

# **Face Recognition & Temperature Measurement Access Control Attendance Panel User Manual (For Windows XP/2003/Win7/Vista/Win 8/Win 10)**

Version: V1.0

The User Manual is applicable to face recognition & temperature measurement access control attendance panel

# Introduction

Thank you for using our face recognition temperature-measurement access control attendance panel products. This series of products are access control attendance panel products that can recognize human face and measure human body temperature and are developed specifically for network video surveillance. Through high-precision infrared temperature detection and combined with such intelligent access control and attendance functions as face and ID recognition, this product realizes contactless rapid detection, registration and record of human body temperature and is widely applicable to crowded places such as office area, hotel, passage gate, office building, school, shopping mall, community and public service and management project.

## Statement:

- The User Manual may differ from the version you use. In case of problems, which you cannot solve as per the User Manual while using this product, please contact the Technical Support Department or supplier.
- The User Manual will be updated irregularly without prior notice.

## Reader:

The User Manual is mainly suitable for the following personnel:

- System planner
- On-site technical support and maintenance personnel
- Person responsible for system installation, configuration and maintenance
- User of this product

## Definition:

- The access control attendance panel mentioned in the User Manual is face recognition & temperature measurement access control attendance panel .
  - Click: Click using left mouse button.
  - Double click: Double click using left mouse button.
  - Items with a square bracket “ **[ ]** ” represent window name, menu name and data sheet, such as
-

## Revision History:

Revision history is used to record events relating to update of the User Manual. The latest version of the User Manual includes contents of all versions updated.

Revision date	Version	Description
April 14, 2020	V1.0	Available for ten languages

# Contents

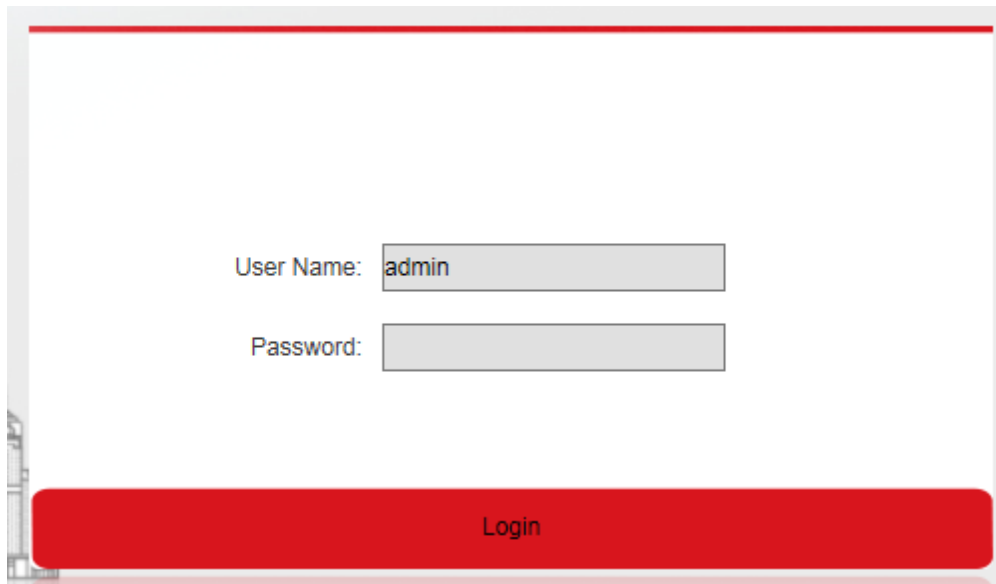
1 System Login.....	5
2 Main Interface .....	5
3 Settings .....	6
3.1 System Parameter .....	6
3.1.1 System Information .....	6
3.1.2 User Management.....	6
3.1.3 Time Settings .....	7
3.1.4 Wired Network Parameter .....	8
3.1.5 Center Link.....	9
3.1.6 Mobile Surveillance.....	10
3.1.7 Face Recognition• Parameter Settings.....	11
3.1.8 Face Recognition• Alarm Settings.....	14
3.1.9 Face Recognition• Access Control.....	17
3.1.10 Face Recognition• Equipment Information .....	18
3.1.11 Factory Reset .....	19
3.1.12 Device Restart.....	19
3.2 Server Parameter .....	20
3.3 HTTP Upload Settings.....	21
3.4 Software Upgrade.....	23
<b>4 List Management .....</b>	<b>24</b>
4.1 List Management.....	24
4.2 Batch import .....	25
5 Contrast Record.....	26
6 Attendance Record.....	26
Appendix 1 Network port occupied by IP camera.....	28
Appendix 2 Default network parameter .....	28
Appendix 3 Frequently Asked Questions .....	28

---

# 1 System Login

Open a browser (Internet Explorer) and enter IP address of the access control attendance panel . e.g.:

Default address of device: 192.168.1.88. While logging in to the page for the first time, enter a username and a password (default username: admin, password: admin), as shown in Fig. 1.



