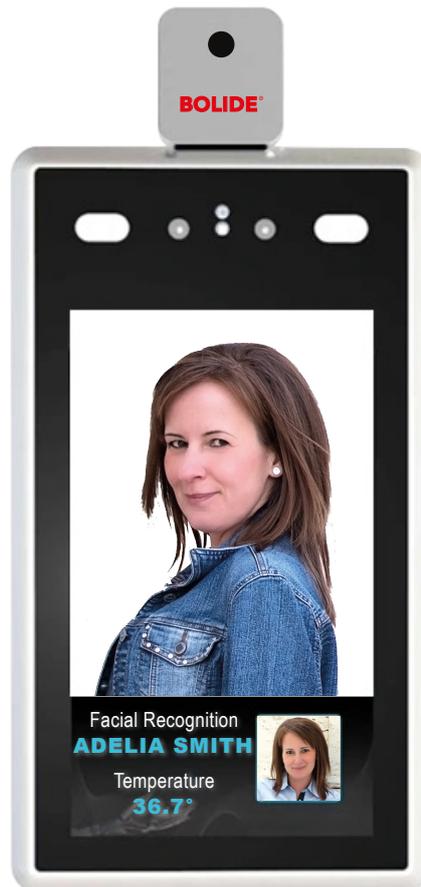




# BN2600-ACTC User Manual



## Introduction

### Product Overview:

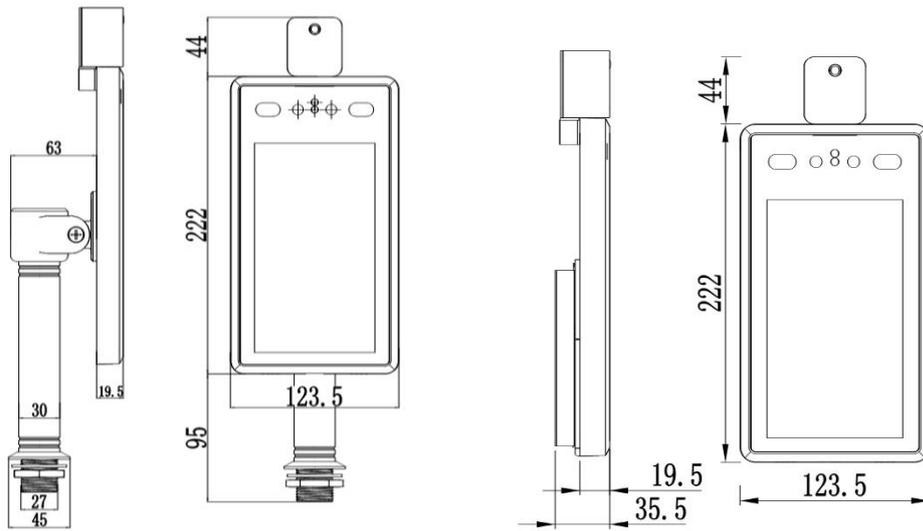
- Non-contact temperature taking automatically while recognizing face, efficient and effective.
- Taking Human Temperature range: 30-45°C, ±0.3 °C accuracy.
- Detecting and reminding if people is not wearing mask (when mask detection is ON)
- Can set high temperature alarm. White list /VIP list alarm.
- Professional face recognition algorithm with high accuracy, recognition time <500ms
- Support wide dynamic≥80dB, can get a clear image under strong backlight environment.
- Linux operation system, reliable and stable.
- Support IE/Edge/Firefox/Chrome/Safari etc. web browser, with multi-language GUI.
- Windows/Linux SDK and HTTP protocol.
- 7 inch IPS high resolution displayer.
- Built in multi-language speaker.
- IP34
- MTBF > 50000 H
- Support 19200 faces database and 100000 face recognition records
- Support one Wiegand output, one alarm I/O output for access control.
- Free professional VMS to export data, attendance and people counting.

### Packing List

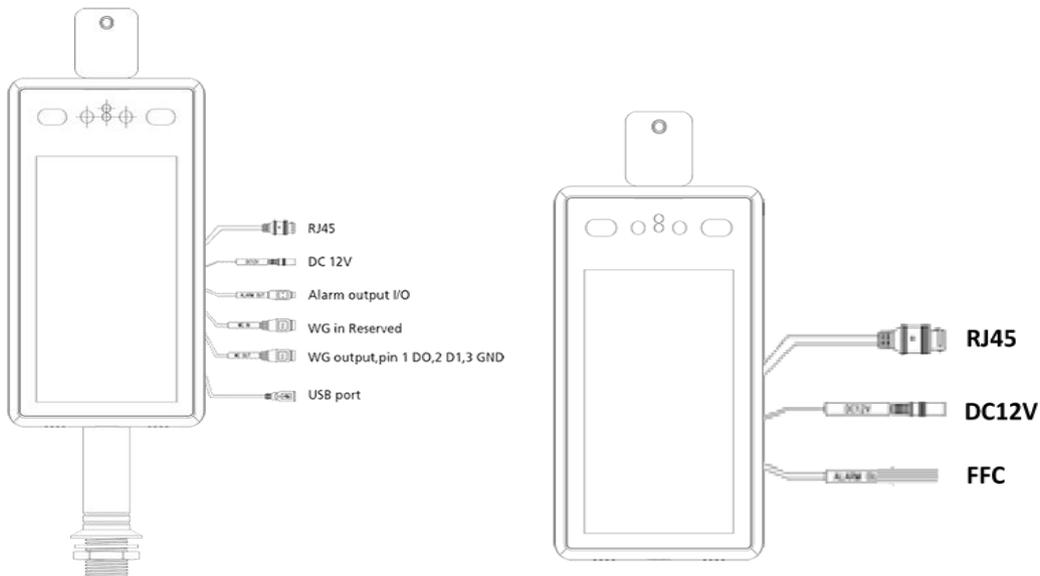
Access Control Camera	Wall Mount	Pole Mount
User Manual	1 piece	1 piece
Power adapter	1 unit, 12V 3A	1 unit, 12V 3A
Accessories	Mounting brackets, Connecting Cable	Cable Ties
	Screw kit, L Wrench	Screw kit, L Wrench
	Network waterproof connector	Network waterproof connector

---

Dimension (cm)



Connection Diagram

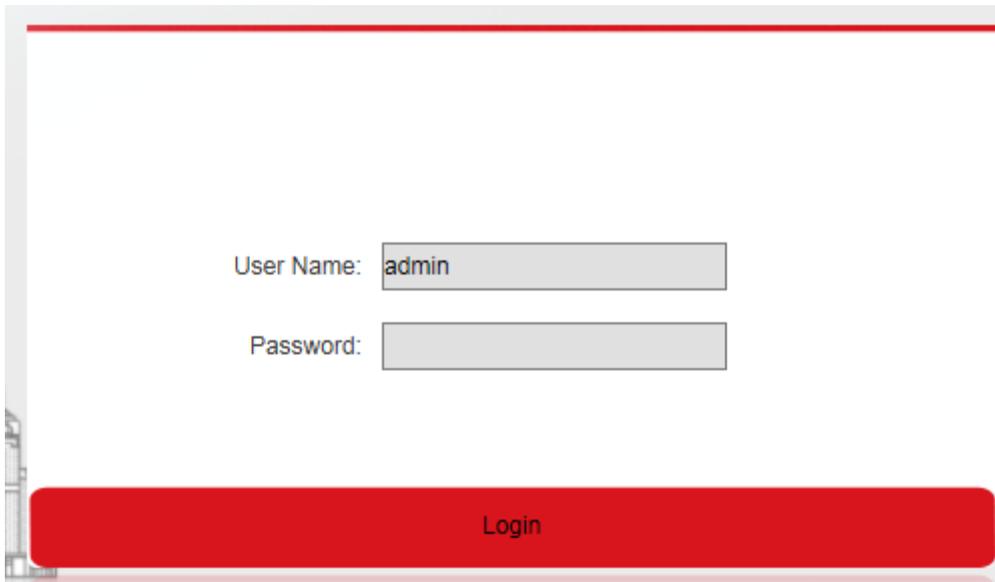


FFC	WG OUT : Orange D0, White D1, Green GND
	WG IN : Brown and white D0, Yellow D1, Gray GND
	ALARM OUT : Brown ALARM+, Purple ALARM
	RS485 : Orange and White 485+, Blue and White 485-
	USB : Red 5V, Blue D-, Green and white D+, Black GND

## Web Browser Settings

### 1 System Login

Open a browser and enter IP address of the access control camera, Default IP address: 192.168.1.88. Default user name: admin, password: admin.

