Smart Pass Operation Manual

contents

1. Server Software Installation and Sign in

1.1. Installation Steps

Run Smart Pass v x.x.x.x.x.exe as an administrator to installation.

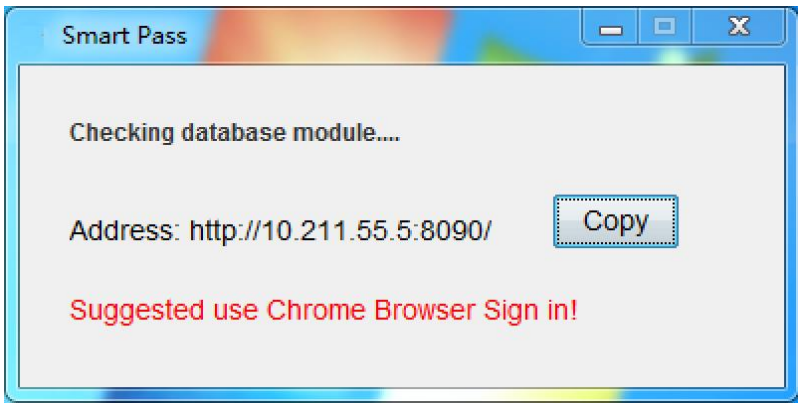
1.1.1. NOTES

(1) Try not to change the default path when installing, and only change the volume if you must;

(2) If anything goes wrong during the installation, you can copy the installation package to the desktop before installing, because the foreign operating system may not recognize the path, resulting in the installation error;

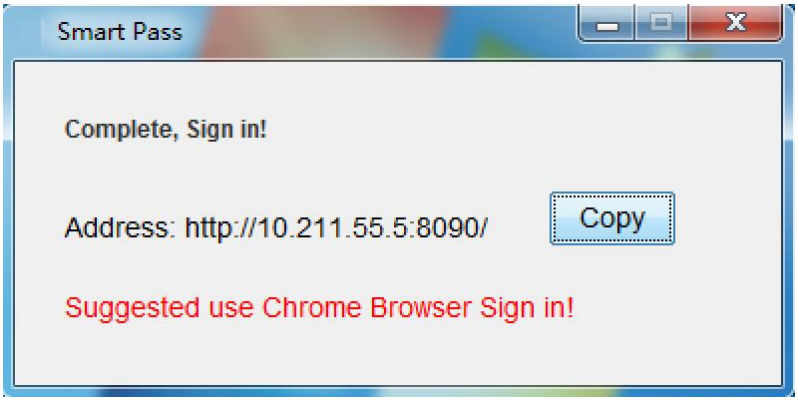
(3) If security software blocker running during installation, select allow to run;

(4) After the installation is complete, restart the computer, open the Application desktop shortcut, and the following screen will be displayed, indicating that the software is starting.



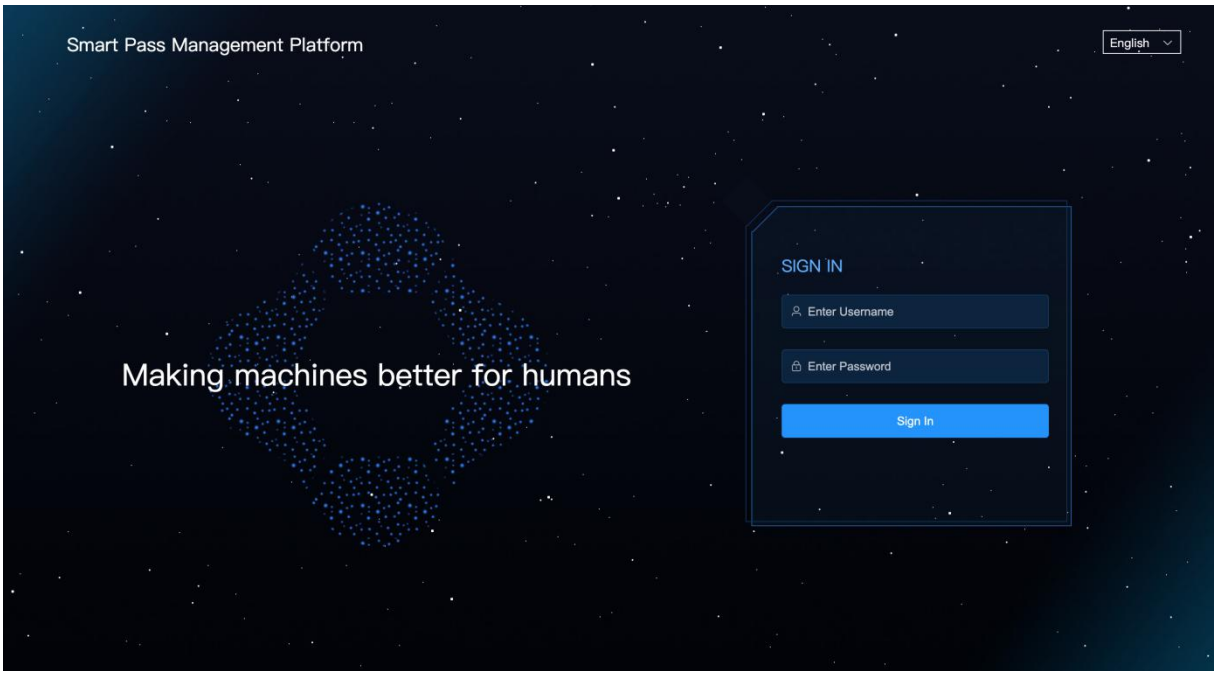
1.2. Start up and Sign in

(1) The boot process is displayed in the boot window, and when display : Complete, Sign in! , it indicates that the start up is complete and you can sign in;



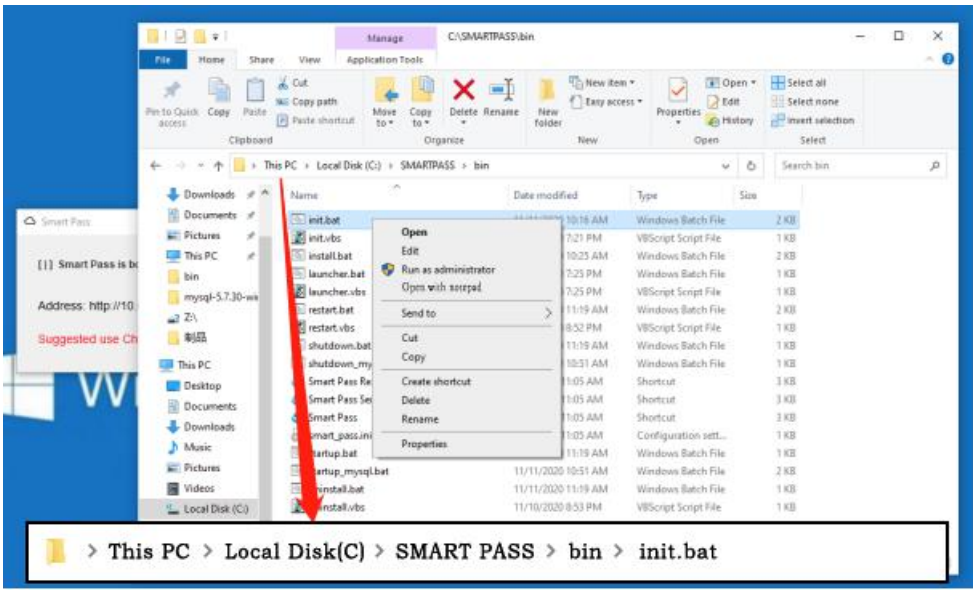
(2) Copy the IP address of the launch window (click the Copy button), paste it in Chrome and open it;

(3) Default login account admin, password 123456.

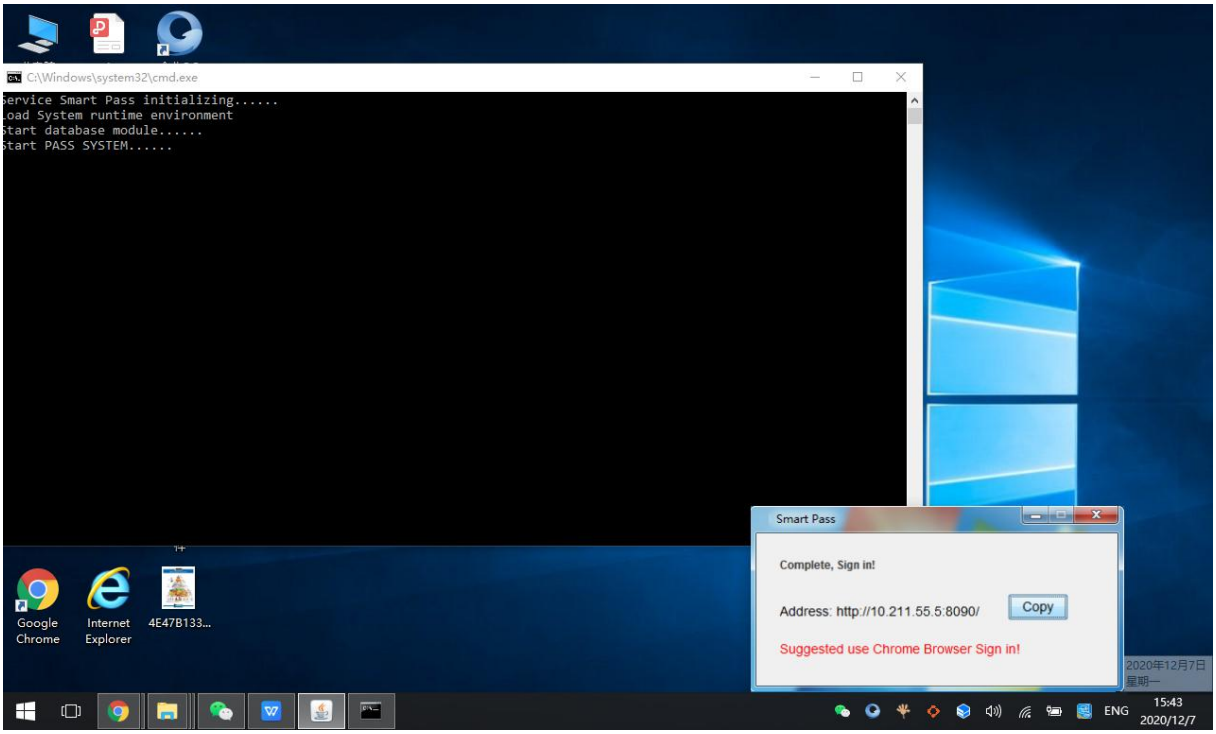


1.2.1. NOTES

If the software is always in "smart pass is booting, please wait..." and fails to start normally, please use the administrator's permission to execute the script: C: "Smart Pass / bin"\ in it.bat.



Until it can start normally, you can close the following black boxes:



1.3. Update

Run smart pass update installer V x.x.x.x.x.exe as an administrator to upgrade the software. After upgrading, the start up program is consistent with the installation program.

2. Device

2.1. Device APP Installation and Update

2.1.1. App Installation

To install smart pass app on the device, you need to install Smart Pass_ GATE_ Basic_ x. Install the x.x.x.x.APK into the U disk, connect the device for installation, find the USB storage in the device resource manager, and click the installation program to install.

2.1.1. App Remote Update

Upload update package in software server to update device remotely (refer to 9.1).

2.2. Device Basic Operation

(1) Connect the mouse with the USB interface. Click the application icon on the desktop of the system to start the software. Long press the desktop icon and drag it to the trash can to uninstall the application.

(2) Click the right mouse button to return to the superior menu or exit.

(3) If you need to switch the language, select setting - language and input method - language on the desktop of the system, select the required language box and drag it to the top of the list with the left mouse button, then the device will switch to the language and broadcast the voice in that language.

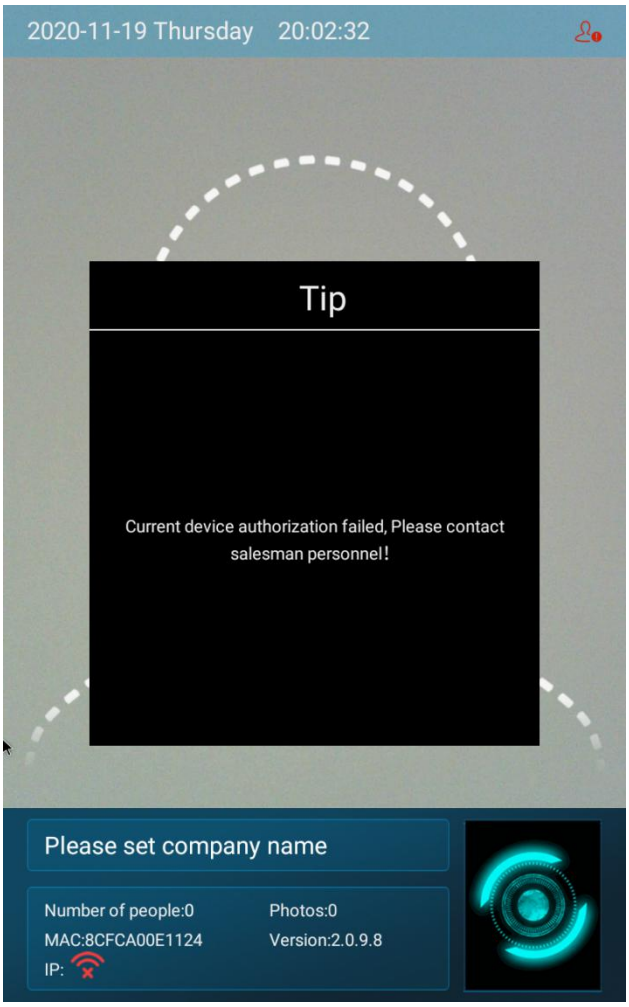
(4) When the application is running, the middle key of the mouse wheel can enter the software Settings (you need to enter the application password).

(5) When the application is running, right mouse button can exit the application and return to the desktop (need to enter the application password).

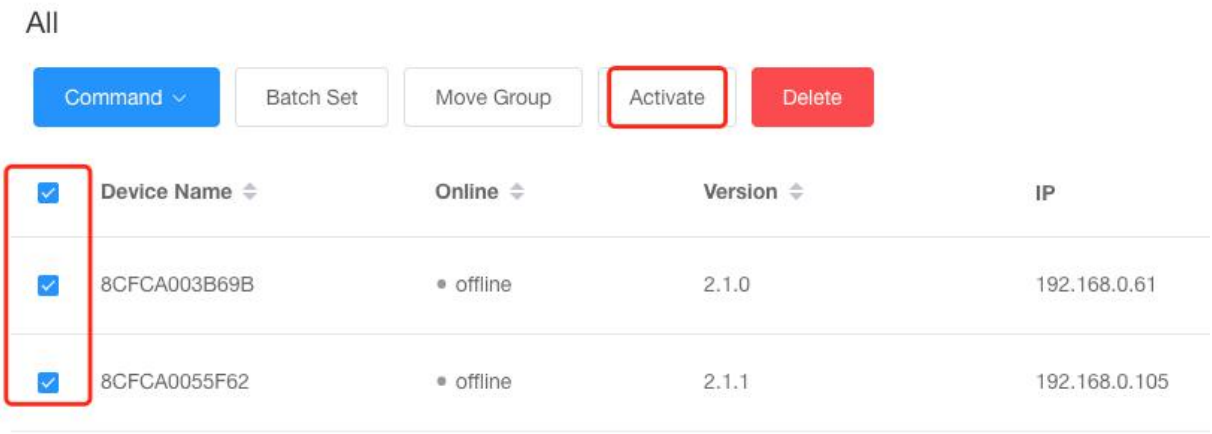
2.3. Activate Unauthorized Devices

2.3.1. Network Remote Activation

(1) Unauthorized new devices will enter the unauthorized screen after start up, and you need to log in with a certain number of activation codes to activate the corresponding number of devices;



(2) In the device management page, select the inactive device by radio or batch selection, click "Activate" (the activated device will not be activated again), the device will be activated, and the screen will exit the inactive interface;



(3) The activated device will automatically connect to the LAN server. If it cannot connect automatically, you need to manually enter the SERVER IP address to connect (refer to 2.3).

(4) The activated device is automatically associated with the default attendance group。

2.3.2. USB Flash Disk Activation

Insert the U disk containing the authorization file compression package, and the device will automatically import the authorization file after automatically identifying it.

2.3.3. NOTES

(1) One activation code can only activate one device, and no more devices can be activated after exceeding the number of super administrator accounts;

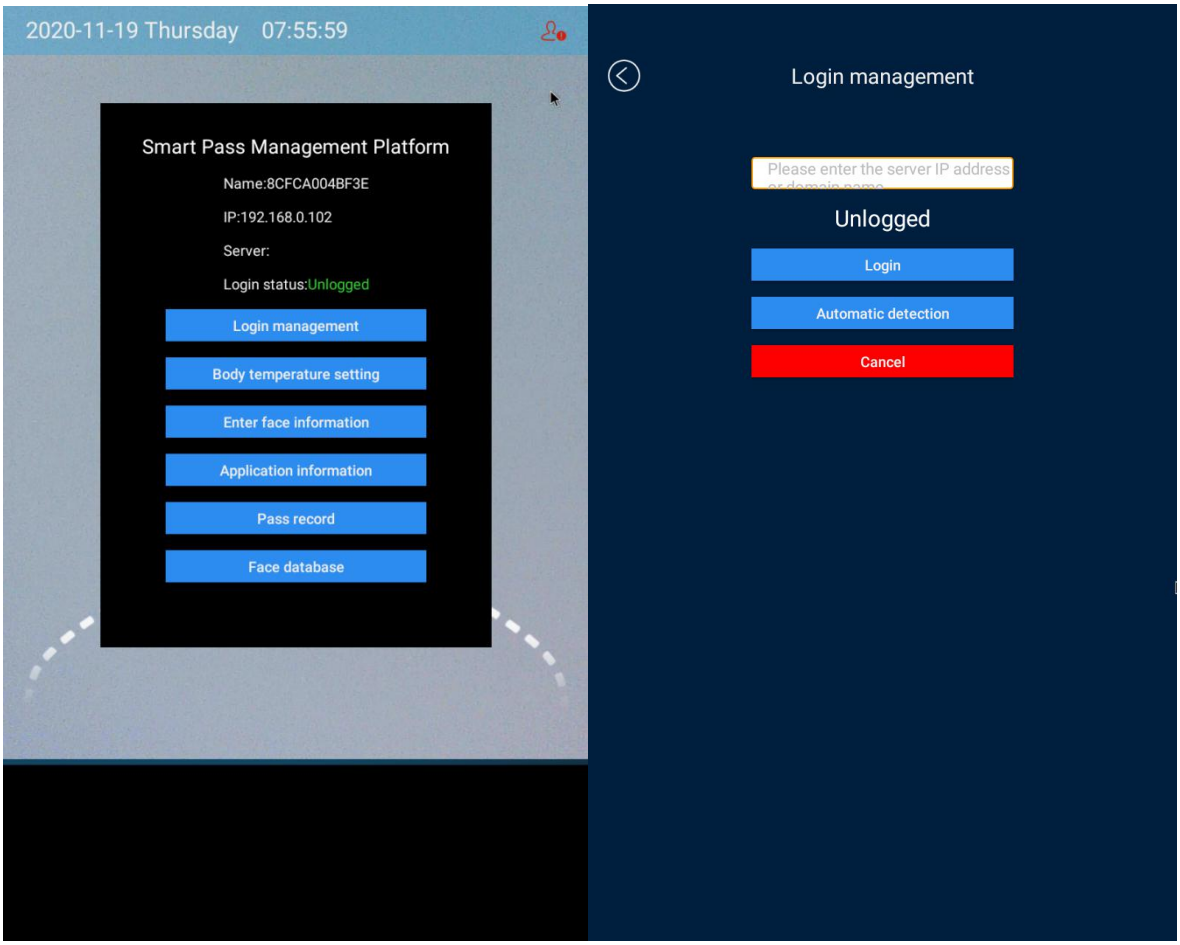
(2) When the device is not activated, face recognition, temperature measurement and other functions are not available, and the main interface will prompt that the device is not authorized; but you can turn the switches on and off;

(3) If the device has been activated, but the authorization file disappears, then the device will be reconnected to the Internet or the USB flash disk will be activated.

