OneScreen GoSafe

Management Platform User Manual

Supports all GoSafe models

800-992-5279 | sales@onescreensolutions.com

Contents

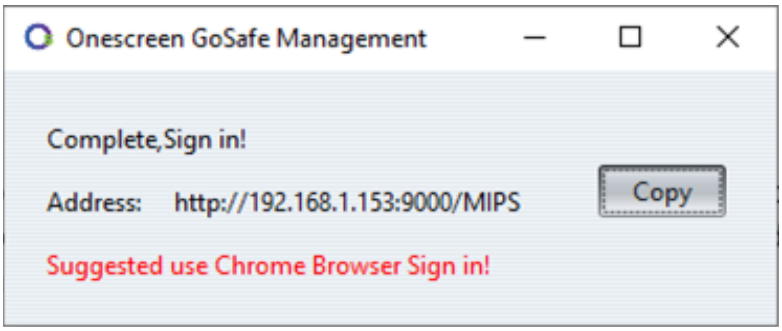
1. Installation and Login

- Double-click the .exe installation file and follow the installation instructions for quick installation. (Click here to download the GoSafe Management software)

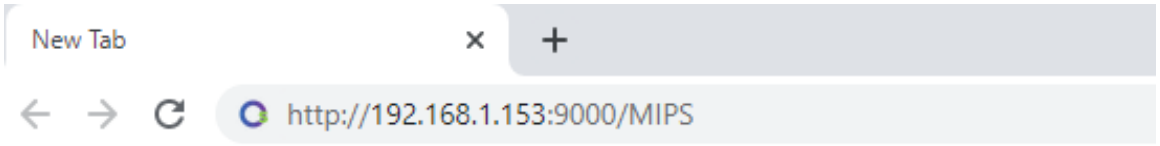
  Note: Please allow firewall exception on your windows system, and if you are using a restricted network, whitelist the application on the network.

  The folder to whitelist can be found on C>Users>[User name]>AppData>Roaming>MIPS>GoSafe Management Software

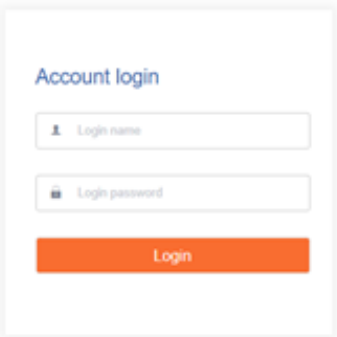
- After the program is installed, the GoSafe management software launches automatically (See below picture for reference)



- After startup is complete, click the “Copy” button. Open Google chrome browser and paste the link to open Management software.



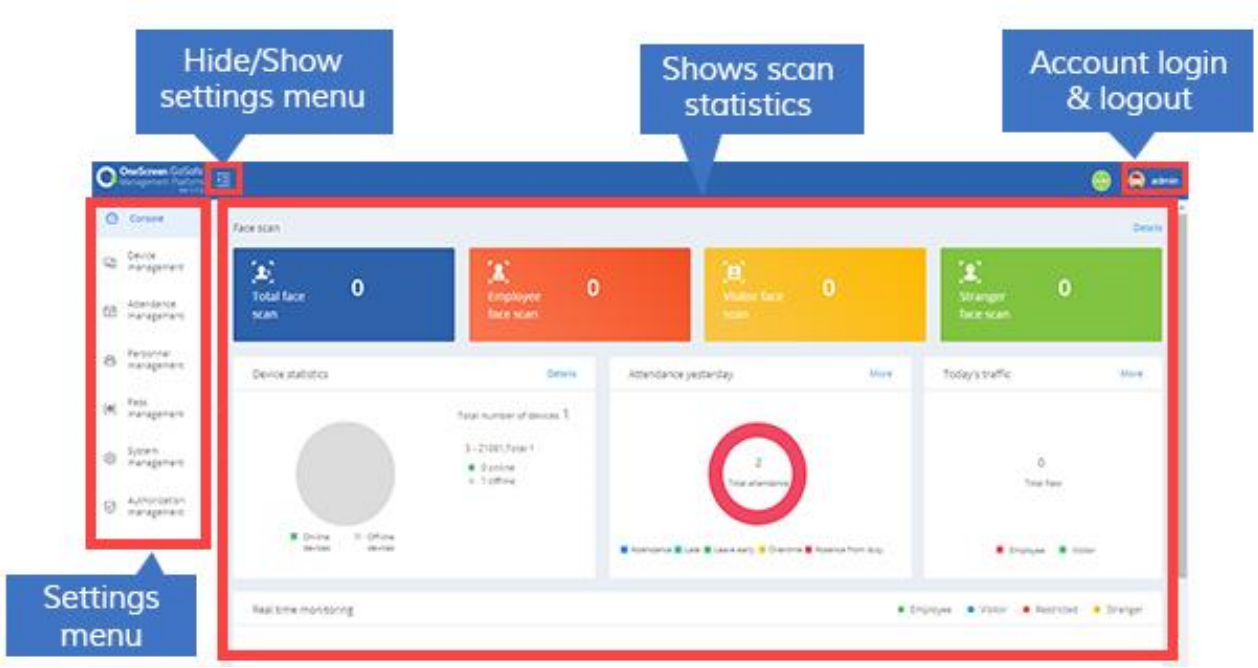
- Enter your username and password to log in
  Standard username: admin
  Standard password: 123456



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

2. Console

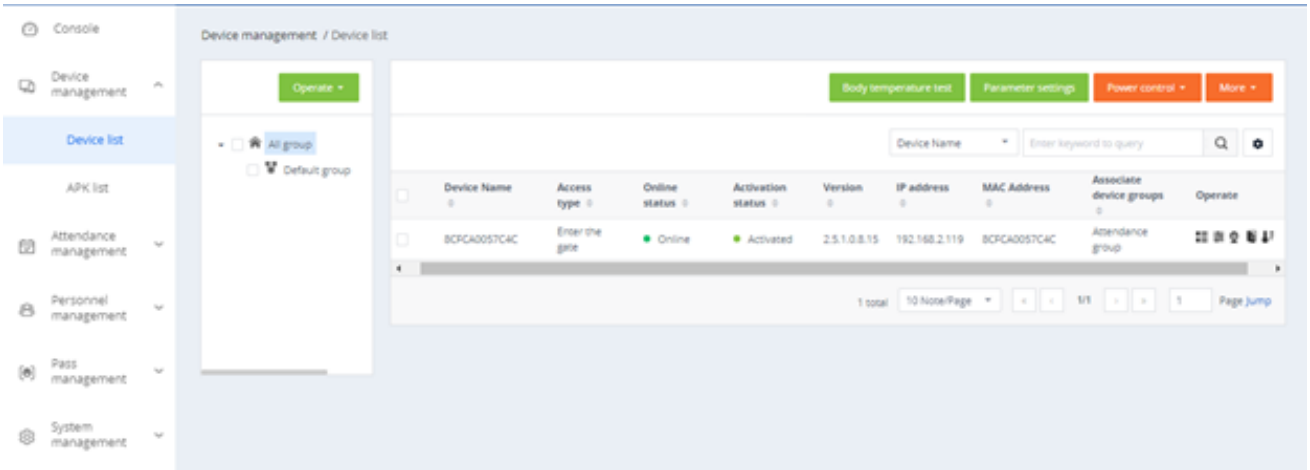
It provides an overview of the number of devices and online status which includes statistics of the face scan (total faces scanned, employee faces scanned, visitor faces scanned, stranger faces scanned), today's pass and real-time monitoring (employees, visitors, restricted, body temperature), and provides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



3. Device Management

3.1. Device List

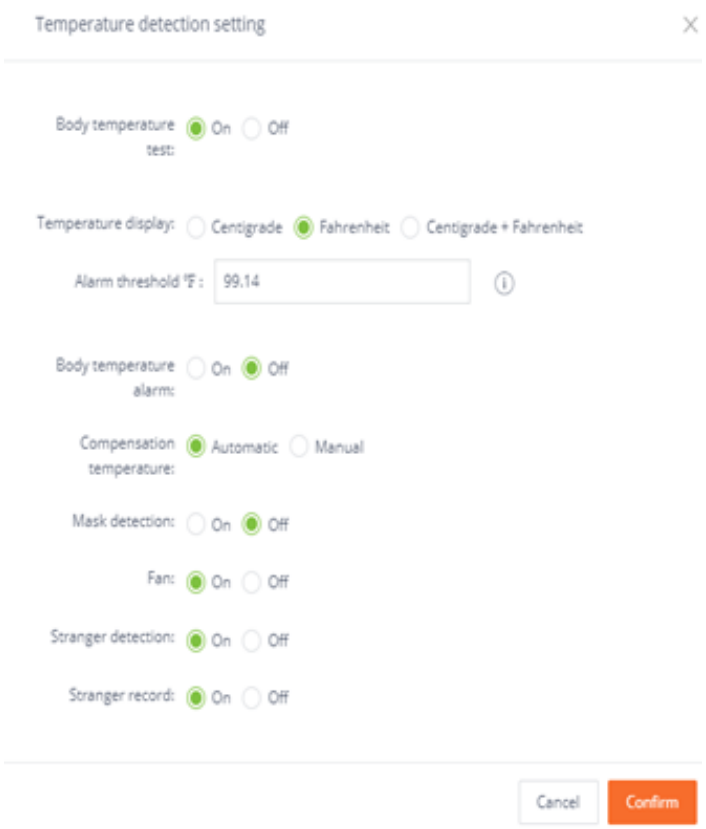
Device list allows you to manage all of the devices connected to your management console using this dashboard. You can alter settings on each individual device or by selecting a group of devices to alter the settings collectively.



3.1.1. Body Temperature Test Settings

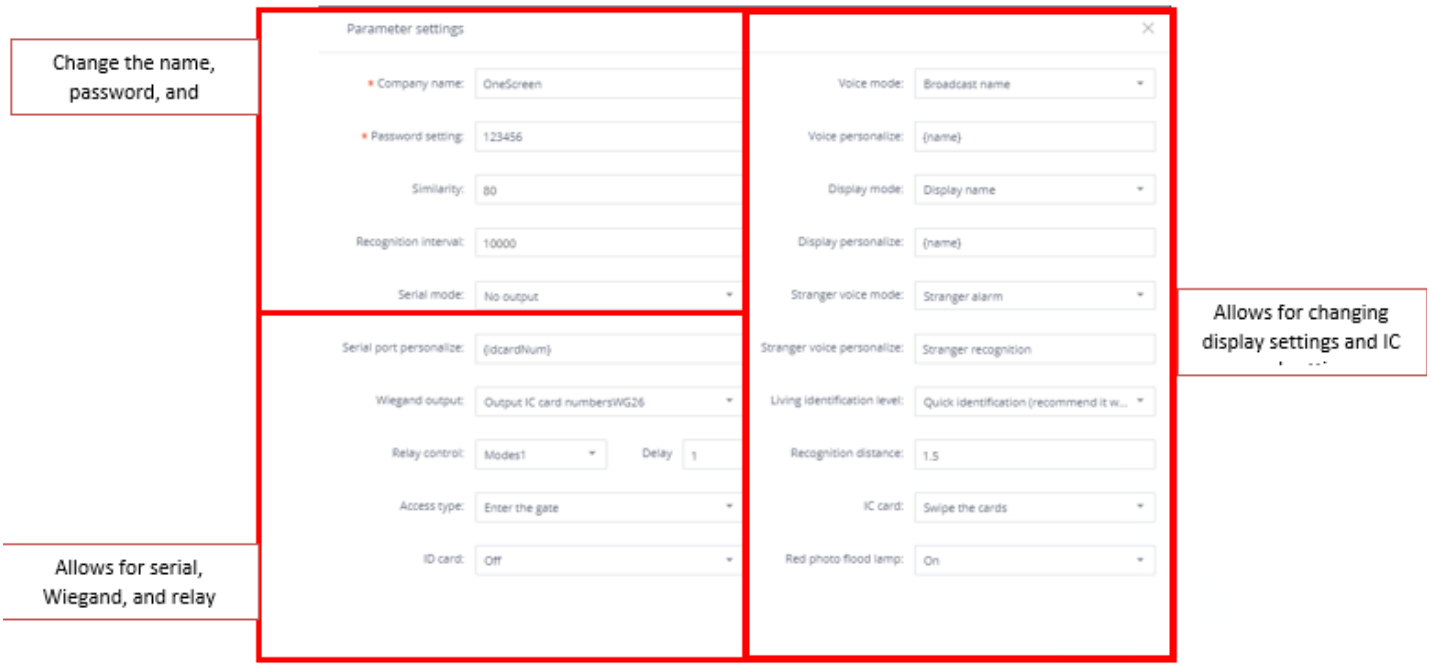
The body temperature test settings allow the user to configure temperature settings on the selected device(s).

- **Body Temperature test:** Turn on/off temperature detection
- **Temperature Display:** Choose to display the temperature in Centigrade, Fahrenheit, or both.
- **Alarm Threshold:** Set the temperature threshold for the device to activate the alarm
- **Body Temperature Alarm:** Turn on/off the alarm function
- **Compensation Temperature:** Allows to input compensation temperature to cater to the high/low ambient temperature
- **Mask detection:** Turn on/off the functionality of scanning the individual's face for a mask
- **Stranger detection:** Allows the device to scan strangers. Turning it on will allow the strangers admittance whereas turning it off won't allow their admittance
- **Stranger Record:** Turn on/off the functionality of updating the database with stranger's data



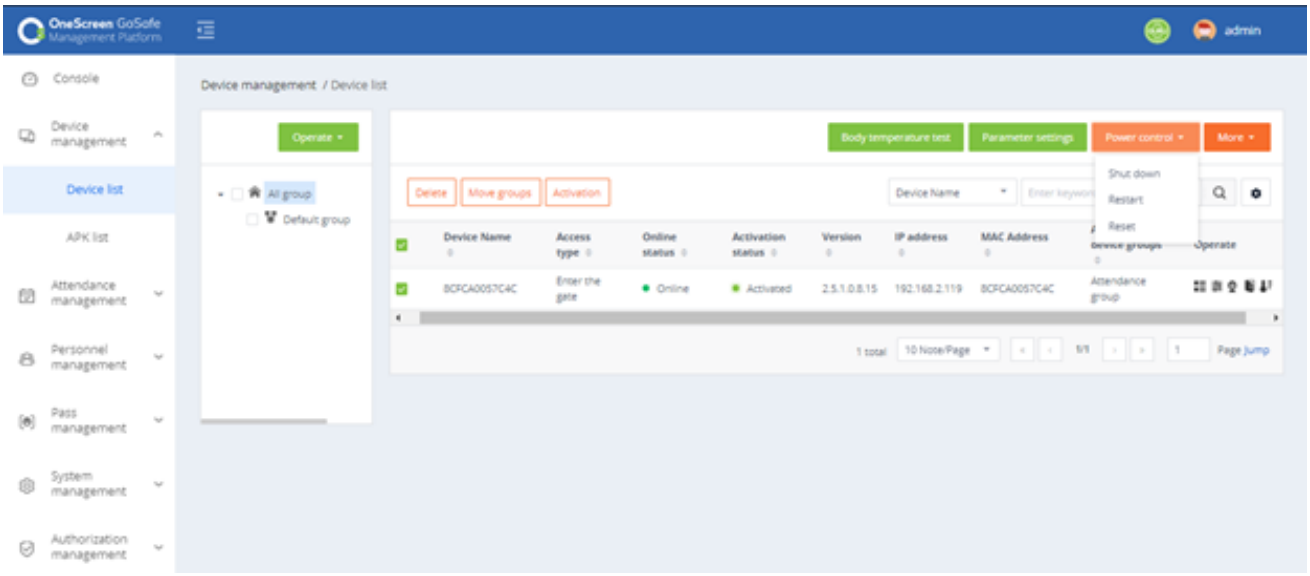
3.1.2. Parameter Settings

Parameter settings essentially allows you to configure your devices with automatic access control systems, Wiegand interfaces, and serial communications.



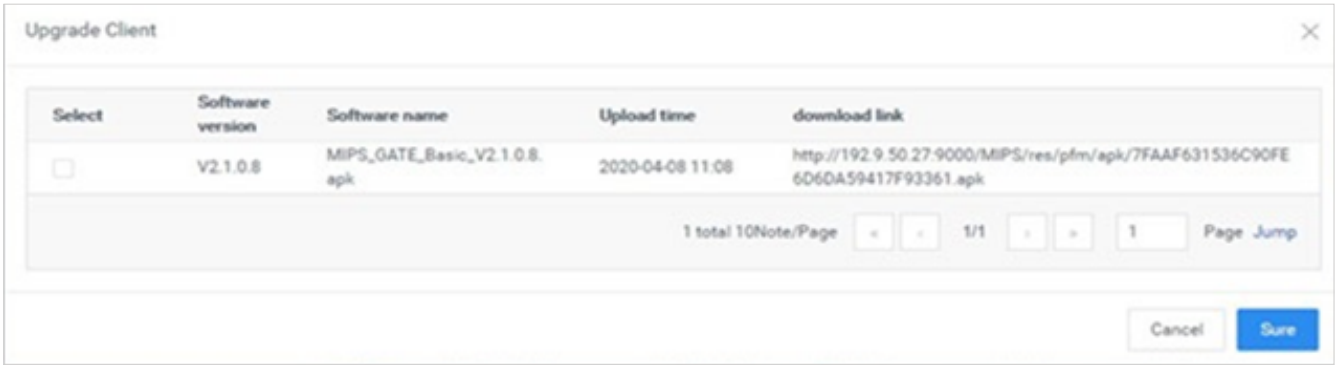
3.1.3. Power Control

Power control settings allow you to remotely **Shut off, Restart,** or **Reset** the selected device(s).



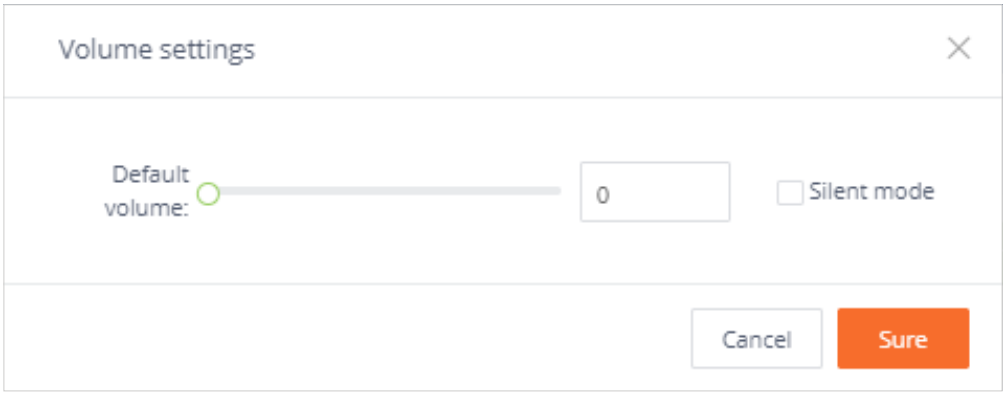
3.1.4. Client upgrade

Select a device from the 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 soft-ware version of the device you want to upgrade to and click upgrade to complete the software upgrade. Both online and offline upgrades are supported.



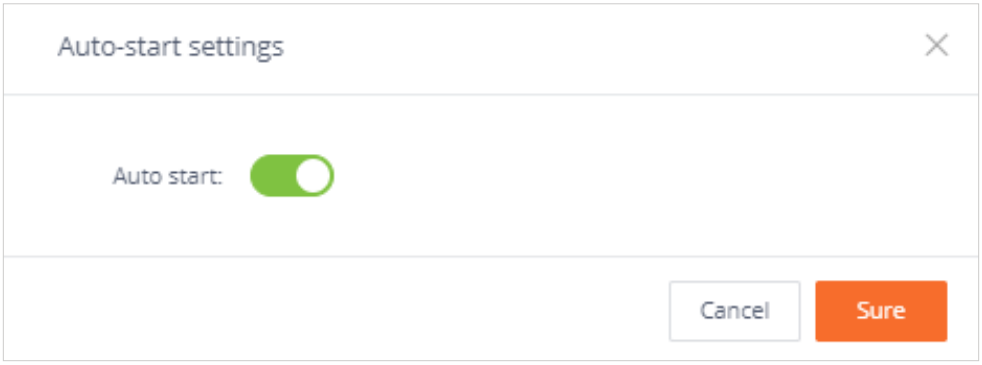
3.1.5. Volume Setting

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.



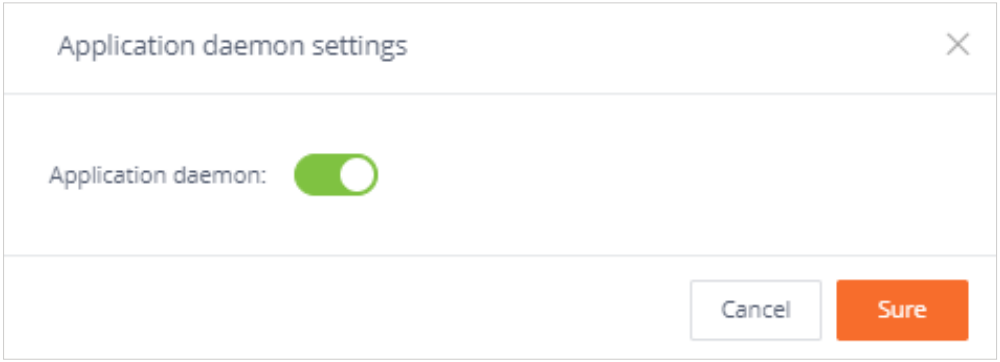
3.1.6. Auto-Start

The Auto-Start settings allows you to turn on the functionality of automatically starting the device with the scanning interface. To enable this feature, turn on the auto-start setting.



