CAN-AM

CAN-AM Linux Access Control with AI Thermal detector

User Manual

- Temperature Detection
- Dual Lens Face Recognition
- 7 inch LCD Screen
- Speaker
- Bracket
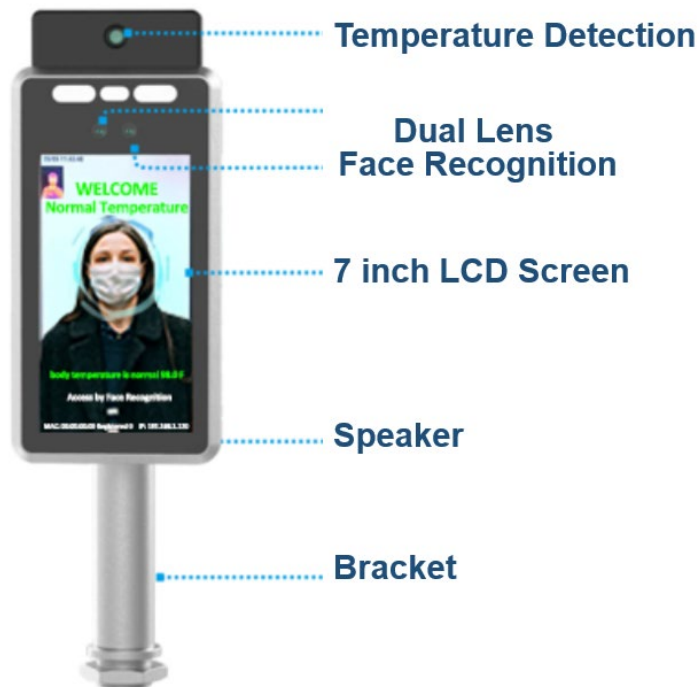
Model: Hero-BK-PM

CONTENTS

1. Product Overview

1.1 Product Introduction

CAN-AM Access Control with AI thermal detector Hero-BK-PM adopts the new AI chip-set, large thermal sensor array, and latest algorithm, providing the cutting-edge face recognition and body temperature detection, with ability to detect wearing the mask. Hero-BK-PM can identify human forehead automatically from 0.3meter ~1.2meter to get ±0.3℃ high accuracy body temperature within 0.05second.

1.2 Product Functions

● Proximity wake-up activation: the device is automatically activated when a person approaches.

● 7-inch touch screen: displays the software interface, operation guidance and face frame. Performs real-time face detection (supports local video preview).

● 2 million pixel binocular wide angle camera.

● Anti-fake function for pictures and videos.

● Facial recognition distance of up to 1 meter, for a height range of 1.4m to 1.9m.

● Use of deep learning algorithms to support a capacity of 50,000 faces. Fast recognition with a higher recognition rate.

● Storage of up to 50,000 events.

● Multiple authentication methods.

● Facial comparison time ≤ 0.5s/person. Recognition rate ≥99.9%.

● Support for importing of card and facial data to devices through TCP/IP transmission or USB interfaces.

● Uploading of data through the internet.

● Uploading of comparison results and interconnected snapshots to the platform for storage.

● Personnel information can be sent down from the platform or uploaded from local devices.

● Stand-alone operation in offline mode.

● Local login for managing, searching and configuring device parameters.

2. Wiring instructions

Face recognition terminal can be docked through the tail line access control locking, in the retention of existing access control system function of the colleague, the access control intelligent operation upgrade. It is possible to simulate the opening of the door with the PUSHOUT signal and directly drive the electromagnetic anode or cathode locks with the LOCKNONC signal.

For direct drive of Anodic or cathodic locks, a 12V/2A switched power supply is recommended.

Note the following while wiring.

● If 1.0mm national standard wire is used, 12V switching power supply is used, and the wiring

distance from the site construction (switching power to equipment distance) does not exceed 20m.

- If 1.5mm national standard cable is used, 12V switching power supply is used, and the wiring distance from the site construction (switching power to equipment distance) does not exceed 30m.
- If 2.0mm national standard wire is used, 12V switching power supply is used, and the wiring distance (switching power to the equipment distance) is not more than 40m.

2.1 Wiring instructions
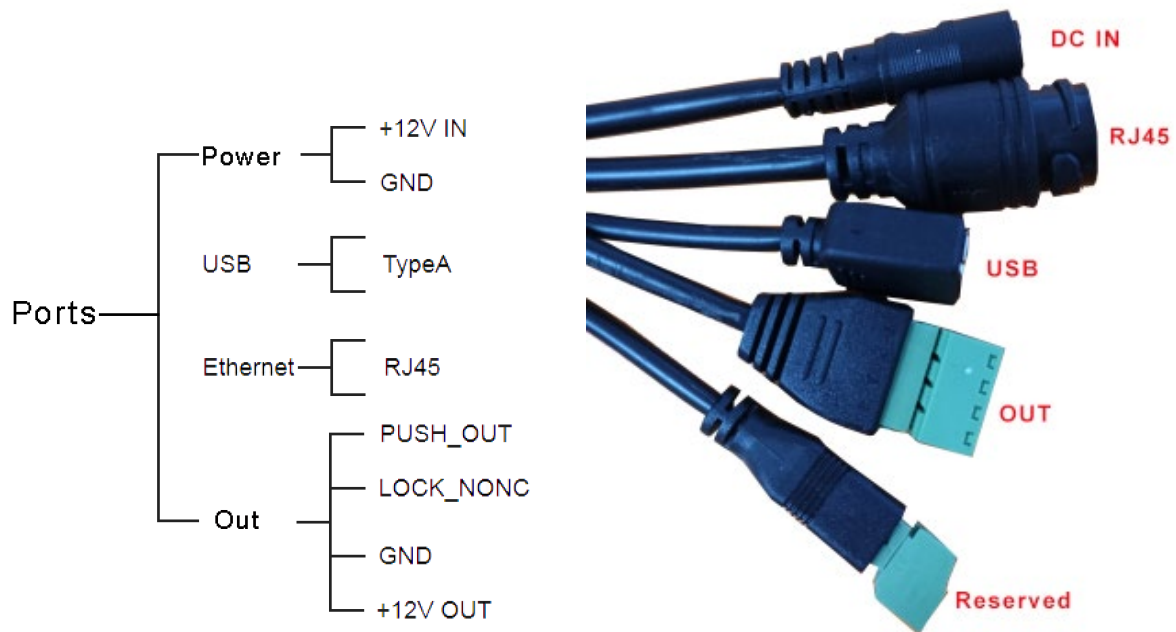
The wiring instructions are shown in the table below.

Wire Description	Function	Wire sequence	Name	Description
A DC IN	POWER	1	12VDC in	12V power supply, 2A
		2	GND	Ground
B Type-A USB	USB Host	1	5V	Only used for factory testing.Do Not connect it.
		2	DN	
		3	DP	
		4	GND	
C RJ45	Ethernet	1	Ethernet	Standard 100 megabit network port, connect to PC for configuration.
D OUT-4pin	lock control signal	1	PUSH_OUT	Switching Level Output
		2	LOCK_NONC_12V	12V switching drive output
		3	GND	Ground

		4	12V out	12V power output
E 2 pin	Reserved	1		N/A, don't connect anything!
		2		

Precautions：

1). Pin 4 (12V out), current limit output 1A, load beyond power, will cause panel machine hardware damage.

2). Pin 2 (LOCK_NONC_12V), current limit output 800mA, beyond the power of the latch access, will cause panel machine hardware damage.

3). Pin 2 (LOCK_NONC_12V) and pin 3 (GND), please do not short-circuit, otherwise it will cause hardware damage to the panel machine.

4). Pin 1 (PUSHOUT) and pin 4 (12V out), please do not short-circuit, otherwise it will cause hardware damage to the terminal.

2.2   Connect the device to PC

Connect the network cable via RJ45 to your PC directly or router.
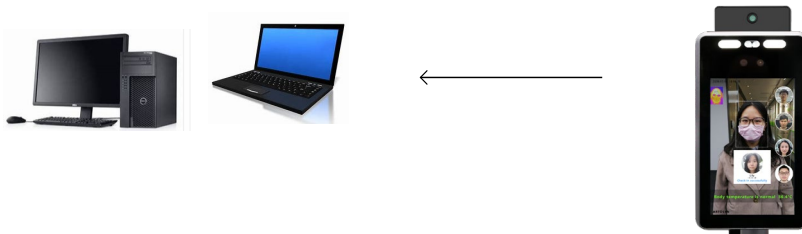
The default IP address of device is 192.168.1.100, and it supports DHCP as default mode.

A. If there is a router, you can connect the device to router via RJ45 cable. Then you will get the current IP address on the TFT screen, then search this device via your PC's ARfacemanger (You PC should be in the same router).

B. If there is a wireless router. You can only add the 192.168.1.*** IP segment in Advanced as the following pictures. And connect the device to your PC directly, then search and set it via ARFacemanager.
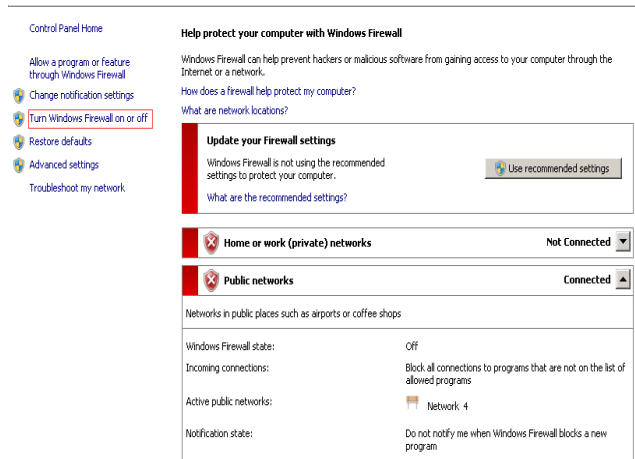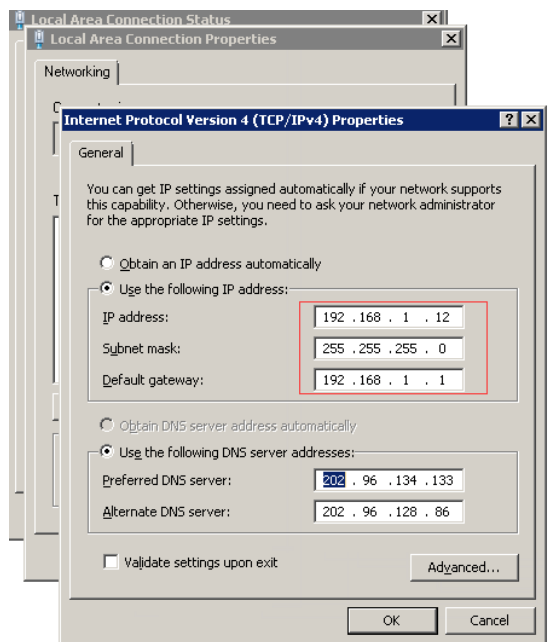
3. *Turn off firewall of your PC （fWindows 10 OS）. After you configure it, you can turn the firewall on again.This is only affect the search IP address of device. If not turn it off, you can add the device by manually.*

## 2.3 Connect the Lock of door (Push_out)

A. Conventional access control system, generally with a button to open the door function, it is recommended that the terminal PUSHOUT terminal directly and connected to the open the door button wiring, in line with the permission to open the door action through PUSHOUT directly simulate the button grounding operation, does not affect the original door button function.
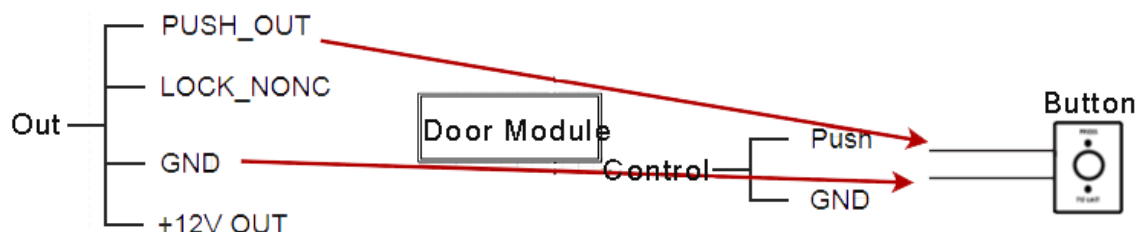
2.4 Wiring instructions（LOCK_NONC_12V ）

The hardware wiring is as follows, the switching quantity signal can be directly output 12V, no external power supply is required to power the lock.