User Name: admin

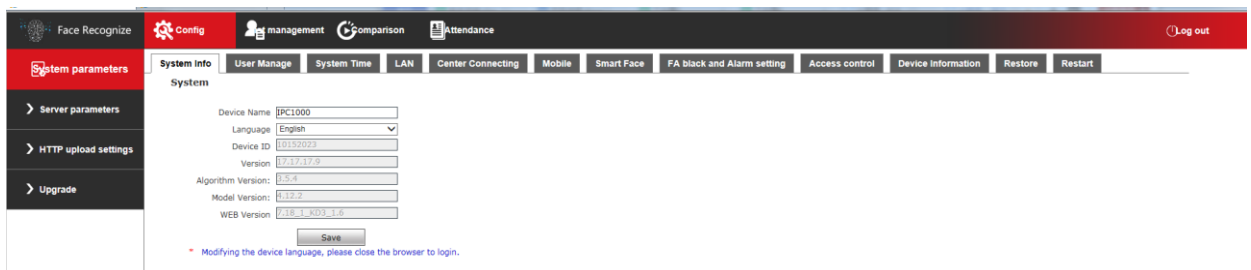
Password:

Login

Fig. 1

# 2 Main Interface

The main interface is shown in Fig. 2:



Face Recognize Config management Comparison Attendance Log out

System parameters System info User Manage System Time LAN Center Connecting Mobile Smart Face FA black and Alarm setting Access control Device Information Restore Restart

System

Device Name: BPC1000

Language: English

Device ID: 00152023

Version: V1.17.17.9

Algorithm Version: V5.4

Model Version: V1.12.2

WEB Version: V1.18.1, 800, 1.6

Save

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

Fig. 2

## 3 Settings

### 3.1 System Parameter

#### 3.1.1 System Information

he setup interface of system information and basic parameters of system parameters of the access control attendnace panel are shown in Fig. 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.

Fig. 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 IE and log in to device again.

#### 3.1.2 User Management

The setup interface of user management of the access control attendnace panel is shown in Fig. 3.1.2:

**User Management**

Validate Mode

Select User

User Name

Password

Confirm Password

**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.

Fig. 3.1.2

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

Administrator permission: All functions and parameters of access control attendance panel can be set.

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 setup interface of user management of the access control attendance panel is shown in Fig. 3.1.3:

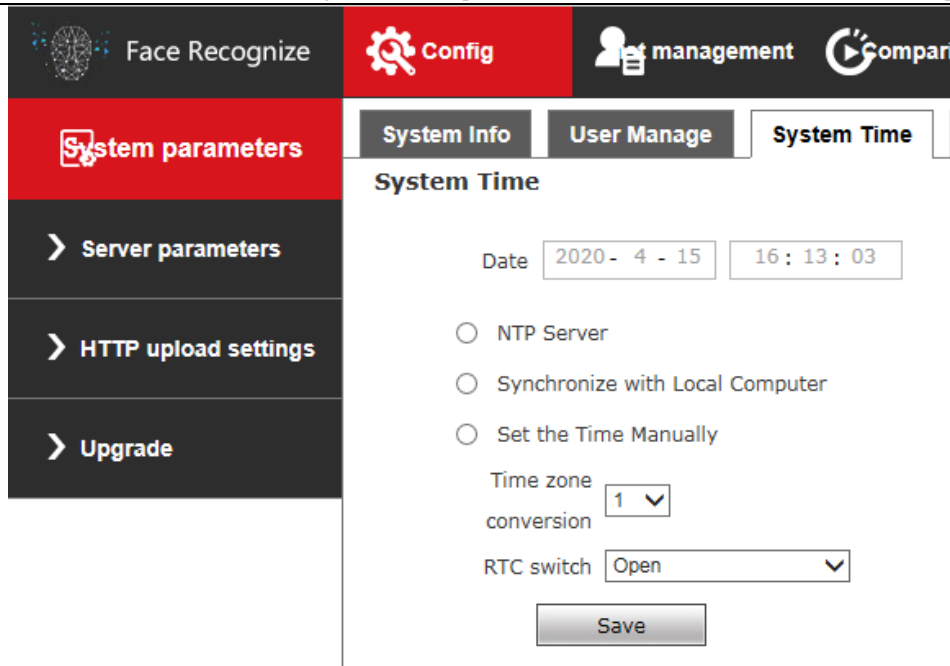


Fig. 3.1.3

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

**【Update using time server】** After this function is enabled, the access control attendance panel will check the clock of the access control attendance panel 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 Wired Network Parameter

