



OneScreen GoSafe

# OneScreen GoSafe

## Management Platform

### User Manual

Supports all GoSafe models





## Contents

1. Installation and Login .....	5
2. Console .....	6
3. Device Management .....	6
3.1. Device List .....	6
3.1.1. Body Temperature Test .....	7
3.1.2. Parameter Settings .....	8
3.1.3. Power Control .....	8
3.1.4. Client upgrade .....	9
3.1.5. Volume Setting .....	9
3.1.6. Auto-Start .....	10
3.1.7. Application Daemon .....	10
3.1.8. Callback Settings .....	11
3.1.9. Door Control.....	11
3.1.10. Delete Device.....	11
3.1.11. Device Groups .....	11
3.1.12. Device Details.....	12
3.1.13. Device Monitoring .....	13
3.1.14. Bulk operations on Group .....	14
3.1.15. Device Group Management .....	14
3.2. APK List .....	15
3.2.1. Delete APK .....	15
3.2.2. New APK.....	15
4. Attendance Management .....	16
4.1. Attendance Rules .....	16
4.1.1. Shift Settings .....	16
4.1.2. Holiday Settings .....	17
4.1.3. Public Holiday Settings .....	18
4.1.4. Device Group Settings .....	19
4.2. Attendance Records .....	20
4.3. Attendance Statistics .....	21
4.4. Attendance Notifications .....	23



5. Personnel Management .....	23
5.1. Employee list .....	23
5.1.1. Add Employee information individually .....	23
5.1.2. Import Employee information in bulk .....	25
5.1.3. Import portrait photos in bulk .....	27
5.1.4. Export employee information .....	29
5.1.5. Refresh employee information .....	29
5.1.6. Employee edit .....	29
5.1.7. Employee groups management .....	30
5.1.8. Employee search .....	30
5.2. Visitor management .....	31
5.2.1. Add visitors individually .....	31
5.2.2. Export visitor's information .....	33
5.2.3. Refresh visitor's information .....	33
5.2.4. Visitor details editing .....	33
5.2.5. Visitor groups management .....	33
5.2.6. Visitor search .....	34
5.3. Restricted management .....	34
5.3.1. Add restricted person individually .....	34
5.3.2. Export restricted management list (blacklist) .....	36
5.3.3. Refresh restricted management information .....	36
5.3.4. Restricted management details and editing .....	36
5.3.5. Restricted groups management .....	36
6. Pass Management .....	37
6.1. Pass records .....	37
6.2. Pass permission .....	37
6.2.1. Employee pass permission settings .....	38
6.2.2. Visitor pass permission settings .....	39
6.2.3. Revoke permission .....	40
6.2.4. Refresh permission information .....	41
6.3. Restricted monitoring .....	41
6.3.1. Restricted monitoring settings .....	41
6.3.2. Identification records .....	42
6.3.3. Remove monitoring .....	42
6.4. Permission records .....	43



7. System Management .....	44
7.1. Organization structure .....	44
7.1.1. New User .....	44
7.1.2. Search organization structure .....	45
7.1.3. Organization structure- operate .....	45
7.2. Role Management .....	45
7.3. Business management .....	46
7.3.1. New company .....	46
7.3.2. Search/Edit/Delete .....	47
7.4. System Log .....	47
7.5. System Settings .....	48
7.5.1. System Settings .....	48
7.5.1.1. Email Settings .....	49
7.5.2. Integrate Services .....	52
7.5.2.1. INTEGRATE .....	52
7.5.3. Prescreen Integration .....	53
8. Troubleshooting .....	54
9. Compliances .....	55

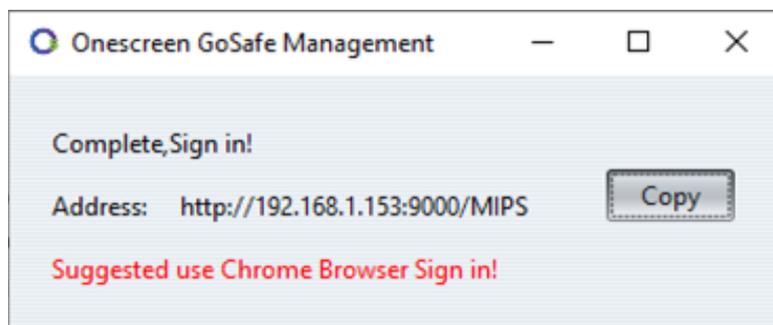
## 1. Installation and Login

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

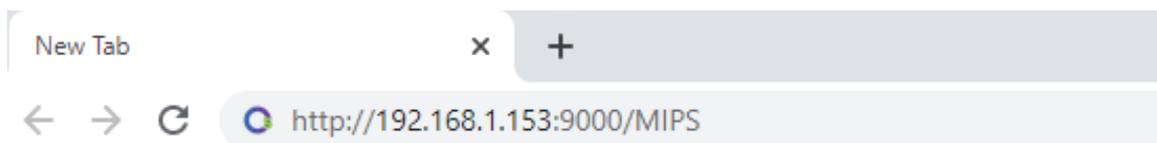
Note: Please allow firewall exception on your windows system, and if you are using a restricted network, whitelist the application on the network.

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.

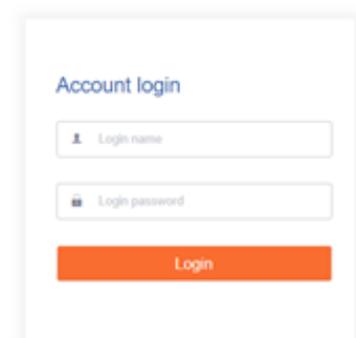


- Enter your username and password to log in

Standard username: admin

Standard password: 123456

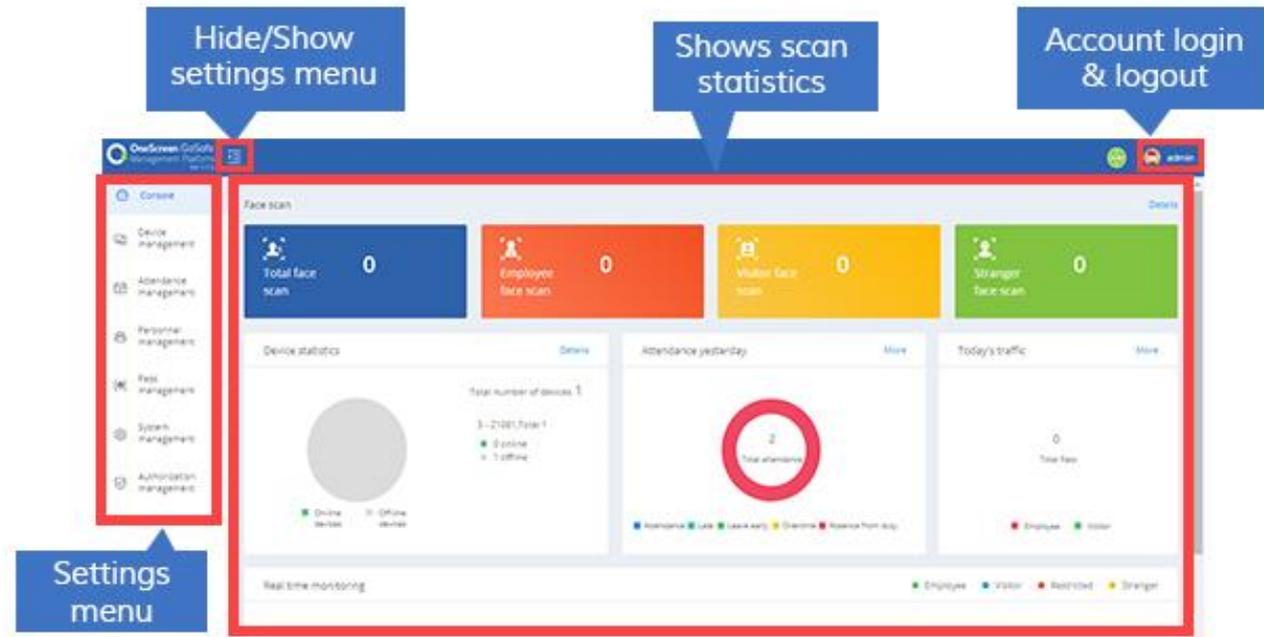
**OneScreen GoSafe**  
Management Platform



- 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

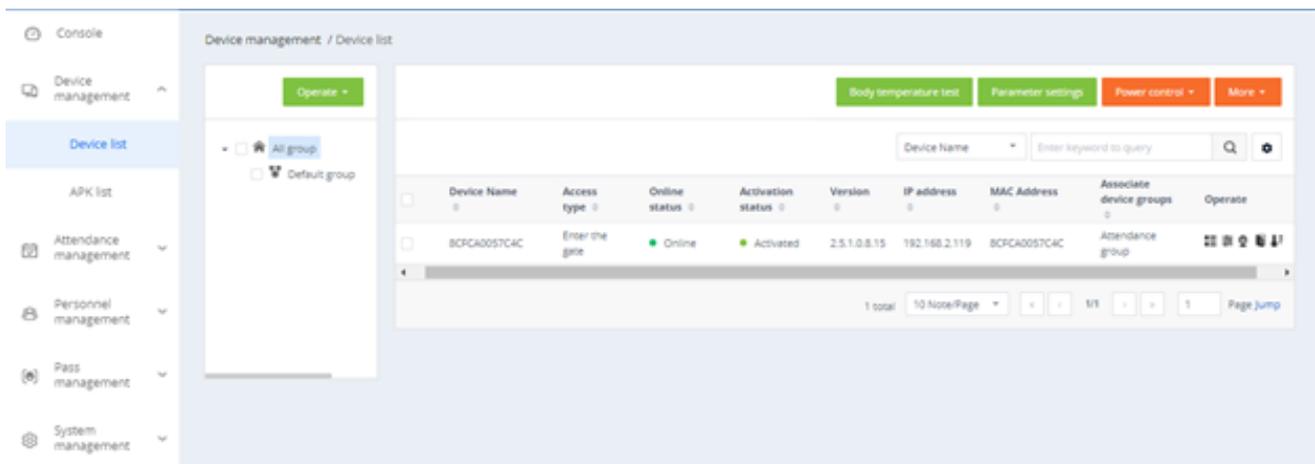
It provides an overview of the number of devices and online status which includes statistics of the face scan (total faces scanned, employee faces scanned, visitor faces scanned, stranger faces scanned), today's pass and real-time monitoring (employees, visitors, restricted, body temperature), and provides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



## 3. Device Management

### 3.1. Device List

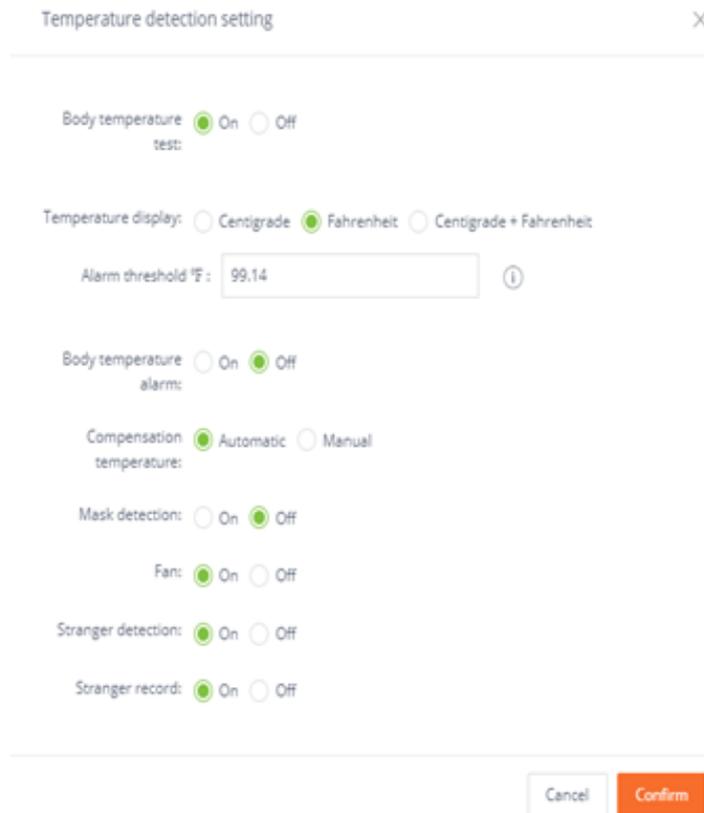
Device list allows you to manage all of the devices connected to your management console using this dashboard. You can alter settings on each individual device or by selecting a group of devices to alter the settings collectively.



### 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



Temperature detection setting ×

Body temperature test:  On  Off

Temperature display:  Centigrade  Fahrenheit  Centigrade + Fahrenheit

Alarm threshold °F:  ⓘ

Body temperature alarm:  On  Off

Compensation temperature:  Automatic  Manual

Mask detection:  On  Off

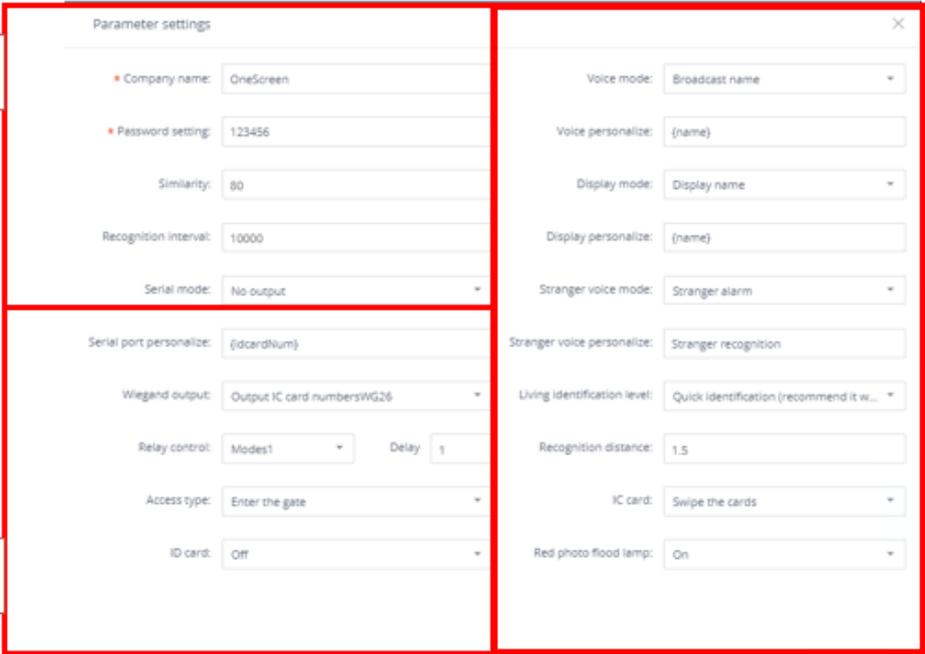
Fan:  On  Off

Stranger detection:  On  Off

Stranger records:  On  Off

### 3.1.2. Parameter Settings

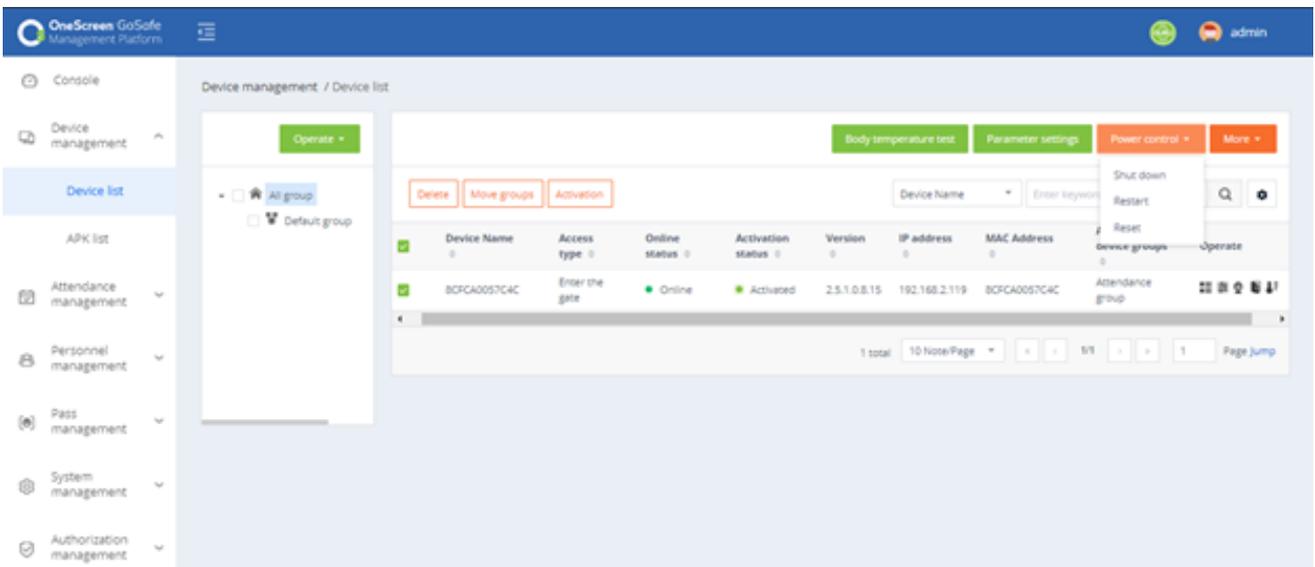
Parameter settings essentially allows you to configure your devices with automatic access control systems, Wiegand interfaces, and serial communications.