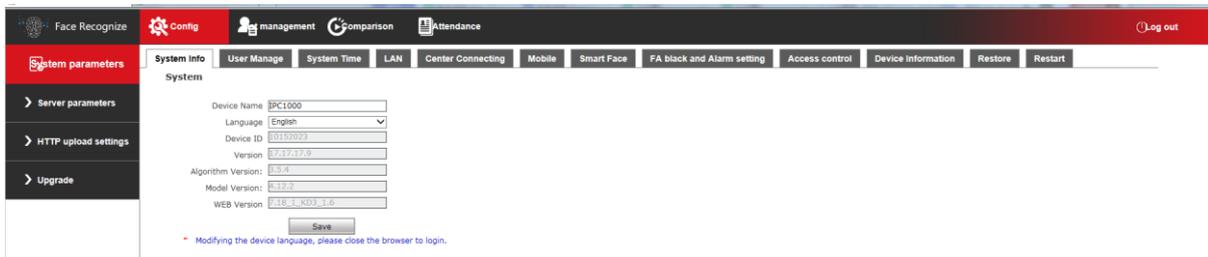


Pic. 1

Remind: Don't forget to change password after log in, and write down the password to avoid forgetting.

### 2 Main Interface

The main interface is shown as Pic. 2:



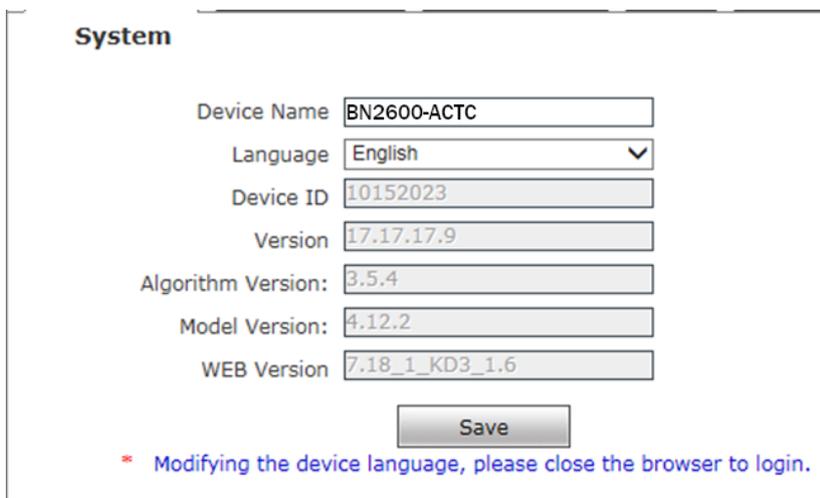
Pic. 2

### 3 Settings

#### 3.1 System Parameter

##### 3.1.1 System Information

The setup interface of system information and basic parameters of the access control camera are shown as Pic. 3.1.1:



**System**

Device Name

Language

Device ID

Version

Algorithm Version:

Model Version:

WEB Version

\* Modifying the device language, please close the browser to login.

Pic. 3.1.1

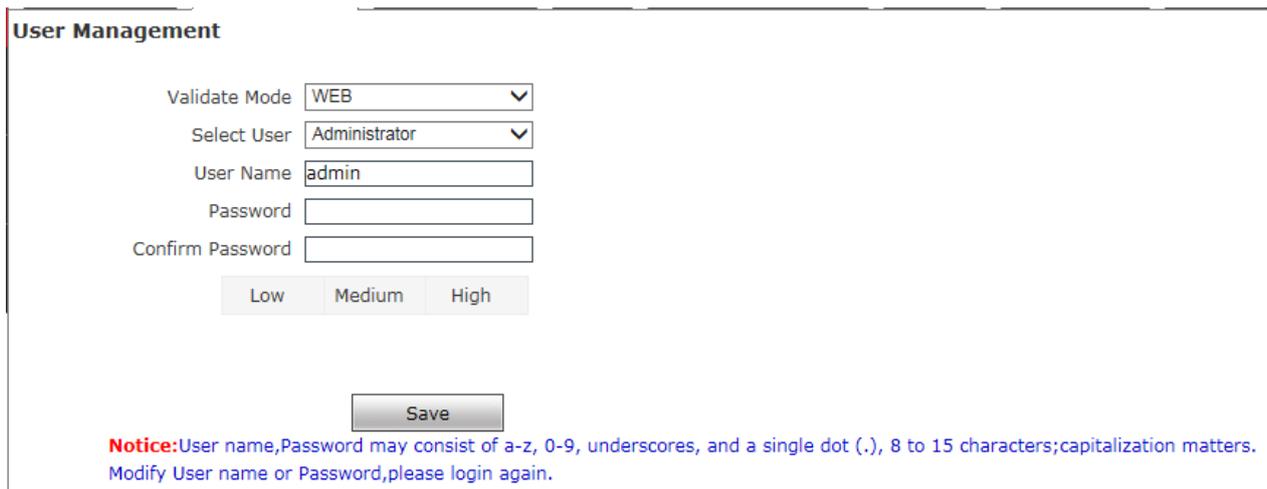
【System information】 Display device name, device number, core version and other information. Device name can be user-defined.

After parameter settings, click on 【Save】 to validate them.

【Device language】 After other languages are selected, close web browser and log in to device again.

### 3.1.2 User Management

The setup interface of user management of the access control camera is shown in Pic. 3.1.2:



**User Management**

Validate Mode

Select User

User Name

Password

Confirm Password

Low  Medium  High

**Notice:** User name, Password may consist of a-z, 0-9, underscores, and a single dot (.), 8 to 15 characters; capitalization matters. Modify User name or Password, please login again.

Pic. 3.1.2

Three users can be set for every access control camera, one is administrator and two are ordinary users.

All functions and parameters of access control camera can be set by three users.