Note: The original door controls cannot be unlocked when the power is removed.
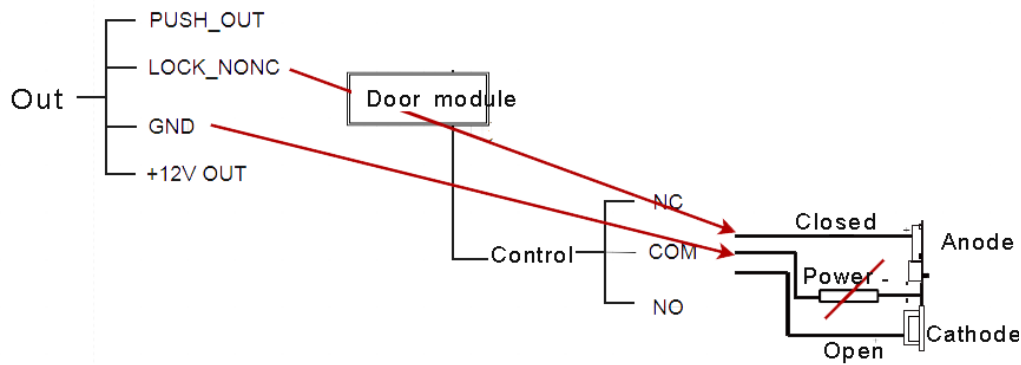
Anode Lock

Software Configuration: In the ARFaceManager tool, go to ***3.2.8 Device Access Control Parameters*** and set the door magnet type to "**Normally Closed**".

Cathode Lock
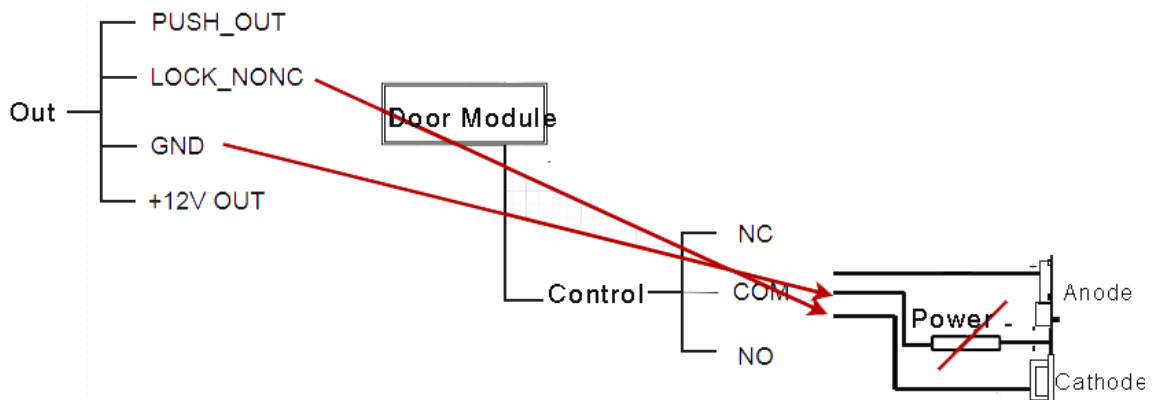
Software Configuration: In the ARFaceManager tool, go to ***3.2.8 Device Access Control Parameters*** and set the door magnet type to "**Normally Open**".

3. Client operations

You can set up and operate your device through client ARFaceManager.exe. This chapter introduces the functions and operating procedures of access control.

The main interface contains System menu, 4-channel preview interface, identified staff info (temperature, mask, name) and UN-identified staff info (temperature, wear mask or not).
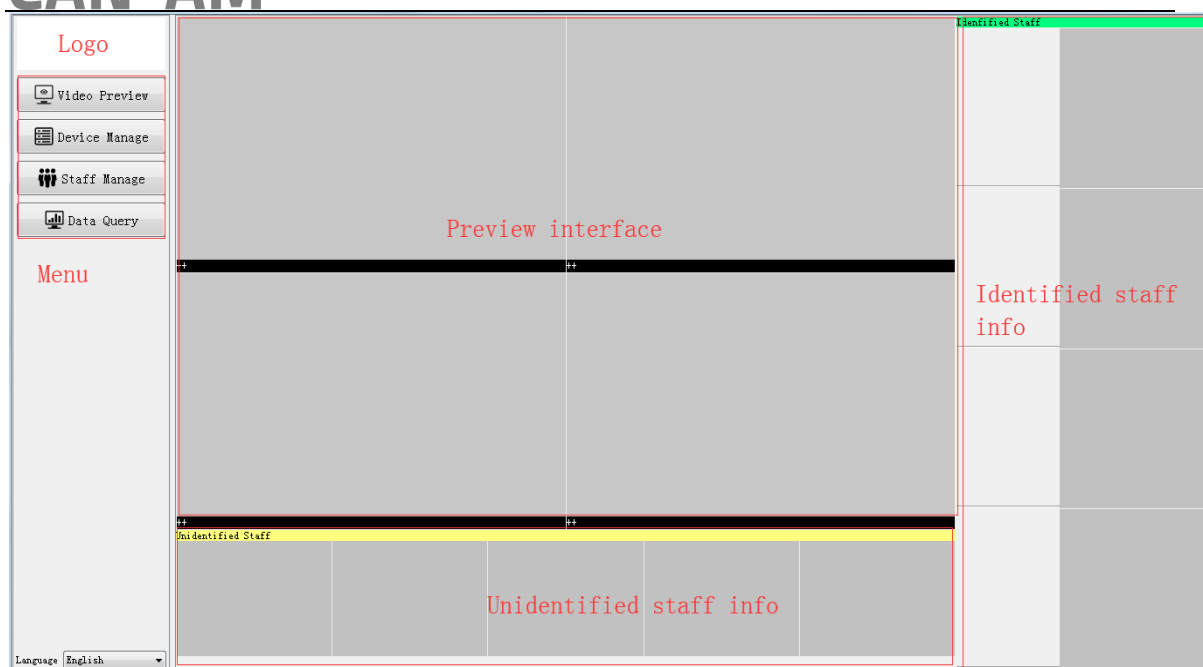
Video Preview: You can get the live streaming info;

Device Manage: Search, edit and set the device.
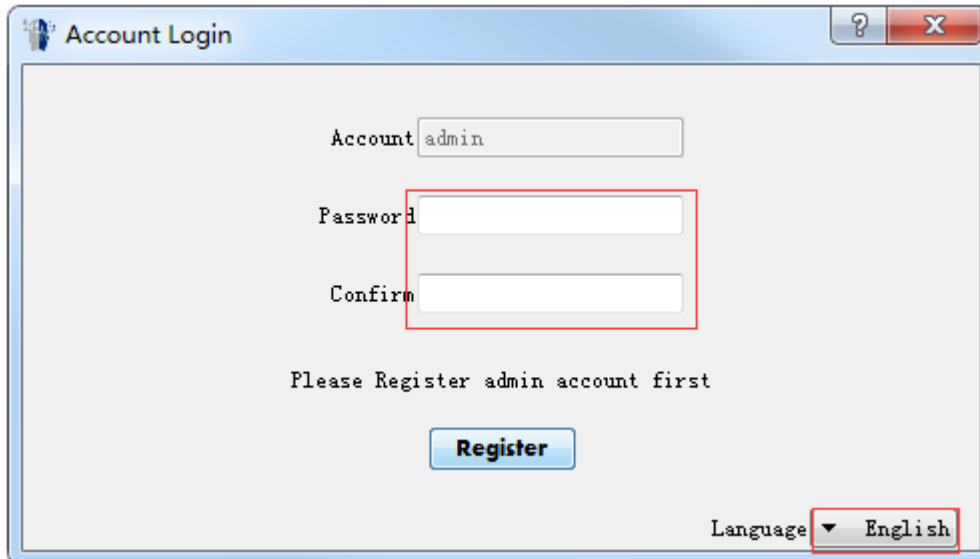
Staff Manage: Add/edit/delete the staff personal info, and authorize the door-Lock function.

Data Query: Export the attendance of registered staff.
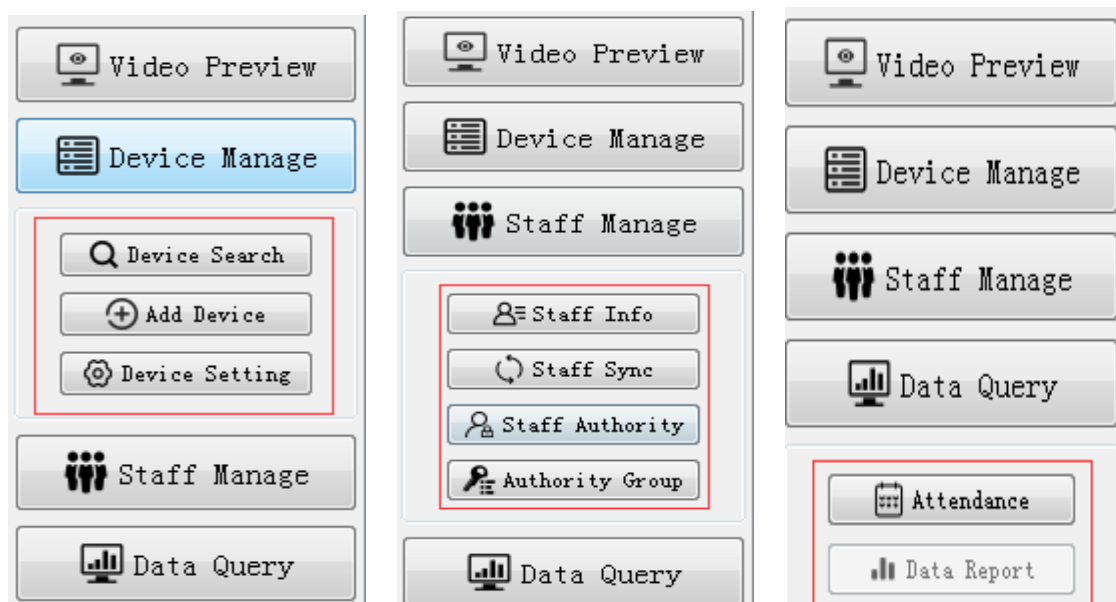
3.1 Device Management