2.4. How Does Device Connect to LAN Server

Under normal circumstances, the device and the LAN server in the same network, that is, will automatically connect to the server, if there is no automatic connection,

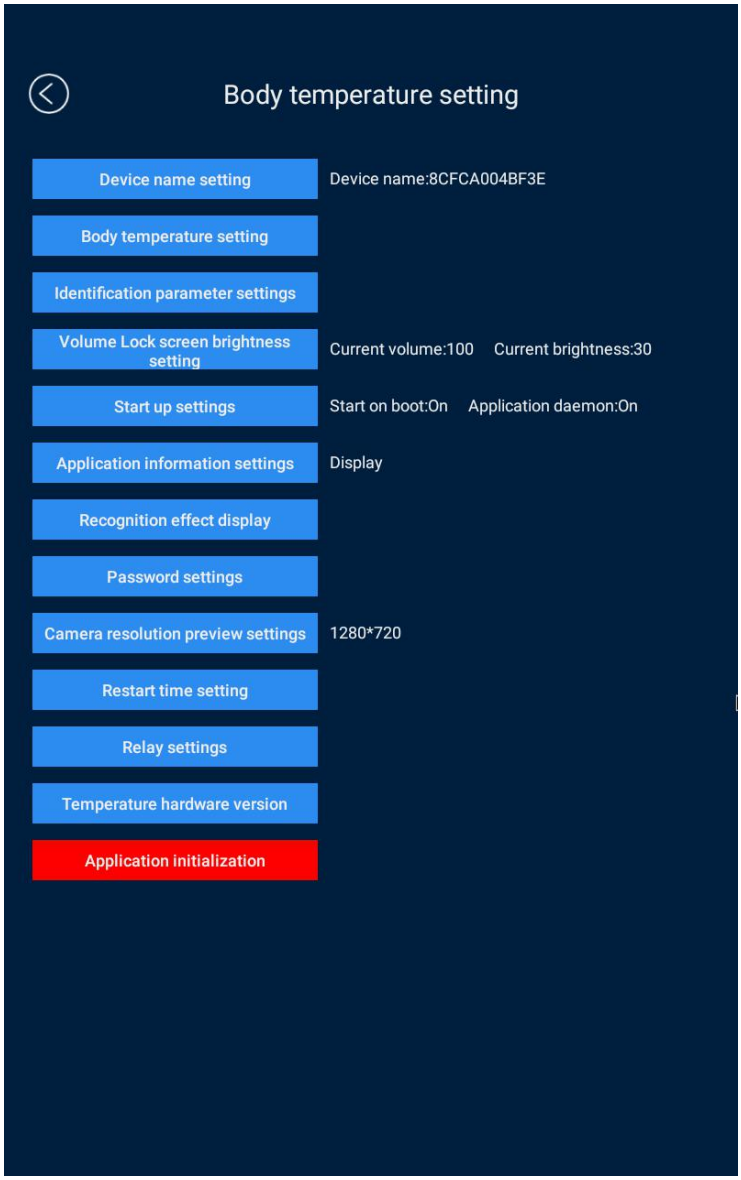
access the mouse, click the middle button of the mouse to open the menu interface, select login management, input LAN IP address and login, you can connect to the LAN server.



2.5. Device Parameter Settings

2.5.1. Login Management (refer to 2.4)

2.5.2. Temperature Settings



（1） Device Name Setting: Modify the device name and company name.

（2） Temperature Settings: Modify the temperature measurement parameters, including:

- Turn on and off of temperature detection
- Compensation temperature can be set automatically or manually
- Choose indoor/outdoor scenes
- Choose the temperature measurement mode (accuracy is the highest value for multiple temperature measurements, speed is the highest value for only one temperature measurement)
- Alarm threshold is set (if the temperature is above the set temperature, the device will alarm and is not allowed to pass)

- Set the minimum passage temperature (below which passage is not allowed)
- Temperature alarm can be turned on or off
- The temperature display is optional in Degrees Celsius or Fahrenheit
- Fans can be turned on or off
- Mask detection mode can be turned on or off
- Stranger mode can be turned on or off;

(3) Identification Parameter Settings: In-vivo detection can be turned on or off, which means whether the face recognition object is living or not (the static image is not passable); in-vivo detection can be turned off, which would not detect the object is living or not.

(4) Volume and Screen Saver Brightness settings: Adjust the audio volume and brightness of the device.

(5) Start up Settings: Set whether the application needs to be started automatically after start up, and the application daemon (the application will be automatically restarted no matter how it exits the application).

(6) Apply Information Settings:

- ●Application information can be selected to hide, that is, device settings home application information bar would be hide, and not show the application details.
- ●There are four modes for IC card setting, namely: turn off the card swiping function; turn on the card swiping pass and face recognition pass and temperature measurement; only turn on the card swiping pass and temperature measurement (face recognition is not recognized); and choose one of two modes: swiping pass or face recognition pass.
- ●The questionnaire mode can be turned on or off, and users can fill in the questionnaire before passing. Refer to 8.6 Questionnaire for details.
- ●When the advertising mode is on, it can play ads when devices are standby. When the mode is off, no advertising screen will be played.

(7) Identification Effect Display:

You can set the device to show the portrait and name when people passing, or only show the name.

- ●whether to turn on the red prompt light after identification is failed .
- ●Fill light optional white traffic lights or monochrome lights.

(8) Application Password Setting: You can modify the application password. You must enter the password when you enter the setting page from the face recognition mode, and exit the application with the right mouse button.

(9) Camera Resolution Setting: Modify the camera resolution of the device.

(10) Device Restart Time Setting: You can choose whether the device needs to be restarted or not. After setting the time, the device will automatically restart on time.

(11) Relay Setting: You can set how long the switch will close automatically after it is opened. You can also set the ALWAYS ON MODE,which the device would open forever unless you turn the mode off.

(12) Temperature Module Version: The temperature module version of the current device can be viewed and upgraded.

(13) Application Initialization: Return to the state after the device is activatied .

2.5.3. Enter Face Information

Entering face information is generally used in the case of device offline status, face information can be input and passed in the device. Local face information can only be staff identity.

2.5.4. Pass Record

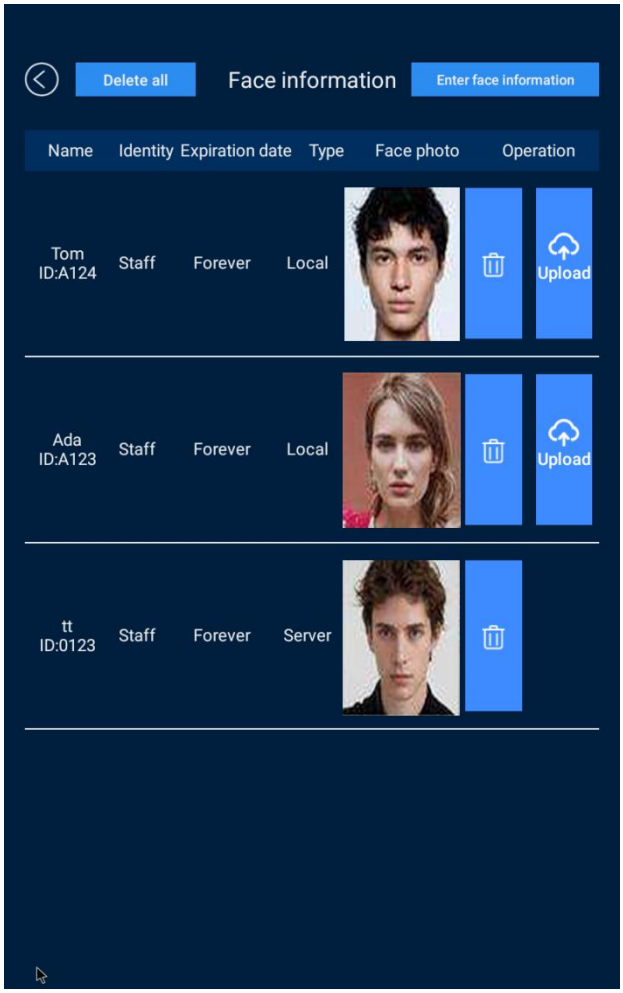
(1) All records of personnel access on this device can be checked by date.U can use a USB flash disk to export the records.

(2) To export the pass record, you need to insert a USB flash disk on the device. After the device prompts "USB Insert", click "Export", and the current pass records would be exported to the insert USB flash disk.

2.5.5. Face Information

(1) Face database displays all the face information synchronized from the server to the device and all local face information.

(2) When the device is connected to internet, the local face information can be uploaded in the face database, the data would be synchronized to the default group of staff management on the server, you can edit the information according to the server operation rules.



2.5.6. NOTES

(1) Among the above Settings, enter face information, IC card setting, compensation temperature, scene selection, fan setting, supplementary light setting, camera preview resolution setting, temperature module upgrading, etc. The above settings can only be operated in the device and cannot be controlled in the LAN server.

(2) Other Settings can be synchronized between the device and the server. If the modification is made on the device, the device can be synchronized in the background. If the modification is made on the [device management] parameter setting in the server background, the device can be synchronized.

2.6. Several Pass Mode

2.6.1. Face Recognition Pass

(1)Personnel information input from the server

On the server,in the personnel management, the personnel information can be input and the face information can be uploaded. When those personnel pass, the captured face would be compared with the face information stored on the server. If the comparison is successful, the personnel can pass through. When the stranger mode is enable, if the comparison fails, the personnel would be regarded as a stranger; when the stranger mode is disable, the comparison fails,the personnel would not be allowed to pass.

(2)Local information input from the device

The personnel information can be input whether the device connect the internet or not, and the information would be stored in the local device (they can be manually uploaded to the server in case of networking).The process of the local personnel passing is the same as personnel input from the server.

2.6.2. Slot Card Pass

(1) You should select the "card recognition first" in the information setting of the device setting menu, or the slot card pass of the access settings on the server, that is, if you have the card,you can slot it to pass;if you have no card ,you still can pass through by face recognition.

(2) In the personnel management of server,you should input and save the IC card number for the person who needs to pass by card. The user can pass by slotting the corresponding IC card on the device "CARD" area, while the IC card number that is not matched,then the user cannot pass. The face recognition process is the same as that in 2.6.1.

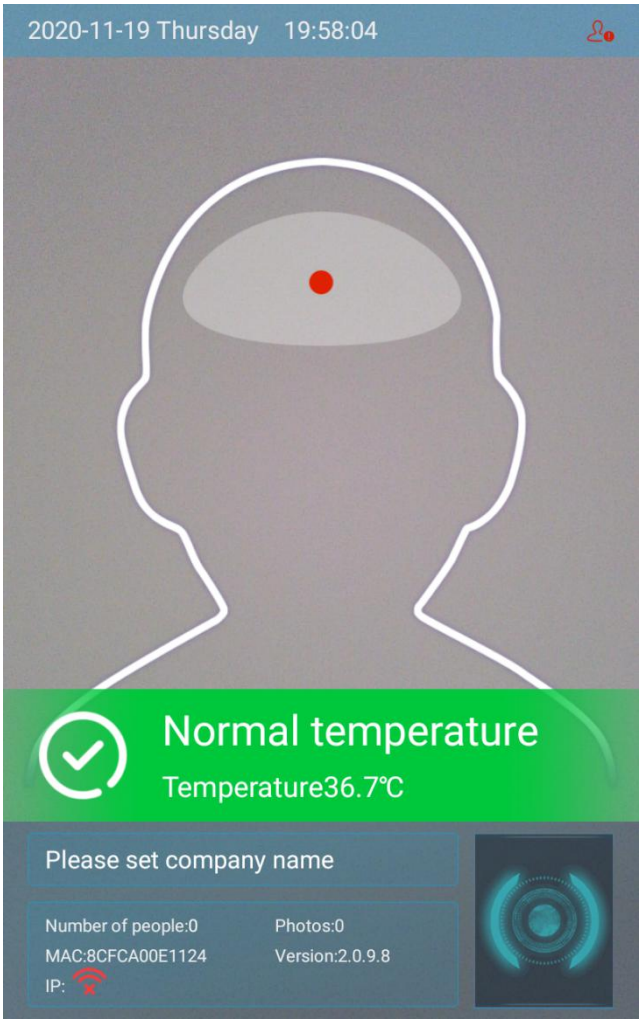
2.6.3. Slot ID Card Pass

Only the ID card slotting device can support the function. When the user slots the ID card, the device would compare the captured face with the ID card photo. If the face comparison is successful, the user can pass. If the comparison fails, the user is not allowed to pass.

2.7. Use Method of Device Stand-alone Version

(1) When the device is disconnected from the network, it will enter the stand-alone mode. The face recognition interface will be prompted by ICONS. The stand-alone mode can still recognize the face, swipe card and measure temperature, and the pass record will be stored in the device.

(2) When the device is offline (stand-alone mode), open the menu with the middle mouse button to modify or enter the face on the device (only stored in the device). When the device is connected to the Internet again, the face and other data entered on the device will be deleted, and the pass records would still exist in the device.



2.8. NOTES

(1) This product is not suitable for use in direct sunlight.

(2) This product is not suitable for outdoor or semi-outdoor use.

(3) The best use environment of this product is indoor, with no wind at 25℃ and temperature measurement distance of 50CM.

(4) When the ambient temperature is lower than 15℃ or higher than 30℃, the temperature measurement error will increase.

(5)

The measured person should have no strong light source directly on the for ehead and face, and no other high/low heat source interference.

(6) When the measured person comes from outdoors or from a place with a big difference from the measured ambient temperature, the measured person should stay in the measured environment for at least 5~10 minutes, and then measure the temperature after it is consistent with the ambient temperature. Otherwise, the accuracy of the measured result will be affected.

(7) The measured person should keep the forehead dry and and not be covered by hair, dust, hats, etc.

(8) Temperature measuring equipment can not be placed at the tuyere, because the cold and hot wind has an impact on the accuracy of temperature measuring equipment.

(9) Do not place this product near or on high temperature objects.

(10) The data measured by the infrared thermal imaging body temperature testing equipment are only used for preliminary screening and cannot be used as medical diagnostic data. Once high body temperature is detected, further screening is required.

(11) Calibration method: Please follow the following steps before using this product for tempera- ture screening:

a. Measure your own forehead temperature with the traditional calibrated high-precision forehead thermometer in the suitable environment for the use of this product, and assume 36.3℃ is obtained.

b. Use this product to measure your own temperature in the suitable environment for the use of this product, and assume that the temperature is 36.0℃.

c. Repeat step 1 and step 2 more than three times to calculate the difference value between the average value measured by the forehead thermometer and the average value measured by this product. If the error range is within 0.3℃, then this product can be used normally. If the difference value is too large, such as 1℃, then you need to long press the middle mouse button. After the dialog box pops up, enter 123456 to enter the apply settings and set compensation settings in the "Temperature Detection Settings".

(12) If you need to upgrade the machine, the power can not be cut off during the upgrade process. The power cut will cause the upgrade to fail, resulting in the failure to upgrade again, which needs to be disassembled.

(13) Note: This product is not a medical professional device!

The following is the LAN server operation guide:

3. System Dashboard

Dashboard display devices, personnel, access records and attendance summary statistics:

Including:

(1) Total users: total amount of users in system, including staff, visitors and residents.

(2) Total devices: total amount of devices in system.

(3) Total access of this month.

(4) Total stranger recognition times of this month.

(5) Access statistics of last 10 days, including times of access, times of stranger recognition, times of fever alarm.

(6) Statistics of devices, including online and offline.

(7) Yesterday attendance summary, including attendance, late arrival, early leaving, work overtime and absence.

(8) Latest 5 access records of today.

4. LAN Server Device Management

Device management displays the name, parameters and status of the connected devices, which can be remotely controlled and managed within the LAN, including device activation, switch opening and closing, parameter settings and so on.

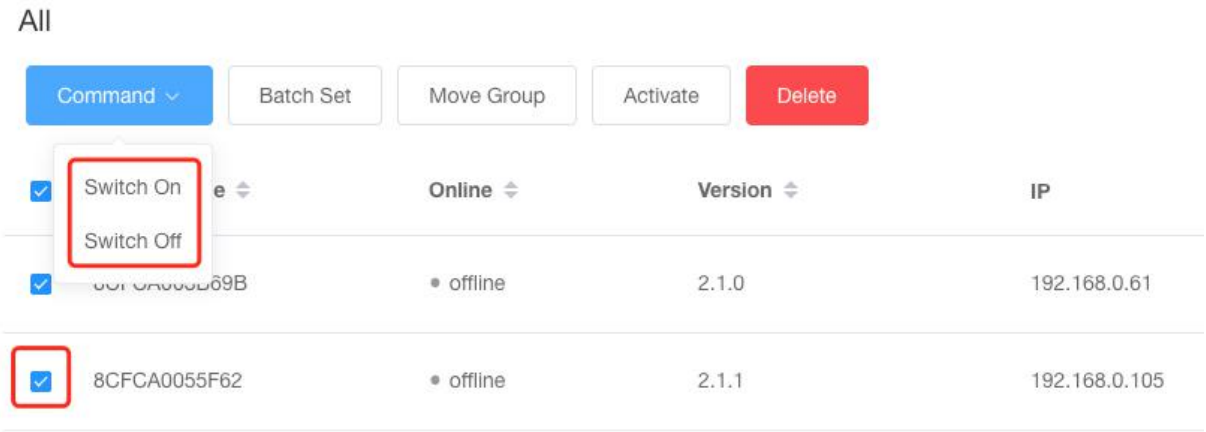
4.1. How does the device connect to the LAN server

When the device is connected to the computer installed with this software in the same LAN, the application on the device can be started to connect to the LAN server automatically or manually. The default initial state is inactive, which needs to be activated manually (refer to 2.3).

