Akuvox Smart Intercom

Akuvox
Open A Smart World

WWW.AKUVOX.COM

ACMS
Administrator Guide

Version: 4.0 | Date: 03.2023

AKUVOX SMART INTERCOM   www.akuvox.com

About This Manual

This manual is intended for the administrators who need to properly manage personnel, devices, access control configurations, personnel attendance and shift schedules on Akuvox ACMS (Access Control Management System).

This manual applies to version 2.2.0.4 of ACMS. For new information or the latest software version, please consult our technical support.

Related Documentation

For more technical documents, please visit at:

https://knowledge.akuvox.com

Contents

1. Product Overview

ACMS (Access Control Management System) is designed with an idea that personnel, device, access control, personnel attendance and shift schedule etc. are separated in their configurations which can later be conveniently incorporated to form a complete and integrated access control and attendance management.

Users using ACMS will be able to:

- Achieve the data synchronization between the ACMS and device(s).

- Manage the personnel and department information of the access control.

- Customize your access control schedule and authority group for the door access, and check and monitor the logs for security purpose.

- Manage personnel attendance, shift schedule.

- Search, check and export the attendance report.

- Import and export system data for the convenience of data sharing and system configuration.

ACMS currently applies to A01/A02/A05 access control terminals, E16, E18, R29, X915S door phones, and A092 access controllers.

2. ACMS Installation

2.1. Installation Requirements

Prior to the installation of the ACMS software, you are required to make sure that the following installation requirements are met:

- Windows 7 operating system or above.

- Only one ACMS is allowed in the same LAN (Local area network).

- No SDMC and ACMS software are turned on your personal computer or on other personal computers in the same network.

- No device is connected to the Akuvox SmartPlus.

- The Firewall on your computer is turned off.

- Anti-virus software is turned off.

2.2. Install ACMS

ACMS is to be installed on your computer using compressed files.

1. Decompress the zip file **ACMS.AK.2.0.1.7**.
2. Click the ACMS setup.exe file.
3. Click "**Yes**" in the pop-out window to continue the installation.
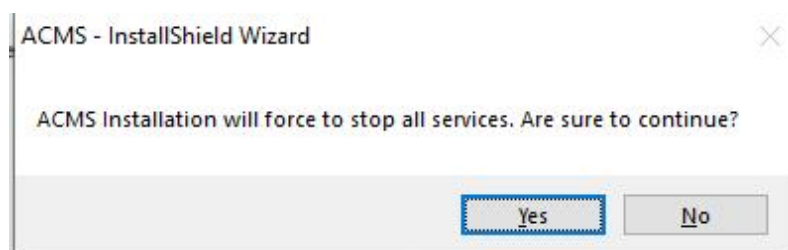
4. Click **Next** to go to the next step.
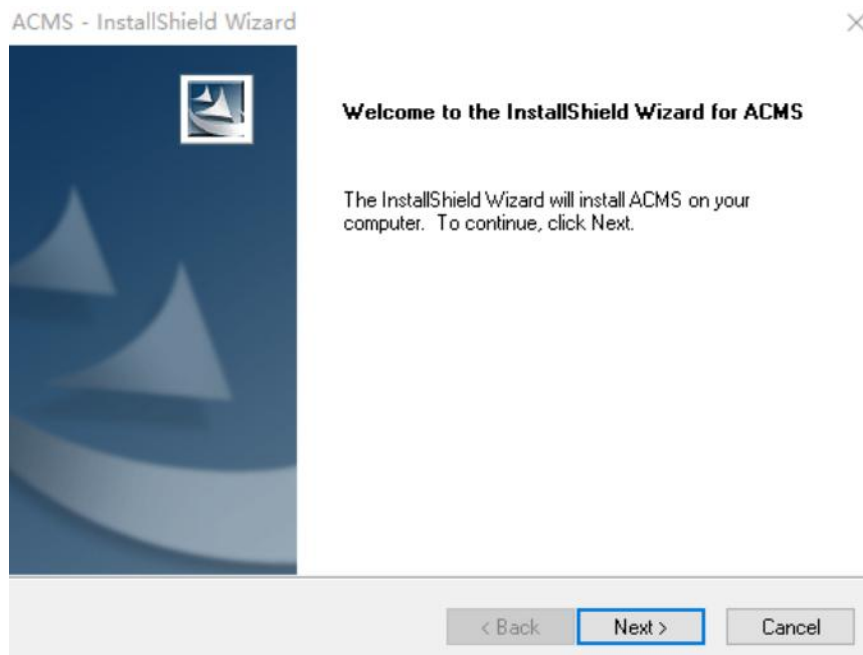
5. Click on **Next** to accept the agreement.
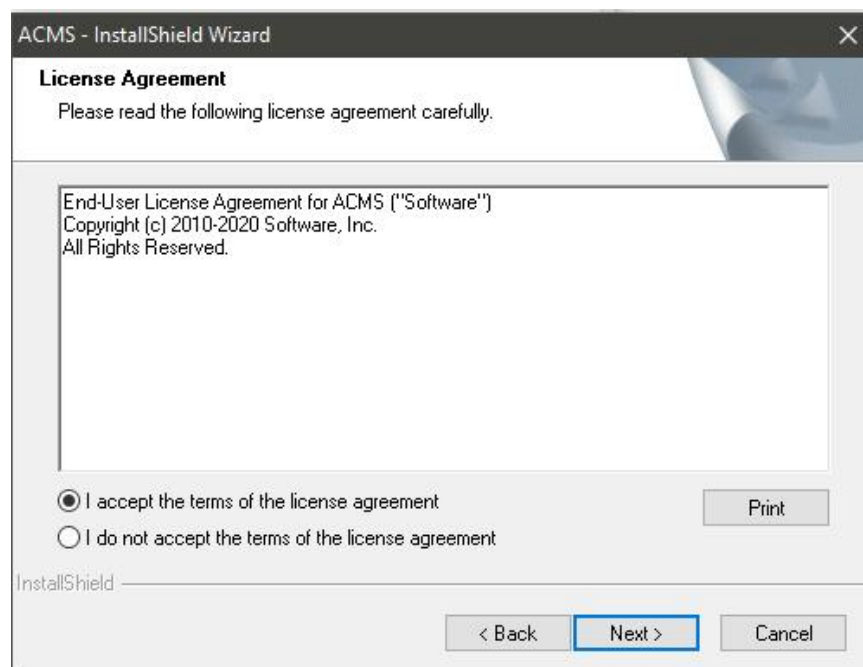
6. Enter the **User Name** and **Company Name** and click **Next.**

7. Select the installation path by default or the other path to your preference and click **Next**.

8. Click on **Install** to finish the installation.

- After the installation is completed, you will see the ACMS icon along with ACMSSeverManage icon on your desktop.

> **Note:**
>
> - The ACMS installation path should be English characters.

2.3. Set up ACMSServer Manage Software

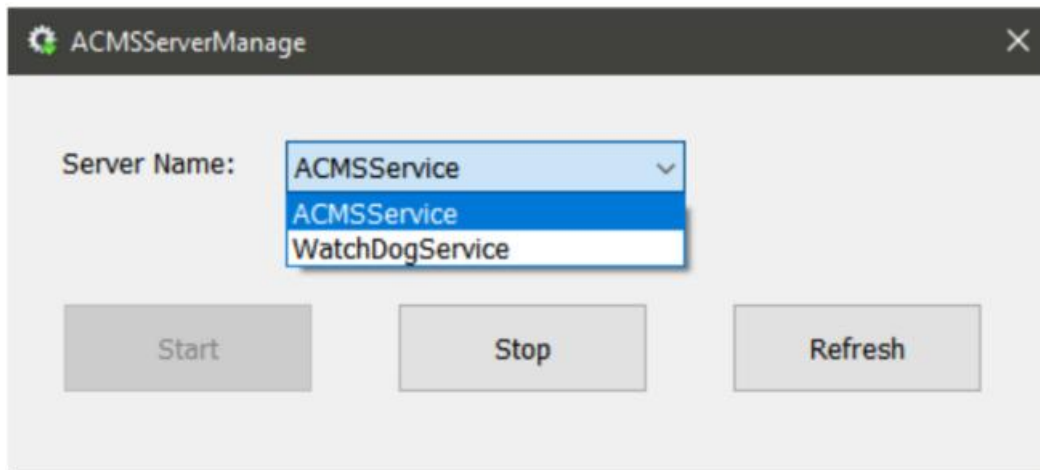ACMSServer Manage is software that is installed along with the ACMS. The software is designed to provide two types of services called **ACMSService**, and **WatchdogService**.

- **ACMSService:** this service is used to facilitate the two-way communication between the ACMS and the devices for the data transmission, therefore the service must be turned on to ensure the smooth running of ACMS.

- **WatchdogService**: Watchdog will be running automatically upon the completion of its installation by default. **WatchdogService** is responsible for monitoring the **ACMSSevice** status. To be more specific, **Watchdog** will turn on **ACMSService** automatically whenever it finds **ACMSService** is not running, which means **ACMSService** will be running nonstop or will be up and running again on the condition that the Watchdog is on.

2.4. Log in ACMS

To log in to ACMS, you are required to enter the username **admin**, and the password **admin** by default.

To log out, just click ☒ on the upper right corner of the screen.
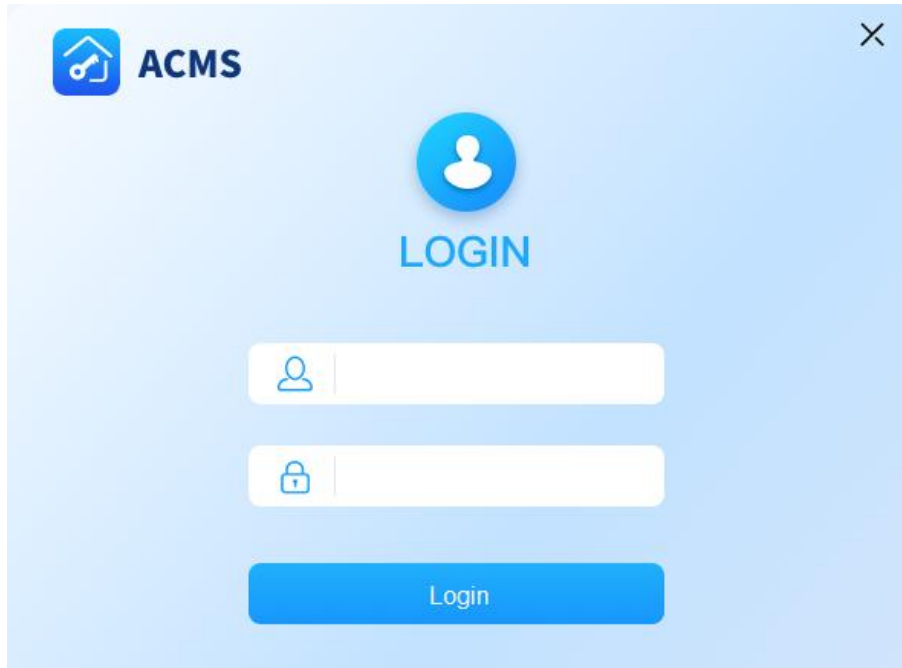
2.5. Configure Network Connection

In order to achieve normal data transmission and interaction with other devices, you are required to select one network adapter that will come with a corresponding IP address so that a sole data transmission port between the ACMS and devices can be established.

> **Note:**
> - We recommend enabling only one network adapter on your PC.

1. Click on ⚙ on the upper right corner and select **System Setting**, then select **Network**.
2. Select your network adapter with its corresponding IP address.
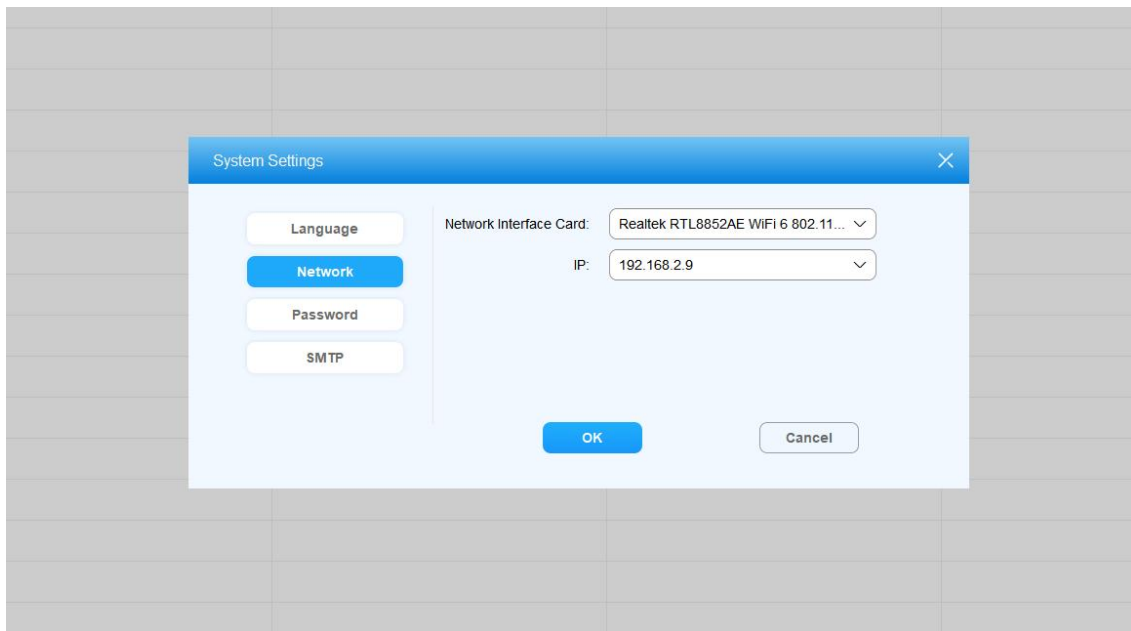
2.6. ACMS Main Interface Introduction

ACMS main interface mainly consists of four modules, namely the **Device Management module**, **Personnel Management module**, **Access module**, and **Attendance module**.
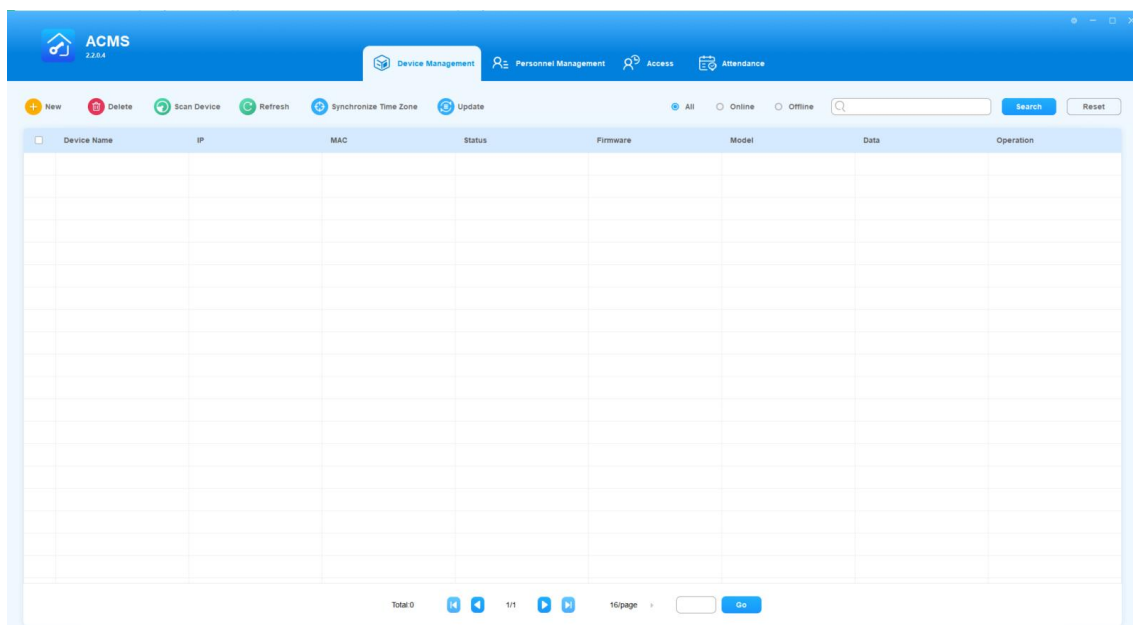
- **Device Management Module**: used to add, delete and search the devices as well as synchronize the data and time zone to the device.

- **Personal Management Module:** used to manage the department-based personnel data in terms of creating department(s), managing the personnel information, and assigning configured PIN and Card numbers to personnel or personnel within a selected access authority group.

- **Access Module:** used to create and manage an inventory of access control time schedules, and it serves as a platform on which you can manage and deploy the access control by establishing a corresponding relation among **device**, **department**, **personnel**, and **access control schedule**, forming an authority group. In addition, you can manage the door log, temperature log, and log data import and export.

- **Attendance Module:** used to manage the holidays, attendance points, employee shift schedule, attendance records, and reports, etc.

3. Device Management

In the device management module, you can manage the device in terms of adding, editing, deleting the device(s) individually or in batch, and synchronizing the time zone to the corresponding device(s) you selected. You can also search the data.
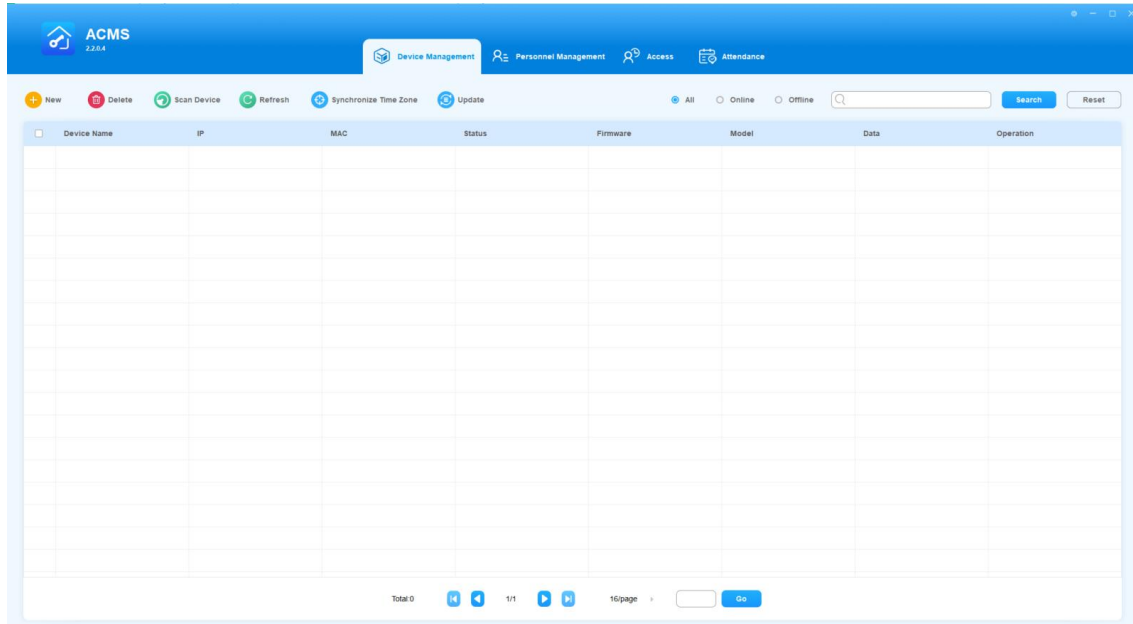
3.1. Add Device

Adding a device in ACMS can be done manually or by scanning.

When a device is in self-configuration mode and is added to ACMS, it will automatically switch to ACMS mode. This mode can be confirmed by accessing the device web interface and going to **Status > Info > Product Information**.
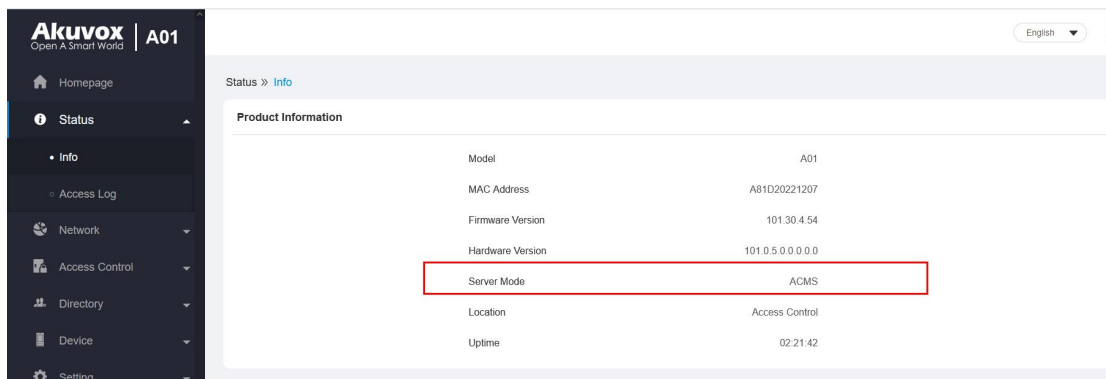
NOTE：

To scan and add devices successfully, the devices cannot be connected to the SmartPlus Cloud.

3.1.1. Add Device Manually

1. Click **New** ⊕ in the upper left to open the Add Device page.
2. Do as the following:
    - Enter the device name and its MAC address.
    - Click **Add Relay** or **Add Security Relay** to add additional relays if needed.

    NOTE:

    You can open 4 relays and 2 security relays at the maximum, with at least one relay or security relay being required. The relay name can be modified.

3. Click **OK**. The added device and its information will be displayed on the Device Management screen.
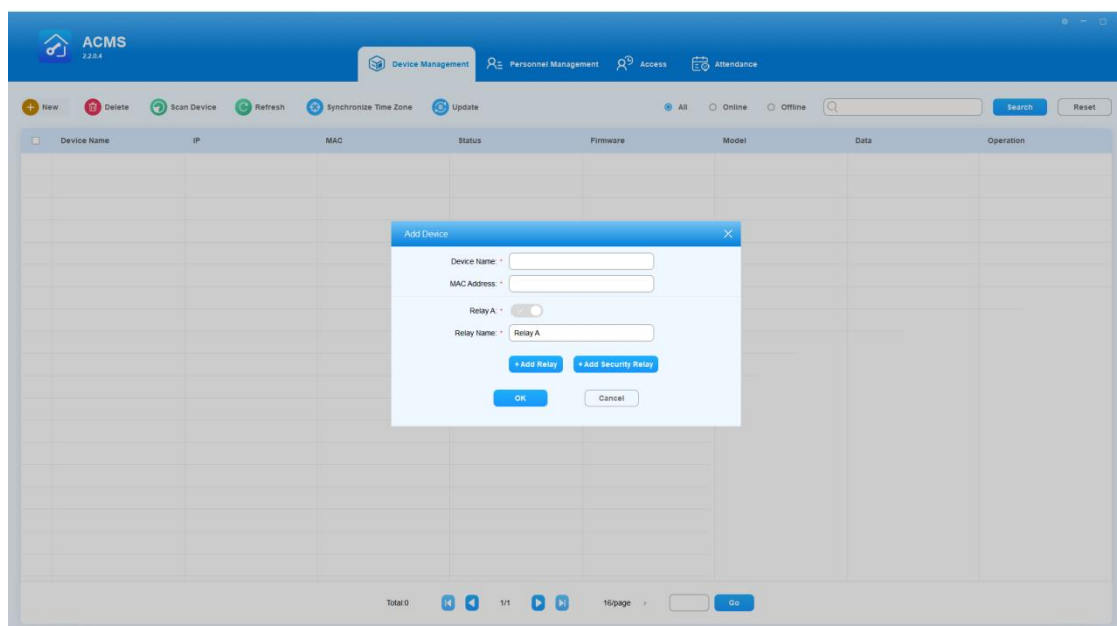

3.1.2. Add Device by Scanning

1. Click **Scanning Device** 🔄 to discover all the devices in the same LAN network.

2. Click **Refresh** 🔄 to refresh the device list if needed.

3. Check off the desired devices and add click **Add** ⊕.

4. Click **Yes** when you are asked.

NOTE:

If a device is added through scanning or already exists in ACMS, and ACMS is subsequently upgraded to the latest version, the device will, by default, have four relays (although some devices may not actually have four relays, the interface may still show four relay options) and two security relays enabled.
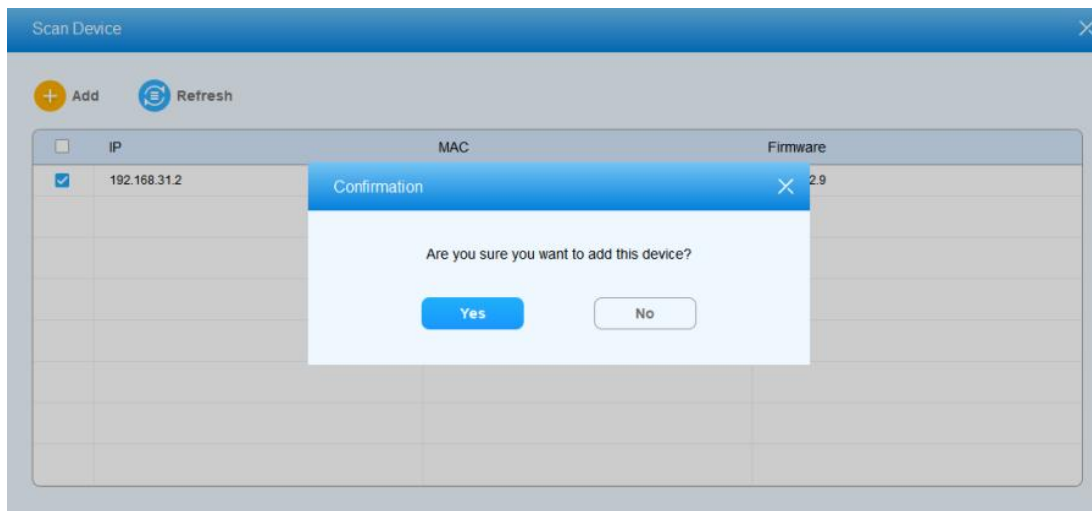
3.2. Edit Device

You can edit the device if needed.

1. Click [icon] of the desired device.
2. Edit the device name, MAC address, or add or disable relays according to your need.
3. Click **OK**.
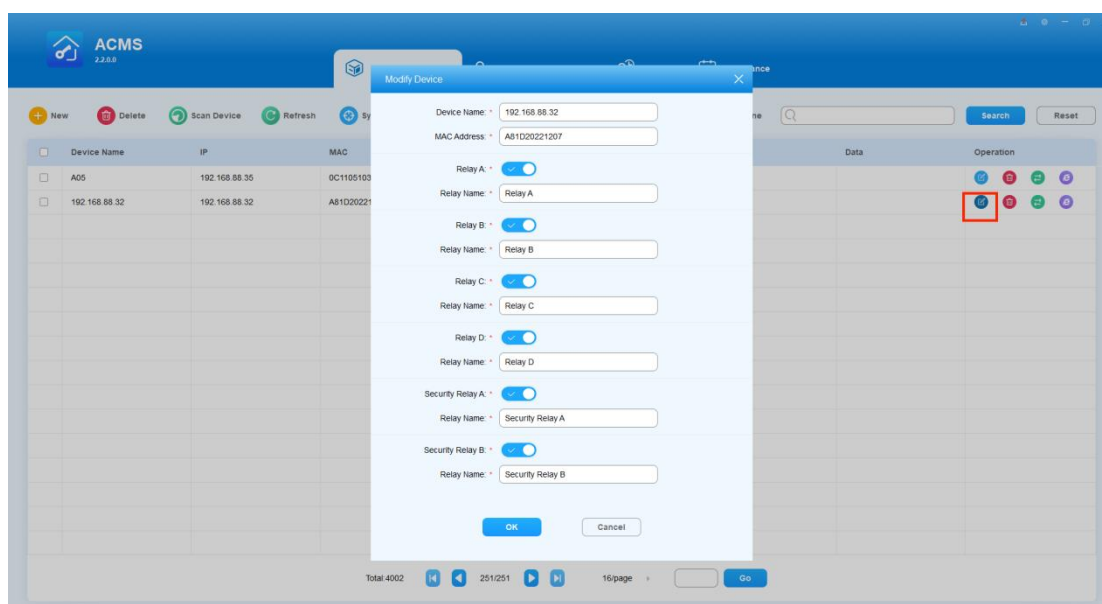
## 3.3. Delete Device

To remove a device, do as the following.

1. Tick the check box of the specific device(s)you want to delete.

2. Click the 🗑 of the specific device to delete the device or you can delete multiple devices by clicking the 🗑 Delete to delete the device in batch at one time.

3. Click **Yes**.
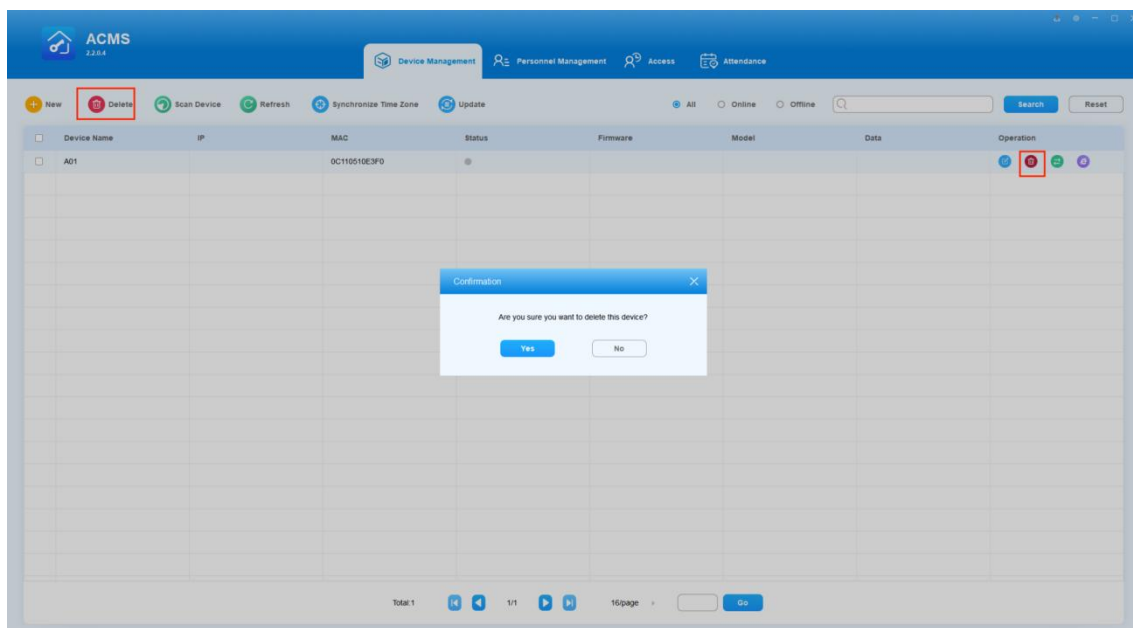
3.4. Search Devices

The device search can be done by first filtering the device status as indicated by **All**, **Online**, and **Offline** before entering the search information for the targeted device search.

