DIGITALHOME

Helping you live smartly.

FR07

FACE RECOGNITION DOOR ACCESS CONTROLLER

User's Manual

Smart-pass System v1.5.9

Operation Manual

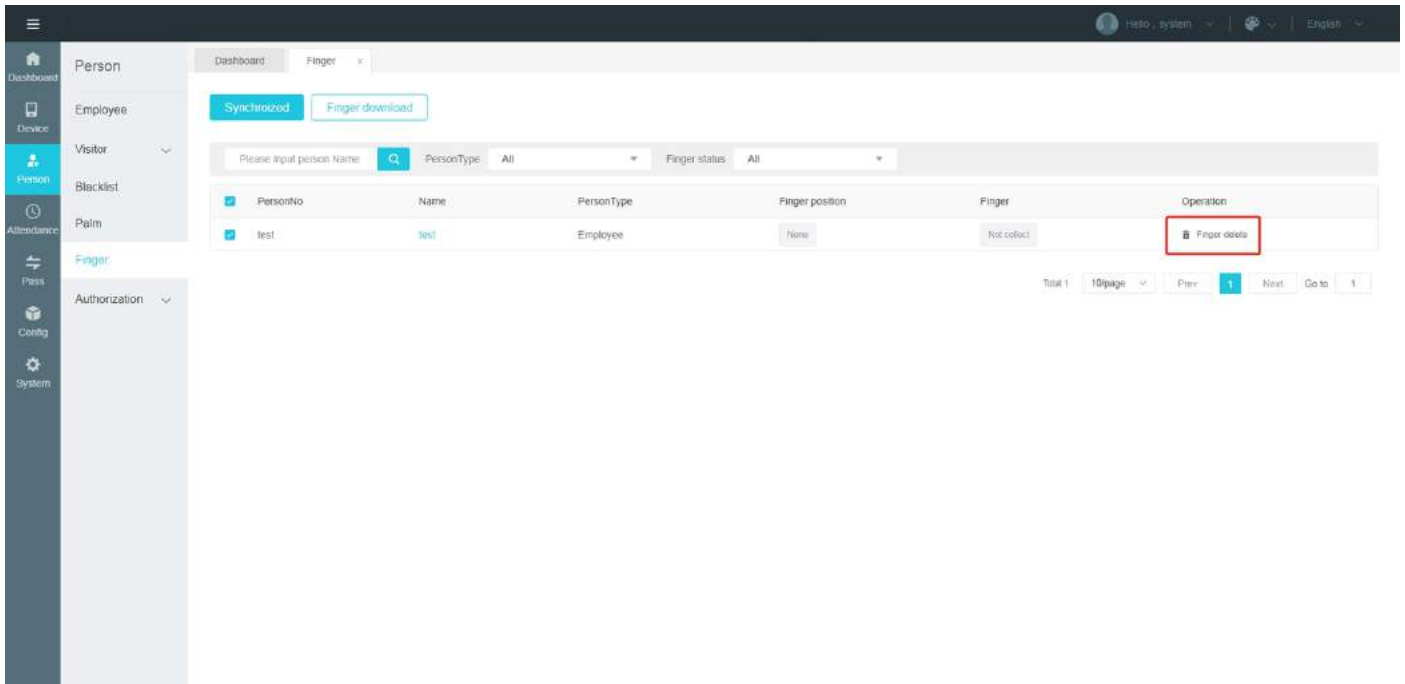**Content**

5.Attendance Management 123

1.System installation and home page display instructions

1.1.Start service access

According to the installation instructions, after installing the software, click copy t

o copy the URL and paste it into the browser to access the system.
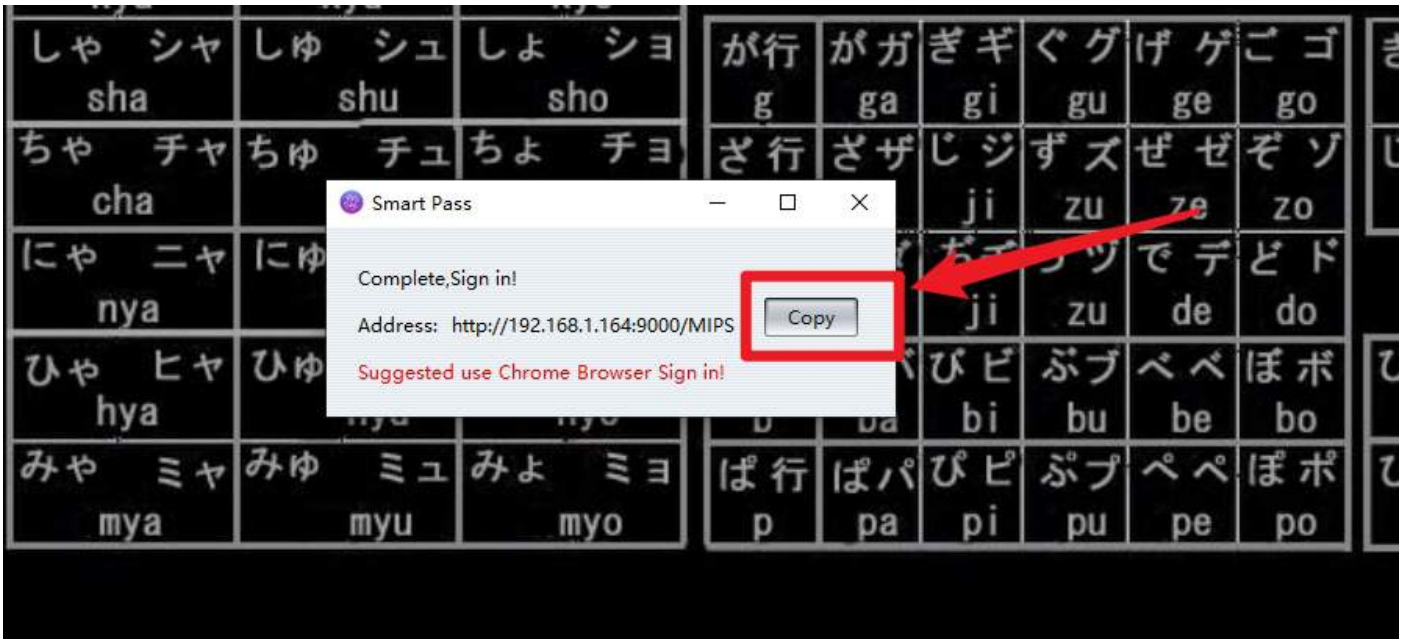
The local deployment access address is: http://localhost:9000/MIPS/

Initial top administrator: Account: system   password： 123456
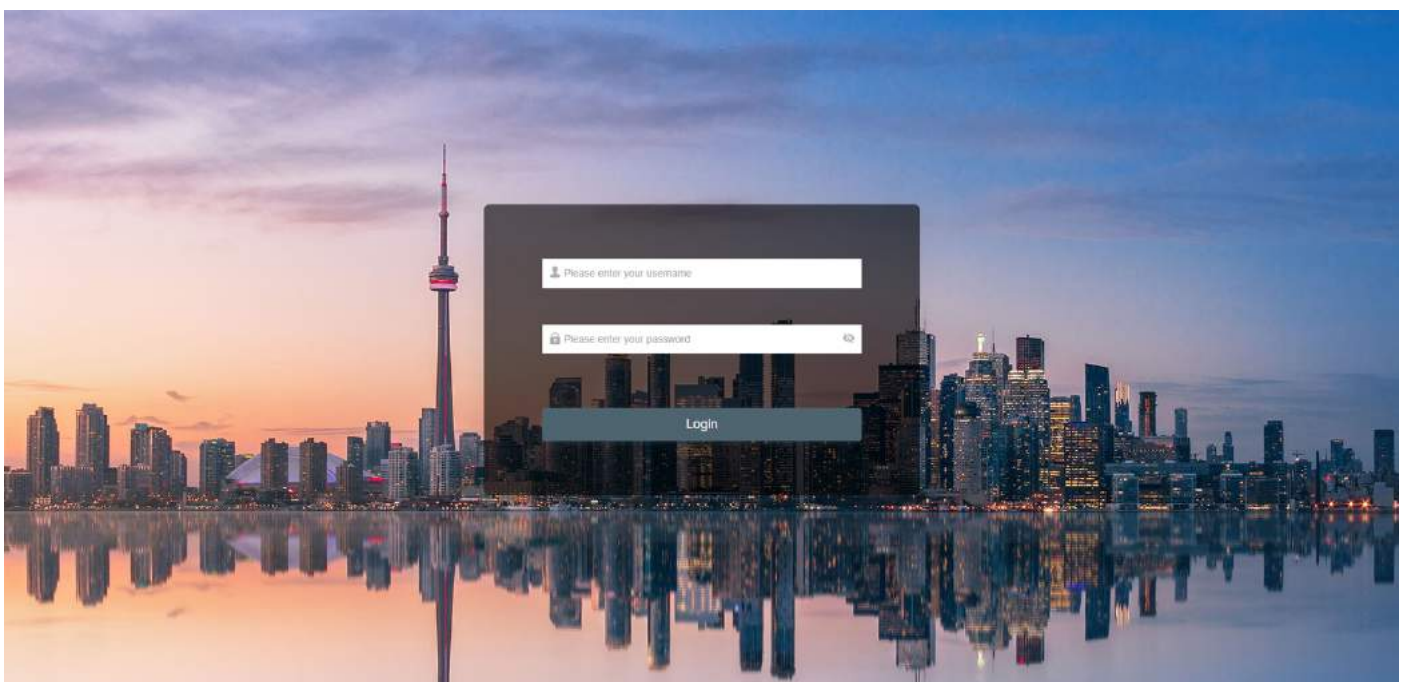
1.2.Background interface

After the super administrator logs in the system correctly, the default working area of the system is mainly composed of the following parts. The interface is mainly divided into three large areas, including the top display area, the left main menu navigation area, and the right main operation area. As shown below:
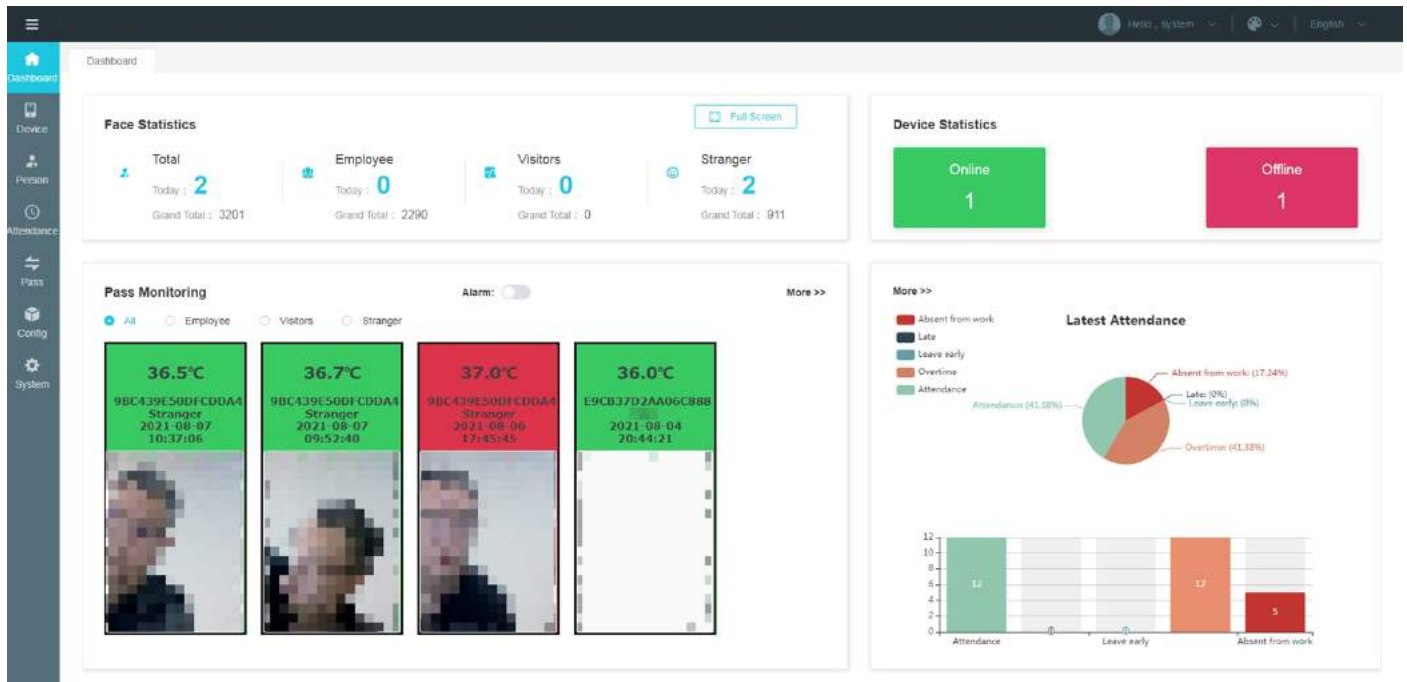
① **Main function menu area: including workbench, equipment management, personnel management, attendance management, traffic management, configuration, system**

② **Sub-function menu area: namely the sub-menu of each main function menu**

1.3.Workbench

1 ） Statistics on the number of face brushes: the number of face brushes by employees, visitors, and strangers on the day and their respective cumulative face brushes, the sum of the number of face brushes on the day and the sum of the cumulat

ive number of face brushes.

2） Equipment statistics: the number of online devices and the number of offline devic

es。

3） Real-time monitoring: The real-time monitoring module automatically refreshes

after about 5s after there is new face data,

4） Last time attendance: display the pie chart of the previous time attendance distribu

tion of all personnel, click to view more to jump to the attendance record interf

ace.
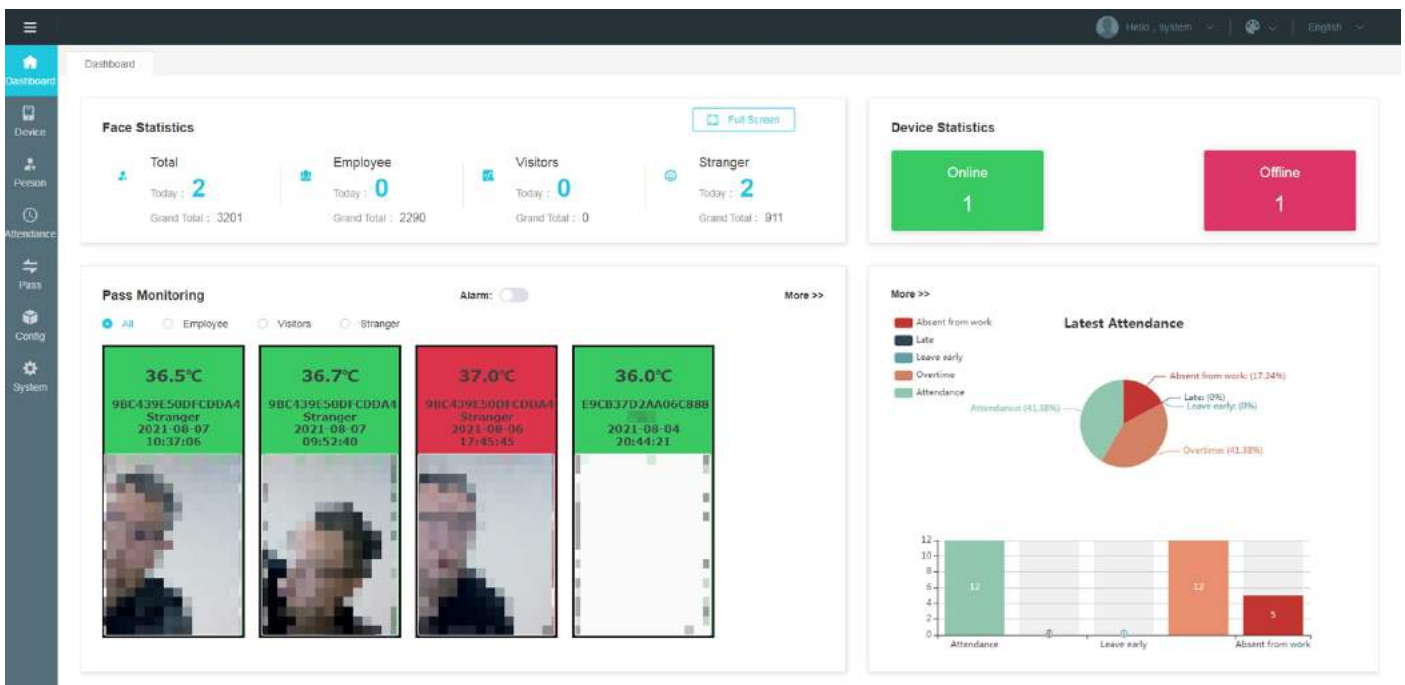
Real-time monitoring: The real-time monitoring module automatically refreshes af

ter about 5s after there is new face data, there is an alarm switch, when the real-tim

e monitoring of high-temperature people passing, the computer will sound an alarm

Pass Monitoring

Alarm: ⬜

◉ All ⚪ Employee ⚪ Visitors ⚪ Stranger
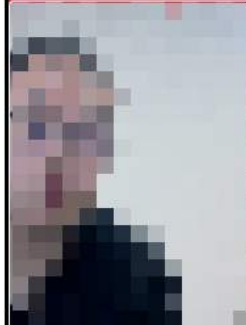
36.5℃	36.7℃	37.0℃	36.0℃
9BC439E50DFCDDA4	9BC439E50DFCDDA4	9BC439E50DFCDDA4	E9CB37D2AA06C888
Stranger	Stranger	Stranger	钟炬
2021-08-07	2021-08-07	2021-08-06	2021-08-04
10:37:06	09:52:40	17:45:45	20:44:21

2.System display and initialization

2.1.System Display

2.1.1.System display language switch

The default language of the system is Chinese (Simplified), click on the far right s

ide of the top navigation bar to switch the language. Currently, four languages includ

ing **Chinese Simplified, Chinese Traditional, English, Spanish and German** are supp

orted.
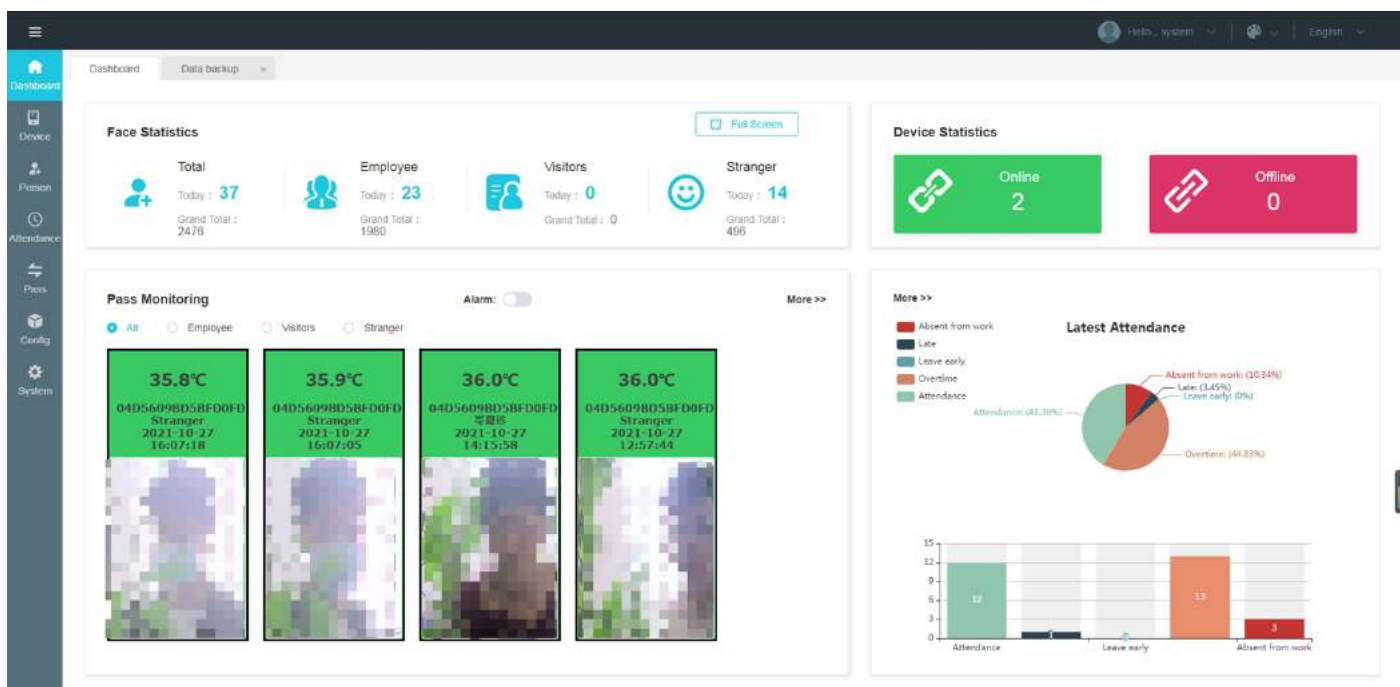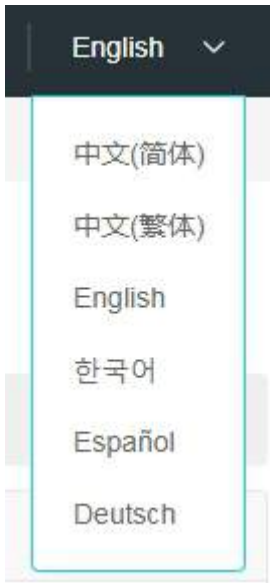
2.1.2 System display theme switch

The default theme color of the system is gray-blue version. Click the theme color button on the right side of the top navigation bar to switch the system theme color.
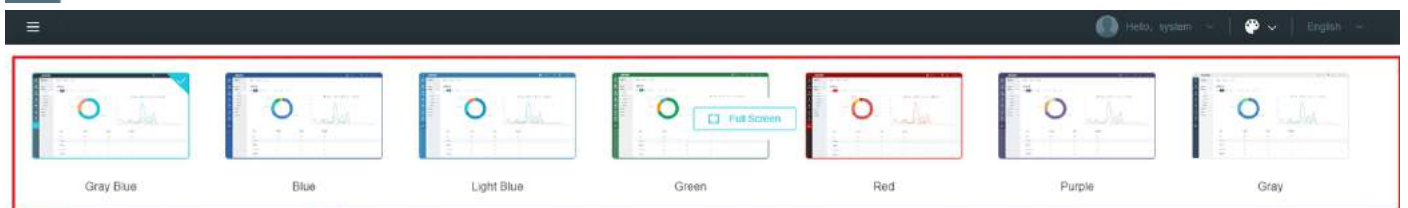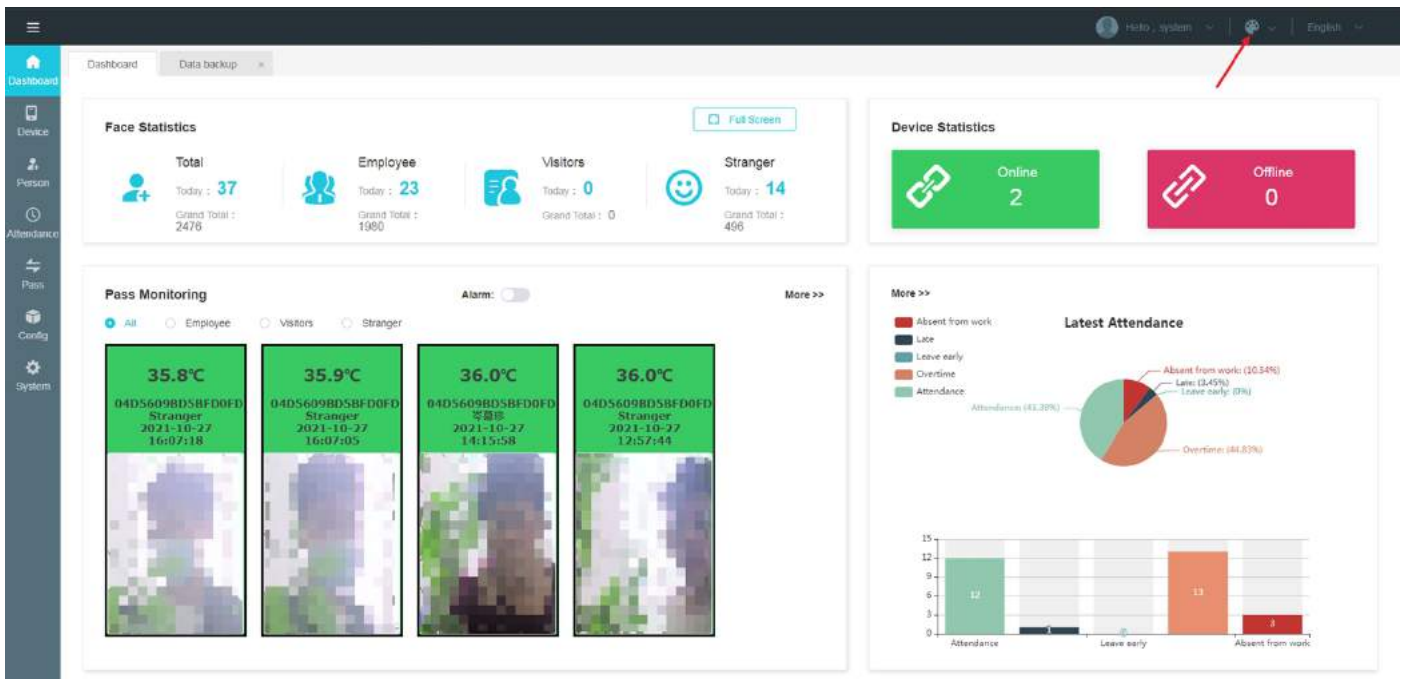
2.2 Initial site configuration

Site settings

➢ ⬚ Click [Configuration] [Site Management] in the system to enter the site management interface.
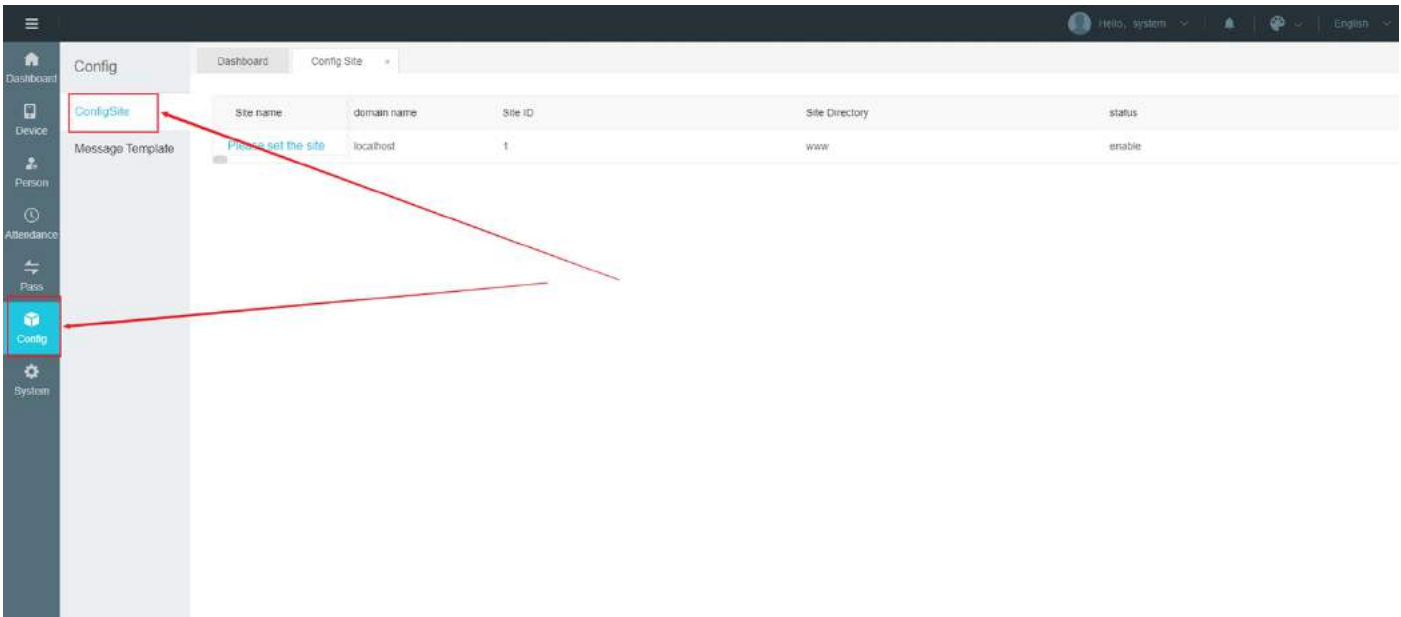
➢ ⬚ Click on the site name column to change the site information

➢ ⬚On this page, you can change the basic information of the site, such as site name , site directory, etc.

➢ ⯀ Click [Extended Configuration], you can modify other configurations of the site, such

as pass configuration, watermark configuration, file upload configuration, etc.

The file upload configuration is as follows:

| File upload configuration

Image file types allowed to upload: [jpg ⊗ + 3] ▼

* Single picture file size limit: [0] MB ▼

"0" means no limit, the default is 0

Document types allowed to upload: [doc ⊗ + 4] ▼

* Single document size limit: [0] MB ▼

"0" means no limit, the default is 0

* Types of attachments allowed: [Set allowed type] ▼

[zip]

* Single attachment size limit: [0] MB ▼

"0" means no limit, the default is 0

* Upload file storage server: ◉ Local server

[Save]

3.Equipment management

Device management is mainly for device management. The specific location directory is shown in the figure below:
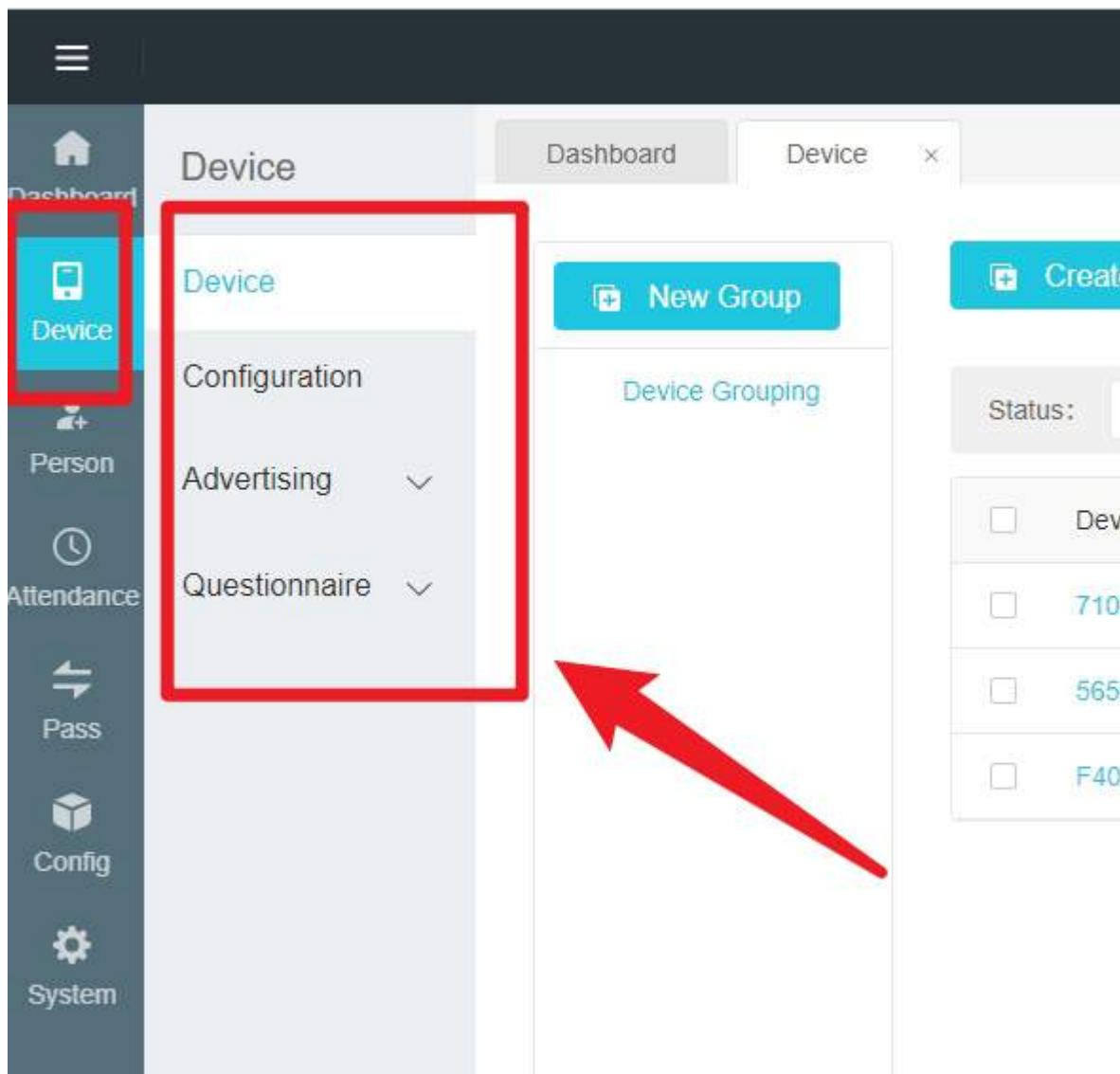
3.1.Device connection System

Note: When the device logs in to the background, do not stop the background software for a long time. When the equipment continues too much records, it will cause the system to crash.

3.1.1.Confirm version

Before the device logs in and connects to the background, please confirm whethe r the download is the LAN version or the cloud version. The LAN version installation package name is smart_pass_setup_v1.**_LAN.exe, and the cloud version name is smar t_pass_setup_v1.**_WAN.exe. For the local area network version, please read the steps of [3.1.2 LAN-device connection background], and for the cloud, please read [3.1.3 clo ud-device connection background] steps.

3.1.2.LAN-device connection System

The LAN version in the local area network system does not provide the entrance of the newly-built device. When the device and the server (computer) are in the sam e LAN, the device list page will automatically appear on the device list page after log ging in to the LAN on the device.

➢ **Step 1** : **Device login to LAN**

Click the settings icon in the upper right corner of the device, enter the passwor d to enter the settings center
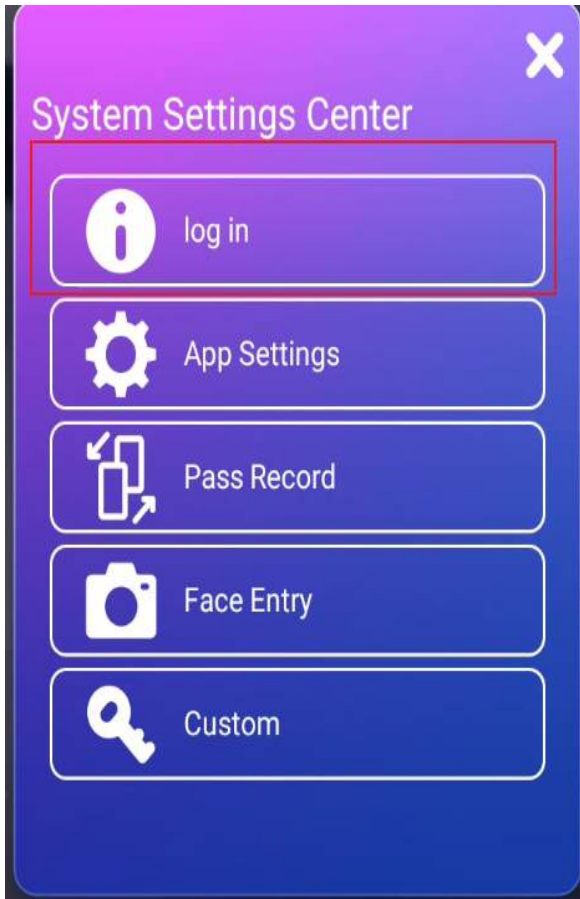
⚙ Login Settings

Password Settings   >

Login LAN   >

Enter the computer ip address (the computer and the device must be in the same LAN)

Login LAN

Enter server ip

Sign in

Network testing

Cancel

➢ ⬚ **Step 2: Device list display**

After the device successfully logs in to the system, the system device list will sho

w the device just logged in and its status is online. If it does not appear, please click

the right mouse button on the device management tab to refresh it manually. If it d

oes not appear, confirm on the device whether the server IP is entered correctly and

whether it shows login success.
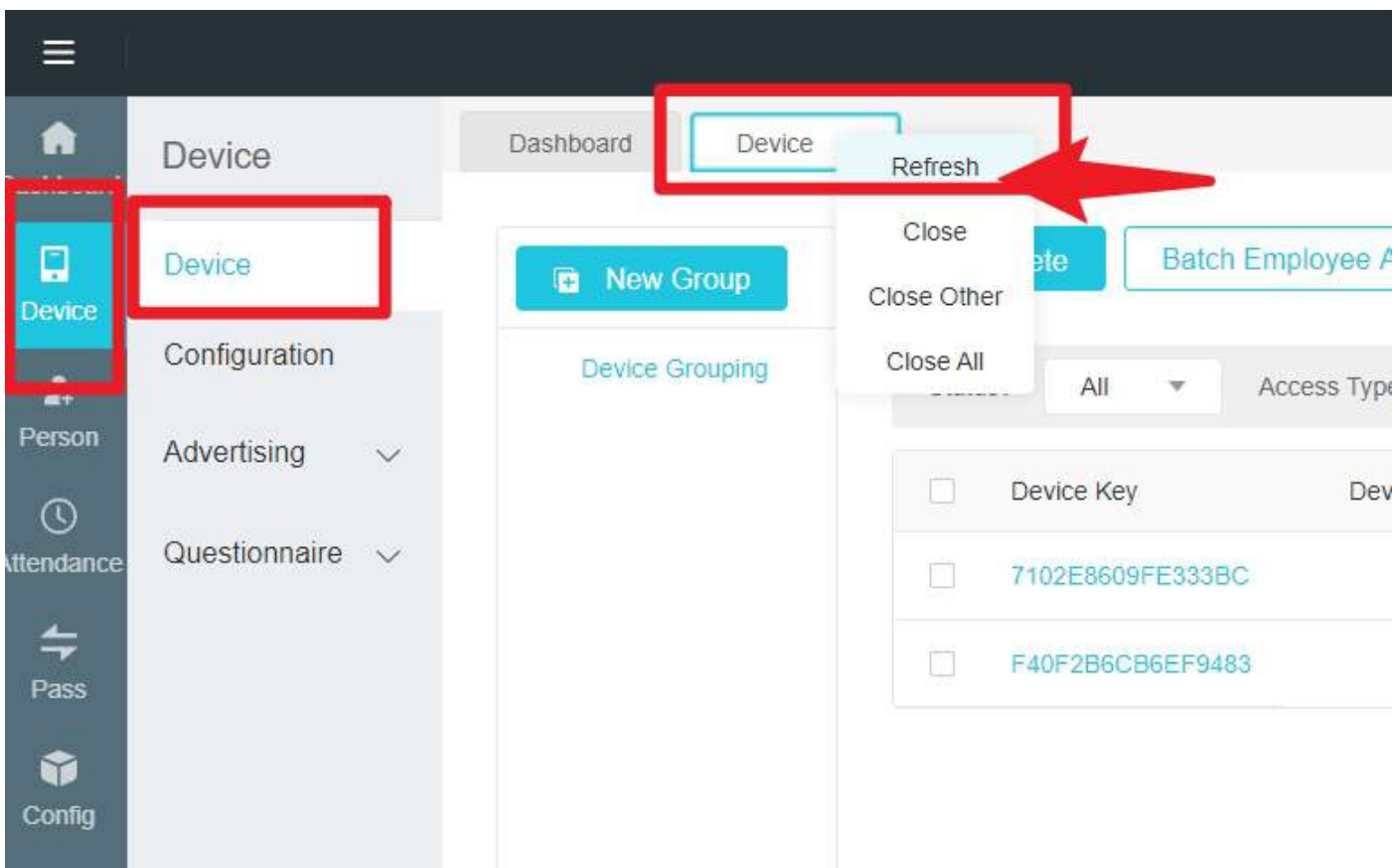
➢ ⬚ **Step 3: Set the initial LAN communication password**

After the device is logged in, if it is the first time to log in, you need to confirm the

initial password of the device, click the device serial number (blue font) on the list display

page, select the network configuration, and modify or confirm the initial password of the

device in the network configuration:

Note: The new and old passwords need to be the same when setting for

the first time, that is, the default old password is 12345678. Enter the new

password 12345678 and click Save. If successful, the initial password is complete.
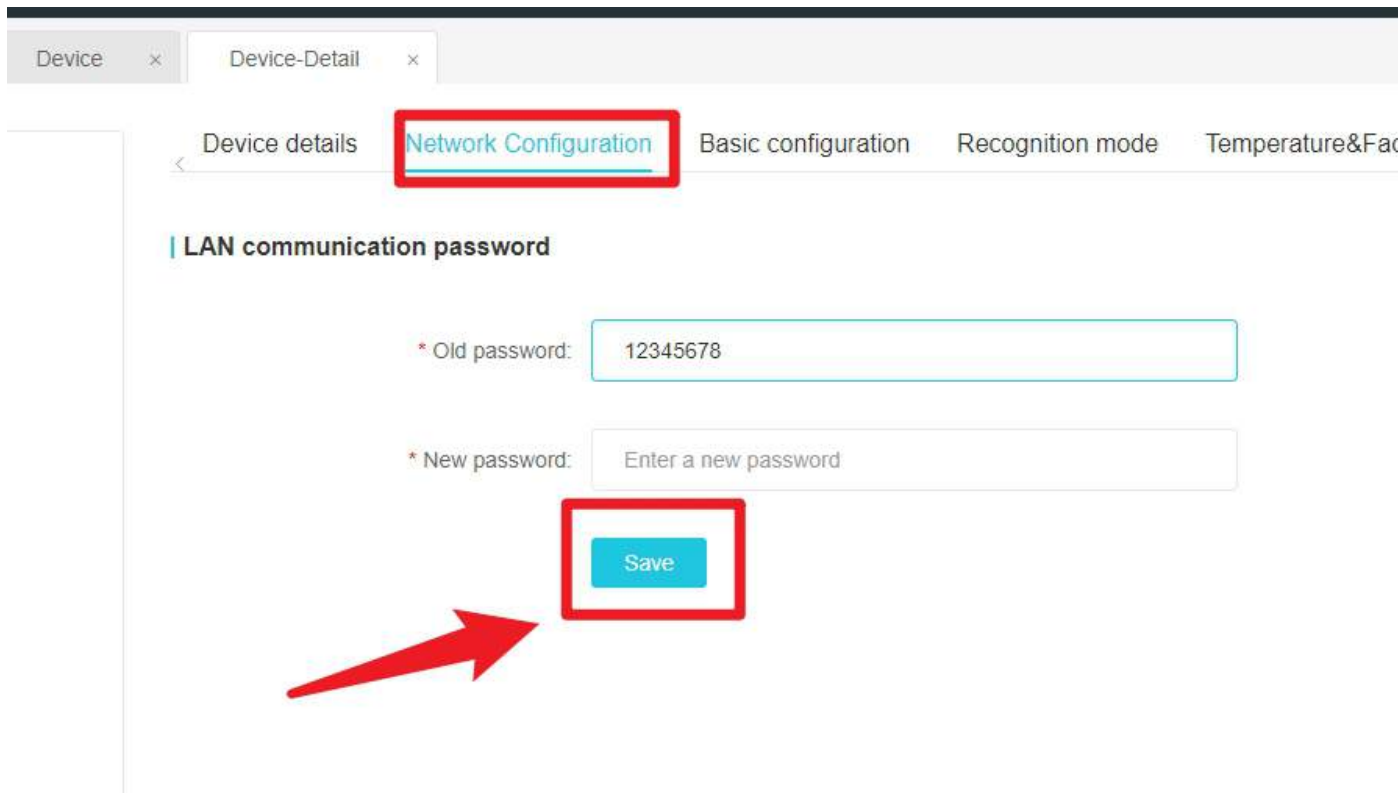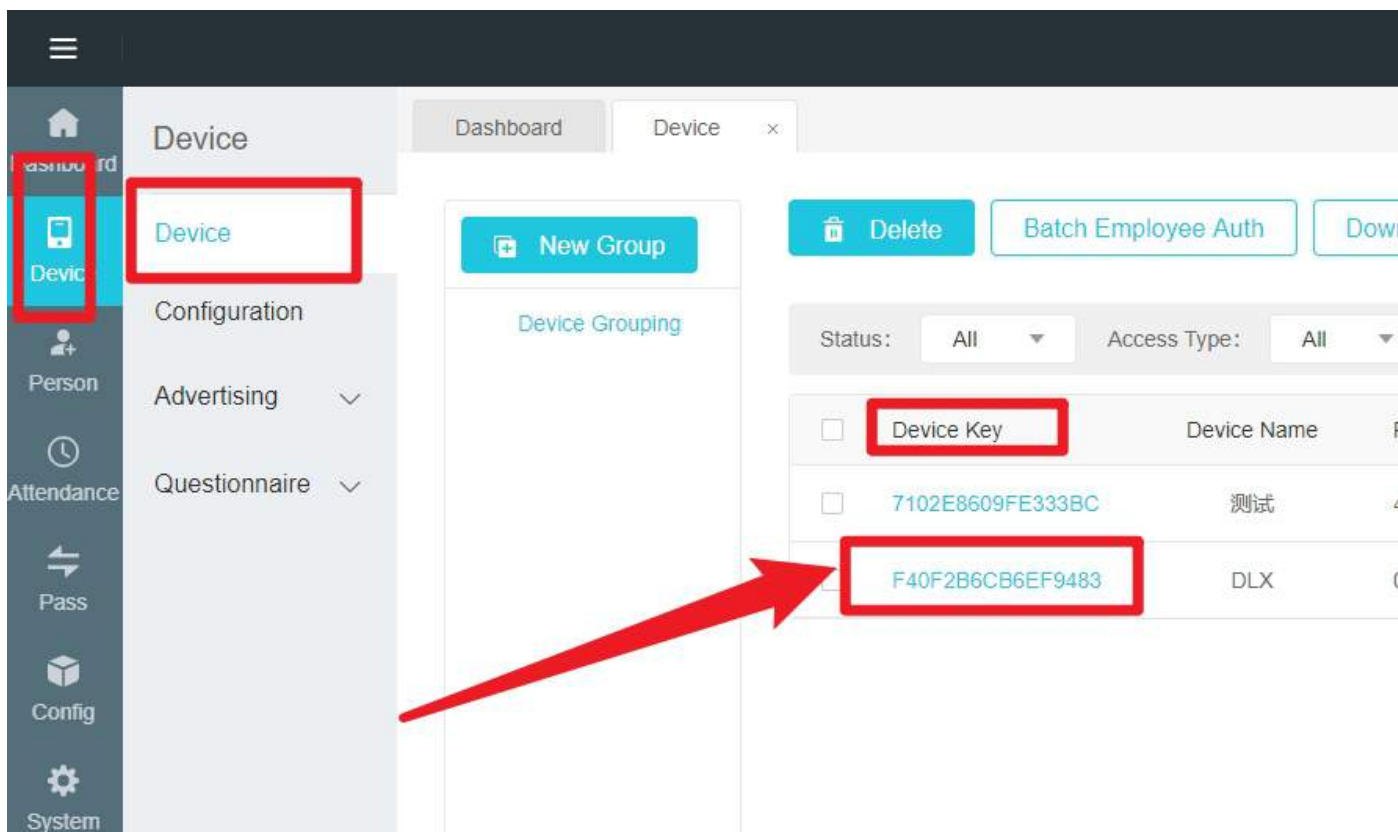
> **Step 4：Confirm that the system can operate the equipment**

After setting the initial LAN communication password, return to the list display pa

ge (device management), select [Other Operations] in the device operation bar, and cl
ick [Remote Door Open] to confirm whether the device is really connected to the sys
tem. If it shows that the door is opened successfully, it means that the device is succ
essfully connected to the system!
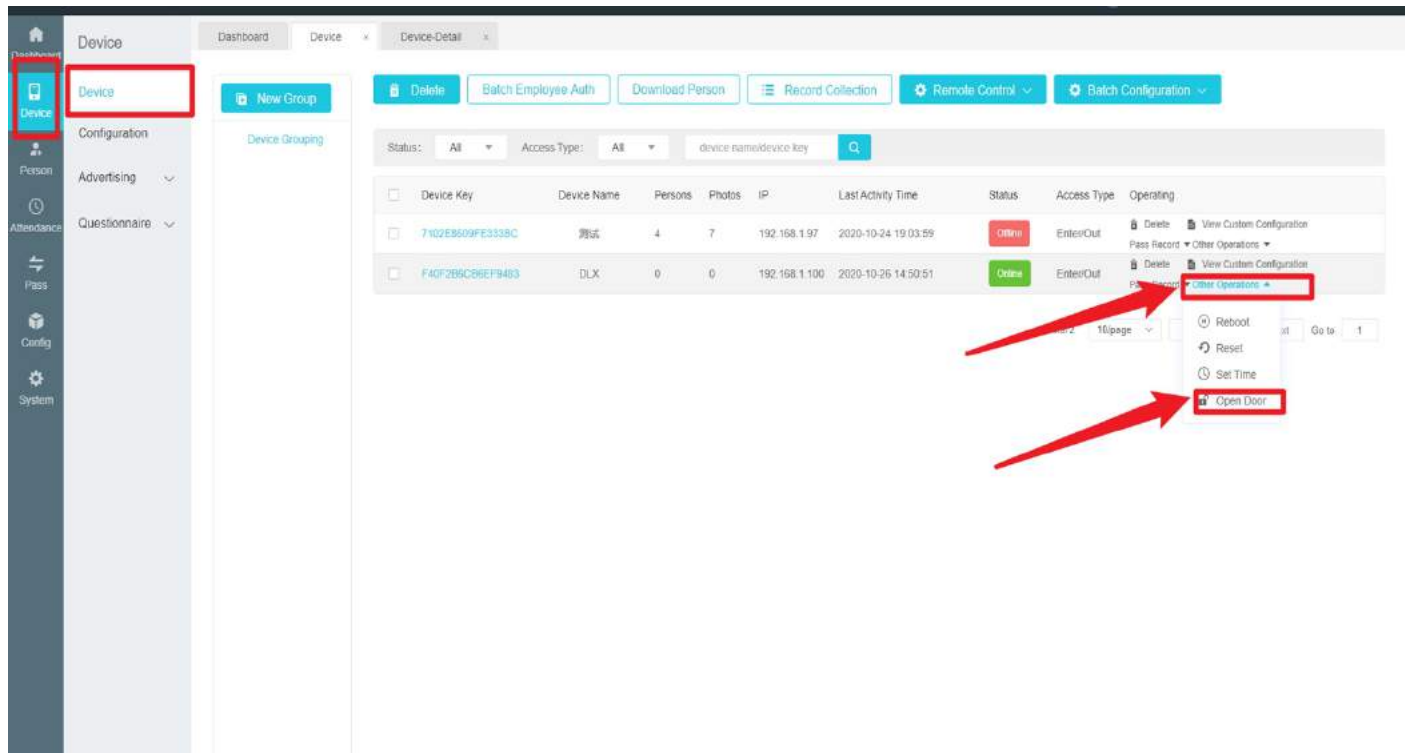
3.1.3.WAN-device connection System

 Step 1: Log the device into the WAN

⚙ Login Settings

Password Settings　　　　　　　　　　　　　>

Login LAN　　　　　　　　　　　　　　　　>

Login Cloud　　　　　　　　　　　　　　　>

Note: The secret key here is the cloud communication password, which must be

the same as the cloud communication password when creating a new device in step

> ➢ ☐ **Step 2: New Device**
>
> **Note: To use the cloud version, you need to open the two ports 10011 an
> d 10010 on the server.**

After the device is logged in to the cloud, click the [New] button on the system l
ist to jump to the new device page, as shown in the figure below. Fill in the basic in
formation of the device in the new page, where [Cloud Communication Password] ne
eds to be consistent with the cloud communication password entered when the devic
e logs in to the cloud. Click [Connection Test], if the information is filled in correctly,
the connection is displayed successfully, click [Save] to skip to the next step.

Set the callback information, set the correct identification callback server IP address
and port or domain name, and then the real-time record of face recognition can be
normally displayed in the real-time monitoring interface of the workbench. The server IP is

the system software computer IP, and the default port is 9000. For example, you can enter

here: [Server IP: 9000]

Device IP, device serial number, device name, and access type are required it

ems. Input errors will affect the interaction between the system and the device.

> ⬥ **Step 3: Confirm that the system can operate the equipment**

After creating a new one, return to the list display page (device management), in

the device operation bar, select [Other operations], and click [Remote door open] to

confirm whether the device is really connected to the system. If it shows that the do

or is opened successfully, it means that the device is successfully connected to the sy

stem!
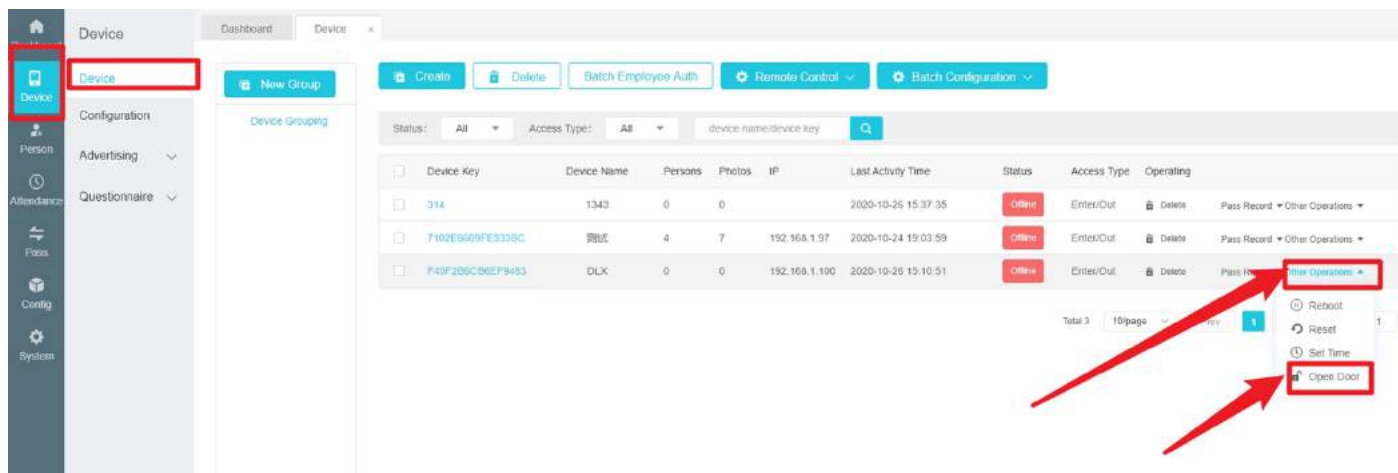
3.2.Device Management

After entering the device list, first we can see the device group on the left, which mainly classifies devices.

Switch list: The device list is displayed in the form of a list by default. Click "Gro up" on the left to switch the grouped device display.

3.2.1.Device List

Device List : The device list displays the collection of devices under all groups in the current system.
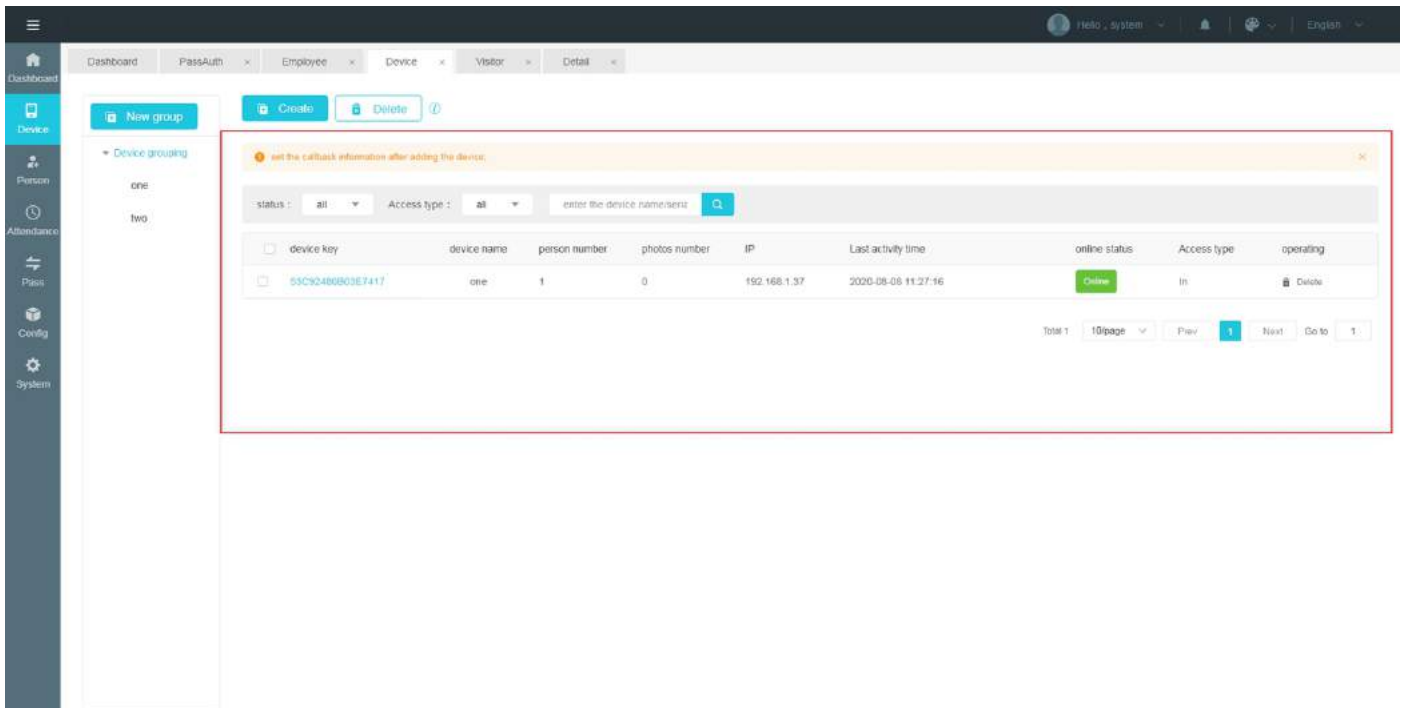
The device list includes device serial number, device name, device IP, device online status, access type and other information. Click the [Delete] button in the operation column to delete the device.

3.2.2.Download staff

After selecting the online device, click the [Download Staff] button to download the staff information on the device to the background system
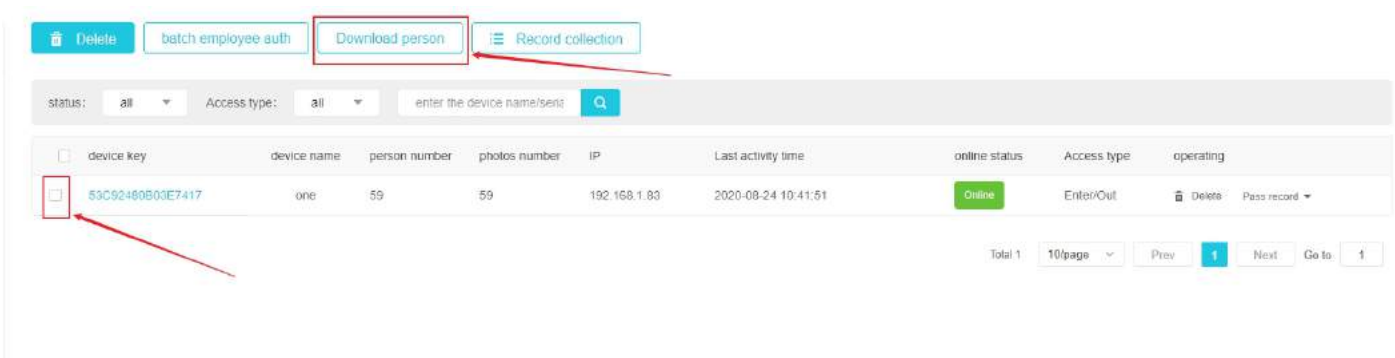
After clicking, it will show that the operation is successful. After waiting for 1~3 minutes, you can refresh and see the personnel information downloaded from the device in [Staff]-[Staff Management].

3.2.3.Record collection

Batch collection: After selecting an online device, click the [Record Collection] butt on to collect all the traffic records on the selected device to the system.

Single collection: place the mouse on the [Pass Record] in the operation bar of e ach device information, you can see the collection and view, and click Collect to colle ct all the pass records on the device into the system.
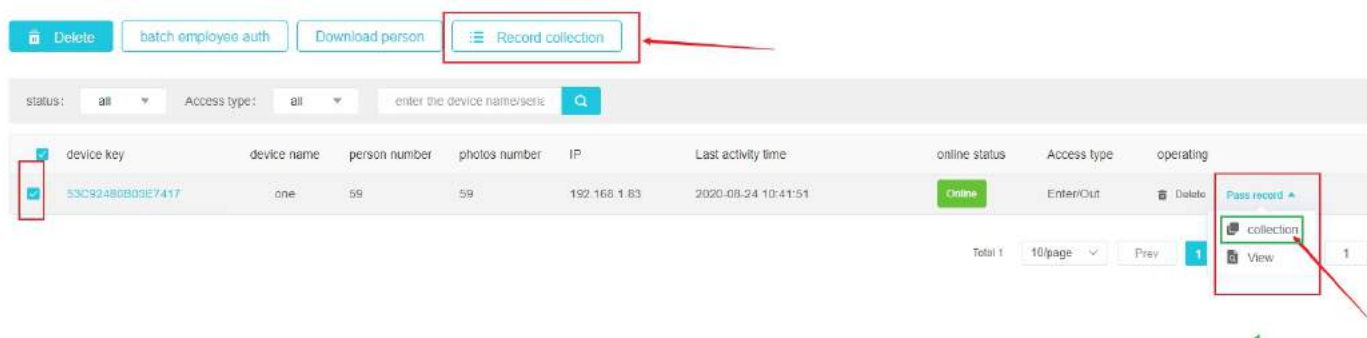
Click [View] to jump to [Pass] [Pass Record] to view the device's pass record.

3.2.4 . Clear the pass record
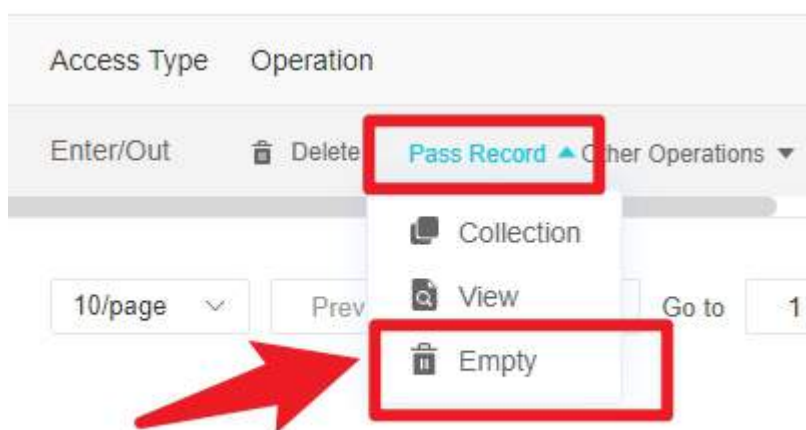
Clear the pass record: Place the mouse on the [Pass record] in the operation bar of each device information, and click [Empty]
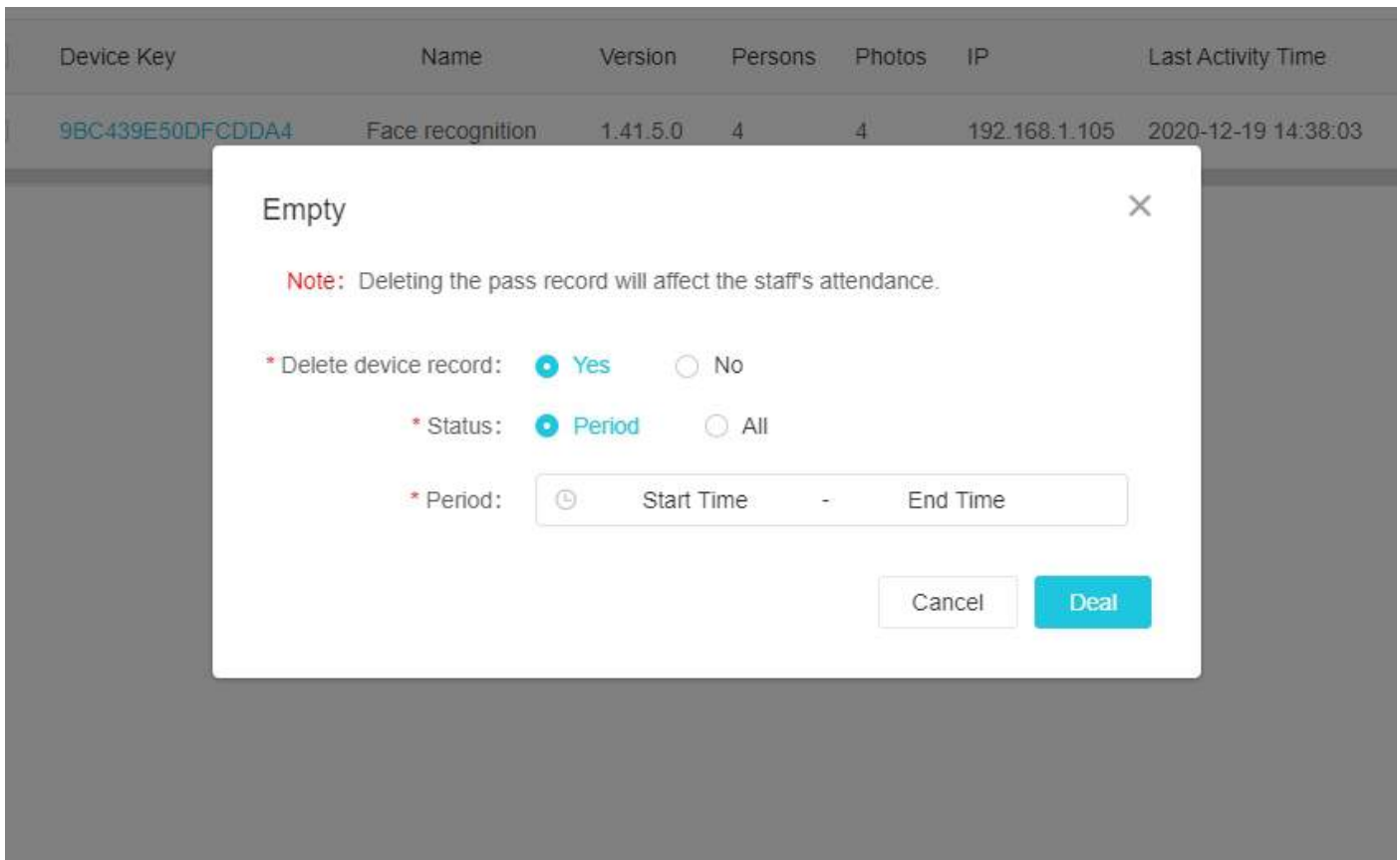
- ➢ **Delete device records:** the default selection is "Yes", after clicking on the process, the pass records in the system will be deleted as well as the pass records on the device.

- ➢ **Status:** You can choose to delete the pass records for a certain time period, you can choose to delete all, and if you choose to delete by time period, you need to select the corresponding time period in the time period.

3.2.5.Employee batch authorization

With this function, employees can choose to authorize or deauthorize devices in batches. The specific steps are as follows:

1、 After selecting the device, click the [Employee Batch Authorization] button,

2、 Click and select [Authorize] or [Remove Authorization]
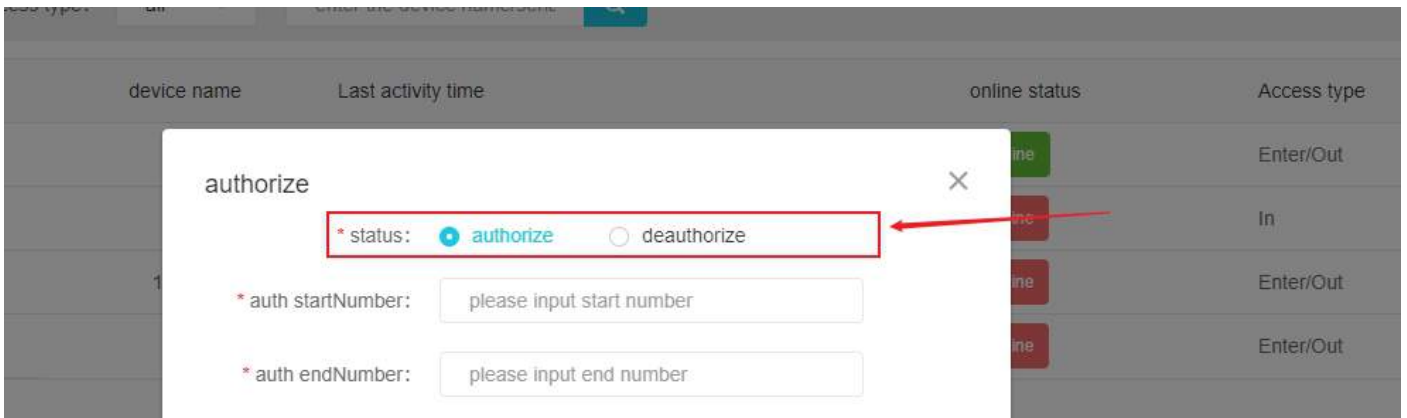
Enter the start number and end number of the employee authorization, as well as the time period allowed on the day, and then the employees in the number range can be authorized to the selected device. Employees can pass through within the allowed time period of the day, otherwise, it will prompt that the authority is insufficient.

