OneScreen GoSafe

Management Platform

User Manual

Contents

1. Installation and Login

- 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 allow, so that the program operates normally. Otherwise, the installation process may fail and the application may become unusable.

- After the program is installed, the EZ-pass service launches automatically.
- After startup is complete, click "Copy" button. Open Google chrome browser and paste the link to open EZ-pass service background. Enter your username and password to log in.
- EZ-pass system upgrade: You only need to overwrite and install the EZ-pass system software version installation package higher than the current version.
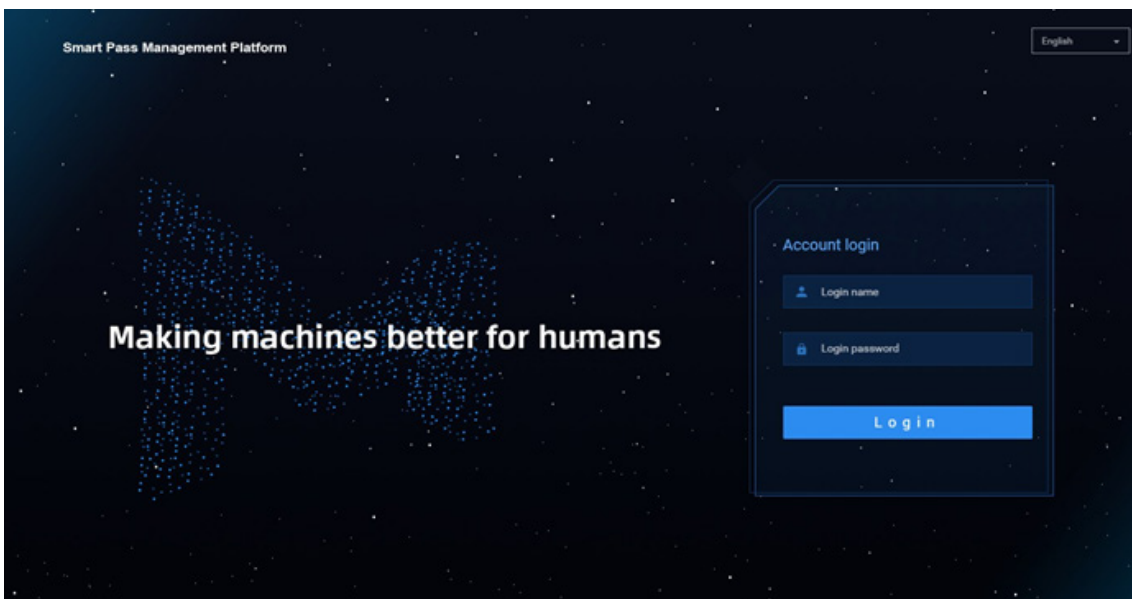
2. Console
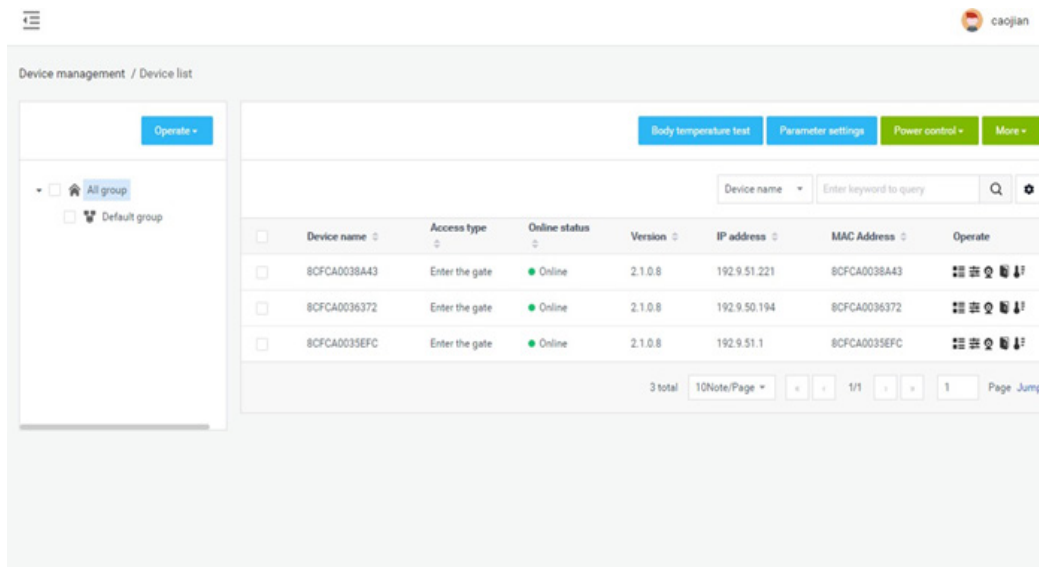
It provides an overview of the number of devices and online status which includes statistics of the face scan (total faces scanned, employee faces scanned, visitor faces scanned, stranger faces scanned), today's pass and real- time monitoring (employees, visitors, blacklists, body temperature), and provides quick access to view details.
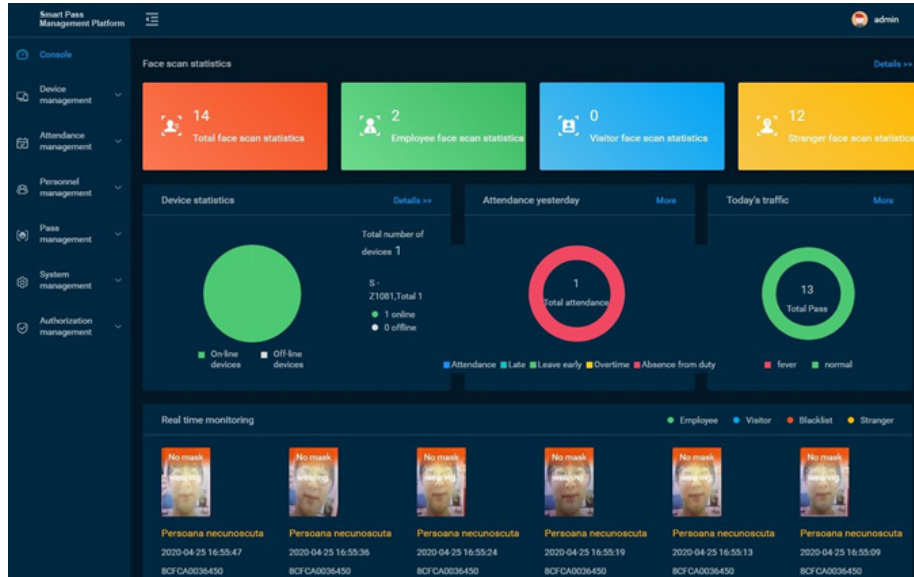
3. Device Management

3.1. Device list

It contains information about all the devices connected to the system. You can perform single, multiple, and grouping management operations on the devices.
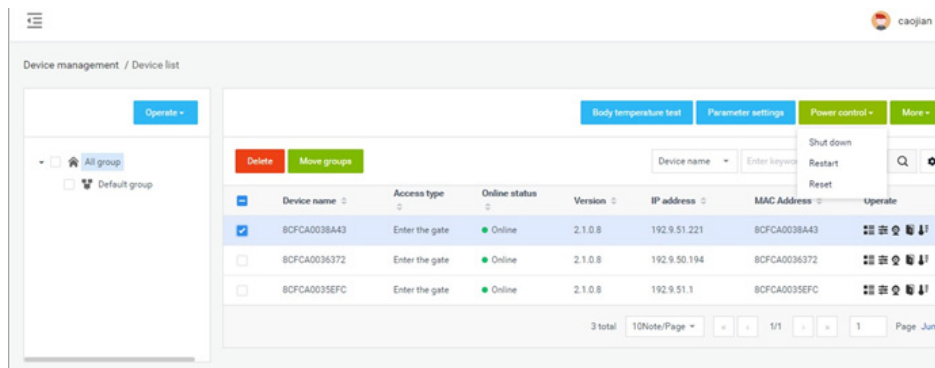
3.1.1. Parameter settings

Select a device from the Device List and click Parameter settings to configure parameter information of that device, as shown in the figure below:

3.1.2. Power control

Select a device from the Device list and click "Shutdown", "Restart", or "Reset" under "Power Control" to remotely shut down, restart, or reset that device.

3.1.3. Body temperature detection

Select a device from the Device list, or select a group of devices and click "Body temperature detection" to set the parameters of temperature detection. By default temperature detection is enabled, alarm threshold is set at 37.3 and is enabled, compensation temperature is at (default + Value 0.3) and mask settings are disabled.
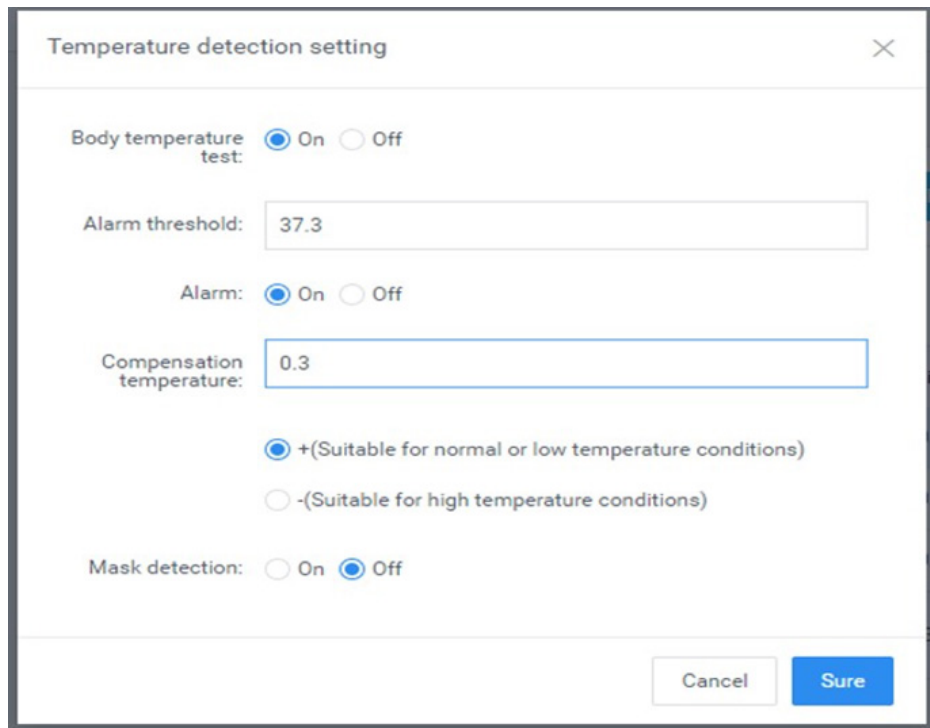
3.1.4. Client upgrade

Select a device from the Device list and click "More-Client upgrade" to enter device software upgrade page. On this page, you can see the list of uploaded device software. Select the software version of the device you want to upgrade to and click upgrade to complete the software upgrade. Both online and offline upgradation are supported.
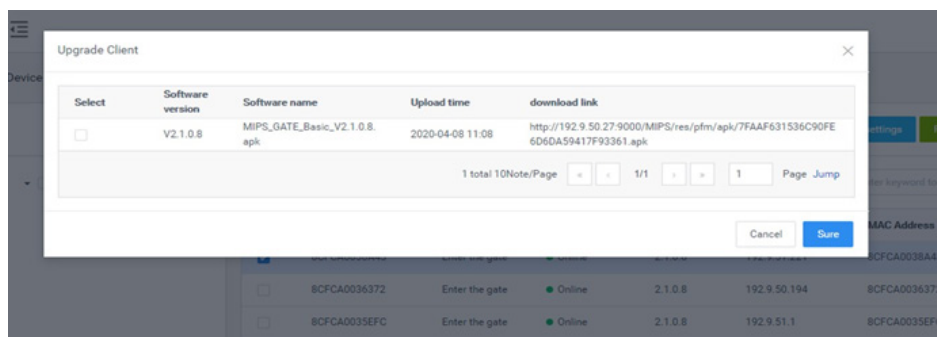
3.1.5. Volume settings

1. General settings: Select a device from the Device List and click "More-Volume setting" to set volume. The volume can be set between 0-100, by default it is at 20.
2. Silent setting: Select a device from the Device list and click "More-Volume setting". Now select "Silent mode" in the pop-up tab.
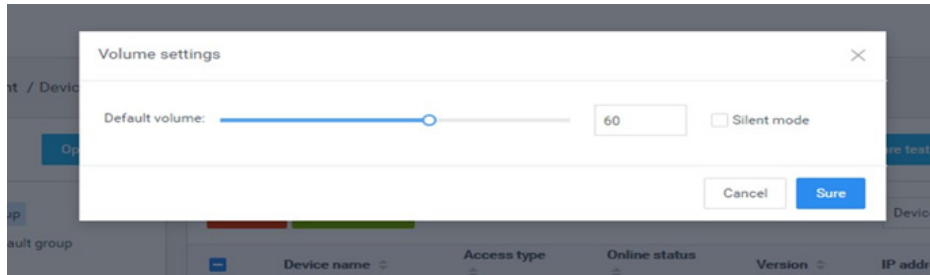
3.1.6. Auto-start

Auto-start: When enabled, the application will be launched on start-up. If you don't want the application to launch on startup, disable the Auto-start feature. In the Device list, select the devices which you want to start automatically, and click "More-Auto-start" option to enable or disable this function.