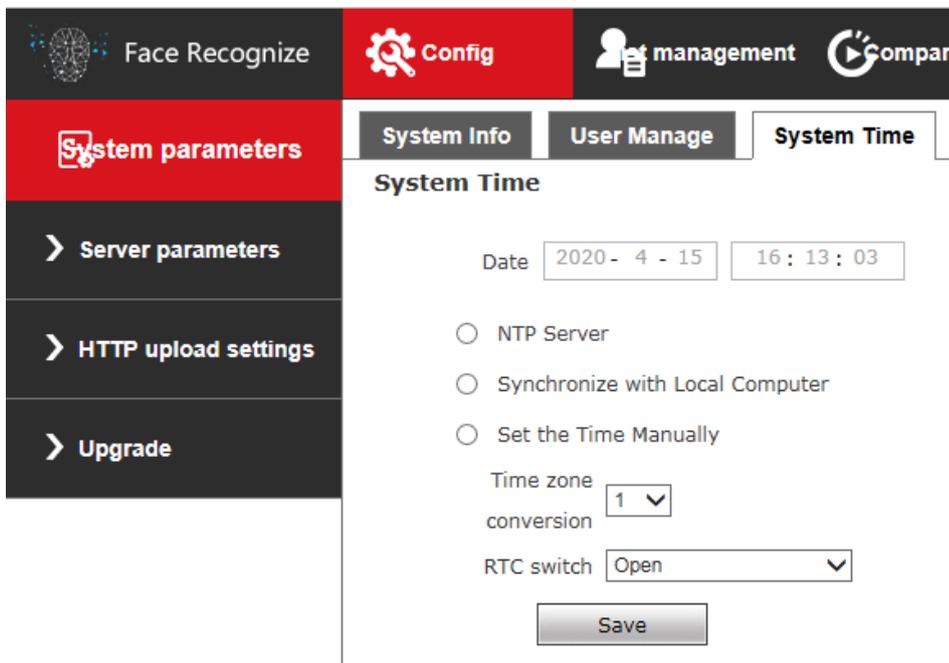
After parameter settings, click on **【Save】** to validate them.



**Important:** Username and password must be a character string with 1-16 characters which consists of letter, figure, underline or point (.). Please pay attention to capital and lower-case form.

### 3.1.3 Time Settings

The time settings of the access control camera is shown in Pic. 3.1.3:



Pic. 3.1.3

**【Current time of device】** Display current date and time of device.

**【Update using time server】** After this function is enabled, the access control camera will check the clock of the access control camera using NTP server at fixed time according to set time zone.

**【Synchronize with local computer】** Click on "Synchronize with local computer" and device date and time will be synchronous with computer date and time.

**【Manual settings】** Click on manual settings to set up device date and time under current time of device.

**【Time zone conversion type】** Time zone definition switch (1/2 is optional)

**【RTC switch】** RTC switch, default: ON.

After parameter settings, click on **【Save】** to validate them.

### 3.1.4 LAN Setting Parameter

The LAN Setting of the access control camera is shown in Pic. 3.1.4:

---

**LAN Setting**

DHCP Enable

IP

Subnet Mask

Gateway

Preferred DNS

Alternate DNS

MAC

Pic. 3.1.4

**【DHCP】** If DHCP function of Router is enabled, after this setting is selected, the access control camera will automatically obtain the IP address from the router.

**【IP address】** Set up IP of the access control camera.

**【Subnet mask】** Default code: 255.255.255.0 (it cannot be modified by client).

**【Gateway】** Set up gateway IP of the access control camera. e.g.: If a device will be connected to a public network through Router, gateway IP should be set as Router IP of the public network.

**【Physical address】** MAC address of access control camera (it cannot be modified by client).

**【DNS address】** DNS address: If DNS is unknown, 8.8.8.8 can be adopted

After parameter settings, click on **【Save】** and restart the device to validate them.



**Note:** After network parameters are modified and saved, the device will be restarted automatically. If the device is used in an LAN, please pay attention to avoid conflict between the IP address and IP address of other devices or computers in the LAN.

### 3.1.6 Mobile P2P

The setup interface of mobile P2P of the access control camera is shown in Pic. 3.1.6:

P2P Server	Port Server
UUID	<input type="text"/>
	
<input type="button" value="Save"/>	

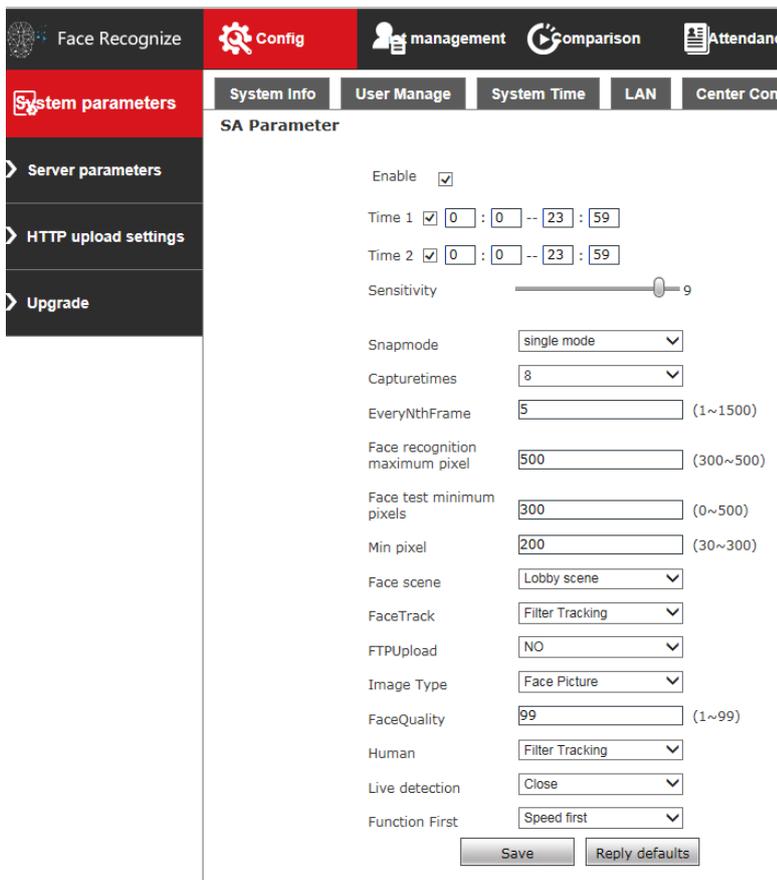
P2P Server	Port Server
Port Server	<input type="text" value="0"/>
<input type="button" value="Save"/>	

Pic. 3.1.6

【P2P service】 Sign of devices of UUID searched by mobile APP in an LAN, or QR code of scanning device, image of devices can be viewed by mobile APP. Mobile apps is “*ikan*”.

### 3.1.7 Face Recognition • Parameter Settings

【Enable】 It is used to enable face recognition algorithm. Face recognition can be conducted and other parameter settings can be validated only when Enable is ticked. It is ON by default.



【Time 1/2】 User can define two periods. To validate it, tick 【Time 1/2】 . Default: Two periods are enabled. Default time: 00 : 00-23 : 59.

Enable

Time 1  0 : 0 -- 23 : 59

Time 2  0 : 0 -- 23 : 59

【Sensitivity】 Setting range: 0-10.

Sensitivity refers to sensitivity of face recognition. When sensitivity is too high, it may snapshot the same face repeatedly or snapshot by mistake. If sensitivity is too low, it might cause miss snapshot. The best sensitivity setting is 3-5.

Sensitivity 

【Capturing mode】 Single mode: Set together with 【Capture times】 and 【Frame interval】 .

Capturetimes 8

EveryNthFrame 5  (1~1500)



**Note:** When many people pass the gate, only the first person (face has the maximum pixel in the screen) is captured. According to set frame interval, a face will be captured at certain frames interval and uploaded to FTP server. Only one face will be displayed in the screen.

【Maximum pixel of face recognition】 Setting range: 300-500. When face pixel in the screen is greater than the set value (maximum pixel of face recognition), face will not be captured.