3.2.6.View custom configuration

In the device list, in the last operation column of each device list, click [View Cus tom Configuration] to view the custom configuration that has been set for the device .
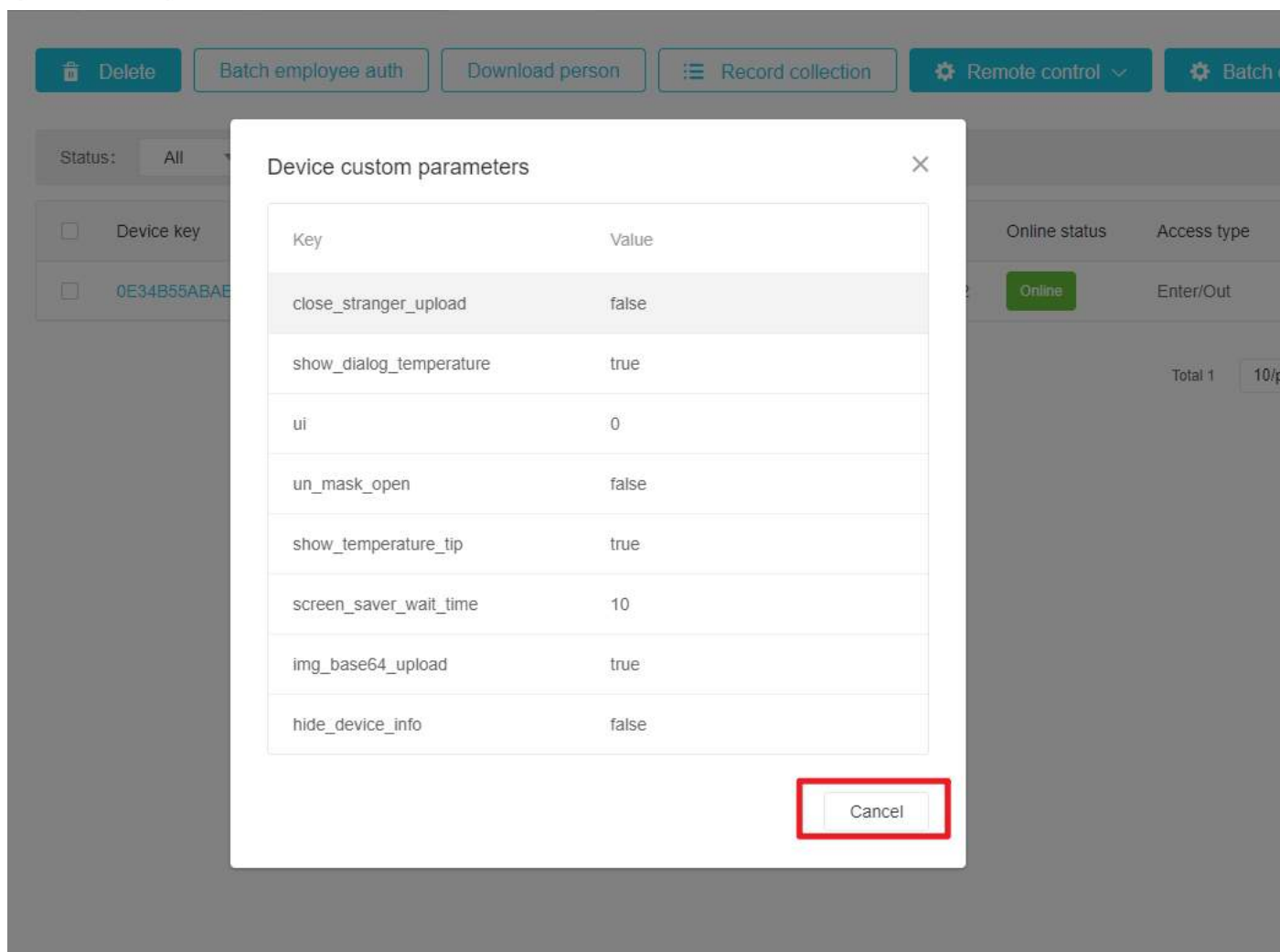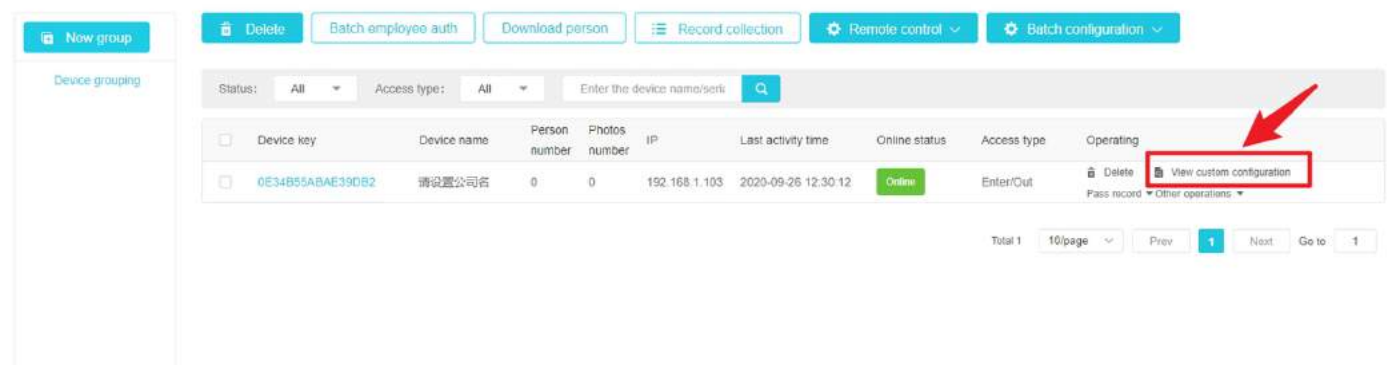
3.2.7.Remote control

In the device list page, you can perform remote operations such as restarting, res etting, opening the device, setting the device time, etc.
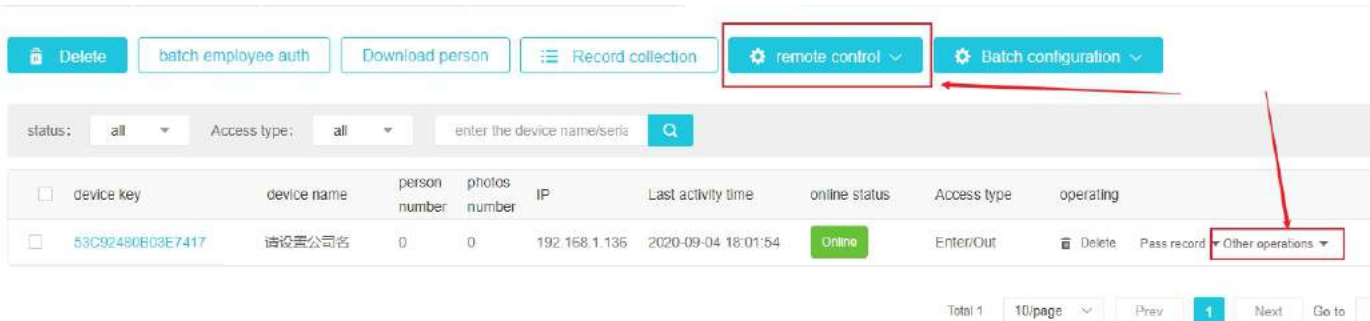
Multiple remote control: After selecting one or more online devices, place the mouse on the [Remote Control] button on the device list page, and the options that can be operated on the device will appear, as shown in the figure below
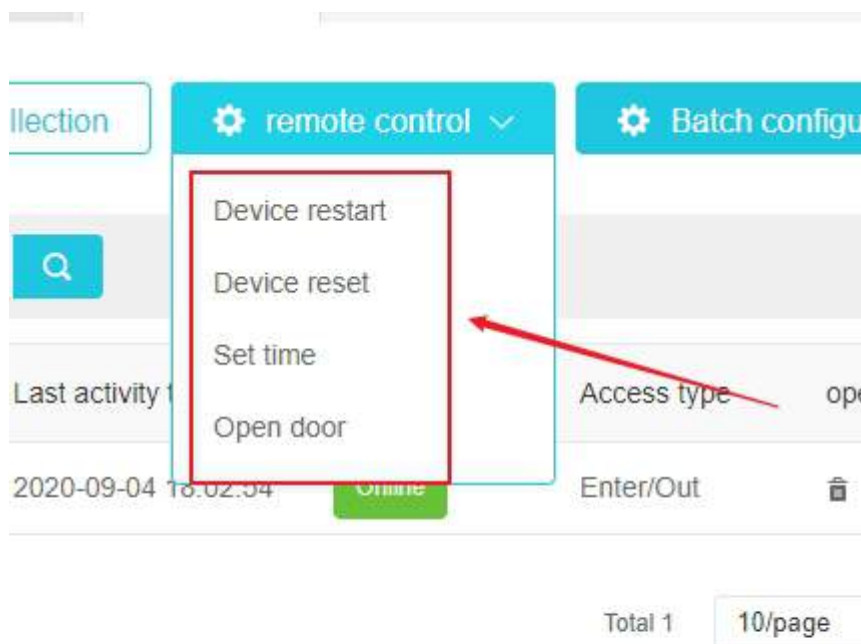
Single remote control: In the operation bar of the device to be operated, place the mouse on [Other Operations], and the options that can be operated on the device will appear, as shown in the figure Below
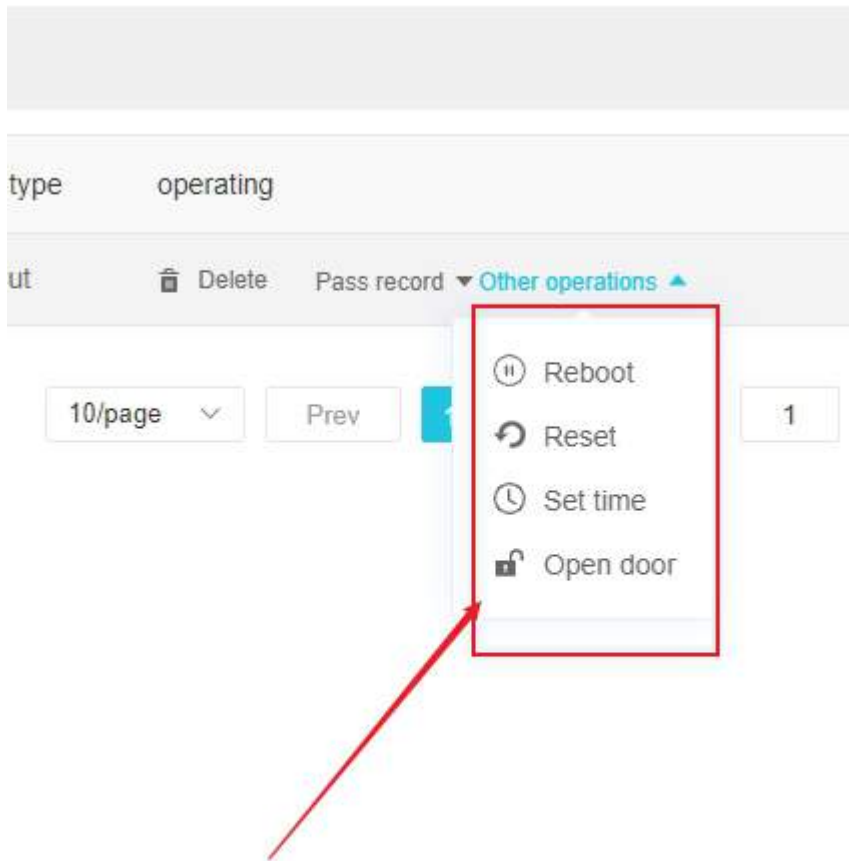
3.3．Cloud equipment management

3.3.1．New equipment in the cloud

The specific operation of cloud system connection equipment and new equipment can be seen in [3.1.3. Cloud-device connection background]

3.3.2．Employee batch authorization

The same as employee batch authorization in LAN equipment management, refer to 3.2.4

3.3.3 ．unit deletion

After the device is removed, the system removes the traffic records and authorization records of the device in the system.

Delete a single device.

Batch delete equipment: After selecting the device, click the [Delete] button above to delete.

3.3.4 . Cloud device setting

See 3.3 for Equipment Settings

3.3.5 . Record collection

See 3.2.3

3.4.Device settings

Click [device key] to enter the device setting interface, the left side of the device setting interface is the device list, you can select the device that needs to be set, and the right is the device setting interface, including device details, network configuration, basic configuration, identification mode, temperature measurement & Mask configuration, callback configuration and device remote control.
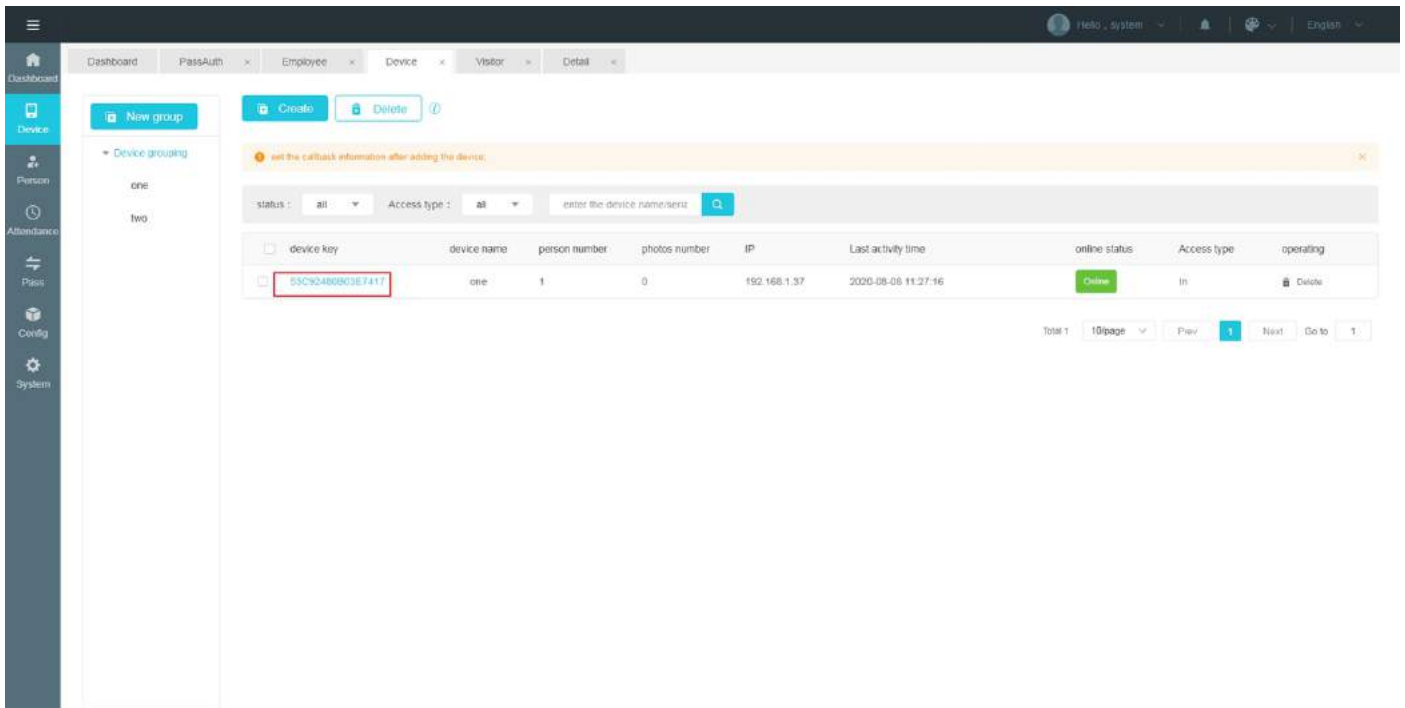
3.4.1.Device details

Device details : Modify the device name, belonging group, device IP, and device access type, upload the device logo, and modify the logo image in the lower left corner of the face machine.

3.4.2.Network Configuration

Network Configuration : The device's LAN communication password can be modified . The old password must be the same as the current password of the device. The def ault password of the device is 12345678.Note: If you change the password on the de vice, you need to configure the LAN communication password in the network configu ration, which must be the same as that saved on the device, otherwise communicatio n will not be possible.

| Device details | Network Configuration | basic configuration | Recognition mode | Temperature&Face mask | Callback configuration | remote |

| LAN communication password

The old password must be the same as the device password

* old password: enter the old password

* new password: enter a new password

Save

3.4.3.Basic configuration

Basic parameter setting : Set face recognition threshold, recognition distance, etc ;

Parameter Description

(1)　Device name: set the [device name] on the device

（2） Recognition distance

● The device detects and recognizes faces within the recognition distance, and faces beyond the recognition distance will not be detected.

● The default is 1, no distance limit, as long as the device detects a face (that is, a face frame appears), it will recognize it.

● The recognition distance is not through distance sensing, but the size of the dete

cted face frame is calculated by a function, so the recognition distance is not acc urate.

● Recognition distance 0: unlimited. Unlimited here means that as long as the face size meets the detection requirements, the face will be recognized.

（3） Recognition score

* Recognition score: — 65 +

● The process of the device's face recognition result is actually to compare the capt ured face with the registered photo of the person in the library. If the compariso n score reaches the score threshold, the face identity is determined.

● The recognition score threshold is 65 by default, and an integer value of 60-100 i s required. The higher the score, the higher the recognition accuracy, but the reco gnition speed will be slower.

● The device compares the same face multiple times. If the score threshold is not r eached in the first few times, the device will not give a recognition result, so the recognition time will be longer and the device response will be slow

● If the score threshold is set to reach 85 points or more, there is a high probabilit y that the comparison between the captured face and the registered photo will n ot reach the score threshold, and the device cannot give a recognition result, that is, "not recognized".

（4） Recognition interval (seconds)

* Recognition interval: — 3 +

- Time interval of repeated recognition of the same face by the device.

- Default 3 seconds, maximum 60 seconds.

（5） Identify recording mode

* Identify recording mode:	Resume	▼

- 1. Resuming 2. No resuming Default: Resuming

（6） Door open delay

* Door open delay:	—	1000	+

- After the recognition is successful, the duration of the relay output switch signal, silent 1000ms. When connected to the access control, the performance is: the time interval from opening to closing after successful identification. The incoming value requirement is 500-25500, the unit is ms.

- According to the use scene, select the time interval between opening and closing the door.

（7） Multi-face recognition

* Multi-face detection:	Detect the largest face	▲
	Detect multiple faces	
* Recognition level:	Detect the largest face	

- Device default: detect the largest face.

- Detect multiple faces: detect multiple faces and recognize them, that is, as long as the device detects a face, it will recognize it, and each face will have a recogniti

on result (success or failure).

- Detect the largest face: only detect and recognize the largest face among multiple faces, that is, if there is only the largest face among multiple faces, there will be a recognition result (success or failure), which is suitable for scenes where one person at a time is waiting for the gate.

（8） Recognition level

- Default: Monocular live detection

- Do not open in vivo recognition

- Turn on monocular in vivo recognition

- Turn on binocular living body recognition, the recognition distance is 1.5 meters

（9） Comparison of whitelists in personal identification mode

- Default direct authentication comparison

- Whitelist authentication comparison: Read the ID number and compare the ID numbers of all personnel in the database, if it exists, compare the ID; if it does not exist, it will prompt insufficient authority.

- Direct authentication comparison: After reading the ID card, the person ID comparison process is carried out directly.

   (10) Voice broadcast mode, voice broadcast mode custom content

- After the device successfully recognizes the person, it will not broadcast by default

- Do not broadcast voice

- Broadcast name

- customize

  - To broadcast custom content, only the {name} field is allowed, and the format of the {name} field is fixed. Other content only allows numbers, English and Chinese characters, and no symbols. The length is limited to 255 characters. Such as: {name} welcome.

  - Uncommon characters, capital Chinese characters, languages other than English cannot be broadcast, but simple English words can be broadcast.

- Uncommon characters, capital Chinese characters, languages other than English cannot be broadcast, but simple English words can be broadcast.

   (11) Recognize text mode, recognize text display mode and customize content

- After the device successfully recognizes the person, it defaults to 1

- Display name

- customize

  - Display customized content, only allow {name} field, {name} field format is fixed, other content only allows numbers, Chinese and English and Chinese and English symbols, the length is limited to 255 characters. Such as: {name}, sign in successfully !

- If the personnel has set the time period authority passTime, the personnel will be recognized in the non-allowed time period, and the device will display "name + insufficient authority" after identifying the personnel .

(12) Serial output mode, custom content of serial output mode

- After the equipment is successful, the default: open the door。

- Open the door, if the device is connected to the access control, it will trigger the door to open after successful identification

- No output

- Wiegand signal output personnel ID

- Wiegand signal output ID/IC card number

- customize

(13) Stranger switch

* Stranger recognition: ○ shut down   ● turn on

- The device is turned on by default

- Off: Does not recognize strangers, that is, only registrants are recognized, and strangers (non-registered persons) detected are not recognized

- Open: Identify strangers

- After selecting the "Identify Strangers" option, the stranger voice broadcast mode and stranger judgment configuration items will take effect.

(14) Number of stranger judgments

* Number of stranger judgments: —   1   +

- The number of failures to recognize a face as a stranger by the device, default 1 ;

- Please choose an integer between 3-10 for the incoming value. 1 means fast determination but the lowest accuracy rate. As the value increases, the determination time increases and the accuracy improves.

(15) Stranger voice mode, customized content for stranger voice

* Stranger voice mode: Announce stranger warning   ▼

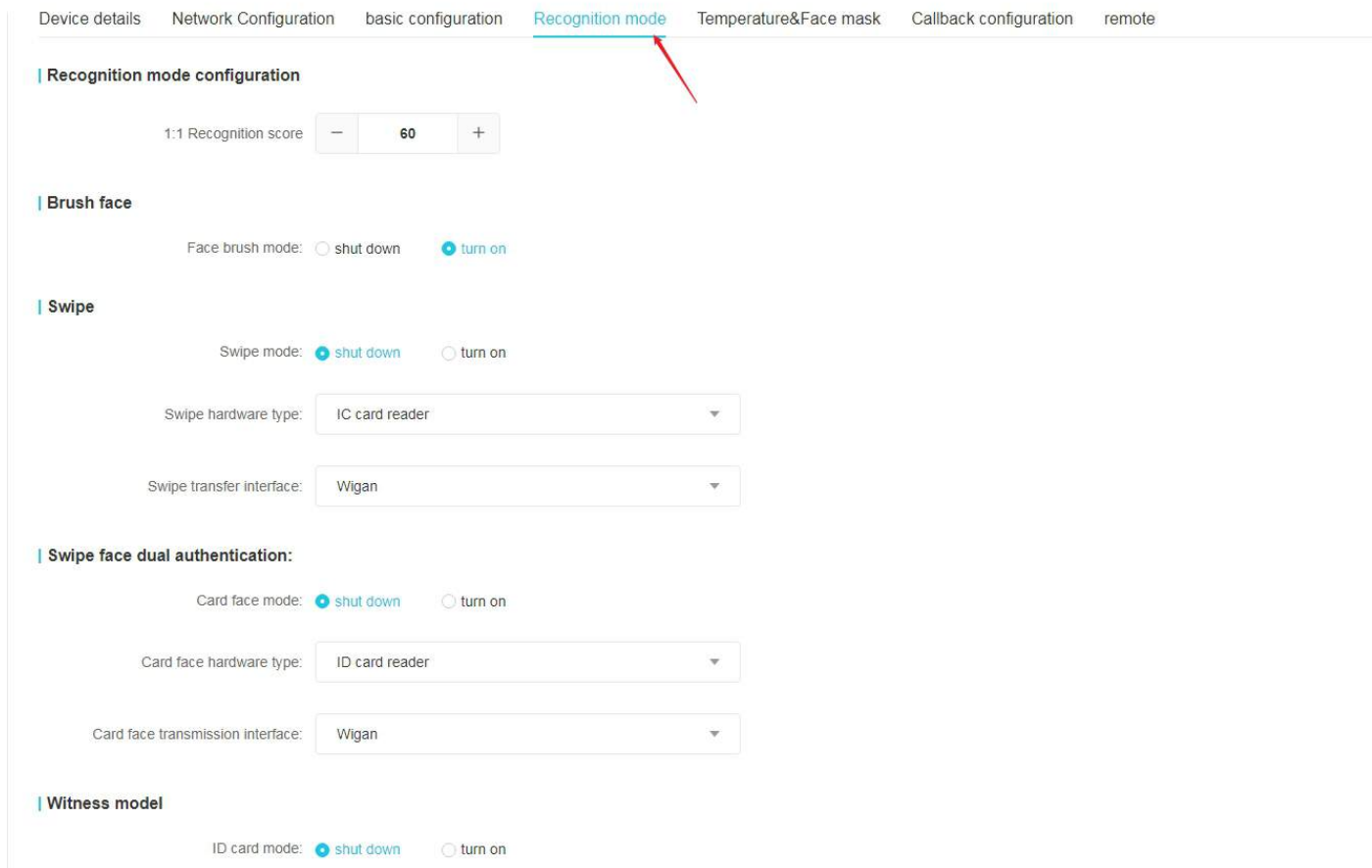Custom content for stranger voice: Alert, watch out for strangers

- After the device recognizes a stranger, it defaults to 2

- Do not broadcast voice

- Voice announcement "Stranger Alert"

- customize

    - Broadcast custom content. Only numbers, English and Chinese characters are allowed, symbols are not allowed, and the length is limited to 255 characters. Such as: watch out for strangers.

    - Uncommon characters, capital Chinese characters, languages other than English cannot be broadcast, but simple English words can be broadcast.

3.4.4.Recognition mode configuration

Recognition mode setting : Set the recognition mode of the face machine: single or combined recognition modes such as face swiping, card swiping, card + face dual authentication, and person-to-card comparison. Card swipe mode and card + face dual authentication cannot be selected at the same time.

| Device details | Network Configuration | basic configuration | Recognition mode | Temperature&Face mask | Callback configuration | remote |

| Recognition mode configuration

1:1 Recognition score   −   60   +

| Brush face

Face brush mode: ◯ shut down   ● turn on

| Swipe

Swipe mode: ● shut down   ◯ turn on

Swipe hardware type: IC card reader ▼

Swipe transfer interface: Wigan ▼

| Swipe face dual authentication:

Card face mode: ● shut down   ◯ turn on

Card face hardware type: ID card reader ▼

Card face transmission interface: Wigan ▼

| Witness model

ID card mode: ● shut down   ◯ turn on

3.4.5.Temperature measurement & mask configuration

Temperature measurement parameter setting: Set whether to enable the body t emperature detection function and temperature measurement voice broadcast functio n of the face machine.

Mask parameter configuration: Set whether to enable the mask detection functi on and mask voice broadcast function of the face machine (in the basic settings, the multi-face detection needs to be set to detect the largest face).

3.4.6.Callback configuration

Identify callback settings : Set the correct IP address and port of the recognition callba ck server to properly display the real-time record of face recognition in the real-time monitoring interface of the workbench. The server IP is the system software computer IP, and the default port is 9000.

3.4.7.Remote control

Set time : Use the computer time to synchronize the device time. The device time in the network must be the same as the computer time, otherwise it may cause errors in the statistics of the people present.

Device reset : Clear all data in the device, including face data and related parameters.

Open the door remotely : Control the face machine to open the door through the computer.
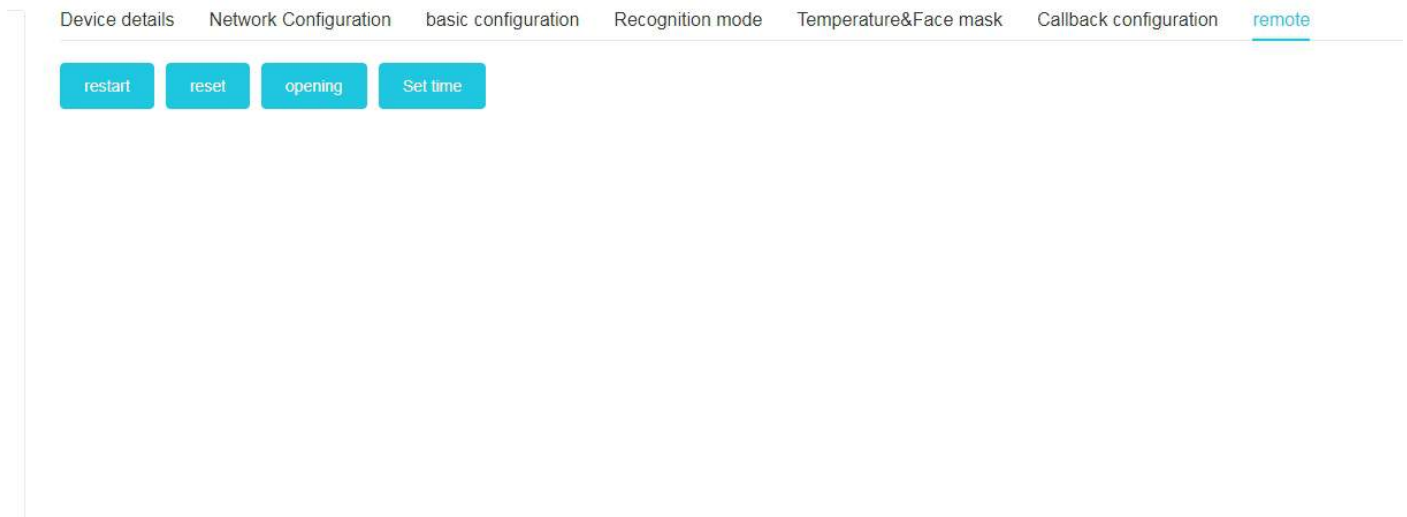
3.4.8.Custom Configuration

The custom configuration in the background is the same as the custom configuration on the device. Some configurations of the device can be changed by entering the corresponding key and value values. The existing custom configuration and description of the device are as follows :

	A	B	D	E
1	键	值	说明	
2	high_temperature_open	true	Open the door at high temperature, not open normally	
3	img_base64_upload	false	Close upload image base64	
4	stranger_open	false	Close stranger open door	
5	un_mask_open	true	Open the door without wearing a mask	
6	record_save_days	1-30 （小于等于30）	Set the number of days to save the recognition record picture	
7	temperature_unit	2	Fahrenheit shows temperature in Fahrenheit	
8	high_temperature_alarm	true	Set high temperature alarm sound	
9	ui	1 or 2	1: First set 2: Second set	
10	key	wg	Increase wg26 configuration: default 34	
11	value	26 or 34	Increase wg26 configuration: default 34	
12	out_232	ttyS1(串口号)	Customized RS232 output information	
13	hide_device_info	true	Information hiding configuration at the bottom	
14	close_upgrade	true	Close upgrade configuration	
15	fixed_temperature	false	Whether to enable the temperature correction configuration, the default is on | off:	
16	fixed_min_temperature	(20 - 34.9)	Temperature correction lower limit configuration, default 33	
17	fixed_max_temperature	(35 - 44.9)	Temperature correction upper limit configuration, default 35.7	
18	close_stranger_upload	true	Configure to close unfamiliar data reporting	
19	show_temperature_tip	true or false	Whether to display forehead temperature	
20				
21				

Single setting:

Click on the device display list, click on the serial number (blue font) of the device that needs to change the custom configuration, then enter the device setting interface, click on custom configuration, as shown in the figure below :
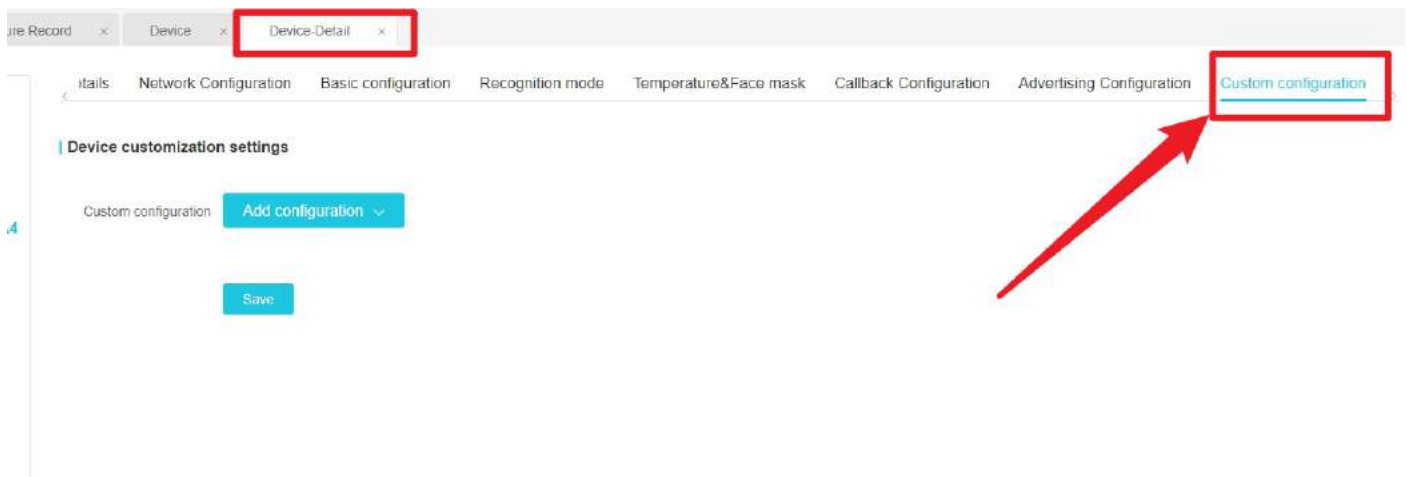
Click [Add Configuration] in the custom configuration, select the common configuration (key and value, value is the value), picture configuration (key and value, value is the picture) to be added. Enter the corresponding value and click Save after

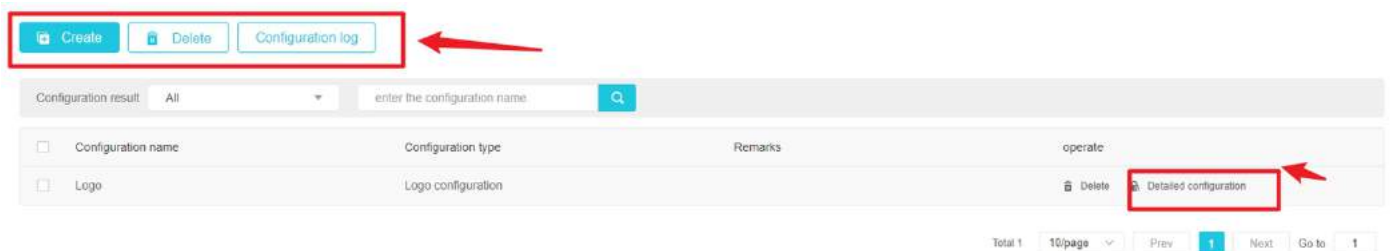adding it to change the custom configuration of the device
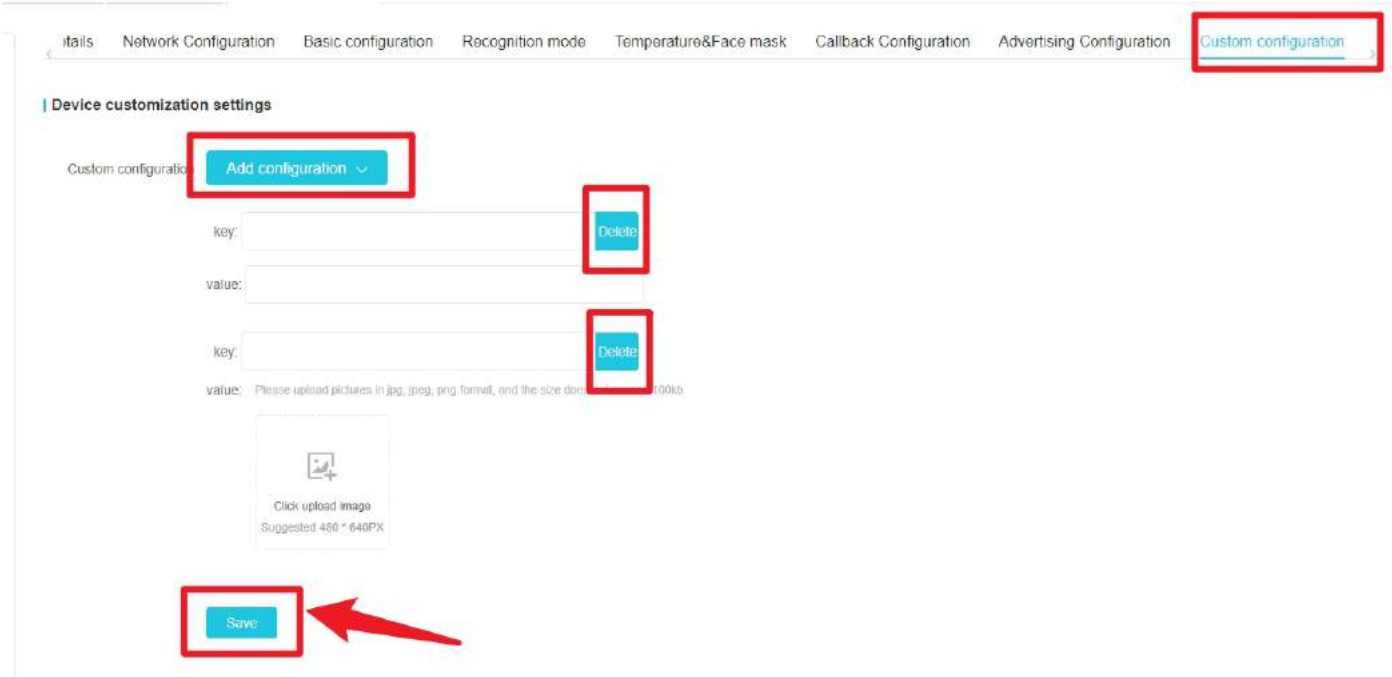
3.4.9. Bulk device settings

Click [Device], [Configuration Management] to configure multiple devices, such as masks, logos, and temperature measurement. The locations are as shown in the figure below:
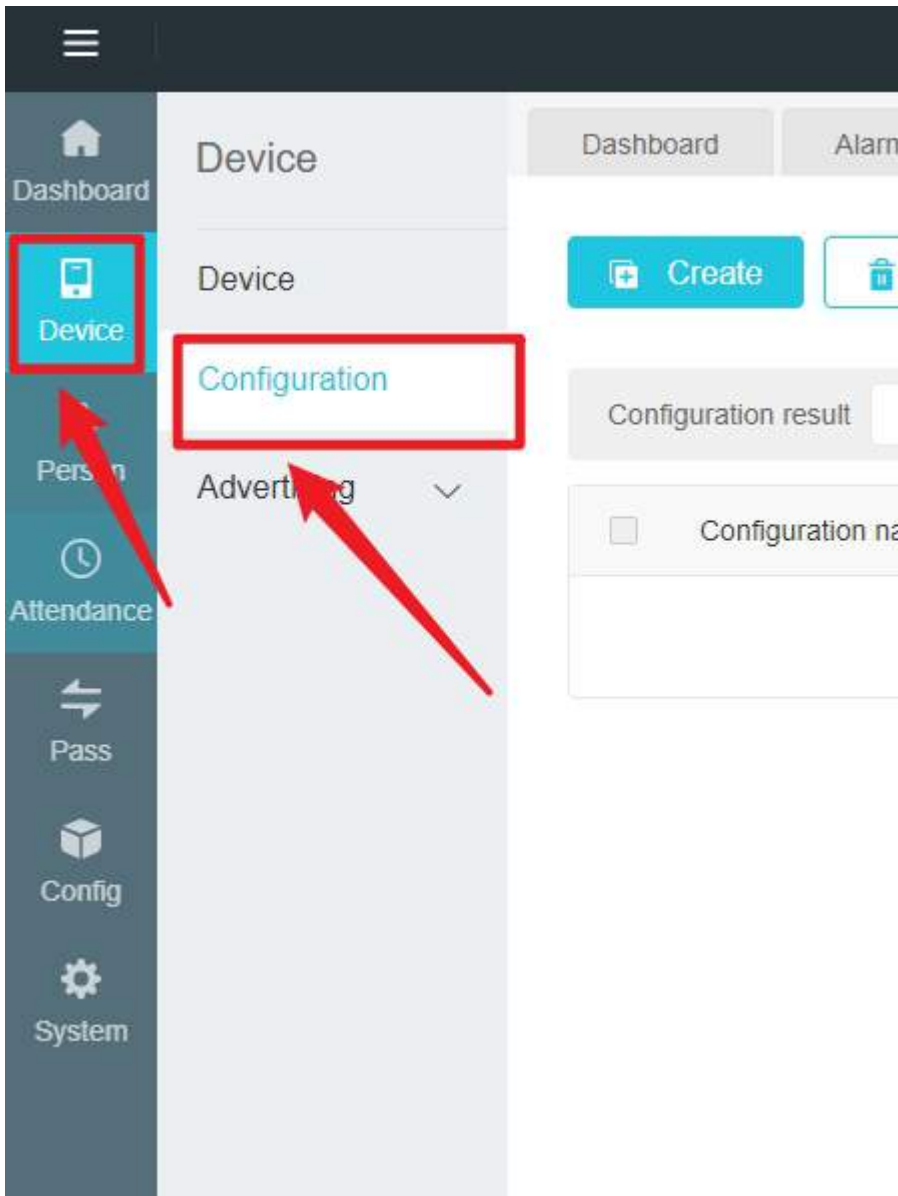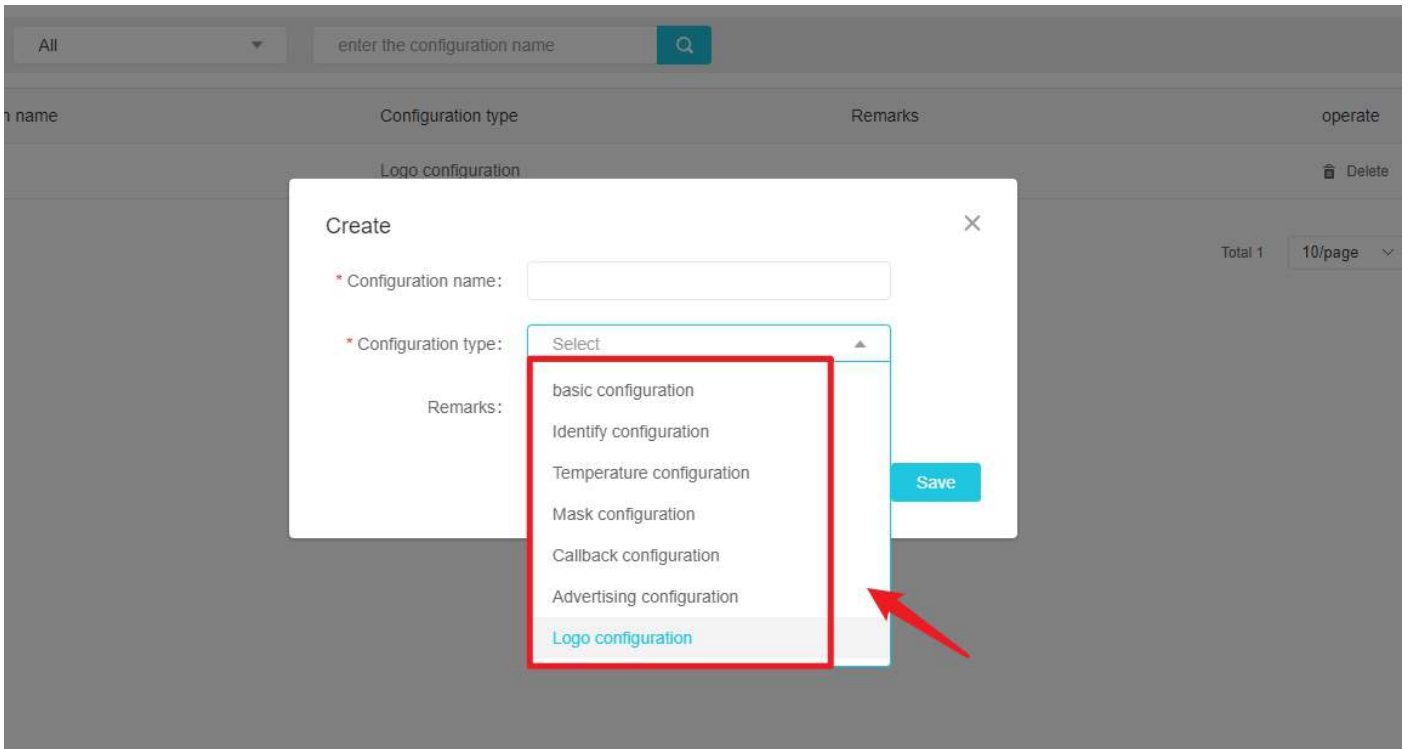
The display list is shown below :

Step 1: Create a new configuration: Click the [New] button in the display list to create a new configuration. In the new page, you need to fill in the configuration name, configuration type, remarks, etc., as shown in the figure below

Step 2: Set up the detailed configuration: After creating the new configuration, the

newly added configuration will appear on the list page. Click [Detailed Configuration] in

the operation bar of the configuration column. The example below is the Logo

configuration. The detailed configuration is shown in the following figure: (If [

Configuration type] For test configuration or other configuration, other configuration

details page will appear)

Set the logo

device Logo (Please upload pictures in jpg, png, jpeg format, and the size does not exceed 500kb)

Click upload image
Suggested 480 * 640PX

Save

Step 3: Batch configuration: After saving the configuration details, go to the device display list (click [Device], [Device Management]), the specific location is as shown in the figure below:
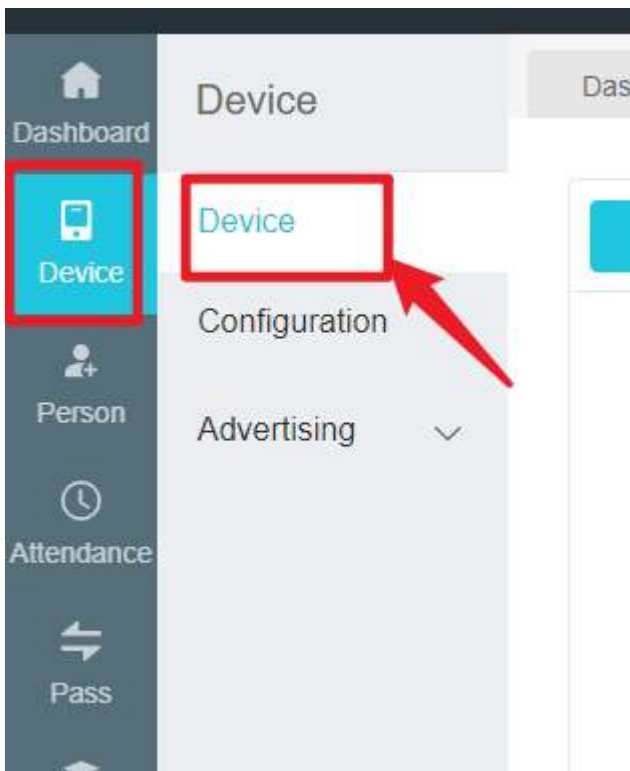
The device list display page is shown below:

1) On the device display page, select one or more online devices, place the mouse on the [Batch Configuration] button, and the type of batch configuration will appear
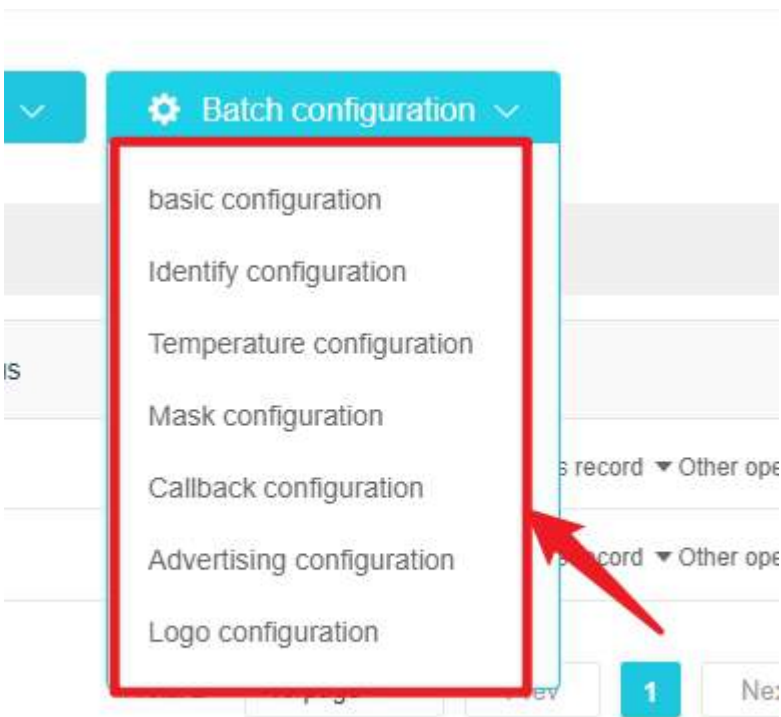
2) Select the configuration type of the configuration newly created in the first step, such as logo configuration, all configuration names with the configuration type as logo configuration will appear, select the name that needs to be configured to the device, click processing, and the configuration of the batch device is completed .
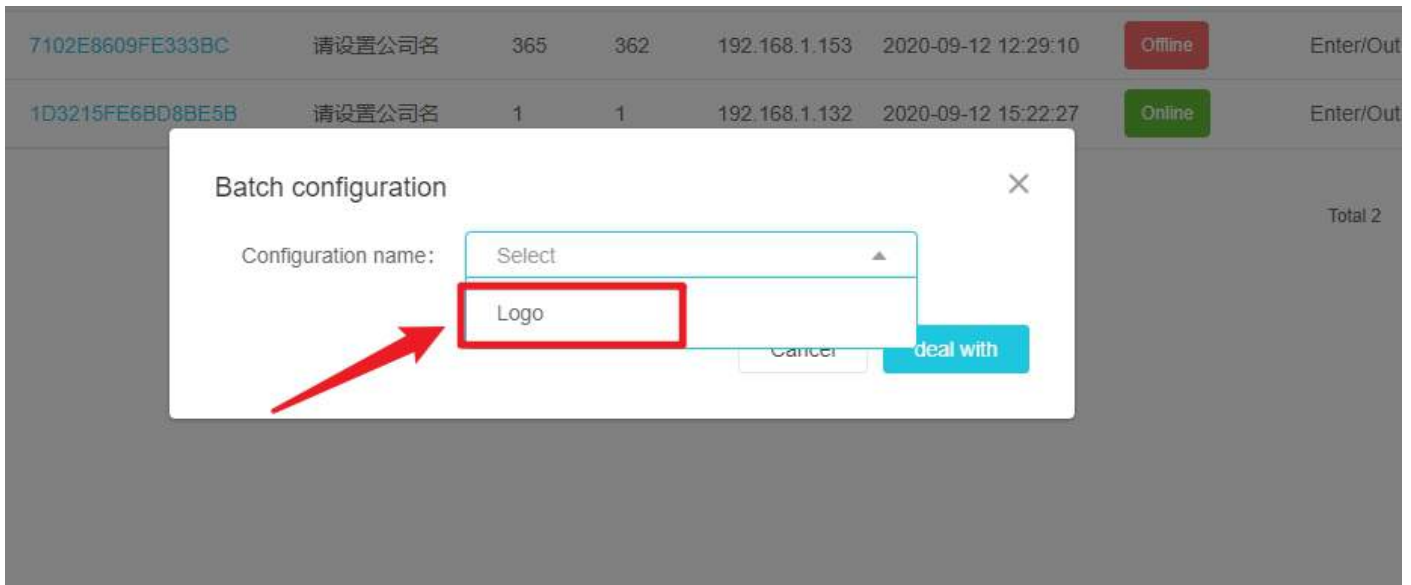
3.4.10. EU Health Code Configuration (EU Health Code Equipment Support)

Description of the setting parameters of the EU health codes:

1. Vaccine certificate rule settings:

    1) Vaccine expiration check setting switch: By default, by opening, the device will check the vaccine information in the health code. If the vaccine has passed the effective number of days of the vaccine, this person can not pass.

    2) Vaccine Effective Time Setting (unit: day): The default is 270 days.

    3) Vaccine antibody effective check switch: By default, by opening, the device will check the vaccine information in the health code, if the vaccination time has not reached the effective time, this person can not pass.

    4) Days of effectiveness of vaccine antibodies: The default is 15 days.

    5) The number of vaccination limits can be set to:

        a) It is not allowed to pass

b) **All vaccines are allowed to pass (default)**

c) **Some of the vaccine is also allowed to pass**

d) **Pass is also allowed without a vaccine**

2. Nucleic acid detection rule setting:

1) **Nucleic acid test expired check switch:** Turn off by default, the device will check the nucleic acid detection information in the health code, if the detection time is more than valid days, this person can not pass.

2) **Effective days for nucleic acid detection:** The default is 15 days.

3) **The detection result limit can be set to:**

a) **It is not allowed to pass**

b) **Nucleic acid normal normal pass (default)**

c) **Nucleic acid irregularities are also allowed to pass through**

3. Rehabilitation rules settings

1) **Rehabilitation rehabilitation limit can be set to:**

a) **It is not allowed to pass**

b) **The rehabilitation certificate is allowed within the validity period (by default)**

c) **The rehabilitation certificate is not valid and is also allowed to pass**

4. Privacy settings

1) **Display vaccine information switch: turned on by default**

2) **Record the EU code information switch: turned on by default**
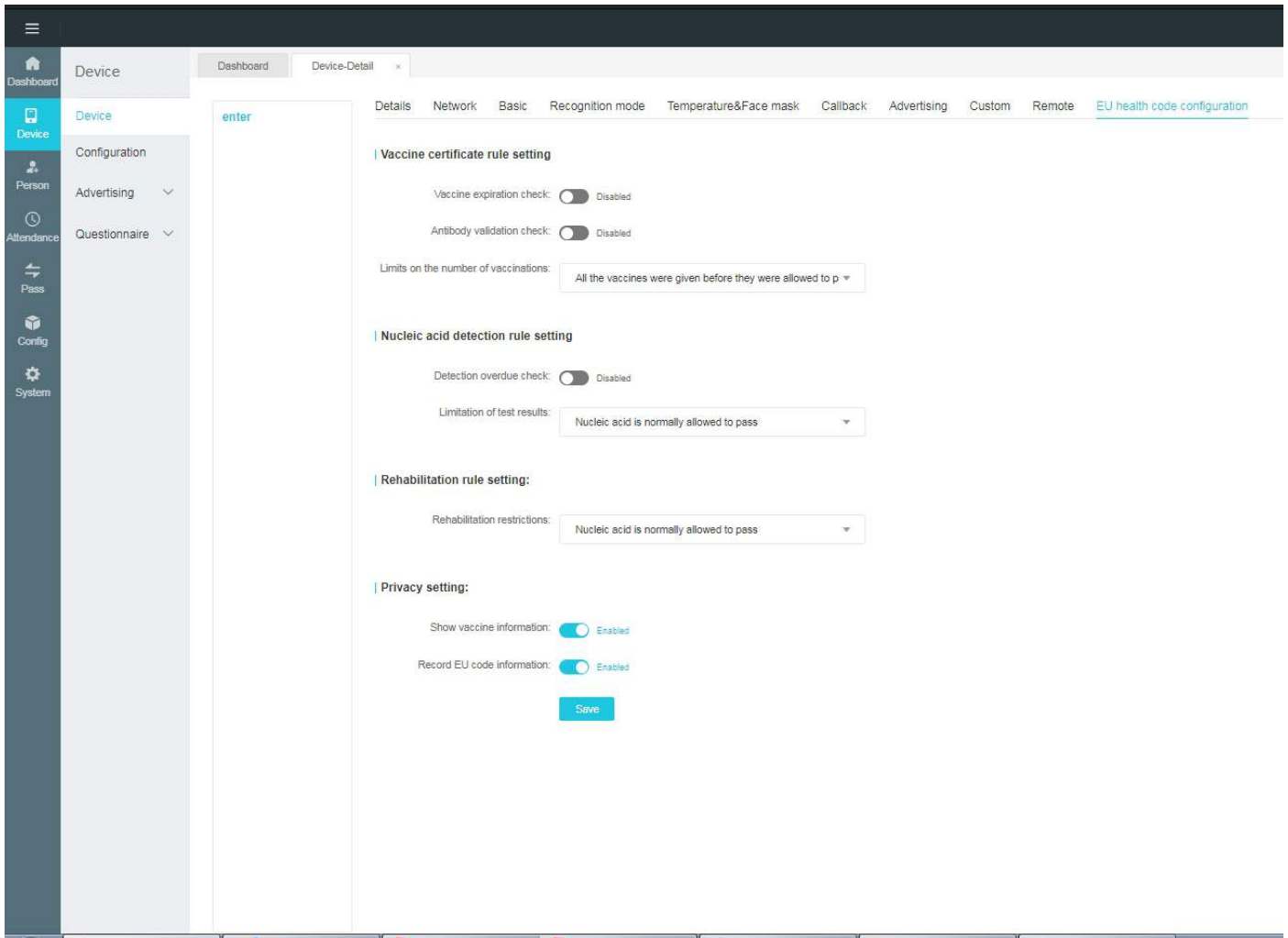
3.5.Advertising management

3.5.1.Advertising information

Click [Equipment], [Advertising Management], and go to the advertising managem
ent module to add and delete advertisements. The location is shown in the figure bel
ow:
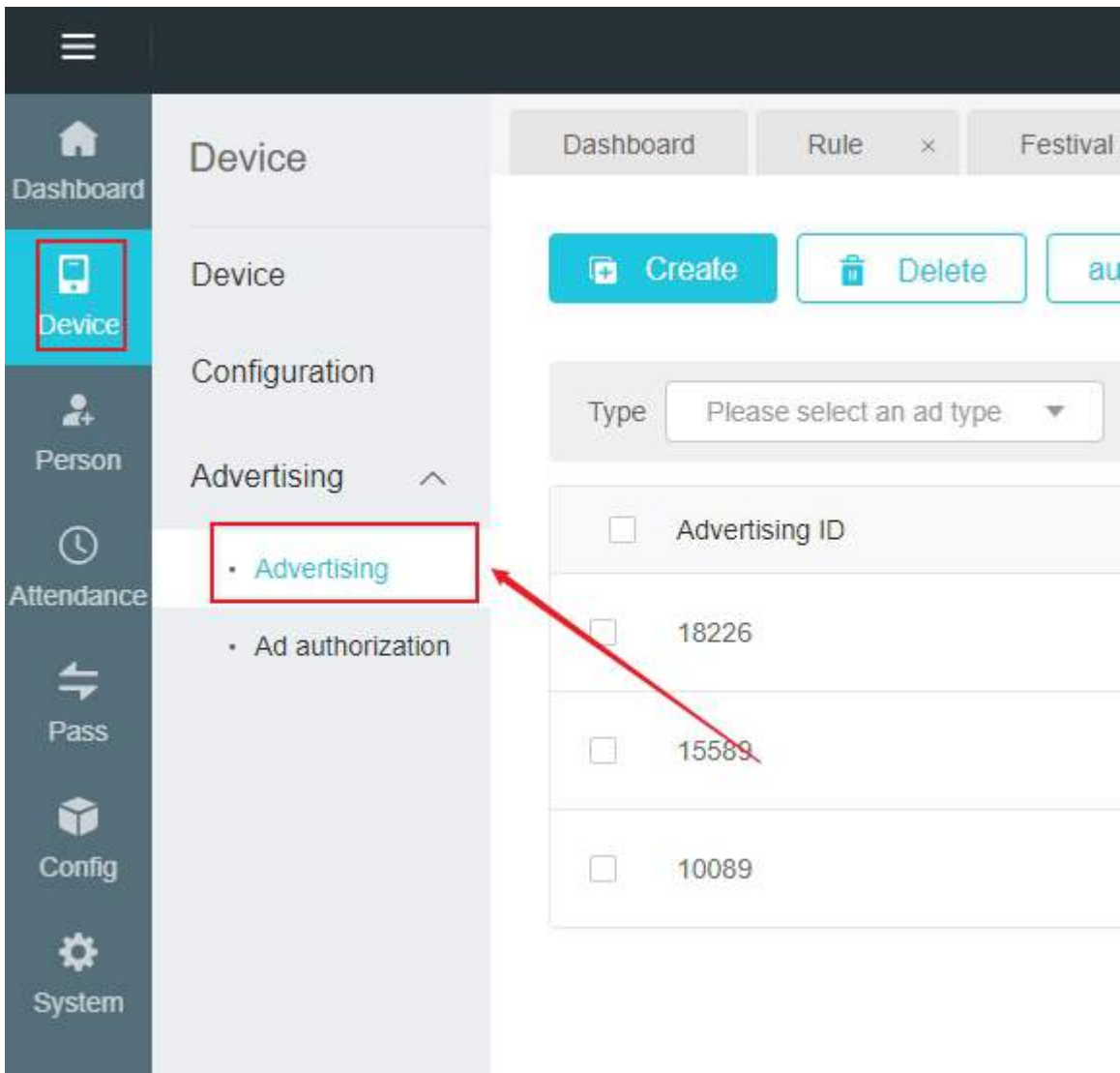
The advertisement display list is shown in the figure below:
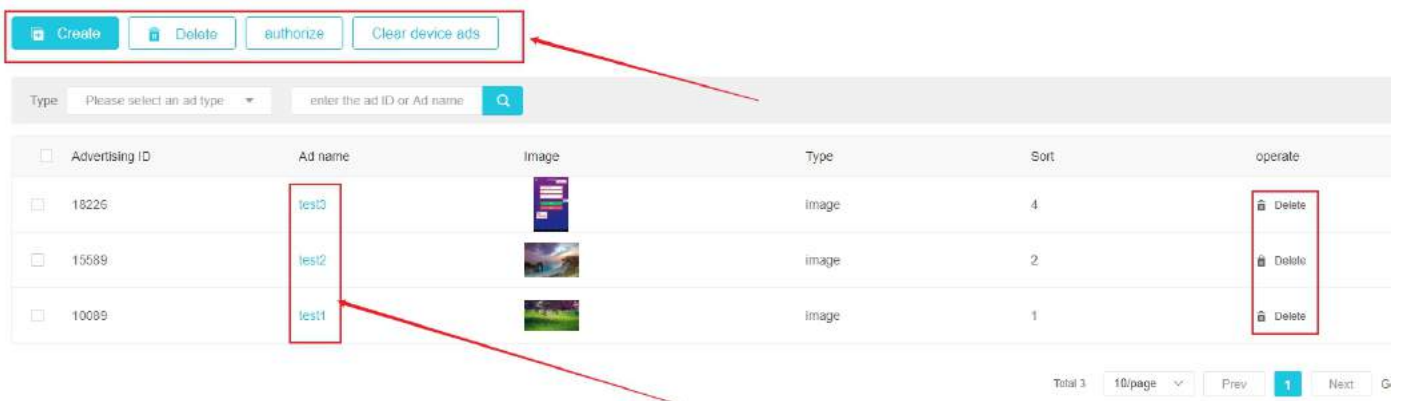
New advertisement: Click the [New] button to jump to the new advertisement page, as

shown in the figure below: Note: [Sort] requires a number to be selected. After

authorization, the device will play advertisements in the order of the order value.

Advertisement type: When the advertisement type is image, the new page is as show n below:

Modify ad: Click on the ad name (blue font) in the display list to jump to the page to

modify the ad

Modify the page as shown:

3.5.2. Clear all ads on the device

On the display page of the advertisement list, click the button [Clear Device Ads] a nd select an online device to clear the advertisements on the selected device.

