MIPS Smart Pass Management Platform User Manual

Contents

1.Chapter One Installation and Login 6

2.Chapter Two Console 8

3.Chapter Three Device Management 9

3.1 Device list 9

3.1.1 Parameter settings 9

3.1.2 Power control 10

3.1.3 Body temperature test 10

3.1.4 Client upgrade 10

3.1.5 Volume settings 11

3.1.6 Auto-start 12

3.1.7 Application daemon 12

3.1.8 Open the door remotely 12

3.1.9 Delete 13

3.1.10 Move group 13

3.1.11 Personalize list 13

3.1.12 Device details 14

3.1.13 Device monitoring 15

3.1.14 Grouping operation in Bulk 16

3.1.15 Device grouping management 17

3.2 APK list 17

3.2.1 Delete APK 17

3.2.2 New APK 18

4.Chapter Four Personnel Management 19
4.1 Employee list 19
4.1.1 Add employee information individually 19
4.1.2 Import employee information in bulk 21
4.1.3 Import portrait photos in bulk 22
4.1.4 Export employee information 23
4.1.5 Refresh employee information 23
4.1.6 Staff details and editing 23
4.1.7 Employee grouping management 25
4.2 Visitor management 25
4.2.1 Add visitor individually 26
4.2.2 Export visitor information 28
4.2.3 Refresh visitor information 28
4.2.4 Visitor details and editing 28
4.2.5 Visitor grouping management 30
4.3 Blacklist management 30
4.3.1 Add blacklist individually 31
4.3.2 Export blacklist 32
4.3.3 Refresh blacklist information 32
4.3.4 Blacklist details and editing 32
4.3.5 Blacklist grouping management 34
5.Chapter Five Pass Management 35
5.1 Pass records 35
5.2 Pass permission 35

5.2.1 Employee pass permission settings 36
5.2.2 Visitor pass permission settings 37
5.2.3 Revoke permission 39
5.2.4 Refresh permission information 40
5.3 Blacklist monitoring 40
5.3.1 Blacklist monitoring settings 40
5.3.2 Identification record query 42
5.3.3 Remove monitoring 42
5.4 Permission records 43
6.Chapter Six System Management 45
6.1 Group structure 45
6.1.1 Attribution of business data 45
6.1.2 Group management 46
6.1.3 User management 46
6.2 Role management 47
6.3 Business management 48
6.4 System log 49
6.5 System setting 50
7.Chapter Seven Client Functions 50
7.1 Client login 50
7.2 Application settings 51
7.2.1 Device name setting 52
7.2.2 Body temperature setting 53
7.2.3 Identification parameter setting 54
7.2.4 Volume setting 55
7.2.5 Start-up settings 55
7.2.6 Application information settings 56

7.2.7 Recognition effect display 56

7.2.8 Application password settings 57

7.2.9 Camera preview resolution setting 58

7.2.10 Screen-saver brightness setting 58

7.2.11 Device restart time setting 59

7.2.12 Relay settings 59

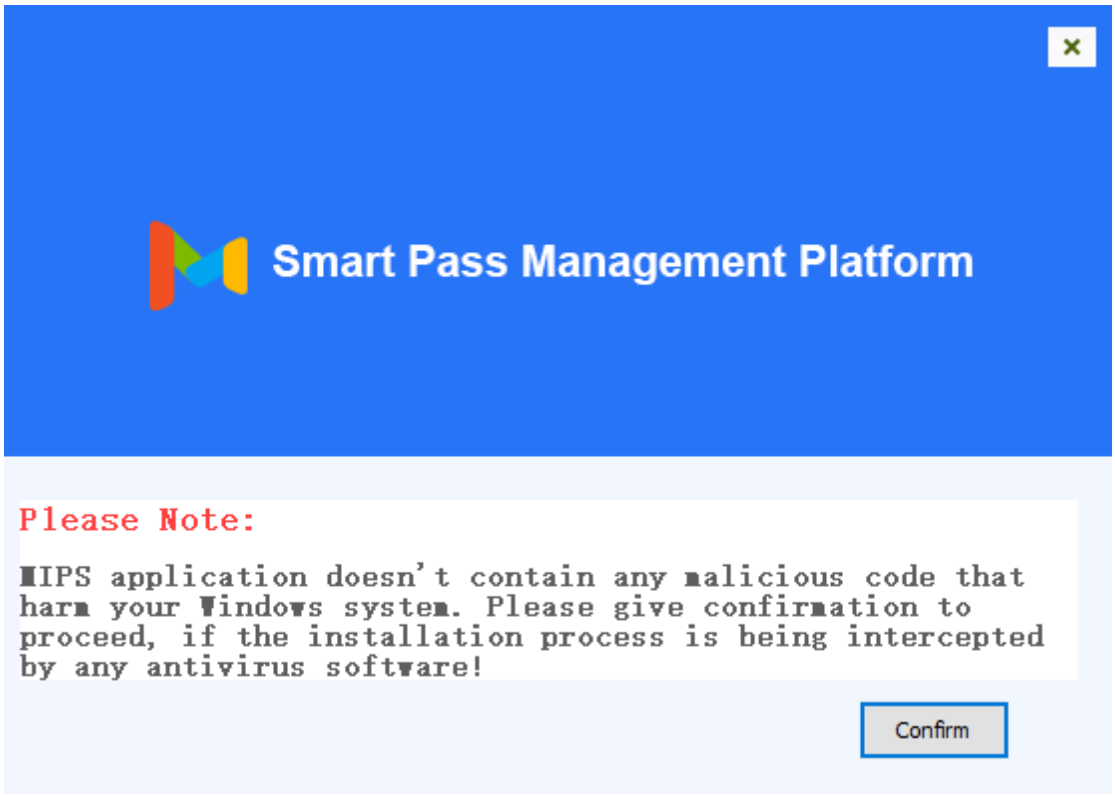
7.2.13 Others 60

7.2.14 Application initialization 61

7.3 Face portrait entry 61
7.4 Personnel import in bulk 62
7.5 Pass records 64
7.6 Application information 65
7.7 Face database 65
7.8 Identify the home page 65
7.9 Others 66

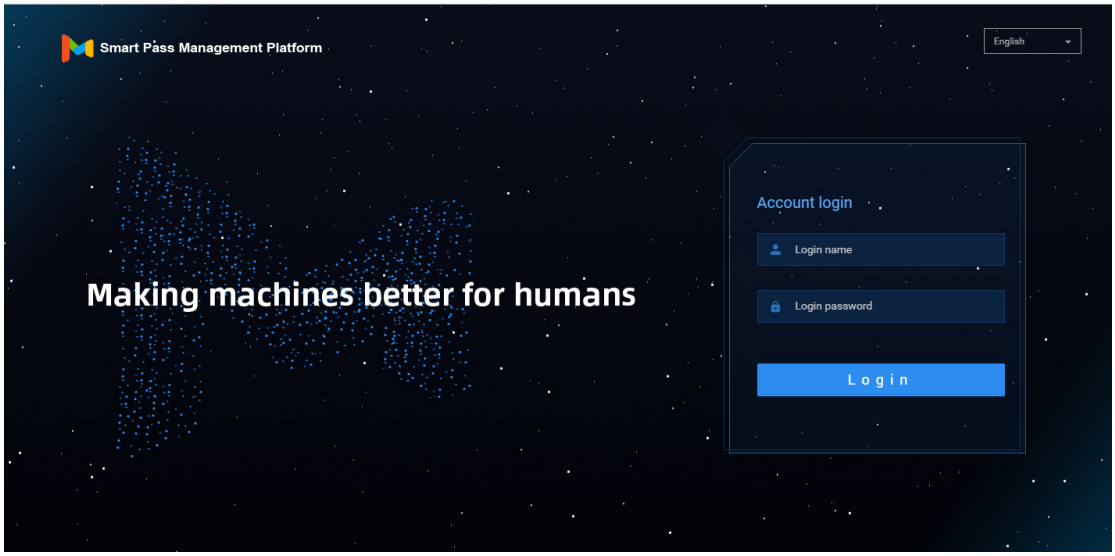
1.Chapter One Installation and Login

- One-click installation: Double-click the exe installation file and follow the installation instructions for quick installation.



Note: If the installation process is blocked by a system firewall or third-party antivirus software, always choose to allow the program to operate. Otherwise, the installation process may fail and become unusable.

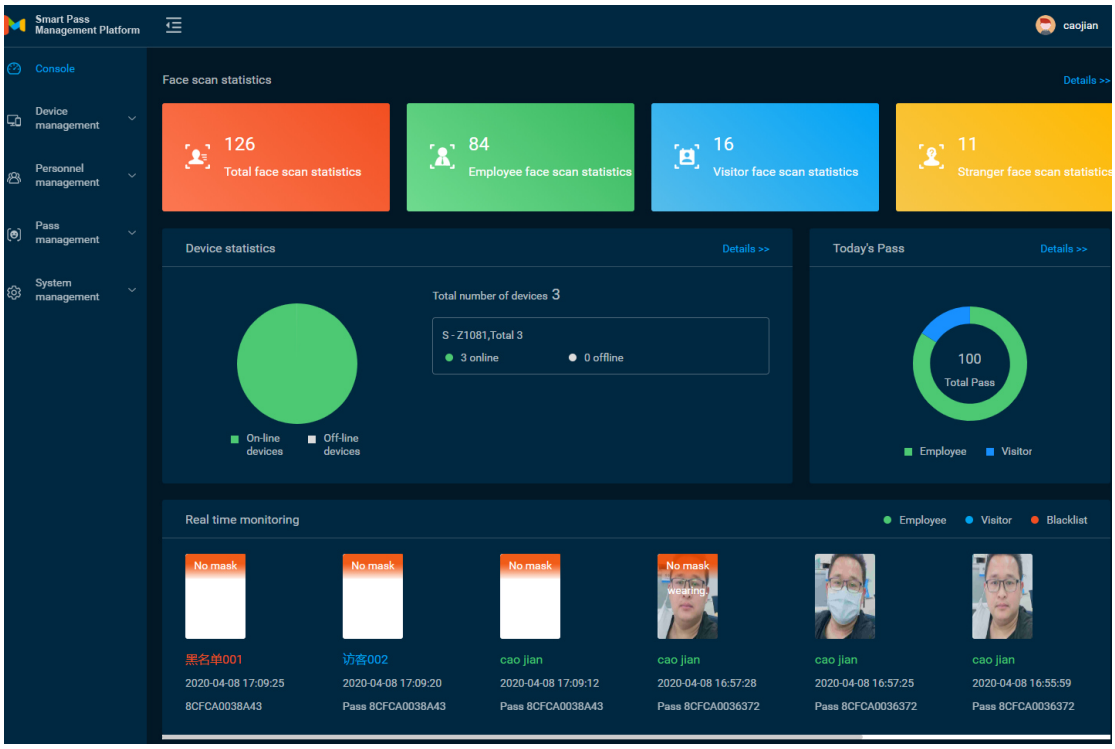
- After the program is installed, the MIPS service is automatically started by default.
- After the start-up is complete, click the "Copy" button. Open the chrome browser and paste the link to open the MIPS service background. Enter your username and password to log in.



- MIPS system upgrade: You only need to overwrite and install the MIPS system software version installation package higher than the current version.

2.Chapter Two Console

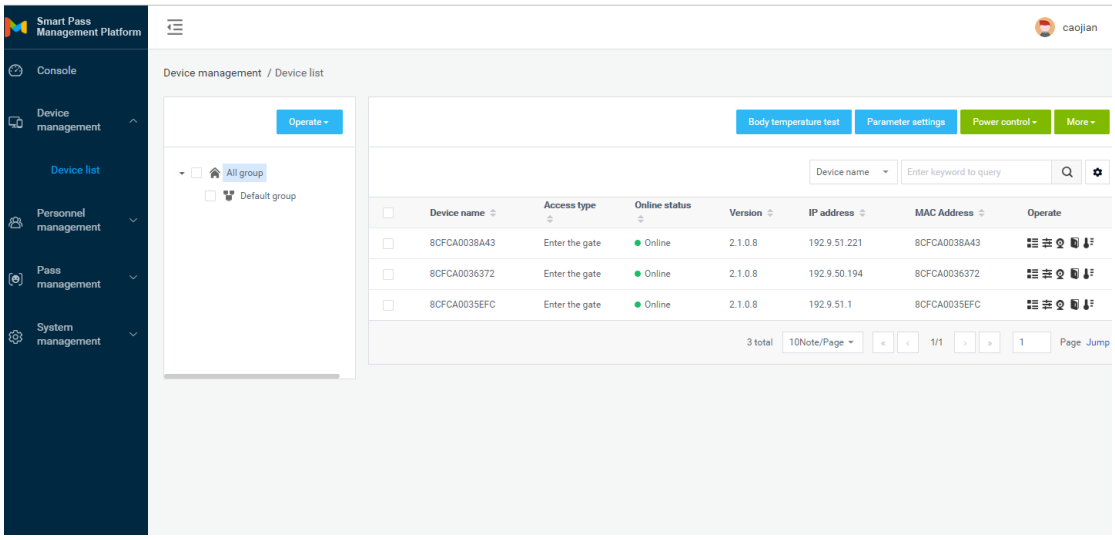
It provides an overview of the number of devices and online status; statistics on the face scan (total face scan, employee face scan, visitor face scan, stranger face scan); today's pass and real-time monitoring (employees, visitors, blacklists, and body temperature); and provides quick access to view details.



3.Chapter Three Device Management

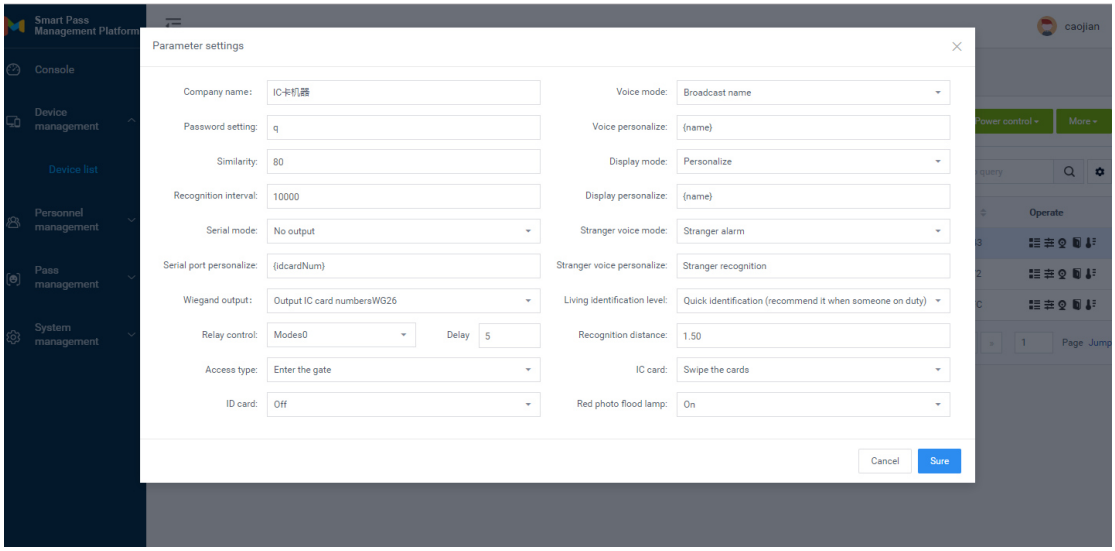
3.1 Device list

[Device List] It contains all device information connected to the system. You can perform single, multiple, and grouping management operations on the device.



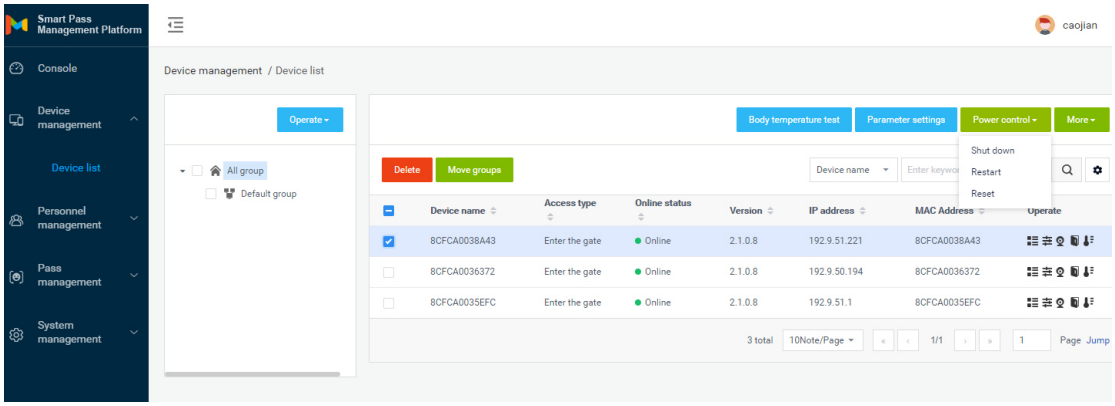
3.1.1 Parameter settings

Select the specified device in [Device List] and click Parameter settings to configure the parameter information of the device, as shown in the figure below:



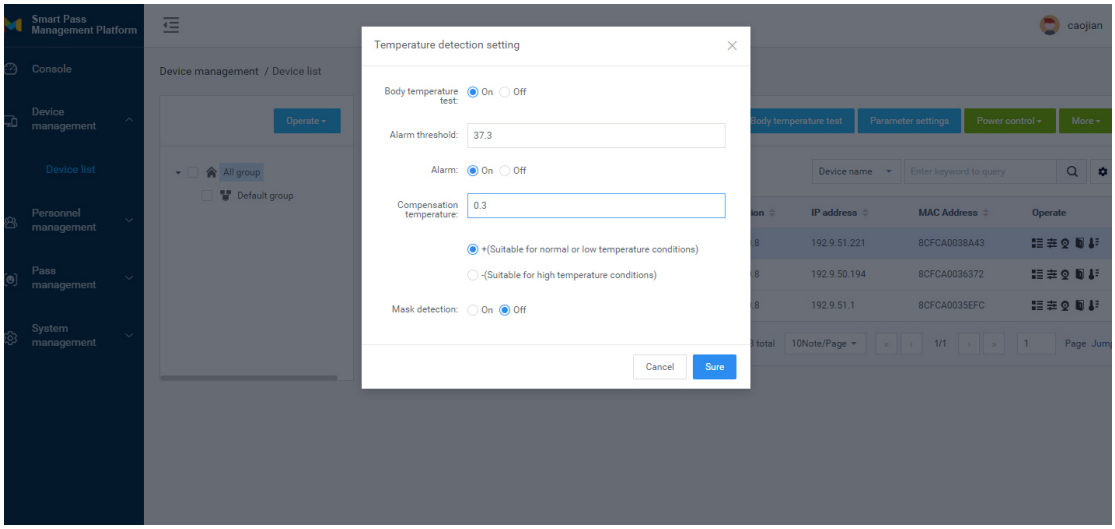
3.1.2 Power control

Select the device in [Device list] and click "Shutdown", "Restart", and "Reset" under "Power Control" to remotely shut down, restart, and reset the device.



3.1.3 Body temperature test

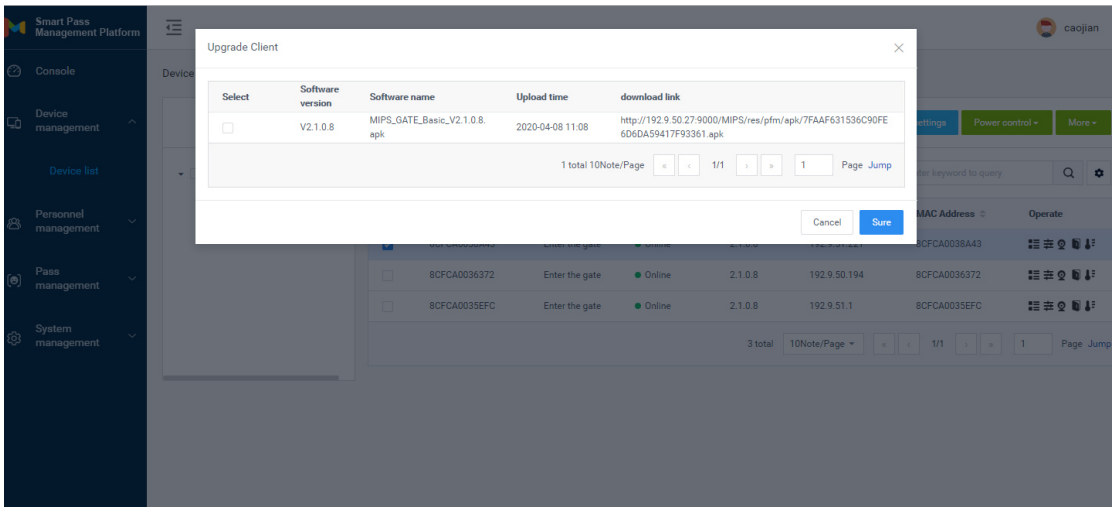
Select the device in [Device list], or select the group, and click "Body temperature detection" to set the parameters of temperature detection: temperature detection switch (default on), alarm threshold (default 37.3) and alarm switch, compensation temperature (default + Value 0.3) and mask settings (default off).



3.1.4 Client upgrade

Select the device in [Device list] and click "More-Client upgrade" to enter the device software

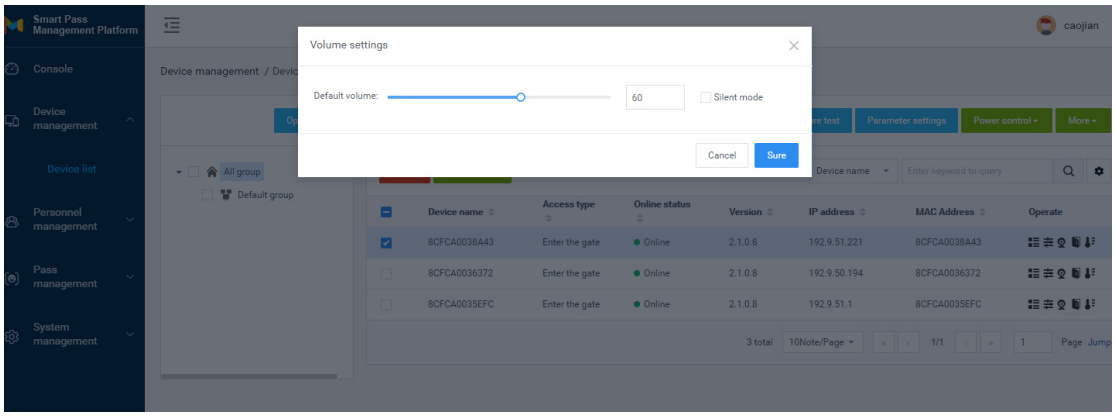
upgrade page. On this page, you can see the list of uploaded device software. Select the software version of the device to be upgraded and click the upgrade button to complete the device software upgrade operation. It supports online and offline upgrade operation.