Face recognition maximum pixel  (300~500)

【Minimum pixel of face temperature measurement】 Setting range: 0-500. When face pixel in the screen is greater than the set value (minimum pixel of face temperature measurement), temperature will not be measured.

Face test minimum pixels  (0~500)

【Minimum pixel of face recognition】 Setting range: 30-300. When face pixel in the screen is greater than the set value (minimum pixel of face recognition), face will not be captured.

Min pixel  (30~300)

【Face scenario】 This parameter is used to adopt different face exposure strategies for different application scenarios. There are two types of application scenarios: Ordinary scenario and lobby scenario. Default: 【Lobby scenario】 .

**Ordinary scenario:** Applicable to conventional environment.

**Lobby scenario:** Applicable to backlight environment.

Face scene

【Face tracking box】 This is set to display the green face tracking frame displayed on the screen when people is close or at the correct distance. It is ON by default.

【 FTP upload】 This parameter is used to set up FTP server to upload human face picture. It is ON by default.

For detailed configuration method, refer to 5.4.7.

FTPUpload

【Picture upload format】 FTP picture can be uploaded in the format of 【Upload face】 or 【Upload face and original picture】 .

【Face picture quality】 Quality of picture uploaded by FTP is 99 by default. The larger the value is the better the picture quality is.

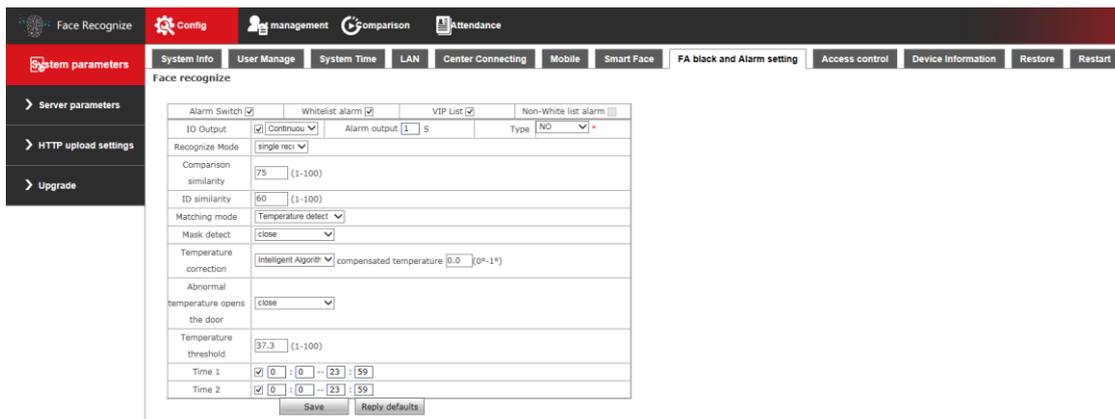
【Human】 It is ON by default.

【Live detection】 Set this On to avoid picture fraud. It is OFF by default.

【Function First】 When choosing speed first, the temperature taking time is quicker, when choosing live first, it detects a living object first before taking temperature. Default: Speed First

### 3.1.8 Face Recognition • Alarm Settings

Alarm of white list and VIP list can be set.



Pic. 3.1.8-1

【Alarm switch】 ON or OFF is optional (it is ON by default)

【Alarm of white list and VIP list】 ON or OFF is optional. White List and VIP list alarm (it is ON by default)

【IO output】 IO output type is optional (continuous output is selected by default)

【Alarm output duration】 Select output alarm duration

【IO output type】 IO output NO or NC is optional (it is NO by default)

【Recognition mode】 Select mode of access control camera (it is single face recognition by default)

**Face recognize**

Alarm Switch <input checked="" type="checkbox"/>	Whitelist alarm <input checked="" type="checkbox"/>	VIP List <input checked="" type="checkbox"/>	Non-White list alarm <input type="checkbox"/>
IO Output	Numbers recognize mode Always identify. Single recognize mode	output <input type="text" value="1"/> S	Type <input type="text" value="NO"/> *
Recognize Mode			
Comparison similarity	<input type="text" value="75"/> (1-100)		
ID similarity	<input type="text" value="60"/> (1-100)		
Matching mode	<input type="text" value="Temperature detect"/>		
Mask detect	<input type="text" value="close"/>		
Temperature correction	<input type="text" value="Intelligent Algorithm"/> compensated temperature <input type="text" value="0.0"/> (0°-1°)		
Abnormal temperature opens the door	<input type="text" value="close"/>		
Temperature threshold	<input type="text" value="37.3"/> (1-100)		
Time 1	<input checked="" type="checkbox"/> <input type="text" value="0"/> : <input type="text" value="0"/> -- <input type="text" value="23"/> : <input type="text" value="59"/>		
Time 2	<input checked="" type="checkbox"/> <input type="text" value="0"/> : <input type="text" value="0"/> -- <input type="text" value="23"/> : <input type="text" value="59"/>		
<input type="button" value="Save"/>		<input type="button" value="Reply defaults"/>	

Pic. 3.1.8-2

**【Numbers recognition mode】** If face picture is not matched in the list within the set recognition times (e.g.: set times recognition value is 5 and face is matched within 5 times of capturing, contrast information will be displayed and recognition will be stopped. If face is not matched after 5 times of recognition, recognition will be stopped and recognition failed) (Only when recognition mode is times recognition).

**【Single face recognition】** Take face picture one times only, if it match the list information, it will display in the contrast information, if not, then stopped and recognition failed. (Single face recognition is recommended for access control camera)

**【Always Identifying】** Will always match the list information till the recognition success.

**【Contrast similarity】** Select similarity of face contrast. If the set contrast similarity is too low, error may occur (contrast similarity is 75 by default)

**【ID Card similarity】** Select ID Card contrast similarity. If the set contrast similarity is too low, error may occur (contrast similarity is 60 by default)

**【Matching mode】** Select contrast mode of access control camera from face recognition, temperature detection, face + temperature detection, ID Card + face + temperature, ID Card + face, ID Card or white list + temperature and ID Card or white list. Matching mode is temperature detection by default.

**Temp, Face Recog & Alarm Setting**

Alarm Switch <input checked="" type="checkbox"/>	Whitelist alarm <input checked="" type="checkbox"/>	VIP List <input checked="" type="checkbox"/>	Non-White list alarm <input type="checkbox"/>
IO Output <input checked="" type="checkbox"/> Continouu	Alarm output 1 s	Type Yes*	
Face Recog Mode	Recognize		
Min. Similarity	75 (1-100)		
ID similarity	<ul style="list-style-type: none"> <li>Face detect</li> <li>Temperature detect</li> <li>Face detect + Temperature detect</li> <li>ID + face + temperature</li> <li>ID + face</li> <li>ID card or whitelist + temperature</li> <li>ID card or whitelist</li> <li>IC card recognition</li> <li>IC card or face recognition</li> </ul>		
Mask Detection			
Temperature Calibration	ed temperature 0.0		
Abnormal temperature opens the door	close		
Temperature threshold	37.3 (1-100)		
Temperature unit	Celsius		
Time period without temperature measurement	0 : 0 -- 23 : 59		

Pic. 3.1.8-3

**【Mask detection】** Open or Close is optional. It is OFF by default (note: If mask detection is OFF, the mask status on record is always NO).

**【Temperature correction】** Intelligent algorithm and low/high temperature algorithm. Under intelligent algorithm mode, compensation temperature can be set. After that, increase the set compensation temperature after temperature is measured each time; low/high temperature algorithm means to convert unreasonable body temperature value into normal body temperature automatically under extreme low or high temperature.