The screenshot shows the 'Parameter settings' window divided into two main sections. The left section is highlighted with a red box and a callout: 'Change the name, password, and'. This section includes fields for 'Company name' (OneScreen), 'Password setting' (123456), 'Similarity' (80), 'Recognition interval' (10000), 'Serial mode' (No output), 'Serial port personalize' (i:cardnum), 'Wiegand output' (Output IC card numbersWG26), 'Relay control' (Modes1, Delay 1), 'Access type' (Enter the gate), and 'ID card' (Off). The right section is also highlighted with a red box and a callout: 'Allows for changing display settings and IC'. This section includes 'Voice mode' (Broadcast name), 'Voice personalize' ((name)), 'Display mode' (Display name), 'Display personalize' ((name)), 'Stranger voice mode' (Stranger alarm), 'Stranger voice personalize' (Stranger recognition), 'Living identification level' (Quick identification (recommend it w...)), 'Recognition distance' (1.5), 'IC card' (Swipe the cards), and 'Red photo flood lamp' (On). A third callout at the bottom left says 'Allows for serial, Wiegand, and relay' pointing to the bottom half of the left section.

### 3.1.3. Power Control

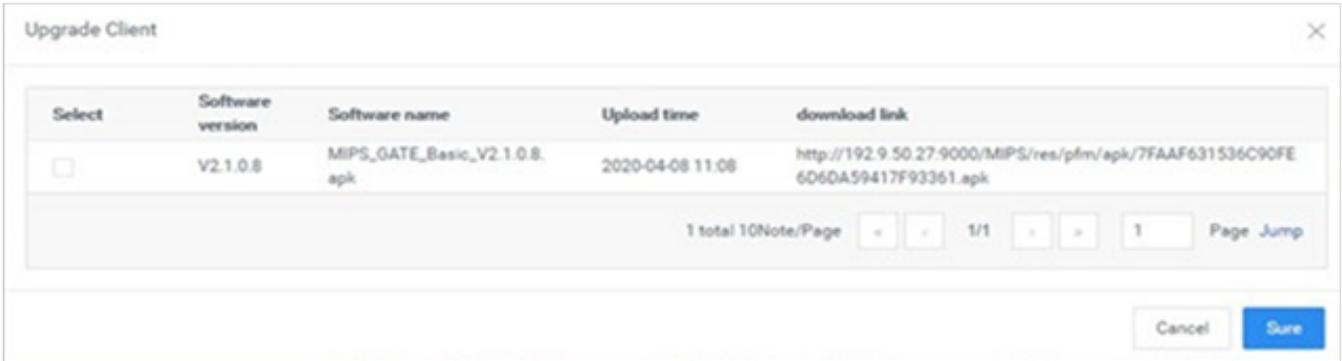
Power control settings allow you to remotely **Shut off**, **Restart**, or **Reset** the selected device(s).



The screenshot shows the 'OneScreen GoSafe Management Platform' interface. The left sidebar contains navigation options: Console, Device management, Device list (selected), APK list, Attendance management, Personnel management, Pass management, System management, and Authorization management. The main content area is titled 'Device management / Device list'. It features a table with columns: Device Name, Access type, Online status, Activation status, Version, IP address, and MAC Address. A single device is listed: BCFCA0057C4C, Enter the gate, Online, Activated, 2.5.1.0.8.15, 192.168.2.119, BCFCA0057C4C. Above the table, there are buttons for 'Delete', 'Move groups', and 'Activation'. A 'Power control' dropdown menu is open, showing options: Shut down, Restart, and Reset. The interface also includes a search bar, a 'Device Name' dropdown, and a 'Page Jump' section at the bottom.

### 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.



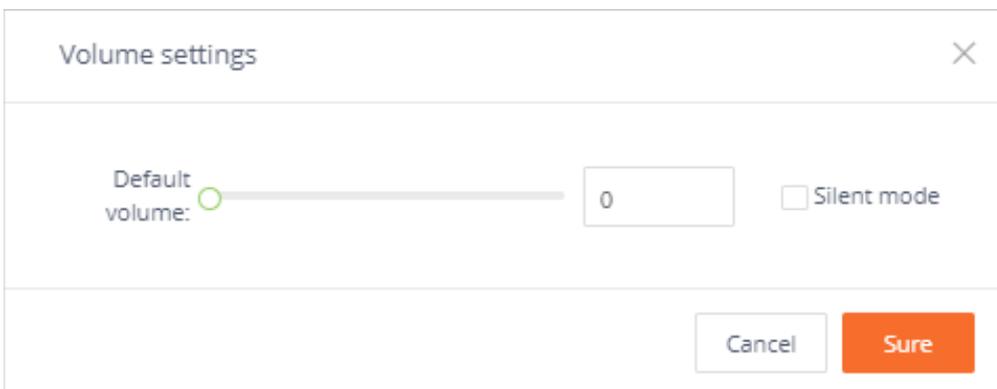
Select	Software version	Software name	Upload time	download link
<input type="checkbox"/>	V2.1.0.8	MIPS_GATE_Basic_V2.1.0.8.apk	2020-04-08 11:08	http://192.9.50.27:9000/MIPS/res/pfm/apk/7FAAF631536C90FE6D6DA59417F93361.apk

1 total 10Note/Page    1/1    Page Jump

Cancel    **Sure**

### 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.



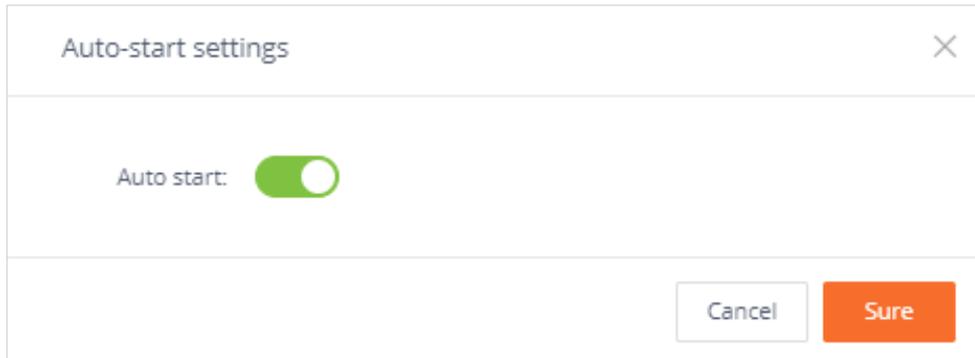
Volume settings

Default volume:  0     Silent mode

Cancel    **Sure**

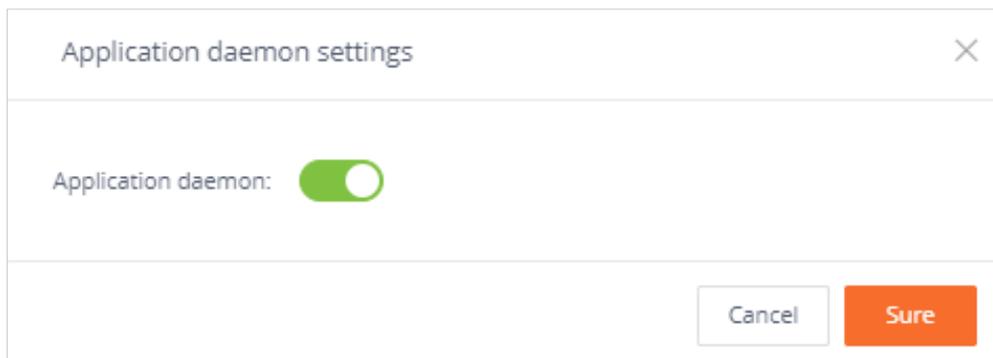
### 3.1.6. Auto-Start

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.



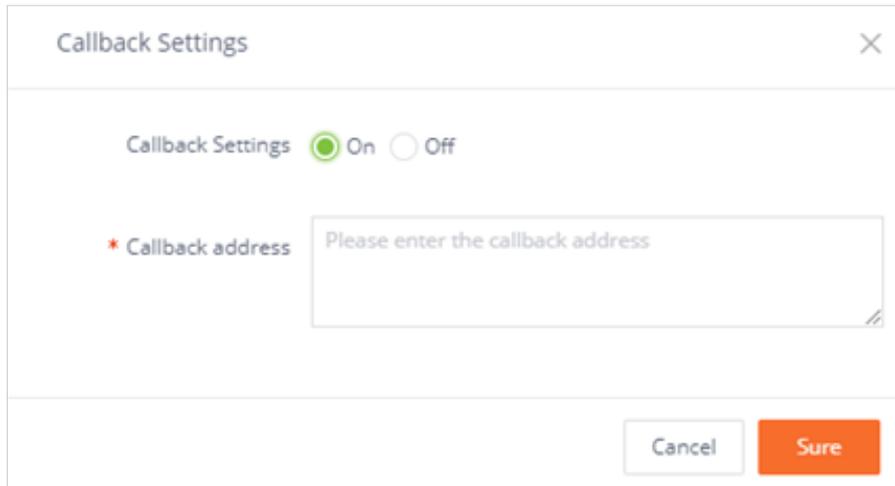
### 3.1.7. Application Daemon

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

A dialog box titled 'Callback Settings' with a close button (X) in the top right corner. It contains a toggle switch for 'Callback Settings' which is currently set to 'On'. Below this is a text input field labeled '\* Callback address' with a placeholder text 'Please enter the callback address'. At the bottom right, there are two buttons: 'Cancel' and 'Sure'.

### 3.1.9. Door Control

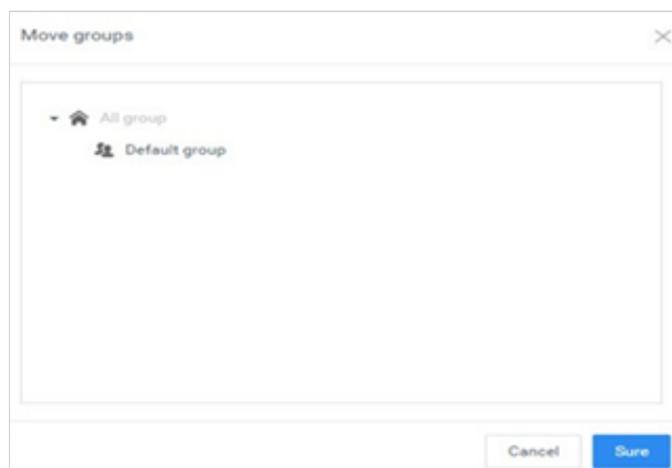
To open a specific gate controlled by a device, go to Device list and click on “open the door remotely” of the desired device. This will open the access control system, which is controlled by that particular device.

### 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.

A dialog box titled 'Move groups' with a close button (X) in the top right corner. It contains a list of groups: 'All group' and 'Default group'. At the bottom right, there are two buttons: 'Cancel' and 'Sure'.

### 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 management / Device list / Device details

Basic information    Device settings    Remote operation

Basic information

Device Name: <input type="text" value="BCFGA0057C4C"/>		
device ID: 1	Access type: Enter the gate	Screen: 800*1280
Software version: 2.5.1.0.B.15	Motherboard model: GM6205	Firmware version: GOSUNCH/GM6205/GM6205.B.1.0/OPM1.171019.026/zwj101
Available space: 8.72 GB	MAC: BCFG A0057C4C	IP address: 192.168.2.119

Device group:

Device address:

Note:

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

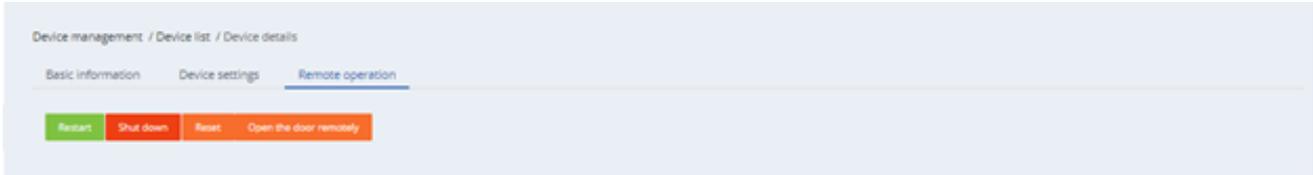
Device management / Device list / Device details

Basic information    **Device settings**    Remote operation

Parameter settings

Company name: <input type="text" value="OneScreen"/>	Voice mode: <input type="text" value="Broadcast name"/>
Password setting: <input type="text" value="123456"/>	Voice personalization: <input type="text" value="(name)"/>
Similarity: <input type="text" value="80"/>	Display mode: <input type="text" value="Display name"/>
Recognition interval: <input type="text" value="10000"/>	Display personalization: <input type="text" value="(name)"/>
Serial mode: <input type="text" value="No output"/>	Stranger voice mode: <input type="text" value="Stranger alarm"/>
Serial port personalization: <input type="text" value="(boardNum)"/>	Stranger voice personalization: <input type="text" value="Stranger recognition"/>
Wiegand output: <input type="text" value="Output IC card number#1026"/>	Living identification level: <input type="text" value="Quick identification (recommend it when someone on duty)"/>
Relay control: <input type="text" value="Modes1"/> Delay: <input type="text" value="1"/>	Recognition distance: <input type="text" value="1.5"/>
Access type: <input type="text" value="Enter the gate"/>	IC card: <input type="text" value="Swipe the cards"/>
ID card: <input type="text" value="Off"/>	Red photo flood lamp: <input type="text" value="On"/>

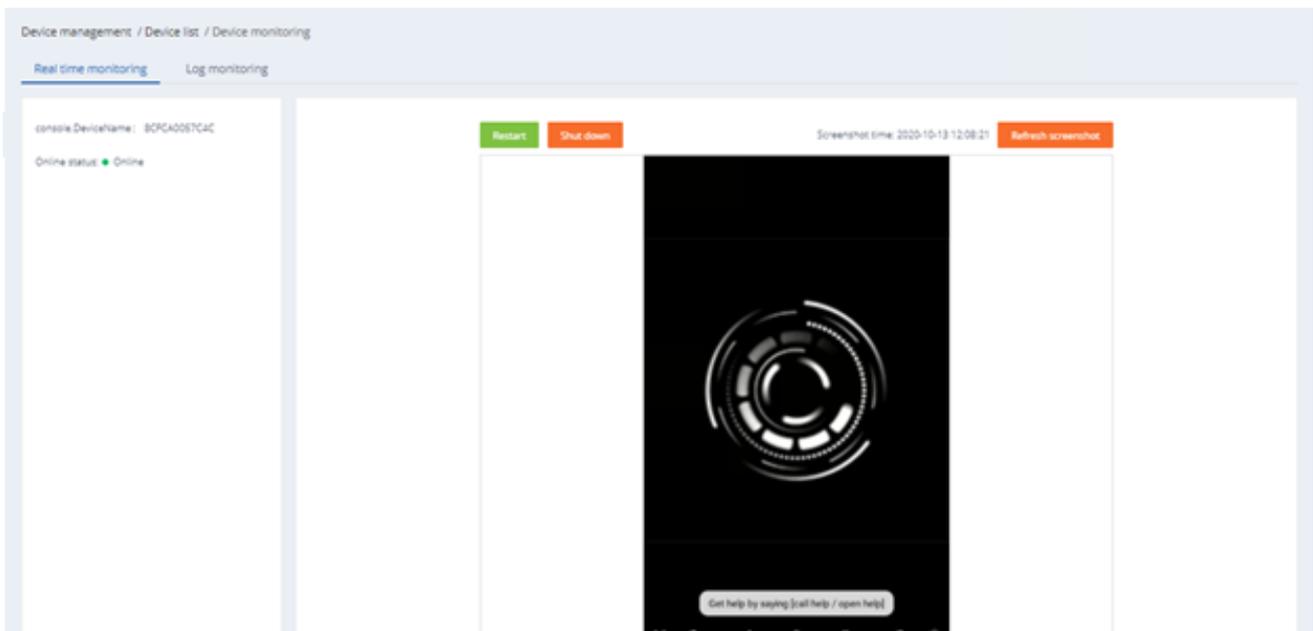
**Remote operation:** restart, shutdown, reset and remote door opening.