1. Click to select the filtering conditions among **All**, **Online**, and **Offline.**

2. Enter the information such as **Device Name**, **MAC**, **IP**, and **Firmware** and click on **Search**. You can click on **Reset** to clear the information in the **Search** field.
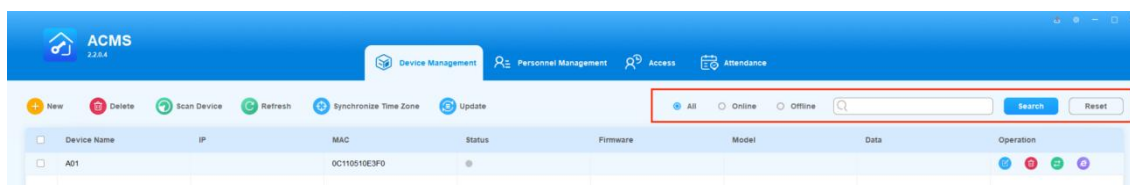
3.5. Refresh Device Information

When any changes are made to the device information displayed on the Device Management screen, such as IP address, MAC, status, firmware, mode and more, you can update such information by clicking **Refresh** in the upper tab bar.
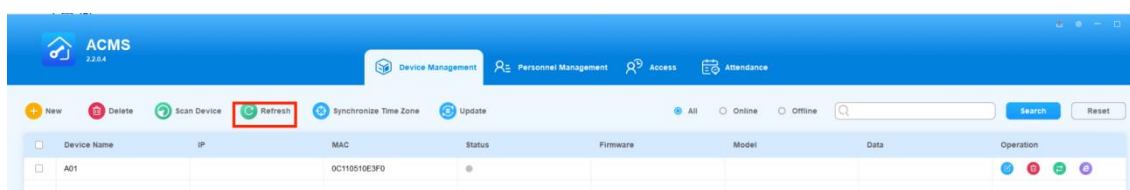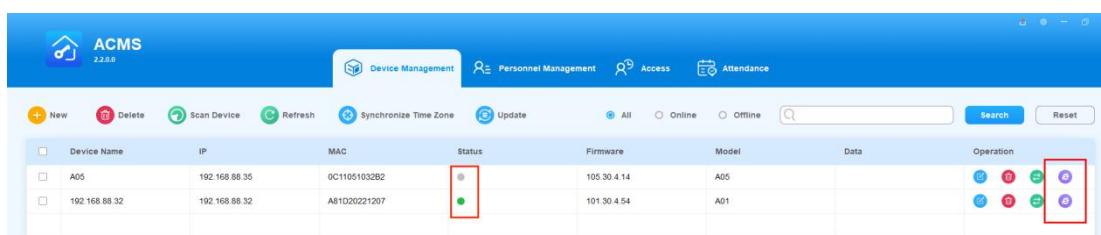

3.6. Go to Device Web Interface by One-Click

You can go to any ONLINE device's web interface by clicking on its icon in the Operation column.

NOTE:

An online device is indicated by a green dot in the Status column, while an offline device is a gray dot. You can only access the web interface of an online device by clicking on it.

3.7. Sync Between ACMS and Devices

3.7.1. Sync Access Authentication Data

ACMS is able to facilitate the synchronization of door access authentication data, e.g., fingerprint and face data, between ACMS and the device(s).

3.7.1.1. Obtain Data from Devices

The Data column displays the identifiers for door access authentication data, such as fingerprints, obtained from each device. When a new device is added, this column will initially be blank until data is retrieved from the device.

To request data from a device, do as the following.

1. Make sure your desired device is online, and click 🔁 in its Operation column.

2. Clicks **Yes** on the confirmation window, the system will start to retrieve data from the device.
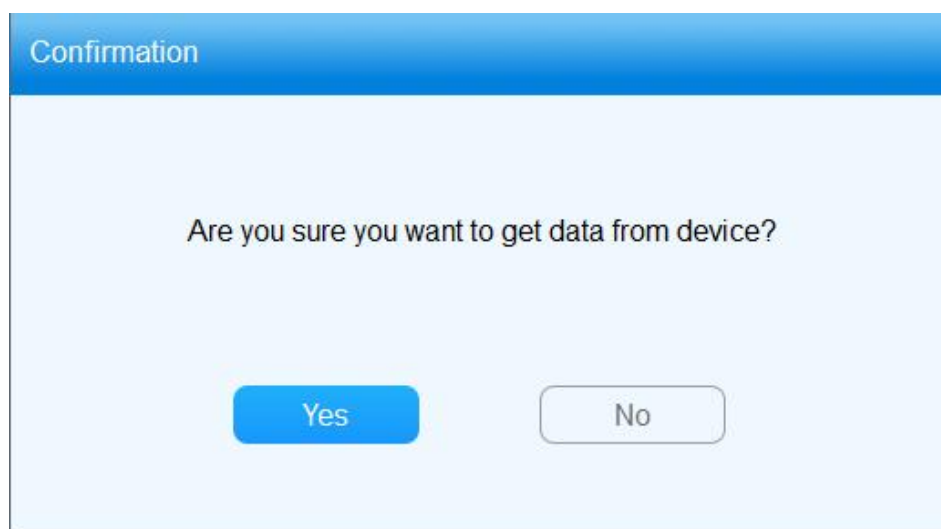
3. The corresponding data identifier will then display in the Data column.

NOTE:

- For an access control device, the data obtained is facial recognition data for all personnel which is displayed as **Personnel Data** in the Data column.

- For an R29 device, the data obtained is fingerprint data and is displayed as **Finger Print**.

3.7.1.2. Send Data to Devices

To transfer door access authentication data between devices, you can synchronize the data obtained from one device to another. For instance, if you have fingerprint data for users 1, 2, and 3 on device A, you can sync this data to device B. This will enable users 1, 2, and 3 to use their fingerprints to access device B.

1. Find the device that you need its door access data, and click the data type in the Data column.

2. The Sync Data to Device screen opens. Check off the device that you want to apply the data to.

    NOTE:

    - If the data to be synced is fingerprints, then the device list only displays available R29.

    - If it is Personnel Data to be synced, then the device list only displays available access control devices.

3. Click **OK**. Wait until the device's status changes to be Succeed.

3.7.2. Sync Time Zone to Devices

In Version 2.2 and later, upon connecting to ACMS, the device will receive an update with the computer's time zone file and current time zone. This ensures consistent times on both ends and avoid the time inconsistency due to daylight saving time.

If the computer's time zone changes, to sync it for selected devices, do as the following.

1. Check off the desired device(s), and click **Synchronize Time Zone** on the upper tab bar.
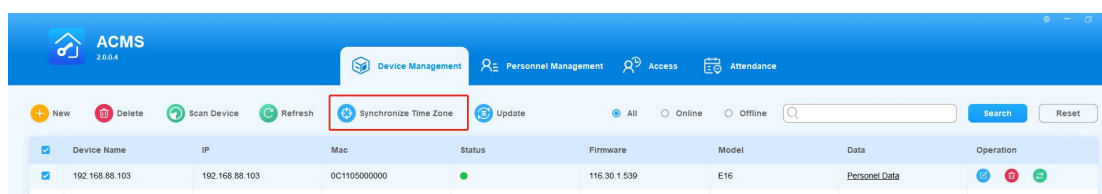
2. Confirm the operation by clicking **Yes**.
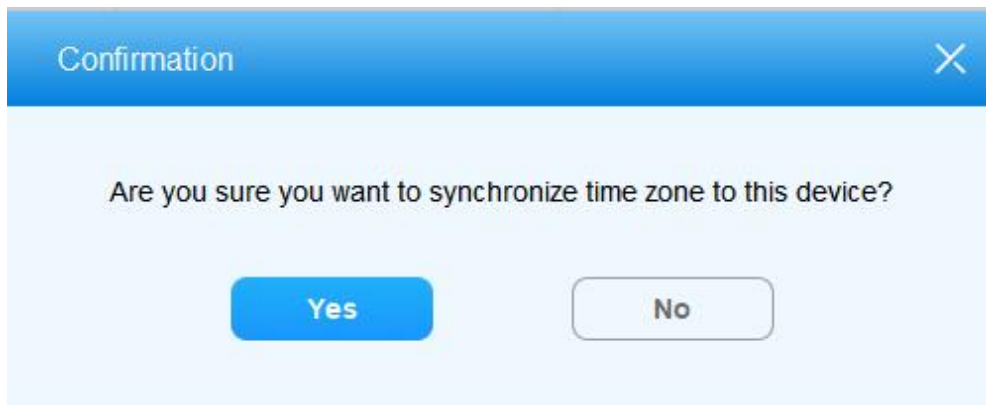
3.7.3. Update Access Control Changes to Devices

To apply access control configurations and changes, including both personnel and access group, to corresponding devices, you need to sync them manually.

3.7.3.1. Update Authority Group

The Update Authority function allows for the synchronization of changes made to the Authority Group associated with devices. If any changes are made to the authority group, the Update Authority button appears in the upper right corner

. Clicking the button will take you to a page that displays all the related devices. To send the updates, just click **Update to Devices.** Once the changes are successfully sent, the button will disappear.
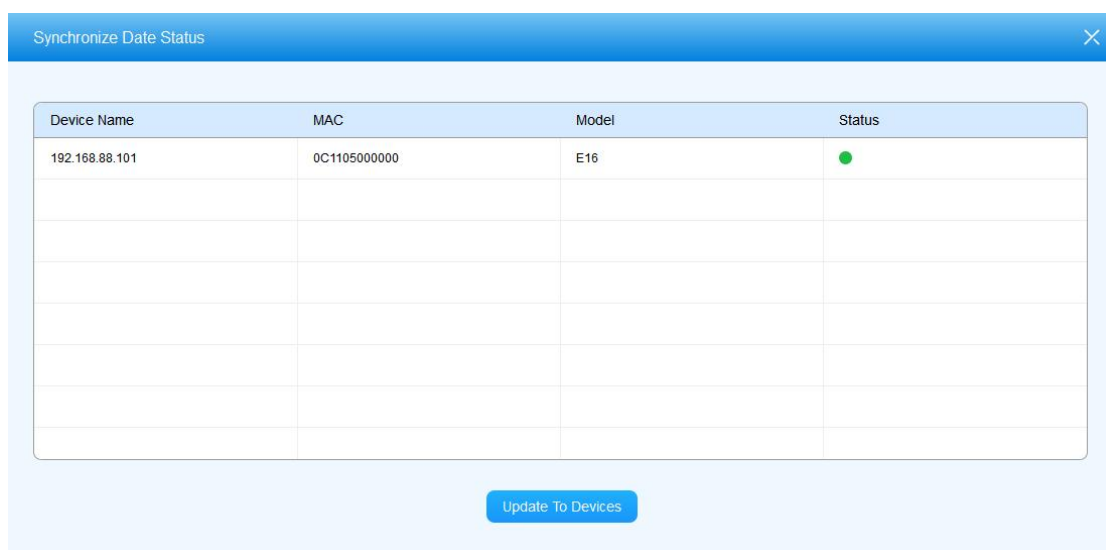
3.7.3.2. Update Personnel and Authority Group

If you make any changes to on the Personnel or Authority Group screens, you need to go to the Device Management page, select the relevant devices, and click to send the changes to the devices.

4. Personnel Access Management

The Personnel Management module is primarily designed to manage department and personnel in terms of adding, deleting, editing personnel and department, importing, and exporting the personnel data and photos, and adjusting the department for personnel. You can also search the personnel to find the information needed.
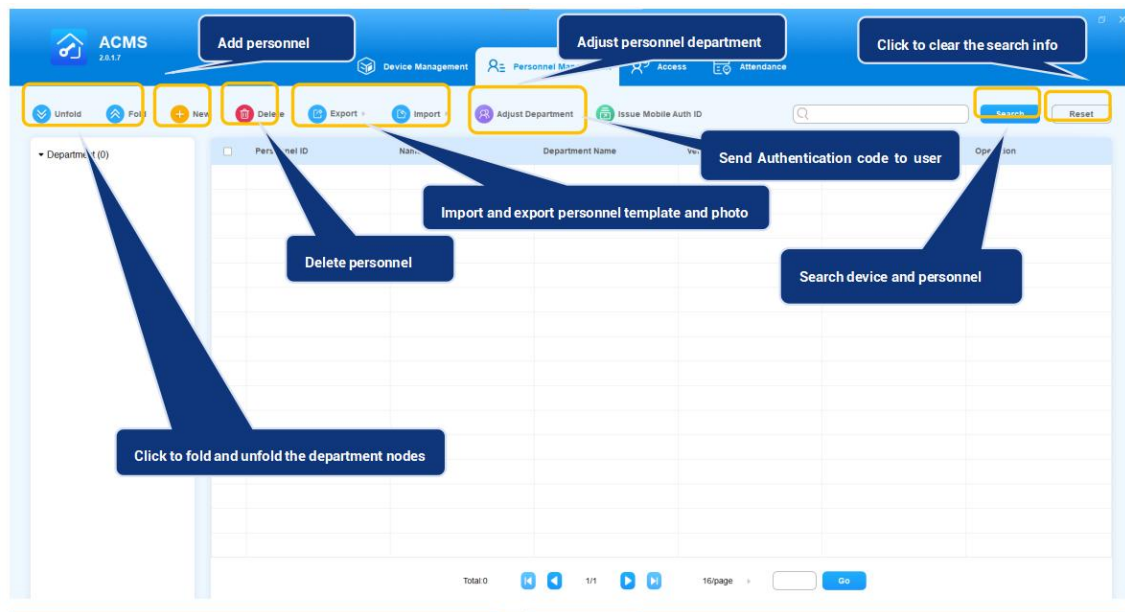

4.1. Add Department

Departments are structured in nodes. Each level of the node can be further extended to the nigh level of subordinating nodes in descending order, however, there is no limitation on the number of paralleled subordinating nodes. You can manage and add the personnel to the designated department at different levels of nodes.
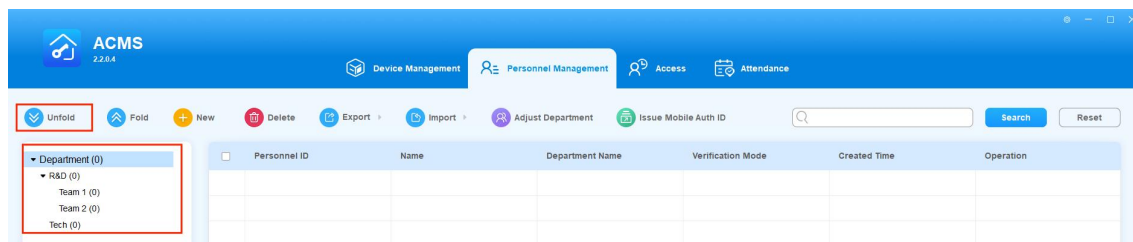
1. Click on ⊕ at the root node.
2. Enter the department name to add a department.
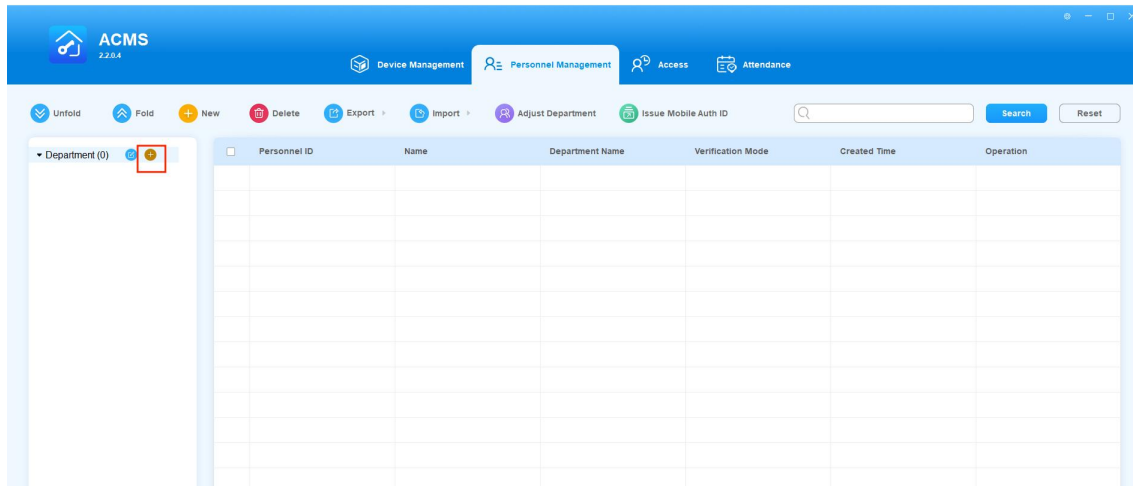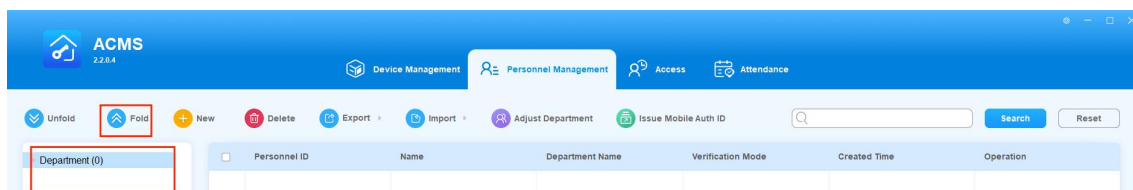
3. Click **OK** for confirmation.
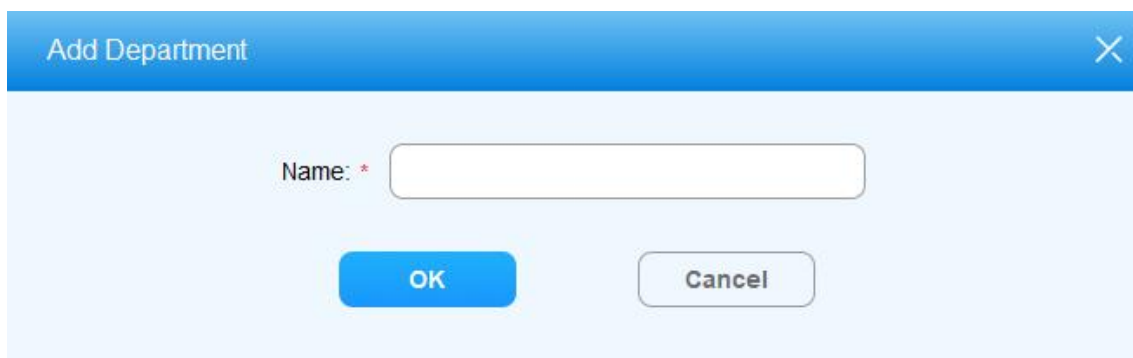
If there are several departments, you cam click on to quickly display all of them.
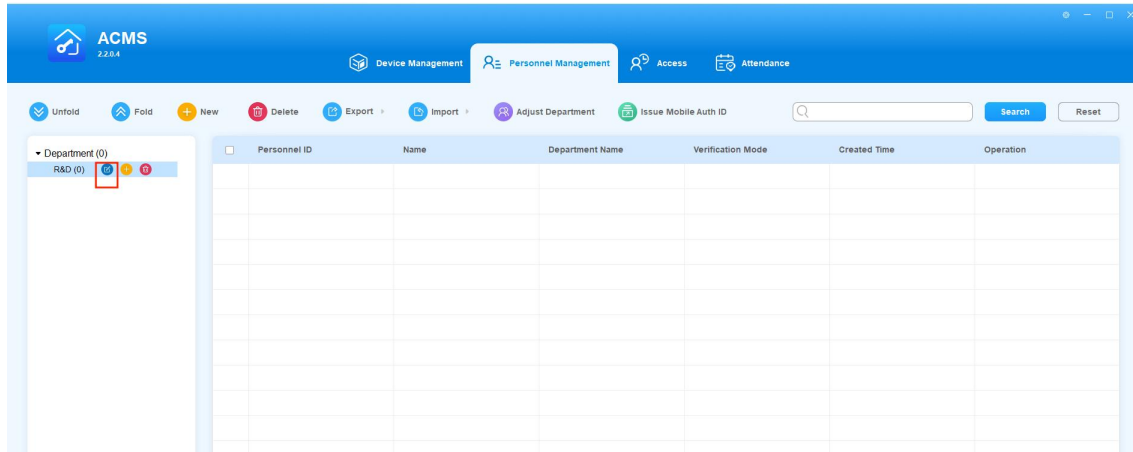

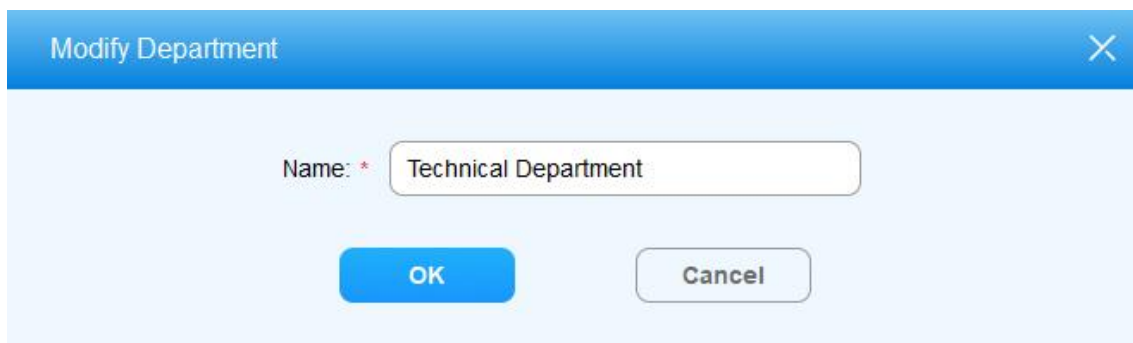You can also click to collapse the list.

4.2. Edit Department Name

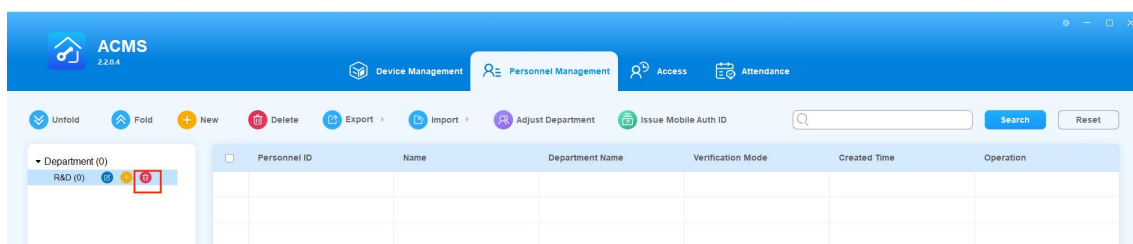1. Click on of the department for which you want to change the name.

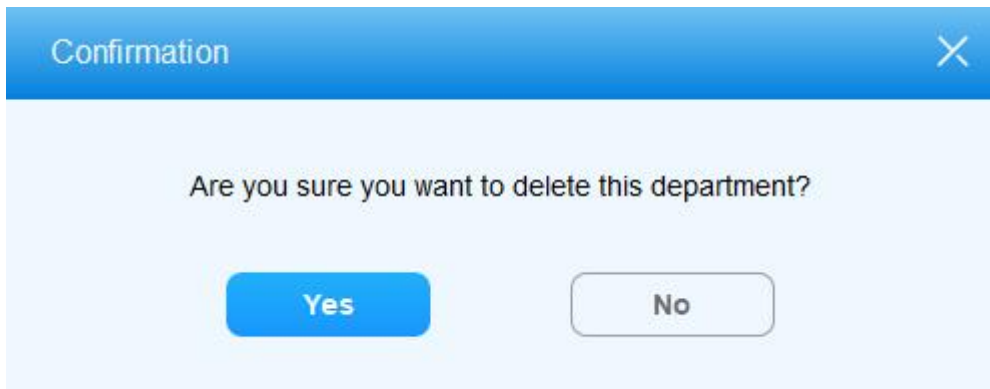2. Change the department name according to your need, and click **OK** for confirmation.

4.3. Delete Department

You can delete the department you created if needed.

1. Click on of the department you want to delete.

2. Click **Yes** for confirmation.

> **Note：**
>
> ● The Department by default can not be deleted.
>
> ● Only when the department (Except for the Department by default) has no other subs or personnel can it be deleted.

4.4. Add Personnel

You can add personnel in the designated department in which you enter the personnel information such as personnel name, ID, photo, etc. While assigning the personnel with the PIN code and card number for the door access.

1. Click on the department in which you want to add personnel.

2. Click ⊕ New to go to **Add Personnel** interface.

3. Enter the personnel information.

4. Click on **Browser** to upload the personnel photo and click on **Reset** if you want to clear the photo.

5. Tick the check box to select the authority group you created in **Access Control** module, or you can search the authority group in the field.

6. Click **OK** for confirmation.

Key information for adding personnel

No.	Information	Description
1	**Personnel ID***	Personnel ID number (employee number) is the required information that can only be consisted of alphabets or numbers with 23 characters maximum.
2	**Name***	Personnel name is the required information with 63 characters maximum.
3	**Department**	The department field automatically displays the node (sub-department) that is immediately subordinated to the exact department you selected. If the department you select has no nodes (sub-department) under it, then the node for the department selected will be displayed. For example: if you click and select the node "**Technical Training**" under the parent node "**Technical Department**", then the node information for the "**Technical Training**" will be displayed.
4	**Gender**	Gender is "---" by default, you can select **"Male**" or "**Female"**.
5	**Email**	Email is left blank by default with a maximum of 127 characters.
6	**Mobile Phone**	Mobile Phone is left blank by default, you can enter the mobile phone number that should be no more than 63 characters.
7	**Certificate Type**	You can select the Certificate type (ID type) from the pull-down list according to your need.
8	**Certificate Number**	You can enter the specific ID number needed for the personnel with 63 characters maximum.
9	**Hire Date**	Hire day refers to the employee start date.
10	**Birthday**	Birthday refers to the data of birth of the employee.
11	**Private Key**	Enter the configured PIN code for the door access. The PIN code can only be consisted of numbers (2-8 characters in combination) and should

		not be duplicated.
12	Card Number	You can enter multiple ID card numbers separated by ";" with no more than 63 characters. And the ID number should not be duplicated.
13	Authentication Code	An authentication code is used for door opening via **My MobileKey** app. Click to obtain the code, or click to delete the code. **Note**: 1. The authentication code is used with My MobileKey for hands-free door unlocking. With the app, the door can be opened automatically as you come close to the door or with a single click on the app. 2. Authentication code will be sent via SMTP server to the user's email after you fill in the user's email and set up the SMTP server.
14	Pairing Status	It will display "Paired" if the authentication code you obtained has already been set up in My MobileKey. It will display "Unpaired" if the code you obtained has not been set up in the app.
15	Web Relay	Select the Web Relay associated with the personnel. The default is 0. After syncing to the device, you can check this info by going to the device web interface **User > Web Relay** page.
16	Floor	Select the floor number(s) that the personnel is allowed to access.
17	Authority Group	Search and select the authority group that incorporates a designated set of door access control schedules, devices and personnel for the door access.

> **Note**：
>
> - The personnel photo(s) to be uploaded for the facial recognition can be in .jpg, .jpeg or .png format with less than 10 MB.

> **Note**：
>
> - Multiple door access types such as Face, PIN code, and ID card number, Authentication codes can be supported at the same time depending on your need. Authority group (group, name, and device) must be assigned to the person before the above-mentioned access type can be valid. However, all these data have to be synchronized to the designated device on the device management module first.

> **Note:**
>
> - icon will appear on the upper right corner of the screen whenever there are any changes occurred to the authority group setting, you are required to click on the icon to synchronize the changes to the device(s).

4.5. Send Authentication Code

Authentication code can be sent to your targeted users for the My MobileKey application. You will need to set up your STMP server first, then select the users you want to send the code to.

1. Click on ⚙ on the upper right corner, and select **System Setting** in the pull-down list, then select **SMTP**.

2. Fill in, for example, your name or company name for identification, then enter your email and email password.

3. Fill in the SMTP server, and the SMTP port of your email.

After all are set up, the authentication code can be sent to the user's account from your Email.
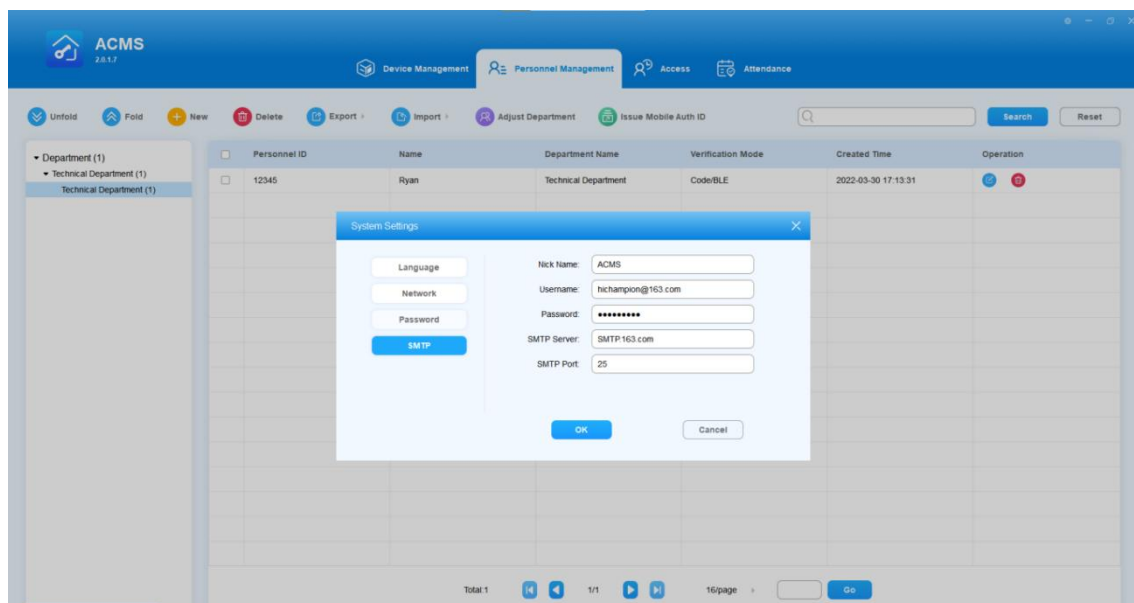
To send the authentication code to the selected users, do as follows:

1. Select Personnel Management Module, then select Issue Mobile Auth ID .

2. Select users you want to send the authentication code to. You can search to find the personnel if needed.

3. Click **OK** for the confirmation.

4.6. Edit Personnel

After adding personnel, you can edit the personnel information if needed.

1. Click on ⬛ or double click on the specific line of the personnel to be edited.
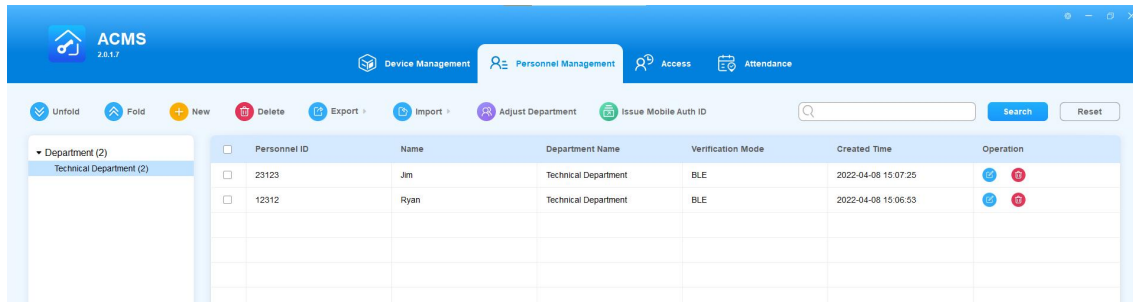
2. Change the personnel information you want to change.
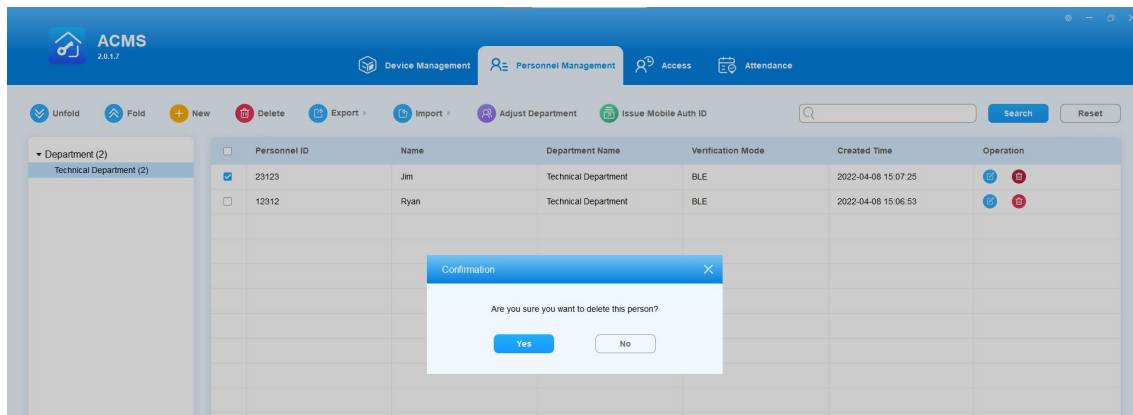3. Click **OK** for the confirmation.