**【Abnormal temperature opens the door】** Open or Close is optional in case of high temperature alarm. It is Close by default. If it is set as Open, even high temperature will still opens the door.

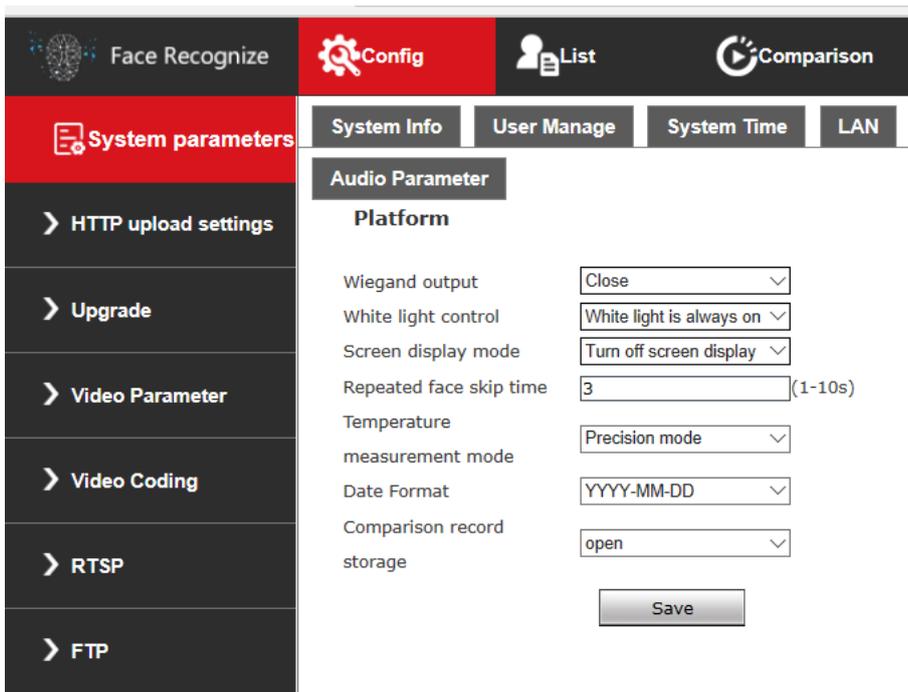
**【Temperature threshold】** Temperature threshold can be set. If temperature exceeds the threshold when contrast mode includes temperature detection, an alarm will be given. Temperature threshold is 37.3 by default.

**【Temperature unit】** Celsius or Fahrenheit can be set, when set as Fahrenheit, default temperature threshold will be changed to 99.1

**【Time period without temperature measurement】** Specific period of time can be set as the temperature measurement is not enabled.

**3.1.9 Face Recognition • Access Control**

Set up related information of access control; Wiegand output control, white light control, same face filtration and screen display mode can be set;



Pic. 3.1.9-1

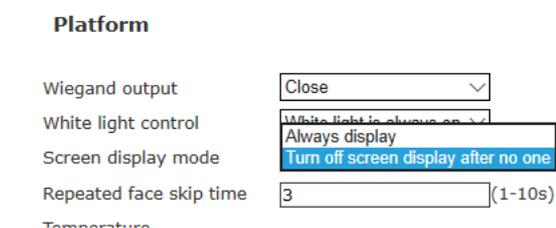
Wiegand output: it can set up Wiegand output off, or turn on Wiegand output, Wiegand 26 or Wiegand 34 is optional; Wiegand output is activated only when face is recognized. Temperature detection mode only will not activate Wiegand output.

White light control: Can set white light always ON or OFF, or set a time schedule, or when screen backlight is off, it will be off when no motion is detected. Default: White light is normally on.



Pic. 3.1.9-3

Screen display mode: Can set the screen display always ON or screen display closed when there is nobody. Default: Screen display is closed within 10s if there is nobody.



Pic. 3.1.9-4

Repeated face skip time: It is to set the same face filtration time of the same list, it is 3s by default.

Temperature measurement mode	<input type="text" value="Precision mode"/> <input type="text" value="Quick mode"/>
Date Format	<input type="text" value="YYYY-MM-DD"/>
Comparison record storage	<input type="text" value="open"/>
<input type="button" value="Save"/>	

Temperature measurement mode, can be selected as precision mode or quick mode, quick mode is selected when there are many visitors in the application field and fast pass is priority.

Comparison record storage can be selected as close, in case some application needs protection of privacy and will not allow to store the comparison records. Default setting is open.

### 3.1.10 Device Information

---

#### Device Info.

Device IP	<input type="text"/>
direction	<input type="text"/>
longitude	<input type="text"/>
Dimension	<input type="text"/>
Manufacturer code	<input type="text"/>
<input type="button" value="Save"/>	

Pic. 3.1.10

It is used to display current device information.

### 3.1.11 Factory Reset

The setup interface of factory reset of the access control camera is shown in Pic. 3.1.11:

## Restore

\* Click this button will make the Device to recover all set the default state.



Pic. 3.1.11

Click on **【Restore factory settings】** and enter a password according to prompt message to restart the device and restore factory settings.

**【Network】** Tick to restore default network parameters. It is 192.168.1.88 by default.

**【User name】** Tick to restore default user name and password. It is admin/admin by default.

### 3.1.12 Device Restart

The setup interface of device restart of the access control camera is shown in Pic. 3.1.12:

## Reboot

### Restart The System Automatically

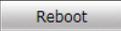
Daily  At 02:00

### Restart The System Manually



Pic. 3.1.12

**【Automatic system restart】** Select a time to restart the device automatically.

**【Manual system restart】** Click  to enter a password according to prompt message to restart the device.

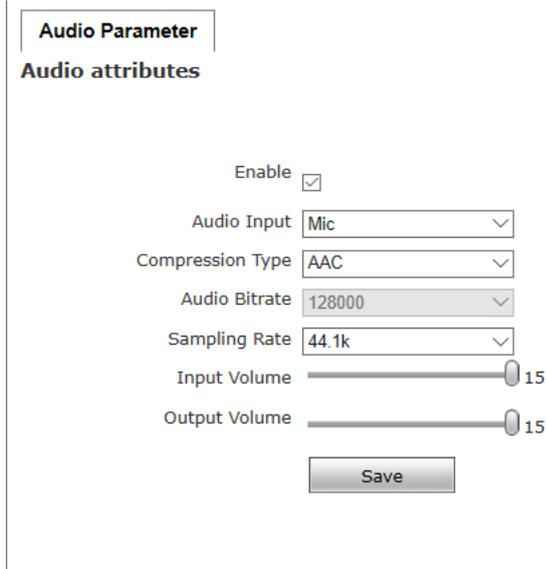
### 3.1.13 Device Setting

#### Device Setting

Choose	No.	TotalSize(M)	FreeSize(M)	Status
<input checked="" type="radio"/>	1 HSD	14800	13690	formatted

Format the EMMC of device will cause the records and list information deleted.

