

Face Recognition & Temperature Measurement Access Control Attendance Panel User Manual

(For Windows XP/2003/Win7/Vista/Win 8/Win 10)

Version: V1.7

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 [【Download link】](#).

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.

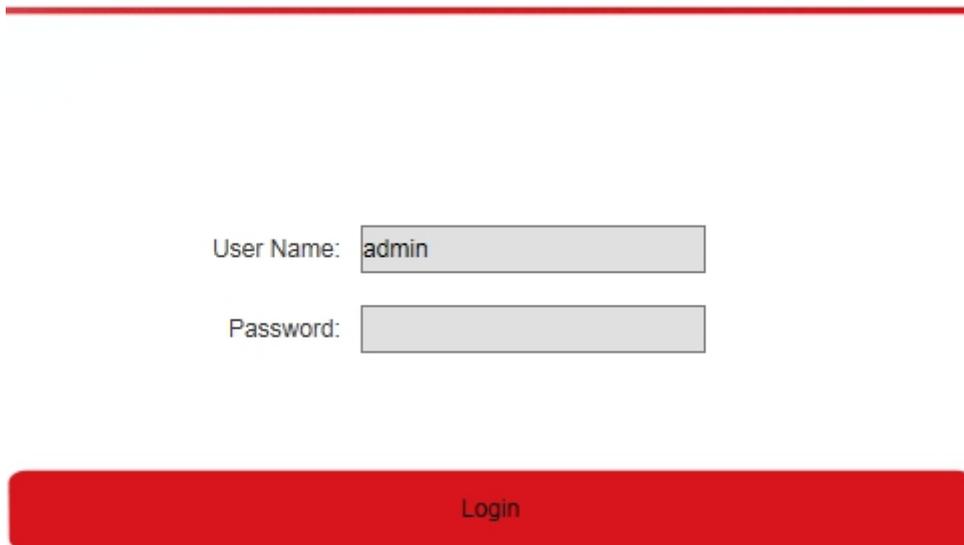
Revision date	Version	Description
April 14, 2020	V1.0	Available for ten languages
May 09 , 2020	V1.1	Add video encoding and other pages
July 06 , 2020	V1.2	Add wireless network parameters and other modules
August 05 , 2020	V1.3	Support open door conditional logic
August 26 , 2020	V1.4	Page layout adjustment
October 29 , 2020	V1.5	Added temperature correction (smart mode + normal mode) function
November 25 , 2020	V1.6	Delete the list batch import related information, add Email parameters, access control function, add RTMP, MQTT, GB28181, GA/T1400 protocol and other pages
December 26, 2020	V1.7	Added 4G parameter page, access control function, face recognition parameter setting function

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 Basic Parameters.....	7
3.1.3 User Management.....	7
3.1.4 Time Settings.....	8
3.1.5 Device Setting.....	9
3.1.6 Factory Reset.....	9
3.1.7 Device Restart.....	10
3.1.8 Software Upgrade.....	10
3.2 Network Settings.....	11
3.2.1 Wired Network Parameter.....	11
3.2.1 HTTP Upload Settings.....	12
3.2.3 Wireless network parameters.....	14
3.2.4 RTSP.....	15
3.2.5 RTMP Parameters.....	16
3.2.6 FTP Parameter.....	17
3.2.7 Email Parameter.....	18
3.2.9 DDNS Parameter.....	21
3.2.10 Mobile P2P.....	22
3.2.11 Platform connecting.....	23
3.2.12 MQTT.....	24
3.2.13 GB28181.....	24
3.2.14 GAT 1400 Agreement.....	26
3.3 Intelligent Analysis.....	28
3.3.1 Face Recognition• Parameter Setting.....	28
3.3.2 Face recognition · Access control.....	30
3.3.3 Face Recognition• Equipment Information.....	35
3.4 Video Settings.....	35
3.4.1 Audio properties.....	35
3.4.2 Video parameters.....	36
3.4.3 Video coding.....	37
4 List Management.....	39
5 Contrast Record.....	40
6 Attendance Record.....	41
Appendix 1 Network port occupied by IP camera.....	43
Appendix 2 Default network parameter.....	43
Appendix 3 Frequently Asked Questions.....	43

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.



The login form consists of two input fields and a button. The first field is labeled 'User Name:' and contains the text 'admin'. The second field is labeled 'Password:' and is empty. Below these fields is a large red button with the text 'Login' centered on it.

Fig. 1

2 Main Interface

The main interface is shown in Fig. 2:

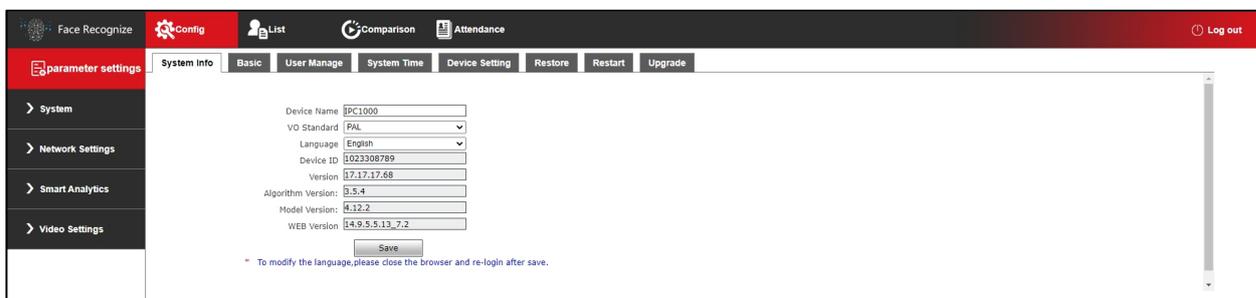


Fig. 2

3 Settings

3.1 System Parameter

3.1.1 System Information

The setup interface of system information and basic parameters of system parameters of the access control attendnace panel are shown in Fig. 3.1.1:

The screenshot shows a web-based configuration interface for system information. It contains the following fields and values:

Device Name	IPC1000
VO Standard	PAL
Language	English
Device ID	1023308789
Version	17.17.1.51
Algorithm Version:	3.5.4
Model Version:	4.12.2
WEB Version	14.9.5.5.13_7.2

Below the fields is a "Save" button. A red asterisk followed by the text: "To modify the language, please close the browser and re-login after save."

Fig. 3.1.1

【Device name】 The device name defaults to IPC1000 and can be customized.

【VO ring out formula】 VO ring out can be set to PAL or NTSC.

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

【Equipment serial number】 The equipment number cannot be modified.

【Kernel version】 The kernel version is the device firmware version

【Version of the algorithm】 The algorithm version is the device algorithm version

【Temperature measuring firmware】 The temperature measurement firmware is the firmware version of the temperature measurement module (T2 only has this information).

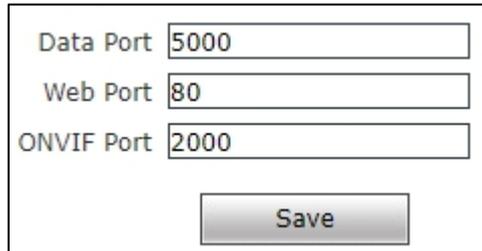
【Model version】 The model version is the device algorithm model version

【WEB version】 The WEB version is the page version

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

3.1.2 Basic Parameters

The UPNP parameter interface of access control machine is shown in Figure 3.1.2 below



The screenshot shows a web interface for setting UPNP parameters. It contains three input fields: 'Data Port' with the value '5000', 'Web Port' with the value '80', and 'ONVIF Port' with the value '2000'. Below these fields is a 'Save' button.

Fig .3.1.2

【Data port】 The default is 5000

【Web port】 The default is 80

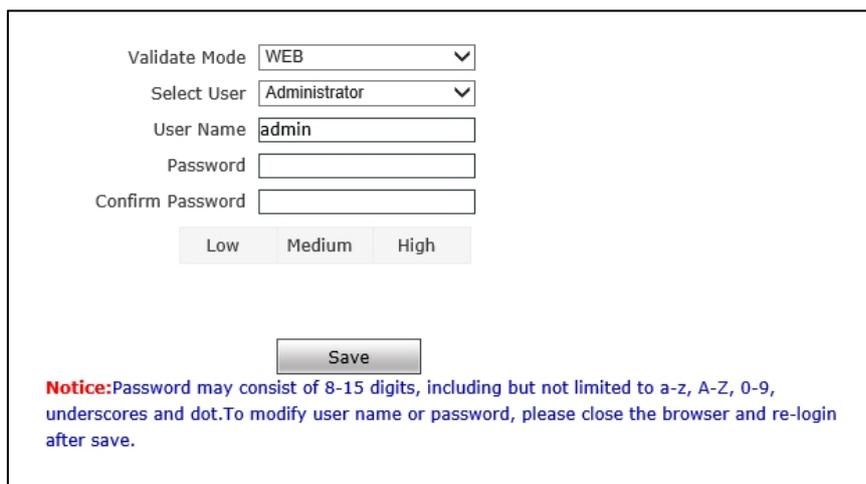
【ONVIF port】 The default is 2000

After setting the parameters, click the "save" button, and it will take effect after the device is restarted.

