Thermal Imaging Fever Screening Terminal

User Manual

V1.3.2

Statement

The contents of this manual will be changed from time to time due to product version upgrades or other reasons, and subject to change without notice. We try our best to ensure that the content in this manual is accurate and reliable. This manual is only used as a guide. All statements, information and suggestions in this manual do not constitute any express or implied guarantee.

Special Statement

Please strictly abide by the applicable laws and regulations for the use and maintenance of the monitoring interface. Using equipment for illegal purposes or snooping on the privacy of others are all illegal surveillance.

Symbol Description

For the symbols that appear in the document, the description is as follows.

⚠ Cautions: general warning signs, reminding things that should be paid attention to during operation.

Instructions: instructions are an emphasis and supplement to the main text.

Historical Version

Version	Reviser	Date	Comments
V1.0.0	DML	2019-11-26	
V1.1.0	BYH	2020-03-31	Add instruction of interface lock control
V1.2.0	YM	2020-04-13	
V1.3.0	ZS	2021-01-04	Update web&client operation

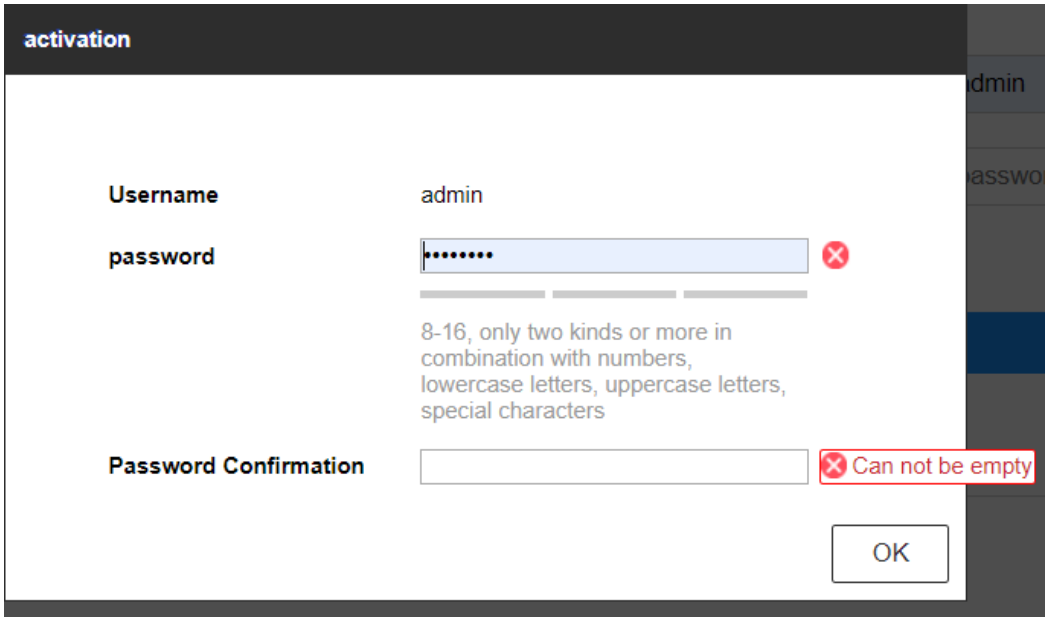
Table of Contents

1. Web Operation

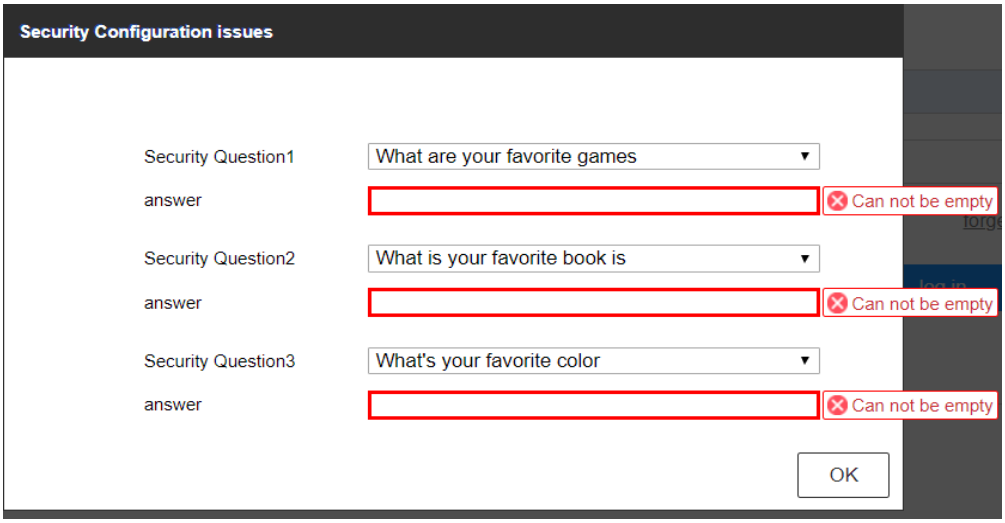
1.1 Passwords Management

1. Initial Passwords Setting

The default administrator account of the camera is admin. For the first time login, set the password according to the popup page box before accessing the camera, as shown in the interface below. After setting the password according to the prompts, click "OK".

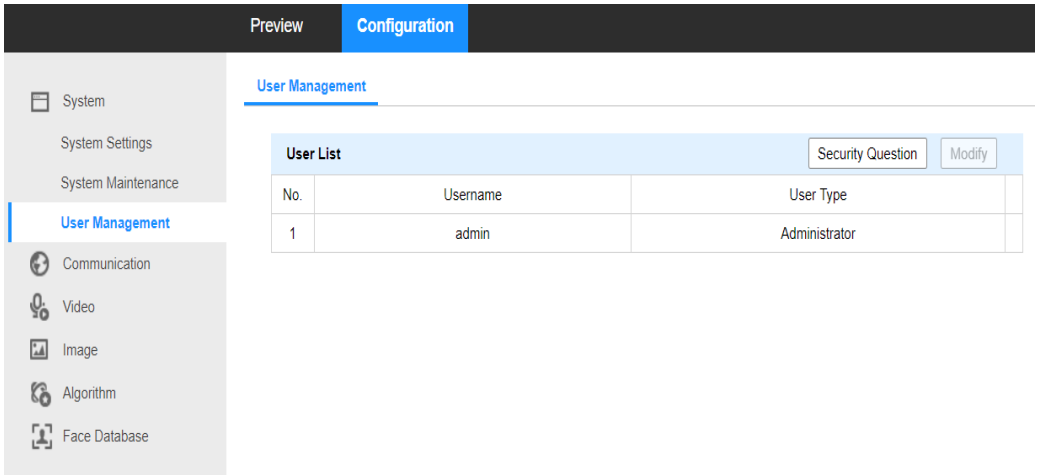


When setting the passwords, it is recommended to set the password security questions at the same time for resetting passwords in case of forgetting the password, as shown in the figure below. Select three security questions and set the answers, and click "OK".



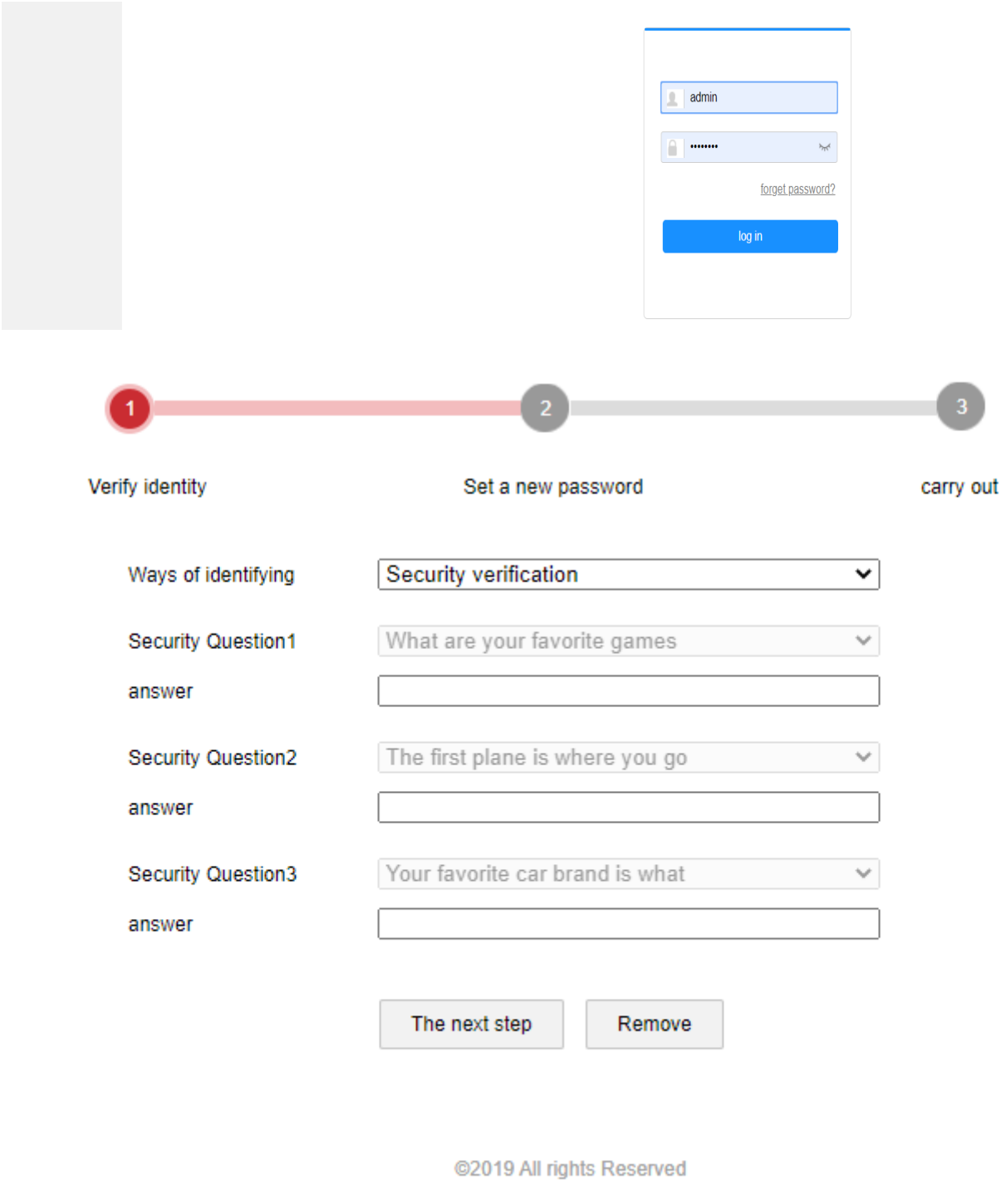
2. Modify Passwords

Users can reset security questions and login passwords through the "configure→ system→user management" path, as shown in the figure below. Click the "Security Question" button to reset the password security questions. Select a user and click the “modify” button to reset the user's password. Administrator rights are required to reset the security questions and change the passwords, and the passwords can be modified only after administrator passwords is entered and verified.



3. Reset Passwords

Click "Forgot password?" button on the login interface when passwords are forgotten, as shown below. Enter the answers to the security questions and reset the passwords.

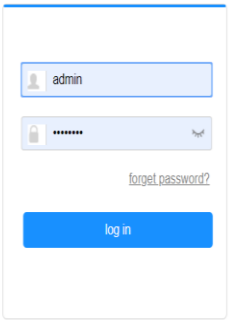


1.2 Interface Introduction

On the Web main interface of the camera, you can preview and configure other functions.

1.2.1 Web Login

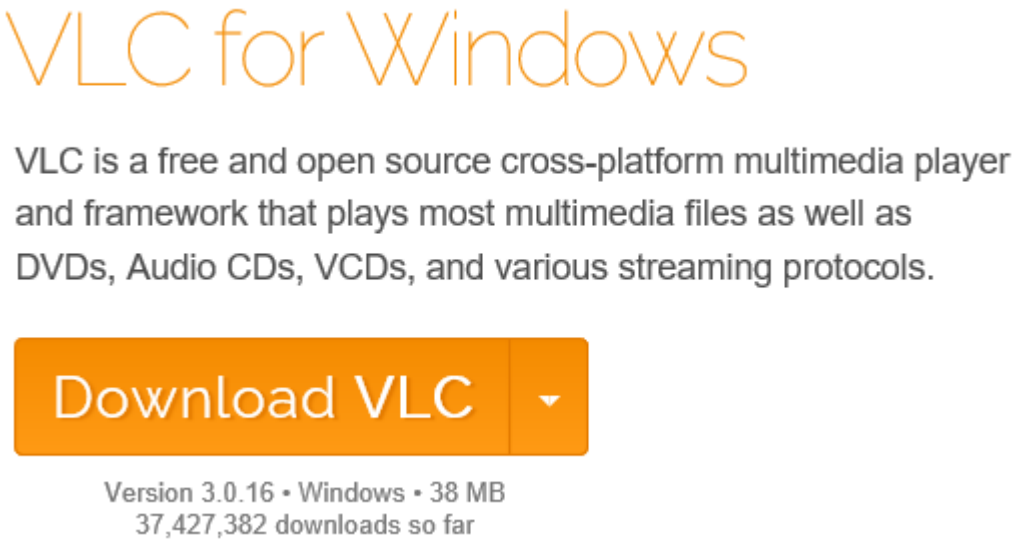
Enter http://IP address in the browser address bar, and the following login interface will appear. Enter user name and password to log in. (The IP by default is http://192.168.1.123).



1.2.2 Preview Interface

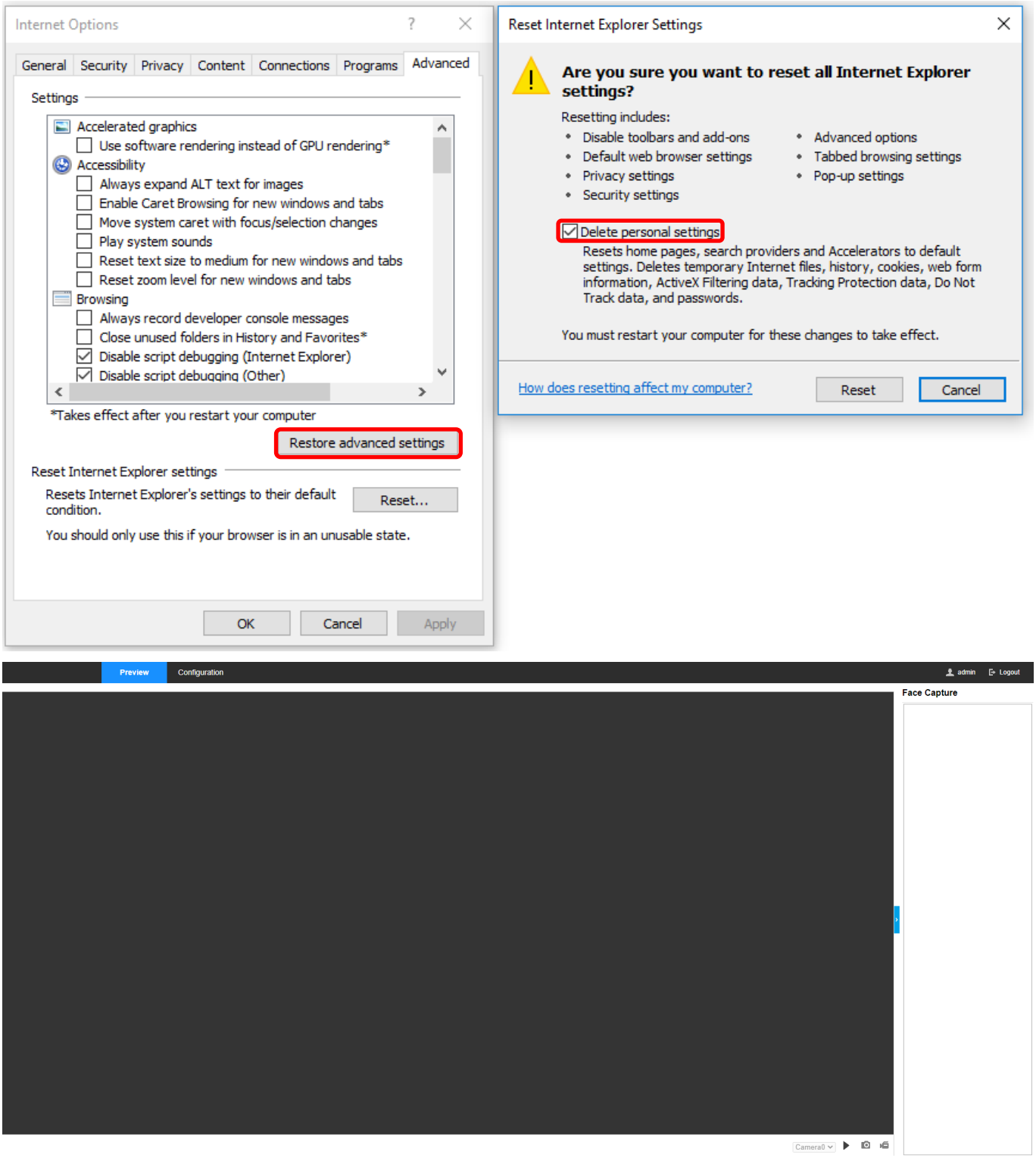
In addition to the preview screen, you can also view the images captured by the camera in real time on the preview interface. Click the triangle icon on the right side of the browser interface as shown in the figure below to expand the collapsed area to view it. Up to 10 images can be displayed.


Preview
Configuration
admin
Logout
Face Capture
Reminder: pls use IE browser
Setp 1: open the URL link https://www.videolan.org
Step 2: Click Download VLC, select 'windows-32-bit'
Step 3: download the software
Step 4: install VLC software
Step 5: restart IE browser
Camera0


VLC for Windows
VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols.
Download VLC
Version 3.0.16 • Windows • 38 MB
37,427,382 downloads so far

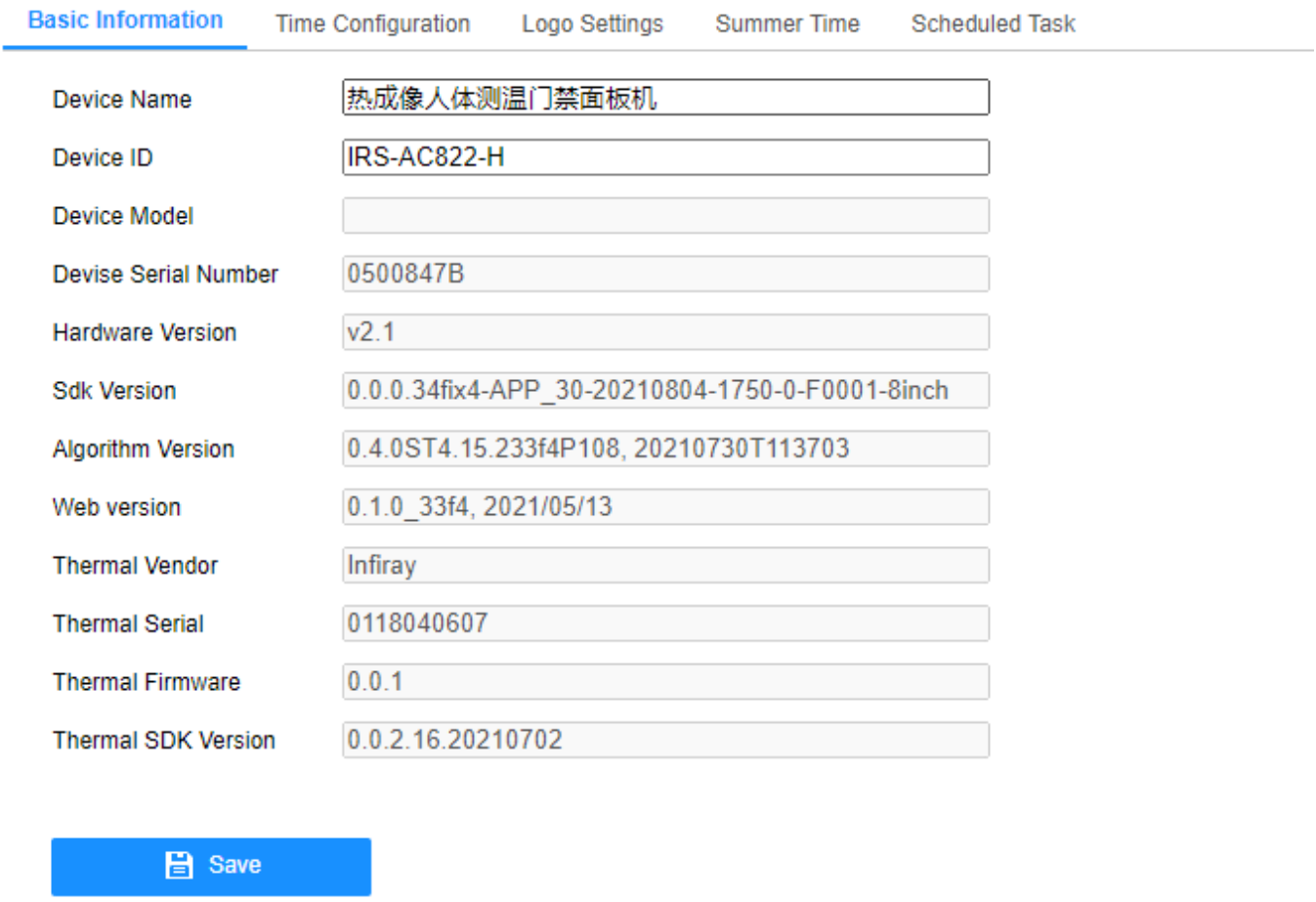

Preview
Configuration
admin
Logout
Face Capture
Camera0


Preview
Configuration
admin
Logout
Face Capture
Reminder: pls use IE browser
Setp 1: open the URL link https://www.videolan.org
Step 2: Click Download VLC, select 'windows-32-bit'
Step 3: download the software
Step 4: install VLC software
Step 5: restart IE browser
Camera0

