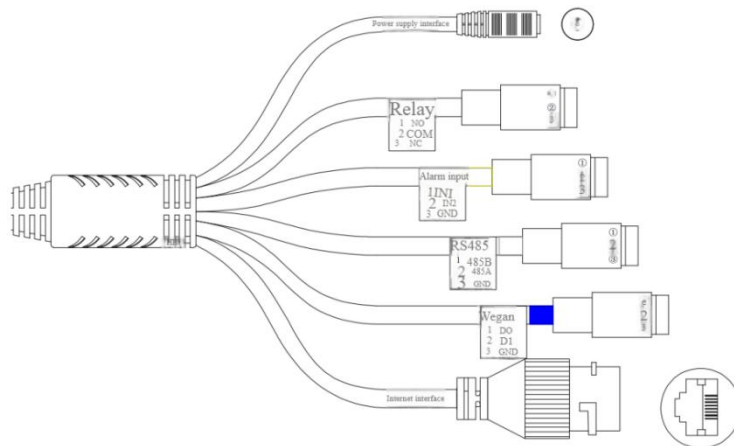


2.5. Interface Definition

Port Description

Screw terminal version

The facial device leads out six wiring terminals, and the wiring is defined according to the wiring terminal markings.



Interface Name	Pin Number	Pin Definition
power interface	DC 圆头	12V
Relay Interface	1	NO: Relay often starts
	2	COM: Relay common terminal
	3	NC: Relay normally closed end
Alarm In	1	IN1: Alarm input 1
	2	IN2: Alarm input 2
	3	GND
RS485	1	485B
	2	485A
	3	GND
Weigand	1	WG0
	2	WG1
	3	GND
Net Interface	RJ45	NET

Bare Wire Version

PIN#	Wire harness color	Pin Definition	Describe
PIN1	red	VCC	positive
PIN2	black	GND	Negative
PIN3	white	485B	-
PIN4	blue	485A	-
PIN5	brown	GND	Negative
PIN6	orange	D0	WG0
PIN7	yellow	D1	WG1
PIN8	green	IN1	Alarm input 1
PIN9	purple	IN2	Alarm input 2
PIN10	gray	NO	Relay often starts
PIN11	pink	COM	Relay common terminal
PIN12	light green	NC	Relay normally closed end

matters needing attention:

For unused pins, insulation treatment must be done!

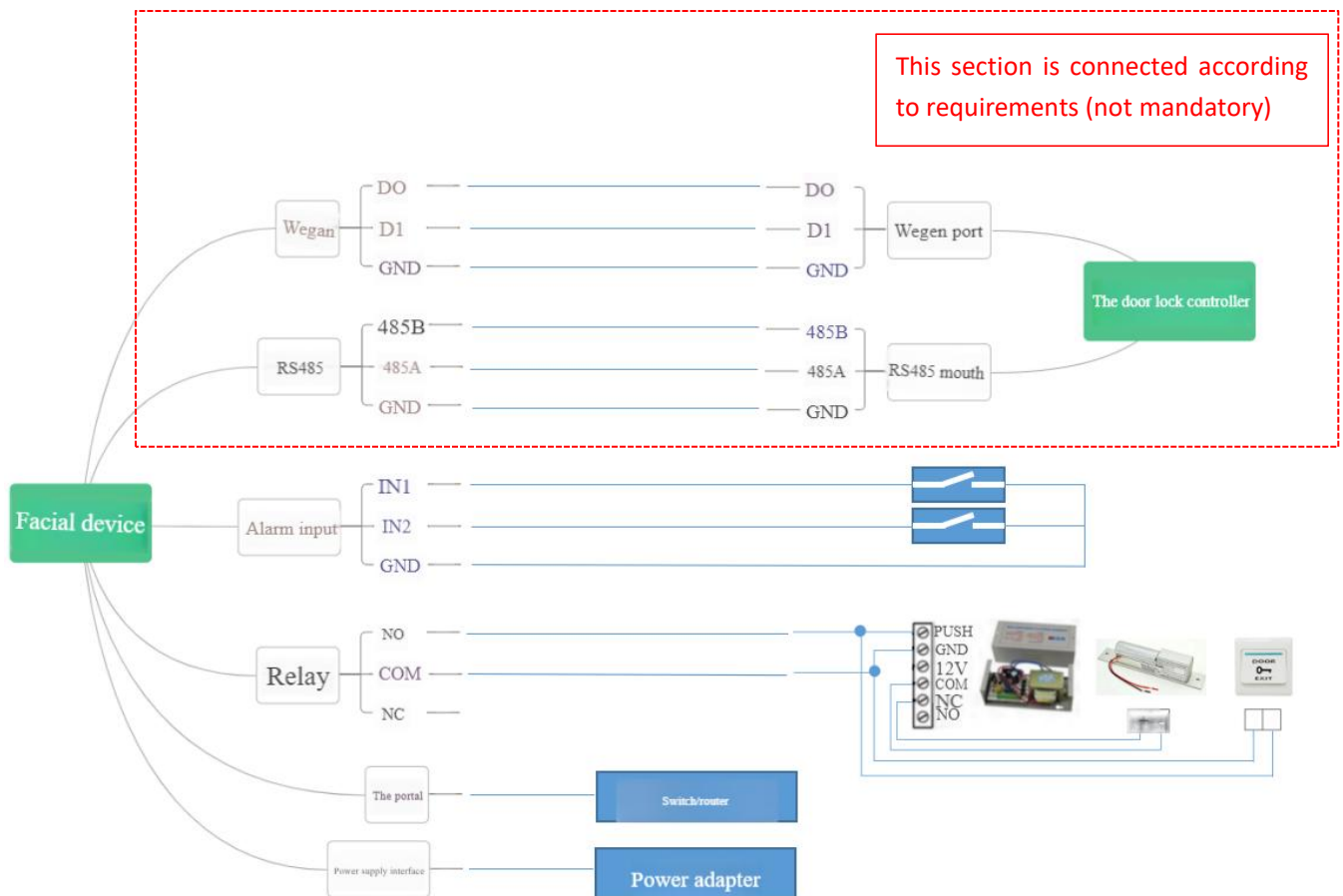
If the equipment is short circuited or damaged due to lack of insulation treatment, the user shall bear the responsibility on their own!

3. Scene application and wiring

3.1. Independent Use

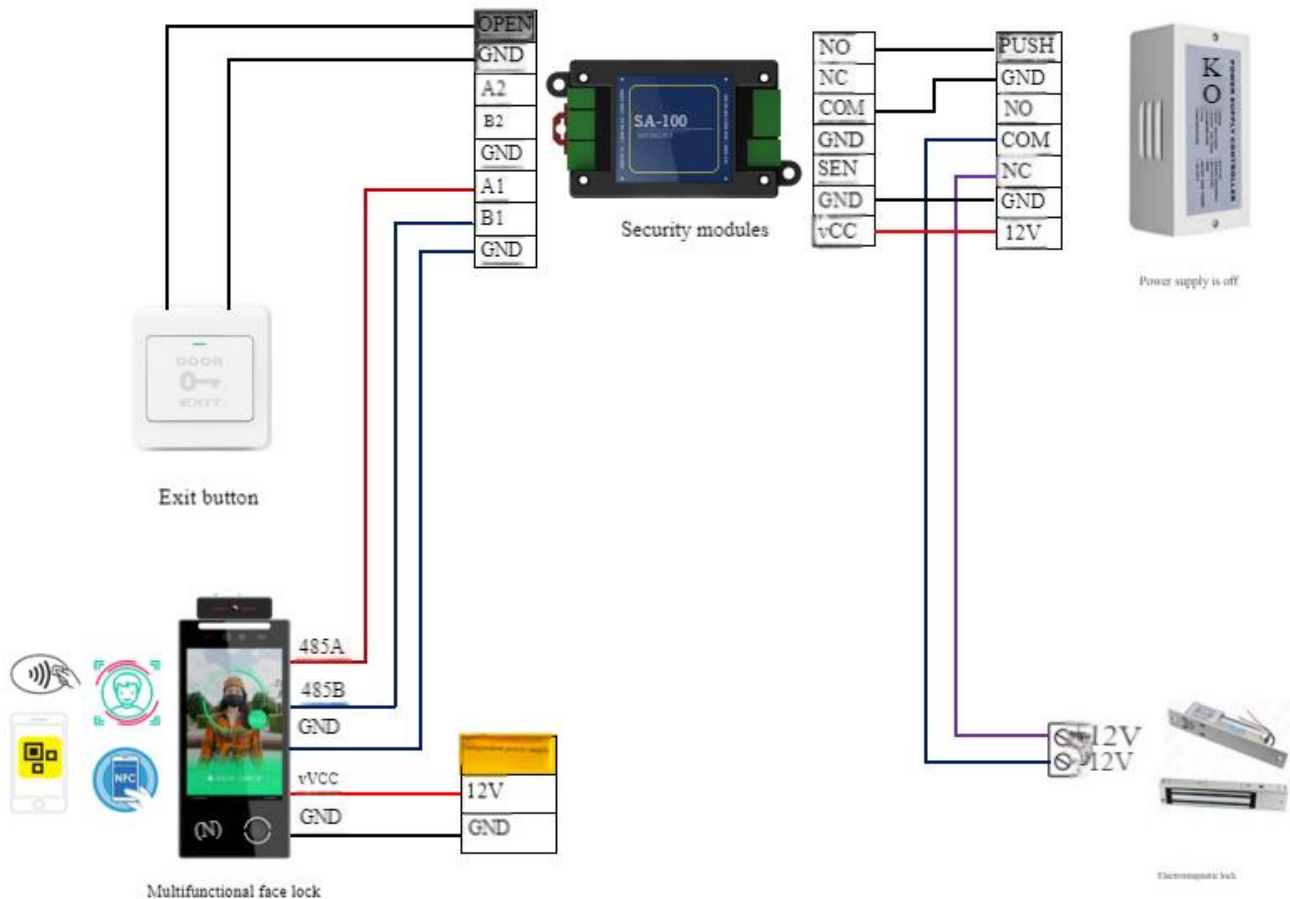
This scenario mainly relies on the network and connects to the server through the network.

The mechanism of the electric plug lock in the figure is power-off unlocking and power on locking (two core wire lock head). If the user uses other types of electric plug locks, they need to be connected according to the characteristics of the electric plug lock.