3.1.3 User Management

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

3.1.2:



The screenshot shows a web interface for user management. It includes a 'Validate Mode' dropdown menu set to 'WEB', a 'Select User' dropdown menu set to 'Administrator', a 'User Name' text input field containing 'admin', and empty 'Password' and 'Confirm Password' text input fields. Below these fields are three radio buttons labeled 'Low', 'Medium', and 'High'. A 'Save' button is located at the bottom. A red notice is displayed below the button: **Notice:** Password may consist of 8-15 digits, including but not limited to a-z, A-Z, 0-9, underscores and dot. To modify user name or password, please close the browser and re-login after save.

Fig. 3.1.3

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.

3.1.4 Time Settings

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

3.1.4:

Date 2020 - 12 - 10 19: 26: 53

NTP Server

Synchronize with Local Computer

Set the Time Manually

Time zone conversion 1

RTC switch Close

Save

Fig. 3.1.4

【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.

3.1.5 Device Setting

The storage device interface of the access control machine is shown in Figure 3.1.5 below:

Choose	No.	TotalSize(M)	FreeSize(M)	Status
<input checked="" type="radio"/>	1 HSD	14800	12342	formatted

Fig. 3.1.5

【Formatting】 You can choose to format device storage (list library, comparison records, and attendance records are all cleared).

【Refresh】 Real-time view of device storage, know the remaining capacity.

3.1.6 Factory Reset

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



Fig. 3.1.6

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.

3.1.7 Device Restart

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

3.1.7:

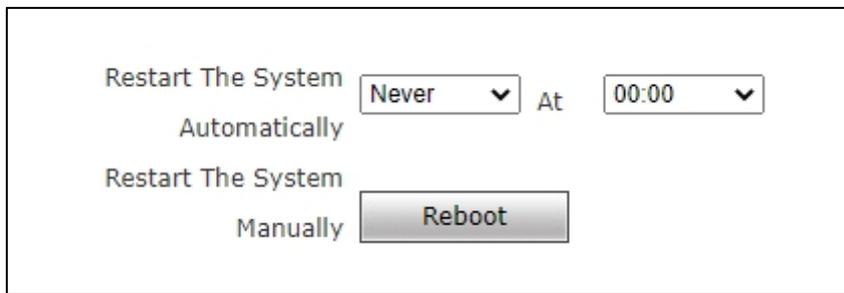


Fig. 3.1.7

【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.

3.1.8 Software Upgrade

The software upgrade interface of the access control attendnace panel is shown in Fig. 3.1.8:

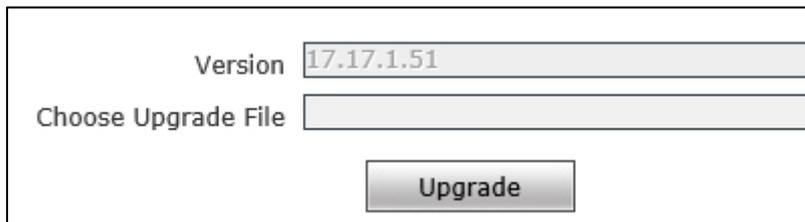


Fig. 3.1.8

【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 attendnace panel will be restarted automatically after upgrade. Log in to the device again, enter the



Important:

- 1、 Please ensure power and network of the access control attendnace 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

3.2 Network Settings

3.2.1 Wired Network Parameter

The setup interface of wired network parameters of the access control attendnace panel is shown in Fig. 3.2.1:

DHCP Enable	<input type="checkbox"/>
IP	128 . 128 . 10 . 26
Subnet Mask	255 . 255 . 0 . 0
Gateway	128 . 128 . 1 . 1
Preferred DNS	202 . 96 . 134 . 133
Alternate DNS	8 . 8 . 8 . 8
MAC	00-b9-42-13-4b-a0

Save

Fig. 3.2.1

【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

【Physical address】 MAC address of access control attendance 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 valid



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.

3.2.1 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. 3.2.2 (picture version is HTTP version 2.0.11by default. HTTP version can be modified according to actual need. The device will be restarted after modification).

The screenshot shows a configuration interface with the following elements:

- Capture upload**:
- Capture information upload address**:
- Compare upload type**:
- Capture information content**: FaceInfo CompareInfo
- upload picture**: Face map Background image List library photo ID photo
- Number of retransmissions**:
- registered**:
- Registration information upload address**:
- Heartbeat upload**:
- Heartbeat information upload address**:
- Heartbeat interval**: (unit:seconds)
- Actively obtain the task address**:
- Address to report task results**:
- Central connection**:
- Central server address**:
- Sign verification**:
- Operating mode**:
- Verification information upload address**:
- Notification information upload address**:
- History upload address**:
- HTTP version**: (The device will restart when switched to V1.0.0 version)
- Save**:

Fig. 3.2.2

【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.

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

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

【Central server address】 The address of the central server.

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

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

【Verify information upload address】 Verify the address where the information is uploaded.

【Notification information upload address】 Notify the address where information is uploaded.

【Historical upload address】 The address where the history was uploaded.

【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.

3.2.3 Wireless network parameters

The wireless network parameter page is shown in Figure 3.2.3 below:

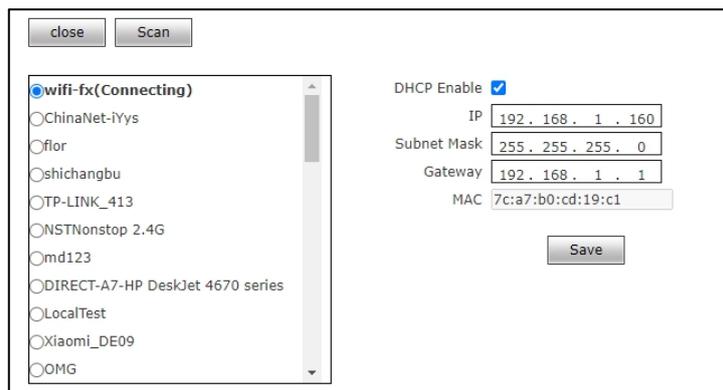


Fig. 3.2.3

【Wireless network switch】 Click this switch to turn on the wireless network function; When the

wireless switch is turned on, the wireless SSID will be automatically scanned.

【Scanning】 Click scan to search for the nearby wireless SSID.

Select the required SSID, the password input box will pop up, enter the corresponding password

to save, the page will automatically refresh, you can select the SSID after the connection status

【DHCP Switch】 Using this feature, when connected to a wireless router, it will automatically get the IP address, subnet mask, and gateway from the router.

【IP Address】 Fixed IP: Set the wireless IP address, such as 192.168.1.160.

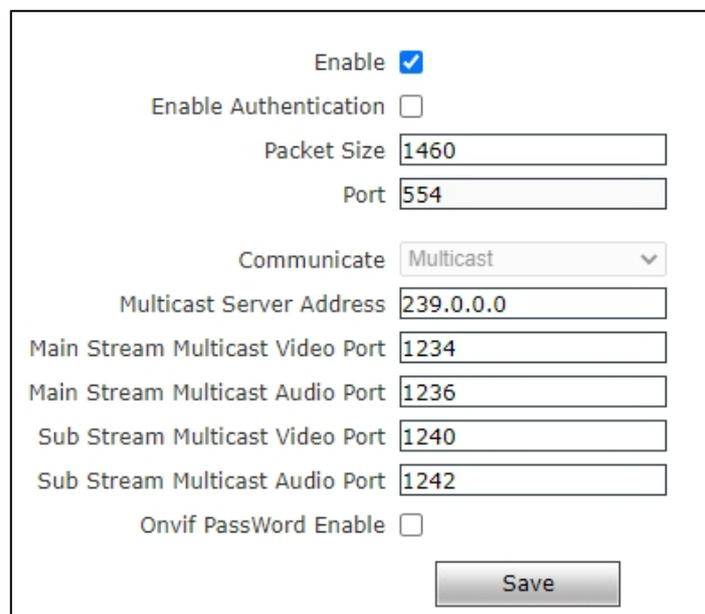
【Gateway】 Set the IP address of the current wireless gateway (router /AP), such as 192.168.1.1.