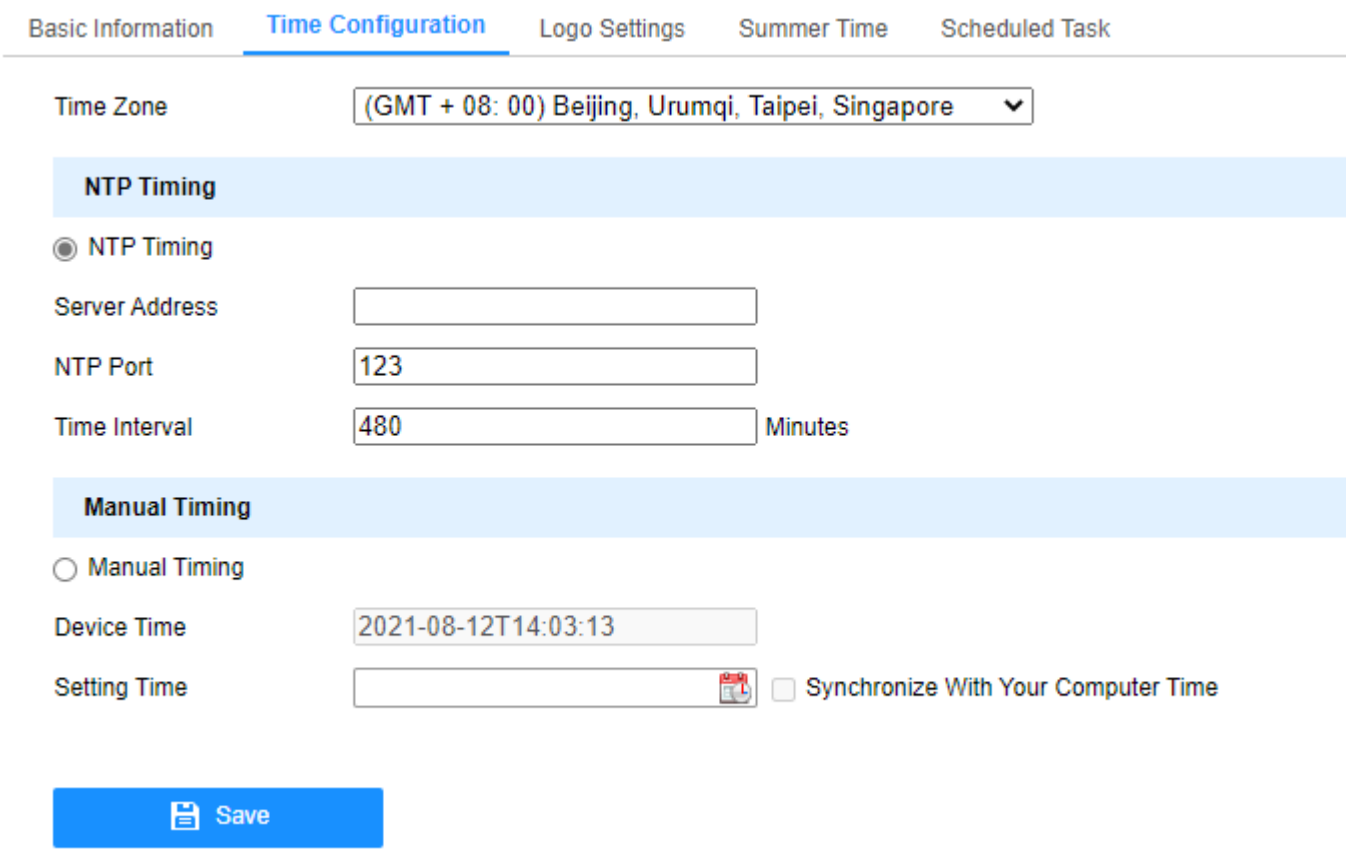


1.3 System Setting

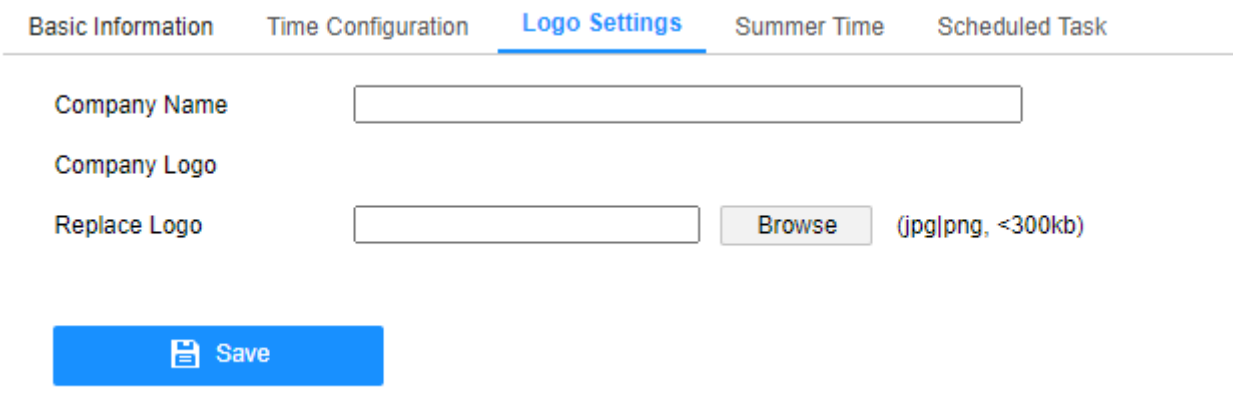
(1)System→System Settings→Basic Information. You can check relevant information of device model and software version, and set device name and number, etc. Click "save" button after setting.



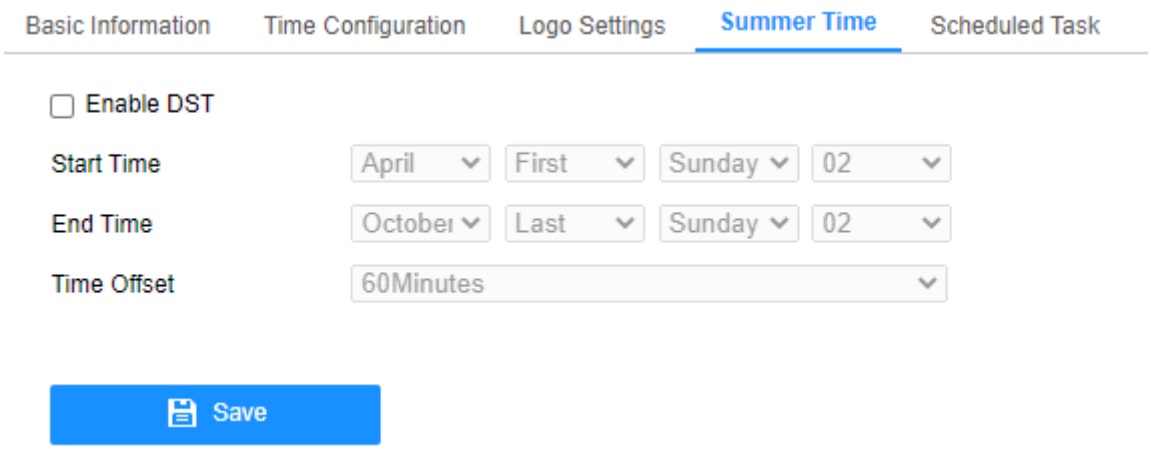
(2)System→System Settings→Time Configuration. Support time zone switch, NTP calibration, manual calibration and other operations. Click the "save" button after selecting the items to be set.



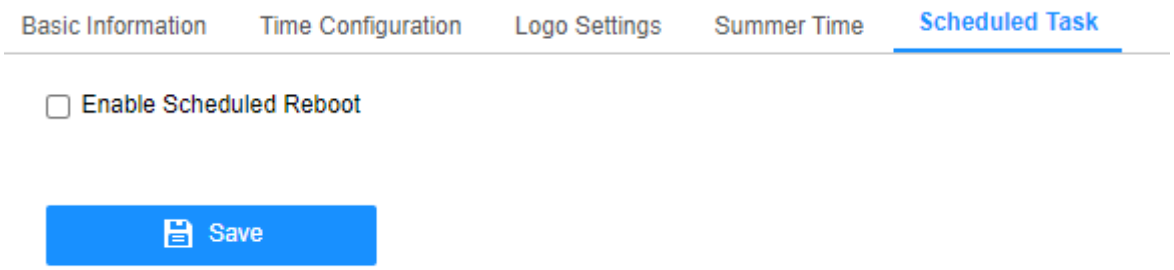
(3)System→System Maintenance→logo. You can set the company name and logo on the web page.



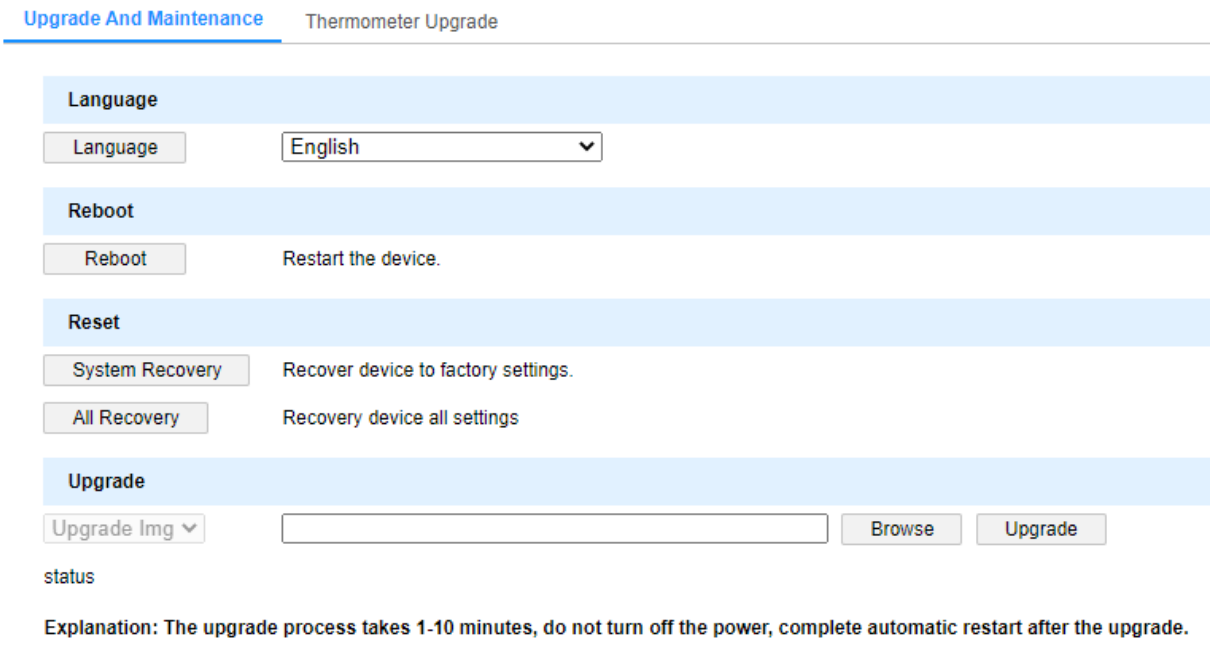
(4)System-System Settings-Summer Time, this can start summer time during a certain period of time.



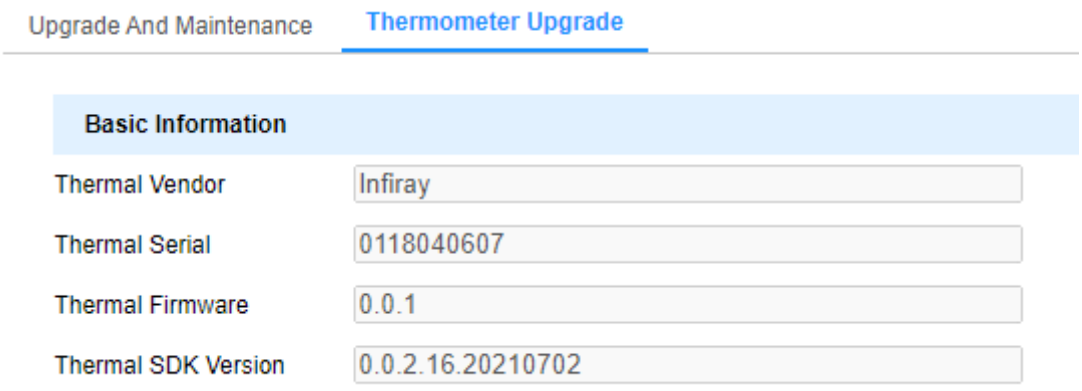
(5) System-System Settings-Scheduled Task, this can only can perform scheduled restart, that is to restart the device at fixed time.



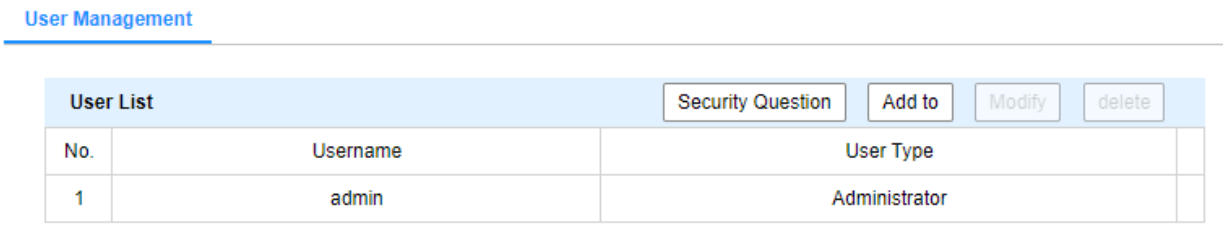
(6) System-System Maintenance-Upgrade, this can restart the camera and update the camera firmware. Select the img file to be updated via browse button, click update and select OK in the pop-up prompt dialogue box to start updating.



(7) System-System Maintenance-Thermographic module update, this function is unavailable for the present model, it can only display the basic information of the thermographic module.



(8) System-User Management, an ordinary user can be added besides the defaulted admin account, which can be added via add button, the ordinary user owns only preview permission, but without configuration permission. The ordinary user can be added or deleted, the password can be changed for the admin account.

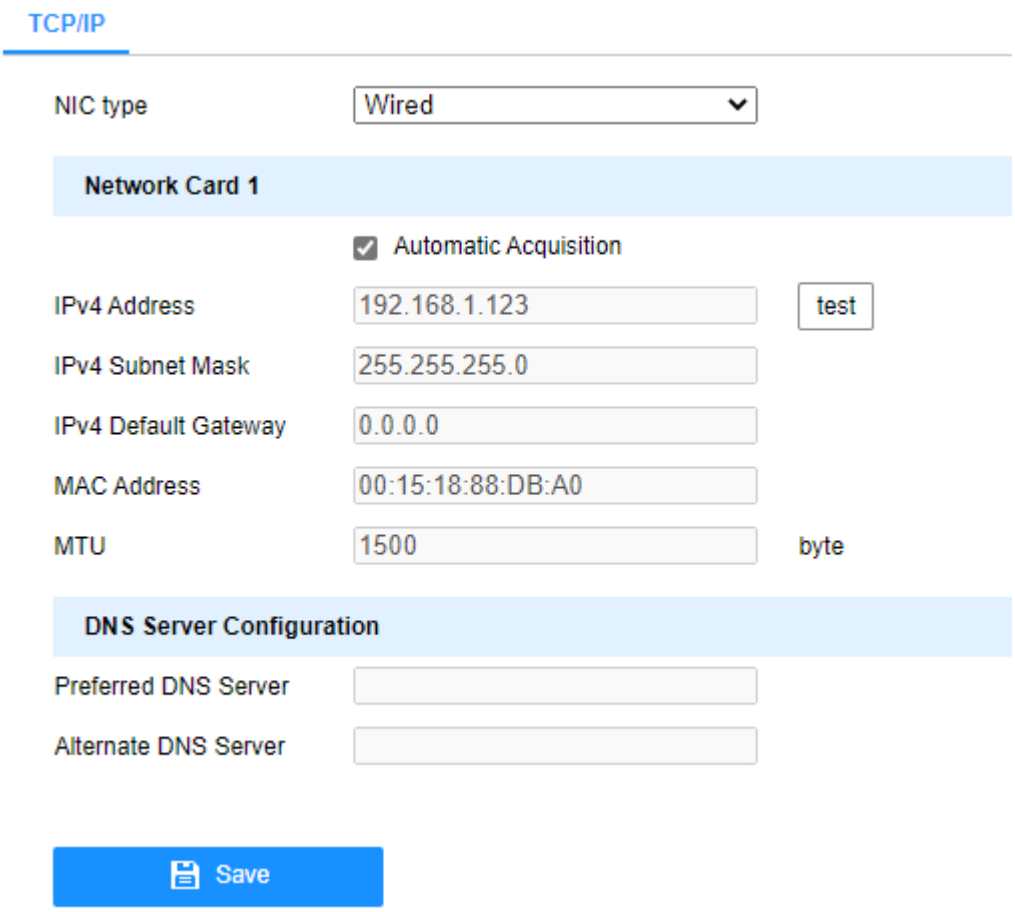


1.4 Advanced Configuration

1.4.1 Network Configuration

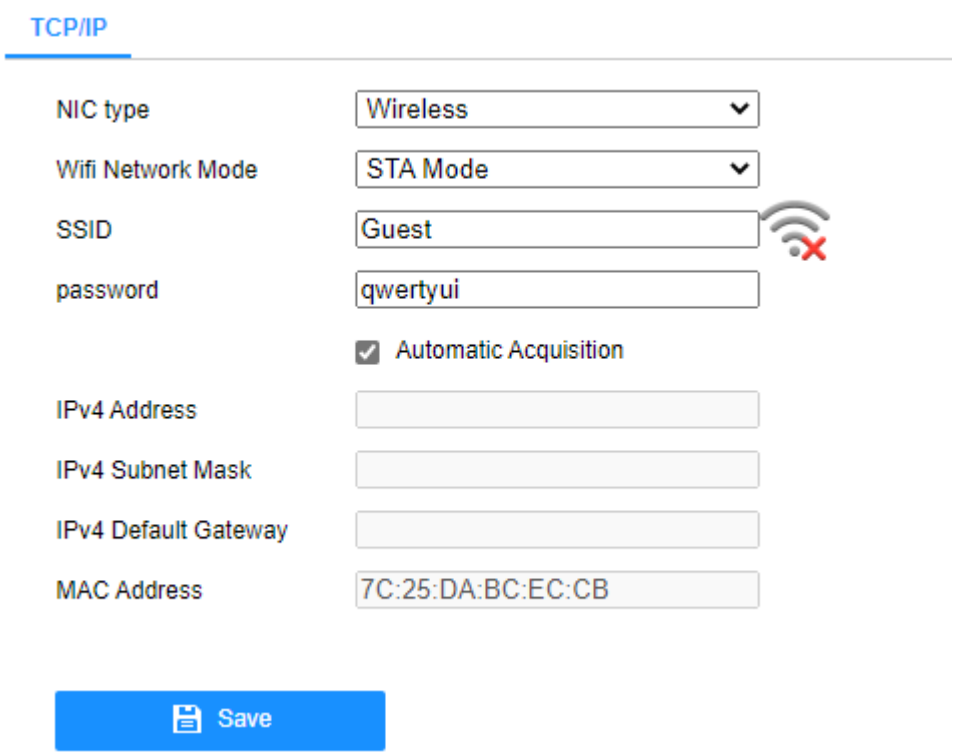
(1) Wired Network

Network- Basic Configuration-TCP/IP, select the wired LAN for the LAN type, which can change the IP address of the camera, click OK to save the settings, the camera will restart and the new IP address will be used, the new IP address should be used to login during the web reconnection.



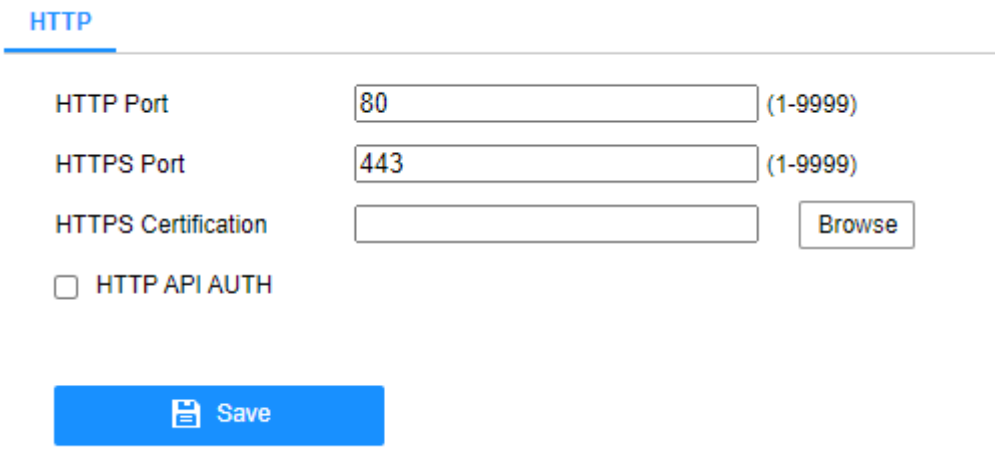
(2) Wireless Network

Network-Basic Configuration-TCP/IP, select the wireless LAN for the LAN type, then connect Wi-Fi after typing in the corresponding Wi-Fi account and password.



1.4.2 Advanced Configuration

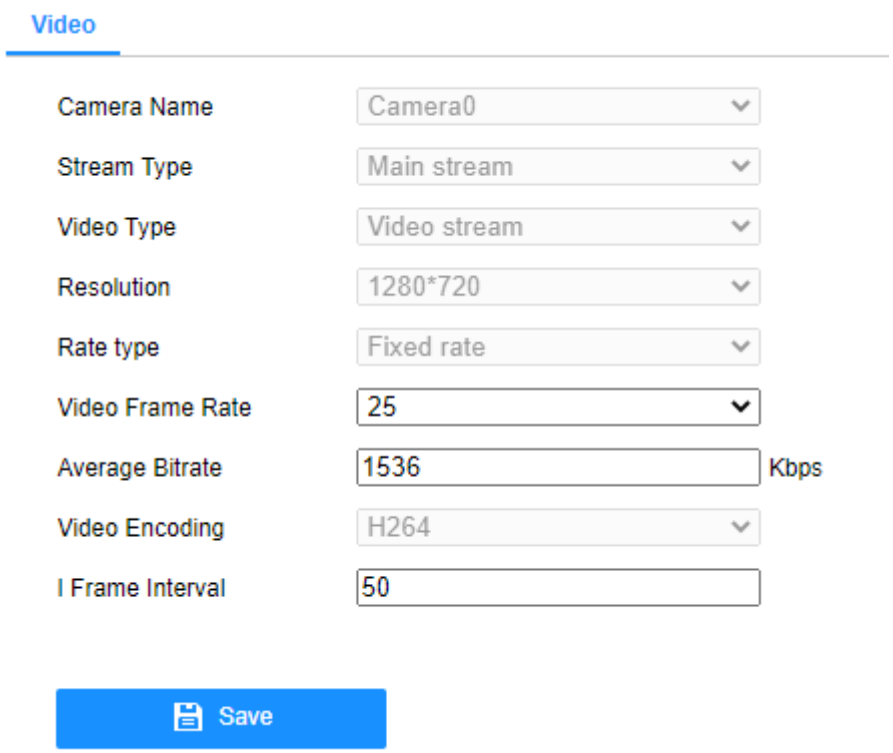
Network-Communication→ Advanced Configuration, the HTTP, HTTPS port settings and certificate update operations can be performed.