3.2. Cooperate with the security module

In this scenario, the FCV4914 facial all-in-one machine and security module form a higher security access control system. The FCV4914 connects to the server through the network to achieve online verification, and then communicates with the security module through encrypted 485 protocol to achieve door lock control. Typical applications are shown in the following figure. For more secure applications, please refer to the FCA4900 product manual.



The reason why it is recommended to use independent power supply instead of access control power supply for the access control machine is to prevent illegal personnel from disconnecting the door and short circuiting the positive and negative power supply, which could burn out the access control power supply and cause the electromagnetic lock to disconnect and open.

4. Technical Parameters

Product parameters		
System Parameters	Operating System: Linux	
	Storage capacity: 8GB	
	Processor: ARM Cortex A7 MP2 1GHz	
Display screen	size: 6-inch LCD display screen	
	Resolution: 720 * 1280	
Communication method	wired: 1 channel 10/100M adaptive network port	
	Wireless: 2.4G WiFi	
	1 RS485	
	1 weigand	
physical interface	tamper proof switch	
	relay: 30V1A	
	2-channel alarm signal input interface	
Power supply	9-24V (DC) (recommended 12V power supply)	
	14.4W	
Camera	RGB Camera	Field of View: D=70.3° H=63° V=38°
		Aperture: 2.0
		Resolution: 1920*1080
		Focal length: 4.35MM
	Infrared Camera	Infrared camera field of view D=68° H=60° V=37°
		Aperture 2.2
		Resolution 1616*1232
		Focal length 2.35MM
Temperature measurement	accuracy	within one meter $\pm 0.3\text{ }^{\circ}\text{C}$
	Working temperature	10 $^{\circ}\text{C}$ -35 $^{\circ}\text{C}$
Speaker	with built-in 8 Ω 2W speaker	
Material	Fireproof ABS+Organic Glass	
Working temperature	non temperature measuring version -20 $^{\circ}\text{C}$ ~55 $^{\circ}\text{C}$	
	Temperature measurement version 8 $^{\circ}\text{C}$ ~33 $^{\circ}\text{C}$ (indoor, without wind environment)	
Working humidity	10%~90% (no condensation)	
Protection level	electrostatic protection: contact 8KV, air 8KV	
	Dustproof and waterproof rating: IP66 (note: the temperature measurement version is not waterproof)	
Card swiping performance parameters		

Antenna specifications	13.56MHz
Antenna size	42mm*28mm
Card reading distance	0-5cm(Card types and specifications may vary, and card swiping distances may differ)
支持卡类型	S50、S70、FM1208、FM1216-137、MIFARE CLASSIC EV1 4K(S70)、mifare desfire ev2 d42、UL、FM12081K+7K、NTAG216、ultralight c、UL EV1、DESFIRE EV2 D41、Ultralight EV1、Mifare Desfire ev2 d82
Scanning performance parameters	
QR code recognition system	QRCODE, PDF417, etc.
Scan code to support device	phone screens
Image sensor	640*480
Read direction	Tilt $\pm 40^\circ$, rotation $\pm 360^\circ$, deflection $\pm 30^\circ$
	Level: 62°
	Vertical: 49°
Reading accuracy	$\geq 7\text{mil}$
Reading distance	0~10cm
Scan code feedback	voice prompt
Environmental light intensity	0~80000Lux
Facial recognition performance parameters	
Support mask detection	
1: N algorithm dynamic face detection (anti photo, video attack)	
Hardware infrared liveness detection (anti photo, video attack)	
Portrait capacity of 5000 sheets	
Recognition distance 0.3-1.5m	
Passing rate: $\geq 97\%$ (when the capacity reaches 5000 sheets)	
Misunderstanding rate $\leq 0.01\%$ (when the capacity reaches 5000 sheets)	
Recognition time $<1\text{s}$	

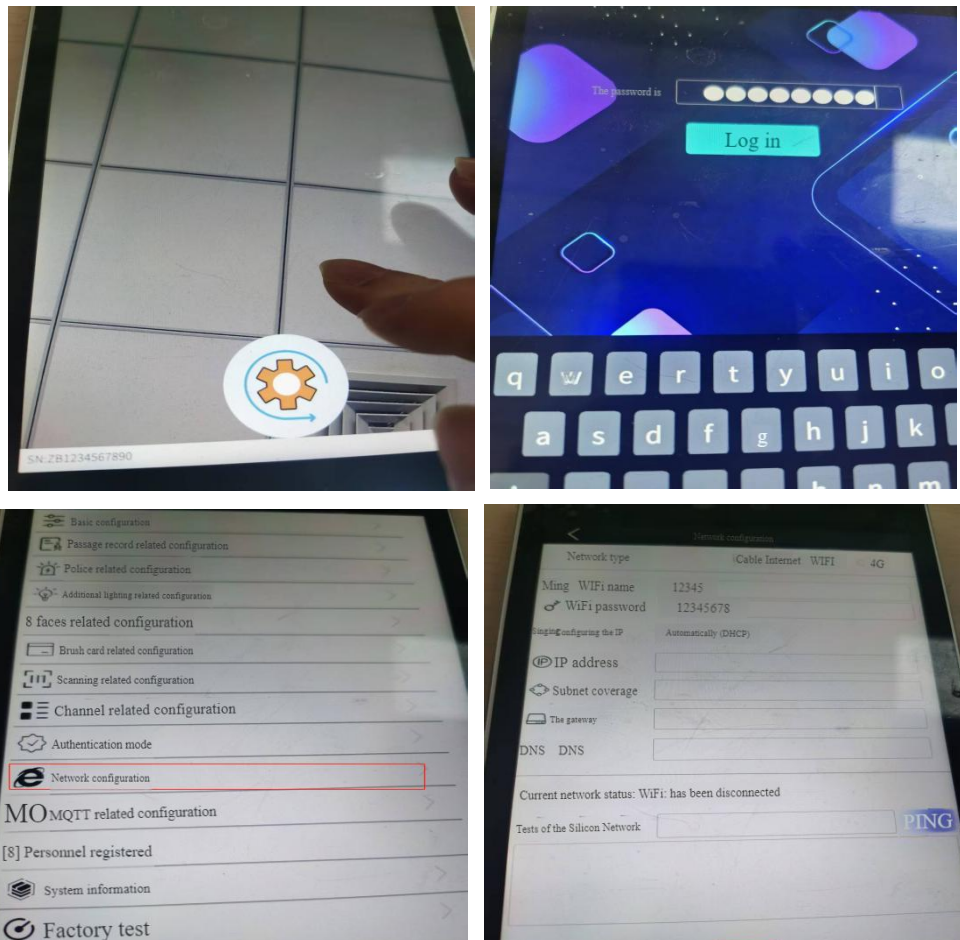
5. Equipment usage instructions

5.1. Equipment Setting Process Description



5.2. Equipment networking configuration

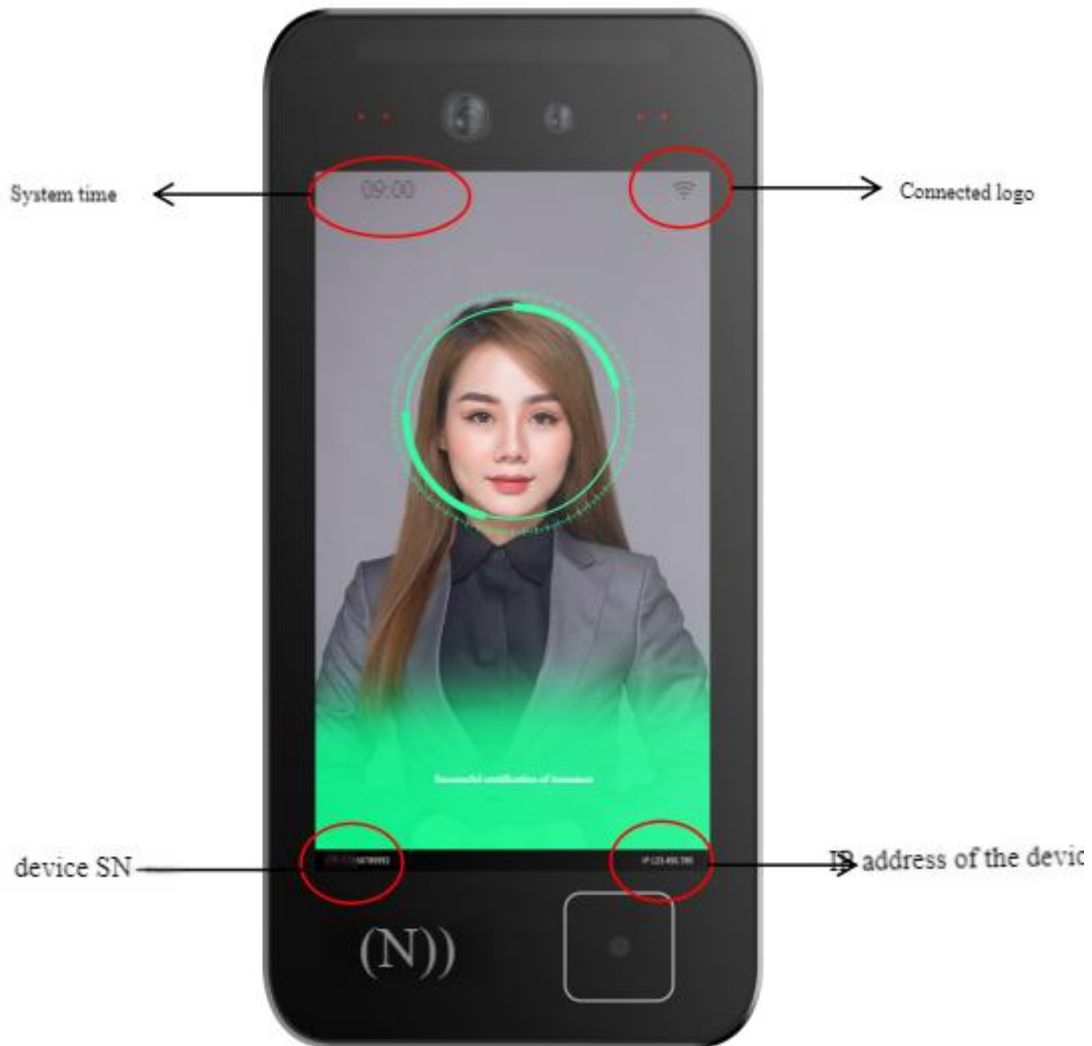
Press and hold the screen for ten seconds to bring up the "gear button", click to enter the login interface, default password: password.