3.5.3.Advertising authorization

Step 1: Select advertisement: In the advertisement information, after selecting the advertisement that needs to be authorized to the device, click the [Authorize] but ton, as shown in the figure below:
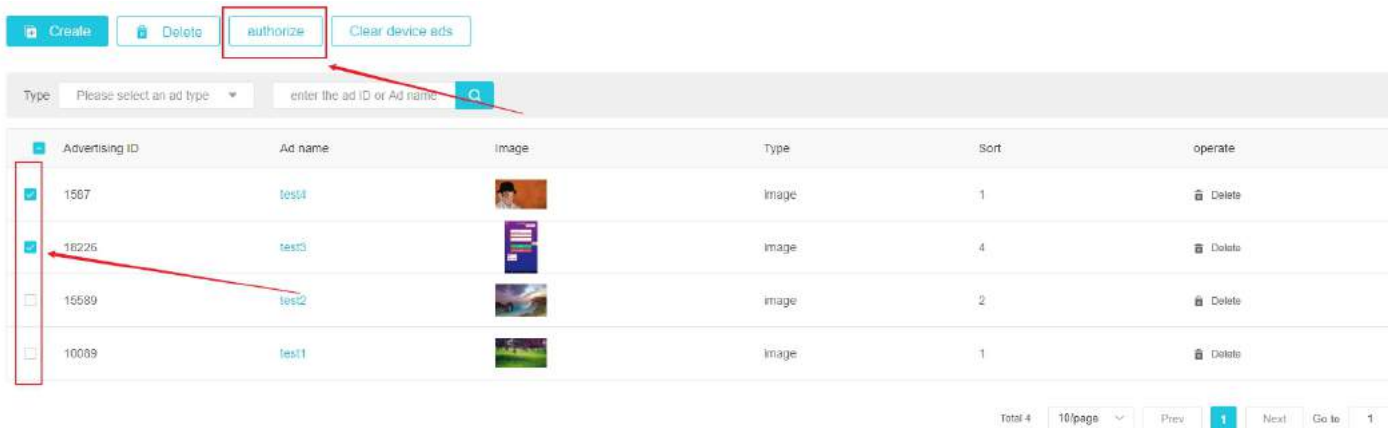
Step 2: Select the device: After clicking [Authorize], the page as shown in the figure below pops up, and the status bar selects authorization or deauthorization, and select s the online device in the online device list, and clicks the [Process] button. The selec ted ad is authorized to the selected device
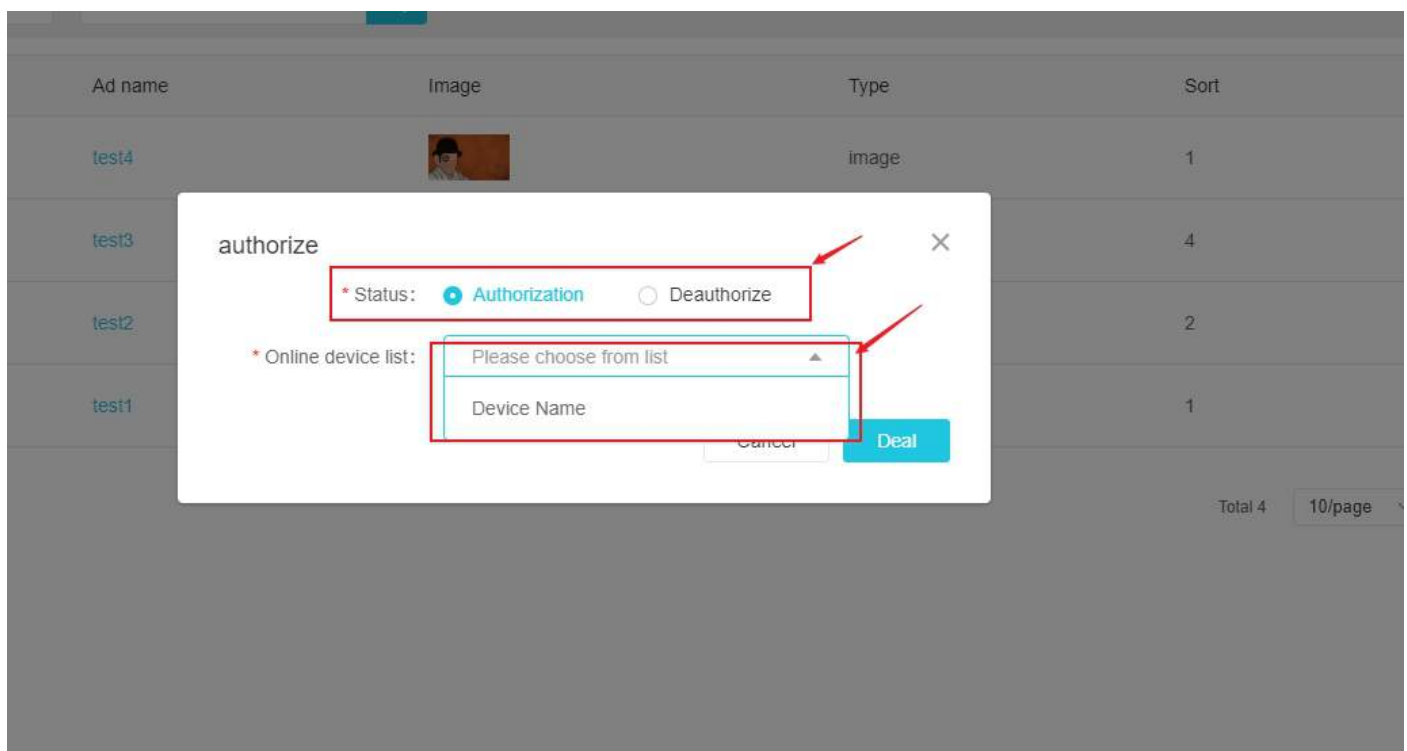
After authorization, you can click [Ad Authorization] in the navigation bar to view the

authorization status and details, as shown in the figure below：

Click [Details] in the operation bar to view the details of the authorization information just

now, as shown in the figure below:

Step 3: Configure ads:

Single device configuration: After authorization is completed, click to enter the device

display list, the location is shown in the figure Below
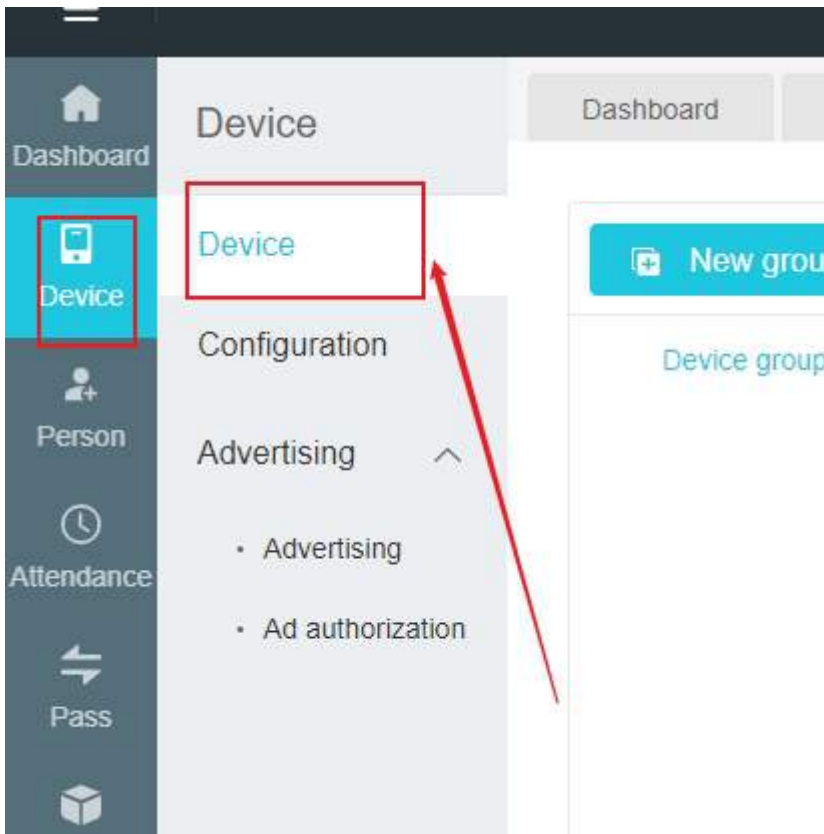
1)The device list display page is as shown in the figure below, click the serial number (blue font) of the device to be configured to enter the configuration interface of the device
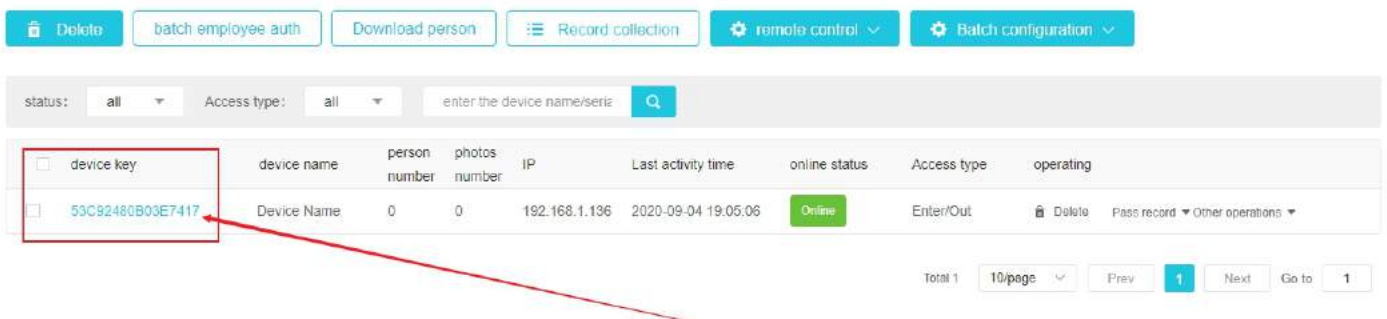
2) Click [Advertising Configuration] in the configuration to start the advertisement, and set the type of advertisement to be played on the device, the type of device split screen, the picture rotation time, etc., and click Save, the setting is successful
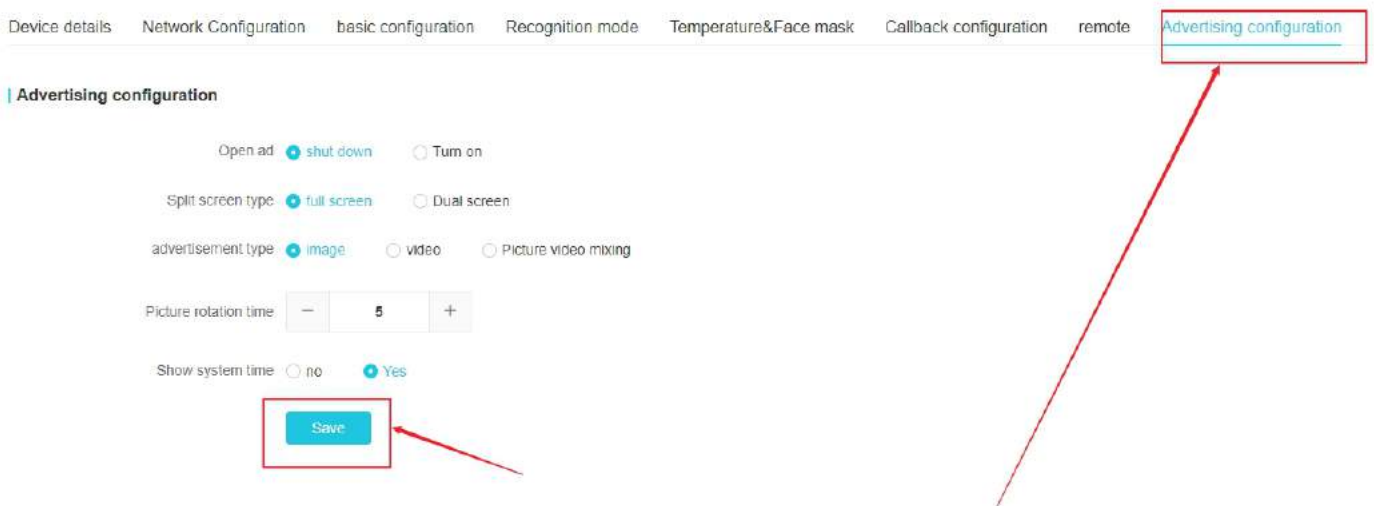
3.6. Questionnaire management

For some functions of the questionnaire, please install the apk version v1.41.4.0 with the face recognition device to use the customized version of the questionnaire. If other apks do not have this function, please ignore.

Part of the function of the questionnaire is: After setting the questionnaire information and topic information in the questionnaire management, the questionnaire can be authorized to be displayed on the device. The questionnaire will pop up when someone passes through the authorized device. After answering the questionnaire information, you can check the specific information and whether the answer is correct in the questionnaire answer. After turning on the questionnaire alarm switch, when the passer makes an incorrect answer. The system will send a questionnaire alert email to the recipient's mailbox. For how to set the email, please refer to [7.6. Mail Service Settings] and [7.5 Alarm Settings]
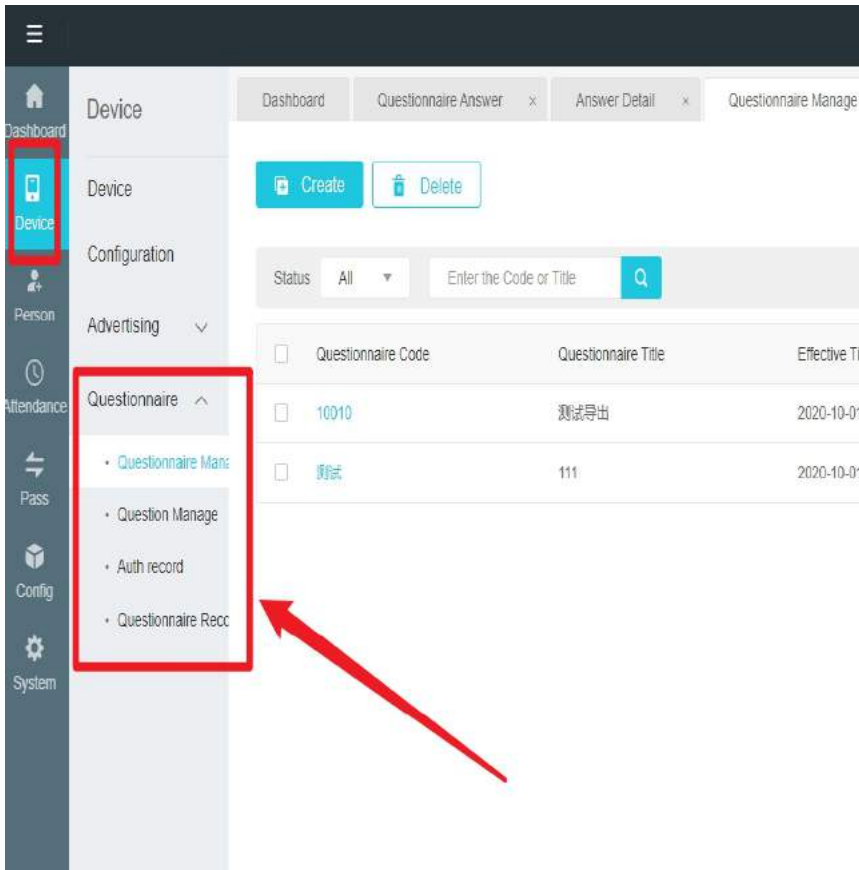
3.6.1.Generate "a questionnaire"

The questionnaire management part is divided into questionnaire information, top

ic information, synchronization records, and questionnaire answers. A real questionnair

e is composed of questionnaire title, questionnaire topic, questionnaire topic options,

etc. How to generate "a questionnaire" and authorize it to use the device? Proceed a

s follows :

➢ □ **Step 1: Create new questionnaire information**
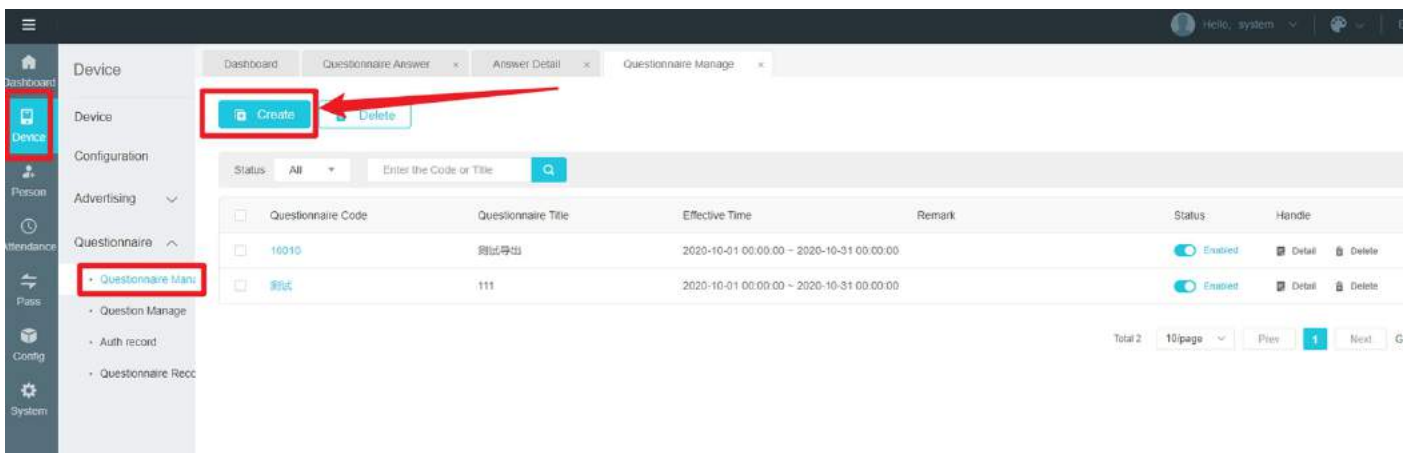
Click the [Create] button on the page, enter the necessary information for the new questionnaire and click Save to create the new questionnaire information, as shown in the figure below:
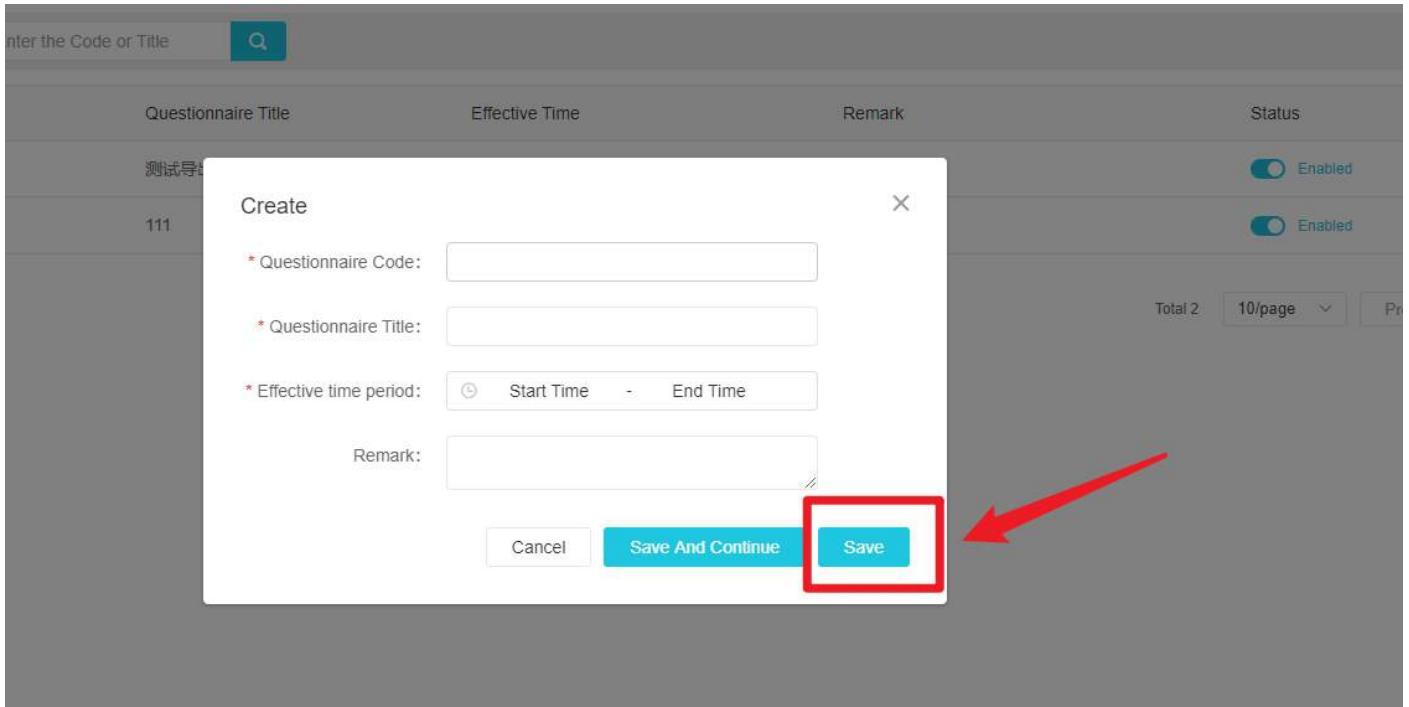
At this time, the questionnaire only has the number, title, etc., and there is no topic information. You need to create new topic information and select the topic to belong to the questionnaire.

➢□ **Step 2: Create new topic information**
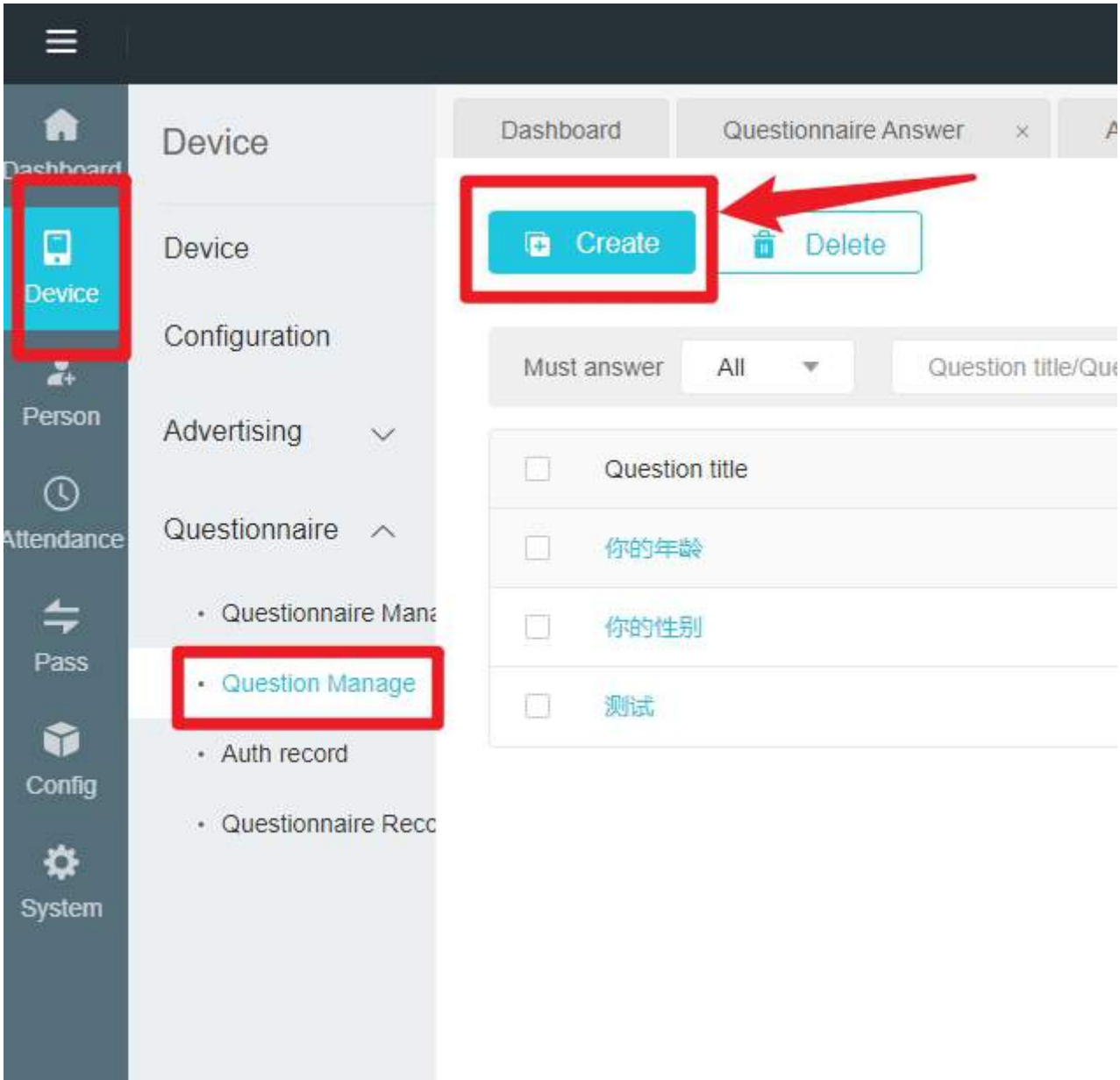
Click the [Create] button on the topic information page to create a new topic

information, and select the questionnaire title to which the topic belongs (for example: the

title of the questionnaire information created in step 1), as shown in the figure below (the

figure below is an example, specific questions and options Please adjust the content

according to the actual situation):

In this example, only one question is created. In actual operation, several questions can be created, and the questionnaire can belong to the same questionnaire.

➢ ⬜ **Step 3: View questionnaire information**

Click into the questionnaire information to view the questionnaire information after adding the question; click [Details] in the operation bar of the questionnaire you want to

view
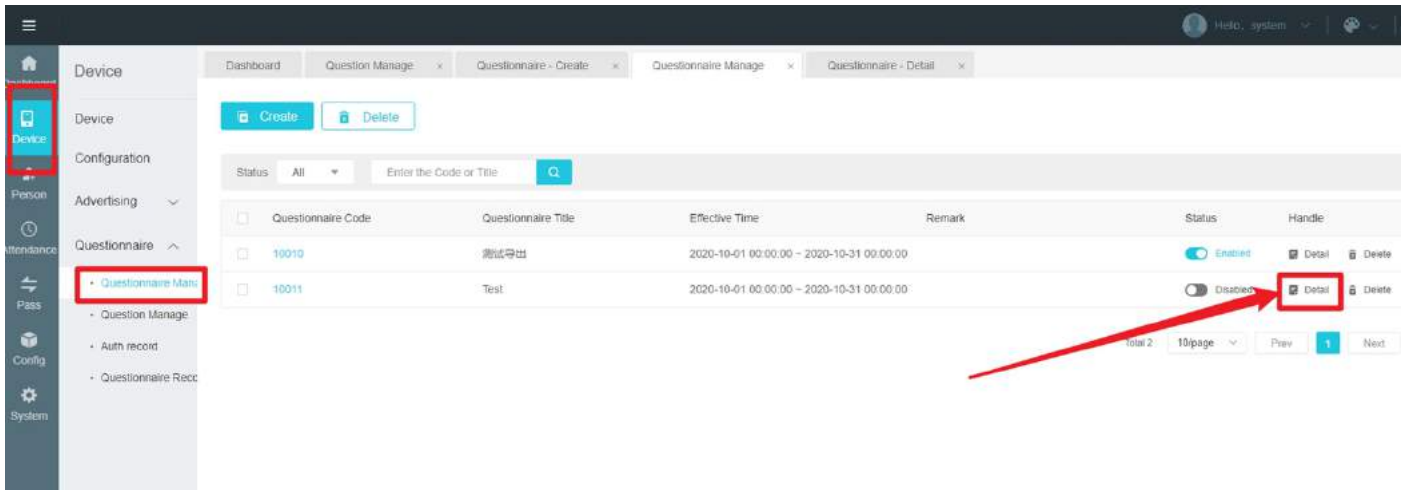
The details of the questionnaire are shown in the figure below:
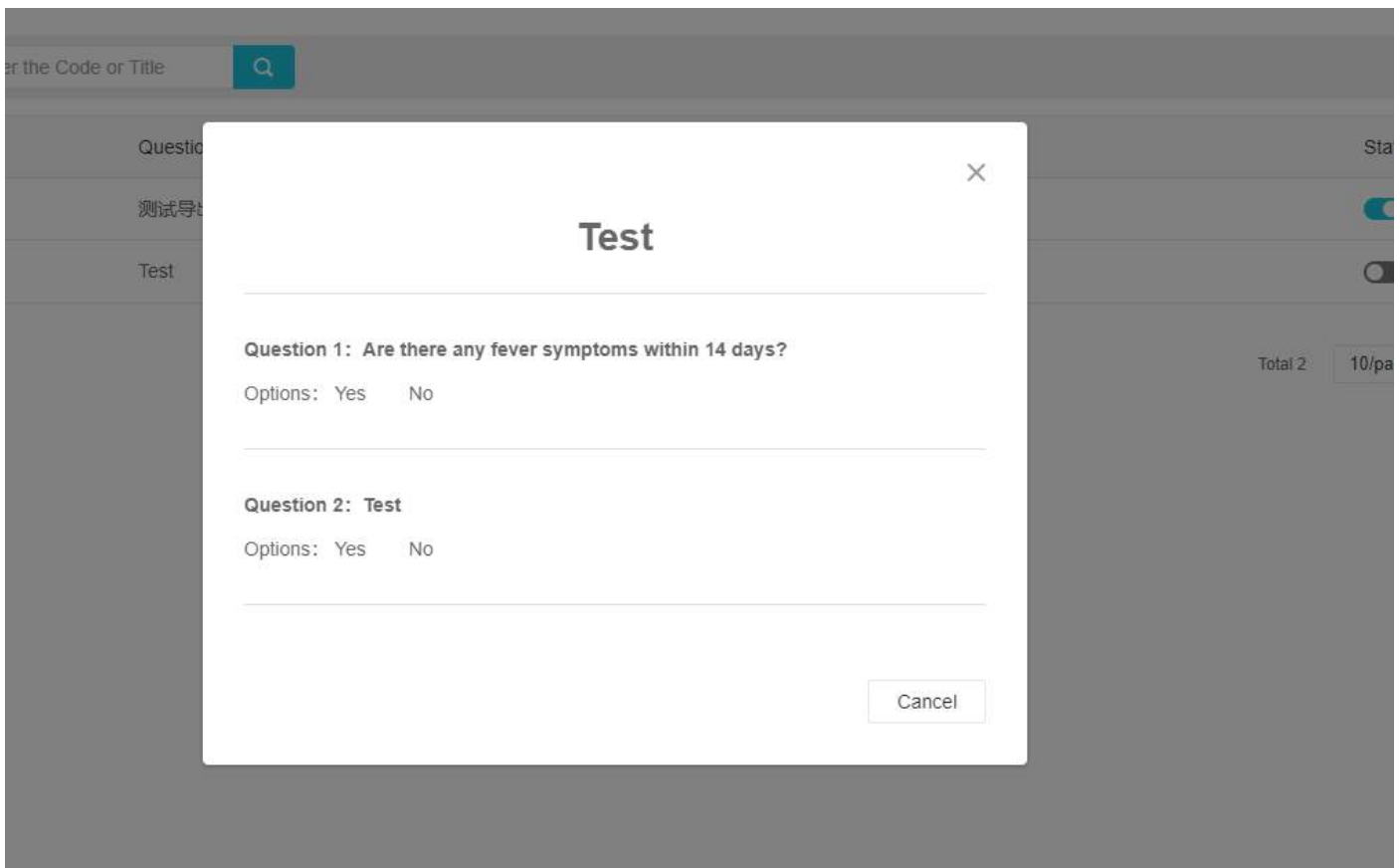
> □ **Step 4: Authorize to the device**

Click Open on the status bar of the questionnaire information that requires authorizat

ion, and the authorization box will pop up
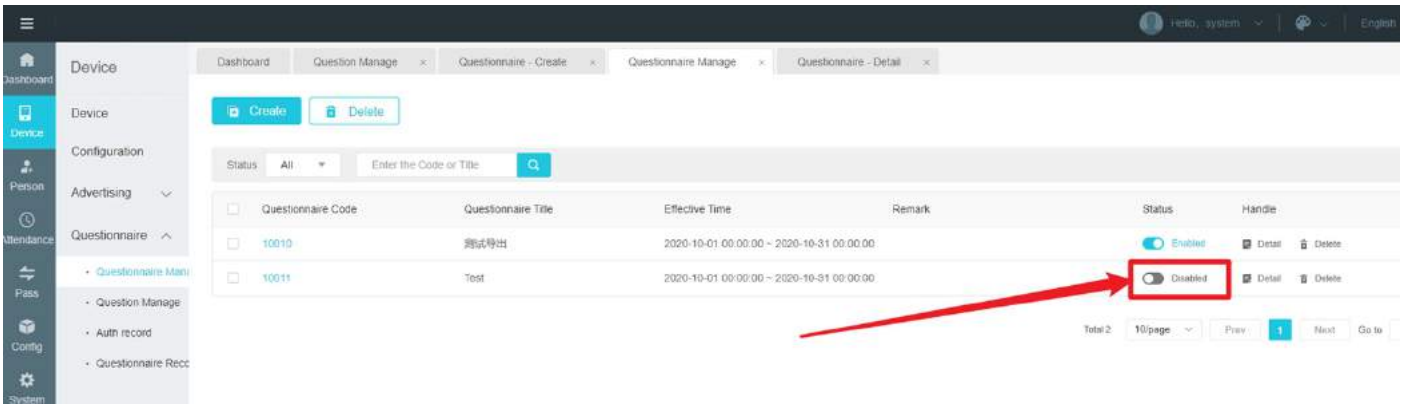
In the pop-up authorization box, select the device that needs to be authorized, and click

"Success", which means that the questionnaire is successfully authorized to the device
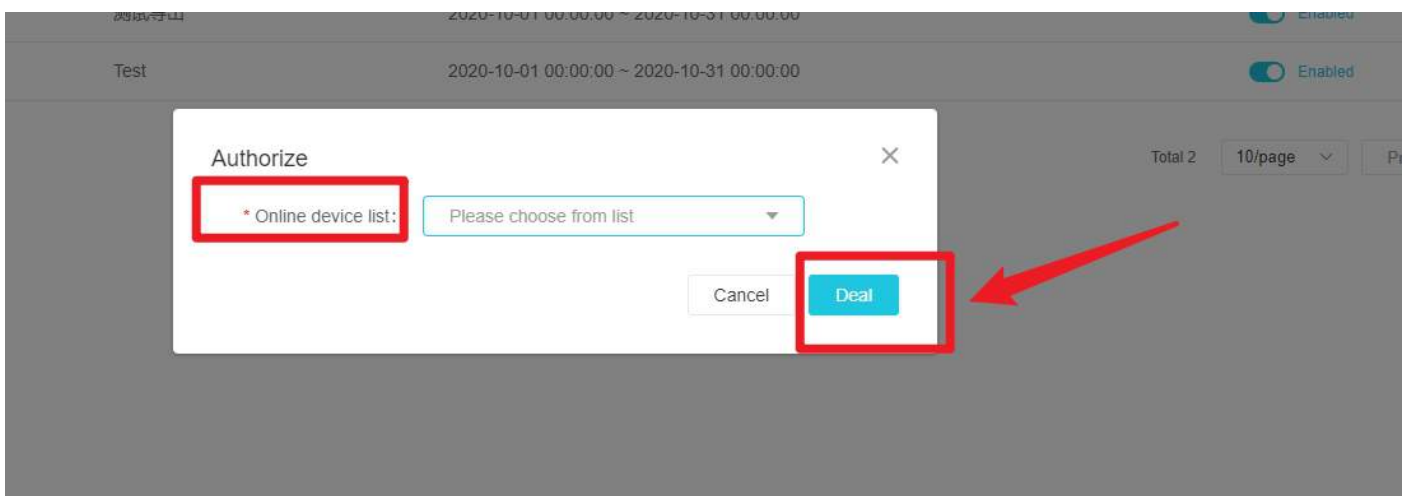
➢ **Step 5: View authorization records**

Click to the synchronization record, you can view the record just authorized
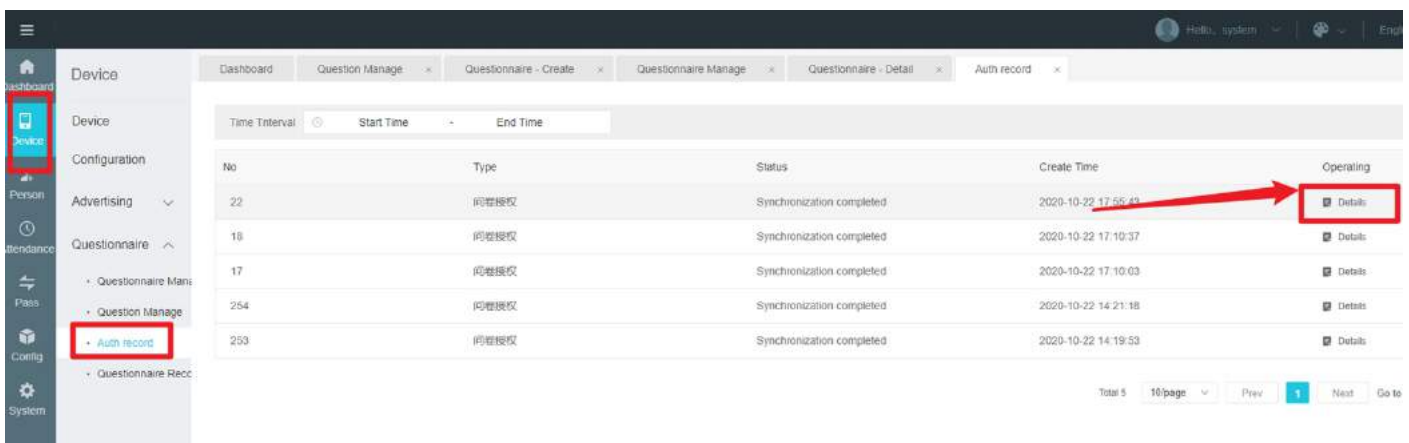
All authorized records will be displayed on this page. Click the [Details] button in each

column to view the details of the information in the just authorization. If the status in the

authorization details shows "Authorization Successful", it means that the questionnaire is successfully authorized to the target device, and you can go to the device to pass verification!

3.6.2.Questionnaire information

The information content of the questionnaire is the questionnaire number, question naire title, valid time, remarks, etc. The display page is as shown below:
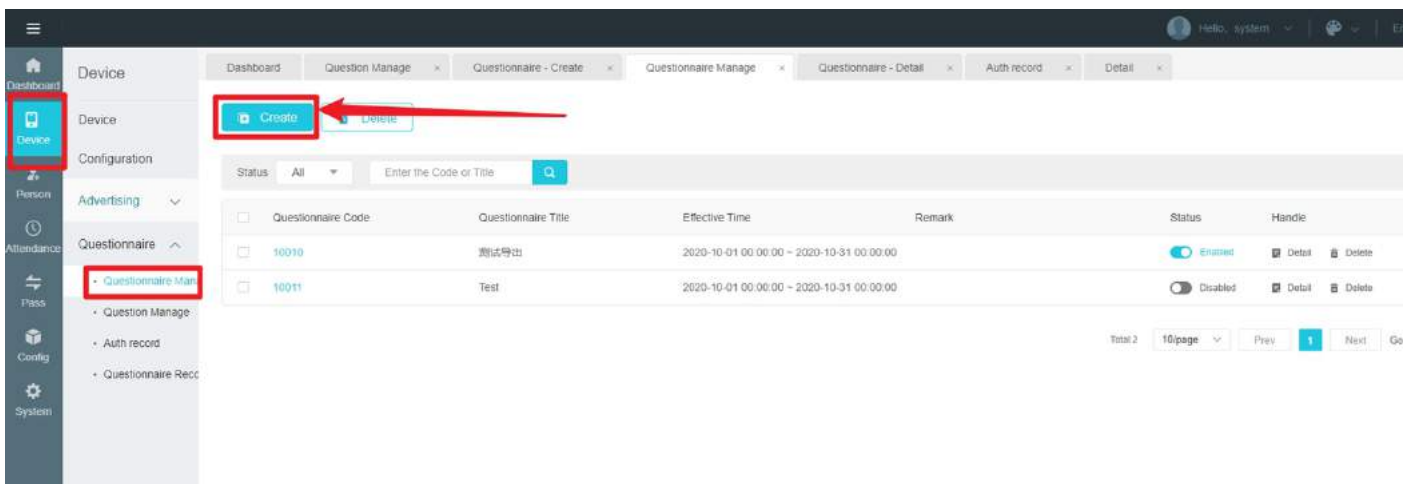
➢ □ **Create**

Click the [Create] button on the displayed page, add required options in the pop-u p box, and click Save to create a successful
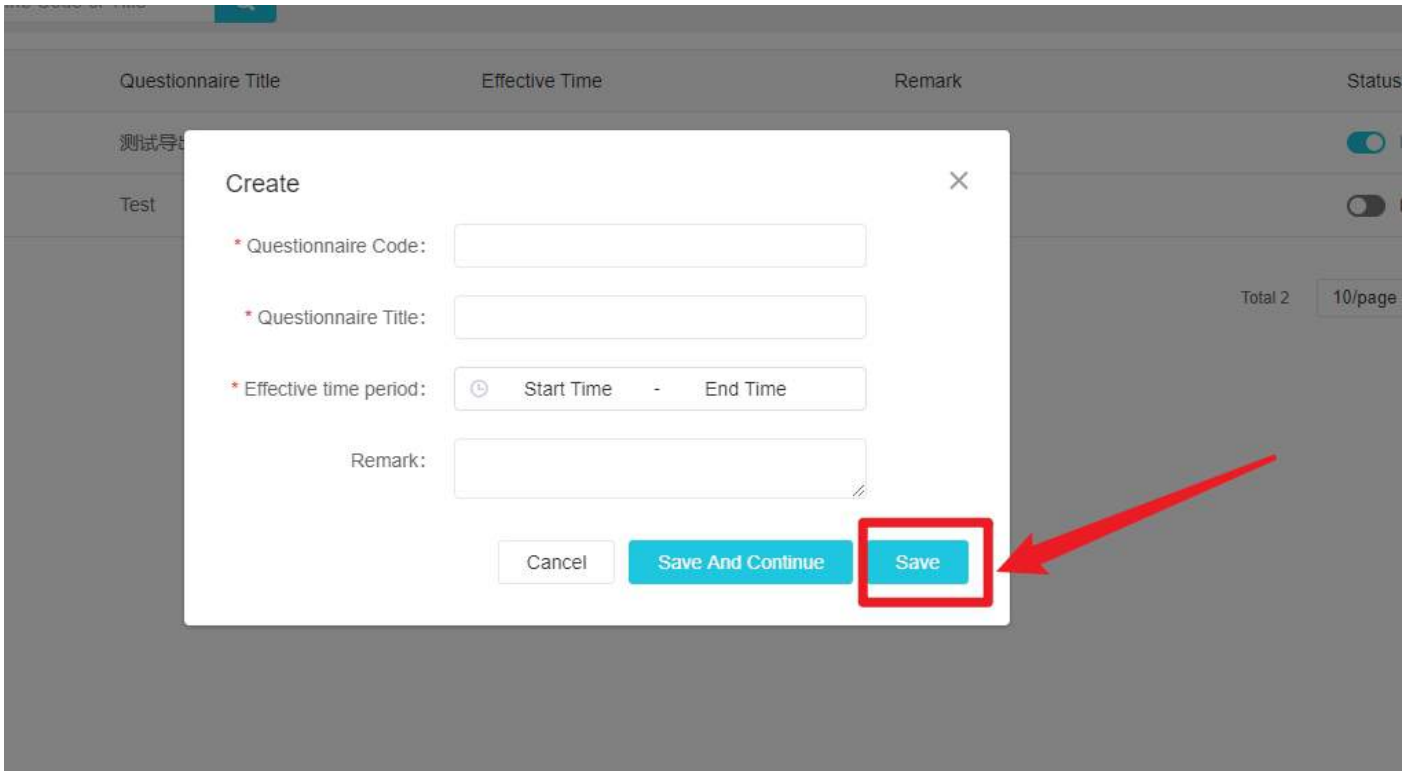
➢ □ **Modify**

On the displayed page, click the questionnaire number (blue font) whose questio

nnaire information needs to be modified, as shown below:
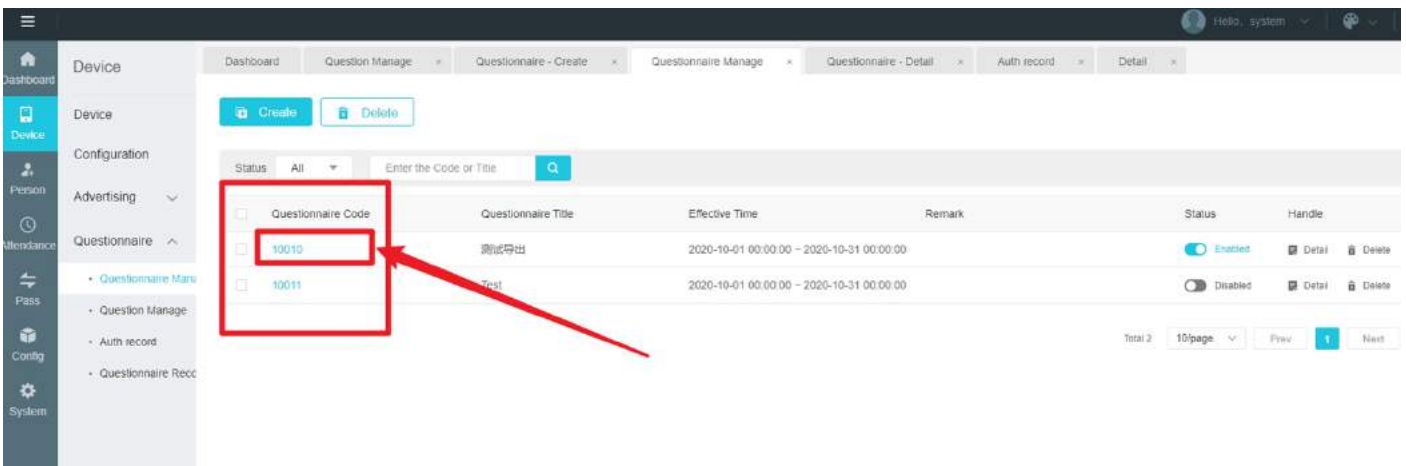
Enter the content you want to modify in the pop-up edit box, click save to modi

fy successfully
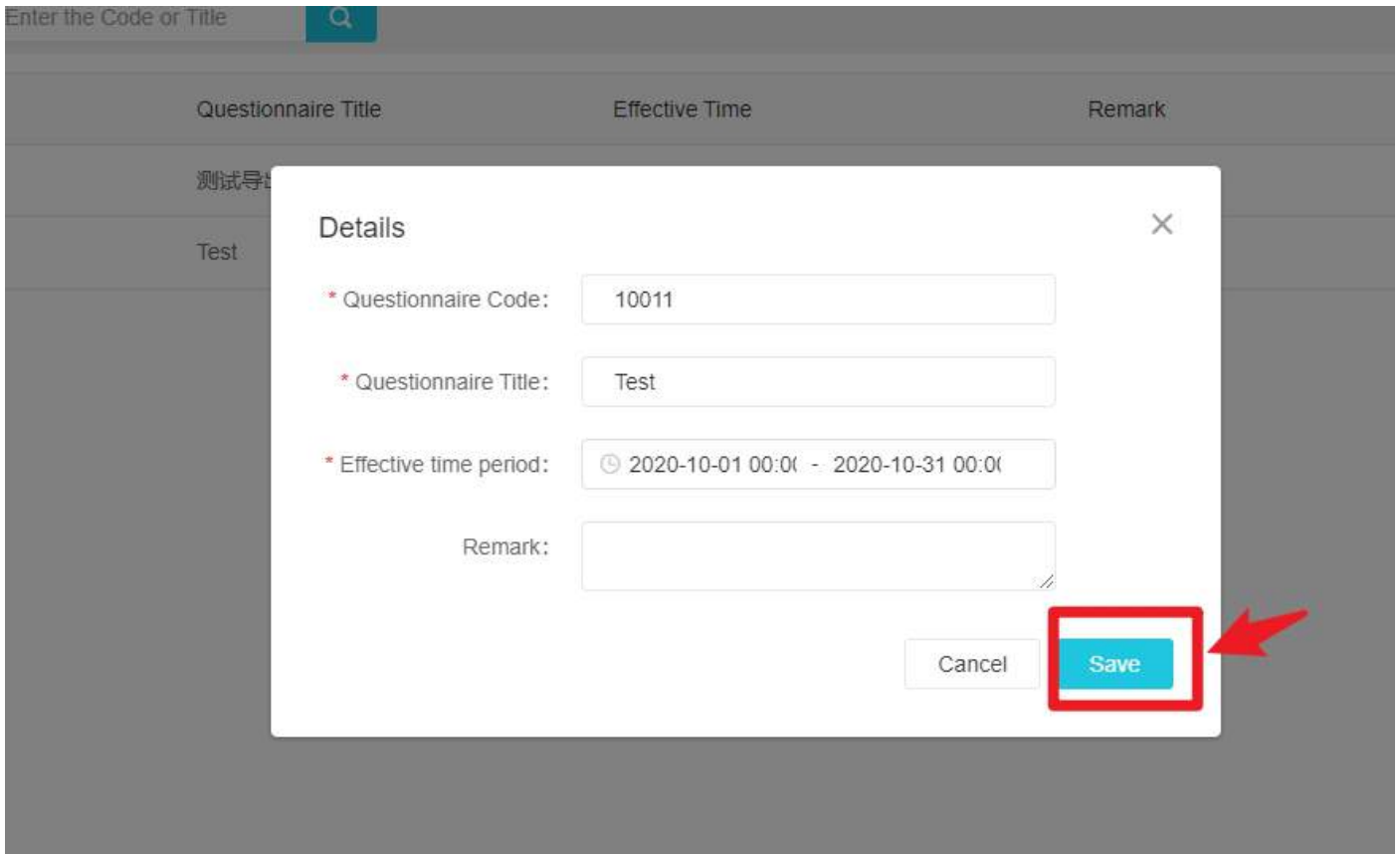
> ➢ Detele

Single delete: Click the delete icon in the operation bar of each row to delete the qu

estionnaire information in this row
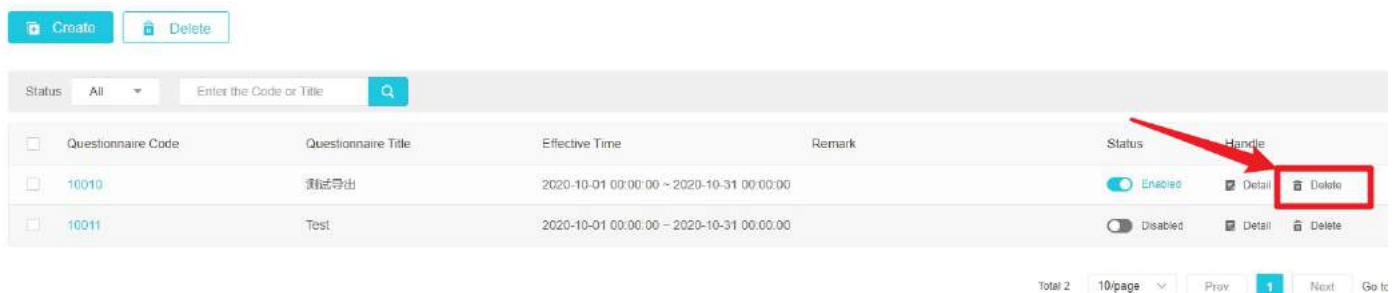
Batch delete: check the box in front of each column of questionnaires, after

selecting multiple questionnaires, click the [Delete] button to delete the selected

questionnaire information
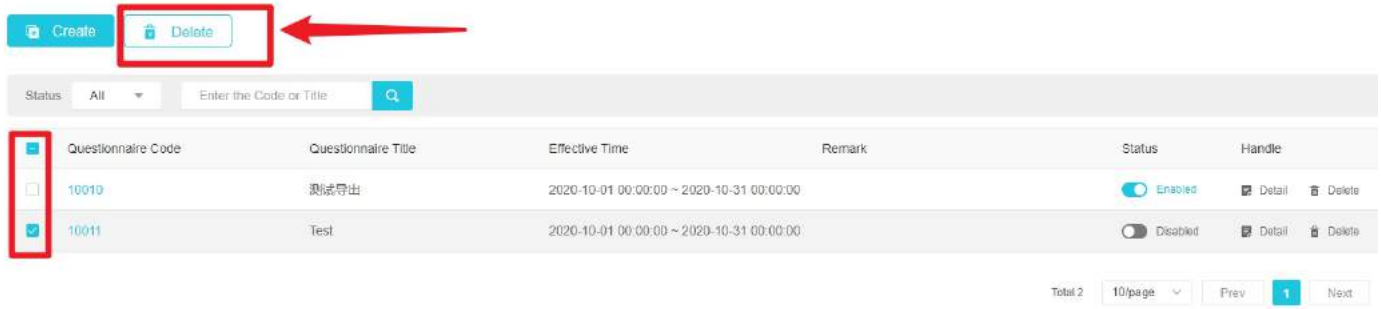
> ➢ Detail

Click the [Detail] icon in the operation bar of each column to view the question an
d option information of the questionnaire
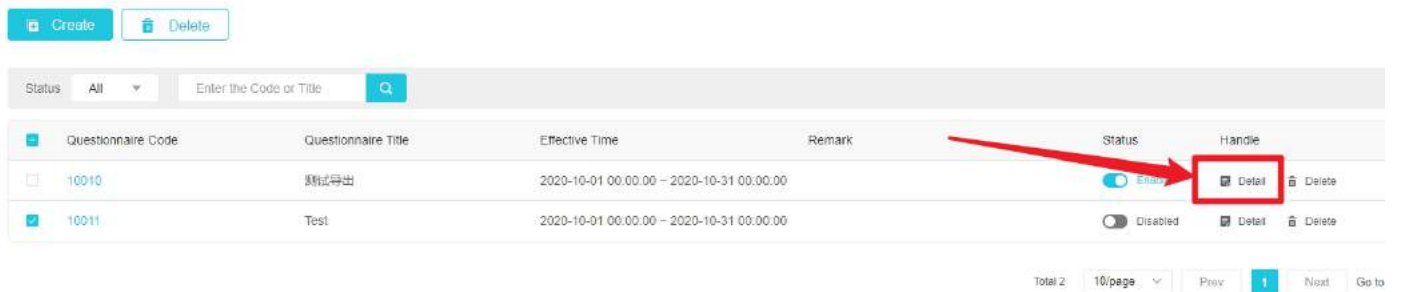
The details of the sample questionnaire are shown below:
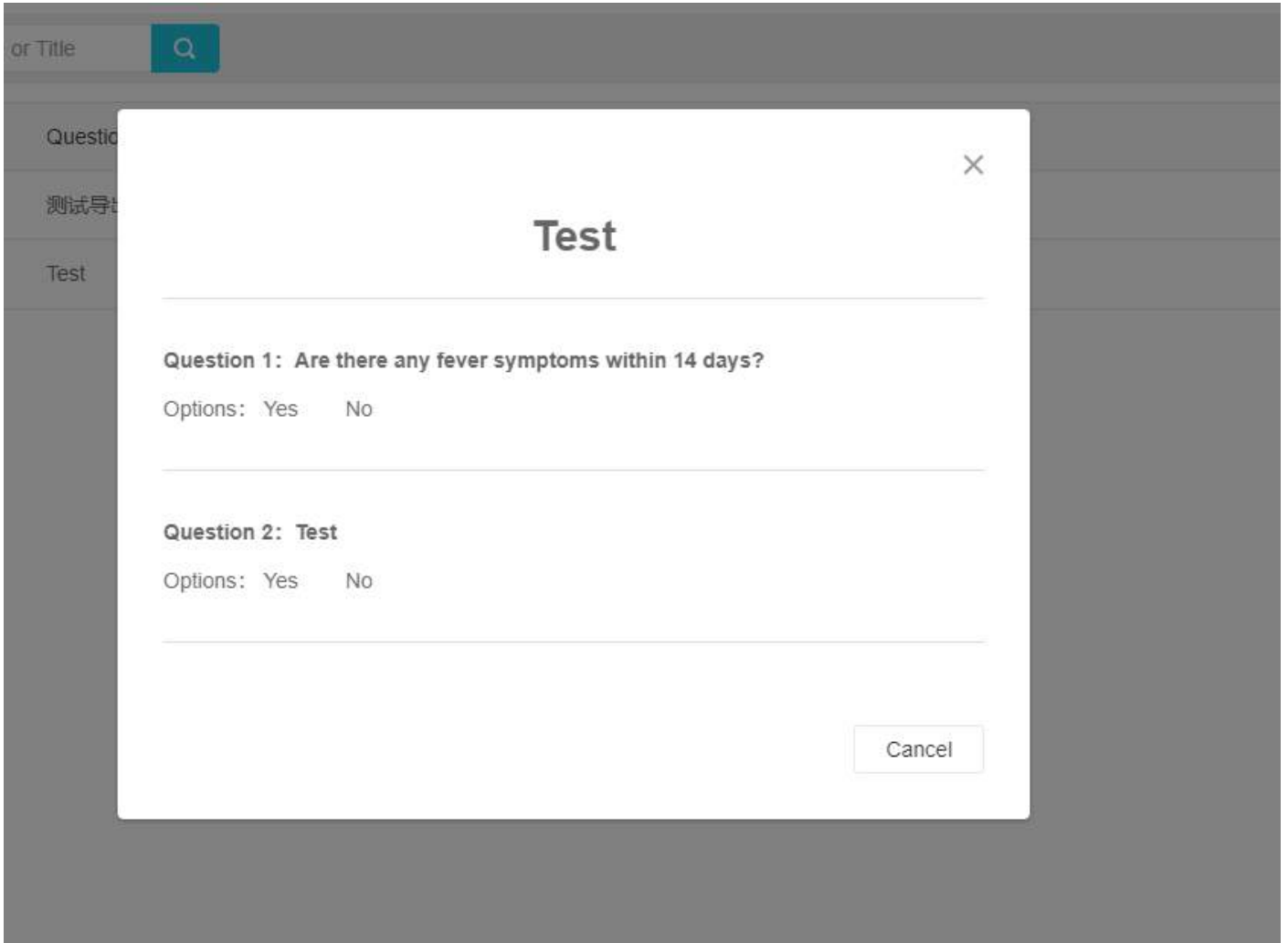
> ➢ ☐ **Authorization**

The authorization function is to authorize the questionnaire information to be use d on the device. Click in the status column of each column of questionnaire informati on on the displayed page:
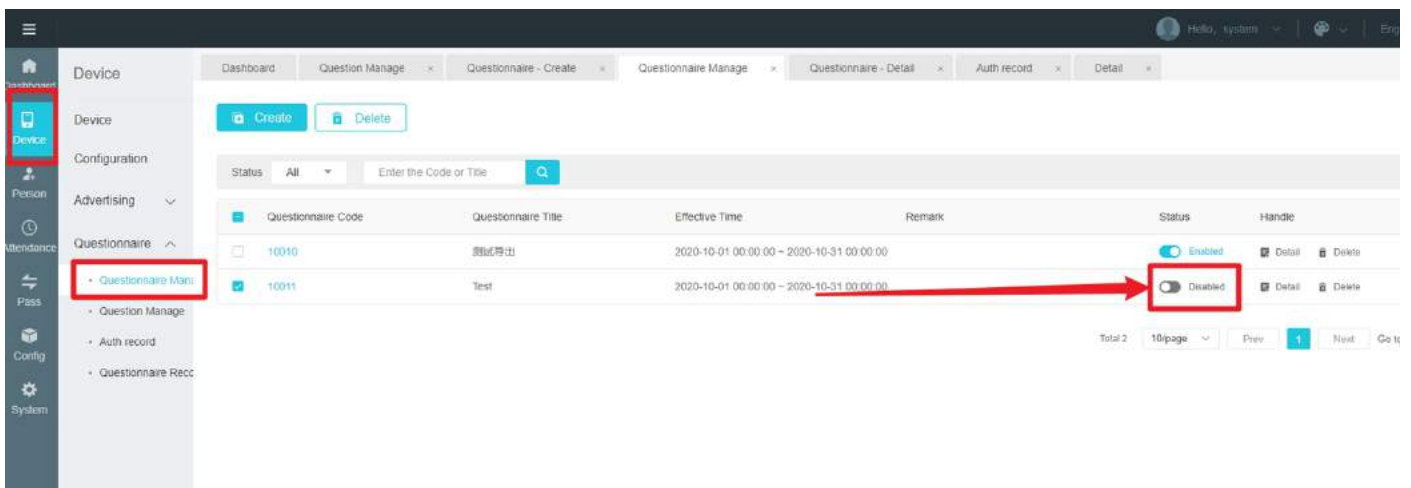
3.6.3. Question information

Create

Click the title management display page, click the [Create] button to jump to the

new page
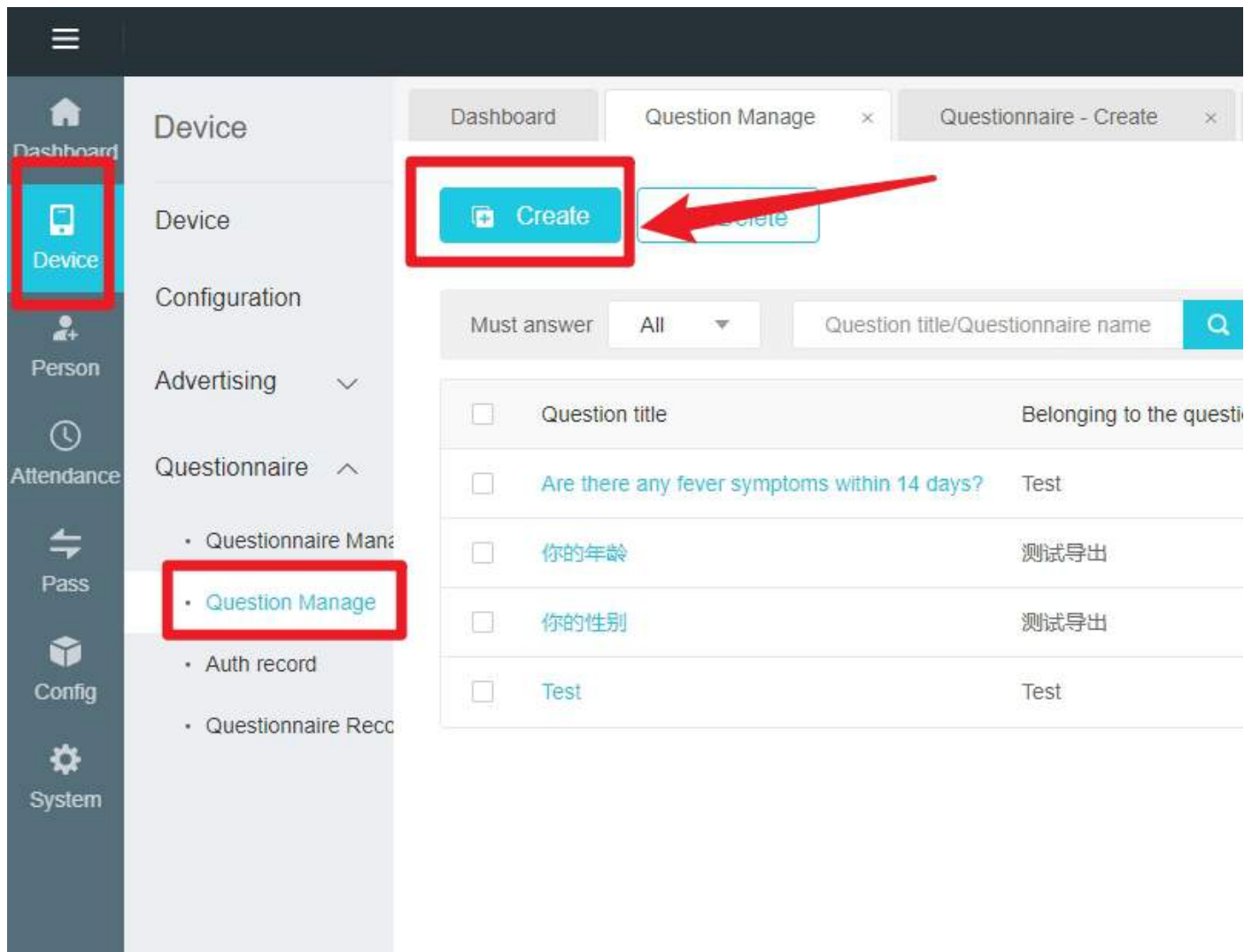
The create page is as follows:

Enter the title of the question, select the name of the questionnaire, choose whether to answer or not, click the [Add option] button, you can add different answers to the question, and set the correct answer, as shown in the figure below:

Dashboard	Question Manage ✕	**Questionnaire - Create** ✕	Questionnaire Manage ✕	Questionnaire

* Question title   Have you been in contact with a fever patient in 14 days

* Questionnaire name   Test   ▼

* Must answer   ⬤ Enabled

Single selection   **Add option**

Yes   Delete

☐ Default   ☐ Correct option

No   Delete

☐ Default   ☑ Correct option

Only one default option and the correct option can be selected for single-choice questions

Save   **Save And Continue**

3.6.4. Questionnaire synchronization

The questionnaire synchronization records the details of the questionnaire authorized to the device, as shown in the figure below:
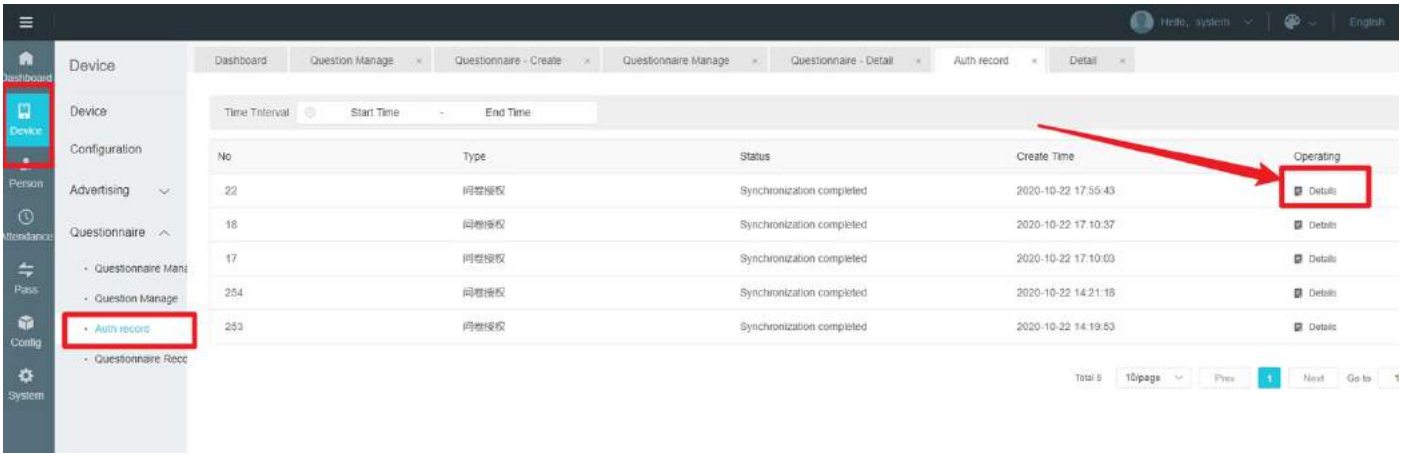
Click the details button in the action bar to view the details:
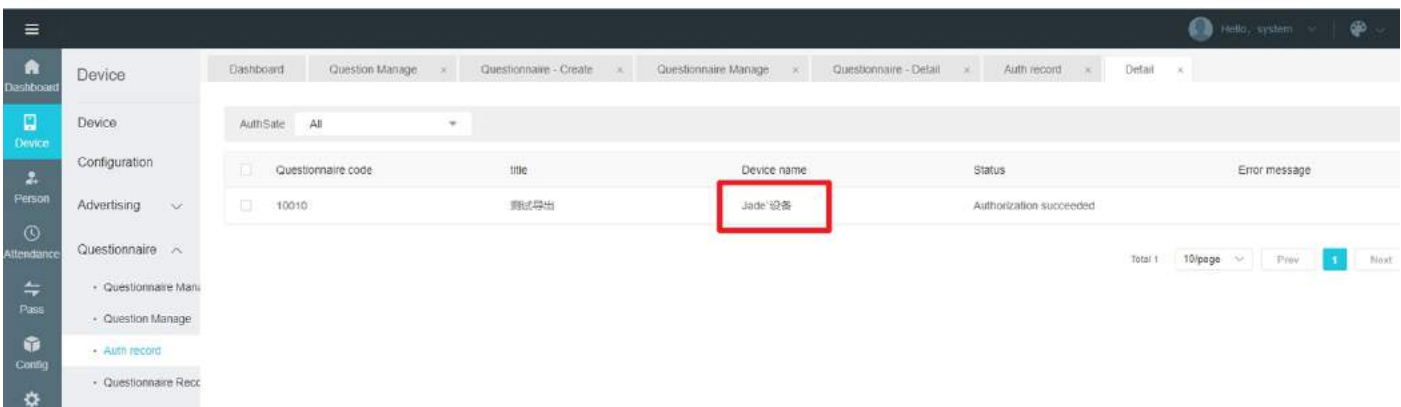
3.6.5. Questionnaire answer

The questionnaire answer records the details of the answers to the questionnaire and the status of the answers after the equipment is passed through.
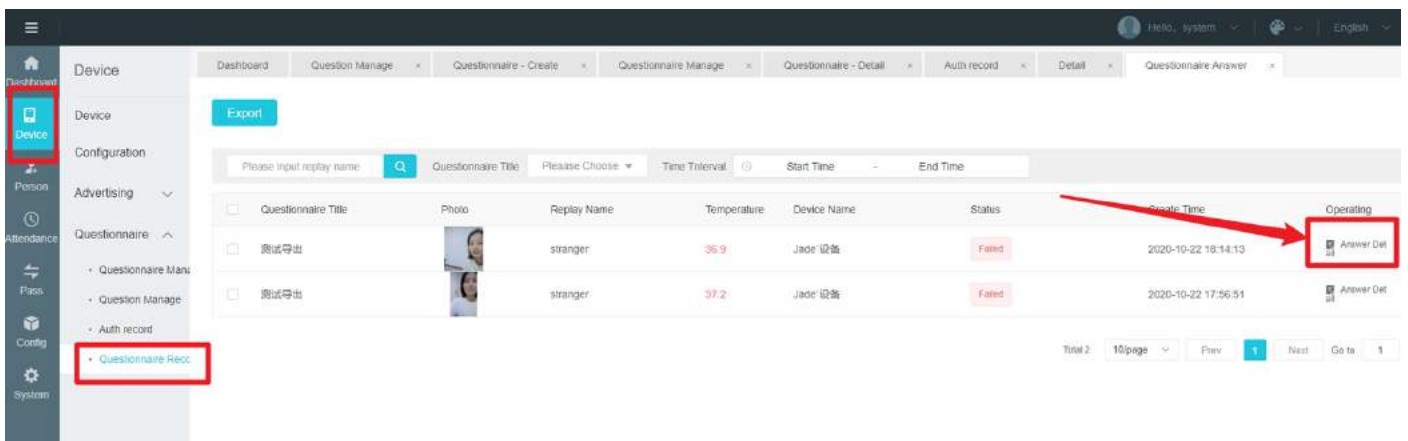
Click [Answer Details] in the operation bar to view the details of personnel's answer

s.

Click the [Export] button at the top to export records for a certain questionnaire and a

certain device.