3.1.7. Application daemon

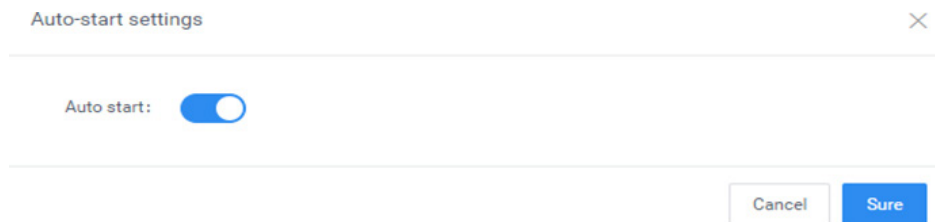Application daemon: When this function is enabled, the application will keep running in the playback interface within 1 minute of exiting the application page. When it is disabled, the application will stop running immediately. In the Device list, select the devices on which you want to enable application daemon, and click "More-Application daemon" option to enable or disable this function.
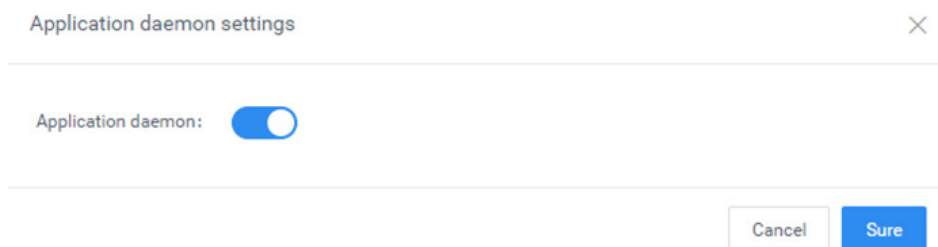
3.1.8. Door control

To open a specific gate controlled by a device, go to Device list and click on "open the door remotely" of the desired device. This will open the gate which is controlled by that particular device.

### 3.1.9. Delete Device

Select the device which you want to delete from the Device list and click "Delete" option to delete it. Only offline devices can be deleted. You can also delete multiple devices.

### 3.1.10. Device groups

From the 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 these devices to, and click confirm. You can move single or multiple devices to a group.
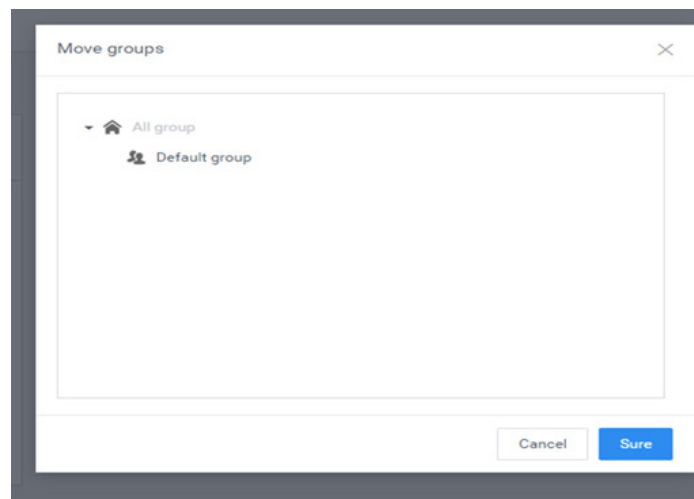
3.1.11. Personalized lists

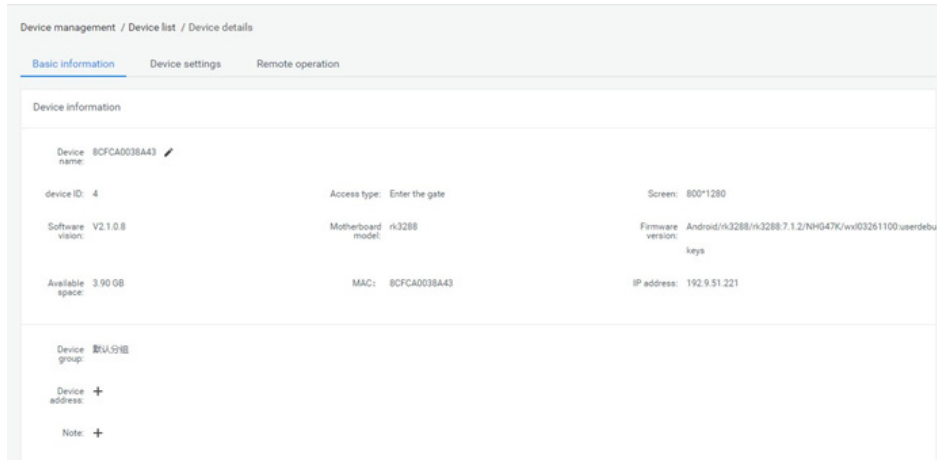The user can personalize his list by including the information that he needs to be displayed.
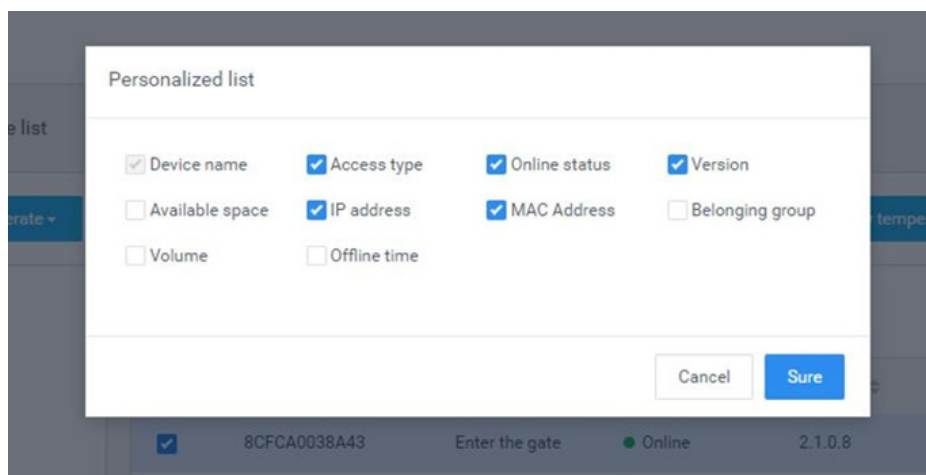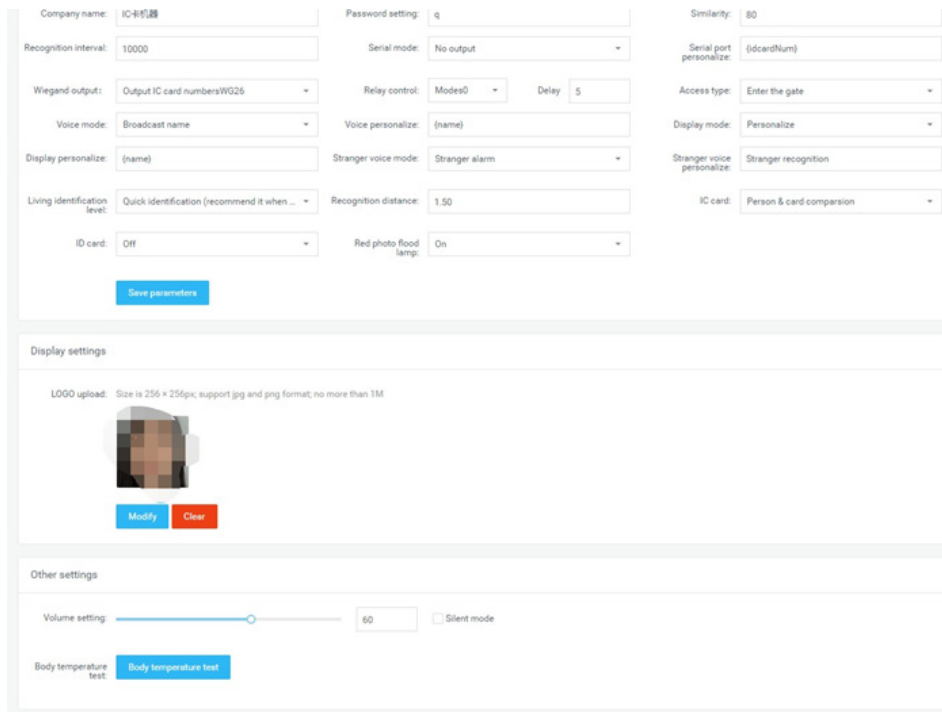
3.1.12.   Device details

The device details include basic information about device settings and remote operations.
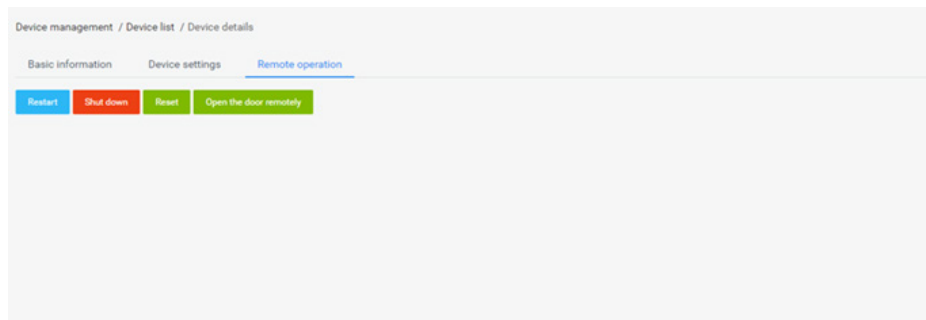
• Basic information: View device information, edit device name, device address, etc.

•

• 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 its online status. You can load and display the current screen of the device. The device can be restarted and shut down from here as well.
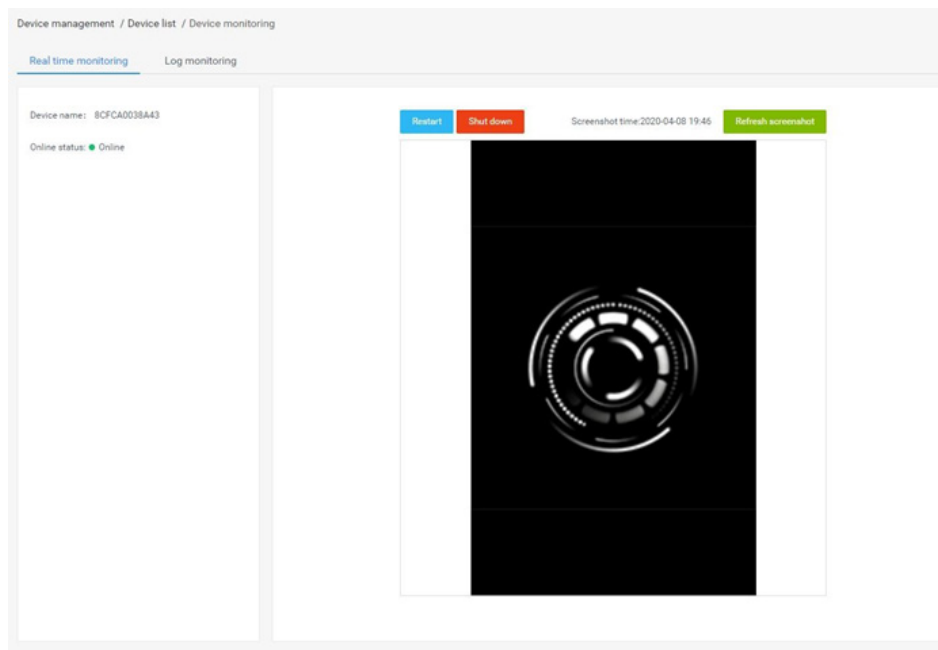
- Log monitoring: View related operation logs of the device.