3.1.5 Volume settings

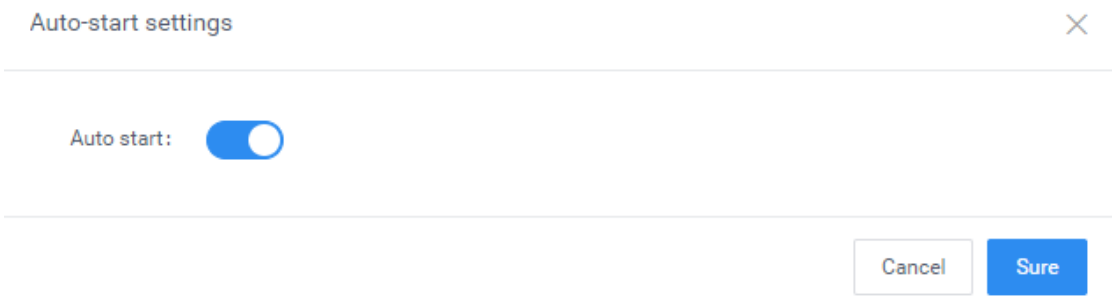
1) General settings: Select the device in the [Device List] and click "More-Volume setting" to set the volume of the selected device. The volume value can be set between 0-100 and the default is 20.

2) Silent setting: Select the device in [Device list], click "More-Volume setting", and select "Silent mode" in the pop-up tab.



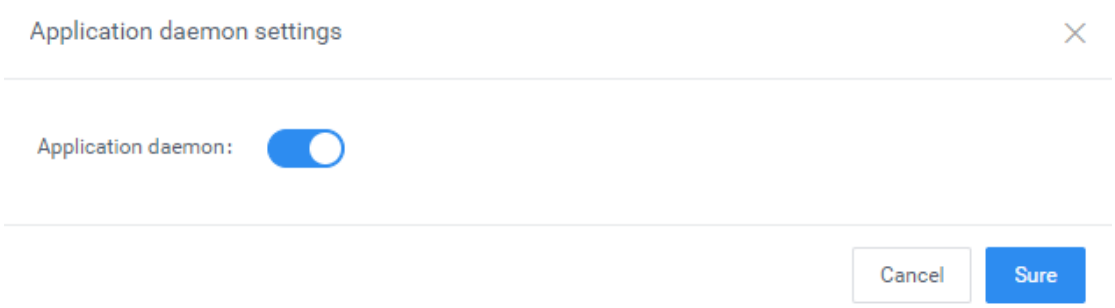
3.1.6 Auto-start

Auto-start: When enabled, the application will start at start-up, and when it is closed, it will not start at start-up. In [Device list], select the devices that need to be set to start automatically, and click the "More-Auto-start" button to enable or disable this function.



3.1.7 Application daemon

Application daemon: When this function is enabled, the application will automatically jump back to the playback interface within 1 minute after exiting the application page. When it is disabled, it will not automatically jump back. In [Device list], select the devices that need to set application daemon, and click the "More-Application daemon" button to enable or disable this function.



3.1.8 Open the door remotely

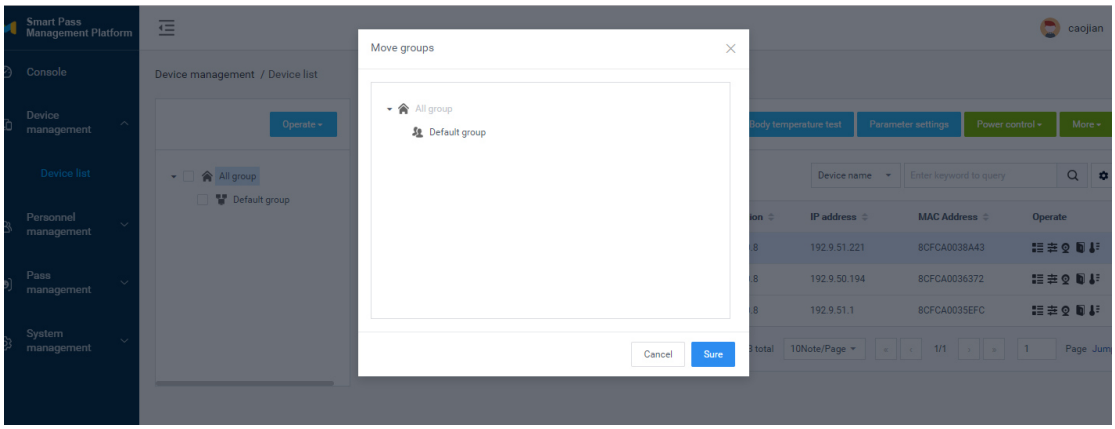
After corresponding to the device records in [Device list], click the "Open the door remotely" button to open the corresponding gate.

3.1.9 Delete

Select the device to be deleted in the [Device list] and click the "Delete" button to complete the delete operation. Only offline devices are supported. It supports single or multiple device operations.

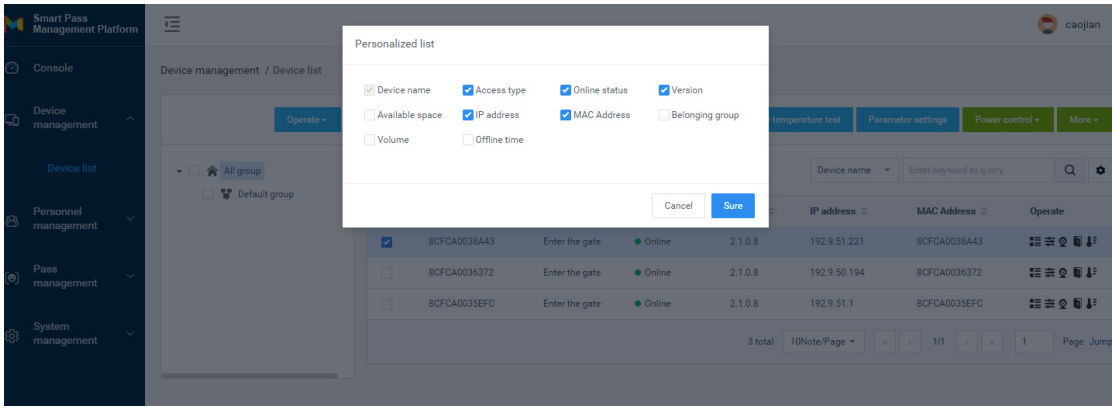
3.1.10 Move group

In [Device list], select the devices that require mobile grouping, and click "Mobile Grouping". In the pop-up window, select the target group you want to move to, and you can complete the group move operation after you confirm it. It supports single or multiple device operations.



3.1.11 Personalize list

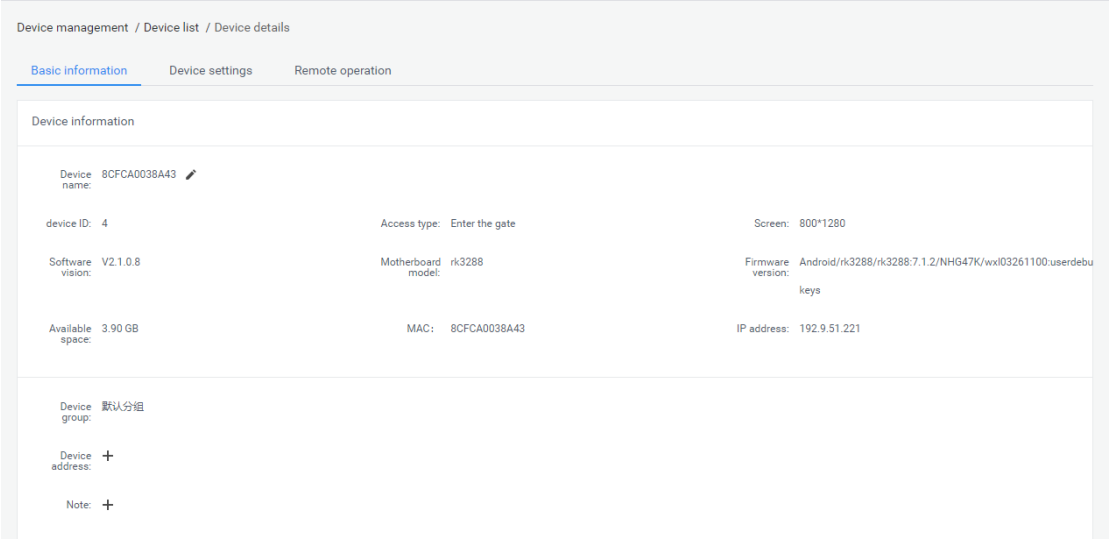
The information displayed in the list can be selected as needed in the Personalize list.



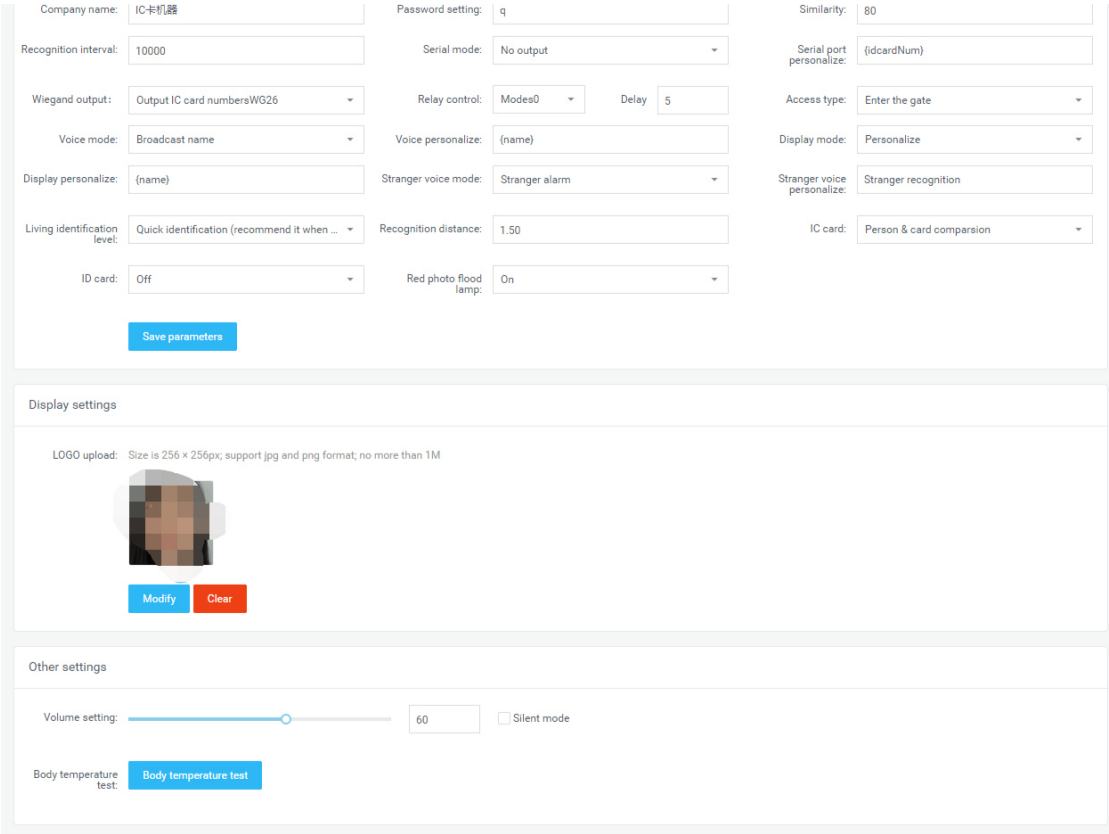
3.1.12 Device details

The device details include basic information, device settings, and remote operation.

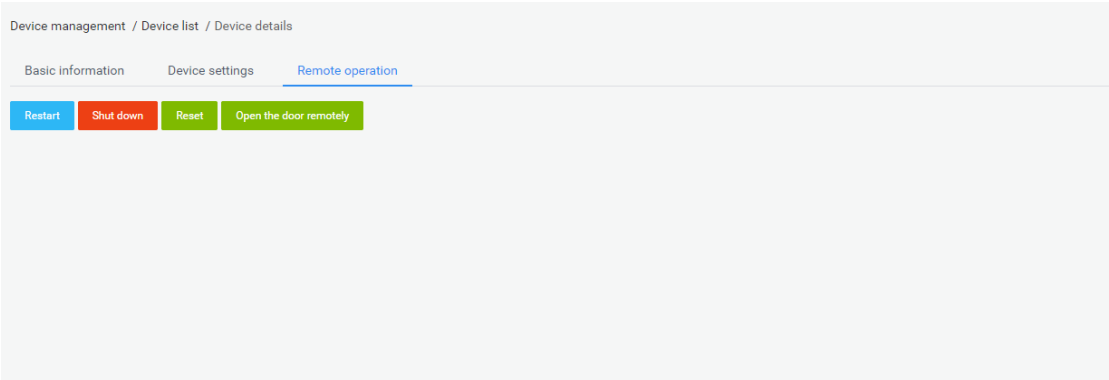
- Basic information: View device information, edit device name, device address, etc.



- Device information: You can view and modify device parameter information, display settings, and other settings.



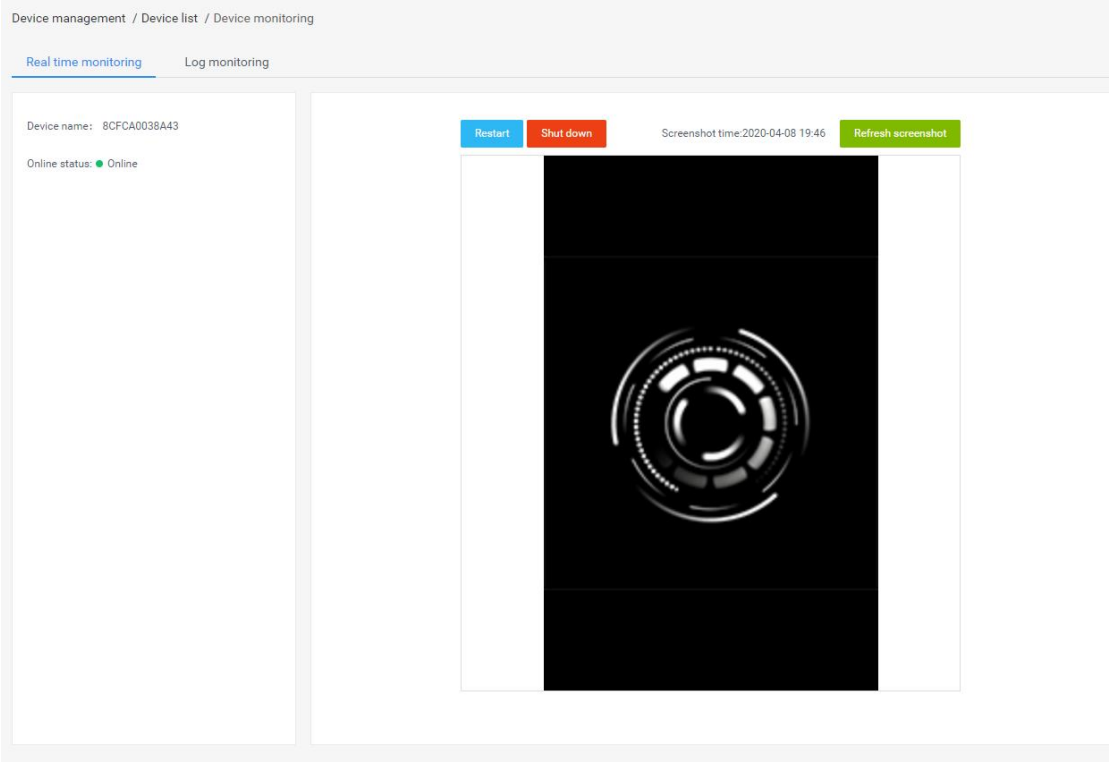
- Device operation: restart, shutdown, reset and remote door opening.



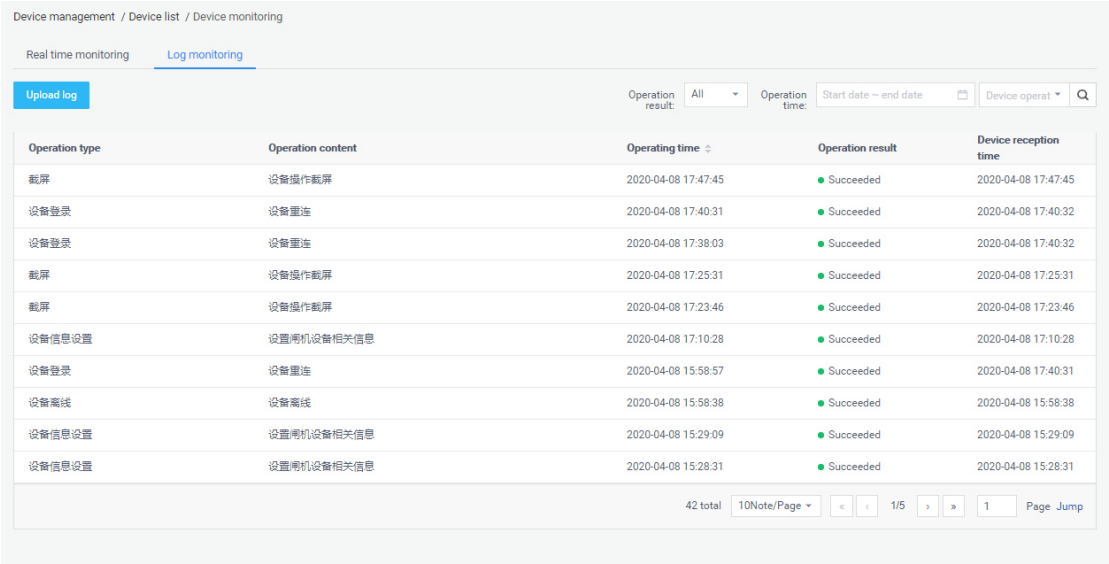
3.1.13 Device monitoring

Device monitoring includes two parts: real-time monitoring and log monitoring.

- Real-time monitoring: You can view the device name and online status, and load and display the current screen of the device. You can also restart and shut down.

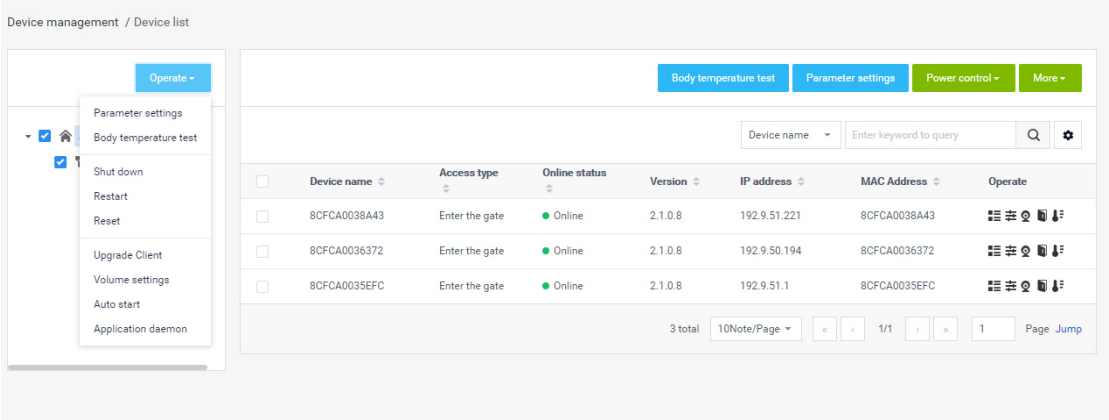


- Log monitoring: View related operation logs of the device.



3.1.14 Grouping operation in Bulk

Batch operations can be performed in the device group by selecting the device group. It supports parameter setting, shutdown, restart, reset, client upgrade, volume setting, auto start and application daemon for the entire device group, as shown below:



If there is no device under the selected group, a prompt will pop up: there is no device under the selected group, please select again. If there are devices under the selected group, the original settings will be overwritten after the batch setting is prompted.

3.1.15 Device grouping management

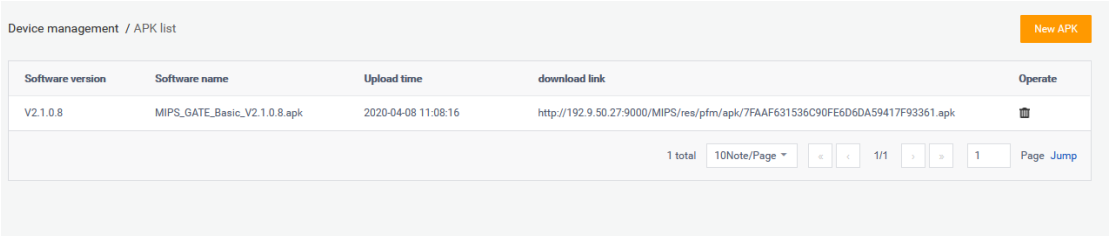
Device grouping uses structure grouping by default. Each user group has a default device group. You can add, modify, and delete device groups on the user group. The operation is similar to the user grouping in [Group structure].

3.2 APK list

[APK list] The page contains client software list information and software version upload and delete operations.

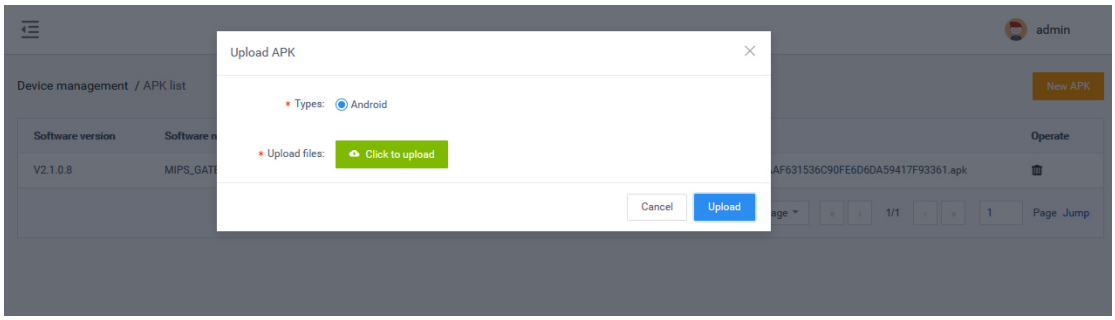
3.2.1 Delete APK

Select the software version to be deleted in the APK list, and click .