The setup interface of wired network parameters of the access control attendance panel is shown in Fig. 3.1.4:



## LAN Setting

DHCP Enable	<input type="checkbox"/>
IP	<input type="text" value="128 . 128 . 60 . 136"/>
Subnet Mask	<input type="text" value="255 . 255 . 0 . 0"/>
Gateway	<input type="text" value="128 . 128 . 1 . 1"/>
Preferred DNS	<input type="text" value="202 . 96 . 134 . 133"/>
Alternate DNS	<input type="text" value="8 . 8 . 8 . 8"/>
MAC	<input type="text" value="00-11-04-02-32-b6"/> <input type="checkbox"/>
<input type="button" value="Save"/>	

Fig. 3.1.4

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

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

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

**【Gateway】** Set up gateway IP of the access control attendnace panel . 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 attendnace panel (it cannot be modified by client).

**【DNS address】** DNS address: Default DNS address of device is DNS address in Guangdong. If DNS is unknown, 8.8.8.8 can be adopted

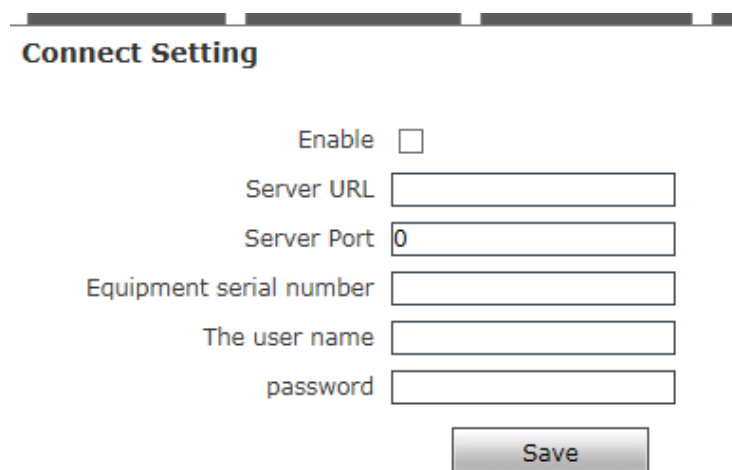
After parameter settings, click on **【Save】** and restart the device to validate them.



**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 preventing conflict between the IP address and IP address of other devices or computers in the LAN.

### 3.1.5 Center Link

The access control attendnace panel is connected to the center through private protocol and the setup



The image shows a web form titled "Connect Setting" with a decorative header bar. The form contains the following elements:

- An "Enable" checkbox, which is currently unchecked.
- A "Server URL" text input field.
- A "Server Port" text input field containing the value "0".
- An "Equipment serial number" text input field.
- A "The user name" text input field.
- A "password" text input field.
- A "Save" button located at the bottom right of the form.

Fig. 3.1.5

**【Switch】** Whether the device is started and connected to the surveillance center;

**【Server address】** Address of the center platform (e.g.: 192.168.55.89).

**【Server port】** Port of the center platform (e.g.: 6000).

**【Device serial No.】** Sign of devices of the center that the access control attendance panel log in to, user-defined.

**【Username】** Login name of center platform.

**【Password】** Password of the center platform.

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

### 3.1.6 Mobile P2P


The setup interface of mobile P2P of the access control attendance panel is shown in Fig. 3.1.6:

P2P Server

Port Server

UUID

un. 0x



Save

P2P Server

Port Server

Port Server

0

Save

Fig. 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 app is “*ikan*”.

### 3.1.7 Face Recognition• Parameter Settings

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

【Deployment period】 It is deployment time and user can define two periods. To validate it, tick 【Deployment period】 . 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. The higher sensitivity is the lower missing report rate is and the higher the probability of re-capturing and accidental capturing is. The lower sensitivity is the higher capturing rate is. However, missing capturing will be caused if sensitivity is too low. Generally, the best effect can be achieved when sensitivity is 3-5.

Sensitivity

【Capturing mode】 Single mode: Used cooperatively with 【Capturing times】 and 【Frame interval】 .

Captures times

EveryNthFrame  (1~1500)



**Note:** Gate of trial site. 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 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.

min pixel   
Face scene

【Face tracking box】 This parameter is used for superposition of face tracking boxes. 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.

FTPUUpload

face and original picture】.

better the picture quality is.