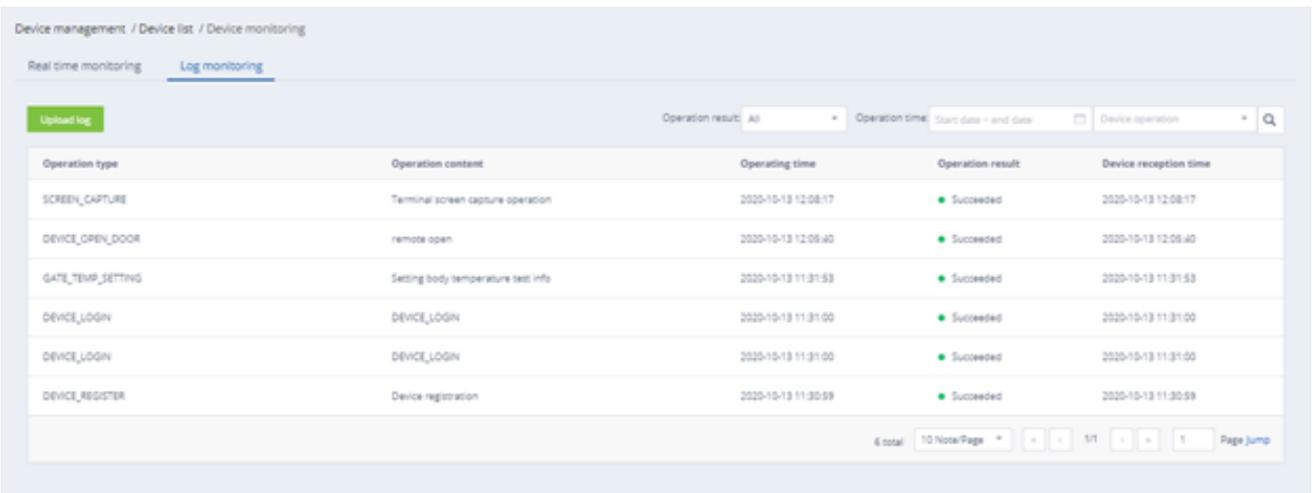
### 3.1.13. Device Monitoring

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.



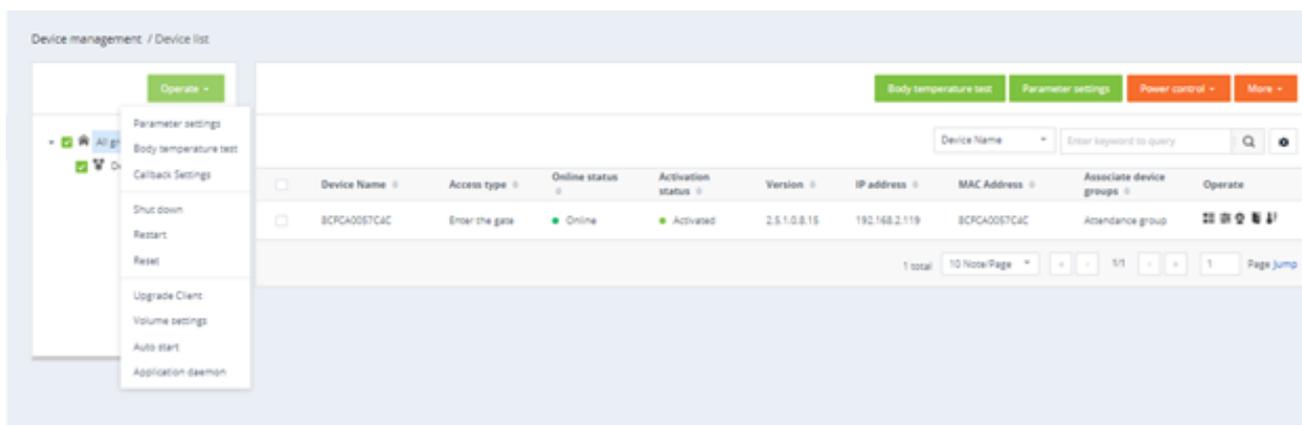
- **Log monitoring:** View related operation logs of the device.



Operation type	Operation content	Operating time	Operation result	Device reception time
SCREEN_CAPTURE	Terminal screen capture operation	2020-10-13 12:08:17	● Succeeded	2020-10-13 12:08:17
DEVICE_OPEN_DOOR	remote open	2020-10-13 12:08:40	● Succeeded	2020-10-13 12:08:40
GATE_TEMP_SETTING	Setting body temperature test info	2020-10-13 11:31:53	● Succeeded	2020-10-13 11:31:53
DEVICE_LOGIN	DEVICE_LOGIN	2020-10-13 11:31:00	● Succeeded	2020-10-13 11:31:00
DEVICE_LOGIN	DEVICE_LOGIN	2020-10-13 11:31:00	● Succeeded	2020-10-13 11:31:00
DEVICE_REGISTER	Device registration	2020-10-13 11:30:59	● Succeeded	2020-10-13 11:30:59

### 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 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 on the delete icon.

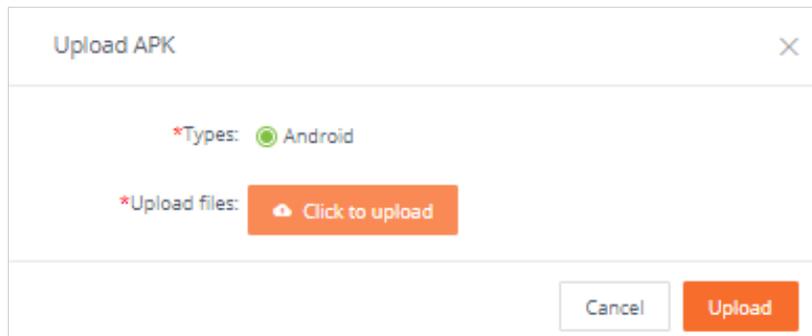


The screenshot shows a web interface titled "Device management / APK list". In the top right corner, there is an orange button labeled "New APK". Below the title is a table with the following columns: "Software version", "Software name", "Upload time", "download link", and "Operate". The table contains one row with the following data: "V2.1.0.8" for software version, "MPS\_GATE\_Basic\_V2.1.0.8.apk" for software name, "2020-04-08 11:08:16" for upload time, and a long URL for the download link. In the "Operate" column, there is a trash can icon. Below the table, there is a pagination control showing "1 total", "10Note/Page", and "Page Jump".

Software version	Software name	Upload time	download link	Operate
V2.1.0.8	MPS_GATE_Basic_V2.1.0.8.apk	2020-04-08 11:08:16	http://192.9.50.27:9000/MPS/res/yfm/apk/7FAAF631536C90FE606DA59417F93361.apk	

### 3.2.2. New APK

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



The screenshot shows a dialog box titled "Upload APK" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "\*Types:" with a radio button selected for "Android". Below this, there is a section labeled "\*Upload files:" with a button that says "Click to upload" and a cloud upload icon. At the bottom of the dialog, there are two buttons: "Cancel" and "Upload".

## 4. Attendance Management

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

### 4.1. Attendance Rules

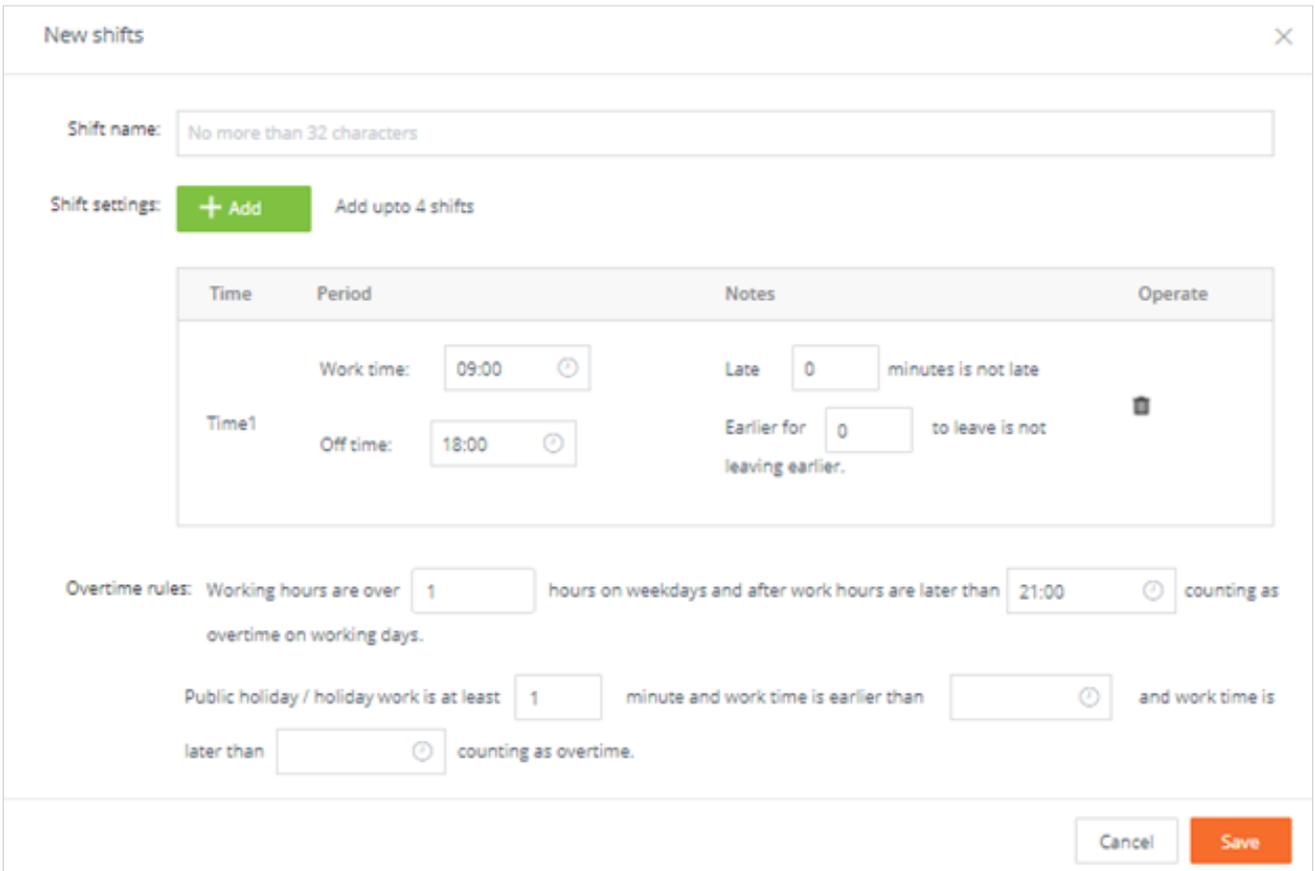
Here you can add, modify and delete attendance rules related to shifts, holidays, public holidays, and device groups.



#### 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.



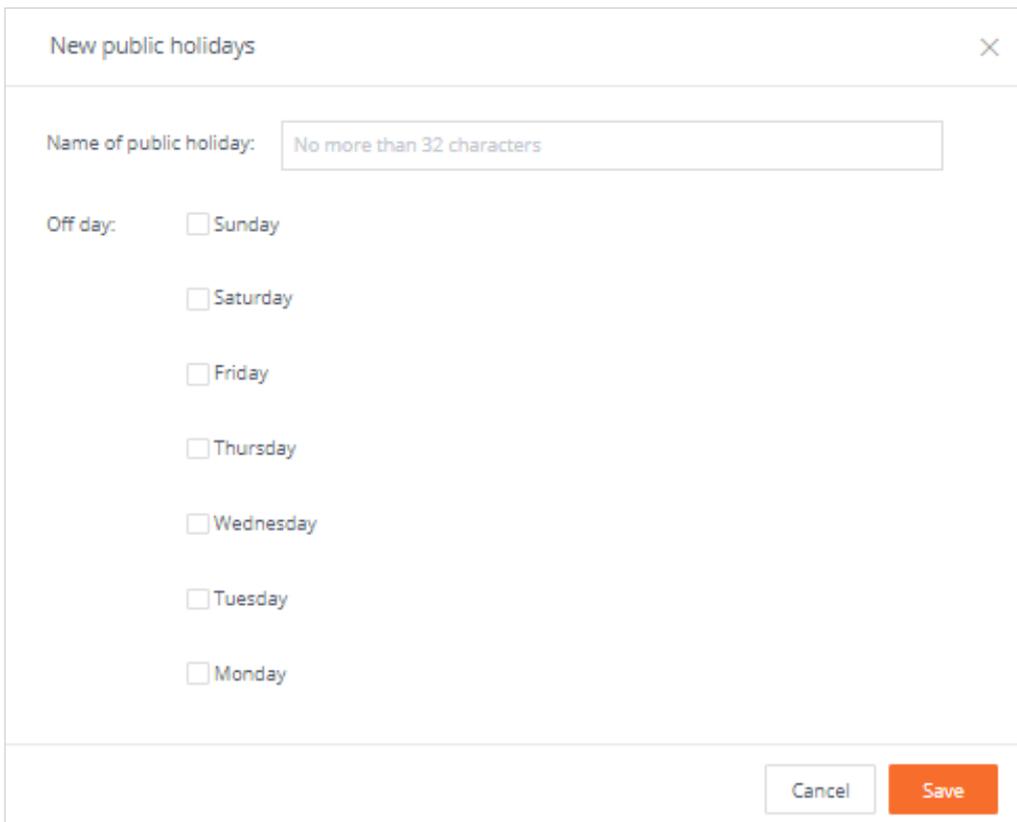
- **New Holiday:** Click on new holiday to go to the settings prompt for adding a new holiday.
- **Festival Name:** Enter the name of the holiday/festival.
- **Start date & End date:** Set the start and end date for the holiday.
- **Notes:** You can write a brief description about the holiday here, or 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.



The 'New public holidays' window has a title bar with a close button. It contains a text input field for 'Name of public holiday:' with a placeholder 'No more than 32 characters'. Below this is a section for 'Off day:' with seven checkboxes for 'Sunday', 'Saturday', 'Friday', 'Thursday', 'Wednesday', 'Tuesday', and 'Monday'. At the bottom right are 'Cancel' and 'Save' buttons.

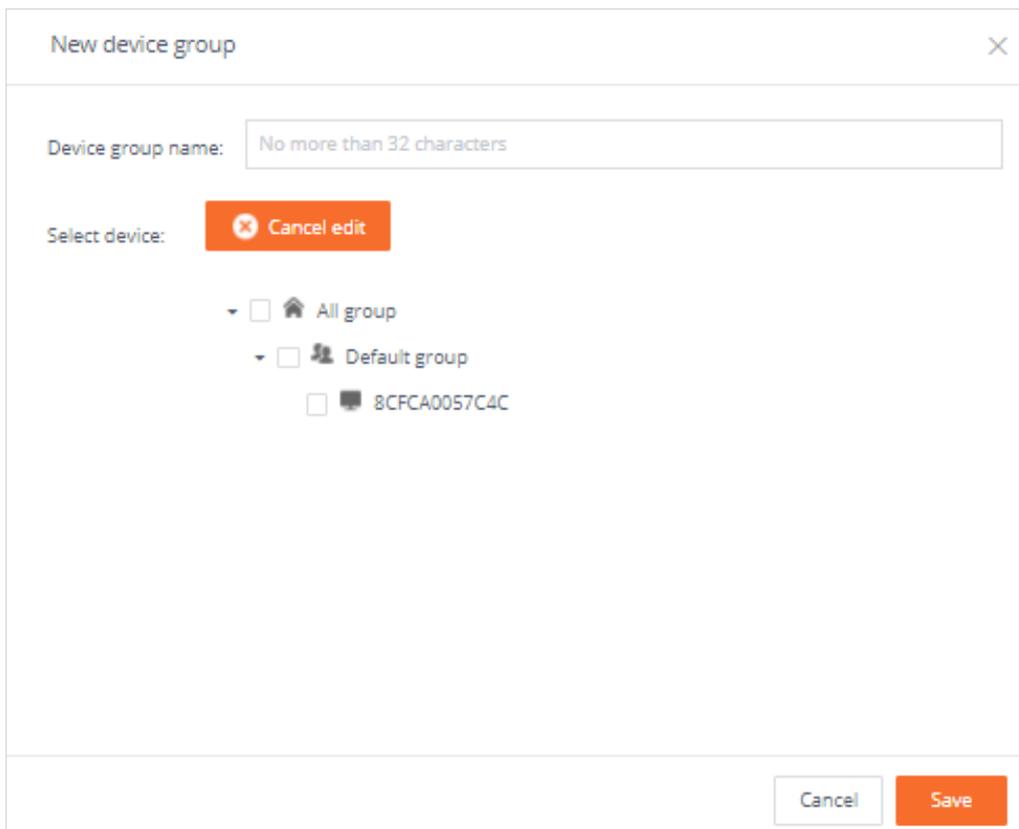
- **Public Holiday Name:** Set a name for the public holiday.
- **Off Day:** Select day(s) which you want to set as public holiday(s) in a week.

#### 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 device group

Device group name:

Select device:

-  All group
-  Default group
  -  8CFCA0057C4C

- **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 setting. You can also choose between different employee groups (set in employee settings). A sample of the list is shown below.