> **Note:**
> - The personnel ID can not be edited or changed.

4.7. Delete Personnel
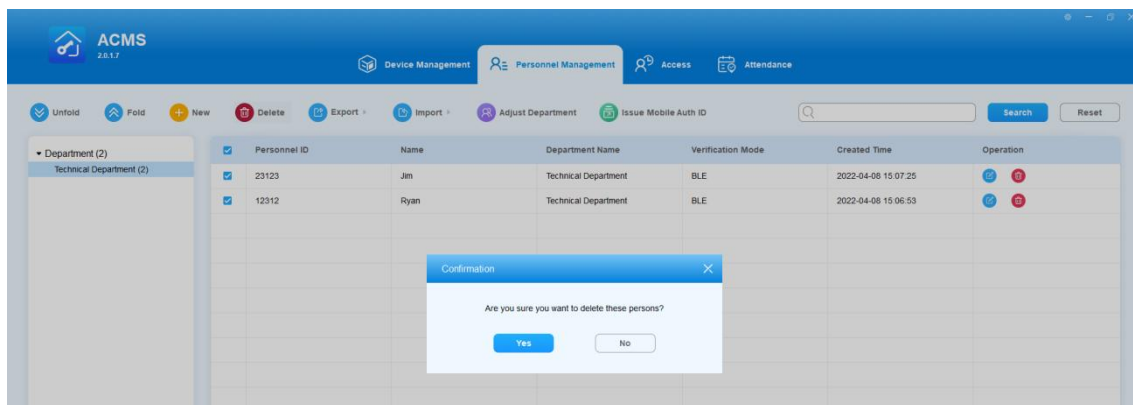
Personnel can be deleted separately or in batch.

- **Delete personnel separately**

1. Click 🗑 of the specific personnel to be deleted.
2. Click **YES** for confirmation.

● **Delete personnel in batch**

1. Tick the check box of the personnel to be deleted.

2. Click 🗑 Delete to deleted the ticked personnel.

3. Click **Yes** for confirmation.

4.8. Import and Export Personnel Data

ACMS allows you to import and export personnel data inclusive of personnel information and personnel photo for the convenience of the personnel management.

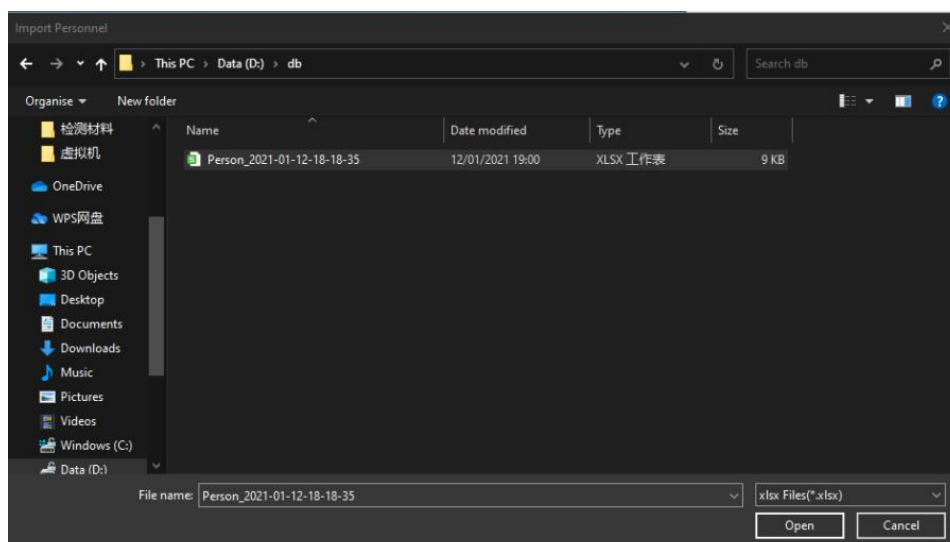## 4.8.1. Import Personal Data

● **Import Personnel Information**

1. Click 📥 Import and click "**Import Personnel**" in the pull-down list.
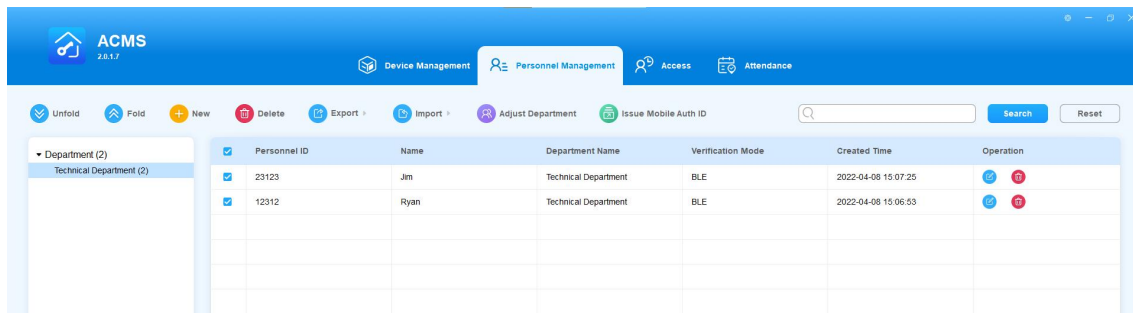
2. Click **Select File** to find the file to be uploaded.
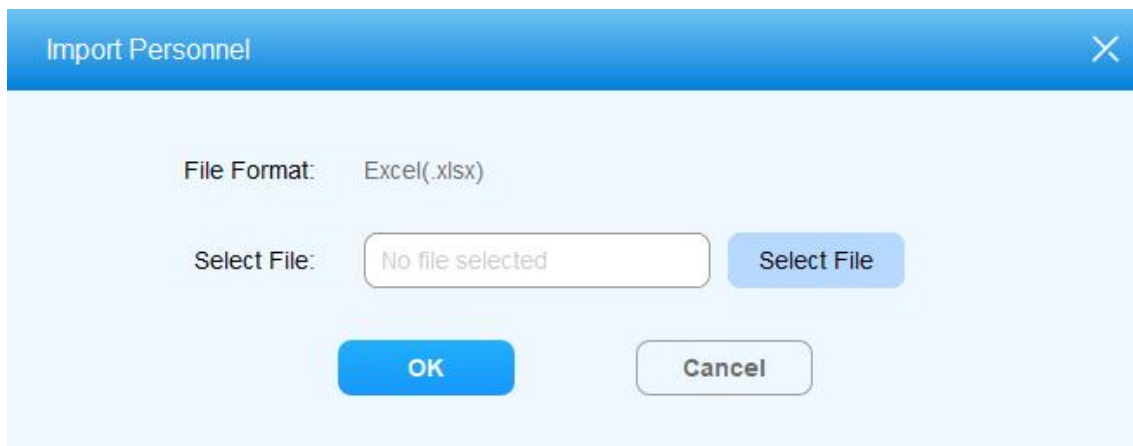
3. Click to select the .xlsx personnel data file and click **Open** to upload the file.

4. Click **OK** for confirmation.

Note:

● Personal data must be filed into the personal data file template without changing the template spreadsheet.

● **Import Personnel Photo**

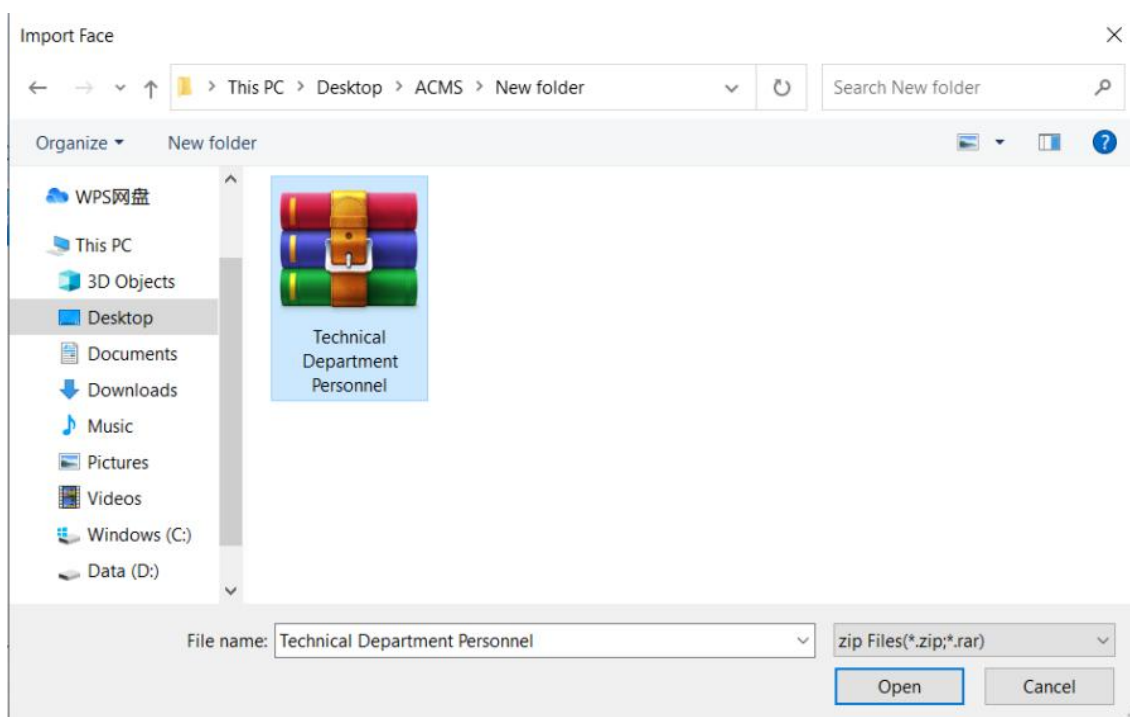1. Select the .jpg or .jpeg photo that are named by "**personnel ID + name**" and right- click to compress them into .zip file directly (for example T1234+Jim).

2. Click and click "**Import Personnel Photo**" in the pull-down list.

3. Click **Select file** and find the .zip photo file.

Import Face

File Format: .zip/.rar

Select File: [No File selected.]   [Select file]
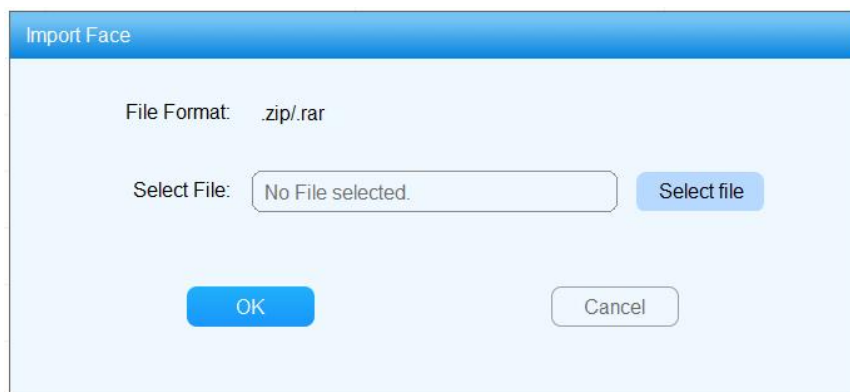
[OK]   [Cancel]

4. Click and select the .zip file and click **Open** to upload the file.

Import Face

This PC > Desktop > ACMS > New folder

Search New folder

Organize ▾   New folder

WPS网盘
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Data (D:)

Technical
Department
Personnel

File name: Technical Department Personnel   zip Files(*.zip;*.rar)

[Open]   [Cancel]

5. Click **OK** for confirmation.
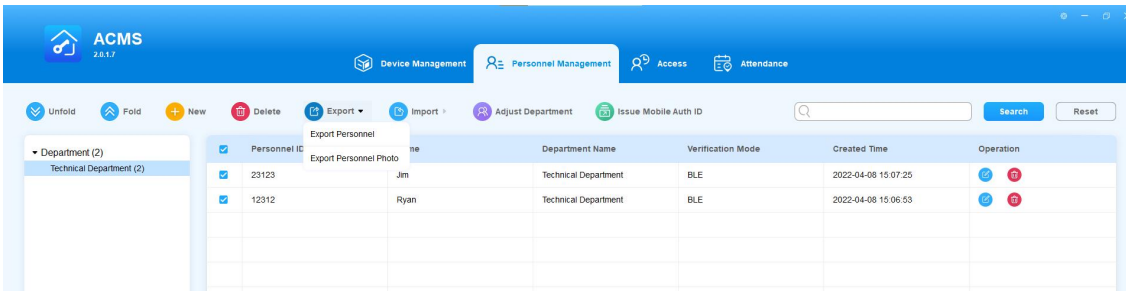
4.8.2. Export Personnel Data

● **Export Personnel Information**

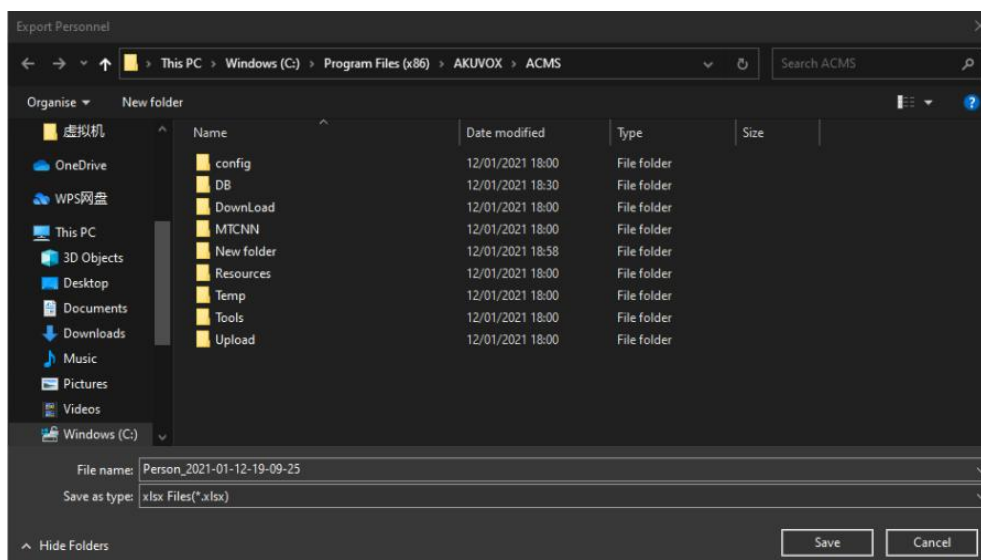1. Click and click on **Export Personnel** in the pull-down list.

2. Select the path in your local PC to export the personnel .xlsx file.
3. Click **Save** to export the file to the designated path on your computer.

Personnel Information File Template:

Key Field Format:

| Field Name	Field Format Requirement
Personnel ID	This is the required field with 23 characters maximum (a～z, A～Z, 0～9).
Name	This is the required field with 63 characters maximum.
Department	This is the required field with 127 characters maximum. **NOTE:** If the department you filled in does not exist in ACMS, the system will not import this employee's info.
Gender	Fill in **Male** or **Female**.
Certification Type	Fill in 1."**Passport**" 2."**Driving License**" 3."**ID Card**" 4."**Other**".
Hire Date	Fill in data format: **Y/M/D**.
Birthday	Fill in data format: **Y/M/D**.
Private Key	If there are several same Private Keys for different imported person, only one person can keep the key, and the Private Key filed of other persons will be left empty.
Card Number	If there are several same Card Number for different imported person, only one person can keep the card, and the Card Number filed of other persons will be left empty.
Web Relay	If the value you filled in is out of the valid range or is empty, the info will not be imported.

| Floor	If the value you filled in is out of the valid range or is empty, the info will not be imported.

Note:

- When using the template, please edit the parameters according to the editing format in the template. If you change the template format at will, it may cause errors.
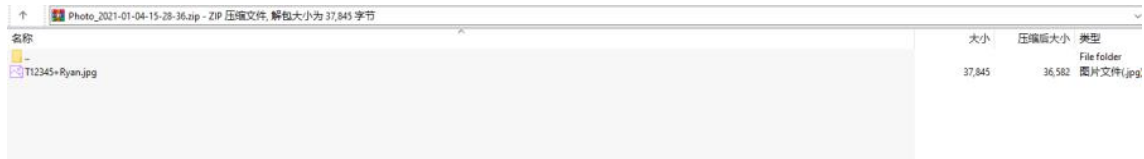
● **Export Personnel Photo**

1. Click and click on **"Export Personnel Photo"** in the pull-down list.
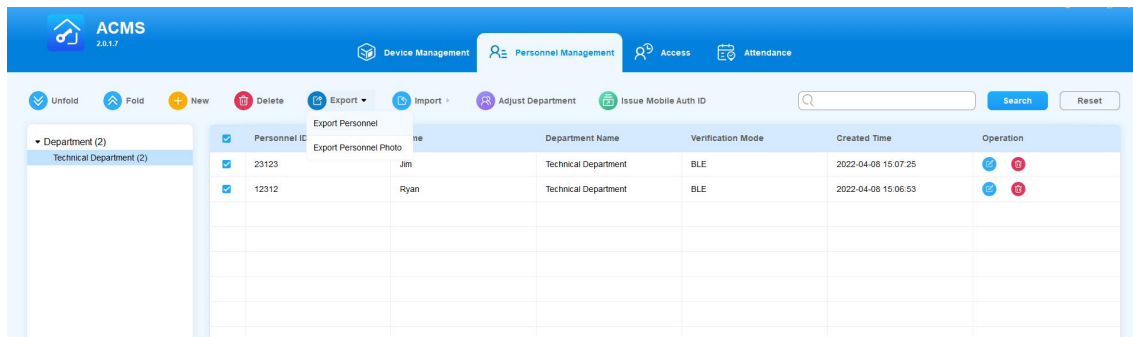
2. Select the path on your local PC to export the personnel photo .zip file.

3. Click on **Save** to export the file to the designated path on your computer.
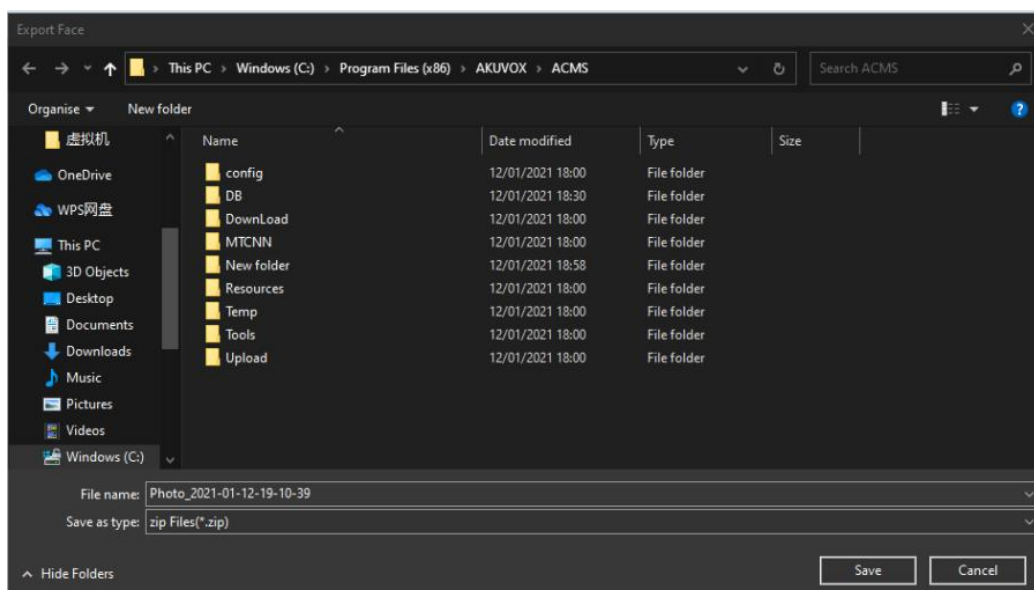
● **Personnel Photo File:**

4.9. Adjust Department for Personnel

You can make personnel adjustments by moving the person to a different department if needed.

1. Tick the check box of the personnel for whom you want to adjust the department.

2. Click and select the department to which you want to move the personnel.

3. Click "**OK**" for confirmation.
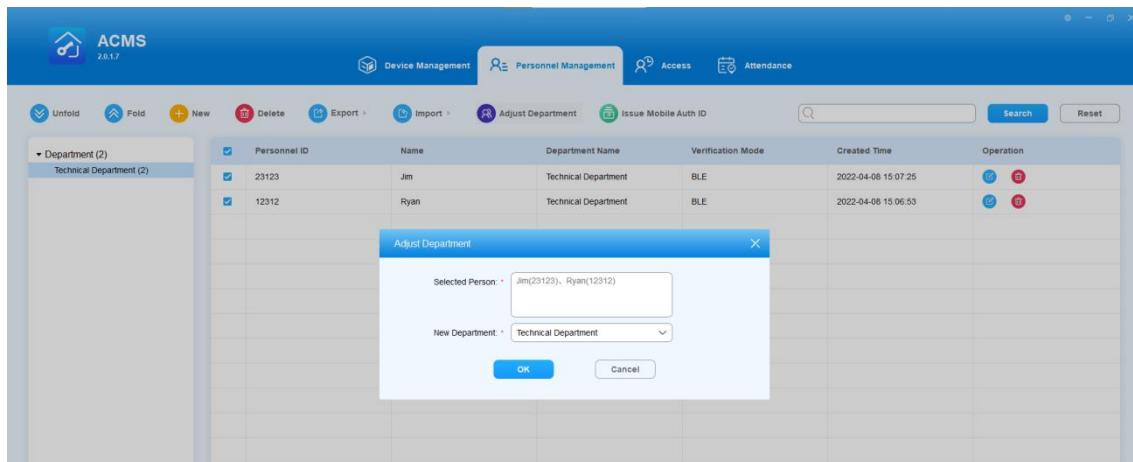
4.10. Search Department and Personnel

You can enter the personnel ID, Name, and department name in the search field to find the information related to specific personnel or department if needed.

1. Enter the **personnel ID**, **name**, and **department name** in the search field.

2. Click **Search** or click **Reset** the clear the search information.

5. Access Control and Logs

In the access module, you can create an inventory of access control schedules that can be readily pulled out to be incorporated with the specific device(s) and authority group as a whole for integrated access control. In addition, the access module allows you to open and close doors with one click, set up anti-passback and see door access logs.
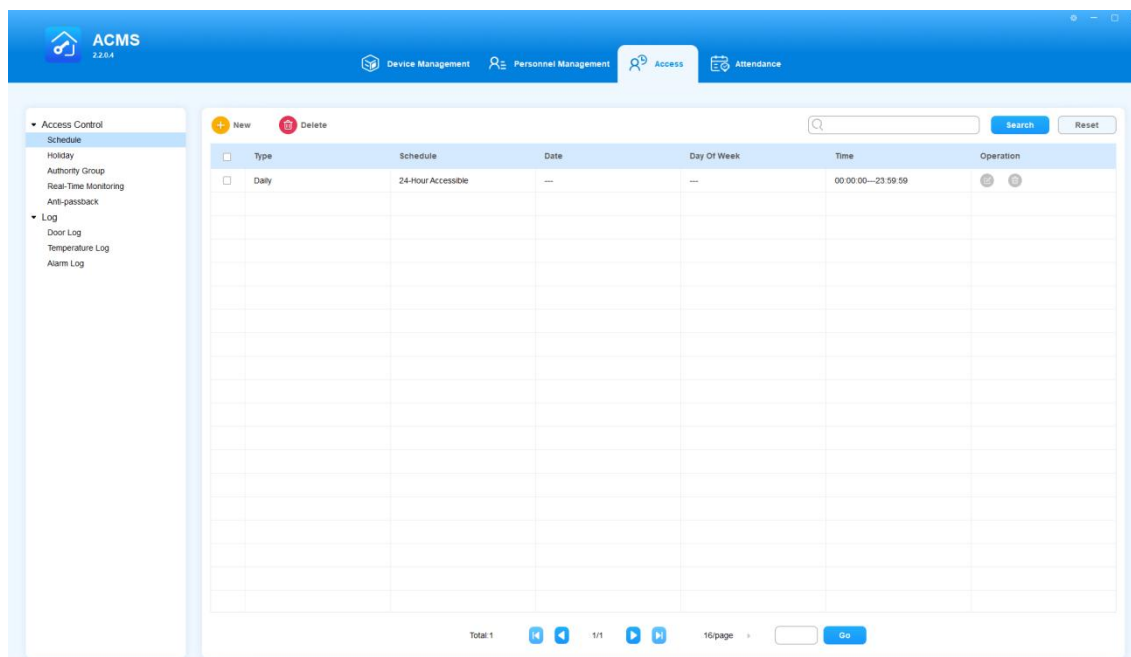
Click to delete the items in the list below

5.1. Manage Access Control Schedule and Holidays

ACMS allows you to create, edit, and delete the access control schedules and holidays.
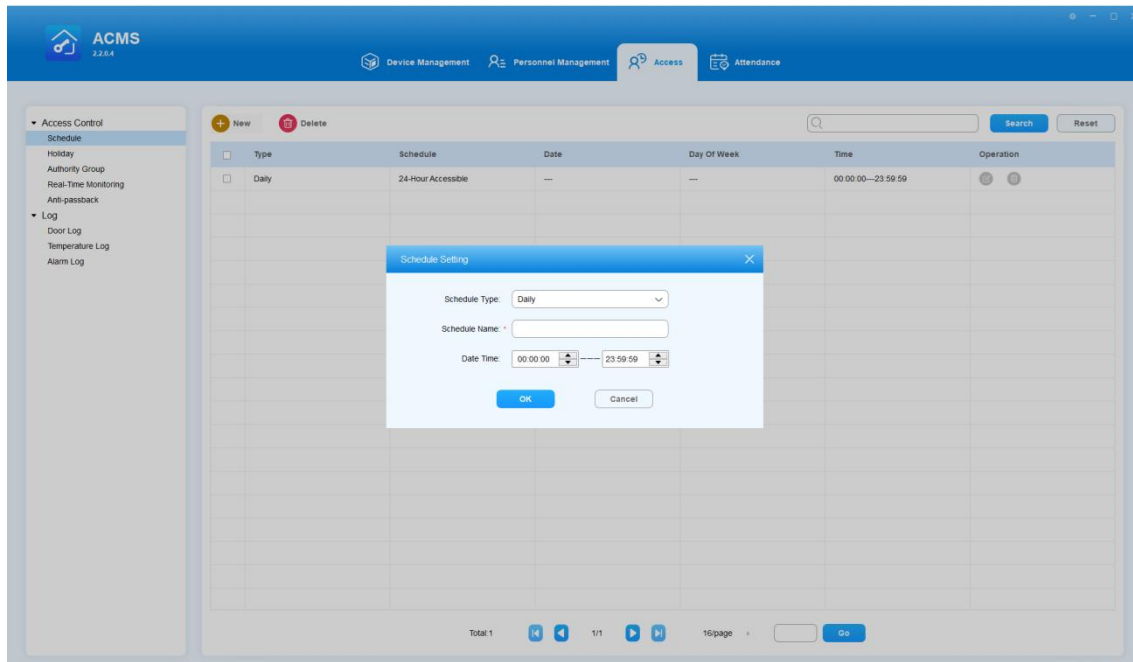
5.1.1. Set the Access Control Schedule

5.1.1.1. Create a schedule

A complete access control schedule includes **schedule type, schedule name** and **time schedule**.

1. Click ➕ New to go to **Schedule Setting.**
2. Select the schedule type among **Daily**, **Weekly**, and **Normal**).

3. Create a proper schedule name.

4. Set the time schedule for the validity of the door access.
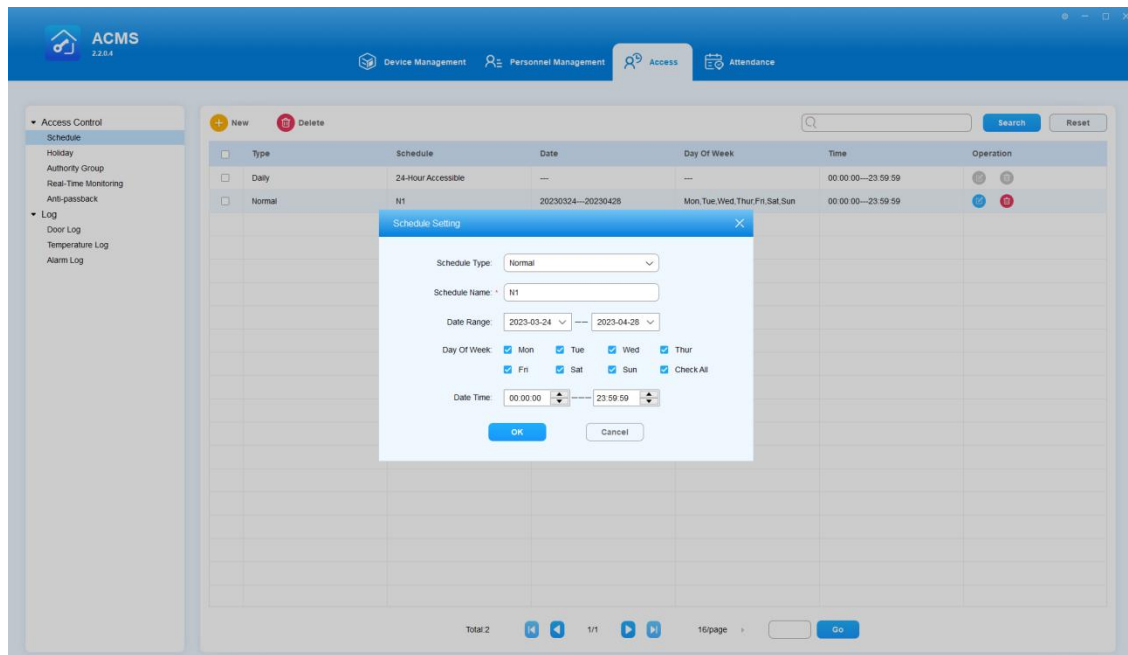
5. Click **OK** for confirmation.

5.1.1.2. Edit Access Control Schedule

To change the schedule settings such as type, time and date, do as the following:

1. Click or double-click on the specific line of schedule type to be edited.

2. Change the schedule related settings according to your need.
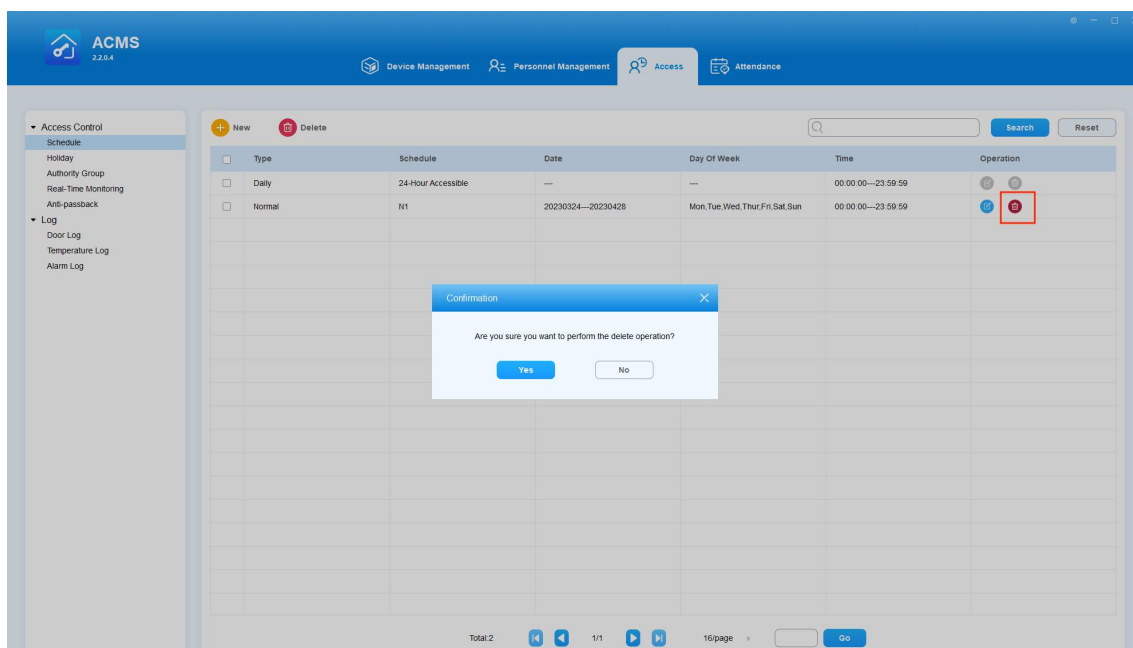
3. Click **OK**.