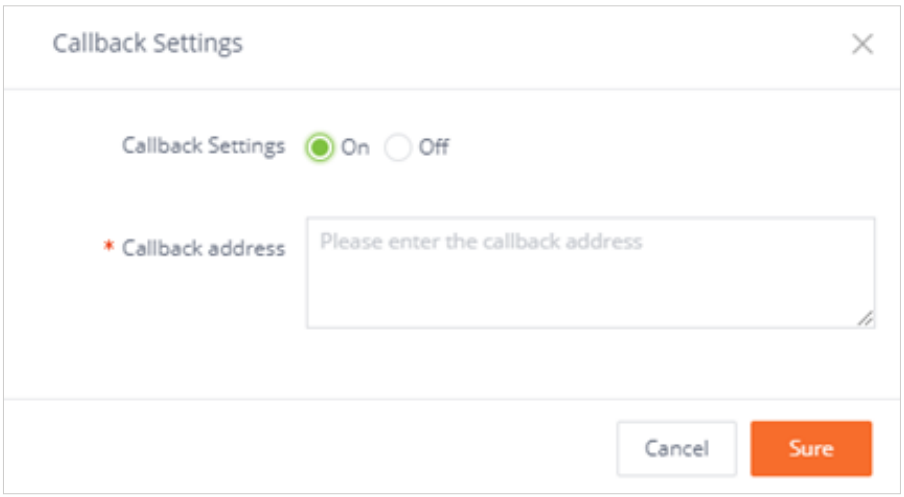
3.1.7. Application Daemon

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. Callback Settings

For API integration with the management console, the callback setting allows information to be sent to a particular URL



3.1.9. Door Control

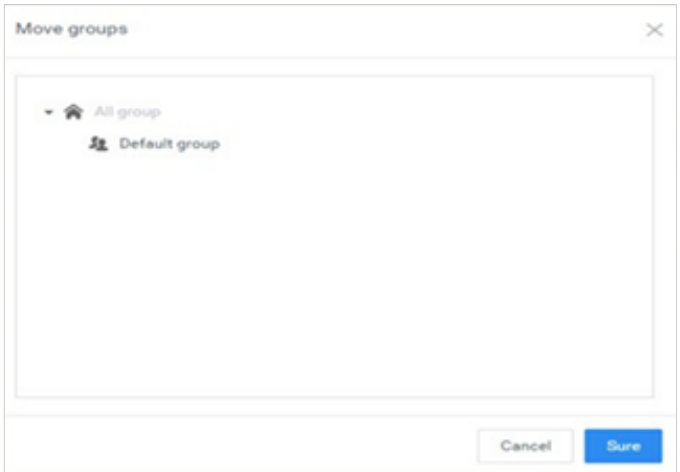
To open a specific gate controlled by a device, go to Device list and click on “open the door remotely” of the desired device. This will open the access control system, which is controlled by that particular device.

3.1.10. Delete Device

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

3.1.11. Device Groups

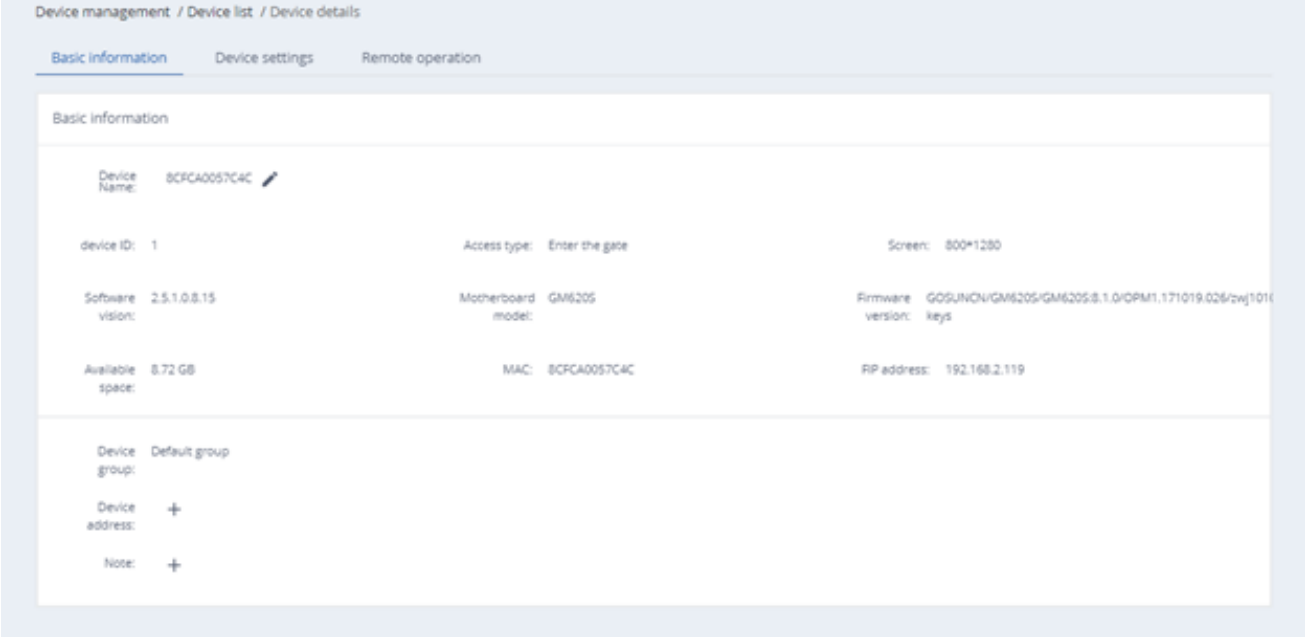
From the Device list, select the devices that require mobile grouping and click “Mobile Grouping”. In the pop-up window select the target group you want to move these devices to, and click confirm. You can move single or multiple devices to a group.



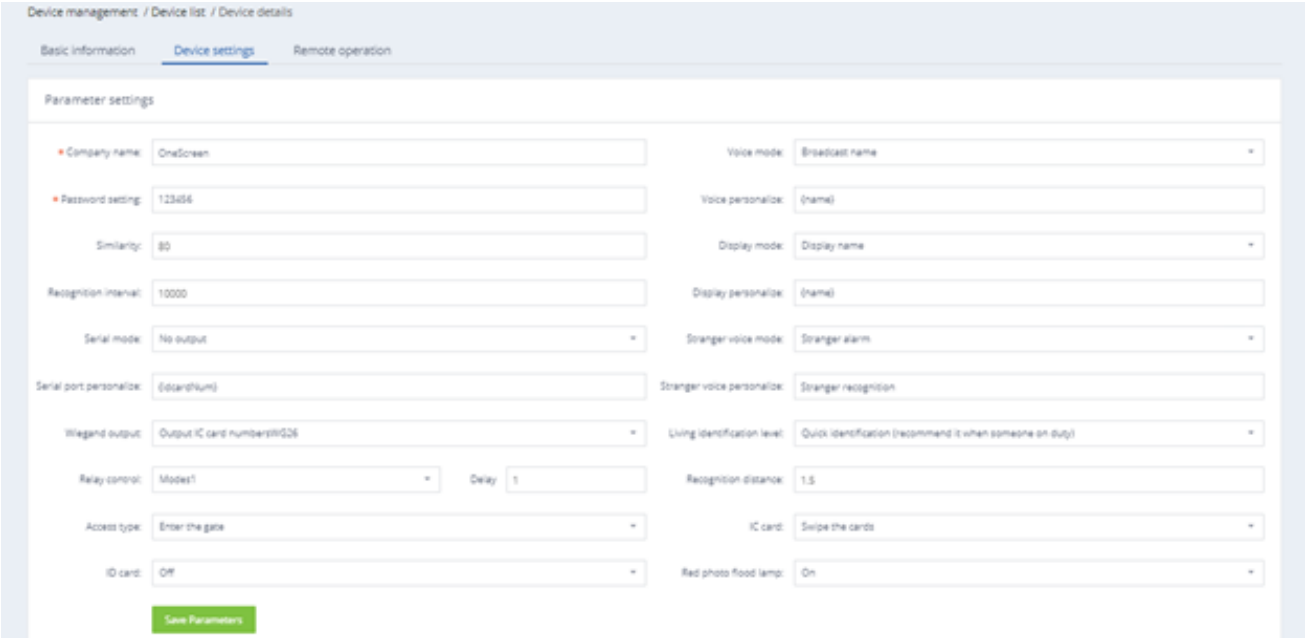
3.1.12. Device Details

The device details include basic information about device settings and remote operations.

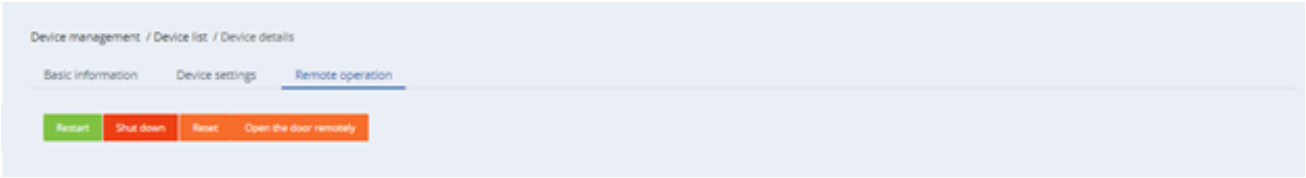
Basic information: View device information; edit device name, device address, etc.



Device settings: You can view and modify device parameter information, display set- tings, and other settings. You can choose to upload your company logo on display settings under device settings as well.



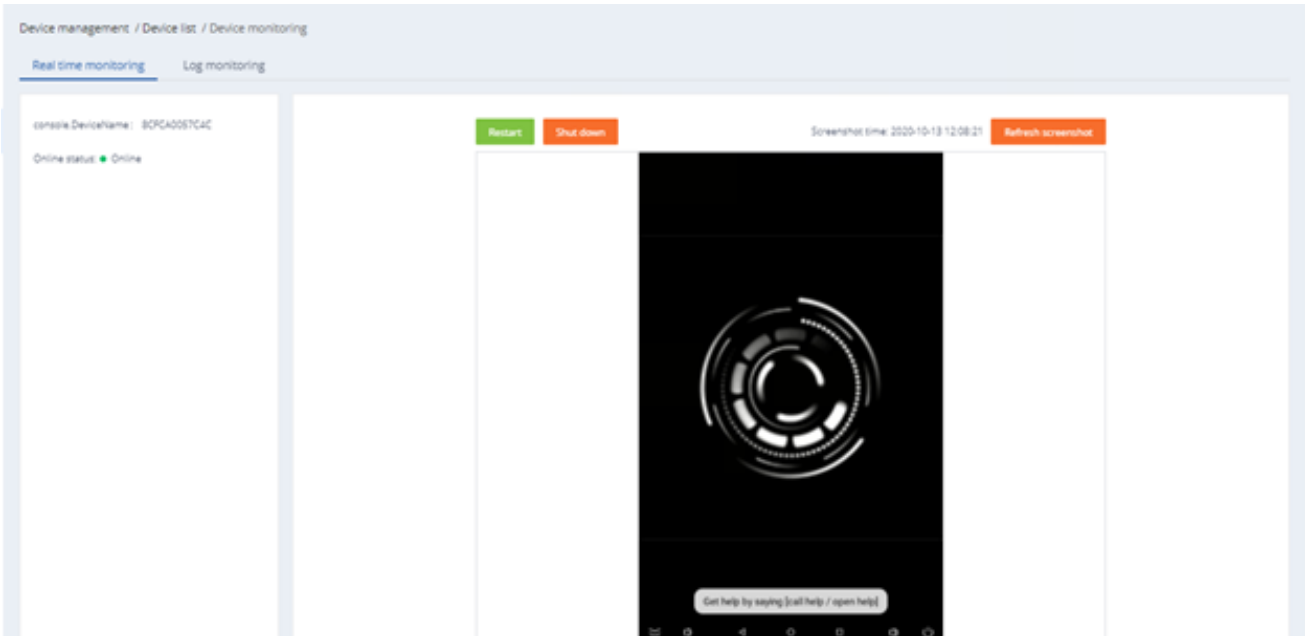
Remote operation: restart, shutdown, reset and remote door opening.



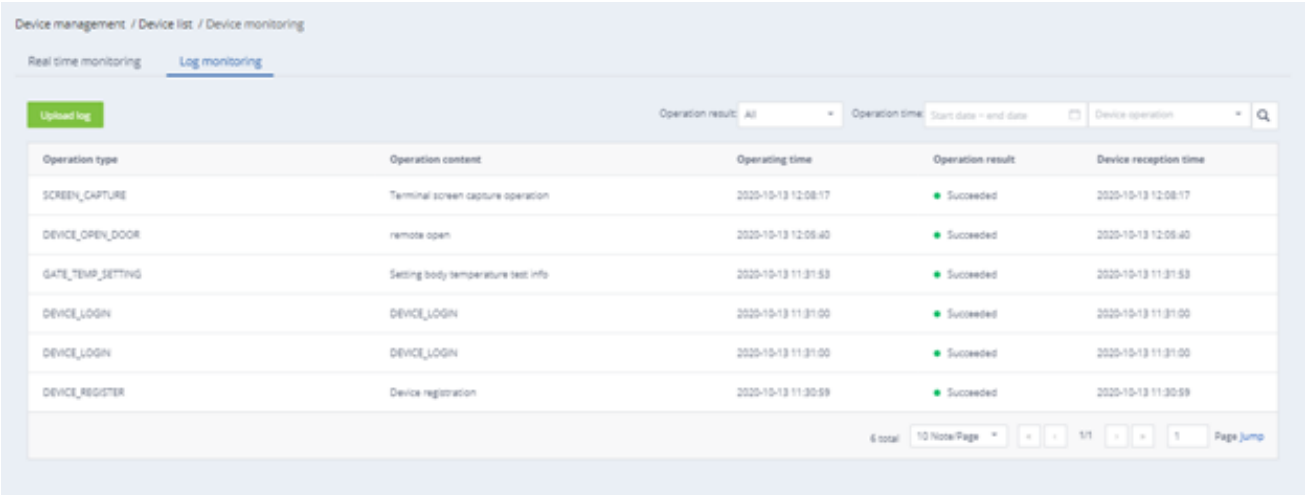
3.1.13. Device Monitoring

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.

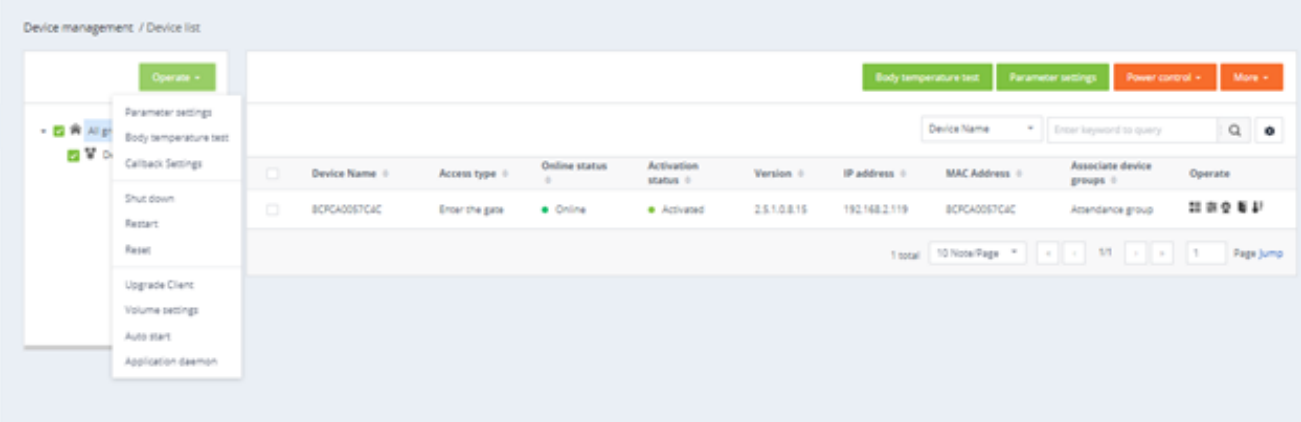


- **Log monitoring:** View related operation logs of the device.



3.1.14. Bulk operations on Group

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 ap- plication 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 select- ed group, please select again. If there are devices in the selected group, the original settings will be overwritten.

3.1.15. Device Group Management

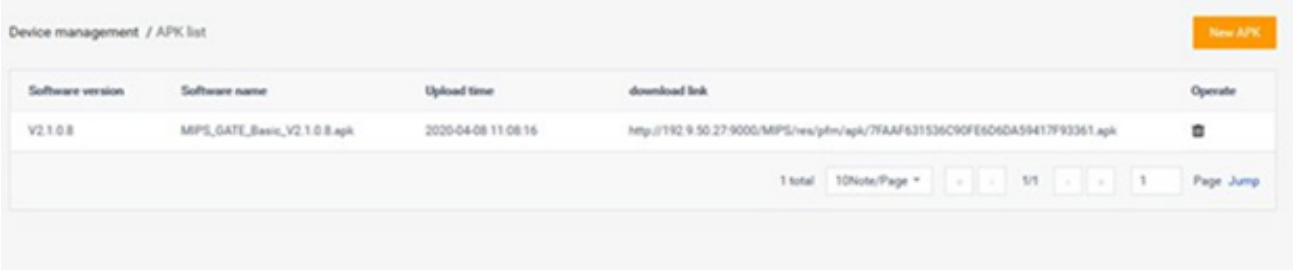
Device grouping uses structured grouping by default. Each user group has a default device group. You can add, modify, and delete device groups on the user group. This operation is similar to the user grouping in Group structure.

3.2. APK List

APK list: This page contains client software list information and software version upload and delete operations.

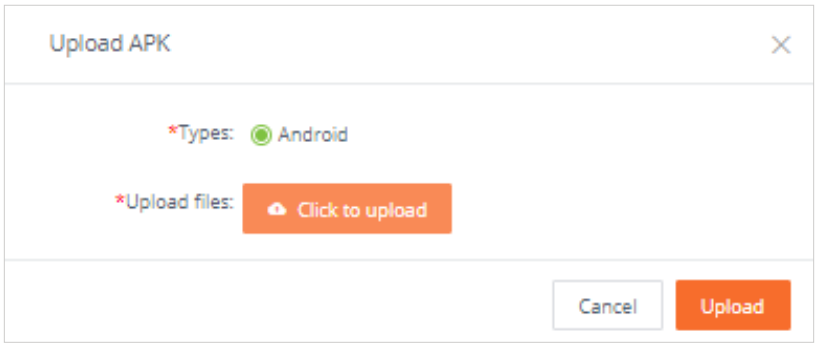
3.2.1. Delete APK

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



3.2.2. New APK

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

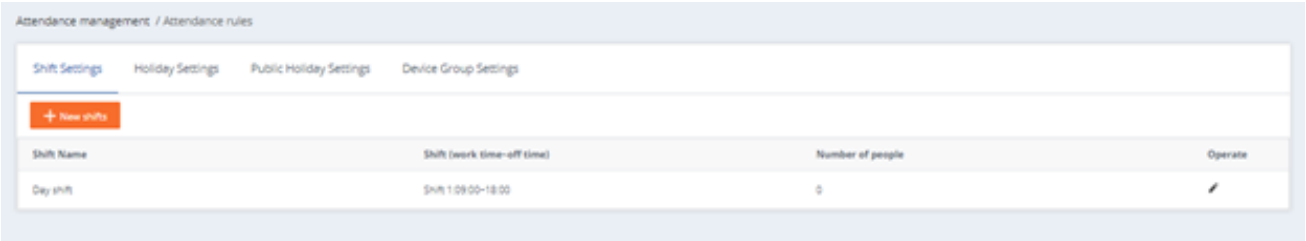


4. Attendance Management

In attendance management, you can change/alter the attendance settings, holiday setting, or view attendance statistics.

4.1. Attendance Rules

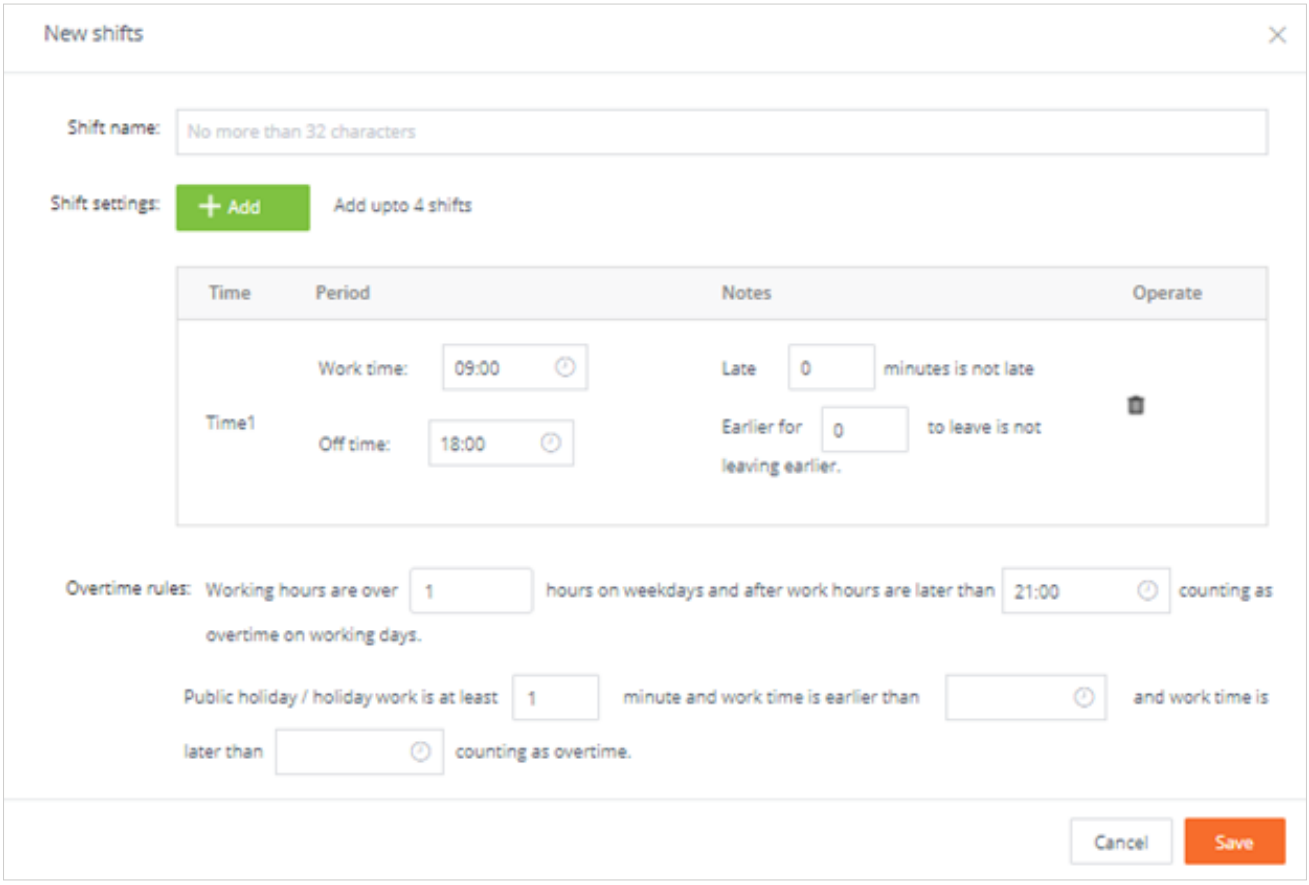
Here you can add, modify and delete attendance rules related to shifts, holidays, public holidays, and device groups.