Attendance management / Attendance records

- All group

Default group

Attendance records Search employee name / ID  Export

Name	Date	Employee group	Employee id	First clock in	Last clock in	Body temperature	Status	Operate
Ebed	2020-10-13	Default group	234567			None	Absence	⊙
Osama	2020-10-13	Default group	123456			None	Absence	⊙
Ebed	2020-10-12	Default group	234567			None	Absence	⊙
Osama	2020-10-12	Default group	123456			None	Absence	⊙
Ebed	2020-10-11 <span style="background-color: #90ee90; padding: 2px;">WEEKDAY</span>	Default group	234567			None		⊙
Osama	2020-10-11 <span style="background-color: #90ee90; padding: 2px;">WEEKDAY</span>	Default group	123456			None		⊙
Ebed	2020-10-10 <span style="background-color: #90ee90; padding: 2px;">WEEKDAY</span>	Default group	234567			None		⊙
Osama	2020-10-10 <span style="background-color: #90ee90; padding: 2px;">WEEKDAY</span>	Default	123456			None		⊙

- **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

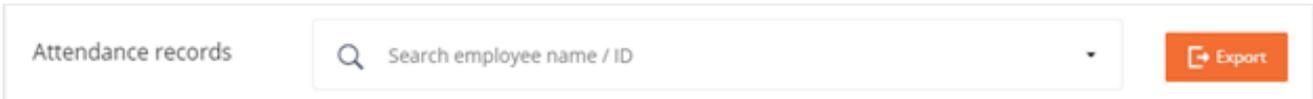
**Early departure:** If the employee clocks out at a time earlier than the shift end (even before the allowance set in shift settings), he will be marked as an early departure

**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.

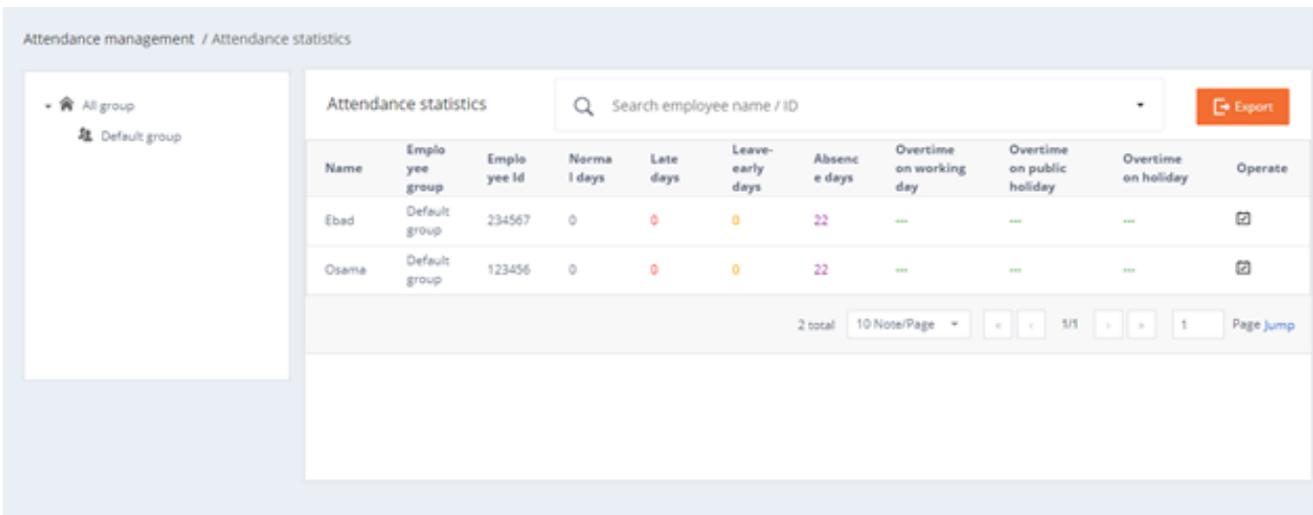
- **Export:** Click on export to download employee attendance record from the current page.

- **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.

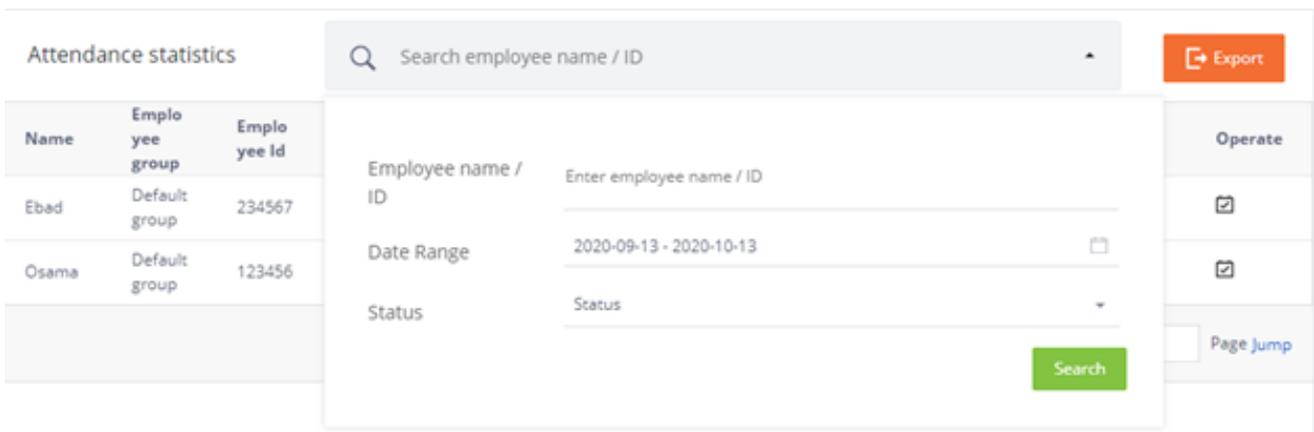


Name	Employee group	Employee Id	Normal days	Late days	Leave-early days	Absence days	Overtime on working day	Overtime on public holiday	Overtime on holiday	Operate
Ebad	Default group	234567	0	0	0	22	---	---	---	
Osama	Default group	123456	0	0	0	22	---	---	---	

2 total | 10 Note/Page | < < 1/1 > > | 1 | Page Jump

- **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.

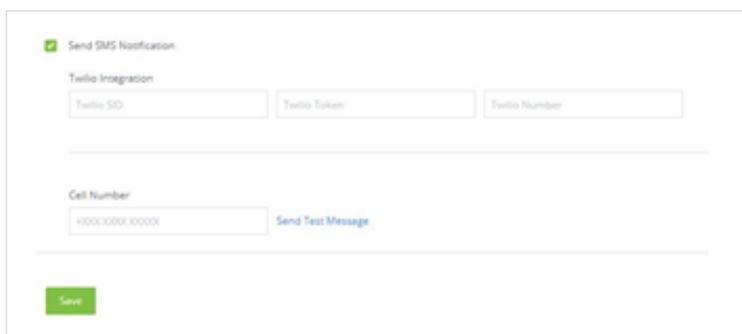


The screenshot shows the 'Attendance statistics' interface. On the left, there is a table with columns 'Name', 'Employee group', and 'Employee ID'. The table contains two rows: 'Ebad' with group 'Default group' and ID '234567', and 'Osama' with group 'Default group' and ID '123456'. A search filter overlay is positioned in the center, featuring a search bar with the placeholder 'Search employee name / ID', a date range field set to '2020-09-13 - 2020-10-13', and a status dropdown menu. A green 'Search' button is located at the bottom right of the filter. To the right of the filter, there is an 'Export' button (orange) and a vertical column of controls including 'Operate' (with a checkbox), another checkbox, and a 'Page Jump' input field.

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.

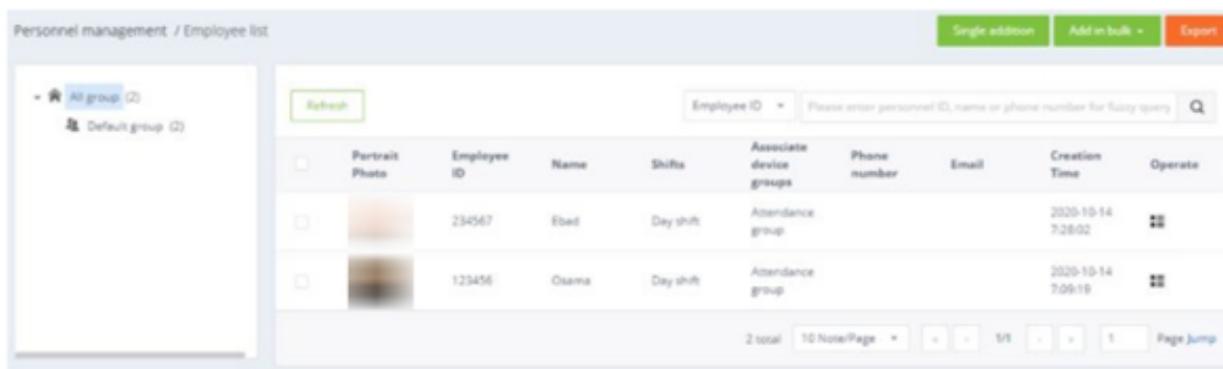


The screenshot shows a form titled "Send SMS Notification" with a checked checkbox. It includes input fields for "Twilio Integration" (Twilio SID, Twilio Token, Twilio Number) and "Cell Number" (with a placeholder +000.0000.00000). A "Send Test Message" button is next to the cell number field, and a "Save" button is at the bottom left.

## 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).



The screenshot shows the "Personnel management / Employee list" interface. It includes a sidebar with "All group (2)" and "Default group (2)", a "Refresh" button, a search bar for "Employee ID" with a placeholder "Please enter personnel ID, name or phone number for fuzzy query", and a table of employees. The table has columns for "Portrait Photo", "Employee ID", "Name", "Shifts", "Associate device groups", "Phone number", "Email", "Creation Time", and "Operate". Two employees are listed: Ebad (ID 234567) and Osama (ID 123456), both on "Day shift" and associated with "Attendance group". The footer shows "2 total" and "10 Items/Page".

#### 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

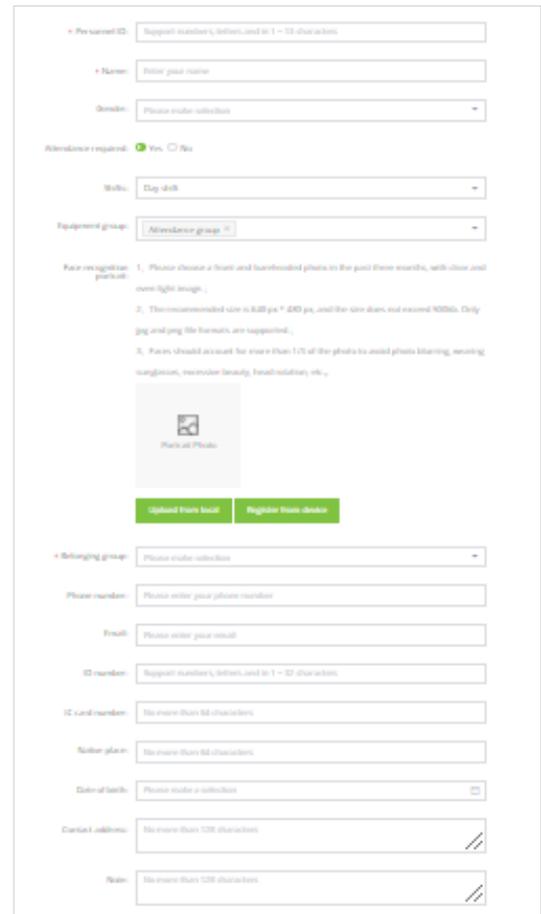
Click “Upload from local” to upload a picture from your system. Simply select a jpg or png portrait, and upload it.

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.

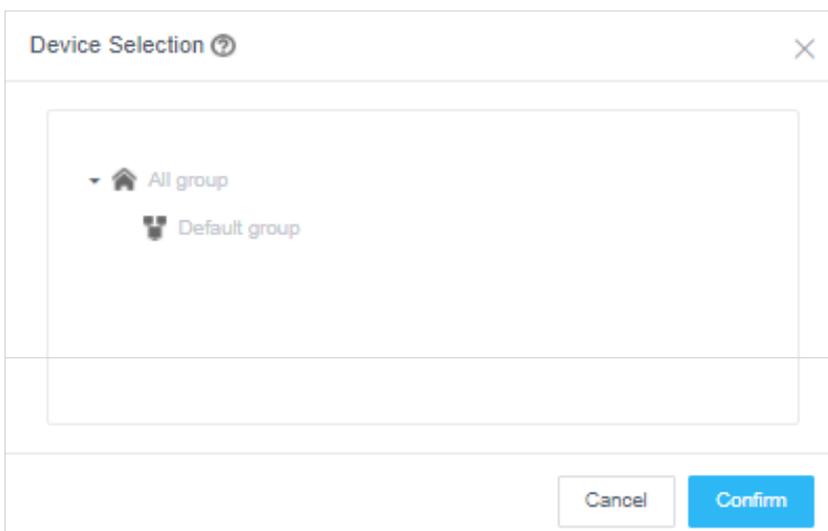
### Register from device

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



The screenshot shows a registration form with the following fields and options:

- Personal ID:** Text input field with a note: "Support numbers, letters, and 0-1-90 char action."
- Name:** Text input field with a note: "Enter your name."
- Gender:** Dropdown menu with a note: "Please make selection."
- Attendance required:** Radio buttons for "Yes" (selected) and "No".
- Shift:** Dropdown menu with a note: "Drop shift."
- Equipment group:** Dropdown menu with a note: "Attendance group."
- Face registration protocol:** A section containing three numbered instructions:
  1. Please choose a front and bareheaded photo in the past three months, with clear and even light image.
  2. The recommended size is 640 px \* 480 px, and the size does not exceed 500kb. Only jpg and png file formats are supported.
  3. Faces should account for more than 1/3 of the photo to avoid photo blurring, wearing sunglasses, excessive beauty treatment, etc.
- Photo upload options:** A "Pick up Photo" button, an "Upload from local" button, and a "Register from device" button.
- Belonging group:** Dropdown menu with a note: "Please make selection."
- Phone number:** Text input field with a note: "Please enter your phone number."
- Email:** Text input field with a note: "Please enter your email."
- ID number:** Text input field with a note: "Support numbers, letters, and 0-1-90 char action."
- IC card number:** Text input field with a note: "No more than 60 characters."
- Native place:** Text input field with a note: "No more than 60 characters."
- Date of birth:** Text input field with a note: "Please make a selection."
- Contact address:** Text input field with a note: "No more than 100 characters."
- Name:** Text input field with a note: "No more than 100 characters."



The screenshot shows a "Device Selection" dialog box with the following elements:

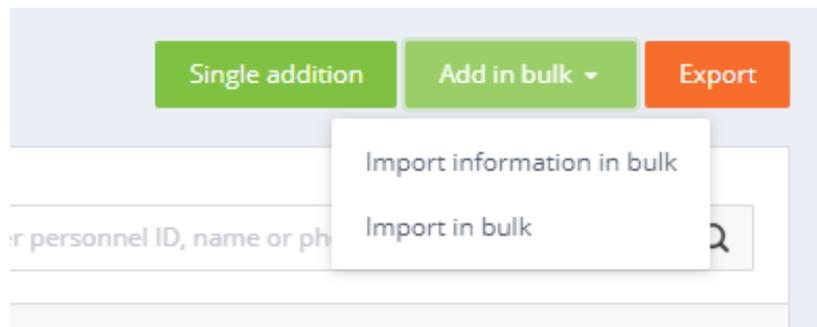
- Title:** "Device Selection" with a help icon and a close button (X).
- Content:** A list of device groups:
  - All group (with a home icon)
  - Default group (with a group icon)
- Buttons:** "Cancel" and "Confirm" buttons at the bottom right.

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:

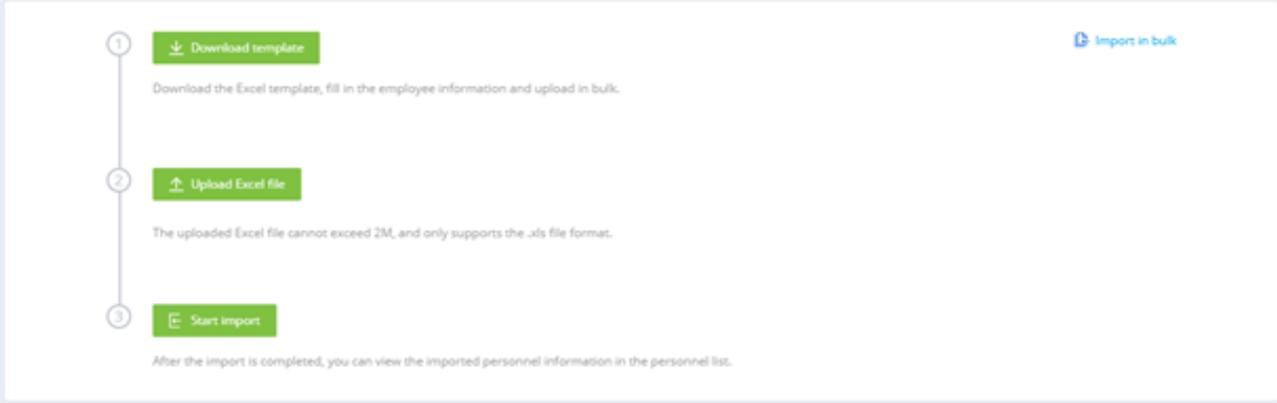
1. **Personnel ID:** required; cannot be repeated; in 1 to 9 characters, only consisting of numbers, letters or their combinations, such as 12345, abcd, a123.
2. **Name:** required; in 1 to 128 characters, consisting of Chinese, English, numbers, or their combinations (can contain Spaces).
3. **Gender:** 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.