After filling in the network configuration, click save and click the top left corner to return to the main interface. After the device is connected to the internet, if the network connection is successful, the device will announce "Network Connected".

5.3. Login to the facial device backend

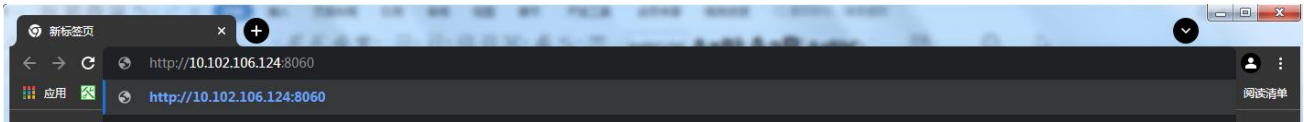
After the facial device is successfully connected to the network, the network icon is displayed in the upper right corner, the device IP is displayed in the lower right corner, the system time is displayed in the upper left corner, and the device SN number is displayed in the lower left corner.



Connect the computer and facial device to the same network. Open the browser, enter `http://device IP address: 8060/` in the address bar, enter enter enter to enter the backend management interface.

Assuming the IP address obtained by calling the bottom right corner of the device is 10.102.106.124.

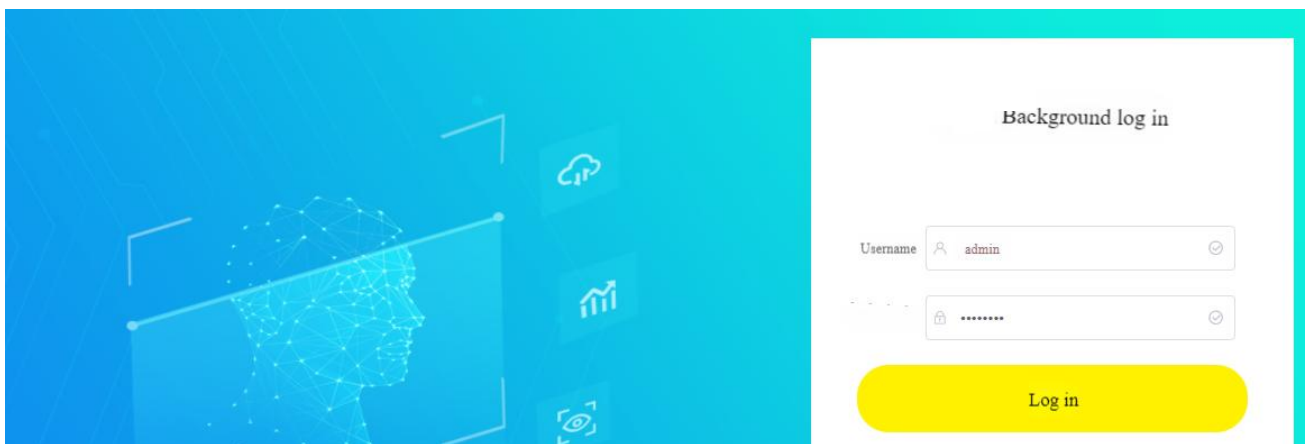
Enter the device address as follows and press Enter.



Enter the backend login interface, which is shown below.

The default username is: admin。

The default login password is: password。



After successful login, the backend prompts to set the "device configuration password".

Please set the device configuration password

Please set the password:

Please confirm the password:

To ensure the security of the system, please change the password first.

Confirmed

This configuration password is mainly used to set the working mode of the scanner, as well as for device upgrades, factory recovery, and other operations. Click confirm to enter the backend system of the following device.

Equipment management system

Help Administrator 退出

Basic settings

§ white list setting

Fixed information

Personal setting

Passage records

Basic configuration

Perceive record related configuration

Speech output related configuration

Police related configuration

Device removal setting

Add lighting related settings

Facial related configuration

Brush card related configuration

Scanning related configuration

Channel related configuration

Authentication mode

Network configuration

MQTT related configuration

Camera is calibrated

Set the device time

Automatically adjust the screen brightness

Screen brightness

Automatically hovered

Automatically place into the video

Automatically shaded

Automatically save time

shows SN

Displays the IP

The volume

Shut down 打开

Shut down open

300 s

Shut down open

30 s

not showing is shown

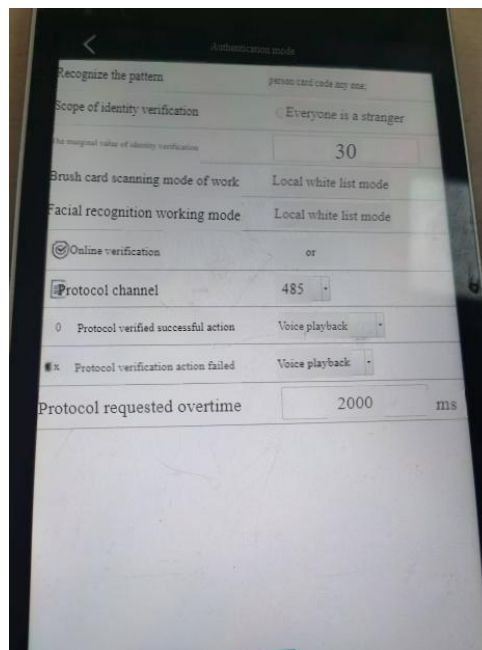
not showing is shown

not showing is shown

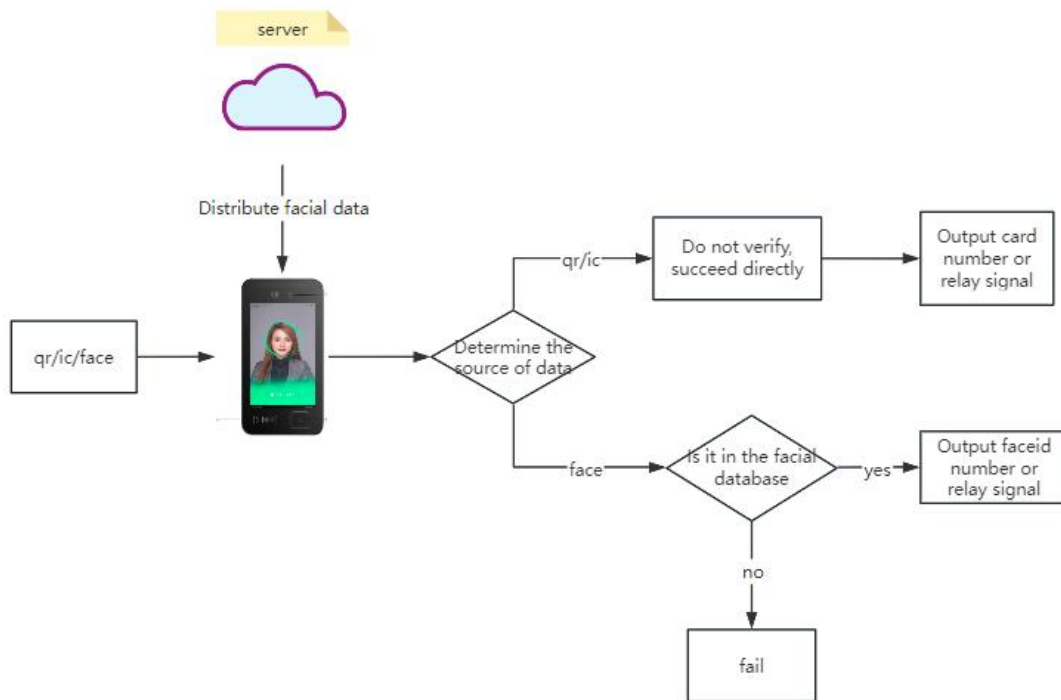
6. Equipment authentication mode description

6.1. Setting method

Refer to the previous content, enter the device backend settings interface, find "Authentication Mode", and select the authentication mode as needed.

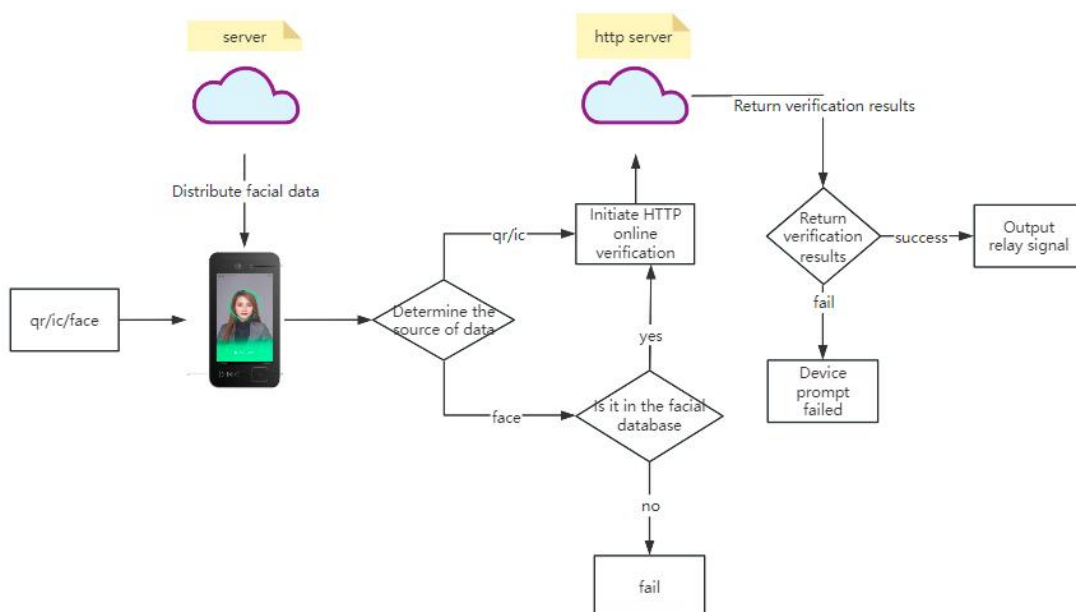


6.2. Transparent transmission mode



In transparent transmission mode, data is directly transmitted by scanning/swiping the code, without any authentication process. Facial recognition only compares with local facial databases.

