ARMATURA

User Manual

Armatura One Security Platform

Armatura One 2.2.0

Date: Nov 2022

Doc Version: 1.0

Trademark

ARMATURA is a registered trademark of ARMATURA. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ARMATURA equipment. The copyright in all the documents, drawings, etc. in relation to the ARMATURA supplied equipment vests in and is the property of ARMATURA. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ARMATURA.

The contents of this manual must be read before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ARMATURA before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel have read, understood, and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ARMATURA offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ARMATURA does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability, or fitness for a particular purpose.

ARMATURA does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ARMATURA in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ARMATURA has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ARMATURA periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ARMATURA reserves the right to

add, delete, amend, or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ARMATURA shall in no way be responsible (I) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on https://armatura.us/

If there is any issue related to the product, please contact us.

ARMATURA Headquarters

Address:190 Bluegrass Valley Parkway Alpharetta, GA 30005

Phone: +1-650-4556863

Email: sales@armatura.us

Website: www.armatura.us

About the Manual

This manual introduces the operations of ARMATURA One software.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g., **OK**, **Confirm**, **Cancel.**
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Content

1. Overview

The ARMATURA One software brings a unified management platform to help the customers in managing and integrating security operations with minimal effort. The data processing capacity of the software is very high such that it can manage 30,000 personnel data at an instance. The user data security is guaranteed since the software adopts role-based multi-level management. The software also ensures to track the events and operations in real-time with relevant notifications to the system user.

Features

- It can manage around 300,000 personnel data with its powerful data processing capacity.
- Users' data are more secured with multi-level management role-based level management.
- It can track events and operations in real-time to ensures prompt feedbacks of data to the system administrators.

Configuration Requirements

- Quad core processor with a speed of 2.5GHz or above.
- System Memory of 16GB DDR4 or above.
- Available space of 500GB or above. We recommend using NTFS hard disk partition as the software installation directory.
- Monitor Resolution of 1920*1080px or above.

Specifications

Supported Operating Systems	Windows 7 Windows 10 Windows Server 2012/2016/2019
Supported Databases	PostgreSQL (Default), SQL Server & Oracle (Optional).
Recommended Browser Version	Internet Explorer 11+ Chrome 33+ Microsoft Edge 88+ Firefox 27+

Modules

- The system is divided into 17 modules which are as follows: -

1.1. Personnel Module

The Personnel Module is used to set person's details and their respective department. It primarily consists of two parts: Department Management settings, which is used to set the company's organizational chart; Personnel Management settings, which is used to enter the person information, assign departments, maintain, and manage personnel.

1.2. Access Module

The Access module is a web-based management system which enables normal access control functions, management of networked access control panel via system, and unified personnel access management. The access control system sets door opening time and levels for registered users.

1.3. Attendance Module

The Attendance module can achieve cross-regional attendance centralized control through the shift and shift management. You can apply for Appended Receipt, Leave, Overtime, etc. in Exception Management. In this module, you can also set the attendance point for access/parking and other functions.

1.4. Elevator Module

The Elevator module is mainly used to set the Elevator parameters (such as the swiping interval for using elevators and elevator key drive duration), manage personnel's access rights to different floors and elevator control time, and supervise elevator control events. You may set registered users' rights to floors. Only authorized users can reach certain floors within a period after being authenticated. And now we support 3rd brand elevator such as KONE/Mitsubishi/Hitachi.

1.5. Visitor Module

The Visitor module is a web-based management system that implements entry registration, exit registration, photo capturing, visitor statistics, booking management, and shares information among registration sites. It is highly integrated with the access control system and elevator control system. It is generally used at reception desks and gates of enterprises, to manage visitors.

1.6. Parking Module

The Parking module is an automatic and intelligent vehicle management which can effectively and accurately monitor and manage vehicles at all exits and entrances.

1.7. Video Module

The Video module is integrated with and Milestone Xprotect, which supports video functions including preview, playback, and video recording. There are other video applications, such as video patrol.

1.8. Office Module

The Office Module is a space management module where you can manage and configure your meeting room, check the status of the meeting room, make reservations, and view the meeting. Once you reserve a meeting room, it will be automatically associated to the corresponding PAD device, and personnel rights will be immediately issued to the PAD for verification.

1.9. Fire Alarm Module

The Fire Alarm module is designed to dynamically display the system's pre-defined alarm information, in combination with the multi-dimensional map which provides a clear understanding of what is happening in the area. It helps the user to better observe and handle alarm situations.

1.10. Entrance Control

This system connects the gate control board through channel Device (such as TDA integrated machine), and directly controls the relevant parameters of the gate through software, thus controlling the entry and exit of the gate and realizing the automatic management of the gate.

1.11. FaceKiosk Control

The FaceKiosk module is based on visible light face is used to verify face by uploading and downloading personnel access level. In addition, advertisement pictures and videos can be sent to the FaceKiosk device to make full use of the functions of the device in different time periods.

1.12. Temperature Detection Module

The Temperature Detection Module uses near-infrared technology to measure and collect human body temperature. It can quickly help you to measure and collect the temperature of large number of people and deny access to unmasked people and whose body temperature status is abnormal. It provides alarm notifications to ensure the safety of you and others.

1.13. Defense Module

The Defense Module includes multiple application functions, such as defining the personnel library, vehicle library, management library and third-party synchronization relationship, performing global target alerts and monitoring, setting occupancy control, etc. It is an important module for system security defense.

1.14. Data Monitor Module

Data Monitor Module is a data module that integrates system basic data collection, data analysis, it can help users understand the security situation of the system with intuitive data, and give different data for different positions, so that the data is more targeted to help and guide users to make judgments on security to improve system security.

1.15. Building Automation Module

Building automation control uses computerized centralized control, which centralizes decentralized control for centralized management. Its decentralized controller usually adopts direct digital controller (DDC), which uses computer for monitoring and management of the screen. Building automation is composed of several systems including: air conditioning HVAC and ventilation monitoring system, water supply and drainage monitoring system, lighting monitoring system, power supply monitoring system, and structured integrated wiring system, and dynamic environmental monitoring system, with the aim of improving occupant comfort, efficient operation of building systems, reducing energy consumption, and operating costs as well as improving the service life of utilities.

1.16. Intrusion Module

Intrusion Alarm module Intuition Alarm is an electronic system that uses sensor technology and electronic information technology to detect and indicate illegal entry or attempted illegal entry into a fortified area (including subjective judgments when faced with hijacking or robbery or other critical situations, intentionally triggering an emergency alarm device), process alarm information, and send alarm messages.

1.17. System Module

System module is primarily used to assign system users and configure the roles of corresponding modules, manage databases such as backup, initialization, and recovery, and set system parameters and manage system operation logs.

2. System Operations

2.1. Login to the System

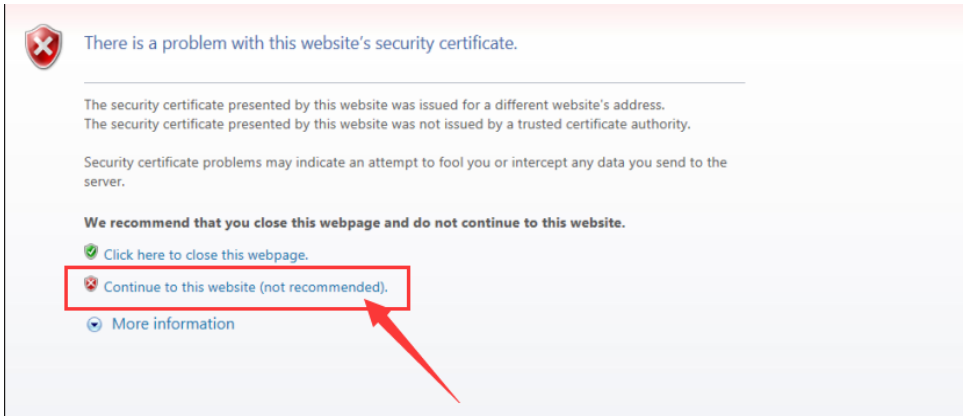
After installing the software, double-click the ARMATURA One icon to enter the system. You may also open the recommended browser and input the IP address and server port in the address bar. The IP address is set as: https://127.0.0.1:8098 by default.

If the software is not installed in your server, you may input the IP address and server port in the address bar.

✍**Note:**

- The username of the super user is [admin], and the password is [Changeme_123]. After the first login to the system, please reset the password.
- If you have selected the HTTPS port during software installation, input the server IP address and port number (for example, https://127.0.0.1:8098) in the address bar and press Enter. The following prompt may be displayed:

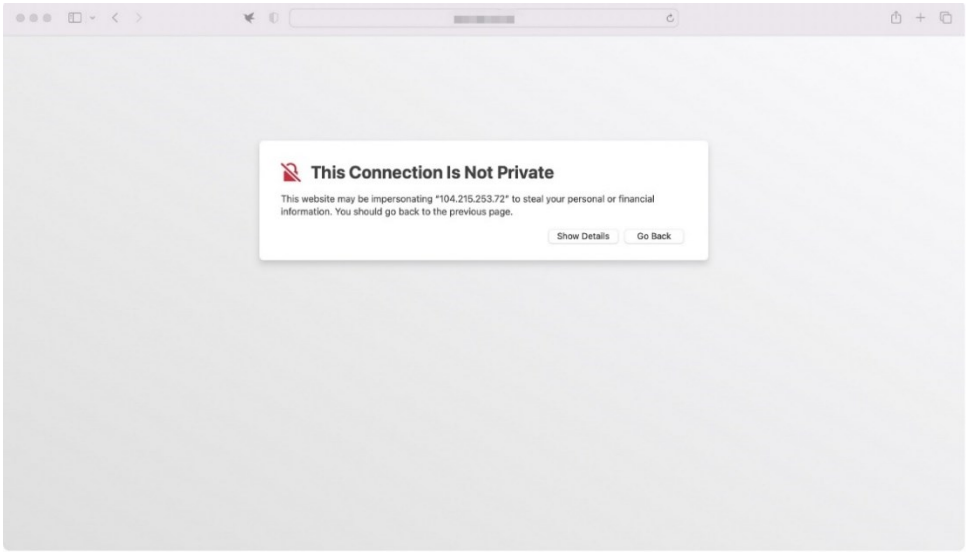
Windows Version:



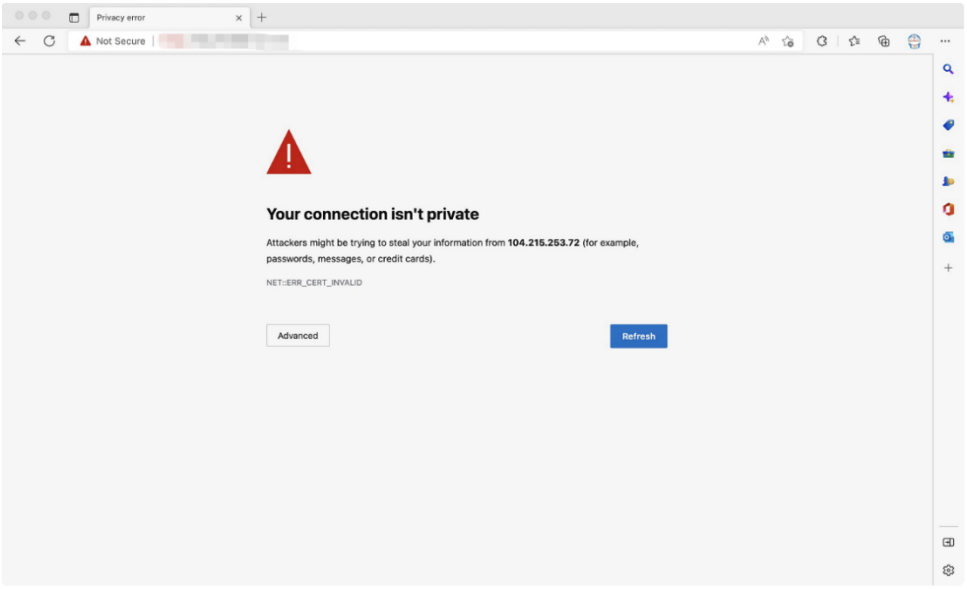
Please click "Continue to this website" as shown. Different browsers may operate differently.

Mac Version:

Safari



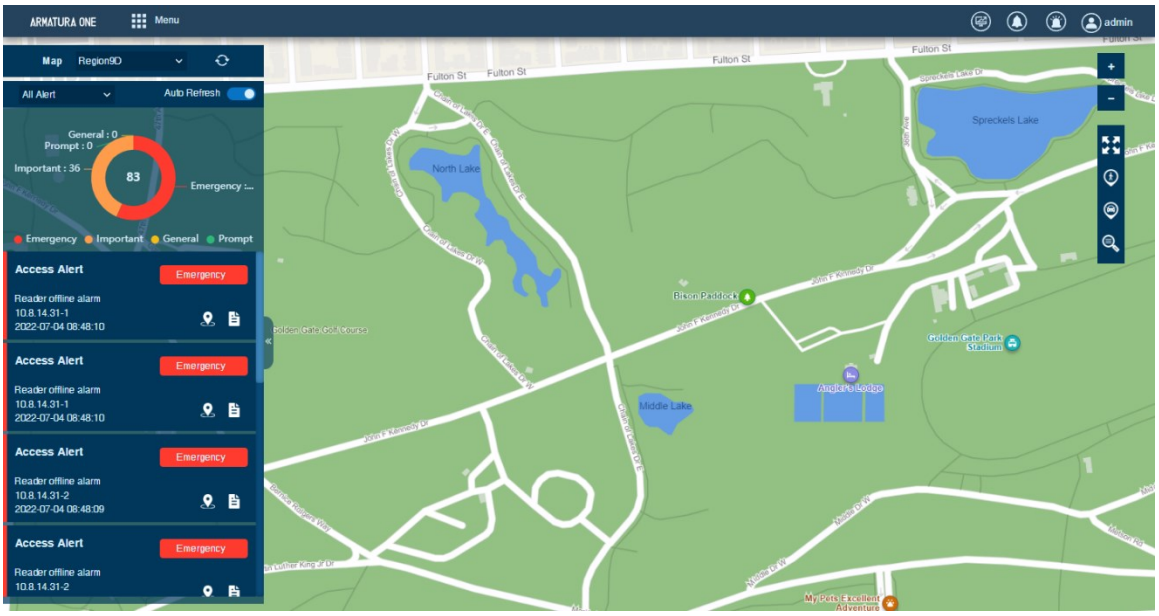
Microsoft Edge:



When show this page, type ‘thisisunsafe’ on keypad

2.2. Alarm Center

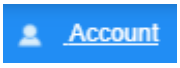
After logging in, the home page is displayed as shown below. If you want to go to home page from any interface, then you can click ‘ARMATURA One’ logo on the upper left corner of the interface to return to the home page.

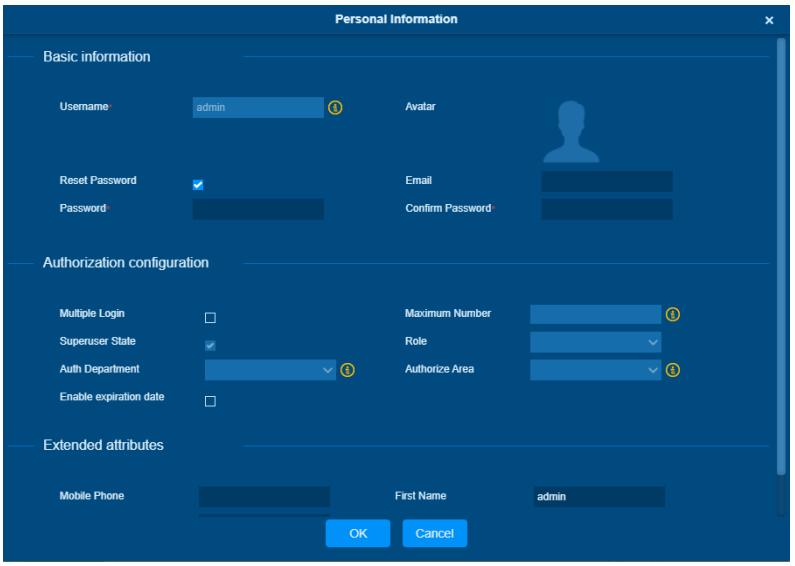


Activating the system

Please refer to the corresponding license document.

2.3. Modifying Password

You can modify the login password in [**Account**]: 



Check [**Reset Password**] box to modify the password.

✍**Note:**

Both, super user and the new user are created by the superuser. The username is not case-insensitive, but the password is case-sensitive.

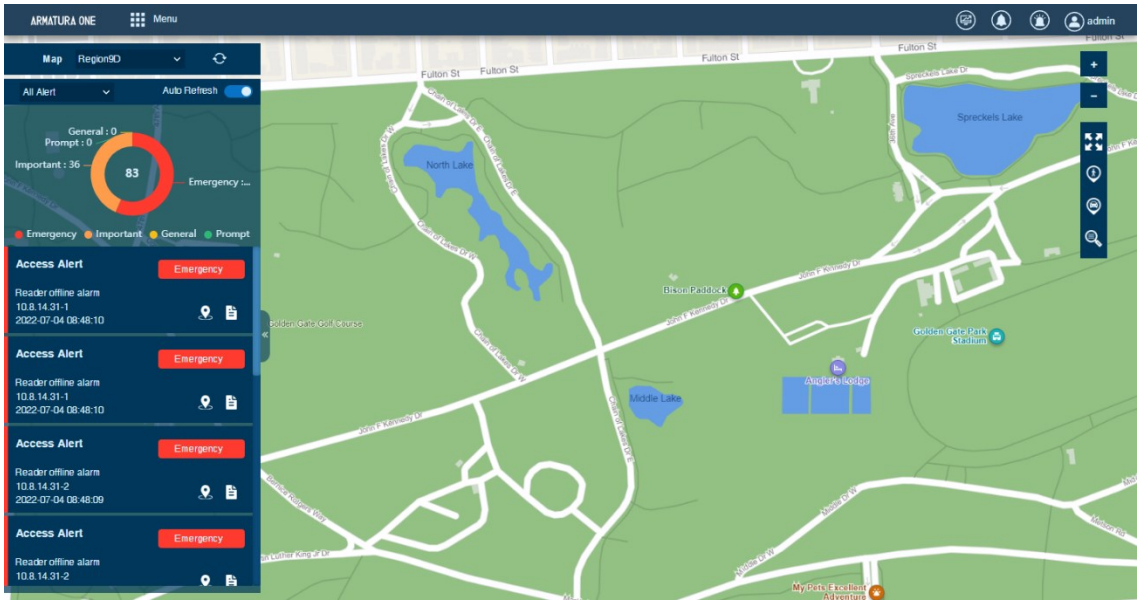
2.4. Exit the system

Click the [**Logout**] button 

on the upper right corner of the interface to exit the system.

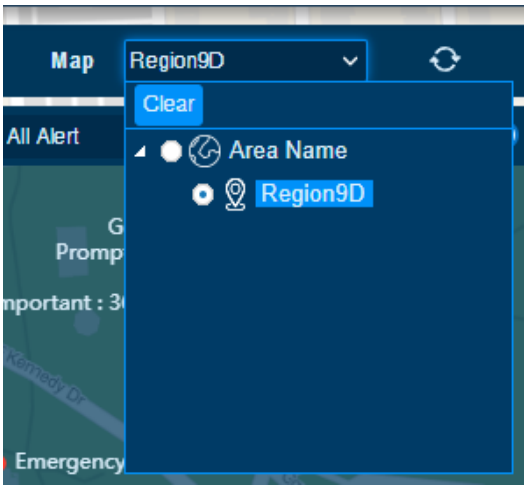
3. Alarm Center

The alarms triggered when the device detects abnormal conditions and meets the alarm conditions are displayed here, and the displayed alarms can be viewed and processed.

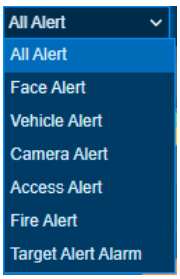


The operation is as follows:

1. Use the drop-down to switch maps in different areas.

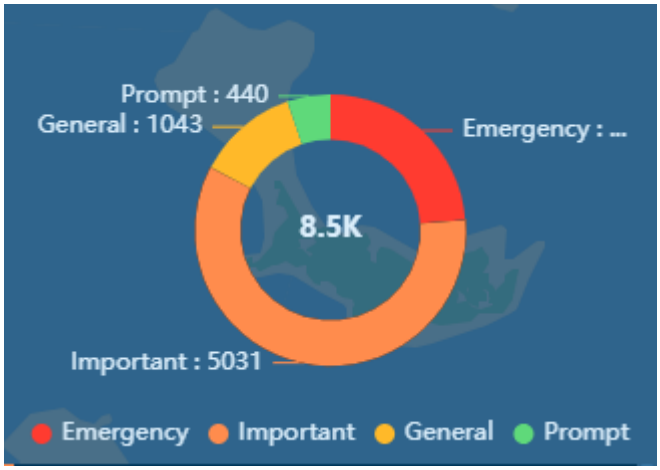


2. Use the drop-down to switch Alerts in different type, Contains four types of alerts: Access Alert, These alarms come from the pre-sets of your Access module and Video module.

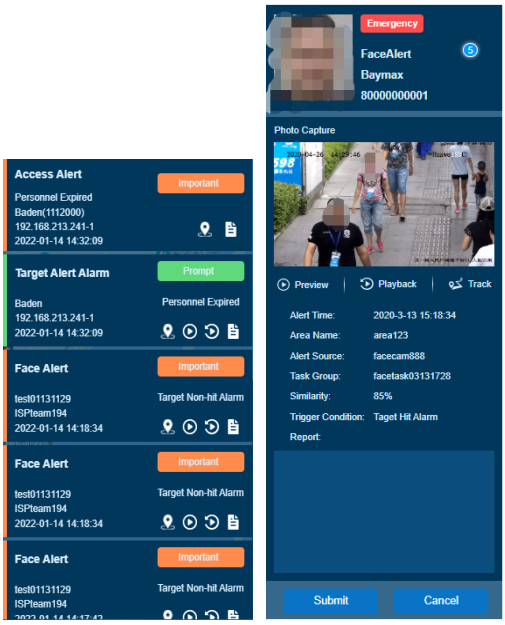


3. Auto Refresh turn on/off to switch between focusing on certain alarms or viewing real-time alarm data.

4. The dashboard not only displays the number of alerts, but you can also use it to filter alerts and help you find content quickly.

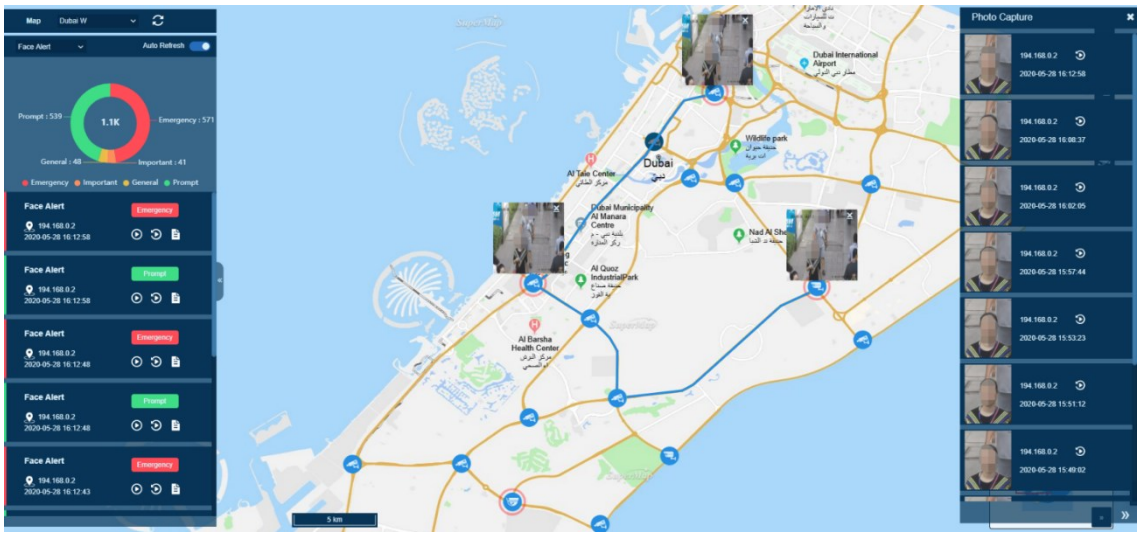


5. Lists help you quickly locate alarm devices, view previews and playback, as well as view details and resolve alarms.

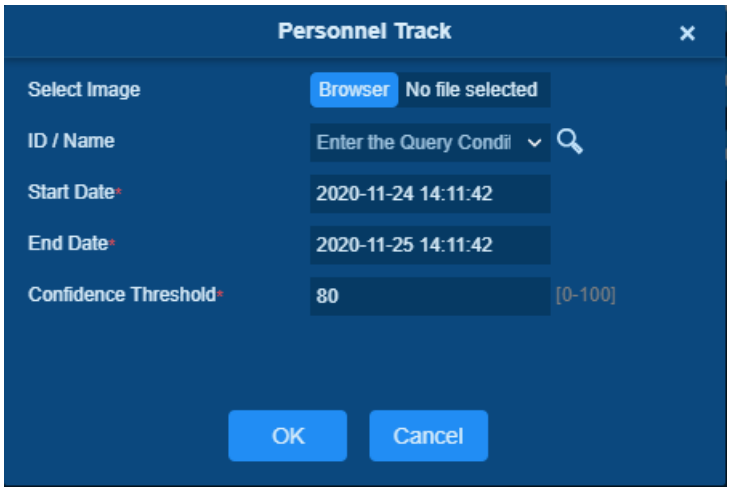


3.1. Personnel Track

Simulate the trajectories of people on the map through the capture of the camera.



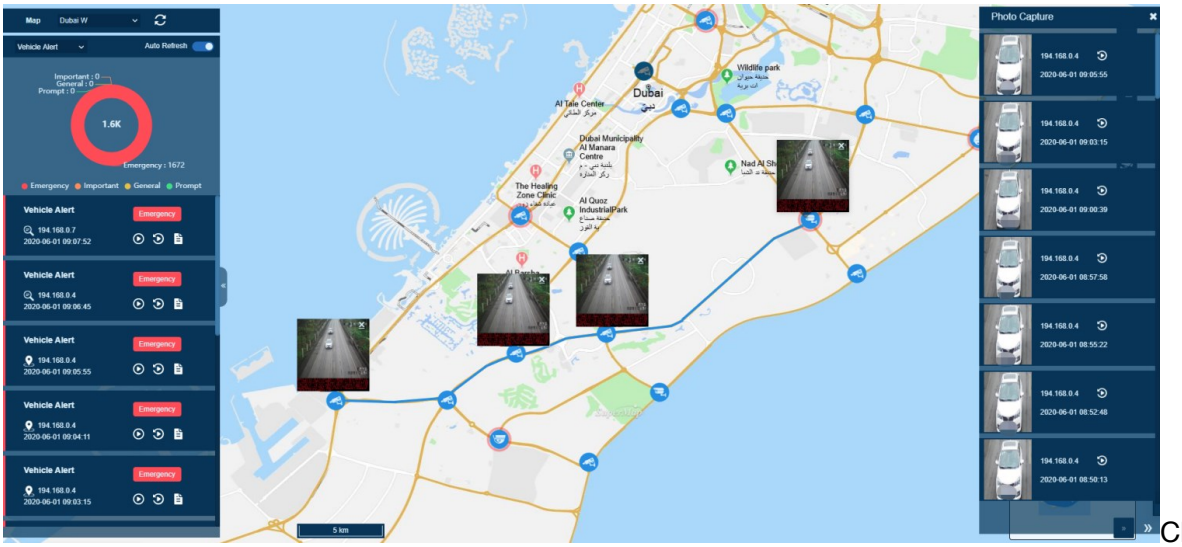
Click "Personal Track", upload a picture of the person in the pop-up window or select the employee/guest and set parameters.



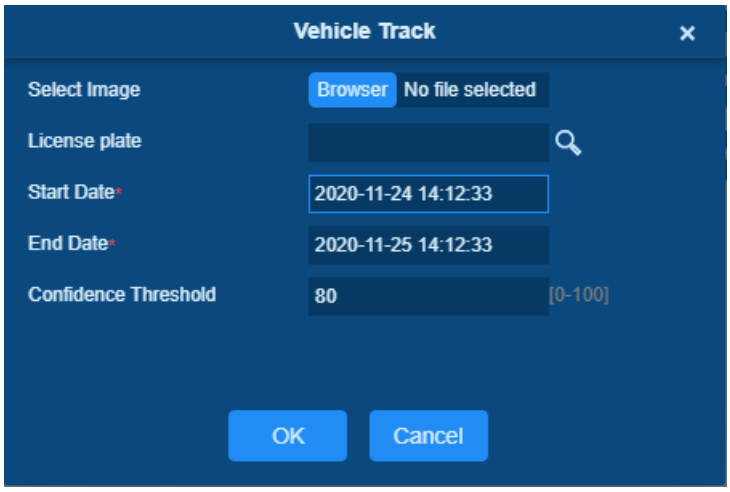
You can Playback the captured images in the right list.

3.2. Vehicle Track

Simulate the trajectories of vehicle on the map through the capture of the camera.



Click "Vehicle Track", upload a picture of the vehicle in the pop-up window or select the license plate from Parking and set parameters.

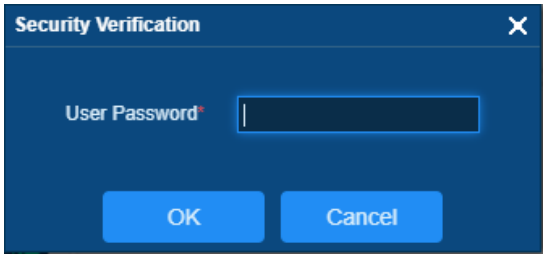


You can Playback the captured images in the right list.

3.3. Batch Door Operations

You can quickly perform batch operations on doors, including remote opening / remote closing / active lockdown / deactivate lockdown / cancel alarm / remote normally open.

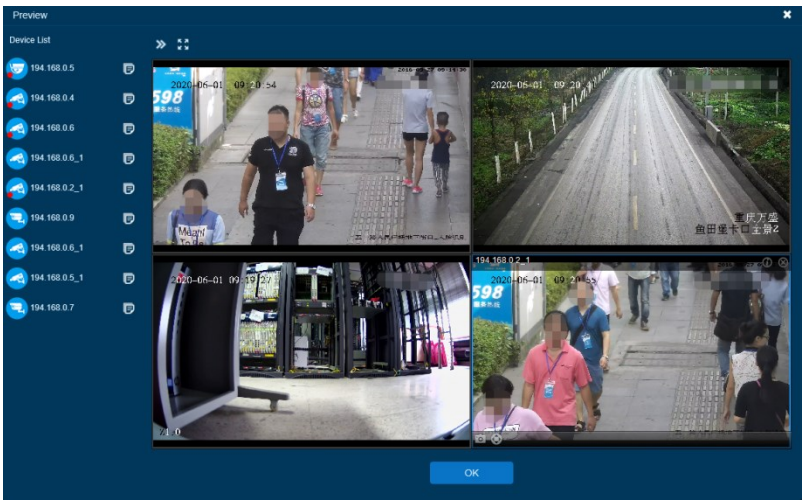
Click the button to Frame Selection or select all with “Add All”, submit and enter user password to process.



3.4. Batch Camera Operations

You can quickly perform batch operations on cameras preview.

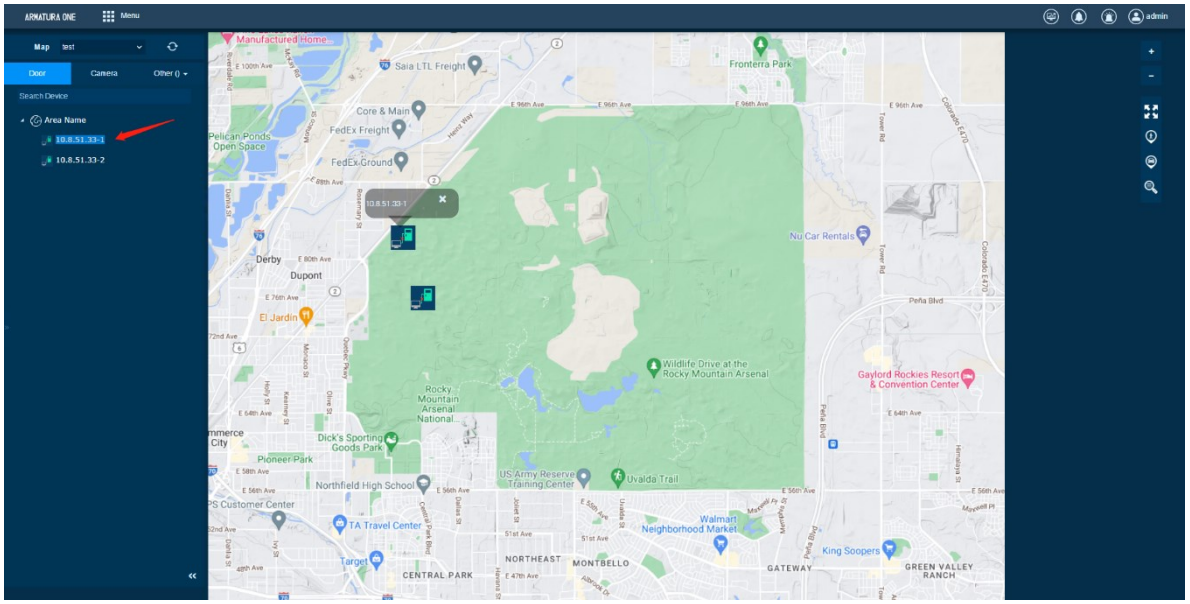
Click the button to Frame Selection or select all with “Add All” and submit.



3.5. Search Device

Use this function to locate and find the device on the map.

Click "Search Device" and locate the device location by entering the device name or selecting the device name from the list.



Click the name of the device, the map will automatically move and focus on the device you selected.

3.6. Browser Notification

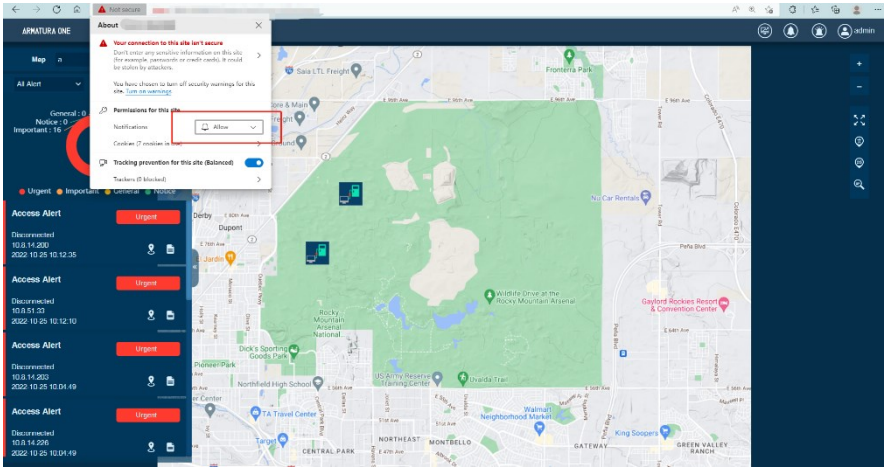
Browser Notification function can prevent users from missing software messages. When the software

authorizes the browser message notification permission, the browser can send pop-up notifications about the alerts and other notifications even when the software is running in the background.

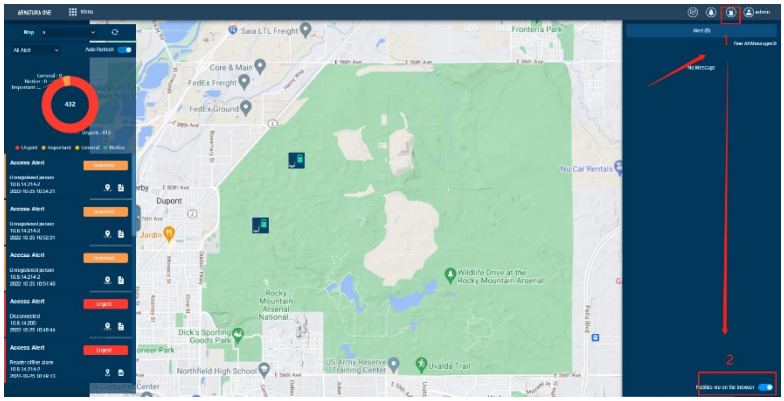
Enable the browser notification

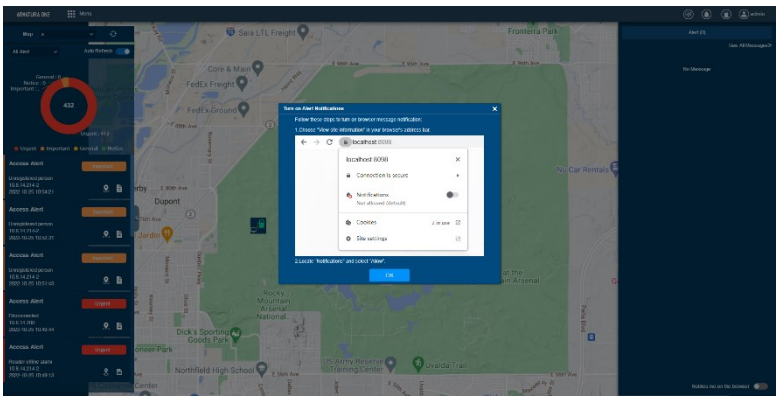
There are two ways to enable the browser notification:

1. After successfully logging into the system, a pop-up window for browser authorization will appear; click the [Allow] button to allow notifications, as shown in the figure below.

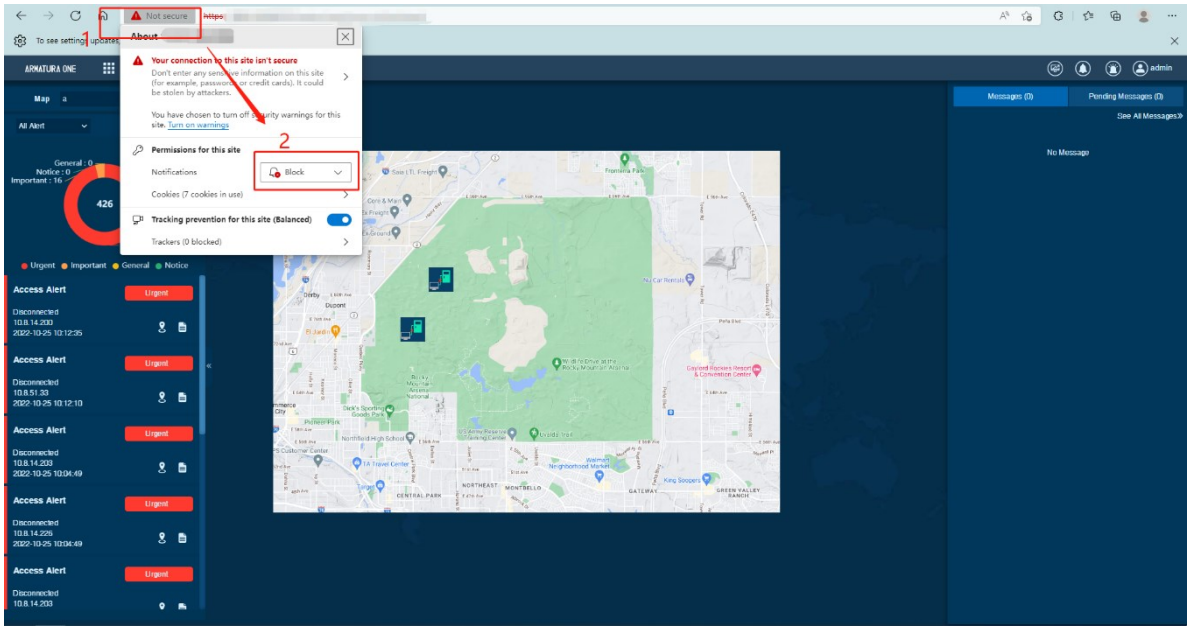


2. If users have already clicked [Block] and need to restart message notification, click .the button on the application's home page, then click the button, there will be a corresponding operation prompt, follow the prompt to allow the browser notification.



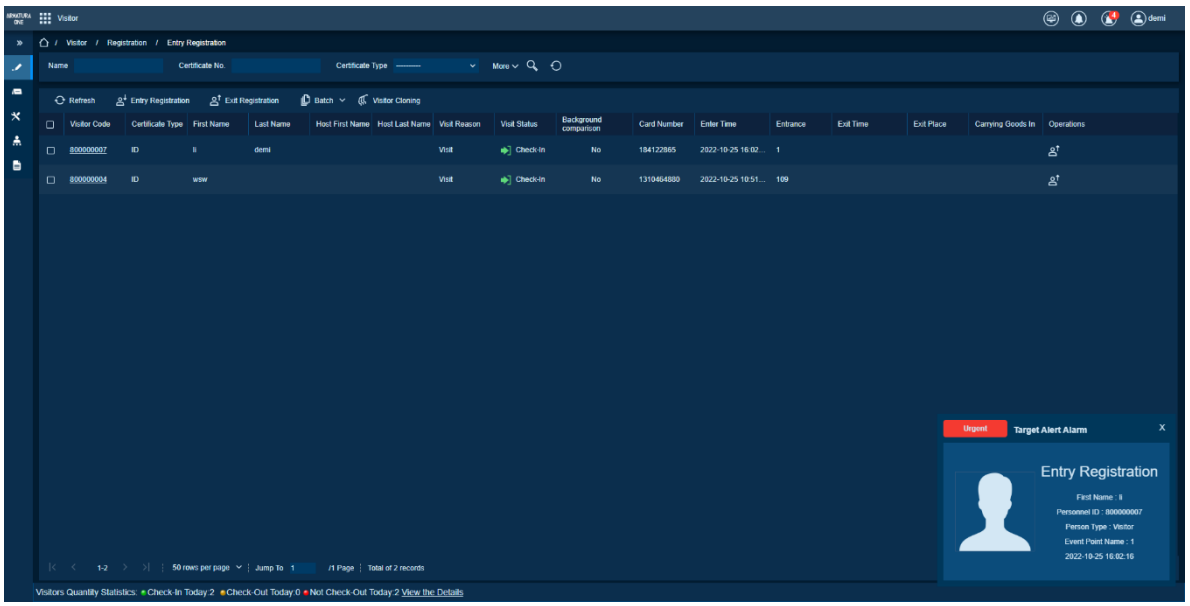


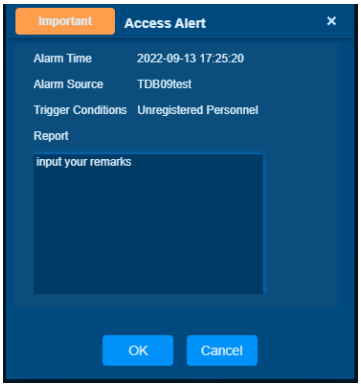
Follow steps ① and ② to change message notification authorization as shown in the figure below:



Viewing Notification Details

If there is a pop-up notification, you can double-click the message interface to view the event details.

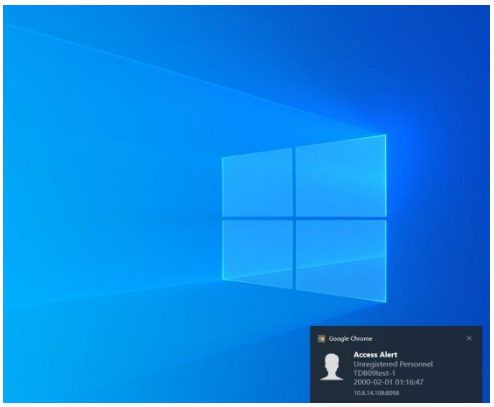




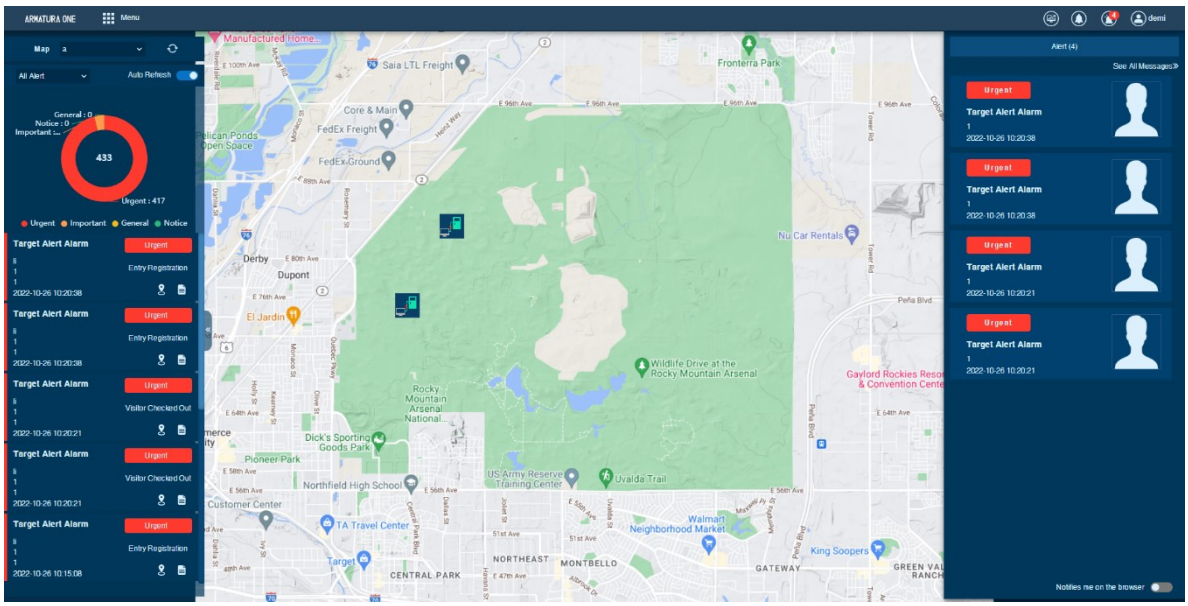
When the software is running in the background, the browser can also send pop-up messages.

✍**Note:**

When you use it, you need to set up your computer to receive the app notifications.



After then, by clicking the alert button  , you can view the List of unread messages.



4. System Message

According to the types of events generated by each module, such as the success and approval of the Visitor module reservation, the Office module meeting room repair report, the meeting room reservation, etc., the message status and detailed list will be sent to the corresponding system personnel so that the user can log in and view the message.

4.1. Message notification Bar

Function Description

Each event generated by the system is sent to the corresponding handler, and the handler can click the message button after logging in (the messages in the notification bar are all unread messages) for processing. The number of messages of the message button (Bell) The overlay of messages that the current user has not completed processing.

Preconditions for Normal Use of Function

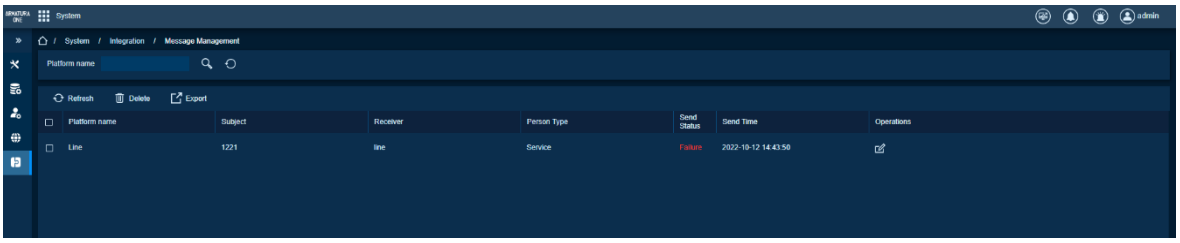
The current login account has permission to operate the notification bar.

Function Usage Scenarios

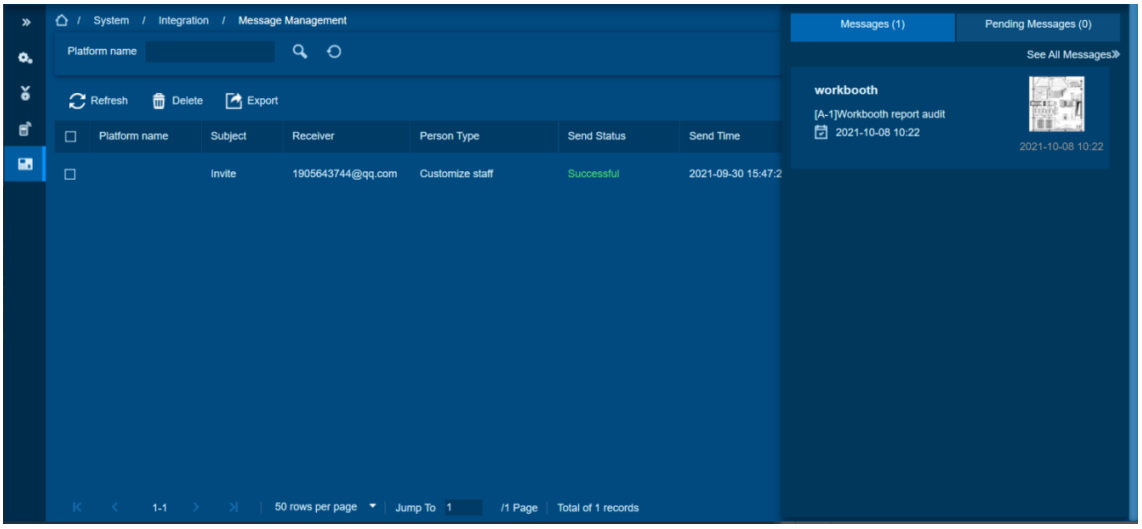
Users need to view messages or process certain messages to advance the progress.

Steps:

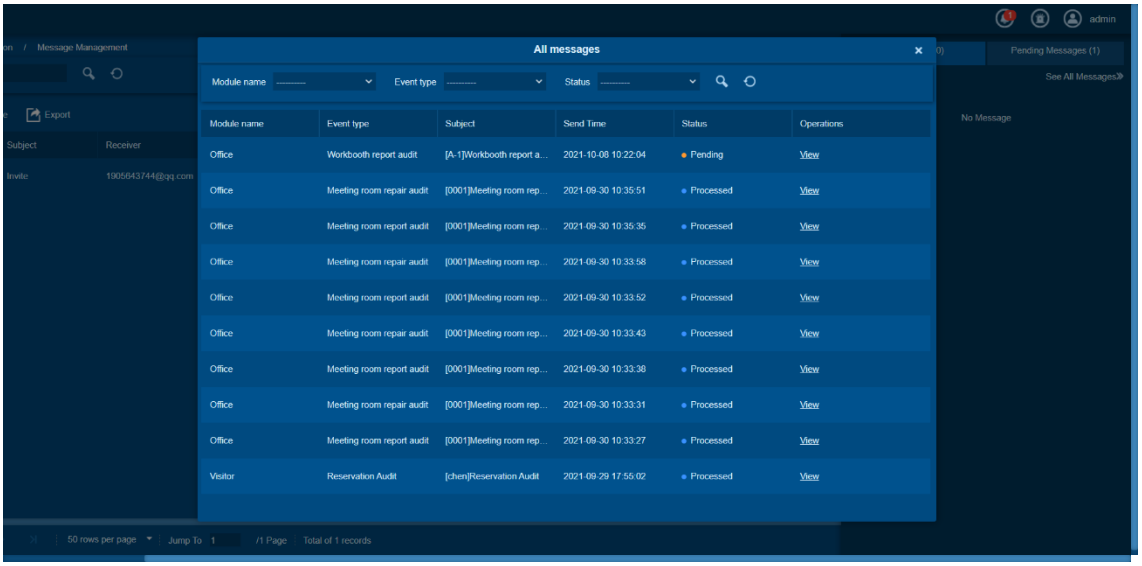
1. The total number of unread and pending messages will be displayed at the upper right corner.



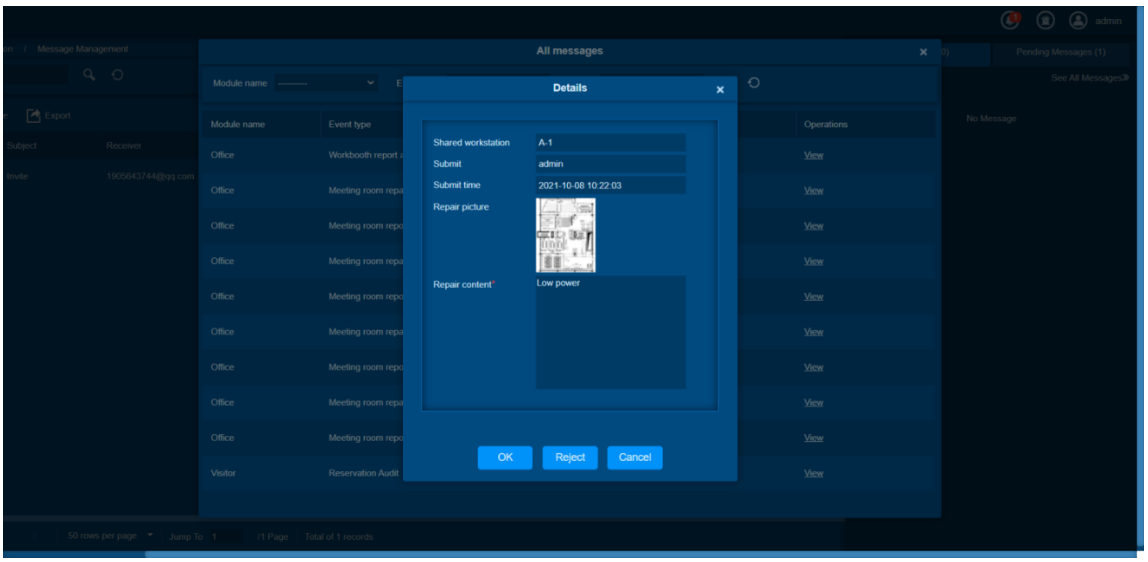
2. Click on the Icon will display the message bar, the left side of the message bar is the unread message, and the right side is the read message that need to be processed.



3. Click the [**See all messages**] to check all history messages.



4. In history, click [**View**] to check the message details.



4.2. Messages Management

Function Description

It Integrate messages sent by third-party messaging platforms.

Delete

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

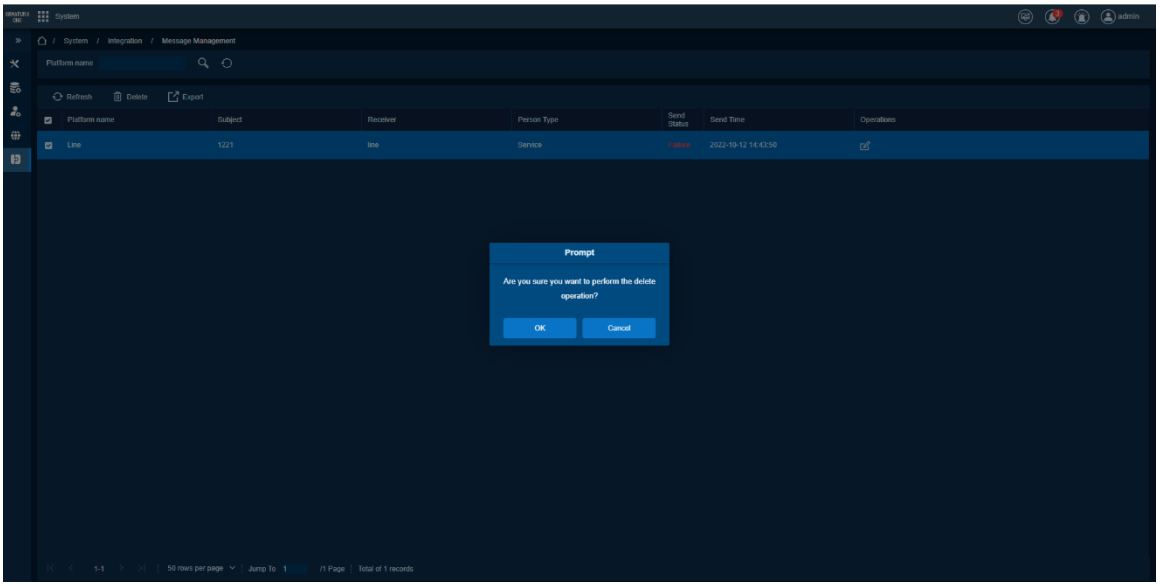
Delete unnecessary or expired data.

Feature Trigger Result

Delete the checked data.

Steps:

1. Check the information that needs to be deleted.
2. Click [**Delete**] button, and a prompt box will pop up.



3. Click [**OK**] button in the prompt box to complete the Delete operation.

Export

Preconditions for Normal Use of Function

The administrator has the export function authority, and there is data in the list.

Function Usage Scenarios

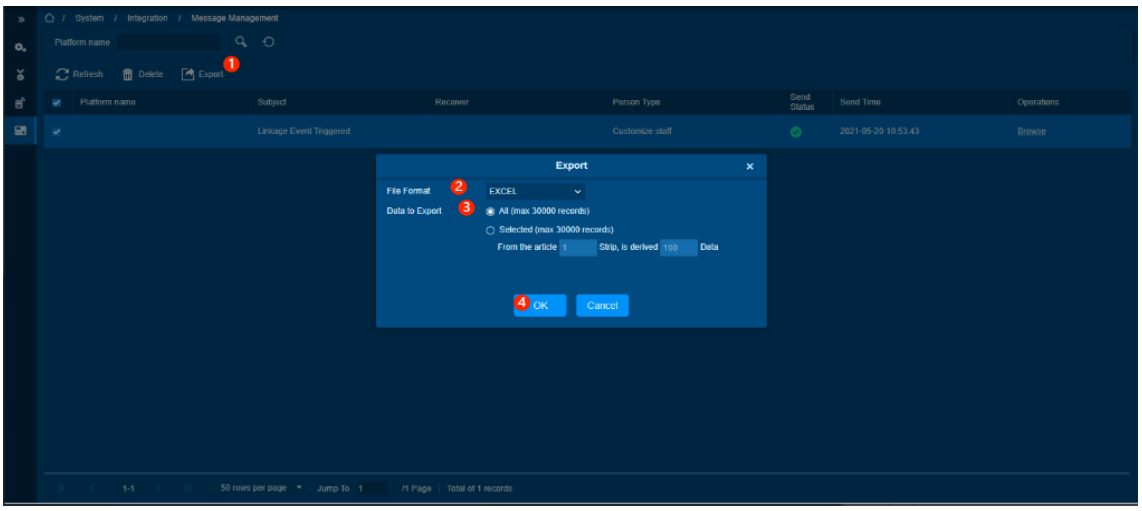
Export the information on the software to the computer.

Feature Trigger Result

Operations	Description
Select Excel	Export the message to EXCEL format
Select PDF	Export the message to PDF format
Select CSV	Export the message to CSV format
Select All Data	Export all data of the message
Select the Amount of Data Export	Export partial data of the message

Steps:

1. Click [**Export**] button to pop up the Export box.
2. Select the file format that needs to export in the pop-up box.



3. Select the scope of export.
4. Click [**OK**] button to complete the Export operation.

4.3. System Message

Function Description

It stores all system messages.

Export

Preconditions for Normal Use of Function

The administrator has the export function authority, and there is data in the list.

Function Usage Scenarios

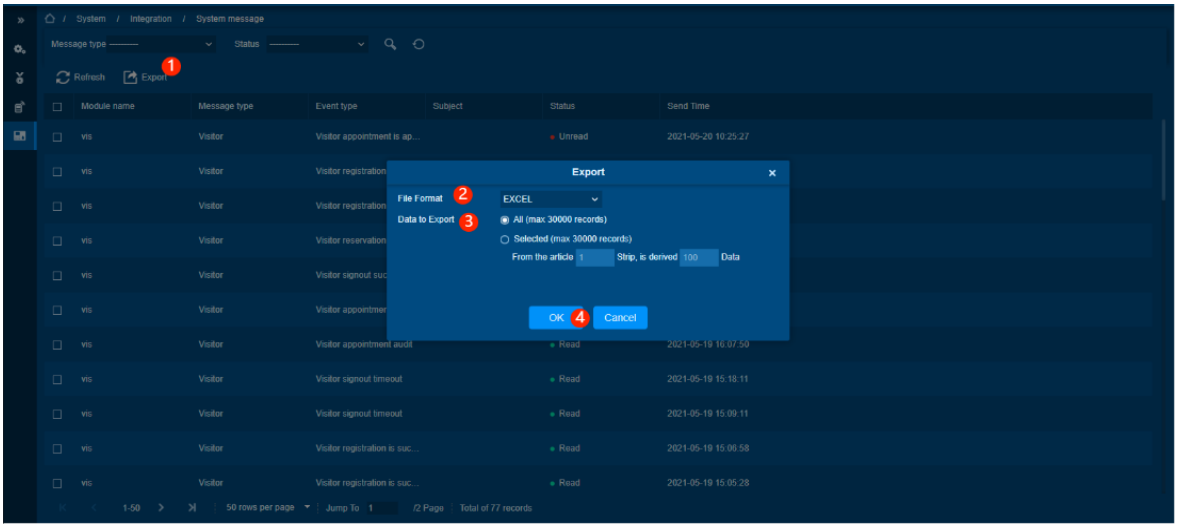
Export the data on the software to the computer.

Feature Trigger Result

Operations	Description
Select Excel	Convert system message export to EXCEL format
Select PDF	Convert system message export to PDF format
Select CSV	Convert system message export to CSV format
Select All Data	Export all data of system message
Select the Amount of Data Export	Export partial data of system message

Steps:

1. Click [**Export**] button to pop up the Export box.
2. Select the file format that needs to export in the pop-up box.



3. Select the scope of export.
4. Click [**OK**] button to complete the Export operation.

5. Personnel Management

Personnel system includes these modules: Personnel, Department, Position, Dismissed Personnel, Temporary Personnel, Custom Attributes, Parameters, Disabled, Face Template Extraction, Personnel Push Log, Card, Wiegand Format, and Issued Card Record.

Module Function List

Functions	Descriptions
Personnel	Enter basic data such as adding, deleting, editing, searching, leaving, synchronization, importing and exporting of personnel.
Department	Enter basic data such as adding, editing, viewing, deleting, importing, and exporting of departments.
Position	Enter basic data such as adding, editing, viewing, deleting, importing, and exporting of positions
Dismissed Personnel	View the information of resigned personnel and perform operations such as restoration of resigned personnel.
Temporary Personnel	View and review temporary personnel.
Custom Attributes	Supports custom staff attributes and staff information in a detailed manner.
Parameters	Set personnel management parameters and choose more appropriate operation method.
Disabled	View and manage banned list member information.
Face Template Extraction	Record the logs of face templates extraction.
Personnel Push Log	Record the log pushed to the VCM by the recorder.
Card	View all issued personnel cards and perform card loss reporting operations.
Wiegand Format	View and manage software Wiegand format, adding, editing, deleting, viewing your Wiegand card format.

Issued Card Record	It includes the information of Issue Card, Reported Lost Card, Reactivate Lost Card, Write Management Card, Write Card, Card Returned, and Card Change.

5.1. Personnel

Function Usage Scenarios

Create new personnel for the system, edit the personnel information, and adjust the organizational structure and authority of the personnel.

Feature Trigger Result

Operation	Description
Check SMS Notification	**Scenario 1:** If “Please add SMS notification platform” is prompted, it indicates that you have not configured the SMS sending platform. For this, please go to the System-Integration module to configure it, and then check. **Scenario 2:** After checking, when this person triggers an Access Control Event or Elevator Control Event, the event notification will be sent to the registered mobile phone number via SMS.
Check The Email Information	**Scenario 1:** The pop-up window is used to set the mailbox parameters. For configuring your sending mailbox, please enter the parameters and then check. **Scenario 2**: After checking, when this person triggers an Access Control Event or Elevator Control Event, the event notification will be sent to registered email account via SMS.
Controller Issuance	Select the reader of the controller through the pop-up window. After selecting, swipe the card you will send to this person to the corresponding reader, and the system will automatically fill up the card number in the text box.
Biological Template-Fingerprint	Enter the Fingerprint Registration interface through the pop-up window. You can select the appropriate finger to register. Before that, connect the corresponding Fingerprint Collector / Access Control all-in-one to the system and select these devices for fingerprint collection and registration.
Biological Template-Finger Vein	Enter the Finger Vein Registration interface through the pop-up window. You can select the appropriate finger to register. Before that, connect the corresponding Finger Vein Collector

	or Access Control Integrated Machine to the system and select these devices for finger vein collection and registration.
Person Avatar-Browse	Click **Browse** to upload the picture on the local computer as a person's profile picture.
Person Avatar-Snapshot	Click **Capture** to enter the interface of real-time capture of people avatars. Before this, please make sure that you are using a USB camera device and the device is properly connected to the server. Some browsers (such as Chrome) require Authorization when calling the camera device, and you need to click **Allow**.
Access Control Settings-Permission Group Check	Add personnel to the selected Access Levels. When the Access Levels has device, the personnel information will be sent to the corresponding module device.
Access Control Settings-Personnel Database Check	Push personnel information to the selected personnel list database. Before that, you need to connect to the and create a personnel database.
Access Control Settings-Super User	The super user is not restricted by the access control rules and has a very high level of authority to open the door.
Access Control Settings-Extended Access	For disabled person, opening time of the device can be extended.
Access Control Setting-Banned List	The access verification authority of the banned persons is prohibited.
Set Access Control Setting-Effective Time	Set the effective period for the person's access control authority. After this time, this person will permanently lose his access control authority, so it is suitable for temporary personnel.
Attendance Settings-Check Attendance Area	Set the attendance area for the person.
Elevator Control Settings-Check the Elevator Control Permission Group	Set the Elevator level for the person.

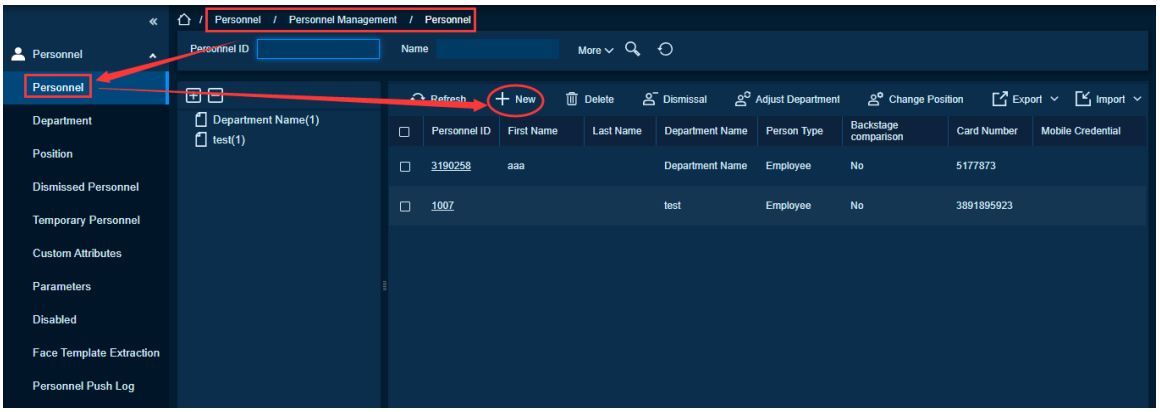
License Plate Registration-License Plate Number	Set the license plate information of this person. Click **Add** button to add a new group of license plate numbers for this person. One person can have up to 6 license plates.
FaceKiosk Settings-FaceKiosk Area	After setting the FaceKiosk attendance, check this option to assign the area of the FaceKiosk attendance to this person.
Detailed Information	Detailed Information is a supplementary record of personnel information.

5.1.1. Personnel

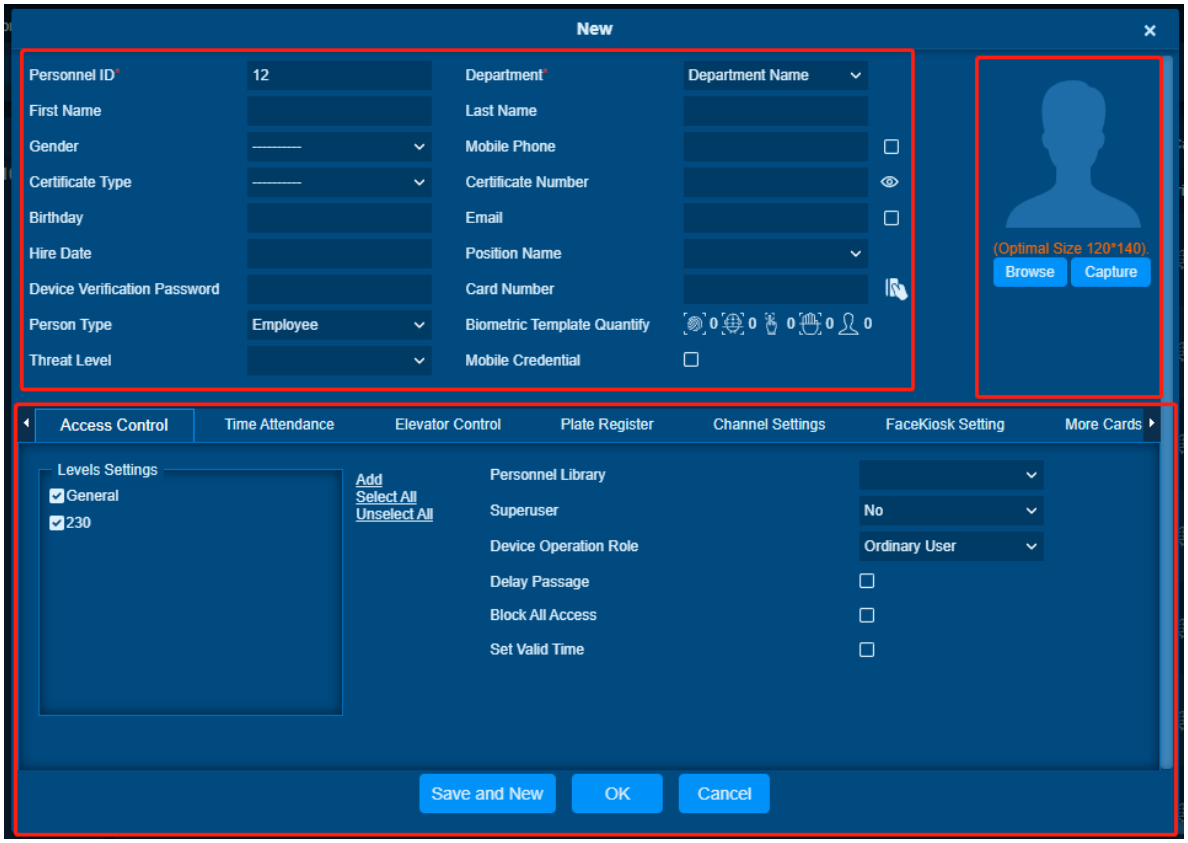
When using this management program, the user shall register personnel in the system, or import personnel information from other software or documents into this system. For details, see Common Operations. The main functions of Personnel Management include Add, Edit, Delete, Export, and Import personnel, and Adjust Department.

Add Personnel

1. Click **[Personnel]** > **[Personnel Management]** > **[Personnel]** > **[New]**.



2. On the New interface, enter Personnel ID, Department, First Name, Last Name, and the other details displaying in the below image.
3. For Personal Permission Settings, click **[Access Control],** select General and select the value for Personnel Library, Superuser, Device Operation Rule, Delay Passage, Disable and Set Valid Time.
4. Click **[OK]** and save the settings.



The fields description are as follows:

Personal Photo: The image preview function is provided. It supports common picture formats, such as **JPG**, **JPEG**, **BMP**, **PNG**, GIF, etc. The best size is 120×140 pixels

- **Browse:** Click **[Browse]** to select a local photo to upload.
- **Capture:** Taking photo by camera is allowed when the server relates to a camera.

Personnel ID: Personnel ID may consist of up to 9 characters, within the range of 1 to 79999999. It can be set based on actual conditions.

✍**Note:**

- When configuring personnel ID, check whether the current device supports the maximum length of characters and whether the letters can be used in personnel ID.
- To edit the settings of the maximum number of characters of each personnel ID and to check whether letters can also be used, click **[Personnel]**> **[Parameters].**

Department: Select from the pull-down menu and click **[OK]**. If the department was not set previously, then only one Department Name **[Company Name]** will appear.

First Name/Last Name: The maximum number of characters are 50.

Gender: Set the gender of personnel.

Mobile Phone: The maximum length is 20, and this is an optional field.

Certificate Type: There are four types of certificates i.e., ID, Passport, Driver License and Others.

Certificate Number: Enter the Certificate Number that matches the Certificate Type.

Birthday: Enter employee's actual birthday.

Email: Set the available email address of the personnel. The maximum length is 30. Punctuations, namely, the "-"," _" and"." are supported. If the Event Notification box is checked, the Email is required.

E-mail Notification: After this field is selected, the system will send an Email to the relevant person once an access or an elevator event occurs. If the Email Server is not set, a settings window will pop up if this field is checked. Please refer **E-mail Management** for the setting information.

Hire Date: It is the date on which the personnel are appointed. Click to select the date.

Position: It is the designation of the personnel.

Device Verification Password: Password used to verify on reader

Card number: The maximum length is 10, and it should not be repeated. Click  ton to read the card number directly from the reader.

Person Type: Set Person Type as Employee or Visitor.

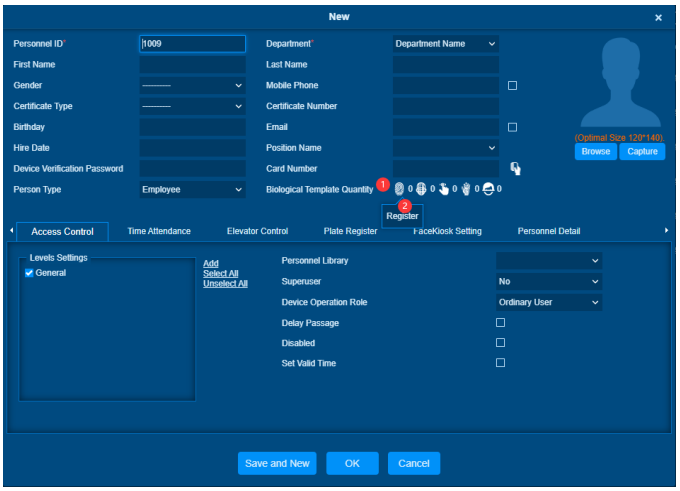
Biometric Template Quantity: Calculate the amount of different credential

✍**Note:**

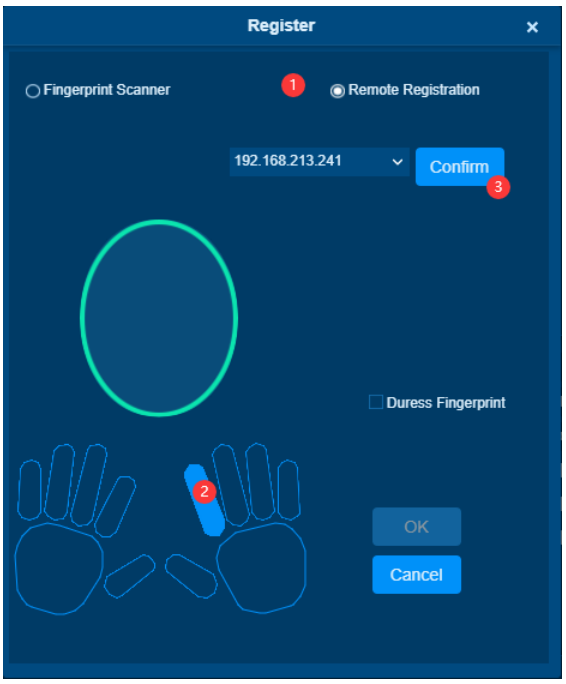
Register Fingerprint/Finger Vein: Enroll the Personnel Fingerprint, Finger Vein, or Duress Fingerprint. The duress fingerprint is used to trigger the alarm and send the signal to the system in case of emergency.

How to register fingerprint:

1) Move the cursor to the fingerprint icon position, a registration pop-up or drive download box will appear, click **[Register]**.

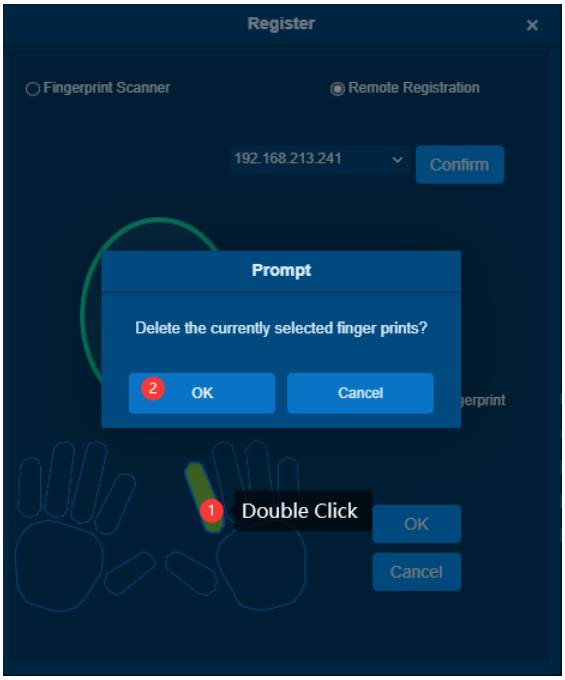


2) Click **Fingerprint Scanner** if using fingerprint reader otherwise click **Remote Registration** for remote device.



3) Select a finger, press on the sensor by three times. Once fingerprint is registered, "**Fingerprint registered successfully**" message will appear on the screen.

4) Click **[OK]** to complete registration.



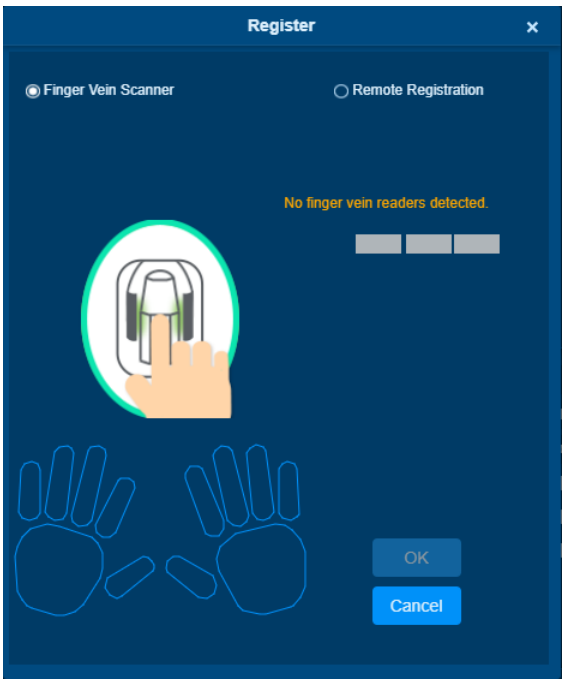
5) If you want to delete fingerprint, double click the fingerprint to delete. If you need to register a duress fingerprint, please check the **Duress Fingerprint** option.

✍**Note:**

- If the fingerprints are duplicate, "Don't repeat the fingerprint entry" will be prompted.

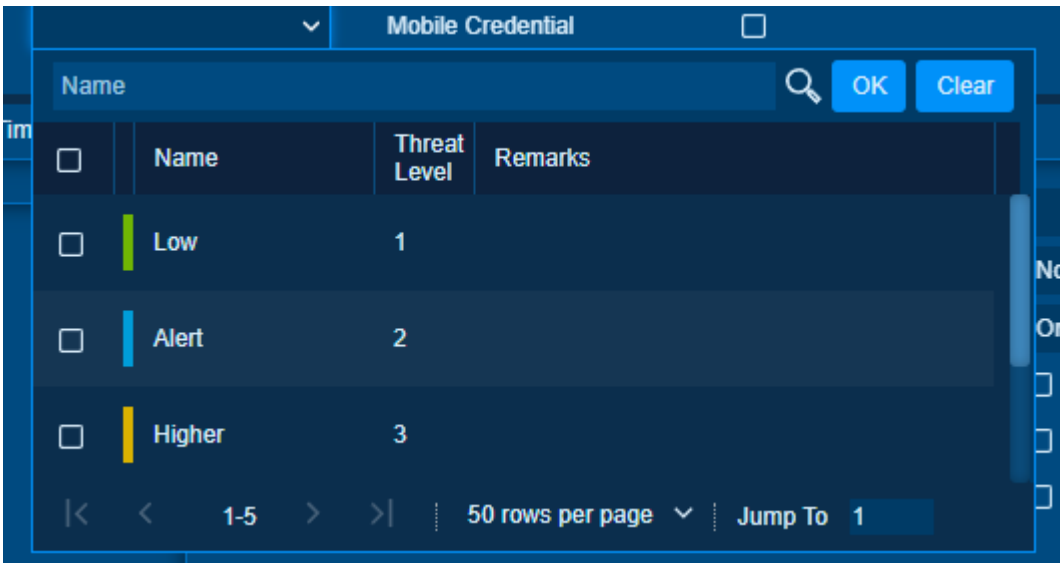
- If the fingerprint sensor driver is not installed, click **"Install driver"** and the system will prompt to download and install driver.
- After installing the fingerprint sensor driver, if the fingerprint register button is grey in IE browser while it is normal in other browsers (such as Firefox, Google), you can change the settings of IE browser, as per the following:

1. In IE browser, click **[Tools]** > **[Internet Options]** > **[Security]** > **[Credible Sites]**, add http://localhost to the credible sites, then restart the IE browser.
2. In IE browser, click **[Tools]** > **[Internet Options]** > **[Advanced]** > **[Reset]** to open the Reset Internet Explorer Settings. Click **[Reset]** to confirm; then restart the IE browser (you may try when Point 1 does not help).
3. If all the above settings do not work, please execute following operations (take IE11 browser as an example): click **[Tools]** > **[Internet Options]** > **[Advanced]** > **[Security]**. Select the option **[Allow software to run or install even if the signature is ...]**, and deselect **[Check for server certificate revocation]**, then restart IE.
4. The system supports access from the Live20R fingerprint device and fake fingerprint prevention function.



Personnel Threat Level

Set a threat level for personnel, if system threat level change, system will check whether Person is the same threat level with current system threat level, if personnel do not include current threat level, this person will be limit for access.



Related function check Threat Level.

Mobile Credential

Armatura Credential Management System
(Referred to as 'ACMS') is an online system where company admin manages employee's mobile credential.

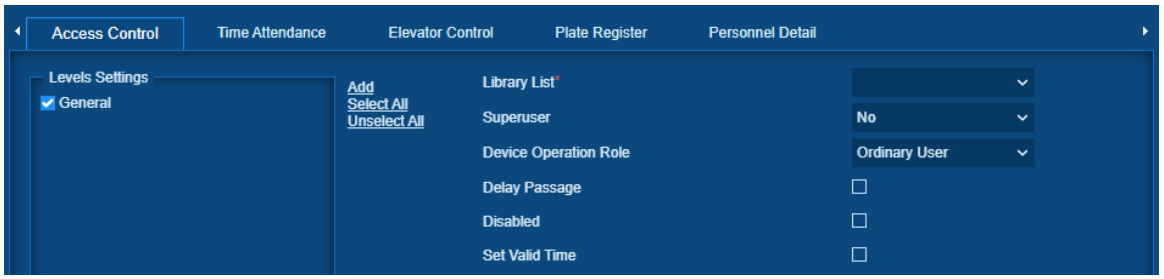
If checkbox is selected, will add a **Mobile Credential** tab in below part.

✍**Note:**

Before enabling this function, need to se**t [System] -> [Integration] ->[Platform Connections]**, set ACMS connection, check Platform Connection

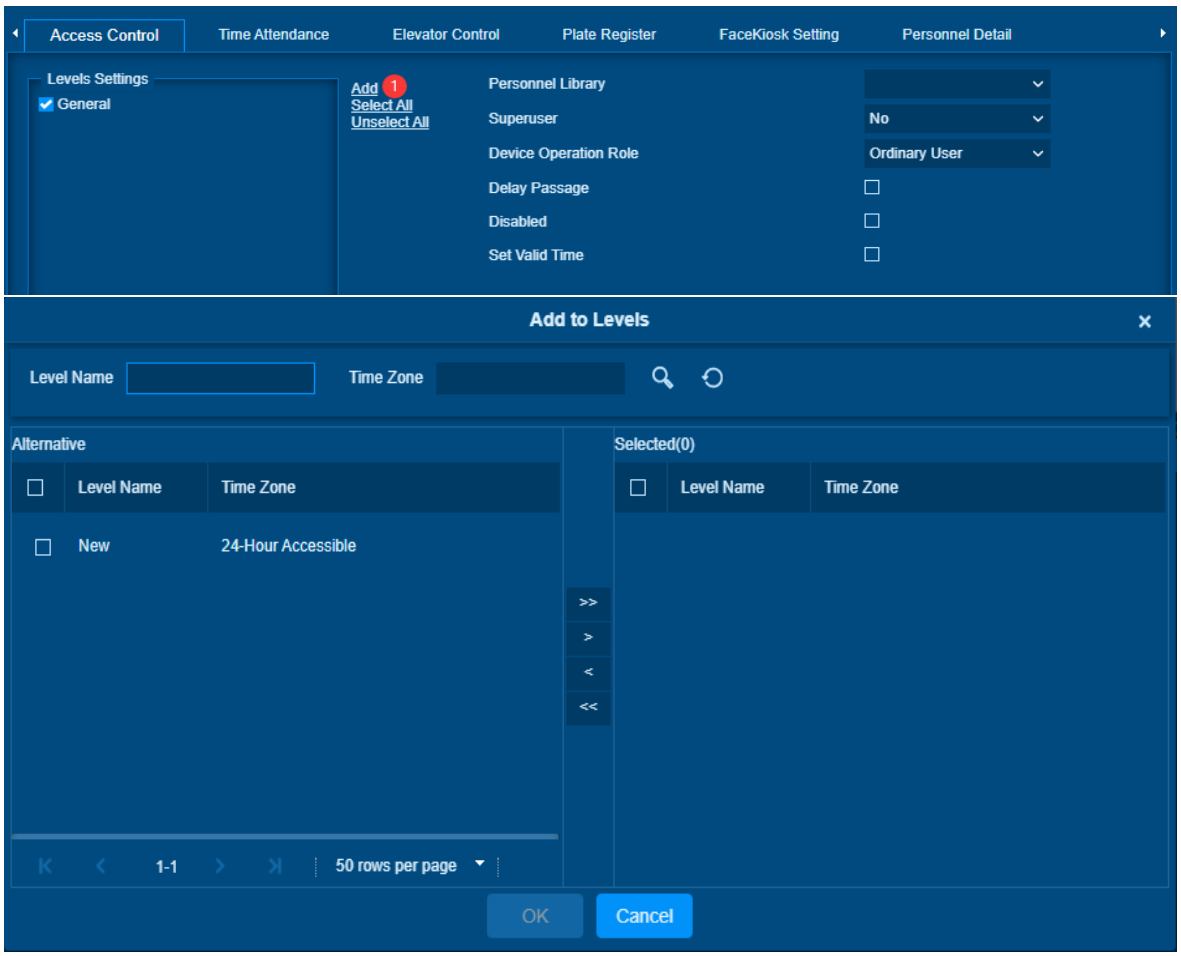
Access Control

Set the Access Control parameters for the personnel by clicking on [**Access Control**].



The fields are as follows:

Level Settings: Click **[Add],** then set passage rules of special positions in different time zones.



Library List: Use this feature to push the person to the appropriate list database for functions such as Personnel Alert, Background Comparison Verification.

Superuser: In access controller device, a superuser is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door-opening priority.

Device Operation Role: Set user permission for standalone terminal, can select Ordinary User/ Administrator/ Enroller.

Delay Passage: Extend the waiting time for the personnel through the access points. Suitable for physically challenged or people with other disabilities.

Disabled: When person is disable, this person will not allow to verify on the system.

Set Valid Time: Set temporary access level. if not set, it indicates person get permanent access.

✍**Note:**

The system will automatically search for the relevant numbers in the departure library during verification.

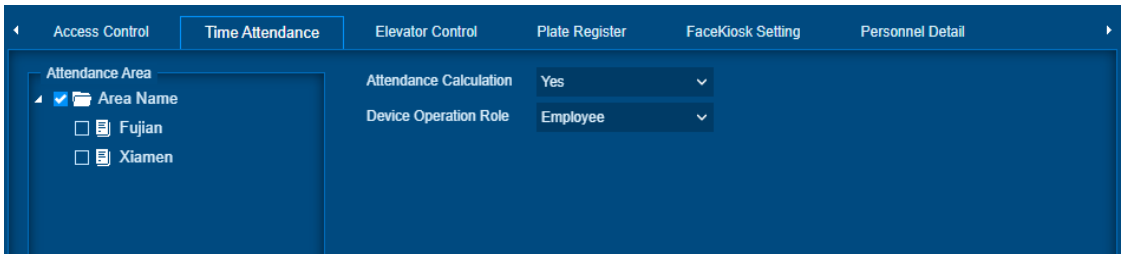
The Personnel Information List, by default, is displayed as a table. If Graphic Display is selected, photos and numbers will be shown. Place the cursor on a photo to view details about the personnel.

✍**Note:**

- Not all devices support the “Disabled” function. When a user adds a device, the system will notify the user whether the current device supports this function. If the user needs to use this function, please upgrade the device.
- Not all the devices support the “Set Valid Time” function of setting the hour, minute, and second. Some devices only allow users to set the year, month, and day. When a user adds a device, the system will notify the user whether the current device supports this function. If the user needs to use this function, please upgrade the device.
- Personnel Background Comparison Verification is supported in the Video module to create lists in the personnel library.

Time Attendance

Set the Time Attendance parameters for the personnel by clicking on **[Time Attendance].**



The fields are as follows:

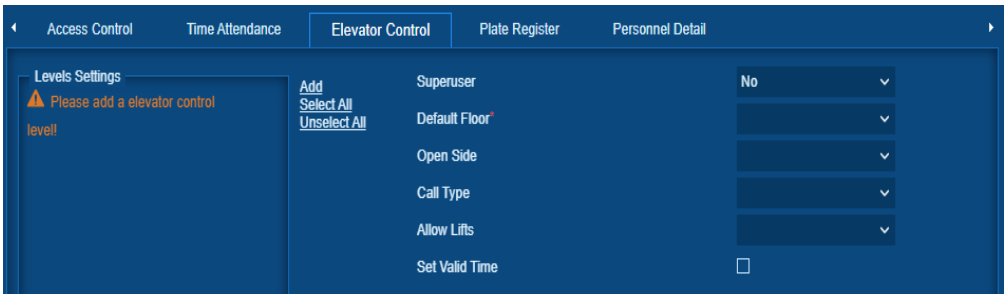
Attendance Area: Set the staff attendance area.

Attendance Calculation: Set if the attendance needs to be calculated or not. Select **[Yes]** for calculating attendance. Select **[No]** to not calculate the attendance.

Device Operation Role: It will set the authority for operating the device and send it to the corresponding device.

Elevator Control

Set the Elevator Control parameters by clicking on **[Elevator Control].**



The fields are as follows:

Superuser: In elevator controller device, a superuser is not restricted by the regulations on time zones, holidays and has extremely high elevator access priority.

Default Floor: Set the default floor that people use for check-ins. Select only one default floor per building.

Open Side: Set up front and back door switches for elevators when arriving at the default floor. There are three modes: Front Door Open, Back Door Open, Both Door Open.

Call Type: Set the Call Type. The corresponding call type can be selected according to the elevator control device connected to each building.

Elevator Type	Type of Call
Kone	Normal Call
	Handicapped Call
	Priority Call
	Empty Car Call
	Space Allocation Call
Mitsubishi	General
	Handicapped Person
	VIP
Hitachi	General
	Handicapped Person
	VIP

Allowed Elevator: Set the elevator which are allowed to use.

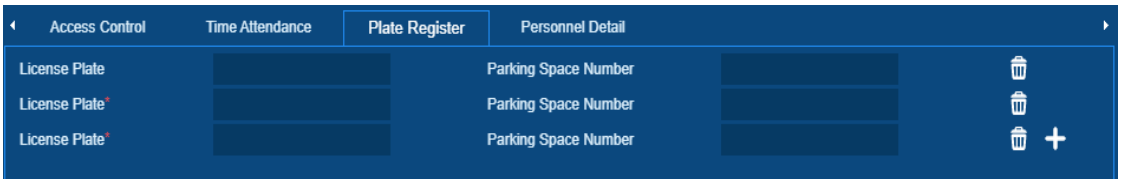
Set Valid Time: Set Temporary Elevator Level. Floor buttons can be set to be pressed only within the time periods. If it is not checked, the time to press the floor button is always active.

✍**Note:**

The Elevator level must be set in advance.

License Plate Registration

Register the license plate numbers for personnel by clicking **[Plate Register]**.



The fields are as follows:

License Plate: The user needs to register the license plate.

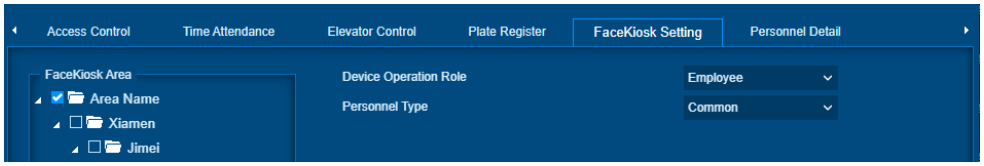
Parking Space: Parking space corresponding to the vehicle.

✍**Note:**

Each personnel may register a maximum of 6 license plates.

FaceKiosk Setting

For FaceKiosk registration, click **[FaceKiosk Setting]**.



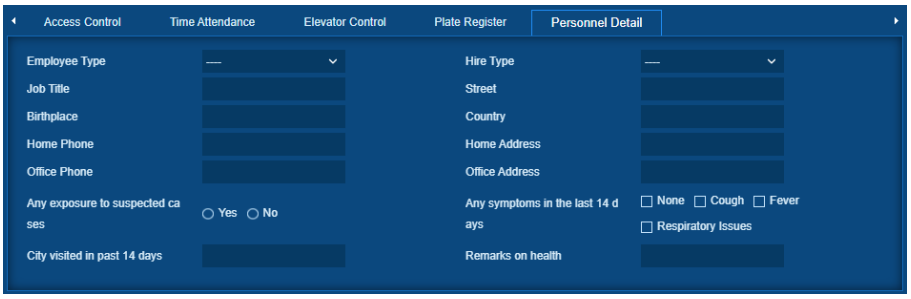
The fields are as follows:

Device Operation Role: Set personnel's device operation authority

Personnel Type: Set the Personnel Type as Ordinary or Block List or VIP.

Personnel Detail

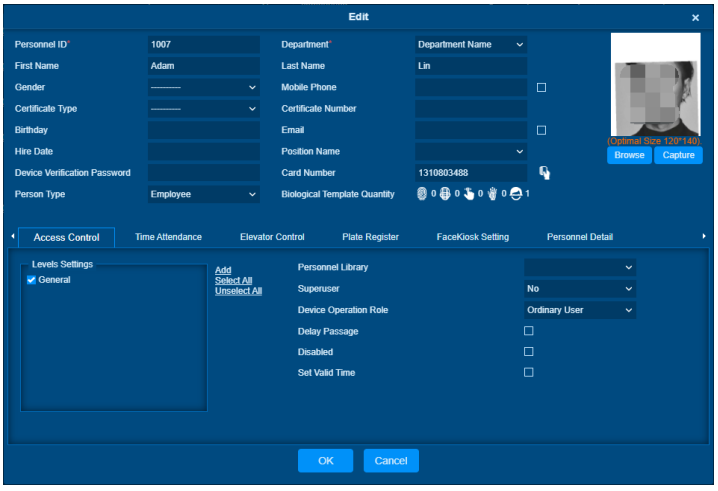
- Click **[Personnel Detail]** to enter the personal details of the user.



After entering the information, click **[OK]** to save and exit.

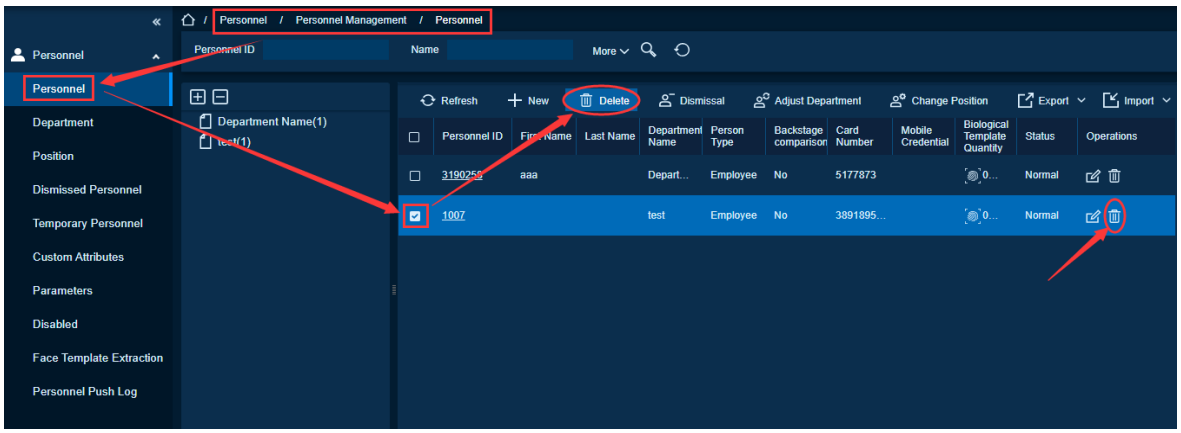
Edit Personnel

- Click **[Personnel]** > **[Person]**. Then select the desired person and click **[Edit]**.

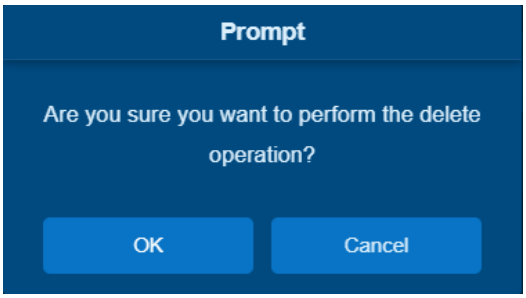


Delete Personnel

- Click **[Personnel Management]** > **[Personnel]**, then select the person.



- Click [**Delete**] > **[OK]** to delete.

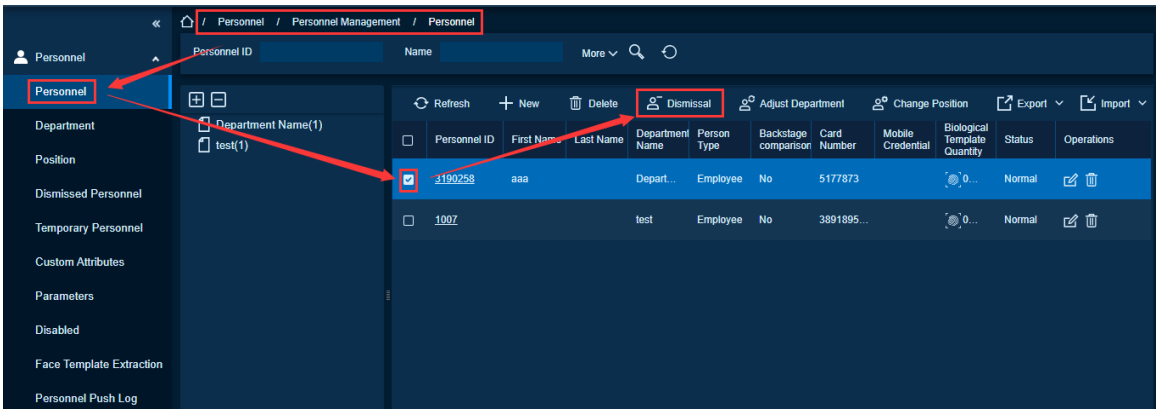


✍**Note:**

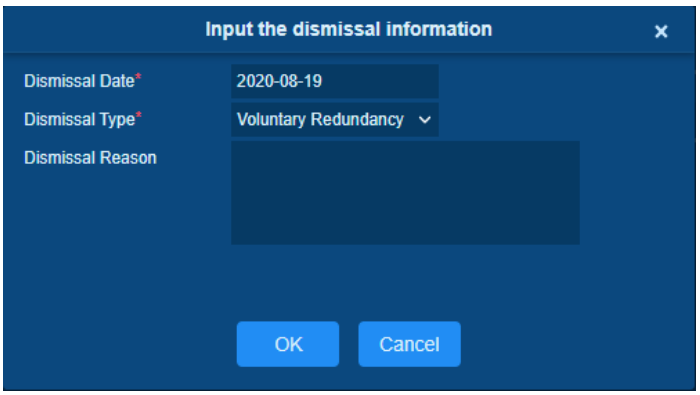
All relevant information about the person will delete.

Dismissal

- Click **[Personnel Management]** > **[Personnel]**. Then select the desired person and click **[Dismissal]**.

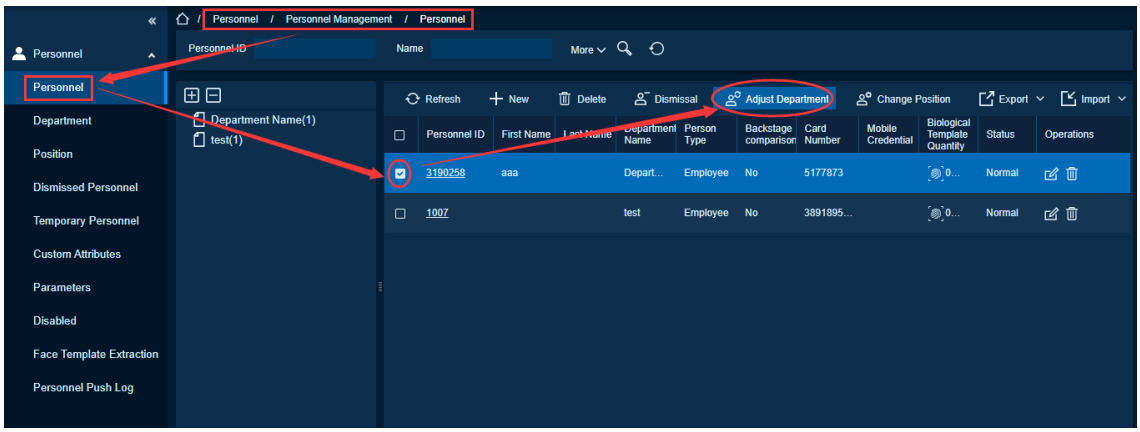


- Select the date, type, and write a reason and click **[OK]**.

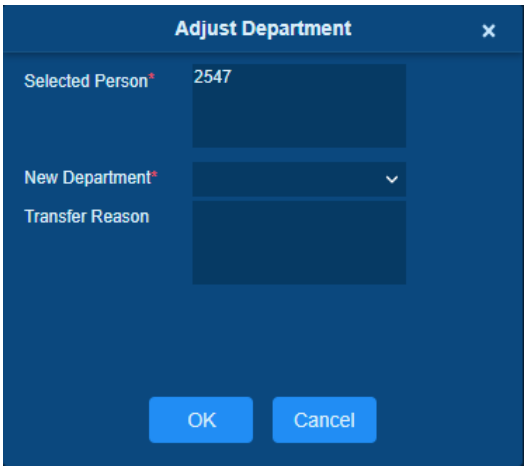


Adjust Department

1) Click **[Personnel Management]** > **[Personnel]**. Then select the desired person, and click **[Adjust Department]**:



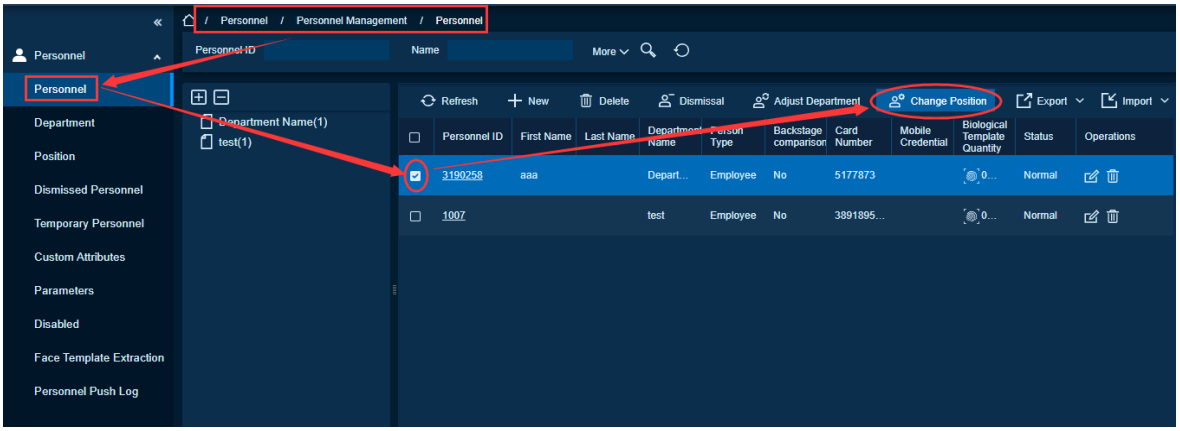
2) On the Adjust Department interface, enter the Selected Person, New Department and Transfer Reason.



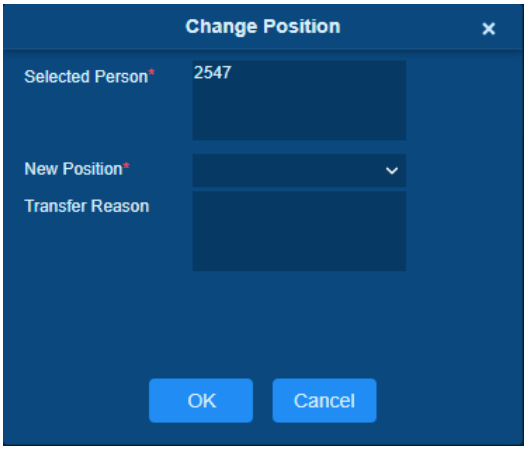
3) Click **[OK]** to save and exit.

Change Position

- Click **[Personnel Management]** > **[Personnel]**. Then select the desired person and click **[Change Position]**.



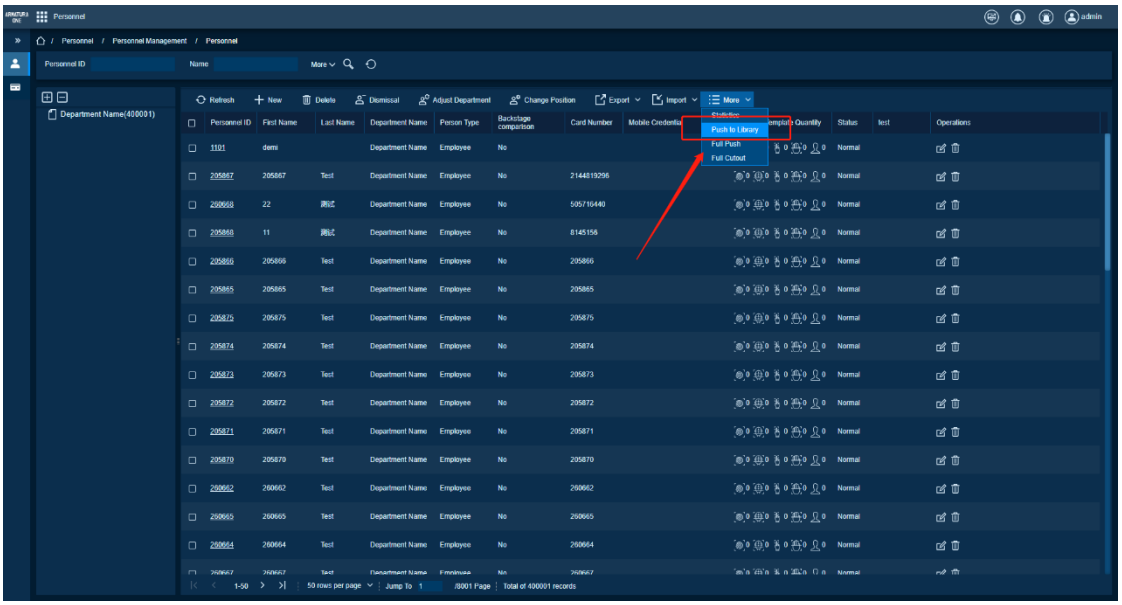
- On the Change Position interface, enter Selected Person, New Position and Transfer Reason.



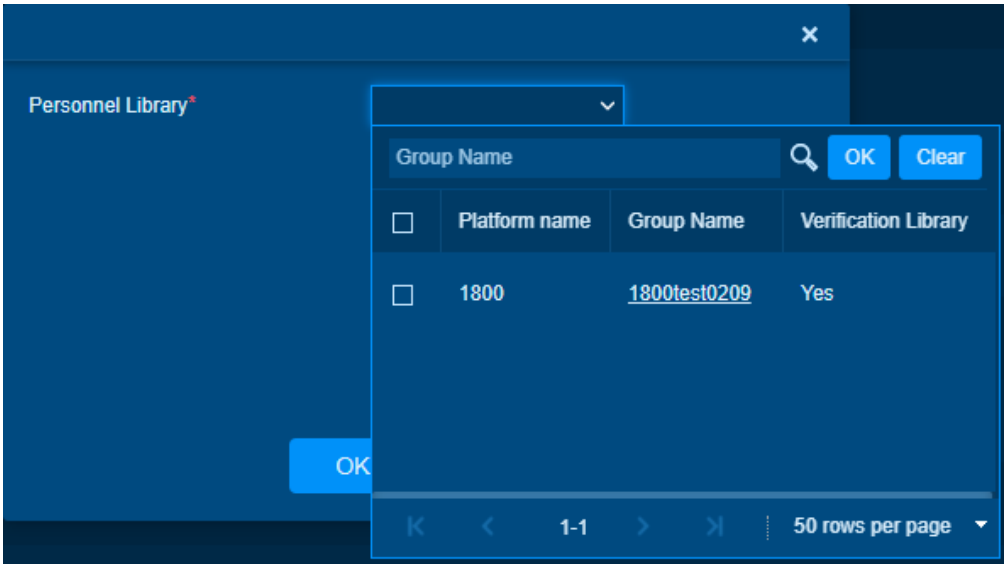
- Click **[OK]** to save and exit.

Push to Library

1) Click **[Personnel Management]** > **[Personnel]**. Then select the desired person and click **[Push to Library]**.



2) Select the Group and click **OK** to save the changes.



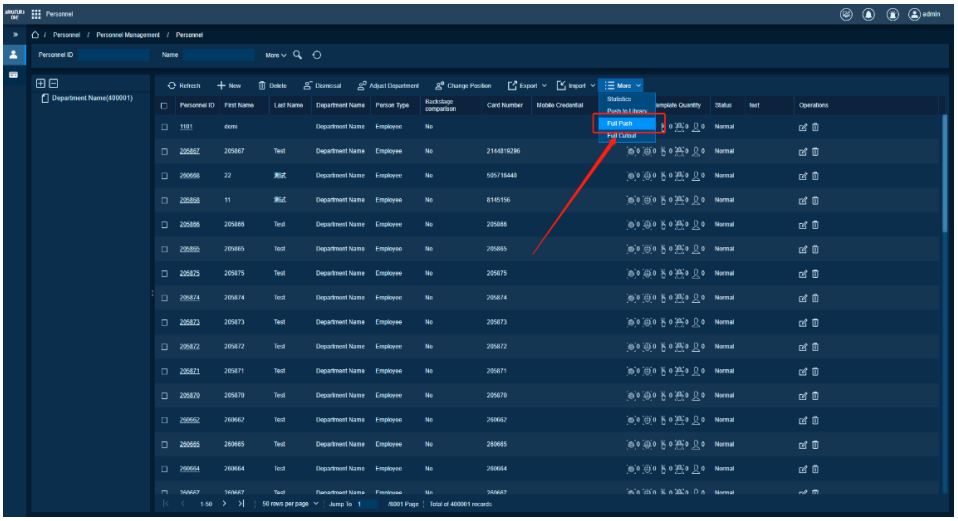
3) After the process ends, the selected personnel will save in selecting Tags library.

4) People who are pushed to the **Personnel Library** will support Personnel Alert or Background Verification function.

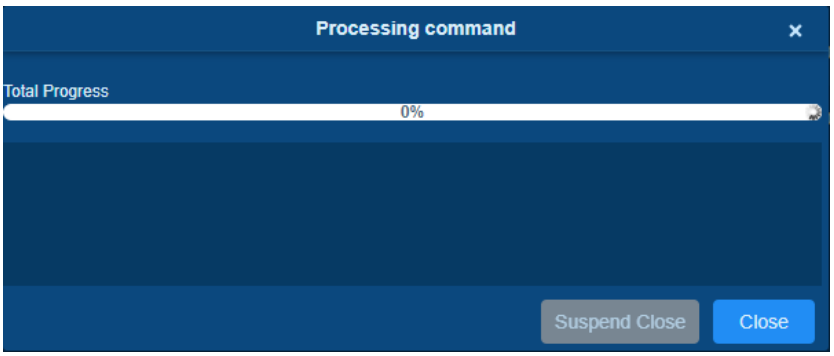
5) Click **[OK]** to save and exit.

Full Push

- Click **[Personnel Management]** > **[Personnel]**, then click **[Full Push]**.



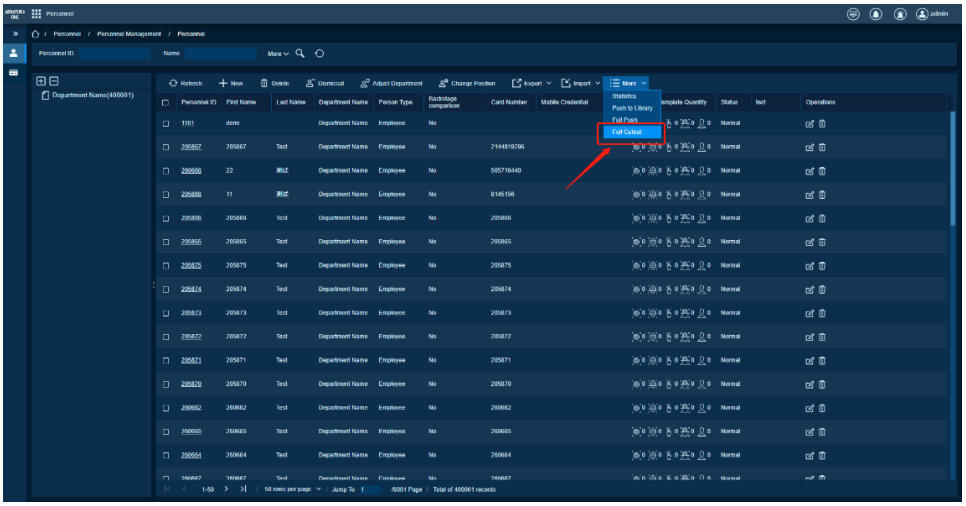
- Wait until process completes.



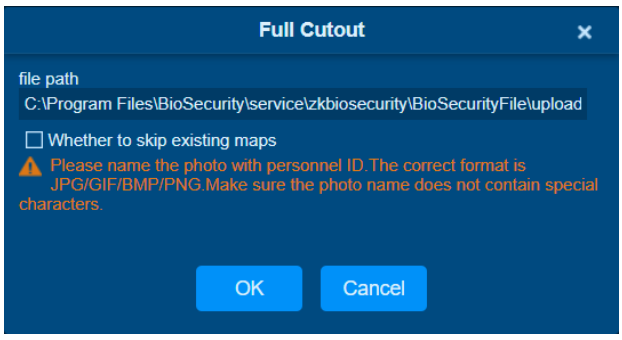
- After the process ends, all staff will push to the library.
- Click **[Close]** to save and exit.

Full Cutout

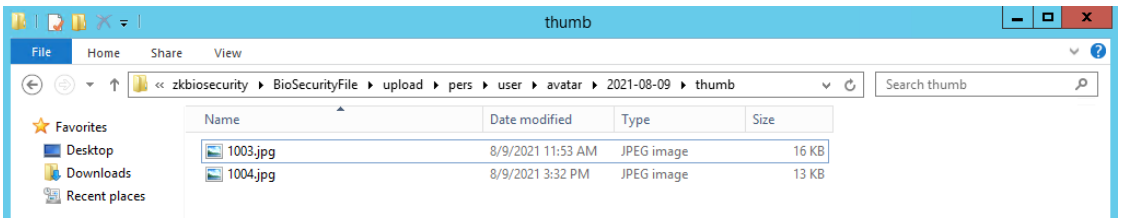
- Click **[Personnel Management]** > **[Personnel]**, then select a person, and click **[Full Cutout]**.



- On the Full Cutout interface, enter the file path and click **OK.**



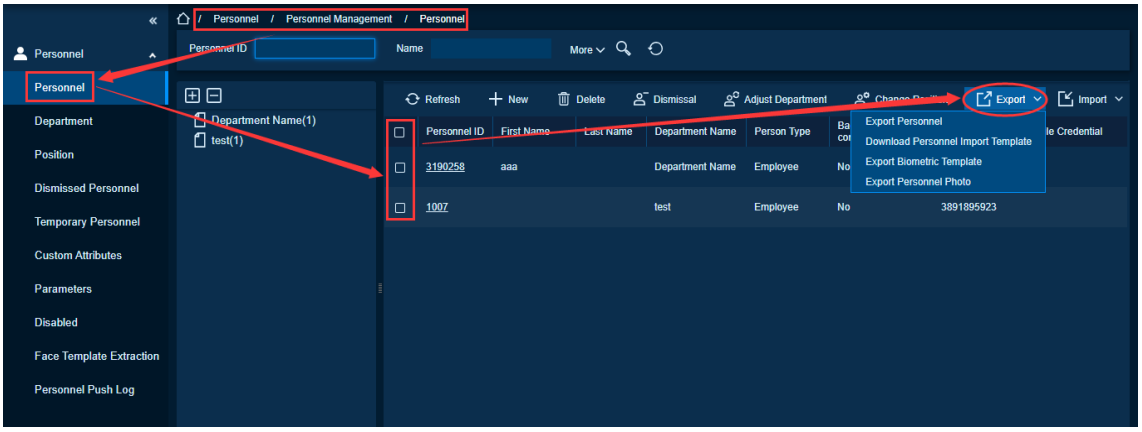
- Select whether to skip existing maps to create a new folder.
- After the process ends, all personnel photos will save in a local folder and named after the person ID.



- All photos will be encrypted and cannot be opened directly, which could be used for the next time you need to import people photos into the system.

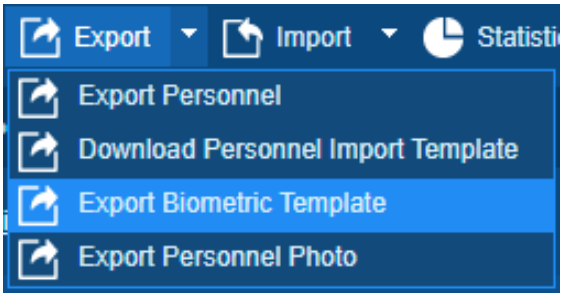
Export

- Click **[Personnel Management]**> **[Personnel]**> **[Export]** to export personnel information, personnel biometric templates.

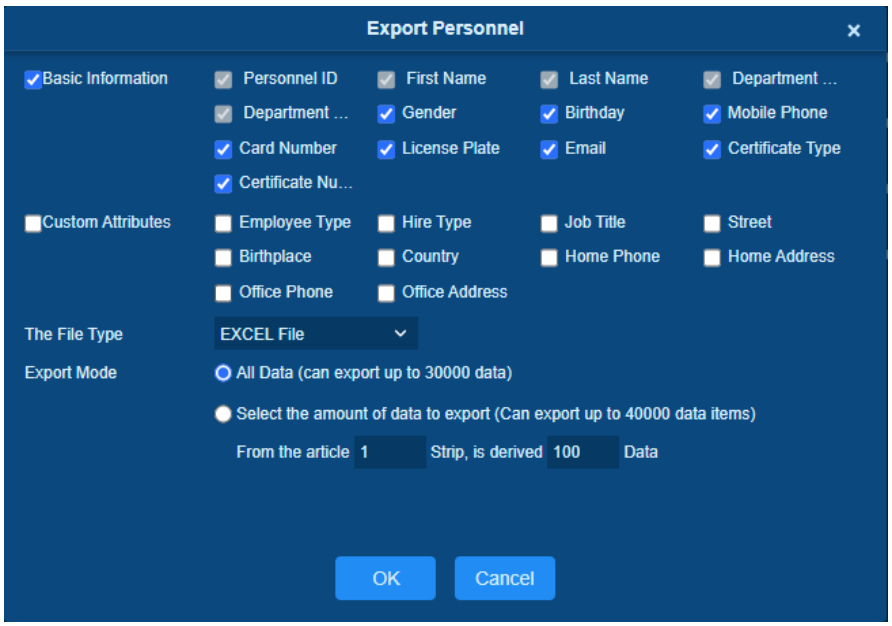


Export Personnel

Personnel's basic information will be exported. Select whether to export all data or a certain range.



On the Export Personnel interface, select personnel's basic information and custom attributes.



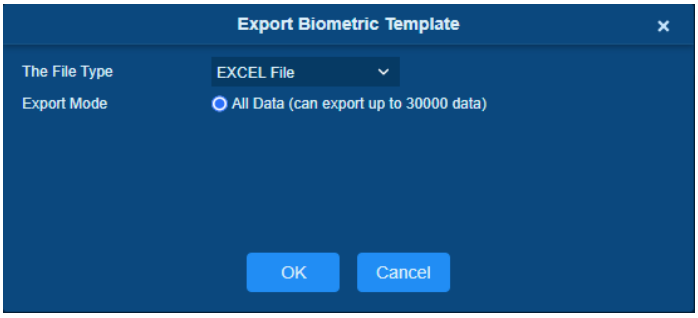
The selected basic information will look like this in xlsx format as shown in below image.

Person

Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Password	Certificate Type	Certificate Number	Card Number	Email	Reservation Code	Mobile Phone
1	Jerry	Wang	1	General	Male	1980-04-23	1	1	TP443566	4461253	abwe@qwe.com	123456	59496464
2	Lucky	Tan	3	Development Department	Female	1992-12-08	2	3	784515	6155266	778@abc.com	123456	4425521
2940	Sherry	Yang	hotel	Hotel	Female	1997-12-01	2940	1	741741	1411237	555@qq.com	123456	145145145
3	Leo	Hou	4	Financial Department	Male	1998-12-22	3	1	23687	13271770	3232@qq.com	123456	34342543
4	Berry	Cao	1	General	Female	2007-12-05	4	4	745688QQWA	13592341	QWA@zzz.com	123456	74755466
5	Necol	Ye	2	Marketing Department	Male	2017-01-10	5	1	32242311	13260079	3322@qq.com	123456	6645454
6	Amber	Lin	4	Financial Department	Female	2017-07-04	6	1	784525004	4628036	787878@eru.com	123456	44620545
7	Jacky	Xiang	1	General		2016-01-05	7	8	ees1213232	6323994	434@qq.com	123456	54243231
8	Glori	Liu	2	Marketing Department	Female	1995-12-05	8	1	433114354	6189166	987@abcd.com	123456	77545353
9	Lilian	Mei	3	Development Department	Female	1992-12-23	9	1	XS22030	9505930	8989@pp.com	123456	221112121

Export the Biometric Template

This option exports the registered biometric details of the users.

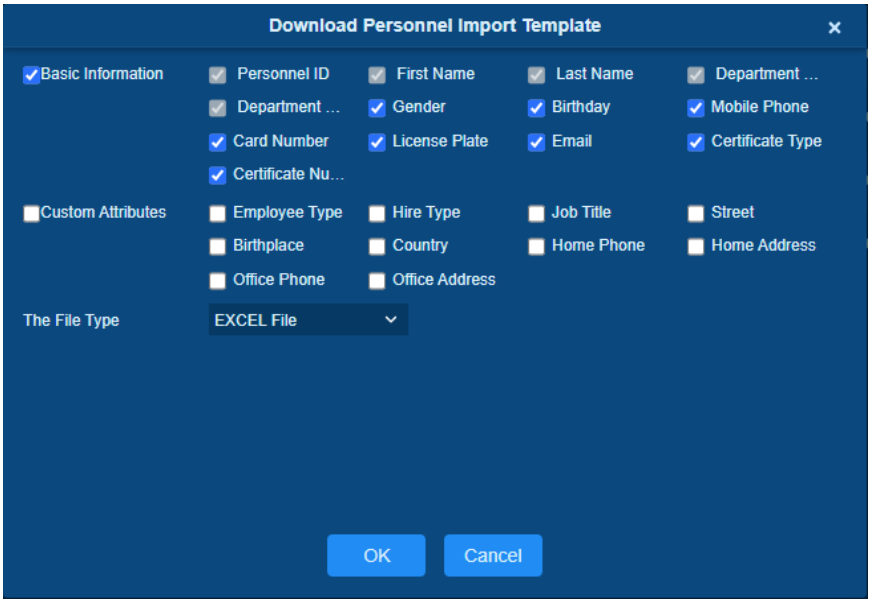


Personnel Biometric Template

Personnel ID	First Name	Last Name	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric Template
1	Jerry	Wang	1	Fingerprint	10	4	1	TExTUzkxAAAFDxEECAUHCc7QAAAdDmkBAAAAhDlvmg/fADwLvgANACkAyQCzAB4PFwD2DzoM1qACAX4H9A/gACgP5QBOABUE8QCHAI4LhACJD+MMNQCfAJ8MSQ8gAVgM0ACQAIMAAAEsAVoJpQAyD+4PKgA6ARwGtw8aAAEPkAB+AOMFjwDhAFILqACwD+QPrgCHANQP6g+5ACAPTAAXAFcAQQCpAN4MNwCDD5iL+wAQAYMFTw8eAVYM0wDyAdQA5gBdABMPiAA/DtUPDAD+ABQK7Q8wAI8IlACBAFsOlQDCAAQLuwCqD/QLagDjABoP3w/vAD4M5gAzADol9wCpAJkEBwBsDw8P8AASAfoEeA82AdMP9QDYAbsKNAADAc8PNgA1Ds8K9gBFAZ8MDA8FAcAK2ADiABYFvOzqOS4S7BK7/X7wtfZqAp6ENfF8gE39fYBofYhyrOrF78btpYdkc5954P1kg+v18DgB7//RXw4ellFyQVphs6KzHZQddf7nYzNnbwDDpyGS8+MPqgVLh4uMjKTd69/Oecw/SMBKRjqUGt1iP6v4KYBSgVe9XlNMjjmBqL6g3XjeBNvQYRlVx+PWQpghCr9tAtiHTgTQFlh9KJbwTHdZcXY7iBmODaHFogy79BBJzBtr0iH1KCzZ/3nNWcFoHYCMpEdcg+B648aUSOo1njYfQrQZdAl2FHACsisgFOXiWlWcNSXPjWb+OPu1g/MPLgBDfkN+tYOQdwjx2nnaev8CrHt4Ee114Y08A7OFIfLC8+vrQIXGbaM5qb9d7sPJU4AArcnJwrFdAVr0/9+/gQAnAFuZAkAaAFrwTppxR0B2wWJ8GaevvOccETAOYNRlkz4XAcFYGAHAYBTLBFQDyGly7e3n0cWpaEACt2YB7zXAcZcHAHAeA1hLCwDmM48Fwm/MZhcBCEITvnTEzsNpcWvAwAQXBAdQkhNyhnROwMRVwAwAz1WJqnyO8BkBC1yQwKhngc1uwMFJwFvBAO9RFI0RAQtmV3XL7zorCwMKEwMtAwWgH/UvDFgB5aYZgwMJ4wMLCOv9vfMIEAMRsD4MHBU14YG1ZEgHlepZKw3dxfG8bUZ+WMH//8FaB8WygwNB/8IRAKpCg8fNw8F2dn5W1QD1ii39g4CAwQWEAQ/nihM7CAB3jBXwwf7BVx0B042nzFh6eG93wDrFxfH+wcLAgQjFNKRRXMNcGAD1YJzFcYjCwsHCwLXBxWR6DgCCsPA7/S3xOcA4CADEdZfEzMCkHAEOsVtkeY/AiHTB/8M6XMWEDwBtst7+6SnE8f5FCADMstL+R1wJAJS3A/84/TUFAcu3HC//jP4OD2i6XHf/wTpFDw+NvHDEwcEHVvoAAaS/D/spO/1GTsEOAKPEHjr8+vH8/lvAM03Fvskm/lo+/8A/1ABVwtL+wP/+wDj/+SROwAUASNSfw/rNBABO1VPAB/4OD5DhNPsywQf8QAoB8eEi/sEFCwWv4zT9+1tFOhlFYeLewPz7/Dn9+PD6wf7BwP46wAMP3/6l/v5RwwDg9DsqwAgQ2MBJRJUGRDvDbpRwtZCjkt+//x+xhD7/TTb5CBEWEpX/xLDPwcQ7RWDvvwSgUQRyBaBVQBH00liUCwFEccuW88ERB9M9M6c80NzcjDwsH/BVkBH+40WkoXEik21nBPP77+vw+l1ZLAhDQPVrAzxA7V+XBb2TACsWN6bXVEQ=

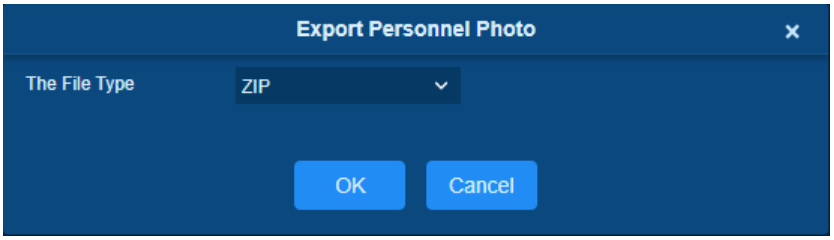
Personnel Import Template

Before exporting personnel template, configure the corresponding fields (including custom attributes fields). The required fields (Personnel ID, Name, Department ID, Department Name) do not support configuration.



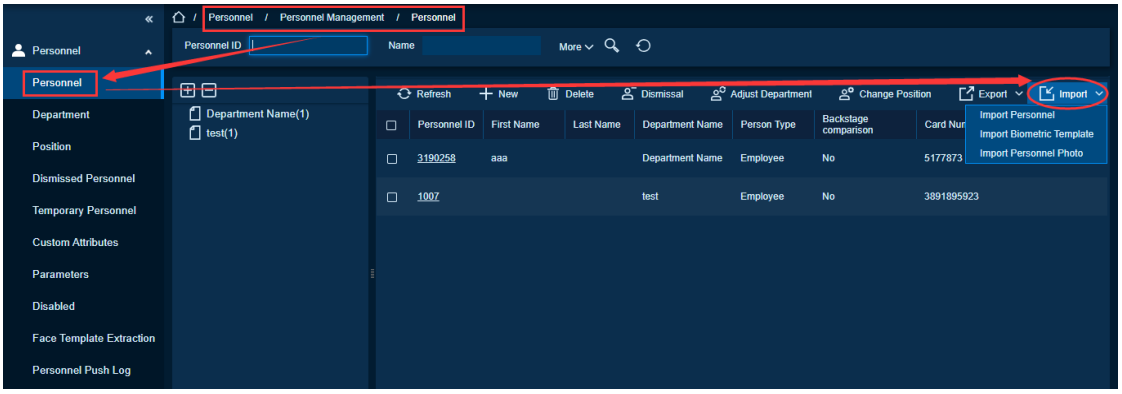
Export Personnel Photo

Choose the File Type and click **OK.**



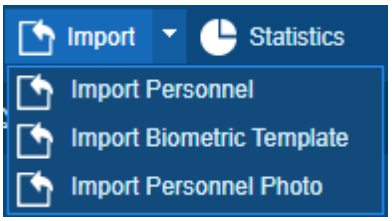
Import

Click **[Personnel Management]** > **[Personnel]** > **[Import]** to import personnel information and personnel biometric templates, personnel photo, and personnel photo with large quantities.

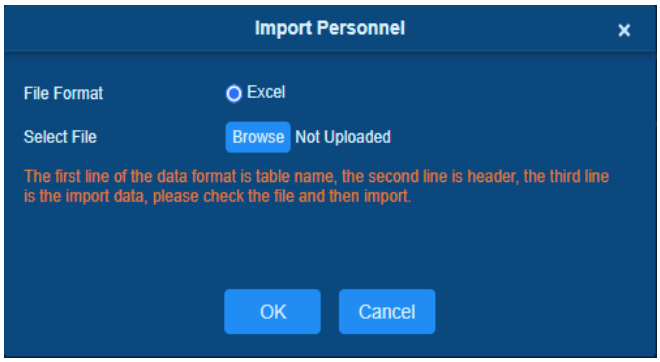


Import Personnel

- Click **Import > Import Personnel.**

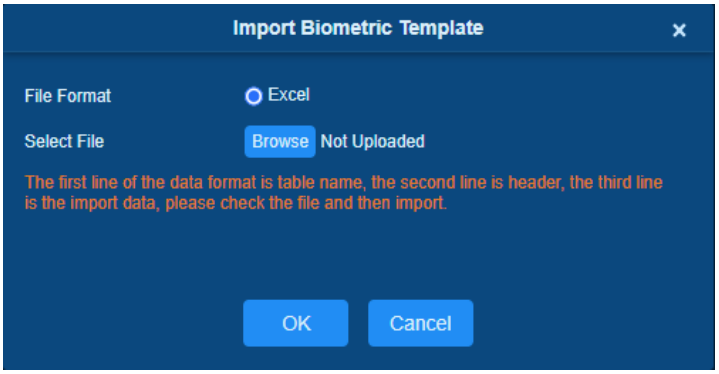


- On Import Personnel interface, click **[Browse]** to select excel file and upload.



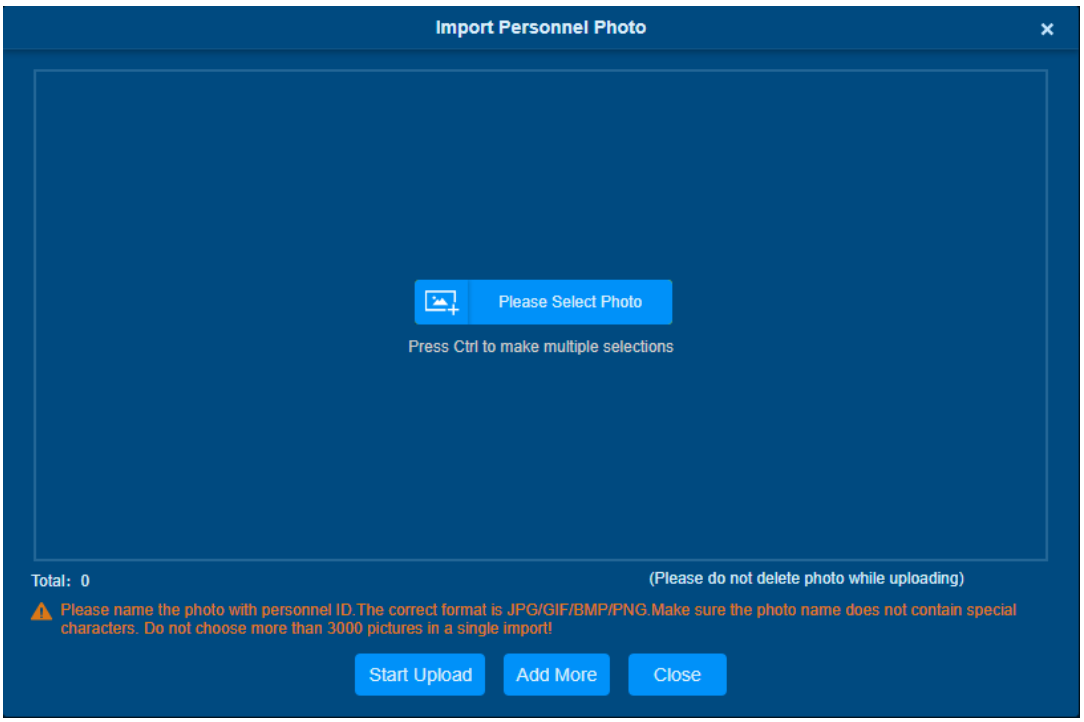
Import Biometric Template

Click **[Browse]** to select excel file and upload.



Import Personnel Photo

The personnel photo needs to be named same as the personnel ID. The supported common picture formats are **JPG, JPEG, PNG, GIF**, etc.

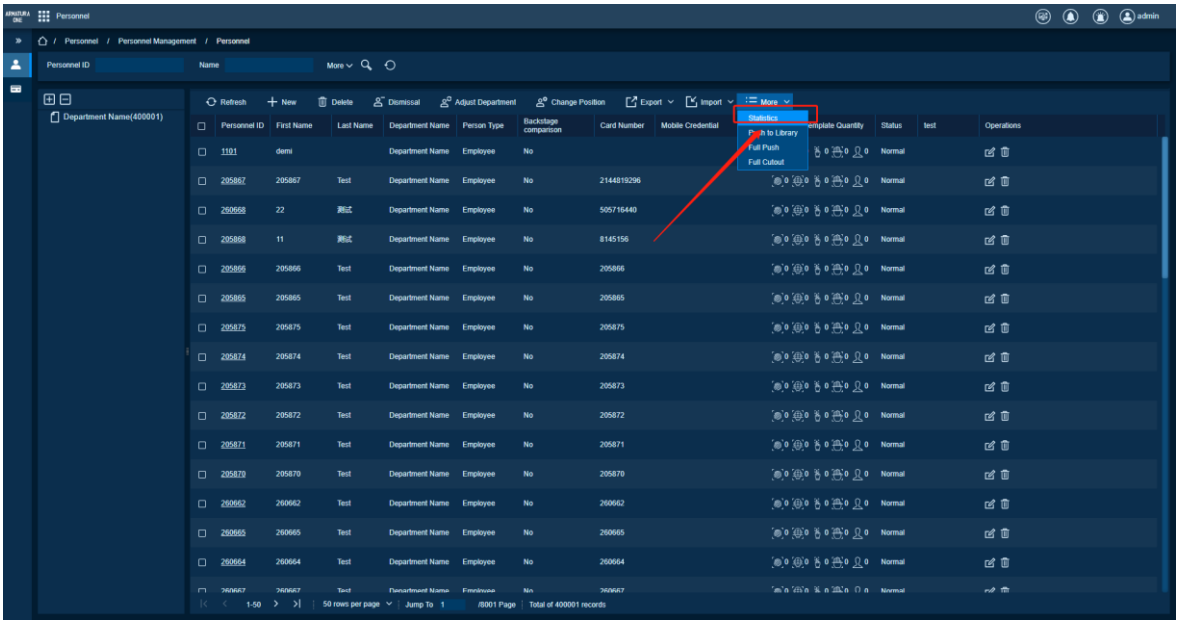


✍**Note:**

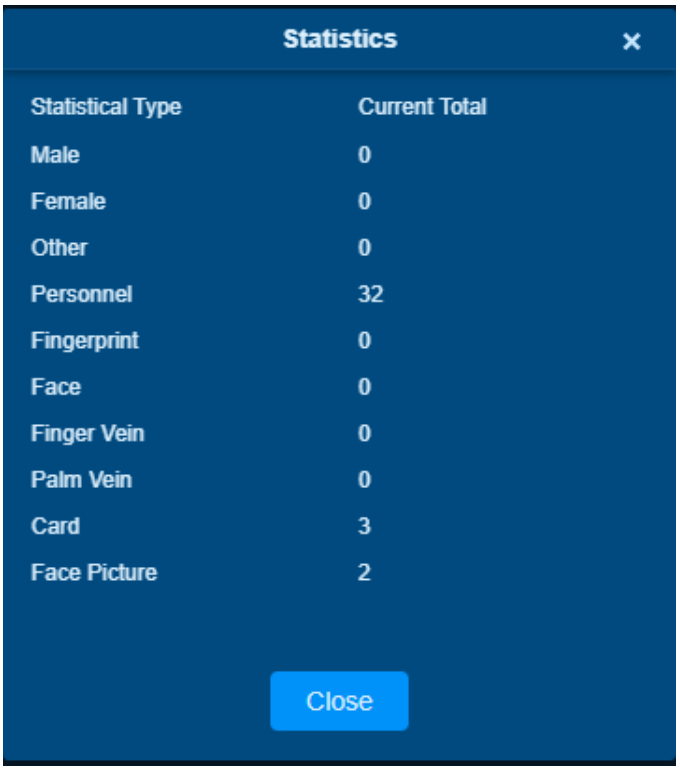
You can import the personnel photos in 2 ways: Import distinctive photos and compressed package. While importing distinctive photos, the user can import a maximum of 3000 photos at a time. While importing the compresses package, it must be in ZIP format and must not exceed 500MB.

Statistics

Click **[Personnel Management]** > **[Personnel]** > **[Statistics]** to view the number of Personnel, number of fingerprints, face templates, finger vein enrolled, card numbers, gender, and other statistical information.

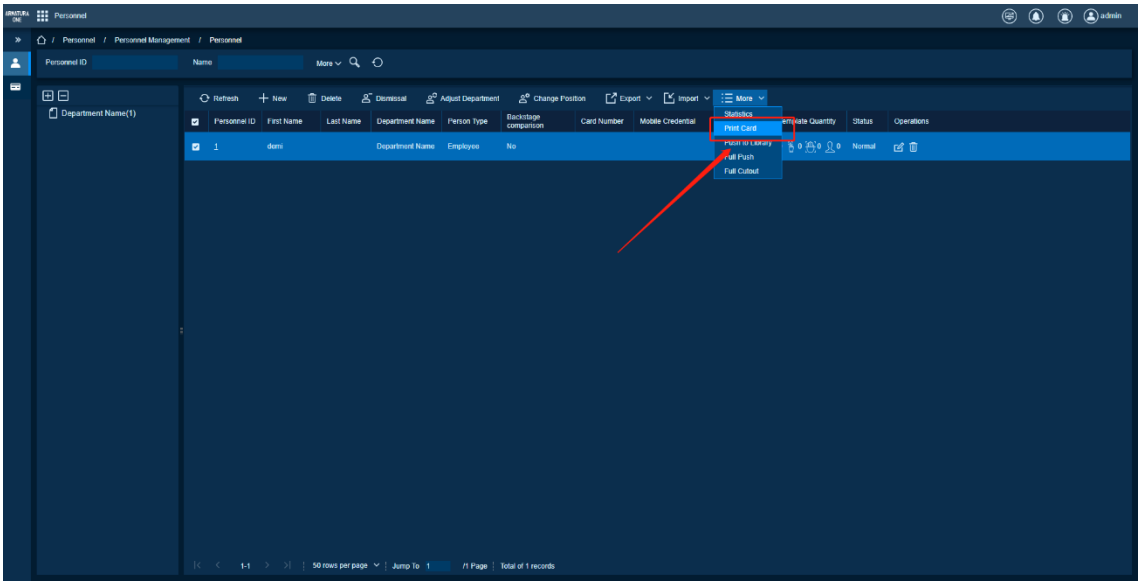


The Statistics interface is shown below: -

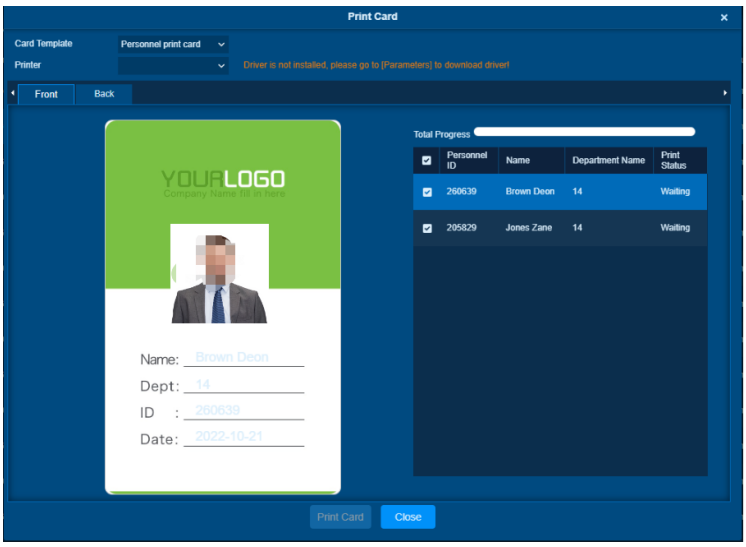


Print Card

- Click **[Personnel Management]** > **[Personnel]** > **[Import]** to open the card printing interface.
- Select the desired Personnel ID and click **Print Card**.



The Print Card interface is shown below: -



✍**Note:**

1. The card template can be defined in **[System]**> **[Basic Management]** > **[Print Template]**.
2. The Driver needs to download and install properly through **[Personnel Management]** > **[Personnel]** > **[Parameters]** > **[Registration Client]**. The registration code can be added through **[System]**> **[Authority Management]** > **[Client Register]**.

5.1.2. Department

Before managing the company's employees, it is required to set a departmental organization chart of the company. On the first use of the system, by default, it has a primary department named **[**General**]** and numbered **[1]**. This department can be modified but cannot be deleted. The main functions of Department Management include Add, Edit, Delete, Export and Import Department.

Function Usage Scenario

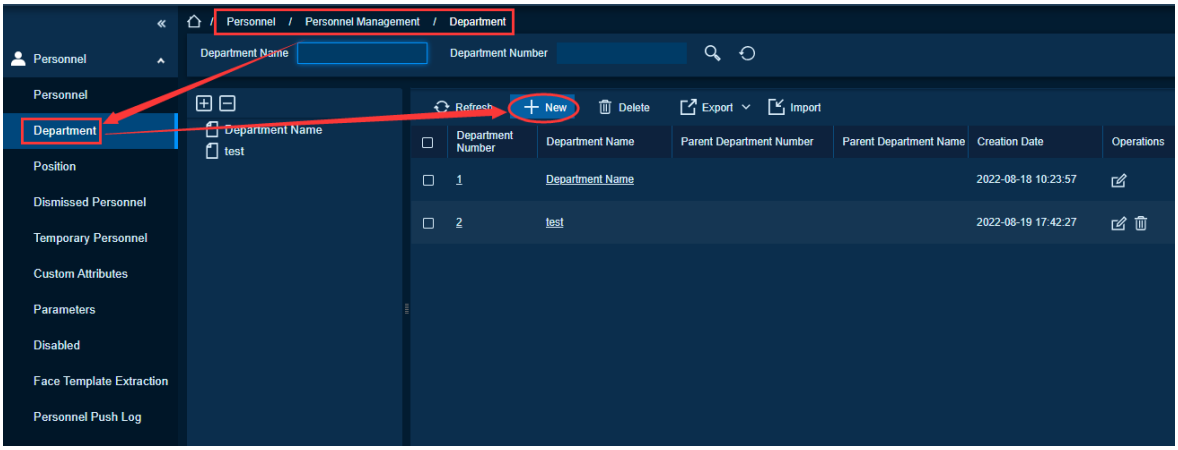
Create a new department for the system, create a department organizational structure, and manage the connection of each department.

Feature Trigger Results

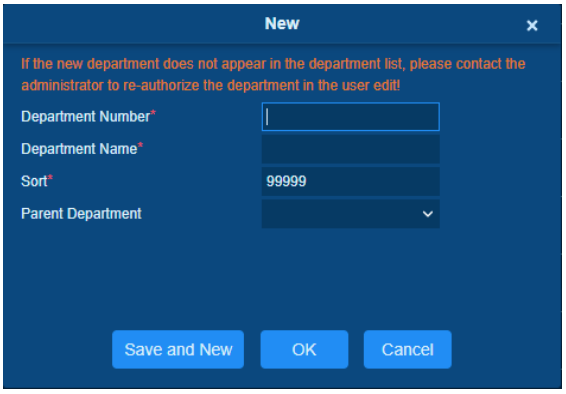
Add a department

Operation	Description
Check the Superior Department	Set your newly added department as a sub-department of an existing department. The personnel authority and structure will be integrated into the configuration of this superior department.

1. Click **[Personnel]** > **[Personnel Management]** > **[Department]** > **[New]**.



2. On the New Interface, enter Department Number, Department Name, Sort and Parent Department.
3. Click OK to save the changes.



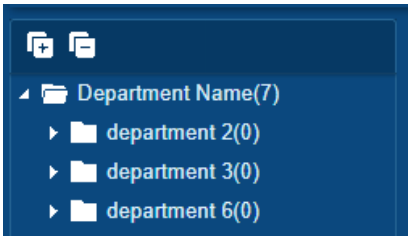
The fields are as follows:

Department Number: Alphabets and numbers can be entered. It cannot be identical to the number of another department. The number shall not exceed 30 digits.

Department Name: Any combination of characters with a maximum of 100 characters. In the case of different levels, the department names can be repeated.

Rank: The valid range is 1-999999999. The smaller the sort of number in the same level, the higher ranks the department will have. If this field is empty, it will be arranged in accordance with the increasing order.

Parent department: Select a parent department from the drop-down list. The Parent Department is an important parameter to determine the company's organizational chart. On the left of the interface, the company's organizational chart will be shown in the form of a department tree.

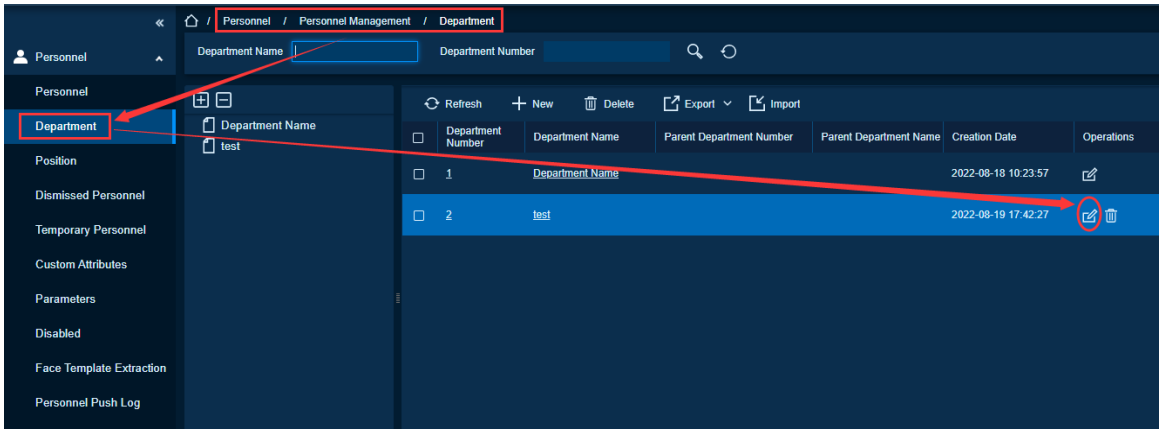


4. After filling the details, click **[OK]** to complete the addition process. Click **[Cancel]** to cancel it or click **[Save and new]** to save and continue adding new department.

5. To add a department, the user can also choose **[Import]** to import department information from other software or other documents into this system. For details, see Common Operations.

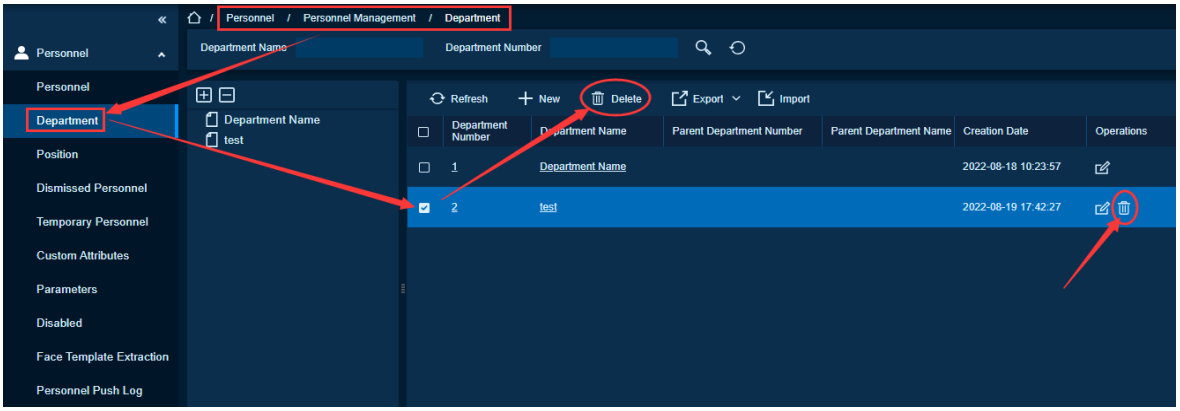
Edit a department

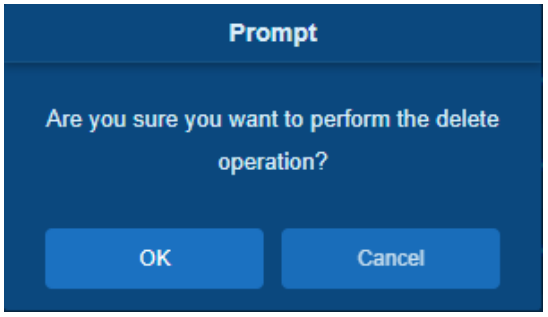
Click **[Personnel]** > **[Personnel Management]** > **[Department]** > **[Edit]**.



Delete a department

1. Click **[Personnel]** > **[Personnel Management]** > **[Department]** > **[Delete]**.





2. Click **[OK]** to delete.

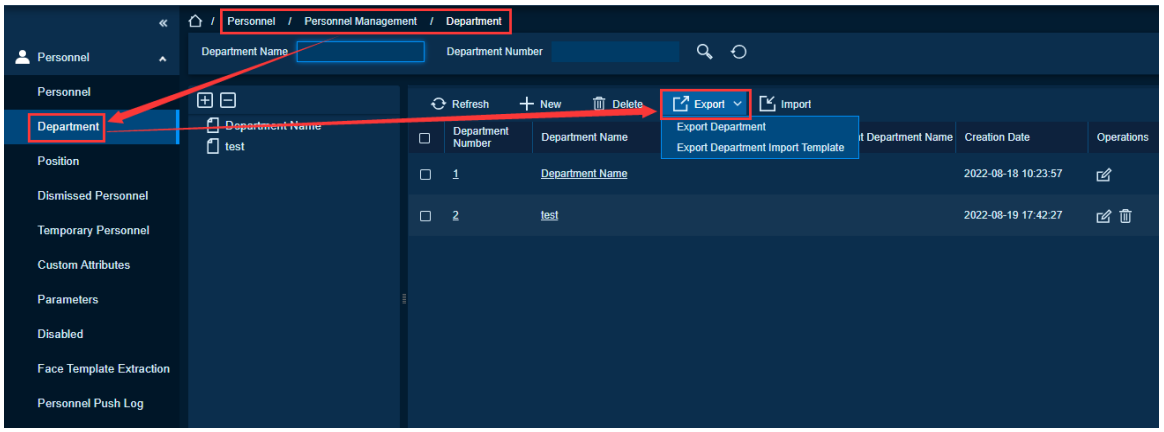
✍**Note:**

If the department has sub-departments or personnel, the department cannot be deleted.

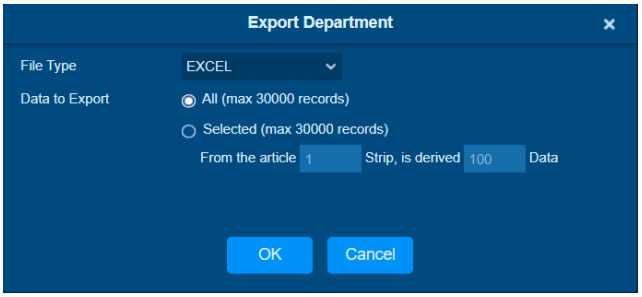
Export

1. Click **[Personnel Management]>[Department]>[Export].**

2. Export includes Export Department and Download Department Import Template.



3. On Export Department interface, choose File Type and Export Mode. Click **[OK].**

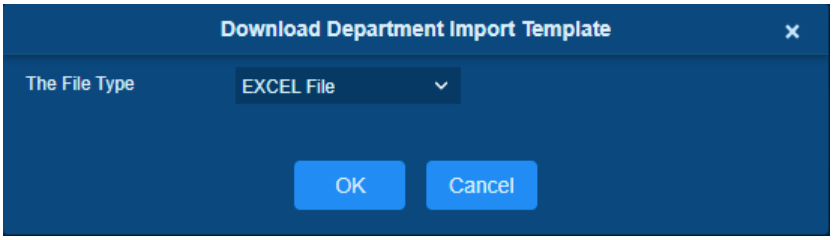


4. The Department details can be exported in EXCEL, PDF, CSV file format.

Department

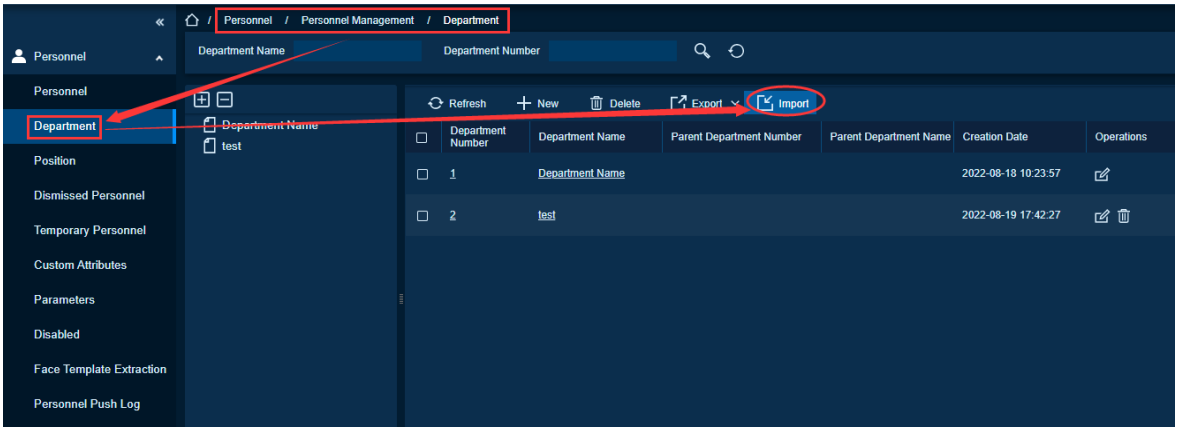
Department Number	Department Name	Parent Department Number	Parent Department	Created Date
hotel	Hotel			2017-12-15 09:06:51
4	Financial Department	1	General	2017-12-15 09:06:48
3	Development Department	1	General	2017-12-15 09:06:48
2	Marketing Department	1	General	2017-12-15 09:06:48
1	General			2017-12-15 09:06:48

5. On Download Department Import Template interface, select EXCEL File option. This Excel template file can be exported, and the user can use this template format to import department.

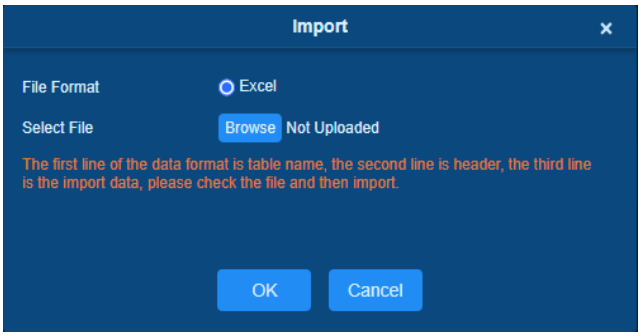


Import

1. Click **[Personnel Management]** > **[Department]** > **[Import]**.



2. Choose the file format as Excel and upload the file. Click **[OK]**.



The department information will be exported in EXCEL file format.

5.1.3. Position

The operator has the account authority of the personnel module. To organize the personnel as per their competency and skills, you can set a designation as required. This helps in sorting out the personnel easily.

Function Usage Scenario

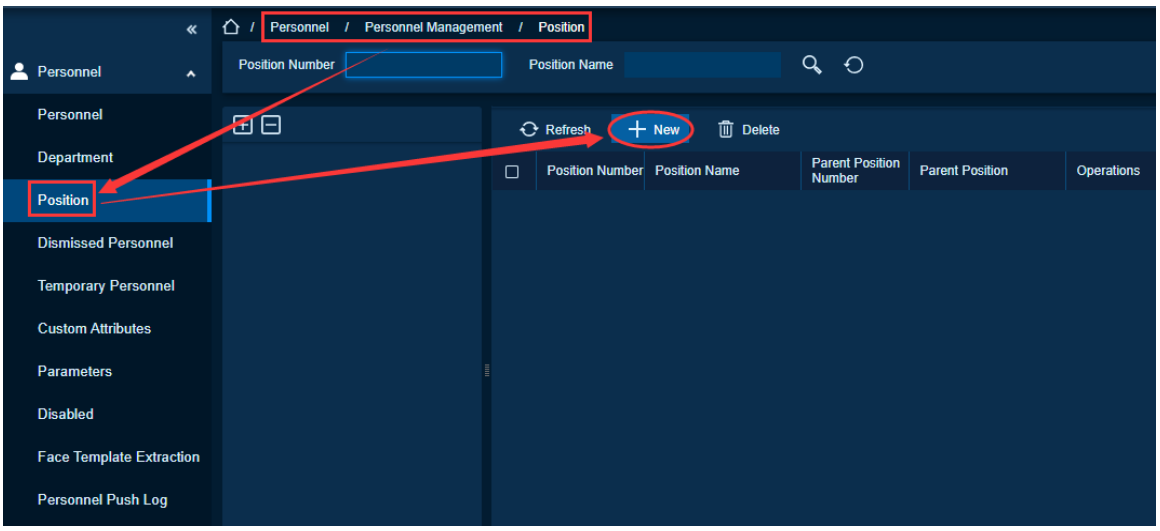
Create position information for the personnel, manage the connection of each position, and set the connection for attendance approval.

Feature Trigger Result

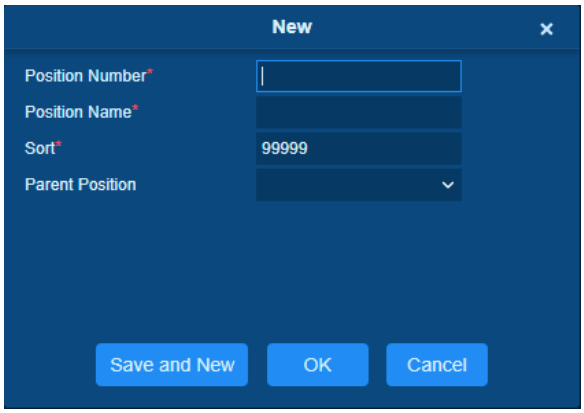
Operation	Description
Check the Superior Position	Set newly added position as a sub-position of an existing position and its personnel attendance will remain same just like the superior position.

Steps:

1. Click **[Personnel]** > **[Personnel Management]** > **[Position]** > **[New]**.



2. On the New interface, enter Position Number, Position Name, Sort and Parent Position.
3. Click **[OK]** to save the settings.



Fields are as follows:

Position Number: Set the value of the position number. It can be letters or numbers, or combination of both. Special characters are not allowed. The length shall not exceed 30 digits.

Position Name: Set the name for the position. It can be any character of a maximum 100 characters. The Position names should not be repeated.

Sort: Supports only numbers. The valid range is 1-999999999. The smaller the number of departments sort in the same level, the higher ranking the department has. If it is not filled in, it will be arranged in accordance with the added order.

Parent Position: By default, there is no position. It is an important parameter to organize the personnel as per their skills and competency.

5.1.4. Dismissed Personnel

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module.

Function Usage Scenarios

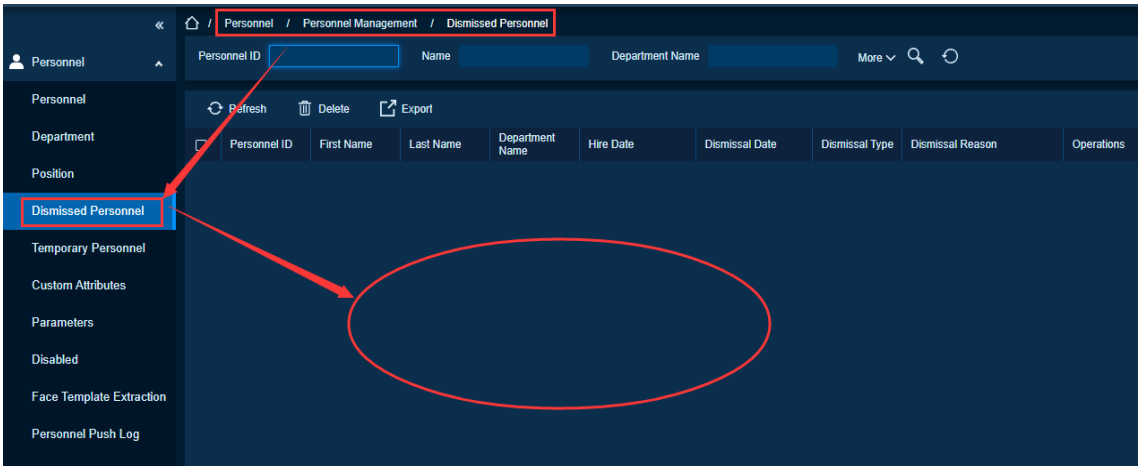
Save the identity information of the resigned personnel, export the message of the resigned personnel, and reinstate the departed personnel.

Feature Trigger Result

Operation	Description
Reinstatement Operation	Reconfirm the personnel information before reinstatement. The user can edit the personnel's information and permissions again.

Steps:

1. Click [**Personnel**]> [**Personnel Management**]> [**Dismissed Personnel**]>[**Reinstatement**].



2. The user can re-employ personnel by selecting the required employee and clicking on **[Reinstatement]** below operations tab.
3. Once the details are updated, click **[OK]** to save.

5.1.5. Temporary Personnel

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module.

In the Personnel-Parameter Setting, turn on the Personnel Self-Service Appointment function, and turn off the Automatic Review function of temporary personnel.

Function Usage Scenario

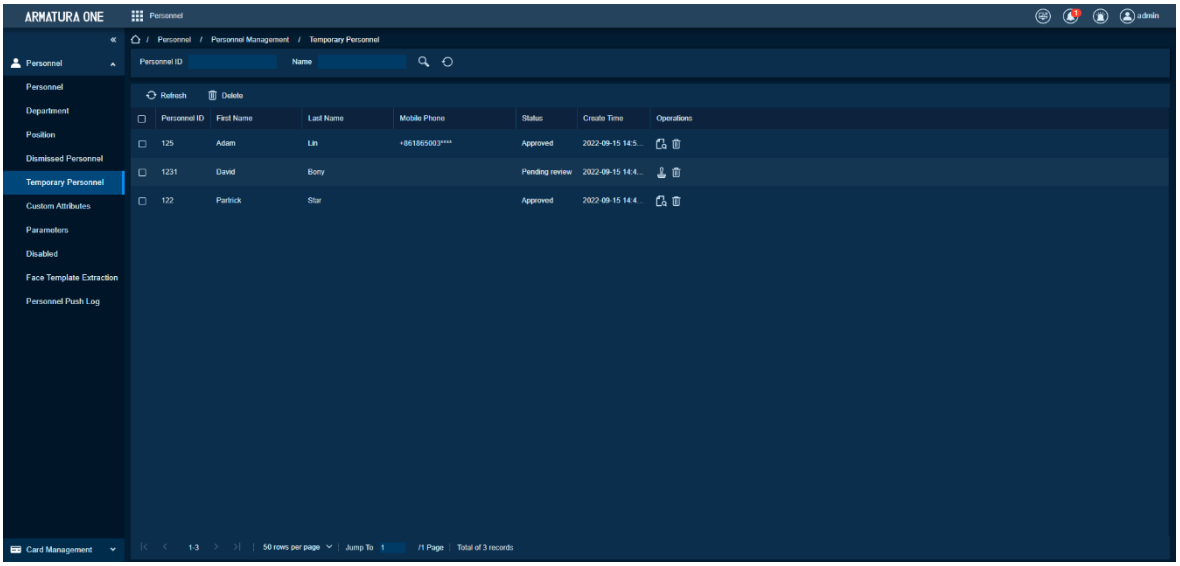
This parameter will display the list of personnel who are added by scanning the QR code of the facial recognition time and attendance device (E.g.: uFace WG100). The temporary personnel have the right to enter a specific area.

Feature Trigger Result

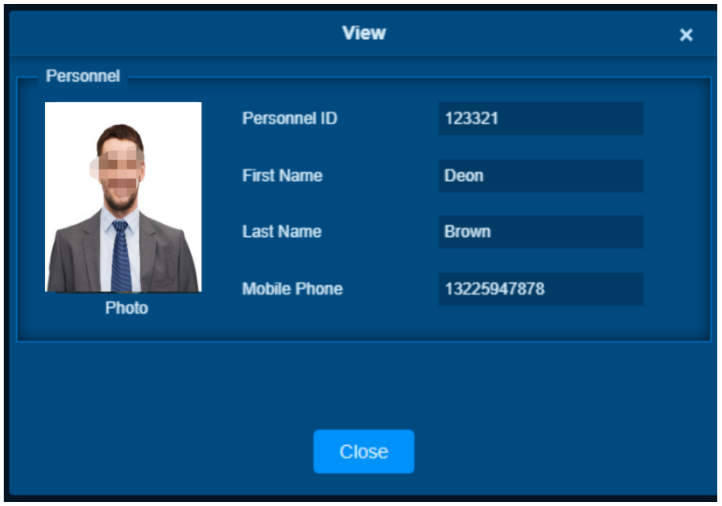
Operation	Description
Review Operation	Review the information of temporary personnel and grant permissions to them.

Steps:

1. Click [**Personnel**] >[**Personnel Management**] > [**Temporary Personnel**]. Then select temporary personnel and click **[Review].**



2. On the Review interface, the user can review Personnel Information. Click **[OK]** to save the changes.



3. The person will be automatically added to the list of Personnel.

Delete: It is used for deleting the selected temporary personnel.

5.1.6. Custom Attributes

Some personal attributes can be customized or deleted to meet different customers' requirements. When

the system is used for the first time, the system will initialize some personal attributes by default. Customized personal attributes can be set for different projects according to requirements.

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module.

Function Usage Scenarios

There are special description requirements for personnel information, such as **"Personal Religion"** and other fields that are not in the default personnel information, which can be manually added here.

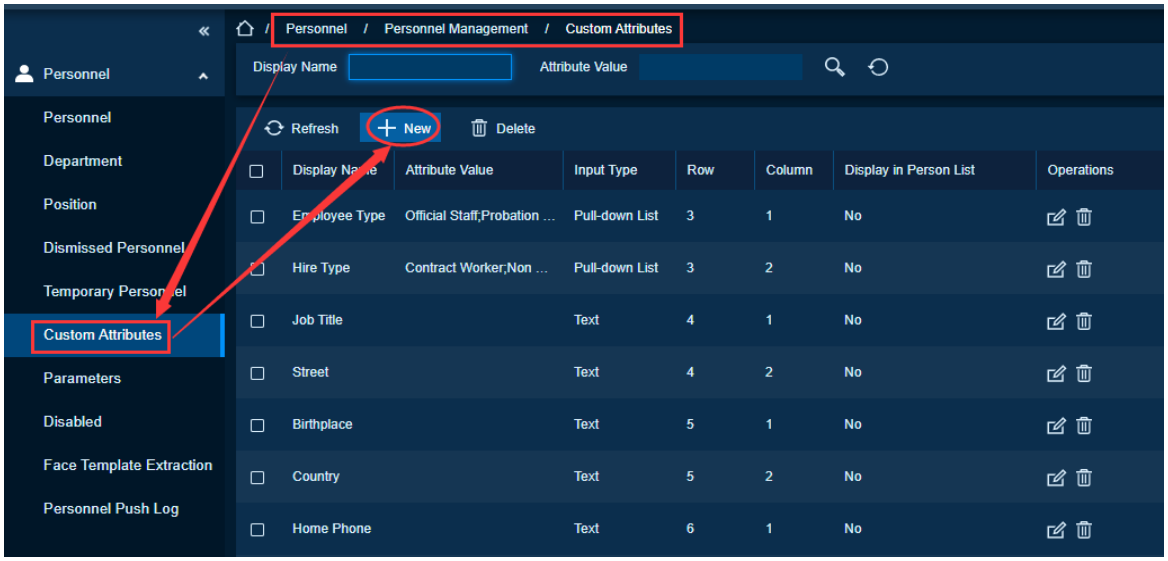
Feature Trigger Result

Operation	Description
Select to Display in the Personnel List	If you select "yes", the personnel information in this field will be displayed in the personnel list.

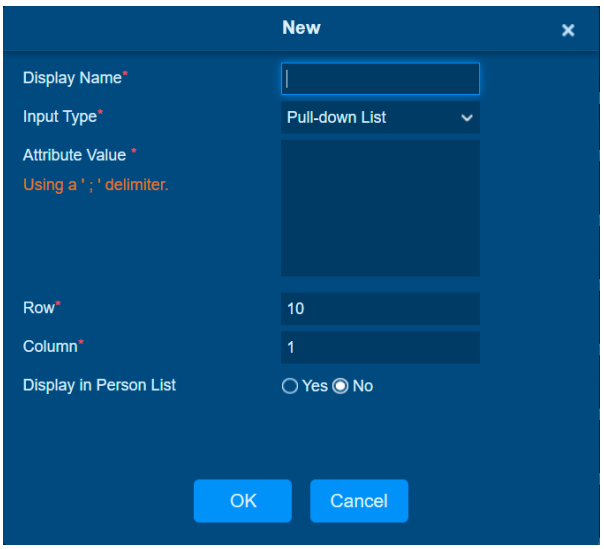
Steps:

For Creating New Custom Attribute:

1. Click **[Personnel] > [Personnel Management] > [Custom Attributes] > [New]**. Then edit the parameters and click **[OK]** to save and exit.



2. On the New interface, enter Display Name, Input Type, Attribute Value, Row, Column and choose the option for Display in Person List.
3. Click **OK** to save the changes.

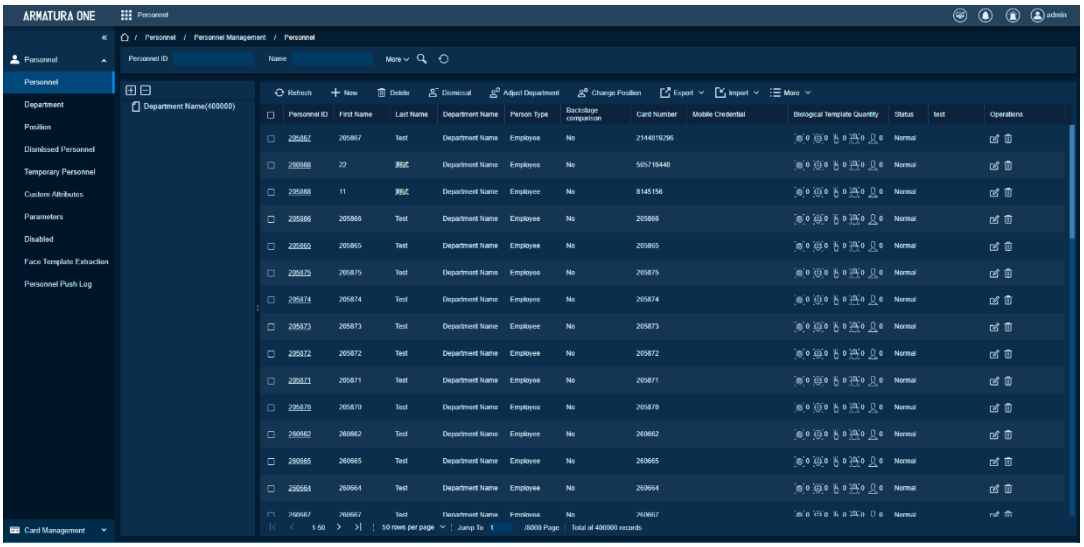


Display Name: The display name should not be repeated, and the maximum length is 30.

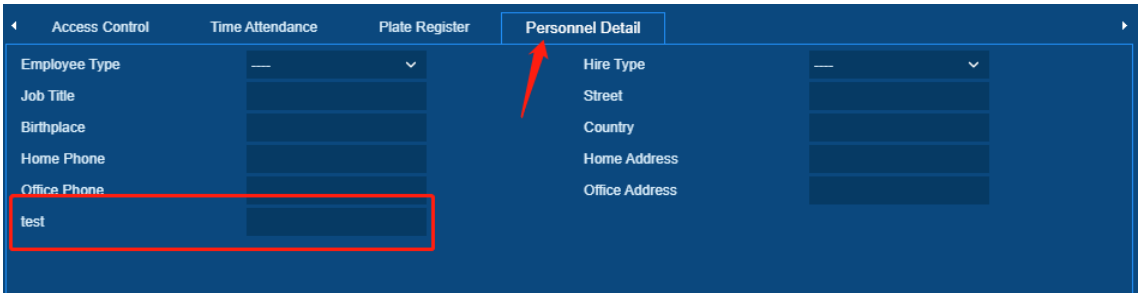
Input Type: Select the display type from “Drop-down List” Multiple Choice”, “Single Choice” and “Text”.

Attribute Value: Suitable for lists displaying as ‘‘Pull-down List’ ’Multiple Choice’’ and ‘‘Single Choice’’ lists. Use a “;” to separate the multiple values. If the input type is “Text”, the attribute value is not suitable.

Row/Column: The column and row of a field are used together to control the display position of the field. Numerals are supported. The column number cannot exceed 99, and the row number can only be 1 or 2. The combination of the column and row must not be duplicated.

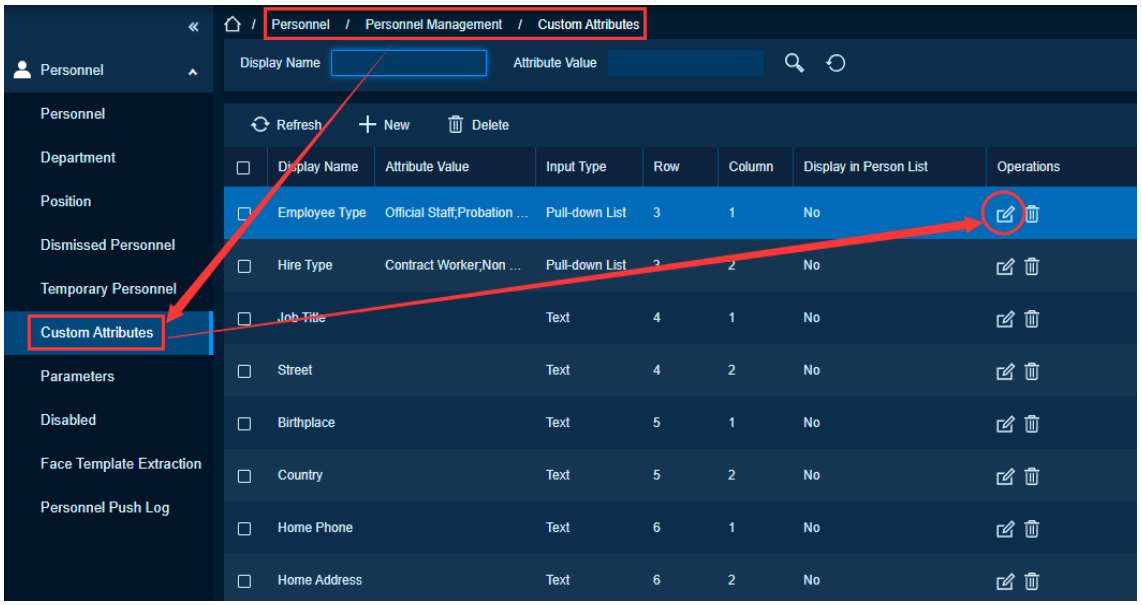


As shown in the following figure, Employee Type, is in the first column and first row, and Hire Type is in the first column and second row.



Edit a Custom Attribute

Click [Edit] to modify the corresponding attributes.



Delete a Custom Attribute

Click **[Delete]** to delete an unused attribute. If the attribute is in use, the system will pop up confirmation before confirming to delete.

✍**Note:**

The custom attribute will not be recovered once deleted.

5.1.7. Parameters

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module. Corresponding licenses are required for document identification and card issuing functions.

Function Usage Scenario

Some preferences for personnel management, such as Personnel Number, Card Number, Certificate Identification, depends upon the usage habits.

Feature Trigger Result

Personnel ID Setting

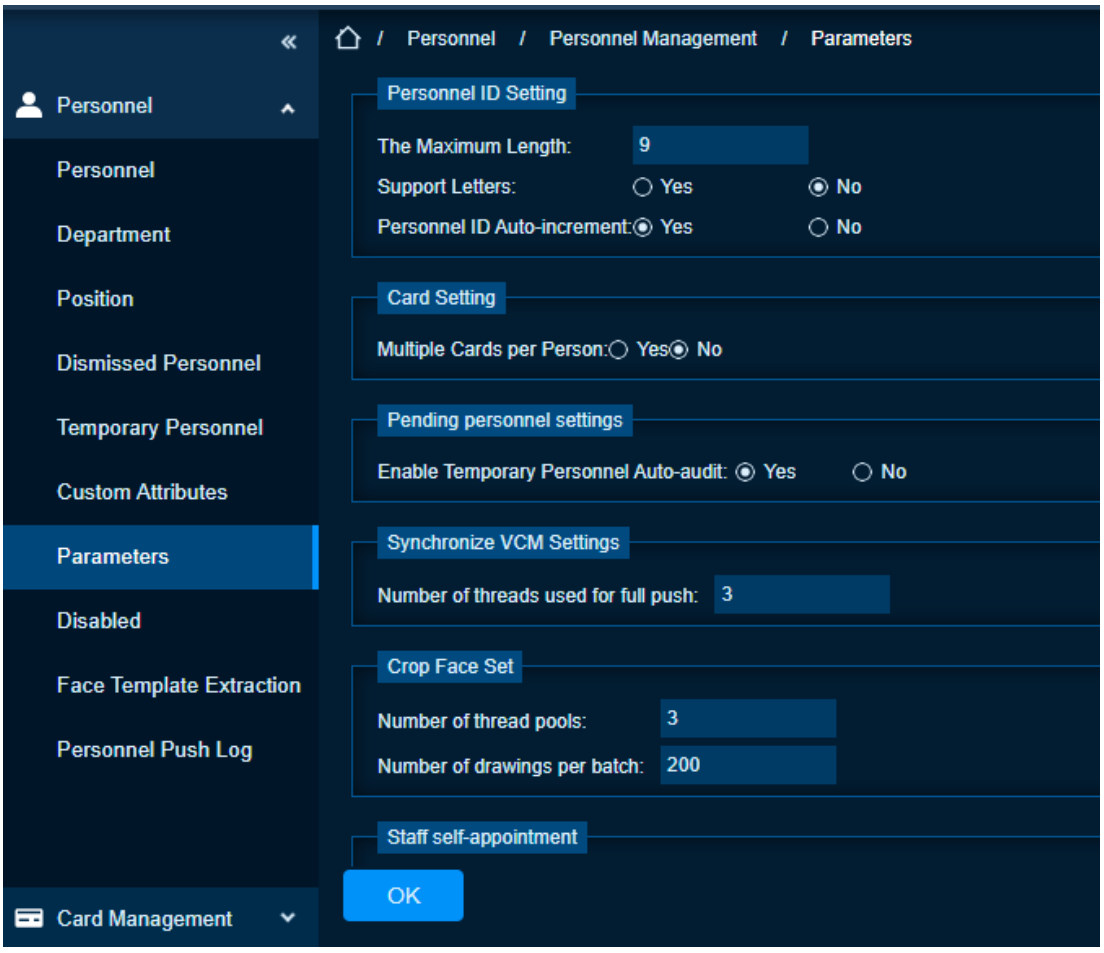
Operation	Description
The Maximum Length	It is the maximum length for a Personnel ID.
Support Letters	Click **Yes** to set the Personnel ID in form of alphabets otherwise click **No.**
Personnel ID-Auto Increment	This item cannot be turned on when the personnel number supports letters. When new person is added after it is turned on, it will be automatically incremented by 1 unit based on the previous personnel number.

Card Setting

Operation	Description
Multiple Cards per person	After turned on, the personnel will support adding up to 16 secondary cards in the personnel authority.

Steps:

Click **[Personnel]** > **[Personnel Management]** > **[Parameters]**.



Personnel ID Settings:

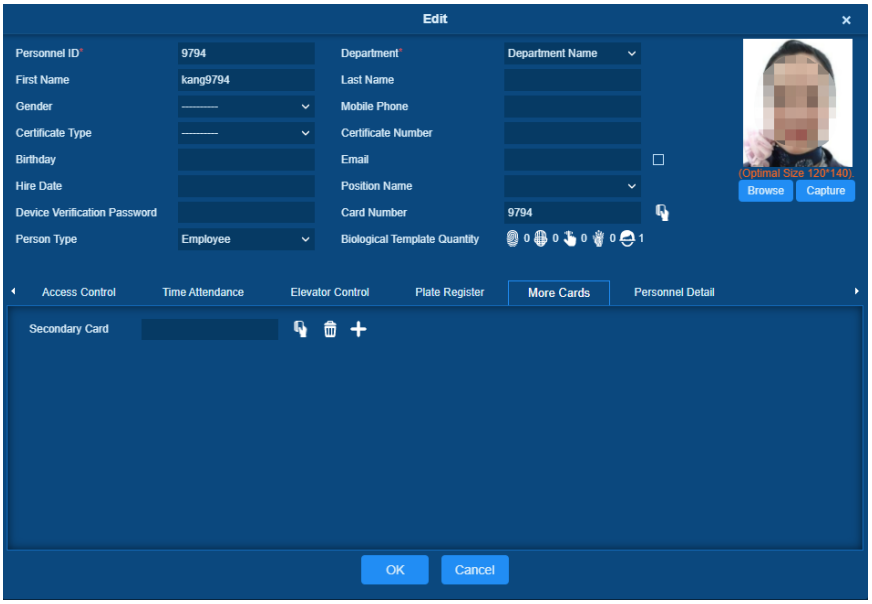
1. Set the maximum length for a Personnel ID and whether it will support alphabets or not. If the Personnel ID Auto increment is selected as Yes, then while adding personnel one by one, the ID in the field automatically increments by one.

Card Settings

Set whether “Multiple Cards per Person” will be allowed. i.e., multiple cards issued to the same person.

More Cards

Enabled the “Multiple cards per person” function, you can set multiple cards on the personal info page.



✍**Note:**

Not all devices support this function. For details, please consult the technical support.

Temporary Staff Setting

Set whether the temporary personnel uploaded and registered by scanning the QR code of the facial recognition time and attendance device need to review.

Synchronize VCM Settings

The VCM Settings define the concurrency of push.

Crop Face Set

This function is used to remove the information other than face image to make it clearer for successful access verification.

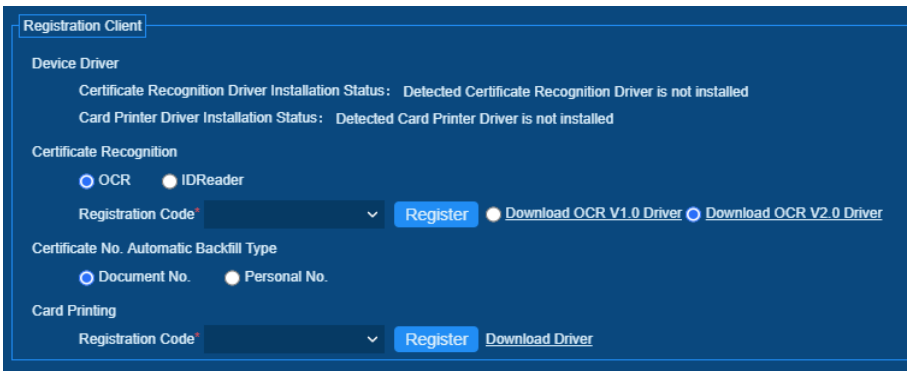
Self-service Registration

Use the QR code for staff to self-registration, update their personal information.

Registration Client

Use this function to perform functional service registration such as OCR document recognition.

If no driver has been installed, the **[Download Driver]** link is displayed on the screen. Click the link to download and install the driver.



1. Select the corresponding Registration Code and click **[Register].**

✍**Note:**

Click **[System]** > **[Authority Management]** > **[Client Register]** to view the registration code.

2. Click **[OK]** to save the settings and exit.

5.1.8. Disabled

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module.

Function Usage Scenarios

When a person is added as Disabled, all his/her access rights will also get disabled.

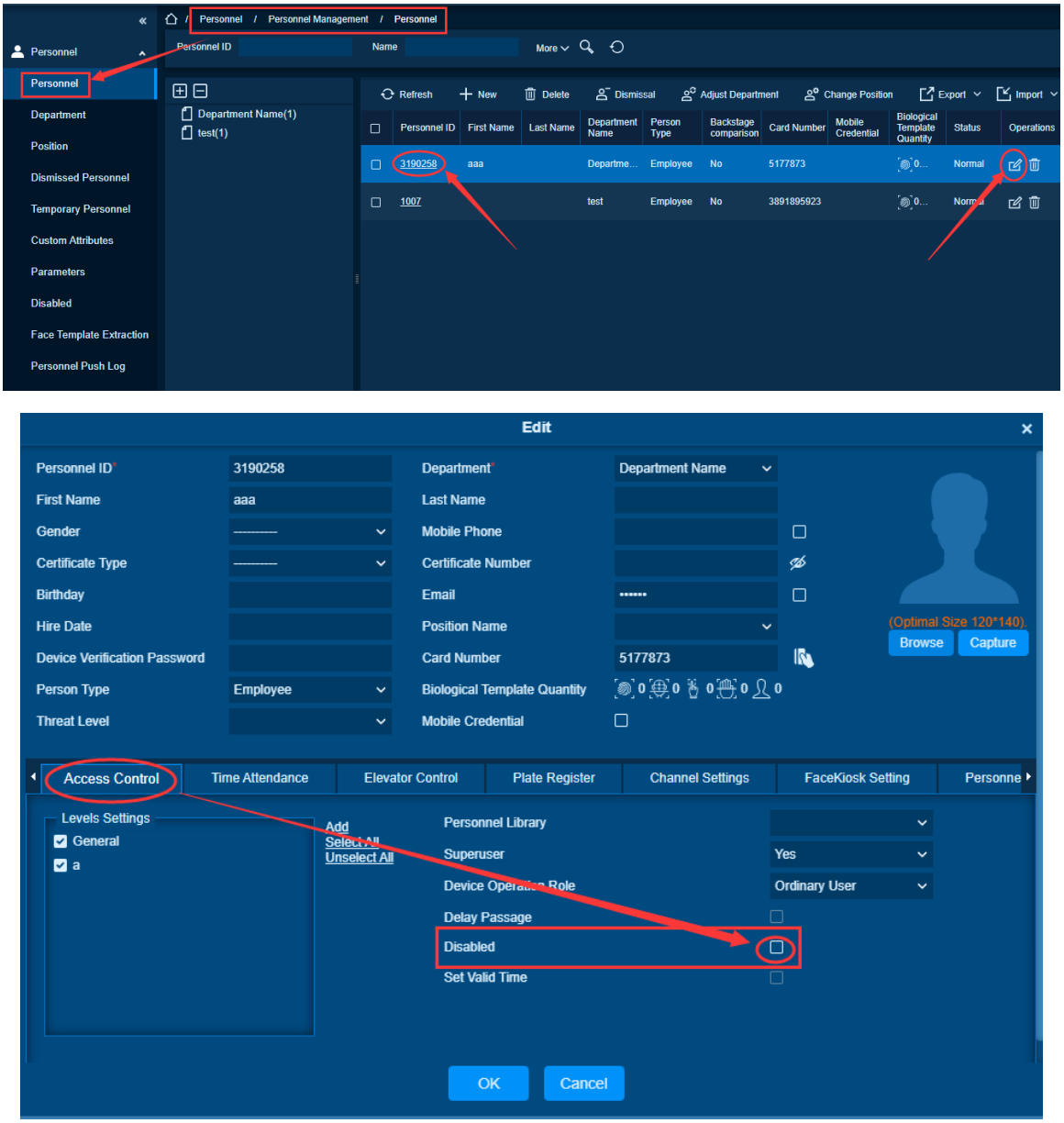
Feature Trigger Result

Operation	Description
Staff Editing-Check the Banned List	Add person to the Disabled and disable all access rights for the person.

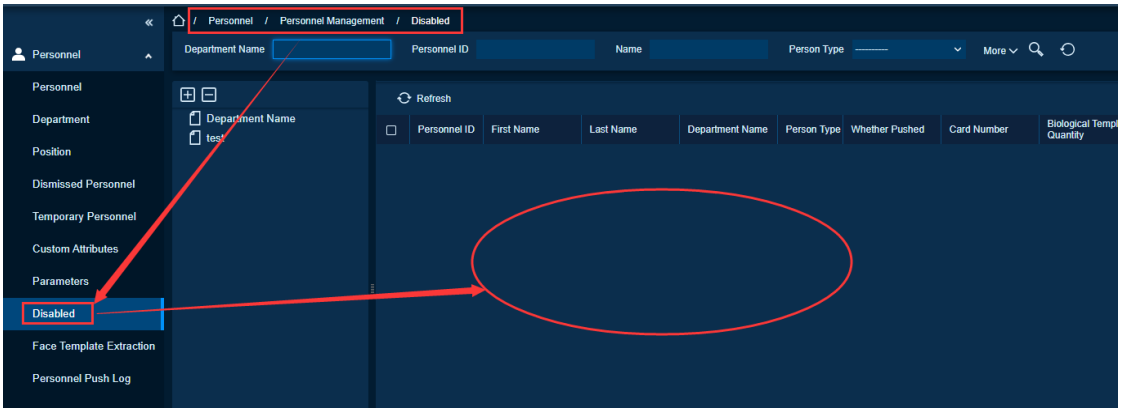
Steps:

Add as Disabled

In the Personnel list, check the person you want to add to the Disabled. Go to Access Control settings and check the Disabled option.

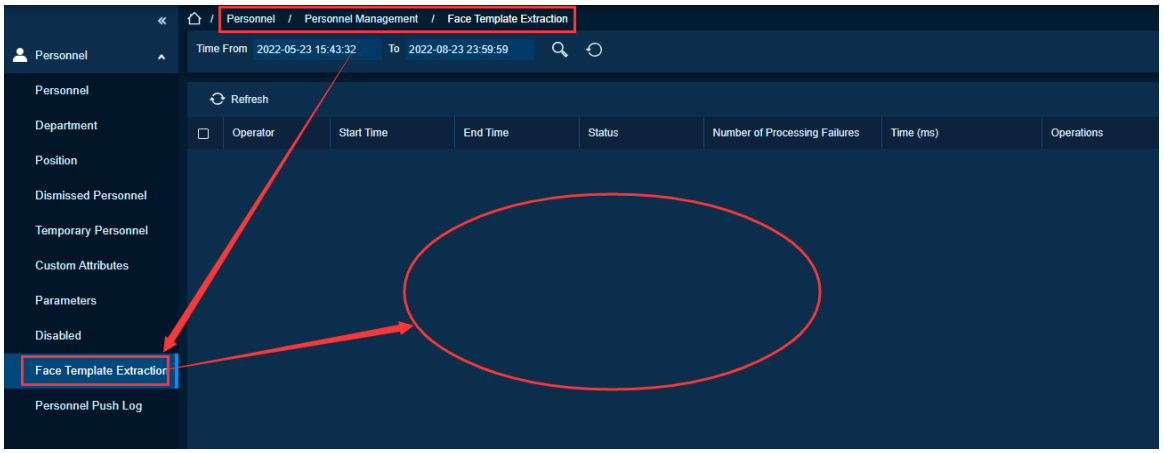


Click [**Personnel**]> [**Personnel Management**]> [**Disabled**] to view all the people who have been added as "Disabled".



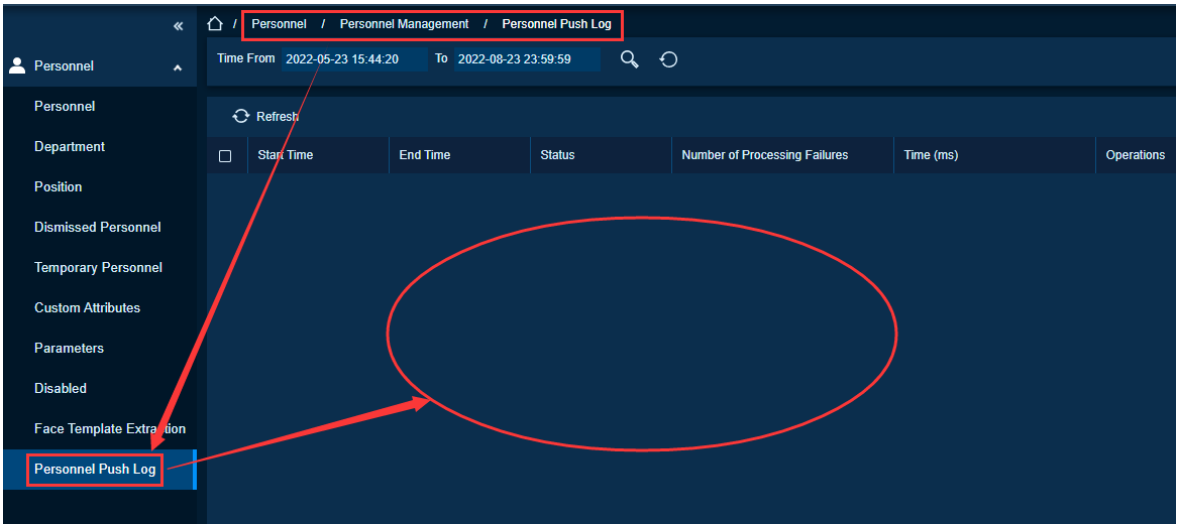
5.1.9. Face Template Extraction

Face Template Extraction will record the above-mentioned "Full cutout" function log. The user can check whether the Full Cutout function is used successfully, and the number of times of execution.



5.1.10. Personnel Push Log

Personnel Push Log will record the log of the "Personnel Full Push Function". It also records the result of staff pushing to the staff database.



5.2. Card Management

The card is one of the important vouchers for the passage. It can help you view and manage all the cards you issued. It supports the management of Wiegand format cards to meet your higher security requirements.

There are three functions in Card management: Card, Wiegand Format, and Issue Card Record.

5.2.1. Card

Preconditions for Normal Use of Functions

The operator has the account authority of the personnel module.

Function Usage Scenarios

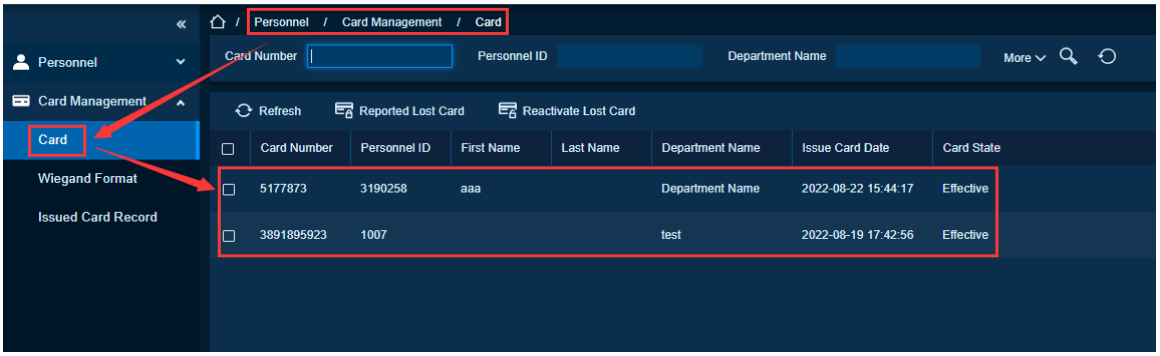
Check the personnel information corresponding to all issued cards and card numbers and perform reported lost card and reactivate lost card.

Feature Trigger Result

Operation	Description
Check the Card Number-Report Lost	When a card is reported as lost, it will lose the original access control authority.
Resolve Lost Report	Once the lost report is resolved, the card number gains the original access control authority.

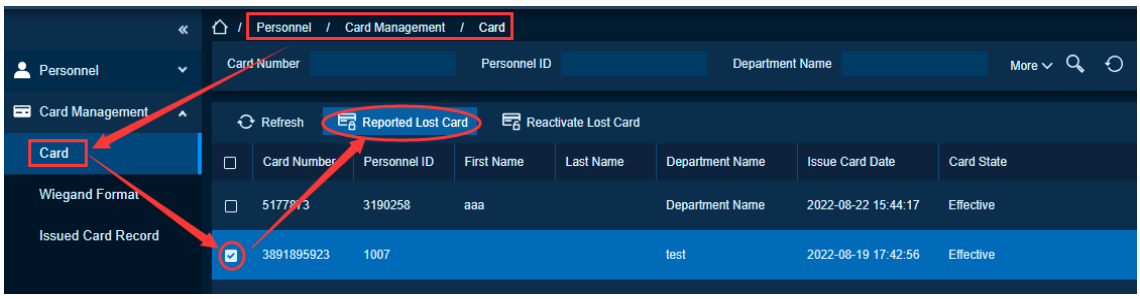
Steps:

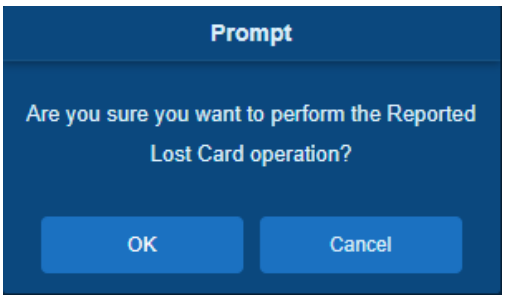
To check the card status review, click **[Personnel]** > **[Card Manage]** > **[Card].**



Reported Lost Card

1. Click **[Personnel]> [Card]**. Then choose the Card Number and click **[Reported Card Lost]**.

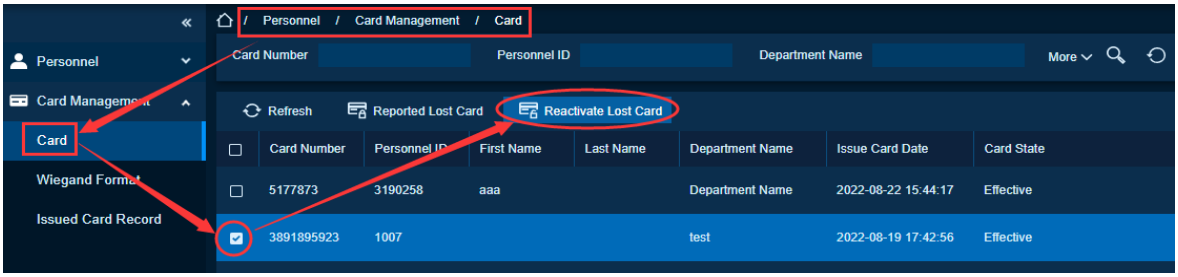


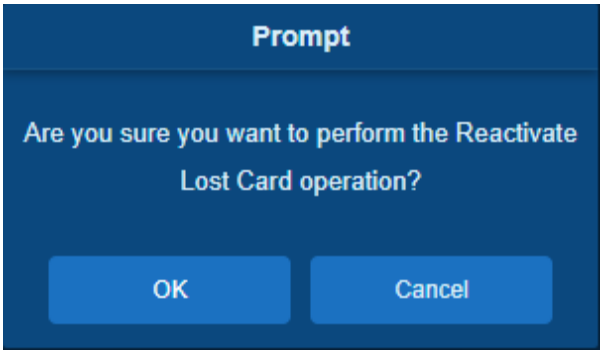


2. Click **[OK]** to confirm that card is lost. After this all permissions on this card will be invalidated.

Reactivate Lost Card

1. Click **[Personnel]> [Card]**. Then choose the Card Number and click Reactivate Lost Card.





2. Click “OK” to reactivate invalidated card and restore card access permissions.

5.2.2. Wiegand Format

Wiegand Format is the card format that can be identified by the Wiegand reader. The software is embedded with 9 Wiegand formats. You may set the Wiegand card format as needed.

Function Usage Scenarios

Check the personnel information corresponding to all issued cards and card numbers and perform reported lost card and reactivate lost card operation.

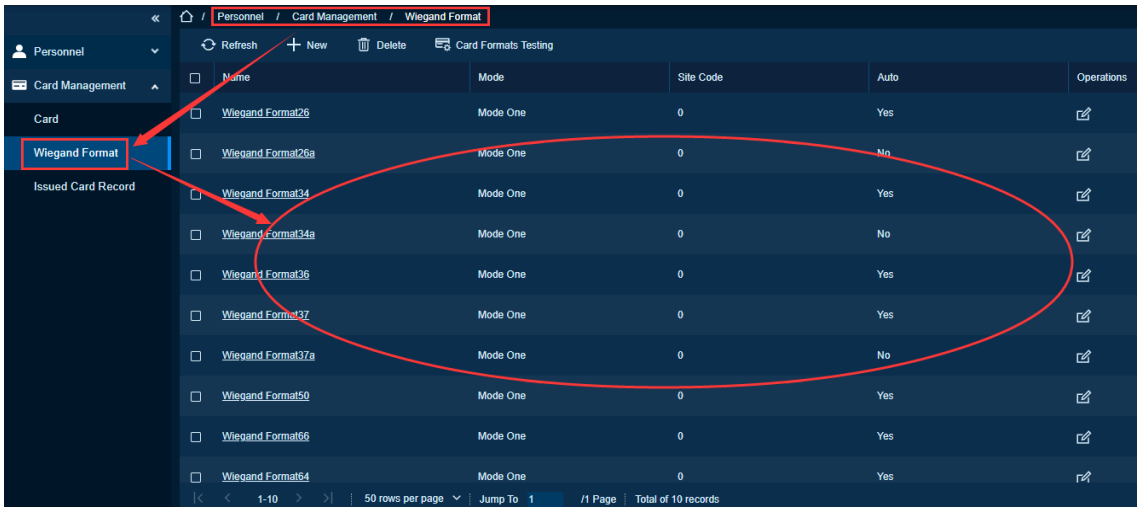
Feature Trigger Result

Operations	Description

Check The Card Number-Report Loss/Resolve Loss Report	Then lost card number loses the original access control authority, and the new card number gains the original access control authority.

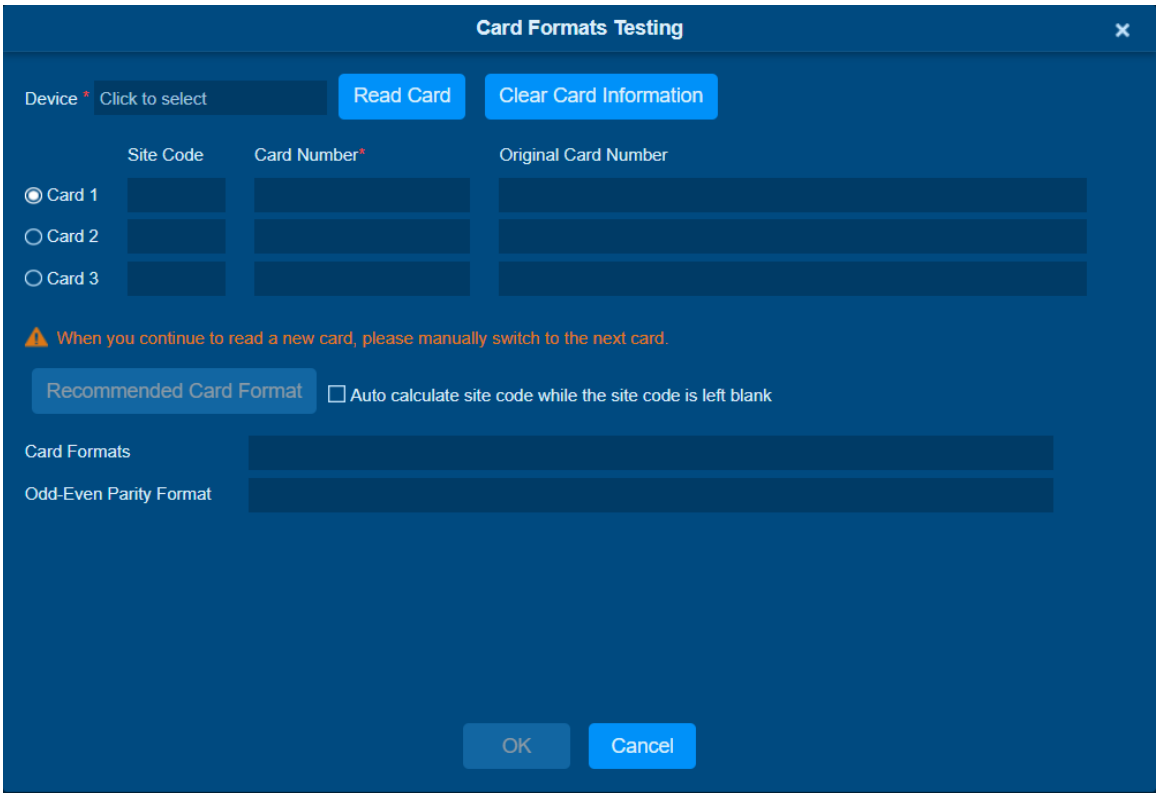
Steps:

Click **[Personnel]**>**[Wiegand Card Format]**.



Card Formats Testing

When the card number does not match with the one which is displayed on the system, the user can use the Card Formats Testing function to calibrate the Wiegand format. The page is explained as follows:



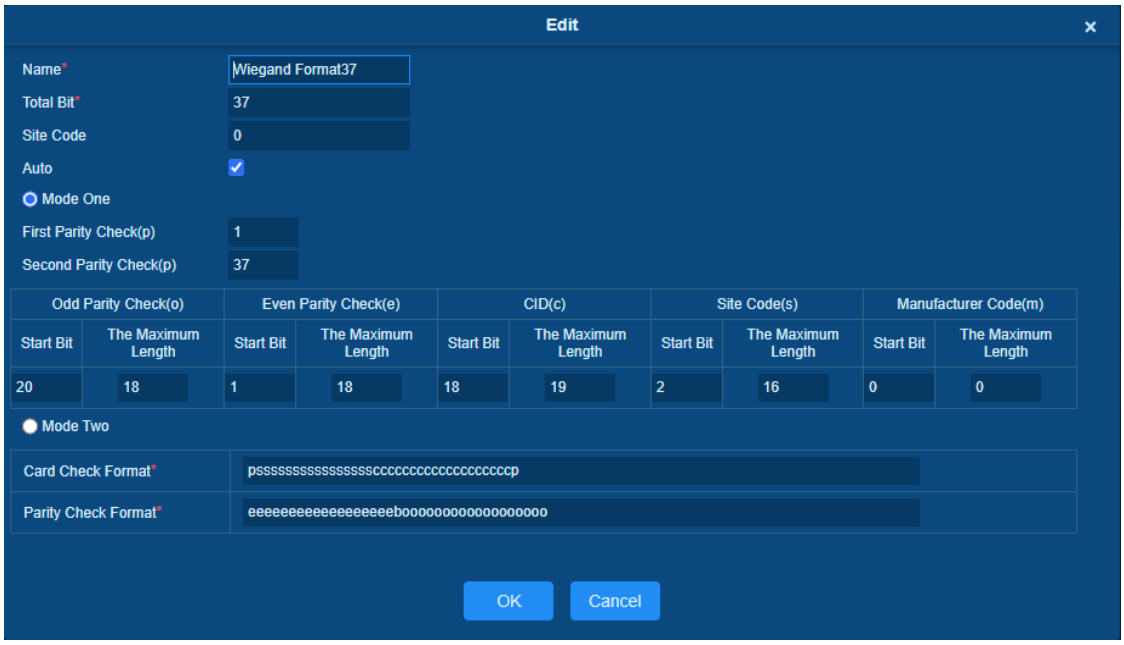
1. Select the device that supports the card format test function and fill the card number and the site code.
2. Click **[Read Card]** and swipe the card on the reader. The original card number will be displayed on the Original Card Number text box.
3. Click **[Recommended Card Format]** and the recommended Wiegand card format will be displayed on the screen.
4. Click **[Auto calculate site code while the site code is left bank]** and the software will calculate the site code according to the card format and card number.
5. Click **[OK]** and the page will jump to the Wiegand format page to save the new Wiegand format.

✍**Note:**

The card format testing function is only supported by few devices.

This software supports two modes for adding the Wiegand Format: If mode 1 does not meet your setting requirements, you may switch it to mode 2.

Take Wiegand Format 37 as an example:



Format Explanation

“P” indicates Parity Position; “s” indicates Site Code; “c” indicates Cardholder ID; “m” indicates Manufactory Code; “e” indicates Even Parity; “O” indicates Odd Parity; “b” indicates both odd check and even check; “x” indicates parity bits no check.

The previous Wiegand Format 37: the first parity bits (p) check “eeeeeeeeeeeeeeeee”; the second parity bits check “ooooooooooooooooo”. Card Check Format can only be set “p, x, m, c, s”; Parity Check Format can only be set “x, b, o, e”.

5.2.3. Issued Card Record

The issued card record displays the history of the card and displays the operations performed on the card.

Function Usage Scenario

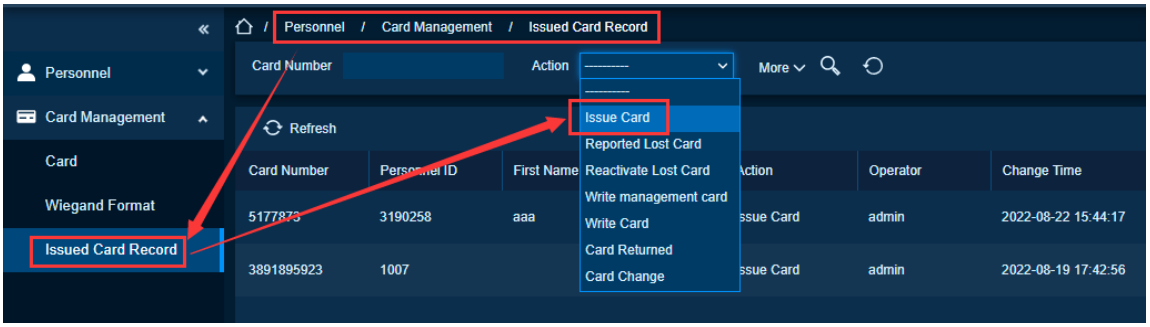
View historical card issuance, report loss, reactivate, write management card, write card, card retuned, and card change records.

Feature Trigger Result

Operation	Description
Switch Operation Type	It displays record results of different operation types.

Steps:

Click **[Personnel]> [Card Management]> [Issued Card Record]**. Then choose the action as “Issue Card Record” from the drop-down.



✍**Note:**

The cards and card issuing records of an employee will be deleted altogether when the employee’s account is deleted completely

6. Access Control Management

The system needs to be connected to an Access Controller to provide access control functions. To use these functions, the users must install the access control devices and connect them to the network first, then set corresponding parameters, so that they can manage devices, upload access control data, download configuration information, output reports, and achieve digital access management of the enterprise.

6.1. Device

Function List

Functions	Operation Instructions
Device	• Device Addition, Deletion, Editing and Search • Control-Clear Administrator • Control-Set Login User Password • Control-Upgrade Firmware • Control-Restart Device • Control-Synchronize Time • Control-Enable & Disable • Control-Synchronize All Data • Control-Reset Device Data • Set Background Verification Parameters • Set Device Time Zone • Set Registration Machine • Set Daylight Saving Time • Modify Fingerprint Comparison Threshold • Set Machine Access Status • Set Echo Parameters • Set Authentication Server Parameters • Set Access Control Parameters • Set Data and Time • Set Access Control Records • Set Face Parameters • Temperature Management • Set Timing Sleep Time • Set Temperature Measurement Parameters • Set Extended Parameters • Obtain Device Parameters • Obtain Personnel Information • Obtain Event Records • Obtain Device Logs • View Devices Medium Access Control Rules • Download Device Logs • Query Device Capacity • Query Device Information

	• Query Firmware Information • View Time and Data • View Access Control Record Settings • View Device Temperature • View Access Control Parameters • View System Parameters • Modify IP Addresses • Modify Communication Passwords • Modify RS485 Address • Switch Network Connection.
I/O Expansion Board	Add, edit, view, delete I/O expansion board.
Door	Edit, remote open, remote close, enable, disable, cancel alarm, remote normally open, remote lock, remote unlock, enable the day's normally open time, disable the day's normally open time.
Reader	Edit reader, bind/unbind camera.
Auxiliary Input	Edit auxiliary input, bind/unbind camera.
Auxiliary Output	Edit, remote open, remote close, remote normally open.
Event Type	Edit and set event type.
Daylight Saving Time	Add, edit, delete, set daylight saving time.
Device Monitoring	Clear command, view command, clear all command.
Real-Time Monitoring	Remotely open and close the door, auxiliary input, and output, cancel alarm, remote lock, remote unlock, remote normally open, enable the day's normally open time zone, and disable the day's normally open time zone.
Alarm Monitoring	Confirm the alarm.
Map Configuration	Add, edit, delete map.

6.1.1. Device

Function Description

Add a device, and then set the communication parameters of the connected device, including system settings and device settings. After the communication is successful, the user can view the information of the connected device, and perform remote monitoring, upload, and download, etc.

New Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority. The device supports adding to the Access Control module.

Function Usage Scenarios

Operations such as Personnel Issuing, Setting Parameters, Synchronizing Data, and Opening & Closing Doors are required for the device.

Feature Trigger Result

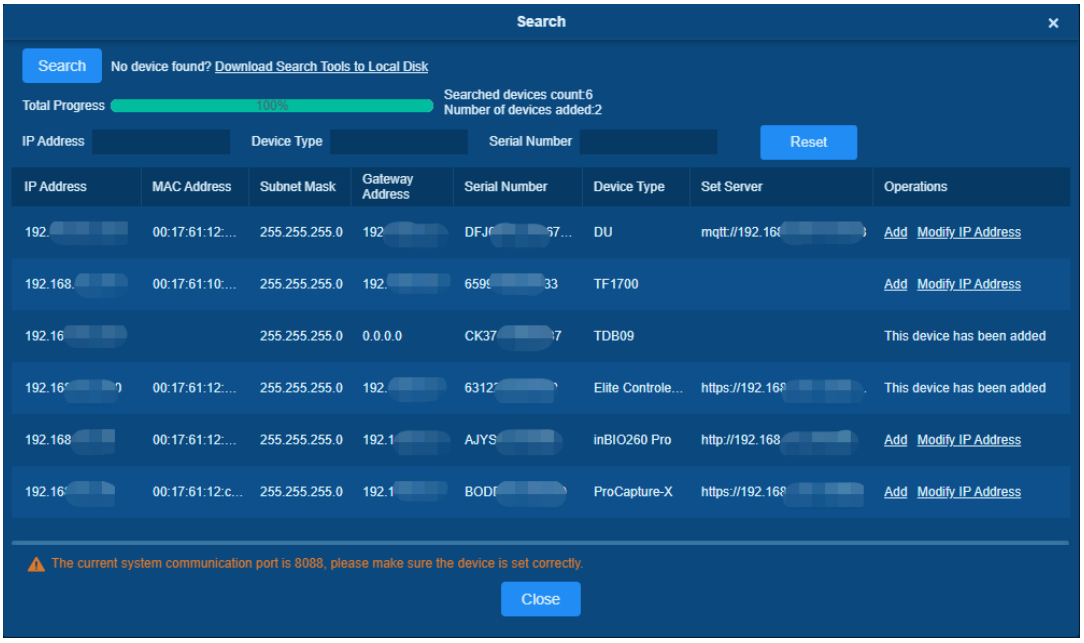
After adding a new device, the data in the device is automatically synchronized to the software, including Personnel Information, Access Control Settings, Device Version Number, etc. After adding the device, the personnel data can be operated through the software, and then sent to the device.

There are two ways to add Access Devices.

OmniAC Series Standalone Terminal

Follow these steps to search the access controllers in the Ethernet: -

- Click **[Device]** > **[Device]** > **[Search Device],** to open the Search interface.
- Click **[Search],** and it will prompt **[**Searching……**]**.
- After searching, the list and total number of access controllers will be displayed.

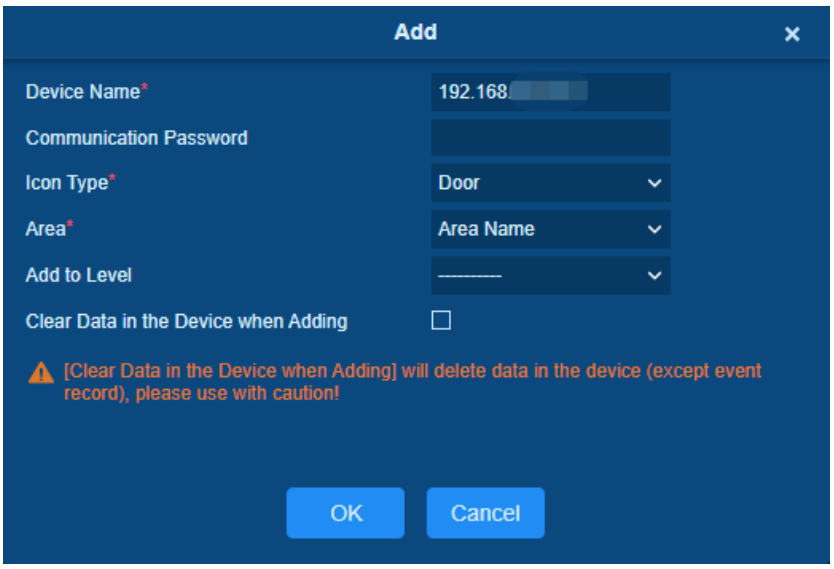


✍**Note:**

UDP broadcast mode will be used to search access device. This mode cannot perform Cross-Router function. IP address can provide cross-net segment, but it must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.

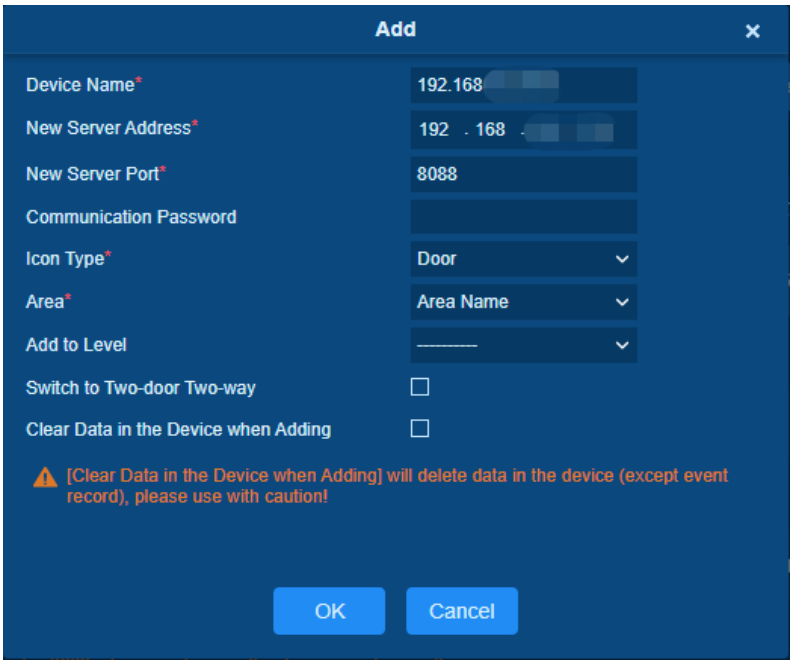
- Click on **[Add]** in the search list.

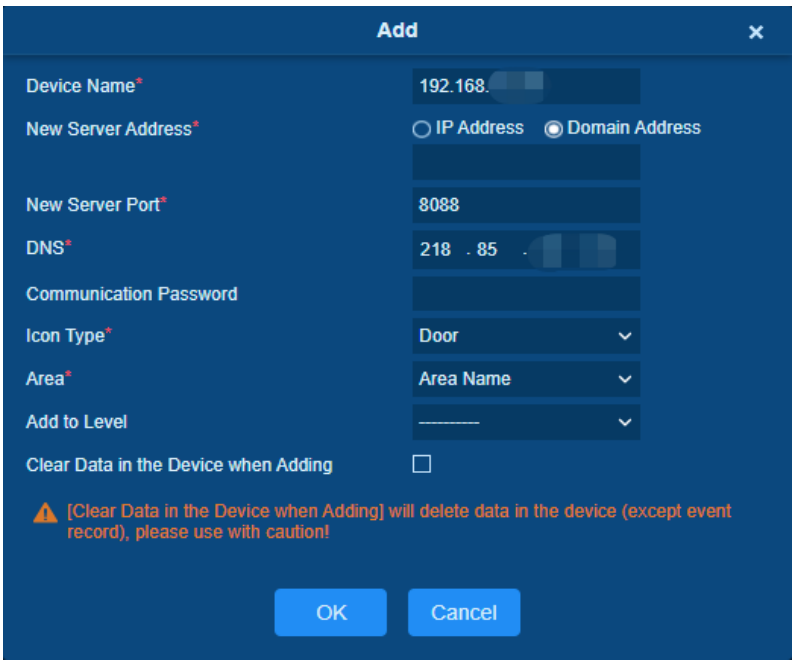
If the device is a pull device, you may input a device name, and click **[OK]** to complete device adding.



Clear Data in the Device when adding: Select this option, after adding device, the system will clear all data in the device (except the event logs).

If the device is a OmniAC Series device, the following windows will pop-up after clicking **[Add].** If IP Address in **[New Server Address]** is selected, then configure IP address and port number. If Domain Address in **[New Server Address]** option is selected, then configure domain address, port number and DNS. Device will be added to the software automatically.





New Server Address: Devices can be added to the software by entering the domain address or IP address.

New Server Port: Set the access point of system.

DNS: Set the DNS address of the server.

Clear Data in the Device when Adding: If this option is selected, then after adding device, the system will clear all data in the device (except the event logs). If you add the device merely for demonstration or testing, there is no need to select it.

✍**Note:**

When using either of the above three device adding methods, if there exist residual data in the original device, please sync original data to it after adding a new device to the software by clicking **[Device]** > **[Synchronize All Data to Devices],** otherwise these original data may conflict with normal usage.

The default IP address of the access device may conflict with the IP of a device on the Local network.

You can modify its IP address: click **[Modify IP Address]** beside the **[Add]** and a dialog box will pop up in the interface. Enter the new IP address and other parameters (Note: Configure the gateway and IP address in the same net segment).

✍**Note:**

Some OmniAC Series Device support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

Horizon Series Controller

Horizon Series Controller include AHSC-1000/AHDU-1160

Security Level

Now System support three security level for adding **Horizon Series Controller**

- **Low Security Level: MQTT without SSL authentication**

  Only Verify pre-shard keys which does not use certificate at all.

- **Normal Security Level: MQTTs, One-Way SSL authentication**

  Server (broker) only authentication. In this case the client connects to the server (broker), the broker sends its certificate to the client. The client checks the certificate is issued (signed) by somebody the client trusts, this proves the server (broker) is who it claims to be and can be trusted. The client and server (broker) then do key negotiation to set up an encrypted tunnel. The act of checking that the server certificate is issued by a trusted party is to check it is signed by a known CA (certificate authority) certificate, this means the client needs to keep a list of trusted certificates.

- **High Security Level: MQTTs, Two-Way SSL authentication**

  Mutual authentication of both client and server (broker). This is pretty much the same as before except the client also sends its own unique certificate to the server (broker) this is also checked to see that it is issued by a known CA and the CN field is used as the user id of the client.

✍**Note:**

System Default is use Normal Security Level. Low and High Security Level need to change some settings for software, need contact technical support for help. Manual Below is about Normal Security Level.

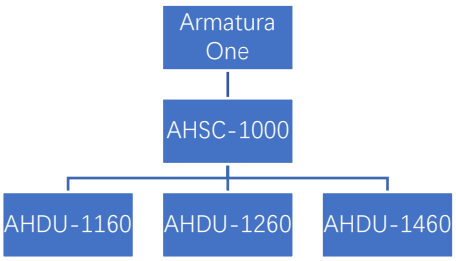
Device Model

- AHSC-1000: Primary Controller
- AHDU-1X60: Distributed Controller

Management Mode

- Master-Slave Mode

There are two types of connection, one is TCP/IP, another is RS-485.

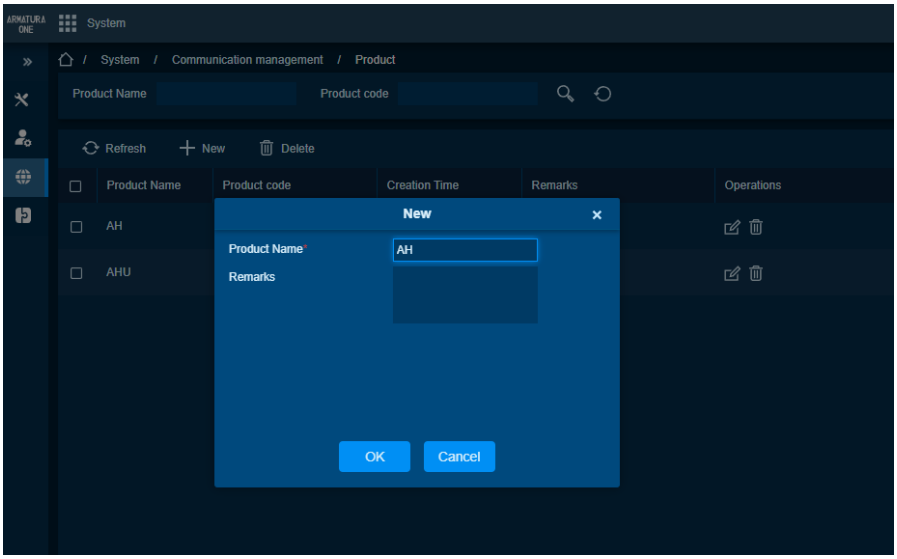


➢ Connect AHDU-1X60 to AHSC-1000 via TCPIP

Step 1 Add Primary Controller

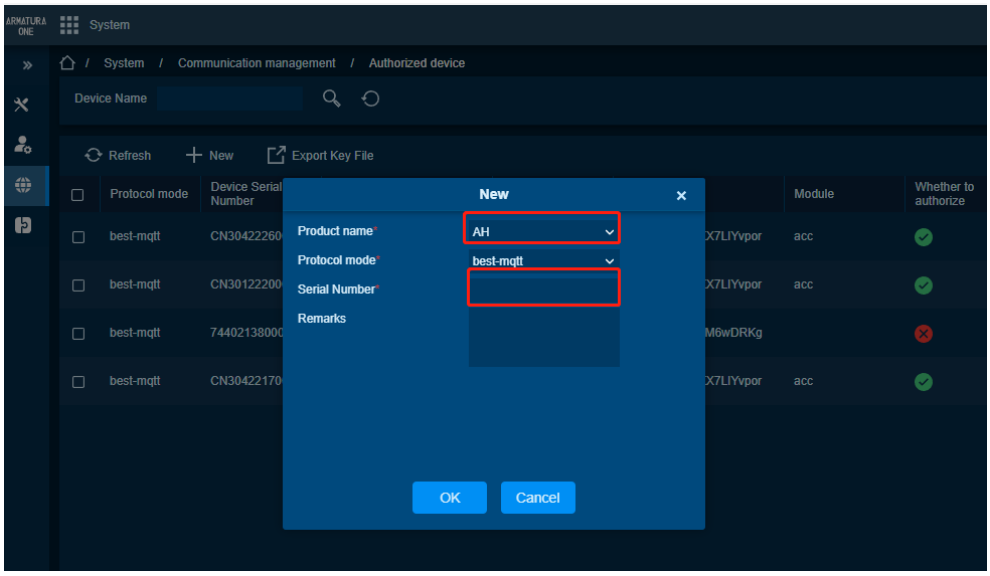
1. Add a product

In **[System]** > **[Communication Management]** > **[Product]**, Click New Button.



2. Add a device

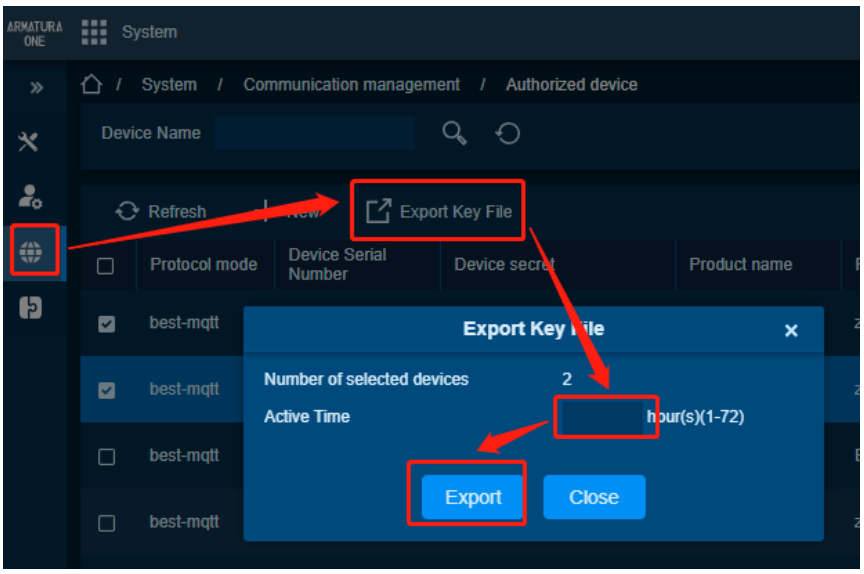
In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click New Button



Select Product just now created, then input serial number

3. Export Key File

In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click 'Export Key File' Button

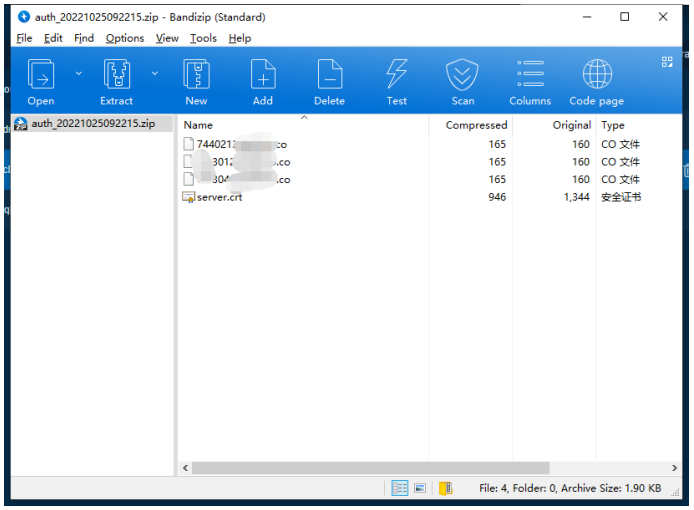


Active time Key file validity, value can be 1-72 Hours

After click Export Button, browser will download a .zip file.

✍**Note:**

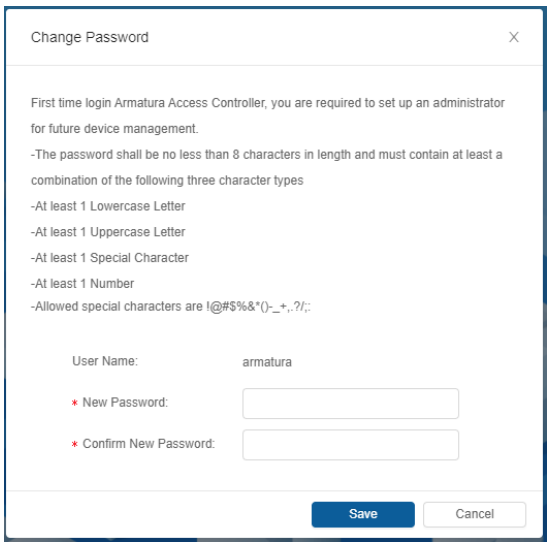
This function support selects multiple devices and click icon, it will generate all controllers .co file and server certificate in a .zip package, just upload this .zip package to controller webserver.