Personnel management / Personnel list / Import information in bulk



The diagram shows a three-step process for importing personnel information in bulk:

- 1 Download template**: Download the Excel template, fill in the employee information and upload in bulk.
- 2 Upload Excel file**: The uploaded Excel file cannot exceed 2M, and only supports the .xls file format.
- 3 Start import**: After the import is completed, you can view the imported personnel information in the personnel list.

An "Import in bulk" button is visible in the top right corner of the interface.

## Types of import methods:

**Import method selection :**

**Overwrite import:** When importing the personnel information in bulk, the personnel information with the same personnel ID will be directly overwritten.

**Uncovered import:** When importing the personnel information in bulk, the personnel information with the same personnel ID will be skipped, and only the new personnel information will be imported.

Buttons: Uncovered import, Overwrite import, Cancel

- **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)

**Error prompt: The current form has the following errors, please modify and upload again.**

Personnel ID	Name	Error details
52300777	John c	The person Id already exists

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

## Import Failures:

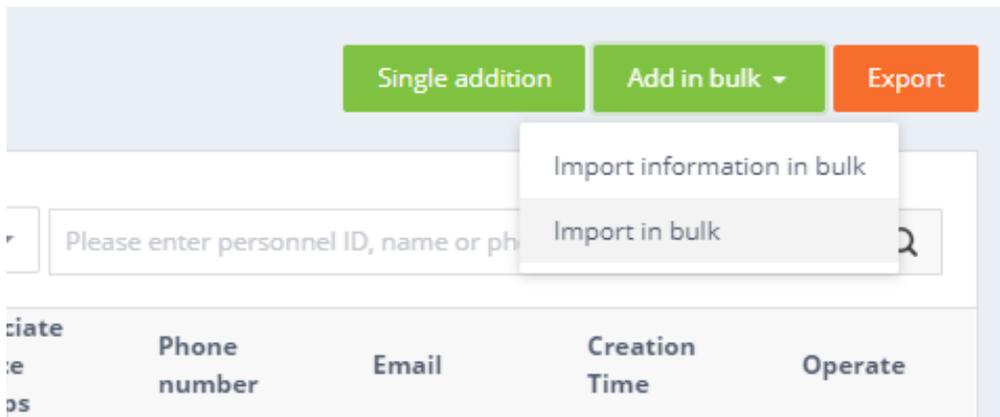
- If the content or format of the uploaded excel file is incorrect and does not meet the template specifications, an error message will appear, with the error specification mentioned for the specific employee. E.g. the employee below has an error on the gender column.

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

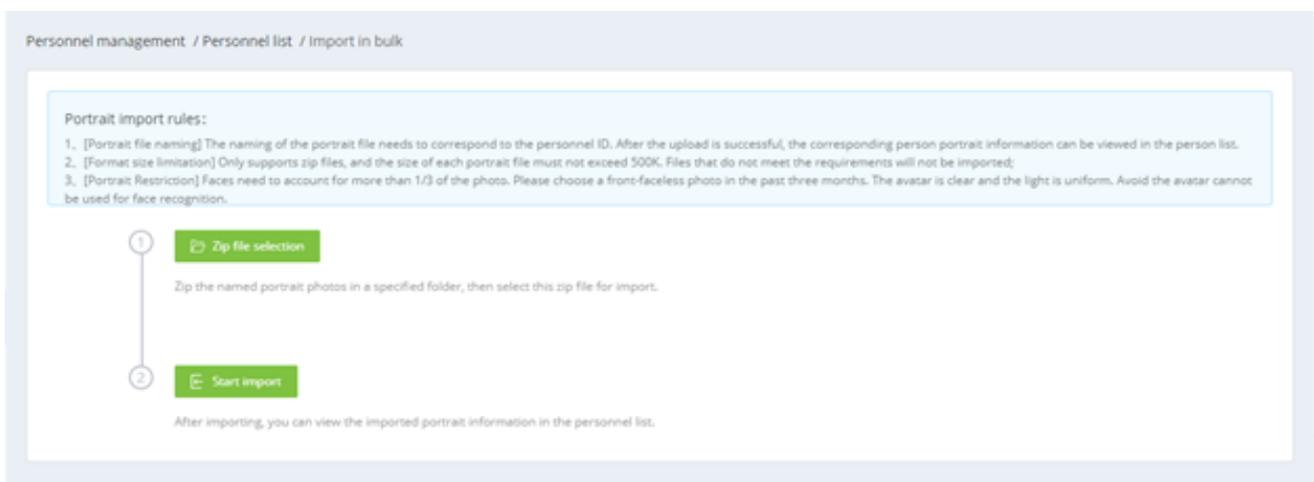
### 5.1.3. Import portrait photos in bulk

#### Steps:

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

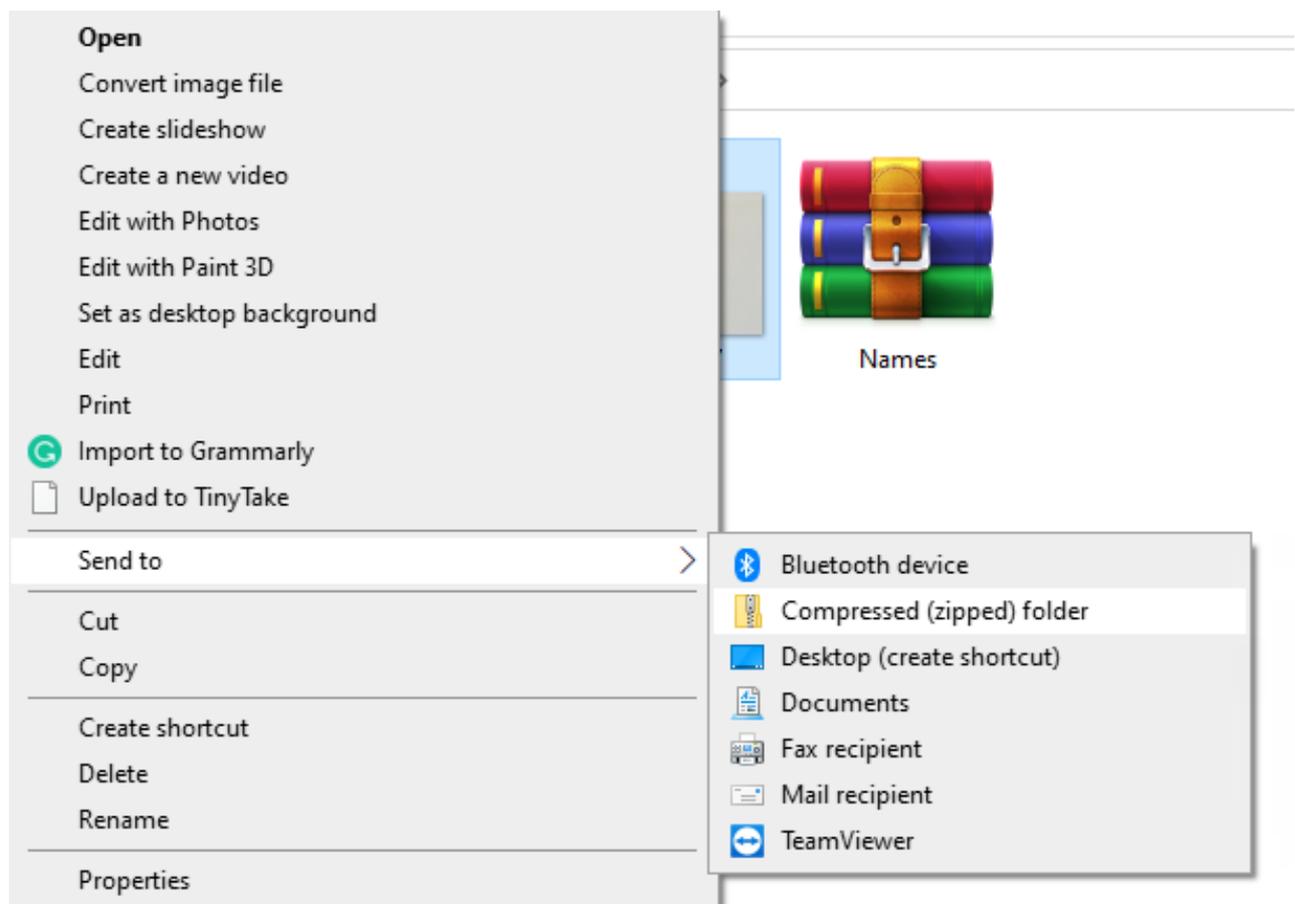


1. Click “Zip file selection” to open a Folder window and select the file which you want to upload (It has to be a compressed folder). After a successful upload, the current file storage path is displayed.
2. Click “Start Import”, and a progress bar will be displayed during the import process: the number 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

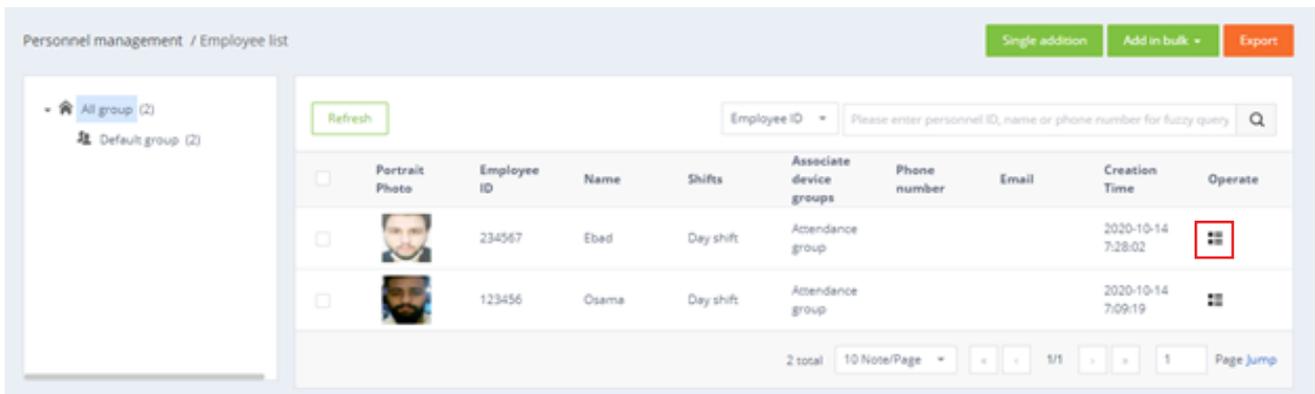
In “Employee List”, click the “Refresh” option to refresh all employee information in the list to their updated state.

## 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.



Personnel management / Employee list

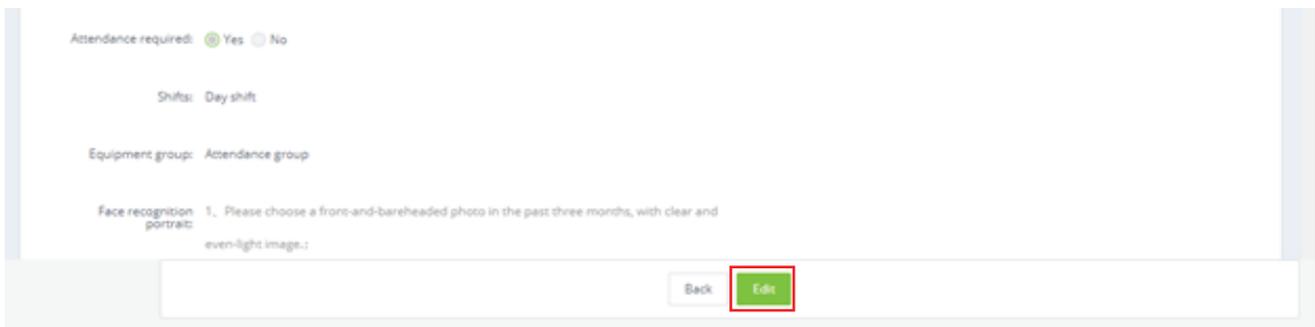
Single addition Add in bulk Export

Refresh

Employee ID  Please enter personnel ID, name or phone number for fuzzy query

<input type="checkbox"/>	Portrait Photo	Employee ID	Name	Shifts	Associate device groups	Phone number	Email	Creation Time	Operate
<input type="checkbox"/>		234567	Ebad	Day shift	Attendance group			2020-10-14 7:28:02	
<input type="checkbox"/>		123456	Osama	Day shift	Attendance group			2020-10-14 7:09:19	

2 total 10 Note/Page 1/1 Page Jump



Attendance required:  Yes  No

Shifts: Day shift

Equipment group: Attendance group

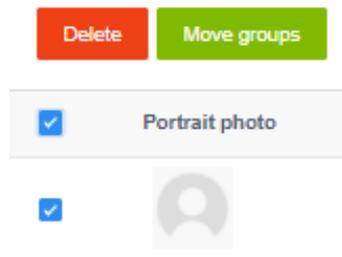
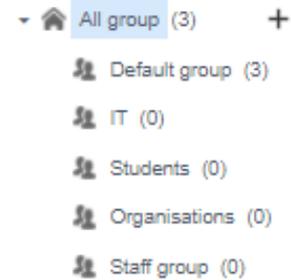
Face recognition portrait: 1. Please choose a front-and-bareheaded photo in the past three months, with clear and even-light image.:

Back Edit

### 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.

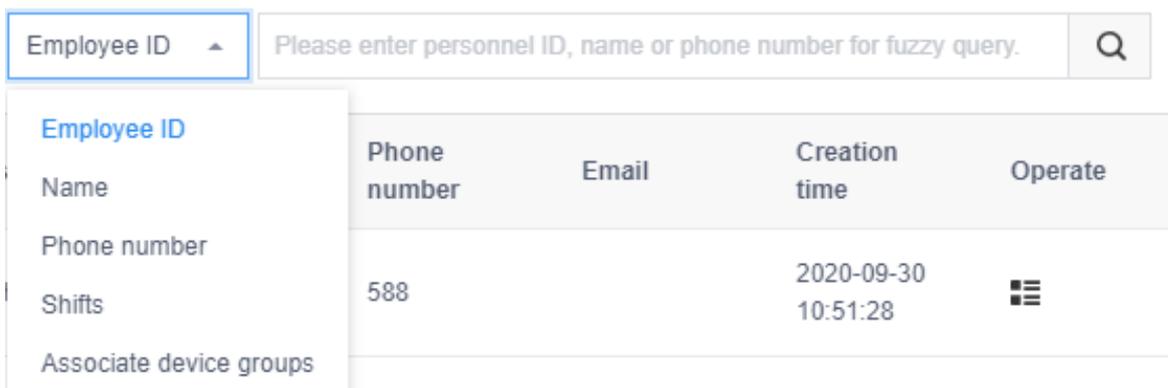
You can delete the employees by selecting them as well.