6.3. Protocol Mode



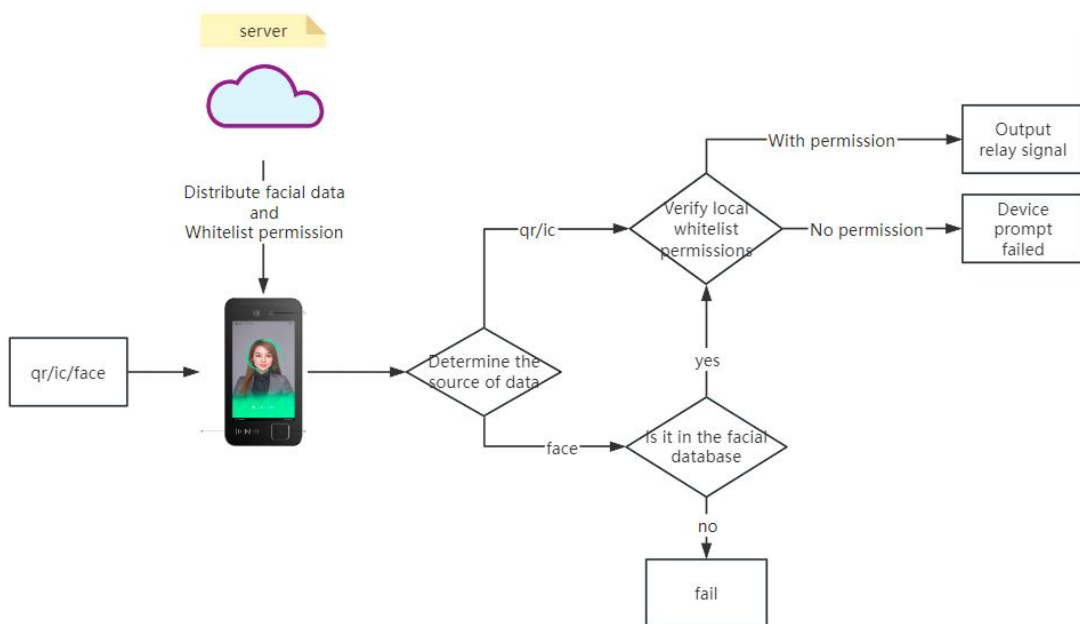
In protocol mode, users need to build an upper computer to receive data and return authentication results through 485, TCP, or HTTP protocols.

The protocol document can be obtained on the official website.

6.4. Development Mode

The development mode is currently only used for card reading and writing operations, and other functions are not currently supported.

6.5. Local Whitelist Mode



7. Quick Settings

Users can refer to the following scenarios for quick settings.

7.1. Scenario 1

Scenario description

- 1, Available for device networking.
- 2, After registering the face, you can freely pass through.
- 3, No need for scanning/swiping card function; Alternatively, you may need to scan/swipe the QR code and physical card number through 485 or Wigan transparent transmission.

Set up process

- 1, Refer to the previous text and log in to the device management backend.
- 2, Select "Add personnel" in the personnel settings.

The screenshot displays the 'Face device background system' web interface. On the left sidebar, the 'Personnel setting' option is highlighted with a red box. The main content area shows the 'Personnel list' management page. At the top, there are input fields for 'Personnel ID' and 'Personnel name', both with placeholder text 'Please enter the person id' and 'Please enter the name of the person' respectively, and a 'Query' button. Below these are four buttons: 'Add personnel' (highlighted with a red box), 'Batch import', 'Batch delete', and 'Batch export'. A table with columns 'Serial number', 'Name', 'id', 'Face picture', and 'Operate' is shown, currently displaying 'No Data'. At the bottom of the table are 'Select all' and 'Deselect' buttons. The footer of the interface includes pagination controls: 'Total 0 Page per page 5 records Total 0 records' and 'Home page', 'Last page', 'Next page' buttons.

- 3, Fill in the personnel ID, such as 123, fill in the personnel name, such as "jack", click the "+" sign, select the local photo, and click confirm; Alternatively, you can directly take photos and input them.

Face device background system

Basic settings

White list settings

Firmware information

Personnel setting

Pass record

Personnel list

Personnel ID: Please enter the person id

Batch delete

Batch export

Serial number

Name

Select all

Deselect

Total 0 Page per page 5 records Total 0 records

Add personnel

ID: 123

Name: jack

Department: list

idCard:

Number:

Sex: Select

Power: Select

Face picture:

Local import

Photo entry

Confirm

英 中 日 俄 韩 越 泰 印 尼 葡 西 德 法 意 加 美 英 中 日 俄 韩 越 泰 印 尼 葡 西 德 法 意 加 美

4, The platform prompts that the input is successful.

5, Set the working mode of facial recognition, QR code scanning, and card swiping to transparent transmission mode.

Face device background system

language: English

Administrator

Quit

Basic settings

White list settings

Firmware information

Personnel setting

Pass record

Basic configuration

Configuration related to access record

Voice and output related configuration

Alarm related configuration

Device anti removal setting

Relevant settings of fill light

Face related configuration

Card swiping related configuration

Code scanning related configuration

Channel related configuration

Authentication mode

Network configuration

MQTT related configuration

Equipment control

Recognition mode	☐ Face / card in one ☐ Witness verification ☒ One of face / card / code
Verification scope of witness card	☐ Strangers only ☒ All
Witness verification threshold	<input type="range"/>
Working mode of swiping card and scanning code	☒ Transparent transmission mode ☐ Local whitelist mode ☐ Protocol mode ☐ Development mode
Working mode of face recognition	☒ Transparent transmission mode ☐ Local whitelist mode ☐ Protocol mode ☐ Development mode
Online verification	☒ No ☐ Yes
Protocol channel	☐ HTTP ☒ 485 ☐ TCP
Protocol verification succeed action	☐ No action ☒ Broadcast voice ☐ Broadcast voice and output relay ☐ Output relay

6, After successful saving, you can swipe your face for authentication, scan the QR code/swipe the card to output the QR code content and swipe the card data.

7.2. Scenario 2

Scenario description

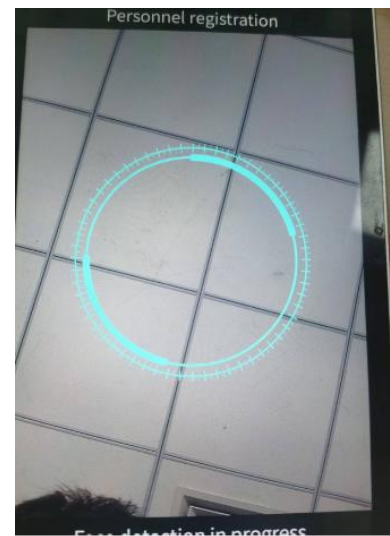
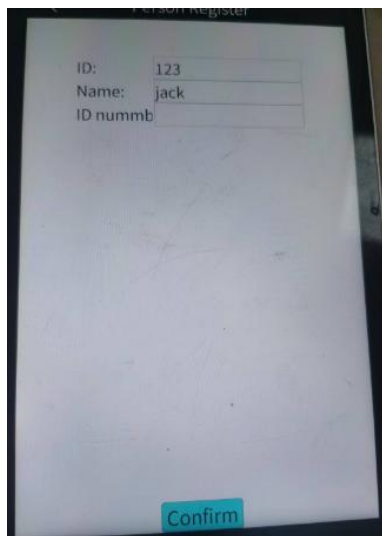
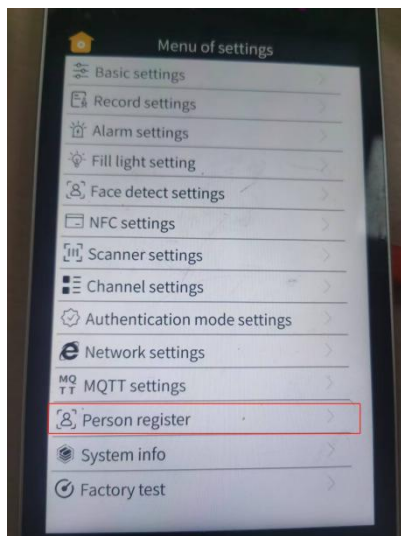
- 1, Unable to connect facial devices to the internet.
- 2, Just register your face and swipe it to pass.

3, The prerequisite for facial recognition authentication is the "transparent transmission mode". The device defaults to "development mode" when it leaves the factory.

Set up process

Need to use touch screen function for personnel registration.

Referring to the previous text, touch the screen to enter the device backend, find "Personnel Registration", enter "ID" and "Name", click "Registration", and enter the "Personnel Registration" recognition interface. At this point, the face enters the recognition box to complete the face registration.



7.3. Scenario Three

Scenario description

1. Available for device networking.
2. Swipe the card to enter the whitelist mode, which means that the card authentication permission is entered into the device in advance, and the card can be swiped to open the door.
3. Face recognition can be done in any mode.

Set up process

1. Refer to the previous explanation and log in to the device management backend.
2. Select the whitelist setting.
3. Select Add.
4. Enter the personnel ID.

The screenshot shows the 'Add' dialog box in the device management backend. The dialog has the following fields and options:

- Person ID:** A text input field with a red border and a red asterisk, containing the placeholder text 'Please enter user ID'.
- Personnel type:** A dropdown menu with a blue border and a blue asterisk, showing 'Please choose personnel type'.
- Start time:** A dropdown menu with a white border, showing 'QR code'.
- End time:** A dropdown menu with a white border, showing 'Card'.
- Repetition type:** A dropdown menu with a white border, showing 'Please choose repetition type'.
- Name:** A text input field with a white border, containing the placeholder text 'Please enter your name'.
- Department:** A text input field with a white border, containing the placeholder text 'Please enter the Department'.

The background interface shows a sidebar with 'Basic settings', 'White list settings', 'Firmware information', 'Personnel setting', and 'Pass record'. The 'White list settings' section is active, displaying a table with columns 'Serial number', 'User type', 'Start time', 'Repeat end time', and 'Operate'. The table has two rows of data. The 'Add' button is visible in the top right corner of the interface.