3.2.2 New APK

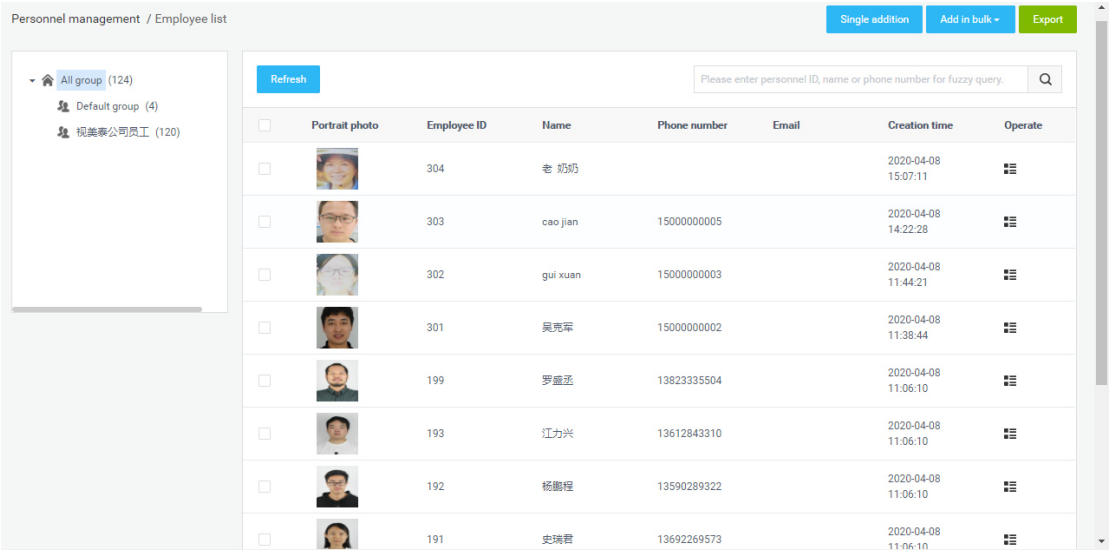
Click New APK to open the [Version Upload] page, and upload software files on this page.



4.Chapter Four Personnel Management

4.1 Employee list

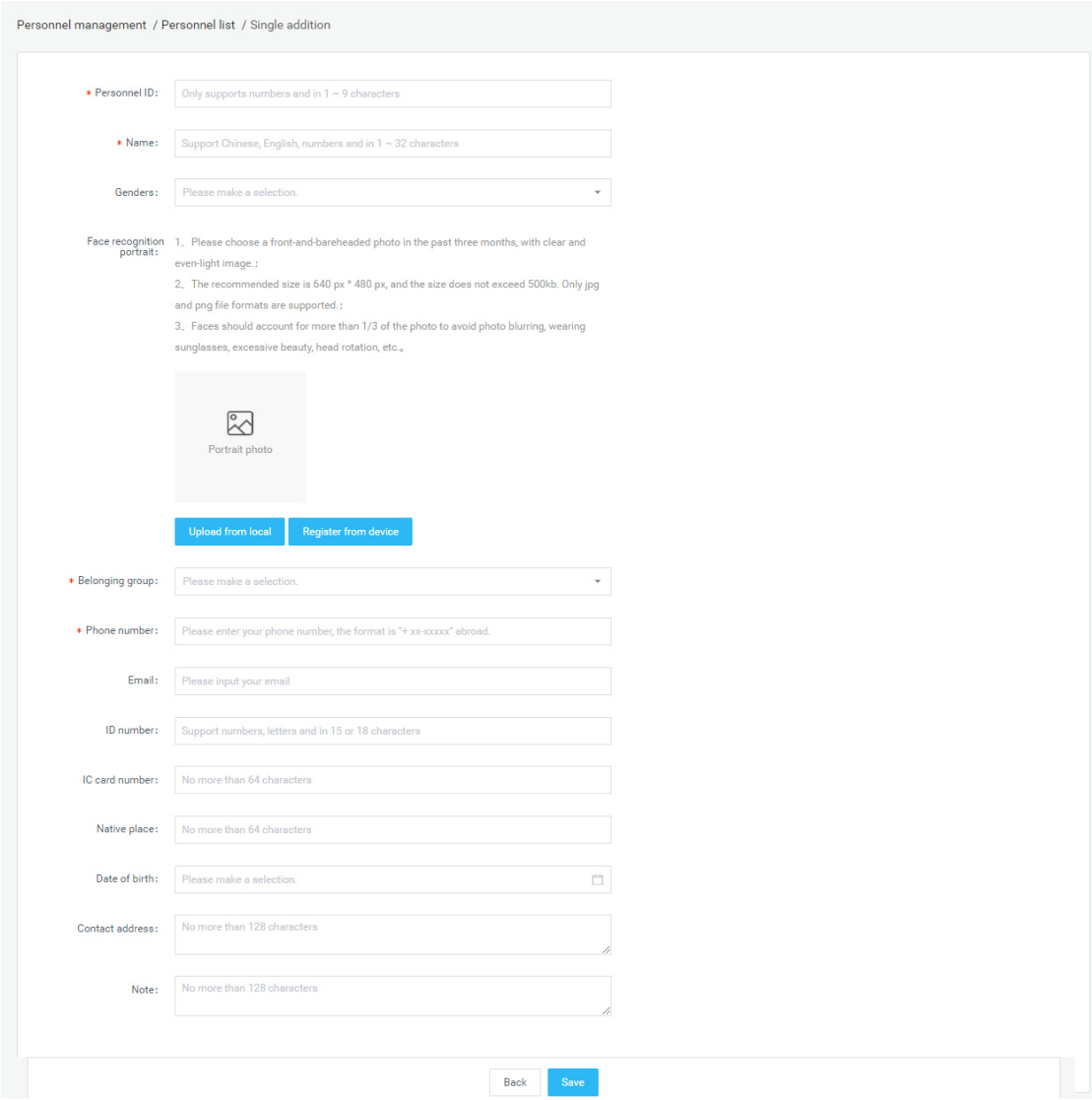
The employee list is used to manage employee information, such as viewing, adding, editing, and exporting employee information. Employee information can be added individually or in bulk. The batch adding operation requires information import in bulk first, and then portrait import in bulk.



4.1.1 Add employee information individually

Steps:

1) In [Employee list], click the "Single addition" button to enter the employee addition page;
2) Fill in the personnel ID, name, gender, belonging group, phone number, ID card number, IC card number, nationality, place of birth, date of birth, contact address and notes. Add a face recognition photo and click "Save" to complete the employee creation operating.



Upload a face recognition photo description

- **Upload from local**

  Click "Upload from local" to open the local folder, select the jpg and png portrait photos in the folder.

  Note: Portrait photo specifications

  1. Please choose a front-and-bareheaded photo in the past three months, with clear and even-light image.

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

  3. Faces should account for more than 1/3 of the photo, avoiding photo blurring, wearing sunglasses, excessive facial-up, and head rotations.

➢ **Register from device**

Click "Register from Device" to open the Select Device window and select an online device. Once determined, the device will enter the photo state. After the photo is taken and verified, the photo will be sent back here from the client.

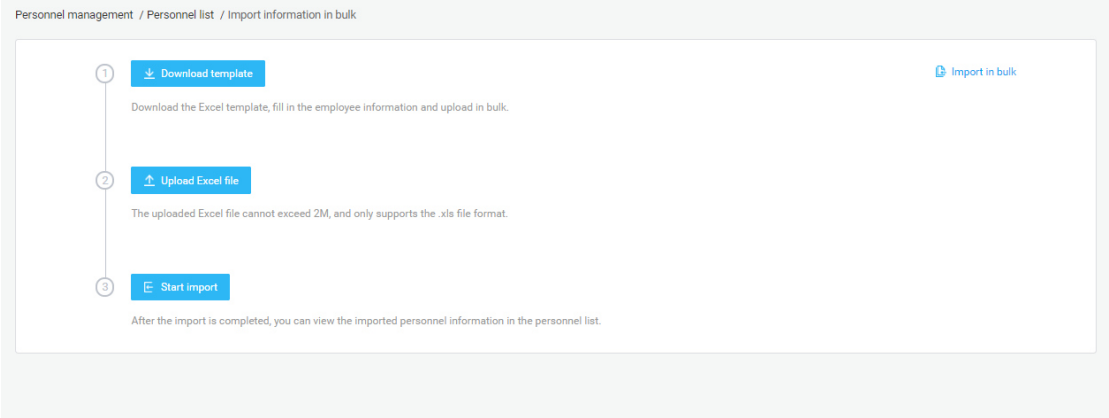
4.1.2 Import employee information in bulk

Steps: In the [Employee list], click the "Add in Bulk - Information Import in Bulk" button.

1) First step, click "Download Template". Download the excel template file to your computer with the file name "MIPS Personnel Add Template in Bulk.xls". Then fill in the employee information in bulk.

2) In the second step, click "Upload excel file". Select the excel file with the employee information filled in and upload it. If the file is uploaded successfully, the upload success status and file name will be displayed.

3) In the third step, click "Start import". During the import, there will be a progress bar showing "Importing personnel information (1 / total number of people)". After the import is completed, it prompts "Successful batch import of personnel information". After the import is completed, return to the [Person List] to view the imported personnel information.



Description of import method

- Import without overwriting: When importing a file two or more times, duplicate employees are not imported. And the system will prompt abnormal duplicate information.
- Overwrite import: The second import will overwrite the information of the employee that was imported

for the first time without prompting for duplicate information.

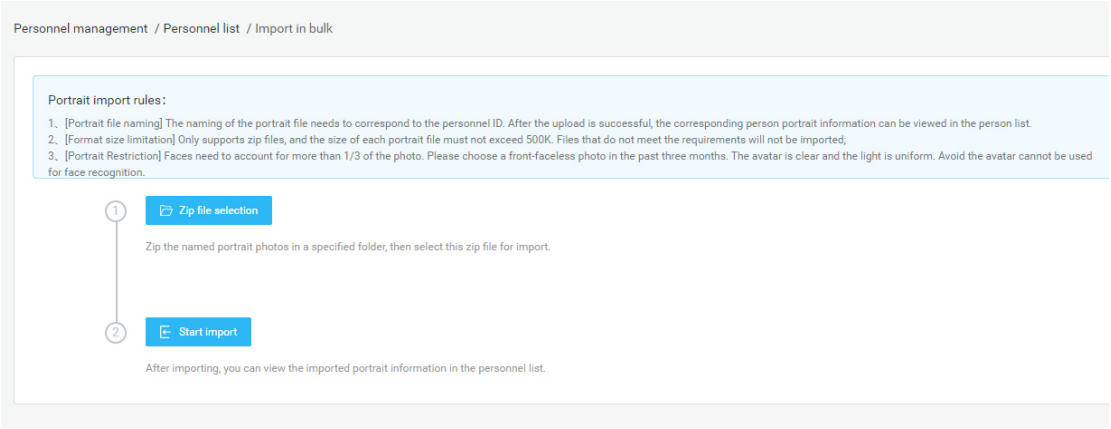
Description of import failure exception

- The content or format of the uploaded excel file is incorrect and does not meet the template specifications. Click to start the import, and a prompt will appear: "The file content or format is incorrect. Please fill in the employee information according to the template requirements.
- A field in the employee is malformed or should not be duplicated. After the import fails, the reason for the failure will be notified in a table. After modification, you can re-import.

4.1.3 Import portrait photos in bulk

Steps: In the [Employee list], click the "Add in bulk - Portrait import in bulk".

1) Step 1, click "Zip file selection" to open the Select Folder window and select the file upload. After the file upload is successful, the current file storage path is displayed.
2) Step 2, click "Start Import", and a progress bar will be displayed during the import: the number of imported files / the total number of folders. And there will be a prompt message: x sheets have been successfully imported, x sheets failed. After the import is complete, the progress bar displays: The portrait photos in this folder have been imported.



Description of portrait import rules:

- [Portrait file naming] The naming of the portrait file needs to correspond to the personnel ID. After the upload is successful, the corresponding person portrait information can be viewed in the person list.
- [Format and size] Only two file formats of jpg and png are supported, and the size of each portrait file must not exceed 500k. Files that do not meet the requirements will not be imported.

- [Portrait Restriction] Faces need to account for more than 1/3 of the photo. Please choose a front-faceless photo in the past three months. The avatar is clear and the light is uniform. Avoid the avatar cannot be used for face recognition.
- [Select Folder Upload] After the above conditions are met, place the named portrait photos in the specified folder and select the folder to import.

Description of failed portrait import

- If the size of an image file does not meet the requirements, the import will fail. After that, a table will appear to display the information of the portrait file that has not been successfully imported. After modification, you can re-import.

4.1.4 Export employee information

In [Employee list], click the "Export" button to export all employee information in the list to the file "Employee Information.xls" and download it.

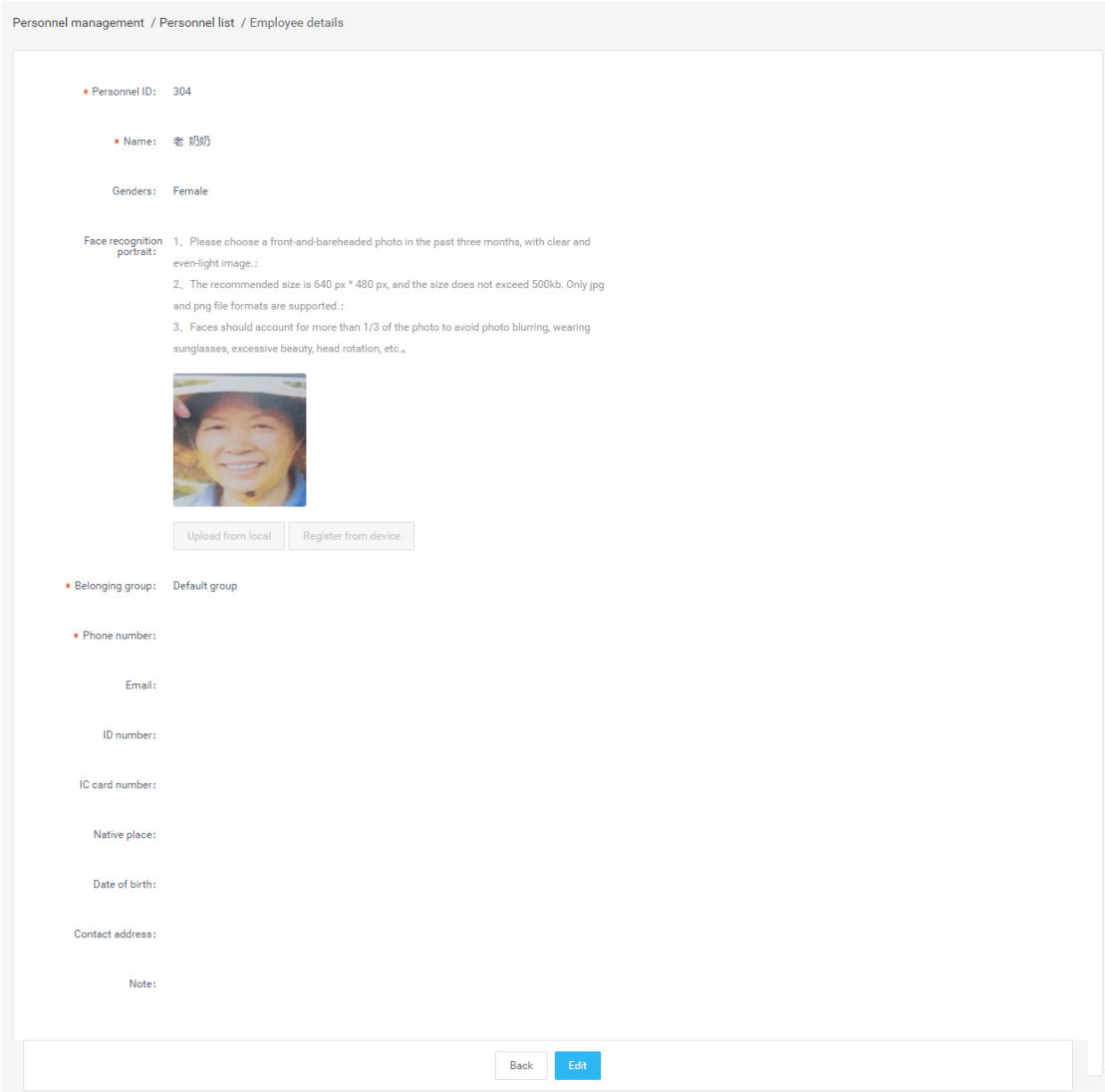
4.1.5 Refresh employee information

In [Employee list], click the "Refresh" button to refresh all employee information in the list to the latest state.

4.1.6 Staff details and editing

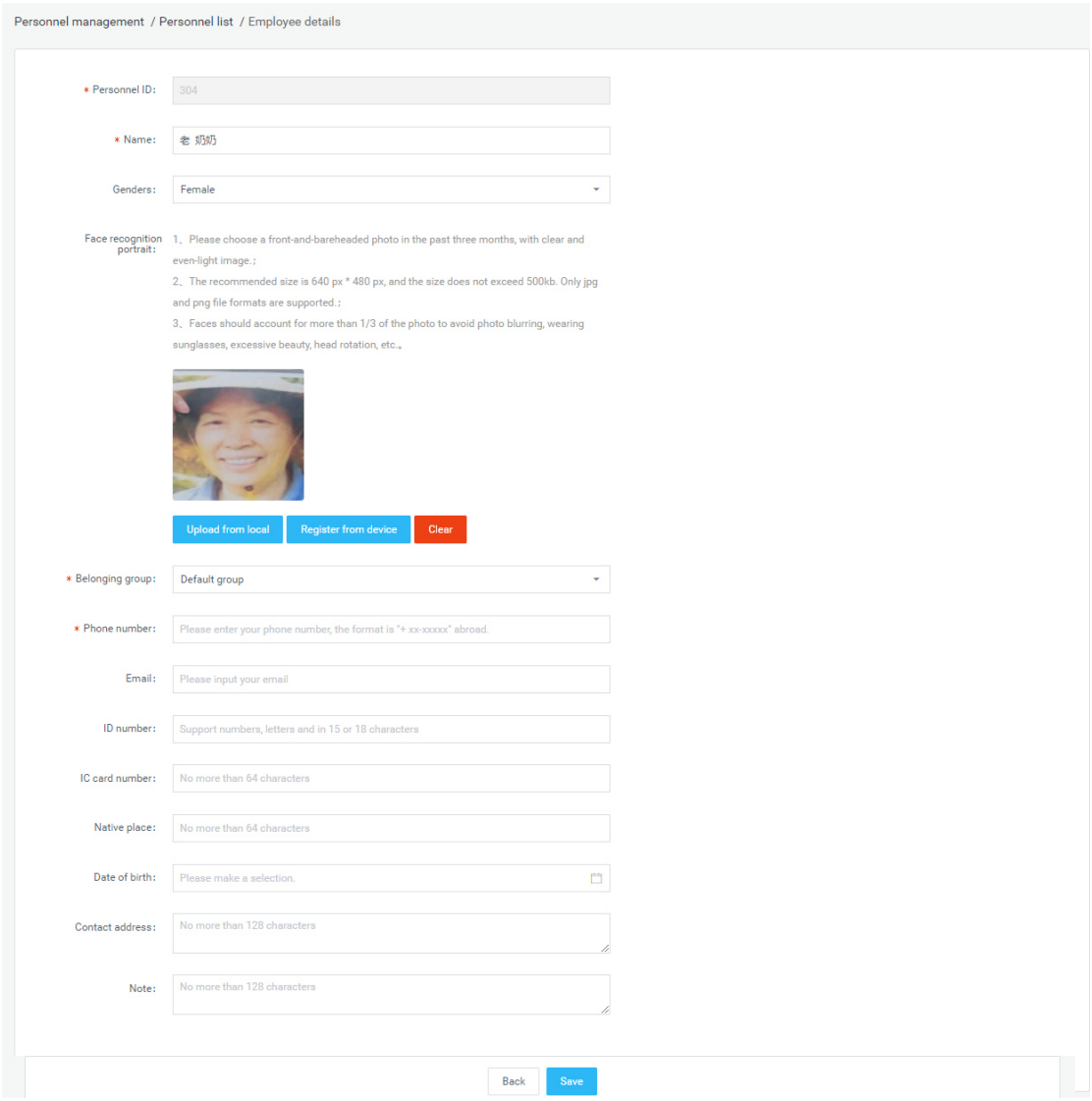
- **Employee details**

In [Employee list], after corresponding employee information, click the "Employee details" button, you can enter the details page to view specific employee information.



- **Employee edit**

On the details page, click the edit button to modify the employee's basic information and photo information. After modifying the information, click Save.

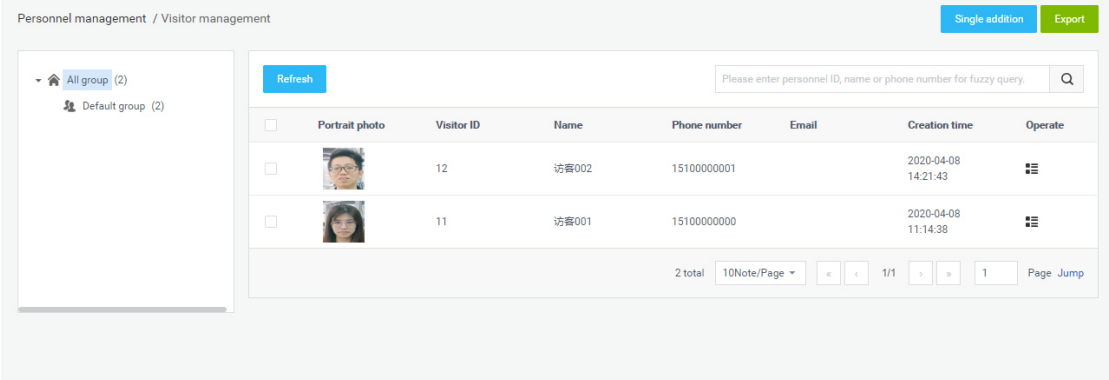


4.1.7 Employee grouping management

Employee grouping uses the organizational structure grouping by default. There is a default employee grouping under each user group. You can add, modify, or delete employee groupings on the user group by yourself. The operation is similar to the user grouping in [Group Structure].

4.2 Visitor management

Visitor management is used to view, add, edit, and export visitor information.