1.5 Video and Audio

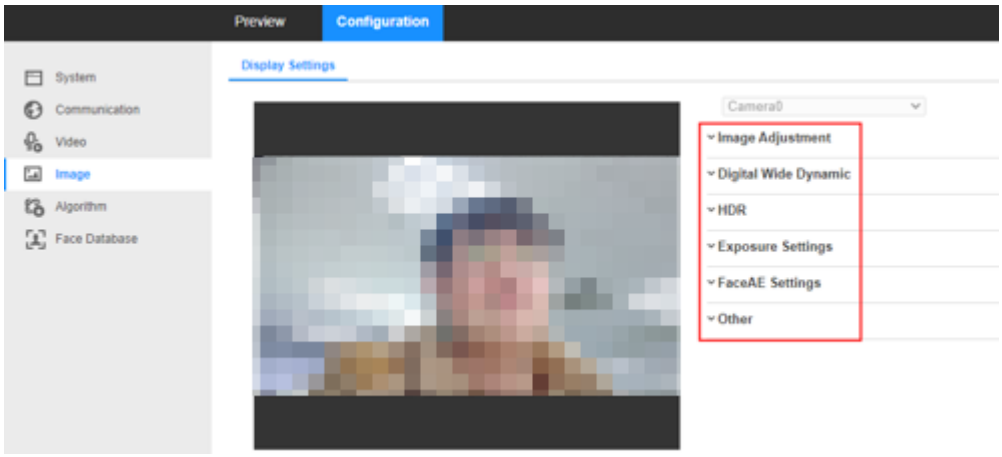
Video and Audio- Video, this can configure the code rate of the video, then click save button.

(1) Configure the video bit rate information, and click the "Save" button after setting.



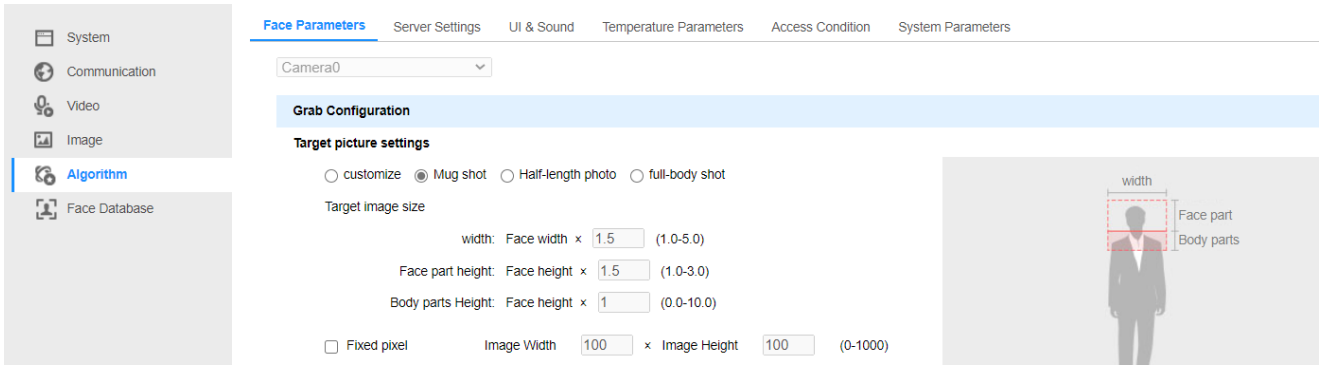
1.6 Image

(1) Image→ Display setting. Image display parameters can be adjusted, including brightness, contrast, saturation, sharpness, digital wide dynamic, HDR, Exposure, Face AE and so on.



1.7 Algorithm

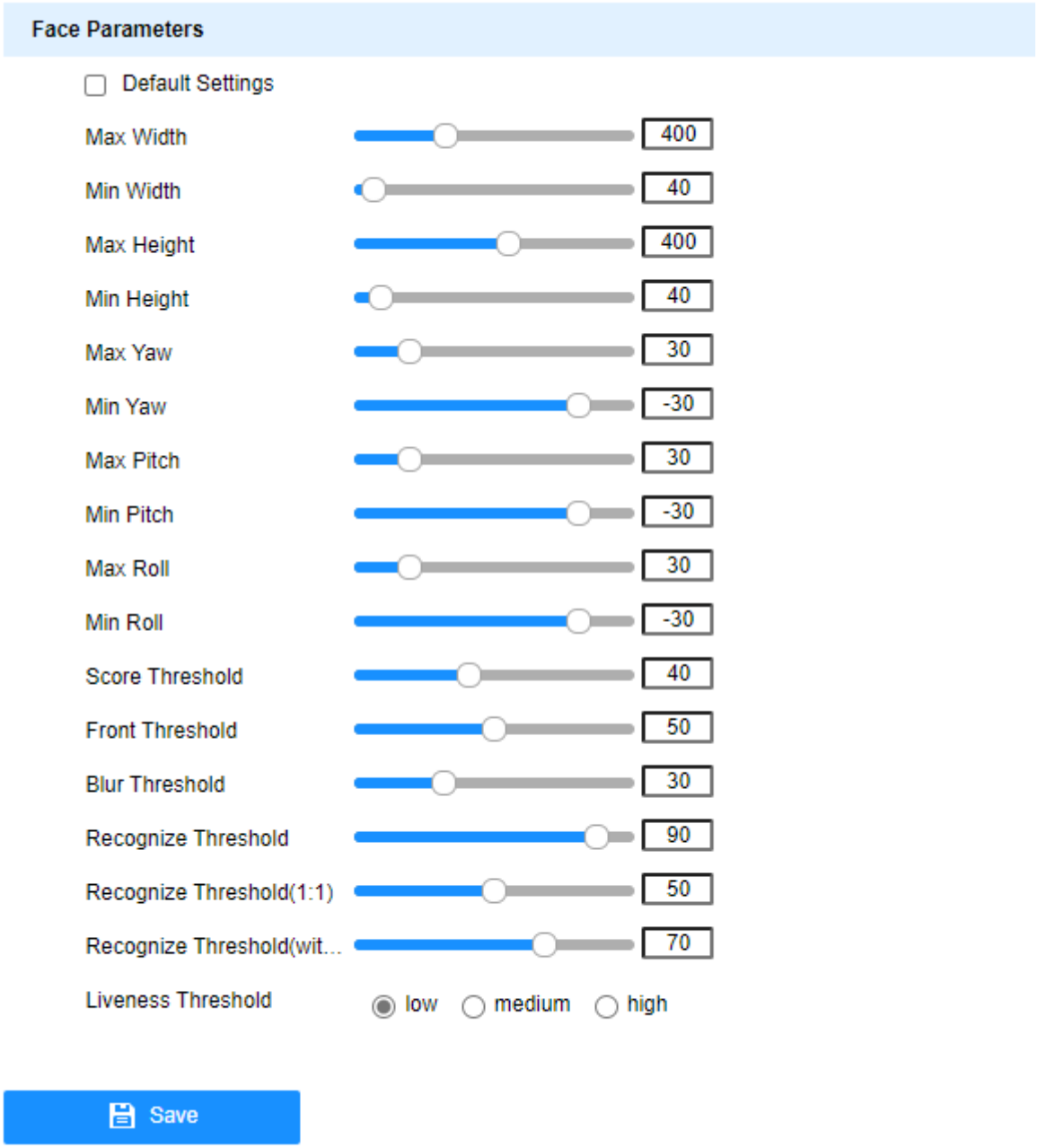
(1) Algorithm→Face Parameters→Grab Configuration, which can set the target image type and size. Click the "save" button after setting.



（2） Algorithm→Face Parameters. You can set the relevant parameters of the snapshot, and click the "Save" button after setting.

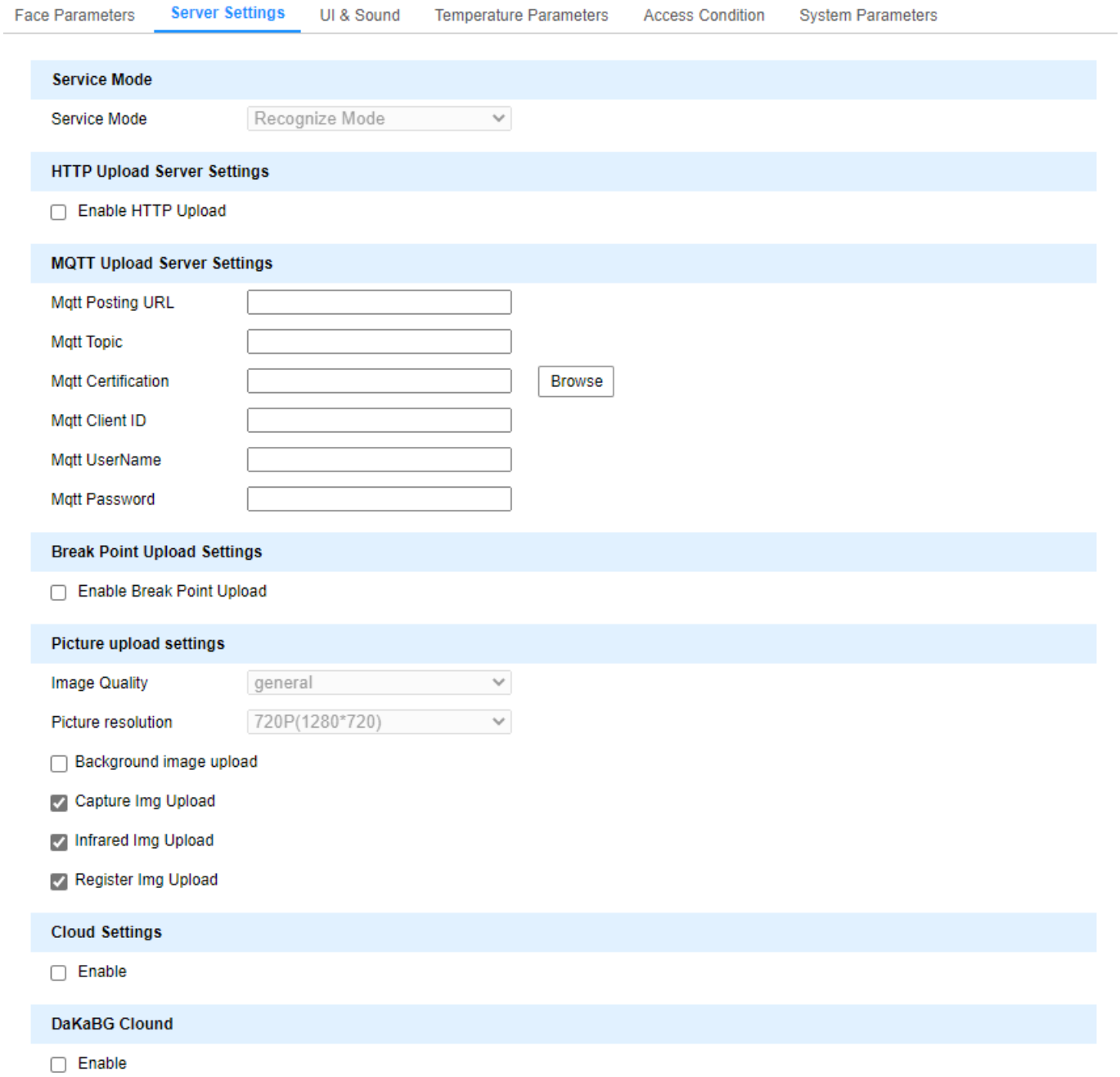
Notes: the face width and height control the filtering face in face parameters; the recognition threshold is used for ordinary face match, 1:1 recognition threshold is used for ID card match, threshold of the mask face recognition is used for face match with masks. There are three levels for liveness threshold: low, medium and

high, it is low by default, the higher the level is , the easier it is to pass.



(3) Algorithm→Threshold→Server Settings, which can set HTTP or MQTT upload services. You can set the resumable upload settings and the upload server address, and private cloud service. Click the "Save" button after setting the relevant information, and then log in to the cloud server to manage users, devices, and

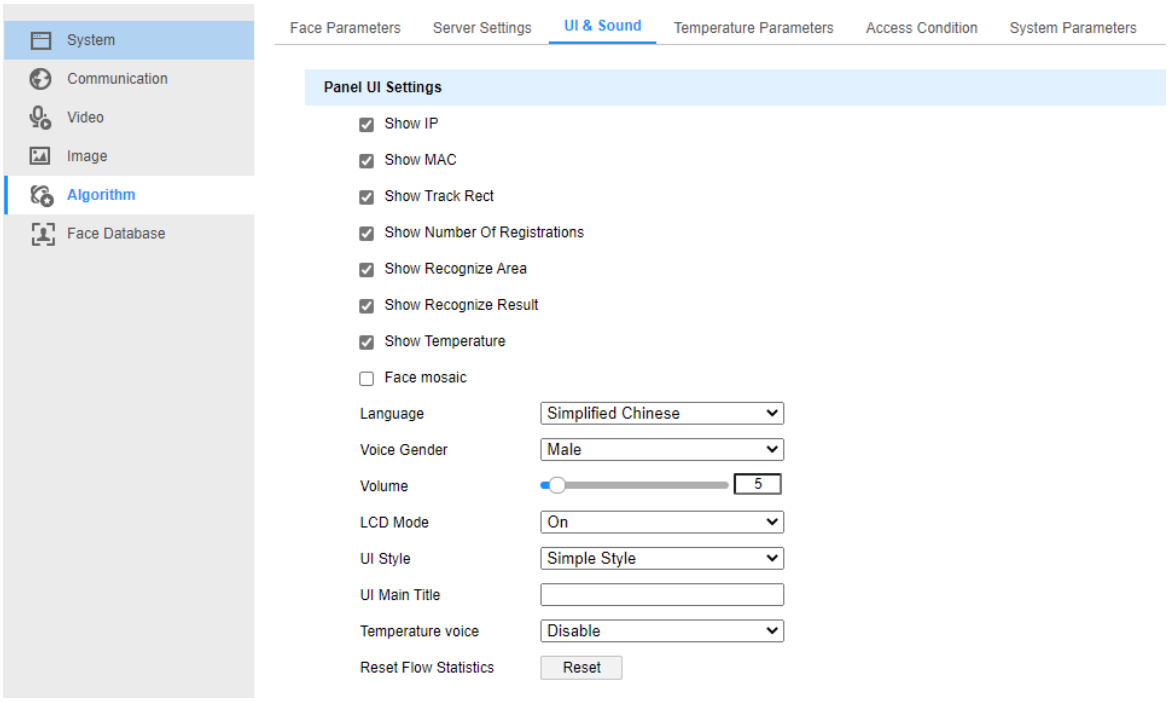
captured images.



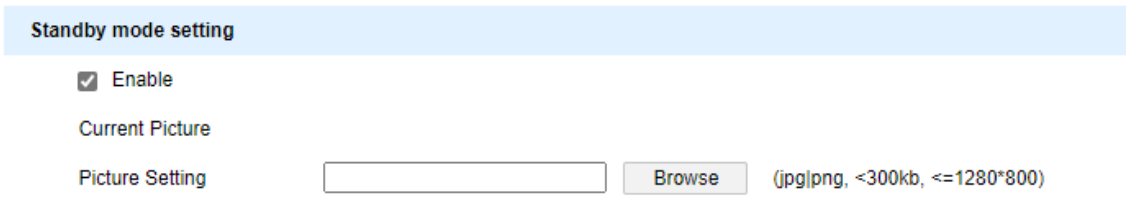
（4）Algorithm→ UI&Sound→Panel UI Setting. It is mainly used to set the interface display of the screening terminal, the audio setting, the control of the compensation light, and the UI display style.

Only the simplified Chinese and English are available for skin temperature voice broadcast, the temperature value broadcast is only available in simplified Chinese and by female voice.

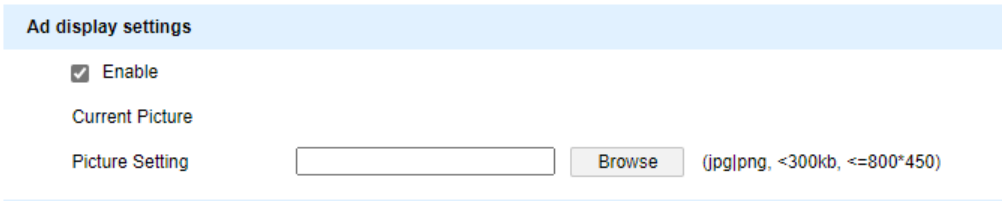
For the screening terminal with the function of access statistics, you can click the button "Reset Access Statistics" at the bottom of UI Settings to reset the access statistics.



(5) Algorithm→ UI&Sound→Standby Mode. If nobody passes in one minute, the device will enter into standby interface after this function is enabled, the custom pictures can be displayed on the standby interface, time display by default.

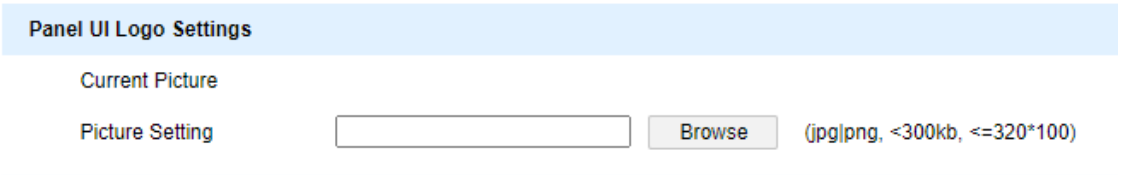


(6) Algorithm→ UI&Sound→Advertising Display. The infrared image area can be replaced by the advertising pictures.

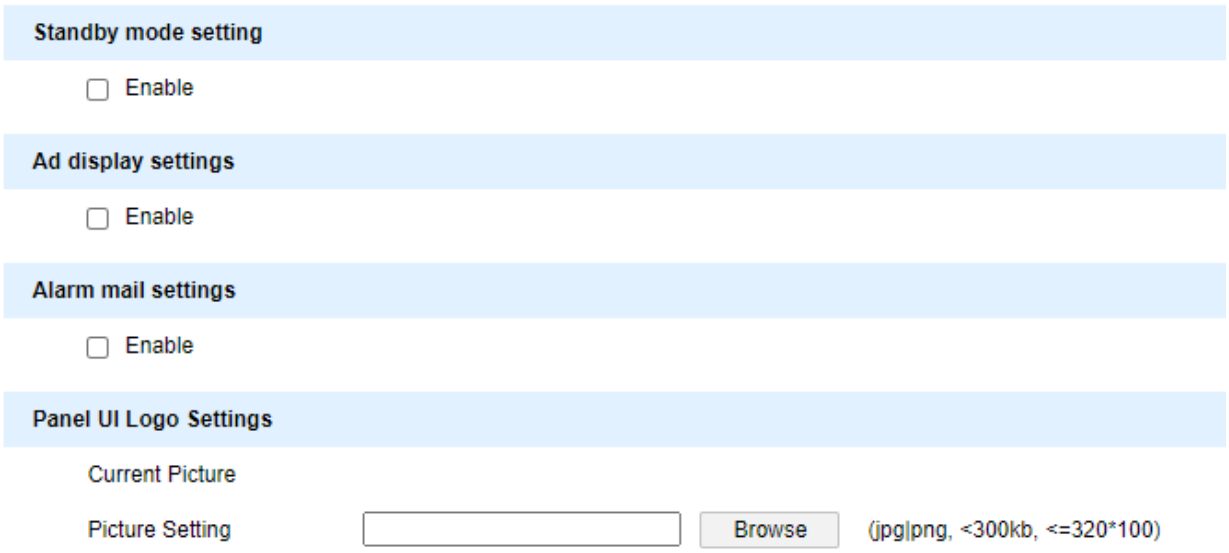


(7) Algorithm→UI&Sound →Alarm Email. This function is to send an Email to the target accounts when the body temperature or mask is abnormal. The “smtpPort” can be set according to 465 by default. Several “emailTargetAddress” can be set, which should be separated by English commas.

(8) Algorithm→UI&Sound →Logo. This can set the logo on the UI, the main interface title will be displayed if the logo is not set. If the main interface title is not set, then “Smart Terminal” will be displayed by default.



(9) Algorithm→UI&Sound→Startup Logo, Standby Mode, Alarm Email and Background Picture.



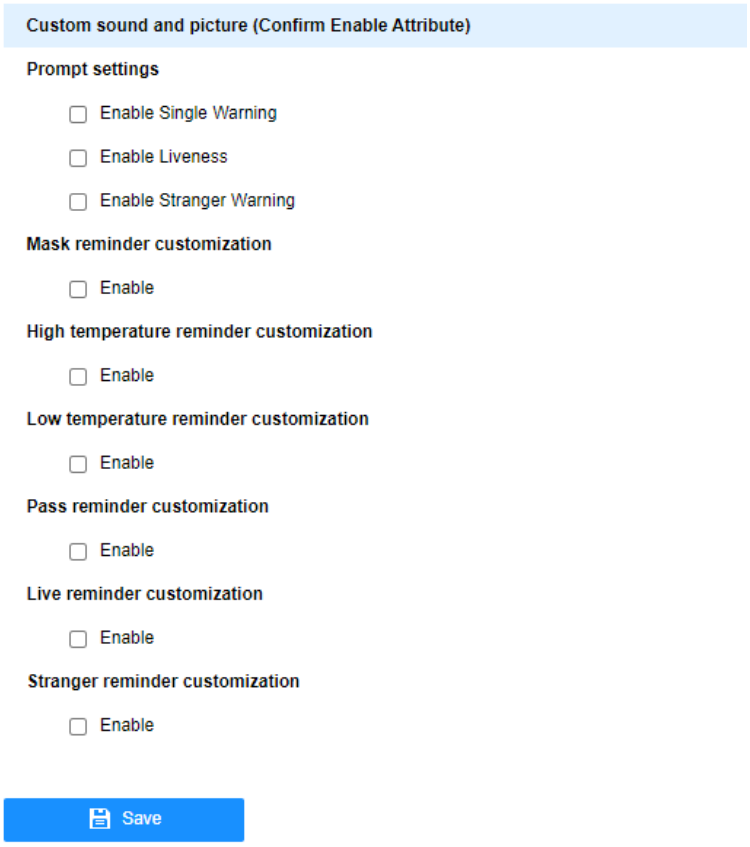
(10) Algorithm→UI&Sound→Panel Sound and Picture Settings (Confirm Enable Attribute)

Single alarm: the alarm warning only appears once for every single face.

When living scene are turned on, the picture and voice of the setting will be displayed when there are no live body faces.