4.1.1. Shift Settings

Shift settings allow you to change information about shifts. It allows you to create new shifts, edit and modify existing shifts. A shift already exists by default (which can be modified), and up to 4 shifts can be created.

- **New Shift:** Click on New Shift to open settings on creating a new shift.



- **New Shift:** Click on New Shift to open settings on creating a new shift.

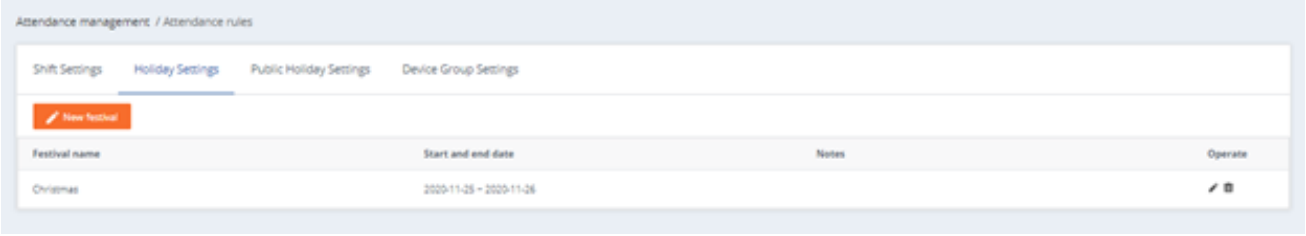
- **Shift Name:** Set a title of a shift.

- **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.

4.1.2. Holiday Settings

You can add public holidays in these setting options, and the attendance for that day will not be marked.



- **New Holiday:** Click on new holiday to go to the settings prompt for adding a new holiday.

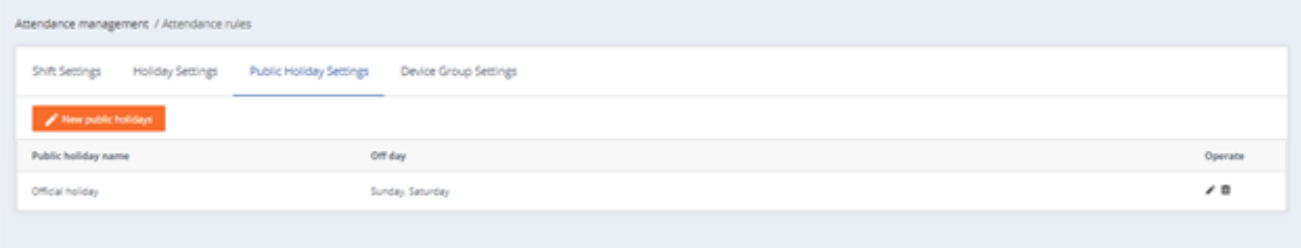
- **Festival Name:** Enter the name of the holiday/festival.

- **Start date & End date:** Set the start and end date for the holiday.

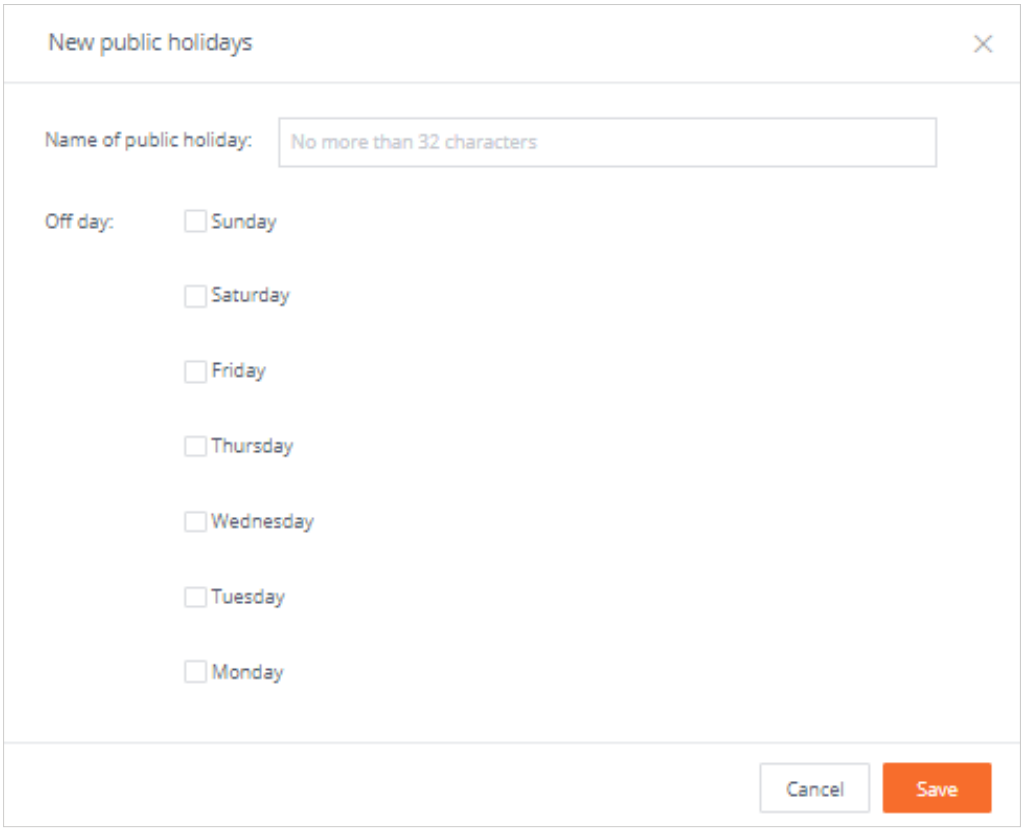
- **Notes:** You can write a brief description about the holiday here, or a message.
  E.g. For Labor Day, you can add a holiday for the day, set the date for it (7th September in this case), and write a note for it such as ‘stay at home’ or ‘Its off due to labor day’, and then save. The attendance for that day will not be marked then.

4.1.3. Public Holiday Settings

You can customize the fixed weekly holidays, which by default are Saturday and Sunday. 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.

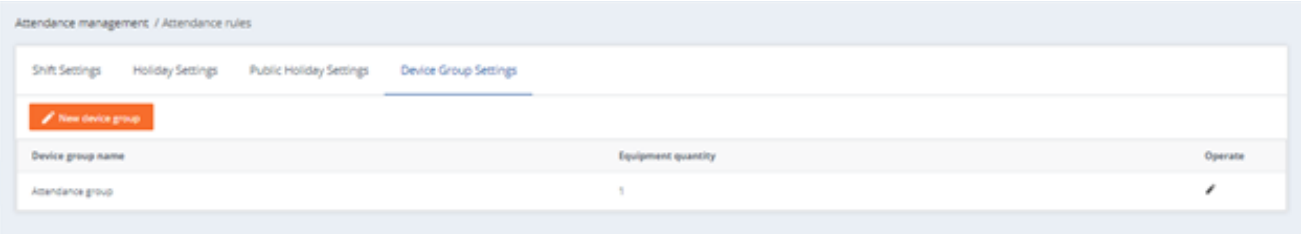


- **Public Holiday Name:** Set a name for the public holiday.

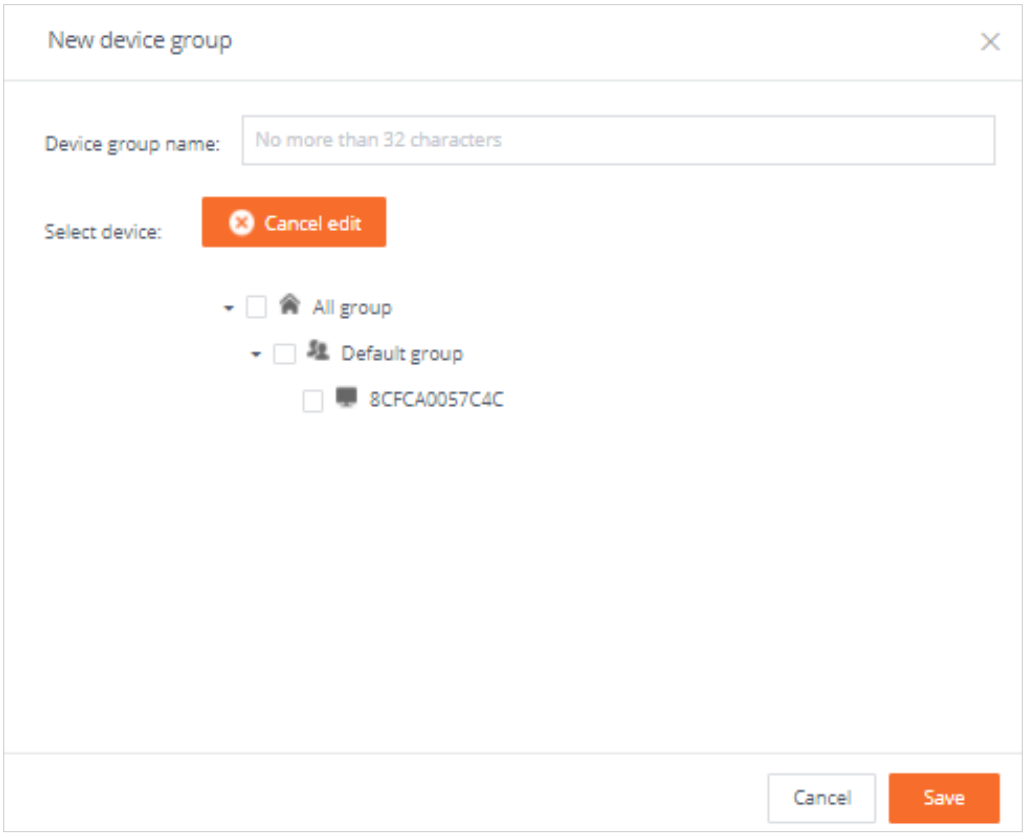
- **Off Day:** Select day(s) which you want to set as public holiday(s) in a week.

4.1.4 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. The shift settings would be linked in group to this list.



- **New group device:** To add a new device group, click on new device group.

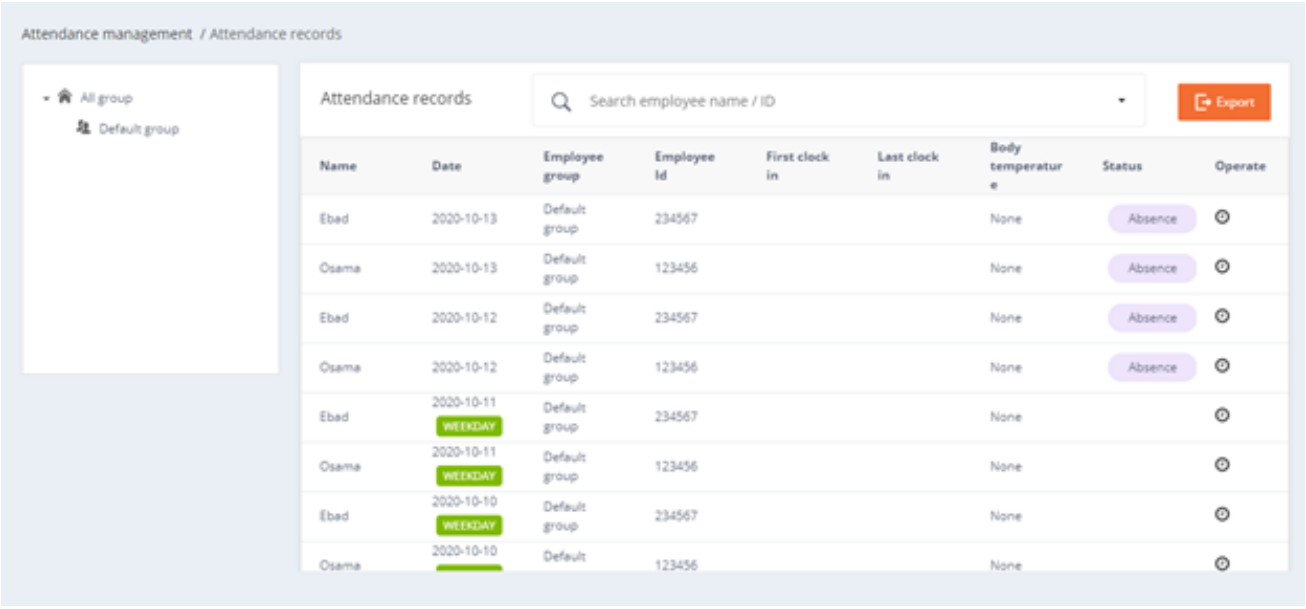


- **New Group Device Name:** Set a name for the new device group.

- **Select Device:** Select the devices you want to include in the new group and click save.

4.2. Attendance Records

You can view the attendance record of employees for particular days in this settinvg. You can also choose between different employee groups (set in employee settings). A sample of the list is shown below.



- **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.

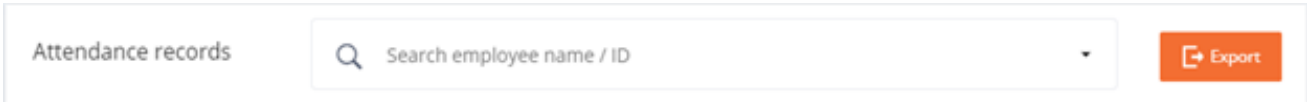
- **Attendance records list:** You can view the employee name, date, employee group, employee ID, First clock in, Last clock out, body temperature and attendance status.
  (Clicking on the operate will take you to Pass Records).

  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:
Status Column: The status column will show the following options when the corresponding conditions are met.
Absent: Employee will be marked absent if they did not clock in/clock out for the day
Late: If the employee clocks in after the allowance time set in shift settings, he will be marked late
Early departure: If the employee clocks out at a time earlier than the shift end (even before the allowance set in shift settings), he will be marked as an early departure
Overtime: If overtime was performed during that day, the display status will state ‘overtime’
If multiple conditions are detected, then all statuses will be displayed e.g. overtime, late etc.

(Note: In case the employee checks out and checks back in, and then checks out again, the first check in time and the last check out time would be considered).

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



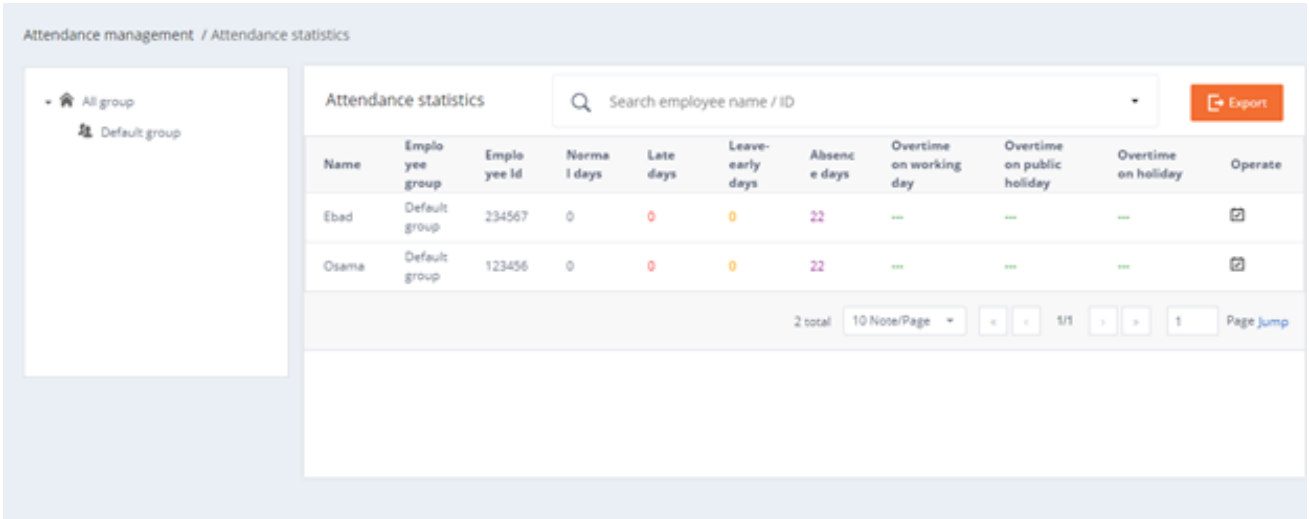
1. By default, attendance records of all employees will be displayed. To view records of a specific employee, you need to enter their name or ID in the search bar.
2. You can sort attendance records according to the status i.e. normal, late, absent, etc. You can also sort and view attendance records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

- **Export:** 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.

4.3 Attendance Statistics

You can download attendance records of your employees from here. You can access and download records of any specific 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, Normal days, Late days, Leave/ early days, Absent days, Overtime on normal working day, Overtime on holiday, and Operate.

  (Operate will take you to the attendance records page)

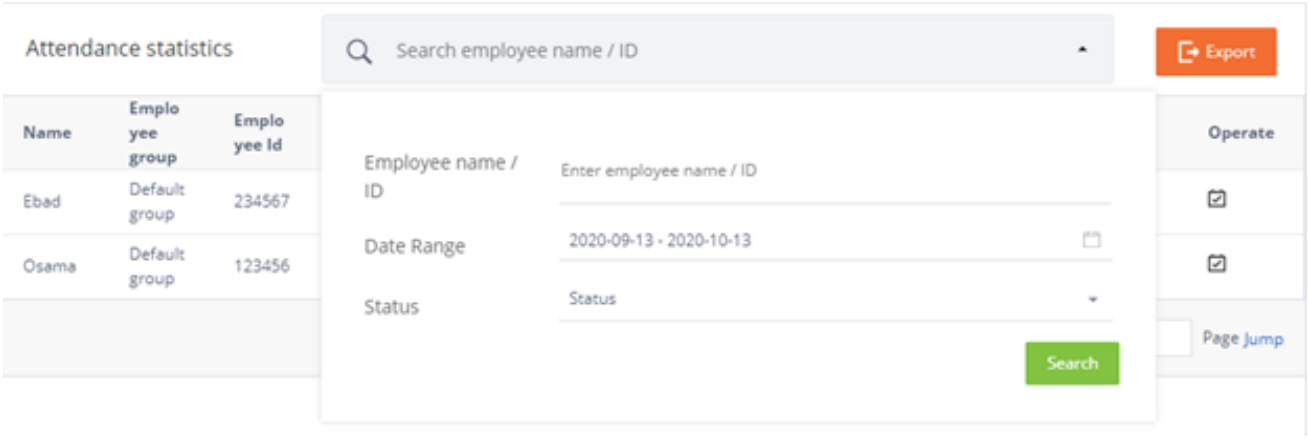
  In the absence of a record for normal days, late days, leave/early days and absence days, '0' will be displayed.

  In the absence of overtime for normal day, holiday and public holiday, '-' will be displayed.

- **Attendance statistics list - Operate:** Click on the operate option at the right side of any marked attendance statistic, and a day to day statistic (attendance record) of that individual would be provided.

- **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.



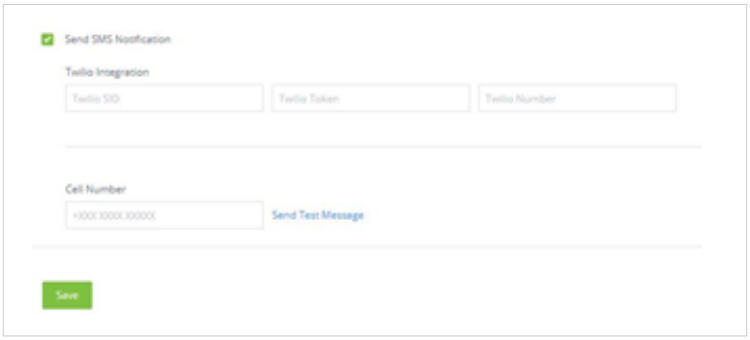
1. If you do not enter the employee name or ID, then attendance records of all the employees will be displayed in the selected range. If you have not set a range, then attendance records for the current month will be displayed.
2. You can set the search status according to the type of data you want to 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.

4.4 Attendance Notifications

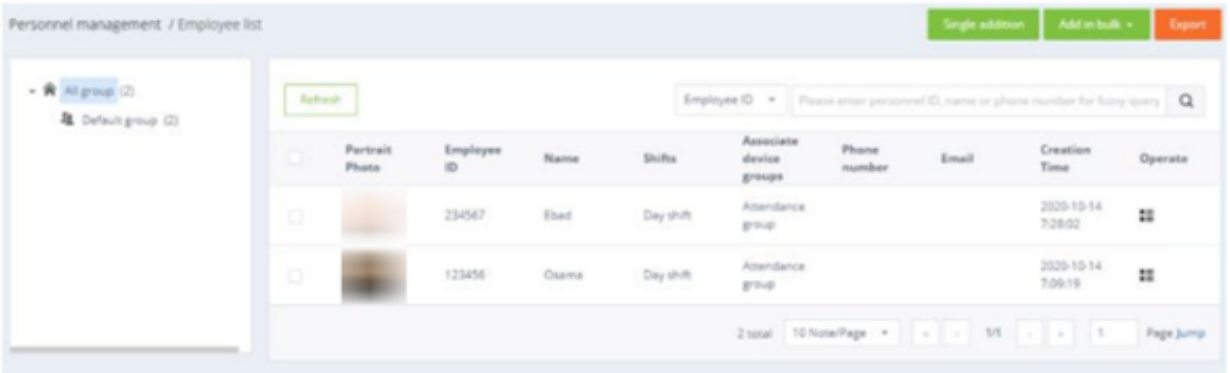
You can set SMS notifications to go out from the console using a Twilio account which can easily be integrated with the GoSafe management console. Simply obtain your Twilio SID, token and number from the Twilio portal and save the details onto the console management system. You may also send a test message to a number to verify if your integration was successful.



5.0 Personnel Management

5.1. Employee list

The employee list is used for managing the information of the employee database. You can add, view, edit, delete, search and export any employee database created. You have the option to add employees individually or in bulk (bulk operation is not possible on the GoSafe device on standalone mode).