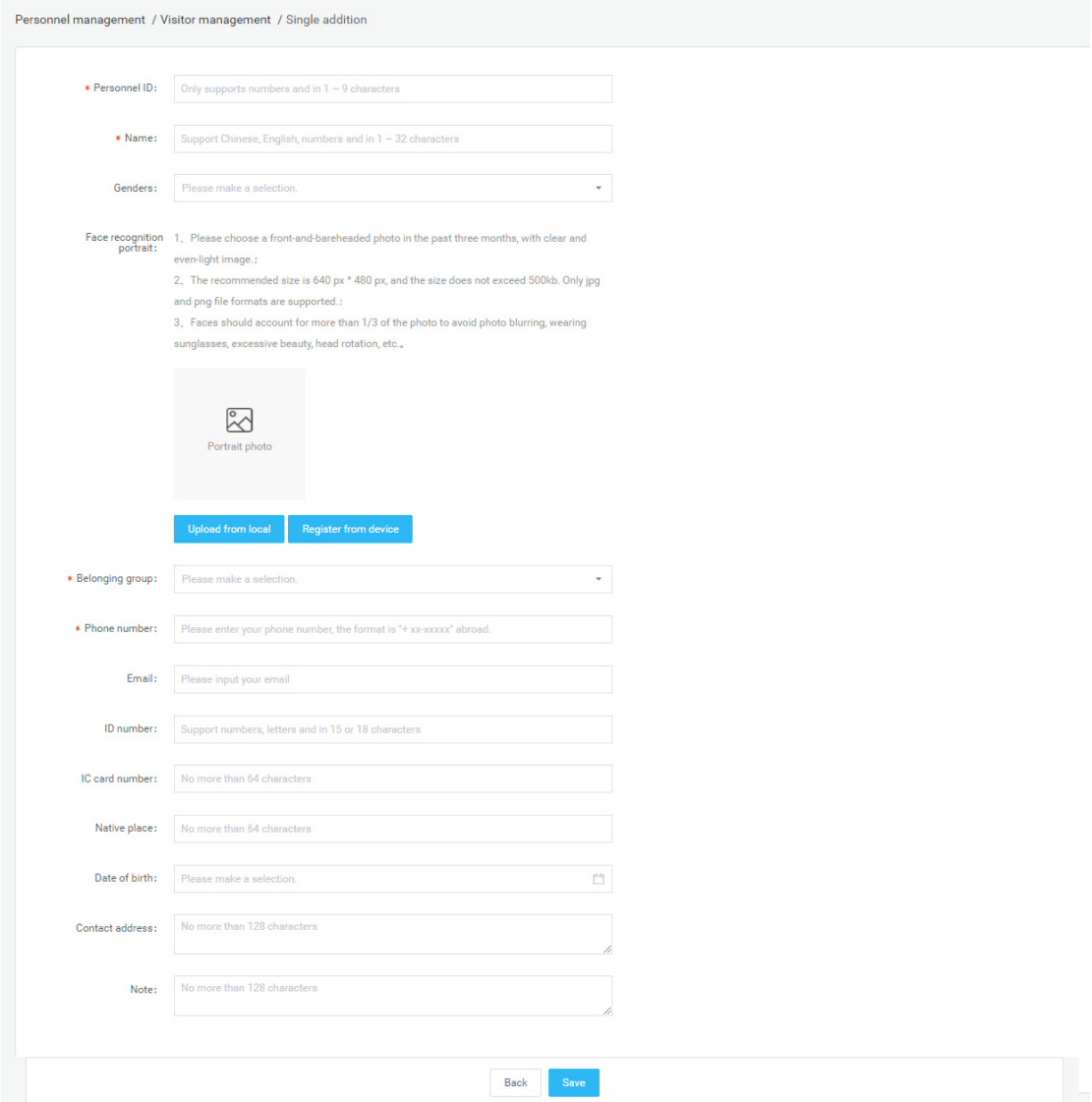


4.2.1 Add visitor individually

Steps:

1) In [Visitor Management], click the "Single Add" button to enter the visitor adding page.

2) Fill in the visitor ID, name, gender, affiliation group, mobile phone number, ID card number, IC card number, ethnicity, nationality, date of birth, contact address and remarks, add face recognition photos and click "Save" to complete the visitor operating.



Upload a face recognition photo description

- **Upload from local**

  Click "Upload from local" to open the local folder, select the jpg and png portrait photos in the folder.

  Note: Portrait photo specifications

  4. Please choose a front-and-bareheaded photo in the past three months, with clear and even-light image.

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

  6. Faces should account for more than 1/3 of the photo, avoiding photo blurring, wearing sunglasses, excessive facial-up, and head rotations.

- **Register from device**

Click "Register from Device" to open the Select Device window and select an online device. Once determined, the device will enter the photo state. After the photo is taken and verified, the photo will be sent back here from the client.

4.2.2 Export visitor information

In [Visitor management], click the "Export" button to export all visitor information in the list to the file "Visitor information.xls" and download it.

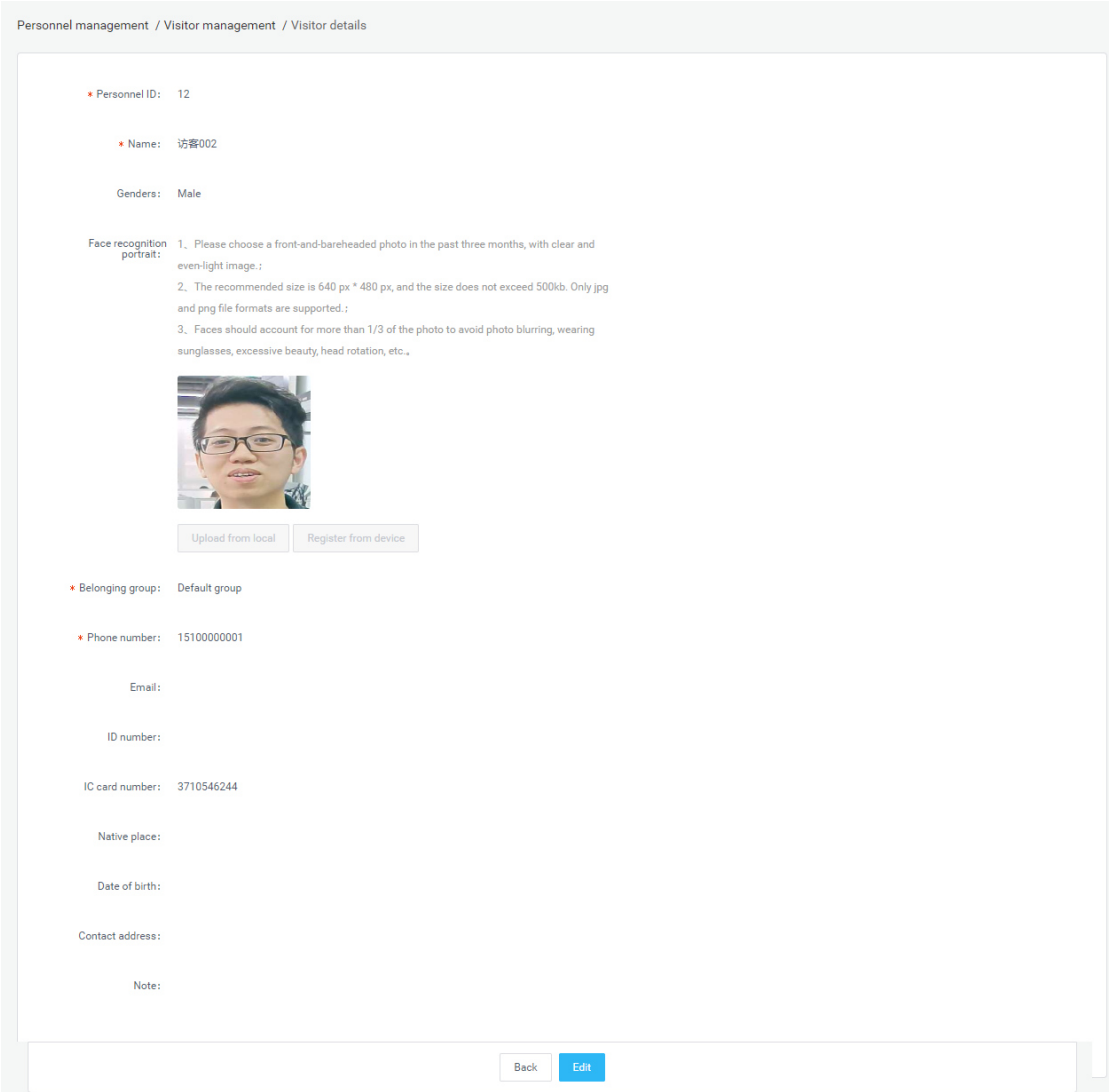
4.2.3 Refresh visitor information

In [Visitor management], click the "Refresh" button to refresh all visitor information in the list to the latest state.

4.2.4 Visitor details and editing

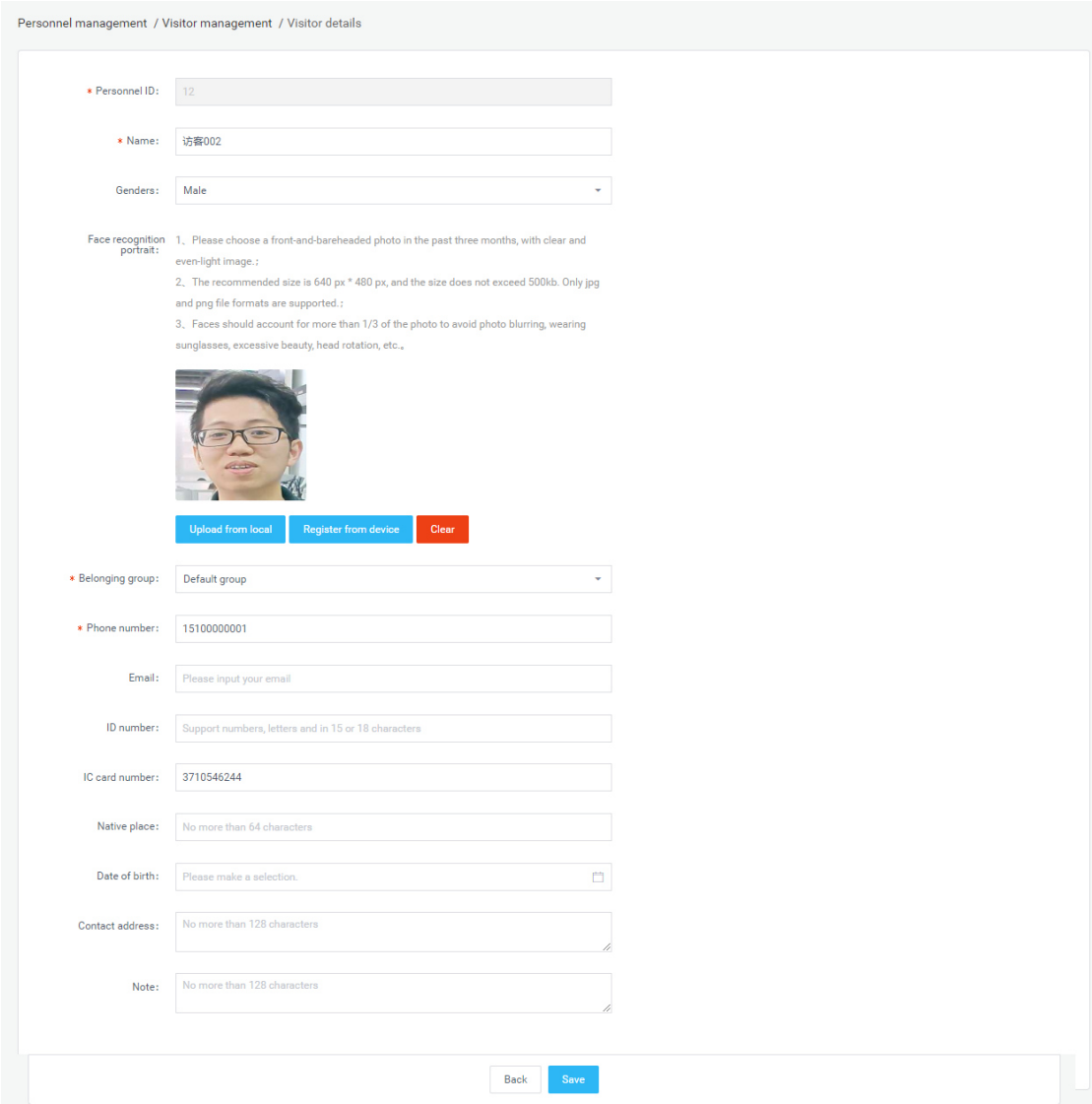
- **Visitor details**

In [Visitor management], after corresponding visitor information, click the "Visitor details" button to enter the details page to view specific visitor information.



- **Visitor edit**

On the details page, click the edit button to modify the visitor's basic information and photo information. After modifying the information, click Save.

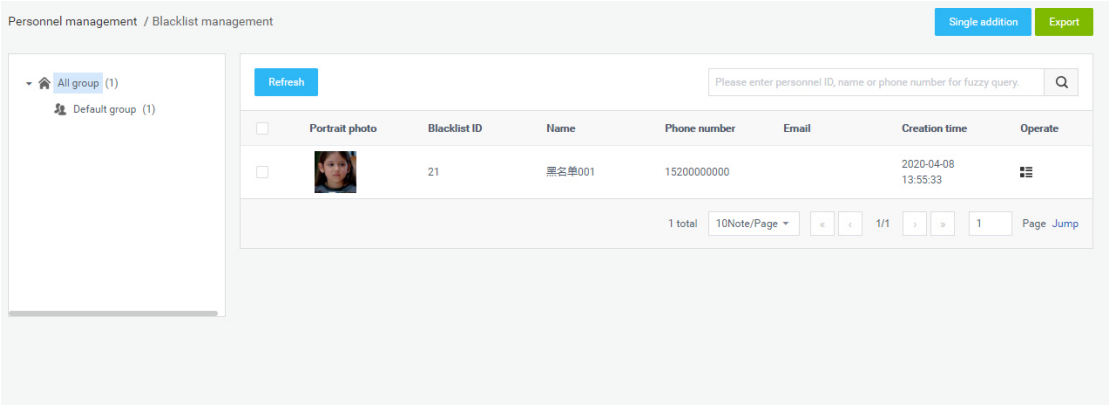


4.2.5 Visitor grouping management

Guest grouping uses the organizational structure grouping by default. Each user group has a default guest grouping, which can add, modify, and delete guest groups on the user grouping. The operation is similar to the user grouping in the [Group structure], which is not described in detail.

4.3 Blacklist management

Blacklist management is used to view, add, edit, and export blacklist information.

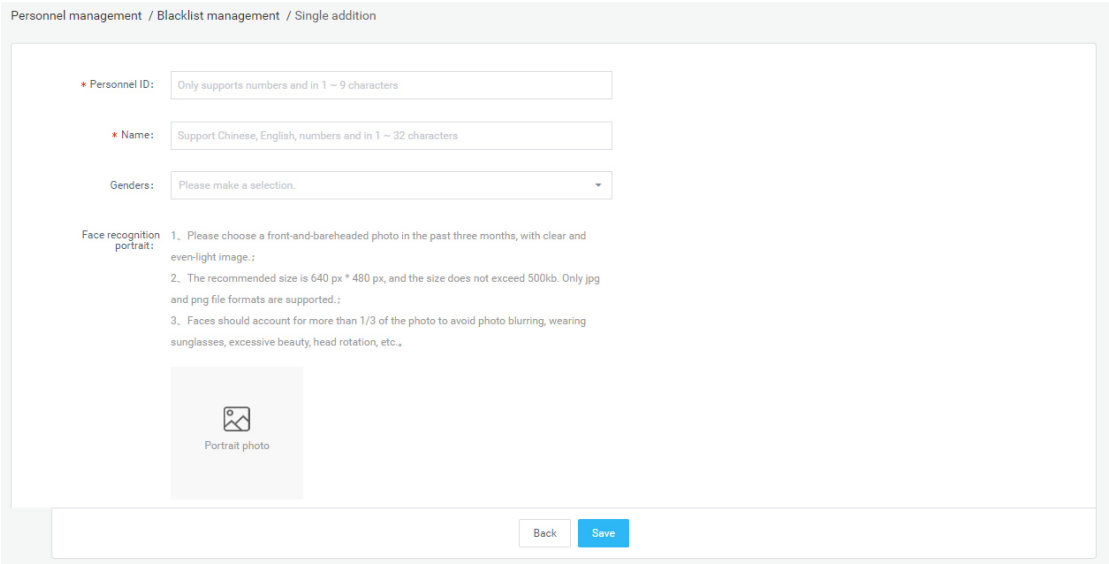


4.3.1 Add blacklist individually

Steps:

1) In [Blacklist management], click the "Single Add" button to enter the blacklist addition page.

2) Fill in the blacklist ID, name, gender, belonging group, phone number, ID card number, IC card number, ethnicity, birthplace, date of birth, contact address and remarks. Add face recognition photos and click "Save" to complete the blacklist create operation.



Upload a face recognition photo description

- **Upload from local**

  Click "Upload from local" to open the local folder, select the jpg and png portrait photos in the folder.

  Note: Portrait photo specifications

  7. Please choose a front-and-bareheaded photo in the past three months, with clear and even-light image.

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

9. Faces should account for more than 1/3 of the photo, avoiding photo blurring, wearing sunglasses, excessive facial-up, and head rotations.

4.3.2 Export blacklist

在【黑名单管理】，点击“导出”按钮，可将列表中所有黑名单信息导出到文件“黑名单信息.xls”并下载。

In [Blacklist management], click the "Export" button to export all the blacklist information in the list to the file "Blacklist information.xls" and download it.

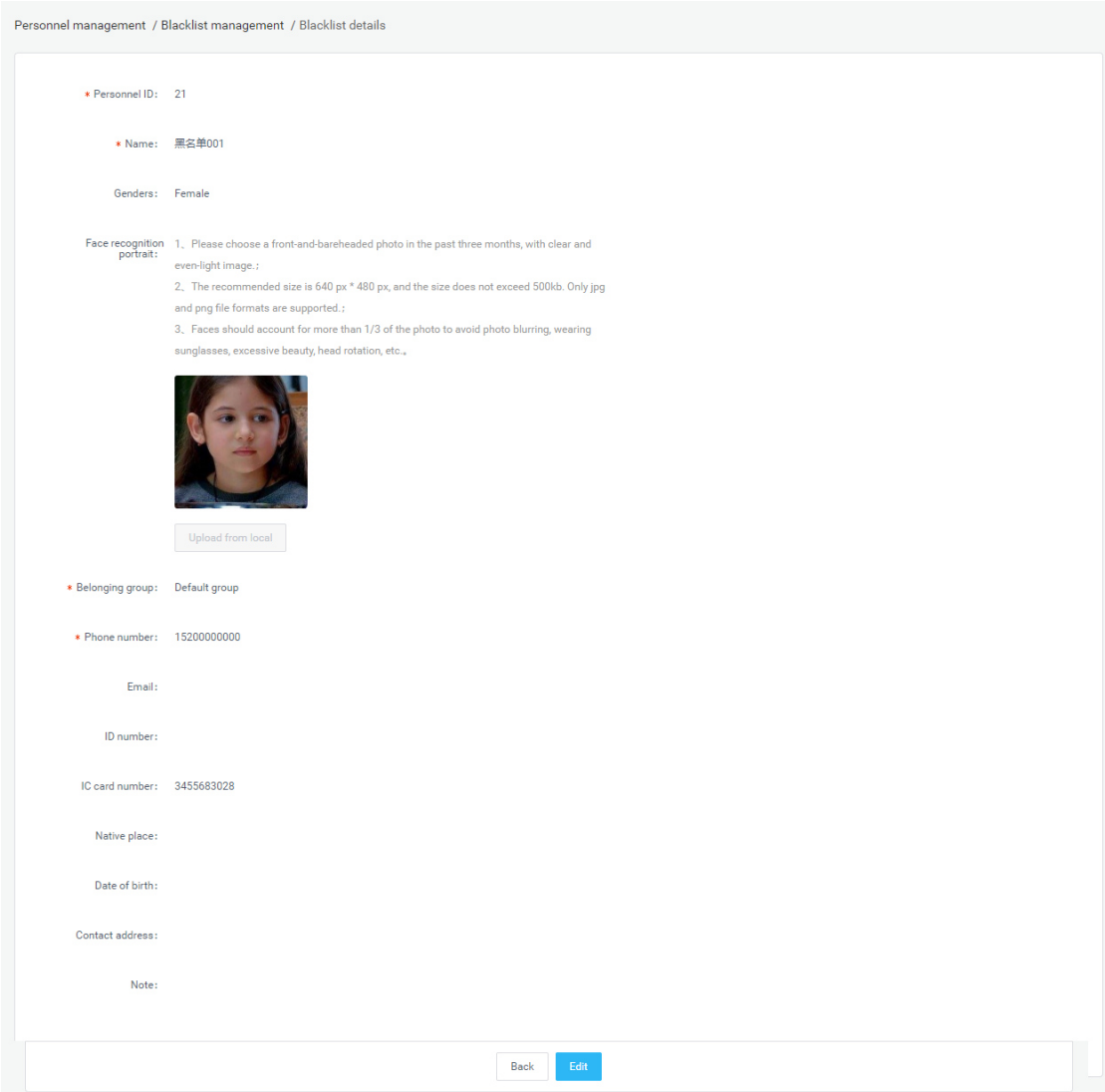
4.3.3 Refresh blacklist information

In [Blacklist management], click the "Refresh" button to refresh all the blacklist information in the list to the latest state.