Note:

● The default daily schedule named 24-HourAccessbile is not editable.

5.1.1.3. Delete Access Control Schedule

Access control schedule can be deleted separately or in batches.

● **Delete the schedule separately**

1. Find the access control schedule you want to delete, and click 🗑 in the Operation column.

2. Click **Yes** for confirmation.
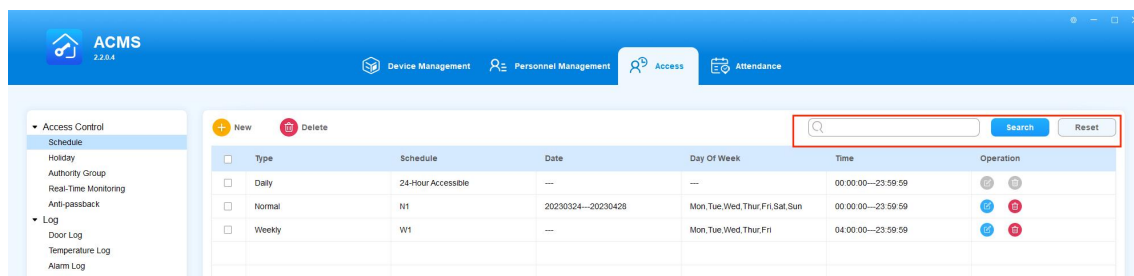
- **Delete schedules in batch**

1. Check off the access schedule to be deleted.

2. Click 🗑 Delete to delete all the schedules that are ticked.

3. Click **Yes** for confirmation.
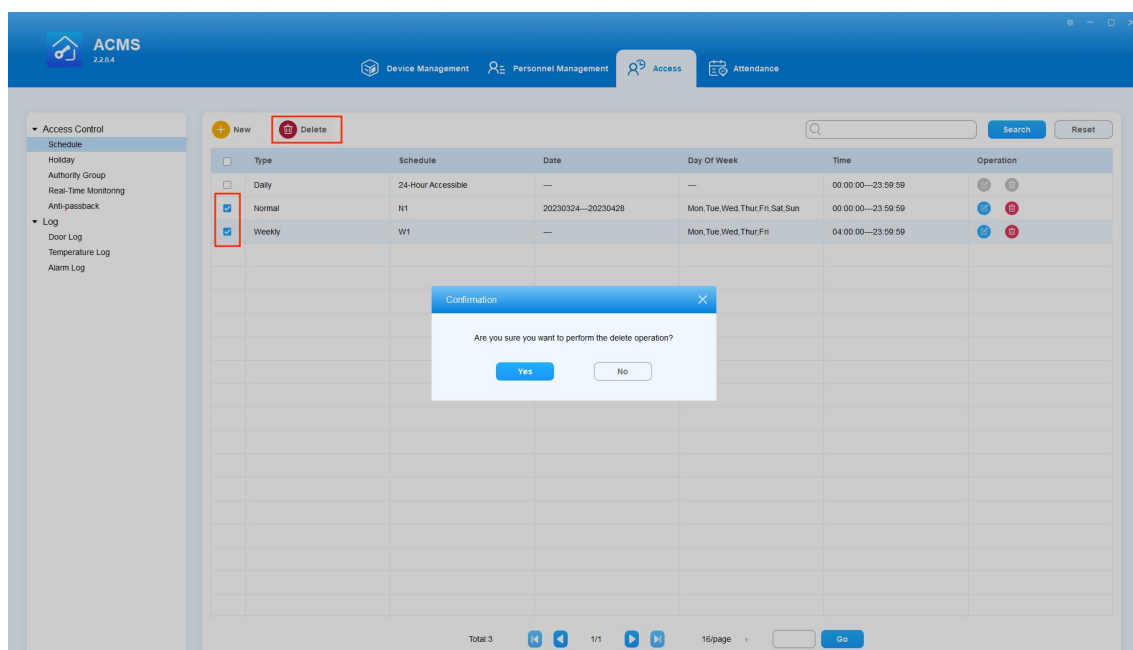
5.1.1.4. Search Access Control Schedule

You can search for a specific access control schedule by entering the keyword in the search field.
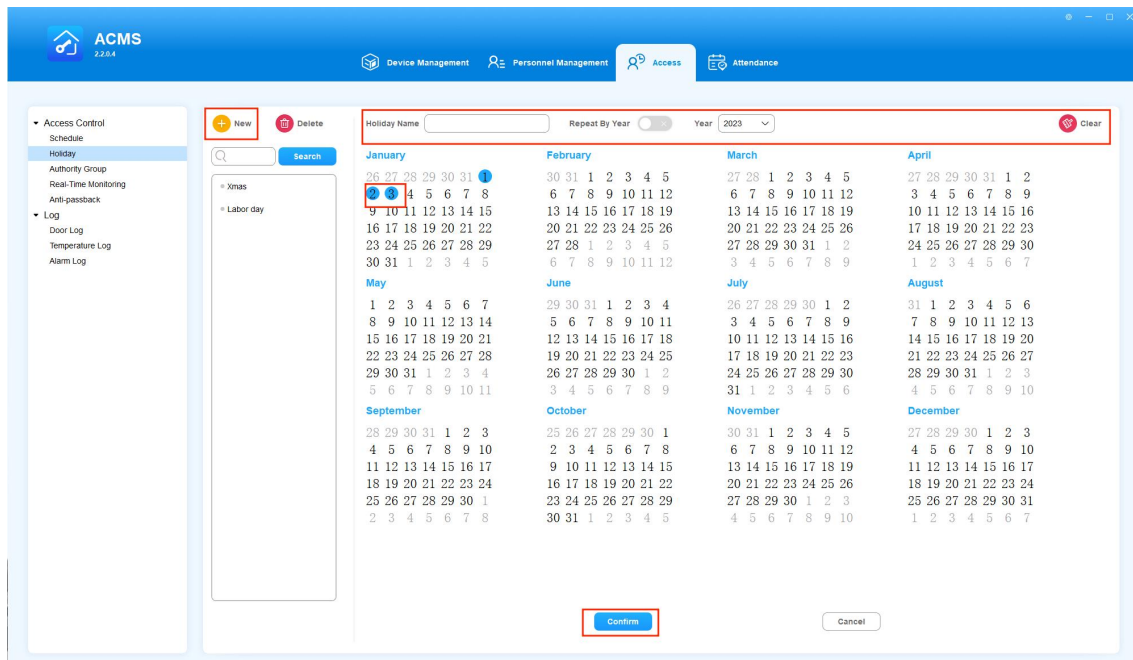

5.1.2. Set Holidays

The Holiday function is used to control access to the office area during the set holiday periods. This feature allows you to add, edit, and delete holidays, and apply them to the Authority Group.

## 5.1.2.1. Add a Holiday

To add a new holiday, do as the following:

1. Click on ⊕ New   on the left side of the screen.

2. Select the desired dates by clicking on them, and they will be marked with a blue circle. To re-select the dates, click   ⊗ Clear   on the upper right.

3. Enter the holiday's name on the upper Holiday Name box. Please note that the name cannot be the same as others.

4. If needed, you can set the holidays to repeat every year by turning on

Repeat By Year ⊘   or change the year   Year 2023 ∨   .

5. Click **Confirm**.

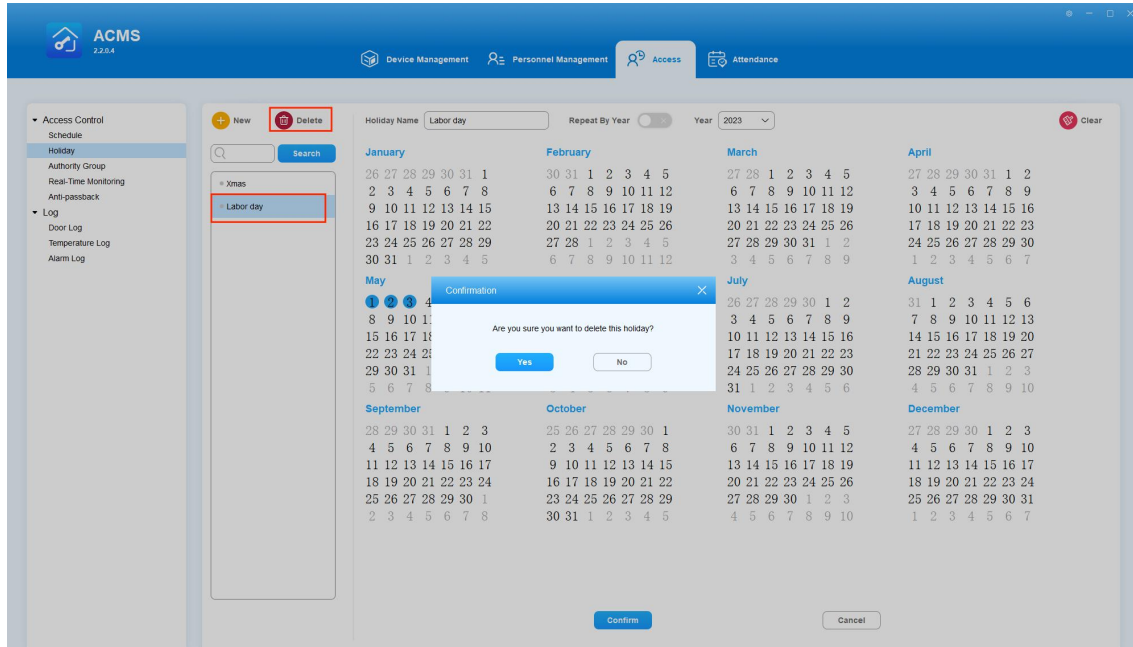Once created, the holiday will be displayed on the left side of the screen.

5.1.2.2. Edit a Holiday

You can edit a set holiday, such as its name, dates, year and more. To do so, just select the desired holiday from left side of the screen, and change the setting.
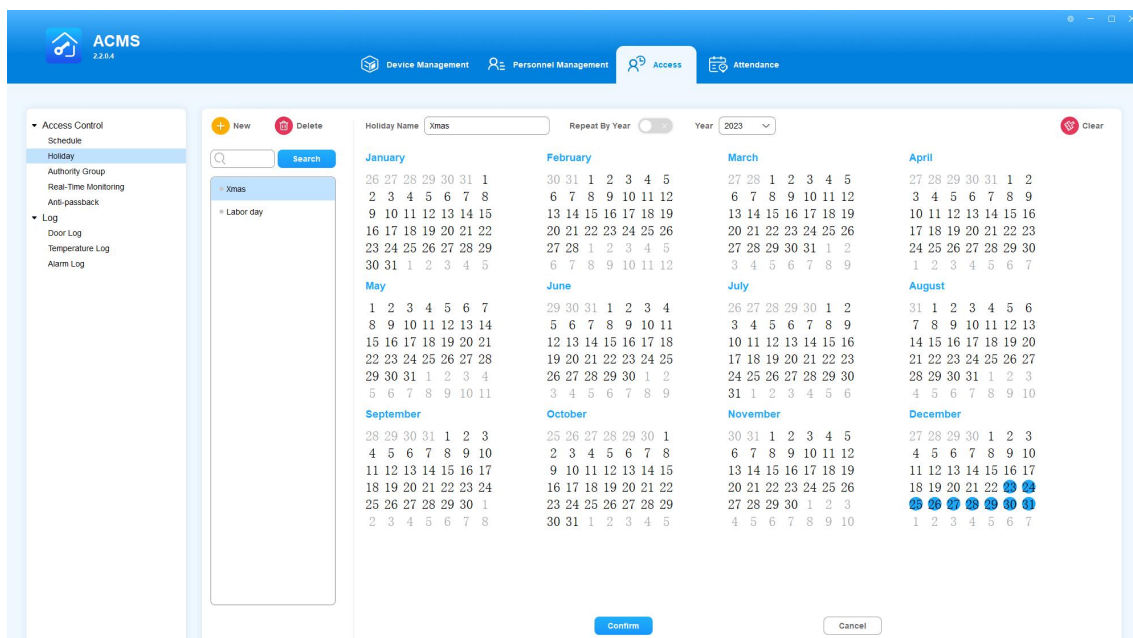
5.1.2.3. Delete a Holiday

To delete a holiday, select it from the left side of the screen, and click 🗑 Delete .

5.2. Manage Access Control

5.2.1. Authority Group

5.2.1.1. Create an Authority Group

You can create an inventory of authority groups that can be applied to the specific person(s), device(s), and access time schedule included in the access control group.

1. Select **Authority Group** in the **Access Control** module.

2. Click ➕ New to create an access authority group.

3. Enter the group name.

4. Select the schedule type and the device(s) together with its relays to be included in the authority group.

5. If needed, select the holidays you want to apply to the group. Once added, the users cannot access preset devices in the holiday period.

6. Add the department and person to be bound with the group.
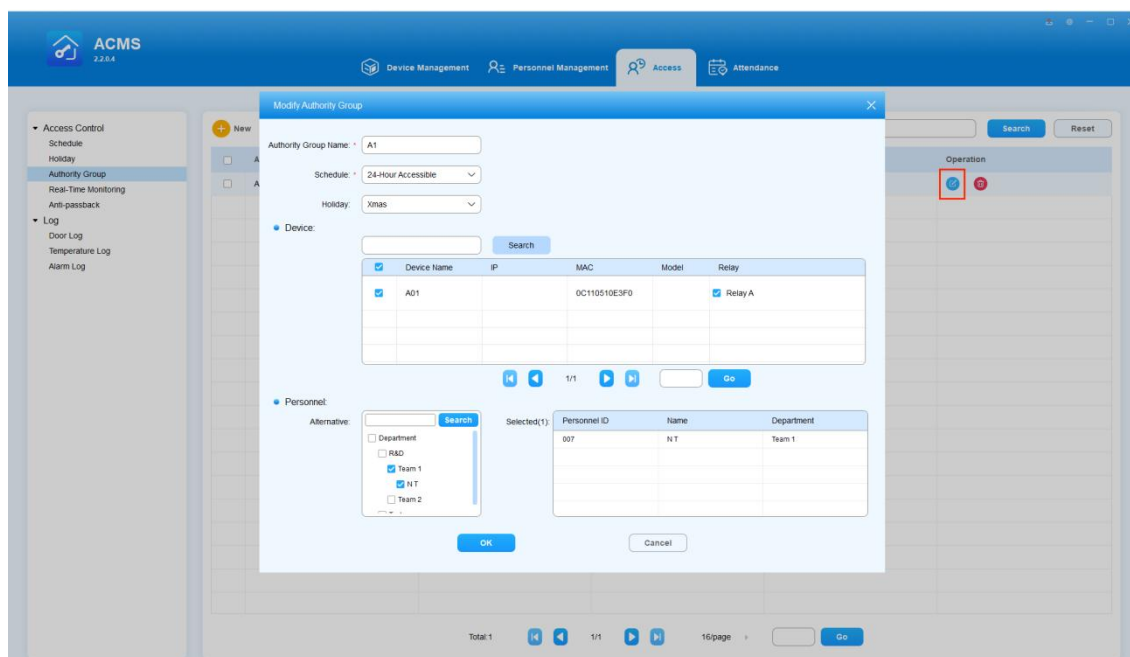
7. Click **OK**.
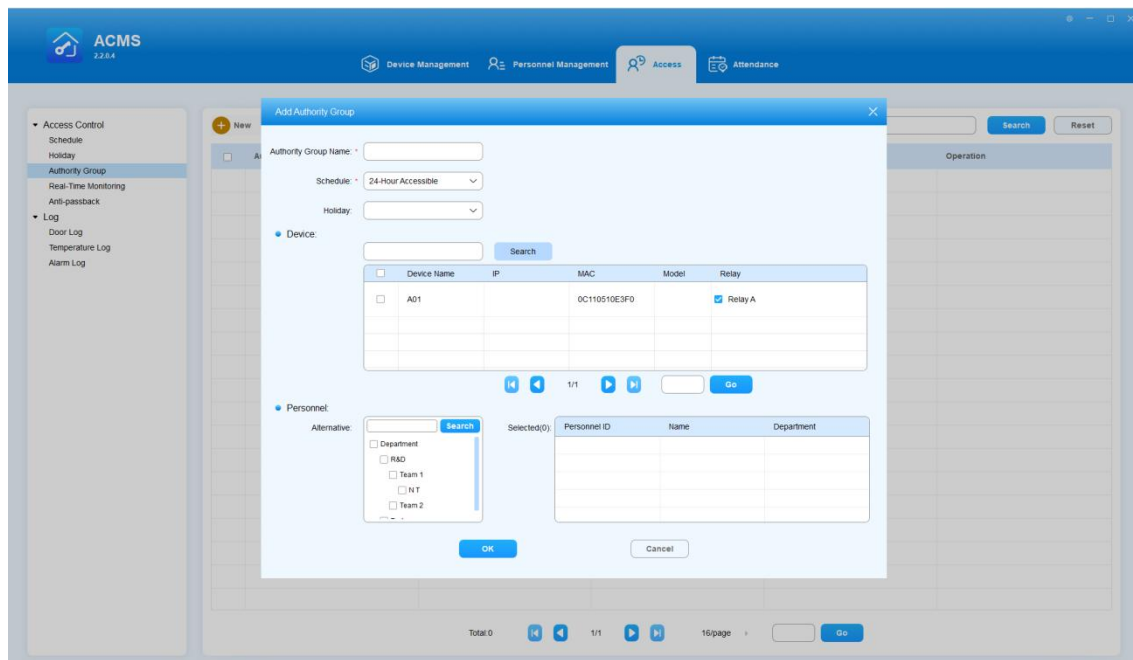
Note:

- Once an authority group is added, you need to go to the Device Management module to sync it to relevant device(s). For detailed instructions, see <u>here</u>.

5.2.1.2. Edit Authority Group

You can edit the authority group in terms of the authority group name, schedule type, device, and personnel.

1. Click or double click on the specific line of authority group you want to edit.
2. Edit the settings in the authority group according to your need.
3. Click **OK** for confirmation.

Note:

- Once an authority group is edited, you need to go to the Device Management module to update the changes to relevant device(s). For detailed instructions, see here.

5.2.1.3. Delete Authority Group

You can delete the authority group separately or in batches.
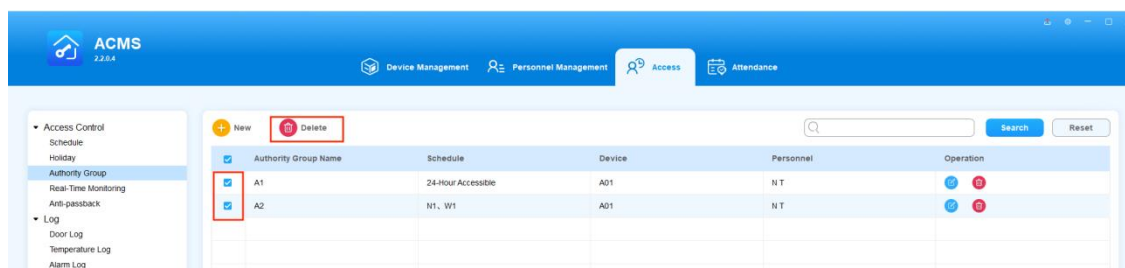
- **Delete authority group separately**

1. Click on 🗑 of the specific line of the authority group you want to delete.
2. Click **Yes** for confirmation.
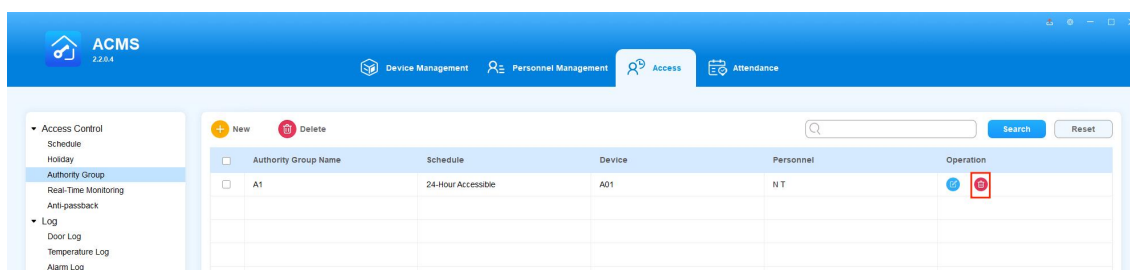
- **Delete authority group in batch**

1. Check off the specific line of the authority group(s) you want to delete.

2. Click 🗑 Delete and click **Yes** for confirmation.

5.2.1.4. Search Authority Group

You can search the specific authority group by entering the authority group name in the search field.

1. Enter the authority group name in the **Search** field.

2. Double click the authority group if you want to see the details.
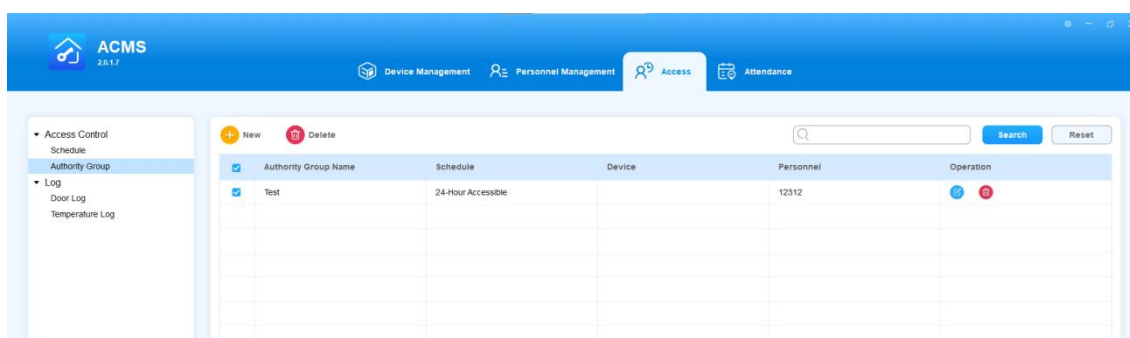
5.2.2. Unlock Doors by One-Click

The Real-Time Monitoring function allows you to take immediate action in emergency situations by either unlocking or locking all doors with a single click.

On the Real-Time Monitoring screen, you can:

- Open or close all doors with a single click in case of an emergency.
- Open or close individual or multiple devices.
- Check the status of devices' door magnets in real-time.
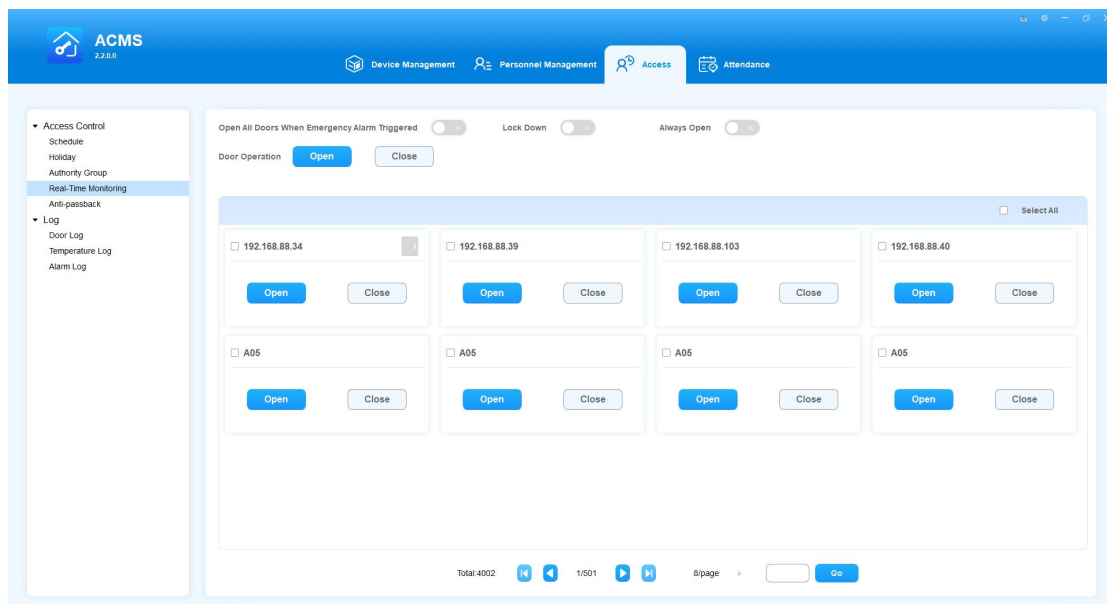
5.2.2.1. Auto-Open Doors When an Emergency Alarm Triggers

When this feature is turned on, an Open All Doors command will be automatically sent to all devices from the ACMS when an emergency alarm is received. By default, this feature is turned off.

To enable this feature, move the toggle marked in the below picture to be ON.
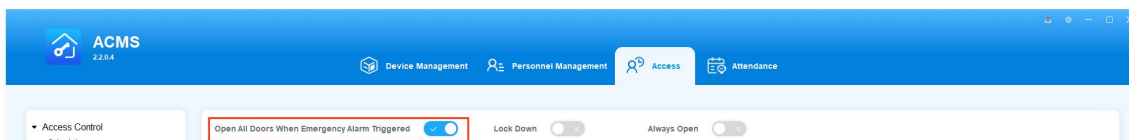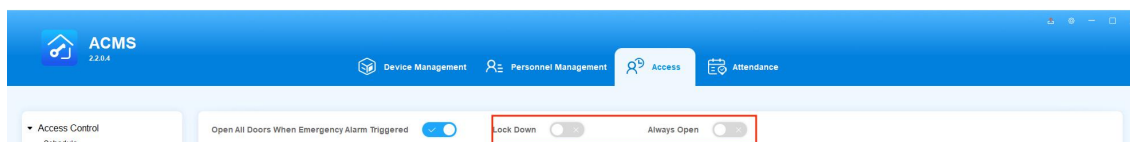

NOTE:

● When an Open All Doors command is received, only relays and security relays that have been set to be Open on ACMS will be triggered. Devices that are not set to Open will not be affected.

● The Open All Doors command will keep the relays open indefinitely until they are manually closed.

5.2.2.2. Lock or Open Doors by One-Click

The **Lock Down** feature allows you to quickly and easily lock online relays and security relays of the devices added on ACMS with a single click.

When the **Always Open** feature is enabled, the relays and security relays will keep open until they are manually closed.

NOTE:

Only those relays and security relays that have been set to Open on ACMS can be controlled by Lock Down and Always Open.

The system will returns the results after you perform Lock Down or Always Open.
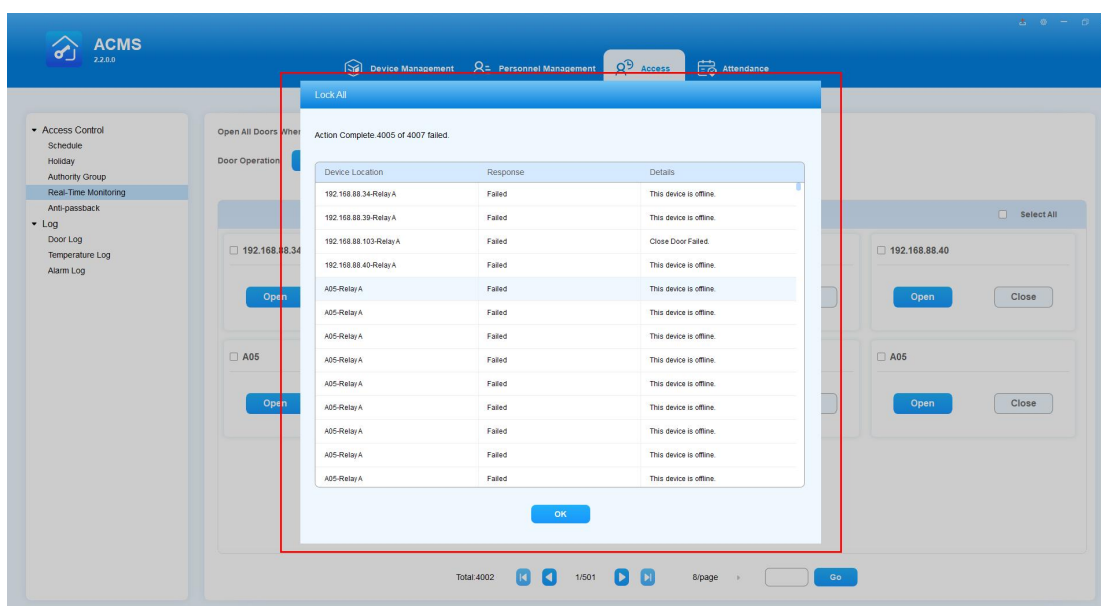
5.2.2.3. Open or Close Specific Doors

You can also open or close doors on individual or multiple specific online devices. On this screen, you can see all devices added to the ACMS and can then click the Open or Close button to operate.

NOTE:

When the Lock Down or Always Open feature is enabled, the Open or Close function on a single device or multiple devices CANNOT work.