Face Recognize
 Config
 Management
 Comparison
 Attendance

System parameters

Server parameters  
 HTTP upload settings  
 Upgrade

System Info
 User Manager
 System Time
 LAN
 Center Connecting
 Mobile
 Smart Face
 FA black and Alarm setting
 Access control
 Device Information
 Restore
 Restart

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"/>
ID Output	<input checked="" type="checkbox"/> Continues	Alarm output	1 s	Type	NO		
Recognize Mode	single rec						
Comparison similarity	75 (1-100)						
ID similarity	60 (1-100)						
Matching mode	Temperature detect						
Mask detect	close						
Temperature correction	Intelligent Algorithm compensated temperature 0.0 (0~1*)						
Abnormal temperature opens the door	close						
Temperature threshold	37.3 (1-100)						
Time 1	<input checked="" type="checkbox"/> 0 : 0 ~ 23 : 59						
Time 2	<input checked="" type="checkbox"/> 0 : 0 ~ 23 : 59						

Save
 Reply defaults

Fig. 3.1.8-1

**Table 1** The number of cases by age group and sex

[illegible]
$$\frac{1}{\sqrt{\pi}} \int_0^y \frac{e^{-t^2}}{t} dt = -\frac{1}{\sqrt{\pi}} \ln y + O(1) \quad \text{as } y \rightarrow 0.$$

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	1	S	Type	NO
Recognize Mode							
Comparison similarity	75 (1-100)						
ID similarity	60 (1-100)						
Matching mode	Temperature detect						
Mask detect	close						
Temperature correction	Intelligent Algorithm compensated temperature 0.0 (0°-1°)						
Abnormal temperature opens the door	close						
Temperature threshold	37.3 (1-100)						
Time 1	<input checked="" type="checkbox"/>	0	:	0	--	23	: 59
Time 2	<input checked="" type="checkbox"/>	0	:	0	--	23	: 59

Save

Reply defaults

Fig. 3.1.8-2

**【Times recognition】** If face picture can be matched in the list within the set recognition times, recognition will be stopped. 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) (Only when recognition mode is times recognition).

**【Single face recognition】** Similar to the mode whose times recognition value is 1, but number of pictures is recognized. (Single face recognition is recommended for access control attendnace panel )

**【Continuous recognition】** Face will be recognized according to set capturing mode

**【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)

**【 Contrast mode 】** Select contrast mode of access control attendnace panel from face recognition, temperature detection, face + temperature detection, ID Card + face + temperature, ID Card + face, ID Card or whitelist + temperature and ID Card or whitelist. Contrast mode is temperature detection 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	<input checked="" type="checkbox"/> Continuou	Alarm output	1 S	Type	NO	*	
Recognize Mode	single rec						
Comparison similarity	75 (1-100)						
ID similarity	60 (1-100)						
Matching mode	<div> <div>Face detect</div> <div>Temperature detect</div> <div>Face detect + Temperature detect</div> <div>ID + face + temperature</div> <div>ID + face</div> <div>ID card or whitelist + temperature</div> <div>ID card or whitelist</div> </div>						
Mask detect							
Temperature correction	<div> <div></div> <div>temperature</div> <div>0.0</div> <div>(0°-1°)</div> </div>						
Abnormal temperature opens the door	close						
Temperature threshold	37.3 (1-100)						
Time 1	<input checked="" type="checkbox"/> 0 : 0 -- 23 : 59						
Time 2	<input checked="" type="checkbox"/> 0 : 0 -- 23 : 59						
<div>Save</div> <div>Reply defaults</div>							

图 3.1.8-3

Fig. 3.1.8-3

【Mask detection】 ON or OFF is optional. It is OFF by default (note: If mask detection is OFF, contrast record and mask use shall be None).

【Temperature correction】 Intelligent algorithm and low 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 temperature algorithm means to convert unreasonable body temperature value into normal body temperature automatically under low temperature.

【Open at high temperature】 ON or OFF is optional in case of high temperature alarm. It is OFF by default. If high temperature is detected at ON, namely alarm signal will be outputted when the temperature exceeds the temperature threshold.

【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.