【WiFi Exception Handling】 When WiFi connection is abnormal, the device will automatically restart. The default is off.

【Network transmission strategy】 When the WiFi signal is poor, the video transmission is processed by frame reduction. The default is off. After all Settings are completed, save the parameters. Access to the device via the camera's wireless IP.

3.2.4 RTSP

The RTSP parameter setting interface of the access control machine is shown in Figure 3.2.4 below:



The screenshot shows the RTSP parameter setting interface. It includes the following fields and options:

- Enable
- Enable Authentication
- Packet Size
- Port
- Communicate
- Multicast Server Address
- Main Stream Multicast Video Port
- Main Stream Multicast Audio Port
- Sub Stream Multicast Video Port
- Sub Stream Multicast Audio Port
- Onvif PassWord Enable
- Save button

Fig.3.2.4

【RTSP Switch】 When the RTSP switch is checked, the RTSP function is turned on.

The default RTSP port is 554.

【RTSP Model】 Active and passive modes are optional.

【Whether The Certification】 When checked, you will need a password to connect to your device using VLC and QuickTime Player.

Open authentication access method: rtsp://ip/av0_0&user=admin&password=admin;

Turn off authentication access method:rtsp://ip/av0_0

【&user=admin&password=admin】 , **【】** Is optional; Where, the first "0" of "av0_0" represents the number of channels: 0,1,2,3, table 1,2,3,4; The network camera has only one channel, fill in "0"; The second "0" represents the primary/secondary code stream, 0 is the primary code stream, 1 is the secondary code stream;When the authentication mode changes, the device restarts.

【Communication Mode】 The default multicast is on.

【Onvif password authentication】 Once checked, adding an operating device via Onvif requires the user to log in.

After setting the parameters, click the "save" button and the setting will take effect.

3.2.5 RTMP Parameters

The RTMP parameter interface of access control machine is shown in Figure 3.2.5 below:

The screenshot shows a configuration window for RTMP parameters. At the top, there is an 'Enable' checkbox which is currently unchecked. Below it is a 'Server URL' text input field. The next row contains 'Push code stream' with a dropdown menu showing 'Main stream'. This is followed by 'Switch 2' checkbox (unchecked) and 'Server address 2' text input field. The next row has 'Push code stream 2' with a dropdown menu showing 'Auxiliary stream'. Below these are four rows for time settings: 'Time 1', 'Time 2', 'Push time period 3', and 'Push time period 4'. Each row has an unchecked checkbox and a time range selector with four input boxes (0, :, 0, --, 23, :, 59). At the bottom center is a 'Save' button.

Fig. 3.2.5

【Switch】 RTMP Switch.

【Server address】 Fill in the RTMP address.

【Push Stream】 Choose to push the code stream, choose the main code stream/auxiliary

【Switch 2】RTMP Switch 2.

【Server address 2】Fill in the RTMP address.

【Push Stream 2】Choose to push the code stream, choose the main code stream/auxiliary code stream.

【Time Of Deployment 1】You can set up a defense period 1.

【Time Of Deployment 2】You can set up a defense period 2.

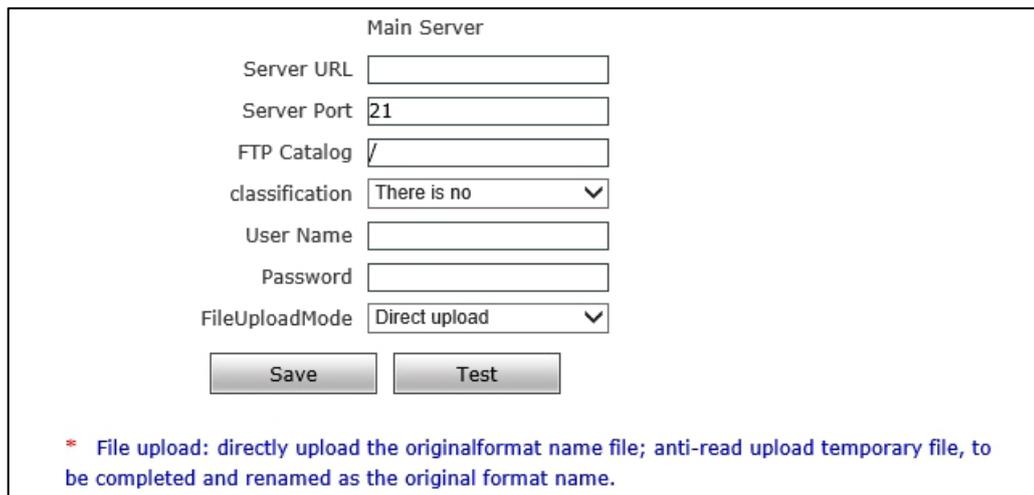
【Push time 1】Push time period can be set 1.

【Push time 2】Push time period can be set 2.

After setting the parameters, click the "save" button and the parameters will take effect.

3.2.6 FTP Parameter

The FTP parameter setting interface of the access control machine is shown in Figure 3.2.6 below:



Main Server

Server URL

Server Port

FTP Catalog

classification

User Name

Password

FileUploadMode

* File upload: directly upload the original format name file; anti-read upload temporary file, to be completed and renamed as the original format name.

Fig. 3.2.6

FTP service will FTP face snapshot pictures to the designated FTP server:

【FTP URL】IP address or HTTP url of the FTP server.

【FTP Port】Port for FTP server, default port is 21.

【Remote Path】The path on the remote FTP server. If the path does not exist or is not filled in, the device will automatically create a folder in the root directory of the FTP server.

【FTP Username And Password】 The username and password for the FTP server.

【File Upload Mode】 FTP file upload, there are two options, direct upload and anti-read upload, the default is direct upload.

Click **【Test】** : Wait for test results; If the test is successful, a test.jpg file will be generated in the user Settings directory.

After setting the parameters, click the "save" button and the setting will take effect.

FTP server application reference:

Step 1: Close the Window firewall.

Step 2: Open FTPServer and set the receiving port, account name, account password, access directory and account permissions.

Step 3: Set the FTP parameters for IPC.

Step 4: Test whether the transfer is successful.

Step 5: Save the FTP parameters entered on the IPC page.

【monitoring port】 , **【account name】** and **【account password】** can be set separately according to their own needs, but they must be consistent with THE IPC FTP parameters;

【Access directory】 is different from **【remote path】** of IPC FTP parameter. This parameter selects the root directory where face pictures are stored for the user.

【Account permissions】 all checked.

Fill in the corresponding parameters in the FTP of the access control machine, and you can use it



Note: To upload video files and capture pictures, the user must have write permission on the FTP server.

3.2.7 Email Parameter

The interface of UPNP parameters of access control machine is shown in Figure:

The screenshot shows a web-based configuration form for email settings. The fields are as follows:

- To:** An empty text input field followed by a dropdown menu showing "126.com".
- Binding email:** A checked checkbox.
- From:** A text input field containing "hello_world100" followed by a dropdown menu showing "126.com".
- Authorization code:** A text input field with seven dots (•••••••).
- MAIL Title:** A text input field containing "Alarm Message".
- SMTP Port:** A text input field containing "25".
- Encryption protocol:** A dropdown menu with "None" selected.
- Push type:** A dropdown menu with "None" selected.
- Buttons:** "Save" and "Test" buttons are located at the bottom center.

Fig. 3.2.7

It is used to push real-time comparison records, and the push types include: no push (no push), abnormal high temperature push, push without wearing masks, push by visitors, push by listed people, push by all.

【Recipient address】 The email address to receive mail, fill in the email name, select the email type in the drop-down menu below, or select "other" to manually fill in the email type.

The original email address is "hello_world100@126.com". Please check "Bind email" to modify the email address of the sender

【Sender user name】 The email address to send the email, fill in the email name, and select the email type from the drop-down menu at the bottom. You can also select "other" to manually fill in the email type.

【Password】 SMTP service authorization password of the mailbox where the email is sent.

The subject of a message sent.

【SMTP port】 SMTP server's port, different mail server, the port is different. For example, the Gmail mail server port is 465.

【Encryption Protocol】 Optional mailbox encryption protocol: no /SSL/TLS.

After setting the parameters, click the "save" button and the setting will take effect.

Click the "Test" button to send a test email and return success/failure.