4.2. Device Activation (refer to 2.3)

4.3. Remote Control Device Switch On and Off

The command button of device management can control the switch on and off.



4.3.1. NOTES

When the device is offline, the switch command does not take effect. When the device is online, the switch can be controlled whether it is activated or not

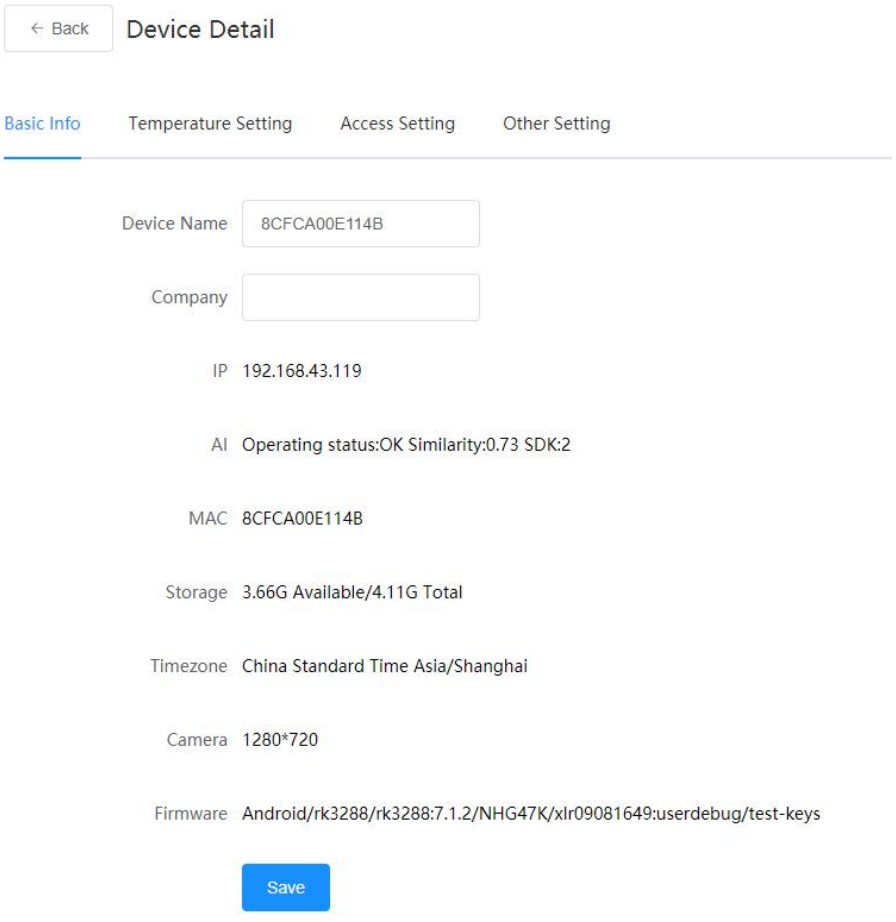
4.4. Device parameter setting

In the parameter setting on the right side of the device list, the parameters of each machine can be set, including basic information, temperature measurement, passage and other settings. The batch set button beside the command button can be set uniformly for multiple devices.

4.4.1. Basic Information

(1) The device name and company name can be set and displayed synchronously on the terminal device;

(2) Other parameters display the parameters of the terminal device by default.



4.4.2. Temperature Settings

(1) Temperature detect: The device would check the body temperature only when the temperature detect is enable, the device would not check the body temperature

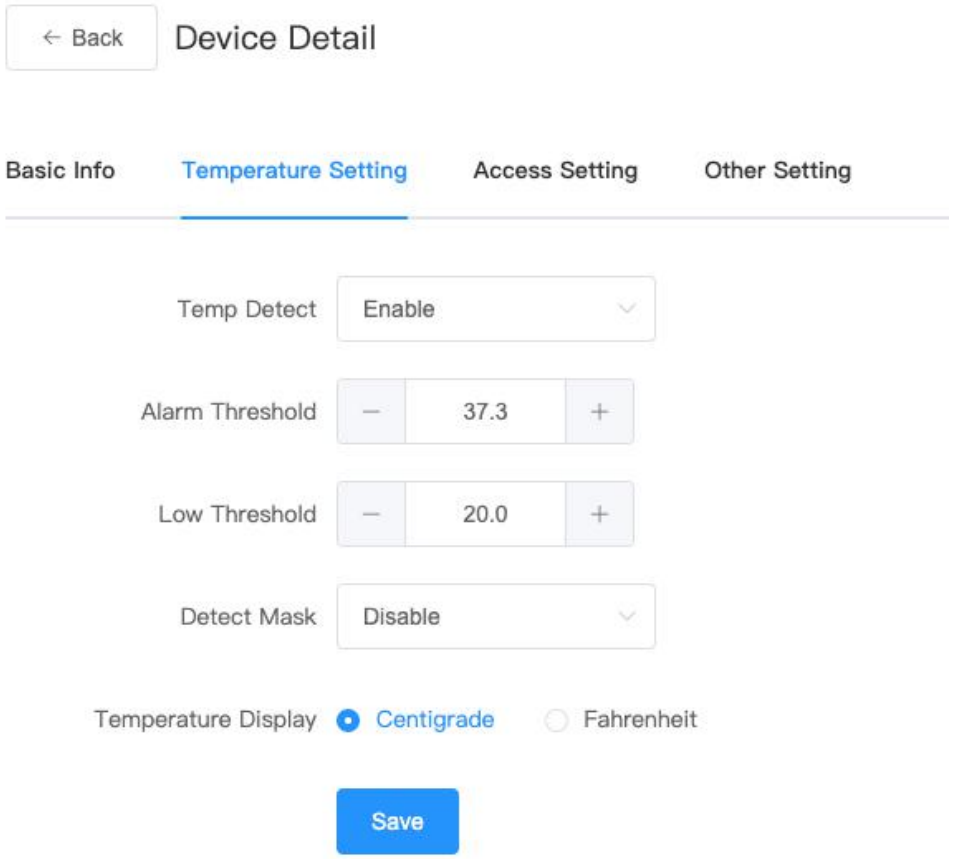
when temperature detect is disable.

(2) Alarm threshold: When the temperature is above the temperature threshold, the high temperature alarm will be issued.

(3) Minimum Pass Temperature: The device would not allow to pass if detected temperature is below the minimum pass temperature.

(4) When mask detection is on, users are allowed to pass only when they are recognized to be wearing masks. The terminal device without masks will voice prompt "Please wear masks" and it is not passable. After the mask detection is successful, users can pass;

(5) Temperature setting can be either Celsius or Fahrenheit.



4.4.3. Pass Settings

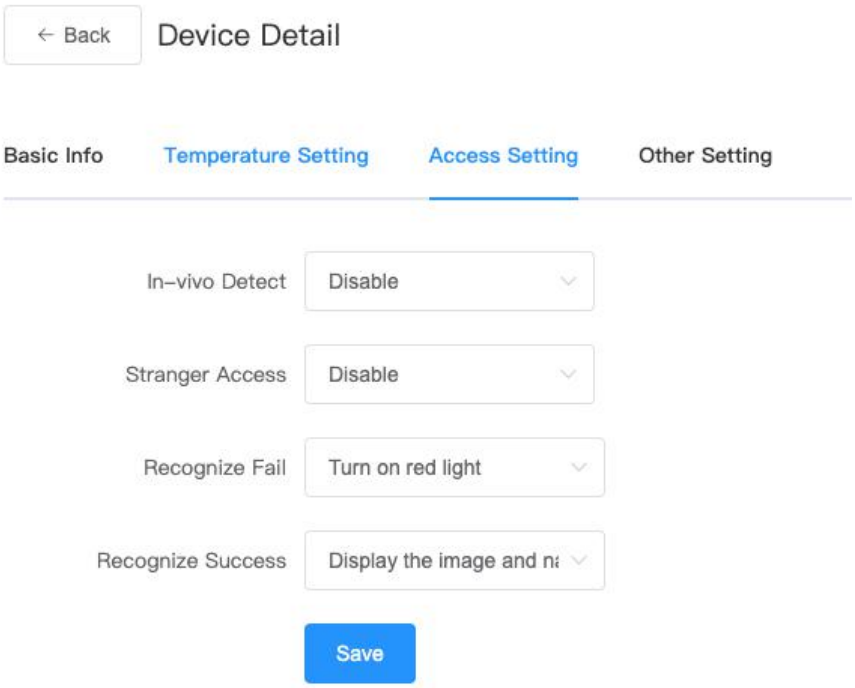
(1) In-vivo Detection: When it is enable, the device would detect whether the target is living, and would not identify static face photos, ;

(2) Stranger Pass: if it is enable, unauthorized users can pass, and when the staff in the attendance group passes, the device would prompt :clock in successful, and record

the attendance; if it is disable, unauthorized users cannot pass;

(3) Identification Failure: When identify failed, you can choose whether to turn on the red light or not;

(4) Identification Success: When identify successed, the portrait and name would be displayed or only the name displayed;



4.4.4. Other Settings

(1) Application acceleration: Speed first means the users pass the device faster, but the temperature measurement is relatively inaccurate; when accuracy first, the temperature of the users would be detected more accurate, but the speed would be slow;

(2) Application information: If choose to display, the application version and other information will be displayed on the device; if hidden, it would not be displayed;

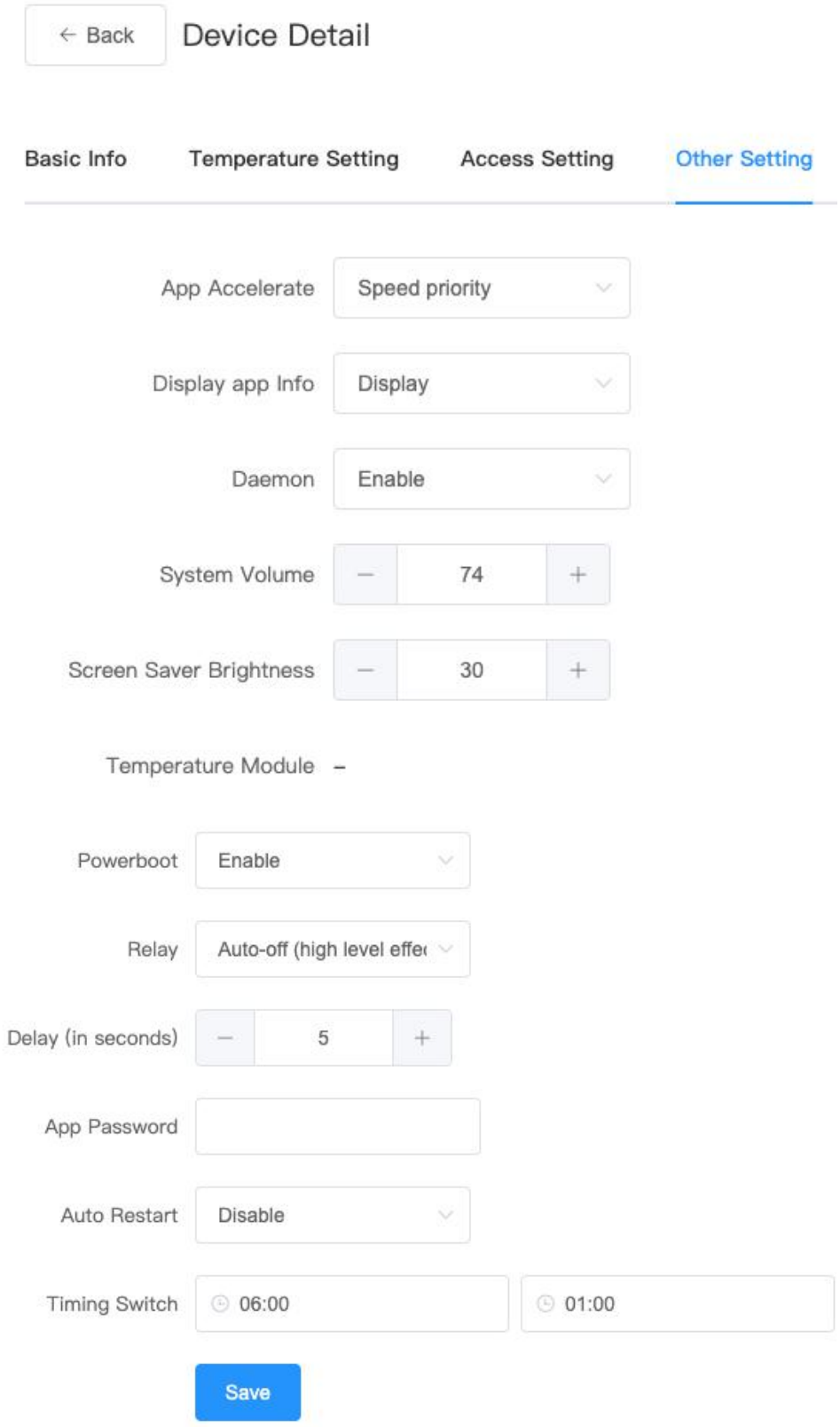
(3) Application daemon: If the application is started, it will automatically restart whether it is quited manually or automatically;

(4) Relay setting: If choose normally open mode, the device brake is normally open and would not be closed; If choose the automatic closing mode, the opening would be closed after a certain period of time. The delay term is used to set the automatic closing within a few minutes after opening;

(5) Temperature module: The version number of temperature measurement module information in the device;

(6) Application password: Modify the application password of the device (input when entering the menu and exiting the application);

(7) NOTES:All the above parameters can be set in devices, and the device and LAN server settings would synchronize with each other when they are changed.



5. Attendance Rules

Attendance consists of attendance group management, shift management and holiday settings.

5.1. Operational Sequence of Attendance Settings

5.1.1. Shift setting

Define work time, overtime and other time points in shift management. Each shift could set 1-3 shift periods.

5.1.2. Attendance group setting

The attendance group can define each day as work day or rest day, and the work day can be correlated with the required shifts.

5.1.3. Other Settings

Holiday time can be set separately. Overtime work on holidays, working days and public holidays shall be counted separately in attendance statistics, and holiday setting shall be effective for all attendance groups.

5.2. Attendance Group Management

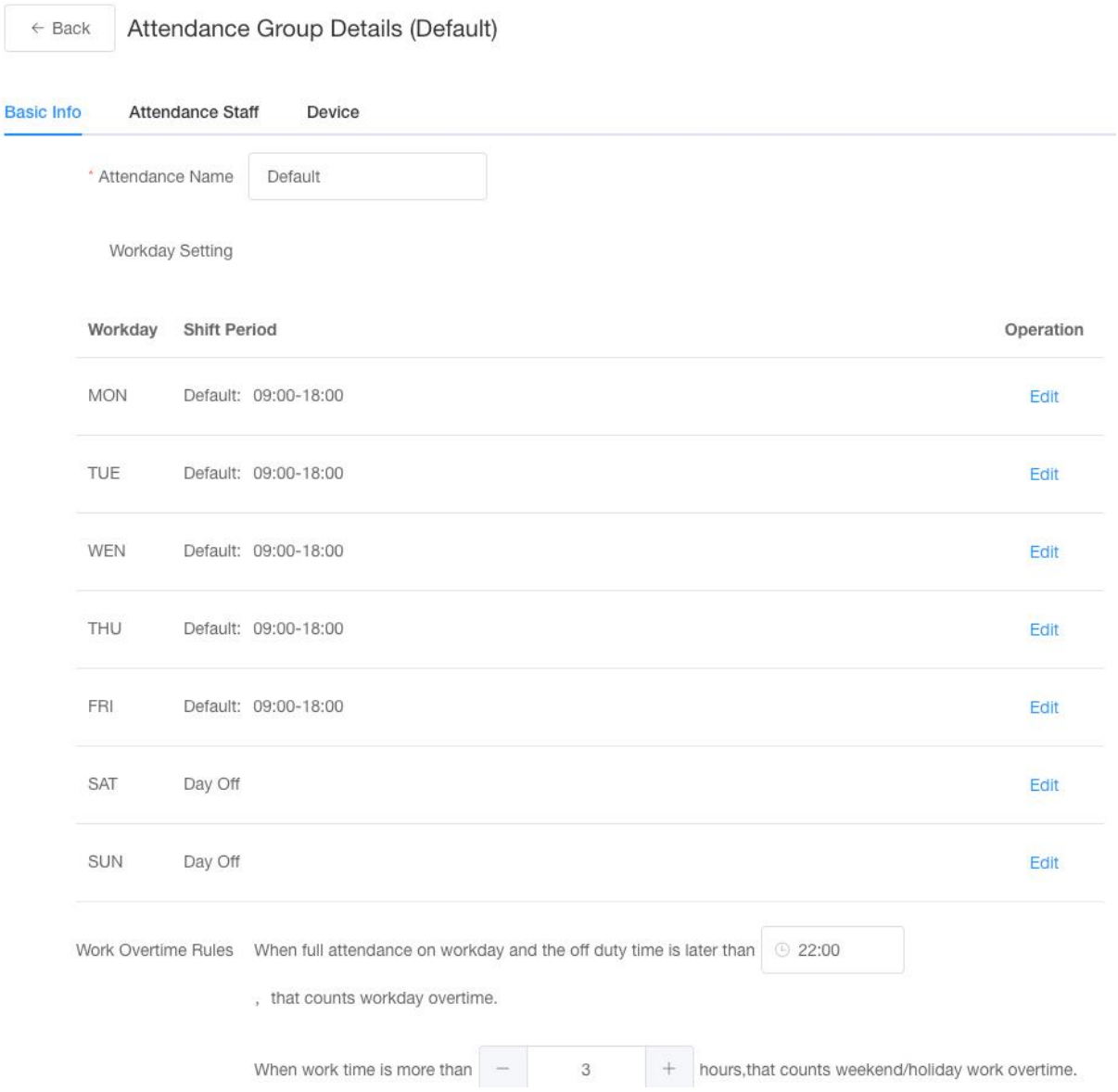
The attendance group management includes the name of the attendance group, the staff of the attendance group, and the pass devices associated with the attendance group. A default attendance group exists in the system, which can be edited but cannot be deleted.

5.2.1. Add and Edit Attendance Group

(1) The newly added or edited attendance group includes three functions: basic information, associated attendance personnel and associated devices.

(2) Basic information of attendance group

The new attendance group name can be customized for work days and weekends, with one shift associated with each work day, and overtime rules for work days and weekends can also be defined (weekends and public holidays' overtime rules are the same).