3.1.14. Bulk operation on Groups

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

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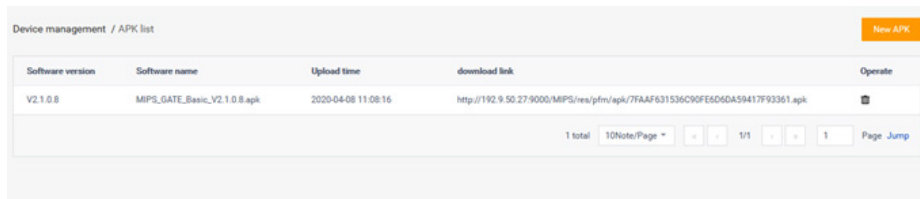
Device grouping uses structured grouping by default. Each user group has a default device group. You can add, modify, and delete device groups on the user group. This operation is similar to the user grouping in Group structure.

3.2. APK list

APK list: This 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.
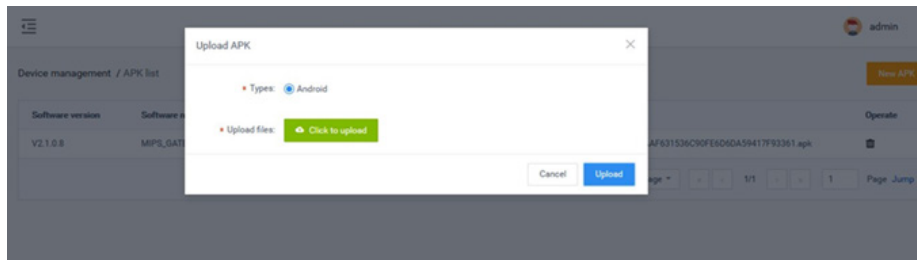
4. Personnel Management

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 to import information in bulk first, and then upload.

4.1.1. Add employee information individually

Steps:

1. In Employee list, click on "Single addition" 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.
3. Add a face recognition photo and click "Save" to complete the employee creation.

Uploading a face recognition photo:

Upload from local disk

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

Note: Portrait photo specifications

1. Please choose a front-and-bareheaded photo from past three months, with clear and evenly distributed light image.
2. The recommended resolution is 640 pixels * 480 pixels, and the size should not exceed 500kb. Only jpg and png files are supported.
3. Faces should account for more than 1/3 of the photo, avoid blurred picture, wearing sunglasses, excessive facial-up, and head rotations.

Capture from device

Click "Capture from Device" to open the Select Device window and select an online device. Now, the device will enter in picture taking mode. After the picture is taken and verified, the photo will be stored in the database using the client device.

4.1.2. Import employee information in bulk

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

1. First step: click "Download Template". Download the excel template file to your computer with the file name "EZ-pass 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. If the file is uploaded successfully, the upload status and file name will be displayed.

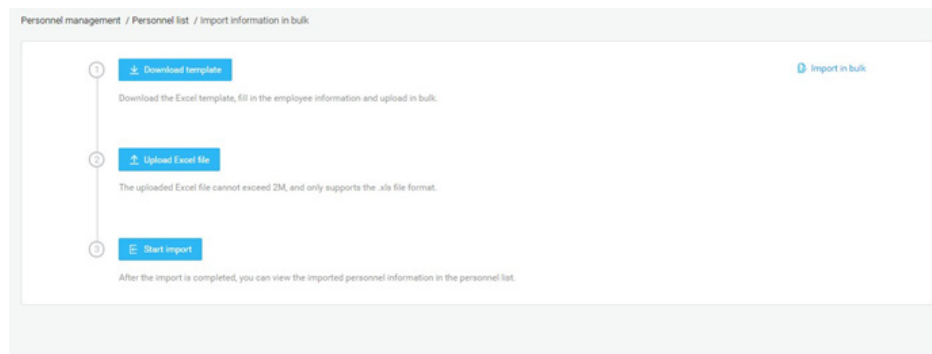3. In the third step, click "Start import". During the import, there will be a progress bar showing "Importing personnel information (1 / total number of people)". After the import is complete, a message "Successful batch import of personnel information" is displayed. Now, return to the Person List to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

Types of import methods:

- Import without overwriting: When you try to import a file two or more times, duplicate employees are not imported, and the system displays "abnormal duplicate information."
- Overwrite import: The second import will overwrite the information of the employee whose information already exists without showing any duplicate information error.

Import Failures:

- The content or format of the uploaded excel file is incorrect and does not meet the template specifications. An error message will appear: "The file content or format is incorrect. Please fill in the employee information according to the template requirements.
- An employee's information field is malformed or 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 "Add in bulk - Portrait import in bulk".

1. Step 1, click "Zip file selection" to open a Folder window and select the file which you want to upload. After a successful upload, the current file storage path is displayed.

2. Step 2, click "Start Import", and a progress bar will be displayed during the import process: the number of imported files / the total number of folders. And there will be a prompt message: x sheets have been successfully imported or, x sheets failed. After completing the import, the progress bar displays: The portrait photos in this folder have been imported.
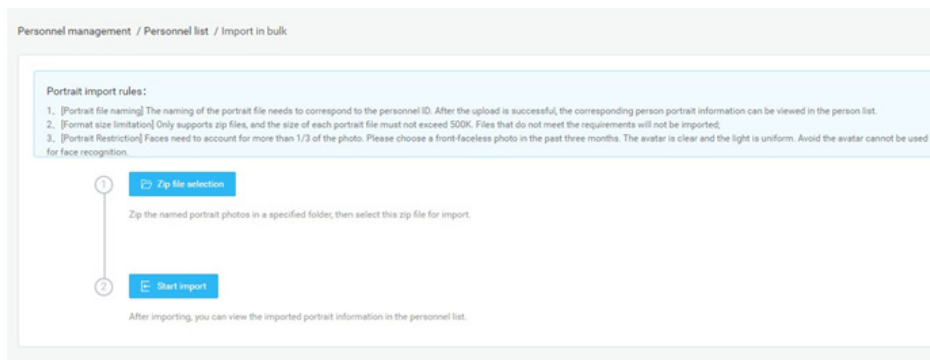
Import Rules:

- [Portrait file naming] The name of the portrait file needs to be same as the personnel ID. After the upload is successful, the information can be viewed in the person list.
- [Format and size] Only two file formats, jpg and png are supported, and the size of each file should not exceed 500k. Files which do not meet these requirements will not be imported.
- [Portrait Restriction] Faces need to account for more than 1/3 of the photo. Please choose a front facing photo from the past three months. The picture should be clear with uniform lighting.
- [Select Folder Upload] After meeting the above conditions, place the named portrait photos in the specified folder and select the folder to import.

Failure of Picture import:

- If the image size is not meeting the requirements then import will fail. A table containing the information about the portrait file that has not been successfully imported will appear. After modification, you can import it again.

4.1.4. Export employee information

In Employee list, click the "Export" option to export all employee information in the list to the file "Employee Information.xls" and download it.
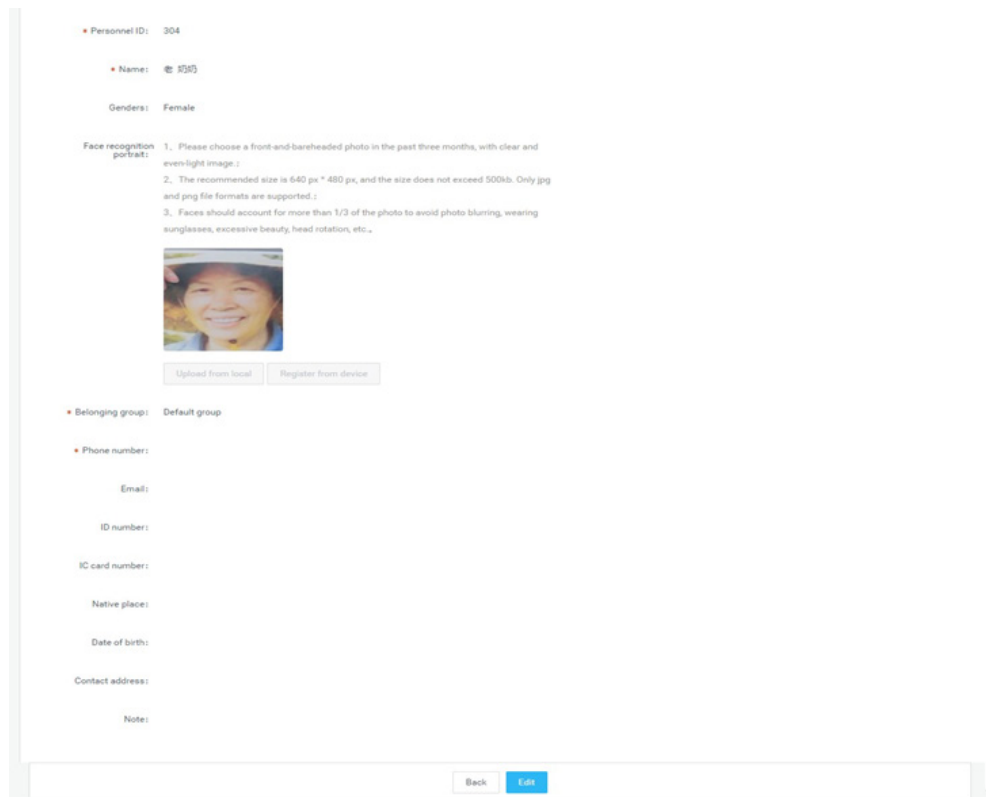
4.1.5. Refresh employee information

In Employee list, click the "Refresh" option to refresh all employee information in the list to their updated state.

4.1.6. Staff details and editing

- **Employee details**

In Employee list, corresponding to the employee information, click on "Employee details" option to view selected employee information.

- **Employee edit**

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

4.1.7. Employee groups management

Employee grouping uses the organizational structured 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. This 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 visitors individually

Steps:

1. In Visitor Management, click on "Single Add" to enter 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, remarks, add face recognition photos and click "Save" to complete the visitor addition.

Uploading a picture for facial recognition:

- **Upload from local**

Click "Upload from local" to open the local folder, select the jpg and png portrait files in the folder. Note: Portrait picture specifications
1. Please choose a front-and-bareheaded picture from past three months, with clear and an even-light image.
2. The recommended resolution is 640 pixels * 480 pixels, and the size should not exceed 500kb. Only jpg and png files are supported.
3. Face should account for more than 1/3 of the picture, avoid blurred picture, wearing sun-glasses, excessive facial-up, and head rotations.

- **Register from device**

Click "Register from Device" to open the Device window and select an online device. Now, the device will enter in picture capturing mode. After the picture is taken and verified, the photo will be stored in the database using the client device.

4.2.2. Export visitors information

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

4.2.3. Refresh visitors information

In Visitor management, click the "Refresh" option to refresh all visitor information in the list to their updated state.

4.2.4. Visitor details and editing

- **Visitor details**

In Visitor management, corresponding to the visitor information, click the "Visitor details" option to view specific visitor's information.