● **Open/close relays on one device**

1. Select the desired device, and click Open or Close button.

2. Select the relays if the device has several relays that have been set to Open when adding it.

3. Click **OK** to allow for one-time door opening or closing.
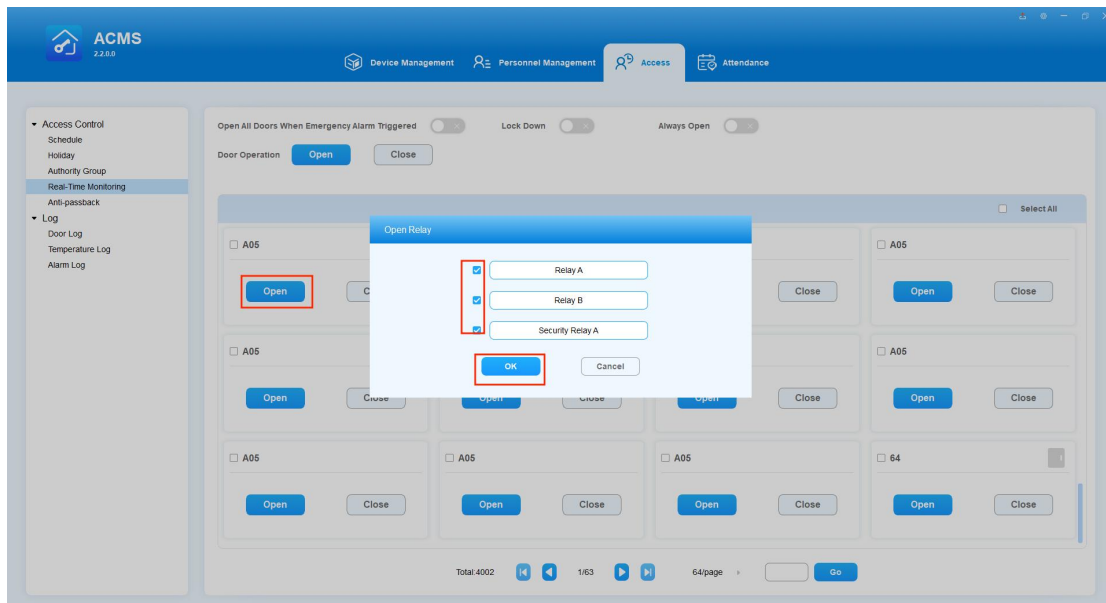
● **Open/close relays on multiple devices**

1. Check off the desired devices.

2. Click on Open or Close button on the top. All relays and security relays that have been set to Open will be triggered.
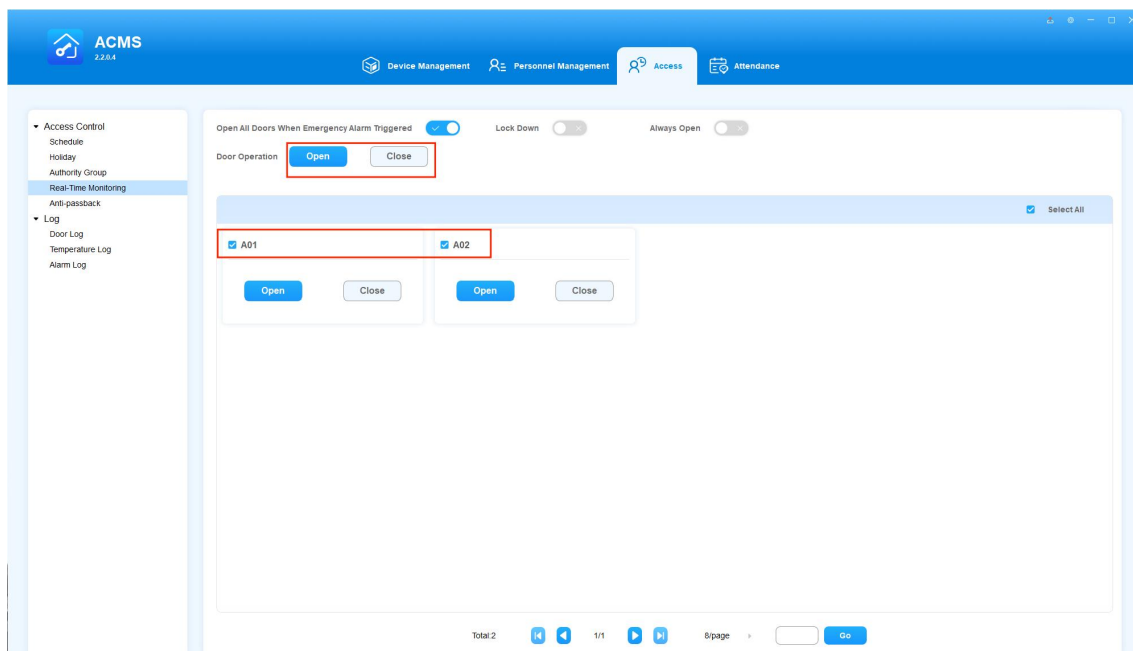

If at least one relay or security relay of a device is successfully opened or closed, the system will display a success message. While if all relays of a device fail to open or close, the system will display a failure message.
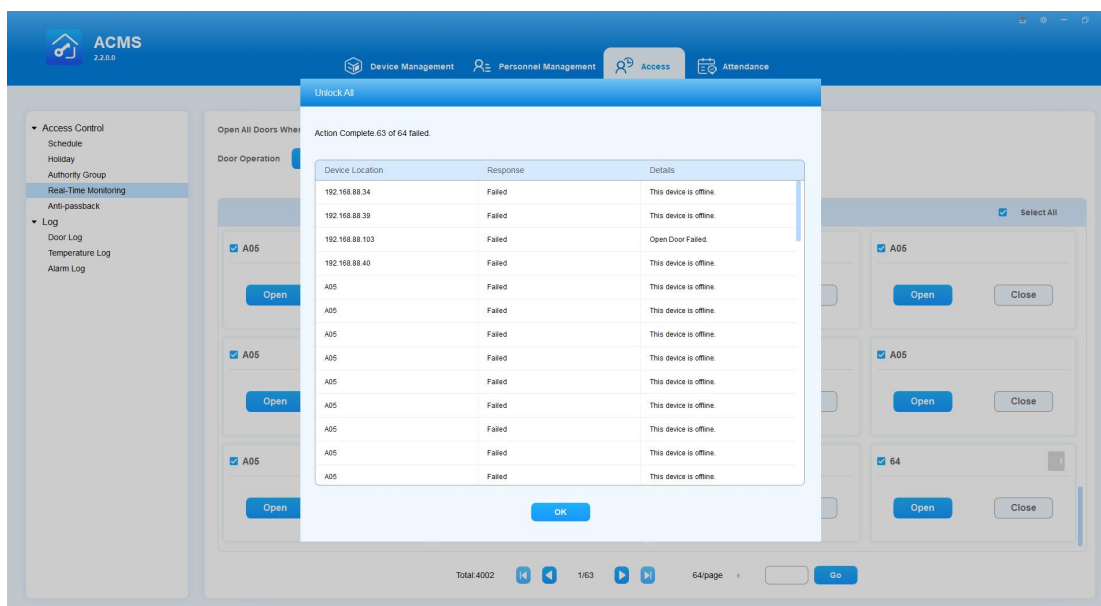
5.2.3. Check Door Magnets Status

Door magnet status is display next to the device name. The gray icon indicates that it is closed, and the blue icon is for open status.
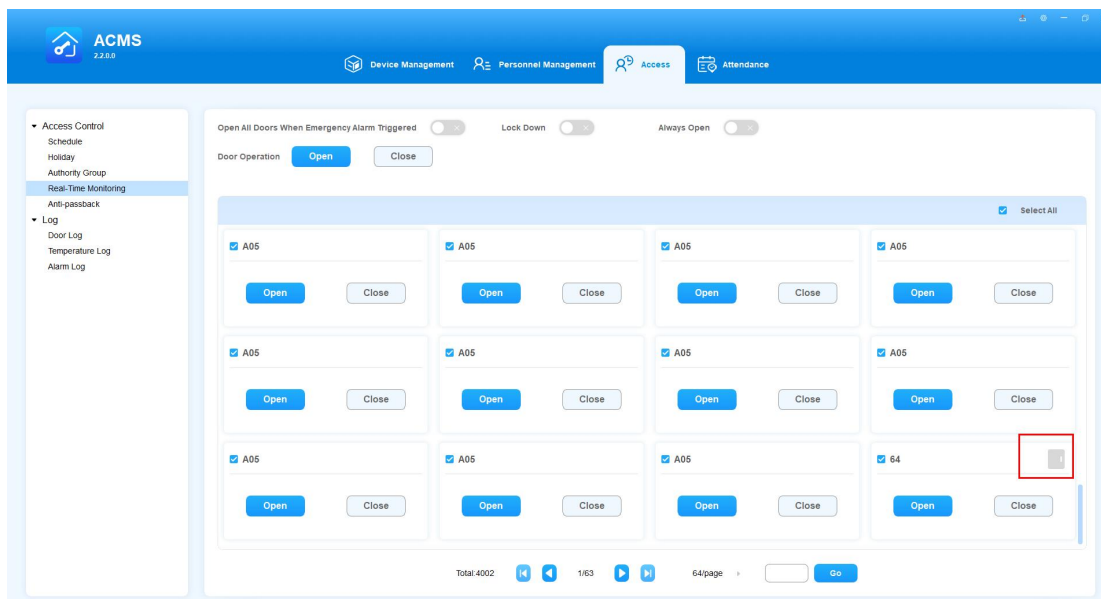
5.2.4. Anti-Passback

Anti-passback is a security mechanism preventing an access card or similar device from being used to enter an area a second time without first leaving it. In this case, each entry must be followed by the exit for the next successful entry.

5.2.4.1. Add Anti-Passback Devices

ACMS needs to add devices and set up its anti-passback methods for both the device and Wiegand. To enable this function, do as the following：

1. On the Anti-Passback screen, click ⊕ New .

2. Check off at least one device to proceed.

3. Select the Internal and Wiegand Anti-passback methods among None, Entry, and Exit.

4. Add additional Wiegand if needed.

5. Click **OK**.

NOTE:

Once Anti-passback devices are added, you have to update the settings to devices on the Device Management module. See <u>here</u> for detailed instructions.
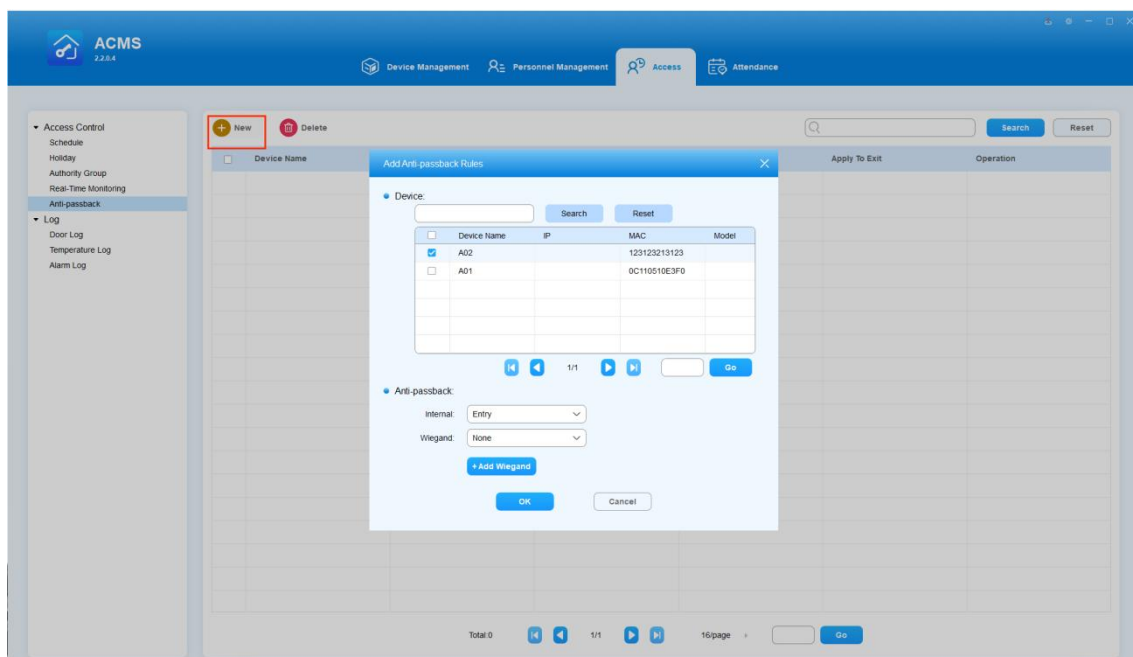
5.2.4.2. Edit Anti-Passback Devices

When editing, you cannot change the device that is set as an anti-passback device.

1. Double-click the desired device or click on its 🖉 in the Operation column.

2. Change its anti-passback methods or add new Wiegand.

NOTE:

Any changes made to anti-passback devices must be updated to the associated devices. See <u>here</u> to know how to update the changes.
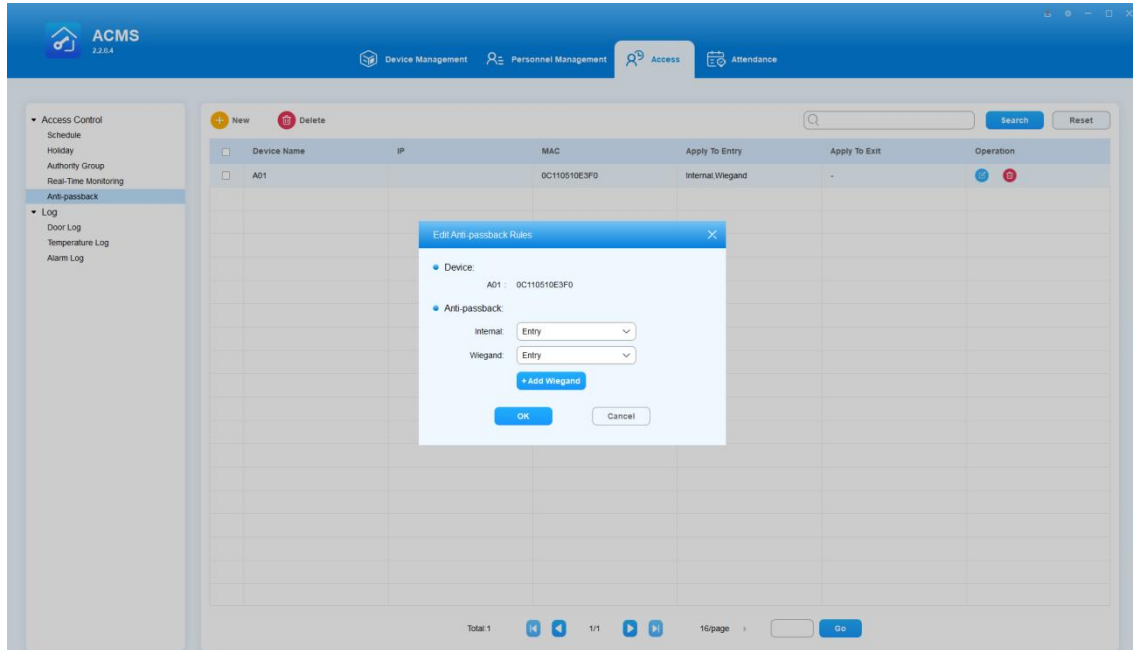
5.2.4.3. Delete Anti-Passback Devices

To delete single device, click on in the Operation column.

To delete multiple devices, check off the desired devices and click on the upper delete button .
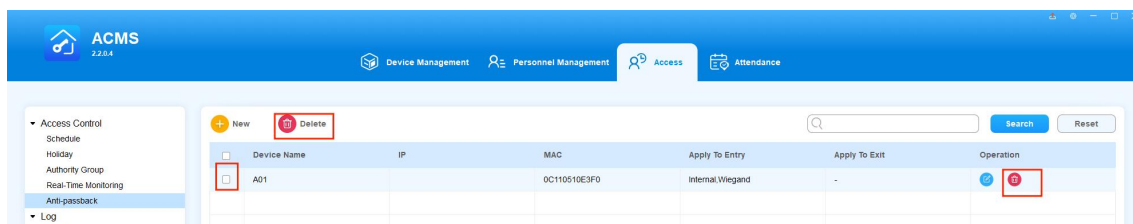
NOTE:

Deleting device will not change the Anti-passback mode that has already been sent to the device. In the Mode column on Door log screen, the mode will still be Entry or Exit even after the anti-passback device is deleted.

5.3. Logs

In the sub-module Log you can check the door access records, temperature records, and alarm records.

5.3.1. Daily Door Logs

On the door log screen and select **Daily Log** on the upper left, you can check and search door access records in terms of what access types are used, and who in which department have been granted or denied the door access during a certain time range.
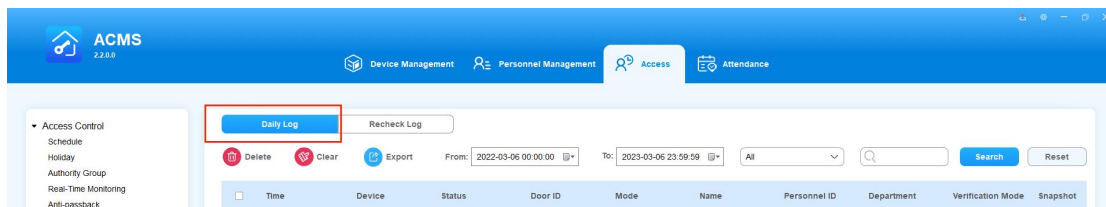
5.3.1.1. See and Search Door Log

● **See Door Logs**

1. Select the time range for the door log.

2. Select filtering range among **All**, **Open Door Succeed**, and **Open Door Failed**.

3. Click **Snapshot** to see photo captured by the device.
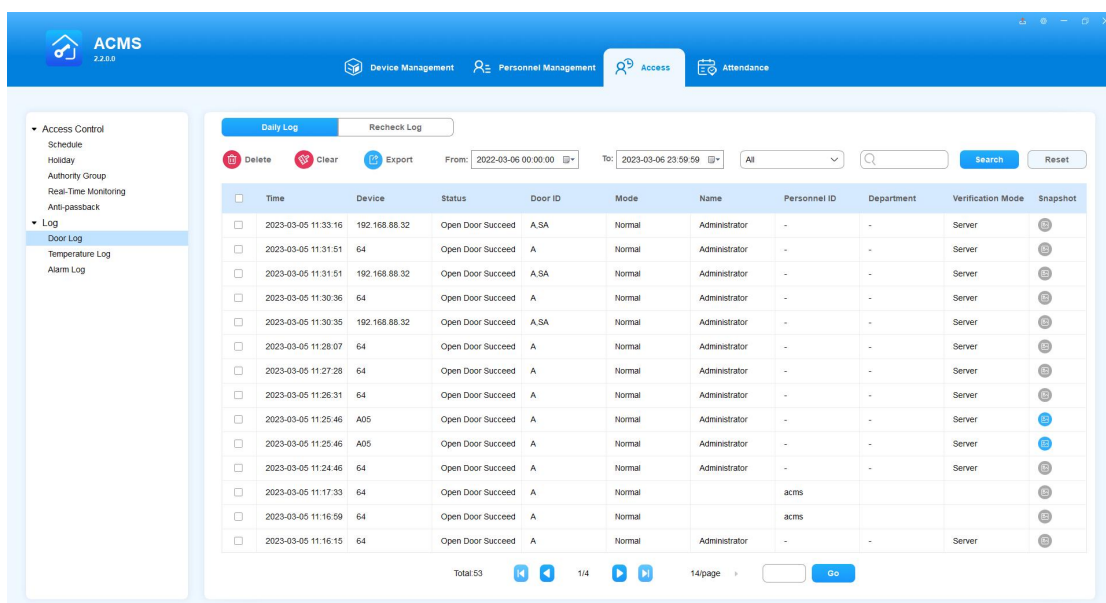
● **Search Door Logs**

1. Enter information, such as Device, Name, Personnel ID, and Department, in the Search field.

2. Click **Search** to find the specific log.
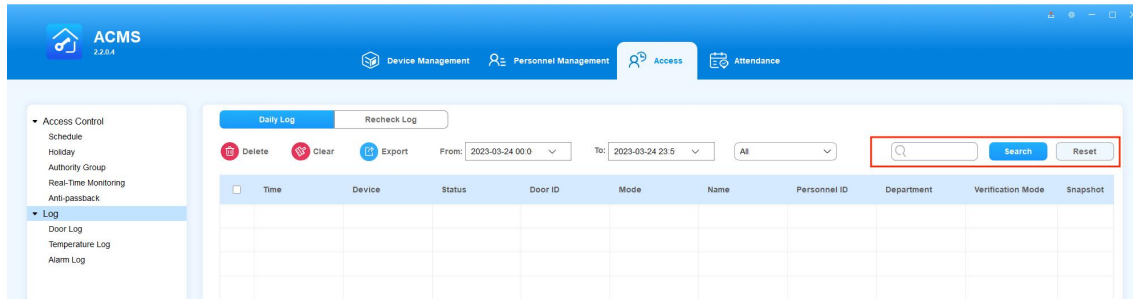
Note:

● The personnel ID field will be displayed as Unknown and the Name field and Department field will be left blank for the unregistered personnel seeking the door access.

5.3.1.2. Delete and Clear Door Log

● **Delete Door Log**

1. Tick the check box of the specific door log.

2. Click ![Delete] to delete the ticked door log.
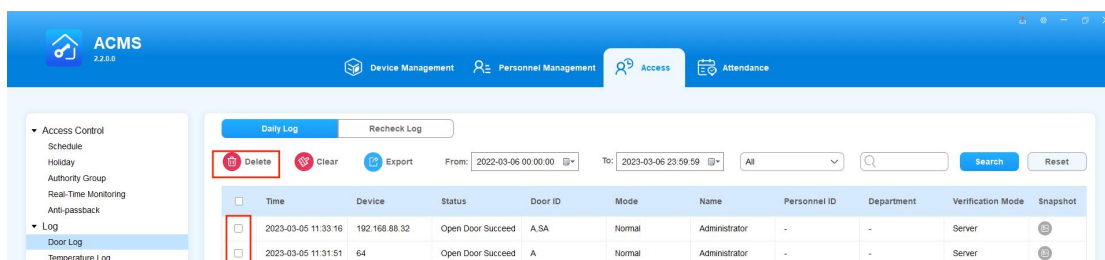
● **Clear Door Log**

1. Click ![Clear] to delete all the logs.

2. Click **Yes** for confirmation.
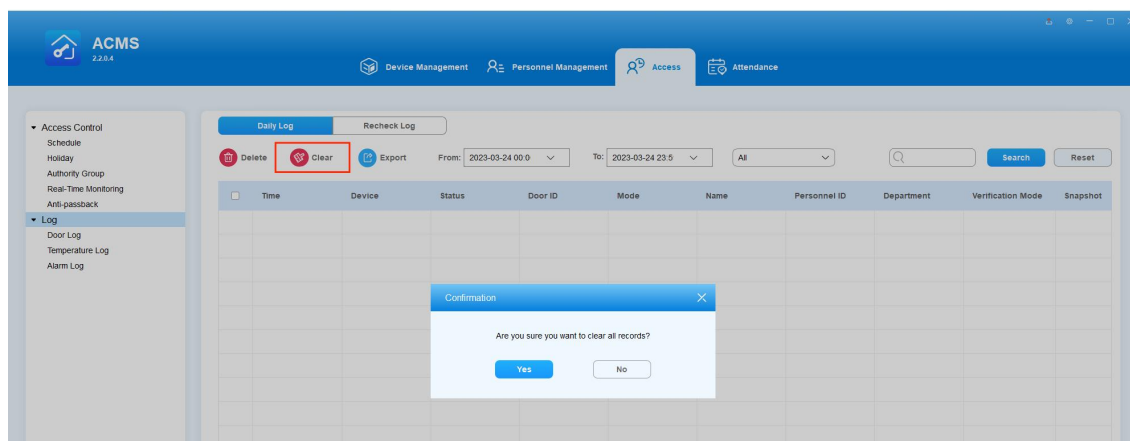
5.3.1.3. Export Door Log

The door log can be exported to a designated path on your computer in .xlsx format.

1. Click [Export] and select the path to which you want to export the file to your local PC.

2. Click **Save**.
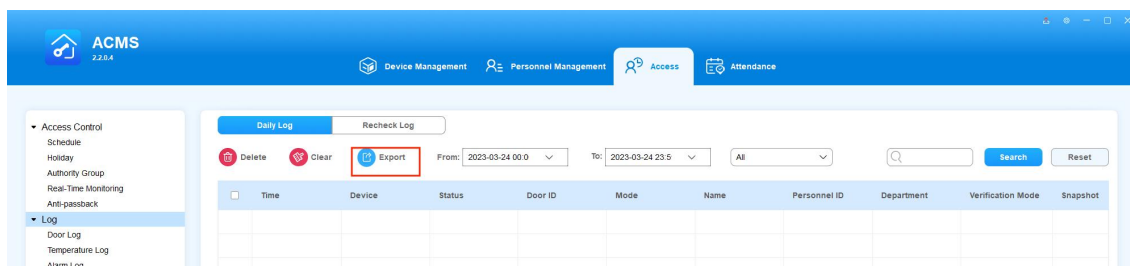
5.3.2. Recheck Log

Recheck Log is a feature that can work in conjunction with the Anti-passback function. It facilitates the situation where a person is unable to enter or exit due to reasons such as being lost or forgetting to swipe a card. You can use this feature to perform recheck operations for the user, thereby relieving the abnormal situation and ensuring that the user can enter or exit normally the next time.

5.3.2.1. Perform the Recheck Operation

To recheck for an user, do as the following.

1. On the Access screen, select Door log on the left-side menu, and click on Recheck button to start rechecking.

2. Select the entry or exit option based on the actual situation of the user.

3. Select the user from the list of ACMS or enter the user's name and ID directly.

4. Choose the time and date.

5. Click **OK**.
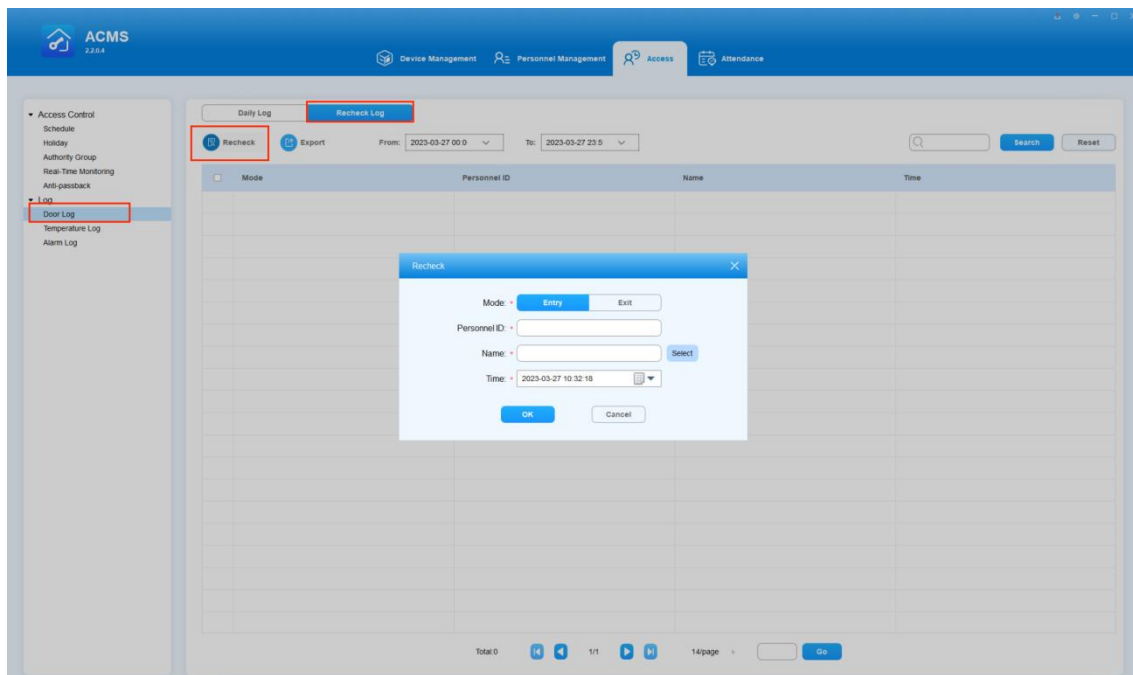
Once the recheck operation is complete, a new door log will be generated. The name of the record will display as Administrator and the verification mode will be Server.
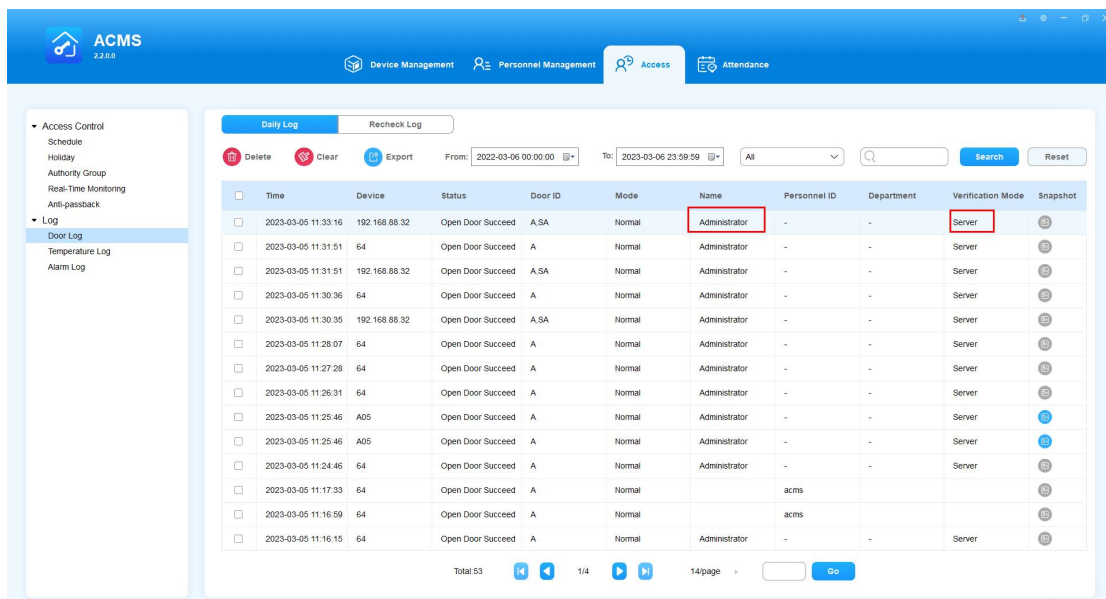
5.3.2.2. Search and Export Recheck Logs

You can filter the logs by specifying time, Personnel ID and name. You are also allowed to export the filtered logs with one click.
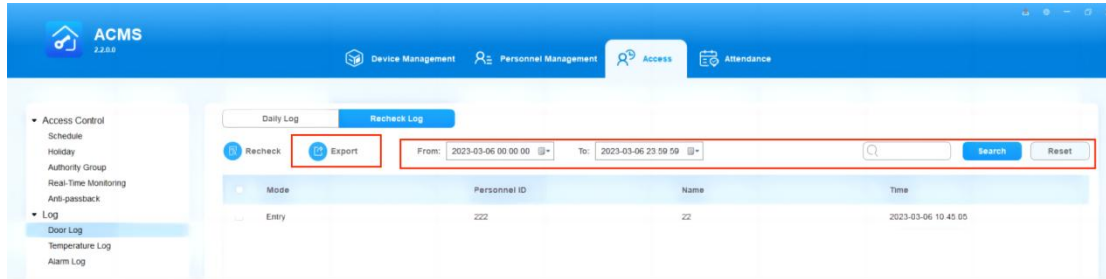
5.3.3. Temperature Log

In the temperature sub-module, you can check and search temperature records collected in the device that is equipped with Akuvox digital temperature detector during a certain time range.

5.3.3.1. See/Search Temperature Log

● **See Temperature Log**

1. Select the time range for the temperature log.

2. Switch the temperature scale (**Celsius** or **Fahrenheit**) if needed.

3. Select filtering range among **All**, **Normal Temperature**, **Abnormal Temperatur**, and **Low Temperature.**

● **Search Temperature Log**

1. Enter the device name in the **Search** field.

2. Click **Search** to find the specific temperature record.
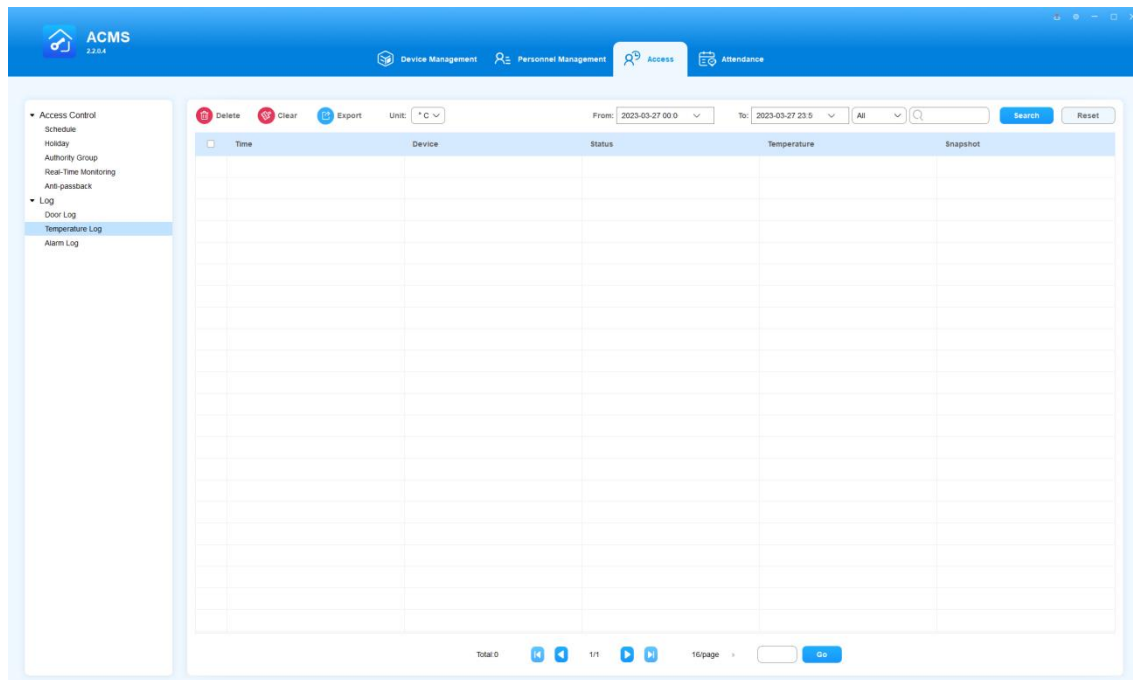
5.3.3.2. Delete/Clear Temperature Log

● **Delete Temperature Log**

1. Tick the checkbox of the specific temperature log.

2. Click 🗑 Delete to delete the ticked temperature log.

● **Clear Temperature Log**

1. Click 🧹 Clear to delete all the temperature logs.

2. Click **Yes** for confirmation.
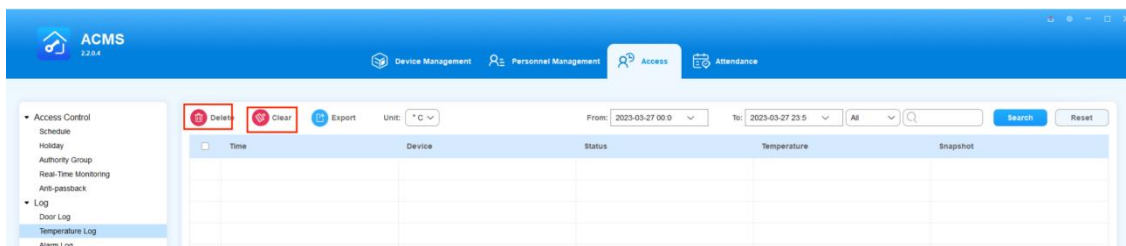
● **Export Temperature Log**

Temperature log can be exported in .xlsx format. to the designated path on your computer.