Common mail server configuration:

Gmail Email Server:

SMTP server: SMtp.gmail.com

SMTP username: username@gmail.com

SMTP port: 465

SSL: enable

Yahoo Mail Server:

SMTP server: smtp.mail.yahoo.com

SMTP username: username@yahoo.com or username@yahoo.com.cn

SMTP port: 465

SSL: enable

163 Mail server:

SMTP server: SMtp.163.com

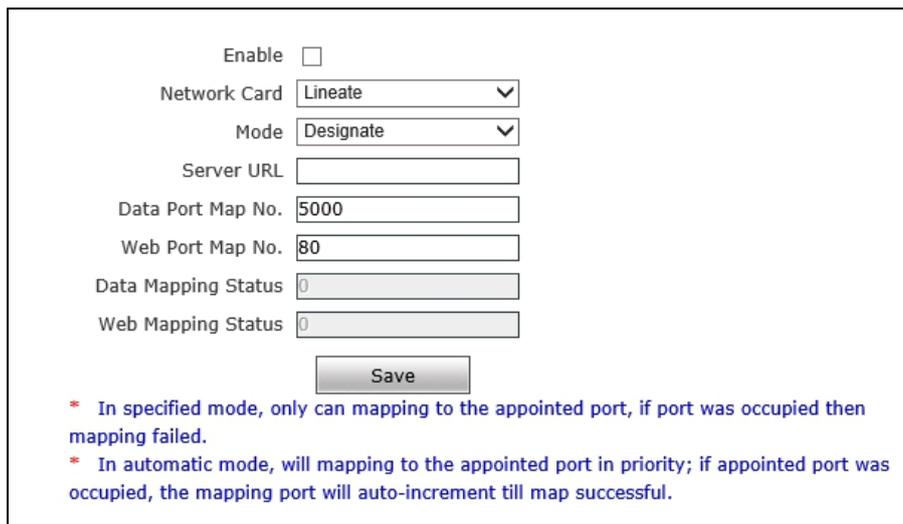
SMTP username: Username

SMTP port: 25

SSL: no

3.2.8 UPNP Parameter

The UPNP parameter interface of the access control machine is shown in Figure 3.2.8 below:



Enable

Network Card

Mode

Server URL

Data Port Map No.

Web Port Map No.

Data Mapping Status

Web Mapping Status

* In specified mode, only can mapping to the appointed port, if port was occupied then mapping failed.

* In automatic mode, will mapping to the appointed port in priority; if appointed port was occupied, the mapping port will auto-increment till map successful.

Fig.3.2.8

Port automatic mapping, when there is a server with UPNP function in the LAN, turn on this function, the server will automatically map the set port to the public network.

【 Network card 】 The type of network card connected to UPNP server.

【Usage mode】 there are two modes: specified and automatic:

Specify a schema that specifies a data mapping port and a Web mapping port to the server.

In automatic mode, the data mapping port and Web mapping port are set by the server.

【Server address】 Network server gateway address with UPNP function.

【Data mapping port】 sets the data ports that are mapped to the server.

【Web mapping port】 sets the Web port mapped to the server.

【Data port mapping state】 displays the status of the mapped data ports.

【Web port mapping state】 displays the state of the mapped Web port.

After setting the parameters, click the "save" button and the setting will take effect.

3.2.9 DDNS Parameter

DDNS parameter interface of access control machine is shown in Figure 3.2.9 below:

The screenshot shows a web-based configuration form for DDNS. At the top, there is an 'Enable' checkbox which is currently unchecked, followed by the text 'URL 3322.org'. Below this are several input fields: 'Service Provider' (a dropdown menu), 'User Name', 'Password', 'Domain', 'Server URL' (containing 'www.3322.org'), 'Server Port' (containing '30000'), 'Data Port' (containing '5000'), 'Web Port' (containing '80'), and 'Update Interval' (a dropdown menu set to '30 minutes'). At the bottom left, there is a note: 'Domain e.g.: test1.3322.org'. A 'Save' button is located at the bottom center of the form.

Fig.3.2.9

Dynamic DNS setting, which binds the device to a fixed domain name and allows access to the device through the domain name no matter how the device's public IP changes.

【Switch】 Set whether to turn on DDNS function.

Link to mvdns.net: Click this link to go to www.mvdns.net where users can register their DDNS account.

【Service provider】 mvddns.net、3322.org and user ddns server。

【Registered name】 User name registered on DDNS server.

【Password】 The user registers the password corresponding to the user name on the DDNS server.

User - set device domain, e.g. Test1.mvddns.net.

【Server address】 DDNS server address, when the DDNS address is a domain name, please set the DNS address in 【wired Network Parameters】 correctly.

【Server port】 The default port is 30000 (the customer is not recommended to make any modification).

【Data mapping port】 Fill in the external data port mapped by the access control machine on the router connected to the public network here.

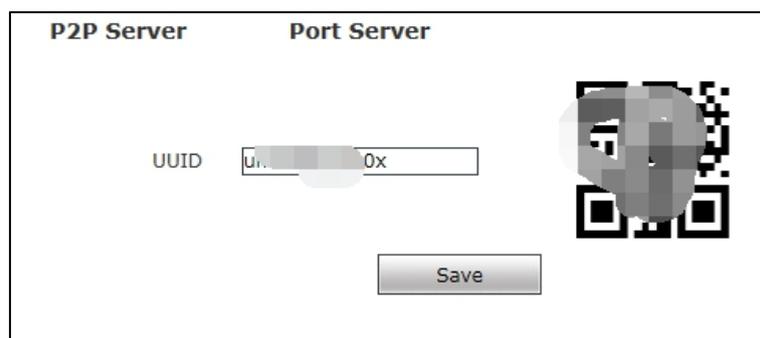
【Web mapping port】 Fill in the external Web port mapped by the access control machine on the router connected to the public network here.

After setting the parameters, click the "save" button and the setting will take effect.

3.2.10 Mobile P2P

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

3.2.10:



The screenshot shows a web interface with two main sections: 'P2P Server' and 'Port Server'. Under 'Port Server', there is a text input field containing the number '0'. Below the input field is a 'Save' button.

Fig. 3.2.10

【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*”.

3.2.11 Platform connecting

The interface of platform connection parameters of access control machine is shown in Figure 3.2.11 below:

The screenshot shows a configuration form with the following elements: an 'Enable' checkbox, a 'Server URL' input field, a 'Server Port' input field containing '0', an 'Equipment serial number' input field, a 'The user name' input field, a 'password' input field, and a 'Save' button at the bottom.

Fig.3.2.11

【Switch】 Platform link switch.

【Server address】 Fill in the address of the facial recognition integrated management platform.

【Server port】 Fill in the port of the facial recognition integrated management platform.

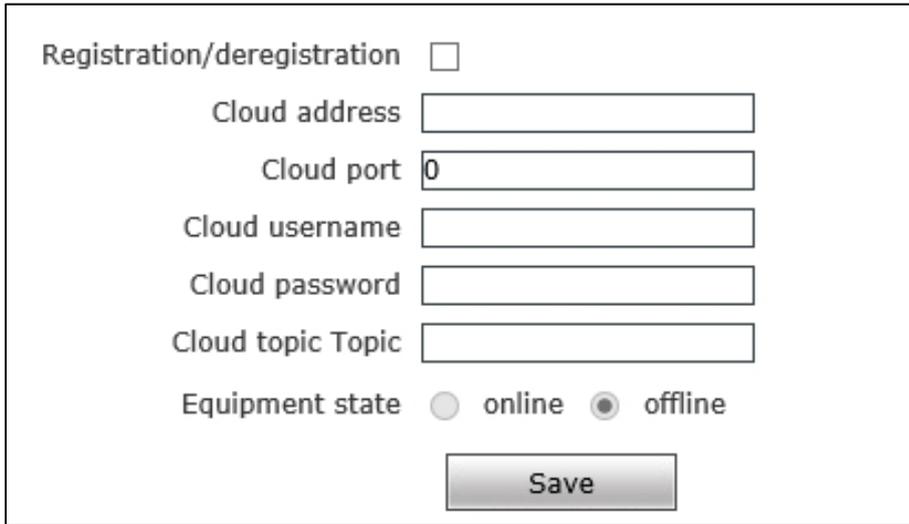
【Device serial number】 Fill in the serial number generated after adding the device to the integrated face recognition management platform.

【Server port】 Fill in the user name of the facial recognition integrated management platform.

【Server port】 Fill in the password of the integrated management platform for face recognition.

3.2.12 MQTT

The interface of MQTT parameters of access control machine is shown in Figure 3.2.12 below



Registration/deregistration

Cloud address

Cloud port

Cloud username

Cloud password

Cloud topic Topic

Equipment state online offline

Save

Fig.3.2.12

【Registration/deregistration】 MQTT registration/Deregistration

【Cloud address】 Fill in MQTT cloud address.