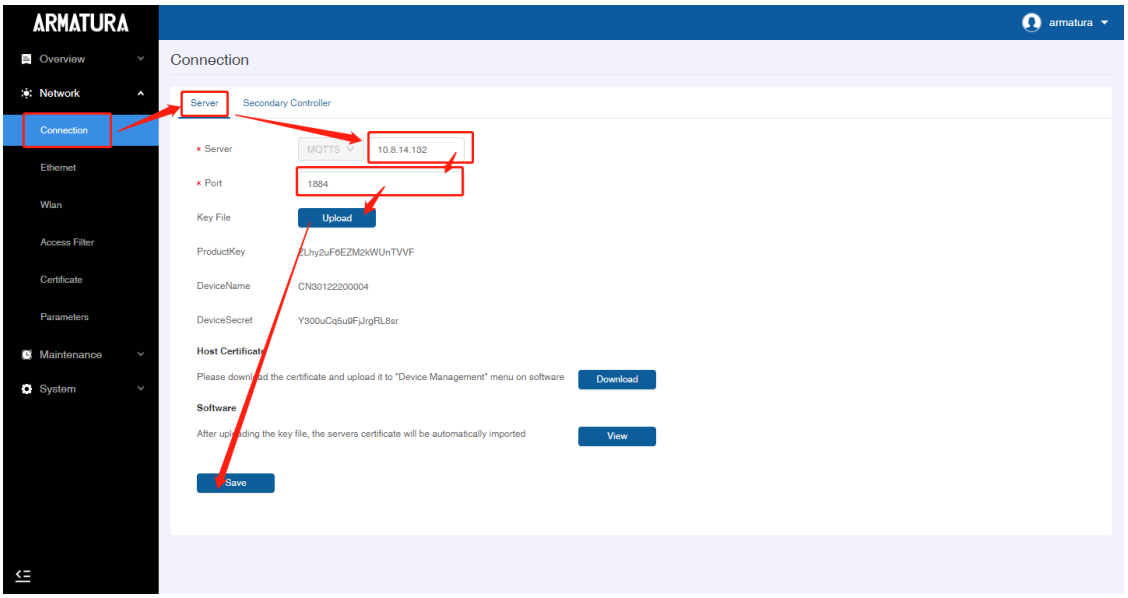
4. Import Key file to controller

Open https:// [controller's IP address] in browser

First time login username and password are armatura. When login will require to change the password for admin.



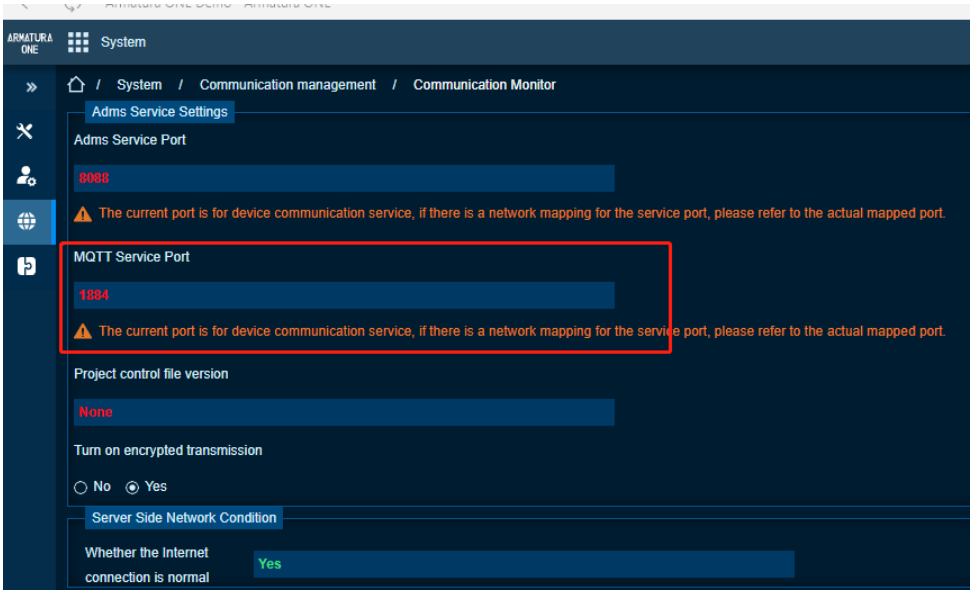
Open **[Network]** > **[Connection]**



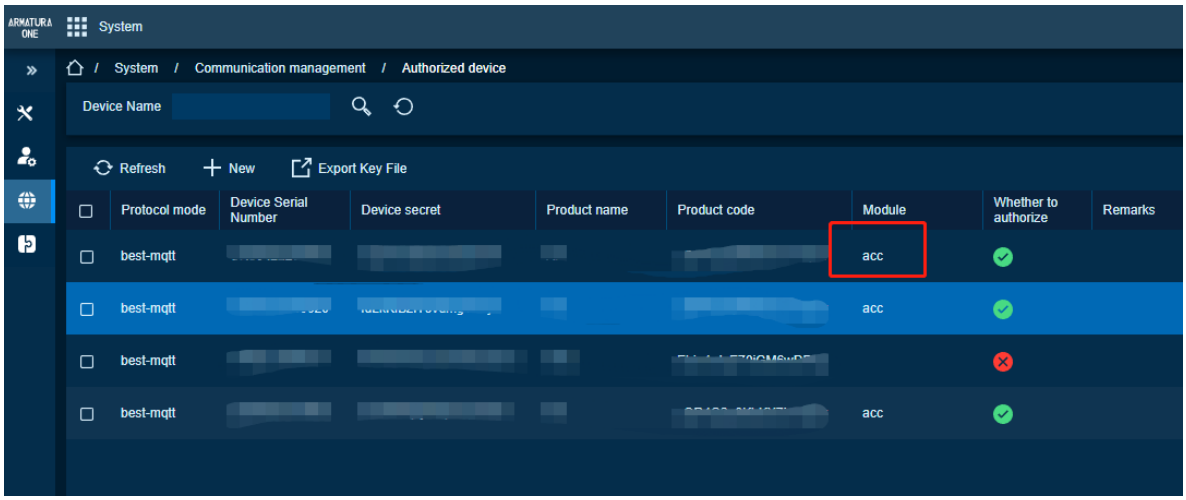
Click ‘Server’ Tab

Server Default is MQTTs protocol, address is the server address

Port Default is 1884, this port can check by **[System]** > **[Communication Management]** > **[Communication Monitor]**, **[ADMS Service Settings]** >**[MQTT Service Port]**



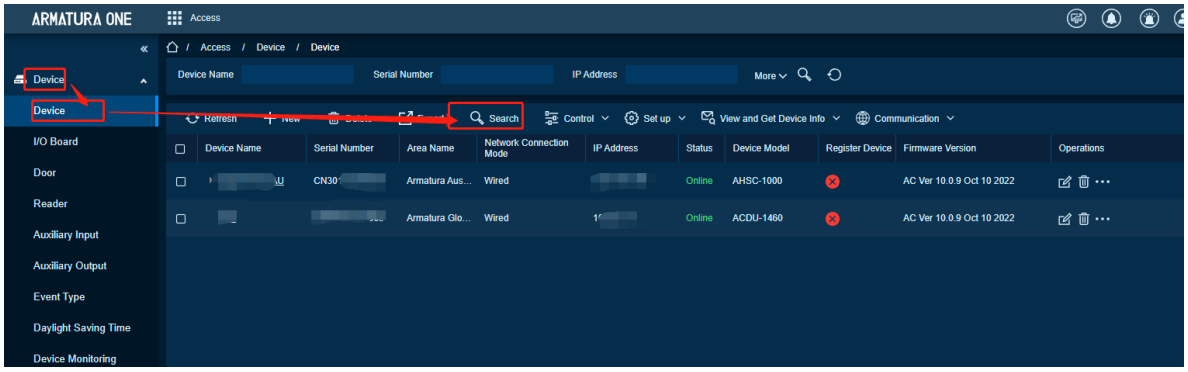
Key File This file is exported from **[System]** > **[Communication Management]** > **[Authorized Device]**



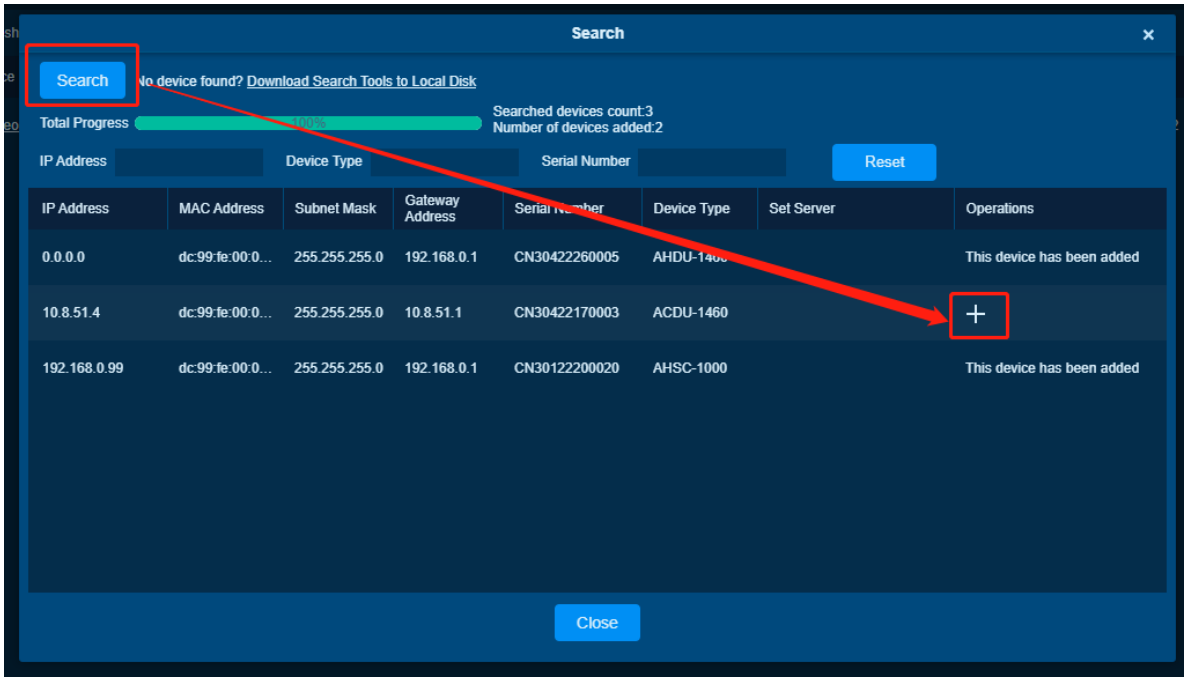
After controller connect to MQTT successfully, Column Module will show ‘acc’. Because device has not authorized to Access Module, will show  .

5. Add Controller in **[Access]** Module

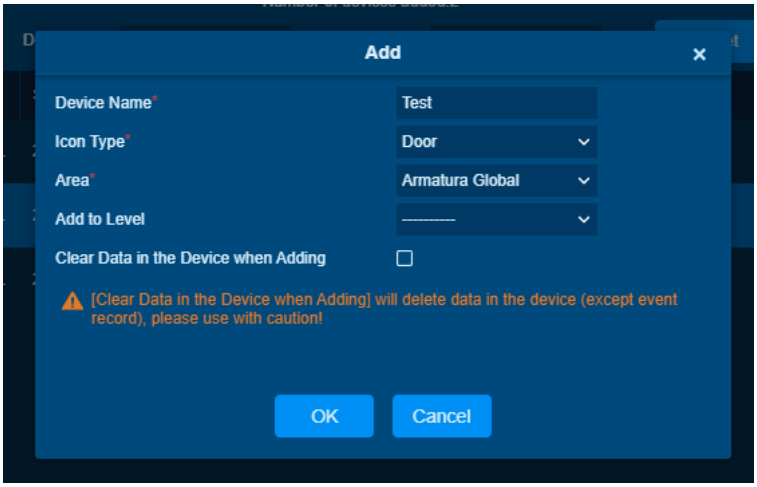
In **[Access]** > **[Device]** > **[Device]**, Click Search Button



In **[Search]** Window. Click search



In **[Add]** window

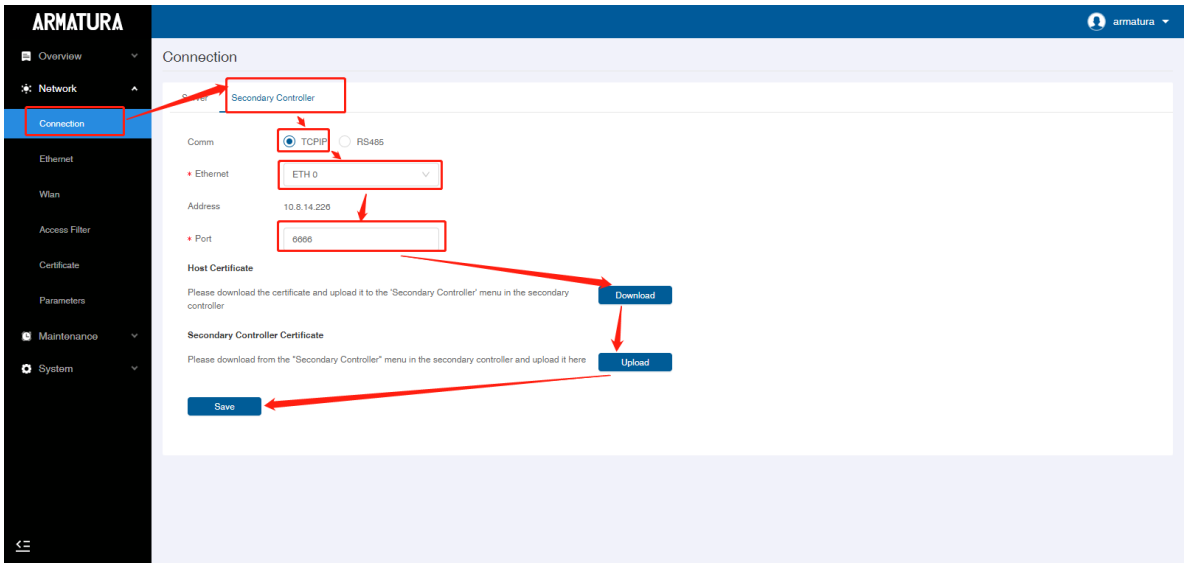


✍**Note:**

Suggest select [Clear Data in Device when Adding] to clear device data.

Step 2 Set Secondary Controller Communication Port

In **[Network]** > **[Connection]**



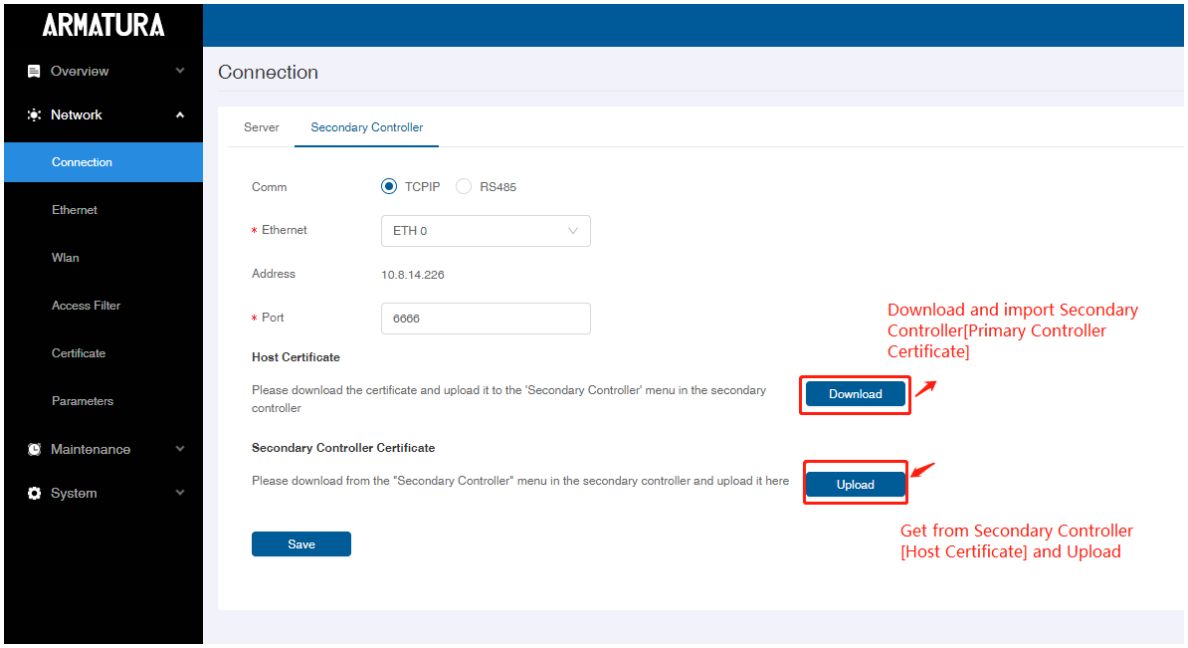
Select TCPIP radio button in Comm

Ethernet Select 'Eth 0' or 'Eth 1'

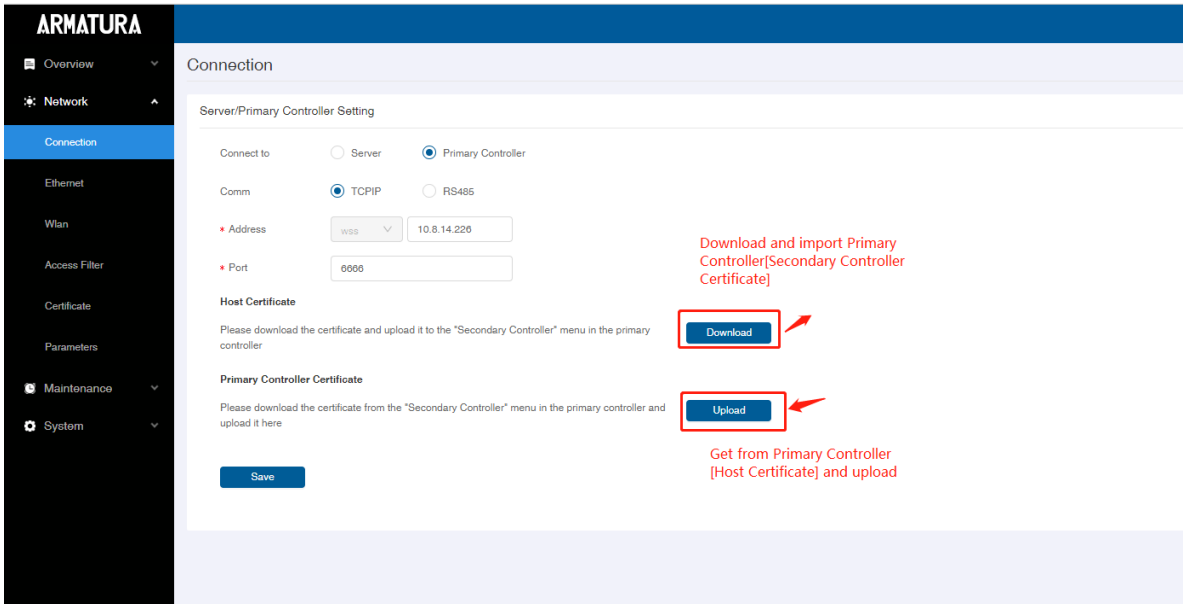
Address Will show IP address to confirm after select

Port This is a port for secondary controller to use WSS protocol to connect.

Primary Controller: Download [Host Certificate] and Upload in Secondary Controller Page [Primary Controller Certificate]

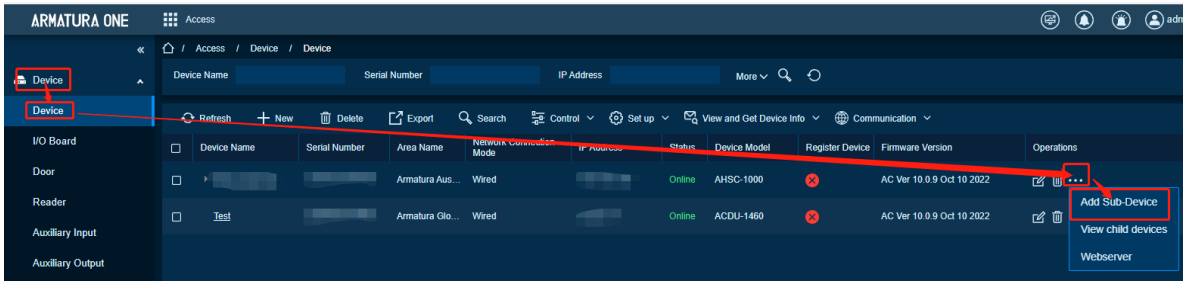


Secondary Controller: Download [Host Certificate] and Upload in Primary Controller Page [Secondary Controller Certificate]



After upload certificate each other, then add secondary controller.

Step 3 Add Secondary Controller

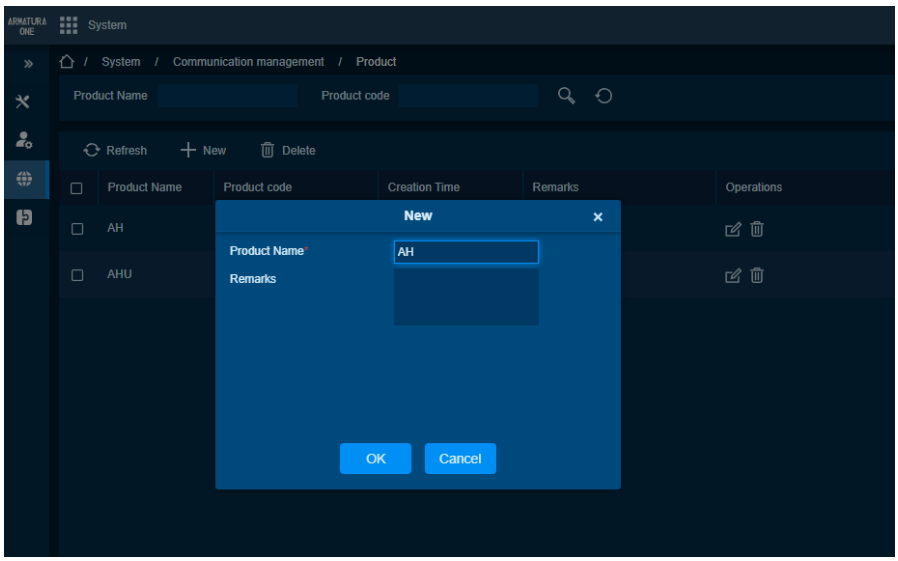


➢ Connect AHDU-1X60 to AHSC1000 via RS-485

Step 1 Add Primary Controller

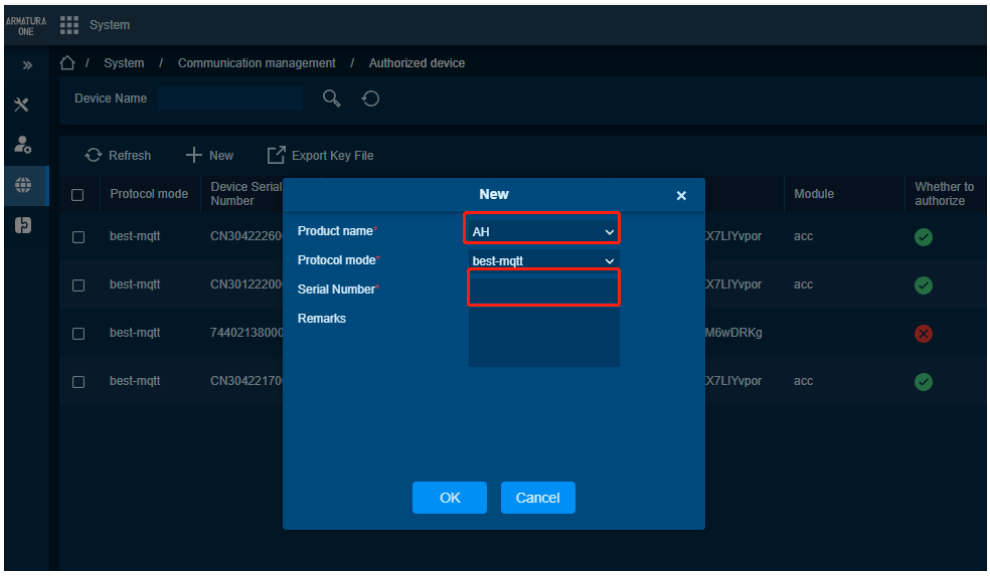
1. Add a product

In **[System]** > **[Communication Management]** > **[Product]**, Click New Button.



2. Add a device

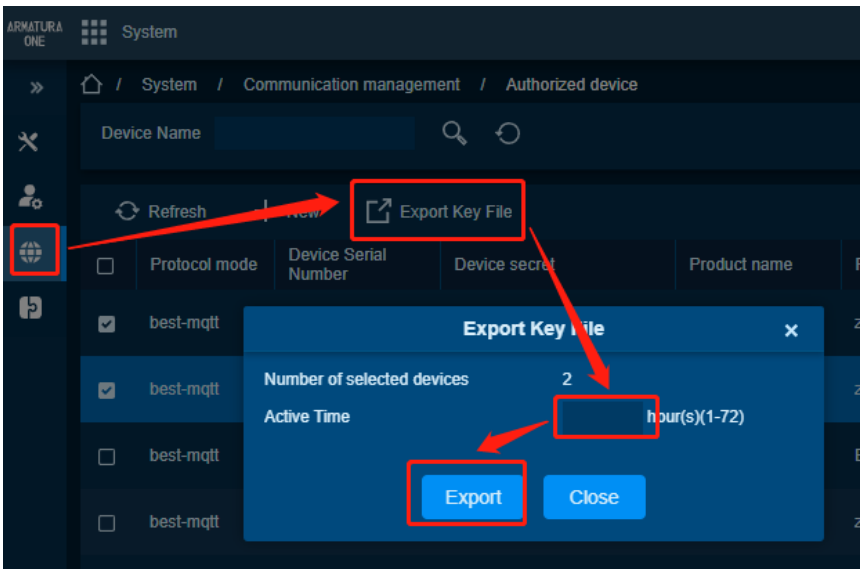
In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click New Button



Select Product just now created, then input serial number

3. Export Key File

In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click 'Export Key File' Button

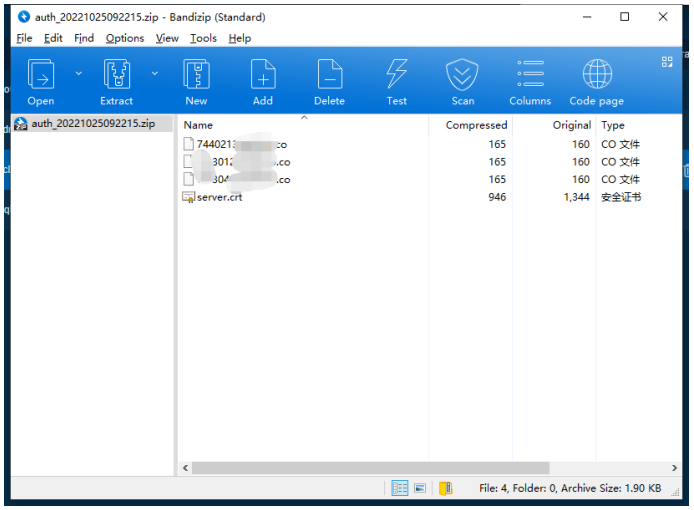


Active time Key file validity, value can be 1-72 Hours

After click Export Button, browser will download a .zip file.

✍**Note:**

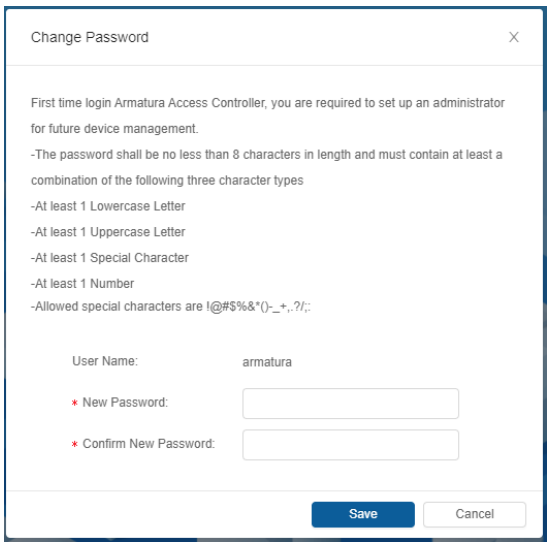
This function support selects multiple devices and click icon, it will generate all controllers .co file and server certificate in a .zip package, just upload this .zip package to controller webserver.



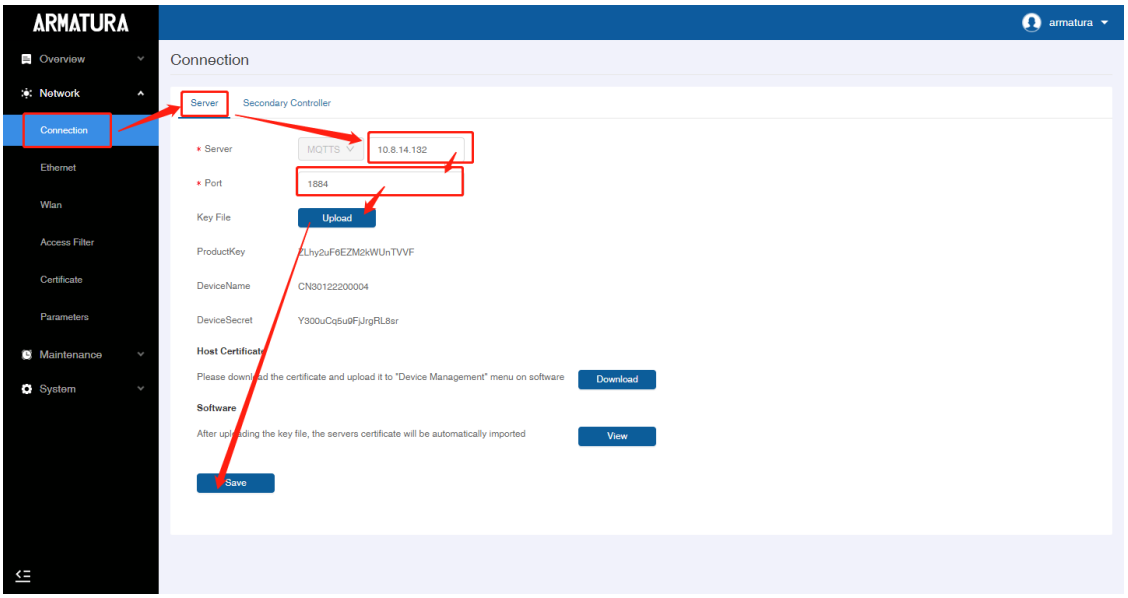
4. Import Key file to controller

Open https:// [controller's IP address] in browser

First time login username and password are armatura. When login will require to change the password for admin.



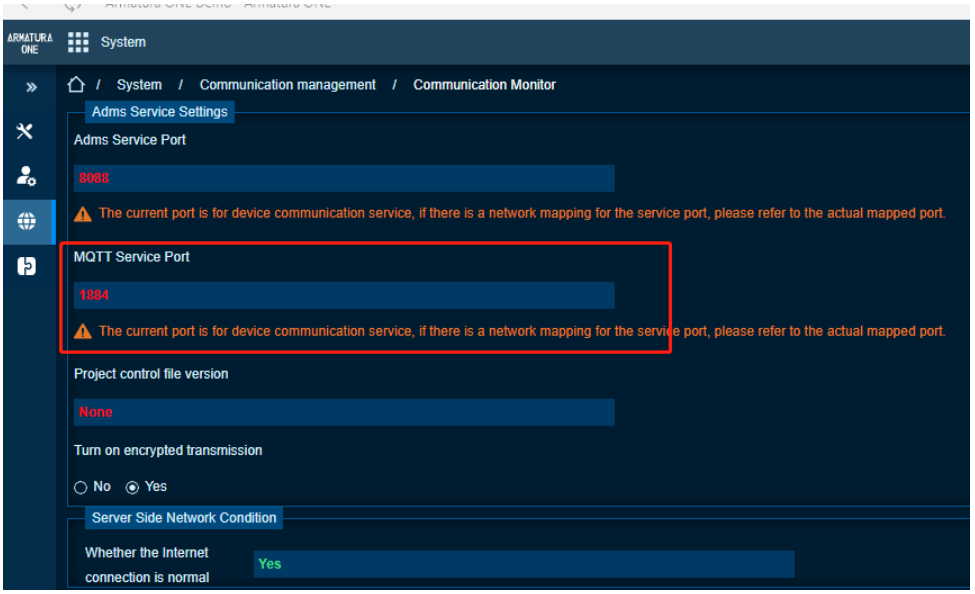
Open **[Network]** > **[Connection]**



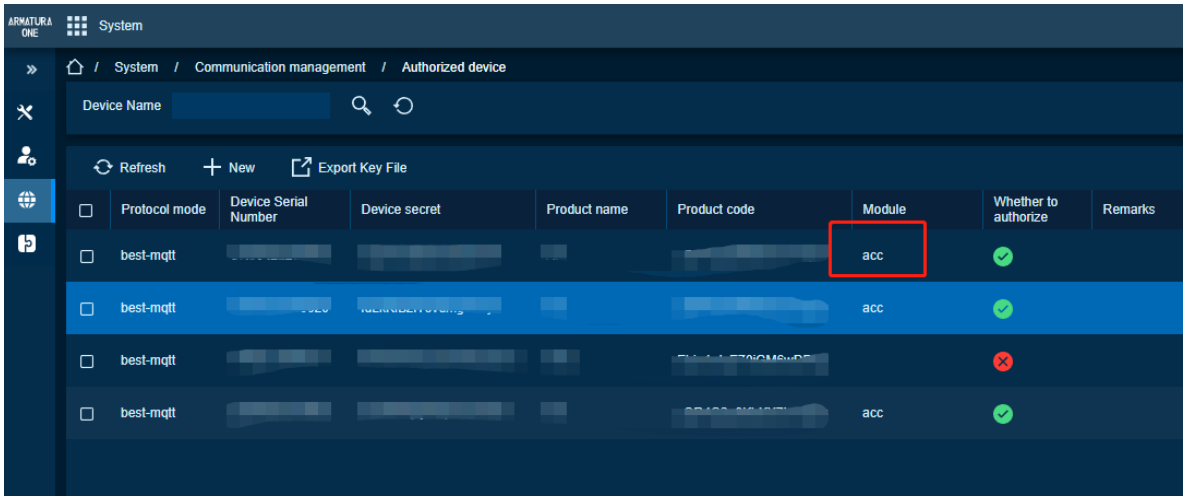
Click ‘Server’ Tab

Server Default is MQTTs protocol, address is the server address

Port Default is 1884, this port can check by **[System]** > **[Communication Management]** > **[Communication Monitor]**, **[ADMS Service Settings]** >**[MQTT Service Port]**



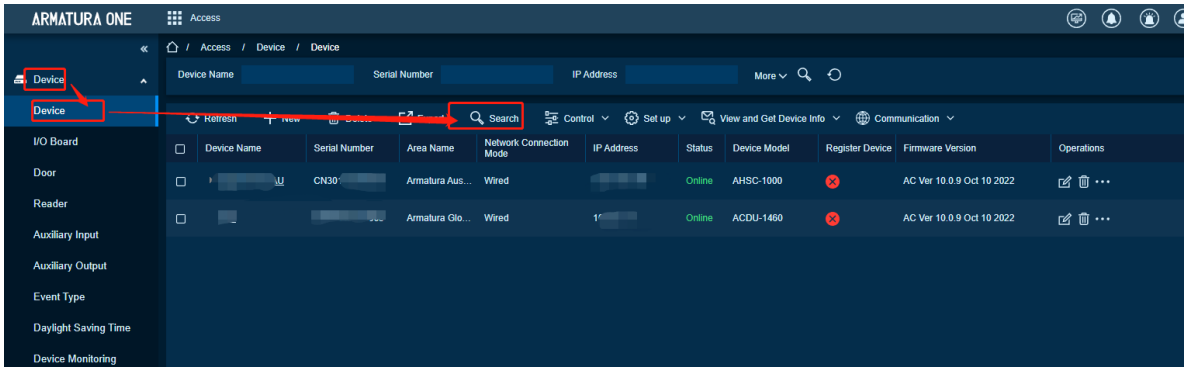
Key File This file is exported from **[System]** > **[Communication Management]** > **[Authorized Device]**



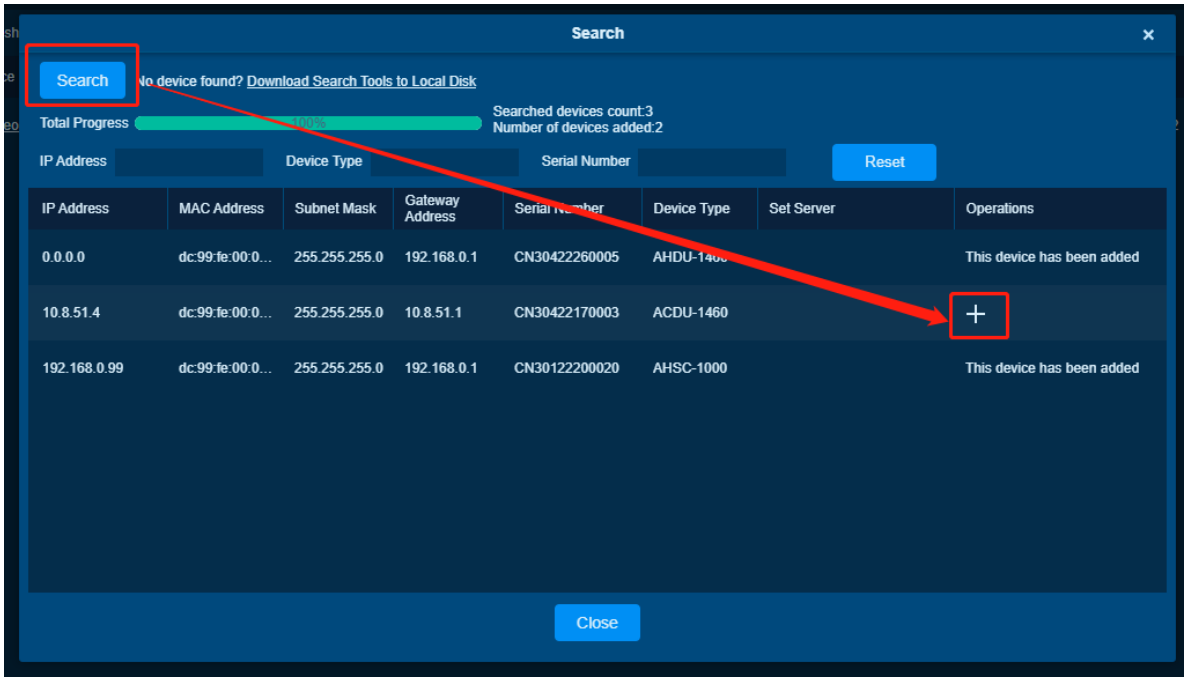
After controller connect to MQTT successfully, Column Module will show ‘acc’. Because device has not authorized to Access Module, will show  .

5. Add Controller in [Access] Module

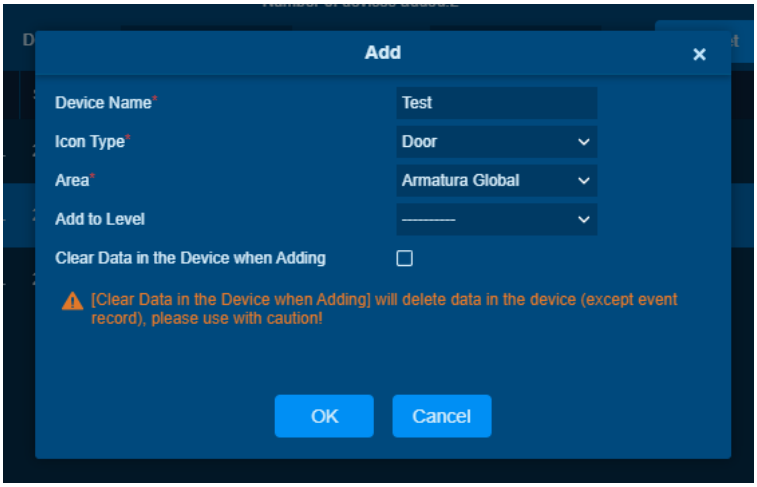
In **[Access]** > **[Device]** > **[Device]**, Click Search Button



In **[Search]** Window. Click search



In **[Add]** window

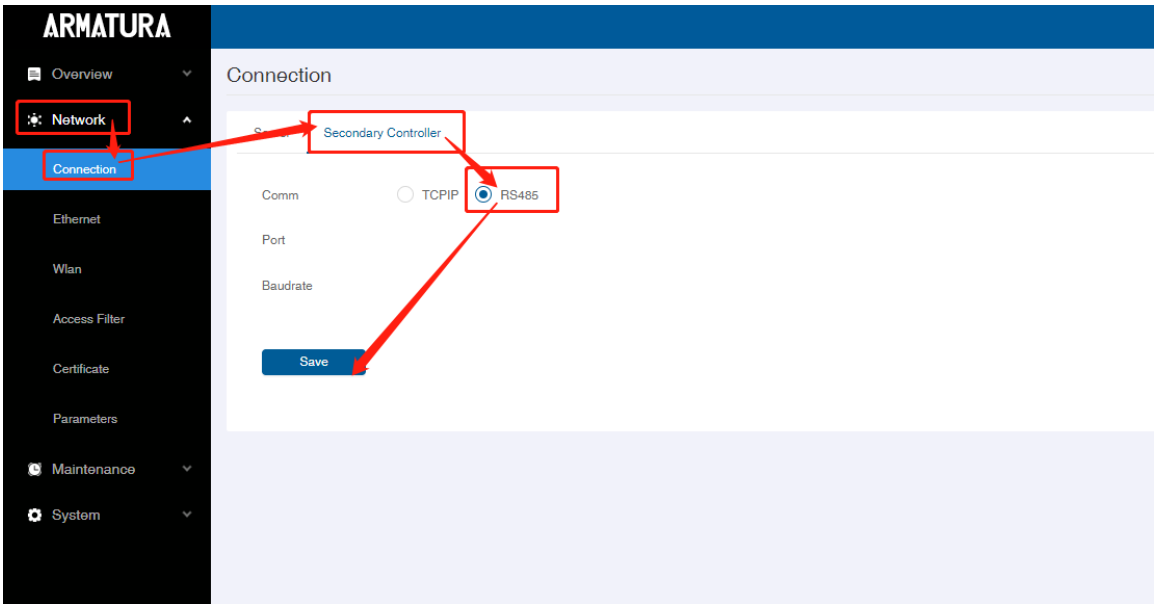


✍**Note:**

Suggest select [Clear Data in Device when Adding] to clear device data.

Step 2 Set Secondary Controller Communication Port

In **[Network]** > **[Connection]**, Secondary Controller Tab



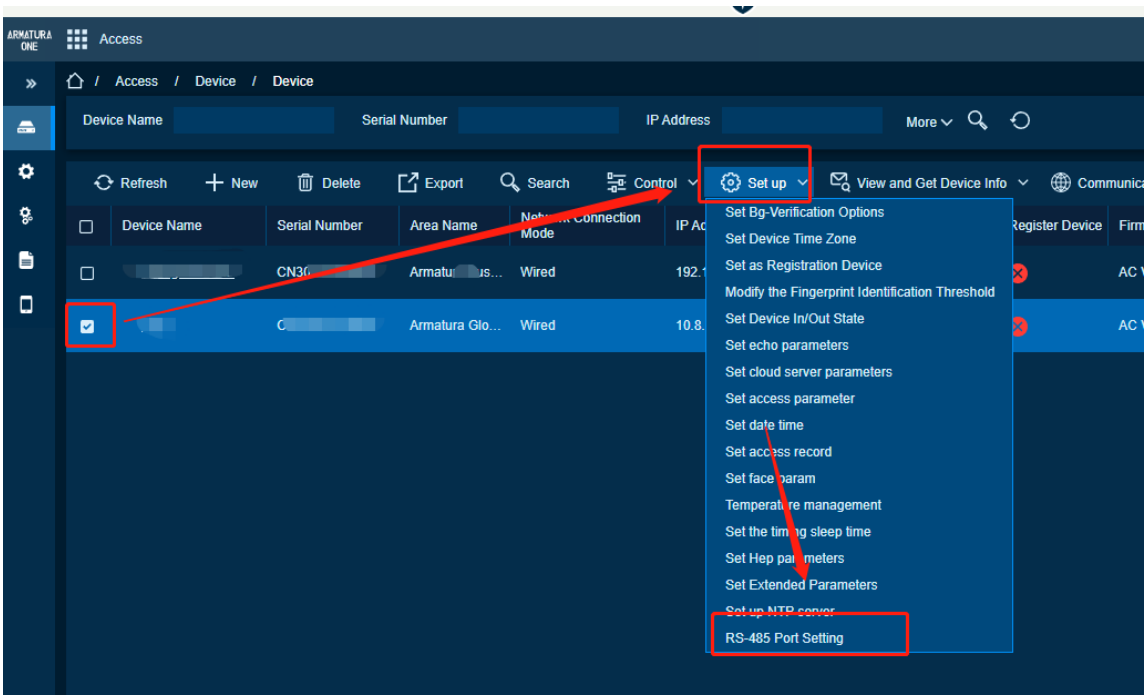
Select RS-485 radio button in Comm

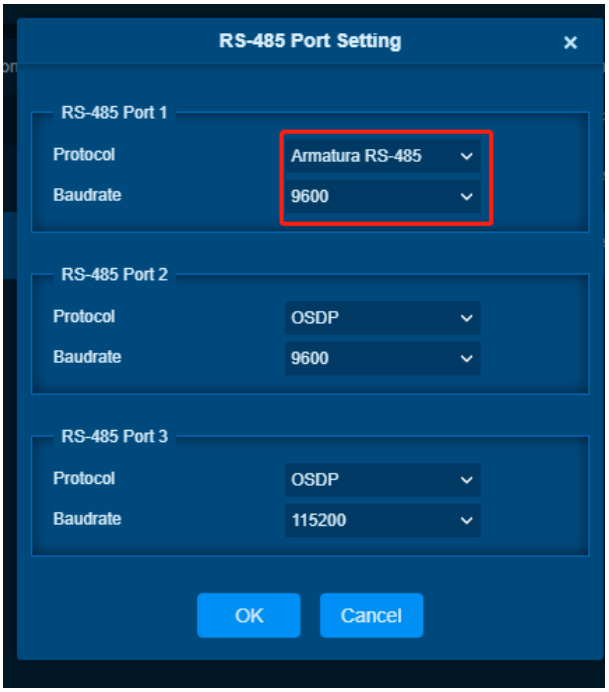
Port This is RS-485 port for secondary controller to connect. This depends on which port is set Armatura RS-485 in RS-485 Port Settings.

Baudrate This is parameter for RS-485 communication. This depends on which port is set Armatura RS-485 in RS-485 Port Settings.

Click Save to save options.

In software **[Access]** > **[Device]** > **[Device]**, select a device and click 'Set up' button in operation bar, click 'RS-485 Port Setting'

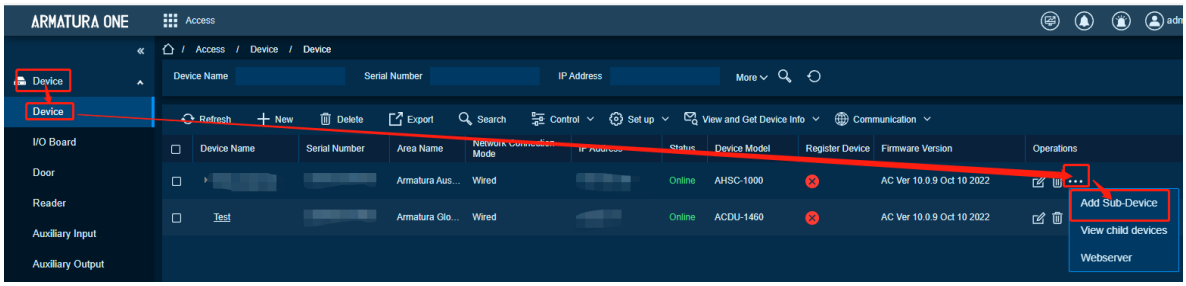




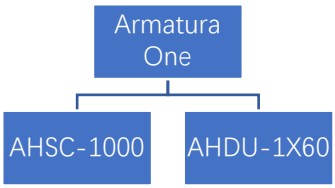
Device has three physical interface, RS-485 Port 1/Port 2/Port 3

Armatura RS-485 is the Protocol used for primary-secondary connection.

Step 3 Add Secondary Controller



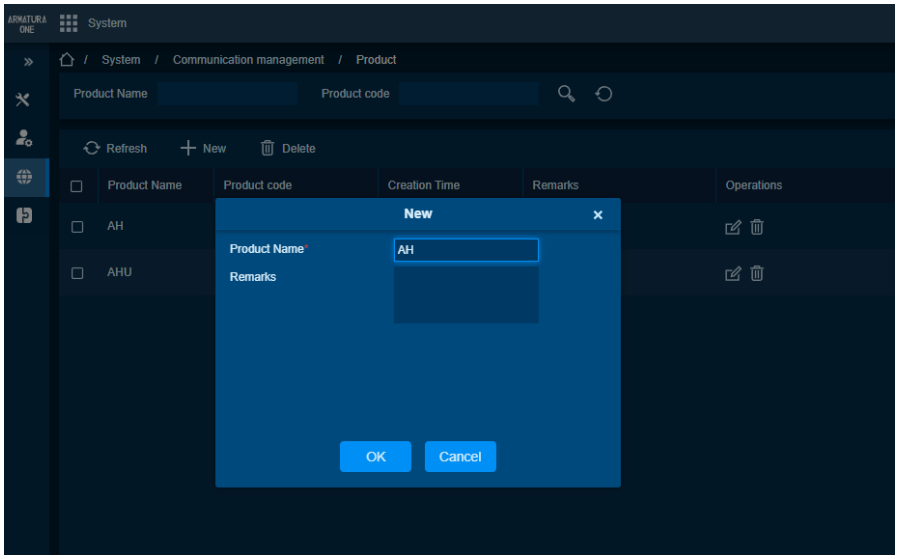
- Master Mode



Step 1 Add Primary Controller

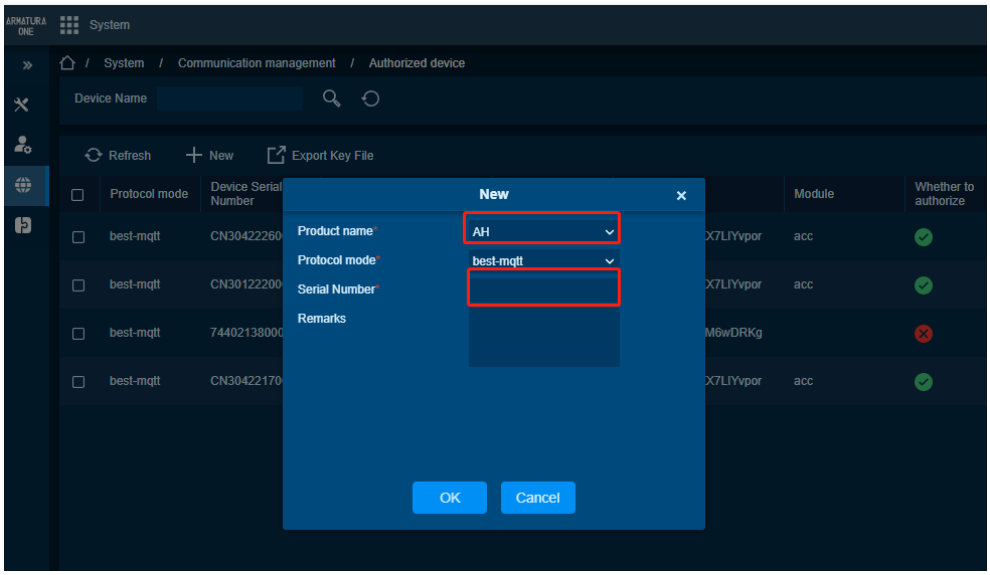
6. Add a product

In **[System]** > **[Communication Management]** > **[Product]**, Click New Button.



7. Add a device

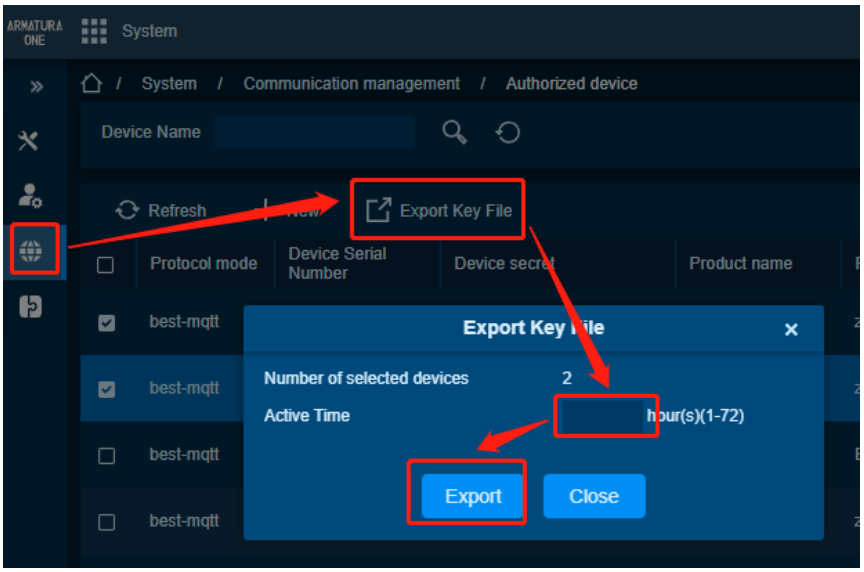
In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click New Button



Select Product just now created, then input serial number

8. Export Key File

In **[System]** > **[Communication Management]** > **[Authorized Device]**, Click 'Export Key File' Button

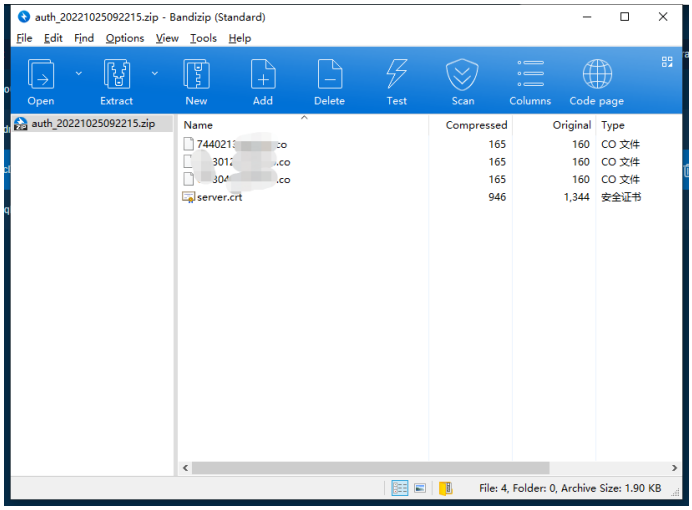


Active time Key file validity, value can be 1-72 Hours

After click Export Button, browser will download a .zip file.

✍**Note:**

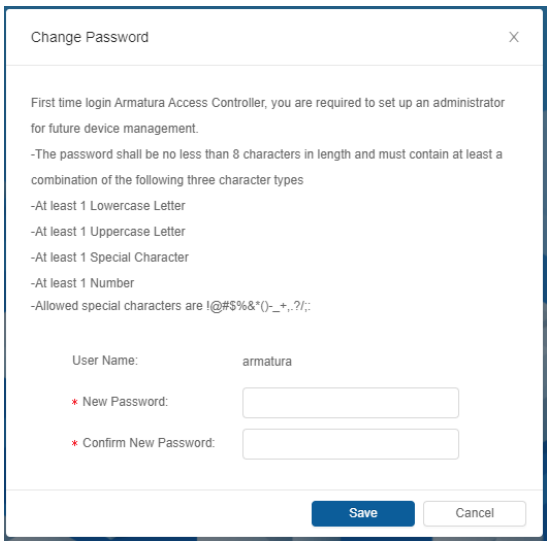
This function support selects multiple devices and click icon, it will generate all controllers .co file and server certificate in a .zip package, just upload this .zip package to controller webserver.



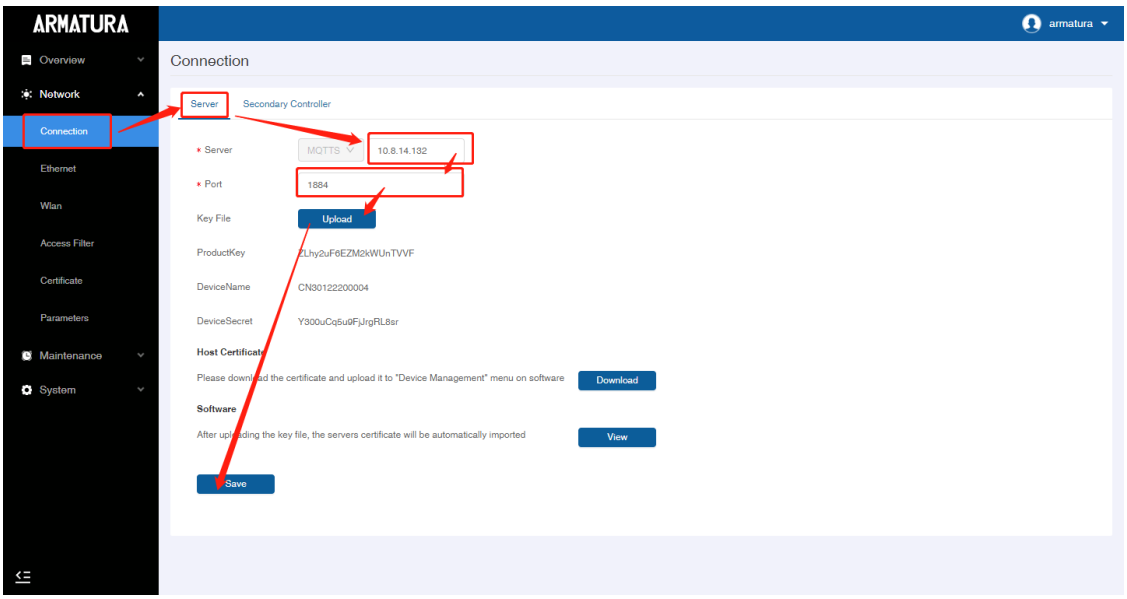
9. Import Key file to controller

Open https:// [controller's IP address] in browser

First time login username and password are armatura. When login will require to change the password for admin.



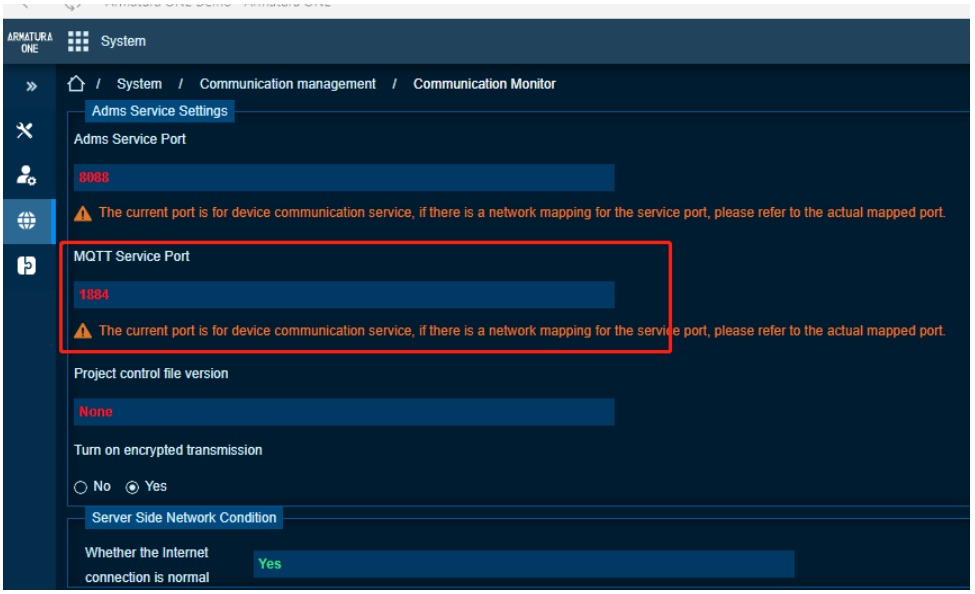
Open **[Network]** > **[Connection]**



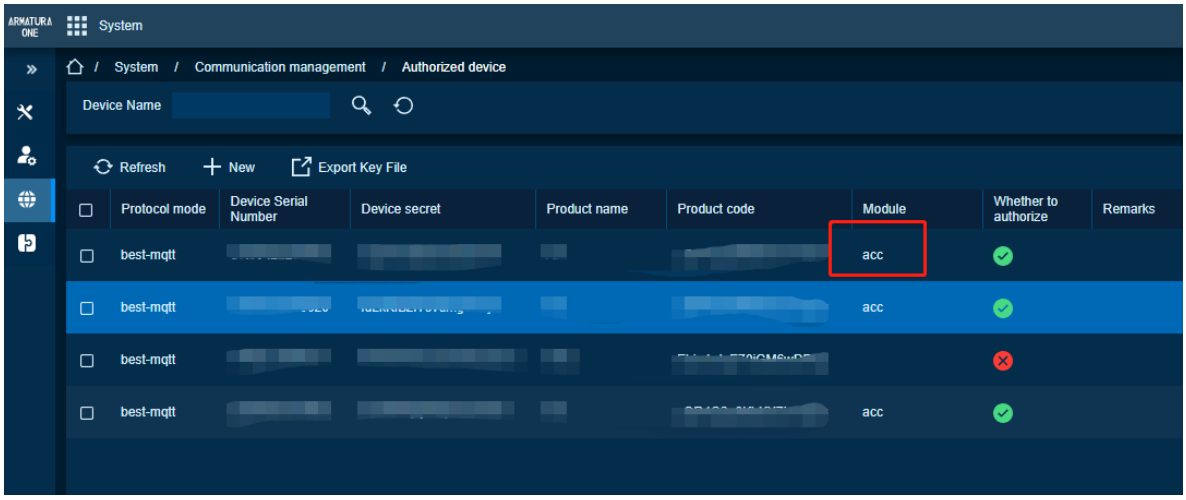
Click ‘Server’ Tab

Server Default is MQTTs protocol, address is the server address

Port Default is 1884, this port can check by **[System]** > **[Communication Management]** > **[Communication Monitor]**, **[ADMS Service Settings]** >**[MQTT Service Port]**



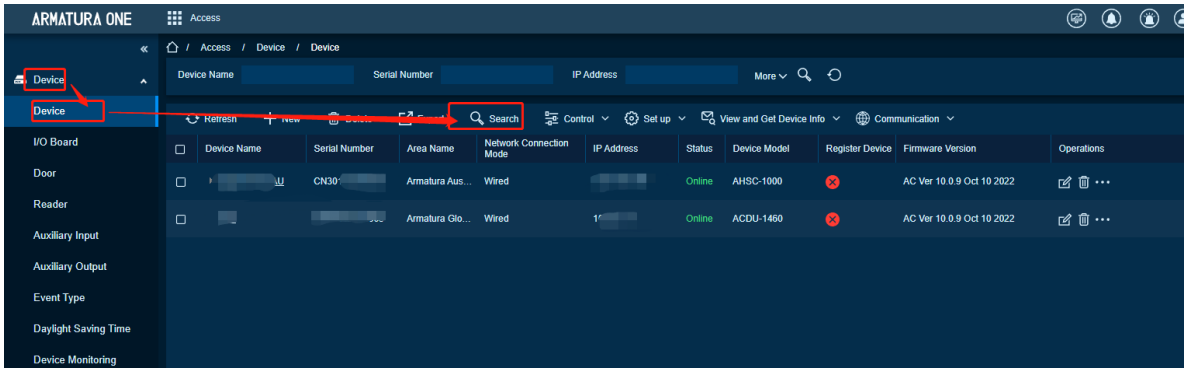
Key File This file is exported from **[System]** > **[Communication Management]** > **[Authorized Device]**



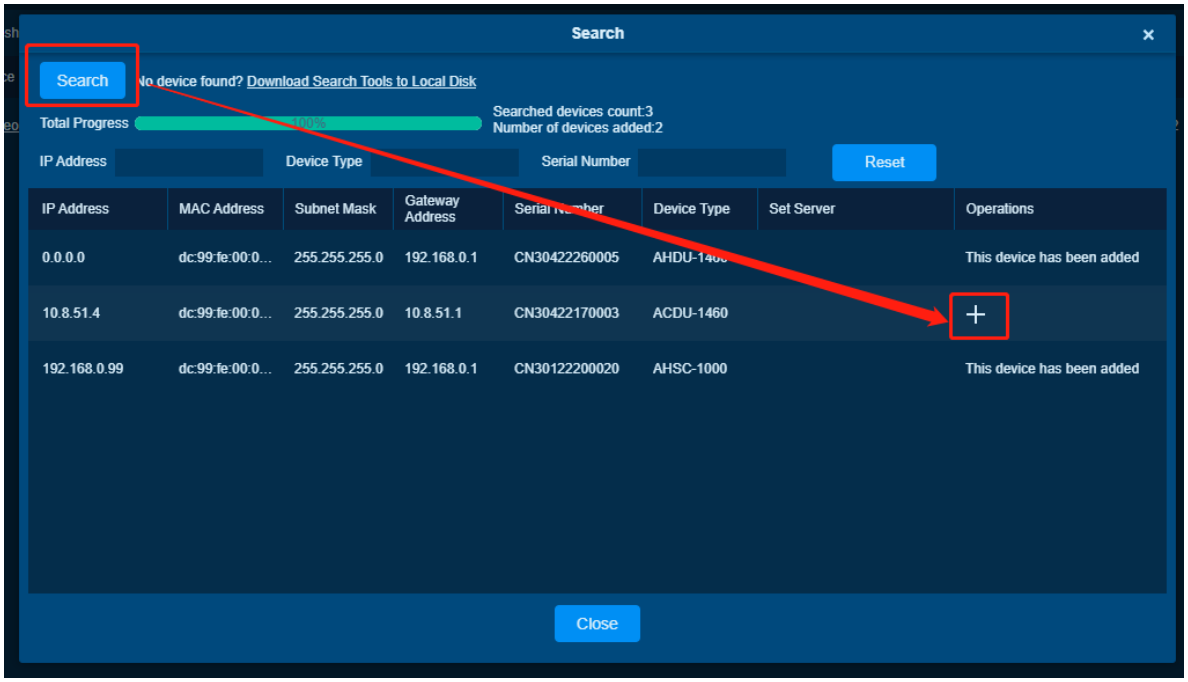
After controller connect to MQTT successfully, Column Module will show ‘acc’. Because device has not authorized to Access Module, will show  .

10. Add Controller in **[Access]** Module

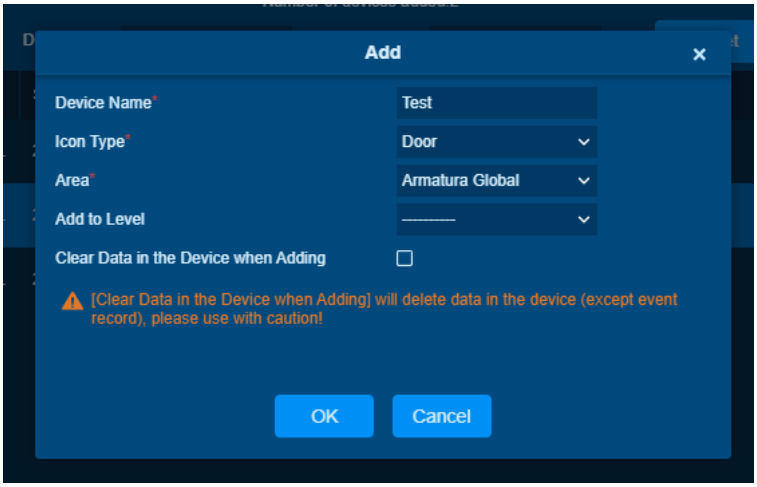
In **[Access]** > **[Device]** > **[Device]**, Click Search Button



In **[Search]** Window. Click search



In **[Add]** window



✍**Note:**

Suggest select [Clear Data in Device when Adding] to clear device data.

Delete Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.

Function Usage Scenarios

The data of the device configuration is wrong and needs to be added again

Feature Trigger Result

If Spada Protocol device, when delete from **[Access]** > **[Device]**, Device in **[system]** > **[Authorized Device]** will also delete.

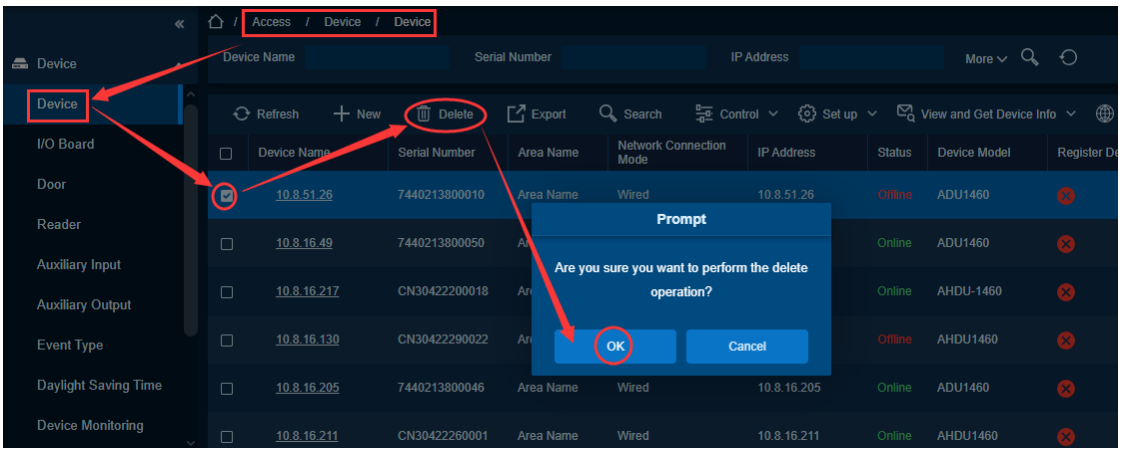
If primary controller deletes from **[Access]** > **[Device]**, secondary controller will also delete.

Limit

If device participate in anti-passback/interlock rules, will not allow to delete.

Steps:

Click **[Access Control Module] > [Device] > [Delete],** the delete page is displayed:



Export Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to operate the device. The device has been added successfully and is online.

Function Usage Scenarios

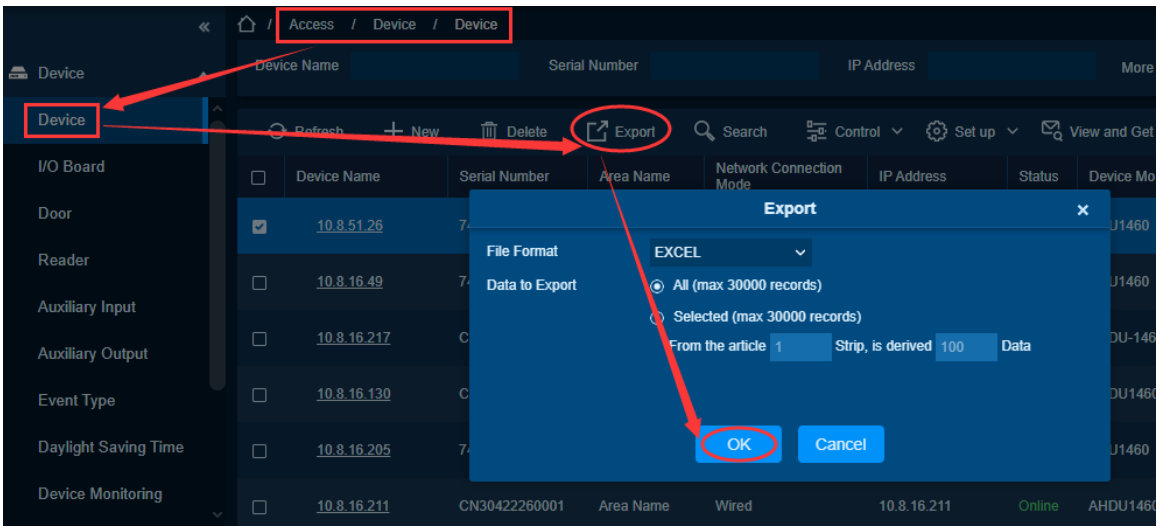
Need to view the information of have been added or added device in the device list.

Feature Trigger Result

1. Export files in Excel/PDF/CSV format. The exported content includes device name, serial number, area name, network connection mode, IP address, status, device model.

Steps:

Click **[Access Control Module]** > **[Device]** > **[Export]** to display the export page:



Device

Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Control

Clear Administrator

Preconditions for Normal Use of Functions

Log in to the system with current account. Make sure that the device is online and supports clearing administrator permissions.

Function Usage Scenarios

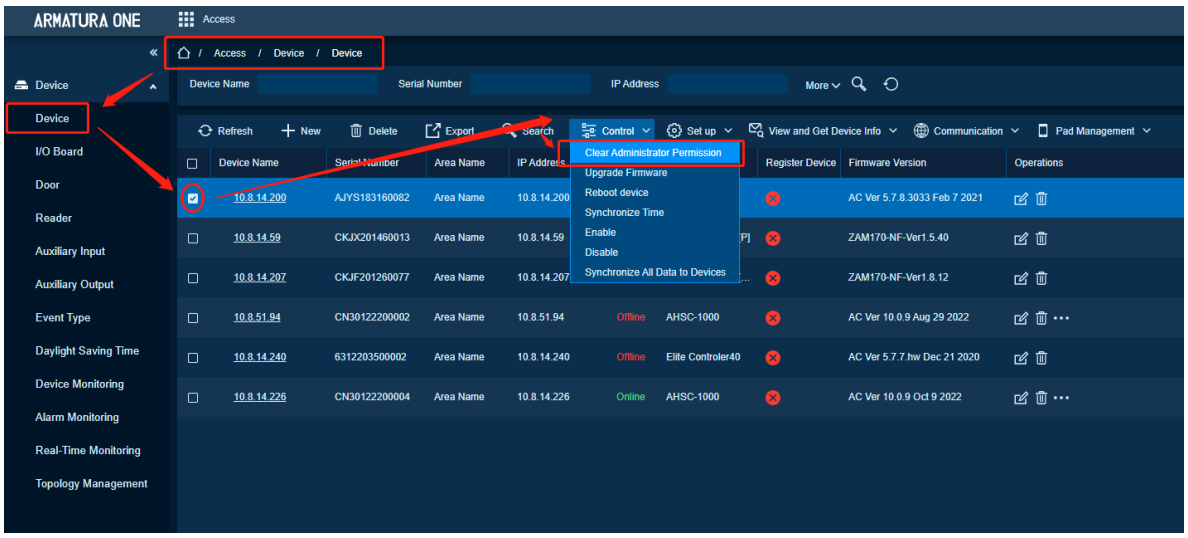
The device does not require an administrator.

Feature Trigger Result

Delete the administrator from the device

Steps:

1. Click **[Access Control Module]** > **[Device]** > **[Control]** to display the control page.
2. Click **[Clear Administrator]** to clear the administrator.



Upgrade Firmware

Precondition for Normal Use of Functions

Log in to the system with current account and have the right to upgrade the firmware. Select a device which want to upgrade.

Function Usage Scenarios

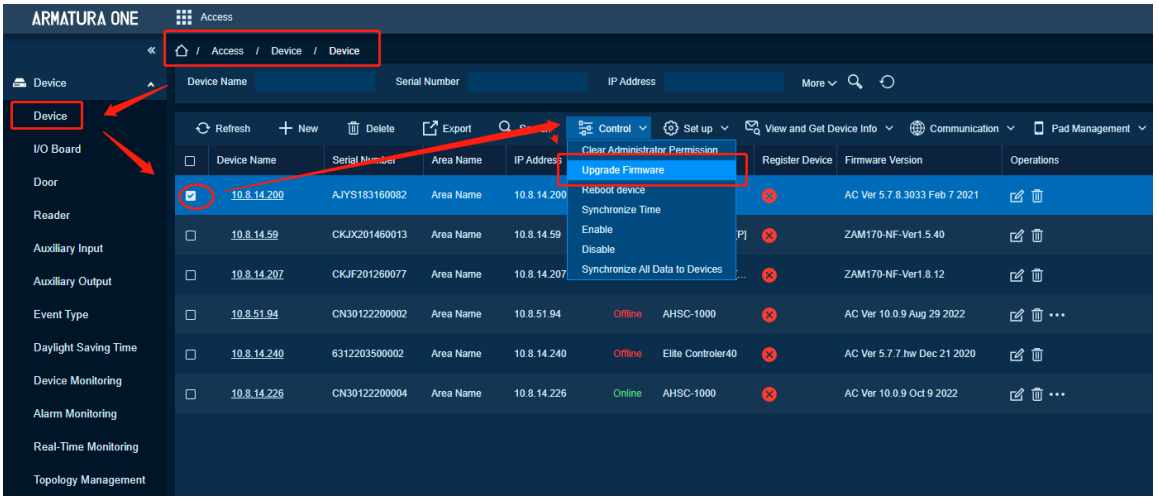
The function needed in the software is not supported in the device and needs to be upgraded again.

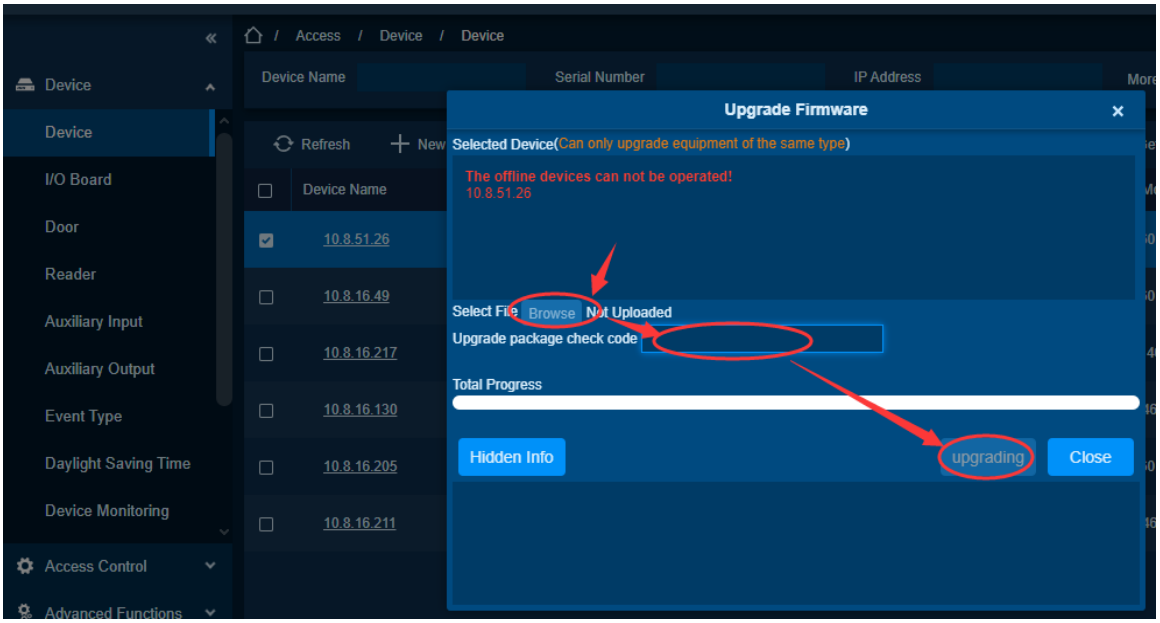
Feature Trigger Result

After the upgrade, the firmware version in the device list will also be updated. It can support the functions required by the software.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Control]** to display the control page.
- Click **[Upgrade Firmware],** click to pop up a window
- Click **[Browse]** to add the upgrade package to be upgraded. Rename firmware package as crtlfw.ar.
- Enter the **[Package Check Code]** if needed
- Click **[Upgrade]**
- Wait for the progress bar run to end once process get complete.





✍Note:

The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware or upgrade it following the instructions of the distributor. Unauthorized upgrade may affect normal operations.

Reboot Device

Preconditions for Normal Use of Functions

Log in to the system with current account. The device is online and has the right to upgrade the firmware.

Function Usage Scenarios

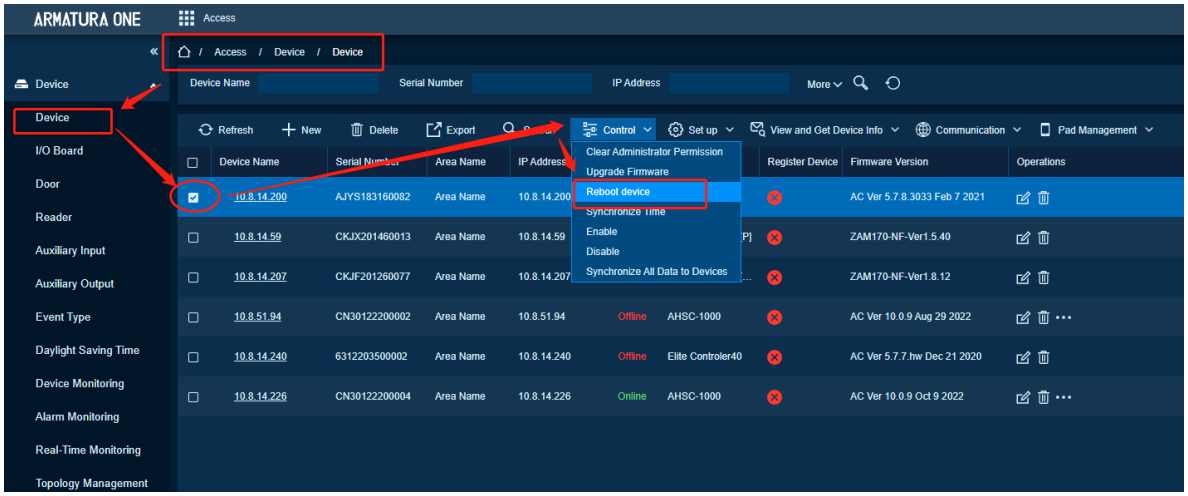
Device data error, re-upgrade, etc. need to restart the device.

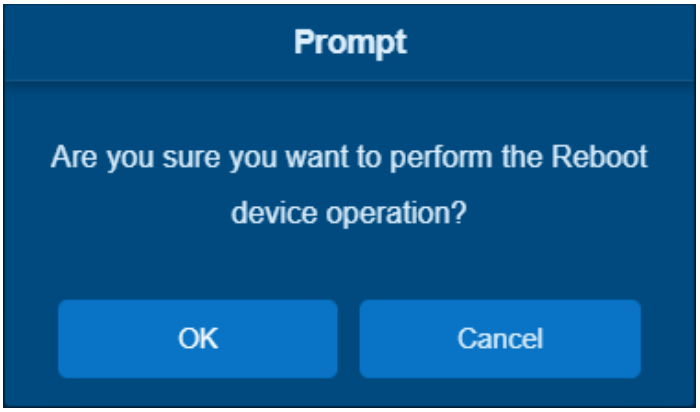
Feature Trigger Result

Restart the device: The software cannot operate when the device restarts. After the restart, the device will automatically connect to the software and go online.

Steps:

- Click **[Access Control Module] > [Device] > [Control]** to display the control page.
- Click **[Reboot Device],** click the start device interface.
- Click **[OK]** to restart the device.





Synchronize Time

Preconditions for Normal Use of Functions

Log in to the system with current account. With this authority, the device is online.

Function Usage Scenarios

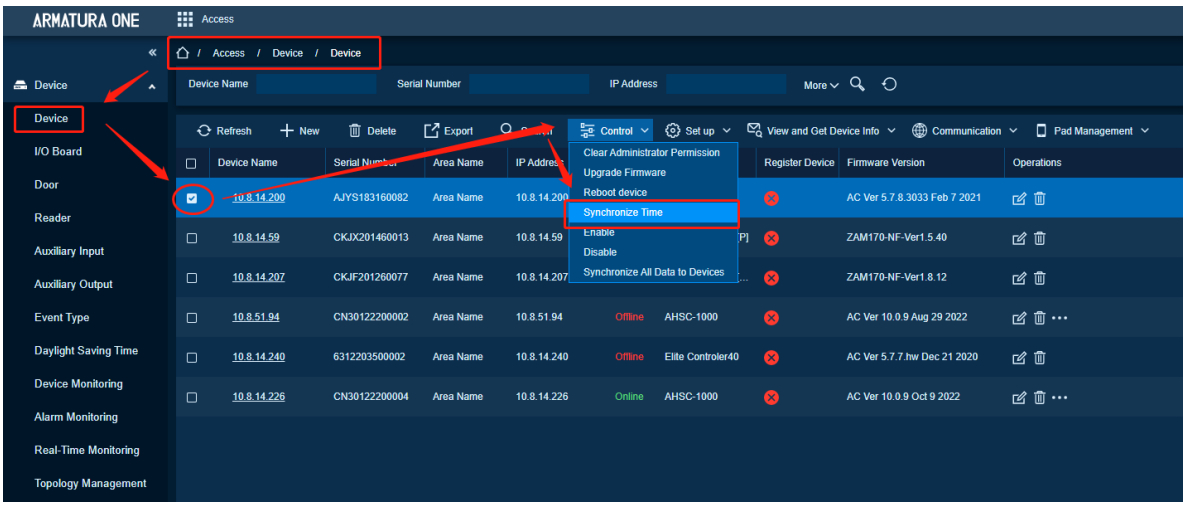
When the time between the software and the device is inconsistent.

Feature Trigger Result

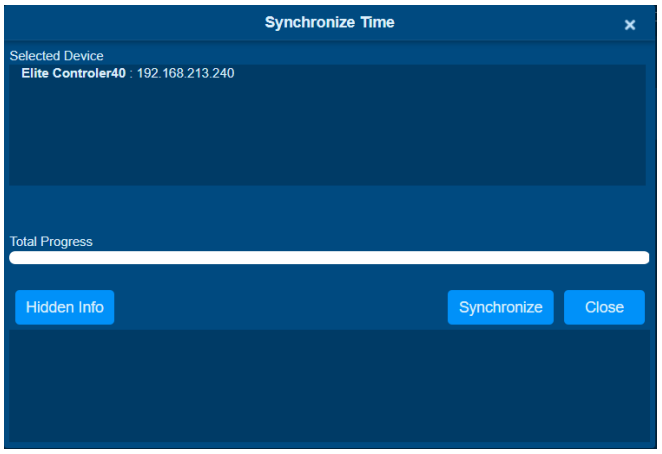
The software is consistent with the time of the connected device

Steps:

1. Click **[Access Control Device]** > **[Device]** > [**Control]** to display the control page.
2. Click **[Synchronize Time],** click to pop up the synchronization time interface.



3. On Synchronize Time interface, click Synchronize and wait until process completes.



✍Note:

If [NTP Server Time Sync] is enabled, the device sync time from the NTP server.

Secondary controller will not get time from Software/NTP server, only from Primary Controller.

Enable

Preconditions for Normal Use of Functions

Log in to the system with current account and have the authority.

Function Usage Scenarios

The device needs to be connected and operated.

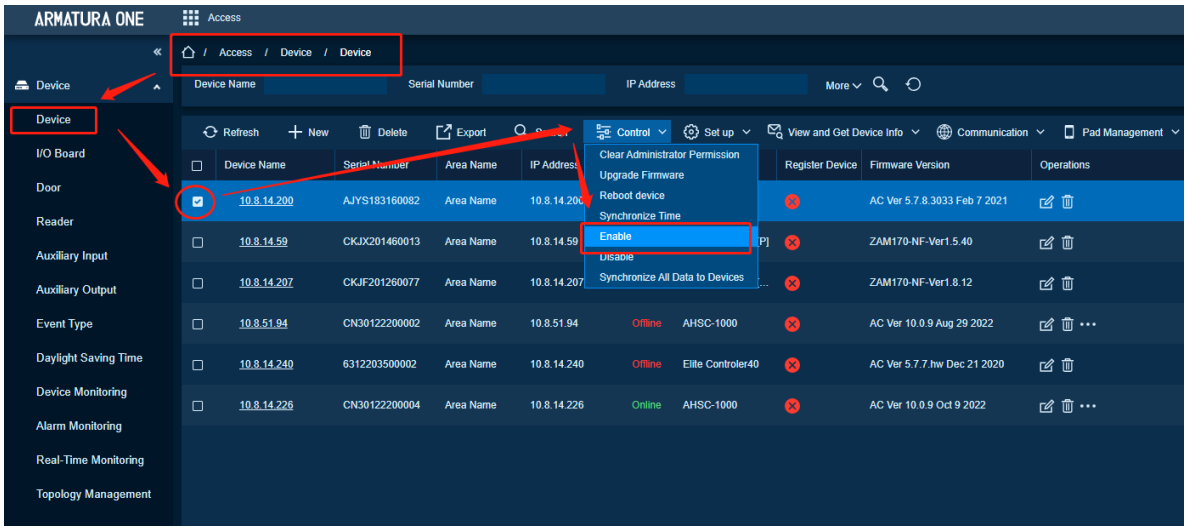
Feature Trigger Result

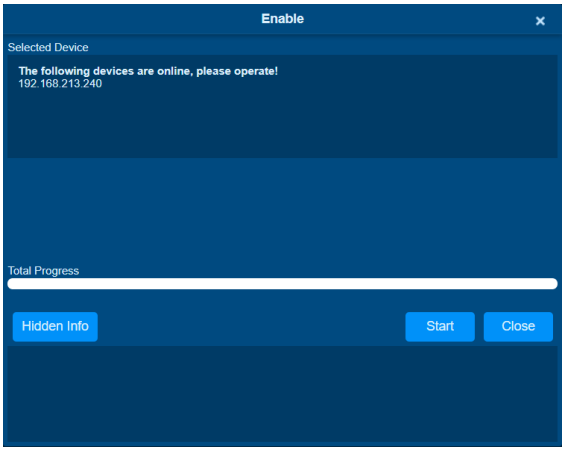
Restore device communication, you can use the device, and perform operations on the device list.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Control]** to display the control page.
- Click **[Enable]**, click to pop up the interface of enabling the device.

- Click **[Start]** to enable the device.





Disable

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority.

Function Usage Scenarios

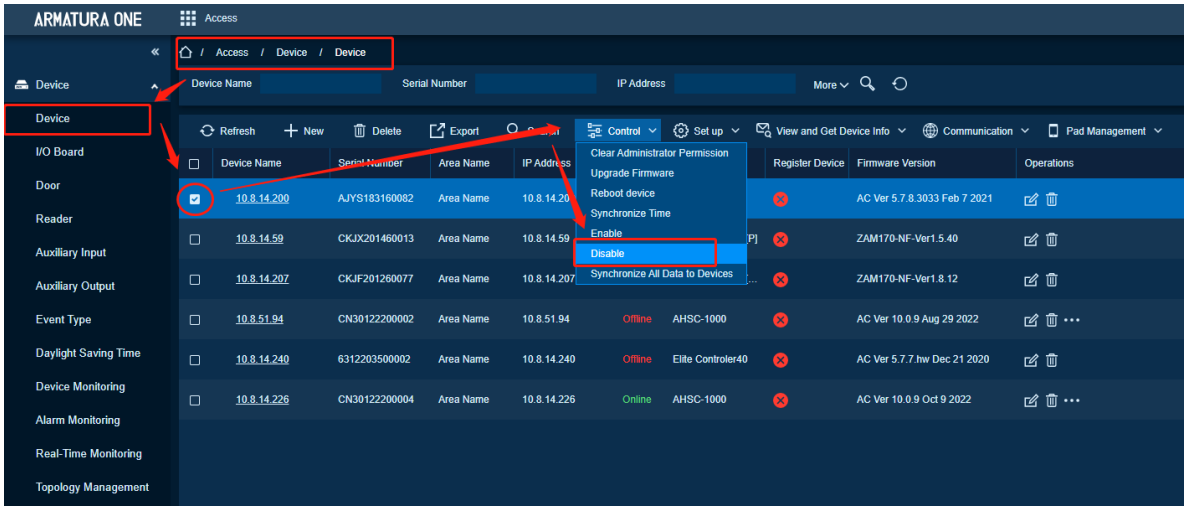
When the communication between the device and the system is interrupted or the device fails, the device may automatically display in a disabled state.

Feature Trigger Result

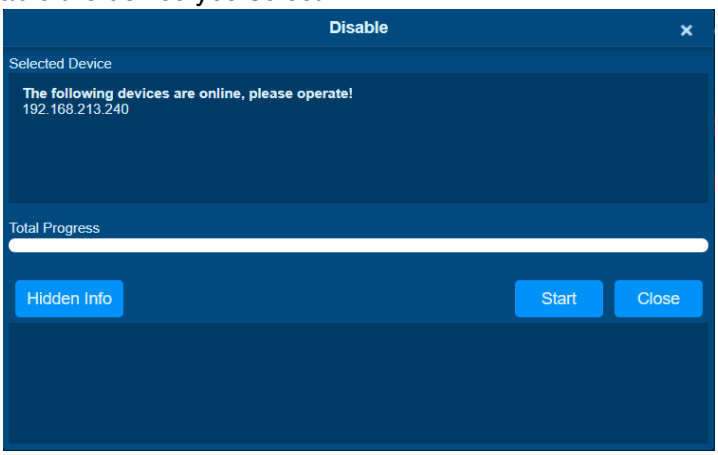
After disabling, the communication between the software and the device will end.

Steps:

- Click **[Access Control Module]** > **[Device]** >**[Control]** to view the control page and select **[Disable]**.



- Click **[Start]** to disable the device you select.



Synchronize All Data

Preconditions for Normal Use of Functions

Log in to the system with current account and have the authority.

Function Usage Scenarios

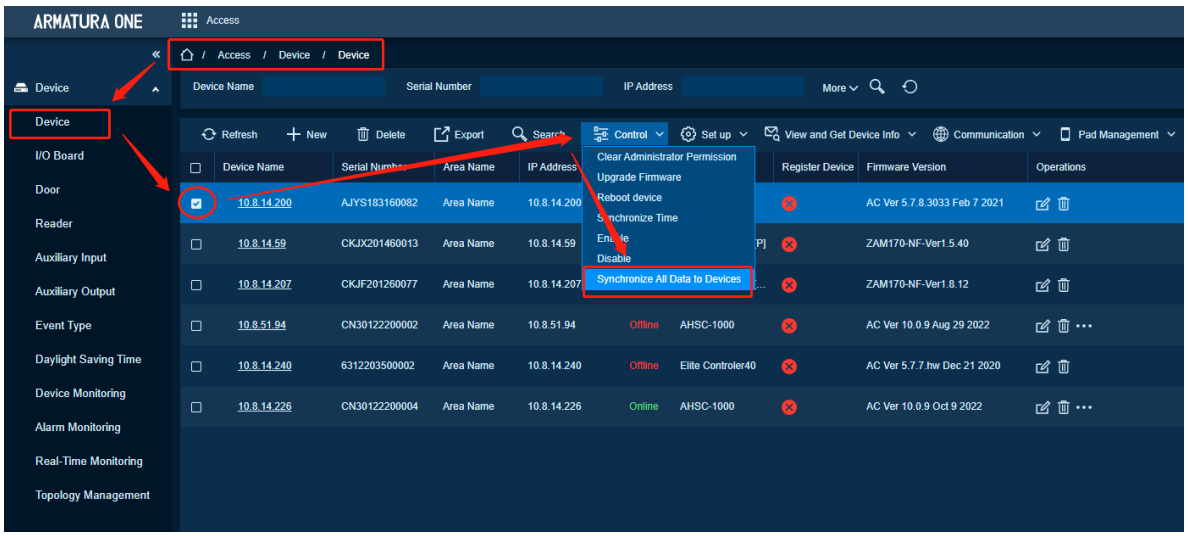
It is necessary to synchronize all the data and parameters set on the software to the connected device.

Feature Trigger Result

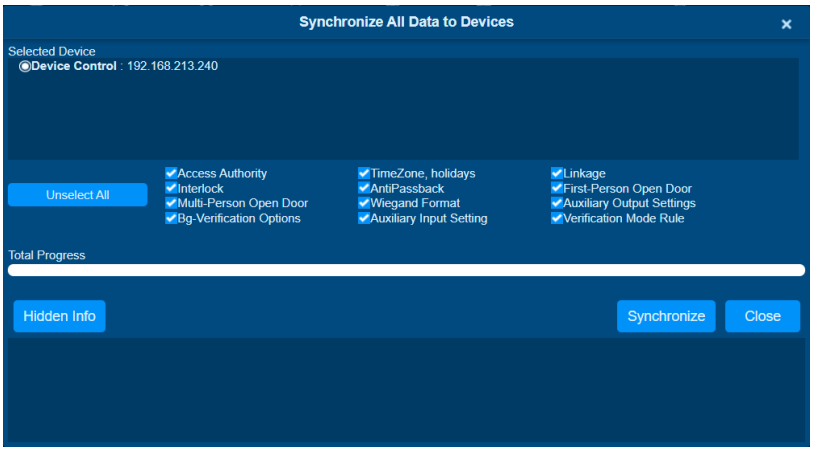
All data on the software is synchronized to the device.

Steps:

- Click **[Access Control Module]** > **[Device]** > **[Control]** to display the control page.
- Click **[Synchronize All Data to Devices]**, click to pop up the interface of synchronizing all data.



- Click **[Synchronize]** to synchronize data to the device.



Set Up

Background Verification Parameters

Preconditions for Normal Use of Functions

Log in to the system with current account and have authority. When the device is offline, the device has standard access permissions or the function of denying users' access.

Function Usage Scenarios

The device connected to the software needs to be verified in the background.

Feature Trigger Result

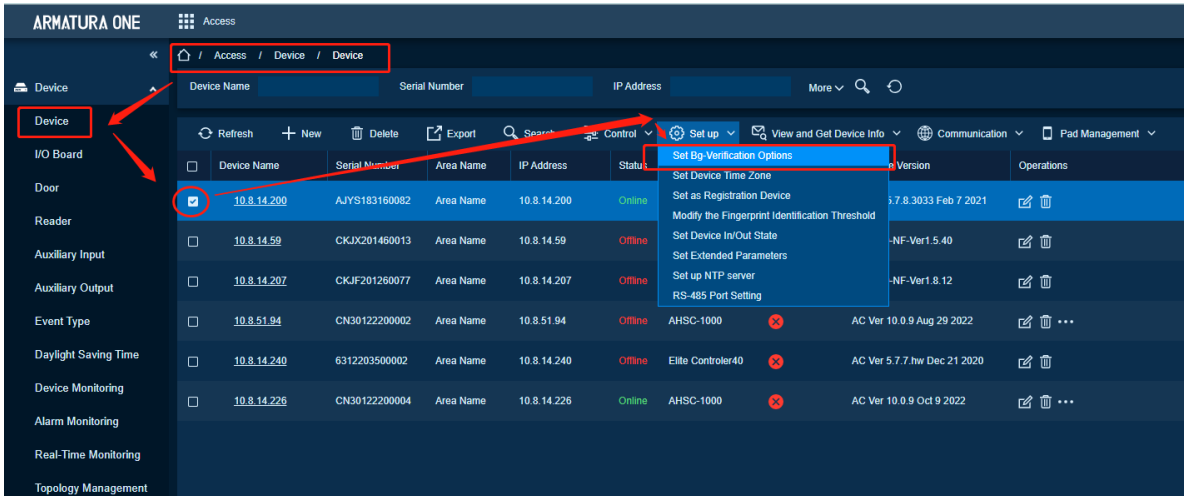
Enable or disable the background verification function of the device and the permissions when the controller is offline.

Limit

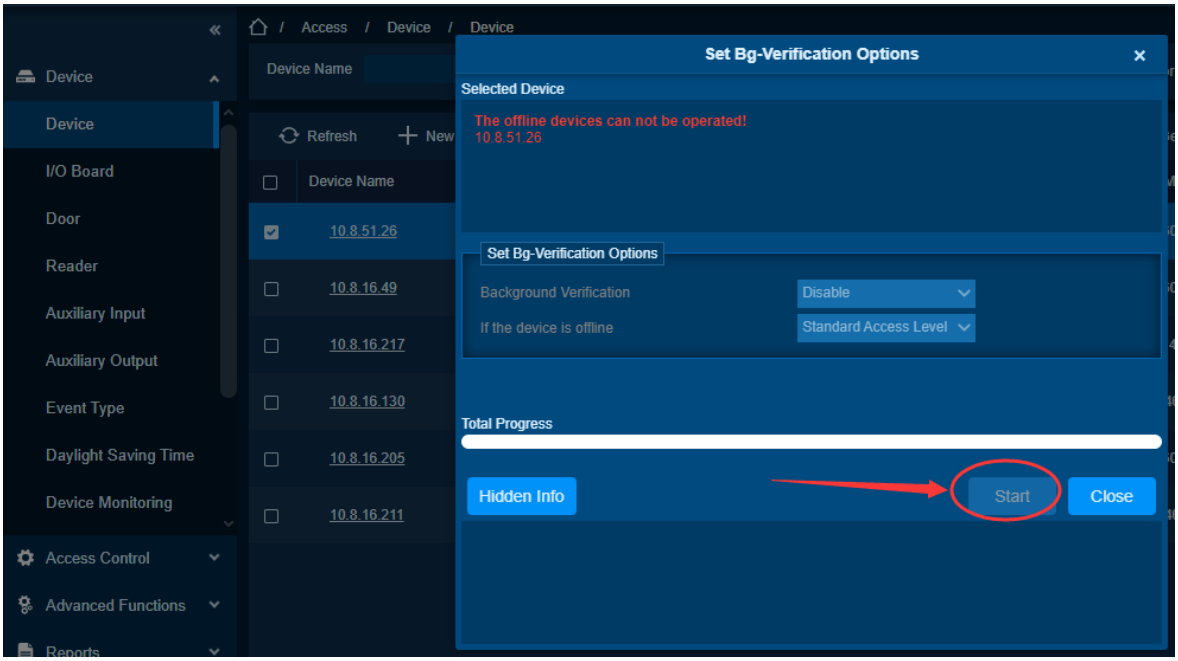
This feature only available when device is online. If offline will not allow to modify.

Steps:

- Click **[Access Control Module]** > **[Device]** > **[Settings]** to display the setting page.
- Click **[Set BG-Verification Options]** and fill in the parameters.



- Click **[Start]** to set up successfully and synchronized to the device.



Set Device Time Zone

Preconditions for Normal Use of Functions

Log in to the system with current account.

Function Usage Scenarios

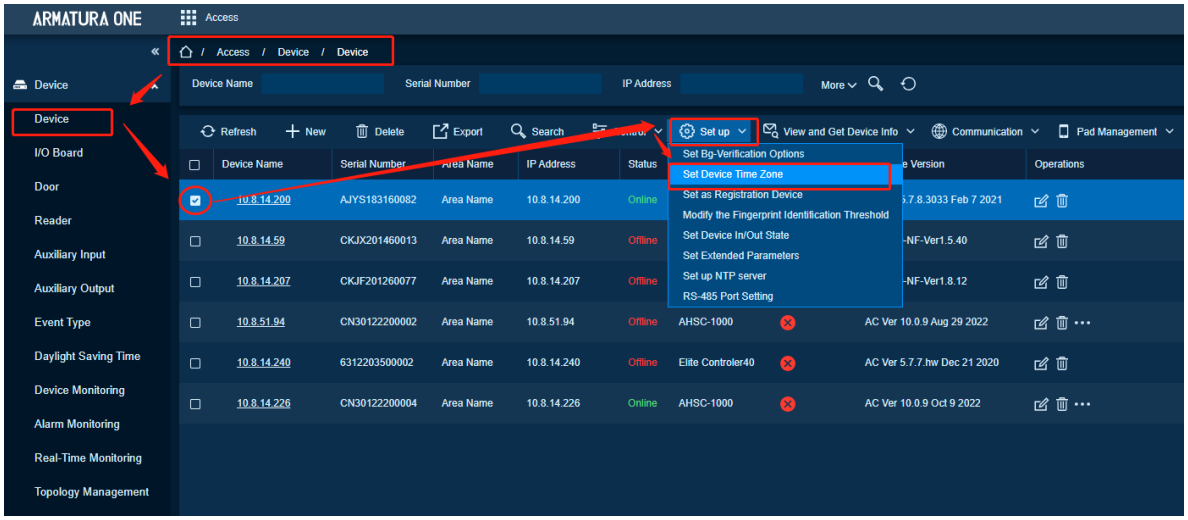
The device time zone configuration is incorrect. The device supports setting the time zone, and the device time zone is not in the same time zone as the server.

Feature Trigger Result

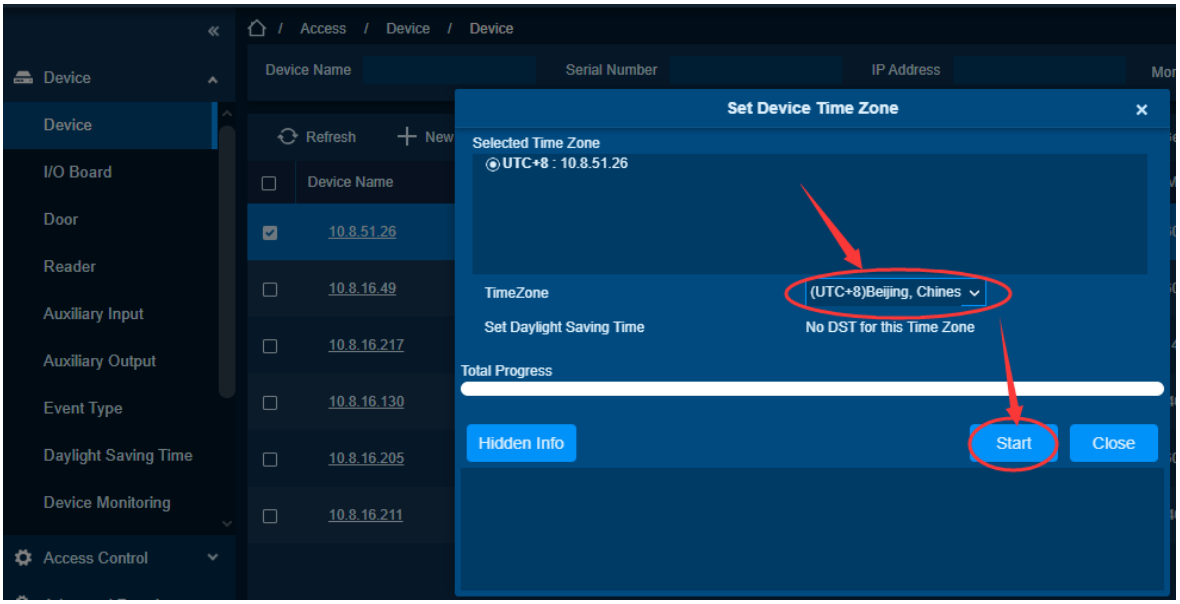
Synchronize the modified time zone to the device

Steps:

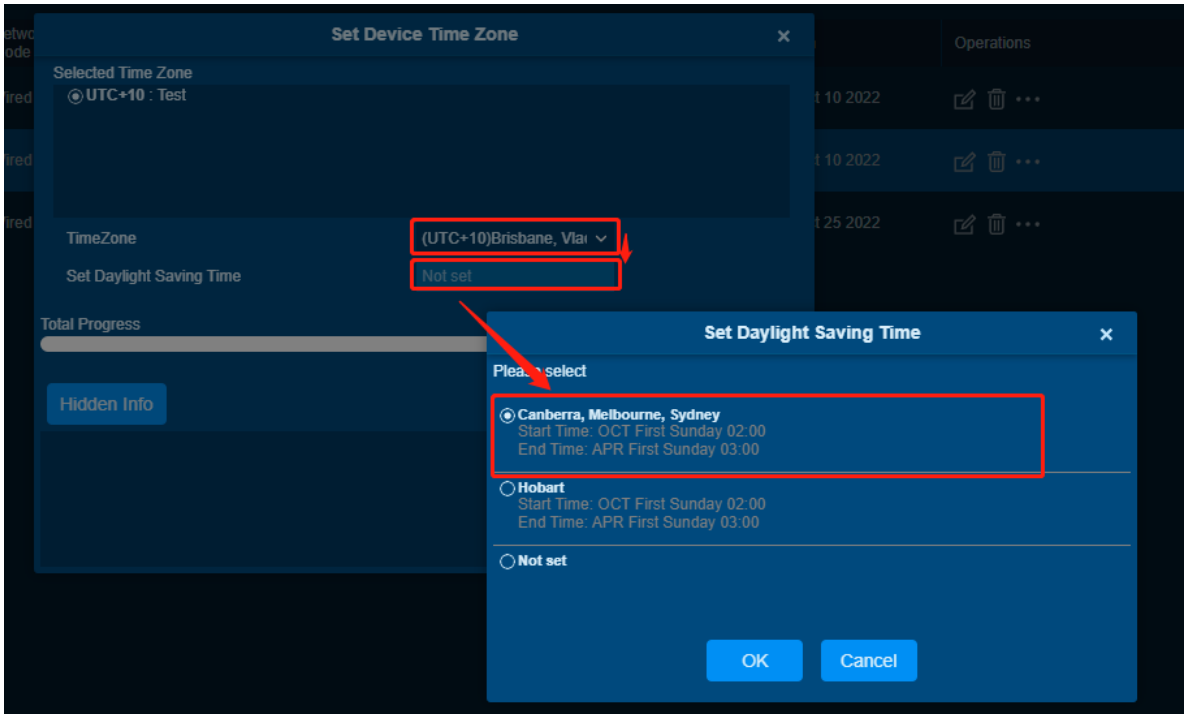
- Click **[Access Control Device]** > **[Device]** > **[Set up]** to display the setting page.
- Click **[Set Device Time Zone]**, select the time zone.
- Click **[Start]** to set the time zone and synchronize to the device.



- Select the **Time Zone**



- Select **[Daylight Saving Time]** if Time Zone support



- Click **OK**
- **Start** to start the process.

Set as Registration Device

Preconditions for Normal Use of Functions

Log in to the system with current account and have the authority.

The connected device supports the registration machine function.

Function Usage Scenarios

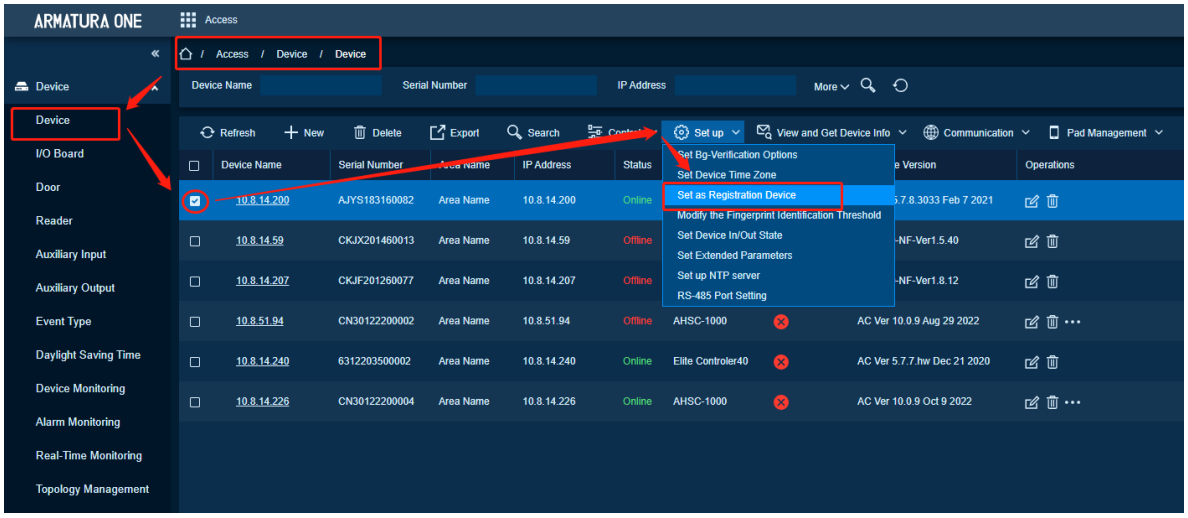
Need to automatically upload device data to the software

Feature Trigger Result

Data such as personnel entered by the device and parameters set can be automatically uploaded to the software.

Steps:

- Click **[Access Control Module] > [Device] > [Set up]** to display the setting page.
- Click **[Set Up Registration Device]** to jump to the setting interface.



Modify Fingerprint Comparison Threshold

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority.

Function Usage Scenarios

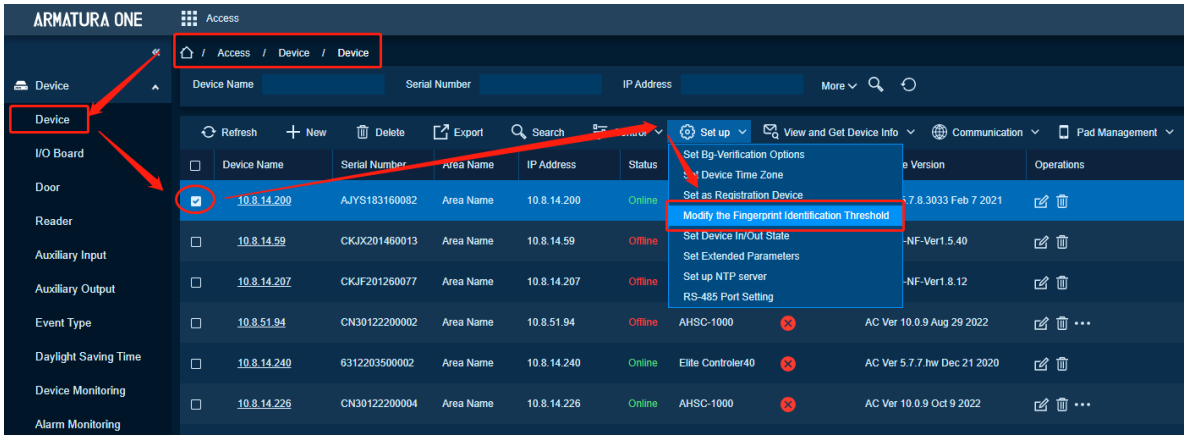
The fingerprint threshold is wrong or needs to be adjusted.

Feature Trigger Result

Modify the fingerprint threshold, and the fingerprint comparison will be compared according to the fingerprint threshold.

Steps:

- Click **[Access Control Module] > [Device] > [Set up]** to display the setting page.
- Click **[Modify the Fingerprint Identification Threshold]** to exit the setting interface.
- Click **[Start]** to modify the latest comparison threshold and synchronize to the device.



Set Device In/Out Status

Preconditions for Normal Use of Functions

Log in to the system with current account and have the authority.

Function Usage Scenarios

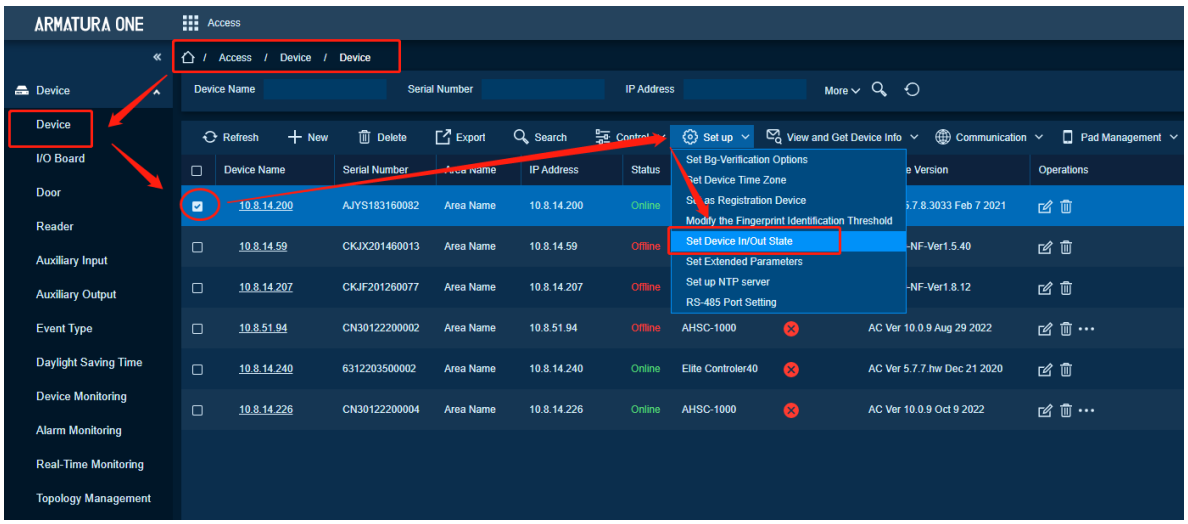
In the anti-passback function of the device, the access status of the device needs to be set.

Feature Trigger Result

In the anti-passback zone, strictly abide by the “one in, one out” rule before the verification will open.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Set up]** to display setting page.
- Click **[Set Device In/Out State]** to exit the setting interface.



Set Extended Parameters

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenario

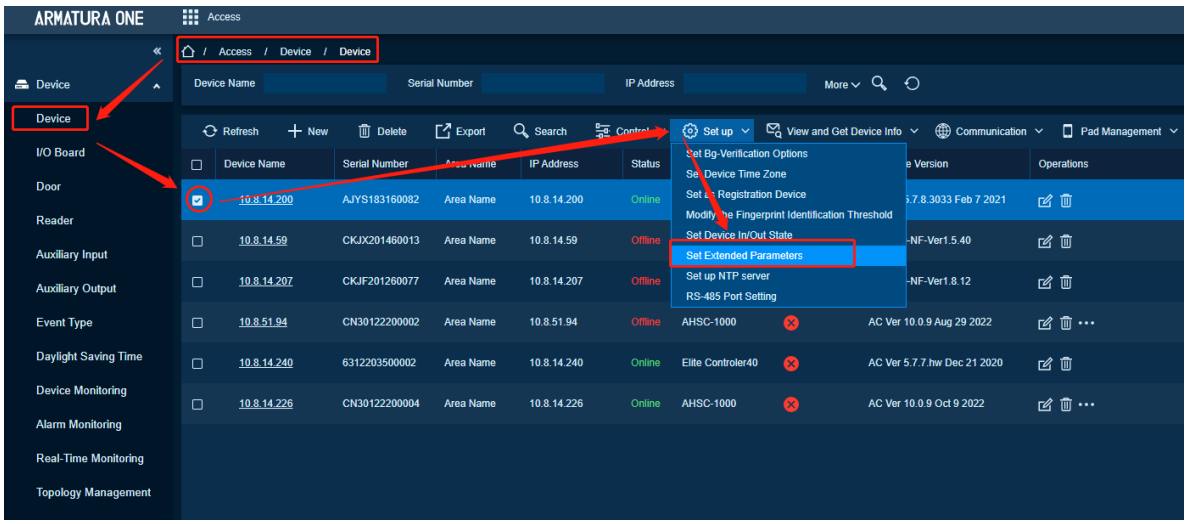
Some data of the device is wrong and needs to be modified.

Feature Trigger Result

You can set the Device Serial Number, Device Type, Firmware Version Number, Auxiliary Input Number, Auxiliary Output Number, Door Number, Device Fingerprint Version, Number of Readers, etc.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Set up]** to display the setting page.
- Click **[Set Extended Parameters]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.



Set NTP Server

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Select target device. Now only AHSC-1000 and AHDU-1X60 support.

Function Usage Scenario

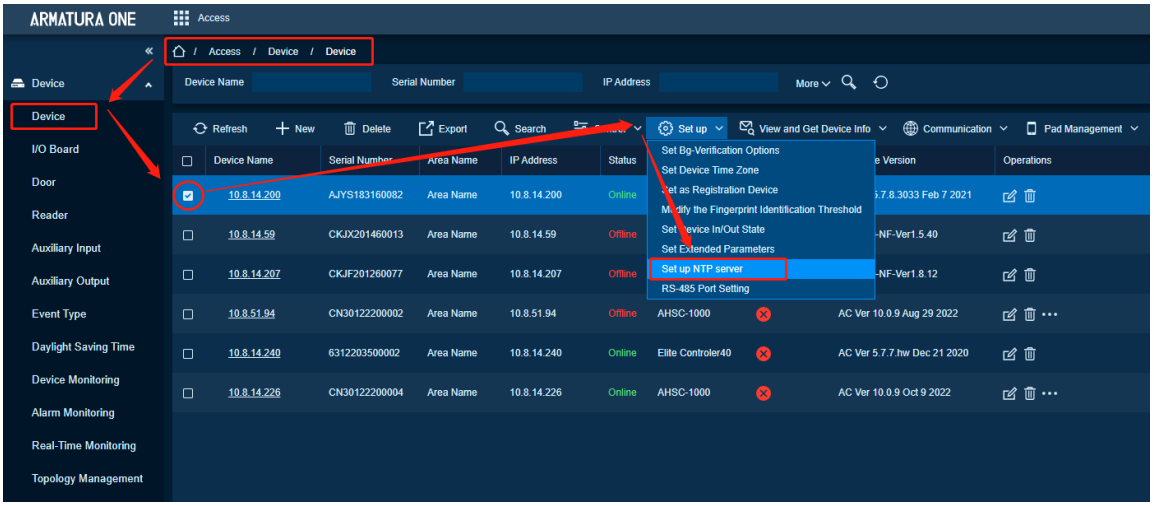
Set the time server for device.

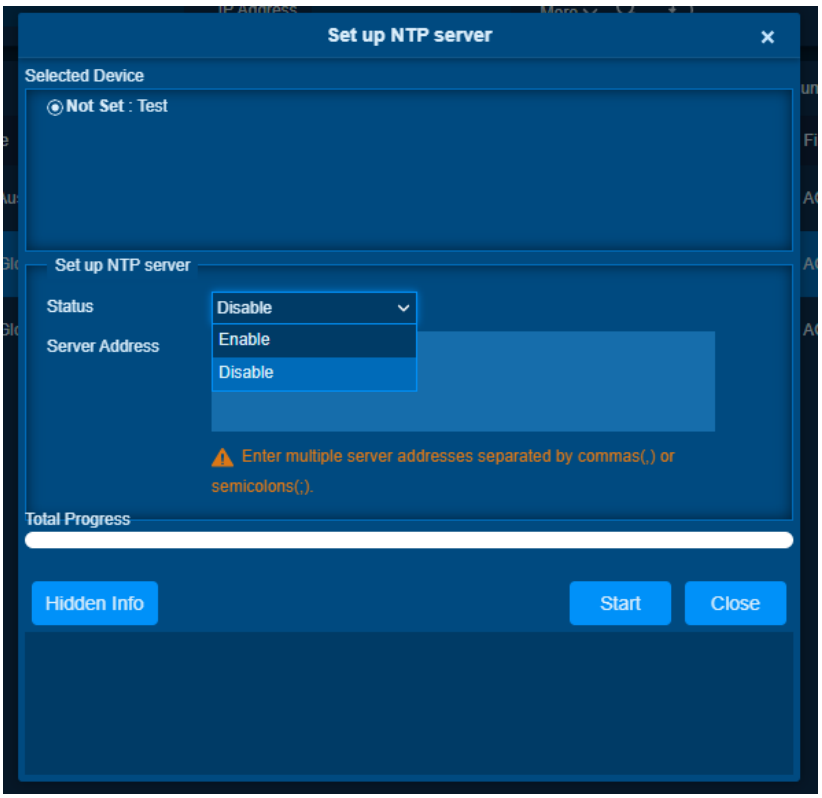
Feature Trigger Result

Device will get time from NTP Server

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Set up]** to display the setting page.
- Click **[Set up NTP Server]** to interface and set the corresponding parameters.





- Check device setting parameters in selected device window, now it shows **not set**, it means Device named Test has not set NTP Server.
- Set **[Status]** to Enable.
- Set **[Server Address]**, Enter multiple server addresses separated by commas (,) or semicolons (;).
- Click **Start**

Set RS-485 Port Setting

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Select target device. Now only AHSC-1000 and AHDU-1X60 support.

Function Usage Scenario

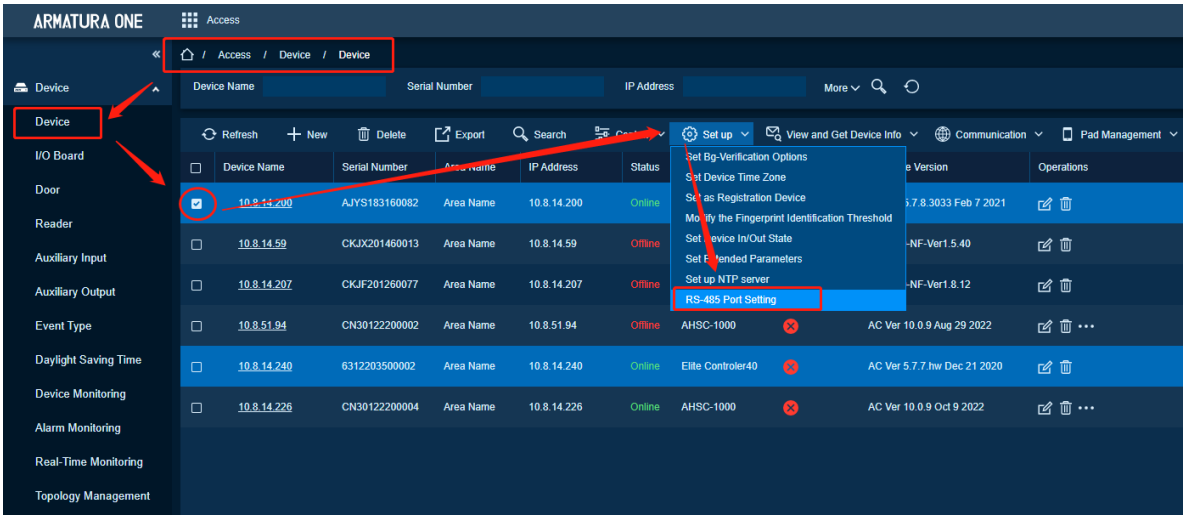
Set the Rs-485 Port Parameter for Device Connecting via RS-485

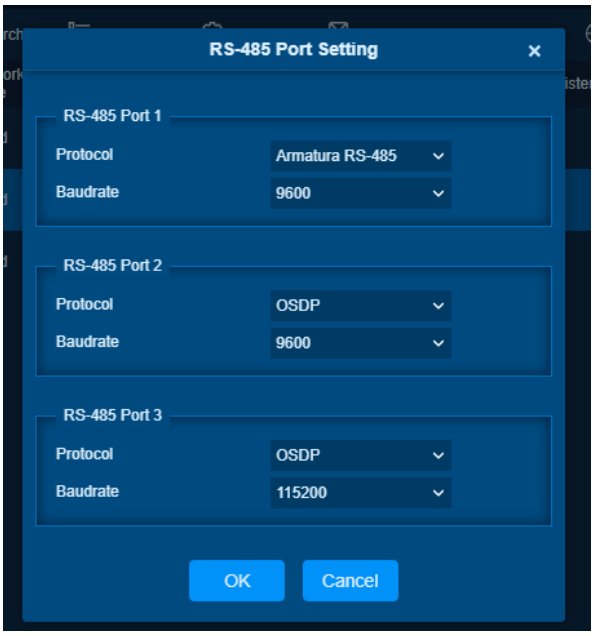
Feature Trigger Result

Secondary Controller/Reader/Expansion Board connect via RS-485 using specific protocol and Baudrate

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Set up]** to display the setting page.
- Click **[RS-485 Port Setting]** to interface and set the corresponding parameters.





Port Introduction

Parameter		Introduction
RS-485 Port 1	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port 2	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200
RS-485 Port 3	Protocol	Armatura RS-485/OSDP/Aperio
	Baudrate	4800/9600/19200/38400/57600/115200

Protocol Introduction

Protocol	Purpose	Supported Device
OSDP	For Reader/Expansion Board	AHSC1000, AHDU1X60

Armatura RS-485	For primary and secondary controllers	AHSC1000, AHDU1X60
Aperio	For ASSA ABLOY Aperio AH30	AHSC1000

- Click **OK**

View and Get Device Info

Get Device Option

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

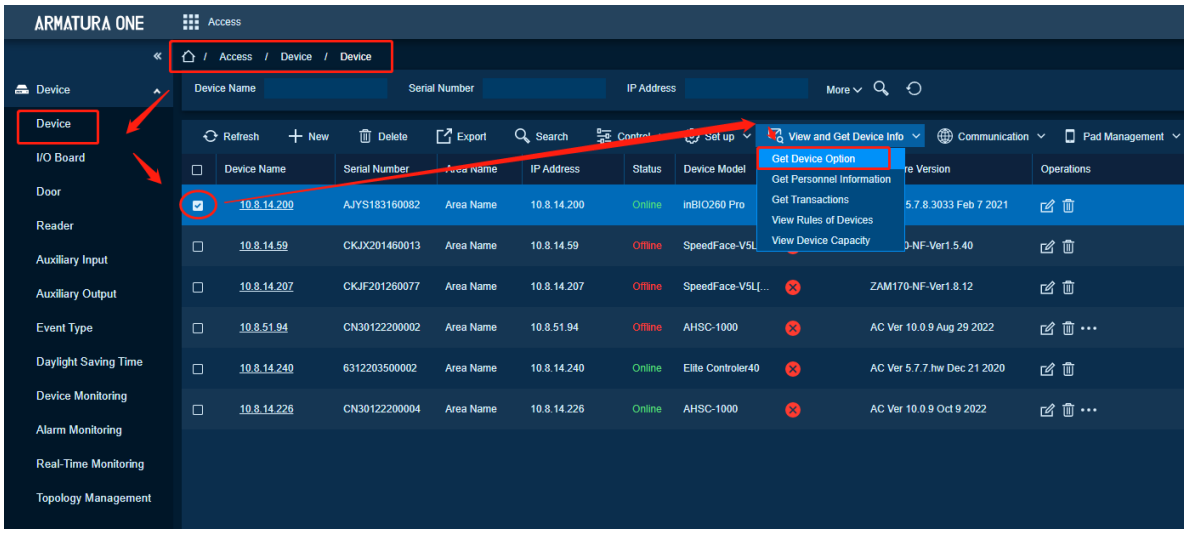
Check whether the device parameters are correct or not. The user needs to view the parameter information of the device.

Feature Trigger Result

Get the parameters commonly used in the device. For example, after upgrading the firmware, you can use this operation to update the firmware version of the device in the software.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[View and Get Device Info]** to display the view page.
- Click **[Get Device Option]** to jump out of the setting interface, select **[OK].**



Get Personnel Information

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

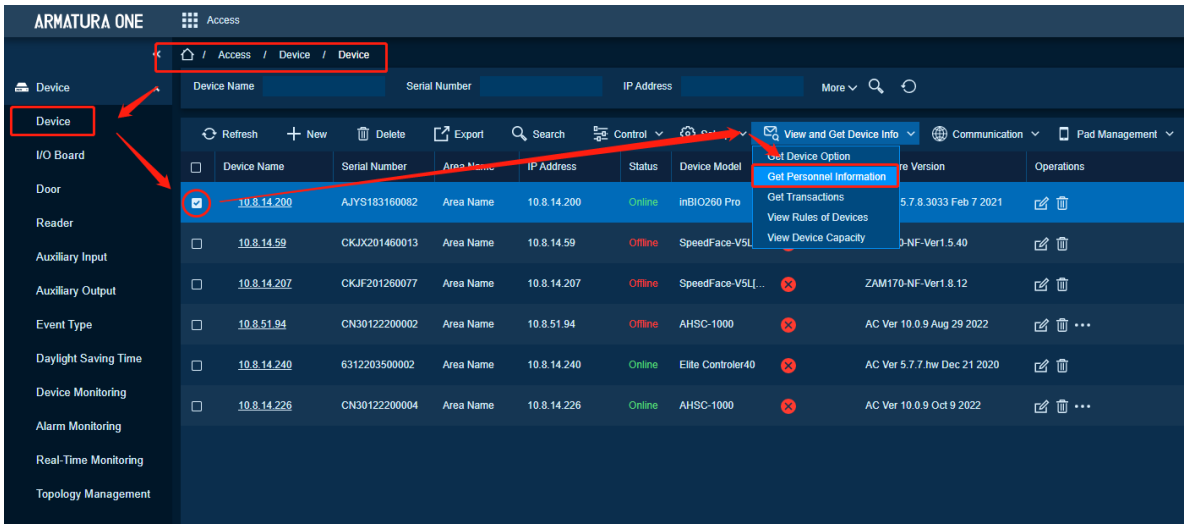
Query the overall personnel information of the device, including personnel personal information.

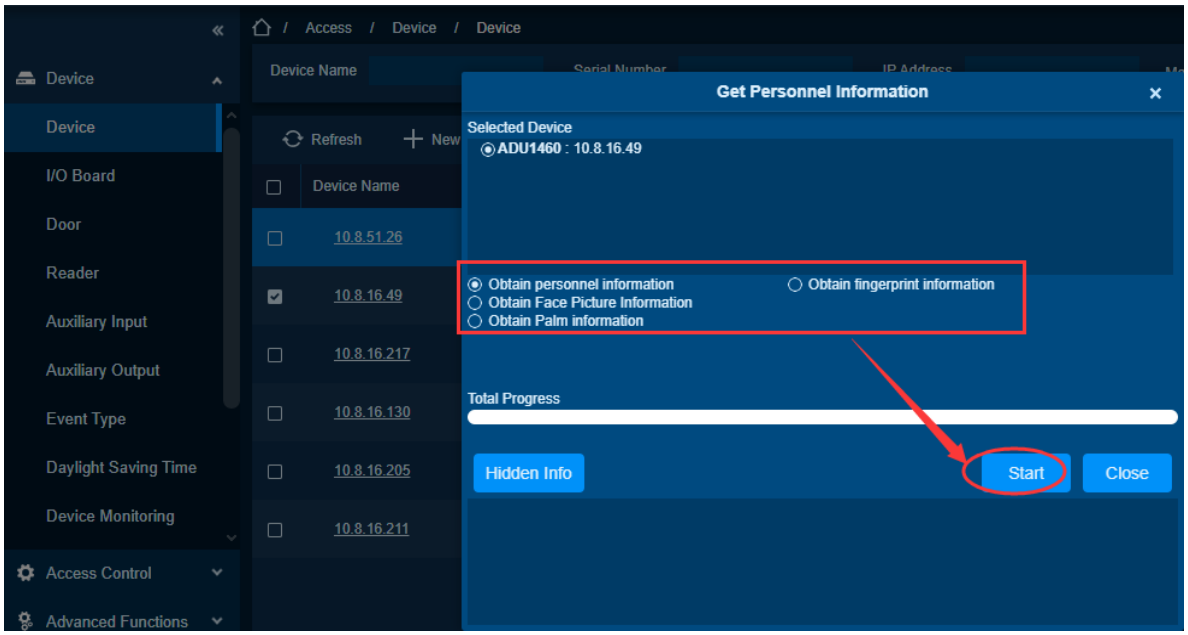
Feature Trigger Result

Obtain personnel, fingerprints, finger veins, and facial data in the device or obtain the corresponding number.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[View and Get Device Info]** to display the view page.
- Click **[Get Personnel Information]** to exit the interface.
- Click **[Start]** to get the corresponding data from the device to the software.





Get Transactions

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

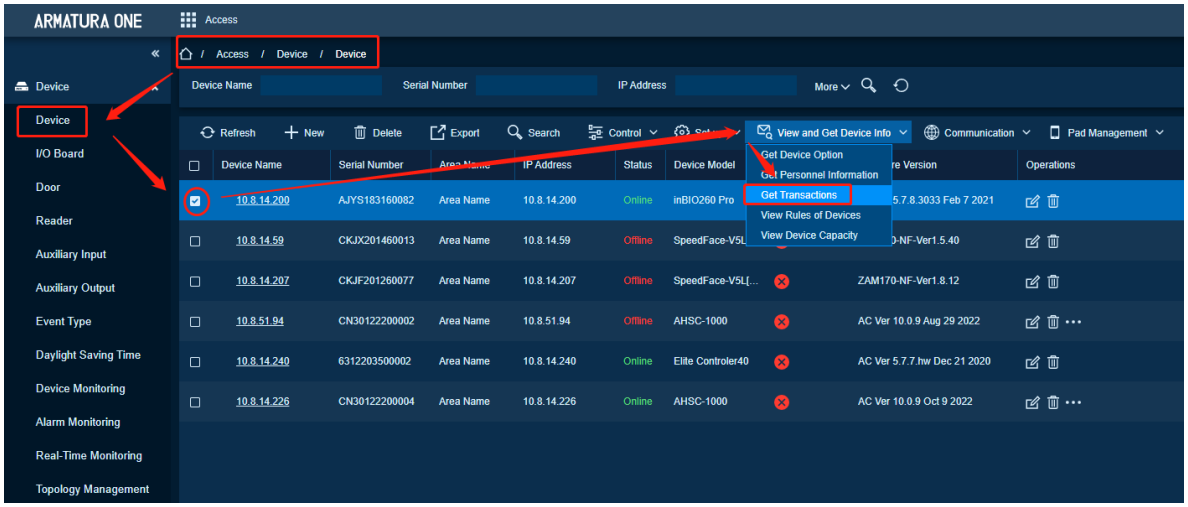
Need to obtain a new record or all records of the events of the connected device

Feature Trigger Result

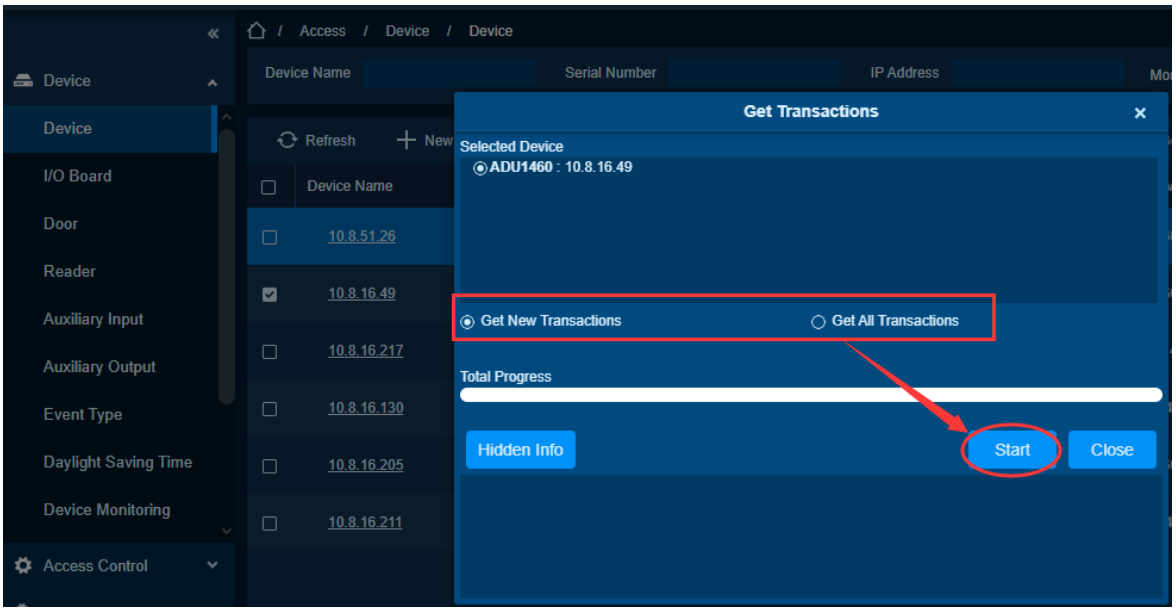
Obtain the event records in the device to the system

Steps:

- Click **[Access Control Device]** > **[Device]** > **[View and Get Device Info]** to display the view page.
- Click **[Get Transactions]** to exit the interface.
- Click **[Start]** to get the corresponding data from the device to the software.



- On Get Transactions interface, click Get **All Transactions> Start**.



1) When the network is in good condition and the communication between the system and the device is normal, the system will obtain the event record in the device in real-time and save it in the database.)

2) When the communication is interrupted, the event record in the device is not uploaded to the system in real-time. At this time, you can perform this operation to manually obtain the event record in the device. By default, the system will automatically obtain event records from the device at 00:00 every day.

✍**Note:**

The access control device can store up to 100,000 event records, and if the record exceeds 10,000, the device will automatically delete the earliest saved records (by default, 10,000 records will be deleted).

View Rules of Devices

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. Ensure the device is online.

Function Usage Scenarios

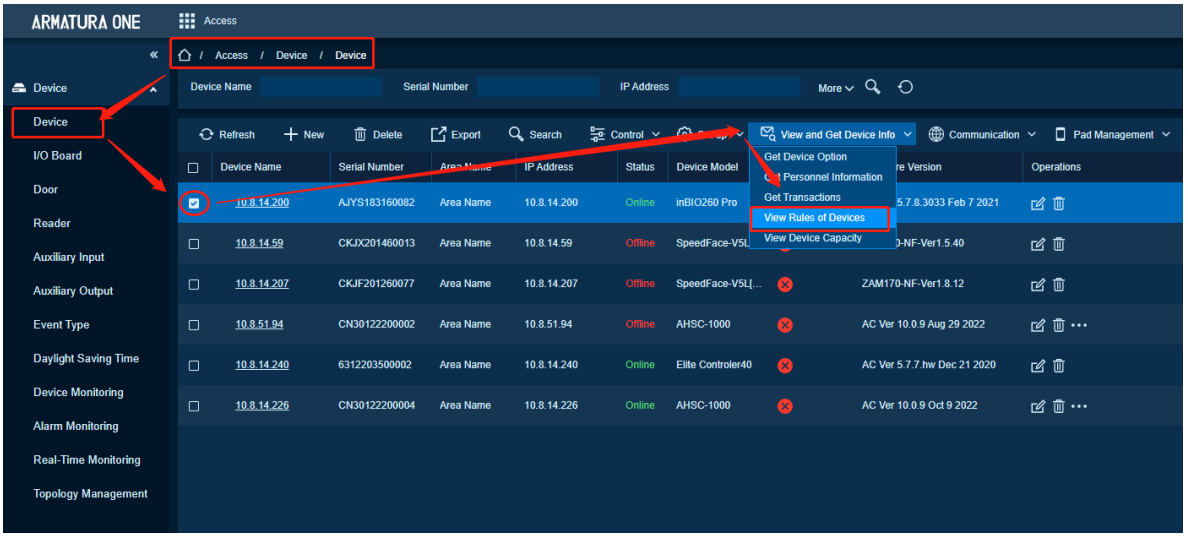
When the software needs to use the Access Control function, it needs to obtain the access control settings in the device.

Feature Trigger Result

View device access control rules.

Steps:

- Click **[Access Control Device] > [Device] > [View and Get Device Info]** to display the setting view page.
- Click **[View Rules of Devices]** to exit the Access Control rules interface in the device.



View Device Capacity

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

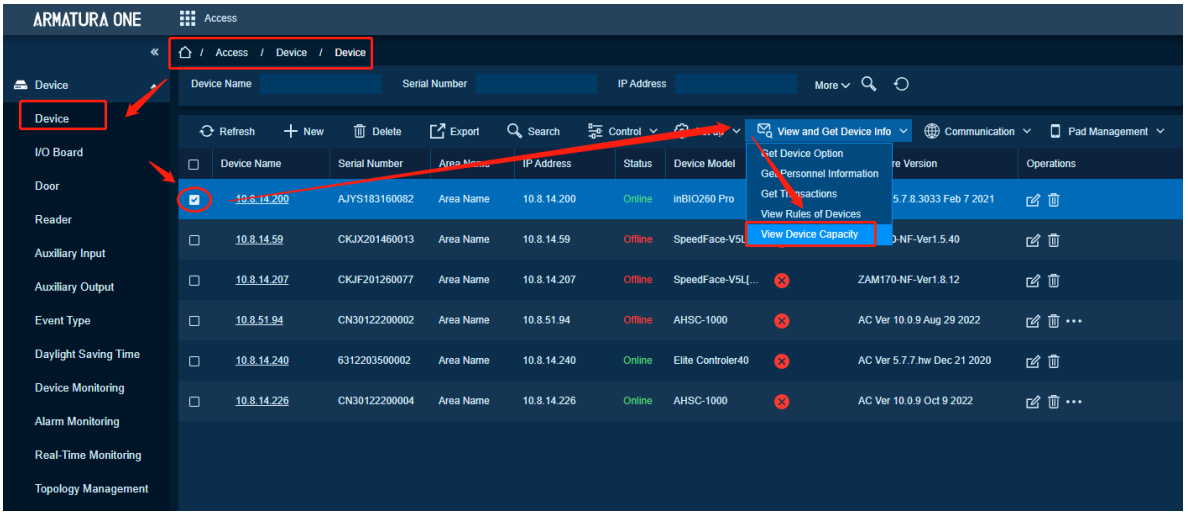
It is necessary to check whether the data of the device and the software are consistent.

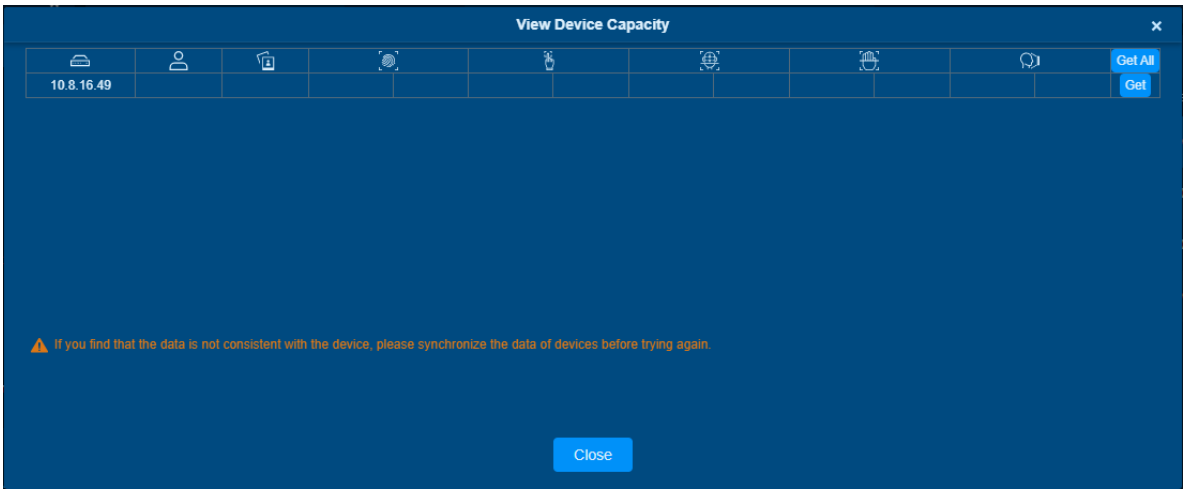
Feature Trigger Result

Query the capacity of each data of the device, such as the number of personnel, the number of fingerprints, etc.

Steps:

- Click **[Access Control Device] > [Device] > [View and Get Device Info]** to display the view page.
- Click **[View Device Capacity]** to pop out the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.





Communication

Modify IP Address

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is online.

Function Usage Scenarios

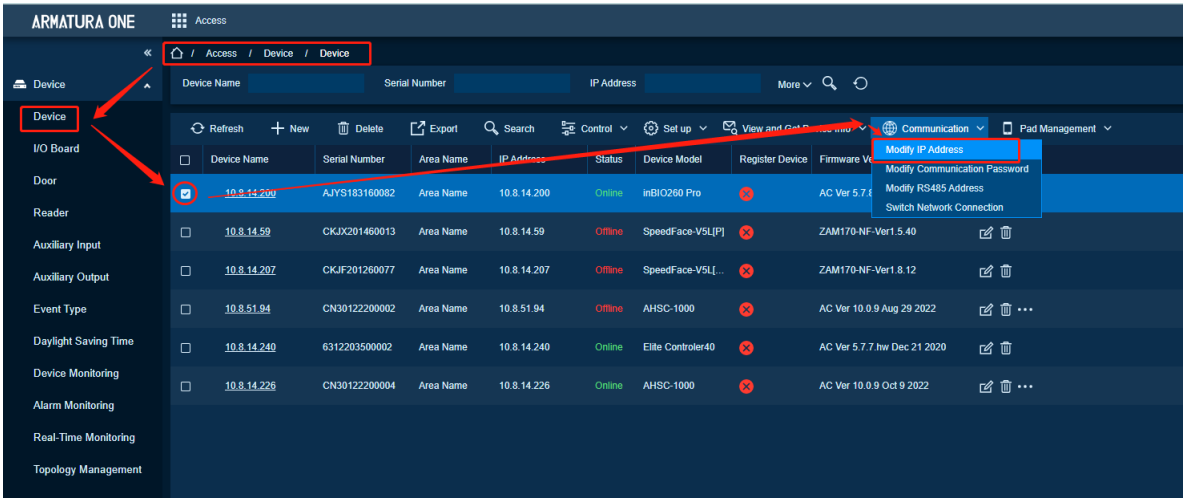
The software needs to modify the IP address.

Feature Trigger Result

Modify device IP address.

Steps:

- Click **[Access Control Device] > [Device] > [Communication]** to display the view page.
- Click **[Modify IP Address]** to jump out of the interface.



✍Note:

Gateway and IP address must be in the same network segment

Modify Communication Password

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is online.

Function Usage Scenarios

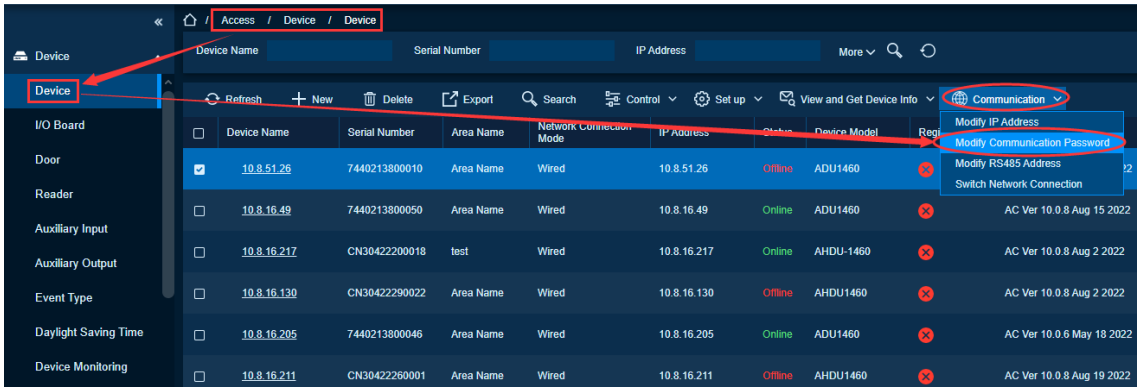
Software needs to view system parameters.

Feature Trigger Result

Get system parameters.

Steps:

- Click **[Access Control Device] > [Device] > [Communication]** to display the view page.
- Click **[Modify Communication Password]** to jump out of the interface.



Modify RS485 Address

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

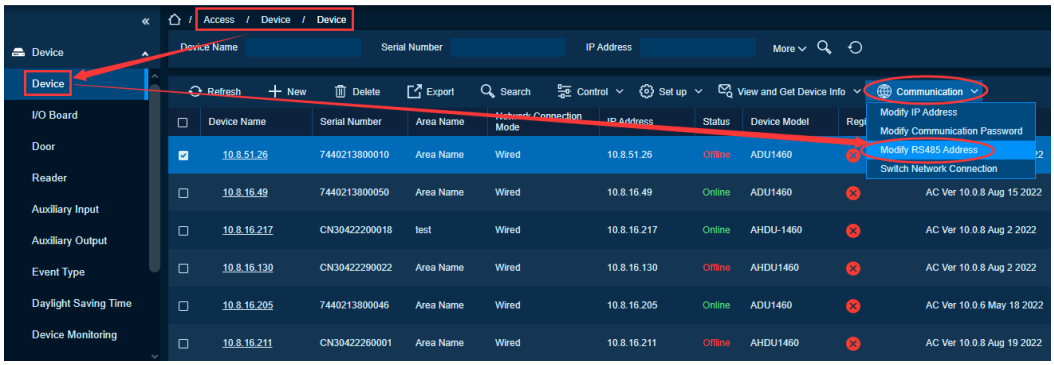
Software needs to view system parameters.

Feature Trigger Result

Get system parameters.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Communication]** to display the view page.
- Click **[Modify RS485 Address]** to jump out of the interface.



Only the devices that use RS485 communication and with no DIP Switch can modify RS485 address.

Switch Network Connection

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is online.

Function Usage Scenarios

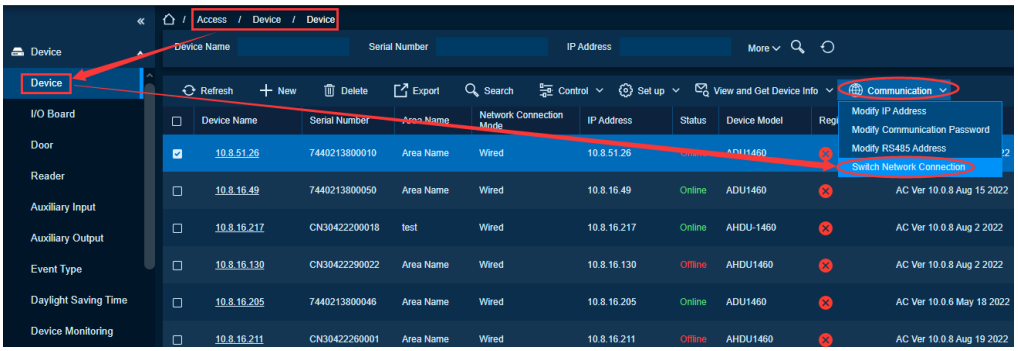
Software needs to view system parameters.

Feature Trigger Result

Get system parameters.

Steps:

- Click **[Access Control Device] > [Device] > [Communication]** to display the view page.
- Click **[Switch Network Connection]** to jump out of the interface.



This function is applicable to InBio5 series access control panels, which is used to switch among different network connection modes of the control panel.

Pad Management

Set the Login User Password

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the operation authority for this function. Only selected devices have this function.

Function Usage Scenarios

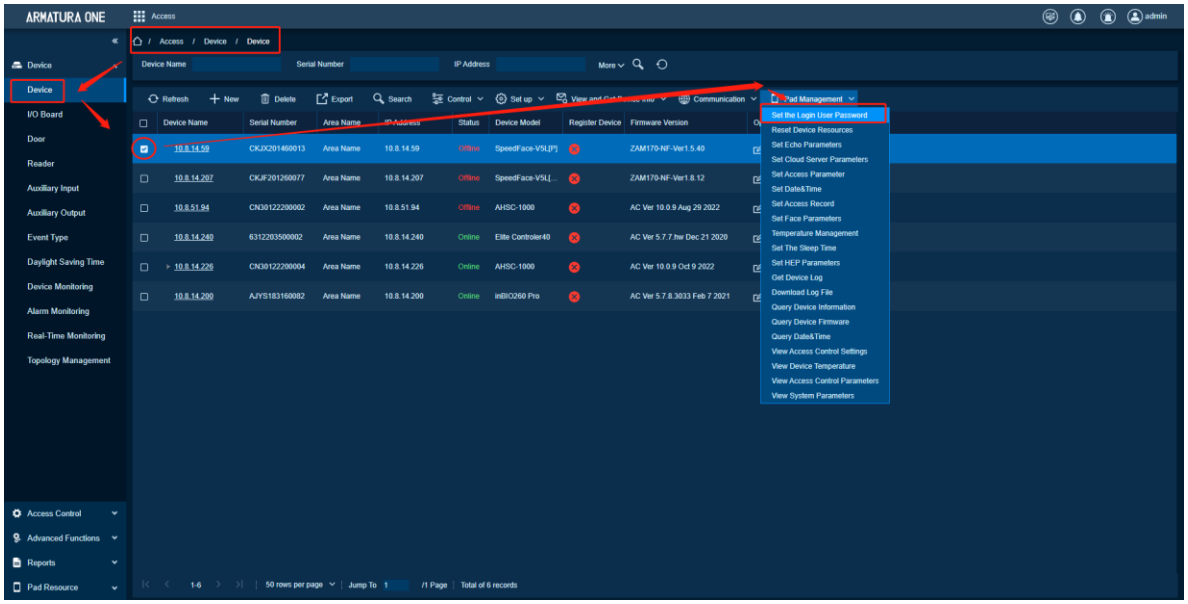
The administrator forgets the login password of the connected device and need to change to a new login password.

Feature Trigger Result

The login password is successfully modified, and a new login password is required when operating the device.

Steps:

- Click **[Access Control Module] > [Device] > [Pad Management]** to display the control page.
- Click **[Set the Login User Password]** to set.



Pad Management-Reset Device Resources

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority.

Function Usage Scenarios

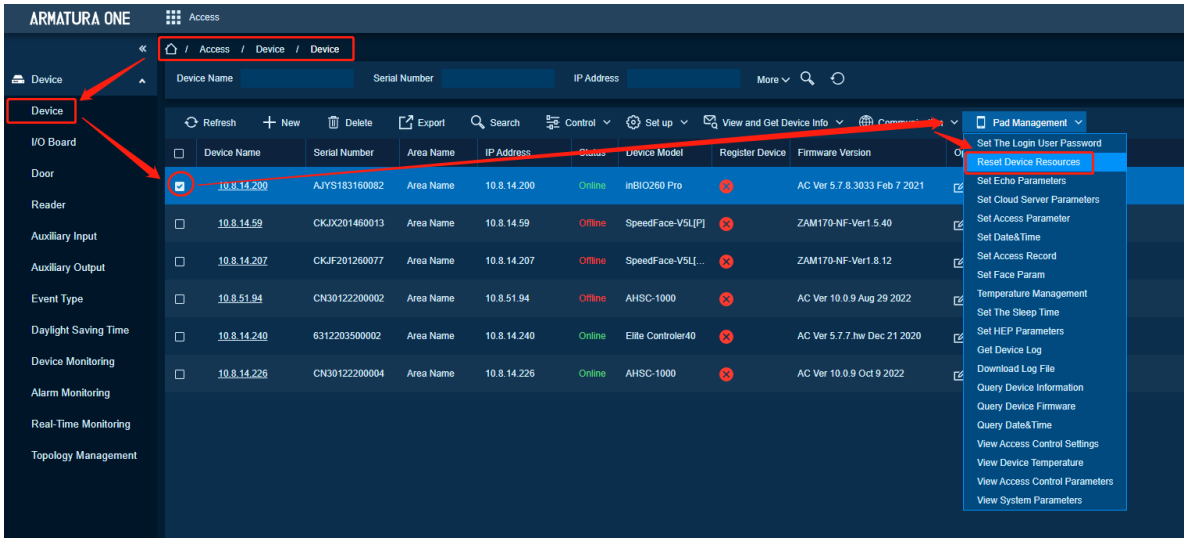
The resource configured on the software is wrong and needs to be reconfigured.

Feature Trigger Result

Reset the resource configuration in the **[Pad Resources]** on the software to the initial state.

Steps:

- Click **[Access Control Module]** > **[Device]** > **[Pad Management]** to display the control page.
- Click **[Reset Device Resources].**



- Click **[Start]** to reset device resources.

Set Echo Parameters

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority. Ensure that the device is online.

Function Usage Scenarios

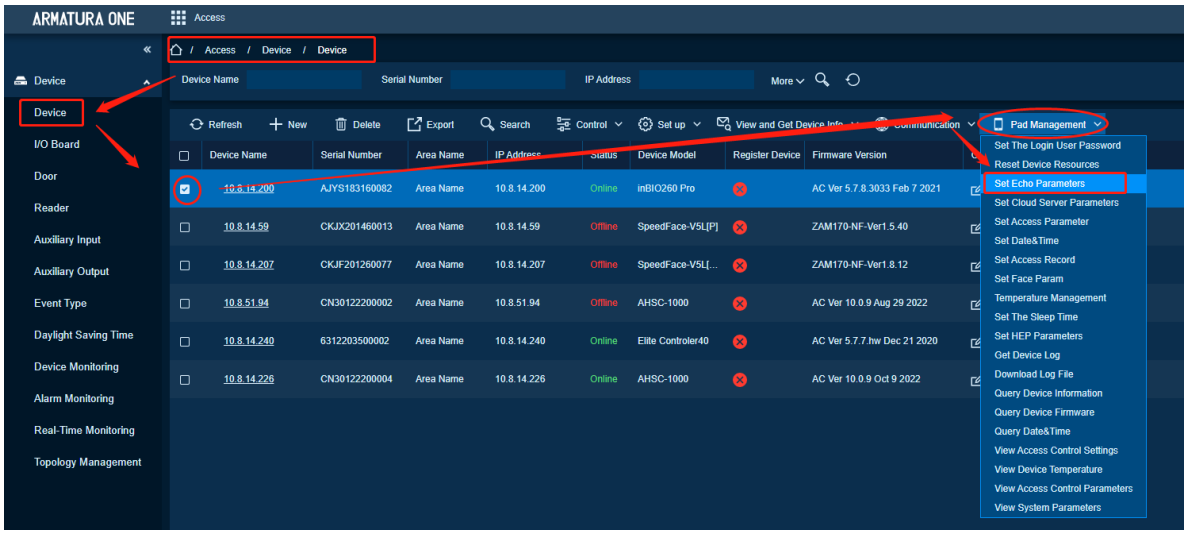
When verifying device personnel, you need to modify whether the personnel is displayed on the device.

Feature Trigger Result

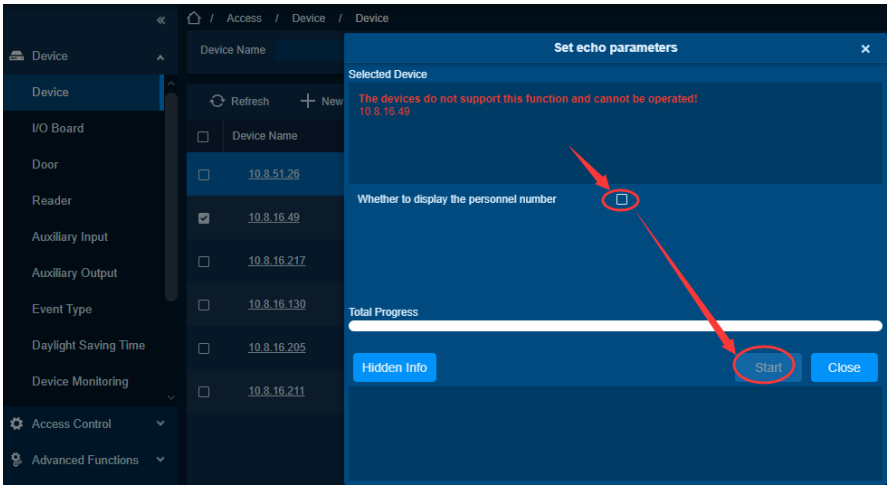
If the software is checked, the personnel number will be displayed during verification; if it is not checked, the personnel number will not be displayed during verification.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the setting page.
- Click **[Set Echo Parameters]** to jump out of the setting interface, choose whether to echo.
- Click **[Start]** to synchronize the settings to the device.



On Set Echo Parameters interface, click **Whether to Display the Personnel Number> Start**.



Set Cloud Server Parameters

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority. Ensure that the device is online and supports this function.

Function Usage Scenarios

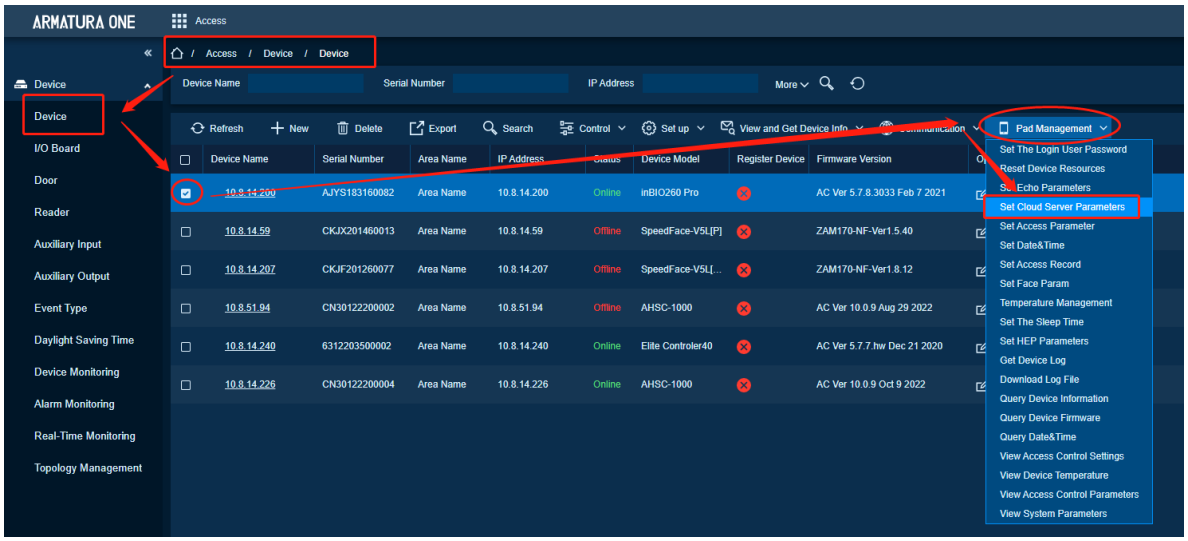
The device needs to connect to the corresponding server and perform operations, such as Background Comparison. Local Priority, etc.

Feature Trigger Result

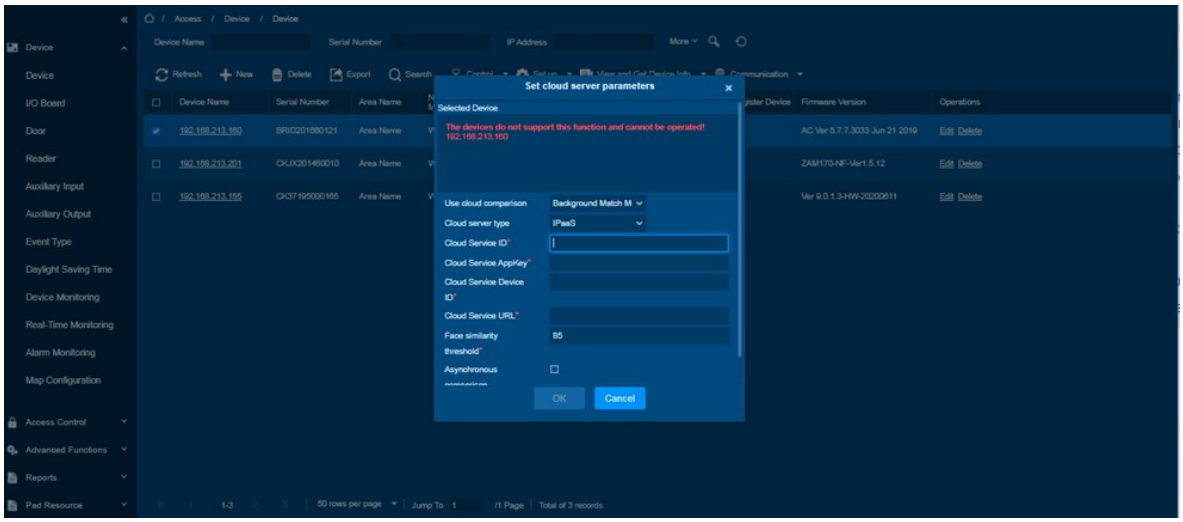
The device can connect to the corresponding server through the Set Server Address and perform corresponding operations.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the setting page.
- Click **[Set Cloud Server Parameters]** to exit the setting interface.
- Click **[OK]** to synchronize the settings to the device.



- On the Set Cloud Server Parameters interface, fill all the fields and click **[OK].**



Fields are as follows:

Use Cloud Comparison: Set cloud server parameters and comparison modes for standard devices: -

Comparison Mode	Description
Local Match Mode	Personnel data is stored in the device, only in the device for comparison.
Background Match Mode	Personnel data is stored in the software, Personnel comparison is stored in the software.
Local Match Priority Mode	Personnel data is stored both in the software and the device. Use device comparison for priority. If person is not found or in low similarity in the device, then would turn to software in second comparison.
Background Match Priority Mode	Personnel data is stored both in the software and the device. Use software comparison for priority if device were offline then would use device for local comparison.
Mixed Match Mode	Personnel data is stored both in the software and the device, The comparison is performed simultaneously in the device and in the software.

Cloud Sever Type: Optional for IPaaS/Biosecurity/Pangu/Smart Park (ROMA)/Video Cloud (VCM), in software we use Biosecurity.

Face Similarity Threshold: It is required to compare the percentage value of face similarity, the higher the value, the higher the security.

Asynchronous Comparison: With this function on, multiple comparisons will be performed at the same time.

Access Logic: Whether to support system access control logic.

✍**Note:**

The device needs to be online for the settings to take effect.

Set Access control Parameters

Preconditions for Normal Use of Functions

Log in to the system with the current account and have the authority. Make sure the device is online and supports this function.

Function Usage Scenarios

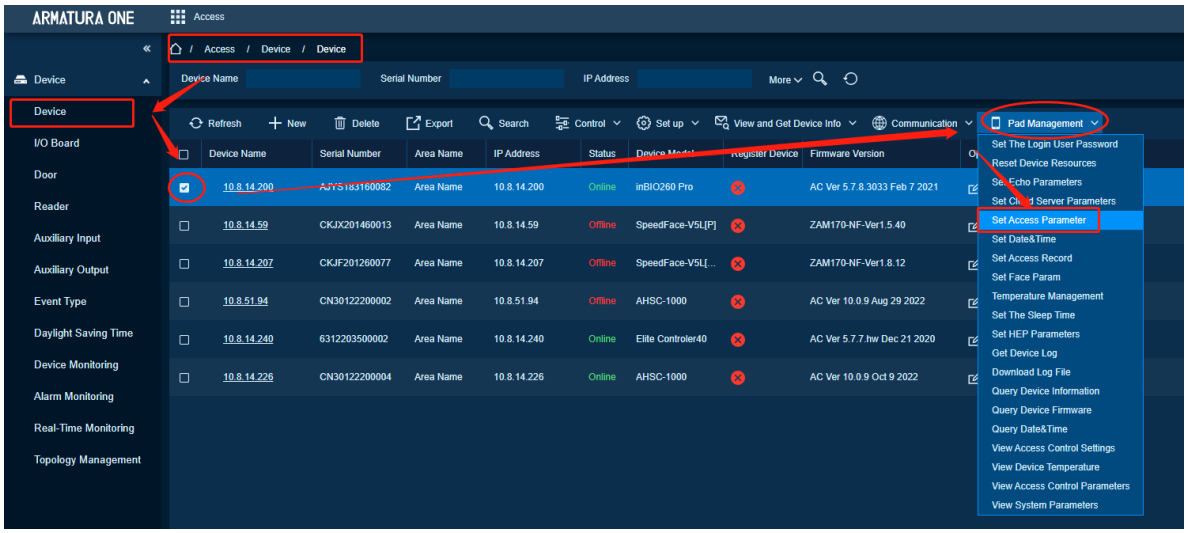
The access control parameters of the device connected to the current software are wrong or need to be adjusted.

Feature Trigger Result

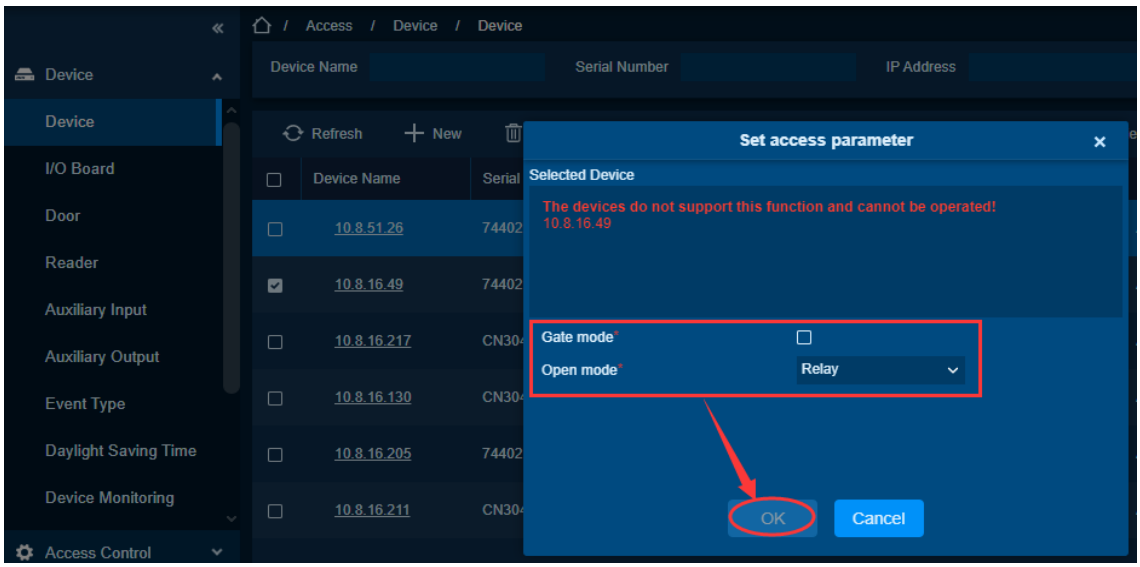
Set the required access control parameters, such as Gate Mode and Door Open Mode.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the setting page.
- Click **[Set Access Parameter]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.

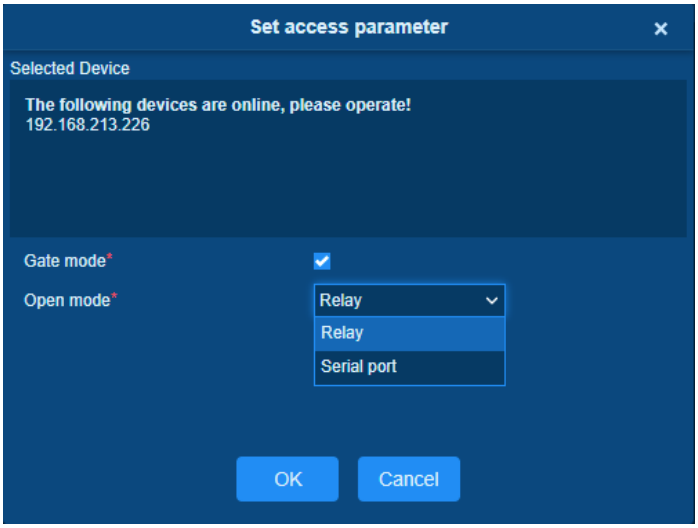


- On Set Access Parameter interface, select Gate Mode and Open Mode.



The corresponding door opening combination method should be selected according to the different device on site.

- Set the device's door opening combination method.



The corresponding door opening combination method should be selected according to the different device on site.

Set Date & Time

Set the method of device synchronization time.

The device can be set to automatically synchronize from the NTP address or synchronize the date, time, and time zone parameters of software system.

Preconditions for Normal Use of Functions

Log in to the system with current account and have the authority.

Function Usage Scenario

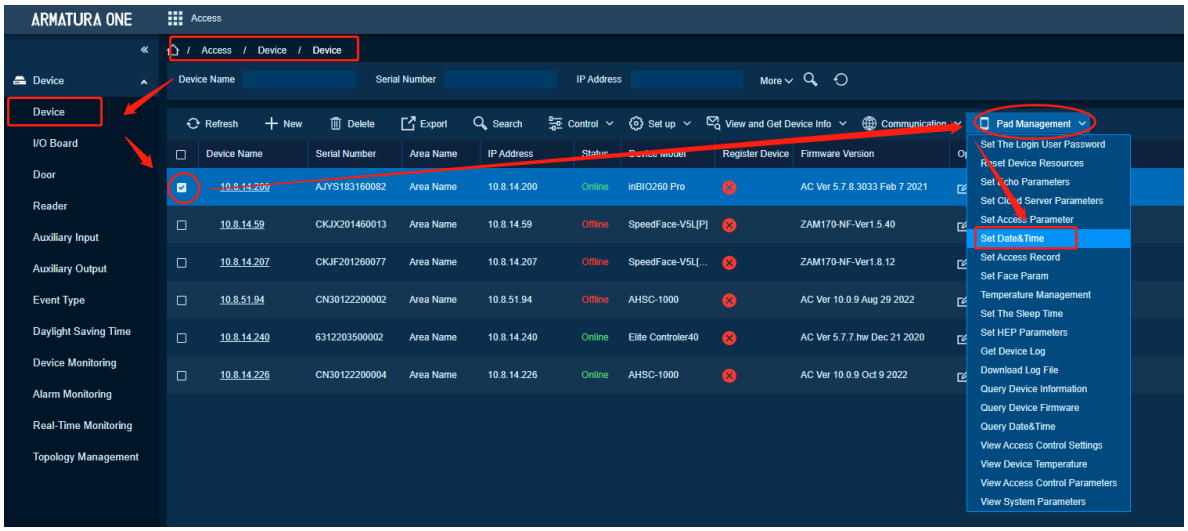
The user needs to modify the device date, date format, setting method.

Feature Trigger Result

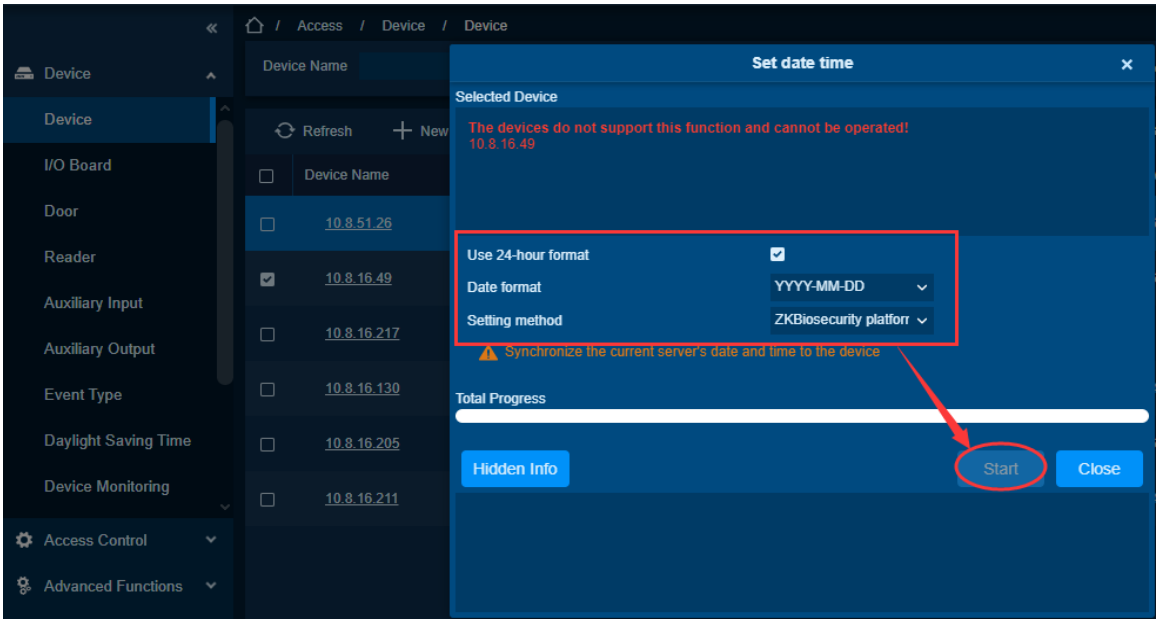
Synchronize the set time format data to the device

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Pad Management]** to display the setting page.
- Click **[Set Date & Time]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.



- On Set Date Time interface, select Use 24 Hour Format and then choose Date Format and Setting Method.



- Click **Start** to start the process.

✍Note:

If the device is set to NTP synchronization mode, you need to wait for the device to synchronize the NTP time successfully or fail before the process ends.

Set Access Control Records

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. Ensure the device is online and supports this function

Function Usage Scenario

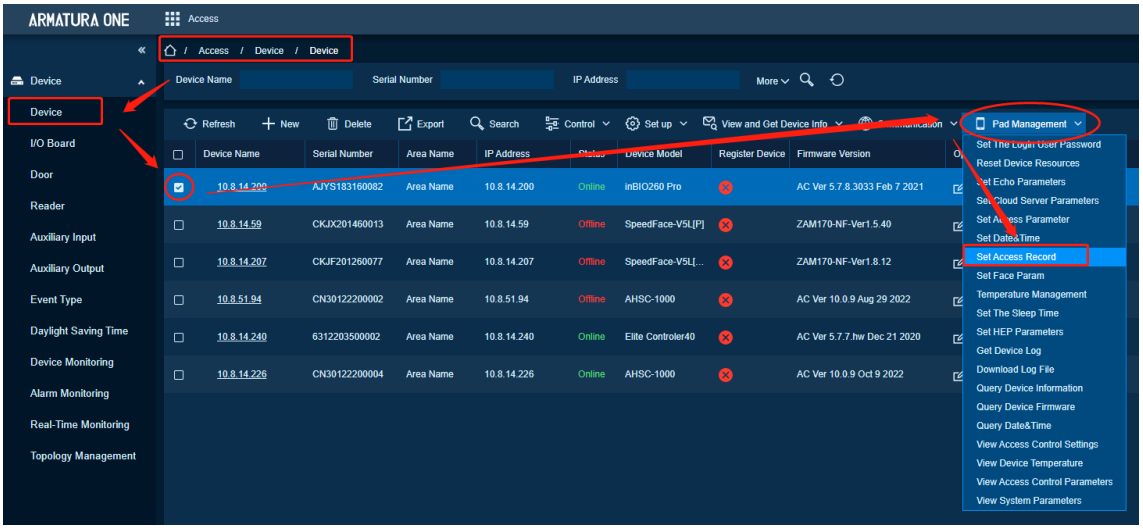
Need to modify the display delay time of access control verification and face comparison interval.

Feature Trigger Result

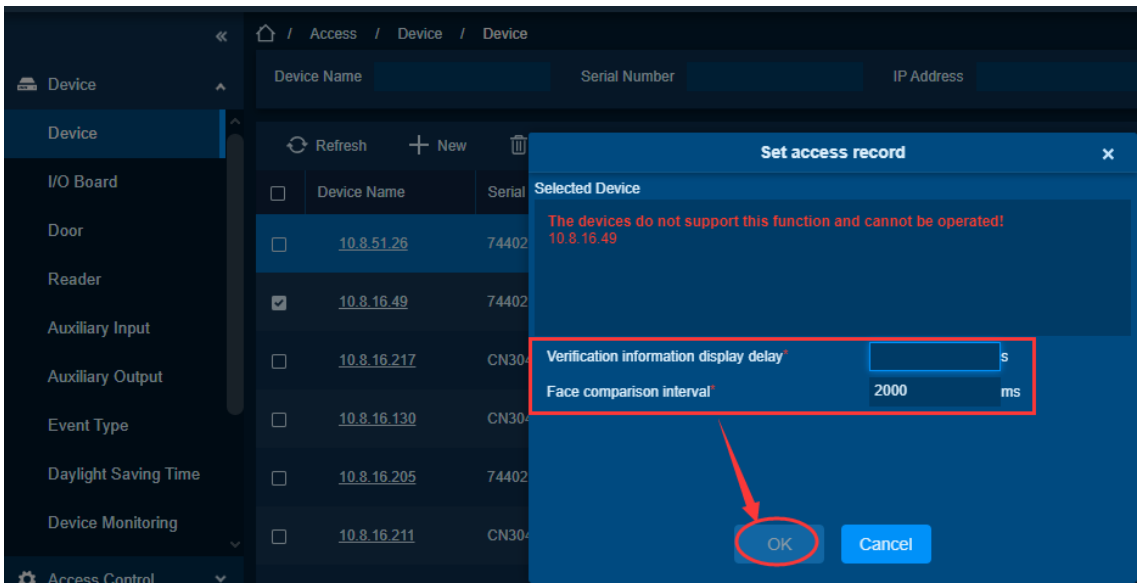
Modify the access control display delay time and face comparison inter to the device.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Pad Management]** to display the setting page.
- Click **[Set Access Record]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.



- On the Set Access Record interface, enter Verification Information Display Delay and Face Comparison Interval. Then click **OK**.



Set Face Parameters

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. Ensure the device supports face recognition.

Function Usage Scenarios

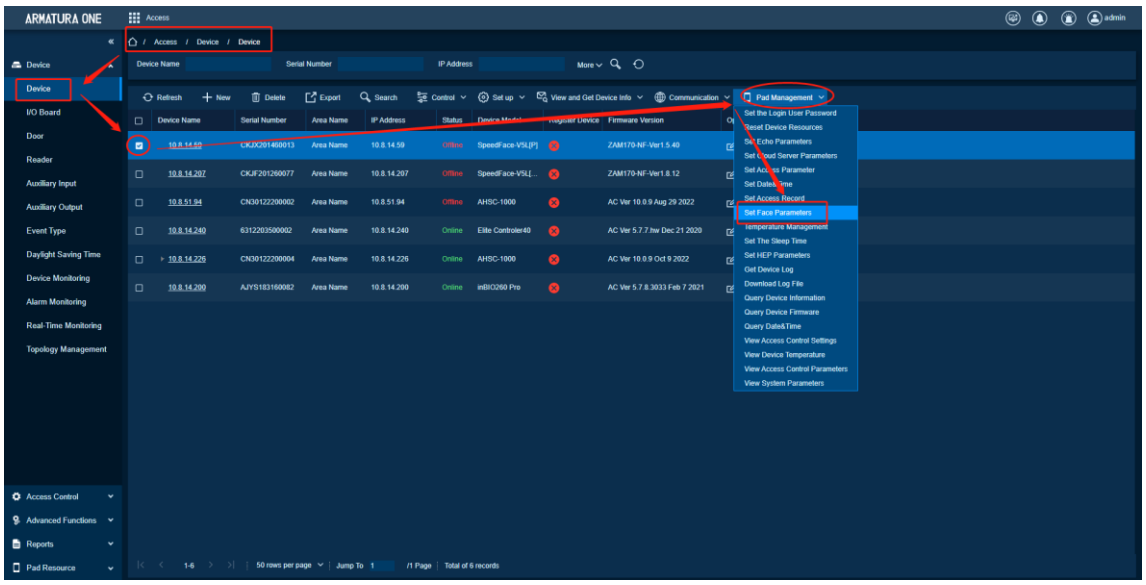
The face parameters in the device needs to be adjusted.

Feature Trigger Result

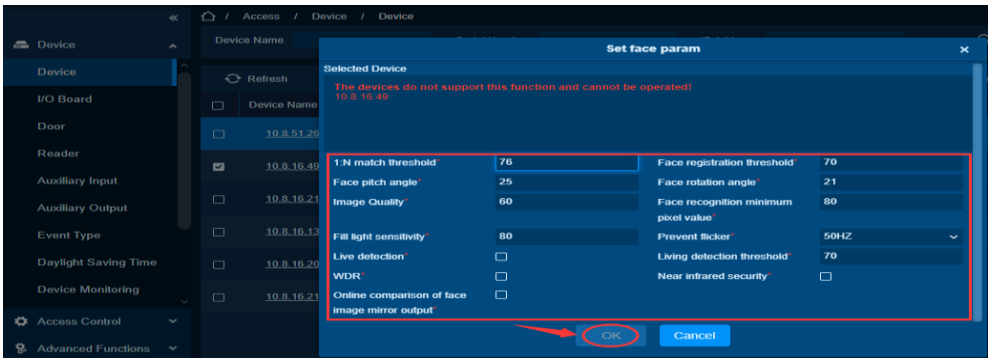
Modify face parameters and synchronize devices.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display setting page.
- Click **[Set Face Parameters]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.



- On the Set Face Parameters interface, after entering value in all fields, click **OK.**



Temperature Management

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. The device supports temperature control function.

Function Usage Scenarios

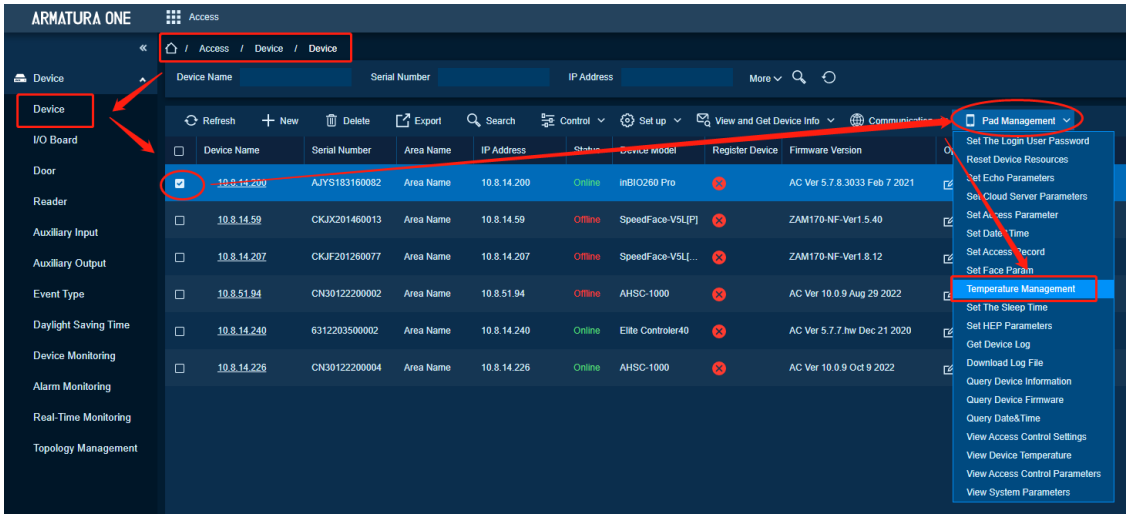
The device connected to the software needs to adjust the values of low temperature heating and high temperature reset.

Feature Trigger Result

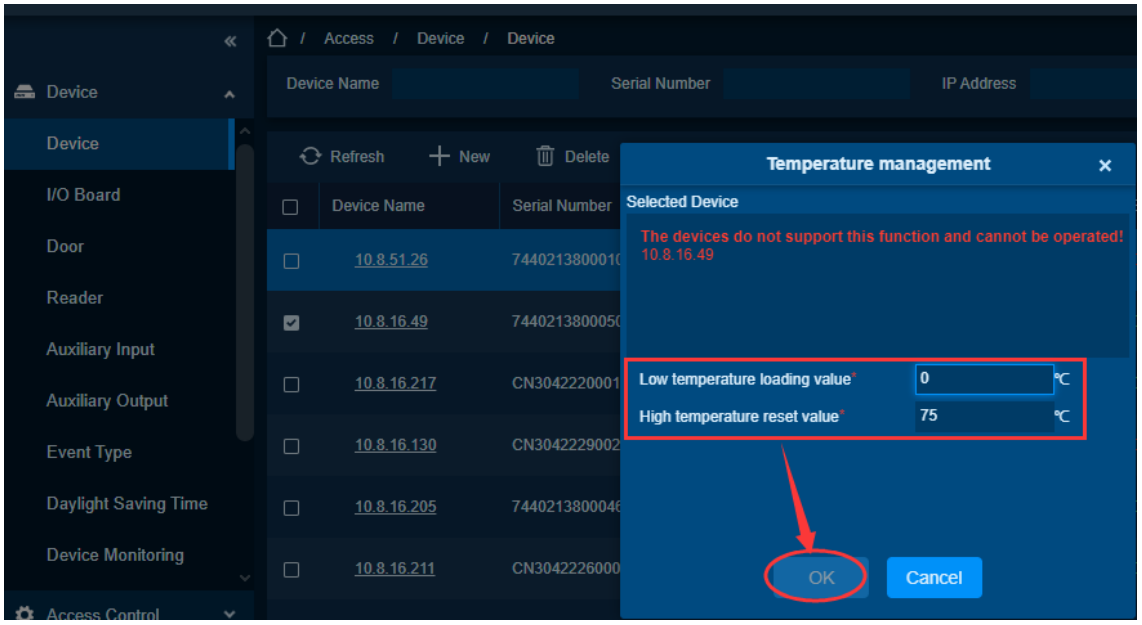
Send the set value to the device, and trigger according to this value at low temperature or high temperature.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the setting page.
- Click **[Temperature Management]** to jump out of the setting interface and set the corresponding parameters.
- Click **[OK]** to synchronize the settings to the device.



- On the Temperature Management interface, enter Low Temperature Loading Value, High Temperature Reset Value and click **OK.**



Set the Sleep Time

Preconditions for Normal Use of Function

Log in to the system with current account and ensure the device is online.

Function Usage Scenario

The device needs to go to dormant status when it has not been operated for a time.

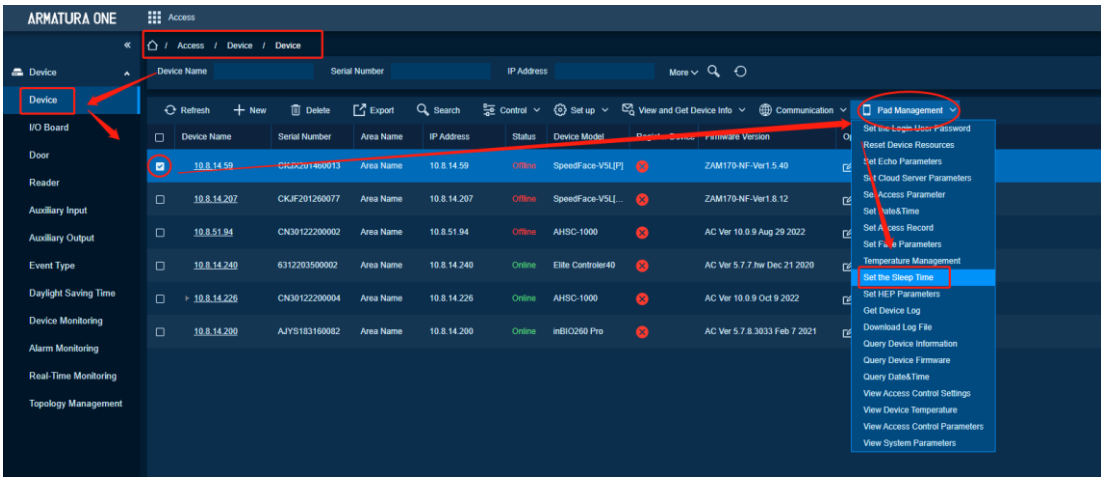
Feature Trigger Result

The device is inactive according to the set sleep time.

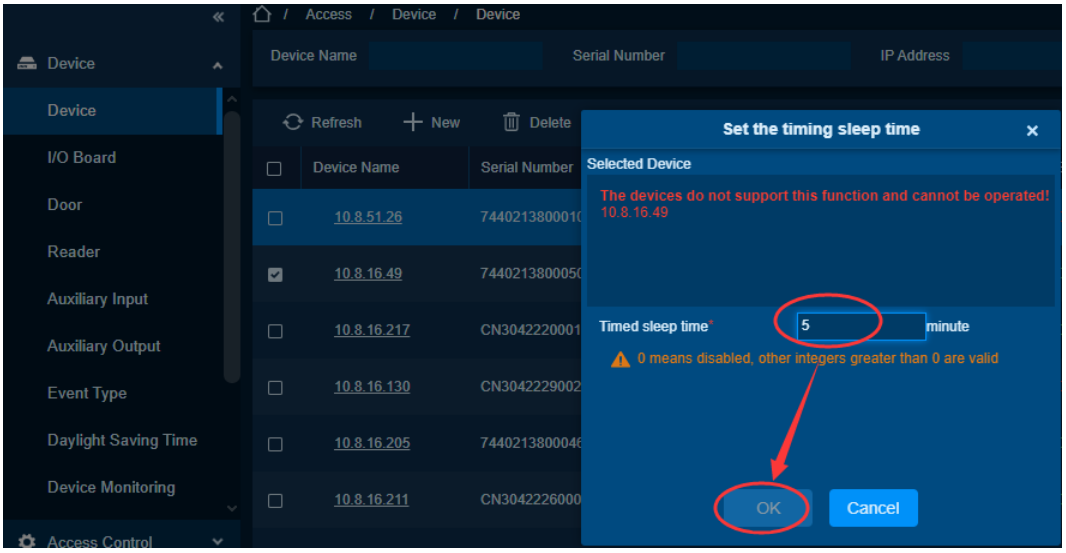
Steps:

- Click **[Access Control Device]** > **[Device]** > **[Pad Management]** to display the settings page.
- Click **[Set the Sleep Time]** to exit the setting interface and set the corresponding parameters.

- Click **[OK]** to synchronize the settings to the device.



- Click **[OK]** to start the process.



Settings-Set HEP Parameters

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device has a temperature measurement function

Function Usage Scenarios

The measurement parameters set by the device are wrong, and the new temperature measurement parameters need to be modified.

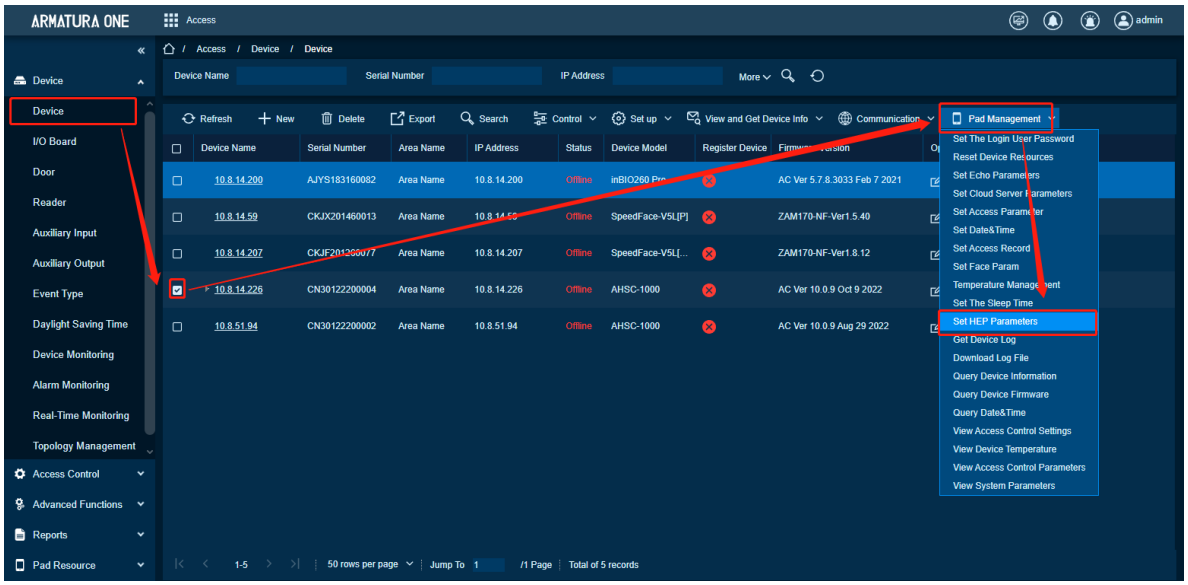
Feature Trigger Result

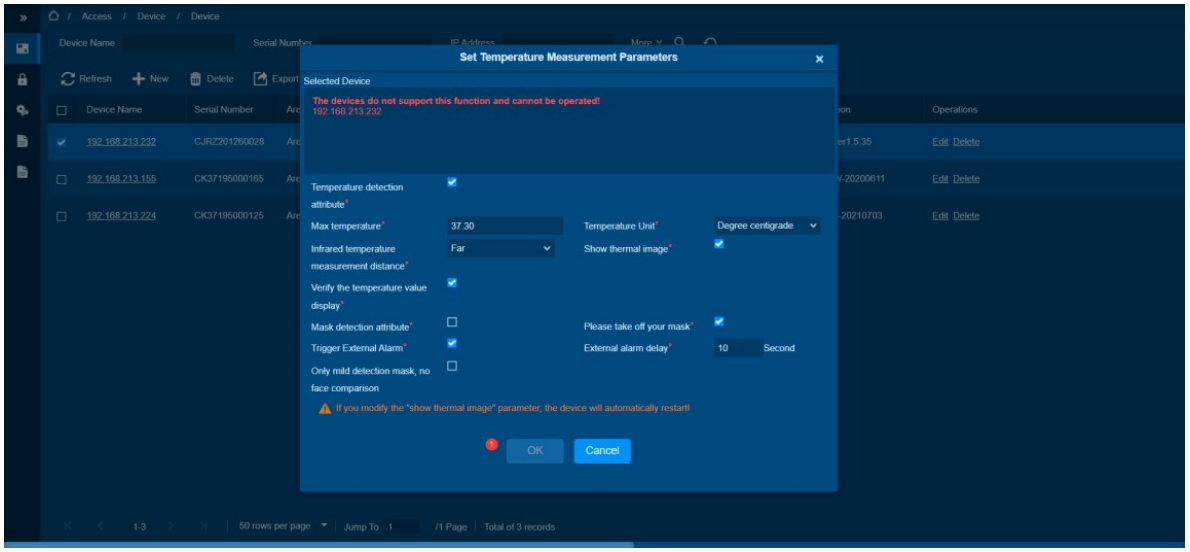
The temperature measurement parameters set by the device synchronization.

Steps:-

- Click [**Access Control Device**] > [**Device**] > [**Pad Management**] to display the setting page.

- Click [**Set HEP Parameters**] to jump out of the setting interface and set the corresponding parameters.
- Click [**OK**] to synchronize the settings to the device.





Get Device Log

Preconditions for Normal Use of Function

Log in to the system with current account and the system have the authority.

Function Usage Scenarios

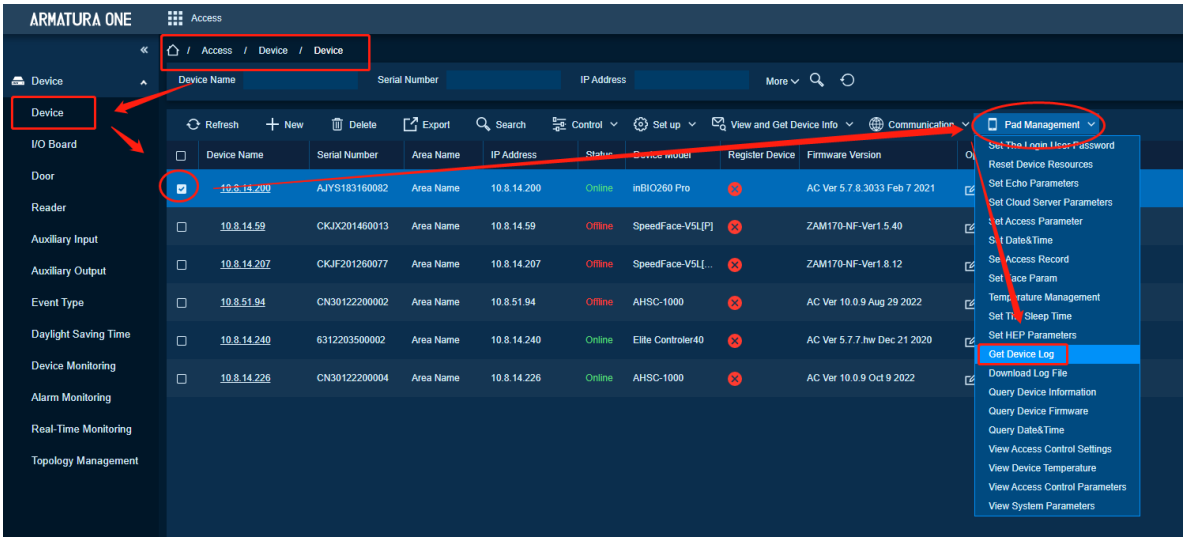
The software needs to obtain the log status of the device.

Feature Trigger Result

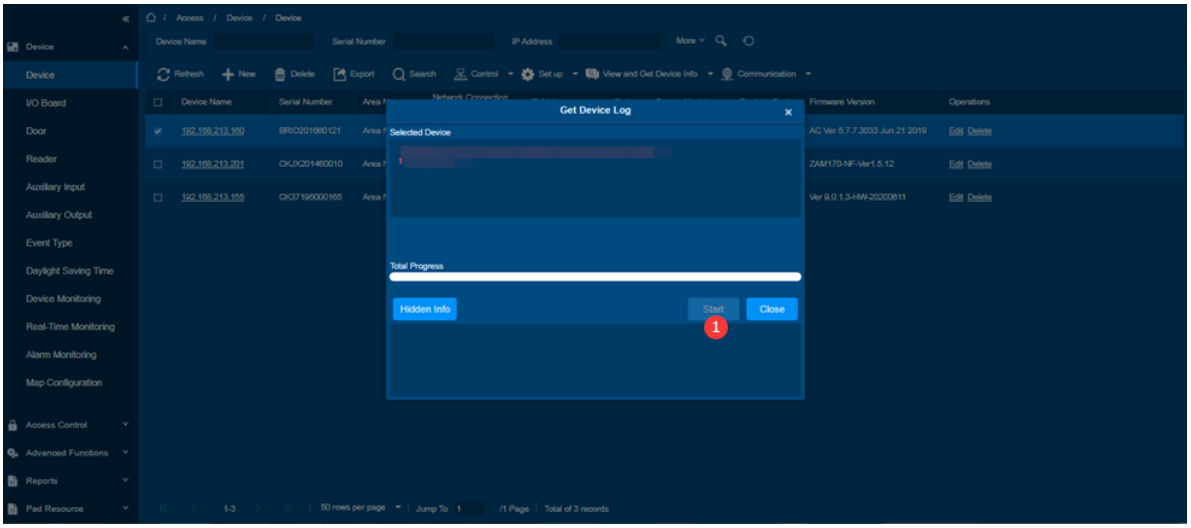
The log in the device is synchronized to the software and can be viewed in **[Access Control]>[Report]>[All Records].**

Steps:-

- Click **[Access Control Device] > [Device] >[Pad Management]** to display the view page.
- Click **[Get Device Log]** to exit the interface.
- Click **[Start]** to get the corresponding data from the device to the software.



- On Get Device Log interface, click **Start** to start the process.



Download Log File

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

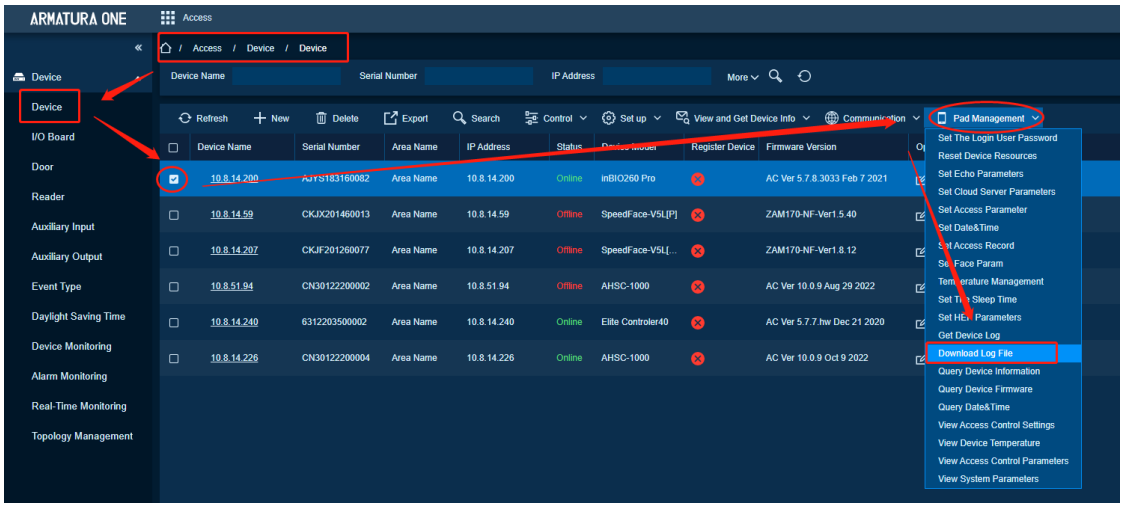
The software needs to view the log of the device.

Feature Trigger Result

Successfully downloaded the log of the device

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the setting view page
- Click **[Download Log File]** to exit the interface and click **OK.**



Query Device Information

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

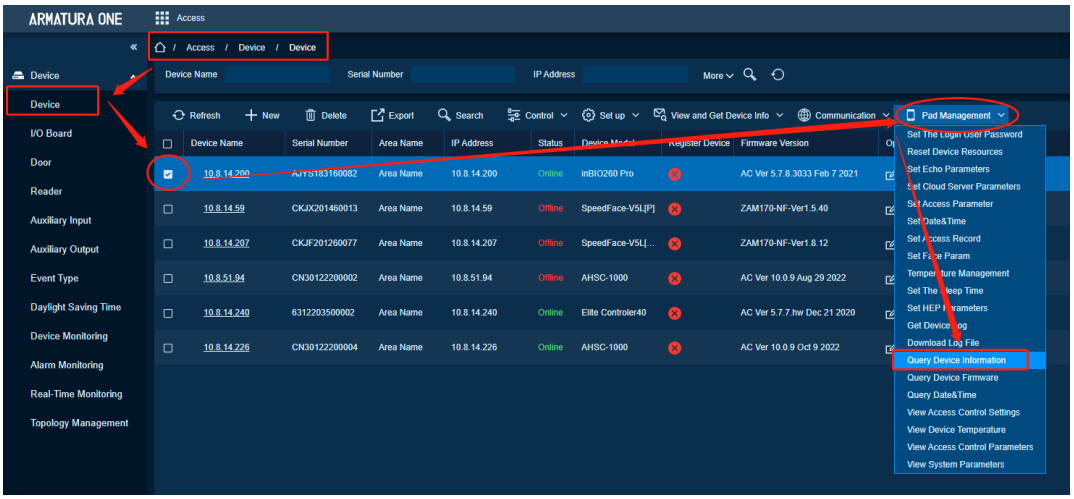
Need to obtain detailed information such as device version.

Feature Trigger Result

Get device information.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the view page.
- Click **[Query Device Information]** to jump out of the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



Query Device Firmware

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

Need to obtain the protocol version, firmware version and other information of the device.

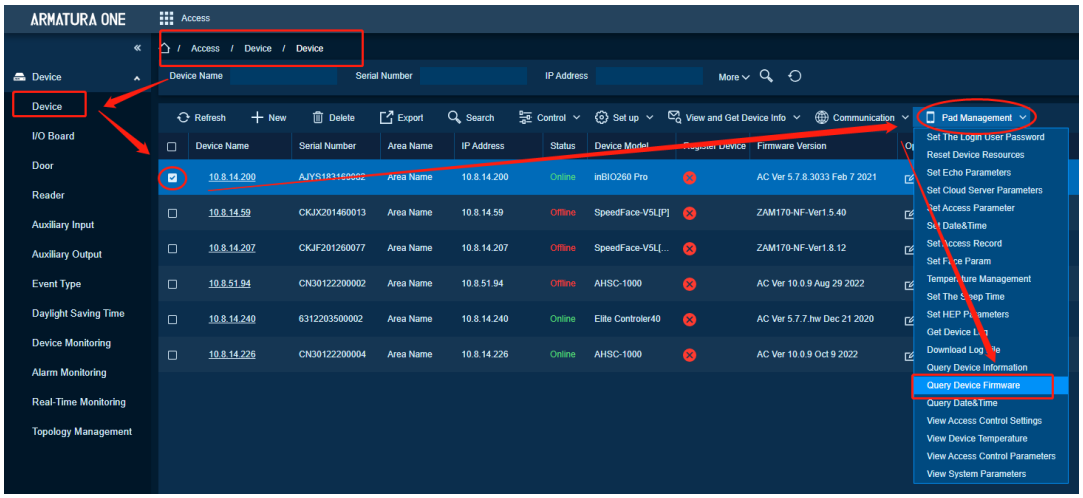
Check whether the version information is correct

Feature Trigger Result

Get firmware information.

Steps:

- Click **[Access Control Device] > [Device] > [View and Get Device Info]** to display the view page.
- Click **[Query Device Firmware]** to jump out of the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



Query Date &Time

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. The device is online.

Function Usage Scenarios

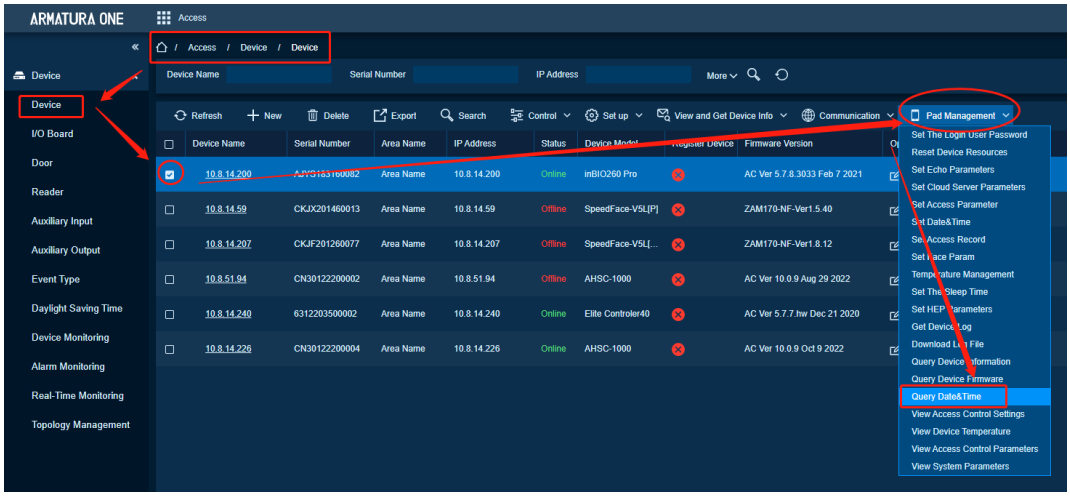
Get the specific time and date of the device. Check the specific time and date of the device

Feature Trigger Result

Get time and date

Steps:

- Click **[Access Control Device] > [Device] > [View and Obtain Information]** to display the view page.
- Click **[Query Date & Time]** to exit the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



View Access Control Settings

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. The device is online.

Function Usage Scenarios

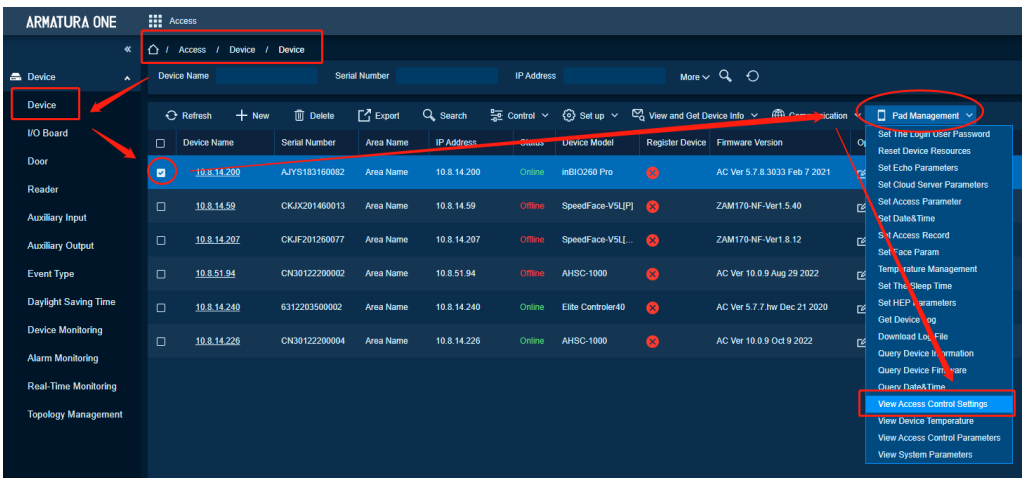
The software needs to check the access control record settings.

Feature Trigger Result

Quickly view access control record settings.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the view page.
- Click **[View Access Control Settings]** to jump out of the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



View Device Temperature

Preconditions for Normal Use of Function

Log in to the system with the current account ad have the authority. The device is online.

The device has a temperature measurement function.

Function Usage Scenarios

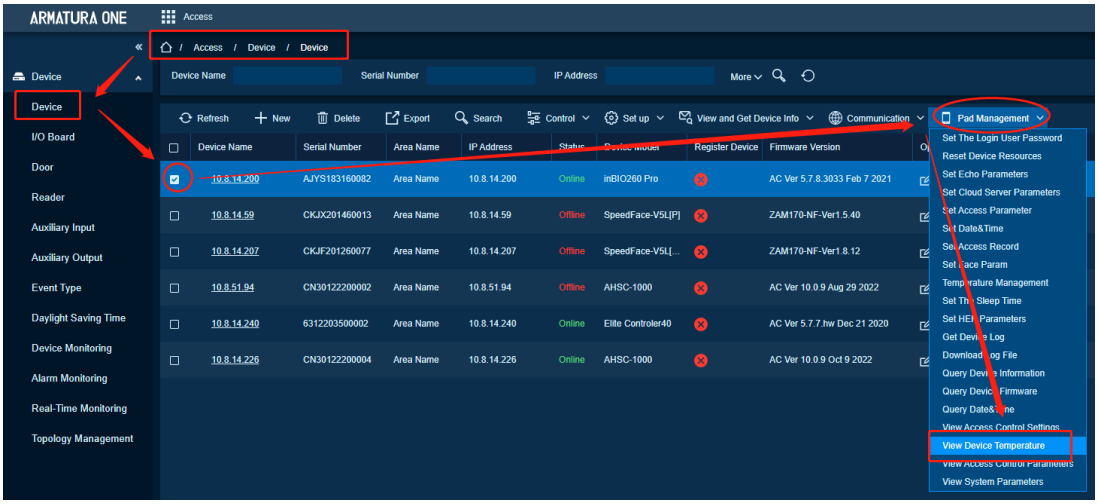
Need to check the temperature setting of the device to check whether the temperature of the device is normal.

Feature Trigger Result

View device temperature.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Pad Management]** to display the view page.
- Click **[View Device Temperature]** to jump out of the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



View Access Control Parameters

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is online.

Function Usage Scenarios

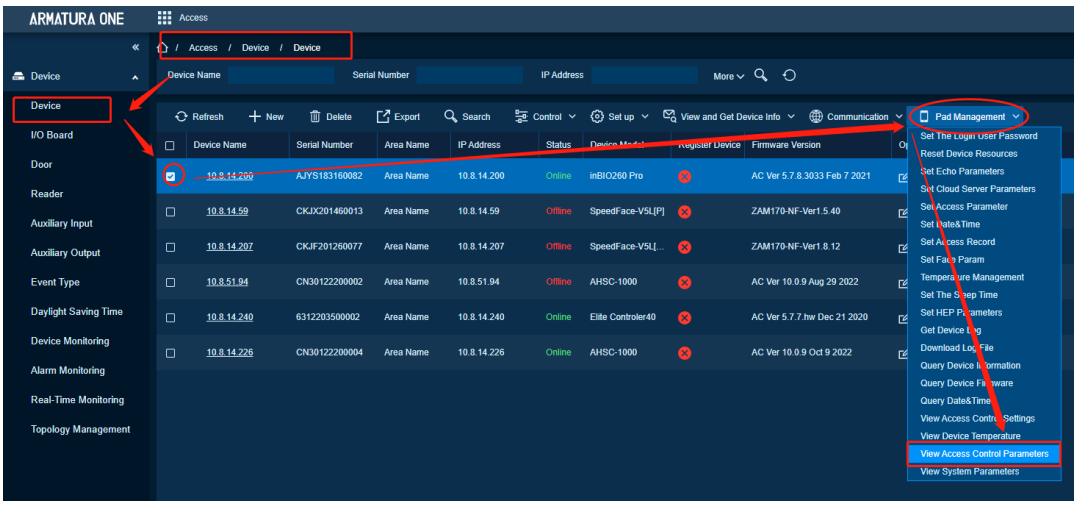
The software needs to check the access control parameters of the current device to configure it correctly in the software.

Feature Trigger Result

View access control parameters, including Gate Mode, Door Opening Mode, and host status.

Steps:

- Click **[Access Control Device]** > **[Device]** > **[Pad Management]** to display the view page.
- Click **[View Access Control Parameters]** to jump out of the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



View System Parameters

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. Ensure that the device is online.

Function Usage Scenarios

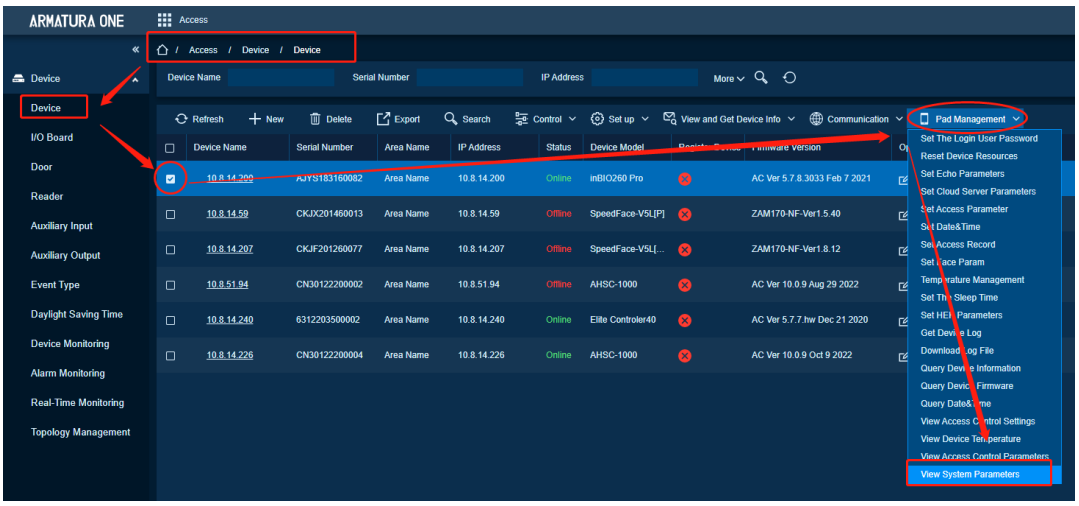
Software needs to view system parameters.

Feature Trigger Result

Get system parameters.

Steps:

- Click **[Access Control Device] > [Device] > [Pad Management]** to display the view page.
- Click **[View System Parameters]** to exit the interface.
- Click **[View]** or **[View All]** to get the corresponding data from the device to the software.



Device Operation

Edit Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.
Select device, or click "Edit" to pop up the [Edit] window

Function Usage Scenarios

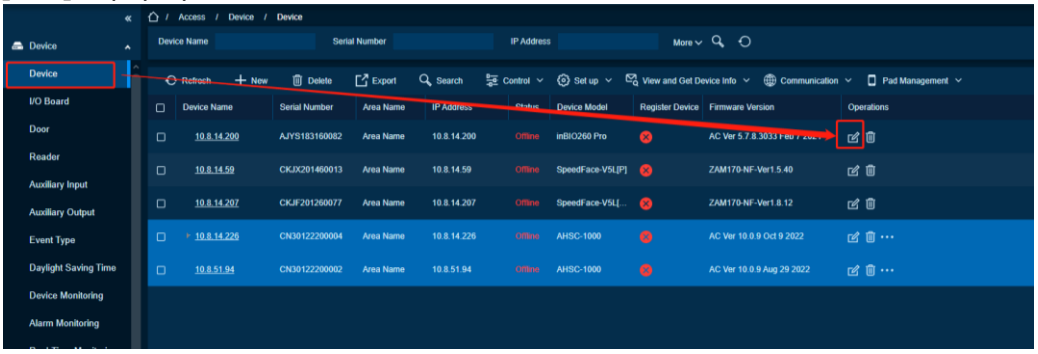
Edit device parameter, enable ‘fire input’ detection, change Time zone and DST, etc.

Feature Trigger Result

After [Fire Input Type] and [Fire Input EOL Resistance] are set, controller will monitor ‘Fire Input’ Interface. When different resistance values are selected, the voltage range used to judge the status is not consistent. There are four states, Active/In-Active/Short/Open.

Steps:

- Click **[Access Control Device] > [Device]** to display the view page.
- Click **[Edit]** to pop up an Edit interface.



Spada Device
Armatura AHSC-1000
Armatura AHDU-1X60

Parameter	Introduction
Device Name*	Editable, will check whether duplicated with other devices
Communication Type*	Read only
IP Address*	Read only, get from device
Communication Port*	Read only, get from device
Icon Type*	Editable, Drop list with selections Door/ Turnstile
Control Panel Type	Read only
Area*	Editable, can select area and child area where user has authorized from system user permission
Fire Input Type	Editable. Drop list with selections None/Normally Open/Normally Closed, if select none, it indicates system will not monitor 'Fire Input' Interface so that will not get Fire Alarm. [Fire Input EOL Resistance] will not allow to select.
Fire Input EOL Resistance	Drop list with selection 1.2K/2.2K/4.7K/10K. This value is from the Resistor used in electric circle.
Time Zone	Editable, select the time zone to which the current device belongs to. System already has a 'Time Zone and DST' list.
Set Daylight Saving Time	Editable. After the device selects a time zone, if the time zone support DST, you can select to enable DST or not according to the actual condition. By default, the DST is disabled. If the time zone does not support it, the system displays that the time zone does not support DST

✍**Note:**

If the device [Control Panel Type] is incorrect, manually delete the device and add it again.

* Indicates mandatory filed

Delete Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.

Function Usage Scenarios

The data of the device configuration is wrong and needs to be added again

Feature Trigger Result

If Spada Protocol device, when delete from **[Access]** > **[Device]**, Device in **[system]** > **[Authorized Device]** will also delete.

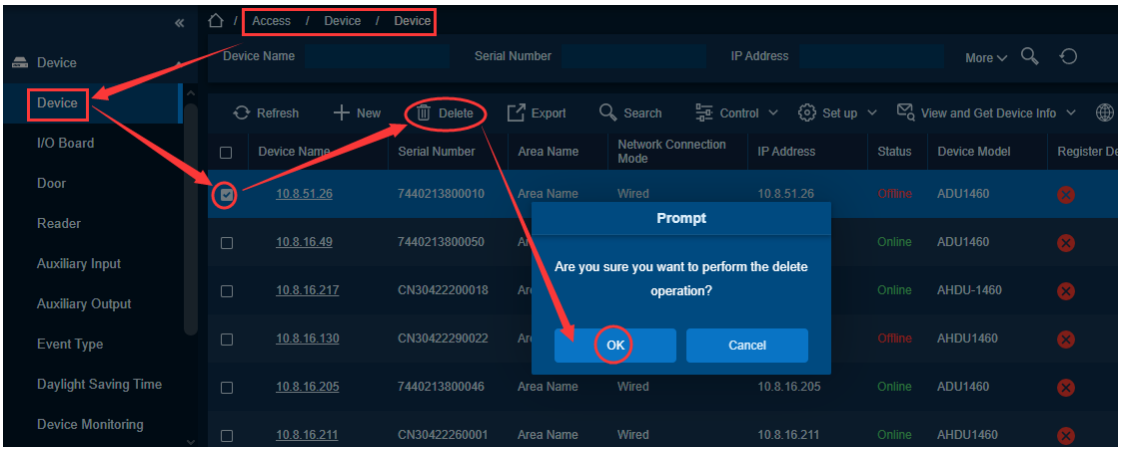
If primary controller deletes from **[Access]** > **[Device]**, secondary controller will also delete.

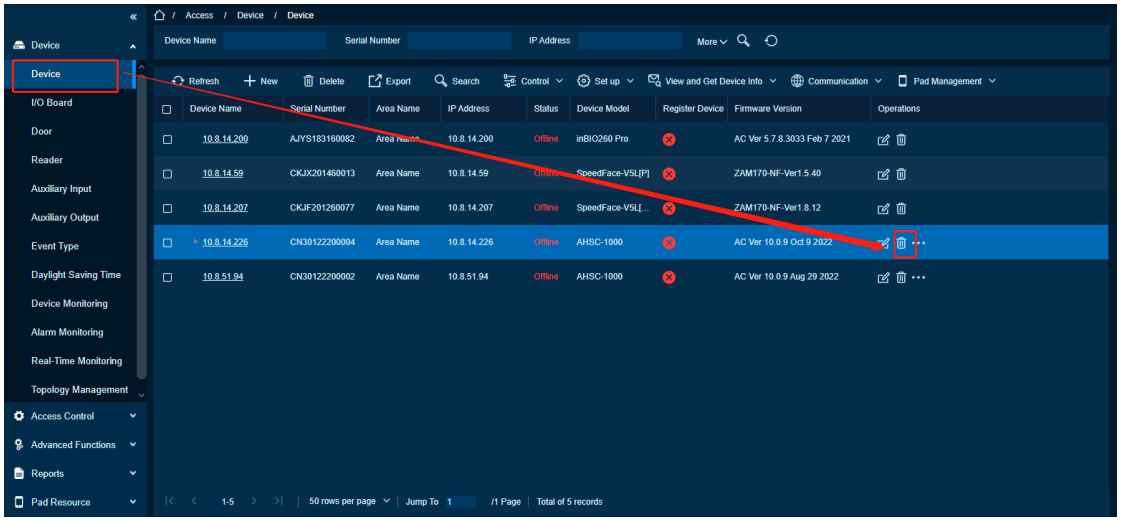
Limit

If device participate in anti-passback/interlock rules, will not allow to delete.

Steps:

Click **[Access Control Module] > [Device] > [Delete],** the delete page is displayed:

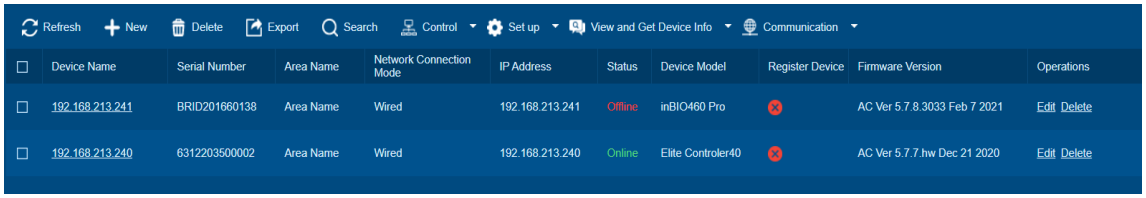




✍Note:

If delete primary controller, all secondary controllers will also be deleted

For communication between the system and device, data uploading, configuration downloading, device and system parameters shall be set. Users can edit the access controllers within relevant levels in the current system. Users can only add or delete devices in Device Management if needed.



Add Sub-Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.

Function Usage Scenarios

After adding primary controller successfully, add a secondary controller

Feature Trigger Result

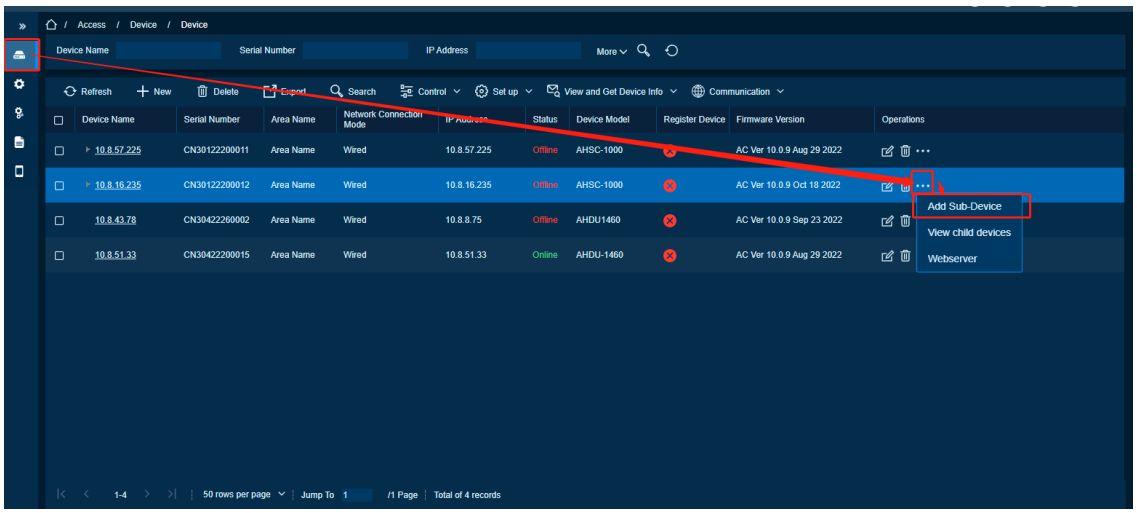
After setting Primary-Secondary Relationship is built up, all commands will send to primary controller, and primary control will distribute command to different secondary controller.

Limit

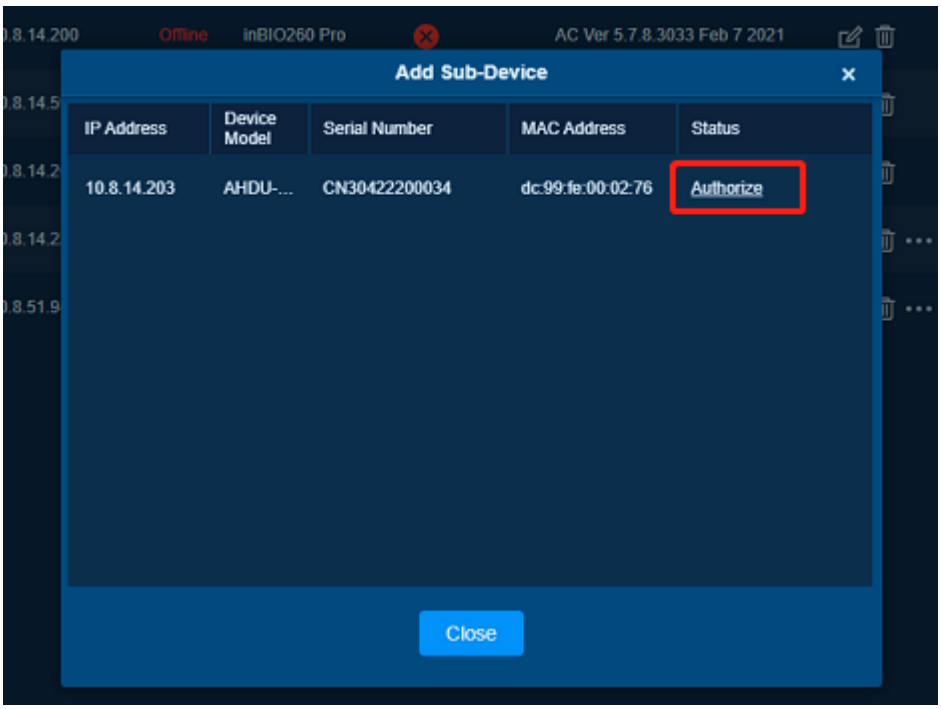
This function only support for AHSC-1000 Device

Steps:

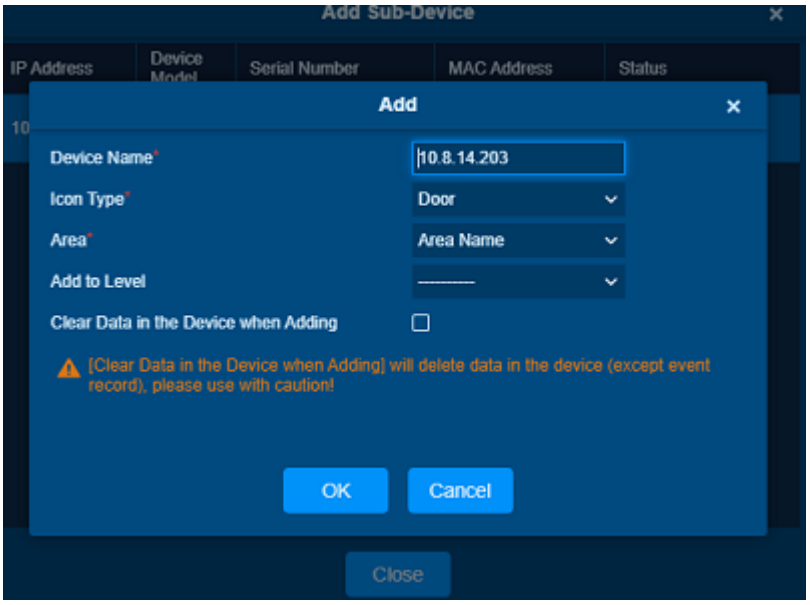
- Click **[Access Control Device] > [Device]** to display the view page.
- Click **[…] > [Add Sub-Device]** to display the Add Sub-Device page.