(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

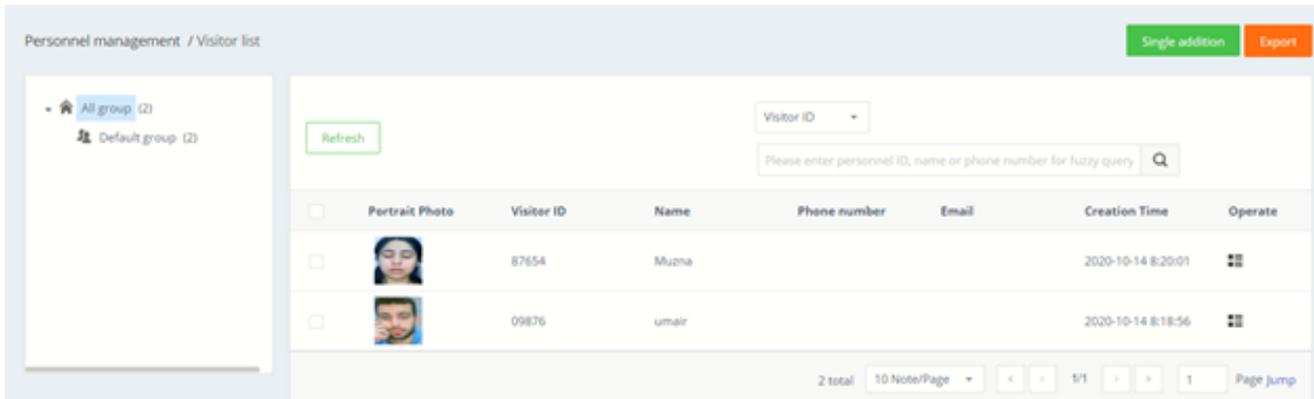
### 5.1.8. Employee Search

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

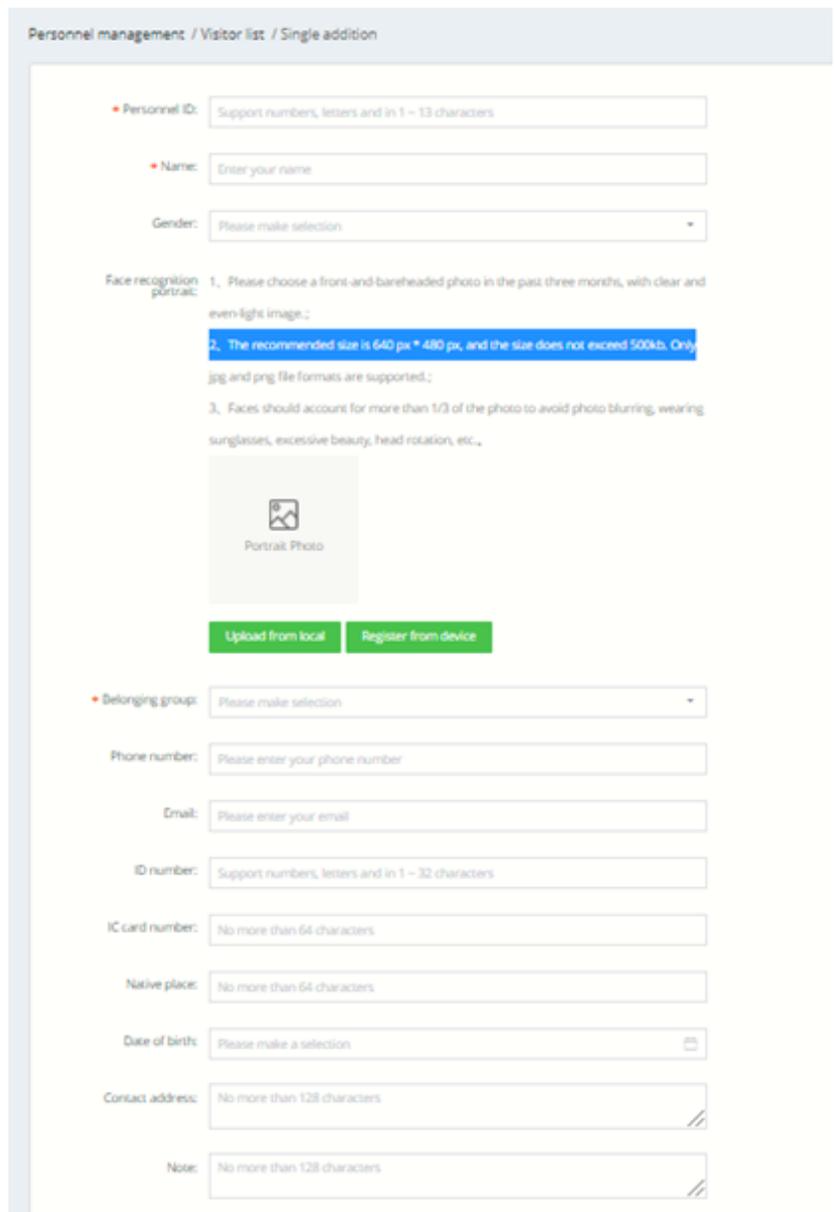
#### Steps

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



Personnel management / Visitor list / Single addition

Personnel ID:  Support numbers, letters and in 1 – 13 characters

Name:  Enter your name

Gender:  Please make selection

Face recognition portrait: 1. Please choose a front and bareheaded photo in the past three months, with clear and even light image.;  
2. The recommended size is 640 px \* 480 px, and the size does not exceed 500kb. Only jpg and png file formats are supported.;  
3. Faces should account for more than 1/3 of the photo to avoid photo blurring, wearing sunglasses, excessive beauty, head rotation, etc.,

Portrait Photo

Belonging group:  Please make selection

Phone number:  Please enter your phone number

Email:  Please enter your email

ID number:  Support numbers, letters and in 1 – 32 characters

IC card number:  No more than 64 characters

Native place:  No more than 64 characters

Date of birth:  Please make a selection

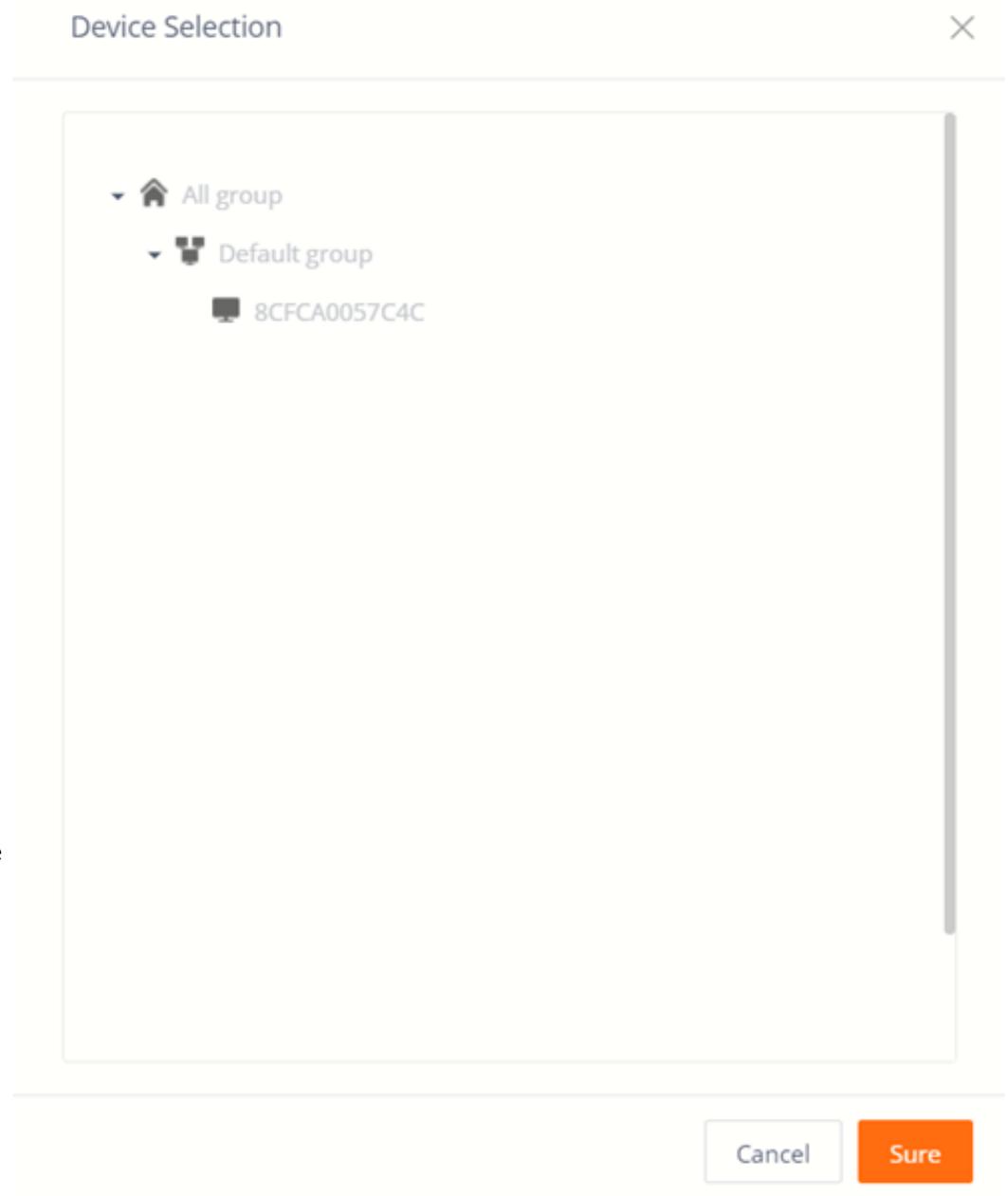
Contact address:  No more than 128 characters

Note:  No more than 128 characters

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.

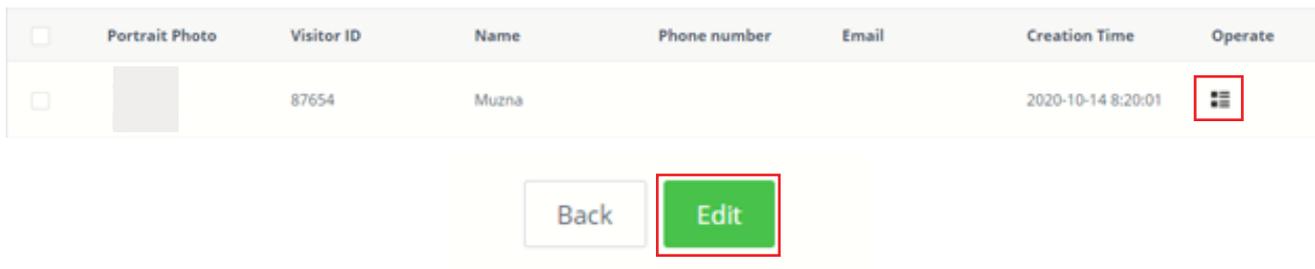
### 5.2.3. Refresh visitor's information

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.

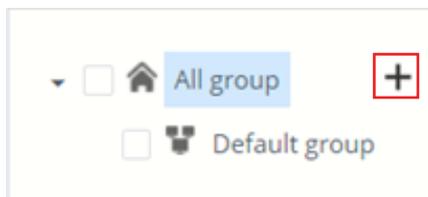
After the changes are made, simply click on save.



### 5.2.5. Visitor groups management

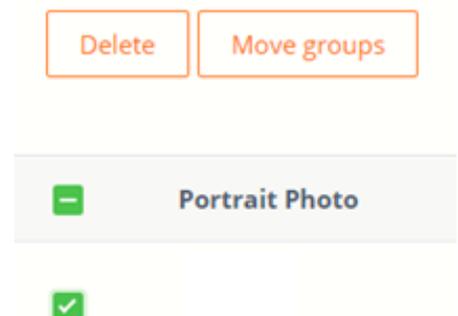
You can shift visitors to different groups (If created).

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.



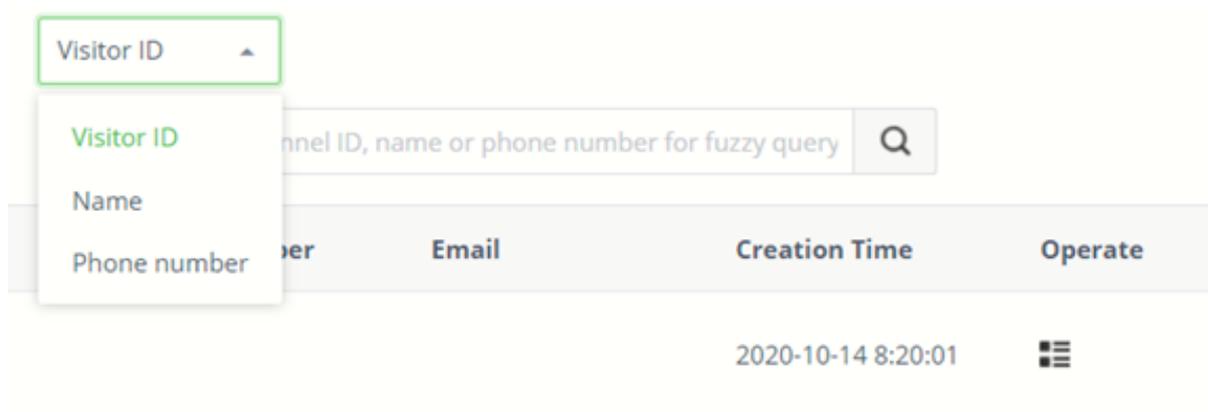
After a visitor group is created, select the visitor (or lists of visitors) you want to transfer, and then move them to the group you want to transfer them.

You can delete the visitors by selecting them as well.



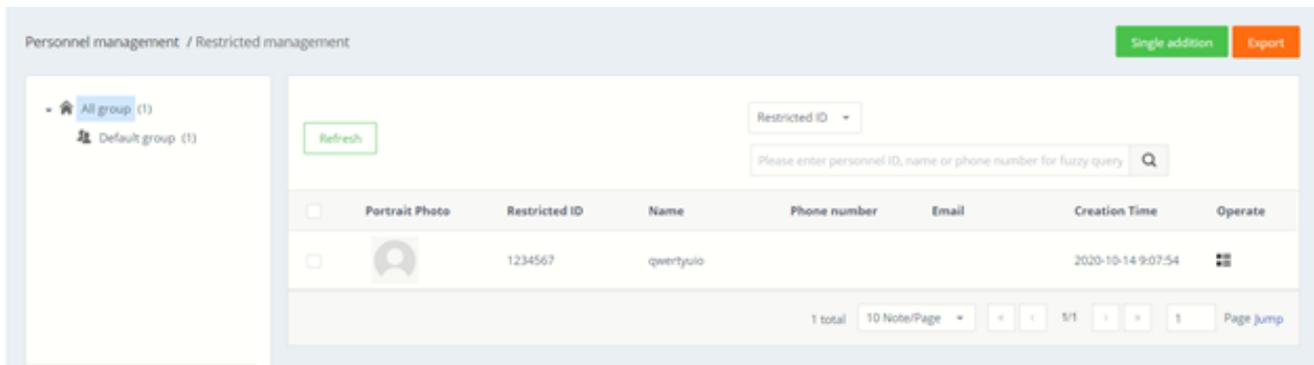
### 5.2.6. Visitor Search

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.

Personnel management / Restricted list / Single addition

• Personnel ID:  Support numbers, letters and in 1 – 13 characters

• Name:  Enter your name

Gender:  Please make selection

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

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

3. Faces should account for more than 1/3 of the photo to avoid photo blurring, wearing sunglasses, excessive beauty, head rotation, etc.,

 Portrait Photo

• Belonging group:  Please make selection

Phone number:  Please enter your phone number

Email:  Please enter your email

ID number:  Support numbers, letters and in 1 – 32 characters

IC card number:  No more than 64 characters

Native place:  No more than 64 characters

Date of birth:  Please make a selection

Contact address:  No more than 128 characters

Note:  No more than 128 characters

### 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.

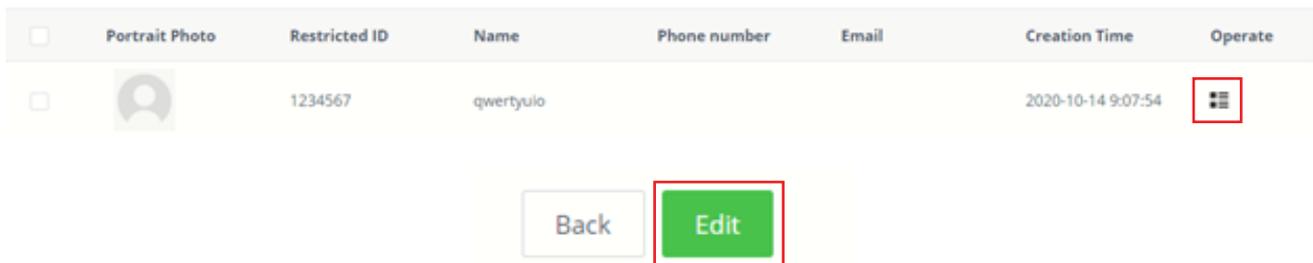
### 5.3.3. Refresh restricted management information

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

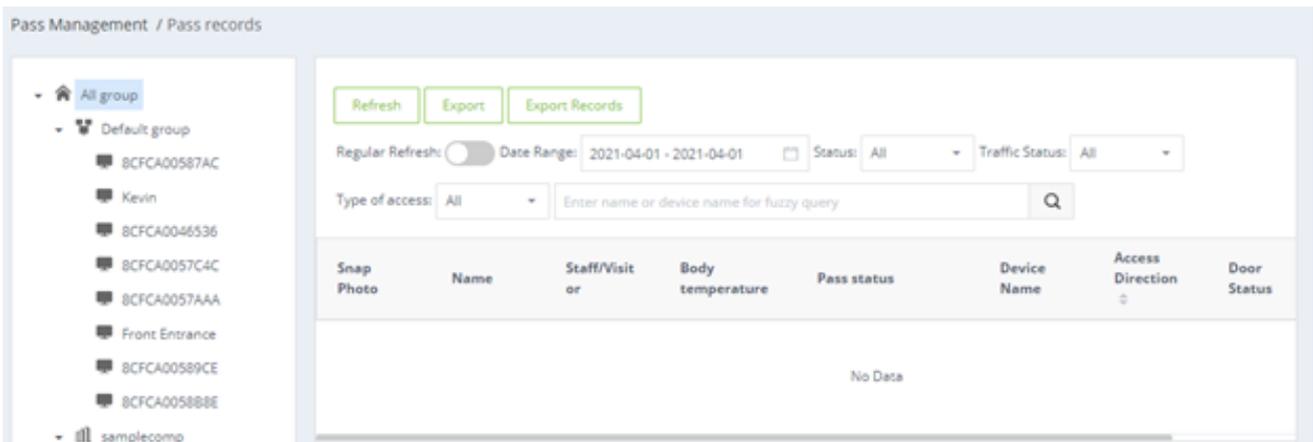
### 6.1. Pass records

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.