3.1.1 Login
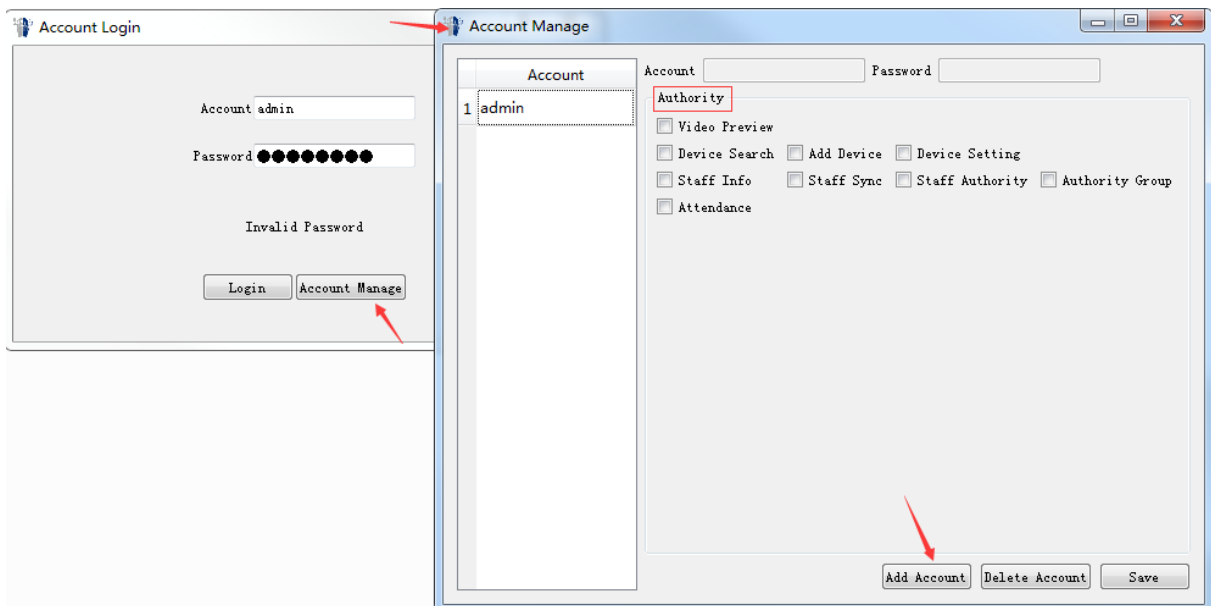
For the first time login, you need set a password (**Six characters at least**) for admin account. After login on, you can create sub-account, and set the role for the sub-account.

Add sub-account, input the user and password. Select the Authority(role) for this account.
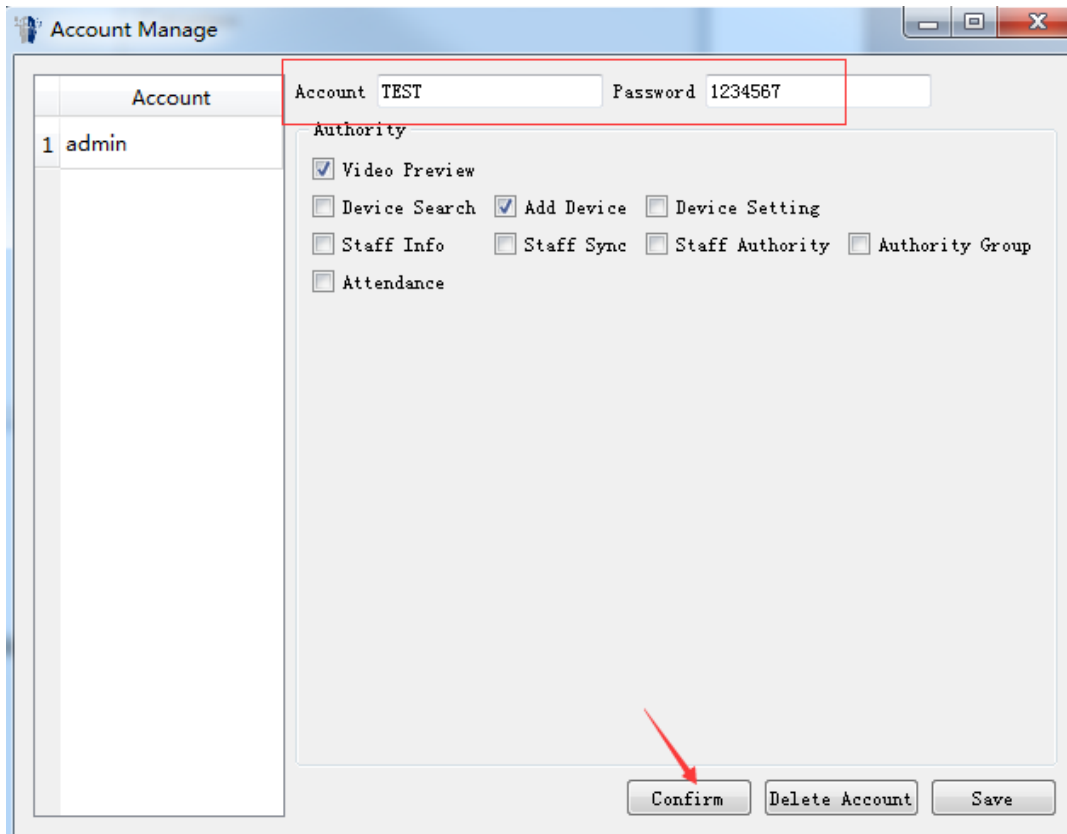
Delete account. Select it first, then Click "**Delete Account**".
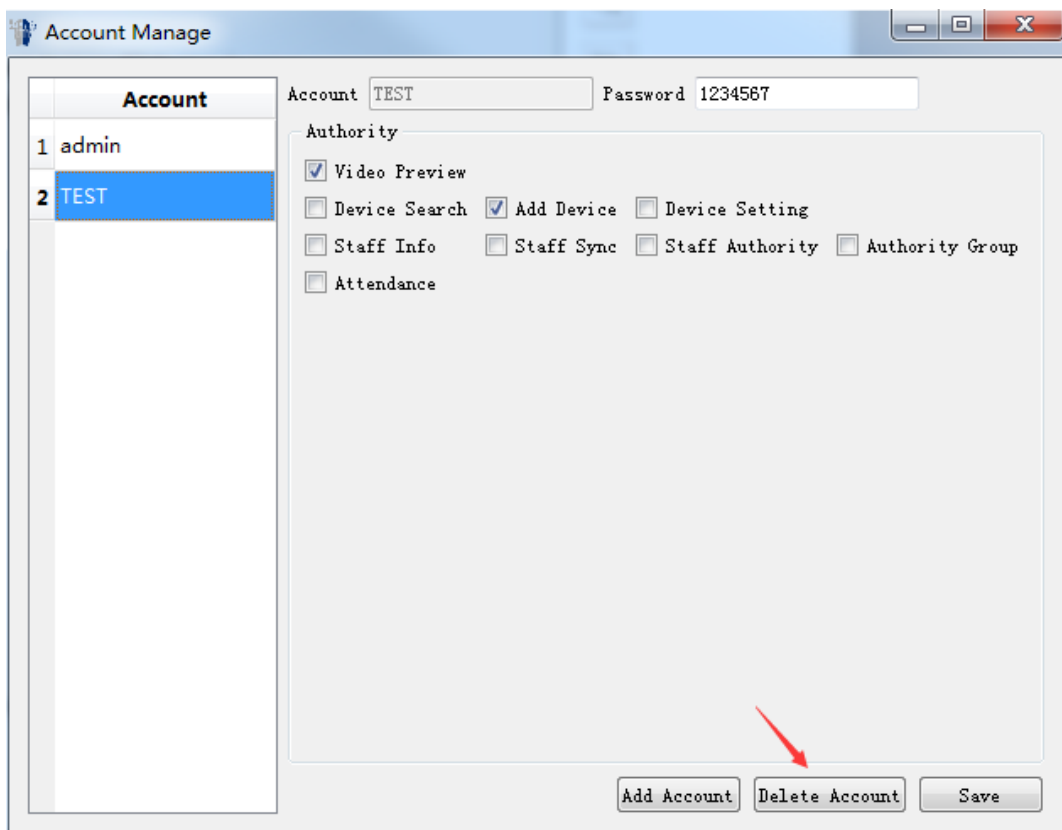
3.1.2 Adding Device