- Click **[Authorize]**



- Click **[OK] to save**



View Sub-Device

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.

Function Usage Scenarios

After adding secondary controller successfully.

Feature Trigger Result

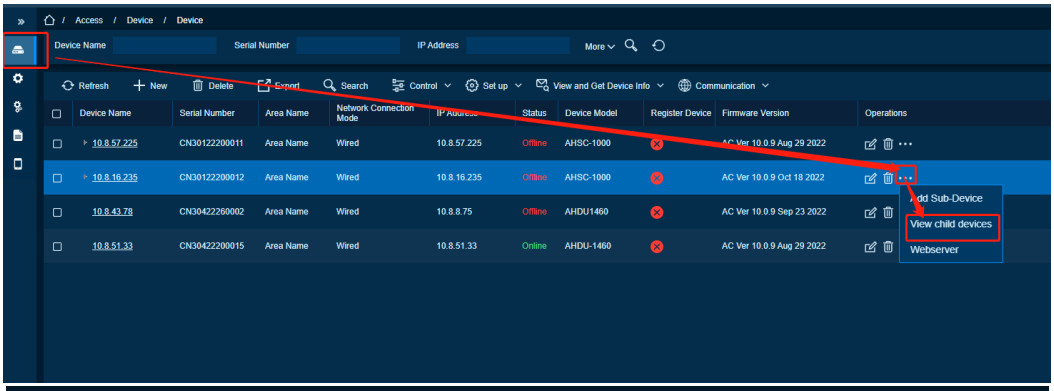
Check Primary-Secondary Relationship

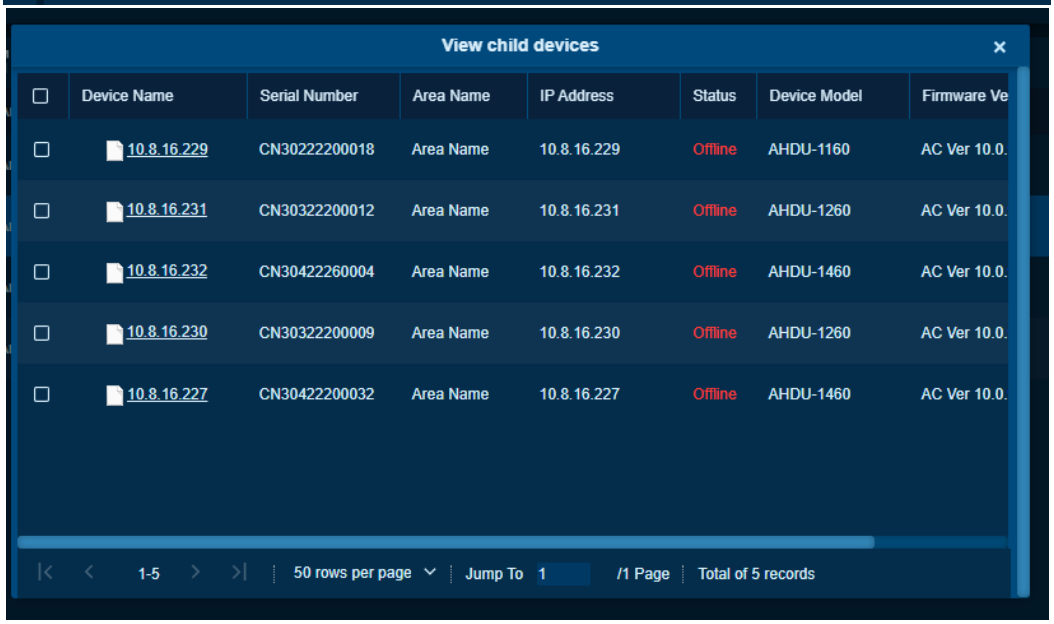
Limit

This function only support for AHSC-1000 Device

Steps:

- Click **[Access Control Device] > [Device]** to display the view page.
- Click **[…] > [View Sub-Device]** to display the Add Sub-Device page.





Webserver

Preconditions for Normal Use of Functions

Log in to the system with the current account and have permission to delete the device.

Function Usage Scenarios

Click icon to view controller's webserver.

Feature Trigger Result

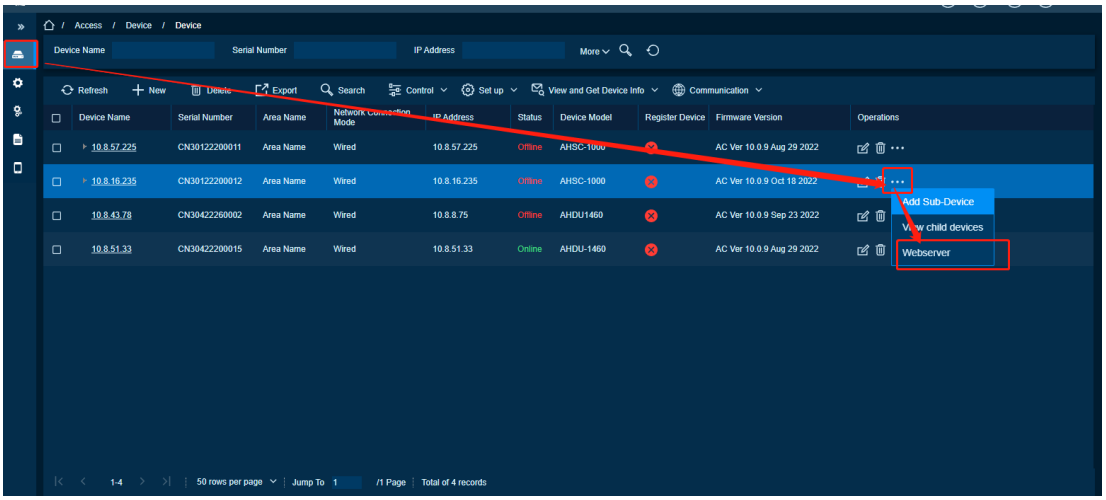
Open Controller's Webserver in new page in Browser.

Limit

This function only support for AHSC-1000 and AHDU-1X60 Device

Steps:

- Click **[Access Control Device]** > **[Device]** to display the view page.
- Click **[Webserver] will jump to device's webserver.**



6.1.2. I/O Board

Function Description

By connecting to the I/O expansion board, the number of doors can be expanded, and more doors can be operated.

New Device

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

The current area needs to be expanded with more doors.

Feature Trigger Result

One device can control multiple doors.

Steps:

Parameter		Introduction
Name*		Editable
Device Name*		Read only, select target device
Protocol Type*		Editable, drop list with selections OSDP/Aperio
I/O Board Type*		Editable, drop list will follow **Protocol Type**, if OSDP, drop list will be [AHEB0216/1602/0808], if Aperio, drop list will be [AH30]
OSDP	**RS-485 Port***	Editable, drop list will follow **Protocol Type**, filter which RS-485 Port is using this protocol.
	RS-485 Address*	Editable, range is from 1-255
Aperio	**Device Addressing Mode***	Editable, drop list will be [Normal address offset/Legacy address offset]
	RS-485 Port*	Editable, drop list will follow **Protocol Type**, filter which RS-485 Port is using this protocol.
	RS-485 Address*	Editable, range is from 1-15

Aperio Device

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

Connect Aperio AH30 hub to AHSC-1000 via RS-485

Feature Trigger Result

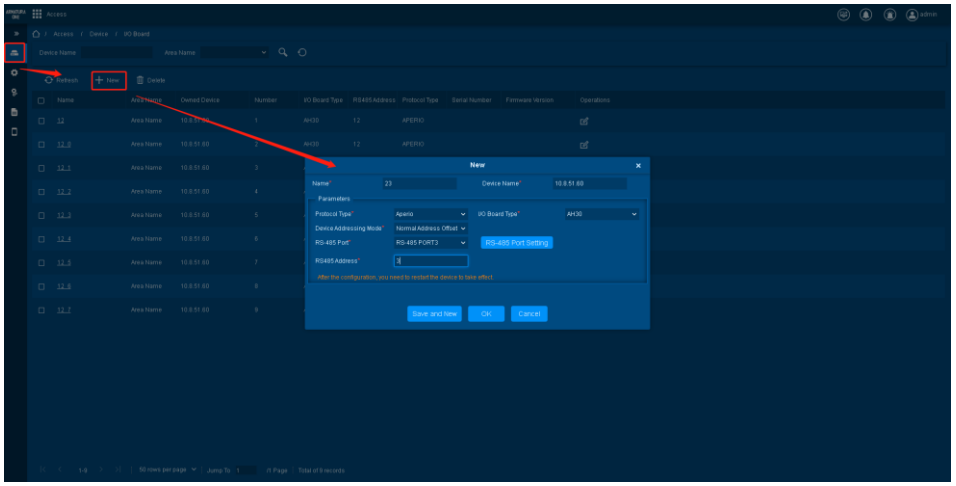
Will create several virtual I/O Boards in **[I/O Board]** and Virtual Doors in **[Door]**

Limit

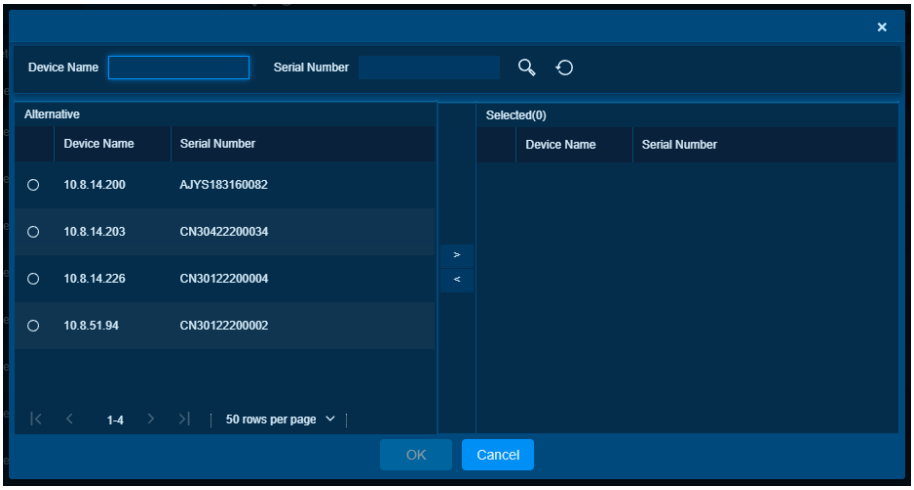
Only AHSC-1000 can support.

Steps:

- Click **[Access Control Device] > [I/O Board] > [New]** to display the new page.
- Enter **Name**



- Click **Device Name** to pop-up a device select window



- Select a device, click **OK**
- Select **Device Addressing Mode**
  - Normal Address Offset

Addressing table – normal address offset

An AH30 communication hub can pair with up to 8 locks. When pairing several locks to a communication hub, the following addresses are used for the address range 1-15. Above this range only one lock can be paired.

DIP 4 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x11, 0x21, 0x31, 0x41, 0x51, 0x61, 0x71
0010	0x02	0x02, 0x12, 0x22, 0x32, 0x42, 0x52, 0x62, 0x72
0011	0x03	0x03, 0x13, 0x23, 0x33, 0x43, 0x53, 0x63, 0x73
0100	0x04	0x04, 0x14, 0x24, 0x34, 0x44, 0x54, 0x64, 0x74
0101	0x05	0x05, 0x15, 0x25, 0x35, 0x45, 0x55, 0x65, 0x75
0110	0x06	0x06, 0x16, 0x26, 0x36, 0x46, 0x56, 0x66, 0x76
0111	0x07	0x07, 0x17, 0x27, 0x37, 0x47, 0x57, 0x67, 0x77
1000	0x08	0x08, 0x18, 0x28, 0x38, 0x48, 0x58, 0x68, 0x78
1001	0x09	0x09, 0x19, 0x29, 0x39, 0x49, 0x59, 0x69, 0x79
1010	0x0A	0x0A, 0x1A, 0x2A, 0x3A, 0x4A, 0x5A, 0x6A, 0x7A
1011	0x0B	0x0B, 0x1B, 0x2B, 0x3B, 0x4B, 0x5B, 0x6B, 0x7B
1100	0x0C	0x0C, 0x1C, 0x2C, 0x3C, 0x4C, 0x5C, 0x6C, 0x7C
1101	0x0D	0x0D, 0x1D, 0x2D, 0x3D, 0x4D, 0x5D, 0x6D, 0x7D
1110	0x0E	0x0E, 0x1E, 0x2E, 0x3E, 0x4E, 0x5E, 0x6E, 0x7E
1111	0x0F	0x0F, 0x1F, 0x2F, 0x3F, 0x4F, 0x5F, 0x6F, 0x7F

When configuring installations that differ from the default configuration described in section DIP 1-5 – Selecting the EAC address/Automatic paring on page 38, use this table to keep track of what addresses are used by the locks/sensors in your installation in order to avoid addressing conflicts according to section *"Installation examples" on page 44* for mixed installations.

Aperio® Online Mechanical Installation Guide, Document No: ST-001323-E Date: 30 mars 2016

- Legacy Address Offset

Addressing table – legacy address offset

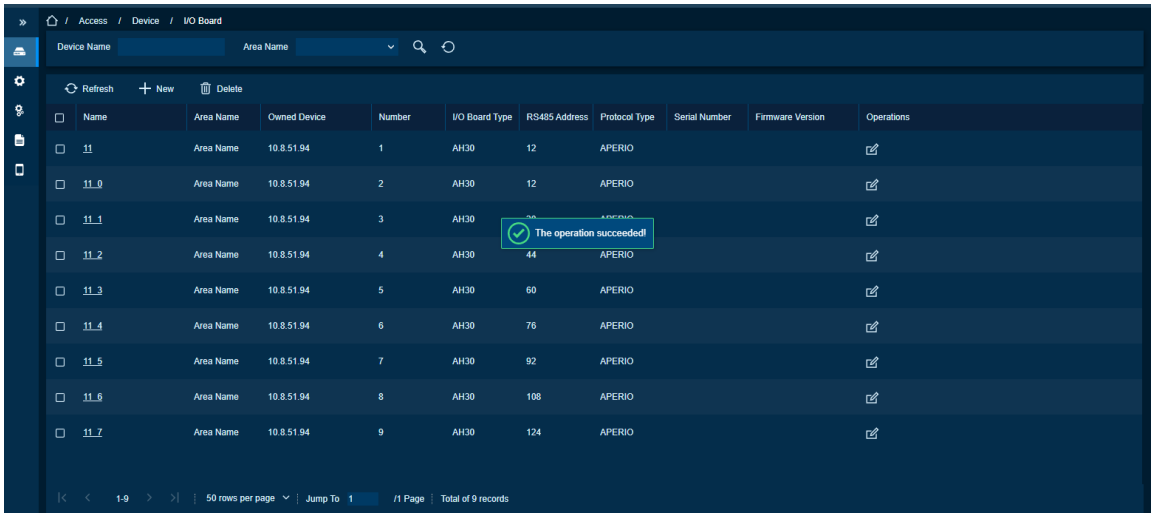
Legacy addressing mode is an alternative addressing mode that can be set by the Programming Application in the configuration wizard. The lock addresses in this mode are set consecutively. For example, if communication hub has address 1, the locks will get address 1-8, 9-16, 17-24 etc.

DIP 5 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08
0010	0x02	0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10
0011	0x03	0x11, 0x12, 0x13, 0x14, 0x14, 0x16, 0x17, 0x18
0100	0x04	0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x20
...		

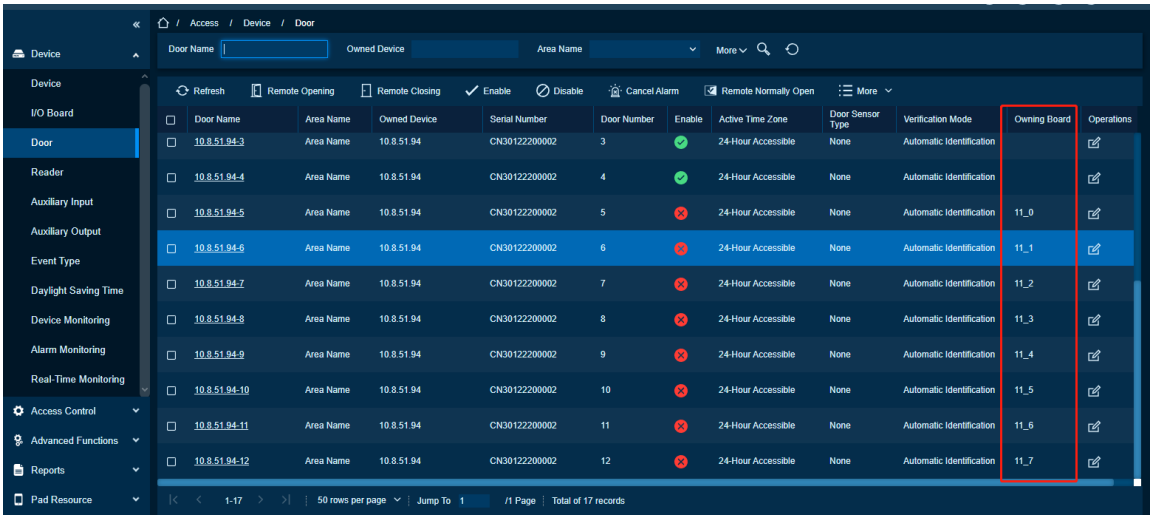
This mode is used for older EAC systems that cannot handle high EAC addresses where the limit for example is 32 or 64.

Picture regards from ST-001323-Aperio Online Mechanical Installation Manual-E-US.pdf

- Select [RS-485 Port], system will filter via Protocol, if check protocol please refer to Set RS-485 Port Setting
- Input [RS-485 Address], range is from 1-15
- Click **OK**



- System will generate several virtual devices in I/O Board



- System will generate several doors which are bound to owning board which is auto generate in I/O Board Page.

AHEB0216/0808/1602

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

Connect AHEB0216/0808/1602 to AHSC-1000 via RS-485

Feature Trigger Result

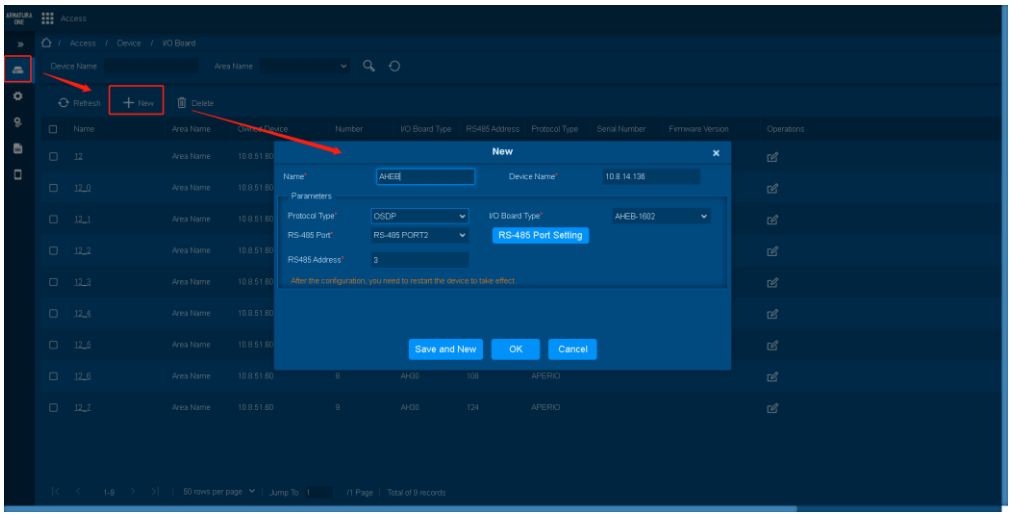
Will create several auxiliary inputs in [Auxiliary Input]and Auxiliary Outputs in [Auxiliary Output]

Limit

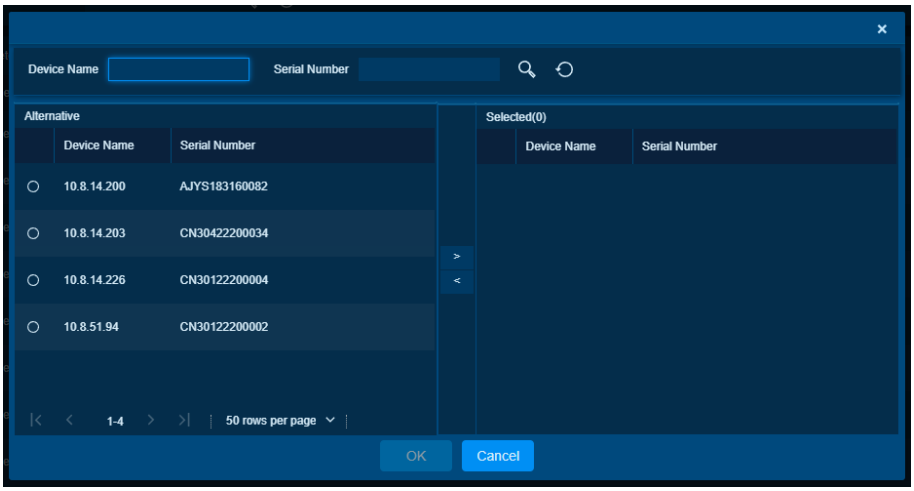
Only AHSC-1000 and AHDU-1X60 can support.

Steps:

- Click **[Access Control Device] > [I/O Board] > [New]** to display the new page.
- Enter each parameter, click **[OK]** to save the expansion board.



- Click **Device Name** to pop-up a device select window



- Select a device, click **OK**
- Select [RS-485 Port], system will filter via Protocol, if check protocol please refer to Set RS-485 Port Setting
- Input [RS-485 Address], range is from 1-255
- Click **OK**

Delete Device

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. There is a successful addition in the extended list.

Function Usage Scenarios

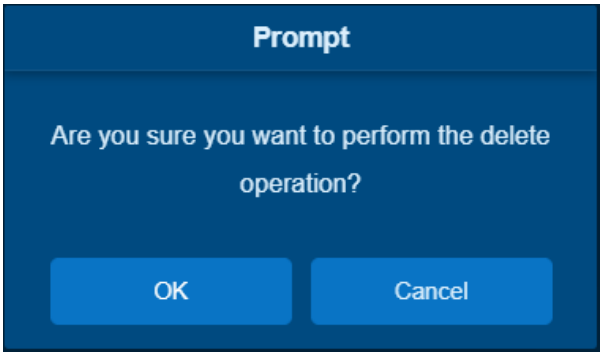
The device in the current area does not need to expand the door.

Feature Trigger Result

Delete the corresponding expansion board.

Steps:

Click **[Access Control Device] > [I/O Board] > [Delete]** to display the delete page.



6.1.3. Door

Function Description

Operate the door of each device, remotely operate the door, and enable or disable the door of the device.

Edit Door

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is added successfully.

Function Usage Scenarios

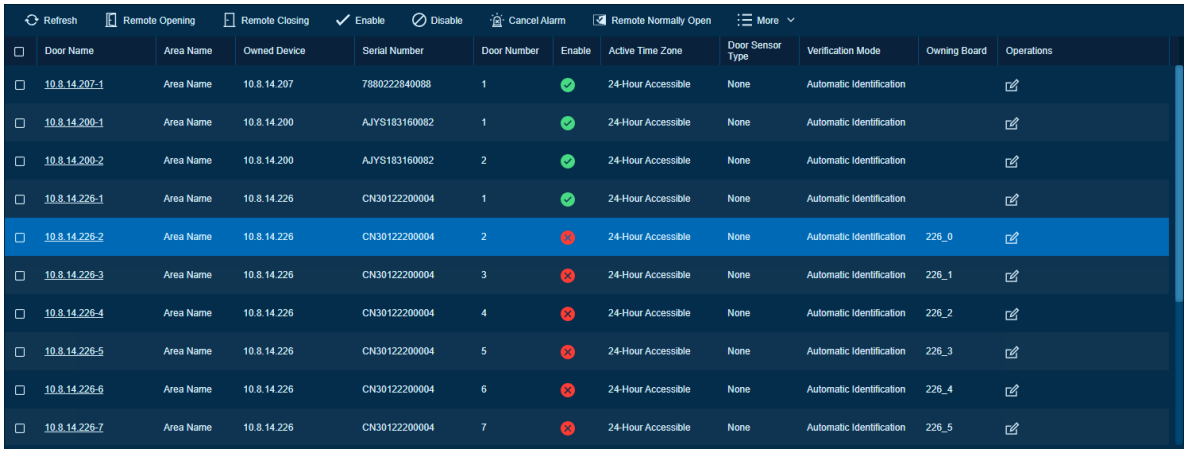
Need to modify the parameter configuration and other information of the corresponding door.

Feature Trigger Result

Modify the corresponding configuration.

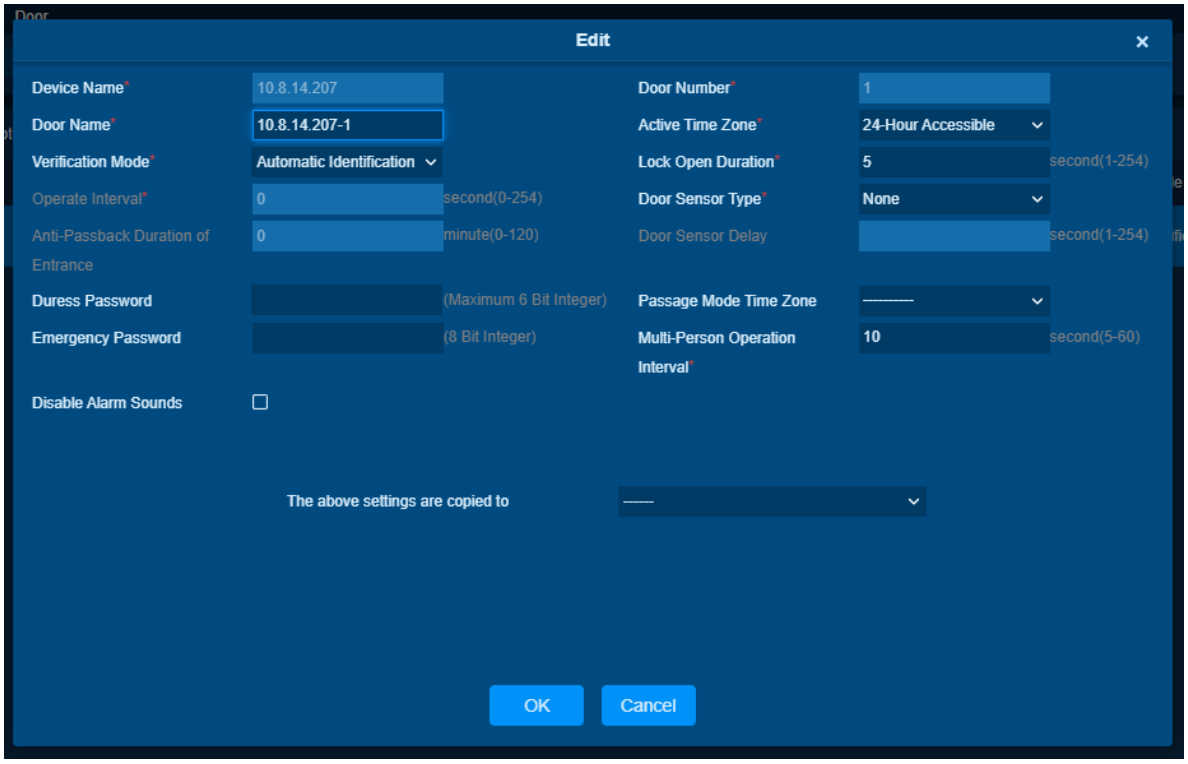
Steps:

Click **[Access Device] > [Device] > [Door]** to enter Door Management interface (click "**Area Name**" in the left, system will automatically filter and display all access devices in this area).



OmniAC Series Controller

Select the door to be modified and click **[Door Name]** or **[Edit]** button below operations to open the Edit interface.



Fields are as follows:

Device Name: Non editable.

Door Number: Non editable. It should be 1, standalone reader only has one relay.

Door Name: The default is “device name - door number”. The field can be modified as needed. Up to 30 characters can be entered.

Active Time Zone: Active Time Zone must be input, so that the door can be opened and closed normally. A Passage Mode Time Zone must be set within the Active Time Zone. By default, **Active Time Zone** is 24-Hour Accessible, **Passage Mode Time Zone** is null.

✍**Note:**

For a door, in Normal Open state, a person who is allowed to be verified 5 times consecutively (verification interval should be within 5 seconds) can release the current Normal Open status and close the door. The next verification will be a normal verification. This function is only effective at the Active Time Zone of specified doors. And within the same day, other Normal Open intervals set for the door and First-Person Normally Open settings will not take effect anymore.

Lock Open Duration: It is the time for which the door remains unlocked after punching. The unit is second (range: 0 to 254 seconds), and the default value is 5 seconds.

Operate Interval: It is the Interval between two punches. The unit is second (range: 0~254 seconds), and the default value is 2 seconds.

Door Sensor Type: None (will not detect door sensor), Normal Open, Normal Close. The default value is NO. If you have selected as Normal Open or Normal Close, you need to set Door Sensor Delay and decide whether Close and Reverse-lock is required. When the door sensor type is set as Normal Open or Normal Close, the default door sensor delay is 15 seconds, and the close and reverse state is enabled.

Anti-Passback Duration of Entrance: Only one entry is allowed with a reader in this duration. The unit is minute (range: 0 to 120 minutes), and the default value is 0 minute.

Close and Reverse State: It will set to either lock or not lock the door after door closing. Check it for locking after door closing.

Verification Mode: Identification modes depends on device features. The default value is Automatic Identification.

For Example, OmniAC20/30 is a palm device which support PIN/Card/Face/Palm, so verification mode drop list will include

Only Pin, Only Password, Only Card, Only Palm Vein, Only Face, Card, or password, Card and Password, Face and Password, Face and Card, Palm Vein and Card, Palm Vein, and Face.

Anti-Passback Duration of Entrance: Based on the lock opening duration, the door sensor delays exit delay. The duration of the entry will be extended. To function this feature, you need to check **[**Delay passage**]** option to extend relevant duration when adding or editing staff information. For example, you may extend the duration of entrance for people with disabilities.

Open Door Delay: The time to keep the door open after the verification completes (range: 1 to 254 seconds).

Duress Password: Duress means any threats, violence, constraints, or other action used to coerce someone into doing something against their will. In these situations, enter the Duress Password (with an authorized card) to open the door. When the door is opened with the Duress Password, the alarm is triggered.

Emergency Password: Upon emergency, the user can use the Emergency Password (named Super Password) to open the door. The emergency Password allows normal opening, and it is effective in any time zone and any type of verification mode, usually used by the administrator.

✍**Note:**

Duress Password Opening (**used with an authorized card**): The Password should be a number not exceeding 6 digits. When Only Card verification mode is used, you need to press [ESC/*] first, and then

press the password and [OK/#] button, then finally swipe the authorized card. The door opens and triggers the alarm. When Card + Password verify mode is used, please swipe the authorized card first, then enter the password and click the [OK] button (same as normal opening in card plus password verification mode), the door opens and triggers the alarm.

Emergency Password Opening: The Password must be 8 digits. The door can be opened only by entering the password. Please press [ESC/*] every time before entering the password, and then press [OK/#] to execute.

When using Duress Password or Emergency Password, the interval for entering each number shall not exceed 10 seconds, and both the passwords should not be the same.

Multi-Person Operation Interval: The time interval between two verifications with cards or fingerprints (range: 5 to 60 seconds).

Disable Alarm Sound: Select the checkbox to disable the alarm sound in the real-time monitoring page.

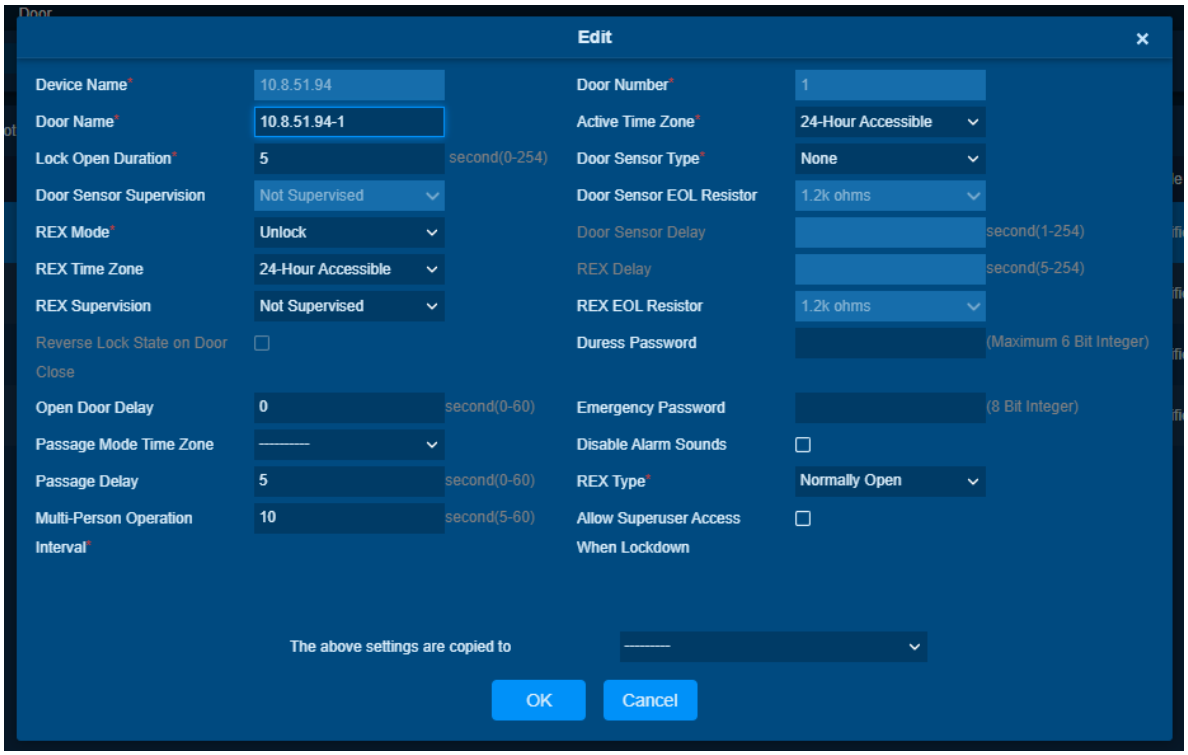
The above Settings are Copied to: It has below two options.

- All doors of current device: Click to apply the above settings to all the doors of the current access device.
- All doors of all devices: Click to apply the above settings to all the doors of all access devices within the current user's level.

After setting the parameter(s), click **[OK]** to save and exit.

Horizon Series Controller

Select the door to be modified and click **[Door Name]** or **[Edit]** button below operations to open the Edit interface.



Fields are as follows:

Device Name: Non editable.

Door Number: Non editable. System will automatically name it according to doors quantity of the device. This number will be consistent with the door number on the device.

Door Name: Editable. The default is “device name - door number”. The field can be modified as needed. Up to 30 characters can be entered.

Active Time Zone: Active Time Zone must be input, so that the door can be opened and closed normally. A Passage Mode Time Zone must be set within the Active Time Zone. By default, **Active Time Zone** is 24-Hour Accessible, **Passage Mode Time Zone** is null.

✍**Note:**

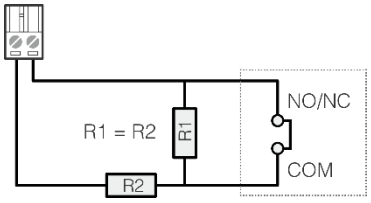
For a door, in Normal Open state, a person who is allowed to be verified 5 times consecutively (verification interval should be within 5 seconds) can release the current Normal Open status and close the door. The next verification will be a normal verification. This function is only effective at the Active Time Zone of specified doors. And within the same day, other Normal Open intervals set for the door and First-Person Normally Open settings will not take effect anymore.

Lock Open Duration: It is the time for which the door remains unlocked after punching. The unit is second (range: 0 to 254 seconds), and the default value is 5 seconds.

Door Sensor Type: None (will not detect door sensor), Normal Open, Normal Close. The default value is NO. If you have selected as Normal Open or Normal Close, you need to set Door Sensor Delay and decide whether Close and Reverse-lock is required. When the door sensor type is set as Normal Open or Normal Close, the default door sensor delay is 15 seconds, and the close and reverse state is enabled.

Door Sensor Supervision: It can select Not Supervised / Default Supervision, this function is available when **Door Sensor Type** is Normally Open/Normally Closed

Door Sensor EOL Resistor: It can select 1.2k ohm/2.2k ohm /4.7k ohm /10k ohm, this value is referring to the resistor used in electric circle. This function is available when **Door Sensor Supervision** selects Default Supervision.



Door Sensor Delay: The duration for delayed detection of the door sensor after the door is opened. When the door is not in the Normally Open period, and the door is opened, the device will start the counting. It will trigger an alarm when the delay duration is expired and stops the alarm when you close the door. The default door sensor delay is 15s (range: 1 to 254 seconds). Door Sensor Delay should be greater than the Lock Open Duration.

Request to Exit (REX Mode): Locking indicates that the door will be locked after the exit button is pressed. Unlocking indicates that the door will be unlocked after the exit button is pressed. The default value is unlocking.

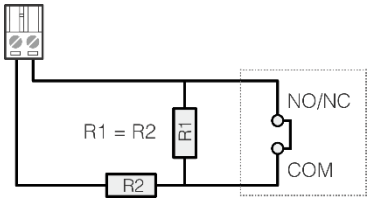
REX Time Zone: The button is available only in the specified time segment.

Request to Exit Delay (REX Delay): It indicates the alarm delay time for door detection after the exit button is locked. When the door is unlocked forcibly, the system will detect the door status after a period. The default is 10s (range: 1 to 254 seconds). The exit button must be locked before setting this option.

REX Type: None (will not detect REX INPUT), Normal Open, Normal Close. The default value is Normally Open.

REX Supervision: It can select Not Supervised / Default Supervision, this function is available when **REX Type** is Normally Open/Normally Closed

REX EOL Resistor: It can select 1.2k ohm/2.2k ohm /4.7k ohm /10k ohm, this value is referring to the resistor used in electric circle. This function is available when **REX Supervision** selects Default Supervision.



Reverse Lock State on Door Close: It will set to either lock or not lock the door after door closing. Check it for locking after door closing.

Open Door Delay: The time to keep the door open after the verification completes (range: 1 to 60 seconds).

Multi-Person Operation Interval: The time interval between two verifications with cards or fingerprints (range: 1 to 60 seconds).

Duress Password: Duress means any threats, violence, constraints, or other action used to coerce someone into doing something against their will. In these situations, enter the Duress Password (with an authorized card) to open the door. When the door is opened with the Duress Password, the alarm is triggered.

Emergency Password: Upon emergency, the user can use the Emergency Password (named Super Password) to open the door. The emergency Password allows normal opening, and it is effective in any time zone and any type of verification mode, usually used by the administrator.

✍**Note:**

Duress Password Opening (**used with an authorized card**): The Password should be a number not exceeding 6 digits. When Only Card verification mode is used, you need to press [ESC/*] first, and then press the password and [OK/#] button, then finally swipe the authorized card. The door opens and triggers the alarm. When Card + Password verify mode is used, please swipe the authorized card first, then enter the password and click the [OK] button (same as normal opening in card plus password verification mode), the door opens and triggers the alarm.

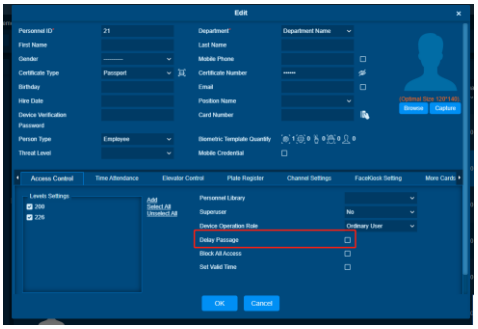
Emergency Password Opening: The Password must be 8 digits. The door can be opened only by entering the password. Please press [ESC/*] every time before entering the password, and then press [OK/#] to execute.

When using Duress Password or Emergency Password, the interval for entering each number shall not exceed 10 seconds, and both the passwords should not be the same.

Disable Alarm Sounds: Select the checkbox to disable the alarm in the real-time monitoring page.

Passage Mode Time Zone: After **Passage Mode Time Zone** is set, when time in this period, door will keep open until out of this time zone, if you want to close the door, you can **disable intraday Passage Mode Time Zone.**

Passage Delay: In [Personnel]-> [Edit Personnel] Page, some personnel who is set **Delay Passage**, when this personnel access granted, he will get an extended time to pass the channel.



Allow Superuser Access When Lockdown: This function is a feature to control whether superuser can access door when lockdown.

The above Settings are Copied to: It has below two options.

- All doors of current device: Click to apply the above settings to all the doors of the current access device.
- All doors of all devices: Click to apply the above settings to all the doors of all access devices within the current user's level.

After setting the parameter(s), click **[OK]** to save and exit.

Remote Opening

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. Ensure that the device is added successfully.

Function Usage Scenarios

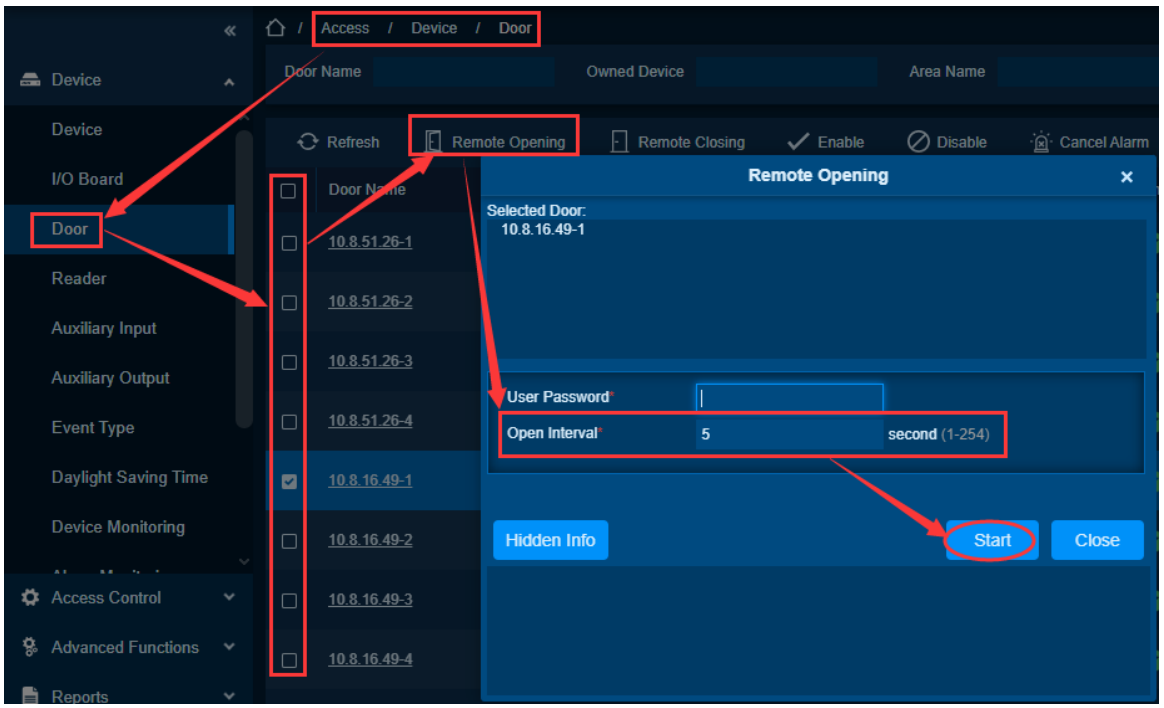
When the administrator is not on site, you can directly open the door remotely.

Feature Trigger Result

The corresponding door sensor opens, and you can enter.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page
- Click **[Remote Opening]** to jump out of the remote door opening interface
- You can choose the device connection password and the door opening interval, click **[Start]** to open the door remotely.



Remote Closing

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

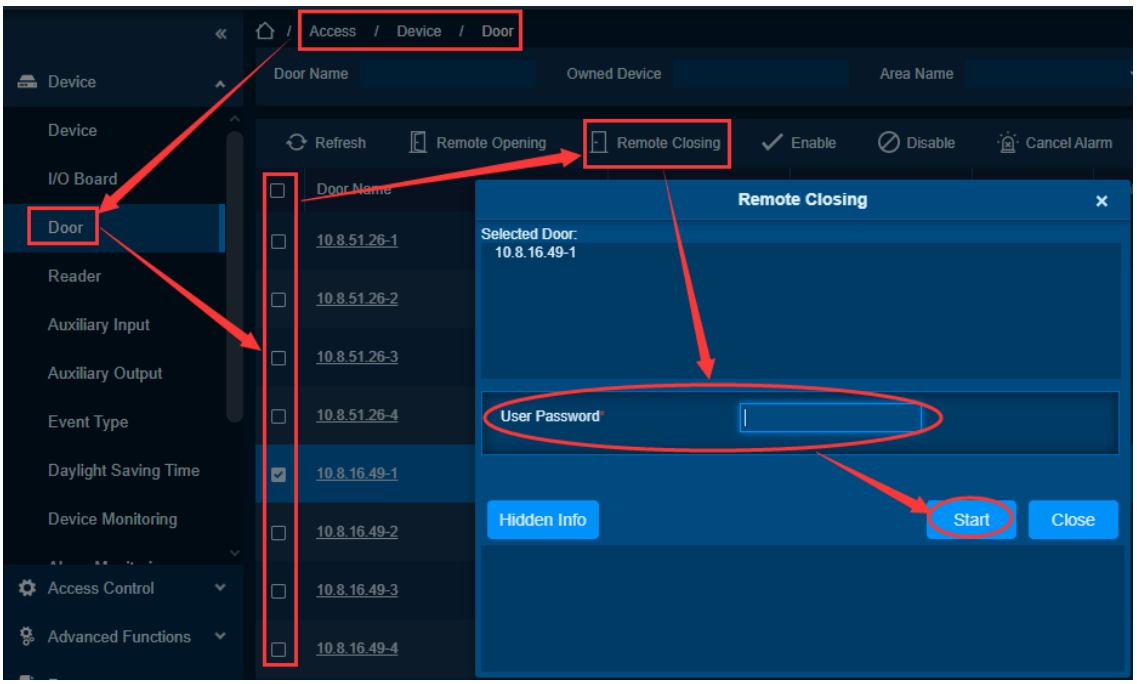
When the administrator is not on site, you can directly close the door remotely.

Feature Trigger Result

The corresponding door sensor is closed, and no entry is allowed.

Steps

- Click **[Access Control Device] > [Device] > [Door]** to display the view page
- Click **[Remote Closing]** to exit the remote interface.
- Choose the device connection password and click **[Start]** to close the door remotely.



Enable

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority. The door is disabled.

Function Usage Scenarios

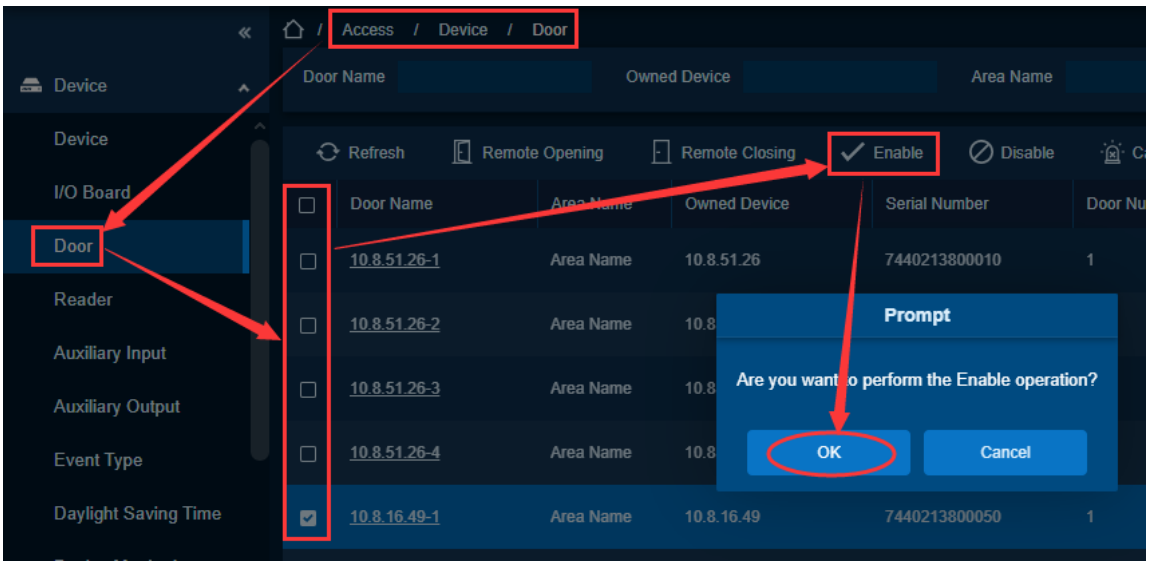
Need to use the device for access control.

Feature Trigger Result

After enabling the device, the software can upload and send data to the device.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[Enable]** to exit the enable selection interface, click **[OK]** to enable the door.



Disable

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. The device is added successfully.

Function Usage Scenarios

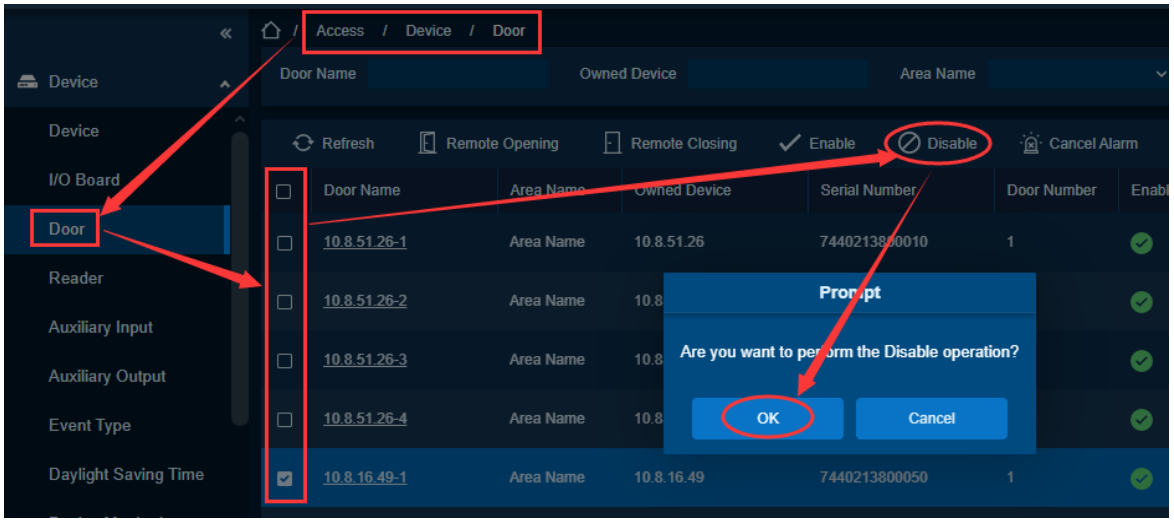
The device has failed and needs to be disabled. Need to add another device

Feature Trigger Result

The door corresponding to the device is not used.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[Disable]** to exit the disabled selection interface, click **[OK]** to disable the door.



Cancel Alarm

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

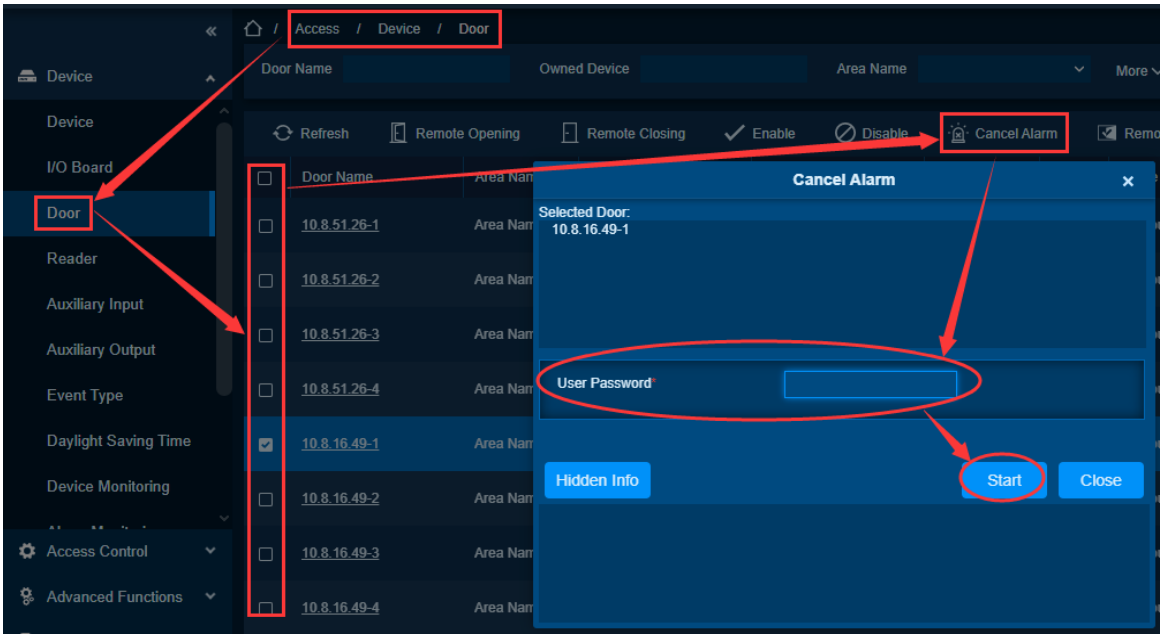
The door alarm event has been processed and can be cancelled.

Feature Trigger Result

Close the alarm sound of the door.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[Cancel Alarm]** to exit the cancel alarm interface.
- You can choose the device connection password and click **[Start]** to cancel the alarm.



Remote Normally Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

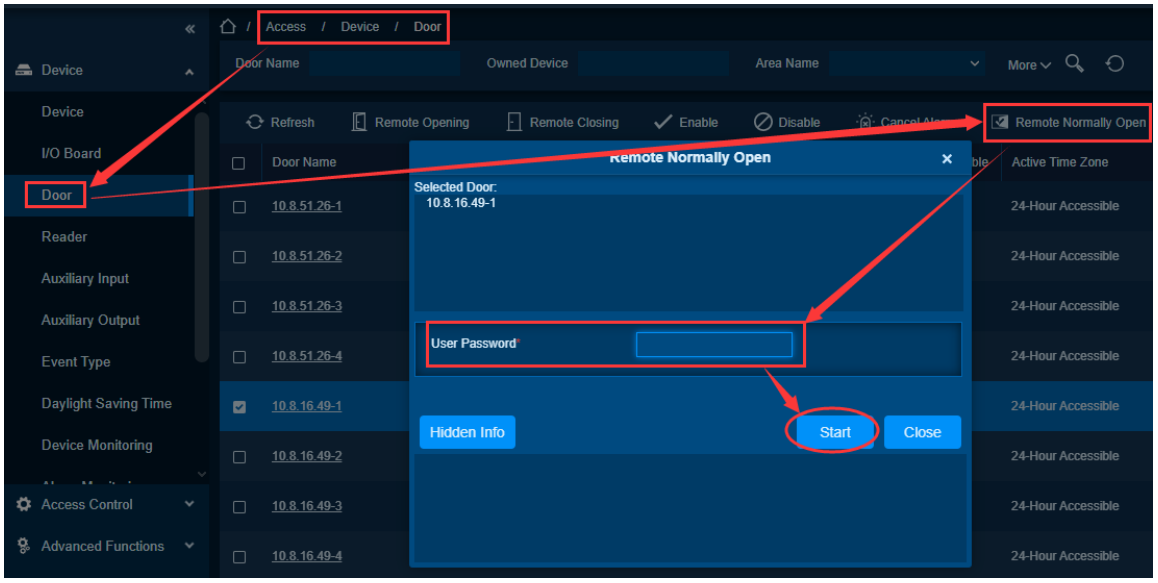
The door needs to be kept open.

Feature Trigger Result

Open the door sensor and keep it open.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[Remote Normally Open]** to exit remote normally open interface.
- You can choose the device connection password can click **[Start]** to remotely normally open.



Activate Lockdown

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

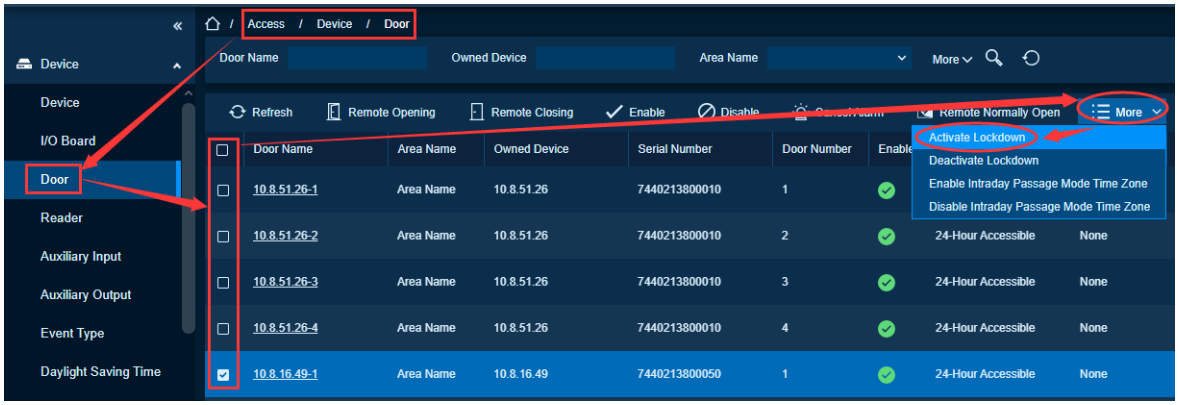
Prevent other personnel from operating the door.

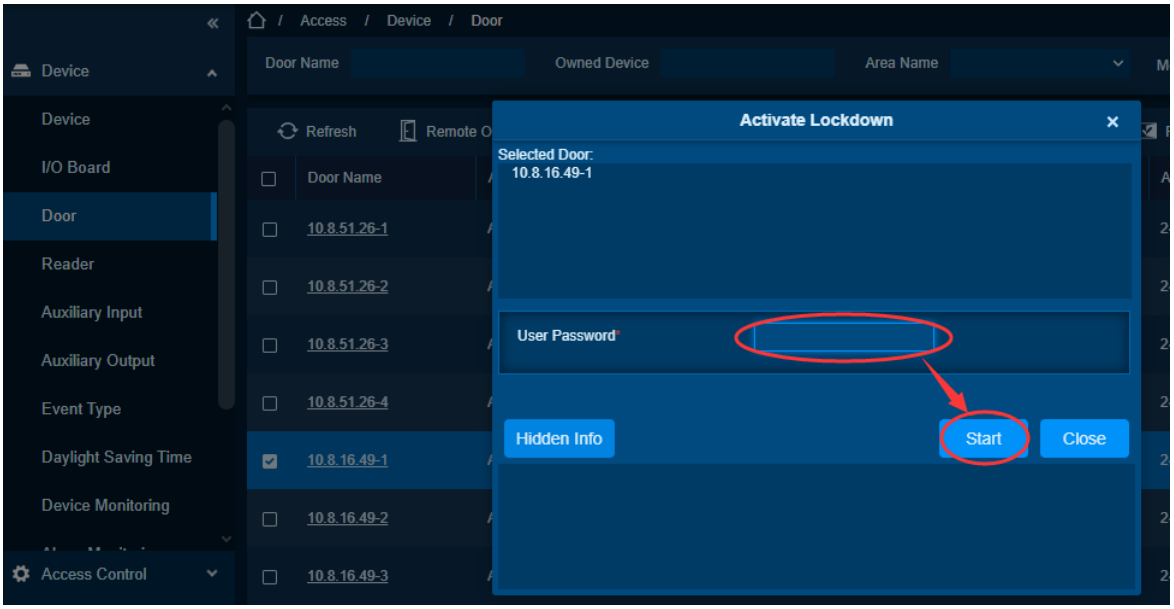
Feature Trigger Result

Set the door to the locked state remotely, the door cannot receive any operation, such as swiping card, remote operation, etc.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[More]> [Activate Lockdown]** to exit the remote lock interface.
- You can choose the device connection password and click **[Start]** to remotely lock.





Deactivate Lockdown

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

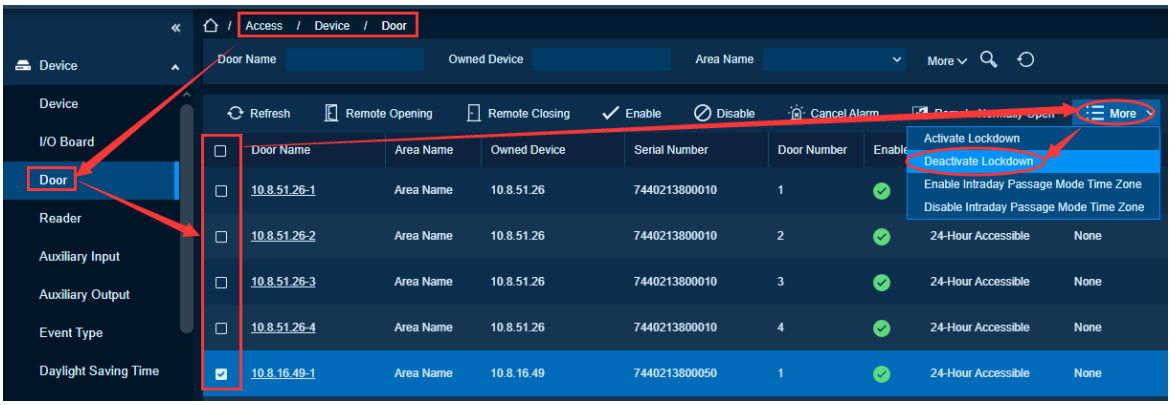
Unlock the locked door.

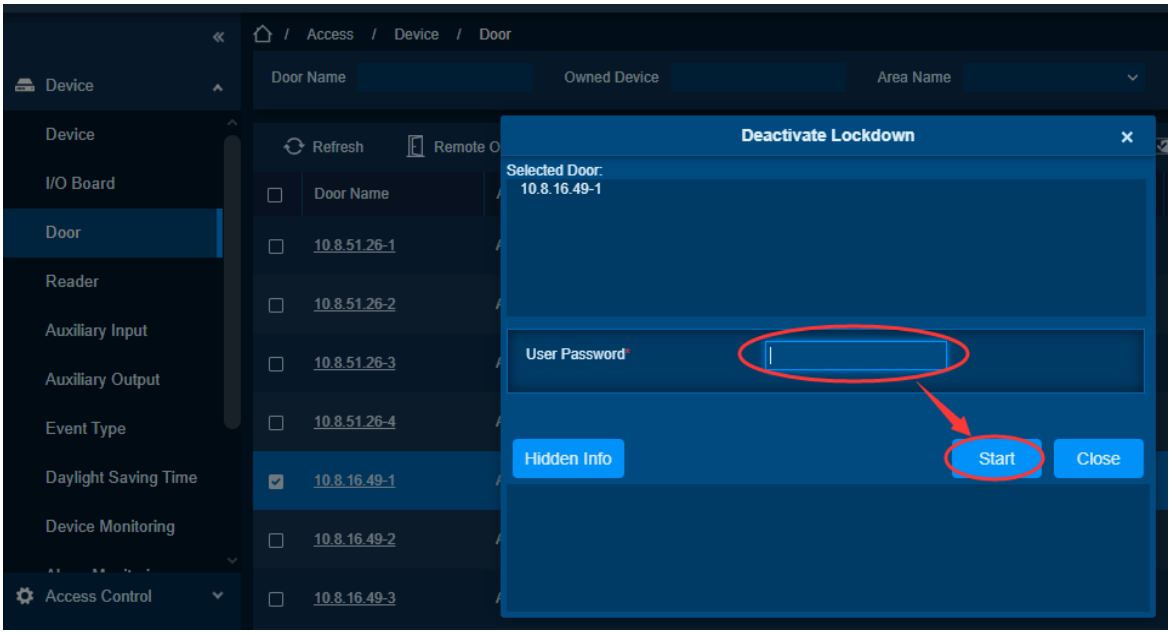
Feature Trigger Result

Set the door to the locked state remotely, the door cannot receive any operation, such as swiping card, remote operation, etc.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[More]> [Deactivate Lockdown]** to exit the remote unlock interface.
- You can choose the device connection password and click **[Start]** to remotely unlock.





Enable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

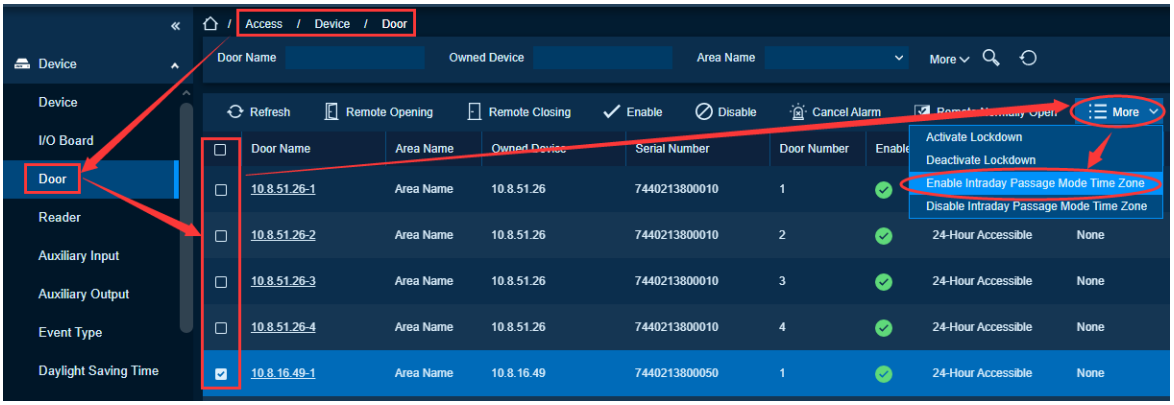
Need to open the door for the designated normally open time.

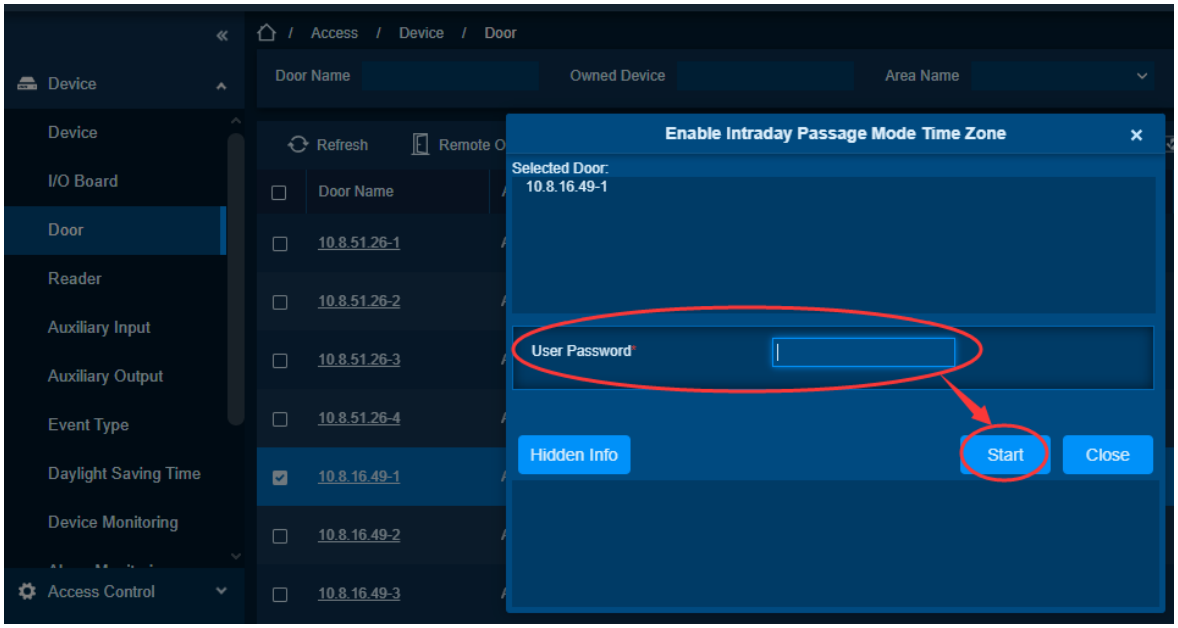
Feature Trigger Result

During the normally open time, the door is open, and you can enter and exit.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[More]> [Enable Intraday Passage Mode Time Zone]** to enable the interface.
- You can select the device connection password and click **[Start]** to enable the normal open time zone of the day.





Disable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

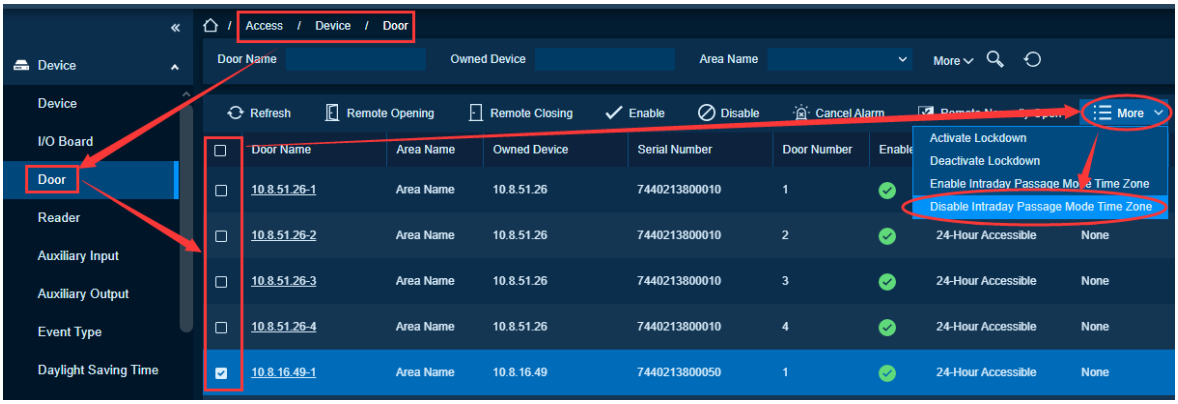
The Normally Open Time Zone cannot be used under special circumstances.

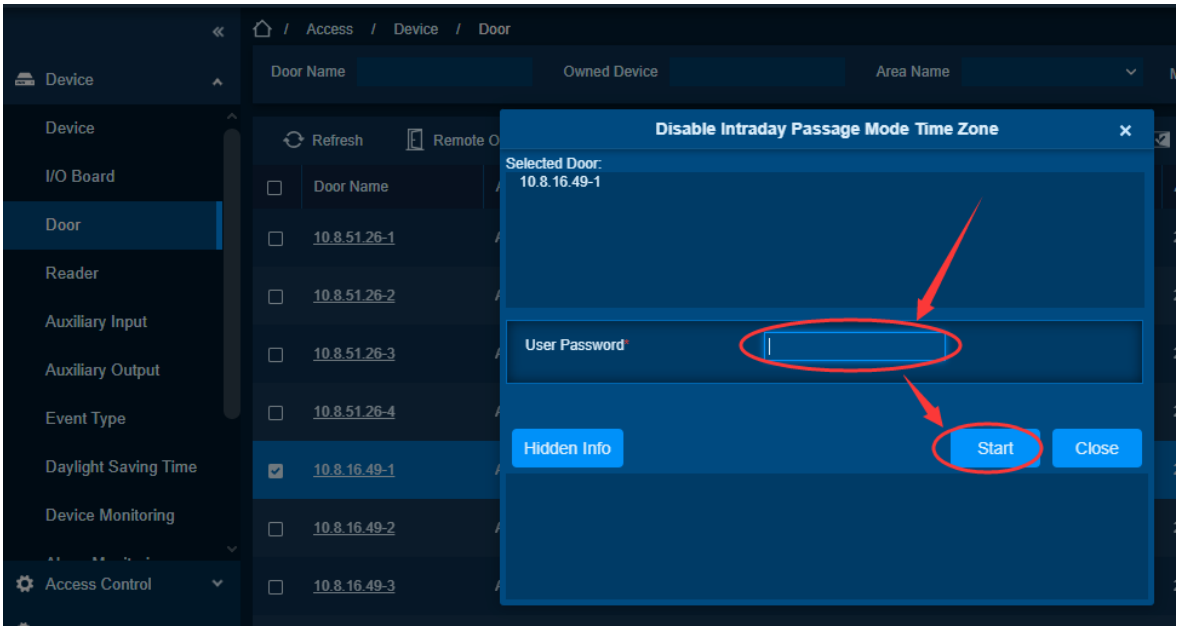
Feature Trigger Result

Disable the normal open time zone of the day and cannot enter and exit at will during the time zone.

Steps:

- Click **[Access Control Device] > [Device] > [Door]** to display the view page.
- Click **[More]> [Disable Intraday Passage Mode Time Zone]** to disable the interface.
- You can choose the device connection password and click **[Start]** to disable the normal open time zone of the day.





6.1.4. Reader

Function Description

The reader list of the added device, the reader can be unbound, and the camera can be bound.

New Reader

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. One reader is deleted from controller.

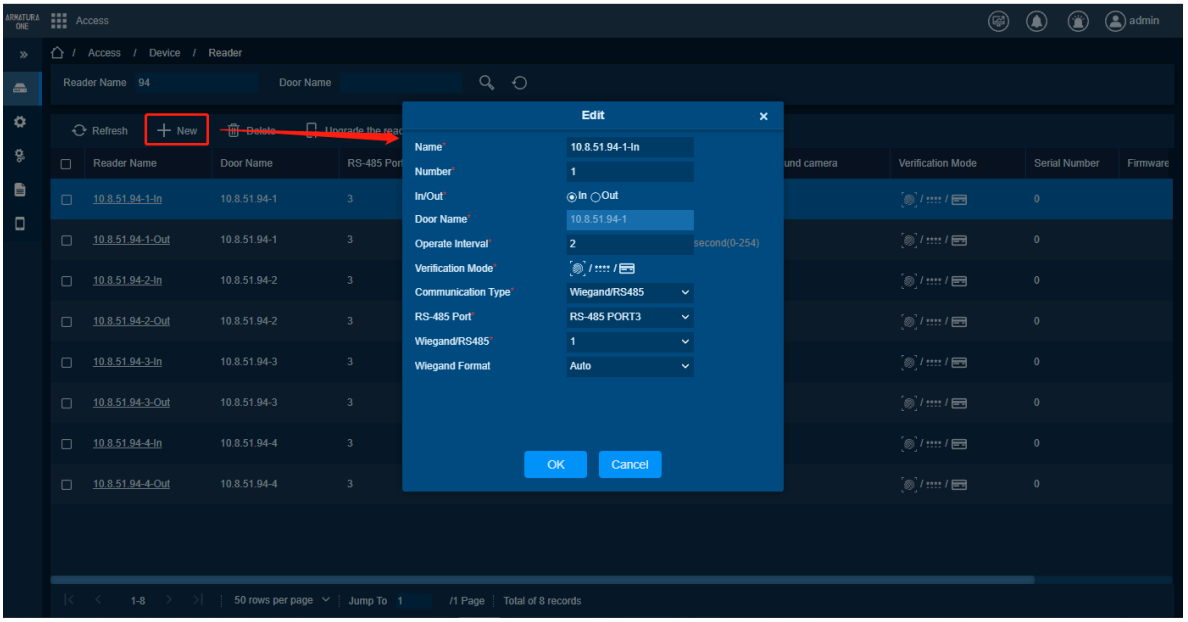
Function Usage Scenarios

Reader on controller is deleted, wants to add again.

Feature Trigger Result

Modify the corresponding configuration.

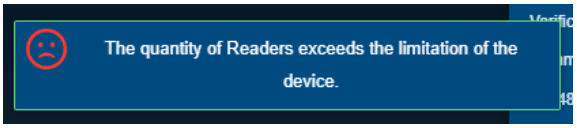
Steps:



- Interface Setting check Edit Reader

✍**Note:**

Reader amount depends on the door amount, the ratio between reader amount and door Amount is 1:2. Reader can be deleted and can be added but not exceed the maximum amount refer to ratio.



Edit Reader

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. Ensure the device is successfully added.

Function Usage Scenarios

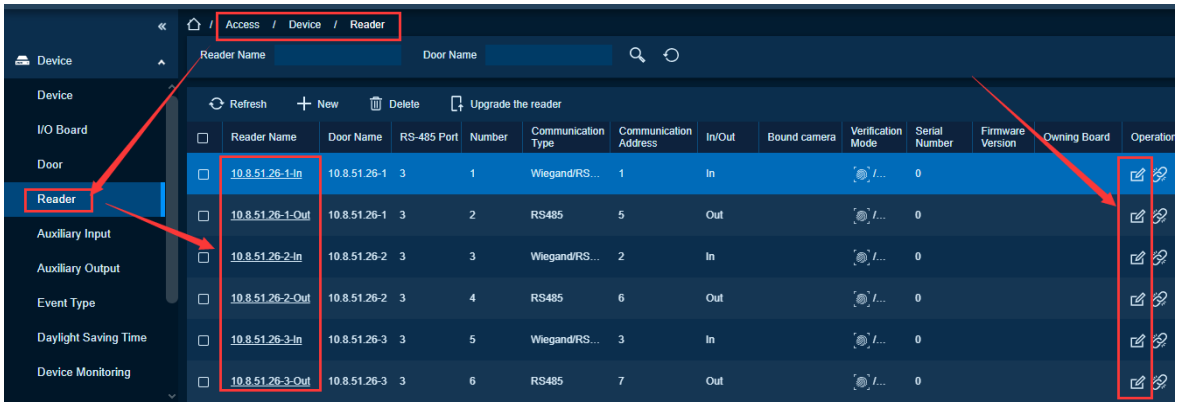
Need to modify the parameter configuration and other information of the corresponding door.

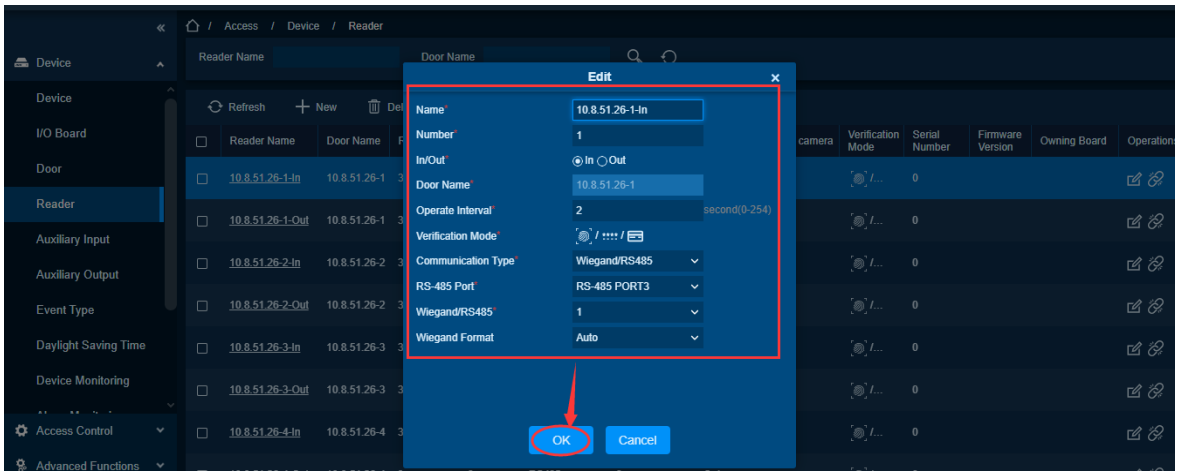
Feature Trigger Result

Modify the corresponding configuration.

Steps:

- Click **[Access Device] > [Reader]** on the Action Menu, click on reader name or **[Edit].**





Name: Name of the reader displayed on the list page.

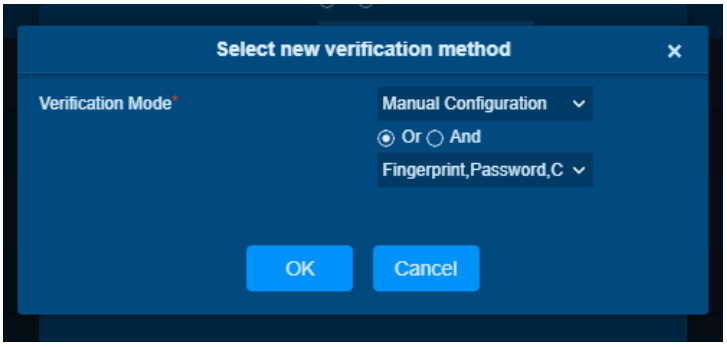
Number: Unique Number to specific id for reader in database.

In/Out: Reader Install in Inside/ Outside of door.

Door Name: Select the reader corresponding door.

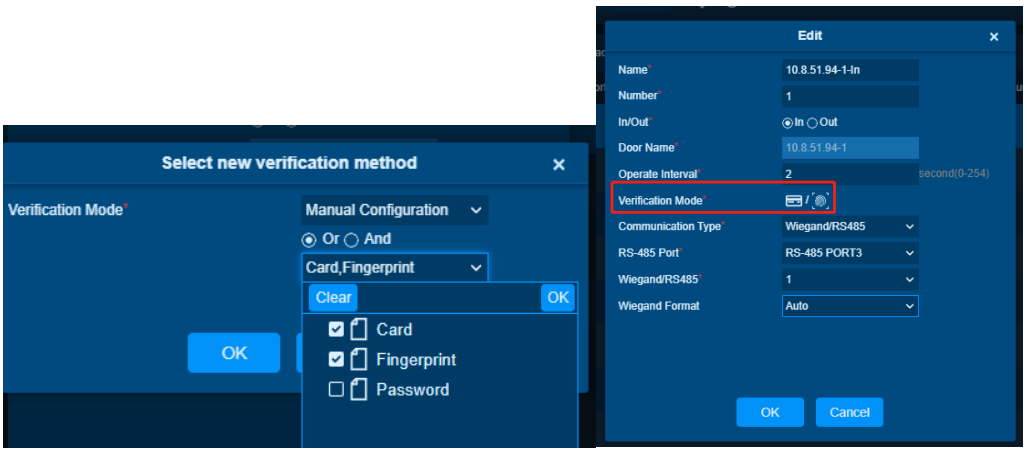
Operation Interval: this feature is controlling the device verification frequency to avoid frequent duplicated punch.

Verification Mode: Select the verification method support in this reader, verification method supported is depending on device function. It supports combination of verification mode.



Verification Mode has two mode Automatic Identification and Manual Configuration, Automatic Identification indicate device will support all types of verification method and select by itself.

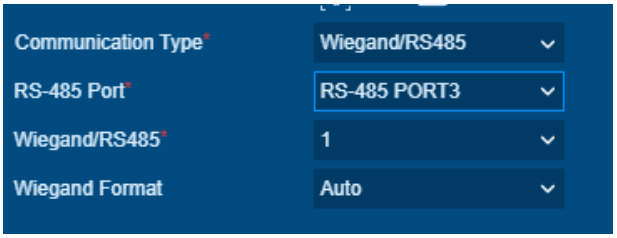
Manual Configuration indicate selected verification support in specific reader. For example, select logic is or, verification is card, fingerprint. It means device only support card or fingerprint.



Communication Type: Wiegand/RS-485, Wiegand, RS-485, Disabled

- **Wiegand/RS-485**

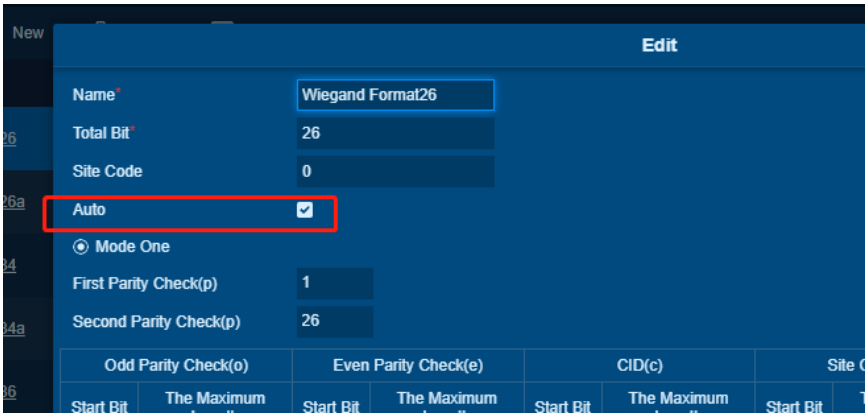
It is only convenient for some controller to quick deploy, no need to select RS-485 or Wiegand.



RS-485 Port: Which port interface reader connect

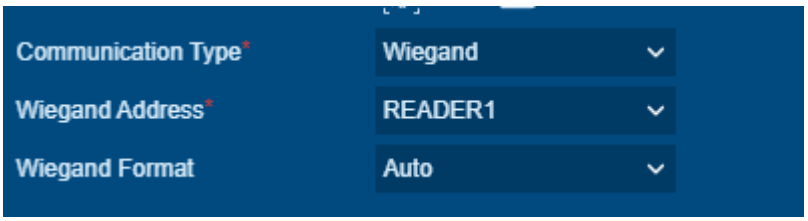
Wiegand/RS-485: Reader connects to Wiegand Port Interface or the RS-485 Address

Wiegand Format: Auto will check select Wiegand Format which set Auto form **[Personnel]->[Card Management]->[Wiegand Format]**



Also, can set specific Wiegand format for specific reader.

- **Wiegand**

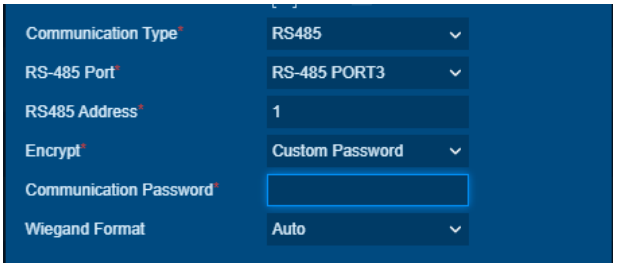


Wiegand Address: Reader connects to Wiegand Port Interface

Wiegand Format: Auto will check select Wiegand Format which set Auto form **[Personnel]->[Card Management]->[Wiegand Format]**

Also, can set specific Wiegand format for specific reader.

- **RS-485**



RS-485 Port: Which port interface reader connect

RS-485 Address: Reader RS-485 Address

Encrypt: Without Encryption/ Default Password/ Custom Password

Without Password: OSDP without Encryption

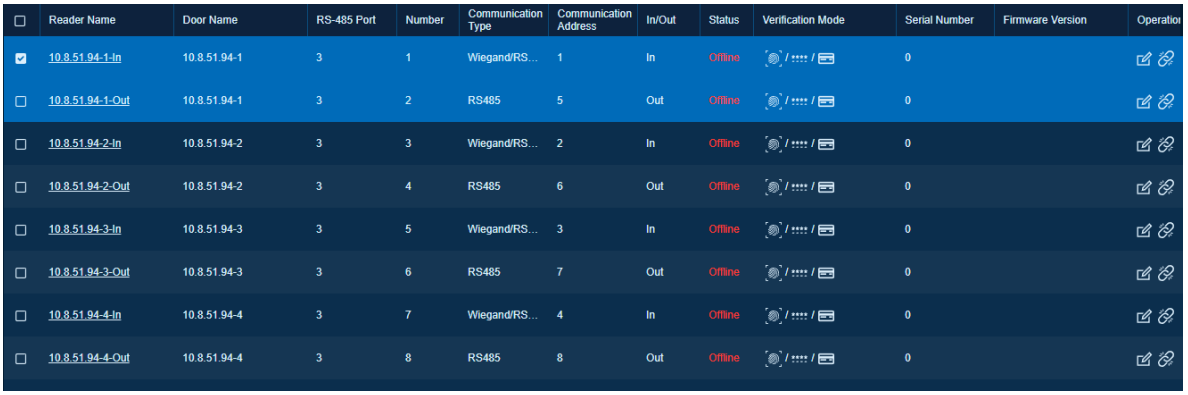
If reader is using OSDP SCP(Secure Channel Protocol) using AES-128, please select RS-485 as Communication Type first, then set Encrypt is Default Password/ Custom Password.

Default Password: According to OSDP 2.1.7 document, default key for SCBK_D is "303132333435363738393A3B3C3D3E3F"

Custom Password: The password defined by customer, should be 128-Bit (32-Digit Hexadecimal Characters), the field is required to input HEX data.

Wiegand Format: Auto will check select Wiegand Format which set Auto form **[Personnel]->[Card Management]->[Wiegand Format]**

Also, can set specific Wiegand format for specific reader.



Reader Name	Door Name	RS-485 Port	Number	Communication Type	Communication Address	In/Out	Status	Verification Mode	Serial Number	Firmware Version	Operation
10.8.51.94-1-In	10.8.51.94-1	3	1	Wiegand/RS...	1	In	Offline	/ **** /	0		
10.8.51.94-1-Out	10.8.51.94-1	3	2	RS485	5	Out	Offline	/ **** /	0		
10.8.51.94-2-In	10.8.51.94-2	3	3	Wiegand/RS...	2	In	Offline	/ **** /	0		
10.8.51.94-2-Out	10.8.51.94-2	3	4	RS485	6	Out	Offline	/ **** /	0		
10.8.51.94-3-In	10.8.51.94-3	3	5	Wiegand/RS...	3	In	Offline	/ **** /	0		
10.8.51.94-3-Out	10.8.51.94-3	3	6	RS485	7	Out	Offline	/ **** /	0		
10.8.51.94-4-In	10.8.51.94-4	3	7	Wiegand/RS...	4	In	Offline	/ **** /	0		
10.8.51.94-4-Out	10.8.51.94-4	3	8	RS485	8	Out	Offline	/ **** /	0		

If Explorer Series Reader, after connecting with OSDP, will show serial number and firmware version in the list.

- **Disabled**

Reader is disable

Bind/Unbind Camera

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

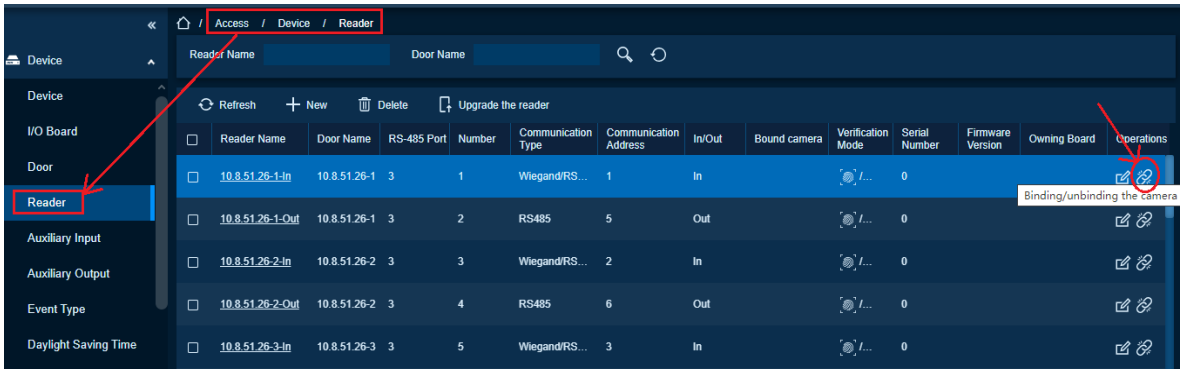
Need to establish a video link (pop-up video, video, or screenshot) and other functions.

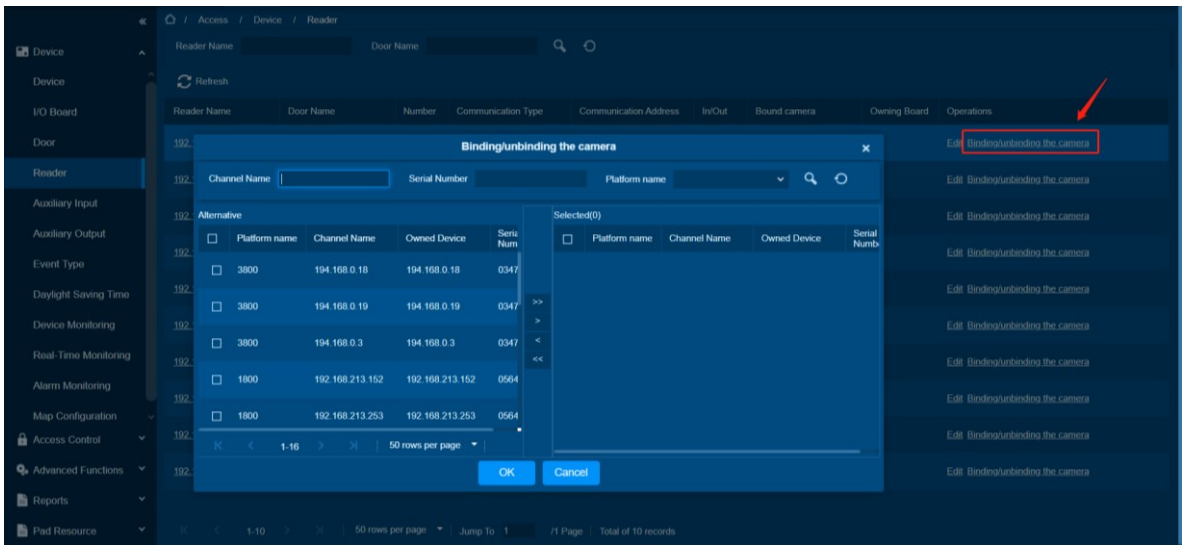
Feature Trigger Result

Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos, or screenshots) once there is a corresponding event occurs.

Steps:

- Click **[Bind/Unbind Camera]** to select channel(s).





- Select and move the required reader towards right list and click [OK] to finish.

✍**Note:**

A reader can bind up to 5 cameras.

Firmware Upgrade

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority. Reader is using RS-485 to controller and connection is good.

Function Usage Scenarios

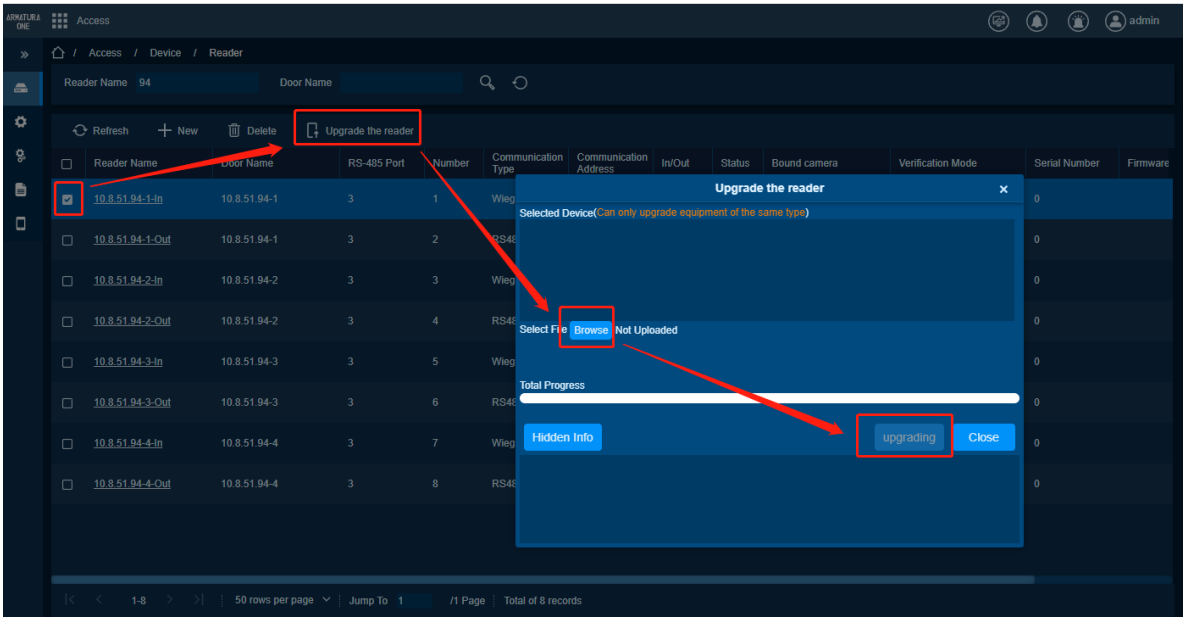
Upgrade reader firmware via controller

Feature Trigger Result

Reader will be upgrade

Steps:

- Select a reader, click **Firmware Upgrade**



- Click **Browser** to select a file from Computer Locally. Reader firmware should be name as rdfw.ar
- Click **Upgrade**

After Reader upgrade successfully, reader will reboot, and firmware in firmware version column will update.

6.1.5. Auxiliary Input

Function Description

The auxiliary input list of the added device, the auxiliary input can be unbound, and the camera can be bound.

Enable/Disable

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

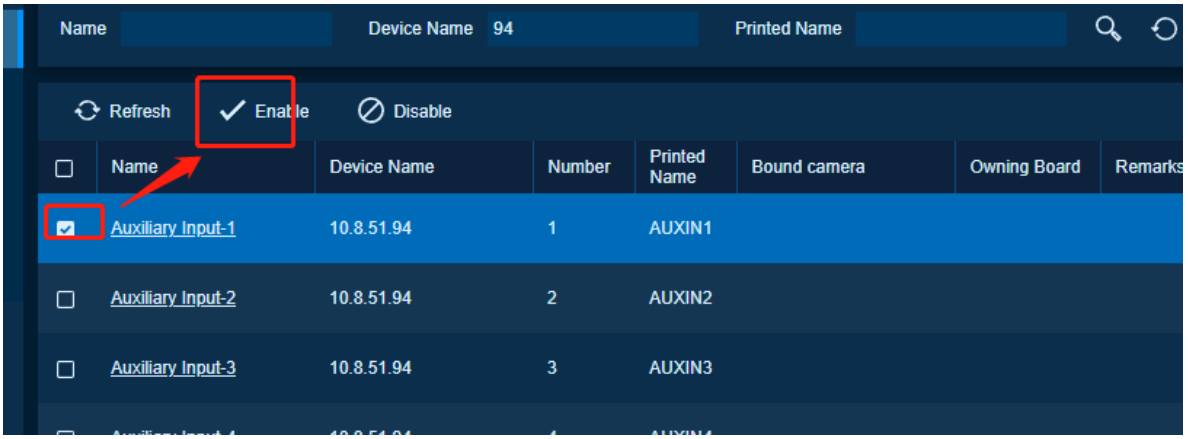
Enable/Disable Input

Feature Trigger Result

If auxiliary input is disable, linkage which input participate will not be trigger, input signal will be masked.

Steps:

- Select Device, click **Enable/Disable**



Edit Auxiliary Input

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

Need to modify the parameter configuration and other information corresponding to the auxiliary input.

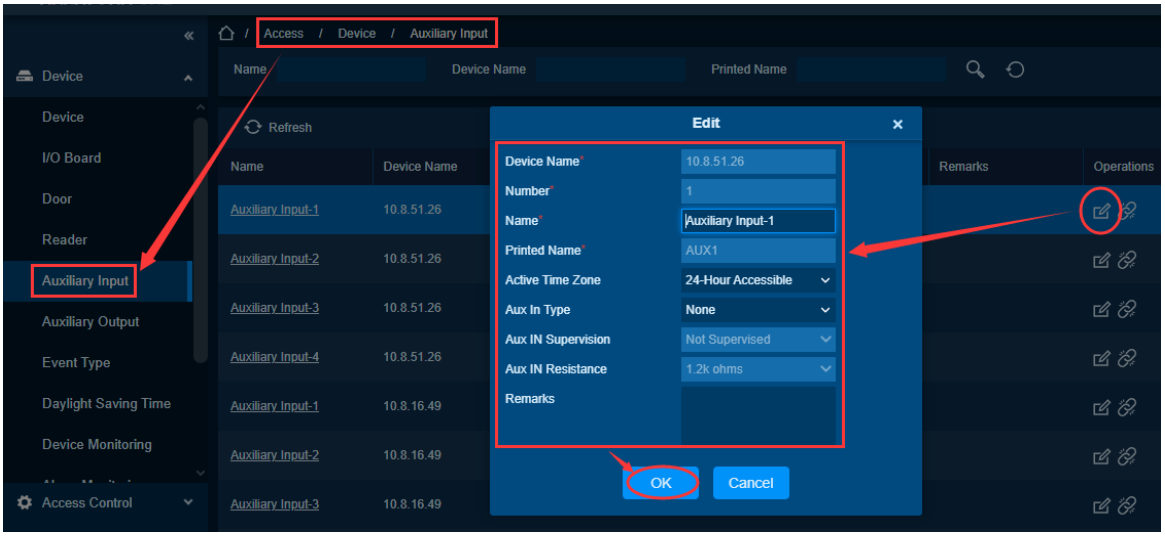
Feature Trigger Result

Modify the corresponding configuration, which can be used to connect infrared sensors, smoke sensors and other device

Steps:

Click **[Access Device]** > **[Auxiliary Input]** on the Action Menu, to access below shown interface:

Click on Name or **[Edit]** to modify the parameters as shown below:



The fields are as follows:

Device Name: Corresponding Device

Number: Unique Number to specific id for Auxiliary Input in database

Name: You can customize the name according to your preference.

Printed Name: It will be the printed name on the hardware, such IN5.

Active Time Zone: Auxiliary input is available only in the specified time segment.

✍**Note:**

Only Name, Active Time Zone and Remarks can be modified.

Click **[OK]** to save the name and remark and exit.

AUX IN Type: None (will not detect Aux Input), Normal Open, Normal Close. The default value is None.

AUX IN Supervision: It can select Not Supervised / Default Supervision, this function is available when **AUX IN Type** is Normally Open/Normally Closed

AUX IN EOL Resistor: It can select 1.2k ohm/2.2k ohm /4.7k ohm /10k ohm, this value is referring to the resistor used in electric circle. This function is available when **AUX IN Supervision** selects Default Supervision.

Remarks: Take some remarks.

Bind/Unbind Camera

Preconditions for Normal Use of Function

Log in to the system with current account and have the authority.

Function Usage Scenarios

Need to bind or unbind the camera corresponding to the auxiliary input.

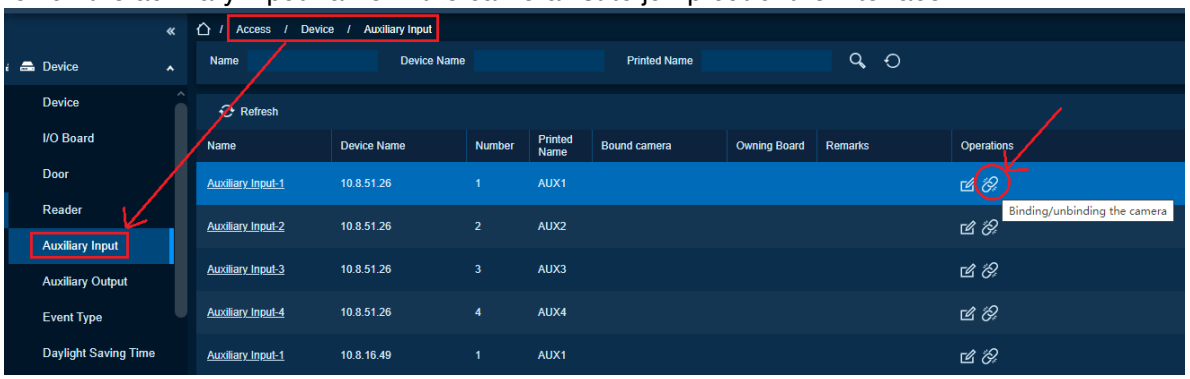
Feature Trigger Result

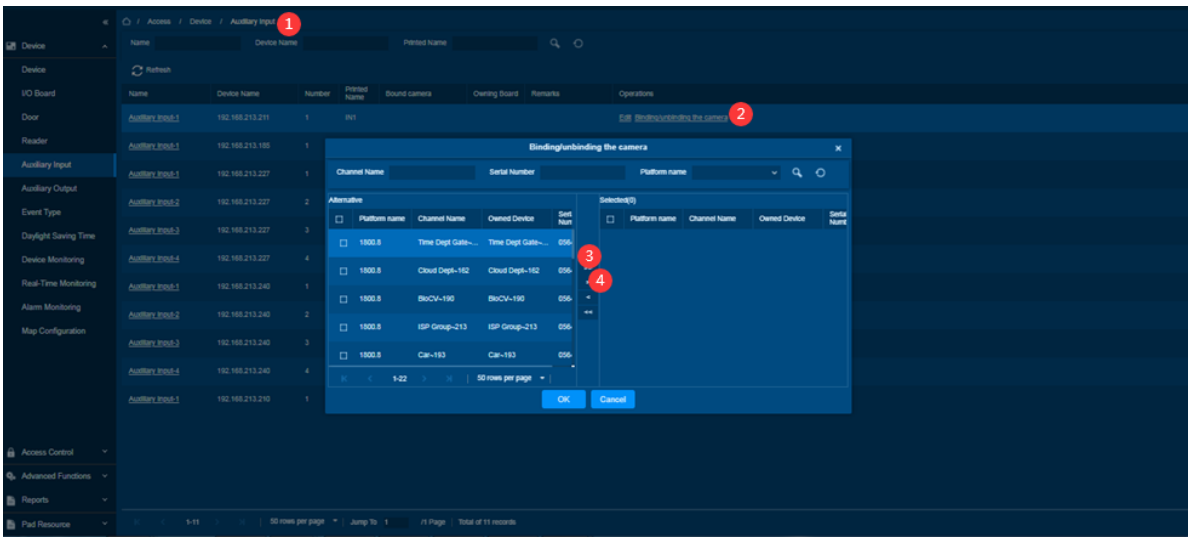
Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos, or screenshots) once there is a corresponding event occurs. For this, the interaction setting in Linkage or in Global Linkage should be done before.

Steps:

Bind the camera

- Click **[Access Control Device] > [Device] > [Auxiliary Input]** to display the view page.
- Click on the auxiliary input name in the camera list to jump out of the interface.





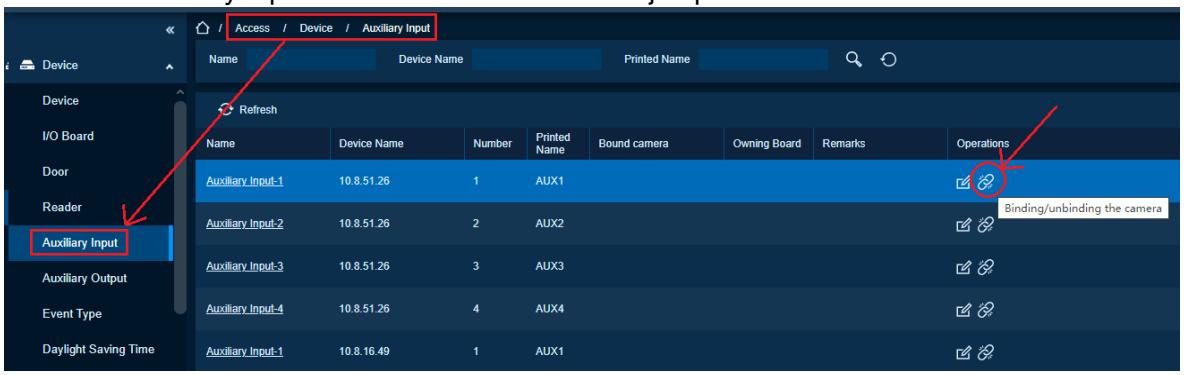
- Click [3]: Transfer all the devices on the left to the right, click **[OK],** add the camera successfully.
- Click **[OK] and** add the camera successfully.

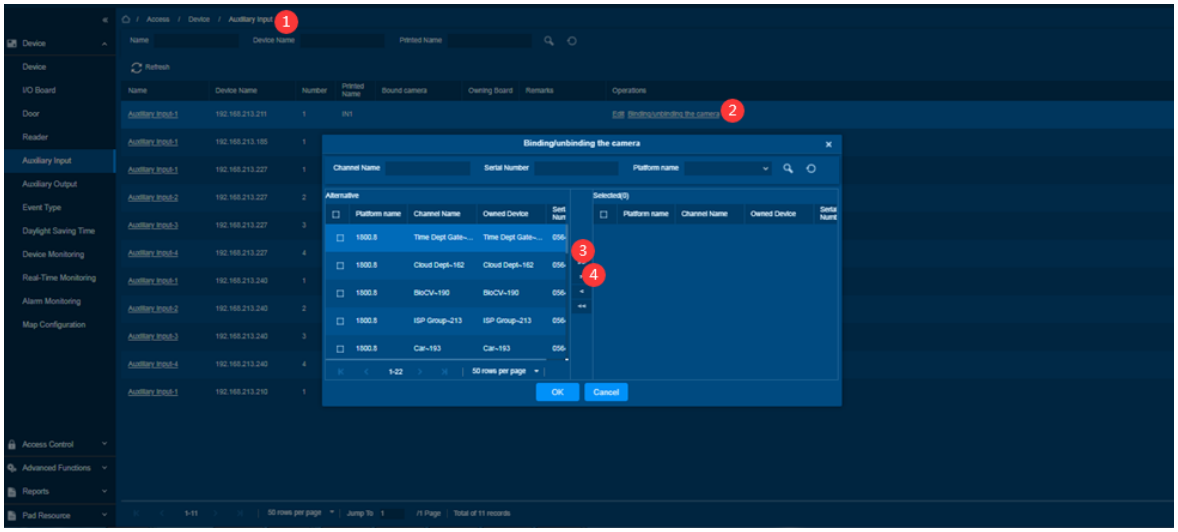
Note:

An auxiliary input point can bind more than one channel.

Unbind the Camera

- Click **[Access Control Device] > [Device] > [Auxiliary Input]** to display the view page.
- Click on the Auxiliary Input Name in the camera list to jump out of the interface.





- Click 3: Transfer all the devices on the right to the left, click **[**OK**]**, unbind the camera successfully.
- Click **[OK],** unbind the camera successfully.

6.1.6. Auxiliary Output

Function Description

The auxiliary output list of the added device, the auxiliary output can be edited.

Edit Auxiliary Output

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

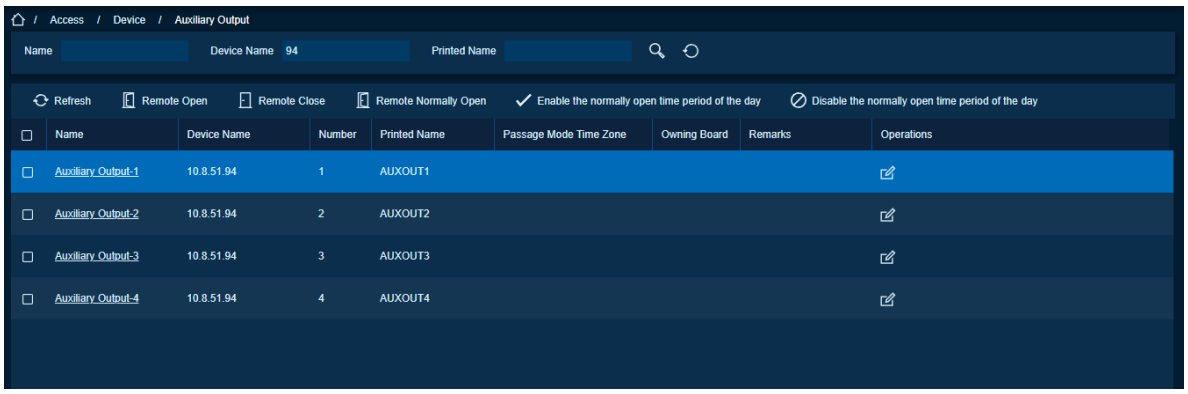
Need to modify the parameter configuration of the corresponding auxiliary output and other information.

Feature Trigger Result

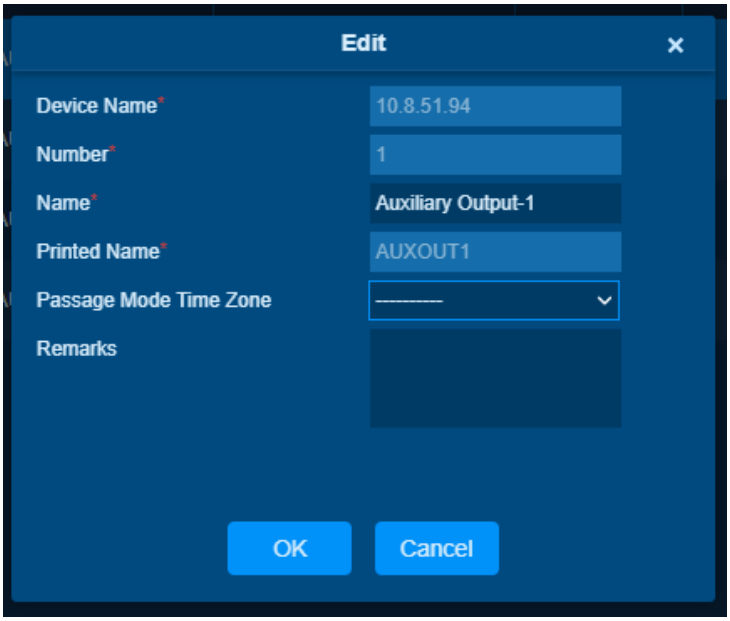
Modify the corresponding configuration, mainly connected to the alarm, etc., used in linkage. The auxiliary output relay can be remotely opened, closed, and normally open. After operation, the relay will perform corresponding actions.

Steps:

- Click **[Access Device] > [Auxiliary Output]** on the Action Menu to access the following interface.



- Click **[Edit]** to modify the parameters.



The fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example OUT2.

Passage Mode Time Zone: The auxiliary output will be in normal open or normal close in the selected time zone.

✍**Note:**

Only Name, Passage Mode Time Zone and Remarks can be modified.

Click **[OK]** to save the name and remark and exit.

Remote Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

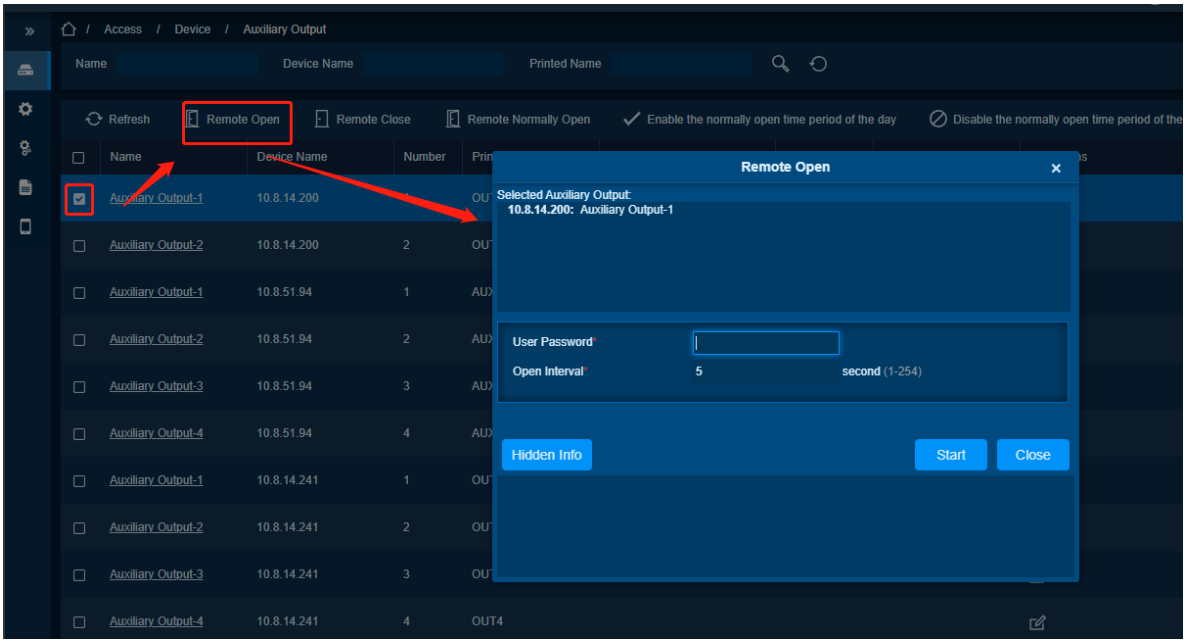
Remote to trigger Speaker to play alarm sound or lighting.

Feature Trigger Result

Aux Output will trigger to open

Steps:

- Select device and click **Remote Open**.



Remote Close

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

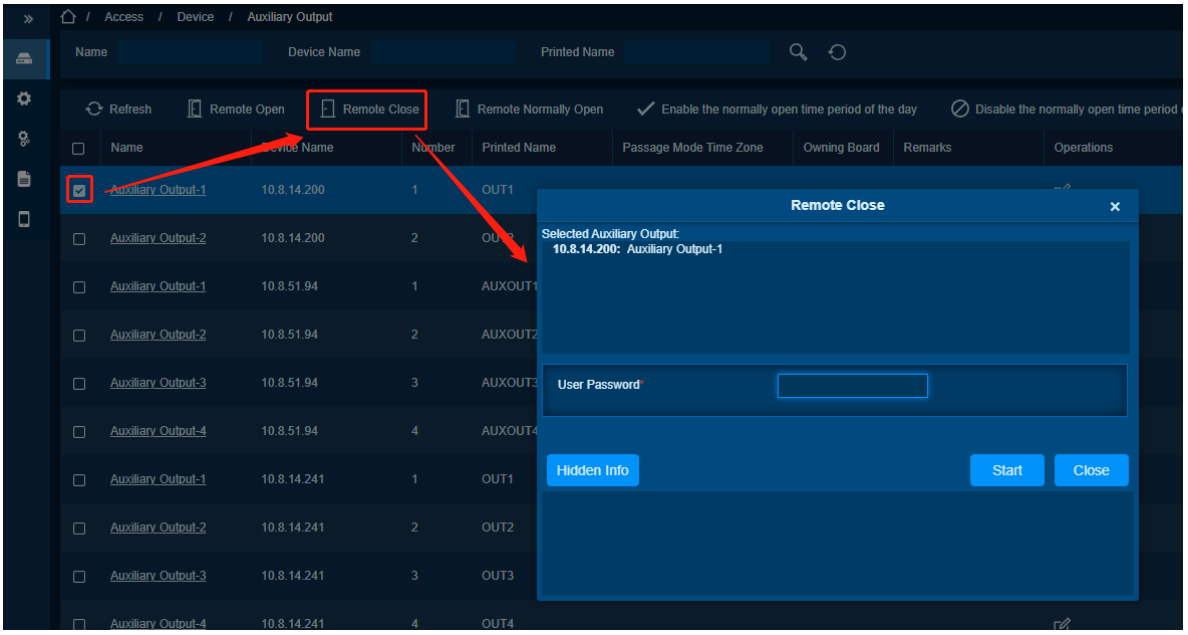
Remote to turn off Speaker or lighting.

Feature Trigger Result

Aux Output will trigger to close

Steps:

- Select device and click **Remote Close**



Enable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

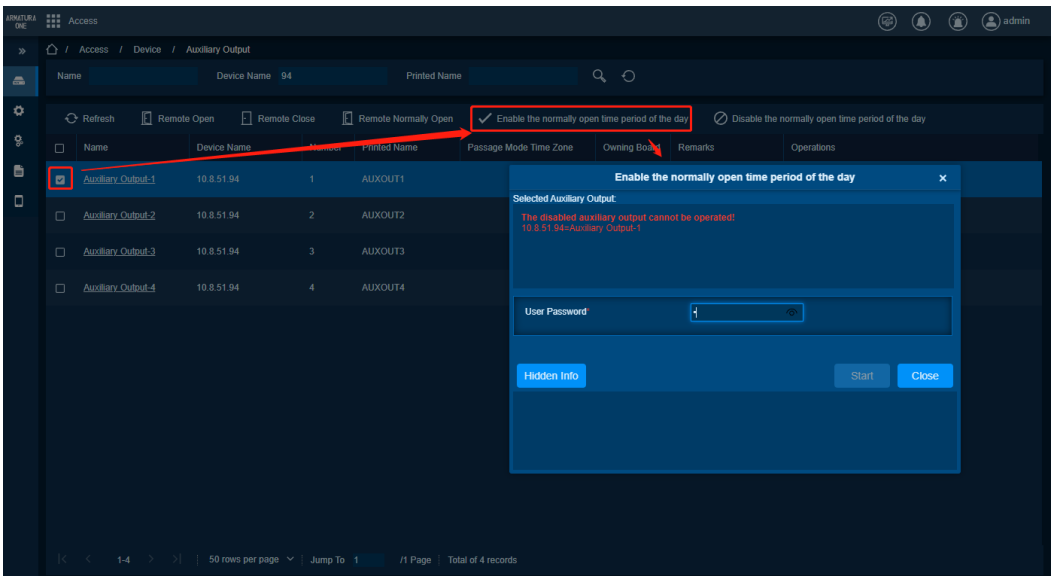
Need to open the Auxiliary Output for the designated normally open time.

Feature Trigger Result

During the normally open time, the Auxiliary Output is open.

Steps:

- Click **[Access Control Device] > [Device] > [Auxiliary Output]** to display the view page.
- Click **[More]> [Enable Intraday Passage Mode Time Zone]** to enable the interface.
- You can select the device connection password and click **[Start]** to enable the normal open time zone of the day.



✍**Note:**

This function is only support for AHSC-1000/AHDU 1X60

Disable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

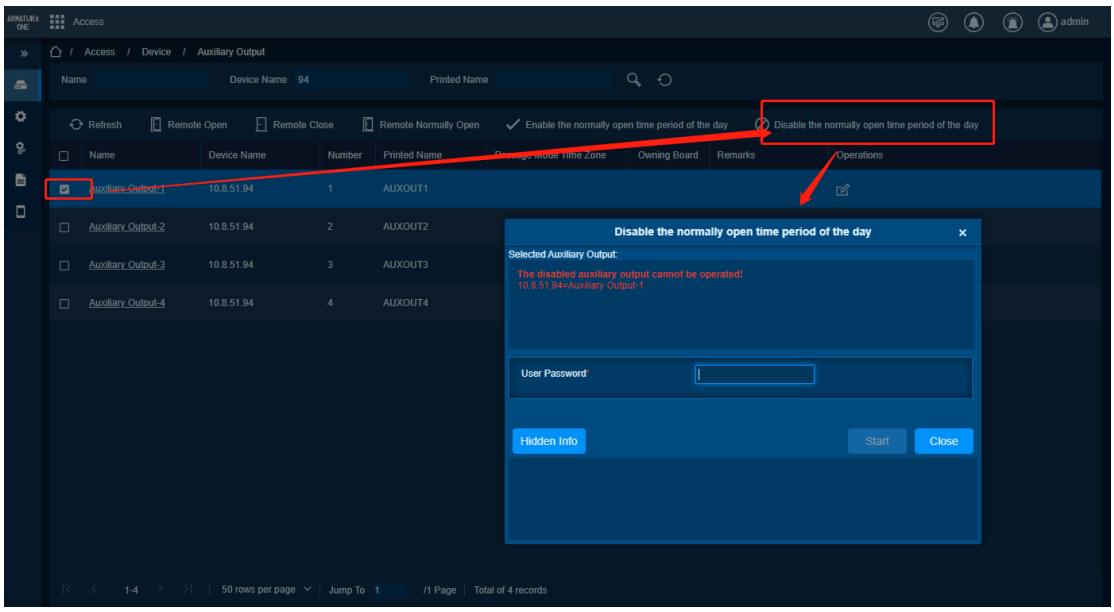
The Normally Open Time Zone cannot be used under special circumstances.

Feature Trigger Result

Disable the normal open time zone of the day and cannot enter and exit at will during the time zone.

Steps:

- Click **[Access Control Device] > [Device] > [Auxiliary Output]** to display the view page.
- Click **[More]> [Disable Intraday Passage Mode Time Zone]** to disable the interface.
- You can choose the device connection password and click **[Start]** to disable the normal open time zone of the day.



✍**Note:**

This function is only support for AHSC-1000/AHDU 1X60

6.1.7. Event Type

Function Description

It is mainly used to display various event types included in the access control device.

Edit Event

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

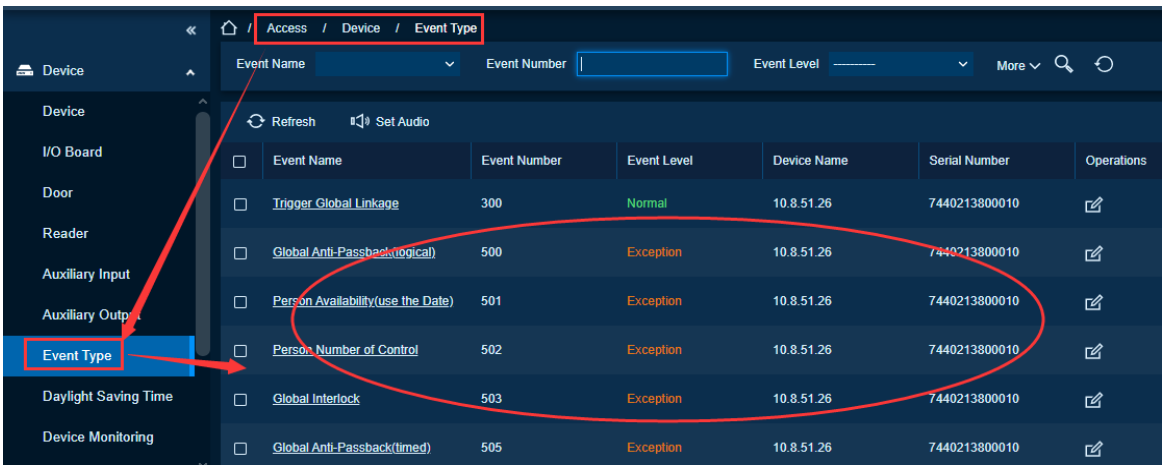
Need to view relevant information about the corresponding event.

Feature Trigger Result

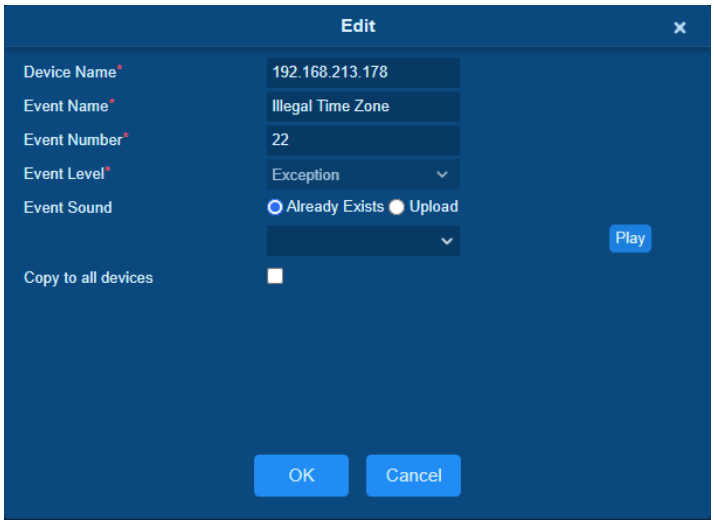
You can view the name, level, serial number, etc. corresponding to all current time types, and edit and set the sound.

Steps:

- Click **[Access Device]** > **[Event Type]** to access the following page.



- Click **[Edit]** or click the event type name to edit.



The fields are as follows:

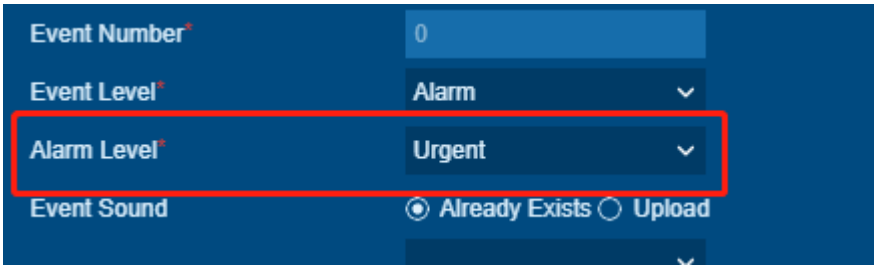
Device Name: Corresponding Device.

Event Name: It can't be modified.

Event Number: This number is from Controller.

Event Level: Normal, Exception, and Alarm are available.

If Event Level is Alarm, system will allow to set Alarm Level(Urgent, Important, General, Notice)



Event Sound: You can set custom sound being played when the event occurs in real-time monitoring.

Copy the above settings to all devices: This event will be applied to all current devices within the purview of the same user event number.

Set Audio

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

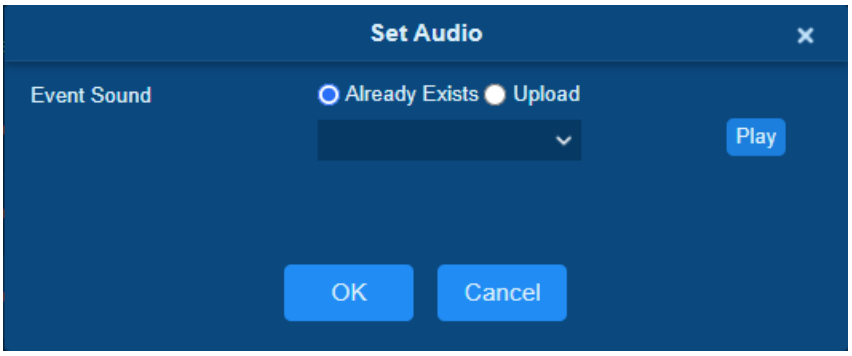
Set audio for event to notify.

Feature Trigger Result

You can set the sound.

Steps:

- Same as the event sound. Click **[Set Audio].**



You can upload an audio from your local PC. The file must be in wav or mp3 format, and it must not exceed 10MB.

6.1.8. Daylight Saving Time

Function Description

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. The regulations are different in different countries. At present, nearly 70 countries adopt DST.

To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

Add Daylight Saving Time

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

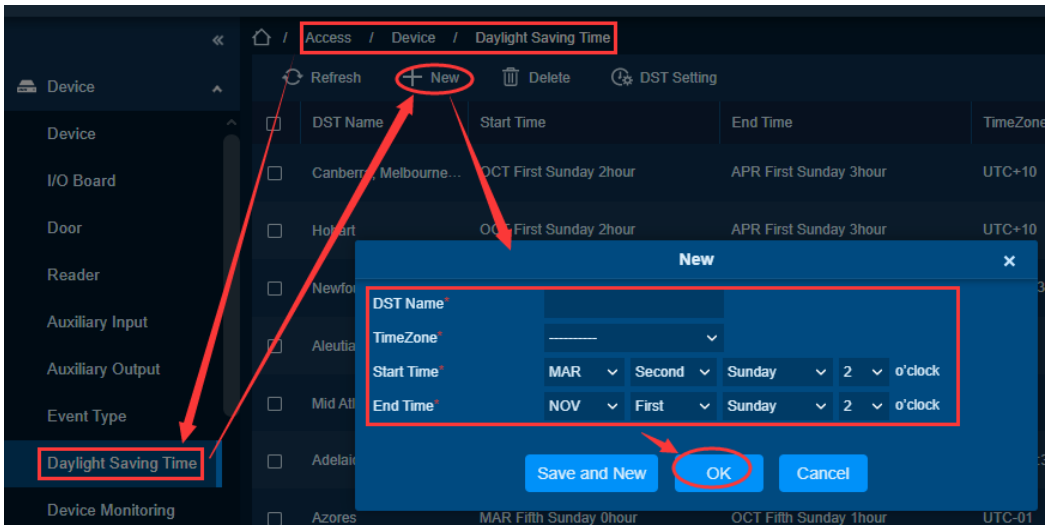
Local demand requires the use of daylight-saving time function.

Feature Trigger Result

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as “second Monday in March, 02:00”. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Steps:

Click **[Access] >[Device] > [Daylight Saving Time] > [New].**



Edit Daylight Saving Time

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

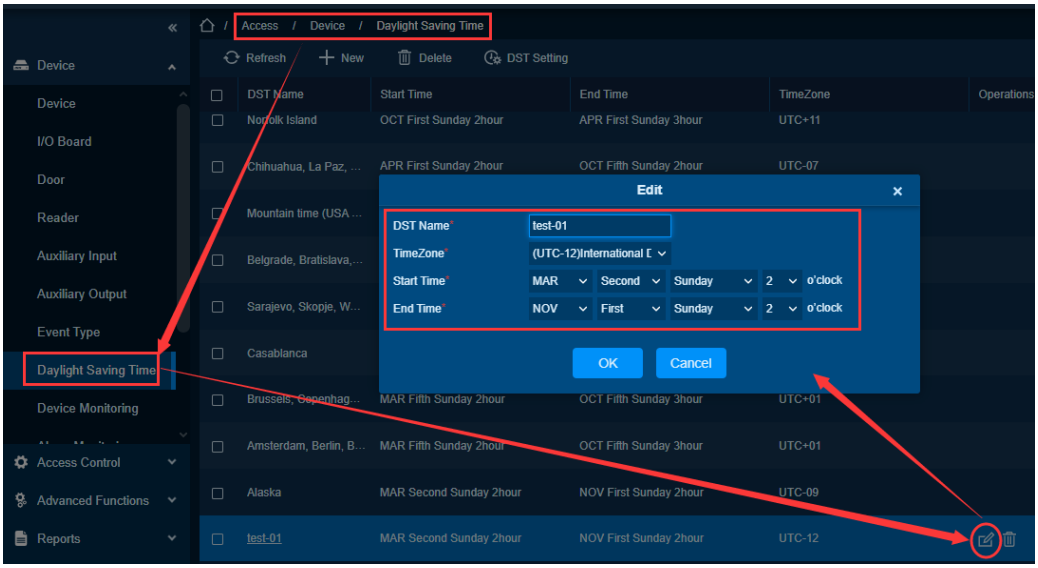
The original daylight-saving time needs to be modified.

Feature Trigger Result

You can modify the name, start time, and end time of daylight-saving time.

Steps:

- Click **[Access Control Device] > [Device] > [Daylight Saving Time]** to display the view page.
- Click **[Edit]** to pop up the edit daylight saving time interface.
- Set DST corresponding **Timezone**
- Set **Start Time**
- Set **End Time**
- Set the new summertime name and time, click **[OK]** to save successfully.



✍**Note:**

The default DST is not allowed to edit.

Delete Daylight Saving Time

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

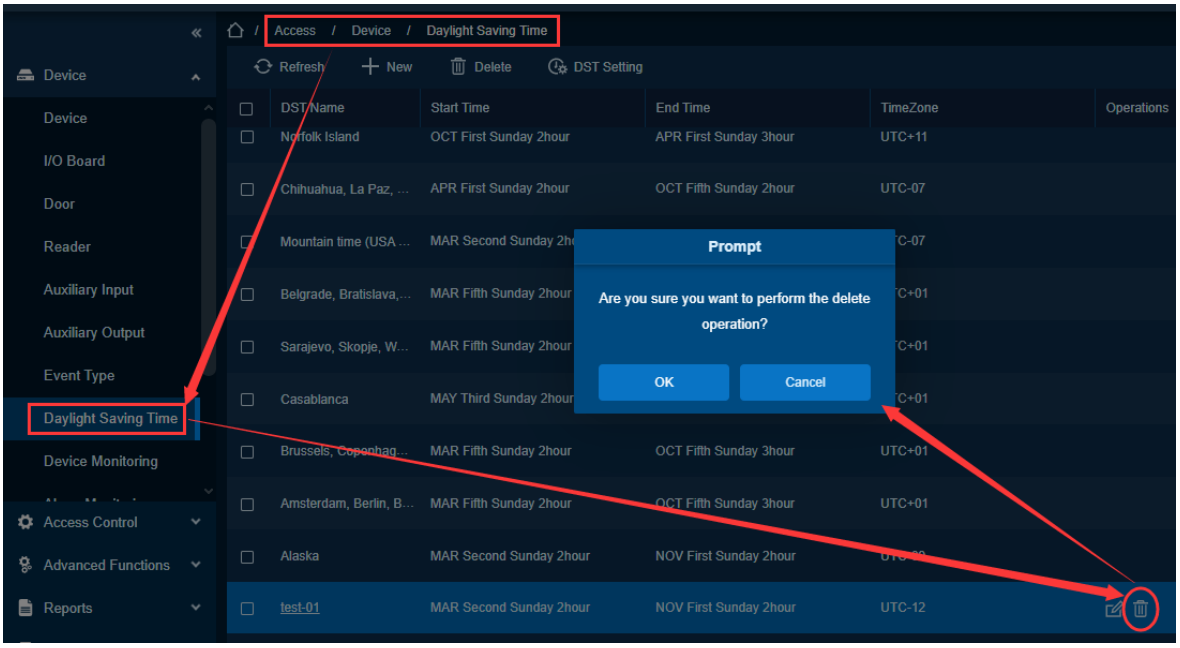
The original daylight-saving time setting is wrong, or it is not necessary to set the daylight-saving time

Feature Trigger Result

Delete this daylight-saving time.

Steps:

- Click **[Access Control Device] > [Device] > [Daylight Saving Time]** to display the view page.
- Click **[Delete]** to pop up the delete daylight saving time interface, click **[OK]** to delete.



6.1.9. Device Monitoring

Function Description

By default, it monitors all devices within the current user's level. You may click **[Access Device] > [Device Monitoring]** to view a list of operation information of devices: Device Name, Serial No., Area, Operation Status, Current status, Commands List, and Related Operation.

Export Device Monitoring Data

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

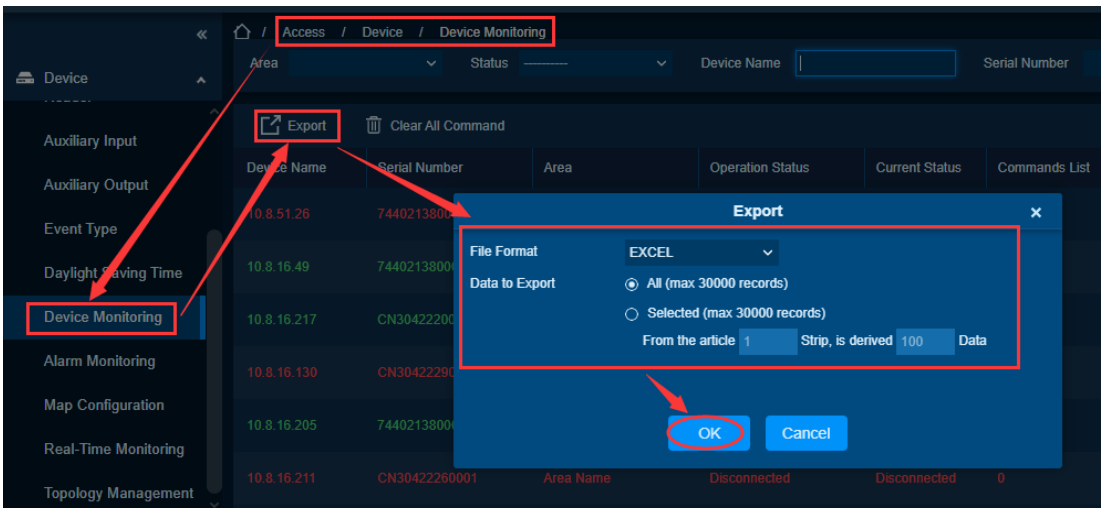
Need to export the event data for further analysis.

Feature Trigger Result

Export all or a certain amount of the data.

Steps:

- Click **[Access] > [Device] > [Device Monitoring] > [Door]** on the Action Menu, the following interface will be shown: -

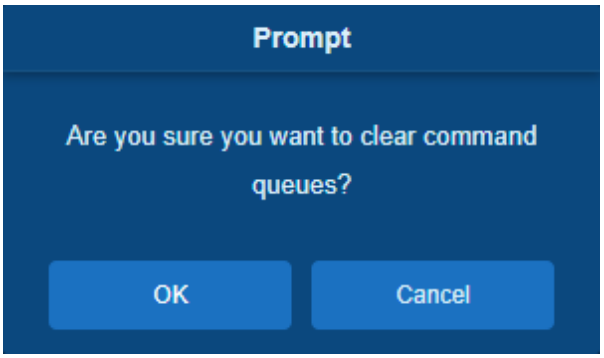


- Device commands can be exported in EXCEL, PDF, CSV file format.

Device Monitoring

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State
192.168.218.60	20100501999	Area Name	Get real-time event	Normal	0	None

- You may clear the command as needed. Click **[Clear Command]** in operations column.



- Click **[OK]** to clear.

✍**Note:**

After the implementation of Clear Command, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you can replace the current device with a higher-capacity one or delete the rights of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.

Operate State is the content of communications equipment of current device, mainly used for debugging.

The number of commands to be performed is greater than 0, indicating that the data is not yet synchronized to the device, so wait for the synchronization to complete.

Clear Command

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

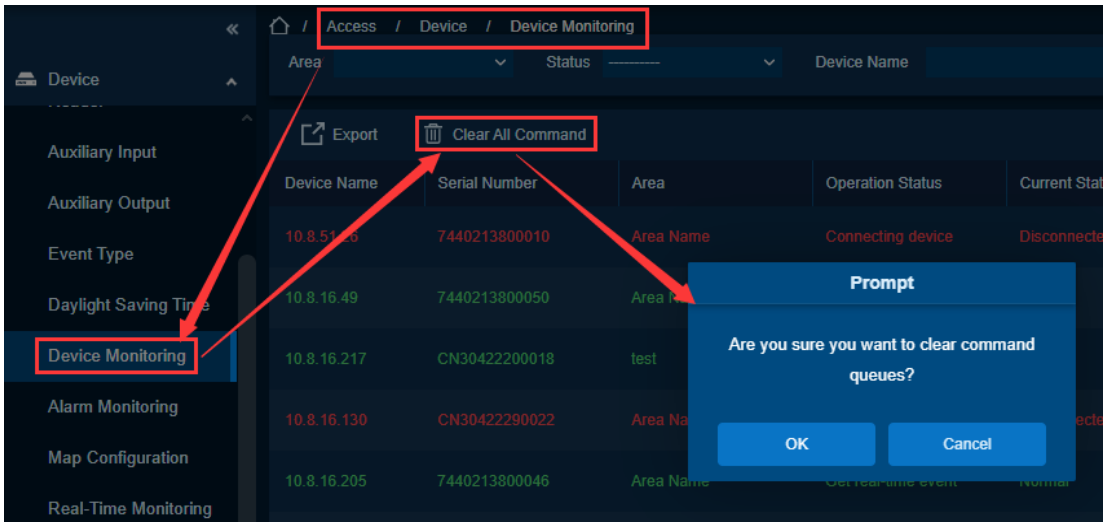
No need for this command.

Feature Trigger Result

Delete the command directly.

Steps:

- Click **[Access] > [Device] > [Device Monitoring] > [Clear All Command]** on the Action Menu, the following interface will be shown:



6.1.10. Alarm Monitoring

Function Description

Monitoring Of Alarm Events: If an alarm occurs on the door and the alarm event is not confirmed, the page will always display the alarm event.

Acknowledge

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

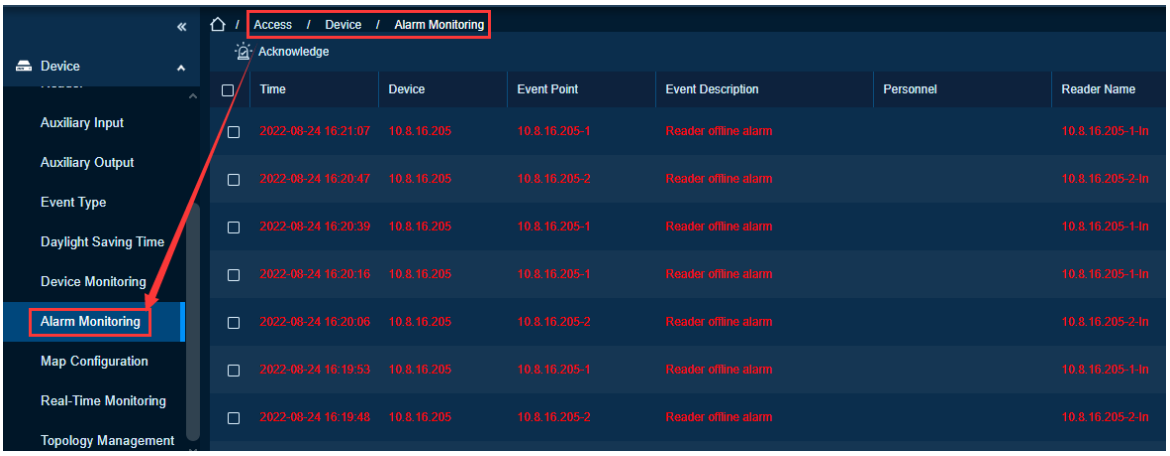
The current alarm event needs to be cleared.

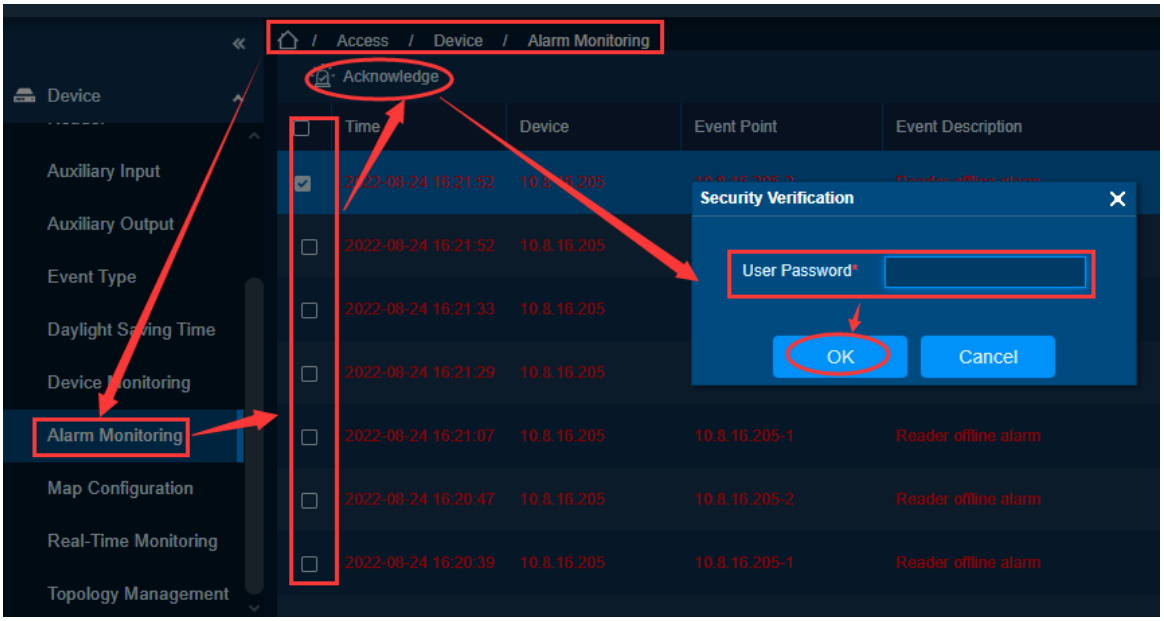
Feature Trigger Result

Uncheck the selected door alarm event and send email notifications (you need to set the alarm monitoring recipient's mailbox in the "parameter setting").

Steps:

- Click **[Access] > [Device] > [Alarm Monitoring]** on the Action Menu, Select the corresponding alarm event, click **[Acknowledge]**, the following interface will be shown: -



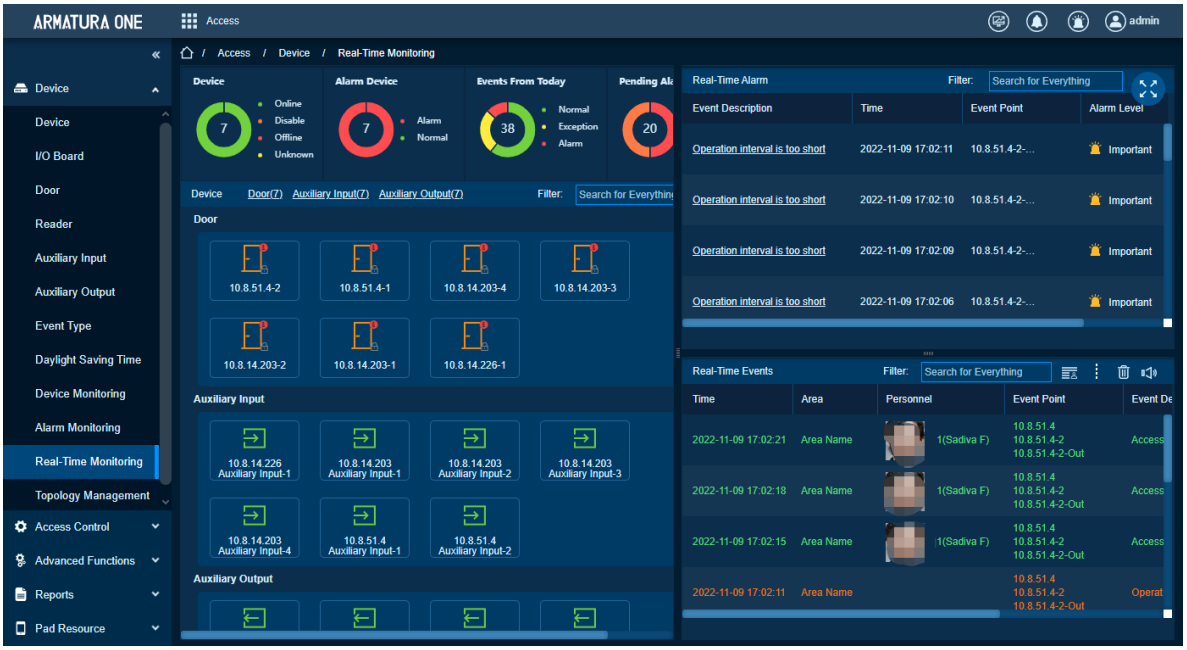


6.1.11. Real-Time Monitoring

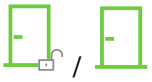
Function Description

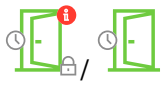
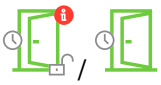
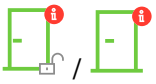
It will monitor the status and real-time events of doors under the access control panels in the system in real-time, including device status, event status, door status, Real-Time Alarm and Real-Time Events.

The Real-Time Monitoring interface is shown as follows:



The different icons represent status as follows:-

Icons	Status	Icons	Status
	Device disabled		Door Offline
	Door sensor unset, Relay closed /Without relay status		Door sensor unset, Relay opened/Without relay status
	Online status Door closed, Relay closed/Without relay status		Online status Door closed, Relay opened/Without relay status
	Online status Door opened, Relay closed/Without relay status		Online status Door opened, Relay opened/Without relay status
	Door opened alarm; Relay closed		Door opened alarm; Relay opened

	Door opening timeout, Relay closed /Without relay status, Door Sensor Opened		Door opening timeout, Relay opened/Without relay status
	Door opening timeout, Relay closed/ Door Sensor Closed		Door opening timeout, Relay opened/ Door Sensor Closed
	Door closed alarm, Relay closed/Without relay status		Door closed alarm, Relay opened/Without relay status
	Door sensor unset, Door alarm, Relay closed		Door sensor unset, Door alarm, Relay opened
	Door opening timeout, without relay status/Door Sensor Closed		Door locking
	Door always locked		Door closed
	Door closed unlocked		Door disabled
	Door no sensor		Door no sensor old
	Door no sensor unlocked		Door offline

	Door offline to device		Door open timeout old
	Door opened		Door opened old
	Door opened unlocked		
Note: If there is no relay status, it indicates that the current firmware does not support "detect relay status" function.			

Event Monitoring

Preconditions for Normal Use of Function

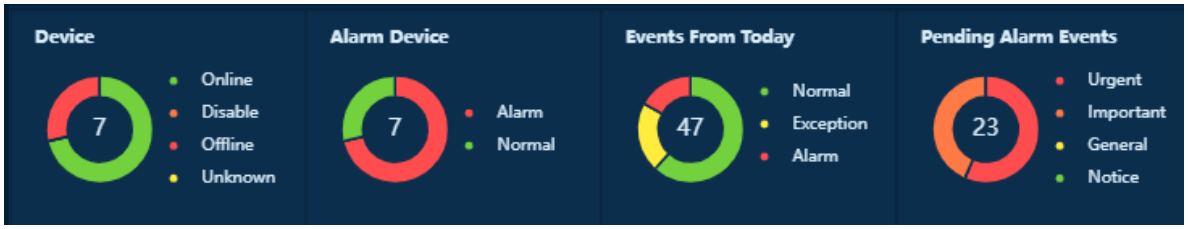
Log in to the system with the current account and have the authority.

Function Usage Scenarios

View the device status in real time on the software and perform operations.

Illustration

User can preview the device status, number of alarm device ,events status, and number of alarm events.



Door Monitoring

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

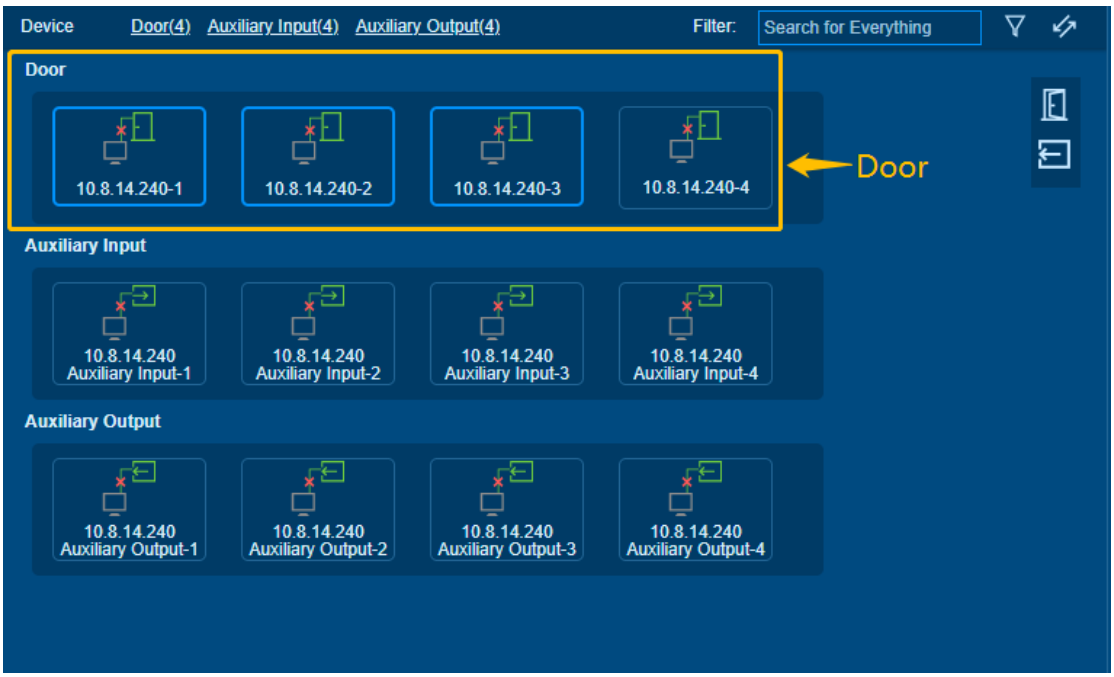
Function Usage Scenarios

View the device status in real time on the software and perform operations.

Feature Trigger Result

You can view the real-time status of the device, and remotely open and close the door and other operations.

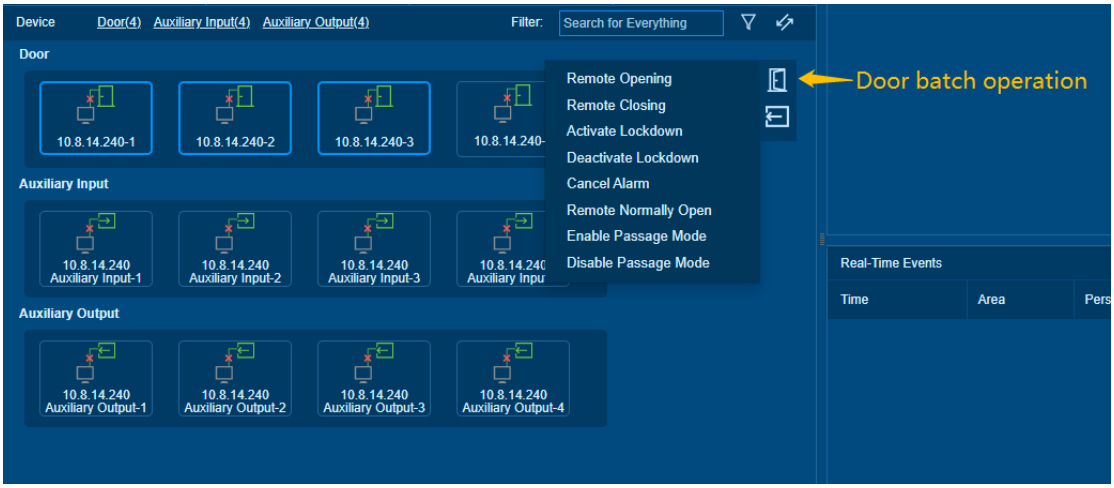
The following interface will be shown:



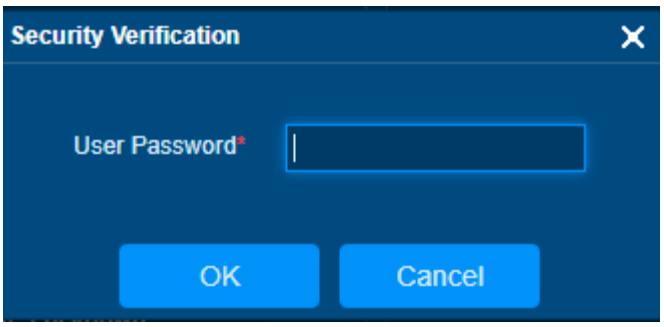
Remote Opening/Closing: It can control one door or all doors.

Steps:-

1. To control a single door or all doors, click over it.
2. Click batch operation, and click **[Remote Opening/ Closing]**



3. Enter user password



✍**Note:**

1. In remote opening, user can define the door opening duration (The default is 15s). You can select **[Enable Intraday Passage Mode Time Zone]** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).
2. To close a door, select **[Disable Intraday Passage Mode Time Zone]** first, to avoid enabling other normal open time zones to open the door, and then select **[Remote Closing]**.

Cancel the alarm: Once an alarming door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door or all door, move the cursor over the door icon, then click **[Cancel Alarm]** in the menu.

✍**Note:**

If **[Cancel the alarm]** fails, check if any devices are disconnected. If found disconnected, check the network.

Remote Normally Open: It will set the device as Normal Open by remote.

Activate Lockdown: It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

Deactivate Lockdown: It will unlock a locked door. This function is supported only by certain devices.

Enable Passage Mode： Enable the door normally open in the specific time quantum.

Disable Passage Mode： Enable the door normally close in the specific time quantum.

Auxiliary Input Monitoring

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority

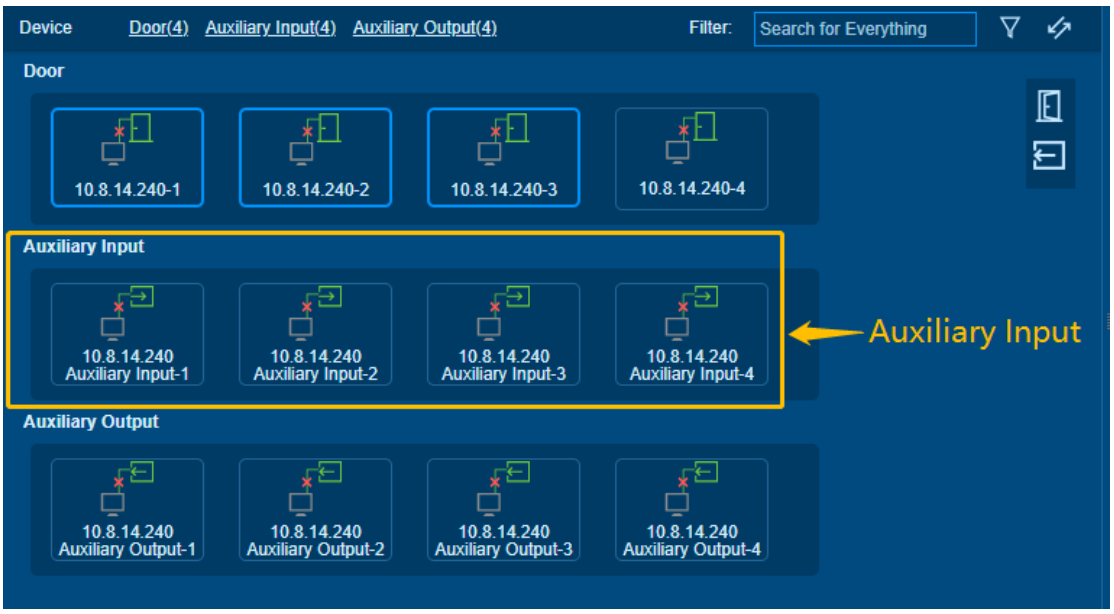
Function Usage Scenarios

Need to monitor real-time events of auxiliary inputs on the software.

Feature Trigger Result

It monitors current auxiliary input events in real-time.

The following interface will be shown:



Auxiliary Output Monitoring

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

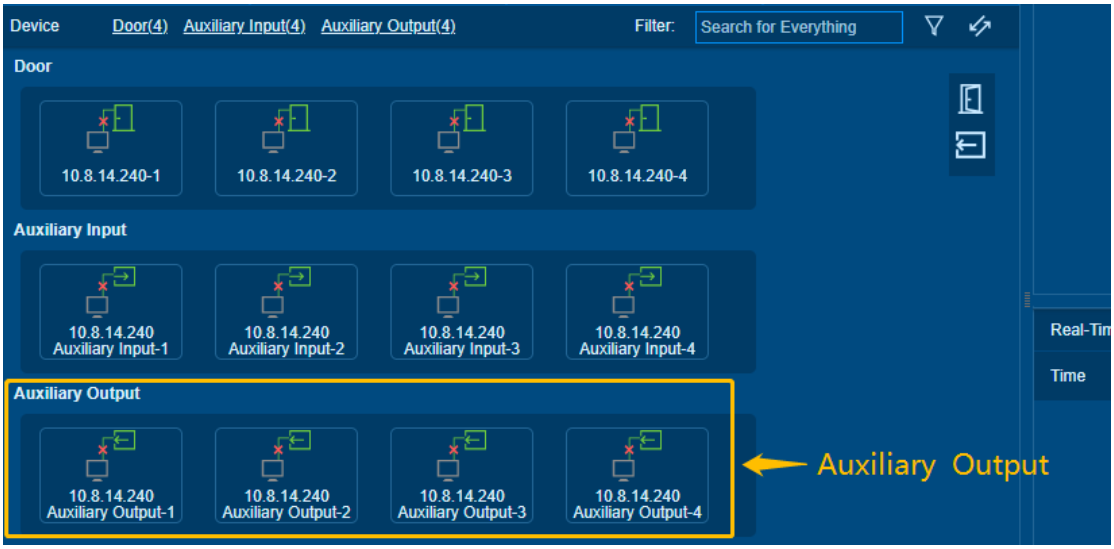
Function Usage Scenarios

It is necessary to remotely open, remotely close, and remotely open the auxiliary output device.

Feature Trigger Result

Here you can perform Remote open, Remote Close, Remote Normally Open.

The following interface will be shown:



Auxiliary Output remote opening/closing:

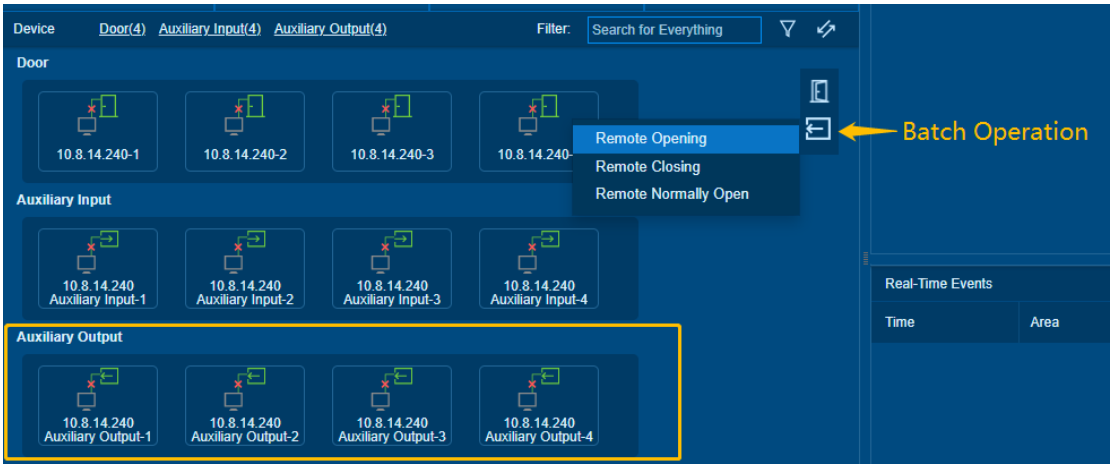
1. To control a single auxiliary device or all auxiliary devices, click over it.

2. Click batch operation and click **[Remote Opening/ Closing].**

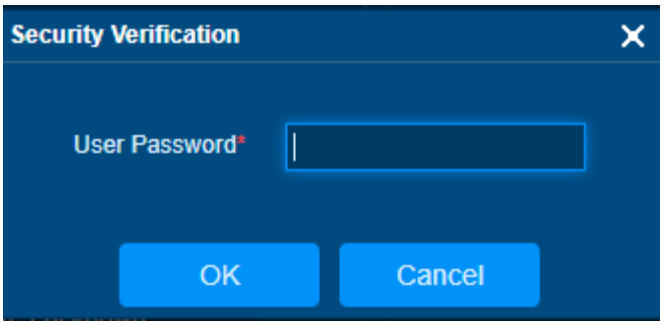
Remote Opening/Closing:

Steps:

1. To control a single device or all auxiliary devices, click over it.
2. 2.Click batch operation, and click **[Remote Opening/ Closing]**



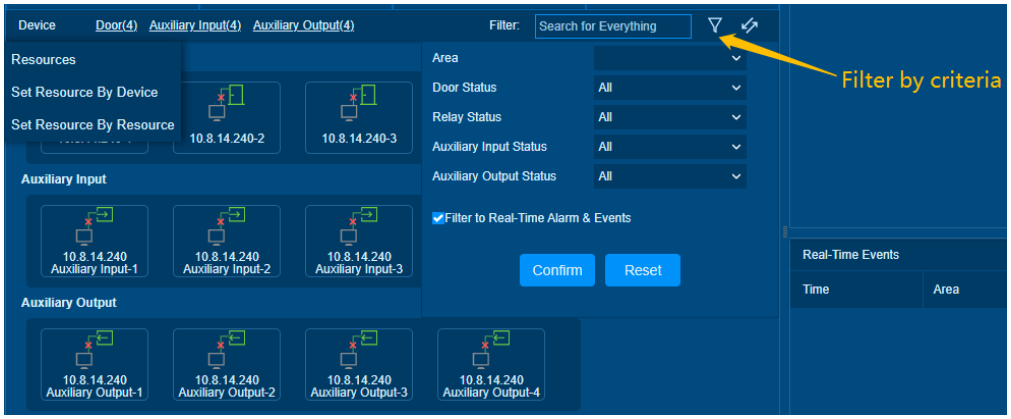
3. Enter user password



Remote Normally Open: It will set the auxiliary device as Normal Open by remote.

Search device： System supports fuzzy search.

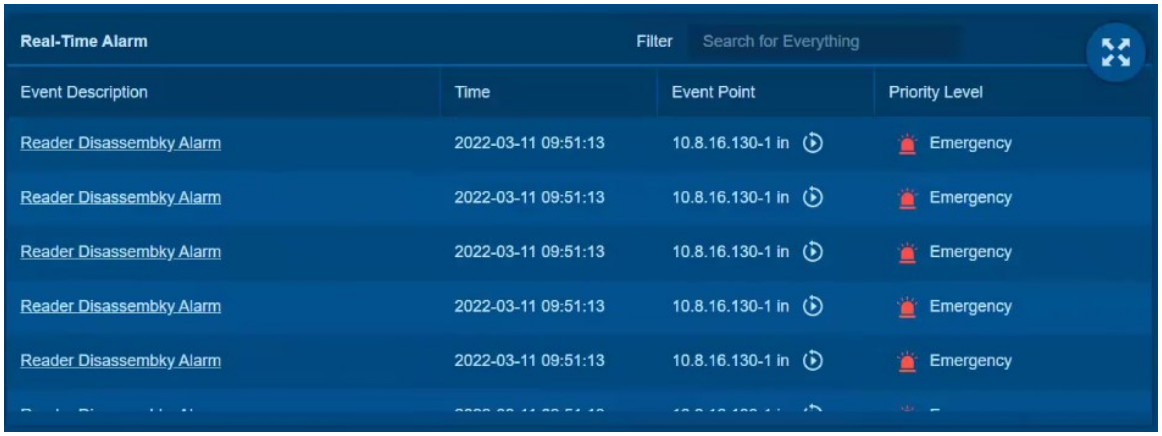
Filter device: System support filter devices by door status, relay status, auxiliary input status and auxiliary output status.



Real Time Alarm

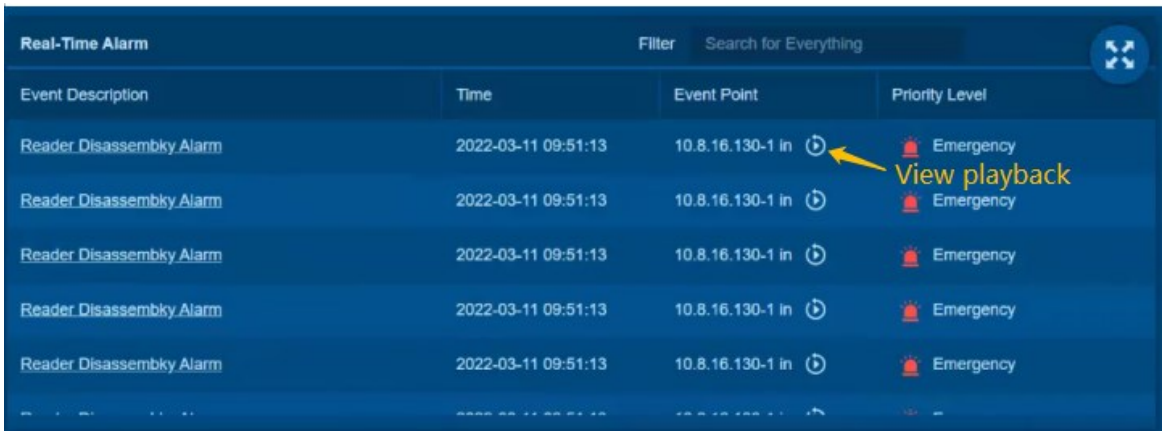
It clearly displays all alarm event in the interface, which user can acquire event description, time, event point, alarm level and personnel information.

The following interface will be shown:



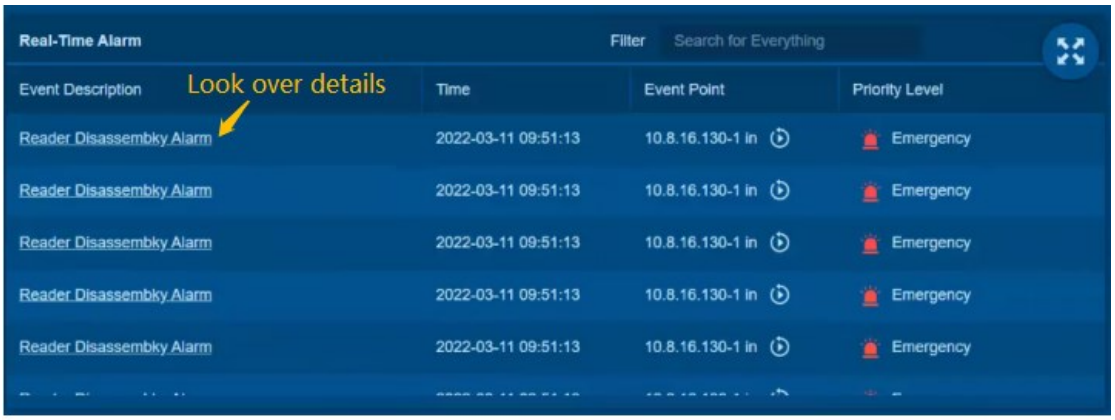
View video playback

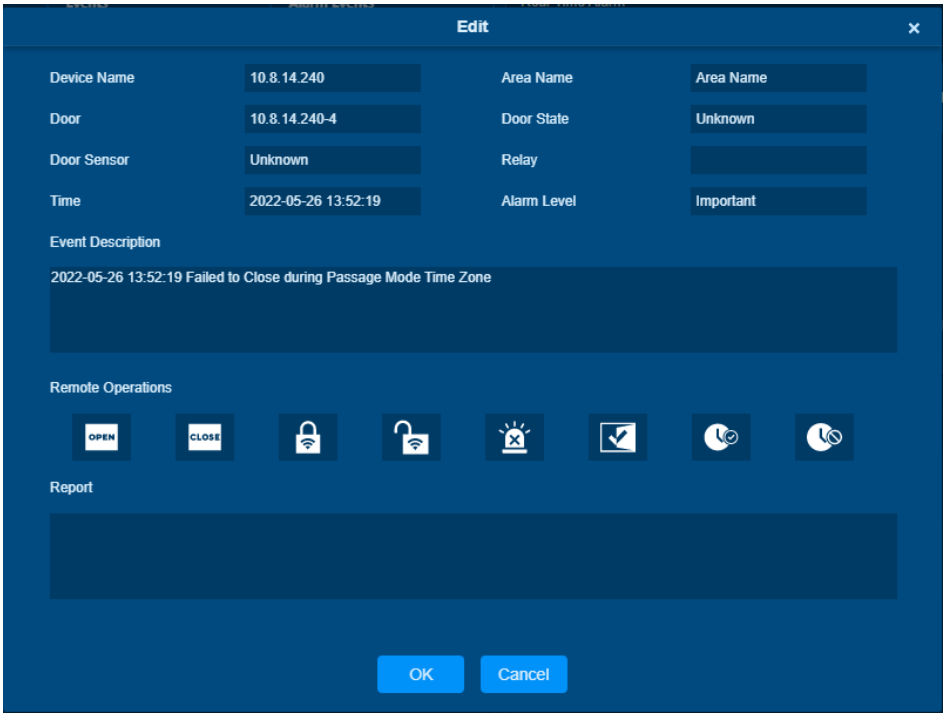
The user can view the video playback corresponding to the alarm event.



Look over details

It can view event details and perform remote operation by user.





Real-Time Events

All devices' events will be recorded in the real-time events, include emergency events, important events, general events, and prompt events.

The following interface will be shown:

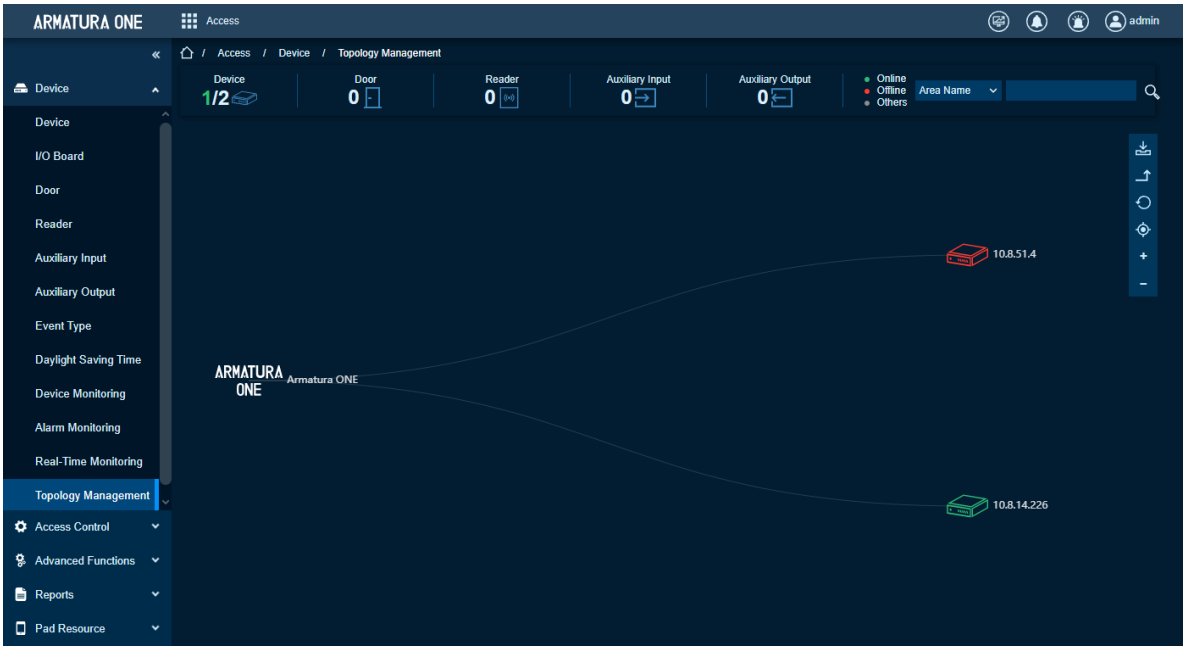
View video playback

The user can view the video playback corresponding to the real-time event.

6.1.12. Topology Management

Function Description

One topology map to check Controller-Door-Reader and IO relationship.



Status Monitoring

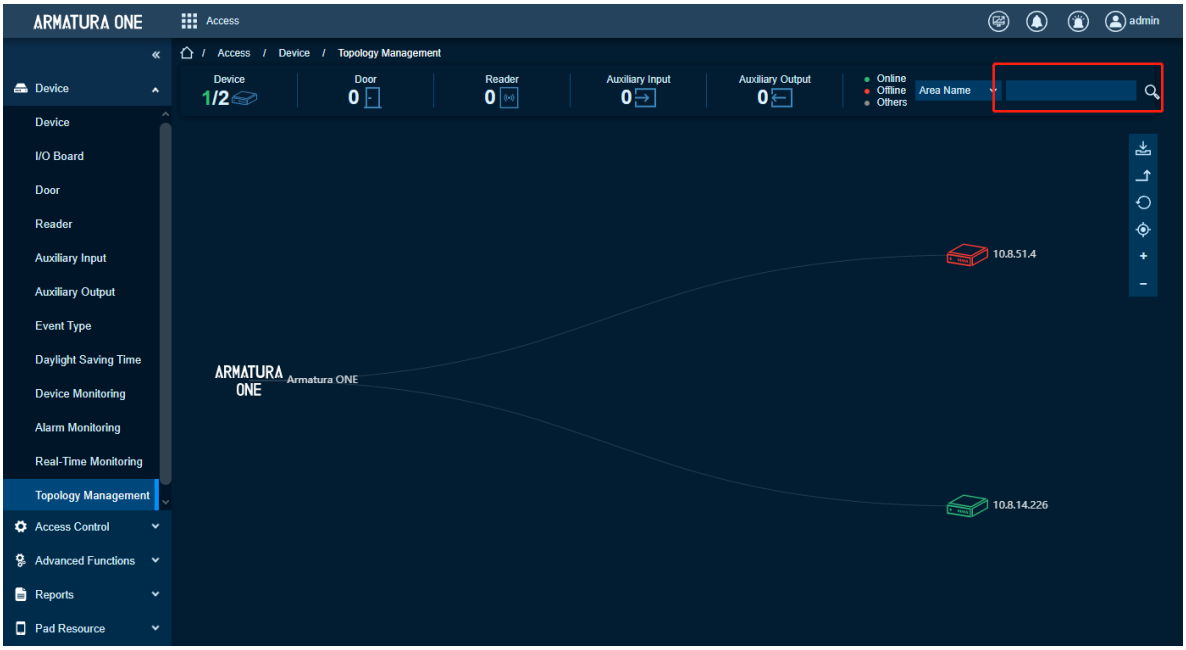
Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

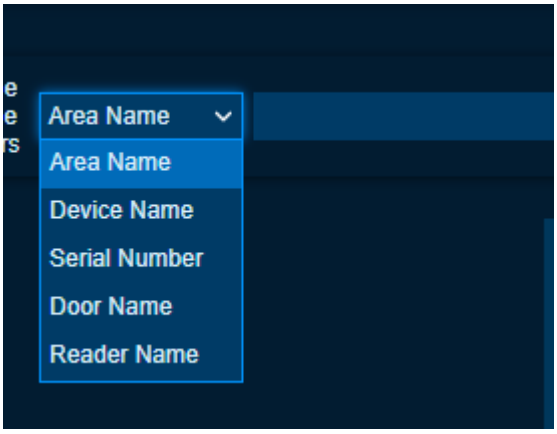
Function Usage Scenarios

From Status Monitoring admin can quick check if device/reader/io expansion board is offline.

Topology Map

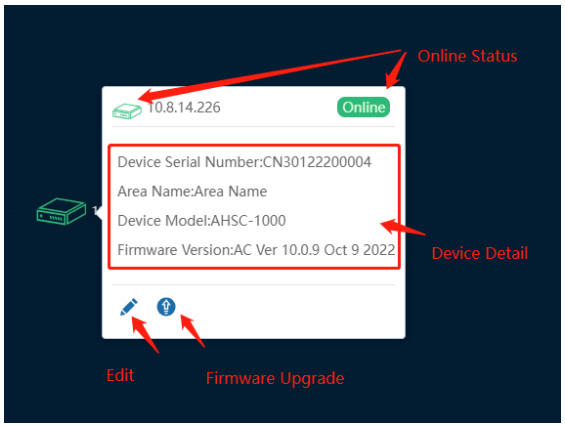
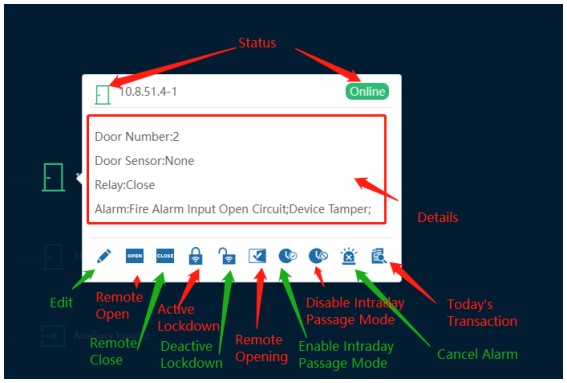
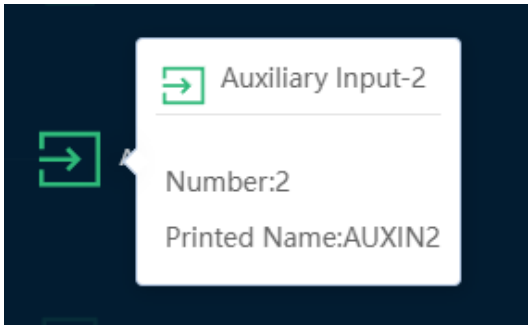


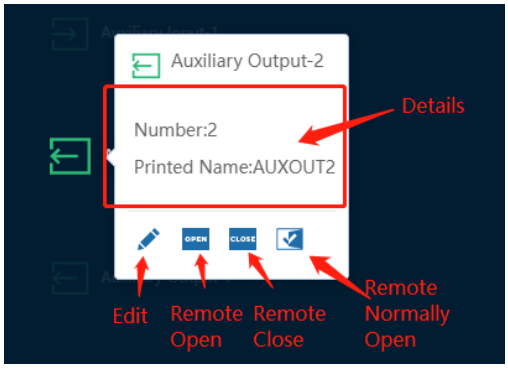
Support Search by Area Name/Device Name/Serial Number/Door Name/Reader Name to filter.



Icon	Introduction
Download	Download this map as a '.png' file
Back to previous level	Back to previous level
Refresh	Refresh Map
Location	Find a location for middle of map

Zoom IN	Map Zoom IN
Zoom Out	Map Zoom Out
*Support mouse scroll wheel scrolling up/down to zoom in and out	

View	Introduction
	**Device Monitoring** Device Status Green: Online Red: Offline Grey: Unknown
	**Door Monitoring** Door Status Green: Online Red: Offline Grey: Unknown
	**Aux IN Monitoring**

	**Aux Out Monitoring**

6.2. Access Control

Functions description:

Operate the access control device, including setting the time, setting the access levels by personnel and department, and performing functions such as interlocking, linkage and anti-passback

Function List:

Function	Description
Time Zones	Add, edit, delete time.
Holidays	Add, edit, delete holidays
Access Levels	Add, edit, add doors, door control-remote door open, door control-remote door close, door control-cancel alarm, door control-remote normally open, door control-enable, door control-disable, door control-remote lock, door control-remote unlock, door control-enable the day's normally open time zone, door control-disable the day's normally open time zone, delete the door, export.
Set Access by Levels	Add, delete, export personnel.
Set Access by Person	Access control settings, add belonged access levels, delete belonged access levels, export.
Set Access by Department	Add default access levels, delete default access levels.
Interlock	Add, edit, delete
Linkage	Add, edit, delete
Anti-passback	Add, edit, delete
First Person Normally Open	Add, edit, delete personnel.

Multi-person Group	Add, edit, delete personnel.
Multi People Opening Door	Add, edit, delete.
Verification Mode	Add, edit, delete door
Verification Mode Group	Add, delete personnel
Parameter Settings	Type of Getting Transactions setting, Transactions Auto-Export setting, Real Time Monitoring setting, Compare photo delivery settings.

6.2.1. Time Zones

Function Description

You can set the time to accurately open and close the door for each function of the device.

Add Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

The device needs to open the door in a specific time.

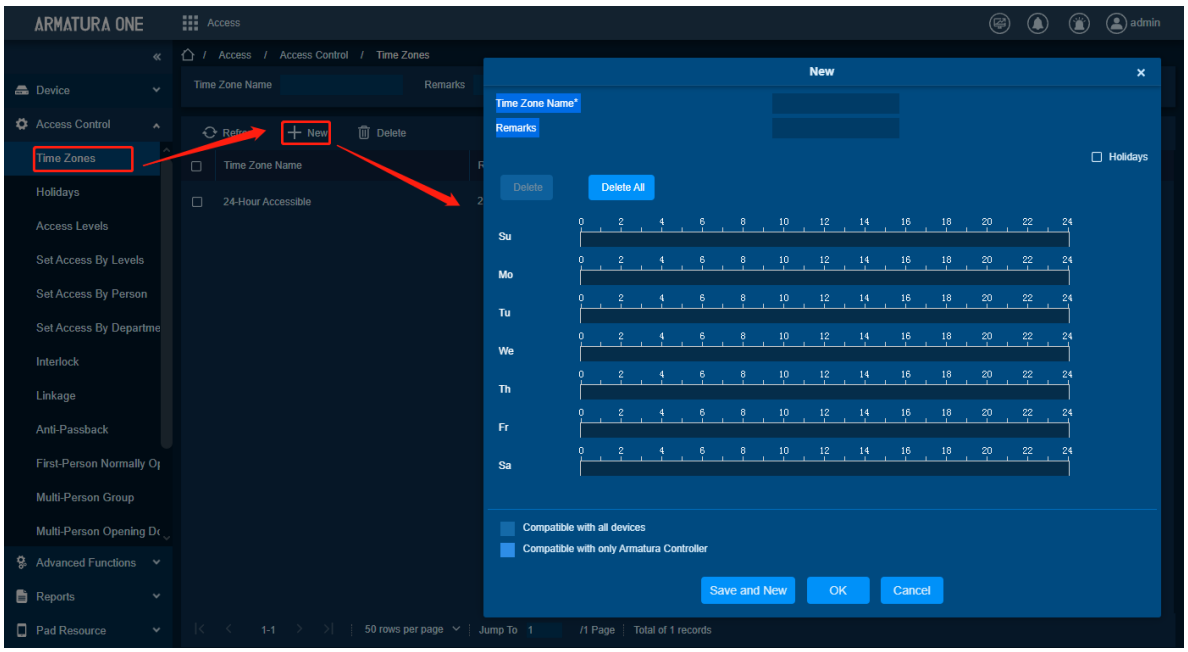
Feature Trigger Result

It sets usage time of a door; the reader is usable during valid time periods of certain doors and unusable during other time periods. Time Zone can also be used to set Normal Open time periods or set access levels so that specified users can only access specified doors during specified time periods (including access levels and First-Person Normally Open).

The system controls access according to Time Zones (up to 255 time zones). The format of each interval for a time zone: HH: MM-HH: MM. Initially, by default, the system has an access control time zone named **[**24 hours Accessible**]**. This time cannot be modified and deleted. The user can add new Access Control Time Zones that can be modified or deleted.

Steps:

- Click **[Access Control] > [Time Zones] > [New]** to enter the time zone setting interface.



The parameters are as follows: -

Time Zone Name: Any character, up to a combination of 30 characters.

Remarks: Detailed description of the current time zone, including explanation of current time zone and primary applications. Users can input up to 50 characters in this field.

Interval and Start/ End Time: One Access Control Time Zone includes 3 intervals for each day in a week, and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as interval 1, and 00:00-00:00 as interval 2/3. If the interval is Normal Close: all inputs will be 00:00-00:00. If users use only one interval, they just need to fill in interval 1, and interval 2/3 will be the default value. Similarly, when users only use the first two intervals, the third interval will be the default value. When using two or three intervals, users need to ensure that the two or three intervals do not overlap, and the time shall not cross the days. Or the system will prompt error.

Holiday Type: Three holiday types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access purpose. The holiday type is optional. If the user does not enter one, the system will use the default value.

Copy on Monday: You can quickly copy the settings of Monday to other weekdays.

After setting, click **[OK]** to save, and it will display in the list.

Edit Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

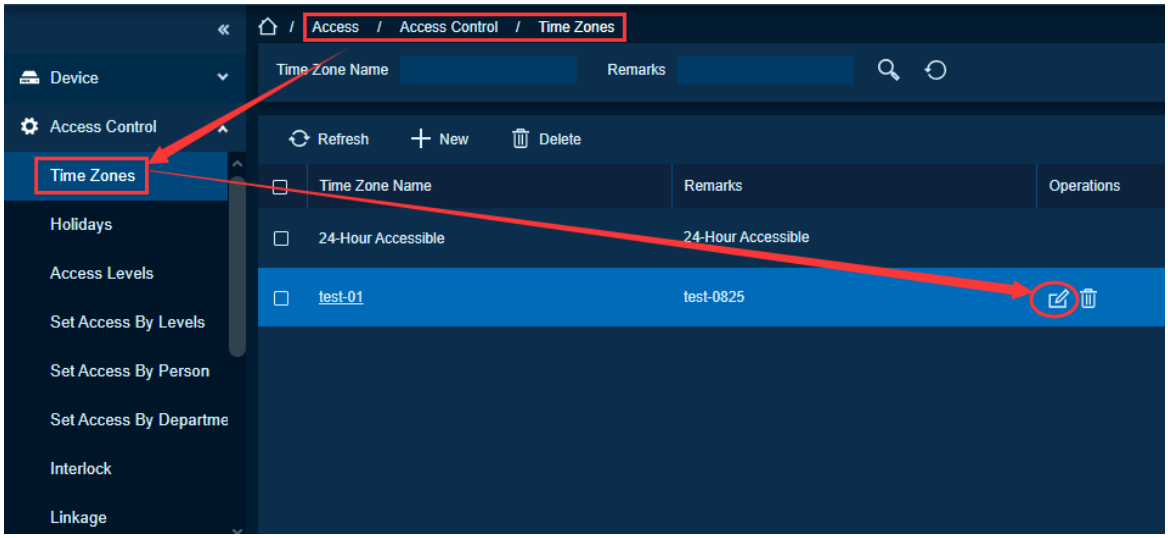
Need to modify the door opening time set before the device.

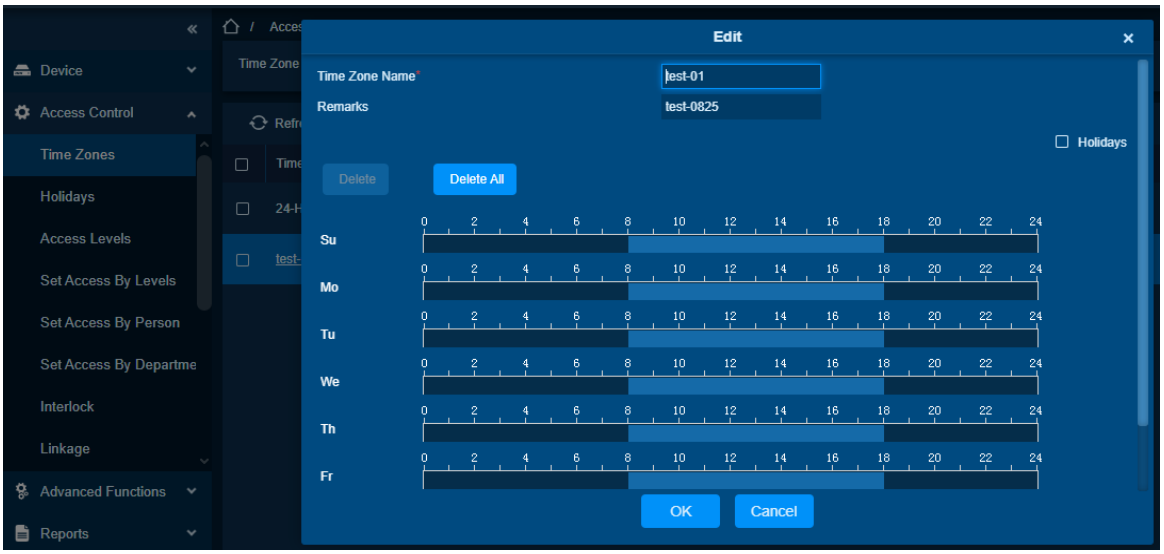
Feature Trigger Result

Modify the time when the device is open.

Steps:

Click the **[Edit]** button under Operation to enter the edit interface. After editing, click **[OK]** to save.





Delete Time Zone

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

Function Usage Scenarios

- There is no need to control the access time of the door.
- The door access time is set incorrectly.

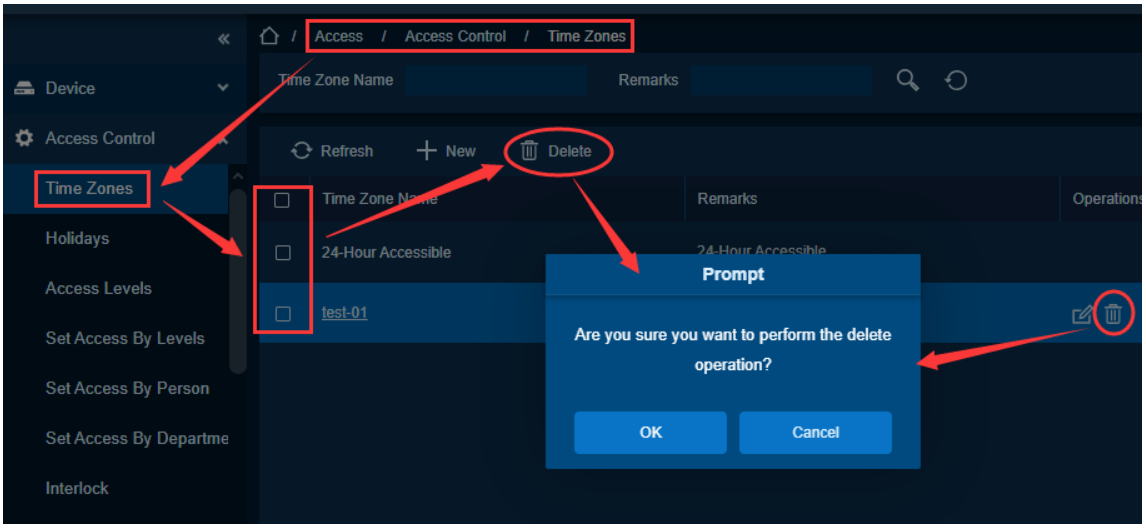
Feature Trigger Result

The time is deleted from the time list and can no longer be used.

Steps:

Click the **[Delete]** button under Related Operation, then click **[OK]** to delete, or click **[Cancel]** to cancel the operation.

A time zone in use cannot be deleted. An alternative way is to tick the check boxes before one or more time zones in the list and click the **[Delete]** button over the list, then click **[OK]** to delete, and click **[Cancel]** to cancel the operation.



6.2.2. Holidays

Function Description

Access Control Time of a holiday may differ from that of a weekday. The system provides access control time setting for holidays. Access Control Holiday Management includes **Add, Modify and Delete**.

Add Holiday

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

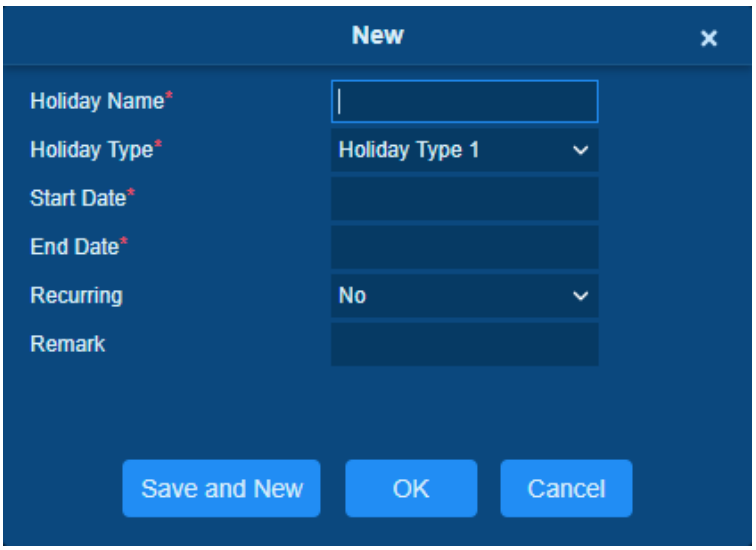
Need to set the time of special holidays.

Feature Trigger Result

Controls such as opening and closing doors according to the access control time set during holidays.

Steps:

- Click **[Access Control]** > **[Holidays]** > **[New]** to enter edit interface.



Fields are as follows: -

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/End Date: The date format: 2010-1-1. Start Date cannot be later than End Date, otherwise the system will prompt an error message. The year of Start Date cannot be earlier than the current year, and the holiday cannot be set across two different years.

Recurring: It refers a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

After editing, click **[OK]** button to save, and it will display in the holiday list.

Edit Holiday

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

- Need to modify the time setting for special holidays.
- The current holiday time set is wrong.

Feature Trigger Result

Modify the new holiday time.

Steps:

Click **[Holiday Name]** or **[Edit]** button under Operations to enter the edit interface. After modification, click

[OK] to save and quit.

Delete Holidays

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

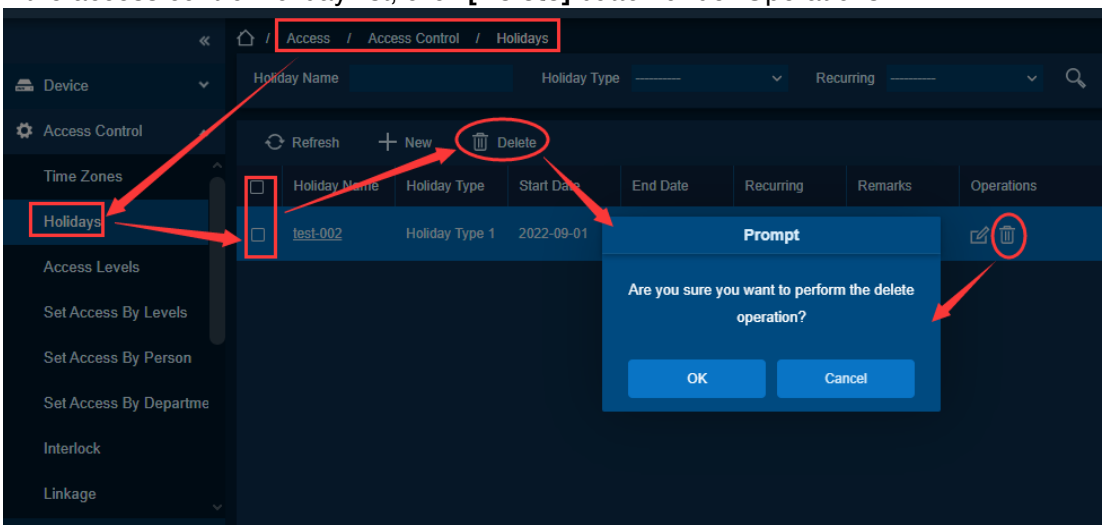
- No need for the holiday time which is currently set.
- The current set holiday time is wrong.

Feature Trigger Result

Delete the selected holiday time.

Steps:

- In the access control holiday list, click **[Delete]** button under Operations.



- Click **[OK]** to delete, click **[Cancel]** to cancel the operation.

If an Access Control Holiday is already in use, then it can't be deleted.

6.2.3. Access Levels

Function Description

Access levels indicate that one or several selected doors can be opened by verification of a combination of different person within certain time zone. The combination of different person set in Personnel Access Level option.

Add Access Level

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The access control module has set access control time and area for selection.

Function Usage Scenarios

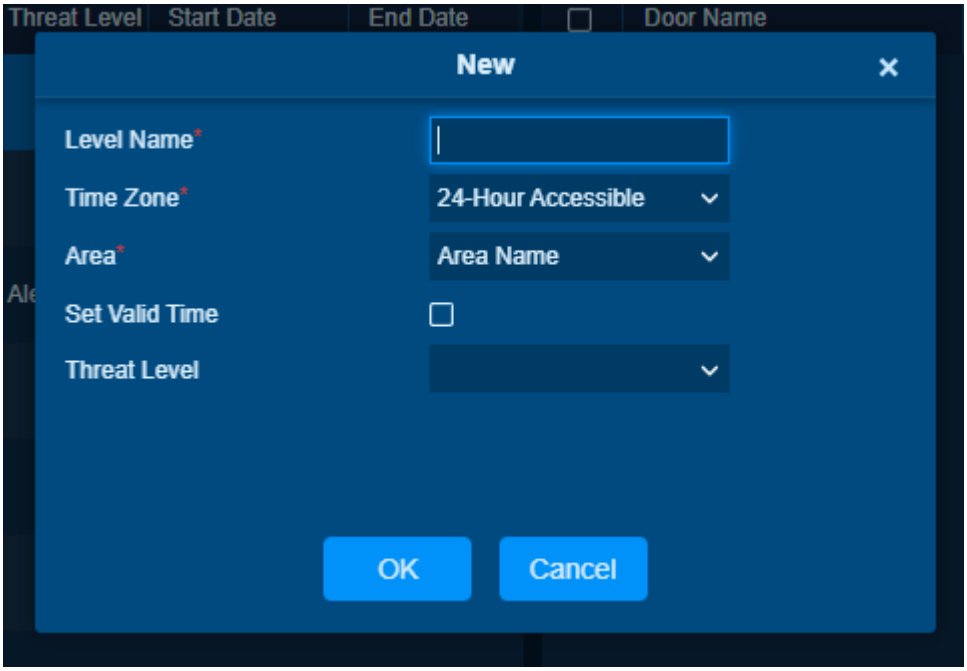
Need to perform the same authority management for certain doors, including access control time and area.

Feature Trigger Result

Set up the access levels corresponding to the area and time.

Steps:

- Click **[Access Control] > [Access Levels] > [New]** to enter the Add Levels editing interface.



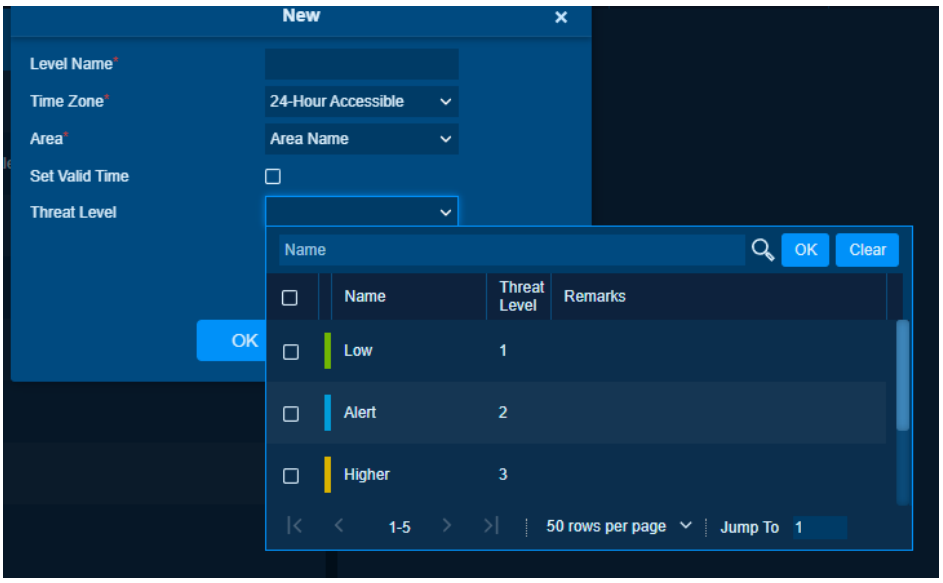
Level Name: Level Name (unrepeatable)

Time Zone: check Time Zones

Area: Set privilege limit for different user

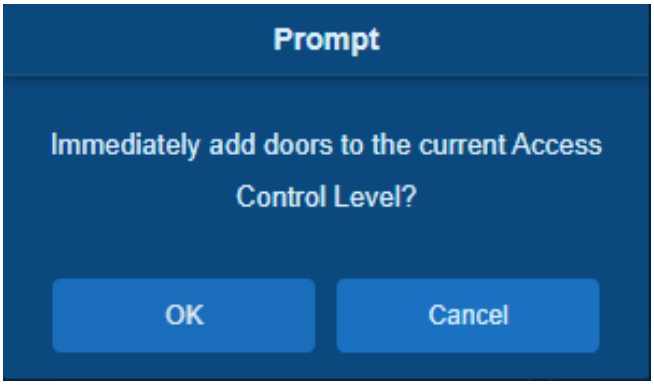
Valid Time: This level only available within this valid period

Access Level Threat Level: Set a threat level for access level, if system threat level change, system will check whether access level is the same threat level with current system threat level, if access level threat level does not include current threat level, this access level will be limit for access.



More details check Threat Level

- Click **[OK]**, the system prompts **"Immediately add doors to the current Access Control Level"**, then click **[OK]** to add doors, then click **[Cancel]** to return the access levels list. The added access level is displayed in the list.



✍**Note:**

Different doors of different panels can be selected and added to an access level.

Edit Access Level

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

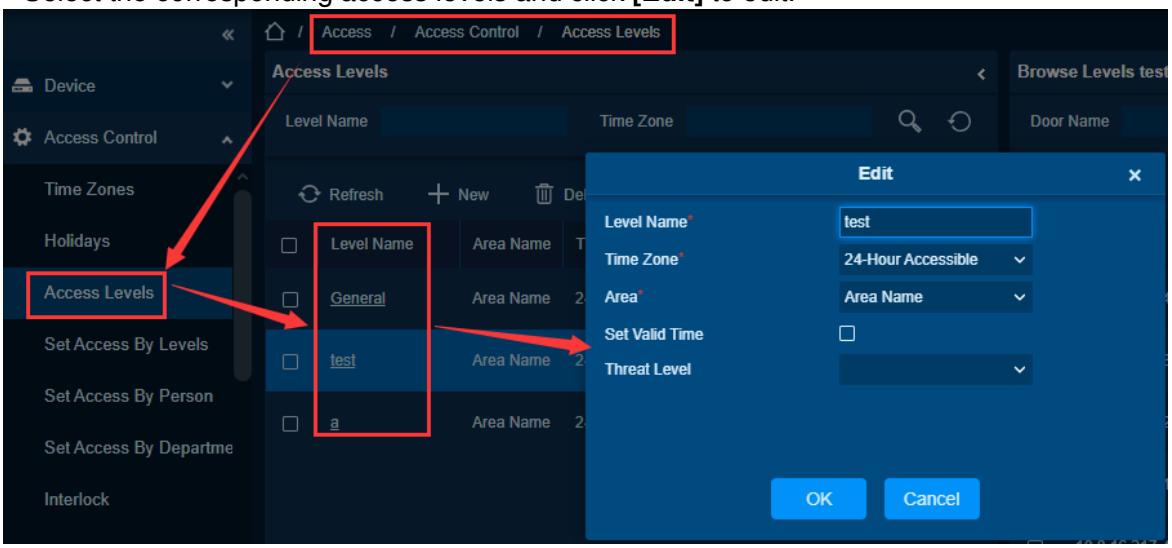
Need to modify the authority management of certain doors, including the authority group name, access control time zone and area.

Feature Trigger Result

Modify the access levels of the corresponding area and time.

Steps:

- Click **[Access]** > **[Access Control]** > **[Access Levels]** to display the access authority group interface.
- Select the corresponding access levels and click **[Edit]** to edit.



Delete Access Level

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

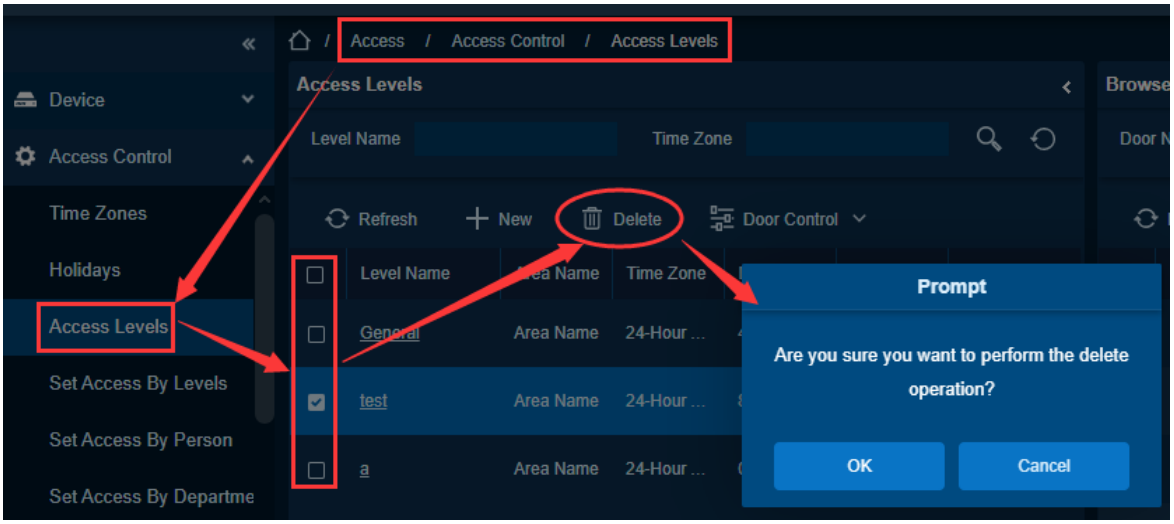
The authority management of some doors is no longer needed.

Feature Trigger Result

Delete the access levels.

Steps:

- Click **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Select the corresponding access levels and click **[Delete]** to edit.



Add Door to Access Level

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

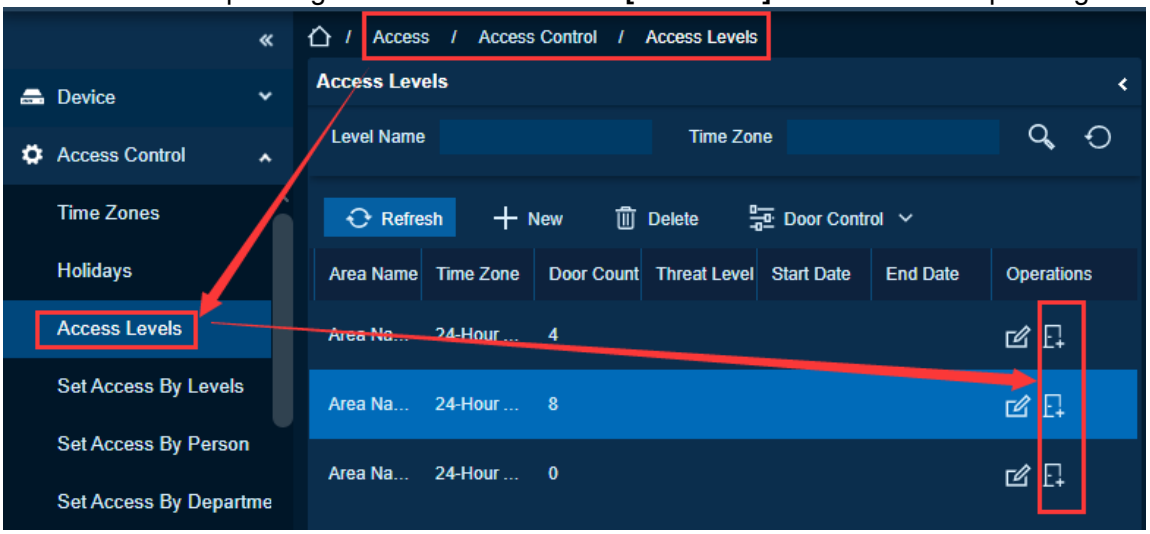
Need to set the access levels for some doors.

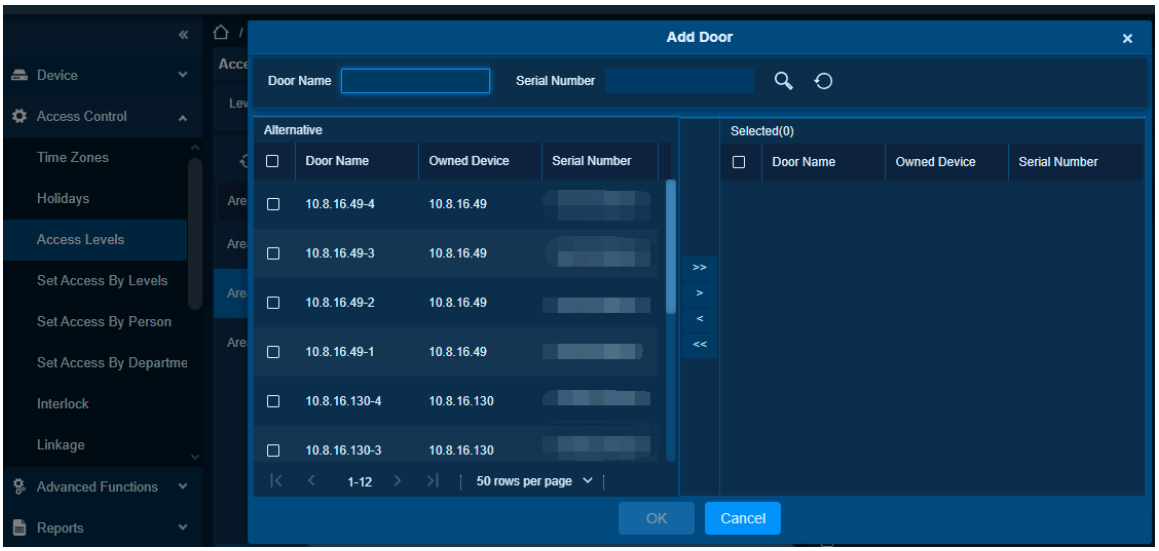
Feature Trigger Result

The settings of the access levels are delivered to the corresponding door.

Steps:

- Click **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Select the corresponding access levels and click **[Add Door]** to add the corresponding door.





Delete Door from Access Level

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

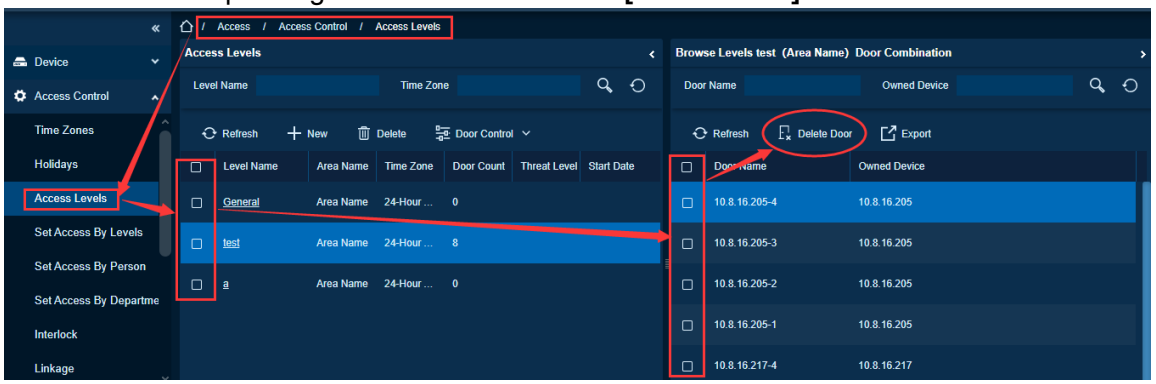
Need to set the access levels for some doors.

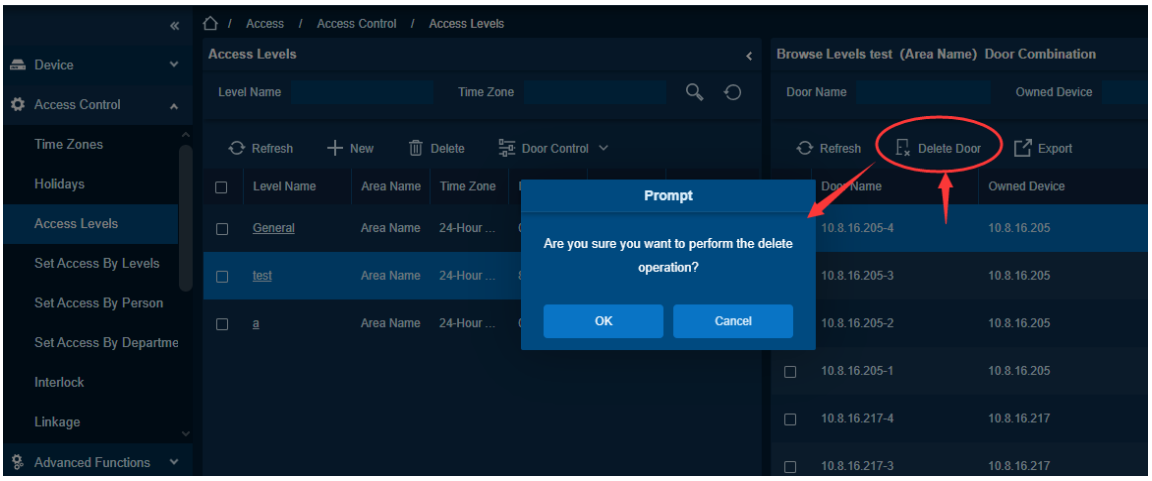
Feature Trigger Result

Delete the corresponding door in the corresponding access control access levels.

Steps:

- Click **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.
- Select the corresponding access levels and click **[Delete Door]** to edit.





Export specific Access Level's Door List

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

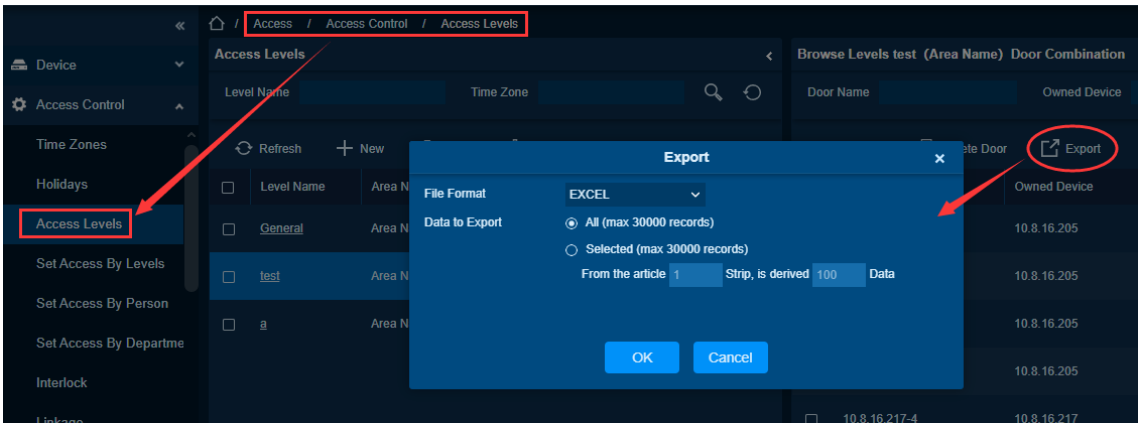
For multiple doors, it needs to be exported for easy viewing.

Feature Trigger Result

You can export files in multiple formats, including door names and their devices.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding access levels, in the column on the right door, click **[Export]**, select the file format and export method, and click **[OK]** to export.



Door Control - Remote Open Door

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

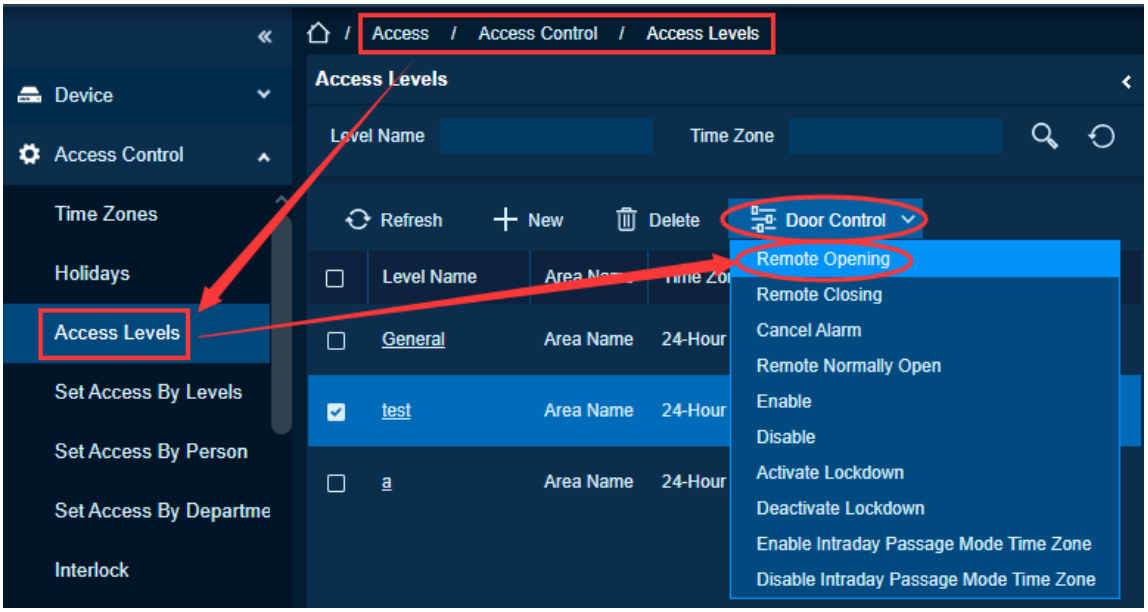
Batch remote opening

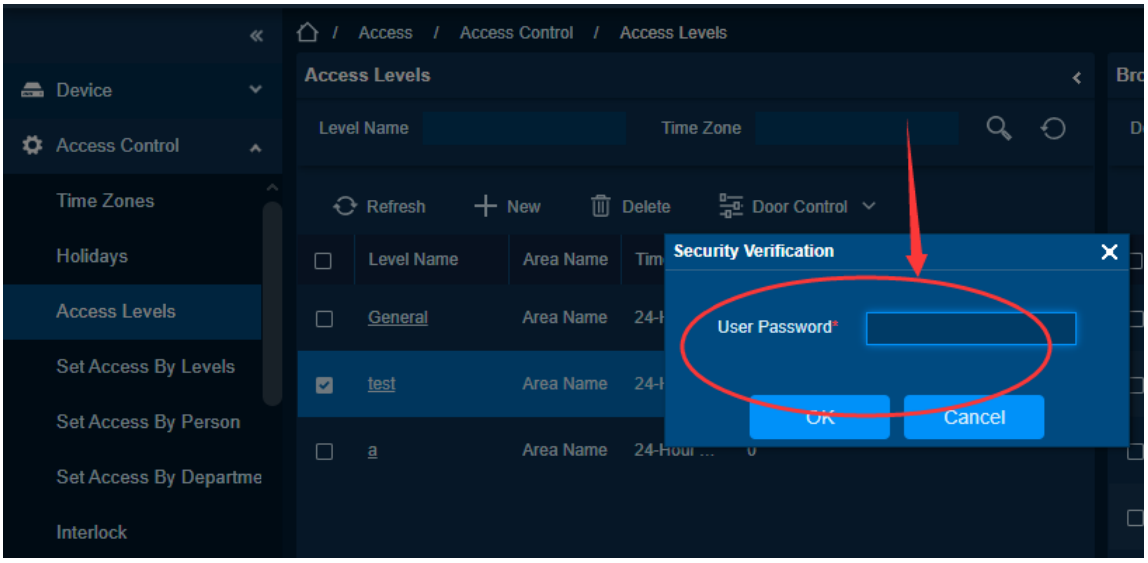
Feature Trigger Result

Open all doors in batches remotely under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding access levels, click **[Door Control]> [Remote Opening]** and enter the user login password to trigger remote door opening.





Door Control - Remote Door Closing

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

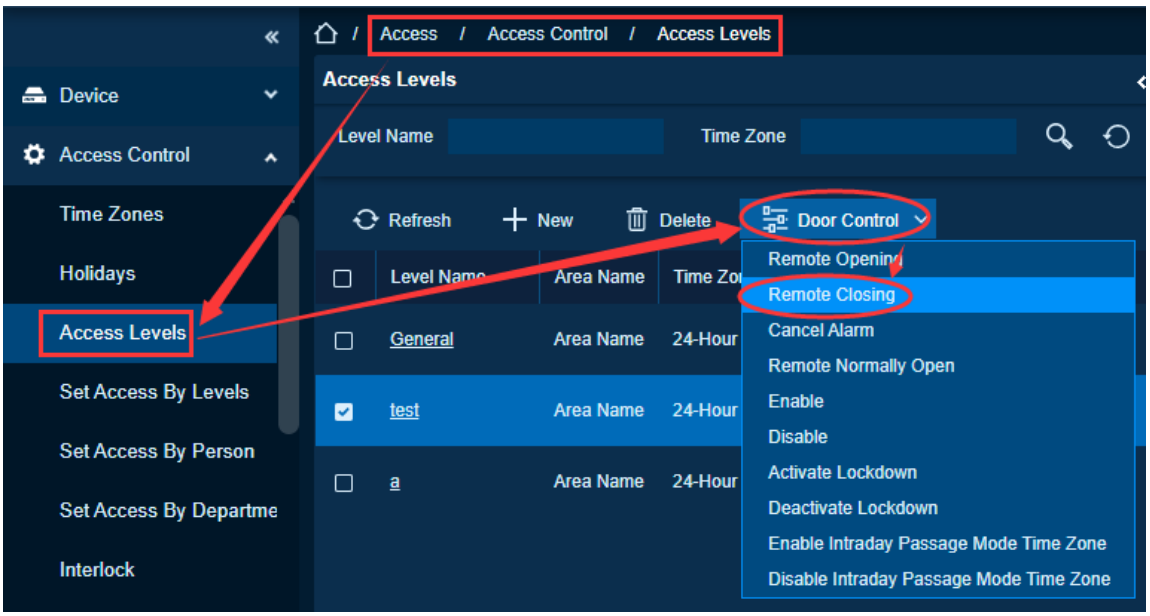
Batch Remote Closing

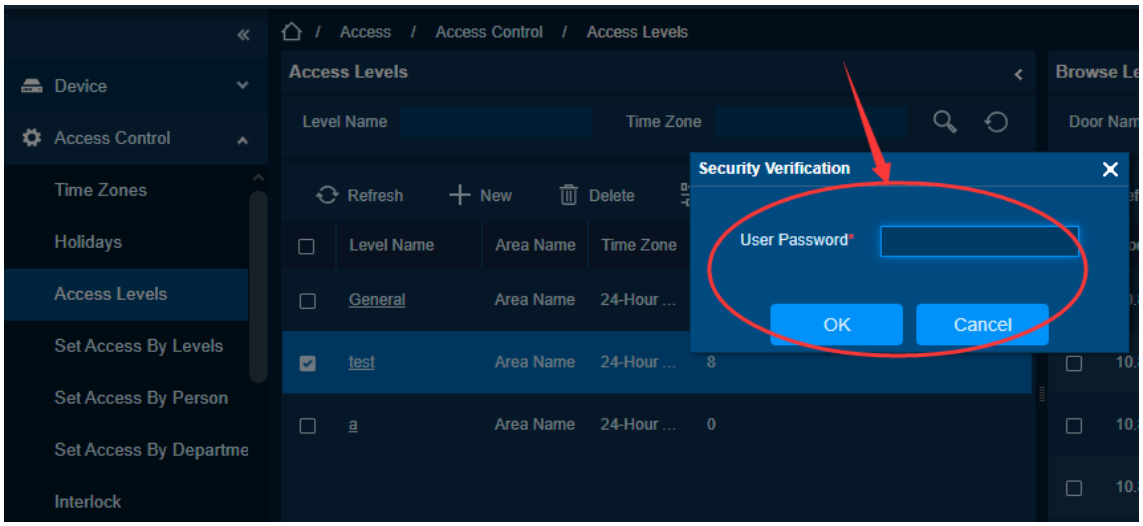
Feature Trigger Result

Perform batch remote closing of all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access authority group interface.
- Select the corresponding access levels, **click [Access] > [Access Control] > [Access Levels]> [Door Control]> [Remote Closing]** and enter the user login password to trigger remote door closing.





Door Control - Cancel Alarm

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

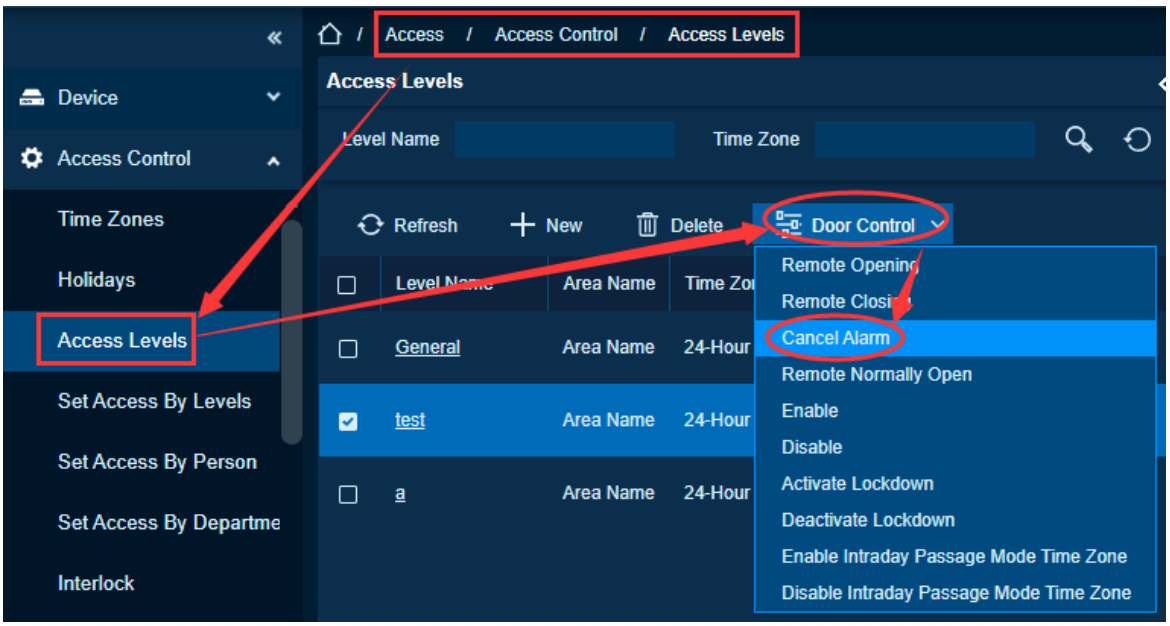
Cancel Alarm in Batches

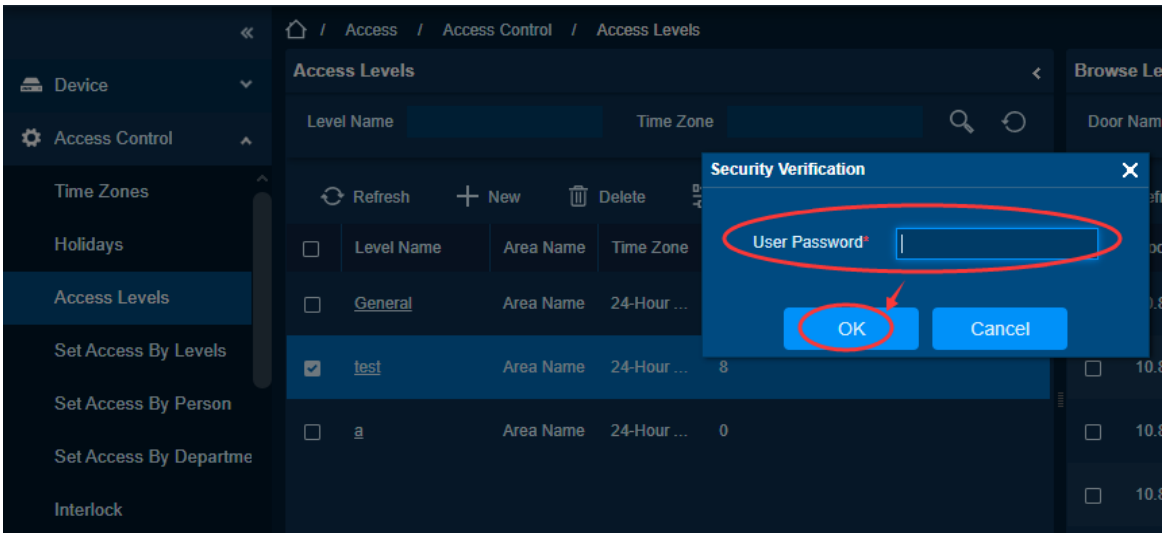
Feature Trigger Result

Batch cancel the alarm for all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]> [Door Control]> [Cancel Alarm]** to display the access levels interface.
- Select the corresponding access levels, click [Door Control]> [Cancel Alarm] and enter the user login password to trigger the cancellation of the alarm.