When the user type is facial: fill in the ID of the person at the time of registration;

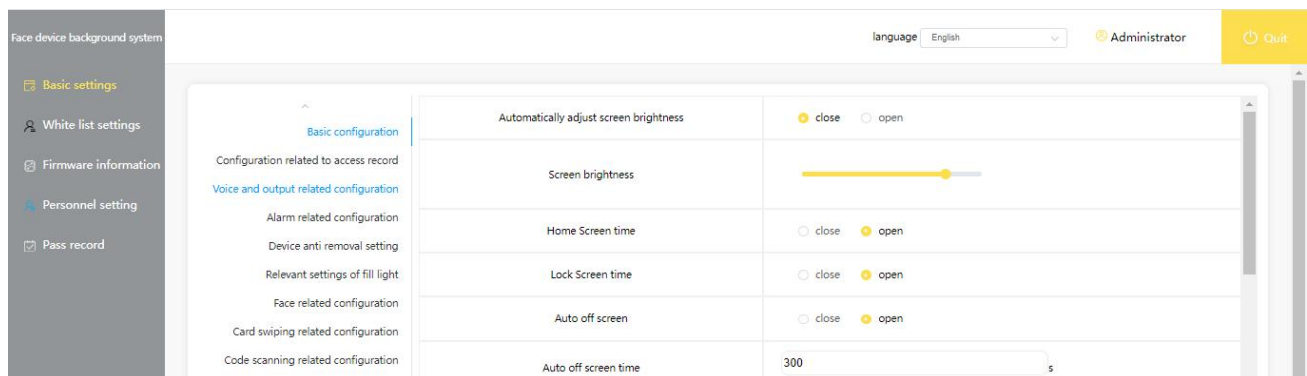
When the user type is a card: the ID is a hexadecimal positive sequence card number, and the letters must be lowercase, such as a9decad1.

5. Select the start time/end time and specify the validity period of the whitelist.
6. Choose not to repeat the type.
7. Click OK to proceed.

8. Background Description

8.1. Basic Settings

Basic configuration

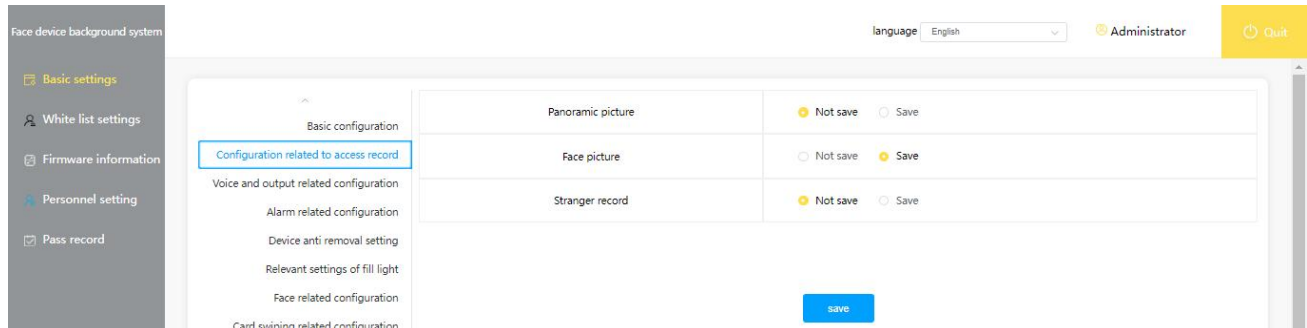


The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Automatically adjust screen brightness	close	Turn on/off the device to automatically adjust the screen brightness
Screen brightness	80	Set screen brightness value
Automatic screen shutdown	open	After a period of standby, the screen will turn off
Automatic screen shutdown time	300 seconds	Off screen standby time
Automatic screensaver	open	After a certain amount of standby time, enter the screensaver screen
Automatic screensaver time	30 seconds	Screen saver standby time
Display SN	display	Is the SN number displayed in the bottom right corner of the screen
Display IP	display	Is the device IP address displayed in the bottom right corner of the screen
volume	60	Adjust the volume level
Automatic update time	open	Automatically update device time through networking
Automatically set time zone	open	Automatically set device time zone through networking

Equipment name	\	Naming devices
----------------	---	----------------

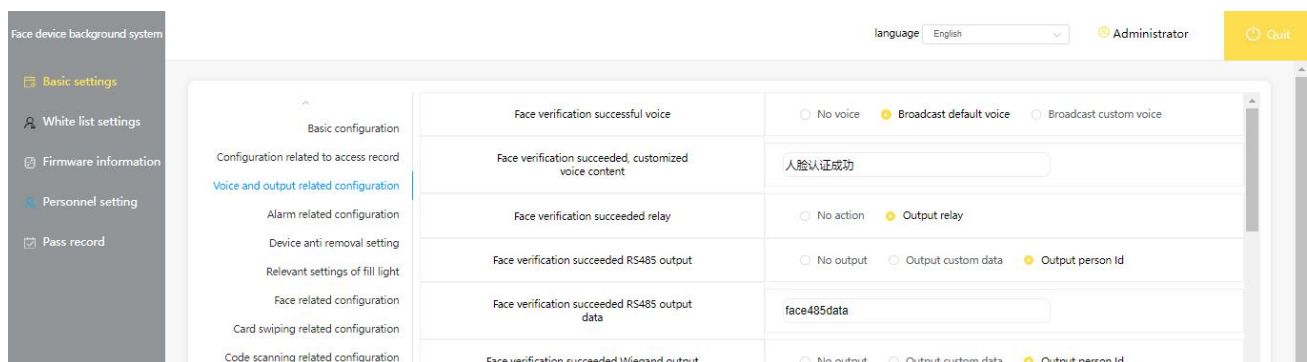
Configuration related to traffic records



The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Panoramic image	Do not save	Set whether to save panoramic images during face brushing
Facial image	preservation	Only save facial photos taken during facial recognition, with priority over panoramic images
Stranger Records	Do not save	Set whether to save strangers' facial recognition records

Voice and output related configurations



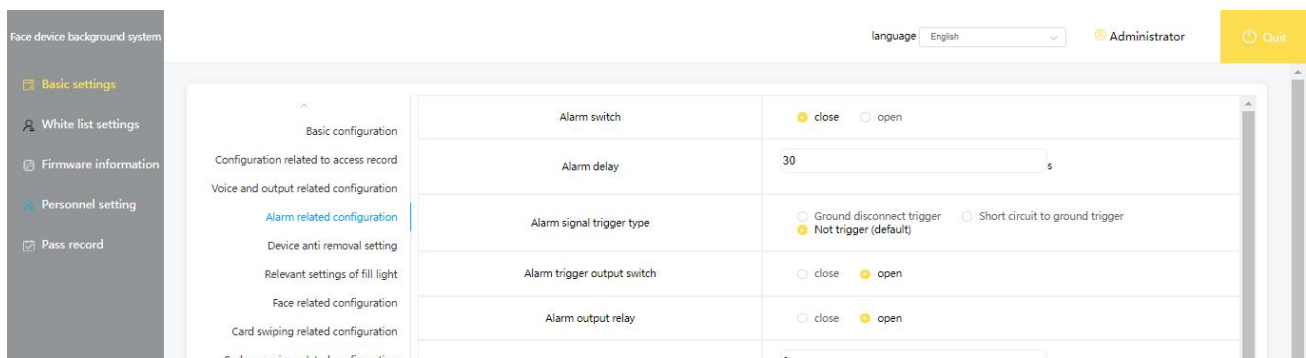
The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Facial verification successful voice	Play voice default	When the facial recognition device successfully recognizes the face, voice feedback action will be taken.
		Play custom voice: not effective in protocol mode and development mode

Facial verification successfully customized voice content	Facial verification successful	Set custom voice content
Facial verification successful relay	Output relay	When facial recognition is successfully set, output relay action
Facial verification successful 485 output	Output personnel ID	When facial recognition is successfully set up, the 485 port outputs data content
Facial verification successful 485 output data	face485data	Effective when the previous option is selected as 'Output custom data '
Facial verification successful, Weigen output	Output personnel ID	When facial recognition is successfully set up, the Wiegand port outputs data content. Personnel ID must comply with Wiegand 26 or Wiegand 34 specifications
Facial verification successful, Weigen outputs data	1234567890	Effective when the previous option is selected as 'Output custom data '
Facial verification failed speech	Play default voice	When the facial recognition device fails to recognize a face, a voice feedback action will be taken.
		Play custom voice: not effective in protocol mode and development mode
Facial verification failed to customize voice content	Facial verification failed	Set custom voice content
Card verification successful voice	Play default voice	When the card swipe is successfully set, a voice feedback action will be taken.
		Play custom voice: not effective in protocol mode and development mode
Card verification successful, customized voice content	Card swipe successful	Set custom voice content
Card swipe verification successful relay	Output relay	When the card swipe is successful, the output relay will activate
Card verification successful 485 output	Output card number	When the card swipe is successful, the 485 port outputs data content
Card verification successful 485 custom output data	card485data	Effective when the previous option is selected as 'Output custom data '
Card verification successful, Weigen output	Output card number	When the card swipe is successful, the Wiegand port outputs data content
Card verification successful, Weigen outputs data	1233211230	Effective when the previous option is selected as 'Output custom data '
Card verification failed via voice message	Play default voice	Voice feedback action when card swipe fails.
		Play custom voice: not effective in protocol mode and development mode
Card verification failed, custom voice content	Card swipe failed	Set custom voice content
Scan code verification	Play default	When the QR code is successfully scanned, a

successful voice	voice	voice feedback action will be taken.
		Play custom voice: not effective in protocol mode and development mode
Scan code to verify successful voice content	Scan code successfully	Set custom voice content
Scan the code to verify the relay successfully	Output relay	When the QR code is successfully scanned, the output relay will activate
Scan code verification successful 485 output	Output card number	When the QR code is successfully scanned, the 485 port outputs the data content
Scan code verification successful 485 output data	qr485data	Effective when the previous option is selected as 'Output custom data '
Scan code verification successful, Weigen output	Output card number	When the QR code is successfully scanned, the Weigen port outputs the data content
Scan code verification successful, Weigen outputs data	9876543210	Effective when the previous option is selected as 'Output custom data '
Scan code verification failed voice message	Play default voice	Voice feedback action when scanning code fails.
		Play custom voice: not effective in protocol mode and development mode
Scan code verification failed to customize voice content	Scan code failed	Set custom voice content