【Deployment period】 Deployment can be conducted within the specified time (deployment time is 00:00-23:59 by default and it is ON by default)



### 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;

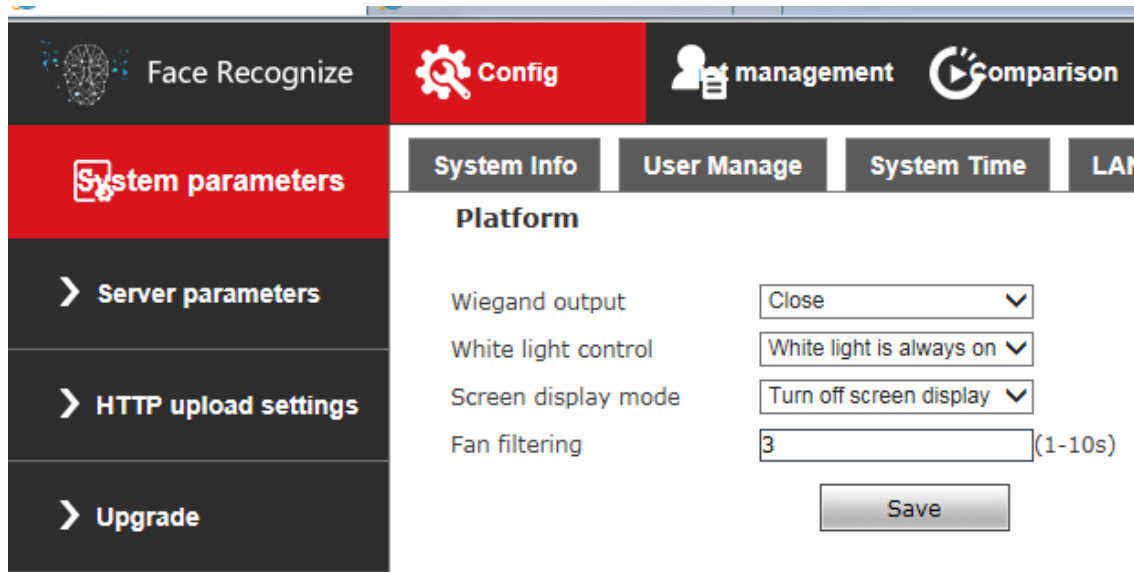


Fig. 3.1.9-1

Wiegand output: it can set up Wiegand output off, or turn on Wiegand output, Wiegand 26 or Wiegand 34 is optional;

#### Platform

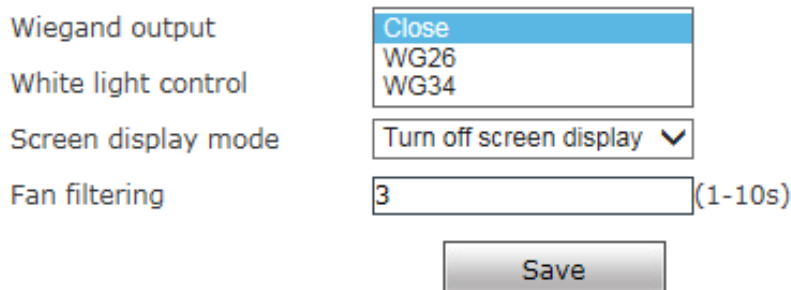


Fig. 3.1.9-2

White light control: White light is normally on, white light time control and white light is normally off are optional; White light time control is set cooperatively with daytime/nighttime on the right. Default: White light is normally on.

Platform

Wiegand output

Close

White light control

White light time control

Turn day0:0:0Turn night23:59:59

Screen display mode

Turn off screen display

Fan filtering

3

(1-10s)

Save

Fig. 3.1.9-3

Screen display mode: Always display and screen display is closed is there is nobody are optional; Default: Screen display is closed within 10s if there is nobody.

Platform

Wiegand output

Close

White light control

White light time control

Turn day0:0:0Turn night23:59:59

Screen display mode

Always display

Turn off screen display after no one

Fan filtering

3

(1-10s)

Save

Fig. 3.1.9-4

Same face filtration: Face filtration time of the same list, it is 3s by default.

3.1.10 Face Recognition• Equipment Information

Device Info.

Device IP

direction

longitude

Dimension

Manufacturer code

Save

Fig. 3.1.10

Used to display current device information.

### 3.1.11 Factory Reset

The setup interface of factory reset of the access control attendnace panel is shown in Fig. 3.1.11:

#### Restore

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

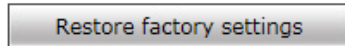


Fig. 3.1.11

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

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

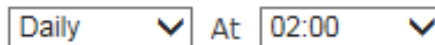
**【Username and password】** Tick to restore default username and password. It is admin/admin by default.

### 3.1.12 Device Restart

The setup interface of device restart of the access control attendnace panel is shown in Fig. 3.1.12:

#### Reboot

Restart The System Automatically



Restart The System Manually

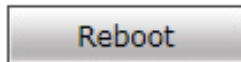
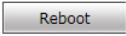


Fig. 3.1.12

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

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

### 3.2 Server Parameter

Set up relevant server parameters in the menu, as shown in Fig. 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).