The format of the exported excel questionnaire record is shown in the figure below:

4.Personnel management

4.1.Staff management

The employee list is used to manage employee information, such as viewing, adding, editing, and exporting employee information. Add employee information individually and batch Volume adding operation; batch adding operation requires batch information import first, and then batch portrait import.
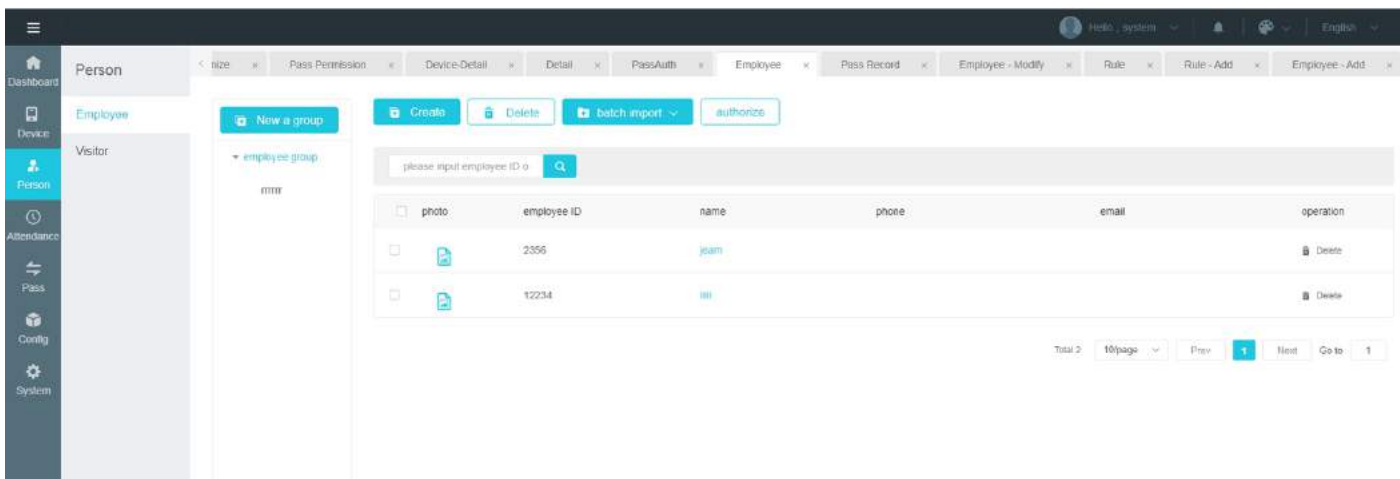

4.1.1.Add employee information individually

Steps：

1）In [Employee List], click the "New" button to enter the employee add page；

2）Fill in basic information and alarm information such as personnel ID, name, gender, group, mobile phone number, ID number, date of birth, etc., and click "Save" to complete the creation of the employee after adding a face recognition photo.Each employee can add up to three photos

Note: The alarm information here is for the personal alarm function service. After the alarm information is set here, you need to turn on the alarm switch in [System-Alarm Settings] to turn on the personal alarm function. For specific operations and instructions, please read 7.5 【Alarm Settings】
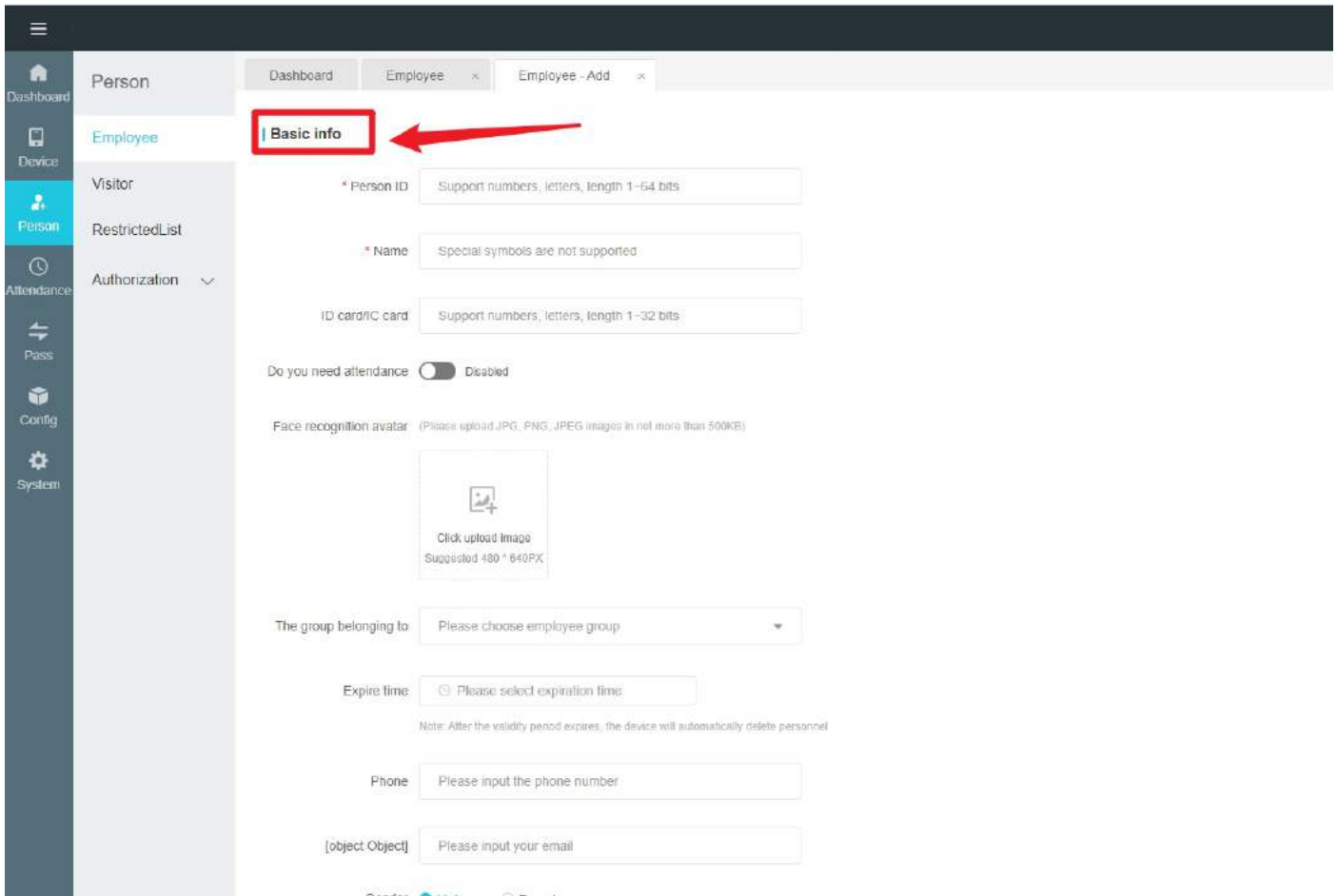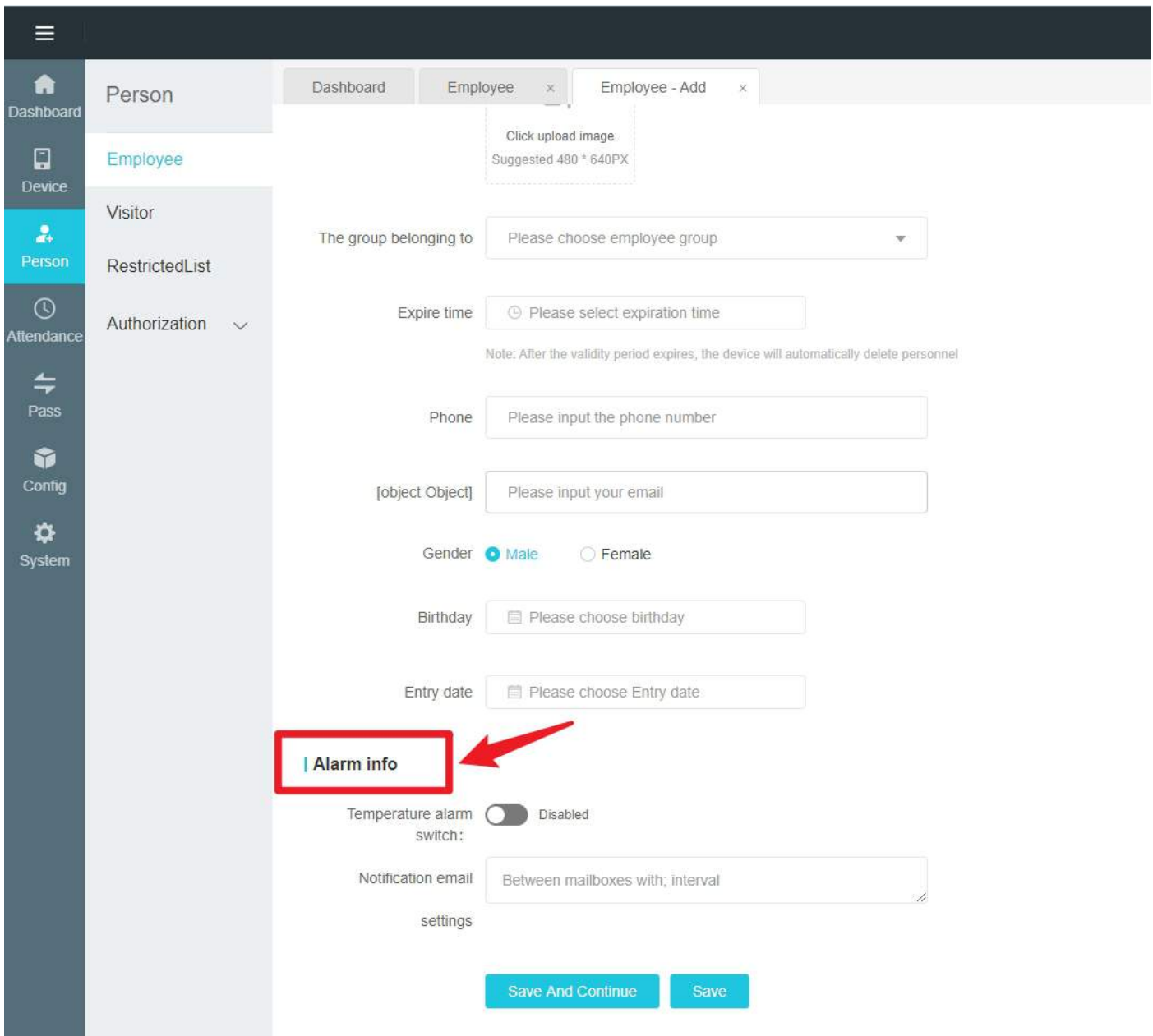
Instructions for uploading facial recognition photos :

  Upload from local

Click "Upload from Local" to open the local folder and select the jpg and png fa ce photos in the folder

  Remarks: portrait photo specifications

  1. Please choose a frontal headless photo in the past three months with a clear head and even light exposure;

2. The recommended size is 640 px * 480 px, and the size does not exceed 500k

b. Only jpg and png file formats are supported ;

3. Faces need to account for more than 1/3 of the photo to avoid blurry photos, wearing sunglasses, excessive beauty, and rotation of the avatar;
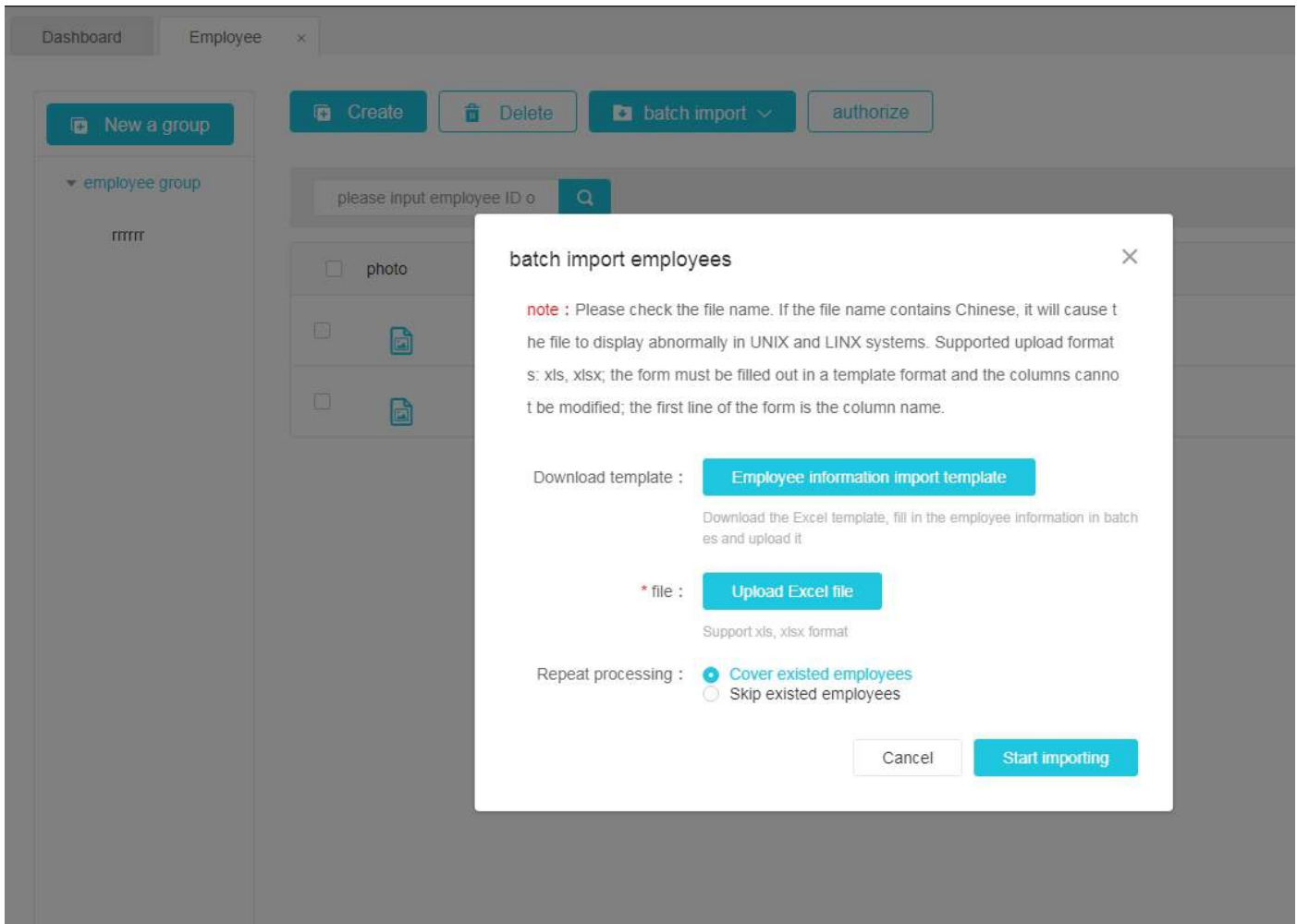
4.1.2.batch Import employee information

Operation steps:

In [Employee List], click the "Batch Import-Employee Information" button to enter the bulk information import pop-up window

1）The first step is to click "Download Template" to download the excel template file to the computer, the file name is "Personnel_import_template.xls",Then fill in empl oyee information in batches;

Note: The format for entry date and birthday is such as: 2019/6/6, 2019/12/21

2）In the second step, click "Upload Excel file", select the excel file that has filled in the employee information, and upload the file.Shows the status of successful upload, and displays the file name;

3）The third step is to click "Start Import". After the import is completed, it will promp "Successfully import personnel information in batches"; after the import is completed, return to [Personnel List] to view the imported personnel information.

How to start import

● Overwrite existing employees: Import the file twice or more, and the duplicate employee information will be overwritten

● Skip existing employees: duplicate employees, the employee information imported for the second time will be skipped

Import failure exception description

● The content or format of the uploaded excel file is wrong and does not meet the template specifications. Click to start importing, and it will directly prompt "File upload error"

4.1.3. Import portraits in batches

Operation steps: In [Employee List], click the "Batch Import-Photo Information" button to enter the batch import portrait pop-up window

In the first step, click "Select File Compressed Package" to open the window for selecting a folder and select the file to upload;

The second step, click "Start Import"。
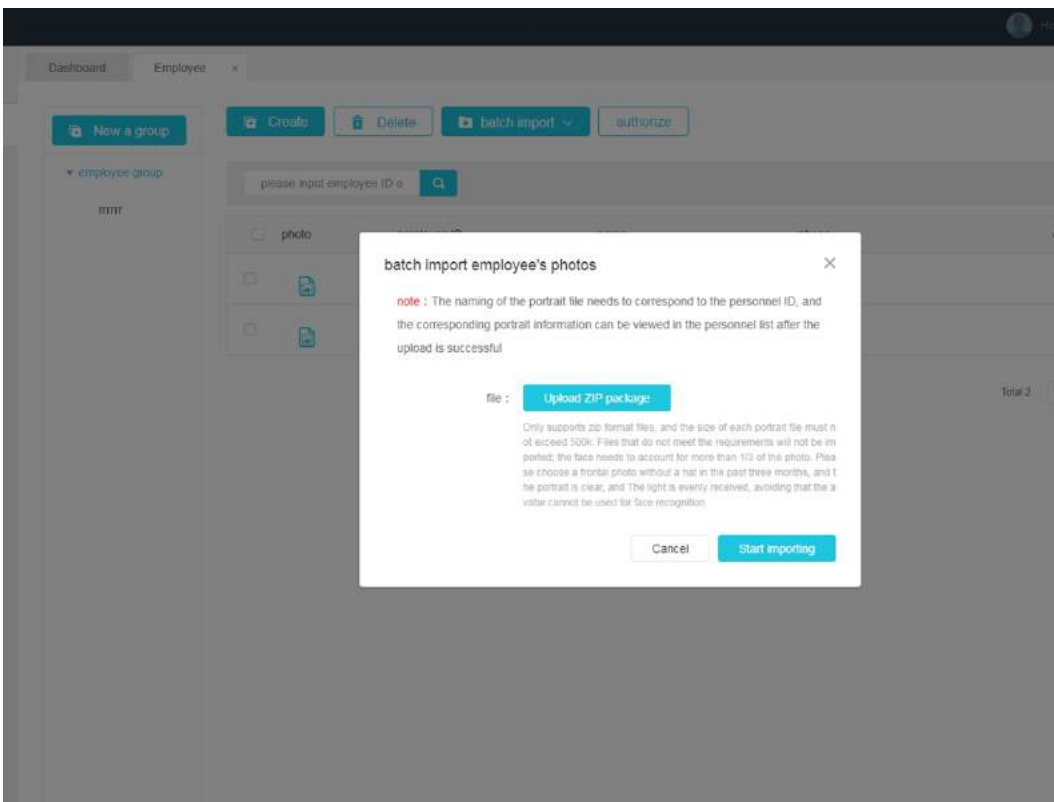
Description of portrait import rules:

● [Portrait file naming] The name of the portrait file needs to correspond to the personnel ID, and the corresponding portrait information can be viewed in the personnel list after the upload is successful;

● [Format size limit] Only two file formats, jpg and png, are supported, and the file size of each portrait must not exceed 500k. Files that do not meet the requirements will be Not imported

● [Portrait Limitation] The face needs to occupy more than 1/3 of the photo. Please choose a frontal photo without a hat for the past three months. The portrait is clear and the light is evenly received, so that the portrait cannot be used

Face recognition

● [Select folder to upload] After satisfying the above conditions, put the named portrait photo in the designated folder, and select the folder to import;

Description of portrait import failure

● The file size of a picture does not meet the requirements, after modification, it can be re-imported

4.1.4.take photo

Select the photo button on the right side of the [Employee Management] list, select the online device in the Bullet frame, and click Process to take a photo on the device. After a few seconds, refresh the page to display the employee photo.
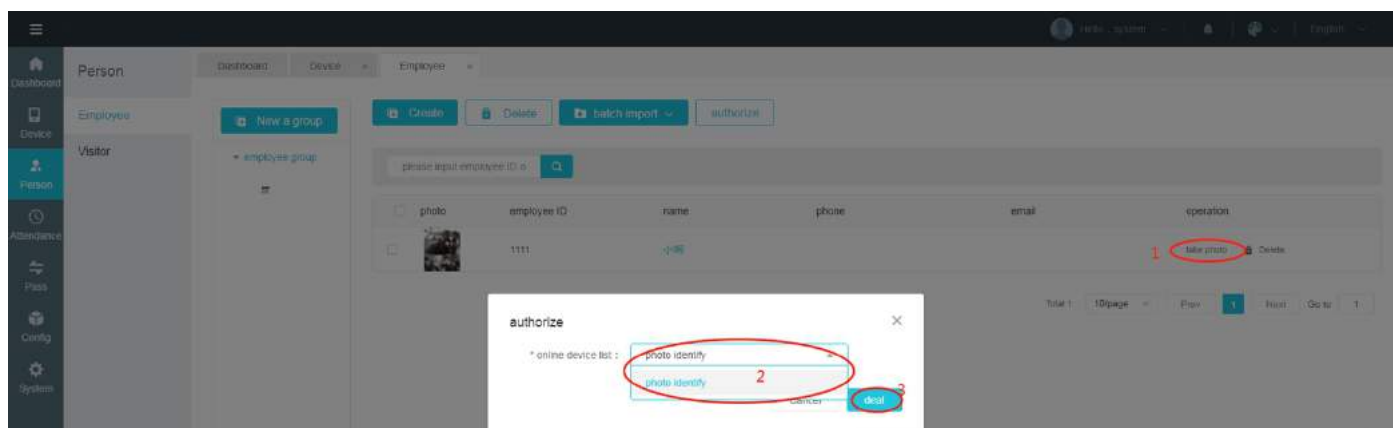
4.1.5.Refresh employee information

Right-click in [Employee Management] and click the "Refresh" button to refresh al
l employee information in the list to the latest state.

4.1.6. View employees and editors

● View employees

You can click View in the operation bar at the end of the employee list to view

employee details, employee track, employee QR code, etc
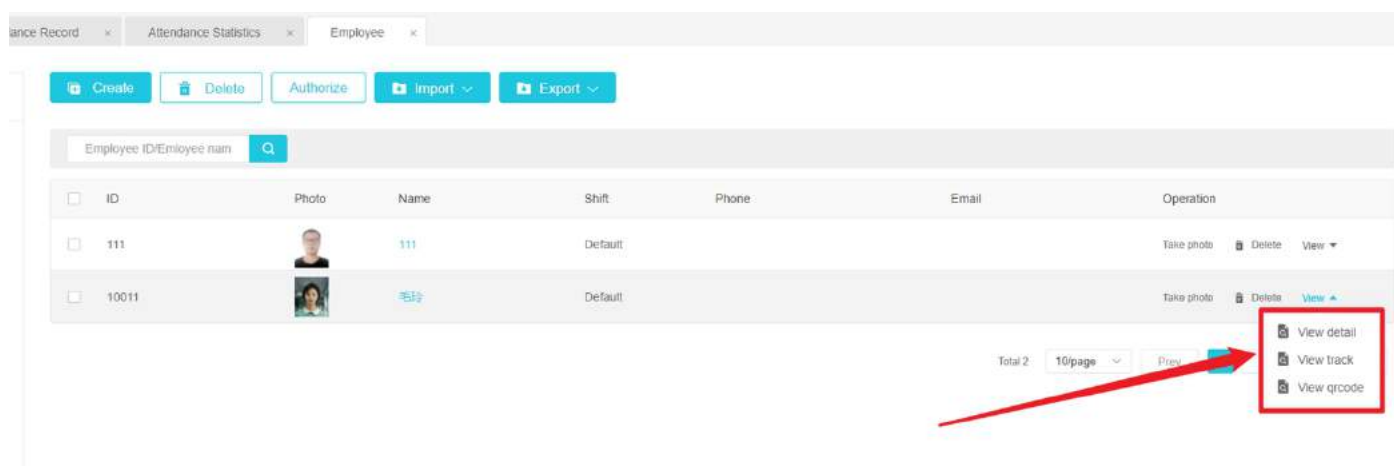
➢ View details ,click to view details
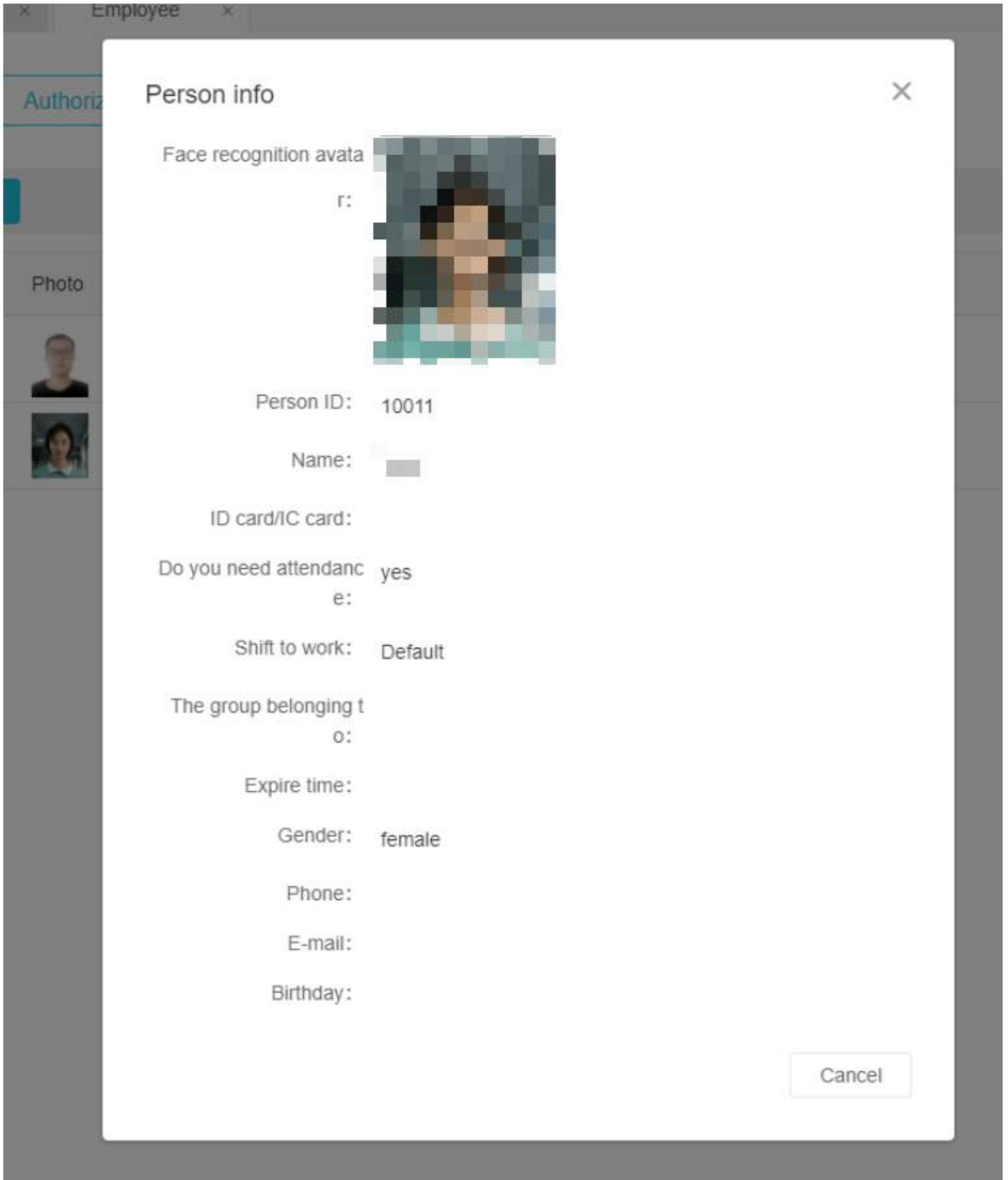
> ➢ View the track to view the corresponding traffic record of the employee

> View the QR code. When a new employee is created, the corresponding QR code is generated. Click View QR code to view the QR code information of the employee
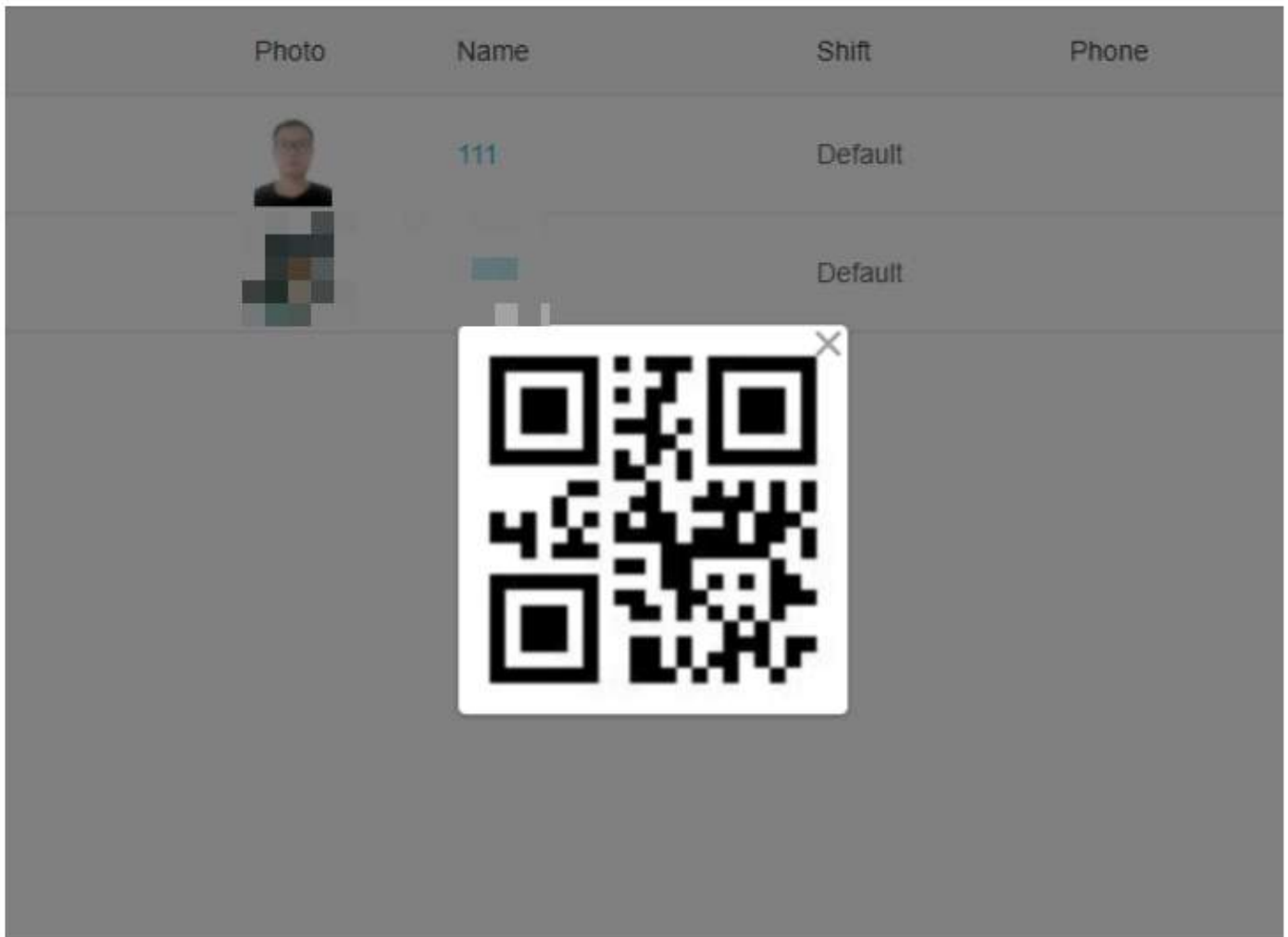
● **Staff editor**

On the details page, edit the content to be modified. You can modify the basic information and photo information of the employee. After modifying the information, click Save.

4.1.7.Delete employees individually and in batches

● **Single delete**

In [Employee List], after corresponding employee information, click the "Delete" button on the right to delete the employee.

●**batch deletion**

In [Employee List], select the employee information to be deleted in batches, and click the "Delete" button next to "New" to delete these employees in batches.

Note: When an employee is deleted, the authorization of all devices of that person will be cancelled accordingly

## 4.1.8.Employee group management

● **New group**

On the left side of [Employee List], first click to select the group name that needs to add a subgroup, then click Add Group, fill in the group name, and click OK to create a new group

● **Add, rename and delete groups**

Find the group name to be modified on the left side of [Employee List], right-click, and select one of the new, rename and delete functions according to your needs to operate
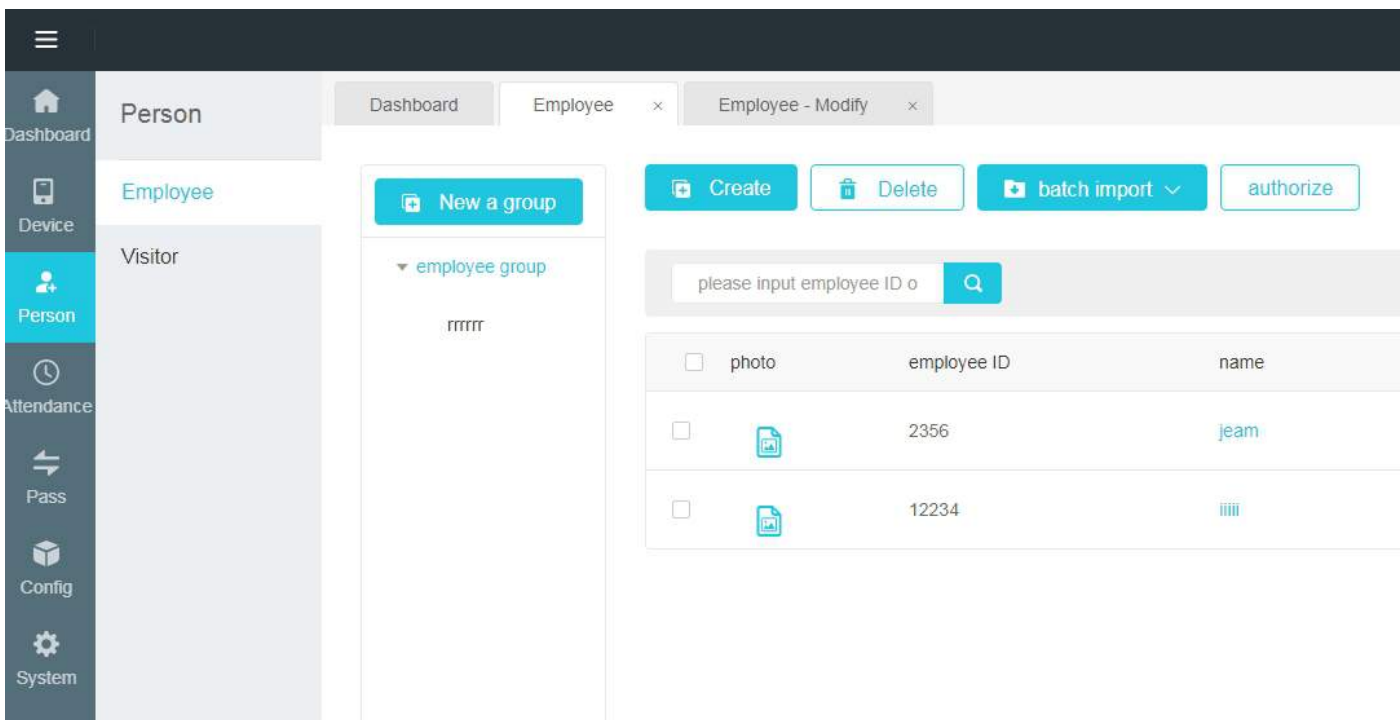
Select personnel and click the Batch Group button to open the Batch Group page to select a group, and you can modify the personnel group in batches.
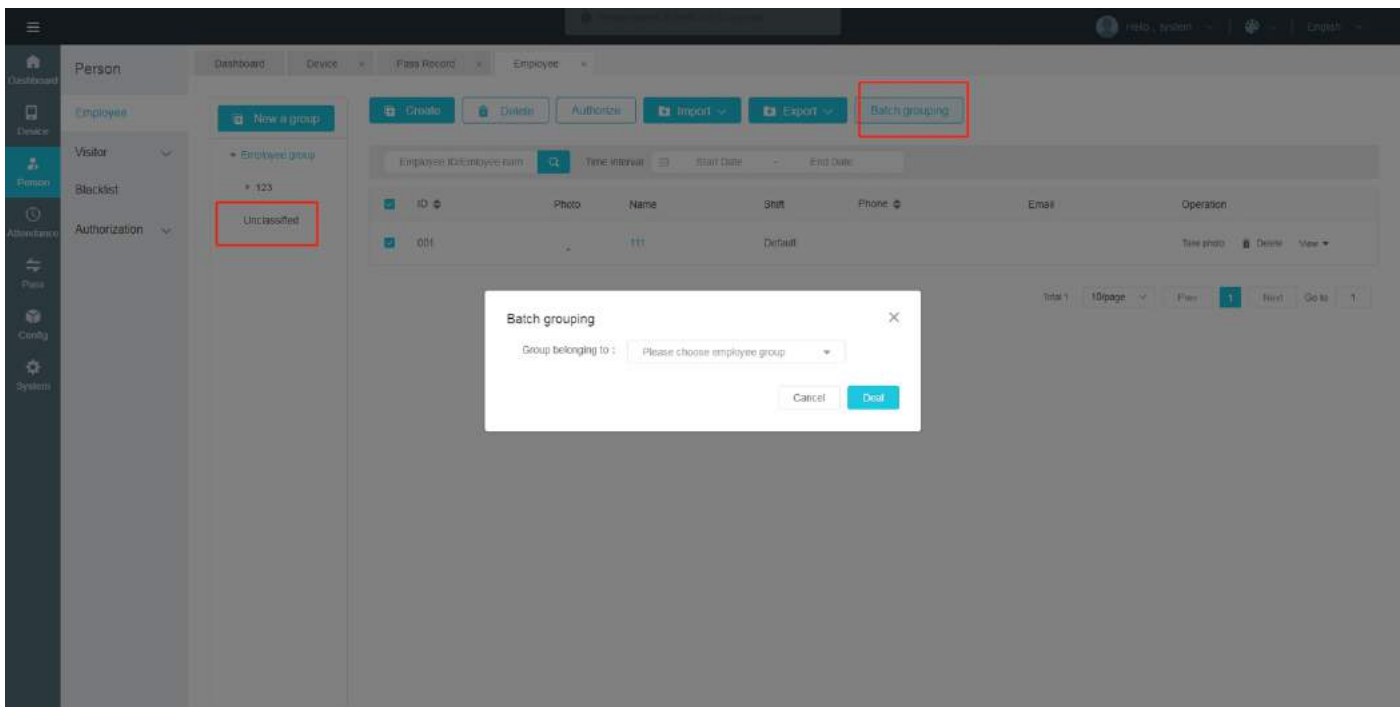
4.1.9.Employee authorization

Steps :

The first step, after selecting the employees who need to be authorized, click the authorization button ;

The second step, is to select the authorization type in the pop-up window.

The third step is to select the devices that need to be authorized (multiple choices are available)

The fourth step, select the type of transit time, (choose to obtain from the personnel information will be configured according to the transit time in the personnel details)

The fifth step, select the time period for the employee to pass (multiple time periods can be selected, up to three) , If you don't fill it, you can pass

The sixth step at any time period of the day by default, and click Process.
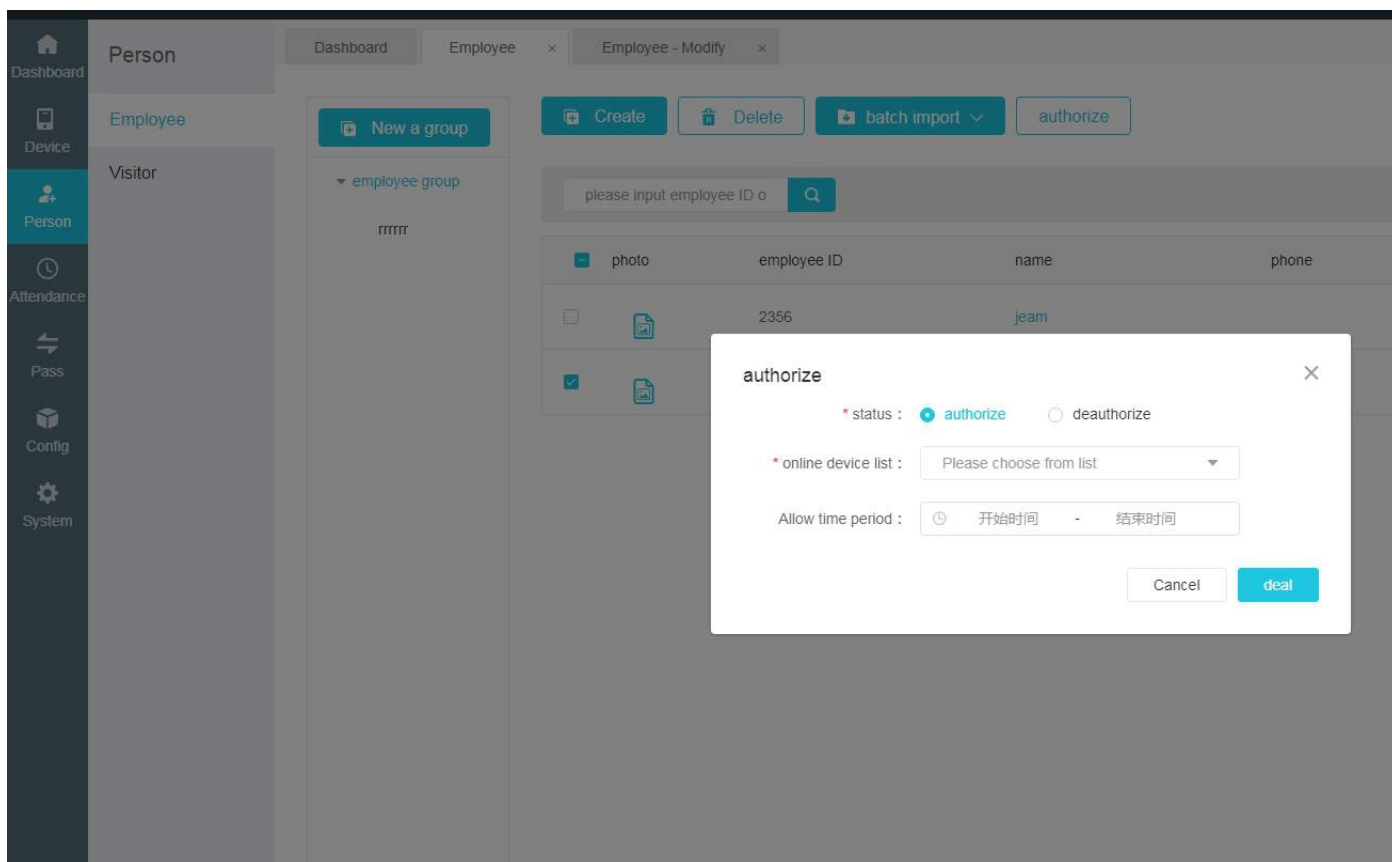

The sixth step, you can view the information of the successfully authorized personnel in the [Auth Record] of the general [Authorization] , or click the device name on the left to view the authorization information of all personnel on the device.
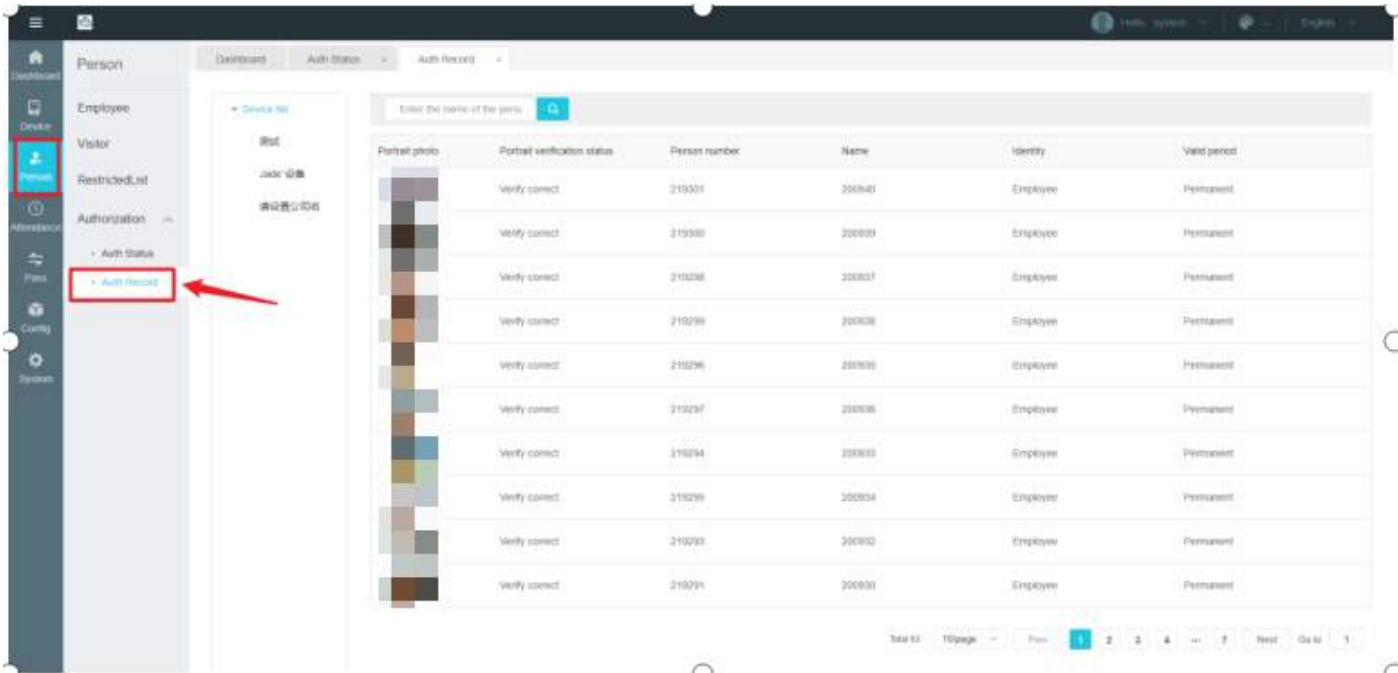
The seventh step, you can check whether the authorization is successful in the [Auth Status] of [Authorization].

Note: If an unregistered photo of a person is created on the device (mainly for drawing cartoons) and both a person created and a registered photo will be displayed
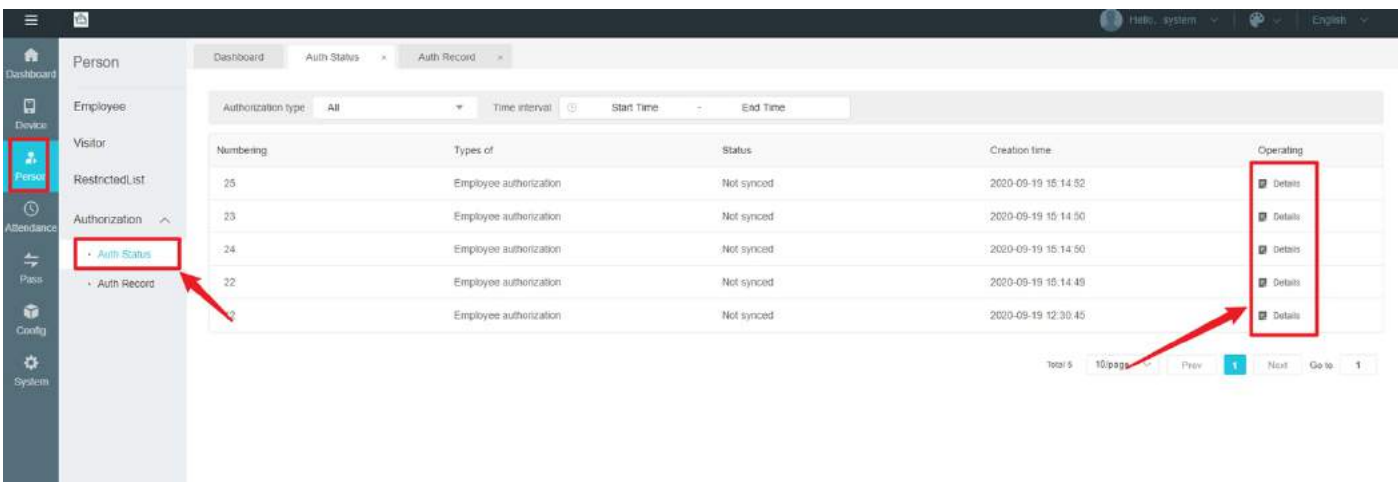
The eighth step, if the status shows that it is not synchronized at this time, you can click the details on the right to view the reason for the failure of an employee's authorization.

Note: You need to make corresponding changes based on the error message for the retry button to work

4.1.10.Employee information export

Click [Employee Staff] on the page to export all staff information on the current

page as excel files



The exported excel format is:

# 4.1.11 Batch grouping

Batch edit selected groups of people
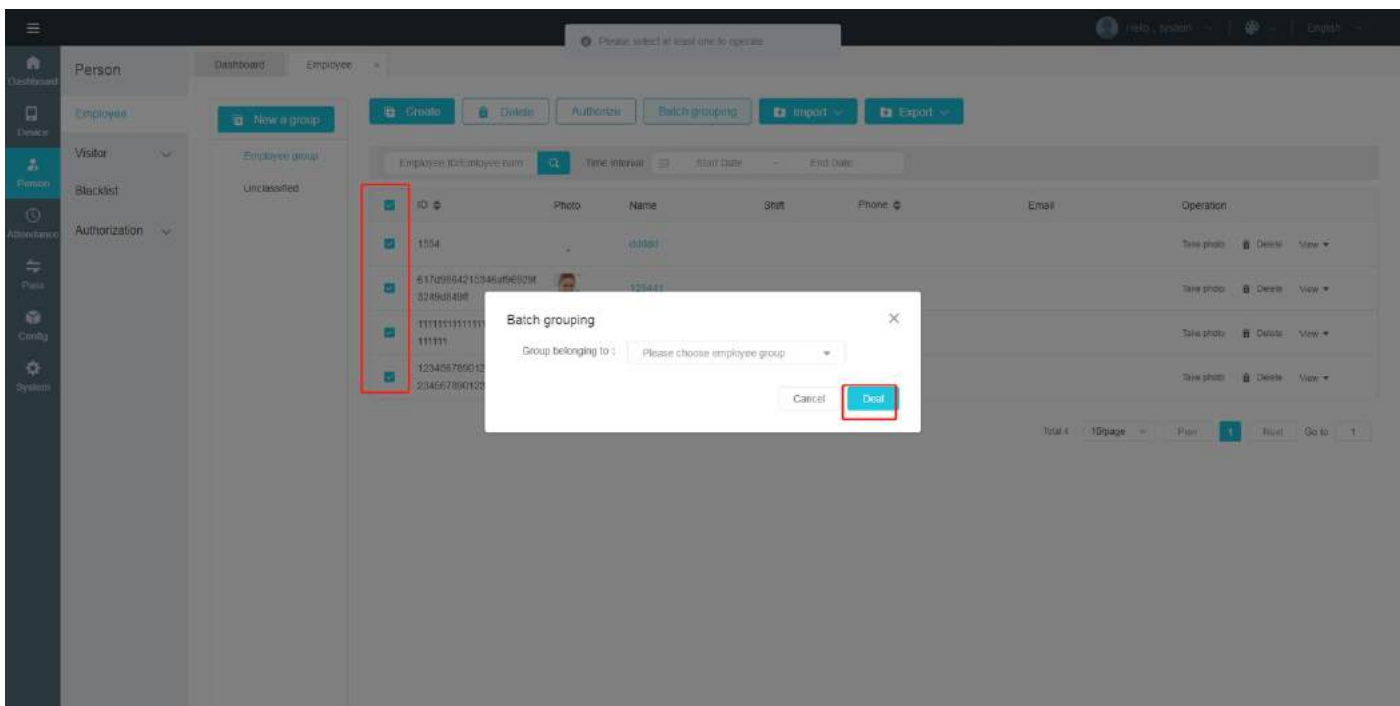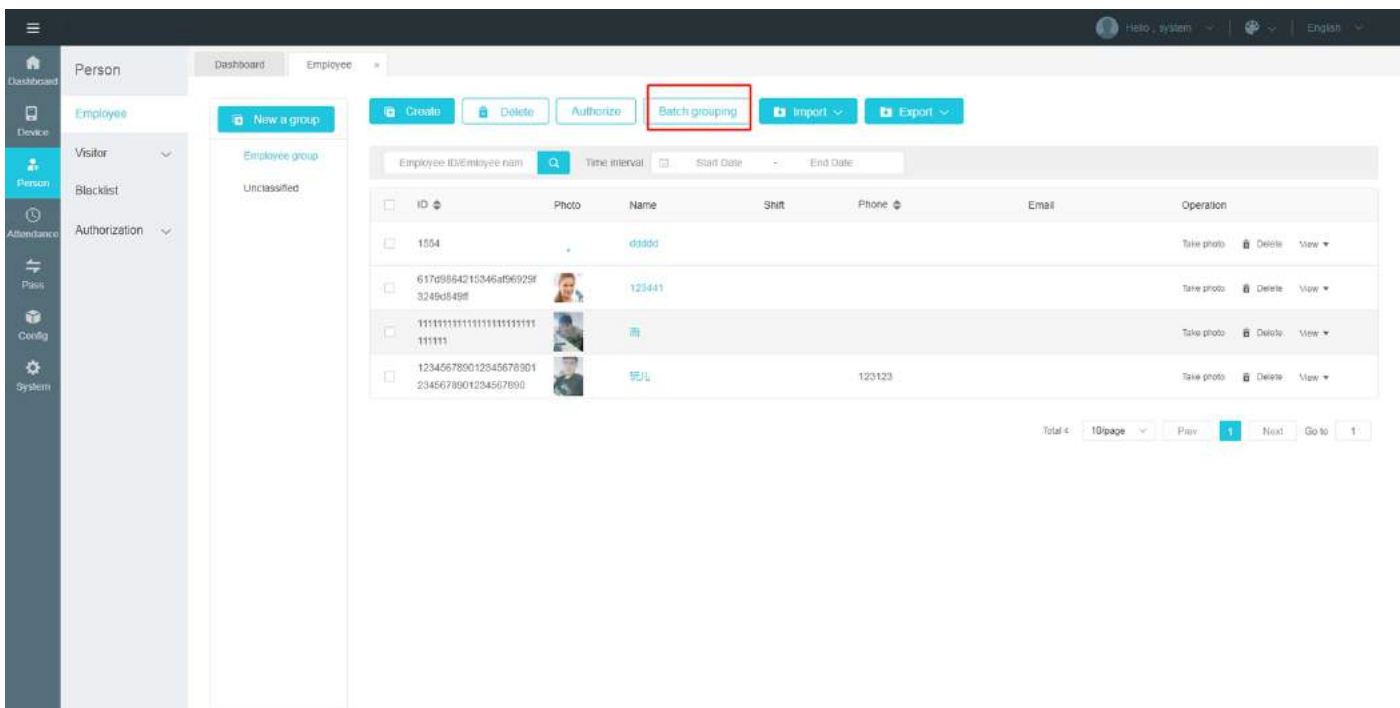
4.1.12．Move to the blacklist

On the employee list display page, you can set employees to blacklist users allowed, but messages are sent to the receive mailbox。**Note: After moving to the blacklist, all the relevant attendance records of the current staff will be cleared**.

Move to the blacklist user steps are listed below :
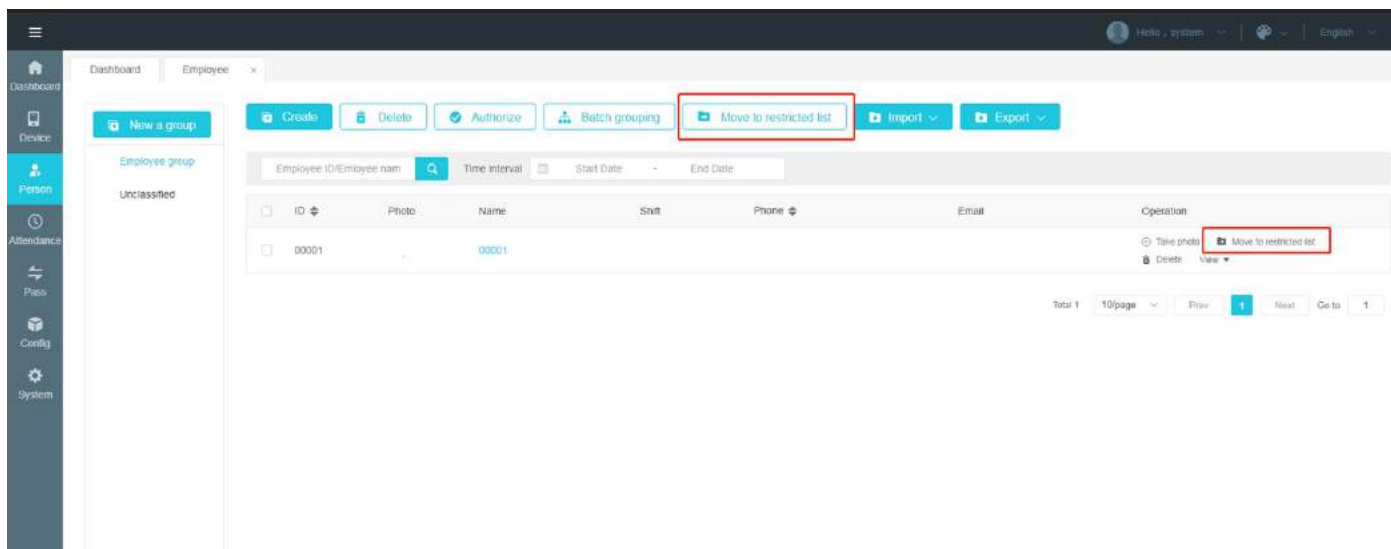
Single move to the blacklist: Click the [Move to the blacklist] of each employee, and click the confirmation in the pop-up prompt box to move the employee to the blacklist
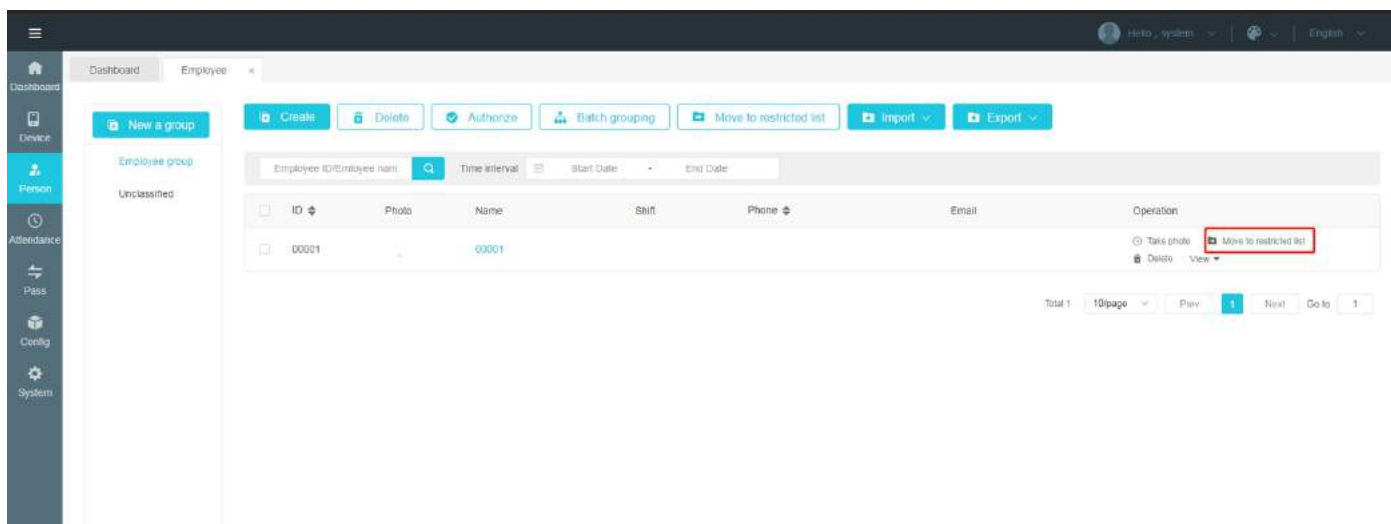
Batch move to the blacklist: select multiple employees, and then click [Move to the blacklist] at the top of the display list to move the selected employees to the blacklist in batch
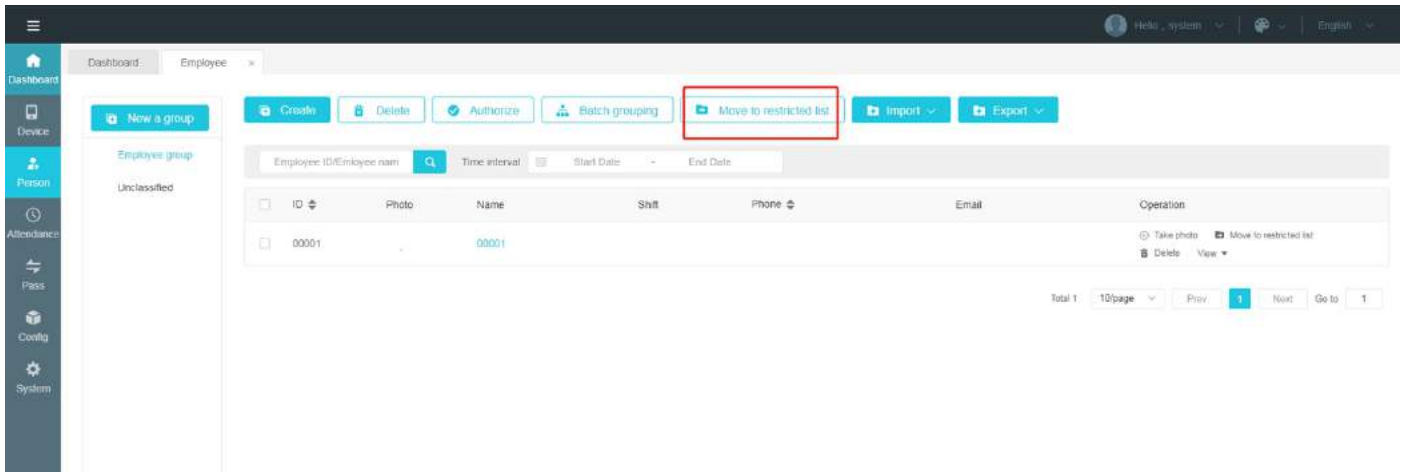
4.2.Visitor management

The visitor list is used to manage employee information, such as viewing, adding, editing, and deleting visitor information.

4.2.1.Add visitor information individually

Steps:

1) In [Visitor List], click the "New" button to enter the guest add page;

2) Fill in the person ID, name, gender, belonging group, mobile phone number, ID number, etc., add the face recognition photo and click "Save" to complete the creatio n of the visitor.

Instructions for uploading facial recognition photos

Upload from local

Click "Upload from Local" to open the local folder and select the jpg and png face photos in the folder

Remarks: portrait photo specifications

1. Please choose a frontal headless photo in the past three months with a clear head and even light exposure;

2. The recommended size is 640 px * 480 px, and the size does not exceed 500kb. Only jpg and png file formats are supported ;

3. Faces need to account for more than 1/3 of the photo to avoid blurry photos, wearing sunglasses, excessive beauty, and rotation of the avatar;

4.2.2.Refresh visitor information

Right-click in [Visit Management] and click the "Refresh" button to refresh all visit or information in the list to the latest state.

4.2.3.Visitor details and editing

●**Visitor details**

In [Visitor List], find the visitor you want to view and click the name to enter the details page to view specific visitor information.

● **Guest edit**

On the details page, edit the content to be modified. You can modify the basic i nformation and photo information of the visitor. After modifying the information, clic k Save

4.2.4.Delete visitors individually and in batches

● **Single delete**

In [Visitor List], after corresponding visitor information, click the "Delete" button o

n the right to delete the visitor.

● **batch delete**

In [Visitor List], select the visitor information to be deleted in batches, and click the "Delete" button next to "New" to delete these visitors in batches.

Note: When the visitor is deleted, the authorization of all devices of the person will be cancelled accordingly

4.2.5.Visitor authorization

It is basically the same as the steps for employees to collect, please refer to 4.1.9 [Employee Authorization]

4.2.6 . Move to blacklist

On the visitor list display page, visitors can be set to a blacklist. Blacklisted users are allowed to pass, but emails will be sent to the receiving mailbox. The steps to move to blacklist users are as follows :
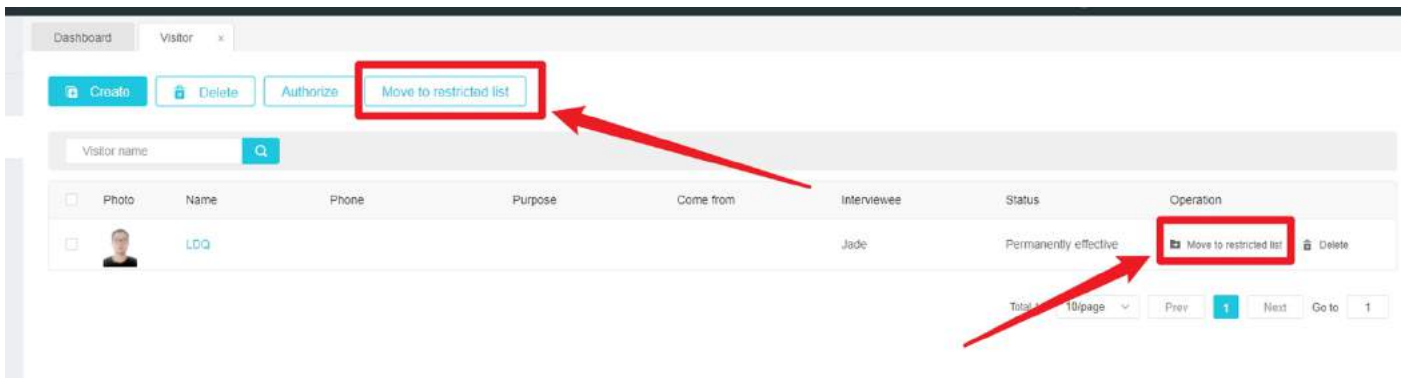
Move to the blacklist individually: Click [Move to Blacklist] in the operation bar of each visitor, and click OK in the pop-up prompt box to move the visitor to the blacklist

Move to the blacklist in batches: Select multiple visitors and click [Move to Blacklist] at the top of the display list to move the selected visitors to the blacklist in batches.

4.2.7. Visitor QR Code

The purpose of the visitor's QR code is: the host adds a visitor to the system and authorizes it to the device, uses a QR code generator to generate a QR code from a link, and then provides the QR code to the visitor, and the visitor scans the code to fill in the ID After verifying the visitor's information, the visitor's exclusive QR code is generated, and the visitor can pass through this exclusive QR code on the device.

> ➢ ⬜ Step 1: Add visitors and authorize them to the device. For how to add visitors, please read 4.2.1 Adding Visitor Information and 4.2.5 Visitor Authorization

> ➢ ⬜ Step 2: Use a QR code generator to generate a QR code with the link. (The QR code generator can be searched on Google or Baidu, no tools are provided here), this link is:

IP/domain name: port+"/qrcode/IdentifyCheck.html ? lang="+language (ch, es, en, ko) ,

Here IP/domain name: port is the IP/domain name: port displayed by the system

browser address at this time,

lang is the language, ch is Chinese, es is Spanish, en is English, ko is Korean,

For example, link 192.168.1.28:9000/qrcode/IdentifyCheck.html？ lang=ch, use this link to generate a QR code with a QR code generator. (The QR code generator can be se arched on Google or Baidu, no tools are provided here)

> ⬜ Send this QR code to the visitor, and the visitor will scan the QR code and enter the ID verification information. If they are consistent, an exclusive QR co de will be generated. The visitor can use the QR code to pass (the visitor's mobile phone and server require In a local area network).

Note: If the LAN version is used, the guest mobile phone needs to be in the sa me LAN as the computer, and there is no restriction on the cloud.

4.2.8 . Batch import of visitor information

Operation steps: in [visitor List], click "Import-> Batch Import Visitors" button to enter the batch information import pop-up

1） The first step, click "Visitor Template" to download the excel template file to the computer with the file name " Visitor Template. xls", then batch in visitor information;

Note: Date format is like：2019/6/6,2019/12/21

2） In the second step, click "Upload Excel file", select the excel file that has filled in the employee information, the file uploaded successfully, display the successful upload status, and display the name of the file；

3） In the third step, click "Start Import", prompt after import completion "to

successfully import the personnel information"; after completing the import, return to

[Personnel List] to view the imported personnel information.
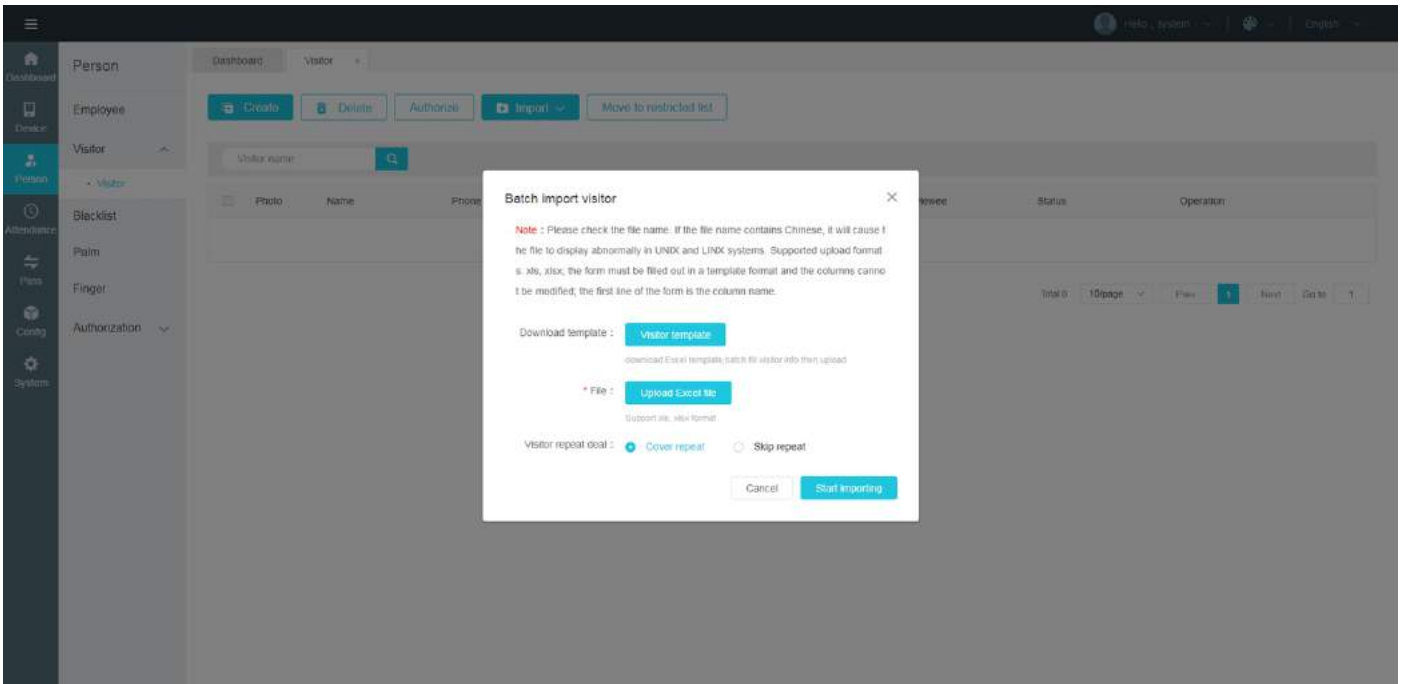
Description of how the import begins

● Overcover existing visitors: import files, duplicate employee information will be

blocked

● Skip Existing visitor: Repeat employee, second imported employee information will

be skipped

Import failed exception description

● The uploaded excel file content or format does not meet the template specification.