【Cloud Port】 Fill in MQTT cloud Port.

【Cloud user name】 Fill in MQTT cloud user name.

【Cloud password】 Fill in MQTT cloud password.

【Cloud Topic Topic】 Fill in MQTT cloud Topic.

【Device status】 Display of connection status between device and MQTT platform.

After setting the parameters, click the "save" button and the parameters will take effect.

3.2.13 GB28181

The interface of access control machine G828181 is shown in Figure 3.2.13 below

Server ID	<input type="text"/>	Server Port	<input type="text" value="5060"/>
Server address	<input type="text"/>	Device Port	<input type="text" value="5060"/>
Device ID	<input type="text"/>	Password	<input type="text"/>
User name	<input type="text"/>	Alarming channel ID	<input type="text"/>
Media channel ID	<input type="text"/>	Manufactory	<input type="text"/>
Device belonging	<input type="text"/>	Constablewick	<input type="text"/>
Administrative region	<input type="text"/>	Confidentiality properties	<input type="text"/>
Installation address	<input type="text"/>	Longitude	<input type="text" value="0"/>
Latitude	<input type="text" value="Latitude"/>	Registration valid time	<input type="text" value="3600"/>
Heartbeating time	<input type="text" value="60"/>	Devicename	<input type="text" value="IPCAMERA"/>
Timeout times	<input type="text" value="3"/>	<input type="checkbox"/> Register <input type="button" value="Log out"/>	
Register Failure			
<input type="button" value="Save"/>		<input type="button" value="Reflash"/>	

Fig.3.2.13

【ServerID】 Fill in Server ID.

【Server Address】 Fill in the server address.

【Server Port】 Fill in the server port.

【Device ID】 Fill in the device ID.

【Equipment port】 Fill in the device port.

【User Name】 Fill in the user name.

【Password】 Fill in the password.

【Media Channels ID】 Fill in the Media Channels ID

【Alarm channel ID】 Fill in the alarm channel ID.

【Equipment Belonging】 Fill in equipment ownership.

【Manufacturers】 Fill in manufacturer.

【Administrative Areas】 Fill in the administrative area.

【Precinct】 Fill in the precinct.

【Confidentiality attribute】 Fill in confidentiality attribute.

【longitude】 Fill in longitude.

【Latitude】 Fill in latitude.

【Valid time of registration】 Fill in the valid time of registration.

【Heartbeat time】 Fill in the heartbeat time.

【Equipment name】 Fill in the equipment name.

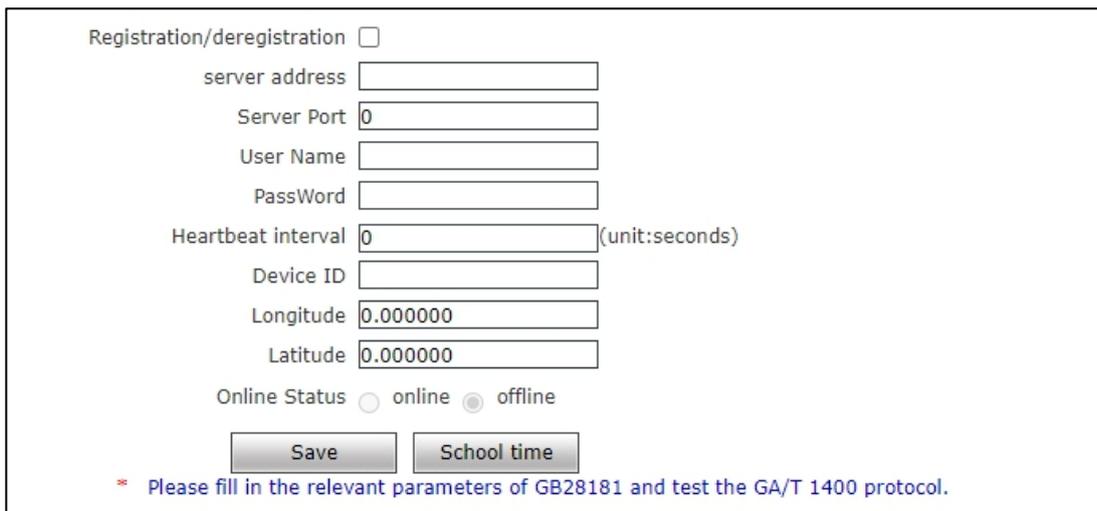
【Maximum heartbeat timeout number】 Fill in the maximum heartbeat timeout number.

After setting the parameters, click the "save" button and the parameters will take effect.

Manually register/logout after checking the box. Click the Refresh button to refresh the state.

3.2.14 GA/T 1400 Agreement

GA/T 1400 protocol interface of access control machine is shown in Figure 3.2.14 below



Registration/deregistration

server address

Server Port

User Name

PassWord

Heartbeat interval (unit:seconds)

Device ID

Longitude

Latitude

Online Status online offline

* Please fill in the relevant parameters of GB28181 and test the GA/T 1400 protocol.

Fig.3.2.14

【Registration/cancellation】 GA/T1400 Registration/cancellation.

【Server address】 Fill in the server address.

【Server port】 Fill in the server port.

【User name】 Fill in user name

【Password】 Fill in the password.

【Heartbeat interval】 Fill in the heartbeat interval.

【Device ID】 Fill in the device ID.

【Longitude】 Fill in longitude.

【Latitude】 Fill in latitude.

【Online status】 Device online status display.

After setting the parameters, click the "save" button and the parameters will take effect.

Click the "reset" button to reset the device and the 1400 server.

3.2.15 4G Parameters

The 4G parameter interface of the access control machine is shown in Figure 3.2.15

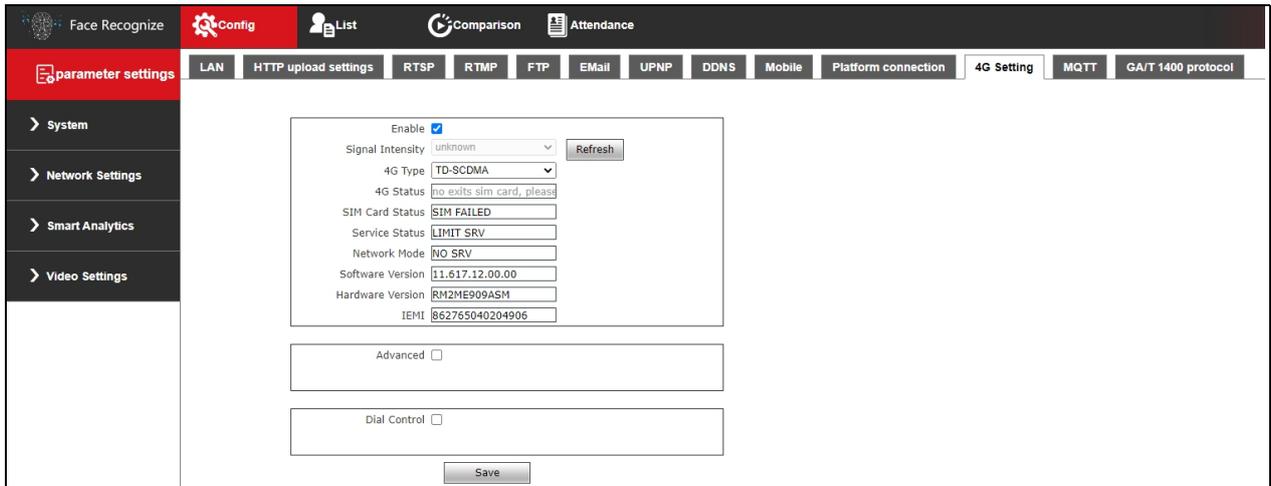


Fig 3.2.15

【switch】 4G function switch。

【Signal Strength】 4G signal strength display。

【4G Type】 4G Type。

【4GState】 4G connection status display ; If the dialing is successful, the 4G card

connection can be used normally。

【Sim Card Status】 SIM card installation status display。

【Service Status】 4G service status display。

【Network Mode】 4G network mode display。

【Software Version】 Software version display。

【Hardware Version】 4G module hardware version display (Note: the module does not display the hardware version number)。