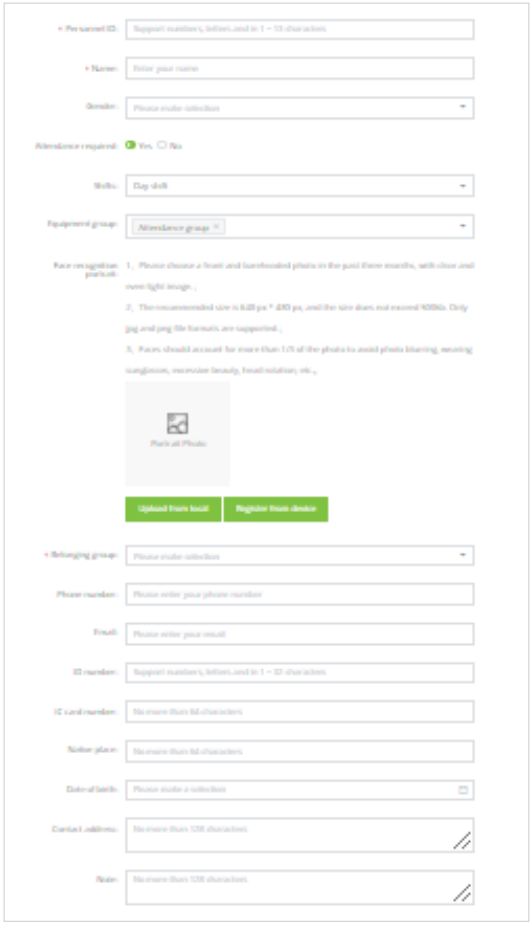
5.1.1. Add Employee information (Single Addition)

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 (Note: The options with ‘*‘are compulsory to fill. You must add the **personnel ID, name and employee group** whereas the rest are optional).

3. Add a face recognition photo (either from the local disk or device) and click “Save” to complete the employee creation.

Uploading a face recognition photo:



Upload from local disk

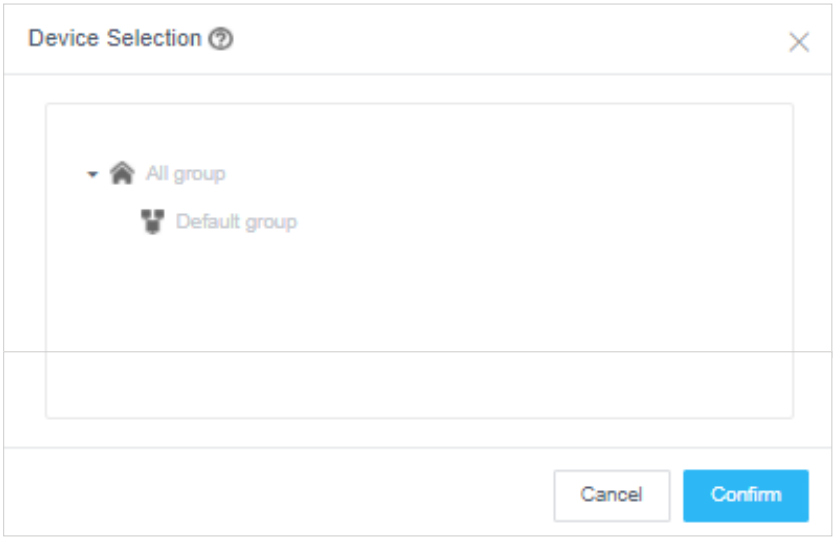
Click “Upload from local” to upload a picture from your system. Simply select a jpg or png portrait, and upload it.

Note: Portrait photo specifications

1. Please choose a front-and-bareheaded photo from the past three months, with a clear and evenly distributed light image.
2. The recommended resolution is 640 pixels x 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, sun- glasses, excessive facial-up, and head rotations.

Register from device

Click “Register from Device” to select a device from which you want to capture the image.

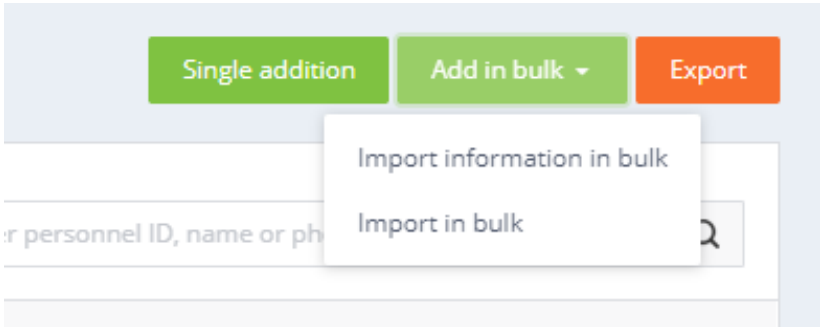


Simply stand in front of the device after clicking confirm, and the device will capture your picture. Once the picture is verified (you can click on register from device again to retake the picture), simply click save and the picture will be stored in the database.

5.1.2 Add Employee information in bulk

Steps:

In the Employee list, click “Add in Bulk - Import Information in Bulk” option.



1. First, click “Download Template”. Download the excel template file to your computer with the file name “Personnel_import_template_en”. Then fill in the employee information in bulk under the corresponding column.

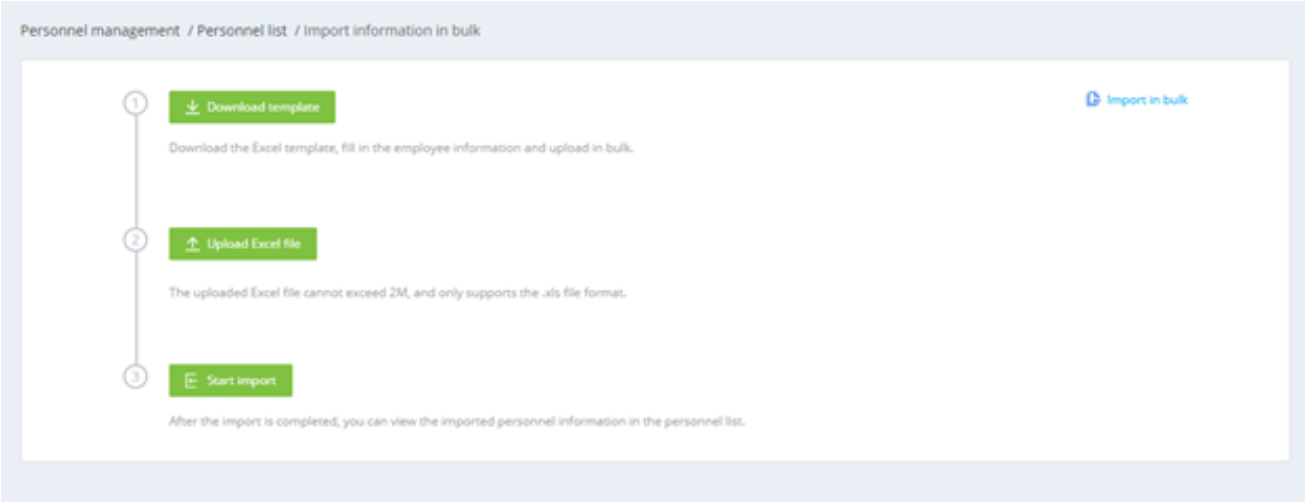
Instructions:
1. Personnel ID: required; cannot be repeated; in 1 to 9 characters, only consisting of numbers, letters or their combinations, such as 12345, abcd, a123.
2. Name: required; in 1 to 128 characters, consisting of Chinese, English, numbers, or their combinations (can contain Spaces).
3. Gender: 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-s
5. Phone number: required; cannot be repeated; in 1 to 20 characters.
6. ID card: optional; cannot be repeated; in 1 to 32 characters, consisting of numbers, letters or their combinations.
7. Email: optional; cannot be repeated; in 1-32 characters, no limitation on character types.
8. IC card: optional; cannot be repeated; in 1-64 characters, no limitation on character types.
9. Ethnic group: optional, the optional range is 56 ethnic groups in China.
10. Native place: optional; in 1-64 characters, no limitation on character types.
11. Date of Birth: optional; the format is "xxxx-xx-xx", and not possible to enter a future date.
12. Address: optional, in 1-128 characters, no limitation on the character types.
13. Notes: optional, in 1-128 characters, no limitation on the character types.
14. Associated device group: optional, in 1-32 characters; must be a device group name that already exists in the system, multiple groups are separated by con

Personnel ID	Name	Gender	Belonging group	Phone number	ID card	Email	IC card	Native place	Date of Birth
52300777	John c	Male	All group-Default group	+8613412345678	430123456789	aff@gmail.com	000230001212	London	05-Dec-80

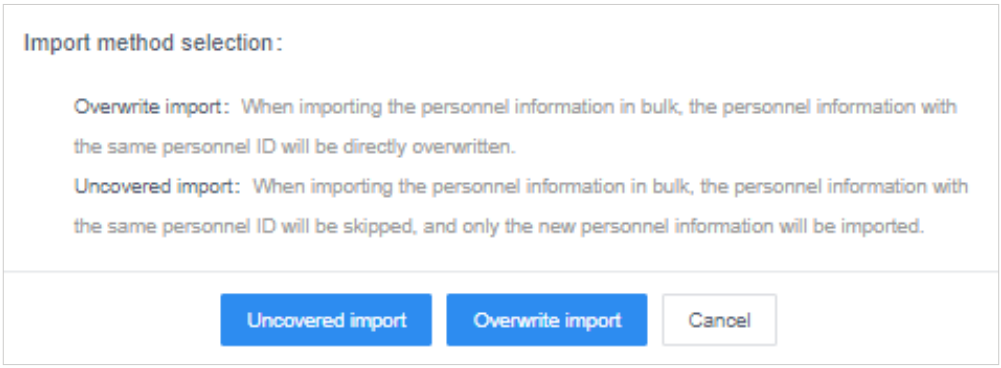
(The sections marked in red need to be filled for upload, however the Phone number is optional).

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.

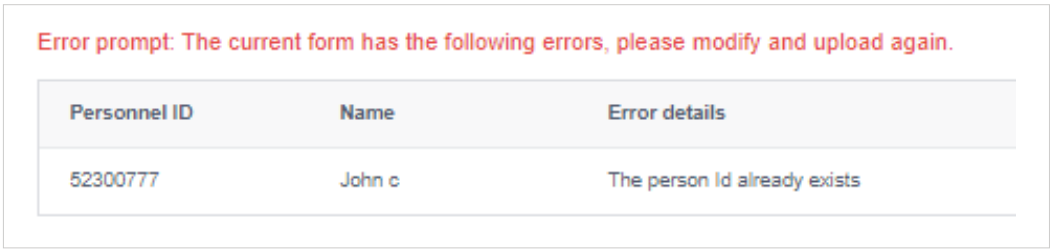
3. In the third step, click “Start import”. During the import, there will be a progress bar showing “Importing personnel information (1 / total number of people)”. After the import is complete, a message “Successful batch import of personnel information” is displayed. You will get two methods of uploading after clicking Start import, details of which are stated below. After that, return to the Employee List to view your imported information.



Types of import methods:



- Uncover Import: This will not overwrite any repeating employee list with changed information, and instead an error message will be prompt for repeated employee individuals, with details of the error stated at the bottom. (An example is given below)



- Overwrite import: The second import will overwrite the information of the employee whose information already exists without showing any duplicate information error.

Import Failures:

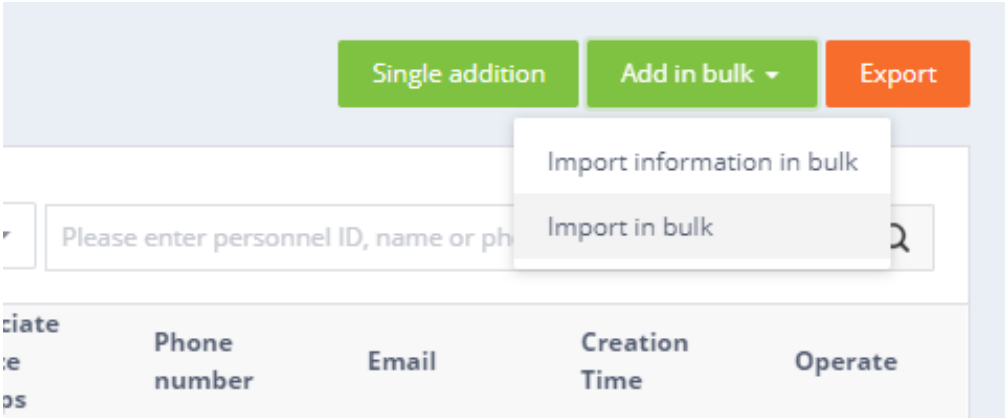
- If the content or format of the uploaded excel file is incorrect and does not meet the template specifications, an error message will appear, with the error specification mentioned for the specific employee. E.g. the employee below has an error on the gender column.

Personnel ID	Name	Error details
1	Test name	Wrong gender input;

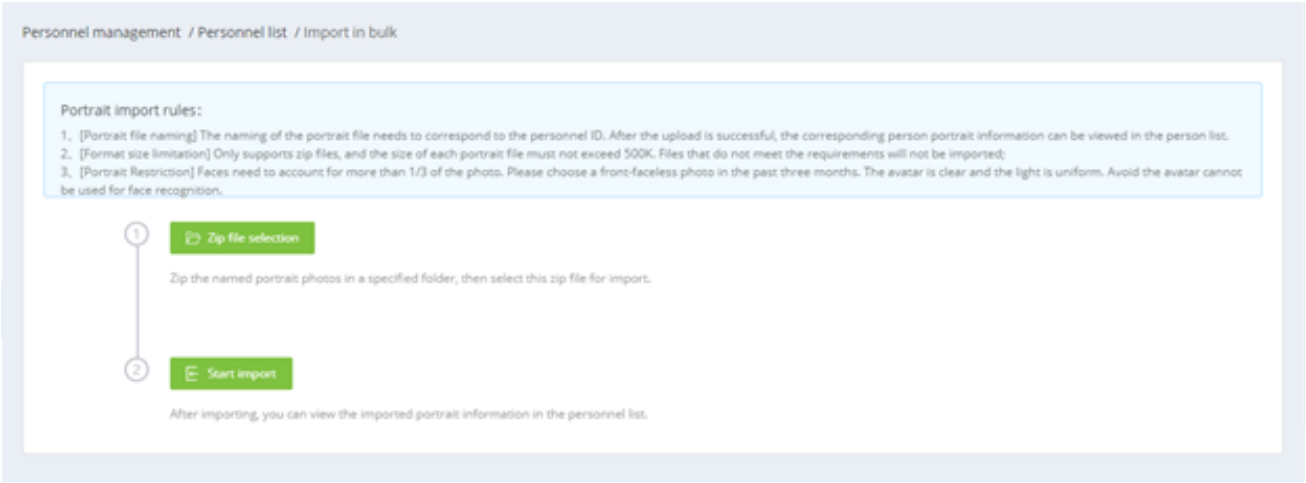
5.1.3. Import portrait photos in bulk

Steps:

In the Employee list, click “Add in bulk - import in bulk”.

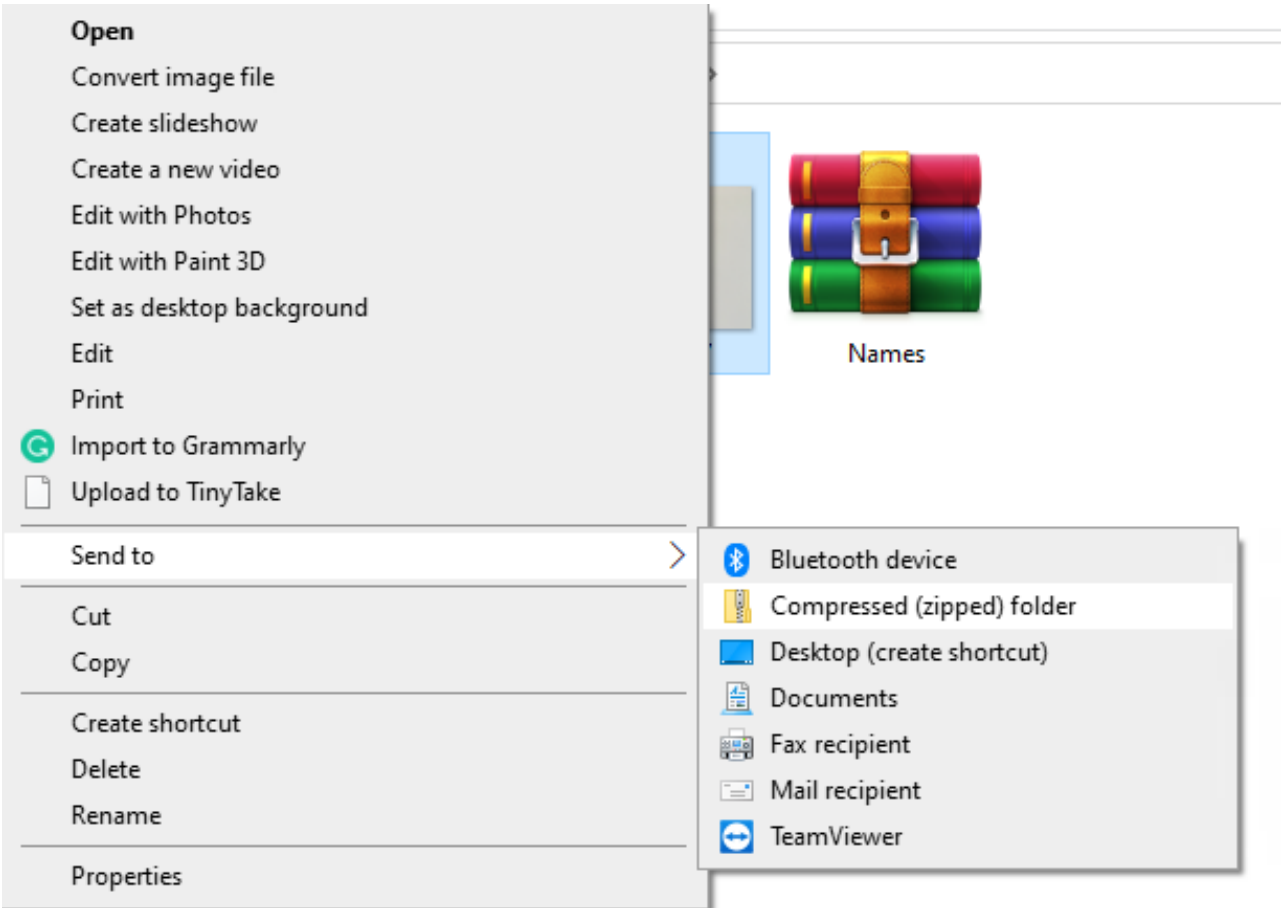


1. Click “Zip file selection” to open a Folder window and select the file which you want to upload (It has to be a compressed folder). After a successful upload, the current file storage path is displayed.
2. Click “Start Import”, and a progress bar will be displayed during the import process: the number of imported files / the total number of folders. And there will be a prompt message after completion: “Import result: x succeeded/ x failed”.



Import Failures:

- Portrait file naming: The name of the portrait file needs to be the same as the personnel ID, so the picture can be linked to the employee.
  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, simply select all pictures, and put them on a compressed folder. An example is shown below on how to



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.

5.1.4. 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. The export would be in excel format.

5.1.5. Refresh employee information

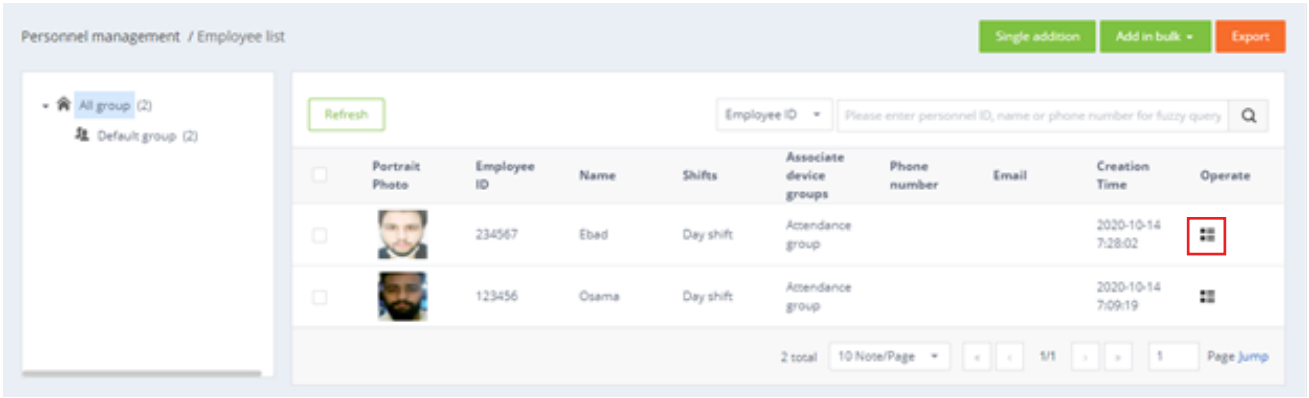
In “Employee List”, click the “Refresh” option to refresh all employee information in the list to their updated state.

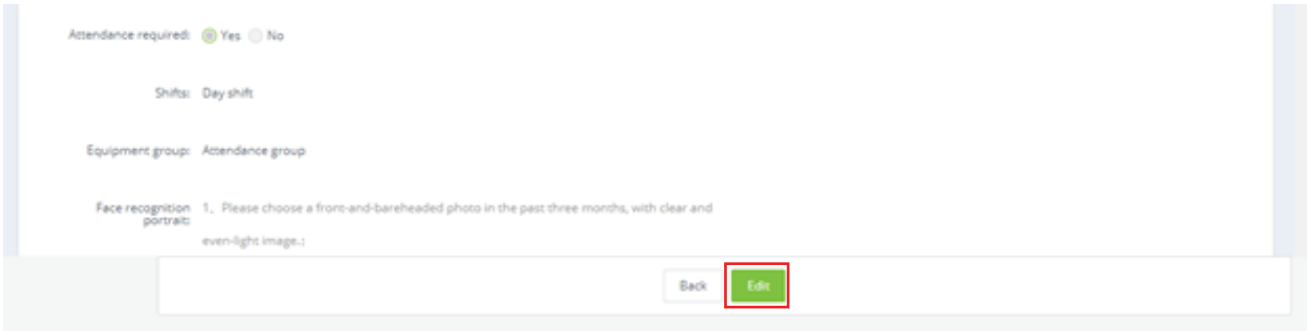
5.1.6. Employee Edit

Employee details

To edit the existing employee information, simply click the symbol under operate, then click on edit at the bottom of the page, and make the edits accordingly.