1) On the left side of the control panel, click Device Management -> Search Device
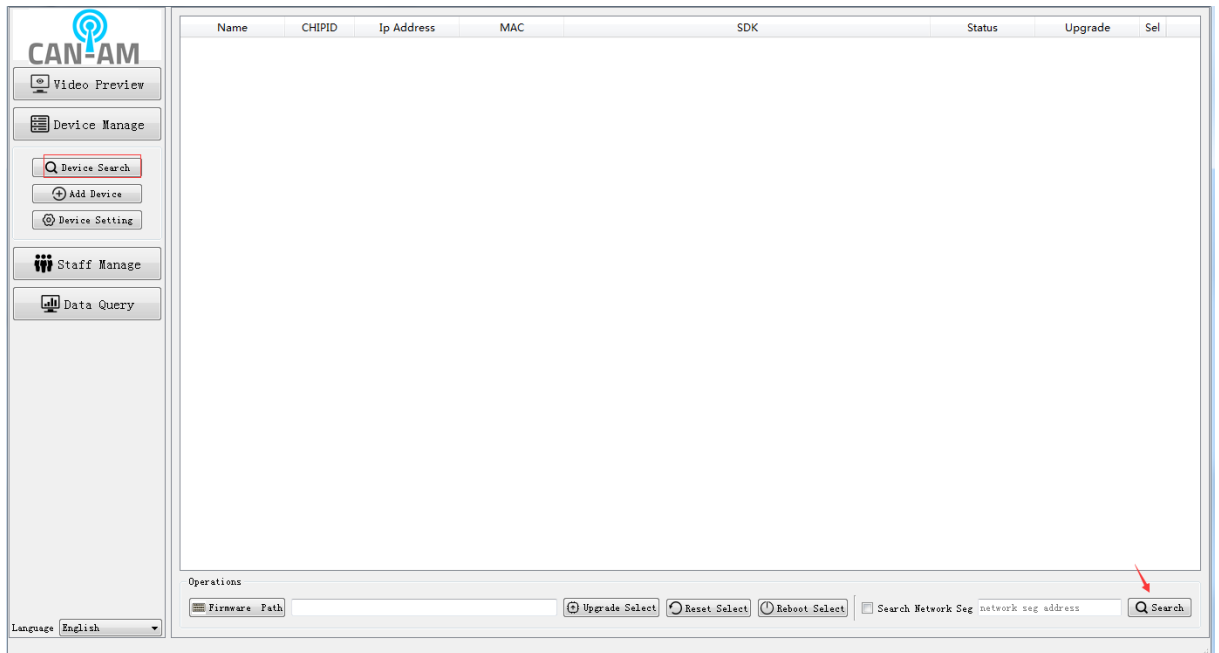
2) Click Device Management -> Add Device
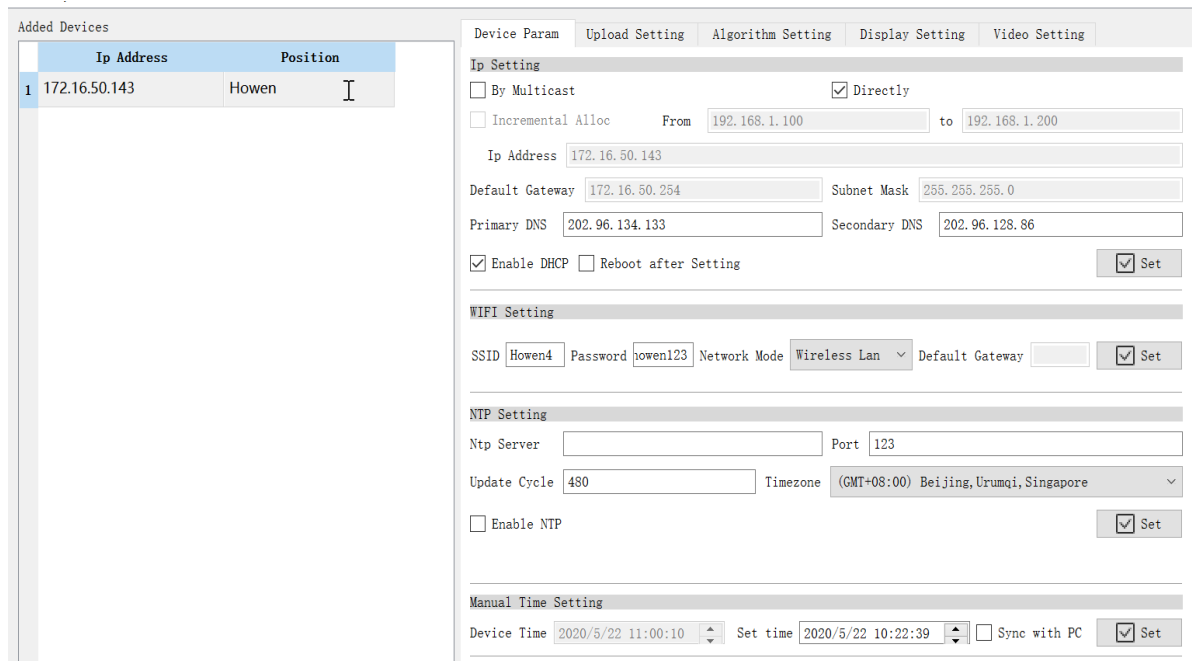
Select the camera you want to add, fill in the device name (required) and position (required), and click "Add select". You can also delete it via " Delete".
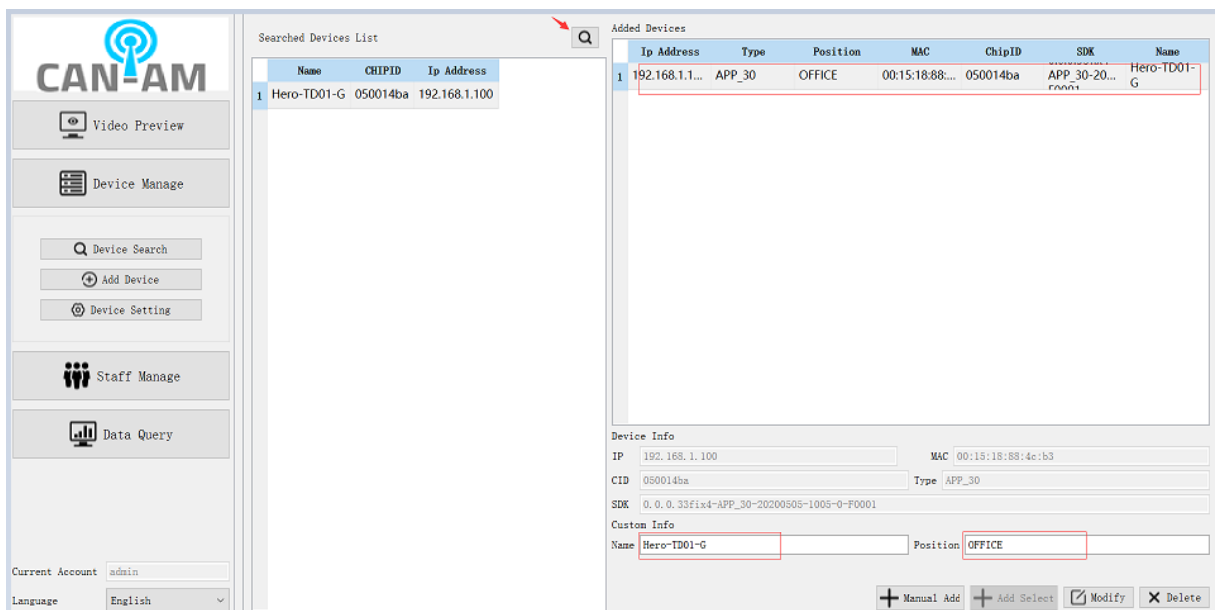
3.1.3 Device Settings

Device settings includes device parameters, upload settings, algorithm configurations, display configurations, and video settings.

3.1.3.1 Device parameters

- IP setting

★ DHCP mode

No need to set, you can get the IP address directly when you connect the RJ45 cable to router. The IP address will display at the bottom of Screen of device.

★ Static IP address settings

1. Check "Directly".Untick "Enable DHCP".

2. Configure unified IP address, Subnet Mask and DNS information, *you can change the IP address as required*. Click " Reboot after setting" .The default IP address is 192.168.1.100.

3. Click "Set up". The parameters will be synchronized to the device.

- WIFI settings:(Not Recommend)
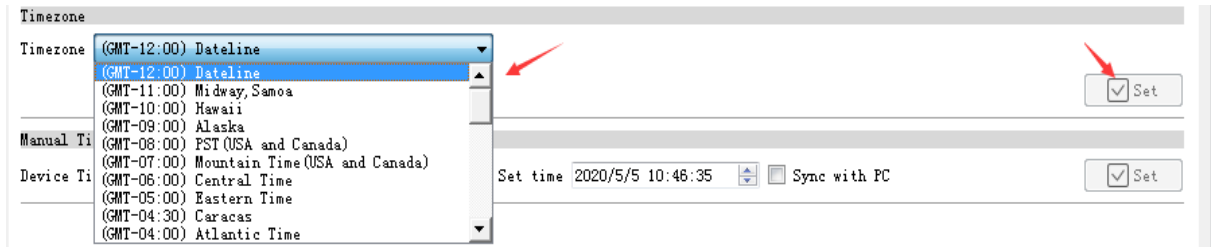
    Input the WIFI SSID and password.

★ Date and time setting, use one of the following to set.

- NTP settings:

1. Configure the NTP server IP address, port number, update cycle and time zone.

2. Check "Enable".

3. Click "Set Up". The parameters will be synchronized to the device.

- Time zone
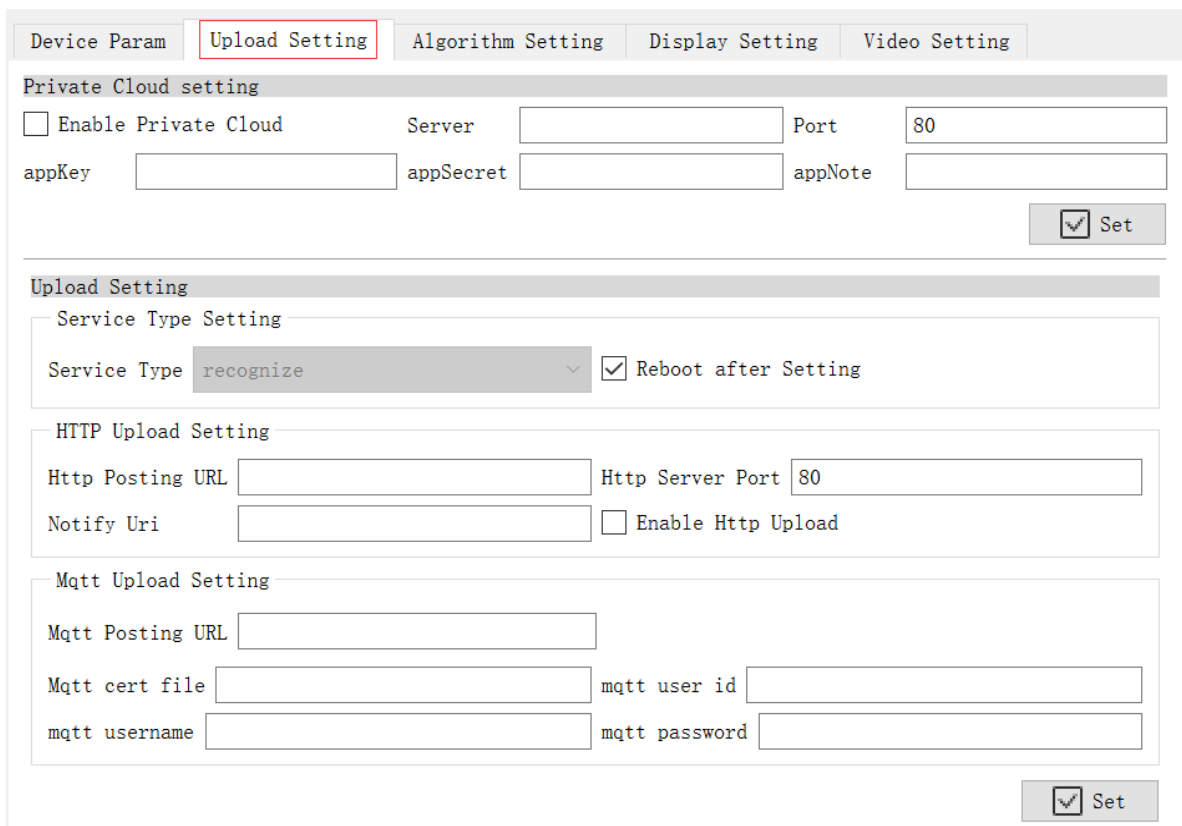
- Manual time setting

Synchronize with your PC's time.