Pass Management / Pass records

Refresh Export Export Records

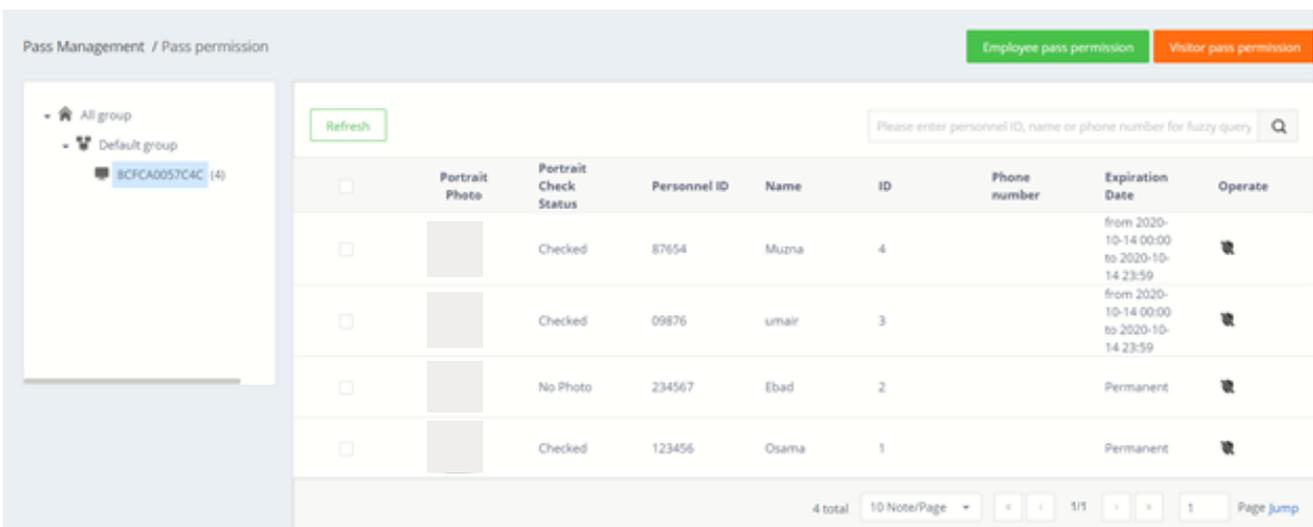
Regular Refresh:  Date Range: 2021-04-01 - 2021-04-01 Status: All Traffic Status: All

Type of access: All Enter name or device name for fuzzy query

Snap Photo	Name	Staff/Visit or	Body temperature	Pass status	Device Name	Access Direction	Door Status
No Data							

### 6.2. Pass permission

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



Pass Management / Pass permission

Employee pass permission Visitor pass permission

Refresh

Please enter personnel ID, name or phone number for fuzzy query

	Portrait Photo	Portrait Check Status	Personnel ID	Name	ID	Phone number	Expiration Date	Operate
<input type="checkbox"/>		Checked	87654	Muzna	4		from 2020-10-14 00:00 to 2020-10-14 23:59	
<input type="checkbox"/>		Checked	09876	umair	3		from 2020-10-14 00:00 to 2020-10-14 23:59	
<input type="checkbox"/>		No Photo	234567	Ebad	2		Permanent	
<input type="checkbox"/>		Checked	123456	Osama	1		Permanent	

4 total 10 Note/Page 1/1 Page Jump

## 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.

#### Step One: Employee Selection

<input type="checkbox"/>	EmployeeID	Name	Phone number	Creation Time
No Data				
0 total   10 Note/Page   < < 1/0 > >   1   Page Jump				

#### Step Two: Device Selection

##### Alternate Device List 0 / 1

- All group
- Default group
  - 8CPCA0057C4C

##### Selected Device List 0 / 0

No Data

#### Step Three: Permission status selection

Pass permission ⓘ
  Revoke Permission ⓘ

Permanent
  Period Selection

## 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.



Device Name	Permission Progress	Number of failures	Number of success
BCFCA003TC4C	0/2	0	0

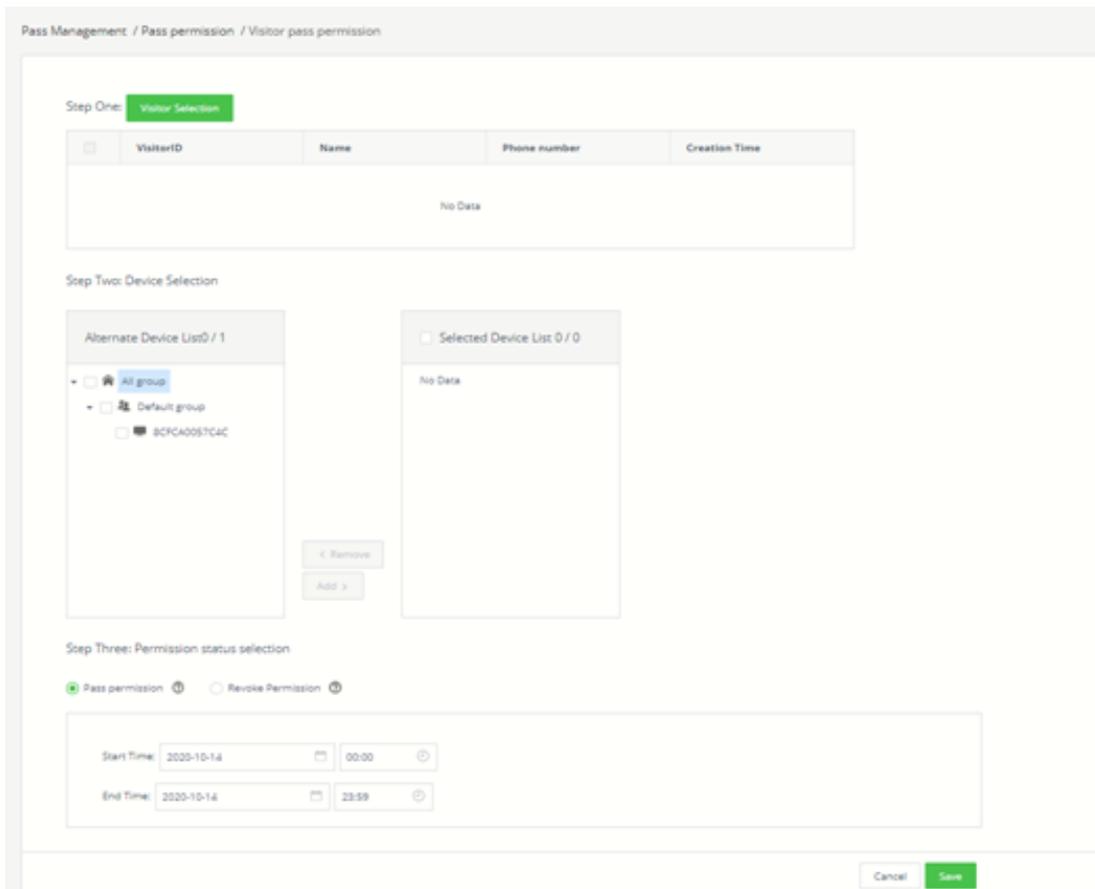
## Revoke pass permission:

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.



Pass Management / Pass permission / Visitor pass permission

Step One: **Visitor Selection**

<input type="checkbox"/>	VisitorID	Name	Phone number	Creation Time
No Data				

Step Two: Device Selection

Alternate Device List 0 / 1

- All group
- Default group
  - BCFCA003TC4C

Selected Device List 0 / 0

No Data

Step Three: Permission status selection

Pass permission
 Revoke Permission

Start Time: 2020-10-14 00:00  
End Time: 2020-10-14 23:59

## Details of Pass Permission:

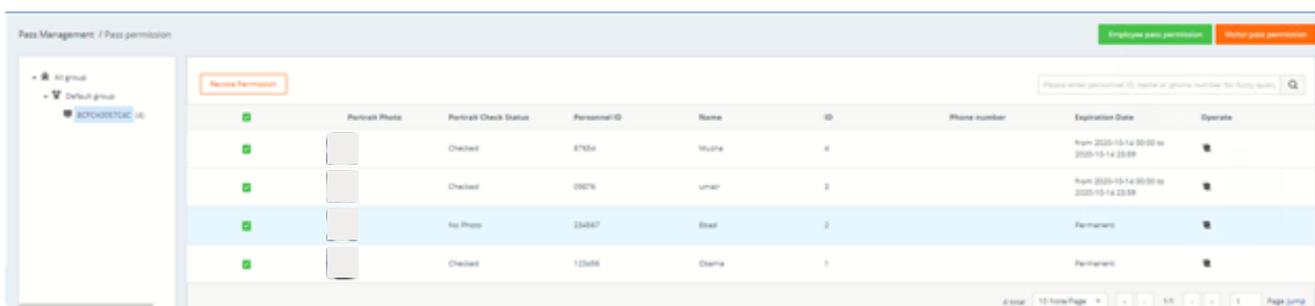
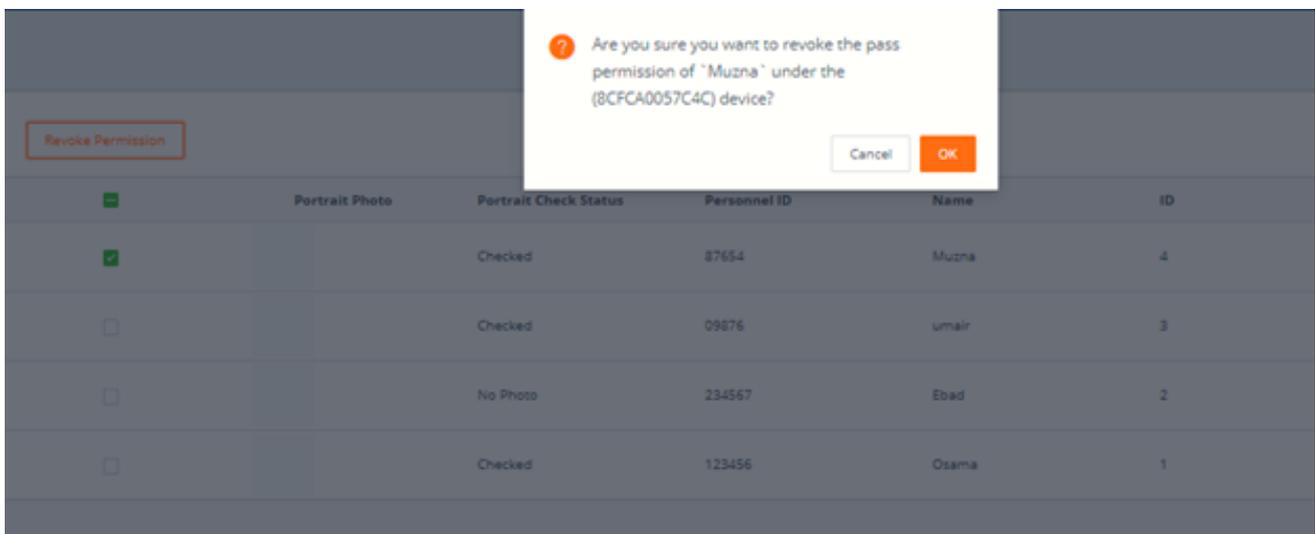
- Click Save to start pass permission. You can see the current synchronization status of each device in the form of a list showing the device name, synchronization pass permission, number of successful and failed authorizations. The person who failed authorization is recorded in the “Verification Failure 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 permission 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.

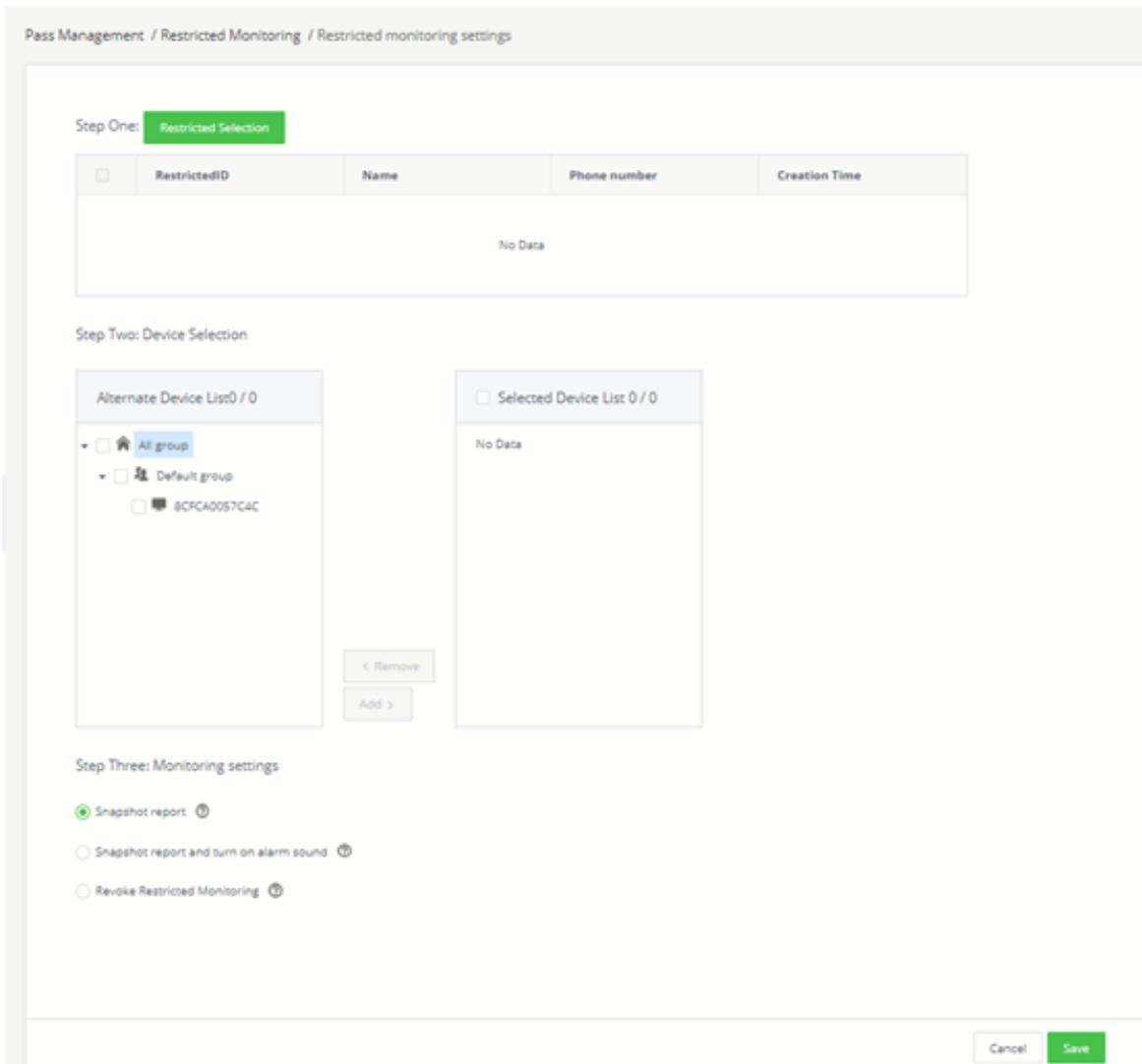
## 6.3. Restricted Monitoring

### 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.



Pass Management / Restricted Monitoring / Restricted monitoring settings

Step One: **Restricted Selection**

<input type="checkbox"/>	RestrictedID	Name	Phone number	Creation Time
No Data				

Step Two: Device Selection

Alternate Device List 0 / 0

- All group
- Default group
  - BCFG0057C4C

Selected Device List 0 / 0

No Data

Step Three: Monitoring settings

Snapshot report ⓘ

Snapshot report and turn on alarm sound ⓘ

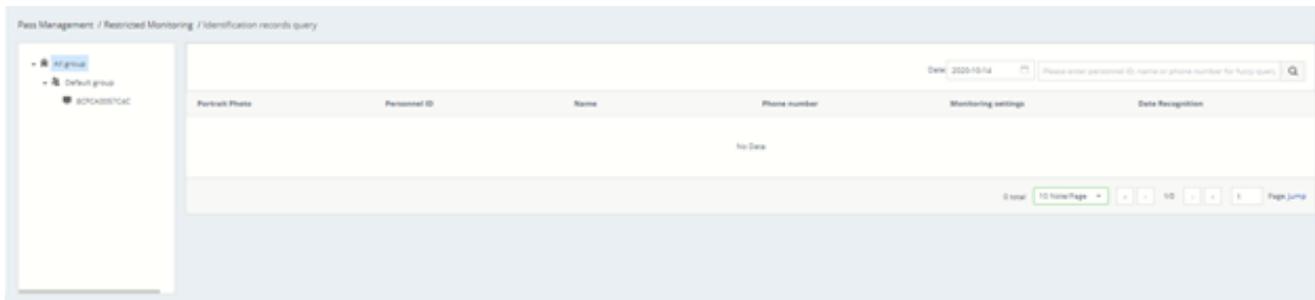
Revoke Restricted Monitoring ⓘ

## 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.

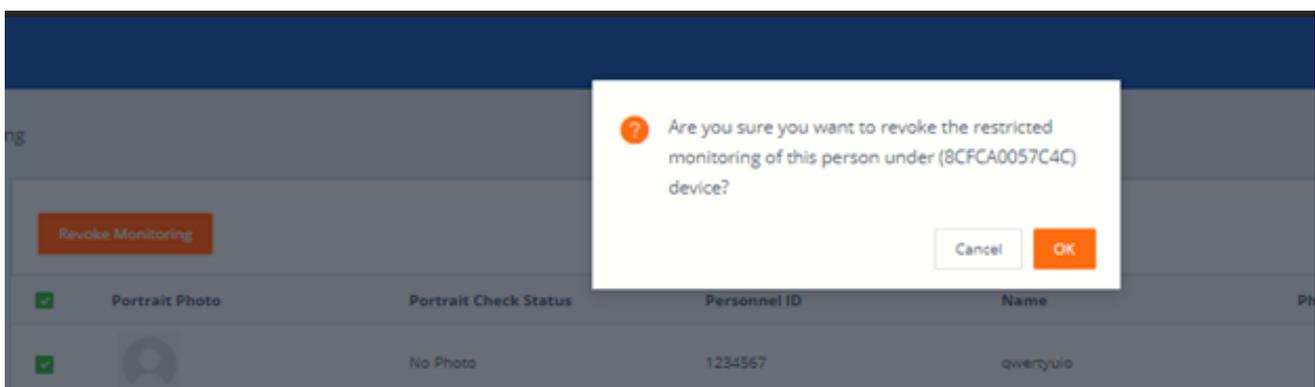
### 6.3.2. Identification records

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.