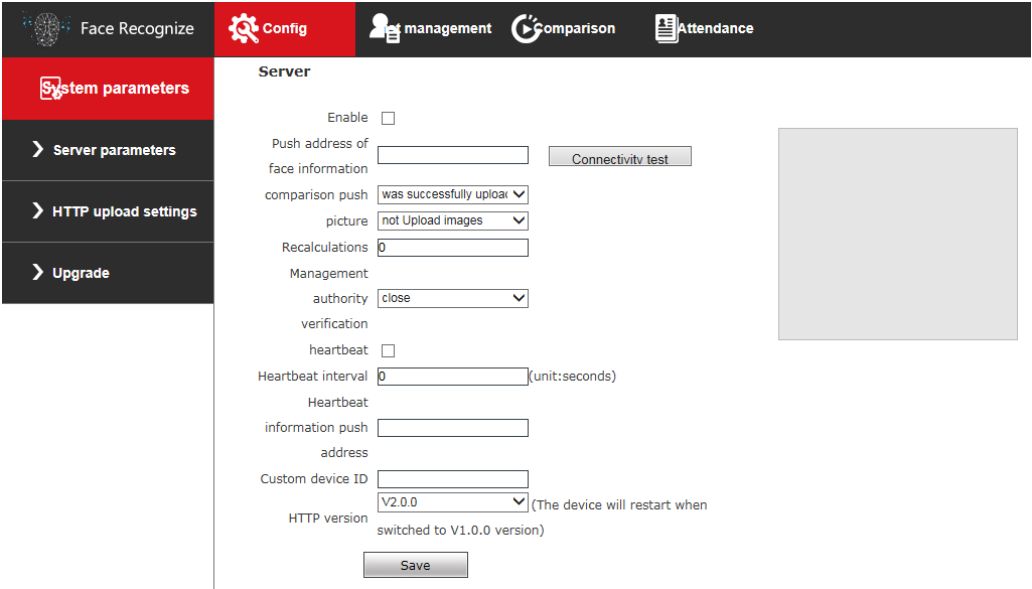


Fig. 3.2

- 【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 attendance panel , set up relevant server parameters in the menu, as shown in Fig. 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).

The screenshot displays the 'HTTP upload' configuration page. The sidebar on the left includes 'Face Recognize', 'System parameters', 'Server parameters', 'HTTP upload settings', and 'Upgrade'. The main panel contains the following settings:

- Capture upload**: ☐
- Capture information**:
- upload address**:
- Compare upload type**:
- Capture information content**: ☐ FaceInfo ☐ CompareInfo
- upload picture**: ☐ Face map ☐ Background image ☐ List ☐ library ☐ photo
- Number of retransmissions**:
- registered**: ☐
- Registration information**:
- upload address**:
- Heartbeat upload**: ☐
- Heartbeat information**:
- upload address**:
- Heartbeat interval**:  (unit:seconds)
- 主动获取任务地址**:
- 任务结果上报地址**:
- Sign verification**:
- Operating mode**:
- HTTP version**:  (The device will restart when switched to V1.0.0 version)
- Save**:

Fig. 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 attendance panel is shown in Fig. 3.4:

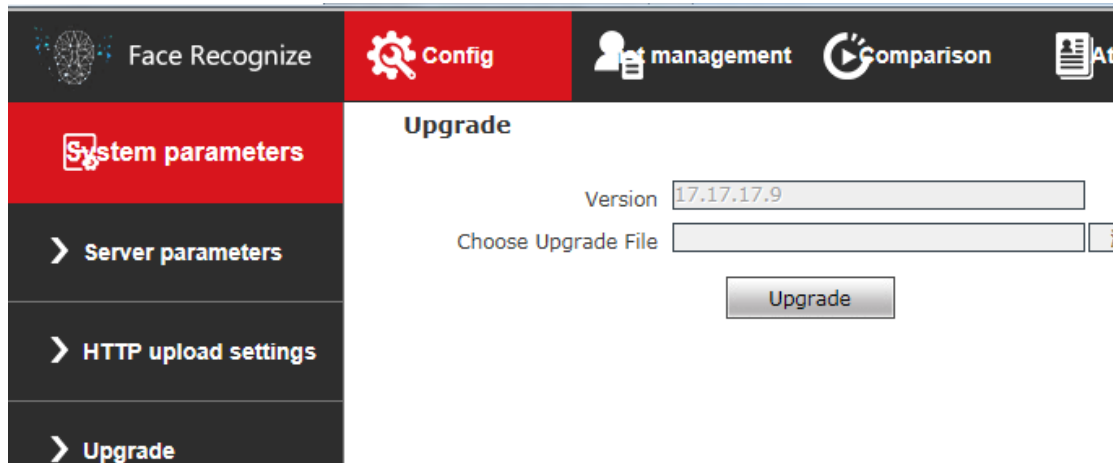


Fig. 3.4

**【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 attendance panel 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 attendance panel 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 whitelist can be added to the library in different ways