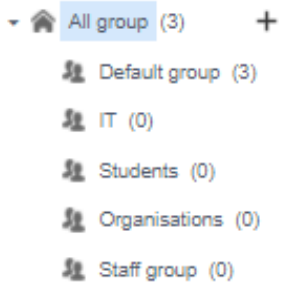
After the changes are made, simply click on save.

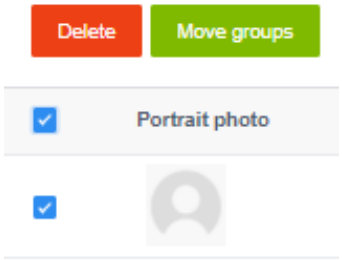




5.1.7. Employee groups management (Delete, Move Group)

You can shift the employees to different groups (If created).
To create an employee group, simply click on the + sign beside “All group”, type in the name of the new group you want to create, and then transfer the employee.





After the employee group is created, select the employee (or lists of employees) you want to transfer, and then move them to the group you want to transfer them.

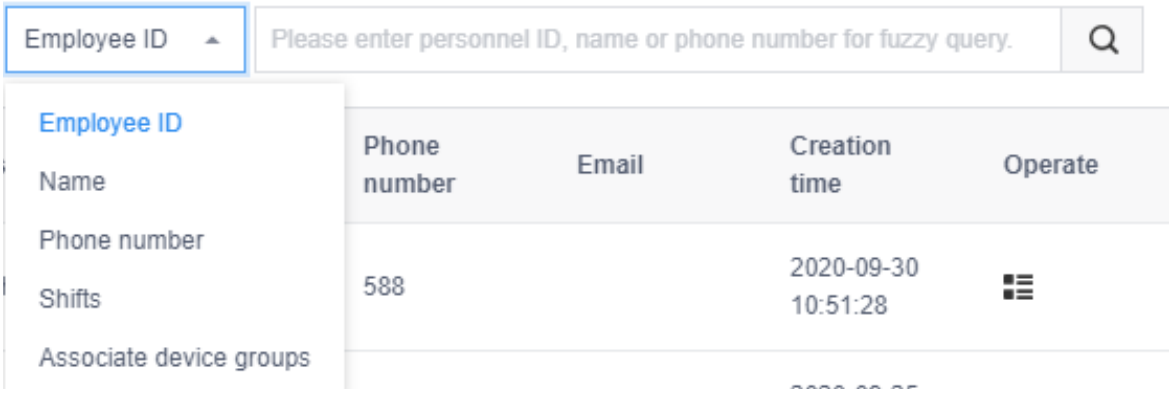
You can delete the employees by selecting them as well.

(Note: To move employees directly into a pre-existing group during bulk information upload, simply select the relevant group under the belonging group. For example, if instead of default group, I want to move an employee to IT group, below information would have to be filled in that case

Personnel ID	Name	Gender	Belonging group	Phone number
52300777	John c	Male	All group- IT	+8613412345678

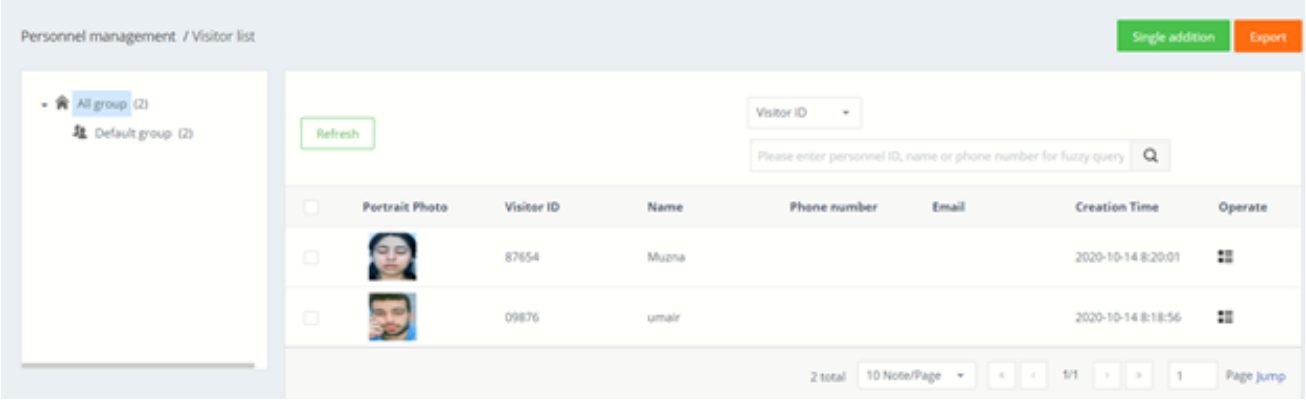
5.1.8. Employee Search

To search for an employee, simply select the Employee ID bar, and choose what you want to search by (Name, Employee ID etc.), input the information you want to search on the search bar, and then click on the Search button (Magnifying glass).



5.2. Visitor management

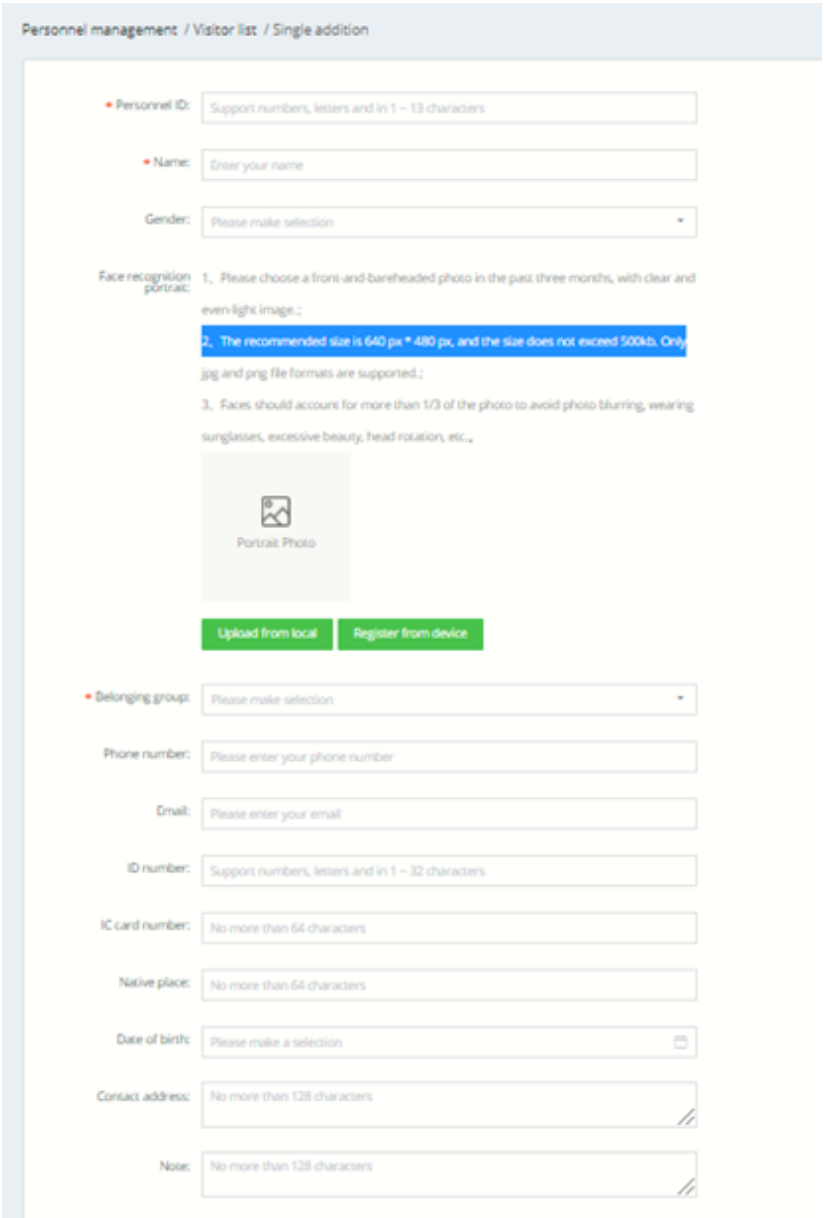
Visitor management is used to view, add, edit, and export visitor information.



5.2.1. Add visitors individually

Steps

1. In Visitor Management, click on “Single Addition” 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:

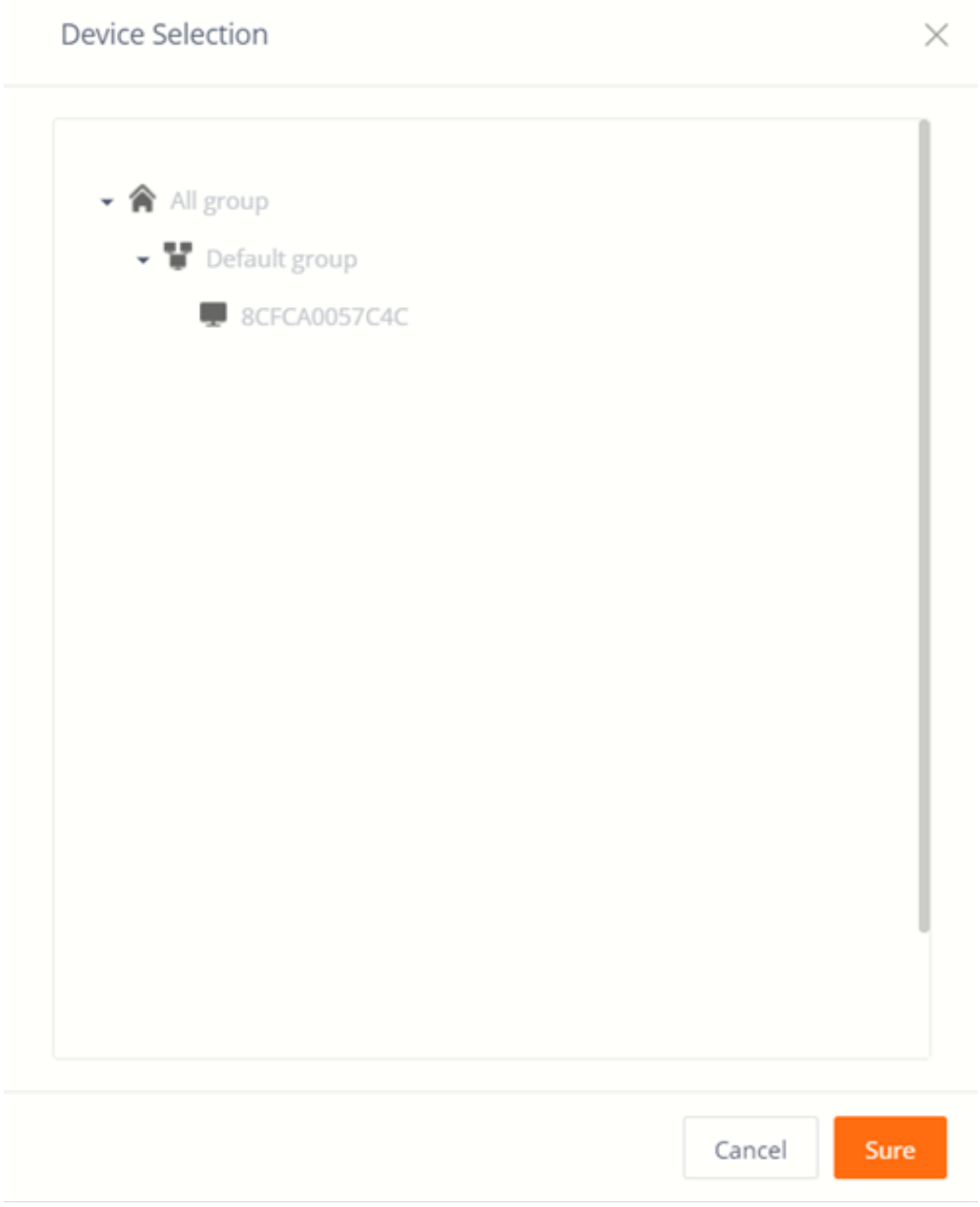
- Upload from local disk
  Click “Upload from local” to upload a picture from your system. Simply select a jpg or png portrait, and upload it.

  Note: Portrait photo specifications

1. Please choose a front-and-bareheaded photo from the past three months, with a 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, sun- glasses, excessive facial-up, and head rotations.

Register from device

Click “Register from Device” to select a device from which you want to capture the image.



Simply stand in front of the device after clicking confirm, and the device will capture your picture. Once the picture is verified (you can click on register from device again to retake the picture), simply click save and the picture will be stored in the database.

5.2.2. Export visitor's information

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

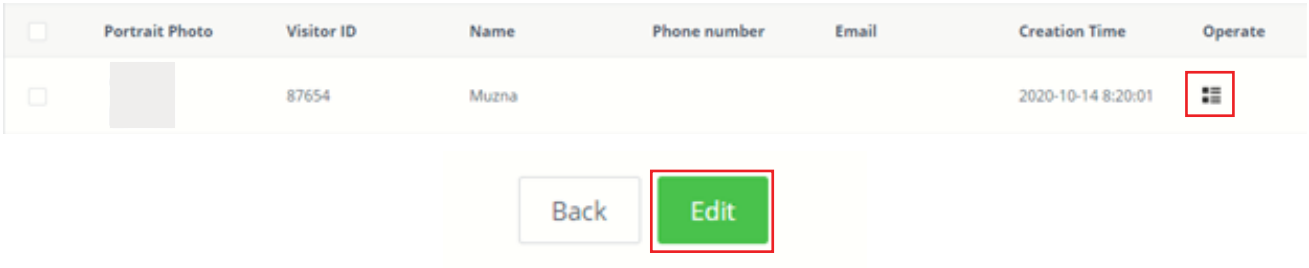
5.2.3. Refresh visitor's information

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

5.2.4. Visitor Edit

To edit the existing Visitor information, simply click the symbol under operate, then click on edit at the bottom of the page, and make the edits accordingly.

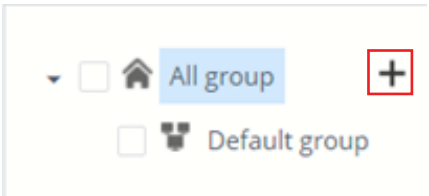
After the changes are made, simply click on save.



5.2.5. Visitor groups management

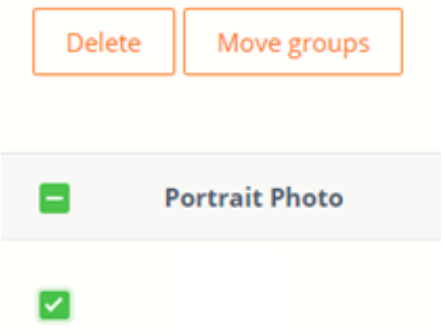
You can shift visitors to different groups (If created).

To create a visitor group, simply click on the + sign besides All group, type in the name of the new group you want to create, and then transfer the visitor.



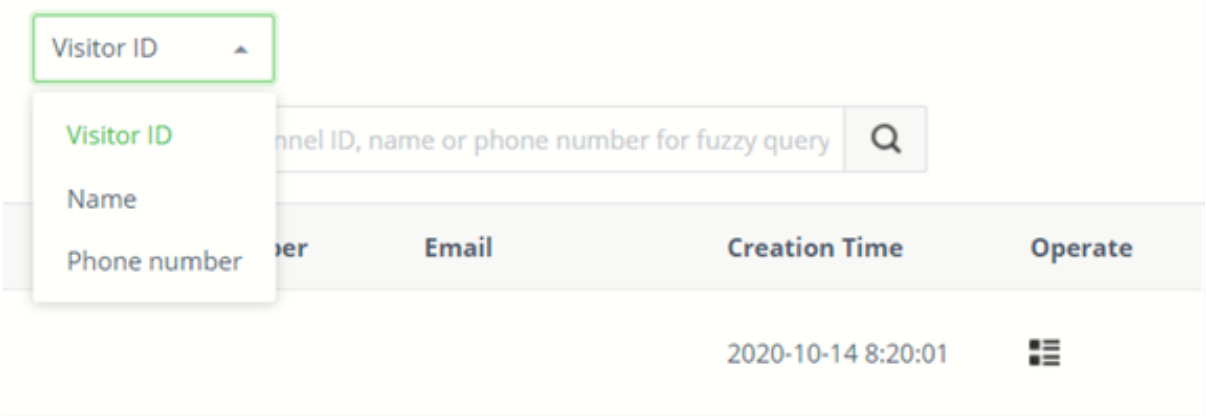
After a visitor group is created, select the visitor (or lists of visitors) you want to transfer, and then move them to the group you want to transfer them.

You can delete the visitors by selecting them as well.



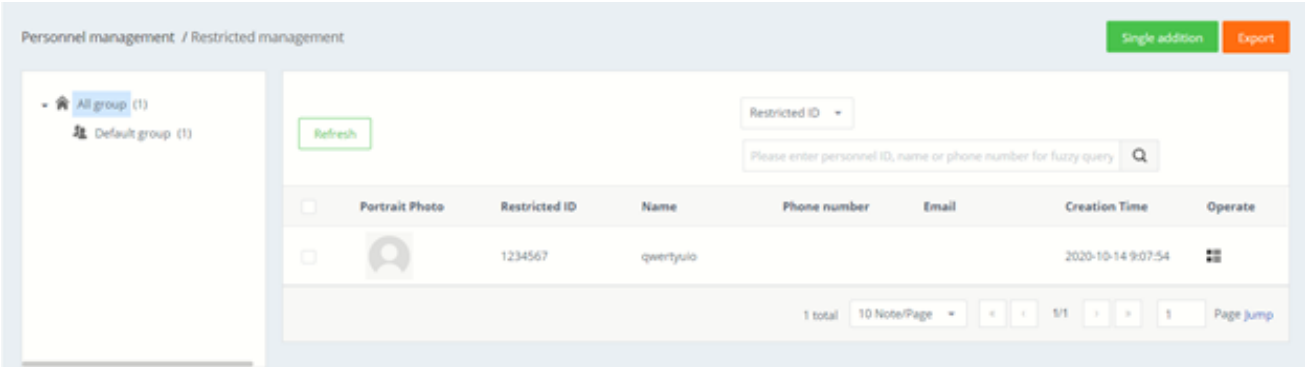
5.2.6. Visitor Search

To search for a visitor, simply select the Visitor ID bar, and choose what you want to search by (Name, Visitor ID etc.), input the information you want to search on the search bar, and then click on the Search button (Magnifying glass).



5.3. Restricted management

Restricted management is used to view, add, edit, and export restricted individuals' information.



5.3.1. Add restricted person individually

Steps:

1. In Restricted management, click on "Single Add" option to enter the restricted addition page.
2. Fill in the restricted 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.

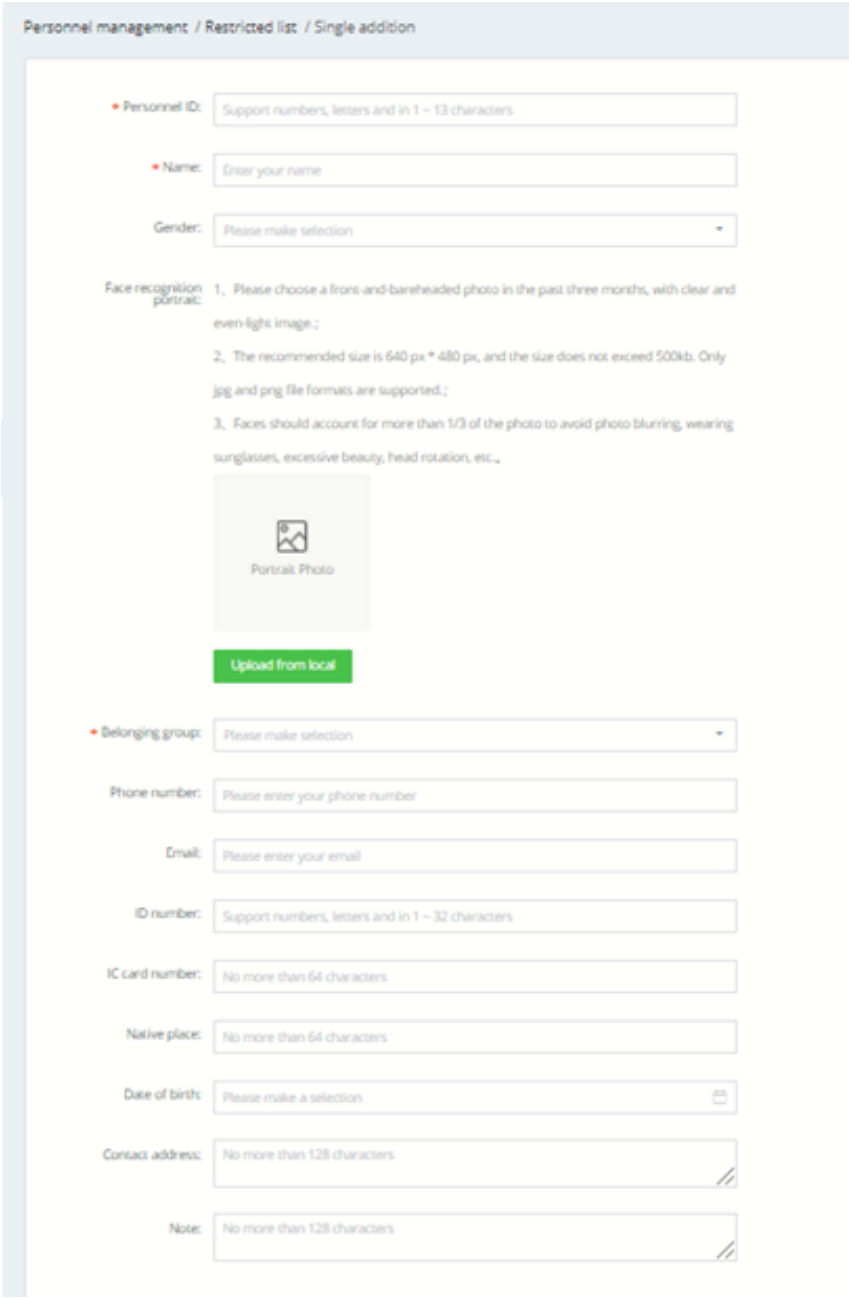
Uploading a picture for facial recognition for restricted management

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 sun- glasses, excessive facial-up, and head rotations.