Alarm related settings

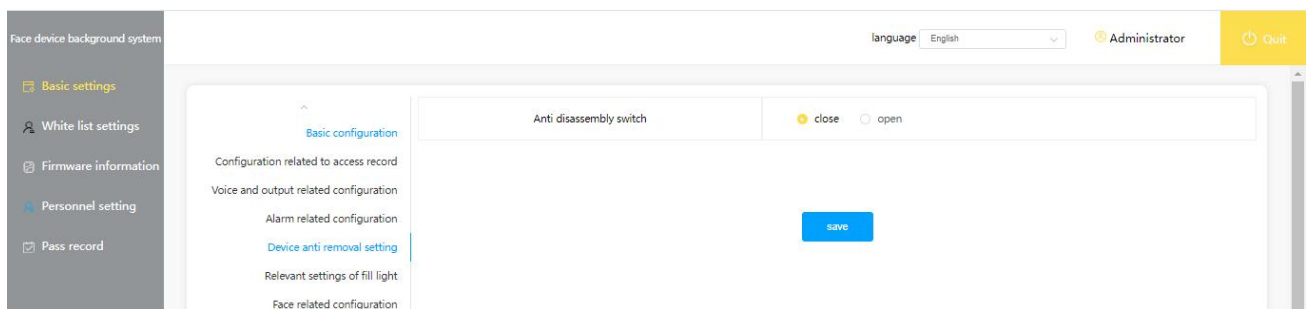


The list of configuration item descriptions is as follows

Configuration items	Default value	explain
Alarm service switch	close	Set up/disable the alarm signal triggering function for facial devices
Alarm delay	3 seconds	The alarm trigger signal needs to last for 3 seconds to trigger the alarm voice

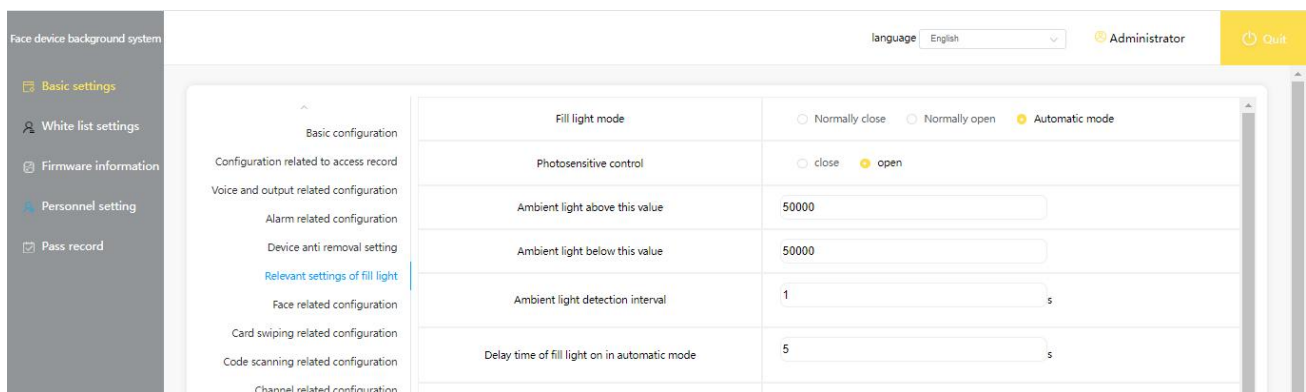
Alarm signal trigger type	Do not trigger	Set the alarm triggering method
Alarm triggers output switch	open	Set the feedback action of the device after triggering the alarm signal
Alarm output relay	open	When the alarm signal is triggered, take immediate action
Alarm Wiegand output	close	When the alarm signal is triggered, immediately output Wiegand data
485 output	close	When the alarm signal is triggered, immediately output 485 data
Voice playback	Default voice	The voice broadcast when the alarm signal is triggered

Equipment anti dismantling setting



By default, it is turned off. When the device is removed or powered on but not installed, an alarm will sound.

Related settings for fill lights

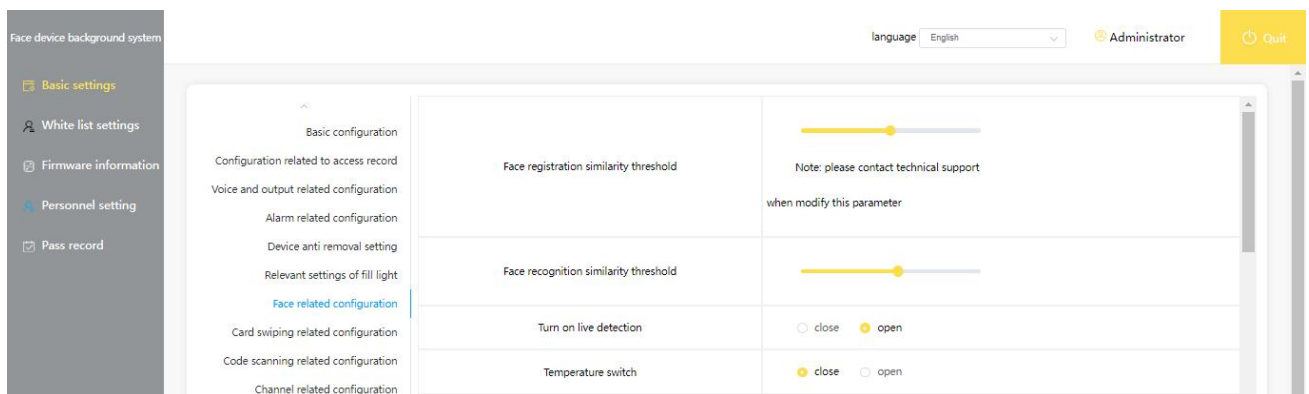


The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Supplementary lighting mode	Automatic mode	Set the working mode of the fill light. In automatic mode, the fill light will automatically turn on or off according to the needs of facial recognition
Photosensitive control	open	This item is temporarily not in effect
The ambient light is higher than this value	1100	Effective in automatic mode: When the ambient light exceeds this value, turn off the fill light
The ambient light is below this value	500	Effective in automatic mode: turn on the fill light when the ambient light is below this value
Environmental light detection interval	1	The device detects the ambient light intensity every second
Delay time for the fill light to turn on in automatic mode	10	Delay time for the fill light to turn on in automatic mode
Brightness of fill light	80	Set the brightness of the fill light

Attention: It is recommended to keep the high and low values of ambient light as default. If the environment requires adjustment, the high value should be at least 600 larger than the low value. Otherwise, the backlight of the device will perform abnormally

Facial related configurations

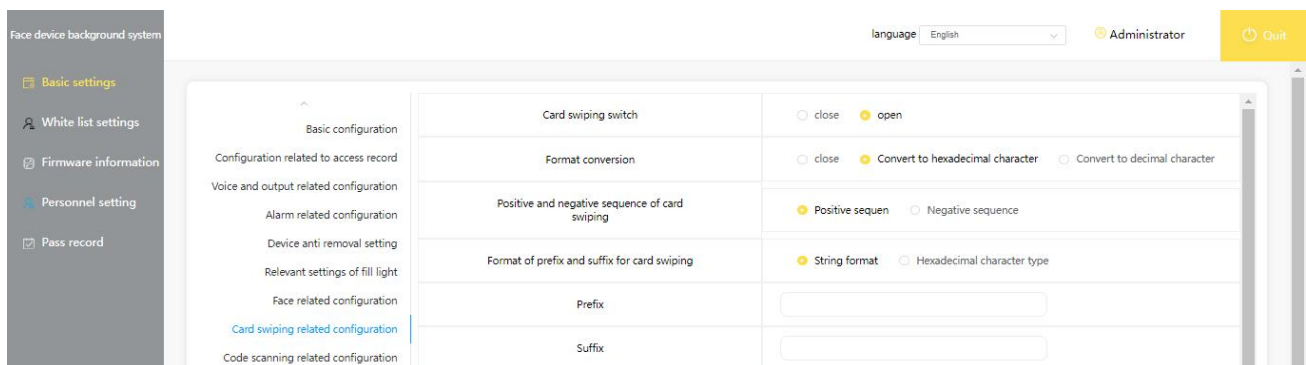


The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Facial registration similarity threshold	50	When setting up registration, it is recommended to maintain the default value for face detection standards. The larger the value , the stricter the detection
Facial recognition similarity threshold	54	When setting the facial recognition standard, it is recommended to maintain the default value . The larger the value , the stricter the detection
Activate biopsy	open	Set whether to enable liveness detection function

Temperature switch	close	Set whether to enable temperature measurement function
Alarm temperature	37.299	Set temperature alarm threshold
Facial recognition number configuration	1	Only supports identifying one person simultaneously
Facial recognition	open	Set whether to enable facial recognition function
Infrared image	close	Set whether to enable infrared imaging. It is recommended to disable it
Live detection threshold	10	Set live detection standards, it is recommended to maintain the default value . The larger the value, the stricter the detection
Mask testing	close	Did the testing personnel wear masks
Mask recognition	open	When the facial recognition personnel wear masks, turning on this option can help identify them successfully
Mask threshold	53	Set detection standards for recognizing the faces of individuals wearing masks. It is recommended to maintain the default values , with larger values indicating stricter detection
Identify distance	150cm	Set the maximum recognition distance for faces
Repetitive broadcast interval	5 seconds	Set the interval for repeated broadcasts
Time interval for repeated recognition	1.5 seconds	Set the interval time for repeated facial recognition
Identify timeout	1 second	Set the timeout period for facial recognition
Duplicate recognition switch	open	Set whether to enable the detection of facial duplicate recognition function
Stranger voice	Hello stranger	Broadcast when identifying unregistered faces
Voice mode	No voice	Set the voice to play when face verification is successful
greetings	No voice	When selecting to play a greeting, choose the type of greeting