Door Control - Remote Normally Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

Batch Remote Normally Open

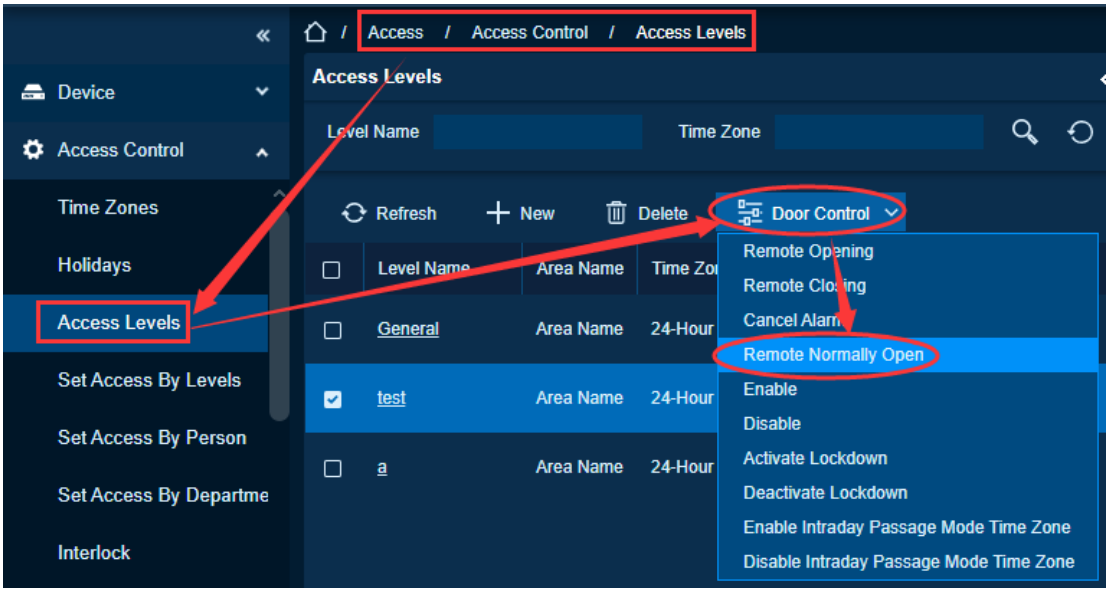
Feature Trigger Result

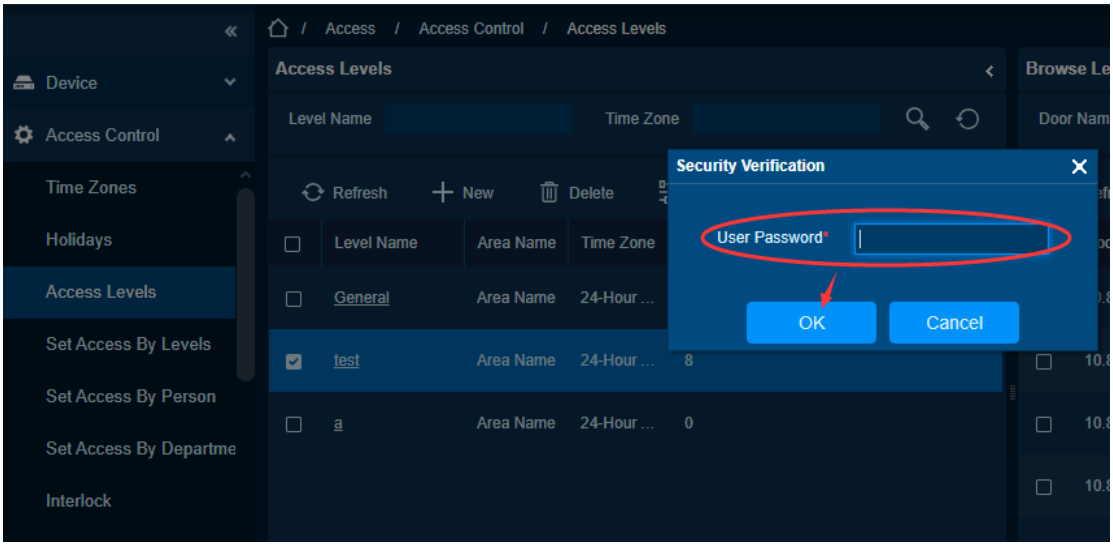
Batch remote normally open all doors under the access levels.

Steps:

- Click **[Access]** > **[Access Control]** > **[Access Levels]** to display the access levels interface.

- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control]> [Remote Normally Open]** and enter the user login password to trigger the remote normally open.





Door Control - Enable

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

Function Usage Scenarios

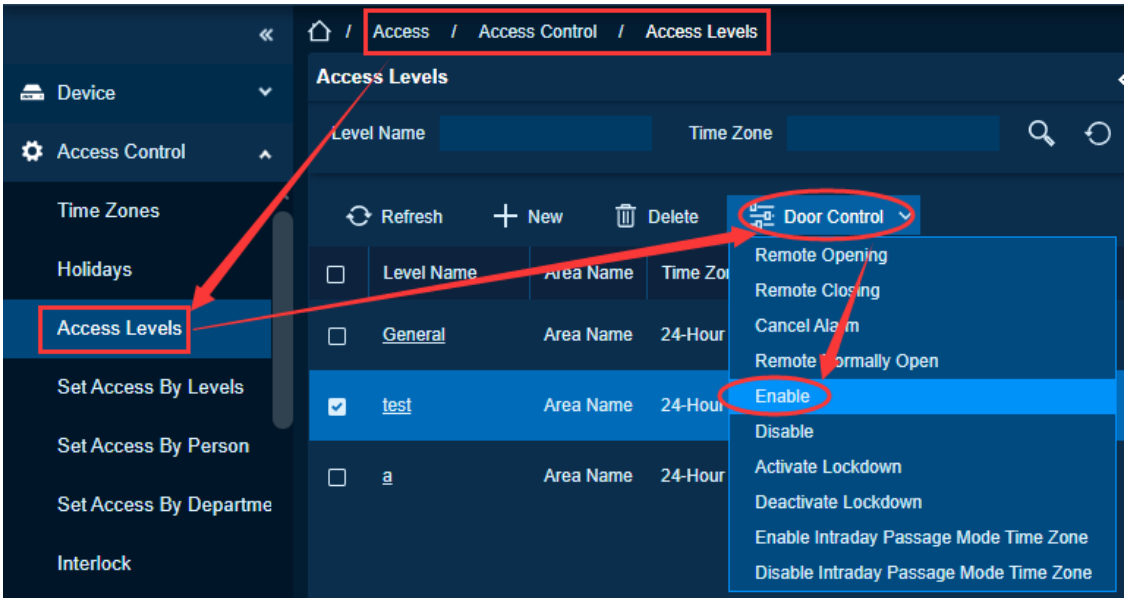
Enable each door of the access control access levels in batch.

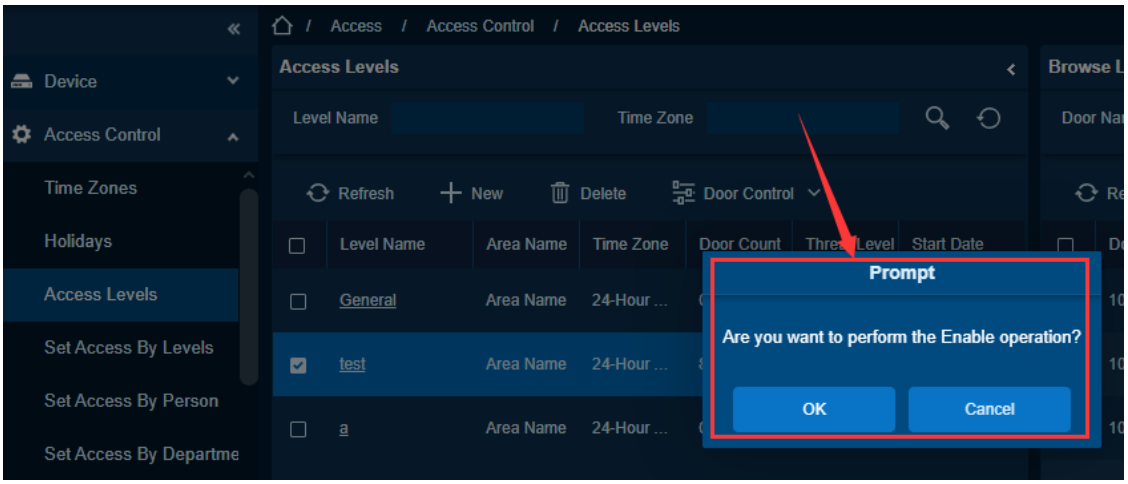
Feature Trigger Result

Batch enable all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control]>[Enable]** and enter the user login password to trigger the opening of the door.





Door Control - Disable

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

Disable all doors of the access control group in batches.

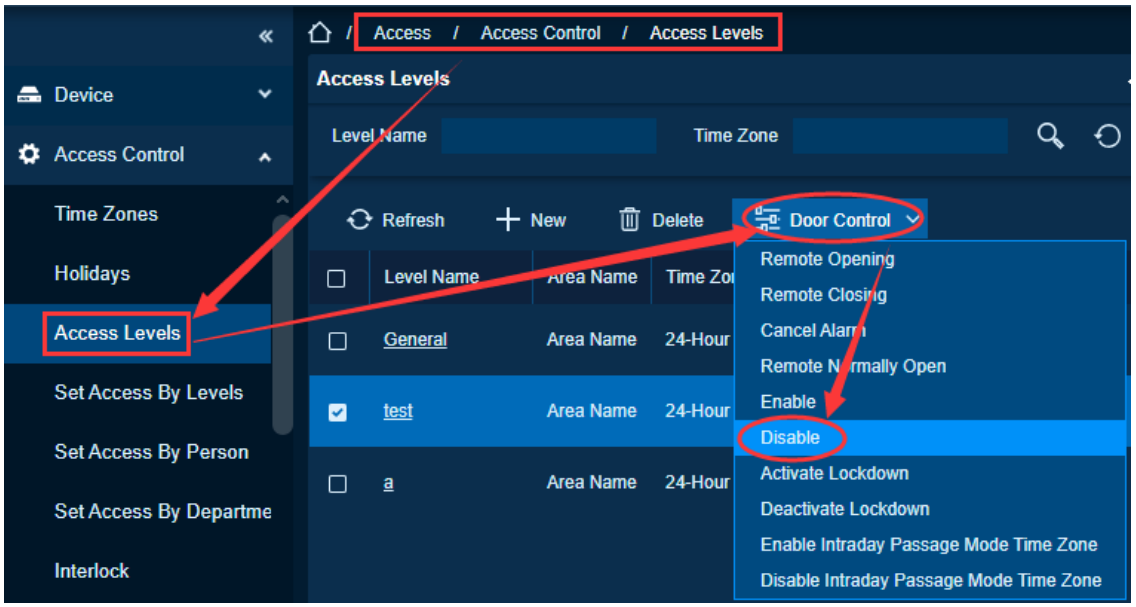
Feature Trigger Result

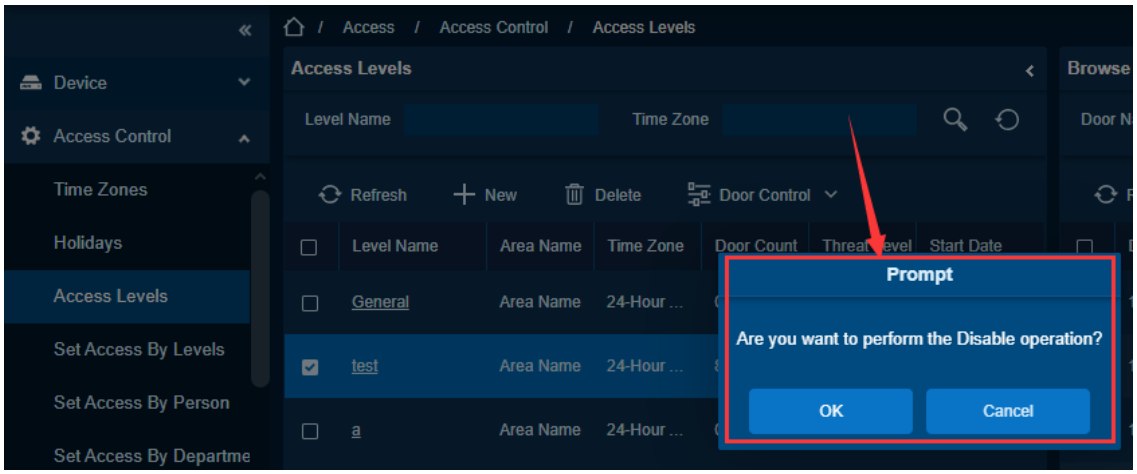
Disable all doors in the access levels in batches.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.

- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control]>[Disable]** and enter the user login password to trigger the disabling of the door.





Door Control – Activate Lockdown

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

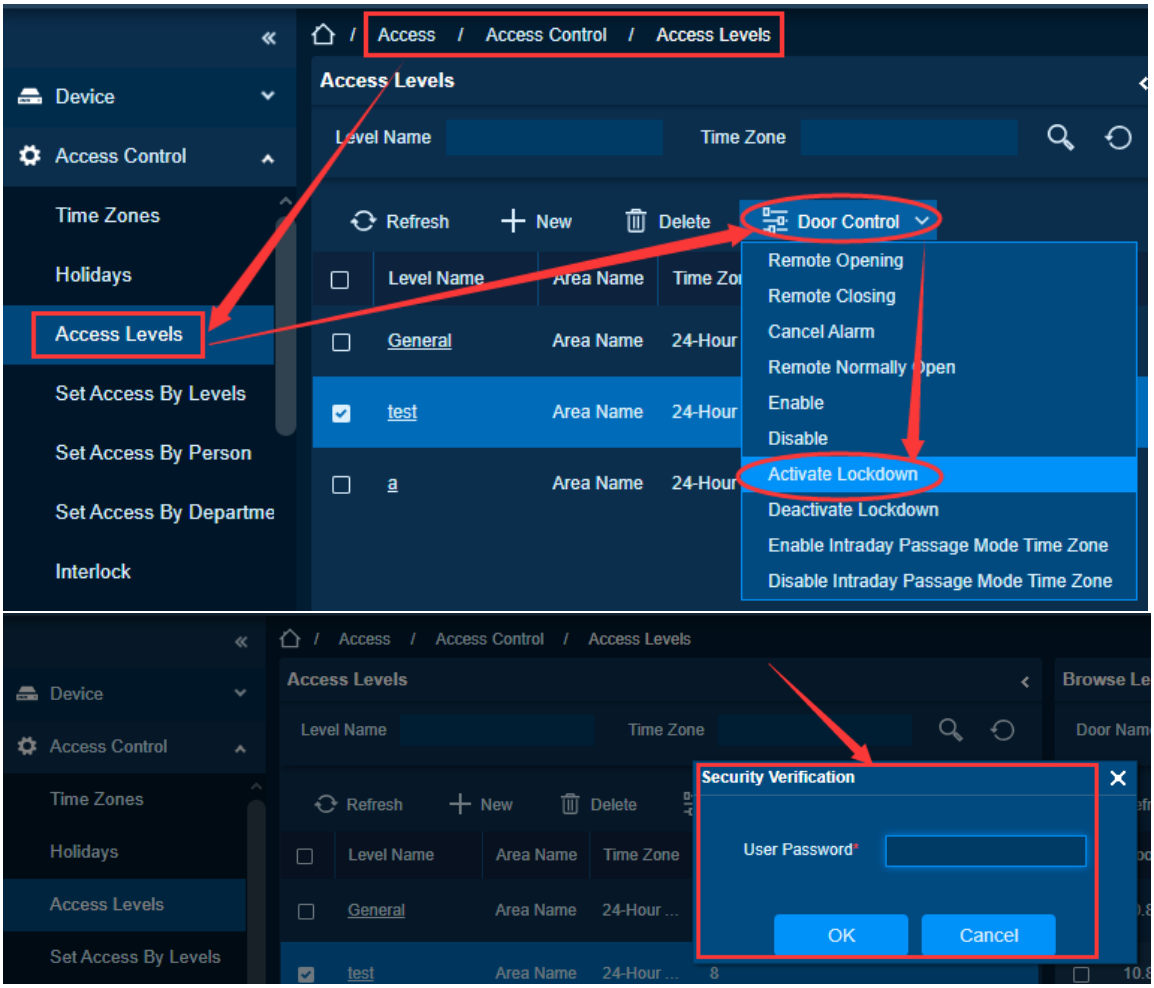
Batch remotes lock each door of the access levels.

Feature Trigger Result

Batch remote lock all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control] > [Activate Lockdown]** and enter the user login password to trigger the door lock.



Door Control – Deactivate Lockdown

Preconditions for Normal Use of Function

Log into the system with the current account and have the meu authority.

Function Usage Scenarios

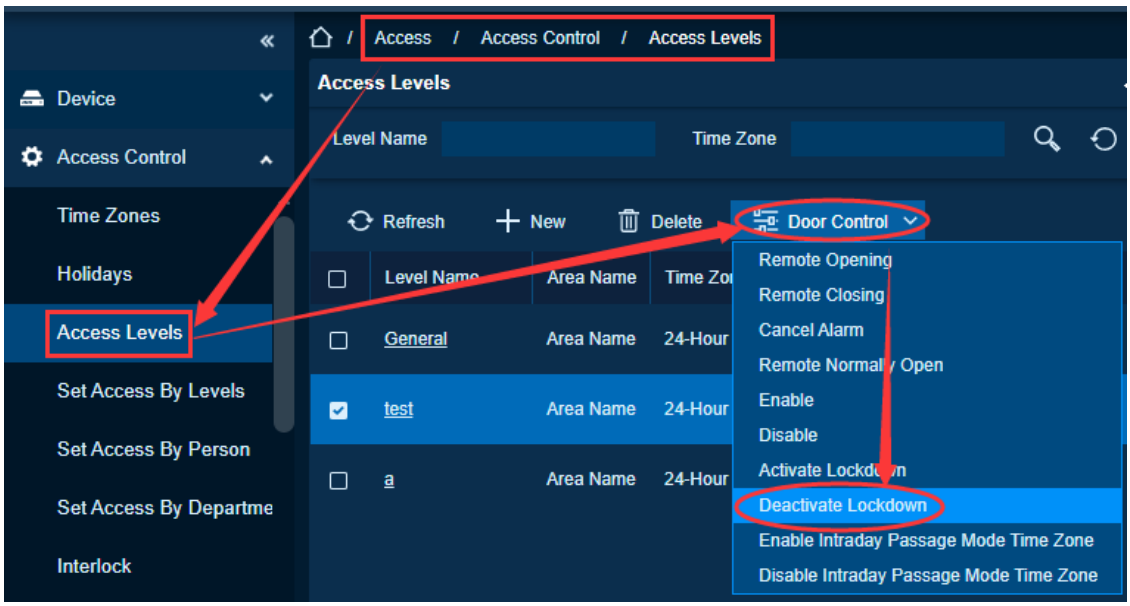
Remotely unlock the doors of the access control group in batches.

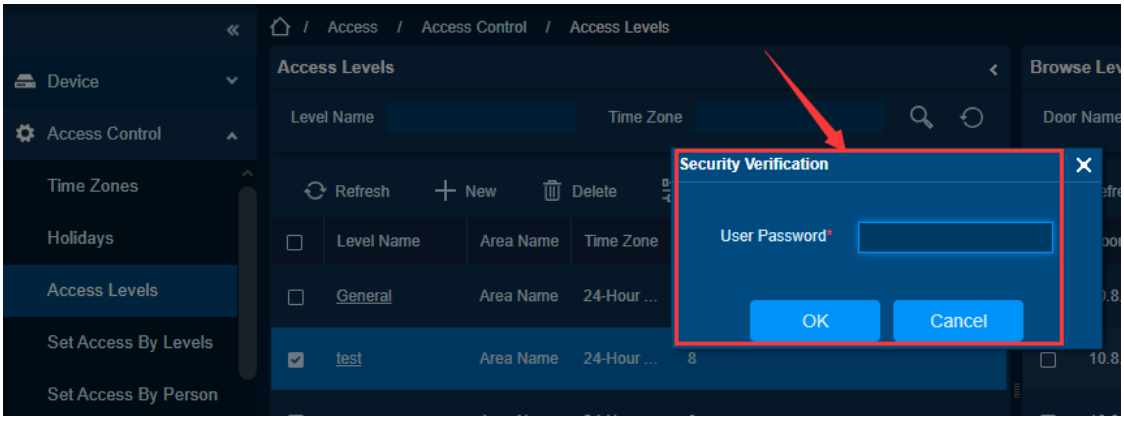
Feature Trigger Result

Batch remotes unlock all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels.
- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control]> [Deactivate Lockdown]** and enter the user login password to trigger the unlocking of the door.





Door Control - Enable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority

Function Usage Scenarios

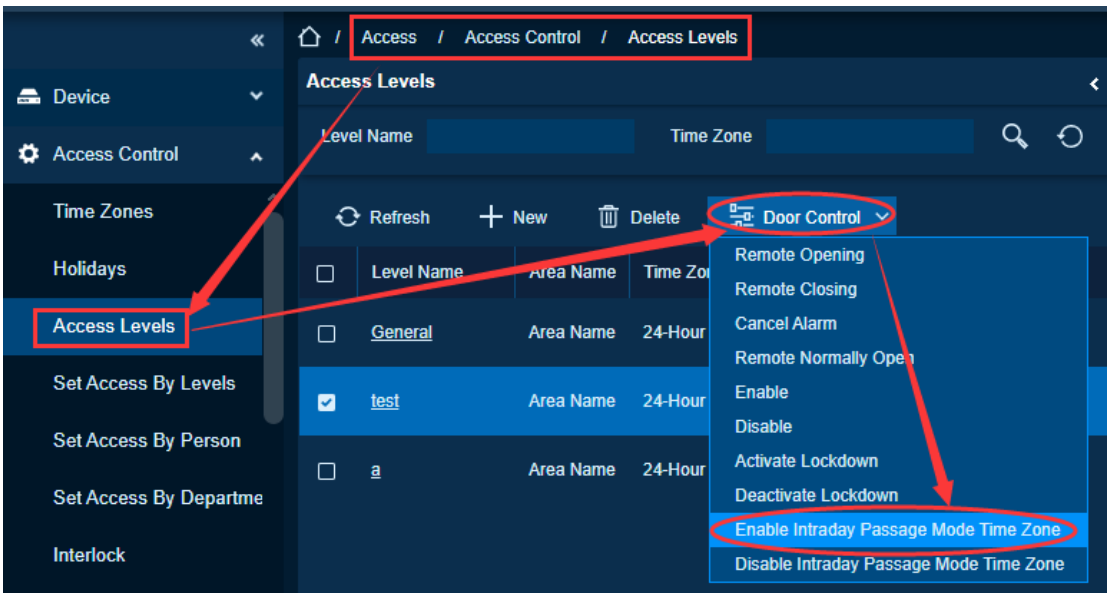
Batch enable the normally open time zone of each door of the access levels.

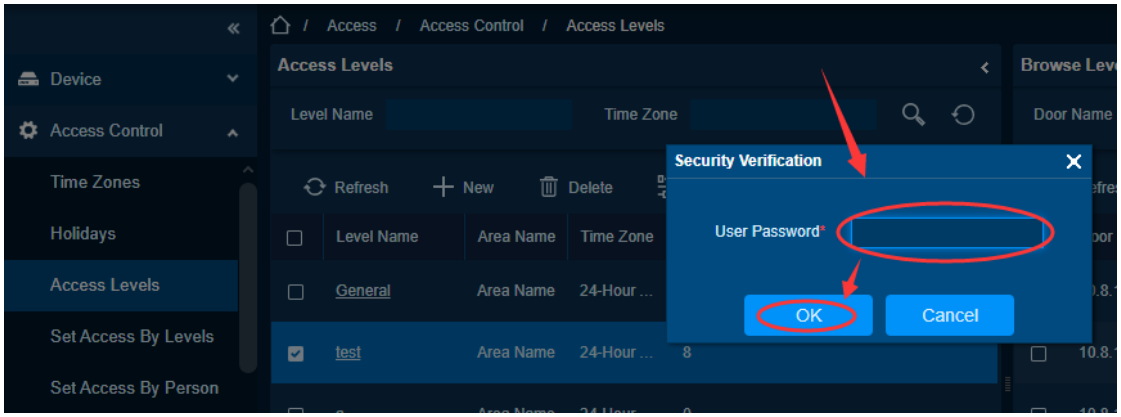
Feature Trigger Result

Batch enable the Normally Open Time Zone for all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding access levels, click **[Access] > [Access Control] > [Access Levels]> [Door Control]> [Enable Intraday Passage Mode Time Zone]** and enter the user login password to trigger the activation of the door time zone.





Door Control - Disable Intraday Passage Mode Time Zone

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

Function Usage Scenarios

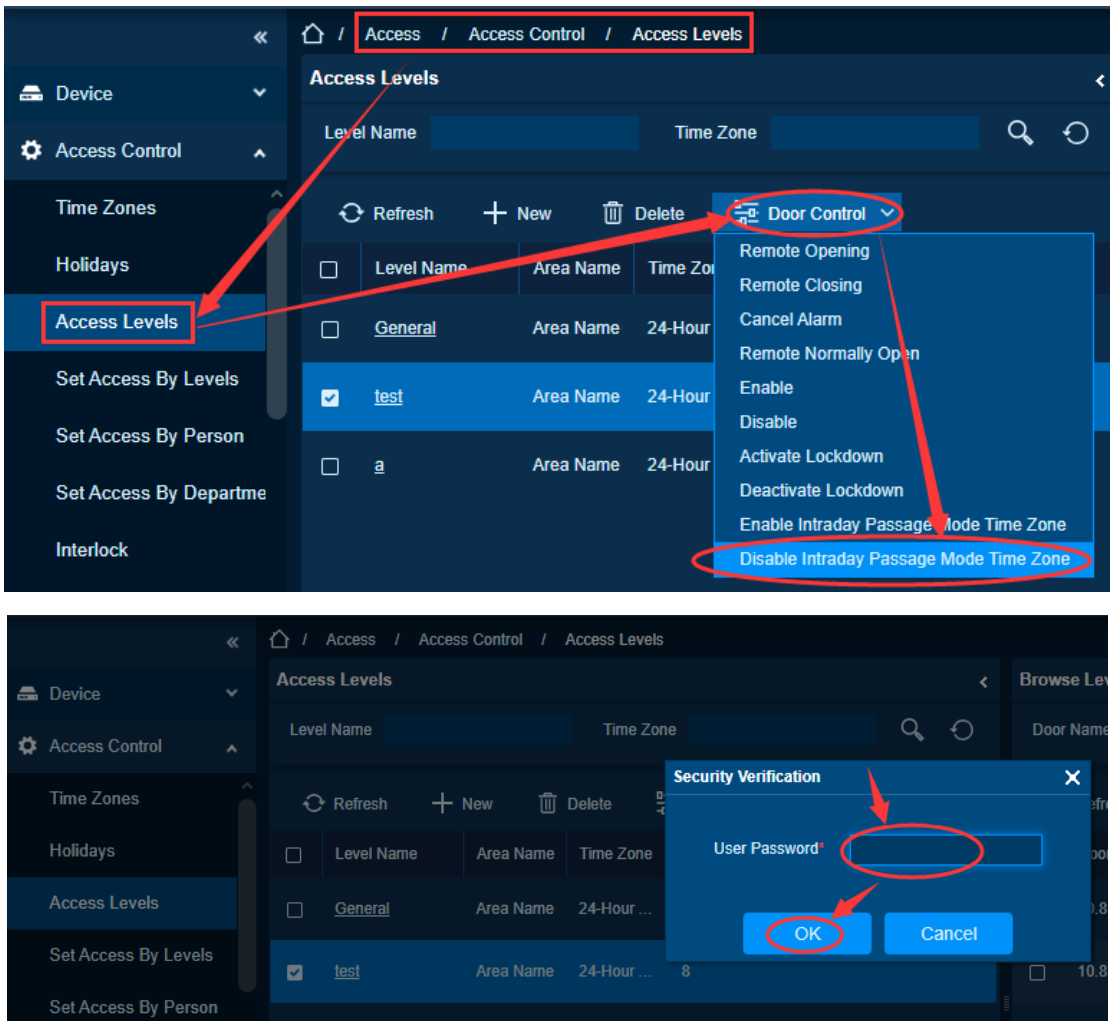
Disable the normally open time zone of each door of the access control access levels in batch.

Feature Trigger Result

Disable the normally open time zone in batches for all doors under the access levels.

Steps:

- Click **[Access] > [Access Control] > [Access Levels]** to display the access levels interface.
- Select the corresponding permission group, click **[Access] > [Access Control] > [Access Levels]> [Door Control]> [Disable Intraday Passage Mode Time Zone]** and enter the user login password to trigger the disablement of the door time zone.



6.2.4. Set Access by Levels

Function Description

According to the access levels, in the way of different authority groups, you can add or delete the personnel in the authority group.

Add Personnel

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

There are already set access levels for selection.

Function Usage Scenarios

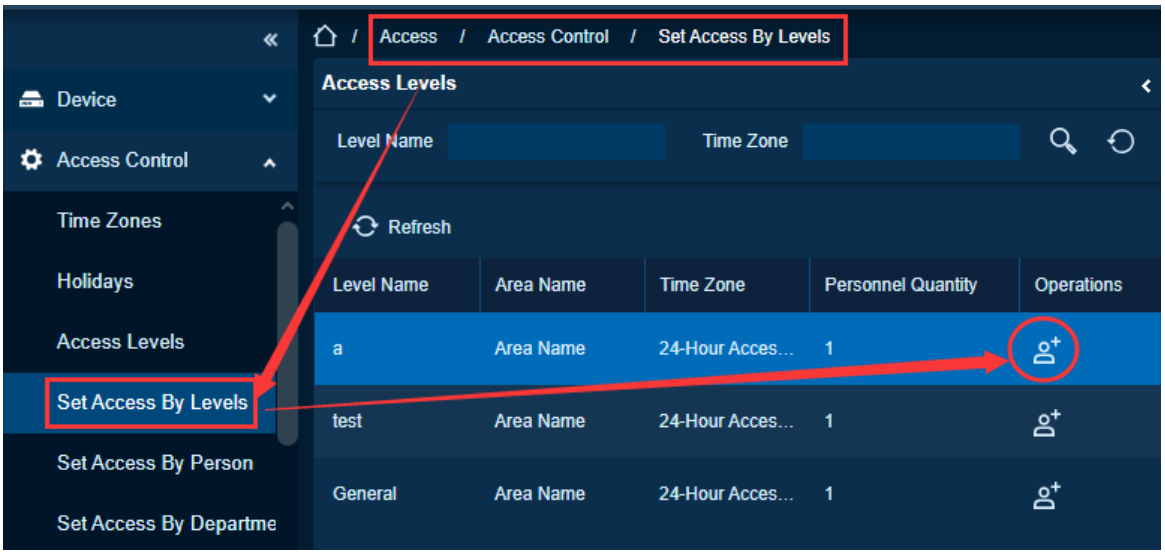
You need to add people to the corresponding door for management according to the corresponding access levels.

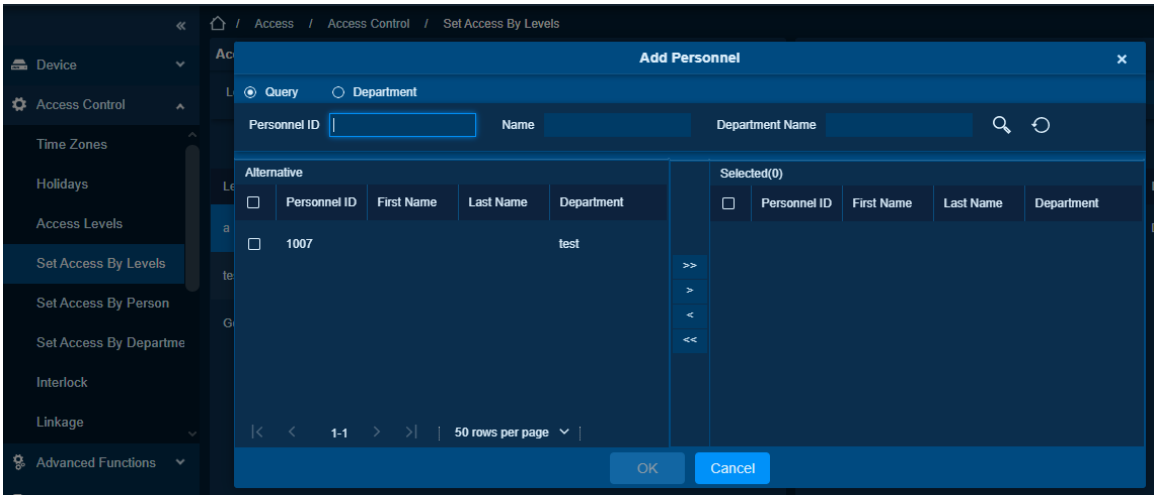
Feature Trigger Result

Add people to the corresponding access control access levels.

Steps:

- Click **[Access Control]** > **[Access Levels]** > **[Set Access by Levels]** to enter the edit interface, then click an Access level in the list on the left, personnel having right of opening doors in this access level will be displayed in list on the right.
- In the left list, click **[Add Personnel]** under Operations to pop up the Add Personnel box; select personnel (multiple) and click > to move to the selected list on the right, then click **[OK]** to save and exit.





Delete Personnel

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

There are already set access levels for selection, and the number of personnel is greater than 0.

Function Usage Scenarios

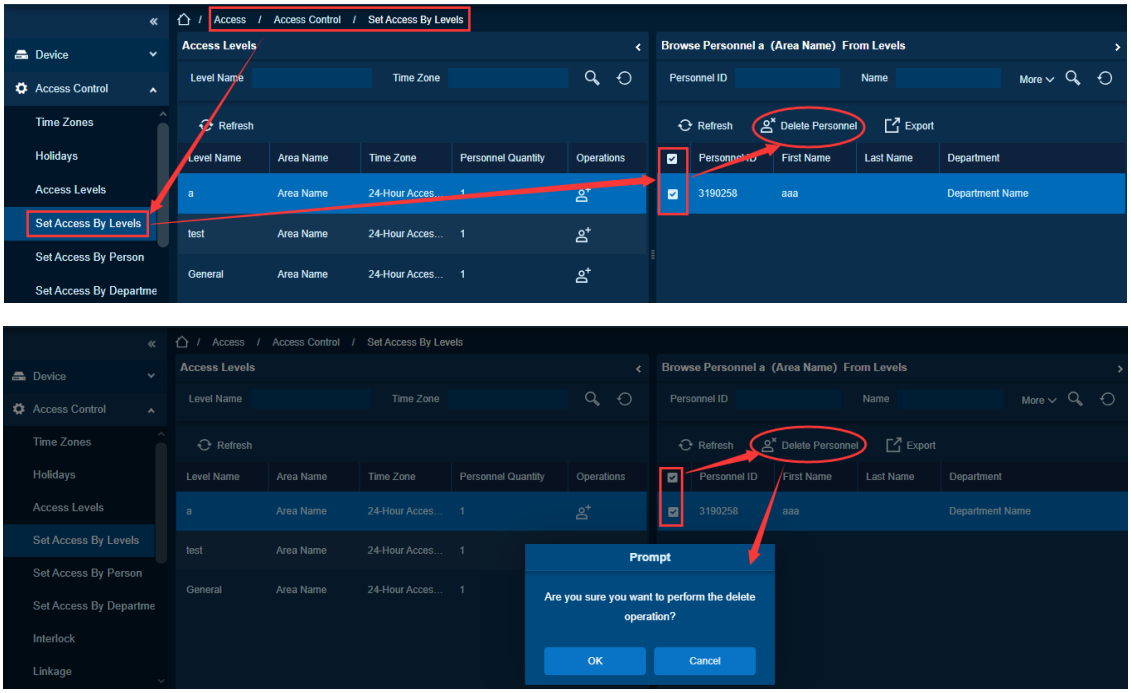
The people who have been added to the corresponding access level need to adjust the access level group or do not need to be in that level.

Feature Trigger Result

Delete the person from the corresponding access levels.

Steps:

Click the level to view the personnel in the list on the right. Select Personnel and click **[Delete Personnel]** above the list on the right, then click **[OK]** to delete.



6.2.5. Set Access by Person

Function Description

According to the access levels, in the way of different authority groups, you can add or delete the personnel in the authority group.

Add Access Level to person's access levels

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

There are already set access levels for selection.

Function Usage Scenarios

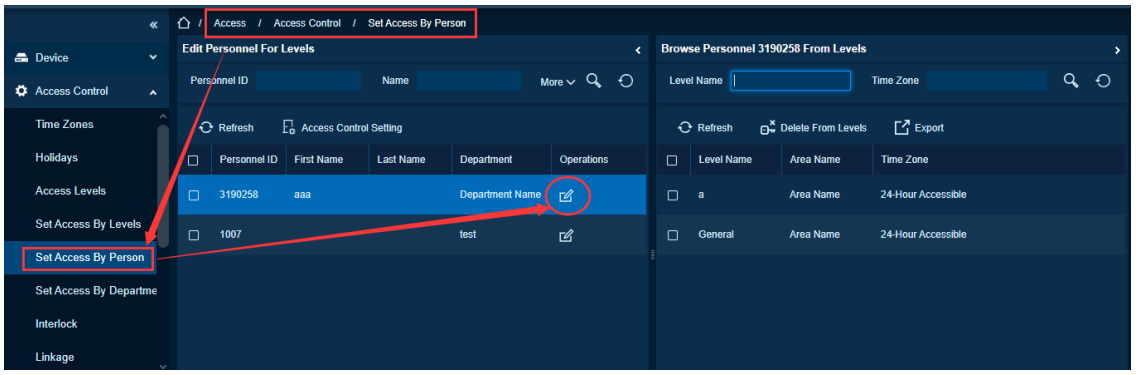
Personnel need to have access control permissions in multiple access levels.

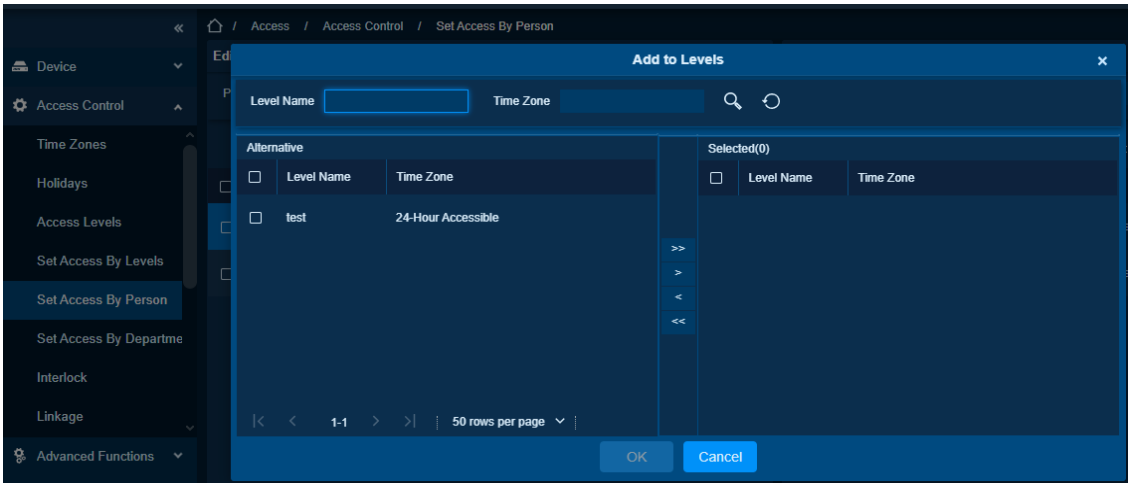
Feature Trigger Result

Personnel have multiple access control permissions.

Steps:

- Click **[Access Control] > [Access Control] > [Set Access by Person],** click Employee to view the levels in the list on the right.
- Click **[Add to Levels]** under Related Operations to pop up the Add to Levels box, select Level (multiple), and click > to move it to the selected list on the right; then click **[OK]** to save.





Delete access level from person's access levels

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

There are already set access levels for selection.

Function Usage Scenarios

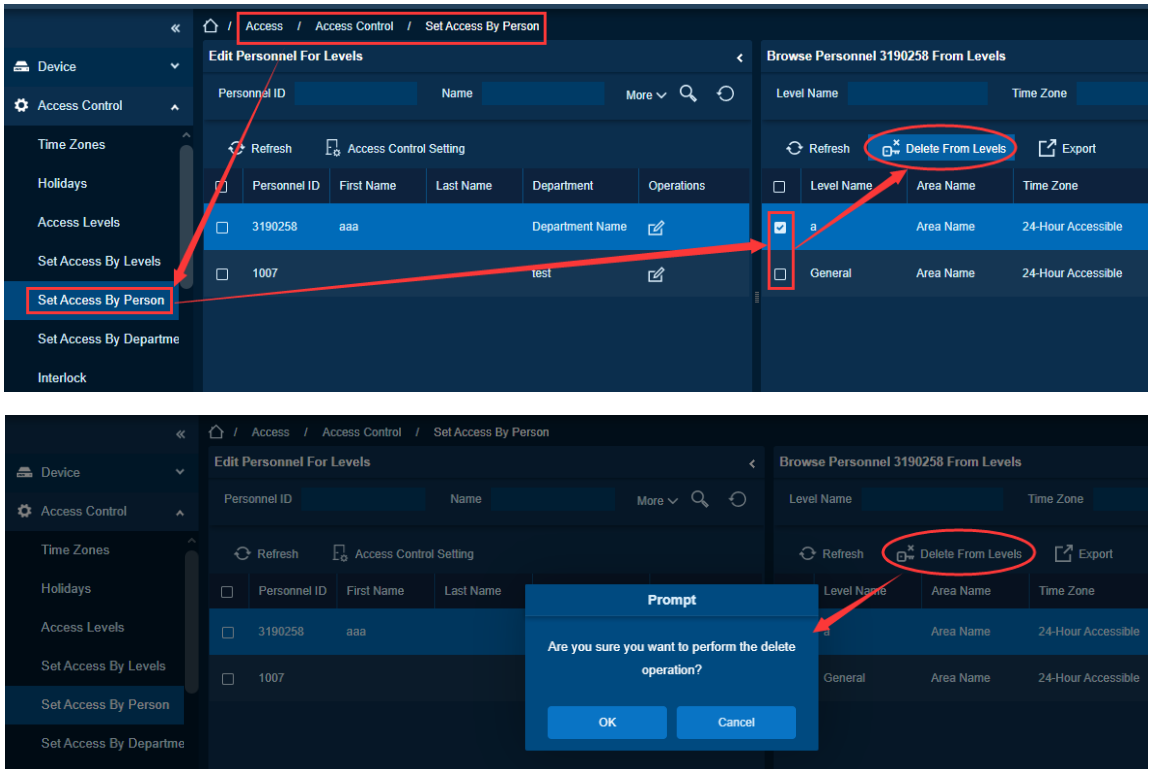
Personnel need to delete access control permissions in a certain access level.

Feature Trigger Result

Personnel delete the access control authority.

Steps:

- Select Level (multiple) in the right list and click **[Delete from levels]** above the list, then click **[OK]** to delete the selected levels.



Access Control Settings

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

There are already set access levels for selection.

Function Usage Scenarios

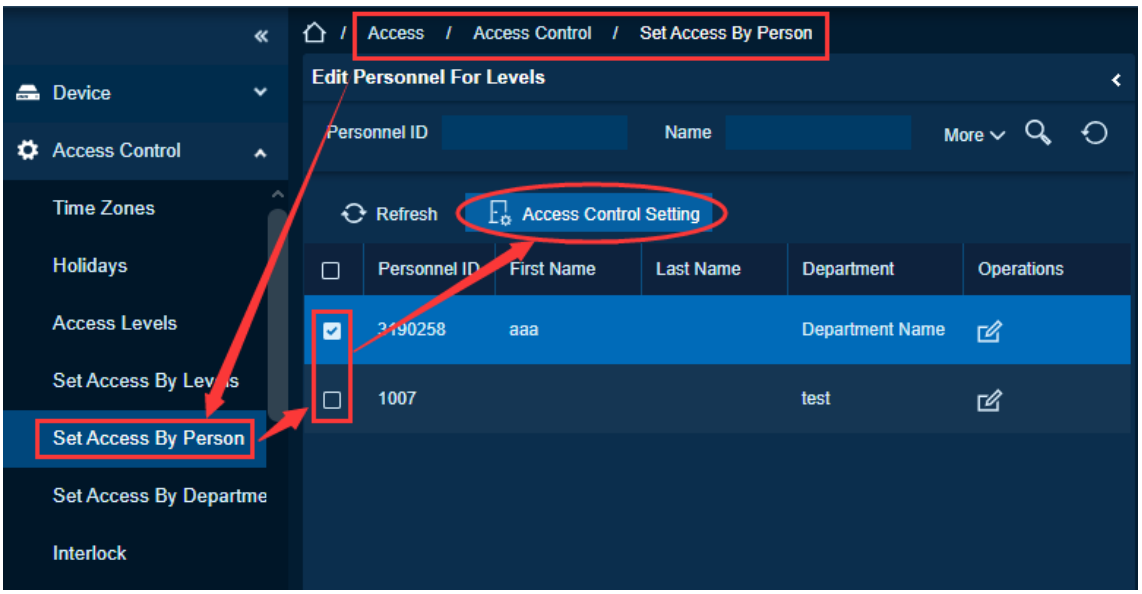
It is necessary to set whether the person is a super user, and the access control configuration such as operation authority.

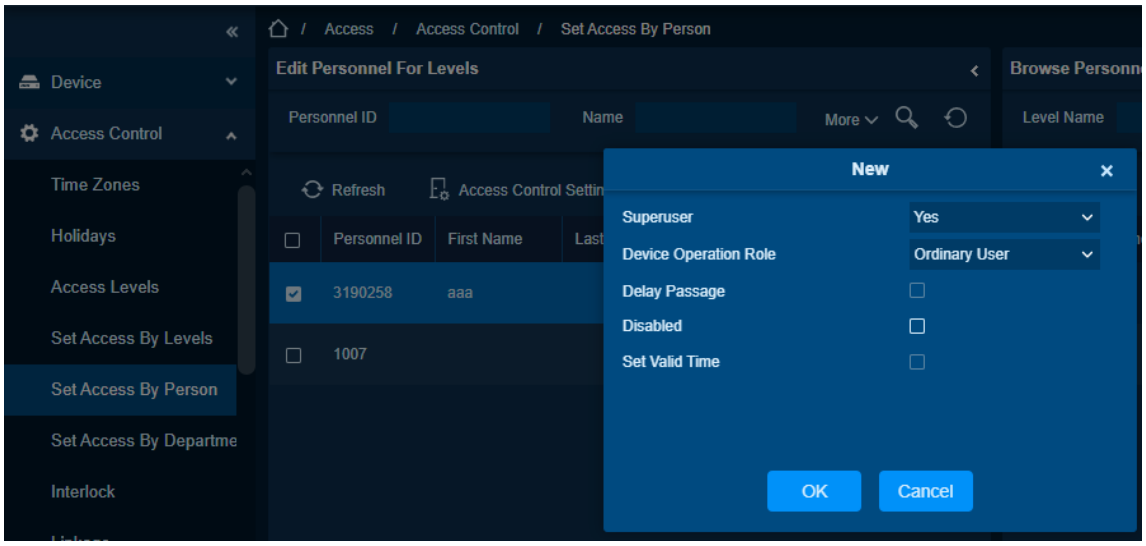
Feature Trigger Result

You can set whether the person is a super user, operation authority, whether to extend the pass time, whether to be a banned list, and whether to set a valid time.

Steps:

- Select a person in the list on the left and click **[Access Control Setting].**
- Set access control parameters and then click **[OK]** to save the settings.





Superuser: In access controller device, a superuser is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door-opening priority.

Device Operation Role: Set user permission for standalone terminal, can select Ordinary User/ Administrator/ Enroller

Delay Passage: Extend the waiting time for the personnel through the access points. Suitable for physically challenged or people with other disabilities.

Disabled: When person is disable, this person will not allow to verify on the system.

Set Valid Time: Set temporary access level. If not set, it indicates person get permanent access.

6.2.6. Set Access by Department

Function Description

Add the selected department to the selected access levels or delete the selected department from the access levels. The access of the staff in the department will be changed.

Add to Default Levels

Preconditions for Normal Use of Function

Log in to the system with the current account and have this menu authority.

There are already set access levels for selection.

Function Usage Scenarios

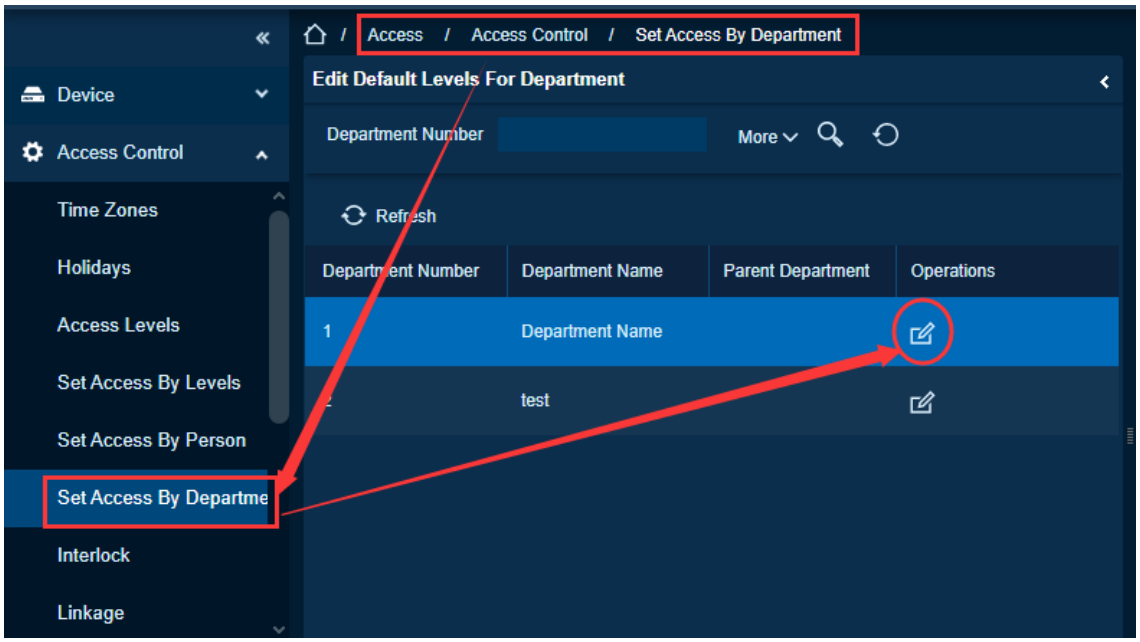
The department needs to have access control permissions in multiple access levels.

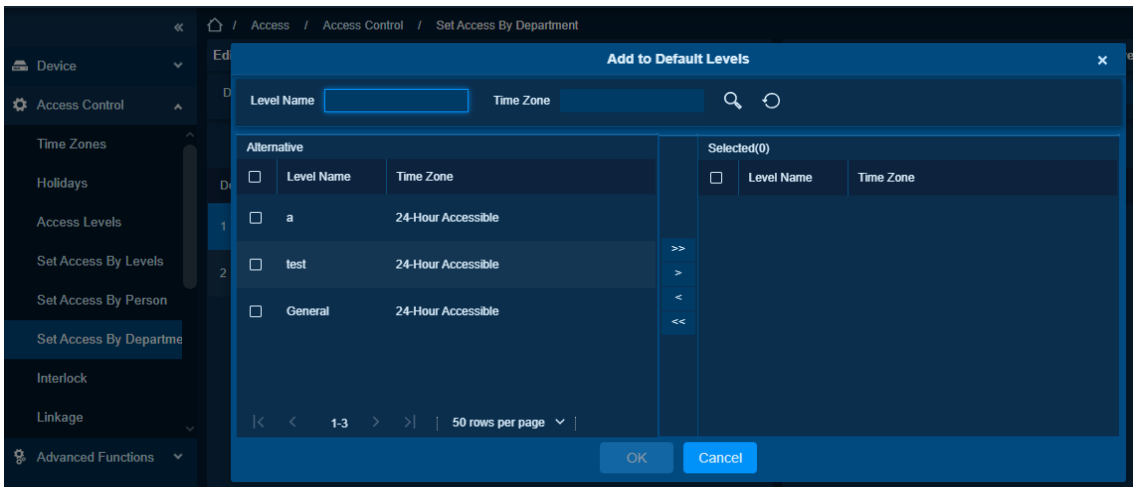
Feature Trigger Result

Department has multiple access control permissions.

Steps:

- Click **[Access] > [Access Control] > [Set Access by Department]** to display the department setting access level interface.
- Select the corresponding Access, click **[Add Default Levels]**, a window for adding access levels pops up, select the access level to be added, click > to move to the right, and click **OK.**





Delete the Default Levels

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The access level has been set up for the department for selection.

Function Usage Scenarios

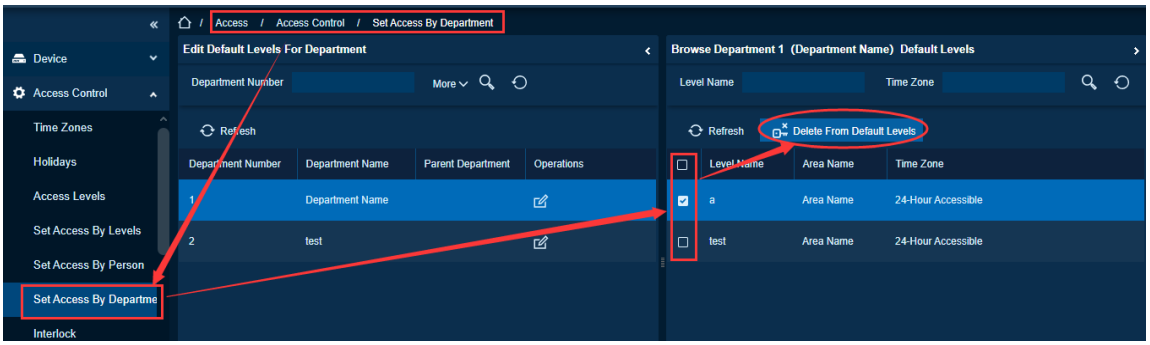
The department needs to delete the access control permission in multiple access levels.

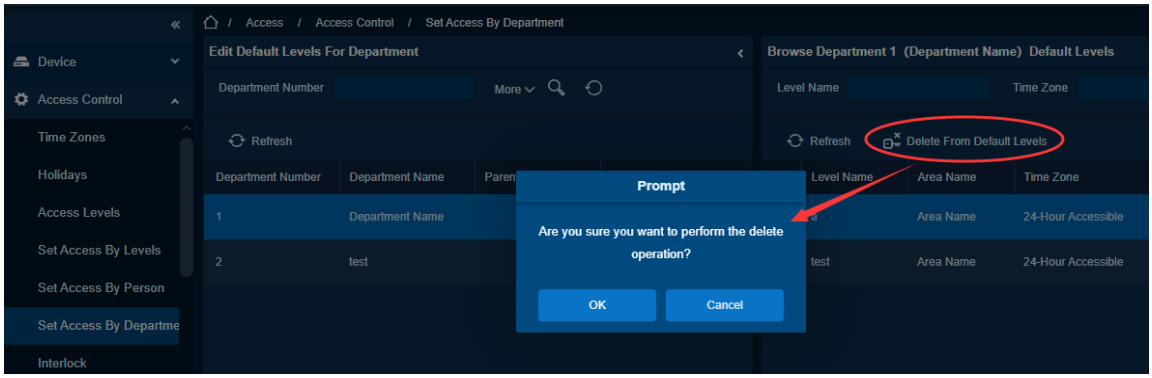
Feature Trigger Result

Delete default access levels for target department .

Steps:

- Click **[Access]** > **[Access control]** > **[Set Access by Department]** to display the department setting access level interface.
- Select the corresponding access levels in the right column and click **[Delete from Default Levels].**





6.2.7. Interlock

Function Description

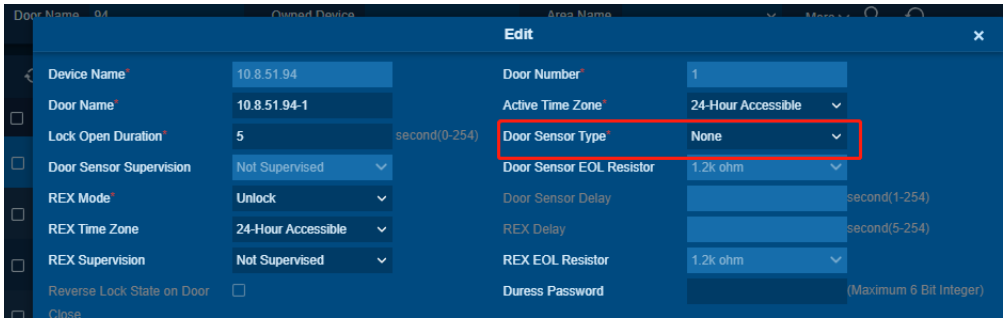
Interlock can be set for two or more locks belonging to one access controller. When one door is opened, the others will be closed, or you cannot open the door.

Add Interlock

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

Before setting the interlock, please check [Access]->[Device]->[Door], edit target doors, check **Door Sensor Type** where must select Normally Open/ Normally Close .



Function Usage Scenarios

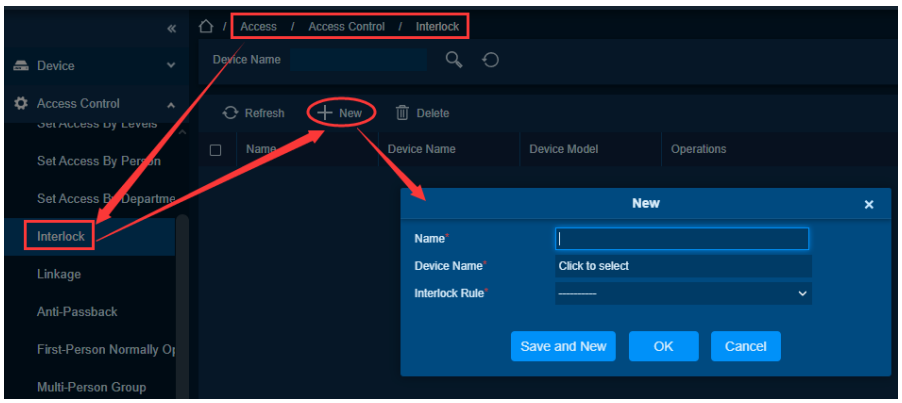
Places with higher security levels require access control.

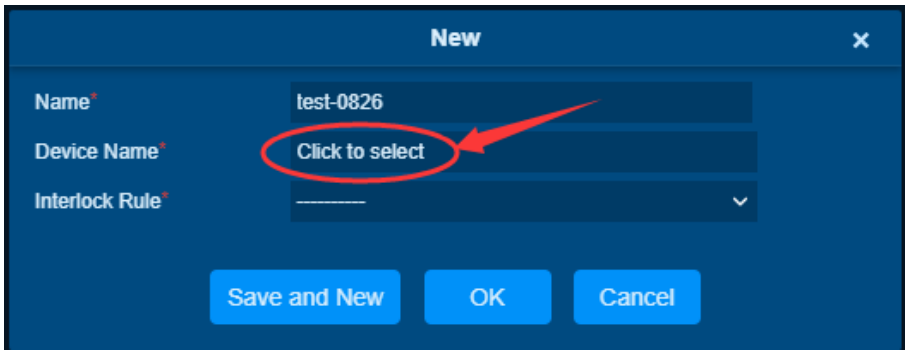
Feature Trigger Result

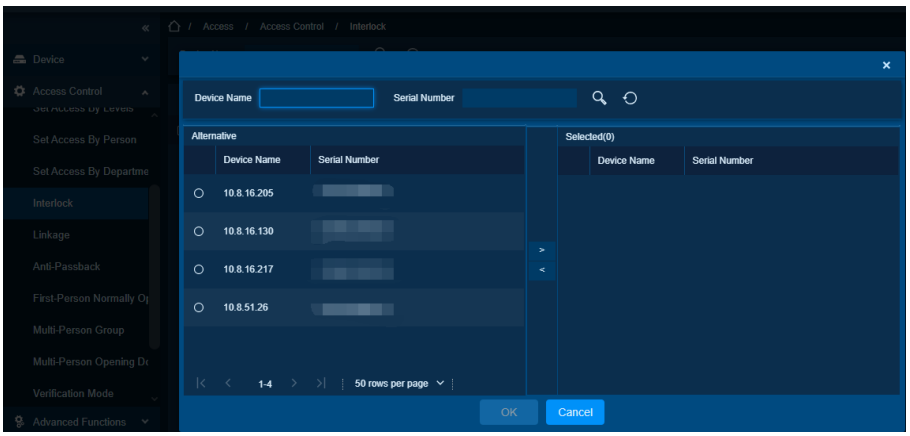
The interlock is added successfully, the door is controlled according to the set interlock state.

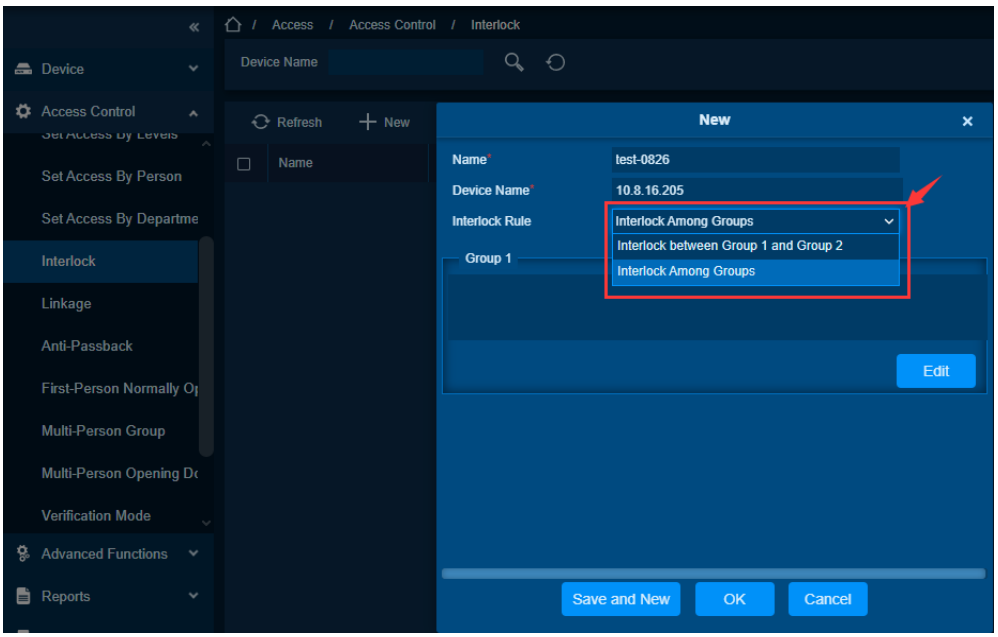
Steps:

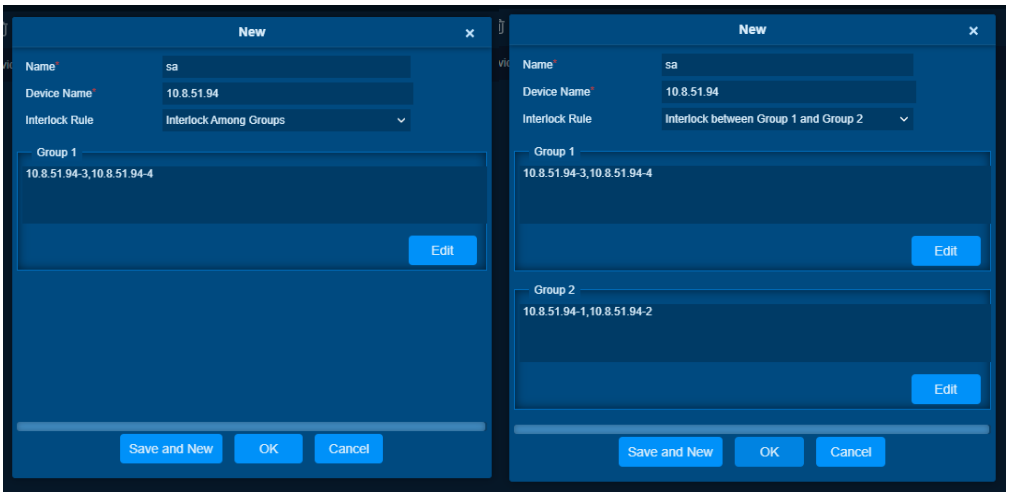
- Click **[Access Control] > [Interlock] > [New]** to enter the edit interface:
- Click **Device Name** to select target device
- Select Interlock Rule, tick an item, then click **[OK]** to complete. The new added interlock settings will be shown in the list.











Interlock Rule: Interlock between Group 1 and Group 2/Interlock Among Groups

Example:

Rule	Interlock between Group 1 and Group 2	Interlock Among Group
Group	Group 1: Door 1, Door 2 Group 2: Door 3, Door 4	Group: Door 1, Door 2, Door 3, Door 4
Door 1 Verify	Check Door 3 and Door 4 door sensor status	Check Door 2, Door 3, and Door 4 door sensor status
Door 2 Verify	Check Door 3 and Door 4 door sensor status	Check Door 1, Door 3, and Door 4 door sensor status

Door 3 Verify	Check Door 1 and Door 2 door sensor status	Check Door 1, Door 2, and Door 4 door sensor status
Door 4 Verify	Check Door 1 and Door 2 door sensor status	Check Door 1, Door 2, and Door 3 door sensor status

Edit Interlock

Preconditions for Normal Use of Function

Log in to the system with the current account and have this menu authority.

Before setting the interlock, please check [Access]->[Device]->[Door], edit target doors, check **Door Sensor Type** where must select Normally Open/ Normally Close .

Function Usage Scenarios

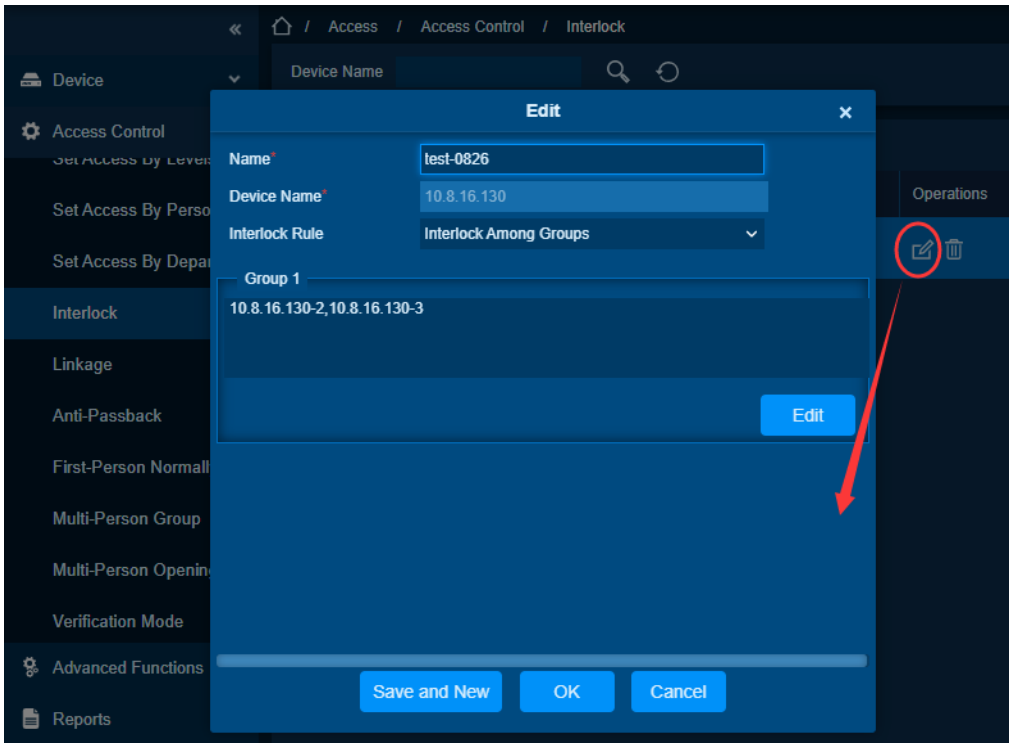
For places with a higher security level, the previously set access control needs to be modified.

Feature Trigger Result

The interlock is successfully modified, and the door is controlled according to the set interlock state.

Steps:

- Click **[Access]** > **[Access Control]** > **[Interlock]** to display the interlock interface.
- Select the device name and click **[Edit]** to modify the interlocking rules.



Delete Interlock

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Before setting the interlock, please check [Access]->[Device]->[Door], edit target doors, check **Door Sensor Type** where must select Normally Open/ Normally Close .

Function Usage Scenarios

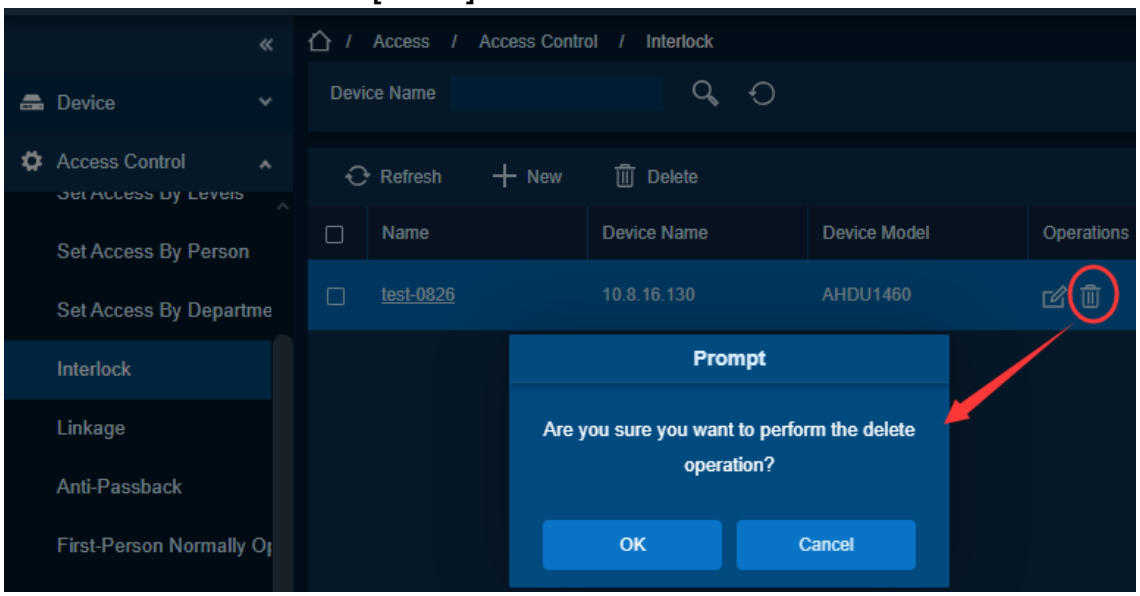
The area does not need to be interlocked, or the door does not need to be interlocked control.

Feature Trigger Result

Successfully deleted interlock.

Steps:

- Click **[Access]** > **[Access Control]** > **[Interlock]** to display the interlock interface.
- Select the device name and click **[Delete]** to delete the interlock rule.



6.2.8. Linkage

Function Description

Linkage setting means when an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control events such as verification, opening, alarm and abnormal of system, and list them in the corresponding monitoring view.

Add Linkage

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

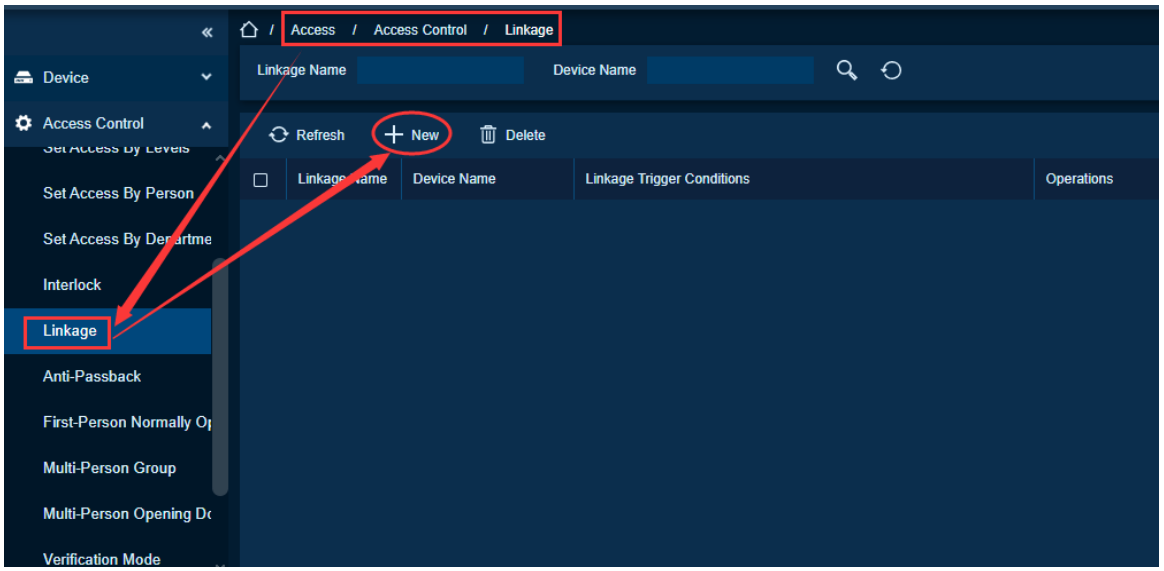
Function Usage Scenarios

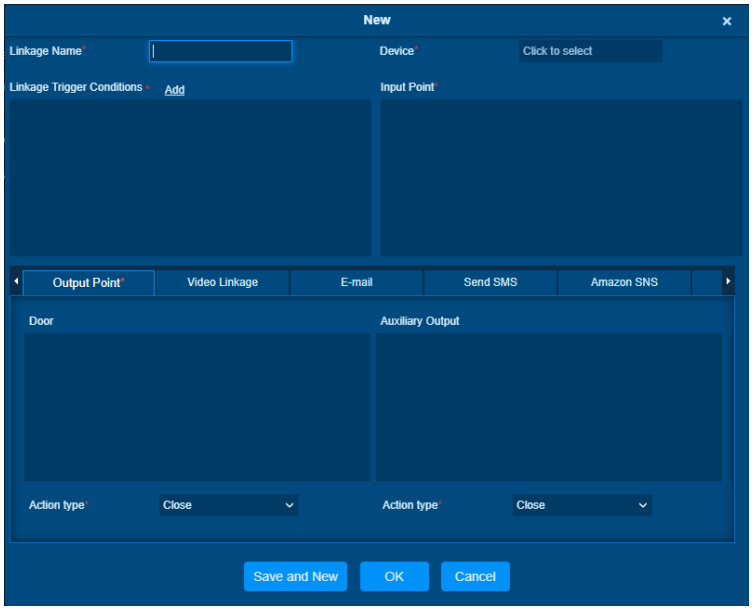
Trigger by device/door/reader/aux in… event to trigger open door/send SMS/ send Email…

Feature Trigger Result

According to the newly added Linkage Event, when an input point triggers the event, a linkage action will be generated at the specified Output Point to control the door event in the system and display it in the corresponding event list for monitoring.

Steps:





- Click **[Access Control] > [Linkage] > [New].**
- Enter the linkage name
- Select a target Device

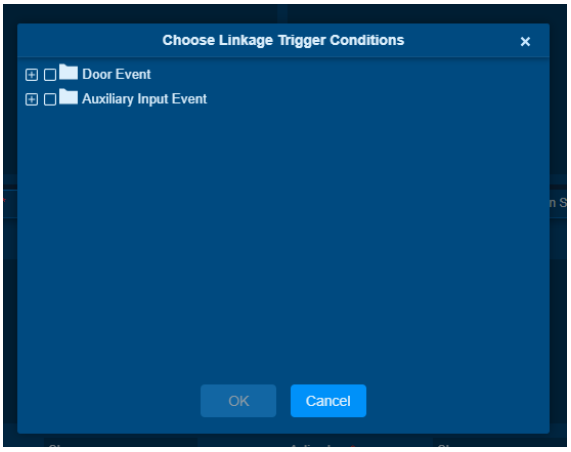
Note:

After selecting devices, corresponding linkage settings will be displayed. The system will first judge whether the device is successfully connected and has read extended parameters. If there are no available extended parameters, the system cannot set any linkage. If there is an available extended

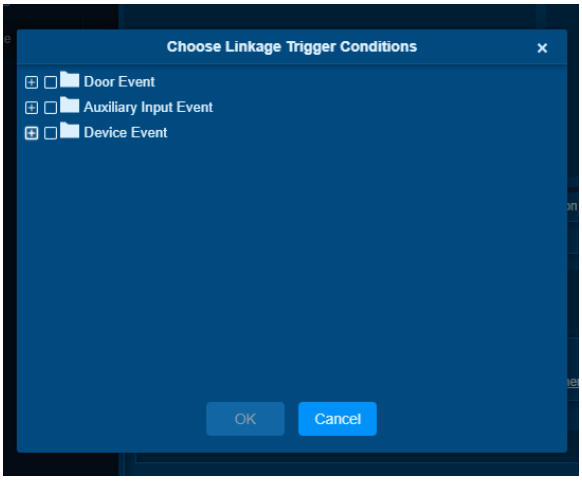
parameter(s), the system will show linkage settings according to the Door Quantity, Auxiliary Input and Output Quantity of currently selected device.

- Select Linkage Trigger Conditions

OmniAC Series

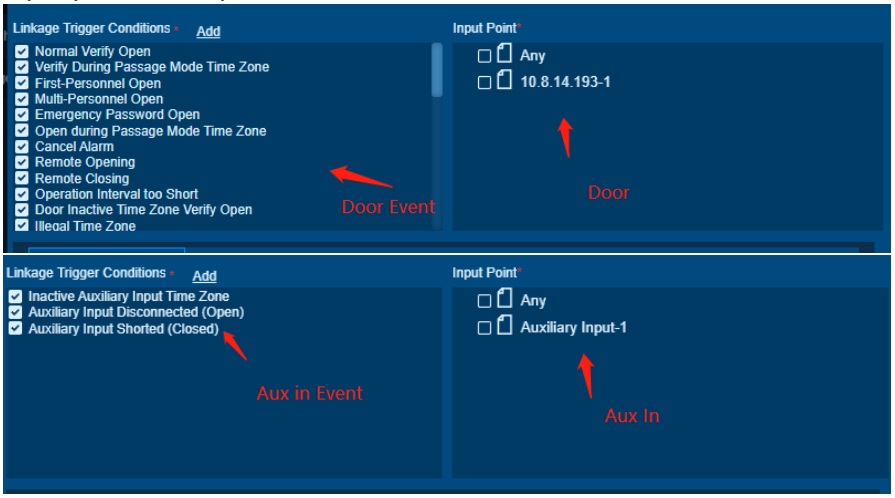


Horizon Series

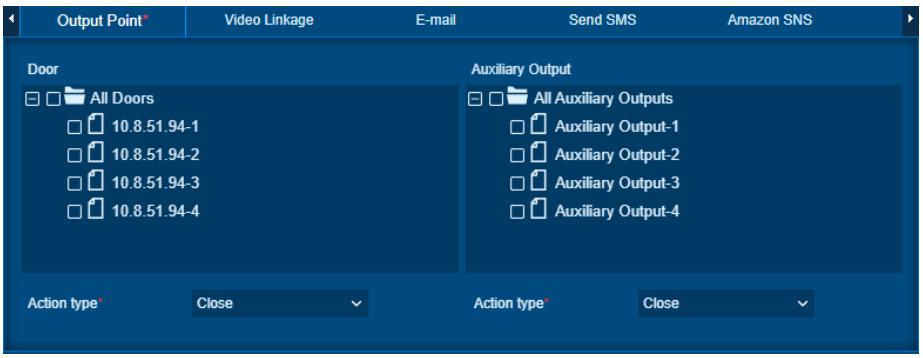


- Select Input Point

Input point will depend on the condition to filter Device/Door/Aux in

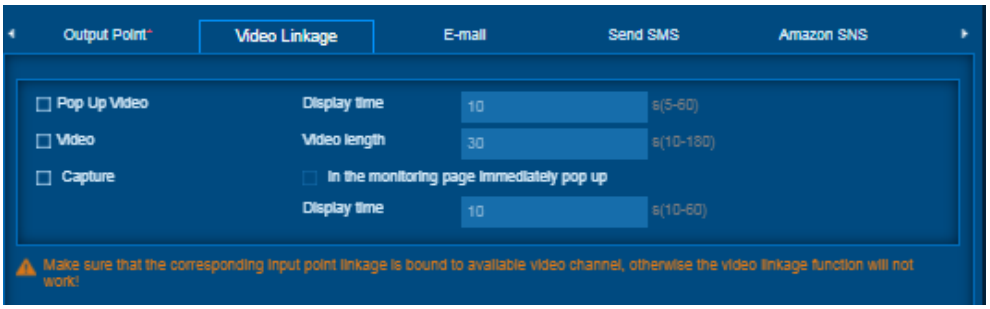


- Set Output Point for door/aux out operation



Select target door/aux out
Door Action: Close/Open/Normally Open/Lock/Unlock
Auxiliary Output Action: Close/Open/Normally Open

- Set Video Linkage

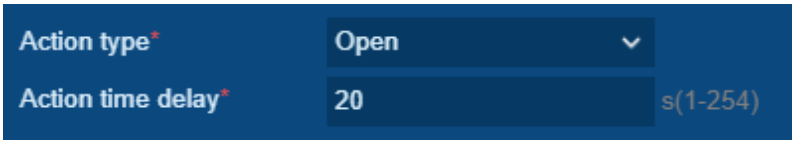


Pop Up Video: Whether to set the pop-up preview page in real-time monitoring and set the pop-long.

Video: Enable or disable background video recording and set the duration of background video recording.

Capture: Enable or disable background snapshots.

Delay: Ranges from 1 to 254 second (This item is valid when Action type is Open).



After editing, click **[OK]** to save and quit, then the added linkage setting will be shown in the list.

For example, if users select Normal Punching Open Door as trigger condition, then the input point is Door 1, output point is Lock 1, action type is Open, delay is 60 second. When Normal Punching Open Door occurs at Door 1, the linkage action of Open will occur at Lock 1, and the door will be open for 60 second.

✍**Note:**

During editing, you cannot modify the device, but modify the linkage setting name and configuration. When delete a device, its linkage setting record, if any, will be deleted.

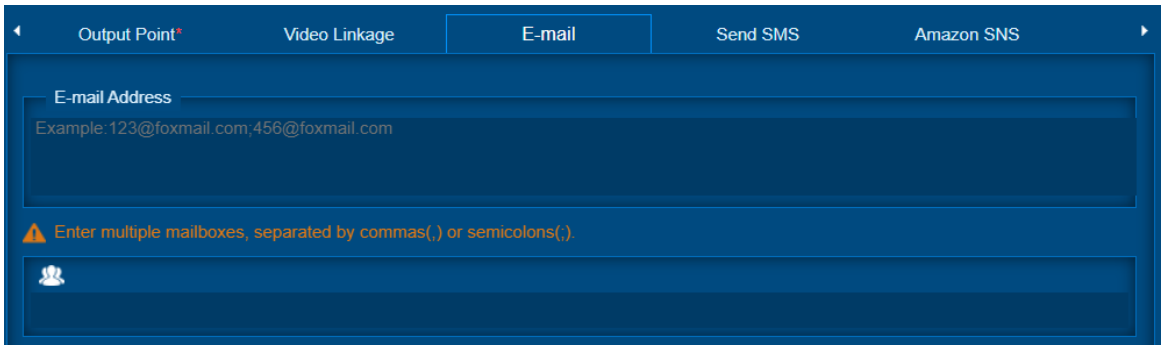
If the device and trigger conditions are the same, and system has linkage setting record where the Input Point is a specific door or Auxiliary Input, it will not allow users to add (or edit) a linkage setting record where the Input Point is any.

On the contrary, if the device and trigger conditions are the same, and the system has linkage setting record where the Input Point is 'Any', it will not permit user to add (or edit) a linkage setting record where the Input Point is a specific door or auxiliary input.

In addition, same linkage setting at Input Point and Output Point is not allowed. The same device permits consecutive logical linkage settings. The system allows to set several trigger conditions for a linkage setting at a time.

- Set Email Notification

The Email service should be set in the system module.

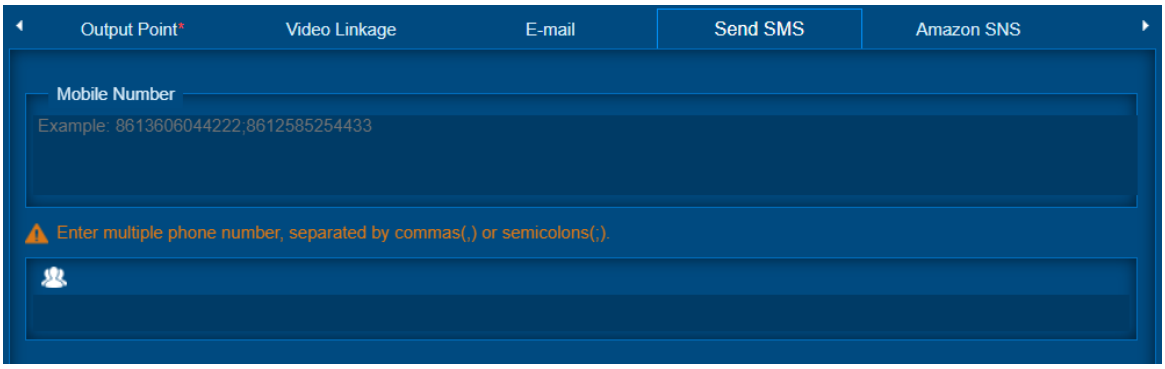


E-mail Address: When the linkage is triggered, the email address to receive the message notification.

Select Personnel: The selected personnel will be notified by e-mail (You need to set personnel e-mail information in the personnel module).

- Set SMS Notification

The SMS service should be set in the system module.

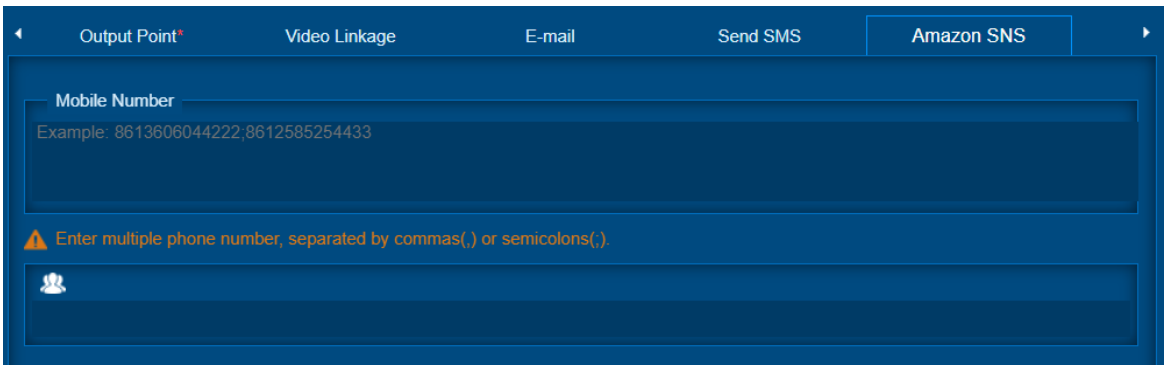


Mobile Phone Number: When the linkage is triggered, the phone number will receive a message notification.

Select Personnel: The selected personnel will be notified by short message. (You need to set personnel phone number information in the personnel module).

- Set Amazon SNS Notification

The Amazon SNS service should be set in the system module.

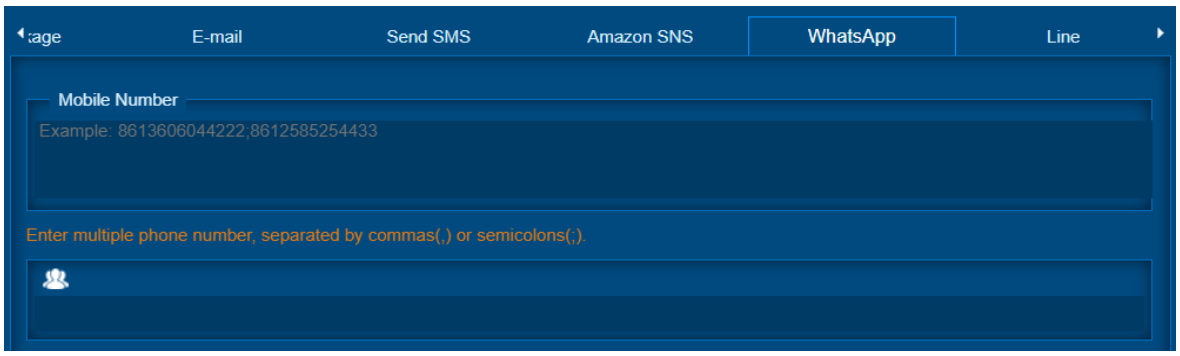


Mobile Phone Number: When the linkage is triggered, the phone number will receive a message notification.

Select Personnel: The selected personnel will be notified by short message. (You need to set personnel phone number information in the personnel module).

- Set WhatsApp Notification

The WhatsApp service should be set in the system module.

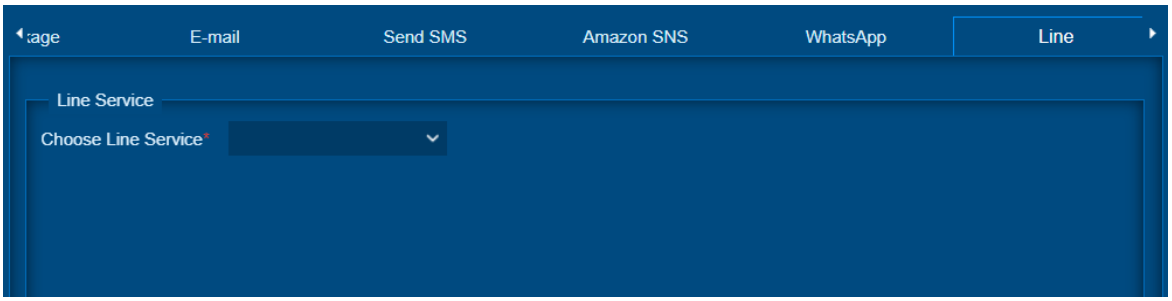


Mobile Phone Number: When the linkage is triggered, the WhatsApp application will receive a message notification.

Select Personnel: The selected personnel will be notified by WhatsApp application. (You need to set personnel phone number information in the personnel module).

- Set Line Notification

The Line service should be set in the system module.



Choose Line Service: When the linkage is triggered, the Line group will receive a message notification.

Edit Linkage

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

There is a linkage.

Function Usage Scenarios

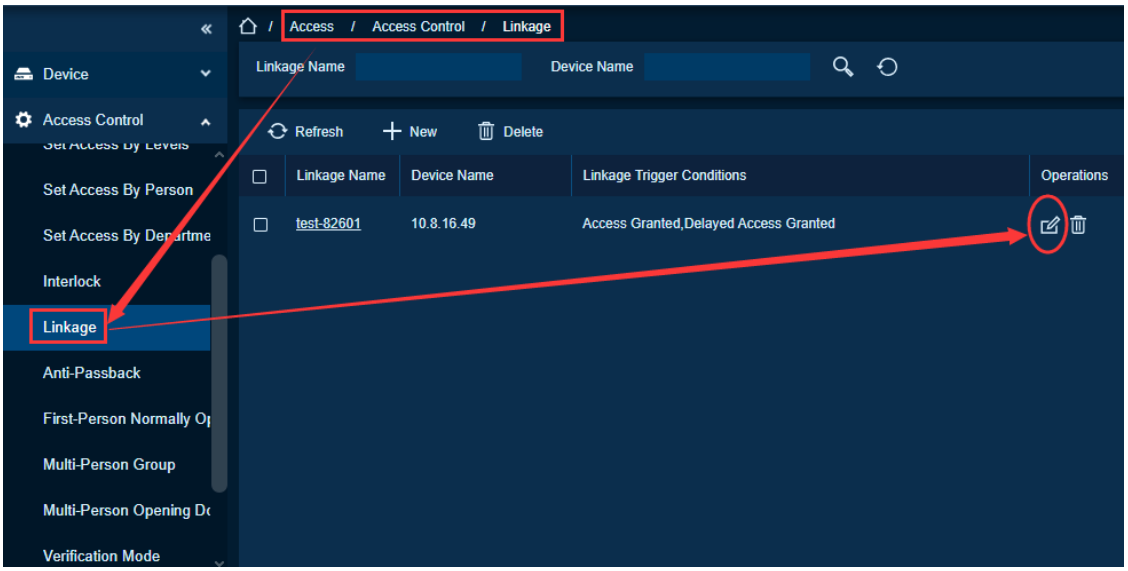
Need to modify the linkage action of the output port when the control input port is triggered.

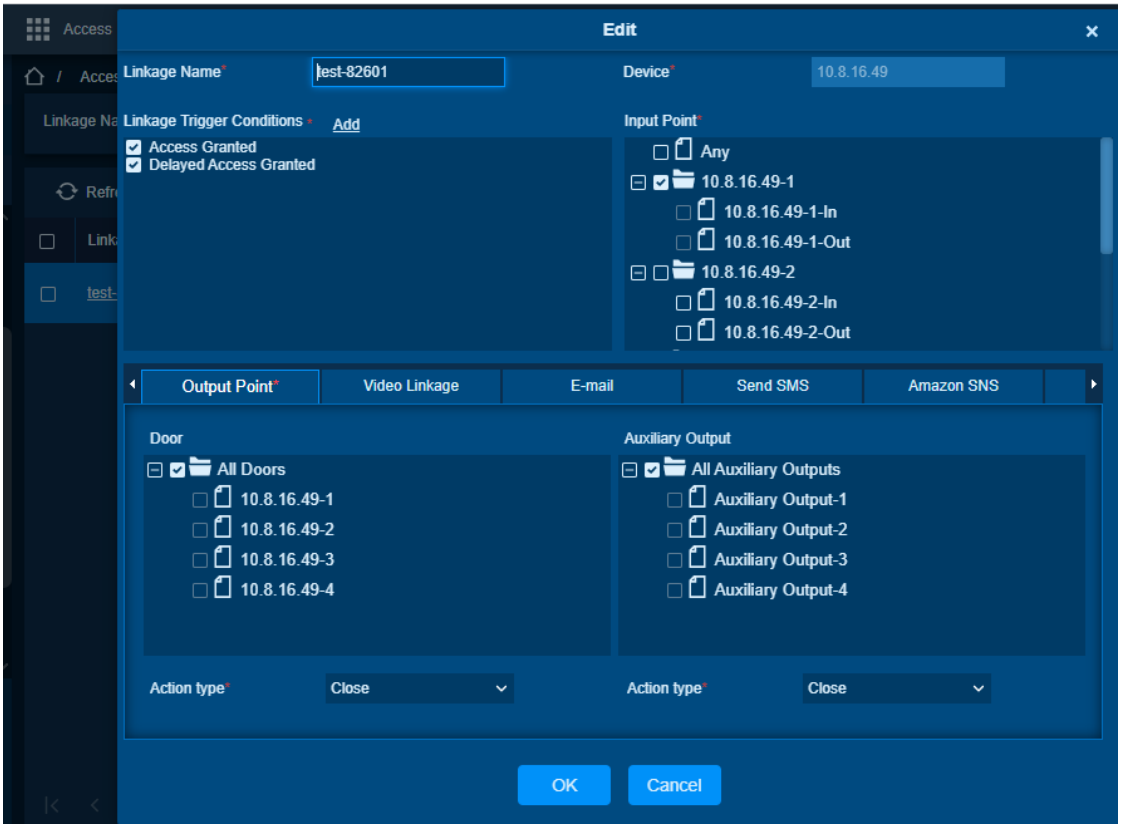
Feature Trigger Result

According to the modified linkage event, when an Input Point triggers the event, a linkage action will be generated at the specified Output Point to control the door event in the system and displayed in the corresponding event list for monitoring.

Steps:

- Click **[Access]** > **[Access Control]** > **[Linkage]** to display the linkage interface.
- Select the linkage you want to modify and click **[Edit]** to modify linkage rules.





Delete Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device supports adding to the Access Control module.

Function Usage Scenarios

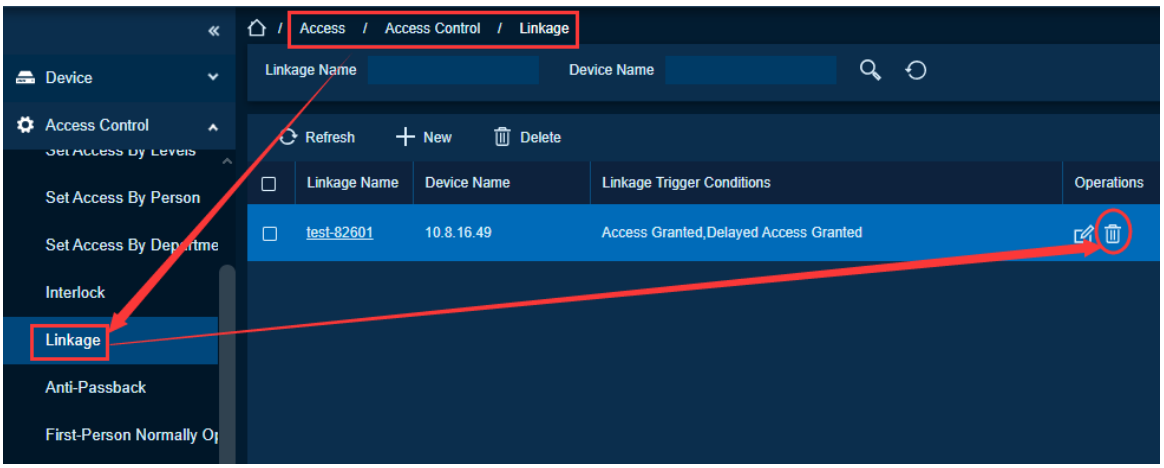
Need to delete the linkage action performed by the output port when the control input port is triggered.

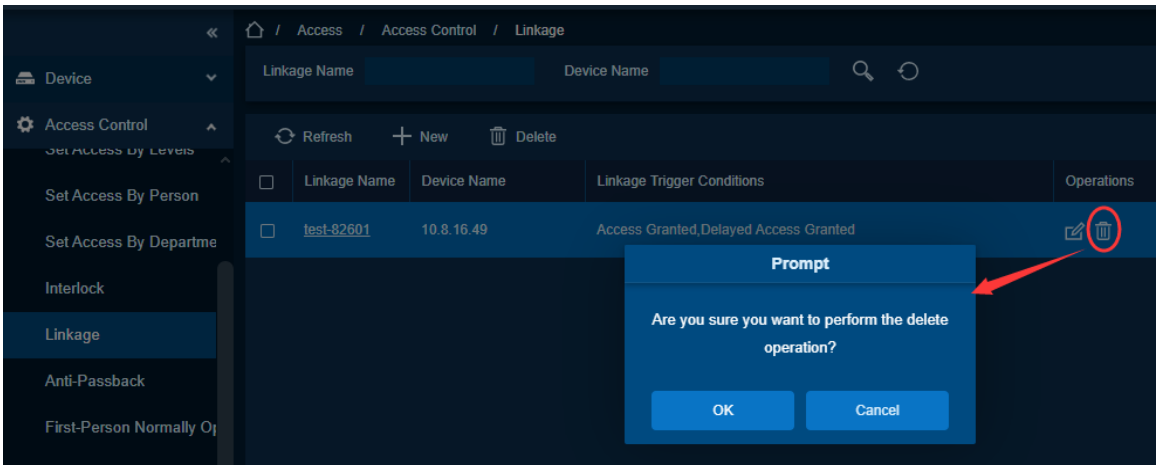
Feature Trigger Result

Delete the linkage event. When the event is triggered by an Input Point, a linkage action will not be generated at the specified output point.

Steps:

- Click **[Access] > [Access Control] > [Linkage]** to display the linkage interface.
- Select the linkage to be deleted and click **[Delete]** to delete the linkage.





6.2.9. Anti-Passback

Function Description

Currently anti-passback settings support in and out anti-passback. In some special occasions, it is required that the cardholders who entered from a room by card swiping at a door device must swipe the cards over a device at the same door when leaving to keep the entry and exit records strictly consistent. The user can use this function just by enabling it in the settings. This function is normally used in prisons, the army, national defense, scientific research, bank vaults, etc.

Add Anti-Passback Rule

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

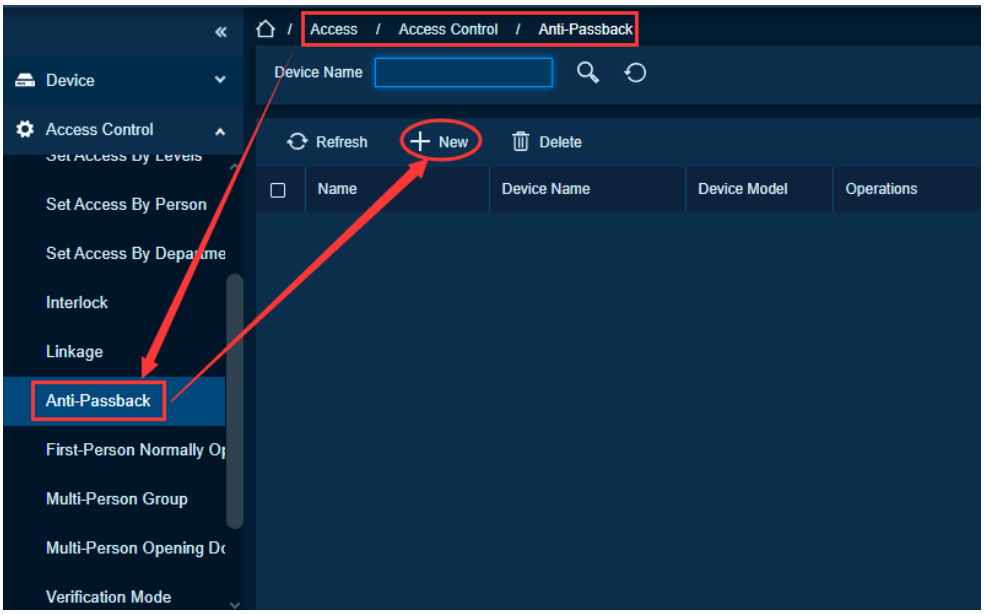
Places with high safety requirements need to control the entry and exit of personnel.

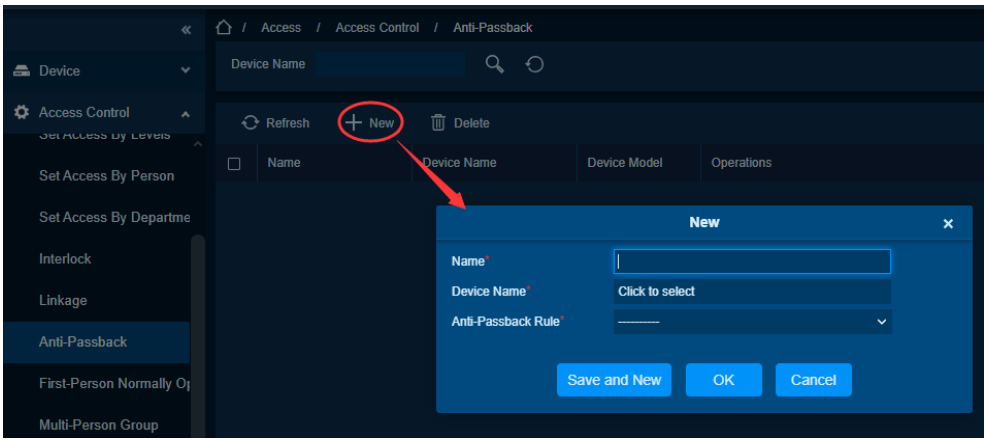
Feature Trigger Result

Add anti-passback, and strictly carry out entry and exit management in accordance with anti-passback rules.

Steps:

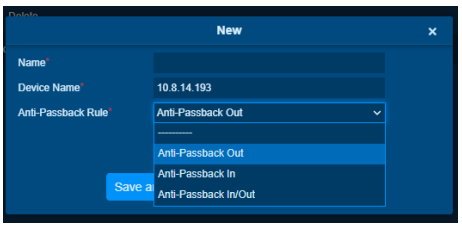
- Click **[Access Control] > [Anti-Passback] > [New]** to show the edit interface.





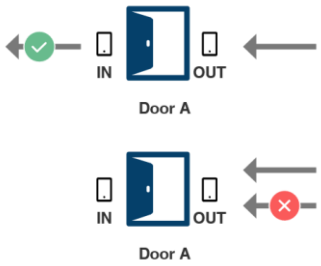
Select devices: -When users are adding Anti-Passback Rules, devices with anti-passback settings cannot be seen in the dropdown list. When deleting established anti-passback information, the corresponding device will appear in the dropdown list again. The settings vary with the number of doors controlled by the device.

- **OmniAC Series Standalone Terminal**

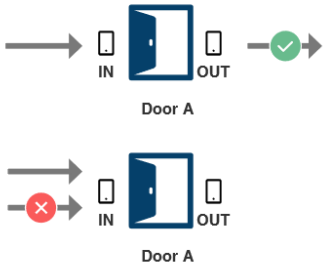


Example for OmniAC 20 (IN Reader), connect with a slave reader (OUT Reader)

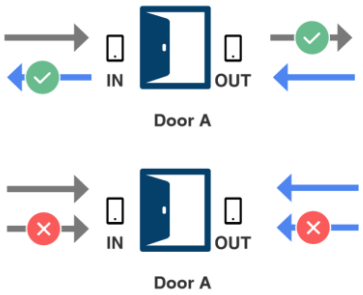
Anti-Passback Out: Person A wants to exit from Room via slave reader (OUT Reader), Device will check whether Person A has a transaction in OmniAC 20 (IN Reader), if not exist, system will deny your access and send an event ‘Anti-Passback’ .



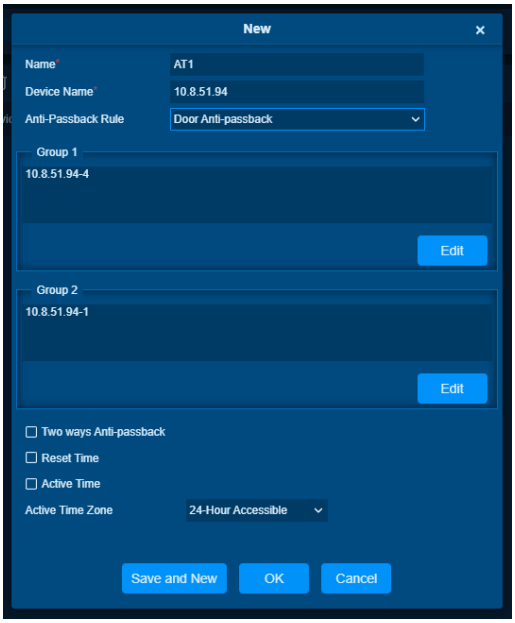
Anti-Passback In: Person A wants to go into Room via OmniAC 20(IN Reader), Device will check whether Person A has a transaction in slave reader (OUT Reader), if not exist, system will deny your access and send an event ‘Anti-Passback’ .



Anti-Passback In/Out: Person A wants to go into/exit from Room via OmniAC 20(IN Reader)/ slave reader (OUT Reader), Device will check whether Person A has a transaction in another device, if not exist, system will deny your access and send an event ‘Anti-Passback’ .



- **Horizon Series Controller**

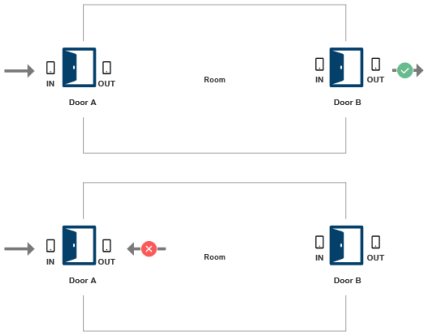


Anti-passback Rule:
Anti-passback supports One-Way and Two-Way Anti-Passback

- **Door Anti-Passback**

Rule 1: Door Anti-Passback
Group 1: Door A
Group 2: Door B

Personnel can only enter Door A (IN) and exit from Door B (OUT), if Enter Door A (IN) and exit from Door A (Out), Device will deny access and send event 'Anti-Passback'

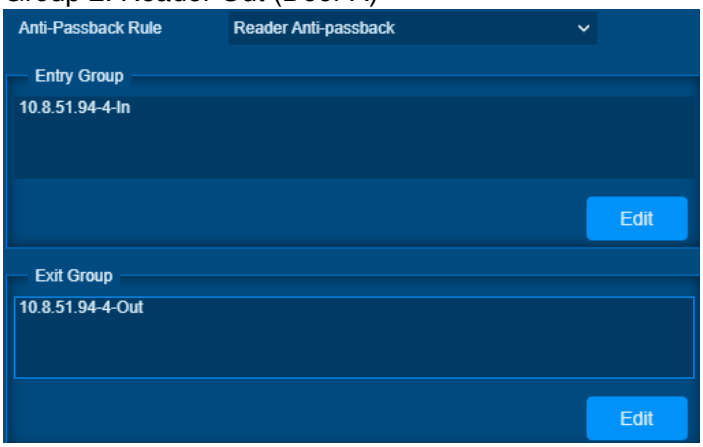


✍**Note:**

Now Anti-Passback is One-Way design, system will not limit Enter from Door B(IN) and Exit from Door A(OUT), if you want to set Two-Way Anti-Passback, need to set a new rule (Group 1: Door B, Group 2: Door A) or select checkbox Two-Way Anti-Passback

- **Reader Anti-Passback**

Rule 2: Reader Anti-Passback
Group 1: Reader IN (Door A)
Group 2: Reader Out (Door A)



Personnel can only enter Reader IN (Door A) and exit from Reader Out (Door A), if Enter Reader IN (Door A) and exit from Reader IN (Door A), Device will deny access and send event 'Anti-Passback'

✍**Note:**

Now Anti-Passback is One-Way design, system will not limit Enter from Reader Out (Door A) and Reader IN (Door A), if you want to set Two-Way Anti-Passback, need to set a new rule (Group 1: Reader Out (Door A), Group 2: Reader IN (Door A)) or select checkbox Two Ways Anti-passback.
Two Ways Anti-Passback: When punch on reader, will check whether have a transaction before in another readers.
Reset Time: When punch on reader, check rules for a specific period.

Active Time: Set validity for rule.

Active Timezone: Set valid Time Zone for rule

✍**Note:**

The door reader mentioned above includes Wiegand reader that connected with access controller and InBio

reader. The single and two doors' controllers with Wiegand reader includes out and in reader. There is only "In reader" for four door control panel. The reader number of 1, 2 (that is RS485 address or device number, the same below) is for door 1, the reader number of 3, 4 is for door 2, etc. No need to consider if it is a Wiegand reader or InBio reader when you are setting the anti-passback between doors or between readers, just make sure the in or out reader is set according to the actual requirements. For the reader number, odd number is for in reader, and even number is for out reader.

Select Anti-Passback Rule, and tick one item, click **[OK]** to complete, then the added anti-passback settings will be shown in the list.

Edit Anti-Passback

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

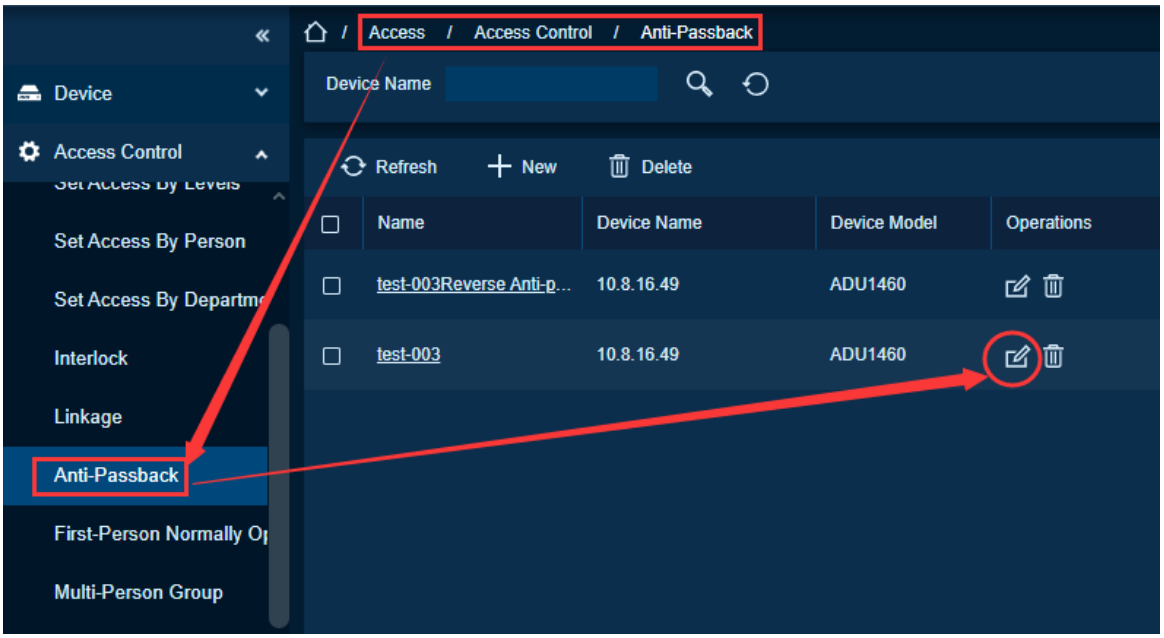
Places with high safety requirements need to control the entry and exit of personnel

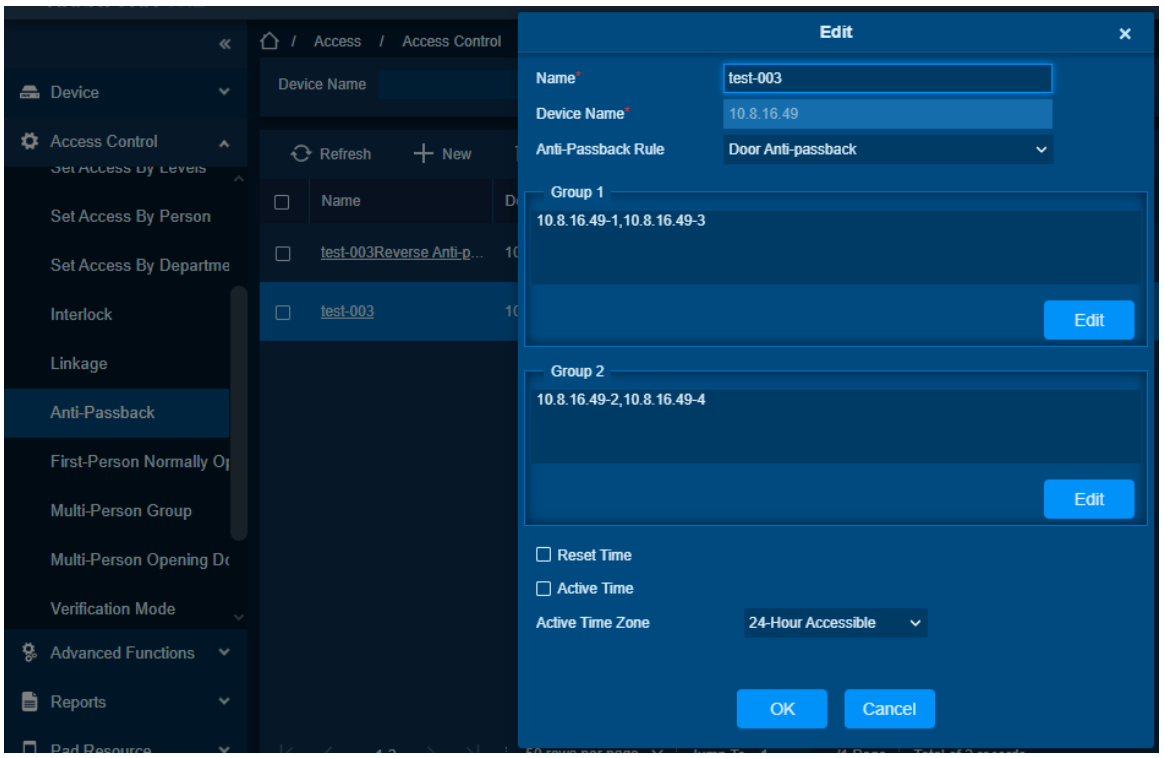
Feature Trigger Result

Edit anti-passback, modify anti-passback rules, and strictly conduct entry and exit management in accordance with anti-passback rules.

Steps:

- Click **[Access]** > **[Access Control]** > **[Anti-Passback]** to display the anti-passback interface.
- Select the device name and click **[**Edit**]** to modify the anti-passback rules.





Delete Anti-Passback

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

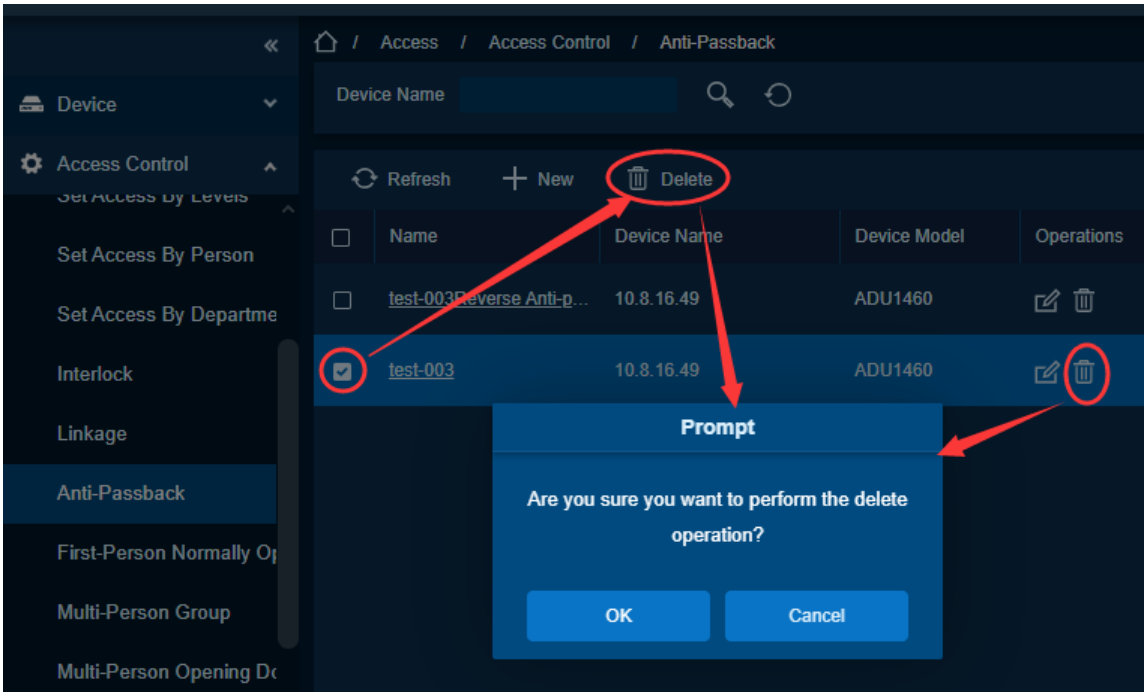
The Place does not need to strictly control the entry and exit of personnel.

Feature Trigger Result

Delete anti-passback, and do not strictly carry out entry and exit management.

Steps:

- Click **[Access] > [Access Control] > [Anti-Passback]** to display the anti-passback interface.
- Select the device name and click **[Delete]** to delete anti-passback.



6.2.10. First-Person Normally Open

Function Description

First-Person Normally Open: During a specified interval, after the first verification by the person having First-Person Normally Open level, the door will be Normal Open, and will automatically restore closing after the valid interval has expired.

Users can set First-Person Normally Open for a specific door (the settings include door, door opening time zone and personnel with First-Person Normally Open level). A door can set First-Person Normally Open for multiple time zones. The interface of each door will show the number of existing First-Person Normally Open.

When adding or editing First-Person Normally Open settings, you may only select door and time zones. After successful adding, add personnel that can open the door. You can browse and delete the personnel on the right of the interface.

Add First-Person Normally Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

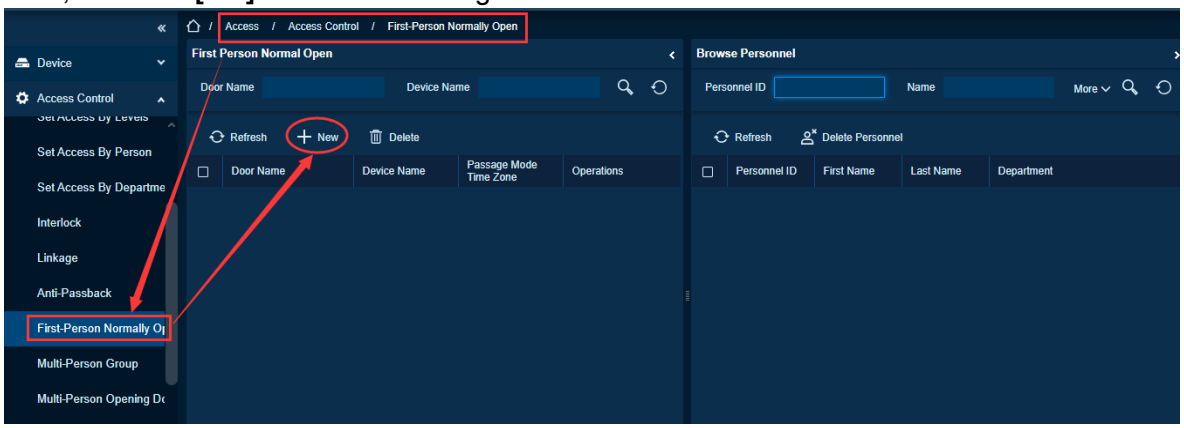
On some occasions, the door needs to be kept open for a certain period.

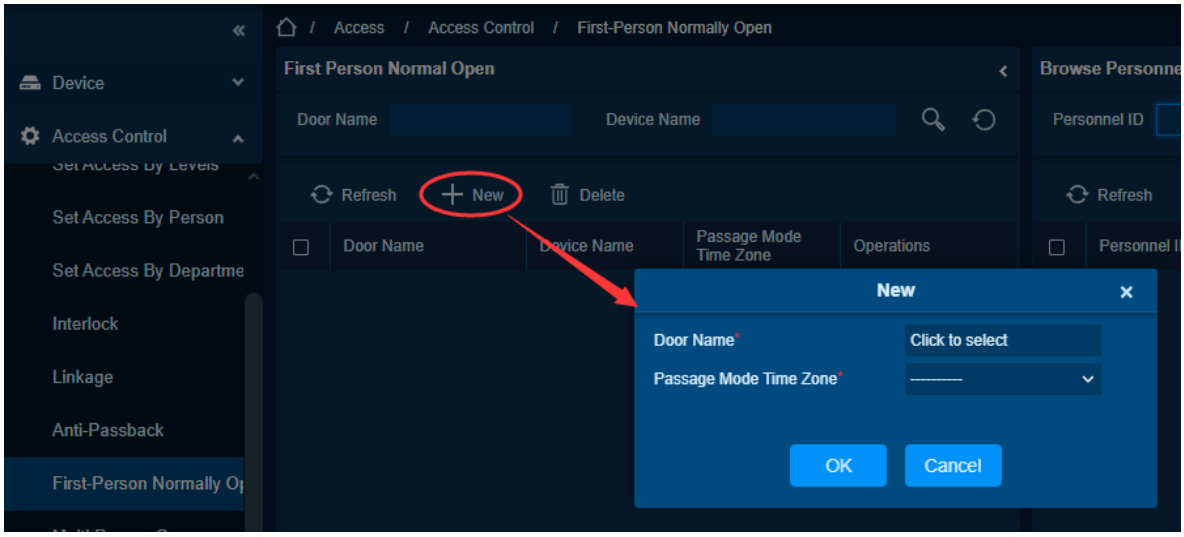
Feature Trigger Result

After a person with the first-person normally open authority opens the door, the door will be kept normally open for a specific period.

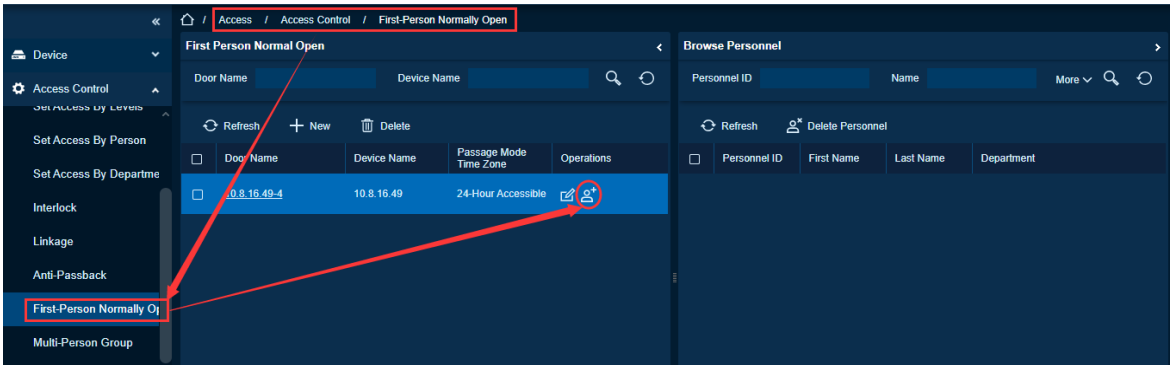
Steps:

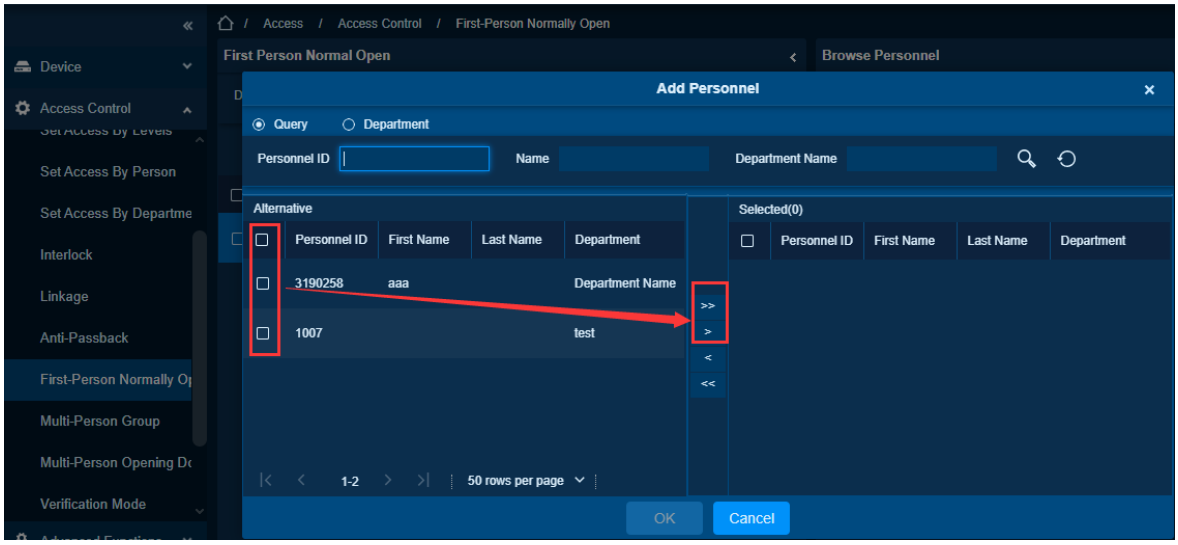
- Click **[Access Control]** > **[First-Person Normally Open]** > **[New],** select Door Name and Passage Mode Time, and click **[OK]** to save the settings.



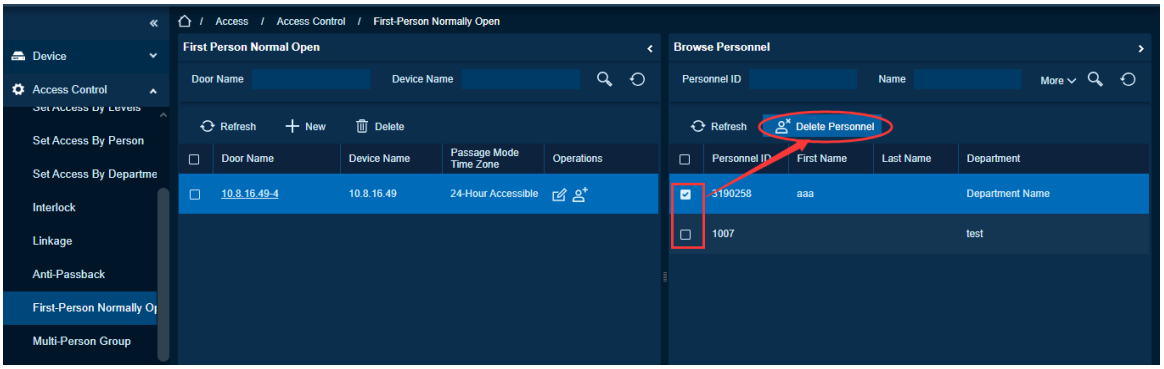


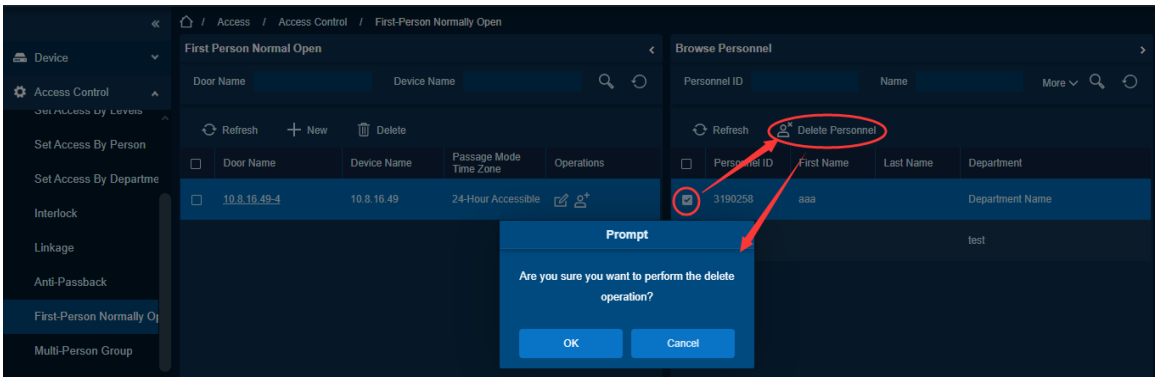
- Click **[Add Personnel]** under Related operation to add personnel having First-Person Normally Open level (these personnel must have access control level), then click **[OK]** to save.





- Select the door that the first-person normally open, select the person to be deleted on the right, and click **[Delete Person]** to delete.





Edit First-Person Normally Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

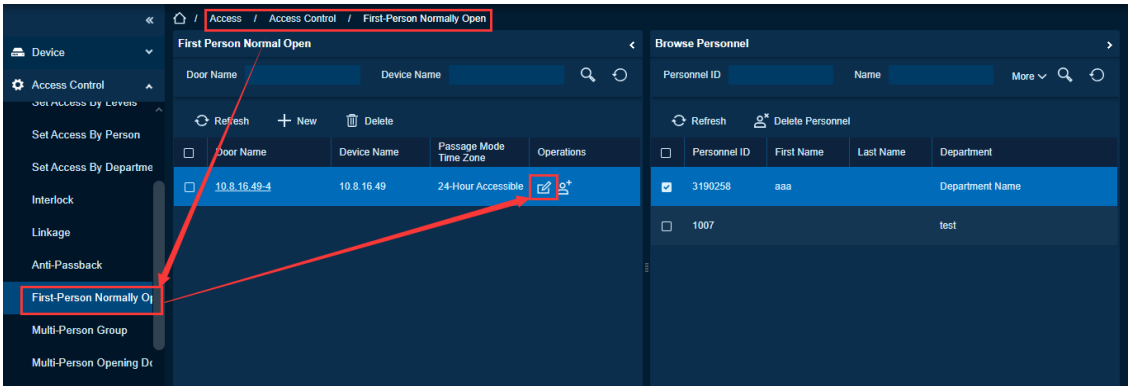
On some occasions, the time during which the door remains normally open needs to be modified.

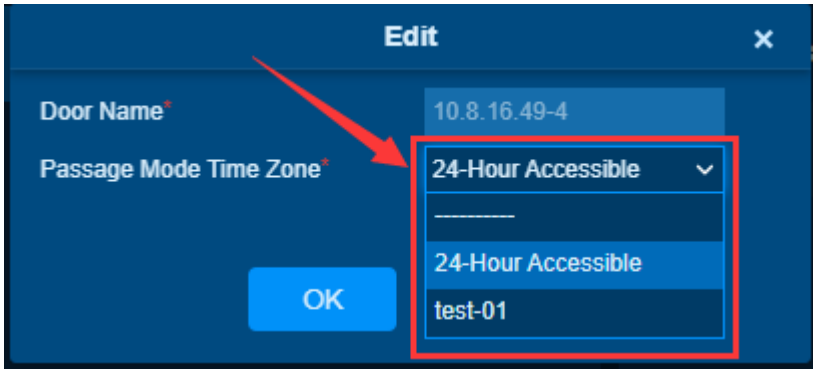
Feature Trigger Result

After a person with the first-person normally open authority opens the door, the door will be kept normally open for a specific period.

Steps:

- Click **[Access] > [Access Control] > [First-Person Normal Open]** to display the First-Person Normally Open interface.
- Select the door and click **[Edit]** to modify the first-person normally open time.





Delete First-Person Normally Open

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

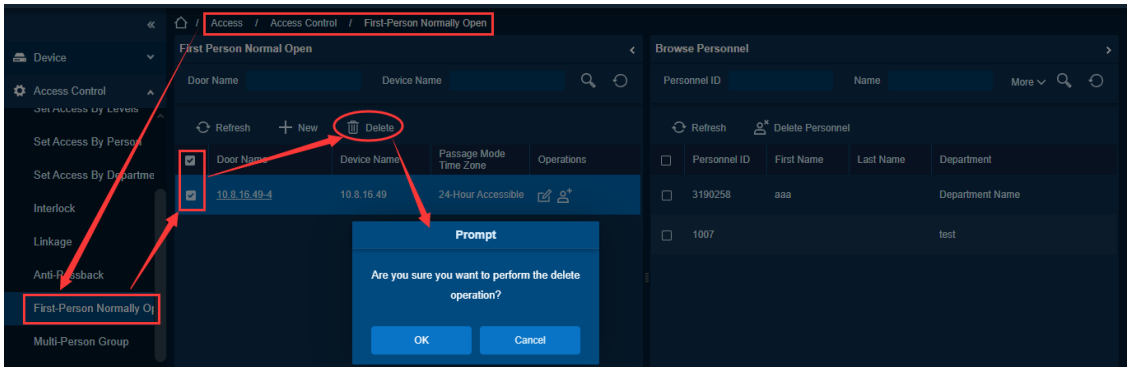
No need to set the first-person normally open for the door.

Feature Trigger Result

There is no function of keeping the door open after the first person opens the door.

Steps:

- Click **[Access] > [Access Control] > [First-Person Normally Open]** to display the First-Person Normally Open interface.
- Select the door and click **[Delete]** to delete the first person normally open time.



6.2.11. Multi-Person Group

Function Description

The door will open only after the consecutive verification of multiple people. Any person who is not belongs to this multi-person group verifies will interrupt the multi-person group verify process.

Add Multi-Person Group

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

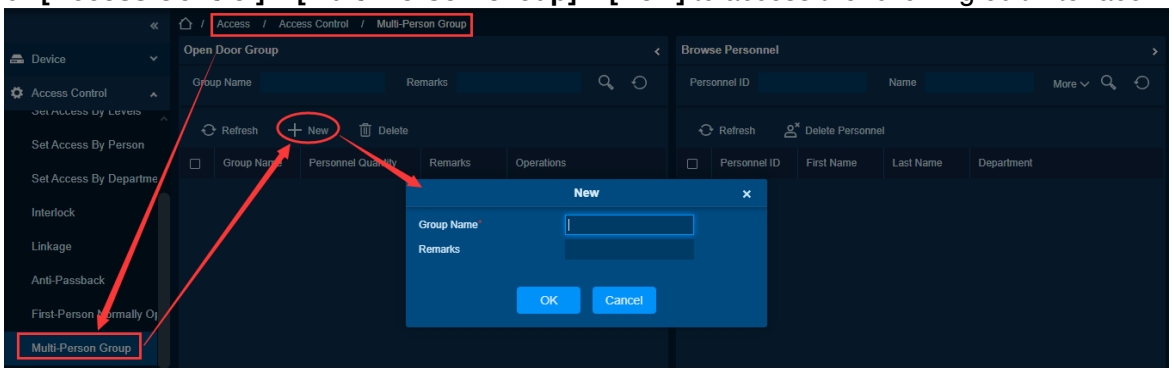
On some occasions, the door can only be opened when several people are present at the same time.

Feature Trigger Result

The door can only be opened after one-time verification by multiple persons who belongs to one Multi-Person Group.

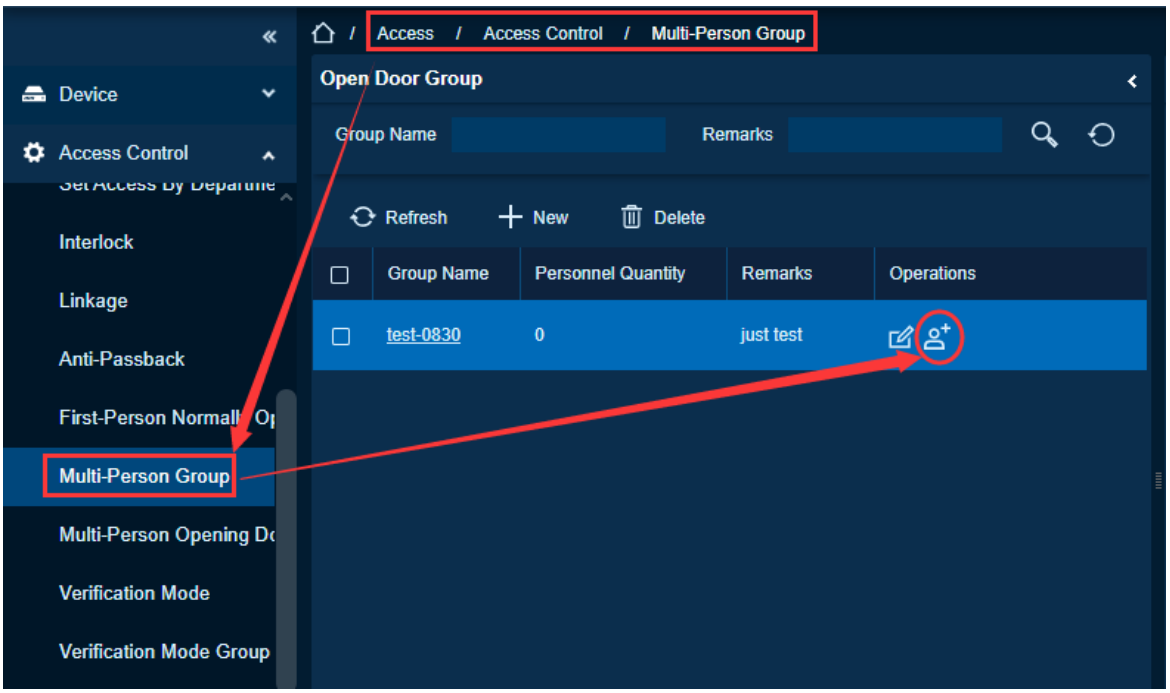
Steps:

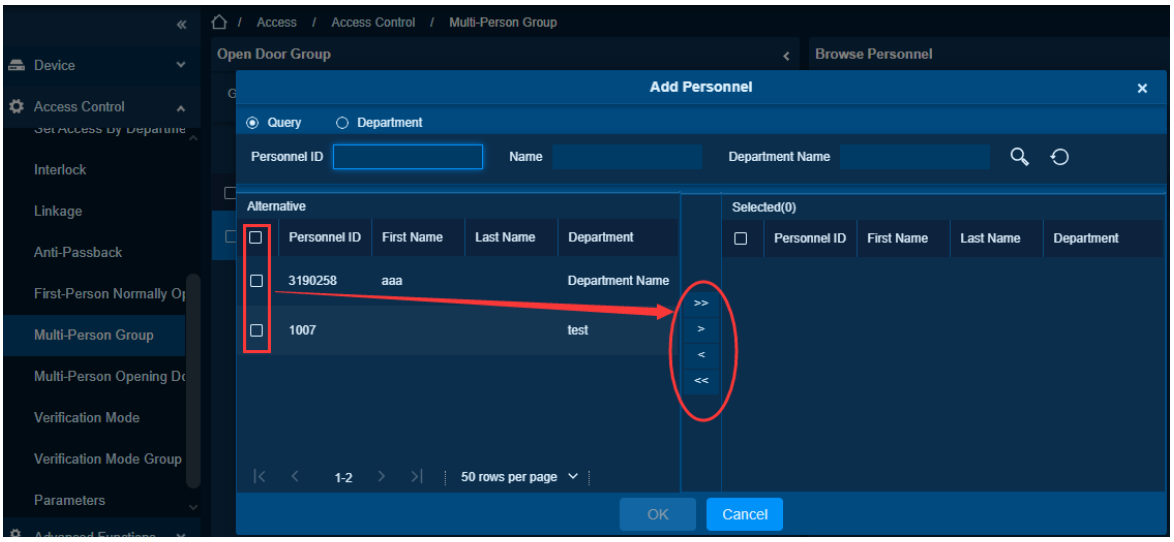
- Click **[Access Control]** > **[Multi-Person Group]** > **[New]** to access the following edit interface.



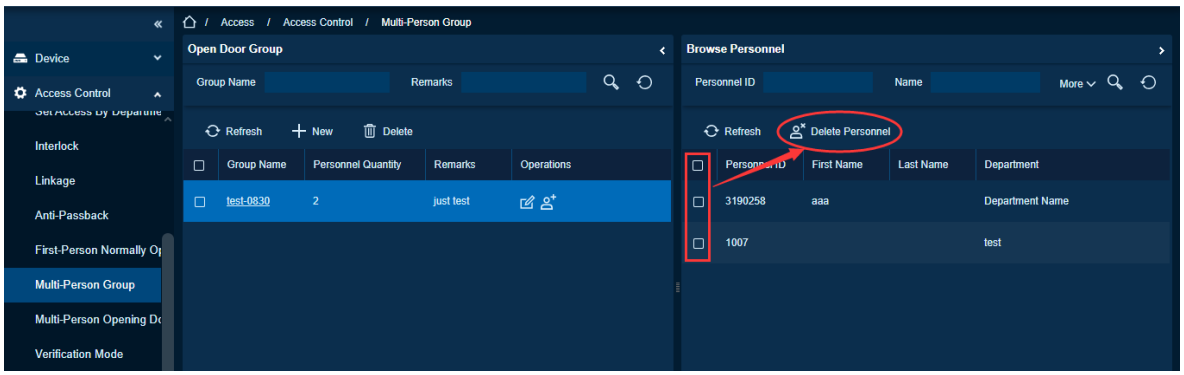
Group name: Any combination of up to 30 characters that cannot be repeated.

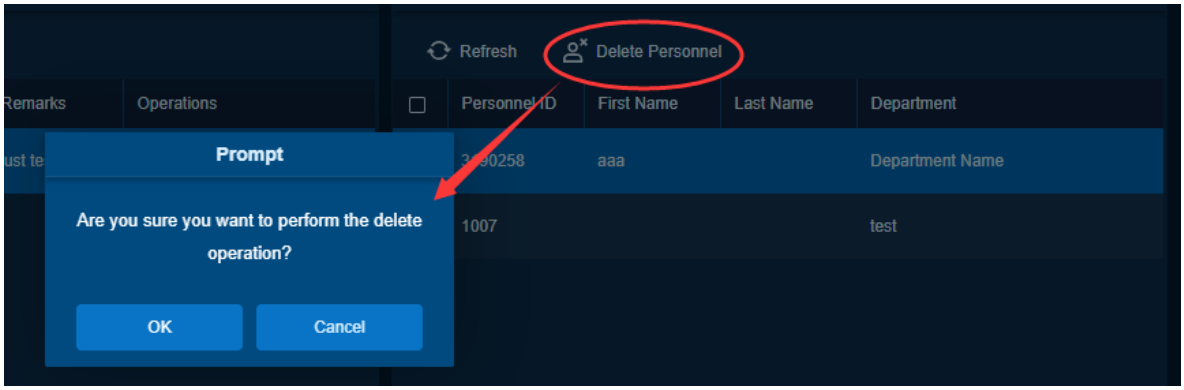
- After editing, click **[OK]** to save. The added Multi-Person Personnel Group will appear in the list.
- Click **[Add personnel]** under Related Operations to add personnel to the group.
- After selecting and adding personnel, click **[OK]** to save and return.





Select the personnel to be in this door opening group and click **[Delete Personnel]** to delete.





✍**Note:**

A person can only be grouped into one multi-person group.

Edit Multi-Person Group

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

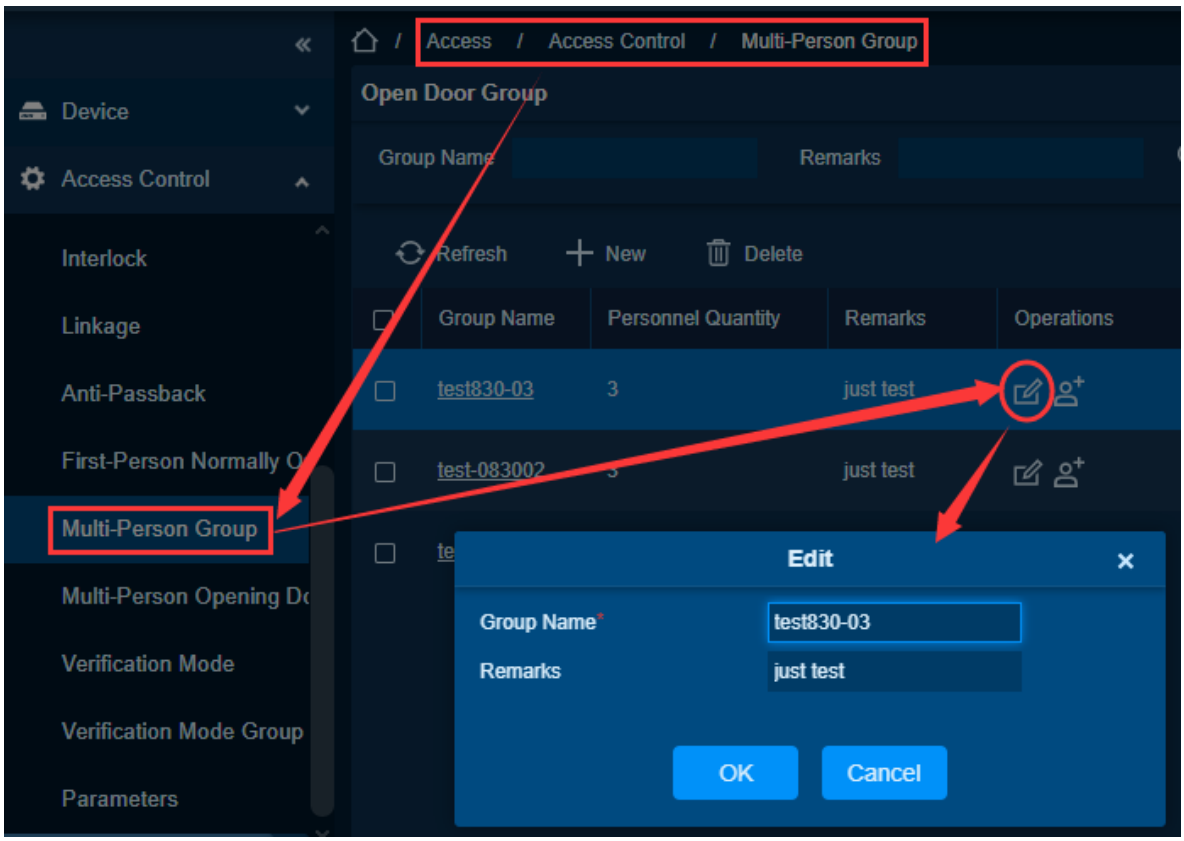
The added multi-person group needs to modify the group name or remarks.

Feature Trigger Result

Modified to a new group name and remarks.

Steps:

- Click **[Access]** > **[Access Control]** > **[Multi-Person Group]** to display the multi-person group interface.
- Select the door and click **[Edit]** to modify the multi-person group.



Delete Multi-Person Group

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

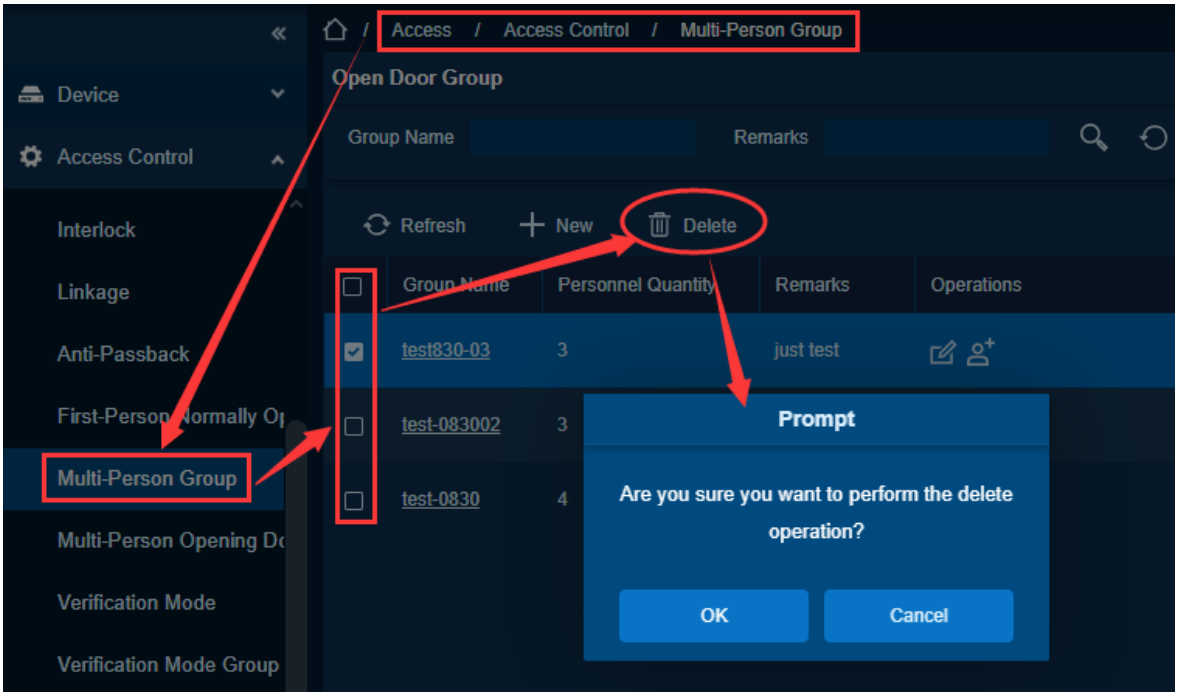
No need to verify by multiple people at the same time to open the door.

Feature Trigger Result

Delete the multi-person group.

Steps:

- Click **[Access]** > **[Access Control]** > **[Multi-Person Group]** to display the multi-person group interface.
- Select the group and click **[Delete]** to delete the multi-person group.



6.2.12. Multi-Person Opening Door

Function Description

Set levels for personnel in Multi-Person Personnel Group.

It is a combination of the personnel in one or more Multi-Person Group. When setting the number of people in each group, you can configure one group (such as combined door opening by two people in one group) or multiple groups (such as combined door opening by four people, including 2 people in group 1 and 2 people in group 2), and at least one group shall consist of number of doors opening people instead of 0, and the total number shall not be greater than 5. In addition, if the number of people entered is greater than that in the current group, Multi-Person Opening Door will be disabled.

Add Multiple People Opening Door Rule

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

A multi-person group has been added.

Function Usage Scenarios

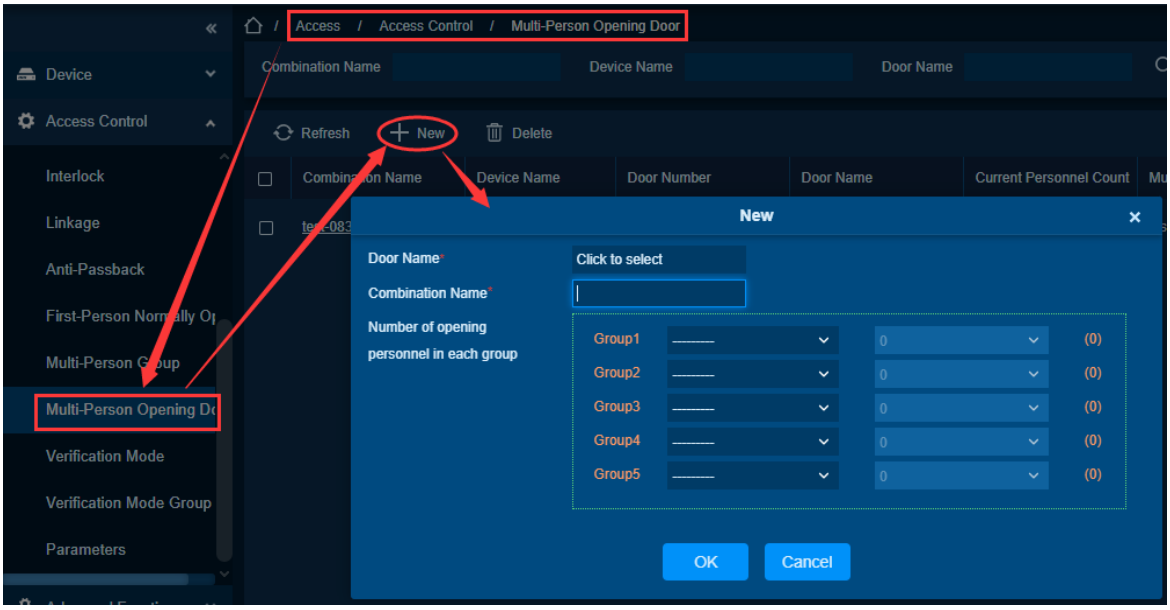
On some occasions, the door can only be opened when several people are present at the same time.

Feature Trigger Result

You can set permissions for the personnel in the **[Multi-Person Group],** and multiple multi-person groups can execute the door open authority together.

Steps:

- Click **[Access] > [Access Control] > [Multi-Person Opening Door] > [New].**



- The maximum number of multi-people opening door people for combined door opening is 5. That in the brackets is the current actual number of people in a group.
- Select the number of people for combined door opening in a group and click **[OK]** to complete.

✍**Note:**

The default Credit Card Interval is 10 seconds; it means that the interval of two personnel's verification must not exceed 10 seconds. You can modify the interval if the device supports.

Edit Multi-Person Opening Door Rule

Preconditions for Normal Use of Function

Log in to the system with current account and have the menu authority.

A multi-person group has been added.

Function Usage Scenarios

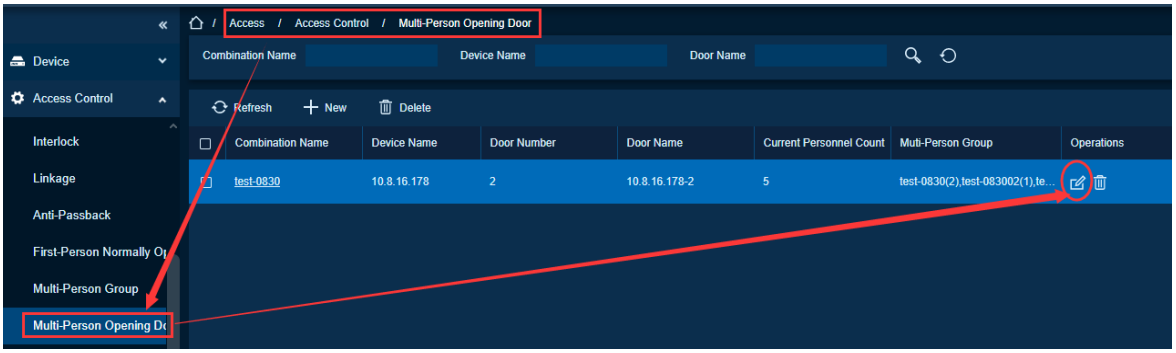
Modify the name of **Multi-Person Opening Door** rule, add/remove door from rule.

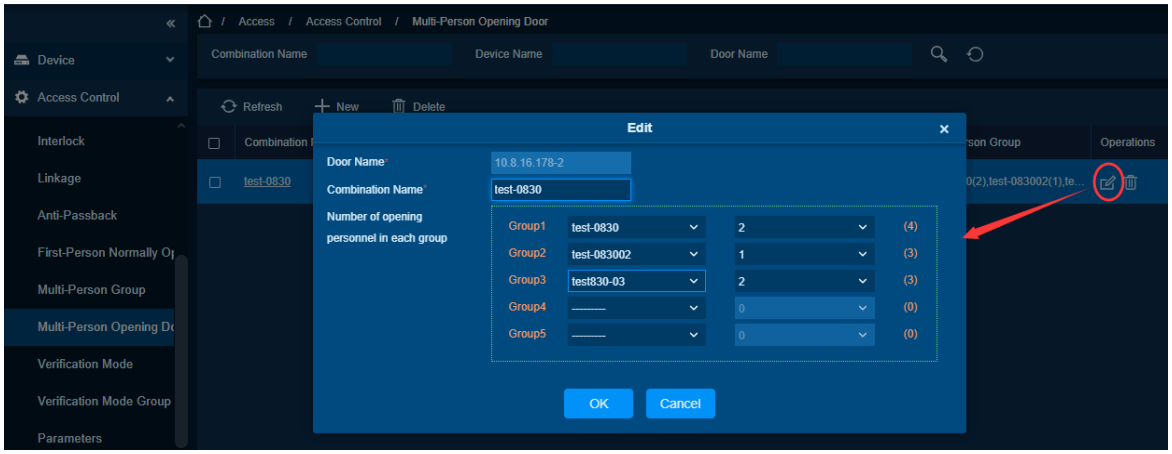
Feature Trigger Result

Person who in Multi-Person Group verify on new door which is newly assigned to Multi-Person Opening Door rule need run multi-person verification process.

Steps:

- Click **[Access]** > **[Access Control]** > **[Multi-Person Opening Door]** to display the multi-person opening door interface.
- Select the door and click **[Edit]** to modify the multi-person door opening configuration.





Delete Multi-Person Opening Door Rule

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

A multi-person group has been added.

Function Usage Scenarios

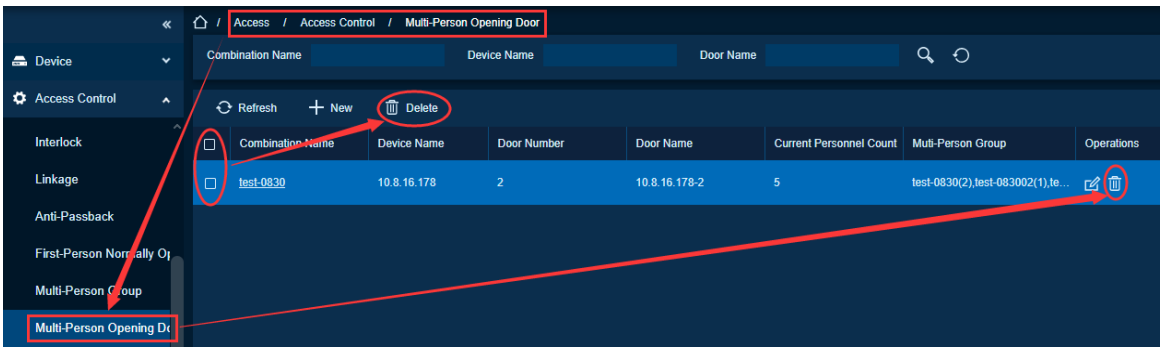
The device corresponding to multiple people to open the door that does not need to be set.

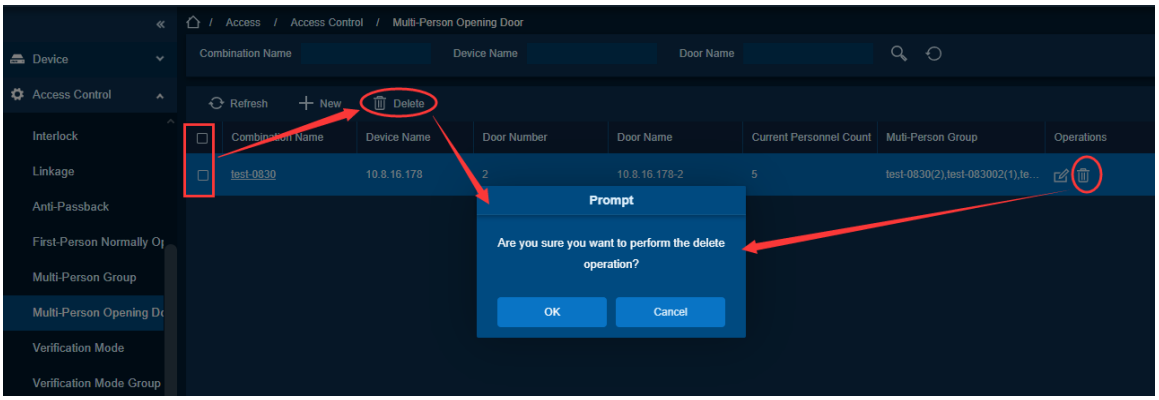
Feature Trigger Result

Cancel the multi-person open door.

Steps:

- Click **[Access] > [Access Control] > [Multi-Person Opening Door]** to display the multi-person door open interface.
- Select the door and click **[Delete]** to delete the multi-person door opening configuration.





6.2.13. Verification Mode

Function Description

The verification method can be set separately for the door and the person within the specified time.

New Verification Mode

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device supports adding to the access control module.

Function Usage Scenarios

Some specific scenarios such as Lobby

Daytime (8:00 – 18:00): Employee verifies on entrance barrier where will request to use Card as verification method

Nighttime (00:00-07:59, 18:01-23:59): Employee verifies on entrance barrier who will request to use Card + Fingerprint as verification method to enhance security level.

So set **Reader Verification** to reader used in entrance barrier is Daytime (8:00 – 18:00) for Card, Nighttime (00:00-07:59, 18:01-23:59) for Card + Fingerprint

For guard: it is request to Face as verify method for whole day (24-Hour).

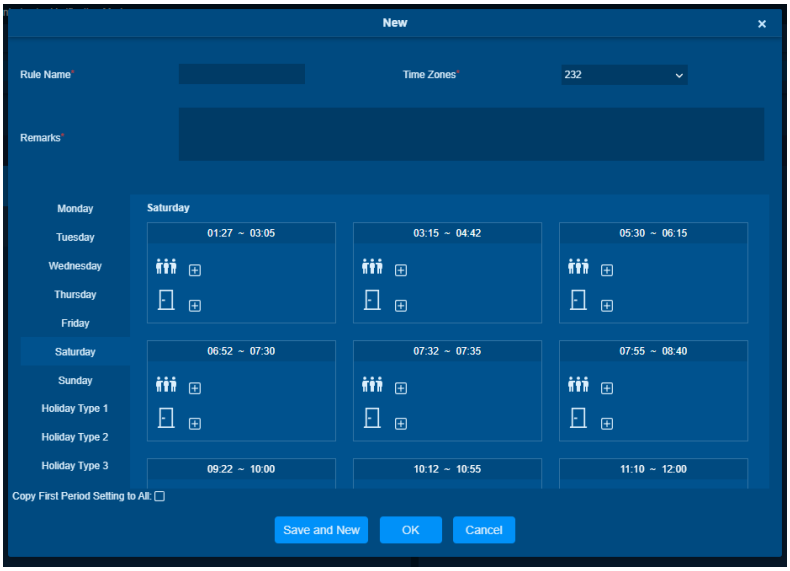
So set **Personnel Verification** to guard for 24-Hour Face

Feature Trigger Result

Can be verified by the set verification method and time.

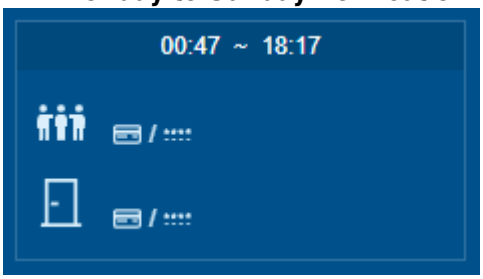
Steps:

- Click **[Access Control] > [Verification Mode] > [New]** to go to the page for adding a verification mode rule.



Set the following parameters:

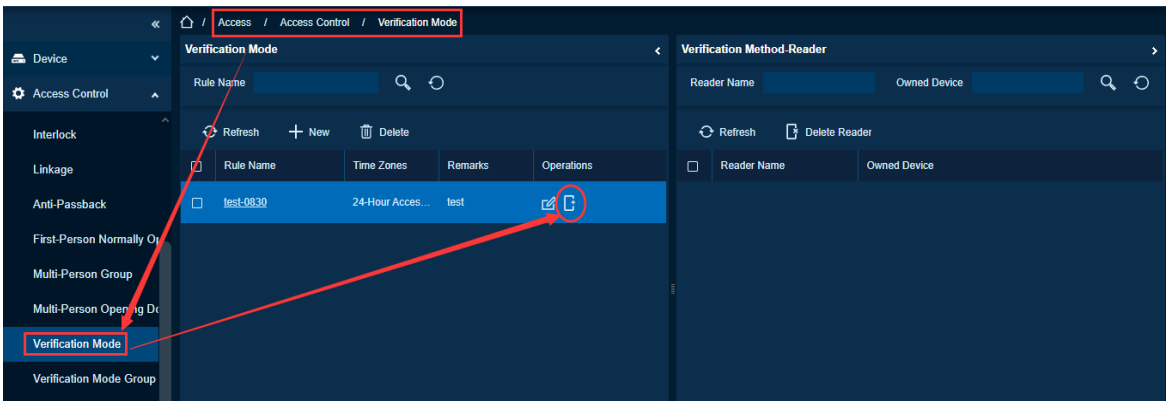
- **Rule Name:** Name for this rule, easily to identify.
- **Time Zones:** Get time zone from [Access]->[Access Control]->[Time Zones]
- **Monday to Sunday Verification Mode Settings:**

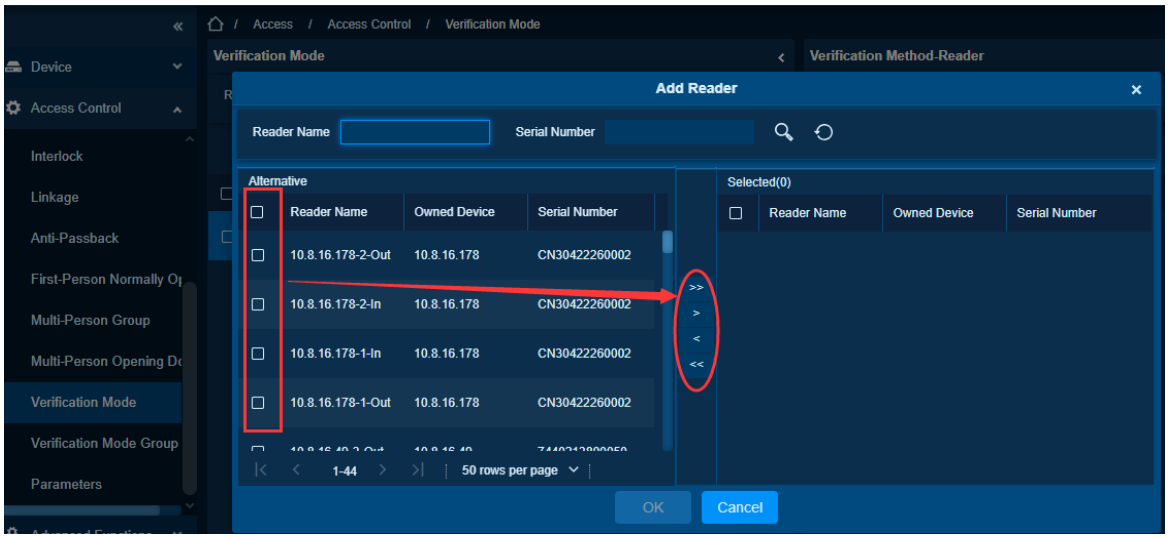


Personnel Verification: Set Verification for specific person
Door Verification: Set Verification for specific person
If person belongs to **Personnel Verification**, when person verify on reader will follow Person Verification first even **Personnel Verification** is not set in **Reader Parameter** and **Reader Verification**.
If person does not belong to **Personnel Verification** but need to verify on reader which is belongs to **Reader Verification**. So, this person verify on reader will follow **Reader Verification**.

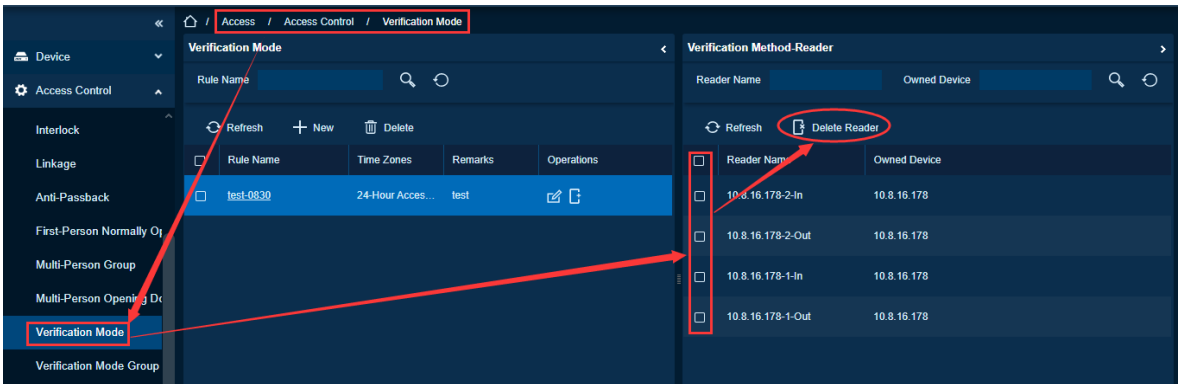
- Click **[OK]** to finish the setting.
- On the list page, you can add or delete doors in the verification mode rule.

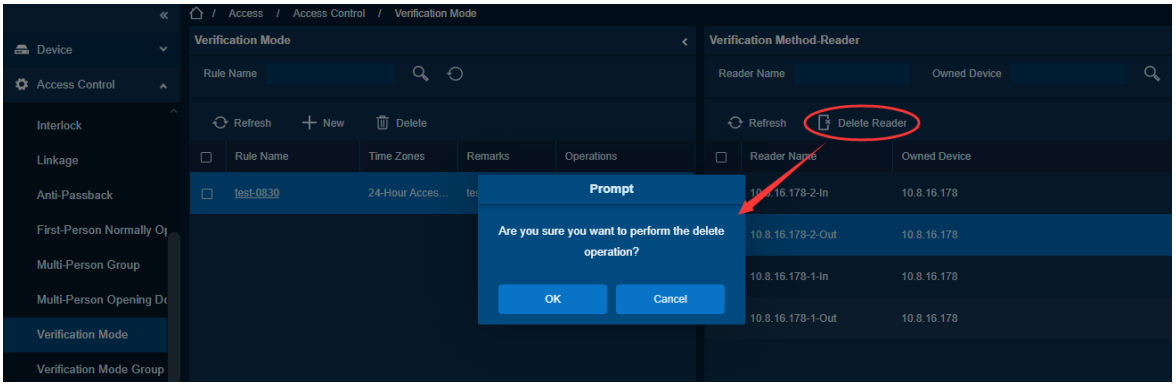
Add Reader





Delete Reader





✍**Note:**

If a rule includes the verification mode for personnel, you cannot select doors with the RS485 readers when adding doors. You can modify only the configuration on the reader setting page before adding doors.

Edit Verification Mode

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

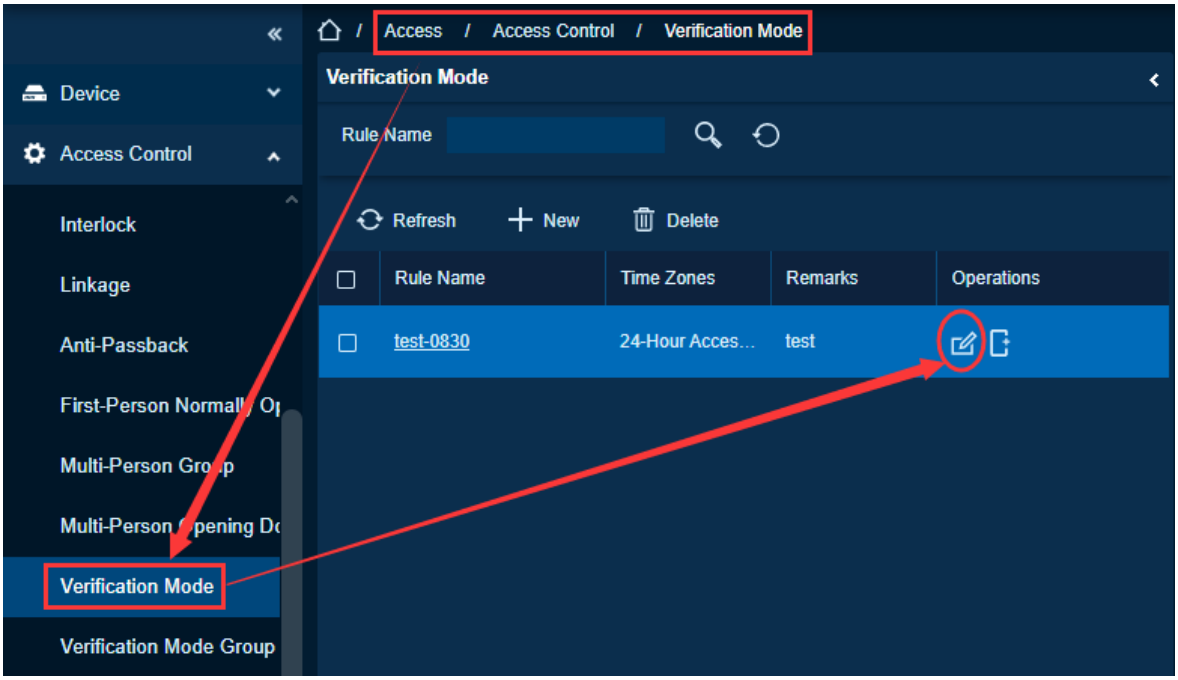
Need to modify the verification method and verification time of a door in batches.

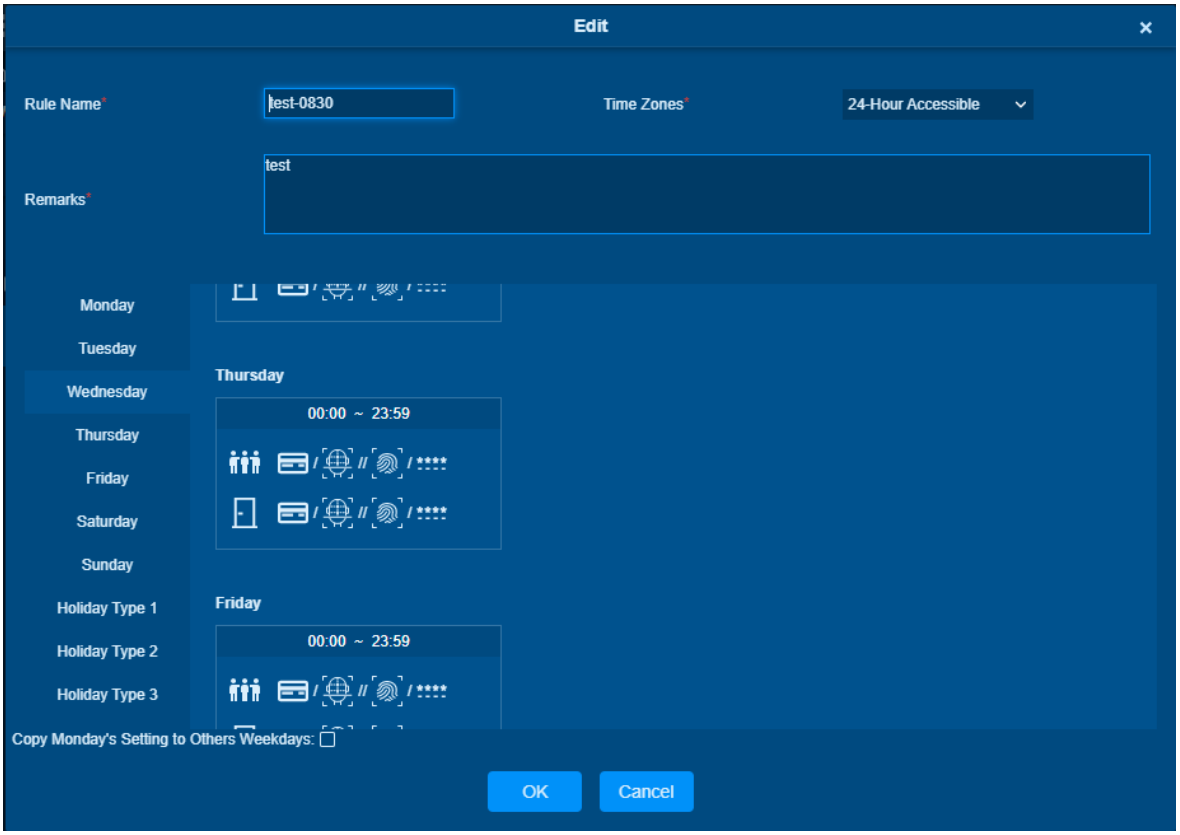
Feature Trigger Result

Can be verified by modified verification method and time.

Steps:

- Click **[Access]** > **[Access Control]** > **[Verification Method]** to display the verification mode interface.
- Select the rule name and click **[Edit]** to modify the verification mode.





Delete Verification Mode

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device supports adding to the access control module.

Function Usage Scenarios

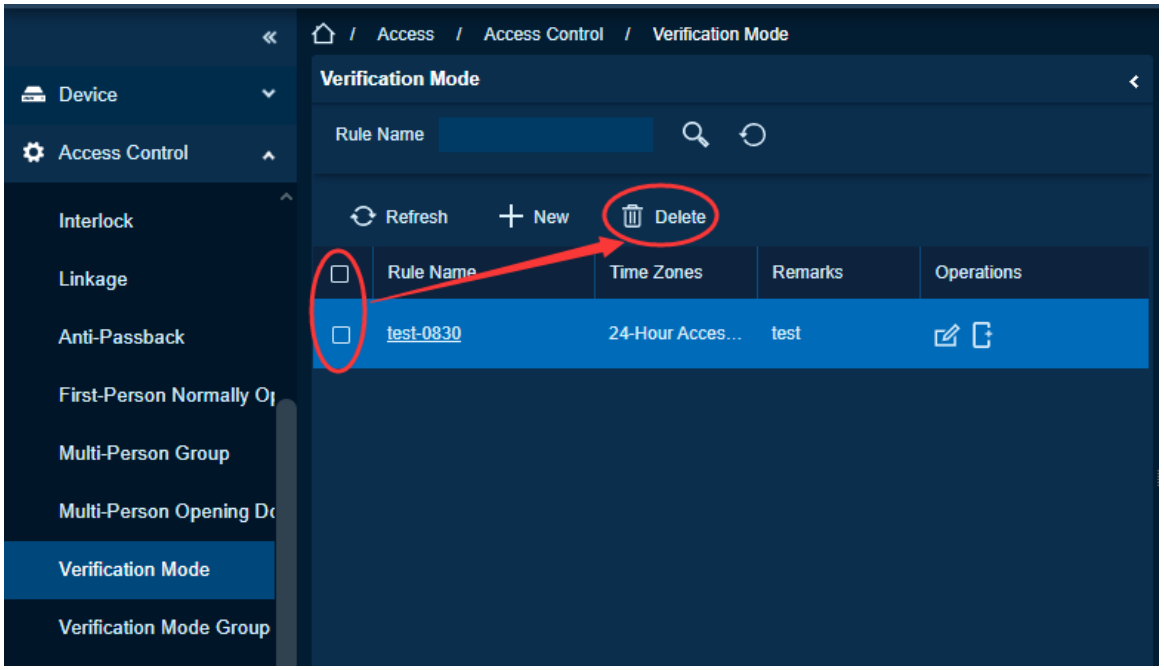
No need for this verification mode.

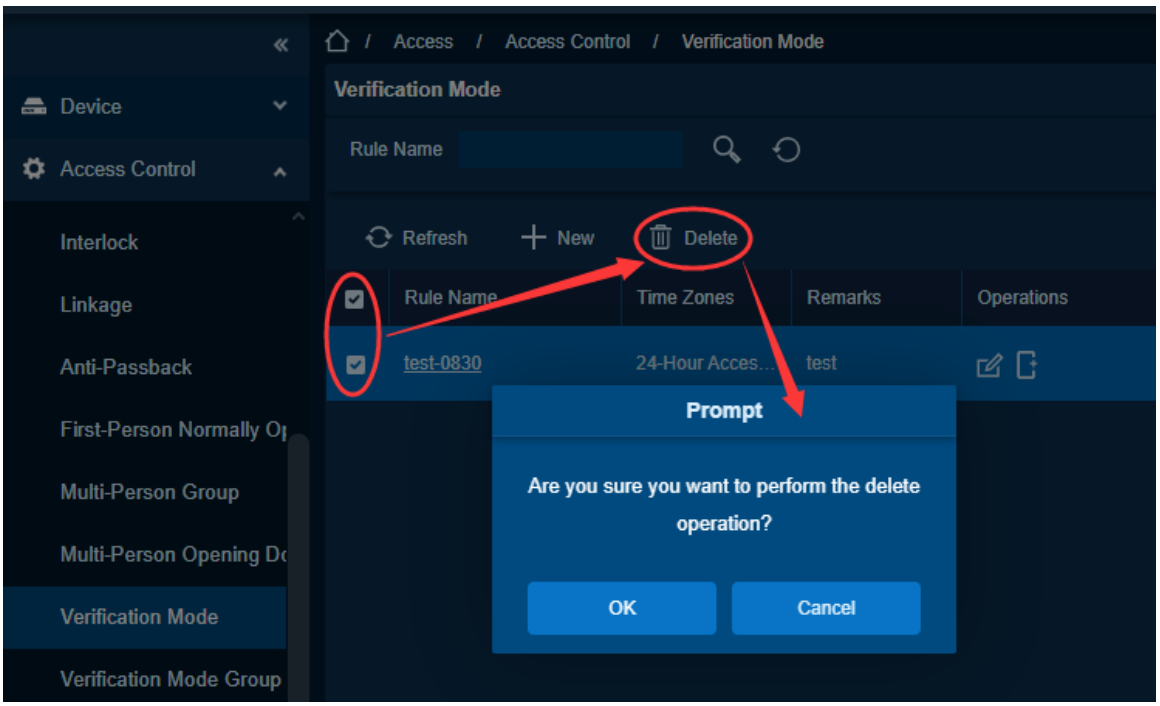
Feature Trigger Result

Failed to verify at this verification method and time.

Steps:

- Click **[Access] > [Access Control] > [Verification Method]** to display the verification mode interface.
- Select the rule name and click **[Delete]** to delete the verification mode.





6.2.14. Verification Mode Group

Function Description

Add personnel to the set verification mode group.

Add Personnel

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device supports adding to the access control module.

Function Usage Scenarios

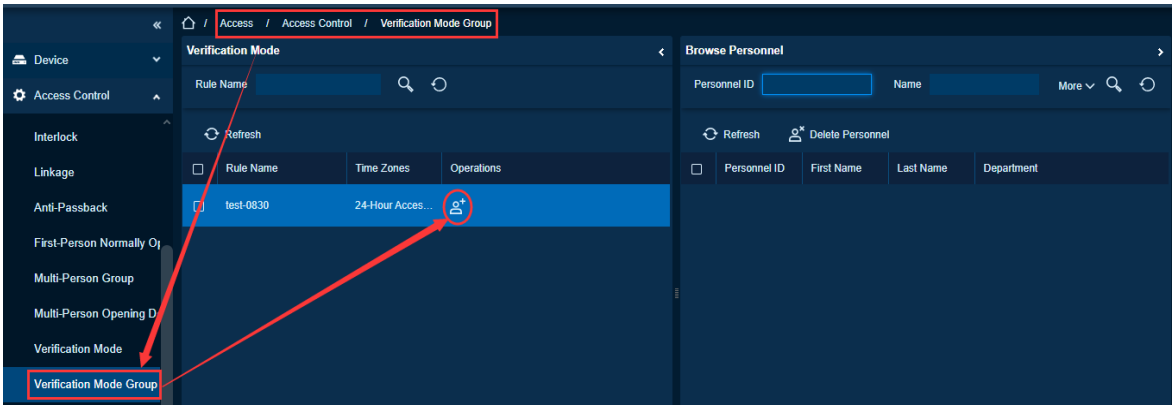
Need to add personnel in batches to verify the corresponding verification method and verification time for a certain door.

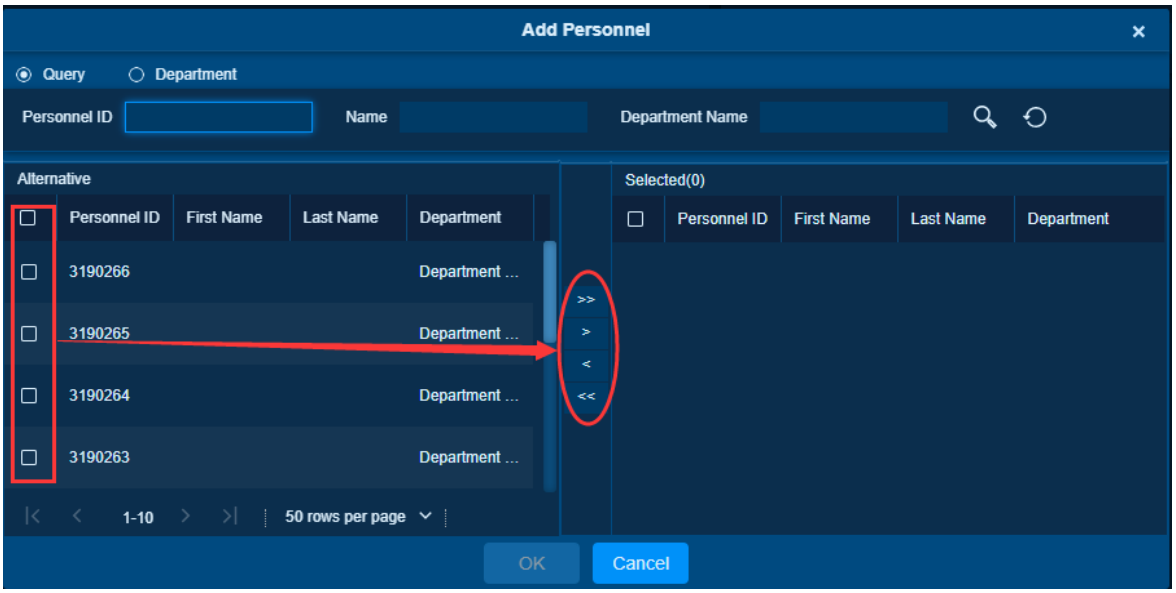
Feature Trigger Result

The added personnel can be verified by the set verification method and time.

Steps:

- Click **[Access]** > **[Access Control]** > **[Verification Mode Group]** to display the add verification mode interface.
- Select the rule name and click **[**Add Person**]** to add personnel.





Delete Personnel

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device supports adding to the access control module.

Function Usage Scenarios

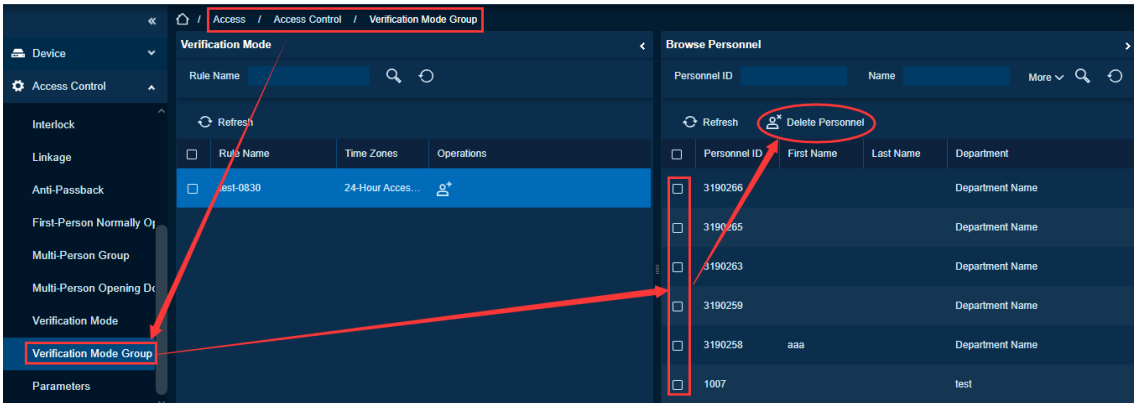
The person is not required to verify in accordance with the corresponding access control verification rules.

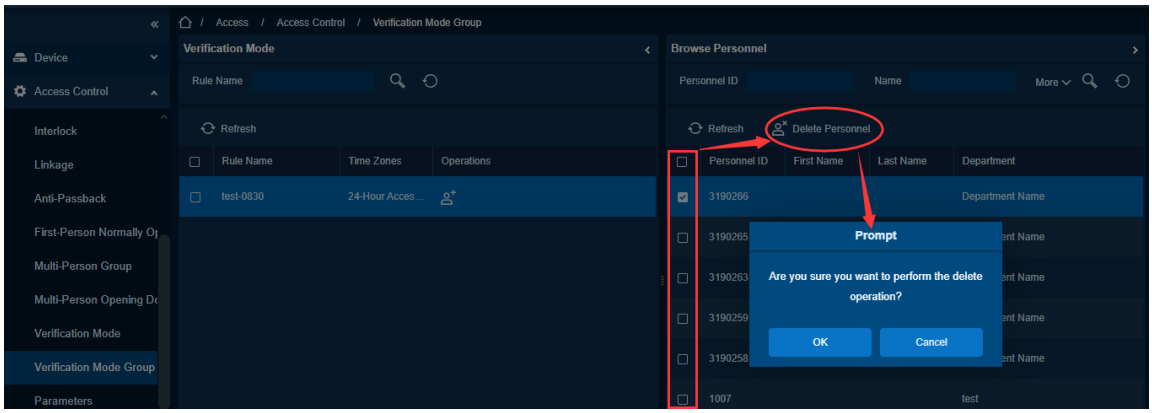
Feature Trigger Result

The person is not allowed to verify in this verification rule.

Steps:

- Click **[Access]** > **[Access Control]** > **[Verification Mode Group]** to display the verification mode interface.
- Select the rule name and click **[Delete Personnel]** to delete personnel.





6.2.15. Parameters

Function Description

Set some parameter s of the access control rules.

Parameter Settings

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device supports adding to the access control module.

Function Usage Scenarios

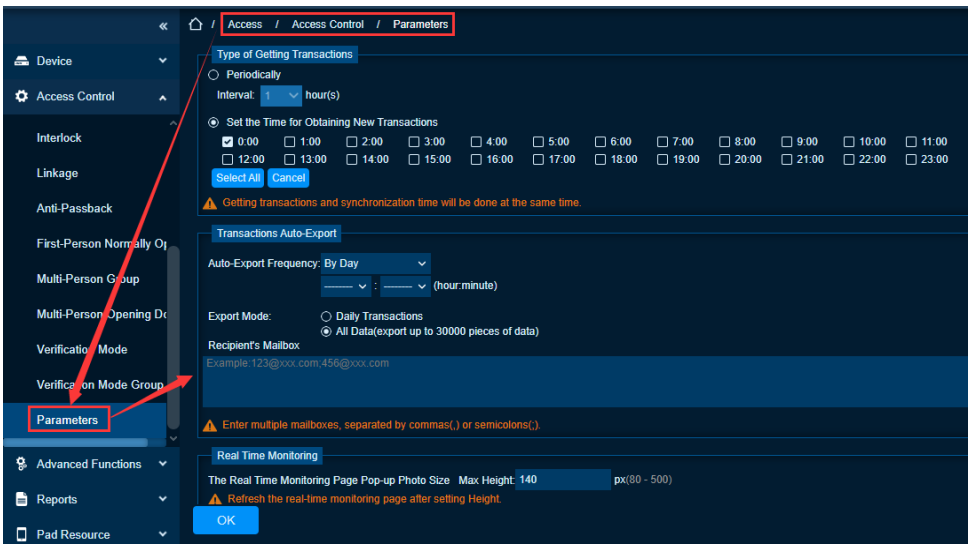
Need to modify the method of obtaining event record, automatic export of event records, real-time monitoring, and other data.

Feature Trigger Result

Different access control can be carried out according to the set access control parameter rules.

Steps:

- Click **[Access Control] > [Parameters]** to enter the parameter setting interface.



Type of Getting Transactions

Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Set the Time for Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

Transaction Auto-Export: -The user can choose the export frequency and the data to be exported each time. If the export frequency is selected as “By day”, you must set the time to export the data. You must also select the mode of export. It can be daily transactions or all the system data (30000 data units can be sent at a time.

If the export frequency is selected as “By Month”, you must select the day to export the data. It can be the first day of the month or you can specify any date. Then select the export frequency as Daily Data or all System data. Finally, add the recipient’s mail address to send the transaction data.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

Alarm Monitoring Recipient Mailbox: The system will send email to alarm monitoring recipient’s mailbox if there is any event.

Compare Photo Delivery Settings: The system sends a comparison photo to the device for storage.

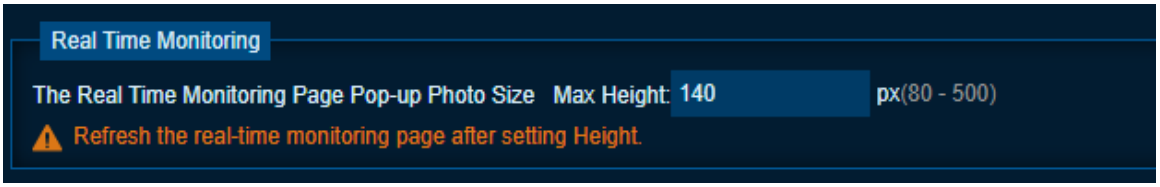
Deliver Permission Thread Pool Settings: Used in the background comparison of some devices.

Transactions Auto-Export

The user can choose the export frequency and the data to be exported each time. If the export frequency is selected as "**By day"**, you must set the time to export the data. You must also select the mode of export. It can be daily transactions or all the system data (30000 data units can be sent at a time).

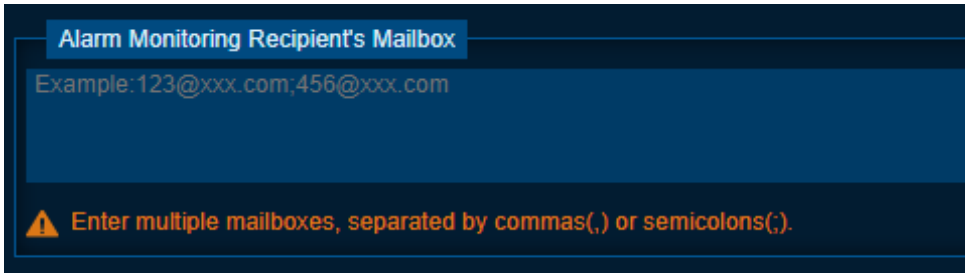
If the export frequency is selected as **"By Month"**, you must select the day to export the data. It can be the first day of the month or you can specify any particular date. Then select the export frequency as Daily Data or all System data. Finally, add the recipient's mail address to send the transaction data.

Real Time Monitoring



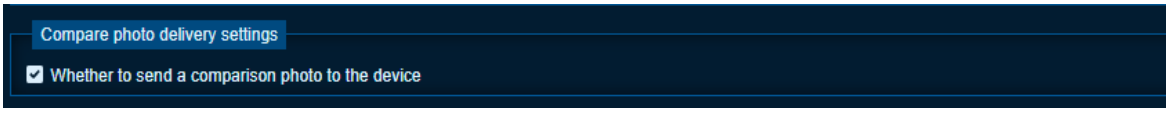
When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

Alarm Monitoring Recipient Mailbox



The system will send email to alarm monitoring recipient's mailbox if there is any event.

Compare Photo Delivery Settings



The system sends a comparison photo to the device for storage.

6.3. Advanced Functions

Function Description

Advanced Access control is optional function. If needed, please contact business representative or pre-sales engineer, you can use these functions after obtaining license and activating.

Function List

Functions	Description
Zone	Add, edit, delete, and view the access control rules in the access control area.
Reader Definition	Adding reader, adding, editing, and deleting readers in batches.
View People in the Area	Delete and export personnel.
Global Anti-passback	Add, edit, delete personnel.
Global Linkage	Add, edit, delete, enable, disable personnel.
Global Interlock Group	Add, edit, delete group.
Global Interlock	Add, edit, delete door.
Staff Availability	Add, edit, delete, and set access control area attributes.
Number Control	Add, edit, delete.

✍**Note:**

Except Global Linkage, to use other advanced functions you need to enable Background Verification.

6.3.1. Zone

Function Description

It mainly uses partition Zones in advanced access control. When using such advanced functions as Global Zone APB, you must define Access Zones.

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

Function Usage Scenarios

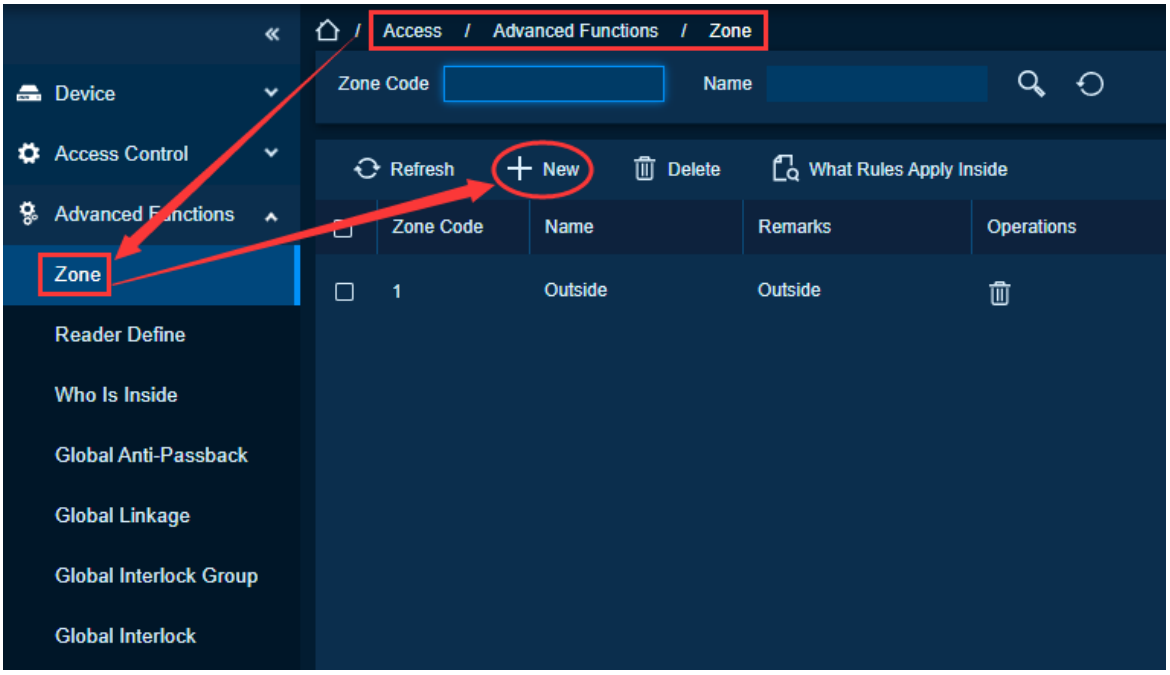
When the device performs advanced access control operations, the area must be set.

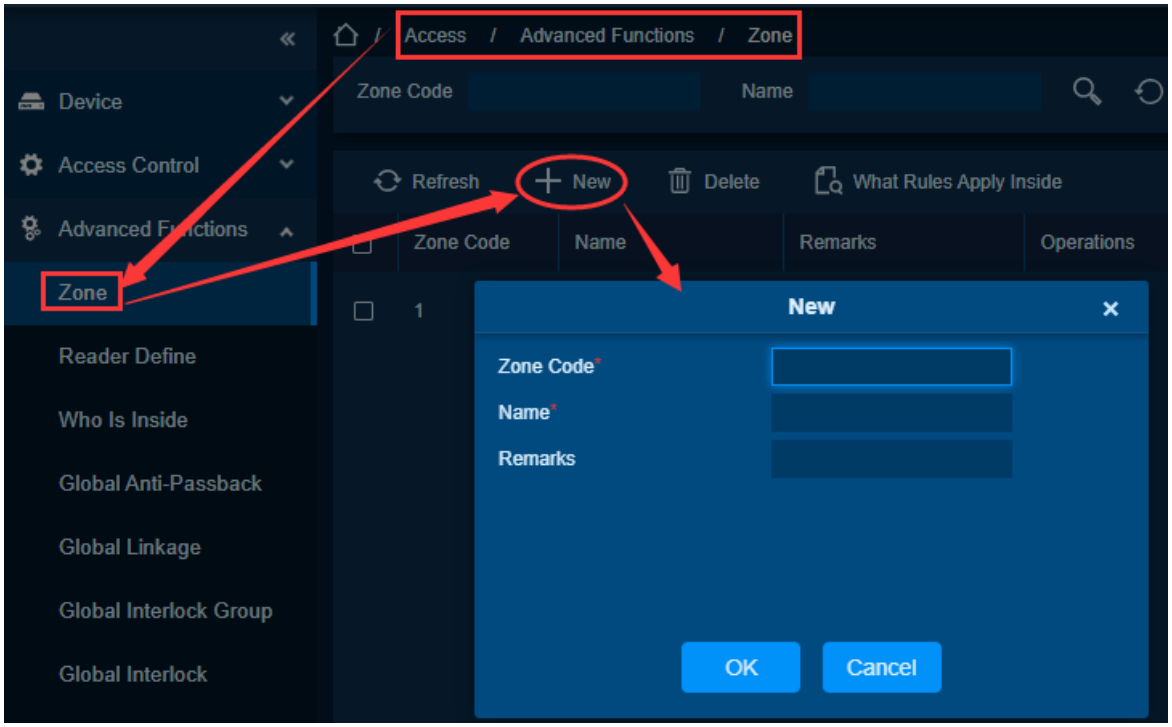
Feature Trigger Result

Add a successful area, you can start to use advanced access control functions.

Steps:

- Click **[Advanced Functions]** > **[Zone]** > **[New]** to enter the Add Zone interface.





- Set Zone Code, Name, Parent Zone, and Remark as required.
- Click **[OK]** to save and quit. The added Zone will appear in the list.

Edit Access Control Area

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

Function Usage Scenarios

The previously set area information is incorrect.

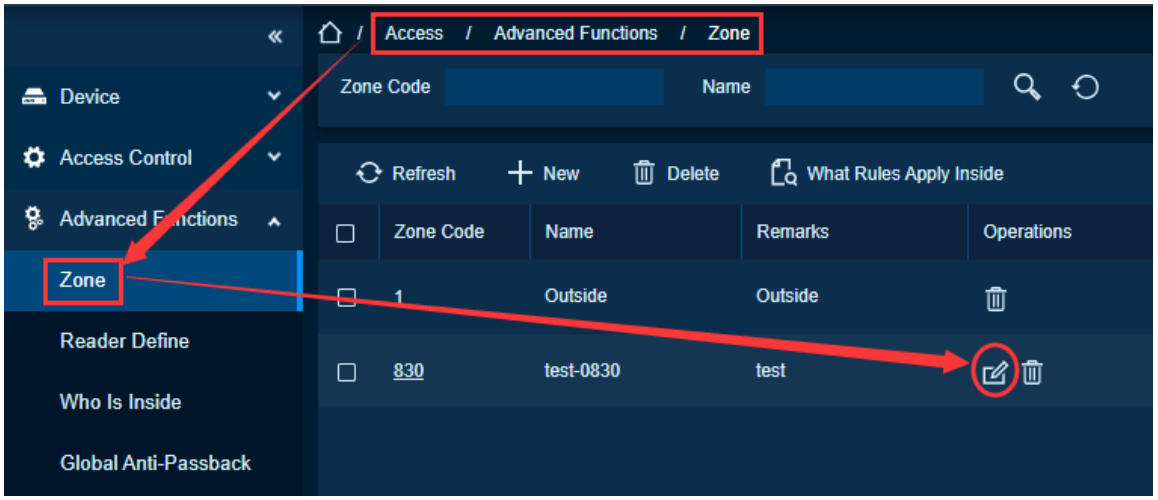
Need to be modified to the new access control area information.

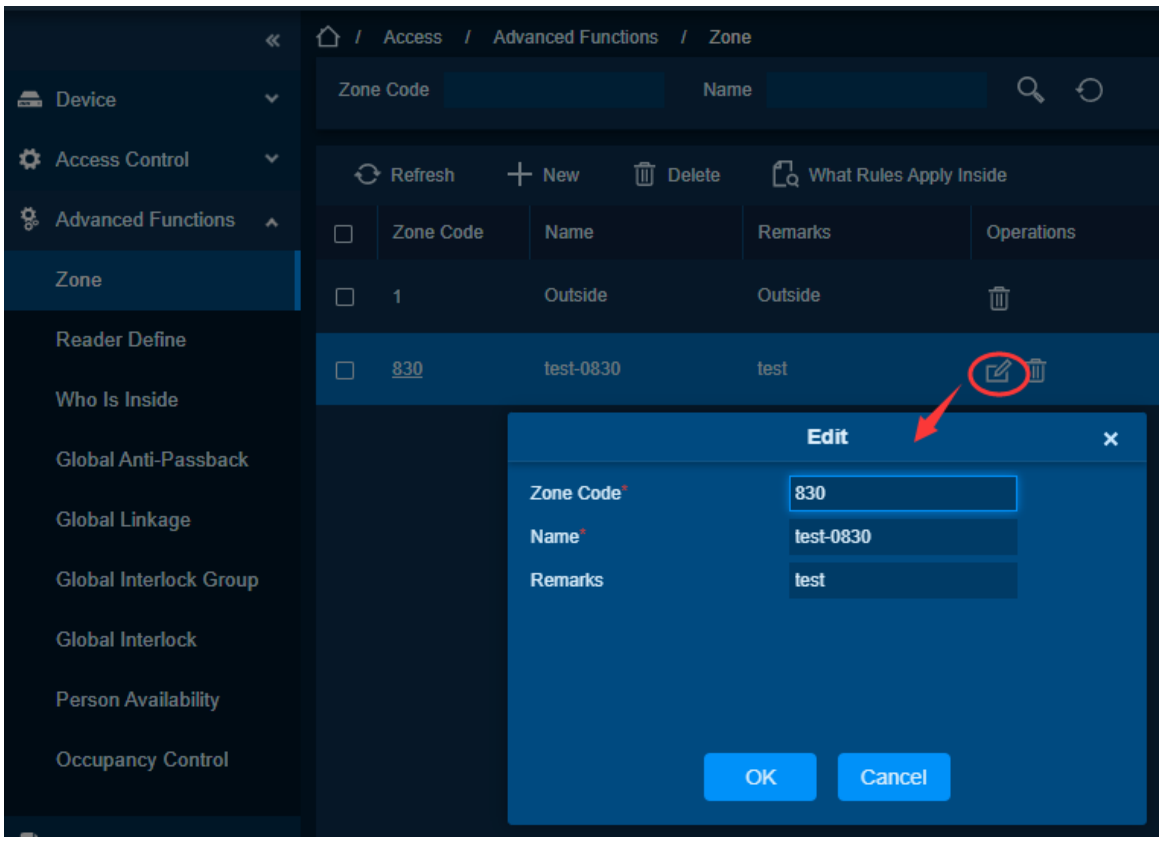
Feature Trigger Result

Modify the successful area, you can start to use the advanced access control function.

Steps:

- Click **[Access] > [Advanced Functions] > [Zone]** to display the access control area interface.
- Select the access control area to be modified and click **[Edit]** to edit.





Delete Access Control Area

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

Function Usage Scenarios

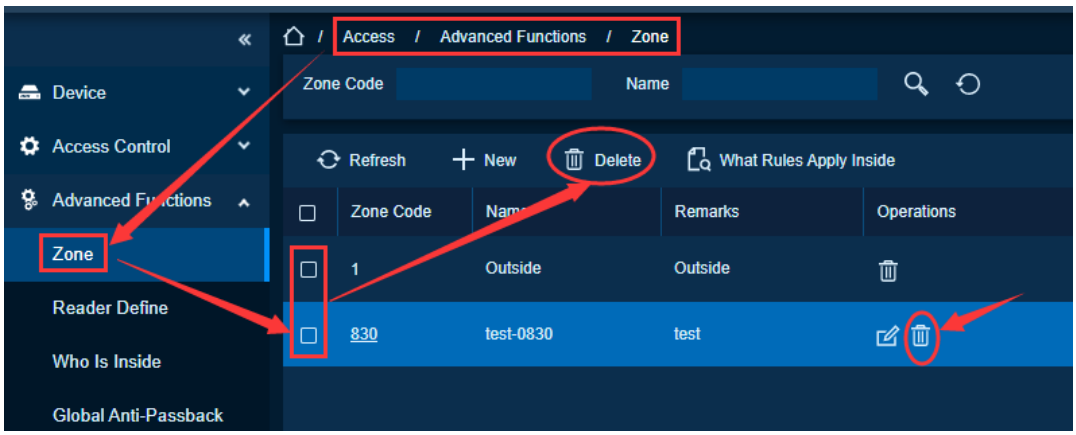
No area information currently set.

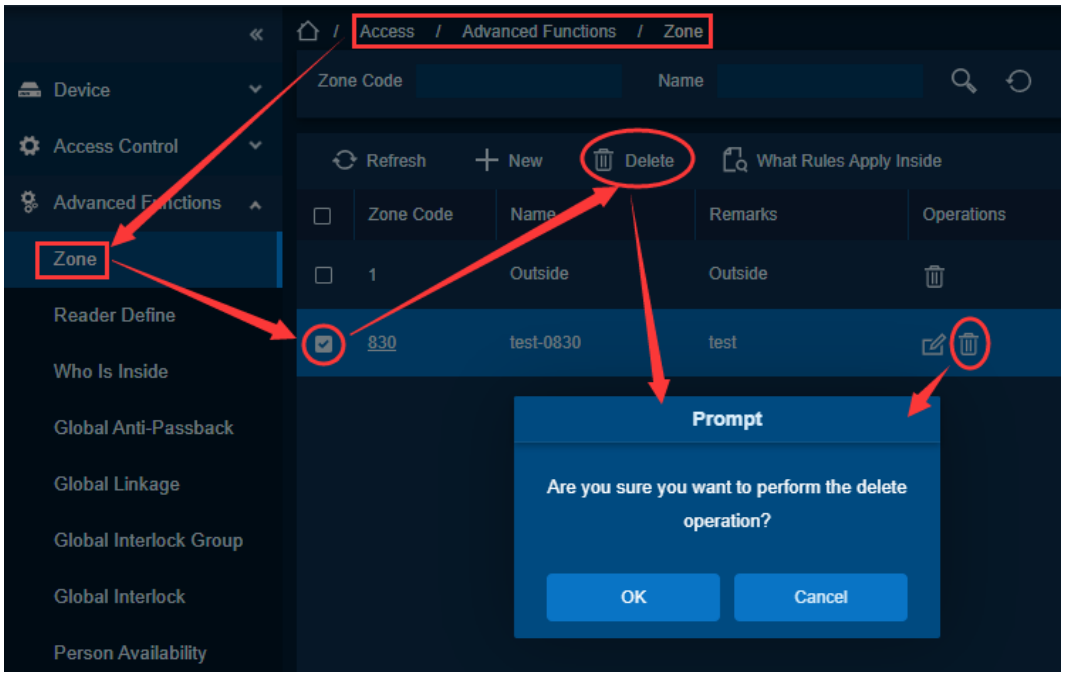
Feature Trigger Result

Advanced access control functions cannot use the access control area.

Steps:

- Click **[Access] > [Advanced Functions] > [Zone]** to display the access control area interface.
- Select the access control area to be deleted and click **[Delete]** to delete the access control area.





What Rules Apply Inside

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

Function Usage Scenarios

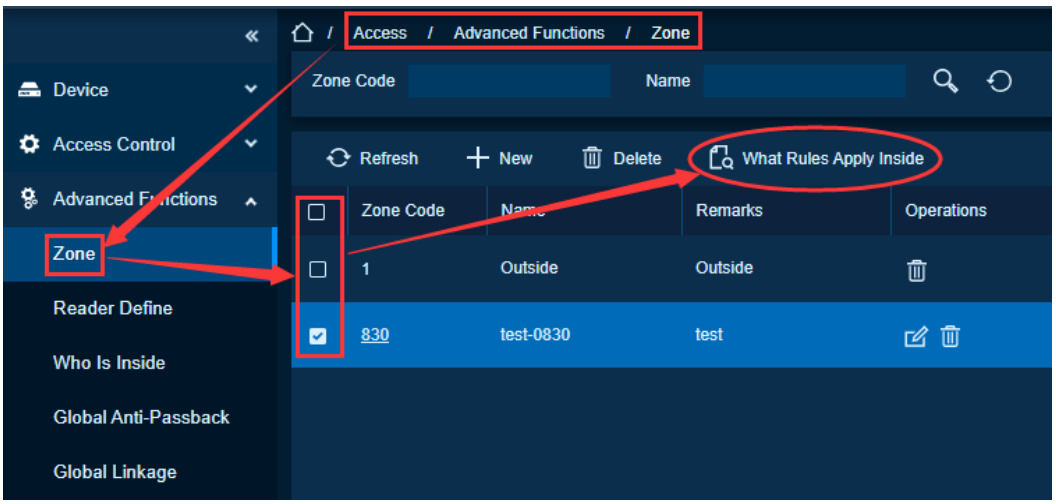
Need to view the type of access control rules that have been set in the current area.

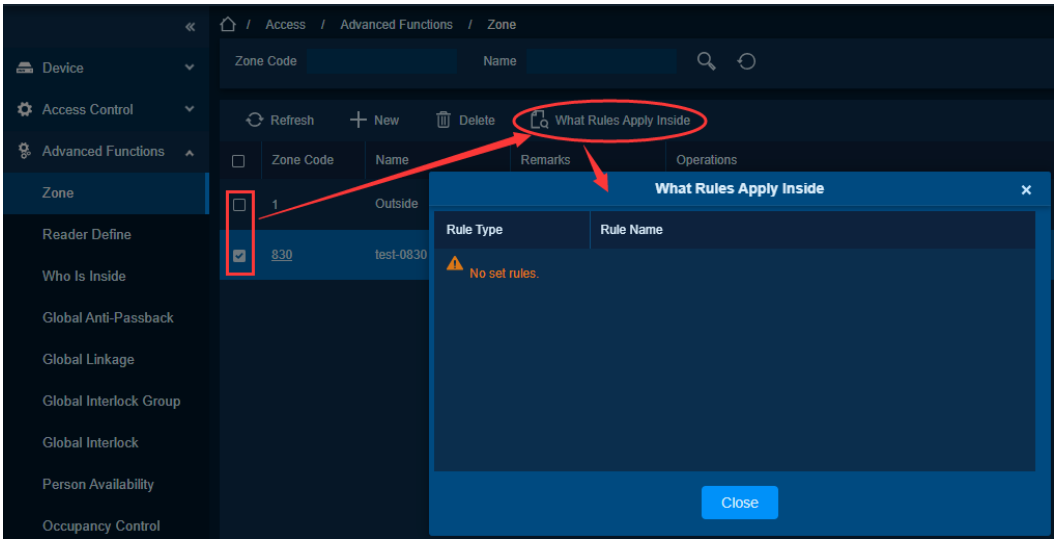
Feature Trigger Result

View the access control rules of the current area, such as global linkage, personnel effectiveness, etc.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Zone]** to display the access control area interface.
- Select the access control area you want to view and click **[What Rules Apply Inside]** to view the access control area rules.





6.3.2. Reader Define

Function Description

Reader Define indicates that Reader control from one access zone to another one, it is based on access zone. If advanced functions are needed, you shall set the Reader Define.

New Reader Definition

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

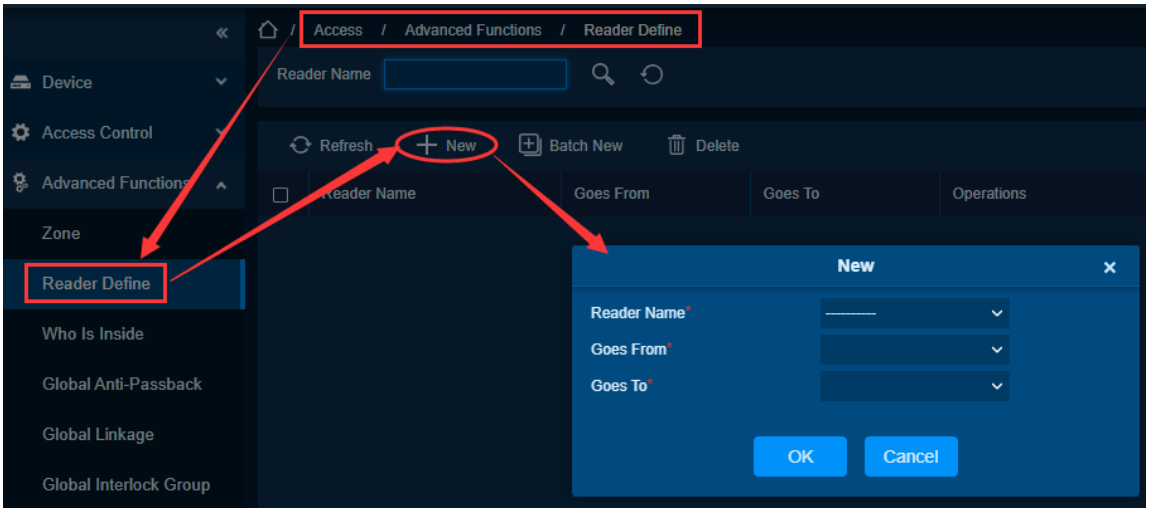
Need to use global anti-passback function.

Feature Trigger Result

The starting access control area of the reader can be added, and the addition is successful, and the global anti-passback can be set.

Steps:

- Click **[Access] > [Advanced Functions] > [Reader Define] > [New]** to enter the add interface.



- Set Reader Name, goes from and Goes To as required.
- Click [**OK**] to save and quit. The added Reader Define will appear in the list.

Add Reader Definitions in Batches

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

Need to use the global anti-passback function.

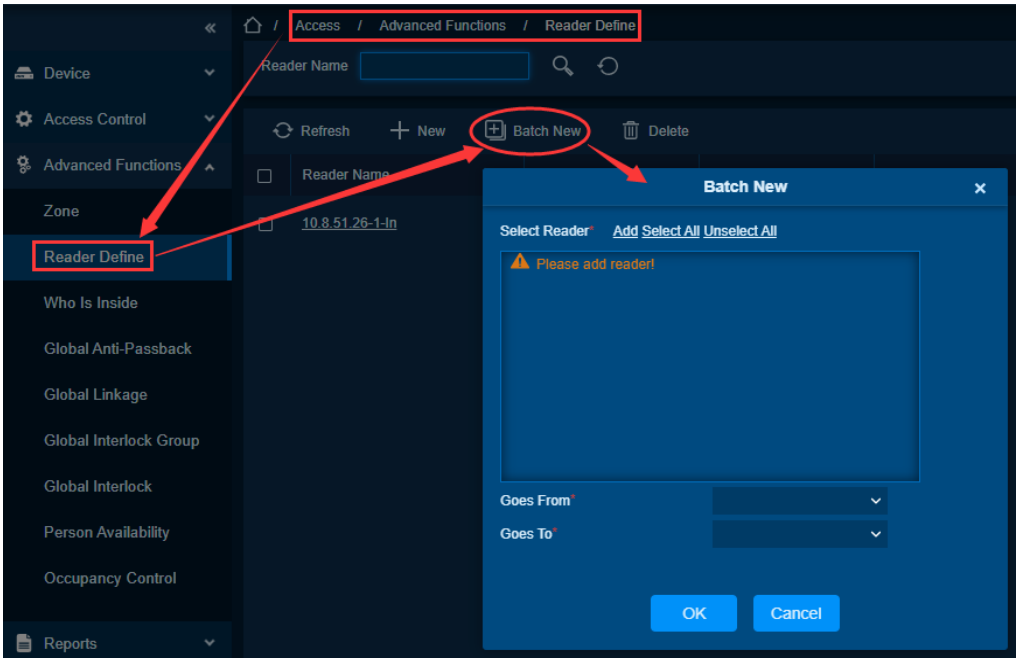
It is necessary to set the same area of multiple reader at the same time.

Feature Trigger Result

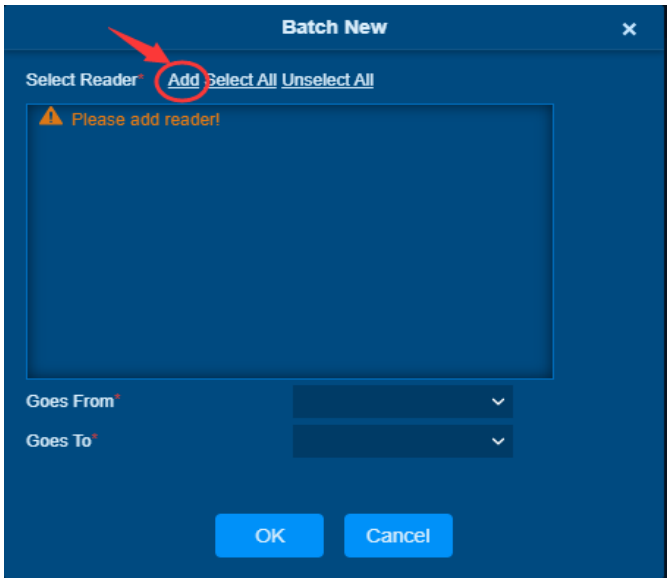
The batch is added successfully, you can set the global anti-passback.

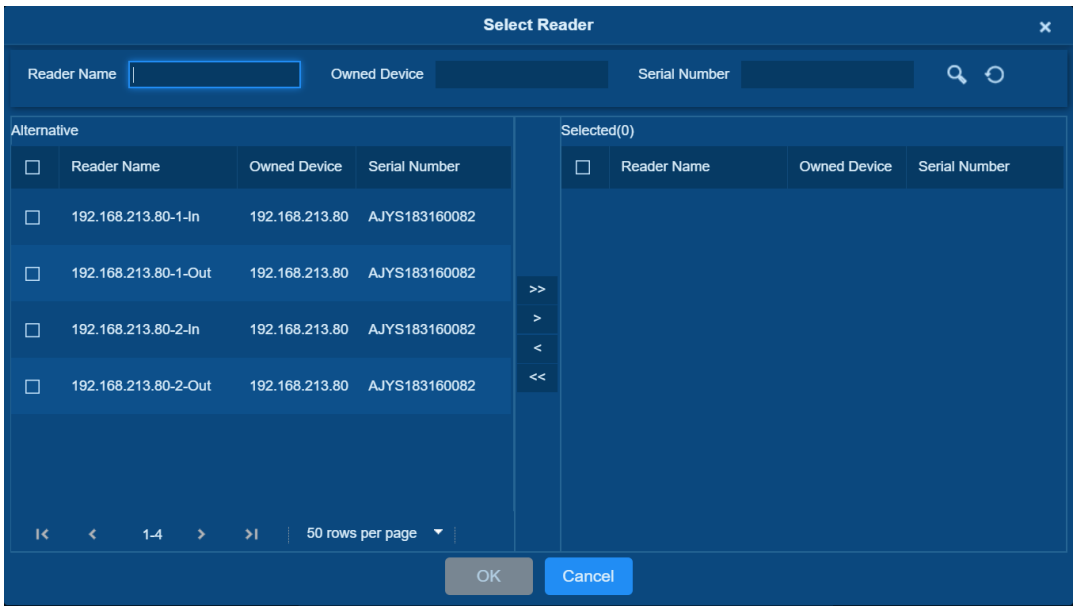
Steps:

- Click **[Access] > [Advanced Functions] > [Reader Define] > [Batch New]** to enter the batch add interface.



- Click **[Add],** select Reader(s) and move towards right and click **[OK].**





Set **Goes from** and **Goes to** as required and press **[OK].**

Edit Reader Definition

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

Need to use the global anti-passback function.

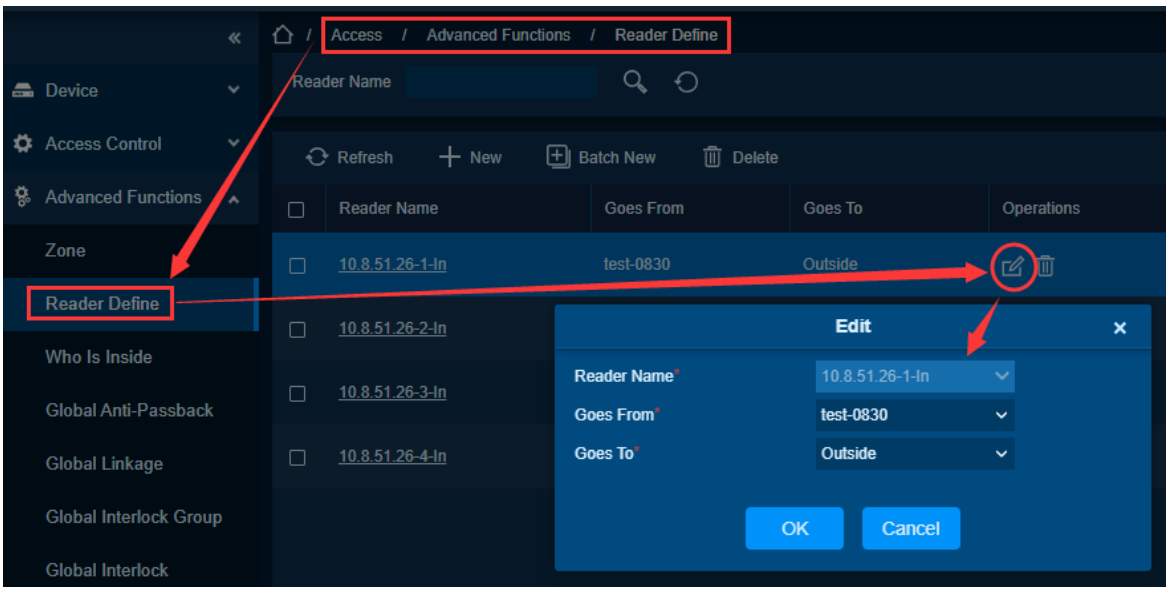
The starting area previously set needs to be modified.

Feature Trigger Result

The batch is added successfully, you can set the global anti-passback.

Steps:

- Click **[Access] > [Advanced Functions] > [Reader Define]** to display the interface of reader definition.
- Select the reader definition to be modified and click **[Edit]** to edit and modify the reader definition.



Delete Reader Definition

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

No need to use global anti-passback function.

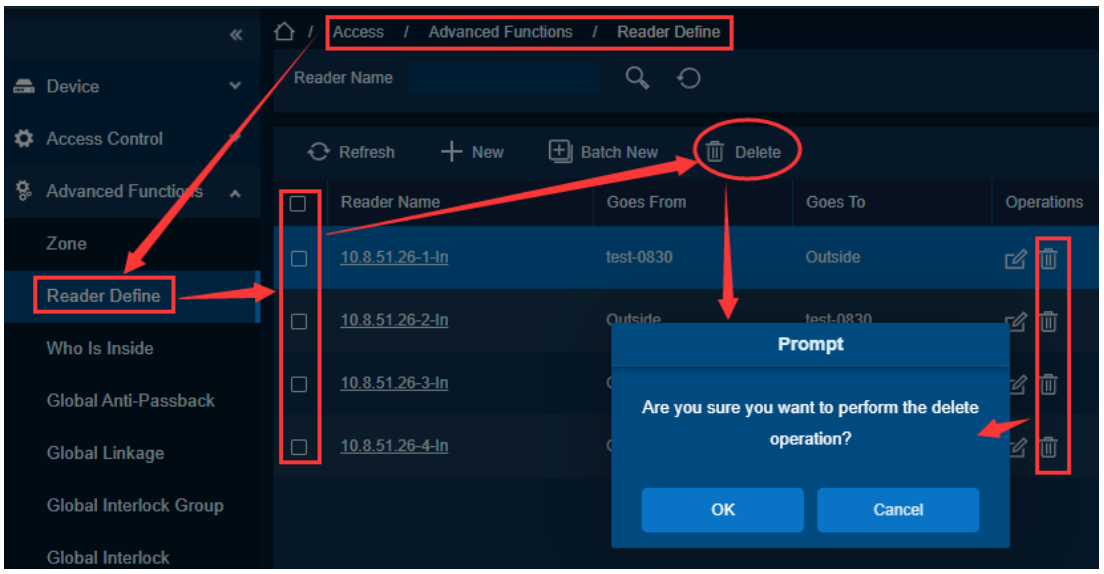
The reader definition is not needed.

Feature Trigger Result

It is not possible to set global anti-passback through this reader.

Steps:

- Click **[Access] > [Advanced Functions] > [Reader Define]** to display the interface of reader definition.
- Select the reader definition to be deleted and click **[Delete]** to delete the reader definition.
- Click **OK** to delete the reader definition.



6.3.3. Who Is Inside

Function Description

After entering the zone, you can view all personnel status in the zone-by-zone tree.

Delete Personnel

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

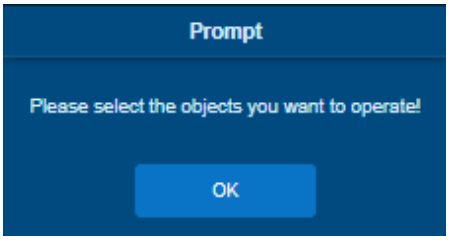
The person needs to be deleted from the access control area. Clear the overall anti-passback status of personnel

Feature Trigger Result

There is no such person in the area, and the person does not have the authority of the area.

Steps:

- Click **[Access] > [Advanced Functions] > [View Personnel in the Area]** to display the area personnel interface.
- Select the person to be deleted and click **[Delete]** to delete the person



Export

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

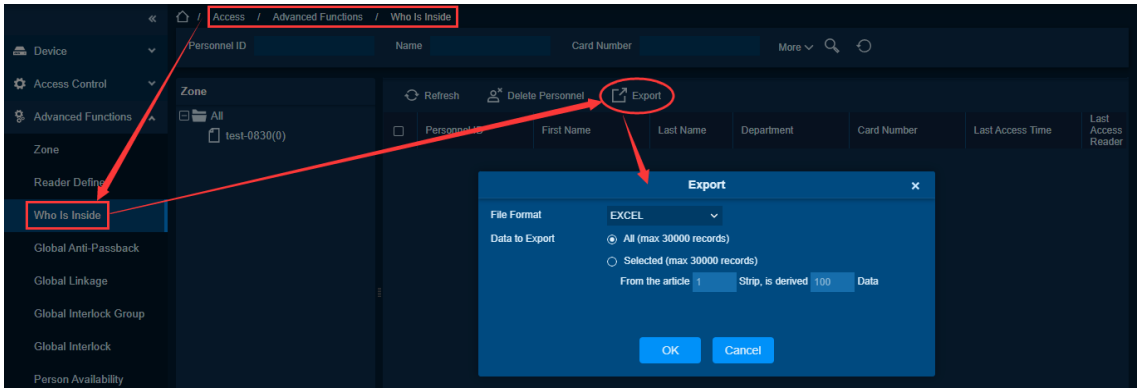
Need to view personnel and personnel information in various regions in the form of files.

Feature Trigger Result

You can export a variety of formats excel/pdf/csv files.

Steps:

- Click **[Access] > [Advanced Functions] > [Who is inside]** to display the area personnel interface.
- Click **[Export]** to export area personnel information.



6.3.4. Global Anti-Passback

Function Description

Global Zone APB can set Anti-Passback across devices; you can use this function after setting Global Anti-passback. You must set Access Zone and Reader Define before using, and the device that has set Anti-Passback shall issue background verification parameters.

New Global Anti-Passback

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

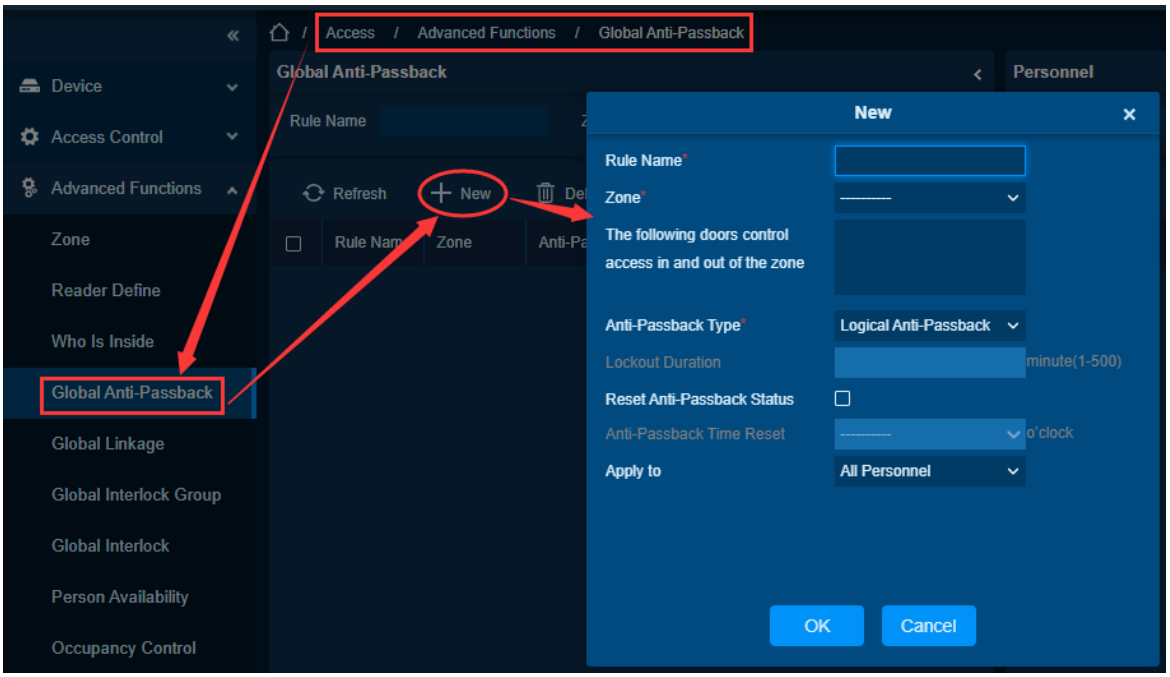
- Place with high safety requirements need to control the entry and exit of personnel
- Anti-Passback settings across devices are required.