5.3.2. Export restricted management list

In Restricted management, click on “Export” option to export all the restricted information from the list to the file “Blacklist_information” and download it.

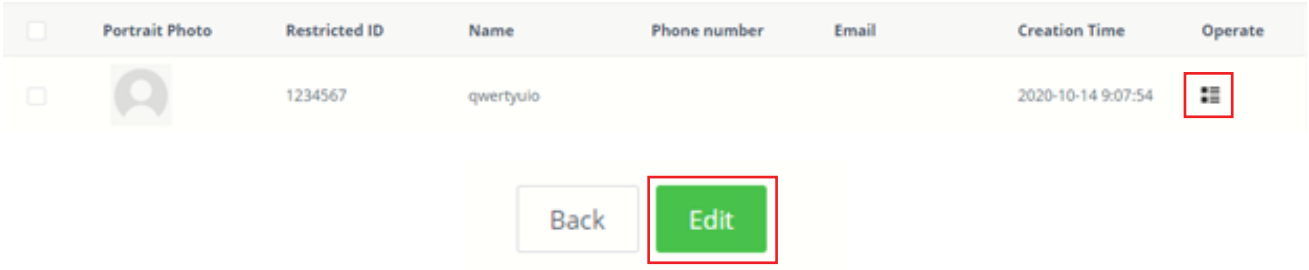
5.3.3. Refresh restricted management information

In Restricted management, click on “Refresh” option to refresh all the restricted information in the list to their updated state.

5.3.4. Restricted management Edit

To edit the existing restricted individual information, simply click the symbol under operate, then click on edit at the bottom of the page, and make the edits accordingly.

After the changes are made, simply click on save.



5.3.5. Restricted groups management

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

6. Pass Management

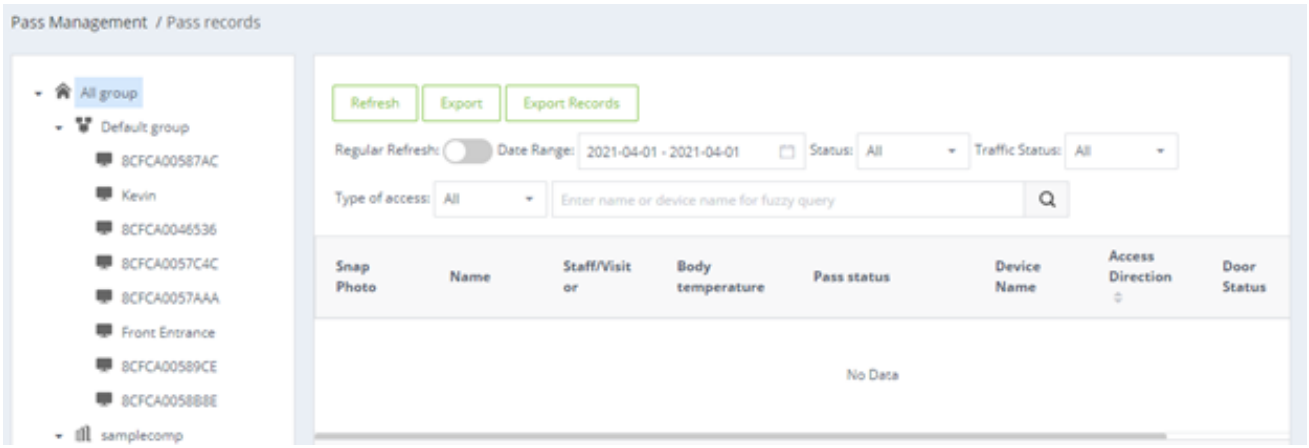
6.1. Pass records

Pass records allows the user to see complete history of the individuals that have been scanned by the device. The pass records dashboard also allows the user to monitor the status of the individual that has been scanned by the device, including the temperature of the individual, access type etc.

The pass records dashboard also gives the functionality of exporting records from the dashboard onto your system in a .CSV format, or see a record of all the exports made.

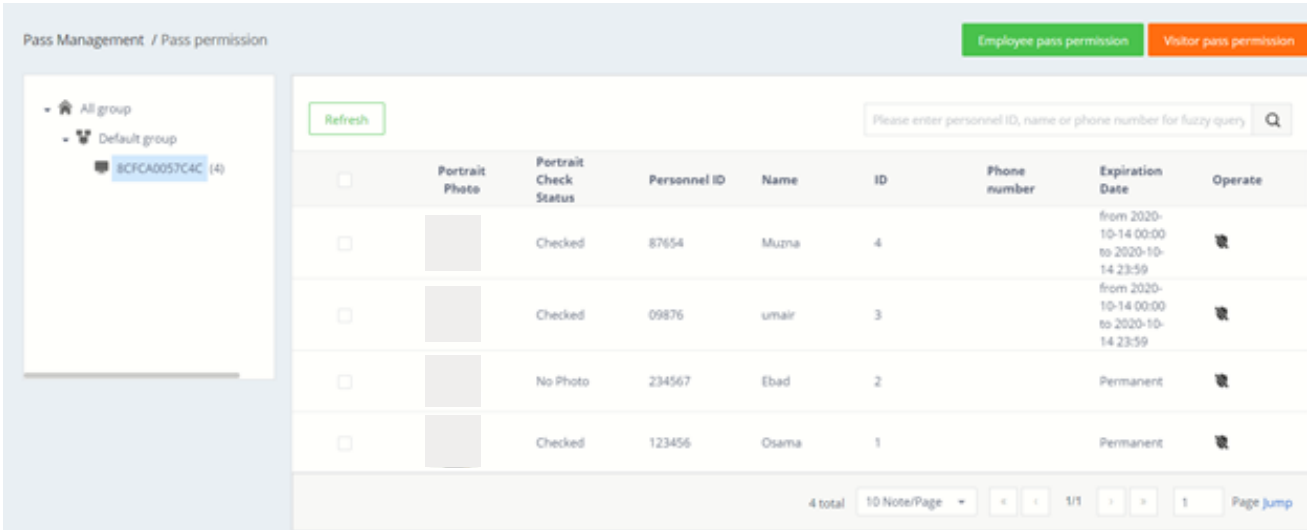
You can search for a specified date period on the date range, or search for a specific employee on the employee search.

You can also enable regular refresh, at which the management software will refresh itself every 6 seconds.



6.2. Pass permission

Pass permission allows the user to provide different levels of access to employees and visitors alike.



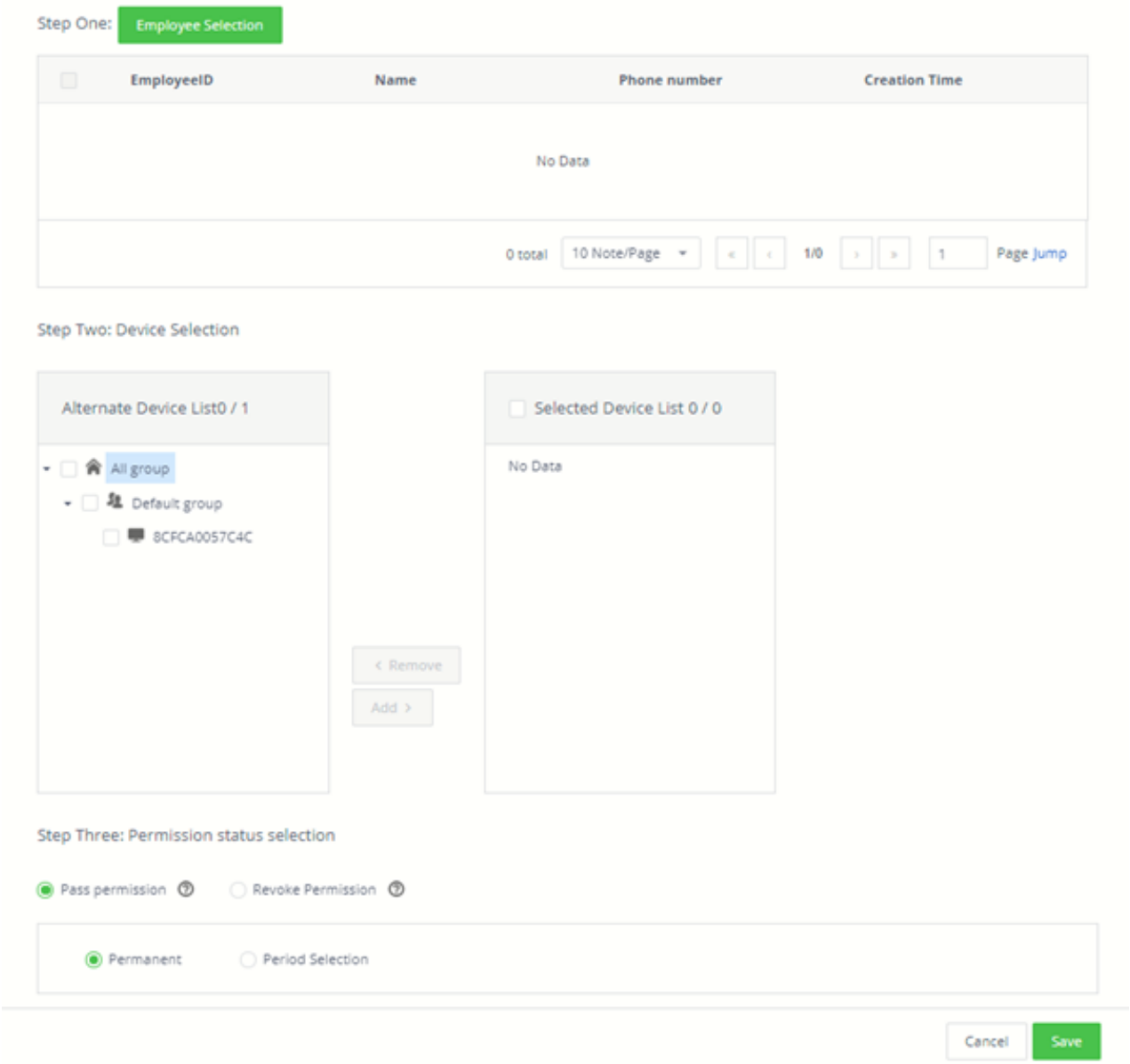
6.2.1. Employee pass permission settings

Manage the access rights of added employees and visitors.

Pass permission:

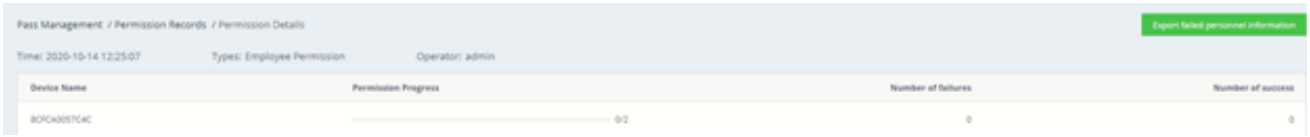
1. Select personnel, devices, pass permission, permanent effective time and click “Save” option to start pass permission. After successful authorization, the person can pass the gate and the validity period is permanent.
2. Select personnel, devices, pass permission, temporary effective time, and click “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.

   You can either allow permanent pass, temporary pass (and select a corresponding time frame), or revoke, which would delete the employee entry of that individual, and not let it pass.



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.



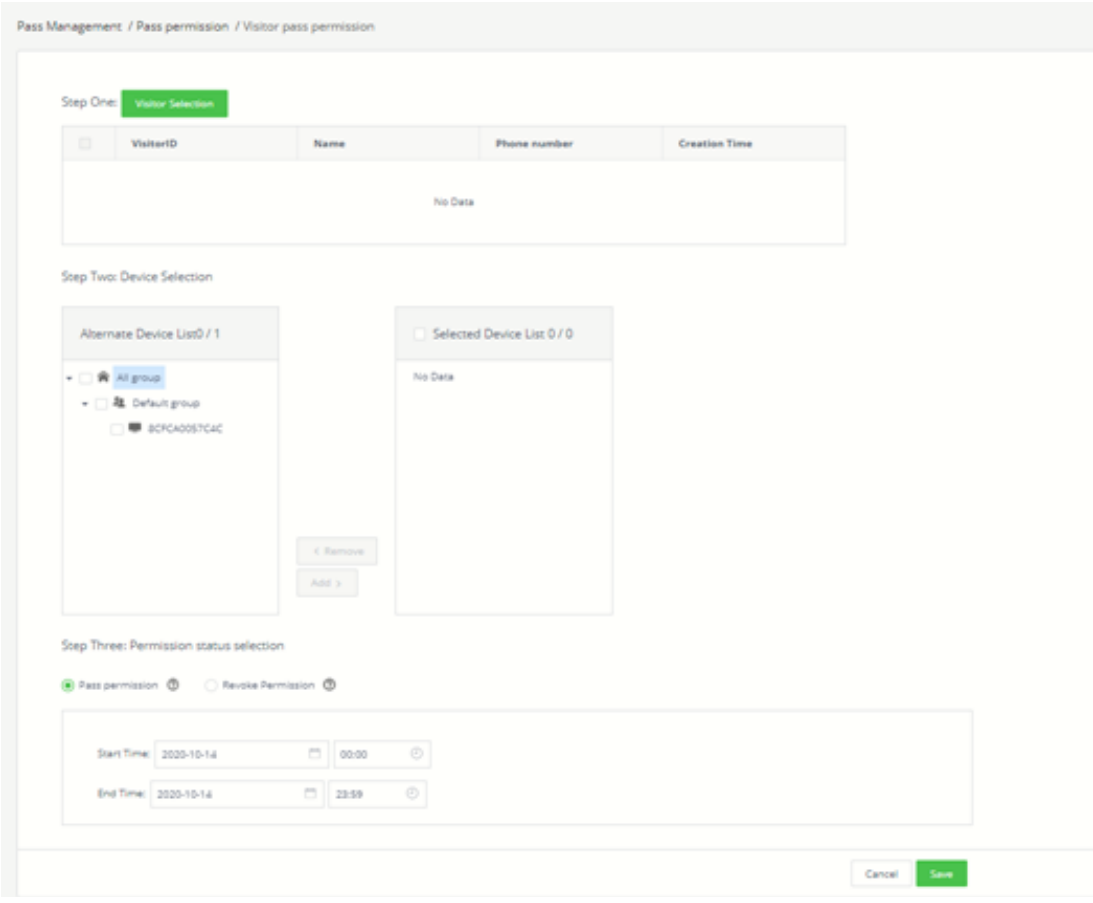
Revoke pass permission:

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 re- moved from the selected device.

6.2.2. Visitor pass permission settings

Steps: On the Pass permission page, click on “Visitor pass permission” option

The pass permission will ask you to specify a time frame during which the visitor can be allowed entry.



Details of Pass Permission:

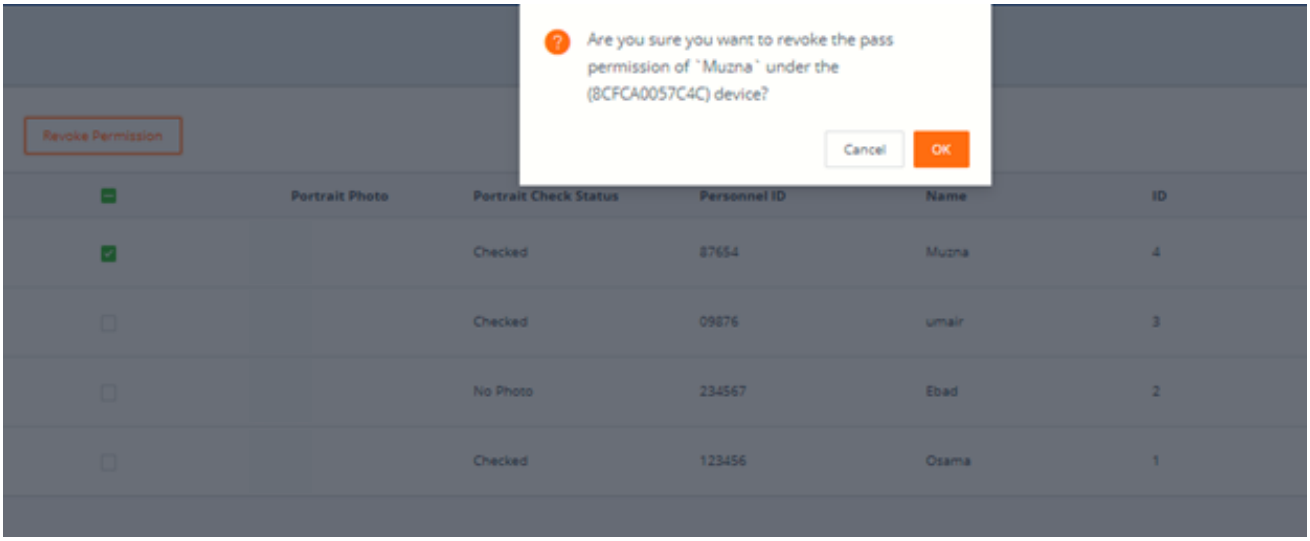
- Click Save to start pass permission. You can see the current synchronization status of each device in the form of a list showing the device name, synchronization pass permission, number of successful and failed authorizations. The person who failed authorization is recorded in the “Verification Failure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

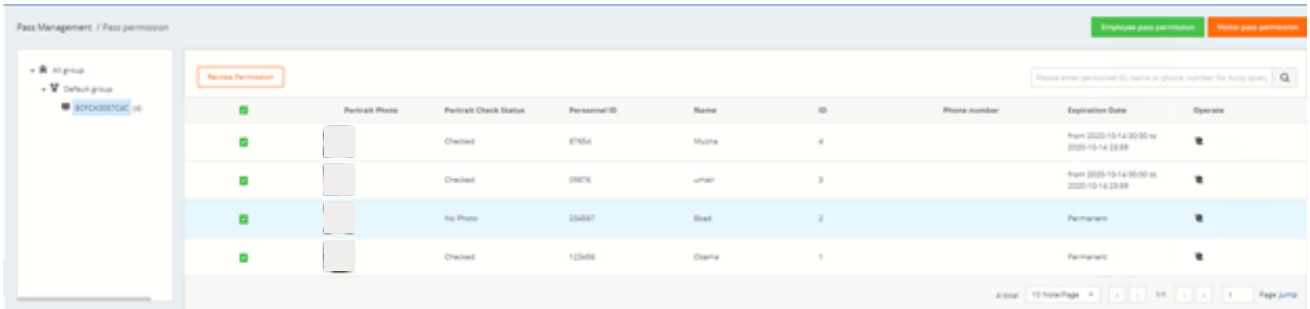
Revoke pass permission

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

6.2.3. 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.





6.2.4. Refresh permission information

On the Pass permission page, click “Refresh” to refresh all authorized information in the list.

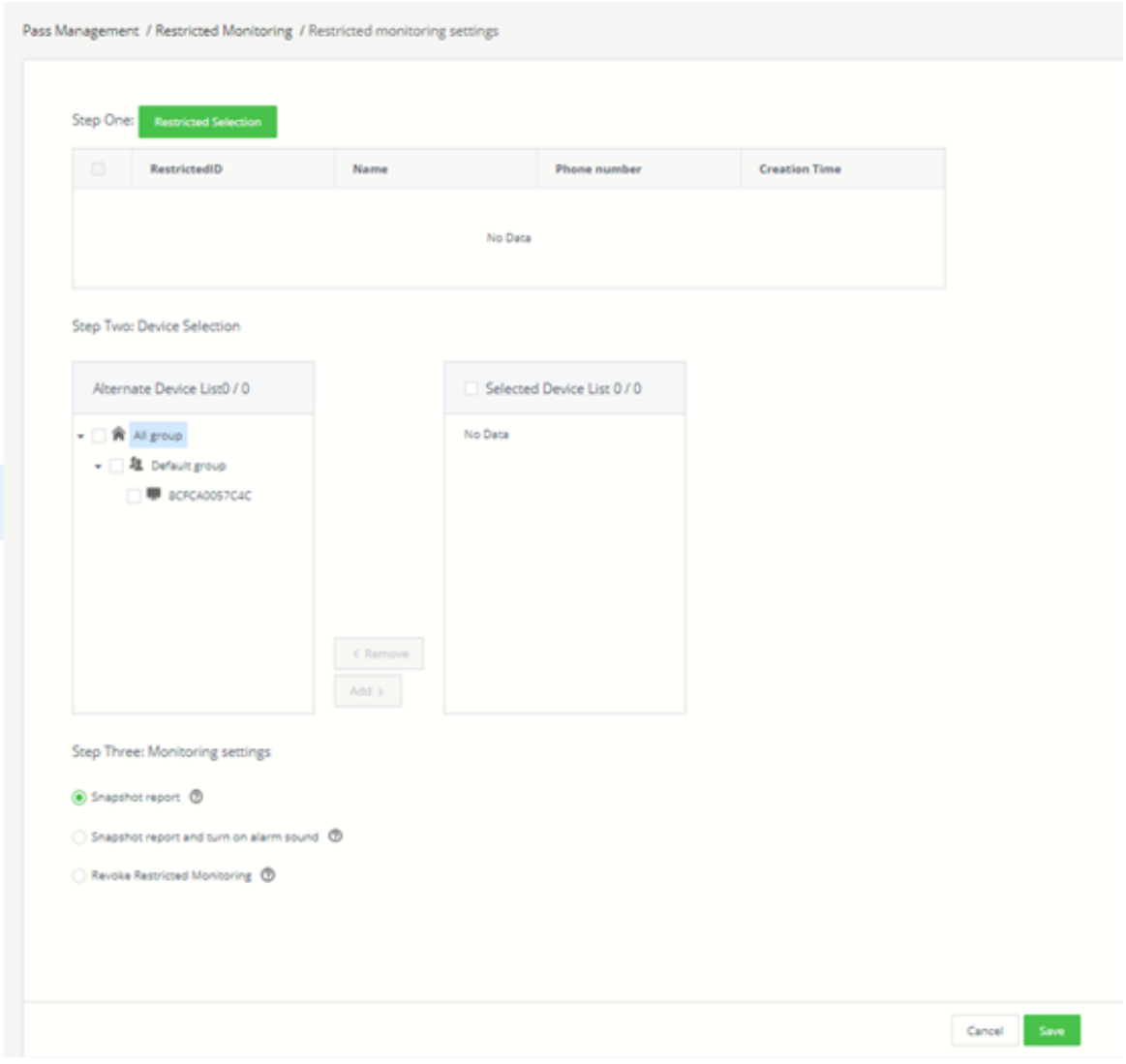
6.3. Restricted Monitoring

6.3.1. Restricted monitoring settings

Steps: Enter the Restricted monitoring page and click “Restricted monitoring settings”

Restricted monitoring settings

1. Select the restricted individual and the device. Click “Save” to start restricted monitoring. When the device is in monitoring mode, the restricted person will be recognized and reported while passing through the gate.
2. Choose between snapshot and snapshot + sound alarm.
3. Snapshot will only take a picture of the restricted individual.
4. Snapshot + sound alarm will take a picture of the restricted individual, and sound an alarm.
5. You can revoke restricted monitoring, and the person will not be restricted by the device.