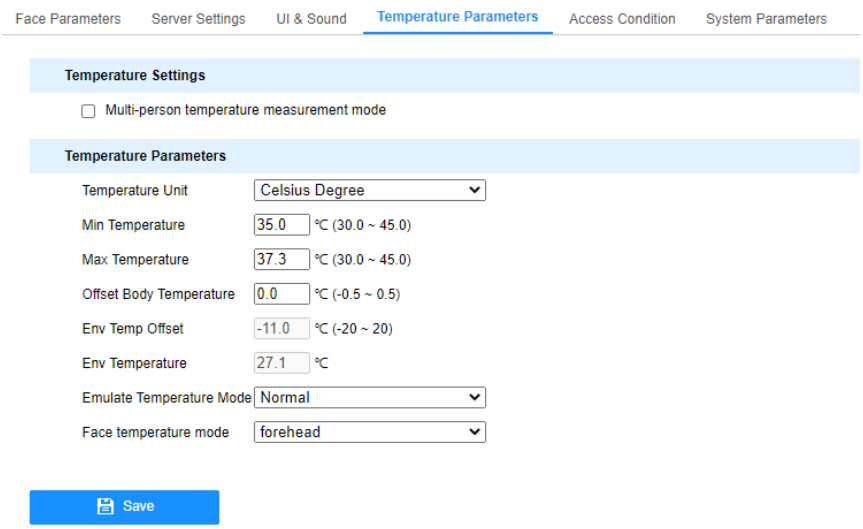
In case of the stranger warning scene is turned on, the picture and voice set in the corresponding scene will be displayed when a stranger appears.

Custom warning include mask, high temperature, low temperature, passthrough, liveness and stranger, the specific pictures and voices are set for different scenes.



(11) Algorithm→Thermographic Parameters

The thermographic parameters include above temperature limit, below temperature limit, curve mode, etc. Several body temperature can be displayed at the same time after the multiple thermographic mode is enabled.



(12) Algorithm→Access Condition→Unlock Condition

The unlock condition is to set the entire access mode, which includes several approval modes and their combinations.

The epidemic prevention mode means whether the requirement of body temperature, mask or QR code is met, which can be single or combination.

Single Approval	Face/card swiping	Face match succeeds or the card match succeeds, then pass with the unlock permission.
	ID card match	Compare between face and ID card, pass if the two matches
	Epidemic prevention passthrough	pass if the epidemic prevention requirements are met.
Combination Approval	Face+Epidemic prevention	The epidemic prevention requirement is met, face match succeeds, then pass with unlock permission
	Card swiping +Epidemic prevention	The epidemic prevention requirements are met, swiping card, then pass with registration and unlock permission
	Face+Card Swiping+ Epidemic prevention	The epidemic prevention requirements are met, then pass with successful face match and card number match

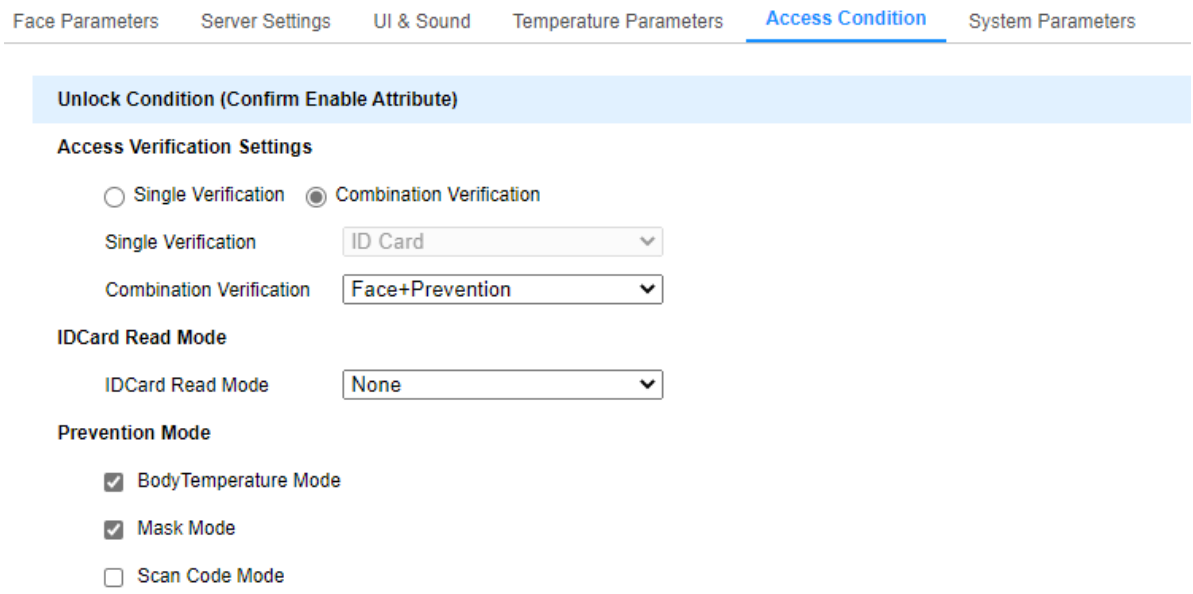
	Health code scanning+Epidemic prevention	The epidemic prevention requirements are met, scan the health code, then pass with non-red code

Meet the epidemic prevention requirement: meet all the ticked modes in the epidemic prevention mode options. If the body temperature is ticked, then the body temperature must be normal; If the mask is ticked, then the mask must be worn. If the code scan is ticked, then the QR code must be scanned（The QR code is just a record）.

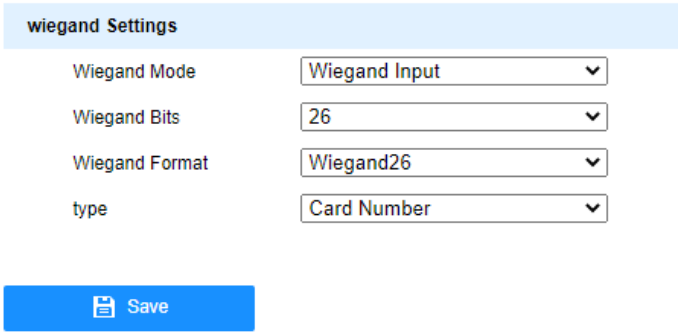
Face match succeeds: the face has been registered in the face database, and must be matched with the swiping face.

Card number match succeeds: the swiping card number has been registered in the face database. The card number can be read via USB card reader, built-in card reader or Wiegand.

Unlock permission: the person registered has white lists or permission group.



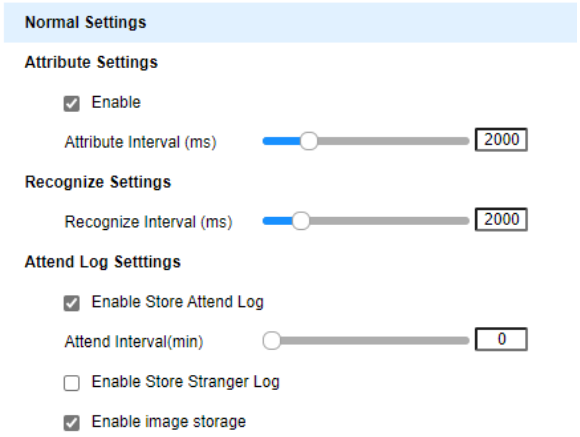
(13) Algorithm→Access Condition→Wiegand Settings.



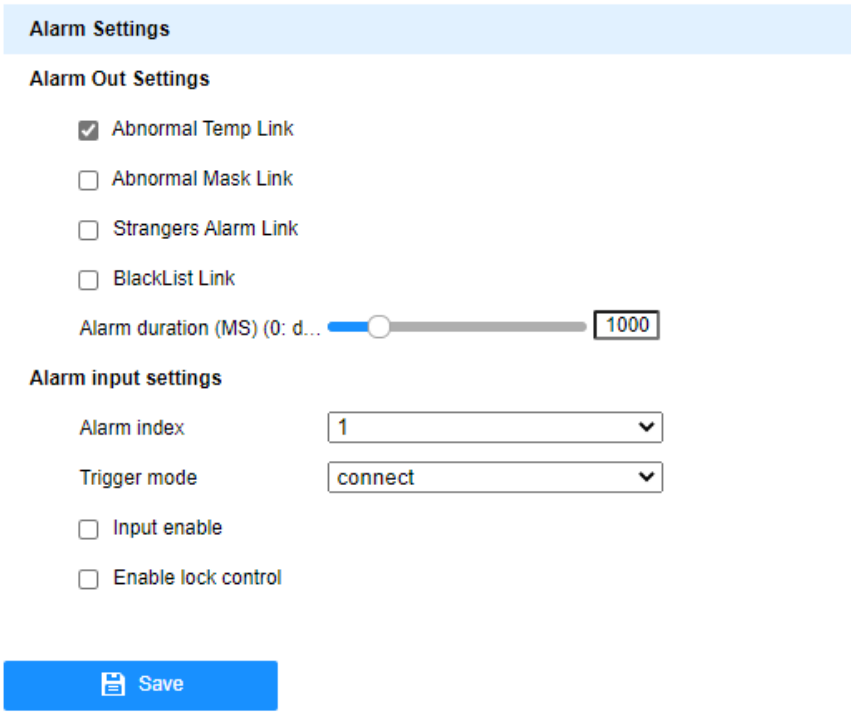
(14) Algorithm→System Parameters→Normal Settings.

The body temperature mode and mask mode should be ticked in the epidemic prevention mode, and also the attribute analysis should be enabled.

If the stranger attendance is not ticked, then the unmatched face records will not be saved in the attendance records after the attendance records function is enabled.



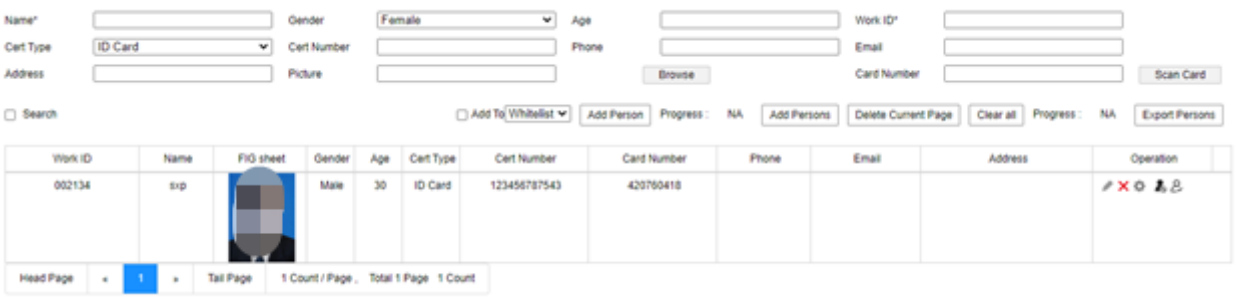
(15) Algorithm→System Parameters→Alarm Settings.



1.8 Face Database

1.8.1 Add Face

The face database can be added, viewed, changed and deleted on the face adding interface.

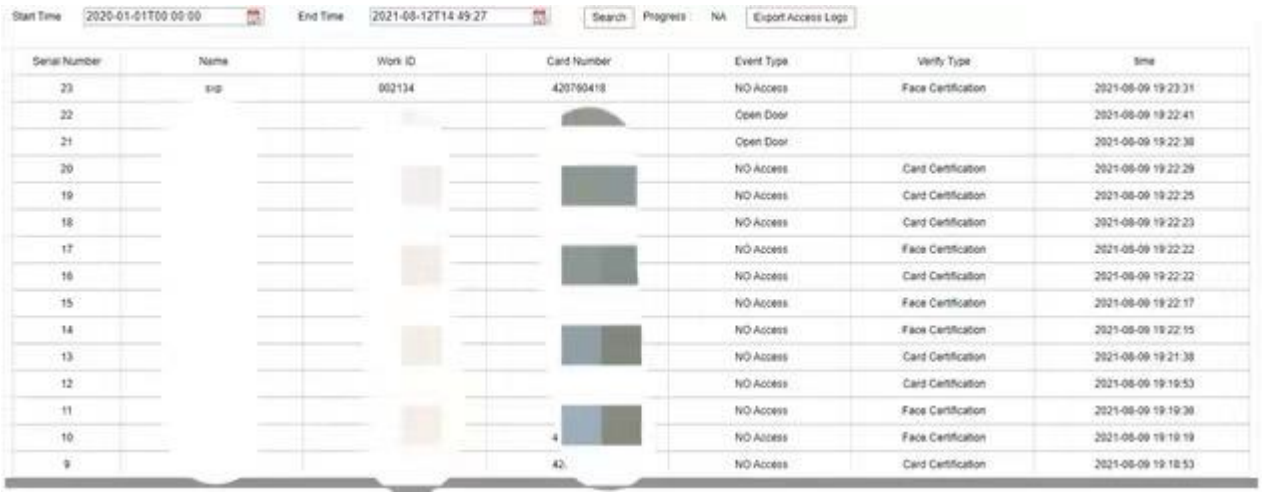


1.8.2 Snapshot Records

Perform real-time person information snapshot, and the enquiry during a given time period is available and attendance records can be exported.

1.8.3 Access Daily Record

All the access information can be searched and exported.



2. Client Software Operation

You can configure and operate the screening terminal through the ARFaceManager client software. This chapter mainly introduces access control related functions and

operation steps.

2.1 Preview Videos

2.1.1 Real-time Preview

2.1.1.1 Real-time Images

The real-time preview interface can watch the real-time images of a group of 4 devices at the same time. If there are more than 4 devices in the local area network, you can right-click in the preview window, and then select the next group/previous group in the pop-up menu.

2.1.1.2 Save Captured Images

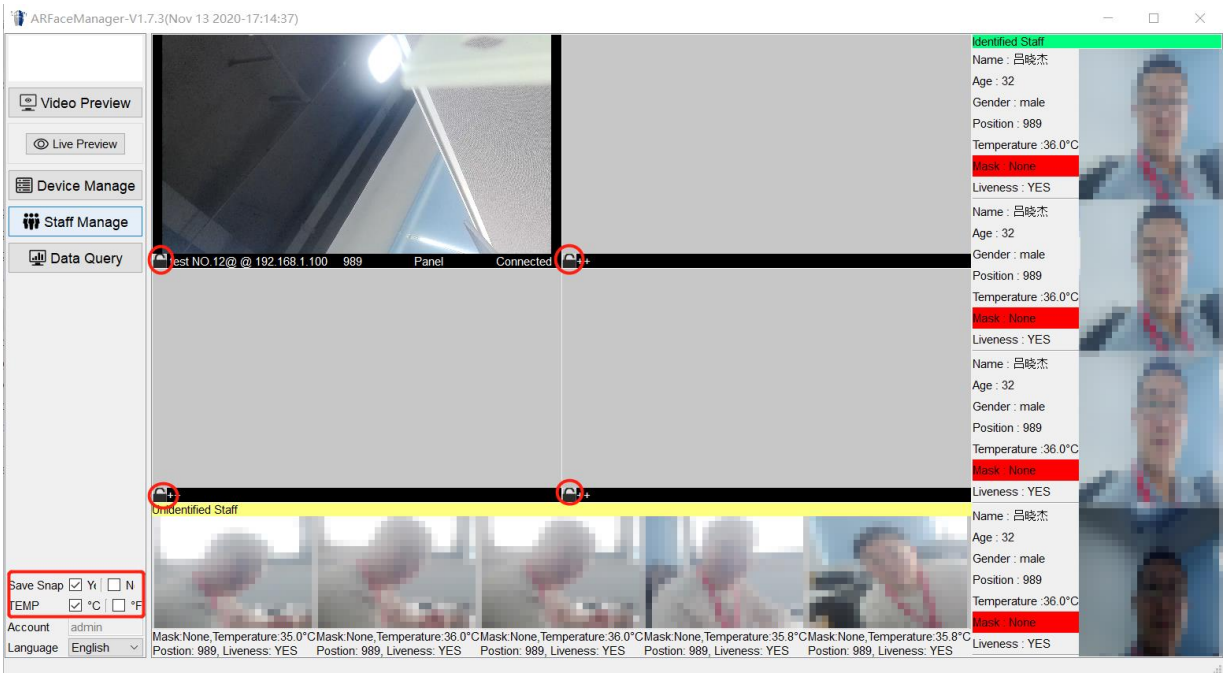
You can set whether to save the captured images. When set to No, the screening terminal will not save (nor export) the captured images.

2.1.1.3 Display Temperature

The temperature unit displayed on the preview interface can be set **(this setting has nothing to do with the temperature unit displayed on the panel or in the export table).**

2.1.1.4 Enable Door Lock

After the screening terminal is correctly connected to the door lock, click the "Unlock" in the red circle to enable the door lock.



2.2 Device Management

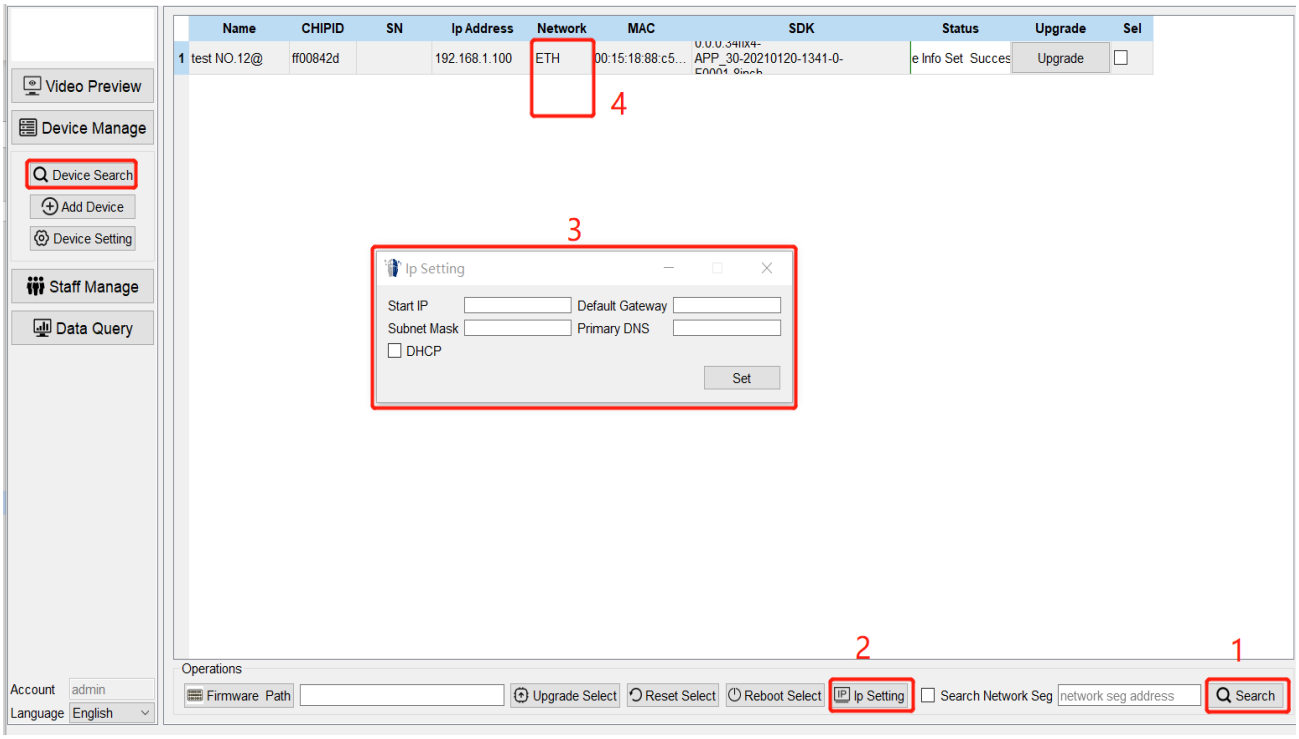
2.2.1 Search and Add Device

Device Manage→Device Search

● Click 1 “Search” button to search, the searched device will be displayed in the list.

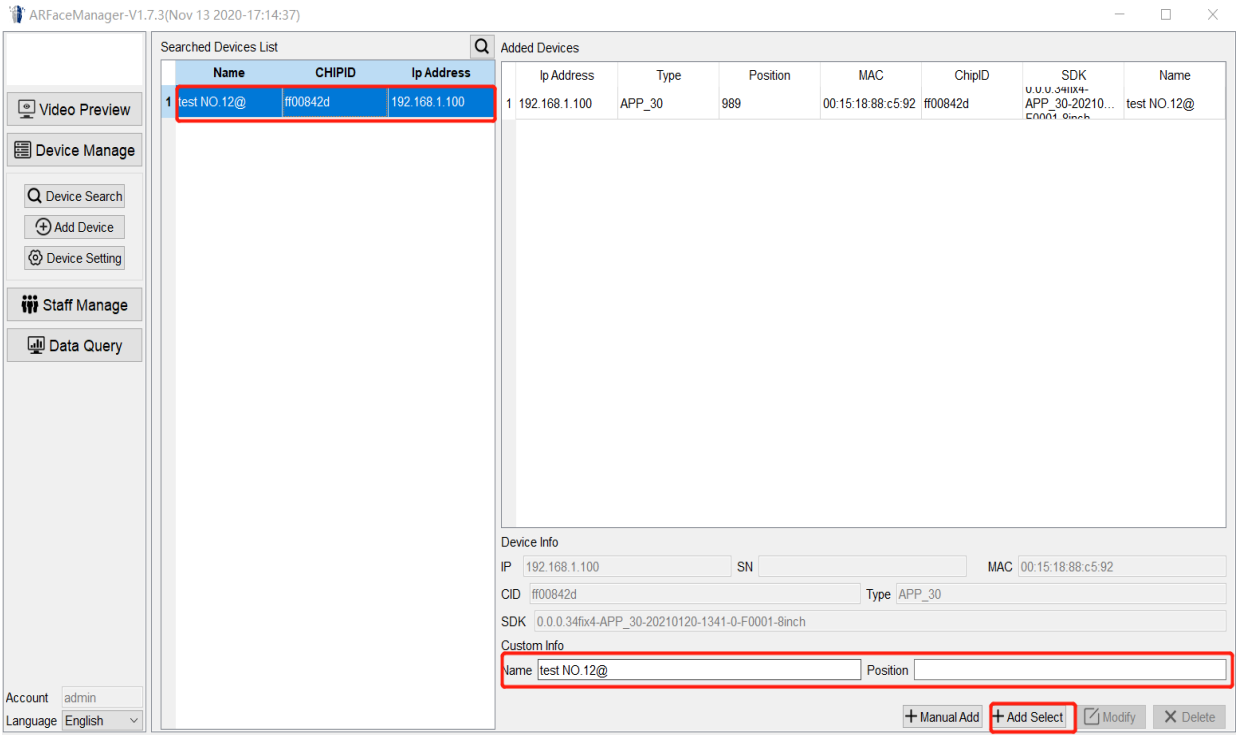
● Select the device in the list, and then click 2 "IP Settings" button. You can modify the IP of the selected device in the pop-up window.