Click to start import and directly prompt "Upload file error"

4.2.9 . Batch import of photo information

Operation steps: In [visitor List], click the "Batch Import-Photo Information" button to

enter the batch import photo pop-up

The first step, click "Upload ZIP Package", open the selection folder window, select the

file upload;

The second step, click on Start Import.
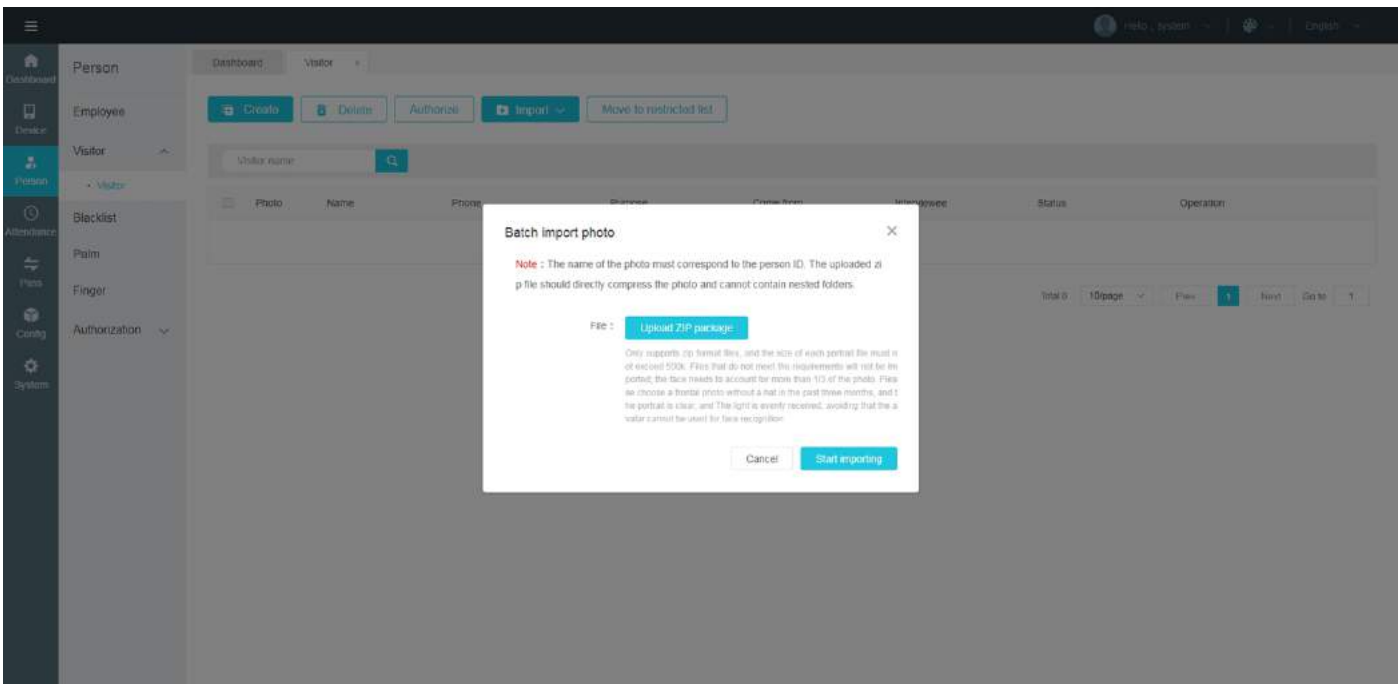
Portrait import rules description:
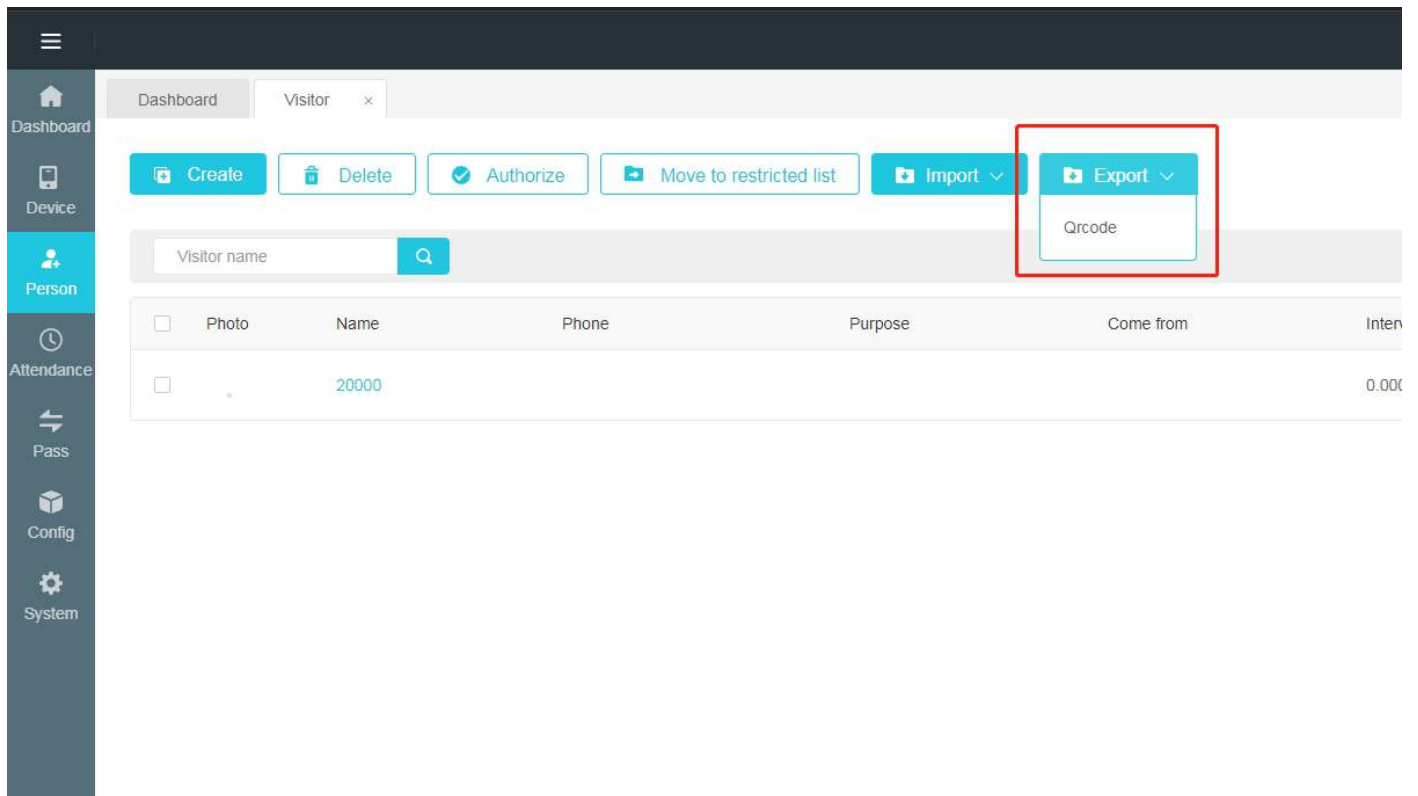
● [Portrait file naming] The naming of the portrait file needs to correspond to the visitor number. After uploading successfully, you can view the corresponding personnel portrait information in the personnel list ;

●[Format Size Limit] Only jpg and png file formats are supported and files with each portrait file size must not exceed 500k, will not be imported ;

●[Portrait Limit] The face should account for more than 1 / 3 of the photos. Please choose the front bareheaded photo in the past three months, with a clear head and uniform light, to avoid the head picture can not be used for face recognition ;

●[Select Folder to upload] After meeting the above conditions, put the named portrait photos in the specified folder, and select the folder for import;

Portrait import failure description

● A picture file size does not meet the requirements, after modified, can be reimported

4.2.10 Visitors' QR code export

Export the QR code generated by the visitor ID, which can be used to scan the code

for identification.

4.3.Blacklist

When creating a new blacklist, you need to select the type of access (no access,

access warning). After setting to prohibit access, the blacklist will not be allowed to p

ass. After setting the access warning, the blacklisted person will be allowed to pass b ut will send a warning email to the recipient. mailbox. Create as shown in the figure below:

After creating a new blacklist user, you need to authorize to the device. If the ac cess type is [Access Warning], you need to set the sending and receiving email addre sses of the alarm. Please read the following for the specific operation steps.

In System->Alarm Settings, after turning on the blacklist alarm switch, the system will automatically send emails to the recipient mailbox for the blacklisted personnel. Note: You need to turn on the mail service settings first, please refer to [7.6 Mail Service Settings]
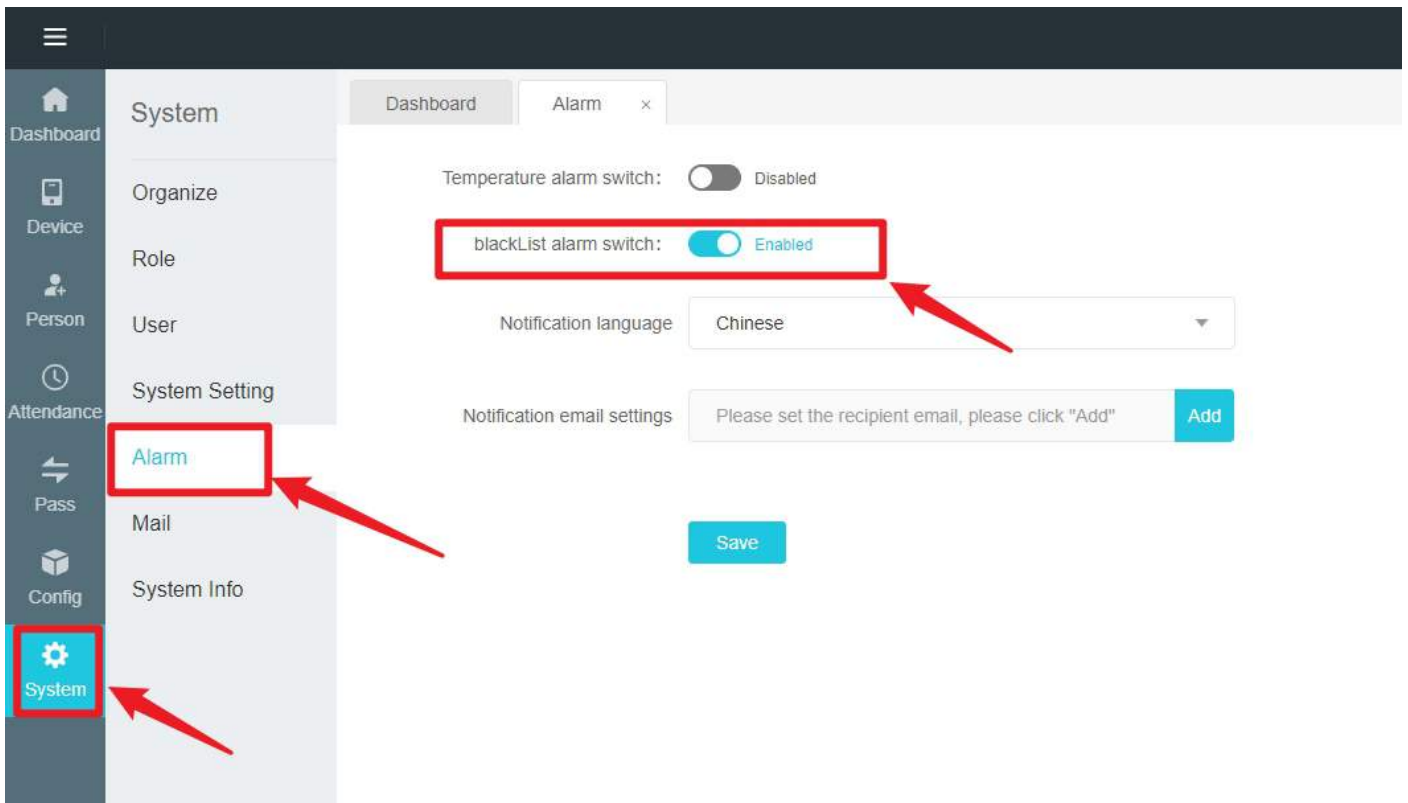
4.4. Palmprint management

Palmprint management is used to manage the palmprint information of employees and visitors. You can view the palmprint input, collect, distribute, and clear the palmprint of employees. （Support for palmprint versions above v1.41.6.4）

4.4.1. Palmprint list

Click personnel > palmprint management to display the palmprint list page to view the palmprint entry of employees and visitors
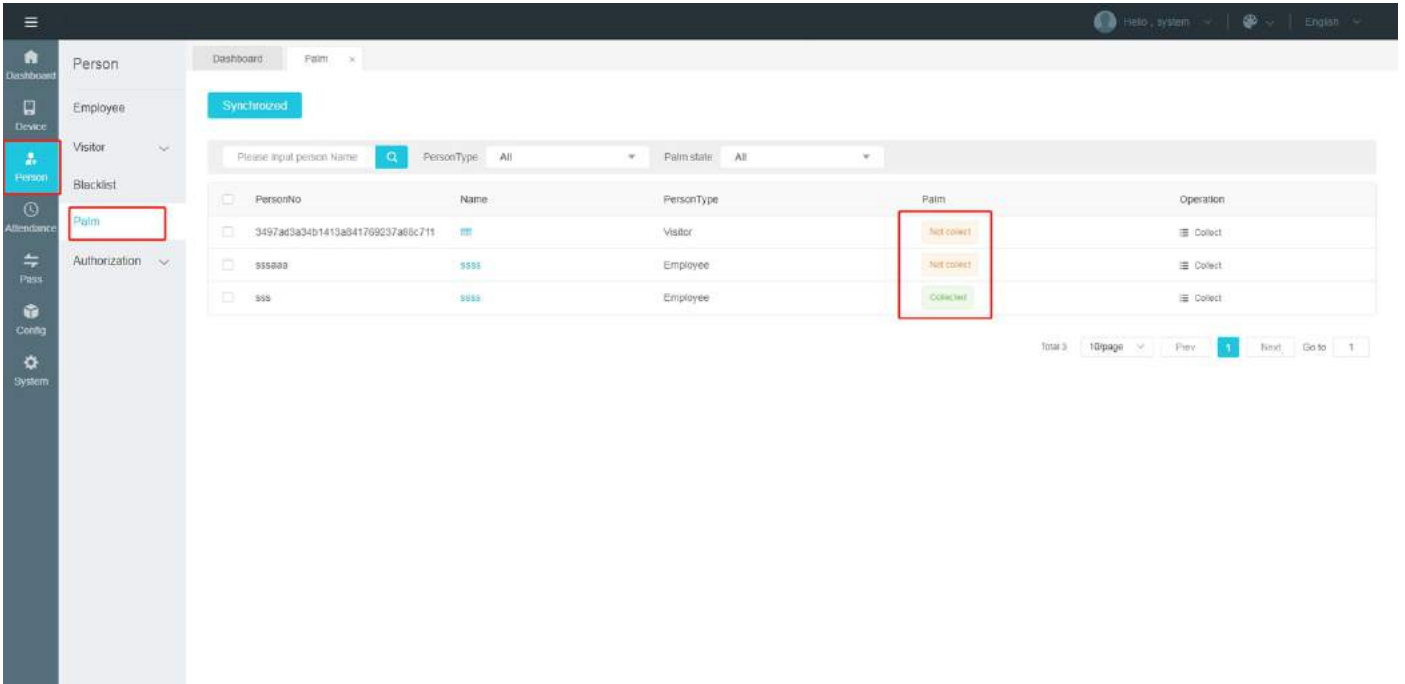
4.4.2. Palmprint collection

Click the operation type acquisition button in the palmprint list, pop up the palmprint collection page, select online equipment, click the processing button to collect palmprint on the device
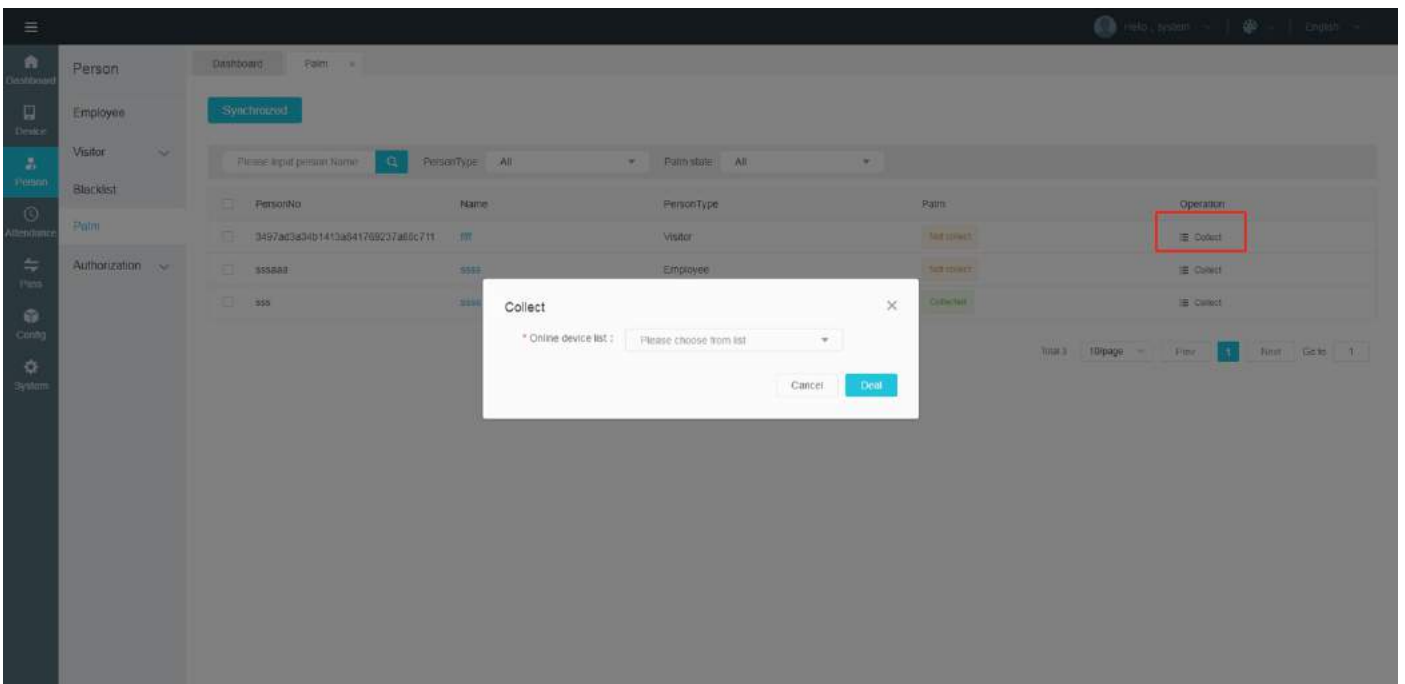
4.4.3. Palmprint synchronization

Click the [synchronize] button to pop up the [palmprint synchronization] page. After

selecting [issue] and [online device], click [process] to synchronize the palmprint

information of personnel to the device, and select [clear] to clear the palmprint

information of corresponding personnel on the device
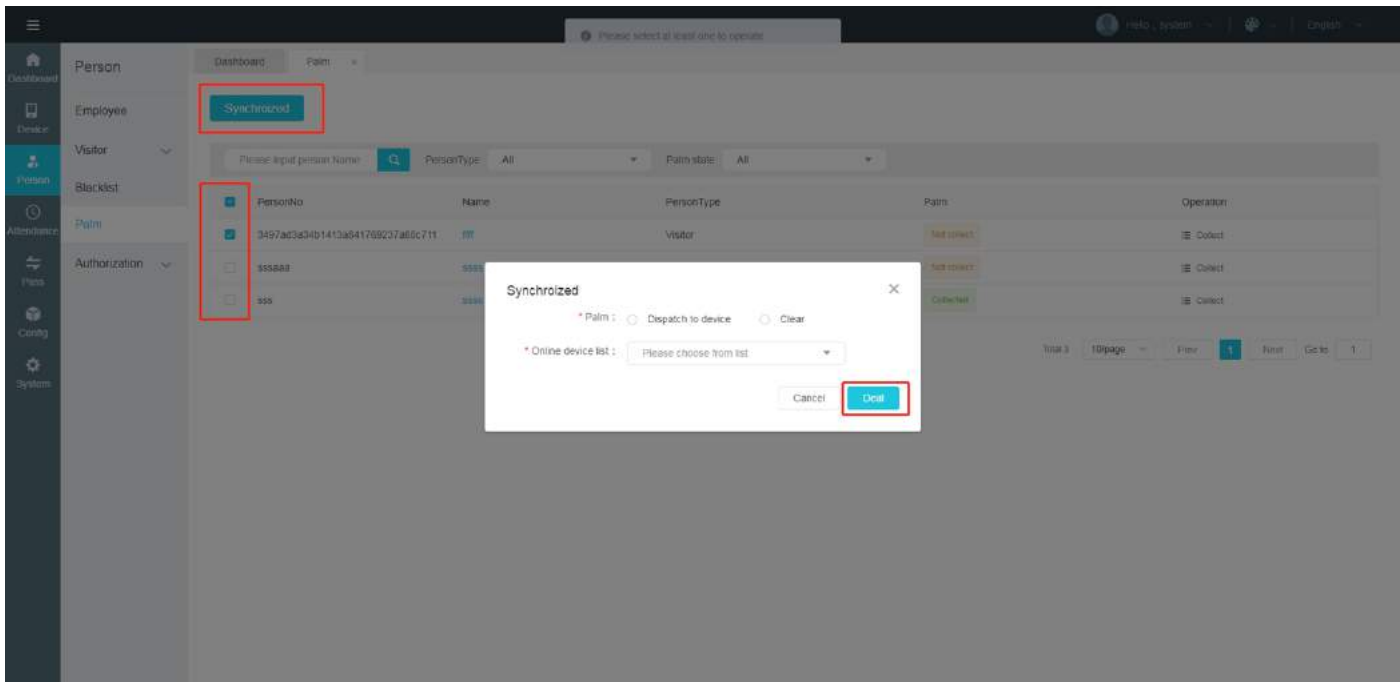
4.5. Fingerprint management

Fingerprint management is used to manage the fingerprint information of employees

and visitors, can check the fingerprint entry status, collect, issue, and clear the fingerprints

of the personnel. (**Fingerprint version device support**)

4.5.1. Fingerprint list

Click People -> Fingerprint Management to display the fingerprint list page, and you can

view the fingerprint entry status of employees and visitors.
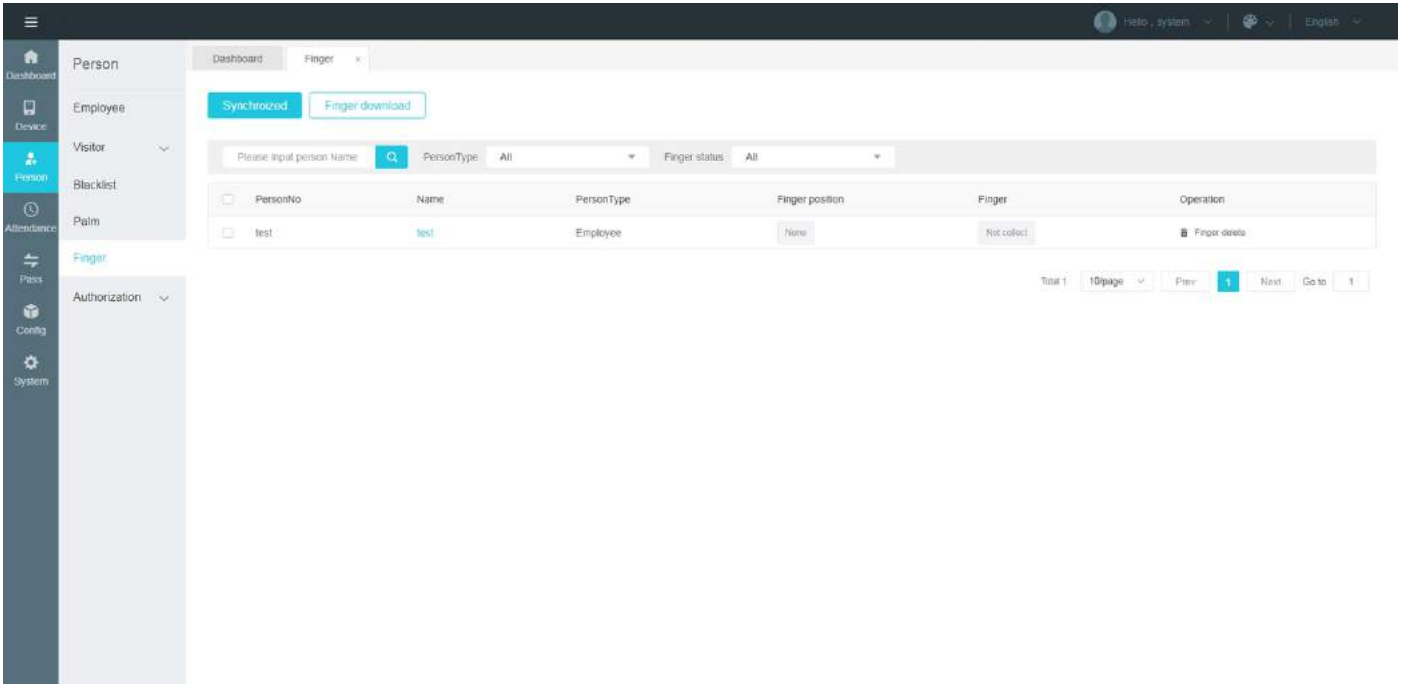
4.5.2. Fingerprint download

Select a person and click the fingerprint download button, and the fingerprint download page will pop up to select an online device, and click the process button to download the fingerprint information of the corresponding person on the device.
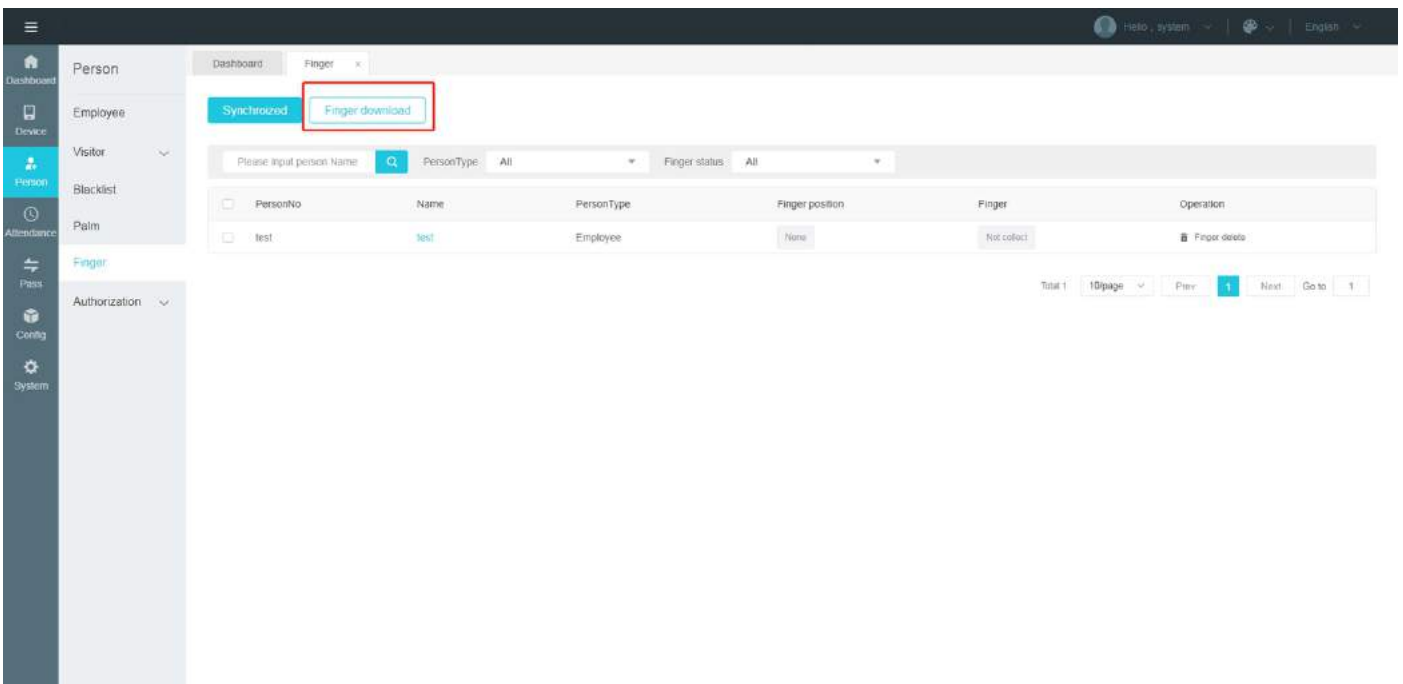
4.5.3. Fingerprint synchronization

Click the [Sync] button to pop up the [Fingerprint Synchronization] page, select

[Download] and [Online Device], click [Process] to synchronize the fingerprint information

of the person to the device, select [Clear] to clear the fingerprint of the corresponding

person on the device information.
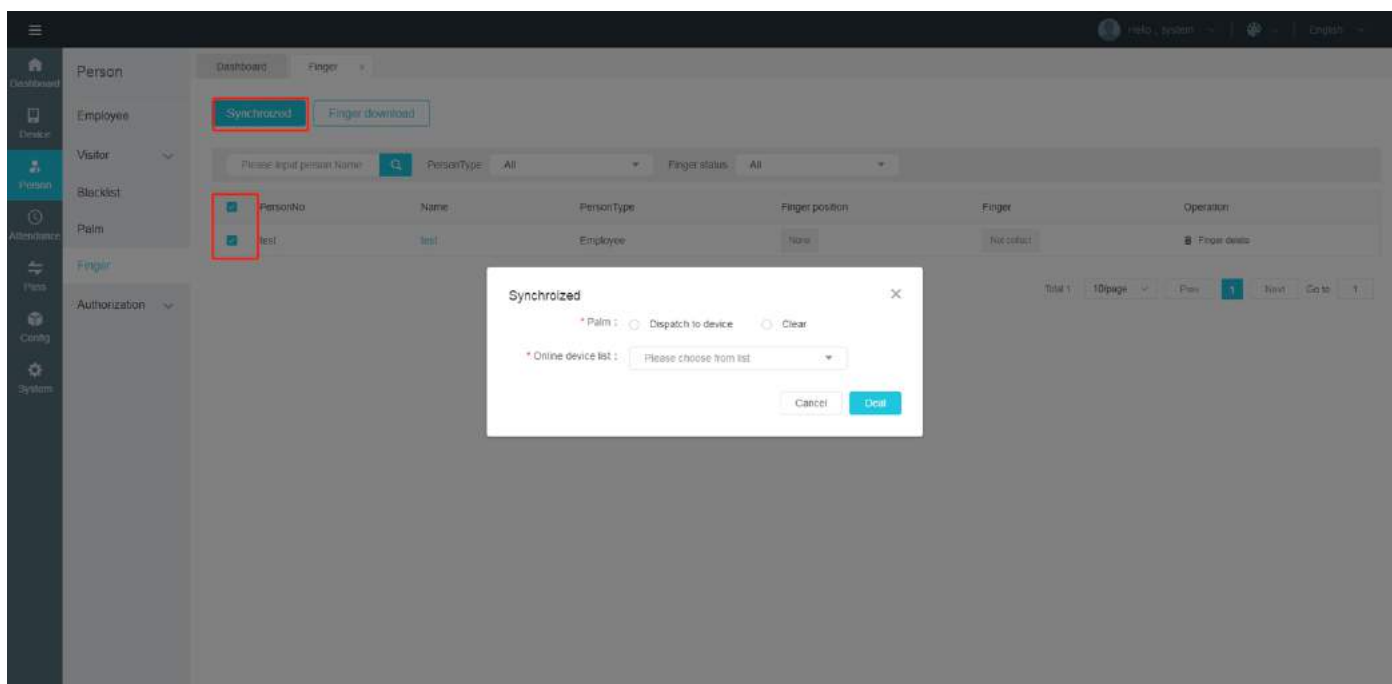
4.5.4 Fingerprint removal

Click the fingerprint clear button in the fingerprint list to clear the relevant fingerprint

information of the corresponding person on the selected device.

5.Attendance Management

[Attendance Management] The module is used to customize attendance rules, query and export all personnel's attendance records, attendance statistics and working hours statistics. If a company needs to use the attendance system, and want to display the calculated attendance, the following points must be ensured:

A: The attendance shift is set in the system

B: Personnel information opens the attendance and selects the attendance shift [select the shift in the personnel information]

The data source on which time attendance is based and the device's pass record. If you have two devices for attendance check-in, set the access type of one device to "in", only use for work check-in, and set the access type of the other device to " "Out" is only used for clocking in after get off work, and the calculated attendance data will be more accurate. If there is only one device used for attendance clocking, you need to set the device access type to "no type", that is, the access/access type. The access type is a device feature, please modify the settings on the device details page.

5.1.Attendance rules

Take Care : If the system is needed to count the company's attendance, please open the system every day and ensure communication with the attendance equipment (i. e., the network is smooth and the personnel identification records from the attendance equipment). If the system is not opened for a long time, the attendance cannot be counted

5.1.1.Period Setting

The main information contained in the Period includes: Period name, Period segm ent (working time ~ working time), overtime rules, etc. The page of shift segment dis play is as shown below. Click the delete icon at the end of each column on the page of Period segment display to delete the Period information of this column.Select the box in front of multiple columns to delete the selected Period information.
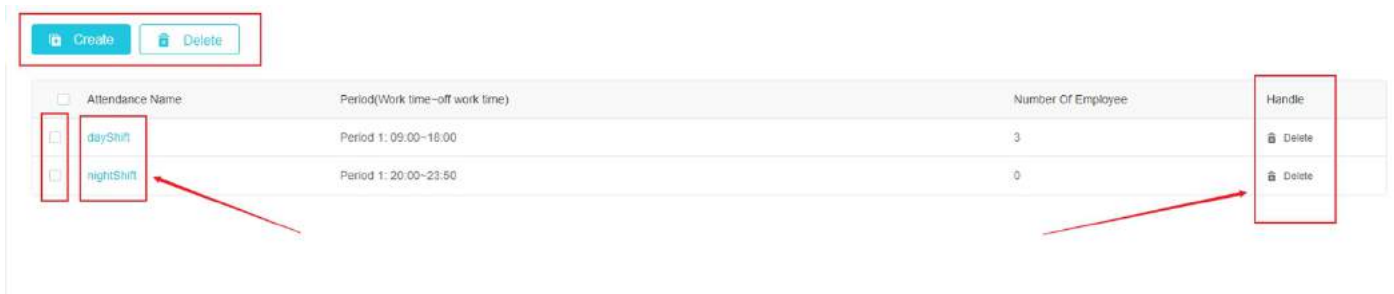
➢ Click the "create" button at the top of the page ,create period setting pa ge can be opened.
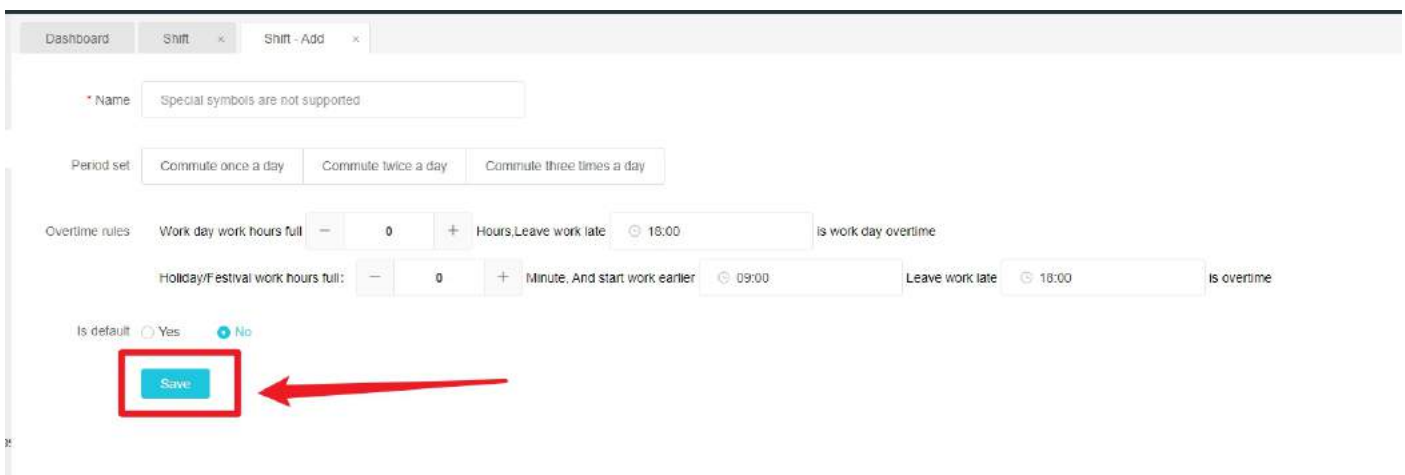
● Name :

1) Custom input Chinese, English and Numbers

● Period Setting :

In the shift setting, you can choose several times a day for commuting, up to three times a day, the first commuting time is shift 1, the second is shift two, and the third is shift three. By default, you need to check in and calculate attendance every time you go to and from get off work. The commuting time should be set in chronological order, as shown in the following figure:

● Overtime Rules

1) You can manually enter/select the time required for working overtime and the time point of leaving the office;

2)You can manually enter the required overtime hours of general holidays and holidays as well as the on-off/off-hours;

➢ Click the work time name information (blue font) to display and modify the detailed information in that shift, as shown in the figure below, the detailed information of the dayShift (example) can be modified on this page, click save to redirect to the shift display page.

5.1.2.Festival Setting

Click the delete icon in the operation to delete the current holiday. Select the bo x in front of multiple columns to delete the selected holiday information.The followin g picture shows the display page for the holiday setting:

➢ Click the "Create" button at the top of the page to open the page of new Festival Settings;

➢ Click the column of festival name (blue font) to display and modify the det ailed information of the festival , as shown in the picture below. The detailed info rmation of Christmas (example) can be modified on this page. Click save to modif y and jump to the festival display page successfully.

5.1.3.Holiday Setting

In the general holiday setting, you can customize the time of various general holi

days by clicking the "Create" button, click the delete icon in the operation to delete the current general holidays, select the box in front of multiple columns, and delete t he selected information of multiple general holidays.The following figure shows the di splay page for the general holiday setting:

➢ Click the "Create" button at the top of the page to open the new holiday setting page;
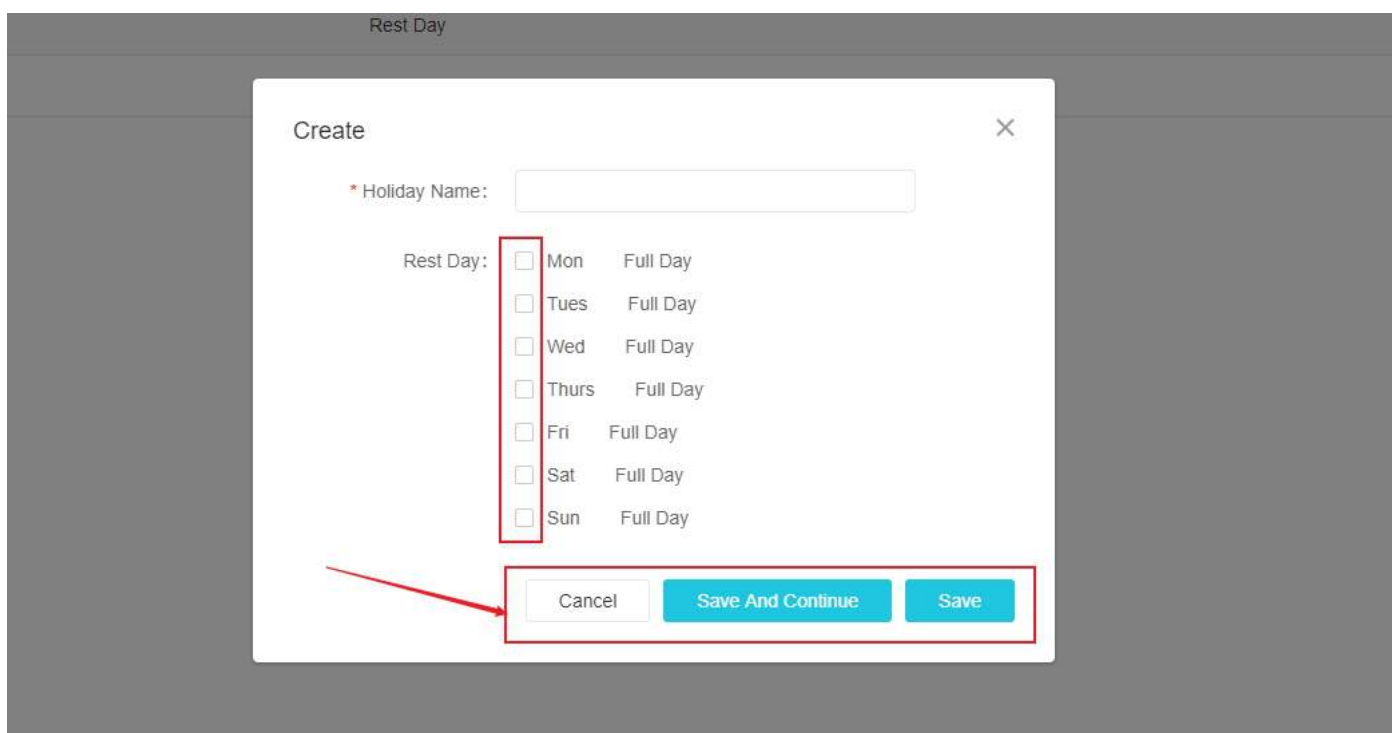
➢ Rest Day : Single or multiple choices from Monday to Sunday are available for custom defined weekly fixed rest days

➢ Click the holiday name (blue font), the detailed information in the holiday can be displayed and modified, as shown in the figure below (for example), can b e modified on this page, click save to modify the successful jump to the holiday

display page.
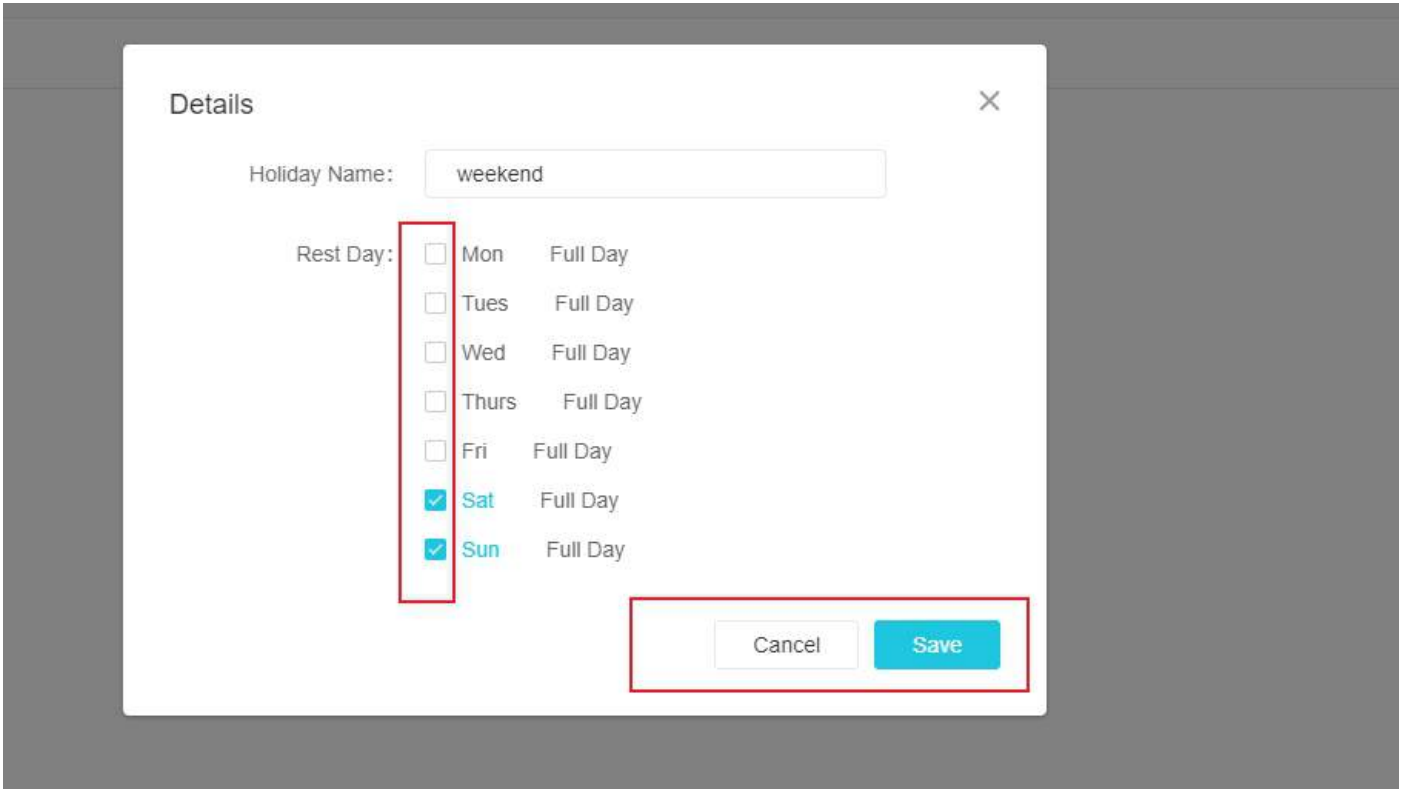
5.1.4.Configuration

Attendance configuration is used to set employee's hourly salary, daily salary, public holiday salary multiples, holiday salary multiples, etc. The salary in 5.4 [Working Hours Statistics] is calculated based on the salary in the attendance configuration. The attendance configuration page is shown below:

Note: The attendance configuration in the system is empty by default, and the salary is not calculated by default in the working hours statistics section. After editing and adding hourly wages, daily wages and other data on this page, click Save, and 5.4 【Working Hours】 will calculate the salary. 【Working Hours】For details, please refer to catalog 5.4.
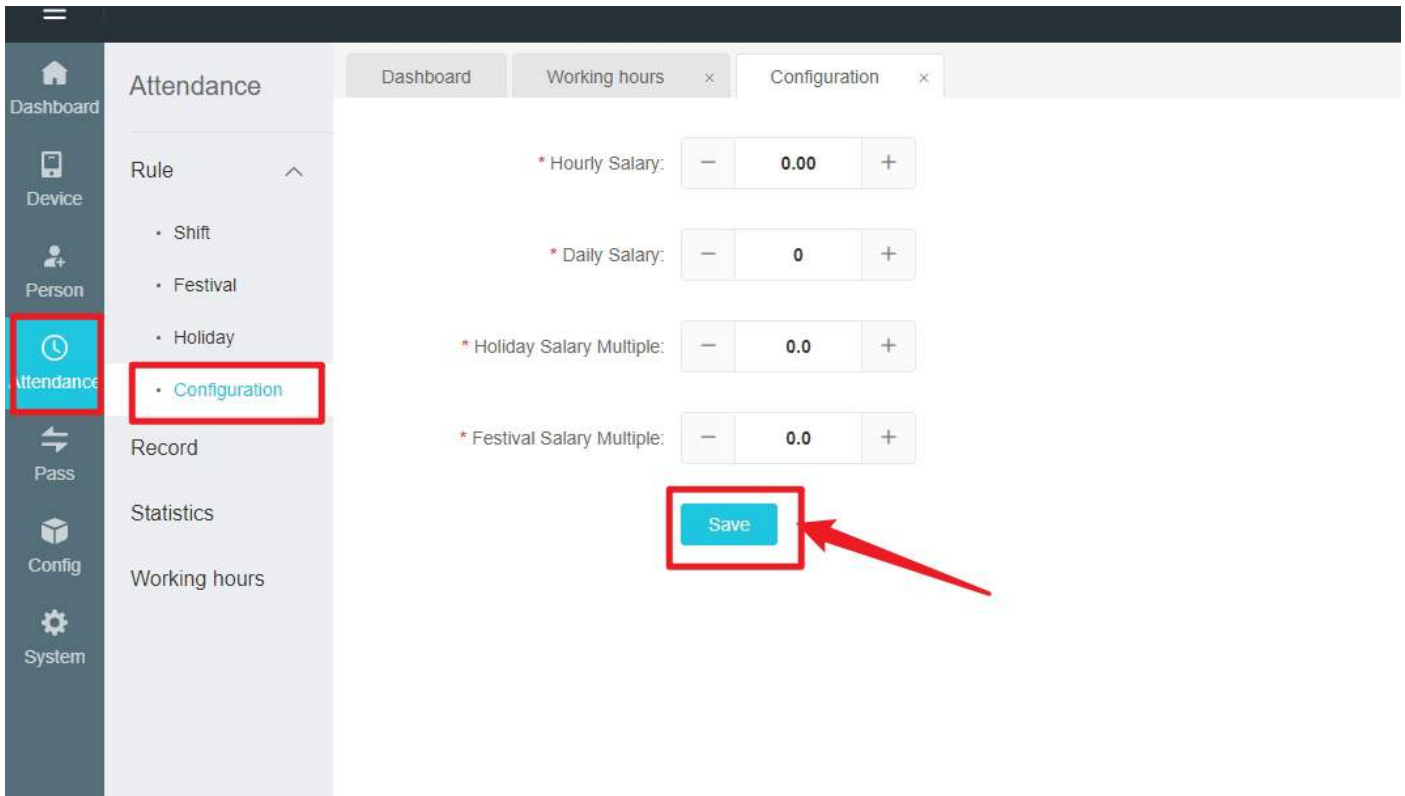
5.1.5．Schedule setting

The shift scheduling setting is used to set the daily attendance shifts of employees. To use this setting, you need to select attendance when creating employees. The shift scheduling setting list displays the current month's shift scheduling by default. After setting public holidays and festival days, the word off will be displayed in the corresponding date column

Set shift: click New button to open the new shift setting, select employee or employee group (selecting employee group will schedule all employees in the group), work shift and shift date (multiple choices are allowed), and then click Save button to set employee shift. After setting, employee attendance will be analyzed according to the shift rules, If there is no shift arrangement, it will be analyzed according to the attendance shift selected when the employee is created
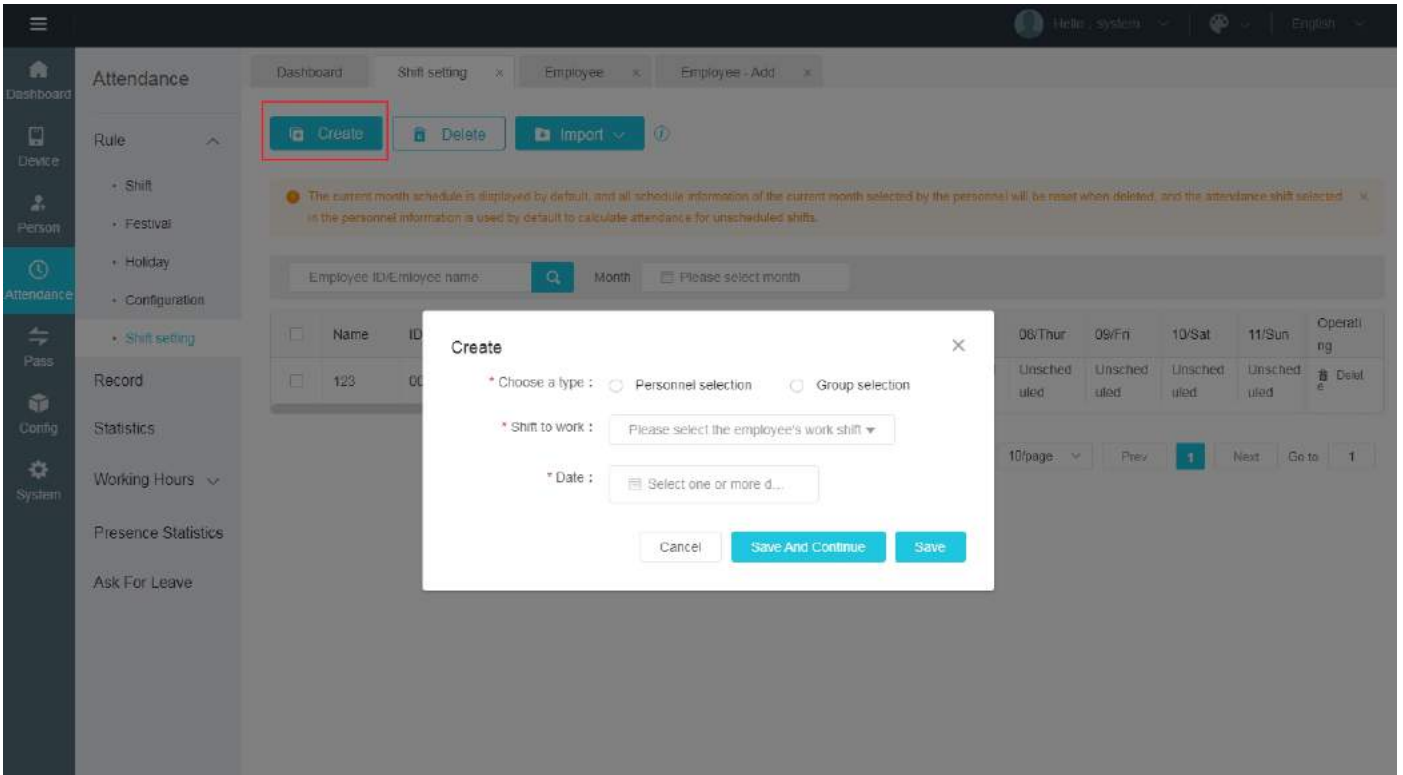
Delete shift information: click the delete button in the figure to reset the shift arr

angement of the month selected by the employee, and reset the shift arrangement o

f the current month by default
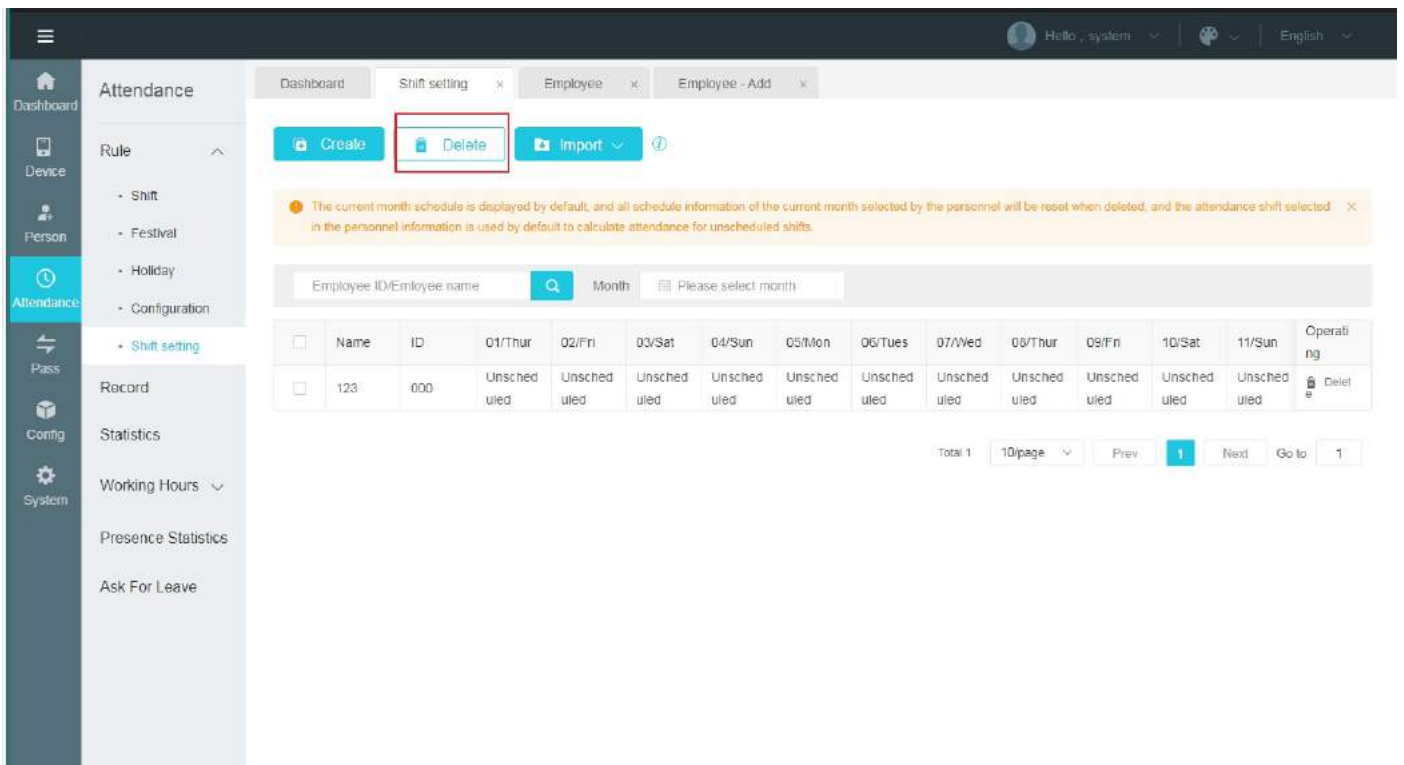
Import: import employee scheduling settings through Excel

Steps: 1. Download the template and fill in the employee name, employee ID (re

quired) and shift information

2.To import the shift schedule, click excel last time, select the completed e

xcel sheet, and then click Import.

5.2.Attendance Record(Save for 120 days by default)

5.2.1. Attendance record list

【Attendance Record】module includes the attendance record of corresponding emplo

yees by time period, grouping query and employee name query, and the list file of e xported query results is downloaded to the local. The attendance record display page is shown in the figure below.
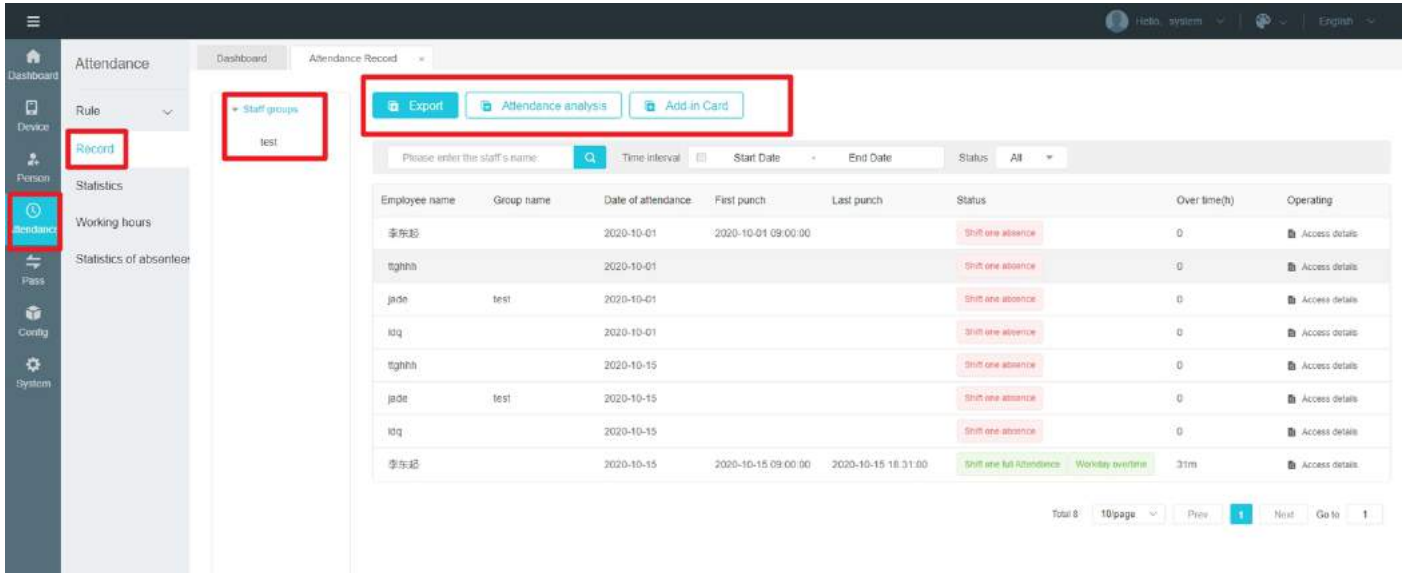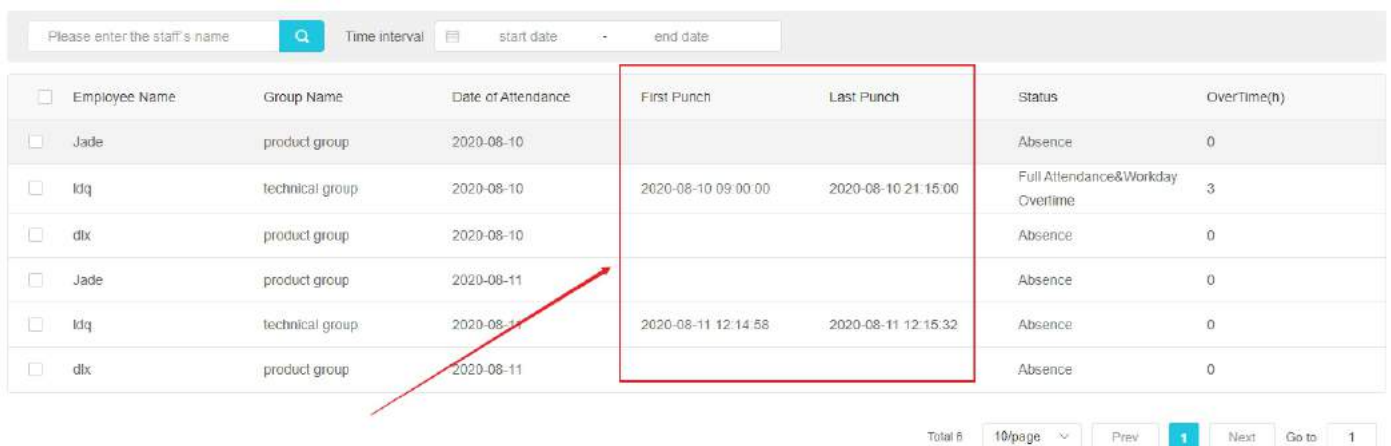

● Date of Attendance

1) The date of attendance record before the current date (excluding the current date) is displayed by default;

● First Punch/Last Punch

1) The employee's first opening time of the day is displayed in the first punch, and the employee's last punch of the day is recorded in the last punch. If the employee does not punch on the day, no data will be displayed.

● Status

1) If the employees clock in and out of the office on the same day, the status bar will show "full attendance" .

2) If multiple shifts are set up, for example, the working time of shift one is 08:00, if it is late, the status bar will display as late for shift one; the same for shift two and three

3) If multiple shifts are set, such as the departure time of the shift is 12:00, if leaving early, the status bar will display as leaving early; the same is true for the second shift and the third shift

4) If the employee is absent from work in a shift (such as being late and leaving early, it is also regarded as absent), the absence of shift in the status bar will be displayed, and the absence of other shifts is the same;

5) If the employee has to work overtime on that day, the status bar will display the "overtime" work on that day.

6) If the date falls within the scope of festival or holiday, the status will display "festival/holiday overtime";

7) If the employee has to work overtime on festival/holiday, the status bar will show "festival/holiday overtime" ;

8) If multiple marker conditions are met on the same day, the status bar will display multiple states.

● export

1）Click the "export" button to download the staff attendance record form file contai

ning the current query page to the local；

5.2.2.Attendance Analysis

Click the [Attendance Analysis] button on the attendance record list page to selec

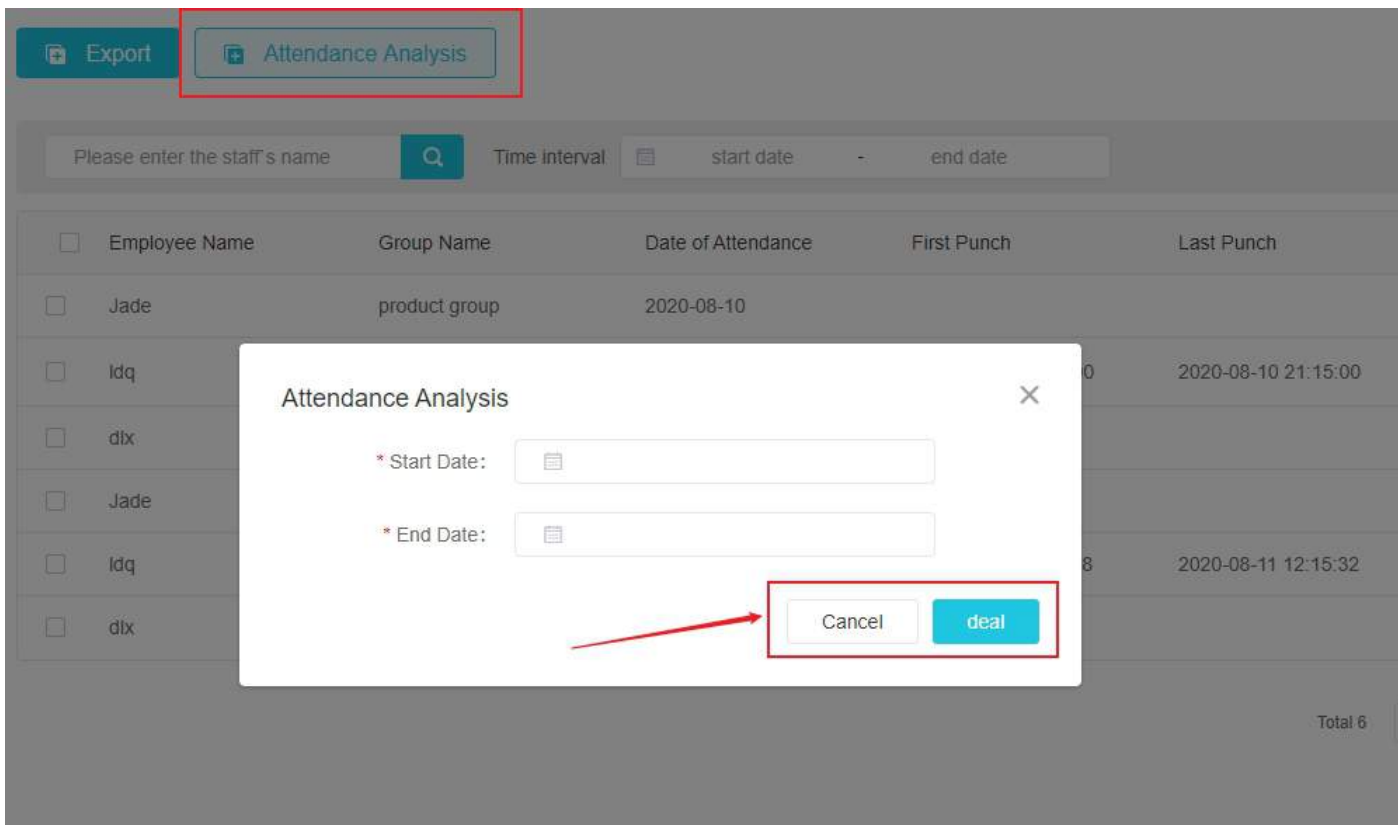t a time period to analyze the attendance at that time
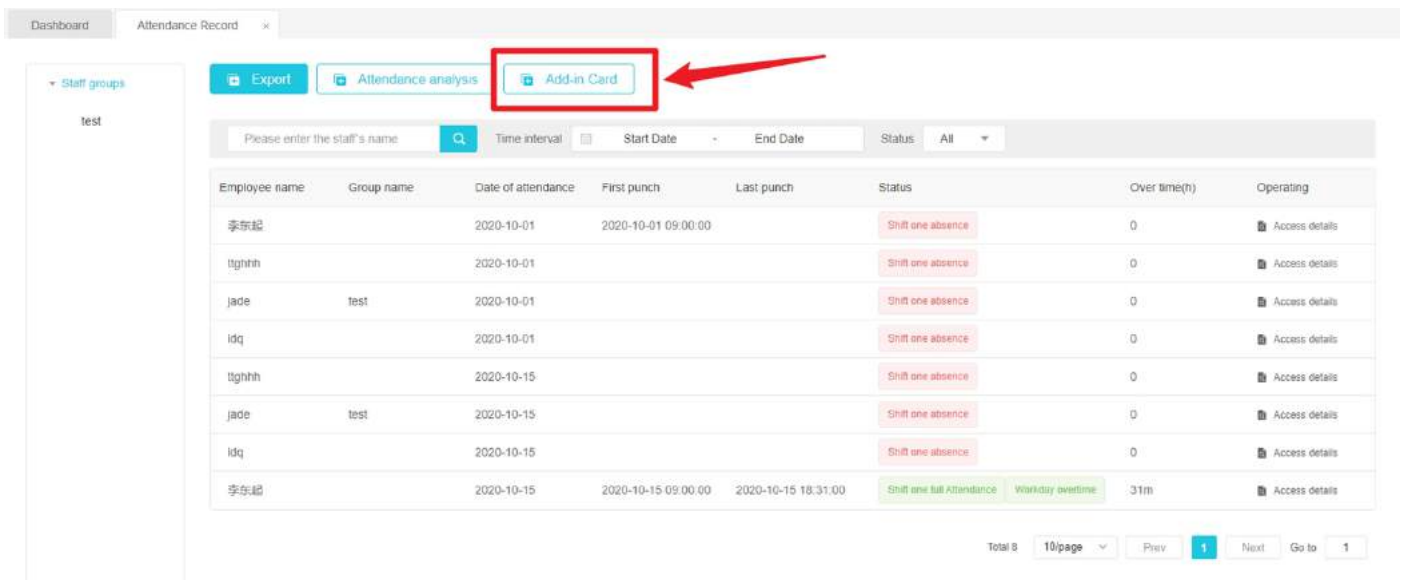

1）The time interval can be selected to recalculate and analyze the traffic record of

this time period to get a new attendance record.

5.2.3.Attendance Add-in Card

Click the [Add-in Card] button on the attendance record list page to replenish th

e card for the forgotten employee.