- **Visitor edit**

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

4.2.5. Visitor groups management

Guest grouping uses the organizational structured grouping by default. Each user group has a default guest grouping, which can add, modify, and delete guest groups on the user grouping. This operation is similar to the user grouping in the Group structure.

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 on "Single Add" option 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, birth place, date of birth, contact address and remarks. Add face recognition pictures and click "Save" to complete the blacklist creation.
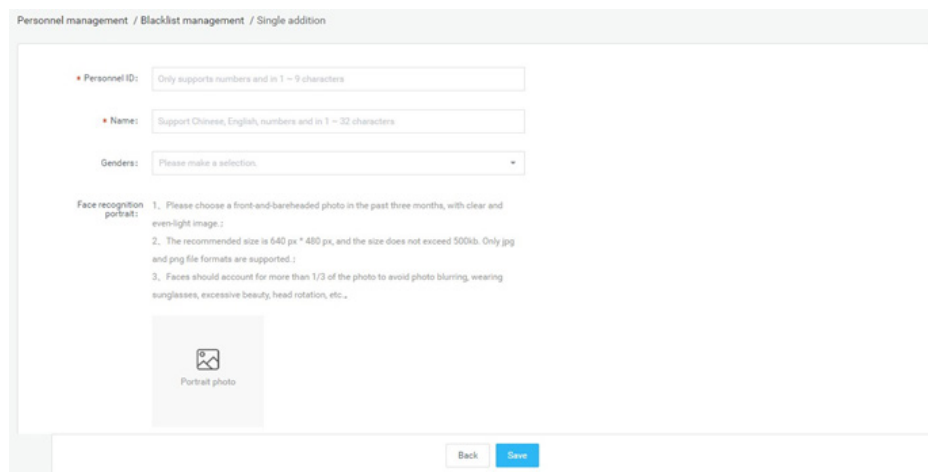
Uploading a picture for facial recognition for blacklist

- **Upload from local device**

Click "Upload from local" to open the local folder, select the jpg and png portrait pictures in the folder.
Note: Portrait pictures specifications
1. Please choose a front-and-bareheaded picture from past three months, with clear and even-light image.
2. The recommended resolution is 640 pixels * 480 pixels, and the size should not exceed 500kb. Only .jpg and .png files are supported.
3. Face should account for more than 1/3 of the photo, avoid blurred pictures, wearing sunglasses, excessive facial-up, and head rotations.

4.3.2. Export blacklist

In Blacklist management, click on "Export" option to export all the blacklist information from the list to the file "Blacklist information.xls" and download it.
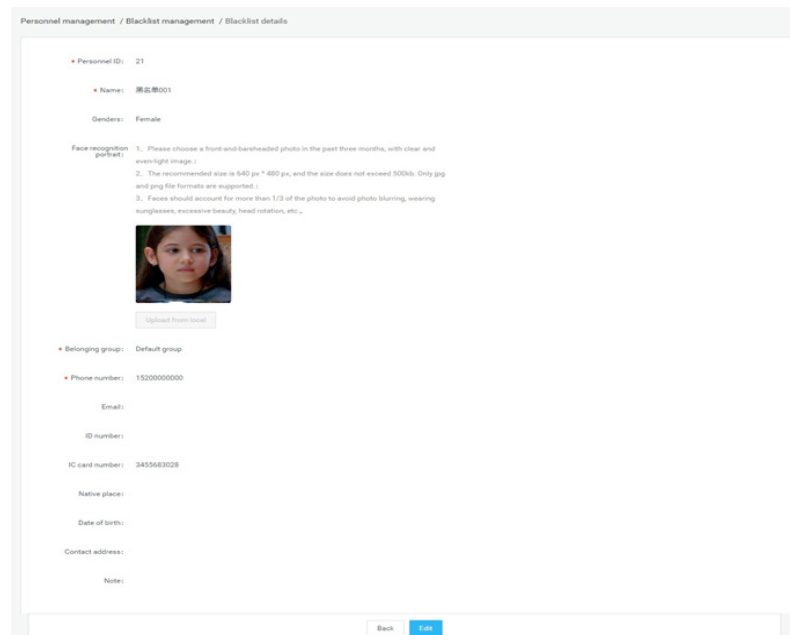
4.3.3. Refresh blacklist information

In Blacklist management, click on "Refresh" option to refresh all the blacklist information in the list to their updated state.

4.3.4. Blacklist details and editing

- **Blacklist details**

In Blacklist management, corresponding to the blacklist information, click on "Blacklist details" option to view the specific blacklist information.
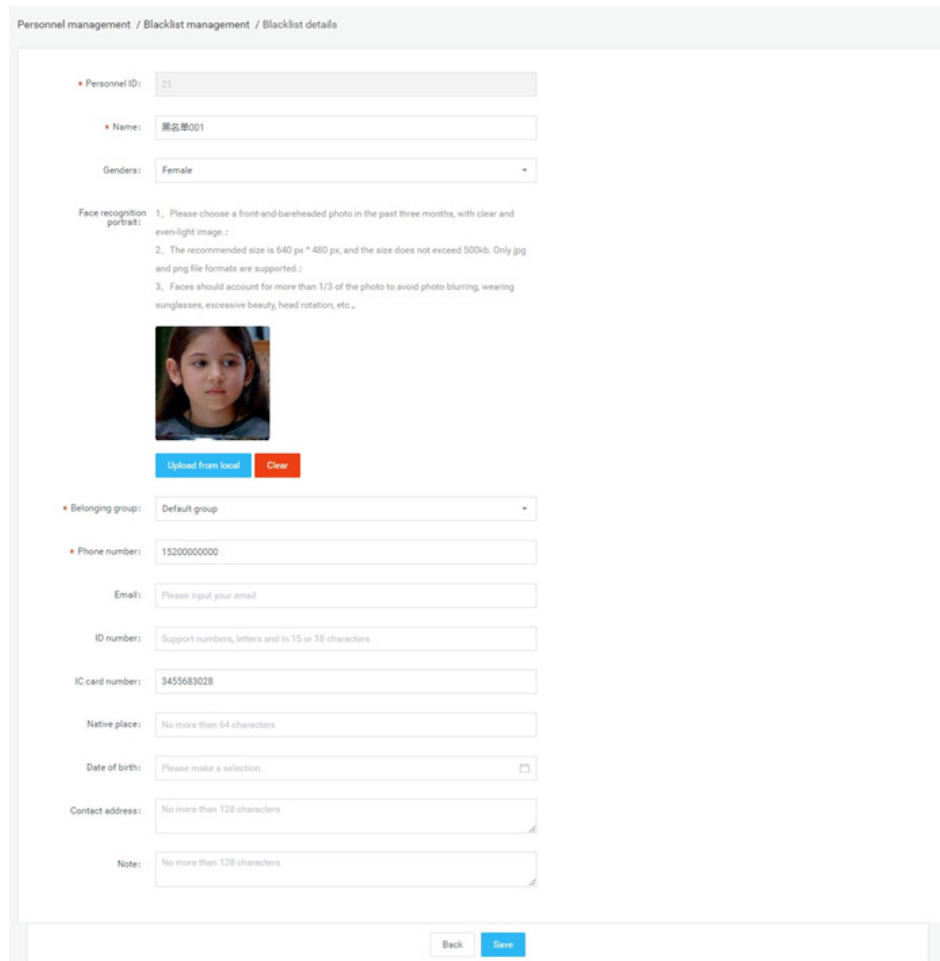
- **Blacklist editing**

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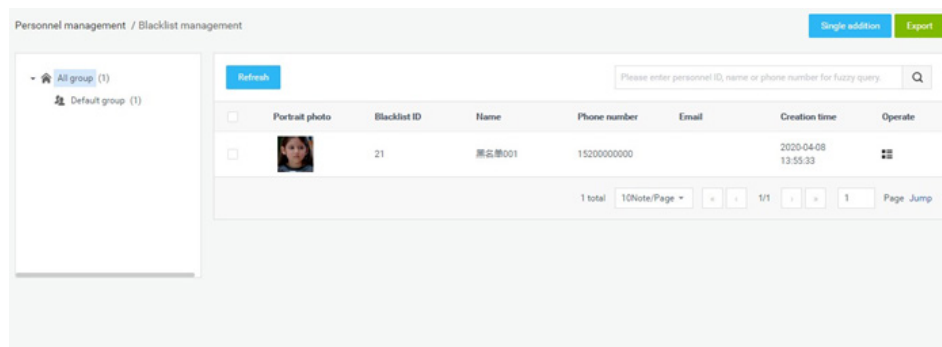

4.3.5. Blacklist groups management

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

5.   Pass Management

5.1. Pass records

View all the identification records on the device, which can be grouped and filtered by device. The data of body temperature greater than or equal to 37.3 degrees will be marked as red, less than 37.3 degrees will be marked green and no temperature data will 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

Manage the access rights of added employees and visitors.

- **Pass permission**
1. Select personnel, devices, pass permission, permanent effective time and click "Save" option to start pass permission. After successful authorization, the person can pass the gate and the validity period is permanent.
2. Select personnel, devices, pass permission, temporary effective time, and click "Save" option to start pass permission. After successful authorization, the person can pass through the gate within the time range set by the validity period. If the validity period is expired, the recognition fails.
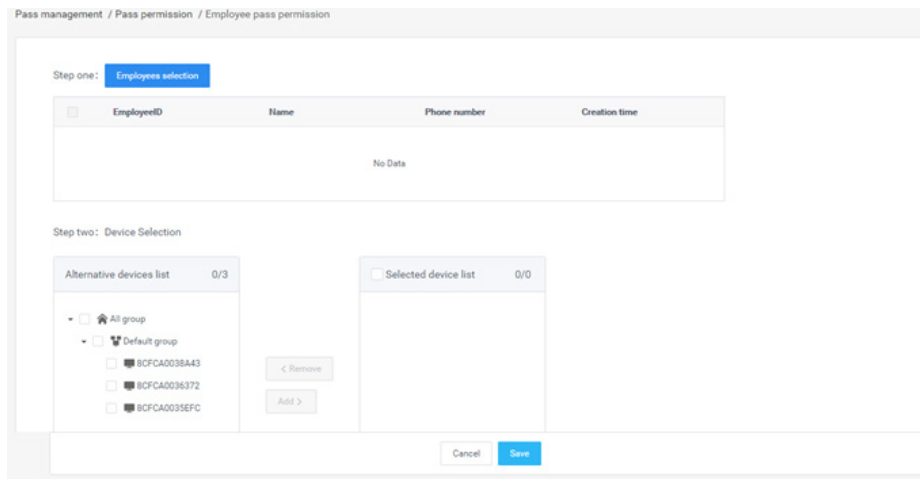
Details of Pass Permission:

- Click Save to start pass permission. This displays the current synchronization status, authorization progress, number of successes and failures of each device in the form of a list along with the device names.
- The person who failed 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 failed authorization after modifying the corresponding failure information can re- authorize until the authorization is successful.