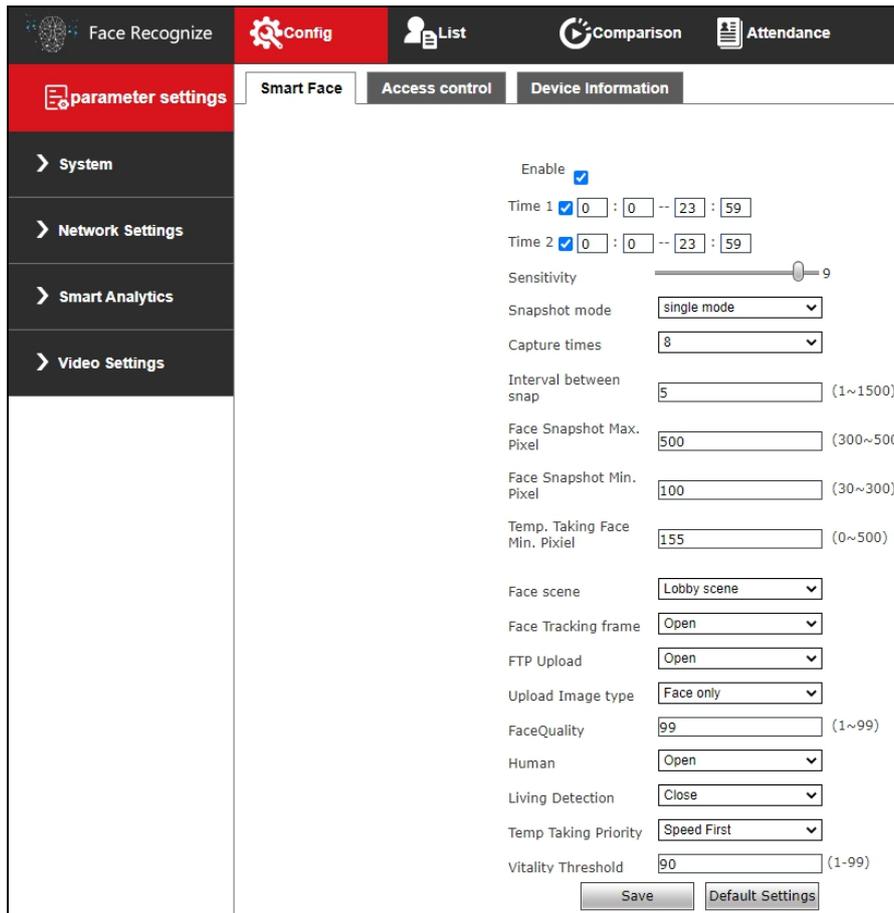
【IEMI】 4G module IEMI number display。

After setting the parameters, click the **【Save】** button to make the parameters take effect. Click the **【Refresh】** button to refresh the 4G connection status。。

3.3 Intelligent Analysis

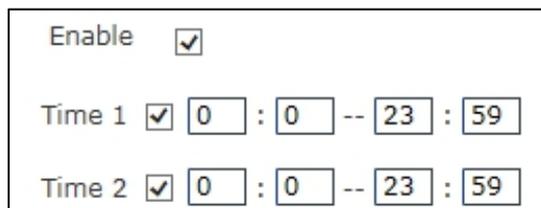
3.3.1 Face Recognition• Parameter Setting

【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.



【 Armed time period 】 It is armed time and user can define two periods. To validate it, tick

【Armed time period】 . Default: Two periods are enabled. Default time: 00: 00-23: 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

Sensitivity	<input type="range" value="9"/>
-------------	---------------------------------

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

Capturetimes	<input type="text" value="8"/>
EveryNthFrame	<input type="text" value="5"/> (1~1500)



Note: Used in the gate scene. When multiple people pass the gate, only the front one (the largest face pixel in the picture) will be captured. According to the set interval frame number, a face photo will be captured every certain number of frames and uploaded to the FTP server. There is only one face frame in the picture.

【 Face Snapshot Max. Pixel 】 Setting range: 300-500. When the pixels of the face in the screen are larger than the set value (maximum pixels for face recognition), no snapshot will be taken.

Face Snapshot Max. Pixel	<input type="text" value="500"/> (300~500)
--------------------------	--

【 Face Snapshot Min. Pixel 】 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.

Temp. Taking Face Min. Pixel	<input type="text" value="155"/> (0~500)
------------------------------	--

【 Temp. Taking Face Min. Pixel 】 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.

Face Snapshot Min. Pixel	<input type="text" value="100"/> (30~300)
--------------------------	---

【 Face scene 】 This parameter setting is used to adopt different face exposure strategies for different application scenarios. There are two modes: Conventional scene and lobby scene. Default: 【Lobby scene】 .

Conventional scene: Applicable to conventional environment.

Lobby scene: Applicable to backlight environment.

Face scene	Conventional scene Lobby scene
------------	-----------------------------------

【Face Tracking frame】 This parameter is used to superimpose the face tracking frame. Open by default.

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

For detailed configuration method, refer to 5.4.7.

FTPUpload	NO
-----------	----

【Upload Image type】 FTP upload image format, select [upload face] or [upload face and original image].

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

【Living detection】 It is OFF by default.

【Temp Taking Priority】 Optional speed priority and living body priority, the default speed priority.

【Vitality Threshold】 Default: 90; used with live detection, the lower the threshold, the more difficult it is to recognize non-living objects such as face color photos and face videos.

3.3.2 Face recognition · Access control

Information related to access control can be set, as shown in Figure 3.3.2.

Temperature and mask settings

Mask temperature detection

Continuous temperature measurement

Temperature measurement mode

Temperature threshold (1-100)

Temperature unit

Temperature Calibration

Smart Time

High temperature correction

Low temperature correction

Maximum temperature measurement

The upper limit of temperature measurement screening (35-40)

The lower limit of temperature measurement screening (20-32)

Body temperature data

Time period without measurement : -- :

Access control

White light control

Screen display mode

Face detection resolution (Switching resolution device will restart)

List similarity (1-100)

ID similarity (1-100)

Repeated face skip time (0-10s)

Time

IP

Date Format

Comparison record storage

Opening conditions

Temperature abnormal setting

IC card swiping module

gate control

Control interface

Hold time (1-60s)

Open the door action

Wiegand Agreement

Wiegand positive and negative order

Printer Settings

Label size

Fig.3.3.2

Temperature mask detection module:

【Mask & Temp Detection】 Choose no, temperature test, mask test, temperature + mask test

This test will not be performed when set to no;

When the temperature is set for temperature detection, the temperature will be detected during identification. The continuous temperature measurement switch can be set.

When set as mask detection, mask detection will be carried out during identification. The mask can be set without wearing: open the door or not open the door;

When setting temperature + mask test, temperature + mask test will be carried out during recognition. It can be set without wearing mask: open the door or do not open the door, it can set continuous temperature test switch.

【 Temperature measurement mode 】 Accurate mode, fast mode, extreme speed mode and default fast mode can be set.

【 Temperature threshold 】 The temperature detection threshold can be set. When the comparison mode contains temperature detection, the alarm will be given if the threshold is exceeded, and the default is 37.3°C

【 Temperature unit 】 Supports two temperature units, namely, Celsius and Fahrenheit

【 Temperature correction 】 Optional intelligent mode and conventional mode;

Intelligent mode: The intelligent mode is that the ambient temperature detected in the low-temperature environment is less than 25°C, and the detected temperature is lower than 36.3°C, which will automatically correct to the normal temperature.

Conventional mode: the ambient temperature is not detected in the conventional mode, and the actual temperature is displayed. If the temperature is lower than 30°C, the temperature measurement fails.

Time period: it is turned off by default, which is actually all day. After it is turned on, it needs to be set in relation to the correction of high and low temperature; otherwise, the time period setting is invalid.

High temperature correction: after turning on, the detection temperature is higher than the set threshold, and it is corrected to normal temperature;

Low temperature correction: the test temperature after being turned on is less than 36.3°C, which is corrected to normal temperature

【 Temperature measurement upper limit 】 The temperature measurement upper limit mode can be set, the default is automatic, and the optional automatic/manual (only T5 module display).

【Upper limit of temperature measurement filter】 The upper limit value of temperature filter can be set (only displayed by T5 module, only displayed when the upper limit of temperature measurement is set to manual).

【Lower limit of temperature measurement filter】 The lower limit value of temperature filter can be set (only displayed by T5 module, only displayed when the upper limit of temperature measurement is set to manual).

【Temperature data】 Can be set to display or not display temperature data on the UI interface.

【Outdoor mode】 The outdoor mode can be set according to the use environment of the equipment (only T4 module is displayed).

【Time period of unexpected temperature】 You can choose the specified time period for protection (the default time is 00:00 to 23:59, and the default state is off)

Access control module:

【White light lamp control】 You can choose to keep the white light on, control the time of the white light, and turn off the white light when no one is present. The white light time control is combined with the turn to day/turn to night time setting on the right side. Default: turn off when no one is present.