Pass Management / Restricted Monitoring

Search: [Personnel records query] [Restricted monitoring settings]

Needs Monitoring

Please enter personnel ID, name or phone number for fuzzy query.

Person Photo	Person Check Status	Personnel ID	Name	Phone number	Monitor settings	Created date	Operate
	No Photo	1234567	xxxxxx		Snapshot report	2020-10-14 9:07:54	

1 total | 10 Rows/Page | Page Jump

## 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.

Pass Management / Permission Records

Select date [ ] Search

Serial Number	Operator	Type	Status	Time	Operate
14	admin	Restricted Monitoring	Not synchronized	2020-10-14 9:09:08	
13	admin	Remove Restricted monitoring	Sync Complete	2020-10-14 9:09:10	
12	admin	Restricted Monitoring	Not synchronized	2020-10-14 9:09:06	
11	admin	Employee Permission	Not synchronized	2020-10-14 9:20:07	
10	admin	Employee Permission	Not synchronized	2020-10-14 9:21:03	
9	admin	Employee Permission	Not synchronized	2020-10-14 9:21:16	
8	admin	Employee Permission	Not synchronized	2020-10-14 9:21:01	
7	admin	Employee Permission	Not synchronized	2020-10-14 9:07:54	
6	admin	Employee Permission	Sync Complete	2020-10-14 9:20:38	
5	admin	Employee Permission	Sync Complete	2020-10-14 9:21:02	

14 total | 10 Rows/Page | Page Jump

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

Pass Management / Permission Records / Permission Details

Export failed personnel information

Time: 2020-10-14 12:39:59      Types: Restricted Monitoring      Operator: admin

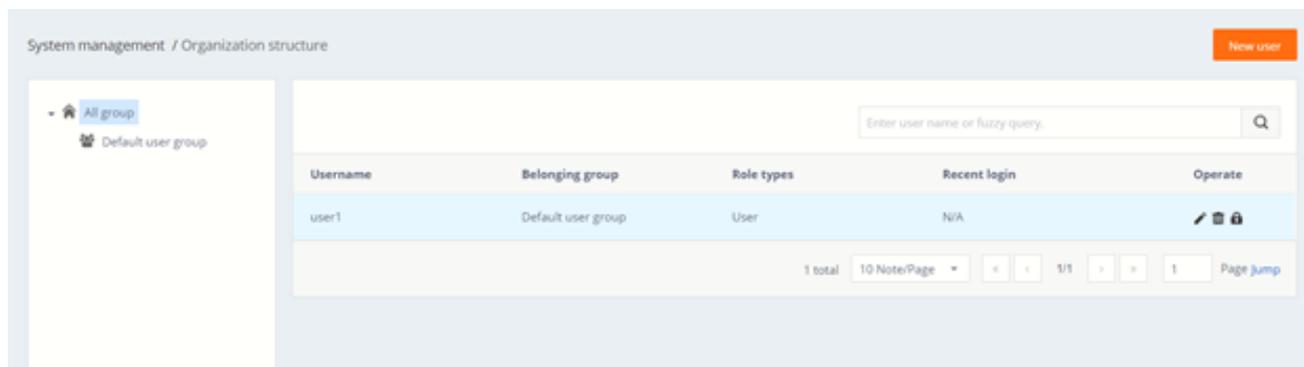
Device Name	Permission Progress	Number of failures	Number of success
BCFCAD0306FC		0	2
BCFCAD03A372		0	2
BCFCAD03BA43		0	2

## 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.

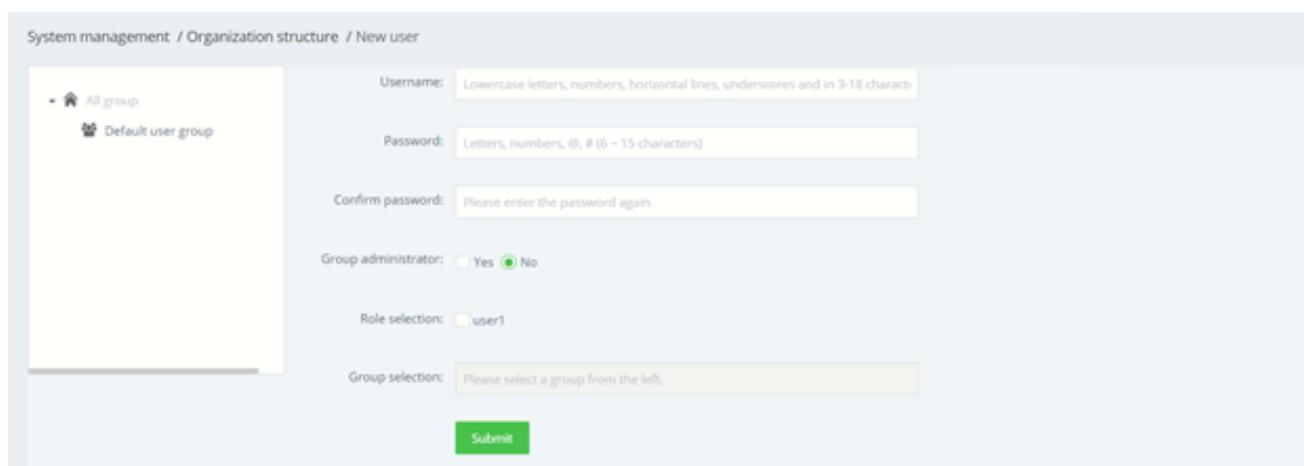


Device grouping can be done, and organization with the new assigned roles can be applied to specific devices in those groups.

#### 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

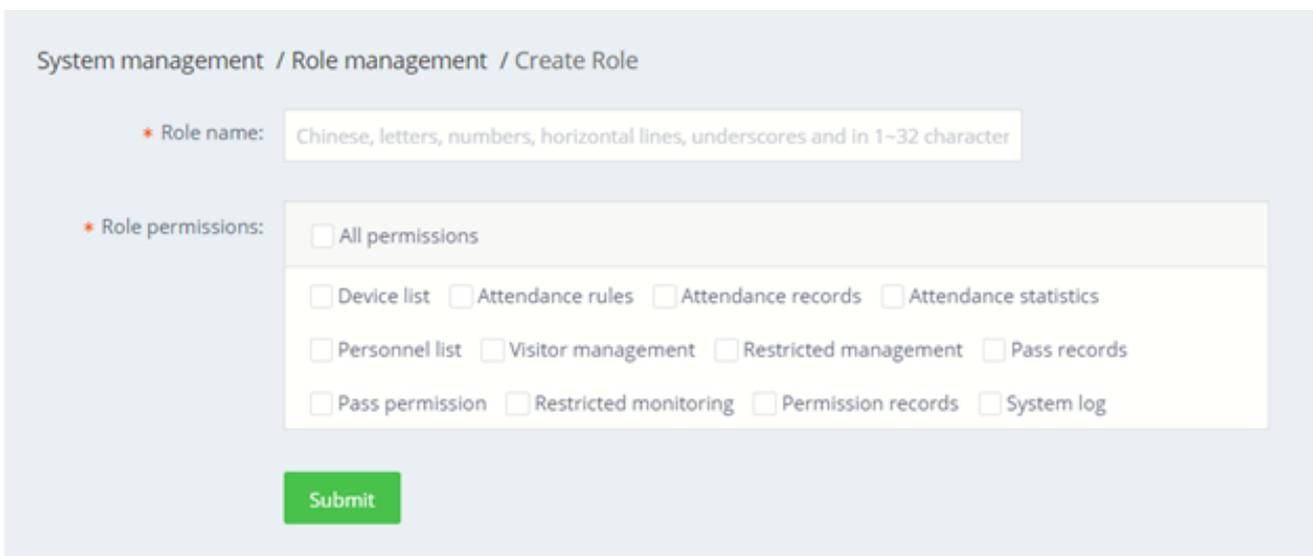
Role management allows you to create different roles, assign authority permission to that role, and this role is then linked to a user account created in the organization structure.

### 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.



System management / Role management / Create Role

\* Role name:

\* Role permissions:

- All permissions
- Device list  Attendance rules  Attendance records  Attendance statistics
- Personnel list  Visitor management  Restricted management  Pass records
- Pass permission  Restricted monitoring  Permission records  System log

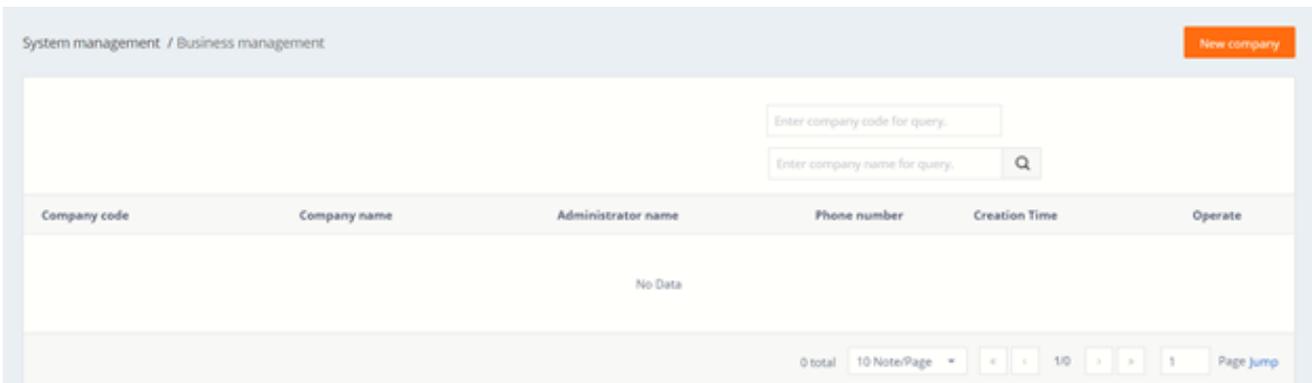
## 7.3. Business Management

### 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:



System management / Business management

New company

Enter company code for query.

Enter company name for query.

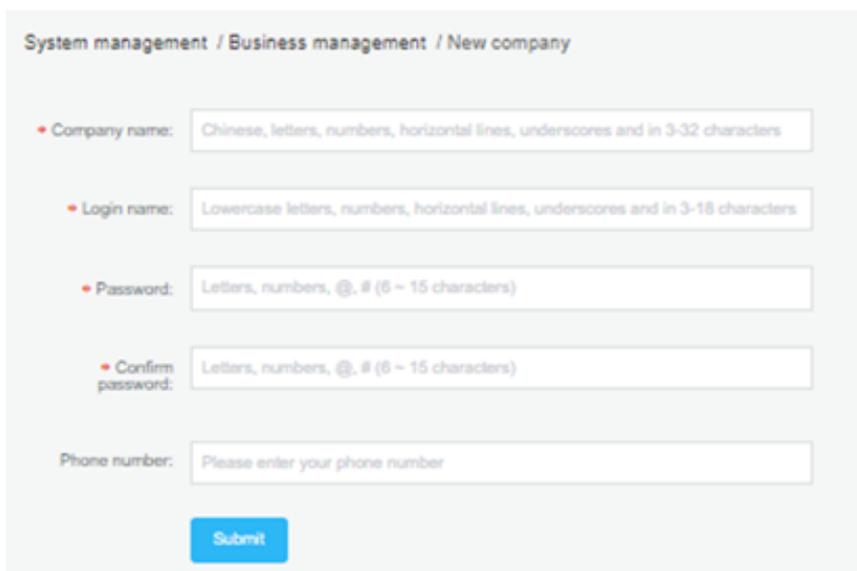
Company code	Company name	Administrator name	Phone number	Creation Time	Operate
No Data					

0 total 10 Note/Page   10   1 Page Jump

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:



System management / Business management / New company

• Company name: Chinese, letters, numbers, horizontal lines, underscores and in 3-32 characters

• Login name: Lowercase letters, numbers, horizontal lines, underscores and in 3-18 characters

• Password: Letters, numbers, @, # (6 - 15 characters)

• Confirm password: Letters, numbers, @, # (6 - 15 characters)

Phone number: Please enter your phone number

Submit

## 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.

System management / Business management New company

Company code	Company name	Administrator name	Phone number	Creation Time	Operate
3282829972073746	Company1	company_one		2020-10-14 09:53:00	

1 total | 10 Note/Page | < < 1/1 > > | 1 | Page Jump

## 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.

System management / Operation log

i The operation log only records important operations, not all user actions.

Functional module: 
Operation result:

Start Time: 
End Time:

Operation Date	Functional module	Log details	Operation result	Operator
2020-10-14 12:53:18	Business management	Add Company: Company1, Add User: company_one	● Succeeded	company_one
2020-10-14 12:50:31	User Management	Add user: user1	● Succeeded	admin
2020-10-14 12:50:10	User Management	Add role:user1	● Succeeded	admin
2020-10-14 12:40:00	Pass management	Set blacklist number employee:5	● Succeeded	admin
2020-10-14 12:39:10	Pass management	Delegating employees:5	● Succeeded	admin
2020-10-14 12:35:56	Pass management	Set blacklist number employee:5	● Succeeded	admin
2020-10-14 12:25:07	Pass management	Authorized number employee:2,1	● Succeeded	admin
2020-10-14 12:21:54	Pass management	Authorized number employee:2,1	● Succeeded	admin

## 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.

System Settings	Integrated Services	Prescreen Integration
Version: MIPS_GATE_Basic_v1.2.7		
System current time: 2021-04-01 15:01:23		
Backstage service port:	<input type="text" value="9000"/>	
	9000~9999 between	
Message service port:	<input type="text" value="7788"/>	
	7000~7999 between	
Database service port:	<input type="text" value="3307"/>	
	3000~3999 between	
Email Settings:	<input type="button" value="Settings"/>	
Temperature display mode:	<input checked="" type="checkbox"/> Celsius	<input checked="" type="checkbox"/> Fahrenheit

## 7.5.1.1 Email Settings

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

### Email Settings

---

#### Sender Information

\* Email Type:  Office  Other Email

\* Sender Email Account:

Email Password:

\* Email Password:  IMAP  SMTP  POP3

\* Email Server:

\* Port Number:

Email Sending Cycle Setting :  One Week  One month

Email Content Settings: Abnormal body temperature.  OFF

Attendance records  OFF

---

#### Recipient Information

\* Recipient email account

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.

Guru URL:   
[Set default URL](#)

Identify Guru:

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.

Face Detection:  ON

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)

Face Recognition:  ON

## 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.

Mask Detection:  ON

## Employee/Visitor Sync

Employee/Visitor sync is used to share the database of 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).

Employee/Visitor Sync:  ON

## 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.

Badge Printing:  OFF

## 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)

Attendance from GoSafe Management Platform:  OFF

## 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)

Block stranger from GoSafe Management Platform:  OFF

## 7.5.2 Integrated Services

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

System Settings	Integrated Services	Prescreen Integration		
Name	User	Password	URL	Operate
● Active Directory				INTEGRATE

### 7.5.2.1 Integrate

Simply fill in the required information, with the relevant credentials

### Integration

\* User

\* Password  

\* URL

Secured  No

Port   
Default port is 389

### 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

System Settings	Integrated Services	Prescreen Integration
<b>Integrated Information</b>		
License Key	6c63ad69f8e9a463f08a471decc813023d5084640478b3dc598733aa9c512cab_1	
License Status	✔ Active	
Allowed Devices	Unlimited	
IP Address	115.186.147.190	
Version	Ver. 1.2.24	
<a href="#">Forcefully Remove Integration</a>		

## 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](mailto:sales@onescreensolutions.com)