4.3.4 Blacklist details and editing

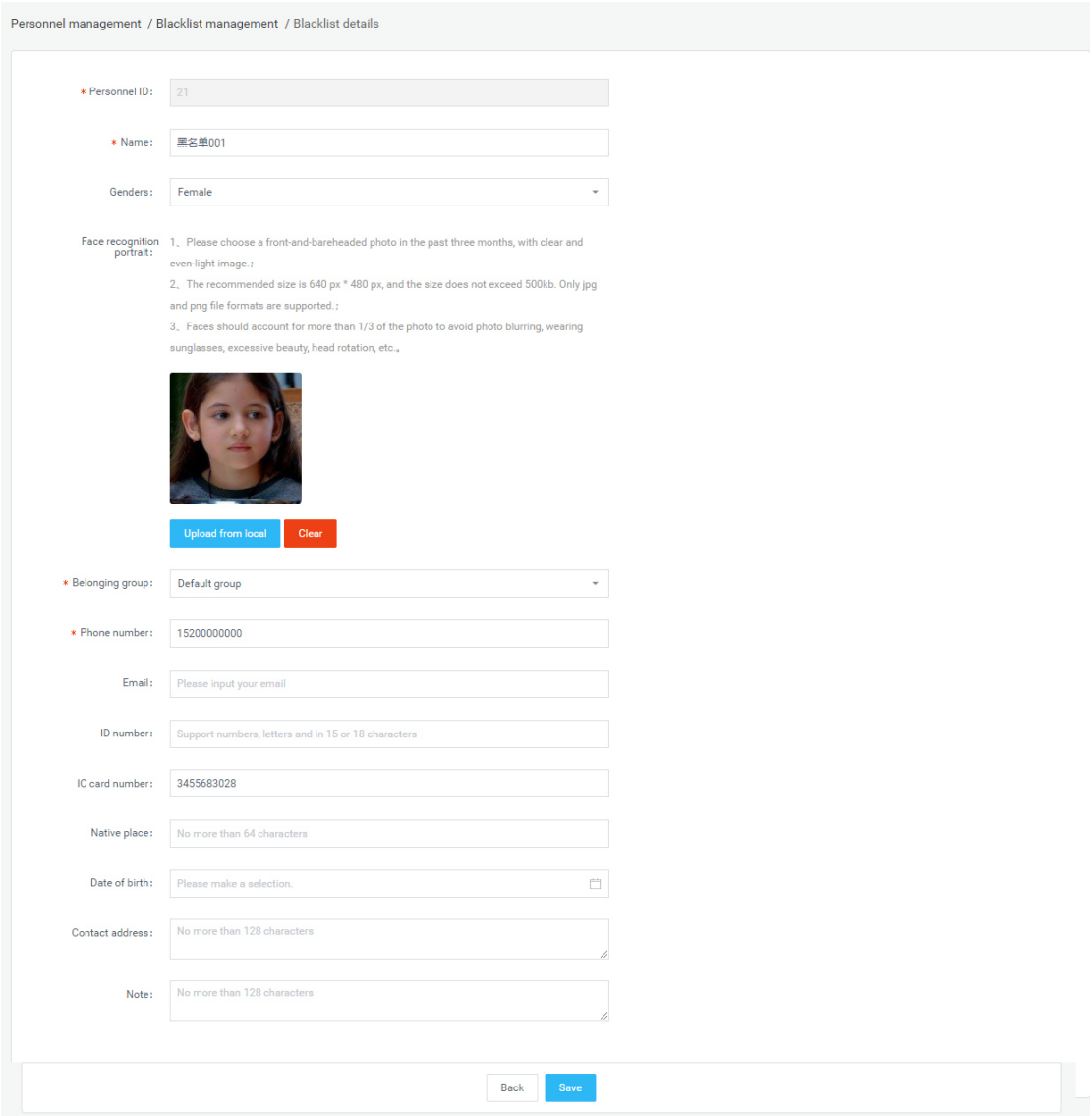
- **Blacklist details**

In [Blacklist management], after corresponding to the blacklist information, click the "Blacklist details" button to enter the details page to view the specific blacklist information.



- **Blacklist edit**

On the details page, click the edit button to modify the basic information and photo information of the blacklist. After modifying the information, click Save.



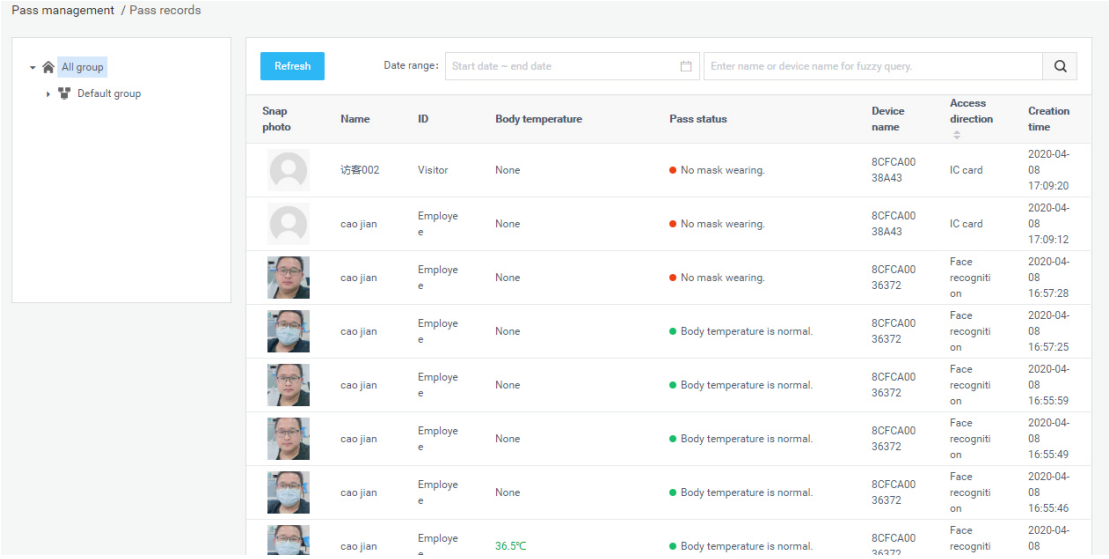
4.3.5 Blacklist grouping management

The blacklist group uses the organizational structure group by default. Each user group has a default blacklist group. You can add, modify, and delete blacklist groups on the user group. The operation is similar to the user grouping in [Group Structure].

5.Chapter Five Pass Management

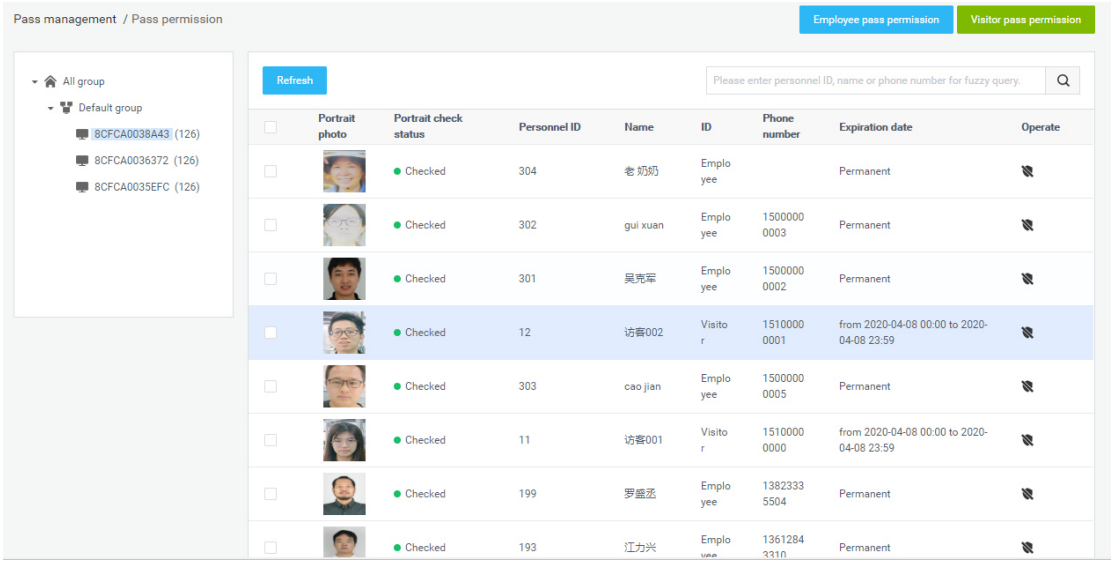
5.1 Pass records

View all the identification records on the device, which can be grouped and filtered by device. The data body temperature value is greater than or equal to 37.3 degrees to display red font, less than 37.3 degrees to display green font, no temperature data display "none". There are three passage states: normal body temperature, abnormal body temperature and no mask.



5.2 Pass permission

Manage the access rights of added employees and visitors.

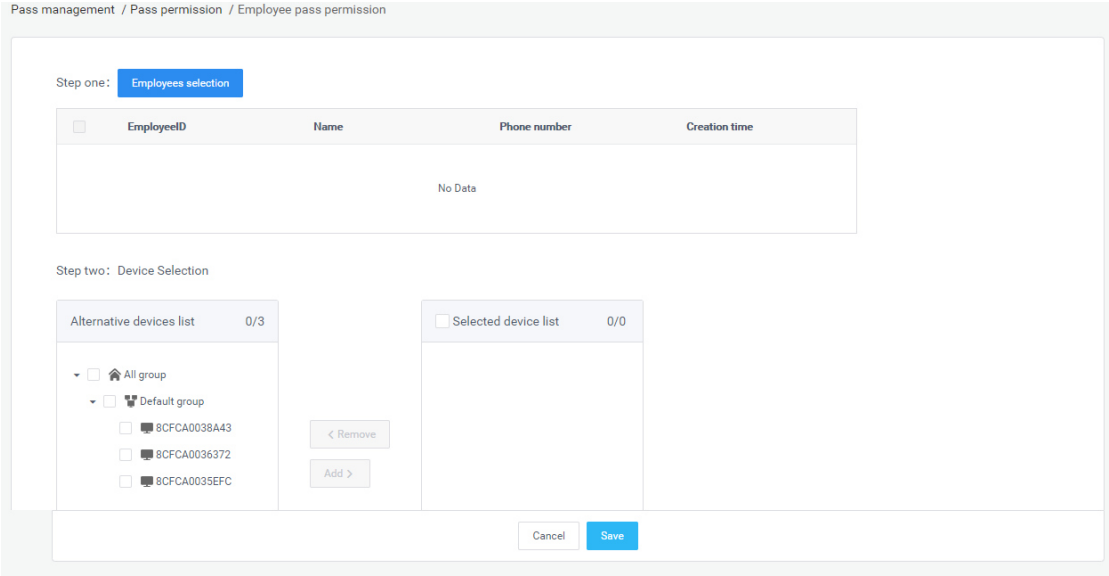


5.2.1 Employee pass permission settings

Steps: Enter the [Pass permission] page and click the "Employee Access Authorization" button.

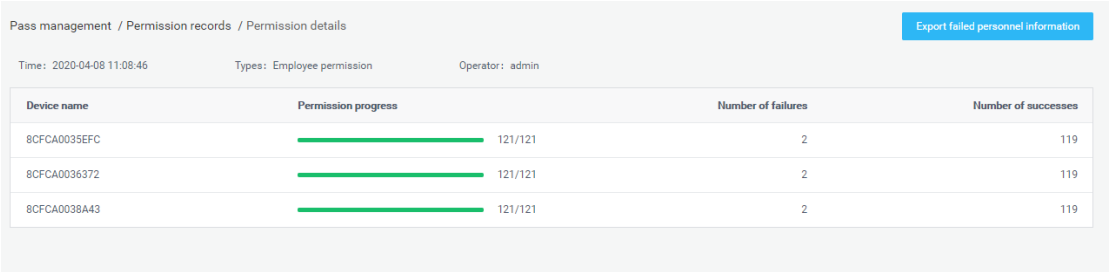
- **Pass permission**

1) Select personnel, devices, pass permission and permanent effective time, and click "Save" button to start pass permission. After the device is successfully authorized, the person can pass the gate and the validity period is permanent.
2) Select personnel, devices, pass permission and temporary effective time, and click "Save" button to start pass permission. After the device is successfully authorized, the person can pass through the gate within the time range set by the validity period. If the validity period is exceeded, the recognition fails.



Description of Pass permission:

- **Click the Save button to start the pass permission. Present the current synchronization status, authorization progress, number of successes and failures of each device in the form of a list, and display device names.**
- **The person who failed the authorization is recorded in the "Verification Failure Description" table. You can click "Export Settings Failed Number" to export and view the authorization failure information.**
- **The person who fails the authorization, after modifying the corresponding failure information, can re-authorize until the authorization is successful.**



- **Revoke pass permission**

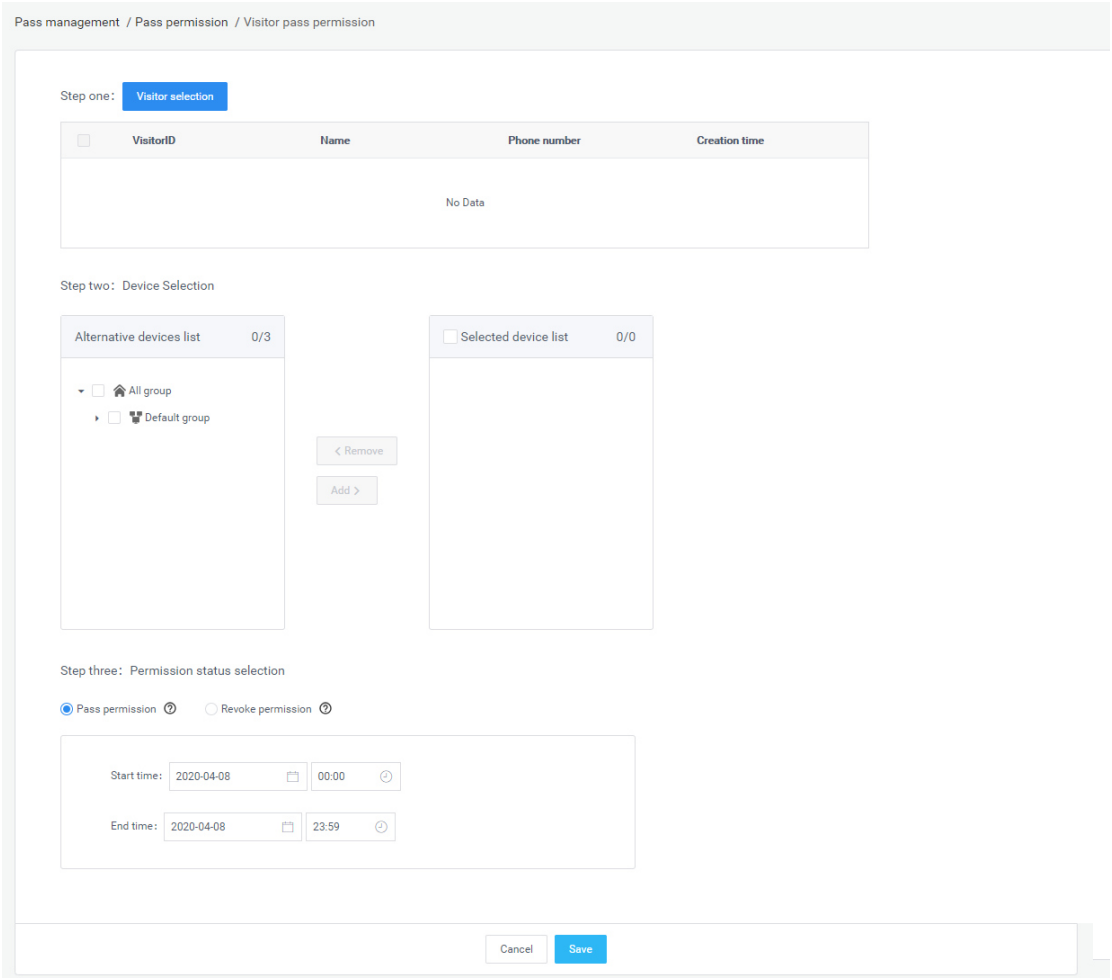
Select a person, select a device, de-authorize, and click the "Save" button to start revoking the permission. The de-authorization is the same as the "pass permission" logic, except that the selected person is removed from the selected device.

5.2.2 Visitor pass permission settings

Steps: On the [Pass permission] page, click the "Visitor pass permission" button.

- **Pass permission**

Select the visitor, select the device, pass permission and valid time range, and click the "Save" button to start the pass permission. After successful authorization on the device side, the visitor can pass the gate to be valid within the set effective time range.



Description of pass permission:

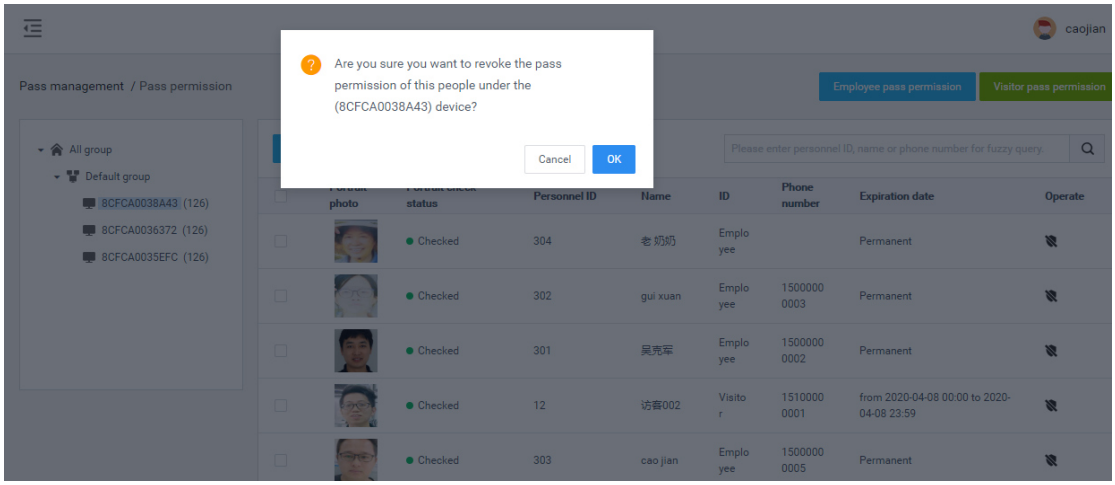
- **Click the Save button to start the pass permission. Present the current synchronization status of each device in the form of a list, showing the device name, synchronization pass permission, number of successful and failed. The person who failed the permission is recorded in the "Verification Failure Description" table. You can click "Export Settings Failed Number" to export and view the permission failure information.**
- **Visitors who have failed authorization can revise the authorization after revising the corresponding failure information until the authorization is successful.**

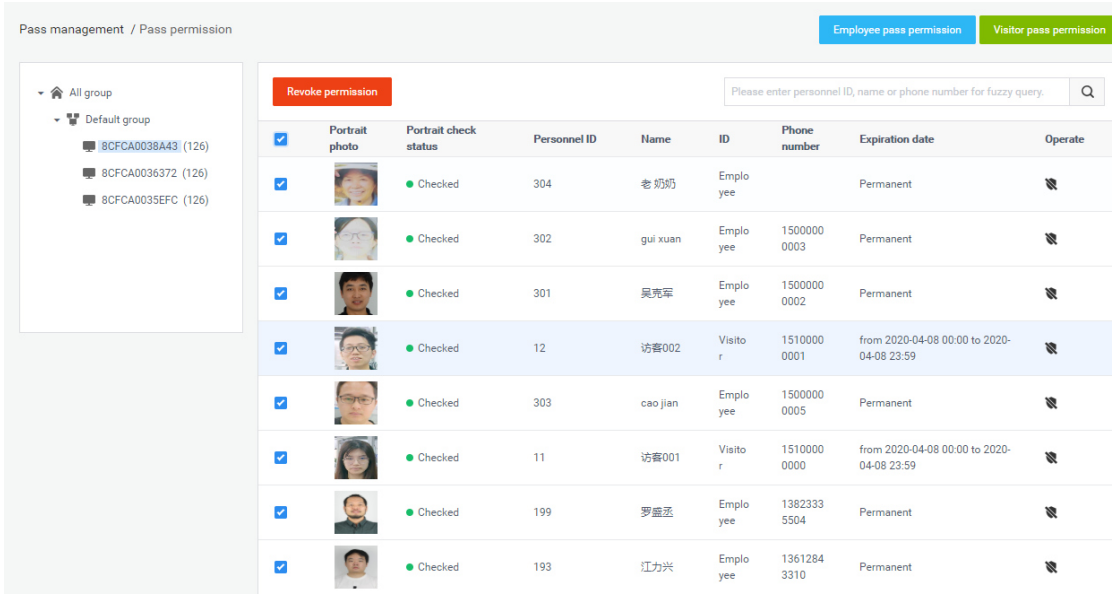
- **Revoke pass permission**

  Select personnel and equipment, and revoke the permission. Click the "Save" button to start. Revoke permission is the same as "Pass permission", except that the reassigned personnel are removed from the original equipment.

5.2.3 Revoke permission

In the authorized personnel list, you can click the "Revoke permission" button behind the list record to release the authorization. After the removal is successful, the corresponding employees and visitors will have no pass permissions. You can also check personnel records and click "Remove permissions" for batch operations.





5.2.4 Refresh permission information

On the [Pass permission] page, click the "Refresh" button to refresh all authorized information in the list to the latest state.

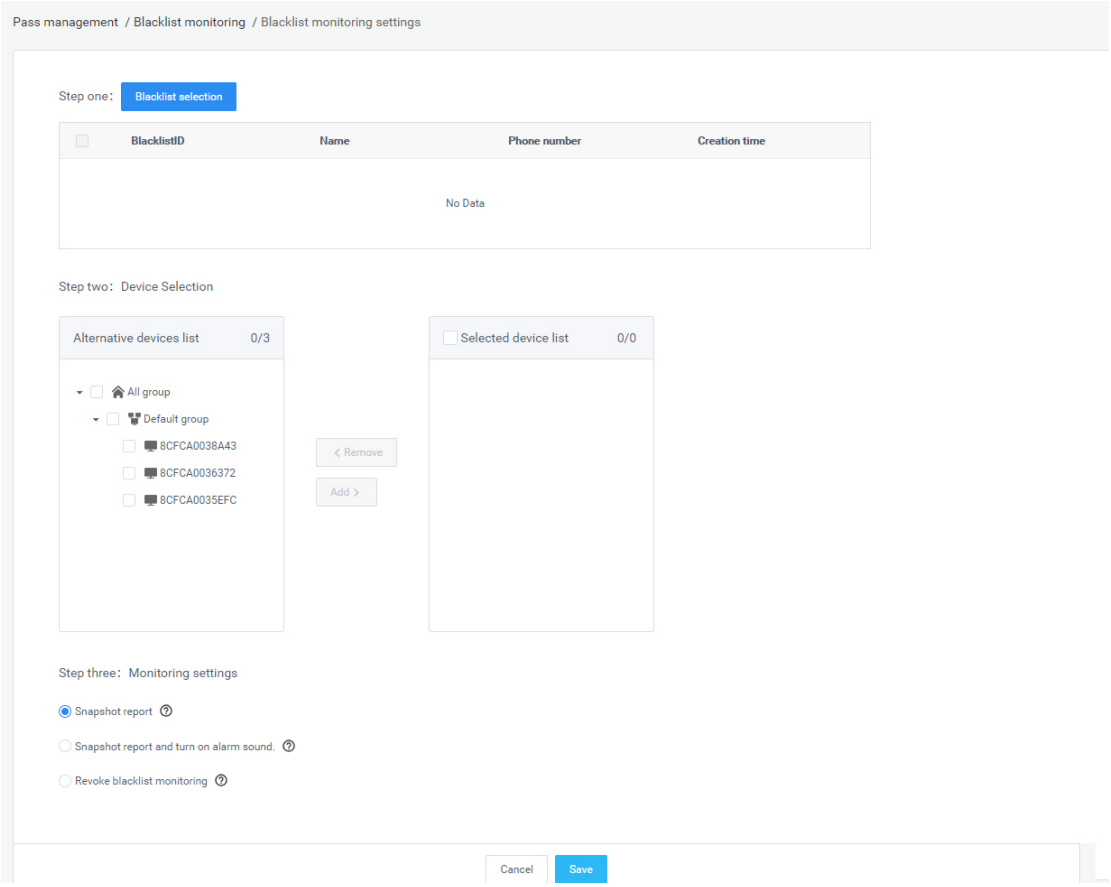
5.3 Blacklist monitoring

5.3.1 Blacklist monitoring settings

Steps: Enter the [Blacklist monitoring] page and click the "Blacklist monitoring settings" button.