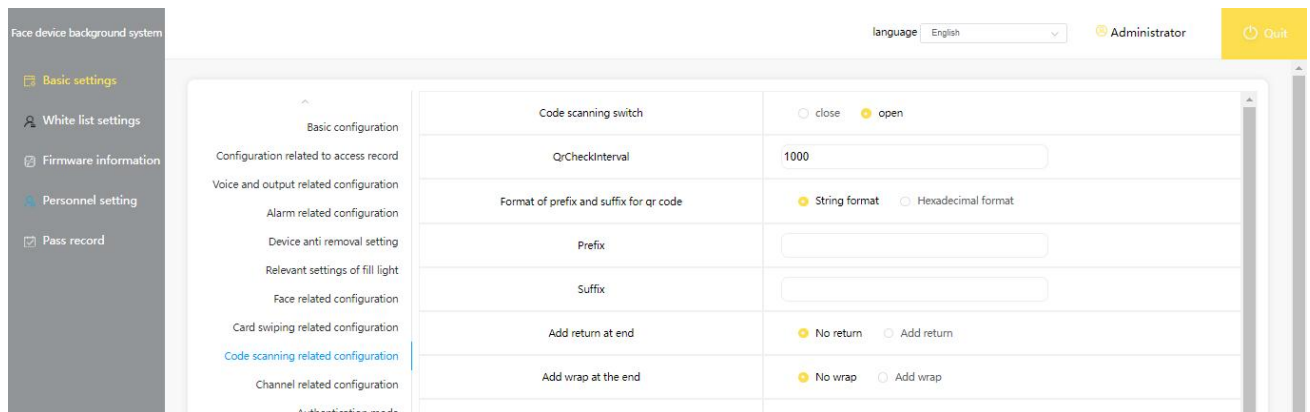
Card swiping related configurations



The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Swipe card switch	open	Set whether to enable card swiping function
format conversion	shut	Set the output format for card swiping
Swipe card in reverse order	positive sequence	Set the forward and reverse sequence formats for card swiping output
Format of card swiping prefix and suffix	Hexadecimal system	Set the format of card number prefixes and suffixes
prefix	(Empty)	Card number prefix
suffix	(Empty)	Card number suffix
Add Enter at the end	close	Add a carriage return after the card number
Add a line break at the end	close	Add a line break after the card number

Scan code related configurations



The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Scan code switch	open	Set whether to enable the scanning function
Format of QR code prefix and suffix	String format	Set the format of the scanning prefix and suffix
Scan code prefix	(Empty)	Scan code prefix
Scan code suffix	(Empty)	Scan code suffix
Add Enter at the end	close	Scan the code content and press enter
Add a line break at the end	close	Scan the code content and add a line break
Weigen output format conversion	Do not convert	When the scanning output channel is set to Wiegand, it takes effect

Channel related configurations

Face device background system

language: English Administrator Quit

Basic settings

White list settings

Firmware information

Personnel setting

Pass record

Basic configuration

Configuration related to access record

Voice and output related configuration

Alarm related configuration

Device anti removal setting

Relevant settings of fill light

Face related configuration

Card swiping related configuration

Code scanning related configuration

Channel related configuration

TCP switch

close open

TCP server IP

10.102.106.116

TCP server port number

8060

RS485 baud rate

115200-8-N-1

Wiegand

Wiegand 26 Wiegand 34

Relay delay time

7000 ms

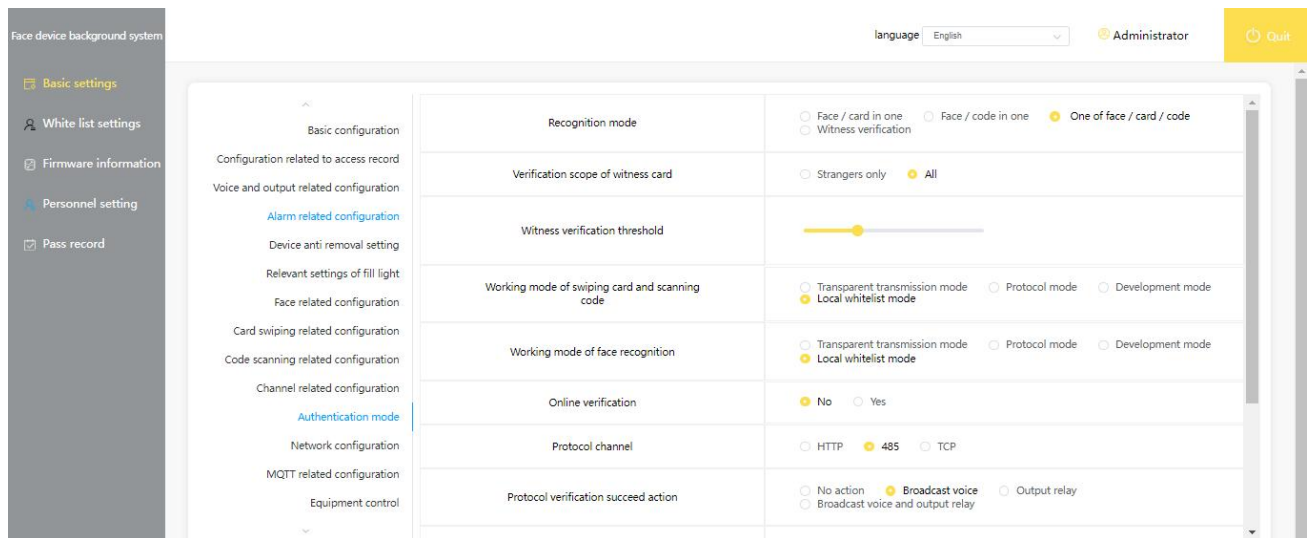
Relay operation mode

Equipment's own relay SA100 Security Module

The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
TCP switch	shut	Set whether to enable TCP transmission channel
TCP server IP	\	Set TCP server-side IP
TCP server port number	\	Set TCP server port number
RS485 baud rate	115200-8-N-1	Set 485 channel parameters
Wiegand	Wigan 34	Set up Wigan Port Protocol
Relay delay time	2000ms	When the authentication is successful, the relay will maintain its action time

Authentication mode

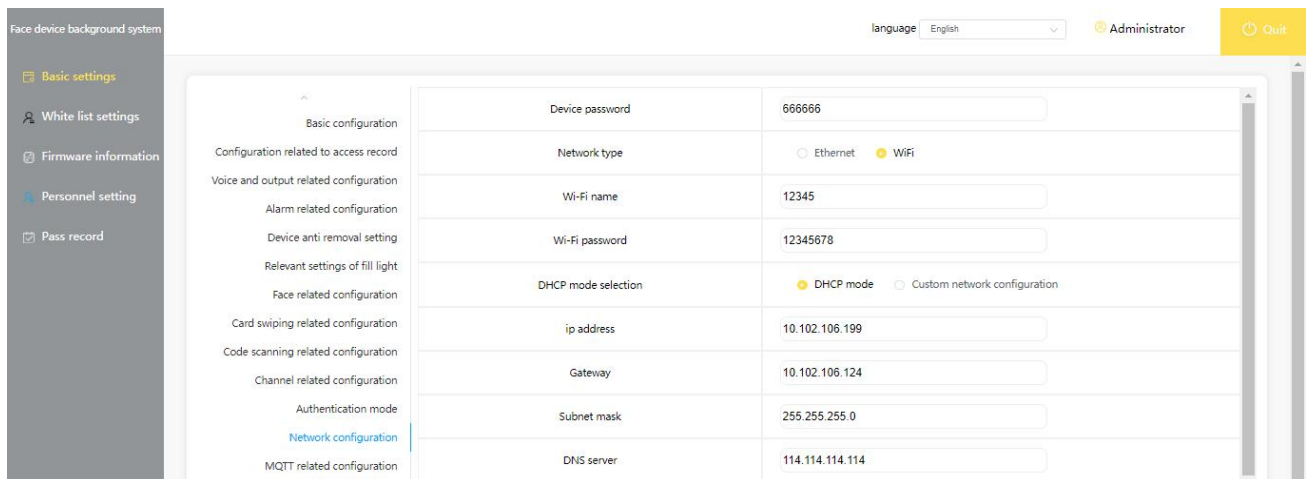


The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Identify patterns	Any person/card/code	The other two items are not currently supported
Swipe card and scan code working mode	Protocol mode	Working mode (for card swiping/scanning 1: transparent transmission mode, 2: protocol mode, 3: development mode, 4: local whitelist mode) Note: When in development mode, the facial recognition working mode will also change to development mode at the same time
Facial recognition mode	Transparent transmission mode	Working mode (for facial recognition 1: transparent transmission mode, 2: protocol mode, 3: development mode, 4: local whitelist mode) Note: When in development mode, the facial recognition working mode will also change to development mode at the same time
Online verification	no	Valid when scanning/swiping card or facial recognition is in whitelist mode Yes: offline priority No: offline only
Protocol channel		Protocol channel (1: HTTP, 2:485, 3: TCP) Note: When in development mode, this configuration does not support HTTP in the channel. If HTTP is configured, TCP will be used by default
Protocol verification successful action		Protocol verification successful action (corresponding bit 1 is valid, bit 1: broadcasting voice, bit 2: outputting relay)

Protocol verification failure action		Protocol verification failure action (bit1: broadcasting voice, bit2)
HTTP protocol callback address		HTTP protocol callback address
HTTP request timeout		HTTP request timeout in milliseconds

network configuration



The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
Device password	Default device password input	The device password set when logging into the system for the first time
Network type	According to the configuration tool, the configuration shall prevail	Set the networking method
Wi Fi Name	\	The wifi name that needs to be configured when setting wifi mode
Wi Fi password	\	The WiFi password that needs to be configured when setting the WiFi mode
DHCP mode selection	DHCP	IP mode selection dynamic/static
IP address	\	Configure when selecting custom network configuration
gateway	\	Configure when selecting custom network configuration
Subnet mask	\	Configure when selecting custom network configuration
DNS server	\	Configure when selecting custom network configuration

MQTT related configurations

Face device background system

language English Administrator Quit

Basic settings

White list settings

Firmware information

Personnel setting

Pass record

Card swiping related configuration

Code scanning related configuration

Channel related configuration

Authentication mode

Network configuration

MQTT related configuration

Equipment control

Camera calibration

Set device time

Disable / enable

Password modification

Server address

tcp://47.122.17.4:61622

Client ID

ZB1234567890

User name

admin

User password

password

Topic prefix

Qos

☐ Qos0 ☐ Qos1 ☒ Qos2

The list of configuration item descriptions is as follows:

Configuration items	Default value	explain
server address	0.0.0.0	Set MQTT server address
client ID	123456788	Set client ID
user name	admin	Set username
User password	password	Set username
Theme prefix	\	Set theme prefix
Qos	Qos2	Set QoS type

Camera calibration

This is a device debugging item and users are prohibited from using this feature.

Set device time

Set the face device system time.

Disable Enable

Disable/start the device.