On the card replacement page, you need to select the add-in card employee, add-i

n card type (punch in,punch out), and the add-in card time. After clicking the submit

button, the attendance record list will display the new attendance record after add-in

card. As shown below:
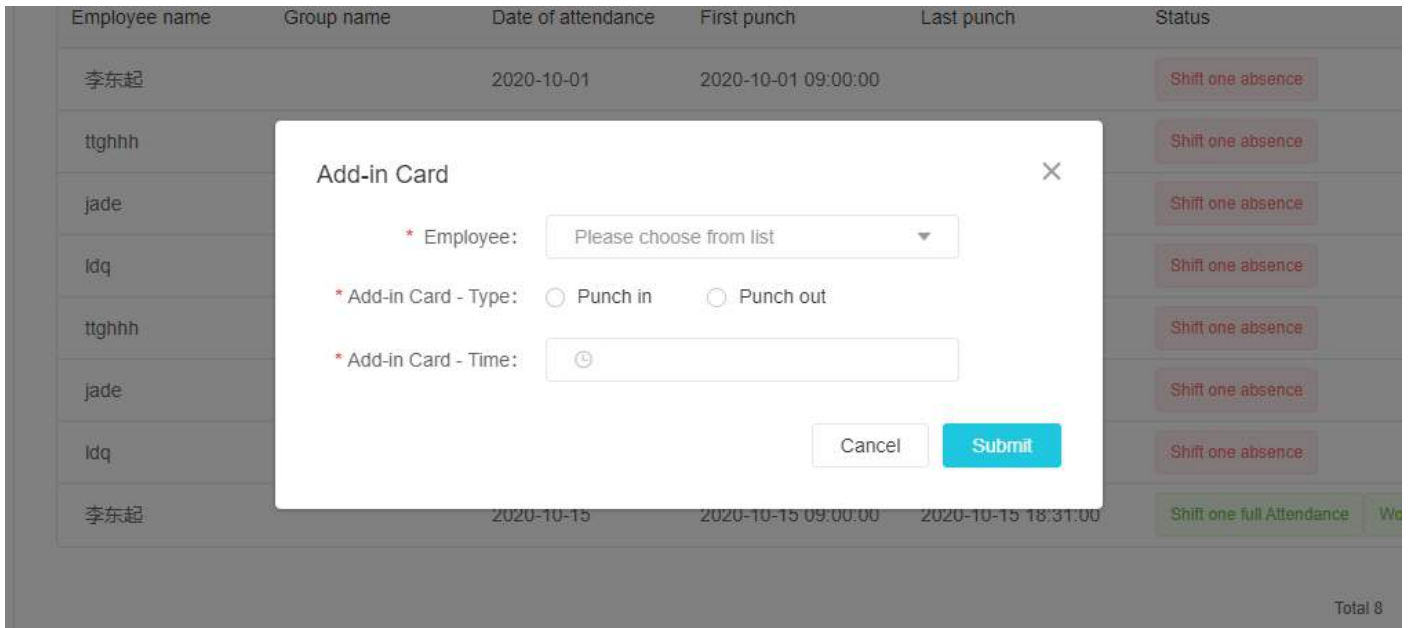
5.3.Attendance Statistics

【Attendance Statistics】module includes data statistics of normal/abnormal attendanc
e of employees in all time/specified time and overtime hours of working days/public
holidays/holidays;
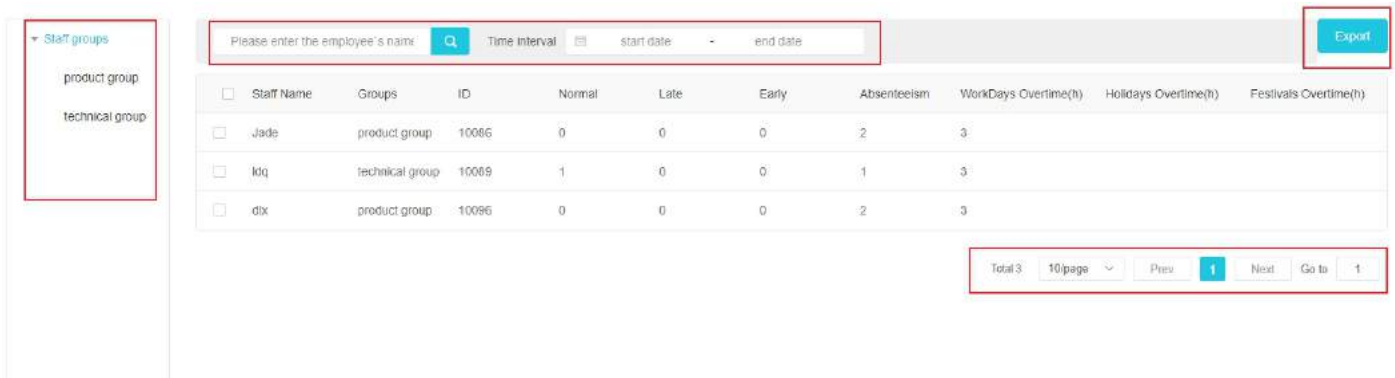
● Staff Group

1) In the employee grouping list, the group name and grouping information are the
same as the grouping data in the [Employee List]. The data changes in the employee
list are synchronized in real time. After selecting all groups, the attendance statistics
of all employees will be displayed on the right side. Click the sub After grouping, onl

y the employee attendance statistics in the sub-group will be displayed;

- Normal、late\early Absenteeism

1）By default, it is selected to display the statistical data of the month before the query date, which respectively display the employees' normal days, late arrivals, early departures, and absences. If there is no record of the corresponding status within the query time range, it will be displayed as 0;

- workDays OverTime(h) 、holidays OverTime(h)、festival OverTime(h)

1) By default, the statistical data of the month before the query date is selected to display the accumulated overtime hours of employees working overtime on working days/public holidays/holidays. If there is no record of the corresponding status within the query time range, it will not be displayed;
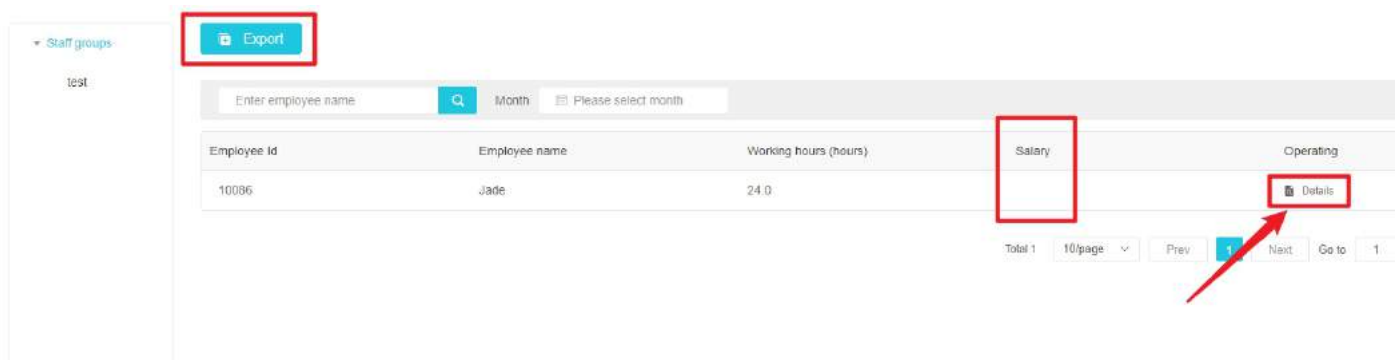
- Export

1） Click the export button to download the employee attendance record form file containing the current query page to the local;

5.4.Working hours

Working hours statistics is to calculate the working hours of the employee today (daily statistics) and this month (monthly statistics) based on the employee's entry time and exit time, and can calculate the salary. The location of working hours statistics is shown in the figure below:
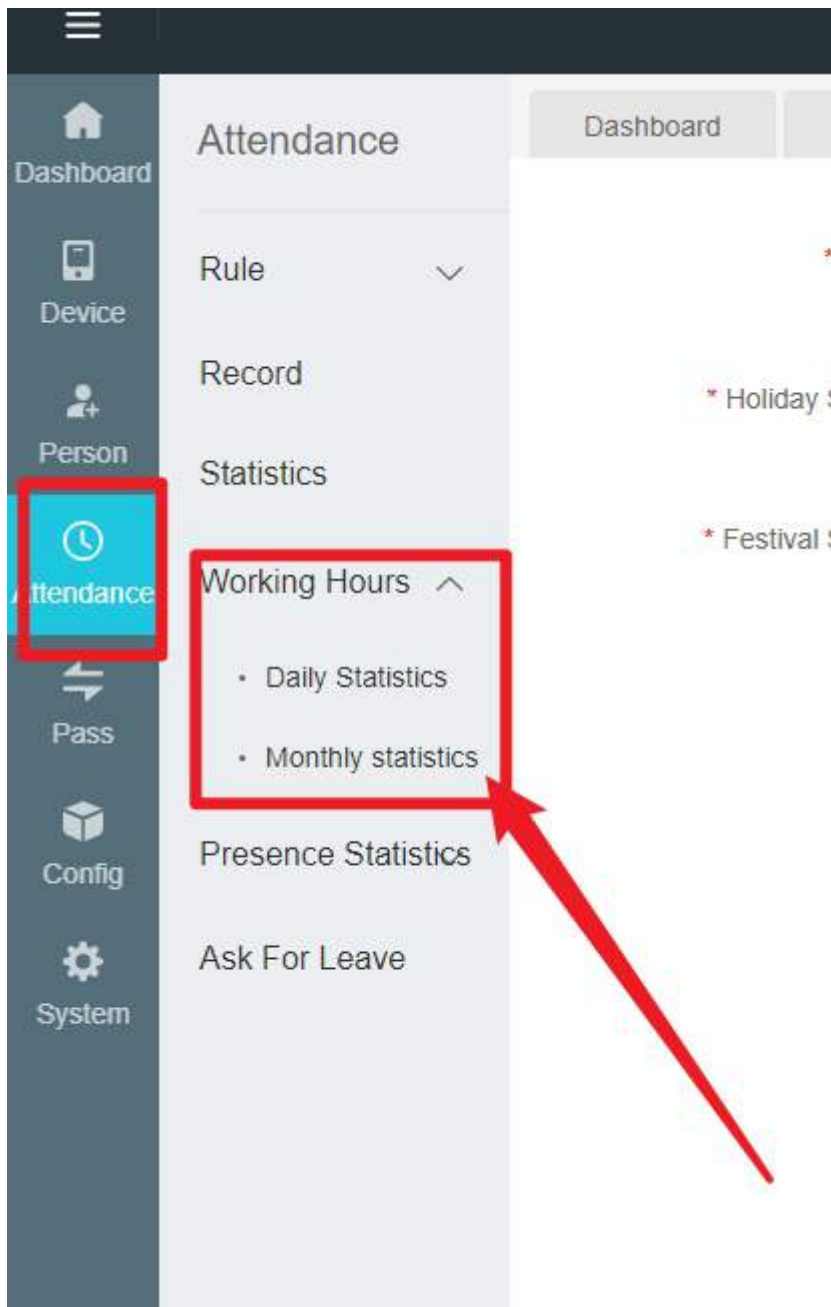
The working hours statistics page specifically displays the employee ID, name, and working hours (the cumulative working hours of the month are displayed by default) as shown in the figure below:

➢ ⬜ Working hours: By default, the accumulated working hours of employees in the current month are displayed

➢ ⬜ Query: Under the [Export] button on the displayed page, you can enter the employee's name and select the month in the search bar to query working hours

➢ ⬜ Salary: The system default salary is empty, and the salary will be calculated after setting [Attendance Configuration]. For details, see 5.1.4 [Attendance Configuration].

（Set according to the actual situation, the following figure is just an example):
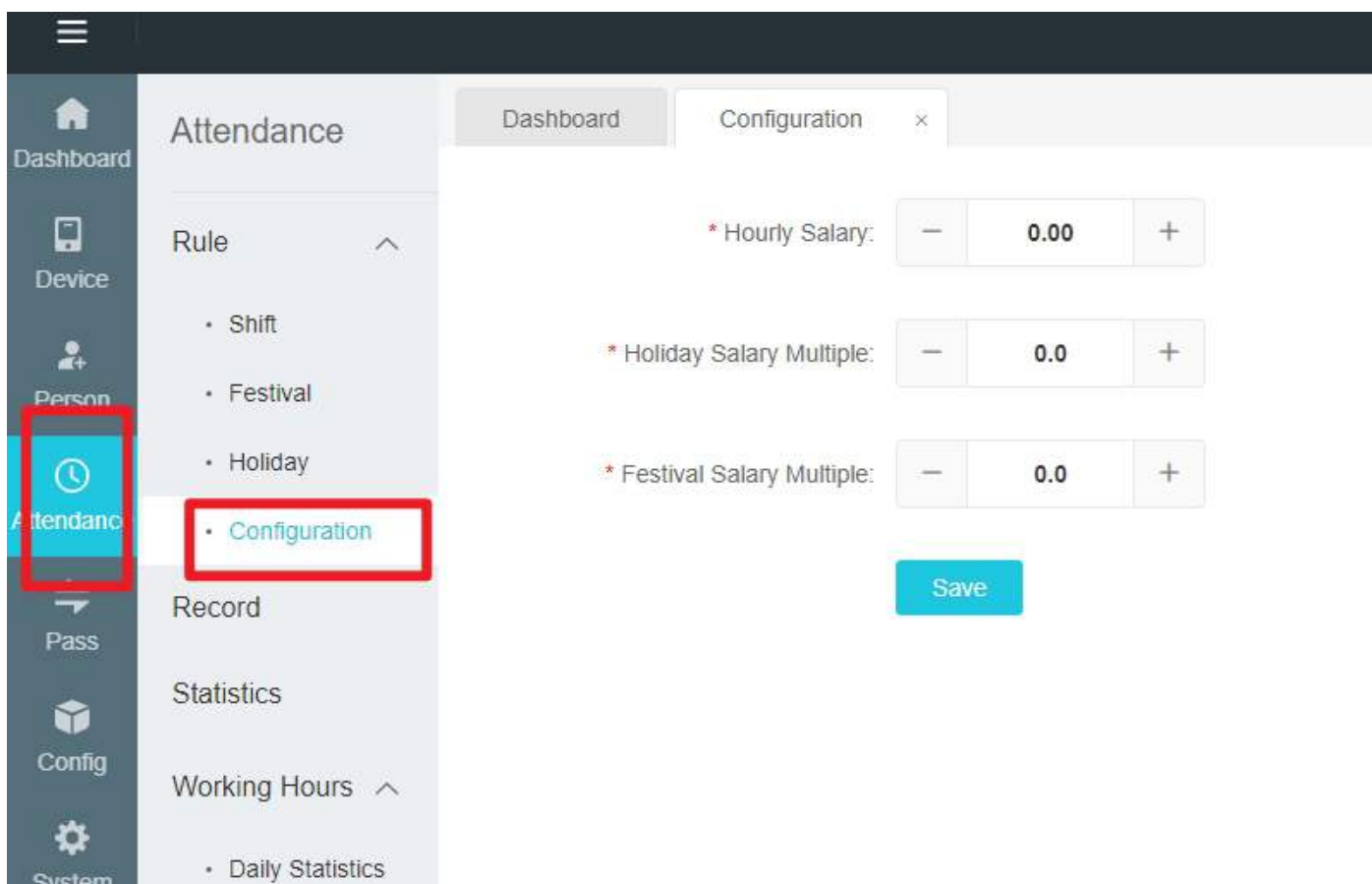
The salary in the working hours statistics is:

> ⬜ Details: Click on the details in the working hours statistics list to see the emplo yee's working hours details for the month, showing the employee's starting tim e, ending time, and working hours per day (minutes) in the month, as shown in t he figure below :

5.5.Presence statistics

The position of the statistics part is as follows :
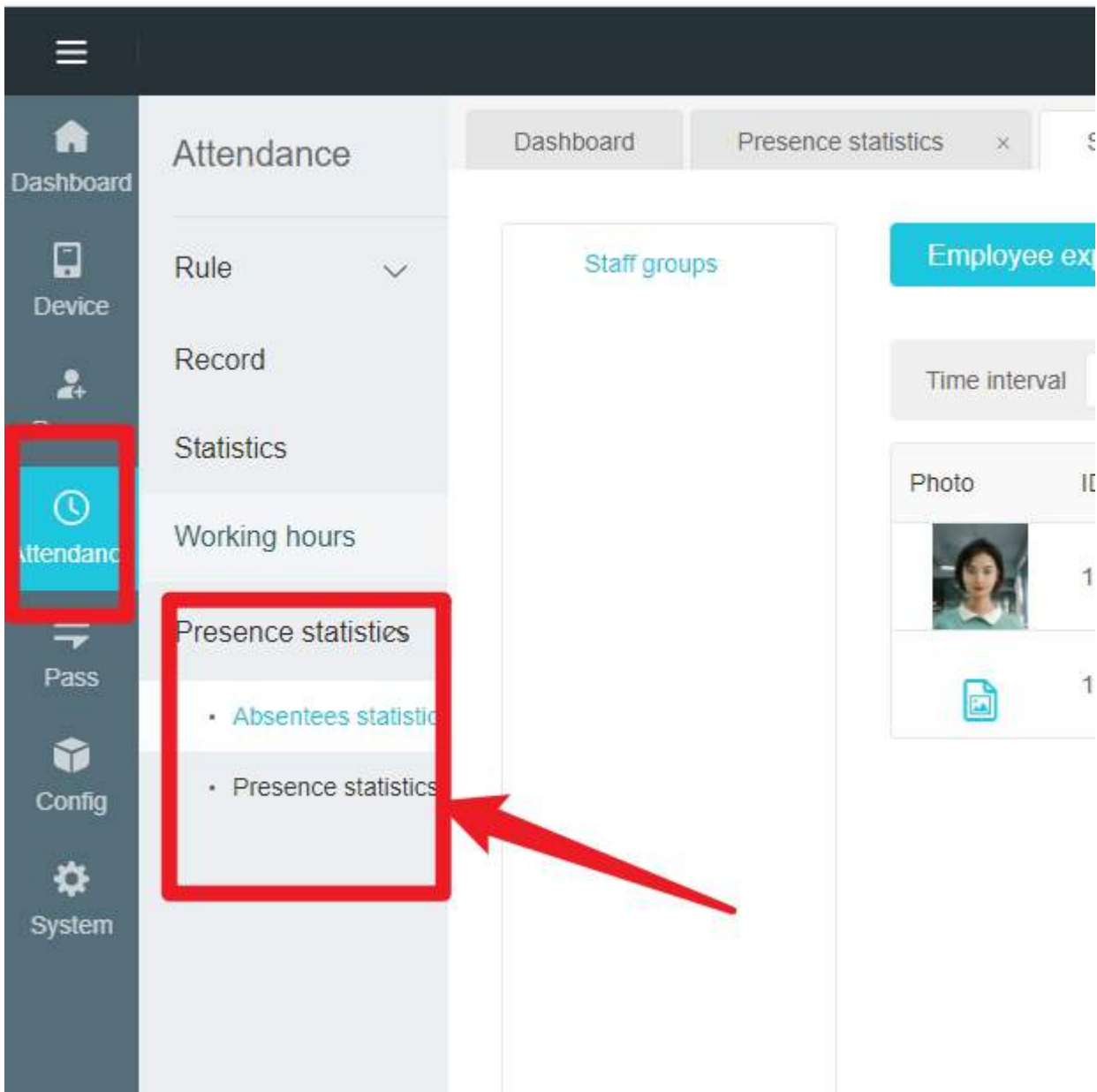
5.5.1.Absence statistics

Absence statistics refers to the number of employees who are not present until a certain time, and displays general basic information of the employees. If there is a pass record, the time when the employee is out will be displayed. The display page is shown below :

- ➢ ⯈ Personnel export: Click the [personnel export] button at the top of the list to export the persons who are not present in excel file format.

- ➢ ⯈ Time interval: select the end time. For example, 2020-10-30 12:00: 00, the list will show employees who are not present as of 2020-10-30 12:00: 00. If no time is selected, the default is the current day.

5.5.2.Statistics of people present

Corresponding to the staff who are not present in 5.5.1, the statistics here are the staff who are present up to a certain time, so I will not repeat them here.
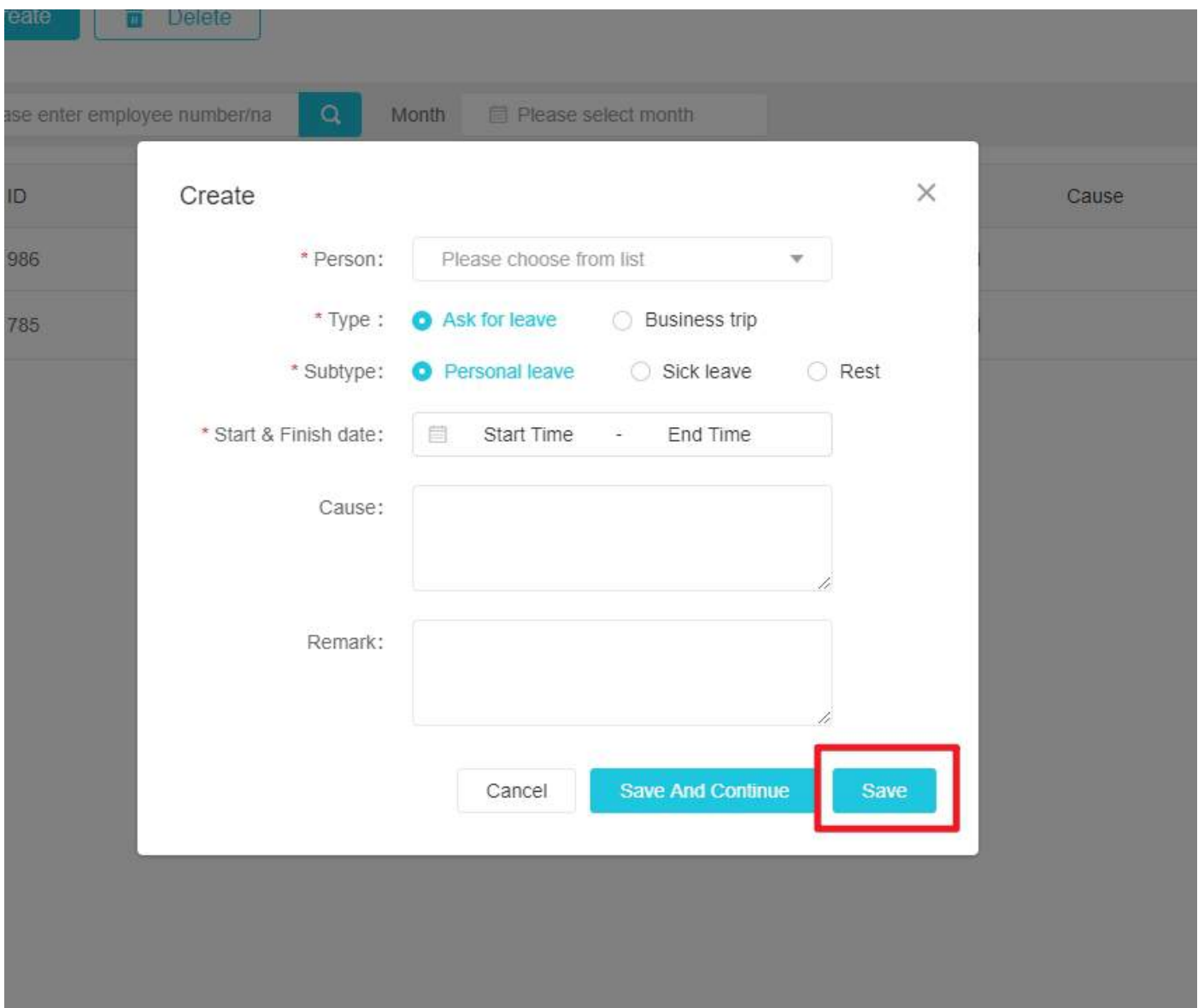
5.6 . Ask for leave
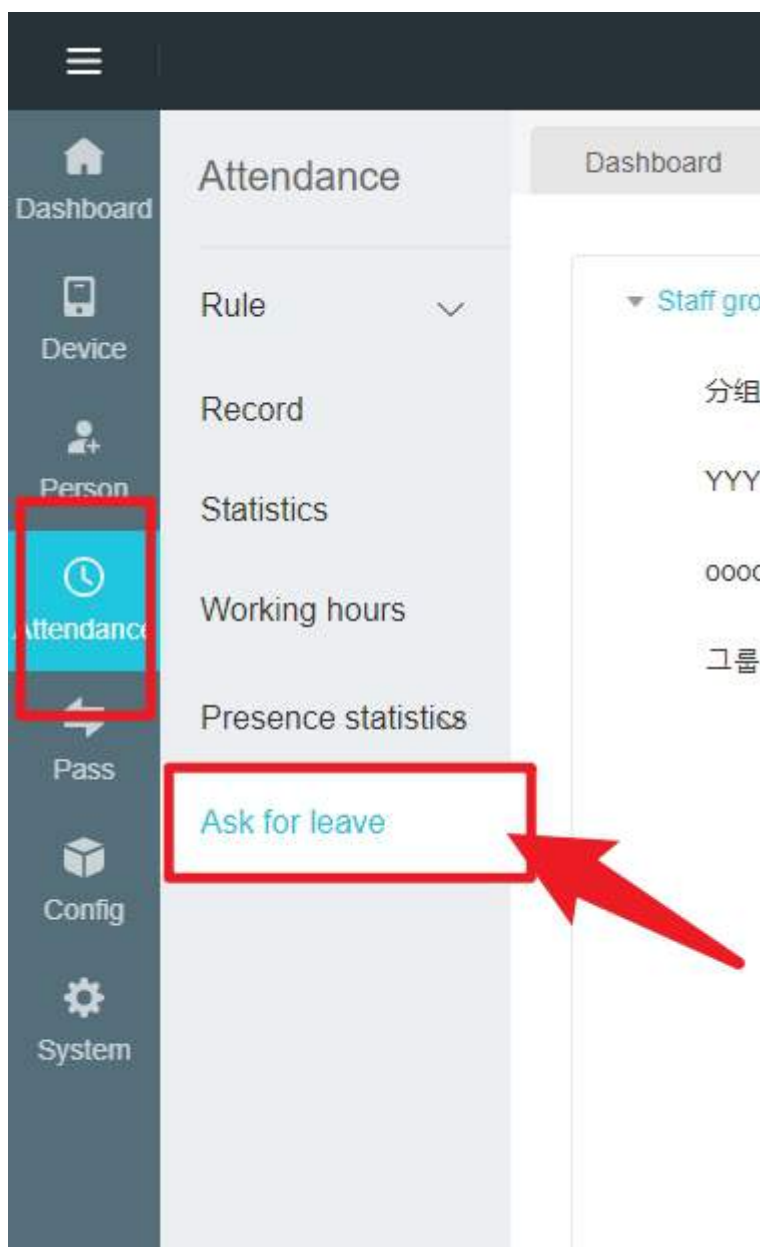
The leave management part is for employees. If you select the employee to creat e a new leave request on this page, the employee's attendance status on the day o f leave will be displayed as: "leave".

The display page is as follows :
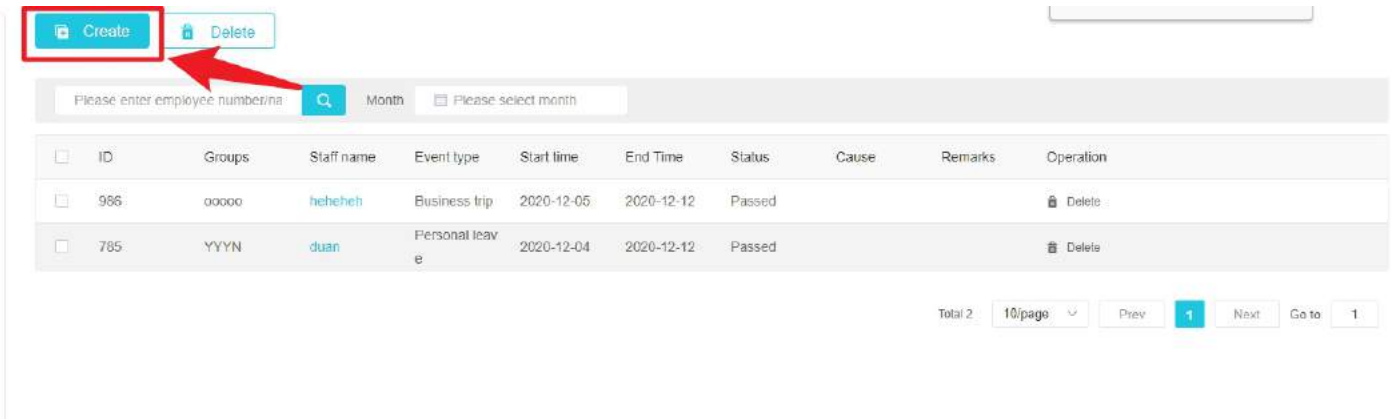
> ▢ New: Click the [New] button at the top of the page, and a window for crea

  ting a new leave message will pop up. Fill in the corresponding information, c

  lick the [Save] button below, the new creation is successful.

> ▢ Modify: Click on the employee name column (blue font) to view the employ

ee's leave details and modify the leave information.

> □ Delete: Select the check box in front of each column and click the [Delete]
>
> button at the top to delete the selected leave information, or click the delete
>
> icon behind each column to delete the leave information in the column.

6.Pass management

Note: there is no traffic record after the device login, please check the device settings-> callback configuration set the device callback address.

6.1.Pass record

Delete the traffic record: Delete the selected record

View all the identification records on the device, through device grouping and device filtering. The data body temperature value is greater than or equal to the [Abnormal temperature judgment value] of the temperature measurement parameter configuration in red font, and less than green font;
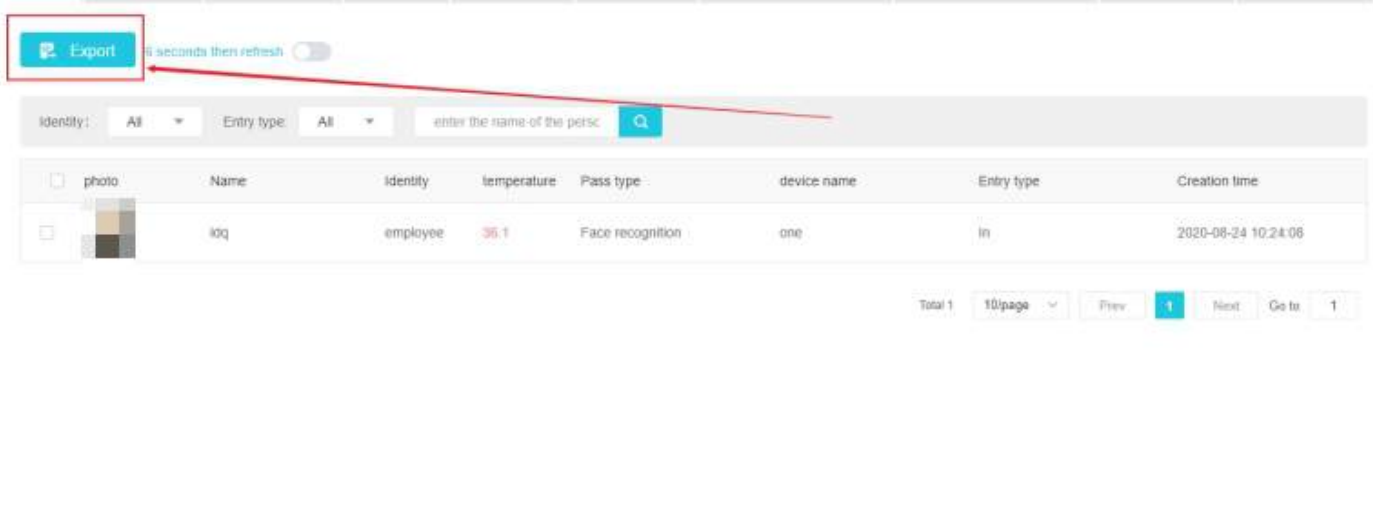
Pass record export: Click the pass record [Export] button on the page to export the existing pass records in the system to the computer in excel file format.

The following figure is the content of the exported excel file

6s refresh of the pass record: When someone passes through the online device of the

system and the pass record is generated, the newly generated pass record can be

refreshed manually. Turn on the 6s refresh switch on the page to refresh it manually, the

pass record will be refreshed every 6s
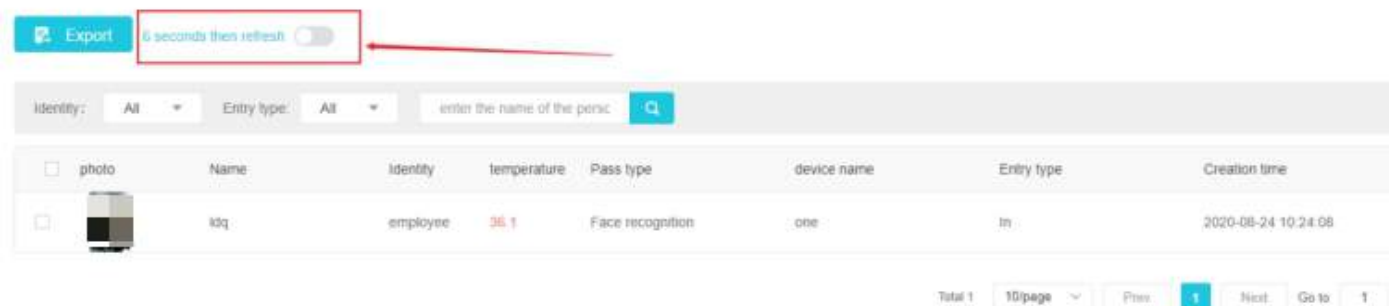
Additional information bar click to view: click the view button in the additional

information bar to view the IC card, ID card, QR code and other content information.
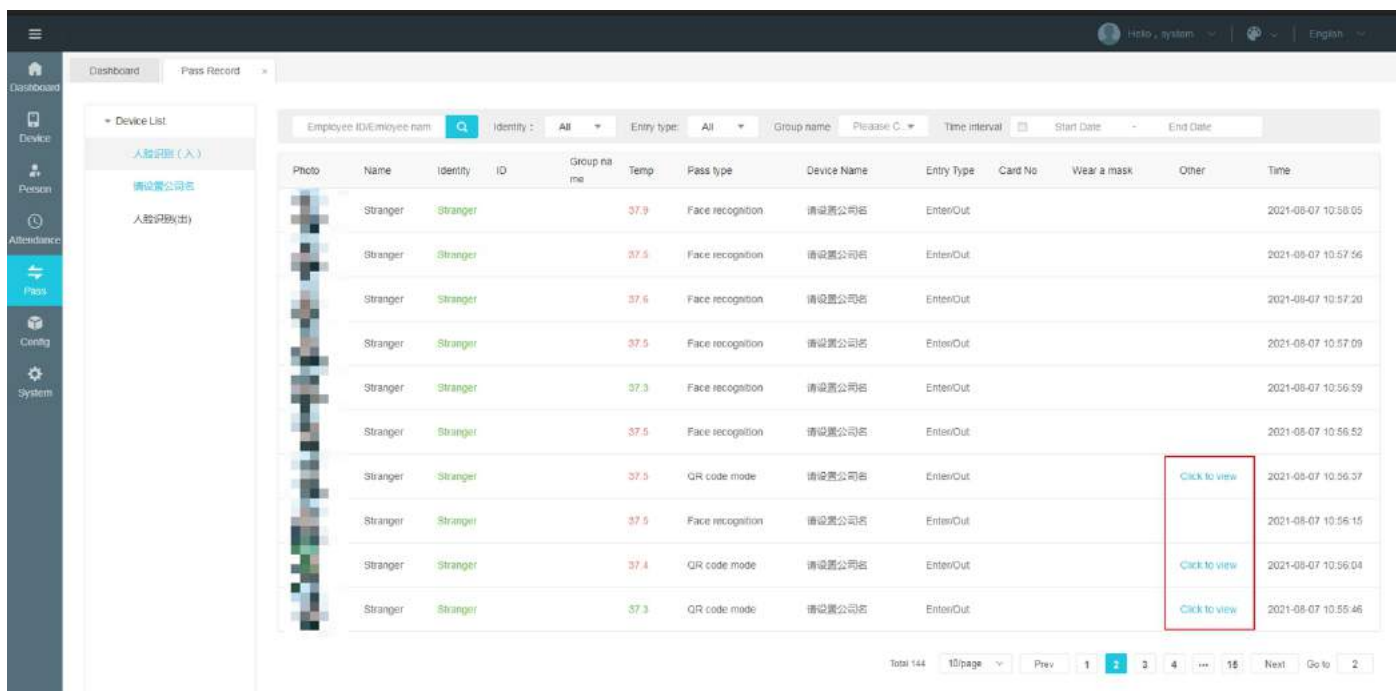
Details ×

Basic information of personnel

First name : V▓▓

Last name : M▓▓

Birthday : 195▓▓
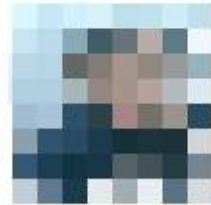
Rehabilitation information

Recovered disease or pathogen : COVI▓▓

Date of first positive test result : 2021-04▓▓

Start time of the certificate validity period : 2021▓▓

End time of certificate validity period : 2021-1▓▓

Certificate issuing authority : Ministero ▓▓

Country : IT

Certificate unique identification : 01IT2DD286278907▓▓

6.2.Capture record
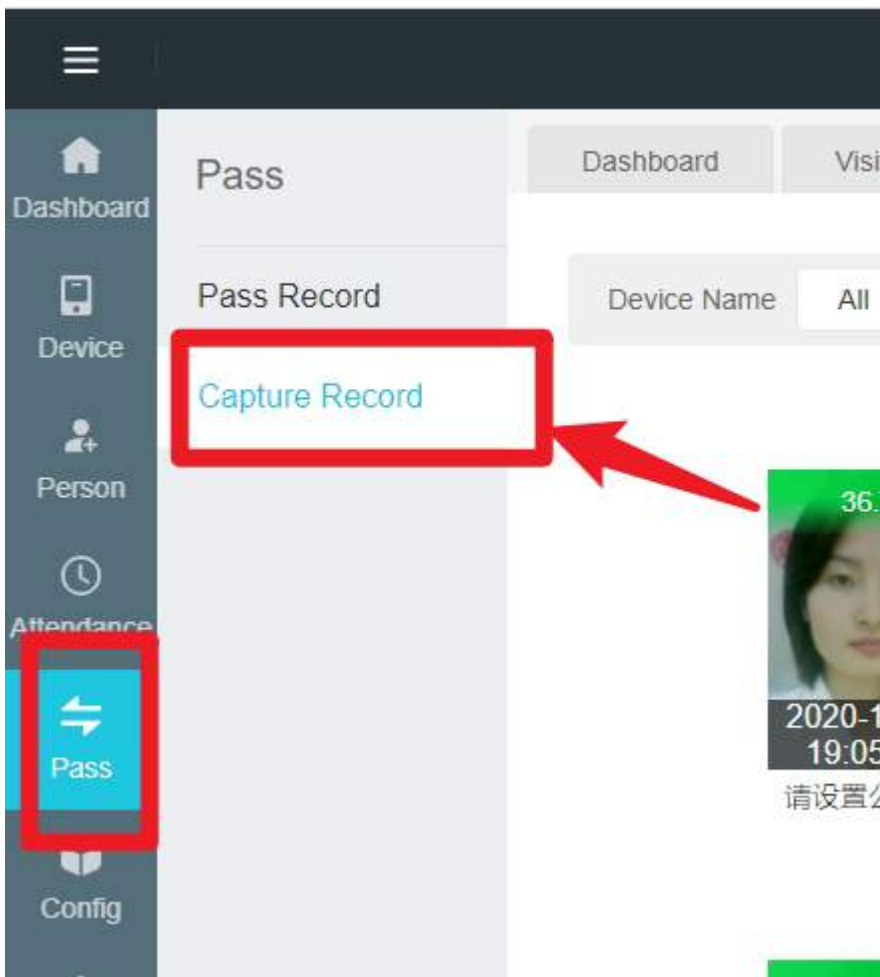
The snapshot record shows the face photos captured by the device. This page only displays the captured photos, the device that captured the photos, and the capture time. You can query the captured photos by device name or time period. The specific page is shown below:
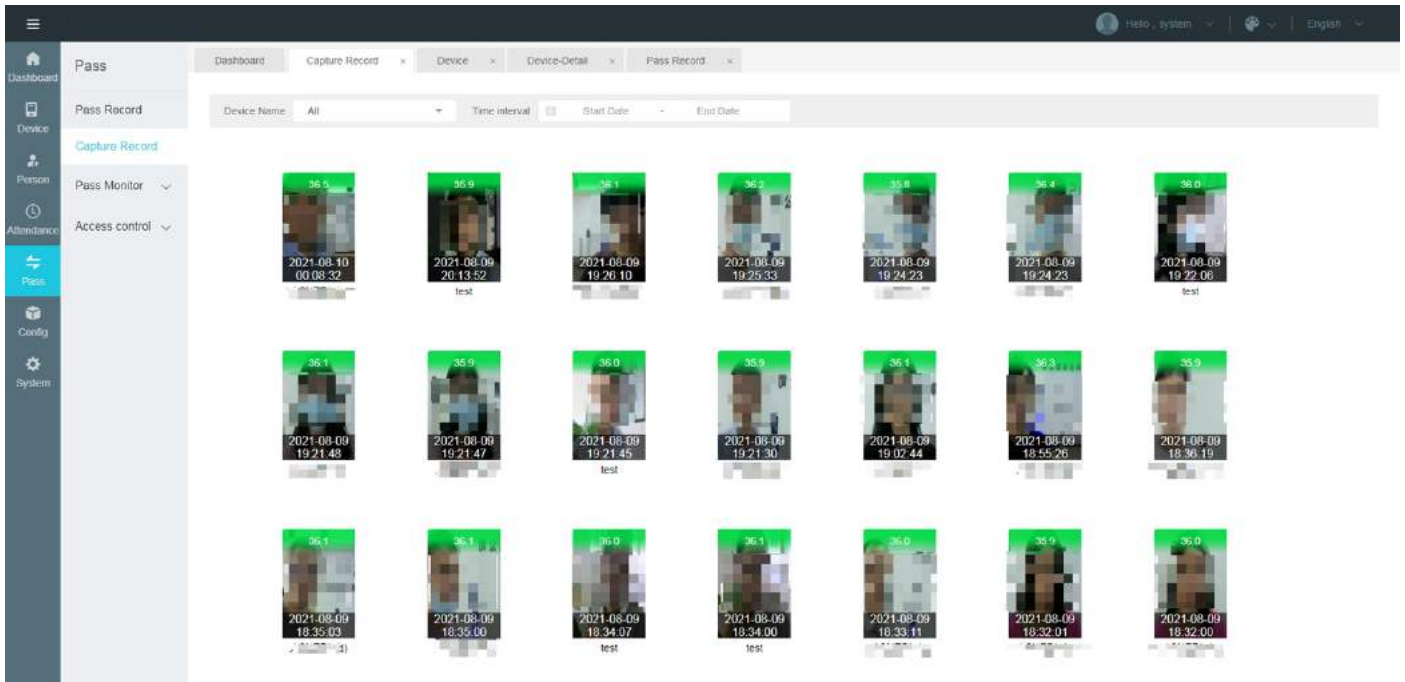
6.3.Pass monitor

The monitoring board is divided into smart board and temperature board. The s mart billboard displays the graphical information of people entering and exiting the s ystem today and in the past seven days, and the temperature billboard displays the graphical information related to temperature.
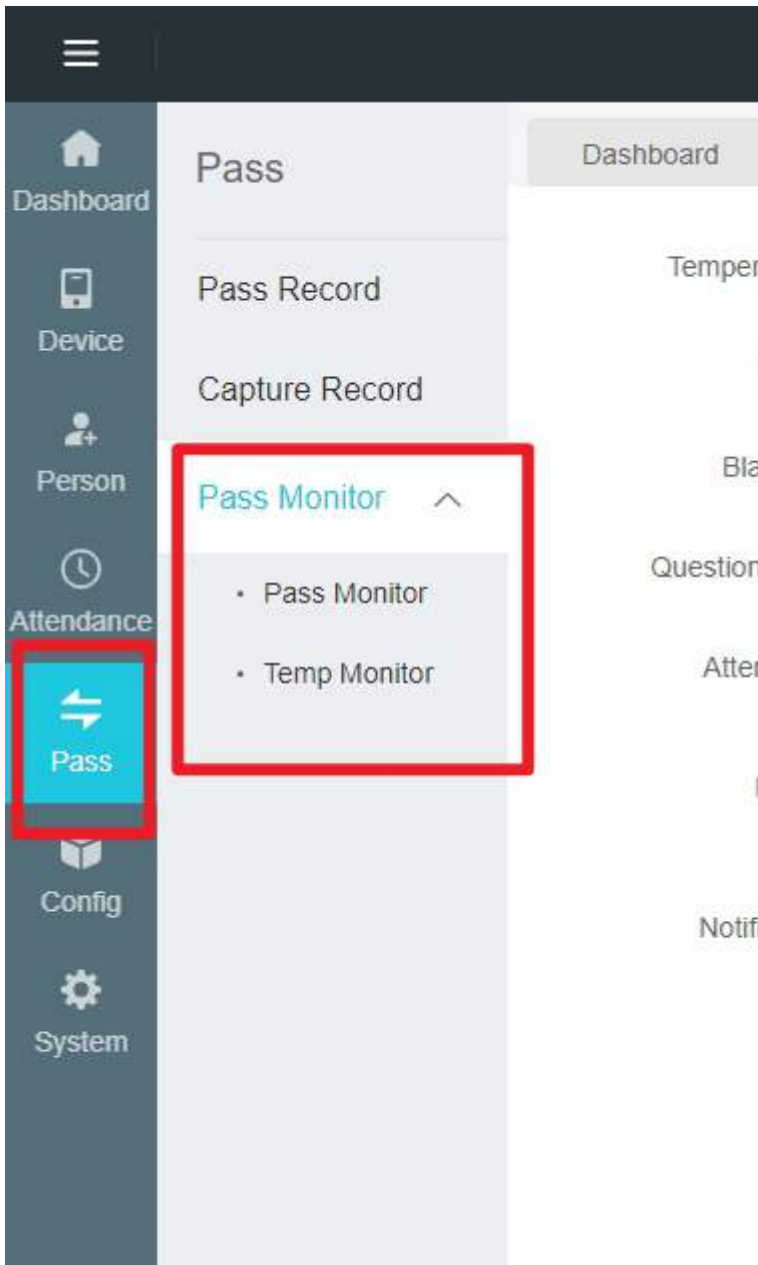
6.3.1.Pass Monitor

This page displays the graphical information of people entering and leaving the

system today and in the past seven days, as shown in the following figure:
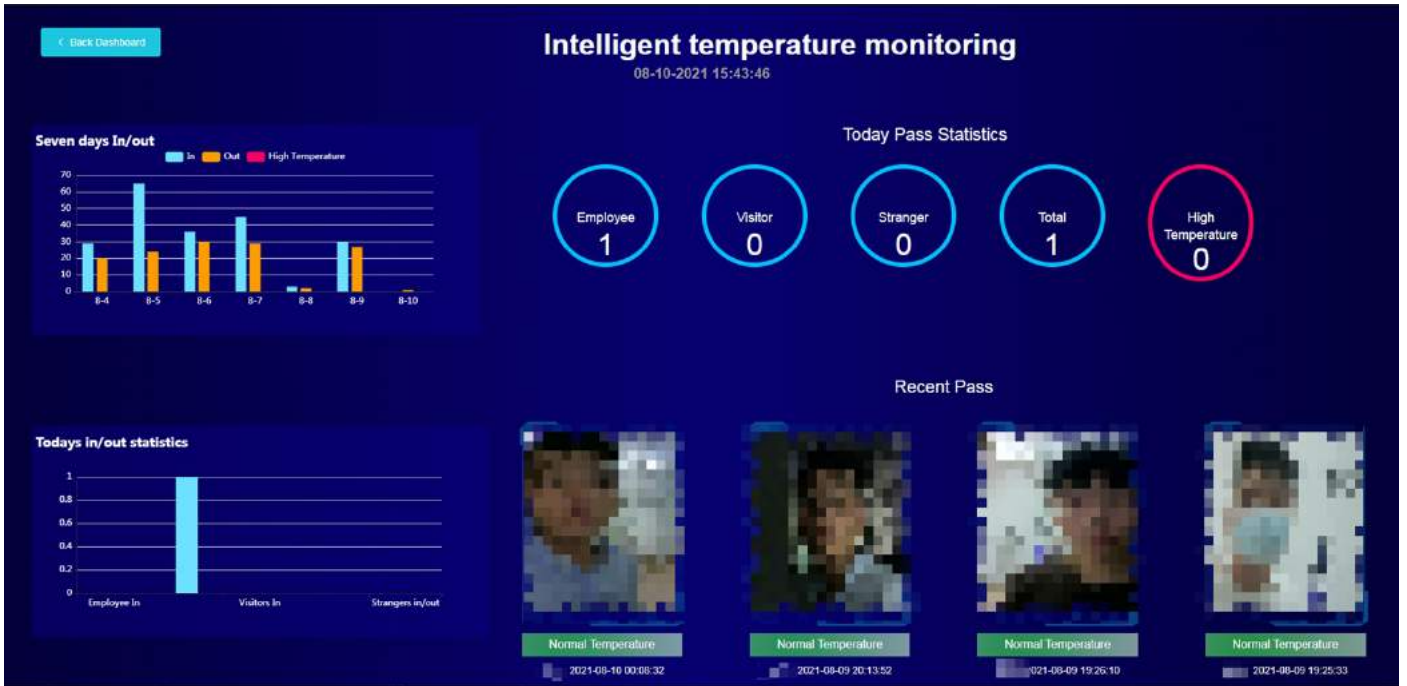
6.3.2 . Temp Monitor

This billboard displays graphical information related to temperature, as shown in t

he figure below :

6.4 .Access control

Access control management mainly sets the pass time of the device. The default pass is all day, and a maximum of three time periods can be added in a day. After the device is configured with access control rules, access is prohibited outside the time period.

6.4.1 .Holiday management

This module mainly sets the access control management holiday dates, and can configure the holiday travel time in the access control rules
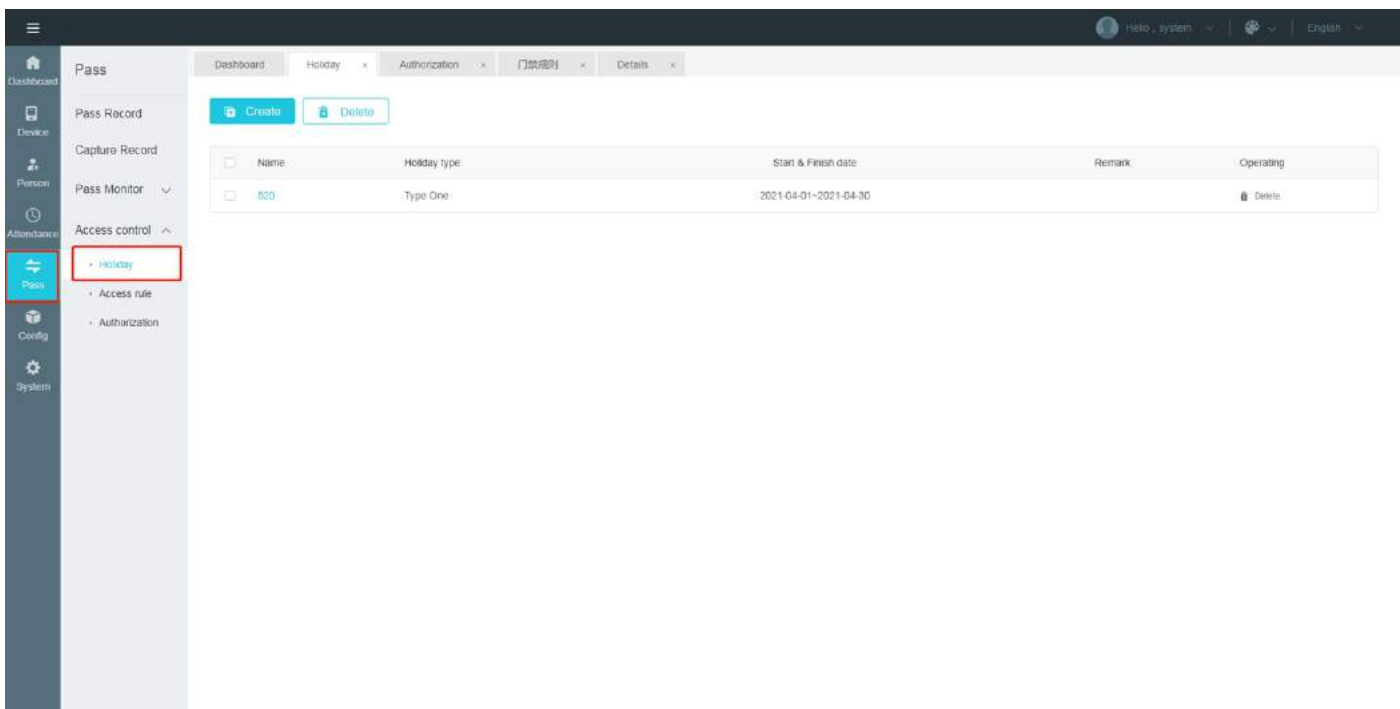
After clicking the new button, open the new page and select the holiday name (required) holiday type (required) start and end date (required) After remarks, click the save button to create a new access control holiday
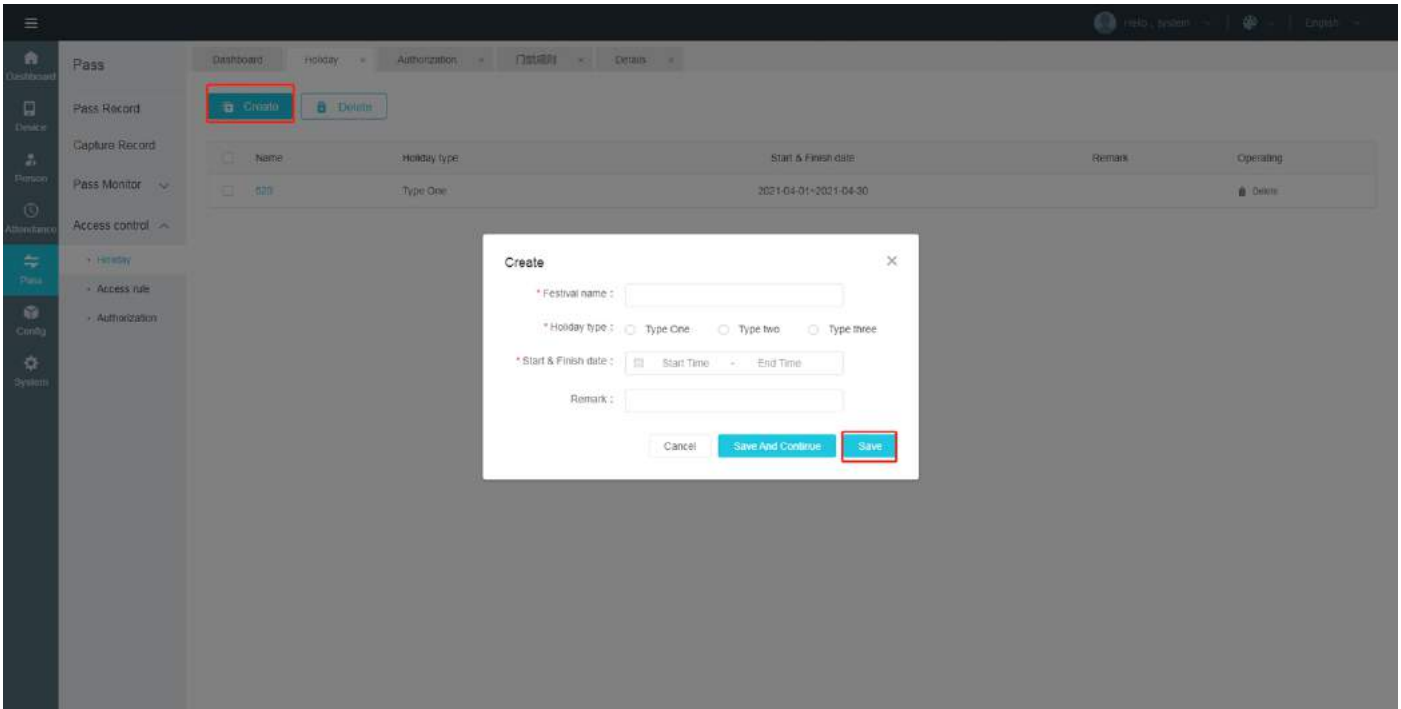
Click the corresponding holiday name in the type to open the holiday details pag

e and modify the details
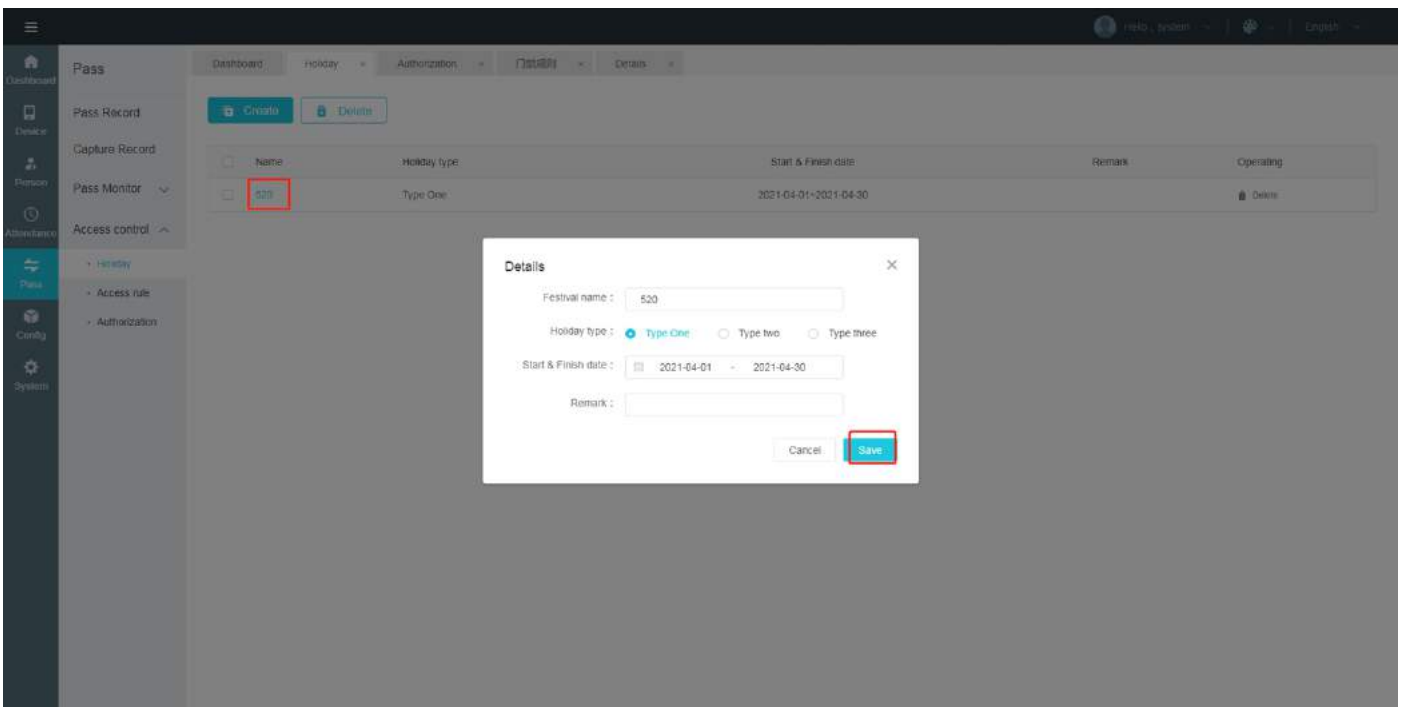
Click the delete button to delete
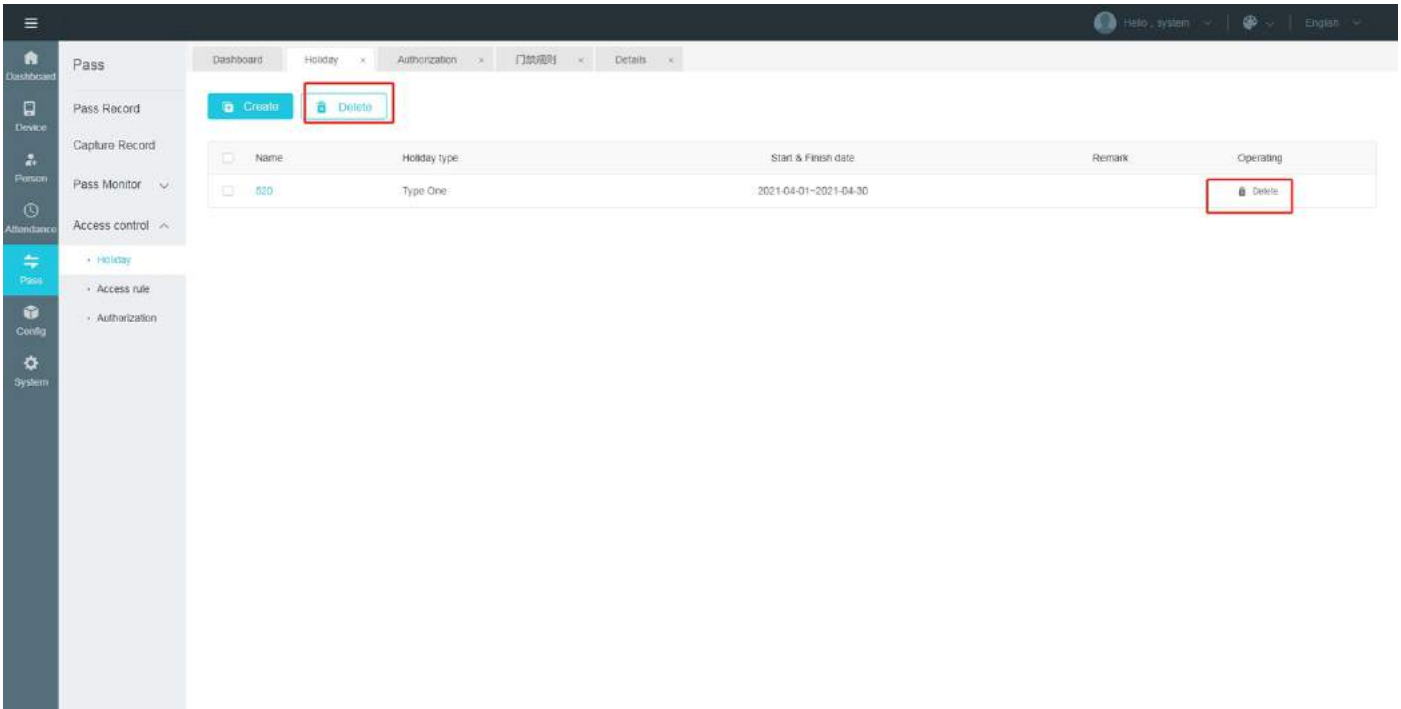
6.4.2 .Access control rules

Set the passable time period for the specified week or holiday type, and up to 3 time periods can be set in a day
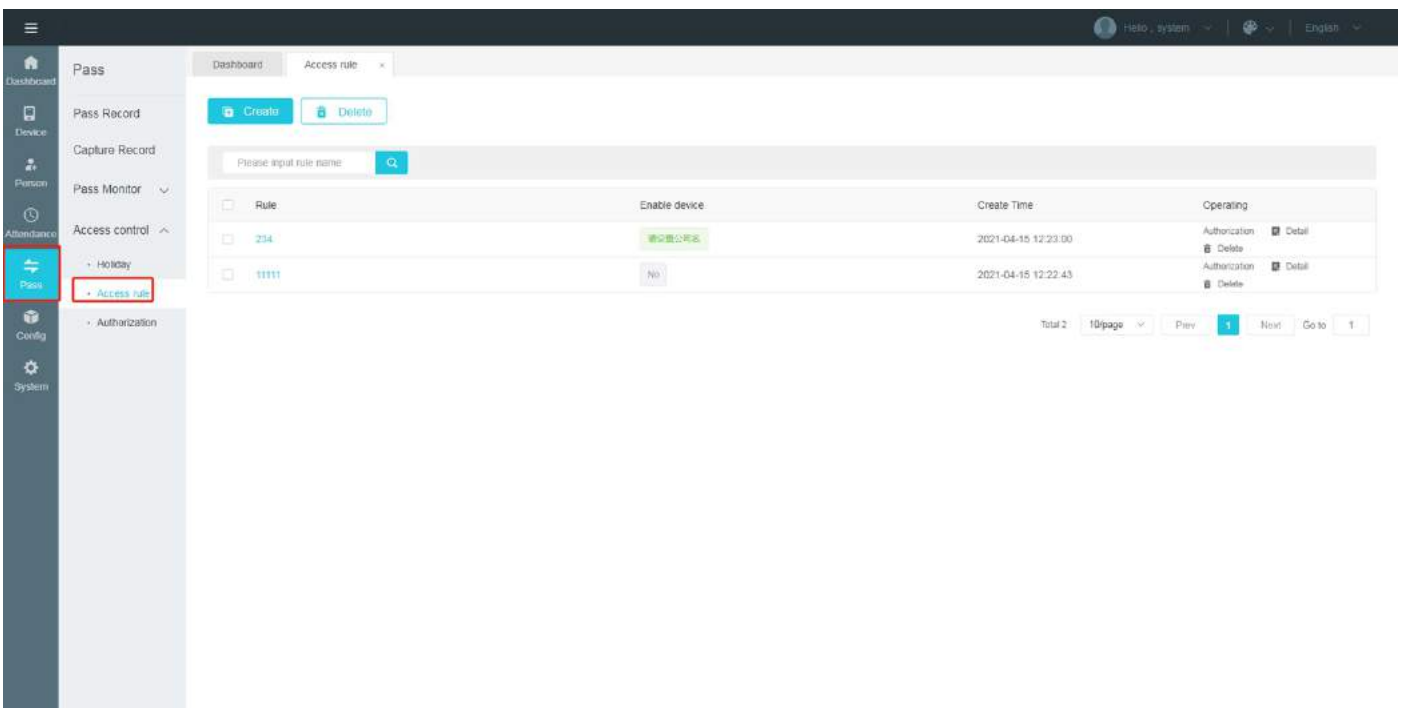
Click the New button to open the new access control rule page, fill in the rule name (required), set the pass time period for the day of the week and the holiday typ

e (after the holiday type is selected, all the corresponding types of time in the holida y management will be set), do not select The default is all-day access, select 00:00-00:0 0 to prohibit all-day access, and add up to three time period settings in a day