1. Click 📤 Export and select the path to which you want to export the file in your local PC.

2. Click **Save.**

5.3.4. Alarm Log

The Alarm Log screen displays all alarm histories reported by devices such as tamper alarm, alarm door opened, break-in intrusion, and emergency alarm. All logs can be deleted, cleared, and exported.
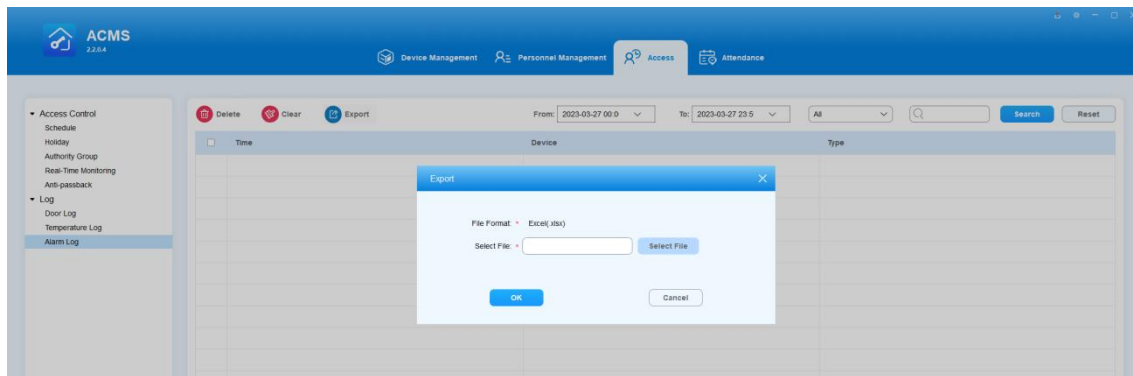
5.3.4.1. Search Alarm Logs

You can filter the logs by specifying date and time, entering the device, and selecting the log type.
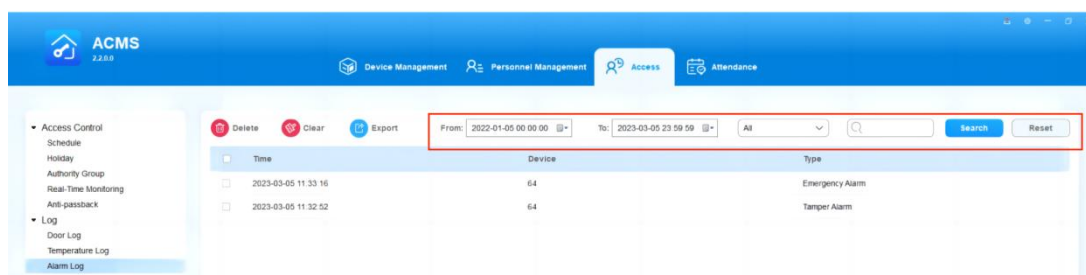
5.3.4.2. Export Alarm Logs

Alarm logs can be exported in .xlsx format. to your computer.

1. Click and select the path to which you want to save the file in your local PC.
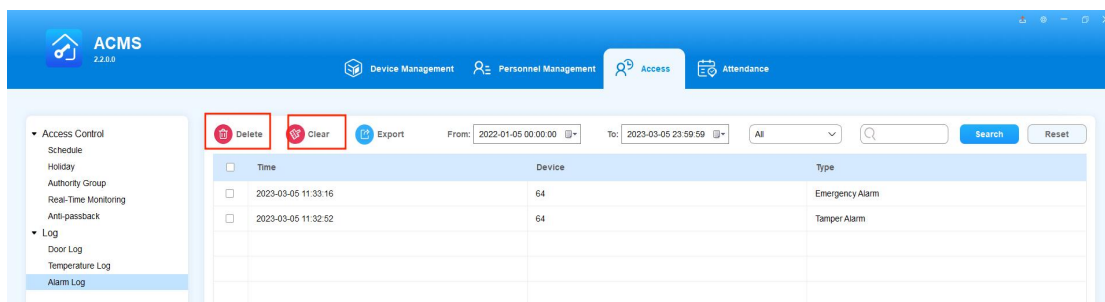
2. Click **Save.**

5.3.4.3. Delete/Clear Alarm Logs

You are able to delete certain logs or clear all logs.

● **Delete Certain Logs**

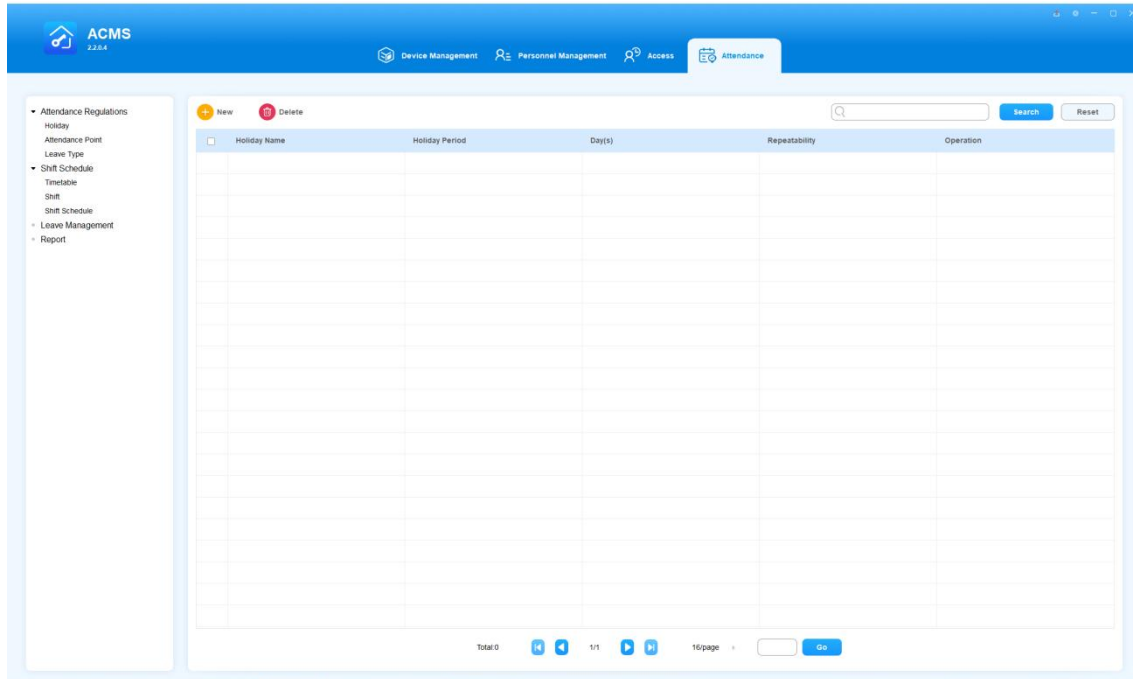1. Check off the specific logs.

2. Click to delete the selected.

● **Clear All Logs**

1. Click on the top.

2. Click **Yes** for confirmation.

6. Attendance Management

The attendance module allows you to set up holidays, attendance device locations, and work timetables, and manage employee shifts, leave, and attendance.
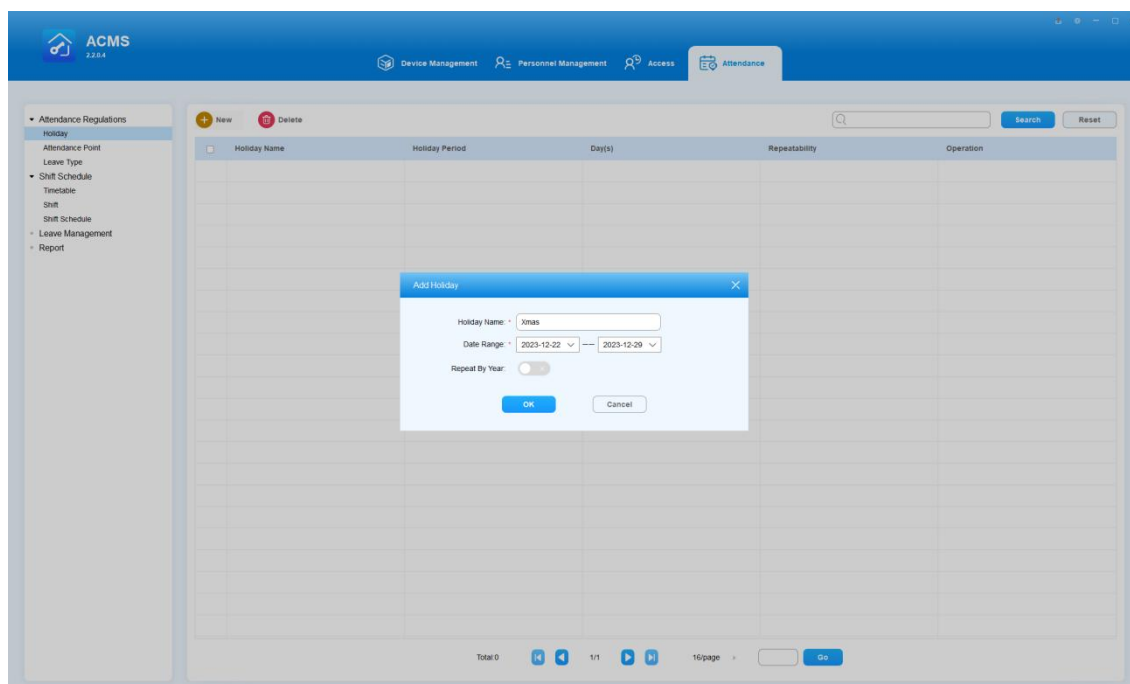

6.1. Holidays

You can set up holidays that can be automatically integrated into your work schedule and attendance.

6.1.1. Add a Holiday

1. Enter the holiday name.
2. Set up the holiday time range.
3. Move the toggle switch to the right if you want the holiday to be repetitive every year.

6.1.2. Edit a Holiday

1. Double click the desired holiday or click on in its Operation column.
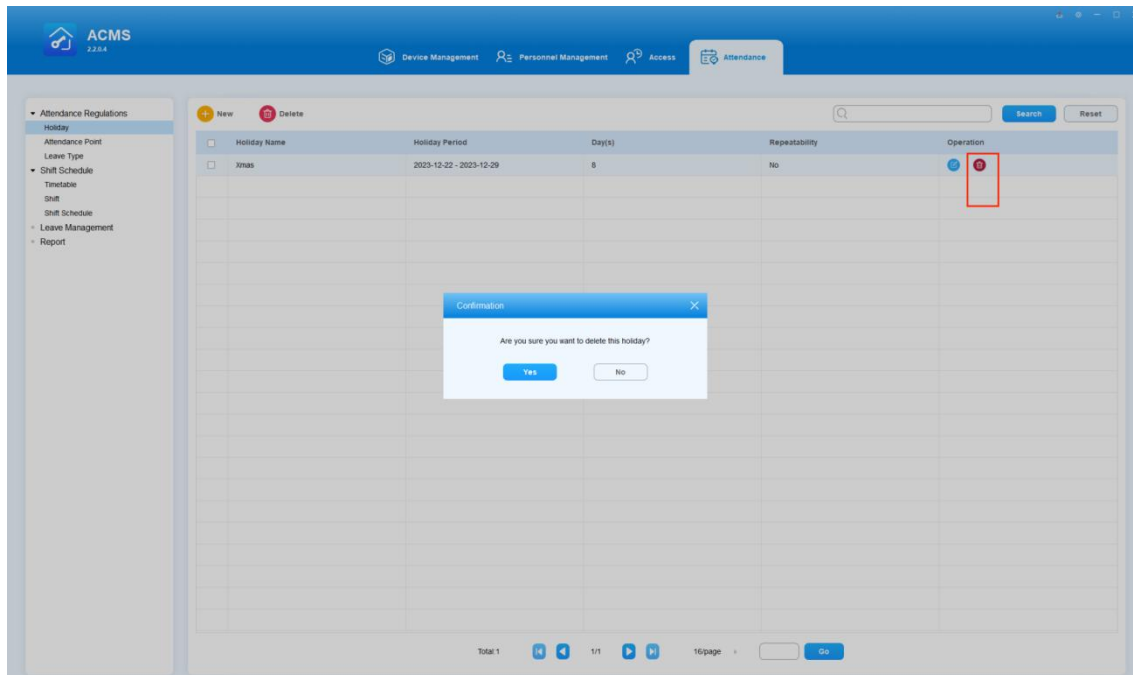2. Edit the holiday information according to your need.
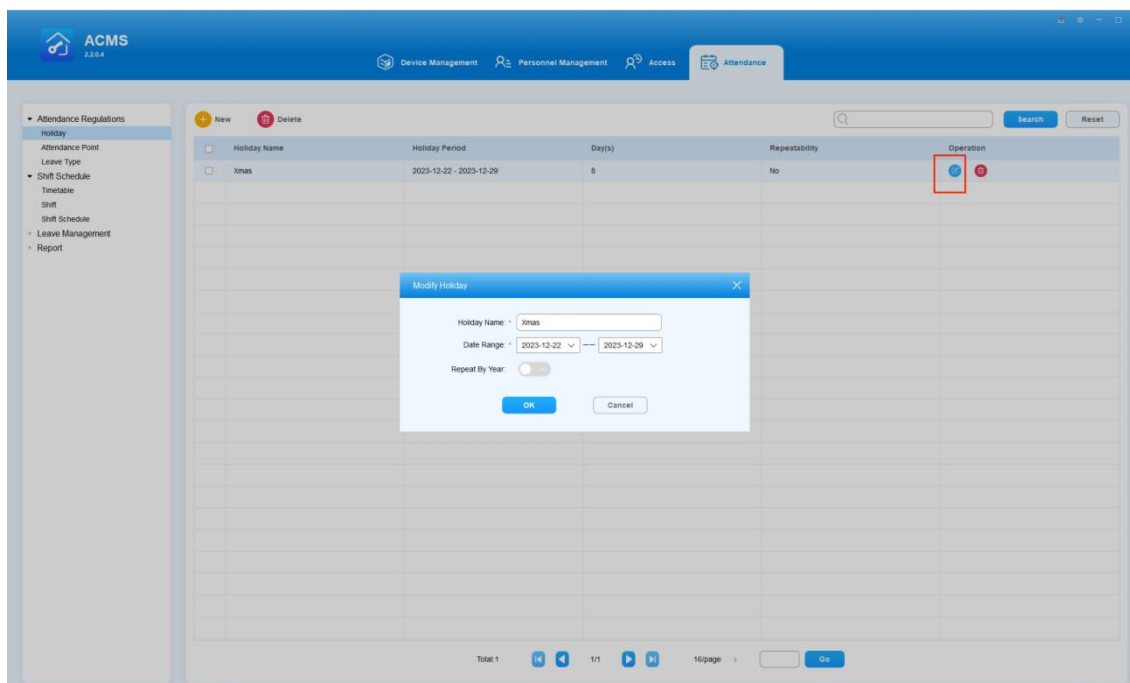
6.1.3. Delete Holiday

You can delete holiday(s) one by one or in batch.

● **Delete Holiday(s) One by One**

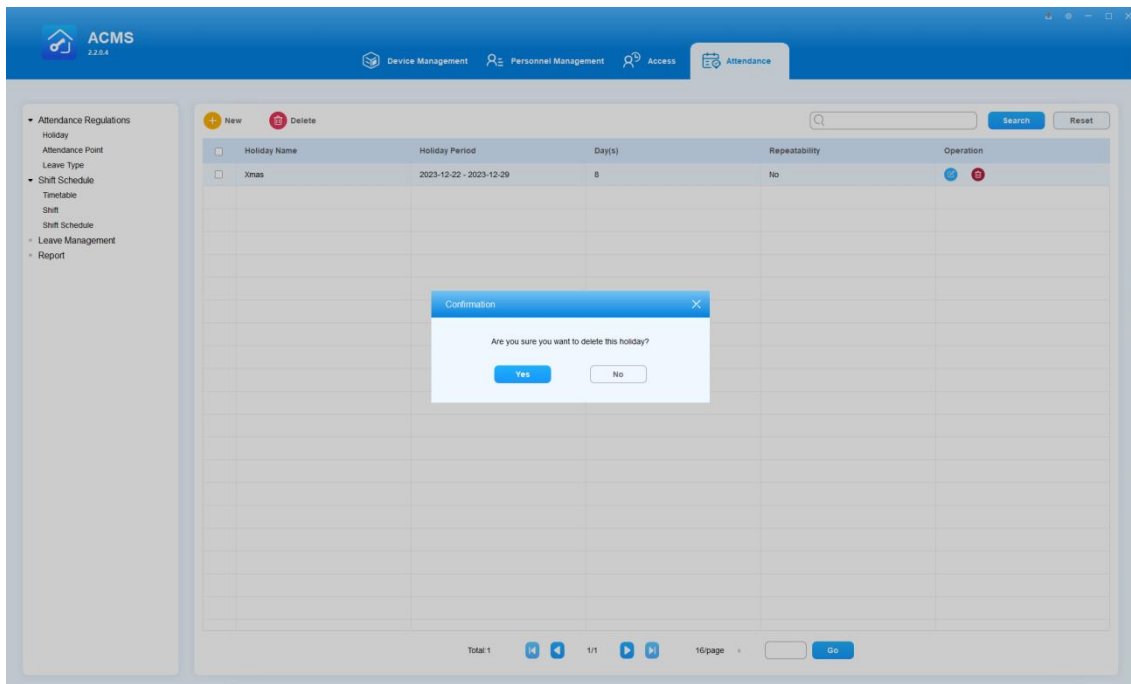1. Click on 🗑 of the specific holiday you want to delete.
2. Click **Yes**.

● **Delete holiday(s) in Batch**

1. Check off the desired holidays, or the box next to Holiday Name ☑ Holiday Name to select all.
2. Click **Yes**.

6.2. Attendance Point

There can be more than one device for personnel's punch-in and punch-out, therefore you might need to name the devices based on their locations (location point) so that attendance records of the specific attendance device(s) can be obtained.

6.2.1. Create Attendance Point

1. Click on ⊕ New .
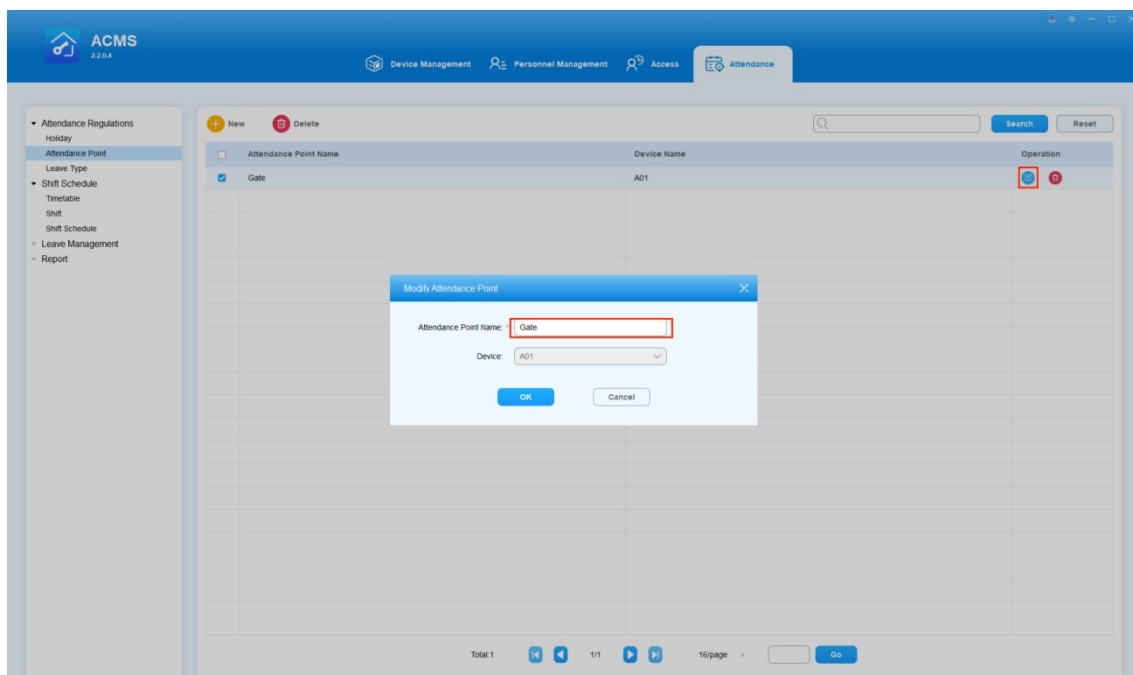2. Fill in the attendance location name and select a device for it.
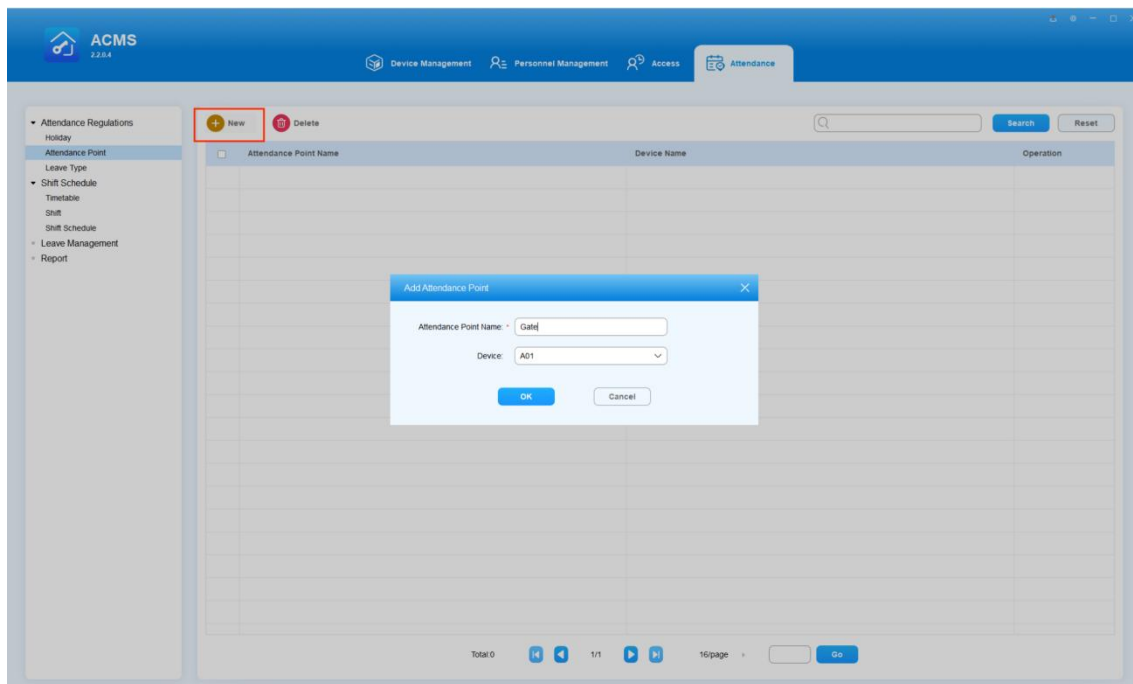
6.2.2. Modify Attendance Point

You can modify the point's name, while the device selected cannot be changed.

1. Double click the desired point or click on in its Operation column.

2. Change the point's name.
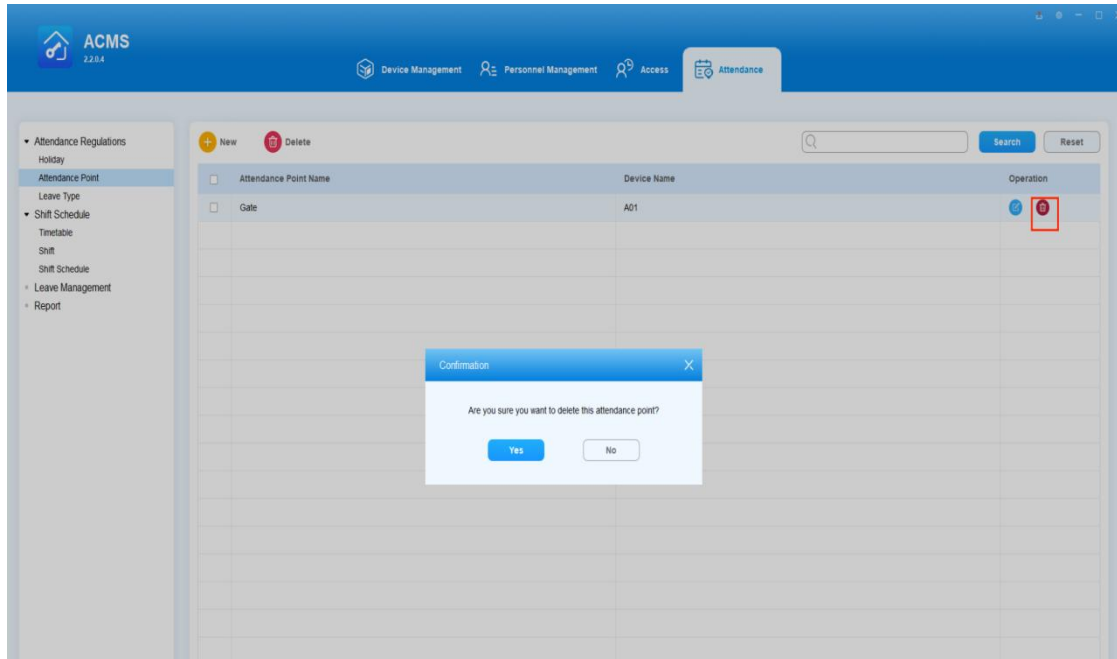
3. Click **OK**.

6.2.3. Delete Attendance Point

You can delete the attendance device point separately or in batch.

● **Delete attendance device point separately**

1. Click on 🗑 in the desired point's Operation column.
2. Click **YES**.

● **Delete attendance device point in a batch**

1. Tick the checkbox ☑ **Attendance Point Name** of the attendance points you want to delete.
2. Tick the checkbox if you want to delete all the existing attendance points.
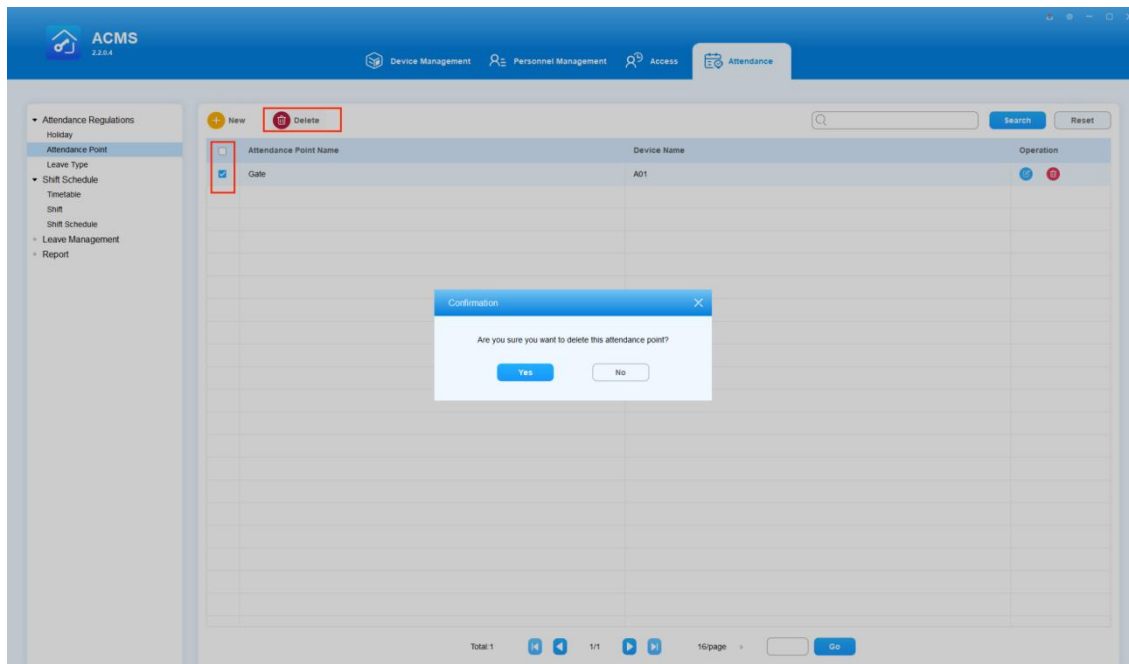
6.3. Shift Schedule

The **Shift Schedule** sub-module allows you to plan for the work shift timetables, shift management, shift adjustment, and manage the attendance record and leave the report for the employees.

6.3.1. Timetables

6.3.1.1. Create Timetable

You can create an inventory of shift timetable templates that can be later conveniently pulled out and applied to the specific work shift(s) for the specific employee(s). You can define time table setting in terms of setting up timetable names, types, as well as work hours and attendance time to be applied to the timetable.