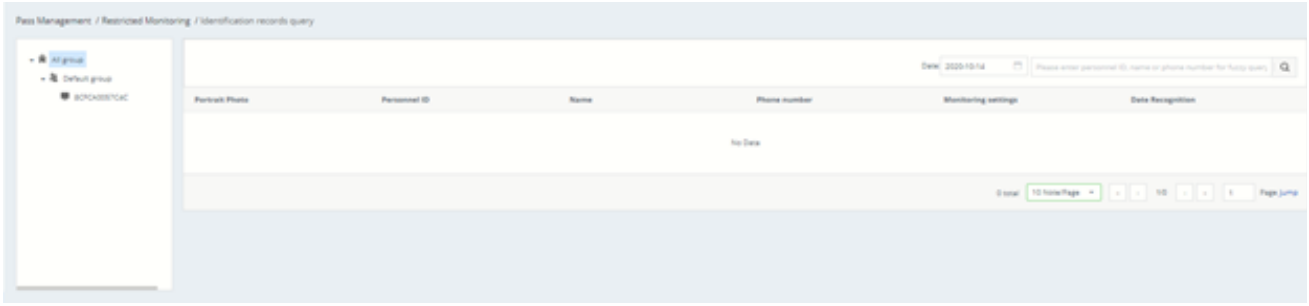


Details of Pass permission:

- Click Confirm to start restricted 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 Restricted Monitoring Failure Information” table. You can click “export table” to view the monitoring failure information.
- If a failure has occurred while monitoring the restricted personnel, the corresponding failure reason can be fixed in the settings and the device can then continue to monitor.
- Revoke restricted monitoring
  Select the restricted individual and the device. Now, select “revoke restricted monitoring”. Click “Save” to start the release.

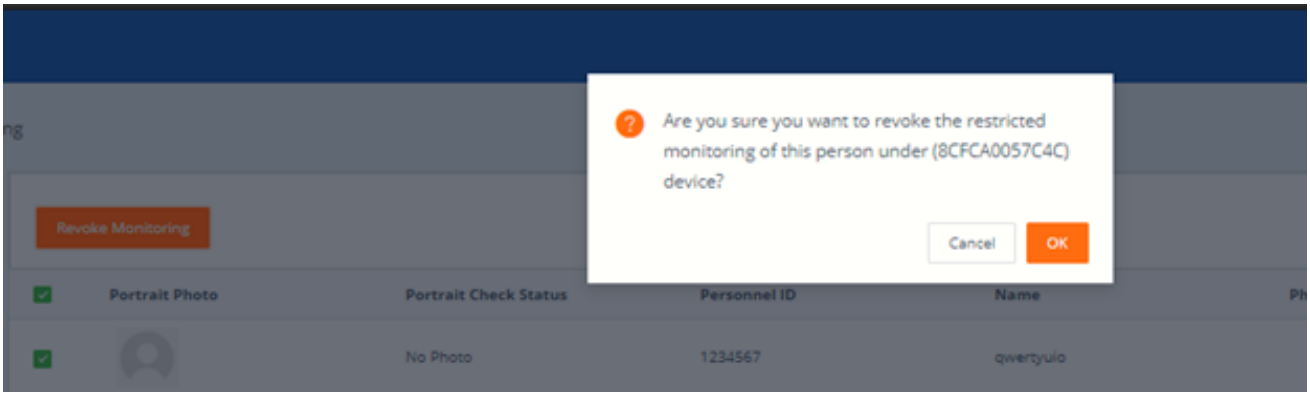
6.3.2. Identification records

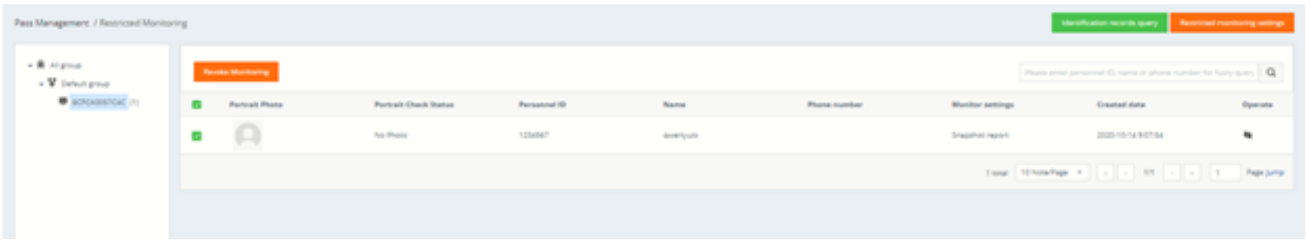
Enter the Restricted monitoring page, click “Identify Record Query” to enter the Identify record inquiry page, and display the identification records of all restricted personnel. Restricted identification records can be selected according to grouping, device, and date range inquiries.



6.3.3. Remove monitoring

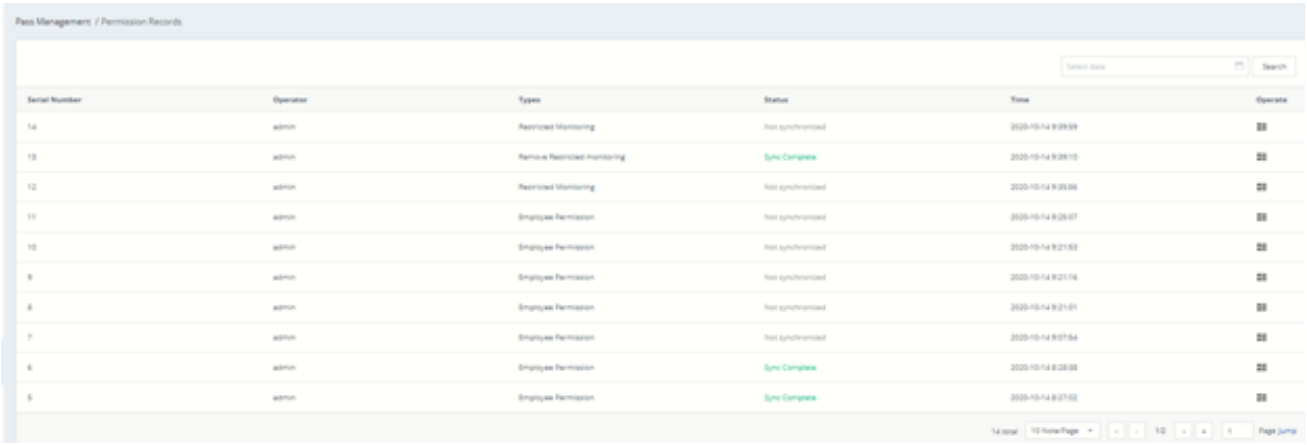
In the Restricted monitoring personnel list, click “remove monitoring” behind the list record to re- lease monitoring. After the removal is successful, the restricted monitoring removes snapshot monitoring or alarm from the selected device. You can also check “personnel record” and click “remove monitoring” to perform batch operations.



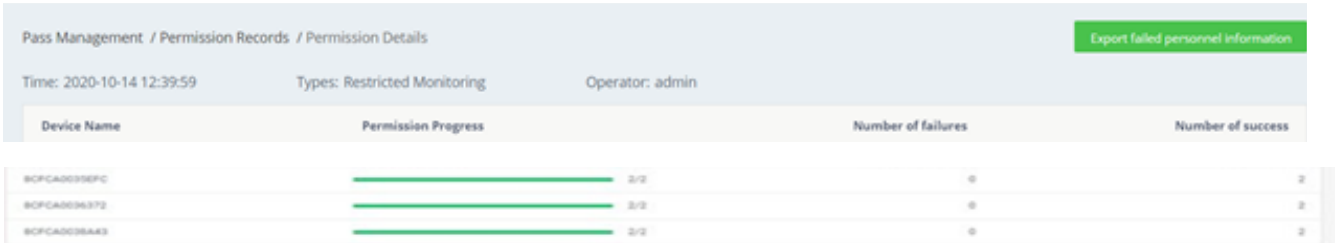


6.4. Permission records

Permission Records: The module contains information records of the “Permission” and “Remove permission” of employees, visitors, as well as the restricted monitoring and contact monitoring setting operations. You can enter the list to view details of the related records, and verify if the action was synched onto the GoSafe units, or not.



Permission details are as follows, once you click on the logo under operate.

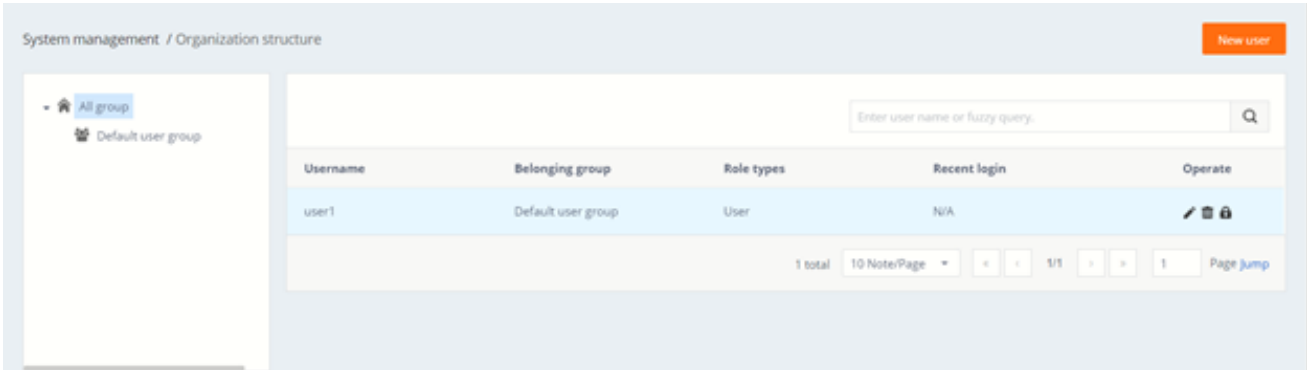


7. System Management

7.1. Organization structure

Organization structure: Initially, a new role has to be created, and organization structure allows you to create a new user to whom a new role can be assigned. The hierarchical relationship is created and managed by an admin or enterprise administrator.

The user will only be given access to the role defined to it.

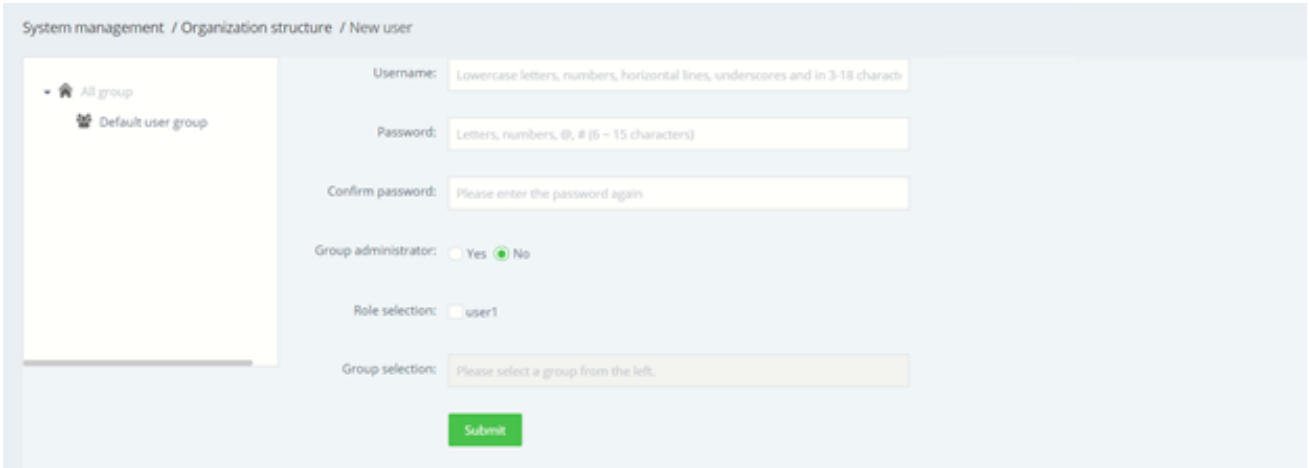


Device grouping can be done, and organization with the new assigned roles can be applied to specific devices in those groups.

7.1.1. New User

Create new users by clicking on the 'New User' icon, and fill in the information (Username, password, confirm password, group administrator, role selection).

Note: A role has to be made first before assigning it.



Simply fill in the specified credentials, select the user group for which you want to create this account (linked with a role), and click submit to create an account.

7.1.2. Search organization structure

You can search a specific organization structure created on the search bar.

7.1.3. Organization Structure – Operate

This will give you information of the organization structure created, and allow you to edit or delete the account. User password modification: Note that only administrators (admin or company administrators) can reset passwords for users in the group.

7.2. Role Management

Role management allows you to create different roles, assign authority permission to that role, and this role is then linked to a user account created in the organization structure.

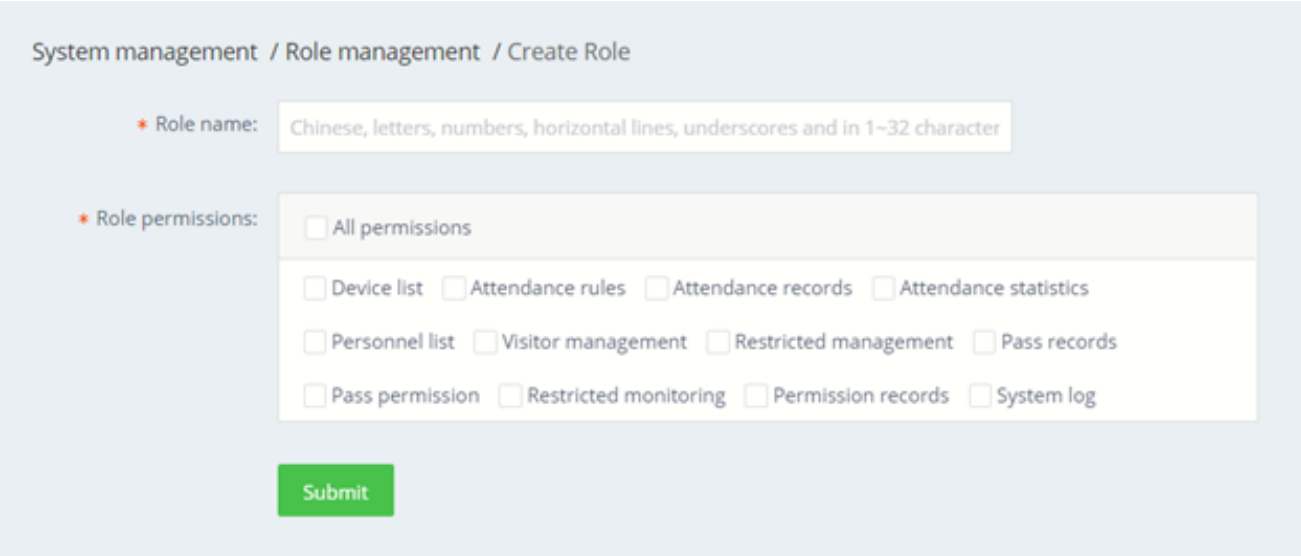
Description of roles

- 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.

Role creation

- Go to [System Management]-[Role Management], click “New Role ‘’ to enter the “New Role” page.

  Simply Write the name of the Role that has to be created, and the level of permission (Authorization) you want to permit that specific role.

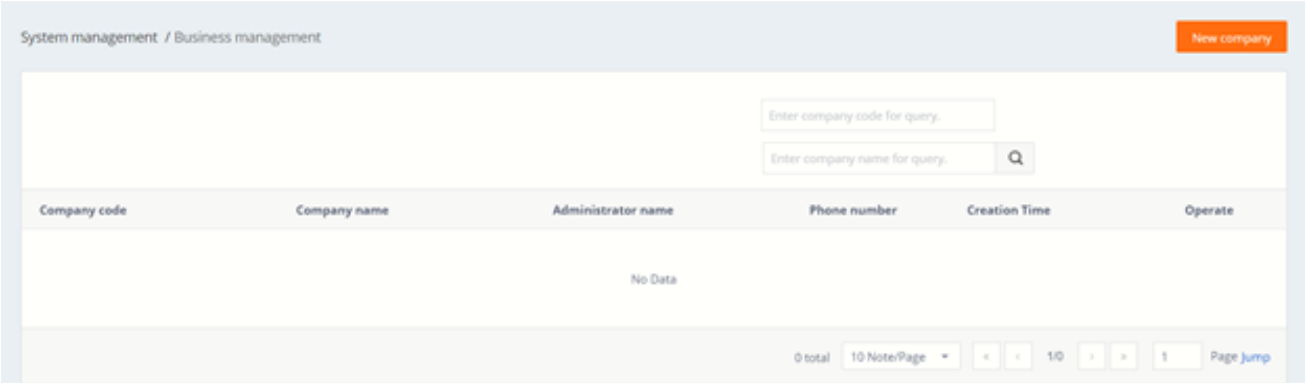


7.3. Business Management

Business Management:

This module can only be operated by the super administrator and is used to create and manage company accounts in the system. Each company 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 company, and can view, manage all business data created by the business management users. However, there is no operation authority for the [System Settings] and [Business management] functions, and you cannot see the data of other enterprise users.

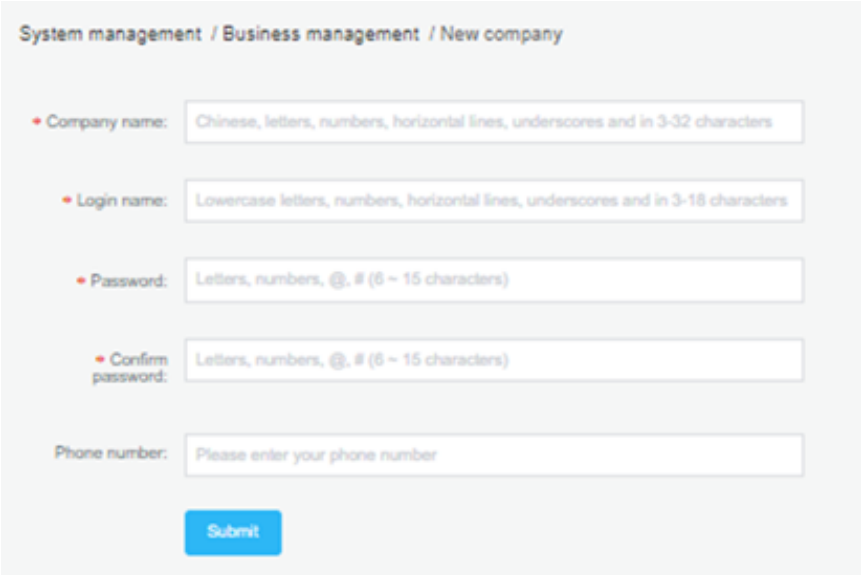
Essentially you link devices to the company created in business management.
Super administrators can create, modify, query, and delete enterprises. This is shown in the following figure:



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

7.3.1 New Company

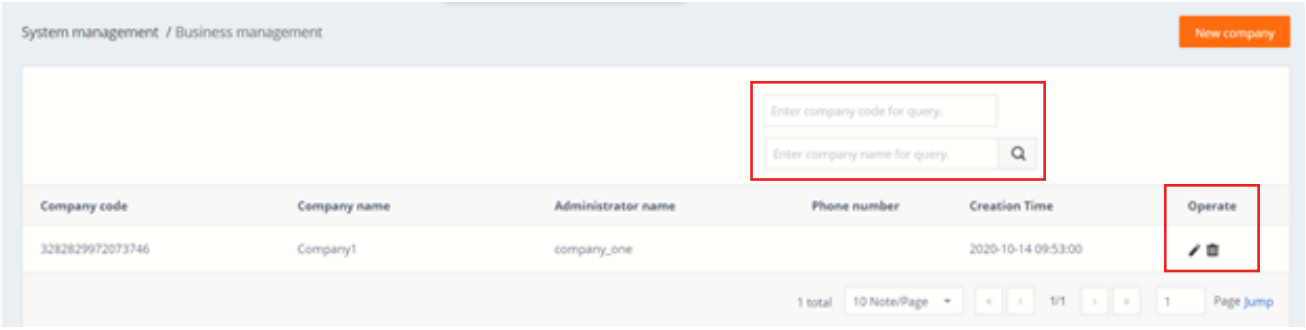
Create a new company, and assign them a new ID. Below are the information about adding a new company
Super administrators can create, modify, query, and delete enterprises. This is shown in the following figure:



7.3.2 Search / Edit / Delete

You can search for a specific company created (by their company code or company name) in the search options available.