- **Blacklist monitoring settings**

1) Select the blacklist and device and snap to report. Click the "Save" button to start the blacklist monitoring. After the device is successfully monitored, the person will be recognized and captured when reporting through the gate.
2) Select the blacklist and device, choose to enable the snapshot report function, and enable the alarm sound. Click the "Save" button to start the blacklist monitoring. After the device is successfully monitored, the person will be identified through the gate, snapped to report and emit an alarm sound.



Description of Pass permission:

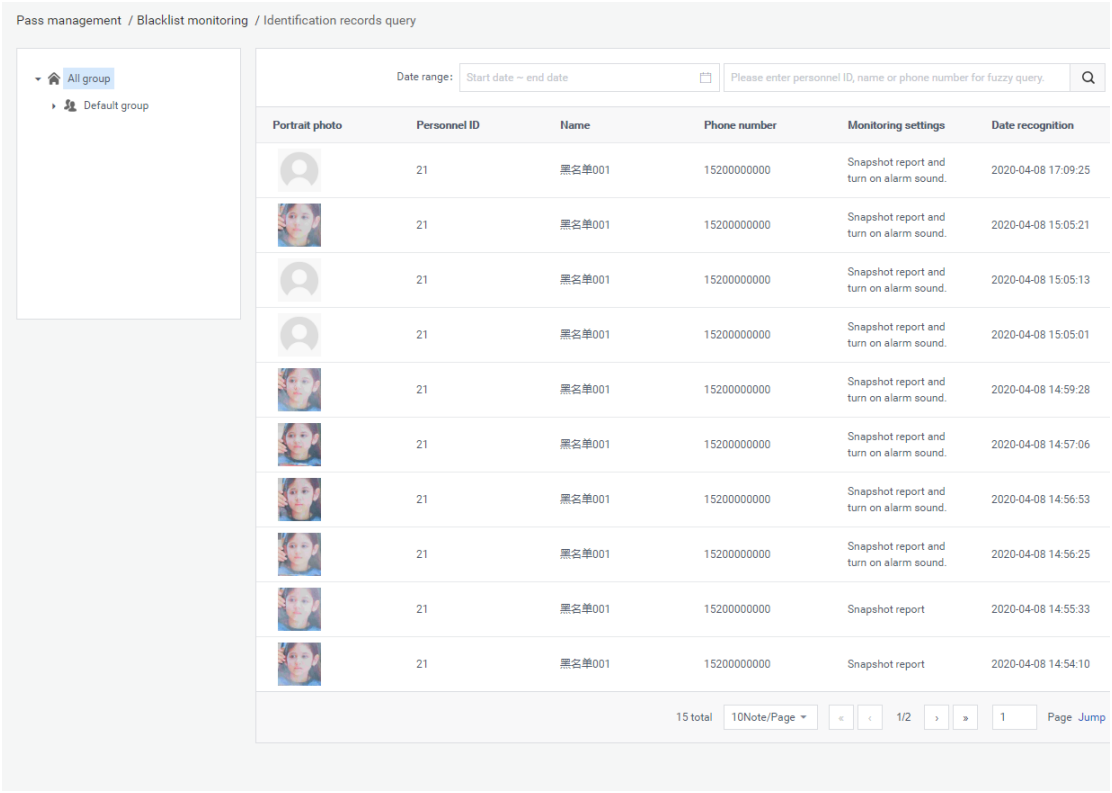
- **Click the Sure to start the blacklist monitoring. Present the current synchronization status of each device in the form of a list, display the device name, synchronization monitoring progress, the number of successful and the number of failed. The monitoring failures are recorded in the "Export Blacklist Monitoring Failure Information" table. You can click the export table to view the monitoring failure information.**
- **Blacklist personnel who failed to monitor, after modifying the corresponding failure information, can re-monitor the settings until the monitoring registration is successful.**

- **Revoke blacklist monitoring**

  Select blacklist and device, and release blacklist monitoring. Click the "Save" button to start the release.

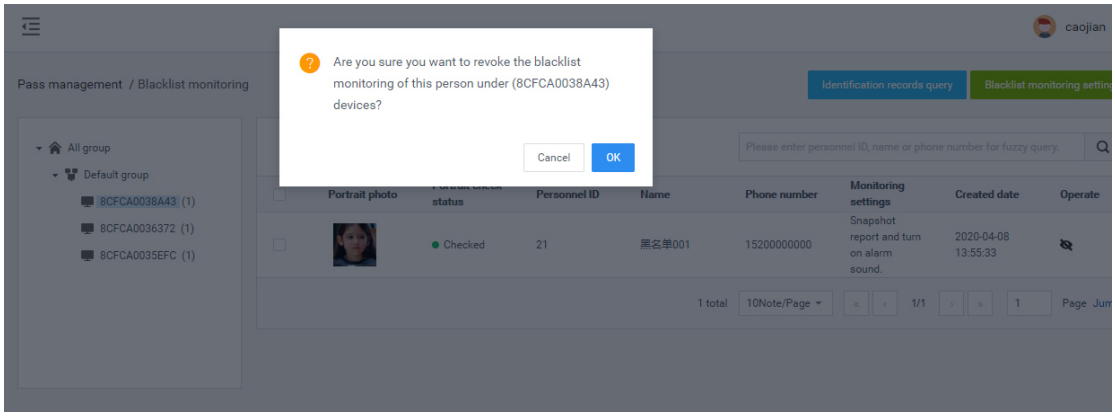
5.3.2 Identification record query

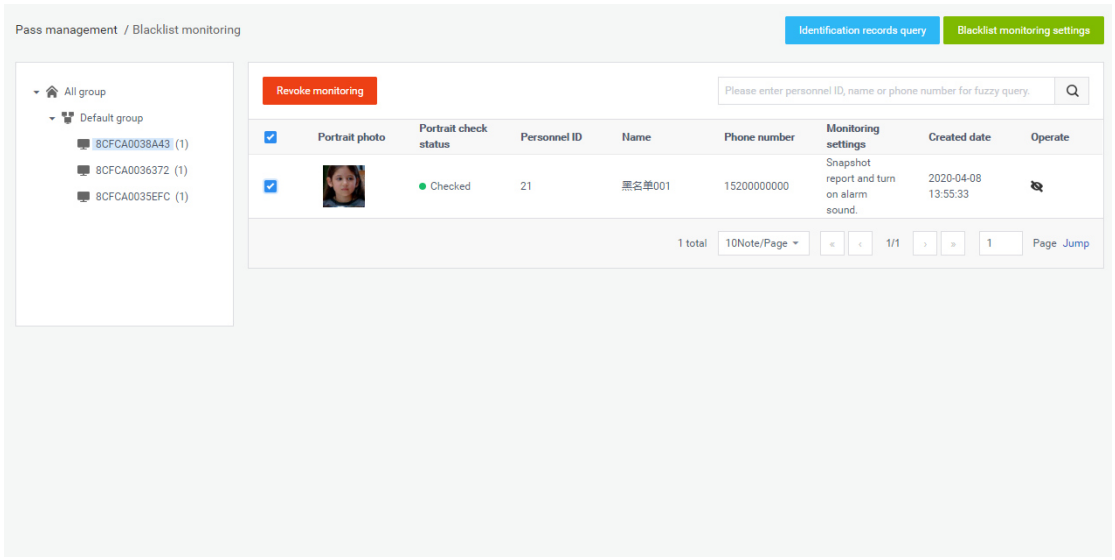
Enter the [Blacklist monitoring] page, click the "Identify Record Inquiry" button to enter the [Identify record inquiry] page, and display the identification records of all blacklist personnel. Blacklist identification records can be selected according to grouping, device, and date range inquiries.



5.3.3 Remove monitoring

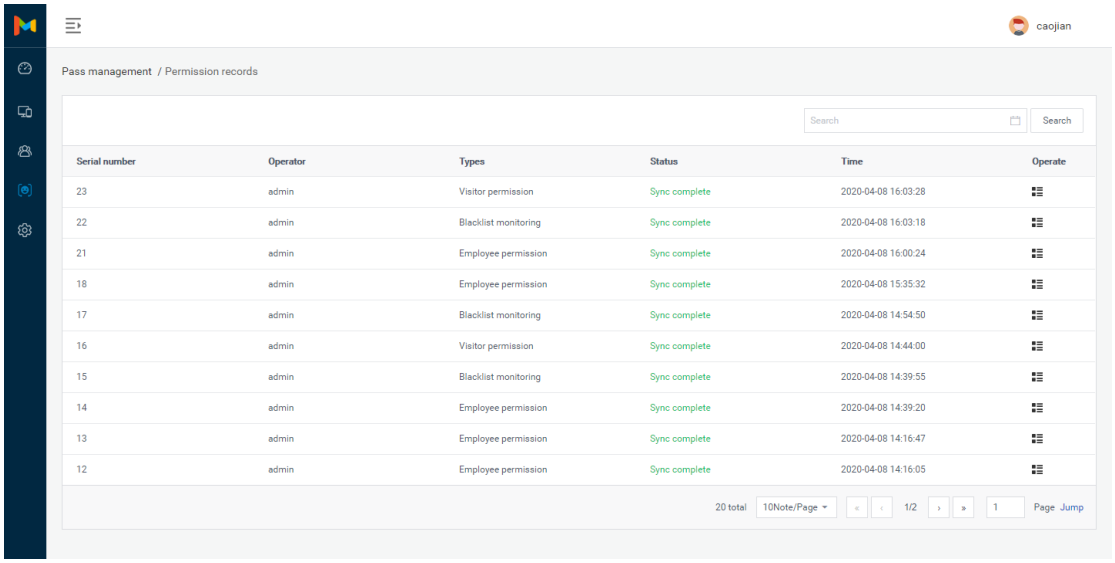
In the blacklist monitoring personnel list, you can click the "remove monitoring" button behind the list record to release monitoring. After the removal is successful, the blacklist removes the snapshot monitoring or alarm from the selected device. You can also check the personnel record and click "remove monitoring" to perform batch operations.



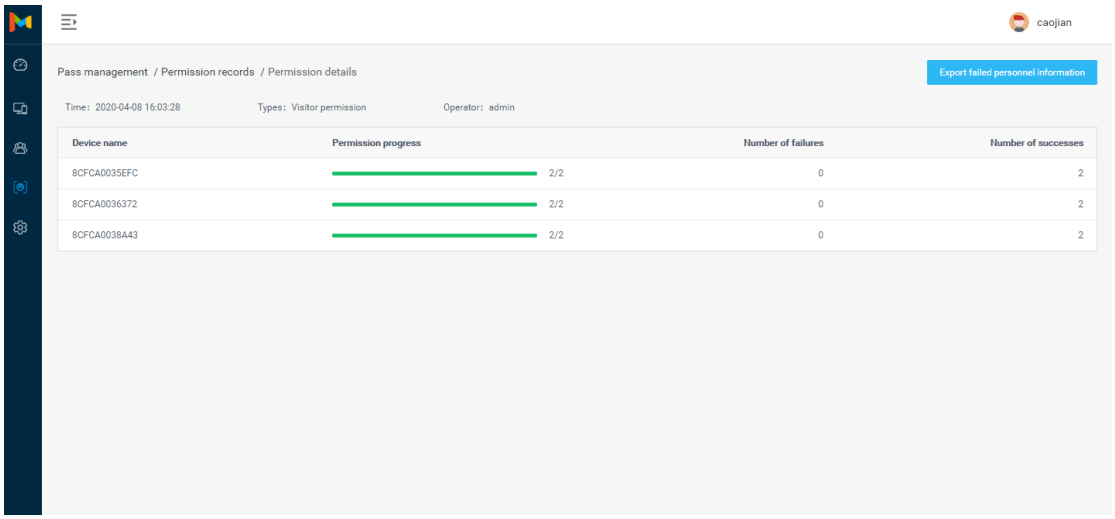


5.4 Permission records

[Permission records] The module contains the information records of the "Permission" and "Remove permission" of employees and visitors, as well as the blacklist monitoring and contact monitoring setting operations. You can enter the list to view the details of related records.



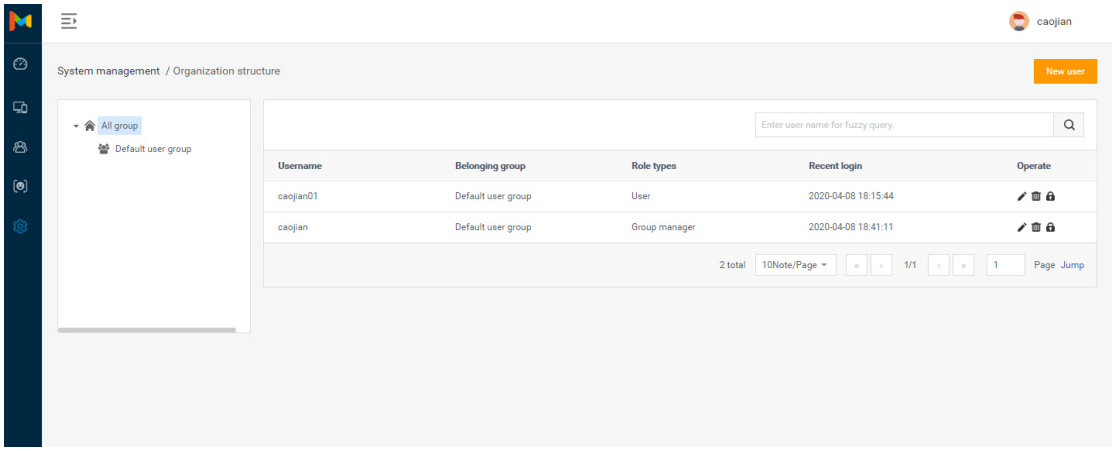
Permission details are as follow:



6.Chapter Six System Management

6.1 Group structure

[Group structure] The module is used to manage the group structure and enterprise user information management in the enterprise. The hierarchical relationship is created and managed by admin or enterprise administrator.

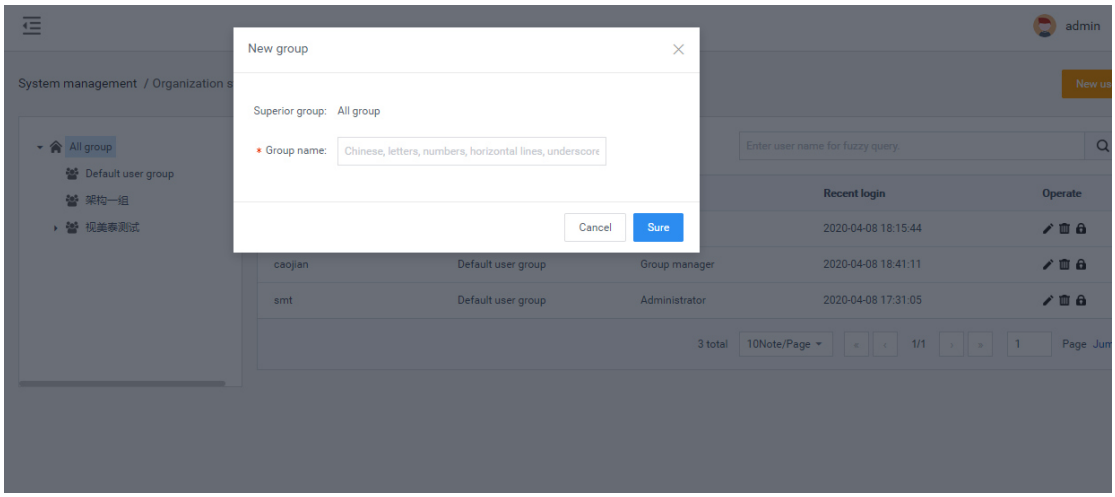


6.1.1 Attribution of business data

- Various business data generated by enterprise users will only be stored under the group structure group in the enterprise where they belong, and all business modules in the enterprise are grouped using the same group structure.
- In the same enterprise organization structure, users at a high level can access business data in a low-level structure. Conversely, low-level users cannot access high-level business data, and other companies cannot access these data.
- In the same enterprise group structure, business data between groups is visible within the group.
- An enterprise administrator can manage all business data in the organization structure of the enterprise, but cannot access data of other enterprises.

6.1.2 Group management

- Create a group: select a group and click + to enter the [New Group] page. On this page, you only need to fill in the group name and save it。
- **Modify and delete operations: (omitted)**
- Group permission description: visible in the default group

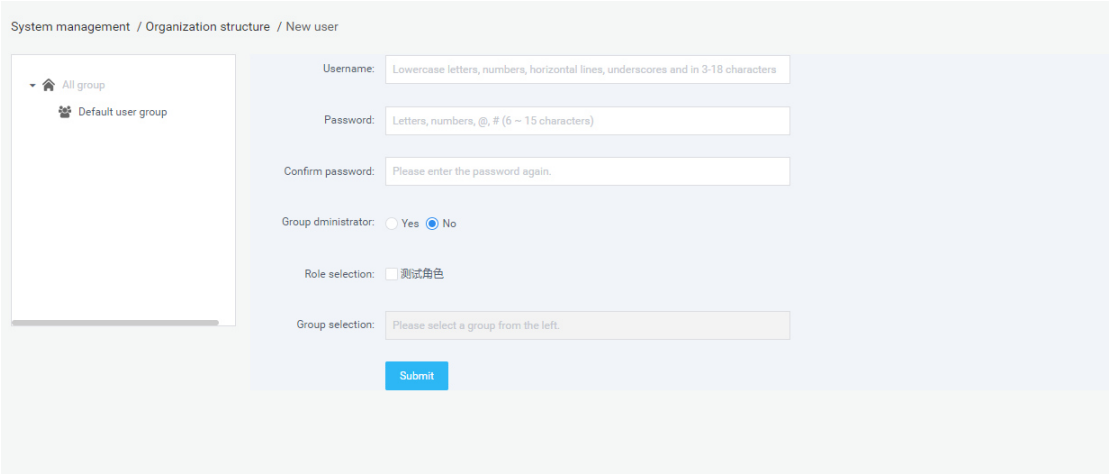


6.1.3 User management

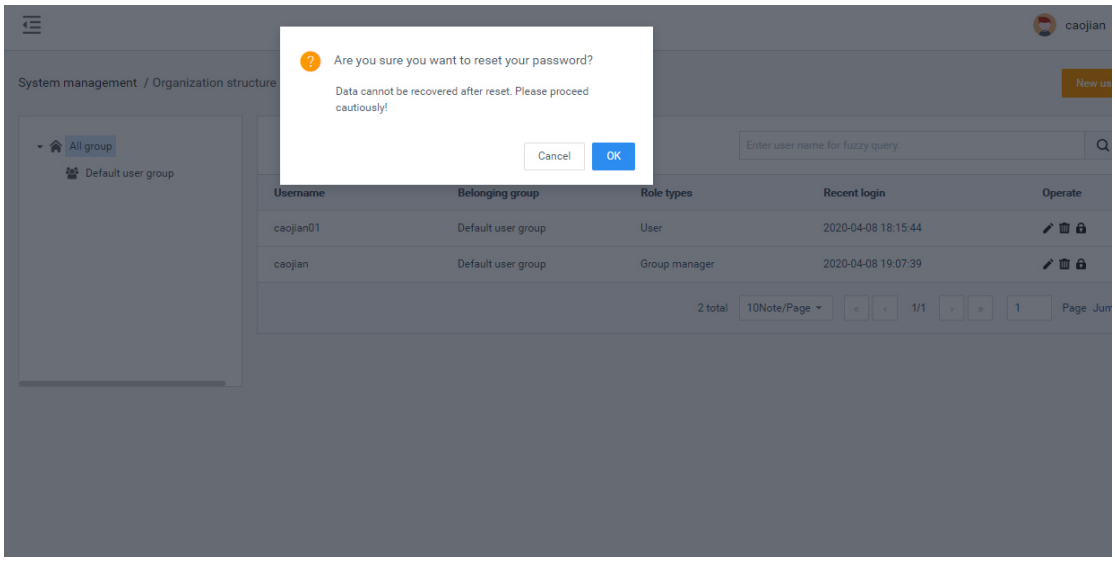
- **User creation**

  Click "Add User" to enter the [Add User] page. Select the group; fill in the user name and password; after confirming the password, group administrator and role, click "Submit", as shown below:

  Note: By default, it is a normal user. After selecting a normal user, you need to select a role; if you select an administrator, you do not need to select a role to have all the permissions under this group.



- **Modify, query, delete operations: (omitted)**
- **User password modification:** Note that only administrators (admin or company administrators) can reset passwords for users in the group. Reset the password to 123456.



6.2 Role management

[Role management] It is used to create and manage roles. Roles are used to control various business function modules and function operations of users in the system. It is composed of different function operation rights.