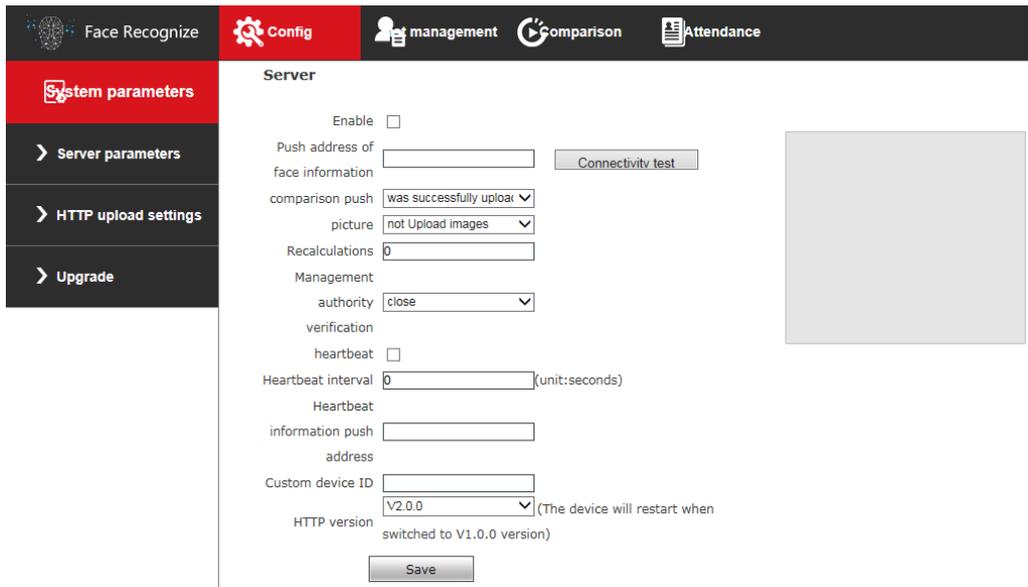
### 3.1.14 Audio Parameters.



Input and output Volume can be adjusted here.

### 3.2 Server Parameter

Set up relevant server parameters in the menu, as shown in Pic. 3.2 (picture version is HTTP version V1.1.14 by default. HTTP version can be modified according to actual need. The device will be restarted after modification).



Pic. 3.2

【Enable】 Switch of face push server.

【Face information push address】 Server address receiving face information. Fill in it and click on the right connectivity test to display the result in the right box.

【Contrast push】 Control of upload contrast result type among successful contrast upload, all people upload, blacklist upload, whitelist upload, VIP list upload, stranger upload and non-whitelist upload. It is successful contrast upload by default.

【Picture】 Picture upload is optional among no picture upload, face picture upload and face and original picture upload.

【Re-upload times】 Re-upload times when contrast record is not uploaded successfully. It is 0 by default

【Management permission verification】 Whether management permission verification is enabled. If is disabled by default.

【Heartbeat】 Switch for whether to upload heartbeat information.

【Heartbeat information interval】 Heartbeat interval time, unit: Second.

【Heartbeat information push address】 Server address receiving heartbeat information.

【User-defined device ID】 Device ID, device number can be viewed in system information.

【HTTP version】 HTTP version can be modified according to actual need and the device will be restarted after modification.

After parameter settings, click on 【Save】 to validate them.

### 3.3 HTTP Upload Settings

When HTTP transmission mode is adopted for servers relating to the access control camera, set up relevant server parameters in the menu, as shown in Pic. 3.3 (picture version is HTTP version V1.1.14 by default. HTTP version can be modified according to actual need. The device will be restarted after modification).

Pic. 3.3

【Capture and upload】 Capture the switch uploaded.

【Capture information upload address】 Server address receiving capture information.

【Contrast upload type】 Control of upload contrast result type among successful contrast upload, all people upload, blacklist upload, whitelist upload, VIP list upload, stranger upload and non-whitelist upload. It is successful contrast upload by default.

【Capture information content】 FaceInfo and CompareInfo are optional. Both should be selected as suggested.

【Picture upload】 Picture upload is optional among face picture, background picture and list picture.

【Re-upload times】 Re-upload times when contrast record is not uploaded successfully. It is 0 by default.

【Registration】 Switch for whether to upload registration information.

【Registration information upload address】 Server address receiving registration information.

【Heartbeat upload】 Switch for whether to upload heartbeat information.

【Heartbeat information upload address】 Server address receiving heartbeat information.

【Heartbeat interval】 Heartbeat interval time, unit: Second.

【Instruction address acquisition】 Address for acquiring instructions.

【Instruction acquisition interval (s)】 Time interval for acquiring instructions, unit: Second.

【Active address acquisition address】 Address for actively acquiring tasks.

【Task result report address】 Address for reporting task result.

【Sign verification】 Sign verification ON/OFF. Default: OFF.

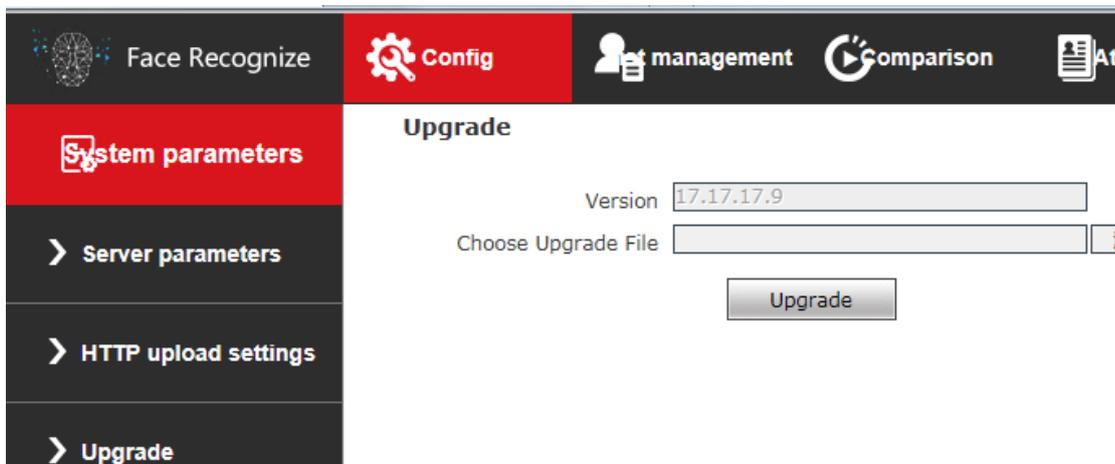
【Operation mode】 Offline mode and online mode are optional. Default: Offline mode.

【HTTP version】 HTTP version can be modified according to actual need and the device will be restarted after modification.

After parameter settings, click on 【Save】 to validate them.

### 3.4 Software Upgrade

The software upgrade interface of the access control camera is shown in Pic. 3.4:



Pic. 3.4

【Upgrade】 Click on “Browse” to select a correct upgrade file (core file, suffix is .uot) and click on "Upgrade" for upgrade. Percentage will be displayed in this process and the access control camera will be restarted automatically after upgrade. Log in to the device again, enter the software upgrade page and check whether core version is the version upgraded.