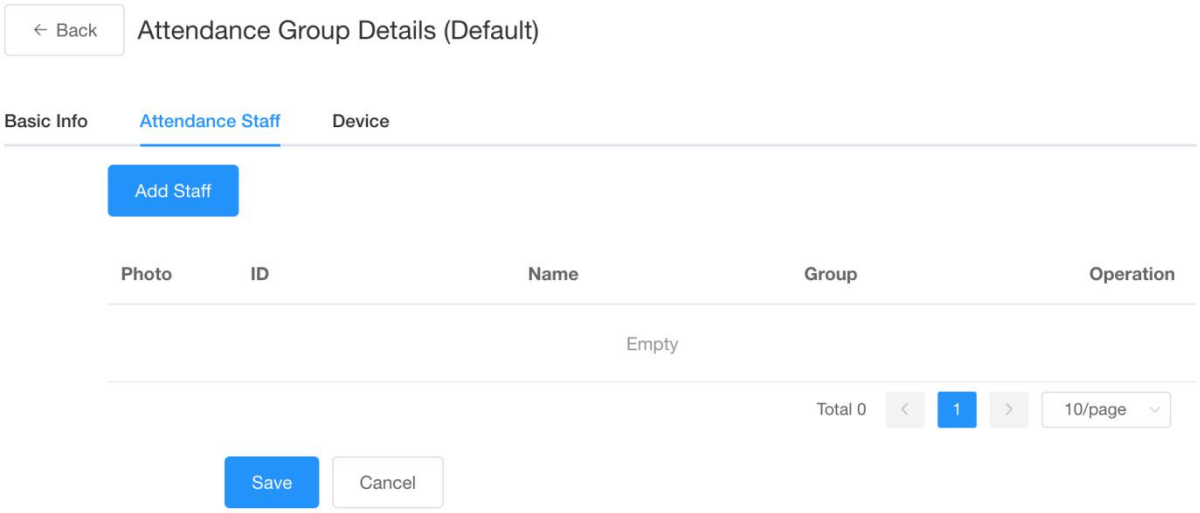


5.2.2. How to Add Staff to Attendance Group

(1) Select the attendance staff from "add a new attendance group" or the "edit" button of the attendance group, and then add the staff to the corresponding attendance group in batch. The staff already in the attendance group will be displayed in the list;

(2) NOTES

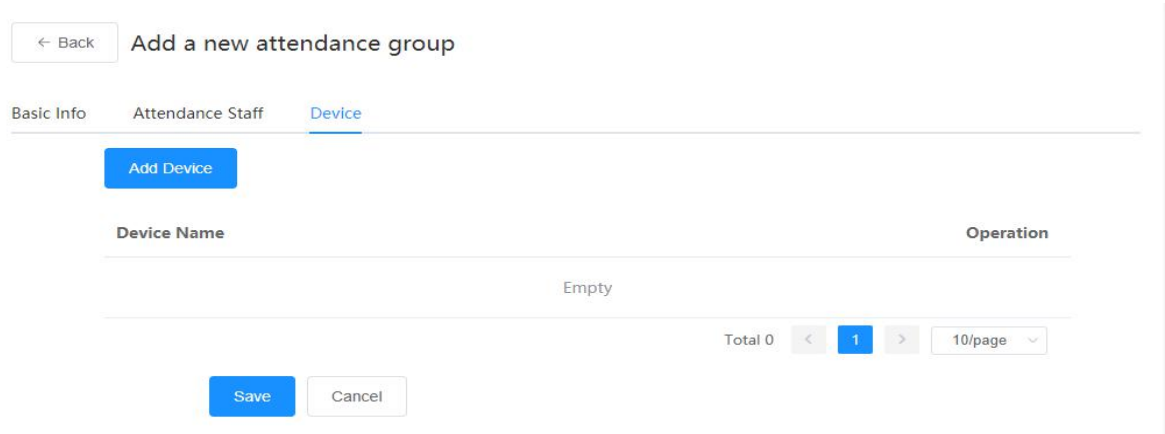
If delete staff from the attendance group, he/she still has the pass authority of the device associated with the previous attendance group, but their attendance would not recorded any more, and the deleted attendance records are still retained in the attendance
statistics.



5.2.3. Set up Attendance Devices

(1) In the "add" and "edit" attendance group, the attendance device can be selected, the added device can record the staff attendance of the group. After the added device is saved successfully, the access right of staff of the attendance group on the added device will be opened.

(2) If an attendance device is deleted, the staff of the attendance group shall not record the attendance on the device, but still have the access right of the device.



- Notes

(1) When a new device is activated and connected to the LAN, it would be automatically associated with the default attendance group, which can be deleted or added by your choice;

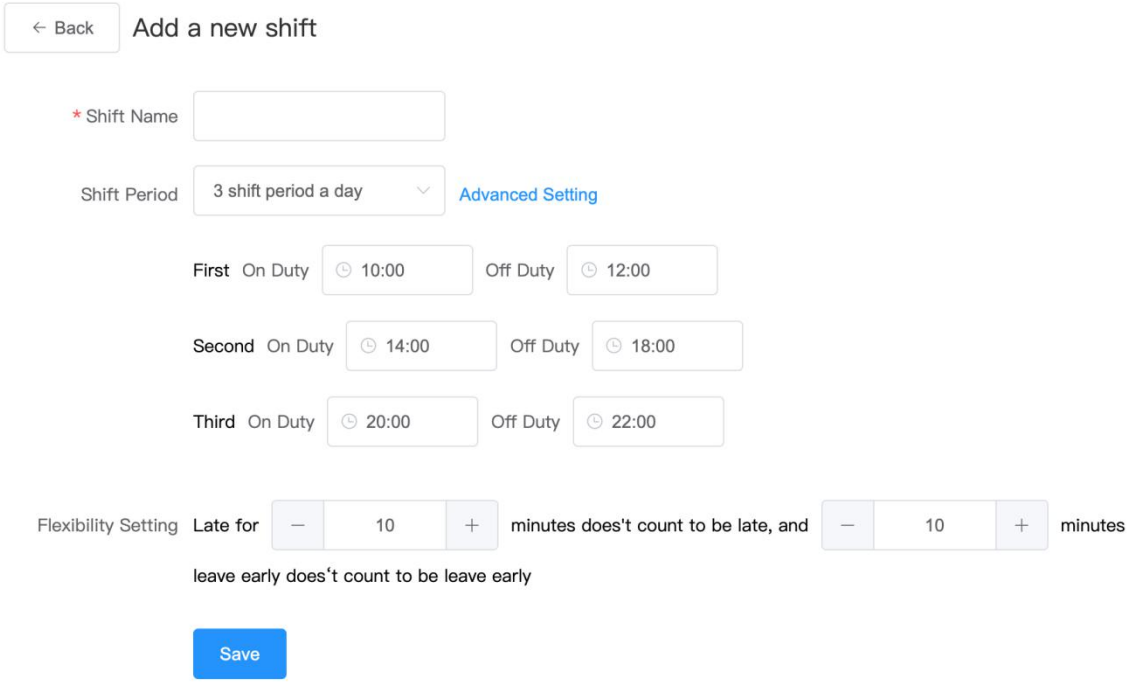
(2) Staff with pass authority of this device will be displayed in the list of access

authority (refer to 8.1).

5.3. Shift management

5.3.1. Shift Period Management

The shift defines the time period for recording attendance on working day, that is, Shift Period. 1-3 shift periods can be set, and the clock in and clock out time of each shift period can be set separately.



5.3.2. Flexibility Setting

On the basis of on-duty and off-duty time, you can set the number of minutes to clock in after on-duty time, or the number of minutes to clock out after off-duty time, and the staff can clock in or out within the flexible minutes,which would not be counted as late or early leave.

5.3.3. Notes

(1) The on-duty time of each shift period must be earlier than the off-duty time;

(2) The shift period can only be set within 24 hours and cannot be set across days.

5.3.4.5 Time Points Setting of Shift Period

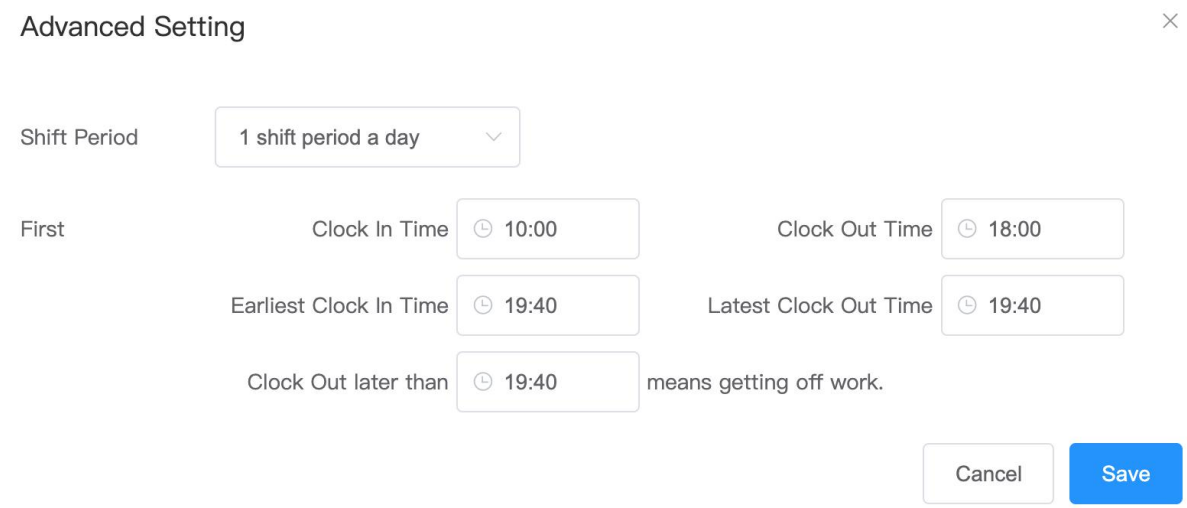
(1) **On-duty time, Off-duty time**: the system records the time according to this two time points, then obtain the status of late arrival, early leave, absence from work or missing clock (the status above all would be conducted on the basis of flexibility setting);

The following three time points are set in the Advanced Settings of shift details:

(2) **Earliest clocking in time**: clocking in before this time point is not counted as clocking in, which is invalid;

(3) **Boundary time of clocking in and out**: set the boundary time point between the on and off duty time points. Clocking in before this time means on-duty clock out, and clock out after this time means off-duty clock out;

(4) **Latest clocking out time**: clocking out after this time point is not counted as off-duty clock in, which is invalid.



5.3.5. Notes about Shift Period Settings

(1) The earliest clocking in time should not be later than the on-duty time;

(2) The latest clocking out time shall not be earlier than the off-duty time;

(3) The boundary time of clocking in and out must be between the on-duty time and off-duty time, and can not be beyond the on-off duty time period;

(4) If the advanced settings are not modified, the system would give the default value.

5.4. Holiday Setting

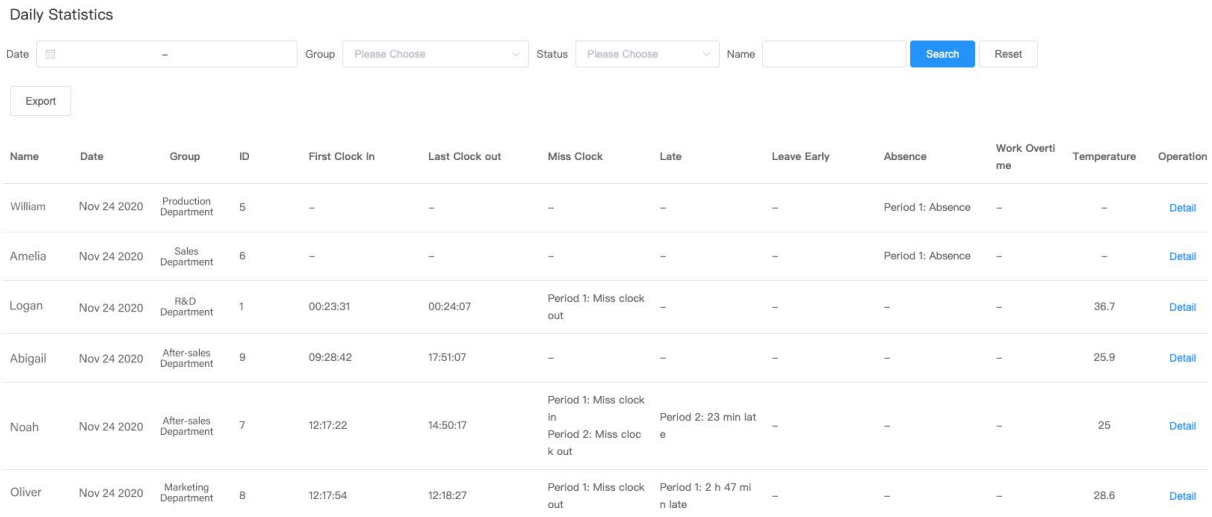
Only the name and starting and ending date of the holiday should be defined. The attendance status of the holiday only can be working overtime, no more absence, late arrival or early leave status, and holiday setting is valid for all attendance groups.

6. Attendance statistics

In attendance statistics, you can view daily statistics and monthly summary statistics data, query records according to time range, grouping and name retrieval, and export the corresponding results to Excel files.

6.1. Daily statistics

6.1.1. Rules of Daily Attendance Statistics


Daily Statistics

Date – Group Please Choose Status Please Choose Name Search Reset

Export

Name	Date	Group	ID	First Clock In	Last Clock out	Miss Clock	Late	Leave Early	Absence	Work Overtime	Temperature	Operation
William	Nov 24 2020	Production Department	5	-	-	-	-	-	Period 1: Absence	-	-	Detail
Amelia	Nov 24 2020	Sales Department	6	-	-	-	-	-	Period 1: Absence	-	-	Detail
Logan	Nov 24 2020	R&D Department	1	00:23:31	00:24:07	Period 1: Miss clock out	-	-	-	-	36.7	Detail
Abigail	Nov 24 2020	After-sales Department	9	09:28:42	17:51:07	-	-	-	-	-	25.9	Detail
Noah	Nov 24 2020	After-sales Department	7	12:17:22	14:50:17	Period 1: Miss clock in Period 2: Miss clock out	Period 2: 23 min late	-	-	-	25	Detail
Oliver	Nov 24 2020	Marketing Department	8	12:17:54	12:18:27	Period 1: Miss clock out	Period 1: 2 h 47 min late	-	-	-	28.6	Detail

(1) Missing clock, late arrival, early leave and absence in the daily statistics are all based on the shift period. For example, there are two periods in a shift. For these two periods, missing clock, late arrival, early leave and absence will be counted respectively ;

(2) Only the first and last clock time point would be shown in the list ;

(3) If there is no clocking records between the earliest clocking in time of a shift period and the boundary time of clocking in and out, this shift period would be deemed as missing clock in ;

(4) If there is no clocking record between the latest clocking time of a shift period and the boundary time of clocking in and out, this shift period would be deemed as missing clock out ;

(5) When there is no clocking at all in a shift period, the period would be recorded as absence ;

(6) The time of arriving late and leaving early will be recorded and displayed in daily statistics ;

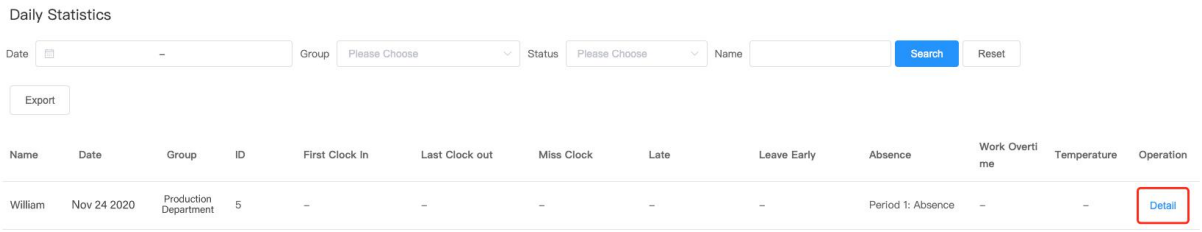
(7) Overtime work on working days would be calculated on the basis of full

attendance.,which is No missing clock. It would not counted as overtime work if missing clock in a workday ;

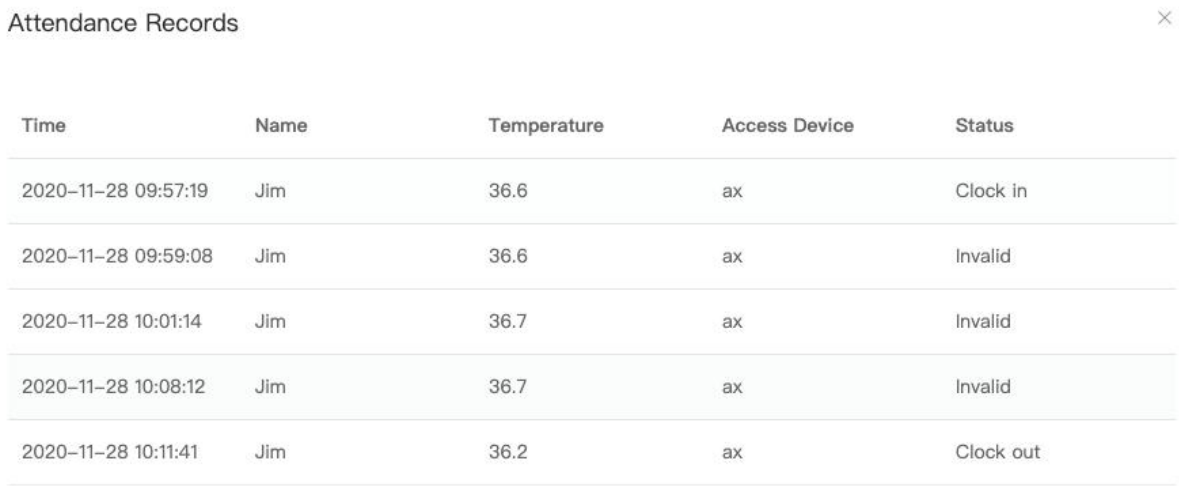
(8) In case of overtime work on weekends or holidays, overtiming would be calculated if you need to punch in twice (the time is more than 1 minute). Overtime work would not be calculated if you only clock once.

6.1.2. Staff Daily Attendance Details

(1) In the daily statistics, you can check the daily attendance statistics of each person and check the attendance record details of the staff.



(2) The attendance record details will list all the clock in records of the day, indicating which are valid and which are invalid.