● The "Network" in the device list indicates the network type of the device (E.g. 4), ETH indicates wired, and WLAN indicates wireless. When the device has both wired and wireless networks, the wired device is displayed first.



Device Manage→Add Device

Select the camera to be added, fill in the device name (required) and position (required), and click the “Add Select” button.

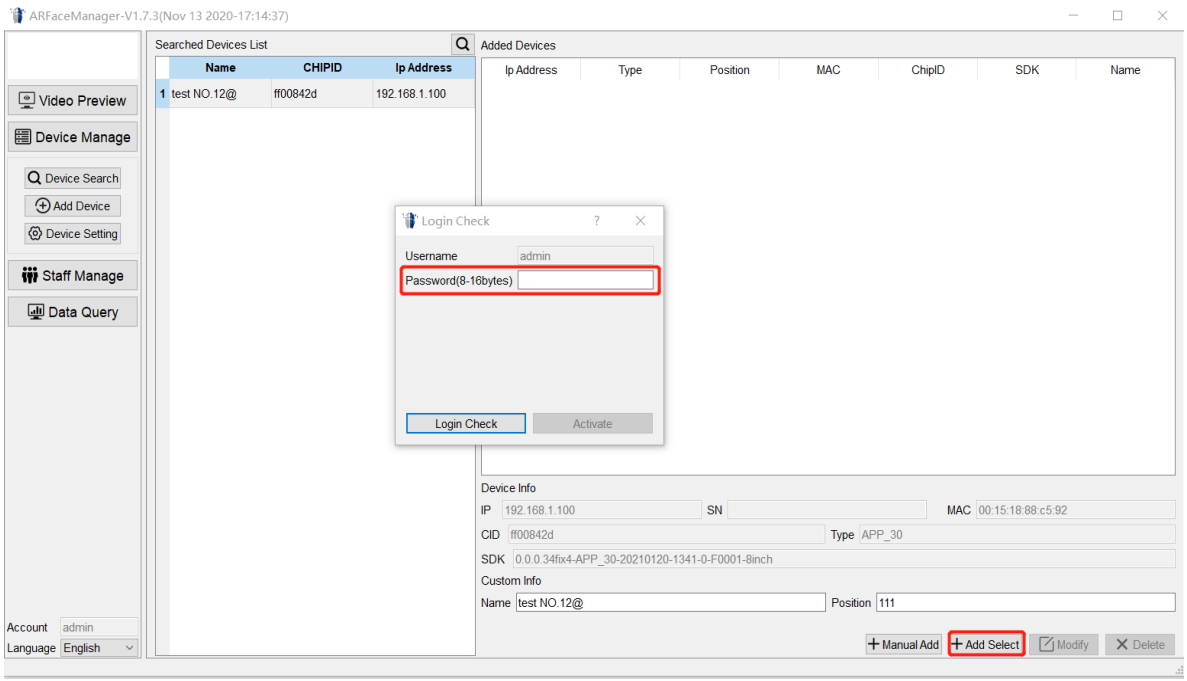


In the verification window that pops up, enter the Web login password of this device, click “modify”, and the addition is successful.

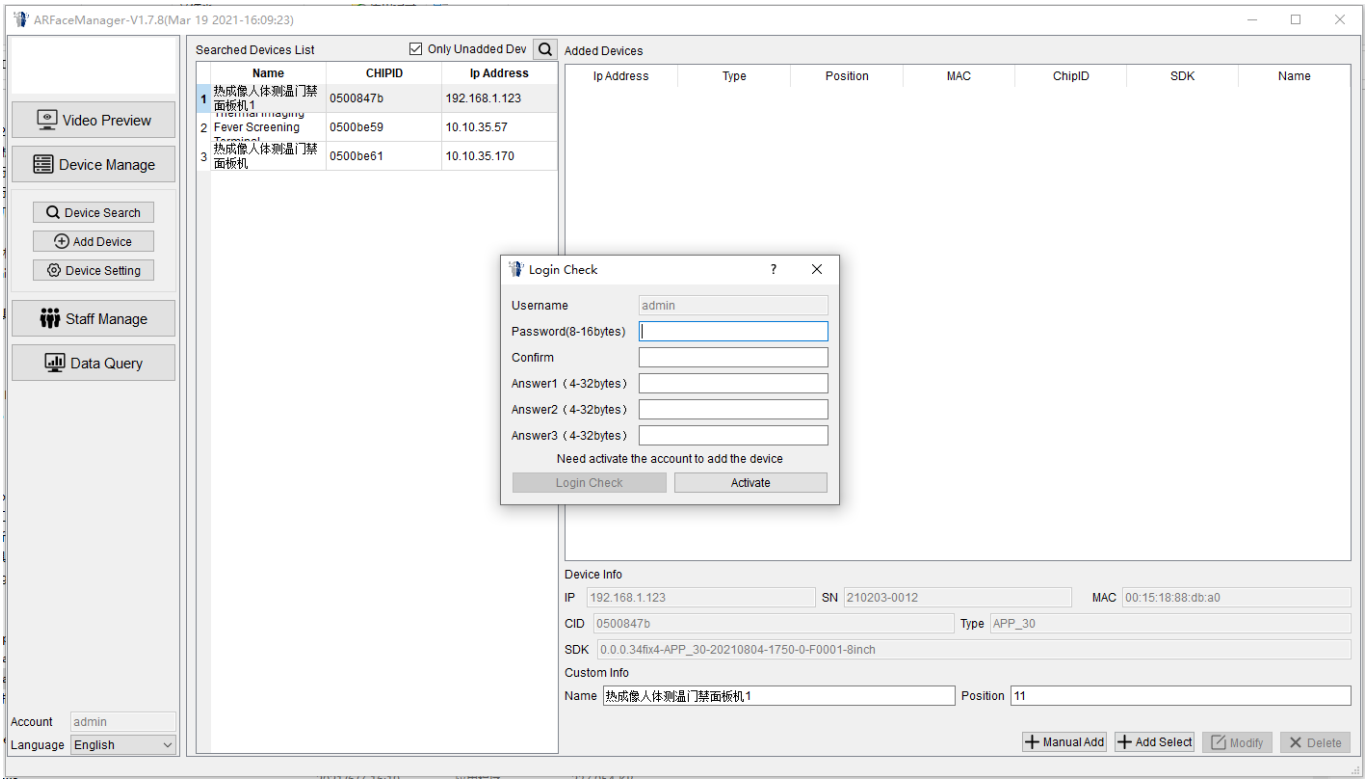
If the device has not set a Web login password, you need to set the Web login password and security answer first, and click “Activate” to complete the addition.

Update added device information

When the device is upgraded or the network information of the device is modified through other means, the search operation is performed.



If the device can be searched again, the information of the device in the "Added Device" database will be updated to the latest.



2.2.2 Camera Settings

Camera settings include system, communication, video and audio, images, and intelligent analysis.

2.2.2.1 System Settings

Check the basic information of the device, and the time configuration.

NTP Setting:

1. Configure server IP address and port number, update period and time zone.

2. Tick "Enable NTP".

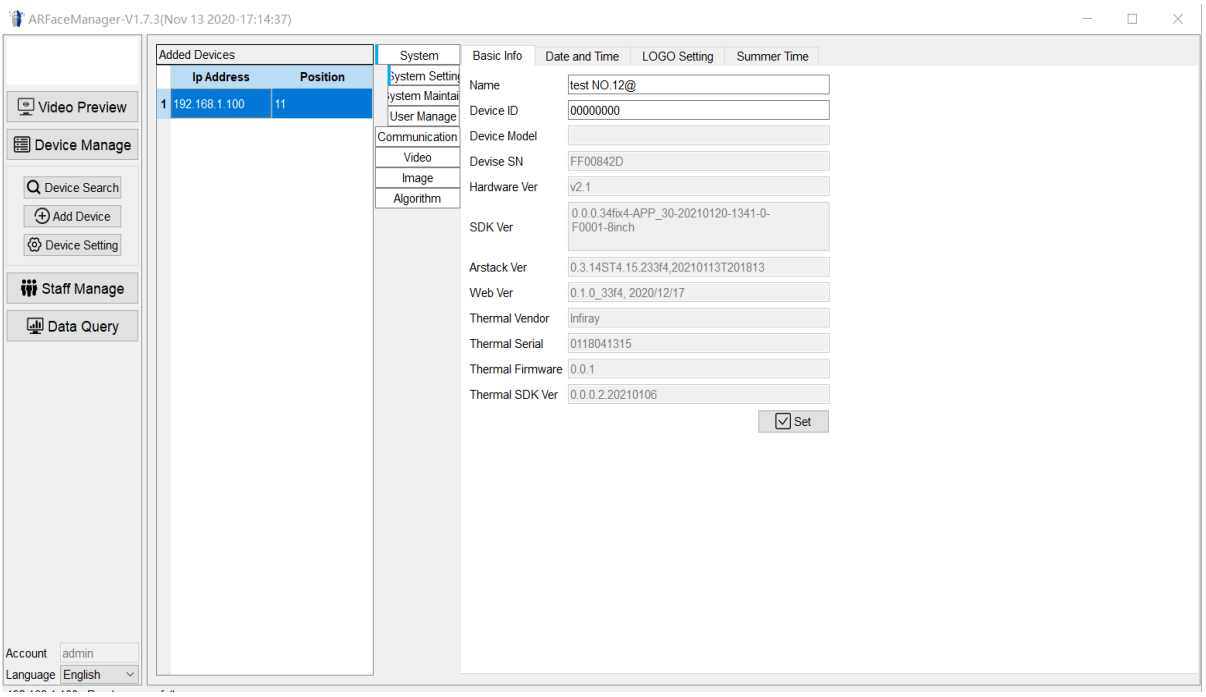
3. Click "Set", and the parameters will be synchronized to the device.

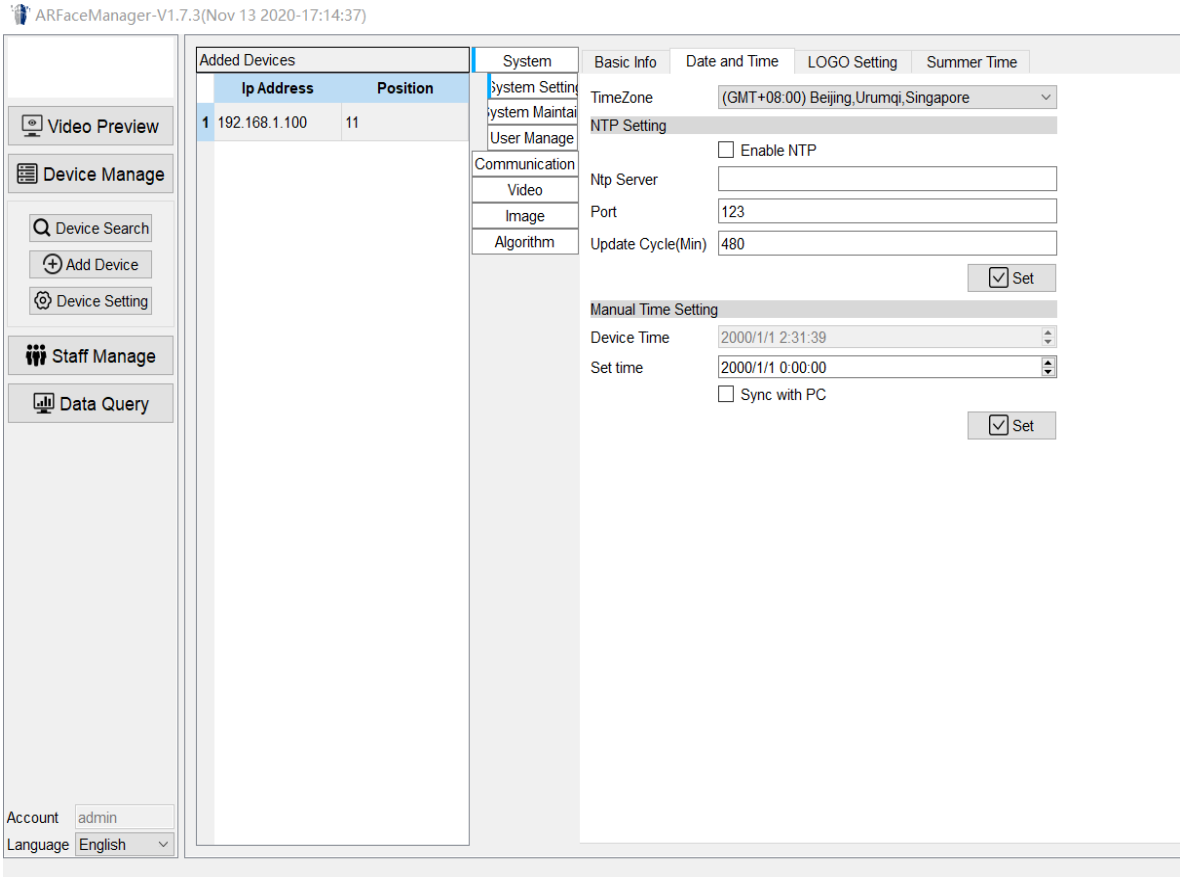
Manual Time Setting:

1. Manually set the time of the device. After the completion of setting, the device will rely on the RCT circuit for automatic timing.

2. Tick synchronization with computer time, and the device will automatically synchronize the current time and time zone from the computer.

3. Click "Set", and the parameters will be synchronized to the device.





2.2.2.2 Communication

- Wired Lan

Static IP settings:

1. Uncheck "Enable DHCP".

2. Configure IP address, default gateway, subnet mask, and DNS.

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

DHCP settings:

1. Check "Enable DHCP".

2. (Optional) Fill in "Preferred DNS" and "Backup DNS".

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

- Wireless Lan

Connect the WiFi

1. Fill in the SSID and password to connect to the wireless network;

2. Select "wireless network card" as network mode;

3. Click "Set" and the device will be connected to the WiFi network.

Set it as a WiFi hotspot

1. Set the SSID and password of WiFi;

2. Select "hotspot mode" as network mode;

3. Set the default gateway, or use the default gateway;

4. Click "Set", and the device will share WiFi hotspots for mobile phones or PCs connection.

PS: using the hot spot mode, the device can be connected with the mobile phone

and other devices point-to-point, and the access control can be managed through the mobile phone and other devices.

- HTTP

1. Enter the HTTP and HTTPS ports to set;

2. If you need to update the HTTPS license, check "Upload Certificate" and click the "File Selection" button to select the certificate file;

3. Click "Set" to set the corresponding parameters;

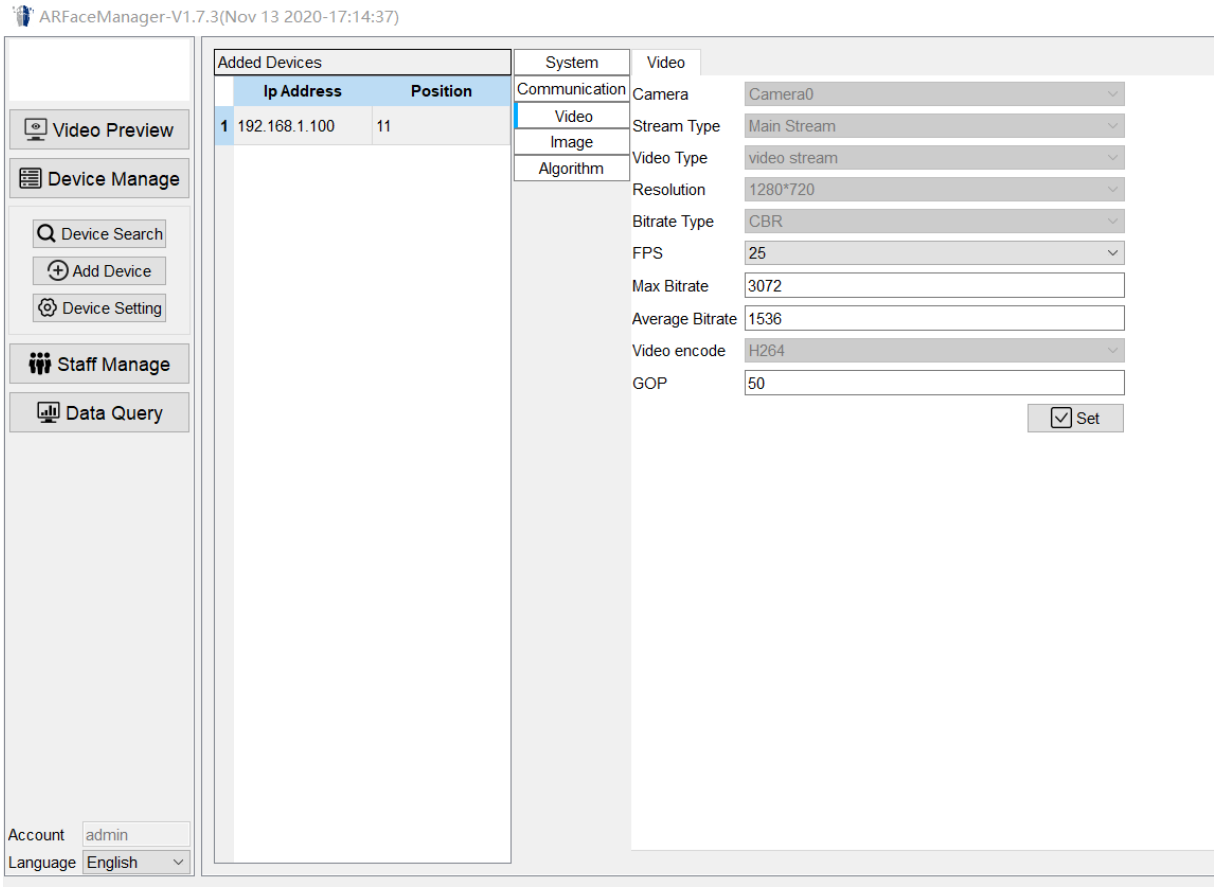
(Note: after modifying the above port, you need to use the modified port to access the Web page normally.)

2.2.2.3 Audio and Video

- **Video**

The video stream parameters of real-time preview can be set, including the resolution, the upper and lower limits of the stream.

PS: fluorescent lamps in different countries have different luminous frequencies, which may cause the display to flicker. This problem can be solved by setting different video frame rates.



2.2.2.4 Image

- Image Setting

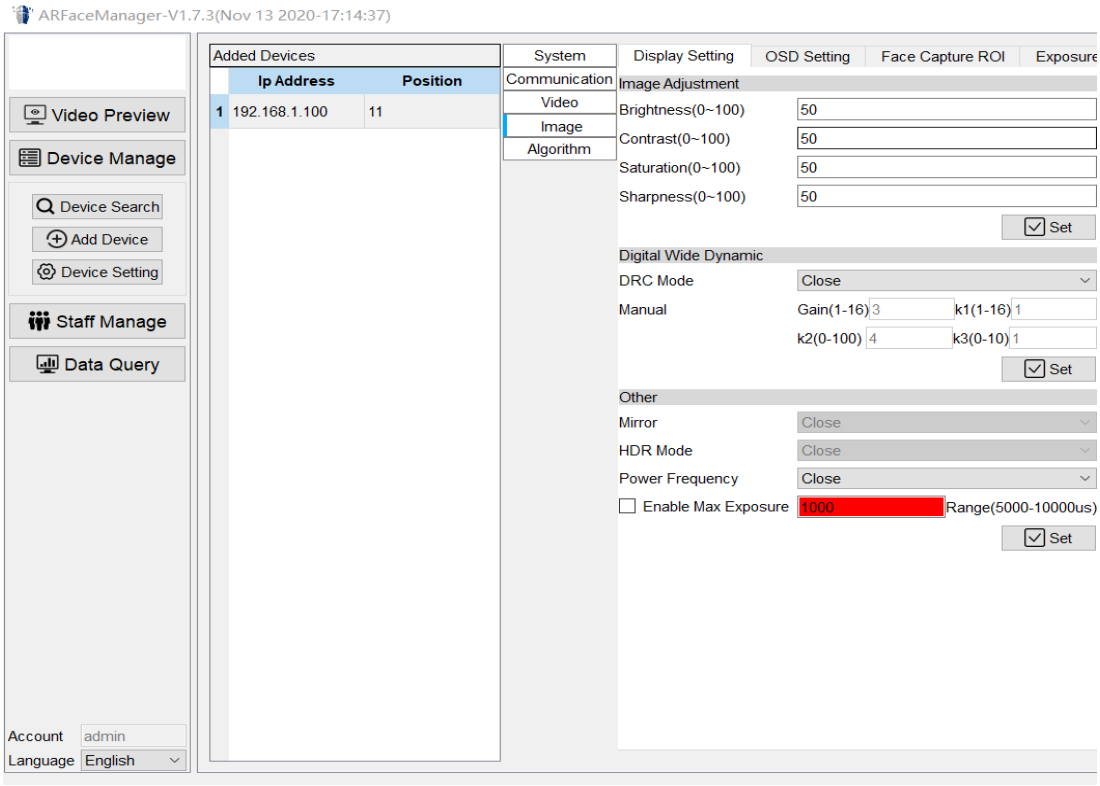
Set display brightness, contrast, saturation, sharpness and other parameters of the device.

- Digital Wide Dynamic Settings

It can be set to adaptive, close or manual mode.

- Other Settings

Other settings include image mirror, HDR mode, power frequency, and exposure limit.



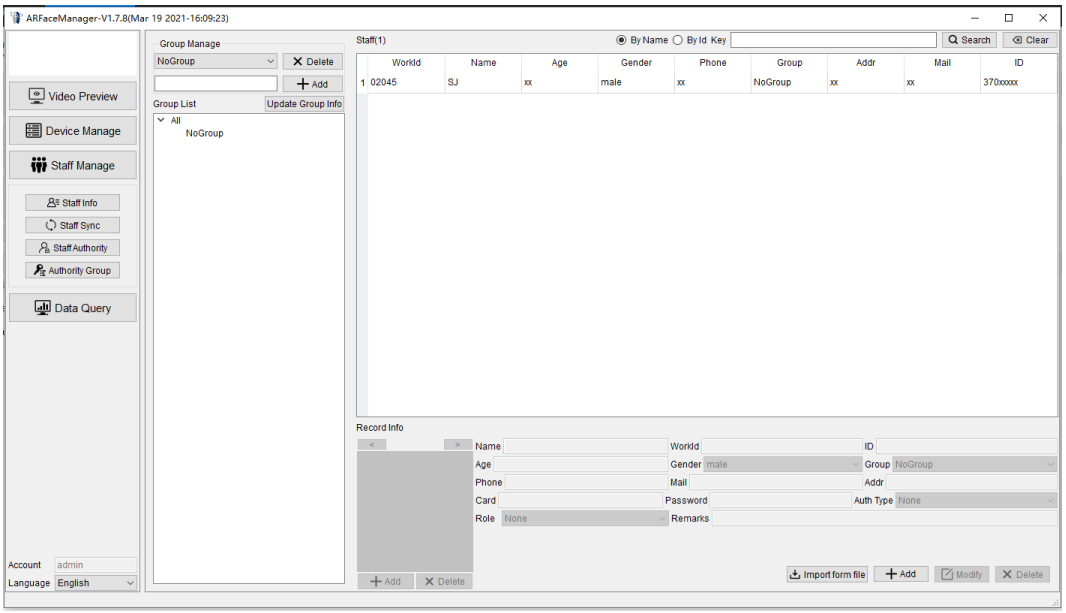
2.2.2.5 Algorithm

Please refer to the algorithm in the web configuration.