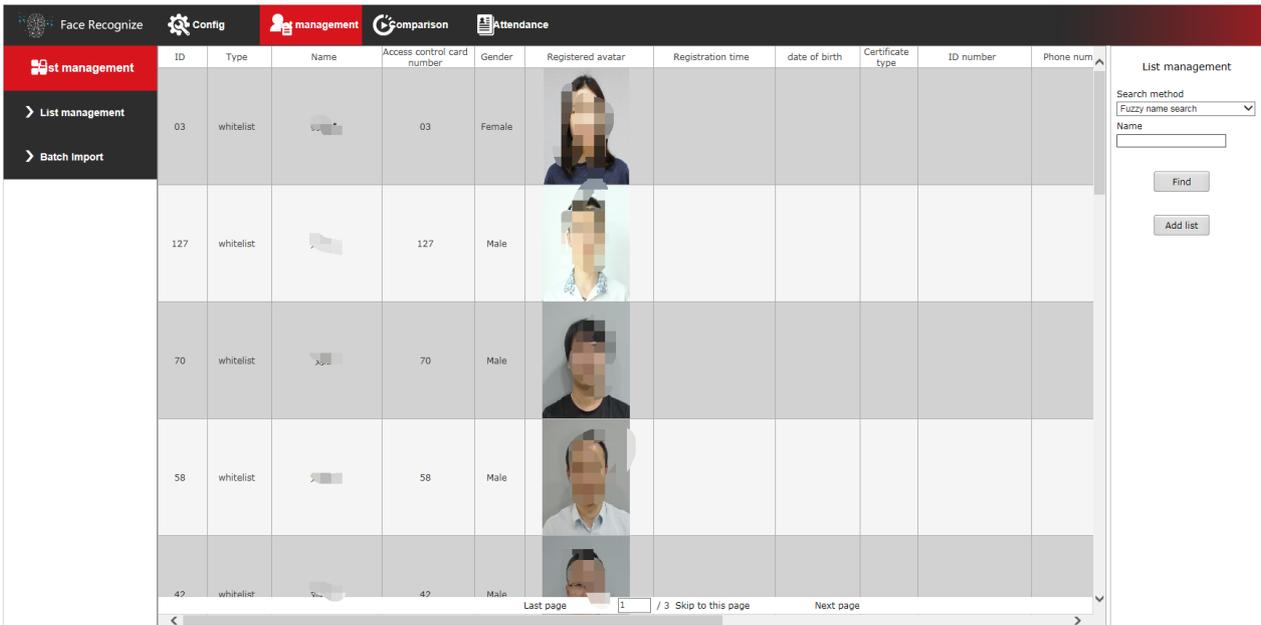
**Important:**

- 1、 Please ensure power and network of the access control camera are not cut off in the upgrade process.
- 2、 For Windows7 system users, please set up IE parameters according to prompt message below before upgrade; otherwise, a prompt message that percentage of upgrade will not be displayed normally may be given. Steps: Open IE browser-tool-Internet option-safety-user-defined level-other-local directory path is included when file is uploaded to server-enable

## 4 List Management

### 4.1 List Management

The face library added can be searched and white list can be added to the library in different ways



Pic. 4.1-1

#### 1. Face list is searched in different ways

**【Condition search】** Carry out accurate search through start time, finish time, list type, sex, age and access card number.

**【Fuzzy search of name】** Carry out fuzzy search of name using the name input box below.

**【Repeated ID number search】** Carry out search according to repeated ID number.

**【Repeated access card number search】** Carry out search according to repeated access card number.

#### 2. Add white list by **【Add list】** as follows



Pic. 4.1-2

Step 1: Click on Add list

Step 2: Click on Browse and select a picture to be imported according to storage path

Step 3: Select access card number generation method among public card number, automatic generation and manual input.

Step 3: Input picture name, ID number and other related information.

Step 4: Click on Save



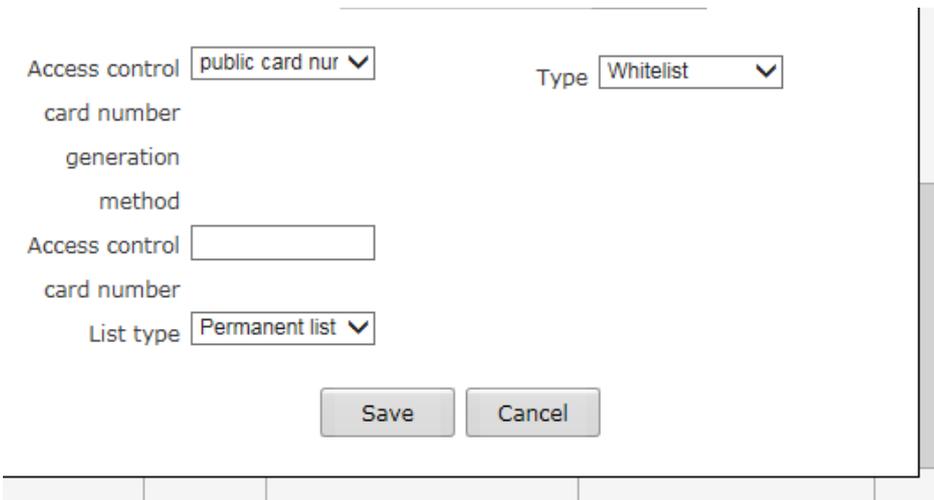
**Note: Picture name and numbering rule: Picture number cannot be repeated**

## 4.2 Batch import

Batch import can be used to refresh list and import white list and VIP list by batches



Pic. 4.2-1



Pic. 4.2-2

Step 1: Click on Batch import

Step 2: Click on Browse and select a picture to be imported according to storage path

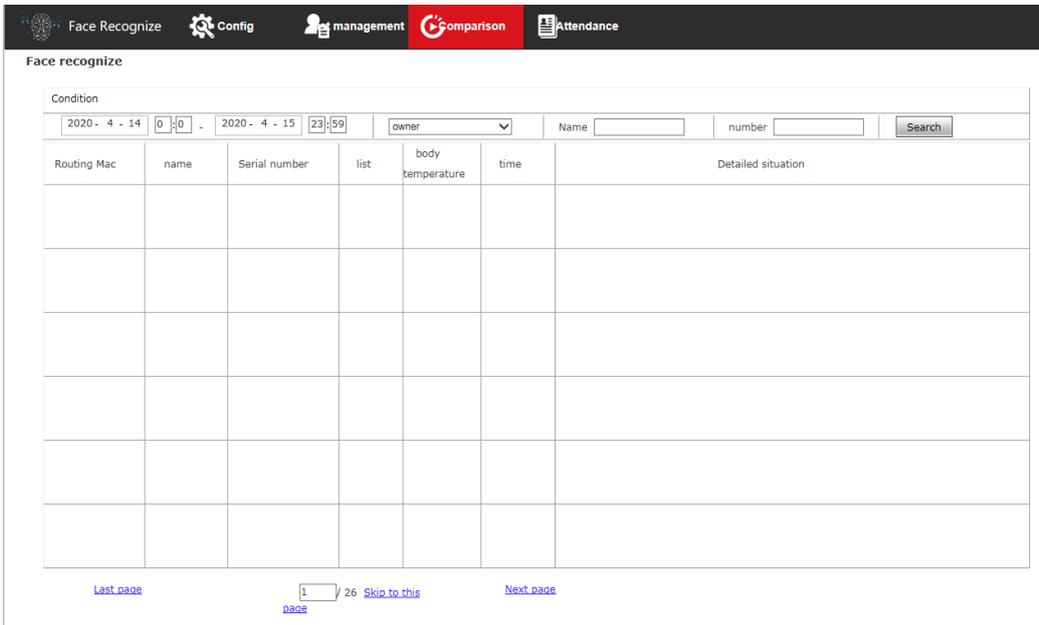
Step 3: Select access card number generation method among public card number, automatic generation and manual input.