6.1.3. Notes on Daily Statistics

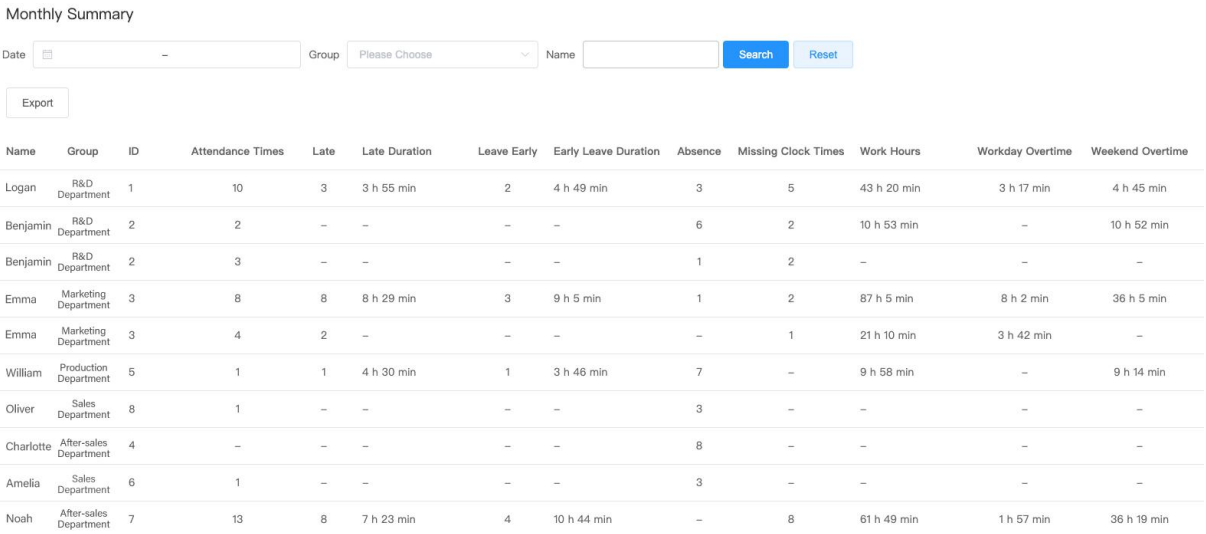
Daily attendance statistics can only view the attendance statistics before the day, but not the attendance statistics of the current day.

6.2. Monthly Statistics

(1) You can use monthly summary statistics view the attendance summary data in a certain period, including attendance times, lateness times, lateness duration, early leave times, early leave duration, absence times, missing clock times, working hours, overtime hours on working days, overtime hours on weekends, overtime hours on holidays, etc.

(2) if the number of absences is -, it means full attendance.

(3) Monthly statistics can be filtered according to time, group and name, and Excel files can be exported according to the filtering results.



Name	Group	ID	Attendance Times	Late	Late Duration	Leave Early	Early Leave Duration	Absence	Missing Clock Times	Work Hours	Workday Overtime	Weekend Overtime
Logan	R&D Department	1	10	3	3 h 55 min	2	4 h 49 min	3	5	43 h 20 min	3 h 17 min	4 h 45 min
Benjamin	R&D Department	2	2	–	–	–	–	6	2	10 h 53 min	–	10 h 52 min
Benjamin	R&D Department	2	3	–	–	–	–	1	2	–	–	–
Emma	Marketing Department	3	8	8	8 h 29 min	3	9 h 5 min	1	2	87 h 5 min	8 h 2 min	36 h 5 min
Emma	Marketing Department	3	4	2	–	–	–	–	1	21 h 10 min	3 h 42 min	–
William	Production Department	5	1	1	4 h 30 min	1	3 h 46 min	7	–	9 h 58 min	–	9 h 14 min
Oliver	Sales Department	8	1	–	–	–	–	3	–	–	–	–
Charlotte	After-sales Department	4	–	–	–	–	–	8	–	–	–	–
Amelia	Sales Department	6	1	–	–	–	–	3	–	–	–	–
Noah	After-sales Department	7	13	8	7 h 23 min	4	10 h 44 min	–	8	61 h 49 min	1 h 57 min	36 h 19 min

6.2.1. Notes

(1) Attendance of each shift period is counted as one attendance (as long as you clock, that would be counted as attendance, no matter how late or early leave you are), and one absence on a shift period would be counted as absence once, and so on;

(2) Monthly summary displays the attendance statistics of the previous month by default, which can be filtered according to your choice;

(3) Monthly summary does not count the attendance of the day, but only the attendance before that day;

(4) The working hours are calculated as the total working hours of working days, workday overtimes, and work overtime on weekends and public holidays. The working hours of working days can only be calculated under the condition that there is no shortage of clocking, and the working hours of the workdays will not be calculated if there

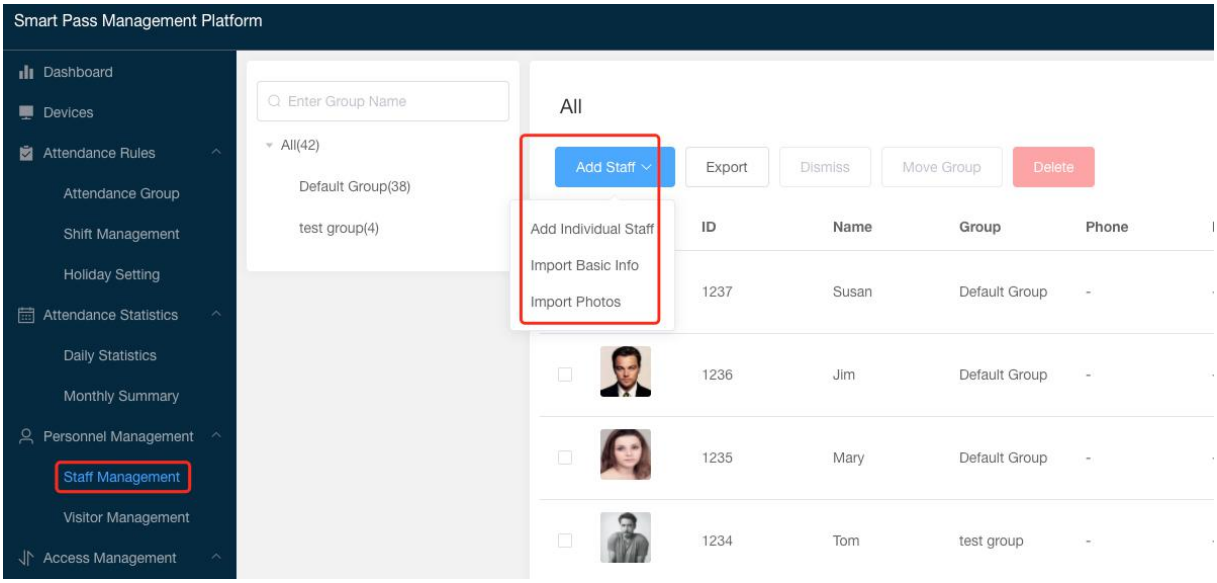
is missing clock.

7. Personnel Management

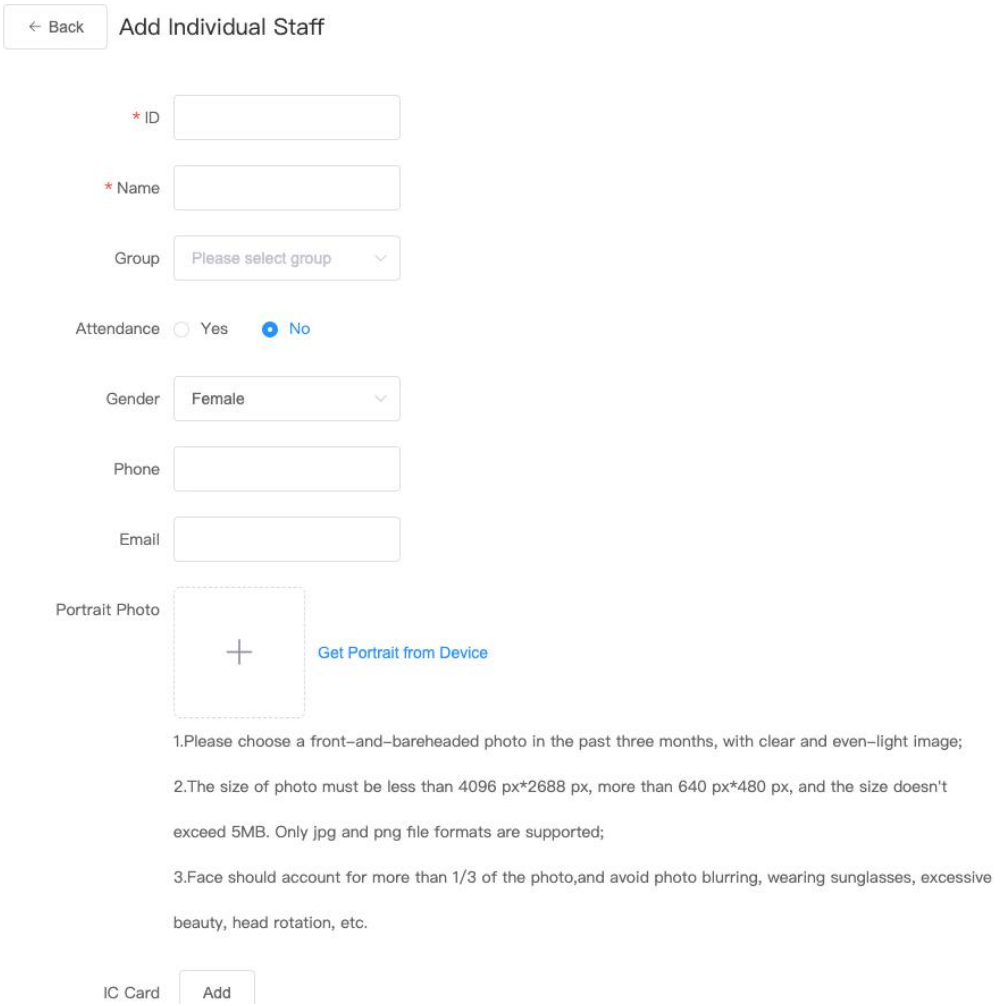
Personnel management includes staff management and visitor management.

7.1. Staff Management

In the staff management, you can select to add individual staff, batch import staff information, batch import portraits, and manage staff in groups.



7.1.1. Add Individual Staff



(1) Staff ID cannot be repeated;

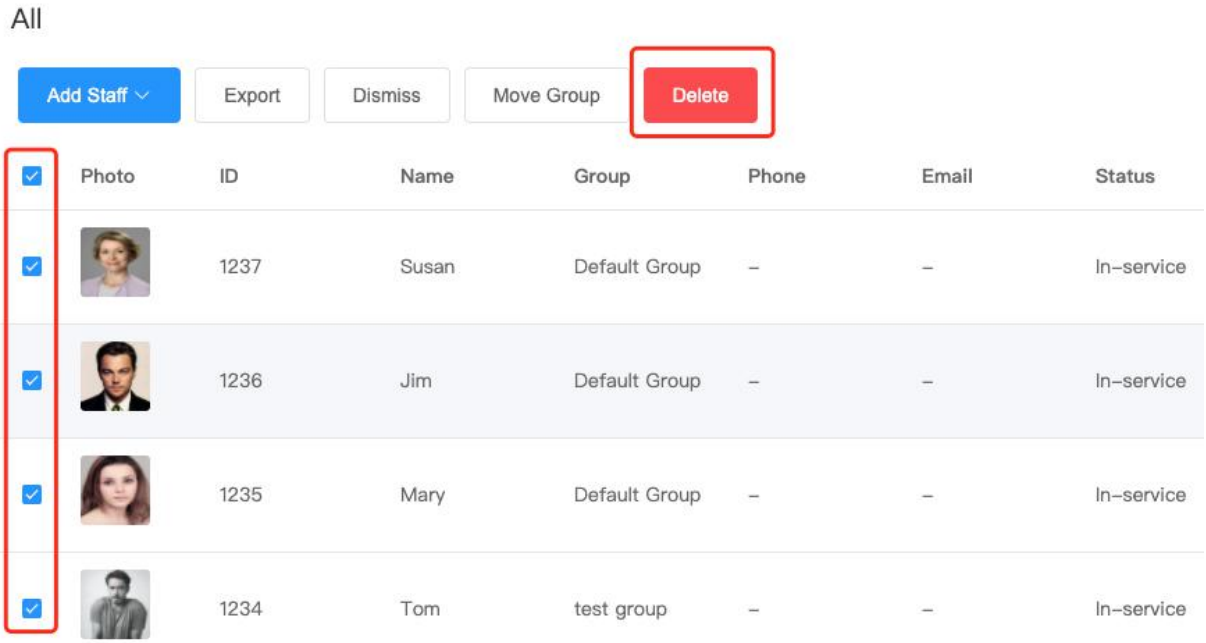
(2) If you want to record the attendance of the staff, you need to select an established attendance group. After adding the staff to the attendance group and saving it successfully, the staff has the authority to corresponding devices of the attendance group;

(3) If attendance group is not selected when adding a new staff, the staff would not have access authority to any devices. If you want to add the staff to the attendance group again, you can add staff from the attendance group settings(refer to 5.2.2), that is, they have the authority of the corresponding devices; you can also add authorization for the staff in the pass authorization. However, this operation only enables authorization, and does not record attendance.

7.1.2. Delete Staff

Select the corresponding staff in the list to delete the staff individually or in batch.

After deletion, the staff would no longer record attendance (but the attendance already recorded in the past can still be viewed in attendance statistics 6.1 and 6.2 for details), the staff would no longer have the corresponding device access authority, and there is no information of the deleted staff in the system.



7.1.3. Group Management

（1） Edit Group Name

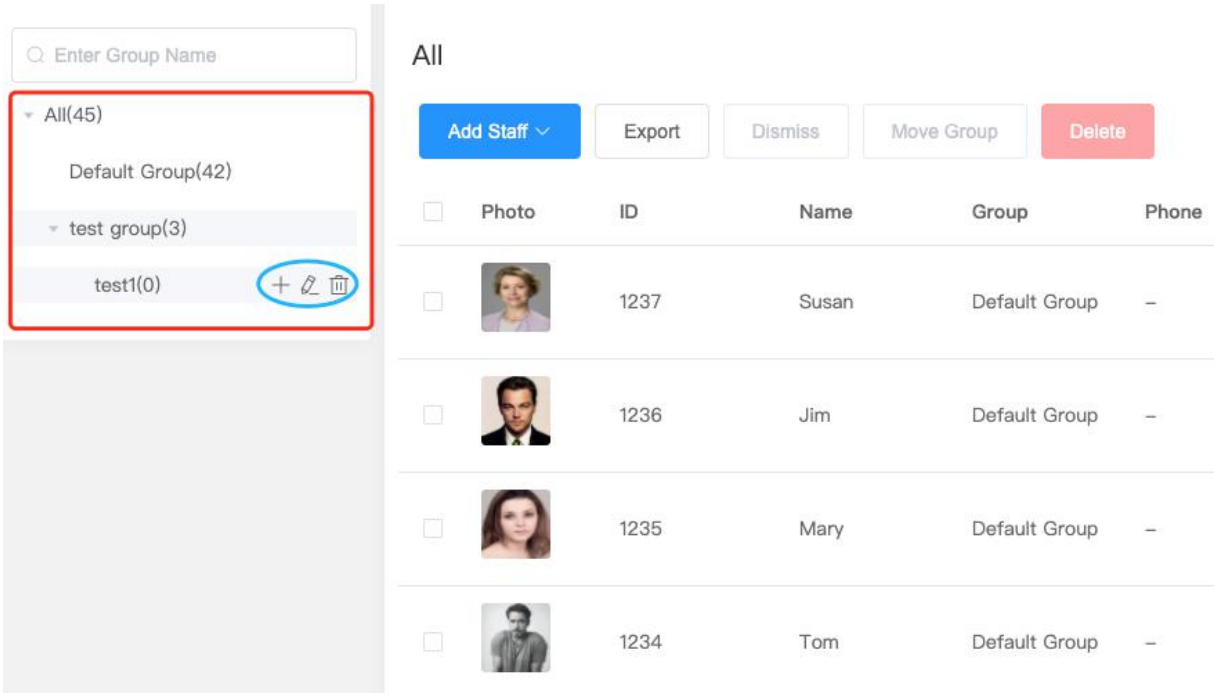
Move the mouse to the group name in the group list, click the pencil icon to change the group name.

（2） Add Subgroup

Move the mouse to the group name in the group list and clicking the + icon, a new group can be added under the group. An individual staff can be added directly under the current group, and the group name would displayed as the current selected group after entering the add page.

（3） Delete Group

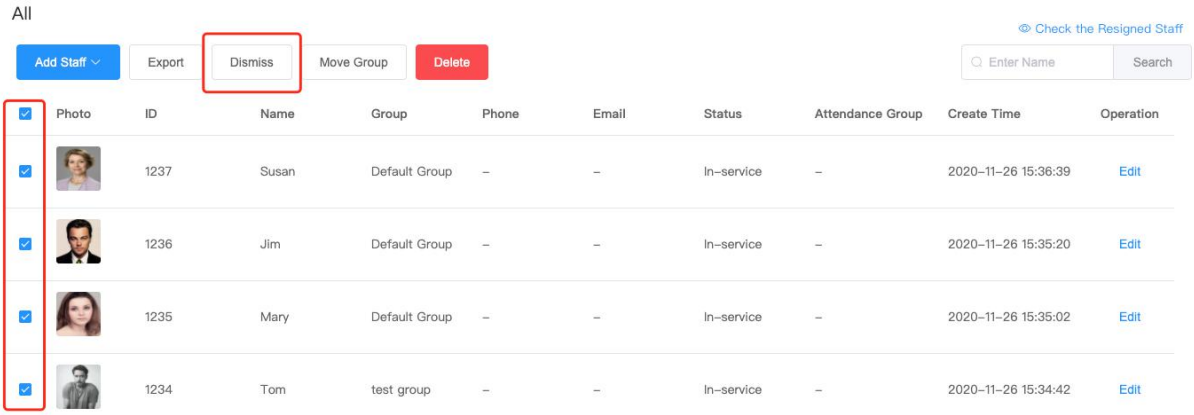
Move the mouse to the group name in the group list, click the trash can icon to delete the group. After deleting the group, the group disappears, but the staff of the deleted group would move to the default group automatically.



7.1.4. Staff Dismission and Join

（1） Dismiss staff Individual and in batch

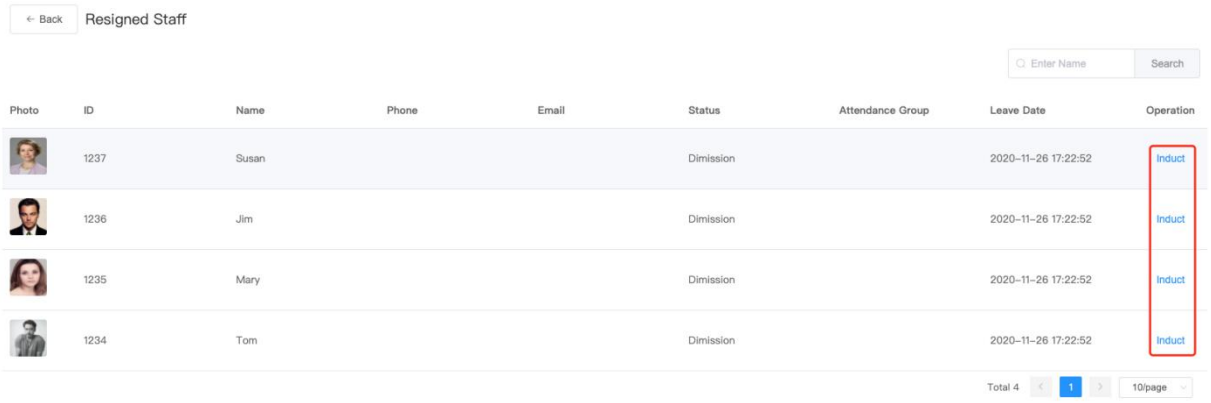
Dismissing staff would cancel all the access authority of the staff, but the staff information would not be deleted. You can view all the departed staff in the list of departed staff.