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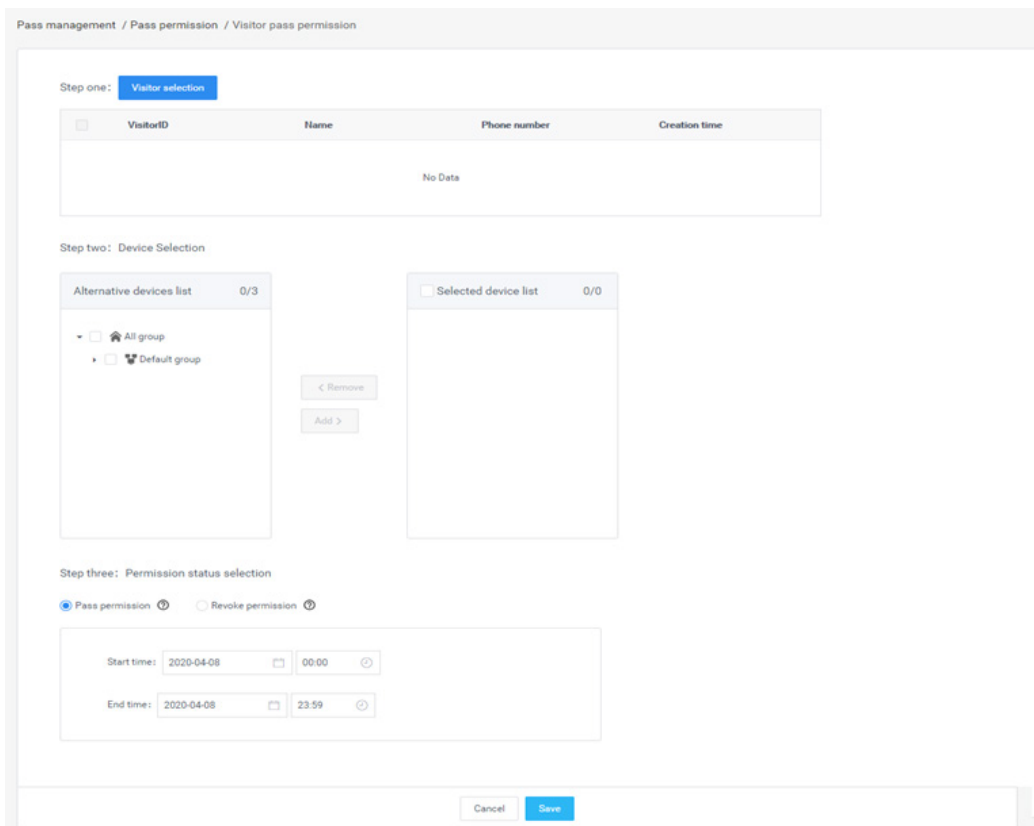
Select a person, select a device, de-authorize, and click "Save" to revoke permission. The de-authorization is the same as the "pass permission" logic, except that the selected person is removed from the selected device.

5.2.2. Visitor pass permission settings

Steps: On the Pass permission page, click on "Visitor pass permission" option.

- **Pass permission**

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

Details of pass permission:

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

Revoke pass permission

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

5.2.3. Revoke permission

In the authorized personnel list, you can click "Revoke permission" behind the list record to release 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.
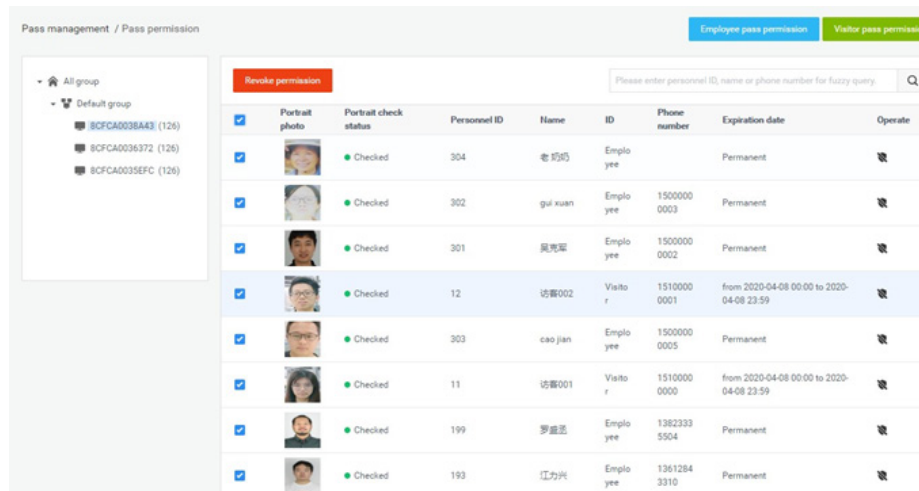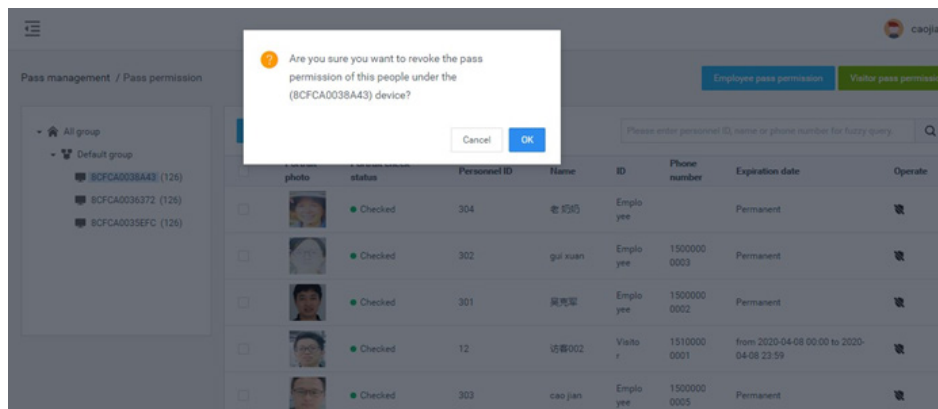
5.2.4. Refresh permission information

On the Pass permission page, click "Refresh" to refresh all authorized information in the list.
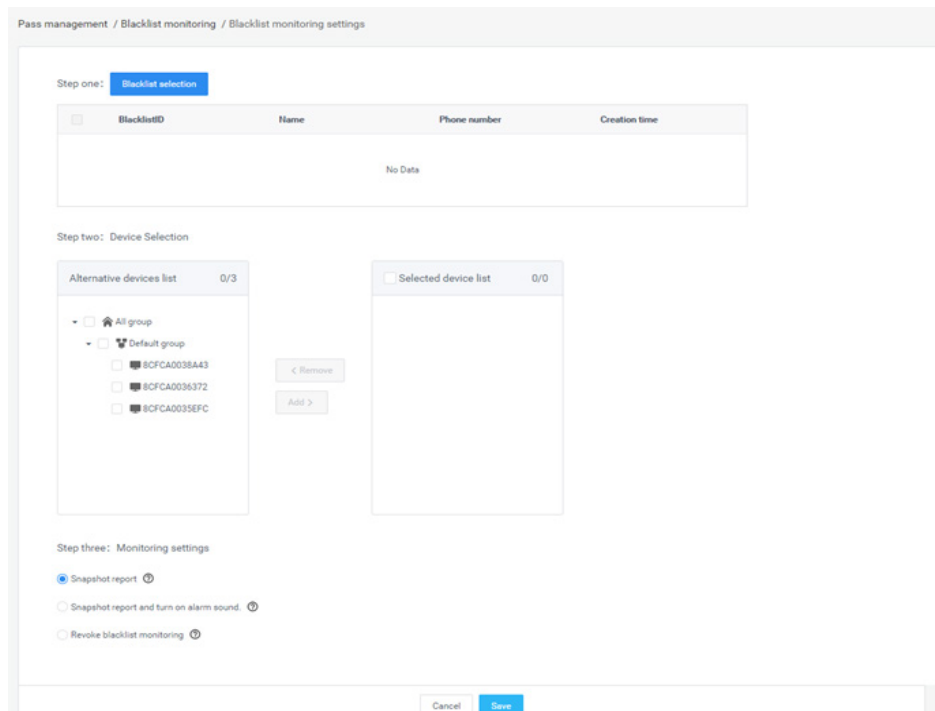
5.3. Blacklist Monitoring

5.3.1. Blacklist monitoring settings

Steps: Enter the Blacklist monitoring page and click "Blacklist monitoring settings"

- **Blacklist monitoring settings**
1. Select the blacklist and the device. Click "Save" to start blacklist monitoring. When the device is in monitoring mode, the blacklisted person will be recognized and reported while passing through the gate.
2. Select the blacklist and device, choose to enable the snapshot report function and enable alarm sound. Click "Save" to start blacklist monitoring. After the device is successfully monitored, the person will be identified through the gate, will be snapped to report and alarm will get triggered.

Details of Pass permission:

- Click Confirm to start blacklist monitoring. Displays current synchronization status of each device in the form of a list, display device name, synchronization monitoring progress, number of successful and failed authorizations. The monitoring failures are recorded in "Export Blacklist Monitoring Failure Information" table. You can click export table to view the monitoring failure information.
- If a failure has occurred during monitoring the blacklisted personnel, the corresponding failure reason can be fixed in the settings and the device can then continue to monitor.

- **Revoke blacklist monitoring**

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

5.3.2. Identification records

Enter the Blacklist monitoring page, click "Identify Record Inquiry" 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, click "remove monitoring" behind the list record to release monitoring. After the removal is successful, the blacklist removes snapshot monitoring or alarm from the selected device. You can also check personnel record and click "remove monitoring" to perform batch operations.
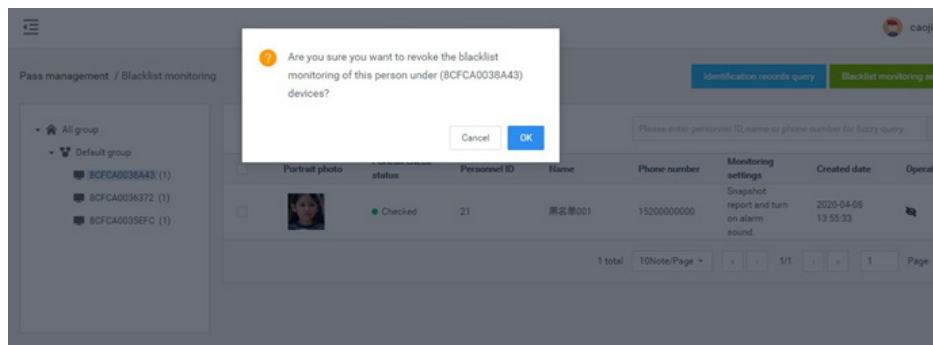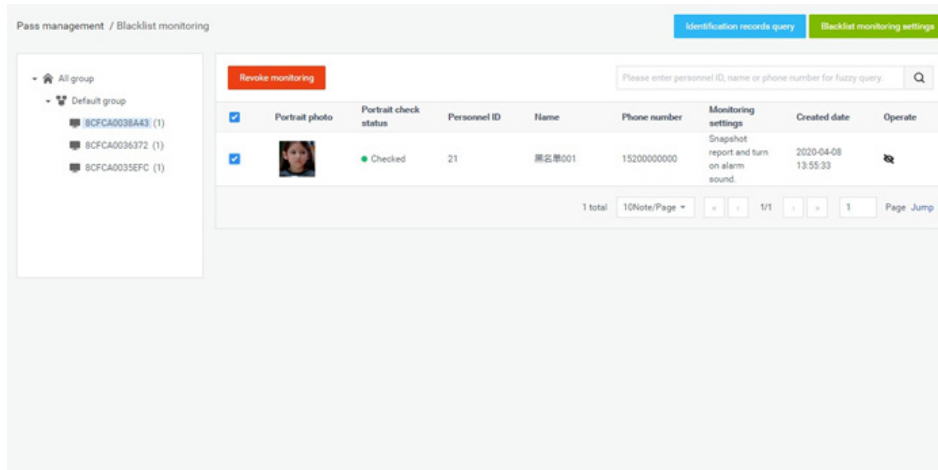
5.4. Permission records