Password modification

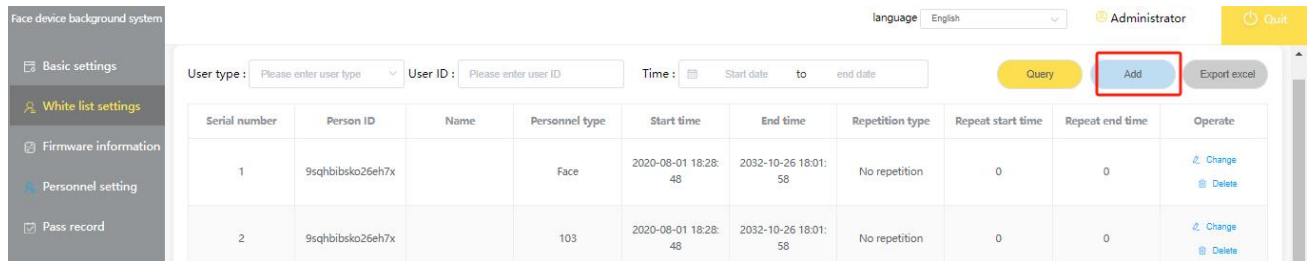
Change the backend login password and device configuration password.

Device restart

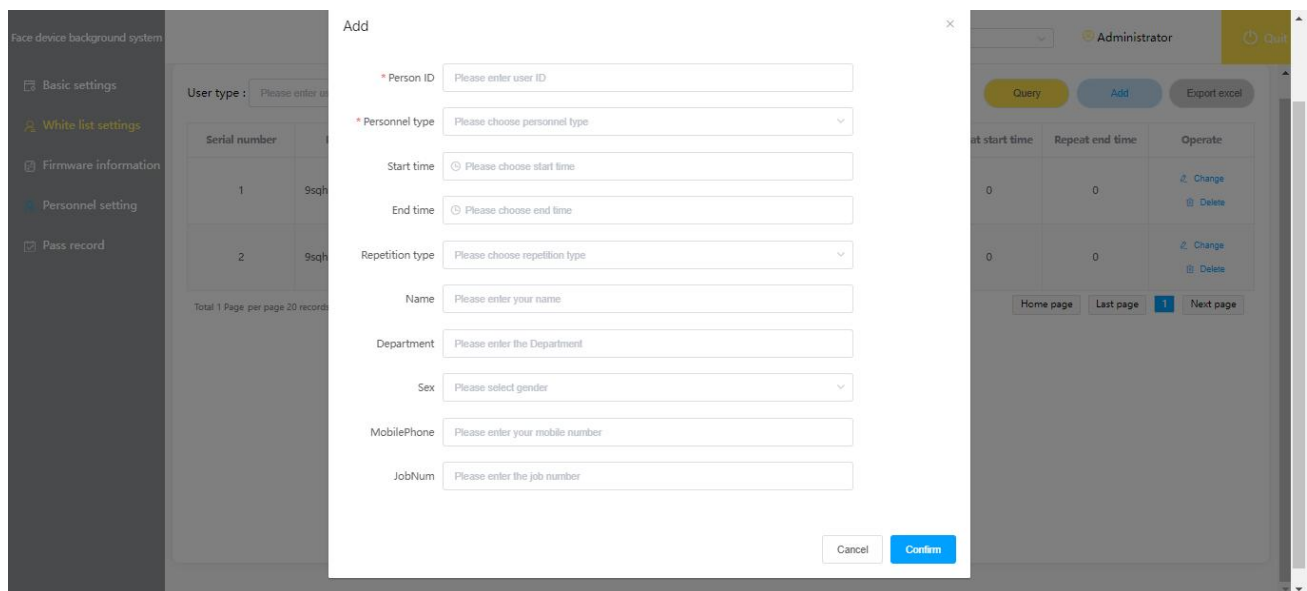
Restart the facial device.

8.2. Whitelist Setting

When the card swiping/scanning code or facial recognition work mode is selected as the whitelist work mode, the personnel ID set through the whitelist can pass normally.



Click to add



Select personnel IDs, user types, whitelist start and end times, and duplicate types to be whitelisted.

When the user type is selected as QR code, a QR code needs to be generated according to the "Authorization Pass Code Mechanism Usage Instructions".

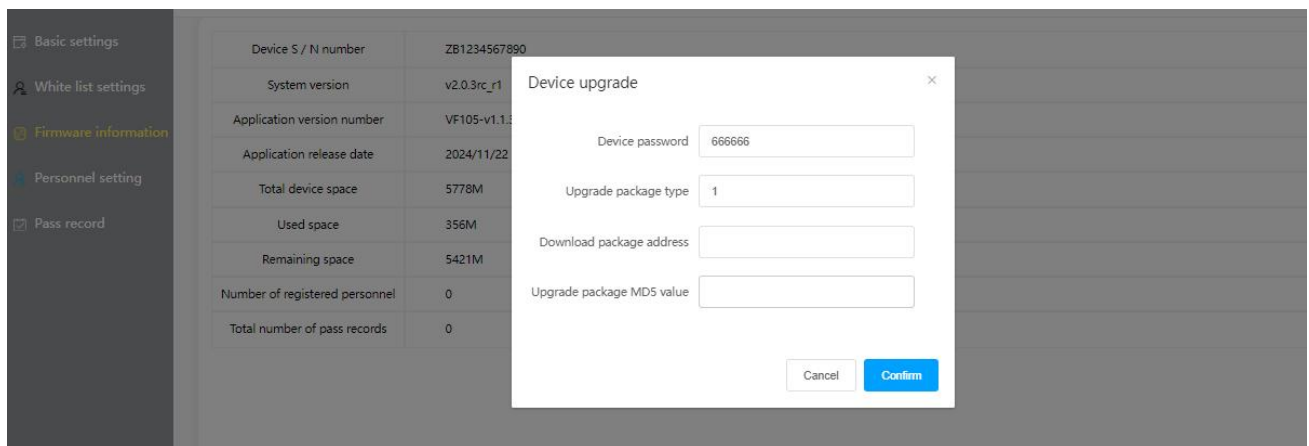
When the user type is selected as face, the user ID is the person ID set when registering face.

When the user type is selected as card, the user ID is the card number.

8.3. Firmware Information

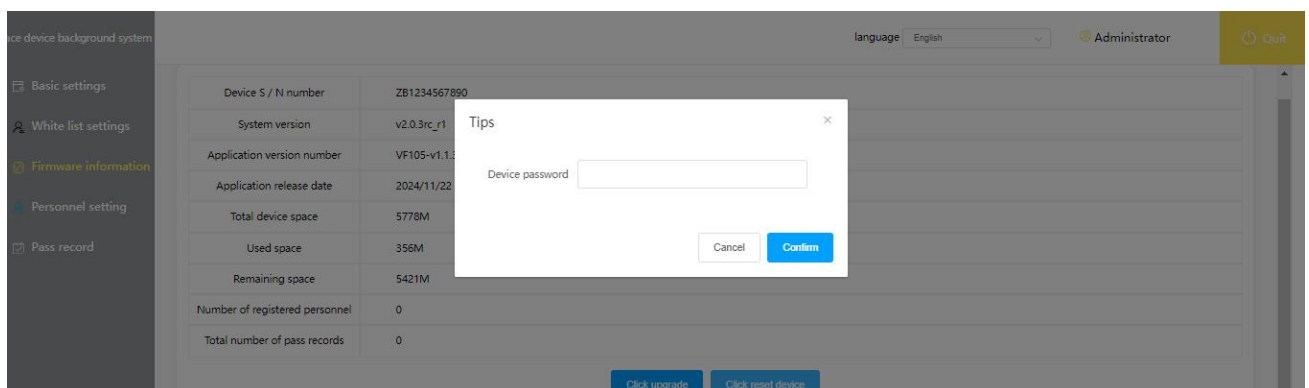
This section is mainly used for upgrading equipment or restoring equipment to factory.

Firmware update



Need to contact the manufacturer to obtain the upgrade address and MD5 value.

Reset device



After entering the device password, click "OK".

The device will be restored to its factory state.

8.4. Personnel Configuration

Add personnel

Local import

The screenshot shows the 'Add personnel' form in the 'Personnel setting' section. The form includes the following fields and buttons:

- ID**: Text input field.
- Name**: Text input field.
- Department**: Text input field.
- list**: Text input field.
- idCard**: Text input field.
- Number**: Text input field.
- Sex**: Dropdown menu with 'Select'.
- Power**: Dropdown menu with 'Select'.
- Face picture**: Section with two options: 'Local import' (selected) and 'Photo entry'.
- Confirm**: Yellow button at the bottom right.

After filling in the personnel ID and name (department and gender permissions are optional), click on local import, and then click the plus sign in the right border image to import the facial photo.

Photo input

After filling in the personnel ID and name (department and gender permissions are optional), click on the photo import button, and the device will enter the photo mode. When employees perform facial recognition, the device will be successfully registered.

Batch import

Download the table template, create the table, and then import it.

8.5. Traffic Records

This item is used to query and delete traffic records, and export traffic record tables.

The screenshot shows the 'Traffic Records' section in the 'Personnel setting' section. It includes the following elements:

- Language**: Dropdown menu set to 'English'.
- Administrator**: User role indicator.
- Quit**: Yellow button in the top right corner.
- Search filters**:
 - Personnel job number**: Text input field.
 - Personnel name**: Text input field.
 - Time**: Date range selector with 'Start date', 'to', and 'end date'.
- Action buttons**: 'Start query' (yellow), 'Batch delete' (orange), 'Export excel' (blue), and 'Export picture' (grey).
- Table**:

	Time	id	Name	Picture	Pass results	Reason	Operate
No Data							
- Select all** and **Deselect** buttons below the table.
- Page info**: 'Total 0 Page per page 5 records Total 0 records'.
- Navigation**: 'Home page', 'Last page', and 'Next page' buttons.

9. matters needing attention

Facial registration photo requirements

Facial pixels: minimum 80, maximum 512

Image size: 50-300K

Image height and width: Width 512-800, Height 640-1024

Image format: JPG

Background requirements: Daily photos, no beauty filters, no heavy makeup, no sunglasses, scarves, masks or other obstructions

Facial recognition registration requirements

When registering with facial recognition, the face needs to be in the registration box, preferably occupying the entire registration box, and staring at the registration box for 2-3 seconds, waiting for the device to complete the registration.