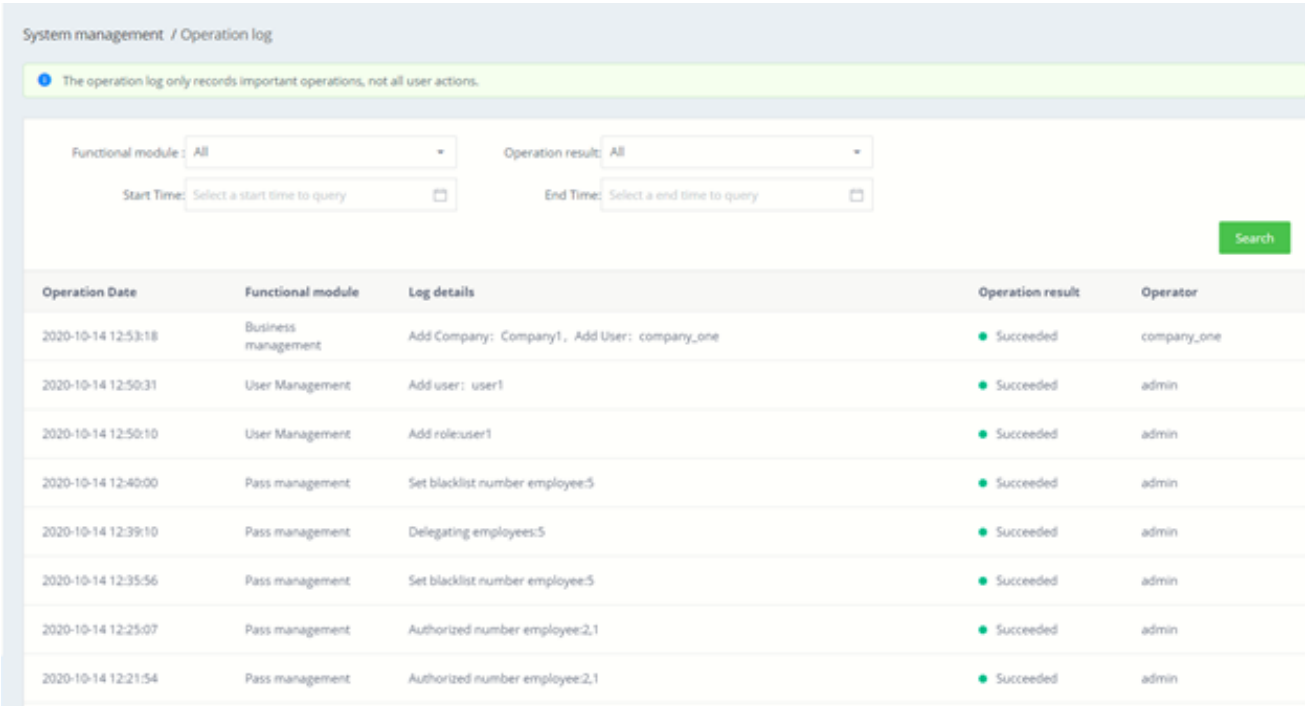
To edit or delete a company created, simply click on the options under operate.



7.4. 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.



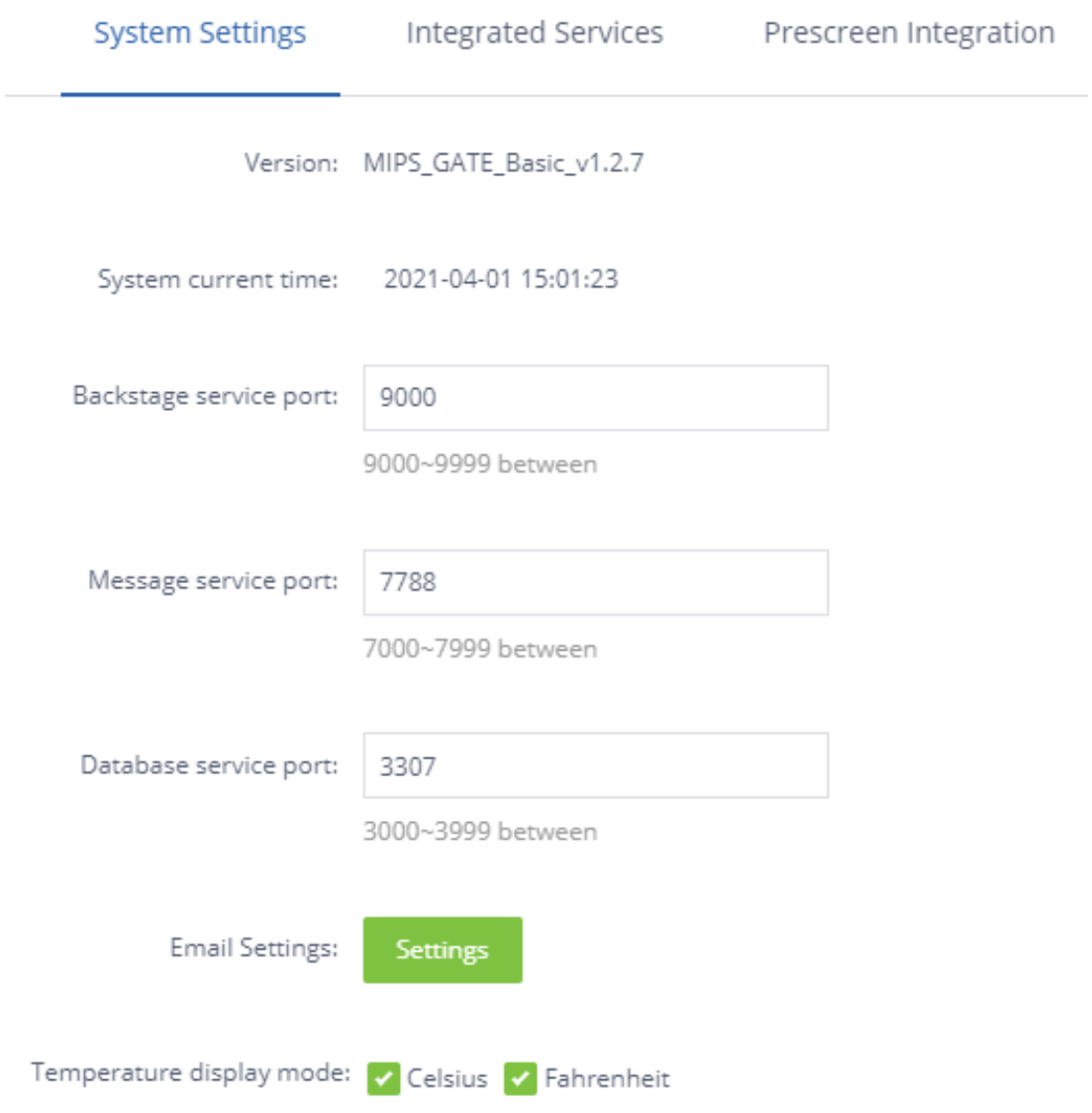
7.5. System Settings

7.5.1 System Settings

The system settings provide functions such as “background server port”, “message service port” and “database service port configuration”. It also allows you to configure your email address for notification of high temperature scans.

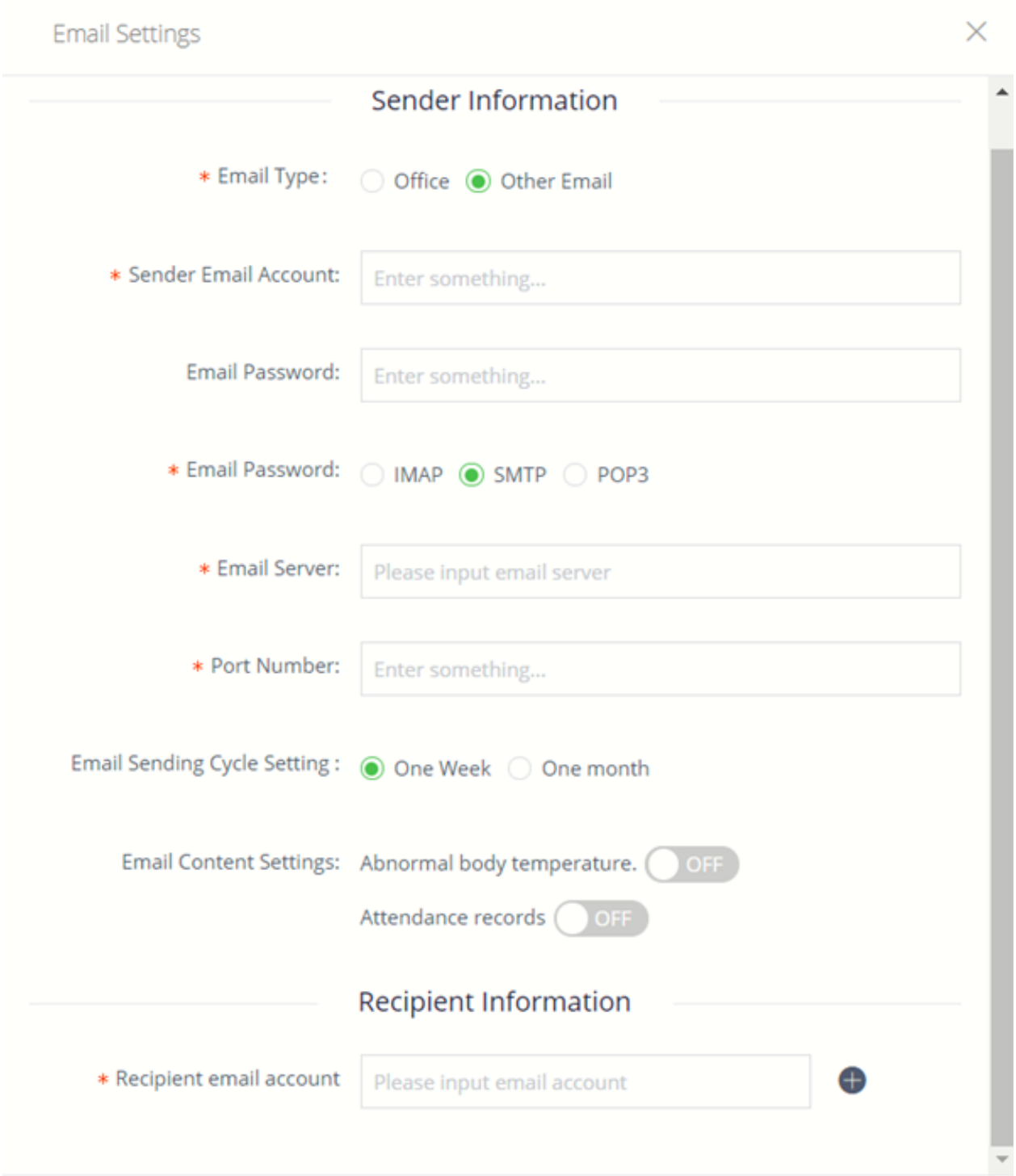
You can also select whether you want records to be generated in C , F or both.

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.



7.5.1.1 Email Settings

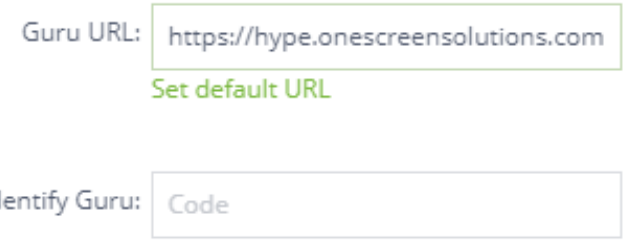
Email setting allows you to send emails to selected individuals, for attendance and body temperature.



Select Email office for local server, other email for public server.

How to Configure Email settings

Please click here for the document on how to configure the email settings.
You can set your own office reception to be connected whenever a user says “Call Guru” or “Call Help” from the device. Please contact the Guru team to get your Identify Guru Code.



System settings also contain important settings for managing facial recognition, mask detection and mask detection etc. on the console. These settings apply to the console interface and not on your standalone devices.

Face Detection Settings

Face Detection is used for facial recognition of individuals added through the Prescreen application. This option can be enabled or disabled, as per end user requirement.

System settings also contain important settings for managing facial recognition, mask detection and mask detection etc. on the console. These settings apply to the console interface and not on your standalone devices.

Face Recognition Settings

You can set whether you want the console to scan for faces and compare faces with the database for a match and store a record on the console or not. This setting is exclusive to the console and will not affect the settings on your device which can be changed from body temperature settings. In this case, facial recognition is being done by the console’s AI compared to the device’s AI. Please make sure to delete all employee lists on the physical device to ensure proper usage of the console’s AI facial recognition.

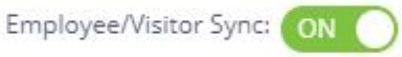
(Please note, to enable facial recognition on the console’s AI, perform an application initialization on the device, and turn on stranger mode + stranger record)

Mask Detection

Mask detection can be enabled or disabled depending upon whether you wish to grant admittance based on the presence of a mask. This will store a record for whether the visitor was wearing a mask or not and grant access accordingly within the console but will not affect the setting on the physical device which can be changed from body temperature settings.

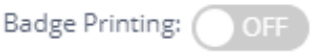
Employee/Visitor Sync

Employee/Visitor sync is used to share the database if visitors and employees on the console with the device. Any employee/visitor created while the setting is on will be copied to the device. You can view the sync status of a user from “permission records” once a user is created. To use the facial recognition AI of the console only, please ensure to turn sync off while uploading the employee list (Console has to be restarted after changing sync settings).



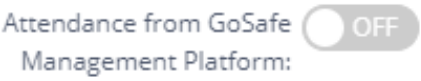
Badge Printing

Enabling Badge Printing allows the Brother label printers to sync with the employee data base on the management console, and print the labels on the basis of the database.



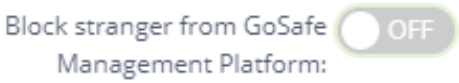
Attendance from GoSafe Management Platform

Allows the relay connection (if any connection was made) to be controlled from the management console instead of the device (Please perform an application Initialization on the device when changing this setting)



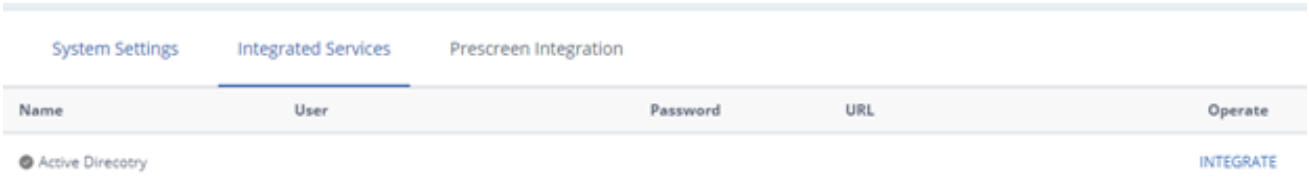
Block Stranger from GoSafe Management Platform

Enabling this setting would deny access to strangers on the management console. (Please make sure that the Attendance from GoSafe Management Platform is also on to enable this setting)



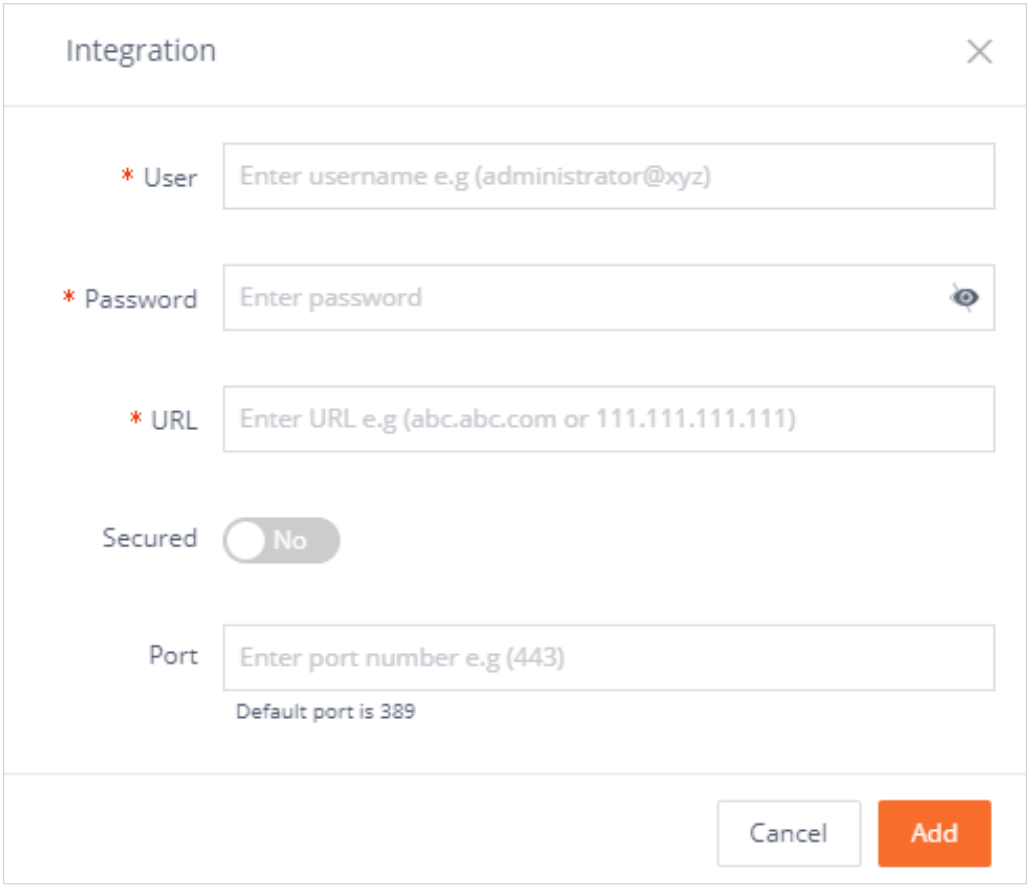
7.5.2 Integrated Services

You can choose to import your employee list from an Active Directory



7.5.2.1 Integrate

Simply fill in the required information, with the relevant credentials



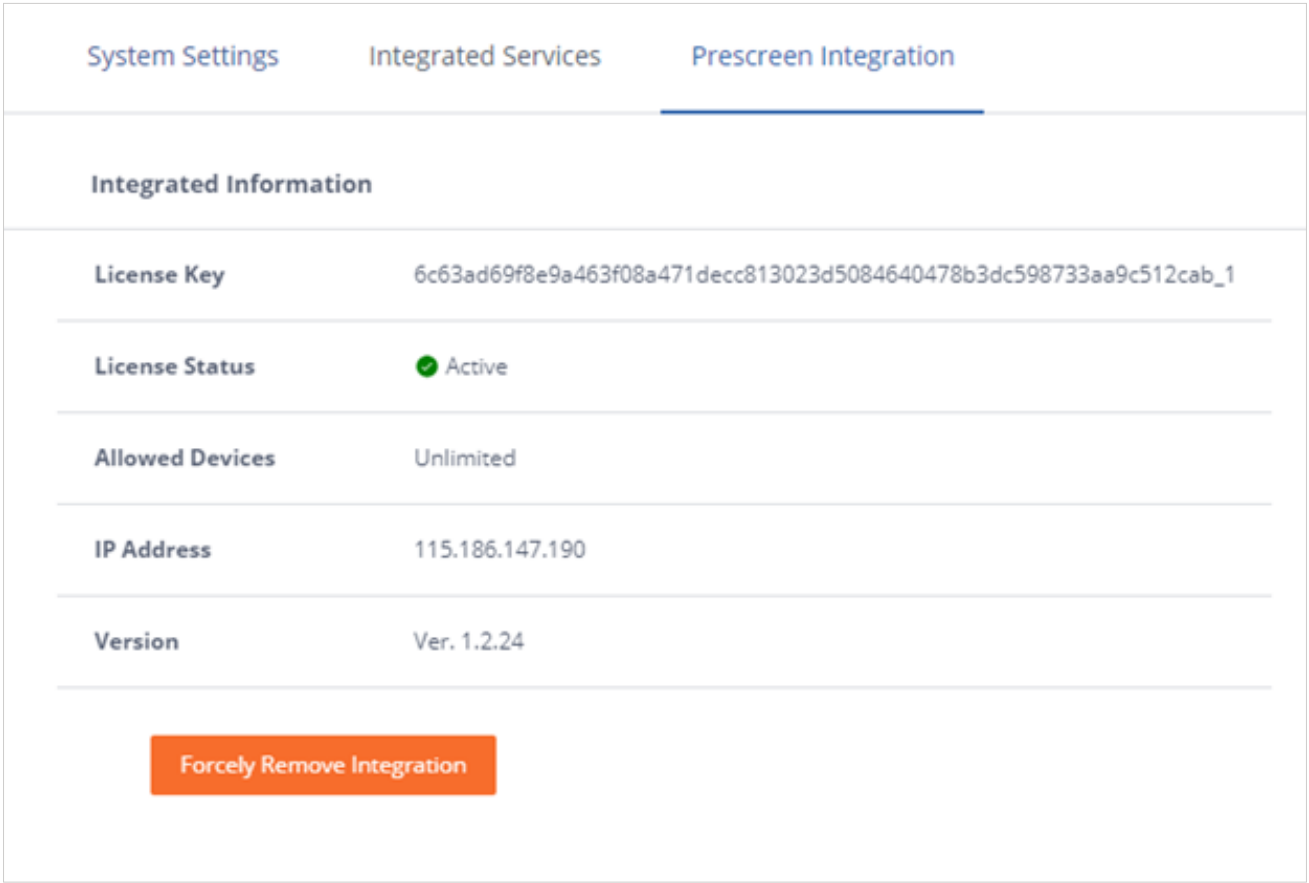
7.5.3 Prescreen Integration

This gives information whether your Pre-Screen has been integrated with the management software, and how many active devices have been currently enabled for the Prescreen

7.5.3 Prescreen Integration

This gives information whether your Pre-Screen has been integrated with the management software, and how many active devices have been currently enabled for the Prescreen

- **License Key:** The key used to activate your Prescreen application
- **License Status:** Status of whether the key is Active or not
- **Allowed Devices:** Number of devices allowed by the Prescreen application
- **IP Address:** The IP Address on which the Prescreen is deployed on
- **Version:** Version of the Prescreen currently being used



8.0 Troubleshooting

Special Tip:

Please check the following table to see if it can help find the reason for the malfunction faced. When the fault is still not removed according to the operation performed in the instruction table below, please contact the support team

Issue	Possible Cause	Troubleshooting
Management software is on a MIPS Chinese page	Incorrect URL input	Simply click on the MIPS seen at the corner, and then refresh
Error prompt 'app crashed'	Incorrect installation of the management software Multiple instances of the software running	Please close all instances of the current's software, go to C>Program Files>MIPS and uninstall the previous version of the software, and download+Install the latest version of the software (can be found directly on our website
Uploading employee list giving error	Incorrect format being followed for the upload	Please make sure that the data input follows the reference format exactly, provided in the excel sheet
Unable to connect to the server error on device	The network might be blocking the software, or the firewall (or antivirus) might be blocking communication	Please perform the following: 1. White list the application by creating new rule in the advanced firewall settings (new inbound and outbound rule) 2. Turn off antivirus (or firewall) temporarily to see if the application needs to be whitelisted.
Saving email info gives error prompt 'info not ok'	Incorrect information saved in the email setting gives this error	Please make sure that the instructions above for the email config has been followed.
Pass recording not showing on management software	Incorrect time zone, or improper configuration of the device	1. Please make sure 'stranger record' is on, in the body temperature setting of the device. 2. Please make sure the GoSafe device and the device where the software is installed on are on the same time zone.

9.0 Compliances

FCC Statement:

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Non-modification Statement:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, that can result in an explosion.

Leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable or gas

OneScreen™

800-992-5279

sales@onescreensolutions.com