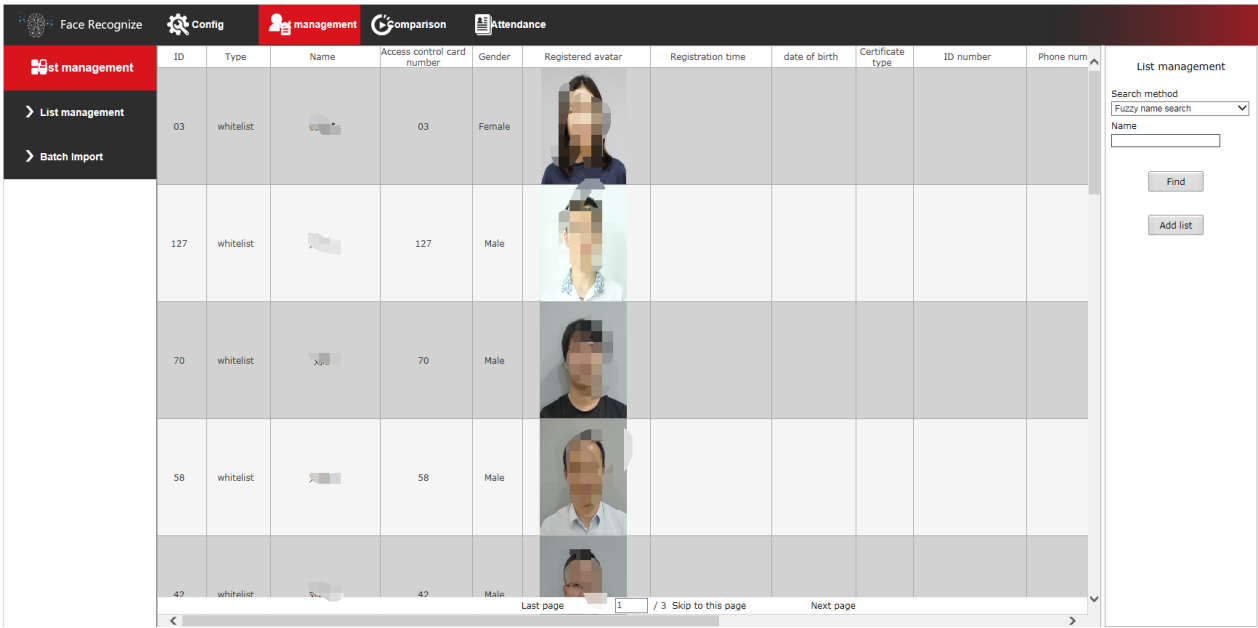


Fig. 4.1-1

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 whitelist by 【Add list】 as follows

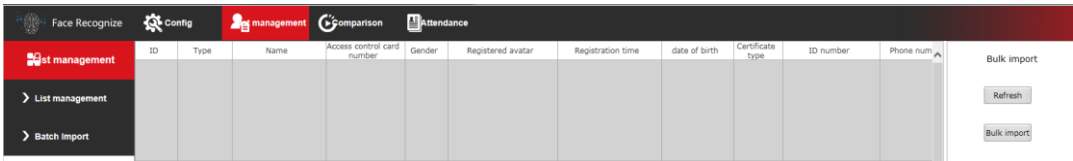


Fig. 4.1-2

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 whitelist and VIP list by batches



Fig. 4.2-1

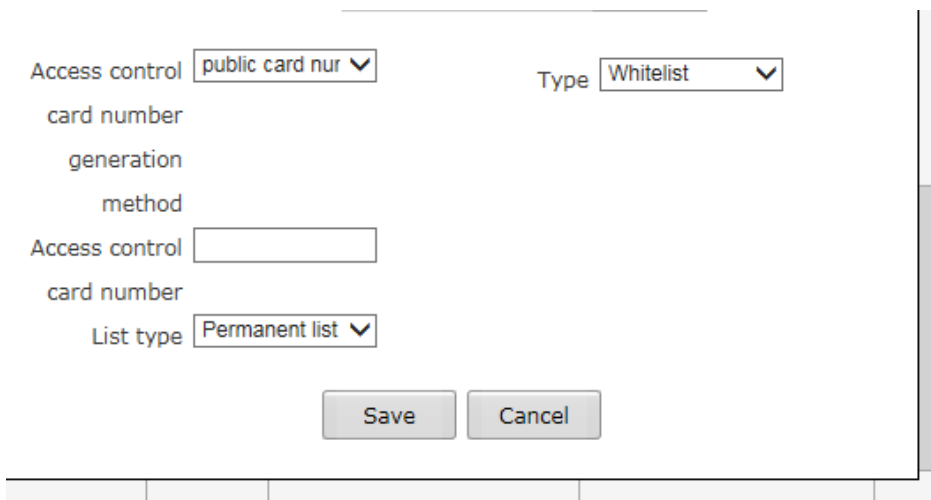


Fig. 4.2-2

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.