Feature Trigger Result

According to anti-passback rules, as well as anti-passback personnel, control personnel entry and exit.

Steps:

Click **[Access]> [Advanced Functions] > [Global Anti-Passback] > [New]** to enter the add interface.



Set Rule Name (Unrepeatable), Zone, Anti-passback Type, Lockout Duration, Reset Anti-passback Status and When to Reset the Anti-passback as required.

Zone: Select an option from the dropdown list, Corresponding doors will display in the text box of "The following doors control access in and out of the zone". At the same time, the doors obey the rule of one door cannot set as the boundary of two independent Anti-passback.

Anti-passback Type: Logical Anti-passback, Timed Anti-passback or Timed Logic Anti-passback.

Logical Anti-passback: The door will not open if the entry and exit records is not in consistent with Anti-passback zone.

Timed Anti-passback: In specified time, user can enter Anti-passback zone only once. After the Time period has expired, user state will be cleared, and allow user to enter this zone again.

Timed Logic Anti-passback: In Specified time, Users who enter Anti-passback zone must obey the rule of Logical Anti-passback. If users exceed timed period, system will time again.

Lockout Duration: Only select Timed Anti-passback and Timed Logic Anti-passback in Anti-passback Type. Lockout Duration can be set.

Reset Anti-passback Status: Tick it to clear Anti-passback status of personnel in the system and recover initial state. Only tick this option. When to Reset the Anti-passback can be select. After the reset time of the anti-passback has expired, system will clear all the Anti-passback status of personnel in zone.

When to Reset the Anti-passback: Select time to reset Anti-passback.

Apply to: All Personnel, Just Selected Personnel and Exclude Selected Personnel three types.

Apply to All Personnel: Can only edit and does not support select personnel.

Apply to Just Selected Personnel: The anti- passback is only effective for these selected personnel.

Apply to Exclude Selected Personnel: The anti- passback only effective for these exclude selected personnel.

Click **[OK]** to save and quit. The added Global Zone APB will display in the list.

Add Personnel

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

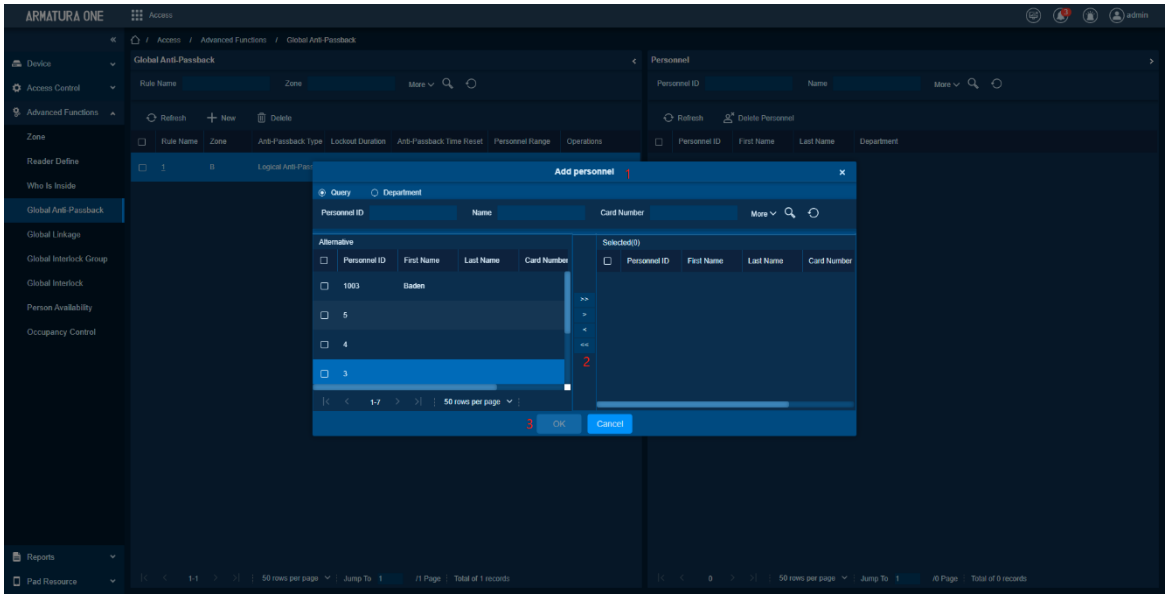
Need to add personnel to the new global anti-passback.

Feature Trigger Result

The added personnel can enter and exit according to the set anti-passback rules.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Anti-Passback]** to display the area personnel interface.
- Select the anti-passback rule of the person to be added and click **[Add Person]** to add.



Delete Personnel

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.

- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

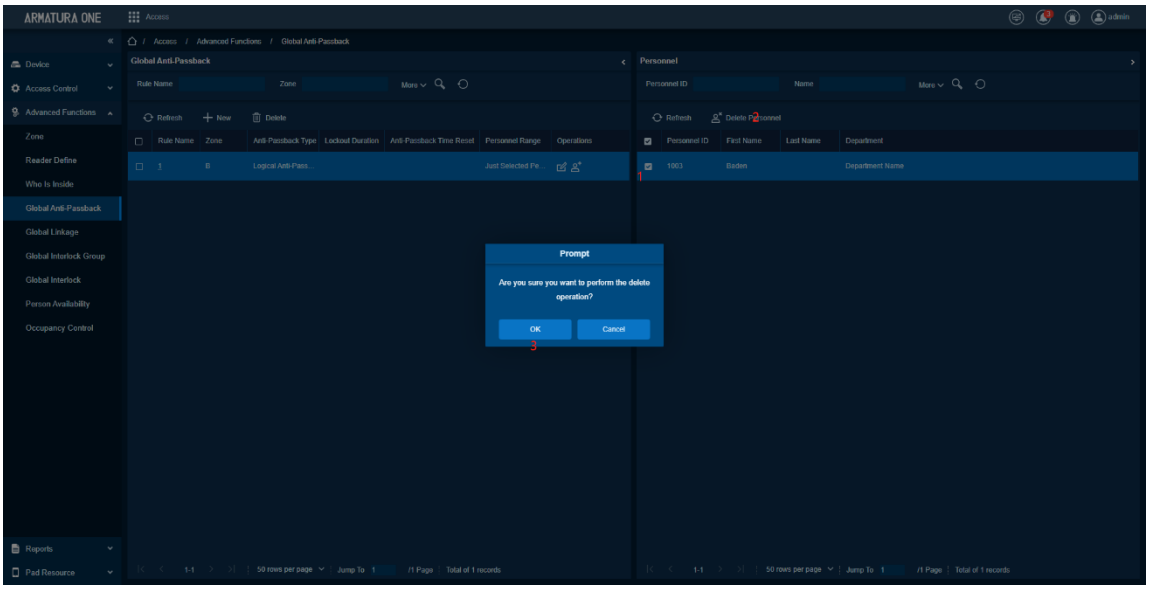
The current global anti-passback personnel do not need to perform anti-passback operations anymore.

Feature Trigger Result

Deleted personnel cannot enter and exit according to the set anti-passback rules.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Anti-Passback]** to display the area personnel interface.
- Select the anti-passback rule of the person to be deleted and click **[Delete Person]** to delete.



Delete Anti-Passback Rules

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

The current anti-passback rules are wrong.

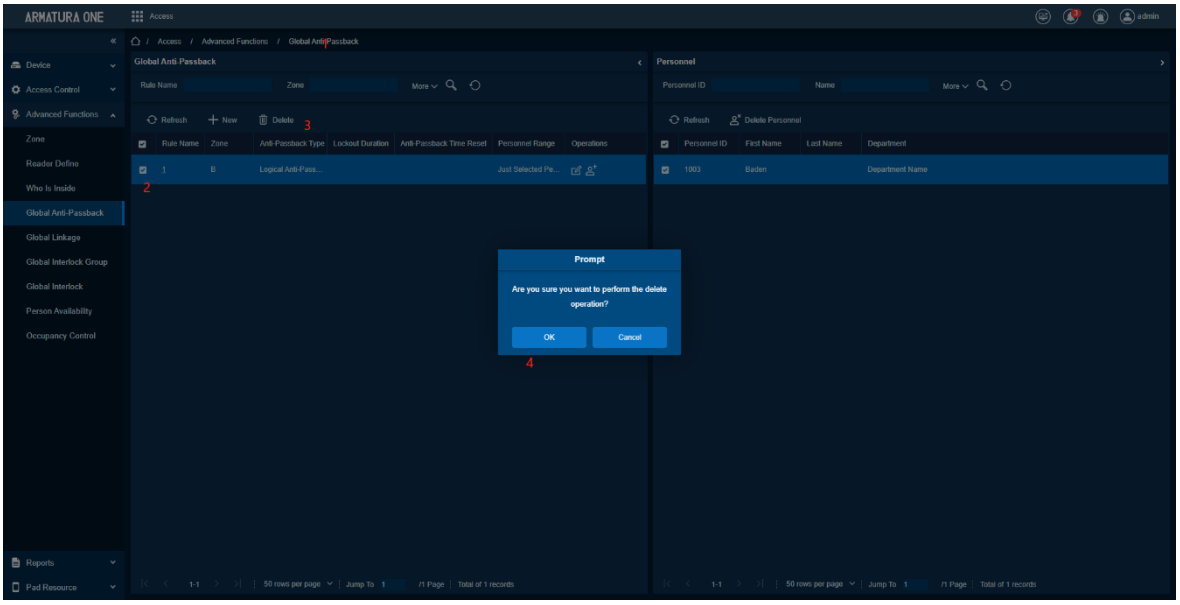
No need to perform anti-passback operations.

Feature Trigger Result

Delete the global anti-passback rule

Steps:

- Click **[Access] > [Advanced Functions] > [Global Anti-Passback]** to display the area personnel interface.
- Select the anti-passback rule you want to delete and click **[Delete]** to delete.



6.3.5. Global Linkage

Function Description

The global linkage function allows you to configure data across devices. At the same time, you can set the action of the door and auxiliary output, as well as the video linkage, the effective period of the linkage, and the type of notification of linkage events.

New Global Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.

Function Usage Scenarios

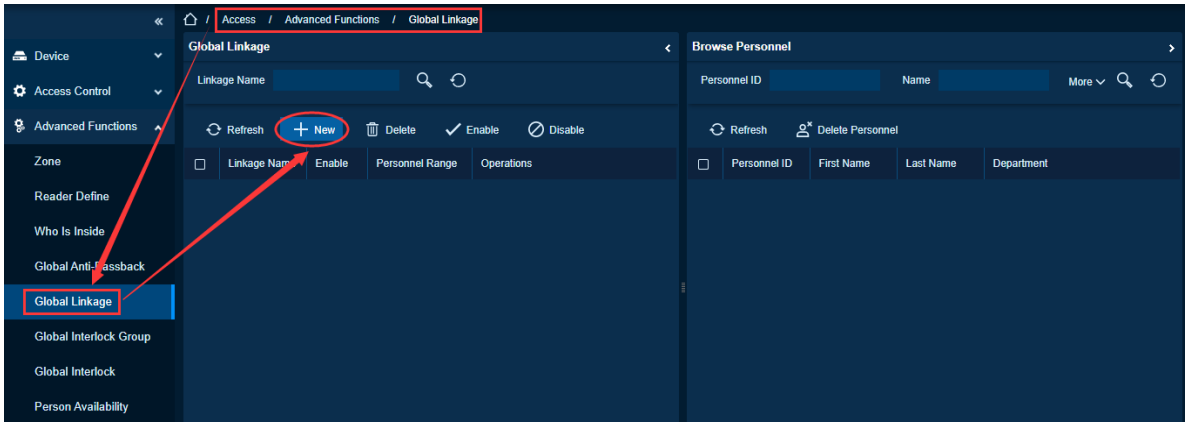
Need to set up linkage across devices.

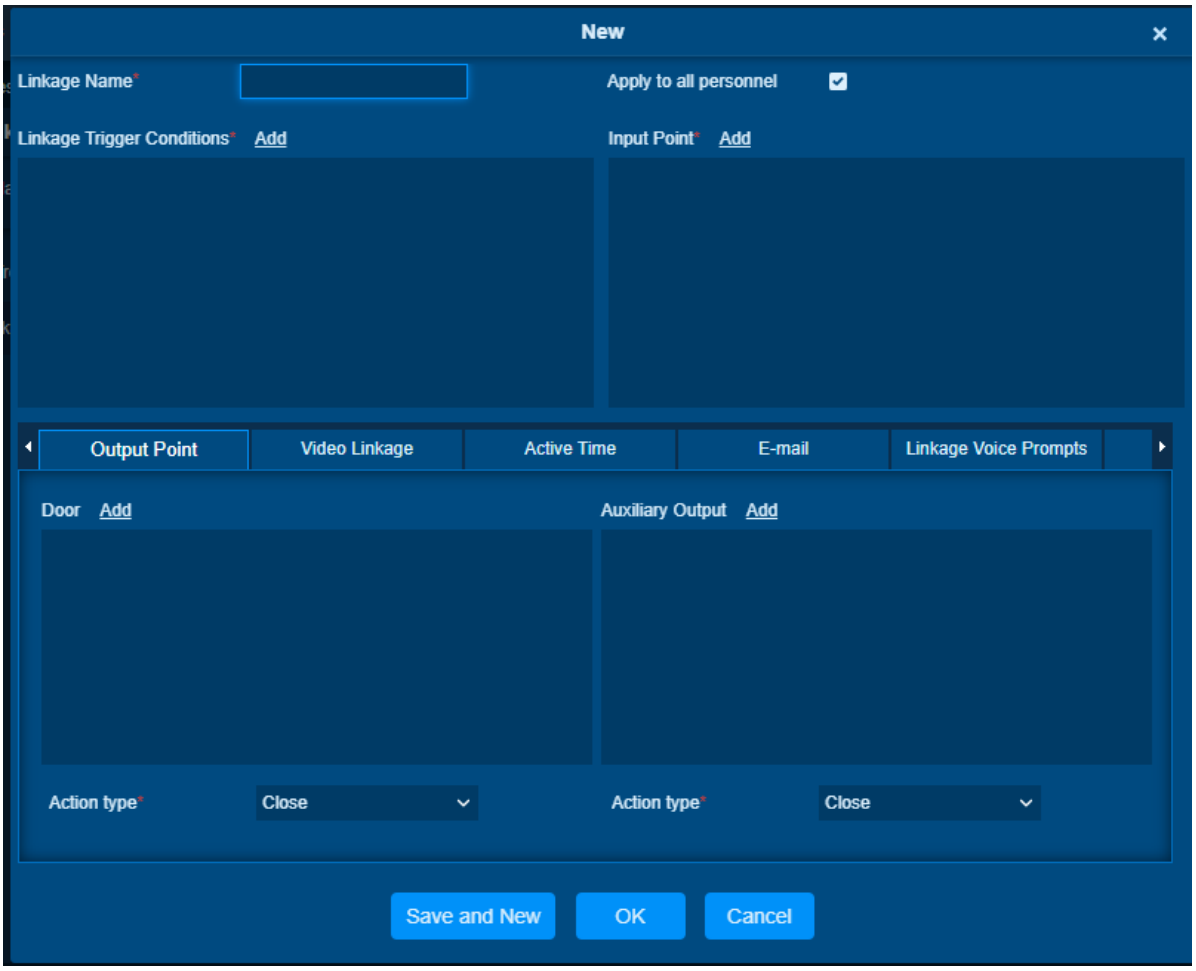
Feature Trigger Result

Linkage control can be carried out across devices.

Steps:

Click **[Advanced Functions] > [Global Linkage] > [New].**





Apply to all personnel: If this option is selected, this linkage setting is effective for all personnel.

Active Time: Set the active time of the linkage setting.

Choose Global Linkage trigger conditions, the input point (System will filter devices according to the choice in first step) and the output point, Set up linkage action. For more details about these parameters, please refer to Linkage Setting.

✍**Note:**

You can select multiple Door Events, but “Fail to connect server”, “Recover connection” and “Device

connection off" will be filtered automatically from Door Event.

Click **[OK]** to save and quit. The added Global Linkage will display in the list.

Edit Global Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.

Function Usage Scenarios

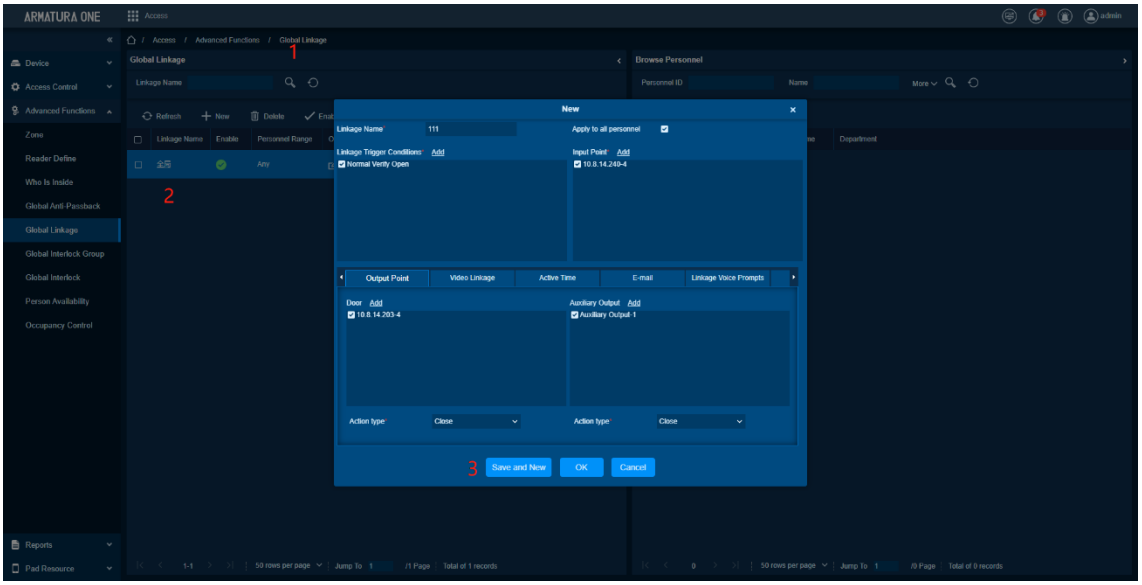
Need to modify the linkage settings of the previous device.

Feature Trigger Result

Linkage control can be carried out across devices.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Global Linkage]** to display the global linkage interface.
- Select the linkage you want to edit and click **[Edit]** to enter the editing interface.



Delete Personnel

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

Delete the personnel in the device linkage settings.

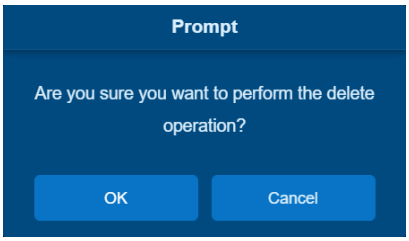
Feature Trigger Result

There is no person deleted in the linkage, and the person cannot perform the corresponding linkage

operation.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Linkage]** to display the global linkage interface.
- Select the linkage event of the person to be deleted and click **[Delete Person]** to delete.



Delete Global Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

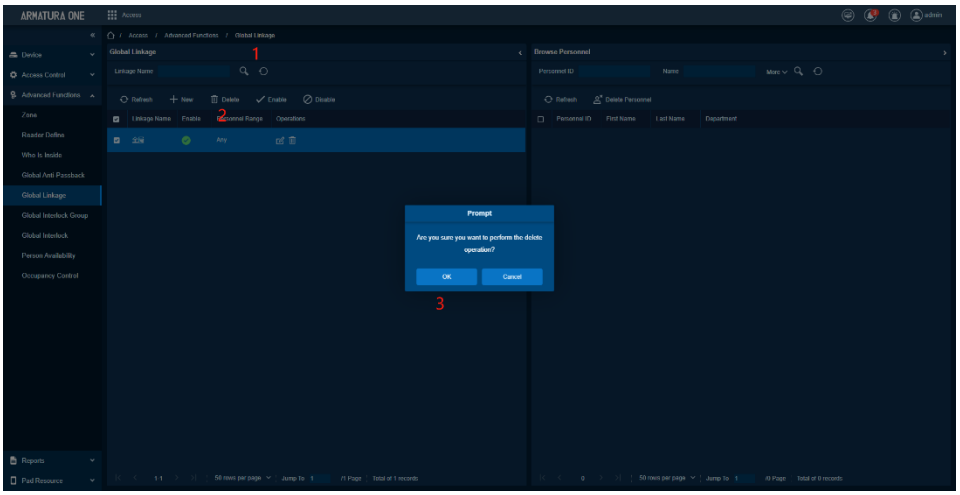
No need for this global linkage.

Feature Trigger Result

Delete the global linkage, the corresponding linkage operation cannot be performed.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Linkage]** to display the global linkage interface.
- Select the linkage event you want to delete and click **[Delete]** to delete.



Enable Global Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.

- There is an access control area.
- The global linkage is disabled.

Function Usage Scenarios

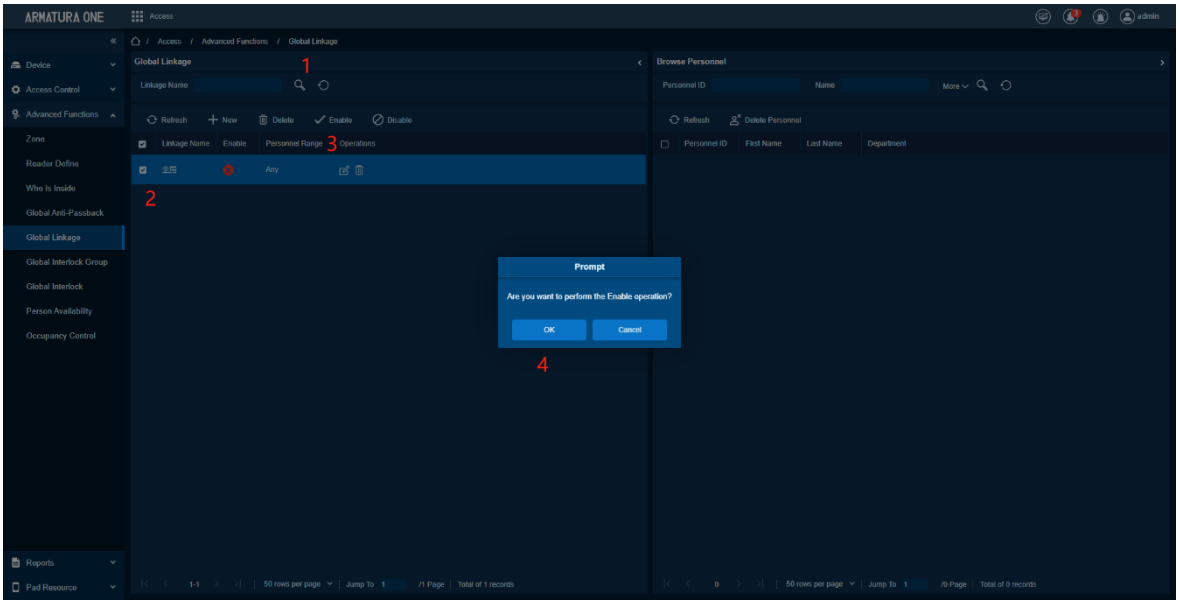
Need to use this global linkage

Feature Trigger Result

Enable this global linkage, the icon turns green, and you can perform corresponding linkage operations.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Linkage]** to display the global linkage interface.
- Select the linkage event you want to enable and click **[Enable]** to enable.



Disable Global Linkage

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.
- The global linkage is enabled.

Function Usage Scenarios

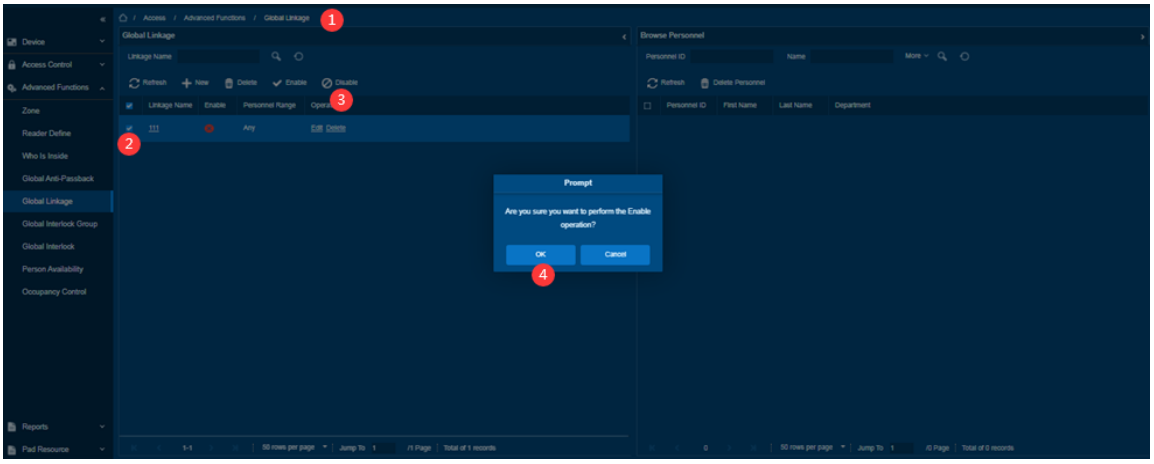
Temporarily disable this global linkage.

Feature Trigger Result

Disable the global linkage, the icon turns red, and the corresponding linkage operation cannot be performed.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Linkage]** to display the global linkage interface.
- Select the linkage event to be disabled and click **[Disable]** to disable.



6.3.6. Global Interlock Group

Function Description

The global interlock group groups the doors in the global interlock, but to use the global interlock function, the device must be enabled with background authentication.

New Global Interlock Group

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module, and the background verification function is turned on.

Function Usage Scenarios

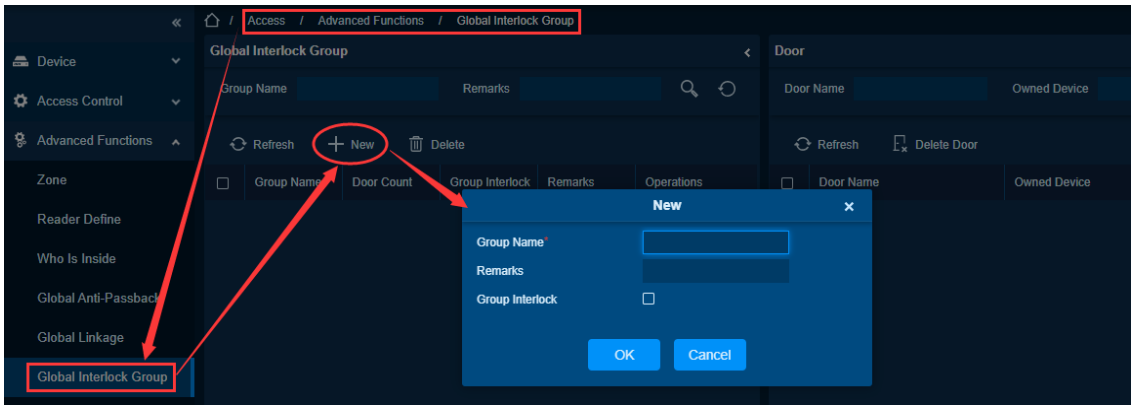
Group the doors to be globally interlocked later.

Feature Trigger Result

Can be used for subsequent global interlock.

Steps:

Click **[Access]> [Advanced Functions] > [Global Interlock Group]> [New].**



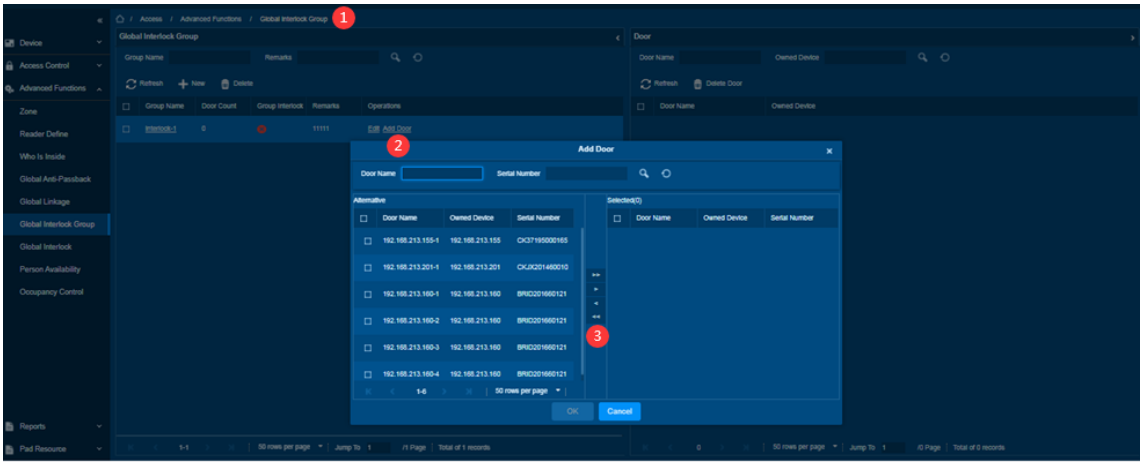
Group Name: Any combination of up to 30 characters that cannot be identical to an existing group name.

Group Interlock: If the option is selected, set global interlock rule for the interlocking group.

After editing, click **[OK]** to save. After confirming that add the door immediately, the information of added door will appear in the list.

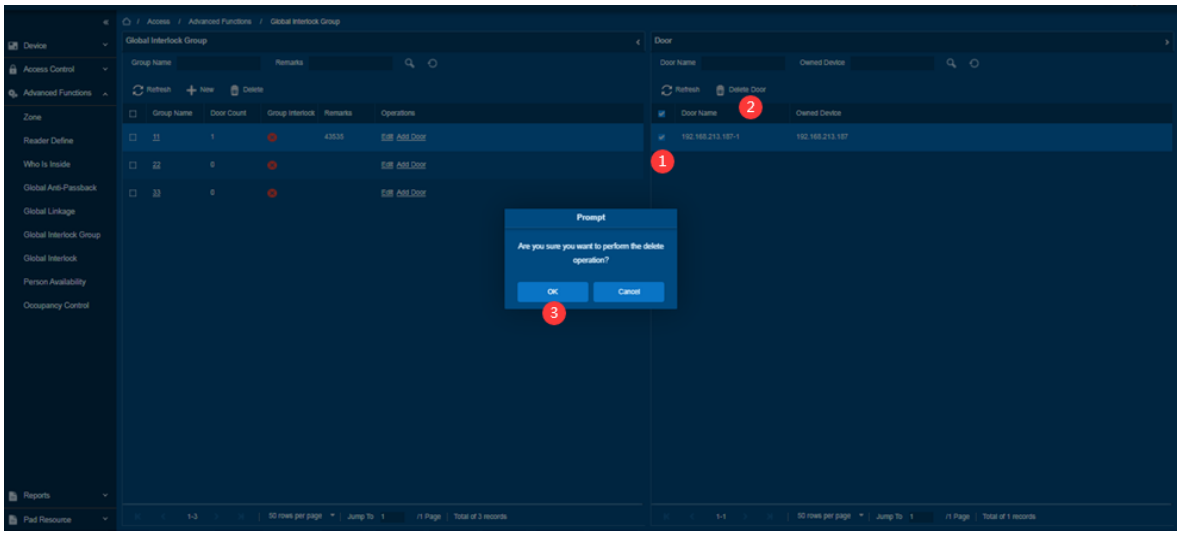
Add Door

- Click **[Access] > [Advanced Functions] > [Global Interlock Group]** to display the global interlock group interface
- Select the interlocking group to be added and click **[Add Door]** to add.



Delete the door

- Click [**Access] > [Advanced Functions] > [Global Interlock Group]** to display the global interlock group interface.
- Select the interlock group of the door to be deleted and click **[Delete Door]** to delete.



Edit Global Interlock Group

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.

- The device has been added to the access control module, and the background verification function is turned on.
- There is an access control area.

Function Usage Scenarios

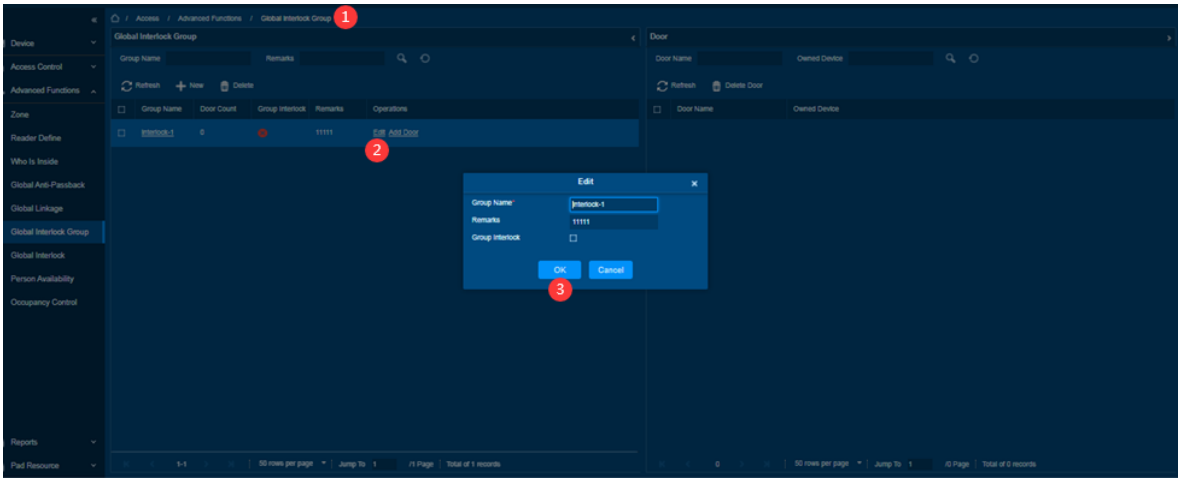
Edit the grouping of doors to be globally interlocked state.

Feature Trigger Result

Can be used for subsequent global interlock.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** to display the global interlock group interface.
- Select the global interlock group to be modified and click **[Edit]** to edit.



Delete Global Interlock Group

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module, and the background verification function is turned on.
- There is an access control area.

Function Usage Scenarios

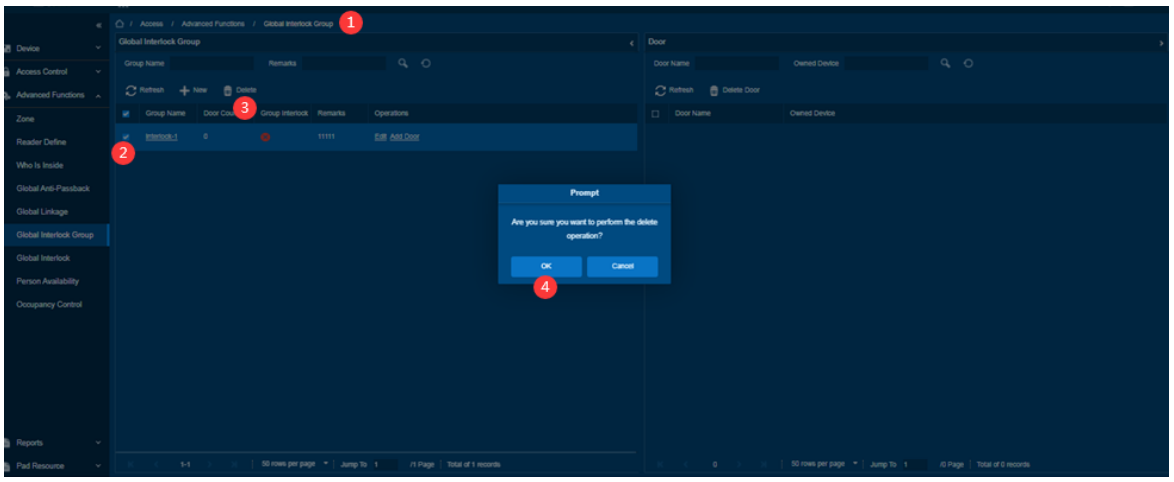
Does not require the door grouping in the current global interlock.

Feature Trigger Result

Subsequent global interlocks cannot be used.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Global Interlock Group]** to display the global interlock group interface.
- Select the global interlock group to be deleted and click **[Delete]** to delete.



6.3.7. Global Interlock

Function Description

The global interlock function allows you to configure data across devices.

Add Global Interlock

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.

Function Usage Scenarios

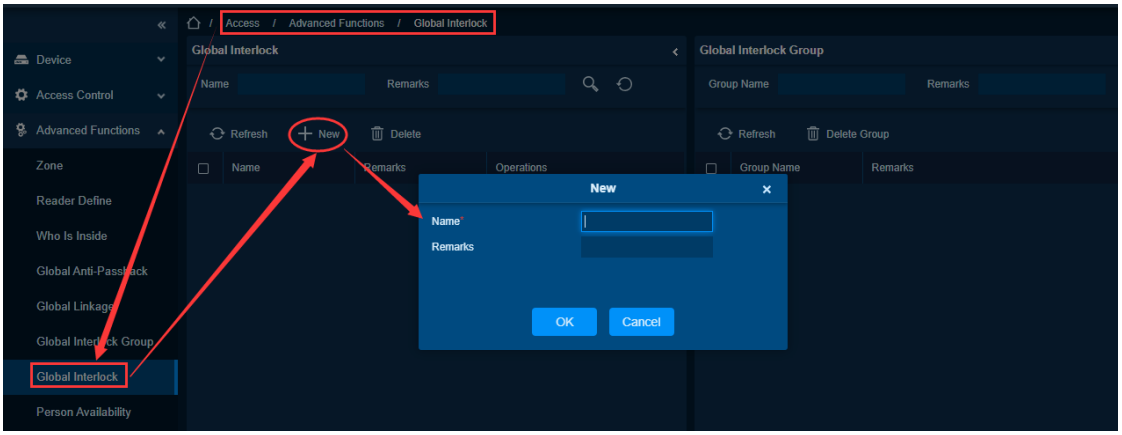
Need to interlock settings across devices.

Feature Trigger Result

It can be interlocked across devices.

Steps:

Click **[Access] > [Advanced Functions] > [Global Interlock]> [New]**.



Name: Enter any name (any combination of up to 30 characters that cannot be identical to an existing

name).

✍**Note:**

In the same interlock, all the doors in the group cannot be duplicated.

If the interlock group exists in the interlock function, it cannot be deleted directly.

Edit Global Interlock

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.

Function Usage Scenarios

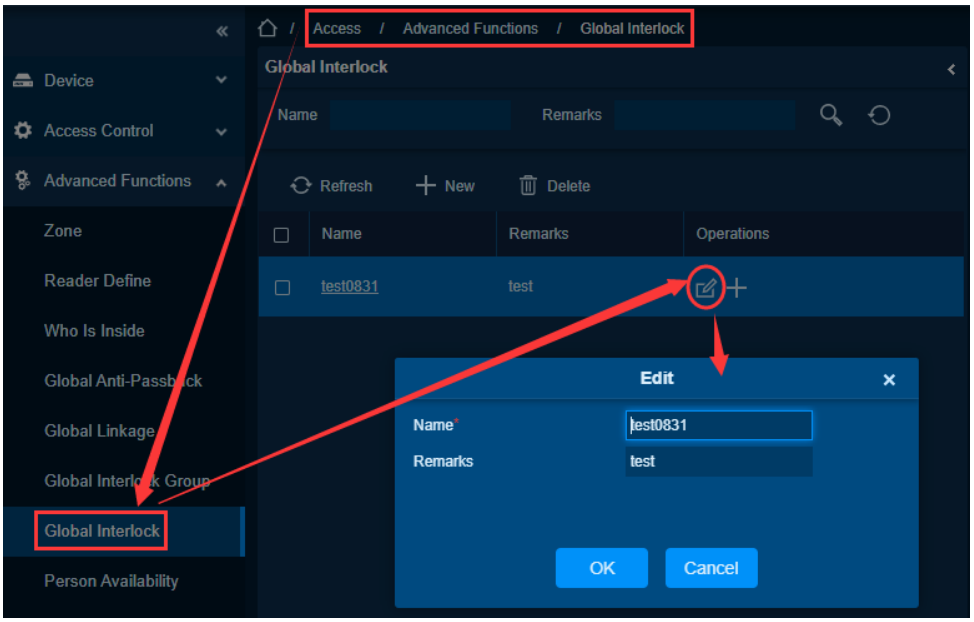
Need to modify the interlock settings across devices.

Feature Trigger Result

It can be interlocked across devices.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Interlock]** to display the global interlock interface.
- Select the global interlock to be edited and click **[Edit]** to enter the editing interface.



Delete Global Interlock

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- There is an access control area.

Function Usage Scenarios

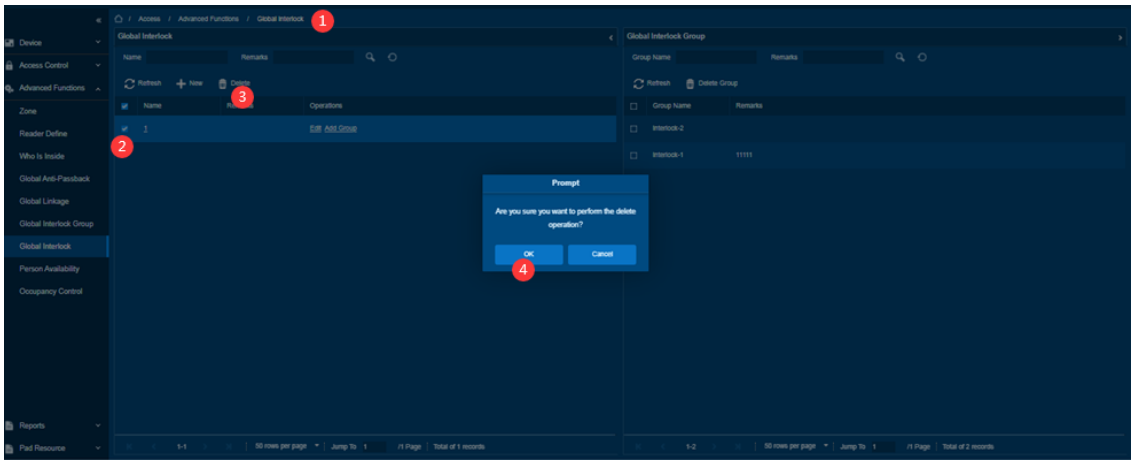
No need for this cross-device interlock settings.

Feature Trigger Result

The interlock can no longer be used.

Steps:

- Click **[Access] > [Advanced Functions] > [Global Interlock]** to display the global interlock interface.
- Select the global interlock to be deleted and click **[Delete]** to enter the delete interface.



6.3.8. Person Availability

Function Description

It is mainly used to limit valid date/ after the first use of valid days/ use number of times of personnel in advanced access control area.

Set Access Control Area Attributes

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

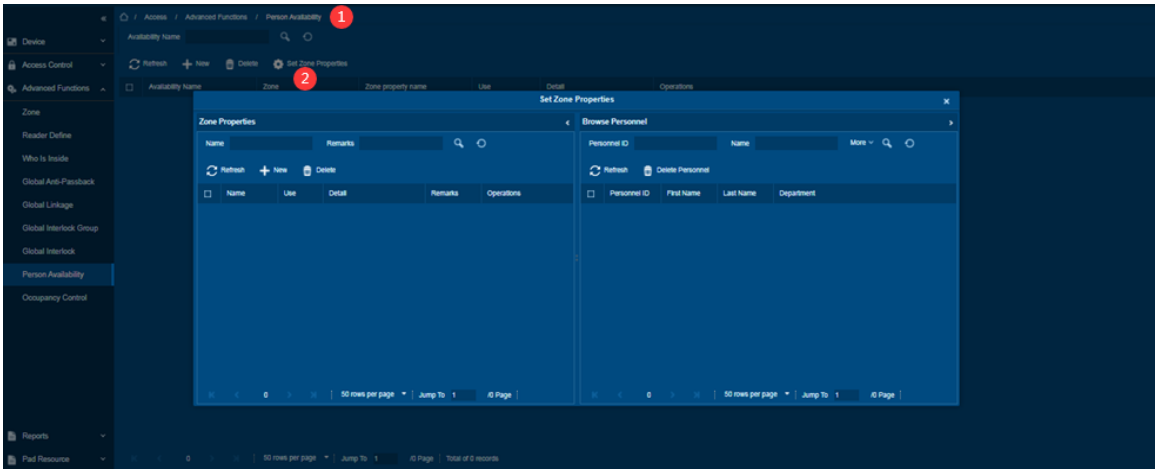
You can assign the set access control area attributes to the corresponding personnel

Feature Trigger Result

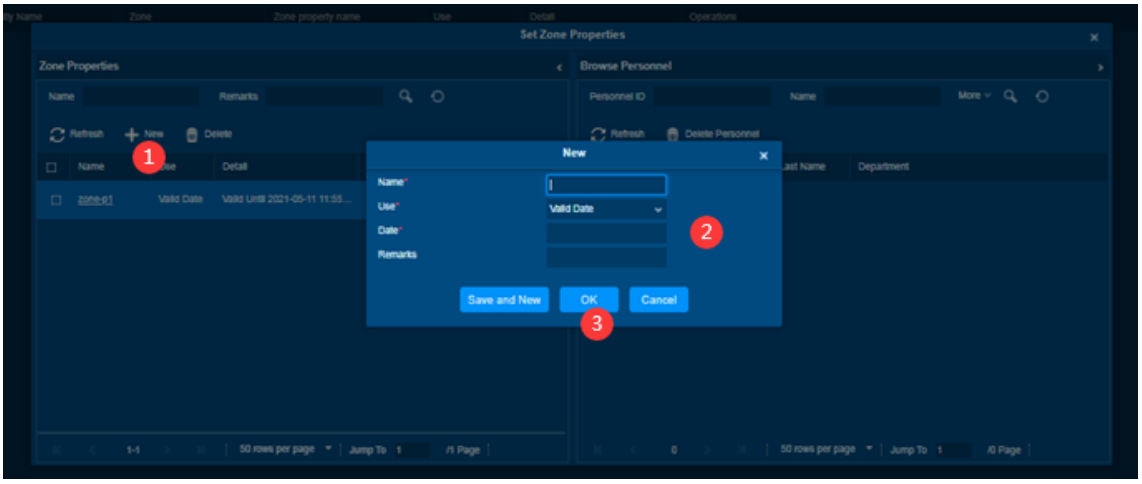
Configure personnel in a specific access control area according to the attributes of the access control area

Steps:

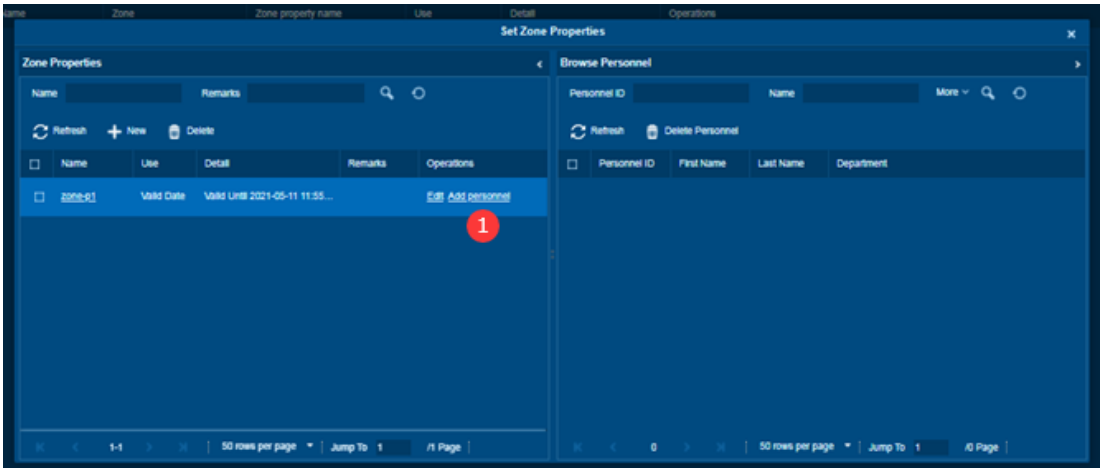
- Click **[Access] > [Advanced Functions] > [Personnel Validity]** to display the personnel validity interface
- Click **[Set Access Control Area Properties]** to enter the setting interface.



- Click [Add] to add the attributes of the access control area.
- You can choose the usage method: effective date, effective days after first use, number of uses.



Add the Personnel of this Access Control Attribute



Add Personnel Effectiveness

Preconditions for Normal Use of Function

- Log in to the system with the current account and have the menu authority.
- The device has been added to the access control module.
- There is an access control area.

Function Usage Scenarios

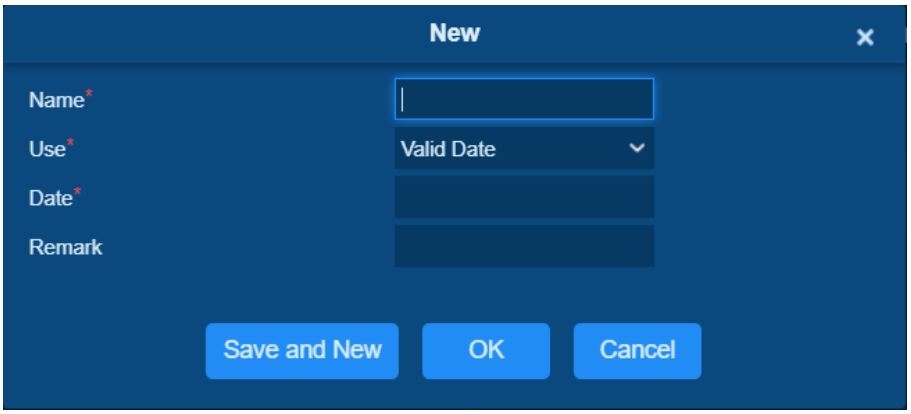
It is necessary to limit the effective days/use times of personnel.

Feature Trigger Result

Control the effective time of personnel in a specific access control area.

Steps:

Click **[Advanced Functions] > [Person Availability] > [Set Zone Properties] > [New]**, the following interface will be shown.



Use: It is divided into Valid Date, after the first use of valid days and Use number of times, corresponding to Date, Days and Times.

Edit Personnel Effectiveness

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority. The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

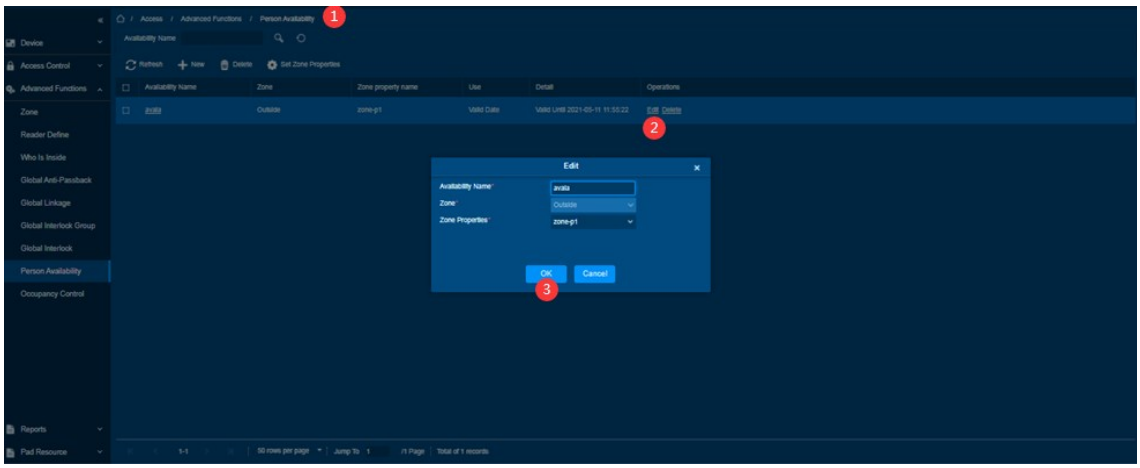
It is necessary to modify the restrictions on the effective days/use times of personnel.

Feature Trigger Result

Control the effective time of personnel in a specific access control area.

Steps:

- Click **[Access] > [Advanced Functions] > [Personnel Availability]** to display the staff effectiveness interface.
- Select the validity of the personnel to be edited and click **[Edit]** to enter the editing interface.



Delete Personnel Effectiveness

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority. The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

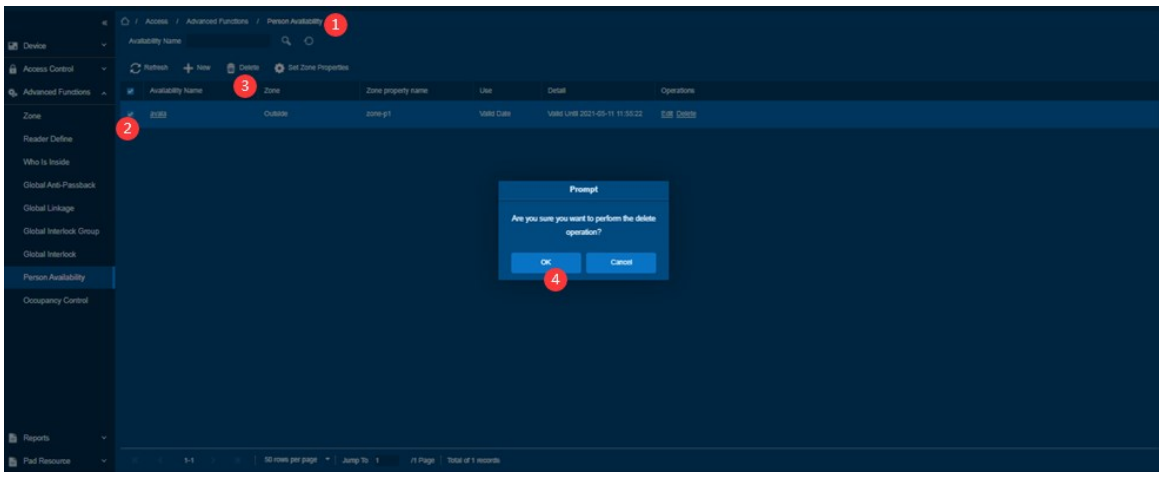
There is no need to limit the number of effective days/uses for personnel.

Feature Trigger Result

It is not possible to control the effective time of personnel in a specific access control area.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Person Availability]** to display the staff effectiveness interface.
- Select the validity of the person to be deleted and click **[Delete]** to enter the delete interface.



6.3.9. Occupancy Control

Function Description

It is mainly used to control the upper and lower limits of the number of people in the area.

Add Number of People Control

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority. The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

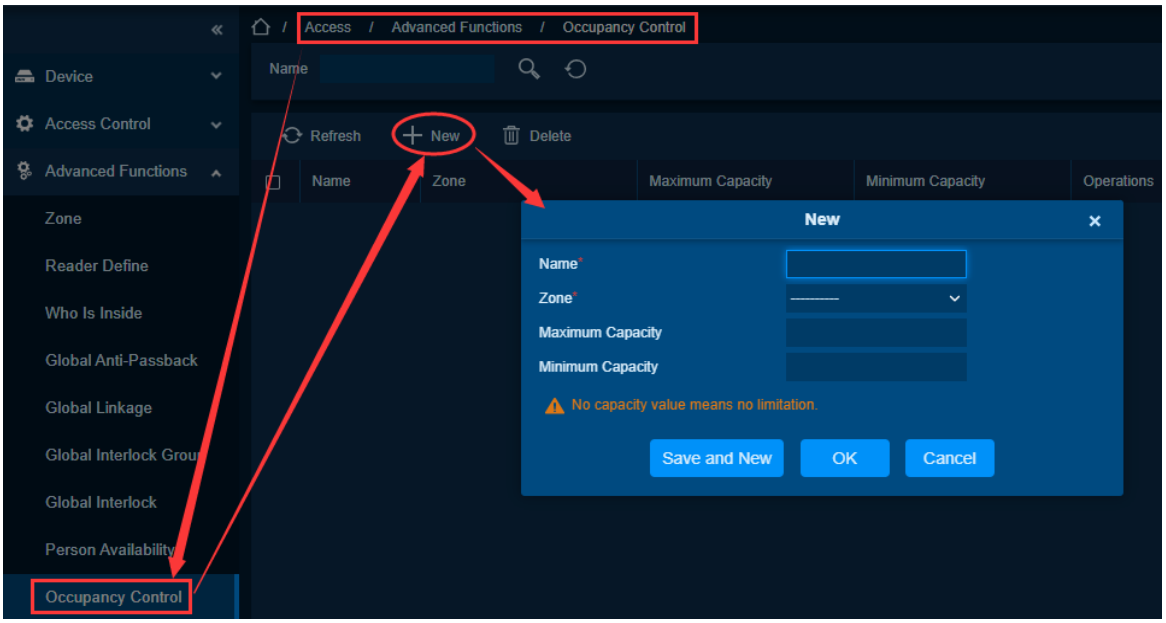
Need to control the upper and lower limits of the number of people in a specific area.

Feature Trigger Result

It can control the maximum capacity and minimum capacity of the access control area.

Steps:

Click **[Access] > [Advanced Functions] > [Occupancy Control] > [New],** the following interface will be shown.



Personnel access will be restricted after setting maximum and minimum values.

Edit Number of People Control

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

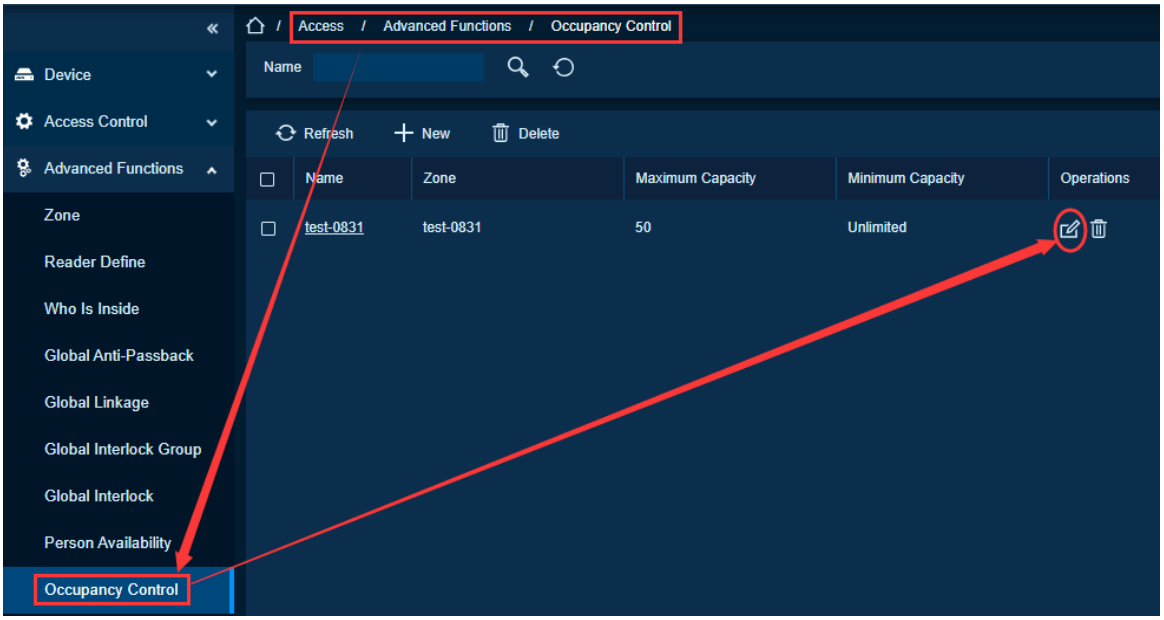
Need to control the upper and lower limits of the number of people in a specific area

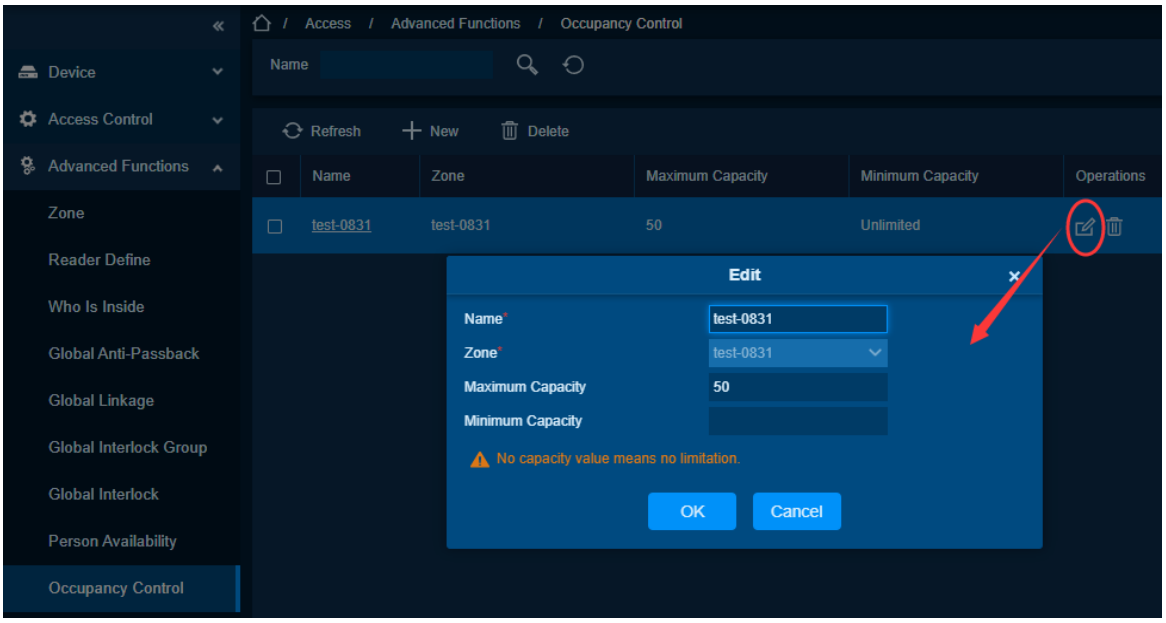
Feature Trigger Result

It can control the maximum capacity and minimum capacity of the access control area.

Steps:

- Click **[Access]** > **[Advanced Functions]** > **[Occupancy Control]** to display the people control interface.
- Select the number control to be edited and click **[Edit]** to enter the editing interface.





Delete Number of People Control

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device has been added to the access control module.

There is an access control area.

Function Usage Scenarios

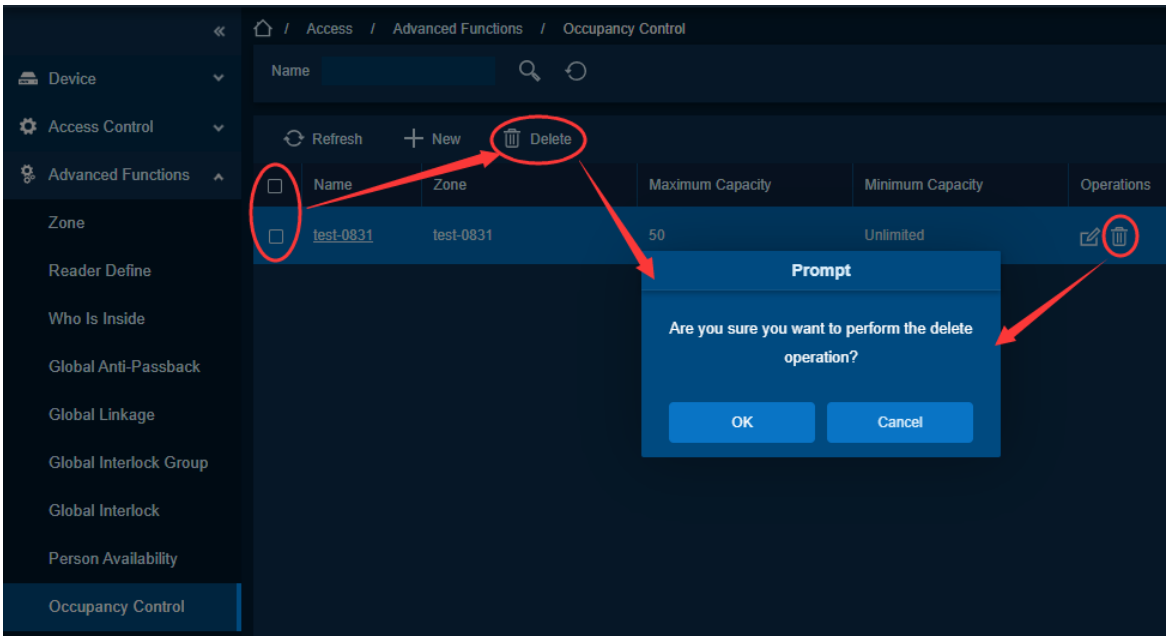
No need to control the upper and lower limits of the number of people in a specific area.

Feature Trigger Result

The maximum capacity and minimum capacity of the access control area cannot be controlled.

Steps:

- Click **[Access] > [Advanced Functions] > [Occupancy Control]** to display the people control interface.
- Select the number of people control you want to delete and click **[Delete]** to enter the delete interface.



6.4. Reports

Function List

Functions	Description
All Records	Comprises of clear data, export, and export photos for all records.
Today's Visit Record	Comprises of today's visit records.

All Exception Records	Comprises of all abnormal records.
Query by Door	Comprises of the basic information of all personnel corresponding to the door.
Query by Personnel	Comprises of personnel's query details.
Personnel Entry and Exit Records	Comprises of entry and exit records of personnel.
Device Log	Comprises of device log.
Device Face Extraction Failure Log	Comprises of face extraction failure log details.
Access Control Alarm Record	Comprises of Access Control Alarm details.

Export

Function Description

It includes "All transactions", "Events from Today", "All Exception Events" and so on. You can export after query.

You can generate statistics of relevant device data from reports, including card verification information, door operation information, and normal punching information, etc.

Verify mode: Only Card, Only Fingerprint, Only Password, Card plus Password, Card plus Fingerprint, Card, or Fingerprint etc.

✍**Note:**

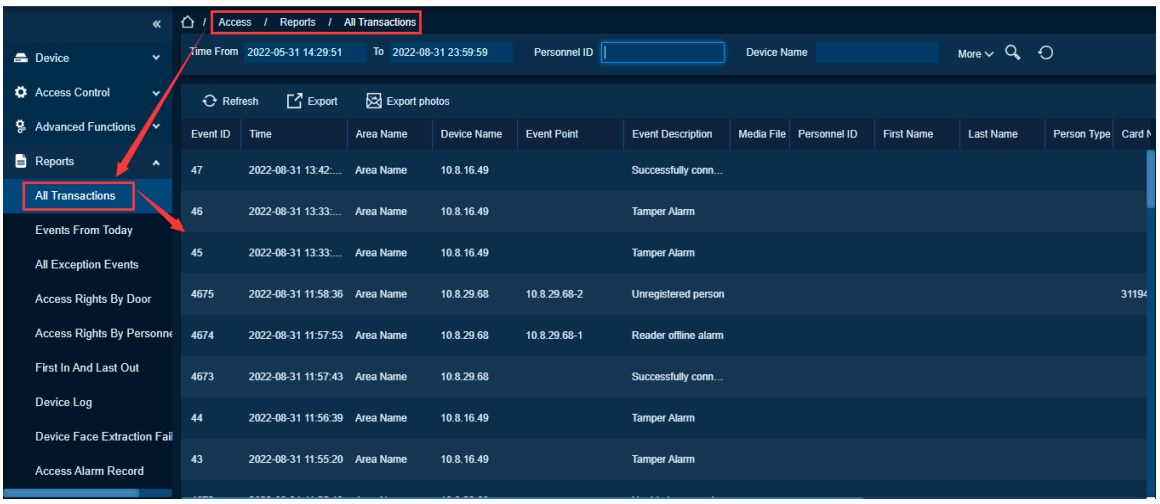
Only event records generated when the user uses emergency password to open doors will include only password verification mode.

6.4.1. All Transactions

Function Description

Because the data size of access control event records is large, you can view access control events as specified condition when querying. By default, the system displays latest three months transactions.

- Click **[Access] >[Reports] > [All Transactions]** to view all transactions.



Clear Data

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

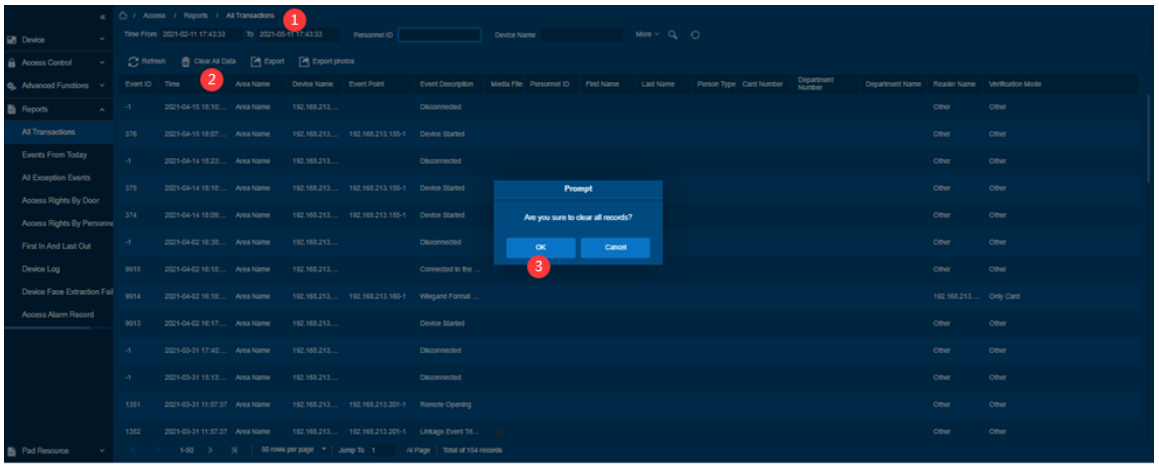
Event log is full, more than 50 pages. No need to save all current event records.

Feature Trigger Result

Delete all records, the record list empty.

Steps:

- Click **[Access]** > **[Reports]** > **[All Transactions]** to display a list of access control records.
- Click **[Clear Data]** to clear all data in the list.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

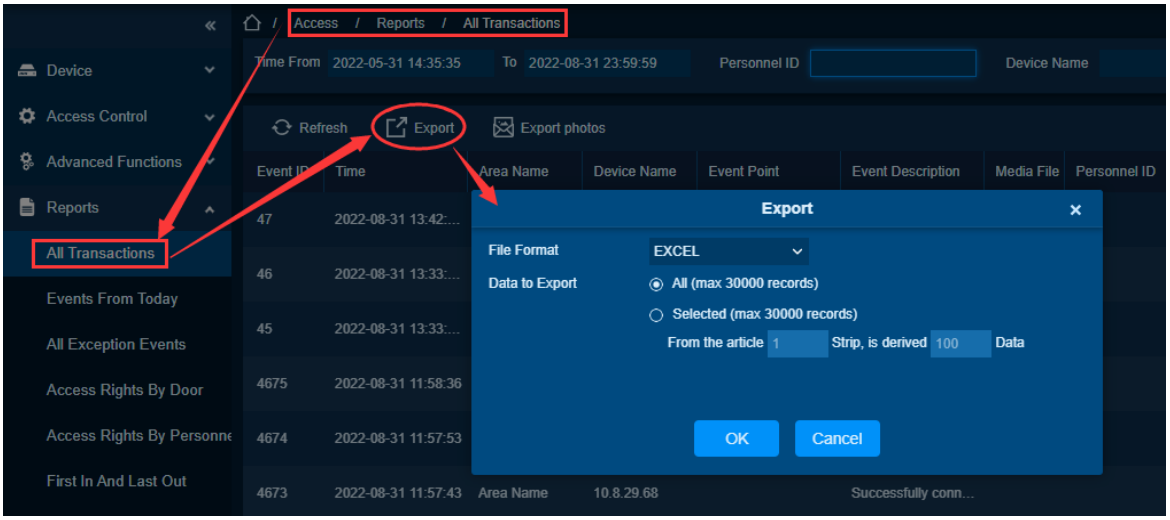
Need to view all records of the current access control in file form.

Feature Trigger Result

Export all records into Excel/Pdf/CSV format files

Steps:

- Click **[Access] > [Reports] > [All Transactions]** to display a list of access control records
- Click **[Export]** to export all data in the list.



Export Photos

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

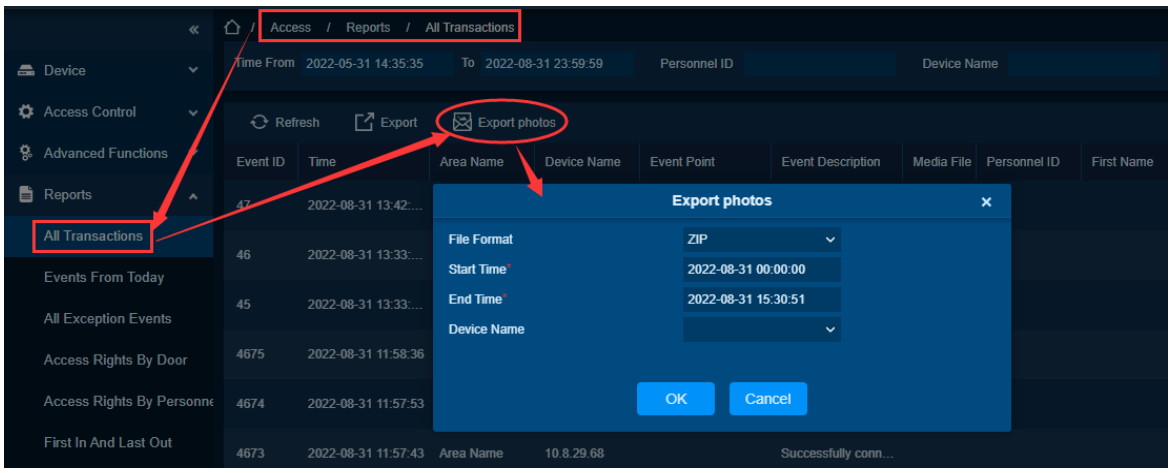
Conveniently view all the photos of the current access control at a specific time and specific device.

Feature Trigger Result

Export the photos generated by the corresponding time record.

Steps:

- Click **[Access] > [Reports] > [All Transactions]** to display a list of access control records.
- Click **[Export Photos]** to export the photos in the list.

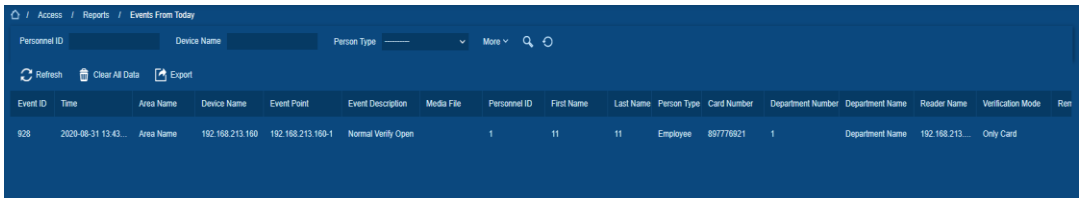


6.4.2. Events From Today

Function Description

Check out the system record today.

Click **[Reports] > [Events from Today]** to view today's records. You can export all events from today in Excel, PDF, CSV format.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

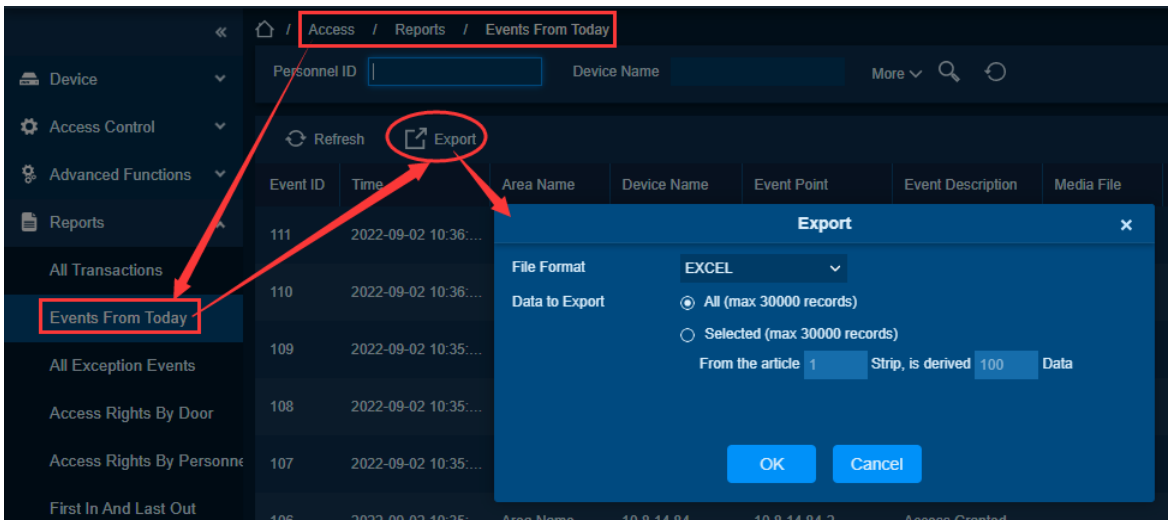
Conveniently view all access event records today.

Feature Trigger Result

Export today's records into Excel/PDF/CSV format files.

Steps:

- Click **[Access] > [Reports] > [Events From Today]** to display a list of today's visit records.
- Click **[Export]** to export today's record data.

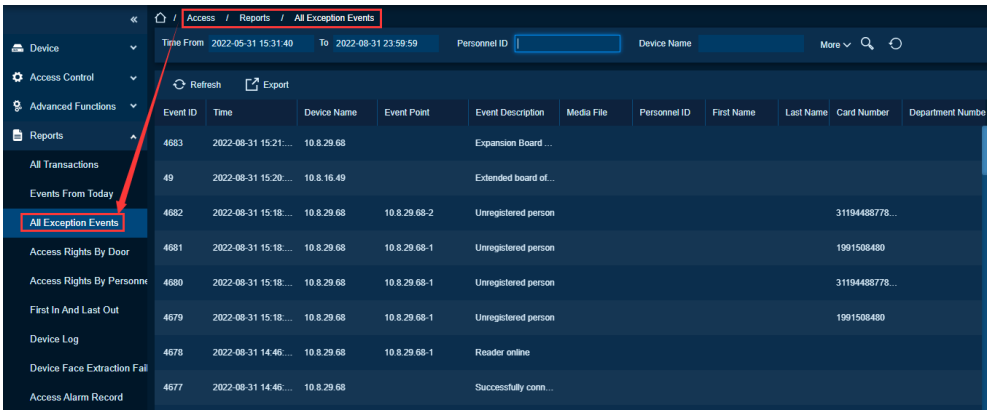


6.4.3. All Exception Events

Function Description

View all abnormal event records, including event generation time, evet description, and information about the personnel who generated the event.

Click **[Access] >[Reports] > [All Exception Events]** to view exception events in specified condition. The options are same as those of **[All Transactions].**



Clear Data

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

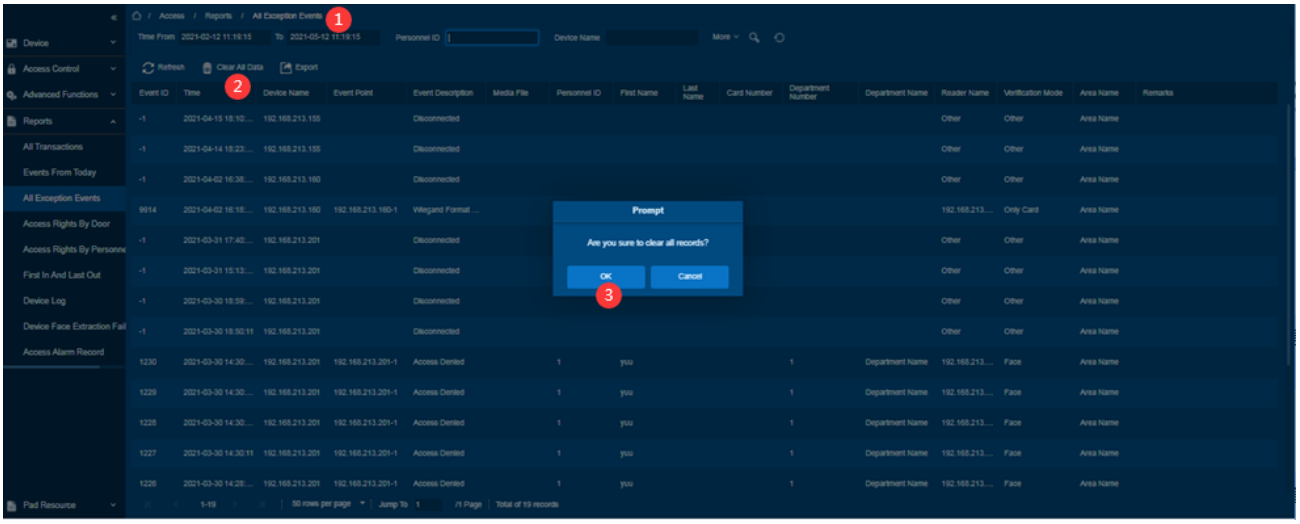
- Event log is full, more than 50 pages.
- No need to save abnormal event records.

Feature Trigger Result

The abnormal record is deleted, and the record list is empty.

Steps:-

- Click **[Access Control Device] > [Reports] > [All Exception Events]** to display a list of all abnormal records.
- Click **[Clear Data]** to clear all abnormal record data.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

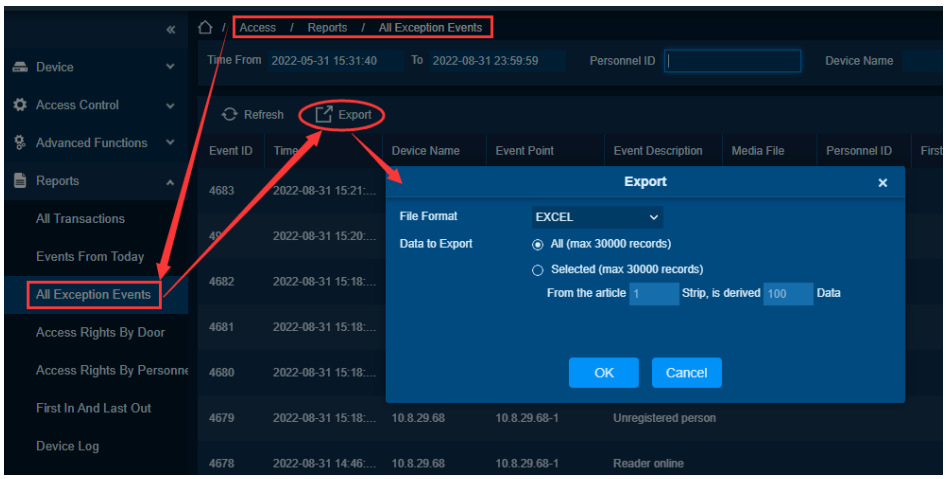
Need to view all exception records in file format.

Feature Trigger Result

Export all abnormal records into Excel/PDF/CSV format files.

Steps:

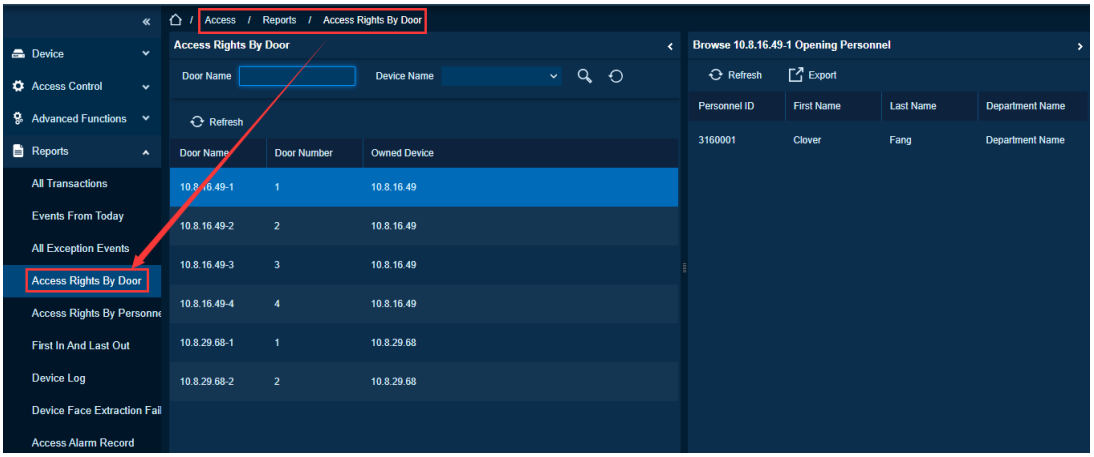
- Click **[Access] > [Reports] > [All Exception Events]** to display a list of all abnormal records.
- Click **[Export]** to export all abnormal record data.



6.4.4. Access Rights by Door

Function Description

View related access levels by door. Click **[Reports] > [Access Rights by Door],** the data list in the left side shows all doors in the system, select a door, the personnel having access levels to the door will be displayed on the right data list.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

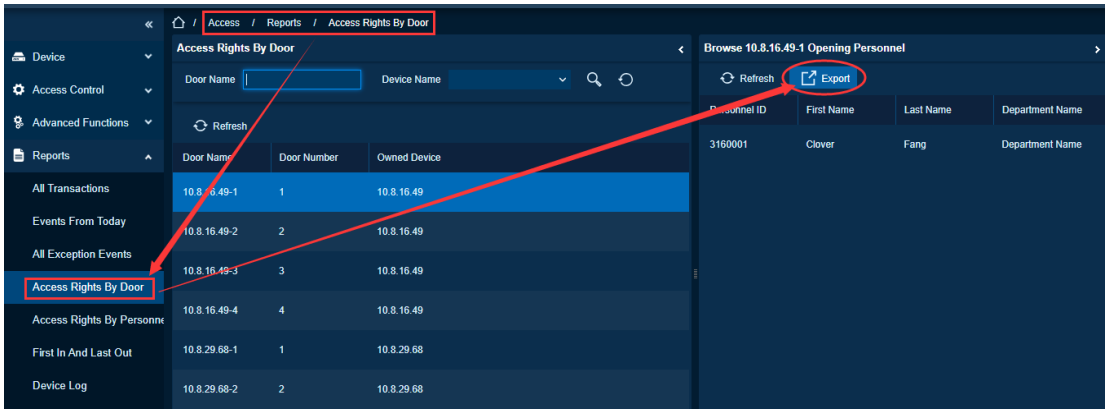
Need to quickly view the information of all personnel who have access to the door, including name, department, and number.

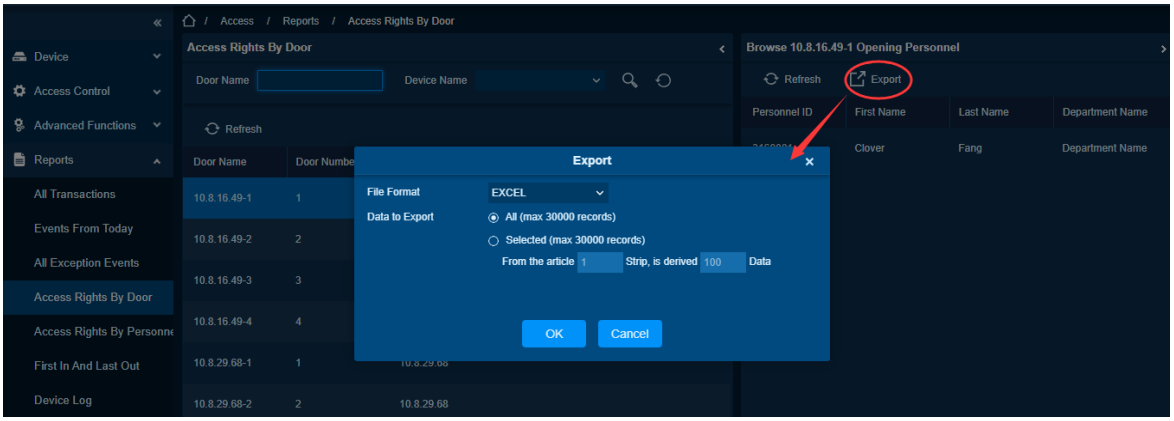
Feature Trigger Result

It can use Excel file format to view the right to access all personnel information.

Steps:

- Click **[Access] > [Reports] > [Access Rights by Door]** to display the door and the list of persons who have access to the door
- In the operation bar on the right, click **[Export]** to export the personnel data of the door.



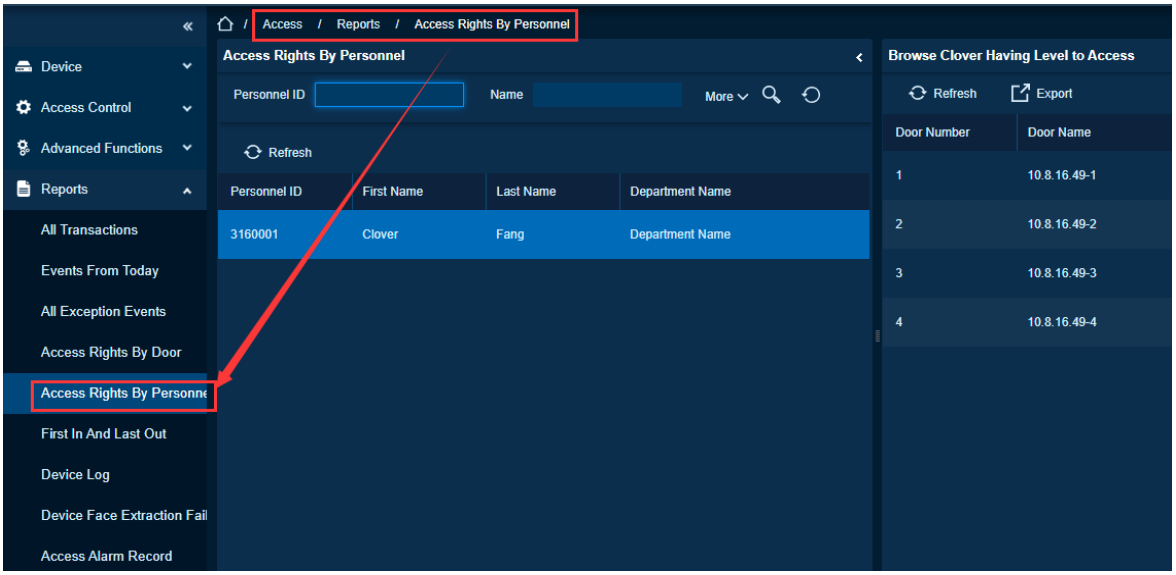


6.4.5. Access Rights by Personnel

Function Description

View related access levels by door or personnel.

Click **[Reports] > [Access Rights by Personnel],** the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

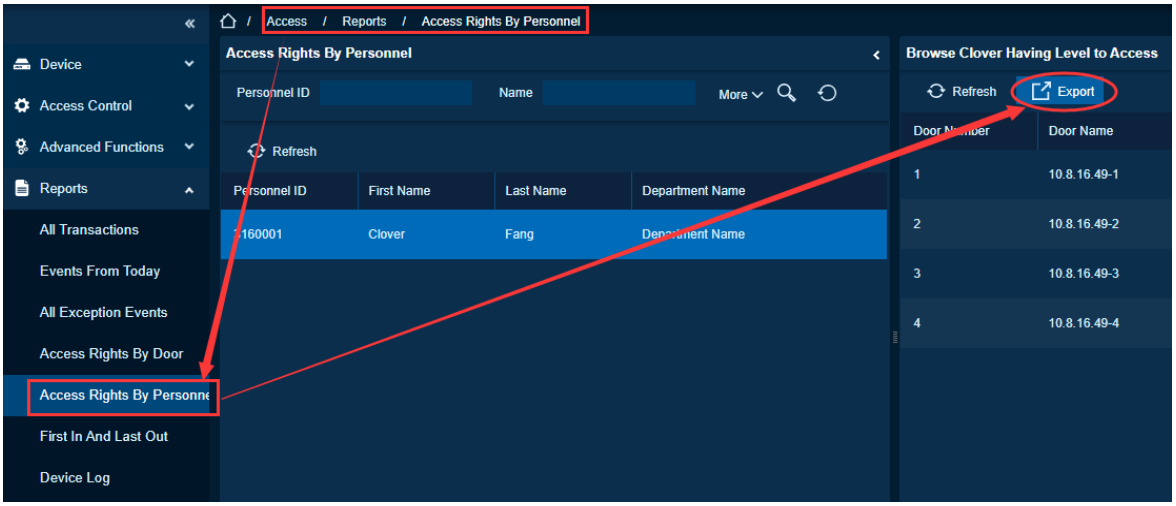
Need to quickly check the door that the corresponding person can enter and exit.

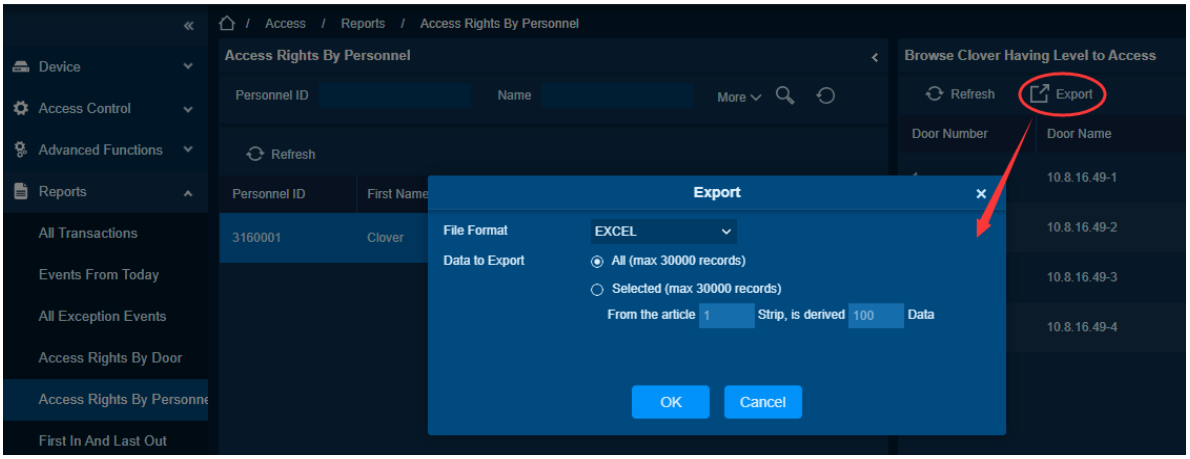
Feature Trigger Result

You can use the Excel file format to view the doors that the corresponding person has access.

Steps:

- Click **[Access]** > **[Reports]** > **[Access Rights by Personnel]** to display the list of personnel and doors.
- In the operation bar on the right, click **[Export]** to export the doors that the person can access.





6.4.6. First In and Last Out

Function Description

You can quickly see the entry and exit of personnel through the list.

Clear Data

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

Event log is full, more than 50 pages.

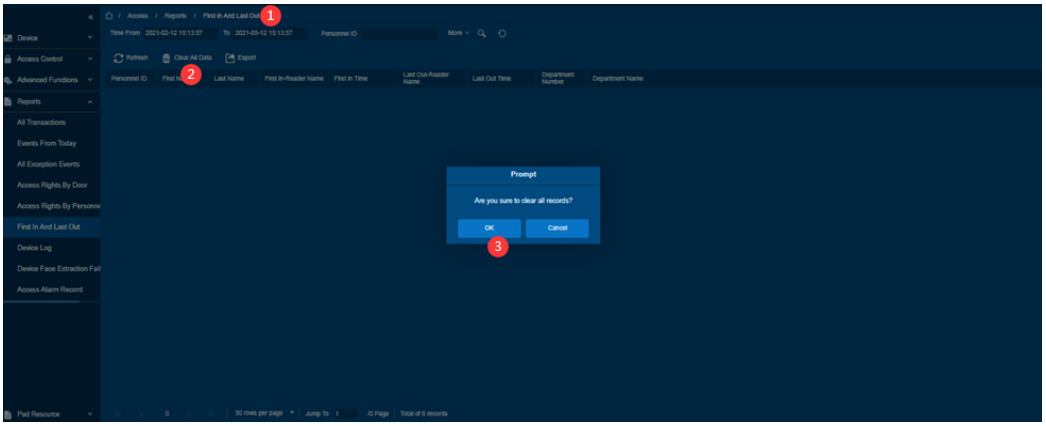
No need to save abnormal event records.

Feature Trigger Result

Clear all personnel entry and exit records in the list.

Steps:

- Click **[Access] > [Reports] > [First in And Last Out]** to display the status table of all personnel access.
- Click **[Clear Data]** to clear all personnel entry and exit records.



Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

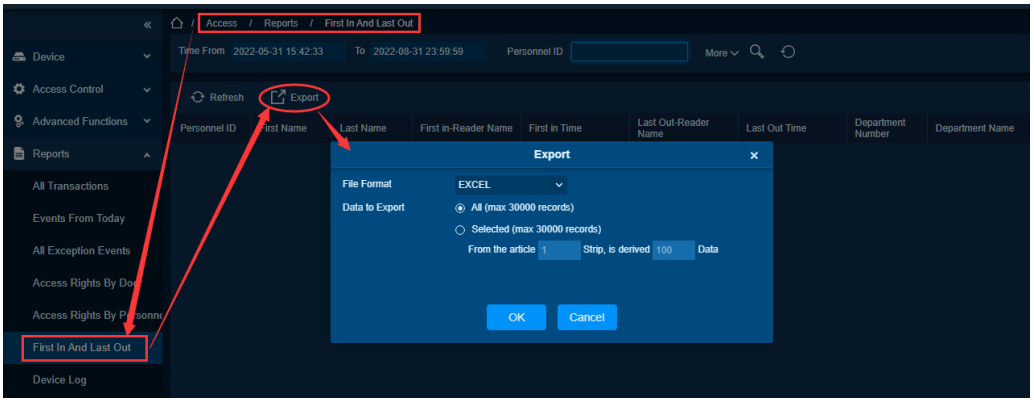
Need to quickly check the entry and exit of all personnel.

Feature Trigger Result

Export all abnormal records into Excel/PDF/CSV format files.

Steps:

- Click **[Access] > [Reports] > [First In And Last Out] to** display the status table of all personnel access.
- Click **[Export]** to export all personnel entry and exit records.



6.4.7. Device Log

Function Description

You can quickly view all operation logs in the device log list, including operating users, device names, operation events, operation types and so on.

Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

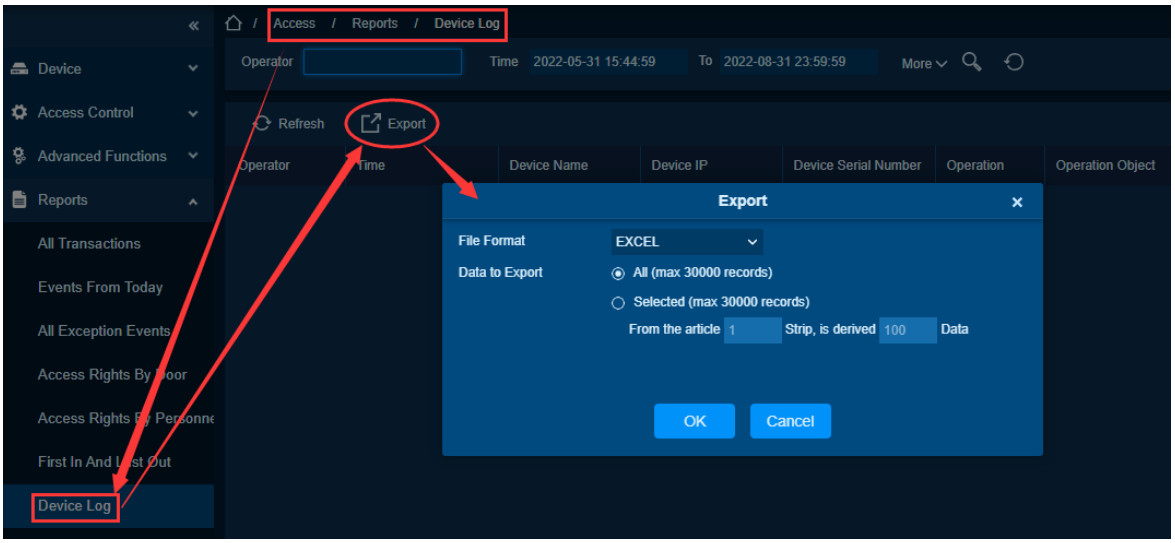
Need to view all device log records of the device

Feature Trigger Result

Export device log records into Excel/PDF/CSV format files

Steps:

- Click **[Access] > [Reports] > [Device Log]** to display all device log tables.
- Click **[Export]** to export device log records.



6.4.8. Device Face Extraction Failure Log

Function Description

Through the list, you can quickly view the failure of device face extraction, including operation type, error description, media file, etc.

Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

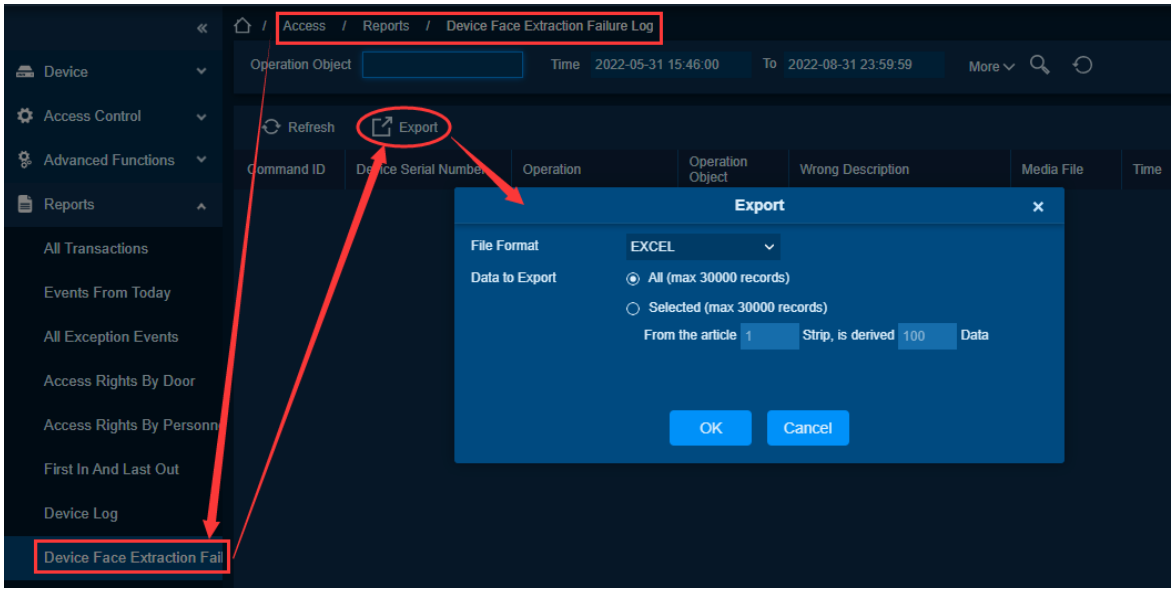
Conveniently check the device's face extraction

Feature Trigger Result

Export the device's face failure situation to Excel/PDF/CSV format file

Steps:

- Click **[Access] > [Reports] > [Device Face Extraction Failure Log]** to display all device face extraction failure log.
- Click **[Export]** to export the face extraction failure log of the device.



6.4.9. Access Alarm Record

Function Description

Through the list, you can quickly view the alarm situation of the personnel, including the description of the event, the time of occurrence, and the device that generated the event.

Export

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

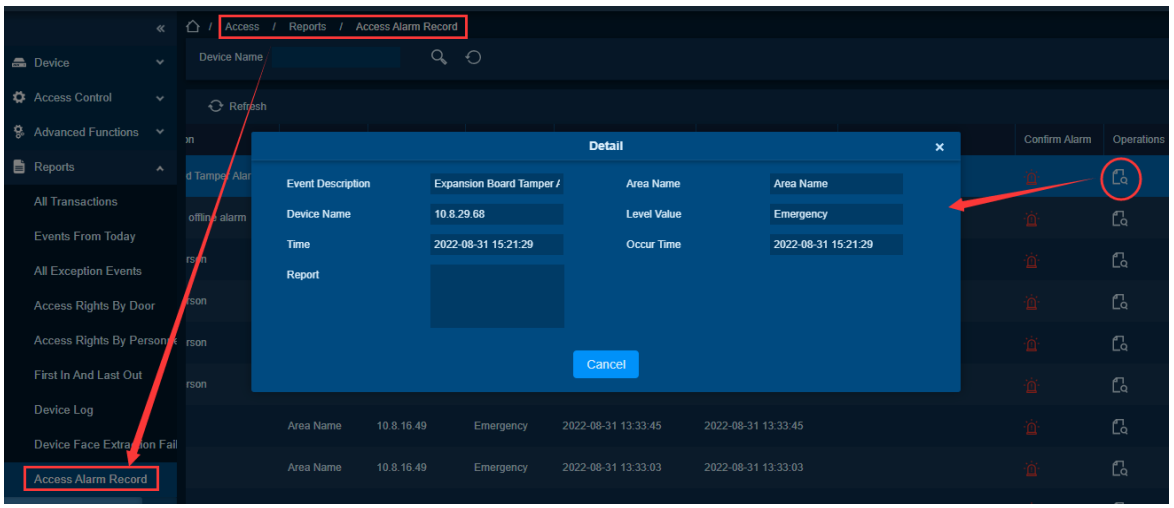
Conveniently view the access control alarm status of the device.

Feature Trigger Result

You can see the detailed record of a single event.

Steps:

- Click **[Access] > [Reports] > [Access Alarm Record]** to display all access control alarm records
- Select the record you want to view and click **[Details]** to view the access control alarm record



6.5. Pad Resource

Function List

Functions	Description
Resources	Add, delete, edit resources.
Set by Device	Add and delete resources by device.
Set by Resources	Add and delete devices by resources.

6.5.1. Resources

Function Description

For the resource management of the Pad device, you can select the Resource Type, Resource Type Name. Then, add resources to the device according to the device or according to the resource settings.

Add Resources

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

If the added resource type is a boot image, it must be of JPG type, other images must be of PNG type, and the size of the image must be 800x1280; if it is voice, the voice must be of WAV type.

Function Usage Scenarios

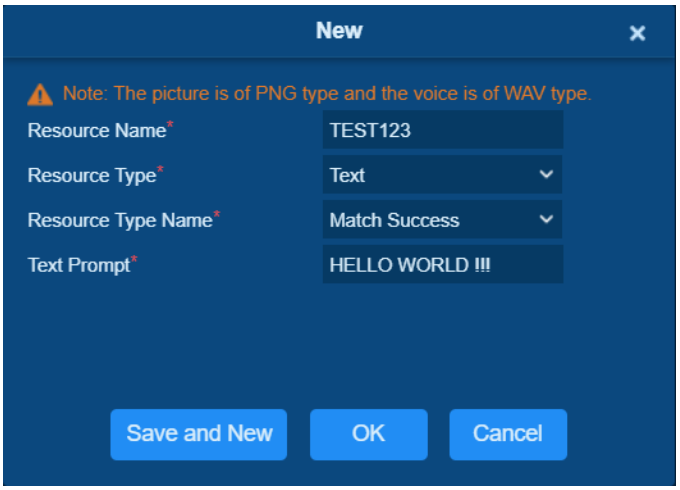
The device needs to use new pictures or voice or text.

Feature Trigger Result

While adding resources, you can choose a variety of resource types and resource type names.

Steps:

- Click **[PAD Resource]> [New]** to enter the new editing interface.
- Click **[View]** to upload the local resource file and click **[Save]** to complete the resource creation.



Resource Name: Define the resources for the name, for easy access.

Resource Type: Optional Image file / Audio file / Text.

Resource Type Name: The definition of resources for the intended use of the optional boot display / welcome page Display / Screensaver displays.

✍**Note:**

The format of the uploaded picture file must be PNG, and the format of the uploaded audio file .must be WAV.

Edit Resources

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority. If the added resource type is a boot image, it must be of JPG type, other images must be of PNG type, and the size of the image must be 800x1280; if it is voice, the voice must be of WAV type.

Function Usage Scenarios

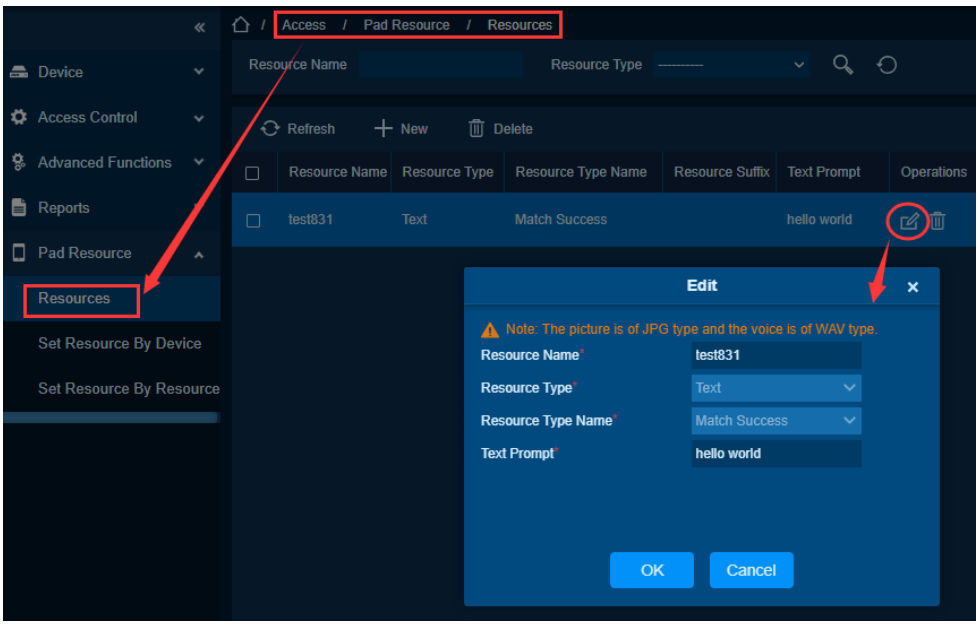
Need to modify the name and resource file in the resource.

Feature Trigger Result

Modified to the new resource name and file.

Steps:

- Click **[Access] > [Pad Resource] > [Resources]** to display all resource names.
- Click **[Edit]** to enter the editing interface.



Delete Resources

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

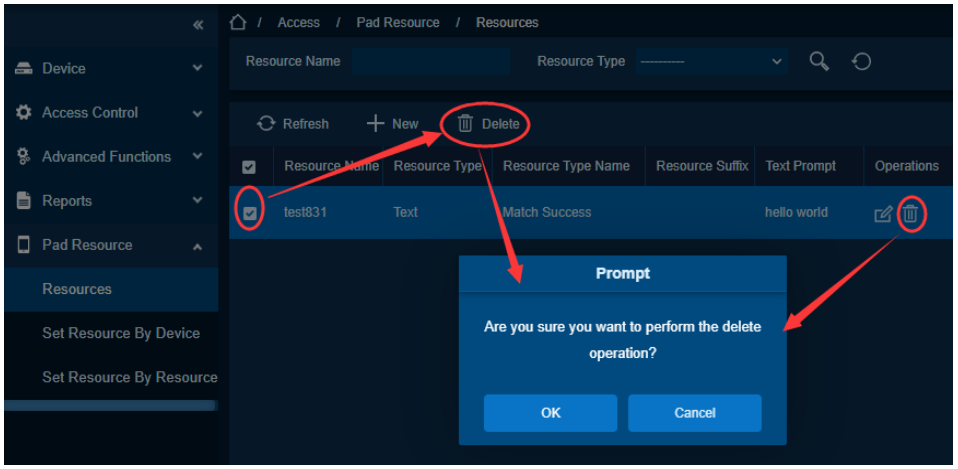
The resource is no longer needed. The resource type and resource type name are incorrect and need to be added again.

Feature Trigger Result

The resource does not exist in the resource list, and the resource cannot be sent to the device for use

Steps:

- Click **[Access]** > **[Pad Resource]** > **[Resources]** to display all resource names.
- Click **[Delete]** to enter the delete interface.



6.5.2. Set Resource by Device

Function Description

After adding resources, you can add resources and delete resources in the corresponding device.

Add Resources

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

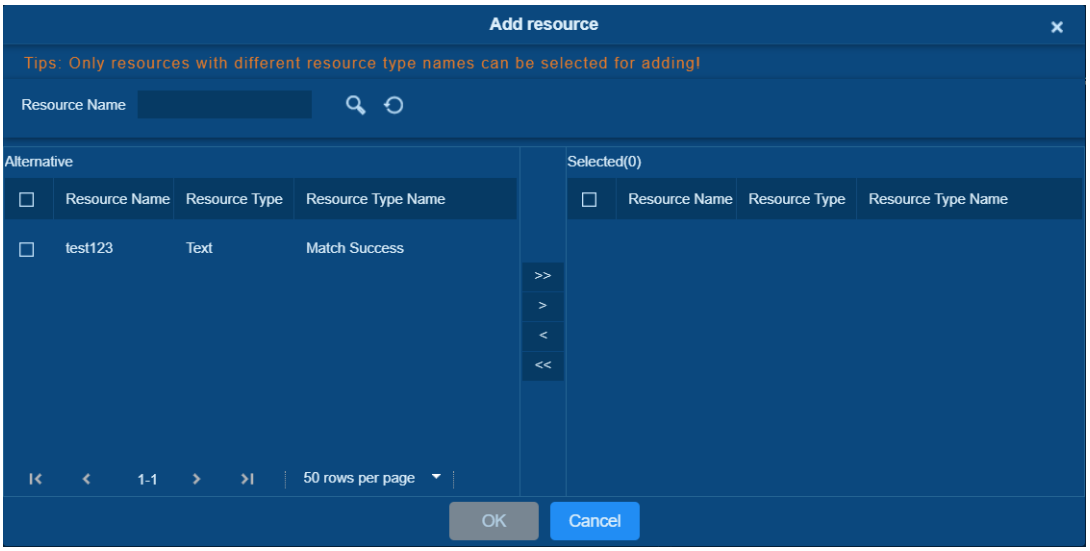
Need to add resources to facilitate distribution to the device for use.

Feature Trigger Result

Multiple resources can be added to the same device.

Steps:

Select the PAD device that needs to deliver resources and click the **[Add Resource].**



Select the required resources and click **[OK]** to complete the resource addition. The device resource list on the right displays the device resources.

Delete Resources

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

Function Usage Scenarios

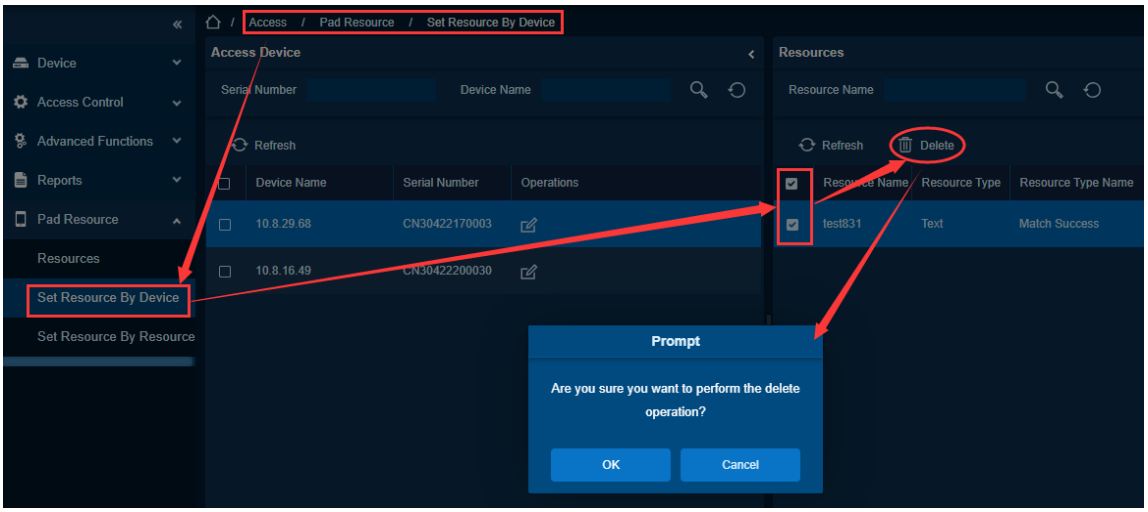
The selected device does not require current resources. There is an error in the set resource, and new resource data needs to be added.

Feature Trigger Result

Delete the resource from the device, the resource cannot be used in the device

Steps:

- Click **[Access]** > **[Pad Resource]** > **[Set Resource by Device]** to display the resources corresponding to all devices.
- Select the device to delete the resource and click **[Delete]** in the right column to enter the delete interface.



6.5.3. Set Resource by Resource

Function Description

After adding resources, you can add the corresponding resources to a variety of devices.

Add Device

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority.

The device does not add other resources of the same type.

Function Usage Scenarios

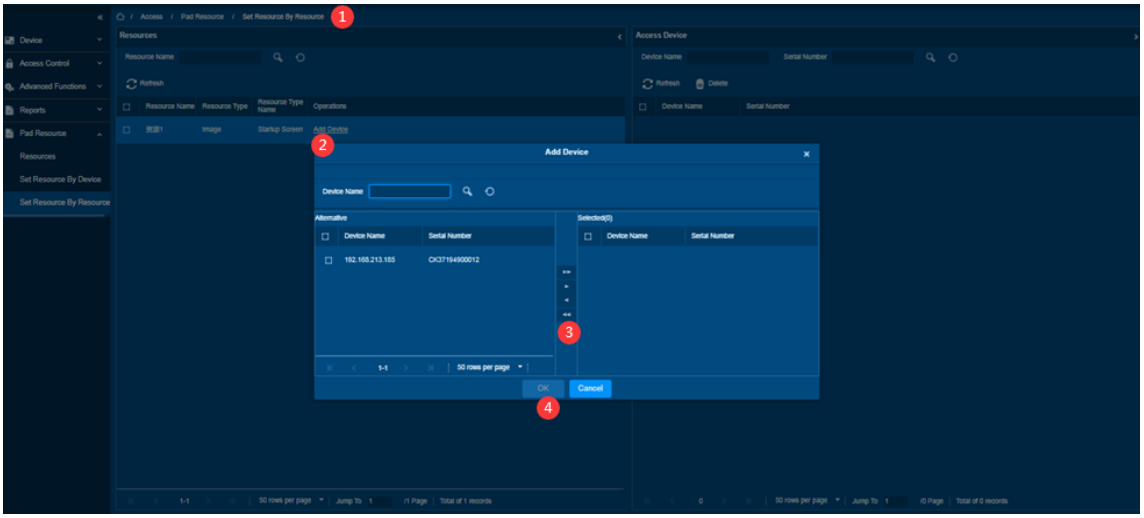
Need to add resources to facilitate distribution to the device for use.

Feature Trigger Result

The same resource can be added to multiple devices.

Steps:

Select a resource click **[Add Device],** the resource will be sent to the selected device.



Delete Device

Preconditions for Normal Use of Function

Log in to the system with the current account and have the menu authority

Function Usage Scenarios

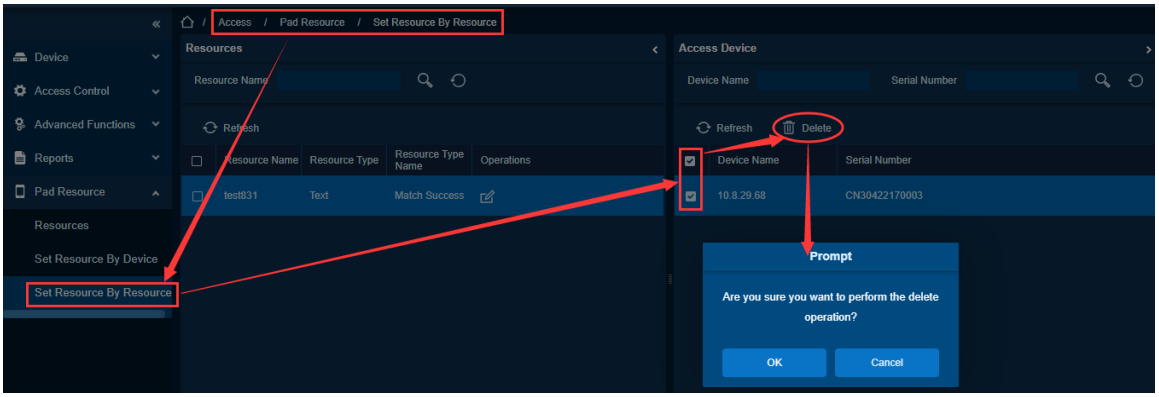
There is no need to distribute the resource to the device

Feature Trigger Result

Delete this resource from the device

Steps:

- Click **[Access]** > **[Pad Resource]** > **[Set Resource by Resource]** to display the resources corresponding to all devices
- Select the device to be deleted and click **[Delete]** in the right column to enter the delete interface.
- Click **OK** to delete the device.



7. Attendance Management

Attendance Management enables the enterprise to achieve the information management of personnel attendance. The purpose is to achieve the automation of personnel attendance data collection, data statistics and information inquiry process, improve the modernization of personnel management, facilitate personnel to sign into work, and facilitate management personnel to count and assess personnel attendance. It is convenient for the management department to inquire and evaluate the attendance rate of each department, accurately grasp the attendance of personnel, and effectively manage and grasp the flow of personnel.

7.1. Attendance Device

Function List

Functions	Description
Set by Region	Operations of adding personnel, deleting personnel, private short messages, and resynchronizing to the device by area.
Set by Personnel	Add area, delete area to personnel.
Device	Attendance devices delete, search, enable, disable, restart device, business short message, synchronize software data to device, obtain device parameters, view device parameters, check attendance data, re-upload data, obtain designated personnel data, clear device commands, relevant functional operations such as clearing attendance photos and clearing attendance records.
Attendance Point	Operations such as adding, editing, and deleting attendance points.
Device Operation Log	Record log for the operation of attendance device.

7.1.1. Set Attendance by Area

Function Description

Use this function to manage the personnel in each area, add personnel to the corresponding area, the area list is all the areas created in the system management module.

Add Personnel in Area

Preconditions for Normal Use of Function

1. Need to have the corresponding area in the system management module and the personnel who have added or imported the required settings in the personnel module.

2. Support the selection of areas and personnel.

Function Usage Scenarios

When regionalized personnel attendance management is required, this function can be used to assign personnel and set their attendance area.

Feature Trigger Result

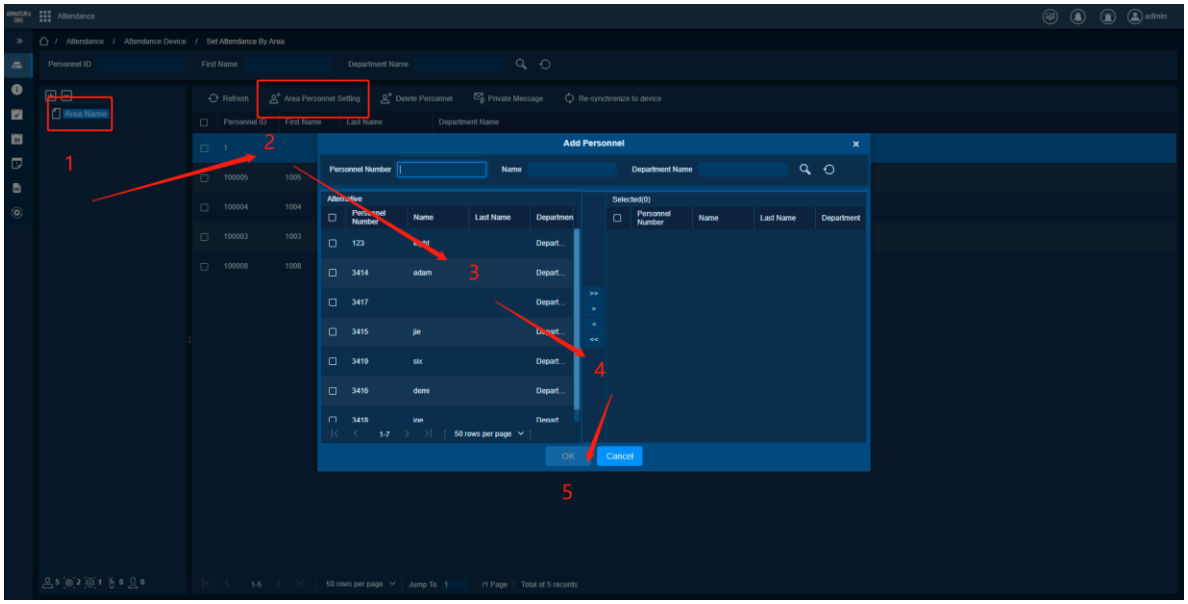
1. After adding personnel to the area, the attendance area corresponding to these personnel will be displayed in the set by personnel module.

2. When there are people under the area, the area cannot be deleted in the system management module.

Steps:-

1. Click **[Attendance Device] > [Set Attendance by Area],** select an area, and click **[Area Personnel Setting]** to display the page for adding personnel.

2. After selecting personnel, click **[OK]** to complete adding personnel and click **[Cancel]** to cancel adding personnel to this area.



Delete Personnel

Preconditions for Normal Use of Function

The area has successfully added personnel.

Function Usage Scenarios

When a person does not need to use this attendance area to check on attendance, this function can be used to delete the person.

Feature Trigger Result

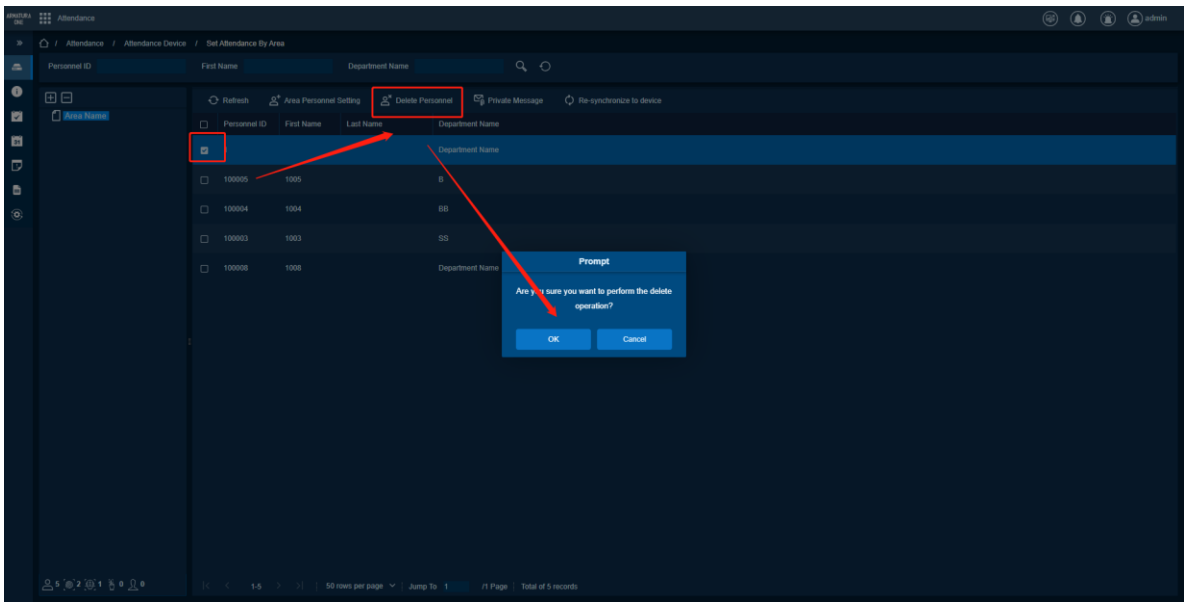
1. The personnel information under the area in the area setting module is deleted.

2. The area where the staff is in the set by staff module is deleted.

Steps:-

1. Click **[Attendance Area] > [Set Attendance by Area]**. Click to select the area and the personnel you want to delete, click **[Delete personnel].**

2. Click **[OK]** to confirm the delete and click **[Cancel]** to cancel the delete.



To Private Short Message

Preconditions for Normal Use of Function

The area has successfully added personnel.

Function Usage Scenarios

When you want to send a separate short message to a specific person when you are checking attendance, you can use this function to set it up.

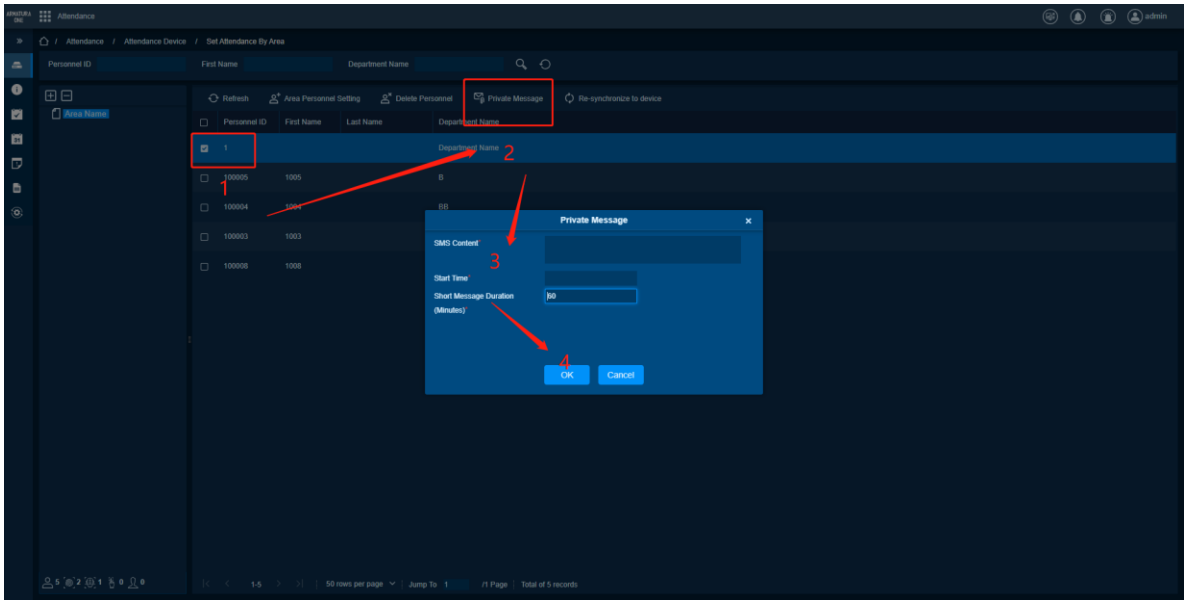
Feature Trigger Result

Operations	Description
Start Time is Required	After this time, personnel will receive a separate short message when they perform attendance
Short Message Duration (Minutes) is Required	Set the duration of short message display, you can always see the displayed message during this period after attendance

Steps:-

1. Click **[Attendance Area]** > **[Set Attendance by Area]**, select personnel, and click **[Private Message]** to display the private SMS page.

2. After entering the content, start time and duration of the short message (minutes), click **[OK]** to complete the setting, and click **[Cancel]** to cancel the setting.



Re-sync to the Device

Preconditions for Normal Use of Function

Attendance device has been added to the area itself or the area where the personnel are located.

Function Usage Scenarios

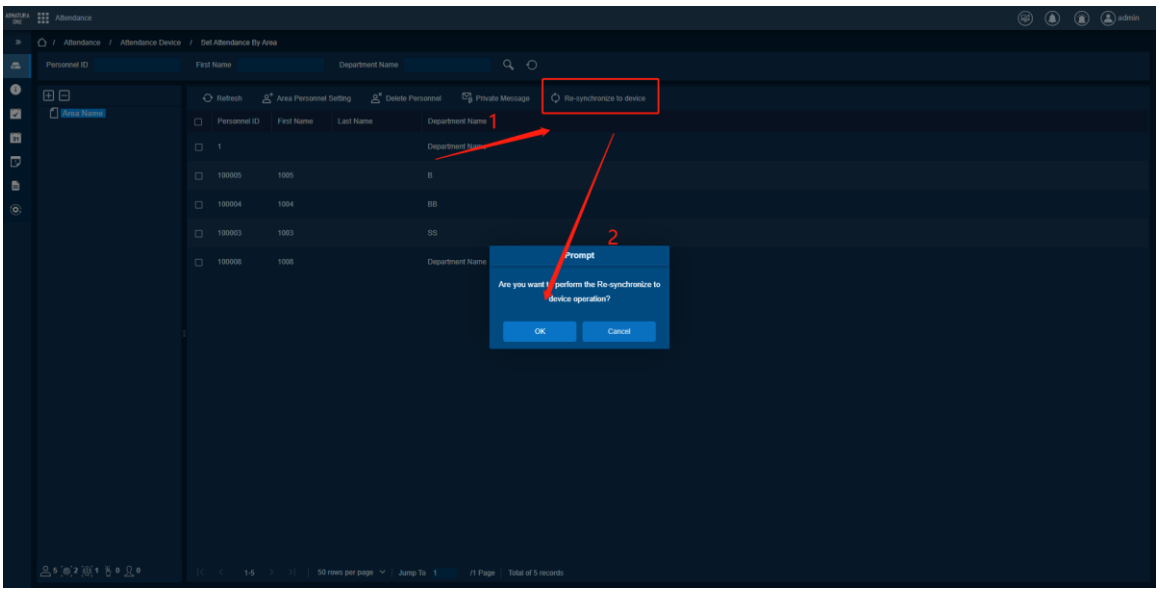
When the regional personnel and other information are modified, but the software cannot automatically send the information to be synchronized to the attendance device, this function can be used to re-issue the personnel regional distribution and other relevant information to the attendance device in the area.

Feature Trigger Result

Select the area and click to resynchronize to the device, and the personnel information will be sent to the attendance device in the area, so that the personnel can perform the attendance.

Steps:-

1. Click **[Attendance Area]** > **[Set Attendance by Area]**, select a region or person, and click **[Re-synchronize to Device]**.
2. Click **[OK]** to resynchronize to the device and click **[Cancel]** to cancel resynchronization to the device.



7.1.2. Set Attendance by Person

Function Description

Use this function to add and select attendance area for personnel, which is convenient for area management settings. The area list is all areas created in the system management module.

Add Area

Preconditions for Normal Use of Function

Need to have the corresponding area in the system management module and the personnel who have added or imported the required settings in the personnel module.

Support the selection of personnel and regions

Function Usage Scenarios

When a person needs to check attendance in the designated area, add and select the corresponding area for the person.

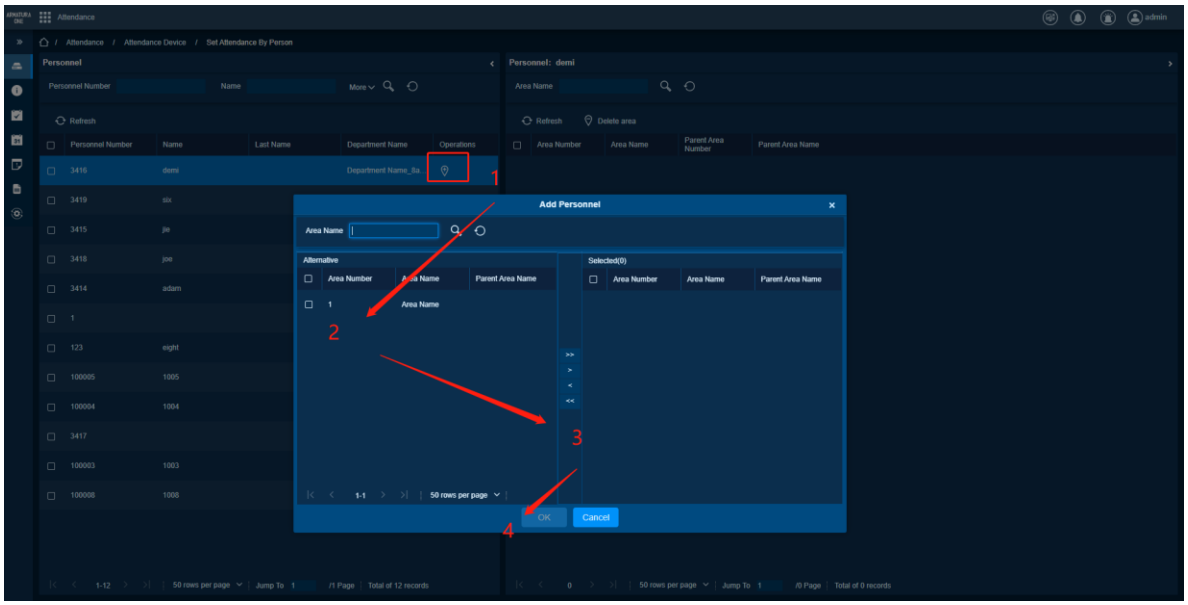
Feature Trigger Result

After adding areas for personnel, the attendance area corresponding to these personnel will be displayed in the module on the right side of the page for setting by personnel.

After adding an area for personnel, when there are personnel under the area, the area cannot be deleted in the system management module.

Steps:-

1. Click **[Attendance Device] > [Set Attendance by Personnel]**, select personnel, and click **[Add Area]** to display the add area page.
2. After selecting single or multiple areas, click **[**OK**]** to add areas for personnel, and click **[**Cancel**]** to cancel adding areas for personnel.



Delete Area

Preconditions for Normal Use of Function

The person has successfully added the area.

Function Usage Scenarios

When personnel do not need to use a certain attendance area for attendance, they can use this function to delete the corresponding area.

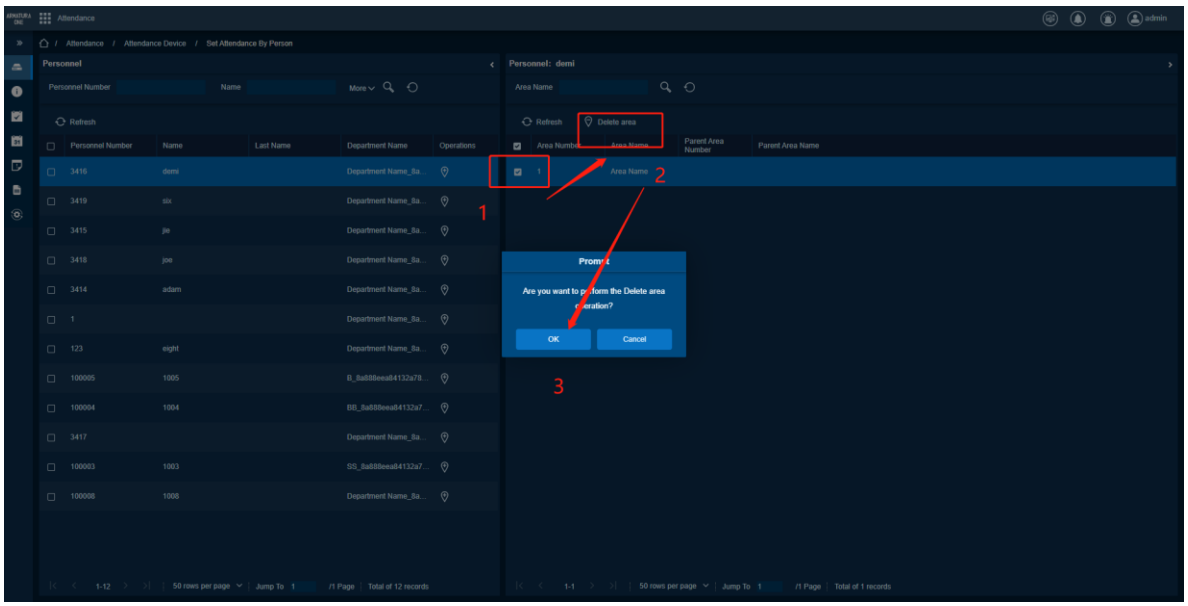
Feature Trigger Result

The personnel information under the area in the area setting module is deleted.

The area where the staff is in the set by staff module is deleted.

Steps:-

1. Click **[Attendance Area] > [Set Attendance by Personnel],** select personnel, select the area in the module on the right side of the page, and click **[**Delete Area**]**.
2. In the pop-up window, click **[OK]** to delete the area and click **[Cancel]** to cancel the delete area.



7.1.3. Device

Function Description

Manage attendance device, support adding, deleting, setting attendance device status, obtaining, and viewing attendance device parameters, clearing device commands, clearing attendance photos, clearing attendance records and other related functions to prepare for personnel attendance records.

Search Device

Preconditions for Normal Use of Function

The attendance devices service parameter is set correctly.

Function Usage Scenarios

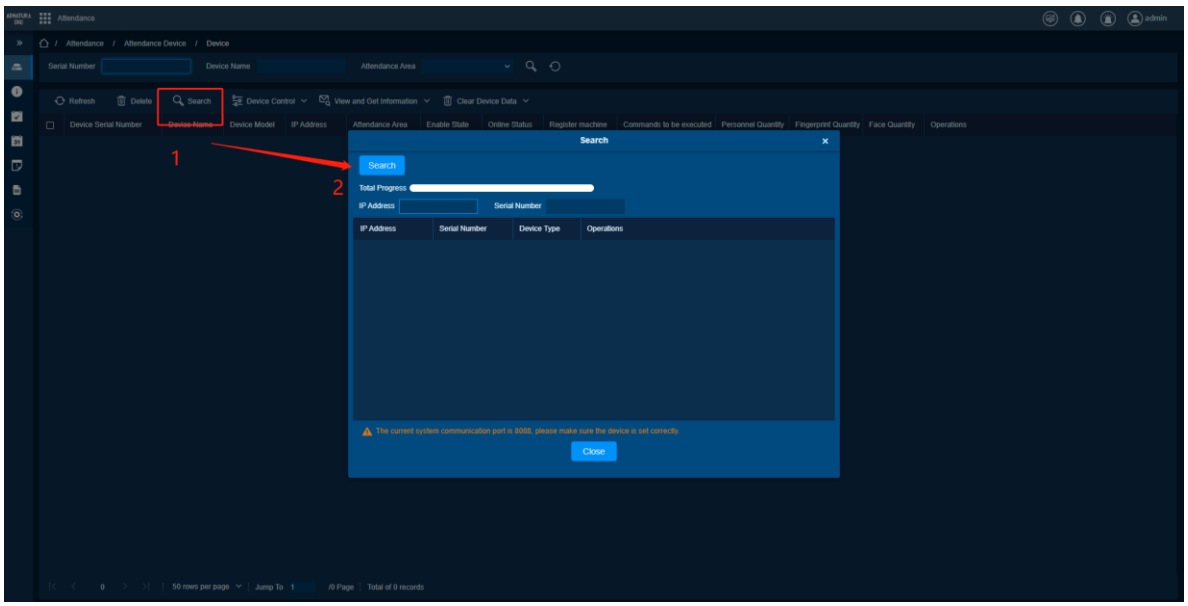
Operation settings can be used for attendance device for personnel attendance records.

Feature Trigger Result

Added new attendance device information which can operate the device.

Steps:-

1. Click **[Attendance Device] > [Device] > [Search]** and click **Search.**
2. Add attendance device, click **[OK]** to add attendance device, and click **[Cancel]** to cancel adding attendance device.



Delete device

Preconditions for Normal Use of Function

The software has successfully added the device.

Function Usage Scenarios

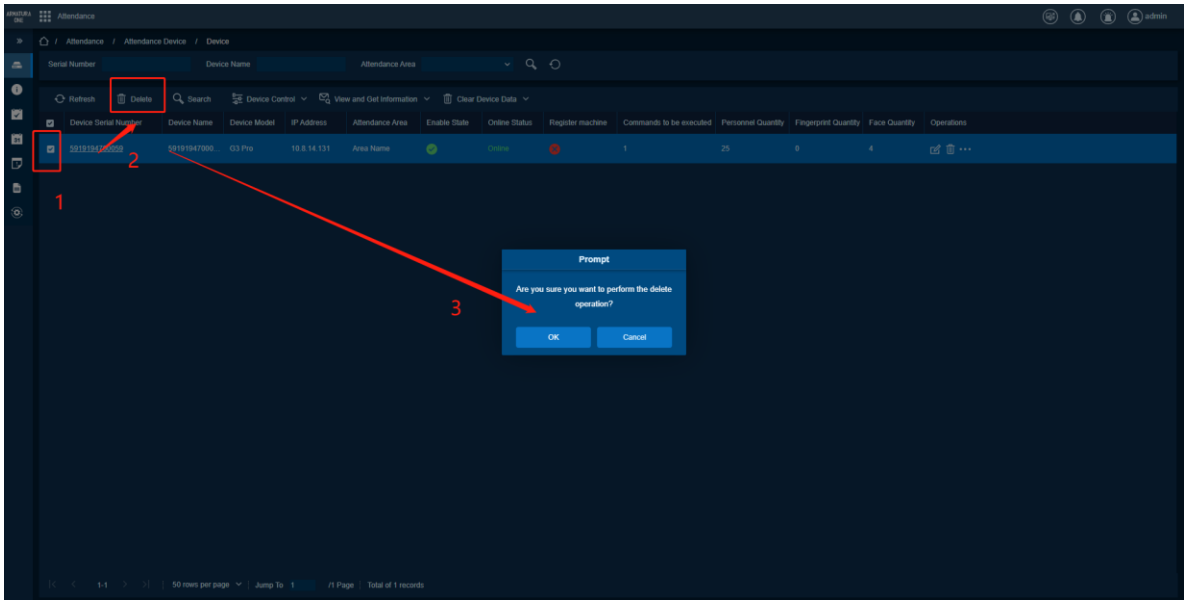
- No need to use and operate attendance device.
- Remove the attendance device information.

Feature Trigger Result

Delete the added device, remove the device information, the device will not be displayed in the device list.

Steps:-

1. Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list and click **[Delete]**.
2. In the pop-up window, click **[OK]** to delete the device and click **[Cancel]** to cancel the deletion of the device.



Device Control-Enable

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

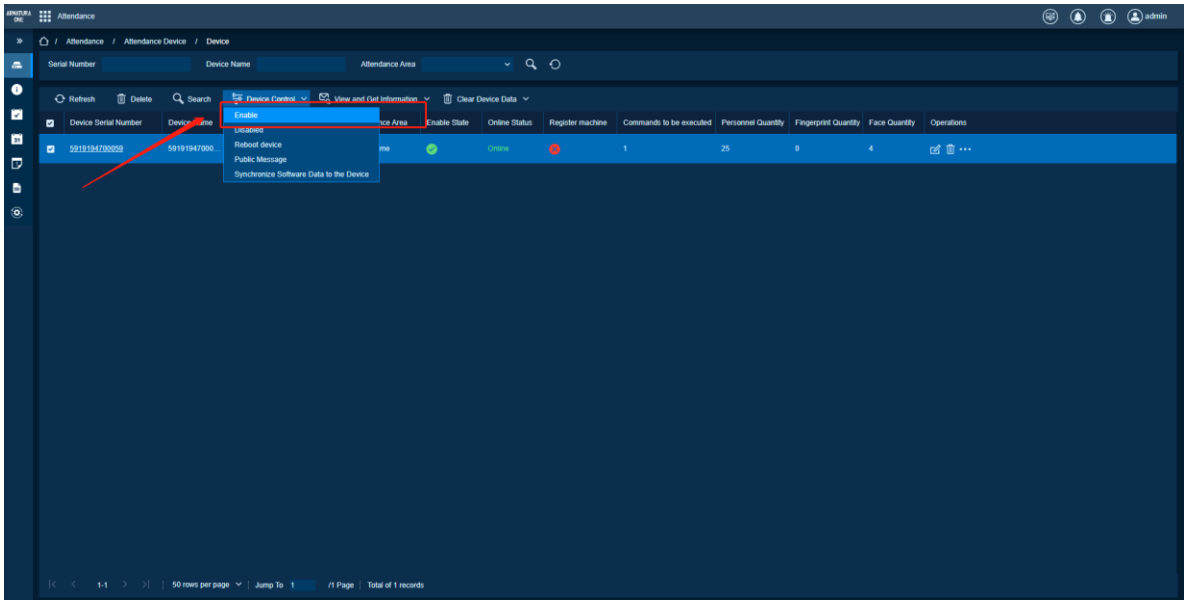
Enable currently disabled devices.

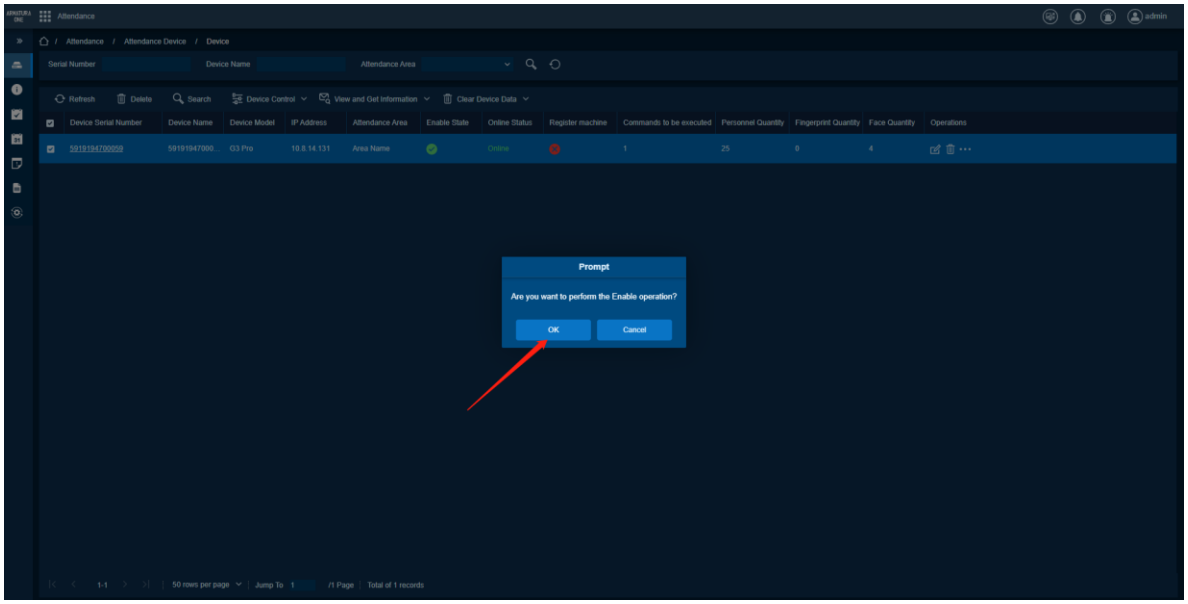
Feature Trigger Result

The device status changes to [Enable] and operations such as management settings can be performed.

Steps:-

1. Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list and click **[Device Control]** > **[Enable]**.
2. In the pop-up window, click **[OK]** to activate the device and click **[Cancel]** to cancel the activation of the device.





Device Control-Disable

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

Disable currently enabled devices.

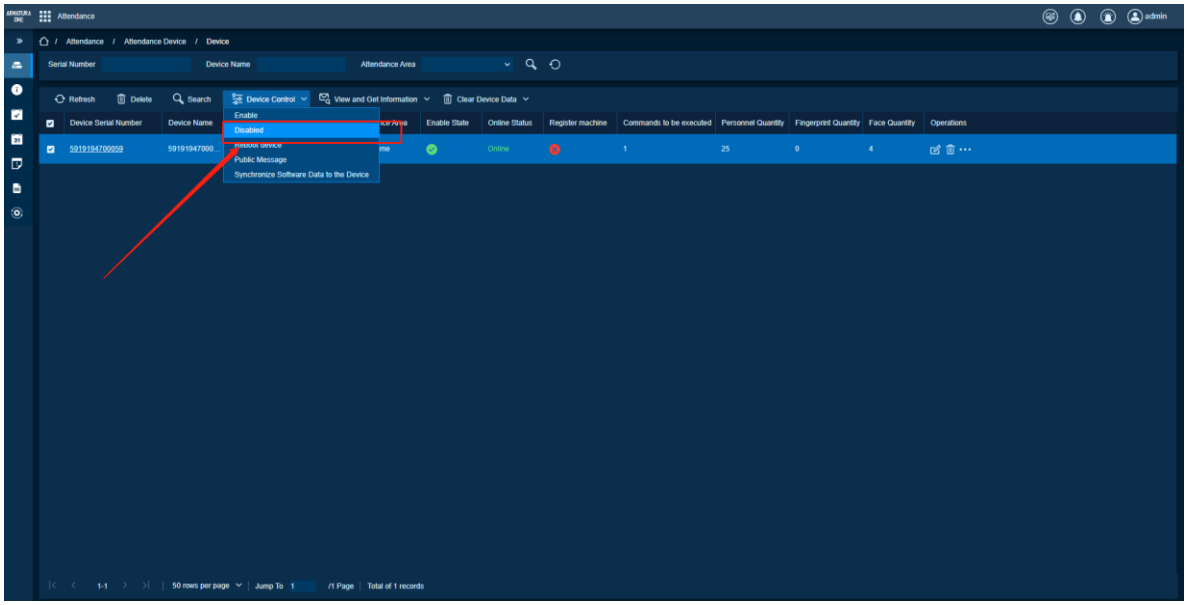
Feature Trigger Result

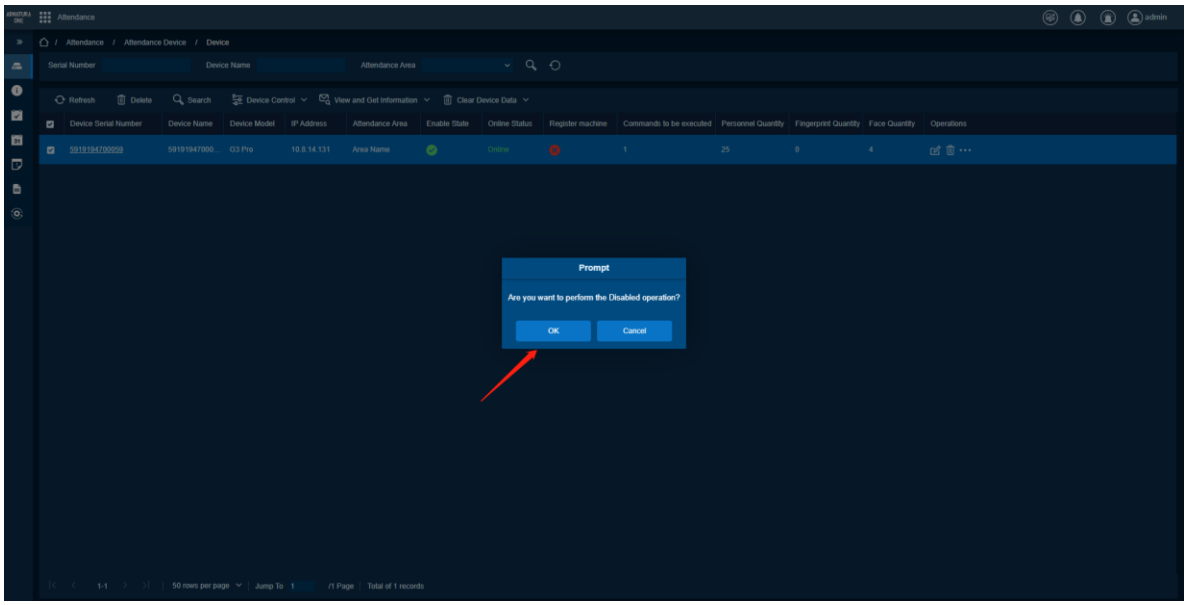
The device status changes to **[Disable]** and operations such as management settings cannot be performed.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list and click **[Device Control]** > **[Disable].**

- In the pop-up window, click **[OK]** to disable the device and click **[Cancel]** to cancel the disabling of the device.





Device Control-Restart Device

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

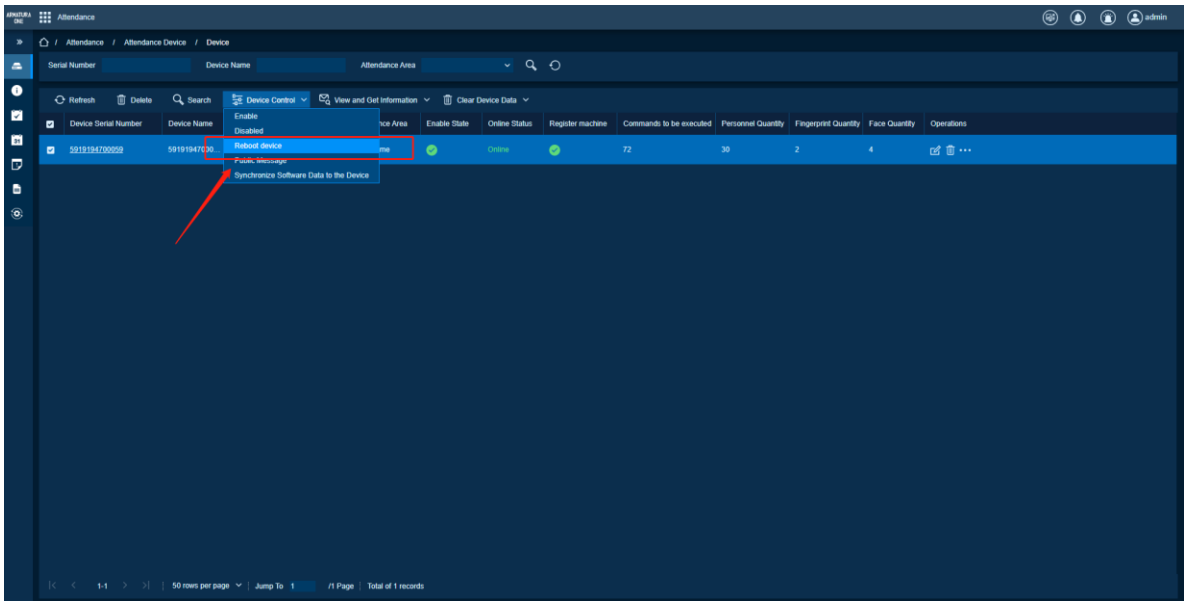
The device needs to be restarted.

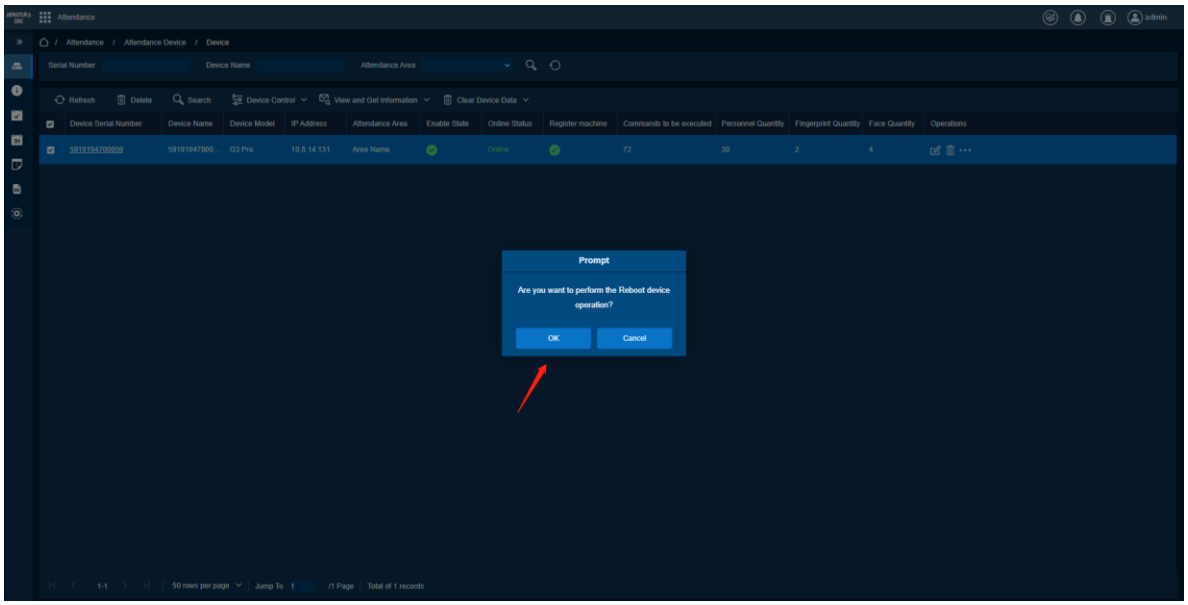
Feature Trigger Result

The device restarts to restore a certain state of the device.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list and click **[Device Control]** > **[Reboot device].**
- In the pop-up window, click **[OK]** to restart the device and click **[Cancel]** to cancel the restart of the device.





Device Control-Public Short Message

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

The device supports the function of public short message.

Function Usage Scenarios

The device can be set, so that the device can scroll through short messages on the page and notify personnel

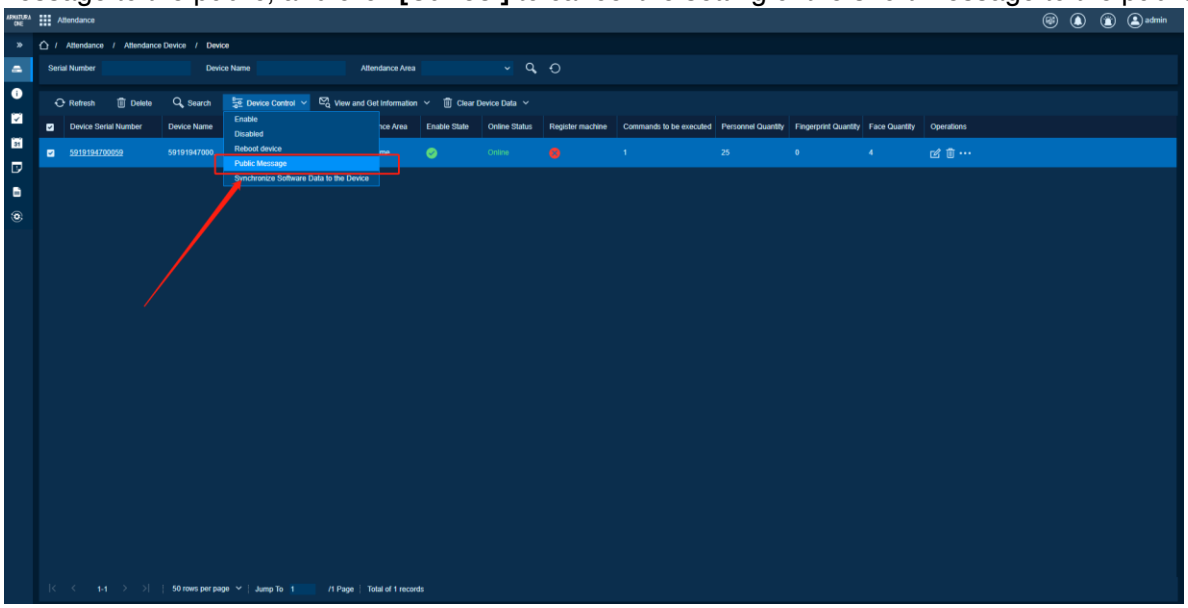
information during attendance.

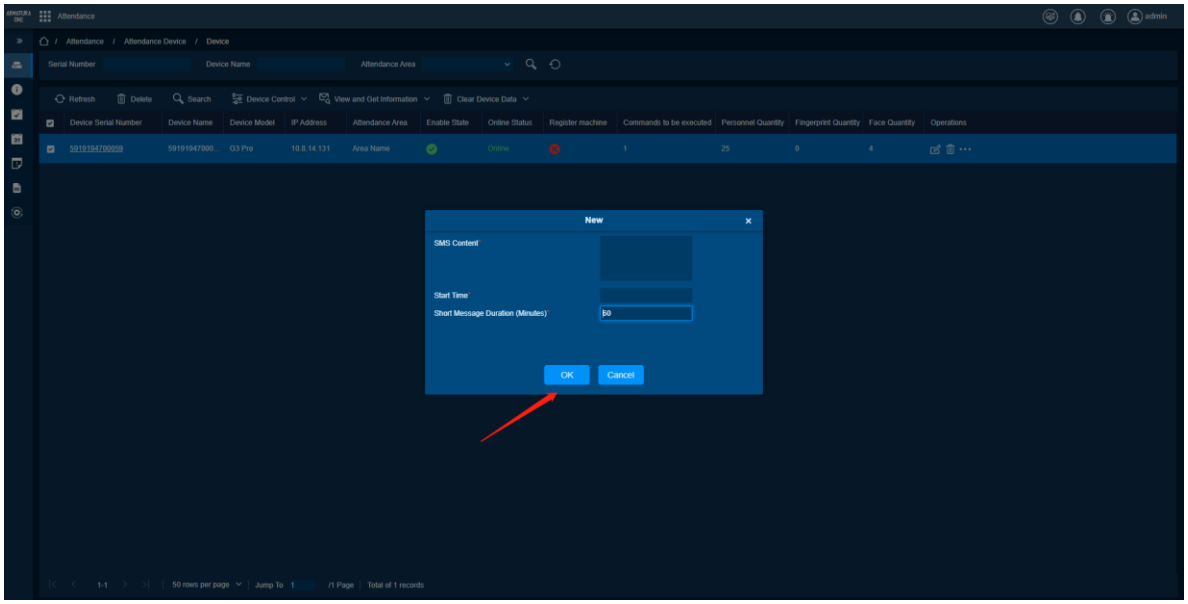
Feature Trigger Result

The short message can be viewed on the device when the staff is checking on work attendance.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list and click **[Device Control]** > **[Public Message].**
- After entering the content, start time and duration of the short message (minutes), click **[OK]** to set the short message to the public, and click **[Cancel]** to cancel the setting of the short message to the public.





Device Control-Synchronize Software Data to the Device

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

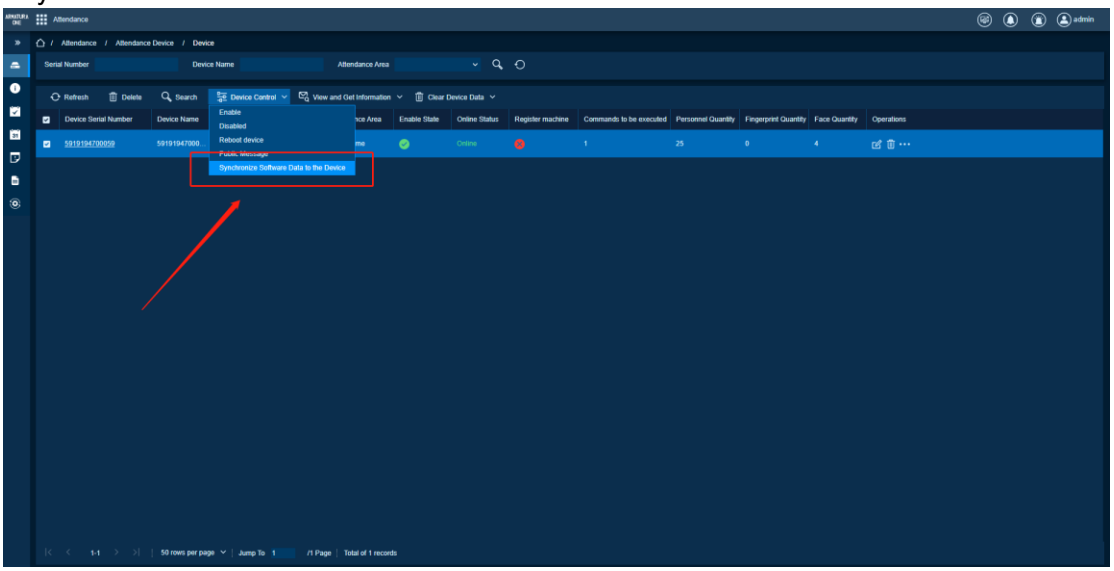
The data on the device is inconsistent with the data on the software.

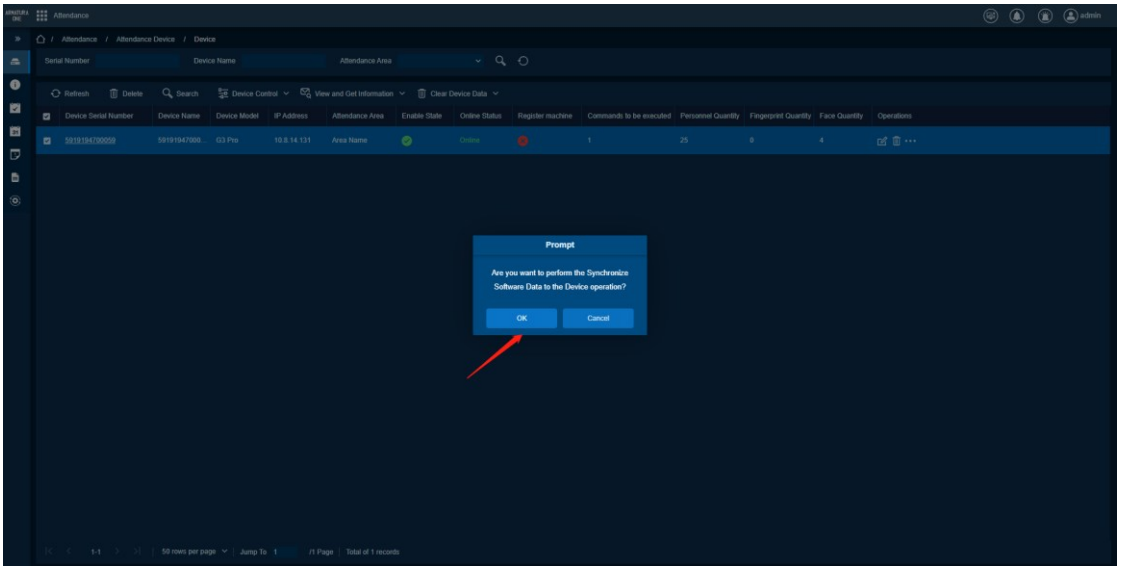
Feature Trigger Result

Send the corresponding device area data in the software to the device, and the data on the device is consistent with the data on the software.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance in the current list and click **[Device Control]** > **[Synchronize Software Data to the Device].**
- In the pop-up window, click **[OK]** to synchronize the software data to the device, and click **[Cancel]** to cancel the synchronize of the software data to the device.





View and Get Information-Get Device Parameters

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

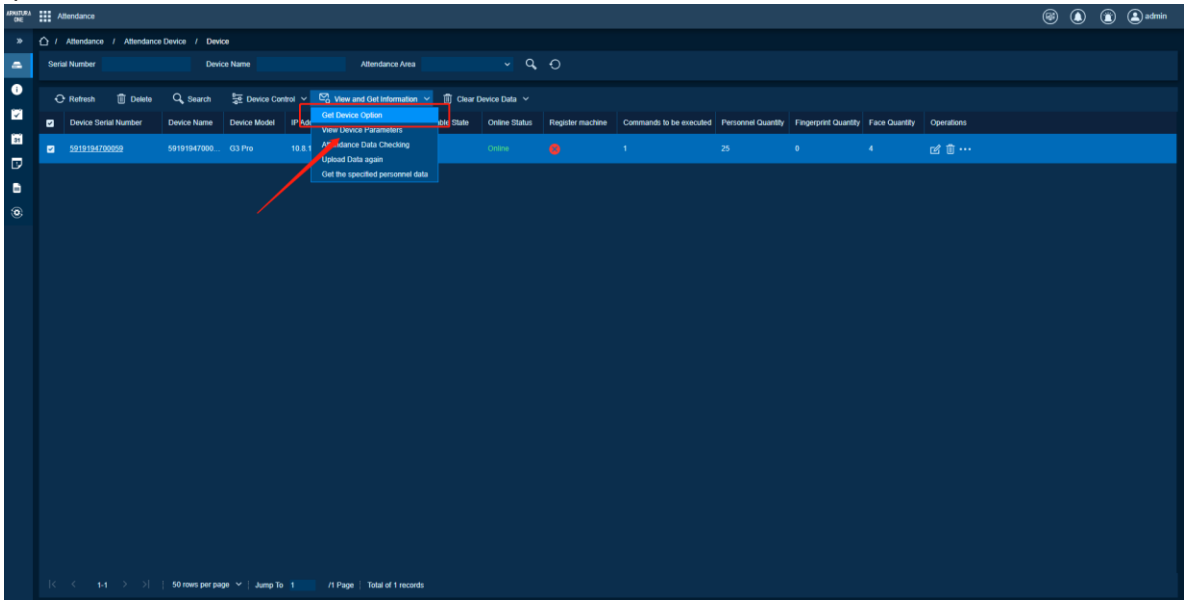
Need to obtain and view the attendance device parameters.

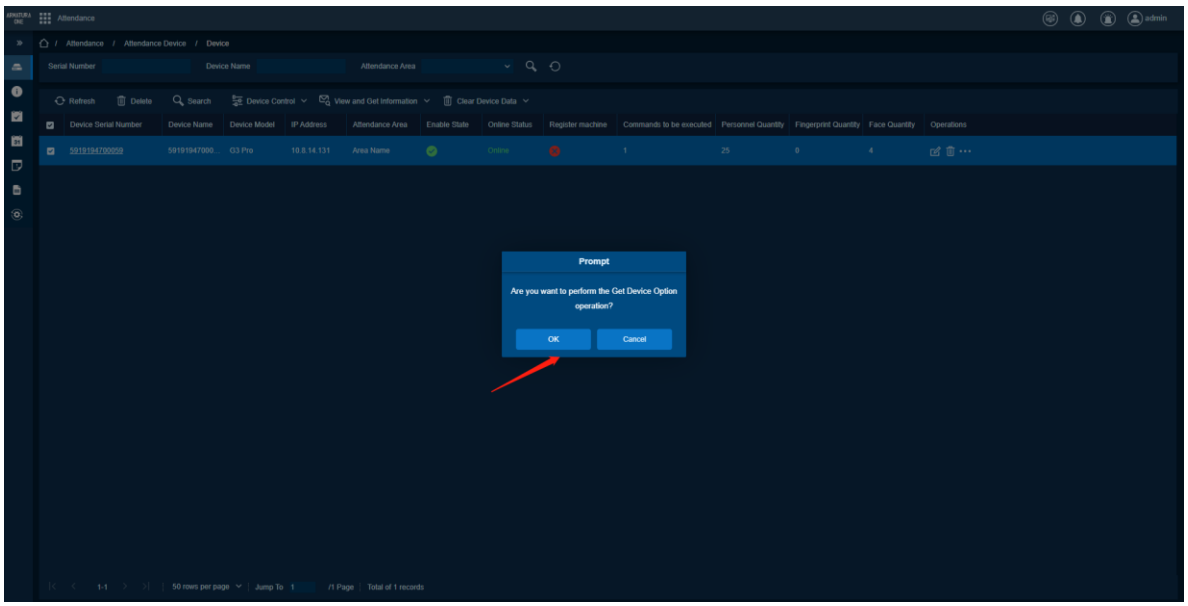
Feature Trigger Result

Get the attendance device parameters, you can click to view the device parameters to display the current device parameters.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, click **[View and Get Information]** > **[Get Device Option].**
- In the pop-up window, click **[OK]** to obtain device parameters and click **[Cancel]** to cancel obtaining device parameters.





View and Get Information-View Device Parameters

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

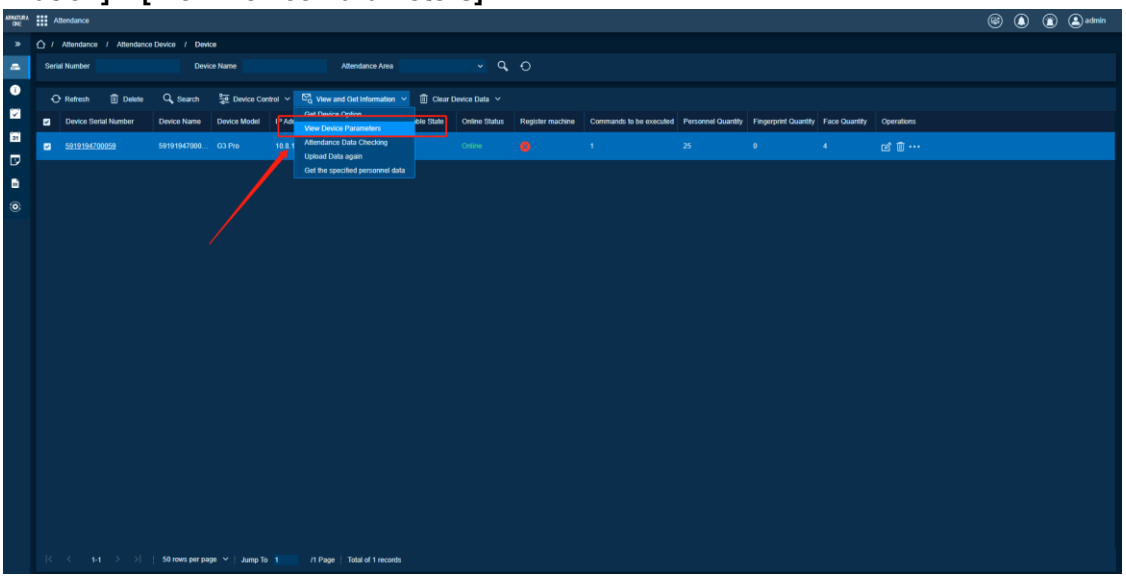
Need to check attendance device parameters.

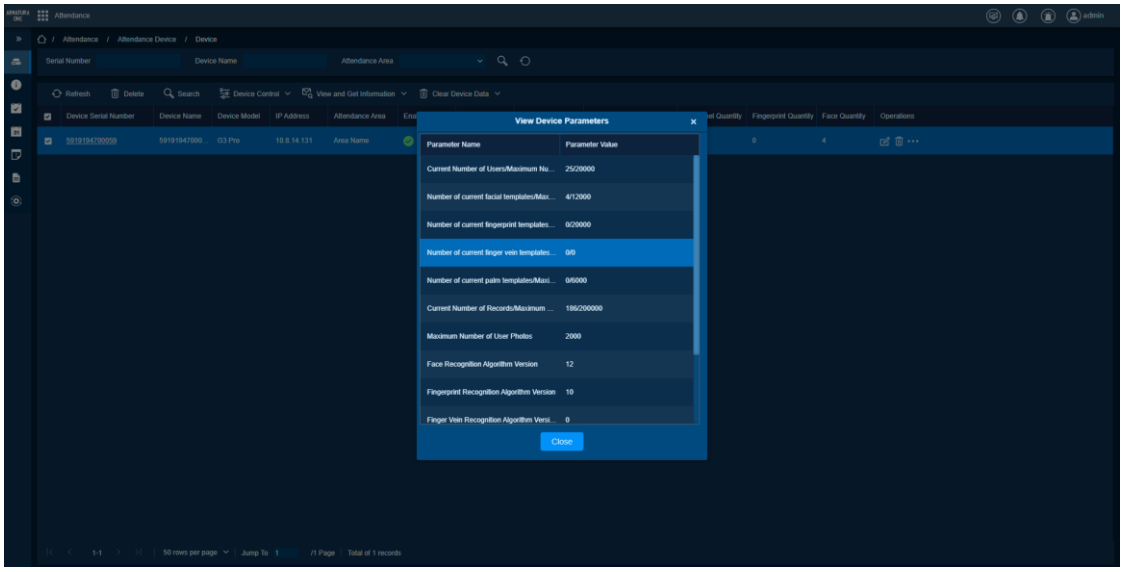
Feature Trigger Result

Page display device parameters.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, click **[View and Get Information]** > **[View Device Parameters]**.





View and Obtain Information-Proofreading of Attendance Data

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

Proofread the attendance data to make the software and device data accurate.

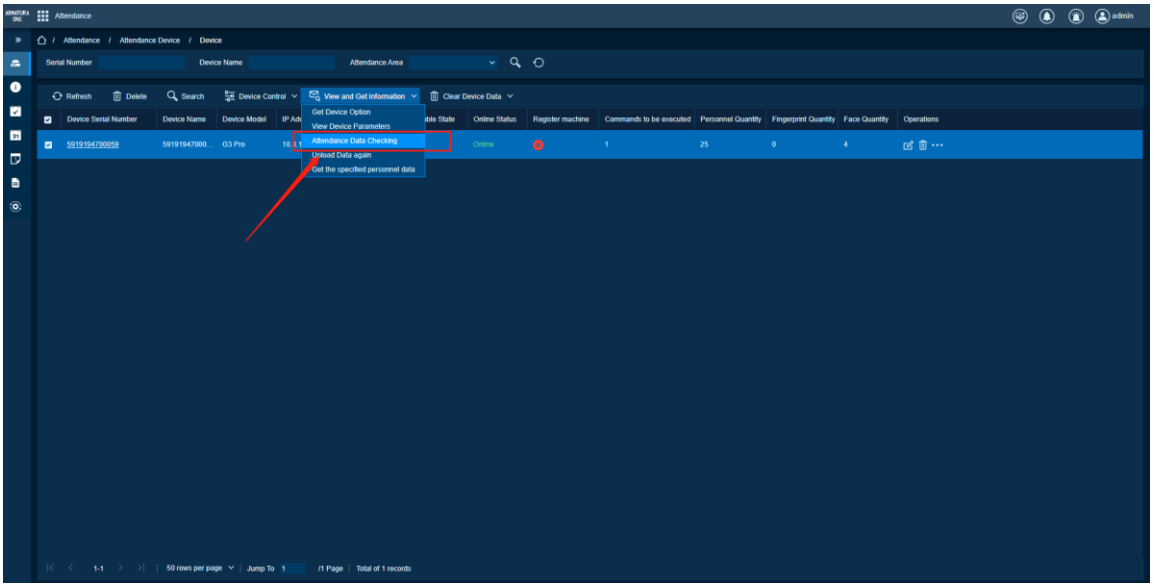
Feature Trigger Result

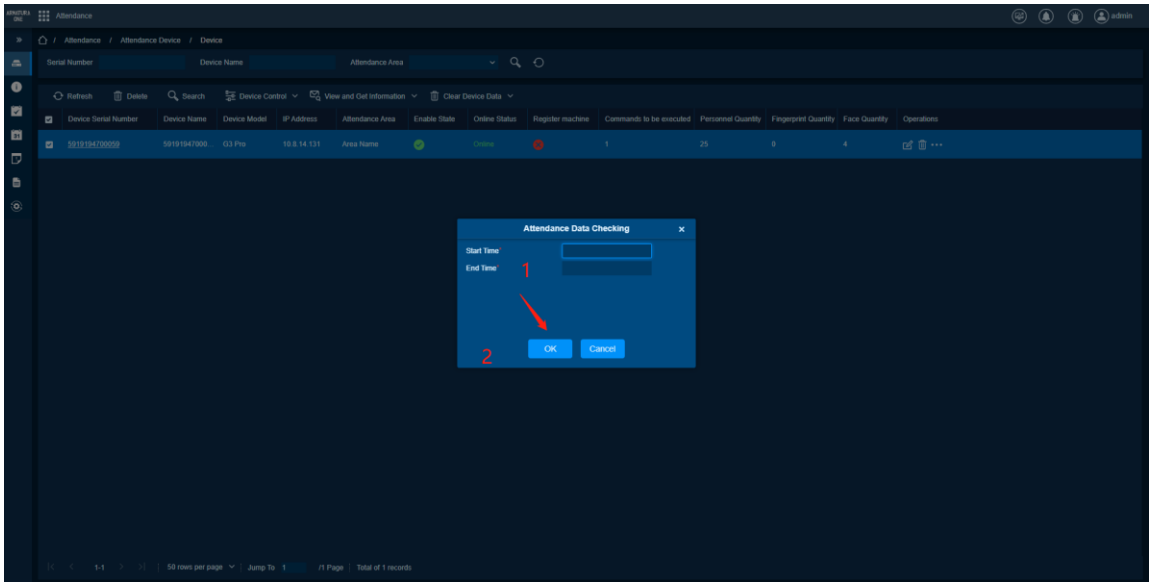
The software issues commands to verify the attendance.

Steps:-

Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, click **[View and Get Information]** > **[Attendance Data Checking].**

Select the **[Start Time]** and **[End Time]** of the proofreading, click **[OK]** to proofread the attendance data and click **[Cancel]** to cancel proofreading of the attendance data.





View and Obtain Information-Re-Upload Data

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

Need to upload the desired data: attendance records/personnel information/attendance photos and retrieve such information from the device.

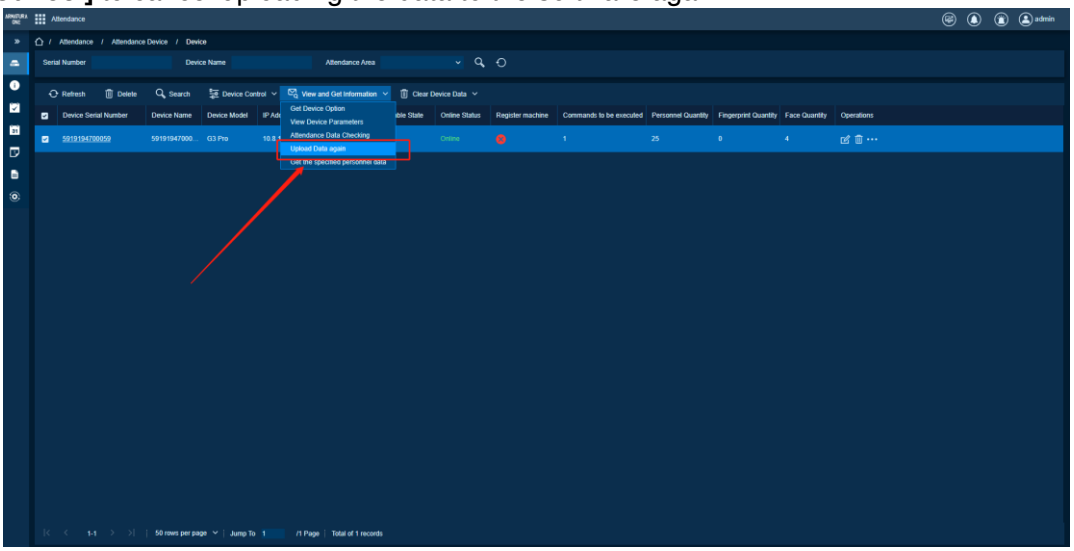
Feature Trigger Result

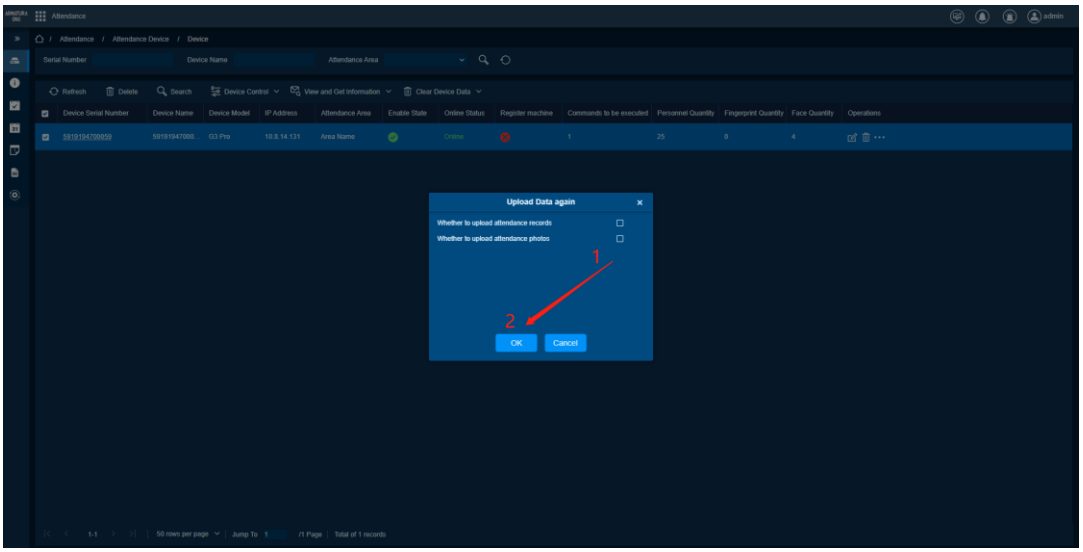
Upload the required data from the device to the software.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, click **[View and Get Information]** > **[Upload Data again].**

- Check the type of data that needs to be uploaded, click **[OK]** to upload the data to the software again, and click **[Cancel]** to cancel uploading the data to the software again.





View and Obtain Information-Obtain Designated Personnel Data

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

Personnel attendance data needs to be reconfirmed.

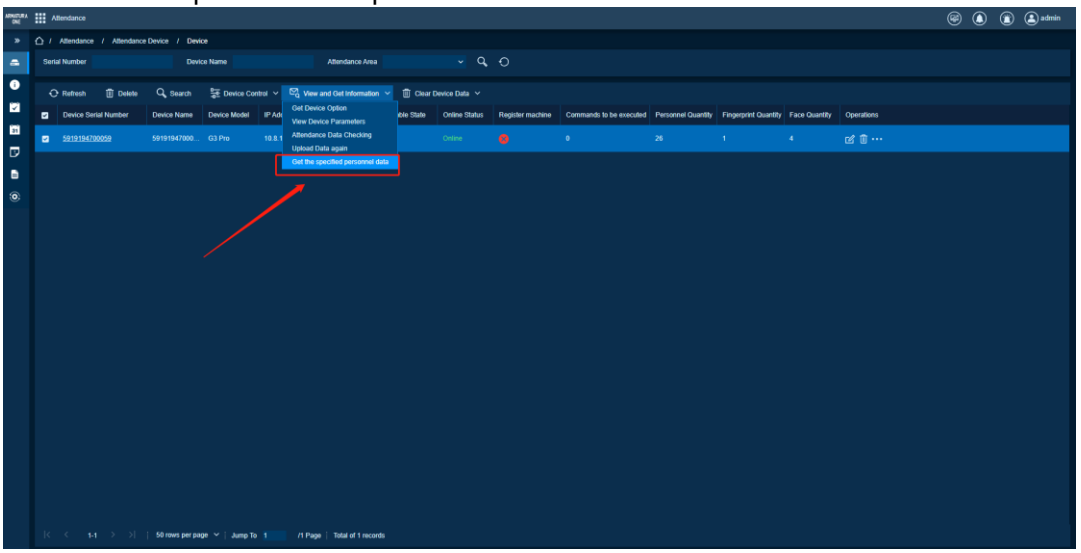
There are personnel attendance data in the device that have not been uploaded.

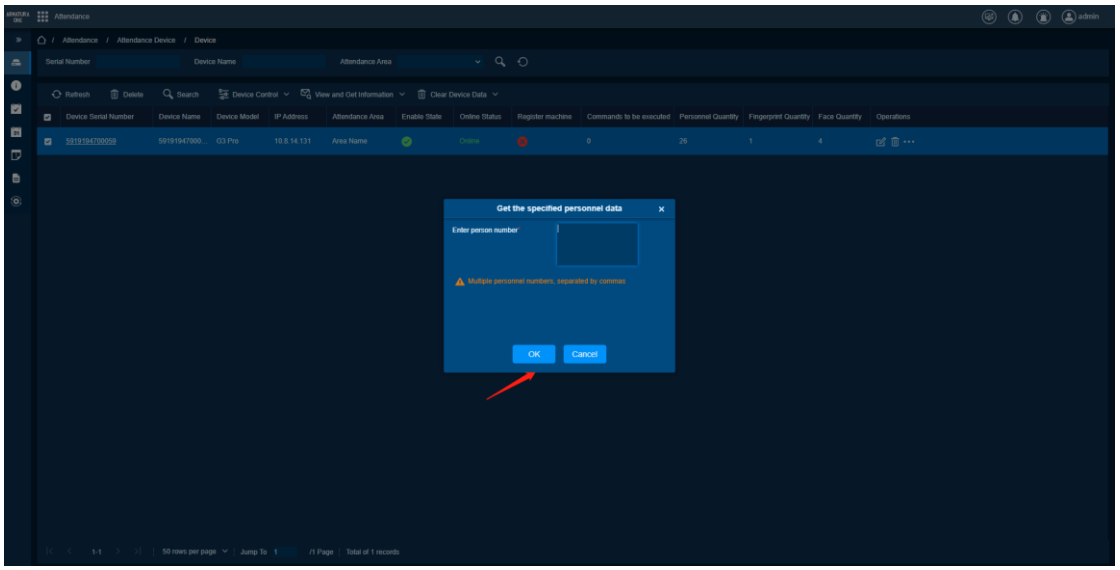
Feature Trigger Result

Obtain the data of the designated person from the device.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, click **[View and Get Information]** > **[Get the specified personnel data]**.
- Enter the number of the personnel you want to obtain, click **[OK]** to obtain the personnel data, and click **[Cancel]** to cancel the acquisition of the personnel data.





Clear Device Data-Clear Device Command

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

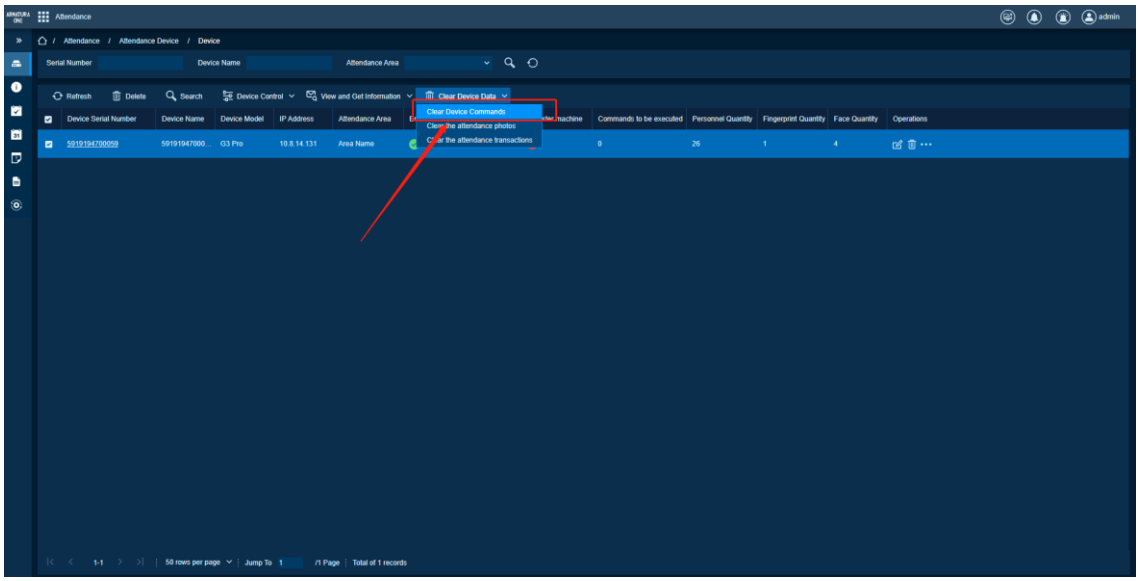
Avoid command stuck.

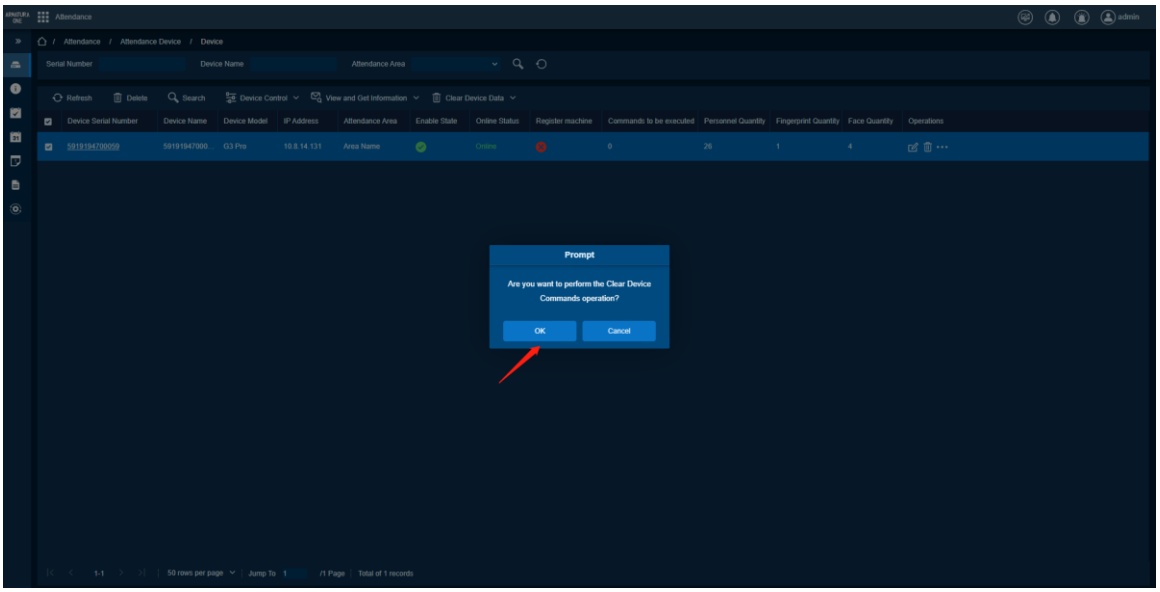
Feature Trigger Result

Clear the operating commands issued by the software in the settings.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, and click **[Clear Device Data]** > **[Clear Device Commands].**
- In the pop-up window, click **[OK]** to clear the device command, and click **[Cancel]** to cancel the clear device command.





Clear Device Data-Clear Attendance Photos

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

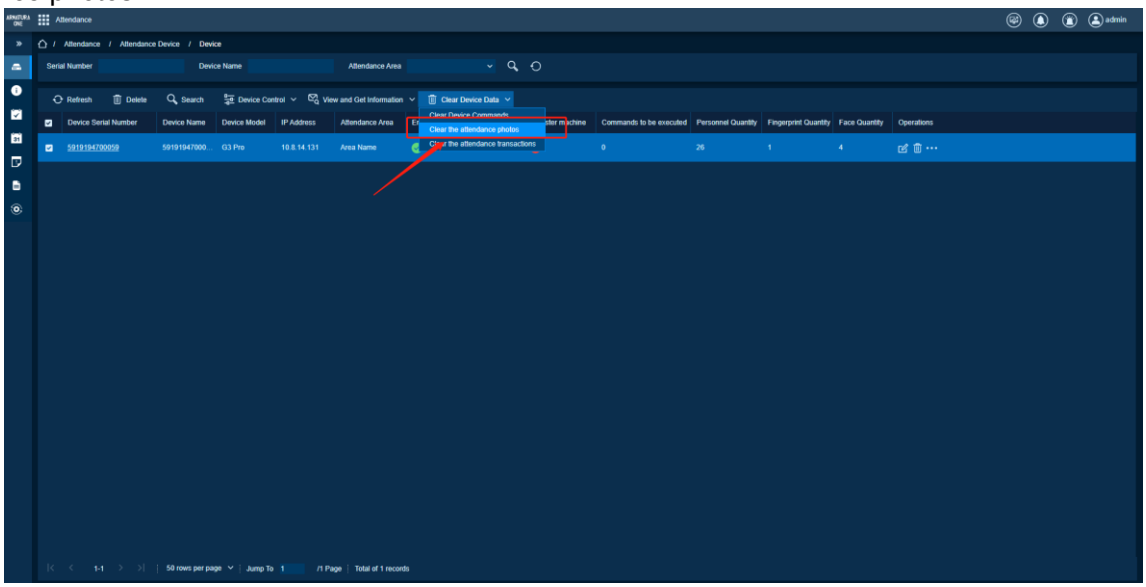
Clear the attendance photos in the device.

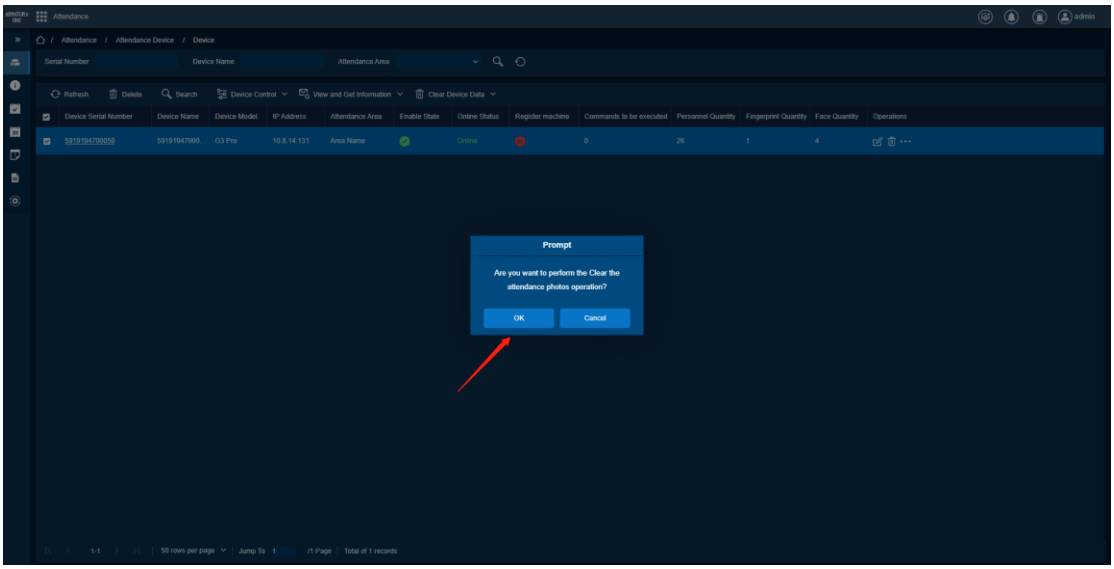
Feature Trigger Result

All attendance photos in the device are cleared.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, and click **[Clear Device Data]** > **[Clear the attendance photos].**
- In the pop-up window, click **[OK]** to clear attendance photos, and click **[Cancel]** to cancel clearing attendance photos.





Clear Device Data-Clear Attendance Record

Preconditions for Normal Use of Function

The software has successfully added the device and the device is online.

Function Usage Scenarios

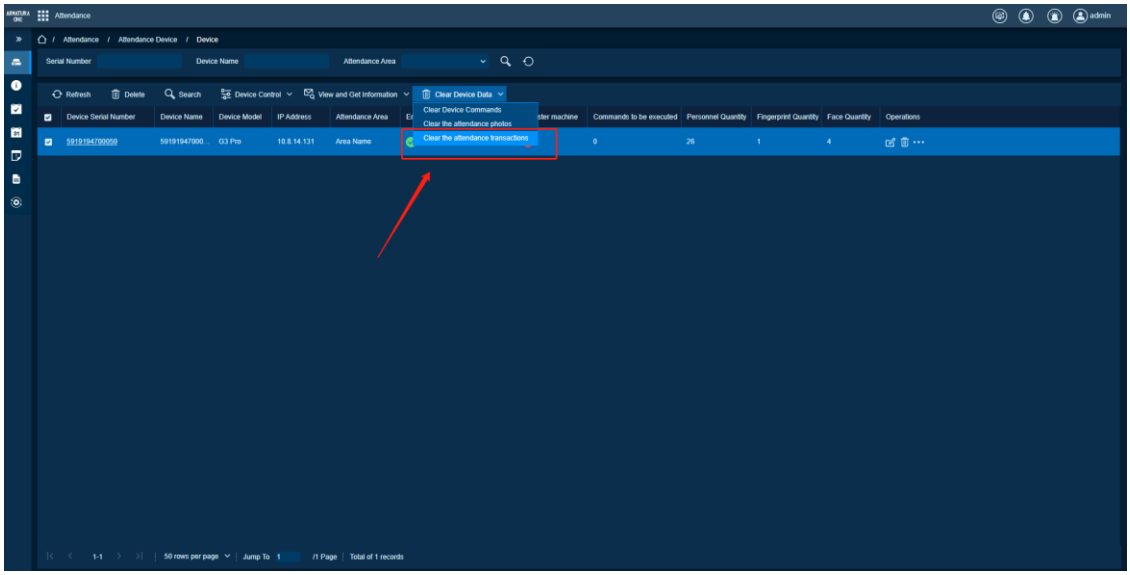
Clear the attendance data record in the device.

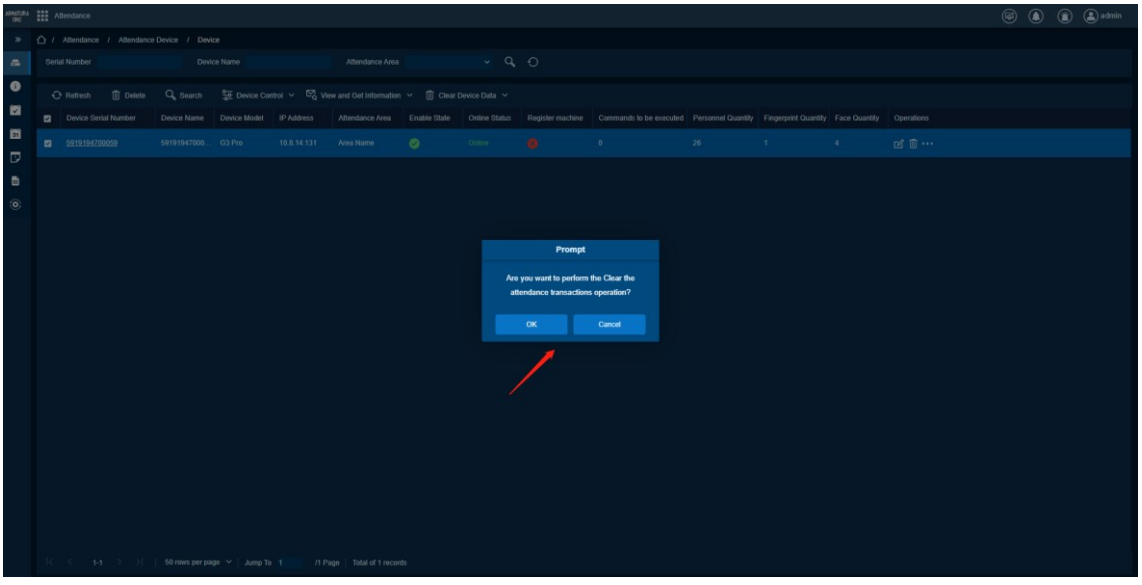
Feature Trigger Result

All attendance data records in the setting are cleared.

Steps:-

- Click **[Attendance Device]** > **[Device]**, select the attendance device in the current list, and click **[Clear Device Data]** > **[Clear the attendance transactions]**.
- In the pop-up window, click **[OK]** to clear attendance records, and click **[Cancel]** to cancel clearing attendance records.





7.1.4. Attendance Point

Function Description

Use this function to link the device of the access control/parking/FaceKiosk/video to set the corresponding attendance point, flexibly manage and operate the attendance point, and personnel can perform attendance at the attendance point.

New Attendance Point

Preconditions for Normal Use of Function

The system has a setting area.

Function Usage Scenarios

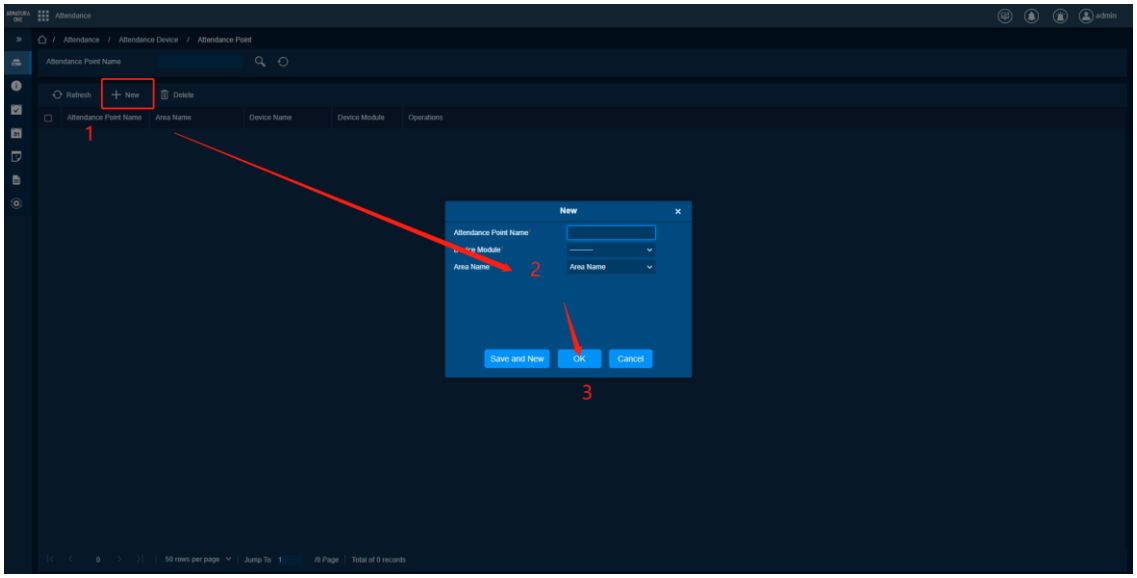
Personnel perform attendance at the set attendance point.

Feature Trigger Result

After adding an attendance point, personnel can perform attendance at the attendance point.

Steps:-

1. Click **[Attendance Device] > [Attendance Point],** click add, enter the attendance point name, and select the device module and area.
2. Click **[Save and Continue]** to add an attendance point, the page will not close, you can continue to add, click [OK] to add an attendance point, click **[Cancel]** to cancel the selection.



Delete Attendance Point

Preconditions for Normal Use of Function

Attendance point has been successfully added.

Function Usage Scenarios

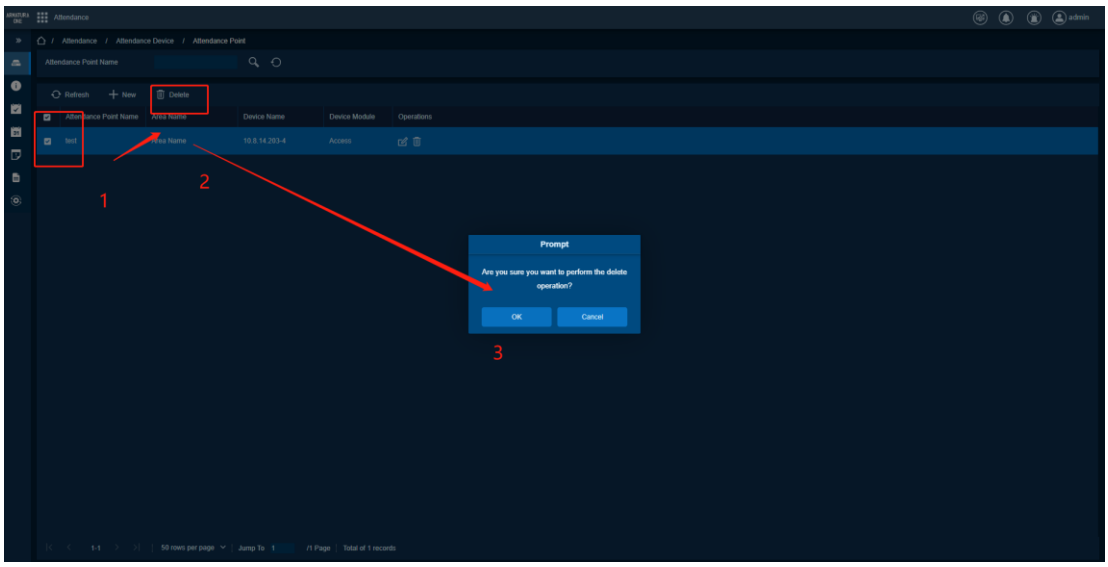
Remove and replace attendance point.

Feature Trigger Result

1. The attendance point list does not display the deleted attendance point.
2. The staff's attendance at the deleted attendance point is invalid.

Steps:-

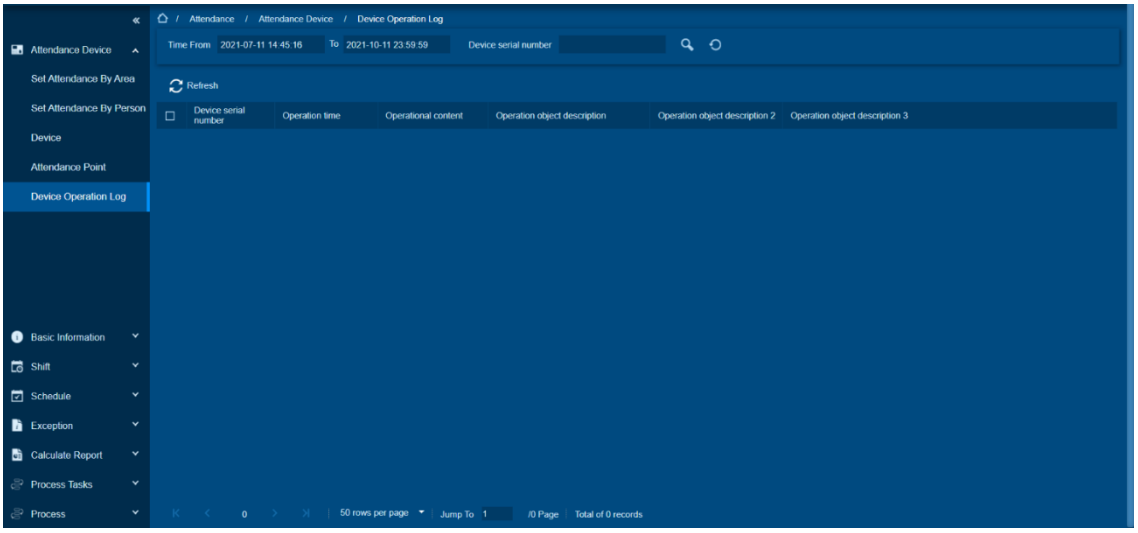
1. Click **[Attendance Device] > [Attendance Point],** select the attendance point, and click **[Delete].**
2. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.1.5. Device Operation Log

Function Description

It displays the operation log of attendance device, search for detailed operation of attendance device according to data and serial number.



7.2. Basic Information

Function List

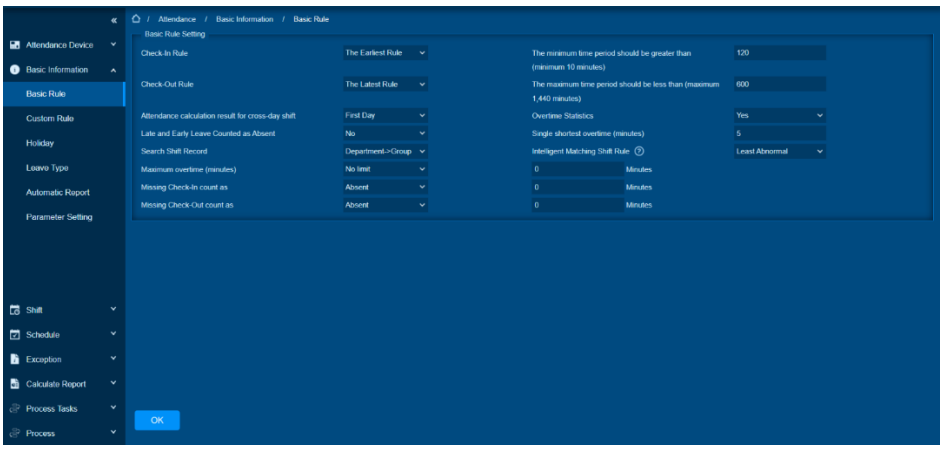
Functions	Description
Basic Rules	Set up basic rules of attendance, such as On/Off Work Sign-in and Card Collection Record Principle, Attendance Period, Maximum Overtime Duration, whether to Count Overtime, Search for Shift Record Sequence and Sign-in/Sign-out Record Status, etc.
Custom Rule	Add, edit, and delete custom rules.
Holidays	Add, edit, and delete holidays.
Holiday Types	Operations such as adding, editing, and deleting holiday types.
Auto Export	Add, edit, and delete auto export settings, enable, and disable auto export settings.
Parameters Setting	Set attendance parameters, such as hour conversion basis, day number conversion basis, absentee days conversion basis, attendance result indication symbol, timing calculation, and enable and disable employee self-service login.

7.2.1. Basic Rule

Function Description

According to the different needs of users of each company, basic attendance rules can be manually set to ensure the accuracy of the final attendance calculation.

Basic Rule Setting



- **Principles of work check-in and card collection records:** The earliest principle (by default, the first check-in record is taken within the valid card collection range), the nearest principle (the check-in record closest to working hours is taken within the valid card collection range).
- **The principle of check-out and withdrawal record after getting off work:** The latest principle (by default, the latest check-in record is taken within the valid card withdrawal range), the nearest principle (the check-in record closest to the off-duty time is taken within the valid card withdrawal range).
- **The shortest attendance period should be greater than (10 minutes):**120 default; range: 10-999; required.
- **The longest attendance period should be less than (1440 minutes):** 600(default); range: 10-1440; required.
- **Arriving late and leaving early are counted as absenteeism:** No (default), yes; if set to Yes, there are late and early leave, and the time is recorded as absenteeism.
- **When the shift time zone is cross-day, the attendance calculation result:** The first day is the case of cross-day, and the working time in the effective shift on the second day is counted into the first day. On the second day, the working time in the effective shift on the first day is counted to the second day under the cross-day situation.
- **Find the sequence of scheduling records:** Department-group, group-department; attendance calculation to find the priority order of the shift.
- **Whether to count overtime:** Yes (default), No; the first switch for counting overtime, if set to No, overtime will not be counted.
- **Principles of intelligent shift finding:** The longest duration and the fewest exceptions(default); the longest duration is to calculate each shift separately and get the one with the most effective duration; the least exception is to analyze each shift separately and get the exception the shift with the least number (such as being late, leaving early, etc.)
- **Minimum overtime duration (minutes):** This parameter is used for the duration statistics of overtime rules. If the overtime duration is less than the set minimum overtime duration, it will not be reflected in the attendance statistics.
- **Maximum overtime duration:** Unlimited (default), this week and this month; set the overtime duration.
- **Unchecked in is recorded as:** Absence (default), leave early, and incomplete; define the attendance settings for those who have not checked in.
- **Non-sign-out is recorded as:** Absence (default), early-leave and incomplete; define the attendance of personnel who have not signed-out.

7.2.2. Custom Rule

Function Description

Since users of different companies have different requirements for the attendance system, the attendance rules can be customized, and the setting of attendance parameters can be flexibly handled to facilitate the use of the company's internal attendance system.

Add Custom Rule

Preconditions for Normal Use of Function

Custom Rule name is not used.

Function Usage Scenarios

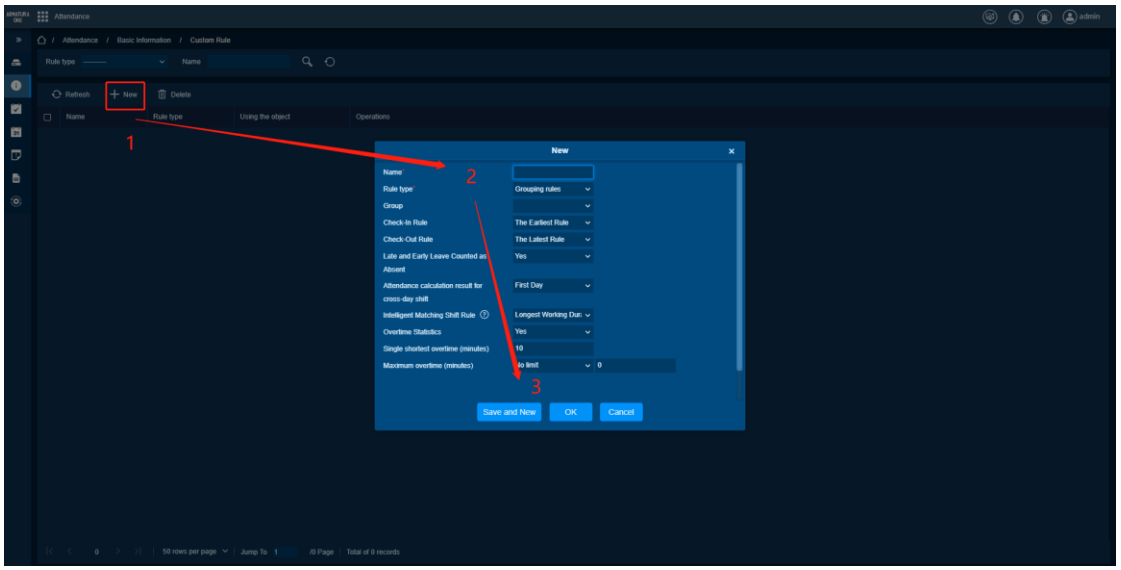
Customized grouping rules and departmental rules can be flexibly used for grouping or department staff attendance.

Feature Trigger Result

- Generate multiple custom rules.
- Grouping rules can be added to the shift grouping module.
- It can be applied to the attendance rules of the department.

Steps:-

- Click **[Basic Information] > [Custom Rule], click [Add]** and enter the rule information.
- Click **[Save and Continue]** to add a new custom rule, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Edit Custom Rule

Preconditions for Normal Use of Function

Successfully added custom rule.

Function Usage Scenarios

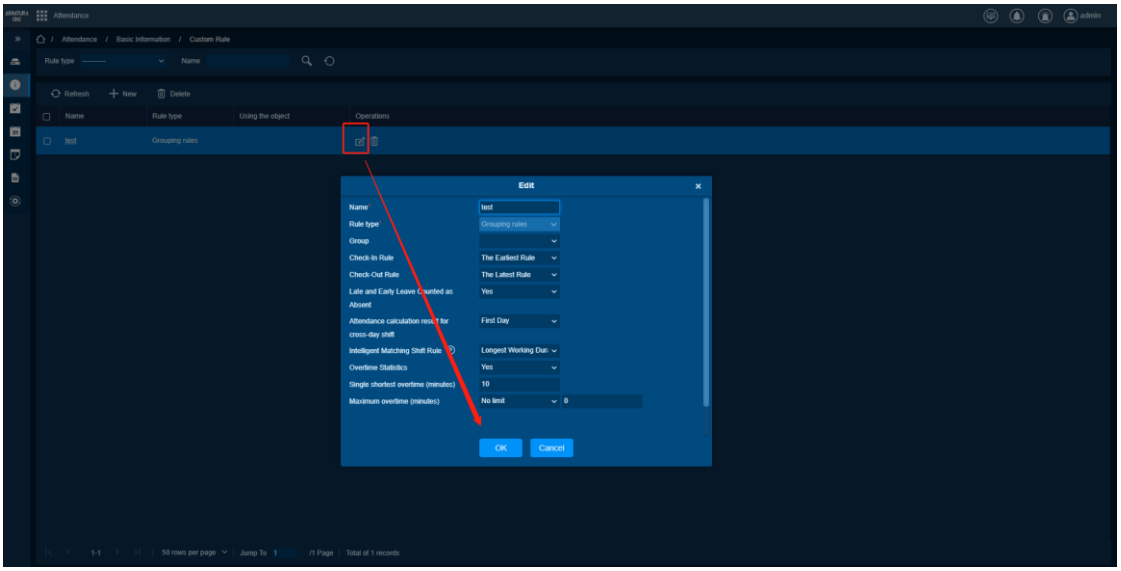
Custom Rule setting error (rule type cannot be edited)

Feature Trigger Result

If the custom rule is edited successfully, the grouping and department rules in the application will also be successfully modified.

Steps:-

- Click **[Basic Information]** > **[Custom Rule]**, click **Custom Rule**, click **[Edit]**.
- Modify rule information, click **[OK]** to edit custom rule, click **[Cancel]** to cancel editing.



Delete Custom Rule

Preconditions for Normal Use of Function

Successfully added custom rule.

Function Usage Scenarios

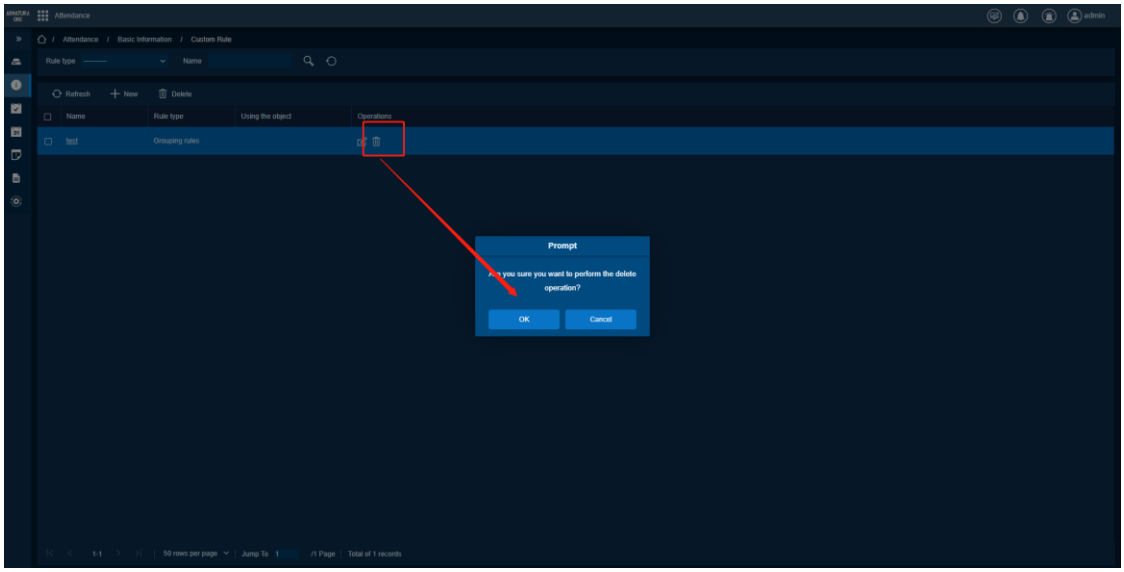
- The custom rule is not required.
- Wrong choice of rule type.

Feature Trigger Result

- No longer displayed in the custom rule list.
- The grouping rules in the scheduling management grouping module are also deleted.
- The department no longer checks attendance according to this rule.

Steps:-

- Click **[Basic Information]** > **[Custom Rule],** select custom rule, click **[Delete].**
- In the pop-up window, click **[OK]** to delete the custom rule and click **[Cancel]** to cancel the deletion.



7.2.3. Holiday

Function Description

Add, edit, and delete holidays information, improve the attendance system.

Add Holidays

Preconditions for Normal Use of Function

Holidays name is not used.

Function Usage Scenarios

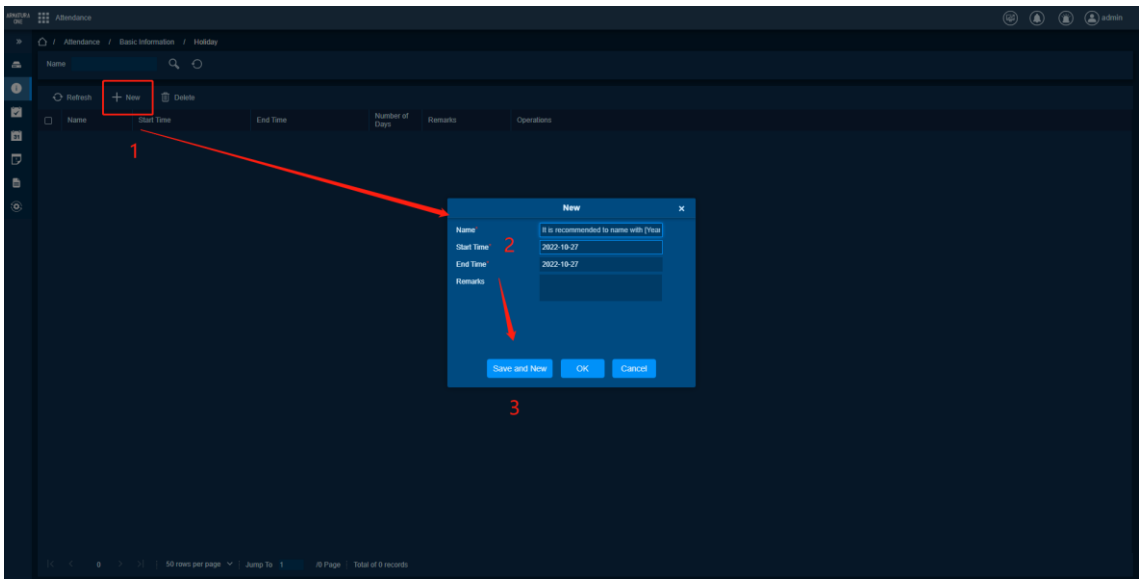
Set the attendance of staff holidays.

Feature Trigger Result

- Show in holidays list.
- It can be used to set the attendance of personnel holidays.

Steps:-

- Click **[Basic Information] > [Holiday],** click **[Add],** enter information.
- Click **[Save and Continue]** to add holidays, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Edit Holidays

Preconditions for Normal Use of Function

Holidays have been successfully added.

Function Usage Scenarios

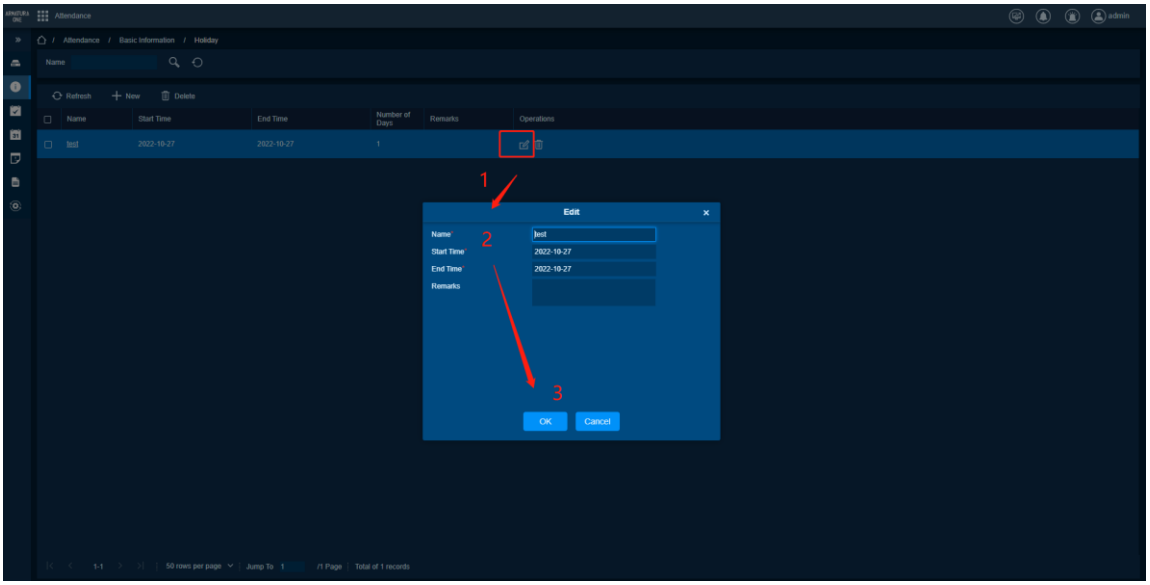
Holidays name, time and remarks need to be modified.

Feature Trigger Result

Holidays information is modified.

Steps:-

- Click **[Basic Information] > [Holiday],** select holidays, click **[Edit]**, enter the modification information.
- Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Holidays

Preconditions for Normal Use of Function

Holidays have been successfully added.

Function Usage Scenarios

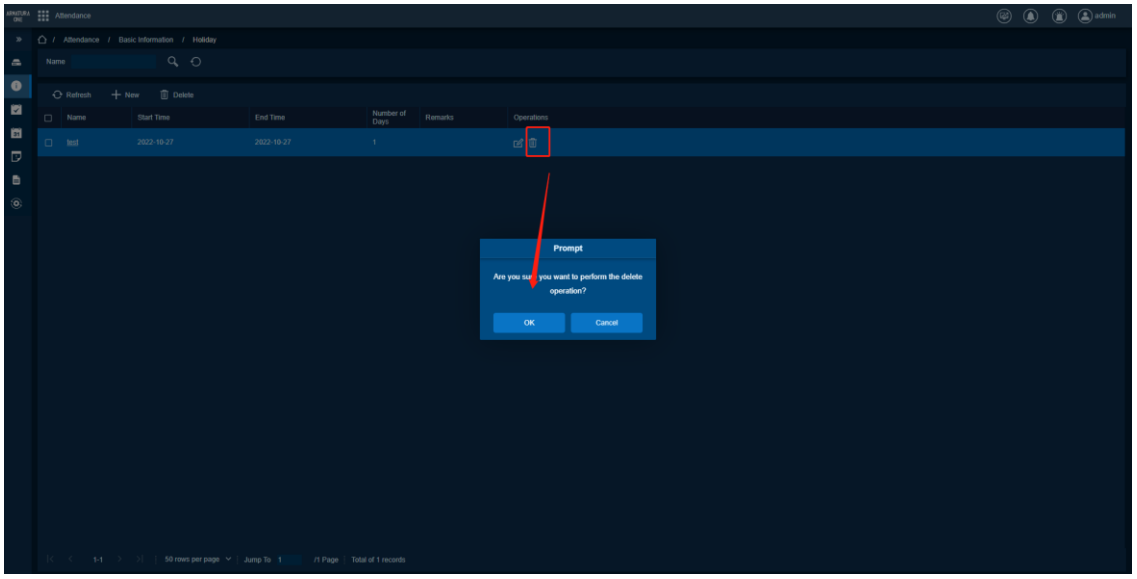
Do not need this time as holidays to participate in the attendance settings.

Feature Trigger Result

- Not shown in holidays list.
- Not participate in holidays attendance.

Steps:-

- Click **[Basic Information] > [Holiday],** select holidays, and click **[Delete].**
- Click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.2.4. Leave Type

Function Description

Add, edit, and delete leave types for personnel attendance settings and improve the attendance system.

Add Leave Types

Preconditions for Normal Use of Function

The name of the newly added leave types does not duplicate the name of the default leave types.

Function Usage Scenarios

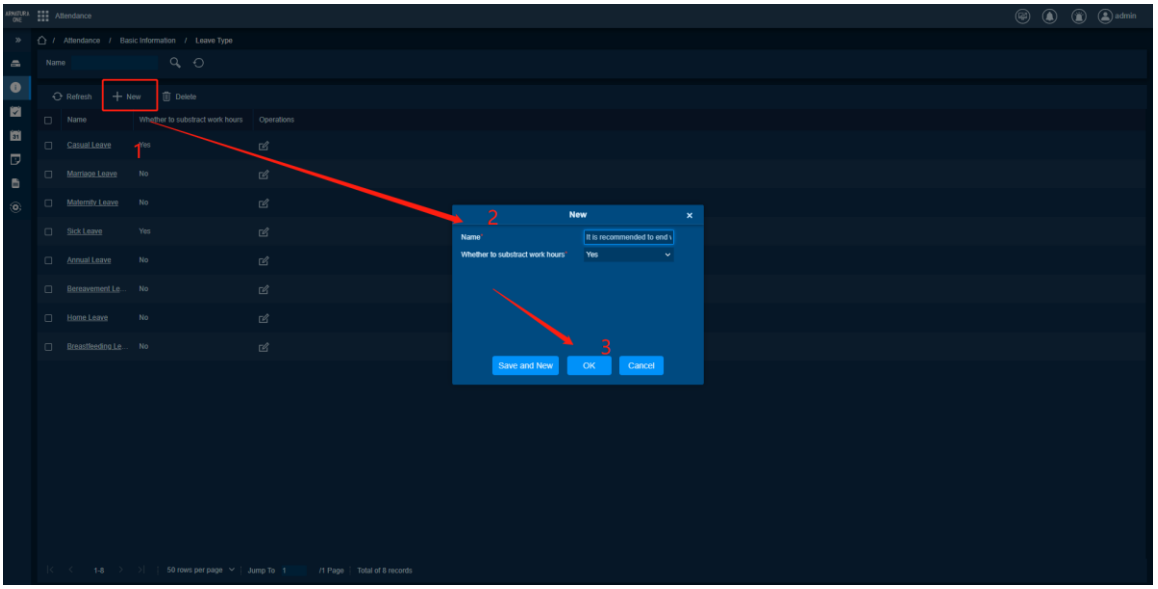
Used to set attendance and improve the attendance system.