（2） Reinstate the departed staff

The reinstating operation would only change the on-the-job status of the staff, and would not restore the attendance information and access authority of the staff, which

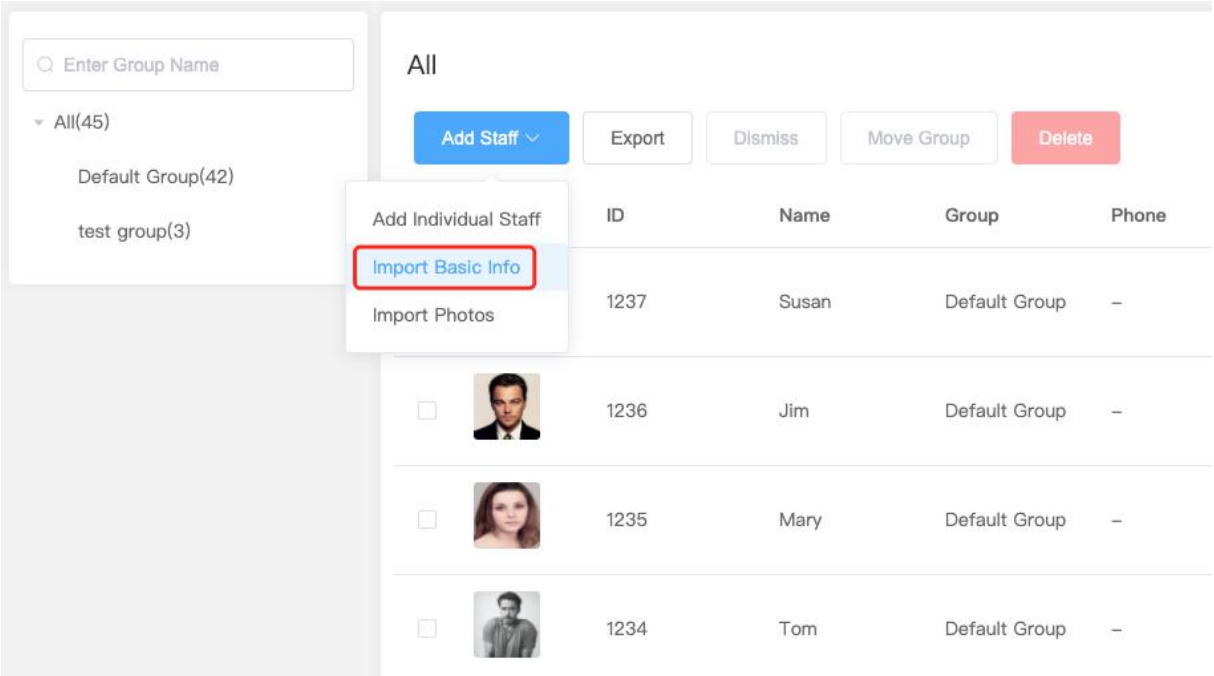
needs to be added again. The reinstated staff belong to the default group. If you need to change the group, you can select single or multiple staff in the staff list to move group, or enter the edit page to select another group.



7.2. Import Staff in Batch

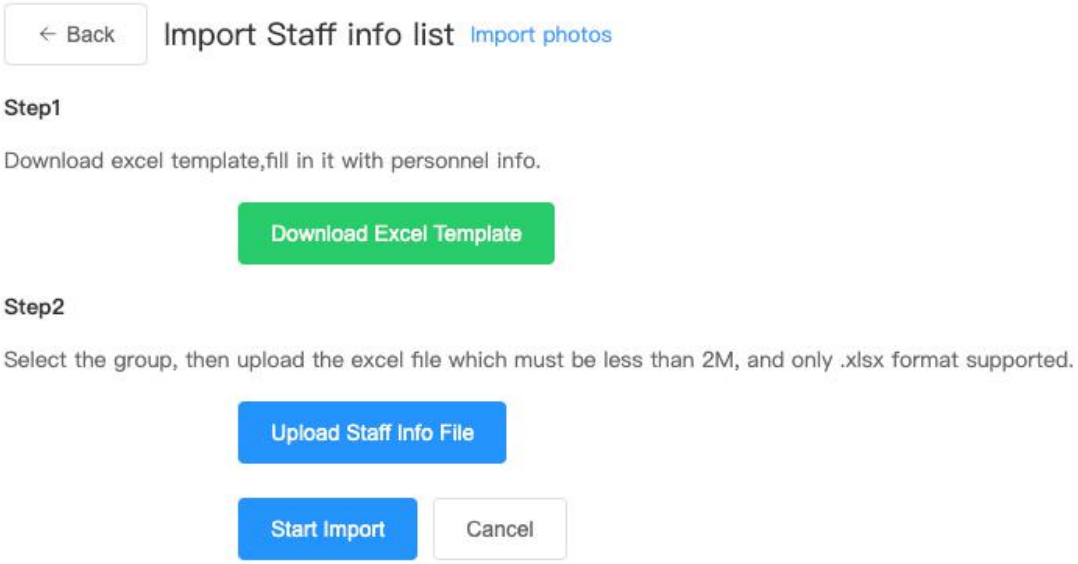
7.2.1. Import Staff Information in Batch

(1) Click "add staff" and select "import basic info", that is, import staff information in the form of Excel in batch.



(2) Download the template according to **Step 1**, fill in the staff information according

to the instructions and temple data, then upload the staff information Excel file according to the Step 2, and click import button.



7.2.2. NOTES

(1) The group input in the template should be completely consistent with the field of the existing group, and English letters should be case-sensitive; otherwise, a new group will be established;

(2) The attendance group in the template shall be exactly the same as the existing attendance group field, otherwise the system would prompt an error report after import and would not allow uploading information until the attendance group field is modified correctly;

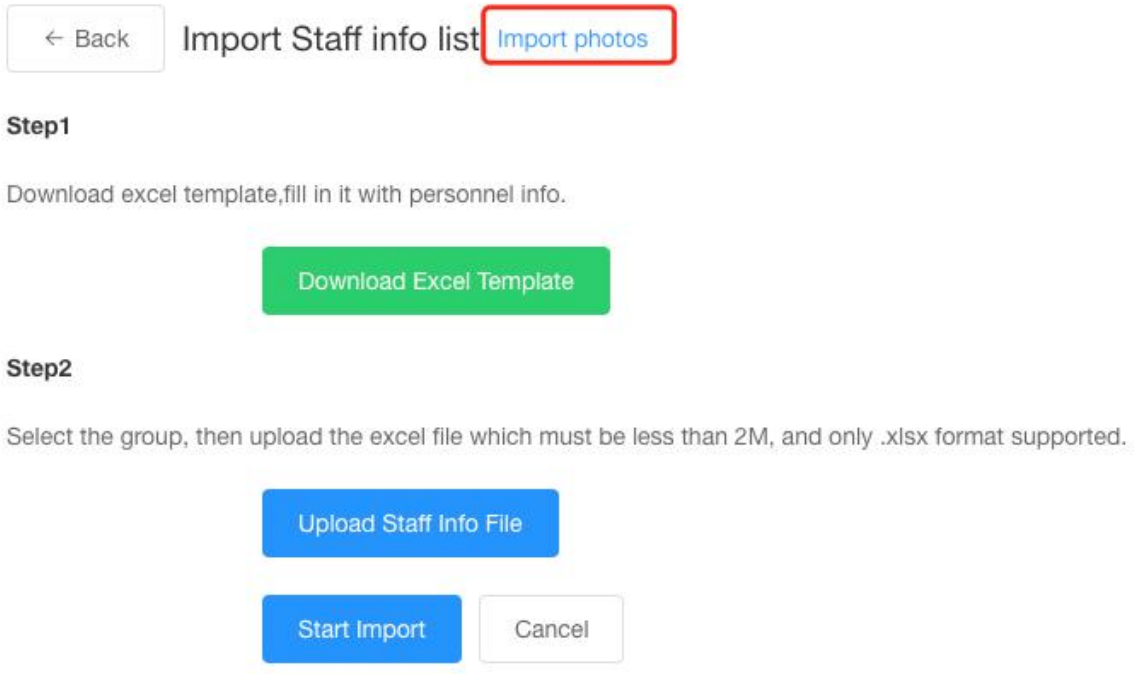
(3) The attendance group is not required. If it is not filled in, there would be no attendance group for imported staff, and no attendance record and no access authority. Besides, the attendance group cannot be selected by editing staff, and staff can be added in the attendance group management (refer to 5.2.2);

(4) If you choose to add staff to attendance group when importing, the staff access authority of the devices associated the attendance group can be viewed in the access authority list.

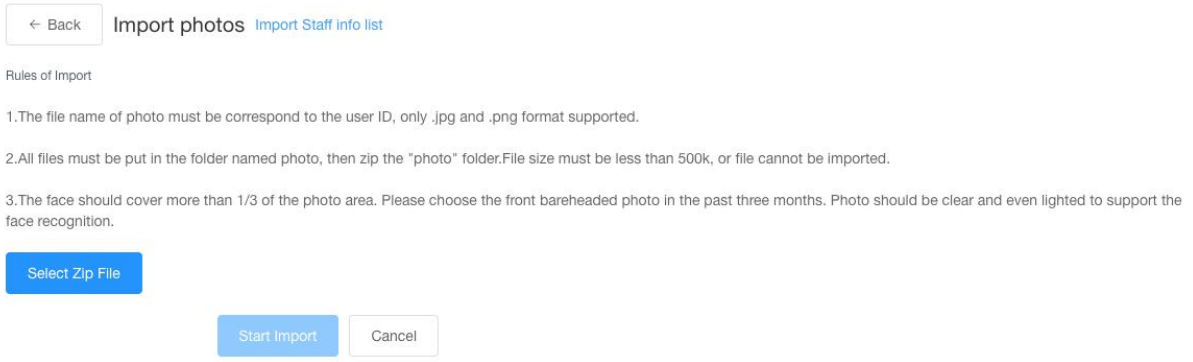
	A	B	C	D	E	F	G	H	I
1	Instructions: 1. Personnel ID: required; cannot be repeated; in 1 to 9 characters, only consisting of numbers, letters or their combinations, such as 12345, abcd, a123. 2. Name: required; in 1 to 128 characters, consisting of Chinese, English, numbers, or their combinations (can contain 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 "Groups-subgroups". 5. Phone number: required; cannot be repeated; in 1 to 20 characters. 6. IC card: optional; cannot be repeated; in 1-64 characters, no limitation on character types. 7. Email: optional; cannot be repeated; in 1-32 characters, no limitation on character types. 8. Notes: optional, in 1-128 characters, no limitation on the character types. 9. Attendance group: optional, in 1-32 characters; must be a Attendance group name that already exists in the system;								
2	ID	NAME	GENDER	GROUP	PHONE	E-MAIL	IC CARD	REMARK	ATTENDANCE GROUP
3	1	Bob	male	Default Group	18088888888	bob@google.com		sample data	Default Attendance Group

7.2.3. Import Staff Portraits in Batch

(1) Click "Add Staff"button, select "import photos", or import photos from import staff information page.



(2) Select the zip package named by photo to upload.



- Notes of the import photos rules

(1) The name of each photo should correspond to the staff's ID, as a consequence, you can view the corresponding photo in the staff list after the successful uploading;

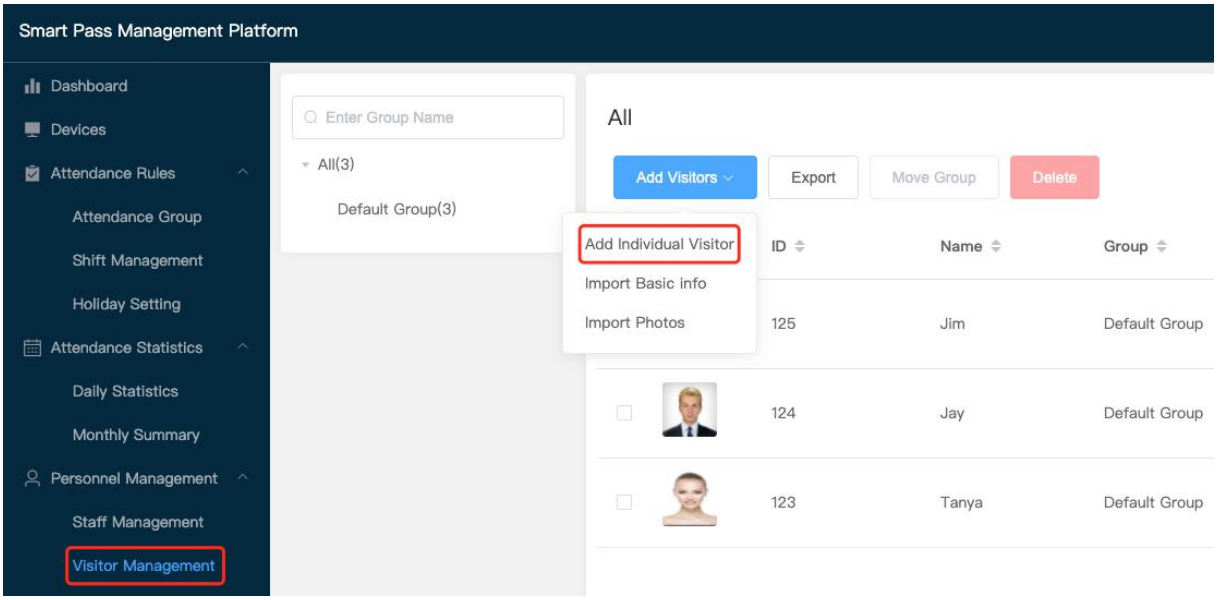
(2) Put the named photos in the specified folder (folder name: Photo) for compression, supporting only.zip file format, and each photo file size shall not exceed 500K, files that do not meet the requirements would not be imported;

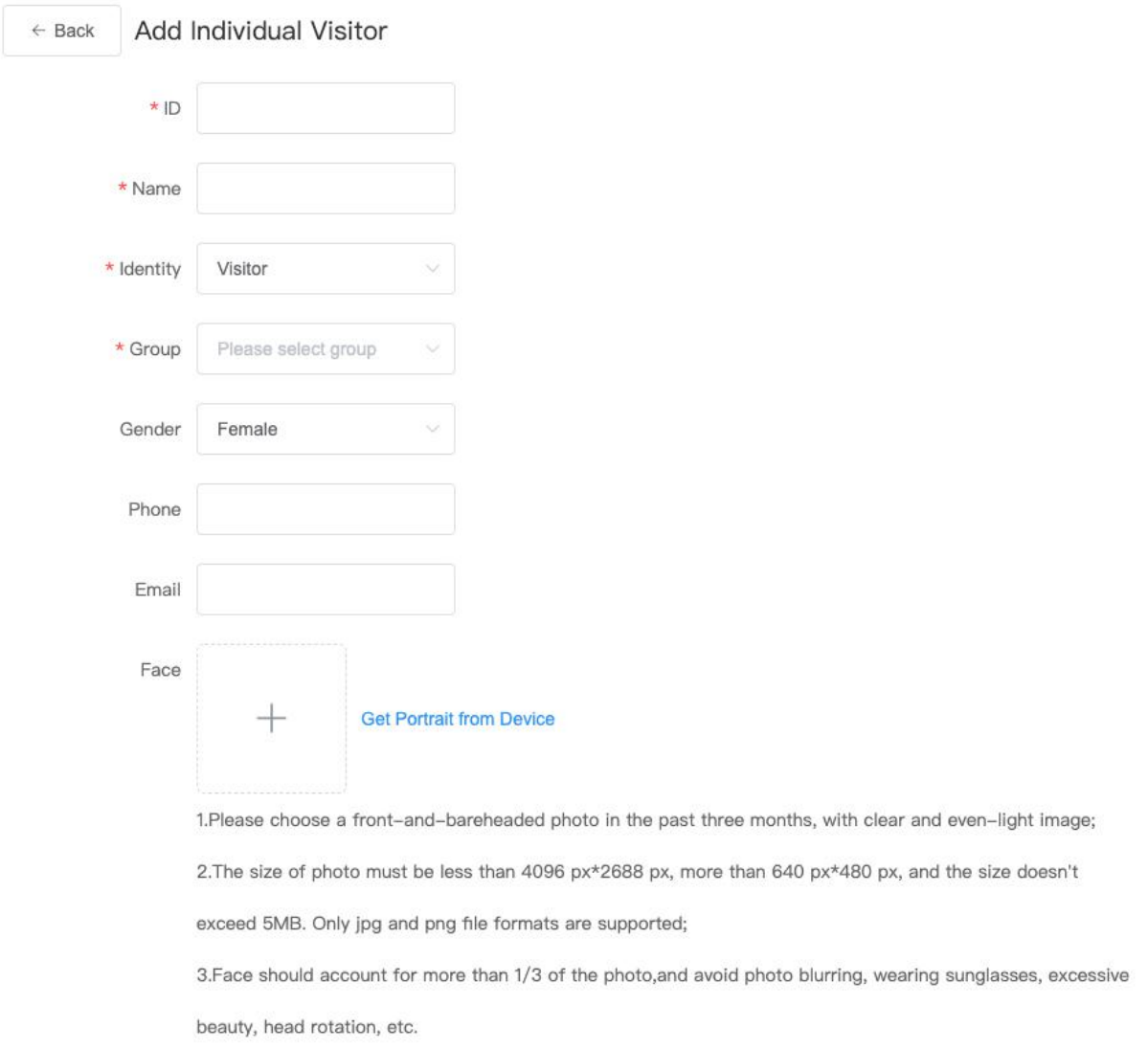
(3) The face should account for more than 1/3 of the photo. Please select a bear headed photo in the last three months, with clear image and the light is even. Avoid that the photo cannot be used for face recognition.

7.3. Visitor Management

7.3.1. Add Visitor

Add individual visitor : fill in all the required items with * to save the visitor information.





- NOTES

(1) The visitor ID cannot be duplicated (the visitor ID can be the same as the staff

ID);

(2) The added visitors do not have corresponding access authority by default, so visitors can be authorized to add in the access authorization in the access management;

(3) Visitors cannot be added to the attendance group and cannot have attendance records.