3.1.3.2 Upload settings (Need develop or integrate the protocol)
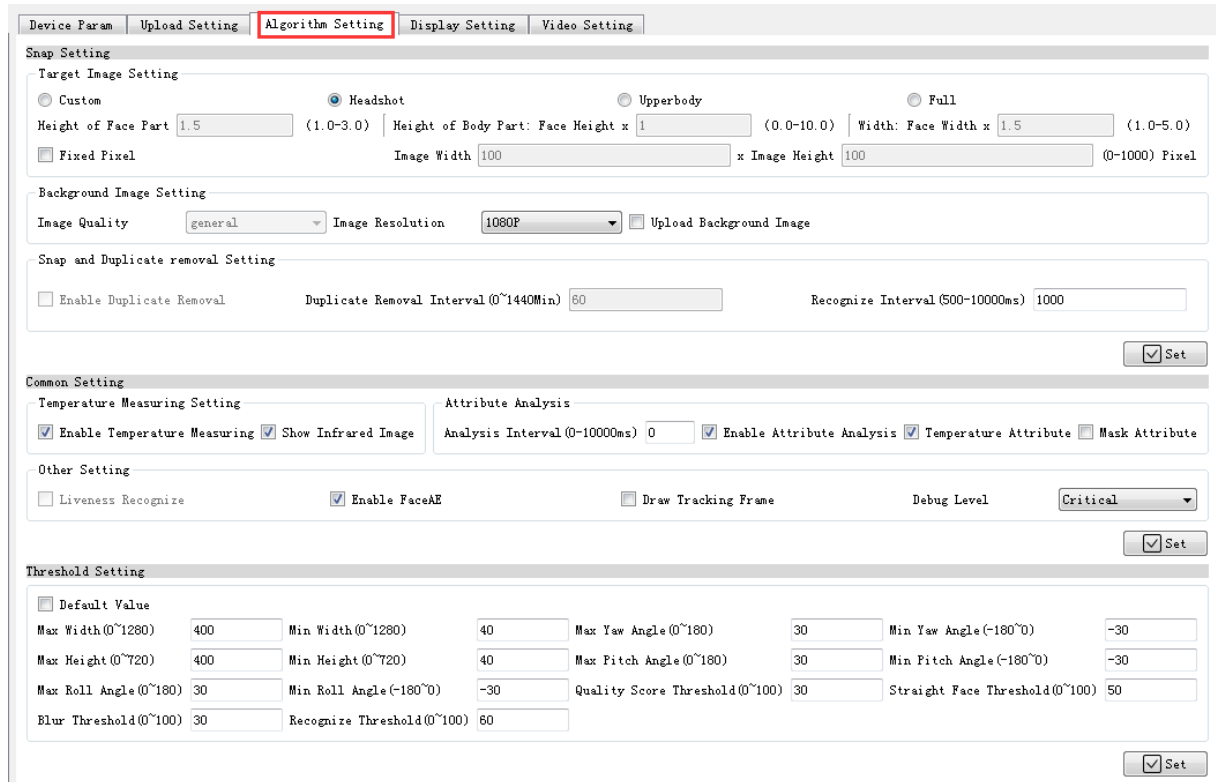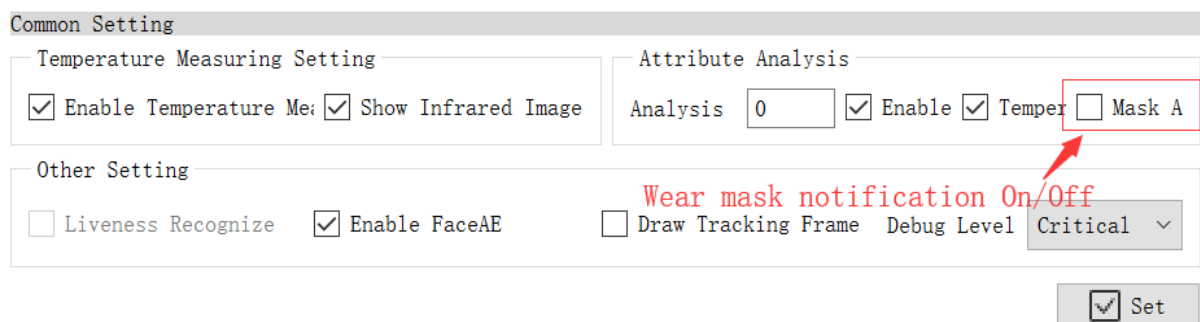
- Upload settings

Server type: Supports snapshot mode and recognition mode.

Supports simultaneous Http and mqtt uploading.

3.1.3.3   Algorithm settings

- Target image settings: Set the staff faces(picture)'s attribute. Keep the default setting.

- Background image settings: No need to set.

- <mark>Common settings</mark>

Temperature Measuring setting: Enable them.

Show Infrared Image: The infrared window will appear on the right top of Screen. Turn it on/off.
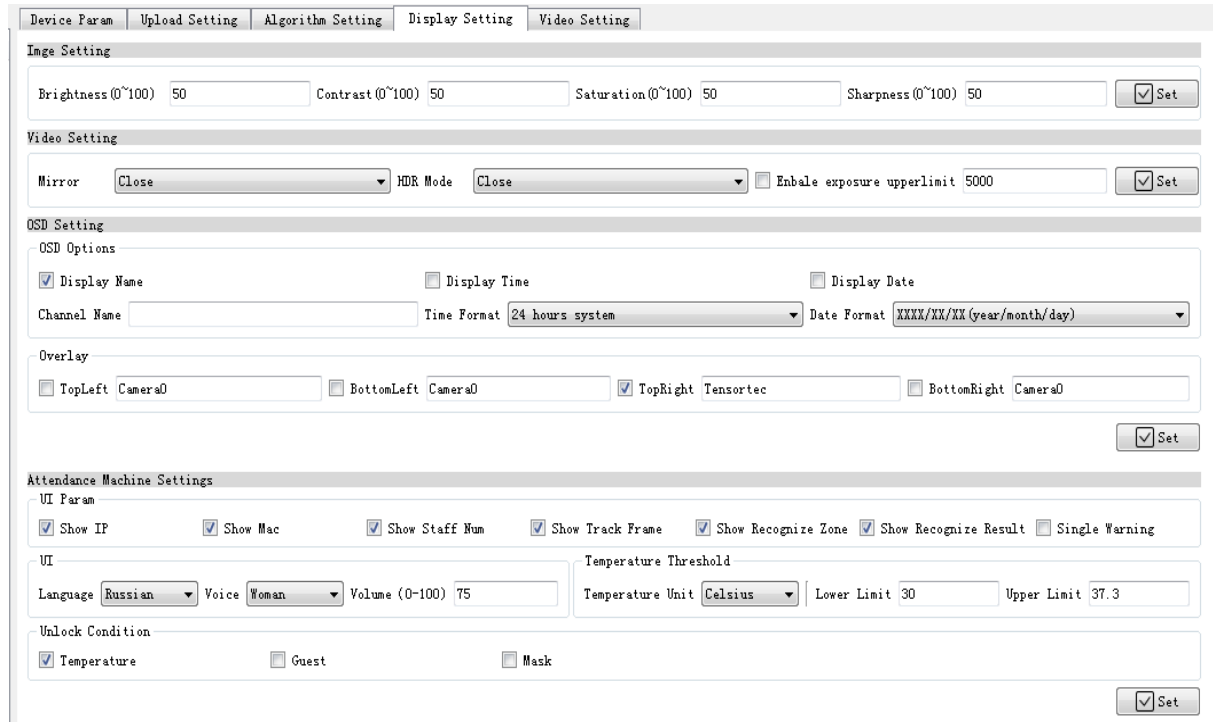
Enable FaceAE: Turn on/off the face recognition under back-lighting environment.

Mask Attribute: Turn on/off the wear mask notification.

After you set them, click " Set" to save the settings.

- Threshold settings --- Algorithm's threshold setting. Keep the default setting.

3.1.3.4 Display settings

- Image settings

- Video settings: You can mirror the preview image.

- OSD settings

Edit it, and check these OSD info (Name, Time & Date), then it will display on the preview image. Click "Set" to save.

- UI Param

15

Attendance Machine Settings
UI Param

☑ Show IP   ☑ Show Mac   ☑ Show Staff Num   ☑ Show Track Frame   ☑ Show Recognize Zone   ☑ Show Recognize Result   ☐ Single Warning

Single Warning: Turn off multiple notification for one person per time, it will only announce one time if he stands in front of the camera for a long time.

● Unlock Condition

Unlock Condition

☑ Temperature   ☐ Guest   ☐ Mask

There are 8 kinds of conditions

1. Temperature: The registered staff who temperature is normal could open the door
2. Mask: The registered staff who wear the mask could open the door
3. Guest: Anyone could open the door, no matter the temperature/mask is normal or abnormal
4. Temperature+Guest: Anyone who temperature is normal could open the door.
5. Mask+Guest: Anyone who wear the mask could open the door.
6. Temperature+mask: The registered staff who temperature & wear mask could open the door.
7. Temperature+mask+Guest: Anyone who temperature is normal & wears mask could open the door.
8. Nothing selected:The registered staff in white-list or authority group, who temperature is normal & wear a mask could open the door.

● Temperature Threshold setting

Input the threshold of temperature, and select Celsius or Fahrenheit.

● Language of notification setting (Multiple notification language can be customized)
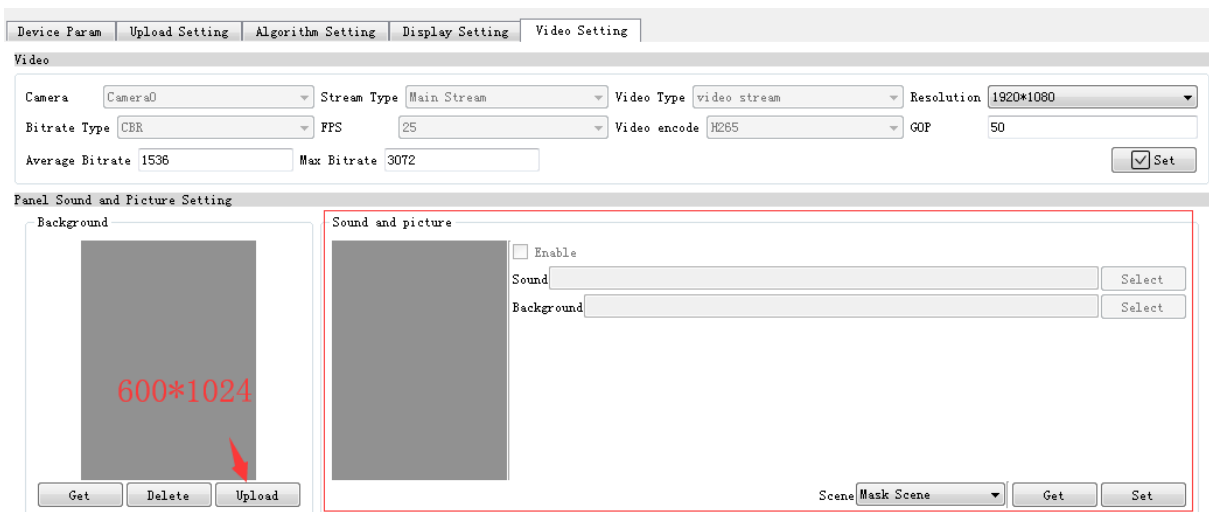
Change the language type, voice type and save it.

Volume: Notification volume.

3.1.3.5   Video setting

Video settings supports changing Resolution, Bit-rate of video.

You can customize the background picture of LCD panel via Upload BG Image （**Size：600*1024 PNG**）

Customize Picture and Audio

Mask scenario: Enable it, and customize the picture or audio when someone is not wearing the mask;

Temperature scenario: Enable it, and customize the picture or audio when temperature is abnormal;
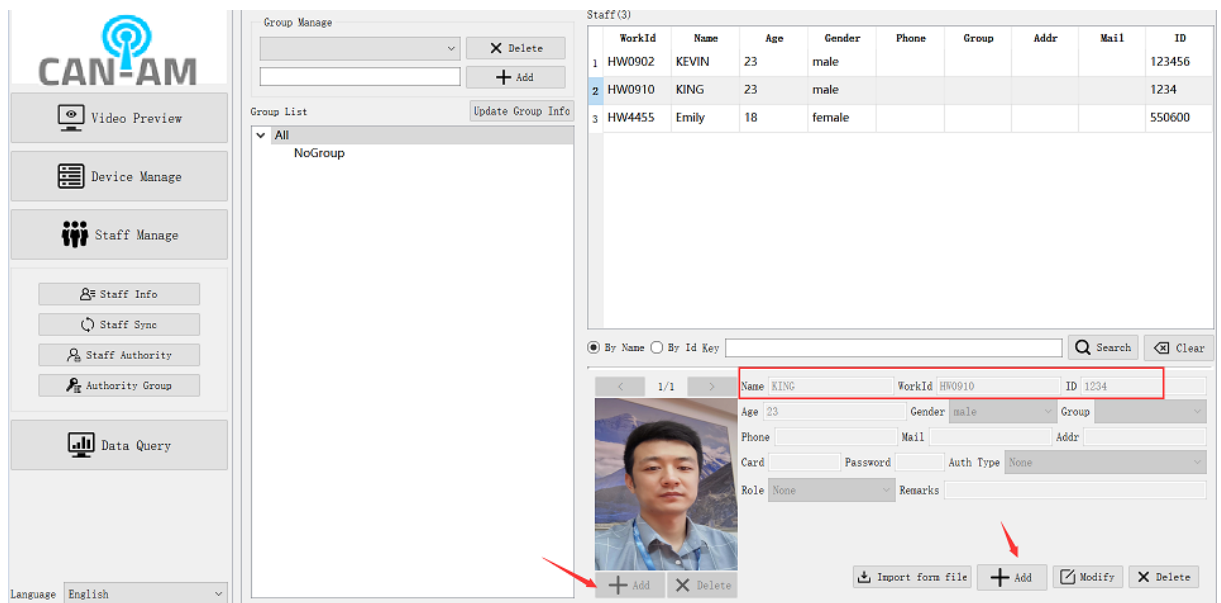
Pass Scenario: Normal (temperature is normal and wear mask) status's picture and audio.