Face Recognize

Config

management

Comparison

Attendance

Face recognize

Condition

2020 - 4 - 14

00:00

-

2020 - 4 - 15

23:59

owner

Name

number

Search

Routing Mac	name	Serial number	list	body temperature	time	Detailed situation

Last page

1 / 26

Skip to this page

Next page

Fig. 5

# 6 Attendance Record

Attendance record of any day or any period can be queried

Face Recognize

Config

management

Comparison

Attendance

Face recognition.

Set Time

Sunday

go to work

06:00

-

09:00

off duty

18:00

-

Advanced

save

default

Working days setting

☐ On Sunday

☒ On Monday

☒ On Tuesday

☒ On Wednesday

☒ On Thursday

☒ On Friday

☐ On Saturday

2020 - 4 - 15

-

2020 - 4 - 15

Name

number

Attendance status

query type

Search

Routing Mac	name	Serial number	Detailed situation
		03	Attendance Date:,Working hours:undefined,Work status:,off time:undefined,After work status:

Last page

1 / 16

Skip to this page

Next page

Fig. 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 attendnace panel 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 Default network parameter

Default network parameter

## Appendix 3 Frequently Asked Questions

### 1. What if the access control attendnace panel 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 attendnace panel and network, connect access control attendnace panel and PC and log in to the access control attendnace panel 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 attendnace panel ?

**Solution:** Modify physical address of the access control attendnace panel .

**Possible cause 5:** Web port has been modified?

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

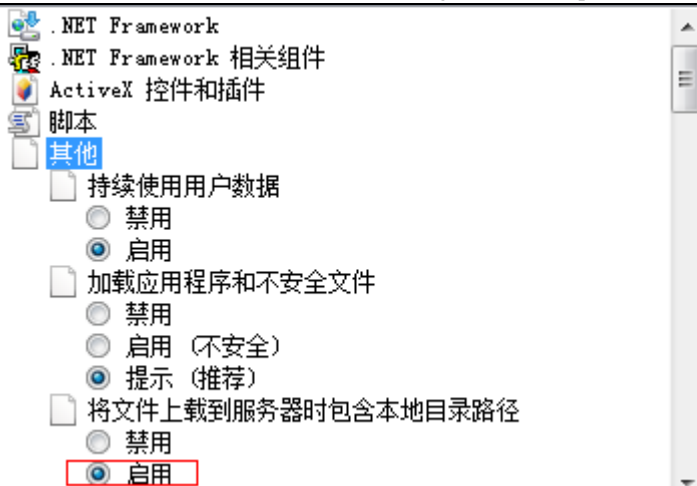
**Possible cause 6:** Unknown?

**Solution:** Click on Reset behind the panel or interface of the access control attendnace panel to restore factory settings and reconnect the device. Default IP address: 192.168.1.88, subnet mask: 255.255.255.0.

### 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 1:** There is a **【RESET】** button on the rear board or interface of the access control attendance panel . Under power-on state, press Reset for 1-2s and release it for 1-2s. Repeat three times and factory settings will be restored. Default IP: 192.168.1.88 Default username and password: admin/admin

**Solution 2:** 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



**Important:** Only professionals can press RESET. After reset, all parameters will be restored to factory settings (except physical address of network).

**11. 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.

**12. Plenty of cameras are offline, how to eliminate fault**

**A camera is always offline**

**Possible cause:** Camera breaks down, or IP addresses conflict with each other

**Solution:** Modify IP or restore factory settings

**Different devices are offline at different time and points**

**Possible cause 1:** The switch has insufficient resources

**Solution:** Estimate bandwidth according to on-site quantity and replace gigabit switch

**Possible cause 2:** Low voltage of centralized power supply

**Solution:** Detect voltage value in the middle and at the far end of centralized power line, check whether voltage drop is large and elevate voltage

**13. Body temperature value is not displayed in the interface**

**Possible cause:** Recognition mode is set as face recognition

**Solution:** Recognition mode is temperature detection or face + temperature detection

**14. 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

**15. 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

**16. 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.

**17. 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

**18. 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.**