- **Description of roles**

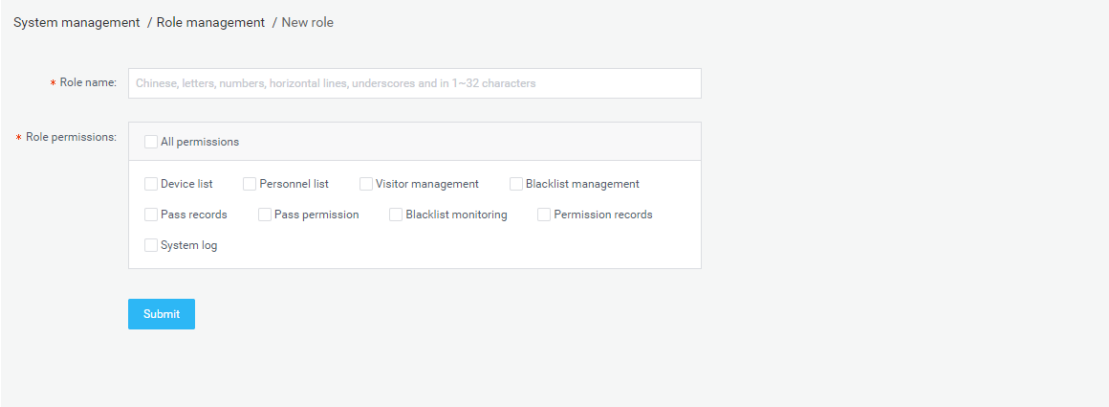
➢ Each enterprise can create one or more roles with different permission scopes, which are used to perform different functions for different users in the enterprise group structure.

➢ Role information is independent between enterprises and cannot be accessed by each other.

Note: The role of admin is the system super administrator, which can manage all the functional modules and business data in the system. Among them, the functions of [System Settings] and [Enterprise Management] can only be managed by admin users, other users cannot see these two modules, including enterprise administrator users.

- **Role creation**

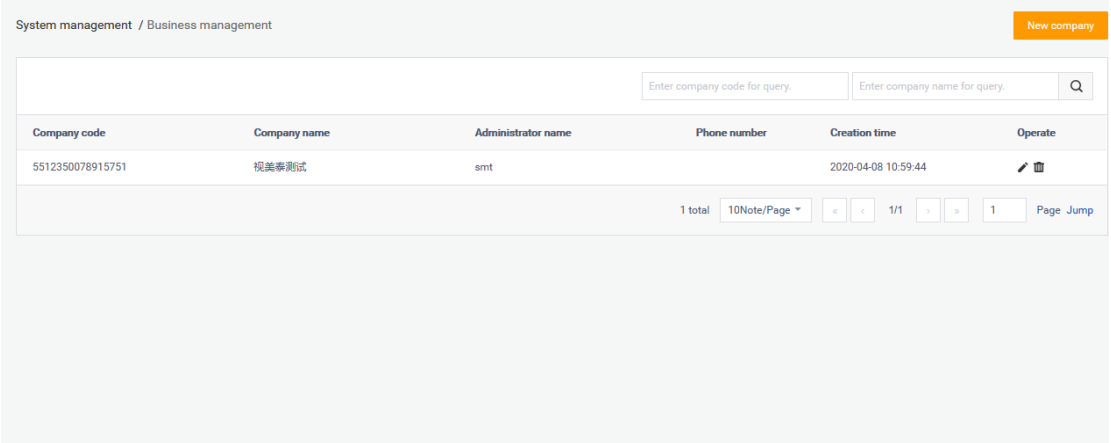
Go to [Permission Management]-[Role Management], click the "Add Role" button to enter the [Add Role] page.



6.3 Business management

[Enterprise Management] The module can only be operated by the super administrator and is used to create and manage enterprise accounts in the system. Each corporate account has corporate administrator rights and can be used to log in to the system. After logging in to the system, the account can manage the organizational structure, users, and roles within the enterprise, and can view and manage all business data created by the enterprise users. But there is no operation authority for the [System Settings] and [Enterprise Management] functions, nor can you see the data of other enterprise users.

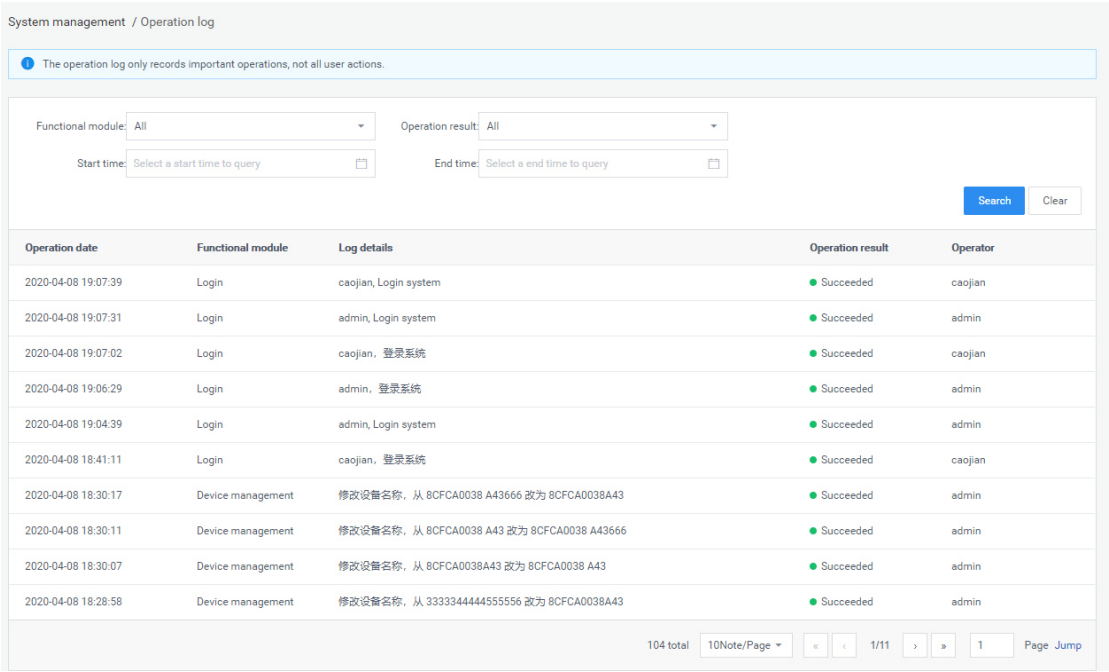
Super administrators can create, modify, query, and delete enterprises, as shown in the following figure:



Note: Enterprise delete operation is supported. After deleting an enterprise, all data associated with the enterprise will be deleted, and the devices under the enterprise will belong to the admin default group.

6.4 System log

[System Log] The system log list on the page contains the user's operation date, function modules, log details, operation results, operator and other information records during the use of the system.

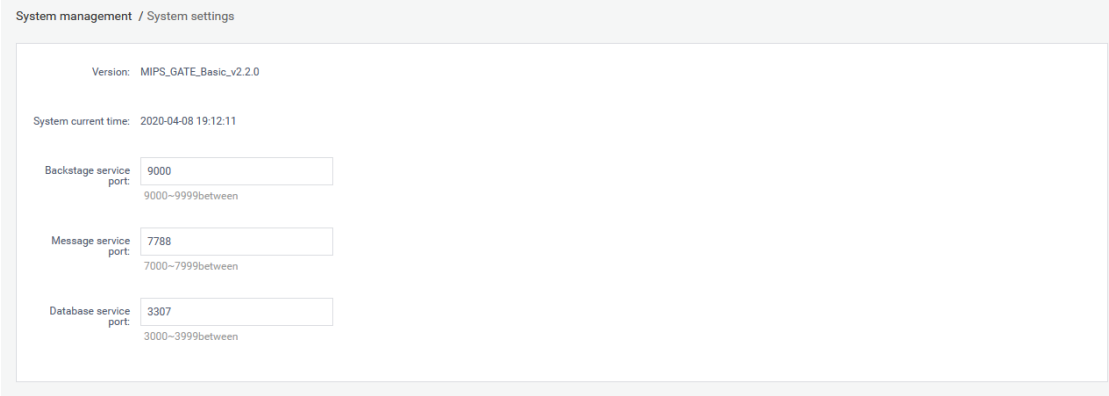


6.5 System setting

The system settings provide several functions such as "background server port", "message service port" and "database service port configuration".

1) Support web service port configurable: background service port can be configured (between 9000-9999), the default is 9000; message service port can be configured (between 7000-7999), the default is 7788; database service port can be configured (Between 3000-3999), the default value is 3306, after setting, you need to restart the background to take effect.

2) 后台支持系统当前时间显示;



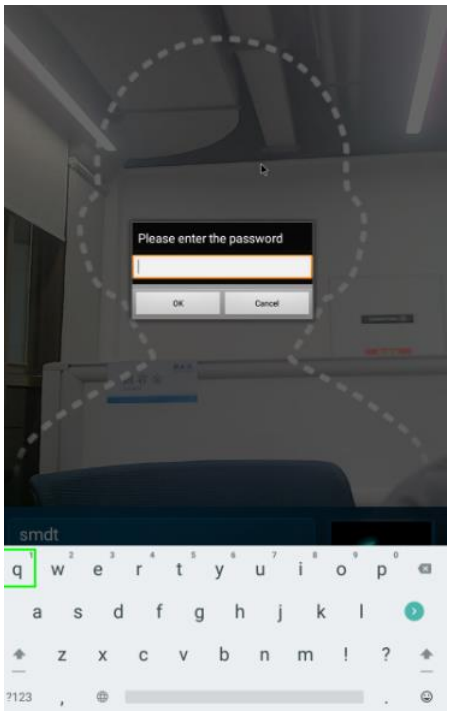
7.Chapter Seven Client Functions

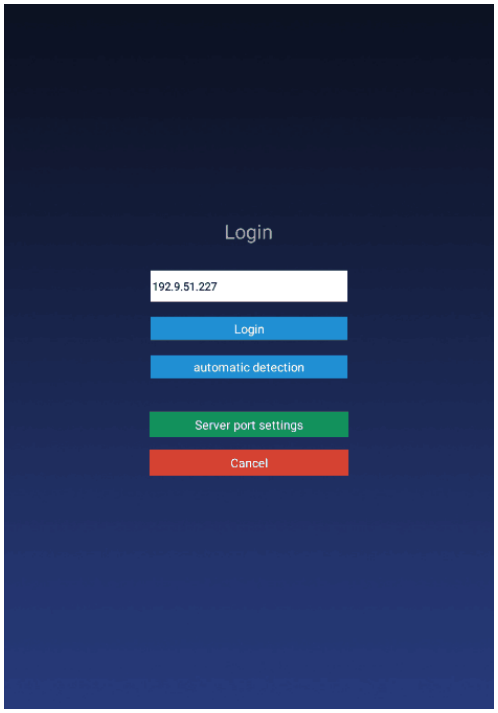
7.1 Client login

- **Steps:**

1) After opening the application on the device, click the middle mouse button to pop up the password input box and enter the default password: 123456 to enter the settings page.

2) Click Login Management to enter the login interface. Enter the same account password as the web page to log in.





Note: You need to enter the set device password before entering the login management, after logging into the application settings and before exiting the application. The password can be set in the "Parameter setting" in the [Device management] on the backstage web page, or can be modified in the "App Password Settings" in the terminal application settings.

- **Application management**

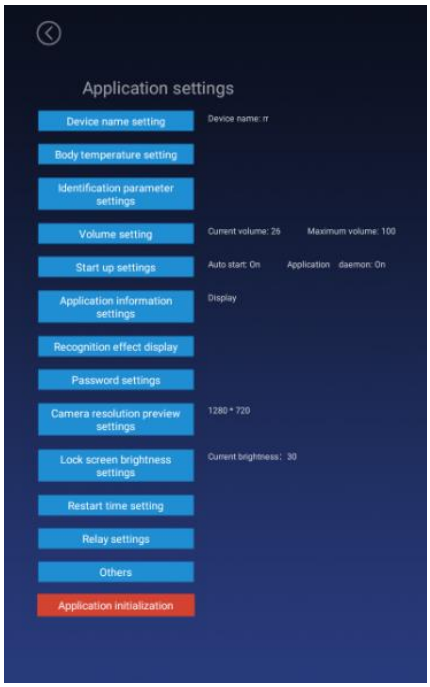
After successful login, click the middle mouse button to open the [Application management] interface. The current page displays the login information: local name, local IP, connected server, current login status, and login management, application settings, face entry, application Six functions of information, pass record and face database.

- **Login management**

After logging in, you can click "Sing out" to log out of the current account.

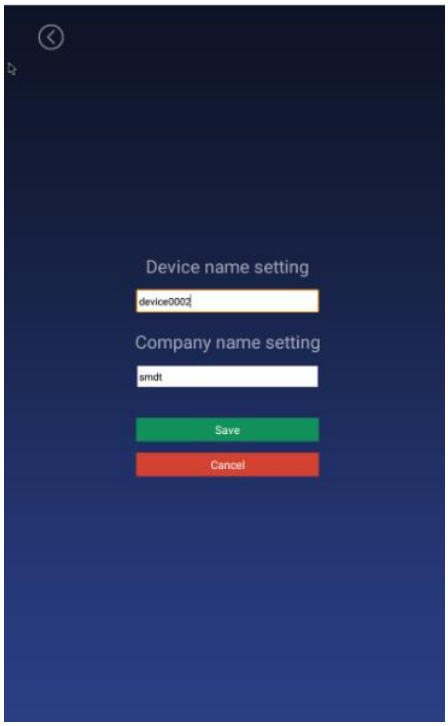
7.2 Application settings

Enter the [Application settings] page, which contains the following function settings:



7.2.1 Device name setting

By default, the device name is the MAC address of the device, which can be modified manually. After being logged in, it will be synchronized to the background after modification, and can also be set in the "device details" in the [device management] of the background web page;



7.2.2 Body temperature setting

- **Body temperature detection switch**

1）Control body temperature detection function. You can choose to turn on or off, the default is on.

2）On: During the identification of personnel traffic, the interface will display and broadcast the body temperature value after the face is recognized.

3）Off: During the recognition of personnel traffic, the outline of the face in the interface is automatically hidden. The interface will not detect body temperature after the face is recognized.

- **Compensation temperature**

1）When the ambient temperature may affect the detected body temperature, the compensation temperature can be set to adjust automatically.

2）The compensation temperature value defaults to 0.3, and the setting range is 0 ~ 1, and a maximum of one decimal can be reserved; "compensation +" is selected by default.

Example: Compensation +0.3 degrees, the problem is 36.1 during identification, then 36.4 is displayed.

- **Alarm threshold**

Set an alarm threshold to control body temperature detection. When the body temperature alarm is turned on, the identified body temperature exceeds the threshold and an alarm is issued. The default is 37.3, and only numbers between 30.0 and 45.0 can be entered, and up to one decimal can be reserved.

- **Body temperature alarm**

1）Control body temperature alarm function. You can choose on or off, the default is on.

2）On: When the detected body temperature is higher than the threshold, the interface displays the body temperature and emits an alarm sound; if the body temperature is lower than the threshold, there will be no alarm.

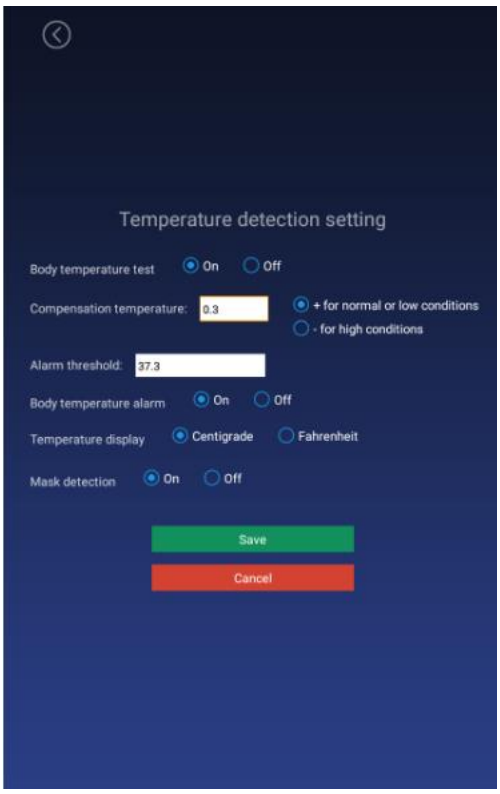
3）Off: No matter the body temperature is high or low, there will be no alarm.

- **Mask detection**

1）Control the mask detection function. You can choose to turn on or off this function, the default is off.

2) On: Recognize without wearing a mask. After recognition, the display style is a red background. Access is prohibited. Please wear a mask. The voice broadcast "Please wear a mask"; wearing a mask can be recognized normally.

3) Off: Does not detect whether to wear a mask during recognition.



7.2.3 Identification parameter setting

- **Test threshold**

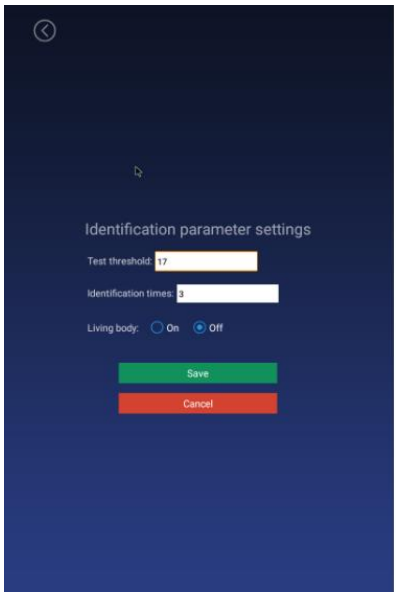
It is used when checking the pictures into the warehouse. The higher the threshold is set, the lower the requirements on the pictures. It needs to be set reasonably. The default value is 17.

- **Number of recognition**

The number of times to identify whether a person is an already-entered person, the default value is 3.

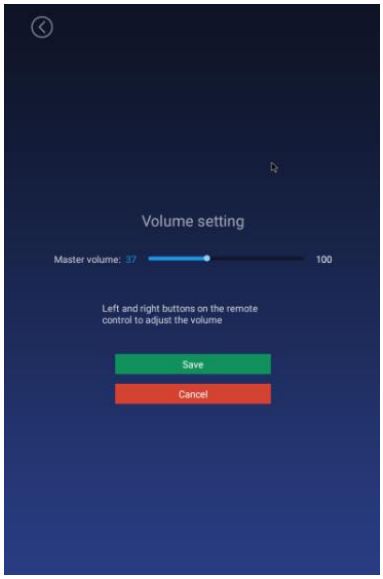
- **Living portrait detection**

Whether to enable live detection when recognizing personnel can be set to on or off, and the default value is off.



7.2.4 Volume setting

While logged in, the volume setting of the synchronization server can also be set locally.



7.2.5 Start-up settings

- **Auto-star**

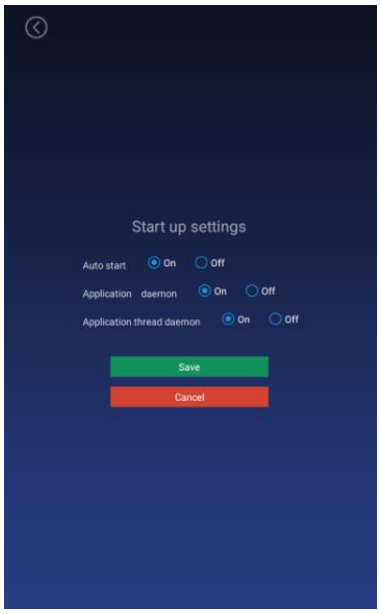
The application will start automatically when it is turned on, and it will not start when it is turned off.

- **Application daemon**

The application will automatically jump back to the playback interface within 30 seconds after opening the application page when opening, and not automatically when closing.

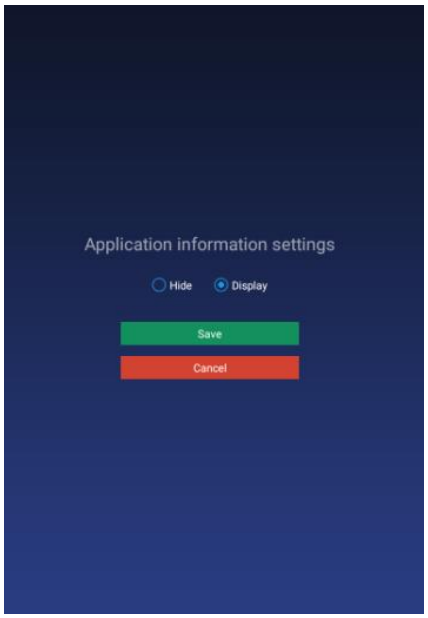
- **Application thread guard**

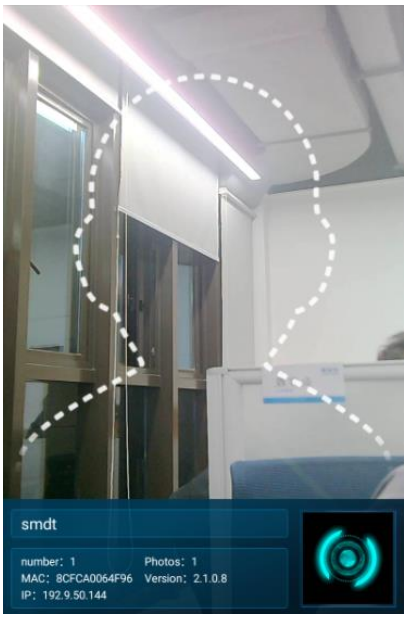
When the camera is turned on, an abnormality occurs and the camera restarts.



7.2.6 Application information settings

After setting, the camera displays or hides the bottom information bar in full-screen display; default: display, which can be set to show or hide.

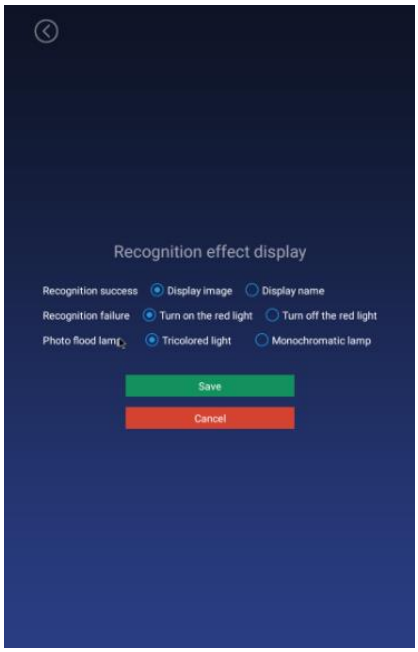




7.2.7 Recognition effect display

Set the effect of face recognition, including the display when the recognition is successful (the default value displays the image) / when the recognition fails (the default value is turned on the

red light), the fill light display (the default value of the three-color light), as shown in the figure:

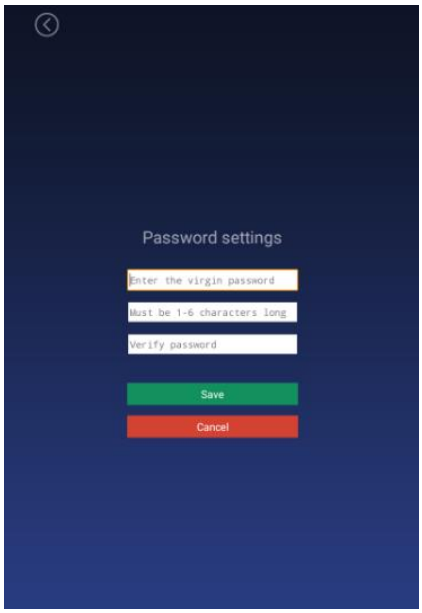


7.2.8 Application password settings

1）Enter the login management, enter the application settings after login, and exit the application before you need to enter the set device password, the initial password: 123456.