Permission Records: The module contains information records of the "Permission" and "Remove permission" of employees, visitors, as well as the blacklist monitoring and contact monitoring setting operations. You can enter the list to view details of the related records.
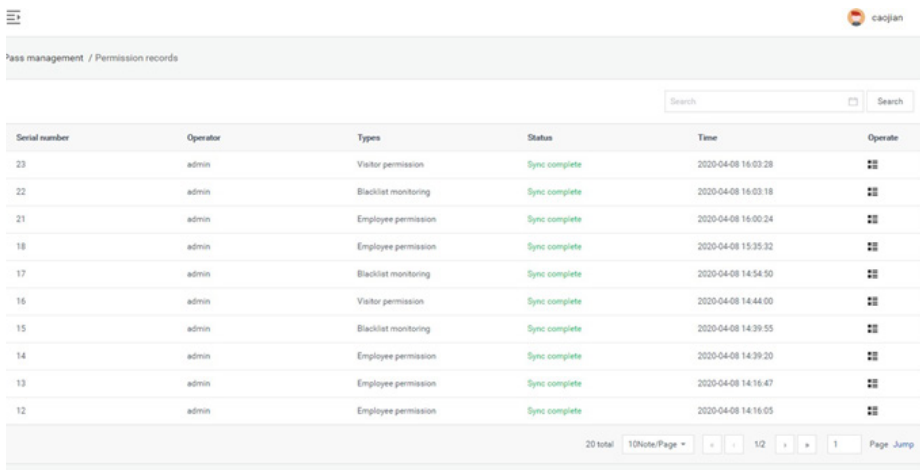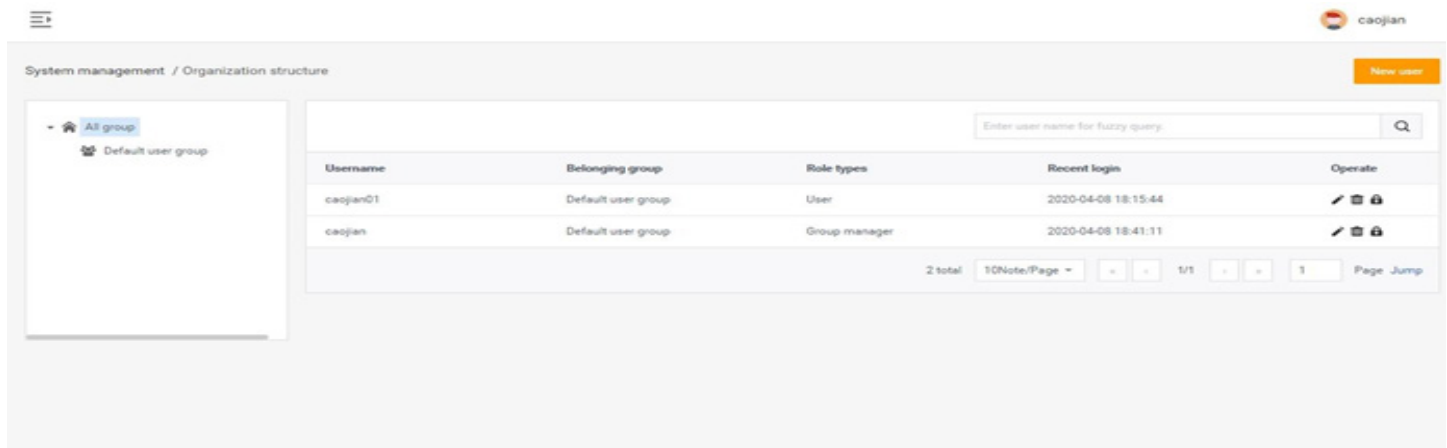
Permission details are as follows
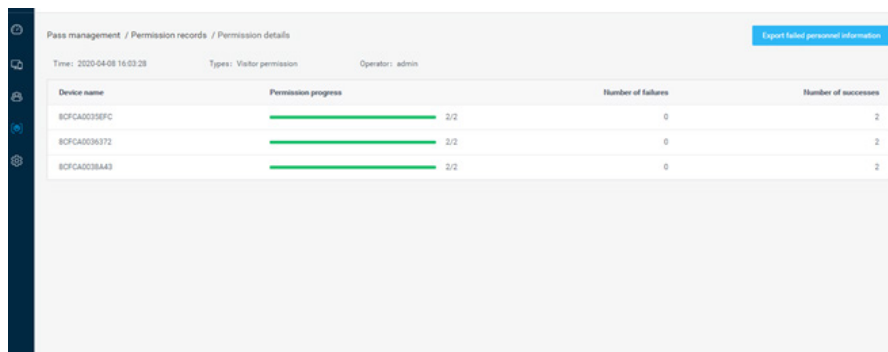
6. System Management

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. Data management in enterprises

- Various business data generated by enterprise users will only be stored under the group in the group structure of 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 the device data in a low-level structure. Conversely, low-level users cannot access high-level device users' 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 data in the organization structure of the enterprise but cannot access data of other enterprises.
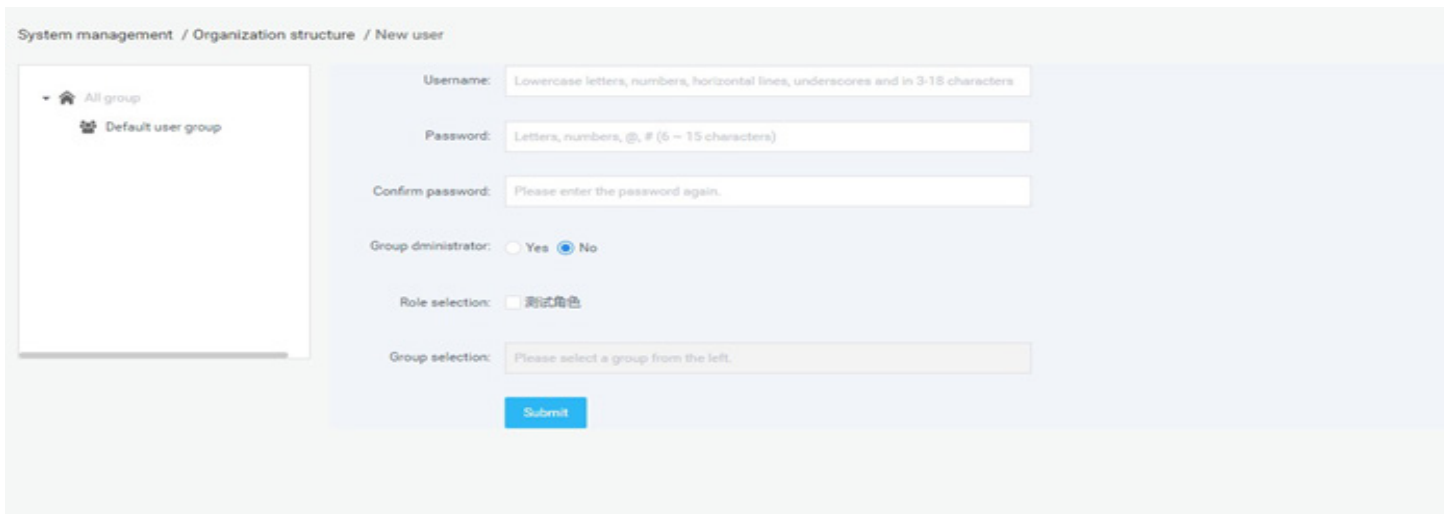
6.1.2. Group management

- Create a group: select a group and click + to enter a 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 Add User page. Select the group, fill in the username 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.
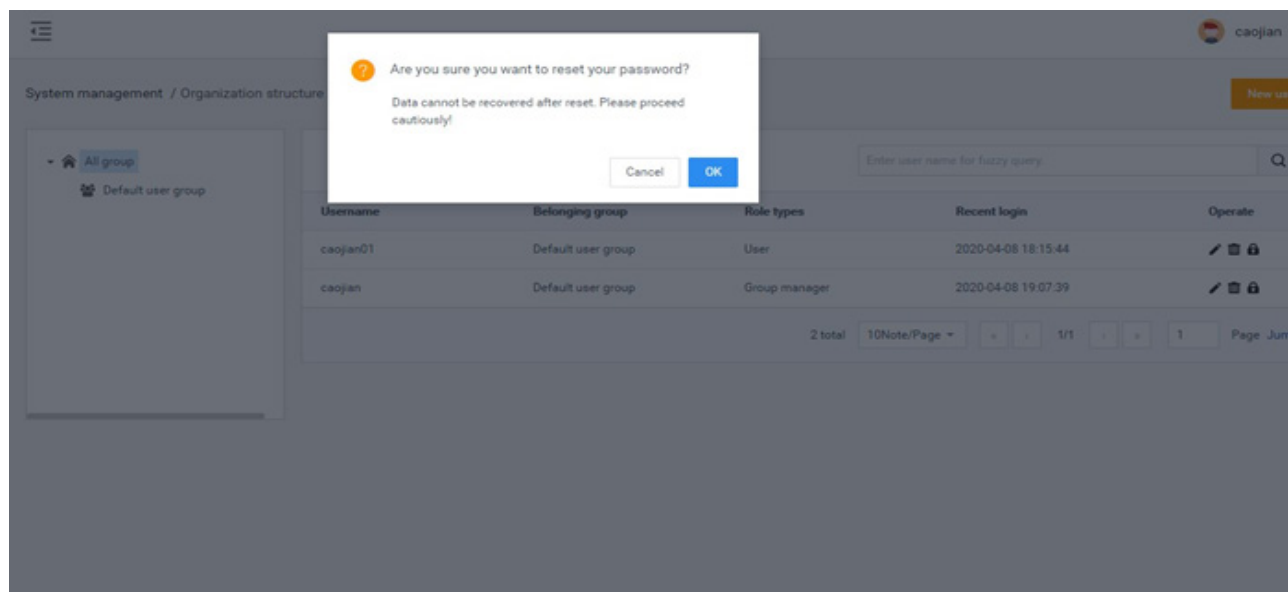
6.2. Role Management
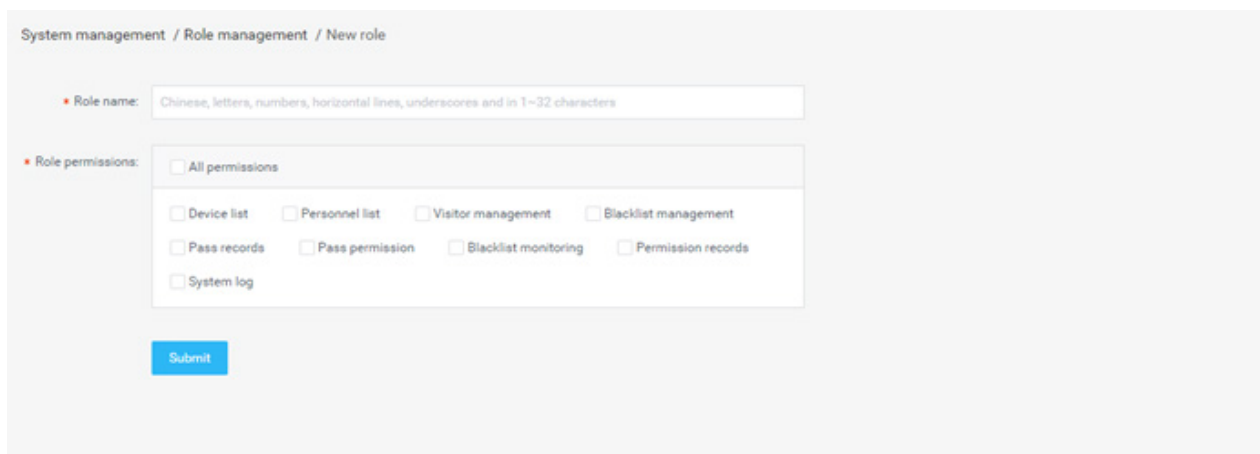
Role management: It is used to create and manage roles. Roles are used to control various business function modules and function operations of users in the system. It is composed of different function operation rights.

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 "Add Role" to enter Add Role page.

6.3. Enterprise Management

Enterprise Management: This 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, manage all business data created by the enterprise users. However, there is no operation authority for the [System Settings] and [Enterprise Management] functions, and you cannot see the data of other enterprise users.

Super administrators can create, modify, query, and delete enterprises. This is 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 Settings

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. The background displays current time.

System management / System settings

Version: MIPS_GATE_Basic_v2.2.0

System current time: 2020-04-08 19:12:11

Backstage service
port: 9000
9000~9999between

Message service
port: 7788
7000~7999between

Database service
port: 3307
3000~3999between

7. Attendance Management

7.1. Attendance Rules

Here you can add, modify and delete attendance rules related to shifts, holidays, public holidays, and device groups.

7.1.1. Shift Settings

Shift settings contain a default shit. Click on new shift to add a new shift. In the popup window, you can modify class parameters related to this new shift. You can add up-to 4 classes in a shit. To delete a class from the shift, click on the delete icon under the operation column.