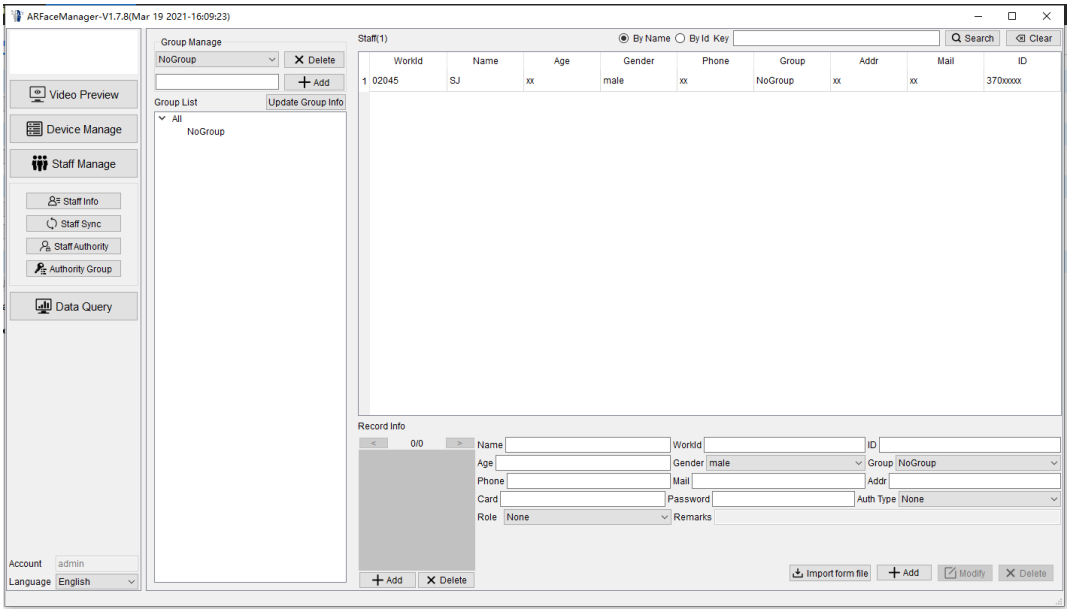
2.3 Staff Management

2.3.1 Add Single Staff

1. Click "Staff Manage" → "Staff Info" on the left side of control panel.



2. Click "Add " button and the staff information becomes available for editing.



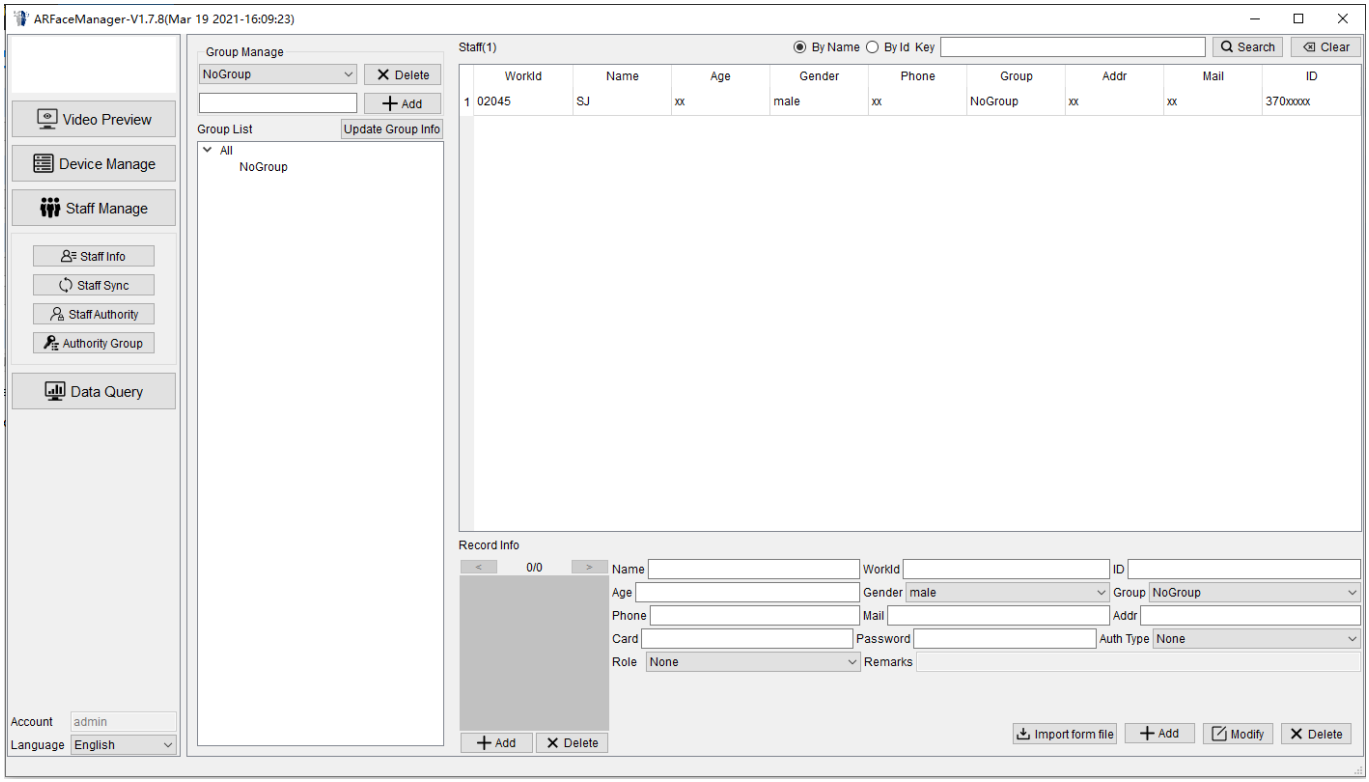
3. Name, employee number (from 1～99999999), certificate, and headshot are required fields. The other fields are optional.

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

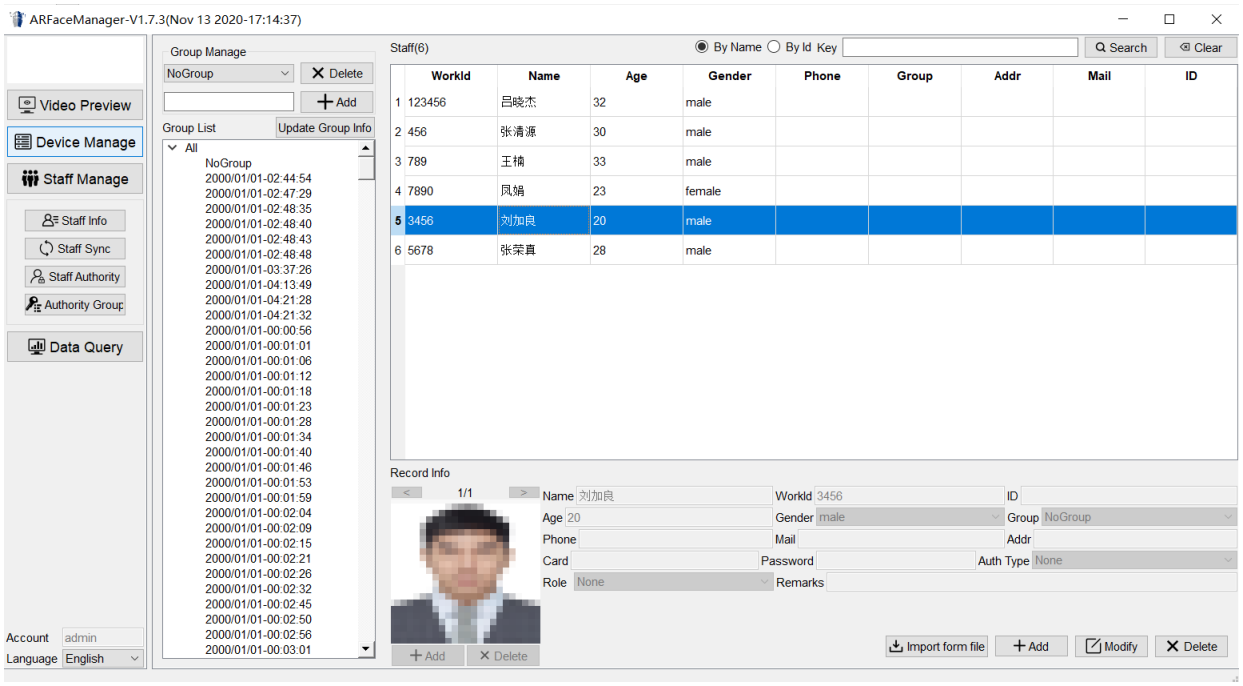
2.3.2 Add Staff from File

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 model document *saff.xlsx* in configuration tools.



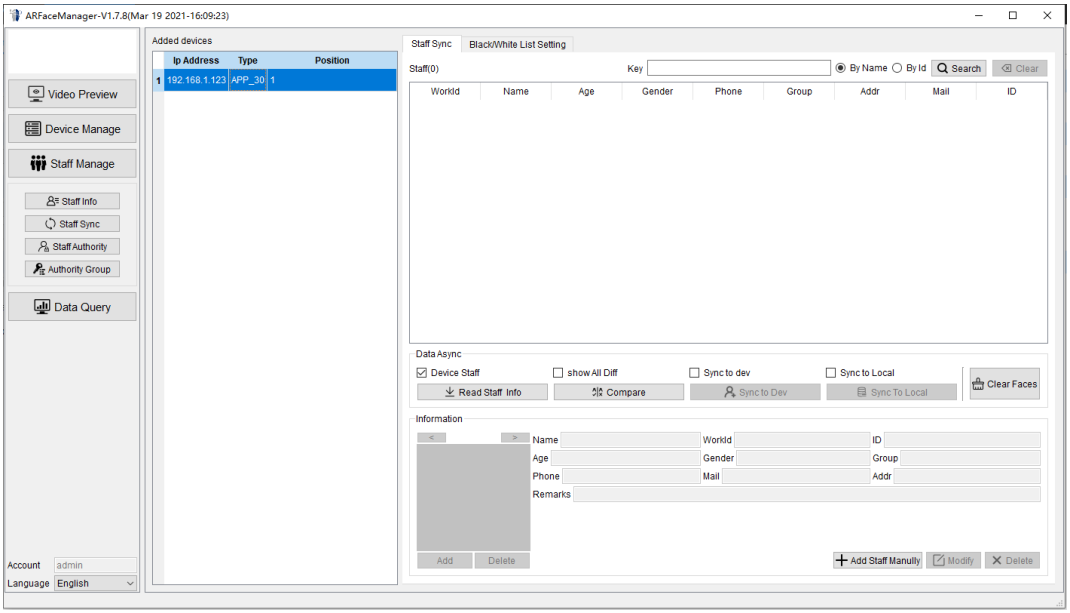
3. Click "Open" and complete the import.



2.3.3 Edit Staff Information

1. Click "Staff Manage" → "Staff Sync" on the left side of control panel.

2. Click "Modify" and the staff sync becomes available for editing.



3. Click "Confirm" after editing. The data will be stored in the local database of the

client.

- **Modify Staff Information**

1. Click "Staff Manage" → "Staff Sync" on the left side of control panel.

2. Select a staff and click "Modify" button to edit staff information.

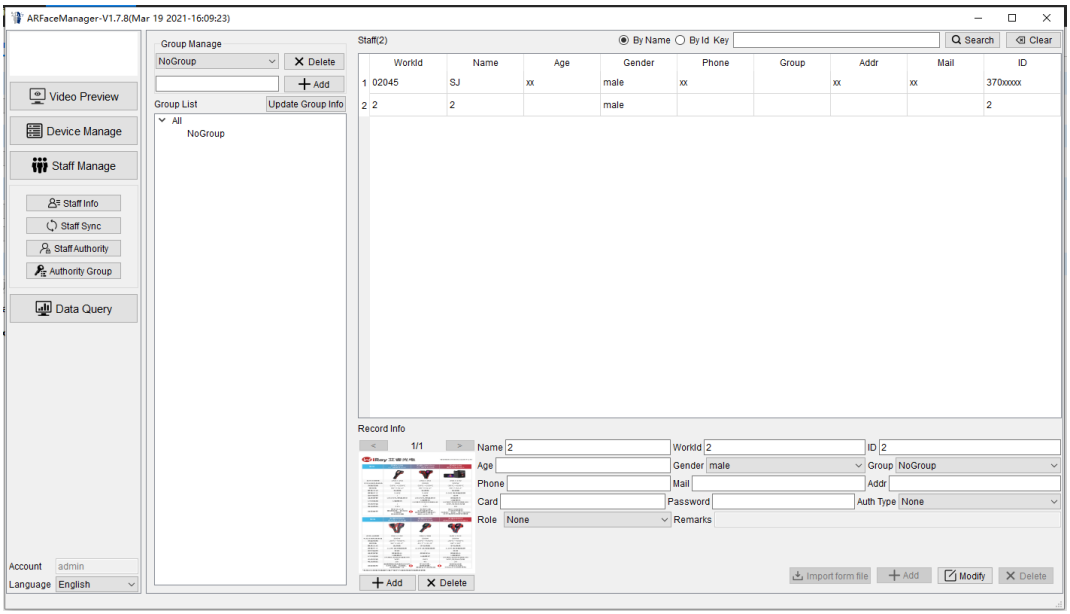
- Add Faces

1. When entering the editable mode, click the "Add/Delete" button below the face picture to add/delete the face picture;

2. You can add up to 3 face pictures, and switch to display different faces through the index button above the face picture;

- Modify groups in batch

1. When a group of persons are selected at the same time, the group information of the currently selected persons can be modified in batches, but other information cannot be modified;



2. After editing, click the "Modify" button again to save the data to the client's local database.

2.3.4 Delete Staff

● Delete staff one by one

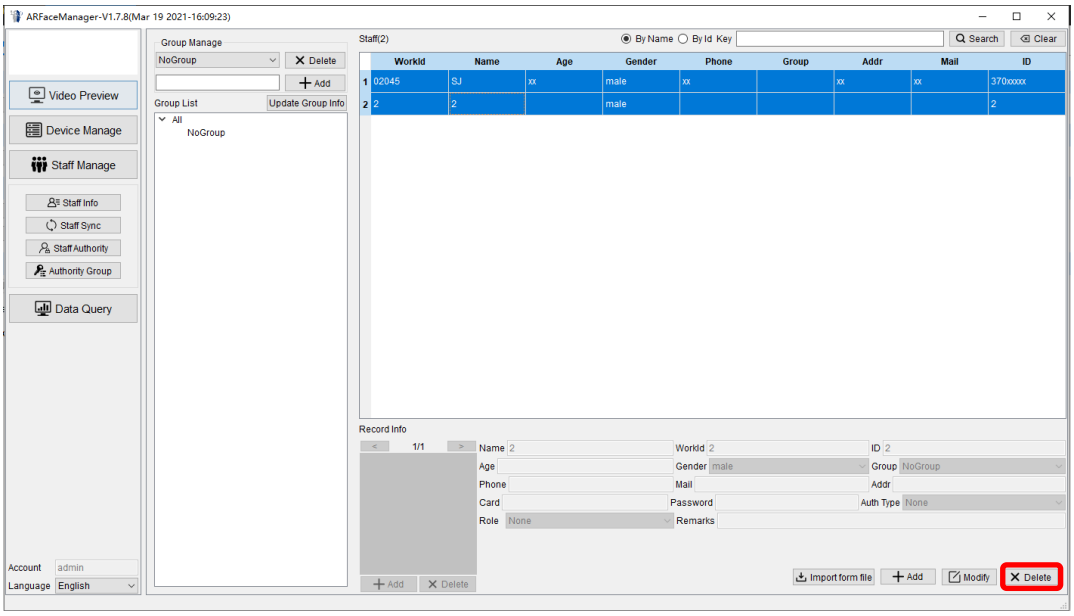
1. Select the staff to be deleted;

2. Click "Delete";

● Delete staff in batch

1. Hold down the Ctrl key to select multiple staff or Ctrl+A to select all;

2. Click "Delete";

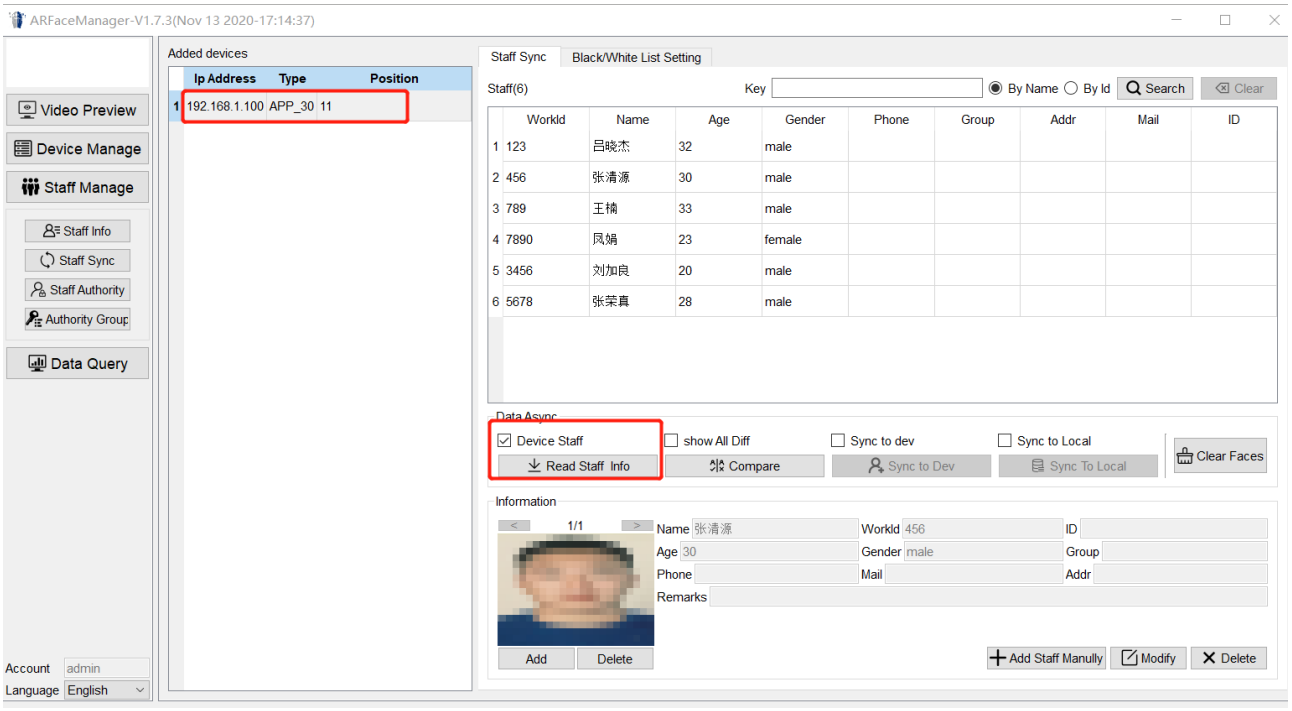


2.3.5 Staff Sync

Staff sync refers to uploading the staff added to the local database to the device.

Click "Staff Manage" → "Staff Sync" on the left side of control panel.

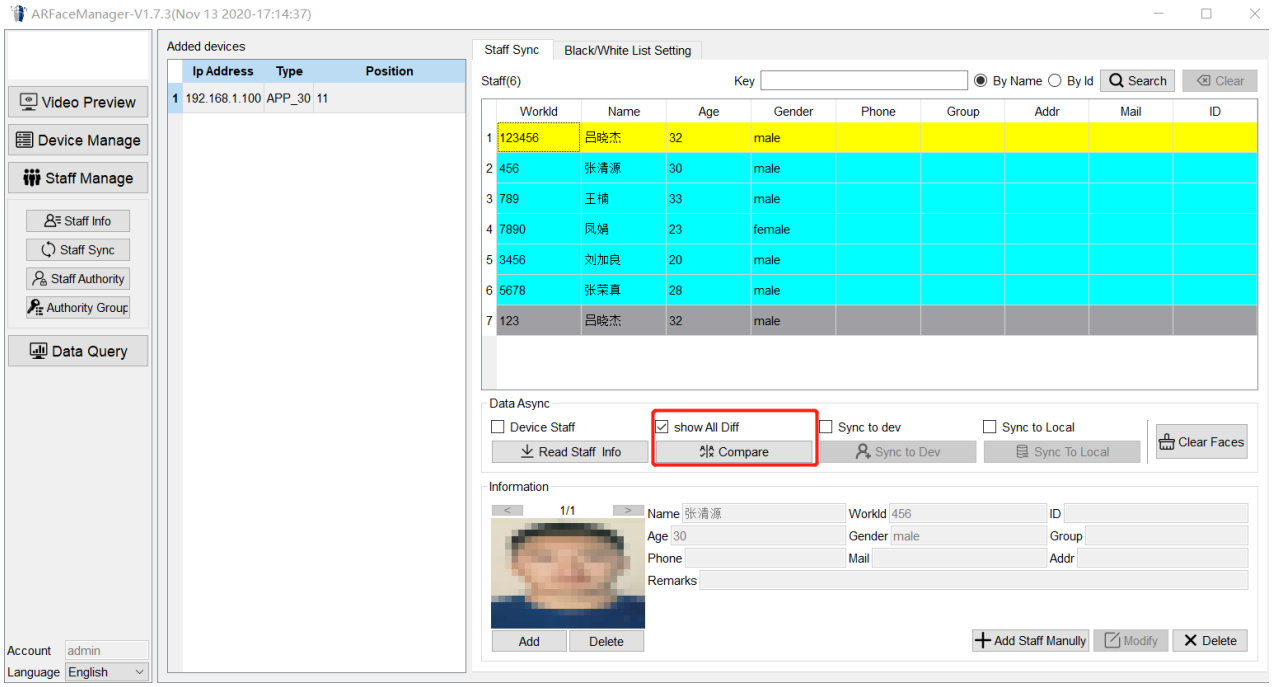
1. Select the device that needs to be synchronized, and click "Read Staff Info" to synchronize the device staff data to the client;



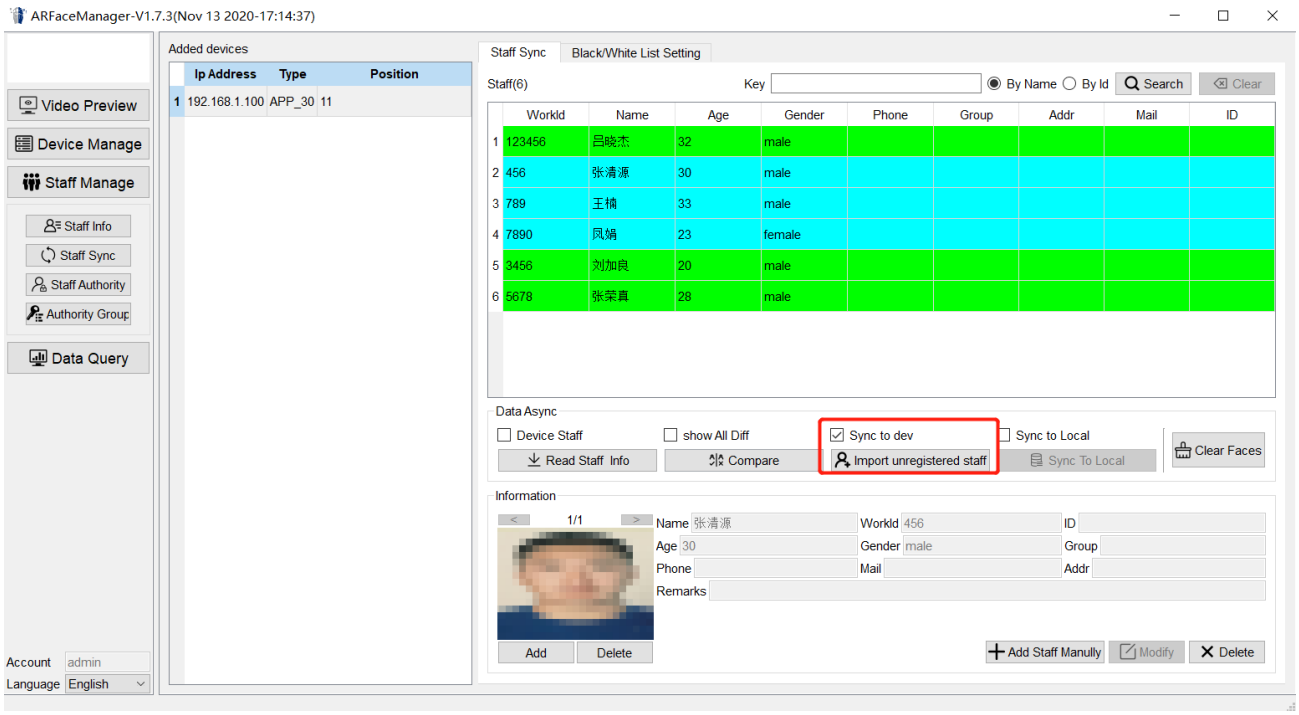
2. Click "Show All Differences", and click "Compare".