Click Rules in the access control rules list to open the details page, and you can modify the rules
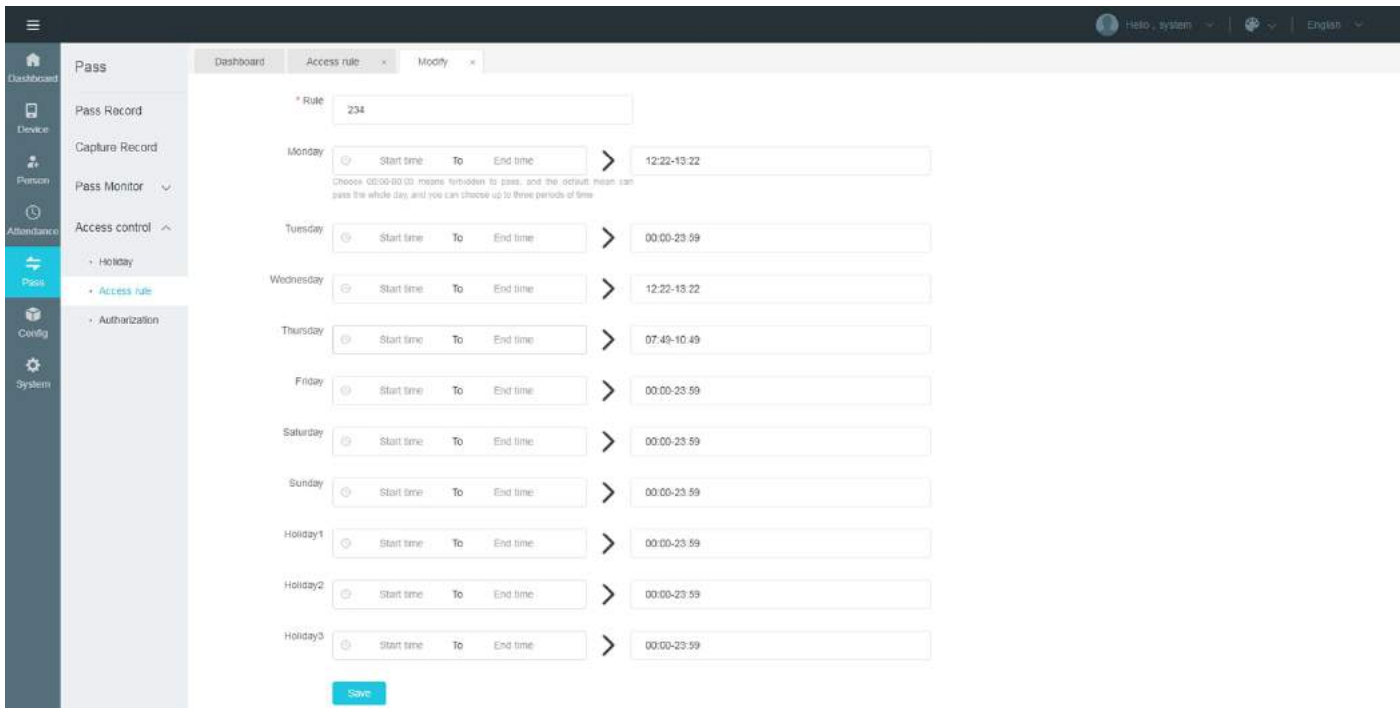
Click the Authorize button to authorize or deauthorize the specified device
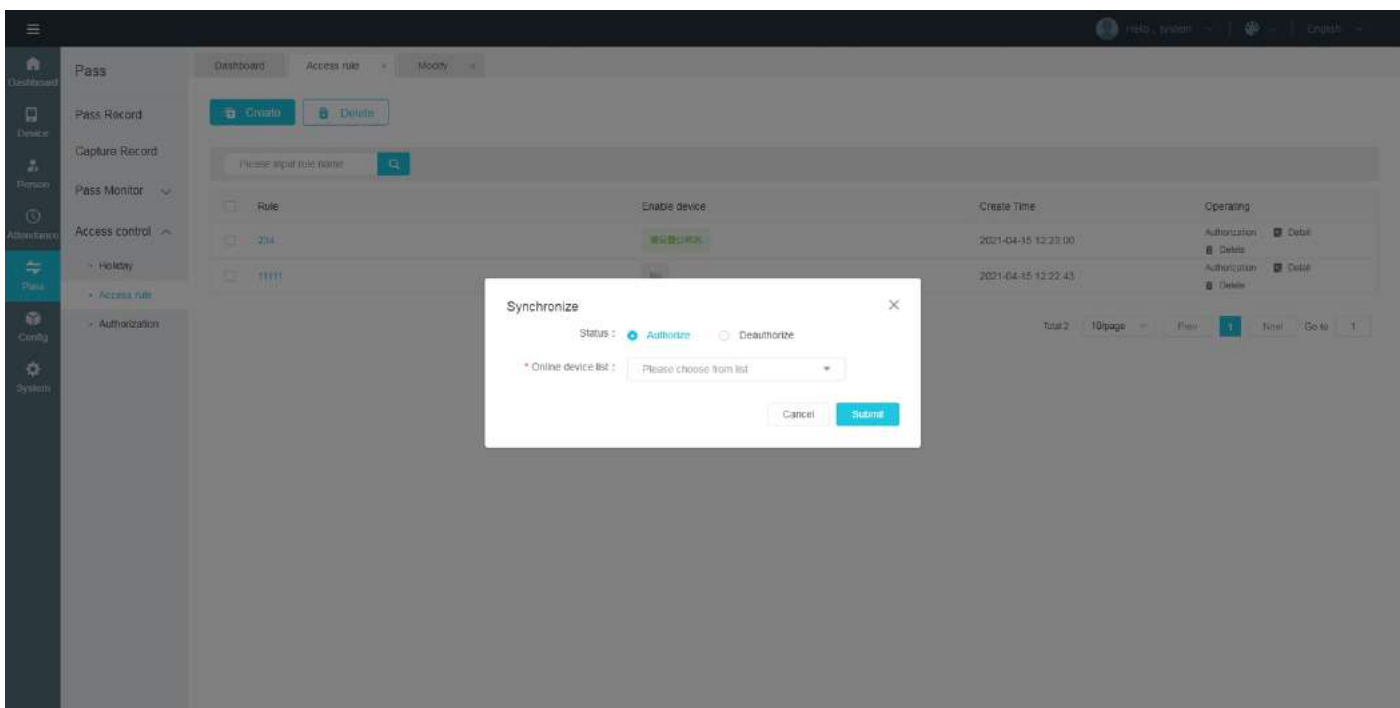
Click the Details button to open the rule details page
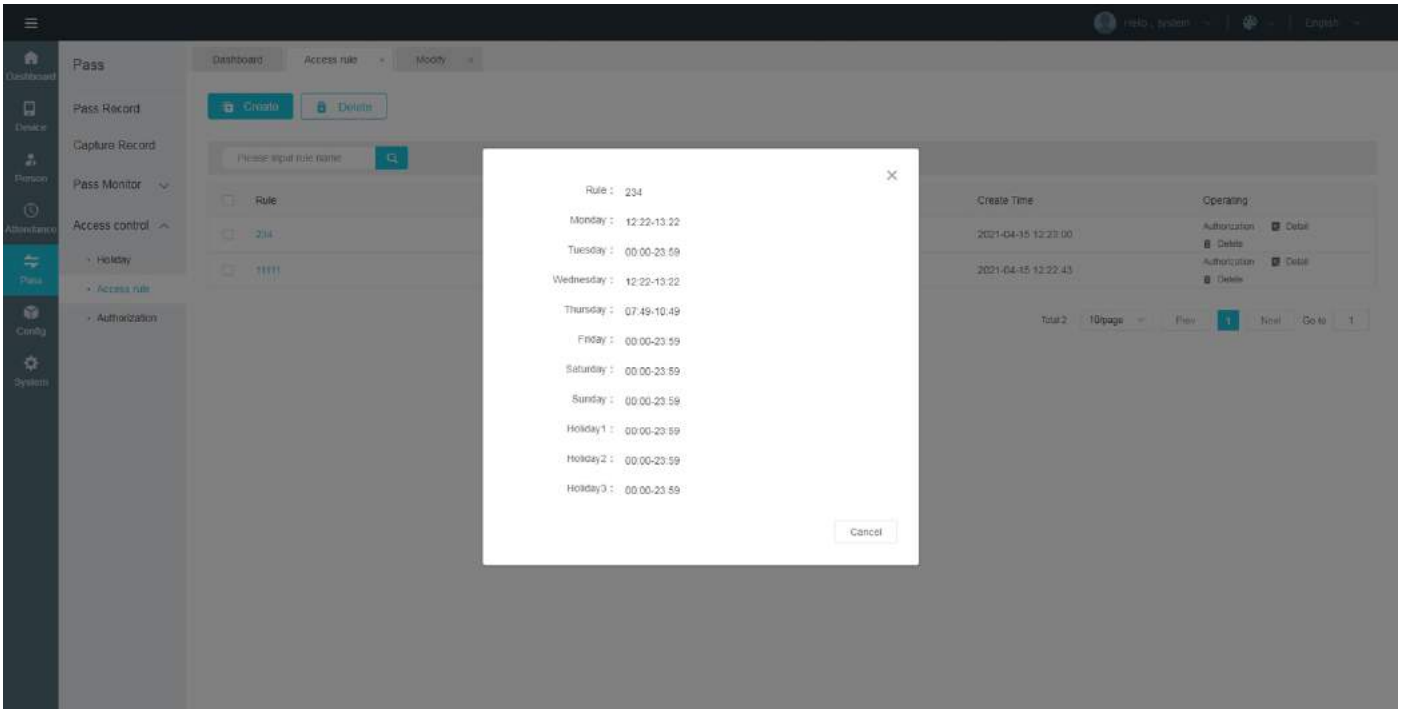
6.4.3 .Authorization information

View the authorization status of access control rules
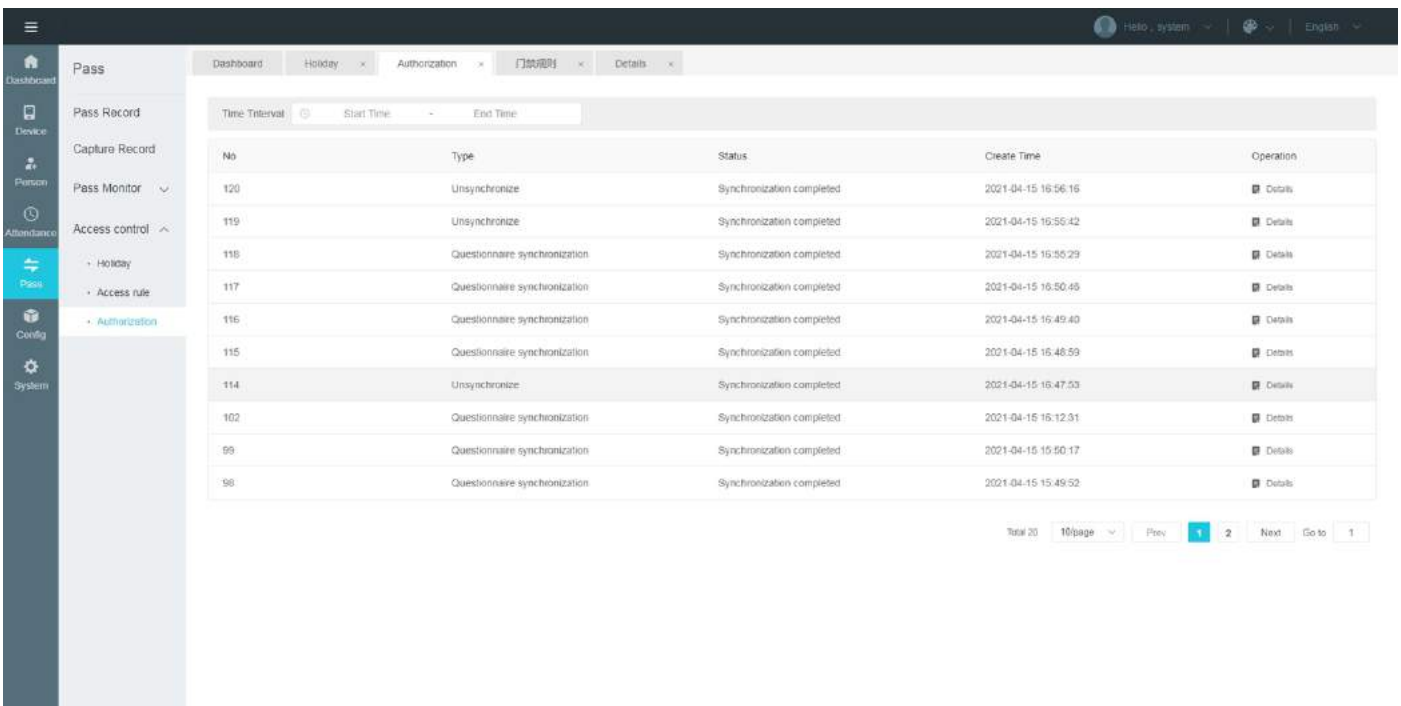
	Pass	Dashboard	Holiday	×	Authorization	×	门禁规则	×	Details	×

AuthSate All

	Access control rules	Device name	Status	Error message
	234	请设置公司名	Authorization succeeded	

Total 1   10/page   Prev   **1**   Next   Go to   1

7.System Management

7.1.Organization Management

[Organization Management] The module is used to manage the internal organizati onal structure of the enterprise and the management of enterprise user information. The hierarchical relationship is created and managed by the system or the enterprise administrator. The page is displayed as shown below:
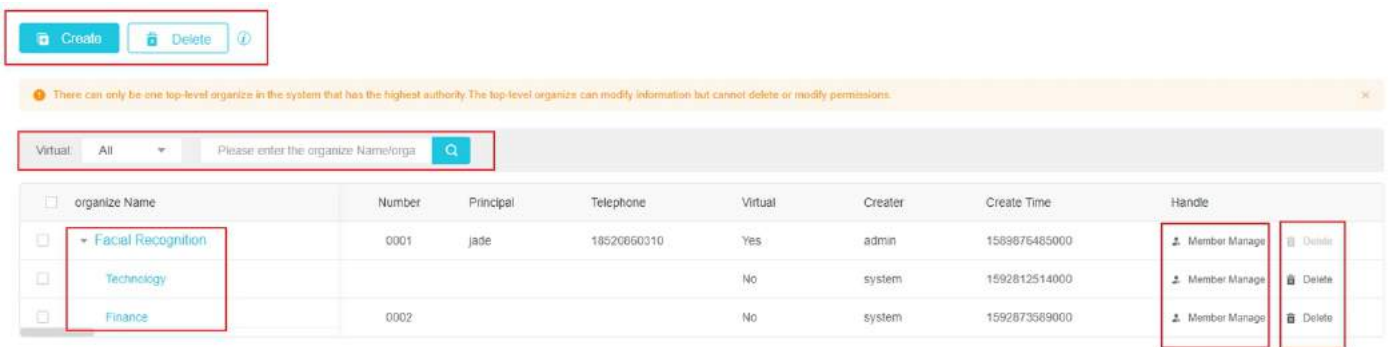
➤ Create an organization

1）Only one top-level organization can exist in the system, and that organization has the highest authority. The top-level organization can modify information, but cannot delete and modify permissions;

2） Click the New button to fill in the content and complete the new organization

Create

* Parent organize:	Please Choose ▼
* organize Name:	Please enter a new organize name
organize No.:	Please enter the organize No.
Principal:	Please enter the name of Principal
Telephone:	Please enter the telephone number
Fax:	Please enter fax
organize Description::	
Virtual:	○ Yes ● No

Cancel | Save And Continue | Save

Creater	Create Time
admin	1589876485000
system	1592812514000
system	1592873589000

➢ Member management

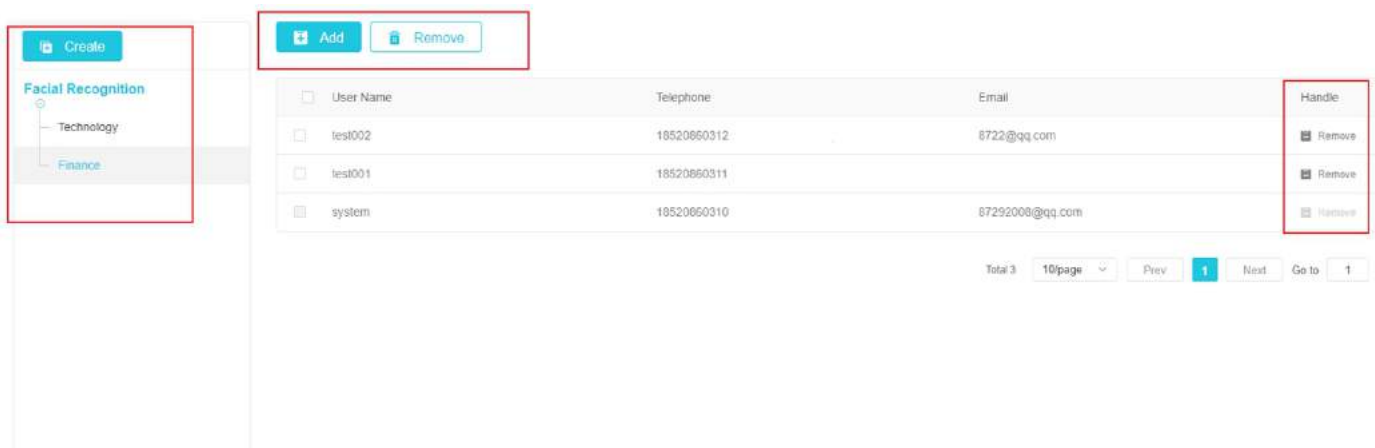Click "Member Management" in the operation of the displayed page to enter the member management display page. The left side of the page displays the tree-shaped organization structure that has been created. You can create new organizations and query members by organization on the left, and the members of the organization, that is, the basic information of the user, are displayed on the right

	User Name	Telephone	Email	Handle
☐	test002	18520860312	8722@qq.com	▦ Remove
☐	test001	18520860311		▦ Remove
☐	system	18520860310	87292008@qq.com	▦ Remove

Total 3 10/page Prev **1** Next Go to 1

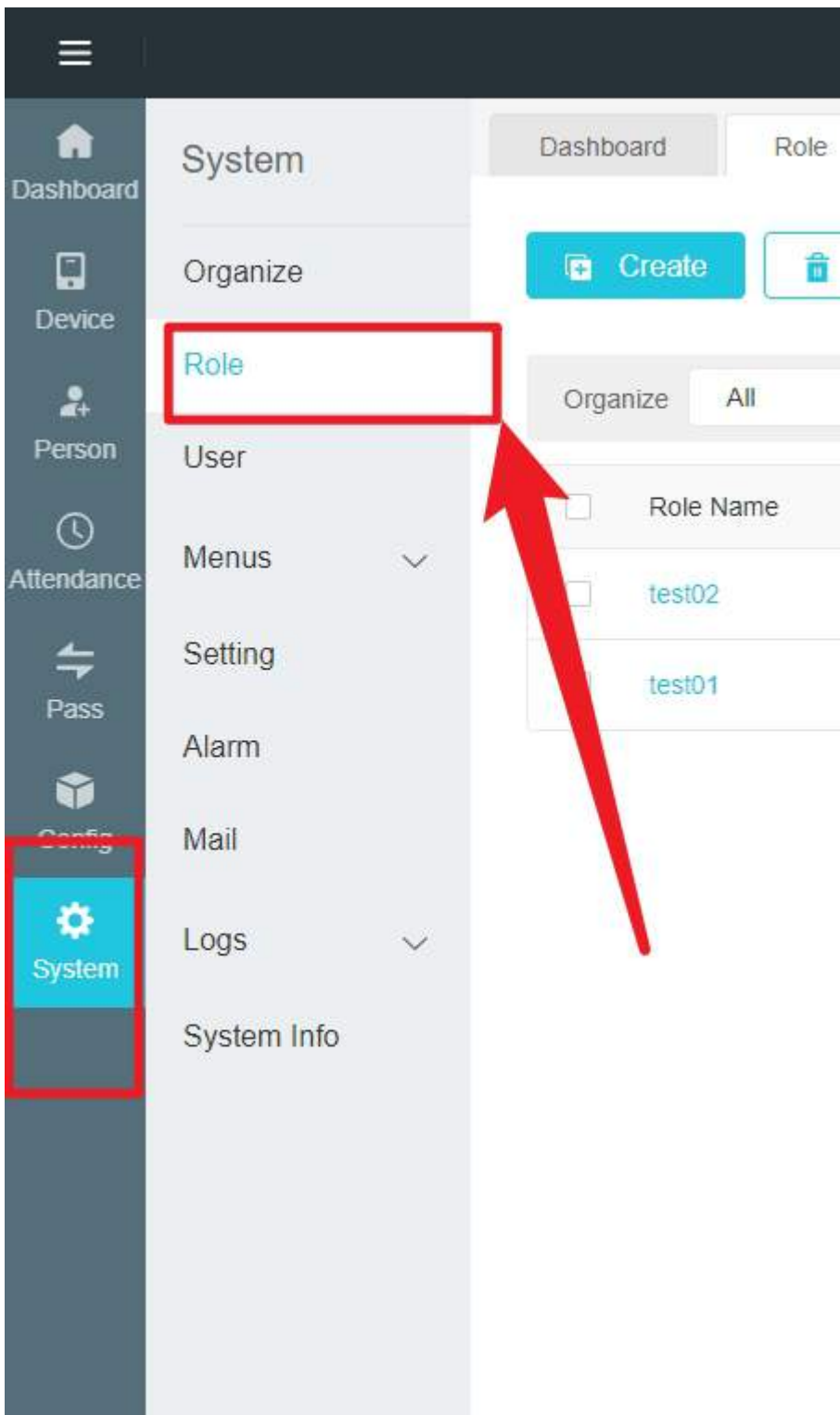Click the "Add" button in the member management, select the desired member from all users in the system, and click Save to add the user to the organization. Remove function (omitted)
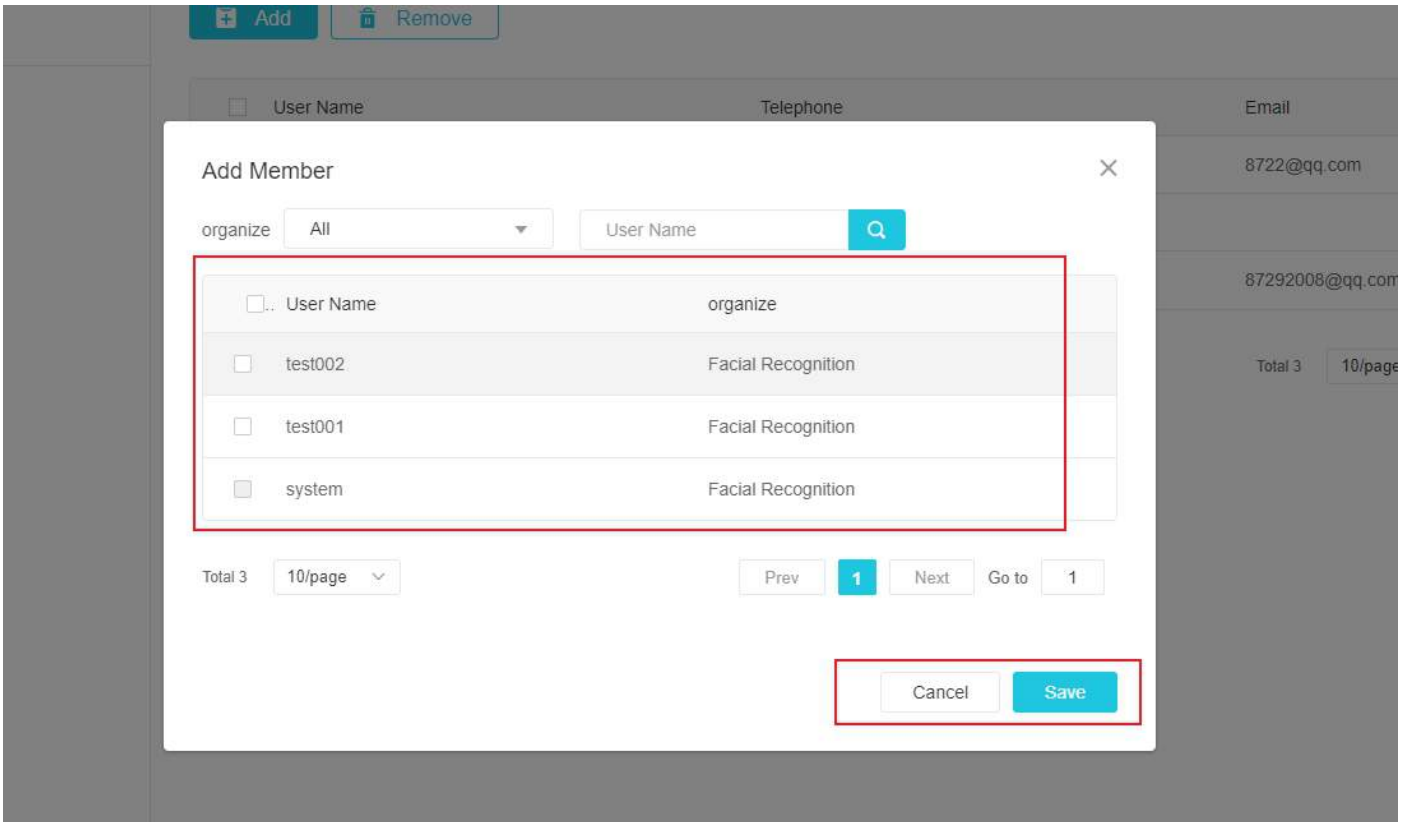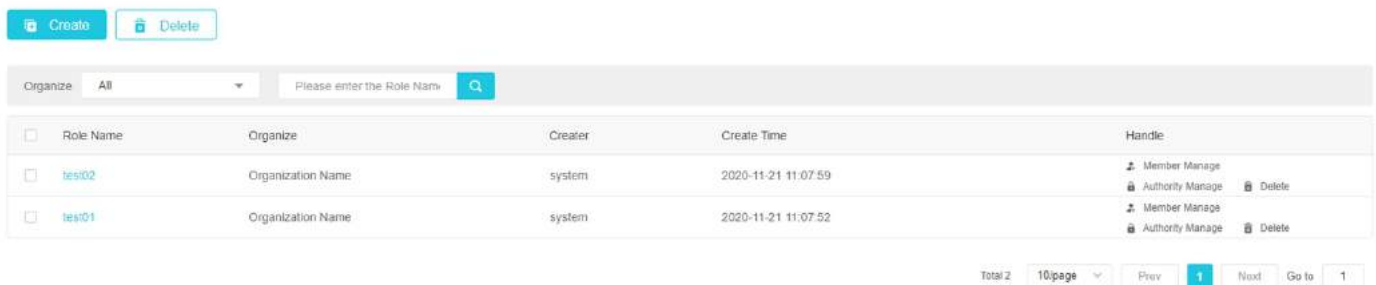
7.2.Role management

【Role management】 It is used to create and manage roles. Roles are used to control

the various business function modules and functional operations of users in the syste

m. It is composed of different functional operation permissions.

➢ **Role description**

Each enterprise can create one or more roles with different scopes of permissions, which are used to perform different functions for different users under the corporate organizational structure; what permissions does the corresponding role have, if the user belongs to this role, it also has the permissions of the role.

➢ **List of roles**

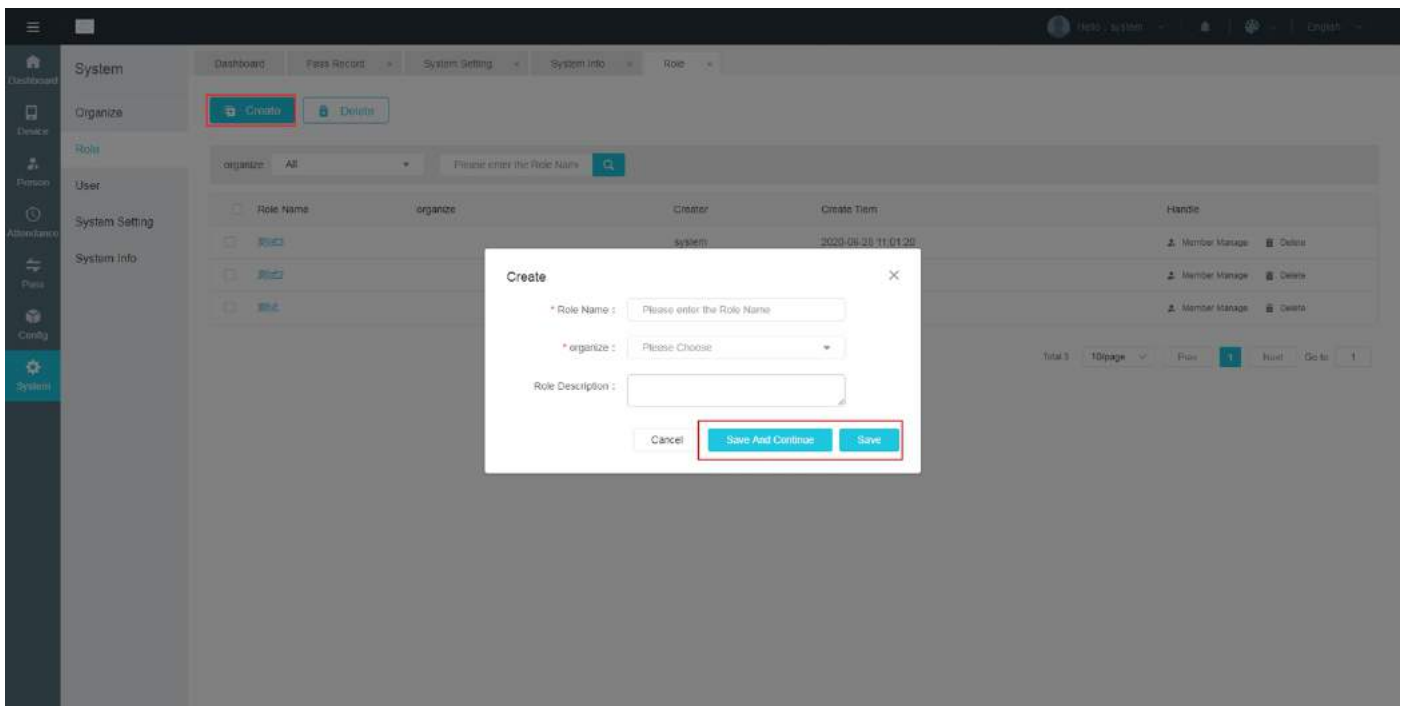The list of roles is shown in the figure below:

➢ **Creating Role**

enter【Role management】, Click on【Create】Button , Pop up 【Create】 page ;

Fill in the role name, and save the organization and role, and click the [Save] button to create a new role.

> ➤ **Role modification**

Click on【Role Name】enter【Role-Modify】page , Left and right to select the role to

be modified for the role list , Character information on the right , Editable role name ,

organize , Role description, click [Save] button after modification to save the modified infor

mation.
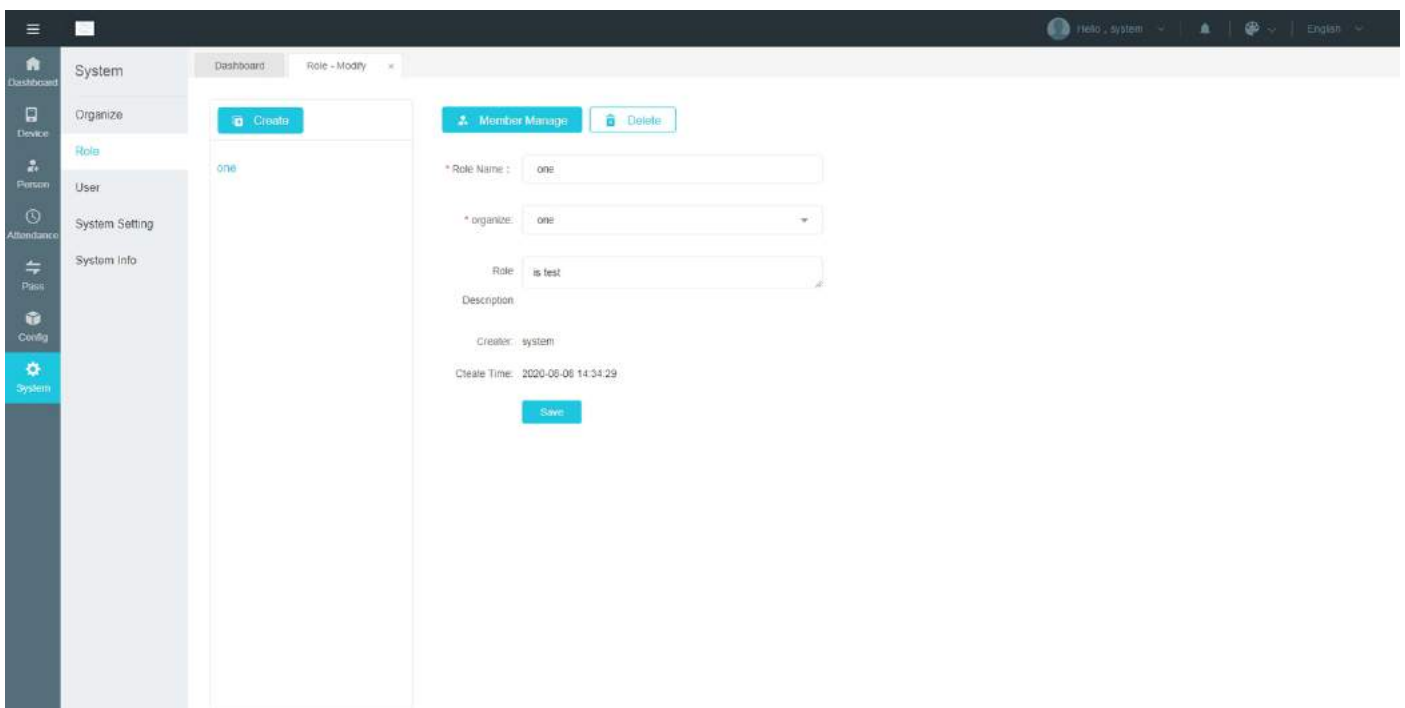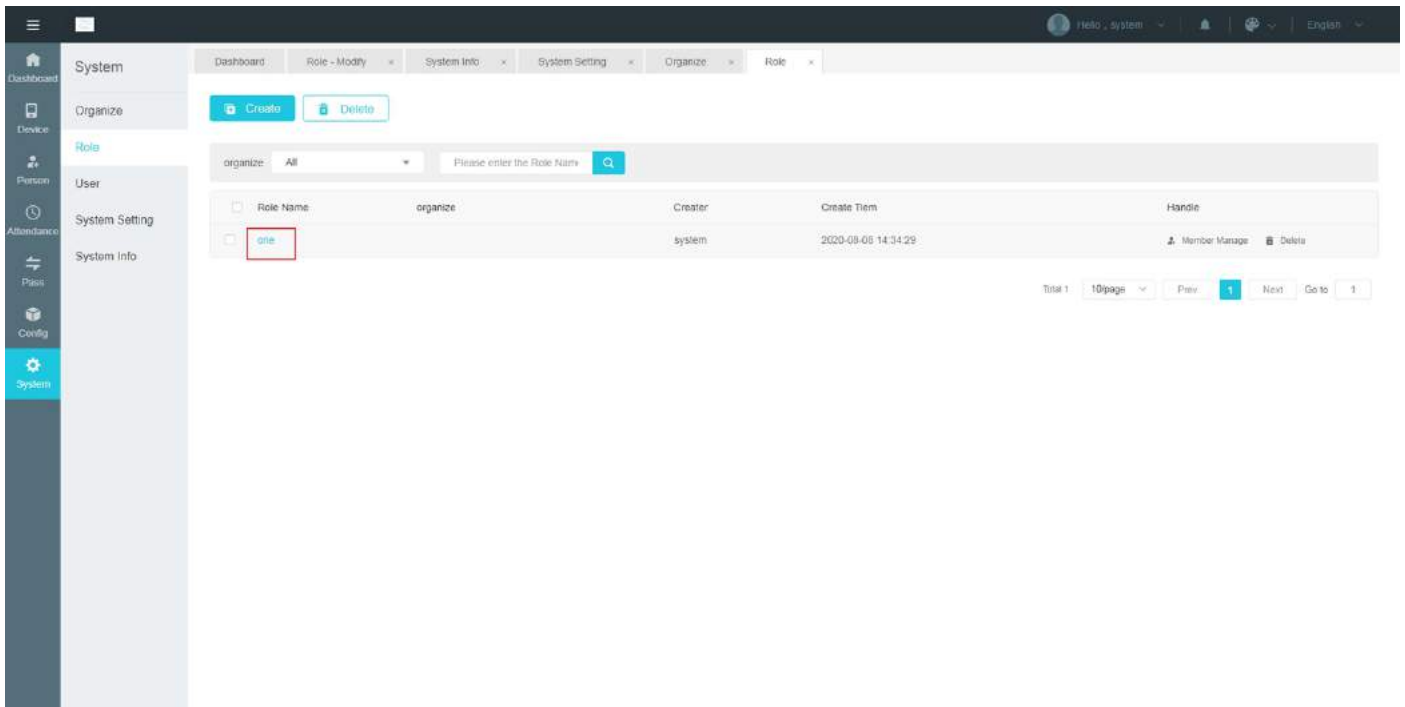
7.2.1.Role permission assignment

Click [Permission Management] on the role list page or click [Permission Manage ment] on the role editing page to assign role permissions
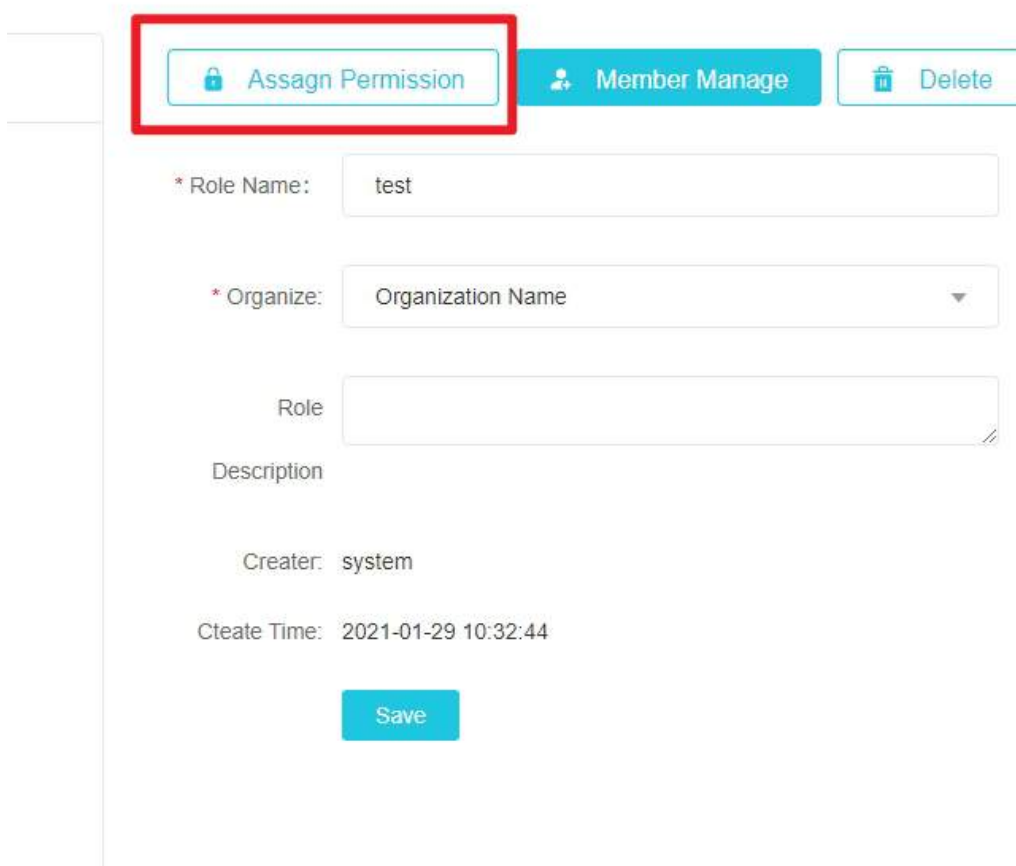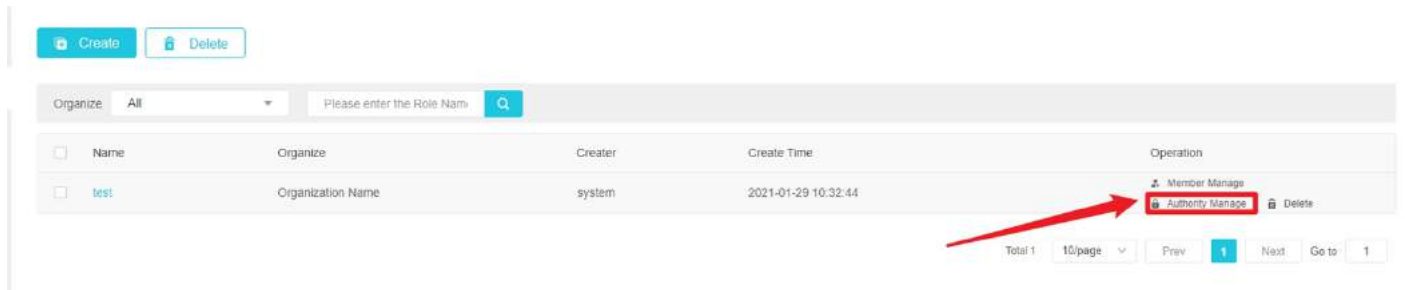
The authority assignment page is divided into menu category authority assignment and device group authority assignment

> **Menu permission assignment**

When assigning permissions, assign permissions based on the menu name. You c an access the menus with permissions, but you can't access the menus without permi ssions, as shown in the figure below.

The permission assignment page is as follows, and the permissions you have are checked
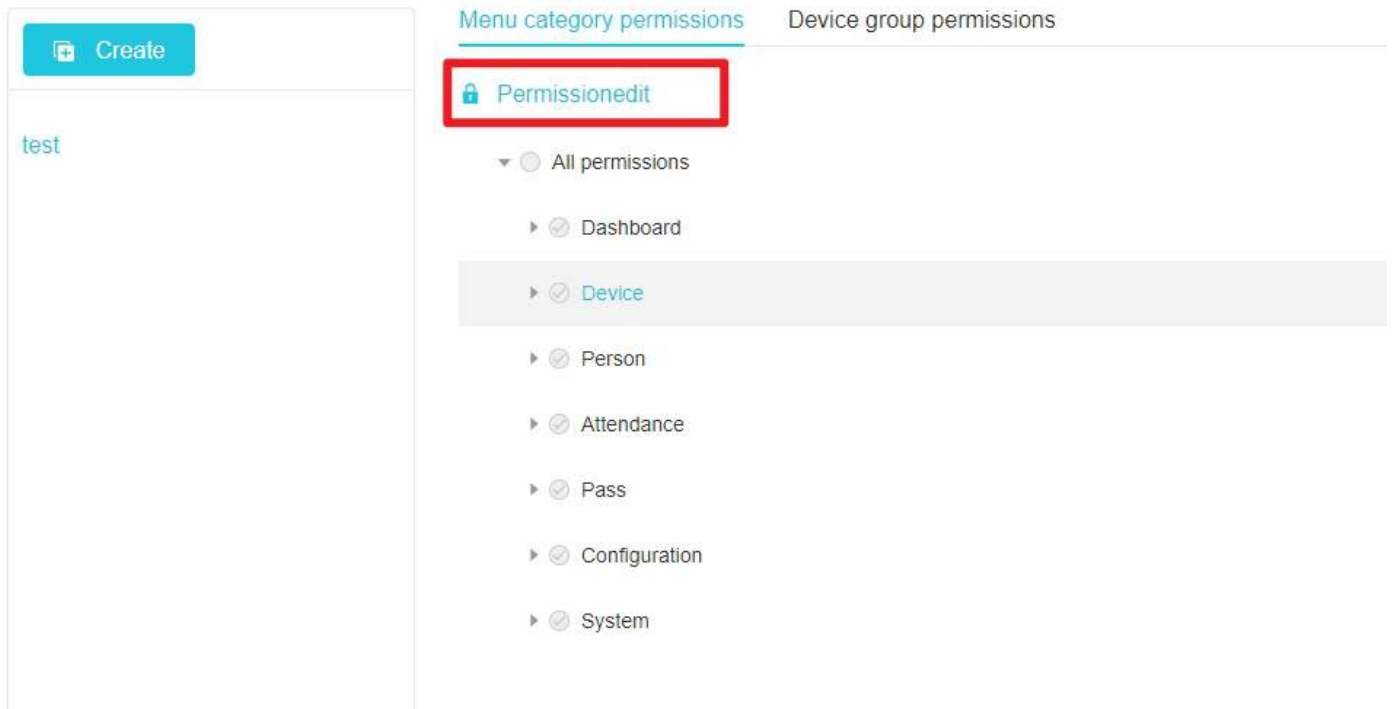
Click [Edit permissions] to check or cancel the corresponding permissions, and click [Save at the bottom of the page] after editing
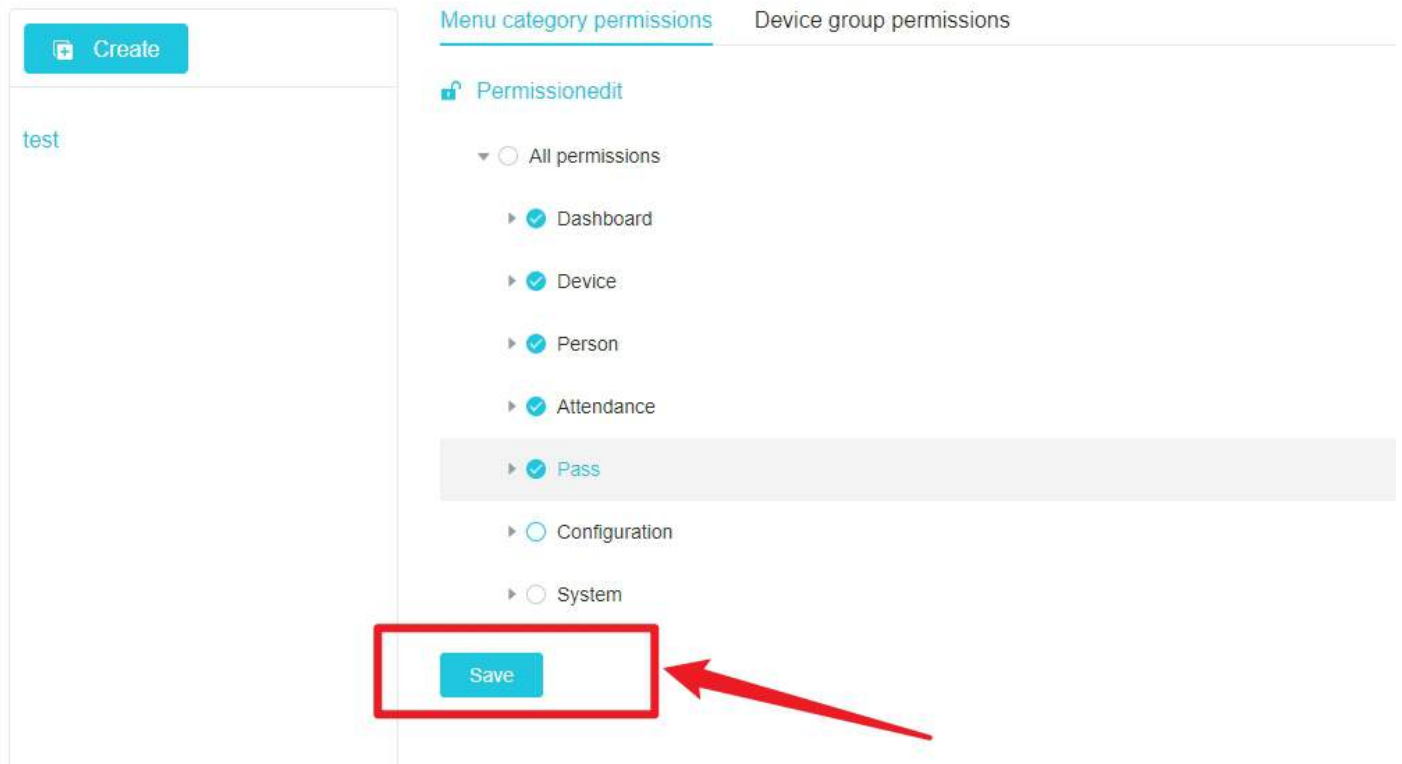
➢ ⬜ Assignment of device group permissions

The device group permissions are assigned to the device group as a unit, and the role is assigned to the device group permissions. If you have the viewing permission of the device group, you can view the device group and all the devices in the device group and modify and delete them. Without the viewing authority of the device, the device group will not be displayed in the device list, and the devices belonging to the device group will not be displayed.

The device group permissions page is shown in the figure below. The permissions you have are in the checked state. Select or cancel the device group and click Save to modify it.

7.2.2.Role Management-Member Management :

Click the member management in the operation bar of the role management list or click the【member management】button on the role modification page to enter the 【role-member management】page。
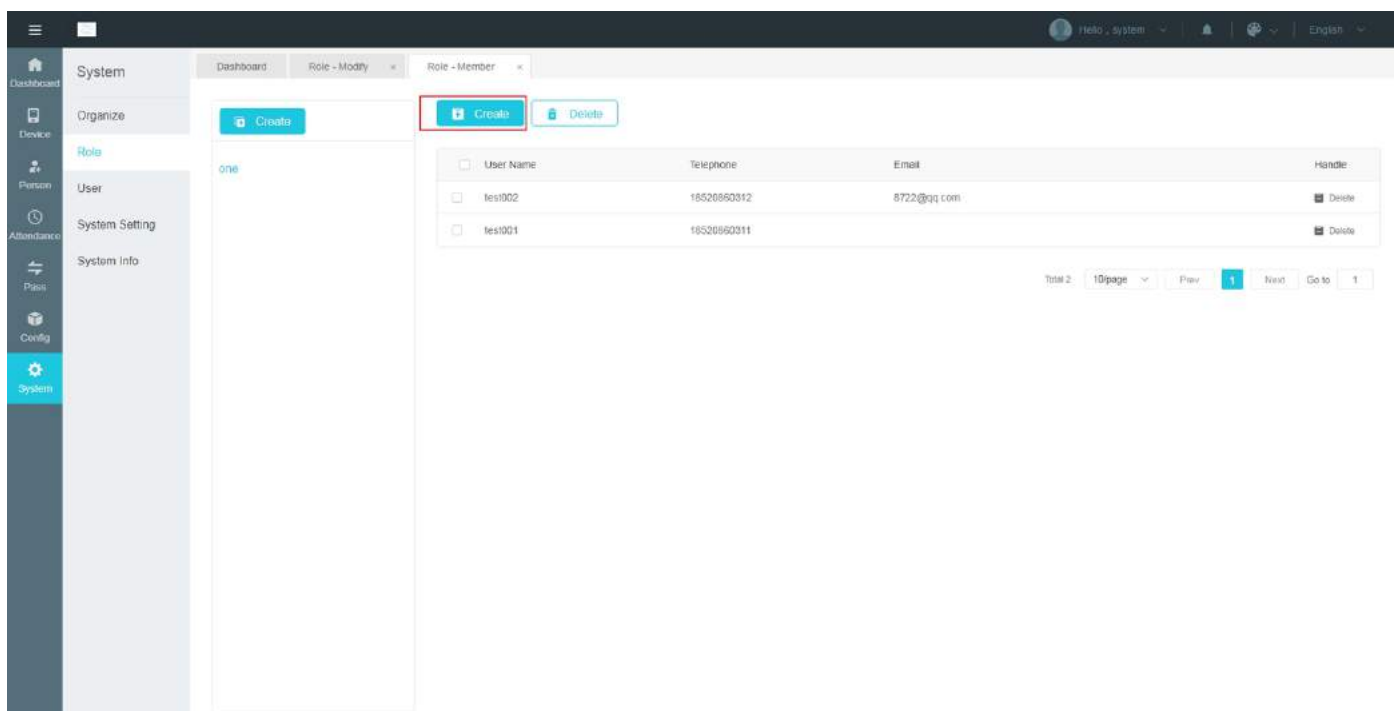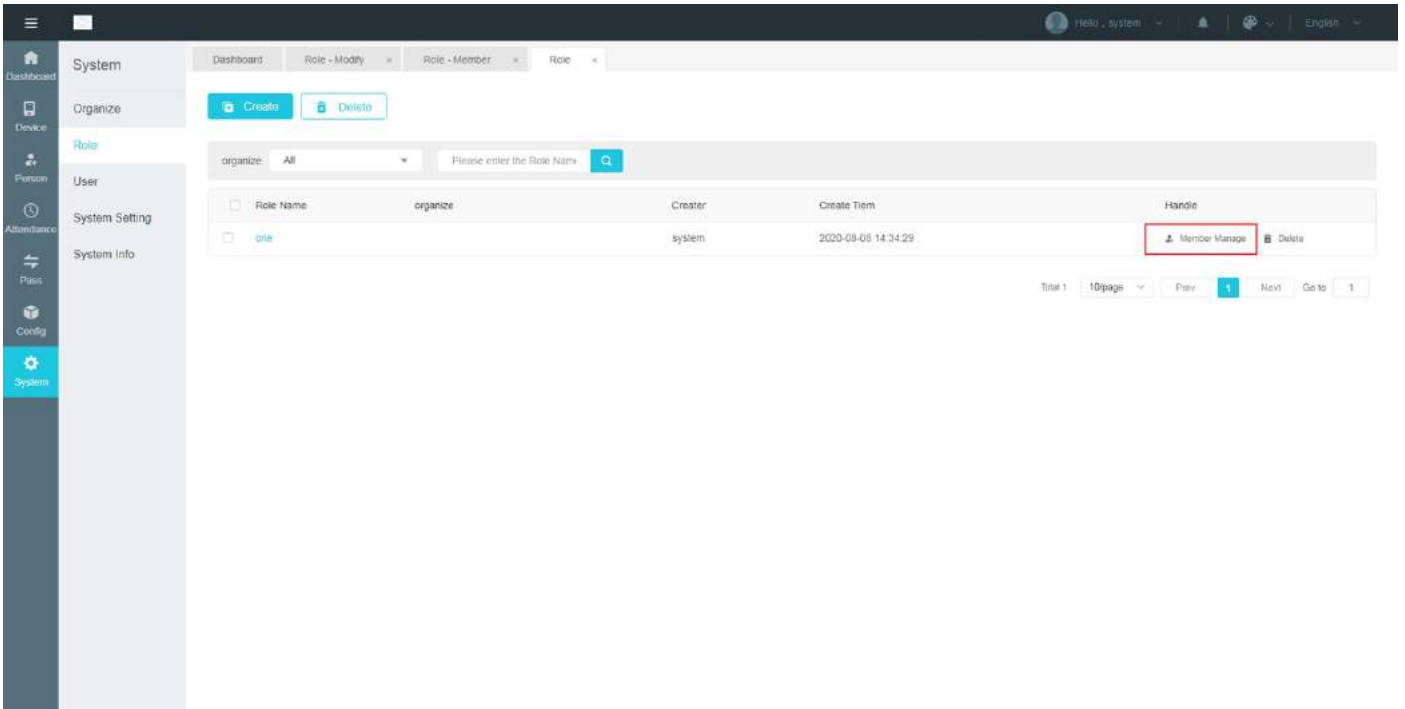
　　【Role-Member】interface , The left part is the role list, you can select the role, click the 【Create】 button above, and the 【Create】 pop-up window will pop up to create a new role.
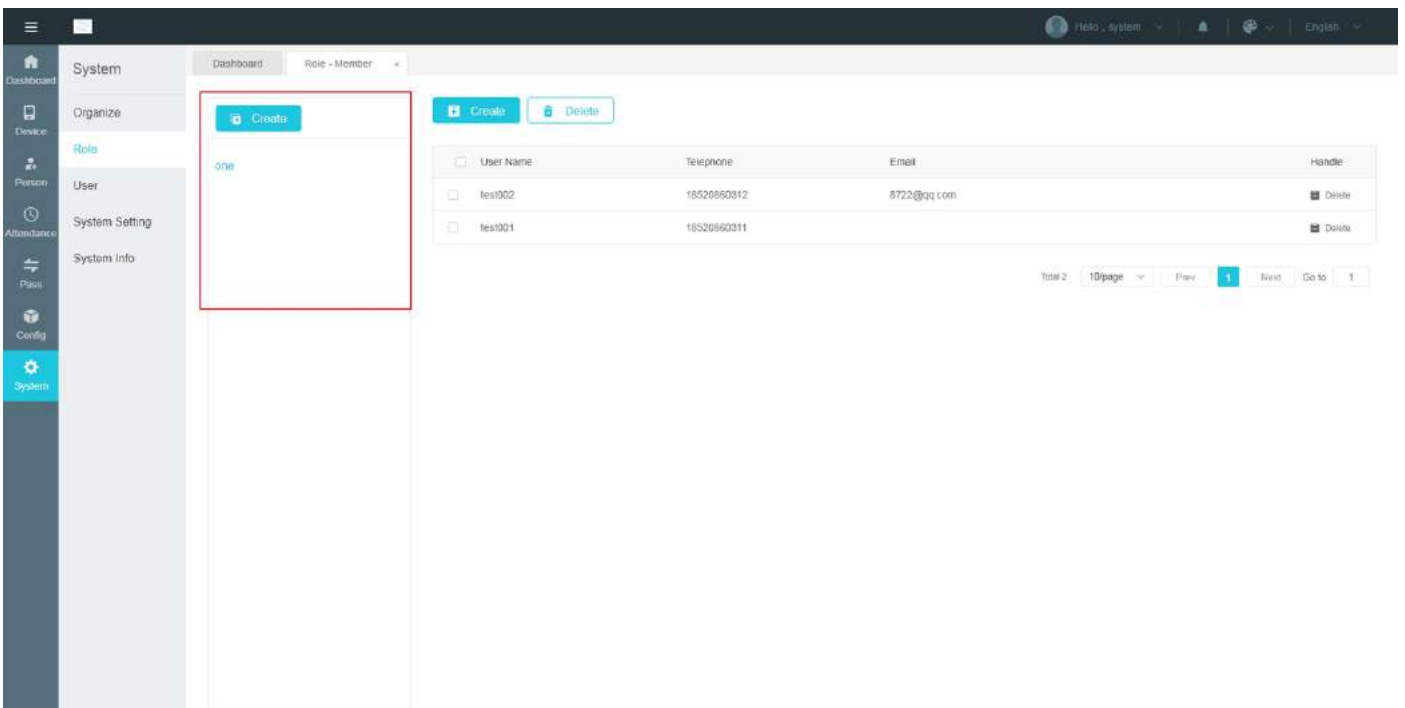
User add role

On the right is the user list, view the user information in the selected role, click t

he【Create】 button, the 【Add Member】 pop-up window will pop up, in the user list , select the user to add to the selected role。
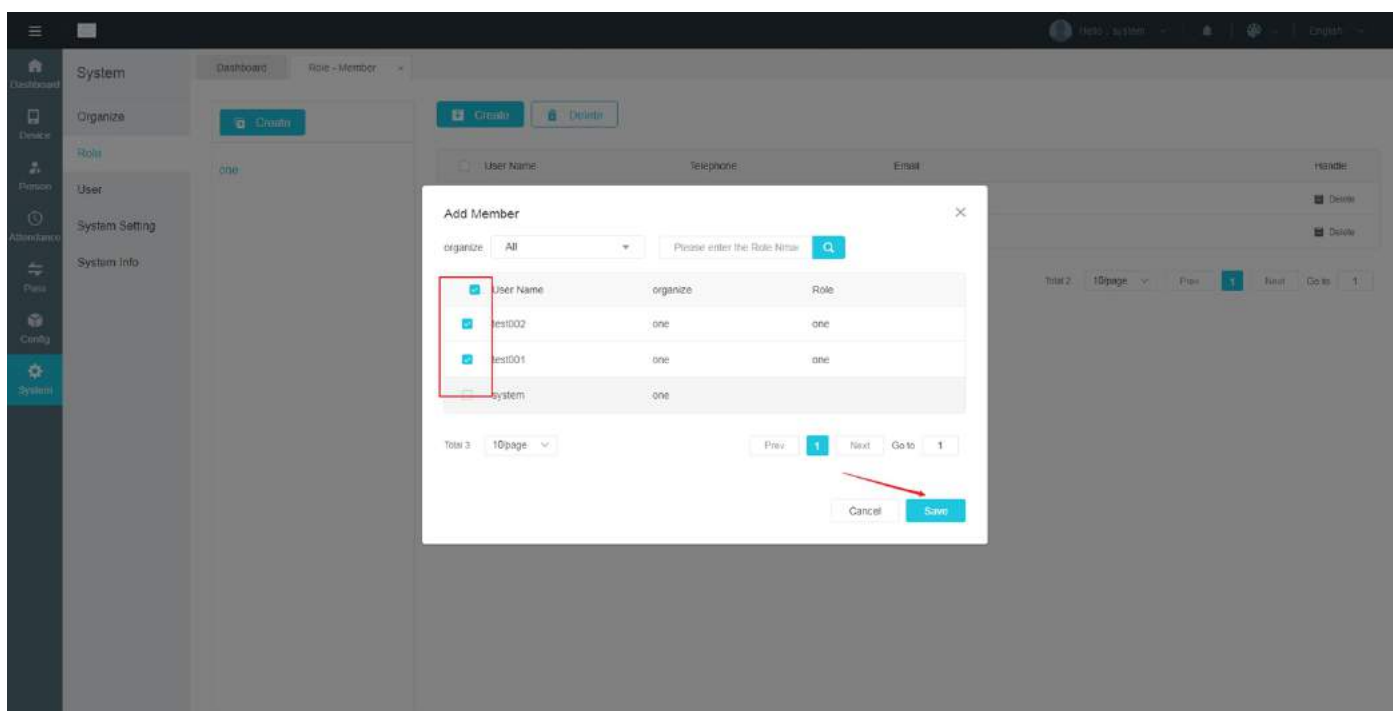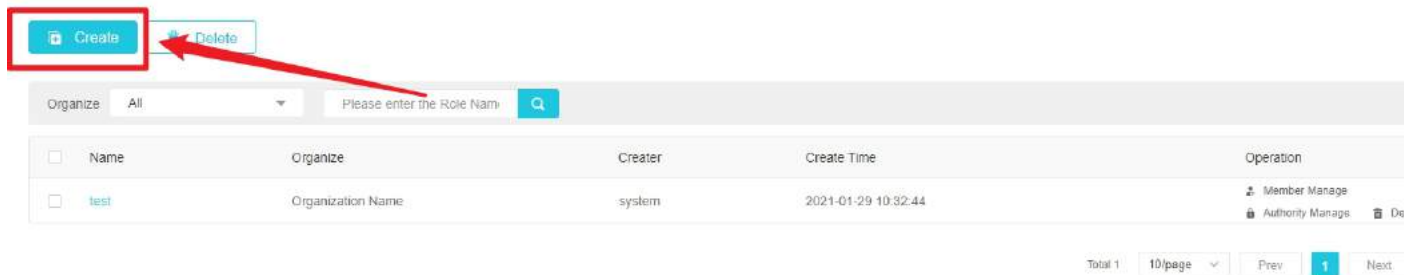
Delete user in role

Click 【Delete】 button to delete users in the role
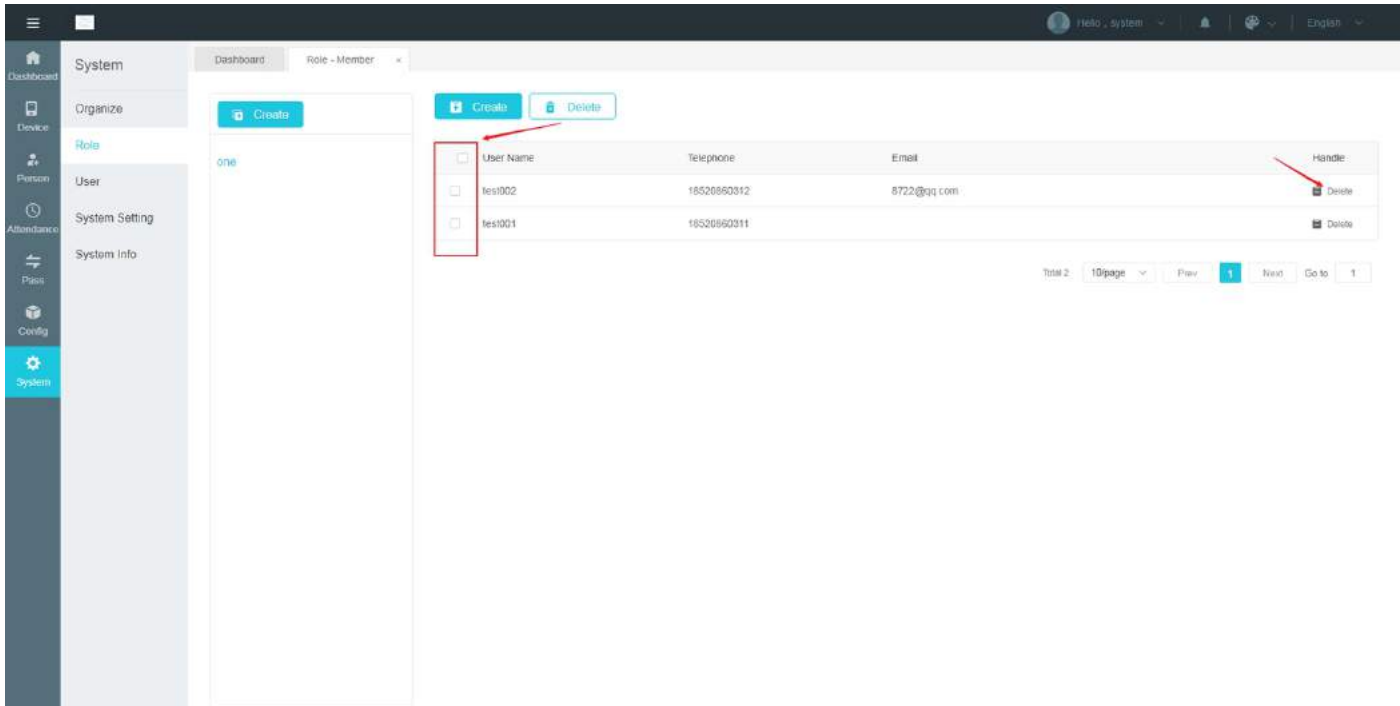
7.3.User Management

7.3.1.User permission assignment

Note: The top-level user system belongs to the top-level organization, does not b elong to any role, and has all permissions. This user can only modify part of the info rmation and cannot be deleted. In addition, the user is not allowed to change the rol e, organization, and authority assignment or modification of the currently logged-in a ccount.

User assignment permissions are similar to the steps of role assignment permissio ns. If the user selects a role, the user will also have the permissions that the role has .

Click [Authority Management] in the operation bar of the user list or the [Authori ty Assignment] button on the user modification page to enter the user authority assi gnment page

Permission allocation is divided into menu category permissions and device group

permissions

> ☐ **Menu category permission assignment**

When assigning permissions, assign permissions based on the menu name. You can ac

cess the menus with permissions, but you can't access the menus without permissions, as

shown in the figure below.

The permission assignment page is as follows, and the permissions you have are checked
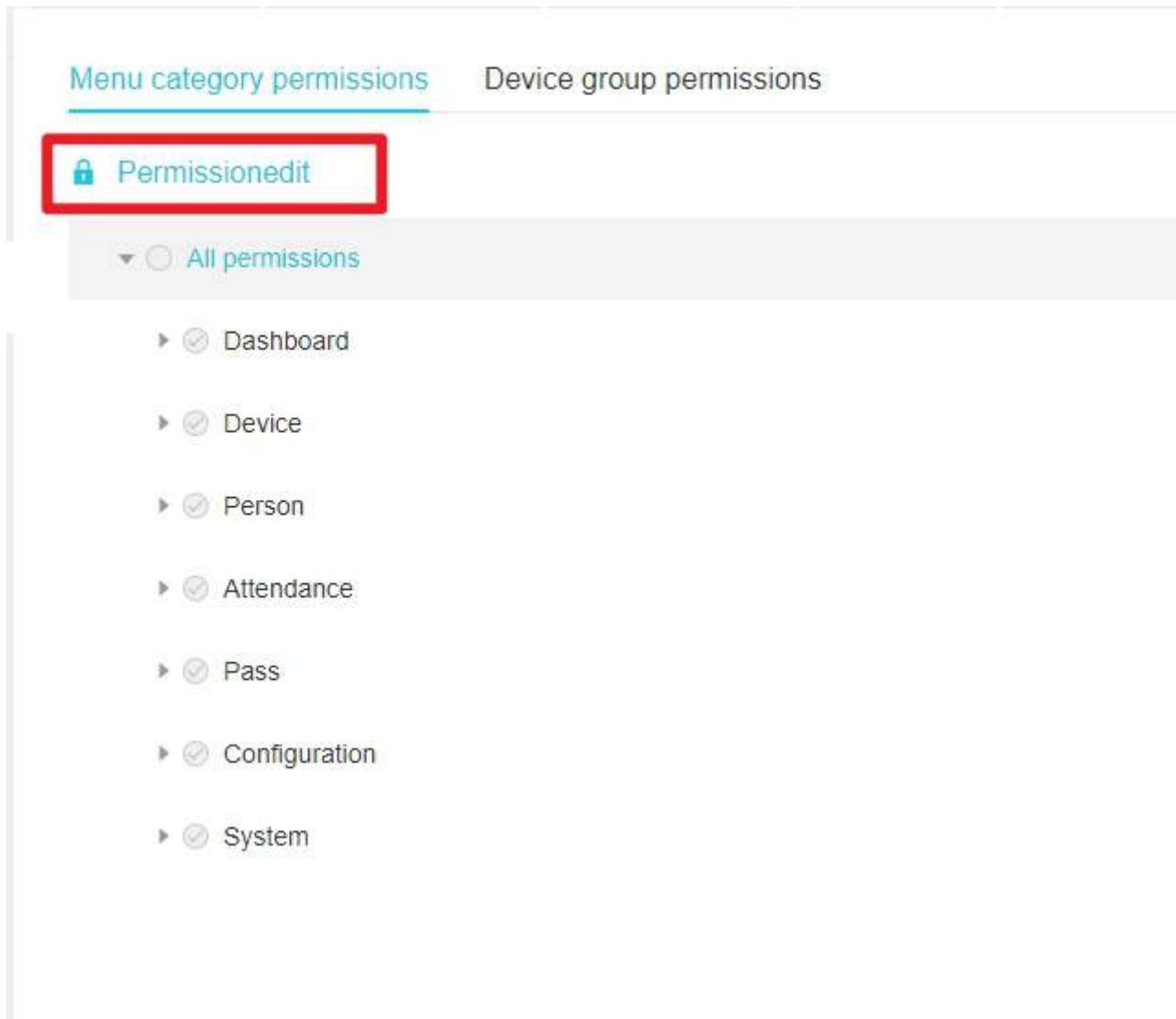
Click [Authorization Edit] to check or cancel the corresponding permissions. After editing, click [Save] at the bottom of the page

> ➤ ▢ **Assignment of device group permissions**

The device group permissions are assigned to the device group as a unit, and the role is assigned to the device group permissions. If you have the viewing permission of the device group, you can view the device group and all the devices in the device group and modify and delete them. Without the viewing authority of the device, the device group will not be displayed in the device list, and the devices belonging to the device group will not be displayed.

The device group permissions page is shown in the figure below. The permissions you have are in the checked state. Select or cancel the device group and then click Save to

modify successfully.

7.4.System settings

The system setting part is divided into body temperature configuration, general c

onfiguration, and other configurations

➢ **Temperature configuration:**

The default unit displayed in the system is Celsius, if you change it to Fahrenheit here, all temperature units of the system will be switched to Fahrenheit.

| Temperature configuration

* Temperature display type: ● Celsius   ○ Fahrenheit   ⑦   The system defaults to Celsius, please choose whether to display Fahrenheit according to the device configuration

➤ **Pass configuration:**

Save pictures of traffic records : By default on, pictures of traffic records will not be saved after shutdown.

Attendance switch is turned on by default. After it is turned off, the system will no longer perform attendance on employees, and the attendance analysis will become invalid and unavailable**.**

Time check record saving days: 120 days are saved by default.

Hide ID number: disabled by default, only the last four digits of the ID number in the pass record will be displayed after opening.

PassRecord saveDays   : is 0, which means it will be kept permanently. The number of days can be set, then the pass record in the system will only be kept for the corresponding number of days.