7.3.2. Delete Visitor

Same as deleting staff and managing staff groups (refer to 7.1.2 and 7.1.3).

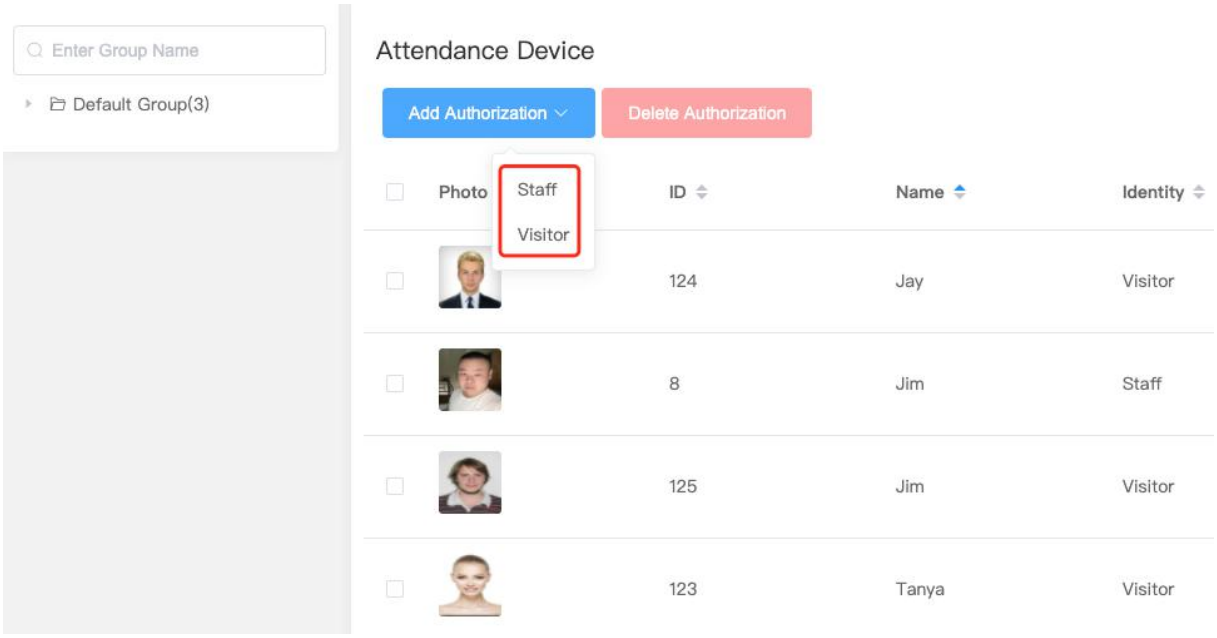
7.3.3. Import Visitor Information and Photos in Batch

Same as staff importing (refer to 7.2), except you cannot select the attendance group and record the attendance for visitors.

8. Access Management

8.1. Access Authorization

On the access authorization page, Select the device for which you want to add an authorized person, select "add authorization", select staff authorization to authorize staff, and select visitor authorization to authorize visitors.

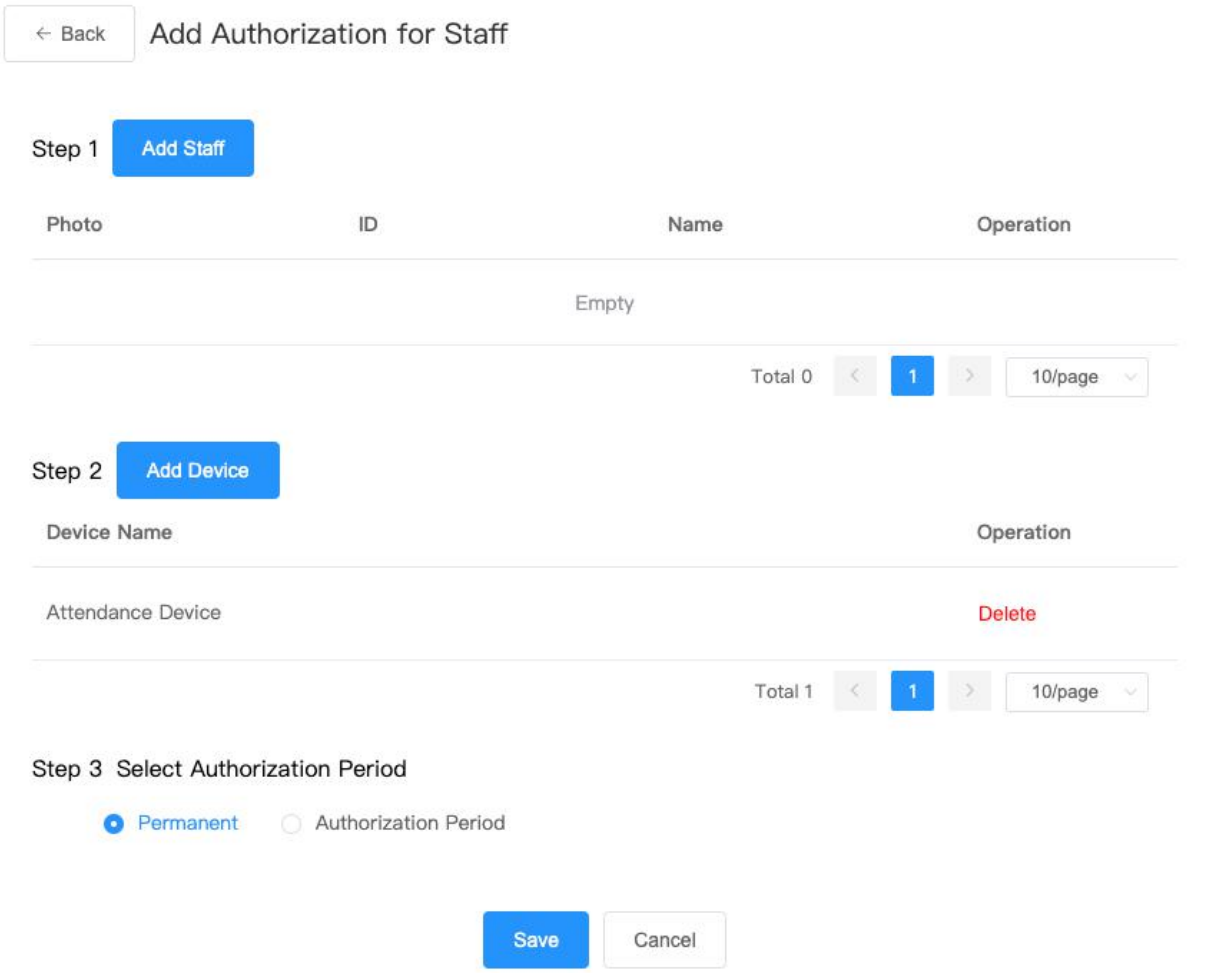


8.1.1. Steps to Add Authorization

(1) Add staff or visitors that have been created in the system;

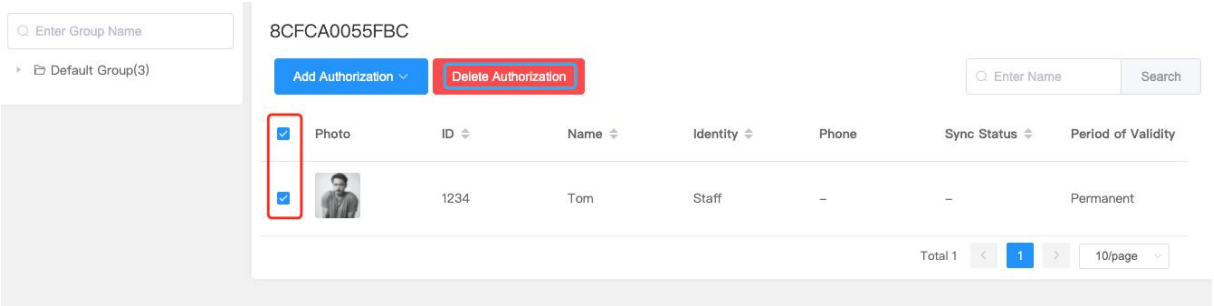
(2) Add devices to allow staff or visitors to pass;

(3) Select the authorization Period, that is, the time limit that staff or visitors are allowed to pass.



8.2. Delete Access Authorization

Select the device from the access authorization page, and select the user with authorization under the device individual or in batch to delete the access authorization, and the user cannot access the corresponding device anymore.



8.3. Blacklist Monitoring

8.3.1. What is Blacklist Monitoring?

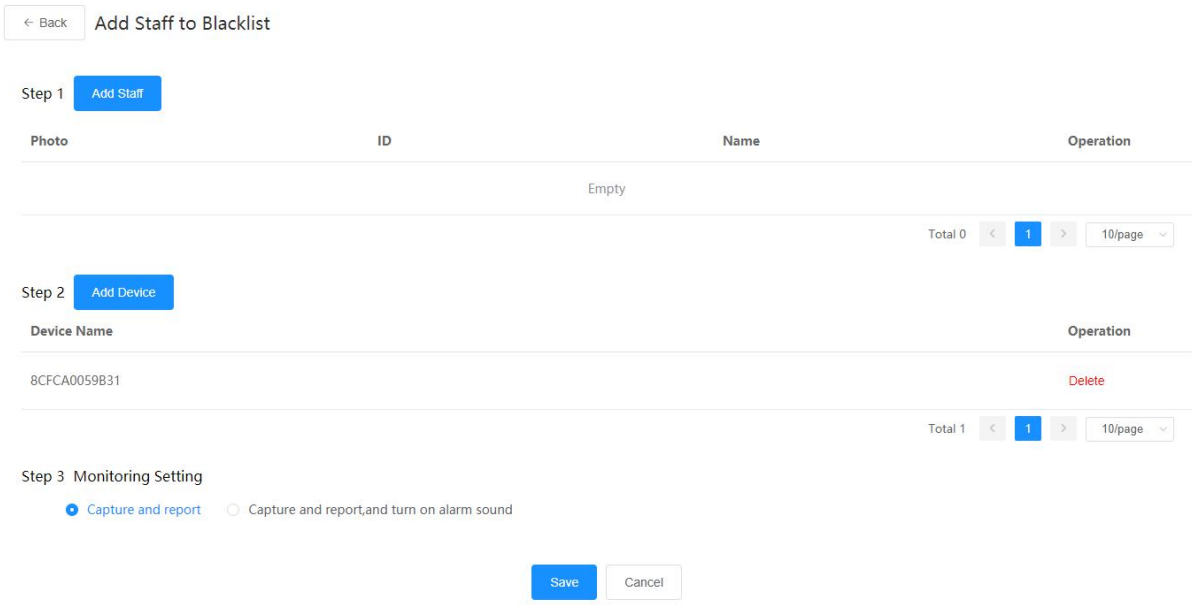
Blacklist refers to the designated users of device monitoring. **The monitored users have no access authorization.** When they are identified by the specified device, they would be forbidden to pass and their blacklist monitoring records would be reported. Staff and visitors both can be blacklist monitored.

8.3.2. Steps to Add Blacklist Monitoring

(1) Add staff/visitors that need to be monitored;

(2) Add device that monitor staff/visitors;

(3) Select the monitoring setting, that is, which way to report and record the monitored user after being identified by the device.



8.3.3. NOTES

(1) Blacklist monitoring has no time limits. Once added, the user would be monitored permanently unless removed them from the blacklist;

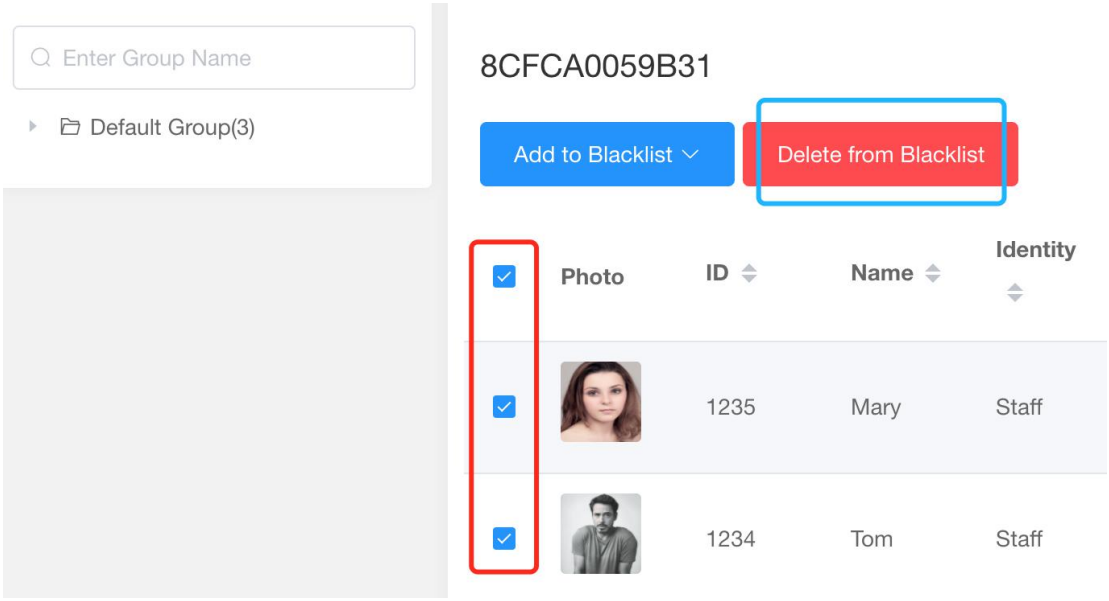
(2) When staff/visitors added to the blacklist, they would automatically lose their access authorization, and their information would no longer be in the access authorization list;

(3) If the staff / visitor in the blacklist is re-authorized in the access authorization,

the access authorization would be restored.

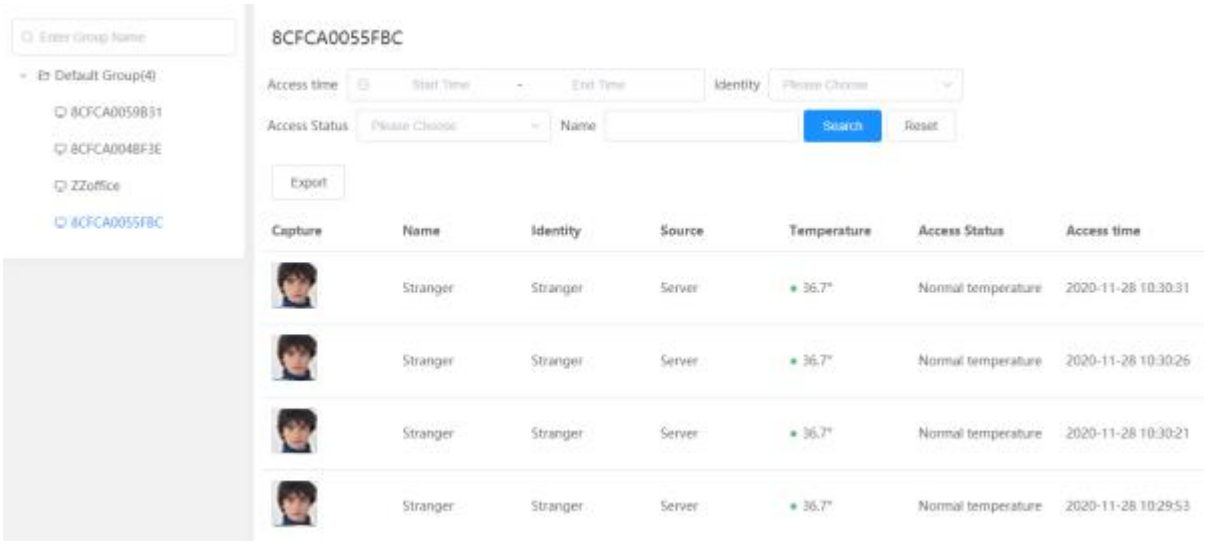
8.4. How to Remove Blacklist Monitoring

Select individual or multiple users in the blacklist monitoring page to delete the users from blacklist monitoring list. **Staff/visitors who are out of blacklist monitoring listhave no access authorization by default, and it needs to be added again in the access authorization.**



8.5. How to View Access and Blacklist Monitoring Records

In the list of access and blacklist monitoring records, the relevant records of the selected device on the left device list are displayed. Records can be retrieved by time period, passage status, user identity and name keywords.