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.

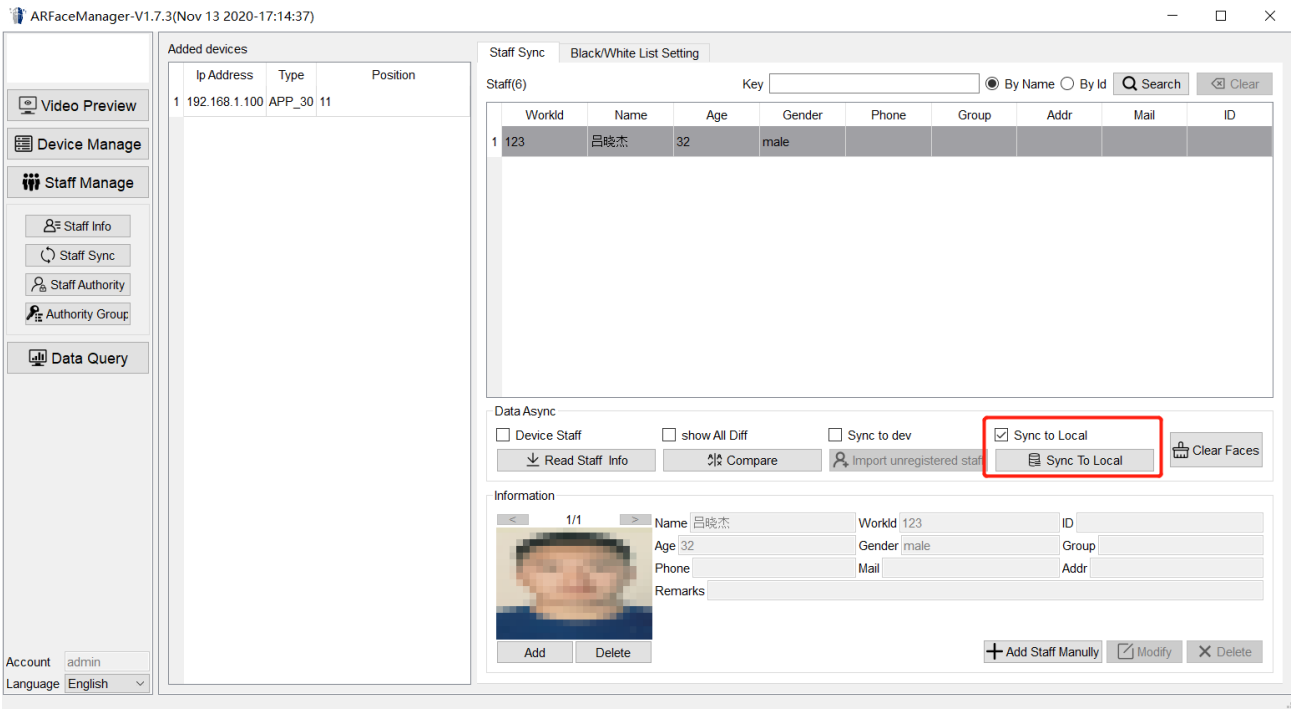


3. Check "Sync to dev", and click "Sync to dev" to import staff from the local client to the device.



4. Click "Sync to local", and click "Sync to local" to import data from the device to

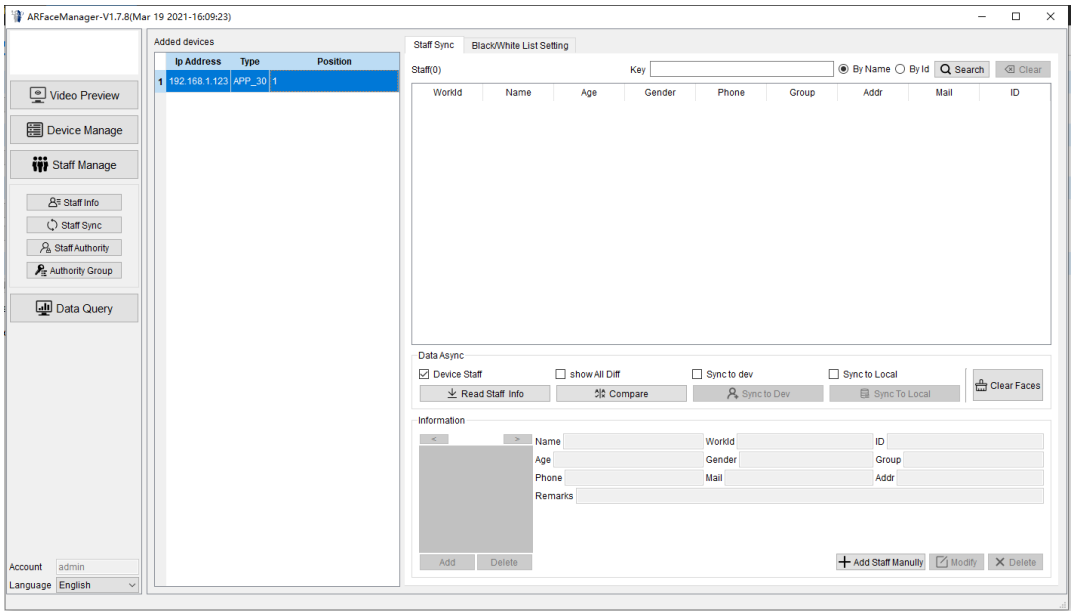
the local database.



2.3.6 Clear Staff Information in Device

Click "Staff Manage" → "Staff Sync" on the left side of control panel.

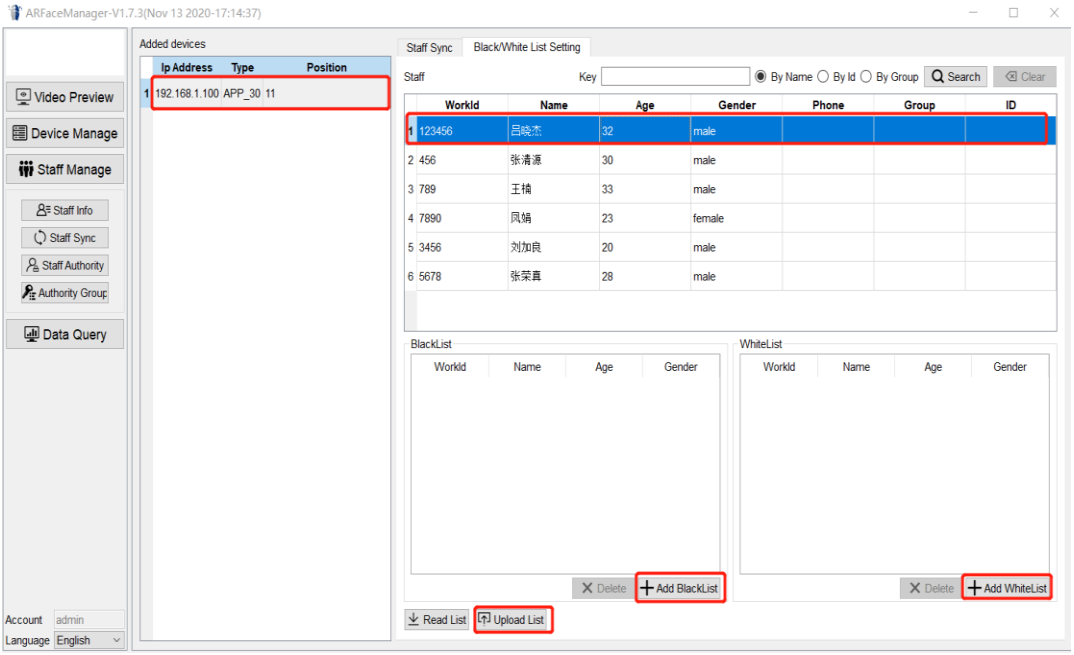
1. Click “Clear Faces” and click “Read Staff Information” to check whether all information is cleared.



2.3.7 Blacklist and Whitelist Setting

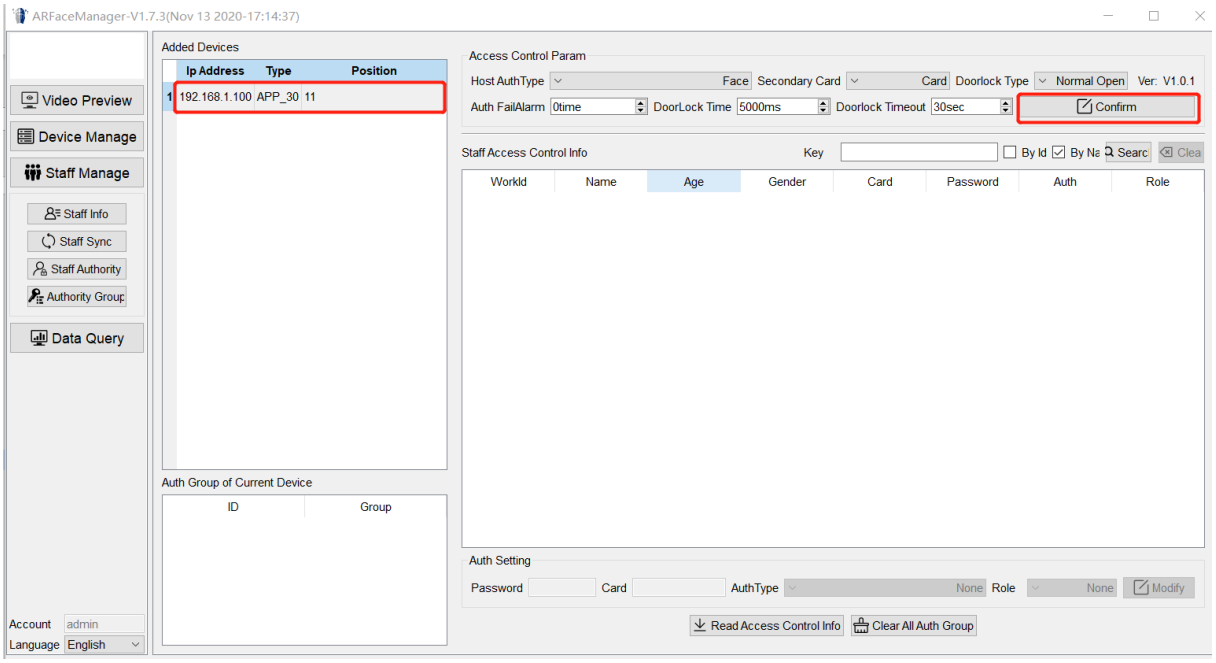
Click "Staff Manage" → "Staff Sync"→"Blackwhite list setting" on the left side of control panel.

1. Select devices for synchronization.
2. Select the staff to add to the blacklist or whitelist.
3. Click "Add to Blacklist/Whitelist".
4. Click "Upload List" to upload the blacklist and whitelist to devices.



2.3.8 Device Access Control Parameters

Click "Staff Manage" → "Staff Authority" on the left side of control panel.



1. Click "Change Parameters".

2."Host Auth Type", "Secondary Card", "Doorlock Time", "Doorlock Timeout" are

subject to change.

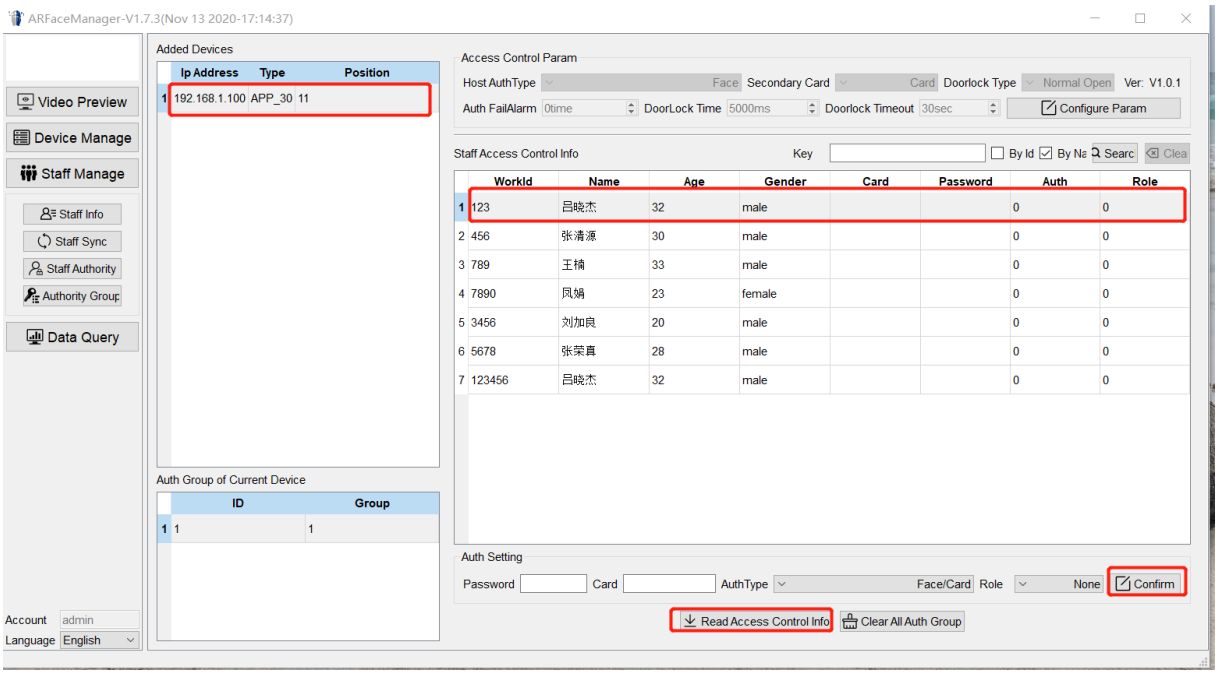
3. Click "Confirm" and the parameters will be synchronized to the device.

Access Control Parameters	Parameters Description
Host authentication methods: it configures the authentication method of the device. Select different combinations to set up your authentication method.	Face is the default setting. O**nly face or face + card swiping is supported.**
Secondary card authentication: set up for connection to an external card reader. The types of authentication are the same as those of the device.	Only card-swiping and password are supported. Card swiping is the default setting.
Magnetic door switch options: None: no door magnetic switch is used. Normally open: the door is open under normal conditions (always open when the power is on). Normally closed: the door is closed under normal conditions (always closed when the power is on).	0 - none 1 - normally open 2 - normally closed (default)
Time for door locking: the duration of time from opening to automatic locking when the door is closed.	1～255 seconds. 5 seconds by default.
Door open timeout alarm: when the magnetic state of the door is inconsistent with the settings, an alarm signal will be issued 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 alarm: when the number of failed verifications (that is, the number of wrong presses) reaches the set value (can be set to 1-9 times), an alarm signal will be issued.	0～9. 0 by default, meaning that no alarm.

2.3.9 Staff Access Control Information

Click "Staff Manage" → "Staff Authority" on the left side of control panel.

1. Click "Read Access Control Information".
2. Select the staff to be edited.
3. Click "Configure Param" to change the password, card number, authentication method (**currently, only facial and face with card authentication is supported**), or role of the personnel.
4. Click "Confirm" and the parameters will be synchronized to the device.

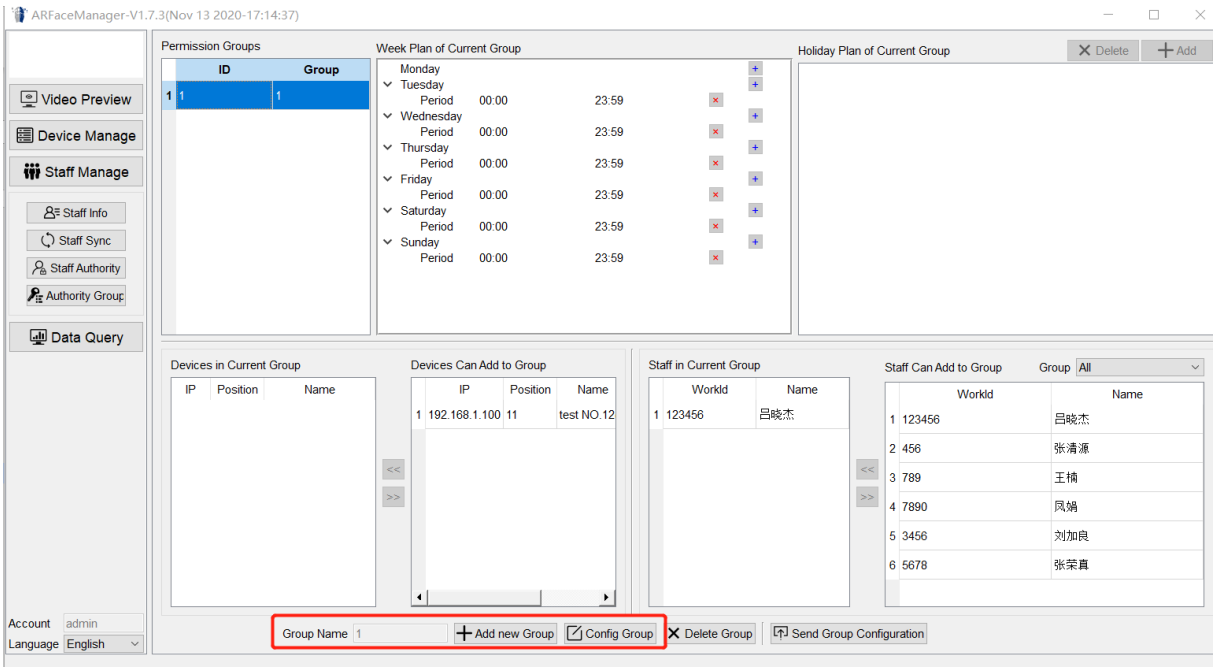


Note: the default authentication method is host authentication. When a user sets up a private authentication method, the device will use the user-personalized method.

2.3.10 Add Permission Groups

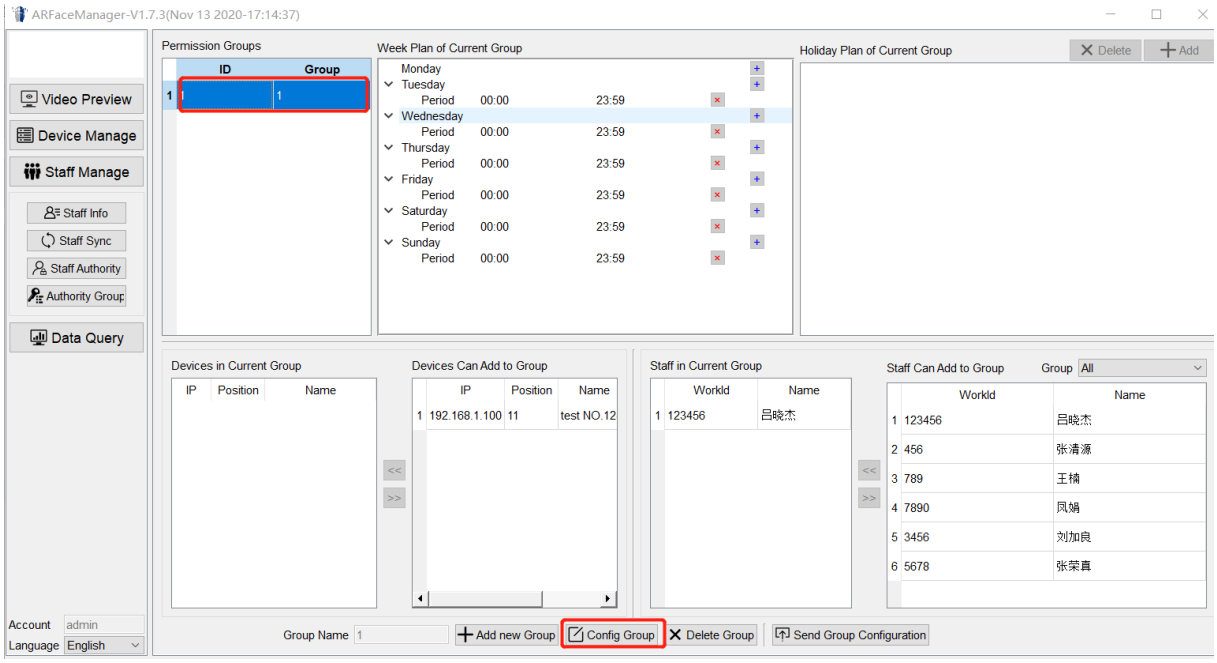
Click "Staff Manage" → "Authority Group" on the left side of control panel.