Attention: This customization notification is for anyone, no matter he have been registered or not.

3.2 Staff Management

3.2.1   Adding Staff

1. On the left side of control panel lick Staff Manage -> Staff Info

2. Click "Add". The staff information display zone becomes available for editing.

3. **Name, workId , ID, photo** are mandatory fields. The other fields are optional.

4. Click "Add". The data will be stored in the client software and local database.

Picture Requirement：

1. Turn off camera beauty function of your smart-phone, to ensure that the picture for the real face, no makeup or edited, no wear a mask.
2. The shooting background is solid color and other walls, the light is normal, avoid strong light, reverse light and other abnormal light.
3. There is only one person in the picture, the front (face is not biased, both ears visible, the head is completely visible), shooting distance of about 1 meter, in the picture, the head of the person must have a head distance from the left and right upper three sides.
4. Face pixels more than 260(between the two ears), determine the face size can use the windows drawing software to open the face picture, drag a box on the face, will show the face size. Mobile phone shooting can be satisfied.

Recommended minimum picture specification:
- 96 dpi
- 442px by 495px
- Head and shoulder shot (face fills approximately 75% of frame)

Reference Image:
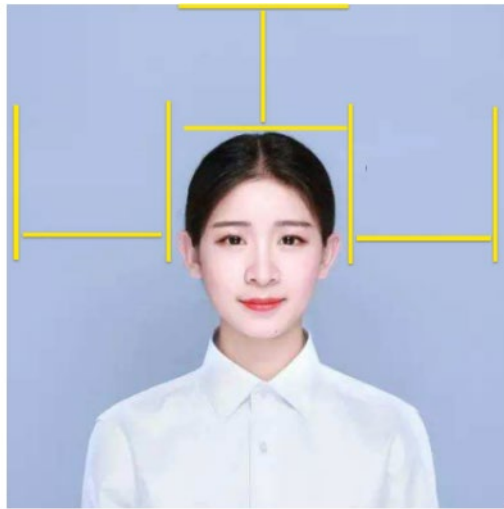
3.2.2　Batch-adding From file

　　1.　Click Staff Manage -> Staff Info on the left side of control panel.

　　2.　Click "Import from file" and select a pre-edited Excel document of user information. You can refer to the example template document HW_staff.*xlsx* in configuration tool.
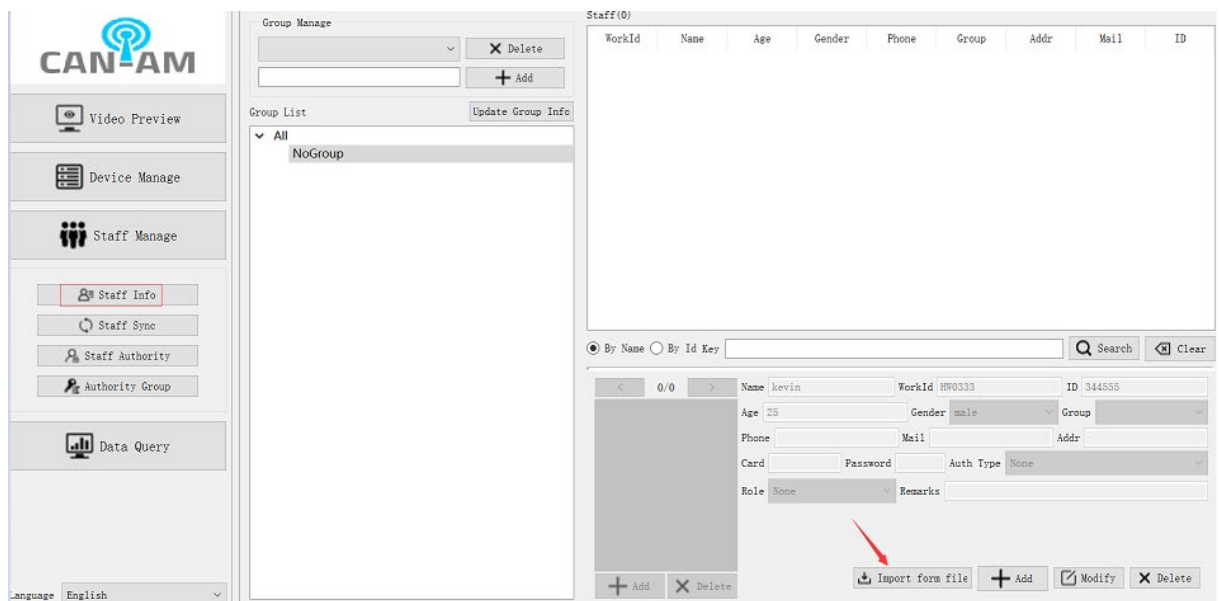
　　3.　Click "Open" and complete the import.

Notice: You can refer to our Excel file's format, and set the pictures' path, then import them.

3.2.3　Edit Users

Attention: If you edit or change the Name and Work ID, the system will deem it's another staff. So

<u>if any wrong message of Name and work ID, you can delete this user, then add again.</u>

For other info, you can change it directly.

1. On the left side of control panel, click <mark>Staff Manage</mark> -> <mark>Staff Sync</mark> , then select the list .

2. Click "<mark>Modify</mark>". The personnel information display zone becomes available for editing.

3. Click "<mark>Modify</mark>" after editing. The data will be stored in the local database of the client.

<mark>Attention</mark>: ***After you edit the user, need synchronize with device end***, *please follow with* <mark>3.2.5</mark> <mark>Staff Sync.</mark>

3.2.4   Delete

● Single removal

1. Select the user to be removed.

2. Click "<mark>Delete</mark>".
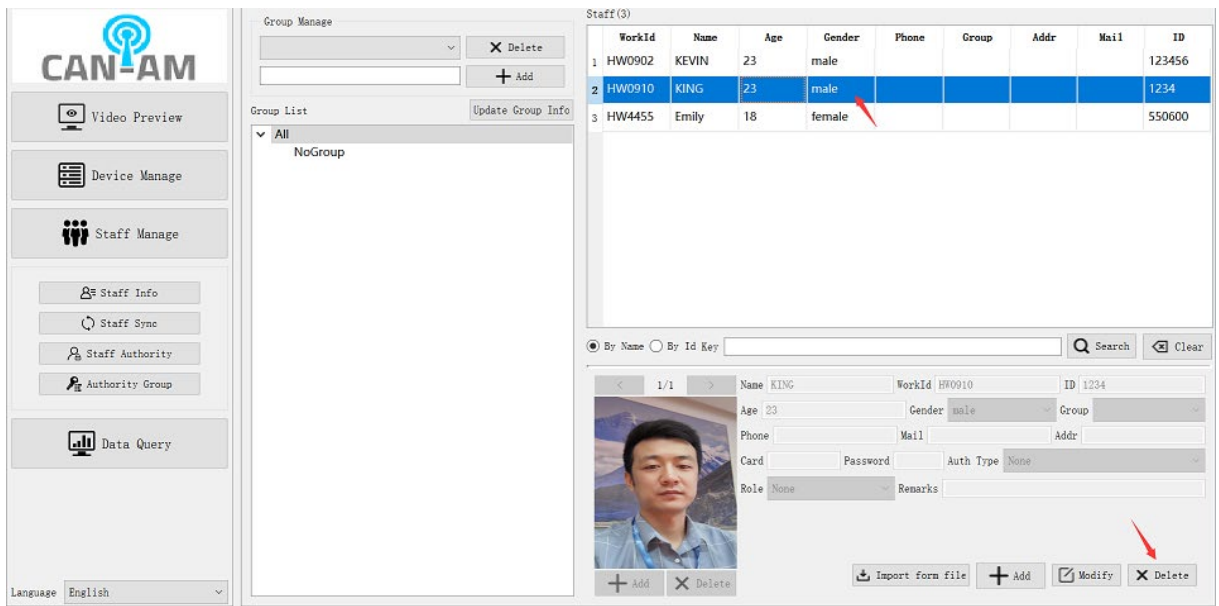
- **Batch Delete**

    1. Select multiple users by pressing **Ctrl** key or select all by pressing Ctrl+A of keyboard.

    2. Click "Delete" to delete all users.

3.2.5 Staff Sync

On the left side of control panel, click Staff Manage -> Staff Sync.
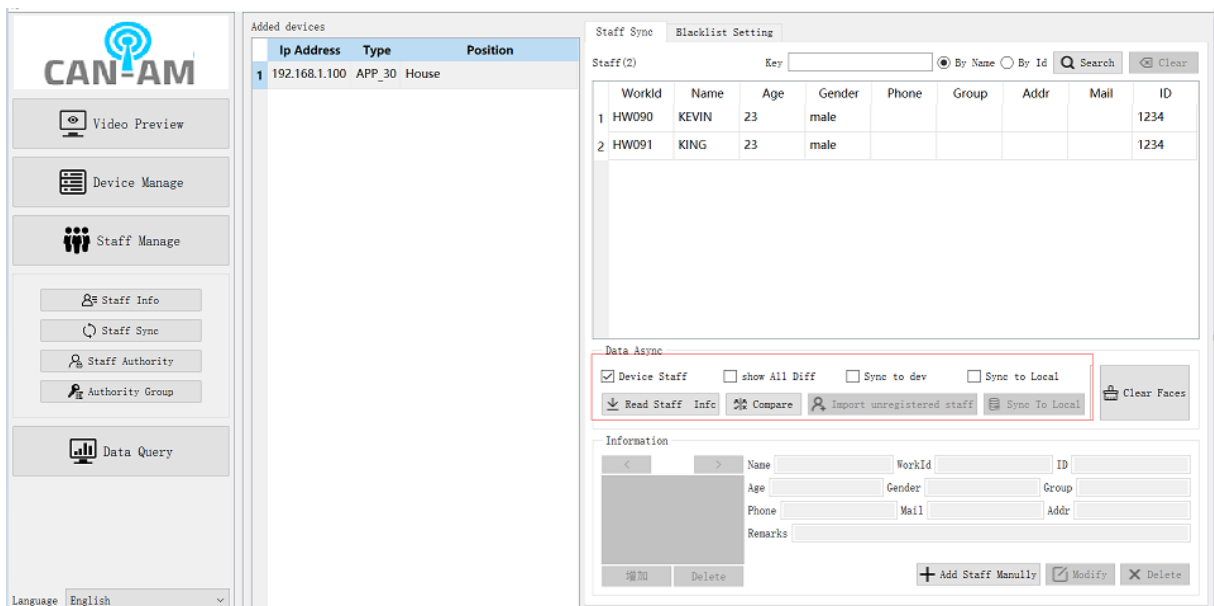
    1. Select the device node to be synchronized and click "Read staff info" to synchronize personnel data between the device and the client.