- **New Shift**

Click on New Shift to open the settings window.

- **Shift Name**

Set a title of a shift.

- **Shift Settings:**
1. By default you have one class in the shift. However, you can add up-to 4 classes in a shift by clicking on the add option.
2. In a class, you can set working hours, after hours, how late can an employee arrive and how early can an employee leave.
3. You can also set the overtime rules by setting how many overtime hours equate to one working day

- **Overtime Rules:**

You can define maximum allowed overtime hours on working days and on holidays.
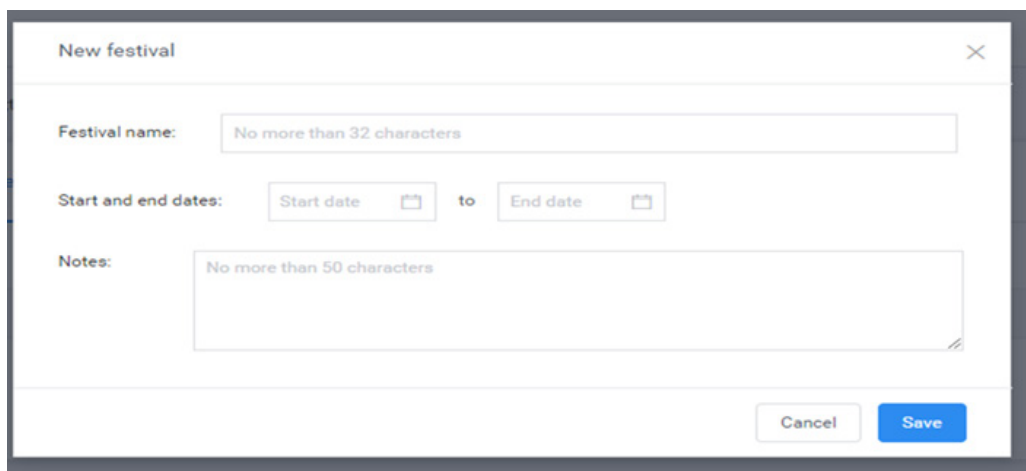
7.1.2. Holiday Settings

List of all the holidays will be displayed here. You can add a new holiday by clicking on New Holiday option.
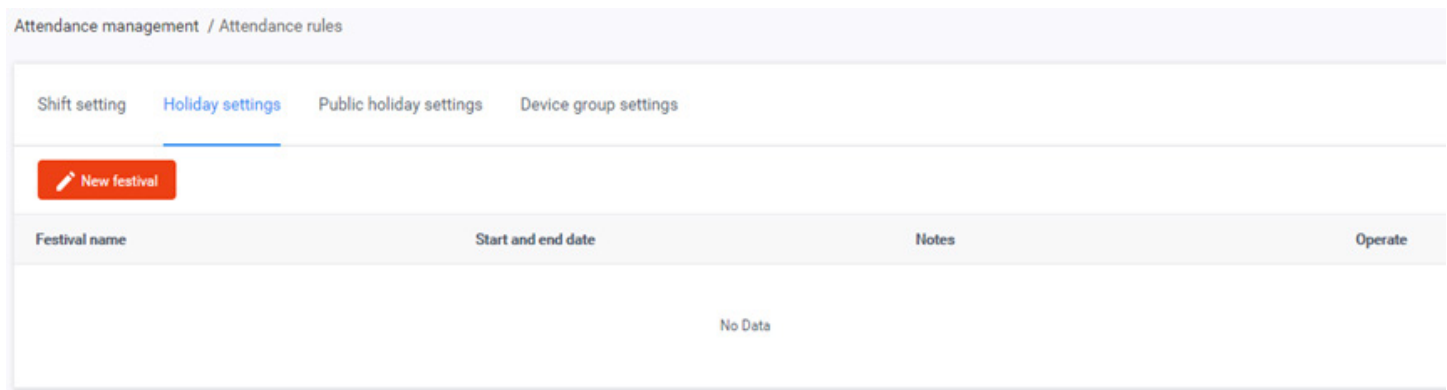
New Holiday:

Click on new holiday to access this settings window.

- **Holiday Name:**

Enter the name of the holiday/festival.

- **Start date & End date:**

Set the start and end date for the holiday.

- **Notes:**

You can write a brief description about the holiday here.

7.1.3 Public Holiday Settings

You can customize the fixed weekly holidays, by default Saturday and Sunday are set as public holidays. To edit this, click on the edit icon under the operations tab and select the days which you want to set as public holidays. You can also delete a set public holiday.
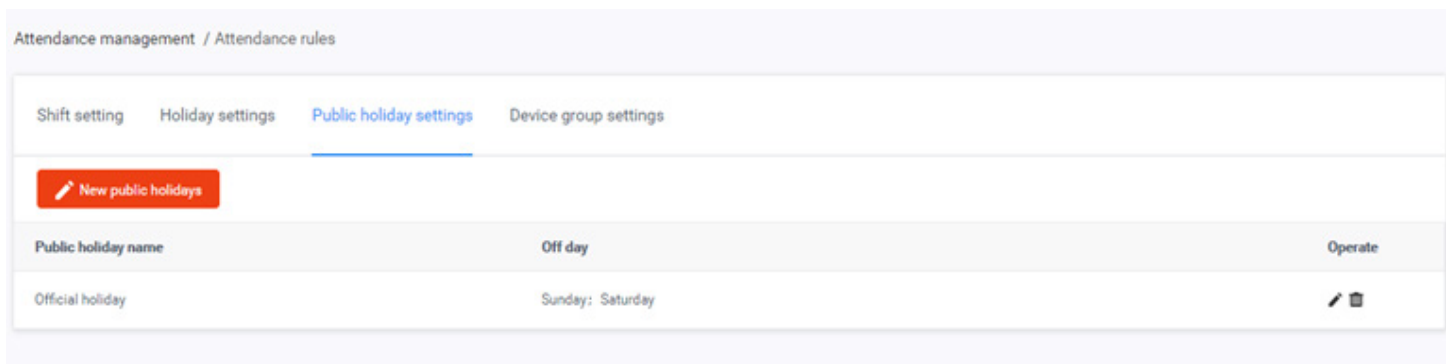
- **New Public Holiday:**

Click on New public holidays to access this settings window.
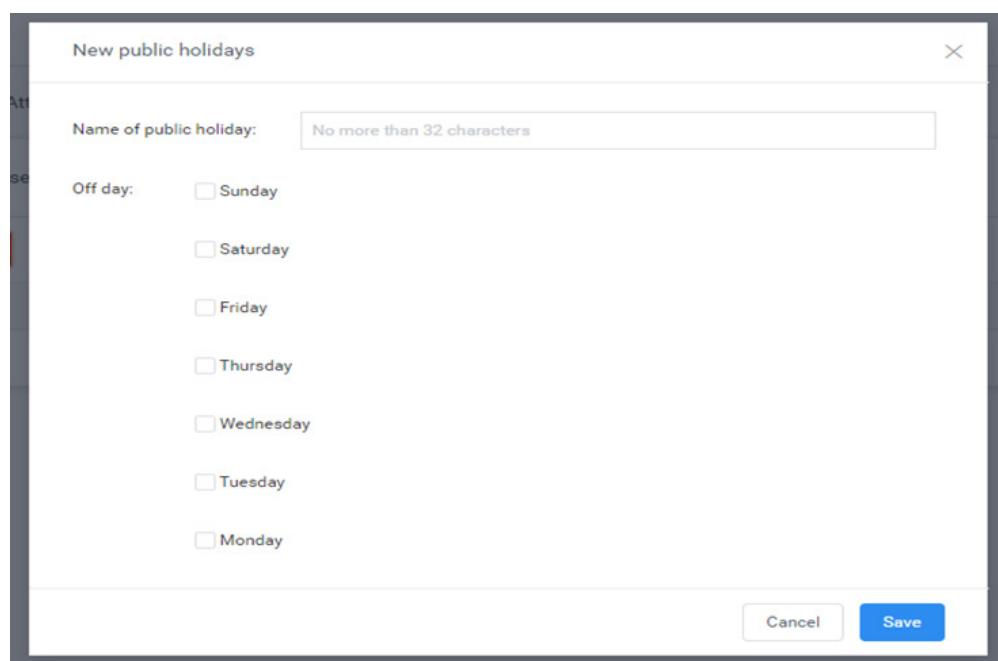
- **Public Holiday Name:**

Set a name for the public holiday.

- **Off Day:**

Select day(s) which you want to set as public holiday(s) in a week.

7.1.4. Device Group Settings

You can add, edit, and delete device groups in these settings. To edit a device group, click on the edit icon under the operations column. To delete a device group click on the delete icon under the operations tab.
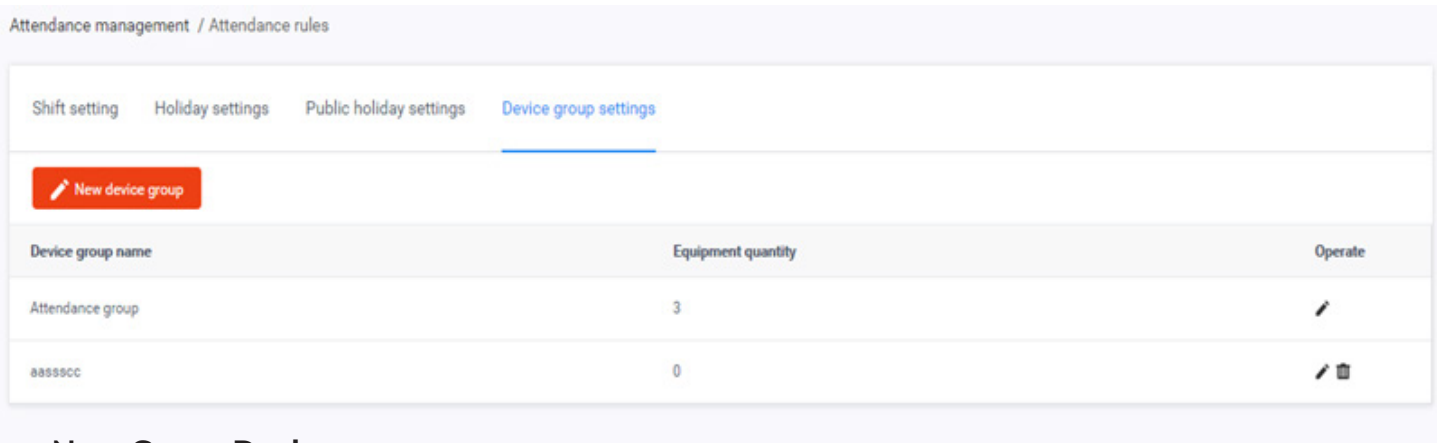
- **New Group Device:**