Feature Trigger Result

- Displayed in the **Leave Types** List.
- Used for personnel attendance settings.

Steps:-

- Click **[Basic Information] > [Leave type],** click **[Add],** enter a name, and choose whether to deduct working hours.
- Click **[Save and Continue]** to add successfully, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel adding.



Edit Leave Types

Preconditions for Normal Use of Function

Existing default leave types or successfully adding leave types.

Function Usage Scenarios

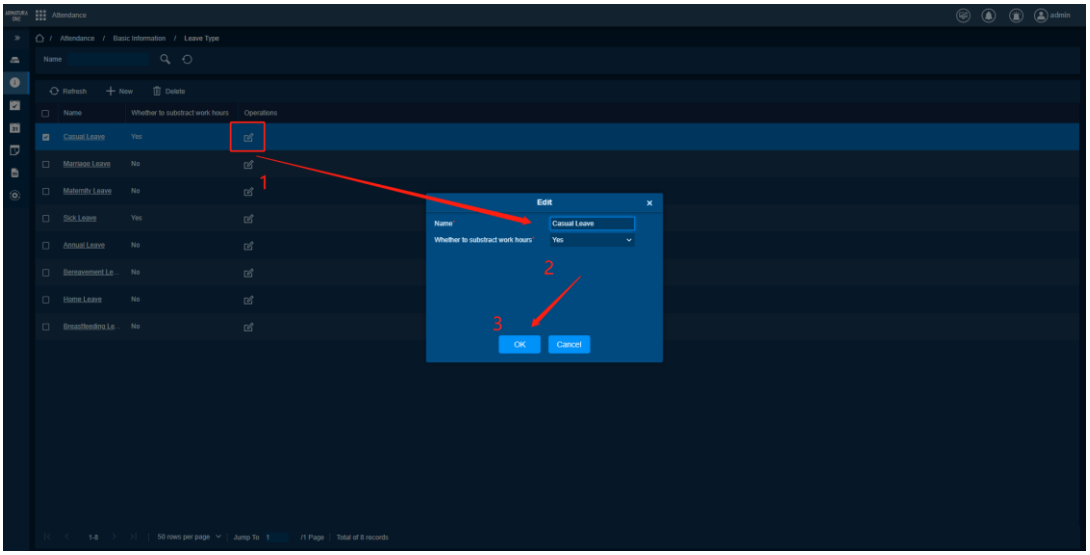
Leave types of information need to be modified.

Feature Trigger Result

The leave types of information are successfully modified and displayed correctly in the list.

Steps:-

- Click **[Basic Information] > [Leave Type],** select leave types, click **[Edit]** to modify the information.
- Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Leave types

Preconditions for Normal Use of Function

Leave types have been successfully added.

Function Usage Scenarios

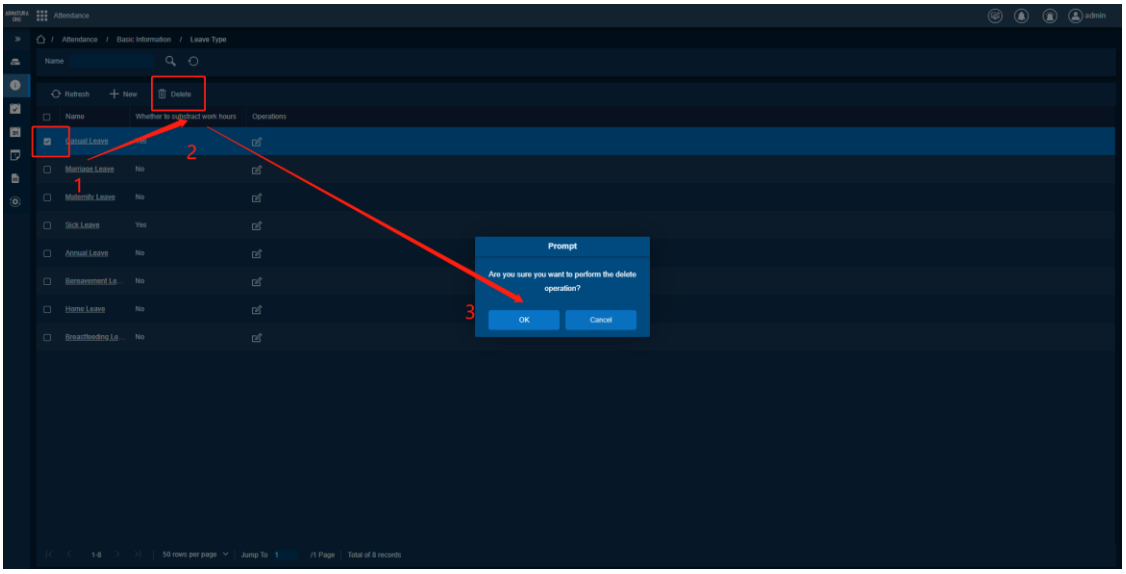
- Delete leave types that have been added successfully but are not needed.
- The default leave types cannot be deleted

Feature Trigger Result

- Not displayed in the leave types of lists.
- The deleted leave types do not participate in staff attendance settings.

Steps:-

- Click **[Basic Information] > [Leave Type]**, select leave types, click **[Delete].**
- Click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.2.5. Automatic Report

Function Description

Add, edit, and delete auto export templates, flexibly set the time and content for obtaining reports, and receive content at a specified frequency and time.

Add

Preconditions for Normal Use of Function

- When selecting the email sending method, the system needs to set the email parameters, and the function is available.
- When selecting the FTP sending method, ensure that the FTP communication is normal, and the function is available.

Function Usage Scenarios

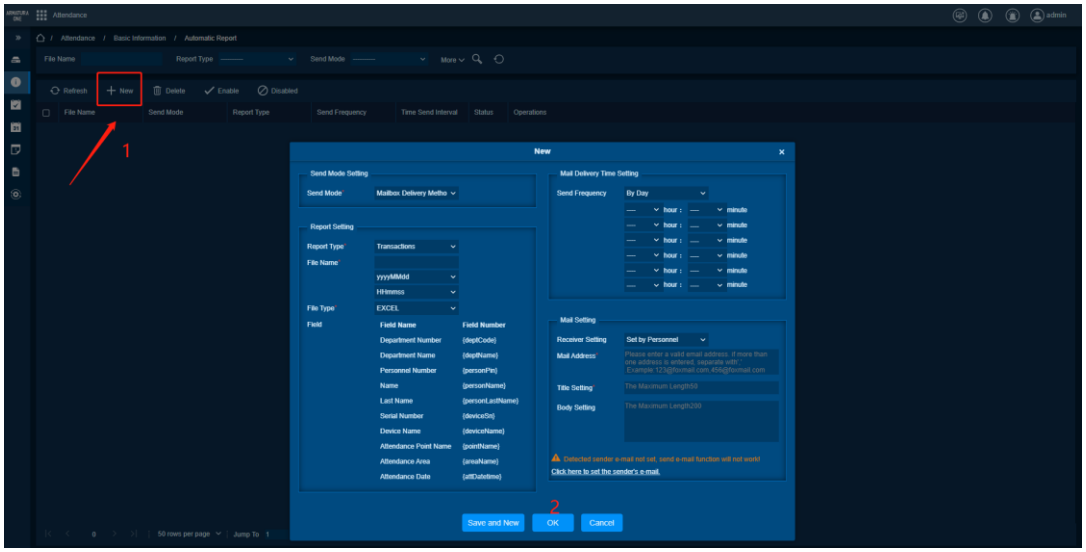
- The report needs to receive within the specified time
- It is necessary to set the automatic receiving frequency when obtaining the report.
- Receive reports via FTP or email.

Feature Trigger Result

- Send the original record sheet and daily punch card details sheet in the specified time, specified frequency and specified method
- Displayed on the Auto Export List.

Steps:-

- Click **[Basic Information] > [Automatic Report],** click **[Add],** enter related setting information.
- Click **[Save and Continue]** to add an auto export template, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Edit

Preconditions for Normal Use of Function

The auto export method has been successfully added.

Function Usage Scenarios

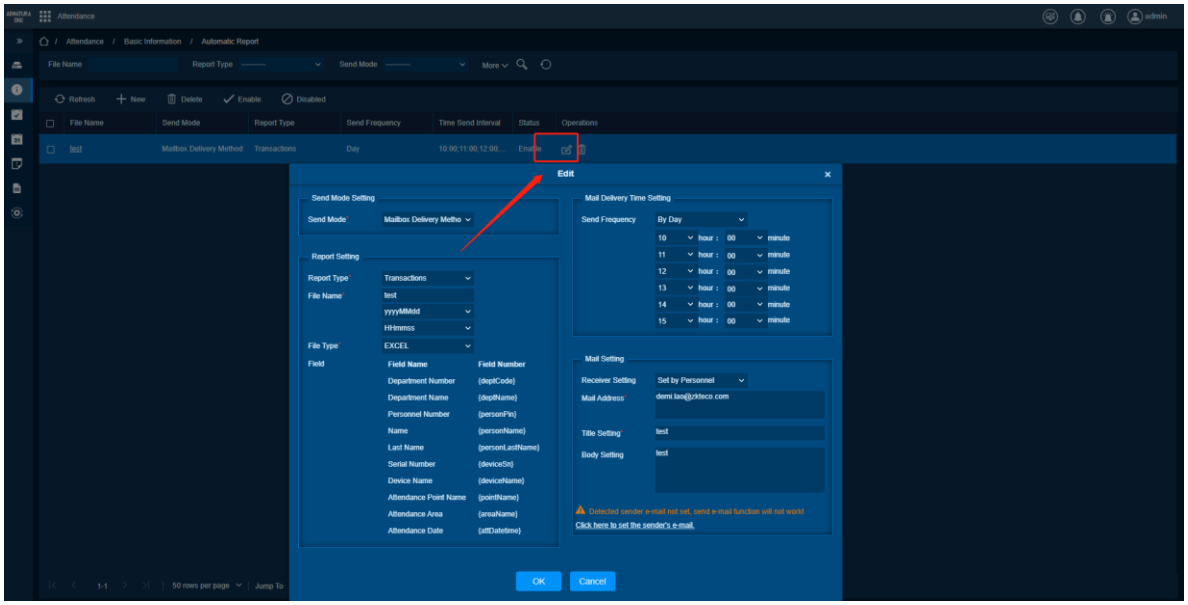
Need to modify the report type, sending time, frequency and sending method of the auto export method.

Feature Trigger Result

Successfully modify the settings of the auto export method.

Steps:-

- Click **[Basic Information] > [Automatic Report],** select an auto export setting, click **[Edit]** to modify the information.
- Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete

Preconditions for Normal Use of Function

The auto export method has been successfully added.

Function Usage Scenarios

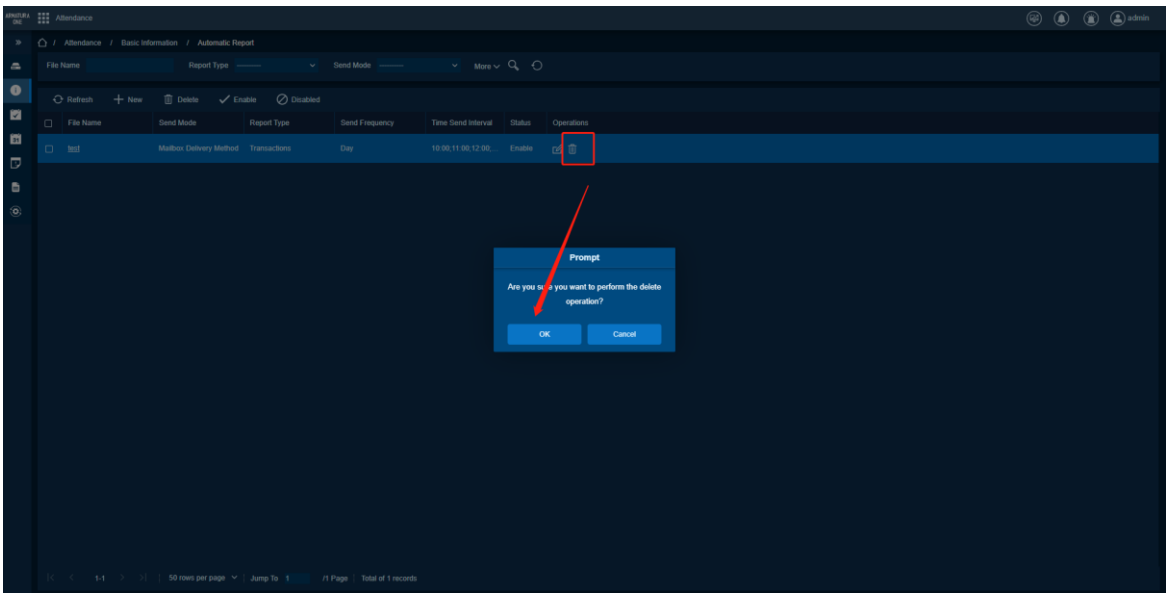
No need to use this automatic setting.

Feature Trigger Result

- The setting of the deleted automatic method is invalid.
- Not displayed in the list of automatic mode settings.

Steps:-

- Click **[Basic Information] > [Automatic Report]**, select an auto export setting, click **[Delete].**
- In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



Enable

Preconditions for Normal Use of Function

The auto export method has been successfully added.

Function Usage Scenarios

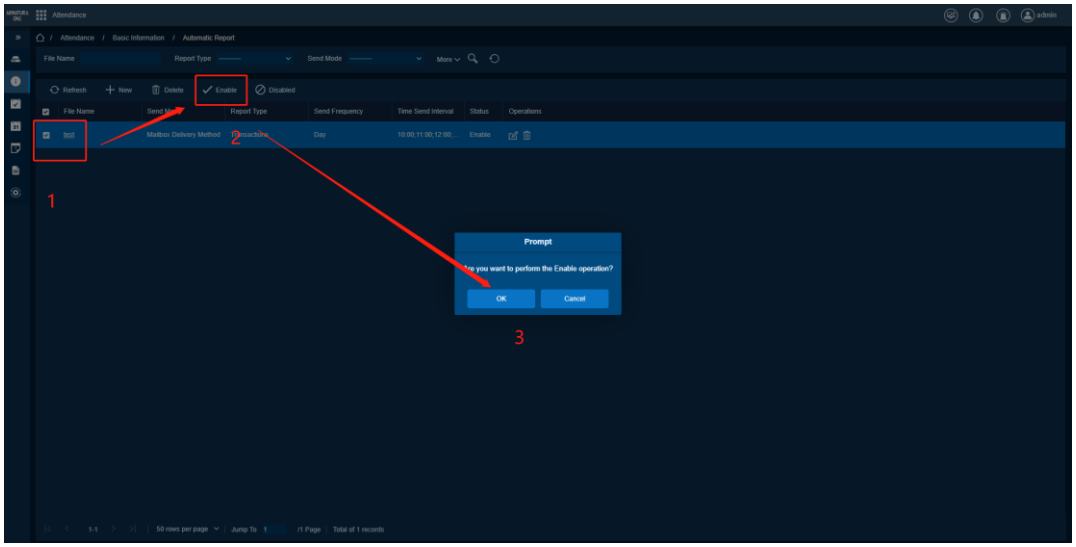
- Need to enable the auto export function that has been set.
- The auto export status of the newly added setting is enabled by default.

Feature Trigger Result

The auto export function takes effect, and according to its settings, the specified report will be sent at the specified time and frequency in a specified manner.

Steps:-

- Click **[Basic Information]** > **[Automatic Report],** select an auto export setting, click **[Enable].**
- In the pop-up window, click **[OK]** to activate successfully, and click **[Cancel]** to cancel the activation.



Disable

Preconditions for Normal Use of Function

- The auto export method has been successfully added.
- Auto export method of setting is enabled.

Function Usage Scenarios

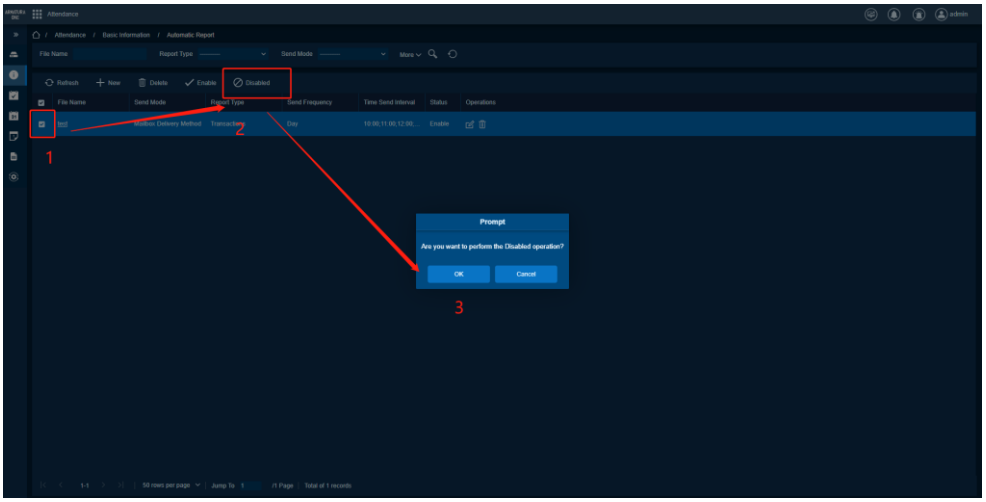
Currently there is no need to use the set auto export method.

Feature Trigger Result

- The auto export function setting is disabled and currently does not take effect.
- The auto export setting status is displayed as “Disabled”.

Steps:-

- Click **[Basic Information]** > **[Automatic Report]**, select an auto export setting, click **[Disable].**
- In the pop-up window, click **[OK]** to disable successfully, click **[Cancel]** to cancel the disable.

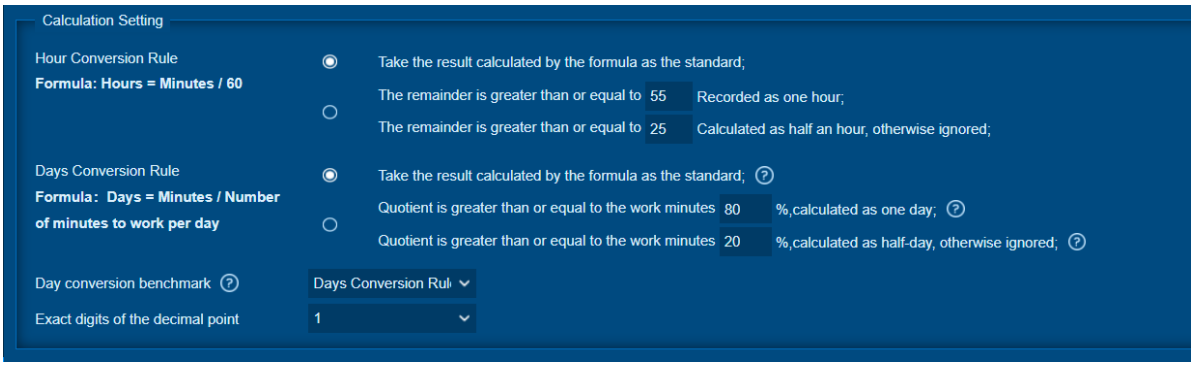


7.2.6. Parameter Setting

Function Description

Flexible setting of attendance related parameters, such as Calculation Conversion Settings, Attendance Display Symbols, Timing Calculations and Employee Self-Service Login.

Calculation Conversion Settings

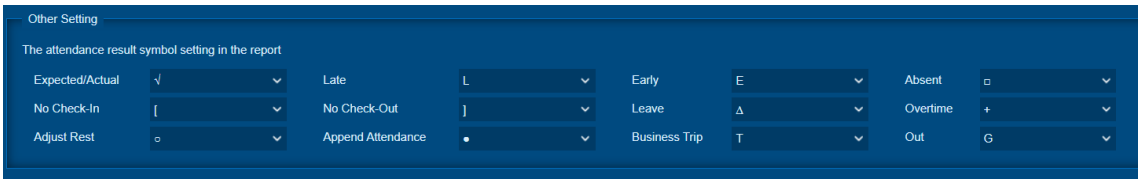


Hour Conversion Basis/Day Number Conversion Basis: the calculation result of the formula shall prevail (the calculation result shall prevail, and the precise digits of the decimal point shall be combined to retain the decimal place of the calculation result), the remainder range (the calculation result shall be processed according to the rules, and then combined the exact number of decimal places to keep the decimal places of the calculation result).

Conversion Basis for Absentee Days: conversion basis for days, recorded as working days shall prevail.

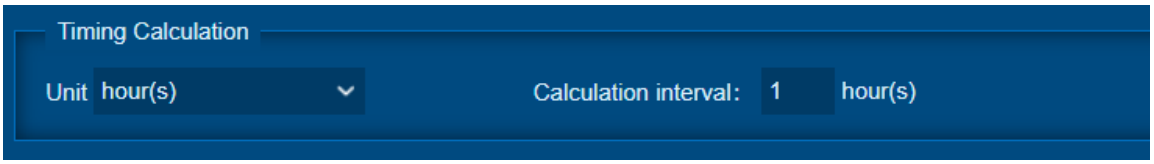
Exact Number of Decimal Places: 1(default), 2, 0.

Other Settings



The attendance result symbol setting in the report: should arrive/actually arrive, arrive late, leave early, absent from work, fail to sign in, fail to sign out, ask for leave, work overtime, transfer time off, make up shift, travel, and go out. Various types of display symbols allow repeated settings.

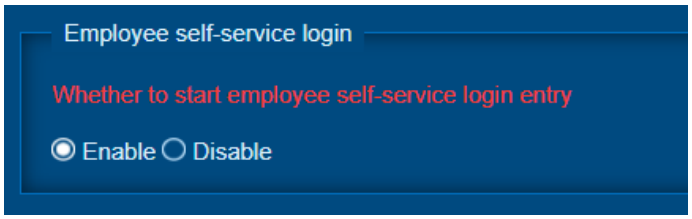
Timing Calculation



Unit: hour (default) and minute.

Calculation Frequency: time interval 5-59 minutes or 1-24 hours.

Employee Self-Login



Choose whether to enable the employee self-service login entrance, which is enabled by default.

7.2.7. Process Settings

Function Description

Setting process, applied to abnormal attendance management, you can set the process of re-signing, asking for leave, going on business, going out, working overtime, etc.

Add Process

Preconditions for Normal Use of Function

Existing job information.

Function Usage Scenarios

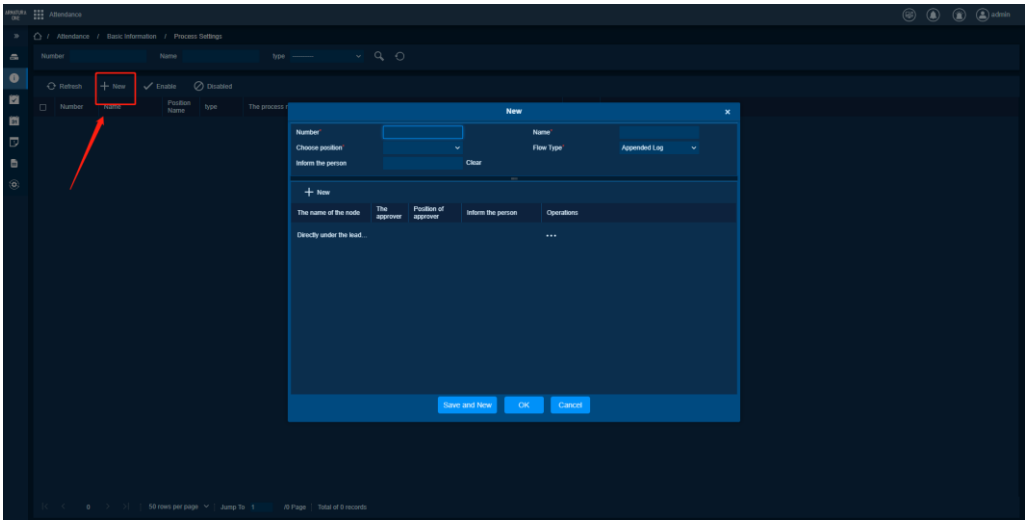
Set up a certain process and apply it to the management of abnormal attendance of personnel.

Feature Trigger Result

The process is added successfully.

Steps:-

1. Click **[Basic Information] > [Process Settings], click [Add]**, enter the number, process type, name, and select a certain position, and you can add an approval node.
2. Click **[Save and Continue]** to add a new process, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel adding.



Enable Process

Preconditions for Normal Use of Function

There is a new process.

Function Usage Scenarios

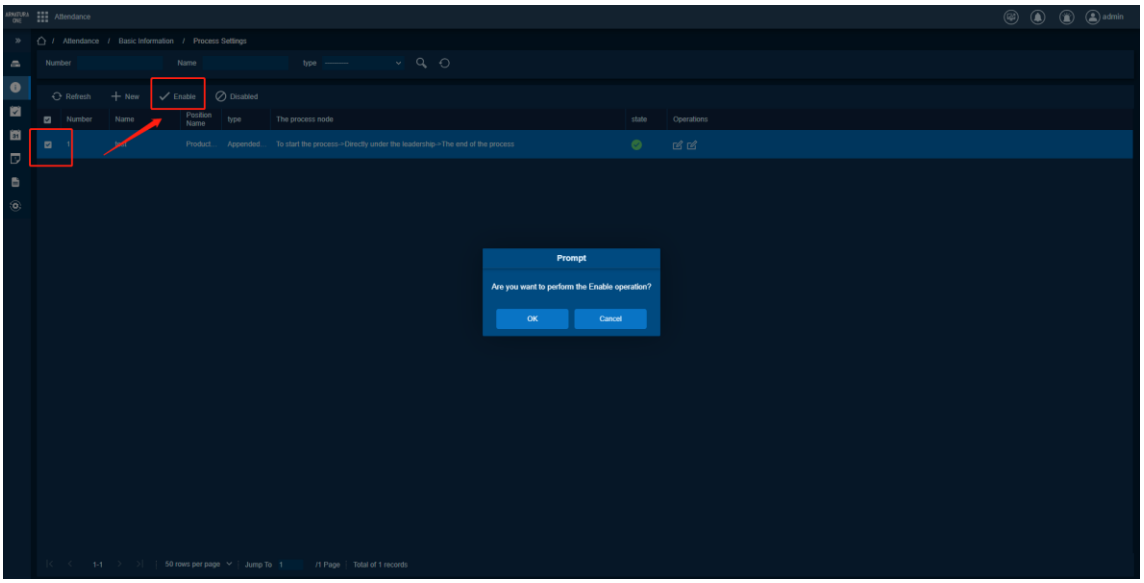
Need to use the set process.

Feature Trigger Result

The process is activated and applied to the management of abnormal staff attendance.

Steps:-

1. Click **[Basic Information]** > **[Process Settings]**, select the process, and click **[Enable]**.
2. In the pop-up window, click **[OK]** to confirm the activation, and click **[Cancel]** to cancel the activation.



Disable Process

Preconditions for Normal Use of Function

There is an activation process.

Function Usage Scenarios

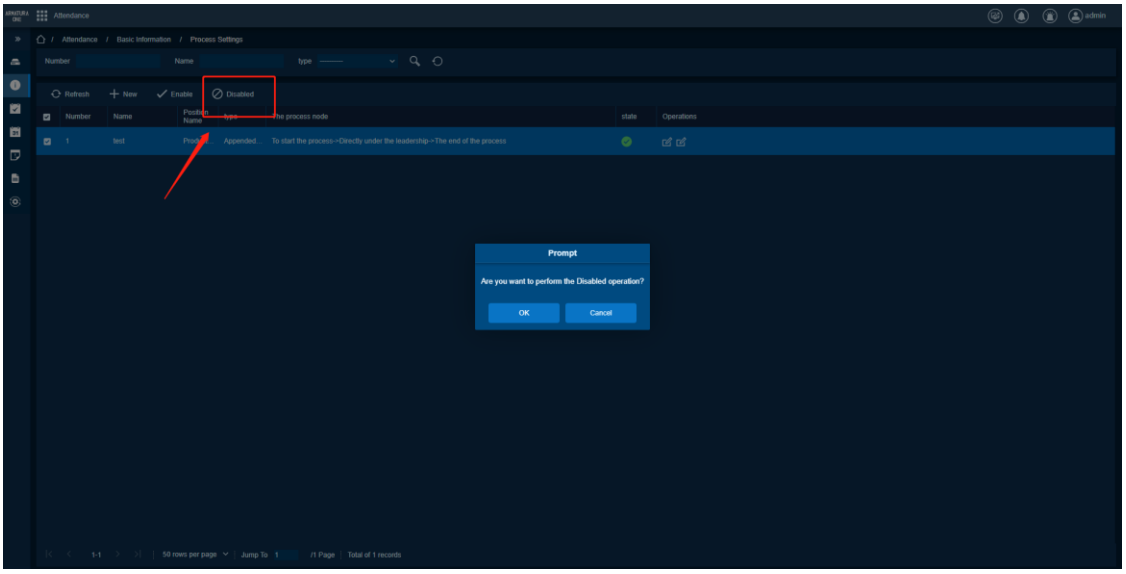
No need for this process.

Feature Trigger Result

The process is disabled and is no longer used in the management of personnel attendance exceptions.

Steps:-

1. Click **[Basic Information]** > **[Process Settings]**, select the process, and click **[Disable]**.
2. In the pop-up window, click **[OK]** to confirm the disabling, and click **[Cancel]** to cancel the disabling.



7.3. Shift

Function List

Functions	Description
Break Time	Add, edit, and delete Break Time.
Timetable	Add, edit, delete, and add Break Time and other operations of time.
Shift	Add, edit, and delete operations of shift.

7.3.1. Break Time

Function Description

Set the Break Time, you can add the Break Time in the time module to prepare for the application of time attendance.

Add Break Time

Preconditions for Normal Use of Function

Break Time name is not used.

Function Usage Scenarios

Need to add Break Time in the Time Period module to complete the time setting of attendance.

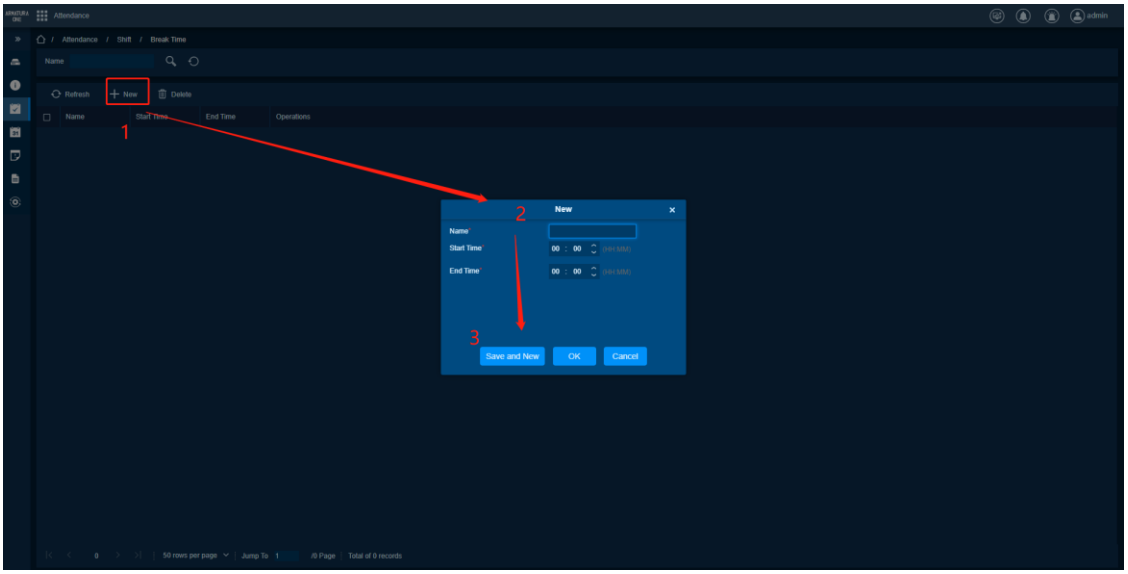
Feature Trigger Result

- Break Time can be added in the Time Period module.

- Displayed in the Break Time list.

Steps:-

- Click **[Shift]> [Break Time],** click **[Add],** enter the name, select the start time, and end time.
- Click **[Save and Continue]** to add a Break Time, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Edit Break Time

Preconditions for Normal Use of Function

Successfully added Break Time.

Function Usage Scenarios

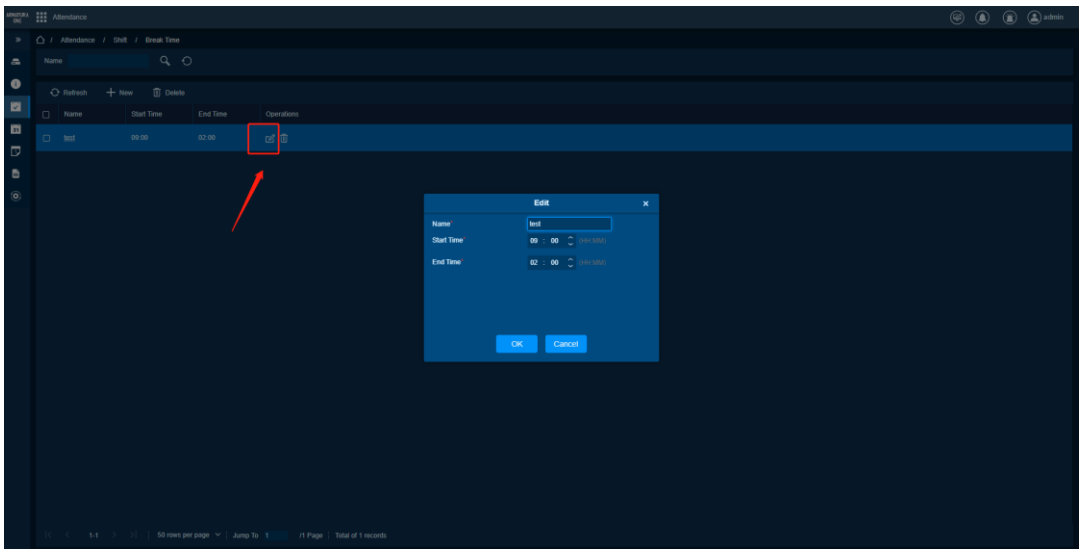
Need to modify the name of Break Time or Time Period.

Feature Trigger Result

- The Break Time in the Time Period module is also modified and continues to be applied.
- The Break Time list shows the modified content.

Steps:-

- Click **[Shift]> [Break Time],** select Break Time, click **[Edit]** to modify the information.
- Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Break Time

Preconditions for Normal Use of Function

Successfully added Break Time.

Function Usage Scenarios

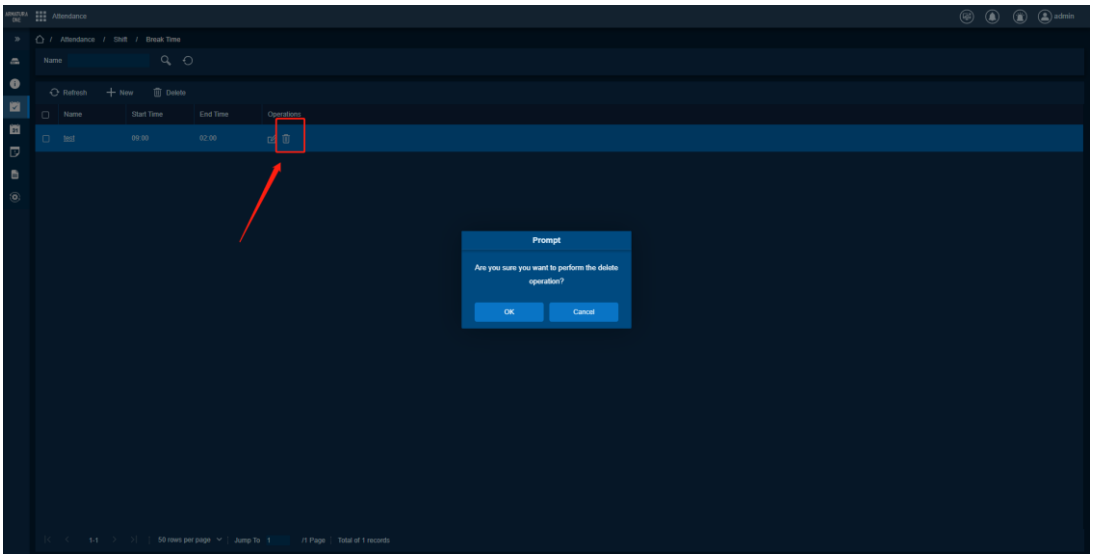
No need for a Break Time.

Feature Trigger Result

- The Break Time applied in the Time Period module is deleted and no longer takes effect.
- Not displayed in the Break Time list.

Steps:-

- Click **[Shift]> [Break Time]**, click **[Delete].**
- In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.3.2. Timetable

Function Description

Set the Timetable that may be used in the attendance process and configure various parameter information. Timetable is the smallest unit of personnel attendance time setting. Before setting Shift, you should set all the Timetable that may be used, that is, Timetable of Attendance. Shift can be set only after Timetable is set. Shift can be set only after Shift is set, and the various settings in the attendance rules Significant.

Add Timetable

Preconditions for Normal Use of Function

Timetable name is not used.

Function Usage Scenarios

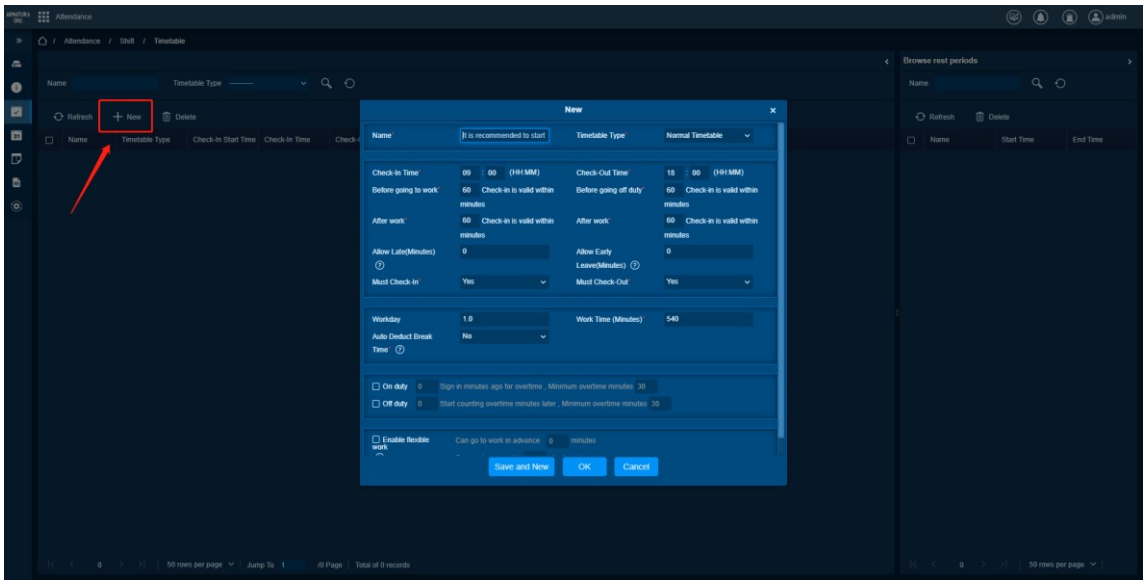
Applied in the attendance time setting, Shift and shift scheduling can be carried out in the follow-up

Feature Trigger Result

- Shift module can use Timetable to complete the settings.
- Displayed in the Timetable list.

Steps:-

- Click **[Shift]> [Timetable],** click **[Add],** enter information.
- Click **[Save and Continue]** to add a Timetable, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Edit Timetable

Preconditions for Normal Use of Function

Timetable has been successfully added.

Function Usage Scenarios

Modify Timetable settings.

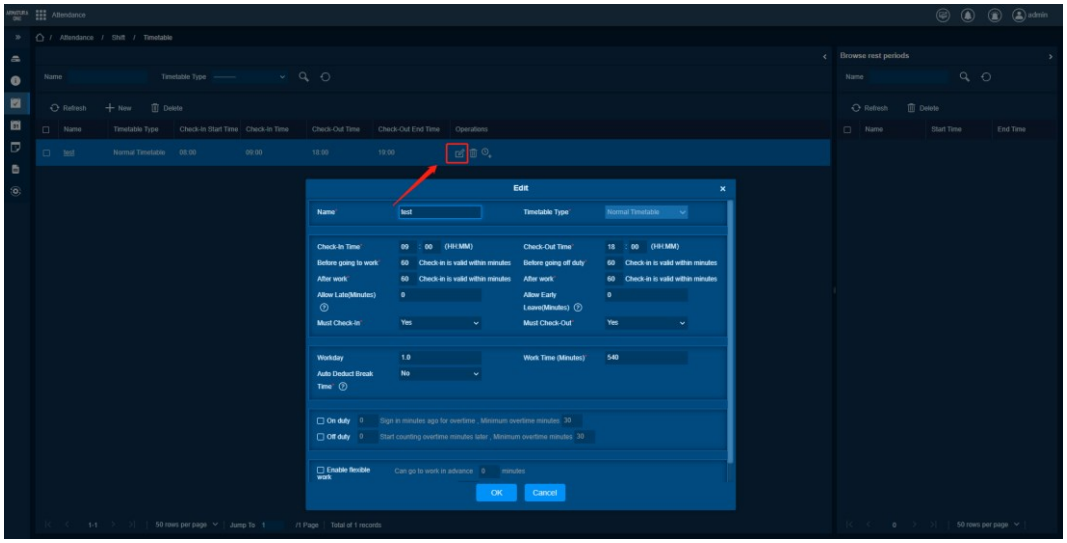
Feature Trigger Result

- The Timetable in the Shift module is also modified and continues to be applied.
- The Timetable list shows the modified content.

Steps:-

(1) Click **[Shift]> [Timetable]**, select Timetable, and click **[Edit]** to modify the information.

(2) Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Timetable

Preconditions for Normal Use of Function

Timetable has been successfully added.

Function Usage Scenarios

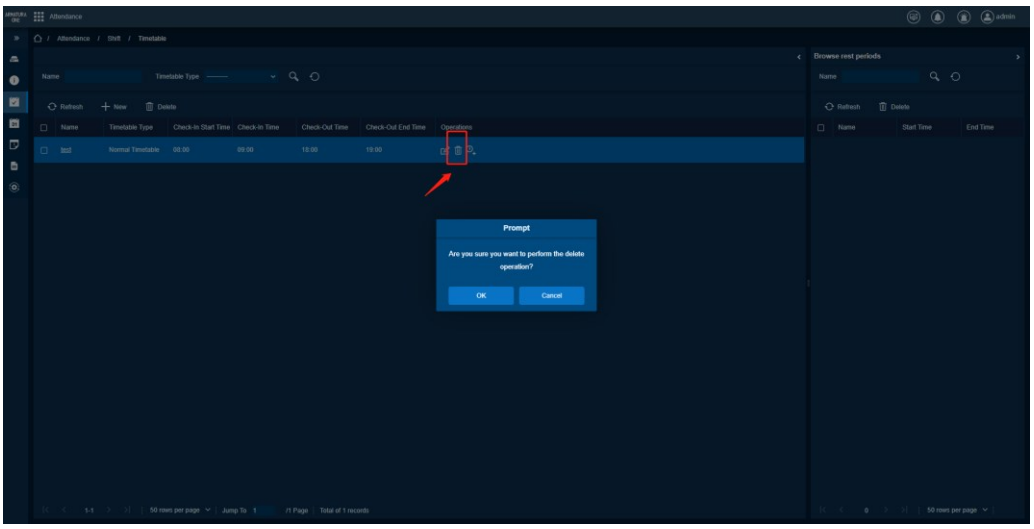
No need for a certain Timetable.

Feature Trigger Result

- The Timetable applied in the Shift module is deleted and no longer takes effect.
- Not displayed in the Timetable list.

Steps:-

- Click **[Shift]> [Timetable],** click **[Delete].**
- In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



Add Break Time for Timetable

Preconditions for Normal Use of Function

- Successfully added Break Time.
- Timetable has been successfully added.

Function Usage Scenarios

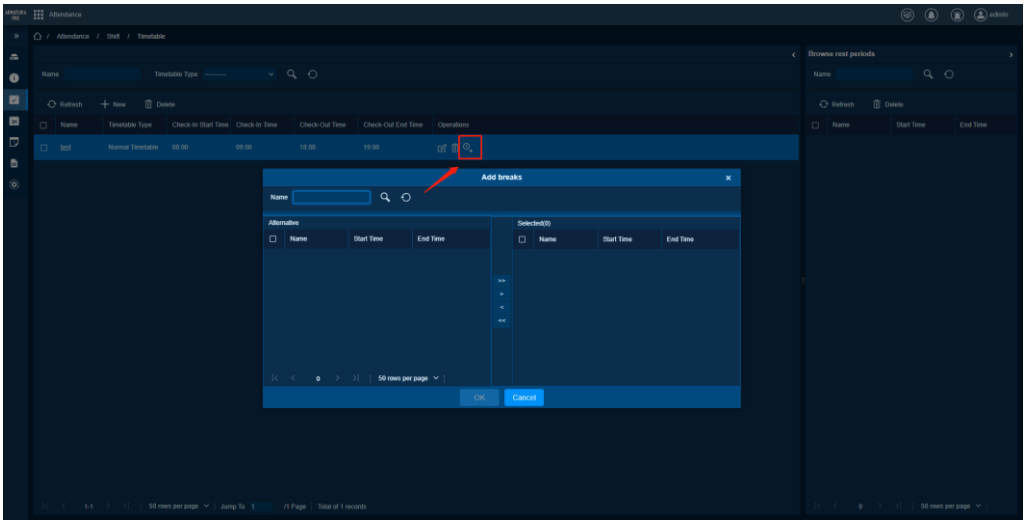
Need to add Break Time to Timetable to complete the time setting of attendance.

Feature Trigger Result

- Timetable includes Break Time; you can choose whether to deduct Break Time for attendance calculation.
- In the Timetable list, click Timetable, the module on the right side of the page can browse the added Break Time.

Steps:-

- Click **[Shift]> [Timetable],** select Timetable, and click **[Add Break Time].**
- Select Break Time, click **[OK]** to add successfully, click **[Cancel]** to cancel adding.



7.3.3. Shift

Function Description

Shift is composed of various pre-set one or more attendance periods according to a certain sequence and cycle period and is a preset staff commuting schedule. To check attendance on personnel, Shift must be set first.

Add Shift

Preconditions for Normal Use of Function

Shift name is not used.

Function Usage Scenarios

Create Shift, which can be used to schedule personnel later.

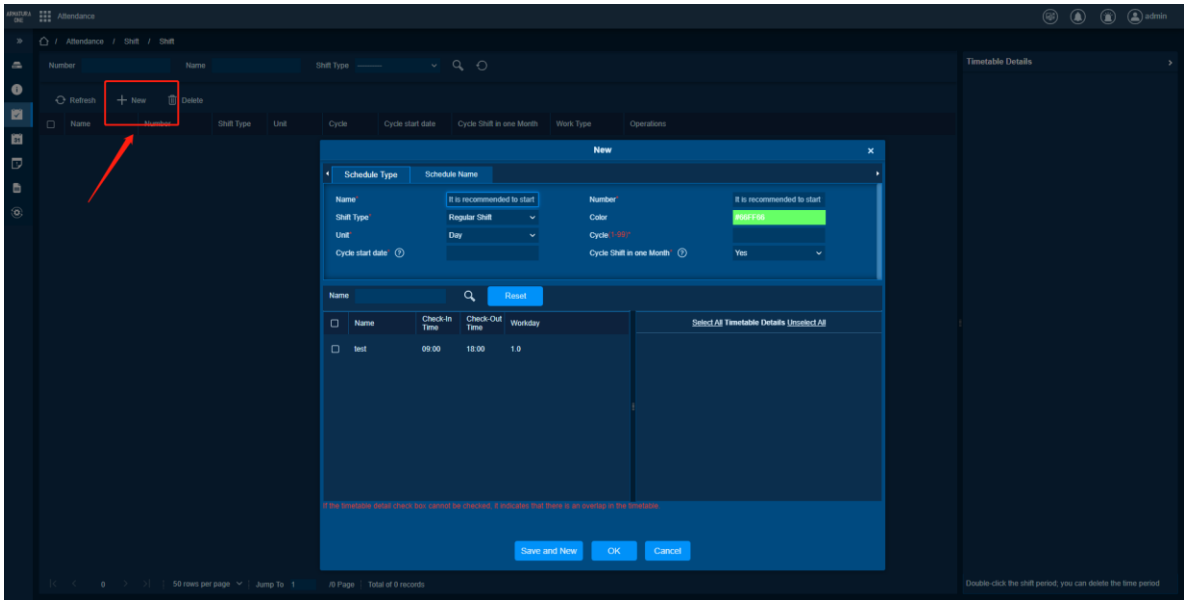
Feature Trigger Result

- Shift can be used in the scheduling module.
- Display in the Shift list.

Steps:-

(1) Click **[Shift]> [Shift],** click **[Add],** and enter information.

(2) Click **[Save and Continue]** to add Shift, the page will not close, you can continue to add, click **[**OK**]** to add successfully, click **[Cancel]** to cancel the addition.



Edit Shift

Preconditions for Normal Use of Function

Shift has been successfully added.

Function Usage Scenarios

Modify Shift settings

Feature Trigger Result

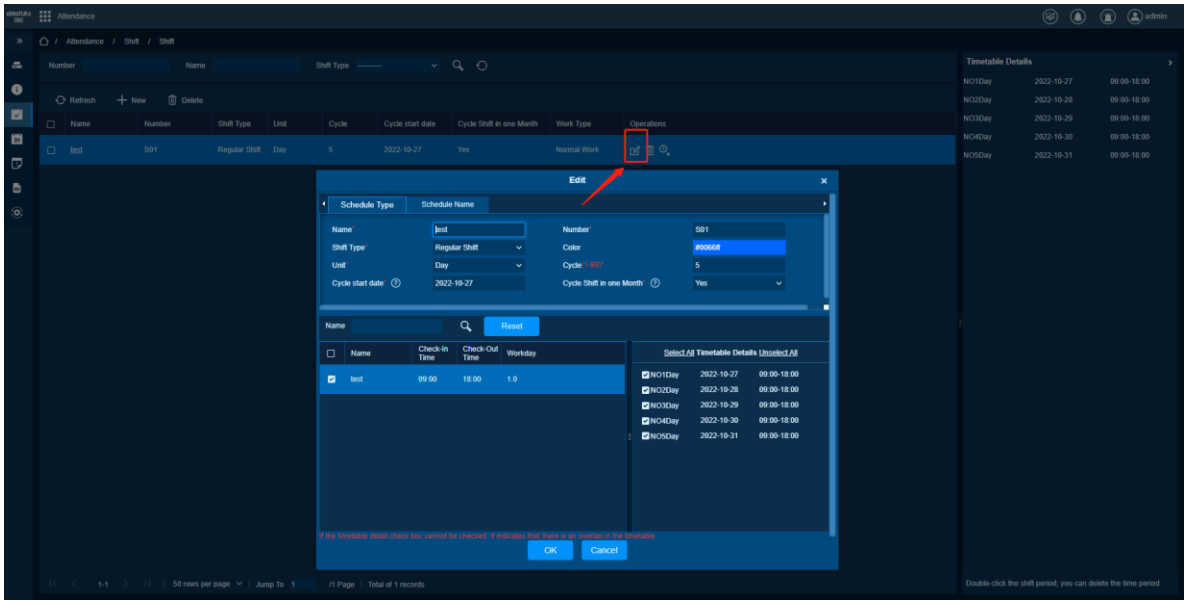
1. The Shift setting is modified and displayed correctly in the list.

2. The Timetable in the scheduling management module is also modified and continues to be applied.

Steps:-

1. Click **[Shift]**> **[Shift]**, click **[Edit]** to modify the information.

2.Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Shift

Preconditions for Normal Use of Function

1. Shift has been successfully added.
2. This Shift is not currently used in any shifts.

Function Usage Scenarios

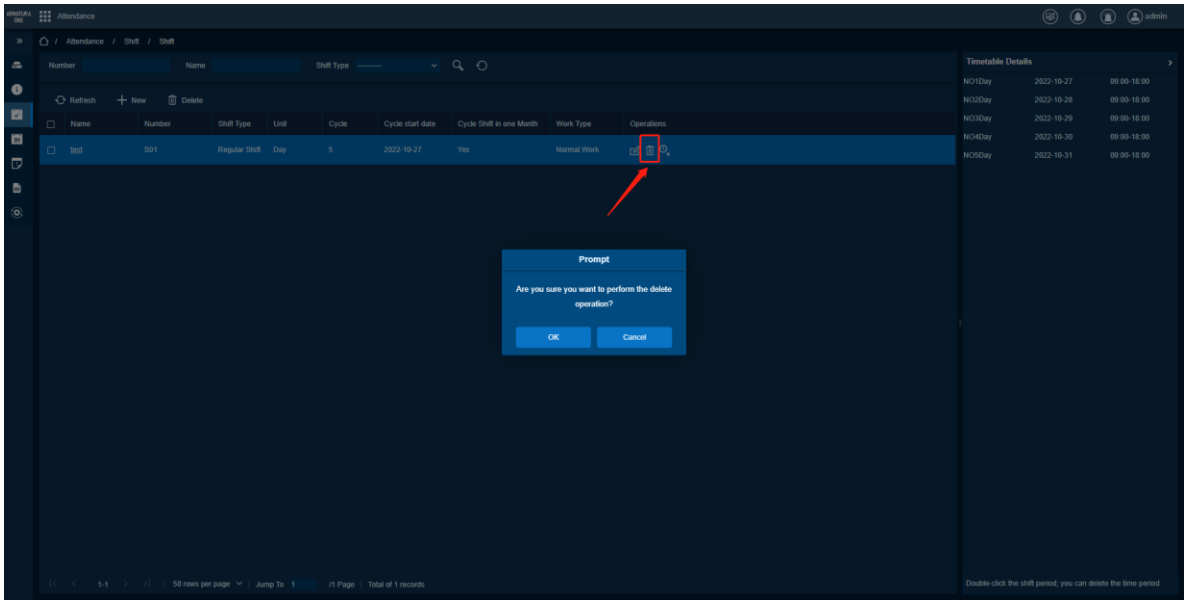
No need for this Shift.

Feature Trigger Result

1. Cannot select the deleted Shift when scheduling.
2. Shift is not displayed in the Shift list.

Steps:-

1. Click **[Shift]**> **[Shift]**, select Shift, and click **[Delete].**
2. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



Clear Timetable

Preconditions for Normal Use of Function

1. The Timetable has been successfully created.
2. New Shift has been successfully created.

Function Usage Scenarios

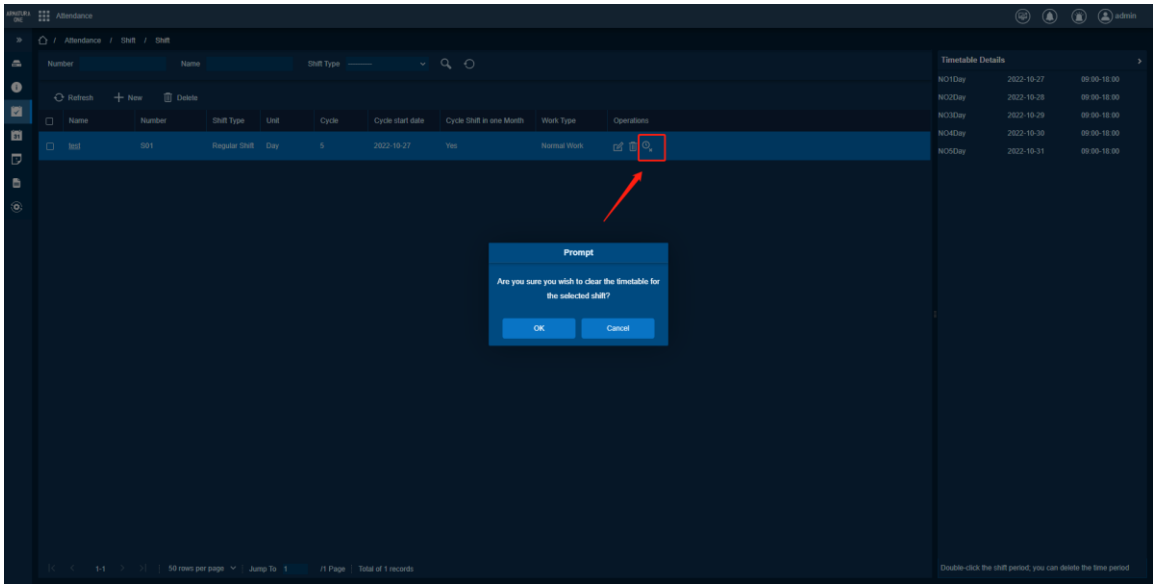
Reset or Modify the Timetable of Shift

Feature Trigger Result

1. Shift's Timetable is cleared.
2. Click **Shift**, it is empty when browsing Timetable in the right module.
3. The Timetable in the scheduling management module is also modified and continues to be applied.

Steps:-

1. Click **[Shift]**> **[Shift]**, select Shift, and click **[Clear Timetable].**
2. Click **[OK]** in the pop-up window to empty successfully, click **[Cancel]** to cancel the emptying.



Delete Shift Timetable

Preconditions for Normal Use of Function

1. The Timetable has been successfully created.
2. New Shift has been successfully created.

Function Usage Scenarios

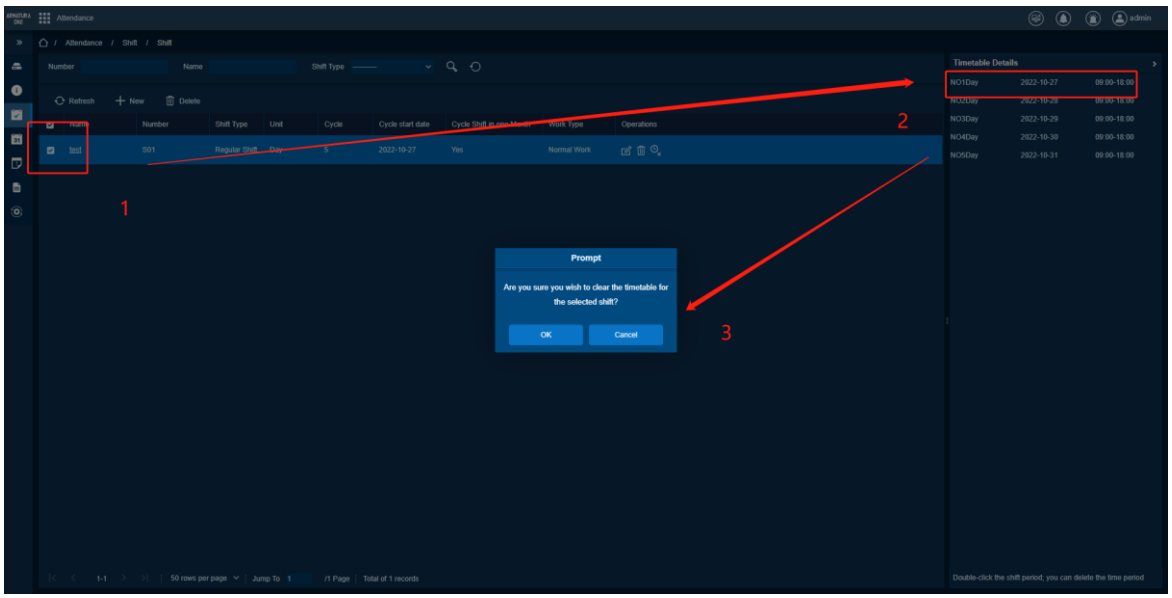
1. Do not clear the Timetable, delete a single Timetable.
2. Flexible choice to delete part of Timetable.

Feature Trigger Result

1. Delete the Shift part of Timetable.
2. Click **Shift**, the deleted part of Timetable is not displayed when browsing Timetable in the right module.
3. The Timetable in the scheduling management module is also modified and continues to be applied.

Steps:-

1. Click **[Shift]**>**[Shift]**, select Shift, and double-click the Timetable you want to delete in the module on the right.
2. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.4. Schedule

Function List

Functions	Description
Grouping	Add, edit, and delete groups, and can add grouping rules and personnel to group settings.
Group Scheduling	Add, delete, or add temporary schedules for grouped personnel and browse the schedule calendar.
Department Scheduling	Add or delete shifts or add temporary shifts for department personnel and browse the shift calendar.
Staff Scheduling	Add temporary schedules for personnel.
Temporary Schedule	Display and query temporary schedule.
Unscheduled Personnel	View unscheduled personnel and schedule unscheduled personnel.

7.4.1. Group

Function Description

Group people with the same attendance rules to prepare for subsequent grouping and scheduling. Enter the main interface of the group, display the query column and group list information, the query function can

facilitate group query; the list shows all groups of the current system, click the row where the group is located, and the list of people who browse the group on the right will list all the groups in detail Personnel information.

New Group

Preconditions for Normal Use of Function

Group name is not used.

Function Usage Scenarios

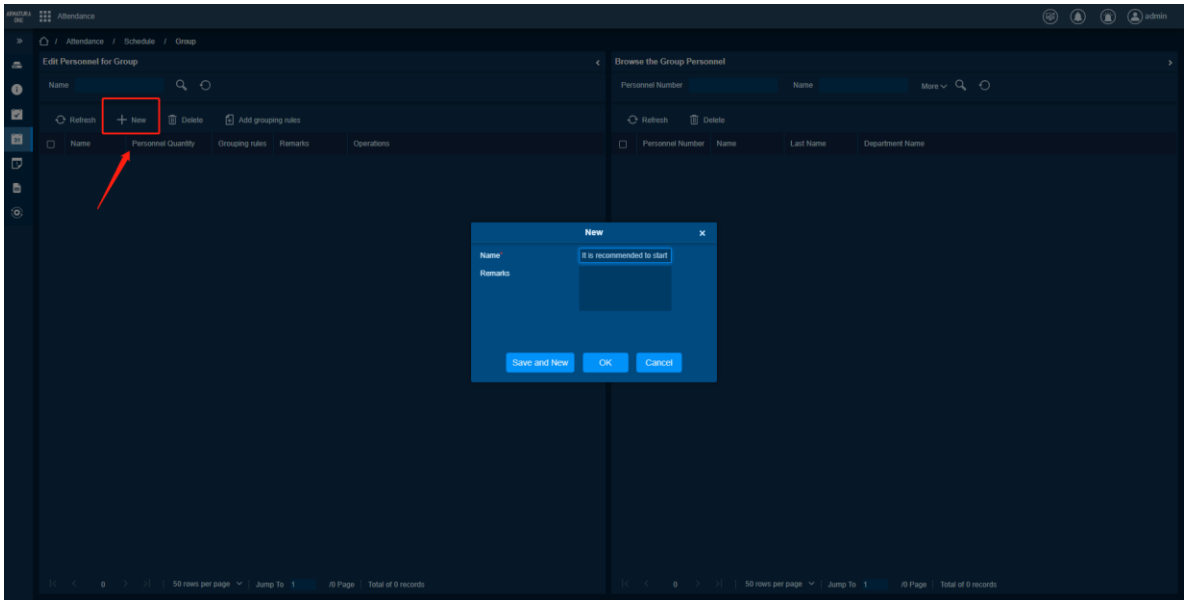
Need to group personnel to facilitate subsequent grouping and scheduling.

Feature Trigger Result

1. The group is successfully added and displayed in the group list.
2. This group of personnel can be set up in subsequent shifts and use the same attendance rule.

Steps:-

1. Click **[Schedule]**> **[Group]**, click **[Add]**, and enter a name.
2. Click **[Save and Continue]** to add Shift, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete Group

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. The group is not used in any group scheduling.

Function Usage Scenarios

When you don't need to use the group, you can delete it.

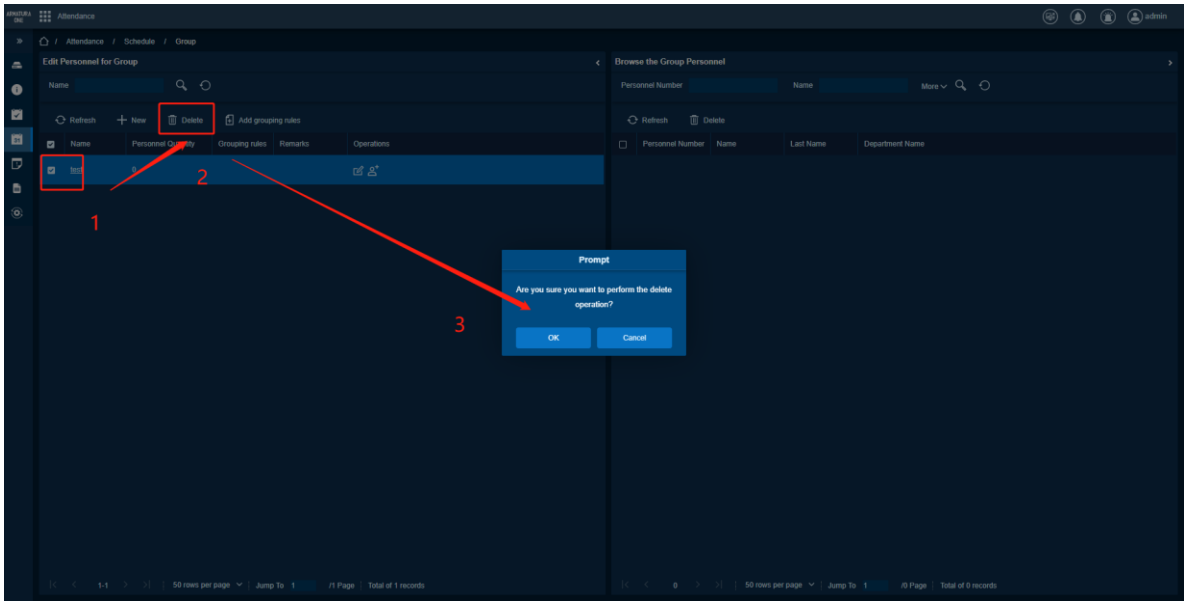
Feature Trigger Result

1. The group is successfully deleted, and it is not displayed in the group list.

2. This group of personnel cannot be selected and set in the subsequent grouping schedule.

Steps:-

1. Click **[Schedule]**> **[Group]**, select a group, and click **[Delete].**
2. Click **[OK]** to confirm the deletion, click **[Cancel]** to cancel the deletion.



Add Grouping Rules

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. In **[Basic Information]** > **[Custom Rule]**, a grouping rule has been successfully added.

Function Usage Scenarios

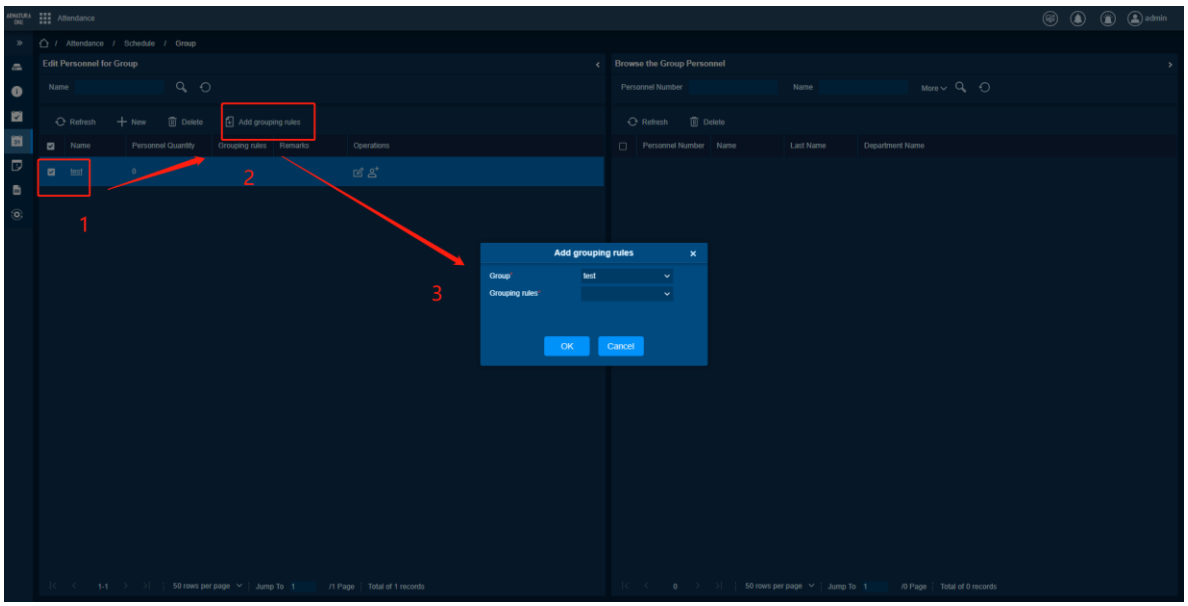
Set custom attendance rules for groups.

Feature Trigger Result

The group has a Custom Rule, which can be applied to the attendance system.

Steps:-

1. Click **[Schedule]**> **[Group]**, click **[Add Group Rule]**, select grouping and grouping rules.
2. Click **[OK]** to add successfully, click **[Cancel]** to cancel adding.



Add Personnel

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. Personnel Module has personnel information.

Function Usage Scenarios

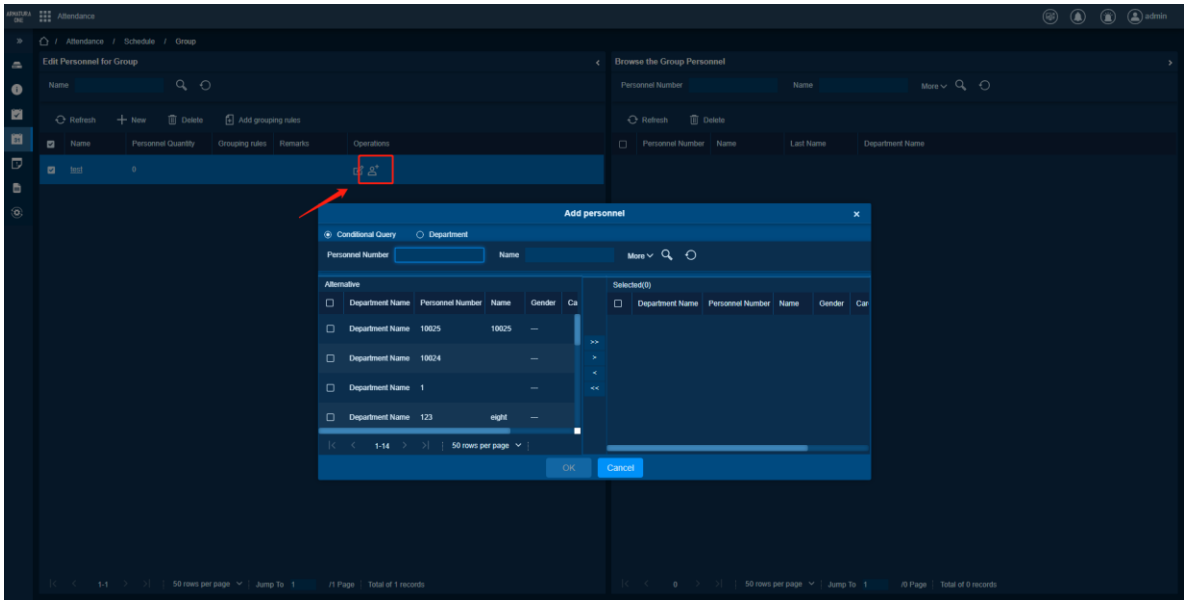
Add personnel to group, and then you can schedule the group of personnel.

Feature Trigger Result

1. Successfully add personnel to this group, and then you can set attendance for this group of personnel.
2. Group people are displayed on the right side of the page.
3. The personnel who have been assigned to this group will be filtered out in the waiting area of the personnel list in the add personnel interface.
4. People who have been added to other groups will be deleted from the original group after being added to this group.

Steps:-

1. Click **[Schedule]**> **[Group]**, select a group, and click **[Add Person]** to select a person.
2. Click **[OK]** to add successfully, click **[Cancel]** to cancel adding.



Delete Personnel

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. Successfully added people to the group.

Function Usage Scenarios

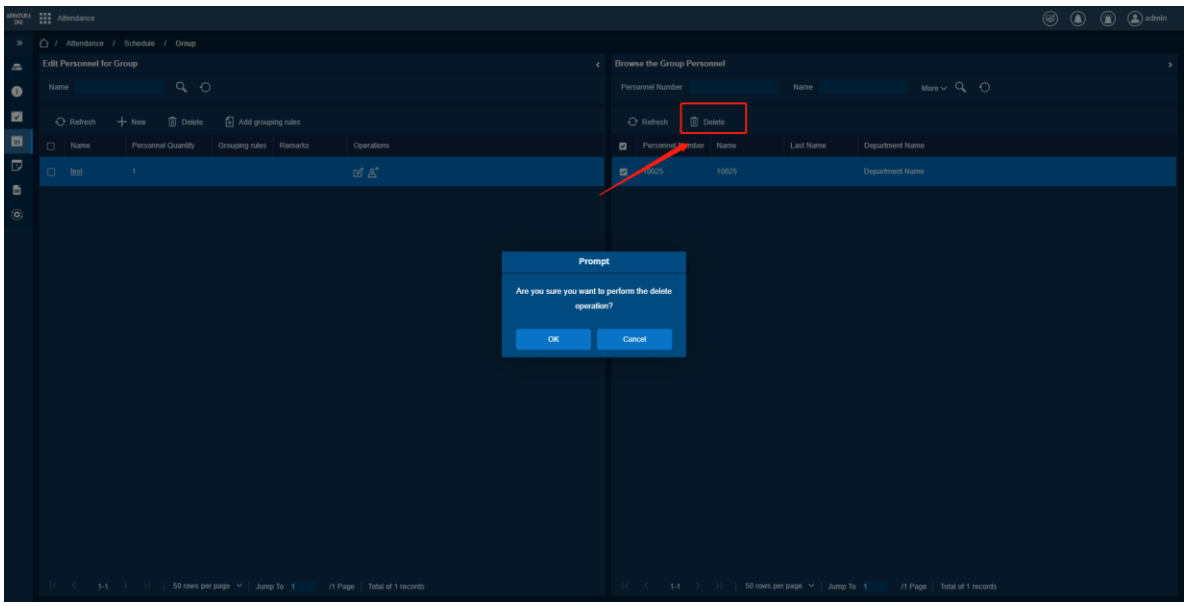
When the personnel are deleted from the group and the personnel no longer need to use the group for scheduling.

Feature Trigger Result

1. Successfully delete the personnel for the group, and the personnel will no longer implement the attendance system of the group.
2. People are no longer displayed on the right side of the page.

Steps:-

1. Click **[Schedule]> [Group]**, select a group, and browse the right side of the page.
2. Select personnel, click **[Delete].**
3. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.4.2. Group Schedule

Function Description

Group shift scheduling is to perform shift operations for grouped personnel. This interface can view the shift scheduling information of each group and display it in the form of a monthly calendar.

Add Group Scheduling

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. Shift has been successfully added.

Function Usage Scenarios

Arranging shifts for group personnel.

Feature Trigger Result

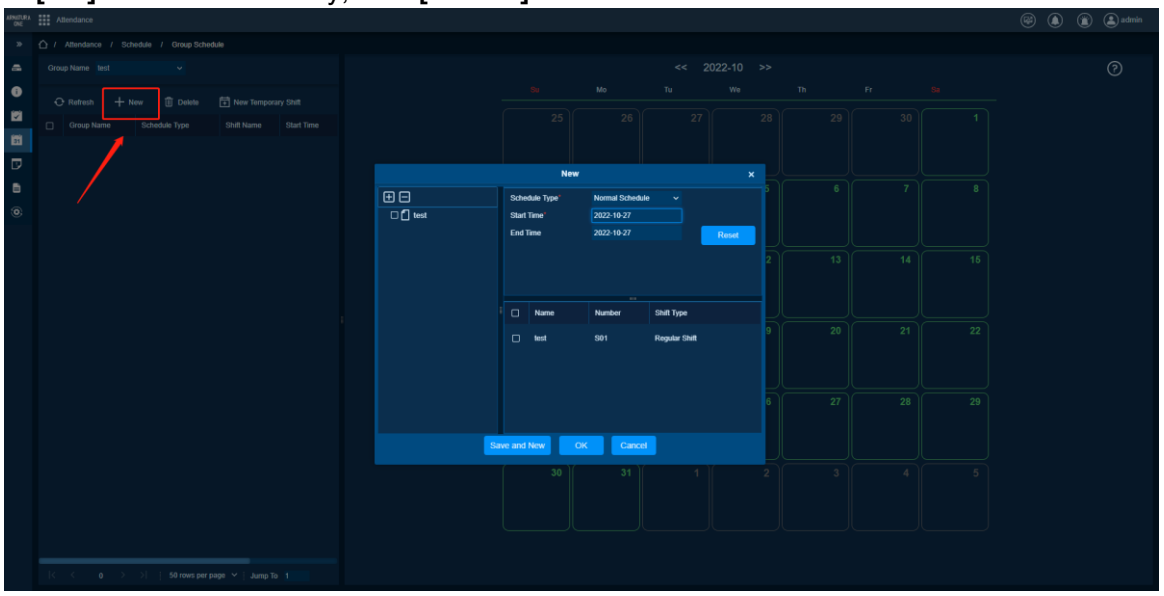
1. The group shift list shows the newly added group.
2. Personnel will check attendance according to the schedule.
3. Group shifts are displayed on the calendar.

Steps:-

- Select a group: select a group on the left side of the grouping interface and click Add.
- Shift type: drop-down menu, there are two ways of normal shift and smart shift. Normal shift can only choose one Shift, and smart shift can select multiple shifts. Choose Smart Shift, and the software will automatically determine the most suitable Shift based on the punch-in record for attendance calculation.
- Start date, end date: On the upper right side of the interface, define which date period the grouping is applied to.

Select Shift: Select the shift that needs to be scheduled for this grouping:-

1. Click **[Schedule]** > **[Group Schedule]**, select group, Shift, shift type, start date and end date.
2. Click **[Save and Continue]** to add a new group schedule, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete Group Scheduling

Preconditions for Normal Use of Function

Group scheduling has been successfully added.

Function Usage Scenarios

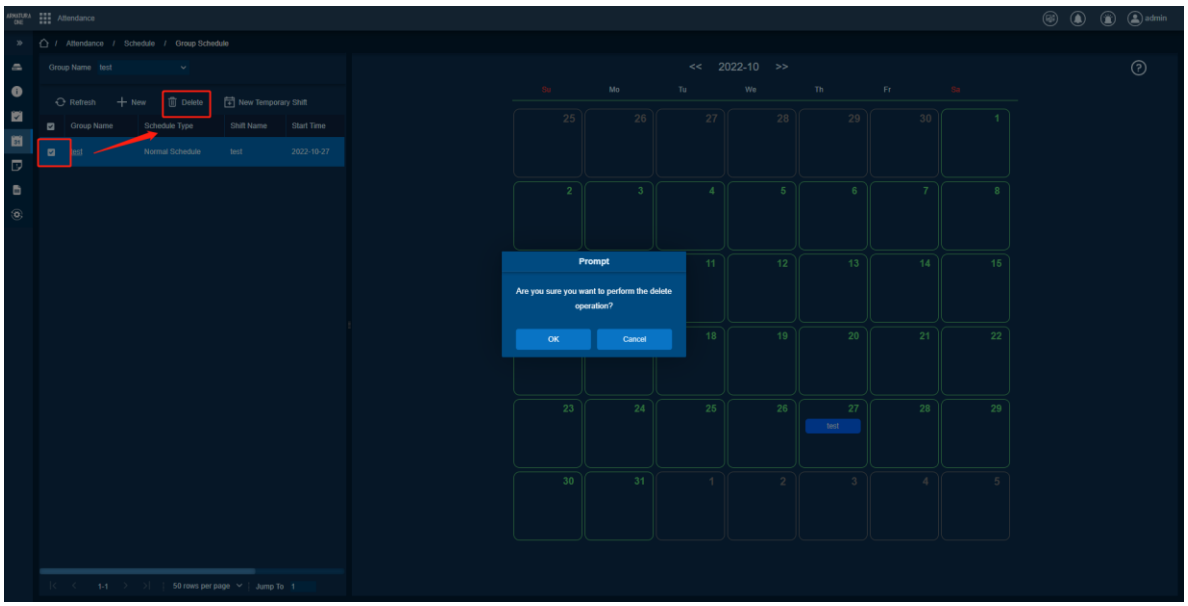
No need to use this group to schedule.

Feature Trigger Result

1. The group schedule is no longer displayed in the group schedule list.
2. The personnel in this group will no longer follow this schedule to check attendance.
3. The group schedule is not displayed on the calendar.

Steps:-

1. Click **[Schedule]** > **[Group Schedule]**, select the set schedule, and click **[Delete].**
2. Click **[OK]** in the pop-up window to delete successfully, click **[Cancel]** to cancel the deletion.



Add Temporary Schedule

Preconditions for Normal Use of Function

1. The group has been successfully added.
2. Shift has been successfully added.

Function Usage Scenarios

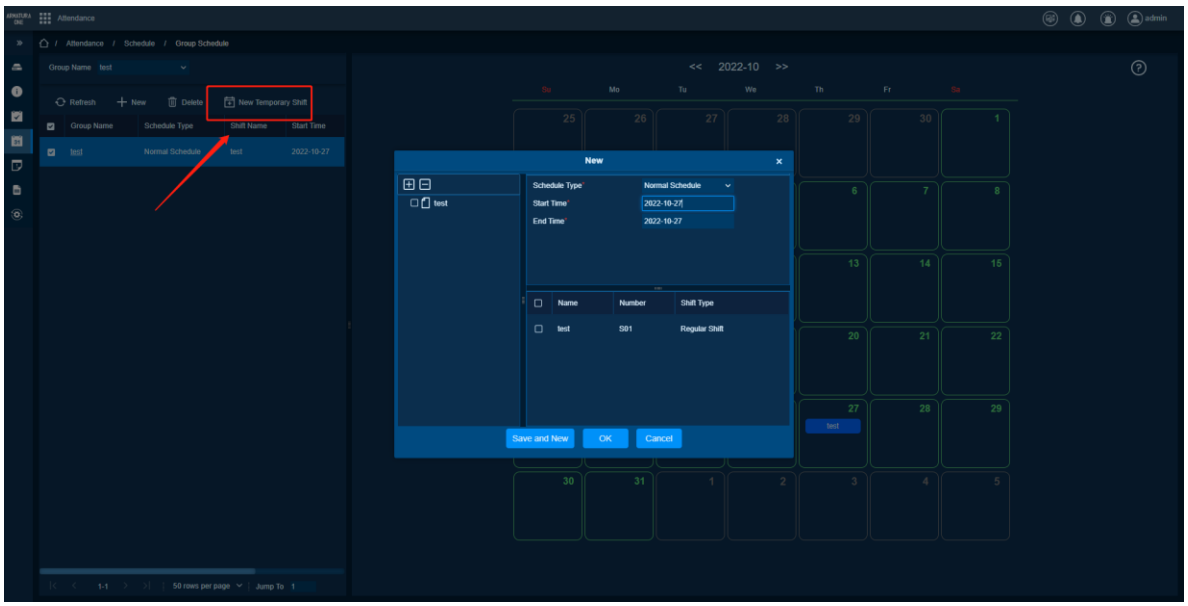
Need to temporarily schedule a group.

Feature Trigger Result

1. Temporary schedule is displayed on the calendar.
2. Temporary scheduling has a higher priority than normal scheduling.

Steps:-

1. Click **[Schedule]** > **[Group Schedule]**, click **[Add Temporary Shift]**, select group, shift, shift type, start date and end date.
2. Click **[Save and Continue]** to add a temporary schedule, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



7.4.3. Department Scheduling

Function Description

The operating functions are basically the same as group scheduling, except that when the department is scheduled, the selected object is the department, which is the entire department.

Add Department Scheduling

Preconditions for Normal Use of Function

1. Existing department information.
2. Shift has been successfully added.

Function Usage Scenarios

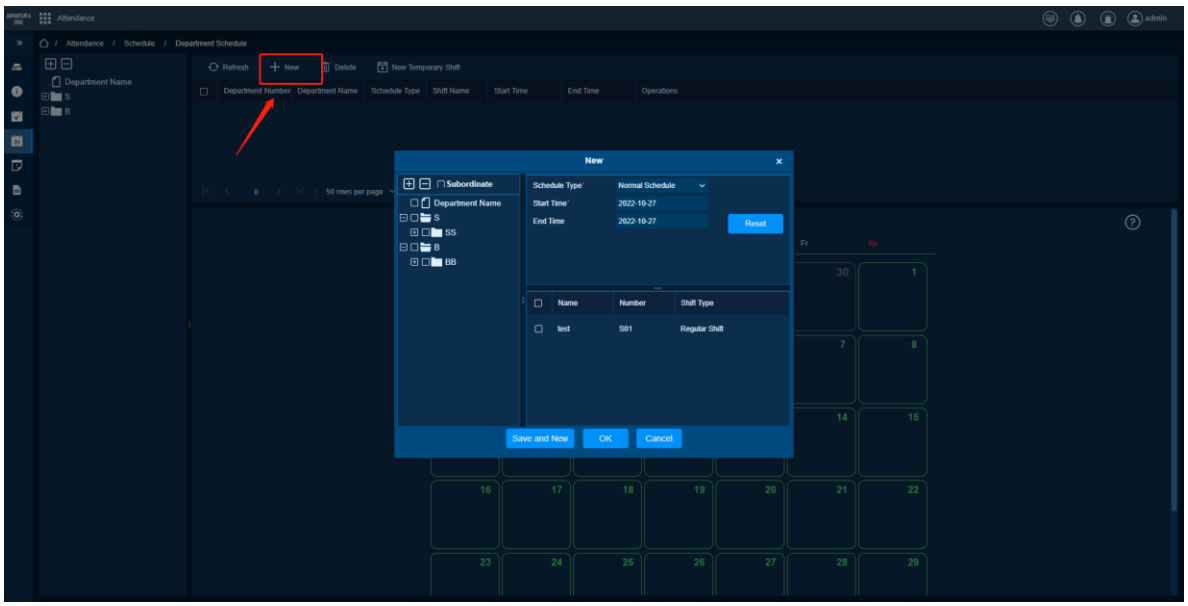
Set up shifts for the entire department.

Feature Trigger Result

1. The department schedule list shows the schedule.
2. Personnel will check attendance according to the schedule.
3. The department schedule is displayed on the calendar.

Steps:-

1. Click **[Schedule]** > **[Department Scheduling]**, select department, shift, scheduling type, start date and end date.
2. Click **[Save and Continue]** to add a new department schedule, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete Department Scheduling

Preconditions for Normal Use of Function

The department schedule has been successfully added.

Function Usage Scenarios

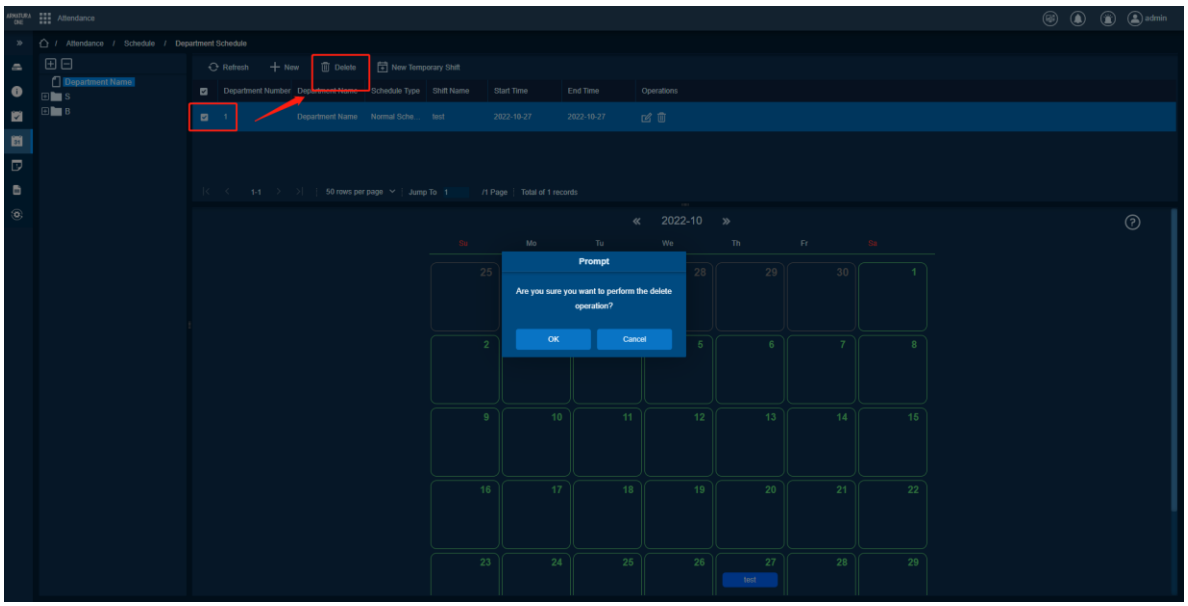
Department does not need this schedule.

Feature Trigger Result

1. The department schedule is no longer displayed in the group schedule list
2. The staff of this department will no longer follow this schedule to check attendance.

Steps:-

1. Click **[Schedule]** > **[Departmental Scheduling]**, select the schedule that has been set, and click **[Delete].**
2. Click **[OK]** in the pop-up window to delete successfully, click **[Cancel]** to cancel the deletion.



Add Temporary Schedule

Preconditions for Normal Use of Function

1. Existing department information.
2. Shift has been successfully added.

Function Usage Scenarios

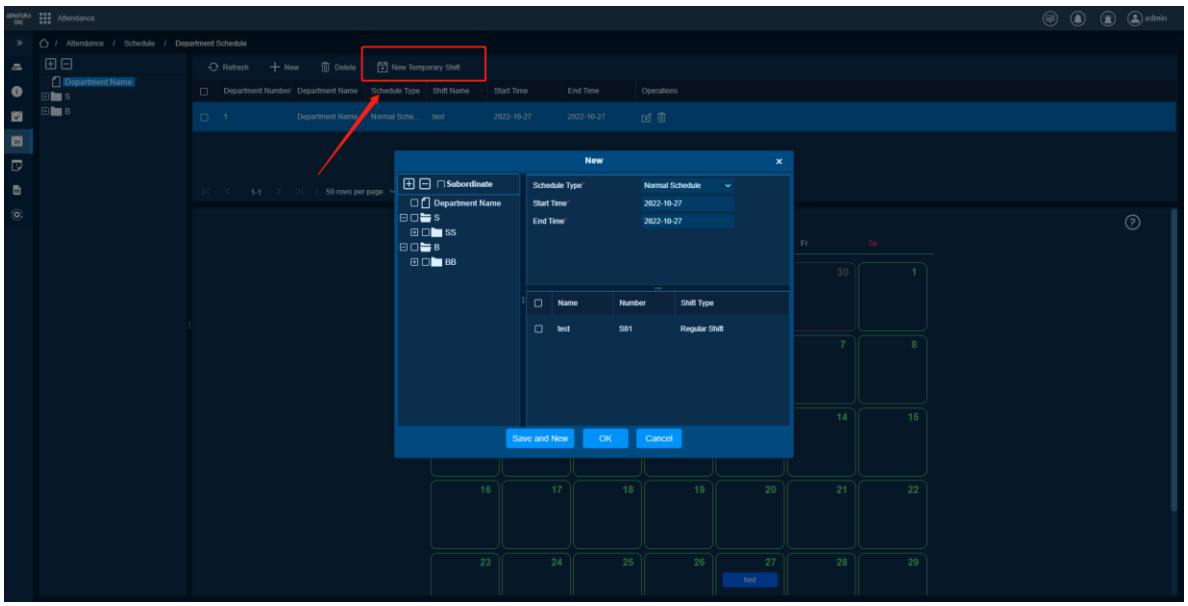
Need to schedule a department temporarily.

Feature Trigger Result

1. Temporary schedule is displayed on the calendar.
2. Temporary scheduling has a higher priority than normal scheduling.

Steps:-

1. Click **[Schedule]** > **[Department Scheduling]**, click **[New Temporary Shift]**, select department, shift, shift type, start date and end date.
2. Click **[Save and Continue]** to add a temporary schedule, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



7.4.4. Personnel Schedule

Function Description

The operation of personnel scheduling is the same as group scheduling, but when personnel scheduling, the selected object is personnel, and personnel scheduling only supports temporary scheduling.

Add Temporary Schedule

Preconditions for Normal Use of Function

1. The personnel module has personnel information.
2. Shift has been successfully added.

Function Usage Scenarios

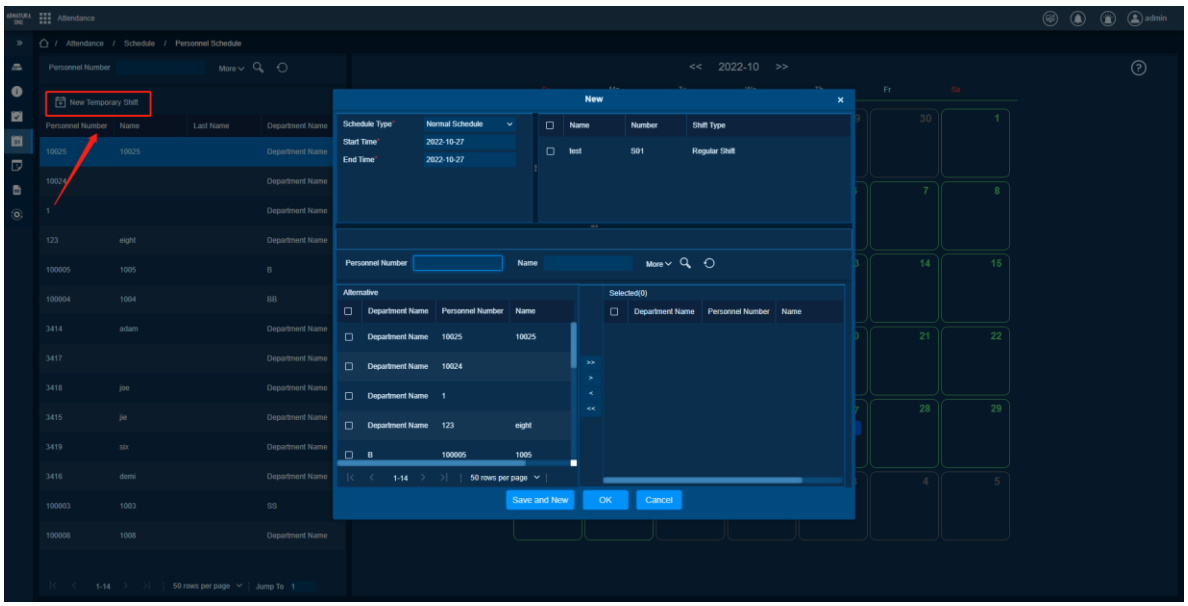
Add temporary schedules for specific personnel and adjust attendance arrangements.

Feature Trigger Result

1. Click on a single person, and its shift status is displayed on the right calendar.
2. Personnel are given priority for attendance according to this temporary schedule.

Steps:-

1. Click **[Schedule]** > **[Personnel Schedule]**, click **[New Temporary Shift]**, select personnel, shift, shift type, start time and end time.
2. Click **[Save and Continue]** to add a temporary schedule, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



7.4.5. Temporary Schedule

Function Description

Temporary schedule is the result display of all temporary schedules (groups, departments, personnel). You can view the Timetable details and support deletion.

Edit Temporary Scheduling

Preconditions for Normal Use of Function

Schedules have been successfully added in group scheduling, department scheduling and personnel scheduling.

Function Usage Scenarios

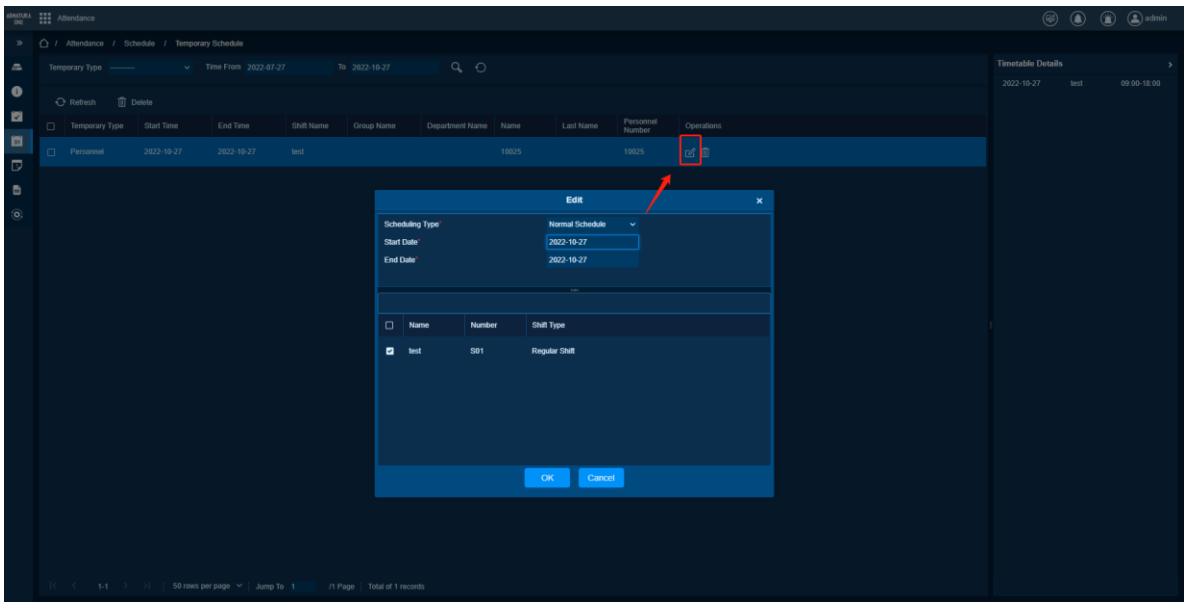
Need to modify the shift type, start date, end date and Shift of the temporary shift.

Feature Trigger Result

Temporary schedule is successfully modified and applied to personnel attendance.

Steps:-

1. Click **[Schedule]** > **[Temporary Schedule]**, select temporary shift, click **[Edit]** to modify the information.
2. Click **[OK]** to edit successfully, click **[Cancel]** to cancel editing.



Delete Temporary Scheduling

Preconditions for Normal Use of Function

The temporary schedule has been successfully added.

Function Usage Scenarios

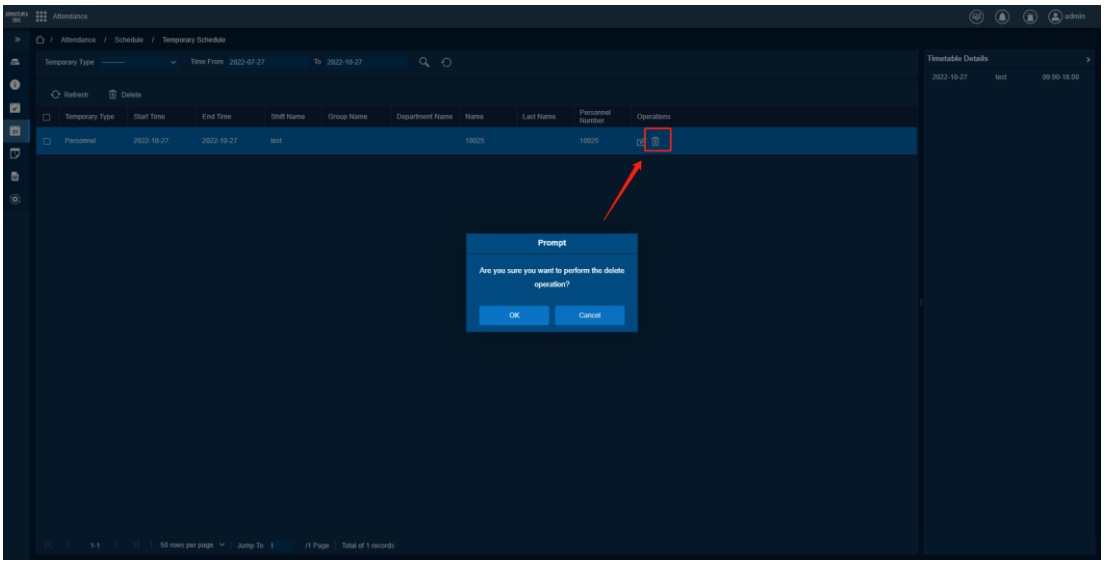
No need for this temporary schedule.

Feature Trigger Result

The temporary schedule is successfully deleted. The temporary schedule that does not appear in the list and is deleted will no longer be used in the attendance.

Steps:-

1. Click **[Schedule]** > **[Temporary Schedule]**, select the temporary shift, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



7.4.6. Unscheduled Personnel

Function Description

View and add temporary schedules to unscheduled personnel.

Add Temporary Schedule

Preconditions for Normal Use of Function

There are unscheduled personnel: -

Function Usage Scenarios

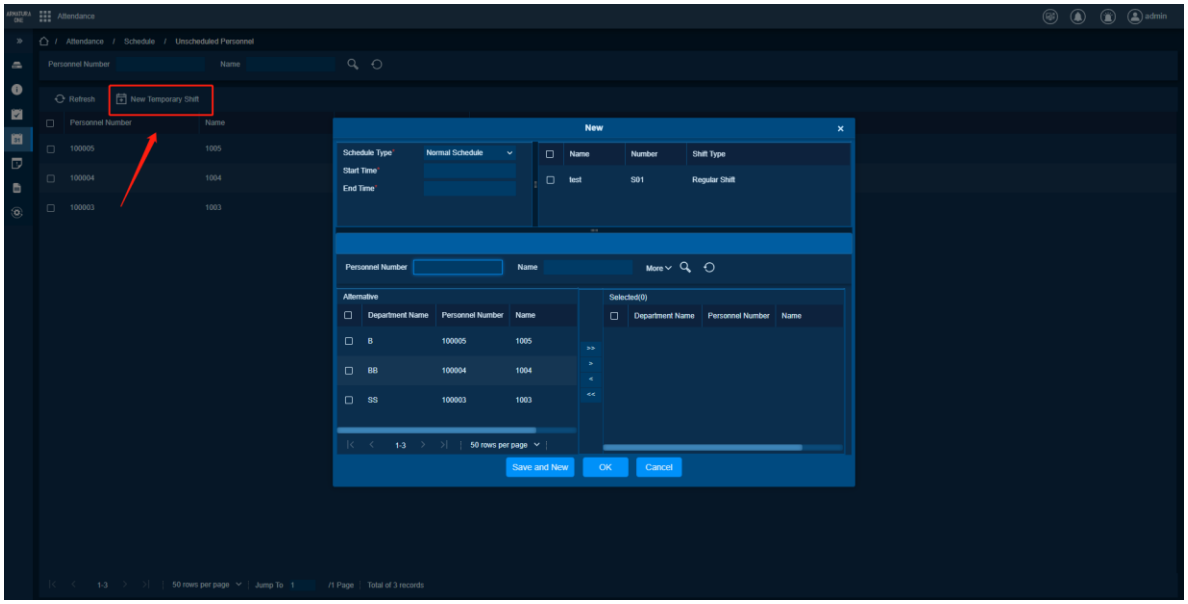
1. View unscheduled personnel.
2. Add temporary schedules to unscheduled personnel.

Feature Trigger Result

1. After adding a temporary shift, the personnel will not appear in the unscheduled personnel information list.
2. Personnel check attendance according to temporary schedule.

Steps:-

1. Click **[Schedule]** > **[Unscheduled Personnel]**, click **[New Temporary Shift]**, select personnel, shift, schedule type, start time and end time.
2. Click **[Save and Continue]** to add a temporary schedule, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



7.5. Exception

Function List

Function	Description
Supplementary Form	Add or delete the supplementary sign list and export supplementary sign list and other operations.
Ask for Leave	Add or delete the supplementary sign and export leave list and other operations.
Business Trip	Add or delete supplementary sign and export business trip list and other operations.
Go Out	Add or delete the supplementary sign list and export supplementary sign list and other operations.
Overtime	Add or delete the supplementary sign and export overtime list and other operations.
Shift	Add or delete the supplementary sign and export shift list and other operations.

7.5.1. Appended Log

Function Description

In the case of personnel going out on business or forgetting to check in, the manual re-enrollment of attendance records in the attendance report is called re-sign card. Generally, after the end of the attendance period, the management personnel will summarize and enter the attendance records according to the attendance results and the company's attendance system. This version supports the approval flow processing of abnormal situations, which can be manually entered into the system, or employees can log in to apply for approval. The data whose overall approval status is passed will have an impact on the attendance calculation results.

Add

Preconditions for Normal Use of Function

Existing Personnel Information

Function Usage Scenarios

When personnel go out on business or forget to check in, etc., they can perform re-signing operations.

Feature Trigger Result

The resignation is successful, and the staff attendance will not be affected.

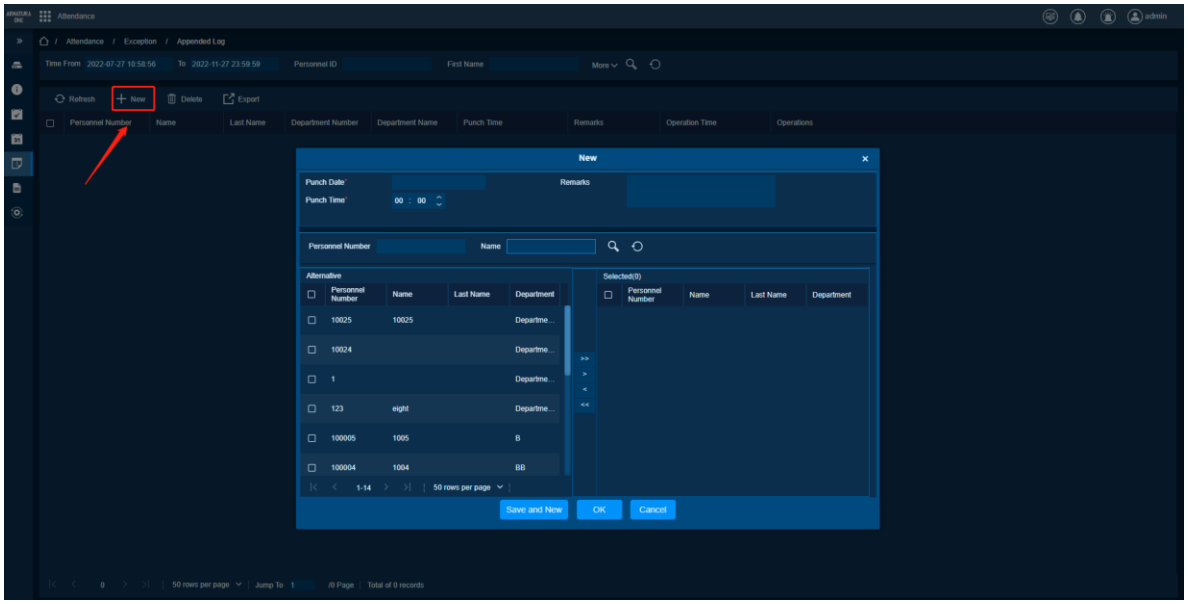
Steps:-

Signing Time: Set the date and time for re-signing the card, and the date and time settings.

Personnel: Choose the person who needs to re-sign the card, you can choose more; how to select the person.

Reason for Signing the Card: Enter the reason for signing the card as required, with a character length of 50.

1. Click **[Exception]** > **[Appended Log]**, click **[Add]**, select personnel, card signing date and card signing time.
2. Click **[Save and Continue]** to add a new supplementary form, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Succeeded in adding a supplementary form.

Function Usage Scenarios

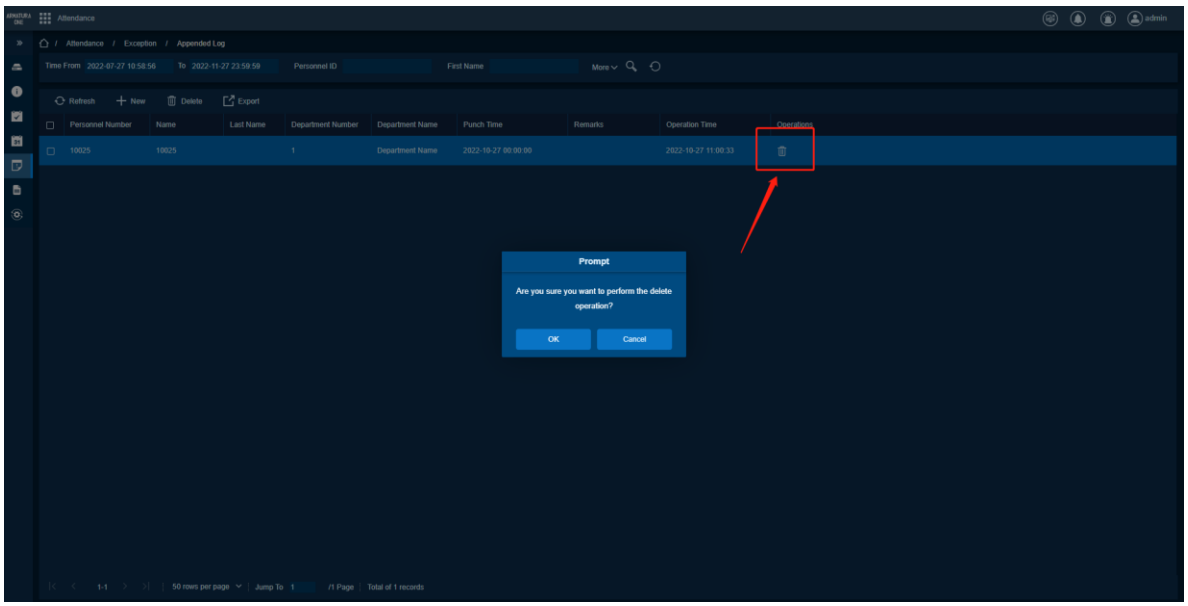
1. The person who made the re-signing form, the date of signing the card, and the time of signing the card need to be modified.
2. This supplementary form is not required.

Feature Trigger Result

Delete the supplementary sign form, and the staff attendance status will be restored to the state before the supplementary sign.

Steps:-

1. Click **[Exception]** > **[Appended Log]**, select Replenishment Form, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to delete successfully, click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Already reissued form information.

Function Usage Scenarios

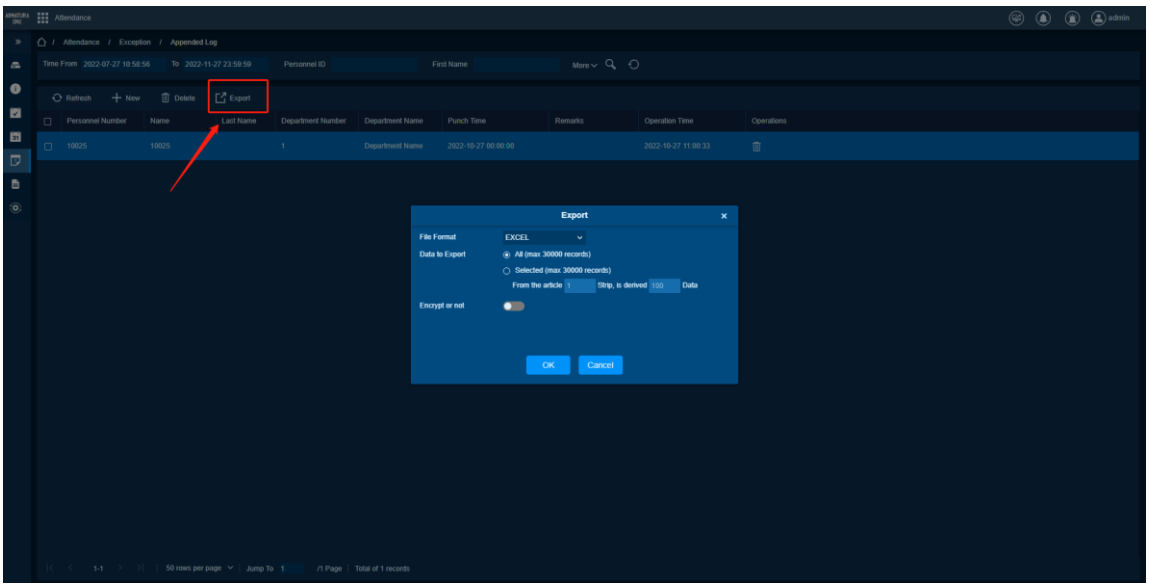
Need to re-sign the order data.

Feature Trigger Result

Obtain a table containing the list of supplementary data.

Steps:-

1. Click **[Exception]** > **[Appended Log]** and click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm Export, and click **[Cancel]** to cancel Export.



7.5.2. Leave

Function Description

When encountering special circumstances, personnel may need to ask for leave for different reasons and hope that the leave can be displayed in the system statistics.

Add

Preconditions for Normal Use of Function

Existing personnel information.

Function Usage Scenarios

Personnel need to ask for leave for different reasons, and the leave should be applied to the attendance system.

Feature Trigger Result

The staff implements the attendance calculation rules for the leave on the selected day of the leave.

Steps:-

Leave types: Set the type of leave for the leave.

Start time: The start time of the leave.

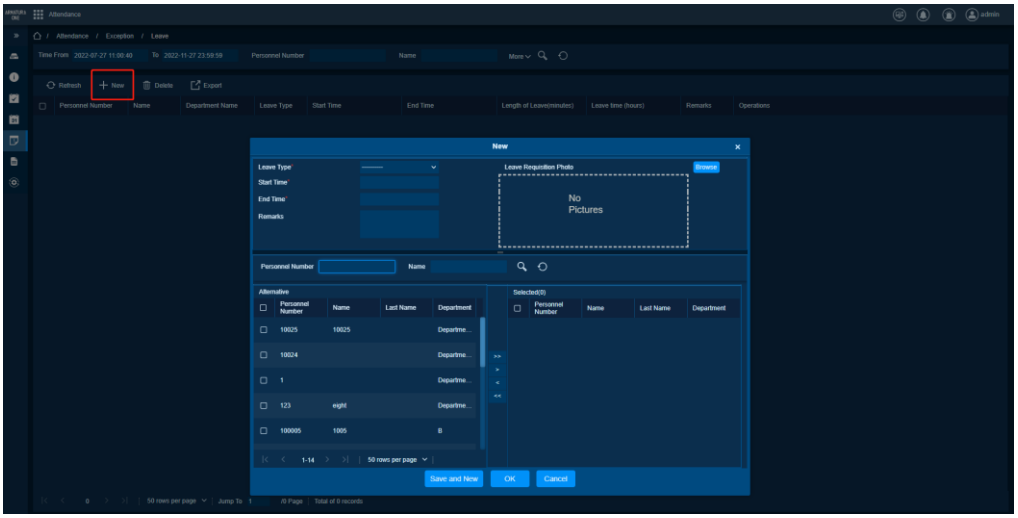
End time: The end time of the leave.

Photo of the leave request form: Upload a photo of the paper version of the leave request form.

Remarks: Leave instructions, character length 50.

Personnel: Select the person who needs to ask for leave, multiple choices.

1. Click **[Exception]** > **[Leave]**, click **[**Add**]**, select personnel, Leave Types, start time and end time, and upload the photo of the request form.
2. Click **[Save and Continue]** to add a leave request form, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Succeeded in adding a leave form.

Function Usage Scenarios

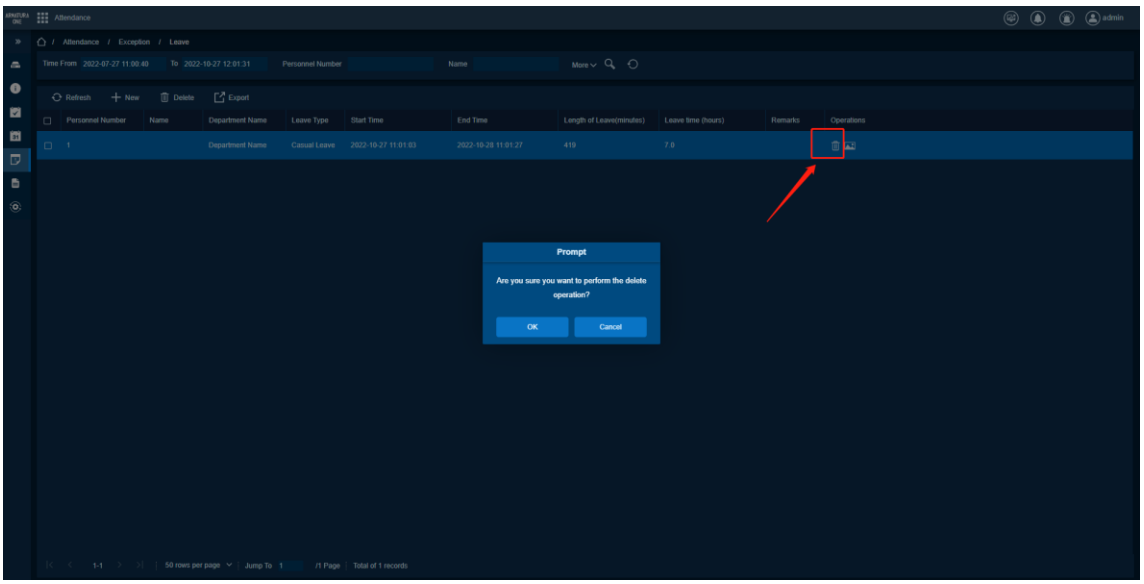
1. Need to modify the leave form information.
2. The leave form is not required.

Feature Trigger Result

The leave request form is deleted, and the staff attendance status is restored to the state before the leave request.

Steps:-

1. Click **[Exception]** > **[Leave]**, select the leave form, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to confirm the deletion, and click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Existing leave form information.

Function Usage Scenarios

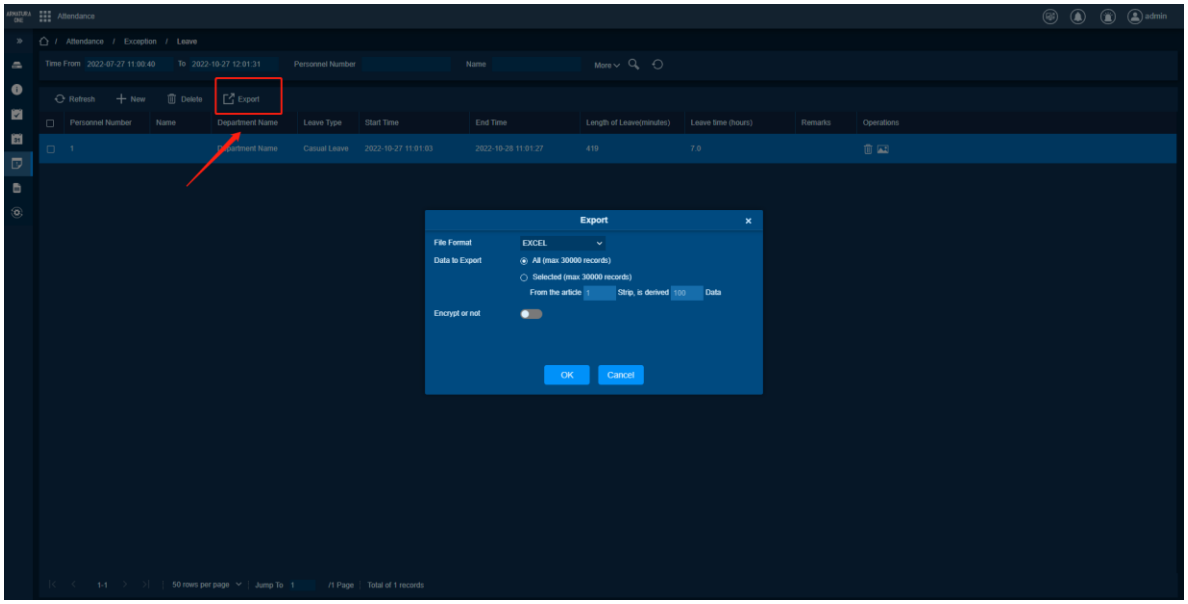
Data form of leave form that takes a period.

Feature Trigger Result

Obtain the form with the leave list data.

Steps:-

1. Click **[Exception]** > **[Leave]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm Export, and click **[Cancel]** to cancel Export.



7.5.3. Business Trip

Function Description

Can be set for personnel on business trips and applied to personnel attendance.

Add

Preconditions for Normal Use of Function

Existing personnel information.

Function Usage Scenarios

Personnel traveling on business, need to be recorded and used in attendance calculation.

Feature Trigger Result

The staff implements the attendance calculation rules for leave on the selected day of the business trip.

Steps:-

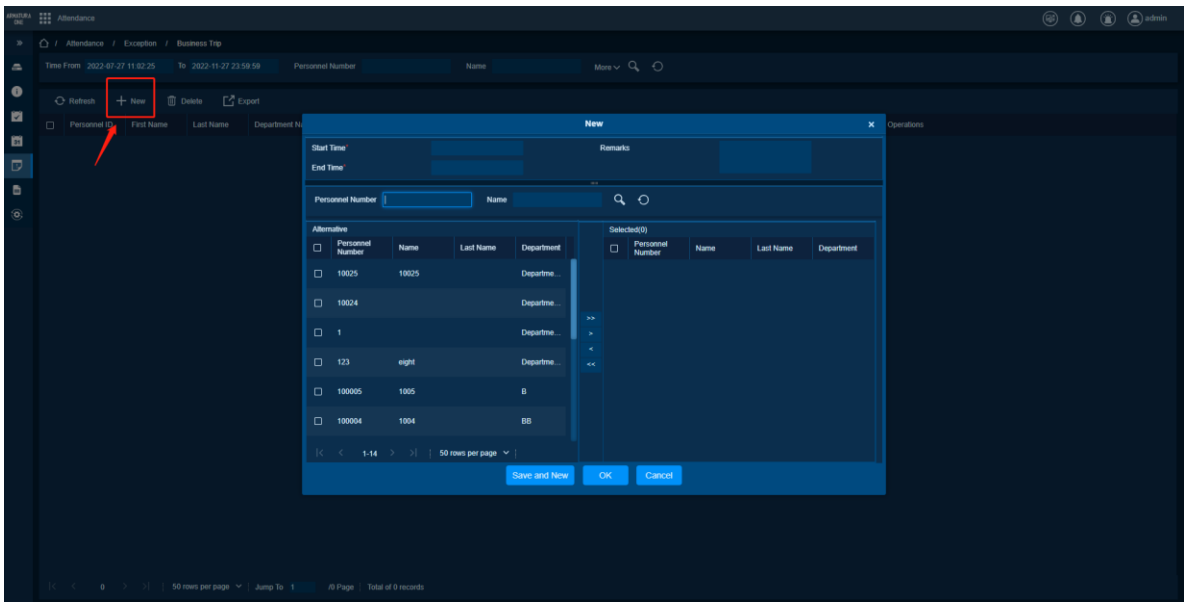
Start time: The start time of the business trip.

End time: the end time of the business trip.

Remarks: Description of business trip, the character length is 50.

Personnel: Choose the person who needs to travel on business, and you can choose more than one person.

1. Click **[Exception]** > **[Business Trip]**, click **[Add]**, select personnel, start time, and end time
2. Click **[Save and Continue]** to add a new travel order, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Successfully added a business travel order.

Function Usage Scenarios

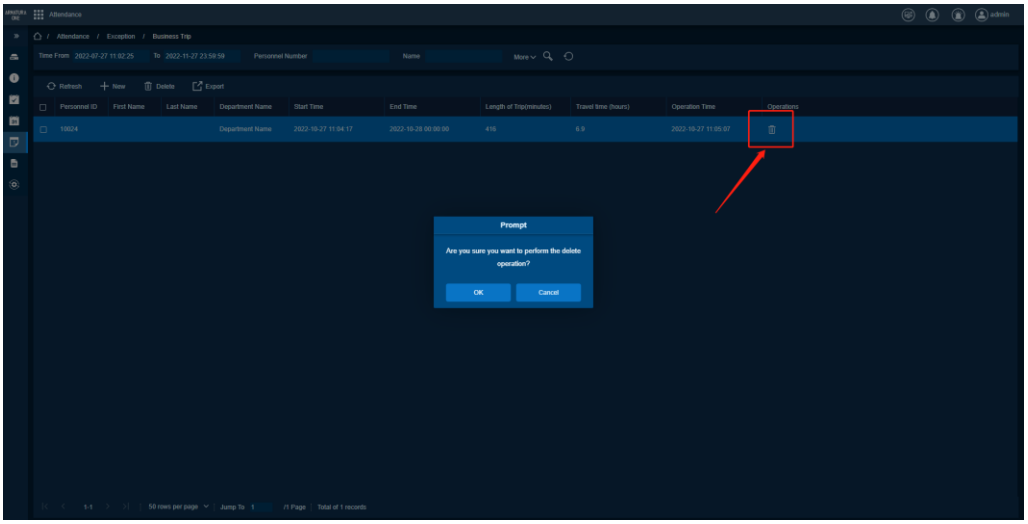
1. The information on the business trip needs to be modified.
2. No need for the business trip.

Feature Trigger Result

Delete the business trip, and the staff attendance status is restored to the state before the business trip.

Steps:-

1. Click **[Exception]** > **[Business Trip]**, select the business trip form, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to confirm the deletion, and click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Already business trip information.

Function Usage Scenarios

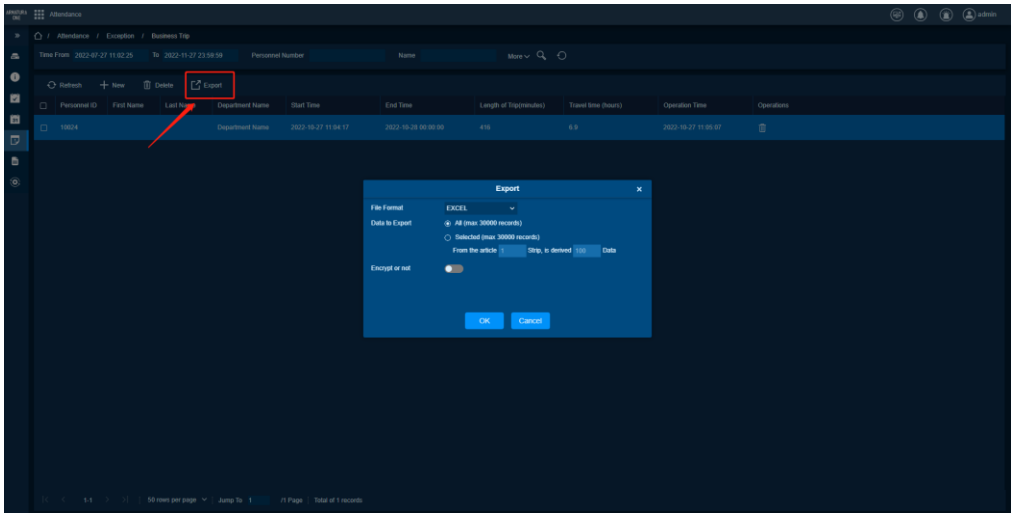
Data form of business travel order that needs a period.

Feature Trigger Result

Obtain a table with business trip list data.

Steps:-

1. Click **[Exception]** > **[Business Trip]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.5.4. Out

Function Description

Can be set for outgoing personnel and applied to personnel attendance.

Add

Preconditions for Normal Use of Function

Existing personnel information.

Function Usage Scenarios

The situation of personnel going out needs to be recorded and used in the attendance calculation.

Feature Trigger Result

The staff implements the attendance calculation rules for leave on the selected date when they go out.

Steps:-

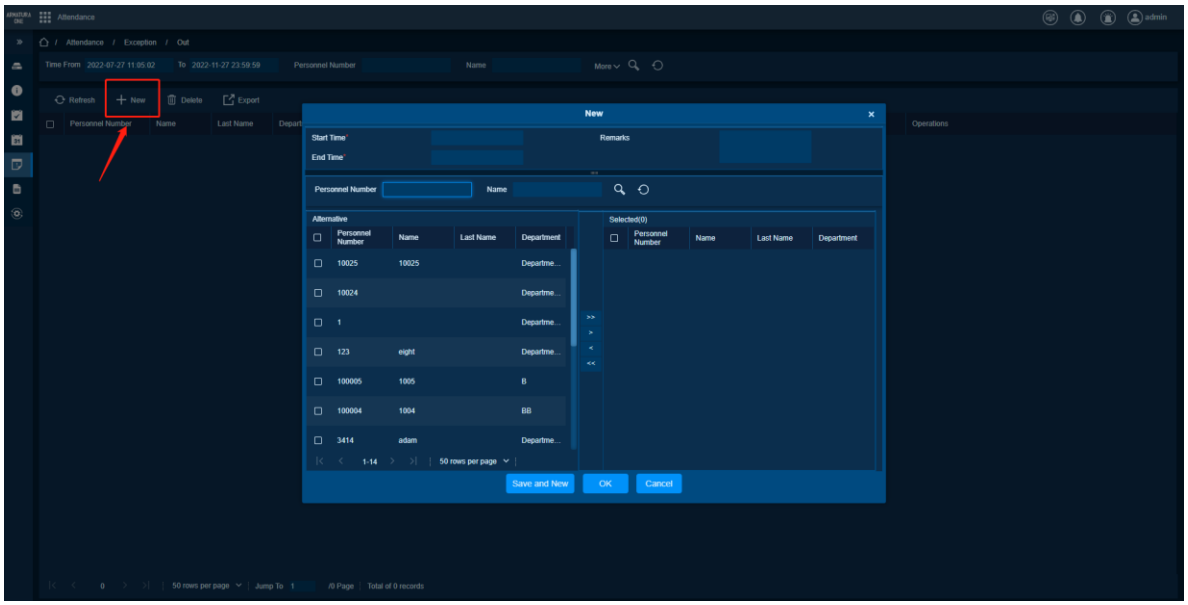
Start time: The start time of going out.

End time: The end time of the outing.

Remarks: Outing description, the character length is 50.

Personnel: Select the person who needs to go out, multiple choices are available.

1. Click **[Exception]** > **[Out]**, click **[Add]**, select personnel, start time, and end time.
2. Click **[Save and Continue]** to add a new outgoing order, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Successfully added outing order.

Function Usage Scenarios

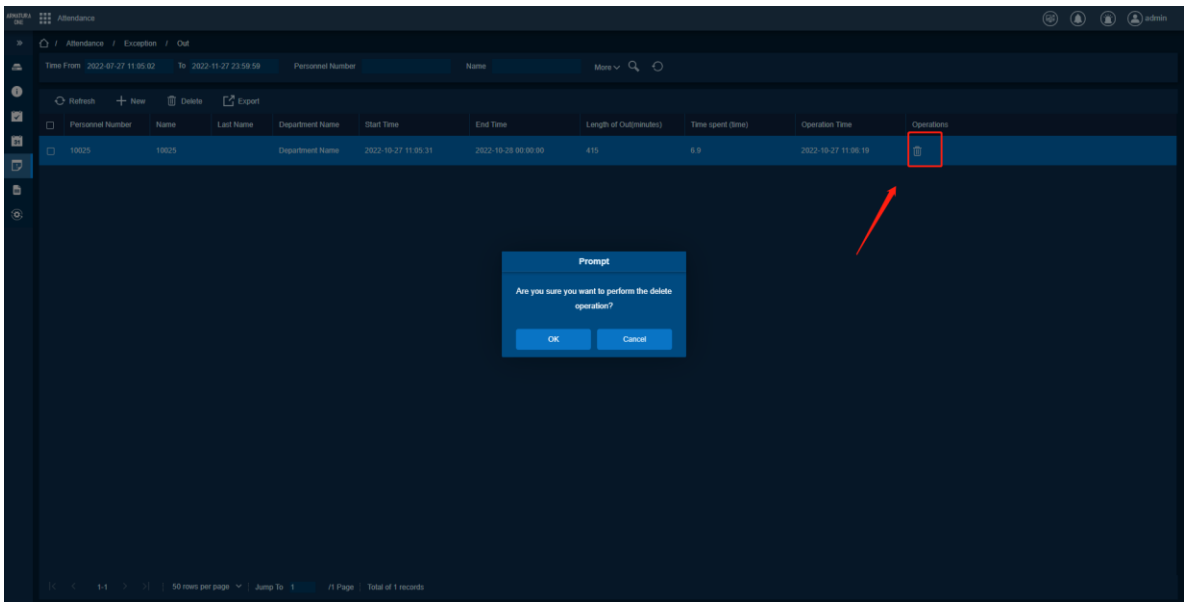
1. Need to modify the outing order information.
2. No need to go out.

Feature Trigger Result

Delete the outgoing order, and the staff attendance status will be restored to the state before going out.

Steps:-

1. Click **[Exception]** > **[Out]**, select the outgoing order, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to confirm the deletion, and click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Already out of order information.

Function Usage Scenarios

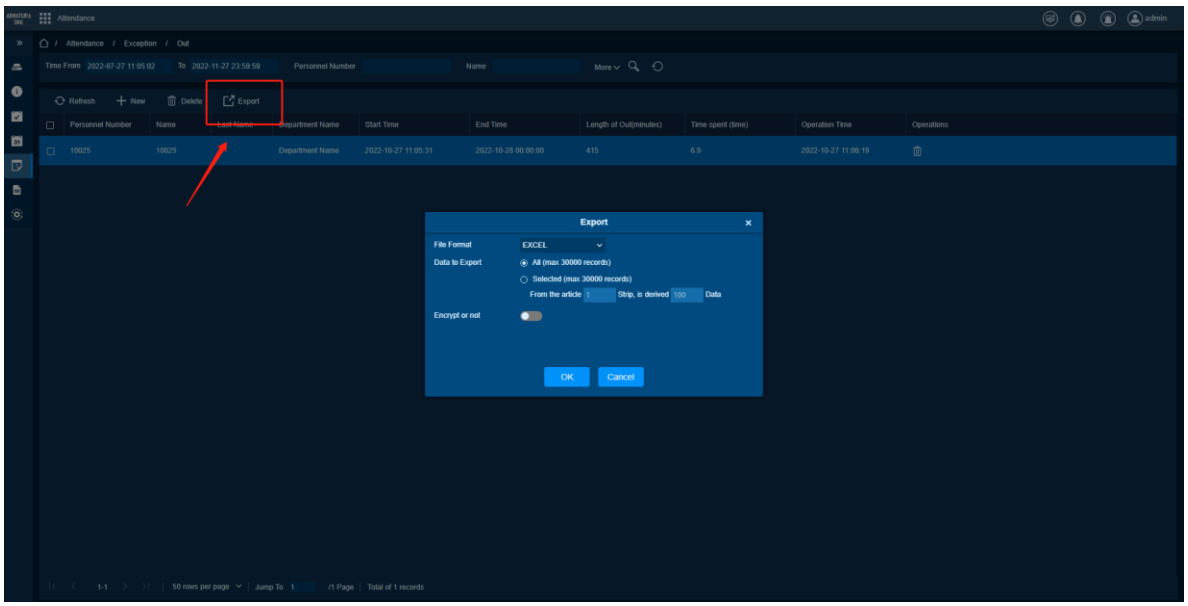
Data table that needs to be out of order within a period.

Feature Trigger Result

Get a table with outgoing list data.

Steps:-

1. Click **[Exception]** > **[Out]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.5.5. Overtime

Function Description

It can be set for personnel who work overtime and applied to personnel attendance.

Add

Preconditions for Normal Use of Function

Existing personnel information.

Function Usage Scenarios

Personnel overtime work needs to be recorded and used in attendance calculation.

Feature Trigger Result

The staff implements the attendance calculation rules for asking for leave on the selected day of overtime work.

Steps:-

Types of overtime: The default is three types of options: normal overtime, holiday overtime, and Holidays overtime.

Start time: the start time of overtime.

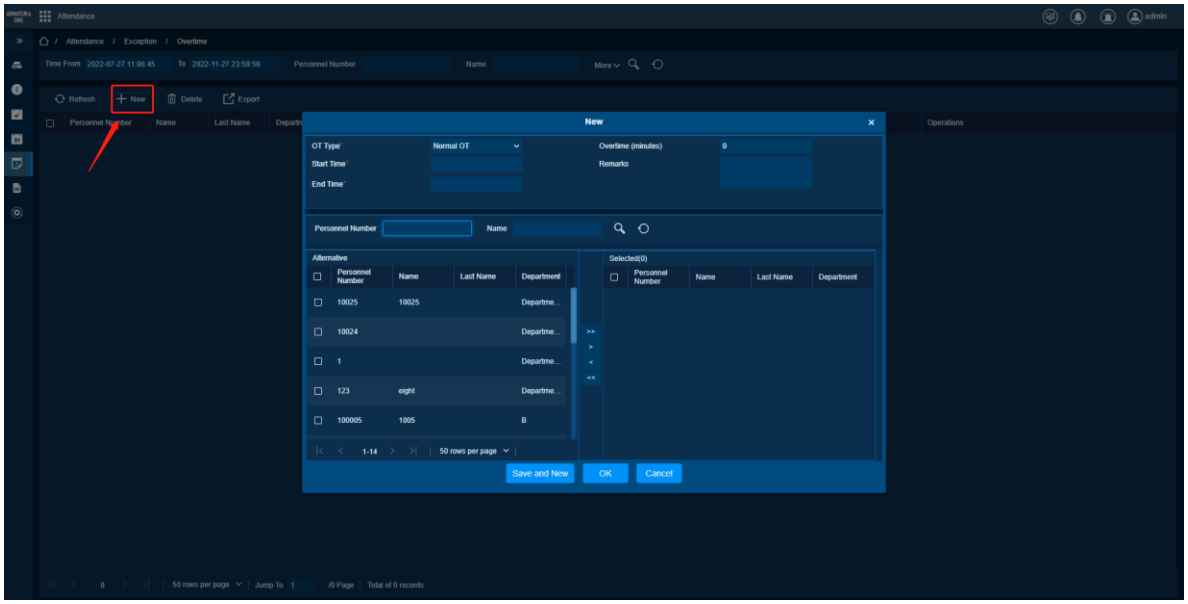
End time: the end time of overtime.

Reason for overtime: description of overtime, character length 50.

Personnel: Select the person who needs to work overtime, multiple choices are available.

1. Click **[Exception]** > **[Overtime]**, click **[Add]**, select personnel, overtime type, start time and end time.

2. Click **[Save and Continue]** to add a new class list, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Successfully added a new class list.

Function Usage Scenarios

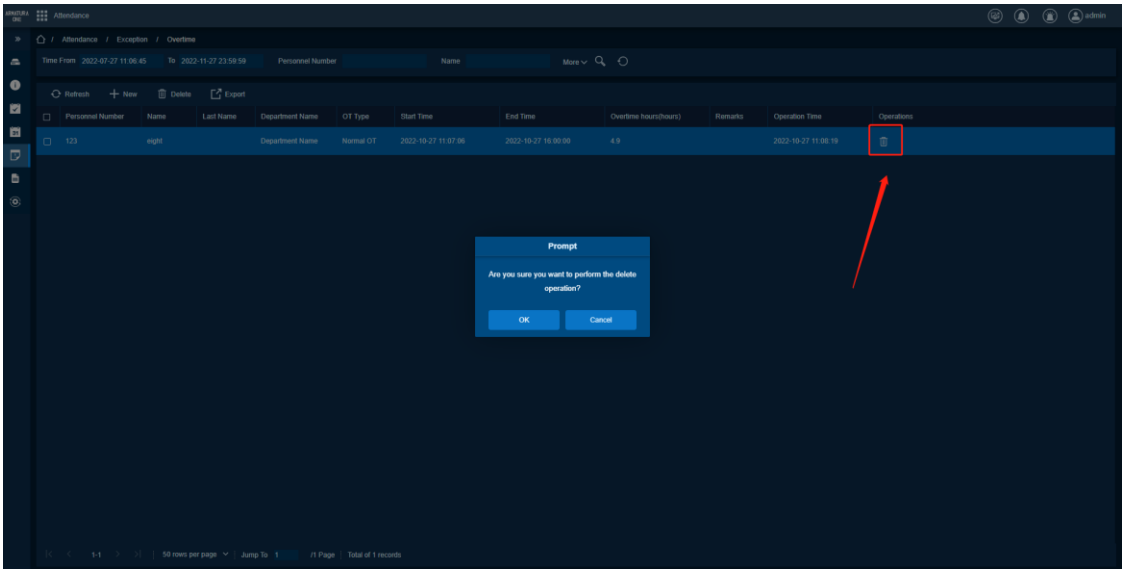
1. Need to modify overtime list information.
2. No need to work overtime.

Feature Trigger Result

Delete the overtime list, and the staff attendance status will be restored to the state without overtime.

Steps:-

1. Click **[Exception]** > **[Overtime]**, select the overtime list, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to confirm the deletion, and click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Existing overtime list information.

Function Usage Scenarios

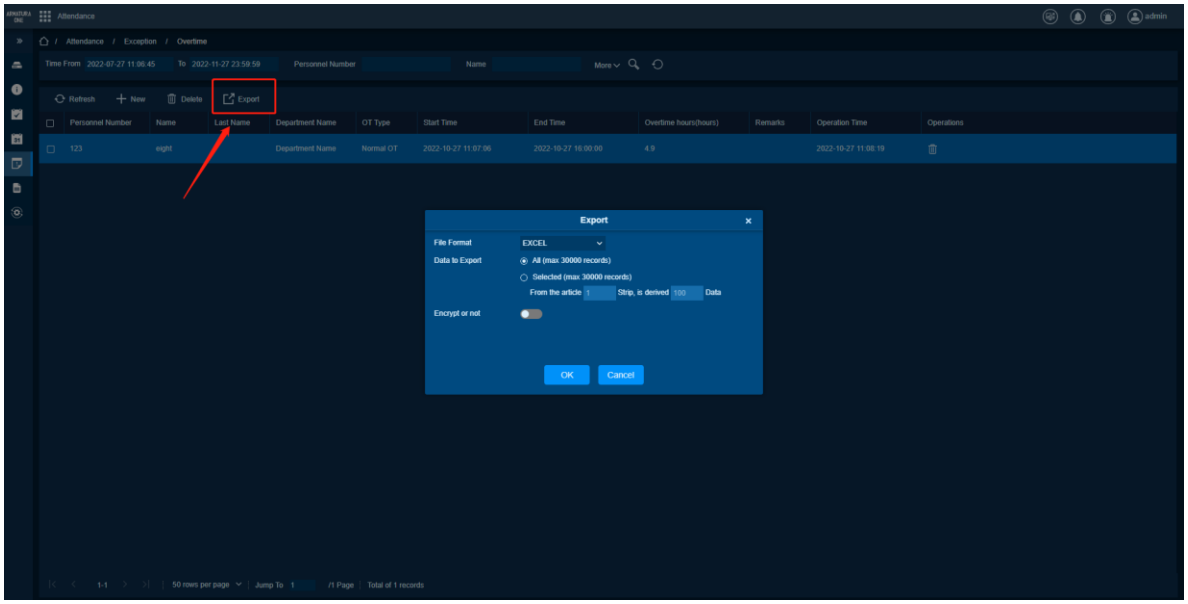
Data table of overtime bills that take a certain period.

Feature Trigger Result

Obtain a table with overtime list data.

Steps:-

1. Click **[Exception]** > **[Overtime]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.5.6. Adjust Shift

Function Description

Personnel can adjust their own Shift. There are three types of Shifts:

1. **Individual Shifts on the Same Date:** Shift shifts performed by the same person on the same day.
2. **Individual Shifts on Different Dates:** Shift shifts performed by the same individual on different dates.
3. **Two-Person Swap:** Shift swap performed by two different people on different dates.

Add

Preconditions for Normal Use of Function

1. Existing personnel information.
2. The staff has a shift on the date when the Shift needs to be adjusted. If two people swap Shift, both personnel need to have a shift on the adjusted date.

Function Usage Scenarios

Individuals need to adjust Shift on the same day/different days/with others.

Feature Trigger Result

1. The shift is successfully transferred, and the shift after shift is displayed on the staff schedule calendar.
2. Shift changes and applies to attendance calculation.

Steps:-

Field description of individual shift on the same date:

Personnel Number: length 32 (only the correct personnel number can be filled in, and the name and department name will be automatically backfilled when the mouse leaves).

Name: Obtain automatically according to the personnel number.

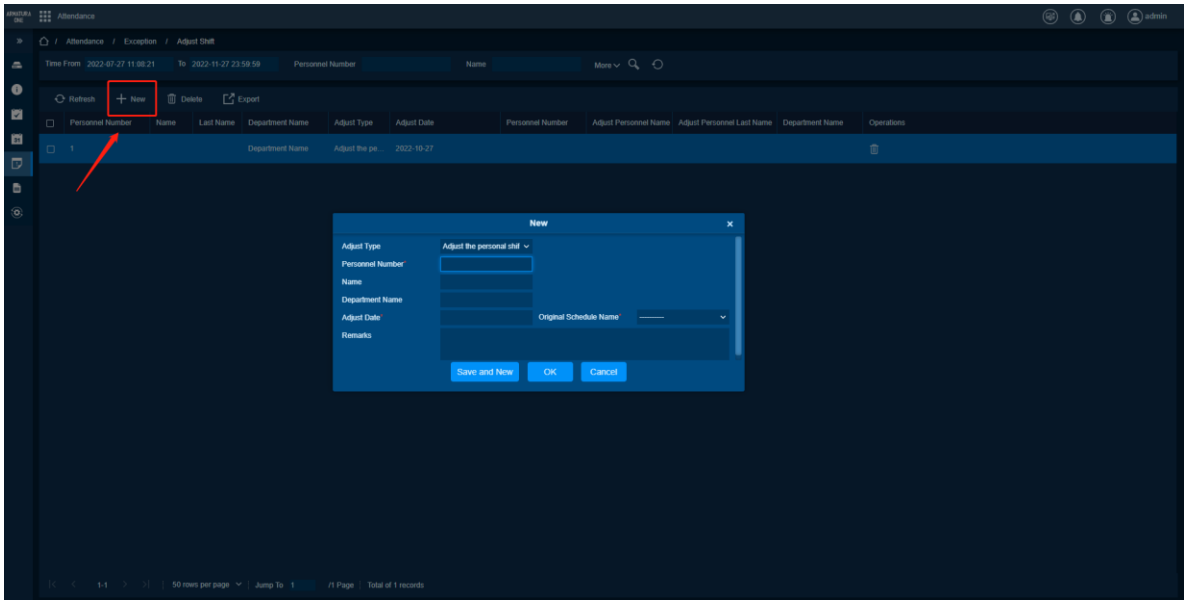
Department Name: Obtain automatically according to the personnel number.

Adjustment Date: the time and date of adjustment.

Adjust Shift Name: Select and adjust the corresponding Shift name.

Remarks: Description of shifts, the character length is 50.

1. Click **[Exception]** > **[Adjust Shift]**, click **[Add]**, select shift type, shift date and Shift name, enter personnel number, name, department name and other information.
2. Click **[Save and Continue]** to add a new shift list, the page will not close, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Two-Person Swap Field Description: -

Personnel ID: The person ID that needs to be adjusted, the length is 32 (only the correct person ID can be filled in, and the name and department name will be automatically filled.

Name: Obtain automatically according to the personnel number.

Department Name: Obtain automatically according to the personnel number.

Swap Personnel Number: the personnel number to be swapped, length 32 (only the personnel number can be filled in, and the name and department name will be automatically backfilled when the mouse leaves).

Swap Name: Obtain automatically according to the number of the swapped person.

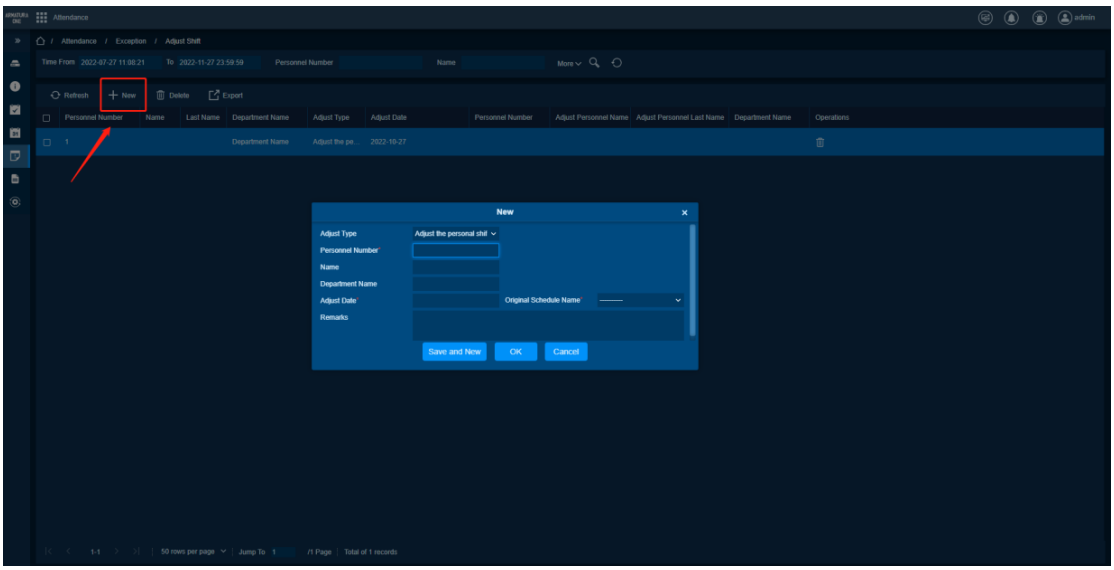
The Name of the Swap Department: It is automatically obtained according to the number of the swap personnel.

Adjustment Date: The time and date of adjustment.

Swap Date: Select the time and date of the swap.

Remarks: Description of shifts, the character length is 50.

1. Click **[Exception]** > **[Adjust Shift]**, click **[Add]**, select shift type, shift date and swap date, enter personnel number, name, department name, and swap personnel number and other information
2. Click **[Save and Continue]** to add a new shift list, the page will not be closed, you can continue to add, click **[OK]** to add successfully, click **[Cancel]** to cancel the addition.



Delete

Preconditions for Normal Use of Function

Successfully added shift information.

Function Usage Scenario

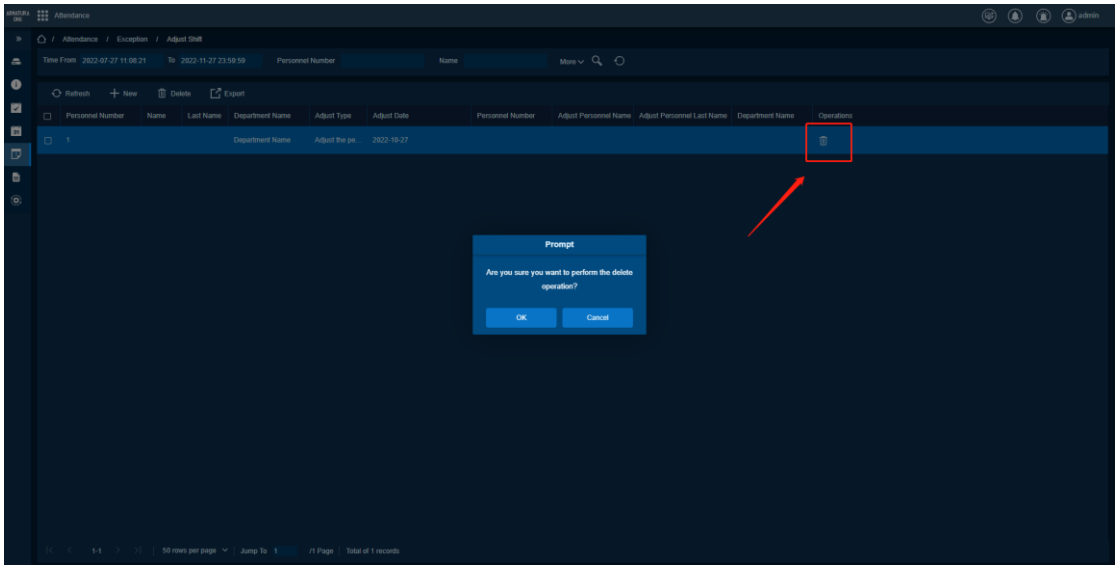
1. Need to modify the shift information.
2. No need to apply this shift.

Feature Trigger Result

Personnel Shift is restored to the state before the shift.

Steps:-

1. Click **[Exception]** > **[Adjust Shift]**, select shift information, and click **[Delete]**.
2. In the pop-up window, click **[OK]** to confirm the deletion, and click **[Cancel]** to cancel the deletion.



Export

Preconditions for Normal Use of Function

Already has transfer information.

Function Usage Scenarios

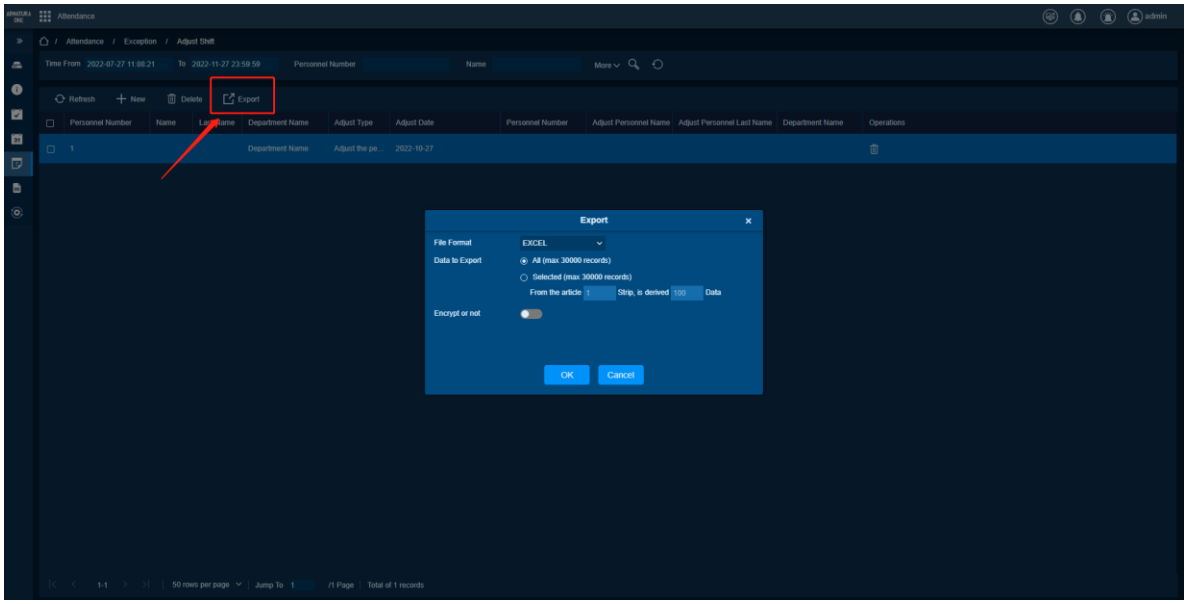
Data table that needs to be transferred within a period.

Feature Trigger Result

Obtain a table with shift list data.

Steps:-

1. Click **[Exception]** > **[Adjust Shift]**, click Export.
2. Select the file format and Export method, click **[OK]** to confirm Export, and click **[Cancel]** to cancel Export.



7.6. Calculate Report

Function List

Function	Description
Manual Calculation	Calculate attendance for departments and personnel.
Original Record Sheet	Display the attendance records of all employees, including attendance records uploaded by the attendance machine and reissued cards.
Daily Details Table	Display the personnel's daily attendance status, clock-in times, earliest time, latest time, and detailed clock-in time during the selected period.

Leave Summary Form	Display the effective time and type of leave of all valid leave records within the selected date range.
Daily Detailed Report	Within the selected date range, the personnel's daily attendance details, including attendance, lateness, and early departure, etc.
Monthly Detailed Report	Within the range of the selected month, the personnel's daily attendance status is reflected in characters, and the actual attendance time of the month is summarized, and the length of abnormal absenteeism, leave, business trip, outing, etc.
Monthly Statistics Report (By Personnel)	Within the range of the selected month, the personnel attendance summary status and detailed information, including attendance, late arrival, early departure, abnormality, etc.
Departmental Statistical Report (By Department)	Select detailed attendance information of all personnel in the department, including attendance, late arrival, early departure, abnormality, etc.
Annual Statistical Report (By Person)	Within the selected year, the personnel attendance summary status and detailed information, including attendance, late arrival, early departure, abnormality, etc.

7.6.1. Manual Calculate

Function Description

Calculating department and personnel attendance.

Attendance Calculation

Preconditions for Normal Use of Function

In the **[Personnel]** module, in the personnel attendance setting **[Whether attendance]** is set to **[Yes]**.

Function Usage Scenarios

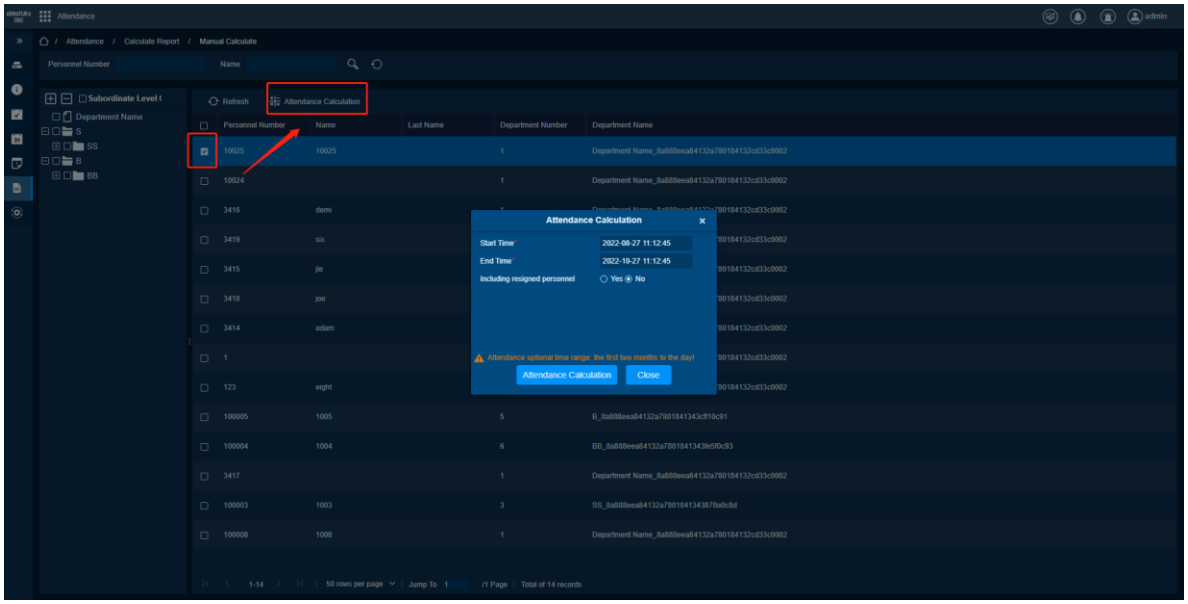
Calculate attendance for departments or personnel.

Feature Trigger Result

Successfully calculate the attendance of the department or personnel.

Steps:-

1. Click **[Calculate Report]** > **[Manual Calculate]**, select department/person, and click **[Attendance Calculation]**.
2. In the pop-up window, select the start time, end time and whether to include resigned personnel, click **[OK]** to confirm the attendance calculation, and click **[Cancel]** to cancel the attendance calculation.



7.6.2. Transactions

Function Description

Display the attendance records of all employees, including attendance records uploaded by the attendance machine and reissued cards. The record of normal clocking on the device will be uploaded to the software as the original record. When a certain piece of data is selected, details will be displayed on the right side of the page.

Export

Preconditions for Normal Use of Function

Existing employee attendance records.

Function Usage Scenarios

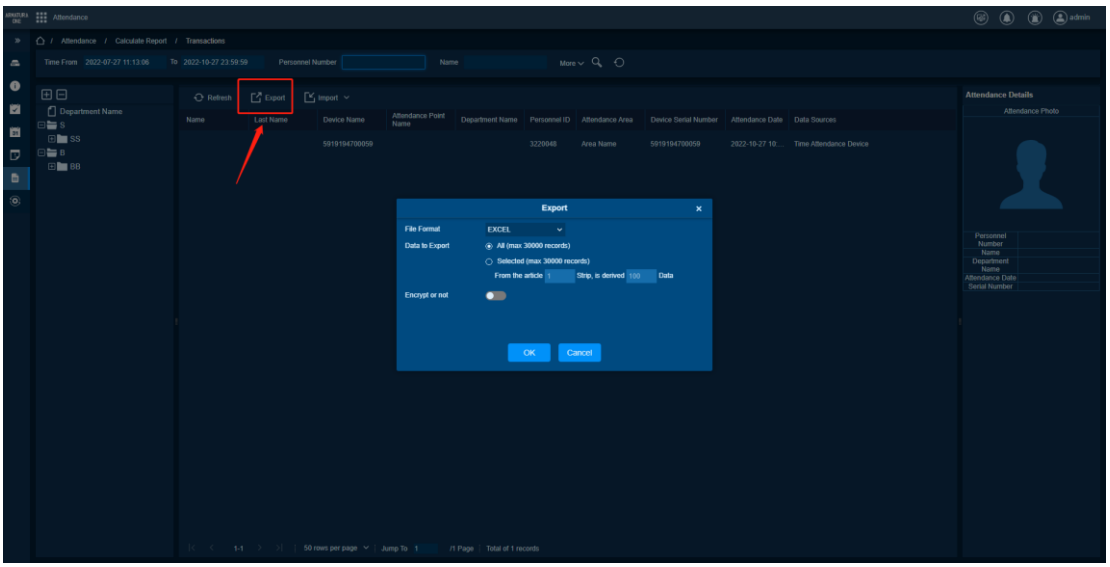
Need to obtain the original record of personnel attendance information.

Feature Trigger Result

Obtain the original record sheet of personnel attendance information.

Steps:-

1. Click **[Calculate Report]** > **[Transactions]**, click **Export.**
2. Select the file format and export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



Import Access Control/Parking/FaceKiosk Records

Preconditions for Normal Use of Function

Existing access control/parking/FaceKiosk record.

Function Usage Scenarios

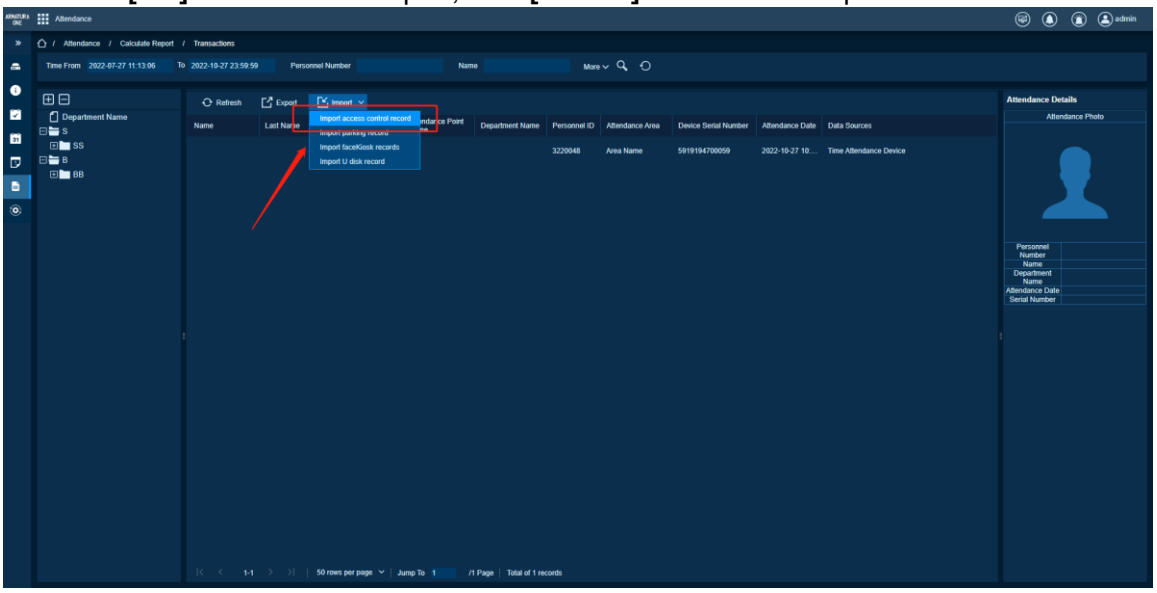
Import access control/FaceKiosk event records as attendance records.

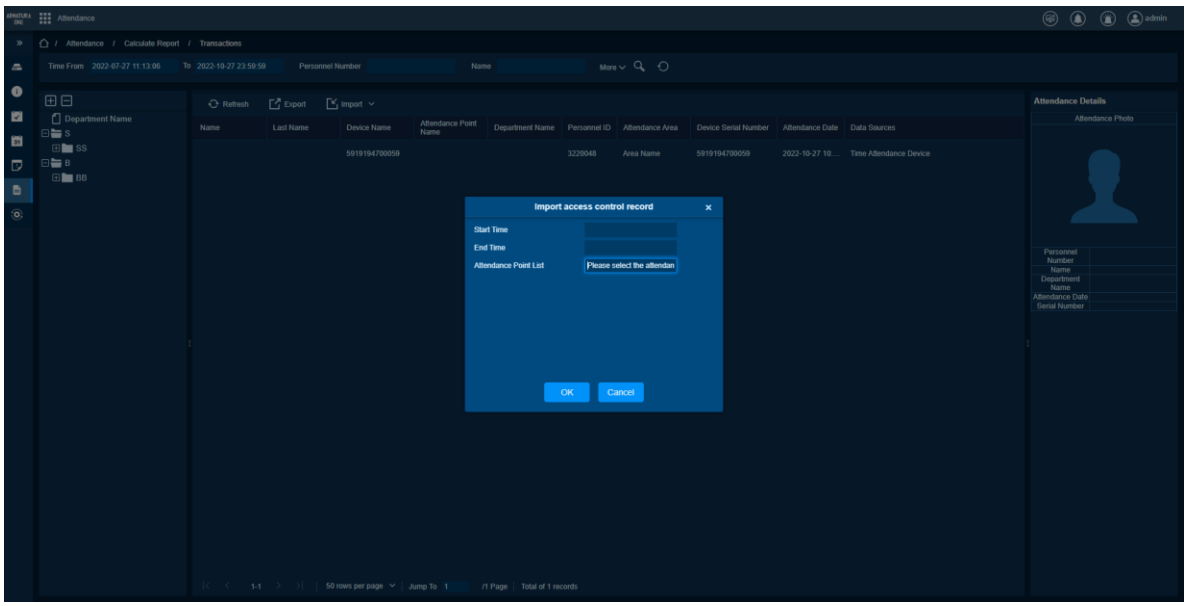
Feature Trigger Result

Use access control/FaceKiosk event records to generate attendance records.

Steps:-

1. Click **[Calculate Report]** -> **[Transactions]** -> **[Import]**, click to import access control/parking/FaceKiosk records.
2. Select the start time, end time and the corresponding attendance point list.
3. Click **[OK]** to confirm the import, click **[Cancel]** to cancel the import.





Import U Disk Record

Preconditions for Normal Use of Function

Existing U disk record.

Function Usage Scenarios

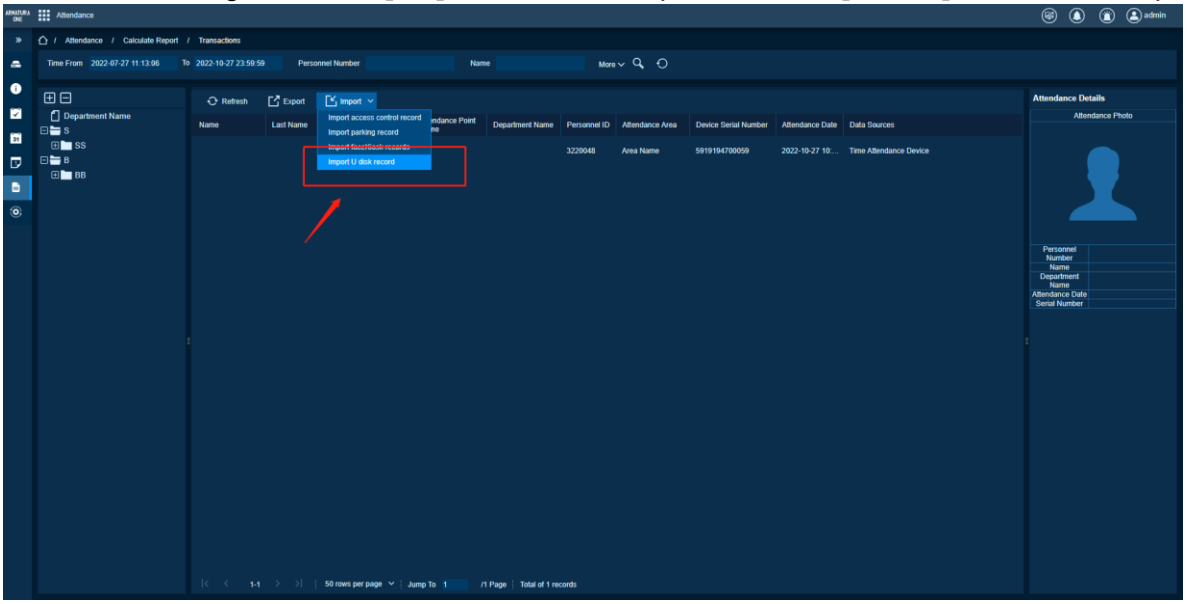
Import U disk records as attendance records.

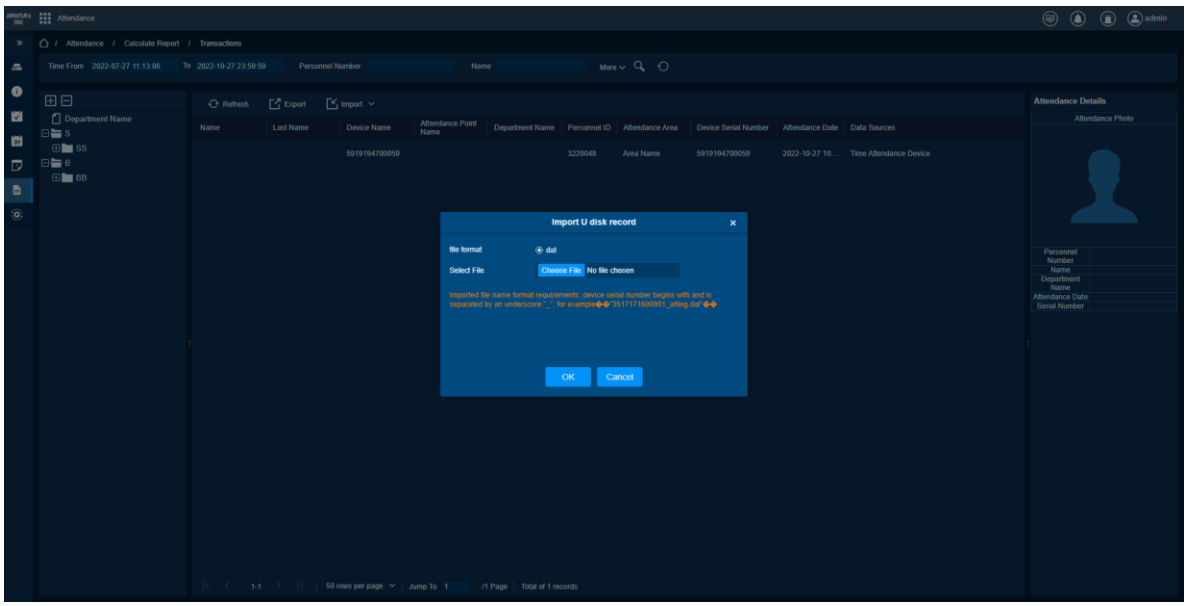
Feature Trigger Result

Use U Disk Record to Generate Attendance Record.

Steps:-

1. Click **[Calculate Report]** > **[Import]** > **[Import U Disk Record]**.
2. Select the target file, click **[OK]** to confirm the import, and click **[Cancel]** to cancel the import.





7.6.3. Daily Attendance

Function Description

This table displays the personnel's daily attendance status, number of clock-in times, earliest time, latest time, and detailed clock-in time during the selected period.

Export

Preconditions for Normal Use of Function

Existing personnel check-ins information.

Function Usage Scenarios

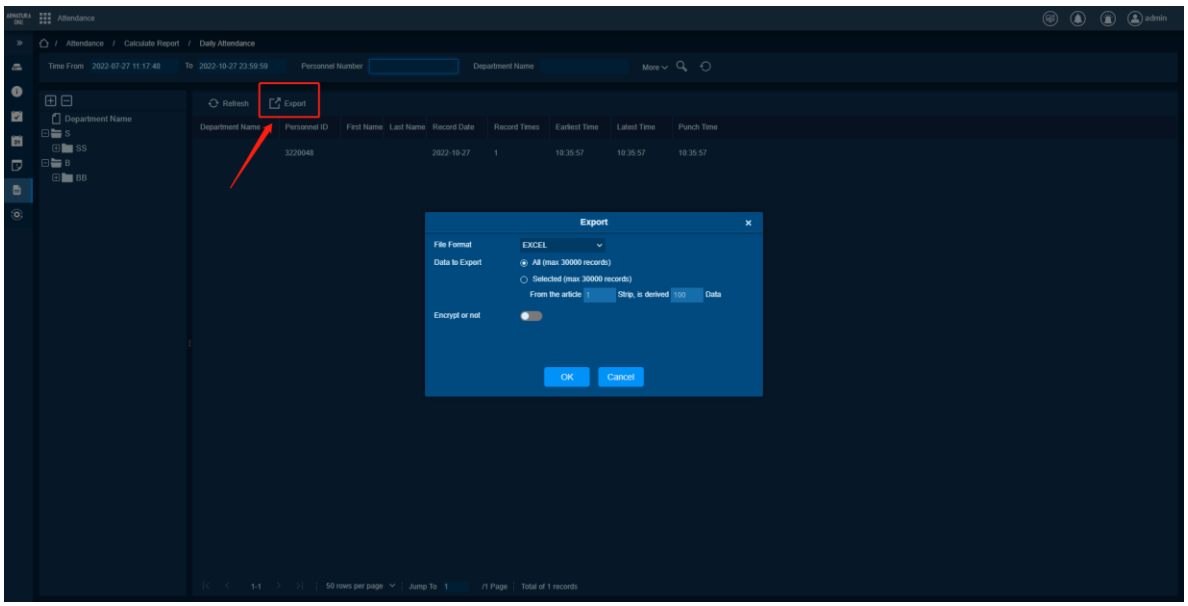
Export staff daily check-ins details table.

Feature Trigger Result

Get the details table of the staff daily check-ins.

Steps:-

1. Click **[Calculate Report]** > **[Daily Attendance]**, click **Export.**
2. Select the file format and Export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.6.4. Leave Summary

Function Description

The report summarizes the effective time and type of leave of all valid leave records within the selected date range. The effective time (minutes) is the number of minutes between the start time and the end time of the leave record.

Export

Preconditions for Normal Use of Function

Existing leave-related data information.

Function Usage Scenarios

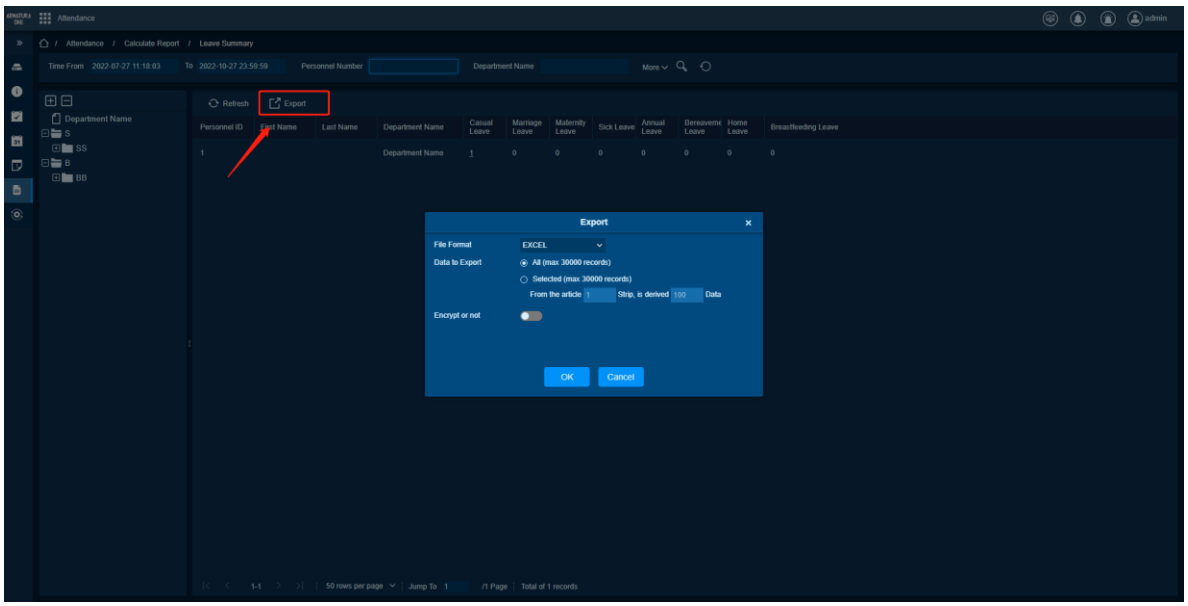
Need to view the summary data of leave.

Feature Trigger Result

Get a table containing all leave data for the currently selected date.

Steps:-

1. Click **[Calculate Report]** > **[Leave Summary]**, click **Export.**
2. Select the file format and export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.6.5. Daily Report

Function Description

Within the selected date range of the report, detailed information about personnel's daily attendance, including attendance, lateness, and early departure, etc.

Export

Preconditions for Normal Use of Function

Existing personnel attendance information.

Function Usage Scenarios

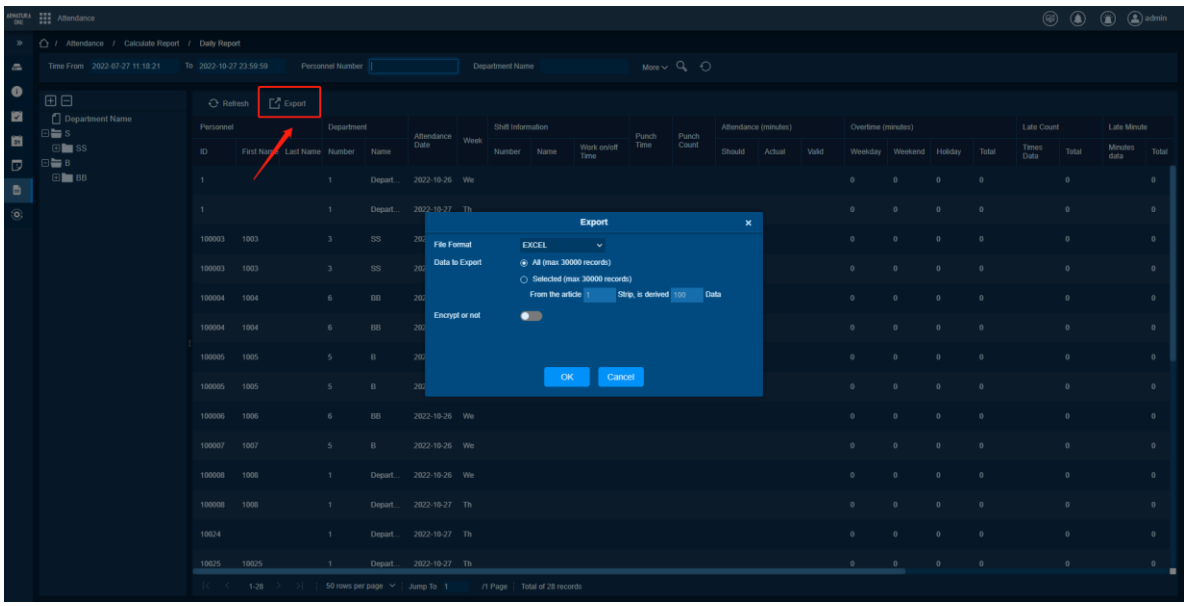
Need to obtain personnel attendance information daily detailed report.

Feature Trigger Result

Obtain the daily detailed report of personnel attendance information.

Steps:-

1. Click **[Calculate Report]** > **[Daily Report]**, click **[Export]**.
2. Select the file format and export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.6.6. Monthly Detail Report

Function Description

Within the range of the selected month of the report, the personnel's daily attendance status is reflected in characters, and the actual attendance time of the month is summarized, and the duration of abnormal absenteeism, leave, business trip, and outing.

The priority of each attendance status display is should arrive/actually <leave early <late <not checked out <not checked in <leave, travel, go out, overtime <absent from work <schedule and rest <not scheduled <shift off, make up Shifts, shifts (the same date for individuals, different dates for individuals, two people swapping) <Holidays.

Export

Preconditions for Normal Use of Function

Existing personnel attendance information.

Function Usage Scenarios

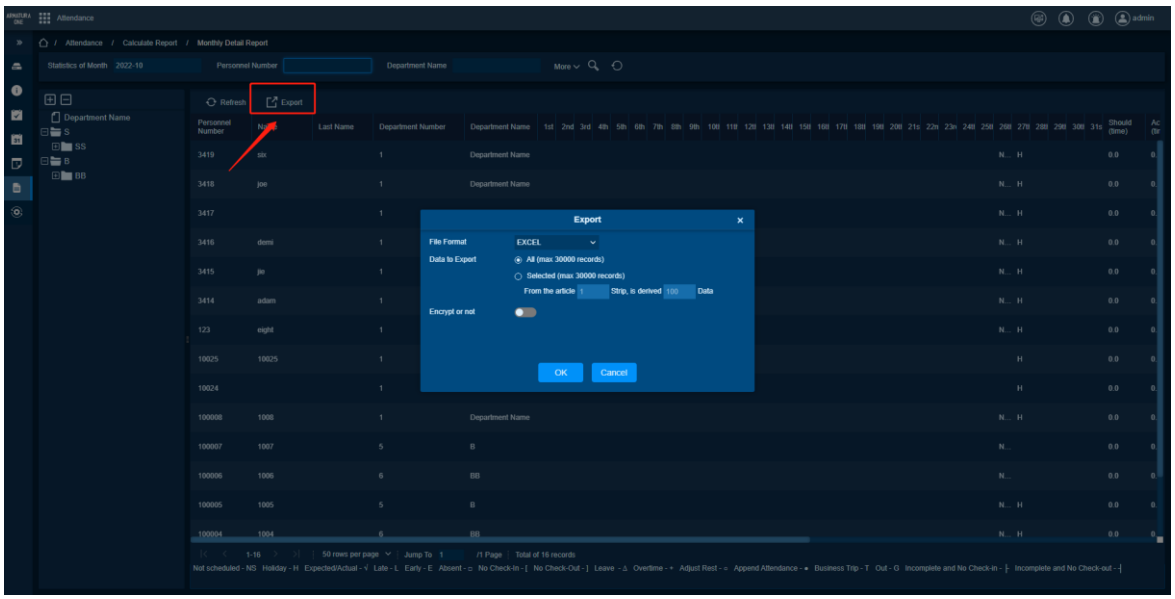
Need to obtain a monthly detailed report of personnel attendance information.

Feature Trigger Result

Obtain the monthly detailed report of personnel attendance information.

Steps:-

1. Click **[Calculate Report]** > **[Monthly Detail Report]**, click **[Export]**.
2. Select the file format and export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.6.7. Monthly Statistical Report (By Person)

Function Description

The summary status and detailed information of personnel attendance within the range of the selected month of the report, including attendance, late arrival, early departure, abnormality, etc.

Export

Preconditions for Normal Use of Function

Existing personnel attendance information.

Function Usage Scenarios

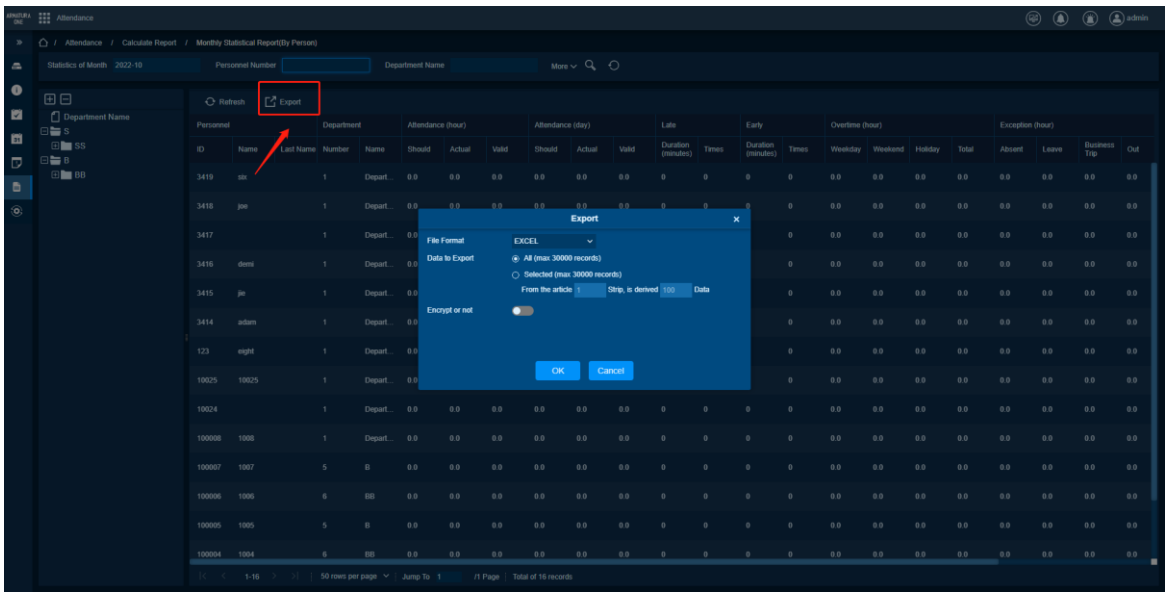
Need to obtain a monthly statistical report of personnel attendance information.

Feature Trigger Result

Obtain the monthly statistical report of personnel attendance information (by person).

Steps:-

1. Click **[Calculate Report]** > **[Monthly Statistical Report** (**By Person**)**]**, click **[Export]**.
2. Select the file format and export method, click **[OK]** to confirm export, and click **[Cancel]** to cancel export.



7.6.8. Departmental Reports (By Department)

Function Description

Within the date range of the report selection, select the detailed attendance information of all personnel in the department, including attendance, late arrival, early departure, abnormality, etc.

Export

Preconditions for Normal Use of Function

Existing personnel attendance information.

Function Usage Scenarios

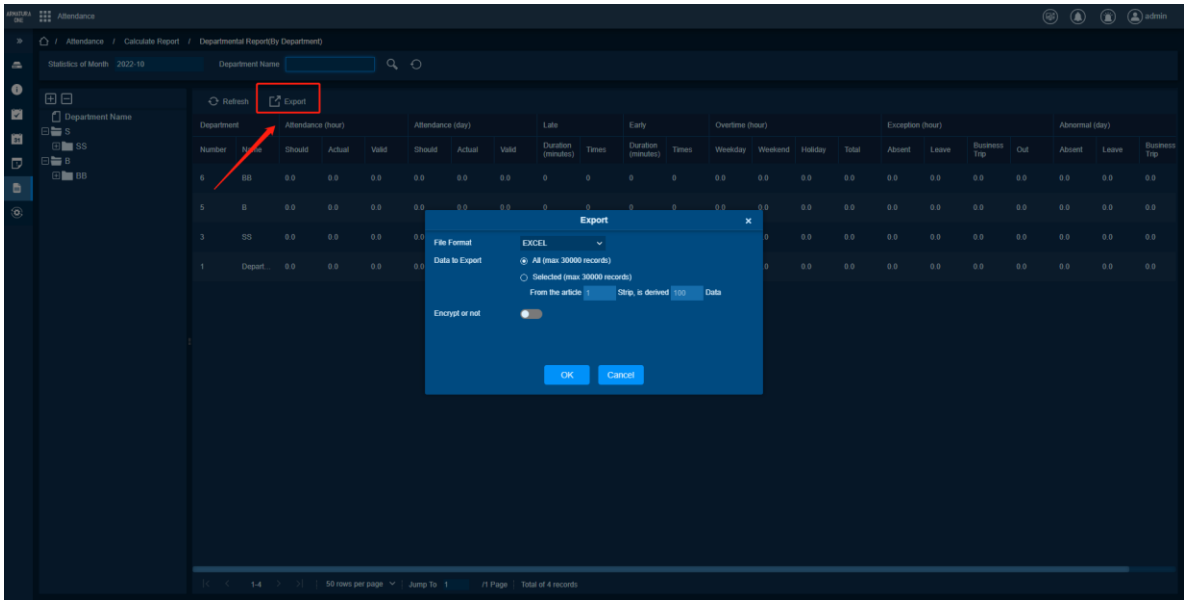
Need to obtain staff attendance information department statistics report (by department).

Feature Trigger Result

Obtain the departmental statistical report of personnel attendance information (by department).

Steps:-

1. Click **[Calculate Report]** > **[Departmental Report** (**By Department**)**]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm Export, and click **[Cancel]** to cancel Export.



7.6.9. Annual Report (By Person)

Function Description

Within the range of the selected year, the personnel attendance summary status and detailed information, including attendance, late arrival, early departure, abnormality, etc.

Export

Preconditions for Normal Use of Function

Existing Personnel Attendance Information

Function Usage Scenarios

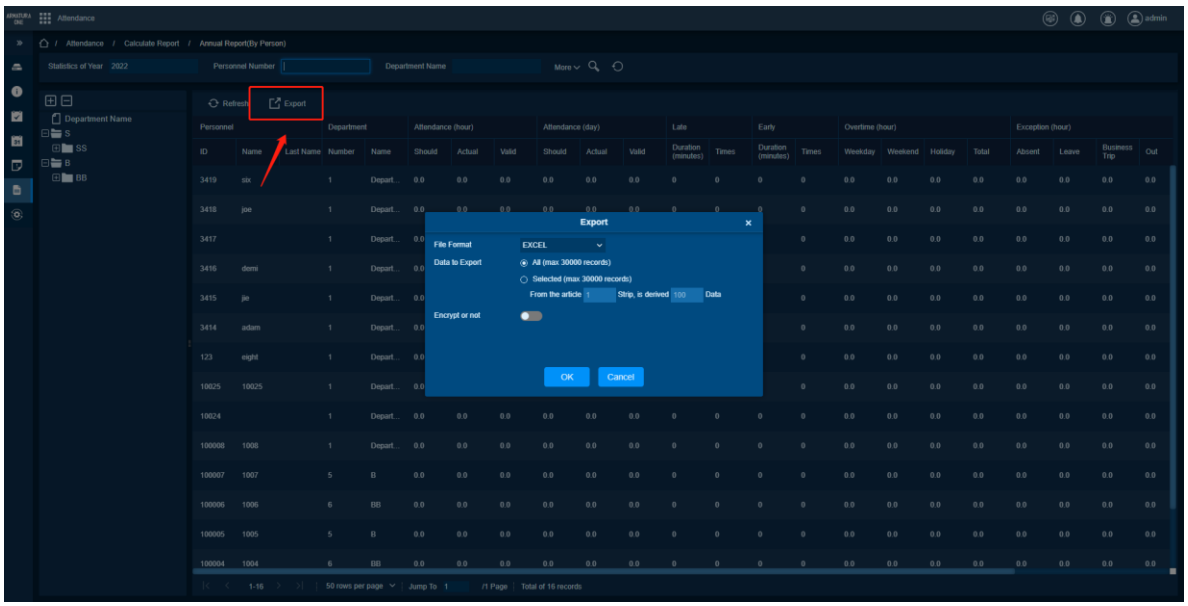
Need to obtain the annual statistical report of personnel attendance information (by person).

Feature Trigger Result

Obtain the annual statistical report of personnel attendance information (by person).

Steps:

1. Click **[Calculate Report]** > **[Annual Report** (**By Person**)**]**, click **[Export]**.
2. Select the file format and Export method, click **[OK]** to confirm Export, and click **[Cancel]** to cancel Export.



7.7. Process Tasks

Function List

Functions	Operations Introduction
My Application	Display the records of exception management requested by the user.
Pending Tasks	Display tasks waiting for the user's approval and can perform approval operations.
Approved Task	Show the tasks that the user has approved.

7.7.1. My Application

Function Description

Display the records of exception management requested by the user.

Export

Preconditions for Normal Use of Function

User requests exception management.

Function Usage Scenarios

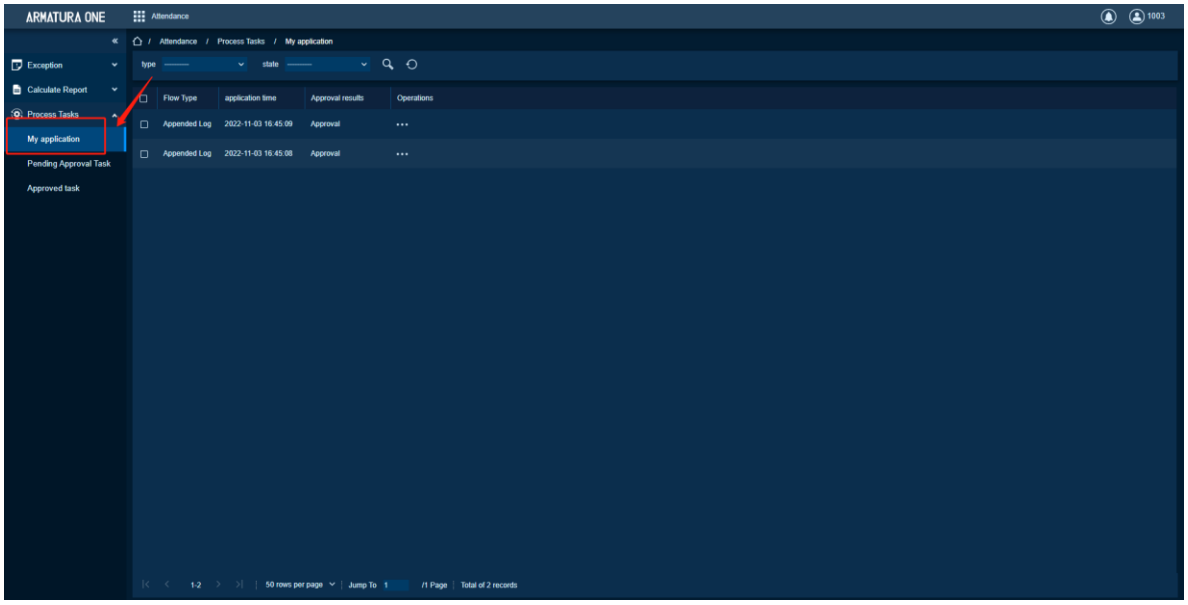
It is necessary to obtain the application record of the employee exception.

Feature Trigger Result

Obtain the application record of the employee's exception.

Steps:-

1. Click **[Attendance Device]** > **[Process Tasks]**, click **[My Application]**.



7.7.2. Pending Approval Task

Function Description

Display tasks waiting for the user's approval and can perform approval operations.

Export

Preconditions for Normal Use of Function

The user requests approval.

Function Usage Scenarios

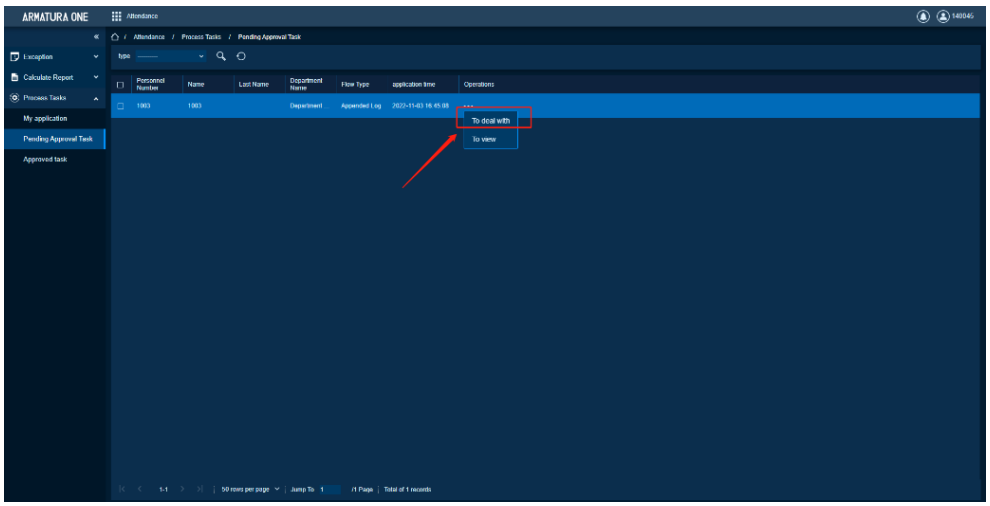
Need to get user pending tasks.

Feature Trigger Result

Get records for approval and take action.

Steps:

1. Click **[Attendance Device]** > **[Process Tasks]**, click **[Pending Approval Task]**.
2. Click **[...]** > **[To deal with]**.



7.7.3. Approved Tasks

Function Description

Show the tasks that the user has approved.

Export

Preconditions for Normal Use of Function

Approve tasks with review.

Function Usage Scenarios

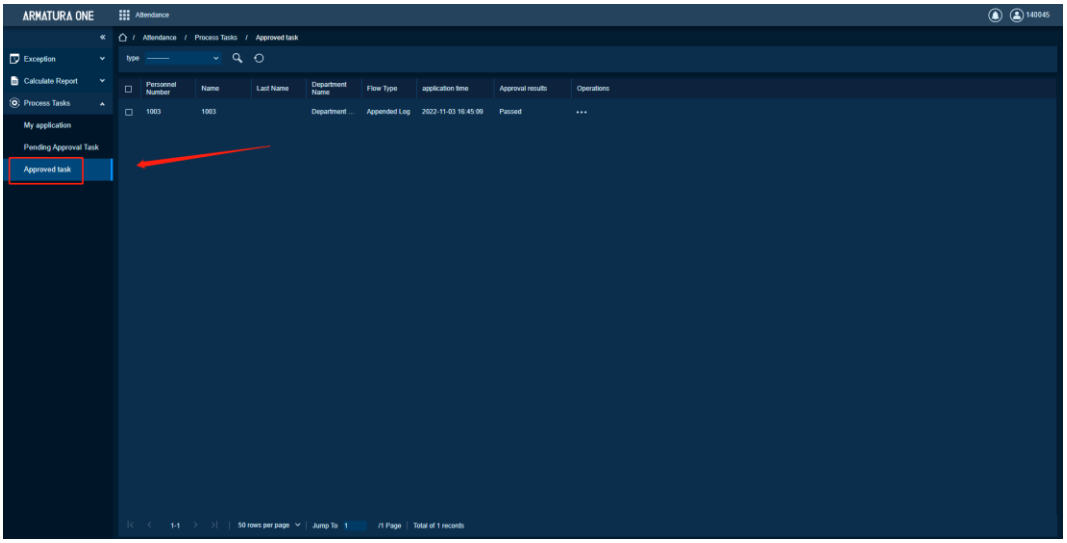
The approved task flow needs to be displayed.

Feature Trigger Result

Get the approved task process.

Steps:

1. Click **[Attendance Device]** > **[Process Tasks]**, click **[Approved task]**.



8. Elevator Control Management

The following is the manual of online elevator control. If you are using offline elevator control.

The Elevator Control System is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's rights to floors and elevator control time, and supervise elevator control events. You can set registered users' rights to floors. Only authorized users can reach certain floors within a period after being authenticated. Now we support 4 brands of elevator, KONE / Mitsubishi / Mitsubishi ELSGW / Hitachi / Schindler.

8.1. Elevator Device

Function List

Functions	Description
Building	Enter basic data such as add, edit, delete, search, etc. of the building.
Devices	Add, delete, export, search, enable, disable, restart the device, upgrade firmware, synchronize time, synchronize all data, modify IP address, modify communication password, modify RS485 address, modify fingerprint comparison threshold, and obtain device parameters of elevator control device, obtain personnel information, obtain event records and other related functional operations.
Readers	Viewing and editing operations of the readers.
Floors	Floor editing, remote release button, remote lock button, remote continuous release button, enable the day’s normally open time, disable the day’s normally open time operation.
Auxiliary Input	Auxiliary input view operation.
Event Type	Elevator control device related time type view operation.
Device Monitoring	Elevator control device for monitoring operation.
Real-Time Monitoring	View the real-time event content of the elevator control device, remotely release the button, and remotely lock the case operation.

8.1.1. Building

Function Description

Manage system building, set building related areas, number of floors, and floor rules, and be able to bind a third-party elevator control system to verify permissions for personnel or visitors to call elevator operations, etc.

Add Building

Preconditions for Normal Use of Function

The system sets the corresponding area and supports the selection area.

Function Usage Scenarios

It is necessary to use elevator control device to configure personnel permissions and call elevator operations.

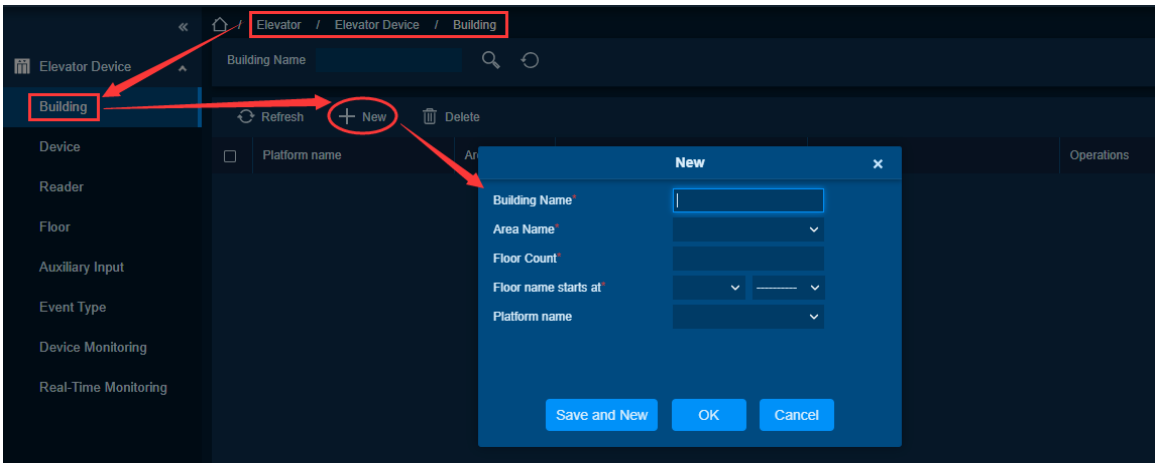
The elevator can be called remotely after using the integrated third-party elevator control system to verify the access authority of the personnel.

Feature Trigger Result

When add building, the floor will add the number of floors set by building and the corresponding floor information.

Steps:

- Click **[Elevator]** > **[Building]** > **[New]** on the Action Menu, the following interface will be shown:



Building Name: Add a name or title to the building.

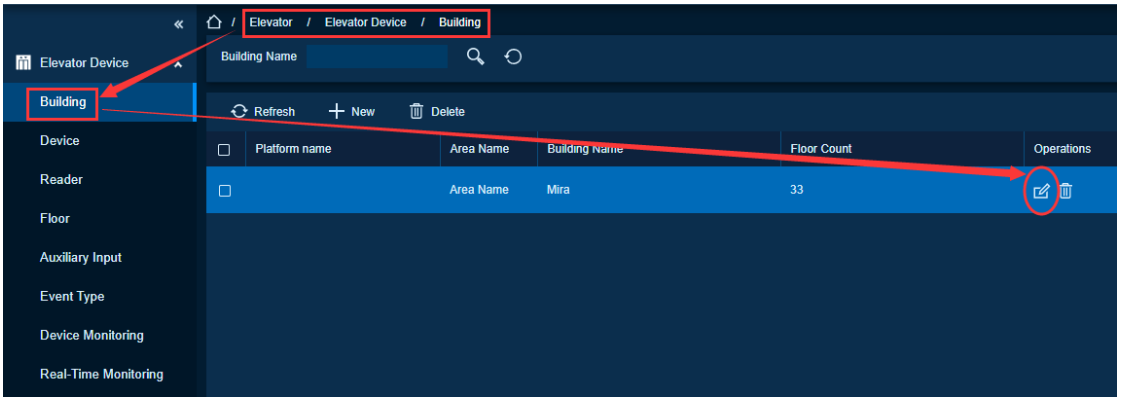
Area Name: Define the area of the building.

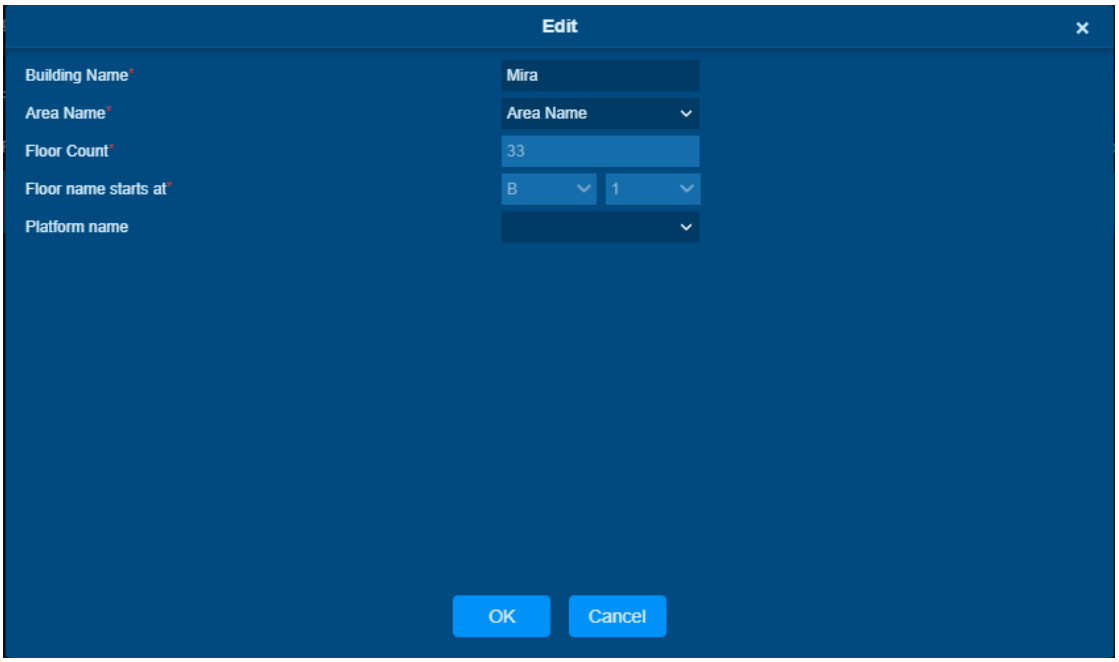
Floor Count: The number of floors added to the building.

Platform name: The third-party integration platform used by elevator control management

Edit Building

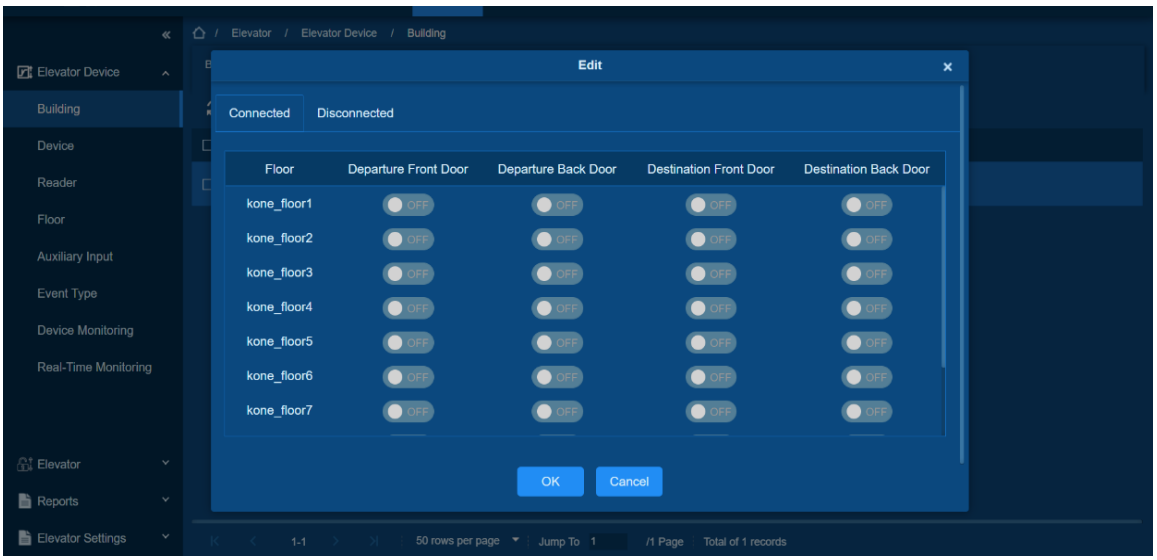
- Click **[Elevator] > [Building] > [Edit]** on the Action Menu, the following interface will be shown:





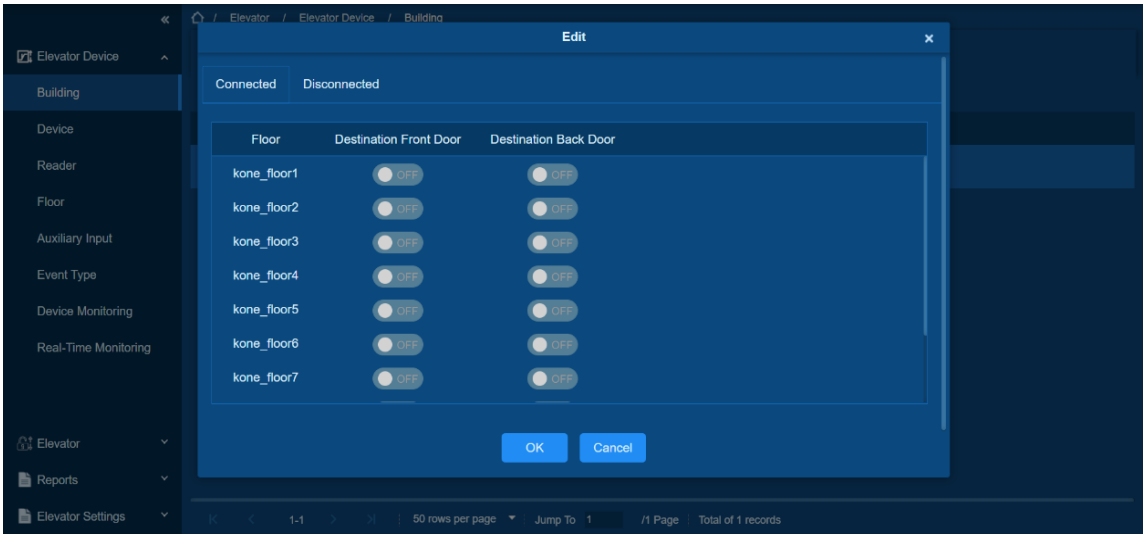
Set External Template

- Click **[Elevator] > [Building] > [External Template]** on the Action Menu, the set templates are divided into connected and disconnected modes. Each mode sets whether the front and back doors of the currently bound building's floor can be opened and closed.



Set Internal Template

- Click **[Elevator] > [Building] > [Internal Template]** on the Action Menu, the set templates are divided into connected and disconnected modes. Each mode sets whether the front and back doors of the currently bound elevator can be opened and closed.



Delete Building

Preconditions for Normal Use of Function

1. Successfully add building.
2. The building floor is not bound to elevator settings-external reader.
3. The building floor is not bound to elevator settings-internal reader.

Function Usage Scenarios

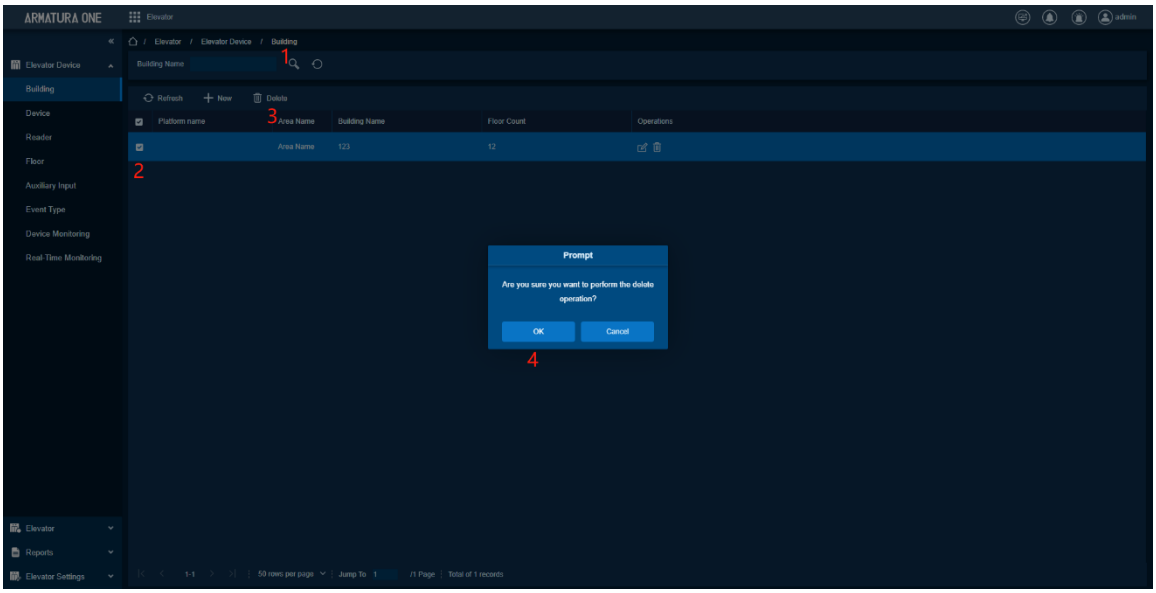
1. Wrong configuration of the number of floors.
2. Building is no longer used.

Feature Trigger Result

1. Delete building information.
2. Delete building corresponding floor information.

Steps:

- Select the Platform name and click **Delete**.



8.1.2. Device

Function Description

Manage elevator control device, support operations such as adding, deleting, setting elevator control device status, setting elevator control device parameters, obtaining elevator control device data, etc., paving the way for configuring personnel permissions and calling elevators

Add Device

Preconditions for Normal Use of Function

System and area information

Function Usage Scenarios

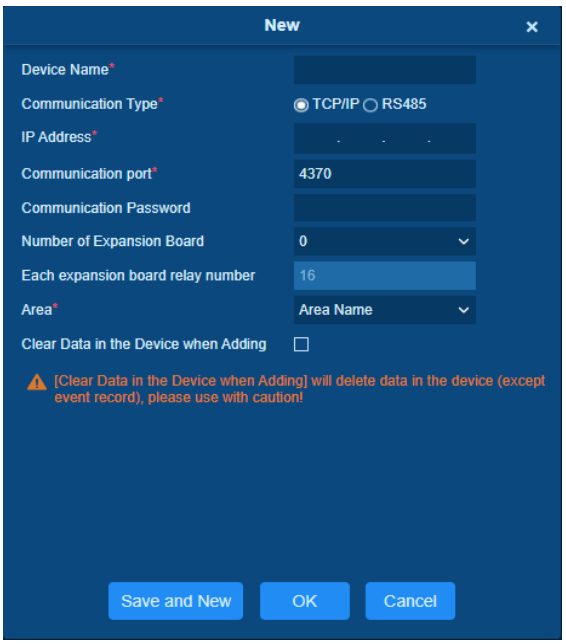
Personnel use elevator device to take the elevator.

Feature Trigger Result

Add elevator control device information, able to operate the device.

Steps:

- Click **[Elevator] > [Device] > [New]** on the Action Menu, the following interface will be shown:



IP Address: Enter the IP Address of the elevator device.

Communication port: The default communication port is 4370.

Communication Password: The maximum length is 6 with numbers or letters. The initialized device's communication password is blank.

✍**Note:**

You do not need to input this field if it is a new factory device or just after the initialization.

Number of expansion board: The expansion board number of elevator device controlling.

Each expansion board relay number: Each expansion board has 16 relays.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-Time Monitoring.

Clear Data in the Device when Adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

Extended Device Parameters: Includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity etc.

- After editing, click **[OK]**, and the system will start to connect the current device.
- If successfully connected, it will read the corresponding extended parameters of the device and save.

✍**Note:**

When deleting a new device, the software will clear all user information, time zones, holidays, and elevator access levels settings from the device, except the events record (unless the information in the device is unusable, or it is recommended not to delete the device in used to avoid loss of information).

Elevator Controller Settings:

TCP/ IP Communication Requirements

Support and enable TCP/ IP communication, directly connect device to the PC or connect to the local network, query IP address and other information of the device.

Delete Device

Preconditions for Normal Use of Function

- The elevator control device is not used.
- The elevator control device is not bound to other functions.

Function Usage Scenarios

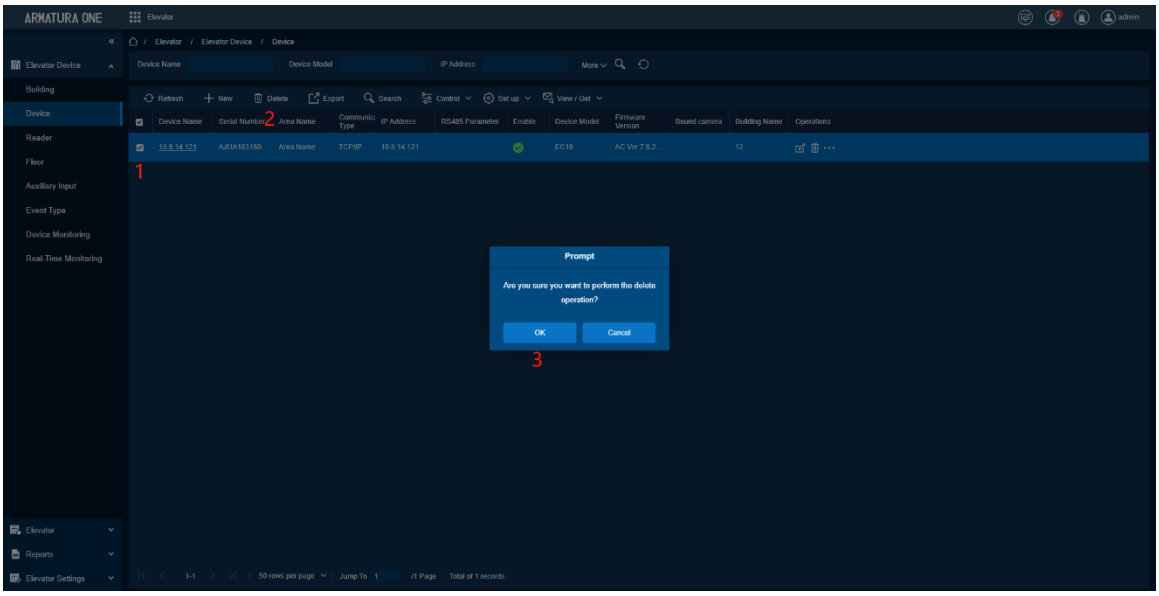
- Device damaged.
- No need to use the device.

Feature Trigger Result

Clear the current elevator control device data.

Steps:

- Select the corresponding device, click **[Delete]**, a confirmation box pops up, click **[OK].**



Export Device

Preconditions for Normal Use of Function

Not yet.

Function Usage Scenarios

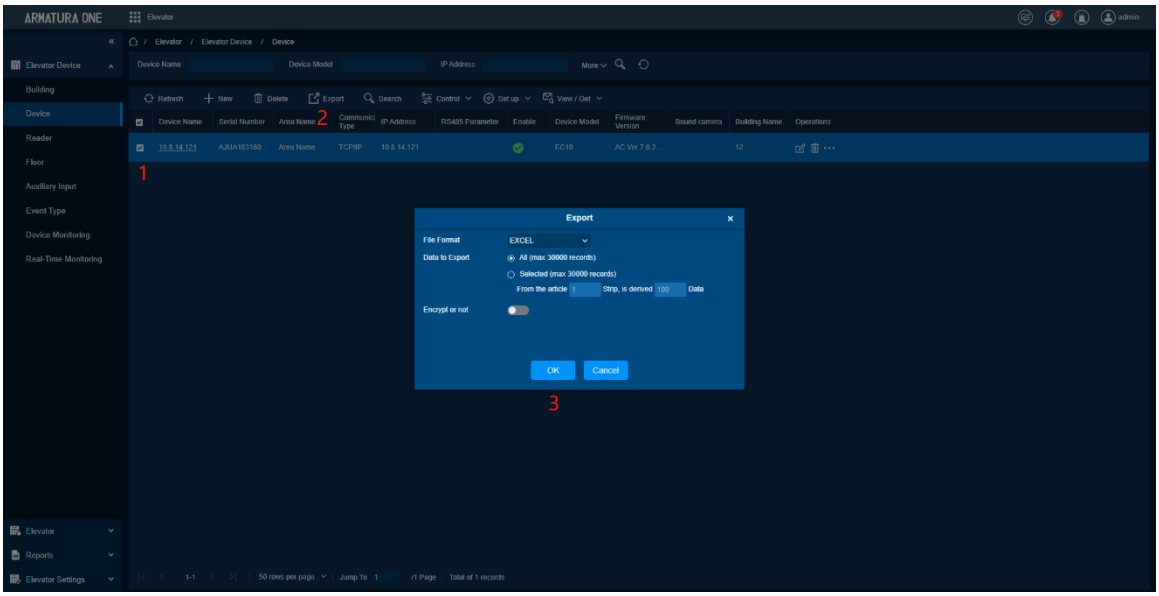
Export device data for viewing.

Feature Trigger Result

Export the data as an Excel table to the local.

Steps:

- Select data (optional), click **[Export]**, select export conditions, and click **[OK].**



Search Device

Preconditions for Normal Use of Functions

Not yet.

Function Usage Scenarios

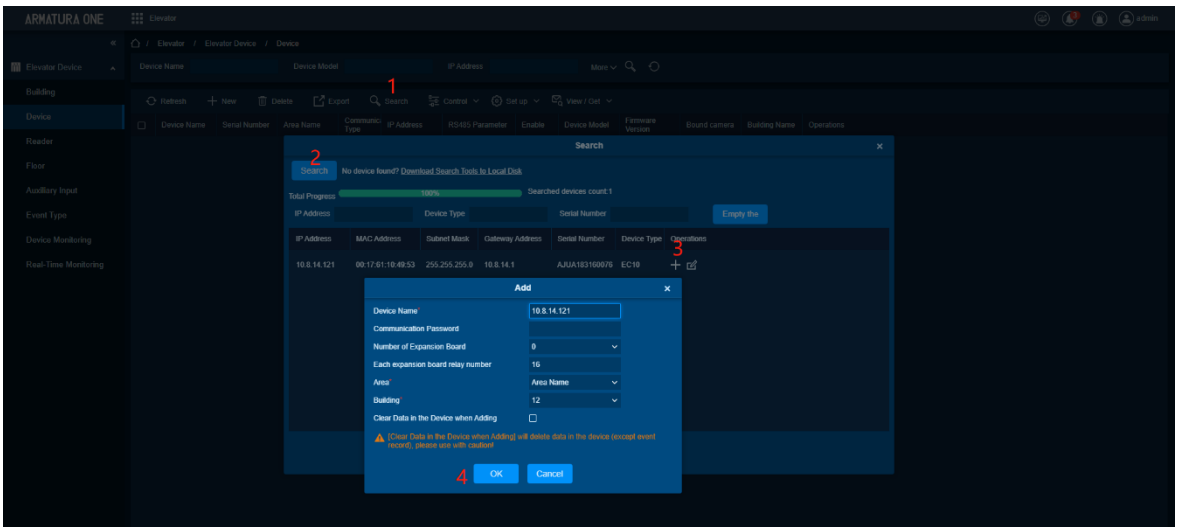
View current network elevator control device and add elevator control device.

Feature Trigger Result

Add elevator control device to the system.

Steps:

- Click the search device button, click **[Search]**, click **[Add]** button, modify the corresponding device parameters, click **[OK]**. Click **[Confirm]** on the pop-up window.



Control-Enable

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

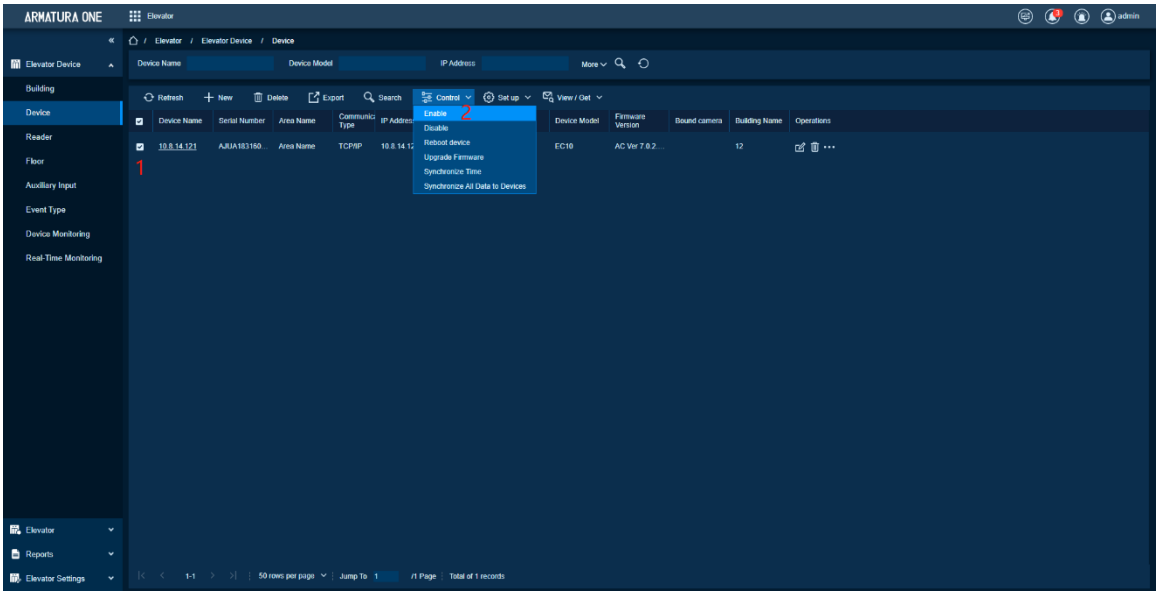
Enable elevator control device.

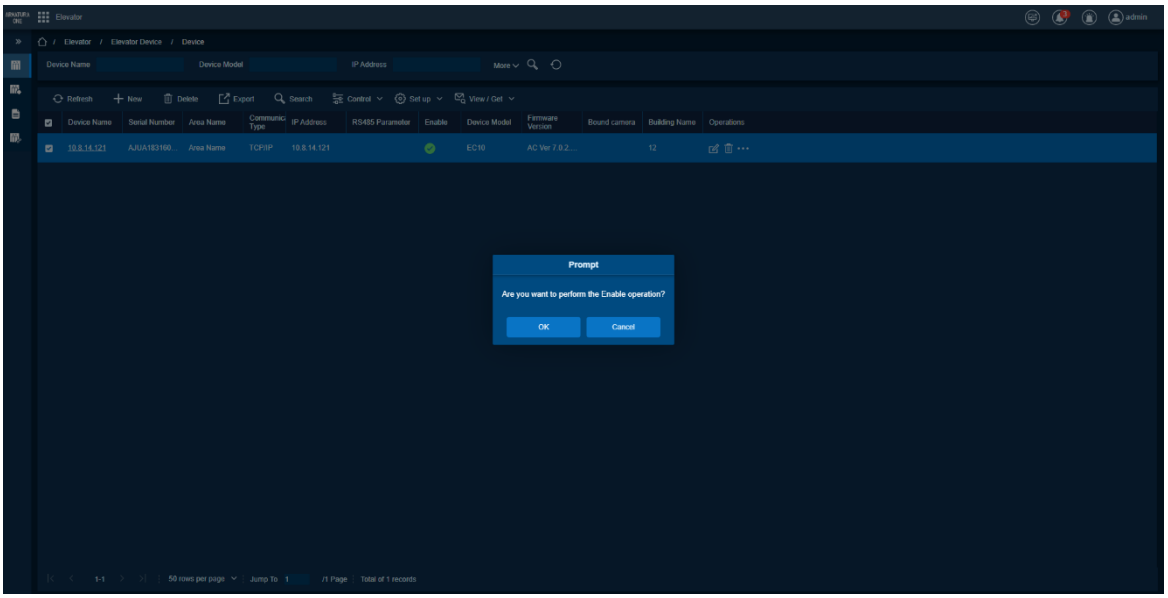
Feature Trigger Result

Elevator control device can be used normally.

Steps:

Select the Elevator Control device, click **[Enable]** button. On the pop-up window, click **[OK].**





Control-Disable

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

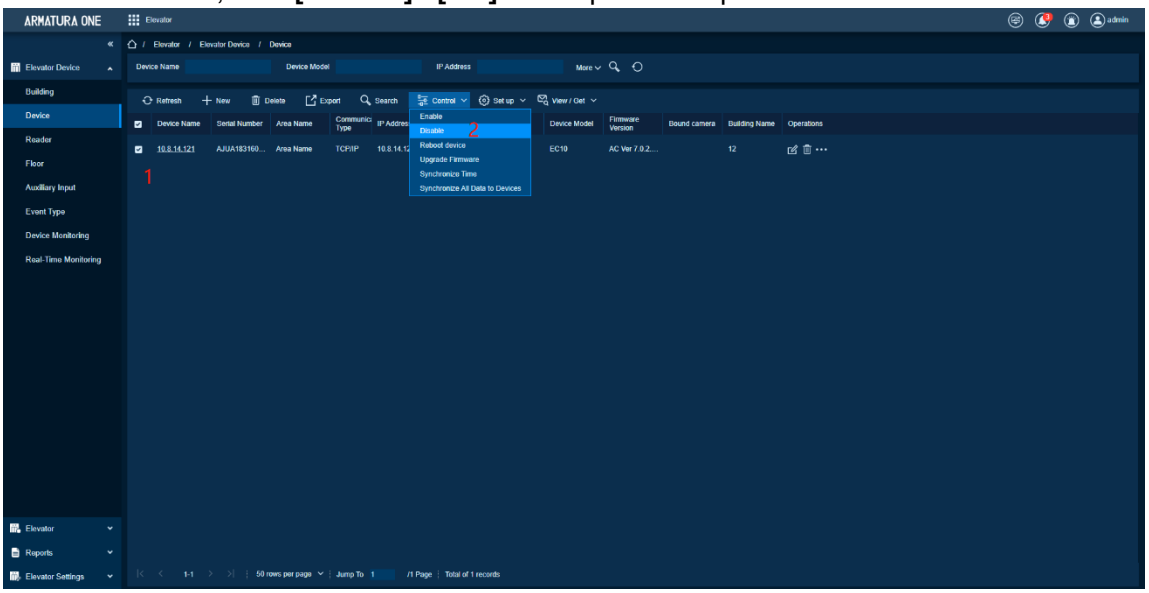
Disable the Elevator Control Device and do not use it.

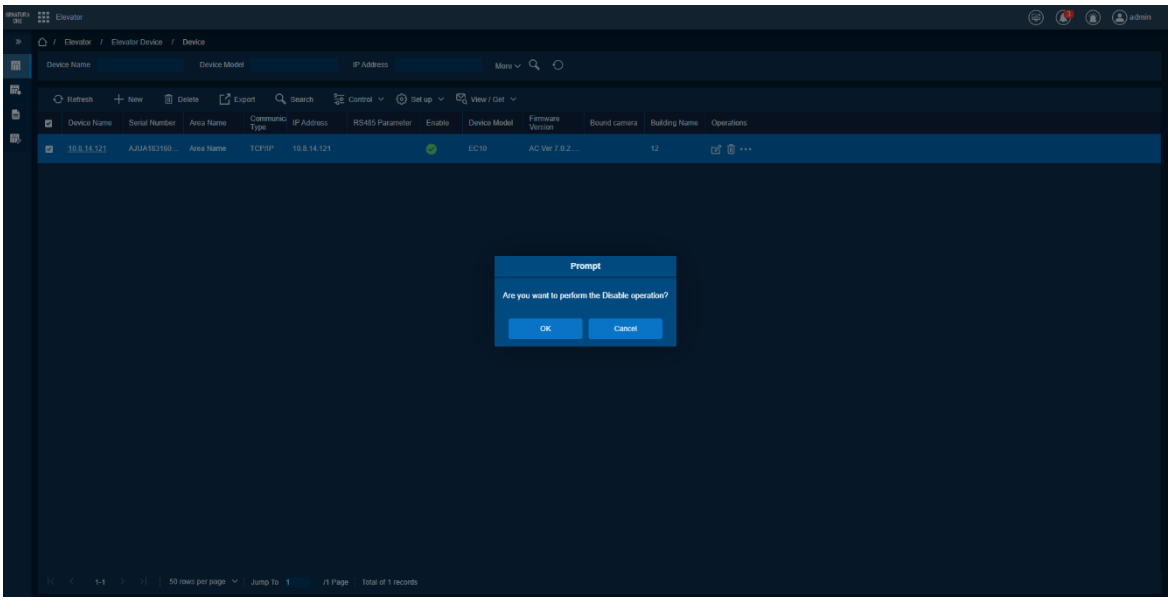
Feature Trigger Result

Elevator Control Device is set to disabled state.

Steps:

Select the device, click **[Disable]> [OK]** to complete the operation.





Control-Restart Device

Preconditions for Normal Use of Function

The Elevator Control Device communicates normally and is added to the system.

Function Usage Scenarios

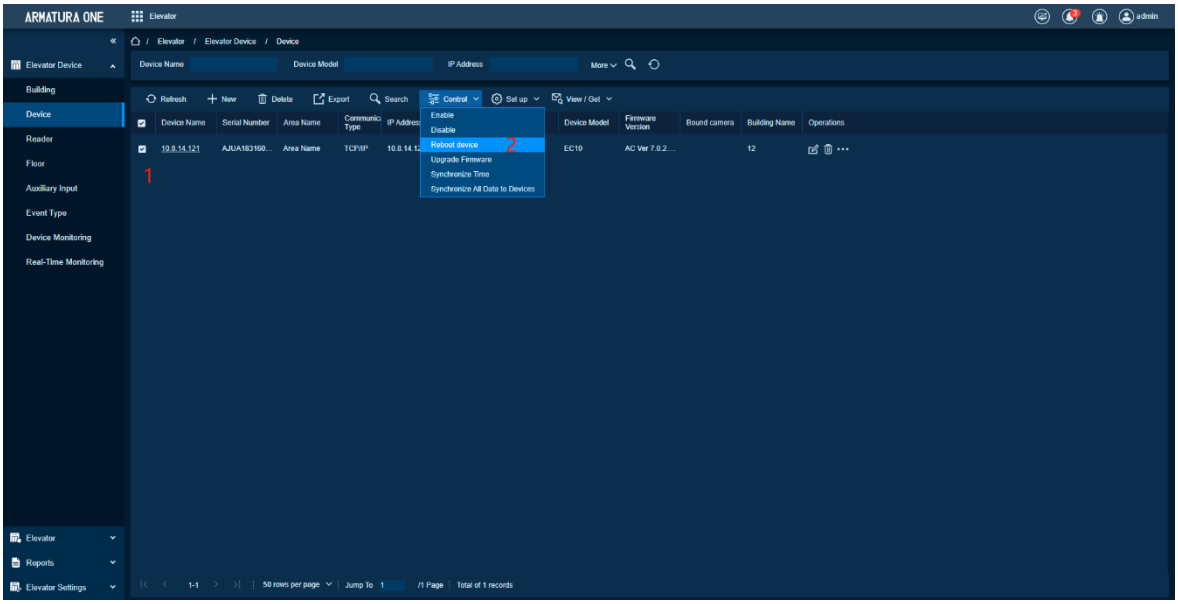
Elevator Control Device needs to be restarted.