2. Click "Show All Differences", and click "Compare".

   Yellow indicates that information is on the local client but not on the device.
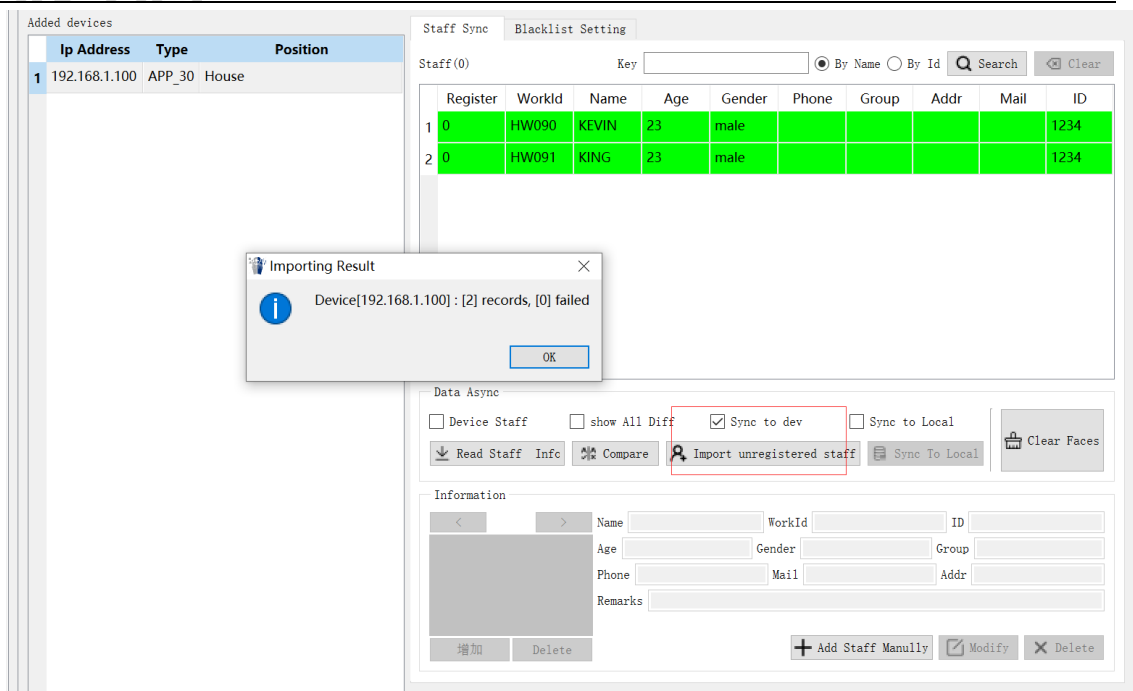
   Grey indicates that information is on the device but not on the local client.

3. Click "Sync to dev", and click Sync to device to import users from the local client to the device.
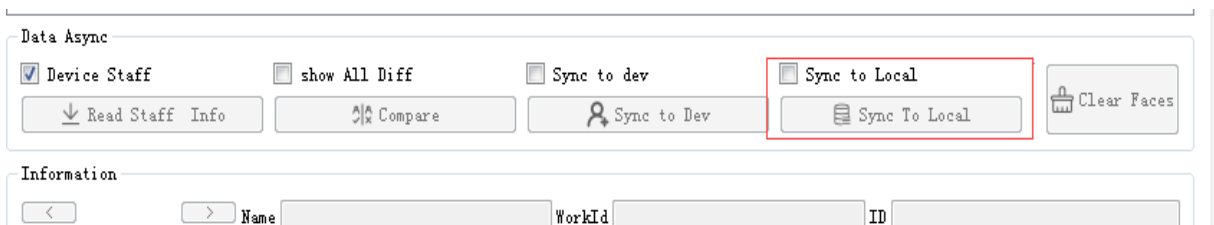
2. If there are some info only saving in device, Click "Sync to local", and click "Sync to local" to import data from the device to the local database.

3.2.6 Clearing Device users

On the left side of control panel, click Staff Management -> Staff Sync.

Click "Clear Faces" and click "Read staff Information" to check whether all information is cleared.

Attention: If you click "Clear Faces", all data will be cleared!

3.2.7 Blacklist and White-list

On the left side of control panel, click Staff Manage -> Staff Synchronization -> Blacklist Settings.
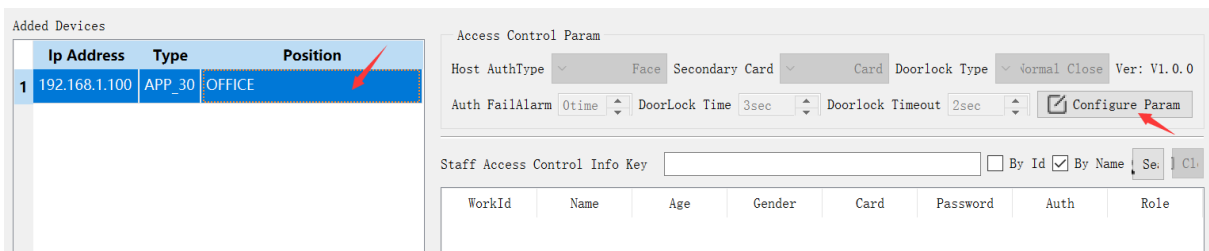
1. Select devices.

2. Select users to add to the blacklist or white-list.

3. Click "Add Blacklist" or "Add white-list".

4. Click "Upload List" to upload the blacklist/white-list to devices.

You can click "Read List" to get the list those have been saved in device.

Notification: White-list user could turn on the lock of door at any time if you have set the door access control system.

3.2.8 Device Access Control Parameters

On the left side of control panel, click Staff Management-> Staff Authority.
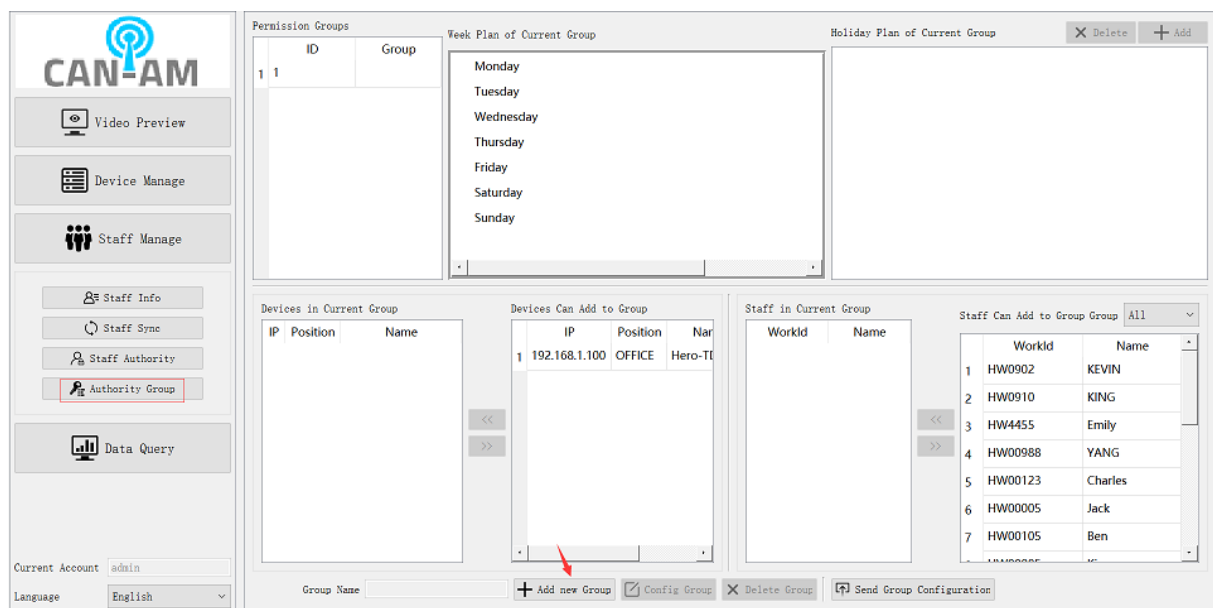
1.Click "Configure Param".

2."*Host Machine Authentication Method*", "*Second Card (Not Available)*", "*Door Lock Time*", "*Lock Timeout*" are subject to change.

3. Click "Confirm". The parameters will be synchronized to the device.

Attention: Only Host AuthType (Face) will work.

Access Control Parameter	Description
Host machine authentication method: configures the authentication method of the device. Select different combinations to set up your authentication method.	Currently, only face authentication is supported.
Second card authentication: set up for connection to an external card reader. The types of authentication are the same as those of the device.	Not available.
3 magnetic door switch options: none, normally open, normally closed. none: no door magnetic switch is used. normally open: the door is open under normal conditions (always open when the power is on).	0 - None 1 - Normally open 2 - Normally closed (default) This depends on the Lock type.

normally closed: the door is closed under normal conditions (always closed when the power is on).	
Time for door locking: the duration of time for device control over locking (from opening to automatic locking) when the door is closed.	1-255 seconds. *1 second by default. You can change it.*
Door open timeout alarm: when the magnetic state of the door is inconsistent with the settings, an alarm will sound after a specified period of time. This period of time is the magnetic alarm delay (effective range from 1 to 999 seconds).	1-255 seconds. 30 seconds by default.
Authentication frequency alarm: when the number of failed authentications (number of times that one presses the wrong button) reaches the set value (from 1 to 9), the alarm will sound. If this is set to "no", then no alarm will sound.	0-9. 0 by default, meaning that no alarm will sound upon any failed trial.

3.2.9   Authority Group
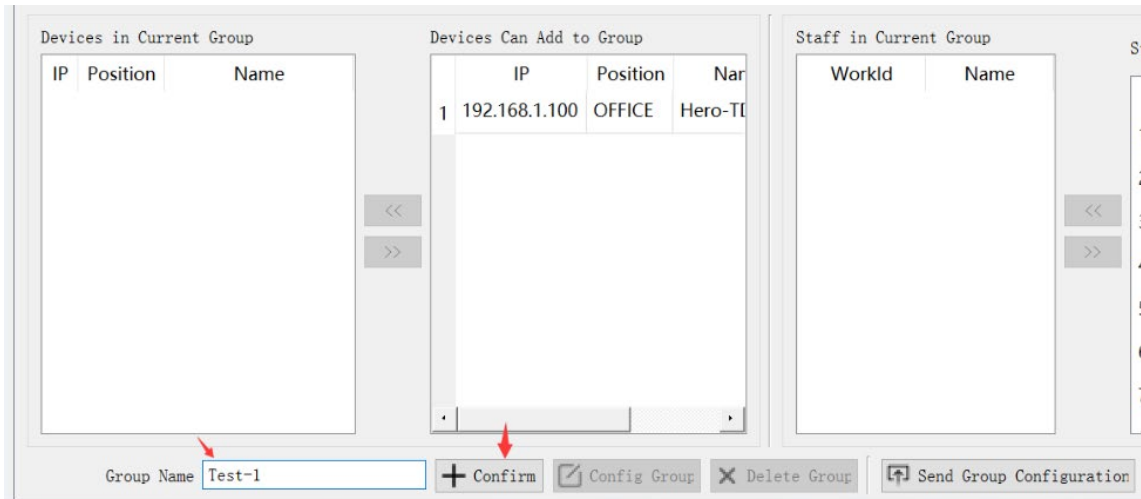
Authority Group is for building the attendance and access-control plan for registered staff.