【Screen display mode】 Can be selected to display all the time or turn off after no one is present; Default: turn off when no one is present

【List similarity】 Select the similarity of face comparison. If the similarity is too low, false ratio may occur (the default comparison similarity is 75).

【ID card Similarity】 Select the id card comparison similarity. If the comparison similarity is too low, false ratio may occur (the default comparison similarity is 60).

【Fan filter】 The same face recognition filtering time can be set. The default is 2 seconds and the range is 0-10s.

【Time】 Can be set to display or not display the current device time on the UI interface.

【IP】 can be set to display device IP on the UI interface or not.

【Date format】 Three formats of YYYY-MM-DD, MM-DD-YYYY and DD-MM-YYYY can be set, and the default is YYYY-MM-DD.

【 [Comparison of record storage](#) 】 All records and high temperature abnormal records can be selected, and all records are default.

When set to all records, the test temperature comparison results of all persons can be found in the comparison records;

When set to abnormal high temperature record, the measurement temperature comparison result of abnormal high temperature can be inquired in the comparison record;

When it is set to off, the comparison results of all people's temperature-measured will not be able to be checked in the records;

【 [Opening conditions](#) 】 You can choose none, whitelist + face authentication, ID + face authentication, whitelist + ID + face authentication, whitelist or ID + face authentication, IC card recognition, IC card or face recognition, IC card + face recognition

【 [Temperature abnormal setting](#) 】 It can be closed, open the door for temperature abnormal, alarm for temperature abnormal, and be closed by default.

When opening the door with abnormal temperature, the alarm signal will be output if the temperature is normal or high.

When turning on the abnormal temperature alarm, the abnormal temperature record is detected, the record of the person on the blacklist and the record of the person without a mask (set without a mask: when the alarm is raised), and the alarm signal is output. 【 [IC card mode](#) 】 You can choose USB access, WG access and serial port access.

Brake control:

【 [Control interface](#) 】 Optional, close, Weigen interface, switch quantity, Weigen + switch quantity;

Set to off, there is no signal output;

Set as the Wigan interface, and the Wigan signal is output;

Set as the switching value, then there is IO signal output;

Set as Weigen + switching value, there are both Weigen signal output and IO signal output;

Default Weigen + switching amount.

【 [Retention time](#) 】 The IO output duration can be set, with the range of 1-60 seconds, and the default is 1 second.

【 [Door opening action](#) 】 Can choose to open or close normally; Normally on by default.

【Weigen Agreement】 Choose Weigen Agreement: 26, 34; The default is 26 bits.

【Weigen positive and negative sequence】 choose Weigen positive and negative sequence;

The default positive order.

【Printer Settings】 Select close, time + temperature, time + temperature + face image + name;

Turn off by default.

3.3.3 Face Recognition• Equipment Information

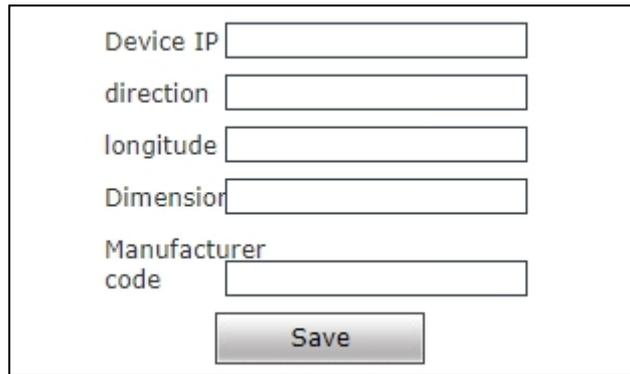


Fig. 3.3.3

Used to display current device information.

3.4 Video Settings

3.4.1 Audio properties

The audio property interface of the access control machine is shown in Figure 3.1.14 below:

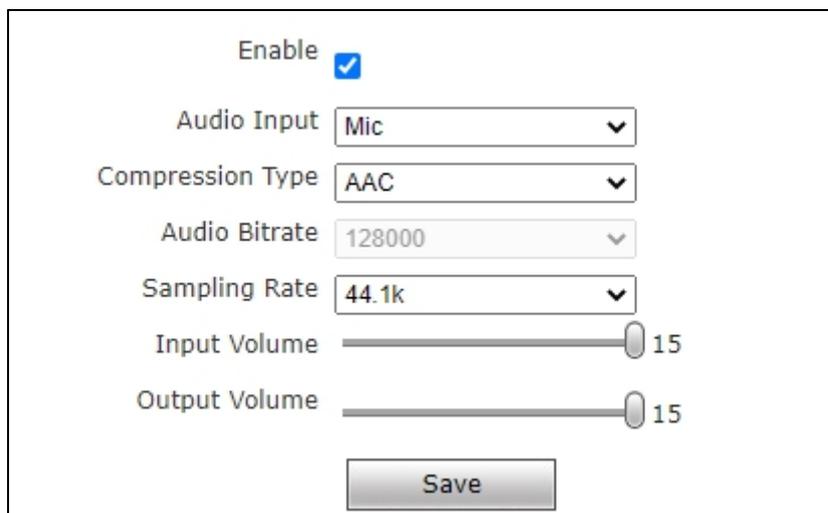


Fig. 3.1.14

【Audio switch】 Can choose to turn on or off the audio switch. When it is turned on, there is voice output when it is recognized. When off, no voice output is recognized. On by default.

【Audio input】 Can choose mike or line input. Default Mike.

【Compression format】 Can be G.726, G.711A, G.711U and AAC compression format, modify the audio compression format, the device will restart. The default ACC, and only AAC compression format, there is voice output.

【Input volume】 Adjust the input volume at the device end to adjust the listening volume of THE PC. The default 15.

【Audio output】 Voice output volume can be adjusted. The default 15.

After setting the parameters, click the "save" button and the setting will take effect.

3.4.2 Video parameters

The video parameter setting of the access control machine is shown in Figure 3.4.2

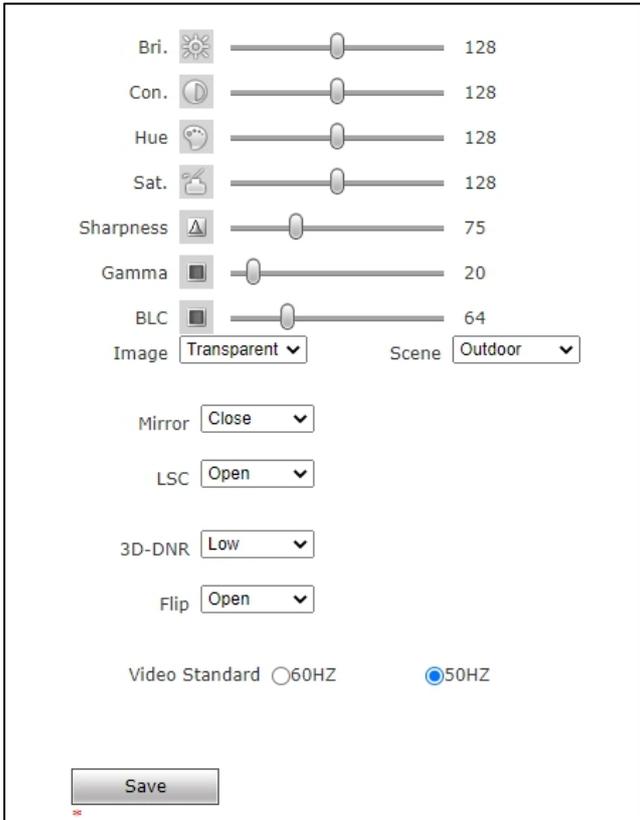


Fig. 3.4.2

Adjust the brightness, contrast, hue, saturation, sharpness, Gamma and compensation

Set the video image and the image flips up and down.

Set lens correction: Adjust lens distortion. When using wide-angle lens, there will be arc change in the four corners in the video. Turning on lens correction can reduce the arc change.

3D noise reduction: Set 3D noise reduction to reduce the shadow of moving objects in low light environment. Drag the bar to set the threshold value of 3D noise reduction starting point.

Set the video to flip and the image to flip left and right.

Video mode: set the lighting frequency of 50Hz and 60Hz to improve the flicker caused by the power supply and the lighting frequency are out of sync. 50HZ corresponds to PAL system and 60HZ to NTSC system.

3.4.3 Video coding

The video coding setting interface of the access control machine is shown in Figure 3.4.3 below:

The screenshot displays the video coding configuration interface, divided into two columns: Main Stream and Sub Stream. Each column contains various settings such as Coding Level, Coding, Face detection resolution, Quality, Advanced options, Rate control, and Bitrate limits. There are also buttons for LAN and WAN settings and a Save button.