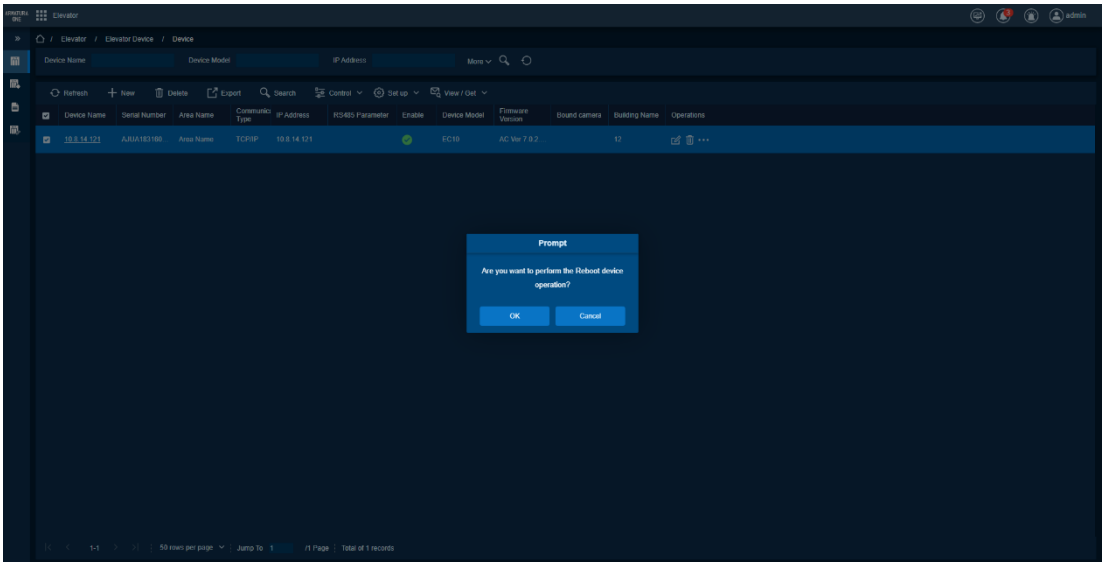
Feature Trigger Result

Elevator control device restarts.

Steps:

Select the device, click **[Reboot Device]**. On the pop-up window, click **[OK]** to complete the operation.





Control-Upgrade Firmware

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Elevator Control Device needs to upgrade the system.

Function Usage Scenarios

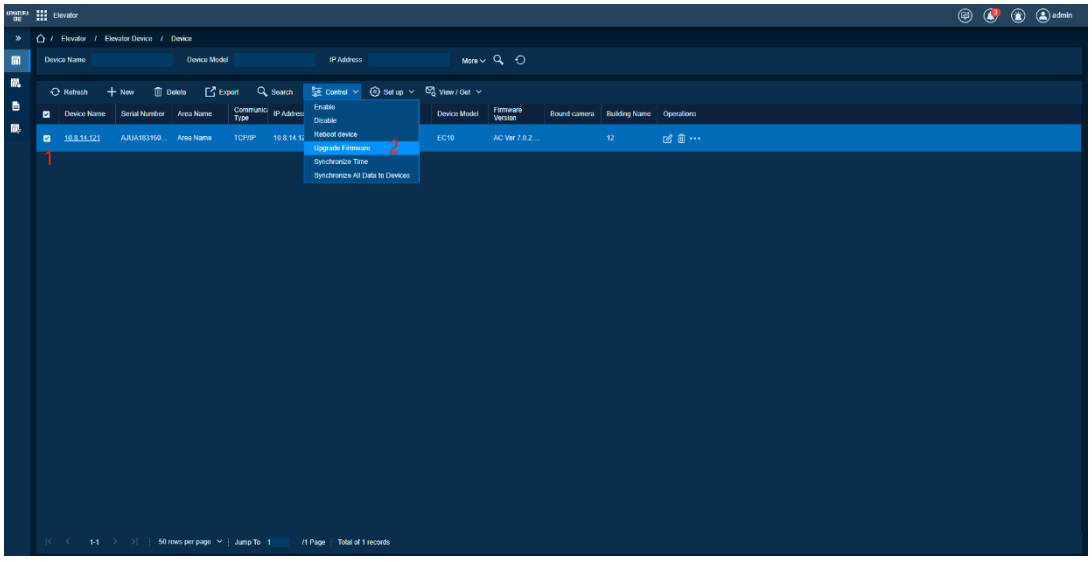
Elevator Control Device firmware needs to be upgraded.

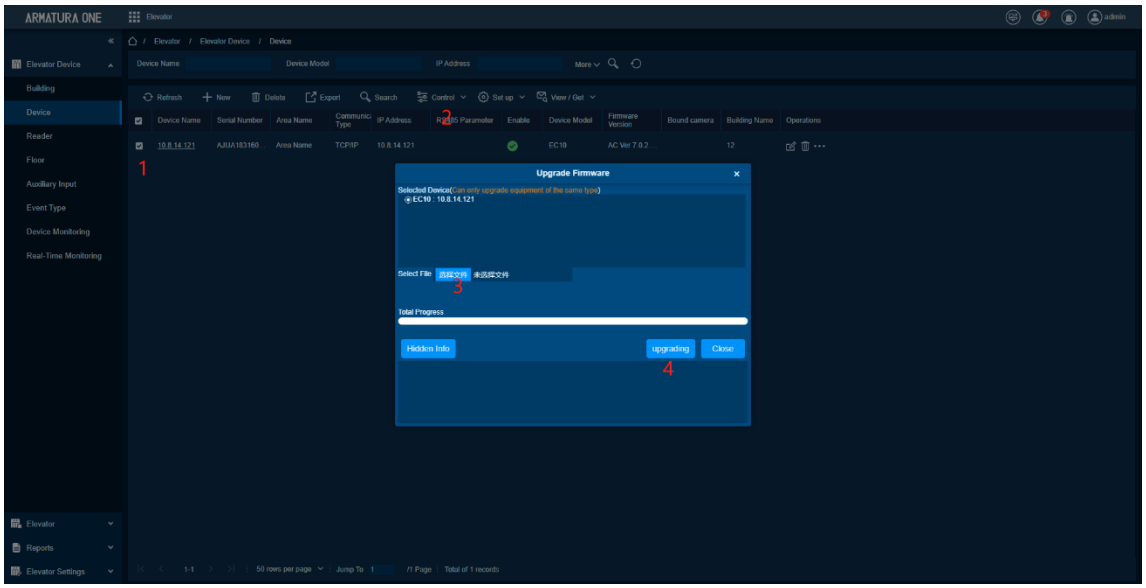
Feature Trigger Result

Update and replace the firmware version of the Elevator Control Device.

Steps:

- Select the device, click **[Upgrade Firmware].**
- On the pop-up window, select the upgrade firmware file, click **[Upgrading]**. Check the progress bar, until the operation completes.





Control-Synchronize Time

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

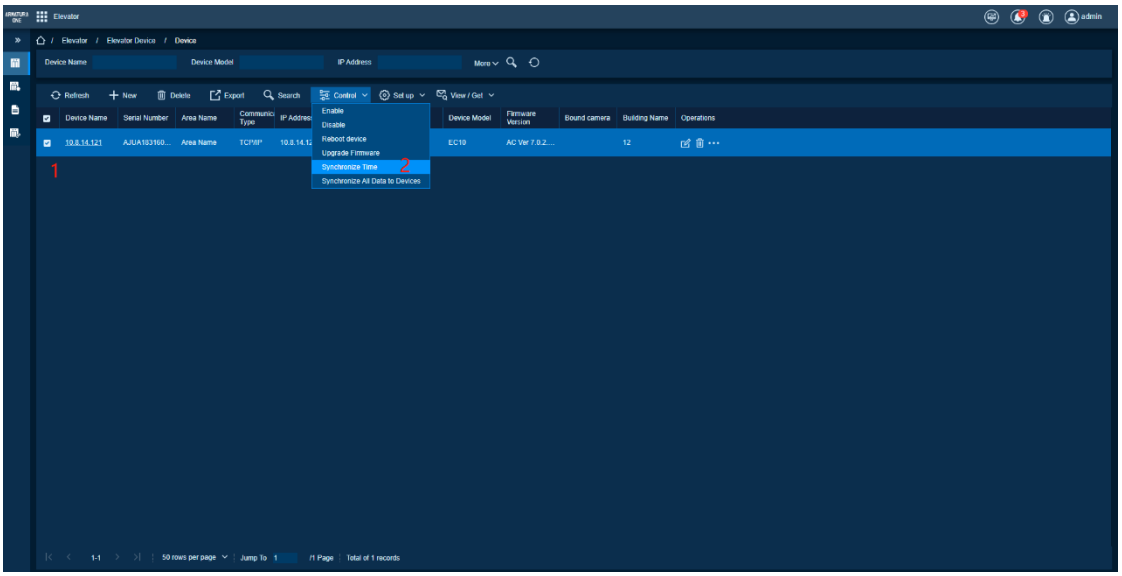
Function Usage Scenarios

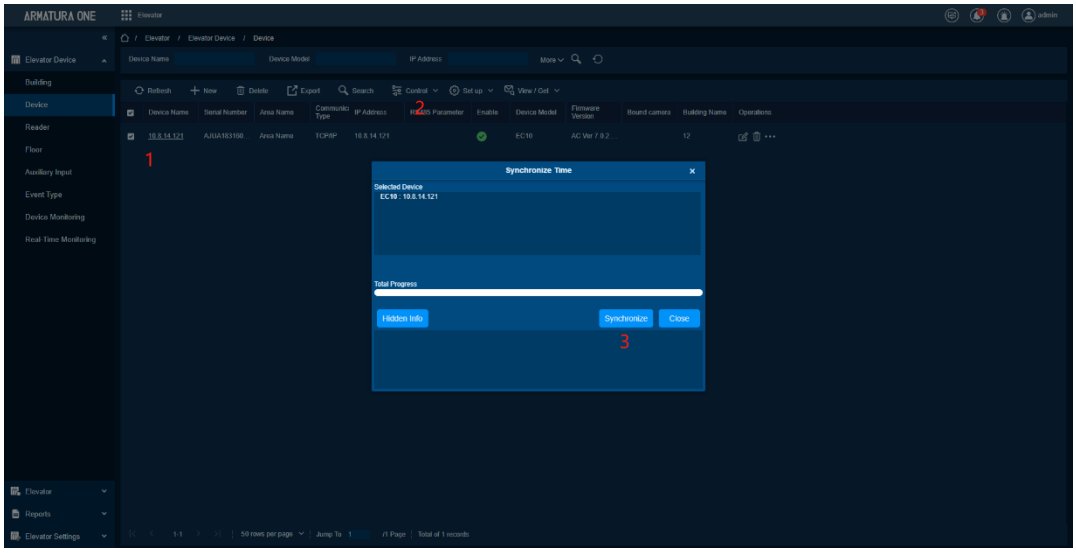
Elevator Control Device time does not match the current system time.

Feature Trigger Result

Elevator Control Device time is modified to be consistent with the current system time.

Steps:





Control-Synchronize All Data

Preconditions for Normal Use of Function

The Elevator Control Device communicates normally and is added to the system.

Function Usage Scenarios

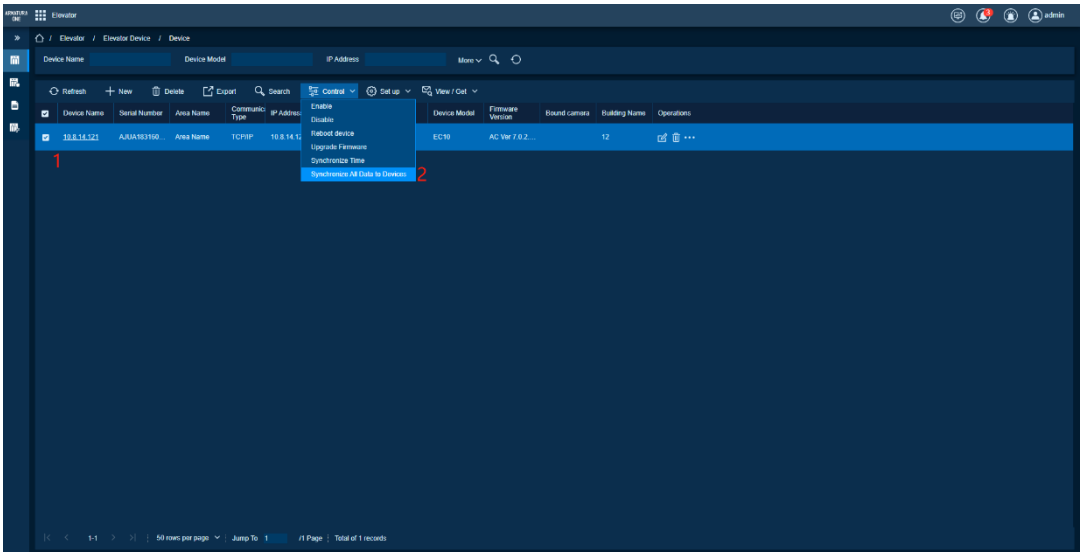
Set the data currently matched with the Elevator Control Device and send it to the Elevator Control Device.

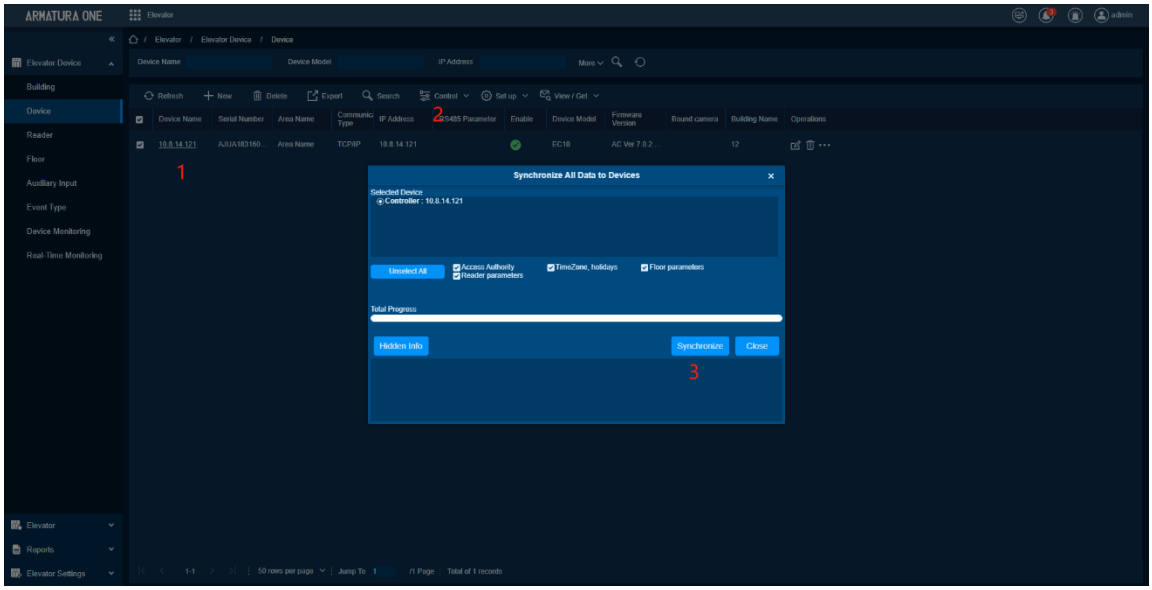
Feature Trigger Result

Send the personnel information in the elevator control authority to the Elevator Control Device.

Steps:

- Select the Elevator Control Device, click the control drop-down box to pop up.
- Select Synchronize All Data to The Device, check the data information that needs to be synchronized in the pop-up box.
- Click **[Synchronize All Data Devices]** button and wait until the operation is completed.





Settings-Modify IP address

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

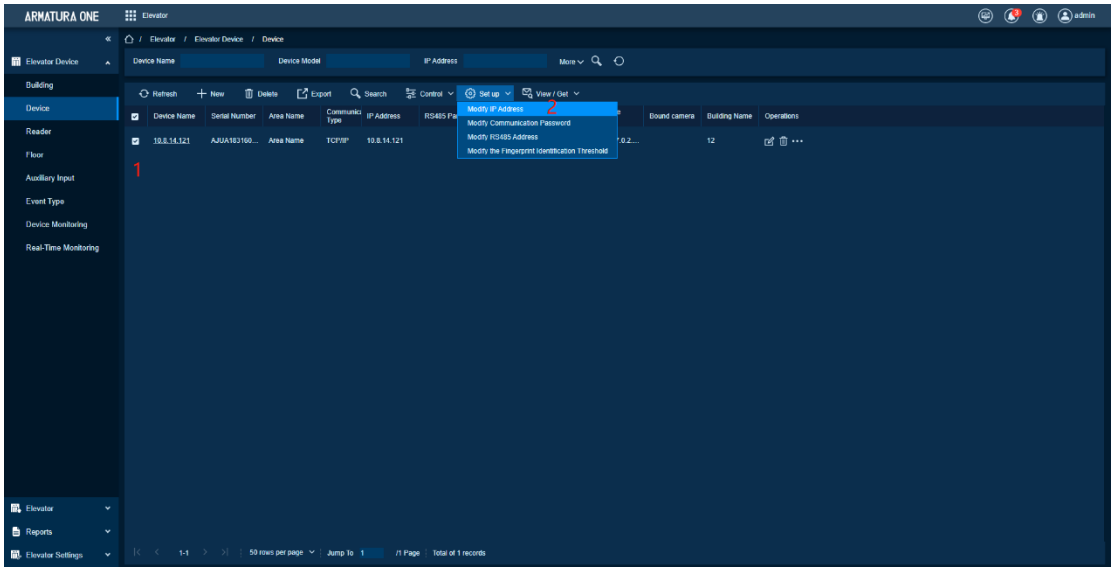
The current elevator control device IP conflicts or some reasons need to modify the elevator control device IP.

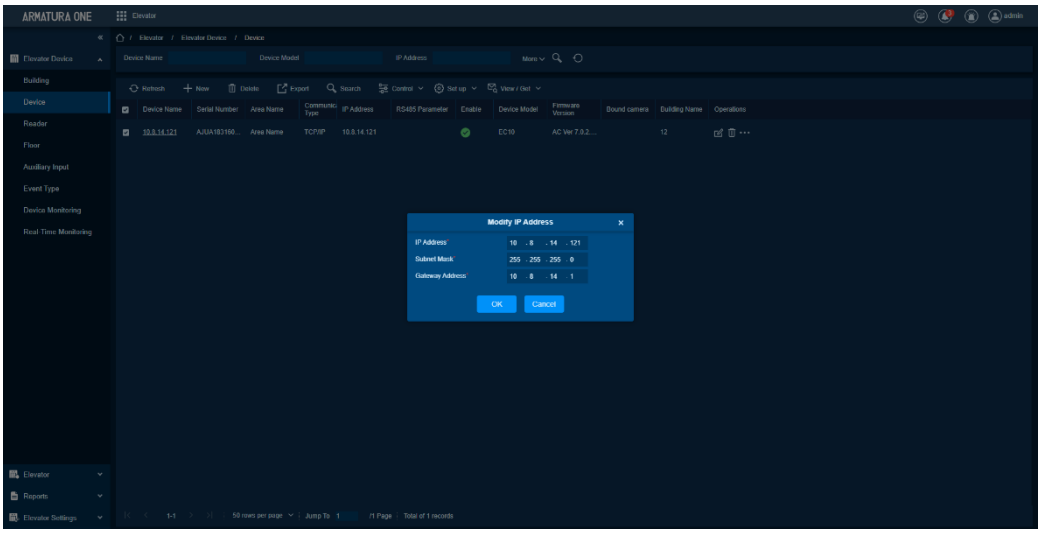
Feature Trigger Result

Elevator Control Device IP changed.

Steps:

- Select the Elevator Control Device, click the **[Modify IP Address]** button, the IP modification window will pop up to modify the parameters such as IP and gateway, click **[OK]** until the operation is completed.





Settings-Modify Communication Password

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

Forbid other systems or other device to operate the Elevator Control Device, and the communication with the

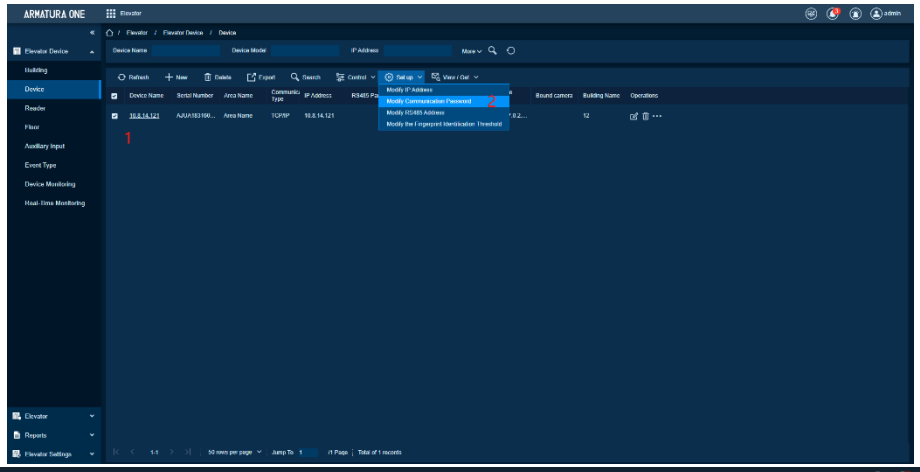
device requires password verification.

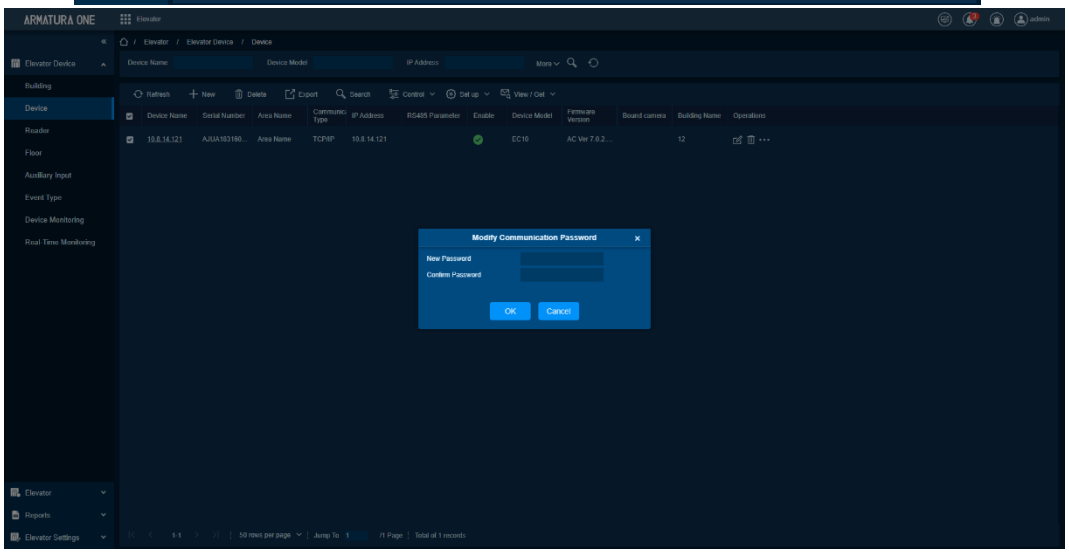
Feature Trigger Result

Set the communication password for the Elevator Control Device. When communicating with the Elevator Control Device, the normal communication can be established only after the password verification is passed.

Steps:

- Select the Elevator Control Device.
- Click **[Modify Communication Password]** button.
- On the pop-up window, enter the new password and confirm the password (the two passwords need to be consistent).
- Click **[OK].**





Settings-Modify RS485 Address

Preconditions for Normal Use of Function

The Elevator Control Device communicates normally and is added to the system.

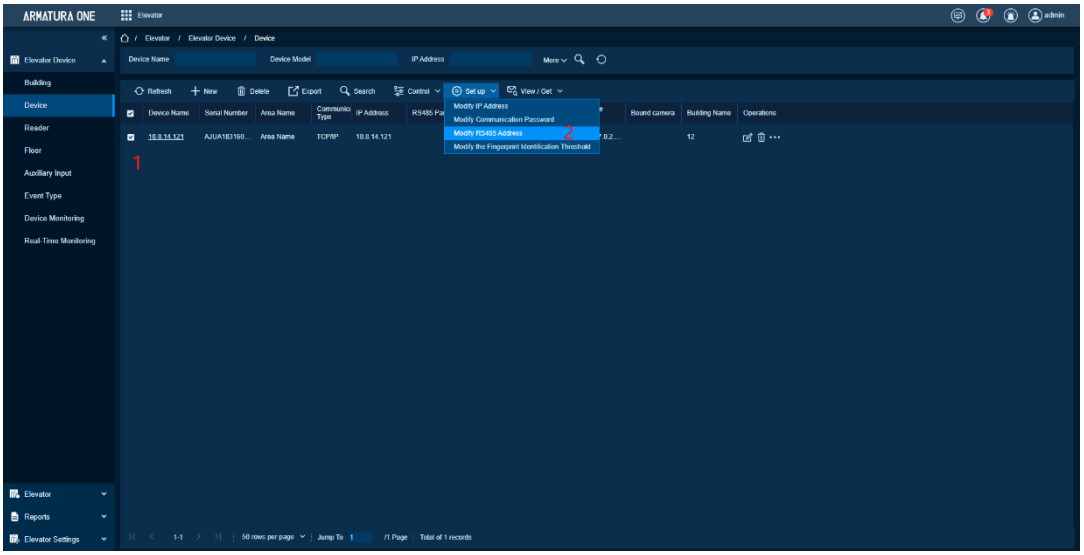
Function Usage Scenarios

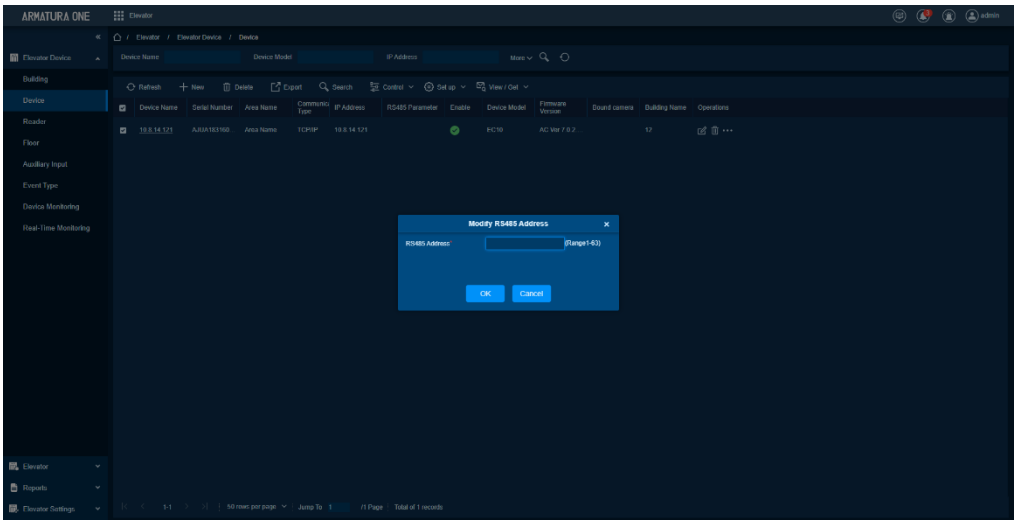
RS485 reader dial code changed, generally do not need to be configured.

Feature Trigger Result

Modification of communication between Elevator Control Device and RS485 Reader Device.

Steps:





Settings-Modify Fingerprint Comparison Threshold

Preconditions for Normal Use of Function

- The Elevator Control Device communicates normally and is added to the system.
- Elevator Control Device supports fingerprint reading and verification, etc.

Function Usage Scenarios

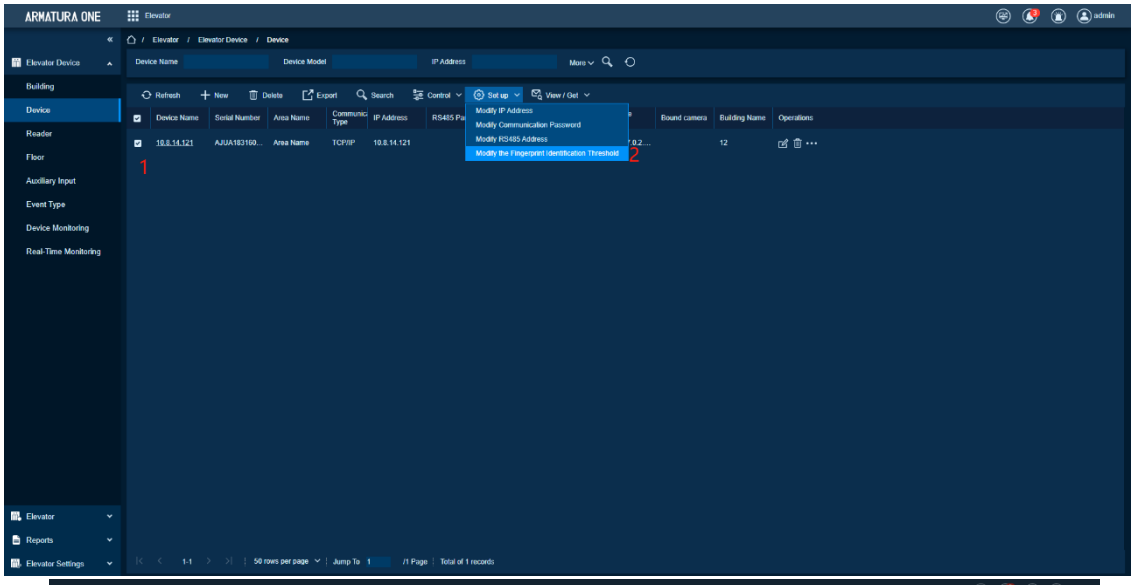
Modify the threshold level of verification fingerprint comparison when verifying elevator control authority.

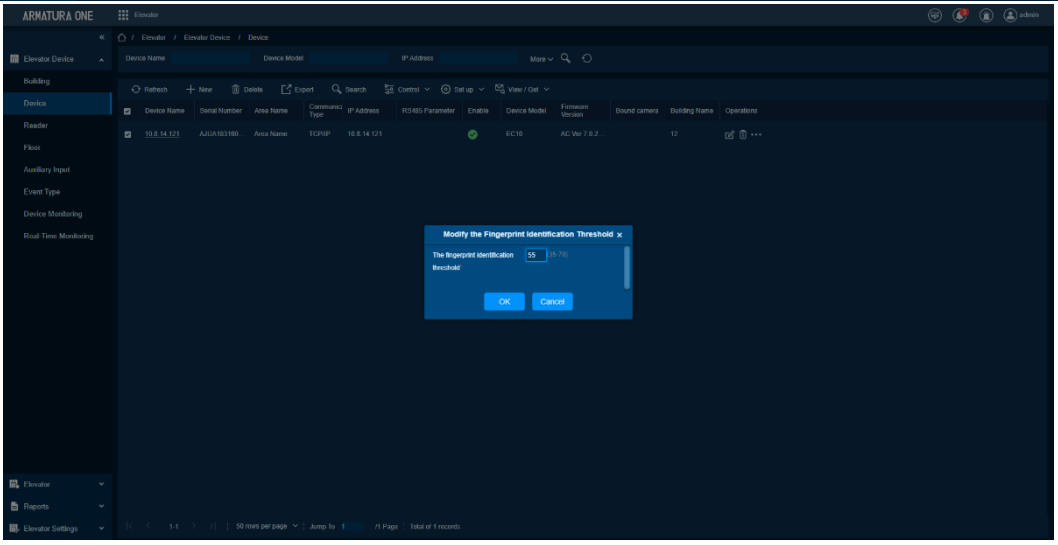
Feature Trigger Result

Modify the fingerprint comparison threshold of the elevator control device.

Steps:

- Select the Elevator Control Device.
- Click **[Modify the Fingerprint Identification Threshold]** button.
- On the pop-up window, click **[OK]** and wait until the operation is completed.





View and Get-Get Device Parameters

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

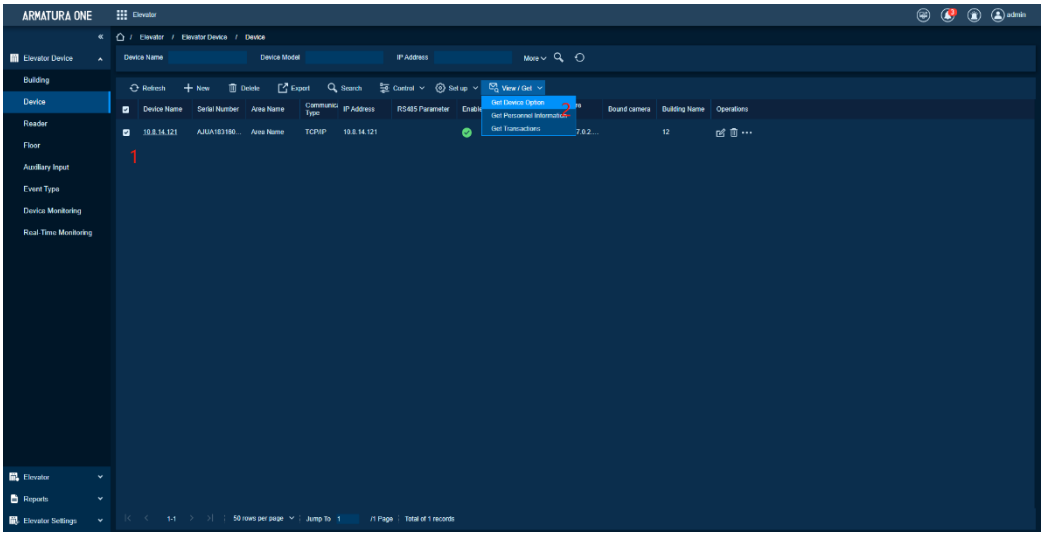
The parameters of the elevator control device do not match the current system, and the current elevator control device parameters in the system need to be synchronized with the elevator control device.

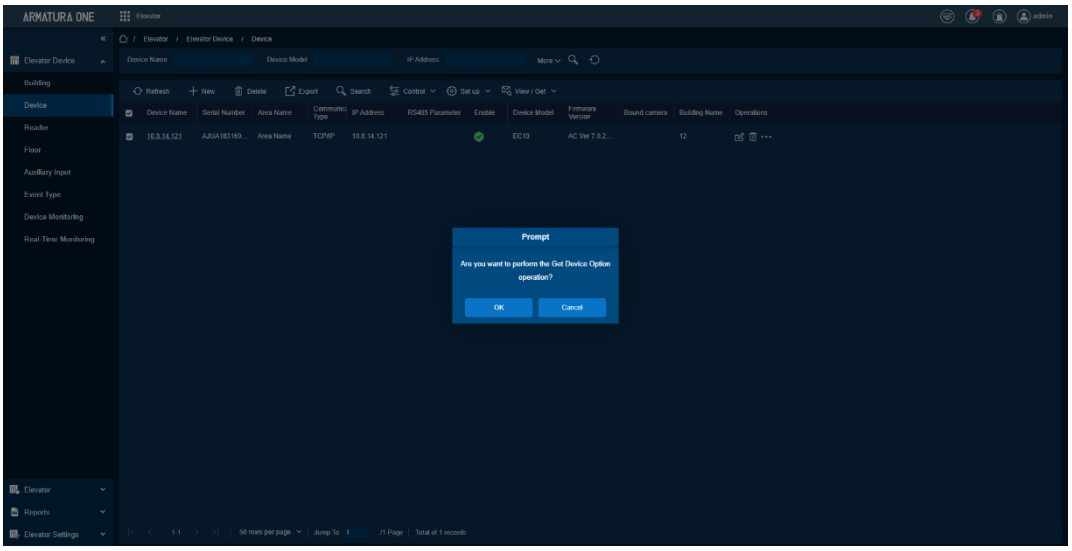
Feature Trigger Result

The current system elevator control device parameters are modified to be consistent with the Elevator Control Device.

Steps:

- Select the Elevator Control Device.
- Click the button **[Get Device Option]**.
- On the pop-up window, click **[OK]** to complete the operation.





View and Get-Get Personnel Information

Preconditions for Normal Use of Function

The Elevator Control Device communicates normally and is added to the system.

Function Usage Scenarios

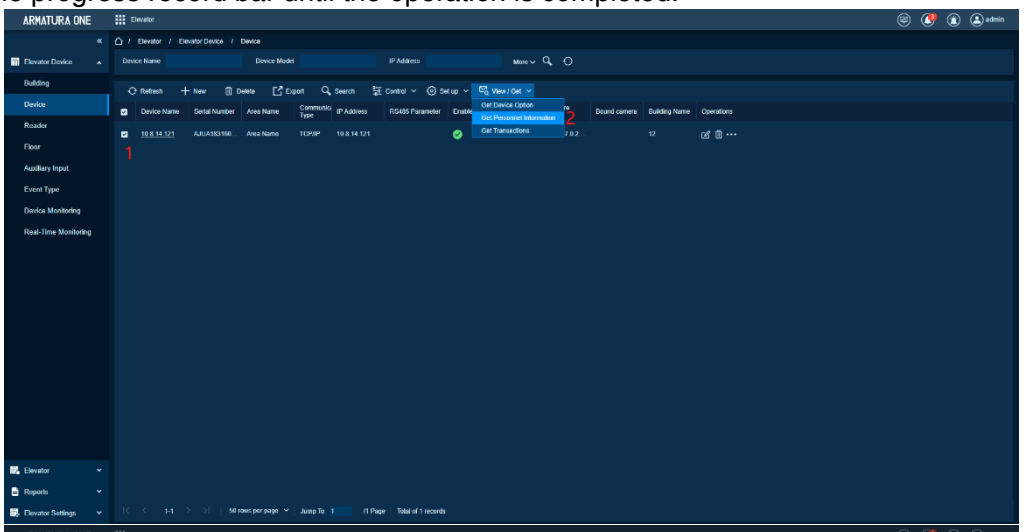
Synchronize the personnel information on the Elevator Control Device to the system.

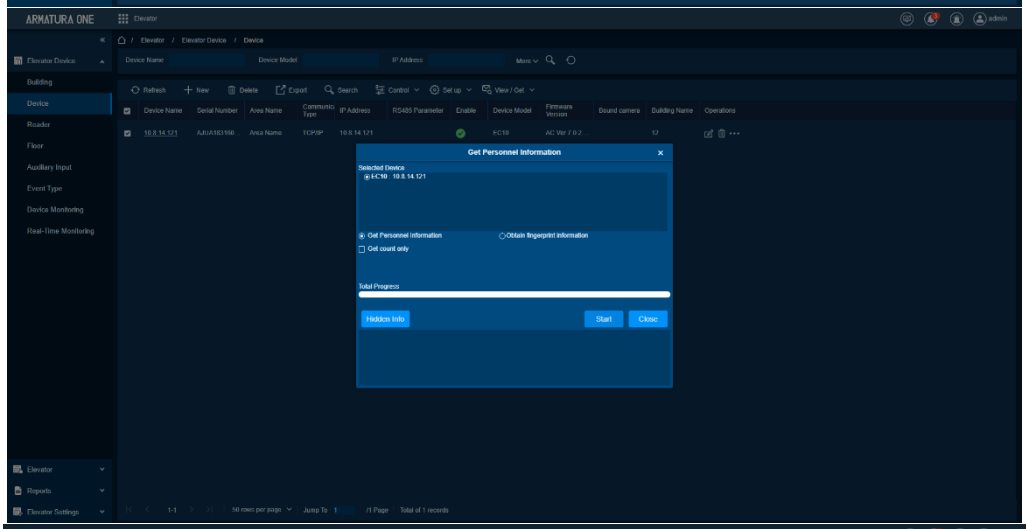
Feature Trigger Result

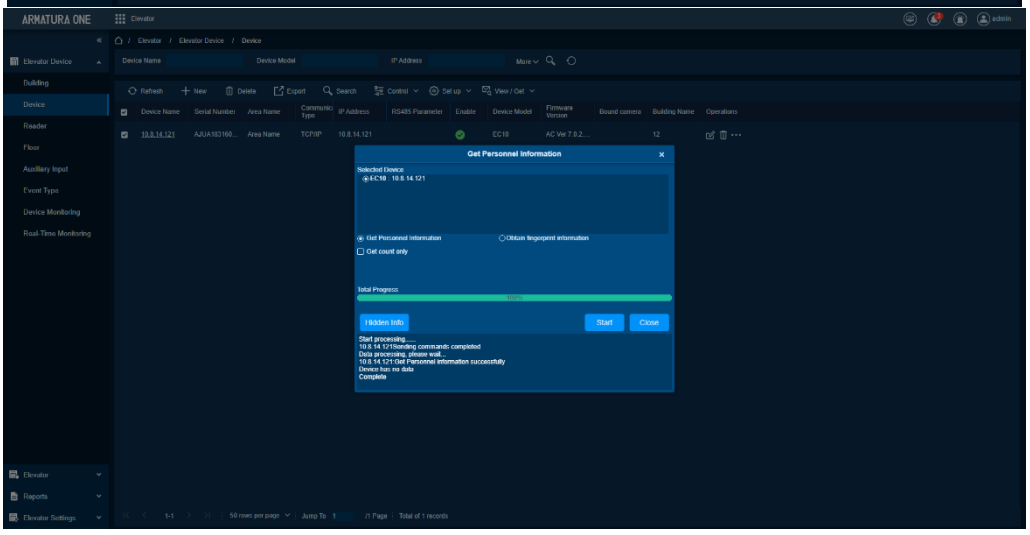
When the elevator control device has personnel information that does not match the current system, the system will synchronize the personnel information on the elevator control device to the system.

Steps:

- Select the Elevator Control Device, click **[Get Personnel Information]** button.
- On the pop-up window, click Get Personnel Information.
- Click Start button to start the execution process.
- Check the progress record bar until the operation is completed.







View and Get-Get Event Record

Preconditions for Normal Use of Function

The elevator control device communicates normally and is added to the system.

Function Usage Scenarios

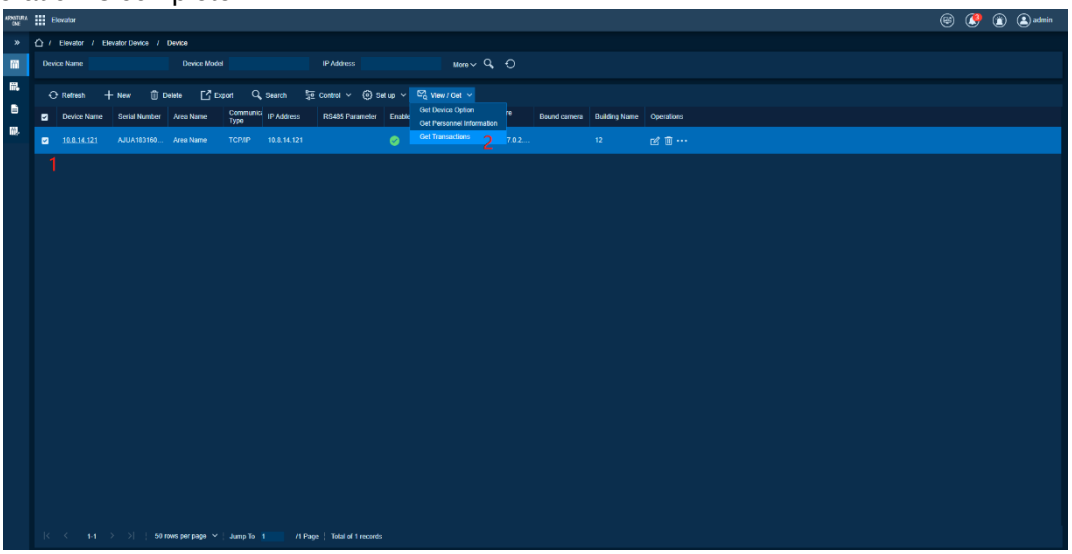
The system needs to obtain all event data of the Elevator Control Device.

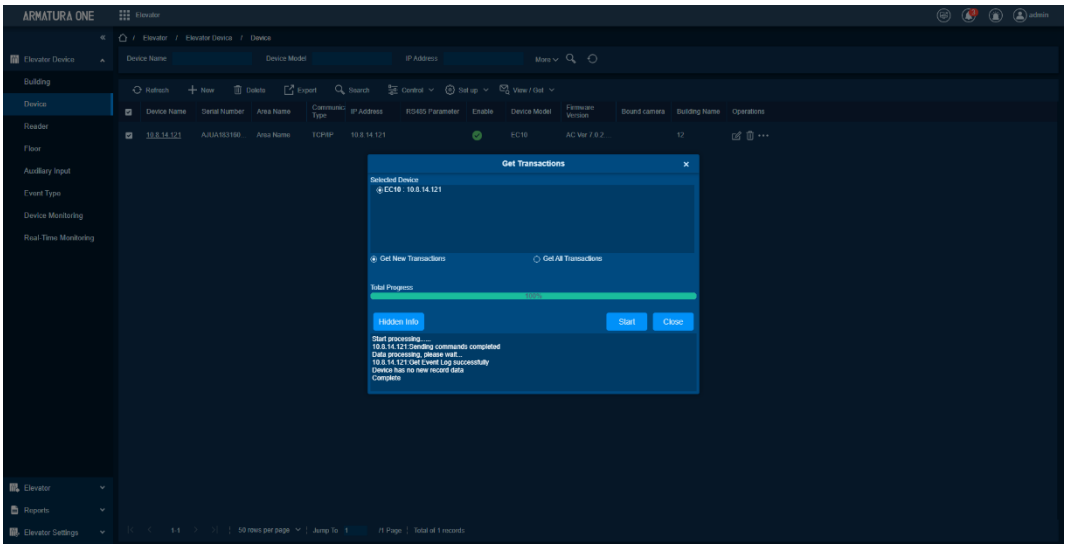
Feature Trigger Result

Elevator control event record report to generate event records of current elevator control device.

Steps:

- Select the Elevator Control device.
- Click the Get Event button.
- On the pop-up window will pop up to choose to get a new record or all records, click the Start button, and the operation is complete.





8.1.3. Reader

Function Description

Each elevator device has a reader, and the reader information can be set.

Edit

Preconditions for Normal Use of Function

The system has successfully added elevator control devices, and each elevator control device will automatically generate the default information of the reader.

Function Usage Scenarios

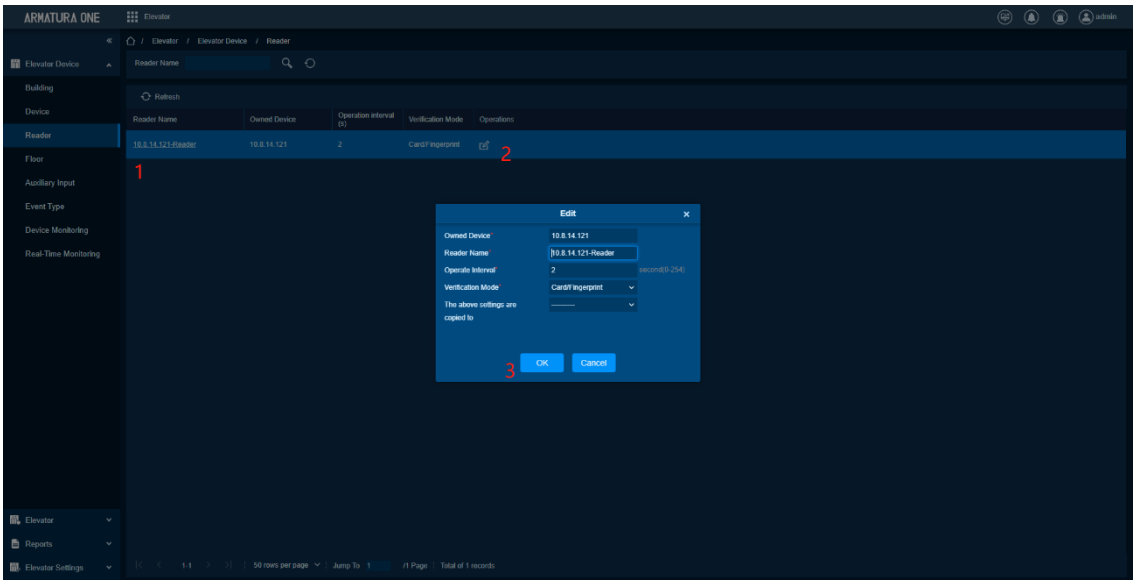
Need to modify the reader operation interval or verification method.

Feature Trigger Result

Modify the reader operation interval and verification method of elevator control device.

Steps:

- Click **[Elevator Device] > [Reader],** select a reader name in the reader list.



Fields are as follows: -

Owned Device: It is not editable.

Reader Name: The default format is “Device Name - Reader”, it is editable within 30 characters.

Operate Interval: The interval between two verifications. The default value is 2 seconds; the range is 0 to 254 seconds.

Verification Mode: The default setting is “Card or Fingerprint”. The Wiegand reader supports “Only Card”, “Only Password”, “Card or Password”, “Card and Password”, “Card or Fingerprint”. The RS485 reader supports “Card or Fingerprint”. Make sure the reader has a keyboard when the verification mode is “Card

and Password".

The above Settings Are Copied to:

All Readers of All Devices: Apply the above settings to all readers within the current user's level.

Click **[OK]** to save and exit.

8.1.4. Floor

Function Description

The floor data of the building information added by the system corresponds to the floor information of the elevator control device bound to the building, and the correspond floor button of the elevator control device can be remotely operated to release or open.

Edit

Preconditions for Normal Use of Function

The system adds building data and the floor data in building is set correctly.

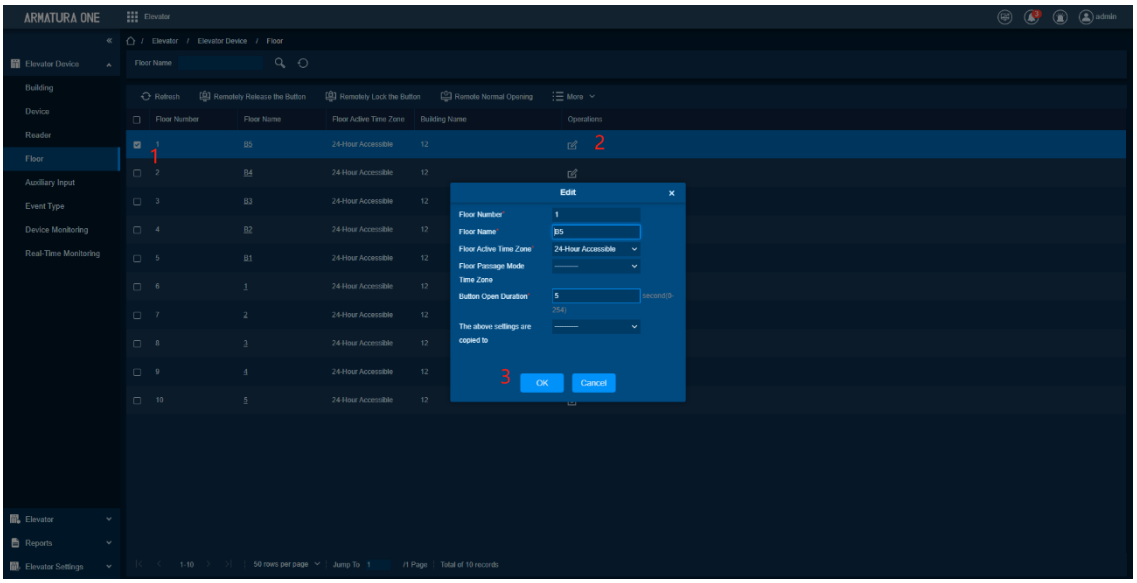
Function Usage Scenarios

Modify the corresponding default parameters of the floor, floor name, time, operation interval, etc.

Feature Trigger Result

Modify the relevant parameter information of the corresponding floor.

Steps:



Fields are as follows:

Floor Number: The system automatically numbered according to the number of relays.

Floor Name: The default setting is "Device Name- Floor Number"; it is editable within 30 characters.

Floor Active Time Zone: Description is required.

Floor Passage Mode Time Zone: The default setting is Null. The Floor Active Time Zones that are initialized or newly added by users will be displayed here so that users can select a period. When editing a floor, the Floor Active Time Zone must be specified. The key for closing the related floor can be released continuously only after the effective periods of this floor are specified. Floor Passage Mode Time Zone takes effect only within the floor effective period. It is recommended that the floor continuous release period be included in the floor effective period.

Button Open Duration: It is used to control the time to press floor button after verification. The default value is 5 seconds; the range is 0 to 254 seconds.

The above settings are copied to:

All Floors of Current Device: To apply the above settings to all floors of the current elevator device.

All Floors of all Devices: To apply the above settings to all floors within the current user's level.

Remote Release Button

Preconditions for Normal Use of Function

- The current floor corresponding to the building has bound elevator control device.
- The bound elevator control device can communicate normally.

Function Usage Scenarios

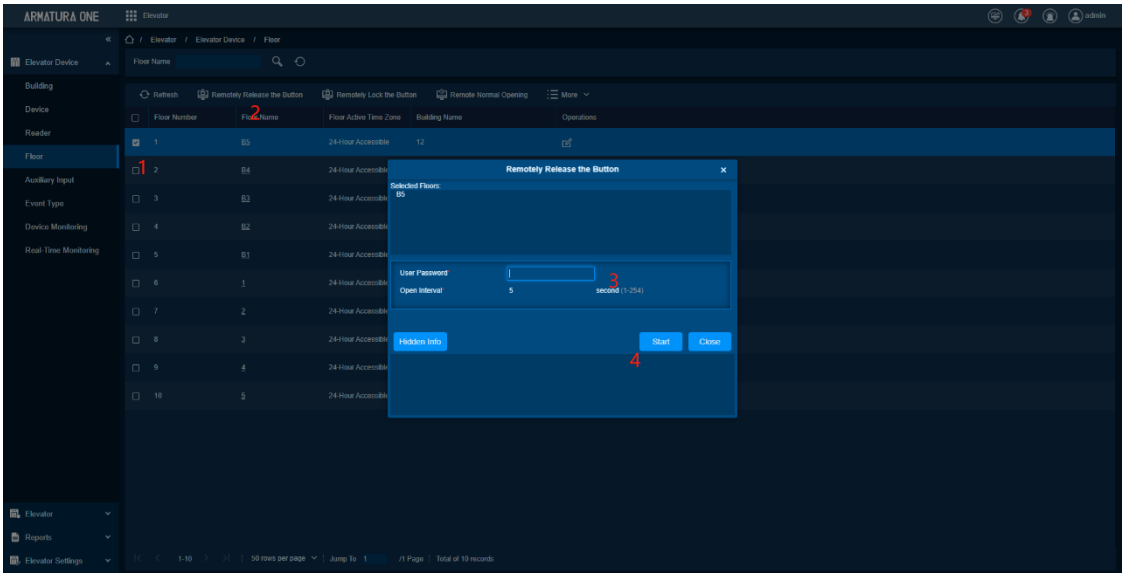
Release the button authority of the current floor of the elevator control device bound to the current building and allow others to perform the button operation of lighting the floor within the specified time.

Feature Trigger Result

Corresponding to the current floor of the elevator control device, the buttons are released for a certain period, and the personnel can perform button operations within the specified time.

Steps:

- Click **[Elevator Device] > [Floor] > [Remotely Release the Button].**
- This function is to remotely release the floorboard permission of elevator device.
- Confirm release after entering the password.



User Password: Enter the system password.

Open Interval: Set the remote release interval.

✍**Note:**

Only the floor from the device supports this operation.

Remote Lock Button

Preconditions for Normal Use of Function

- The current floor corresponding to the building has bound elevator control device.
- The bound elevator control device can communicate normally.

Function Usage Scenarios

Lock the button permissions of the current floor of the elevator control device bound to the current building and prohibit others from performing the button operation to light the floor.

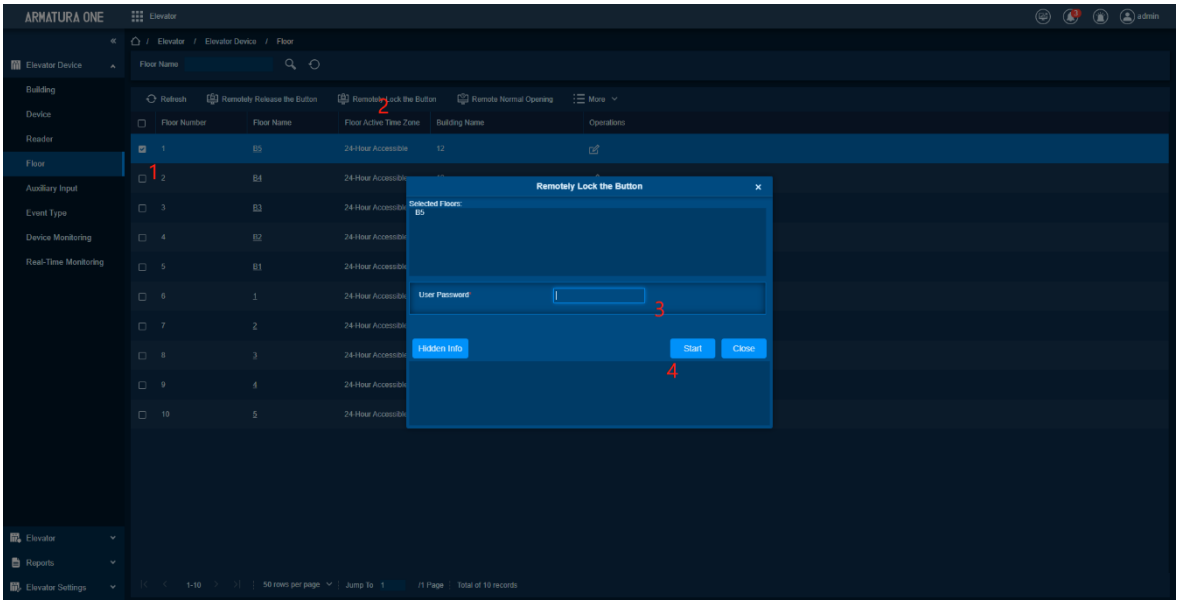
Feature Trigger Result

Corresponding to the current floor key lock of the elevator control device, personnel are not allowed to perform key operations.

Steps:

- Click **[Elevator Device] > [Floor] > [Remotely Lock the Button].**

This function is to remotely lock the floorboard permission of elevator device. After confirmation, you will not be able to operate the button until you release it again. Confirm lock after entering the password.



✍**Note:**

Only the selected floor from the device supports this operation.

Remotely Release the Button Continuously

Preconditions for Normal Use of Function

- The current floor corresponding to the building has bound elevator control device.
- The bound elevator control device can communicate normally.

Function Usage Scenarios

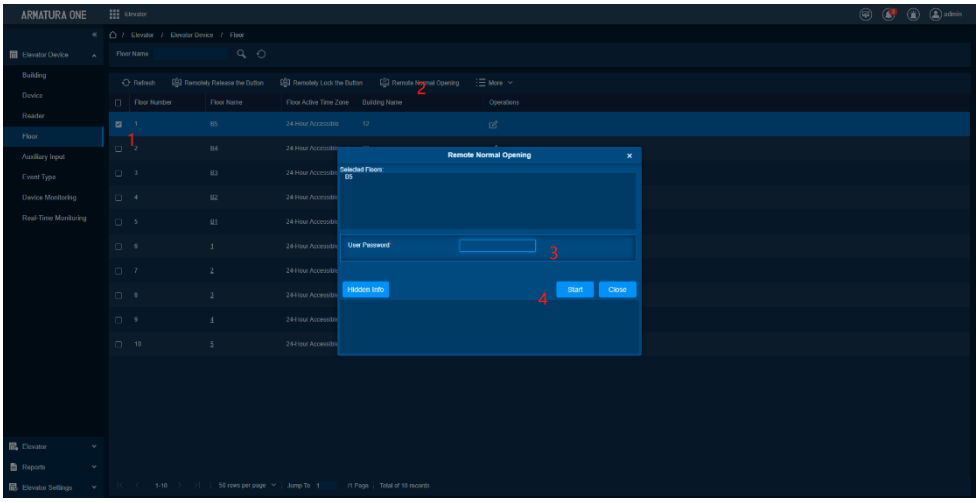
Release the button authority of the current floor of the elevator control device in the current building, and you can operate the floor buttons at any time.

Feature Trigger Result

The current floor buttons of all elevator control device in the current building can be operated all the time.

Steps:

Click **[Elevator Device] > [Floor] > [Remotely Normal Opening].** This function will keep your elevator control buttons in an unlocked state for a long time, and you can click on the floor to operate without any verification. Confirm operation after entering the password.



✍**Note:**

Only the floor from the device supports this operation.

Enable the Day's Normally Open Timetable

Preconditions for Normal Use of Function

- The current floor corresponding to the building has bound elevator control device.
- The bound elevator control device can communicate normally.

Function Usage Scenarios

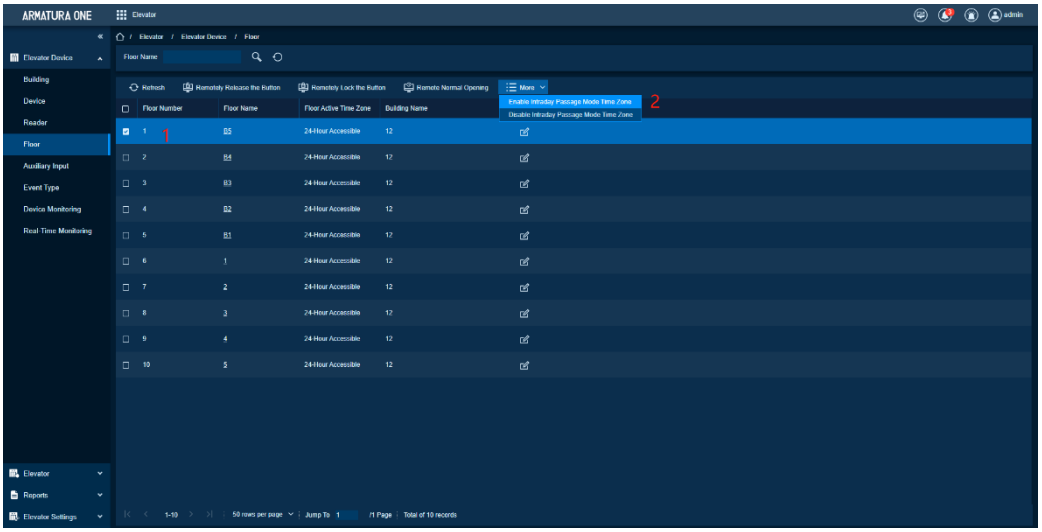
The elevator control device in the building to which it belongs activates the normally open time limit of the current floor.

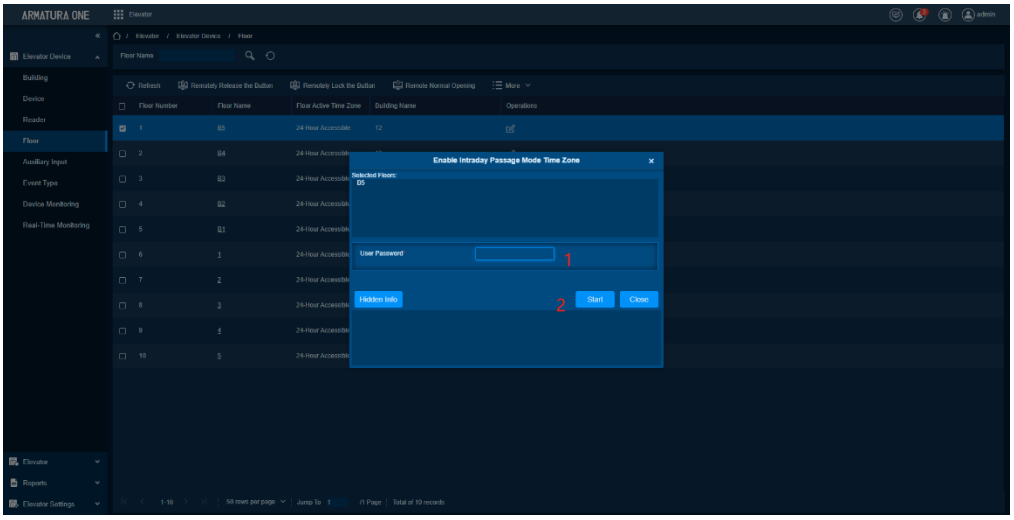
Feature Trigger Result

The current floor of all elevator control device of the building is turned on the normally open time limit set on the current floor.

Steps:

Click **[Elevator Device] > [Floor] > [Enable Intraday Passage Mode Time Zone].** This feature will enable the preset normally open time of the day. Confirm operation after entering the password.





✍**Note:**

Only the floor from the device supports this operation.

Disable Day's Normally Open Timetable

Preconditions for Normal Use of Function

1. The current floor corresponding to the building has bound elevator control device.
2. The bound elevator control device can communicate normally.

Function Usage Scenarios

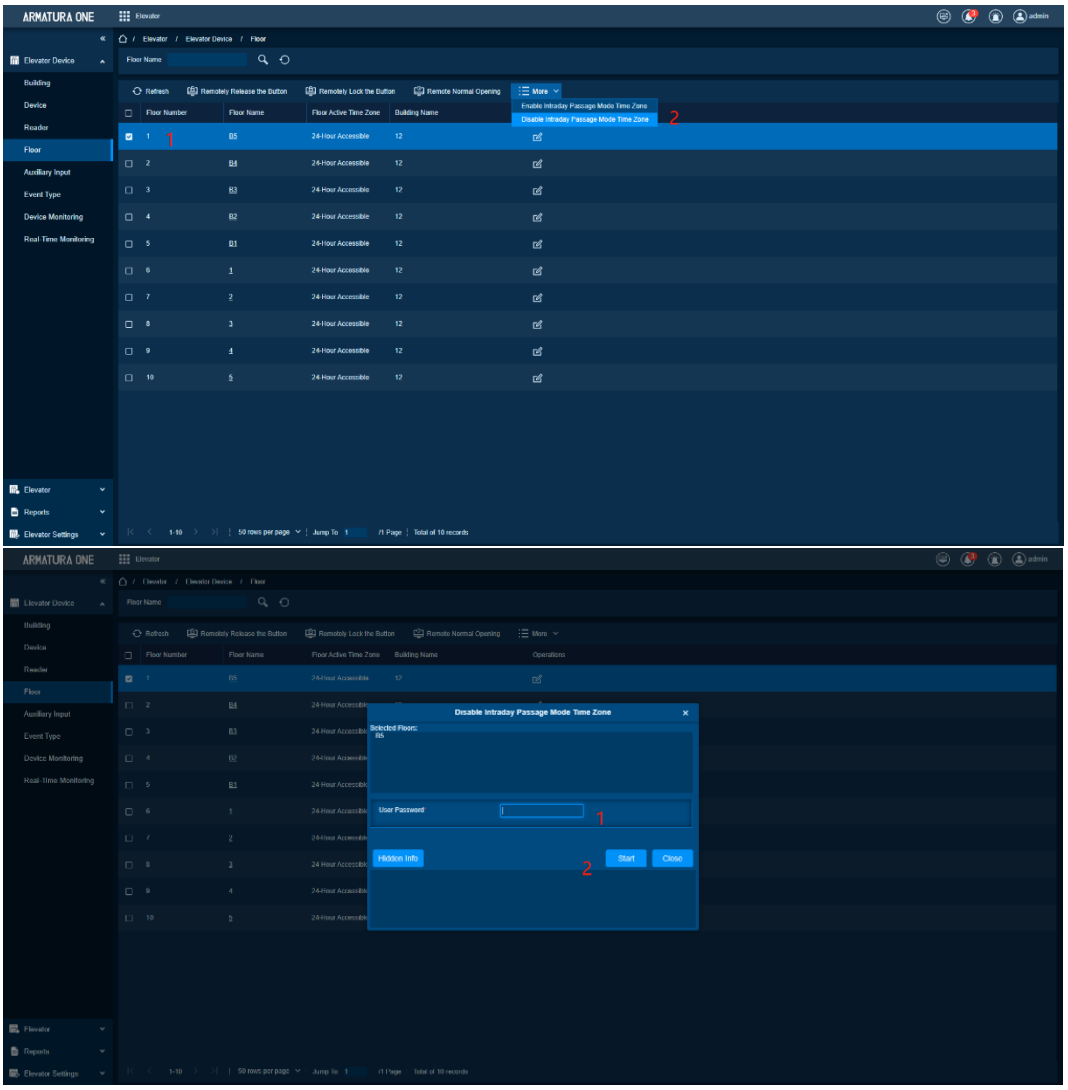
The elevator control device in the building that belongs to disable the normally open time limit of the current floor.

Feature Trigger Result

The current floor of all elevator control device belonging to the building disables the normally open time limit set on the current floor.

Steps:

Click **[Elevator Device] > [Floor] > [Disable Intraday Passage Mode Time Zone].** This feature will disable the preset normally open time of the day. Confirm operation after entering the password.



✍**Note:**

Only the floor from the device supports this operation.

8.1.5. Auxiliary Input

Function Description

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

Edit

Preconditions for Normal Use of Function

The current system successfully added elevator control device.

Function Usage Scenarios

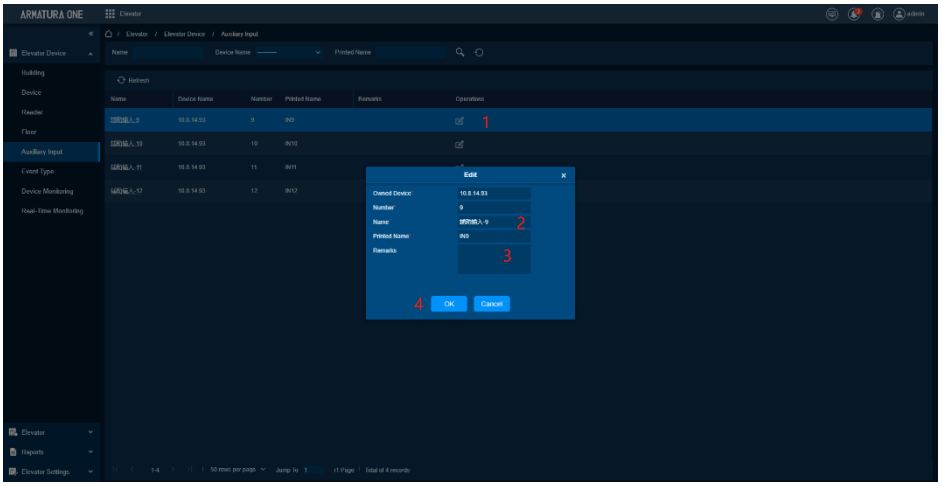
Modify the default name of auxiliary input.

Feature Trigger Result

Modify the default name.

Steps:

- Click **[Elevator Device] > [Auxiliary Input]** on the Action Menu, enter the following page.
- Click **[Edit]** to modify the parameters.



The fields are as follows:

Owned Device: Enter the IP address of the owned device.

Number: -Enter the number of the owned device.

Name: You can customize the name according to your preference.

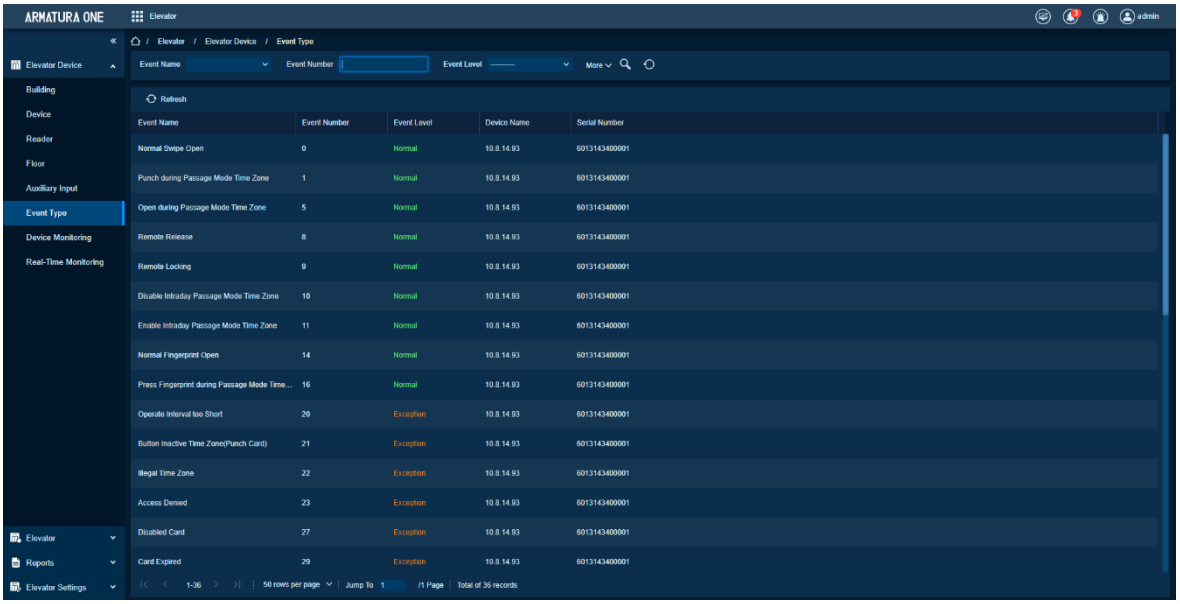
Printed Name: The printing name in the hardware, for example IN9.

Click **[Edit]** to modify the name and remark. Others are not allowed to edit here.

8.1.6. Event Type

Function Description

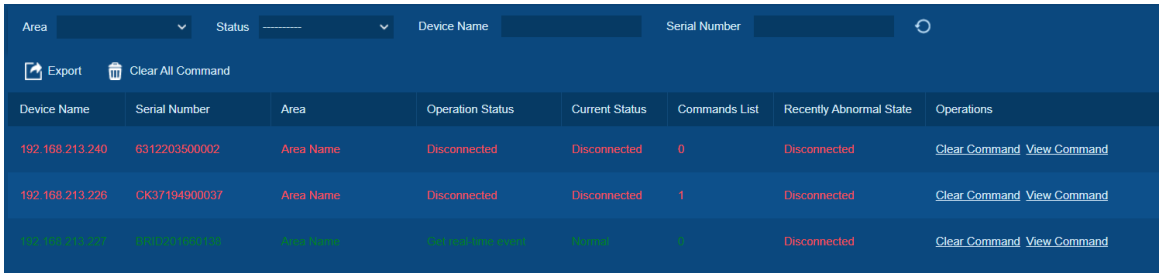
Its display the event types of the elevator devices.



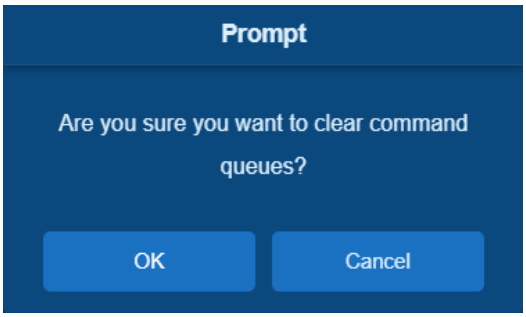
8.1.7. Device Monitoring

Function Description

By default, it monitors all devices within the current user's level, click [Elevator Device] > [Device Monitoring], and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, status, commands List, and Related Operation.



You can clear command as required. Click **[Clear Command]** behind the corresponding device.



Click **[OK]** to clear.

✍**Note:**

After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on

the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you can replace the current device with a large capacity one or delete the right of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.

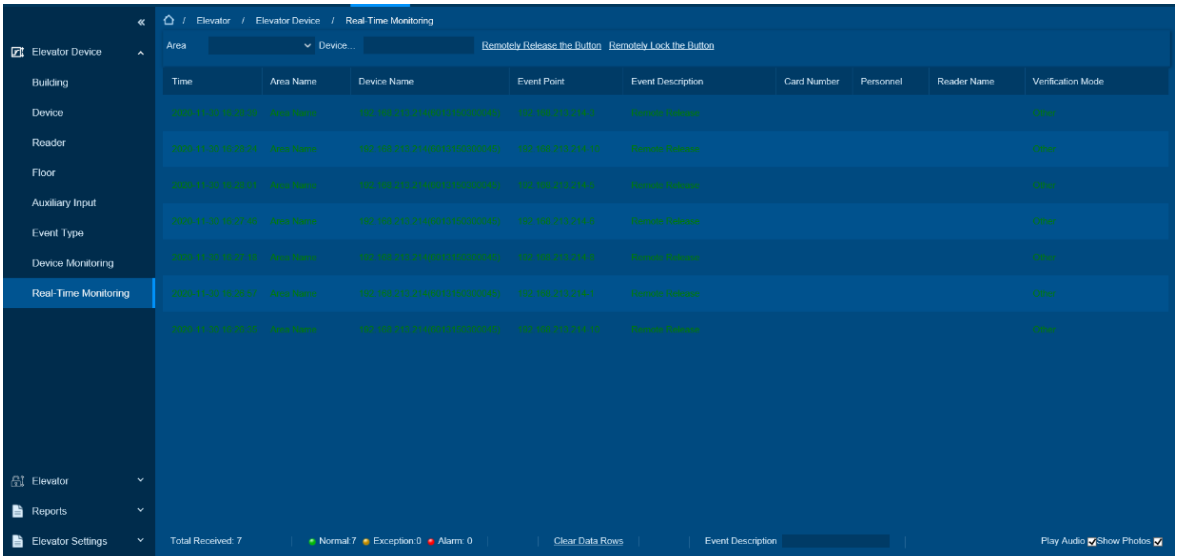
Operate State is the content of communications equipment of current device, mainly used for debugging.

The number of commands to be performed is greater than 0, indicating that data is not synchronized to the device, just wait.

8.1.8. Real-Time Monitoring

Function Description

Click **[Elevator Device] > [Real-Time Monitoring],** real-time monitor the status and real-time events of elevator controllers in the system, including normal events and abnormal events (including alarm events). Real-Time Monitoring interface is shown as follows:



Event Monitoring

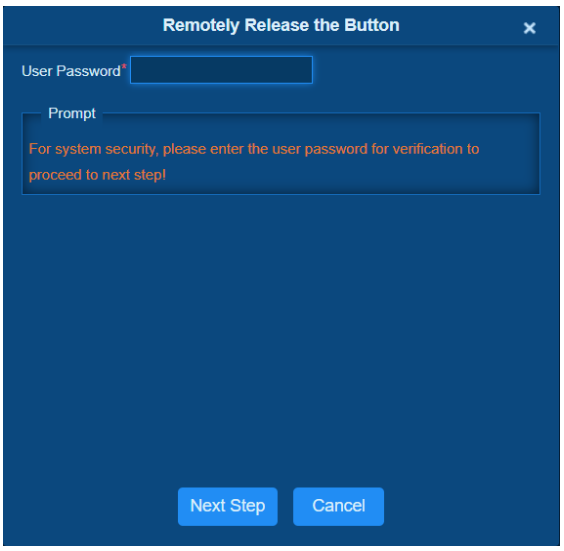
System automatically acquires monitored device event records (by default, display 200 records), including normal and abnormal elevator control events (including alarm events). Normal events appear in green; alarm events appear in red, other abnormal events appear in orange.

Monitor Area: All floors with elevator controller in the system is monitored by default, you can target to monitor one or more floors by Area, Status, Device Name and Serial NO.

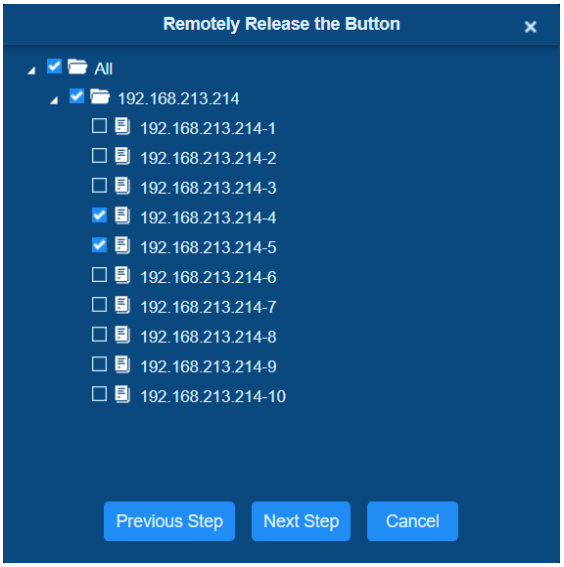
Show Photos: If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

Remotely Release Button

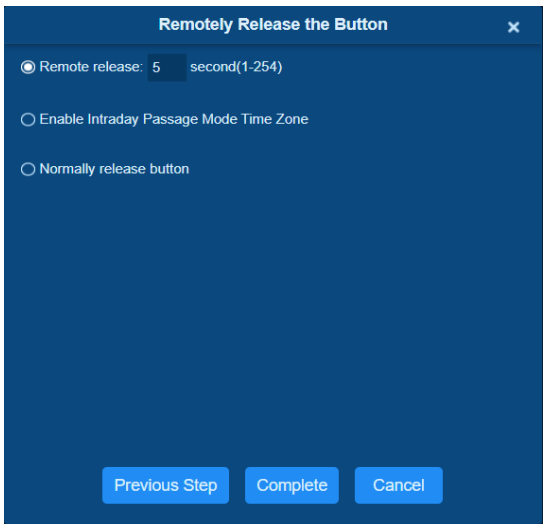
- Click **[Remotely Release Button].**



- Input the user password (the system logging password), click **[Next Step].**



- Select the floor and click **[Next Step].**



The fields are as follows:

Remote Release: It determines whether the corresponding key to the selected floor can be pressed. You can customize the key release duration (15s by default) or select Enable Intraday Passage Mode Time Zone. You can also directly set the status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

Enable Intraday Passage Mode Time Zone: To close a floor, you must first set Disable Intraday Passage Mode Time Zone to prevent the case that the floor is opened because other continuous open periods take effect. Then, you need to set to close the Remote Lock Button.

Sustained Release Button: The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

✍**Note:**

If a failure message is always returned for the remote release key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

Select the options, click [Complete] to finish enabling the button.

8.2. Elevator

Function List

Functions	Description
Timetable	Enter basic data such as add, delete, edit, search.
Holidays	Enter basic information such as add, delete, edit, search, etc. of holidays.
Elevator Level	Enter add, edit, delete of the elevator level, and bind the system floor operation.

Set by Permission Group	Add personnel to the elevator level, the personnel can have the authority to enter the elevator to reach the corresponding authority floor.
Set by Personnel	Manage the current personnel's elevator level or directly set the super administrator authority.
Set by Department	Set the department's elevator level authority.
Global Linkage	Set the event operation triggered by the elevator control event and the person who triggered the event.
Parameters Setting	Set up the method of obtaining the event record of the elevator control device and the size of the pop-up photo of the real-time monitoring page.

8.2.1. Time Zones

Function Description

Set the time of the elevator control floor, and only within the time can you use the authority to verify the elevator ride.

Add Timetable

Preconditions for Normal Use of Function

Not yet.

Function Usage Scenarios

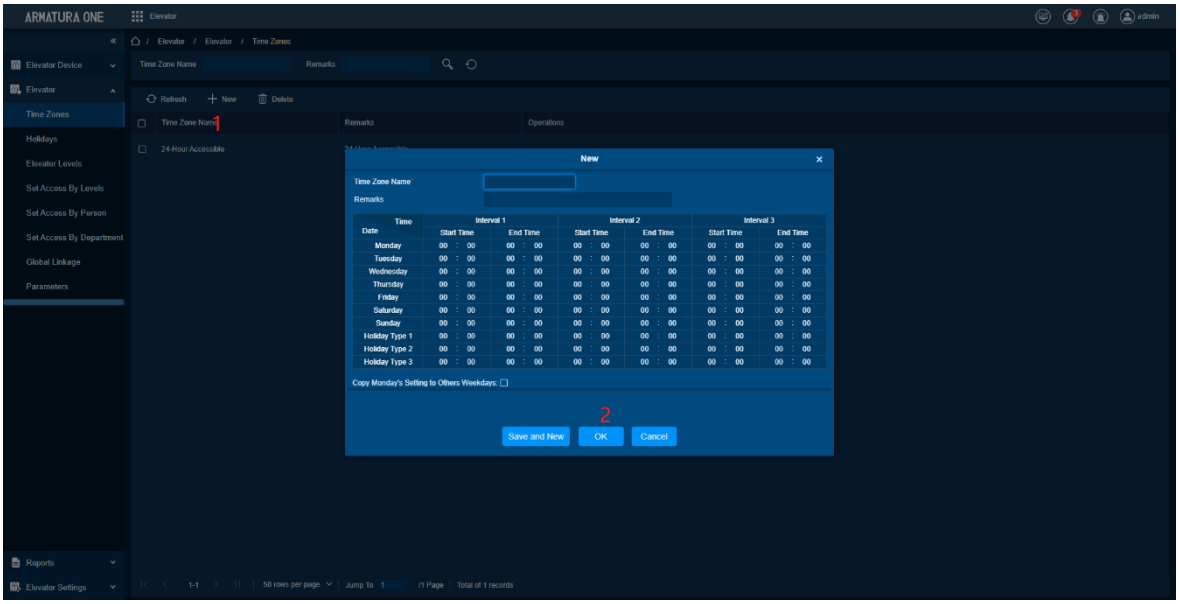
Add a custom time elevator control to the elevator control floor.

Function Triggered Result

Add a time data.

Steps:

Click **[Elevator]** > **[Time Zones]** > **[New]** to enter the time zone setting interface.



The parameters are as follows: -

Time Zone Name: Enter any character, up to a combination of 30 characters.

Remarks: The detailed description of the current time zone, including explanation of current time zone and primary applications. The field is up to 50 characters.

Interval and Start/End Time: One Elevator Control Time Zone includes 3 intervals for each day in a week, and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as the interval 1, and 00:00-00:00 as the interval 2/3. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, user just needs to fill out the interval 1, and the interval 2/3 will use the default value. Similarly, when only using the first two intervals, the third interval will use the default value. When using two or three intervals, user needs to ensure two or three intervals have no time intersection, and the time shall cross over to 2nd day, or the system will prompt error.

Holiday Type: Three leave types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access. The holiday type is optional. If the user does not enter one, system will use the default value.

Copy on Monday: You can quickly copy the settings of Monday from Tuesday to Sunday.

After setting, click OK to save, and it will display in the list.

Maintenance of Elevator Time Zones

Edit: Click the **[Edit]** button under operation to enter the edit interface. After editing, click **[OK]** to save.

Delete: Click the **[Delete]** button under Related Operation, then click **[OK]** to delete, or click **[Cancel]** to cancel the operation.

A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list and click the **[Delete]** button over the list. Then click **[OK]** to delete, click **[Cancel]** to cancel the operation.

Delete Timetable

Preconditions for Normal Use of Function

Select the added time.

Function Usage Scenarios

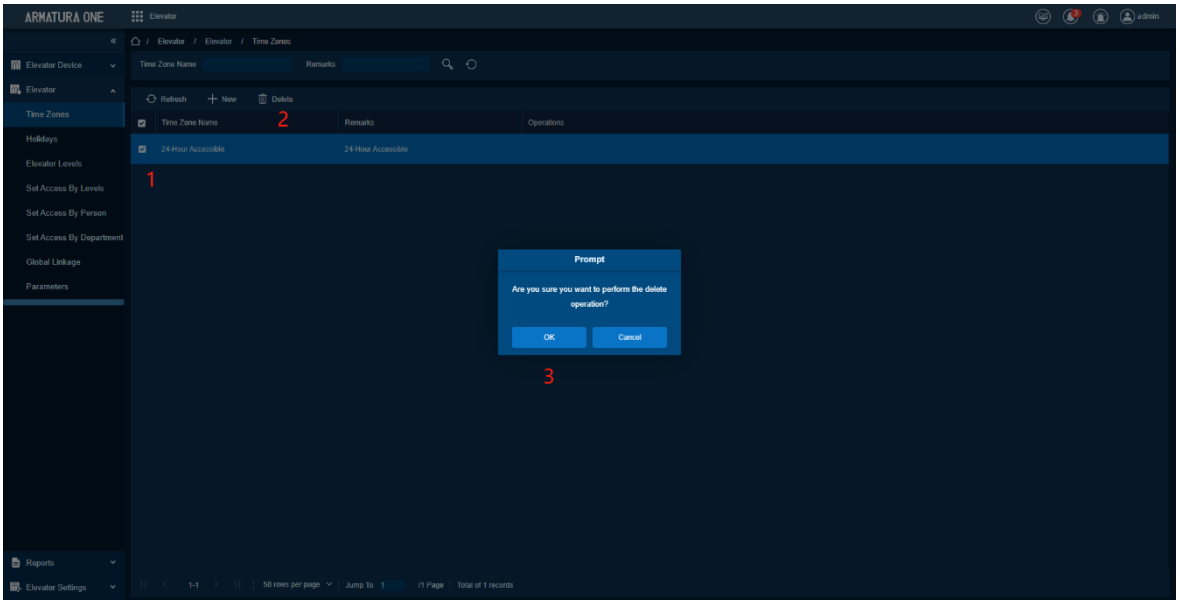
Timetable requires deleted not to be used.

Function Triggered Result

Delete the currently selected time data.

Steps:

Select the corresponding time, click **Delete.**



8.2.2. Holidays

Function Description

It provides configuration time nodes for leave types in the time function.

Elevator Control Time of a holiday may differ from that of a weekday. The system provides elevator control time setting for holidays. Elevator Holiday Management includes Add, Modify and Delete.

Add Holidays

Preconditions for Normal Use of Function

Add a new Holiday for system

Function Usage Scenarios

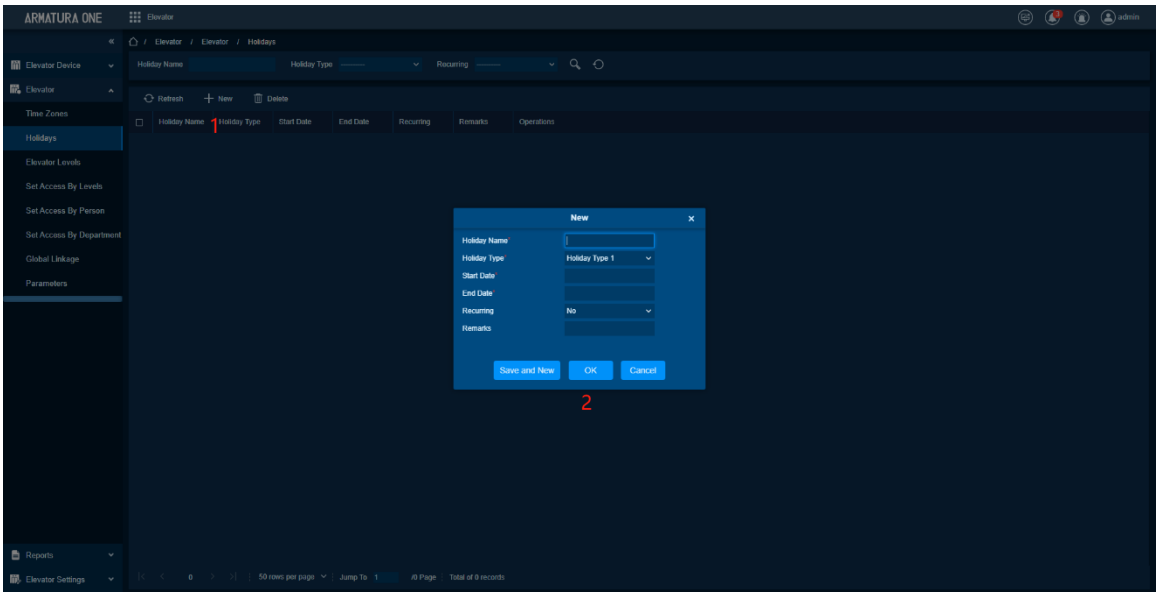
In the time, if you need to avoid the holidays time configuration, you need to add the holidays configuration.

Function Triggered Result

Add holidays data, configure the time configuration corresponding to the holiday type in time then it will take effect.

Steps:

Click **[Elevator]** > **[Holidays]** > **[New]** to enter edit interface.



The fields are as follows: -

Holiday Name: Enter any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/End Date: The date format should be 2010-1-1. Start Date cannot be later than End Date otherwise system error will occur. The year of Start Date cannot be earlier than the current year, and the holiday cannot span years.

Recurring: It means that a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

Delete Holidays

Preconditions for Normal Use of Function

Select the corresponding holidays data.

Function Usage Scenarios

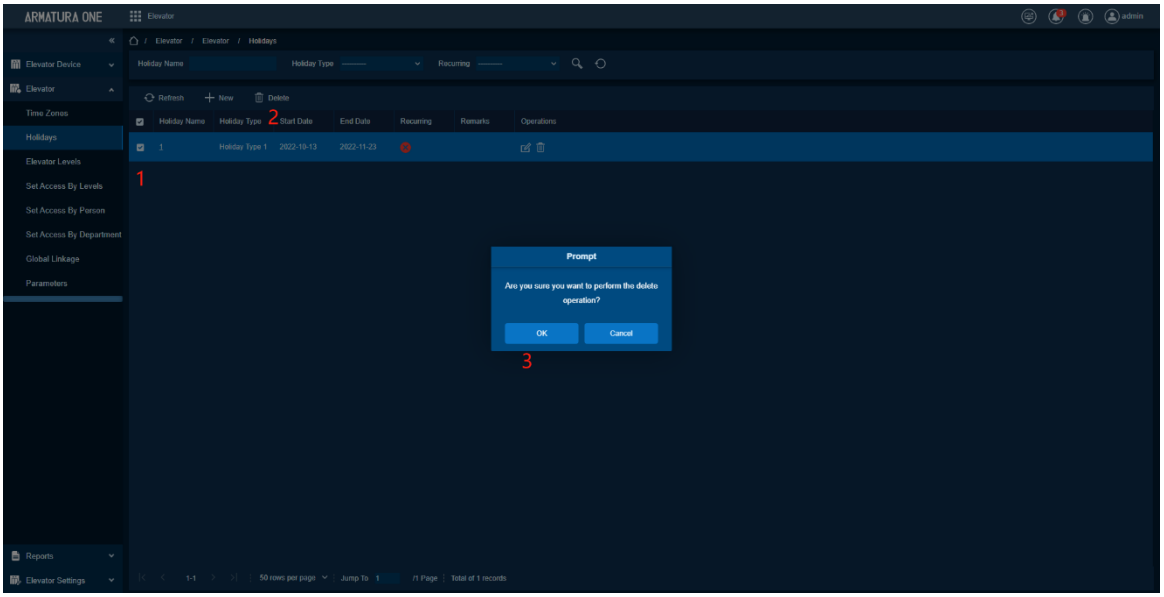
No need to use holidays configuration

Function Triggered Result

The system deletes the currently selected holidays data.

Steps:

- In the Access Control Holiday List, click [Delete] button under operations.
- Click **[OK]** to delete, click **[Cancel]** to cancel the operation. An Elevator Holiday in use cannot be deleted.



8.2.3. Elevator Levels

Function Description

Elevator levels indicate that one or several selected doors can be opened by verification of a combination of multi person within certain time zone. The combination of multi-person set in Personnel Access Level option.

Add Permission Group

Preconditions for Normal Use of Function

Need to add time and data.

Function Usage Scenarios

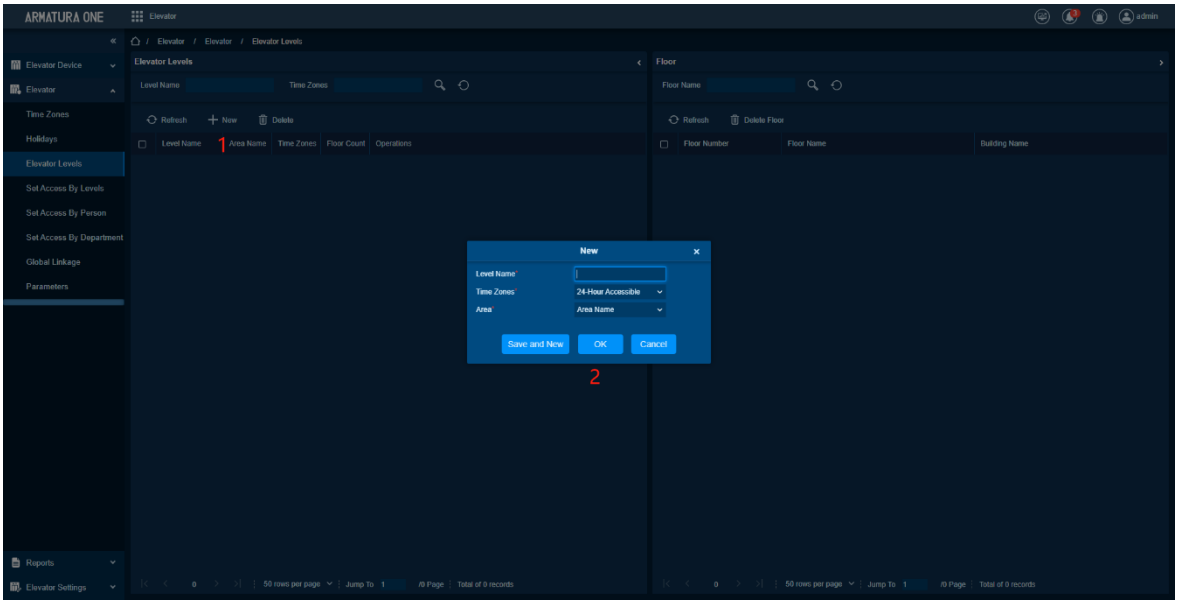
Configure the corresponding authority group for the elevator control floor.

Function Triggered Result

Add access levels configuration, and it can configure the corresponding permission floor for the access levels.

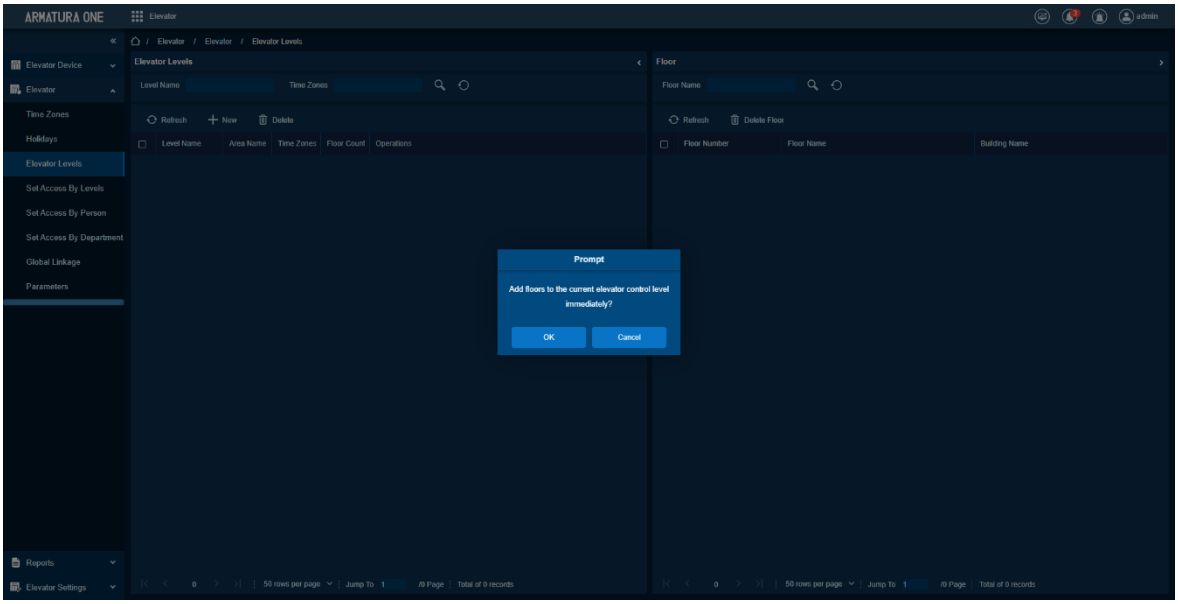
Steps:

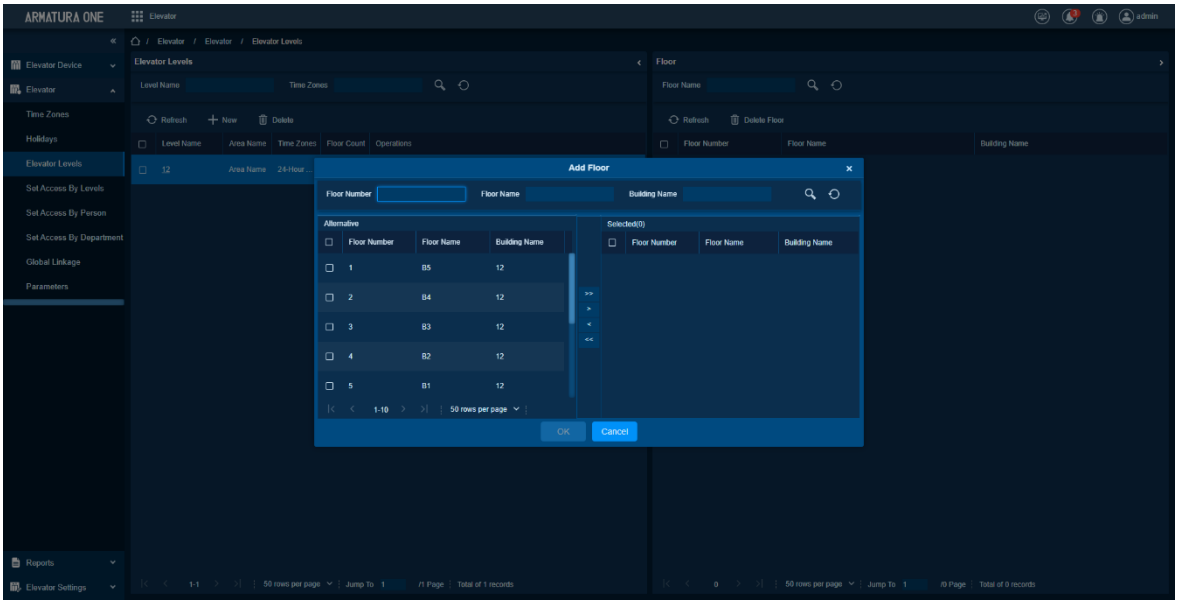
Click **[Elevator] > [Elevator Levels] > [New]** to enter the add levels editing interface.



Set Each Parameter: Level Name (unrepeatable), Time Zone and Area.

- Click **[OK],** the system prompts “Add floors to the current elevator control level immediately”.
- Click **[OK]** to add floors.
- Click **[Cancel]** to return the elevator levels list. The added level is displayed in the list.





✍**Note:**

Different floors of different elevator controllers can be selected and added to an elevator level.

Delete Permission Group

Preconditions for Normal Use of Function

Need to select the corresponding elevator levels that needs delete.

Function Usage Scenarios

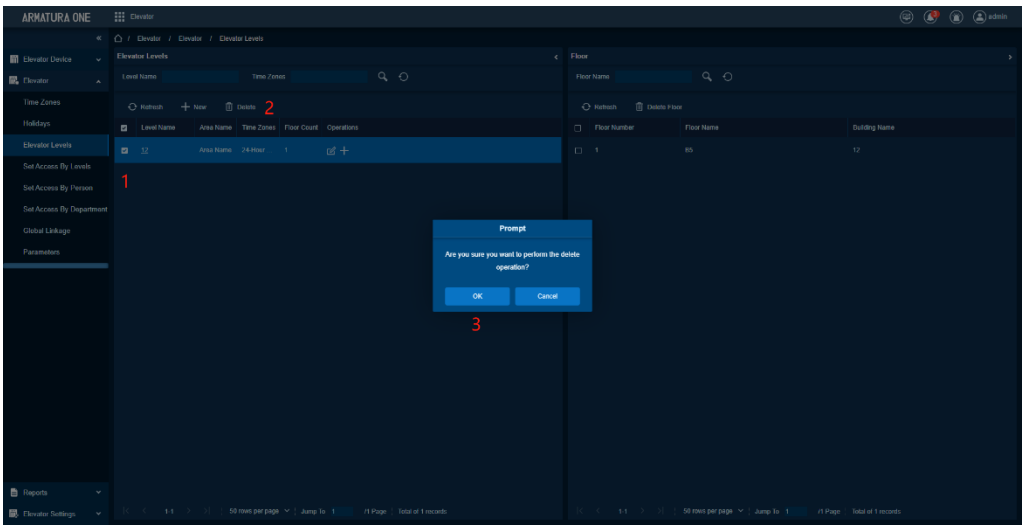
The elevator level does not need to be used.

Function Triggered Result

Delete selected elevator levels data.

Steps:

- Select the data, click the **[Delete]** button.
- On the pop-up confirmation box, click **[OK].**



Add Floor

Preconditions for Normal Use of Function

There is an elevator level in the current system.

Function Usage Scenarios

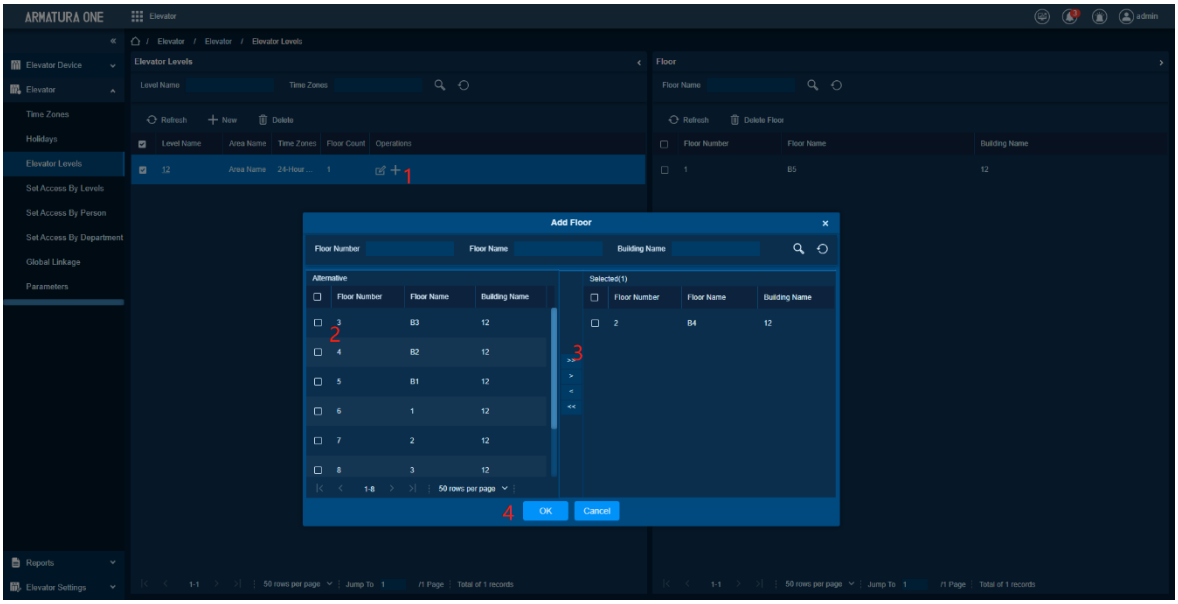
Configure the corresponding elevator level for the elevator control floor.

Function Triggered Result

Elevator control floor and elevator level binding completed.

Steps:

- Click **[Elevator] > [Elevator Levels]** to enter the edit interface, click an elevator level in left list, personnel having right of opening door in this access level will display on right list.
- In the left list, click **[Add Personnel]** under operations to pop-up the add personnel box; select personnel (multiple) and click > to move it to the right selected list, then click **[OK]** to save and complete.



Delete Floor

Preconditions for Normal Use of Function

The elevator level has been added to the corresponding floor data.

Function Usage Scenarios

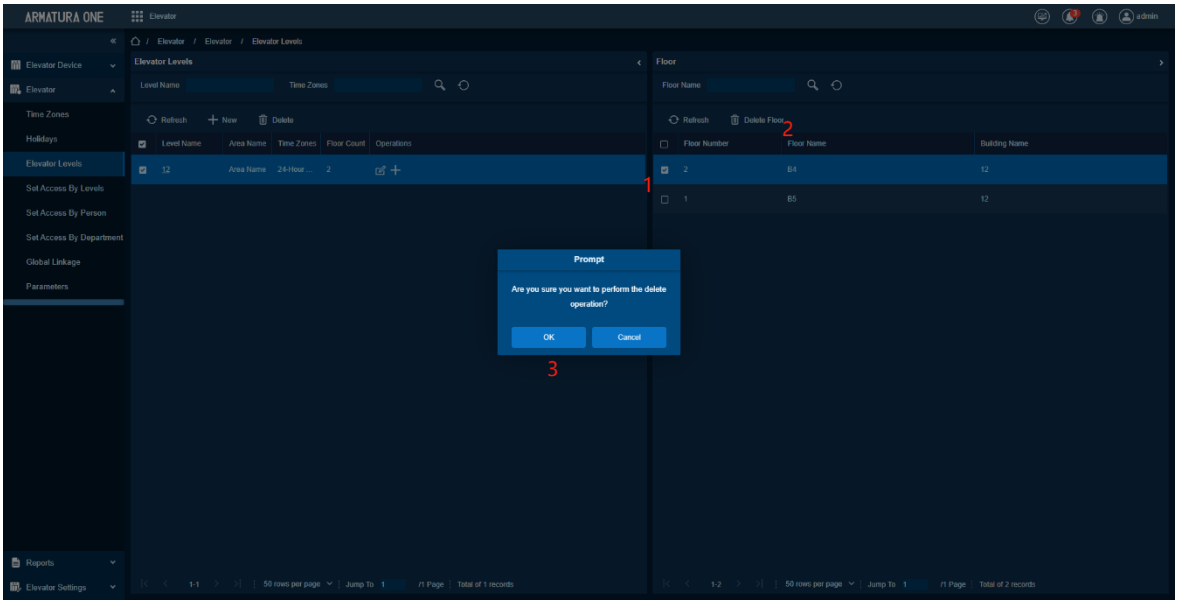
Delete the current elevator levels of the floor.

Function Triggered Result

Releasing the binding relationship between elevator control floors and elevator levels.

Steps:

Click the level to view the personnel in the right list. Select personnel and click **[Delete Personnel]** above the right list, then click **[OK]** to delete.



8.2.4. Set Access By Levels

Function Description

Add selected personnel to selected elevator levels or delete selected personnel from the elevator levels.

Add Personnel

Preconditions for Normal Use of Function

The system adds the corresponding elevator level.

Function Usage Scenarios

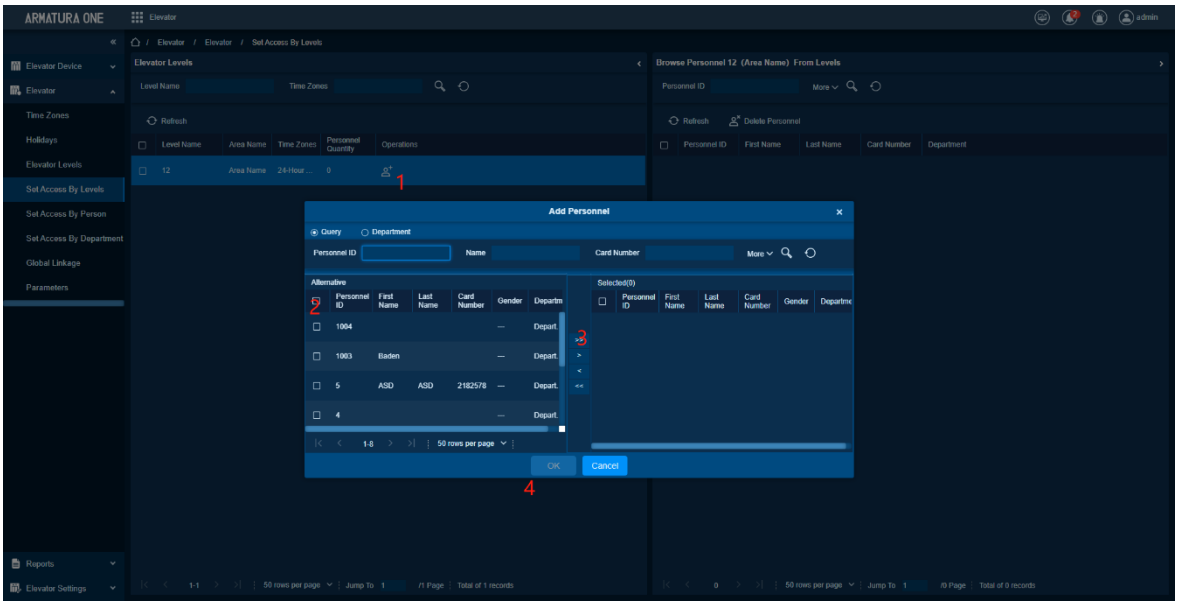
Add the corresponding elevator control authority configuration for the system personnel, so that the personnel can have the authority to operate the elevator.

Function Triggered Result

Personnel have the authority of the elevator level and can take the elevator to the corresponding floor.

Steps:

- Click **[Elevator]** > **[Set Access By Levels]** > **[Set by Person],** click employee to view the levels in the right list.
- Click **[Add to Levels]** under operations to pop-up the Add to Levels box, select Level (multiple), and click > to move it to the right selected list; click **[OK]** to save and complete.



Delete Personnel

Preconditions for Normal Use of Function

The currently selected elevator level has binding personnel information.

Function Usage Scenarios

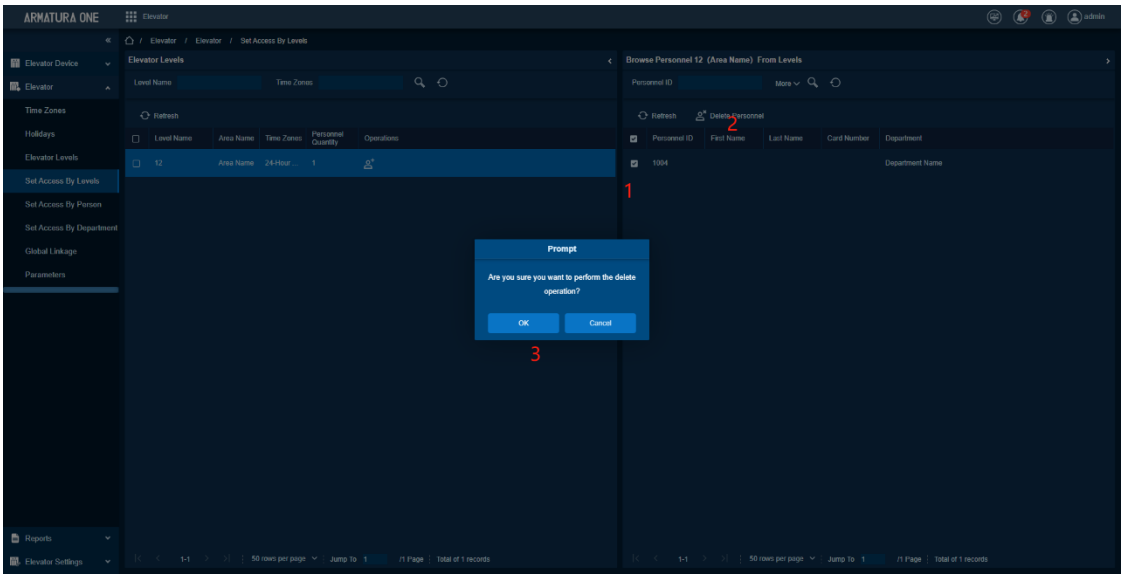
Delete the current personnel's elevator levels permissions.

Function Triggered Result

Delete the permission of the current personnel's elevator levels and cannot take the elevator to reach the corresponding floor.

Steps:

Select Level (multiple) from the right list and click **[Delete from Levels]** above the list, then click **[OK]** to delete the selected levels.



8.2.5. Set Access By Person

Function Description

According to personnel configuration, set the corresponding authority group authority for the personnel, it can add authority group for the personnel, or delete the elevator level of the corresponding personnel.

Elevator Control Settings

Preconditions for Normal Use of Function

Need to select personnel.

Function Usage Scenarios

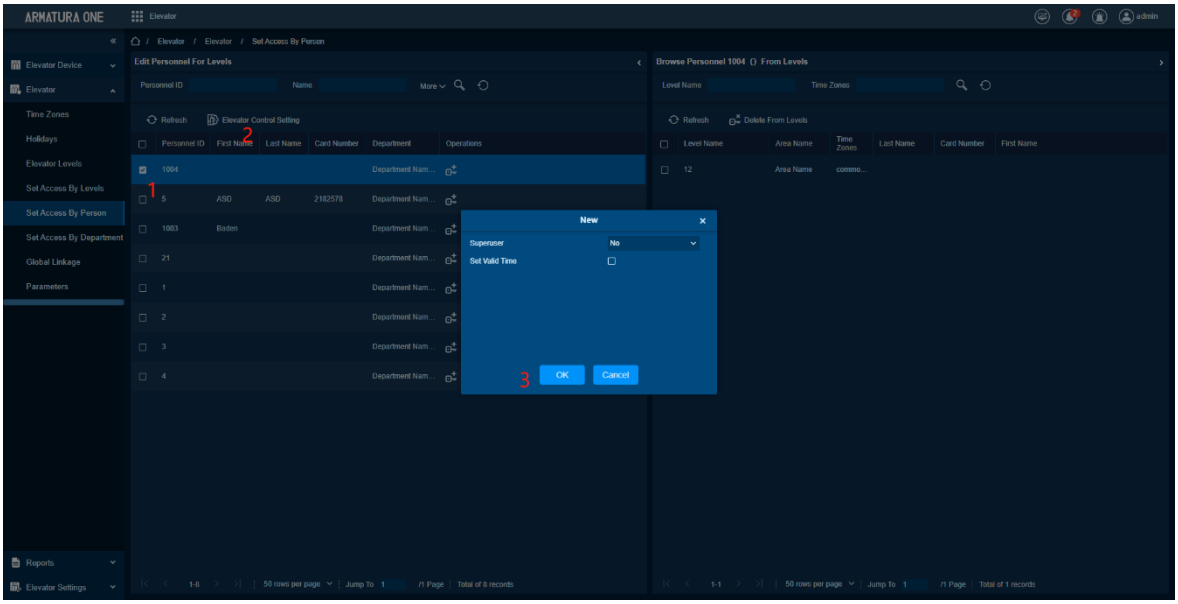
Set the super administrator authority for the current person or set the effective time of the current person.

Function Triggered Result

Set the current person's super administrator authority and effective time.

Steps:

Select a person in the list on the left and click **[Elevator Control Setting].** The following page is displayed:



Set elevator control parameters and click **[OK]** to save the setting.

Add Permission Group

Preconditions for Normal Use of Function

Persons to be selected.

Function Usage Scenarios

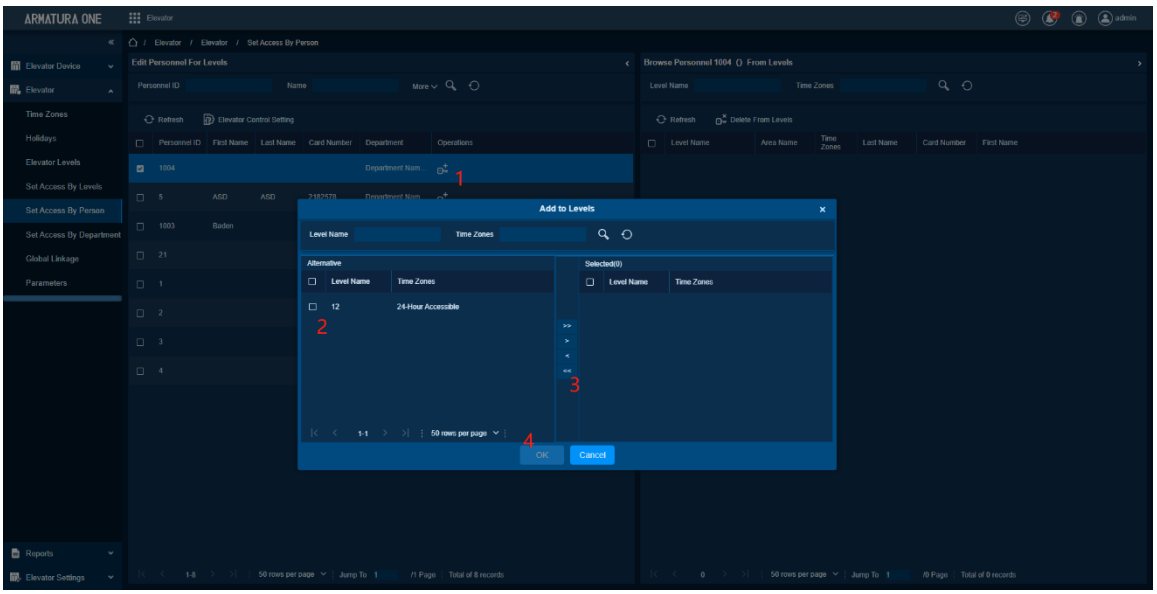
Add authority group configuration for corresponding personnel, so that personnel have authority group authority to take elevator.

Function Triggered Result

Add a binding relationship between a person and an elevator level.

Steps:

- Click to add an elevator level.
- Select the corresponding elevator levels in the pop-up window and click **[OK].**



Delete Permission Group

Preconditions for Normal Use of Function

Personnel bound to elevator levels management.

Function Usage Scenarios

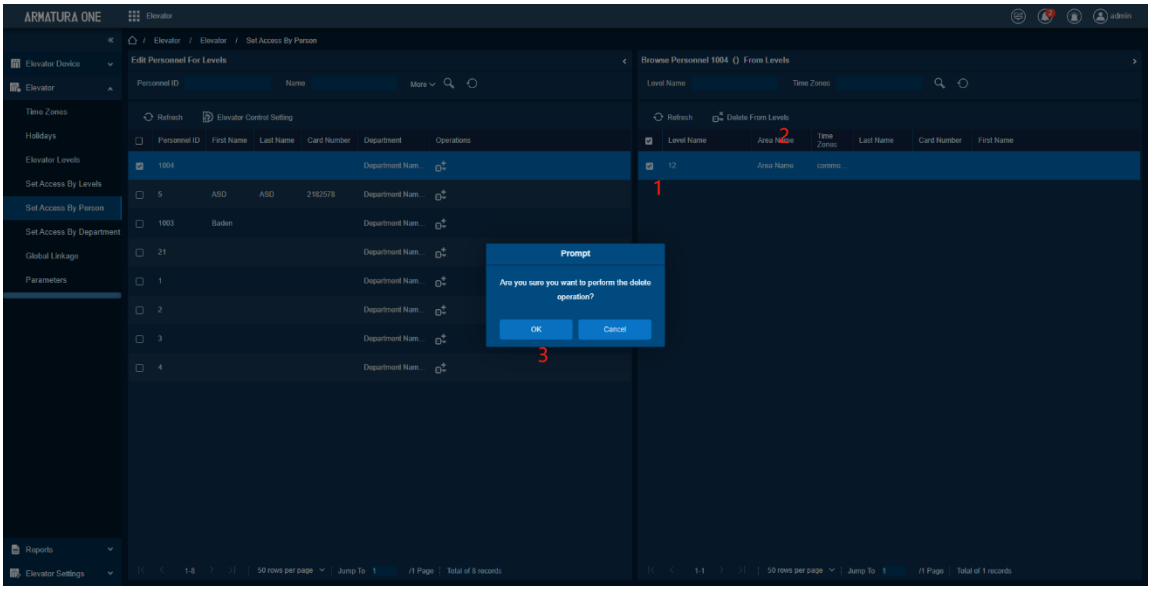
Delete personnel corresponding to the authority group relationship, personnel shall not use the authority group authority to take the elevator.

Function Triggered Result

Delete the corresponding binding relationship between personnel and elevator levels.

Steps:

- Select the corresponding authority group of the personnel, click **[Delete].**
- On the pop-up confirmation box, click **[OK].**



8.2.6. Set Access By Department

Function Description

Add selected department to selected elevator levels or delete selected department from the elevator levels. The access of the staff in the department will be changed.

Add Default Permission Group

Preconditions for Normal Use of Function

Not yet.

Function Usage Scenarios

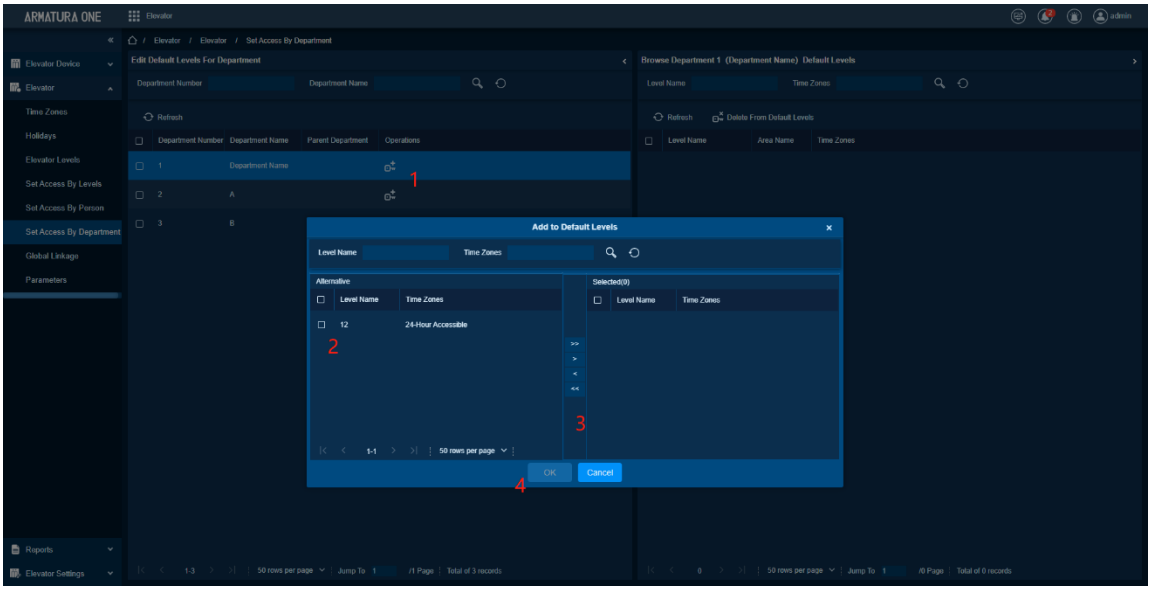
Configure elevator levels for all personnel in the entire department.

Function Triggered Result

All personnel in the entire department have the current elevator level authority.

Steps:

- Click to add an elevator level.
- On the pop-up box, select the corresponding elevator levels, click **[OK].**



Delete Default Permission Group

Preconditions for Normal Use of Function

The current department has added elevator levels configuration.

Function Usage Scenarios

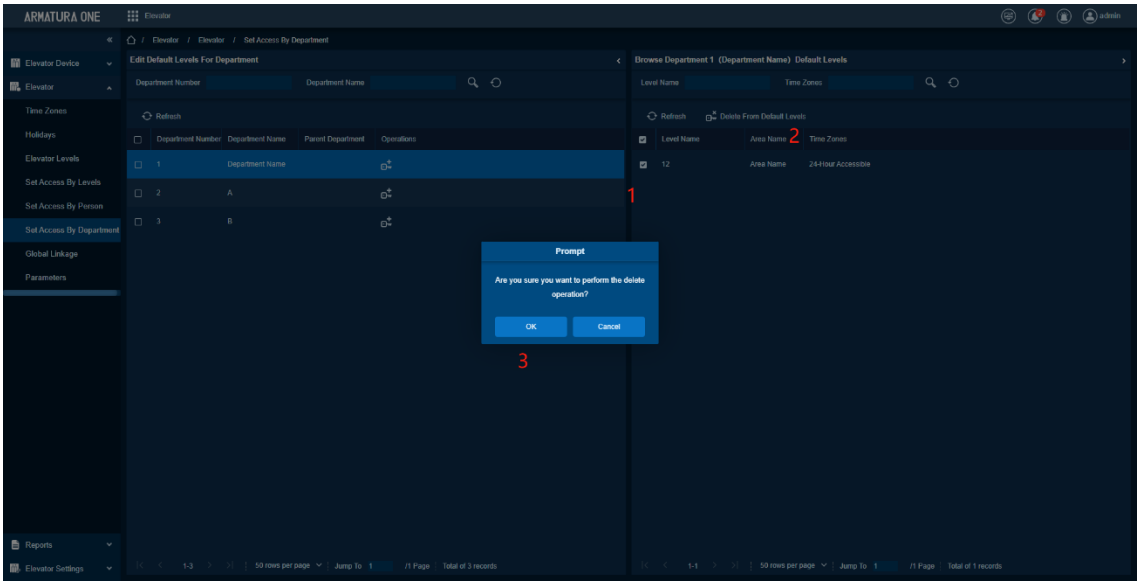
The deleted elevator levels configuration of the current department, all personnel in the department do not have a corresponding elevator level.

Function Triggered Result

All personnel in the current department cannot use the deleted elevator levels permission to take the elevator.

Steps:

- Select the Permission Group Data, click **[Delete]** button.
- On the pops up box, click **[OK].**



8.2.7. Global Linkage

Function Description

The global linkage function enables you to configure data across devices.

Add

Preconditions for Normal Use of Function

Need to add an elevator control device, the elevator control device has an event type.

Function Usage Scenarios

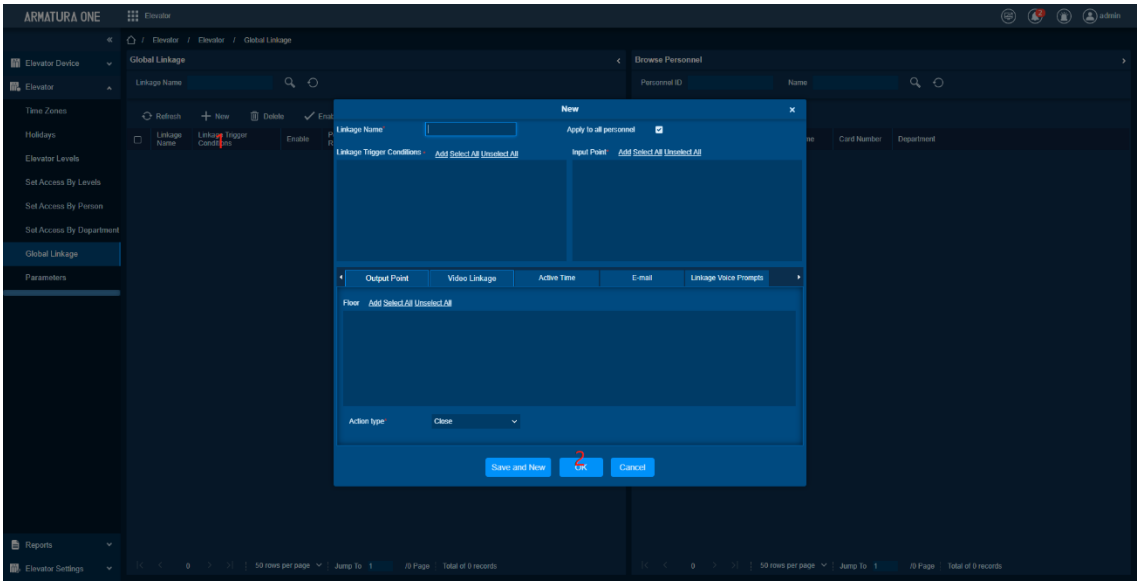
The elevator control device generates the corresponding event system to make linkage processing, it can bind the camera to capture or pop-up video, and it can send mail and other information to the corresponding configuration information.

Function Triggered Result

Add a linkage configuration information.

Steps:

Click **[Elevator] > [Elevator] > [Global Linkage] > [New].**



The fields are as follows:

Linkage Name: Set a linkage name.

Linkage Trigger Condition: Linkage Trigger Condition is the event type of selected device. Except Linkage Event Triggered, Cancel Alarm, Enable/Disable Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refers to specific device parameters).

Output Point: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, and Auxiliary Output 10 (the specific output point please refers to specific device parameters).

Linkage Action: Close, Open, Normal Open. The default is closed. To open, delay time shall be set, or select Normal Close.

Video Linkage

Pop up video: Whether to set the pop-up preview page in real-time monitoring and set the pop-long.

Video: Enable or disable background video recording and set the duration of background video recording.

Capture: Enable or disable background snapshot.

Delay: It ranges from 1 to 254s (This item is valid when Action type is Open).

Click **[OK]** to save and quit. The added Global Linkage will display in the list.

✍**Note:**

It is not allowed to set the same linkage setting at input point and output point. The same device permits consecutive logical linkage settings. The system allows you to set several trigger conditions for a linkage setting one time.

Delete

Preconditions for Normal Use of Function

Select linkage configuration data.

Function Usage Scenarios

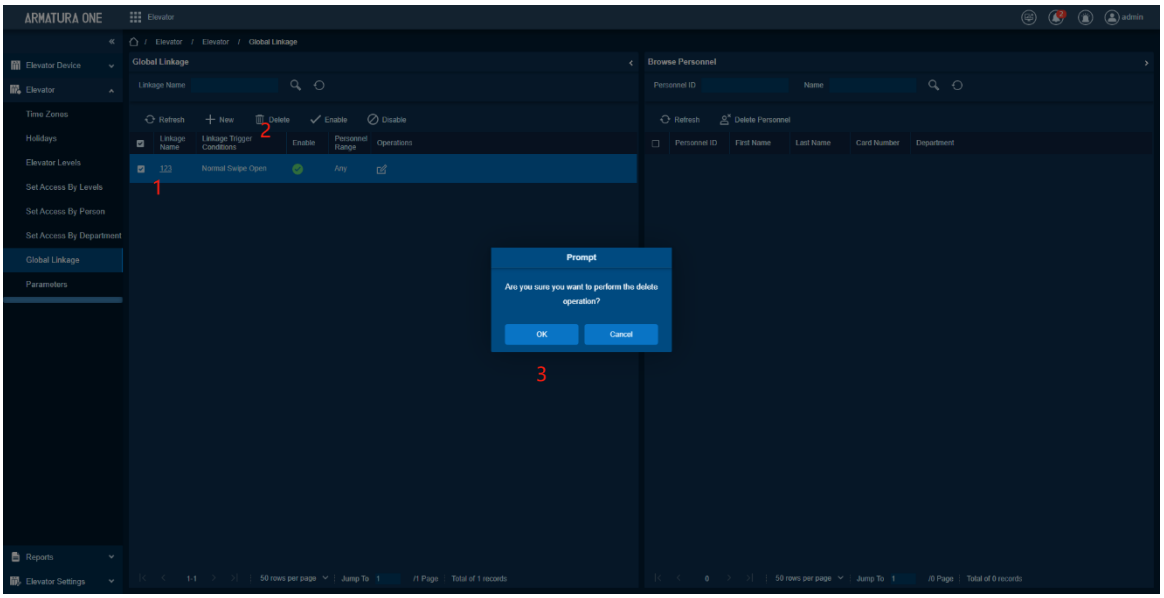
The current linkage configuration is not needed for obsolete.

Function Triggered Result

Delete current linkage configuration information, no linkage operation.

Steps:

- Select Linkage Configuration Data, click **[Delete].**
- On the pop-up interface, click **[OK].**



Enable

Preconditions for Normal Use of Function

Select the linkage configuration that has been added.

Function Usage Scenarios

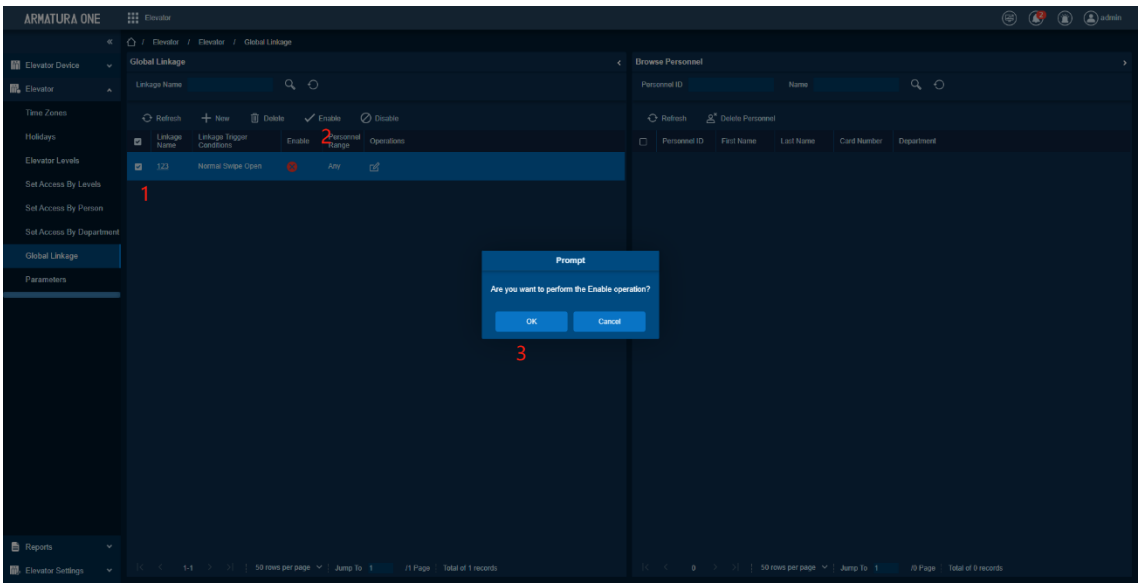
Enable linkage configuration, execute linkage trigger.

Function Triggered Result

Execution of linkage configuration results, sending emails or video camera linkage, etc.

Steps:

- Select the linkage configuration, click **[Enable]** button.
- On the pop-up window, click **[OK].**



Disable

Preconditions for Normal Use of Function

Select the linkage configuration that has been added.

Function Usage Scenarios

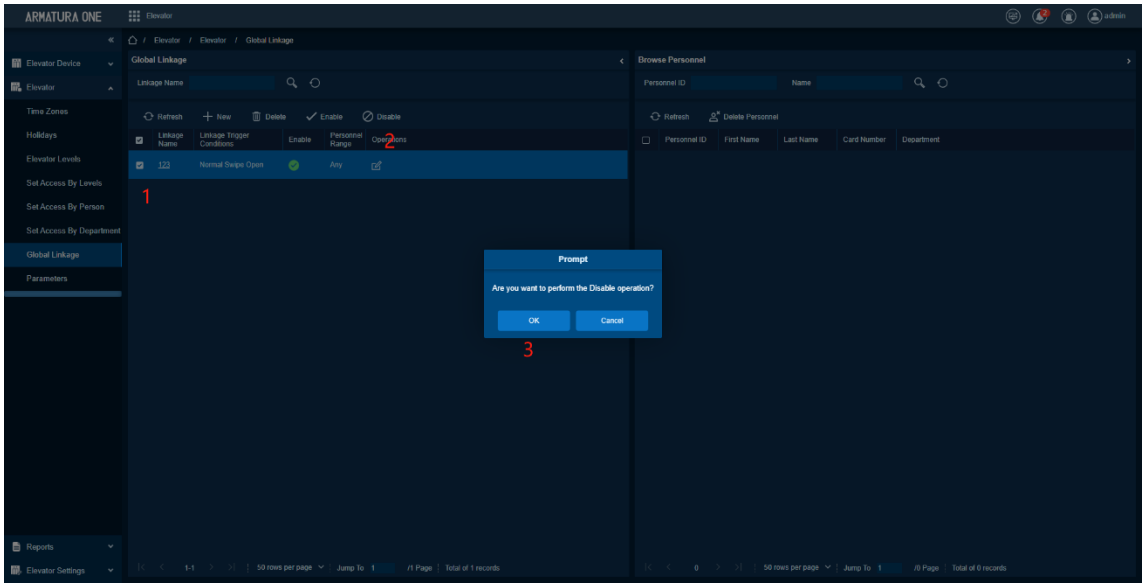
Cancel the activation of the linkage configuration, and do not execute the current linkage configuration.

Function Triggered Result

The linkage is changed to a disabled state, and linkage configuration is not performed.

Steps:

- Select linkage configuration, click **[Disable]**.
- Click **[OK]**.



Add Personnel

Preconditions for Normal Use of Function

The range of linkage configuration personnel is the selection type.

Function Usage Scenarios

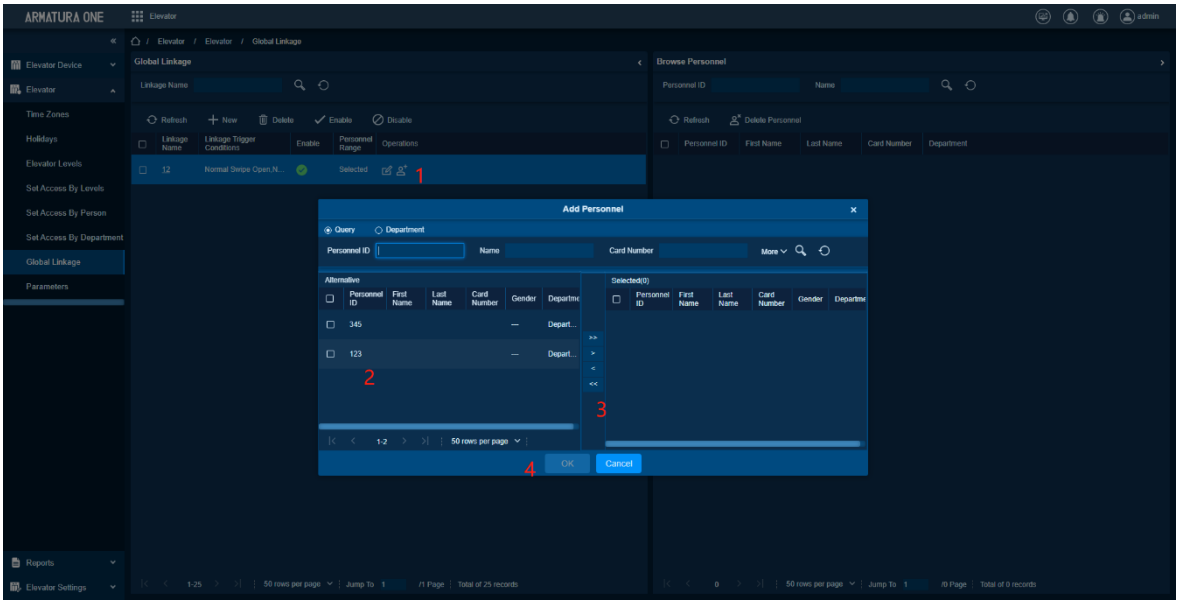
Set up linkage configuration for certain people.

Function Triggered Result

Linkage configuration to add designated personnel.

Steps:

- Click Add Personnel button, a window will pop up to select the corresponding personnel information, click **[OK].**



Delete Personnel

Preconditions for Normal Use of Function

- The range of linkage configuration personnel is the selection type.
- Linkage configuration has been added personnel.

Function Usage Scenarios

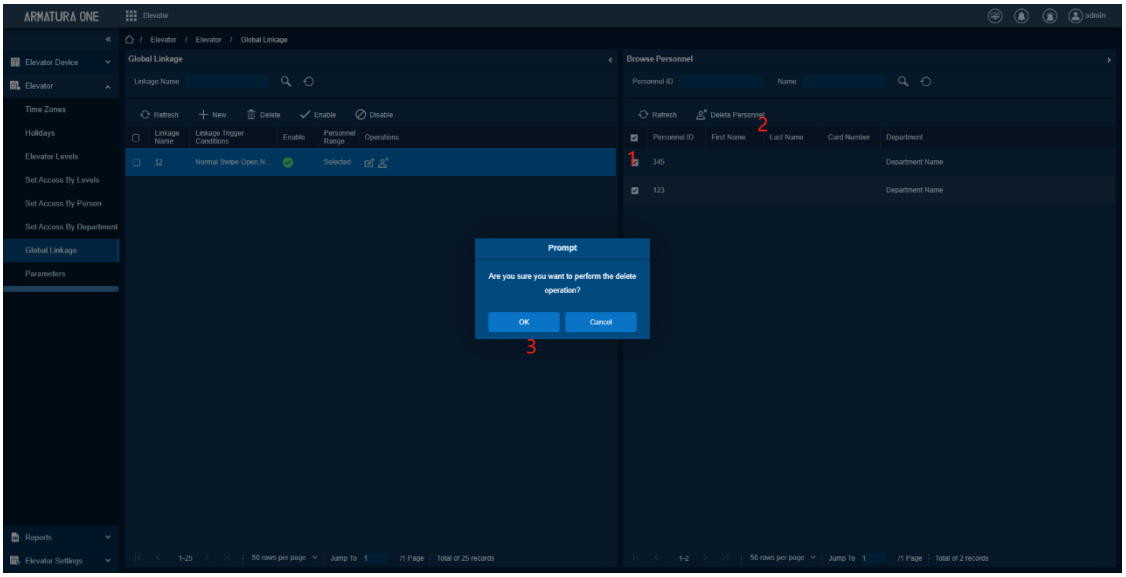
Delete linkage of designated personnel.

Function Triggered Result

Delete the association between personnel and linkage configuration.

Steps:

- Select Personnel, click **[Delete]**.
- A confirmation window pops up, click **[OK].**



8.2.8. Parameters

Function Description

The guest module uses parameter configuration.

Preconditions for Normal Use of Function

Set custom parameters.

Function Usage Scenarios

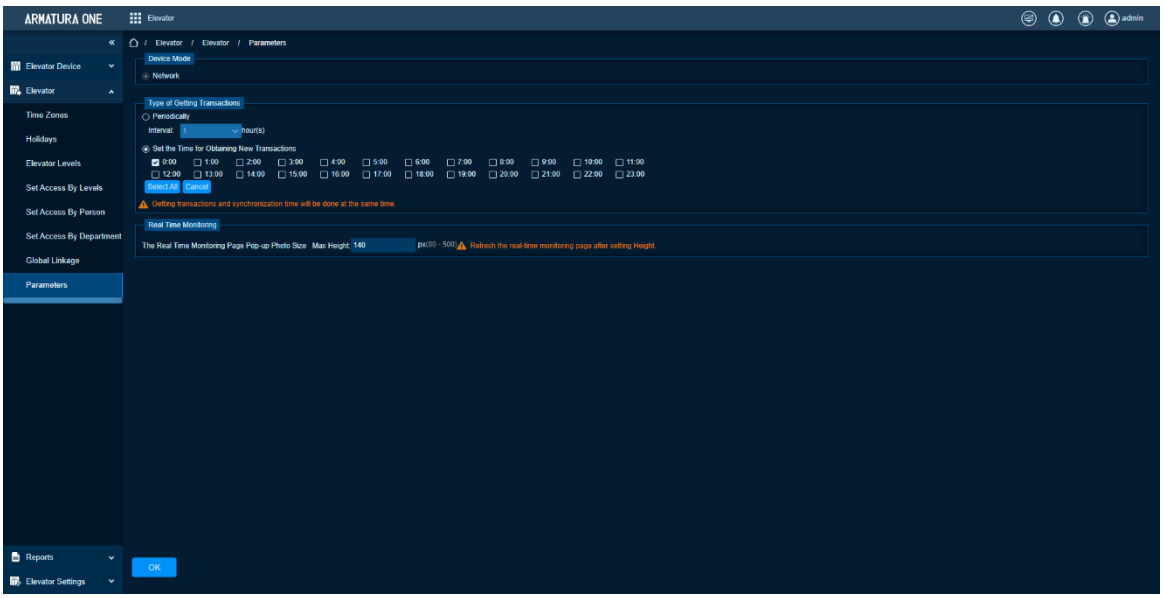
Modify the default method of obtaining event records or modify the height of the photo pop-up window on the real-time monitoring page.

Function Triggered Result

Modify the default method of obtaining event records to custom or modify the height of the photo pop-up window on the real-time monitoring page to custom.

Steps:

Click **[Elevator] > [Elevator] > [Parameters].**



Type of Getting Transactions:

Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Set the Time for Obtaining New Transactions

The selected time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

8.3. Report

Function List

Functions	Description
All Records	View elevators control all records, clear data, and export function.
All Exception Records	All abnormal record management of elevator control, data can be cleared and export operation.
Query by Floor	View the personnel in the corresponding permission list of the floor and be able to export the corresponding personnel list information.
Query by Personnel	View system personnel's corresponding floor permissions and be able to export corresponding personnel floor information.

8.3.1. All Transactions

Function Description

View the records of all events generated by the current system elevator control module, support clearing data and exporting data. Because the data size of elevator access control event records is large, you can view elevator access control events as specified condition when querying. By default, the system displays the latest three months' transactions.

Clear Data

Preconditions for Normal Use of Function

Not yet.

Function Usage Scenarios

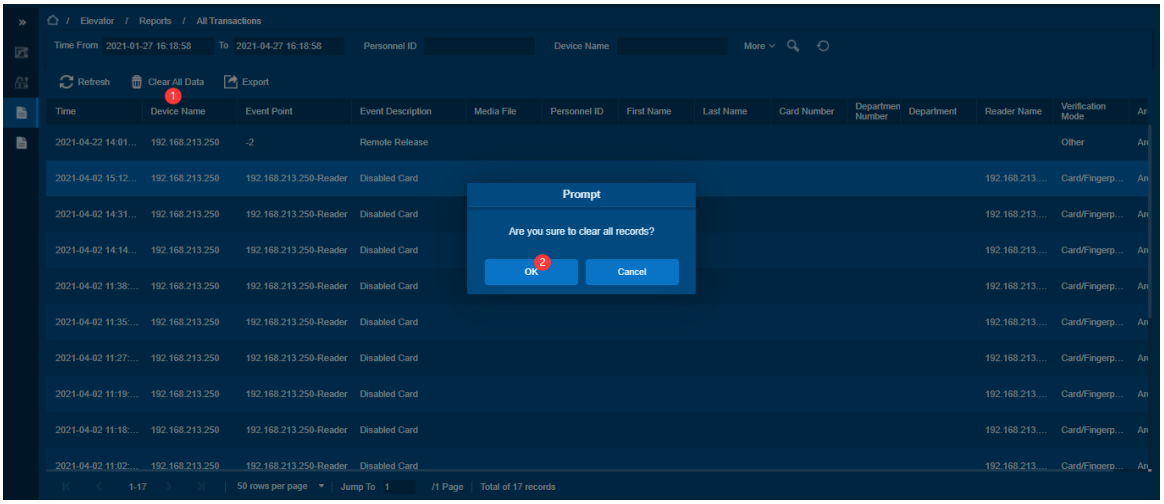
Clear historical data.

Function Triggered Result

Clear all event records of elevator control in the current system.

Steps:

Click **[Clear All Data]** to pop up prompt and click **[OK]** to clear all transactions.



Export

Preconditions for Normal Use of Function

The current system elevator control event record has data.

Function Usage Scenarios

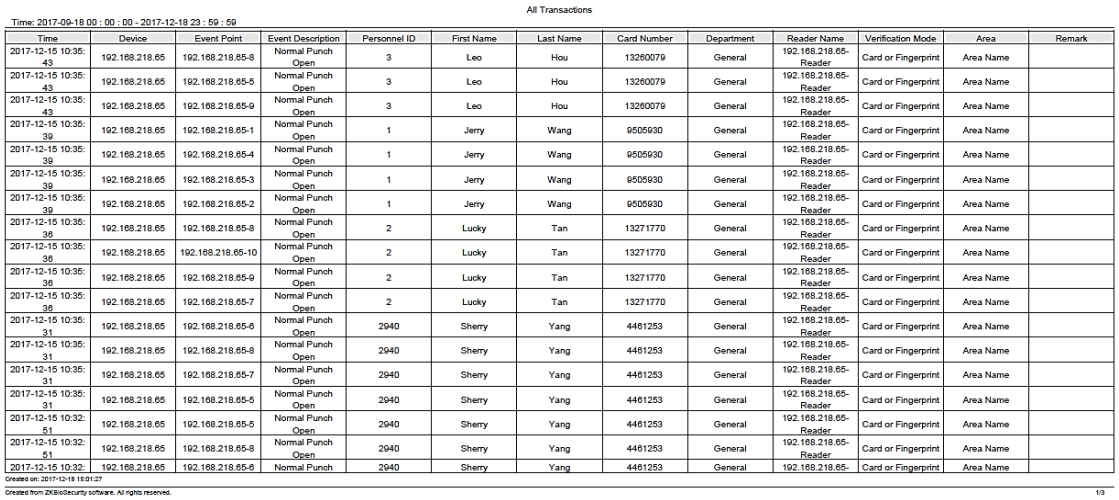
Export data to a local computer for viewing or processing.

Function Triggered Result

The local computer generates an Excel table, and the content of the table is exported data.

Steps:

You can export all transactions in Excel, PDF, CSV format.



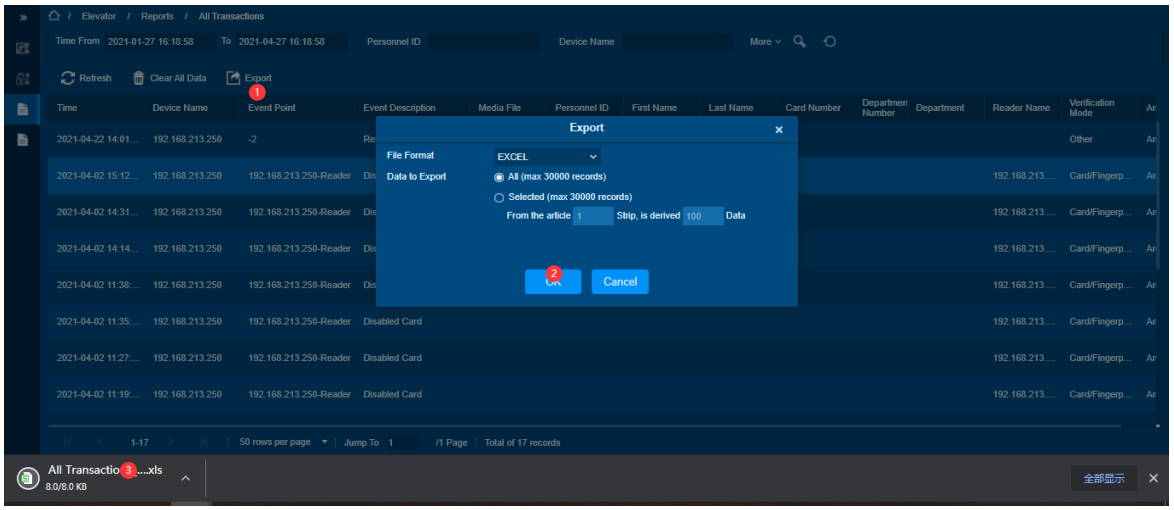
All Transactions

Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

Time	Device	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area	Remark
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-8	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-5	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-9	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-1	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-4	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-3	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-2	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-8	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-10	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-9	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-7	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-6	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-7	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:	192.168.218.65	192.168.218.65-6	Normal Punch	2940	Sherry	Yang	4461253	General	192.168.218.65-	Card or Fingerprint	Area Name	

Created on: 2017-12-18 18:01:27

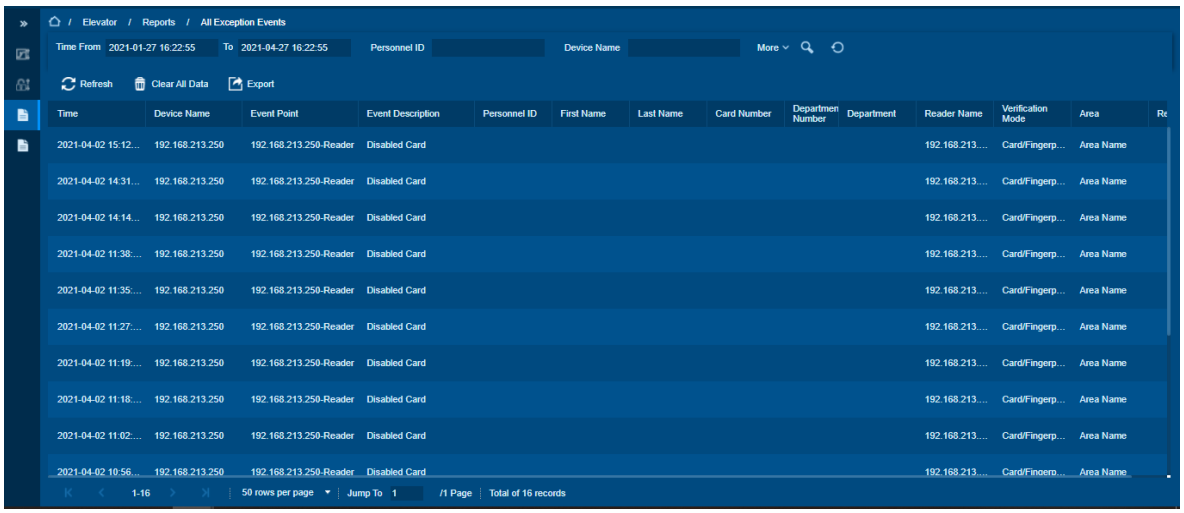
Created from ZKBioSecurity software. All rights reserved. 1/3



8.3.2. All Exception Events

Function Description

- Click **[Reports] > [All Exception Events]** to view exception events in specified condition. The options are same as those of **[All Transactions].**



Clear Data

Preconditions for Normal Use of Function

The current system elevator control event record has data.

Function Usage Scenarios

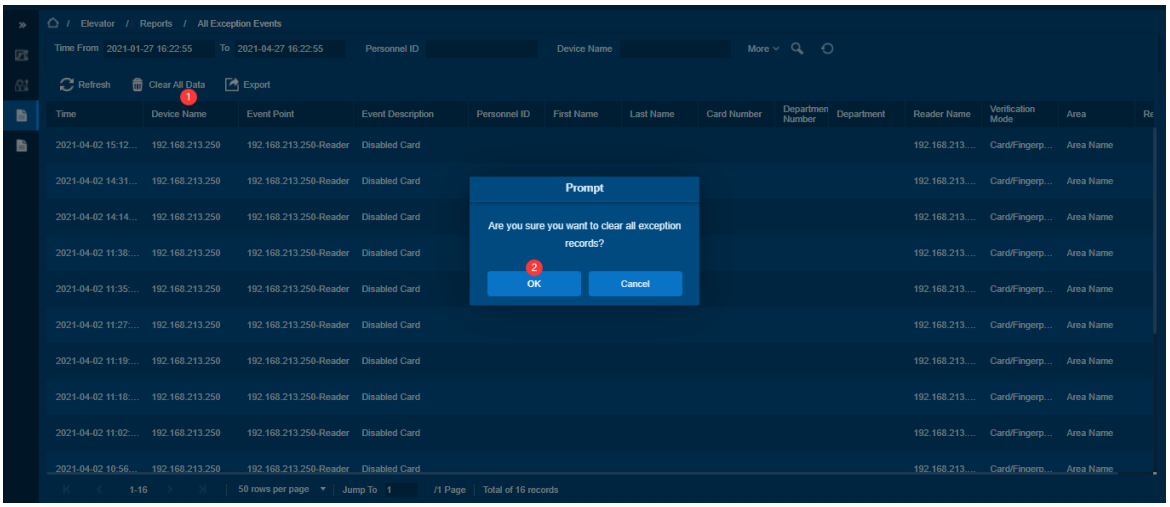
Clear historical data.

Function Triggered Result

Clear all event records of elevator control in the current system.

Steps:

- Click **[Clear All Data]** to pop up prompt, click **[OK]** to clear all exception events.



Export

Preconditions for Normal Use of Function

The current system elevator control event record has data.

Function Usage Scenarios

Export data to a local computer for viewing or processing.

Function Triggered Result

The local computer generates an Excel table, and the content of the table is exported data.

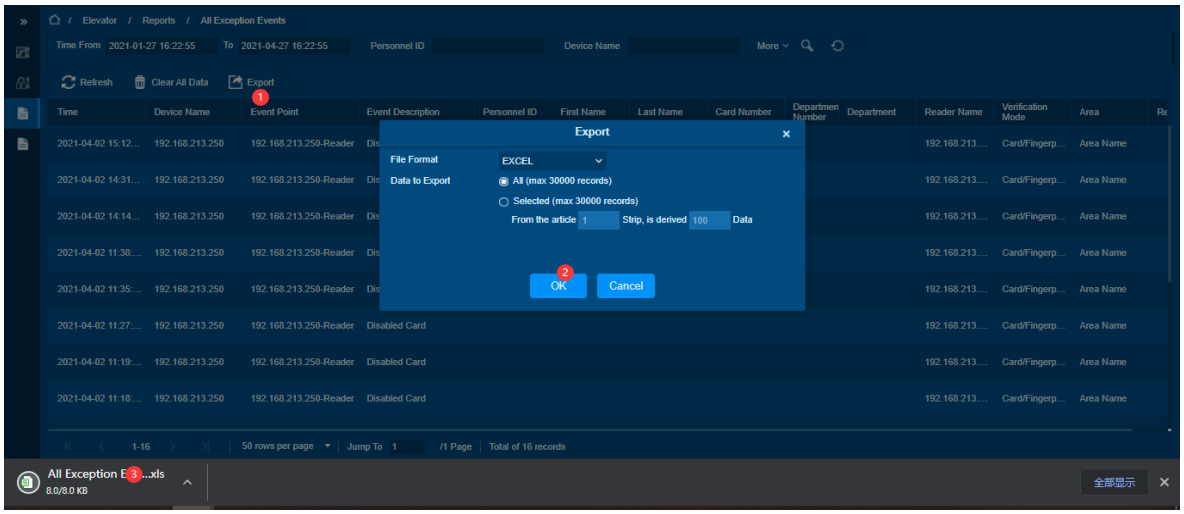
Steps:

You can export all exception events in Excel, PDF, CSV format.

All Exception Events

Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Department	Reader Name	Verification Mode	Remark
2017-12-15 10:29:11	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	9505930	1	Jerry	Wang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:14	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	4461253	2940	Sherry	Yang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Operate Interval too Short	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	



8.3.3. Access Rights By Floor

Function Description

View related access levels by door. Click [Reports] > [Access Rights by Floor], the data list in the left side shows all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.

Export

Preconditions for Normal Use of Function

Query personnel floor access rights.

Function Usage Scenarios

Export data associated with elevator control floors and personnel information to local.

Function Triggered Result

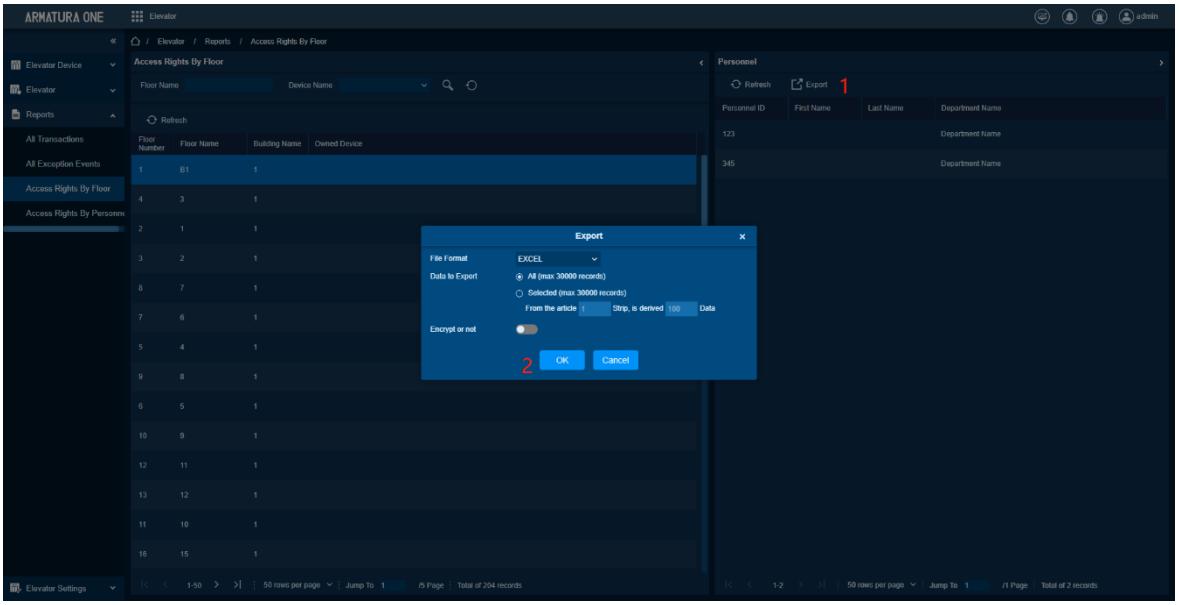
Save locally generated files.

Steps:

You can export all the personnel having access levels to the floor data in Excel, PDF, CSV format.

192.168.218.65-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department



8.3.4. Access Rights By Personnel

Function Description

Click [Reports] > [Access Rights by Personnel], the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

Export

Preconditions for Normal Use of Function

Personnel have corresponding floor authority.

Function Usage Scenarios

Export the floor information corresponding to the personnel to the local computer.

Function Triggered Result

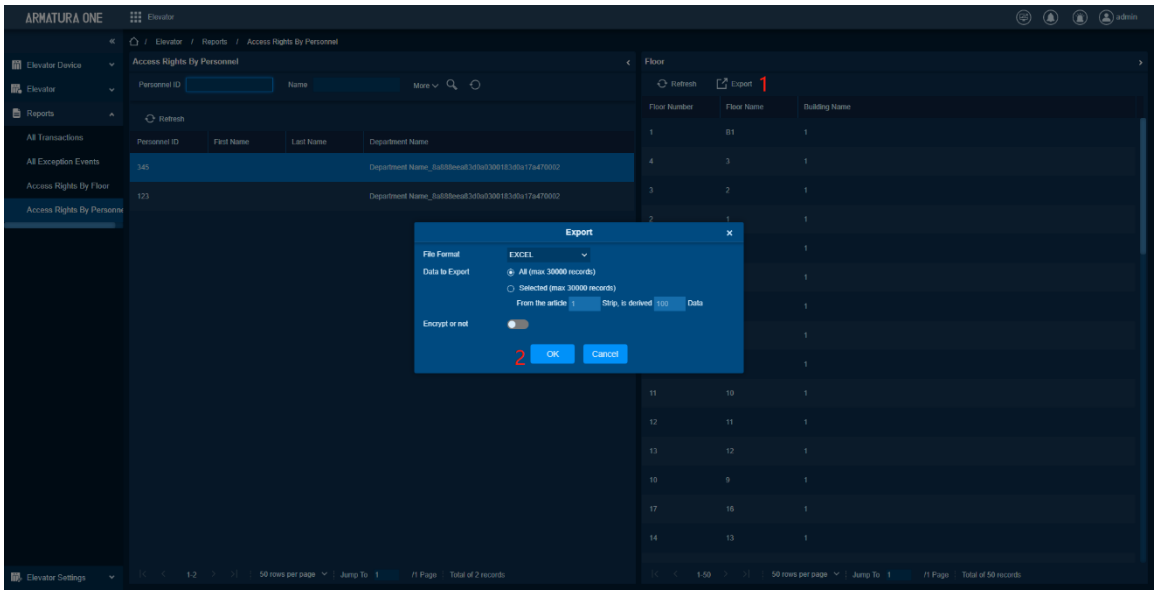
Generate export data files locally.

Steps:

You can export all the floor information in Excel, PDF, CSV format.

2940(Sherry) Having Level to Access

Floor Number	Floor Name
1	192.168.218.65-1
2	192.168.218.65-2
3	192.168.218.65-3
4	192.168.218.65-4
5	192.168.218.65-5
6	192.168.218.65-6
7	192.168.218.65-7
8	192.168.218.65-8
9	192.168.218.65-9
10	192.168.218.65-10



8.4. Elevator Settings

Function List

Functions	Description

Integrated Device	Add and delete access control device integrated elevator control module.
Elevator Group	Add, edit, delete elevator group configuration, add, edit, delete elevator.
External Reader	Add, edit, delete reader, configure template, clear template.
Internal Reader	Add, edit, delete reader, configure template, clear template.
Operation Log	View operation records with third-party elevator control systems.

8.4.1. Integration Device

Function Description

Add access control device to the elevator control module and provide the elevator control docking to verify the access control authority to use the elevator function.

Add

Preconditions for Normal Use of Function

Add Access Control Device

Function Usage Scenarios

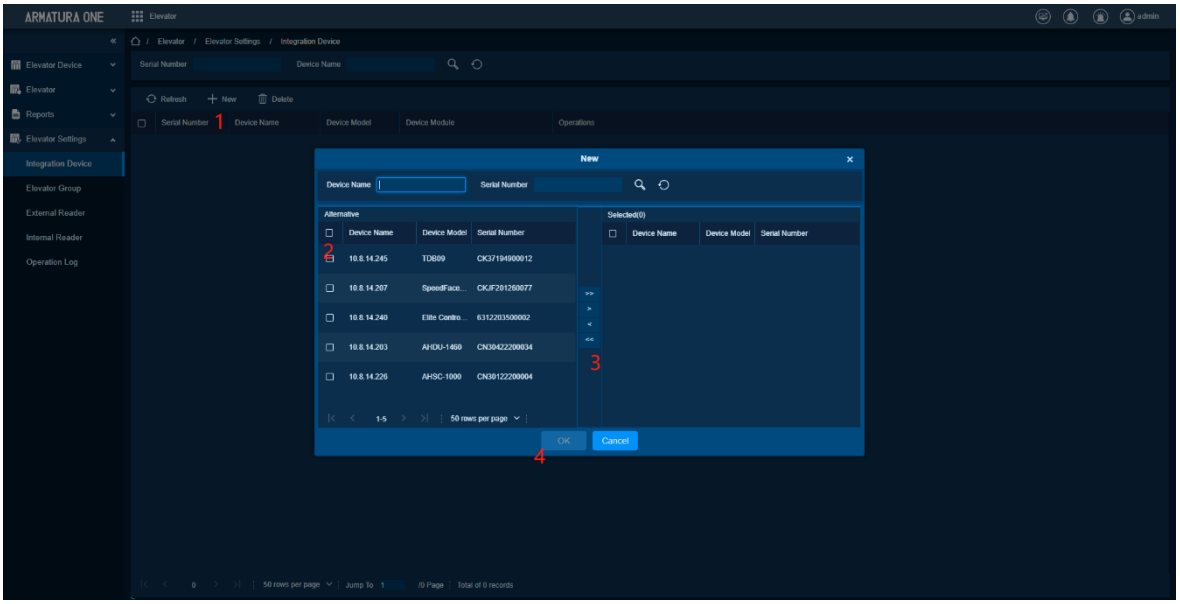
The door of the access control device is bound with external reader or internal reader for access control permission verification, and then directly call the elevator to take the elevator.

Function Triggered Result

Add the access control device to the current menu.

Steps:

- Click Add, a double list pops up to select the access control device.
- Select the corresponding access control device, click **OK.**



Delete

Preconditions for Normal Use of Function

- Choose Access Control Device.
- The door information of the selected access control device is not bound to the external reader.
- The door information of the selected access control device is not bound to the internal reader.

Function Usage Scenarios

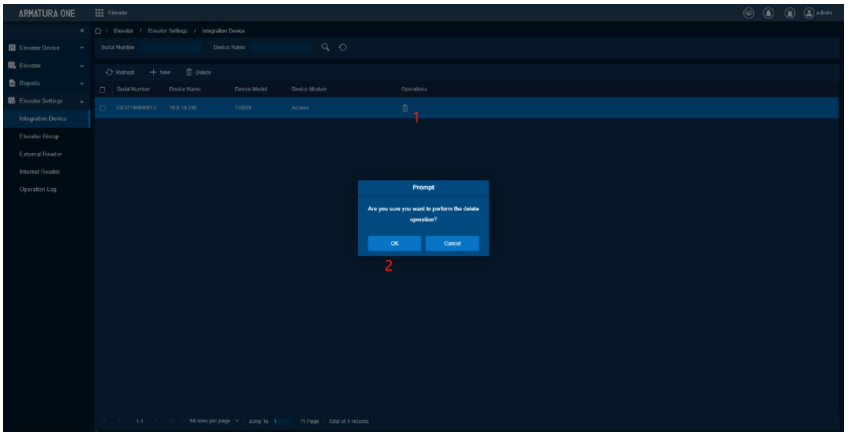
Access control device is not used.

Function Triggered Result

Delete the associated information of the selected access control device and elevator control module.

Steps:

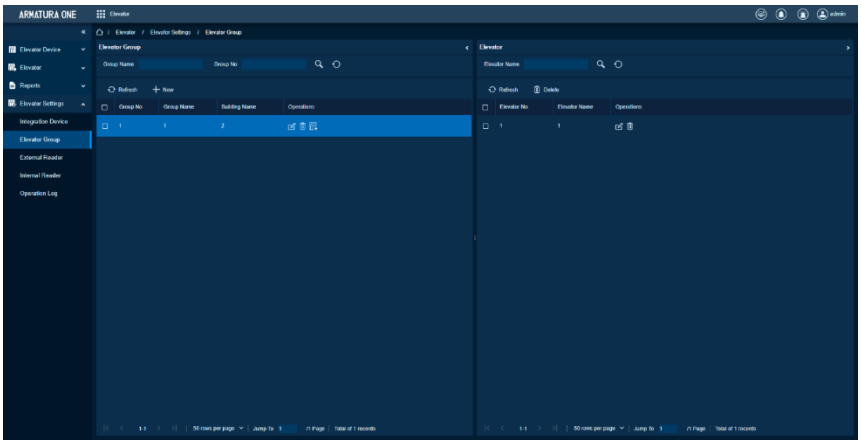
- Select the device, click **[Delete]** button.
- On the pop-up interface, click **[OK].**



8.4.2. Elevator Group

Function Description

This function is to create elevators and elevator groups, and associate elevators with buildings.



Add Elevator Group

Preconditions for Normal Use of Function

System adds building information.

Function Usage Scenarios

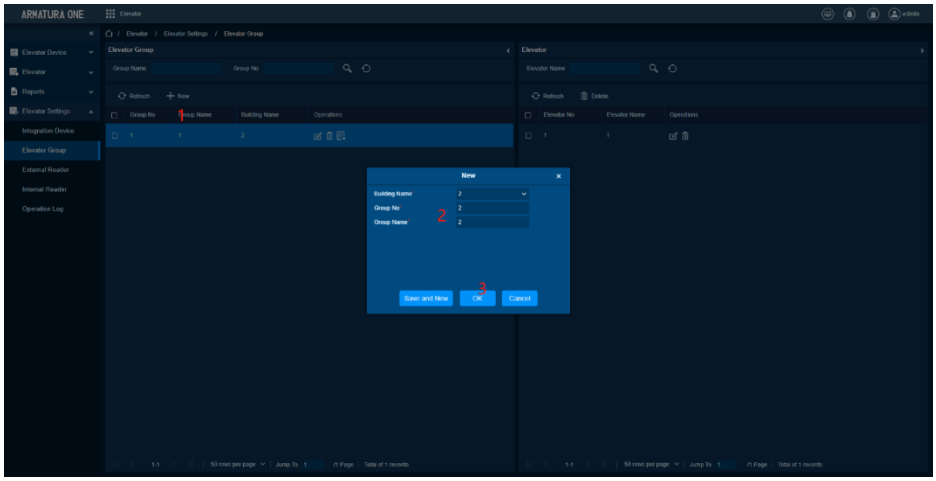
Add building binding elevator group settings.

Function Triggered Result

Add an elevator group data.

Steps:

- Click **[Add]** button, a window will pop up, fill in the group number and group name, select the corresponding building information
- Click **[OK].**



Delete Elevator Group

Preconditions for Normal Use of Function

- Currently elevator group does not have elevator binding.
- The current elevator group or elevator is not bound to internal reader information.

Function Usage Scenarios

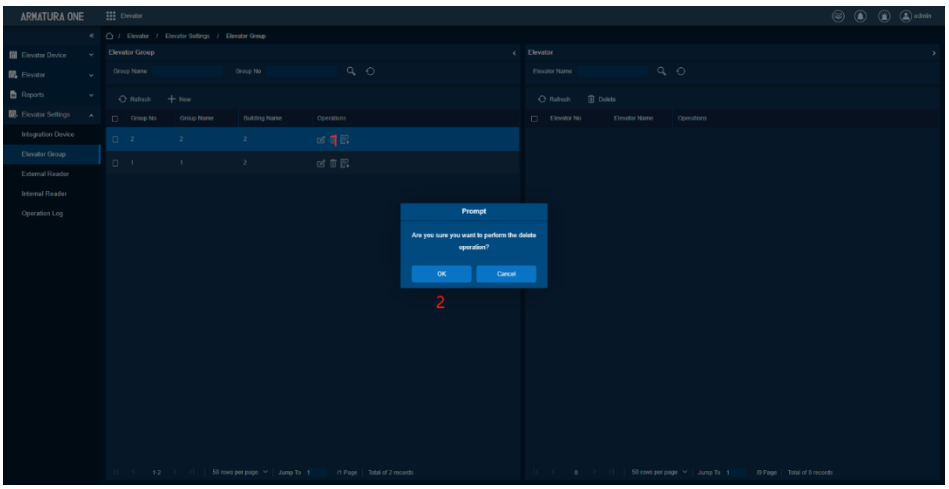
Elevator group does not use or requires delete.

Function Triggered Result

Delete the currently selected elevator group information.

Steps:

Click the **"Delete"** button in the operation bar to delete the elevator group.



Add Elevator

Preconditions for Normal Use of Function

Add elevator group information.

Function Usage Scenarios

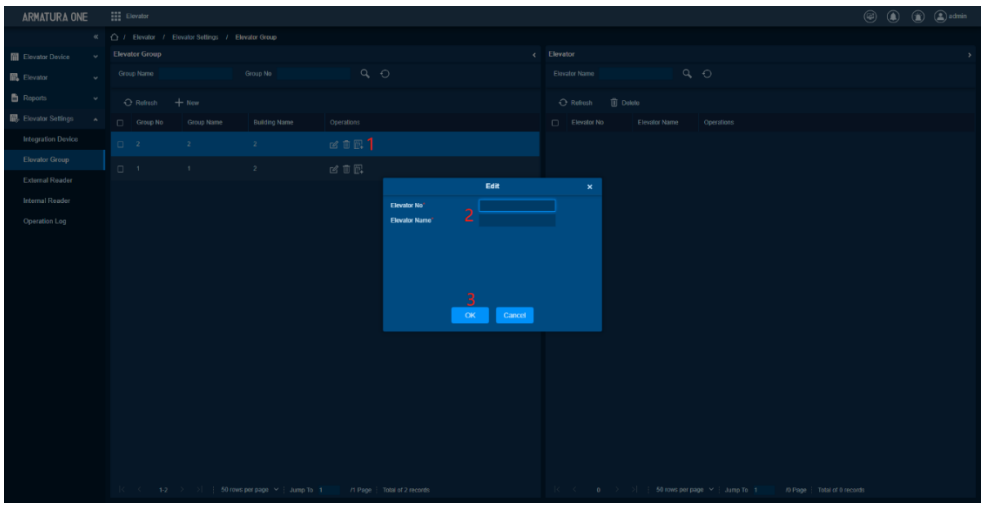
Add elevator group elevator, provide internal reader for binding use.

Function Triggered Result

Add an elevator information for the specified elevator group.

Steps:

- Click the **[New Elevator]** button in the operation bar to add an elevator.



Elevator No: Set elevator number. Elevator Numbers are not repeatable and are significant Numbers.

Elevator Name: Name of the new elevator.

Delete Elevator

Preconditions for Normal Use of Function

The elevator is not bound with internal reader.

Function Usage Scenarios

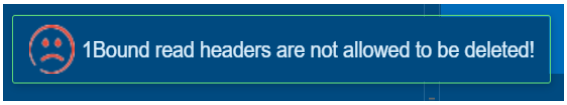
Elevator data does not need to be used or delete.

Function Triggered Result

Delete the currently selected elevator data.

Steps:

Click the **"Delete"** button in the operation bar to delete the elevator.



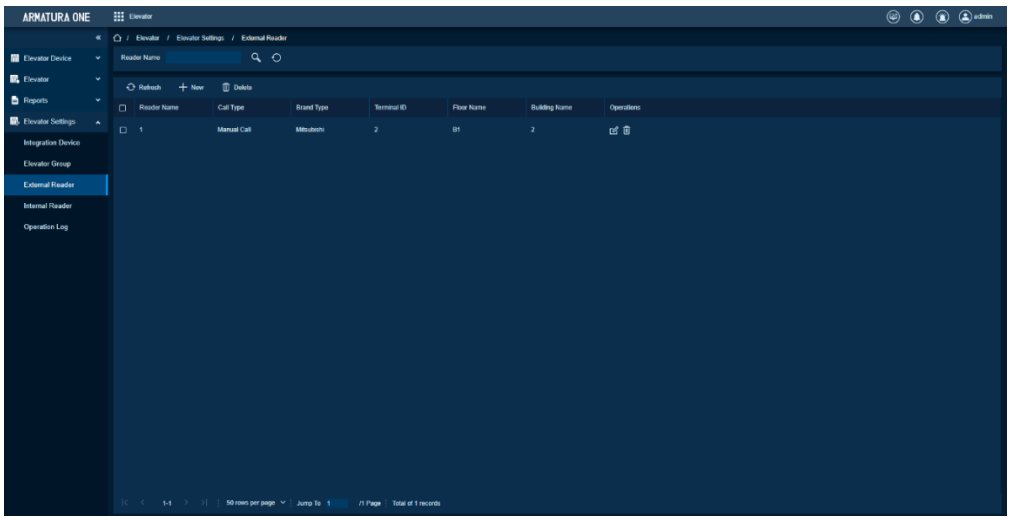
✍**Note:**

The elevator cannot be deleted when the elevator has a bound internal reader.

8.4.3. External Reader

Function Description

Click **[Elevator Settings] > [External Reader]**. The edited external read page displayed on the current page. Using the system, you can manage and edit the connection between external reader and buildings and set the default floor and call mode. Each elevator call type is different from the building to which it is bound.



Add External Reader

Preconditions for Normal Use of Function

- Need to add access control device.
- Need to choose door reader.
- Need to add building floor information.

Function Usage Scenarios

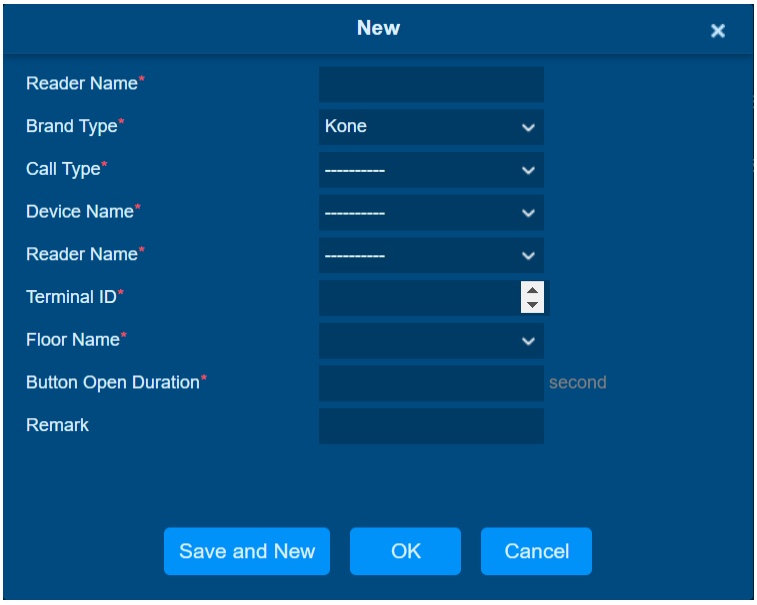
Add the information associated with the access control device to form external reader.

Function Triggered Result

Generate an external reader data message.

Steps:

- Click **[Elevator Settings]** > **[External Reader]** > **[NEW]** to add new external reader.



Reader Name: Name of the external reader displayed on the list page.

Brand Type: Select different elevator brands and the corresponding brand names will be listed. such as KONE, Mitsubishi, Hitachi, Schindler, Otis.

Call Type: Depending on the brand type of elevator chosen, there are different call types.

Elevator Type	Type of Call	Description
KONE	Normal Call	Normal call
	RCGIF Call	DOP Side
Mitsubishi	Manual Call	Manual call (for the VIP or the everyman)
	Auto Call	Automatic call (for the disabled)
Hitachi	Manual Call	Manual call (for the VIP or the everyman)
	Auto Call	Automatic call (for the disabled)

Device Name: Select the added integration device.

Reader Name: Select the reader from integration device.

Terminal ID: Set the terminal ID. Each elevator brand type must have a non-repeatable terminal ID and a significant number that can only range from 1 to 255.

Floor Name: Select the floor in the bound building.

Button Open Duration: It is used to control the time to press floor button after verification. The default value is 5 seconds; the range is 0~254 seconds.

Delete External Reader

Preconditions for Normal Use of Function

Delete an external reader.

Function Usage Scenarios

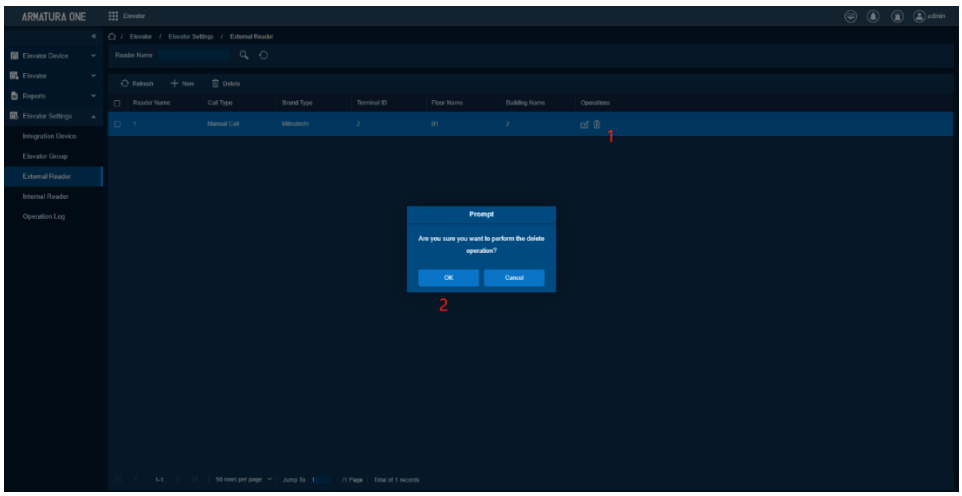
Currently external reader is not used or requires delete.

Function Triggered Result

Delete the currently selected external reader information.

Steps:

Click the delete button of the list data, a confirmation box pops up, click ok, the operation is complete.



Set Template

Preconditions for Normal Use of Function

Add external reader information

Select the external reader information that needs to be set.

Function Usage Scenarios

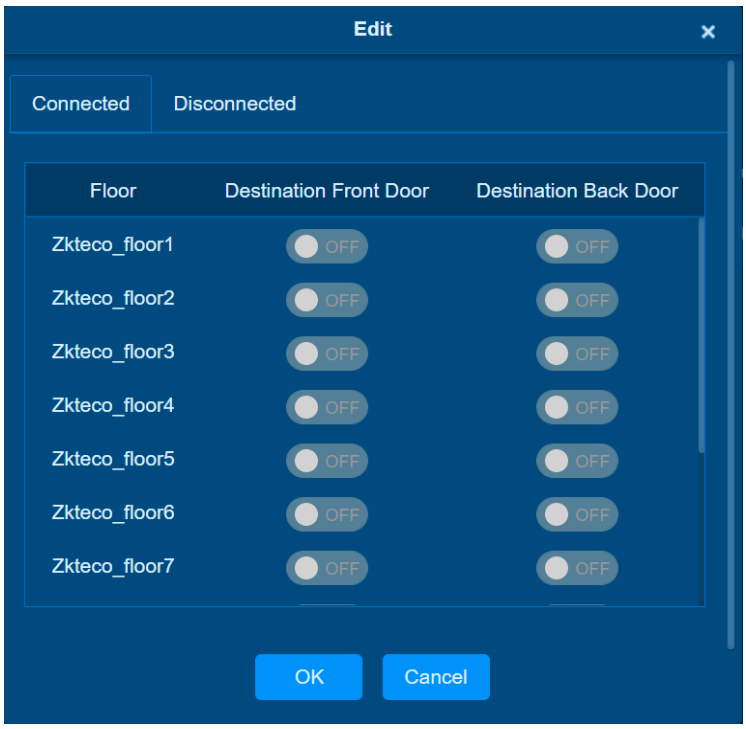
Set the external reader to configure the opening and closing status of the door before and after arriving on the floor and support the configuration of the online and offline status settings of the device.

Function Triggered Result

Set the open status of the front and rear doors on the arrival floor when the current external reader is online and offline and send it to the third-party elevator control system.

Steps:

Set a particular reader template that takes precedence over the building's generic template, or default to the building's generic template if it is not set or clear.



Clear Template

Preconditions for Normal Use of Function

Select the corresponding external reader information.

Function Usage Scenarios

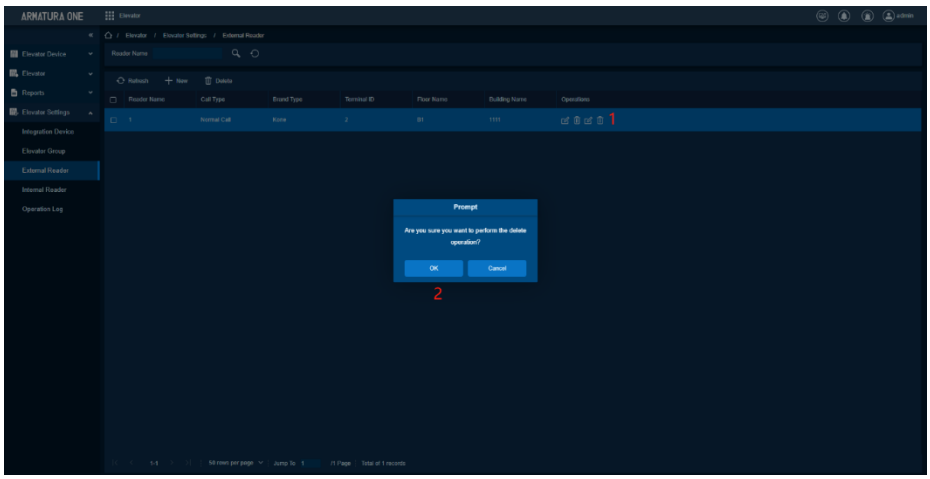
Empty or reset the external reader template.

Function Triggered Result

Clear the currently configured external reader template information and send it to the third-party elevator control system.

Steps:

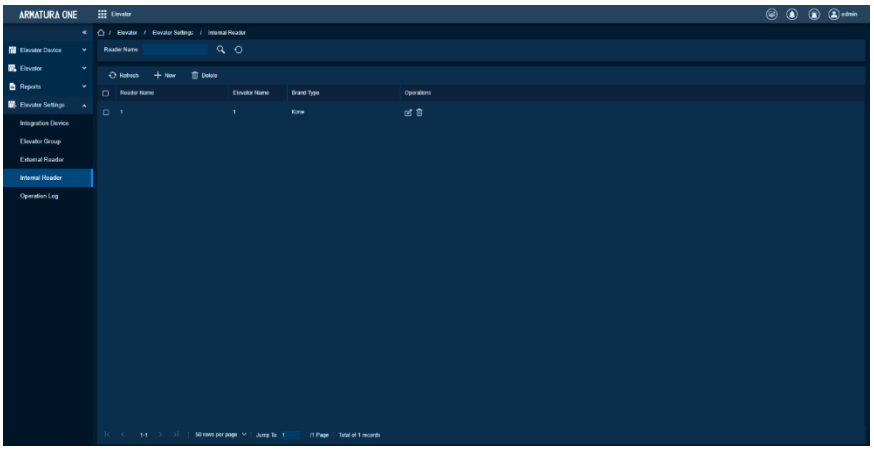
- Select the Reader Name, click **"Clear Template"** button.
- On the pop-up confirmation box, click **OK.**



8.4.4. Internal Reader

Function Description

This feature can be configured to bind the Internal Reader inside the elevator to the corresponding elevator in the Elevator Group.



Add Internal Reader

Preconditions for Normal Use of Function

- Need to add elevator data.
- Need to add access control device.
- Need to choose door reader information.

Function Usage Scenarios

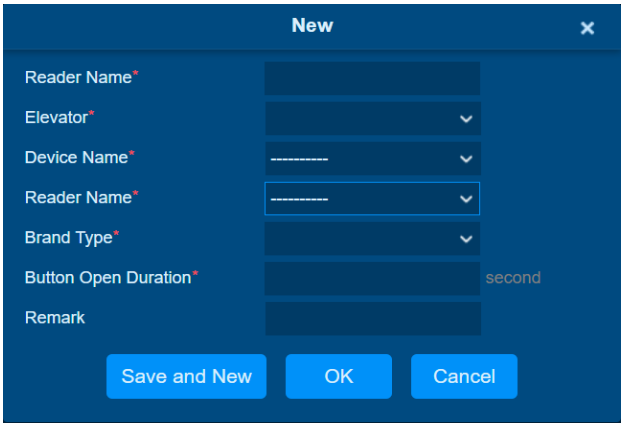
Add the information associated with access control device and elevator data to form internal reader information.

Function Triggered Result

Add an internal reader data message.

Steps:

- Click **[Elevator Settings] > [Internal Reader] > [New]**.



Reader name: Name of the Internal reader displayed on the list page.

Elevator: The data source comes from the corresponding elevator group and elevator added to the elevator group.

Device Name: The device name is derived from the integration device and is obtained by adding the integration device.

Reader Name: Select the reader from device.

Brand Type: Set brand type as Kone, Mitsubishi, Hitachi, Schindler, Otis and so on.

Button Open Duration: It is used to control the time to press floor button after verification. The default value is 5 seconds; the range is 0 to 254 seconds.

Remark: Add the remark**.**

Delete Internal Reader

Preconditions for Normal Use of Function

Not yet.

Function Usage Scenarios

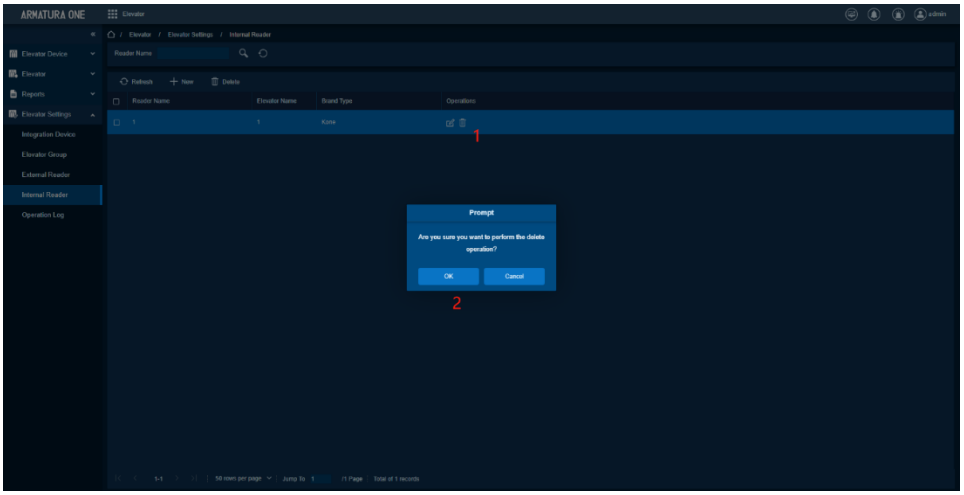
The current internal reader is no longer used or needs delete.

Function Triggered Result

Select the internal reader information and delete it.

Steps:

- Select the Reader name, click **Delete.**
- On the pop-up interface, click **OK**.



Set Template

Preconditions for Normal Use of Function

Add internal reader information.

Function Usage Scenarios

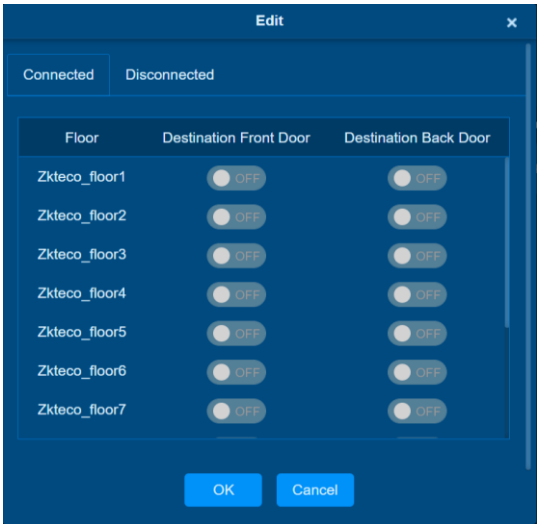
Set the internal reader to configure the opening and closing status of the door before and after arriving on the floor and support the configuration of the online and offline status settings of the device.

Function Triggered Result

Set the open status of the front and rear doors of the arrival floor when the current internal reader is online and offline, and sent it to the third-party elevator control system.

Steps:

Set a particular reader template that takes precedence over the building's generic template, or default to the building's generic template if it is not set or clear.



Clear Template

Preconditions for Normal Use of Function

Select the corresponding internal reader information.

Function Usage Scenarios

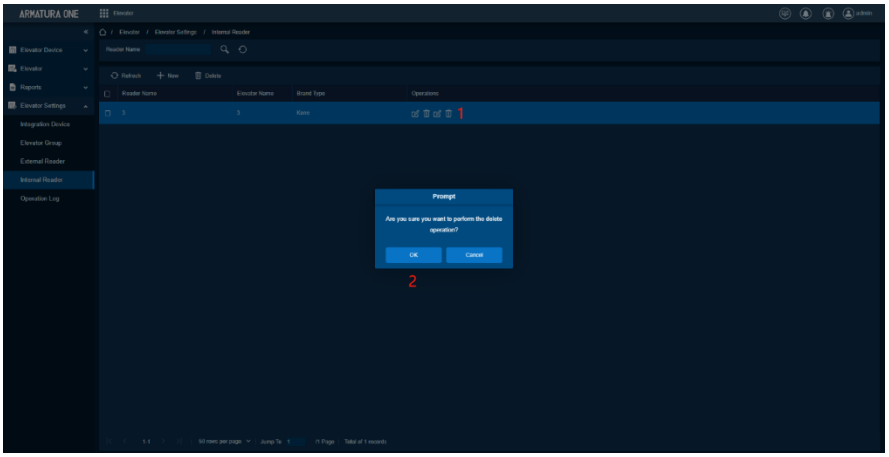
Empty or reset the external reader template.

Function Triggered Result

Clear the data information of the currently selected internal reader template.

Steps:

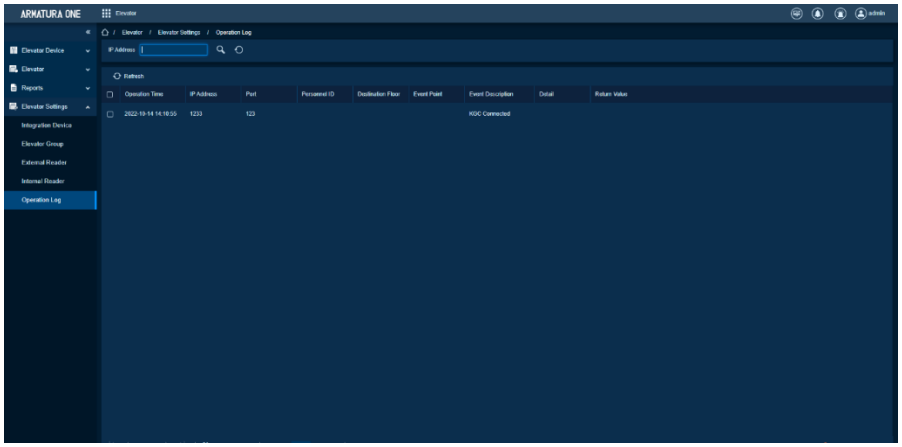
- Select the Reader Name and click **Delete.**
- A confirmation box will pop up, click **OK** to delete.



8.4.5. Operation Log

Function Description

- Click **[Elevator Settings] > [Operation Log]** to query and view all operation records of elevator equipment (such as heartbeat check, device connection status, elevator arrival to default floor, etc.)



9. Visitor Management

The visitor module conducts unified management of foreign visitors, including visitor status management, visitor reservation, visitor authority setting, device management and parameter configuration during visitor registration, etc.

9.1. Registration

Function List

Functions	Description
Visitor Registration	Visitor registration, check-out, batch registration, batch check-out, visitor cloning.
Visitor Information	Guests delete, add to blocklist, remove from banned list, export.

9.1.1. Entry Registration

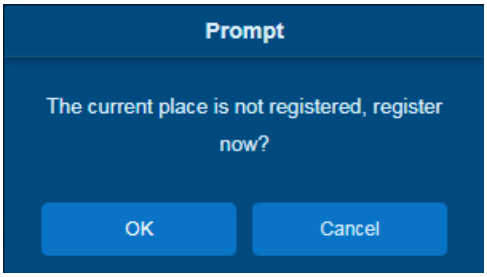
Entry Registration

Function Description

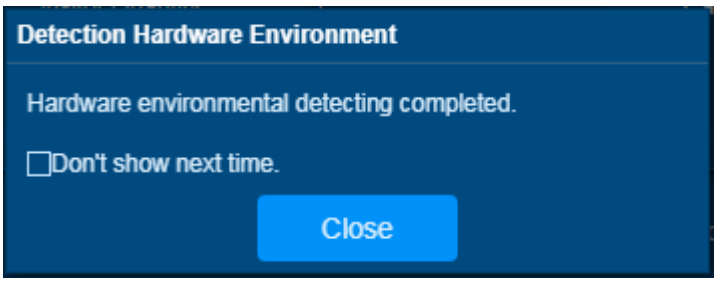
Perform operations such as check-in, check-out, batch check-in, batch check-out, and visitor cloning for visitors.

Preconditions for Normal Use of Function

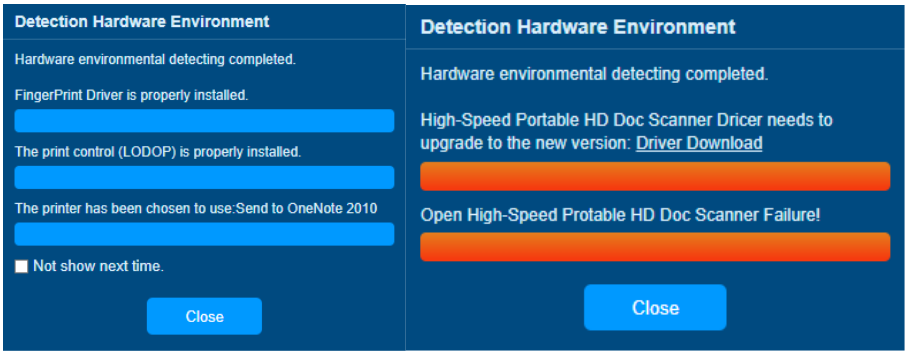
1. After clicking **[Guest],** the following window will pop up.
2. Click **[OK]** to use the current location IP as the registration location IP. For more information on where to register, see where to register.



3. Click **[Guest Registration]** button, the system will check the hardware environment according to the parameters of **[Parameters Setting]** in **[Basic Management]** before entering the registration page.



4. After the detection is completed, click **[Close]** to continue registration, as shown in the left figure below. If the test fails, please click **[Close],** the system will prompt to download the driver, click **[Close]** to close the registration window, as shown in the right figure below.



Function Usage Scenarios

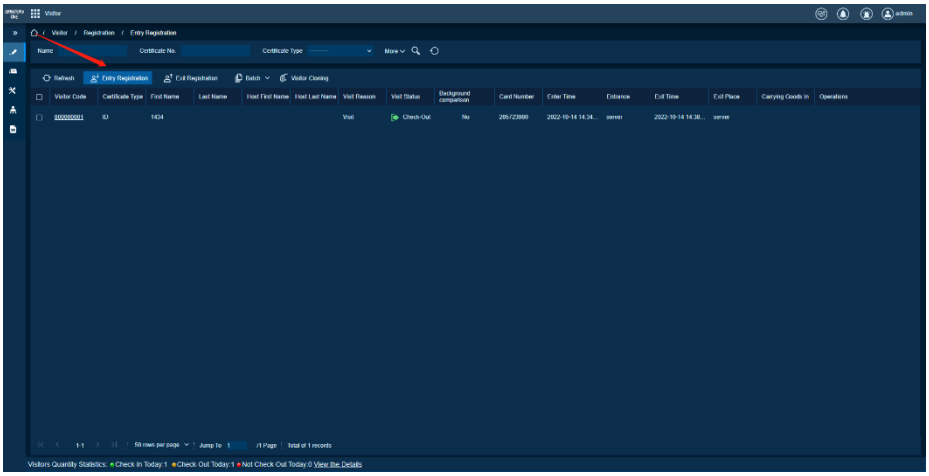
The visitor registration function is used for individual visitors to perform guest registration and registered visitors to perform registration.

Feature Trigger Result

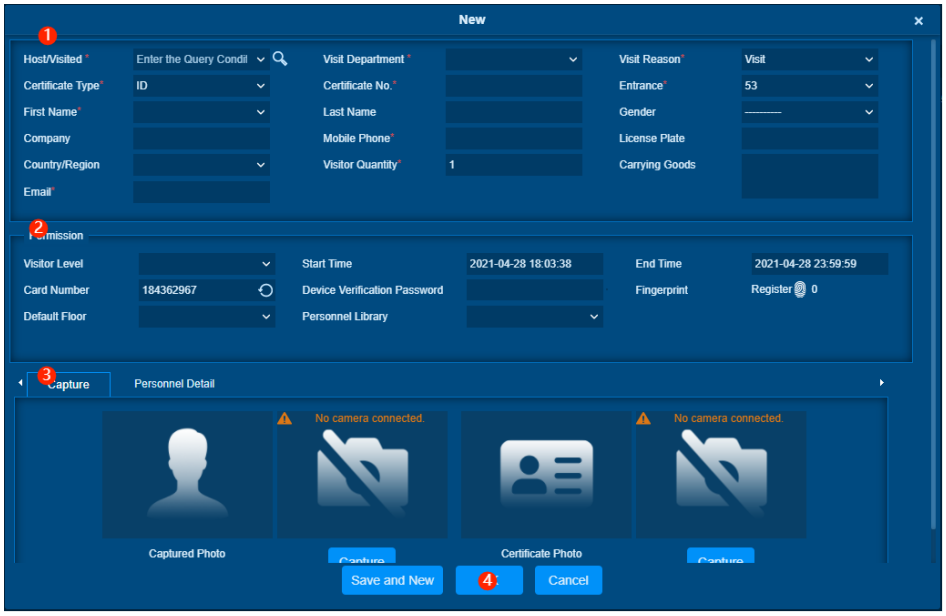
Operations	Description
Personnel Pool Selection	Omni visitor information to the corresponding personnel list database.
Guest Permission Selection	Add visitors to the corresponding module permission, such as access level, elevator level and so on. When the permission has device, the personnel information will be sent to the corresponding module device.
Click OK Button	Add the visitor to the visitor registration list and visitor information list.

Steps:

1. Click **[Entry Registration]** on the visitor registration interface, and the visitor registration window will pop up.



2. After entering the visitor registration interface, fill in the relevant information. The items marked with * are required, and the items without * are optional.
3. After filling in the information, click the **OK** button and a prompt indicates that the visitor registration is successful.
4. You can also enter the successfully reserved items of the visitor's certificate number and certificate type are filled in with the visitor's information for registration.



Exit Registration

Preconditions for Normal Use of Function

The guest check-out operation can only be performed on visitors whose guest status is visited or check-out timeout, and only one person can check-out at a time.

Function Usage Scenarios

The visitor check-out function is used for a single visitor to perform a check-out operation.

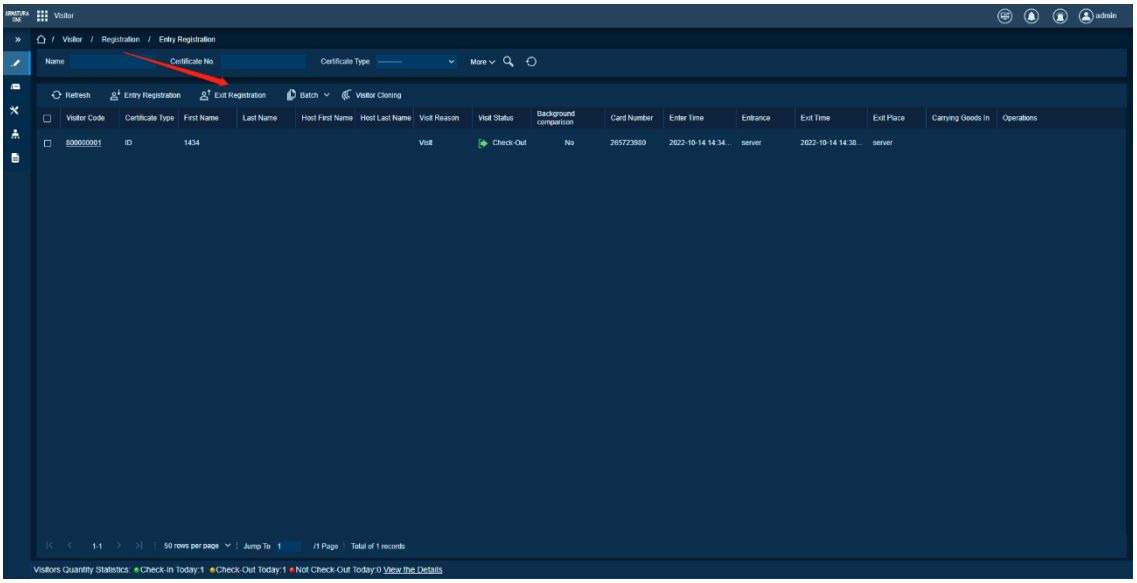
Feature Trigger Result

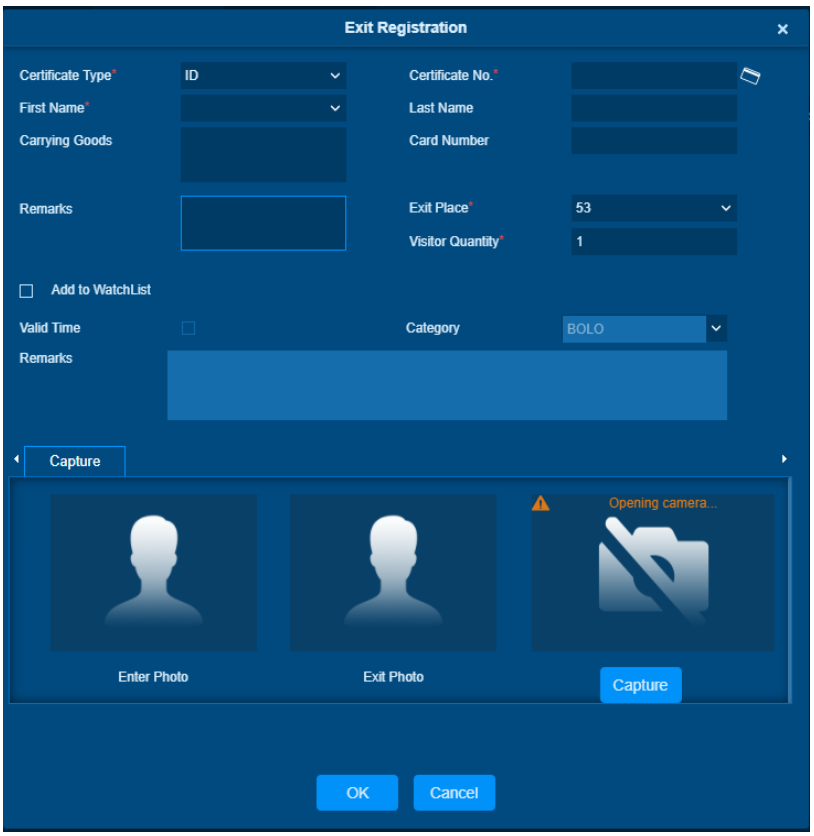
Operations	Description
Check to Add to the Monitoring List	Select the monitoring time and type. Visitors will be prompted in the monitoring list when they register again during the monitoring time.
Click the Snapshot Button for Taking Photos of the ID Card	Snap a photo of the visitor when they sign out.
Click the OK Button	Complete the guest check-out operation.

Steps:

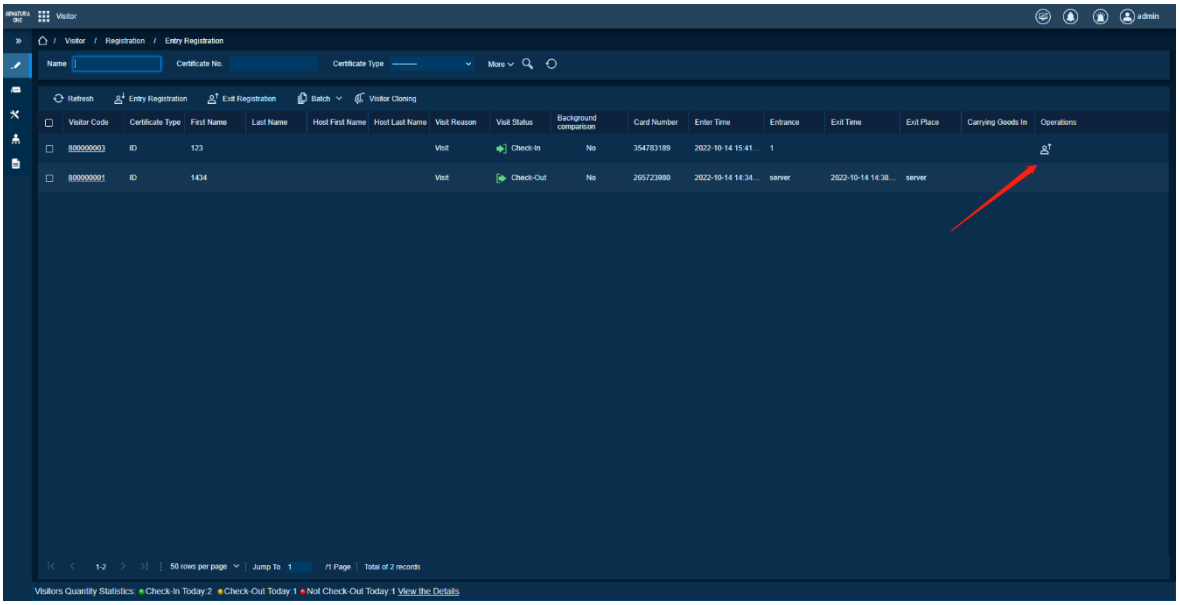
There are two ways for a single visitor to sign out.

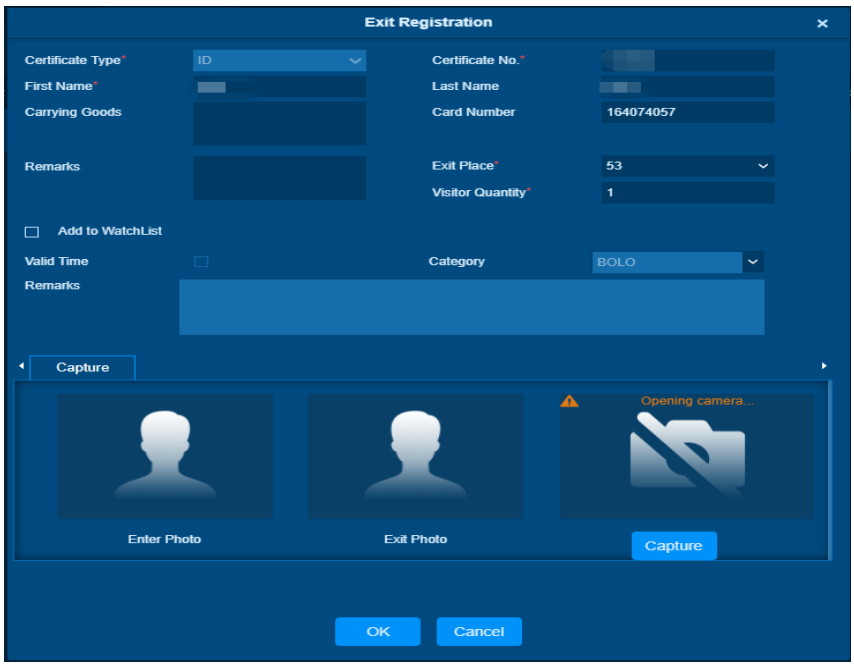
Method 1: Click the Check-out button, the visitor check-out window pops up, enter the certificate type and certificate number to fill in the visitor information, and then perform the check-out operation.





Method 2: Click the Check-out button in the visitor information operation column, and the visitor Check-out window pops up. You do not need to enter the **Certificate Type** and **Certificate Number** to directly fill in the visitor information, and then perform the check-out operation.





Whether to add to the monitoring list and snapshot photo is optional. After filling in the relevant information, click **[OK].** If prompt “The operation succeeded.” It means that the visitor has successfully checked out.

Batch Check-in

Preconditions for Normal Use of Function

It is used when there is visitor reservation information, and the reservation status is future visit.

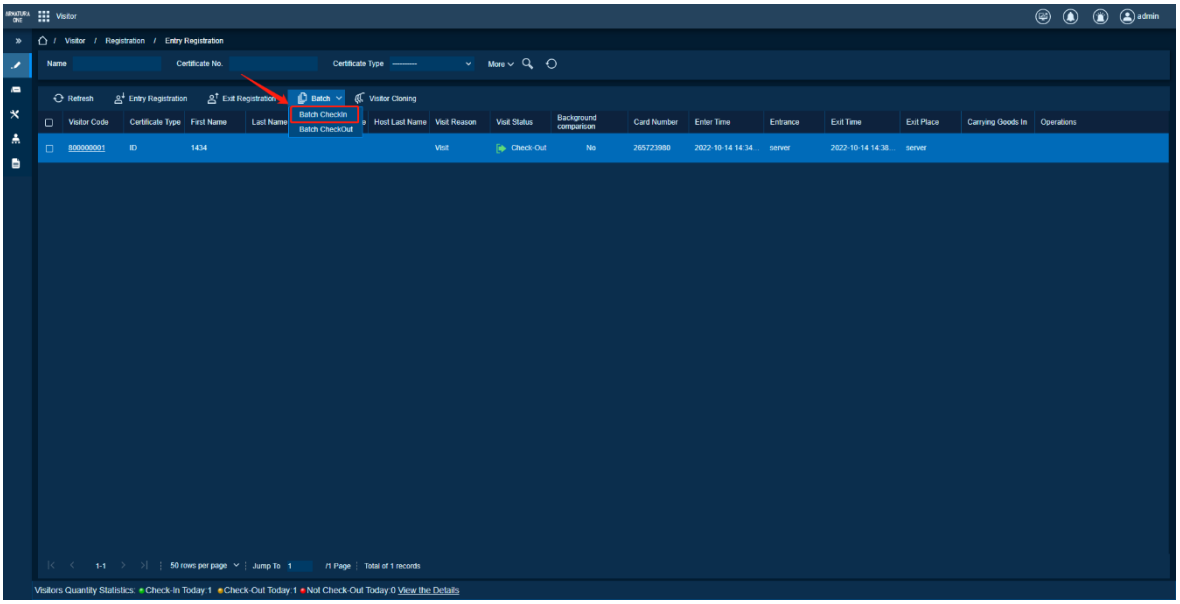
Function Usage Scenarios

It is used when the same group of visitors is successfully reserved for registration or when a single visitor is successfully reserved for registration.

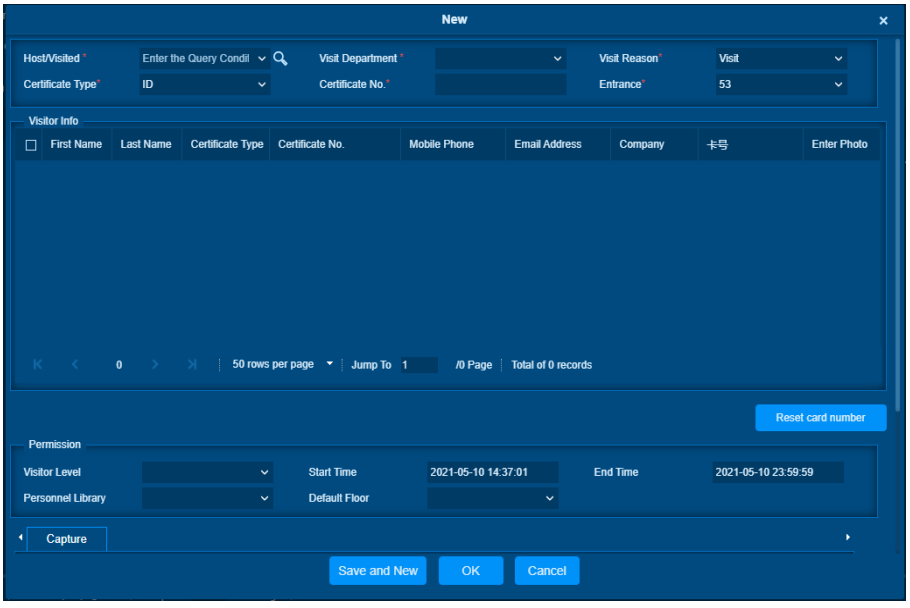
Feature Trigger Result

Operations	Description
Click Reset Card Number	Reset the card number information of all visitors.
Click the Snapshot Button for Taking Photos of the ID Card	Select a visitor and click the capture button to capture the visitor’s entry photo.
Personnel Pool Selection	Push visitor information to the corresponding personnel list database.
Guest Permission Selection	Add visitors to the corresponding module permission. When the permission has device, the personnel information will be sent to the corresponding module device.

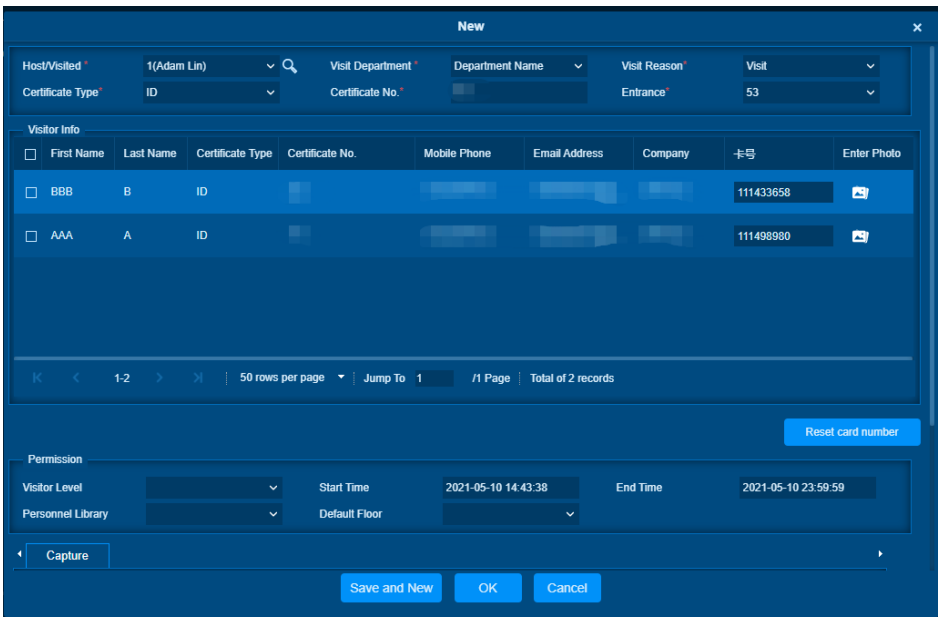
Steps:



1. Click **[Batch]** drop-down box and click the **[Batch Check-In]** in the pop-up drop-down box to enter the batch registration interface.



You can manually enter the certificate number and certificate type of the person who made the reservation to fill in the visitors who are reserved in the same batch, or you can use the device to identify the certificate to fill in the visitors who are reserved in the same batch.



After bringing out all the visitor information of the same batch of reservations, click one of the visitor information, click **Capture** button, you can capture the visitor's entry photos, set unified permissions and personnel database for all visitors of the same batch, check the visitors who need to sign in, and click **[OK]** complete the batch check-in operation.

Batch Check-out

Preconditions for Normal Use of Function

In the current visitor information, visitors whose visitor status is registered can perform batch check-out operations.

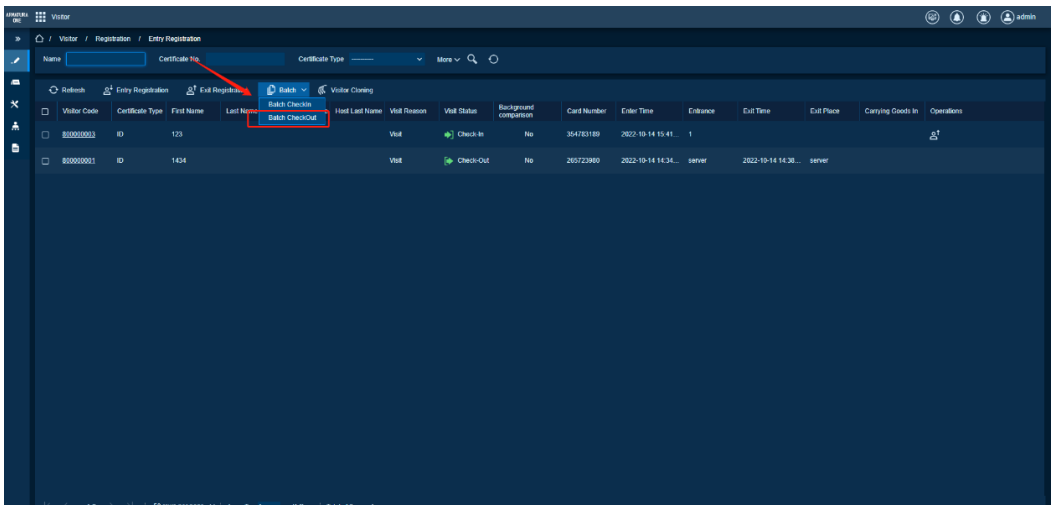
Function Usage Scenarios

The batch check-out operation can support a single visitor check-out or a unified check-out of the same batch of visitors.

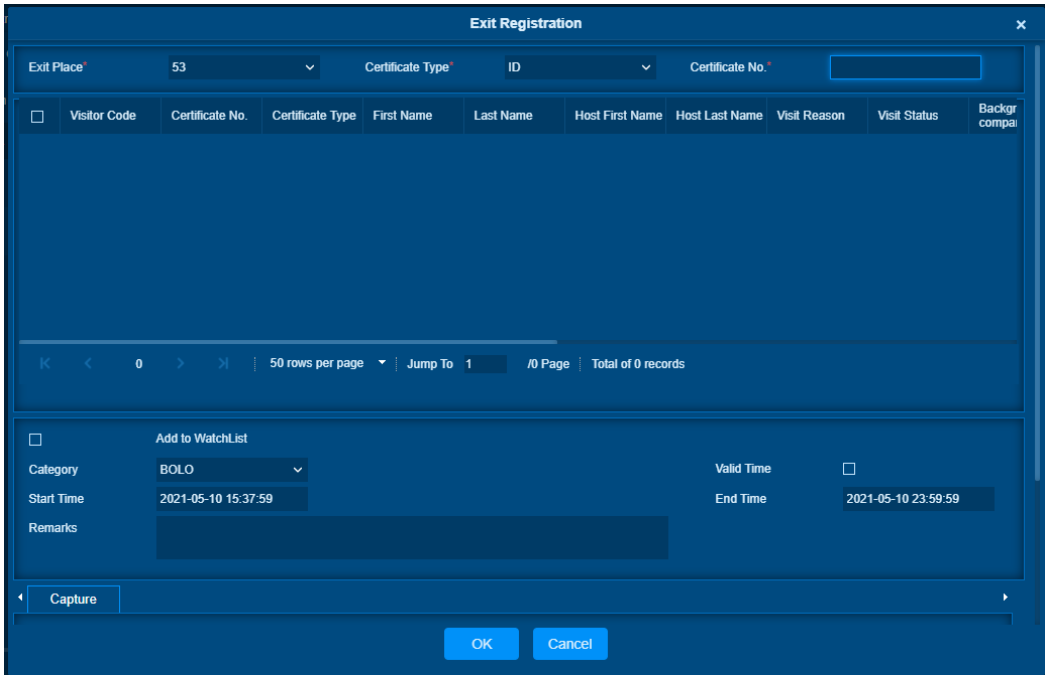
Feature Trigger Result

Operations	Description
Check to Add to the Monitoring List	Select the monitoring time and type. Visitors will be prompted in the monitoring list when they register again during the monitoring time.

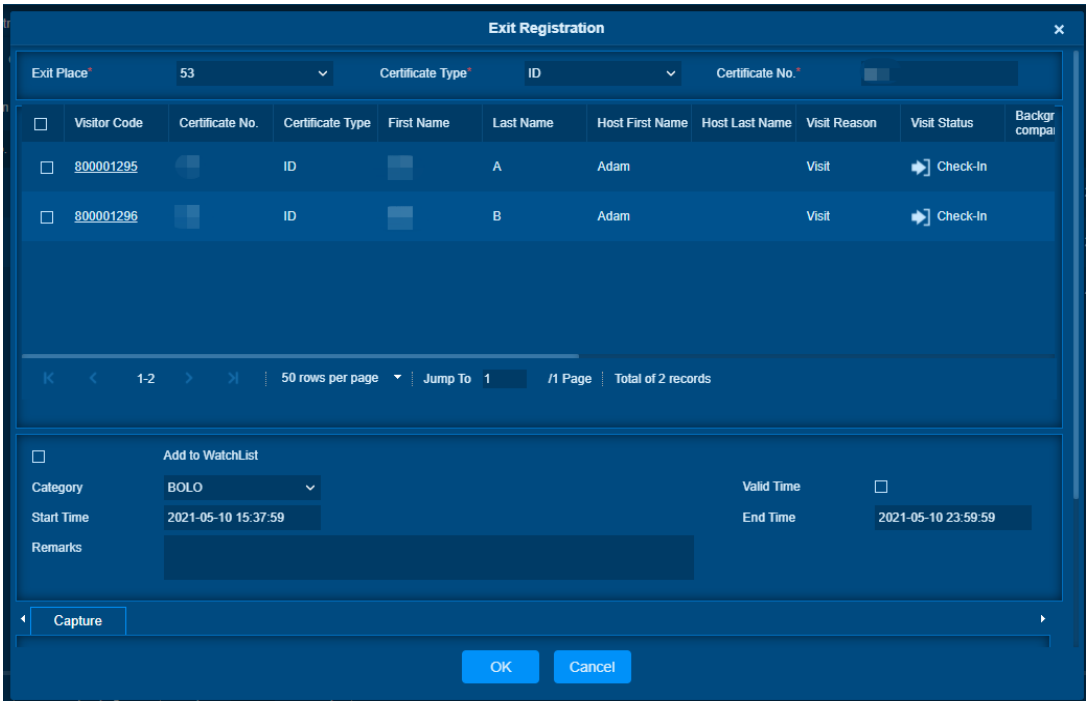
Steps:



Click **[Batch]** drop-down box button and click **[Batch Check-Out]** button in the pop-up drop-down box to navigate to the Guest Batch Check-Out window.



You can manually enter the Certificate Type and Certificate Number to backfill the visitors who have signed in in the same batch, or you can backfill the information of the visitors who have signed in in the same batch by identification.



Whether to join the monitoring list and snap a photo is optional, select a visitor information, click **Capture** button, capture the visitor's check-out photo, tick the visitor who needs to check-out, and click **[OK]** to check out the checked visitors uniformly, the batch guest check-out operation ends.

Visitor Cloning

Preconditions for Normal Use of Function

The administrator has the guest cloning permission, and you need to check a piece of guest information that needs to be cloned before operation.

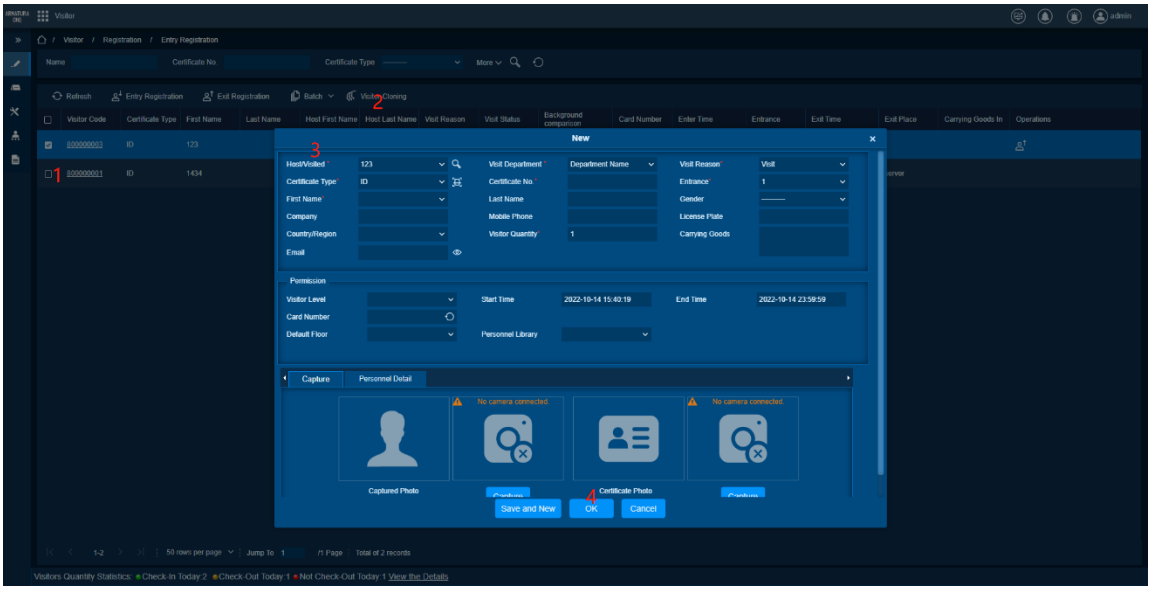
Function Usage Scenarios

When the visitor belongs to the same company and the interviewee uses the name.

Feature Trigger Result

Clone a new visitor data.

Steps:



1. Check a piece of visitor data that needs to be cloned.
2. Click **[Visitor Cloning]** button to pop up a window.
3. Fill in the information, the items marked with * are required.
4. Click **[OK]** button to complete the complete the cloning operation.

9.1.2. Visitor

Function Description

View the information of all scheduled, checked-in, and checked-out visitors.

Delete

Preconditions for Normal Use of Function

There is visitor information in the list, and the checked visitor status cannot be reserved or registered.