1. You can sort the staffs by different groups (for example, different department), then make attendance plan.

2. Create holiday plan for staff.

3. Release this plan to device.

Tips: Staff in authority group could only open the door during the attendance plan's time. While in white-list person could open the door at any time.

Steps:

1. Click "Add new Group"

2. Input the Group name, and "confirm" it.
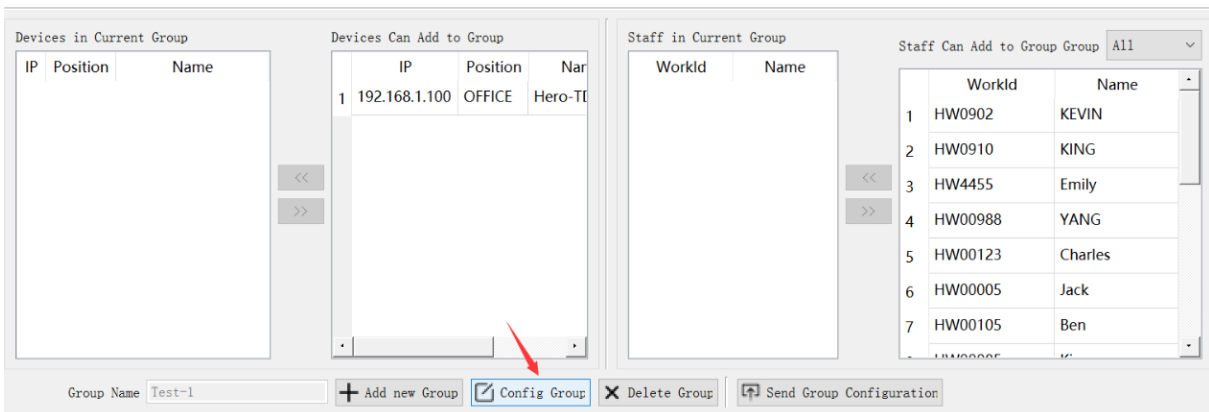
3. Click "Config Group"
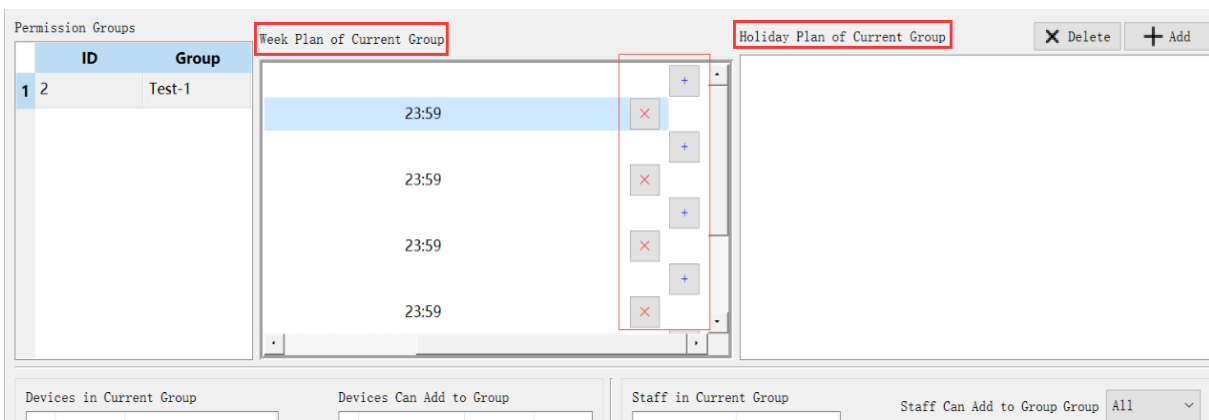
4. Make workday plan and Holiday plan.

5. Move the staff to the current group.

6. Move the device IP address to the current group.

7. Save the Configuration.

8. Release the configuration to device.

3.3 Voice of notification

None: Just temperature display. Means this person has not been registered.
Welcome: White-list or in the Authority Group's staff.
No passing: Blacklist staff.
Check in Successfully：The normal staff who have registered the info.
Please Wear mask: People who not wear the mask, no matter has registered or not.
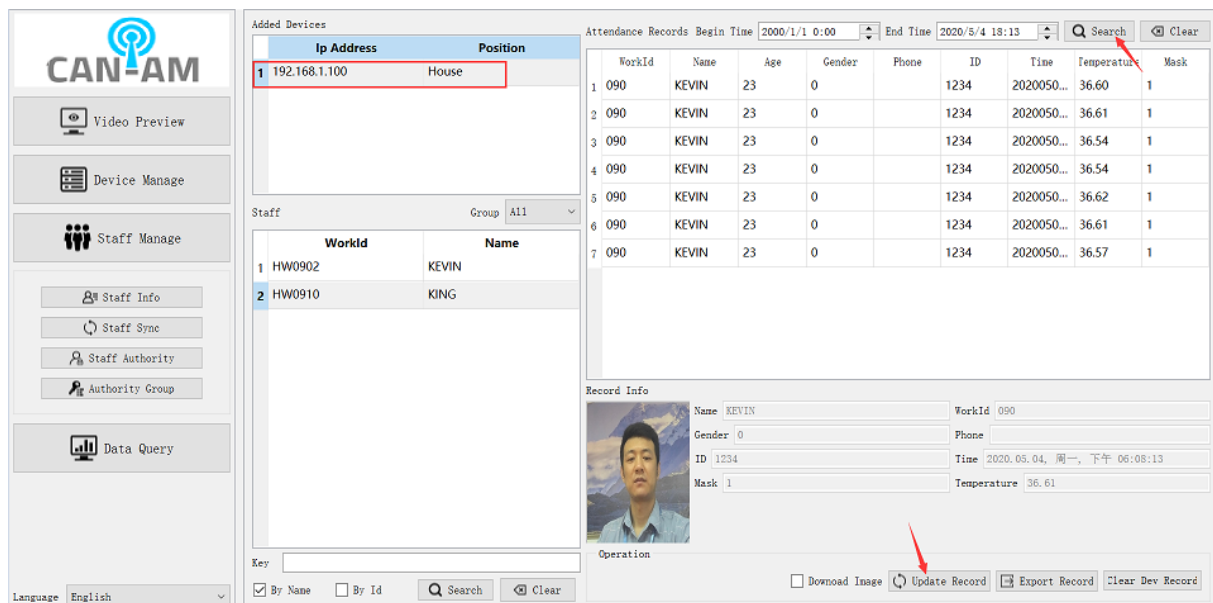**Abnormal body temperature**: High temperature alert, no matter this person has registered or not
Attention: We suggest let the device run10 minutes in advance, then the accuracy will be better.

4.   Data Query

4.1 Updating Attendance Records
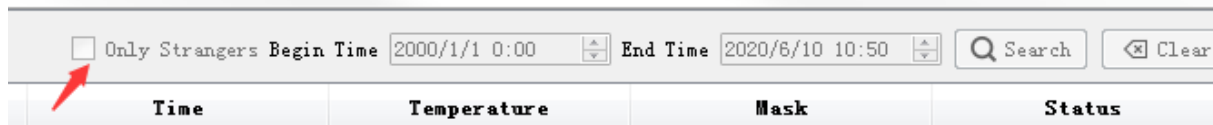
Click Attendance Record -> Data Query on the left side of control panel;

1. Select device and click "Update Record". The client will automatically download the latest record from the device. It will take some minutes.

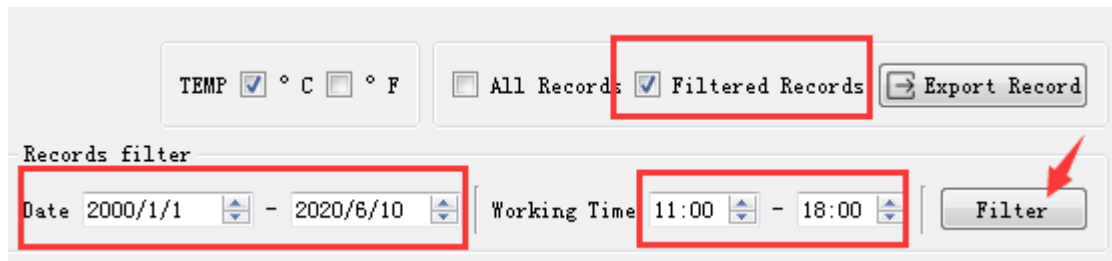2. It will get the whole record of register staff and strangers.

A. Just get strangers record.

B. Just the first and last record of Register staff

1. Tick "Filter Records"
2. Input the working time and date
3. Click "Filter", then it will just export the first and last attendance record of staff.

WorkId	Name	Time	Temperature	Mask	Status
HW00089	Clark	2020/06/10-10:48:41	36.50	None	Sign On
HW00089	Clark	2020/06/10-10:48:51	36.61	None	Leave early
HW0902	KEVIN	2020/06/10-10:42:04	36.83	None	Sign On
HW0902	KEVIN	2020/06/10-10:45:46	36.64	None	Leave early

4.2 Export Attendance Record

1. Click "Export Record". The client will export data into the Excel document.

2. Find the path information on the left bottom of interface. The default path is the installation folder.

4.3 Clear Record

The device will save all records and cover old records, you can clear them.

5. FAQ

1. Cannot search the device

Make sure the device is on, and your PC's IP address in the same segment with Device (The default IP address is 192.168.1.100). Besides, turn-off firewall of your PC (Windows 10).

2. What's the adaptor spec?

DC:12V, 2A at least.

3. What's port and password of web browser?

Port: 8080; Default password: admin123456

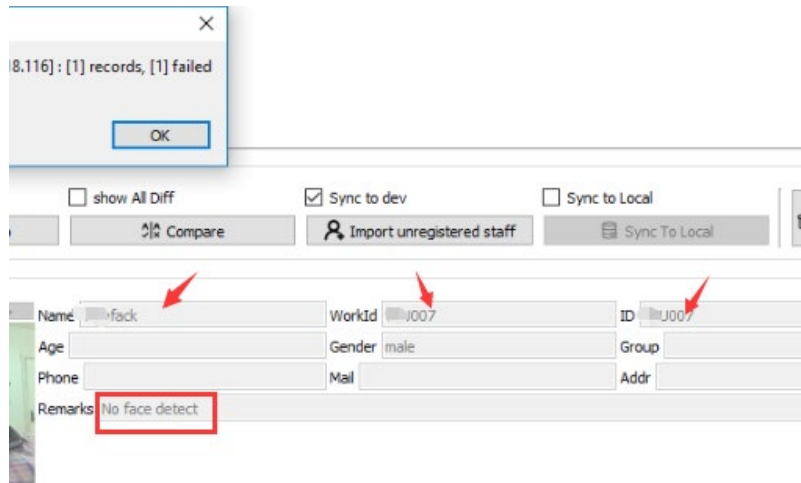4. How to set the Temperature threshold

Please refer to *3.1.3.4 Display setting*.

5. Turn on /off Mask detect function.

Please refer to *3.1.3.3 Algorithm settings*.

6. Synchronic device failed.

Check the picture and WorkID /ID, there is a Remarks about it.

7. How to customize ARFaceManger tool's Logo.

Prepare 120*40 PNG Logo picture, replace the one in **Res** folder.