1. Click "Add new group";

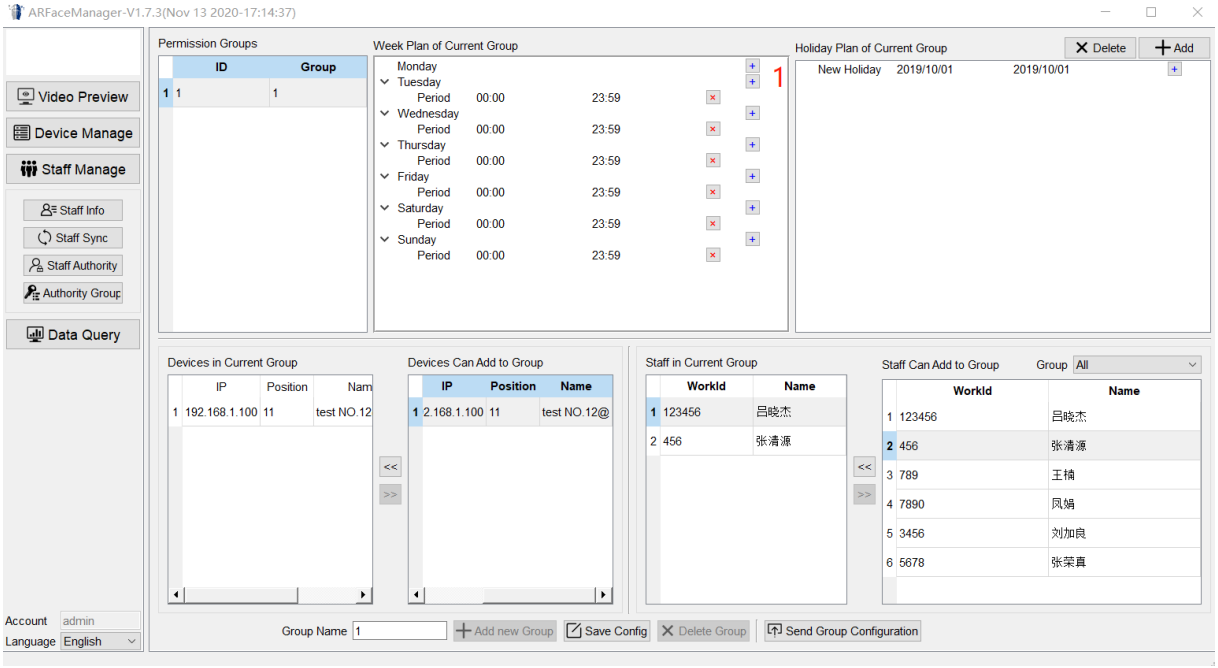


2. Fill in "Group Name" and then click "Confirm";

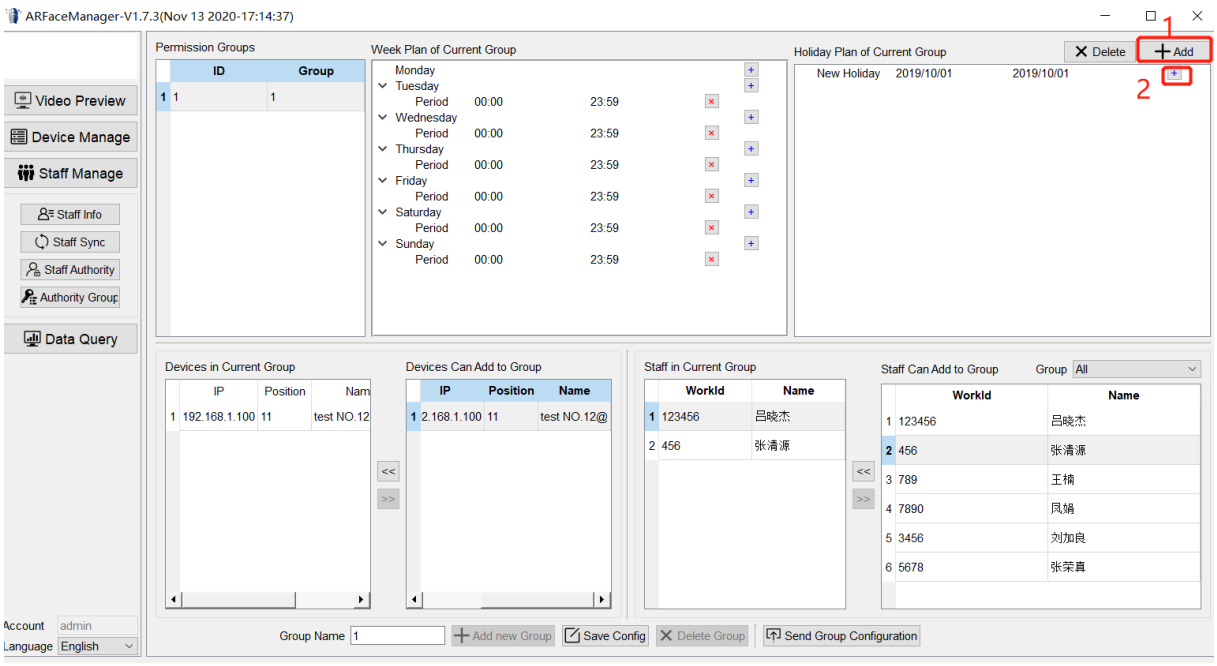
3. Click "Config Group" to edit the group;



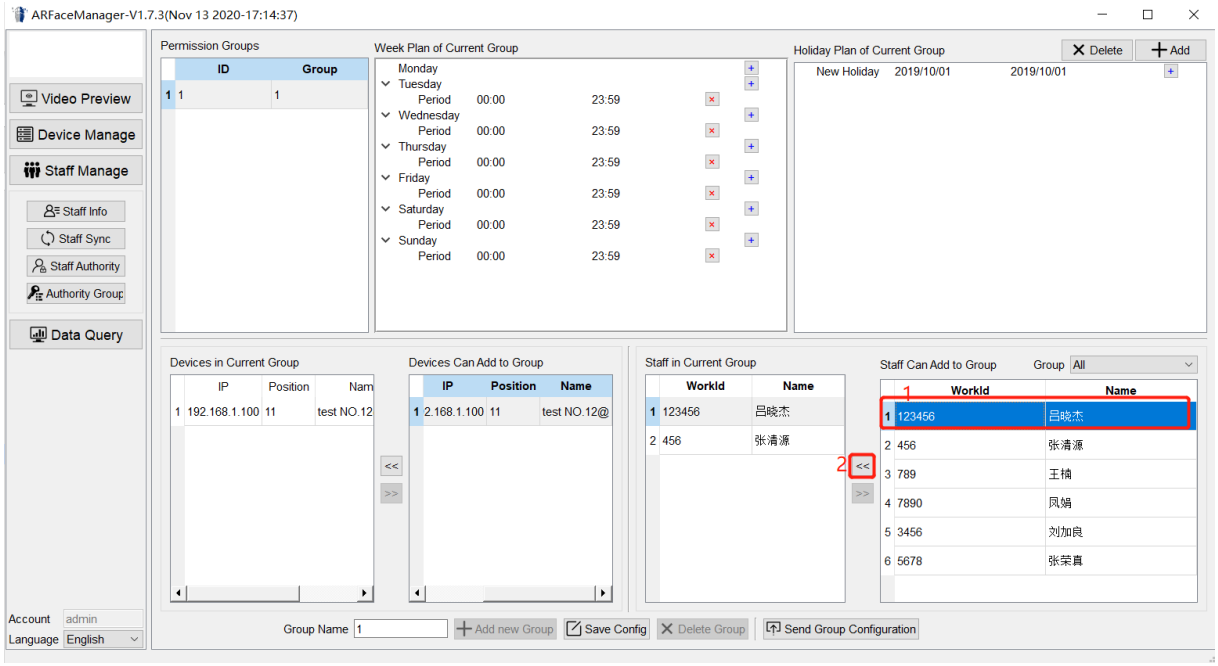
4. Edit Week Plan. "+" button can add a time period, "x" button can delete a time period, and up to 24 time periods can be added every day;



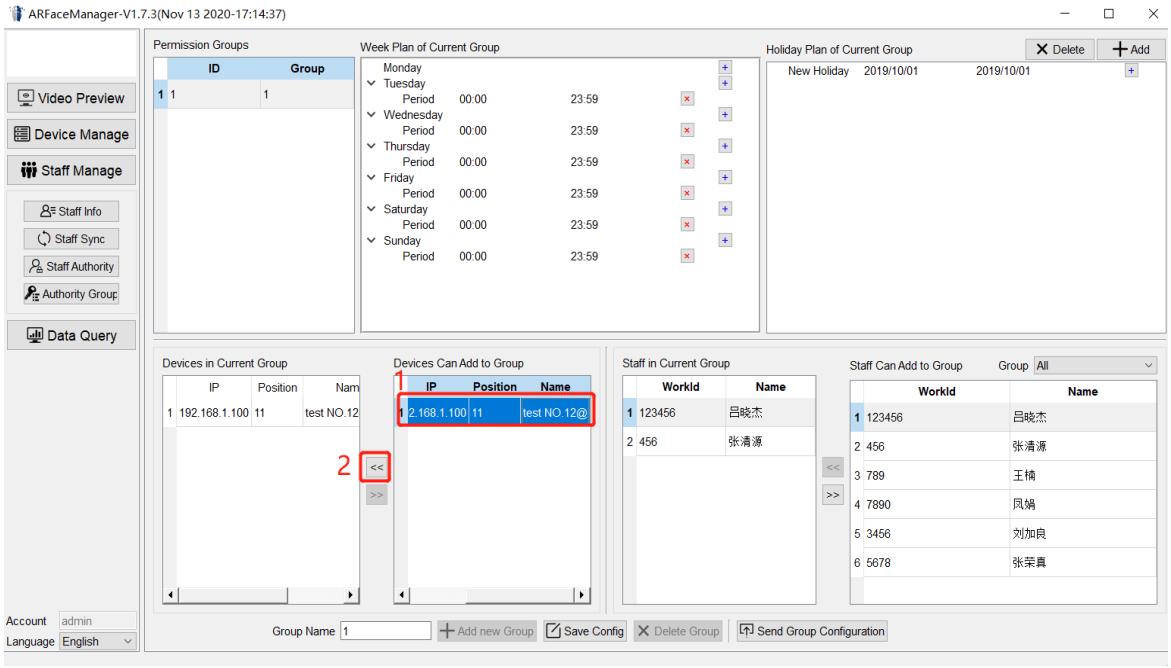
5. Edit Holiday Plan. Click "add" to edit the holiday name, start and ending date.



6. Associate the staff. Select the staff to be associated in the "Staff Can Add to Group", click "《" button, and add them to the "Staff in Current Group" list;



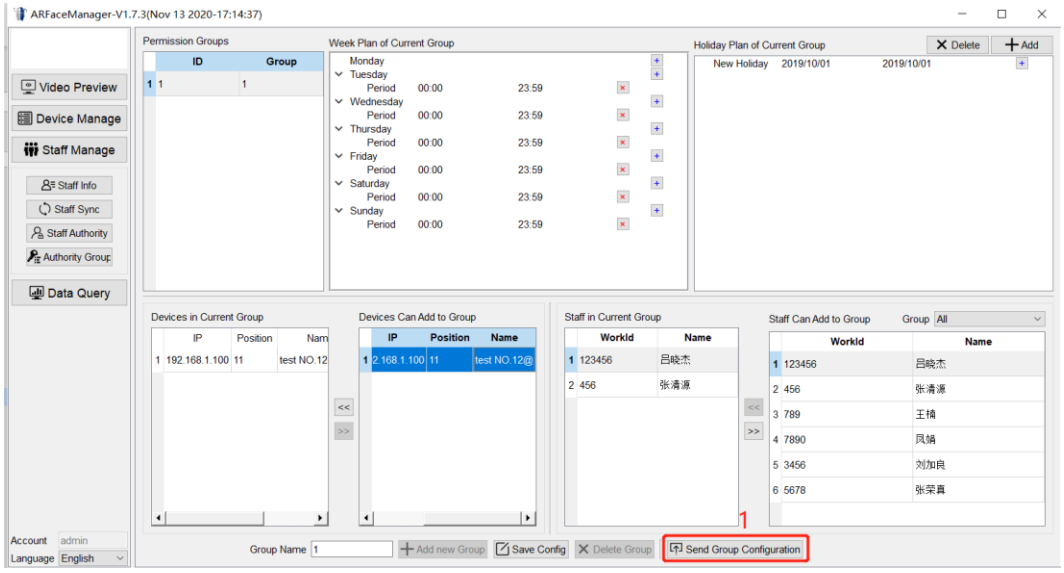
7. Associate the device. Select the device to be associated in the "Device Can Add to Group ", click "《" button, and add it to the " Staff in Current Group " list;



8. Click "Save Config", and the permission group configuration is saved to the local database of the client software.

2.3.11 Send Permission Configuration

1. Click "Send Group Config" to synchronize the permission group configuration to the device.



3. Data Query

3.1 Update Attendance Records

Click "Attendance Records" → "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. The update progress of the attendance record will be displayed in the lower left corner of the window.

2. Search attendance records for a specified time period by setting start and end time.

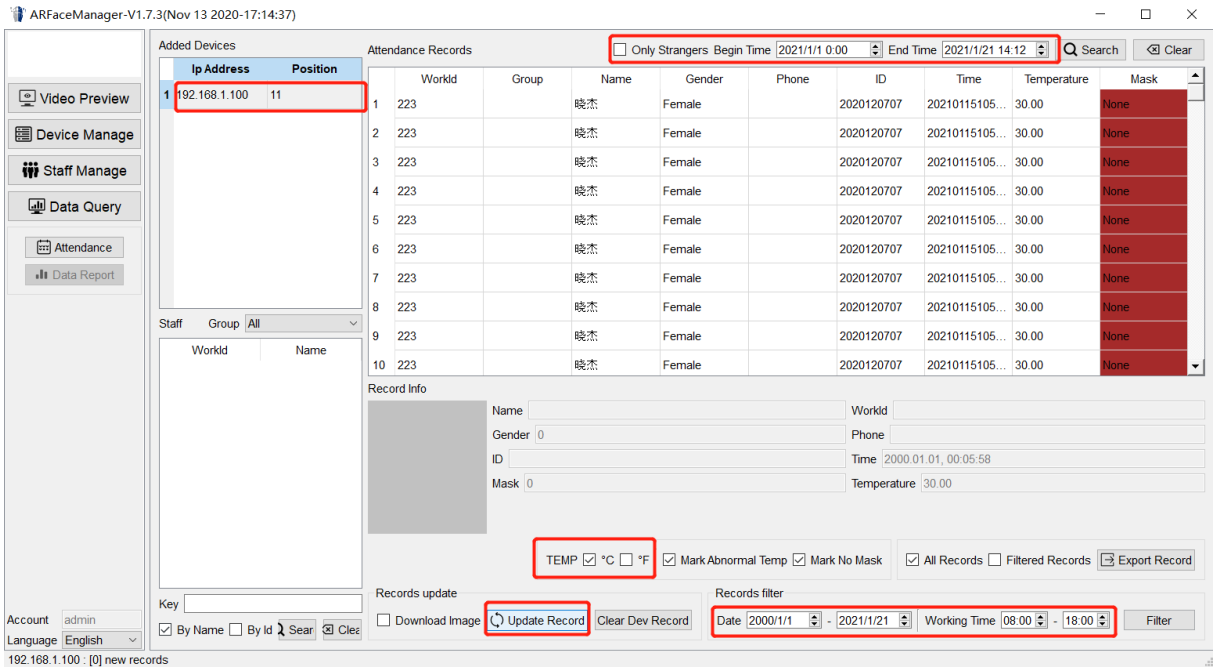
3. By specifying the attendance time period, the records of personnel being late, leaving early, absent from work, etc. can be filtered.

4. The temperature unit shown in the attendance record can be set through the temperature display.

5. Check the "Download Image" button and the snapshot image will be exported to the SNAPSHOT folder in the IP named folder of the device.

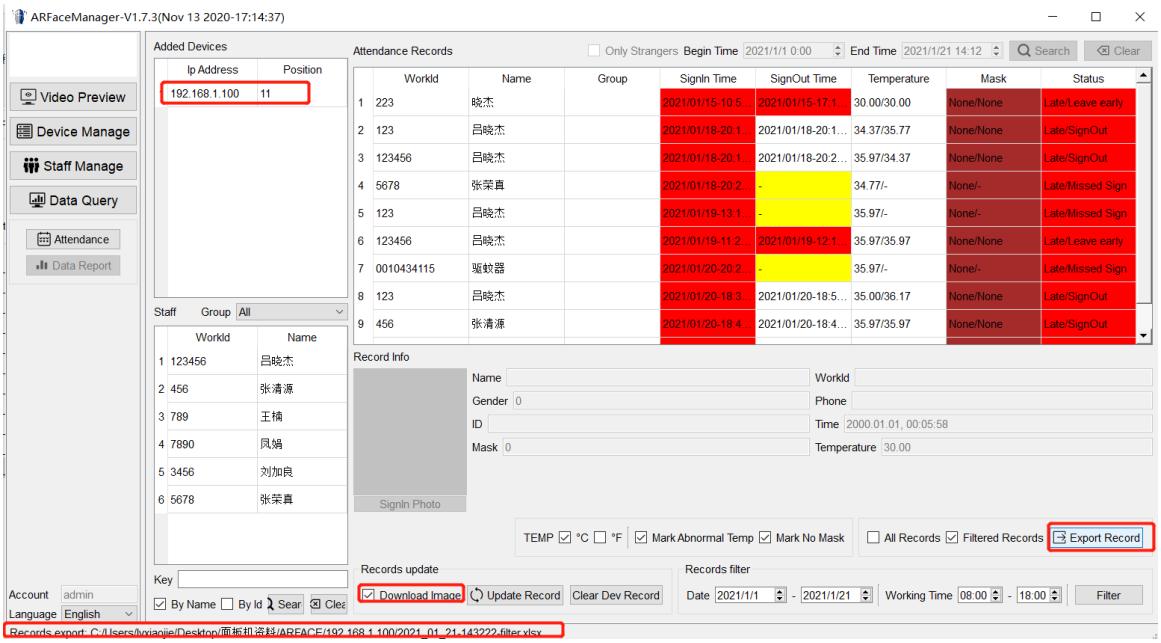
NOTE: If the attendance records cannot be updated, please check whether the settings for saving attendance records are turned on (Algorithm configuration -- General Settings).

NOTE: If you cannot synchronize to the image, make sure that the "Save snapshot Settings in Video Preview - Live Preview "are turned on.

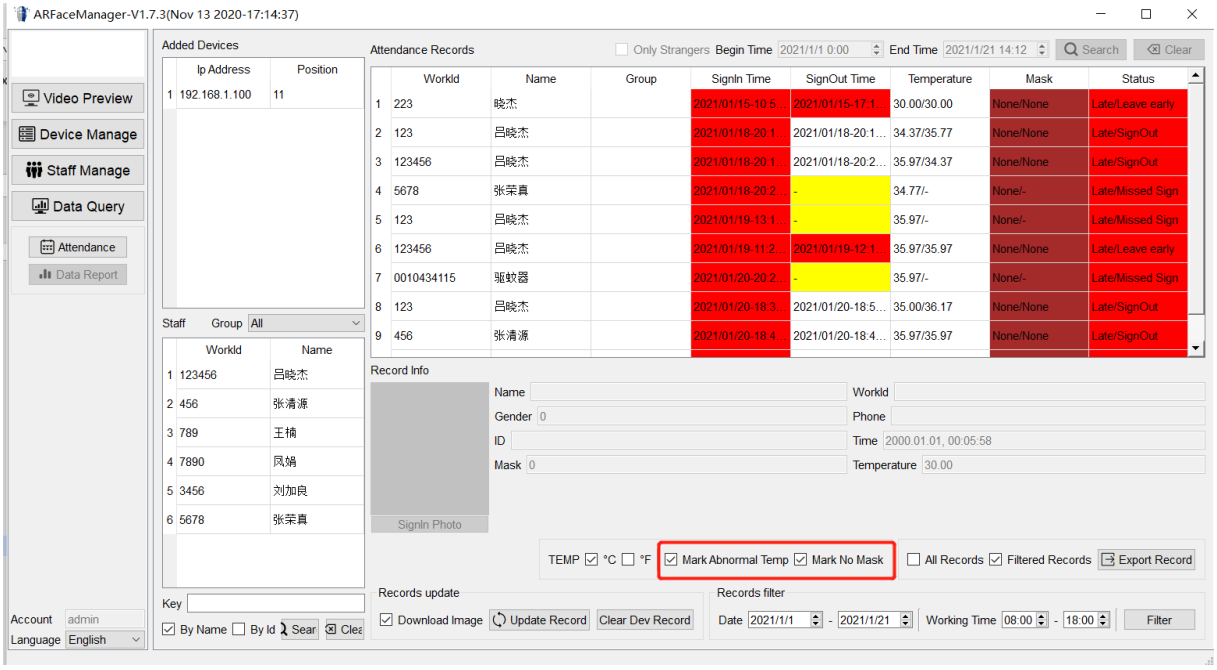


3.2 Export Attendance Records

1. Click "Export Record" and the client will export the data to an excel document, and the status bar will show the saved path of the file. (By default, it is saved in the folder named after the IP of this device in client installation directory).



3.3 Mark Exception Records



1. Mark No Masks and Abnormal Temperature

Check "Mark Abnormal Temperature". When the recorded temperature is higher than 37.3°C, the recorded temperature field will be marked with the background color.

Check "No Mask". When the recorded information is no mask, the recorded mask field will be marked with the background color.

2. Mark Abnormal Attendance Records

In the filter interface, background color marks will be carried out for the corresponding fields of records such as late arrival, early departure and missed attendance.

3.4 Clear Attendance Records

Click "Clear Device Record" to clear all the record of attendance identification saved

in the device.

NOTE: The client can also check the attendance record that was previously kept locally. If you want to delete locally saved attendance records, delete the folder named after the device IP after exiting the client.

NOTE: This device can keep about 30,000 attendance identification records, and the oldest 1000 records will be deleted when the memory is insufficient to store the new records.