1. Go to **Attendance** module and navigate to **Shift Schedule > Shift.**

2. Click ➕ New to add a timetable.

3. Set up timetable names and types, and attendance time in the timetable.

Parameters Setup

No.	Field Name	Description
1	Period Name	Enter the name of the work timetable, which is required. Period name is mainly used for identification and search purpose.
2	Template Type	Select the timetable type between **Flexible** and **Fixed**. The type is **Fixed** by default. ● If **Fixed** is selected, then you are required to specify the work start-time, end-time, valid punch-in and punch-out time for the employees. ● If **Flexible** is selected, then you need to fill in the total work hour required of employees per day, and the work start time, ignoring the work end time and valid punch-in and punch-out time as long as the employee work hour meets the total work hour you defined.

| 3	Start Work Time	Set up work start-time. The default start time is **09:00**.
4	End work Time	Set up work end-time. The default end time is **18:00**.
5	Valid Check Time	Set up a valid punch-in time range for **Fixed** timetable. The default valid punch-in time range is from **08:30-18:30.** If an employee clocked multiple times, the earliest recorded time will be considered the clock-in time and the latest will be considered the clock-out time.
6	Auto Deduct Break Time	Enables automatic deduction of break time. When this option is turned on, the system will deduct the specified break time from the total work time when calculating work hours.
7	Break Time	The period of time designated as break time.
8	Allow Late (Minutes)	The amount of time allowed for being late, ranging from 0 to 1440 minutes. When set to 0, no late arrival is allowed. When set to a value other than 0, the specified number of minutes is allowed for being late, but the attendance record will not be marked as late. For example, if the work start time is set at 9:00 and Allow Late is set to 5, any record before 9:05 will be considered normal and will not be marked as late.
9	Allow Early Leave (Minutes)	The amount of time allowed for early departure, ranging from 0 to 1440 minutes. Setting it to 0 means no early departure is allowed. If set to a non-zero value, the specified number of minutes is allowed for early departure, but the attendance record will not be marked as early departure. For instance, with work end time set to 18:00 and Allow Early Leave set to 5, any record after 17:55 is considered normal.
10	Working Hours Per Day	(**For Flexible type only**) Set up the total work hour required of employees per day. The total work hour shall not be more than **24** hours. The default work hour is **8** hours .
11	Start Time Of Timetable	(**For Flexible type only**) Set up the work start time for the flexible type timetable. For example, if you set the start-time as **09:00**, then the end time will automatically be **09:00** the next day (24 hours a cycle), requiring employees to punch in and punch out during the 24 hours (In this example, the valid punch-in time will start at 09:00, while the valid punch-out time will end at 08:59 the next day). The default start-time is **00:00**.

6.3.1.2. Edit Timetable Template

After timetables are created, you are allowed to edit the timetables if needed.

1. Click on of the specific timetable you want to edit.
2. Edit the timetable according to your need.

NOTE:

If a timetable has been assigned to a shift, any changes to it will be updated to the relevant shifts and shift schedules.
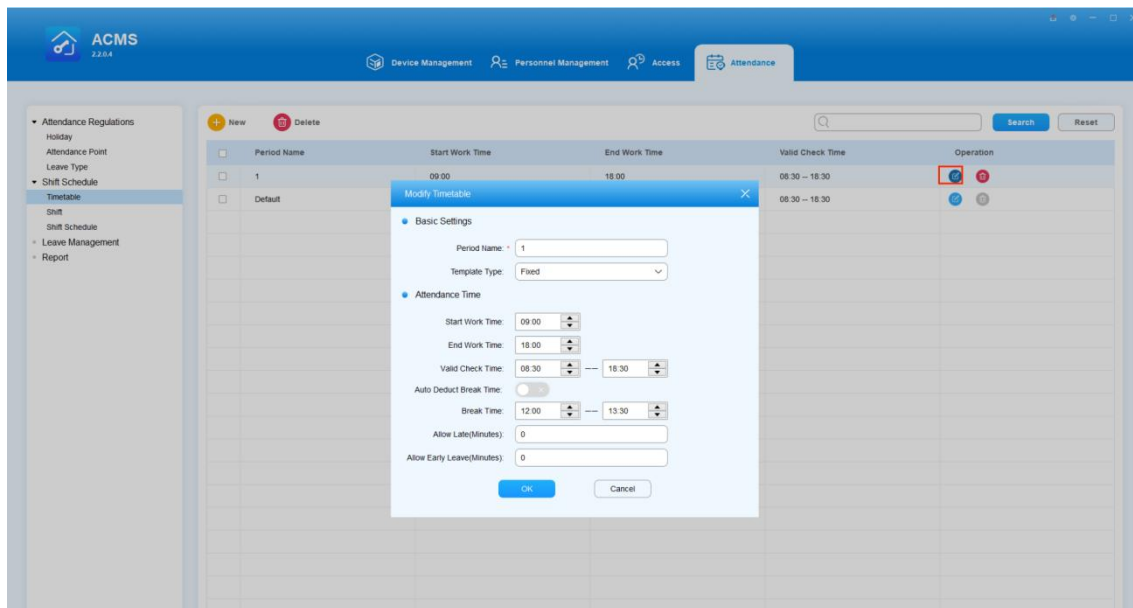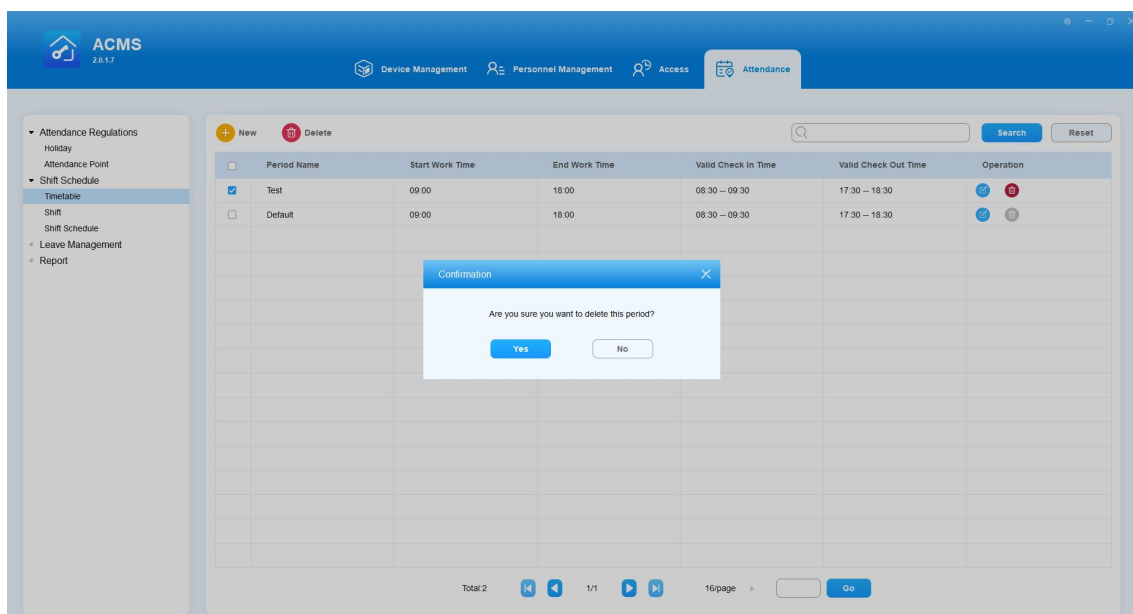
6.3.1.3. Delete Timetables

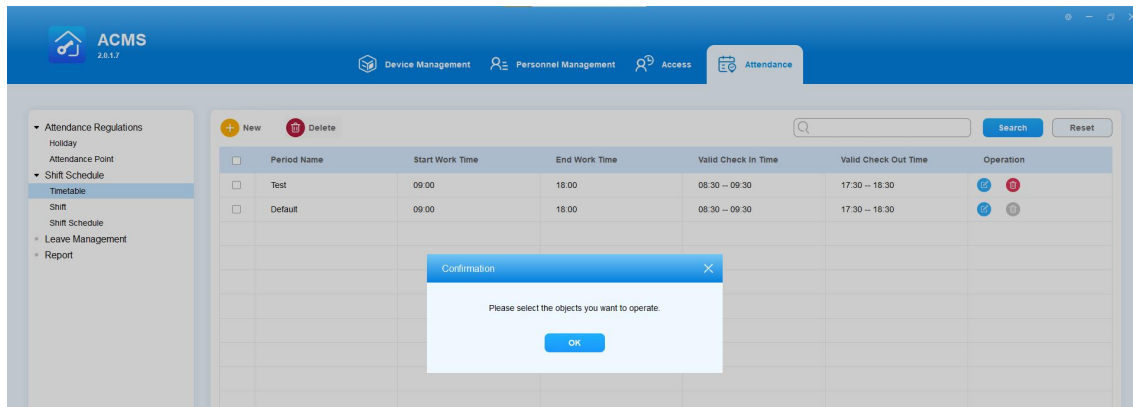You can delete the existing timetables separately or in batch if needed.

● **Delete timetable separately**

1. Tick the checkbox of the specific timetable you want to delete.
2. Click **Yes** for the confirmation.

● **Delete timetable in batch**

1. Tick the checkbox ☐ Period Name of the timetables you want to delete.

2. Tick the checkbox if you want to delete the existing timetables.

> **Note:**
>
> ● The default timetable CANNOT be deleted.
>
> ● Timetables that have been assigned to shifts CANNOT be deleted.

6.3.2. Shifts

You can create shift templates and assign them to employees.

6.3.2.1. Create a shift

To create a shift template, do as the following.

1. Click on ⊕ New to start creating shift schedules.

2. Select the created timetable template(s) for the shift schedule in the **Period** field.

3. Setting up the shift schedule to be carried out by day, week, or by month as well as the shift cycle times.

4. Click on and blue high-light days you want to implement the shift and click 🔧 Clear if you want to clear the day(s) high-lighted.

Parameters Setup

No.	Field Name	Description
1	Period	Select the timetable template to be applied to the shift to be created. You can select multiple timetable templates for the shift on a weekly and monthly basis if needed.
2	Shift Cycle	Select the shift to be carried out on a daily, weekly, or monthly basis and the shift cycle times. For example, if you set the shift by month and shift cycle as three times, then you will be getting a total of 9-month shifts with a three-month cycle, meaning the following two "three-month" shifts will be carried out in the same way as the first three-month shift.
3	Shift Name	Name the shift according to your need.

6.3.2.2. Search a Shift

You can search the needed shift when there are multiple shifts.

1. Enter the shift name in the search box.
2. Click on **Search**.
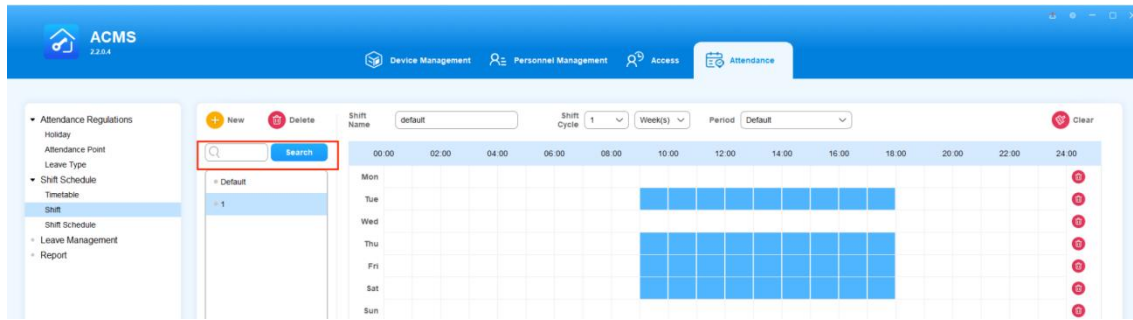
6.3.2.3. Edit a Shift

You can edit the shift templates in terms of changing the shift name, shift cycle, and shift timetable (**Period**).

1. Click on the shift template you want to edit in the shift column.

2. Change the shift name, shift cycle, and shift timetable (Period) according to your need.

3. Click on **Confirm**.
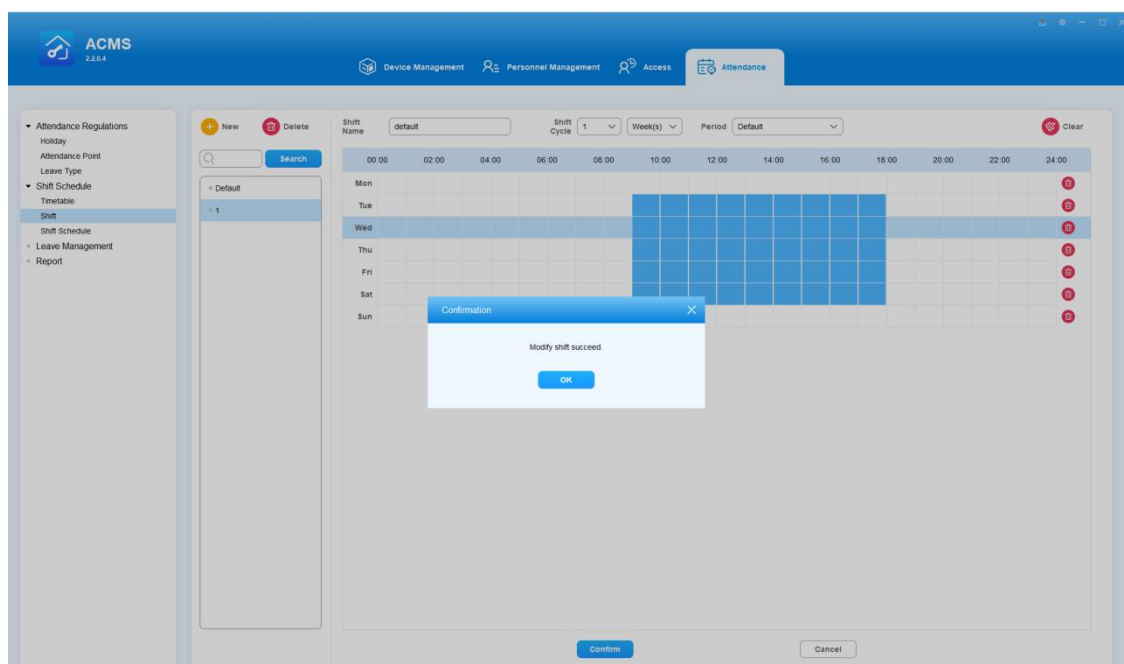
6.3.2.4. Delete a Shift

1. Click on the shift template you want to delete in the shift column on the left.

2. Click on to delete the shift.

3. Click on **Confirm**, and then **Yes**.
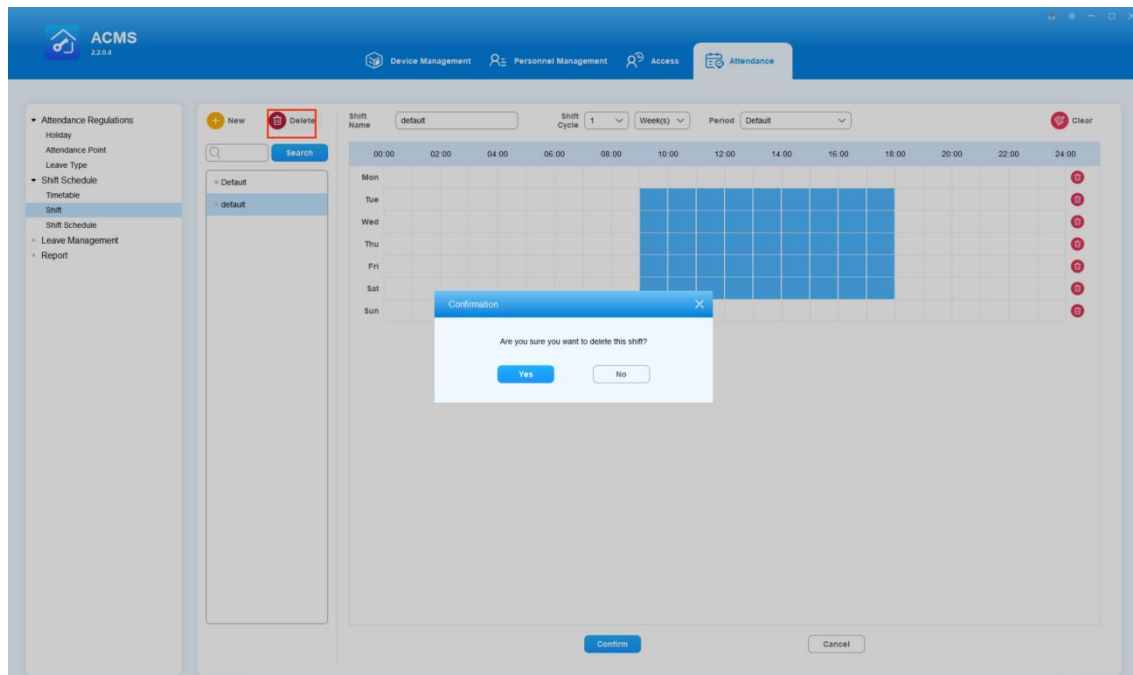
Note:

- A shift template cannot be deleted if the shift template is being applied to any employees.

6.3.3. Shift Management

After you created shift template(s) you can select the specific shift template from the shift inventory and applied it to the employees' regular shift and temporary shift schedule while defining how long a shift should last, and to which department(s) and employee(s) the shift is to be assigned. And you can search, check, and delete shift(s) afterward if needed.

6.3.3.1. Assign Regular Shift to Employees

You can assign a regular shift template to the specific department(s)and employee(s).

1. Click on .

2. Select the shift schedule template and the time range you want to apply.

3. Select the department(s) and employee(s) you want the shift to be applied to.
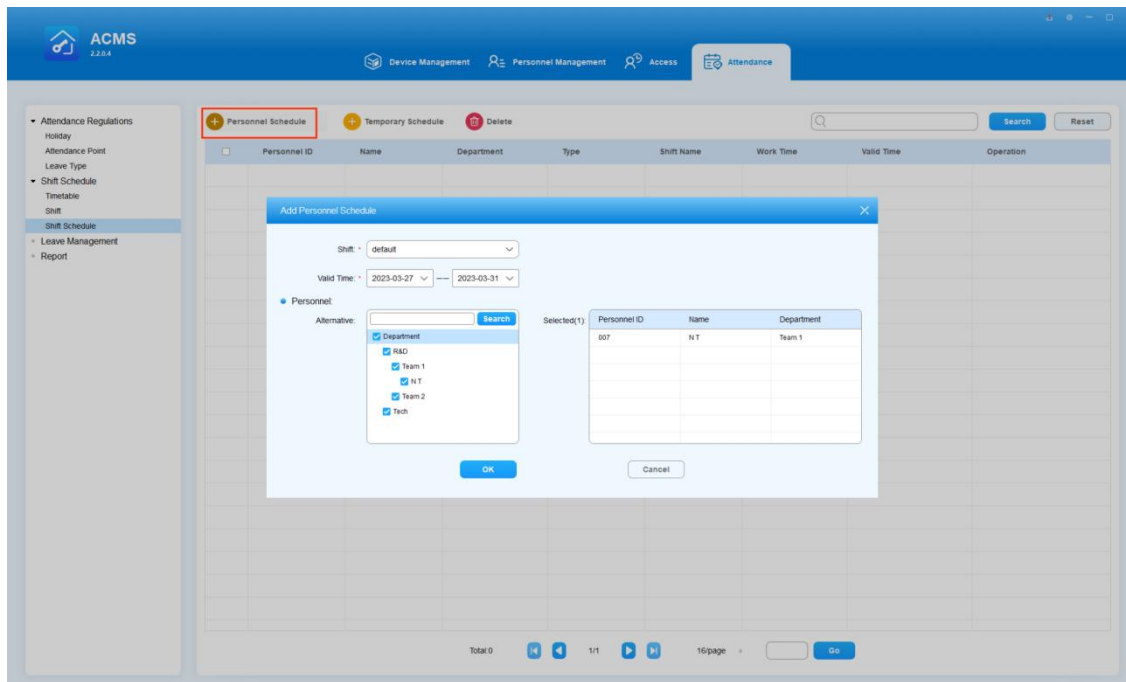
Note:

- An employee can only be assigned one regular shift schedule, therefore the previous one will be replaced automatically by the new one if you insist on the replacement.

Note:

- A shift cannot be deleted if the shift is being applied to a specific employee.

6.3.3.2. Assign Temporary Shift to Employees

You can assign a temporary shift schedule to the specific employees of the specific department when a temporary change or adjustment of shift for the employee is needed.

1. Click on ⊕ Temporary Schedule .

2. Select the shift and the time range you want the shift to be applied.

3. Select the department(s) and employee(s) you want the shift to be applied to.
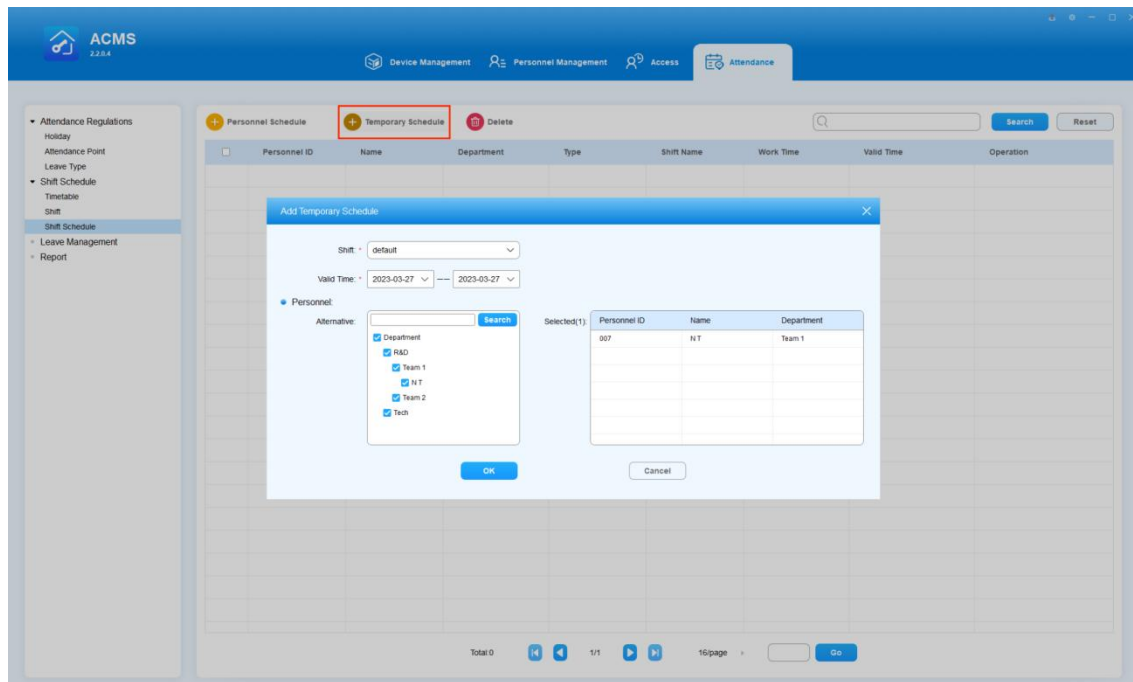
> **Note:**
>
> ● An employee can only be assigned with one temporary shift schedule, therefore the previous one will be replaced by the new one if you insist on the replacement.

6.3.3.3. Search/Check the Assigned shift

You can search the regular and temporary shifts that are assigned to the employees. You can also check the work calendar of the employee for the details.

1. Search the employees' shift by entering the employee's name and ID number in the search field. Click on **Reset** to quickly clear the search field if needed.

2. Click on of the specific employee if you want to check the employee's work calendar.
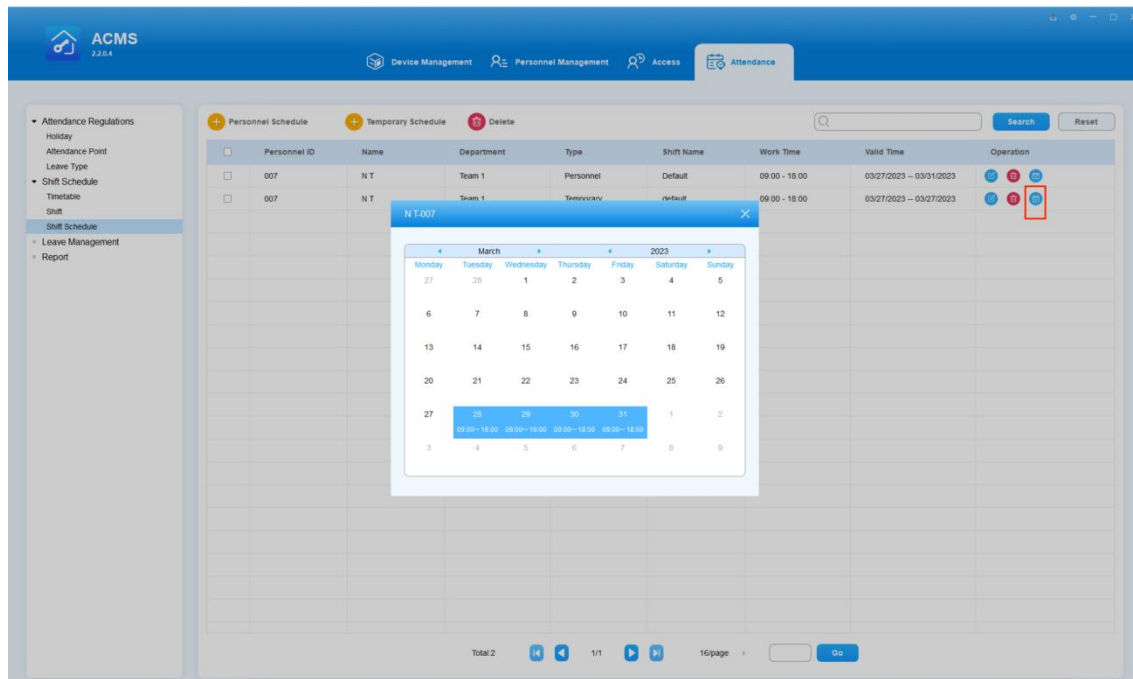
6.3.3.4. Edit the Assigned Shift

You can edit the assigned shift in terms of changing the shift and shift valid time range for the specific employee if needed.

1. Click on ✏️ of the specific assigned shift you want to edit

2. Change the shift and shift valid time range for the assigned shift.
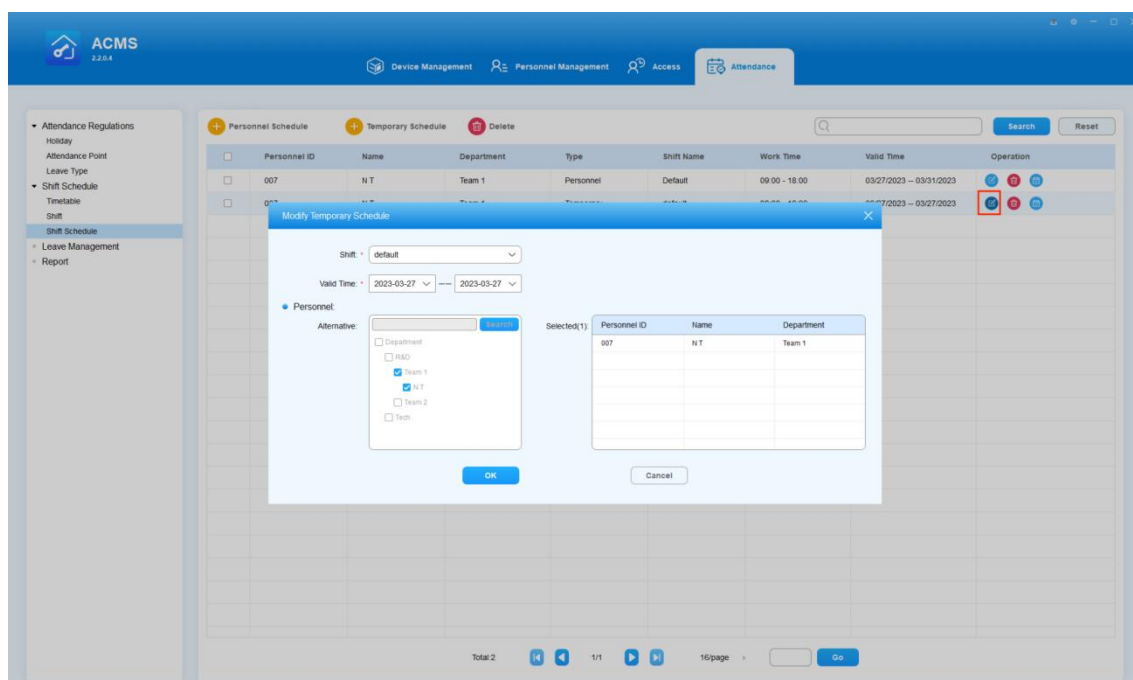
6.3.3.5. Delete the Assigned Shift

You can delete the assigned shift(s) if needed.

1. Click on the 🗑 of the specific assigned shift if you want to delete it separately.

2. Tick the checkbox(s) of the assigned shift(s) and click 🗑 Delete to delete all of the shifts.
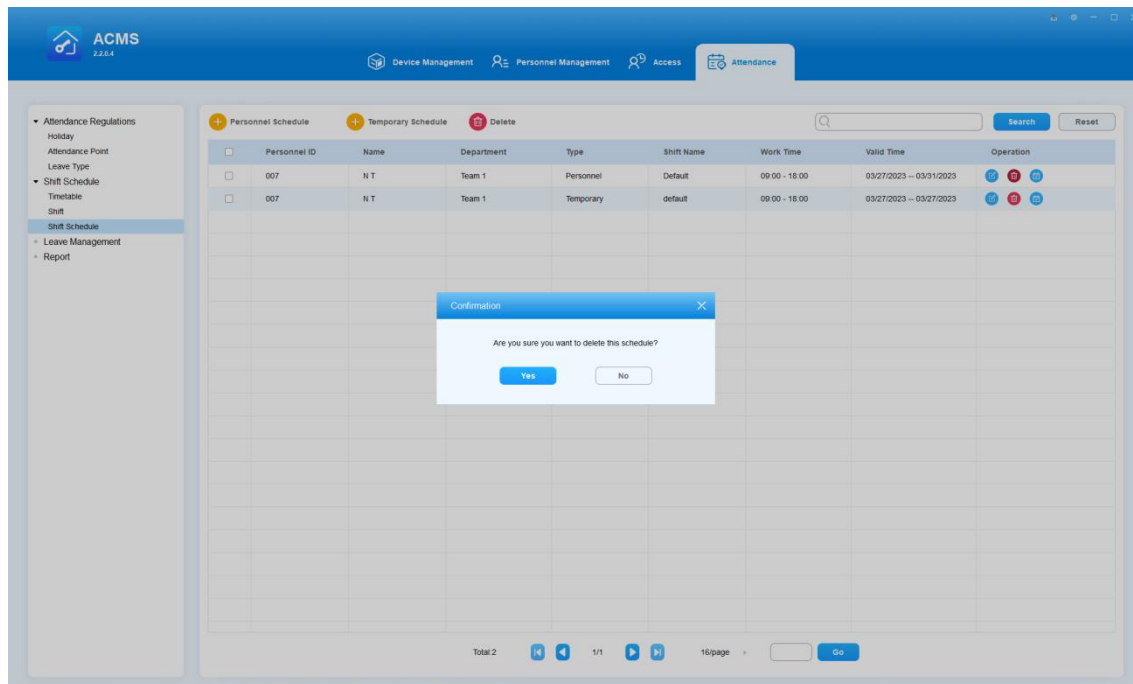
6.4. Leave Management

You can create, search, edit and delete employee leaves.

6.4.1. Customize Leave Types

AMCS allows you to add additional leave types if the default ones cannot meet the actual needs. This feature is used in conjunction with the Leave Management.

6.4.1.1. Add a new leave type

1. On the Attendance Regulations > Leave Type, click on [+ New] .

2. Name the leave type. Note that the name must not be empty or duplicate with existing types.

3. Click **OK**.
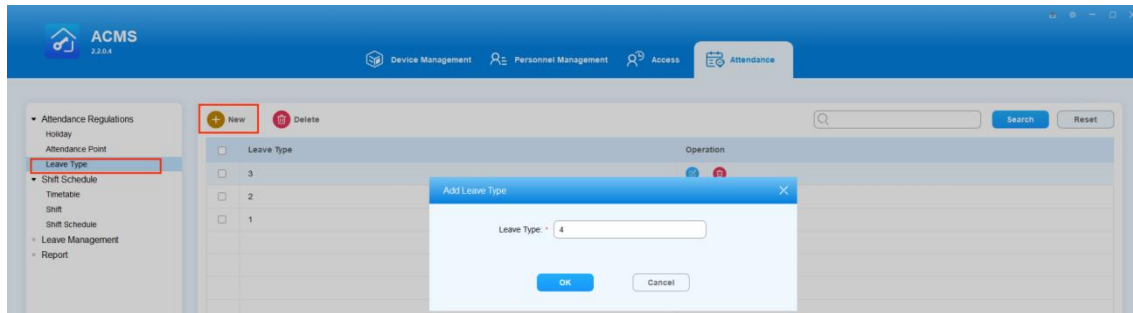
6.4.1.2. Edit a Leave Type

When editing a leave type, the new name will be synchronized in real-time with the Leave Management module.