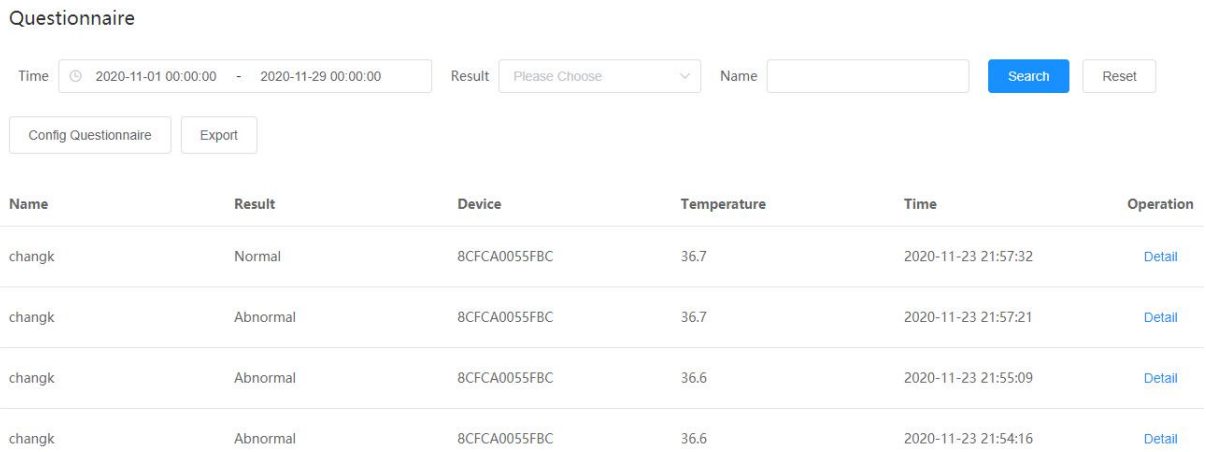


8.6. Questionnaire

8.6.1. How to Use Questionnaire

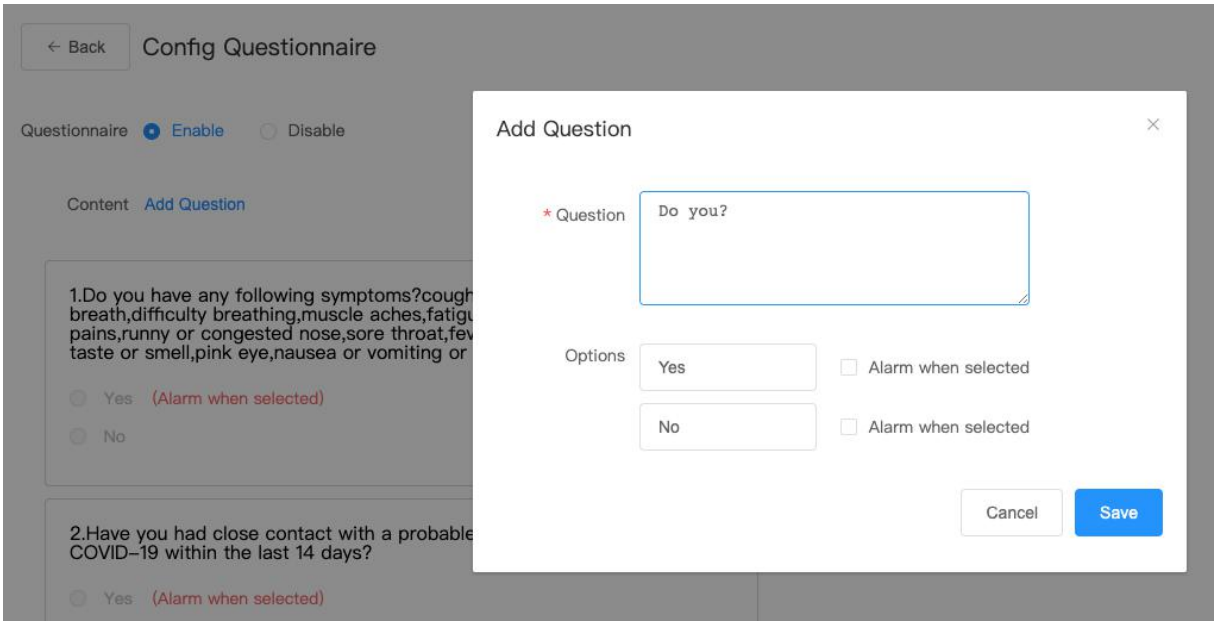
(1) In the access management, the questionnaire function of the device can be set, and the user access records of the questionnaire survey can be viewed, retrieved and exported;

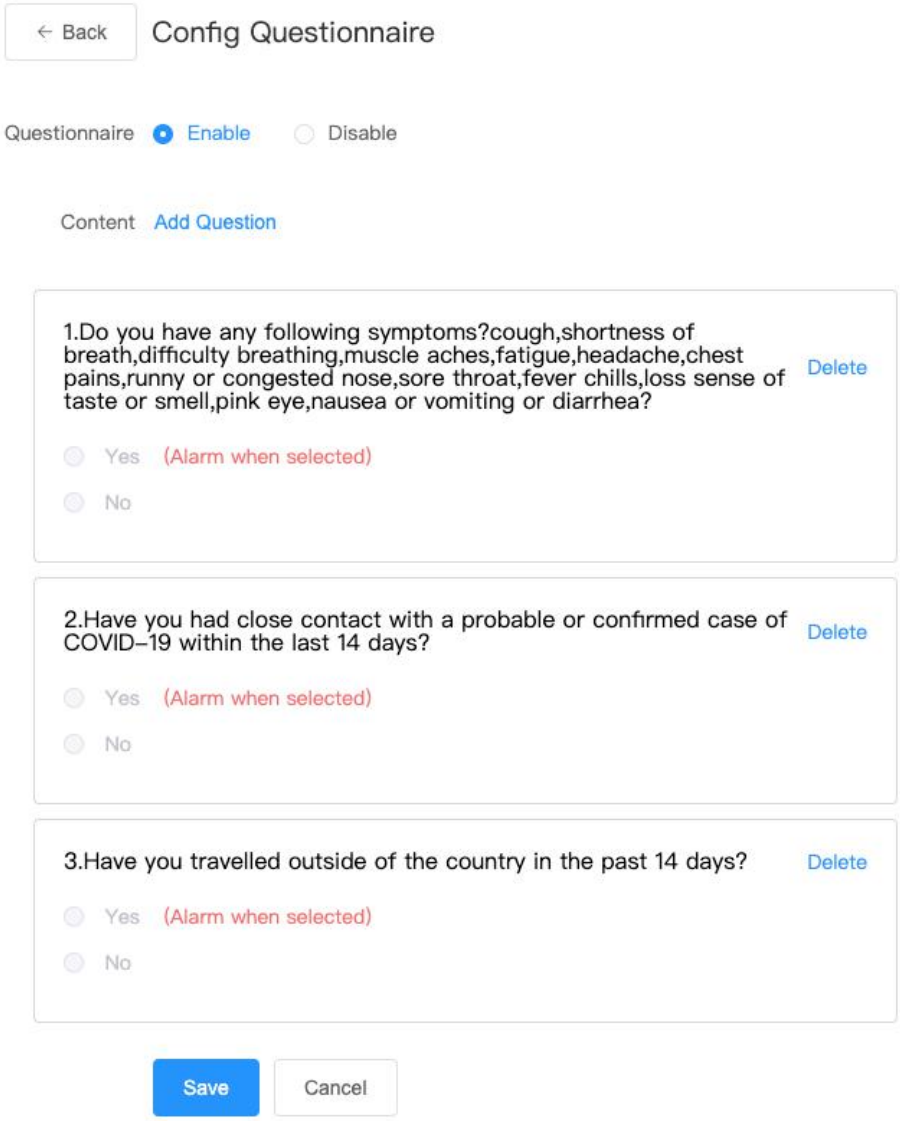
(2) When the user passes through, after the temperature measurement and face recognition are successful, the questionnaire contents would pop up, and corresponding questionnaire options should be selected according to the user's situation. If some options are set to alarm, the device would alarm and prevent the user from passing through.



8.6.2. How to Configure the Questionnaire

Click “configure questionnaire” to edit the contents of the questionnaire. This function can be turned on or off. If no questions are set, the function cannot be turned on. When setting the problem, you can choose an option to alarm. When the option is selected, the device would alarm and forbid the personnel to pass.





9. System Setting

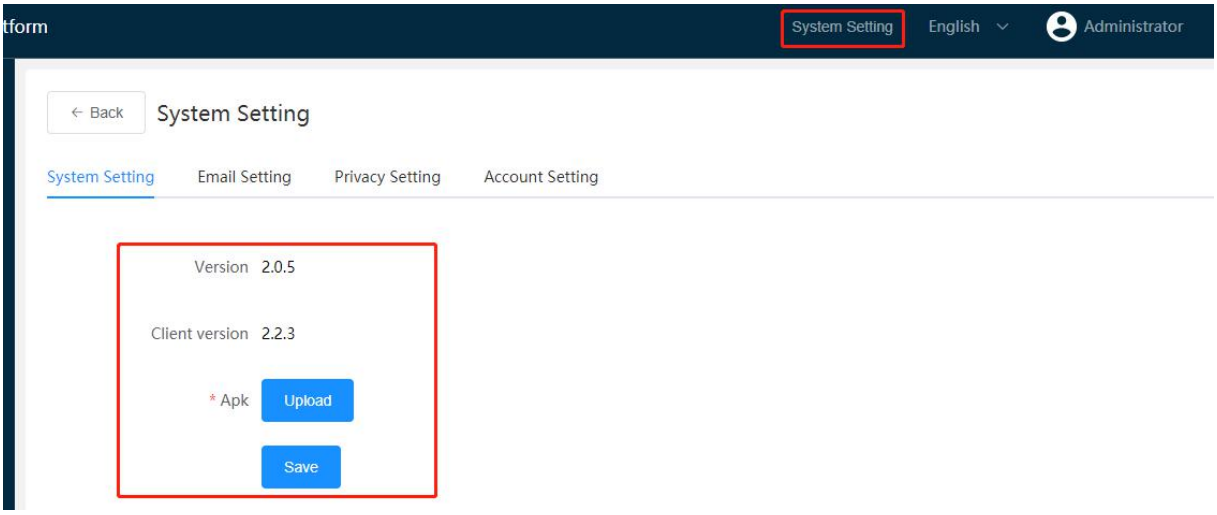
9.1. How to Update the Device APP Remotely

9.1.1. System Settings

(1) The version number is the server version of the current LAN;

(2) The device version is the uploaded version of the updated package;

(3) When the device is connected to the Internet, the uploaded version of the updated package would be synchronized to the device for updating.

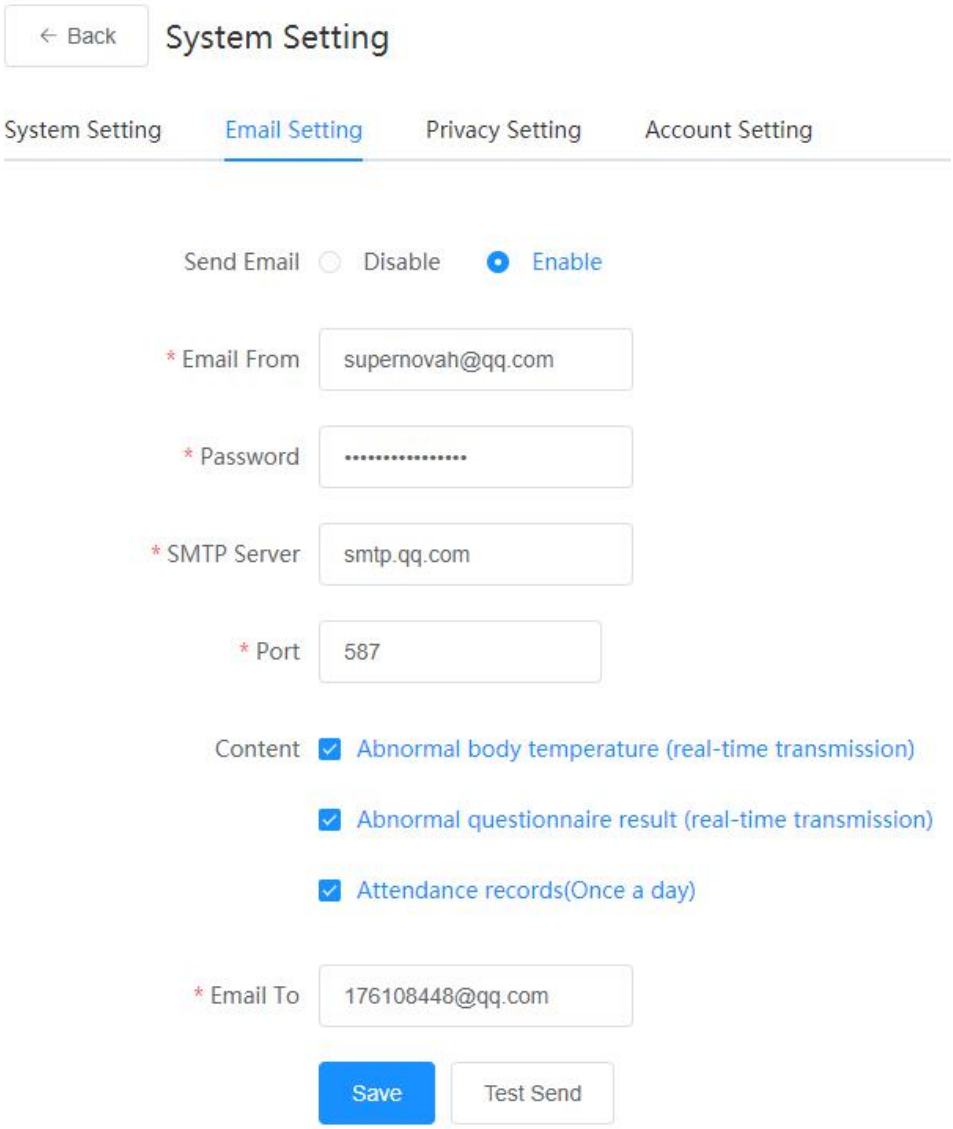


9.1.2. NOTES

You must upload a more advanced version than the current terminal application. The same and low-end versions cannot be saved and synchronized.

9.2. E-mail Setting

After configuring the sender and recipient mailbox information, you can send the pass records of abnormal body temperature and questionnaire results by email, or choose to send the attendance record once a day; multiple mailboxes use semicolon';' optional.



9.2.1. NOTES

(1) Generally you should fill in the sender's email password with email login password, but some email operators need to fill in the authorization code instead of the email password;

(2) SMTP server address and port number need to be checked in the setting item of sender mailbox.

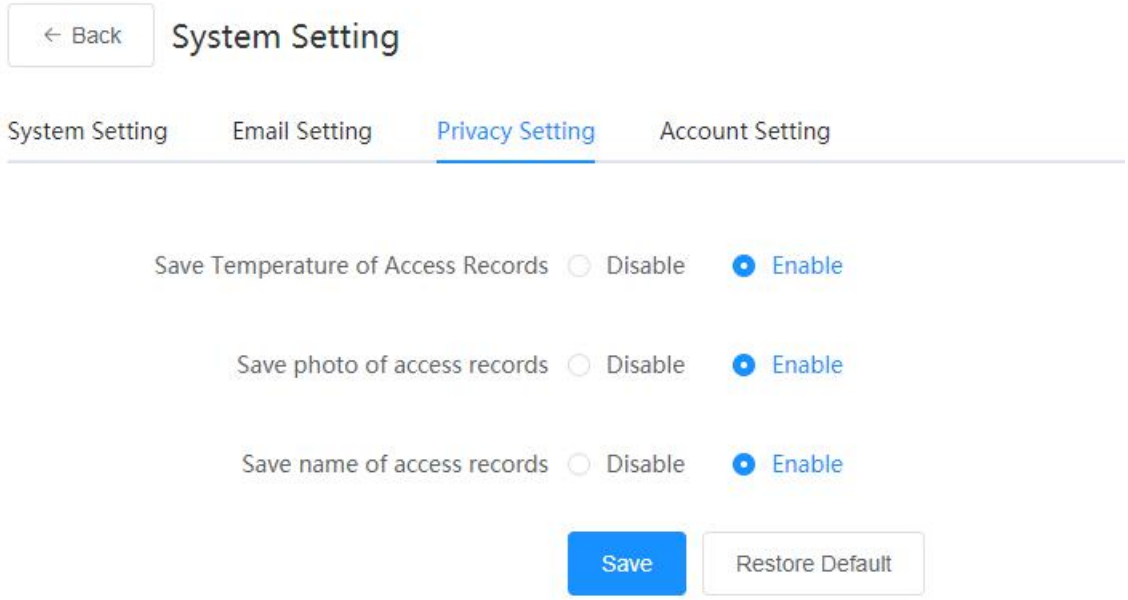
9.3. Privacy Settings

(1) When "Save Temperature of Access Records" is enable, the temperature is displayed in the list; when it is disable, the temperature is not displayed;

(2) When "Save photo of access records" is enable, the portrait photos would be displayed

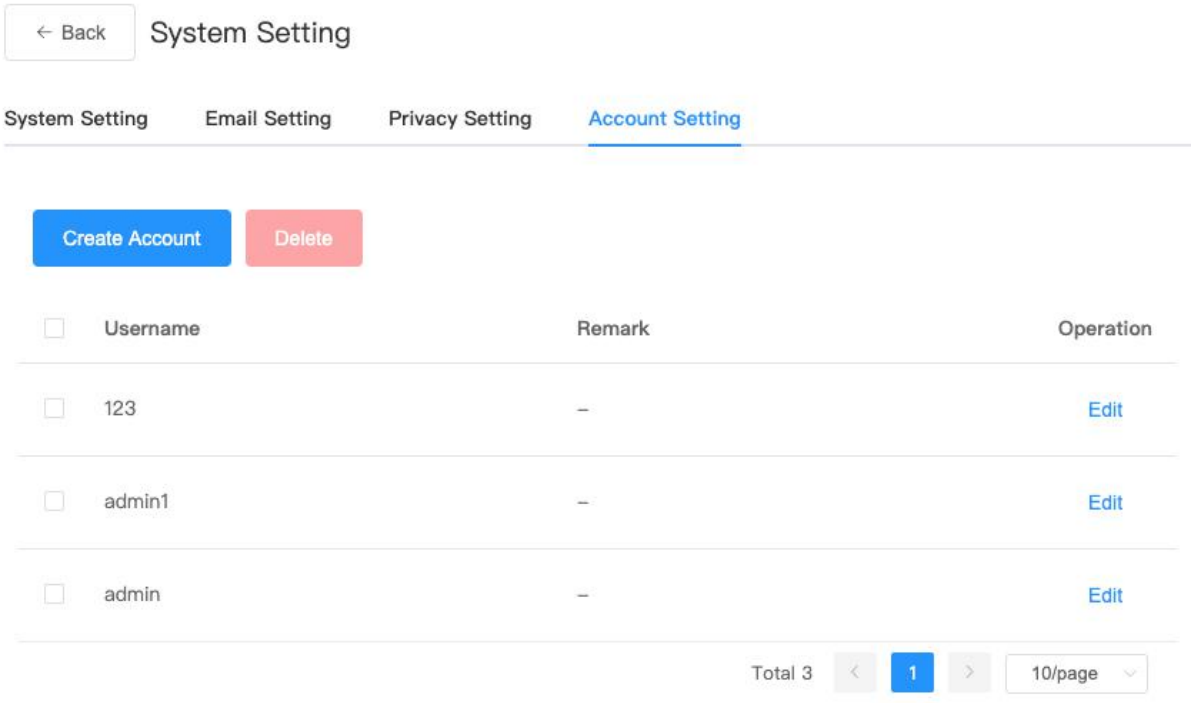
in the list; if it is disable, the photo would not be displayed;

(3) When "Save name of access records" is enable, the user name would be displayed in the list; if it is disable, the user name will not be displayed.



9.4. How to Create New Account

Only administrator account (account name "admin") can be used to create other accounts, password can be changed.



10. FAQ

● When uninstalling system software on the LAN server, prompt "Another application has exclusive..." Unable to continue unloading?

Solution: Open task manager, select service, right - click "Smart Pass DB" and stop service.

● After the software is uninstalled and re-installed on the LAN server, double-click the "Smart Pass" icon to boot unsuccessful?

Solution: Please confirm whether to follow the correct unloading and reloading steps: 1. Unloading, 2. Restart, 3. Delete C:\SMARTPASS files, 4. Install the Smart Pass program.

● After the software is installed successfully on the LAN server, double-click the "Smart Pass" icon to launch the software unsuccessfully?

Solution: Restart the computer and wait for the program to start automatically.

● After the successful installation of the application on the device, the device does not automatically log in and come online?

Solution 1: If there are 2 or more network CARDS on the computer deployed by the server, it is necessary to disable the redundant network CARDS and keep only one network card. After operation, restart the server computer.

Solution 2: Connected mouse to the device, click the mouse in the middle ball, enter the password you set the default password (123456), click 'ok' to, open the menu button interface, and then click "login" management, in the login interface management, enter your server's IP address (open the IP address of the server backstage after start copying), input after click "login" link.