Step 3: Select type of list to be imported

Step 4: Click on Save

## 5 Contrast Record

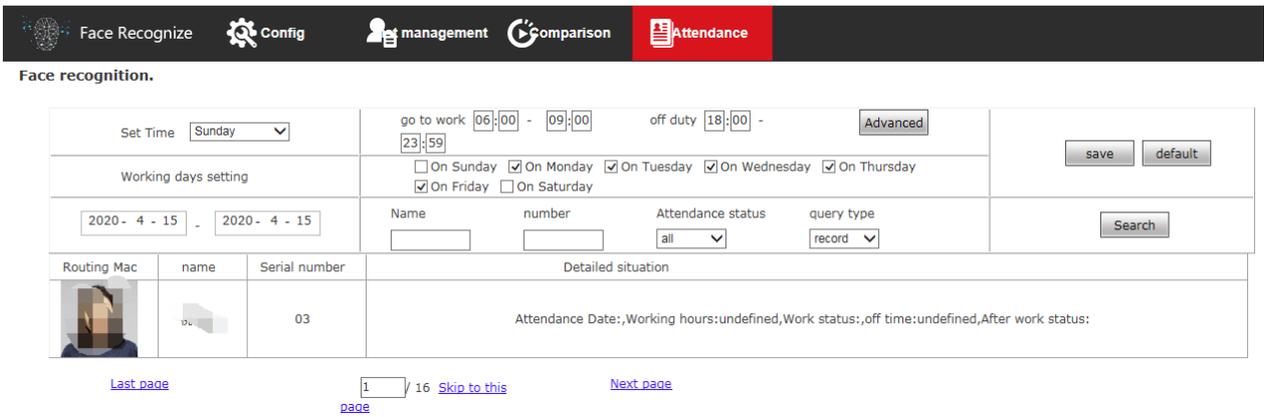
Contrast record list includes head portrait (existing picture or stranger's on-site picture), name, number, list, body temperature, time and details. Details include similarity, visit times, first visit time, mask use condition and body temperature detection result (details of stranger just include mask use condition and body temperature detection result). The latest 10000 contrast records can be queried according to time, list type, name, number and other query conditions.



Pic. 5

## 6 Attendance Record

Attendance record of any day or any period can be queried



Pic. 6

1. Time and workday settings, any period of a day can be set as attendance time and any time of a week can be set as workday

2. Query condition:

1. Period query: Enter any period to query attendance record of the designated period

2. Attendance query: Select any state to query attendance record of the designated state

3. Name and number query: Enter name and number of any existing person to query name and number of the designated person

## Appendix 1 Network port occupied by IP camera

The access control camera occupies the following network ports by default:

TCP	80	Web port
	5000	Communication port, AV(audio/video) data transmission port, talkback data transmission port
UDP	5000	AV(audio/video) data transmission port
Multicast port	Multicast initial port + channel number	
ONVIF	2000	

## Appendix 2 Frequently Asked Questions

### 1. What if the access control camera cannot be visited by IE browser?

Possible cause 1: Network is blocked?

**Solution:** Connect network using PC to test whether network is connected. First, eliminate cable failure, power failure and network failure arising from PC virus until Ping can be connected using PC.

Possible cause 2: IP address is occupied by other devices?

**Solution:** Disconnect access control camera and network, connect access control camera and PC and log in to the access control camera to modify IP address.

Possible cause 3: IP address is in a different subnet?

**Solution:** Check settings of server IP address, subnet mask address and gateway and add IP to server network segment as IP Camera.

Possible cause 4: Physical address in the network conflicts with the access control camera?

**Solution:** Modify physical address of the access control camera.

Possible cause 5: Web port has been modified?

**Solution:** Contact network administrator to acquire corresponding port information.

### 2、 Device cannot be upgraded by IE?

Possible cause 1: Safety level of IE is too high

**Solution:** Change IE permission, IE tool->Internet option->safety->user-defined level. In other options, local directory path is included when file can be uploaded, as shown below:

Possible cause 2: The device is being upgraded, but progress is not displayed

**Solution:** Controls mismatch IE page and consequently progress is not displayed. Re-download and install controls. For installation process, refer to the User Manual.

### 3、 Device Search and sVMS search software cannot search the device

Possible cause 1: Whereas Device Search and CMS software searches device network information across network segment using multicast protocol; while firewall does not allow pass of multicast data package, so device network information cannot be searched.

**Solution:** Close firewall.

Possible cause 2: Device and server are not in the same LAN

**Solution:** Detect network and ensure device and server are in the same LAN

### 4、 Log in to the device, but no parameters can be modified

Possible cause: Other people than administrator log in to the device

**Solution:** Please log in to the device using administrator permission

### 5. What if password is forgotten?

**Solution:** Search the device using special reset tools and select the device of which password is forgotten. The device will restore factory settings by "Factory reset". Default IP: 192.168.1.88 Default username and password: admin/admin

### 6. After device is successfully upgraded, log in to the device again and abnormalities are displayed in the IE interface.

Possible cause: IE layout is changed, cache data is called while logging in to the device again and consequently layout is abnormal

**Solution:** Open the browser, click on "Tool", select "Internet option" and click on "Delete file" in "Internet temporary file" to delete ID cache.

### 8. Body temperature value is not displayed in the interface

Possible cause: Recognition mode is set as face recognition

**Solution:** Change mode to temperature detection or face + temperature detection

### 9. The measured temperature is inaccurate

Possible cause: The environment temperature has not been calibrated before startup

**Solution:** Re-plug the power to start the device and ensure there are no people, obstacles and heat sources in front of the device before startup

**10. Only captured pictures are displayed in the interface**

Possible cause: Recognition mode is set as temperature detection

**Solution:** Change recognition mode into face recognition or face + temperature detection

**11. Partial voices (such as please wear a mask; temperature measurement fails, please re-measure the temperature) are played more than once**

Possible cause: Abnormal face picture (e.g.: Mask is not worn, face whose measured temperature is lower than 34°C) is captured several times

**Solution:** Wait patiently until voice broadcast is completed, stop mask detection or effectively detect body temperature once.

**12. After the same person is contrasted or temperature is measured, return to the interface, record disappears, and recognition and detection still fail**

Possible cause: Face ID is not refreshed

**Solution:** Exit and reenter

**13. There is no face mark or face box**

Possible cause: It is too far or too close and not consistent with minimum pixel or maximum pixel of face recognition

**Solution:** Adjust the standing position or minimum pixel or maximum pixel of face recognition

## II . Common Problems of Backend Connection

1. Connect to NVR through ONVIF protocol, time is not correct

Possible cause 1: ONVIF protocol of NVR is different from ONVIF protocol of ONVIF

**Solution:** Log in to camera web, enter Settings->System parameter->Time settings and switch time zone conversion type into 2

Because onvif protocol of NVR or platform is different. There are two types of time zone now and most manufacturers adopt type 1, such as HiKvision, Dahua, XM and TVT; while some manufacturers adopt type 2, such as TIANDY and some Taiwanese manufacturers.

## 二、 How to calculate video capacity

**Calculation method:** R is capacity of hardware needed, B is code rate, N is number of video channels and D is number of days of video.

Size of video file per hour of single-path image:  $R = B \div 8 \div 1000 \times 3600$

Size of video file per day (24h) of N-path image:  $R = B \div 8 \div 1000 \times 3600 \times 24 \times N$

Size of video file per D days of N-path image:  $R = B \div 8 \div 1000 \times 3600 \times 24 \times D \times N$

General H.264 coder and decoder, storage capacity of 24h video of 1 million pixel camera is about 13G, that of 1.3 million pixel camera is about 17G and that of 2 million pixel camera is about 23G.

Storage capacity of several types of common code streams

Code stream value (kb/s)	Storage capacity (G/day)
2048	21
4096	42
6144	63



**Important:**

**Enable DirectDraw acceleration, Direct3D acceleration and AGP texturing speed functions of DirectX function. If such functions cannot be enabled, it means that DirectX is not installed correctly or hardware is not supported.**