Daily limit: The default is 0, which means unlimited people. After setting, after the number of passers reaches the set number, the device with the access type of in and out will announce that the number of people has reached the upper limit, and the door will no longer be opened to allow people to pass.

| Pass config

Attendance switch: 🔵 Enabled ⑦

Hide ID number ⚪ Disabled

PassRecord saveDays: [—] [0] [+] 0 Default permanent storage

Daily person limit: [—] [0] [+] Enter an integer between 0-999999, 0 means unlimited

Displays the language selection switch：It is on by default, and the top right language selection bar is closed

| Language settings

Display language selection 🔵 Enabled

Other configuration： Set system logo, login page logo, system header logo
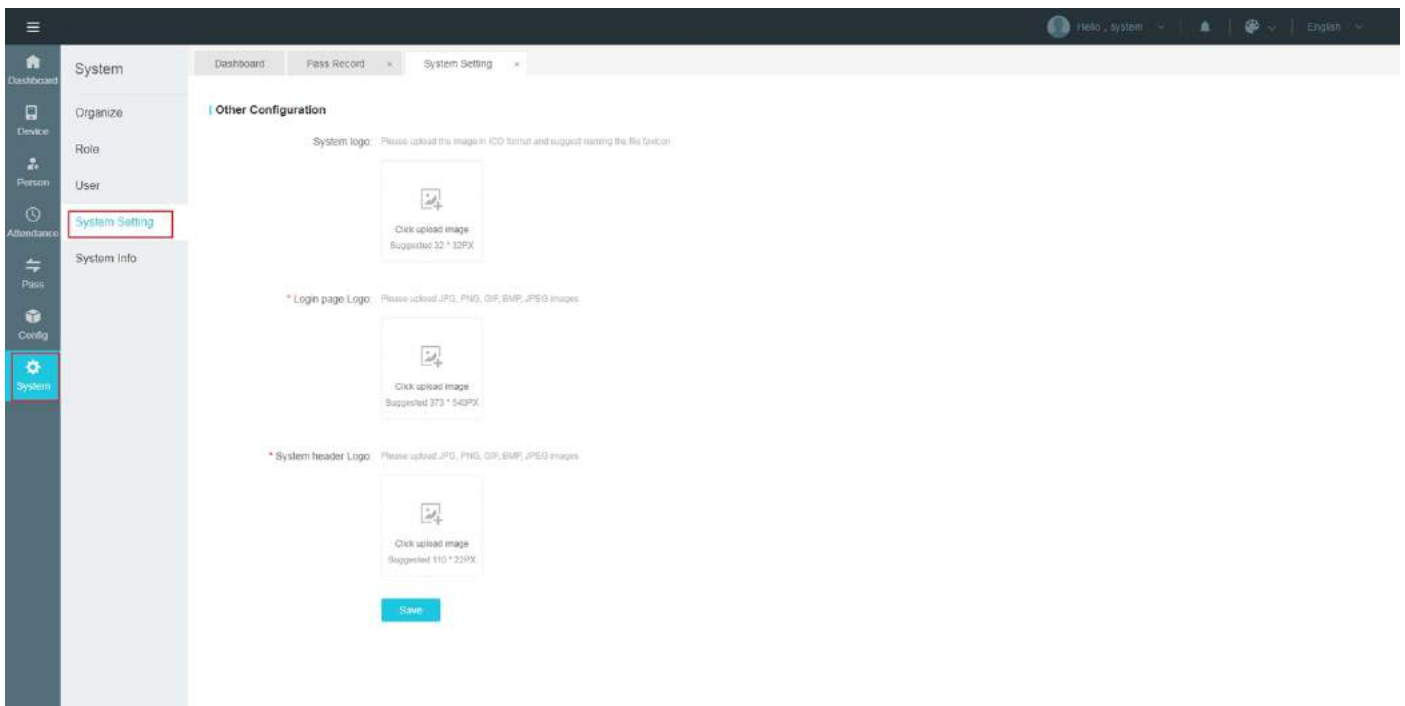
System identification：

【Format size limit】Support ico format , The recommended size is 32 * 32 px, and

the recommended file name is favicon ;

log in page Logo :

Click upload image
Suggested 32 * 32PX
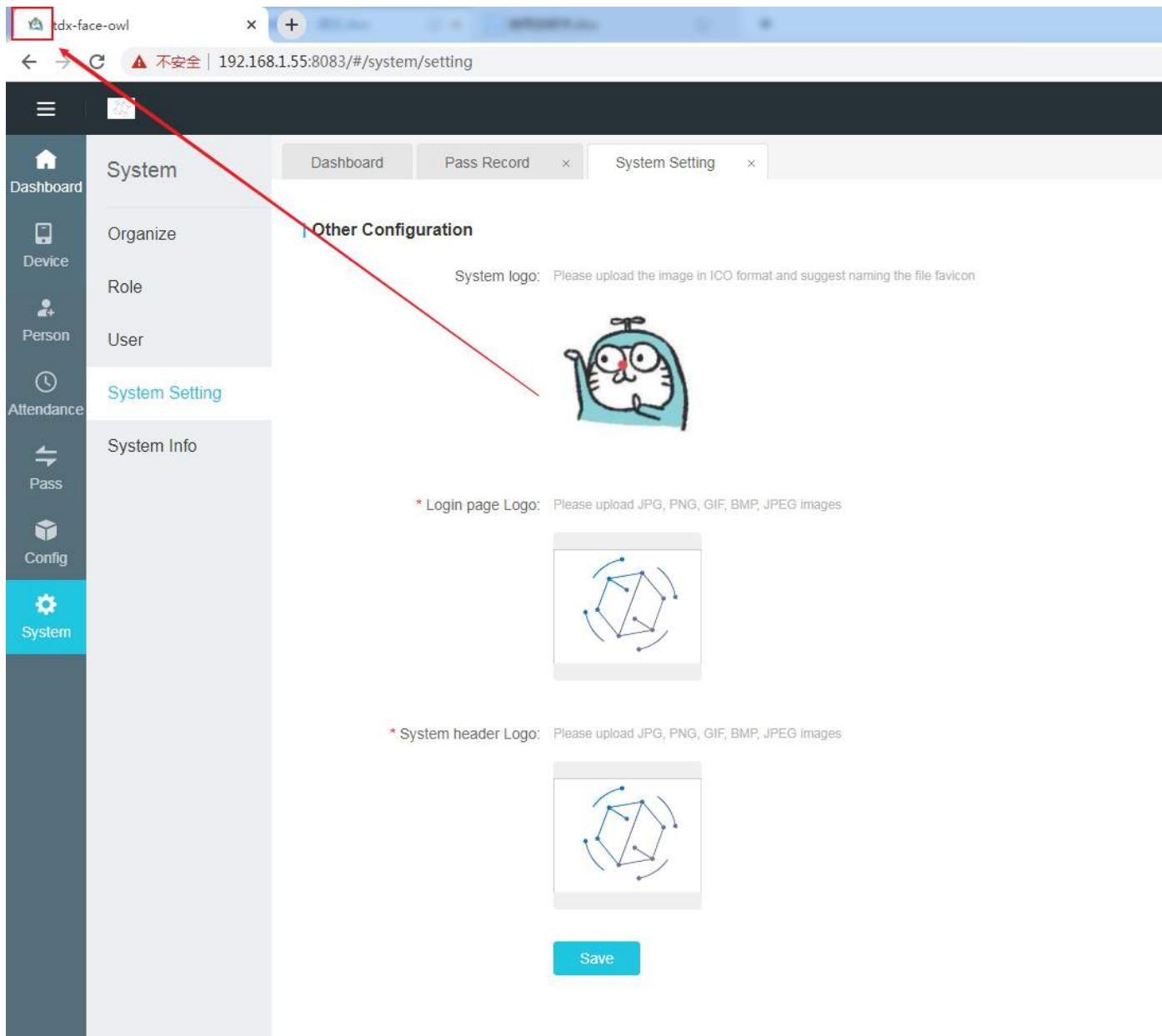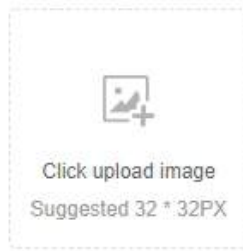
Background image of login page: Please upload JPG, PNG, GIF, BMP, JPEG images

System header Logo: Please upload JPG, PNG, GIF, BMP, JPEG images

【Format size limit】Support jpg，png，gif，bmp，jpeg format，Suggest 373 * 540 px；
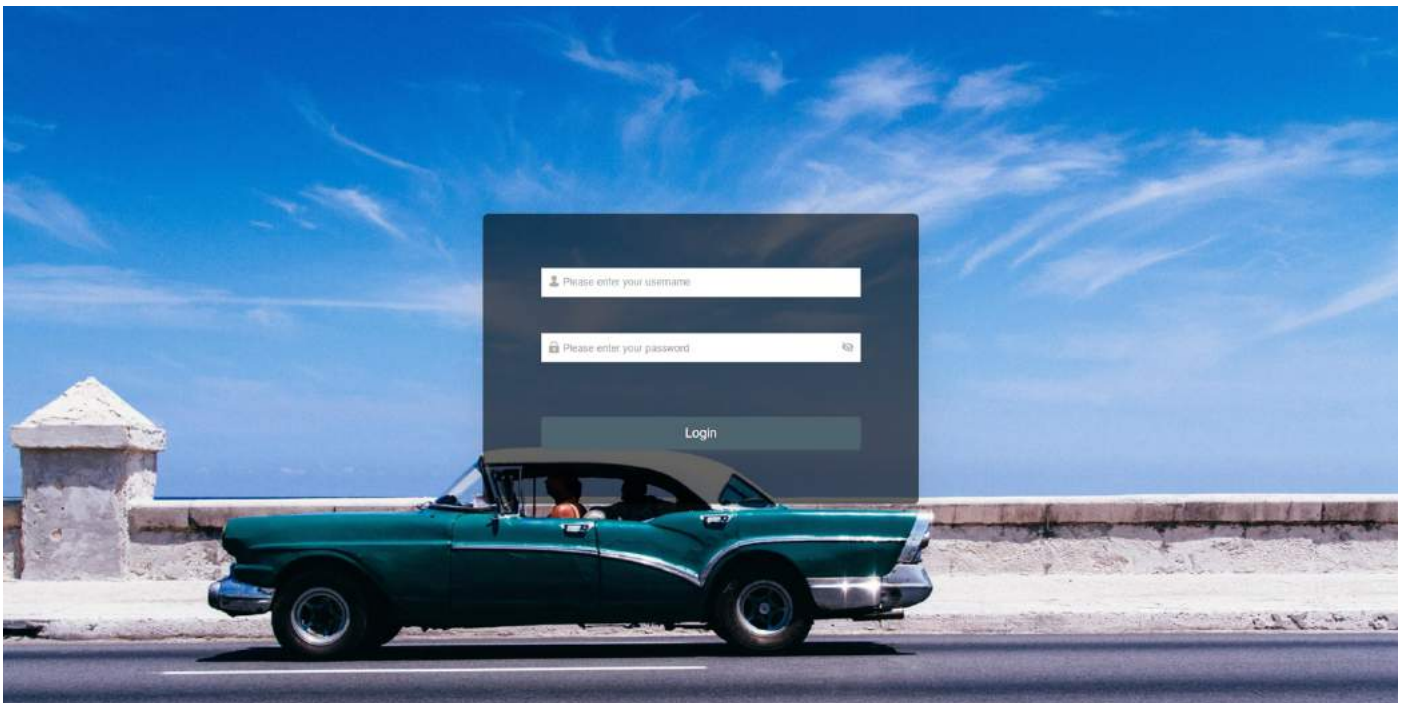
System head Logo：

【Format size limit】Support jpg，png，gif，bmp，jpeg format，Suggest 110 * 22

px；
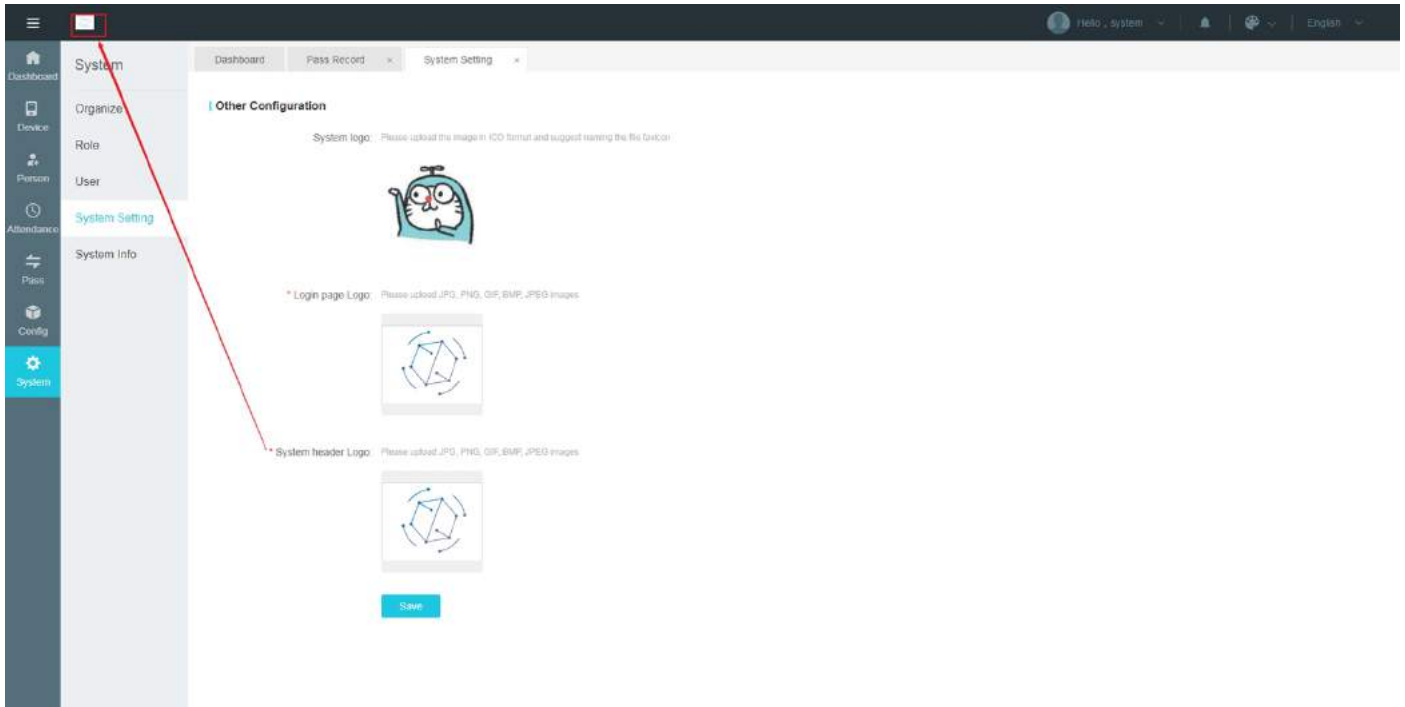
7.5.Alarm settings

Alarm settings Set the recipient address of the email, and the conditions for sending the email, such as sending emails at high temperature, sending emails without wearing a mask, sending emails from the blacklist, etc. The sending mailbox is set in 7.6 Mail Service Settings. If you want to use any function of email alarm, you need to fill in this part of the alarm settings and the 7.6 Email service settings.
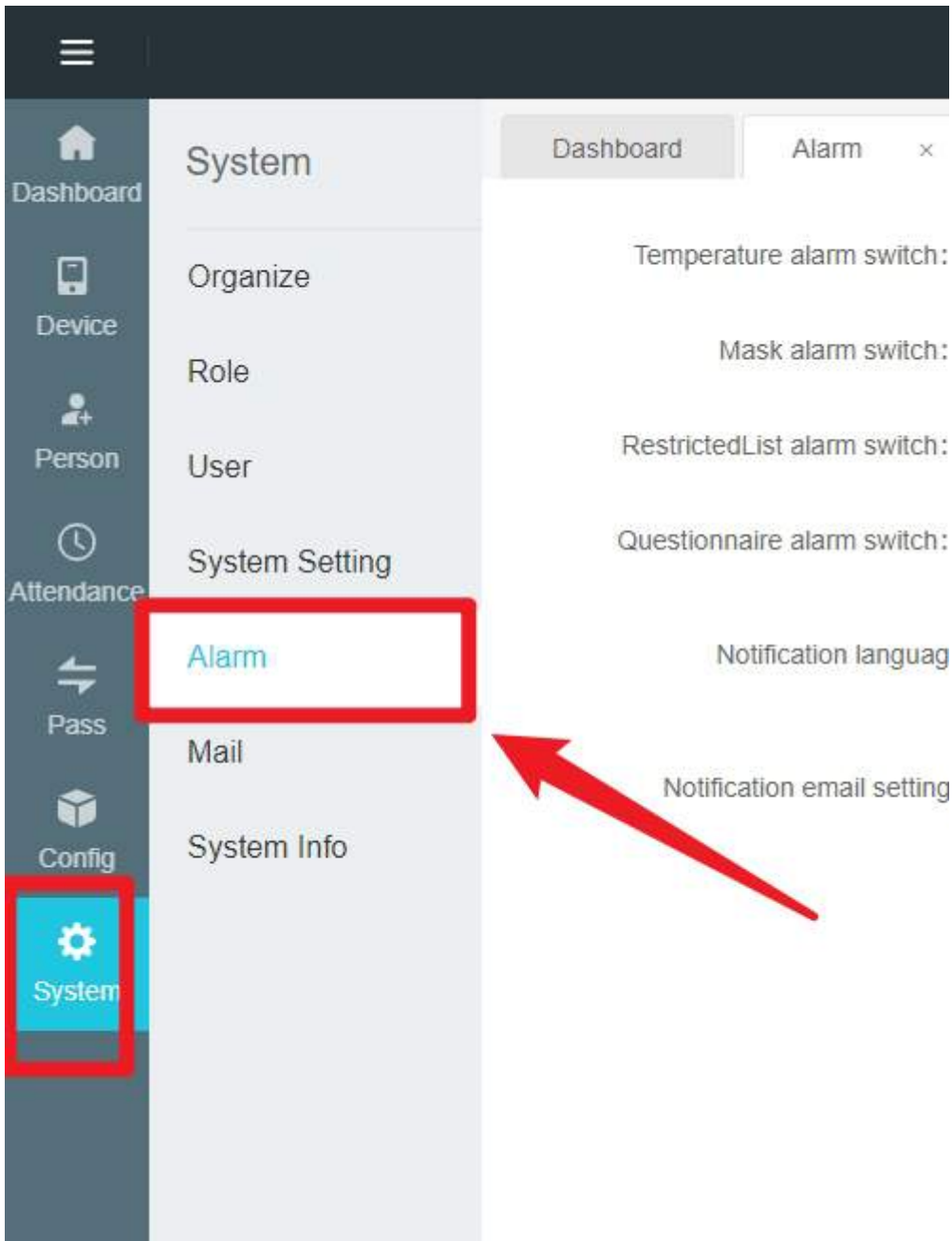
7.5.1.Global Alert

Click [System] [Alarm Settings] to turn on or off the alarm function. The page is as follows :
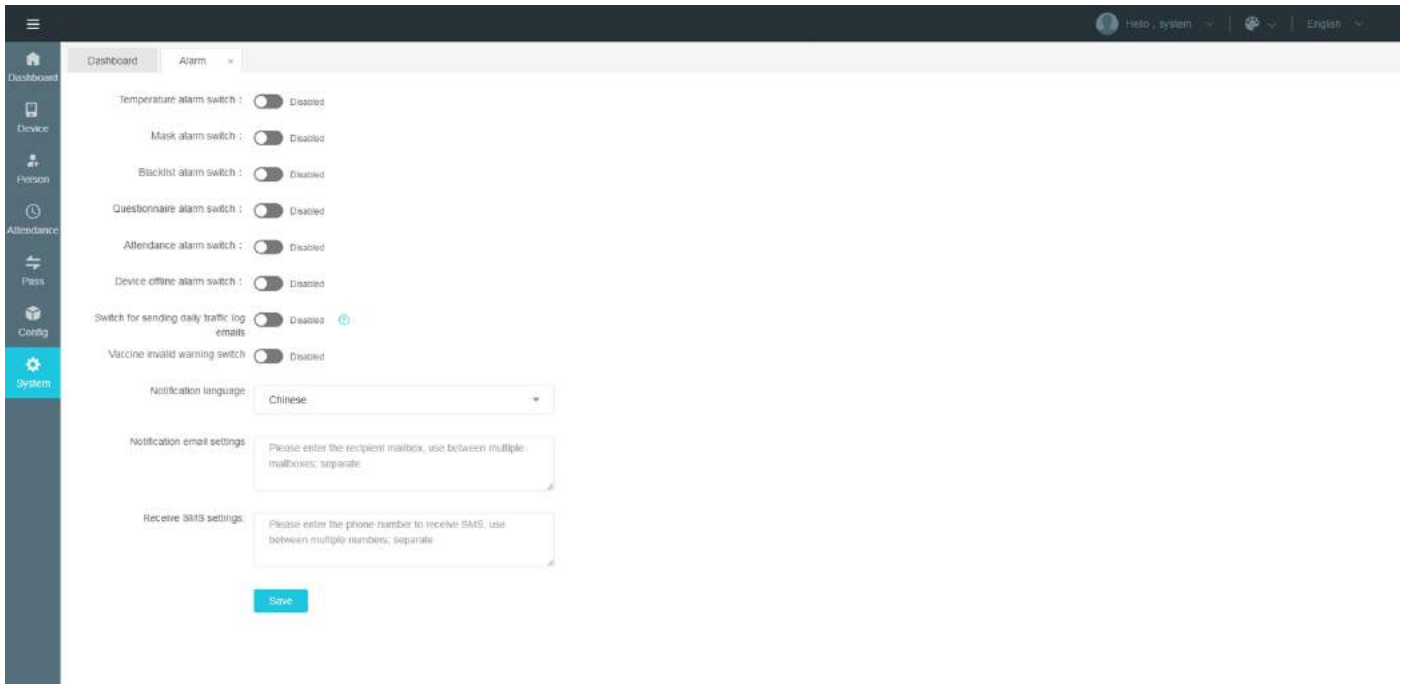
➢ ☐ Temperature alarm switch: After turning on this switch, you need to enter th e temperature alarm threshold, such as setting 37.5. When the temperature of the pedestrian exceeds 37.3, the system will send a high temperature alarm e mail to the set recipient mailbox.

➢ ☐ **Mask alarm switch:** When this switch is turned on, when the passer-by doe s not wear a mask, the system will send a mask warning email to the set reci pient mailbox for alarm (the device needs to open the mask for detection)

➢ ☐ **Blacklist alarm switch:** After turning on this switch, when the blacklisted pe rsons pass, the system will send a blacklist alarm email to the set recipient m ailbox

➢ ☐ **Questionnaire alarm switch**: This function corresponds to the [equipment] [

Questionnaire management] function. After turning on this switch, if the questionnaire answered by the passer is wrong, the questionnaire error alarm switch will be automatically sent to the set recipient mailbox

> ➢ **Attendance alarm switch**: This function corresponds to the attendance part of employees punching in. If the employee selects the corresponding attendance shift, after turning on this switch, the list of late arrivals will be sent to the set receiving mailbox at 22:00 every night, and the format of the sending The content is shown below:

2020/12/12Attedance late employee info:

Employee	PersonNo	Due time	Real time	Total late time
哈哈	12546	09:20:00	11:21:10	2.02 hours
呵呵	54678	09:20:00	11:21:29	2.03 hours
哦哦	96541	09:20:00	11:21:36	2.03 hours
喔喔喔	9874	09:20:00	11:22:13	2.04 hours

> ➢ **Device offline alarm setting:** When this switch is turned on, when the device is offline, a reminder email will be sent to the set recipient mailbox. Device offline alarm setting: After this switch is turned on, when the device is offline, a reminder email will be sent to the setting. 'S receiving email

> ➢ **Switch for sending daily traffic log emails**: All traffic record attachments csv format the day before sending.

> ➢ **Pass-through record mail delivery time**:Set the time to send traffic record messages.

> ➢ **No valid vaccine alarm switch**:When this switch is turned on, send an alarm message when the identification person's vaccine message is invalid.

> ➢ **Outgoing address:** The outgoing e-mail address of the mail sent by the sys

tem can be opened, added or modified in [System] [Mail Service Settings] (ple

ase read 7.6 Mail Service Settings)

➢ ⯀ **Recipient address**: The recipient's email address is in the "notification mai

lbox setting" in the alarm settings, as shown in the figure below. After clickin

g Add, you can enter the recipient address, and you can set up to ten recipie

nt addresses.

➢ ⯀ Sending content: The content of the email sent by the system is the con

tent in the [Configuration] [Message Template]. In the alarm settings, you can cho

ose to send the existing Chinese template or English template in the [Message Te

mplate] to the recipient mailbox, as follows As shown
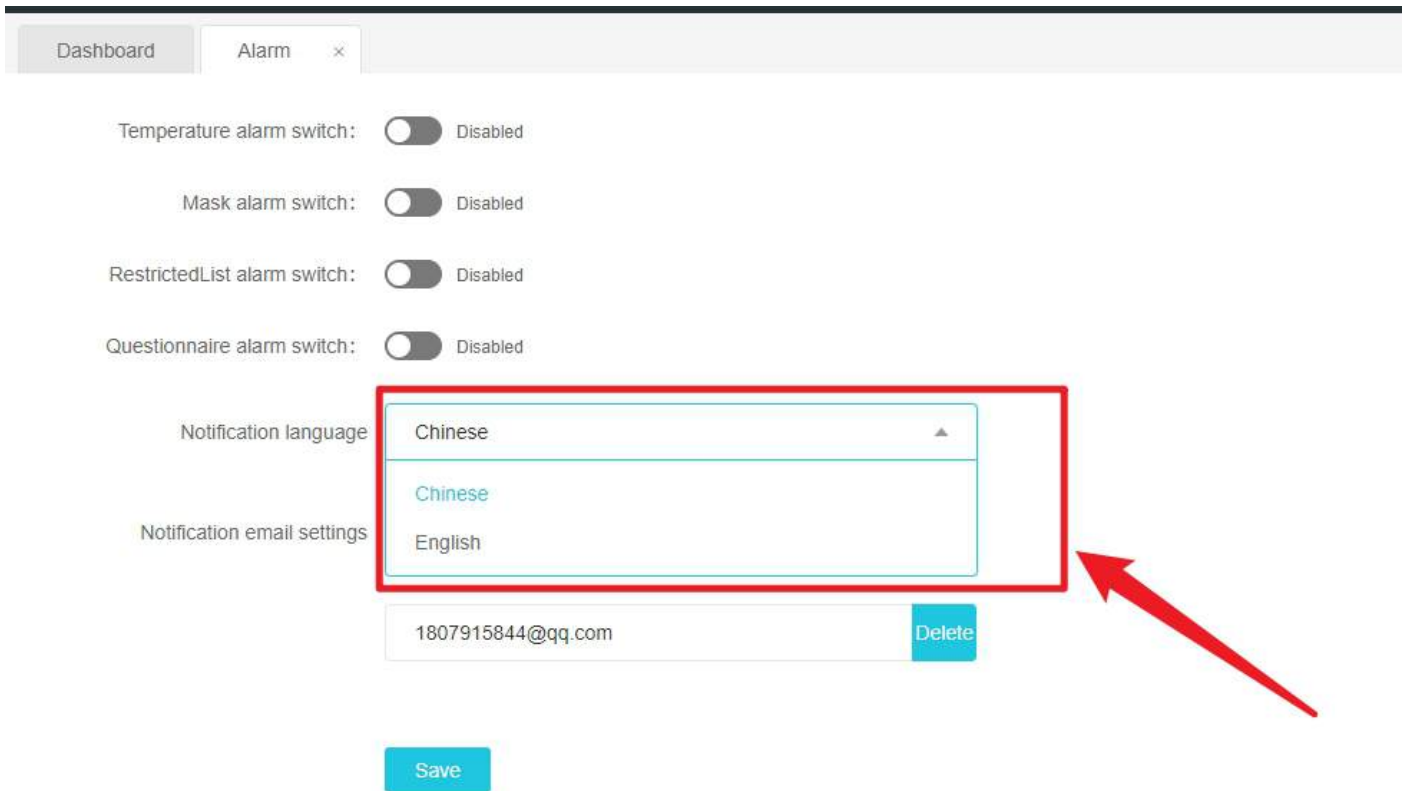
7.5.2.Personal Alarm

The personal Alarm is that when a designated employee passes through the device and the temperature exceeds the set temperature, the system will automatically send an email to the set mailbox. Turning on this feature requires two steps:

Step 1: Add alarm information in Employee Management-Employee Information, turn on the alarm switch and set the alarm receiving mailbox.
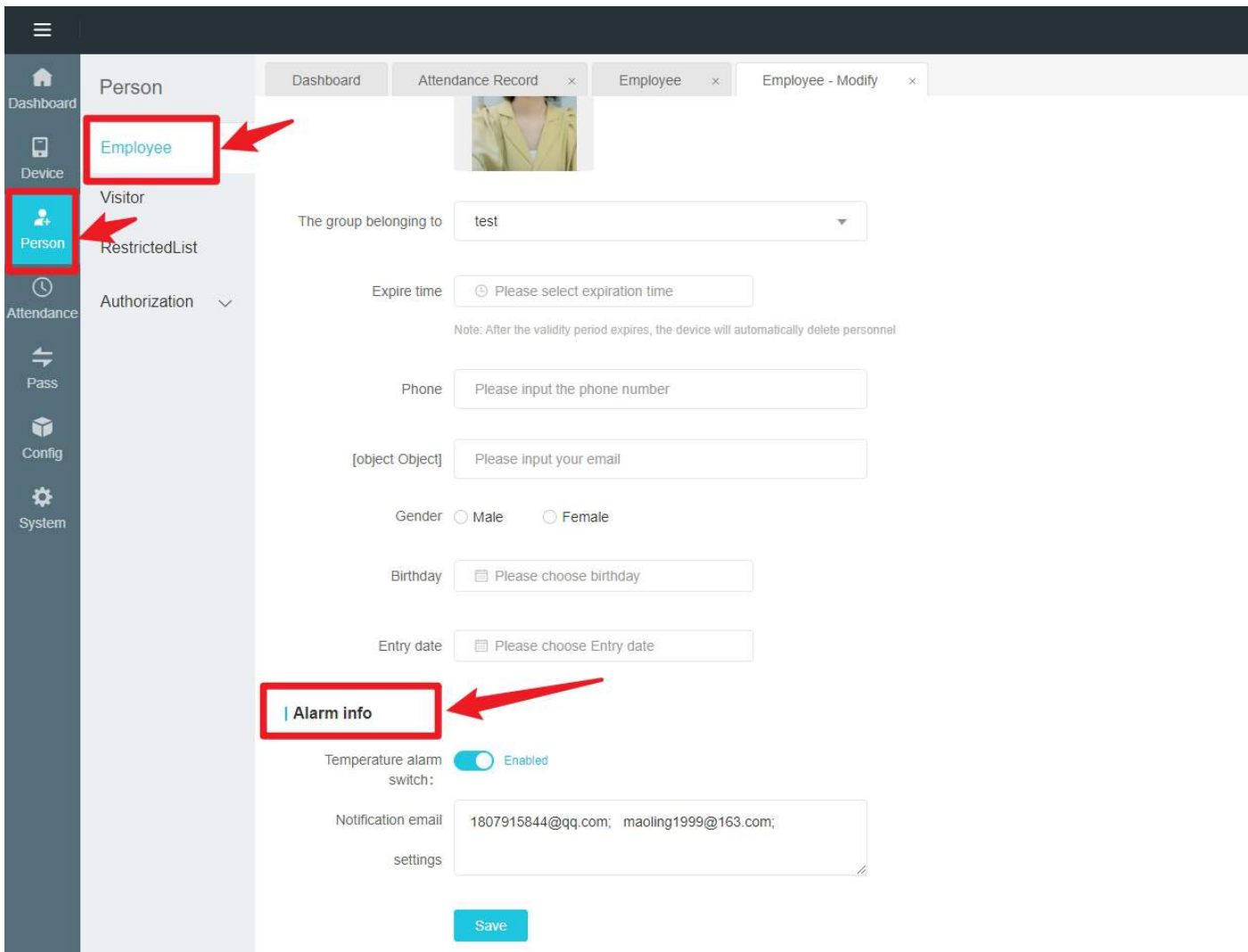
Step 2: In the system-alarm setting, turn on the temperature alarm switch and se

t the temperature alarm threshold and notification language.
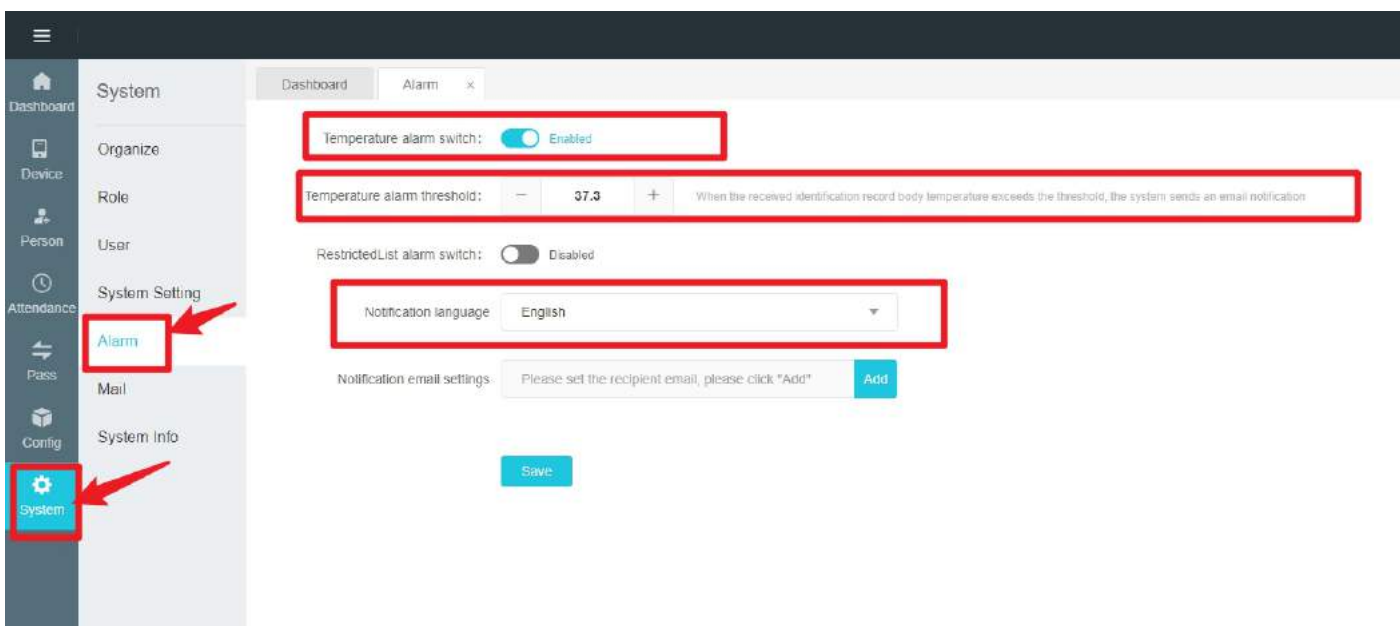
After setting steps one and two, the personal alarm service can be turned on. When

employees who have set alarm settings pass, the system will automatically send an e

mail to the notification mailbox (staff information-notification mailbox in the alarm inf

ormation) when the temperature exceeds the set temperature.

7.6.Mail service settings

The mail service setting is the email address sent in the system, and the receivin

g email address is set in [7.5 Alarm Settings].

Mail service settings are in [System] [Mail Service Settings], the location is as foll

ows
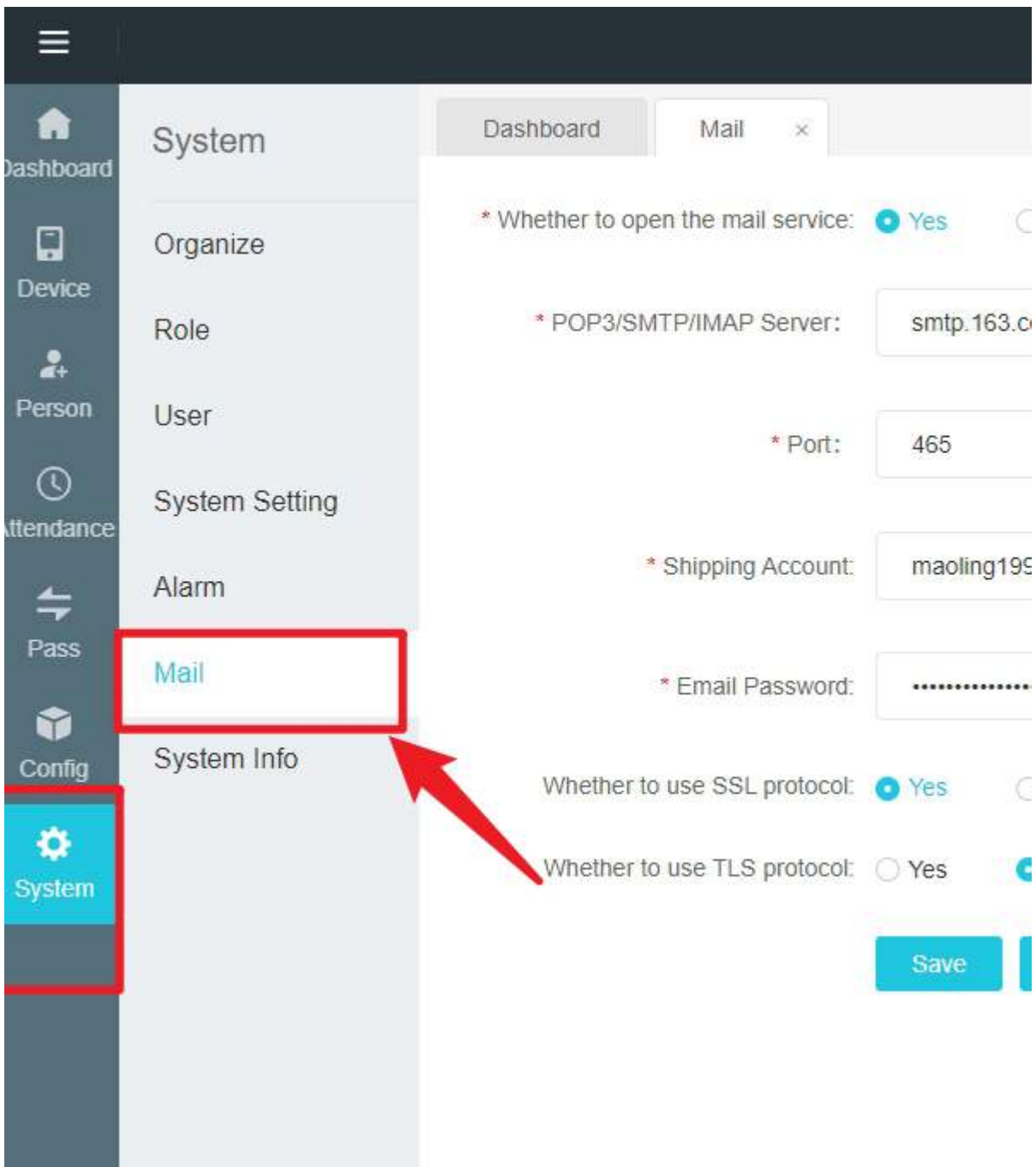
The mail service setting page is as follows :

Mail service switch: You can choose whether to open the mail service

Sending mailbox information:

The outgoing mailbox information needs to be checked in the mail service provider. For example, the 163 mailbox needs to be checked in the POP3/SMTP/IMAP setting page in the mailbox, and the POP3/SMTP/IMAP service needs to be enabled in the mailbox.

(1) POP3/SMTP/IMAP server

Please fill in according to the server address listed in the sender's mailbox server, which is usually listed on the mail service provider's settings page. Please select the v

erified server according to the mailbox's protocol.

(2) Port

Please fill in according to the port number listed by the sender's email service provider, usually listed on the mail service provider's help page, if not listed, 465 defaults to the https protocol, and 465 is recommended;

(3) Shipping account

Enter the name of the mailbox that needs to send mail; Note: Due to the different automatic judgment strategies and mechanisms of each mail service provider, if the newly registered mailbox is used as the sender to send mail frequently, various restrictions of the mail service provider may be triggered;

(4) Email password

Enter the mailbox password that needs to send emails. Note: Different mailbox servers may have different requirements. For example, 163 mailbox and QQ mailbox need to open the authorization code separately on the account setting page, and then fill in the authorization code; the right side of the input box Click the icon to switch the password plaintext/ciphertext display;

(5) Whether to use SSL protocol, TLS protocol

Please select the protocol type according to the type supported by the sender's mailbox server. Usually it will be listed on the mail service provider's help page. The system only supports SSL\TLS two protocols, and you can only choose one of the two protocols. Choose a different POP3/SMTP/IMAP server for the protocol suggested by the mailbox service provider.

(6) Mail inspection

After filling in all the parameters and information, you can click the [Test Sending] button to check whether the email is sent and received normally. If the sending is successful, it means the filled content is correct. Just click Save; if the sending fails, please check the filled content or contact After-sales personnel help deal with.

Here is an example of the settings of 163 mailbox and outLook mailbox:

163 mailbox needs to fill in the content as :

Fill in the outLook mailbox as :

7.7.SMS settings

If you need to use the function of sending SMS, please apply for an account on a third-party SMS platform and recharge to obtain apiKey, fill in the account informat ion in the system, and apply for the SMS template before it can be used normally. Pl ease contact after-sales personnel for assistance.
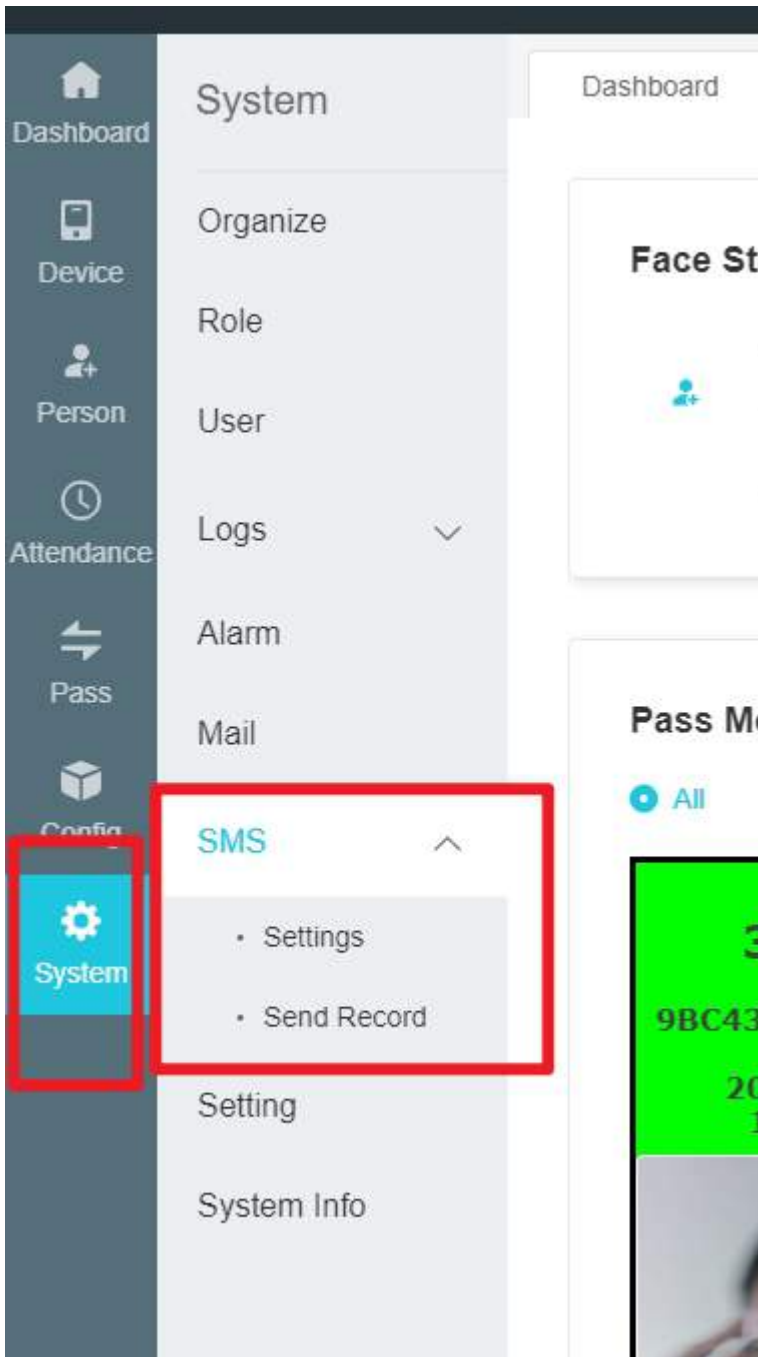
7.7.1.Settings

The settings on this page are equivalent to sending SMS, the receiving SMS phone number is filled in [7.5. Alarm Settings], currently only supports high temperature SMS notification.

SMS service providers support two platforms, Yunpian and umssoft. If you need to use them, please apply for an account or apiKey from the service provider.

The page when the service provider chooses the cloud :

The page when the SMS service provider chooses umssoft :

Whether to enable SMS service: disabled by default, if yes, it will turn off the function

of sending SMS

SMS area: can be selected according to the information applied to Yunpian

SMS Signature: Smart Pass

ApiKey: can be selected according to the information applied to Yunpian

SMS platform account: Please fill in the umssoft account

SMS platform password: Please fill in the password of umssoft

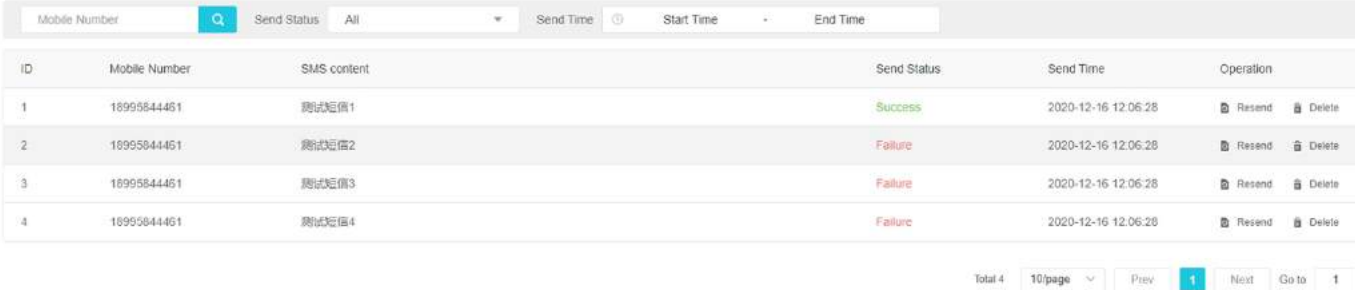[7.5. Alarm Settings] set the recipient's short phone number, as shown in the figure bel

ow :

7.7.2.SMS sending record

After the message is sent, you can view the record of the message sent on this page, and find the record according to the conditions. The specific page is shown in the figure below :

7.8. Log management

Monitor and record the operations in the system. Users can view different operations and requests sent on the system at different times on this page. It is divided into system log and business log. The operations related to system settings are system logs, and other operations related to equipment, personnel and attendance are business logs. Log management location is as follows :
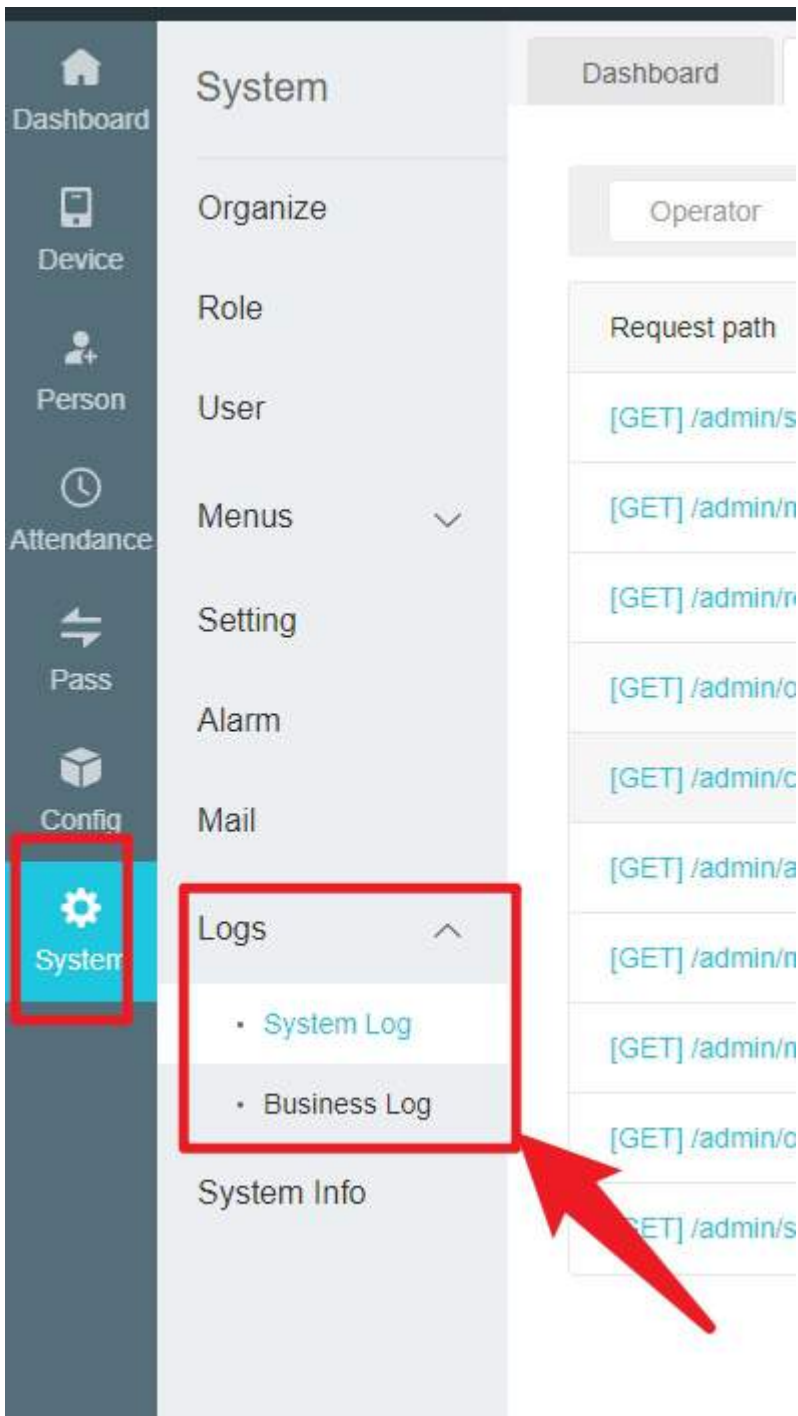
The system log display list is as follows:

Request path	Event type	Operation type	Results	Operator	Client IP	Response time	Operation time
[GET] /admin/system/info	System event	Query	Success	system	192.168.1.72	37ms	2020-11-12 10:05:44
[GET] /admin/menus/tree	System event	Query	Success	system	192.168.1.72	122ms	2020-11-12 10:05:49
[GET] /admin/roles/page	System event	Query	Success	system	192.168.1.72	7ms	2020-11-12 10:05:56
[GET] /admin/orgs/tree	System event	Query	Success	system	192.168.1.72	39ms	2020-11-12 10:05:56
[GET] /admin/config/global	System event	Query	Success	system	192.168.1.72	3ms	2020-11-12 10:05:36
[GET] /admin/alarm_config	System event	Query	Success	system	192.168.1.72	10ms	2020-11-12 10:05:46
[GET] /admin/message_tpl/page	System event	Query	Success	system	192.168.1.72	3ms	2020-11-12 10:05:41
[GET] /admin/message_tpl/page	System event	Query	Success	system	192.168.1.72	2ms	2020-11-12 10:06:00
[GET] /admin/orgs/list	System event	Query	Success	system	192.168.1.72	7ms	2020-11-12 10:05:57
[GET] /admin/sites/tree	System event	Query	Success	system	192.168.1.72	42ms	2020-11-12 10:05:41

Total 126   10/page ∨   Prev   **1** 2 3 4 ⋯ 13   Next   Go to 1

Click the request path (in blue font) to view the details：

Operation type	All ▼
Results	All ▼
Time Tnterval ⏱	

Detail ✕

|	
Request Path:	[GET] /admin/system/info
Operation Results:	Success
Log Category:	System Log
Event Type:	System event
Operation Type:	Query
Operator:	system
Client IP:	192.168.1.72
Response Time:	37ms
Operation Time:	2020-11-12 10:05:44
Operating System:	Win 7
Browser Type:	chrome 86
User Agent:	mozilla/5.0 (windows nt 6.1; wow64) applewebkit/537.36 (kh tml, like gecko) chrome/86.0.4240.111 safari/537.36
Request Parameters:	{}

Cancel

Client IP

192.168.1.72
192.168.1.72
192.168.1.72
192.168.1.72
192.168.1.72
192.168.1.72
192.168.1.72
192.168.1.72
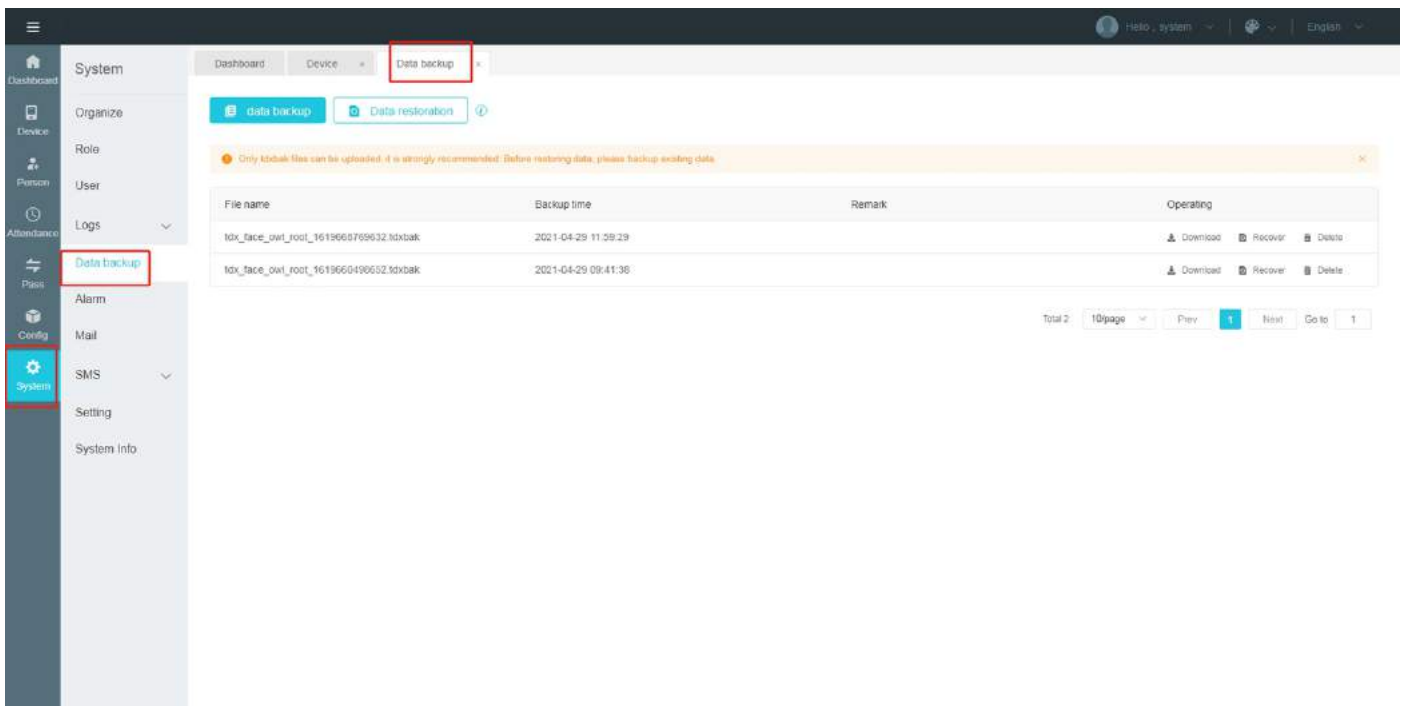192.168.1.72
192.168.1.72

10/page

7.9.System message

system message : View basic system information
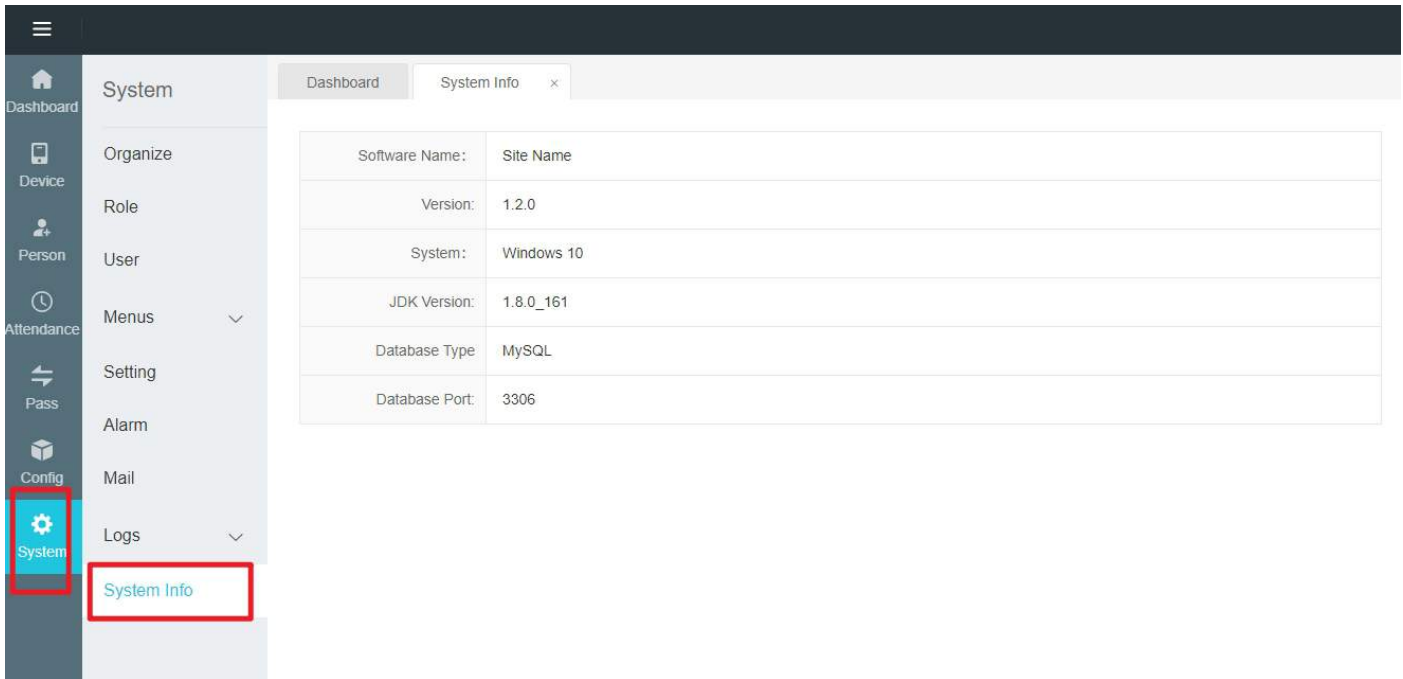
7.10. data backup

Data backup function module: Back up and restore the system database. It is strongly recommended: Before restoring the data, please back up the existing data and download it.
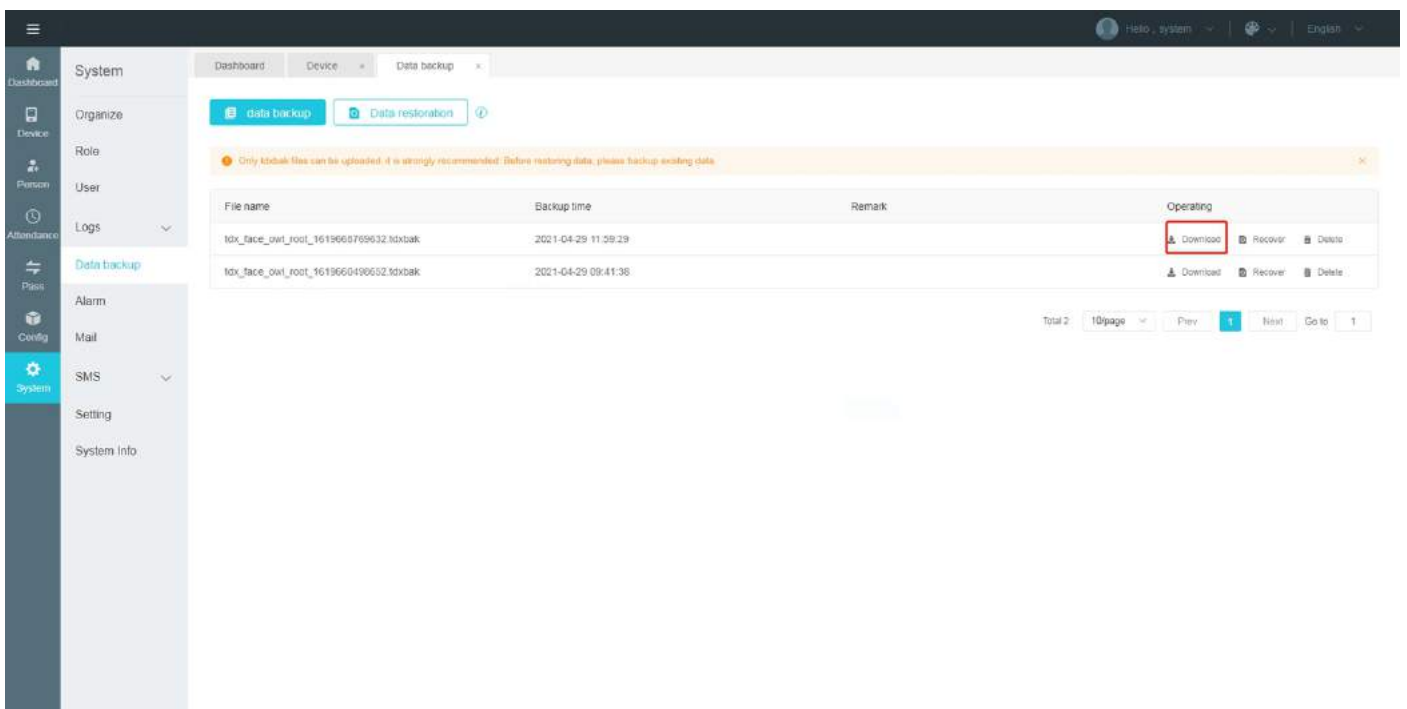

Data backup: Click the data backup button, fill in the remarks on the data backup page, and click the save button to back up the existing data of the system.
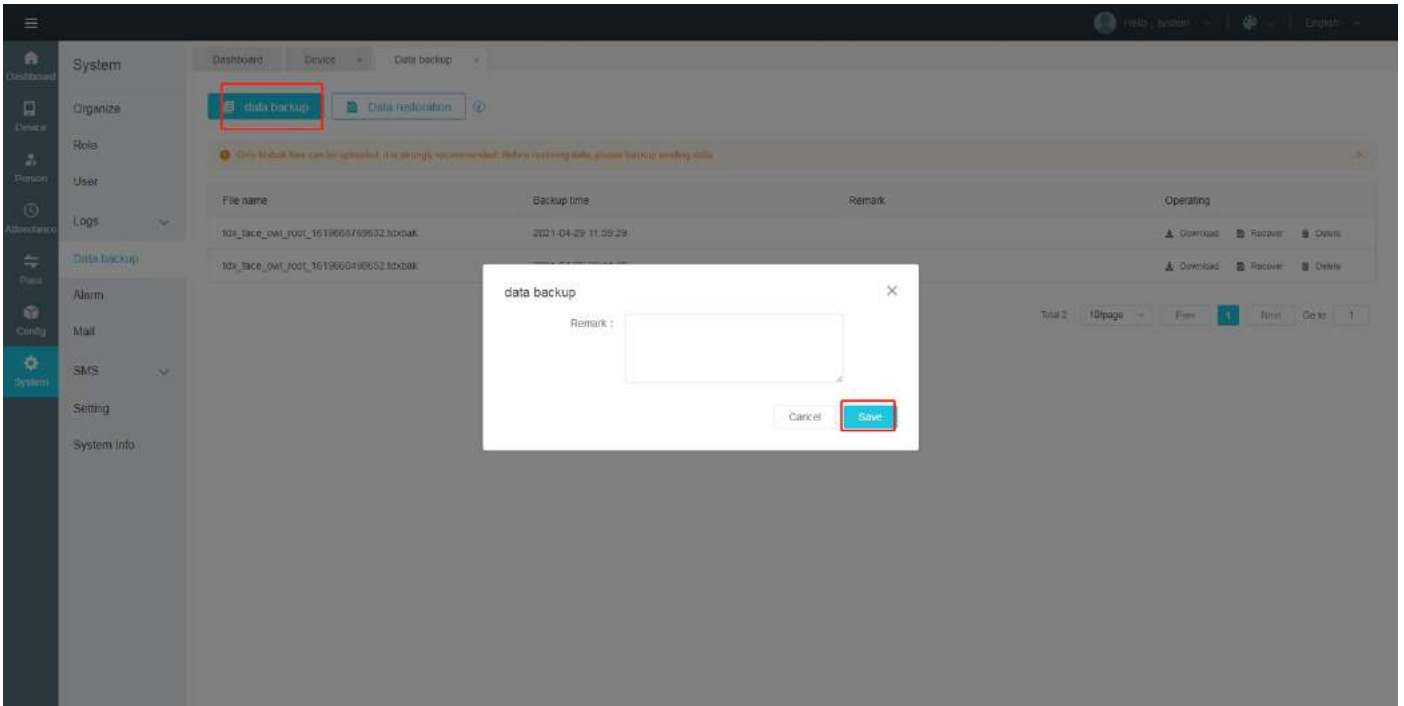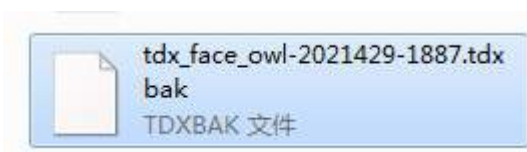
Data file download: Click the download button in the list operation bar to downlo ad the corresponding recorded data file to the local computer.
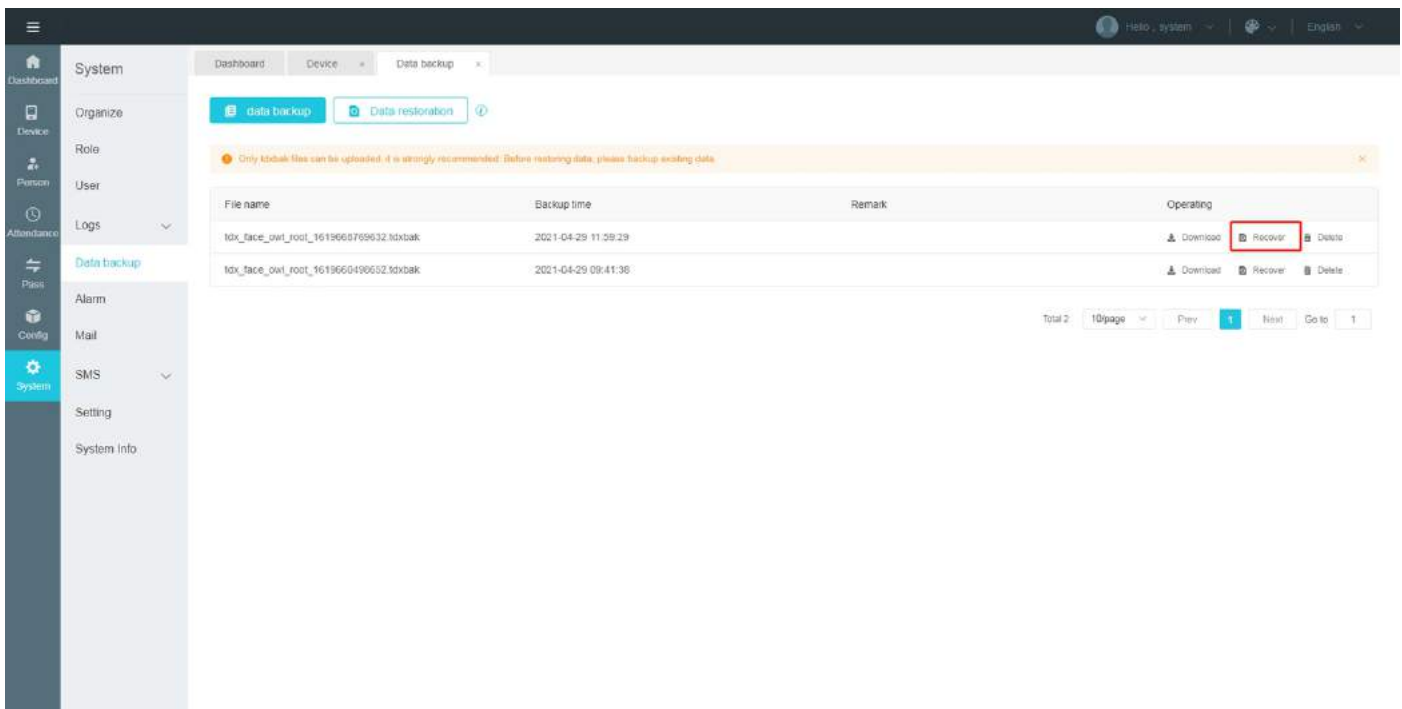

The data file format is .tdxbak

Data recovery: Click the restore button in the list operation bar to restore the system

data to the data at the backup time.It is strongly recommended: Before restoring the data,

please back up the existing data and download it.

Data restoration: Click the Data Restore button, on the data restoration page, click the

Upload button, select the downloaded .tdxbak file, and restore the data.It is strongly

recommended: Before restoring the data, please back up the existing data and download it.