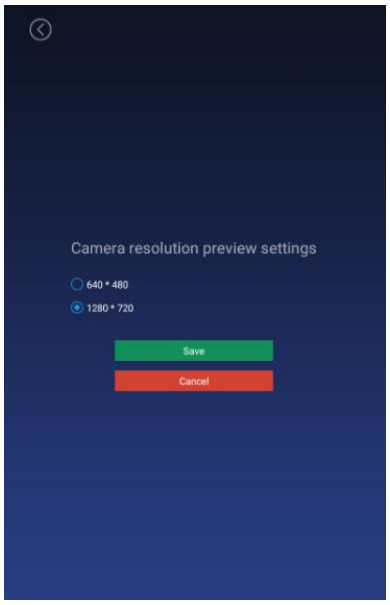
2) The password can also be set in the "Parameter Setting" of [Device Management] on the background web page.

3）Enter the original password, new password, confirm the new password, and save it to modify the password; the password length limit: 1-6 digits, can not be set to blank.



7.2.9 Camera preview resolution setting

Set the camera resolution when performing face recognition. The default value is 1280 * 720.



7.2.10 Screen-saver brightness setting

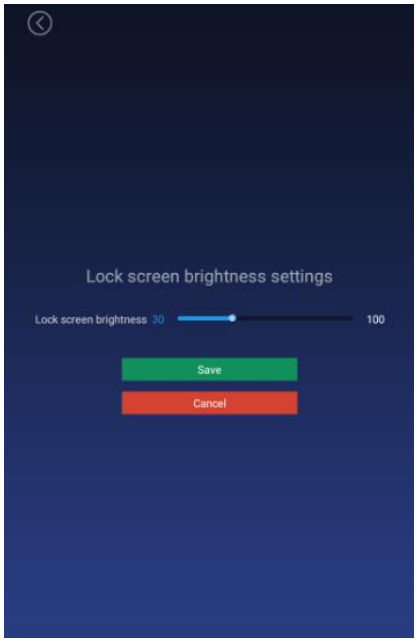
- **Screen-saver**

1）When face recognition is not required, a screen-saver is required. After recognizing a face, jump to the home page.

2）The app starts to display the homepage, there is a face recognition homepage within 30s, and no face recognition screen-saver within 30s.

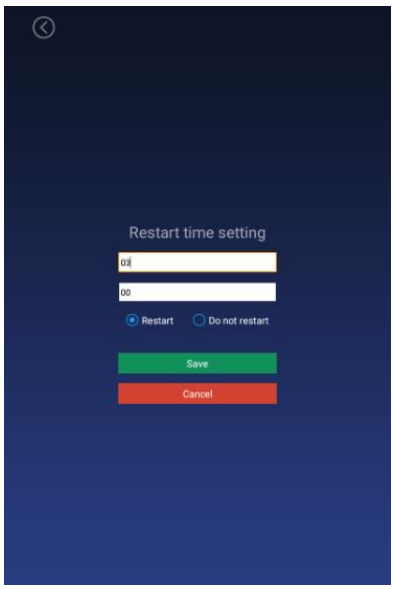
- **Screen-saver brightness setting**

Adjust the brightness value displayed on the screen saver, drag the set value, and save it.



7.2.11 Device restart time setting

Set the device restart time: hour-minute (default value 03:00) and 24-hour system. If you choose to restart, the device will automatically restart at the selected restart time. If you choose not to restart, it will not restart. The default value is to restart.

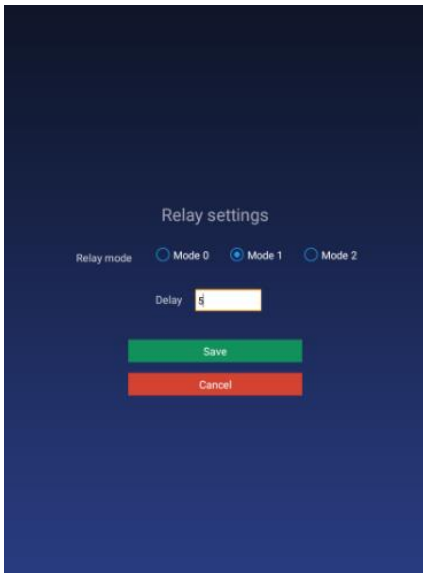


7.2.12 Relay settings

- **Relay mode:**

0: indicates no automatic closing mode, that is, it will not automatically close after opening the relay, the default value.

1: Indicates automatic closing mode (high effective-default low level, then high level for X seconds, and finally low level). That is, after opening the relay, a delay of X seconds will automatically close.
2: Indicates auto-close mode (active low-default low level, then high level for X seconds, and finally low level). That is, after opening the relay, a delay of X seconds will automatically close.
Delay time: The default unit is 5 seconds and the maximum value is 63 seconds.



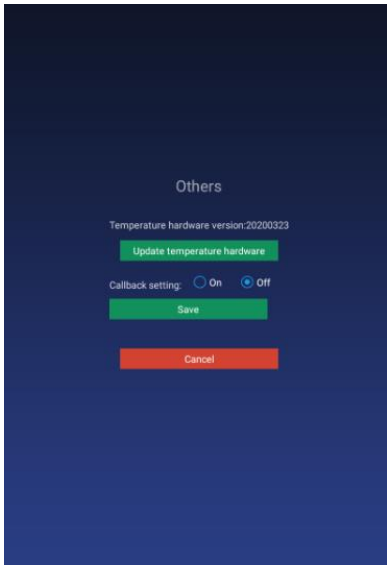
7.2.13 Others

- **Upgrade firmware of temperature module**

The firmware of the temperature measurement module can be manually upgraded through application settings. First insert the U disk, and then enter the temperature measurement module upgrade function of the application settings to select the firmware that can be upgraded for manual upgrade. After the upgrade, you can view the version number of the new firmware of the temperature measurement module. (The firmware file needs to be placed in the root directory of the U disk, and the file name must be updateTemp.bin

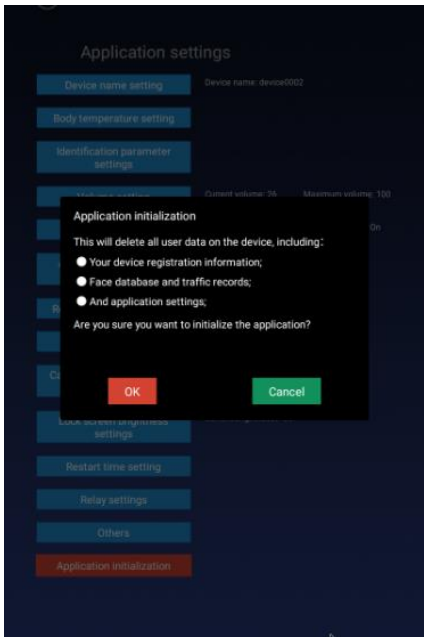
- **Callback settings**

1) This setting includes on and off.
2) On: You need to enter the callback address, the callback address is implemented according to the callback interface document provided by us.
3) Off: The callback function is turned off, the recognition record is not callback.



7.2.14 Application initialization

The application initialization function will clear all data in the application and restore it to its initial state, including user login information, entered face information, access records, and settings in the application settings.



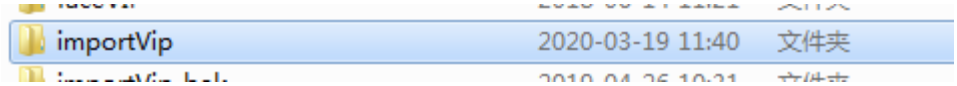
7.3 Face portrait entry

You can enter personnel information locally, collect faces, enter employee ID, name, gender, and save. After the entry is successful, it will be synchronized to the background; after the face is collected, the picture will be verified and the verification result will be displayed.

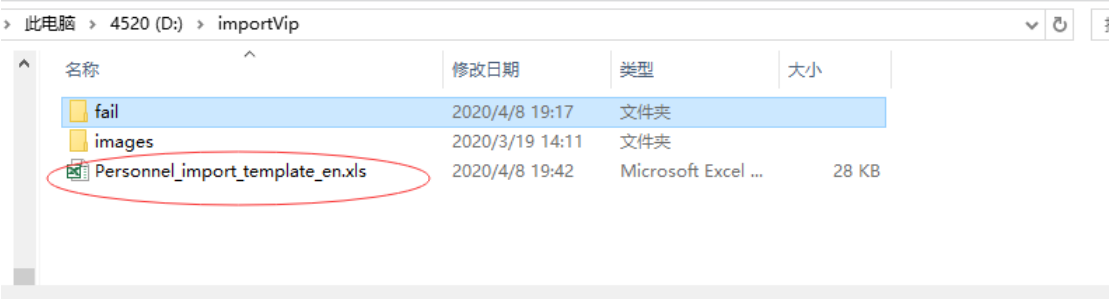
7.4 Personnel import in bulk

In addition to a single entry method, you can also import personnel to the client in batches via a U disk. The import method adopts excel format and folder method. The detailed operation steps are as follows:

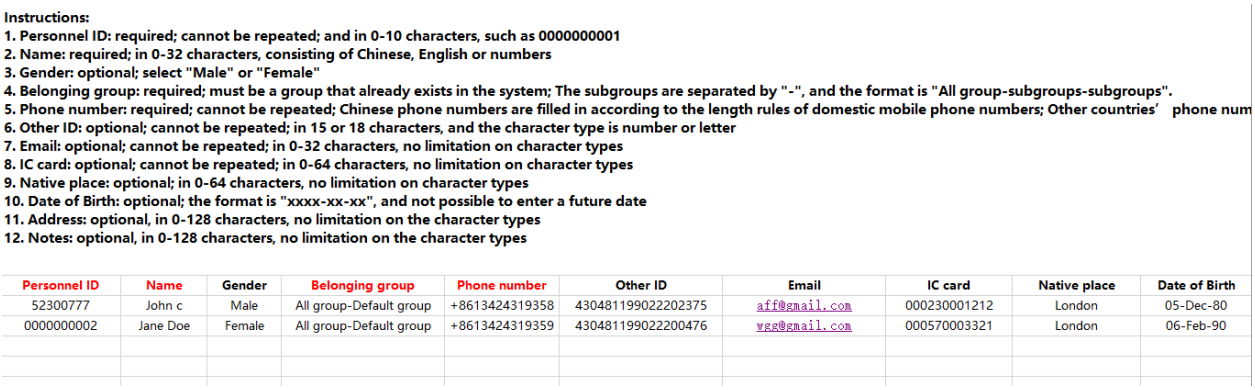
1. Create importVip directory with U disk.



2. Put the excel file in the importVip directory, please refer to the template file for the excel template. Note that excel 2003 is used and can only exist in one excel file.

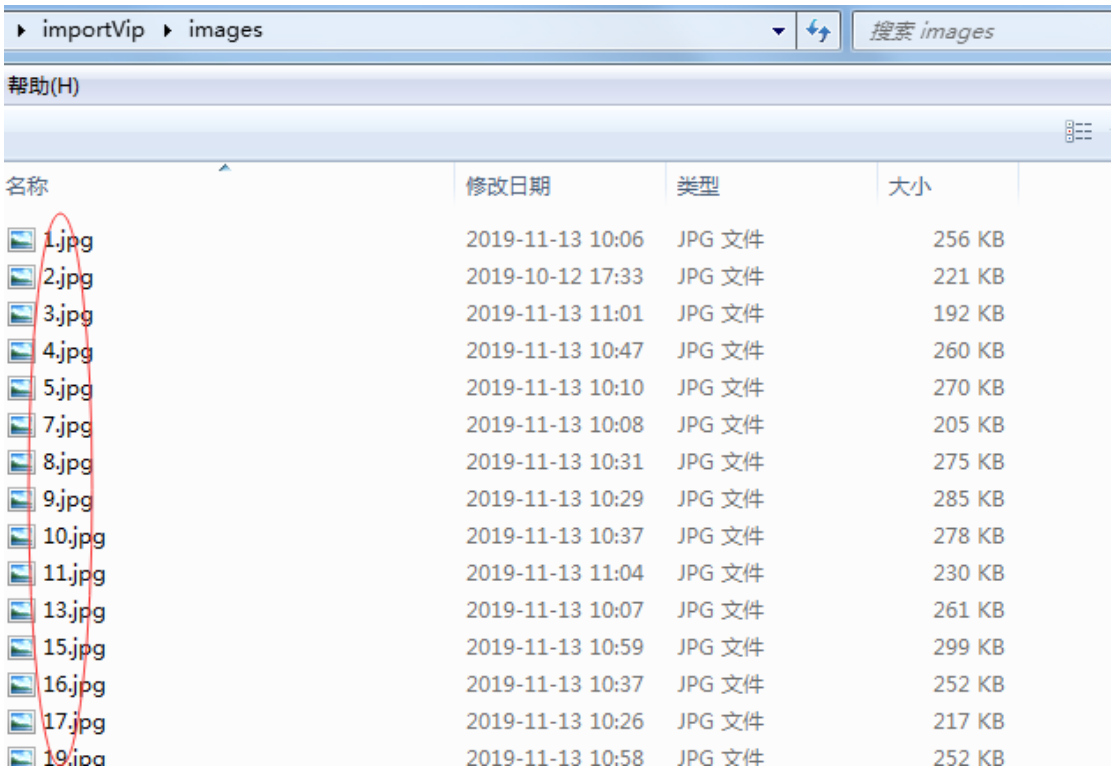


3. Create an images directory to store the face photos of the people to be imported. The photo name is the employee ID of the excel form, and the photo supports png or jpg format.

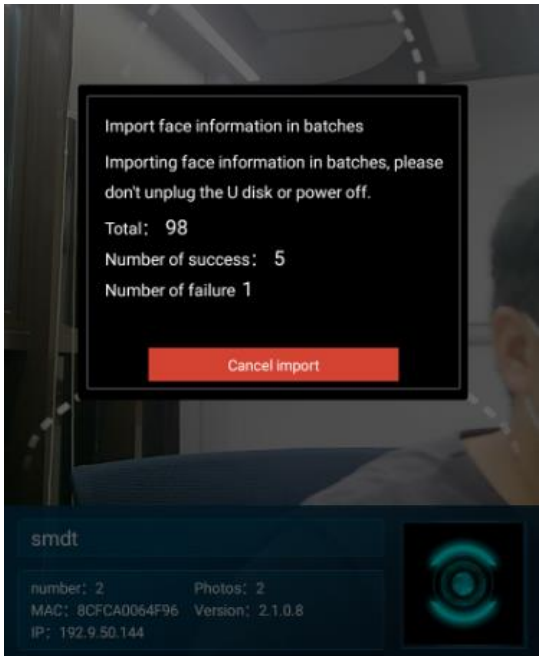


Instructions:
1. Personnel ID: required; cannot be repeated; and in 0-10 characters, such as 0000000001
2. Name: required; in 0-32 characters, consisting of Chinese, English or numbers
3. Gender: optional; select "Male" or "Female"
4. Belonging group: required; must be a group that already exists in the system; The subgroups are separated by "-", and the format is "All group-subgroups-subgroups".
5. Phone number: required; cannot be repeated; Chinese phone numbers are filled in according to the length rules of domestic mobile phone numbers; Other countries' phone num
6. Other ID: optional; cannot be repeated; in 15 or 18 characters, and the character type is number or letter
7. Email: optional; cannot be repeated; in 0-32 characters, no limitation on character types
8. IC card: optional; cannot be repeated; in 0-64 characters, no limitation on character types
9. Native place: optional; in 0-64 characters, no limitation on character types
10. Date of Birth: optional; the format is "xxxx-xx-xx", and not possible to enter a future date
11. Address: optional, in 0-128 characters, no limitation on the character types
12. Notes: optional, in 0-128 characters, no limitation on the character types

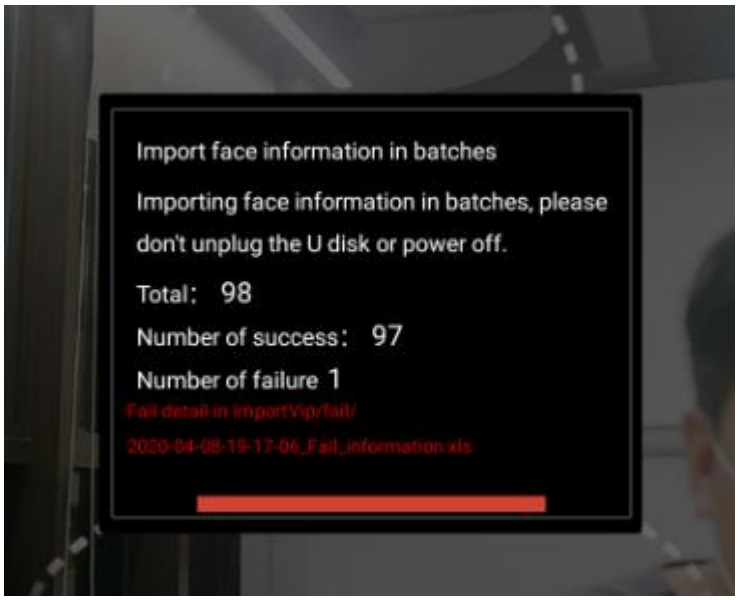
Personnel ID	Name	Gender	Belonging group	Phone number	Other ID	Email	IC card	Native place	Date of Birth
52300777	John c	Male	All group-Default group	+8613424319358	430481199022202375	aff@gmail.com	000230001212	London	05-Dec-80
0000000002	Jane Doe	Female	All group-Default group	+8613424319359	430481199022200476	wgg@gmail.com	000570003321	London	06-Feb-90

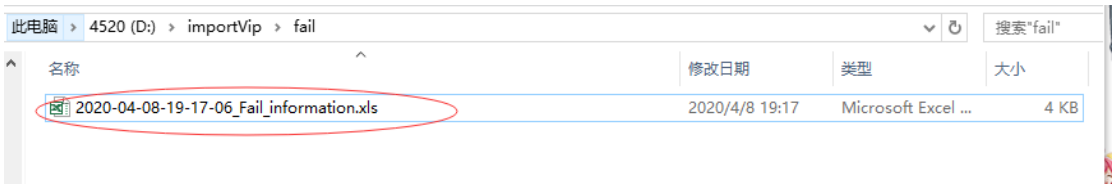


4. Insert the USB port of the device after it is created and import it automatically. The current total number of imported people, successful people and failed people will be displayed.



5. After the import is completed, a fail folder will be created under the importVip directory, and a description of the reason for the import failure will be generated.



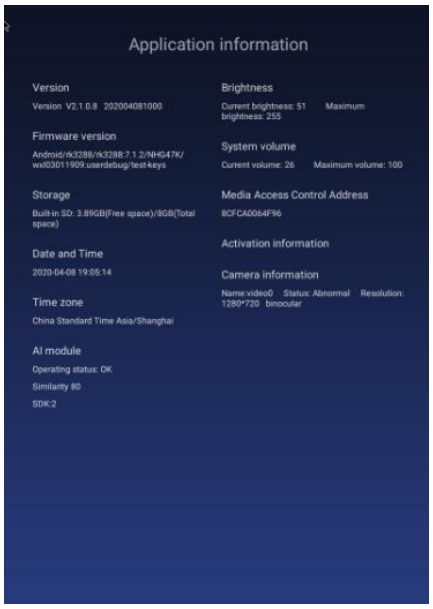


7.5 Pass records

By default, the travel records of the current day are displayed, and the data of the travel records can be queried and exported by day (the data of the current day is displayed by default, and the export record needs to be inserted into a U disk). The name, identity, time of passage, temperature and snapshot of the passage will be displayed.

7.6 Application information

Display application and terminal system related information, as shown below:



7.7 Face database

The face database page can view the face database information of the current device. The list will display the name, identity, expiration date, type and pictures. Records can be deleted, and local personnel can also be uploaded to the background.

7.8 Identify the home page

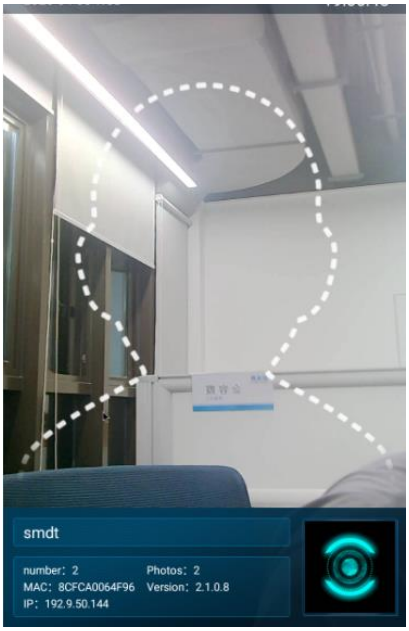
- **Homepage description**

1) The top information bar: The time information bar will automatically synchronize the server time and day of the week.

2) Camera screen: The camera screen is displayed in full screen, and the recognition result is displayed when passing through.

3) The bottom information bar: The company name, number of people, photo, MAC address, IP address and version number will be displayed.

1. Company name: The default is to set the company name, which can be set through the background.
2. Number of people and photo information: The number of people refers to the total number of people in the device, and the number of photos is the number entered in the face database, which changes automatically after synchronizing data.
3. MAC address: It is the mac address information of the current device.
4. Version number: the current version number of the client.
5. IP address: It is the current IP of the client. If there is no address, the display is blank, and the address needs to be displayed dynamically.



- **Pass recognition**

It can be identified based on the person's identity. You can also check the body temperature of the identified person, whether to wear a mask, and display the identification results.

7.9 Others

- **Person & Paper Comparison**

The client accesses the ID card to identify the peripherals, and the device ID is set to "Person & Paper comparison". Swipe the ID card on the peripheral device. When the ID card matches the currently recognized person, the gate will be opened.

- **Client languages**

The English version has been adapted. After exiting the client, the system language is set to English, and the interface automatically changes to the English version after entering the

application.