Main Stream	Sub Stream
Coding Level: Main Profile	Coding Level: Main Profile
Coding: H.264	Coding: H.264
Face detection resolution: 1920 * 1080	Resolution: 1920 * 1080
Quality: Fine	Quality: Normal
Advanced: <input checked="" type="checkbox"/>	Advanced: <input checked="" type="checkbox"/>
Rate control: VBR	Rate control: VBR
Quality: Better	Quality: Bad
Bitrate limits: (30~16384Kb/S)	Bitrate limits: (30~16384Kb/S)
Bitrate(Kb/S): 4096	Bitrate(Kb/S): 1024
Frame rate(F/S): 25 (1~25)	Frame rate(F/S): 25 (1~25)
GOP(F): 50 (1~200)	GOP(F): 50 (1~200)
LAN... WAN...	LAN... WAN...
Save	

* LAN...:Default. LAN
* WAN...:Default. WAN

Fig. 3.4.3

【Coding level】 Baseline is suitable for occasions with low delay and high real-time requirements; Main Profile is suitable for situations where there is no special requirement on real-time performance and high requirement on image quality. The High Profile supports

more features than the Main Profile, allowing for a higher compression ratio and smaller video files of the same quality.

【Coding algorithm】 H.265, H.264 and MJPEG are optional.

【Resolution】 Set the resolution of the image here.

【Video Effect】 Users can select the appropriate image quality according to their needs: best, good and general, or they can customize each parameter after checking the box of "Advanced Settings".

【I frame interval】 The number of I frame intervals is adjustable from 1 to 200 (primary stream) and from 1 to 200 (secondary stream). The smaller the number of frame intervals, the higher the image bit rate and the better the image quality. It is generally recommended to set the I frame interval above 25.

【Frame rate】 Sets the encoding frame rate per second. When the network condition is not ideal, the frame rate can be reduced to control the code rate so as to make the moving image smoother.

【Bit rate control】 Fixed code stream (CBR) and variable code stream (VBR) are optional. CBR adopts constant bit rate coding and VBR adopts variable bit rate coding.

【bit rate】 The setting range of primary and secondary streams is 30 ~ 16384Kbps. The higher the bit rate setting is, the better the image quality will be, but the bandwidth utilization will also increase. Please adjust the setting according to your actual bandwidth situation.

Under the fixed bit rate setting: **【bit rate】** represents the constant bit rate value of the current code.

Under the variable code rate setting: **【code rate】** represents the maximum code rate value allowed.

【Image quality】 Under the fixed bit rate setting: set the fluctuation range of the bit rate through **【Image quality】**, and you can choose to control it by yourself.

In the variable bit rate setting, the image quality is set through **【image quality】** to provide multiple levels. The higher the level is, the better the image quality will be, but the upper limit will not exceed **【bit rat】**.

【Default value of LAN】 I frame interval is 25, frame rate is 25, bit rate control is

【Wan default value】 I frame interval is 25, frame rate is 5, bit rate control is fixed rate, bit rate is 384kbps, image quality is 2.

After setting the parameters, click the "save" button, and the setting will take effect (if the resolution is changed, the device may restart).



Note: Non-professional users should use advanced Settings with caution.

4 List Management

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

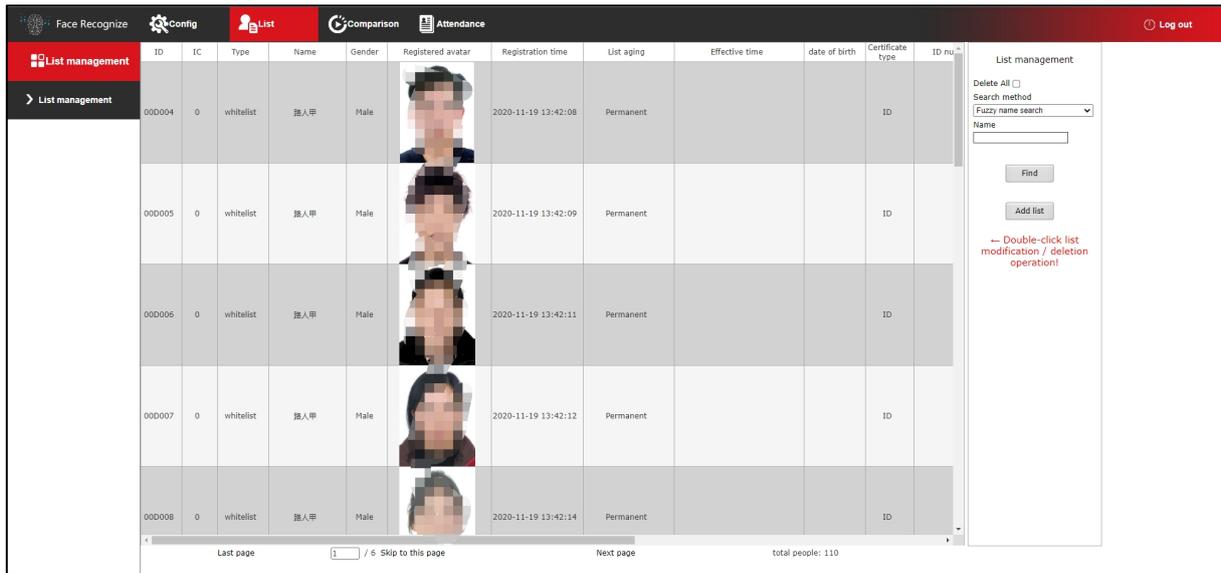


Fig. 4.1.1

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

Step 5: Select list for aging. Step 6: Click on Save



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

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

Condition							
2020 - 4 - 20	0:00	2020 - 4 - 21	16:16	owner	Name	number	Search
Routing Mac	name	Serial number	list	body temperature	time	IC	Detailed situation
	-	-	Guest	36.50	2020-04-21 16:15:50		Mask:NO ,body temperature:Normal
	115	46567	whitelist	0.00	2020-04-21 16:15:48		Similarity:90%,Visits:7,Time of first visit:2020-04-21 16:14:25,Mask:NO ,body temperature:NO
	-	-	Guest	36.60	2020-04-21 16:15:36		Mask:NO ,body temperature:Normal
	70	46567	whitelist	0.00	2020-04-21 16:15:35		Similarity:90%,Visits:6,Time of first visit:2020-04-21 16:14:25,Mask:NO ,body temperature:NO
	-	-	Guest	36.60	2020-04-21 16:15:22		Mask:NO ,body temperature:Normal
	115	46567	whitelist	0.00	2020-04-21 16:15:21		Similarity:91%,Visits:5,Time of first visit:2020-04-21 16:14:25,Mask:NO ,body temperature:NO

[Last page](#) 1 / 268 [Skip to this page](#) [Next page](#)

Fig. 5

6 Attendance Record

Attendance record of any day or any period can be queried

Face recognition.

Set Time							
Sunday	go to work	06:00	09:00	off duty	18:00	Advanced	save default
Working days setting		<input type="checkbox"/> On Sunday <input checked="" type="checkbox"/> On Monday <input checked="" type="checkbox"/> On Tuesday <input checked="" type="checkbox"/> On Wednesday <input checked="" type="checkbox"/> On Thursday <input checked="" type="checkbox"/> On Friday <input type="checkbox"/> On Saturday					
2020 - 4 - 21		2020 - 4 - 21		Name	number	Attendance status	query type
						all	record
Routing Mac	name	Serial number	Detailed situation				
	115	46567	Attendance Date:2020-04-21,Working hours:16:14:25,Work status:Late,off time:16:17:41,After work status:Leave early				
	70	70	Attendance Date:2020-04-21,Working hours:00:00:00,Work status:Not Attendance,off time:00:00:00,After work status:Not Attendance				
	58	58	Attendance Date:2020-04-21,Working hours:00:00:00,Work status:Not Attendance,off time:00:00:00,After work status:Not Attendance				
	42	42	Attendance Date:2020-04-21,Working hours:00:00:00,Work status:Not Attendance,off time:00:00:00,After work status:Not Attendance				
	091	091	Attendance Date:2020-04-21,Working hours:00:00:00,Work status:Not Attendance,off time:00:00:00,After work status:Not Attendance				
	110	110	Attendance Date:2020-04-21,Working hours:00:00:00,Work status:Not Attendance,off time:00:00:00,After work status:Not Attendance				

[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.

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

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).

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.

7. 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

8. 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

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.

2. 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.