To add a new device group, click on new device group.
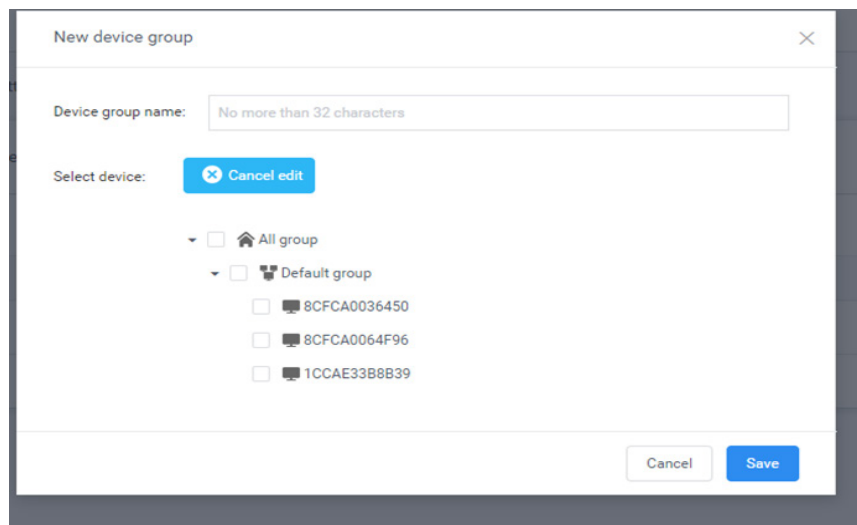
- **New Group Device:**
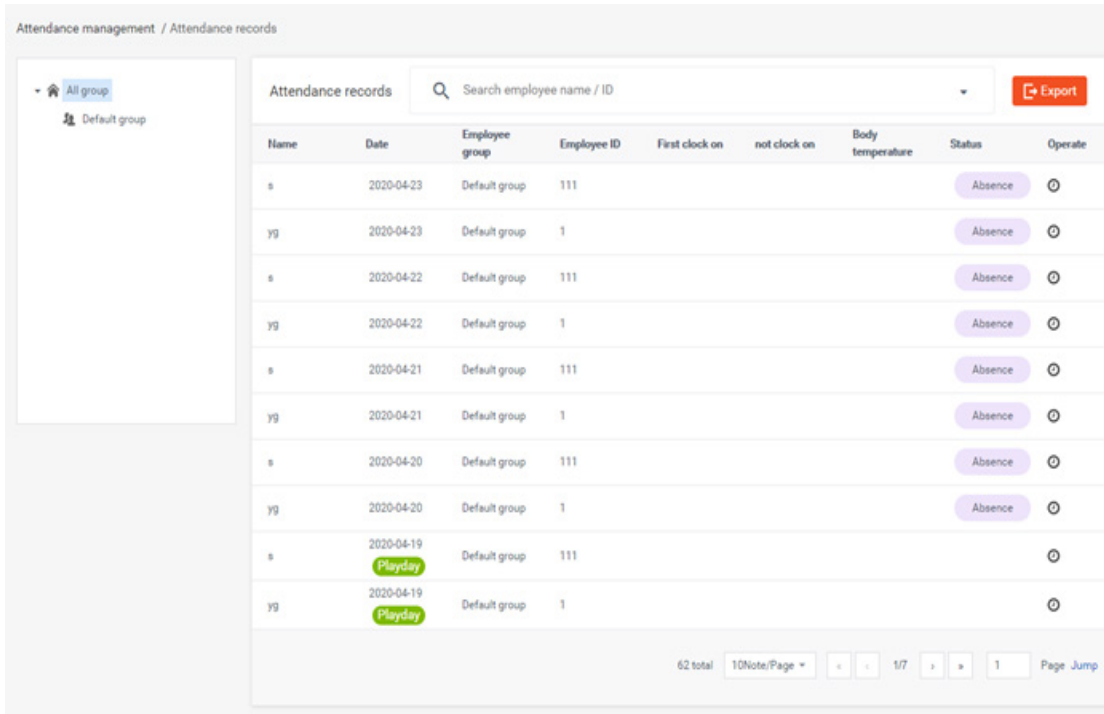
Set a name for the new device group.

- **Select Device**:

Select the devices you want to include in the new group and click save.

7.2. Attendance Records

You can access attendance records of all employees according to a defined time period and their group. You can also track employees according to their attendance status. Check attendance records of a specific employee by name and ID. You can also download this attendance data in the form of a list.

- **Employee Grouping list:**

Select all groups to view attendance records of all employees. These records will be displayed on the right side of the screen. To view attendance records of a specific group, select the relevant sub-group and the records will be displayed.

- **Attendance records list - Employee name, Employee ID, Employee group:**

Employee name, group and ID information is included in the attendance record list.

- **Attendance record list - Date:**
1. By default, attendance records prior to the selected date are displayed.
2. If there was a holiday on the selected date, then this information will be displayed in the list.
3. If there was a public holiday on the selected date, then "OFF" will be displayed.
4. If there was a public holiday and a customized holiday on the selected date, then "OFF" and "Holiday" will be displayed.

- **Attendance - First clock on, Last clock on:**

1. If the employee reporting time is not out of the specified range, then no mark will be displayed under the status column.
2. If the employee reports late to the office, then the status column will display this information.
3. If the employee leaves early, then the status column will show early departure.
4. If the employee is absent, then absent is marked in the status column.
5. If the employee did overtime that day, then overtime will be displayed in the status column.
6. If multiple conditions were detected from the employee's activity, then those statuses will be displayed under the status column, e.g. late, overtime.
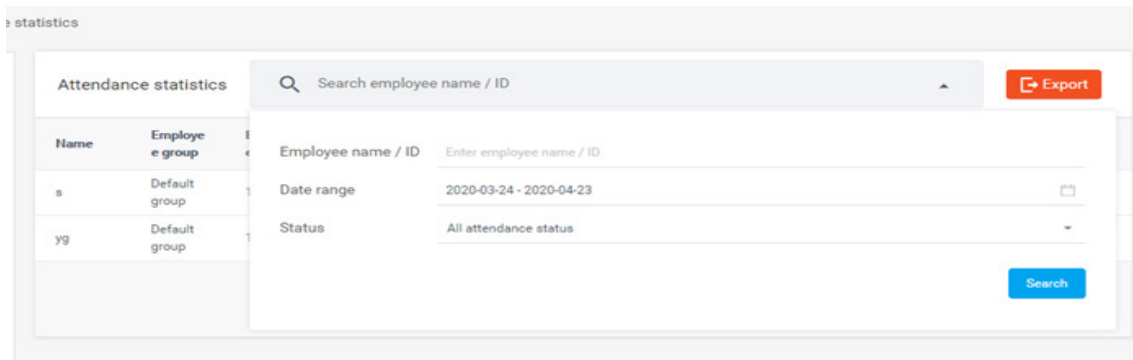
- **Attendance records list - Operate:**

You can enter the Pass management - Pass record page to view the employee's attendance details for the day.

- **Search bar:**

Enter the employee name or employee ID in the search bar to view employee's attendance record.

- **Range search:**

Click on the arrow and set a range.

1. By default attendance records of all employees will be displayed. To view records of a specific employee, you need to enter their name or ID in the search bar.
2. You can sort attendance records according to the status i.e. normal, late, absent, etc. You can also sort and view attendance records of a specific employee after entering their name or ID.

- **Search bar:**

Click on export to download employee attendance record from the current page.

- **Turn page:**

1. By default, 10 attendance records are displayed per page. You can view up-to 100 records per page.
2. You can navigate between the pages by using the arrow icons below. If you want to jump to a page, enter the page number and then click on jump.

7.3. Attendance Statistics

You can download attendance records of your employees from here. You can access and download records of any specified day(s), public holidays, working days and overtime attendance records of the holidays.
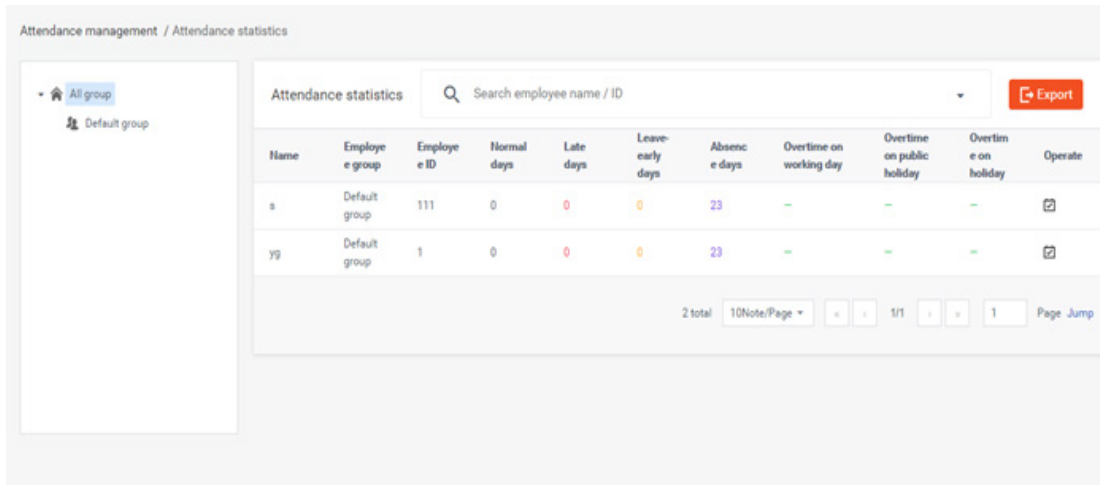
- **Employee Grouping list:**

Select all groups to view attendance records of all employees. These records will be displayed on the right side of the screen. To view attendance records of a specific group, select the relevant sub-group and the records will be displayed.

- **Attendance statistics list - Employee name, Employee ID, Employee group:**

The attendance record contains information about employee's name, group, ID, etc.

- **Attendance statistics list-normal days, late arrivals, early departures, absences:**

By default, attendance records of the current month will be displayed. The attendance record will contain information about employee's normal days, late arrivals, early departures, and absences. If there is no record, then 0 will be displayed.

- **Attendance statistics list - Overtime on working days, Overtime on public holidays, Overtime on holidays:**

By default, overtime records of the current month will be displayed. You can view information about employees working overtime on working days, public holidays and holidays. If there is no record then a "-" will be displayed.
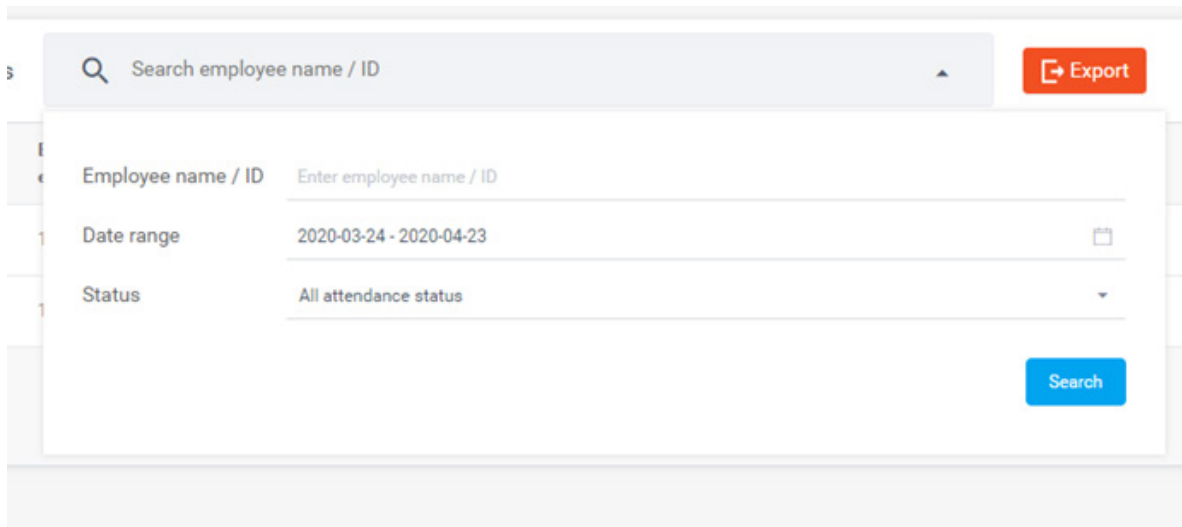
- **Attendance statistics list - Operate:**

Click the Attendance record icon on the left side of the interface to enter the Attendance management - Attendance record page to view the employee's attendance record for the day. Click the Attendance record icon on the right side of the interface to enter the Pass management - Pass record page to view the employee's attendance details for the day.

- **Search bar:**

Enter the employee name or employee ID in the search bar to view employee's attendance record.

- **Range search:**

Click on the arrow icon on the search bar and set range.

1. If you do not enter the employee name or ID, then attendance records of all the employees will be displayed in the selected range. If you have not set a range, then attendance records for the current month will be displayed
2. You can set the search status according to the type of data you want to view e.g. full attendance, late, etc. By entering employee's name or ID, you can view his/her records according to the set status

- **Export:**

Click export to download employee attendance records from the current page.

- **Turn page:**
1. By default, 10 attendance records are displayed per page. You can view up-to 100 records per page.
2. You can navigate between the pages by using the arrow icons below. If you want to jump to a page, enter the page number and then click on jump.