NOTE:

However, the leave type that has already been used cannot be modified.

To edit a leave type, just double click it or click on [edit icon] in its Operation column.
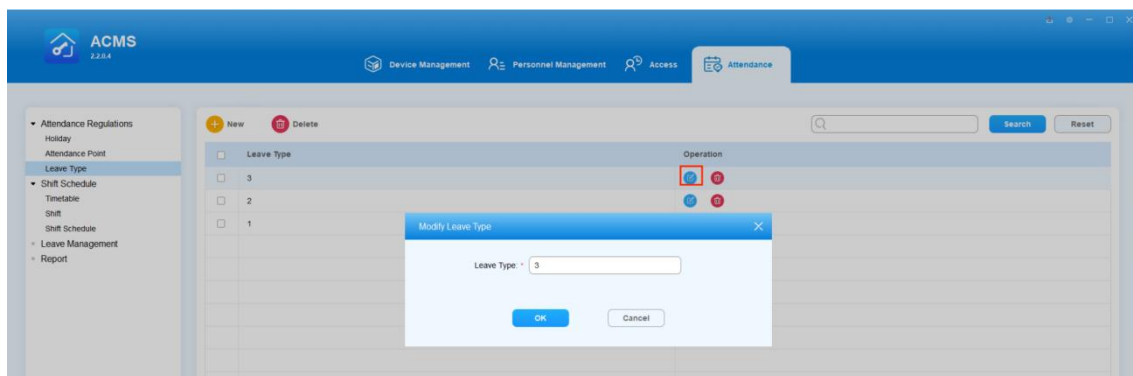
6.4.1.3. Delete the Leave Type

You can delete a leave type if it is no longer needed. Once a leave type is deleted, it will no longer be displayed on Leave Management module.

NOTE:

The used leave type cannot be removed unless all associated leave applications are first deleted.

To delete single leave type, just click on 🗑 in its Operation column. If you want to delete more than one of them, check off the desired types and click on 🗑 Delete .
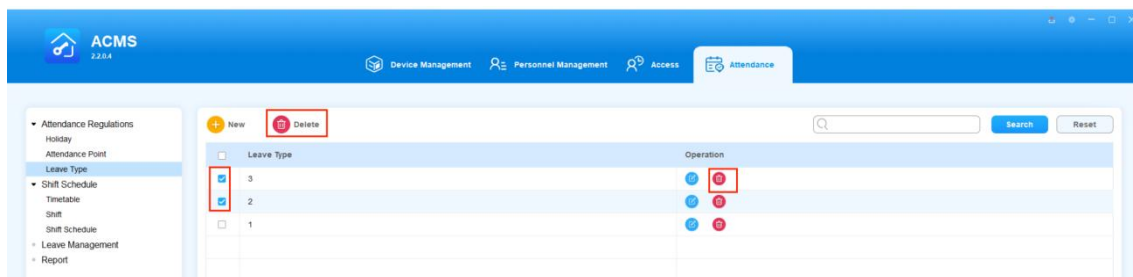
6.4.1.4. Search a Leave Type

The Leave Type interface allows you to search for leave types by entering the name of the type.
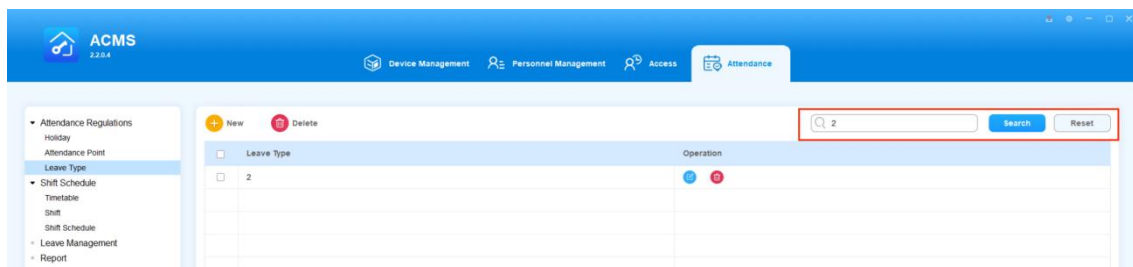
6.4.2. Add a Leave

You can create leaves for the employees by defining what the leave types are, when the leave starts and ends, to which employee the leave is to be applied, etc.

1. Enter the leave information.
2. Select the employee(s) to whom the leave is to be applied.
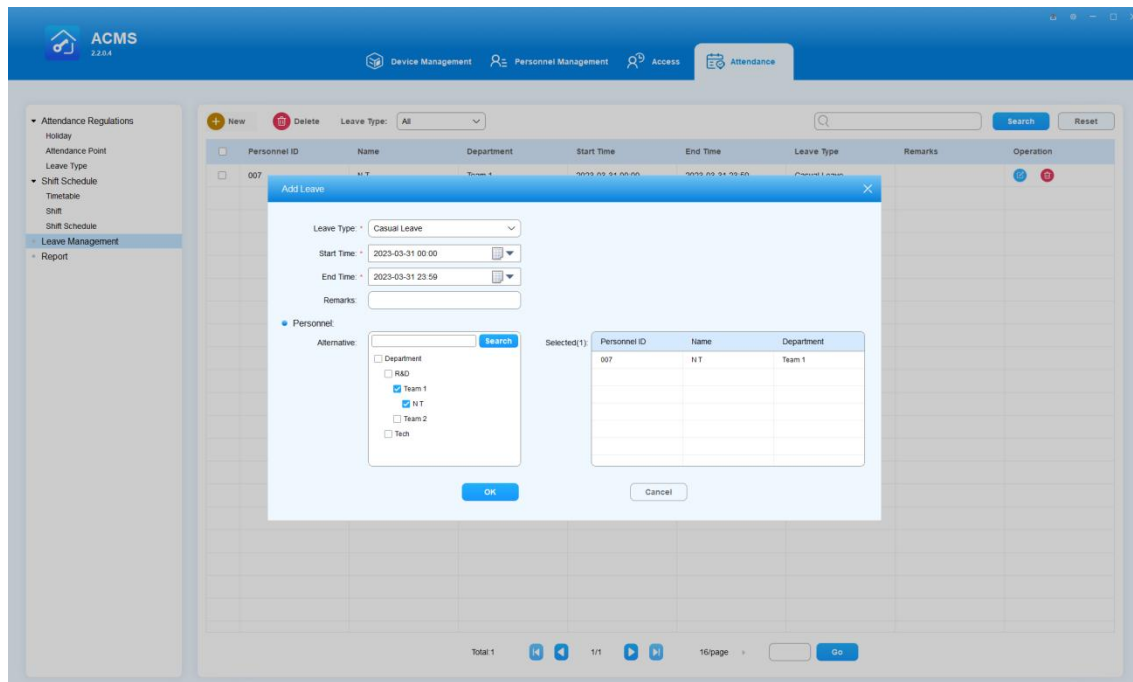
6.4.3. Search a Leave

1. Select the leave type to narrow down the search range if needed.
2. Search leaves by entering the employee ID or name in the search field.
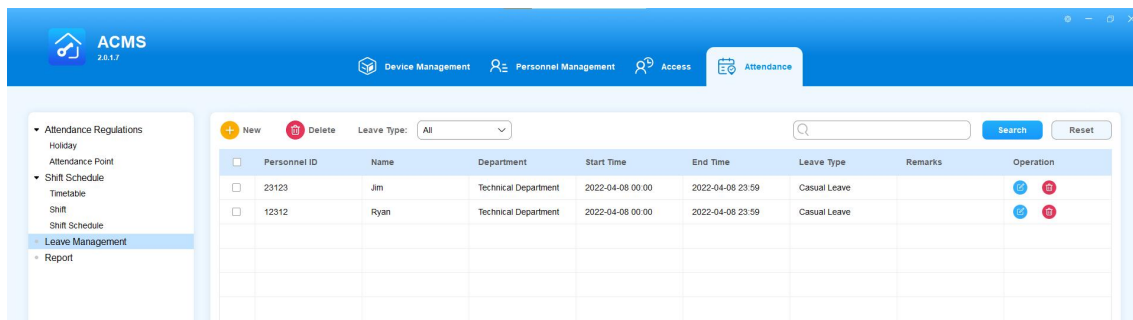
6.4.4. Edit a Leave

You can edit leave in terms of changing the leave type, leave start time, and end time.

1. Click on of the specific leave you want to edit.
2. Change the leave information.
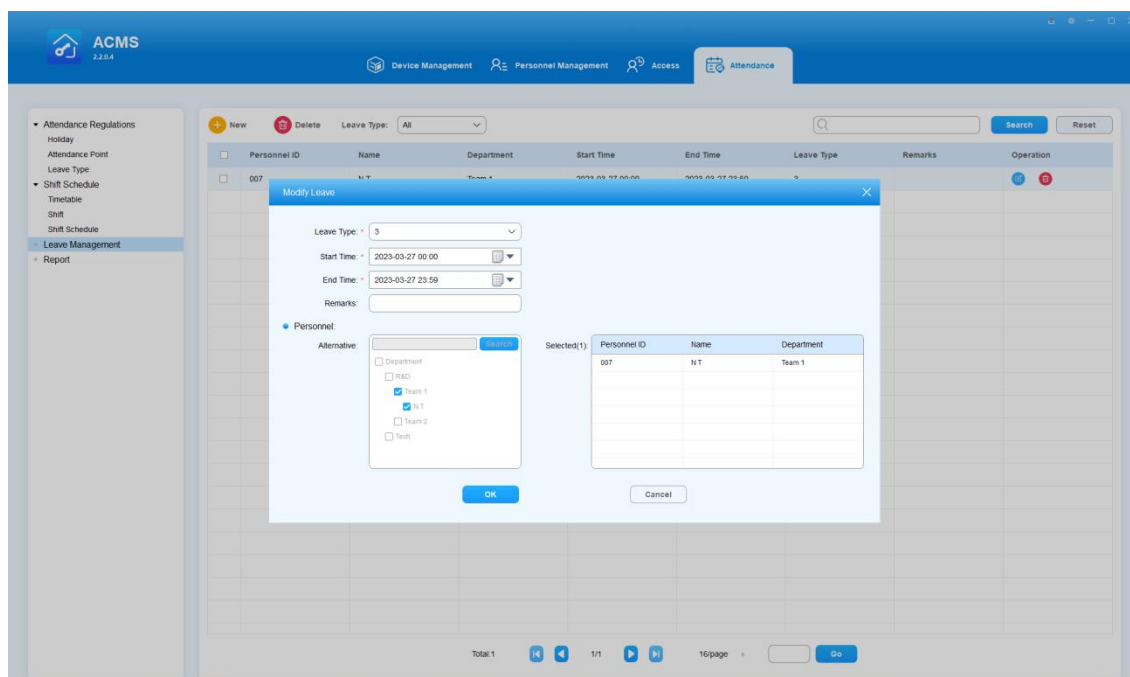
6.4.5. Delete a Leave

You can delete leave separately or in batch.

1. Click on 🗑️ of the specific leave you want to delete.

2. Tick the checkbox ☑️ Personnel ID of the leaves you want to edit or tick to delete all the leaves.
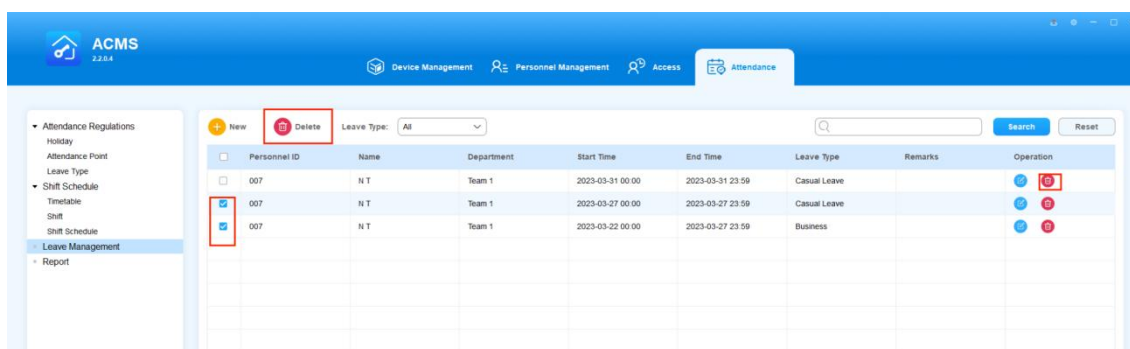
6.5. Attendance Report

6.5.1. Search/Check/Export Daily Attendance Report

You can manage your attendance report in terms of searching, checking, and exporting your attendance report on a daily basis.

Click on **Daily Report**, you can see all employees daily attendance reports. Do any of the following if needed:

- Search specific reports by

    - Entering employee's name or ID number,

    - Selecting a certain attendance type from the pull-down list; Or

    - Choosing a time range.
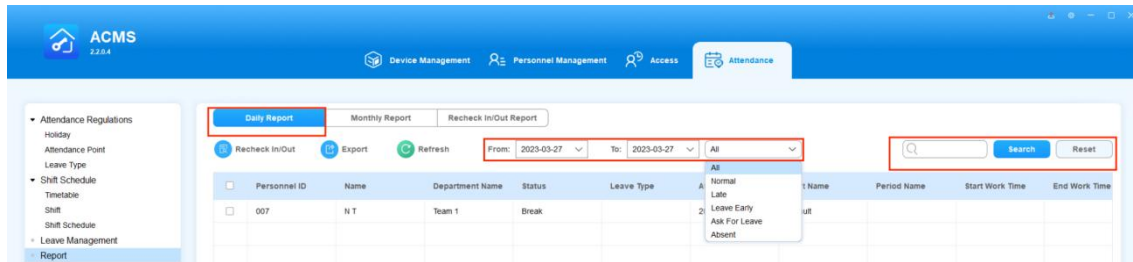
- Export an xls. format reports by clicking on **Export** and selecting the information display on the reports.
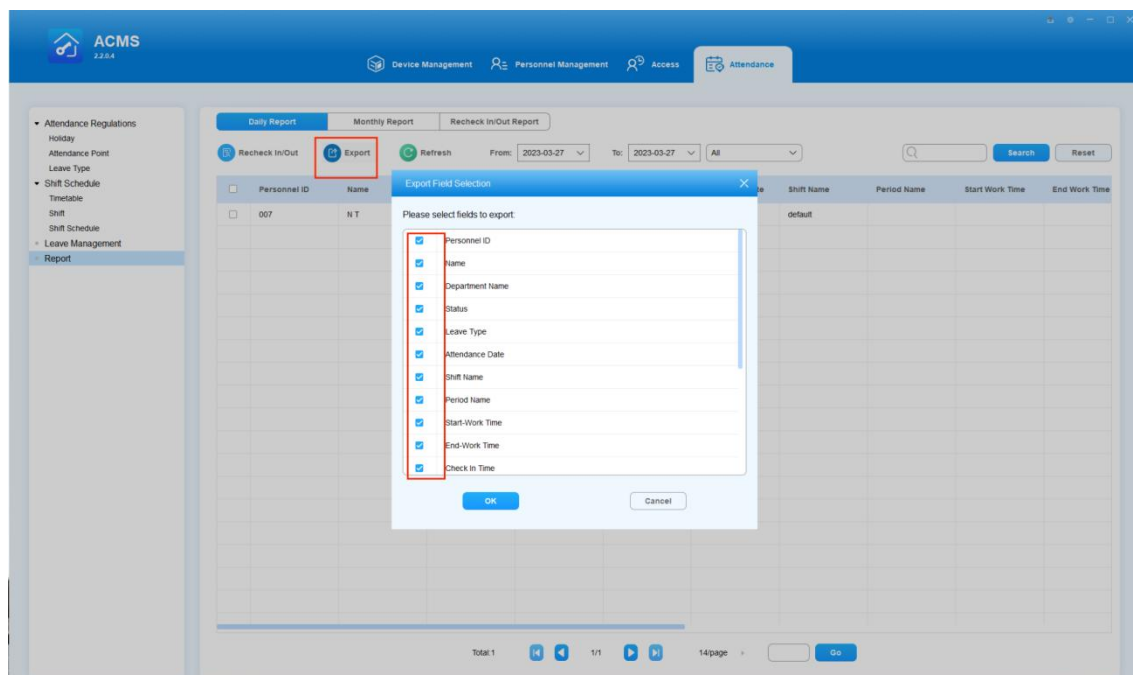
The following is a daily attendance report example.

6.5.2. Search/Check/Export Monthly Attendance Report

Click on **Monthly Report**, you can see all employees monthly attendance reports. Do any of the following if needed:

- Search specific monthly report by
  - Entering employee's name or ID number.
  - Select a certain month.
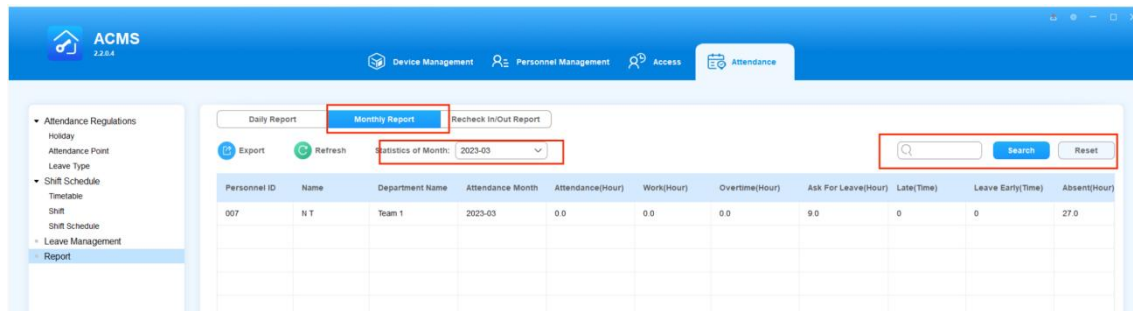
- Export an xls. format reports by clicking on **Export** and selecting the information display on the reports.
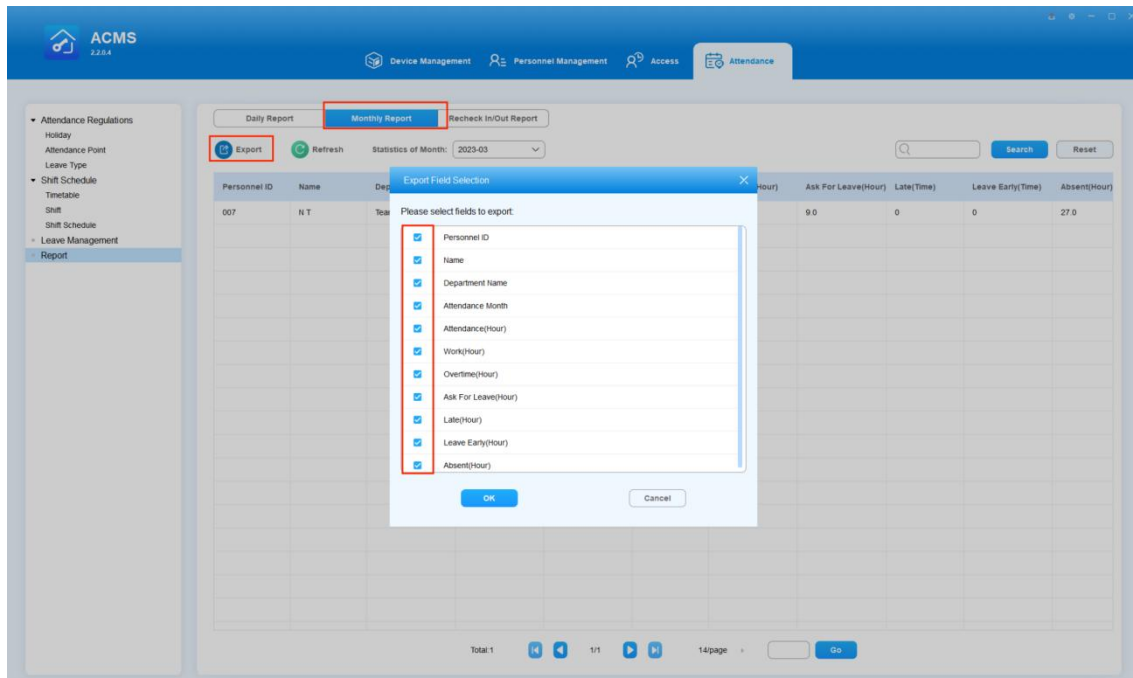
6.5.3. Correct Check-In/Out Time

You can correct employee's clock in/out time by performing a rechecking. You can also fix the missed punch if employees forgot to clock in or out.

1. Click on **Daily Report**.

2. Check off the record(s) that you want to fix the check-in/out time.

3. Click on **Recheck In/Out** .

4. Tick the checkbox of the missing check-in or check-out, and click **OK**. The employee's attendance record will be updated accordingly.


Note:

- The time for the re-clock must be within the employee's designated working hours, otherwise the re-clock will fail.

- If you need to recheck for multiple employees at one time, they must be assigned with the same shift.

6.5.4. Check/Export/Delete the Recheck-In/Out Record

Click on [Recheck In/Out Report], then you can see all employees rechecking reports. Do any of the following if needed:

- Search specific rechecking report by
  - Entering employee's name or ID number.
  - Select a certain time range.

- Export an xls. format reports by clicking on [Export].

- Delete reports by checking off the specific reports and clicking [Delete].
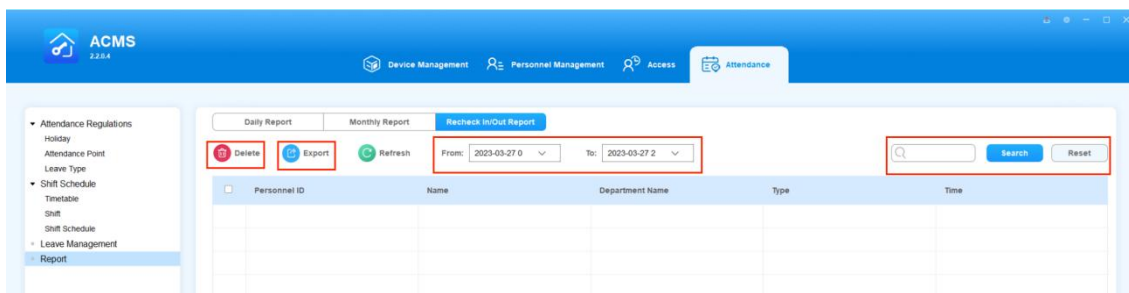
7. System Settings

ACMS allows you to export the system data to your PC as a backup in advance, which can be later imported back to the ACMS in case missing data occurs. In addition, you can also create and modify the password.
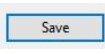
7.1. Set a System Language

ACMS now supports 4 languages: English, Chinese, Russian, and Turkish.

To set your preferred language, click on ⚙ in the upper right corner, and select **System Settings > Language**.
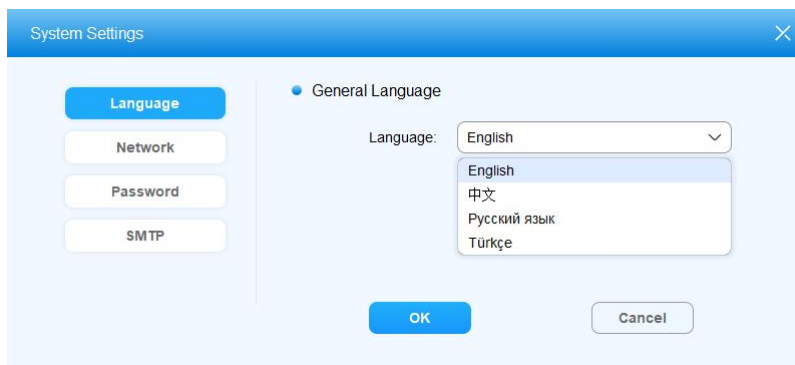
7.2. Import and Export System Data

● **Export System Data**

1. Click on ⚙ in the upper right corner and select **Database** from the pull-down list.

2. Click ⬆ Export and select the path to which you want to export the data to your computer.

3. Click on Save in your computer to confirm the path.

4. Click **OK** for confirmation.
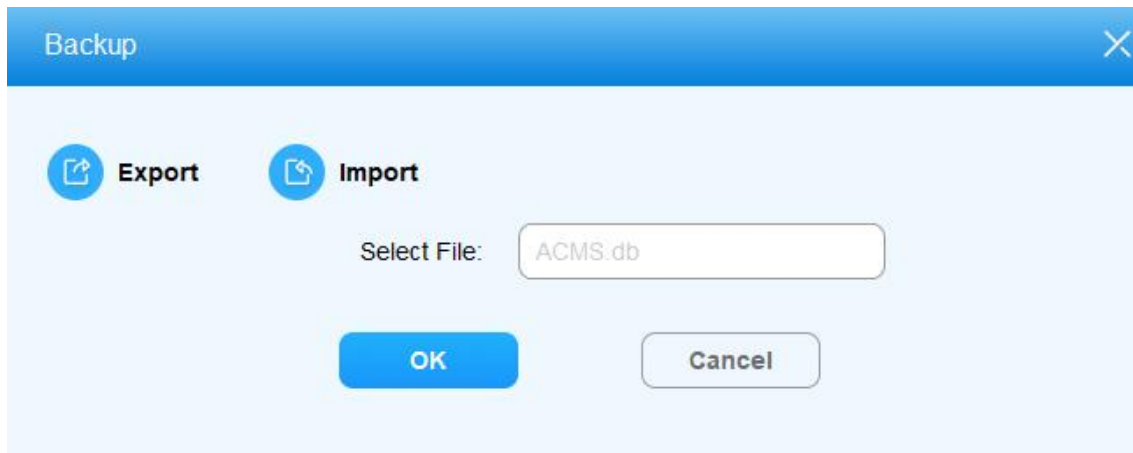
● **Import System Data**

1. Click on [icon] in the upper right corner and select **Database** from the list.

2. Click on [Import icon] to select the data file to be imported to the ACMS.

3. Click **Open** to upload the file, then click **Yes** for confirmation.

> **Note:**
>
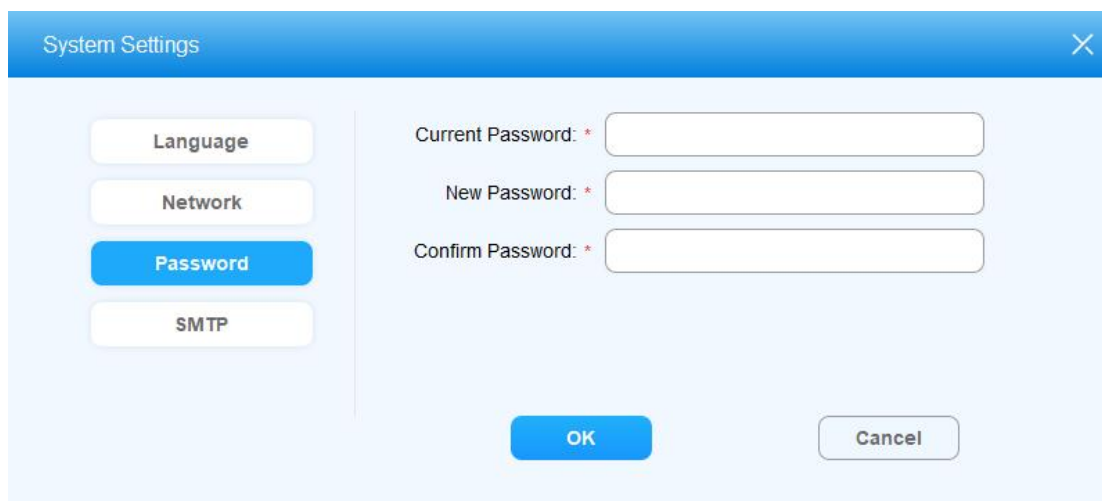> ● The data file to be imported into ACMS should be in .db format.

7.3. Modify Login Password

1. Click on [icon] in the upper right corner and select **System Setting** in the pull-down list.

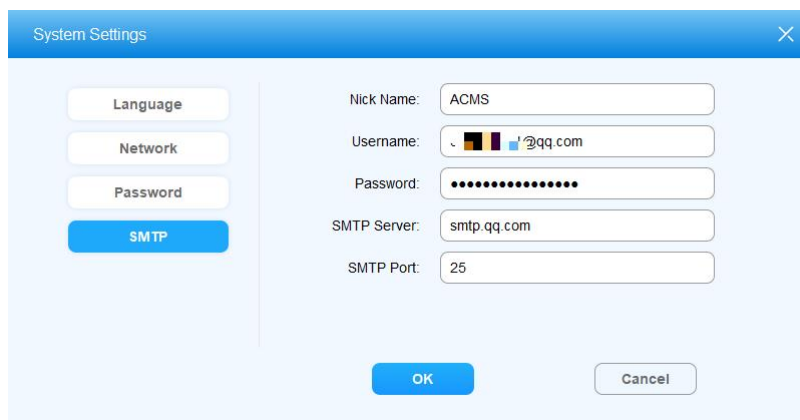2. Click on **Password.**

3. Change the password.

4. Click on **OK**.

7.4. SMTP Configuration for Emails

SMTP is used for sending employees PIN codes when creating authentication codes. To set this up, click on [gear icon] in the upper right corner, and select **System Settings > SMTP.**

NOTE:

Some email servers require enabling the SMTP service before sending and receiving emails successfully.
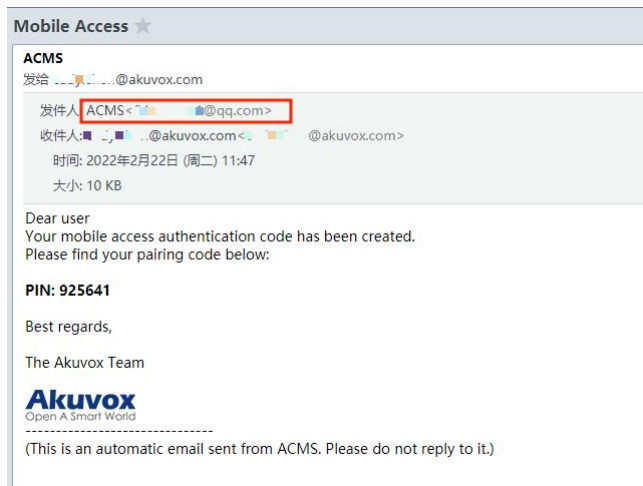

Parameters Setup:

- **Nick Name**: To customize the sender's name.
- **Username**: The email address used for sending emails.
- **Password**: The password of the email that you used for sending emails.
- **SMTP Server**: The address of the SMTP server.
- **SMTP Port**: The port number of the SMTP server.

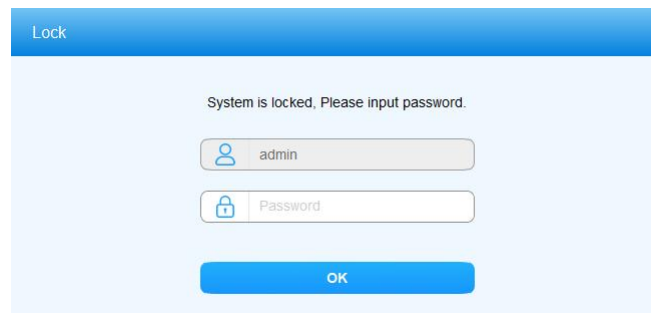Employees will receive such a PIN code email:

7.5. Lock/Unlock ACMS

You can lock the ACMS interface using the Login password when you are managing the ACMS for security purpose.

To lock the software, click on [icon] in the upper right corner, and select **Lock** from the pull-down list.

To unlock, you have to enter the login password.

> **Note:**
>
> ● The default unlock password is **admin**.

8. Contact Us

For more information, please visit us at www.akuvox.com or feel free to contact us by
Sales email: sales@akuvox.com
Technical support email: support@akuvox.com
Telephone: +86-592-2133061 ext.7694/8162
We highly appreciate your feedback about our products.