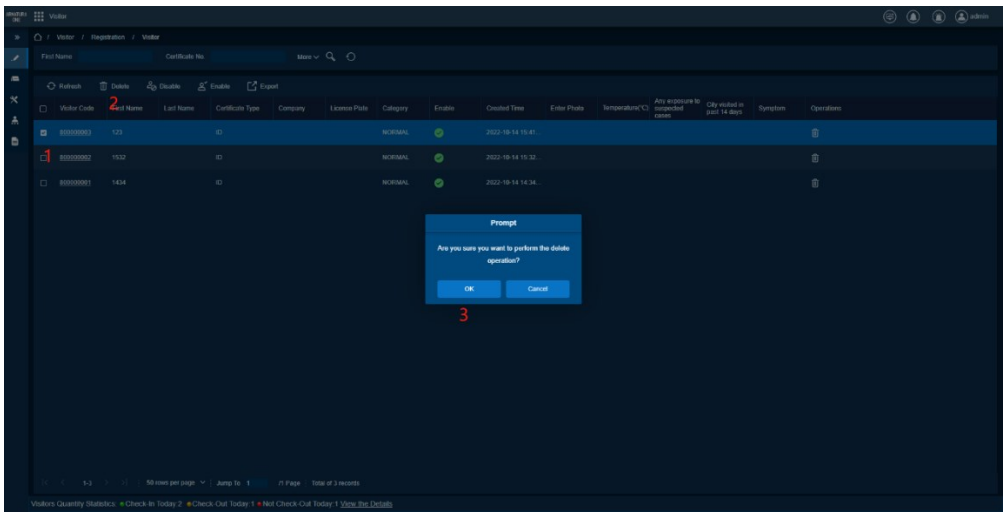
Function Usage Scenarios

Delete unnecessary visitor information (multiple selection supported).

Feature Trigger Result

Operations	Description
Check Visitors	Delete the checked visitors.

Steps:



First select the visitors who need to delete and click the **[Delete]** button on the visitor information interface to perform the delete operation.

Join the Banned List

Preconditions for Normal Use of Function

You need to check the visitors to be added to the banned list, and the ticked visitors cannot be visitors who already have a banned list.

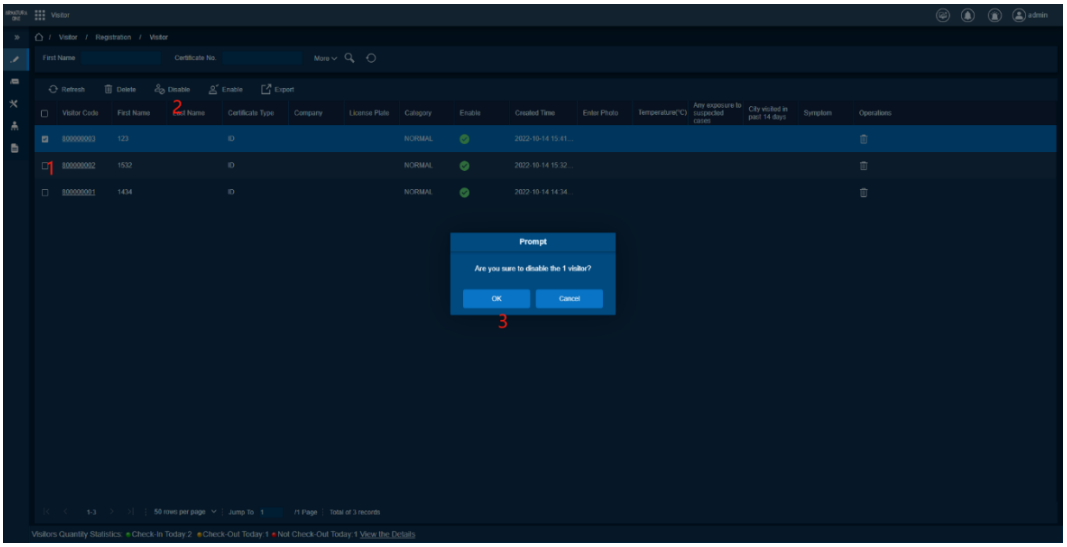
Function Usage Scenarios

When a visitor violates the company's system or has an adverse effect on the company, the visitor shall be added to the banned list and may not register again or make an appointment.

Feature Trigger Result

Operations	Description
Add the Banned List	When the visitor visits again, it is prompted that it is in the prohibited list and cannot sign in or make an appointment.

Steps:



1. Select the visitors who need to be added to the banned list, support multiple selection, and click the **[Disable]** button to complete the operation of adding to the banned list.

Remove from the Banned List

Preconditions for Normal Use of Function

The guest to be removed is already in the banned list.

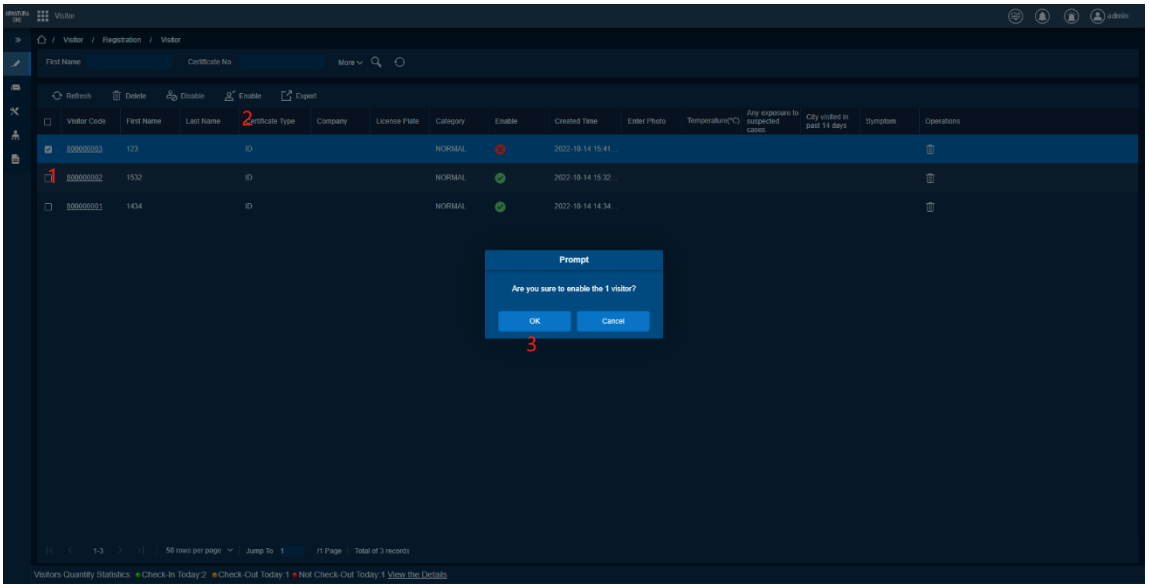
Function Usage Scenarios

Remove visitors from the blocklist.

Feature Trigger Result

Operations	Description
Remove Banned List	Remove this piece of visitor information from the banned list and make reservations and registration operations.

Steps:



1. Select the visitors who need to remove from the banned list, support multiple selection.
2. Click the **[Enable]** button to complete the operation of removing the banned list.

Export

Preconditions for Normal Use of Function

There is visitor information in the visitor information list.

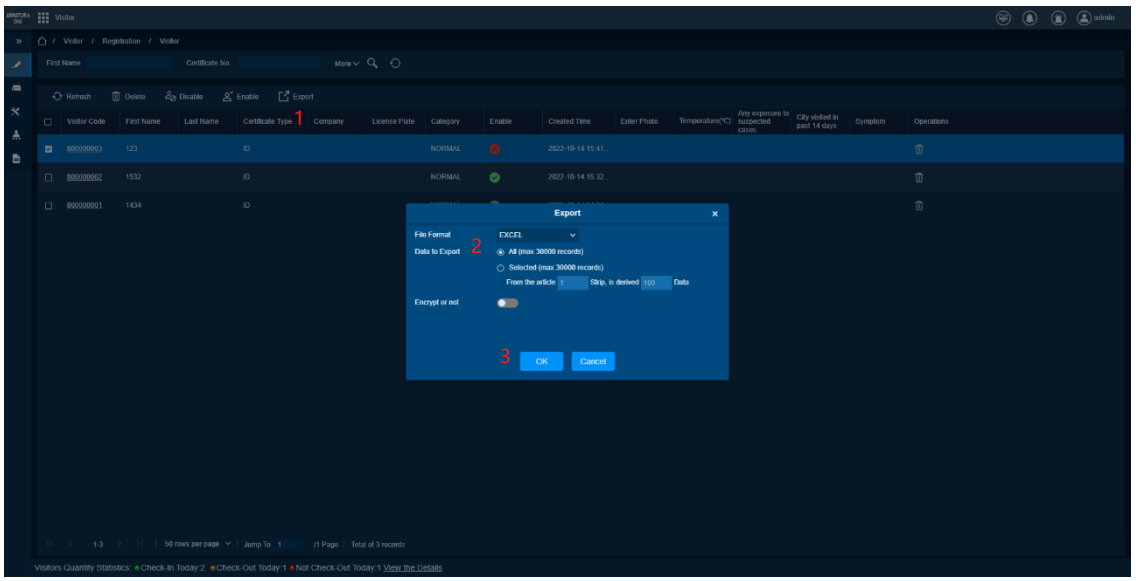
Function Usage Scenarios

Export visitor information.

Feature Trigger Result

Operations	Description
Select Excel	Exported document format is Excel.
Select PDF	Exported document format is PDF.
Select CSV	Exported document format is CSV.
Select All	Export all visitor information.
Select Selected	Export visitor information within a certain range.

Steps:



1. Click **[Export]** button to pop up the Export box.
2. Select the format that needs Export in the pop-up box.
3. Select the Scope of export.
4. Click **[OK]** button to complete the Export operation.

9.2. Reservation

Function List

Functions	Description
Reservation	The visitor makes an appointment for a certain time to visit someone.
Invitation	Send invitation emails to visitors and invite visitors to visit.
Reservation Audit	Guest self-service appointments need to be reviewed before the appointment can be successful.

9.2.1. Reservation

Function Description

Check the visitor's appointment information, make an appointment before the visitor comes, you can tell the interviewee and the visitor when to visit someone in advance.

Add

Preconditions for Normal Use of Function

Visitors who currently need to make an appointment can only make an appointment if the status of the visitor is checked out or expired and has not made an appointment.

Function Usage Scenarios

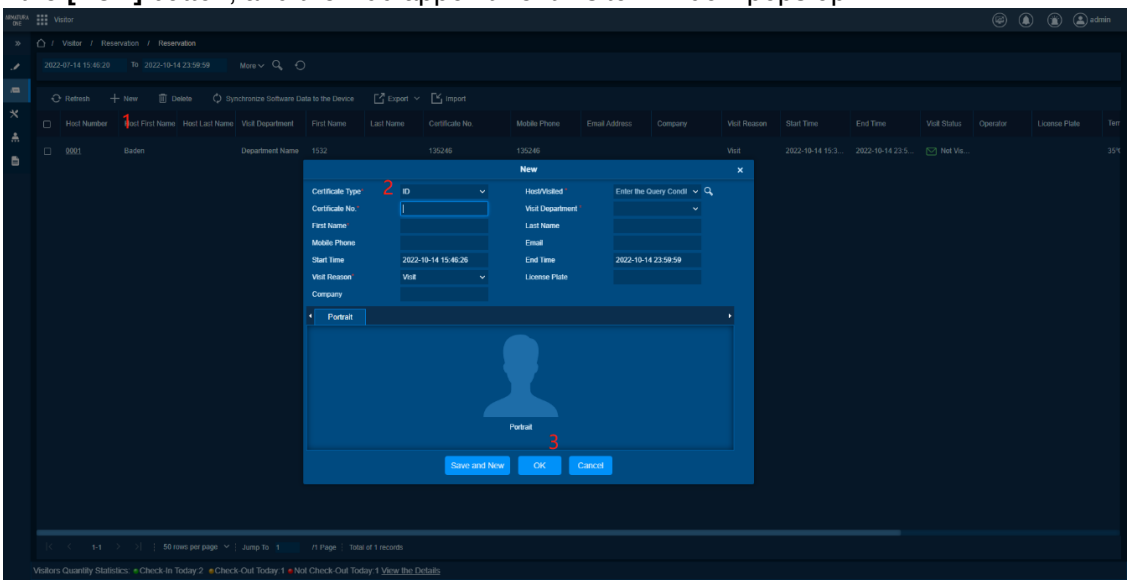
When a visitor needs to make an appointment in advance, call or send a text message to the front desk staff, and inform the front desk staff of their personal information, who needs to be visited and the visiting time, and the front desk staff will help the visitor to make an appointment on the software.

Feature Trigger Result

Operations	Description
Click the **[OK]** Button	Add a visitor reservation information.

Steps:

1. Click the **[New]** button, and the Add appointment visitor window pops up.



Fill in the relevant information, the fields are explained as follows: -

Certificate Type: Enter the type of certificate.

Certificate No.: Enter the certificate number.

First Name: Enter the first name

Mobile Phone: Enter the phone number

Start Time: Enter the start time.

Visit Reason: Enter the visit reason.

Company: Enter the company name.

Host/Visited: Select the right option Host/Visited.

Visit Department: Enter the department you are going to visit.

Last Name: Enter the last name.

Email: Enter the email ID.

End Time: Enter the end time.

License Plate: Enter the license plate name.

Items marked with * are required, items without * are optional.

2. After filling in the relevant information, click **[OK]** button to complete the Add appointment operation.

Delete

Preconditions for Normal Use of Function

Delete the visitor reservation information from the list.

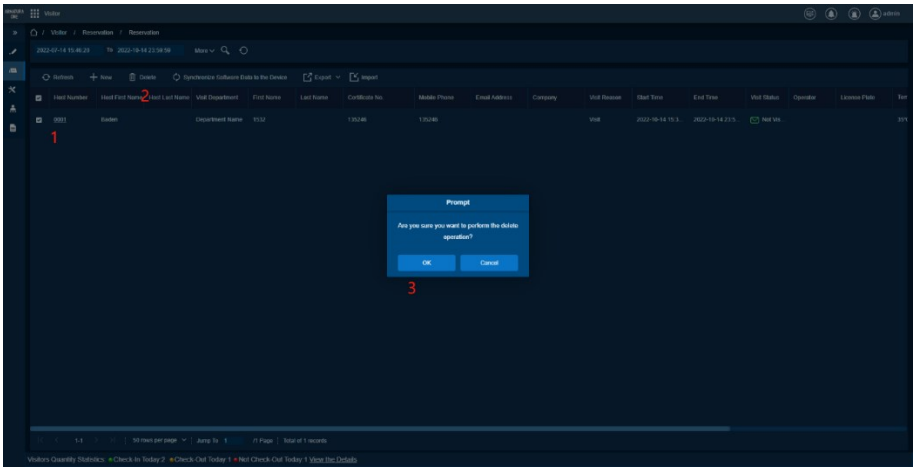
Function Usage Scenarios

Delete useless or expired visitor reservation information in the list.

Feature Trigger Result

Operations	Description
Check the visitor information and click **[Delete].**	Delete the checked guest appointment information.

Steps:



1. Check the reservation visitor information that needs to be deleted.
2. Click **[Delete]** button, and a prompt box will pop up.
3. Click **[OK]** button in the prompt box to complete the Delete reservation visitor information operation.

Synchronize Software Data to the Device

Preconditions for Normal Use of Function

There are online devices that support the visitor module and there is information in the visitor reservation list.

Function Usage Scenarios

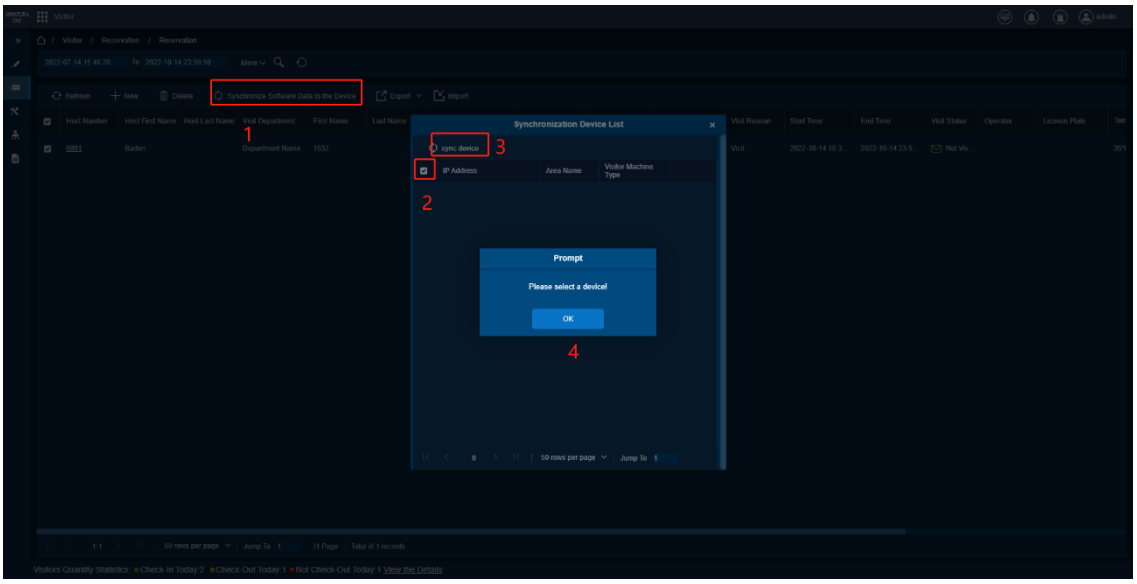
Synchronize the reserved visitor information to the device.

Feature Trigger Result

Operation	Description
Check the device and click [sync device]	Synchronize visitor appointment information to the checked devices.

Synchronize all the information in the list to the checked devices.

Steps:



1. Click the **[Synchronize Software Data to the Device]** button to pop up a list of synchronized devices.
2. Select the device to be synchronized.
3. Click **[Sync Device]** button, and a prompt box will pop up.
4. Click **[OK]** to complete the synchronization operation.

Export Reservation Visitor Information

Preconditions for Normal Use of Function

There is visitor reservation data in the list.

Function Usage Scenarios

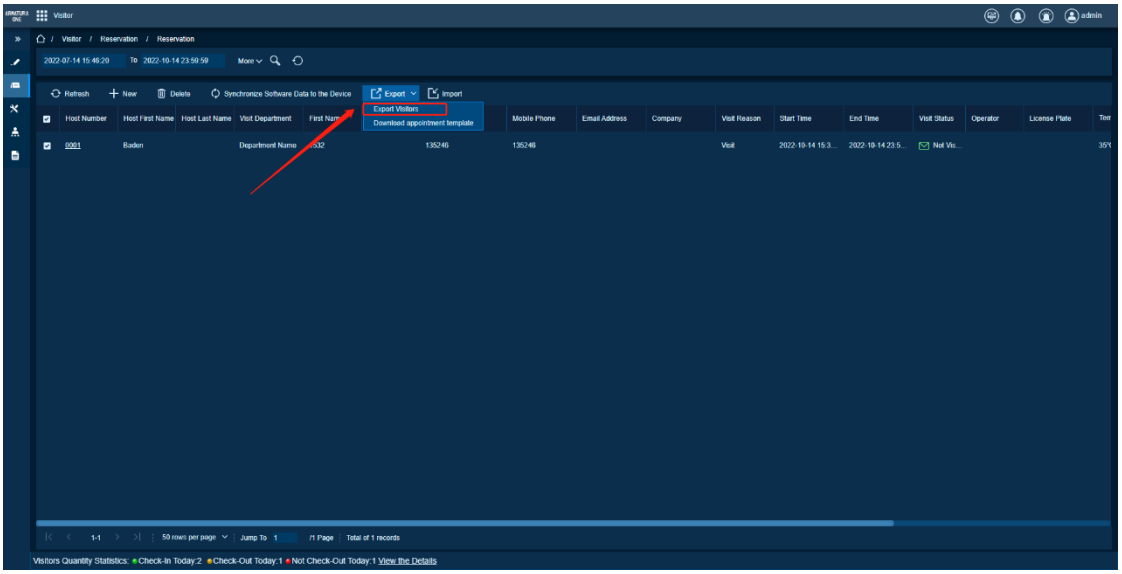
Export the reserved visitor information to EXCEL, PDF, or CVS format.

Feature Trigger Result

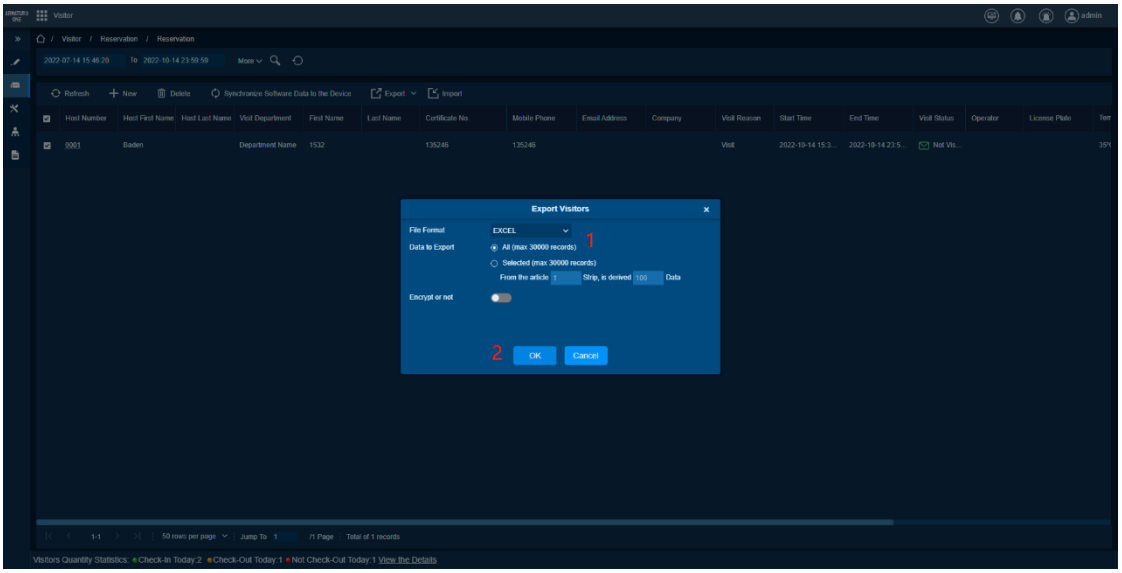
Operations	Description
Select Excel	Exported document format is Excel.
Select PDF	Exported document format is PDF.
Select CSV	Exported document format is CSV.
Select All	Export all visitor reservation information.

Select Selected	Export reservation information of visitors within a certain range.

Steps:



1. Click the **[Export]** drop-down box.
2. Select **[Export Visitors]** in the drop-down box option, and the Export Visitors window will pop up.



In the pop-up box:

1. Select the type of document that needs to be exported.
2. Select the data range that needs to be exported.
3. Click the **[OK]** button to complete the Export operation. The export document can be viewed in the download center of the browser.

Export Reservation Template

Preconditions for Normal Use of Function

The login staff has the right to Export reservation template.

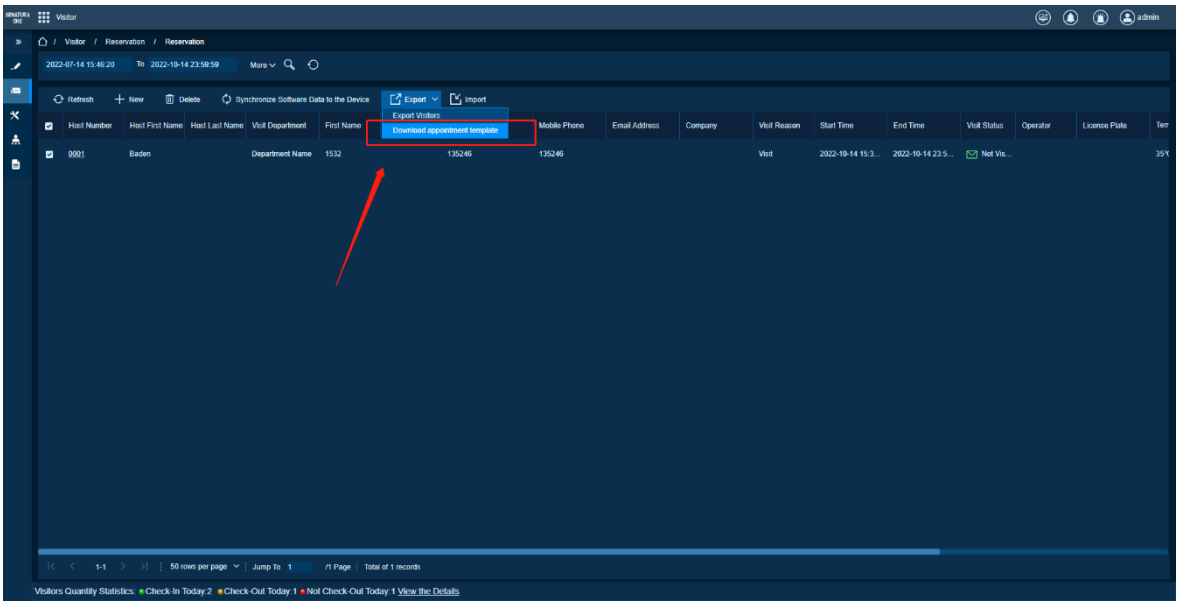
Function Usage Scenarios

When there is a team to make an appointment and the number of the team is greater than or equal to two, you can use this function to export a template, fill in all the personnel information, and then import it through the import function.

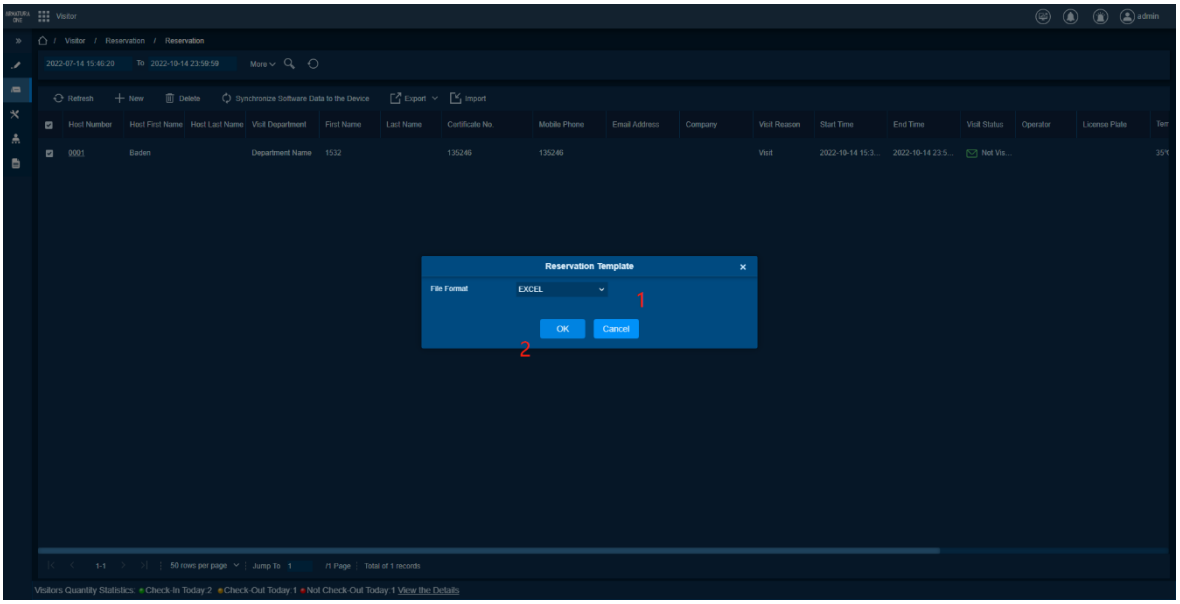
Feature Trigger Result

Operations	Description
Click **[Export Appointment Template]**	Export a table in Excel format.

Steps:



1. Click the **[Export]** drop-down box.
2. Click **[Export Appointment Template]** option.



3. Click **[OK]** in the pop-up box to complete the Export reservation template operation. The Export reservation template can be viewed in the download center of the browser.

Import

Preconditions for Normal Use of Function

The administrator has the authority of the import function. The imported template must be consistent with the current software language. In the imported information, the personnel field cannot have non-existent personnel id, the certificate type and certificate number cannot be empty, or the format is wrong, and the mobile phone number It cannot be empty, and the format cannot be wrong, the mailbox cannot be empty, and the format cannot have errors, the start date cannot be less than the date of the day, and the end date cannot be less than the start date.

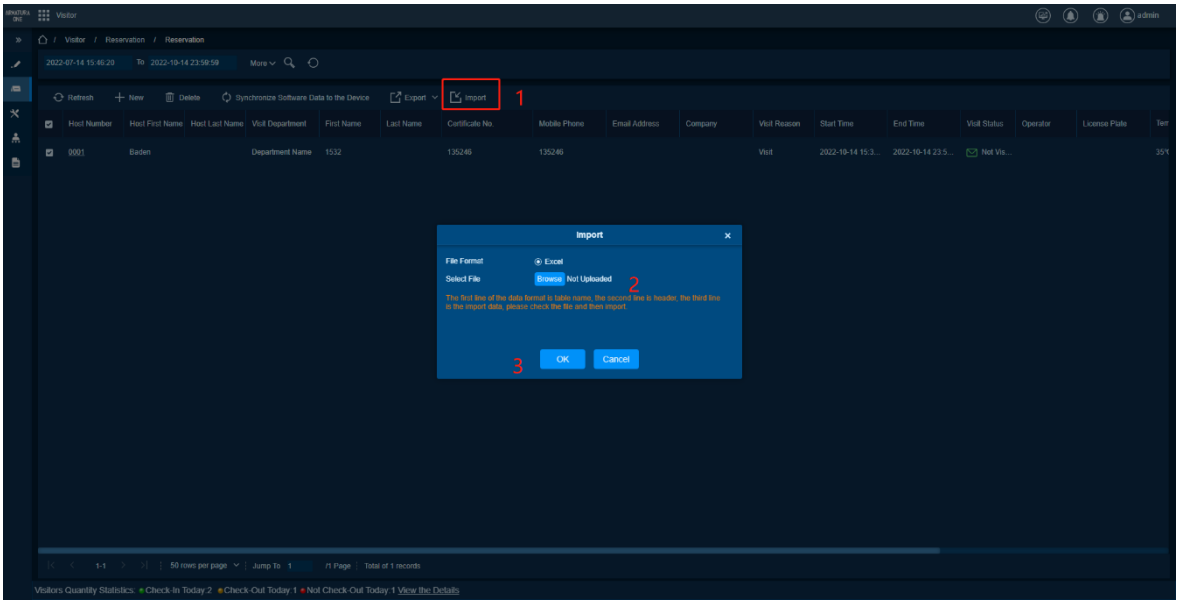
Function Usage Scenarios

When there is a team to make an appointment, and the number of the team is greater than or equal to two, you can use the Export appointment template function to export a template, fill in all the personnel information, and then import through the import function to complete the batch appointment operation.

Feature Trigger Result

Operations	Description
Import Template	Add all personnel in the imported form to the appointment list.

Steps:



1. Click **[Import]** button.
2. Click **[Browse]** button in the pop-up box and select the template to be imported.
3. Click **[OK]** button to complete the batch import operation.

9.2.2. Invitation

Function Description

View and invite visitors to visit the interviewee at a certain point in time.

Add

Preconditions for Normal Use of Function

The administrator has the permission to add the invitation function, and in the system management module, there are configuration mailbox parameters.

The linkage function of the Visitor module has been configured

If the invitation is sent by SMS, you need to configure the SMS modem in System module.

Function Usage Scenarios

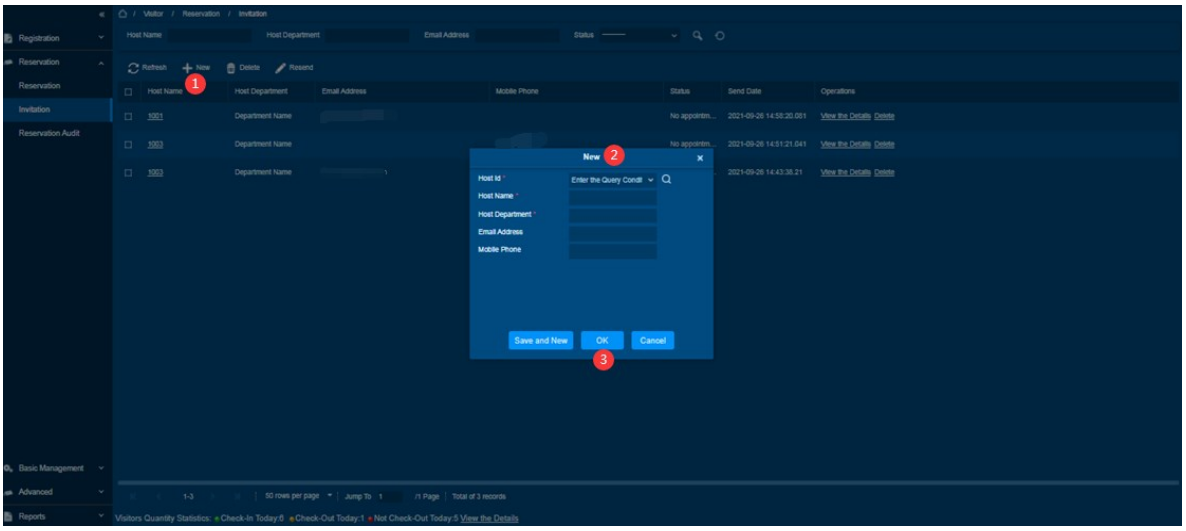
When the interviewee asks the visitor to visit, he can send an email or phone to the visitor in advance through the invitation function to notify the visitor to visit at a certain time.

The sending content and recipients can be configured uniformly through the Alert Template function.

Feature Trigger Result

Operations	Description
Click [OK] Button	Send an invitation email to the visitor's mailbox or send an invitation message to visitor's Mobile Phone.

Steps:



1. Click **[New]** button.
2. Fill in the relevant information in the pop-up window, the field descriptions are as follows:

Host ID	Enter host ID.

Host Name	Enter host name.
Host Department	Enter host department.
Email Address	Enter email address.
Mobile Phone	Enter mobile phone

Fields marked with * and are required.

E-mail address and mobile phone number must be filled in at least one.

3. After filling in the required items, click **[OK]** button to complete the visitor invitation operation.

Delete

Preconditions for Normal Use of Function

The administrator uses the Delete invitation function permission, and there is invitation information in the list.

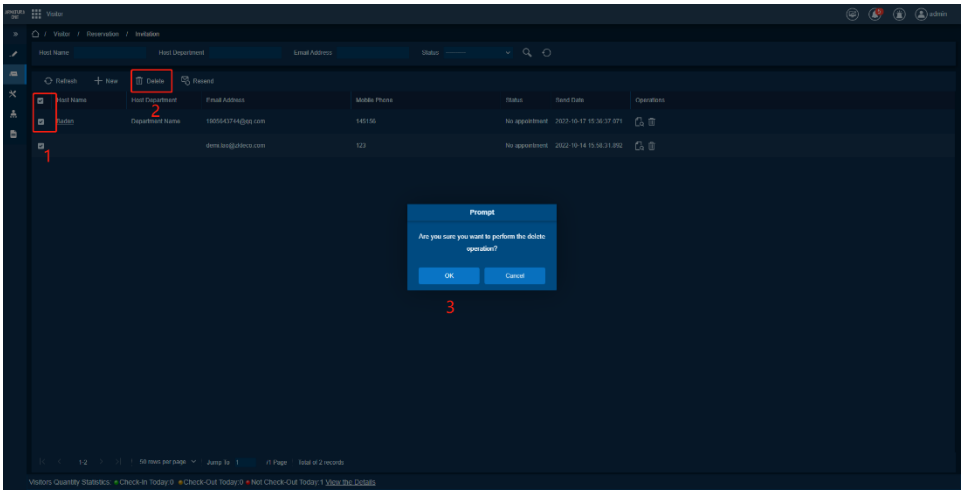
Function Usage Scenarios

Delete the invitation information that has expired or expired.

Feature Trigger Result

Operations	Description
Click [Delete]	Delete the checked information.

Steps:



1. Check the invitation information that needs to be deleted.
2. Click **[Delete]** button.
3. Click **[OK]** in the pop-up box to complete the Delete invitation information operation.

View the Details

Preconditions for Normal Use of Function

Click the pop-up window to send the record of the invitation, showing the template type, subject, sending content (including body and endnotes), sending status, and sending time.

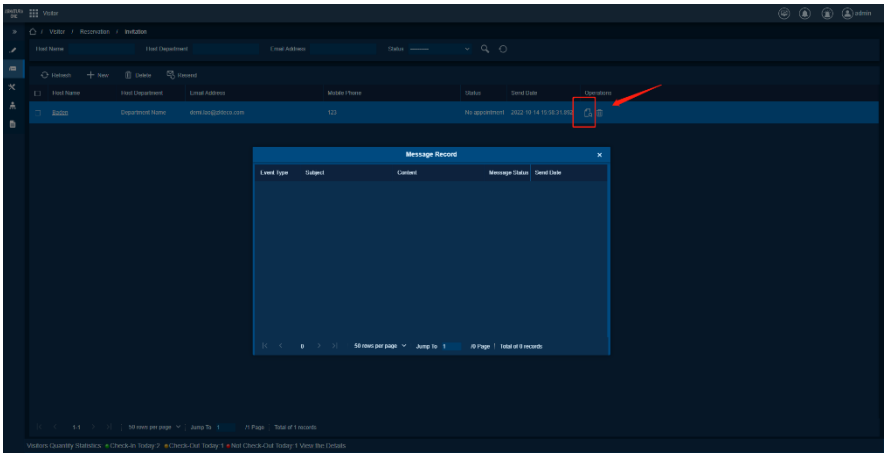
Function Usage Scenarios

View the record of the invitation.

Feature Trigger Result

Operations	Description
Click [View the Details]	Displays all the history records of the invitation information

Steps:



1. Click **[View the Details]** button.
2. Click **[X]** in the pop-up box to complete the View the detail invitation information operation.

Resend

Preconditions for Normal Use of Function

The administrator has the authority to resend, there is invitation information in the invitation list, and the system module has set mailbox parameters.

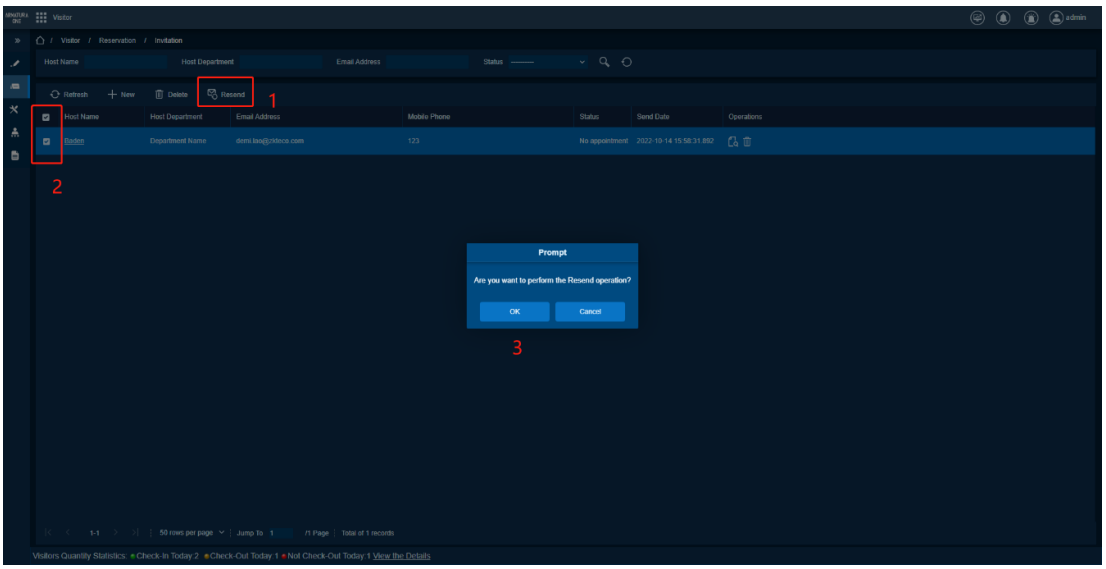
Function Usage Scenarios

It is used when the status of the email sent to the visitor is sending failed or reminding the visitor to come again.

Feature Trigger Result

Operations	Description
Click [Resend]	Resend the email/message to the guest mailbox/phone

Steps:



1. Check the invitation information that needs to be resent.
2. Click **[Resend]** button.
3. Click **[OK]** button in the prompt box to complete the resend operation.

9.2.3. Reservation Audit

Function Description

When the visitor appointment review function is enabled, all self-appointed visitors will be stored in the appointment review list, and the administrator can review the self-appointed visitors or reject the visit operation.

Check

Preconditions for Normal Use of Function

The administrator has review authority, there are visitor appointment data in the list and the visitor appointment review function is enabled in the Parameters Setting.

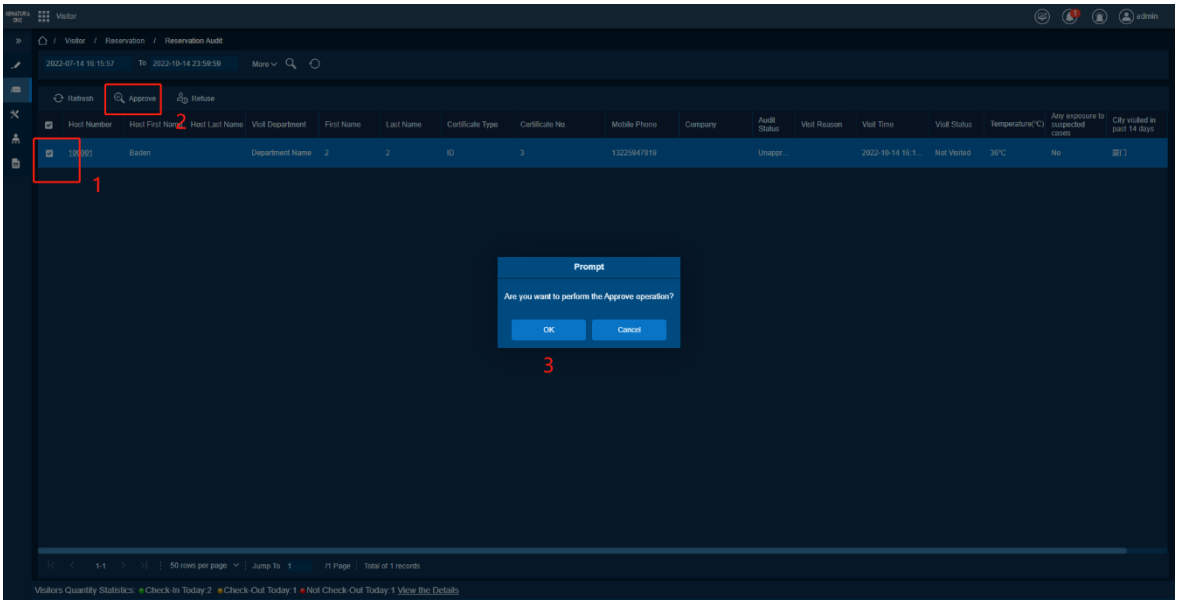
Function Usage Scenarios

When a visitor makes a self-service appointment, the visitor can be allowed to make an appointment based on the visitor information. Save the information to the guest appointment list.

Feature Trigger Result

Operations	Description
Click [Approve]	Allow the ticked visitors to make appointments and send an approved email to the visitors.

Steps:



1. Check the appointment information that needs to be approved.
2. Click **[Approve]** button, and a prompt box will pop up.
3. Click **[OK]** in the pop-up prompt box to complete the approval operation.

Rejection

Preconditions for Normal Use of Function

The administrator has review authority, there are visitor appointment data in the list and the visitor appointment review function is enabled in the Parameters Setting.

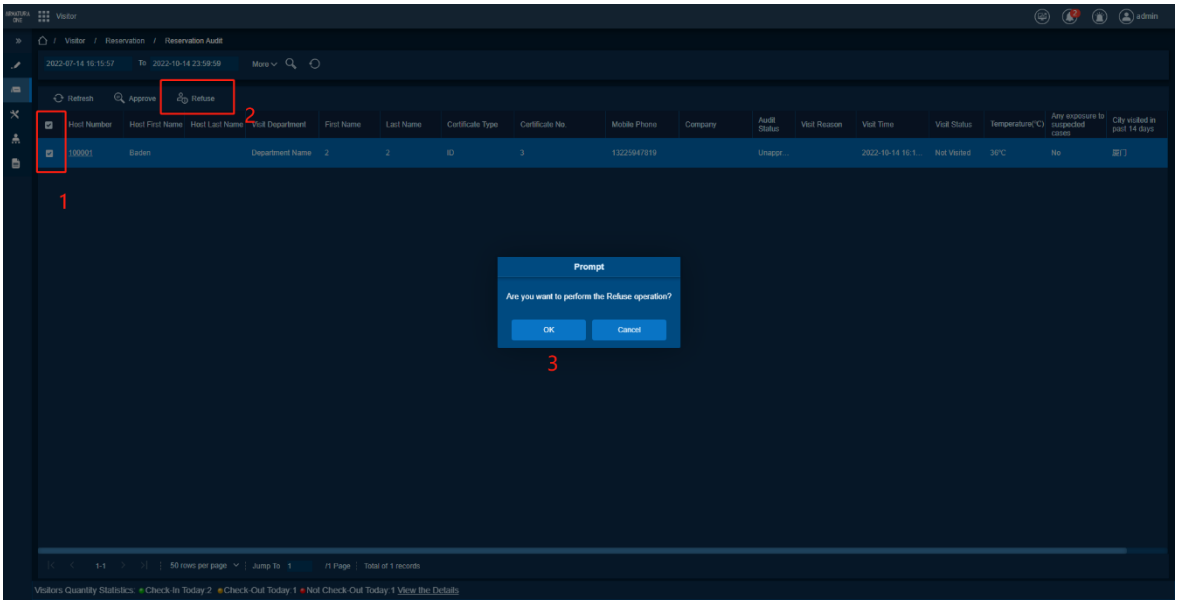
Function Usage Scenarios

When a visitor makes an appointment by himself, he can reject the visitor's appointment based on the visitor's information.

Feature Trigger Result

Operations	Description
Click [Refuse]	Reject the checked guest appointments and send a review rejection email to the visitor.

Steps:



1. Check the visitor reservation information that needs to be rejected.
2. Click **[Refuse]** button, and a prompt box will pop up.
3. Click **[OK]** button in the pop-up prompt box to complete the review rejection operation.

9.3. Basic Management

Function List

Functions	Description
Parameters	Set the parameters of the guest module
Device Debugging	Set the parameters of the equipment used by the guest module
Print Settings	Set the parameters of the print function
Visitor Levels	Set permissions for visitors
Host Levels	Set the visitor levels according to the interviewee
Visited Department Levels	Set visitor levels according to the visited department
Entry Place	Set the Place of Registration for visitors
Visit Reason	Set visitor's Visiting Reason
Custom Attributes	Customize some visitor attributes

9.3.1. Parameters

Function Description

Unified management of some parameter configurations of the guest module.

Field Description

Carrying Goods Capture: Turn on or off the function of capturing photos of visitors' personal belongings during Visitor Registration.

Exit Registration: Turn on or off the guest check-out function. When it is turned on, you can set the automatic check-out function and turn on the timer check-out function for visitors who have expired.

Permission: When Visitor Registration is turned on or off, whether Authorization is required, and the Authorization method can be selected when opening Authorization.

Select the Required Field: You can choose whether the interviewee and visiting department are required options.

Visitor Vehicle Authorization Mode: If it is set as a temporary car, the license plate is a temporary car when the license plate is filled in in Visitor Registration or reservation. If it is set as an allowed list, the license plate is a VIP car when the license plate is filled in for Visitor Registration or reservation.

Capture: Set the snapshot mode during Visitor Registration.

Camera Mode: Set the opening mode of the camera.

Floating Window: Whether to open the floating window of Visitor Registration sign-out.

Visitor History Information: When it is turned on, you can set the backfill information for Visitor Registration.

Copy ID Number as Card Number Automatically: When it is turned on, use the ID number as the card number.

Watchlist Option: During Visitor Registration, the monitoring list pop-up window is triggered by the set matching options.

Maximum Visitor Check: Enable the detection of the maximum number of visitors in a single day.

The Visitor List the Recipient Mailbox: Set the sending time to the visitor and the visitor who needs to be sent.

Audit: After opening, the guest self-registration needs to be reviewed.

QR code URL: The path of visitor self-registration.

Mobile URL: The access path of the mobile terminal.

Open the Declaration of Health Information: After opening, visitors need to fill in their health status during self-registration.

Privacy Statement: After it is turned on, the content of the privacy statement will be displayed on the guest self-registration interface.

9.3.2. Device Debugging

Function Description

Manage the equipment of the visitor module, including the current location, print control download, device driver downloads, scanner, high-speed camera, USB camera debugging.

Field Description

Current Location: Display the name, IP, and avatar collection device of the current Place of Registration.

Printing Environment: Check whether the current computer's printing environment is normal.

Device Driver: Check if the device driver has been downloaded.

Other Scanner: Debug the scanner device.

High-Speed Portable HD Doc Scanner: Debug high-speed camera equipment.

USB Camera: Debug the USB camera.

9.3.3. Print Settings

Function Description

Set the receipt printed during Visitor Registration.

Field Description

Template Selection: Select the type of printing.

Print Card Number: After checking, the printed QR code is the visitor's card number.

Print Personnel Number: After checking, the printed QR code is the personnel number.

Printer Use: Select the printer type.

Select Paper Type: Select the paper type.

Custom Paper Size: Customize the paper size for printing.

Custom Paper Width: Customize the paper width for printing.

9.3.4. Visitor Levels

Function Description

View visitor's authority and unified management of visitor's authority.

Visitor Levels

Add Access Level

Preconditions for Normal Use of Function

The administrator has the permission to add an access level, and the access control module has an access level.

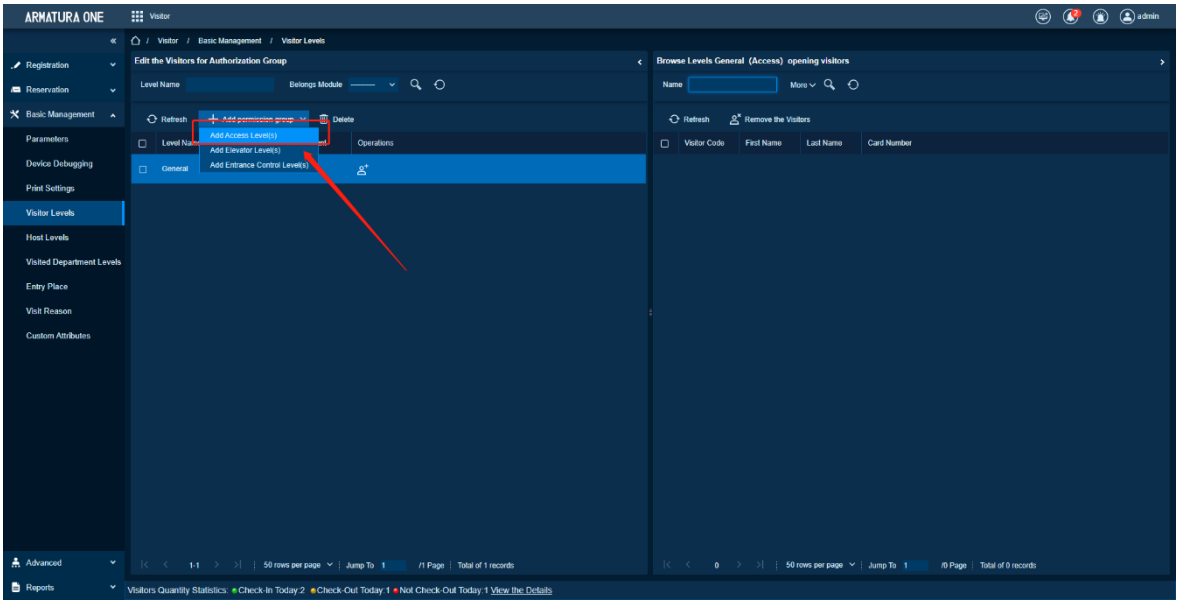
Function Usage Scenarios

Set visitor's access level.

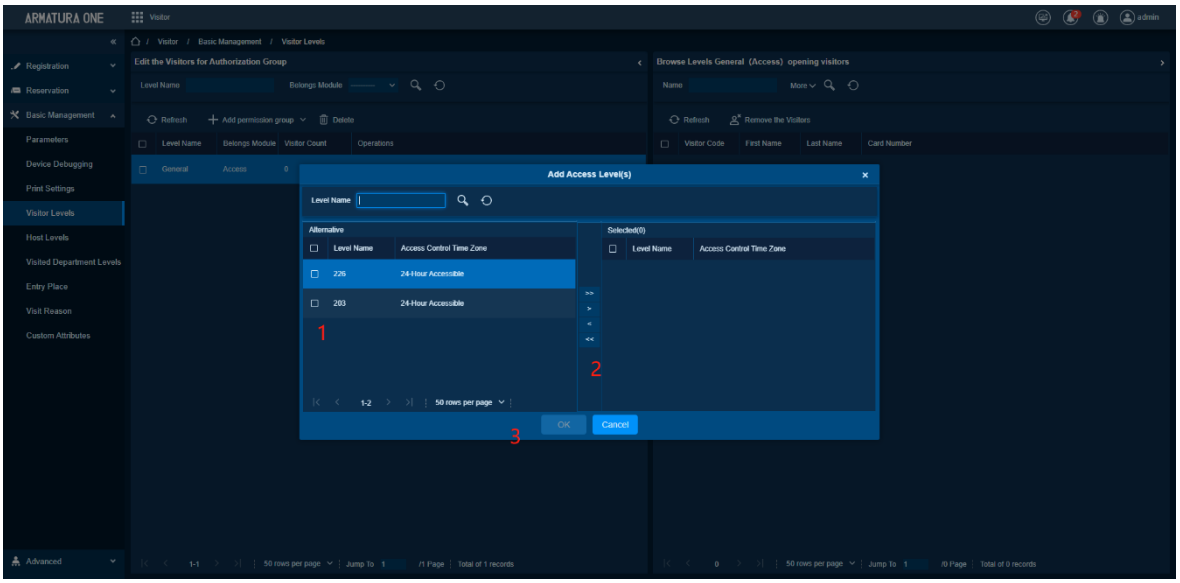
Feature Trigger Result

Operations	Description
Click [OK]	Add Access Level.
Click [Add Visitors]	Add visitors to Access Level

Steps:



1. Click **[Add Access Level(s)]** drop-down box.
2. Select **[Add Access Level(s)]** in the pop-up drop-down box to pop up a list.



In the pop-up list:

1. Select the access level that needs to be added in the list on the left.

2. Click ">" symbol to add the checked access level to the list on the right.
3. Click **[OK]** button to complete the operation of adding an access level.

Add Elevator Level

Preconditions for Normal Use of Function

The administrator has the authority to add the elevator level, and the elevator control module has the elevator level.

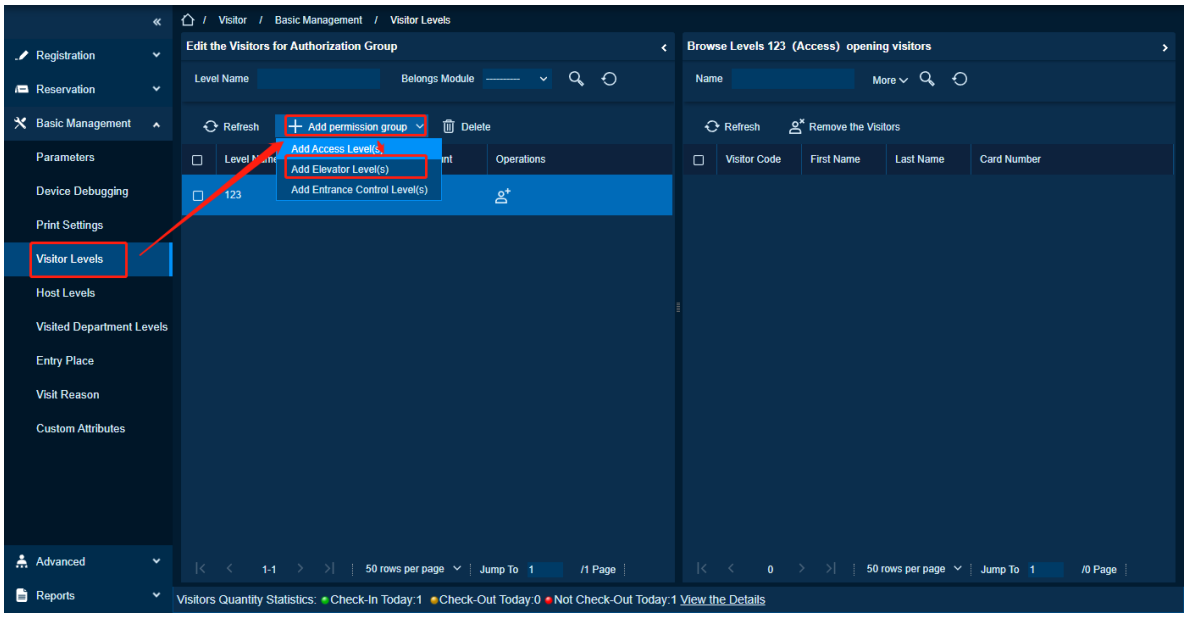
Function Usage Scenarios

Set visitor's elevator level.

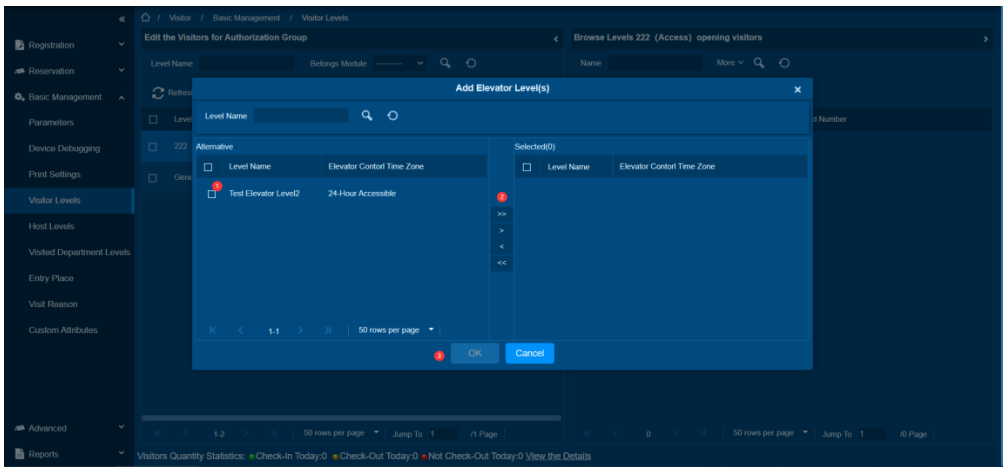
Feature Trigger Result

Operations	Description
Click [OK]	Add elevator level.
Click [Add Visitors]	Add visitors to elevator level.

Steps:



1. Click **[Add Permission Group]** drop-down box.
2. Select **[Add Elevator Level(s)]** in the pop-up drop-down box to pop up a list.



In the pop-up list:

1. Select the elevator level that needs to be added in the list on the left.
2. Click ">" symbol to add the checked elevator level to the list on the right.
3. Click **[OK]** button to complete the operation of adding an elevator level.

9.3.5. Host Levels

Function Description

Set permissions for Host, and the added Host can be chosen to visit during guest self-registration.

Add Host and set default visitor level

Preconditions for Normal Use of Function

The administrator has the adding function permissions.

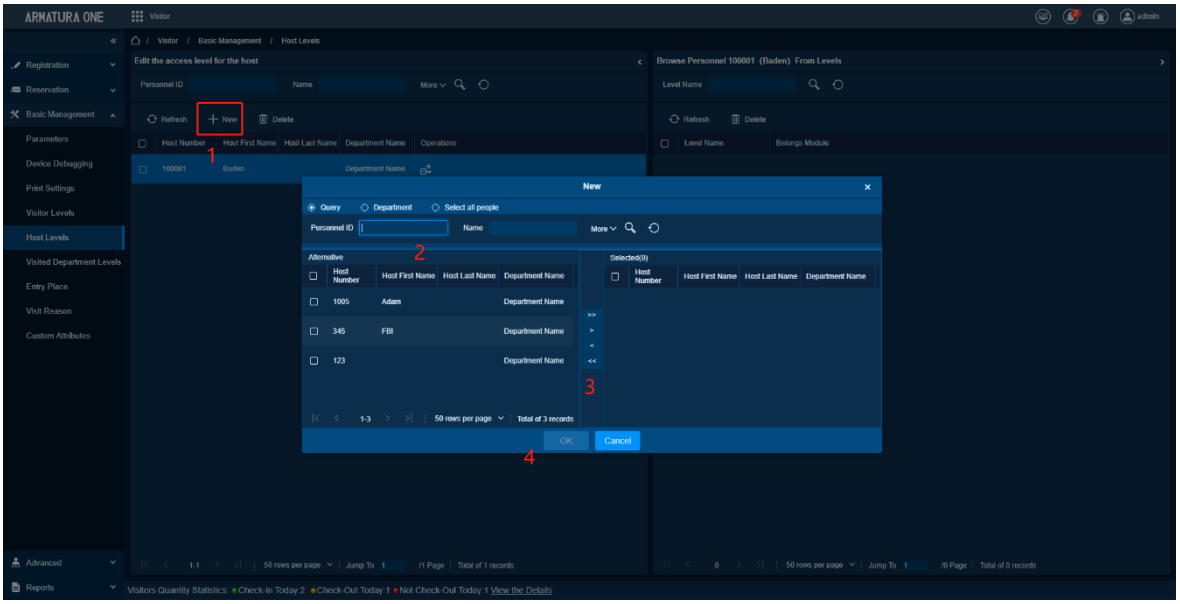
Function Usage Scenarios

Add Host so that visitors can choose Host when making a self-service appointment.

Feature Trigger Result

Operations	Description
Click [OK] Button	Add Host levels.
Click [Add Visited Level(s)]	Add default visitor Level to Visitor.

Steps:



1. Click the [New] button to pop up a list.
2. Check host who needs to be added in the list on the left.
3. Click the ">" symbol to add the selected host to the list on the right.
4. Click the [OK] button to complete the adding operation.

Delete Host

Preconditions for Normal Use of Function

The administrator has the delete permission, and the interviewee information is in the list.

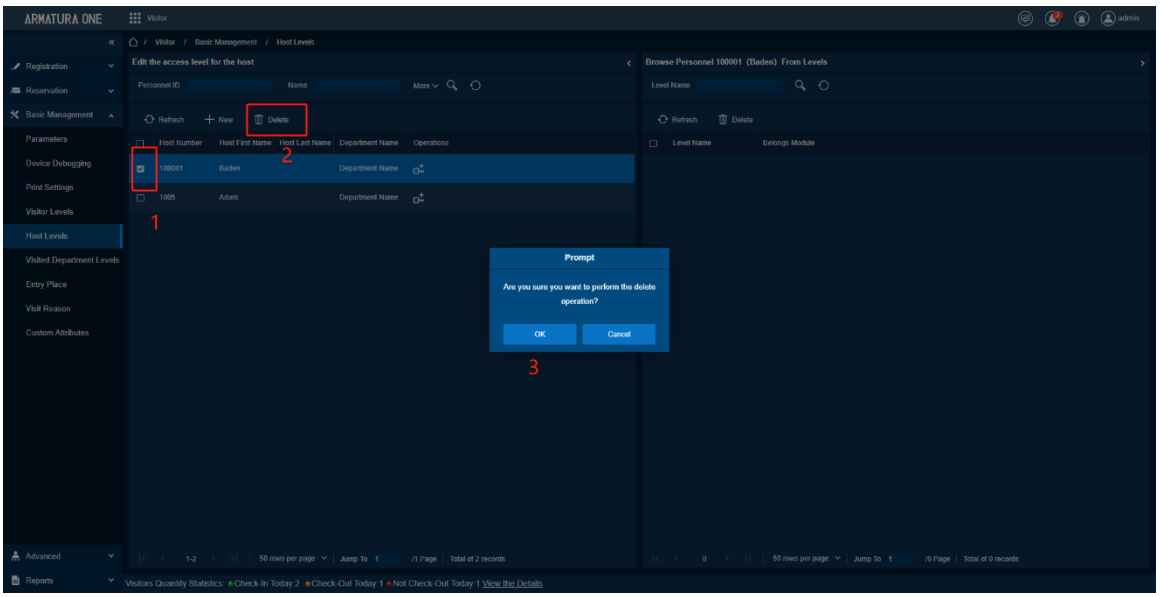
Function Usage Scenarios

Delete invalid interviewee information.

Feature Trigger Result

Operations	Description
Click [OK]	Delete host from left list.

Steps:



1. Check the Host who need to be deleted.
2. Click the [Delete] button, and a prompt box will pop up.
3. Click the [OK] button in the prompt box to complete the delete operation.

Delete default visitor level from Host's default visitor level

Preconditions for Normal Use of Function

The administrator has the delete permission.

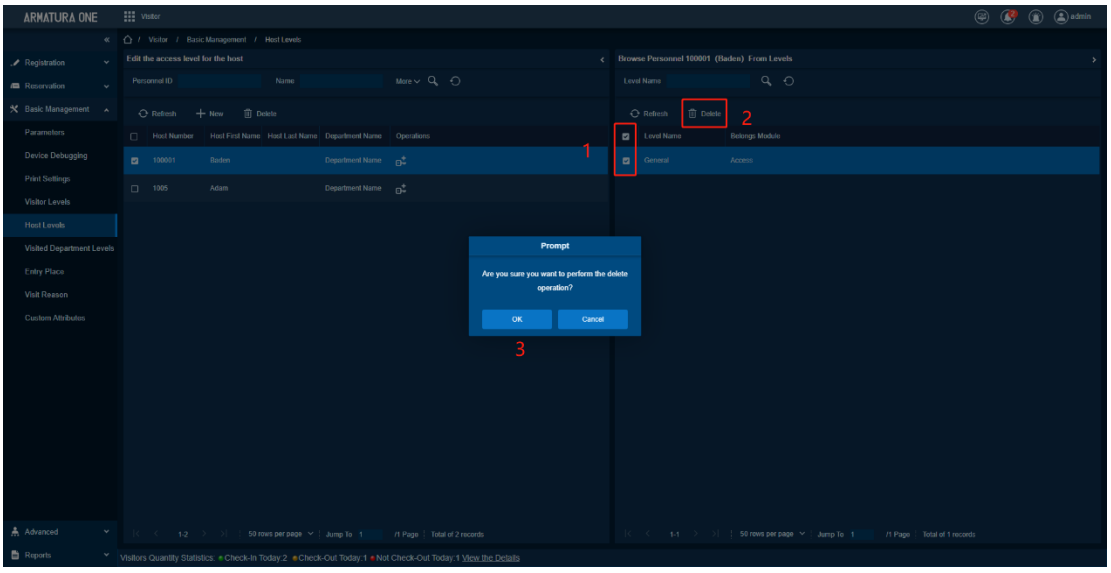
Function Usage Scenarios

Used when the interviewee does not need a certain permission.

Feature Trigger Result

Delete the permission of the interviewee.

Steps:



1. Select the Host's information in the list on the left and backfill the permission group of the visitor in the list on the right.
2. Check the permission group of the visitor that needs to be deleted.
3. Click the [Delete] button, a prompt box will pop up
4. Click the [OK] button in the prompt box to complete the operation of deleting the Host's default visitor level.

9.3.6. Visited Department Levels

Function Description

Set up permission groups according to the interviewed department.

Add visited department and set its default visitor level

Preconditions for Normal Use of Function

The administrator has the authority to add new visited departments, and the personnel module has department settings.

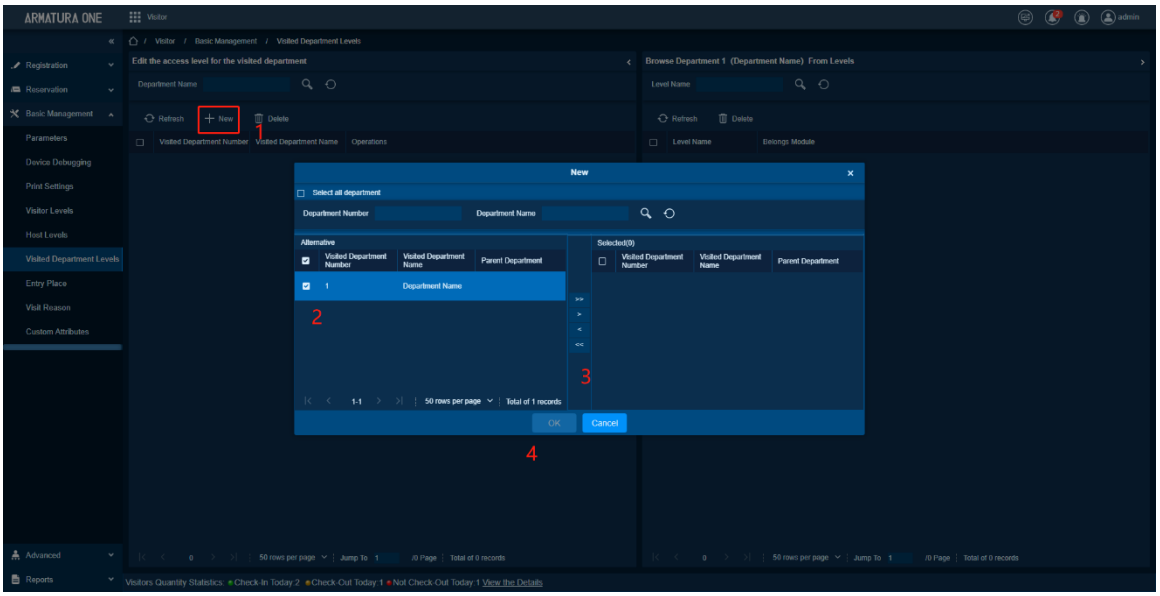
Function Usage Scenarios

Used when the interviewed department needs unified authority.

Feature Trigger Result

Operations	Description
Click [OK] Button	Add visited department.

Steps:



1. Click the [New] button to pop up a list.
2. Select the data in the list on the left.
3. Click the ">" button to add the data from the list on the left to the list on the right.

4. Click [OK] to complete the adding operation.

Delete Visited Department Level

Preconditions for Normal Use of Function

The administrator has the delete permission.

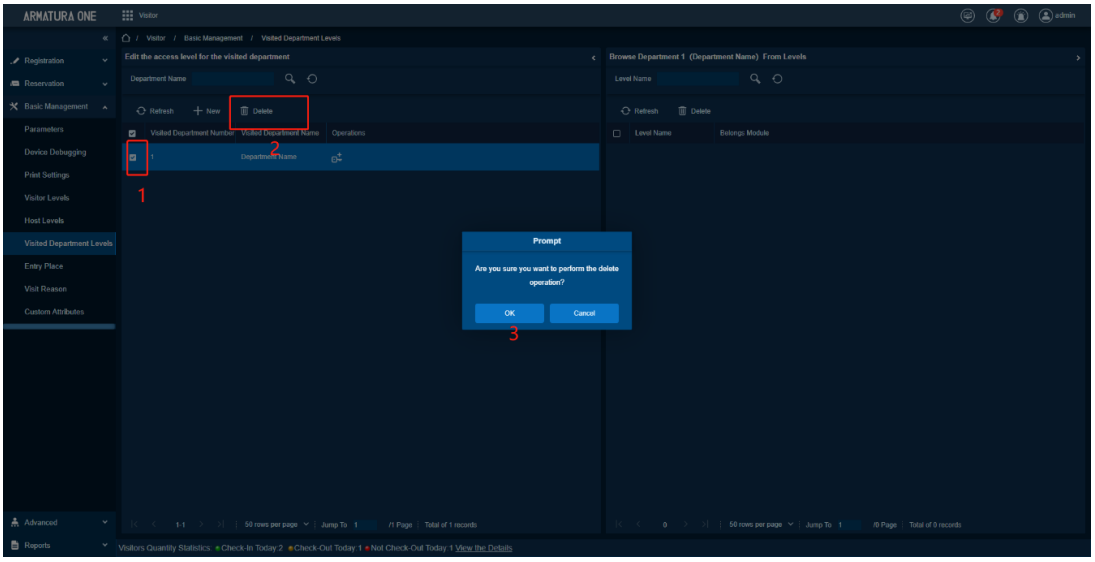
Function Usage Scenarios

Delete invalid or redundant departments.

Feature Trigger Result

Delete the selected interviewed department.

Steps:



1. Check the interviewed department that needs to be deleted.
2. Click the [Delete] button, and a prompt box will pop up.
3. Click [OK] to complete the delete operation.

Delete default visitor level from visited department level

Preconditions for Normal Use of Function

The administrator has the delete permission, and the selected department has the permission group assignment.

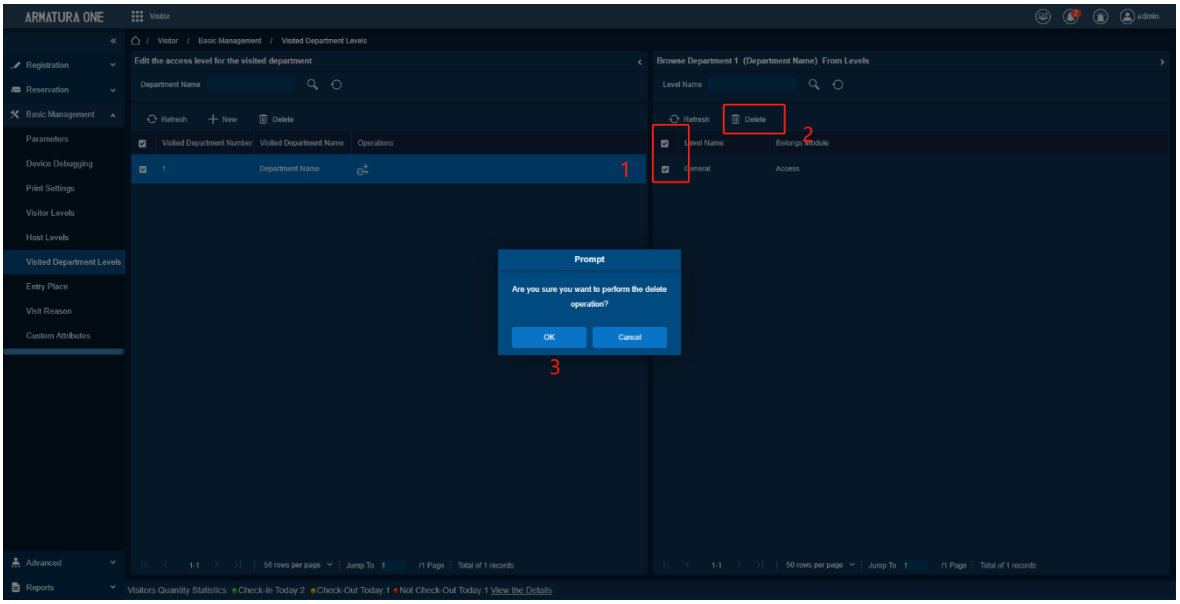
Function Usage Scenarios

The administrator deletes some unnecessary permissions of the department.

Feature Trigger Result

Operations	Description
Click [OK] Button	After deletion, the department no longer has the permission.

Steps:



1. Select the visited department whose default visitor level needs to be deleted.
2. Check the permissions that the department needs to delete.
3. Click the [Delete] button, a prompt box will pop up.
4. Click the [OK] button in the prompt box to complete the delete default visitor level operation.

9.3.7. Entry Place

Function Description

View and set the location of visitor registration.

Add

Preconditions for Normal Use of Function

The administrator has the right to add a registration location.

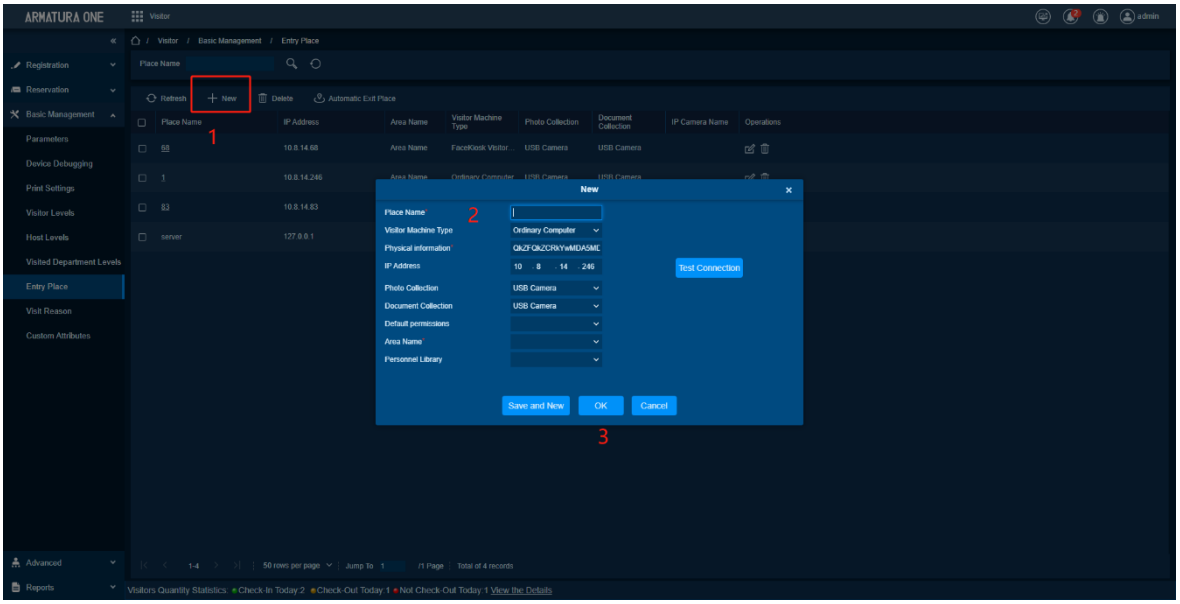
Function Usage Scenarios

When a visitor registers, it is necessary to set a registration location to allow the visitor to register and enter.

Feature Trigger Result

Add a new registration location as a visitor registration location.

Steps:



1. Click the [New] button to pop up a window.
2. Fill in the pop-up window information, the field descriptions are as follows:

Place Name: Set the name of the registration place (required)

Visitor Machine Type: Visitor machine type (normal computer, desktop visitor machine, ID2000, FaceKiosk)

Physical information: Physical information of the visitor machine

IP Address: The IP address of the visitor machine

Photo Collection: Head portrait collection method (USB camera, web camera, dual camera high shot meter)

Document Collection: Document collection method (USB camera, web camera, dual-camera high-speed camera)

Default permissions: Default permissions

Area Name: Area name (required)

Personnel Library: Personnel Library

3. Click the [OK] button to complete the operation of adding a new registration location.

Delete

Preconditions for Normal Use of Function

The administrator has the authority to delete registration locations, and the registration locations that need to be deleted are not associated with the linkage module.

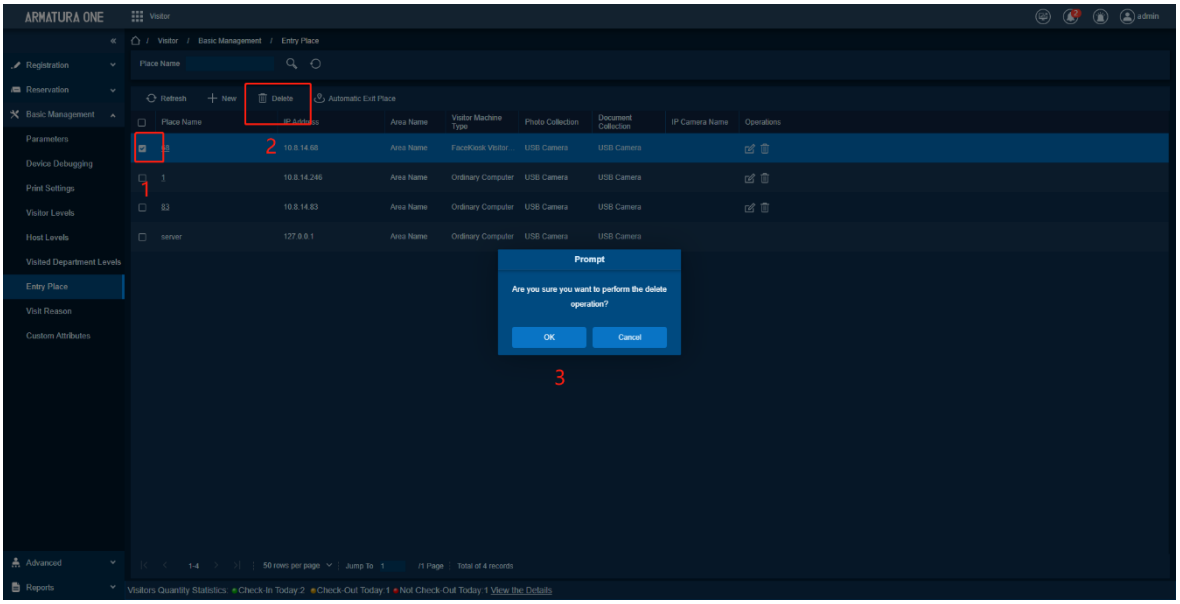
Function Usage Scenarios

Delete the registration location that is no longer needed, and the registration location with the IP address of 127.0.0.1 cannot be deleted.

Feature Trigger Result

Delete the registration location, there is no longer the registration location when the visitor registers.

Steps:



1. Check the registration location that needs to be deleted.
2. Click the [Delete] button, and a prompt box will pop up.
3. Click the [OK] button in the prompt box to complete the operation of deleting the registration location.

Automatic check-out location setting

Preconditions for Normal Use of Function

The administrator has the authority to set the automatic check-out location, the parameter setting has the function of setting the automatic check-out location, and the device that supports the check-out is online.

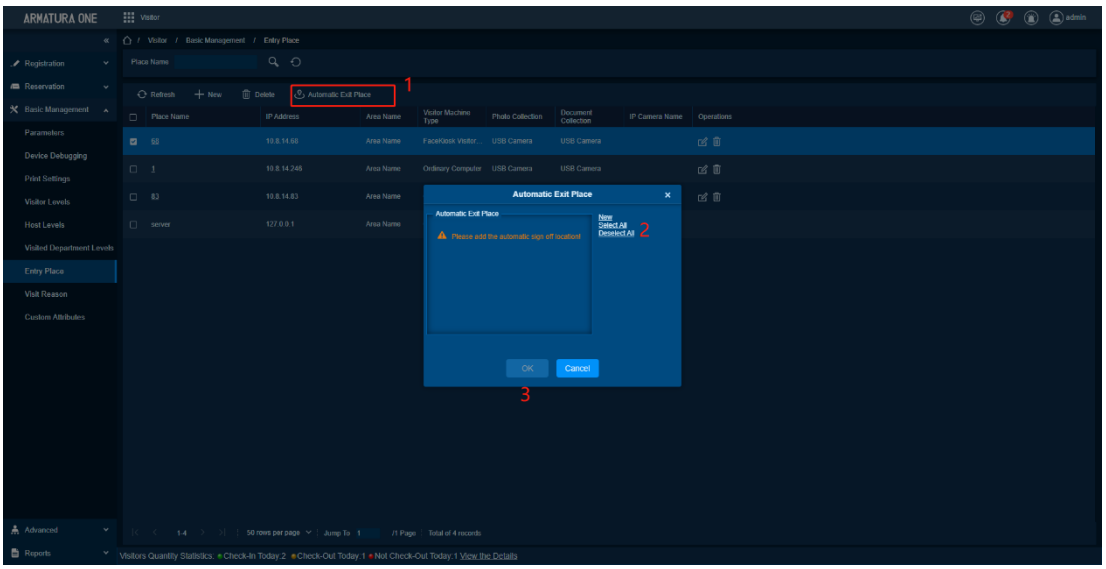
Function Usage Scenarios

Visitors do not need to check out at the front desk registration location, they only need to swipe their card or fingerprint on a device that supports check-out, and the check-out can be successful.

Feature Trigger Result

Set up an automatic check-out location, visitors do not need to go to the front desk to check-out at the check-out location.

Steps:



1. Click the [Automatic Exit Place] button to pop up a window.
2. Click to add as needed.
3. Click [OK] to complete the setting of automatic check-out location.

9.3.8. Visit Reason

Function Description

View, edit, and add to the visitor's reason.

Add

Preconditions for Normal Use of Function

The administrator has the adding permission, and the name of the new visit reason cannot be repeated.

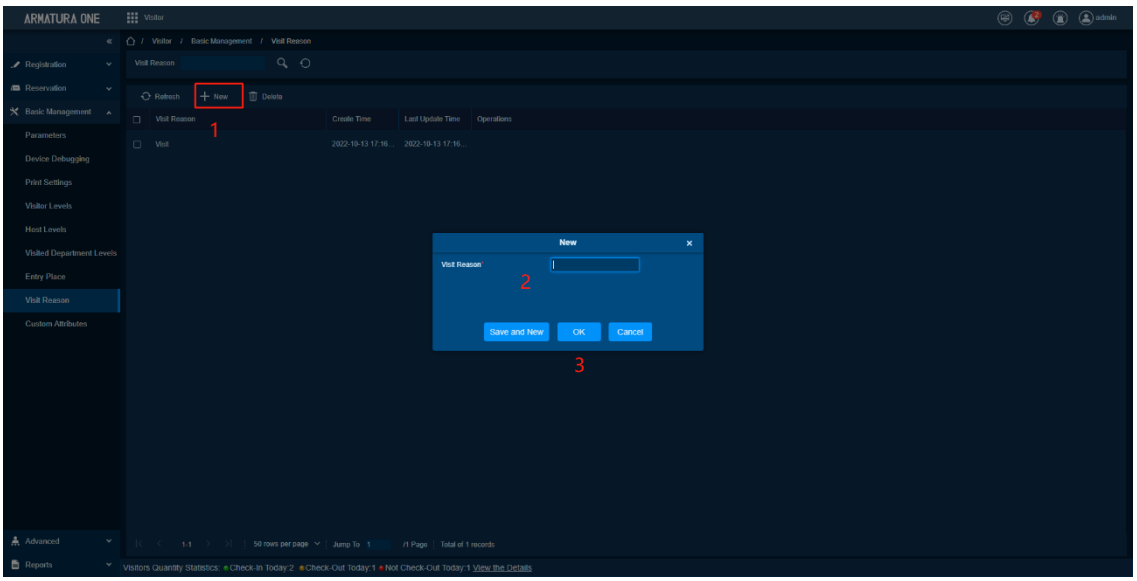
Function Usage Scenarios

When the visitor's reason does not match the current system's visit reason, you can add a visit **reason to match.**

Feature Trigger Result

Add a reason for the visit.

Steps:



1. Click the [**New**] button.
2. Enter the name of the reason for the visit.
3. Click the [**OK**] button to complete the operation of adding the reason for the visit.

Delete

Preconditions for Normal Use of Function

The administrator has the permission to delete the visit reason, and the visit reason list has information that can be deleted.

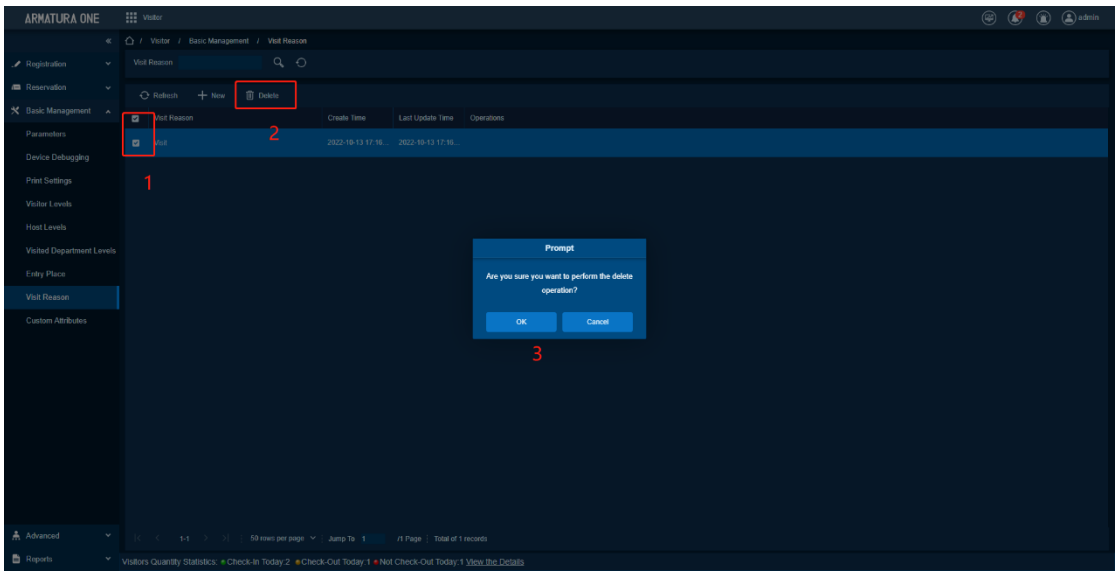
Function Usage Scenarios

Delete redundant visit reasons.

Feature Trigger Result

Delete the reason for the visit.

Steps:



1. Check the reason for the visit that needs to be deleted.
2. Click the [**Delete**] button, and a prompt box will pop up.
3. Click the [**OK**] button in the prompt box to complete the operation of deleting the reason for the visit.

9.3.9. Custom Attributes

Function Description

In order to display the visitor's information in more detail, some attributes can be customized.

Add

Preconditions for Normal Use of Function

The administrator has the right to add custom attributes.

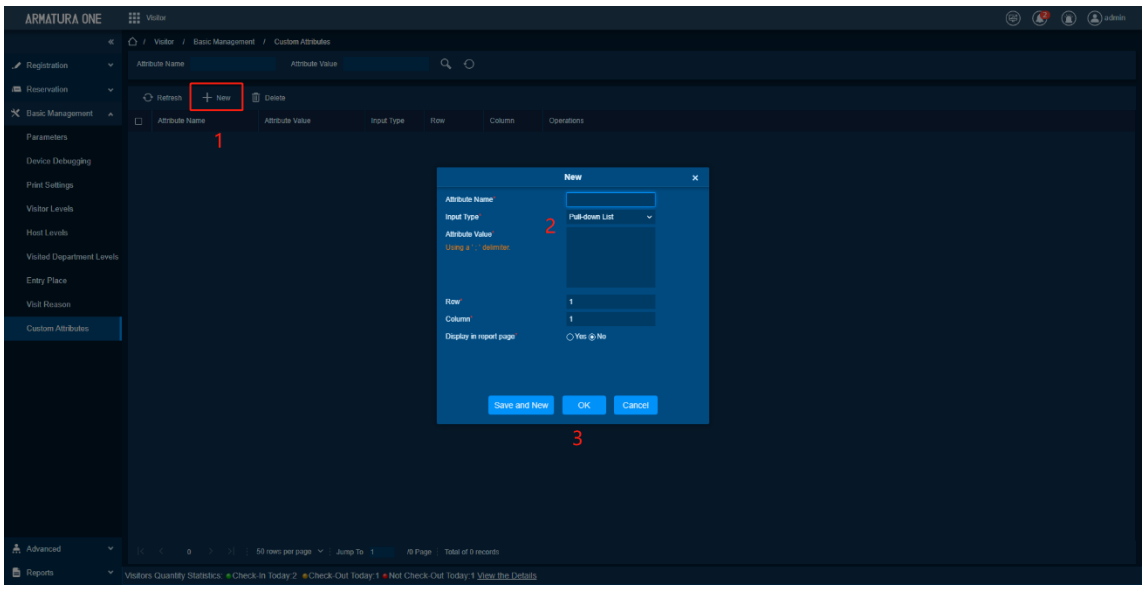
Function Usage Scenarios

When registering a visitor, if you need to register some other information, you can add the required fields here.

Feature Trigger Result

When the visitor is registered, the added field is displayed in the detail's information.

Steps:



1. Click the [**New**] button to pop up a window.
2. Enter the field information that needs to be added in the pop-up window, the field description is as follows:

Attribute Name: Attribute name (required)

Input Type: Input type (drop-down list, single selection, multiple selection, input box) (required)

Attribute Value: Field value (required)

Row: Number of rows (required)

Column: The number of columns (required)

Display in report page: Whether to display in the visitor list (required)

3. After filling in, click the [OK] button to complete the adding operation.

Delete

Preconditions for Normal Use of Function

The administrator has the right to delete custom attributes, and there is custom attribute information in the list.

Function Usage Scenarios

When some custom attributes are not needed, they can be deleted.

Feature Trigger Result

Delete unnecessary custom attributes.

Steps:

1. Check the custom attributes that need to be deleted.
2. Click the [Delete] button, and a prompt box will pop up.
3. Click the [OK] button in the pop-up prompt box to complete the delete operation.

9.4. Advanced

Function List

Functions	Description
Category	Set the parameters of the guest module
Watch List	Set the parameters of the equipment used by the guest module
Alert Template	Set the parameters of the print function
Linkage	Set permissions for visitors

9.4.1. Category

Function Description

View and edit personnel types.

Add

Preconditions for Normal Use of Function

The administrator has the permission to add new person types, and the new name cannot be repeated.

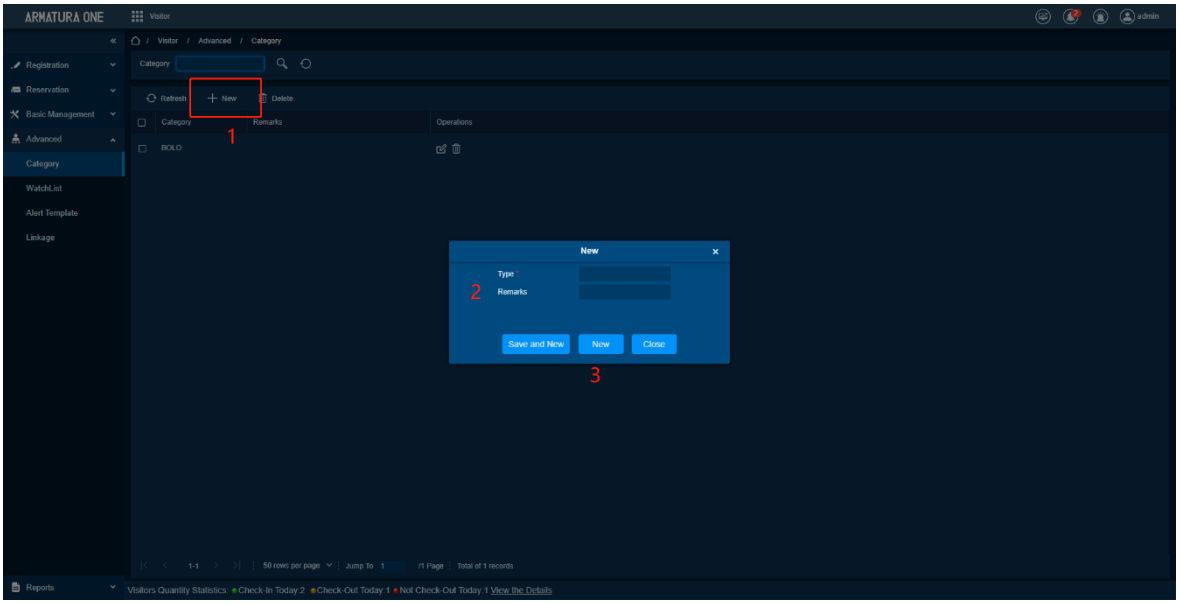
Function Usage Scenarios

When a visitor checks out, different visitors sometimes need to be distinguished by the monitoring list.

Feature Trigger Result

Add a monitor type.

Steps:



1. Click the **[New]** button to pop up a window.
2. Fill in the information in the pop-up window, the field descriptions are as follows:

Type: Monitoring type (required)

Remarks: Remarks

3. Click the **[New]** button to complete the adding operation.

Delete

Preconditions for Normal Use of Function

The administrator has the right to delete the type of personnel, and the type of personnel to be deleted has no data.

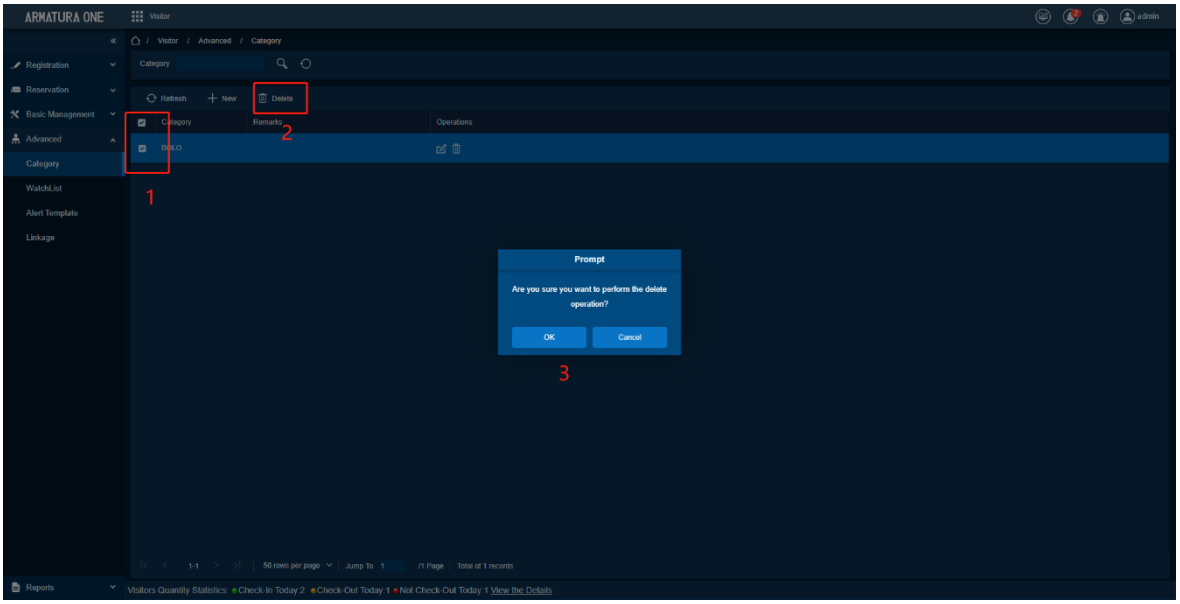
Function Usage Scenarios

Delete unnecessary personnel types.

Feature Trigger Result

Delete personnel type.

Steps:



1. Check the type of personnel to be deleted.
2. Click the [Delete] button, and a prompt box will pop up
3. Click the [OK] button to complete the operation of deleting the personnel type.

9.4.2. Watch List

Function Description

Can manage the visitors added to the monitoring list.

Add

Preconditions for Normal Use of Function

The administrator has adding permissions.

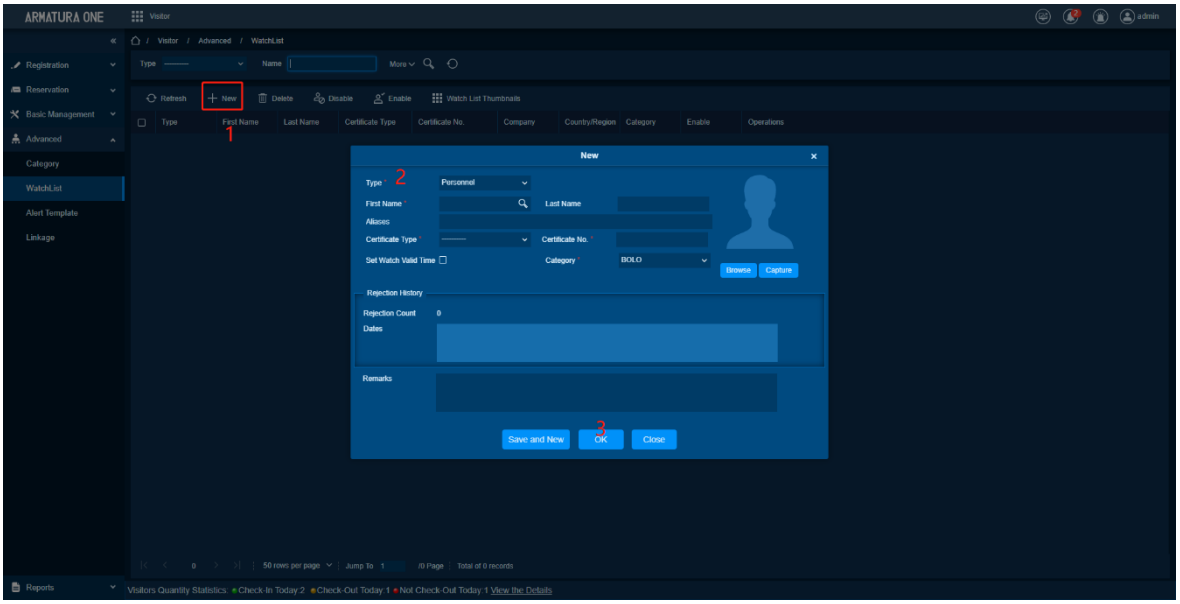
Function Usage Scenarios

When a visitor has irregular operations or other behaviors that affect the park, the visitor will be monitored. When the visitor registers again, it will be prompted on the monitoring list.

Feature Trigger Result

Visitors added in the monitoring list.

Steps:



1. Click the **[New]** button to pop up a window.
2. Fill in the relevant information in the pop-up window, the field descriptions are as follows:

Type: Monitoring type (personnel, company, nationality) (required)

First Name: First Name (required)

Last Name: Last name

Aliases: Alias

Certificate Type: Certificate type (required)

Certificate No.: Certificate number (required)

Set Watch Valid Time: Set the valid Timetable

Category: Monitoring type (required)

Start Time: Start time

End Time: End time

Browse: Browse photos

Capture: Snap a photo

Rejection Count: The number of rejections

Dates: Rejection date

Remarks: Remarks

3. Click [**OK**] to complete the new operation.

Delete

Preconditions for Normal Use of Function

The administrator has deleted permission, and data in the list can be deleted.

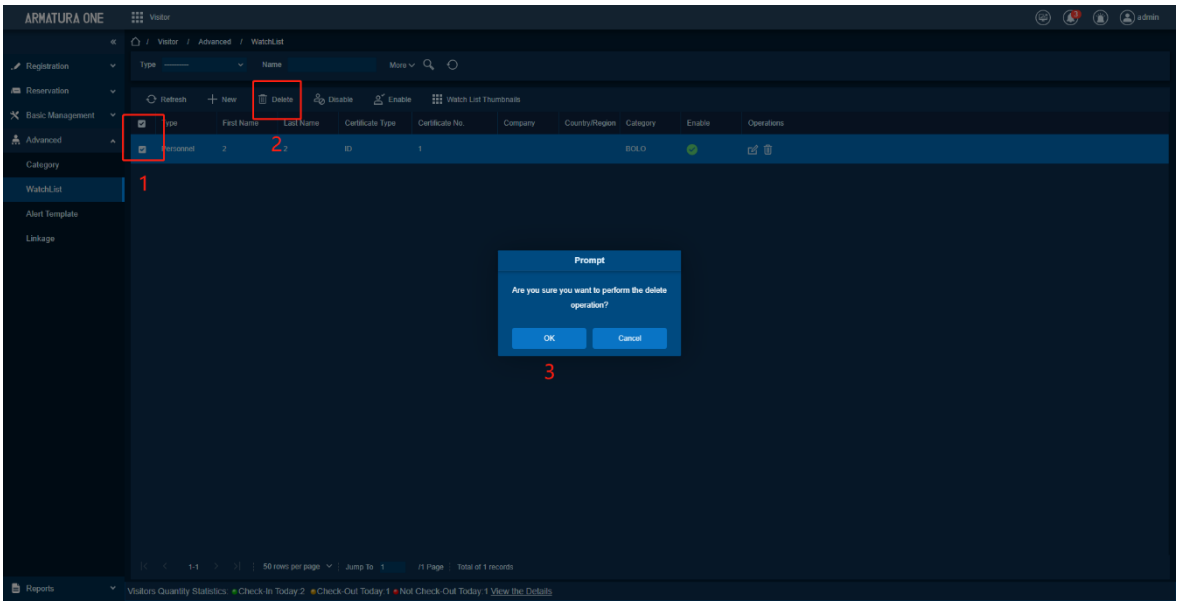
Function Usage Scenarios

Used when you don't need to add a visitor to the monitoring list.

Feature Trigger Result

Delete monitoring, the visitor will no longer be prompted in the monitoring list when registering.

Steps:



1. Check the monitoring data that needs to be deleted.
2. Click the [Delete] button, and a prompt box will pop up.
3. Click [OK] to complete the operation of deleting the monitoring list.

Disable

Preconditions for Normal Use of Function

The administrator has the permission to disable, and there is data in the list, and the data status is enabled.

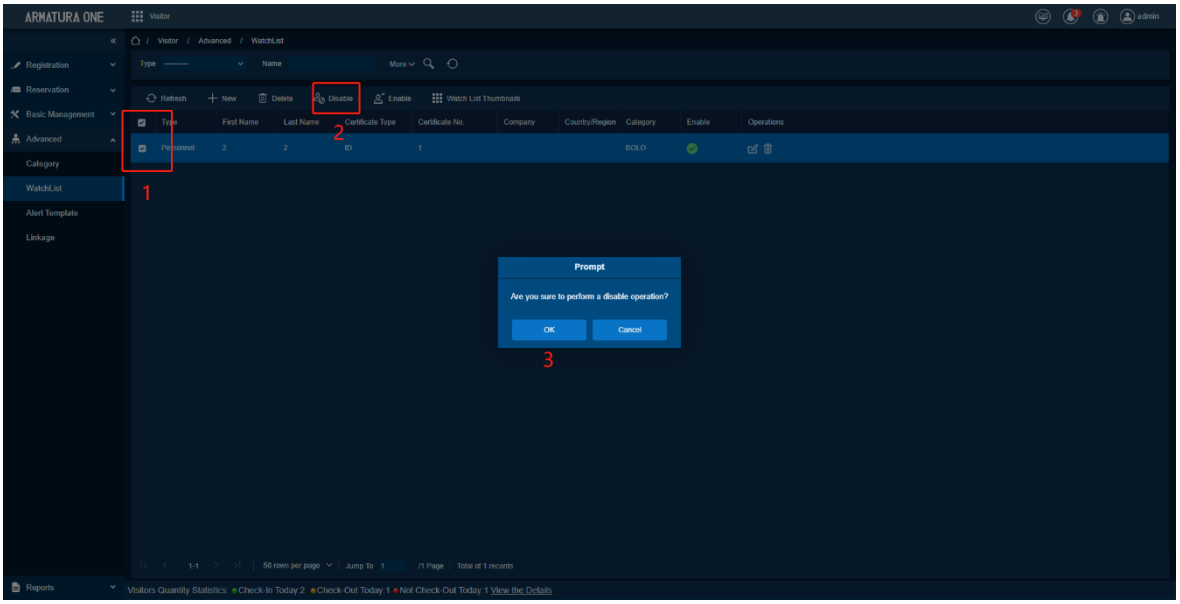
Function Usage Scenarios

There is no need to monitor this piece of data for the time being, but it may be used for monitoring again later.

Feature Trigger Result

Disable this piece of data. When registering, the visitor will not be prompted in the monitoring list in the pop-up window, and it can register directly.

Steps:



1. Check the data that needs to be disabled.
2. Click the [Disable] button, and a prompt box will pop up.
3. Click the [OK] button in the prompt box to complete the disabling operation.

9.4.3. Alert Template

Function Description

For visitors' sign-in, sign-out, appointment, sign-out timeout, appointment timeout, and audit events, send different emails or short messages to the corresponding personnel for unused events. You need to configure the mailbox parameters and SMS message platform in the system module to send short messages and mail.

Add

Preconditions for Normal Use of Function

The administrator has the Add Prompt Template permission, and the name of the Add Prompt Template cannot be repeated.

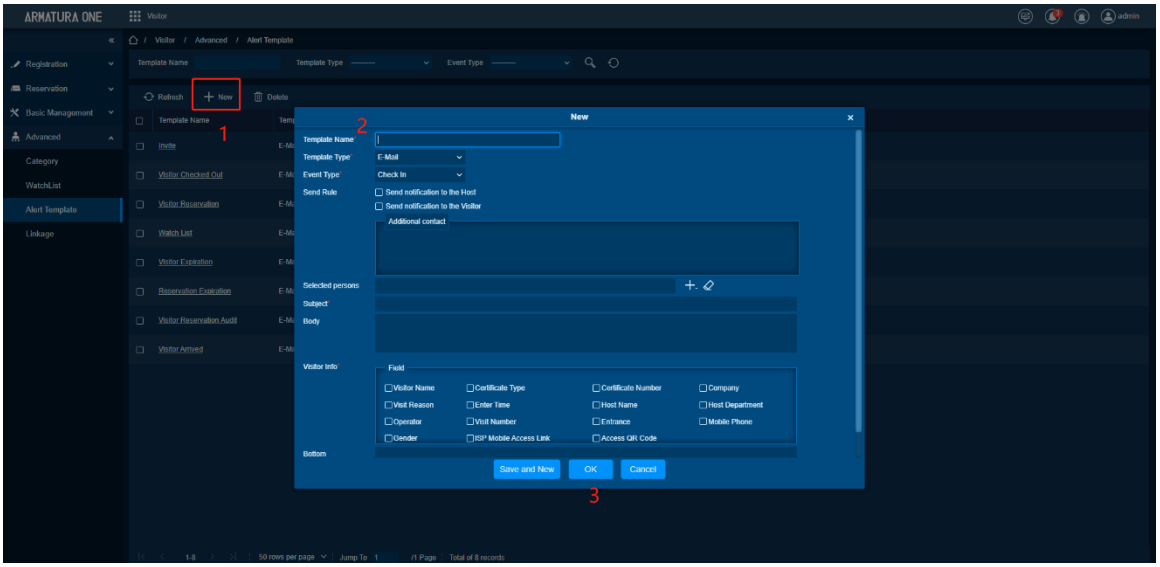
Function Usage Scenarios

Add a Prompt Template type that meets the needs to apply to different visitor events.

Feature Trigger Result

Add a Prompt Template.

Steps:



1. Click **[New]** button to pop up a window.
2. Fill in the relevant information in the pop-up window, the field descriptions are as follows:

Template Name	Template name (required and cannot be repeated)
Template Type	Template type (email, WhatsApp, Amazon SMS, SMS modem, Line) (required, when selecting Line, you need to select the corresponding platform)
Event Type	Event type (check-in, check-out, appointment, Monitoring List, check-out timeout, appointment timeout, approved\rejected) (required)
Send Rule	Sending rules
Additional contact	Additional informant
Selected persons	List of selected persons
Subject	Subject (required)
Body	Body
Visitor Info	Visitor information (required)
Bottom	Enter endnote.

3. Click **[OK]** button to complete the Add operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete permission, and there are data that can be deleted in the list.

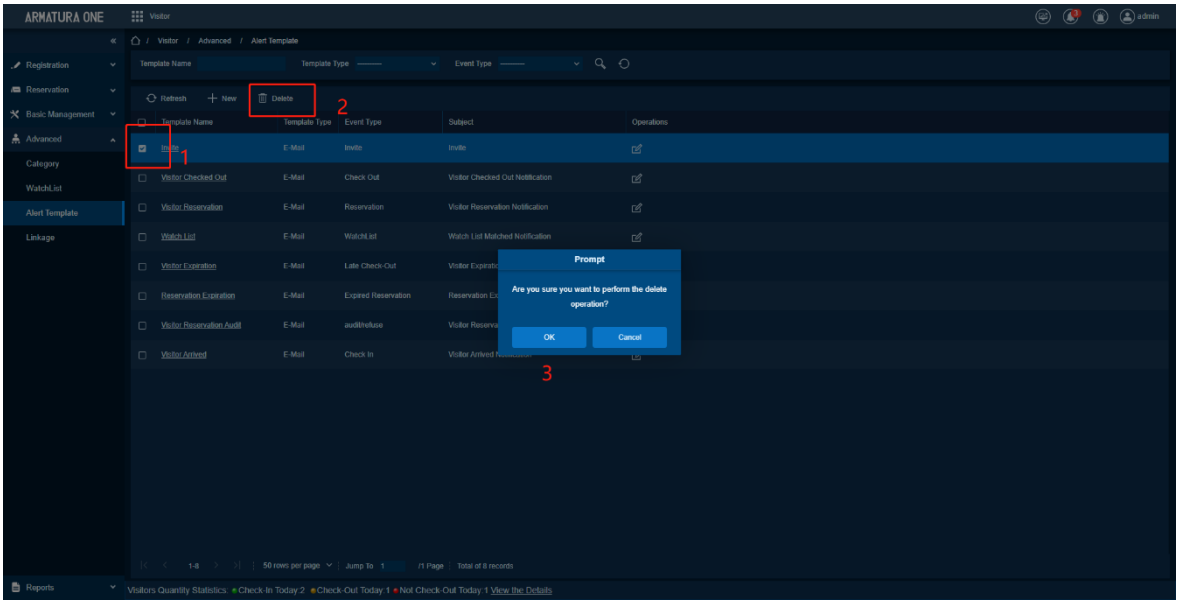
Function Usage Scenarios

Delete unnecessary or redundant Prompt Template.

Feature Trigger Result

Delete Prompt Template

Steps:



1. Check the data that needs to be deleted.
2. Click **[Delete]** button, and a prompt box will pop up.
3. Click **[OK]** button in the prompt box to complete the Delete Prompt Template operation.

9.4.4. Linkage

Function Description

In response to different visitor trigger events, send SMS or email to the corresponding personnel, and edit the sending rules in the Prompt Template function.

Add

Preconditions for Normal Use of Function

The administrator has the add linkage permission, and the permission name of add cannot be repeated.

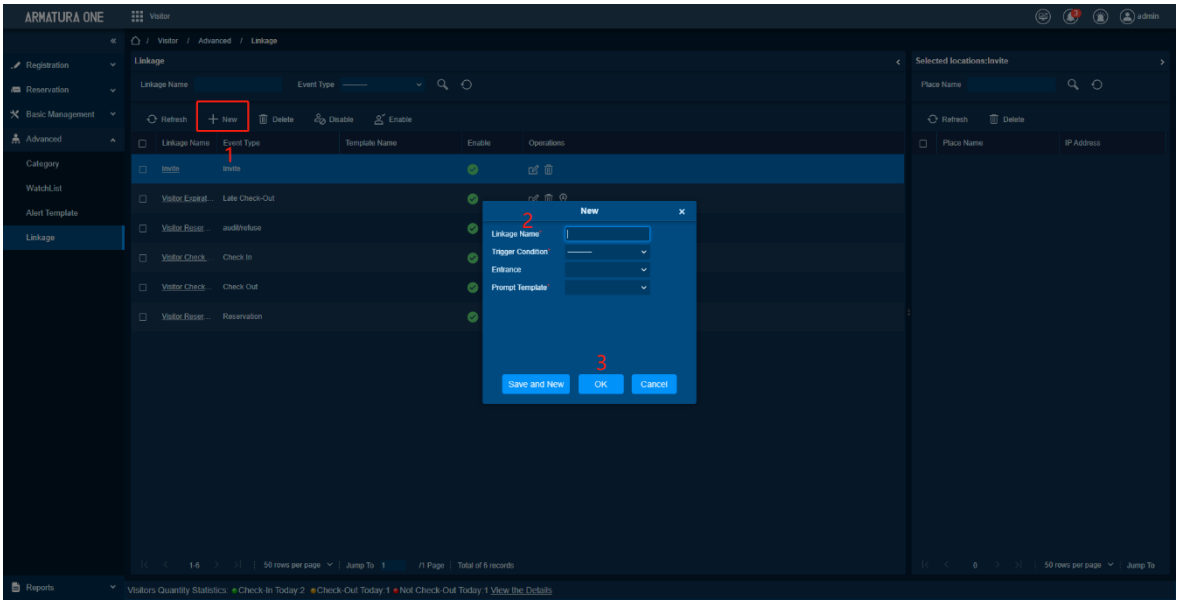
Function Usage Scenarios

The existing Linkage is not suitable for certain event types.

Feature Trigger Result

Add a Linkage data.

Steps:



1. Click **[New]** button to pop up a window.
2. Select the relevant information, the field descriptions are as follows: -

Linkage Name: Linkage name (required, cannot be repeated)

Trigger Condition: Trigger condition (required)

Entrance: Entry location

Prompt Template: Prompt Template (data from the Prompt Template list)

3. Click **[OK]** button to complete the Add Linkage operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete linkage permission, and there are data that can be deleted in the list.

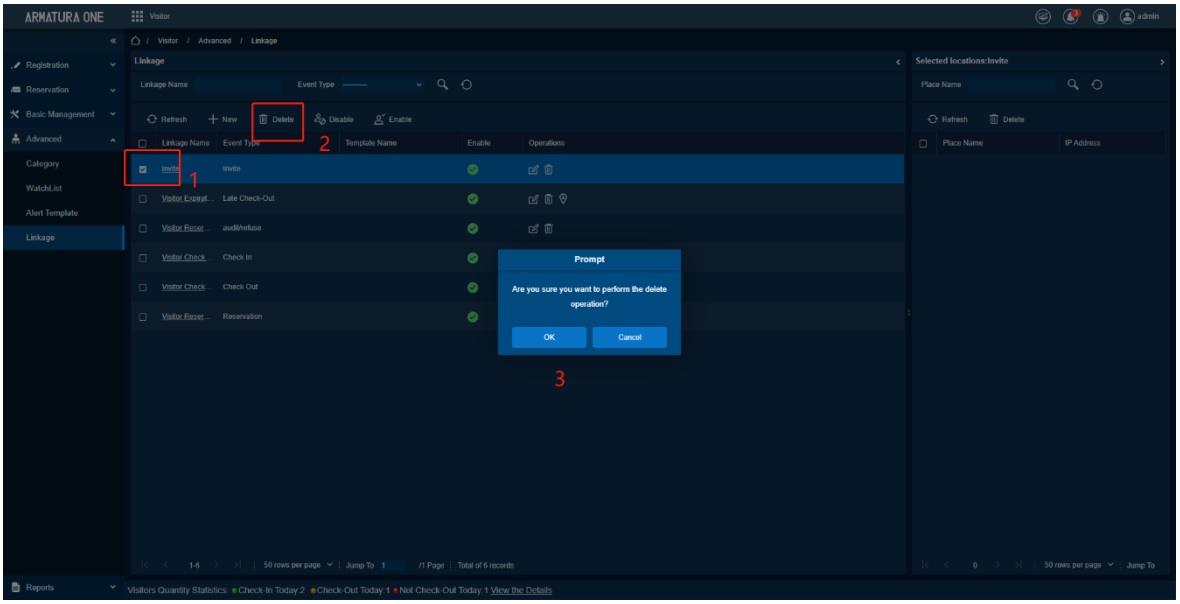
Function Usage Scenarios

You can use the delete function when you don't need some Linkage, or when linkage is redundant.

Feature Trigger Result

Delete the checked linkage.

Steps:



1. Check the Linkage that needs to be deleted.
2. Click **[Delete]** button, and a prompt box will pop up.
3. Click **[OK]** button in the prompt box to complete the Delete operation.

Disable

Preconditions for Normal Use of Function

The administrator has the right to disable.

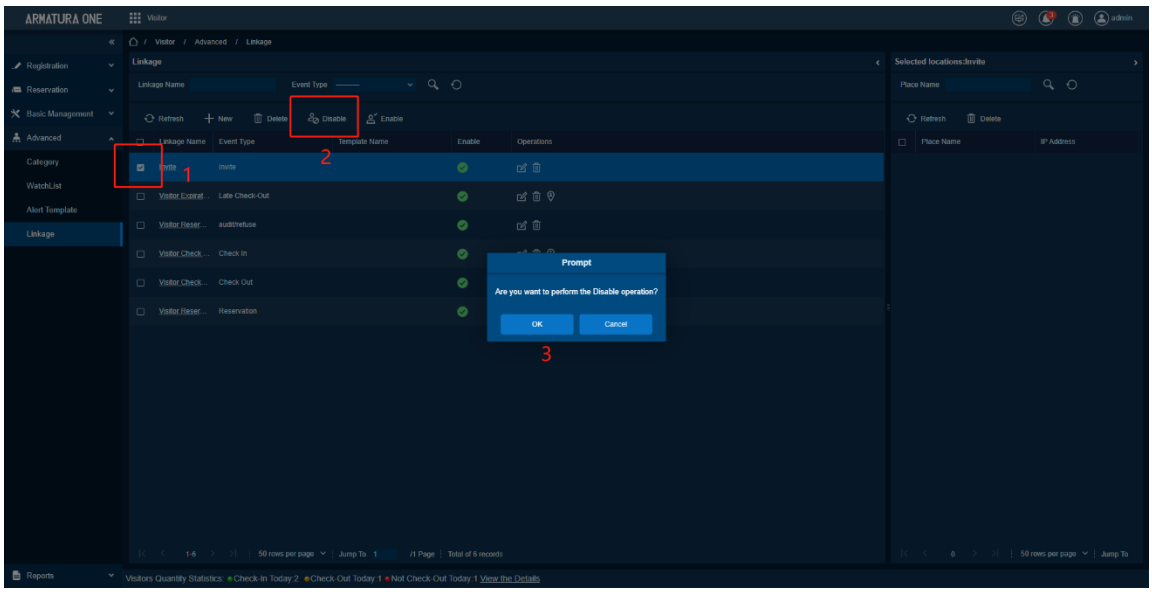
Function Usage Scenarios

Used when a certain Linkage is not needed temporarily.

Feature Trigger Result

After disabling, the trigger event of this Linkage will not send email or SMS.

Steps:



1. Check the Linkage that needs to be disabled.
2. Click **[Disable]** button, and a prompt box will pop up.
3. Click **[OK]** button in the prompt box to complete the disabling operation.

Enable

Preconditions for Normal Use of Function

The administrator has enabled permissions, and there are disabled data in the list.

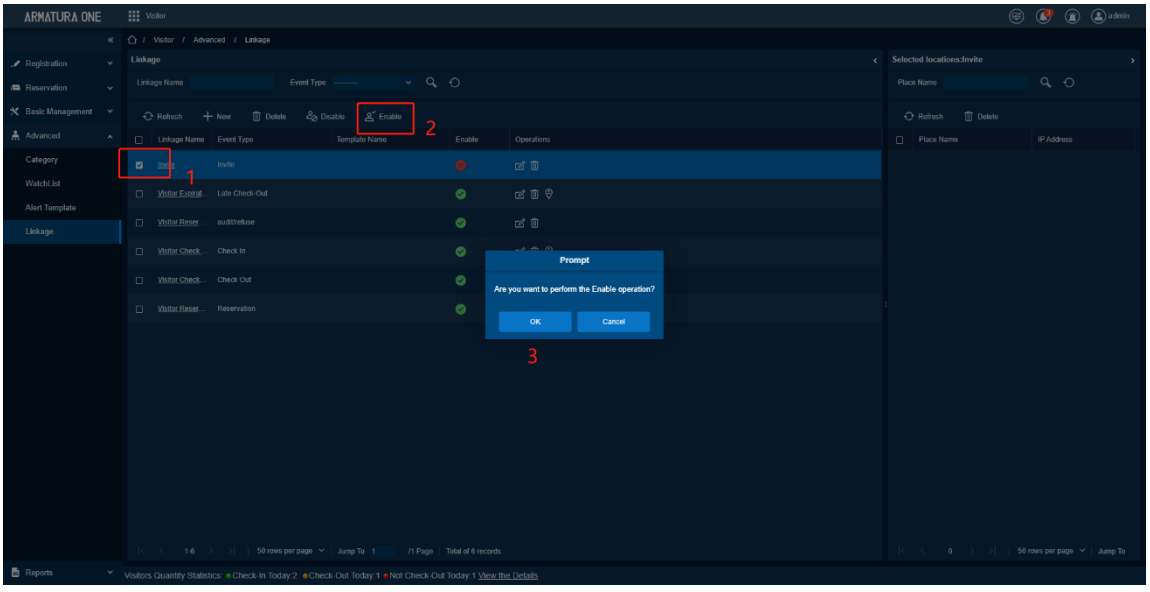
Function Usage Scenarios

When you need a certain Linkage and this Linkage is disabled, you can click to enable.

Feature Trigger Result

After enabling, the trigger event of this Linkage will send SMS or email.

Steps:



1. Check Linkage that needs to be enabled.
2. Click **[Enable]** button, and a prompt box will pop up.
3. Click **[OK]** in the prompt box to complete the activation operation.

Delete Place of Registration

Preconditions for Normal Use of Function

The administrator has right to delete Place of Registration permission, Linkage and Place of Registration.

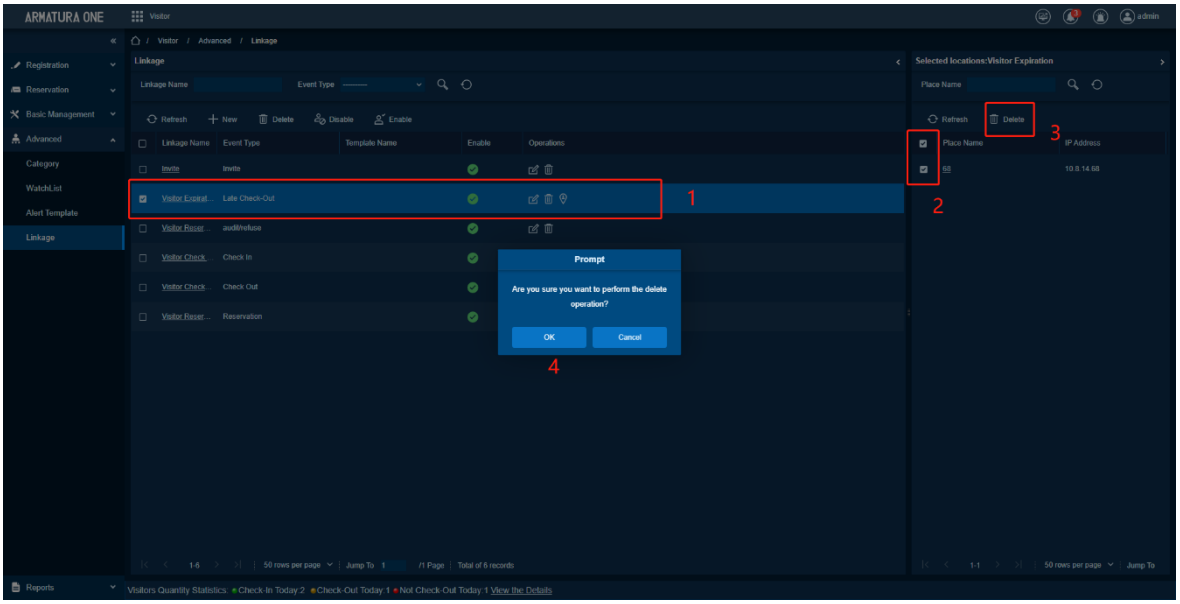
Function Usage Scenarios

Place of Registration not needed in Delete Linkage.

Feature Trigger Result

Place of Registration in Delete Linkage

Steps:



1. Select the Linkage on the left that requires Delete Place of Registration.
2. Select the Place of Registration that needs to be deleted on the right.
3. Click **[Delete]** button, a prompt box will pop up.
4. Click **[OK]** in the prompt box to complete the Delete Place of Registration operation.

9.5. Reports

Function List

Functions	Description
Last Visited Location	View and export the last visitor location of visitors.
Visitor History Record	View, delete, and Export visitor's history.

9.5.1. Last Visited Location

Function Description

Record the location of the access control device each time the visitor swipes the card to enter.

Export

Preconditions for Normal Use of Function

The administrator has export permission.

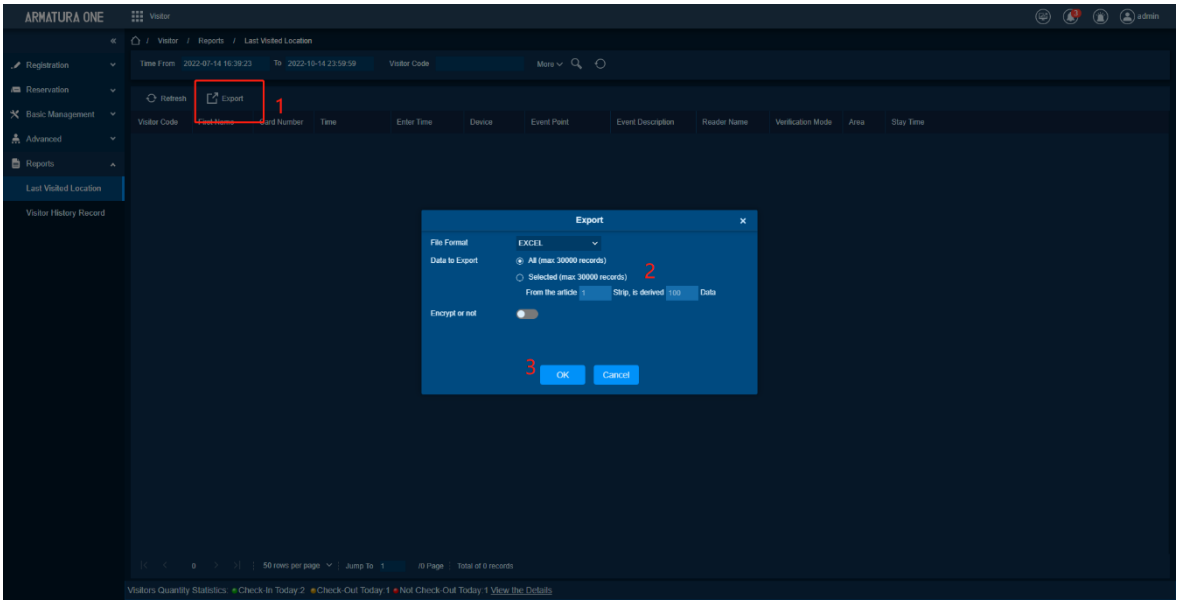
Function Usage Scenarios

Use when you need to export the information to the software.

Feature Trigger Result

Operations	Description
Select Excel	Exported format is EXCEL.
Select PDF	Exported format is PDF.
Select CSV	Exported format is CSV.
All Data	Export all data.
Choose the Exported Quantity	Export the data in the selected range.

Steps:



1. Click **[Export]** button to pop up a window.
2. Select Export format in the pop-up window.
3. Select the data range of export.
4. Click **[OK]** button to complete the export operation, and the export data can be viewed in the download content of the browser.

9.5.2. Visitor History Record

Function Description

Record the time, status, interviewee, and other information of each visitor's Place of Registration and check-out location.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there is information that can be deleted in the list.

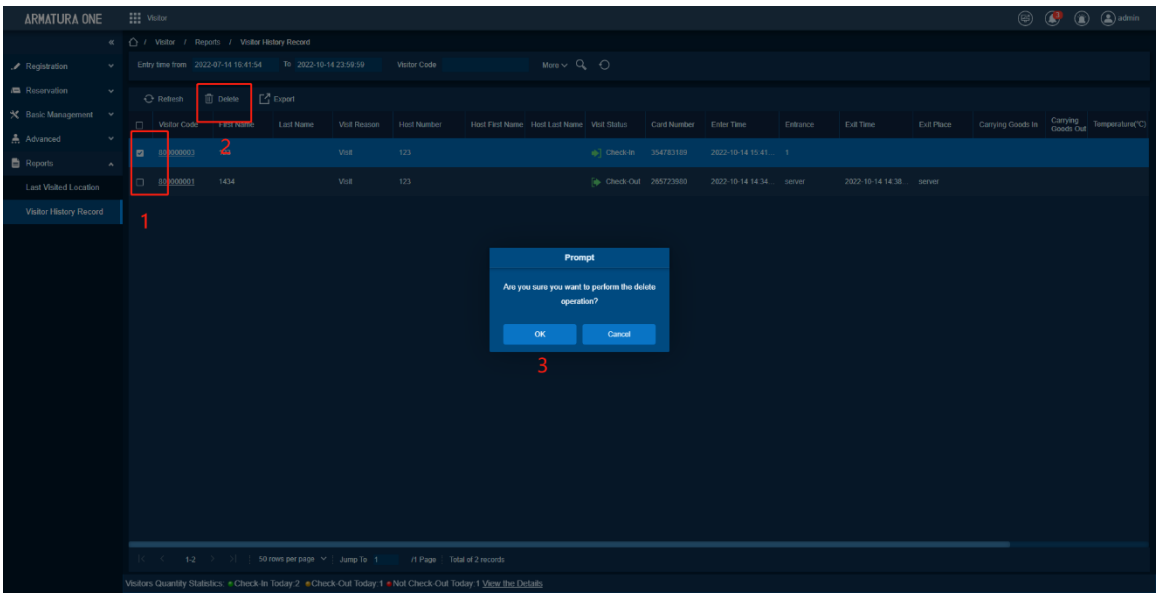
Function Usage Scenarios

Delete redundant or unnecessary data.

Feature Trigger Result

Delete the checked data.

Steps:



- Select the data that needs to be deleted.
- Click **[Delete]** button, and a prompt box will pop up.
- Click **[OK]** in the prompt box to complete the Delete operation.

Export

Preconditions for Normal Use of Function

The administrator has the export function authority.

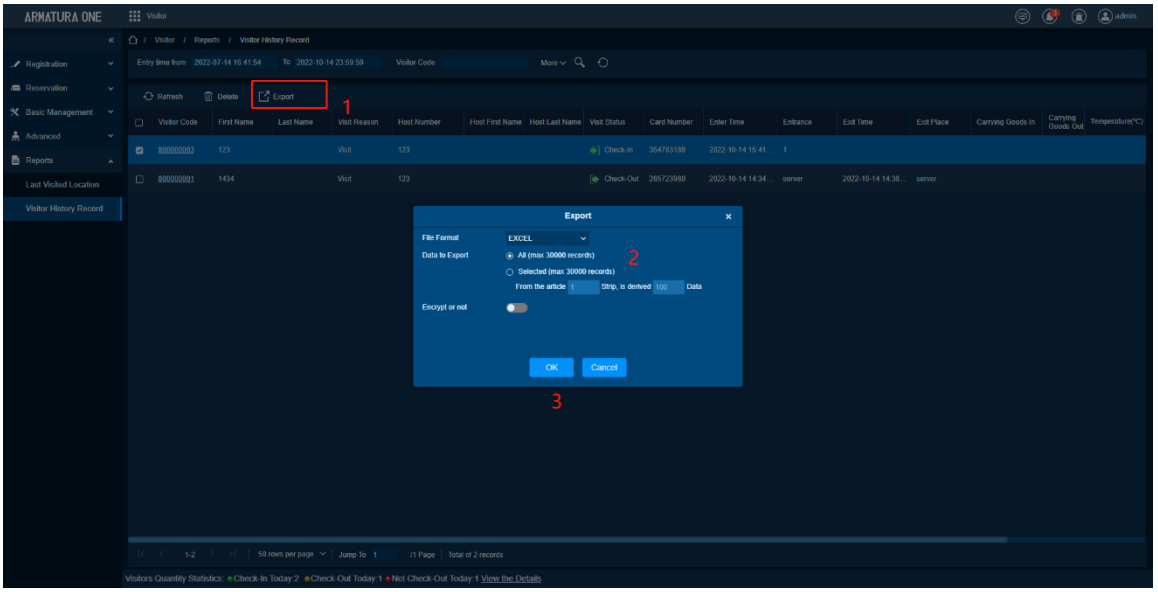
Function Usage Scenarios

It is used when the information export software is needed.

Feature Trigger Result

Operations	Description
Select Excel	Exported format is EXCEL
Select PDF	Exported format is PDF
Select CSV	Exported format is CSV
All Data	Export all data
Choose the Exported Quantity	Export the data in the selected range

Steps:



- Click **[Export]** button to pop up a window.
- Select the format that needs exported.
- Select the data range that needs to be exported.
- Click **[OK]** button to complete operations everywhere, and the export data can be viewed in the download content of the browser.

10. Parking Management

Modern parking management involves all aspects of management, of which vehicle management is an important part. In special areas, such as special parking lots, military districts, government agencies, and residential areas, vehicles must be strictly managed in real time, that is, strictly monitor the time of entry/exit, and register and identify vehicles (including internal vehicles and external vehicles). In large-scale areas, there are many incoming/outgoing vehicles. If you need to manually identify each car, it will be time-consuming and difficult to implement management, query, and maintenance, resulting in inefficiency. To improve this management model that is not suitable for modern parking lots, military areas, government agencies and residential areas, it is necessary to use computer networks to realize automatic and intelligent vehicle management to monitor and manage all vehicles at entrances and exits effectively and accurately. This requires corresponding application software to manage the parking lot efficiently and intelligently.

10.1. Operation Wizard

This function is used to quickly configure your parking lot, and quickly complete the software configuration according to the sequence of steps.

Function List

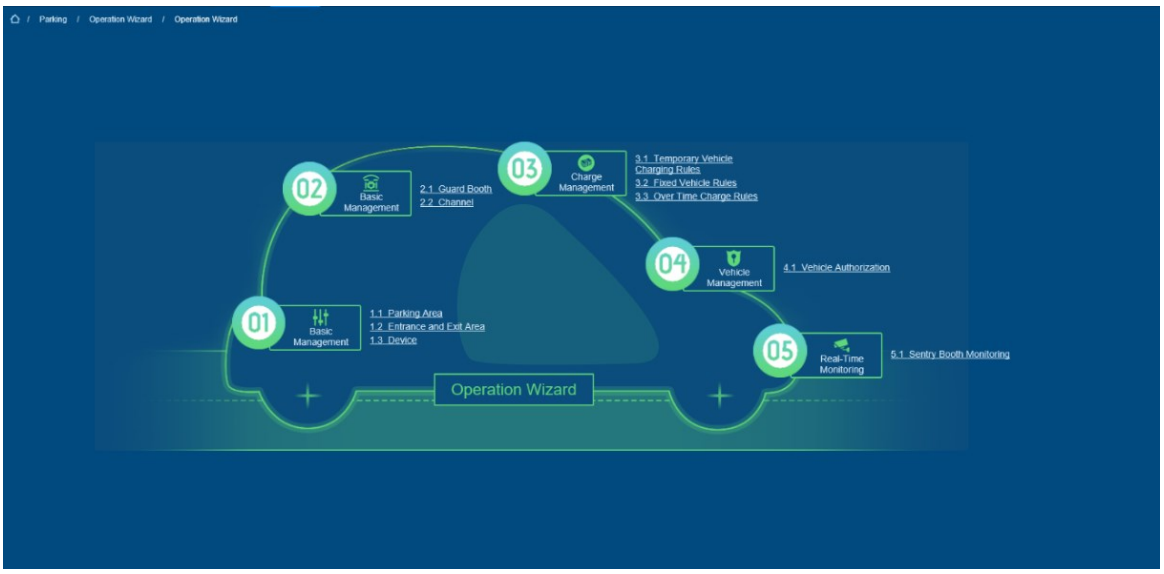
Operations	Description
Operation Wizard	Guide the user to perform the basic configuration of the system according to the operating steps.

10.1.1. Operation Wizard

Function Introduction

The "Operation Wizard" page guides the user through the basic configuration of the system according to the operating steps. After completing all the basic configurations, you can use the online monitoring function.

Interface Display



Click the cue point on the page to go to the corresponding function page for setting.

10.2. Basic Management

This function is used to configure the basic settings of your parking lot. Here you can define the parameters of your parking lot, add devices that bind each of your guard boxes, define the vehicles in your parking lot and perform shift operations for your employees.

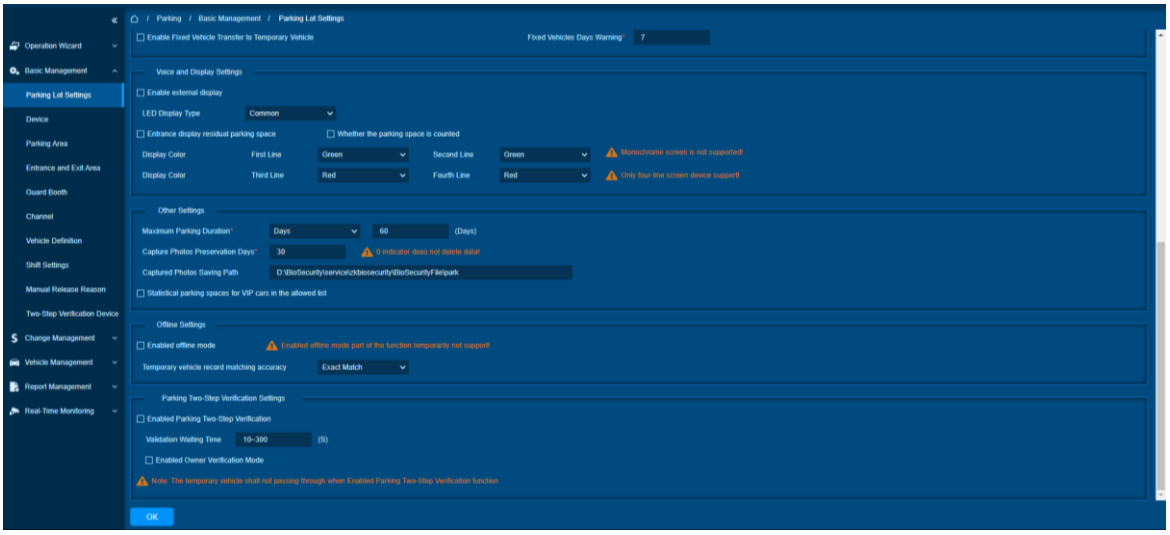
Function List

Operations	Description
Parking Lot Settings	Set the basic public parameters of the parking lot.
Device	Manage parking device.
Parking Area	View, add, delete parking area.
Entrance and Exit Area	View, add, delete entrance, and exit area.
Guard Booth	View, add, delete guard booth.
Channel	View, add, delete channel.
Vehicle Definition	View, add, delete vehicle definition.
Shift Settings	View, add, delete shift.
Manual Release Reason	View, add, delete manual release reason.

10.2.1. Parking Lot Settings

Function Introduction

Set the basic public parameters of the parking lot.



Field Descriptions are as follows:

Parking Lot Name: Set the name of the parking lot.

Company Name: Set the company name.

Parking Lot Mode: Set the parking lot mode of the parking lot.

Show parking space number: Set whether to display the parking lot number.

Enable Fixed Vehicle Multiple in and Out: After checking, the fixed car can enter and exit multiple times.

Enable Temporary Vehicle Multiple in and Out: After checking, the temporary car can enter and exit multiple times.

Matching Precision of Entrance and Exit: Set matching accuracy.

Enable Shift Process: Start shift after check.

Types of Vehicles Allowed to Release under Full Parking Yard: Set the vehicle definition that is allowed to enter after the parking space is full.

Special license plate contains characters: Set the characters contained in the special license plate.

Duplicate license plate waiting time: Set the time to wait when the license plate is repeated.

Enable Fixed Vehicle Charges: After ticking, the fixed car charging standard is enabled.

Enable the Consumer Discount: After checking, enable consumption discount.

Print Fee Receipts: After checking, print the fee receipt.

Unmatched Processing Mode: Set the processing method when the license plate is not matched.

Custom Currency: Set the custom currency.

Statistical analysis of fixed parking spaces: After checking, the fixed car will count the parking spaces.

Enable Fixed Vehicle Transfer to Temporary Vehicle: After checking, the fixed car will be turned into a

temporary car.

Fixed Vehicles Days Warning: Set the number of days for fixed vehicle warning.

Enable external display: After checking, enable external display.

LED Display Type: Set the display language.

Entrance displays residual parking space: After checking, the display shows the remaining parking spaces.

Whether the parking space is counted: After checking, count parking spaces.

Display Color: Set the display color.

Maximum parking duration: Set the maximum time the vehicle can stay.

Capture Photos Preservation Days: Set the number of days the captured photos can be saved.

Captured Photos Saving Path: Set the save path of the captured photos.

Enabled offline mode: After checking, enable offline mode.

Temporary vehicle record matching accuracy: Matching accuracy when setting offline mode.

Enable Parking Two-Step Verification and Set Validation Time: For security-critical environments, scenarios that require verification of the driver's identity before entering or leaving. Driver should be verification both identity and vehicle license plate number within validation time.

Enable Owner Verification Mode: Only the identity of the registered vehicle owner can be successfully verified.

10.2.2. Device

Function Introduction

Manage the device of the parking module.

Add

Preconditions for Normal Use of Functions

The administrator has the function rights of the newly added device, and the administrator knows the IP, port, username, and password of the newly added device.

Function Usage Scenarios

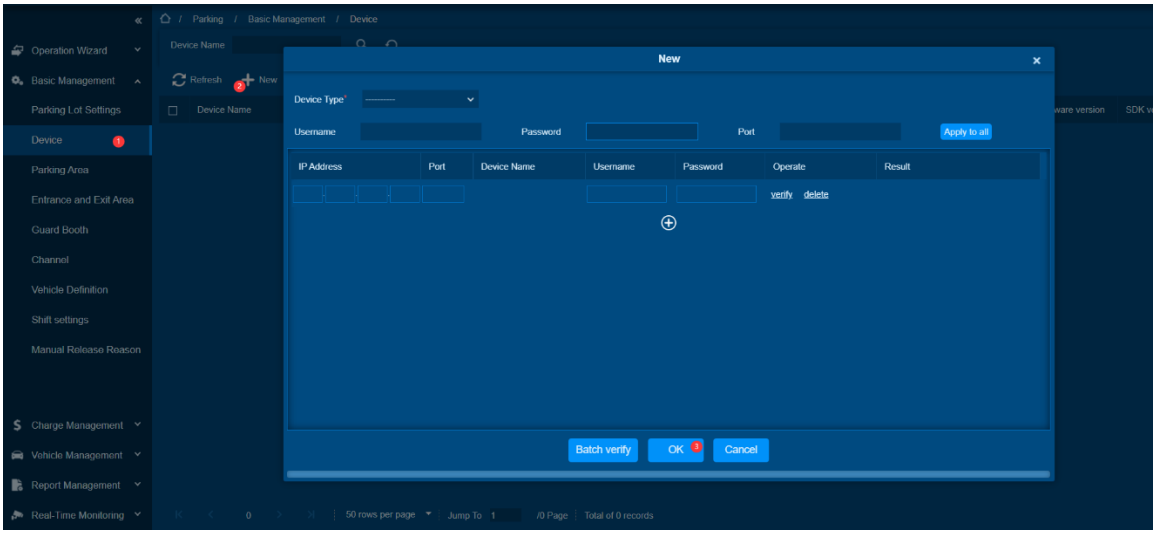
Use when you need to add parking device.

Feature Trigger Result

Add a parking device.

Steps:-

- Click [**New**] button, and a new window will pop up.



- Select the device type to fill in the device parameters and complete the device addition.

Device Type: Select the device type, optional LPRC series device and LPR CarID device.

Username (Menu Bar): Quickly configure the username of all devices, which can be applied to all devices in the form.

Password (Menu Bar): Quickly configure the password of all devices, which can be applied to all devices in the form.

Port (Menu Bar): Quickly configure the ports of all devices, which can be applied to all devices in the form.

Apply to All: Apply the username, password, and port number on the menu bar to all the device content added in the form.

IP Address: Set the IP address of the device.

Port: Set the port number.

Device Name: Set the device name.

Username: Set the username.

Password: Set the password.

Verify: To verify whether the device can be successfully connected, the result of the verification will be displayed in the Result column.

Delete: Delete this line of device.

- Click [**OK**] to complete the operation of adding device.

Delete

Preconditions for Normal Use of Functions

The administrator has the permission to delete devices, and there is device information that can be deleted in the list.

Function Usage Scenarios

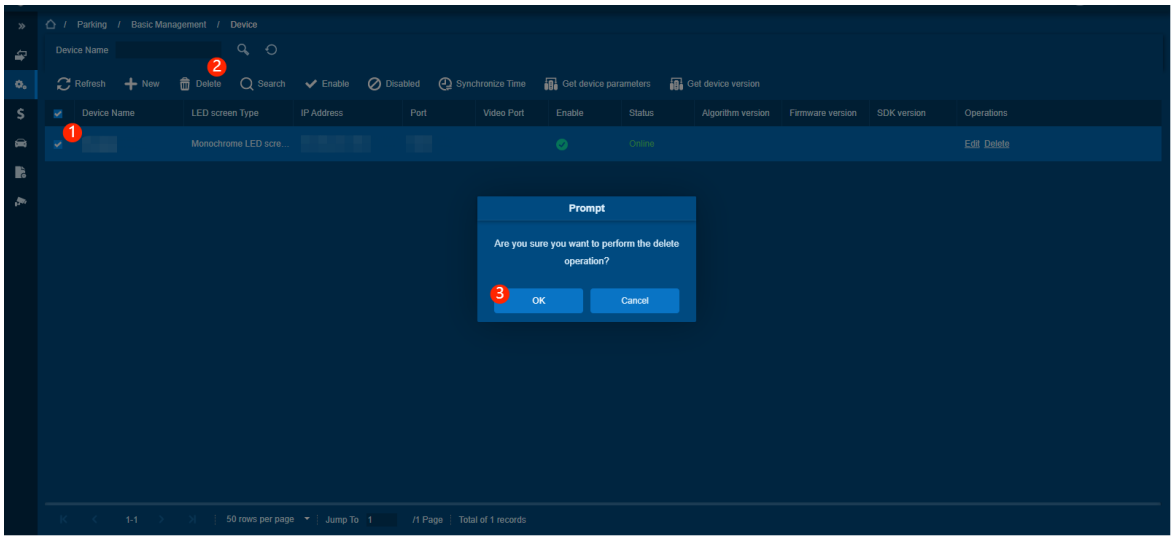
When you don't need a device, you can check it and delete it.

Feature Trigger Result

Delete checked device.

Steps:-

- Check the device that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete operation.



Search

Preconditions for Normal Use of Functions

The administrator has the search function permission.

Function Usage Scenarios

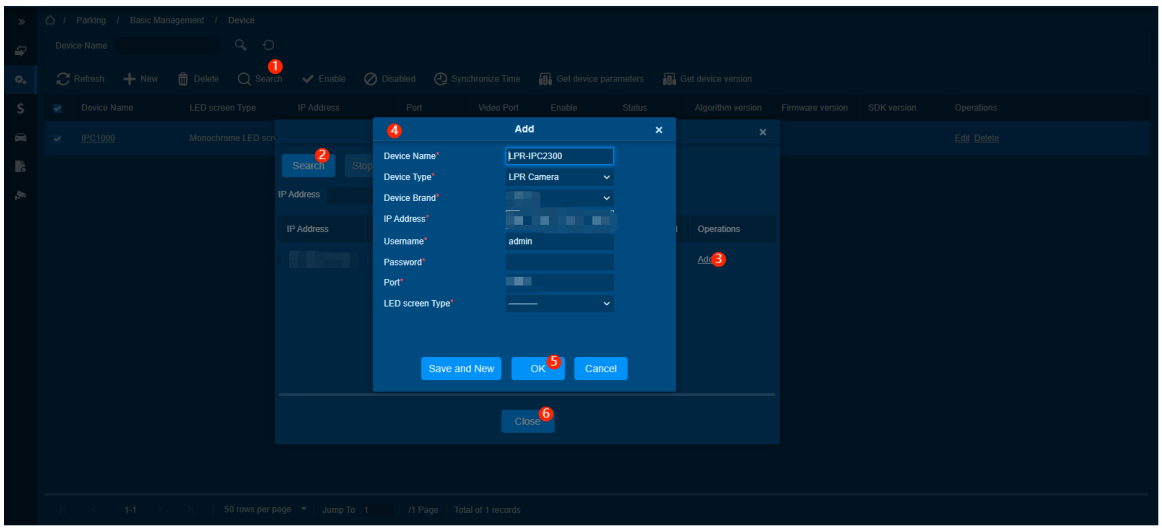
When the administrator wants to add a device, he can search for online parking devices through the search function.

Feature Trigger Result

Search all online parking device.

Steps:-

- Click [**Search**] button, and a window will pop up.
- Click [**Search**] button in the pop-up window to start searching for devices.
- Click [**Add**] for the searched device, and a new window will pop up.
- Fill in the relevant information, the items marked with * are required and the field description is the same as the new function.
- Click [**OK**] button to complete the adding operation.
- Click [**Close**] to close the search window.



Enable

Preconditions for Normal Use of Functions

The administrator has the authority to enable the function, there are data that can be operated in the list, and the device that needs to be operated is online.

Function Usage Scenarios

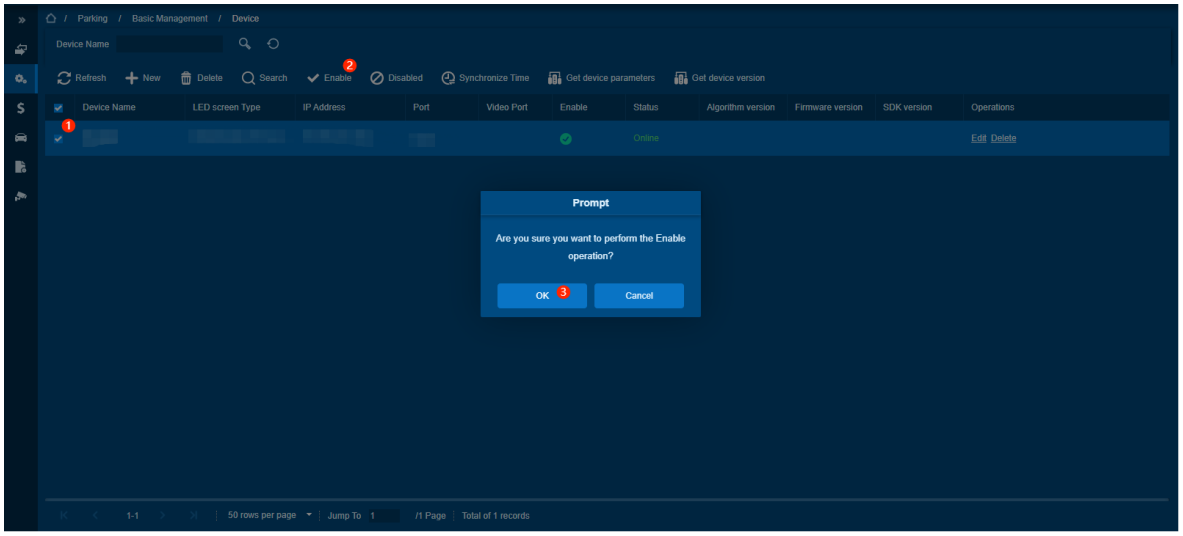
It is used when the disabled device needs to be reused.

Feature Trigger Result

Enable checked devices.

Steps:-

- Check the devices that need to be enabled.
- Click [**Enable**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the activation operation.



Disable

Preconditions for Normal Use of Functions

The administrator has the authority to disable functions, there are data that can be operated in the list, and the devices that need to be operated are online.

Function Usage Scenarios

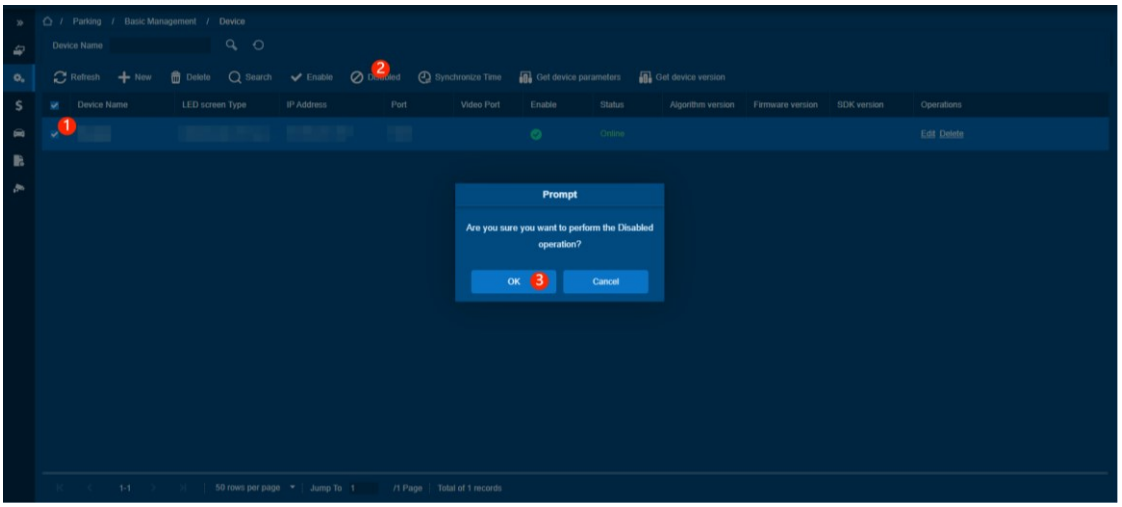
Used when the administrator needs to disable a certain device.

Feature Trigger Result

Disable checked devices.

Steps:-

- Check the devices that need to be disabled.
- Click [**Disabled**] button, a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the disabling operation.



Synchronize Device Time

Preconditions for Normal Use of Functions

The administrator has the permission to synchronize the time of the device, the list contains operable data, and the operated device is online.

Function Usage Scenarios

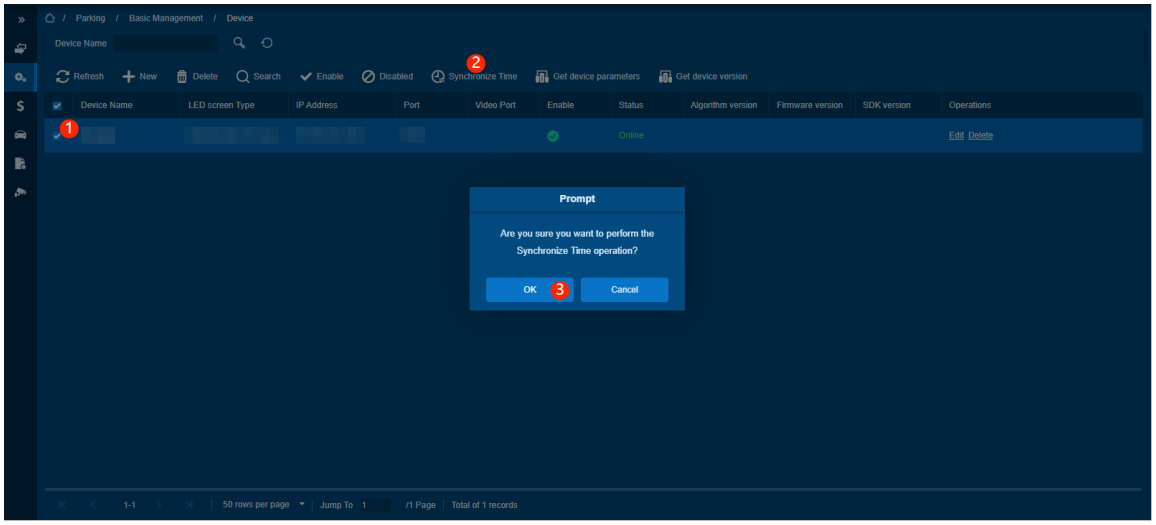
When the device time does not match the current system time, you can use this function to **synchronize the time.**

Feature Trigger Result

Synchronize device and current system time.

Steps:-

- Check the devices that need to synchronize time.
- Click [**Synchronize Time**] button, a prompt box will pop up.
- Click [**OK**] to complete the synchronization time operation.



Get Function Parameters

Preconditions for Normal Use of Functions

The administrator has the authority to obtain functional parameters, the list contains operable data, and the device that needs to obtain function parameters is online.

Function Usage Scenarios

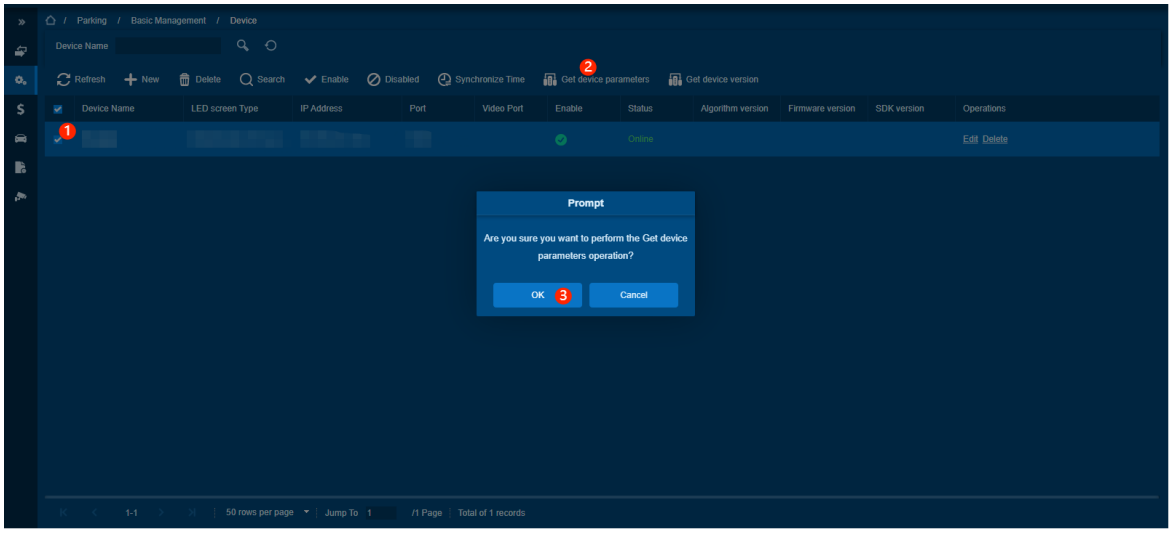
Use when the administrator wants to get the parameters on the device.

Feature Trigger Result

Get the parameters on the device.

Steps:-

- Check the devices that need to obtain parameters.
- Click [**Get device parameters**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the operation of obtaining device parameters.



Get Device Version

Preconditions for Normal Use of Functions

The administrator has the authority to obtain the device version, and the list contains operable data, and the device version is online.

Function Usage Scenarios

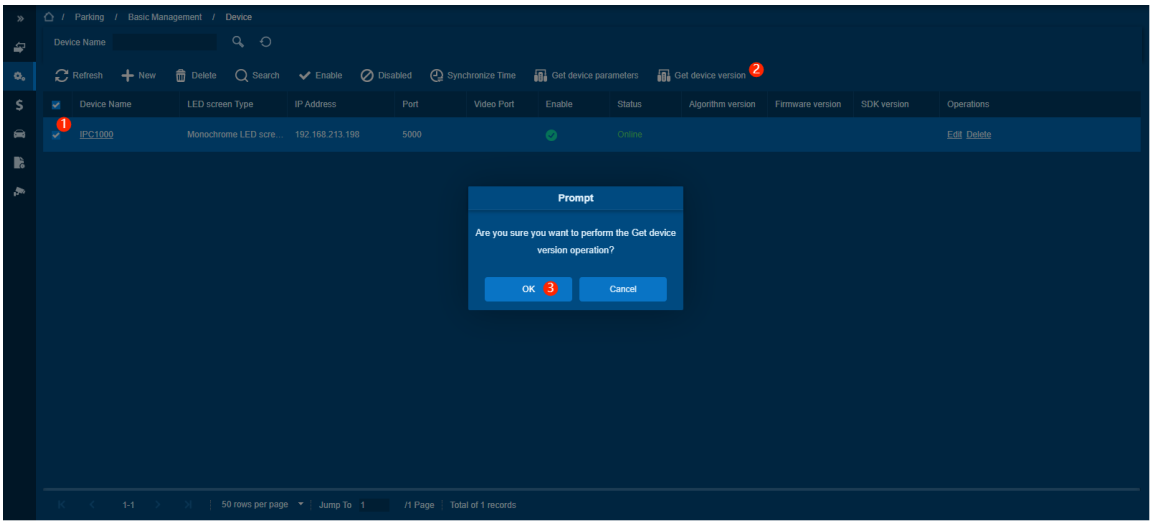
Used when the administrator needs to obtain the version of the device.

Feature Trigger Result

Get the version of the device.

Steps:-

- Check the device that needs to get the version.
- Click [**Get device version**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the operation of obtaining the device version.



10.2.3. Parking Area

Function Introduction

This module function is used to set areas for different vehicle definitions.

Add

Preconditions for Normal Use of Functions

The administrator has the add parking area permission.

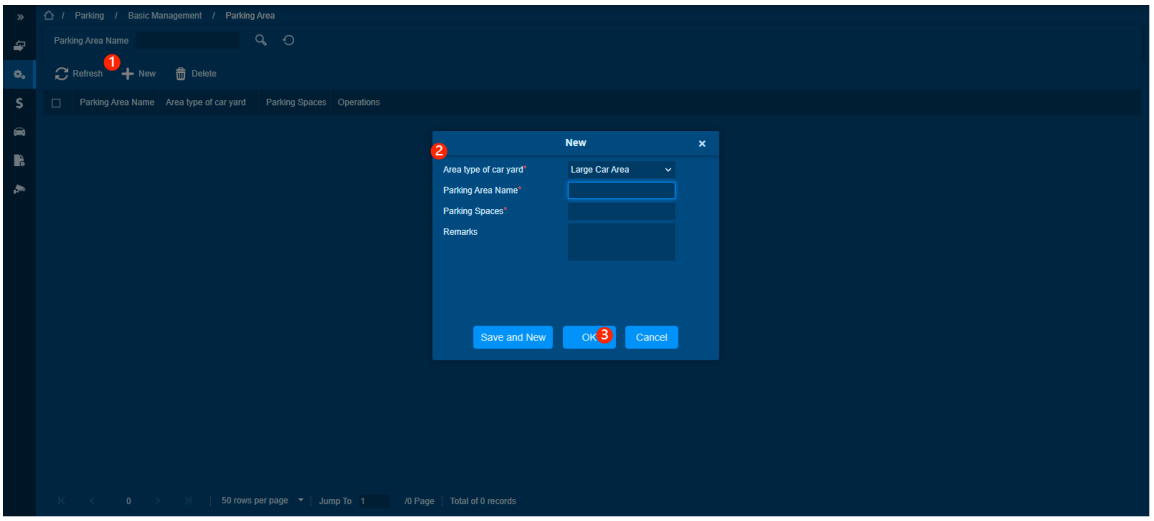
Function Usage Scenarios

It is used when it is necessary to give luxury parking areas for different vehicles.

Feature Trigger Result

Add a new vehicle area.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Area type of car yard: Set the parking area type.

Parking Area Name: Set the parking area name.

Parking Spaces: Set the parking spaces.

Remarks: Set the remarks.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function authority, the list contains data that can be removed, and the parking area that needs to be deleted is not used in the entrance and exit area.

Function Usage Scenarios

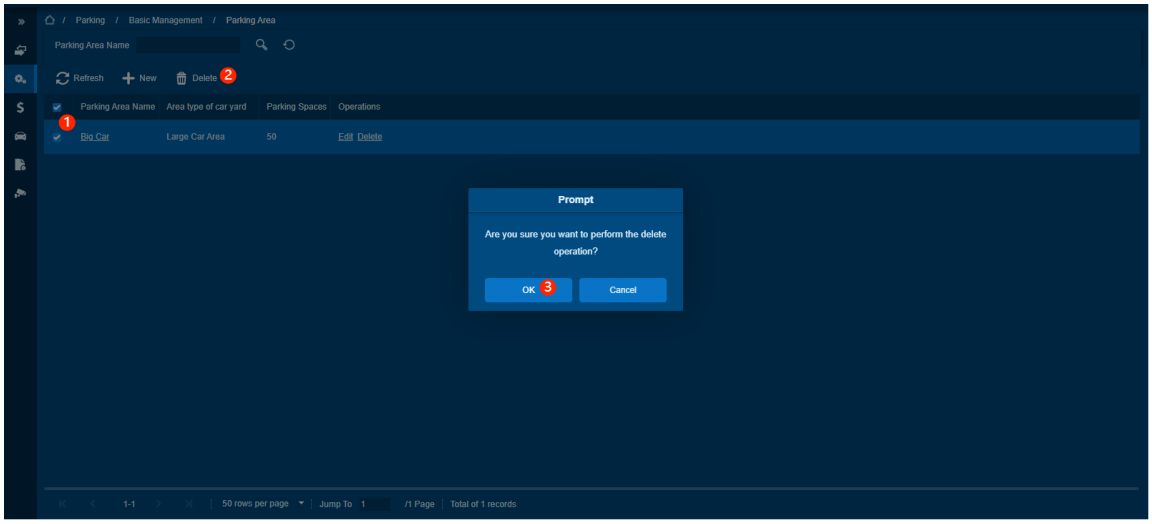
When a parking area is not needed, you can delete it to change the area.

Feature Trigger Result

Delete checked parking area.

Steps:

- Check the parking area that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete parking area operation.



10.2.4. Entrance and Exit Area

Function Introduction

Perform add and delete operations on the entrance and exit area of each parking lot.

Add

Preconditions for Normal Use of Functions

The administrator has the permissions to add entrance area, exit area, parking area.

Function Usage Scenarios

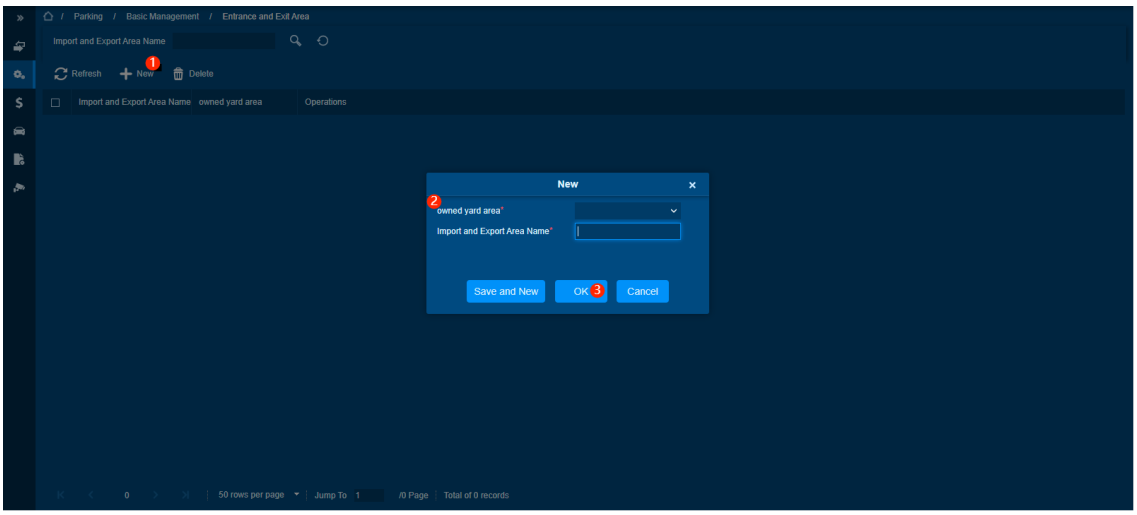
Used when setting up the parking area for import and export.

Feature Trigger Result

Set up the entrance and exit of a parking area.

Steps:-

- Click [**New**] button, and the add window will pop up.
- Select the parking area that needs entrance and exit area and set the name of the entrance and exit.
- Click [**OK**] to complete the add entrance and exit area operation.



Delete

Preconditions for Normal Use of Functions

The administrator has the permission to delete entrance and exit area. In the list, there are areas for entrance and exit that can be removed. And the guard booth does not use the entrance and exit areas that need to be deleted.

Function Usage Scenarios

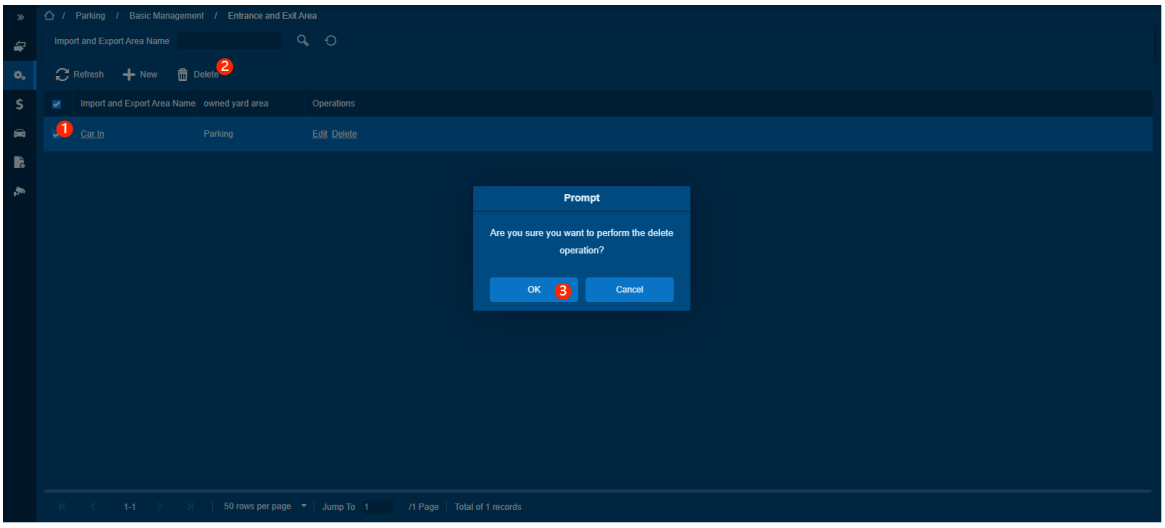
Delete redundant or unnecessary entrance and exit area.

Feature Trigger Result

Delete checked entrance and exit area.

Steps:-

- Check the entrance and exit area that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the operation of delete entrance and exit area.



10.2.5. Guard Booth

Function Introduction

Set the guard booth and guard booth parameter settings of entrance and exit area.

Add

Preconditions for Normal Use of Functions

The administrator has the add guard booth permission and can set the entrance and exit area of the guard booth.

Function Usage Scenarios

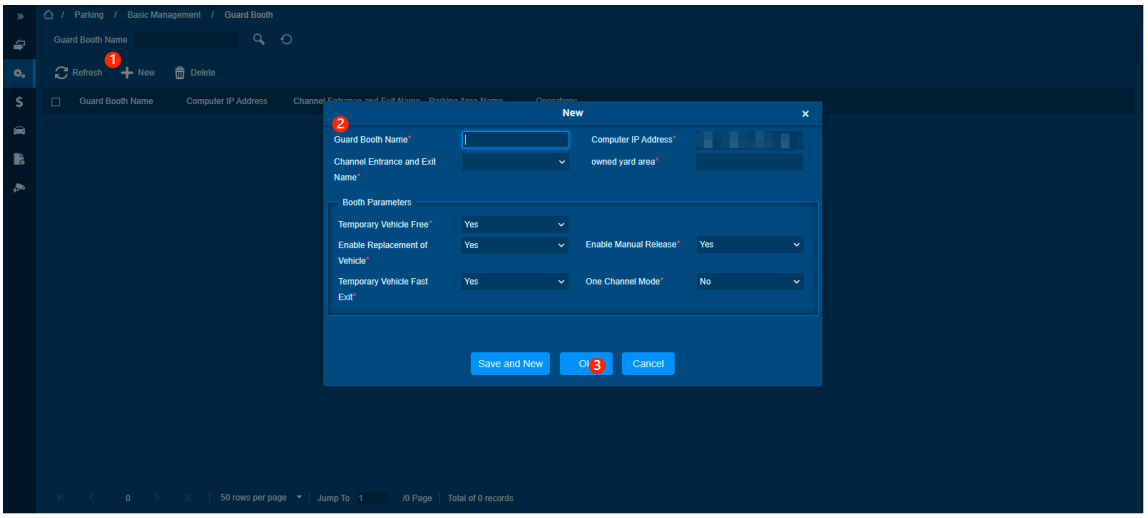
After adding entrance and exit area, you need to set guard booth to manage entrance and exit area.

Feature Trigger Result

Add a guard booth.

Steps:-

- Click [**New**] button, and the add window will pop up.



- Fill in the relevant information, all fields are required; field description are as follows:

Guard Booth Name: Set the name of Guard Booth.

Computer IP Address: Set the IP address of the Guard Booth computer.

Channel Entrance and Exit Name: Set the Entrance and Exit Area of Guard Booth.

Owned yard area: Parking Area to which Entrance and Exit Area belongs.

Temporary Vehicle Free: Whether to allow free parking.

Enable Replacement of Vehicle: Whether to enable replacement models.

Enable Manual Release: Whether to enable manual release.

Temporary Vehicle Fast Exit: Whether to support the quick exit of temporary vehicles.

One Channel Mode: Set whether the channel mode is single channel.

- Click [**OK**] to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete guard booth permission. The list contains data that can be removed. And the guard booth that needs to be deleted is not used in the channel.

Function Usage Scenarios

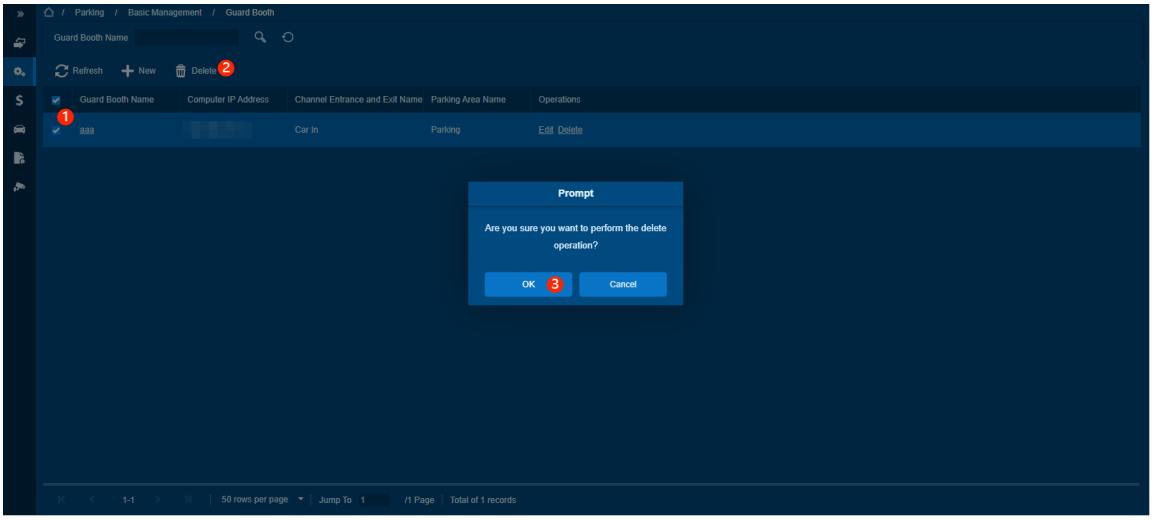
Use when you need to delete the extra guard booth.

Feature Trigger Result

Delete checked guard booth.

Steps:-

- Check the Guard Booth that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete guard booth operation.



10.2.6. Channel

Function Introduction

Set up the channel, guard booth and corresponding device for the entrance and exit of the parking lot.

Add

Preconditions for Normal Use of Functions

The administrator has the add function authority. When adding, there is guard booth and device support.

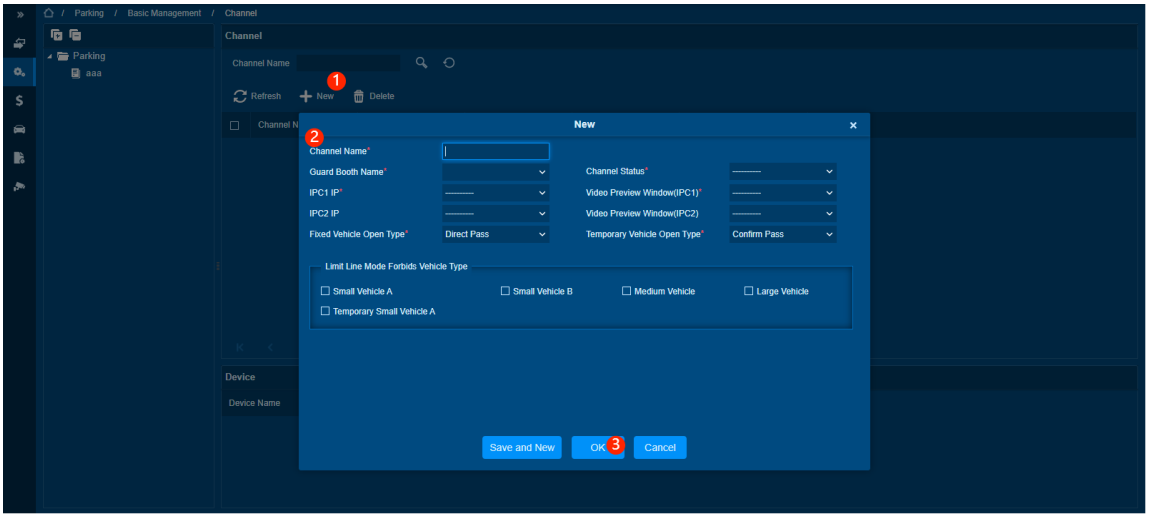
Function Usage Scenarios

It is used when the entrance and exit channel of the parking lot needs to be added.

Feature Trigger Result

Add a channel.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Channel Name: Set the channel name.

Guard Booth Name: Select the Guard Booth.

Channel Status: Select the entrance and exit status.

IPC IP: Select the camera device. If there is already one type of device in the sentry box, such as LPR series device, then only the same type of device can be selected here, and only the same type of device can be used in the same sentry box.

Video Preview Window: Set the camera in which window.

Fixed Vehicle Open Type: Set the opening method of the fixed car.

Temporary Vehicle Open Type: Set the opening method of temporary vehicles.

Limit Line Mode Forbids Vehicle Type: Check the vehicle definition that prohibits traffic in the restricted mode.

- Click [**OK**] button to complete the add channel operation.

Delete

Preconditions for Normal Use of Functions

The administrator uses the delete channel permission, and there are data that can be deleted in the list.

Function Usage Scenarios

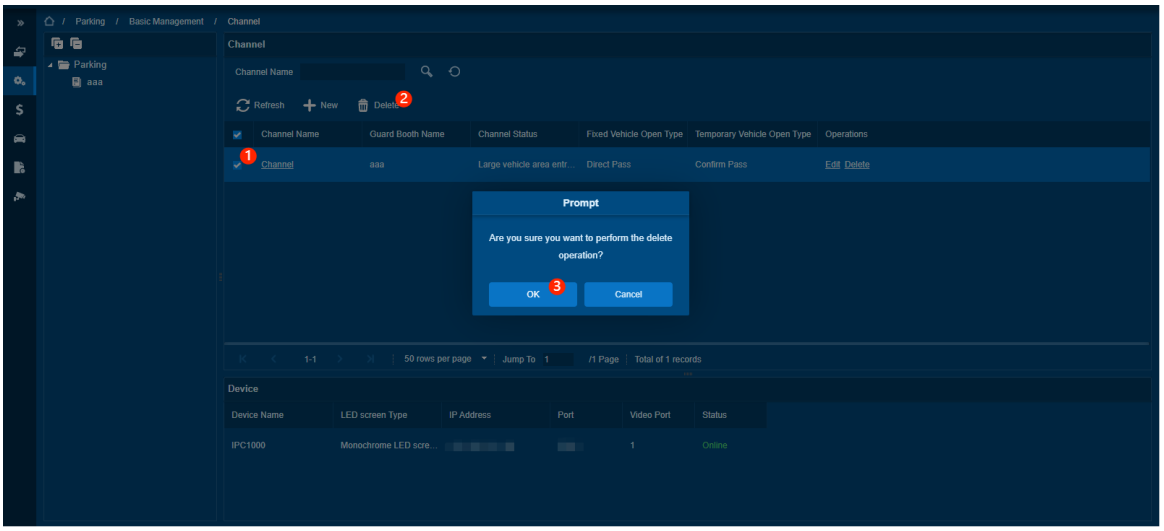
Delete unnecessary channels.

Feature Trigger Result

Delete checked channel.

Steps:-

- Check the channel that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete operation.



10.2.7. Vehicle Definition

Function Introduction

Manage the vehicle definition that can or cannot be entered in the channel.

Add

Preconditions for Normal Use of Functions

The administrator has the add vehicle definition permission.

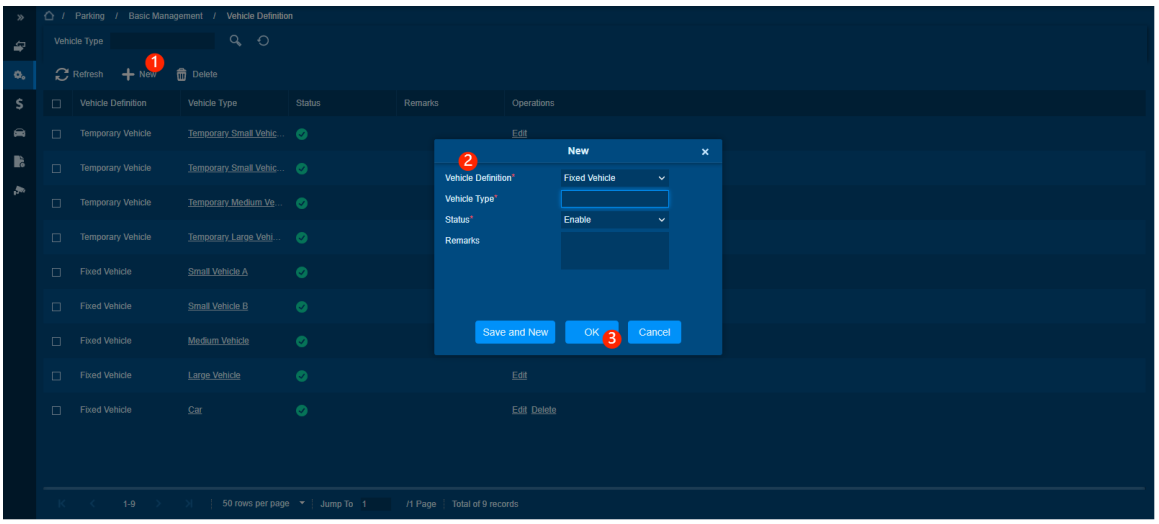
Function Usage Scenarios

Use when you need to manage certain types of vehicles.

Feature Trigger Result

Add a vehicle definition.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Vehicle Definition: Set Vehicle Definition as a fixed car or a temporary car.

Vehicle Type: Set the car type.

Status: Set the status.

Remarks: Set the remarks.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete vehicle definition permission, and the data in the list except the initialization data can be deleted.

Function Usage Scenarios

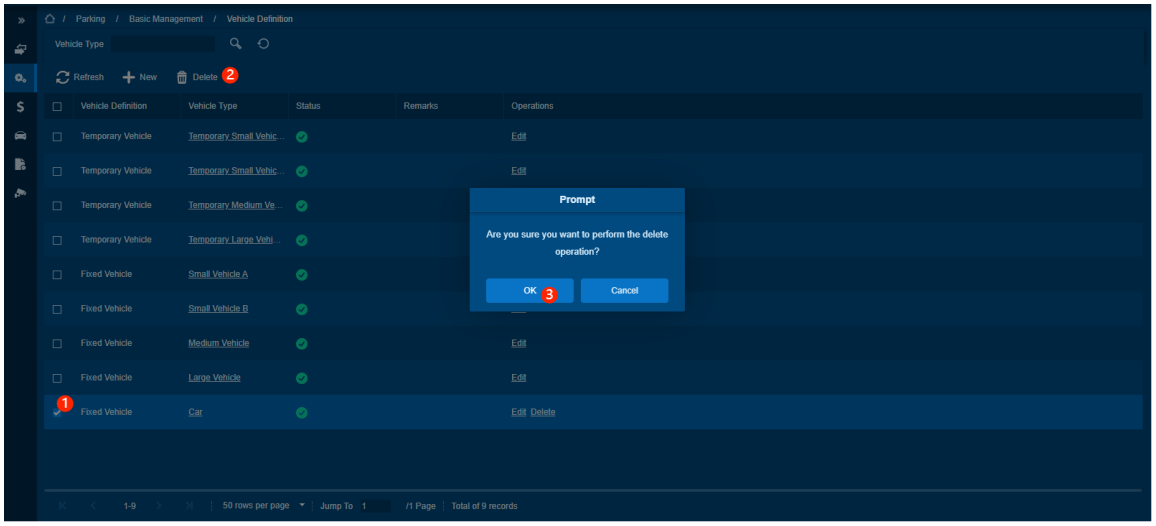
Delete redundant, useless vehicle definition.

Feature Trigger Result

Delete checked vehicle definition.

Steps:-

- Check the vehicle definition that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button to complete the delete vehicle definition operation.



10.2.8. Shift Settings

Function Introduction

Manage guard booth's shift settings.

Add

Preconditions for Normal Use of Functions

The administrator has the permission to add shifts and has guard booth to set shifts.

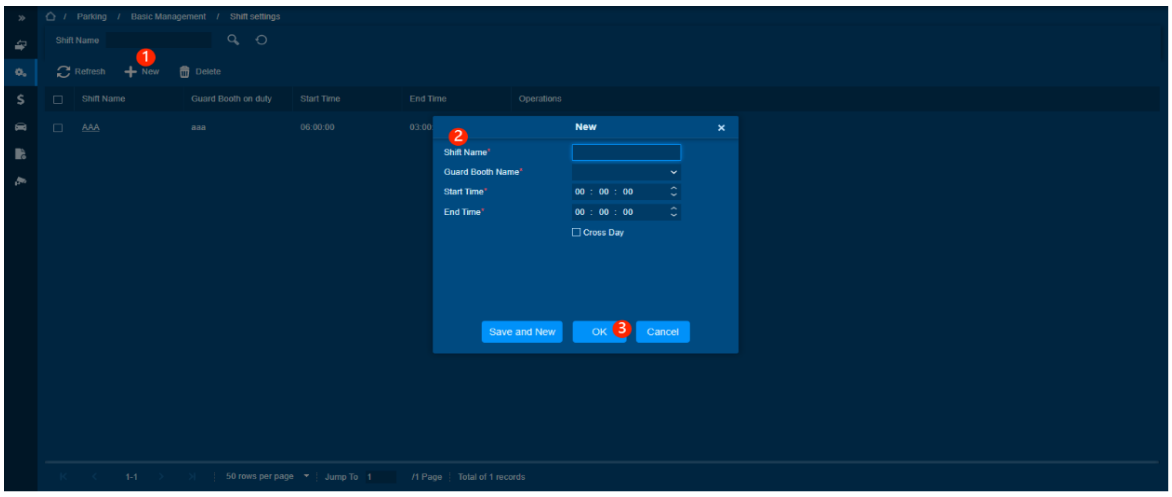
Function Usage Scenarios

Used when the administrator sets the shift of a guard booth.

Feature Trigger Result

Add a shift setting.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in relevant information, the items marked with * are required, field description a as follows:

Shift Name: Set the shift name.

Guard Booth Name: Select the guard booth name.

Start Time: Shift the start time.

End Time: Shift the end time (if [**Cross Day**] is not checked, the start time cannot be less than the end time)

- Click [**OK**] button to complete the add shift operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the permission to delete shifts, and the list contains data that can be deleted.

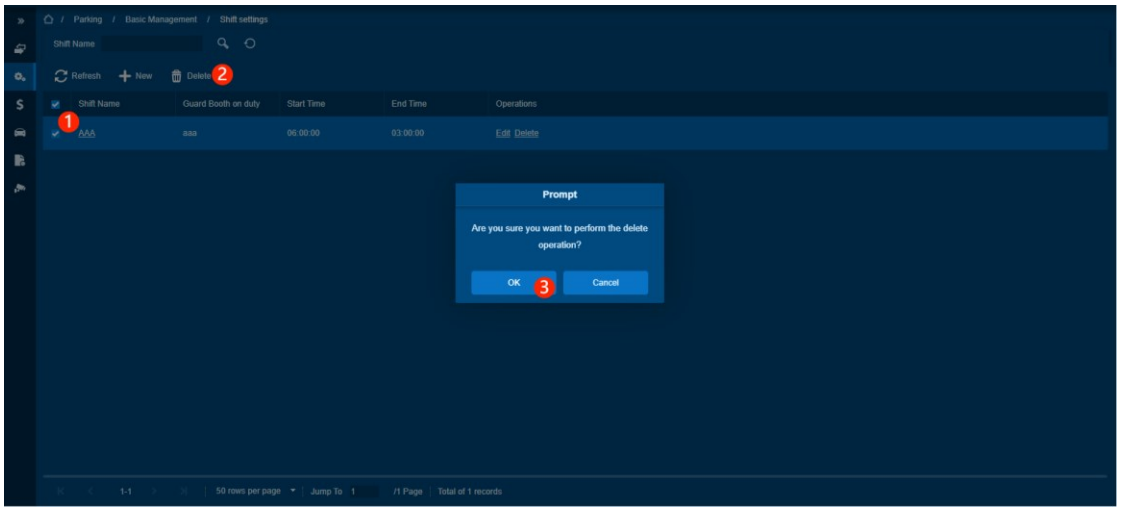
Function Usage Scenarios

Delete redundant, useless shifts.

Feature Trigger Result

Delete checked shift.

Steps:-



- Check the shifts that need to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the delete shift operation.

10.2.9. Manual Release Reason

Function Introduction

Manage manual release reason.

Add

Preconditions for Normal Use of Functions

The administrator has the add manual release reason permission.

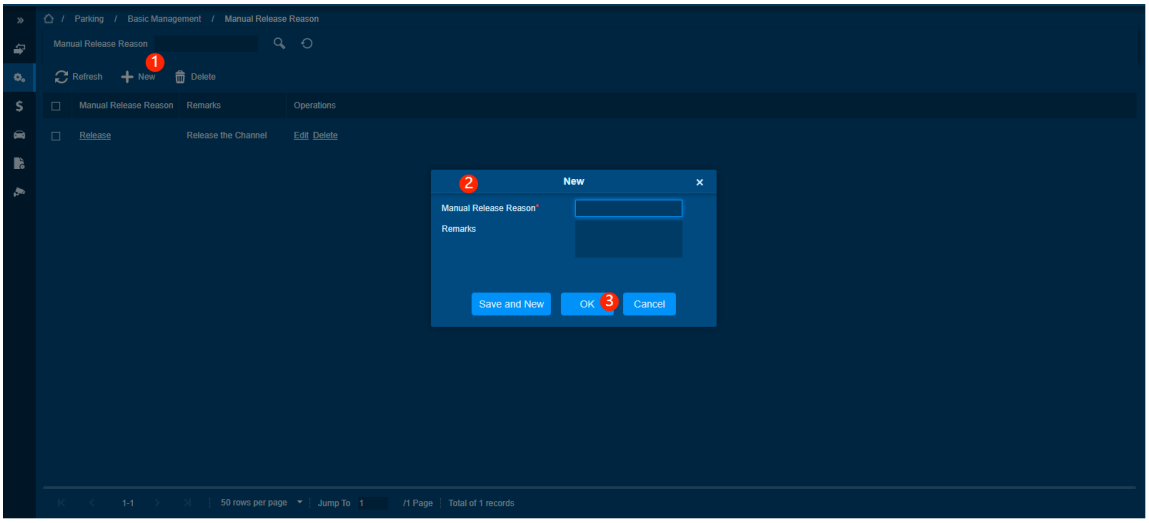
Function Usage Scenarios

When manual release is required, it is used when the reason for release needs to be explained.

Feature Trigger Result

Add a manual release reason.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Manual Release Reason: Set the Manual Release Reason.

Remarks: Set the remarks

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and there are data that can be deleted in the list.

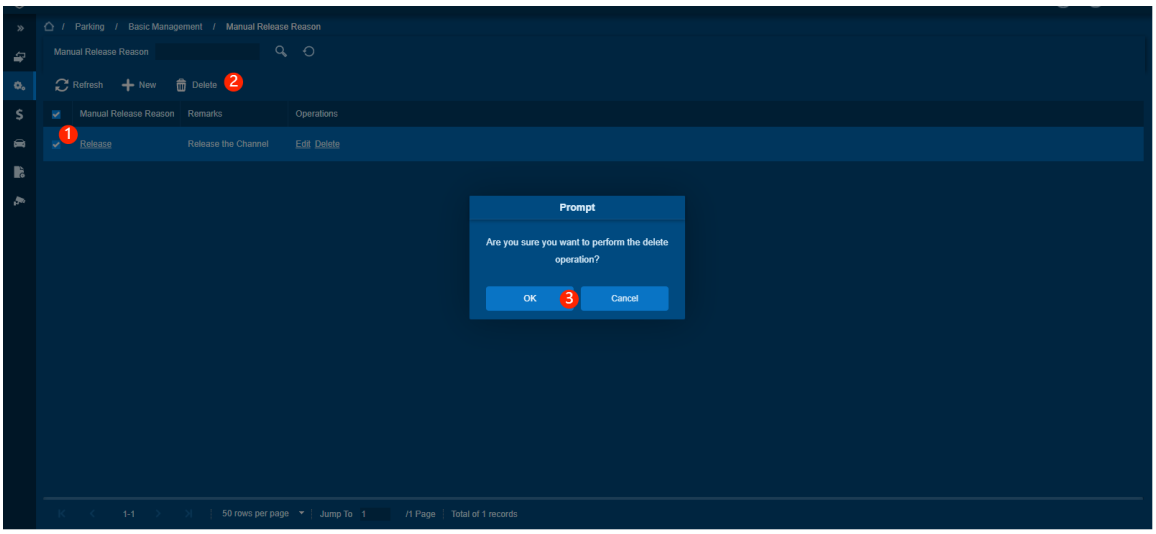
Function Usage Scenarios

Delete redundant and useless manual release reason.

Feature Trigger Result

Delete checked data.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button to complete the delete operation.

10.2.10. Two-Step Verification Device

Function Introduction

Manage Two-step verification device, set Access control device and Parking vehicle verification device bind relationship.

Add

Preconditions for Normal Use of Functions

The operator has the menu permission on this page.

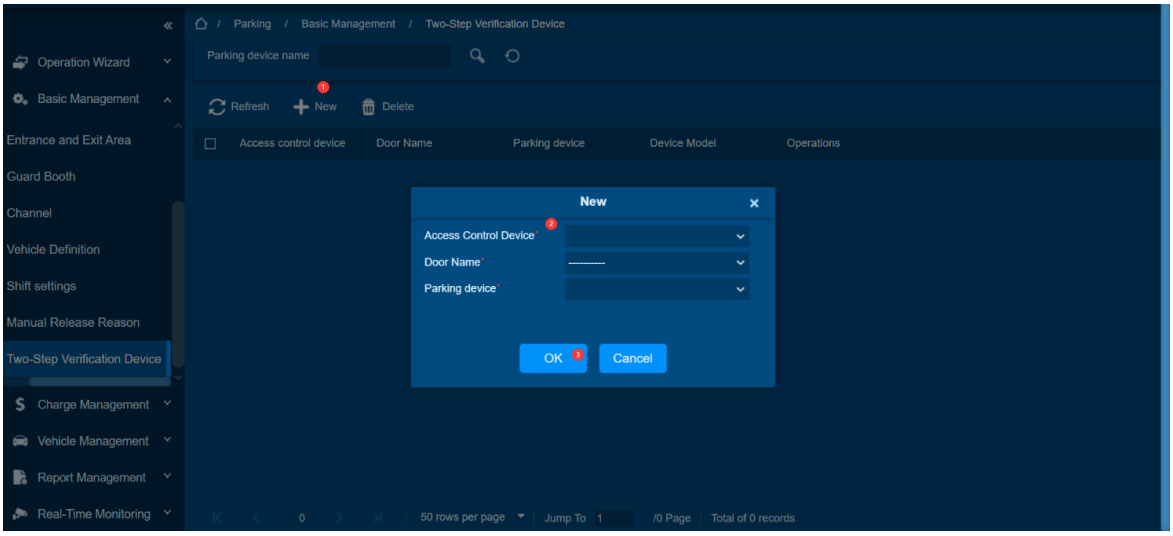
Function Usage Scenarios

For security-critical environments, scenarios that require verification of the driver's identity before entering or leaving.

Feature Trigger Result

Add a bind relationship between Access control device and Parking vehicle verification device .

Steps:-



1. Click [**New**] to create new bind relationship between Access control device and Parking device.

2. Select Access control device and its doors, each door and parking device could be bind only once.

3. Select Parking device which been added, and after all set the Channel that used this parking device should have two-step verification while entering or leaving the parking area.

10.3. Charge Management

Change Management is used to configure the charging rules of your parking lot, set the permanent vehicles in your parking lot, and set detailed parking charging systems such as temporary vehicles, overtime vehicles, discounts, etc.

Function List

Operations	Description
Fixed Vehicle Rules	View, add, delete fixed vehicle rules
Temporary Vehicle Charging Rules	View, add, delete temporary vehicle charging rules
Over Time Charge Rules	View, add, delete over time charge rules
Discount Strategy	View, add, delete discount strategy
Business Management	View, add, delete business management
Financial Reconciliation	View, add, delete financial reconciliation

10.3.1. Fixed Vehicle Rules

Function Introduction

Set up charging rules for fixed vehicles.

Add

Preconditions for Normal Use of Functions

The administrator has the add permission.

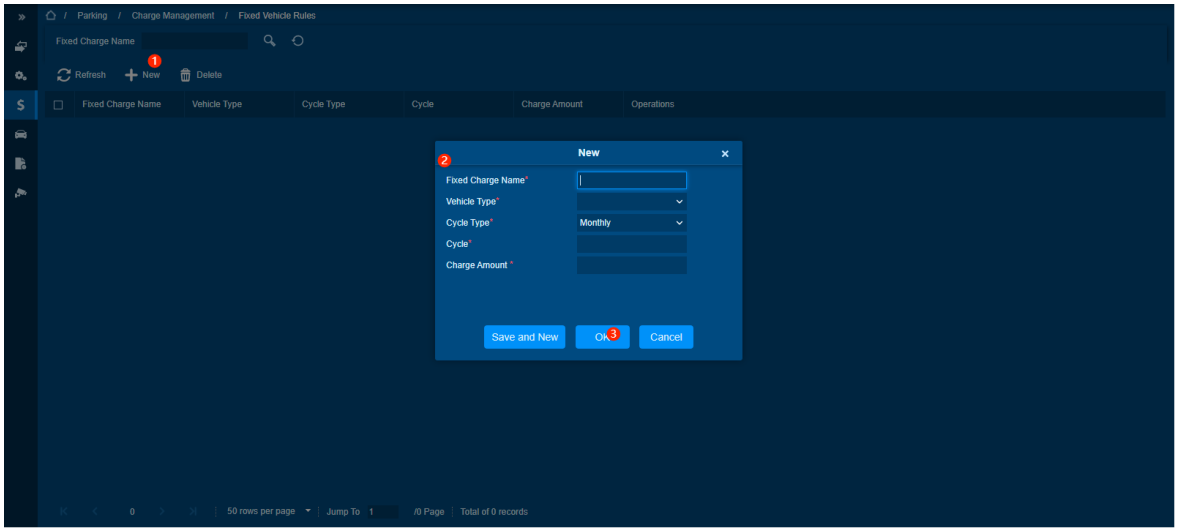
Function Usage Scenarios

Add to the charging rules for fixed cars.

Feature Trigger Result

Add fixed car charging rules.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in relevant information, all fields are required, field description is as follows:

Fixed Charge Name: Set the fixed car toll name.

Vehicle Type: Choose the car type.

Cycle Type: Select the period type.

Cycle: Set the cycle.

Charge Amount: Set the amount.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and the list contains data that can be deleted.

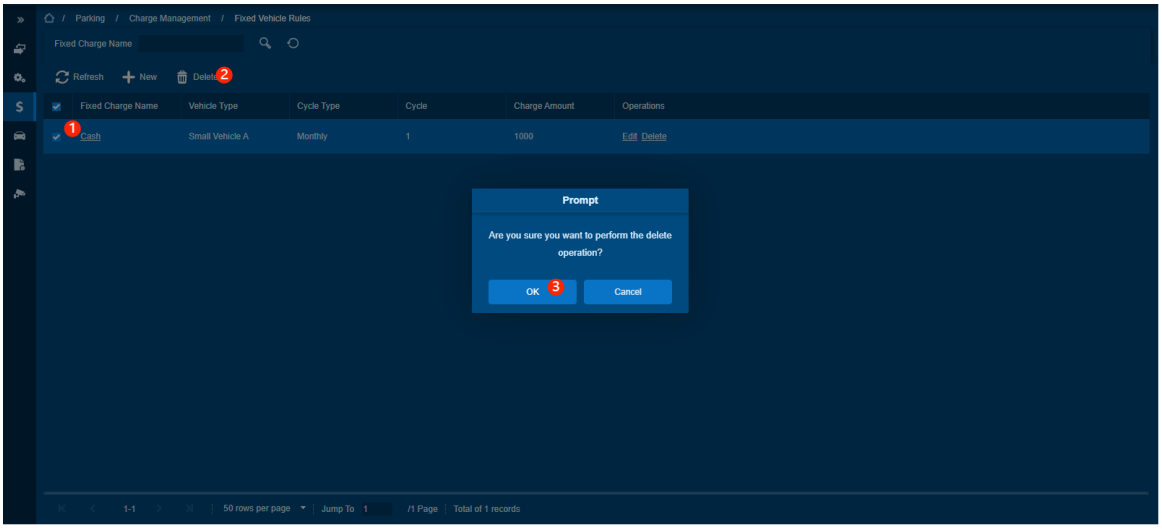
Function Usage Scenarios

The administrator deletes redundant charging rules.

Feature Trigger Result

Delete checked data.

Steps:-



- Check the data that needs to be deleted.
- Click [Delete] button, and a prompt window will pop up.
- Click [OK] button in the prompt box to complete the delete operation.

10.3.2. Temporary Vehicle Charging Rules

Function Introduction

Set up charging rules for temporary vehicles.

Add

Preconditions for Normal Use of Functions

The administrator has the permission of add temporary vehicle charging rules.

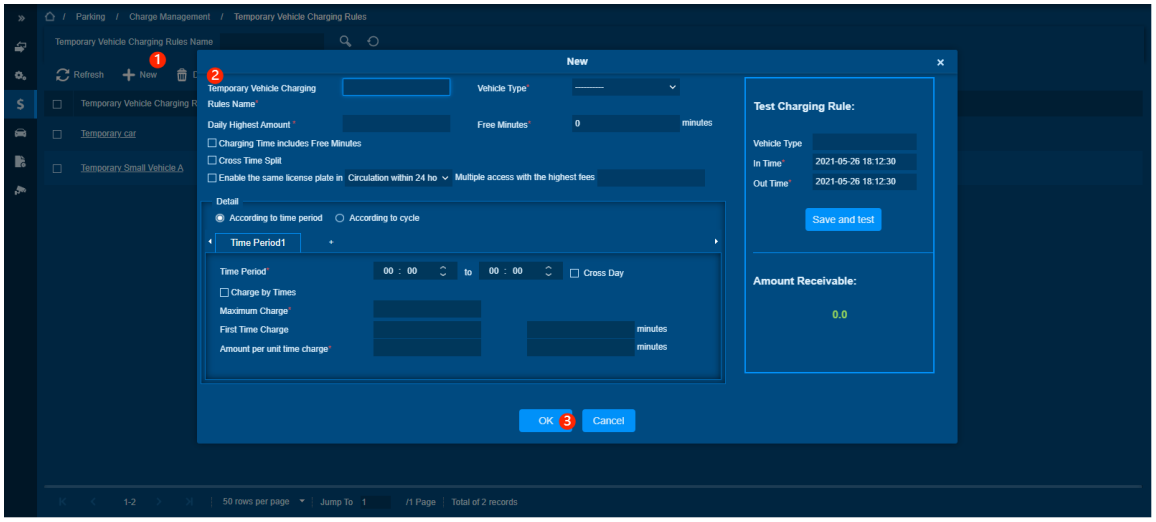
Function Usage Scenarios

Administrators can add charging rules when they need to charge for temporary vehicles.

Feature Trigger Result

Add temporary vehicle charging rules.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Temporary Vehicle Charging Rules Name: Set the Temporary Vehicle Charging Rules Name.

Vehicle Type: Select the vehicle type.

Daily Highest Amount: Set the maximum amount charged throughout the day.

Free Minutes: Set the free parking time for each vehicle.

Charging Time includes Free Minutes: After checking, the timing time includes free parking time.

Cross Time Split: After checking, split across Timetables.

Enable the same license plate in: After checking, when is the same license plate.

Multiple access with the highest fees: Set the maximum charge for multiple entry and exit of the same license plate.

Detail: Detailed settings, set according to time or cycle.

Timetable: Set the Timetable.

Cross Day: After ticking, the time of the time is cross-day.

Charge by Times: Checked and charged by the number of times.

Maximum Charge: Set the maximum charge.

First Time Charge: Set the first-time charge.

Amount per unit time charge: Set the amount per unit time charge.

In Time: Set the vehicle in time.

Out Time: Set the vehicle out time.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and there are data that can be deleted in the list.

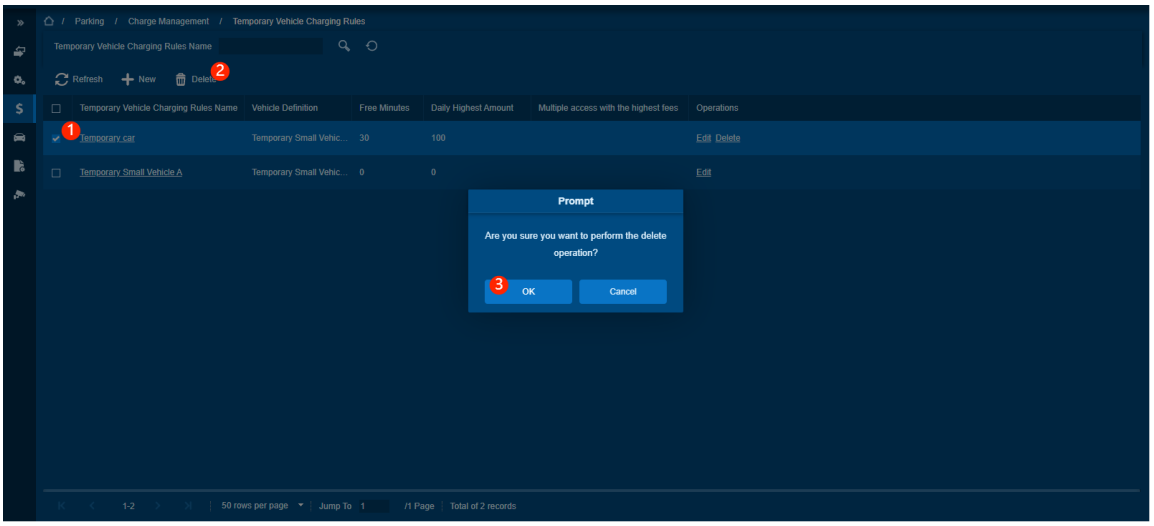
Function Usage Scenarios

The administrator deletes redundant and invalid temporary vehicle charging rules.

Feature Trigger Result

Delete checked temporary vehicle charging rules.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the delete operation.

10.3.3. Over Time Charge Rules

Function Introduction

Existing vehicles in the parking lot overtime will be charged for overtime.

Add

Preconditions for Normal Use of Functions

The administrator has the add over time charge rules permission.

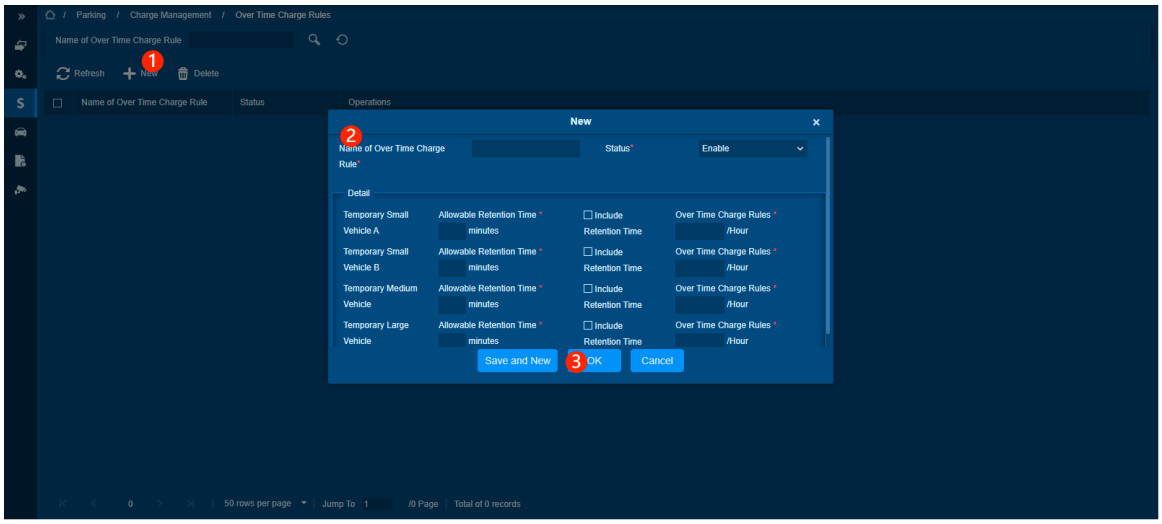
Function Usage Scenarios

Set respective over time charge rules for different vehicle definitions in the parking lot.

Feature Trigger Result

Add over time charge rules.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in relevant information, all fields with *are required, field description is as follows:

Name of Over Time Charge Rule: Set the name of Over Time Charge Rules

Status: Set the status of the rule

Allowable Retention Time: Set the allowable retention time.

Include Retention Time: After checked, the residence time is included.

Over Time Charge Rules: Set the rules for overtime charging, the unit is hour.

- Click [**OK**] button to complete the add over time charge rules operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete over time charge rules permission.

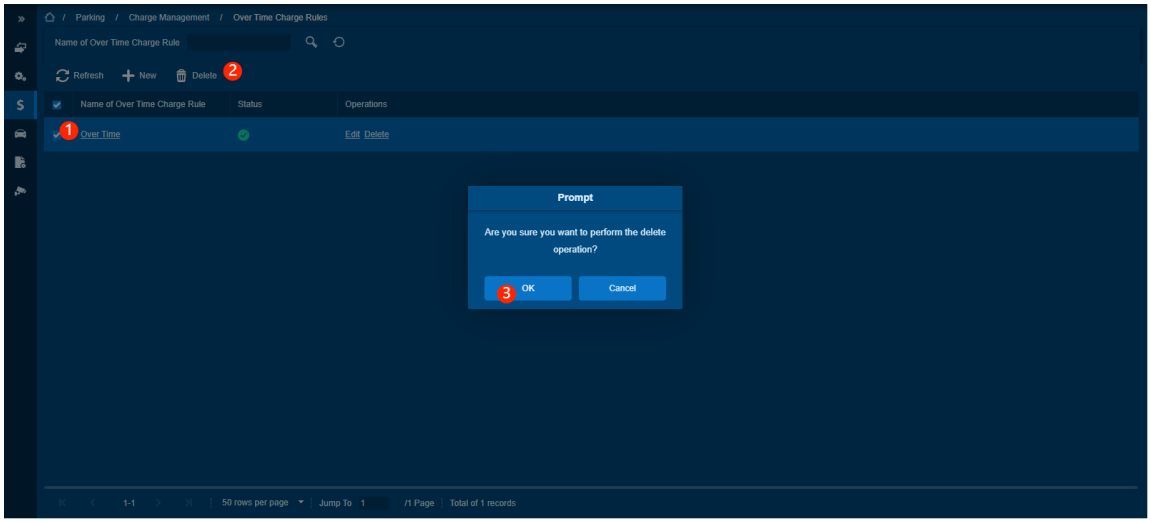
Function Usage Scenarios

The administrator deletes redundant and useless over time charge rules.

Feature Trigger Result

Delete checked over time charge rules.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button to complete the delete operation.

10.3.4. Discount Strategy

Function Introduction

Set discounts for different promotions.

Add

Preconditions for Normal Use of Functions

The administrator has the add discount strategy permission.

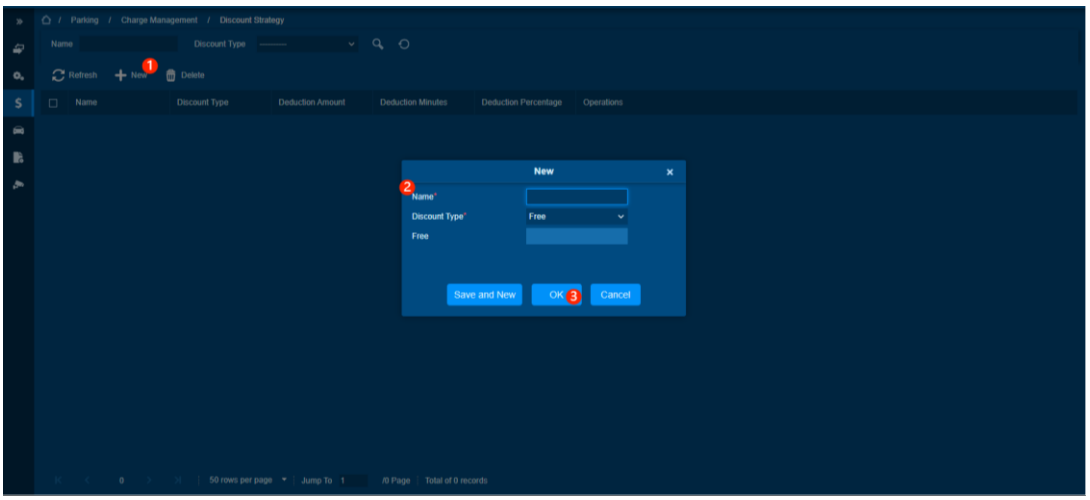
Function Usage Scenarios

Administrators need to set different discount strategies for different discounts.

Feature Trigger Result

Add a discount strategy.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Name: Set the name of Discount Strategy

Discount Type: Choose the Discount Type

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and there are data that can be deleted in the list.

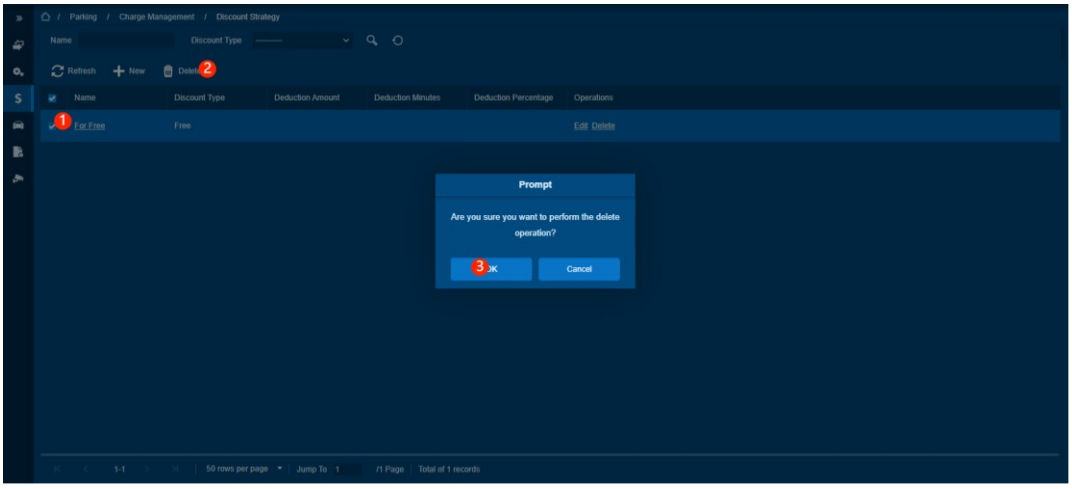
Function Usage Scenarios

The administrator deletes redundant and unnecessary discount strategy.

Feature Trigger Result

Delete checked discount strategy.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the delete operation.

10.3.5. Business Management

Function Introduction

Manage merchants and merchant's discount strategy.

Add

Preconditions for Normal Use of Functions

The administrator has the add merchant permission.

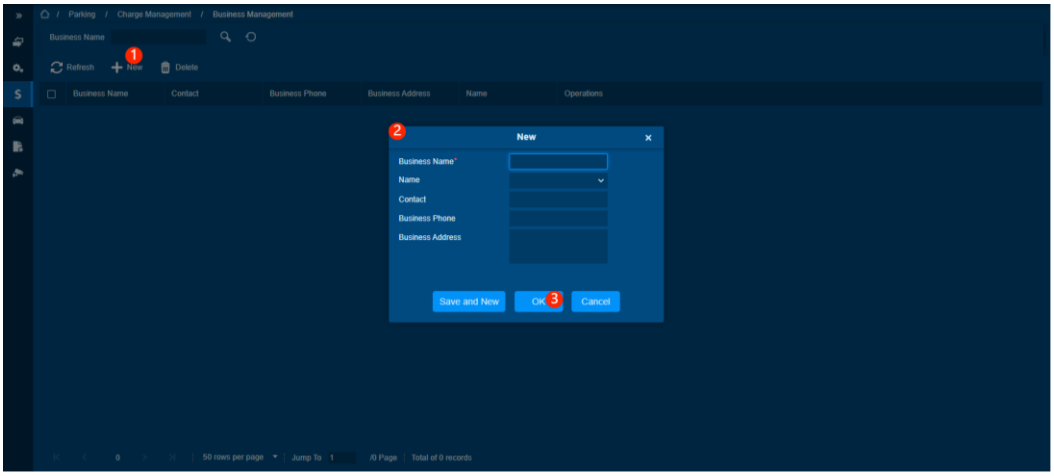
Function Usage Scenarios

Used when the administrator wants to add a merchant or the discount strategy corresponding to the merchant.

Feature Trigger Result

Add business management.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the items marked with * are required, and the field description is as follows:

Business Name: Set the business name.

Discount Way: Select the discount strategy.

Contact: Set up the business contacts.

Business Phone: Set the business's contact number.

Business Address: Set the address of the business.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete permission, and there are data that can be deleted in the list.

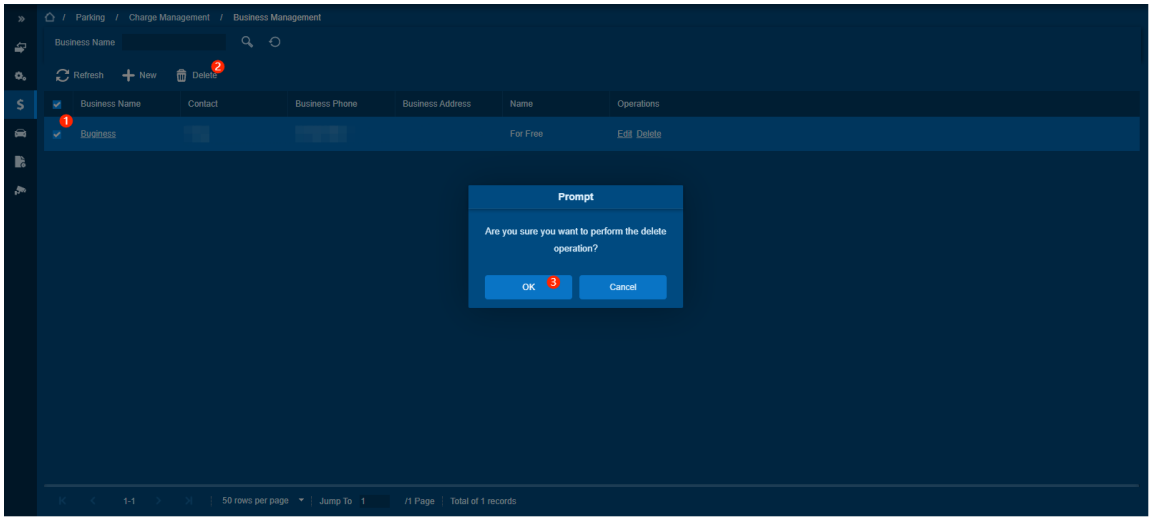
Function Usage Scenarios

The administrator deletes redundant and useless data.

Feature Trigger Result

Delete the checked data.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button in the prompt box to complete the delete operation.

10.3.6. Financial Reconciliation

Function Introduction

Save the financial data obtained from each shift.

Reconciliation

Preconditions for Normal Use of Functions

The administrator has reconciliation authority, and there are financial records generated by shift changes in the list.

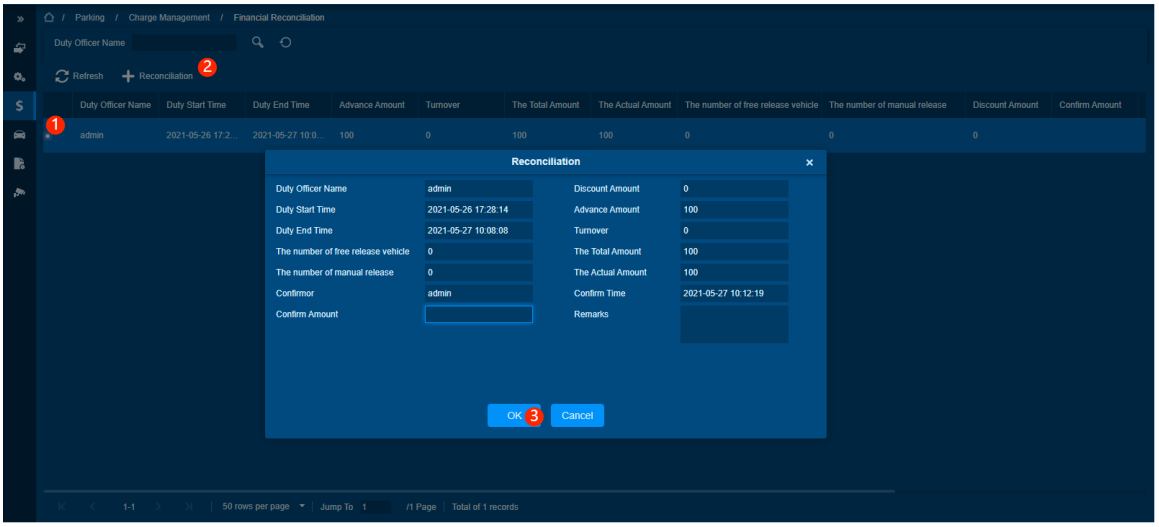
Function Usage Scenarios

It is used by the administrator to reconcile the finances generated by each shift.

Feature Trigger Result

View the details of each bill.

Steps:-



- Check the data that needs to be reconciled.
- Click [**Reconciliation**] button to pop up the detailed information of the account.

Click [**OK**] button to complete the reconciliation operation.

10.4. Vehicle Management

Vehicle management used to manage your vehicles system , such as query fixed vehicles, and reauthorize fixed vehicles that are about to expire. Manage and add your parking lot's allowed list and blocklist to control which cars can and cannot freely enter and exit your parking lot or parts of it.

Function List

Operations	Description
License Plate Registration	View, add, delete, download, import license plate information
Vehicle Authorization	View, fixed vehicle batch authorization, temporary vehicle authorization, synchronized fixed vehicle, cancellation
Fixed Vehicle Extension	View and log off fixed vehicles
Block and Allow List Management	View, add, delete, synchronization prohibited list, synchronization allowed list

10.4.1. License Plate Registration

Function Introduction

Register and manage the license plates of personnel.

Add

Preconditions for Normal Use of Functions

The administrator has the add function permission, and the personnel data in the personnel list.

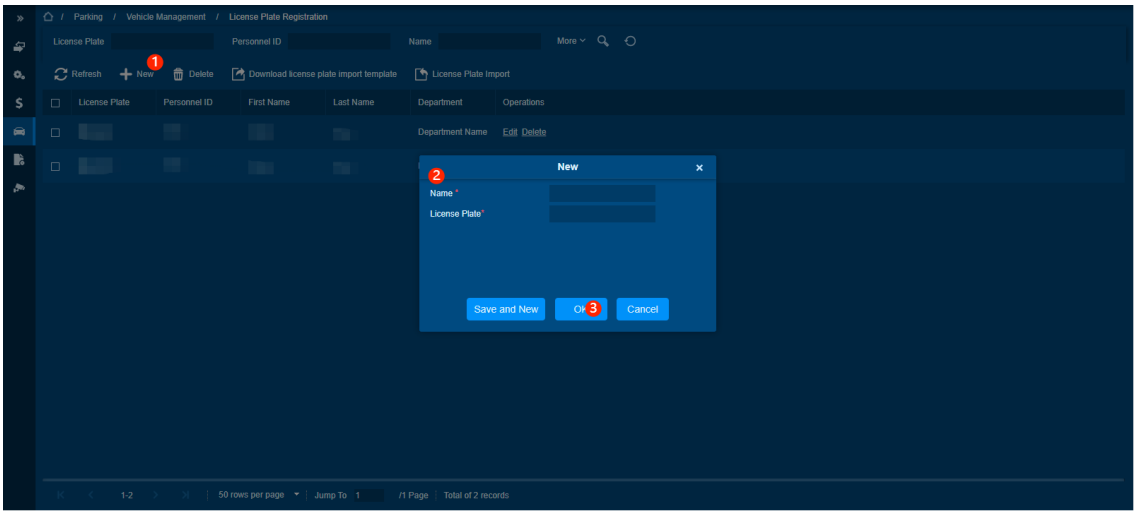
Function Usage Scenarios

It is used when the administrator adds the license plate of the personnel.

Feature Trigger Result

Add personnel license plate information.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information, the field description is as follows:

Name: Choose the name of the personnel.

License Plate: Fill in the person's license plate.

- Click [**OK**] button to complete the add license plate operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete permission, and there are data that can be deleted in the list.

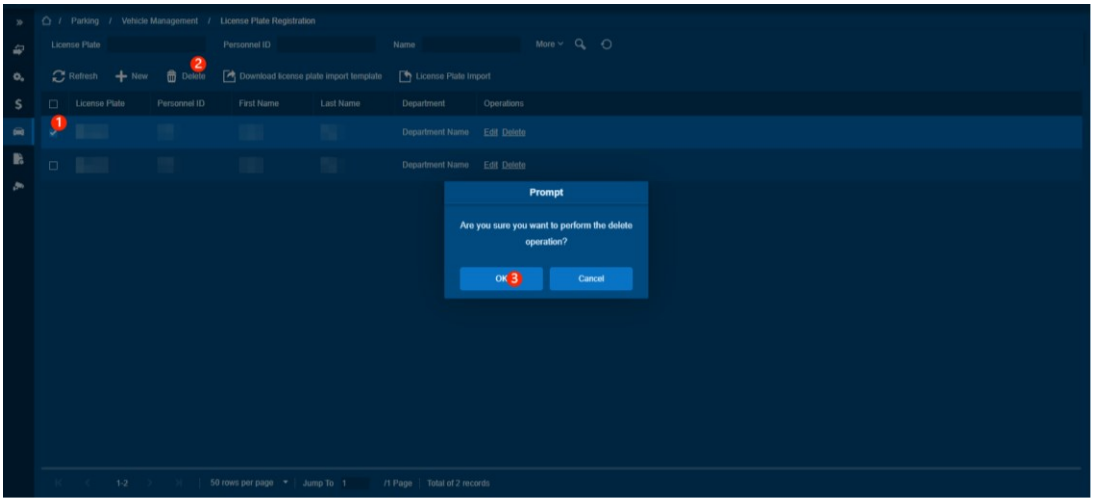
Function Usage Scenarios

It is used when the administrator deletes the license plate of personnel.

Feature Trigger Result

Delete checked license plate information.

Steps:-



- Check the license plate information that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete operation.

Download License Plate Import Template

Preconditions for Normal Use of Functions

The administrator has the permission to download the license plate import template.

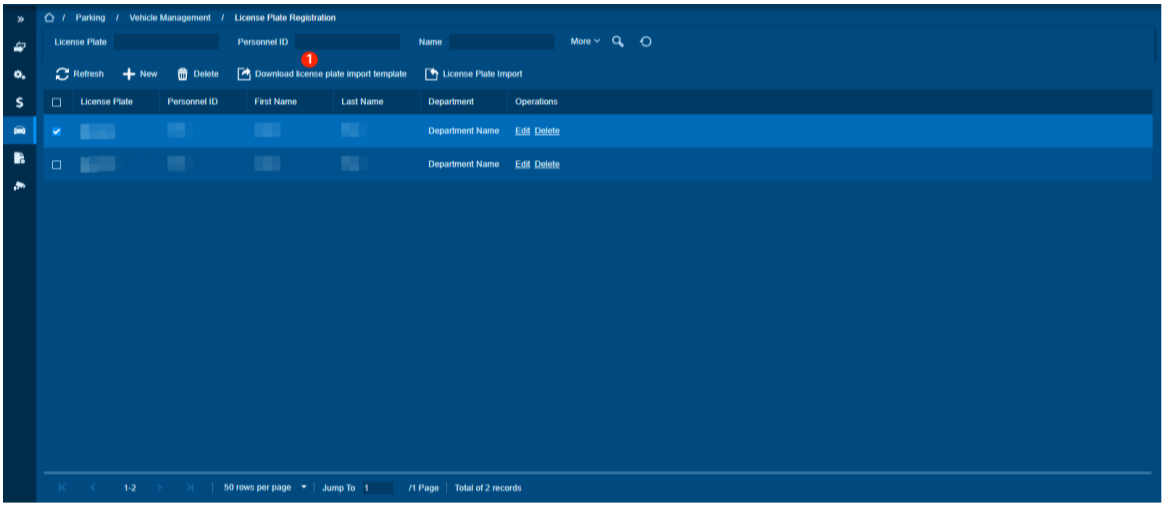
Function Usage Scenarios

When you need to import multiple pieces of information at once, you need to use the imported template.

Feature Trigger Result

Download import template.

Steps:-



Click [**Download license plate import template**] button, and the import template will be downloaded automatically.

License Plate Import

Preconditions for Normal Use of Functions

The administrator has the license to import license plates, and there are data in the imported form.

Function Usage Scenarios

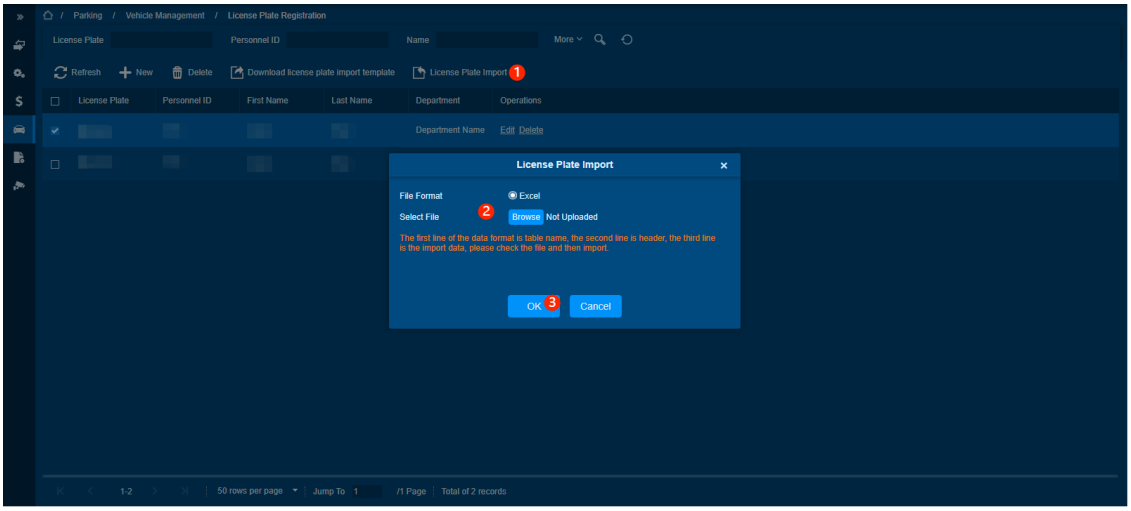
It is used when the administrator wants to import multiple pieces of license plate data at one time.

Feature Trigger Result

Import license plates in batches.

Steps:-

- Click [**License Plate Import**], the import window will pop up.
- Click [**Browse**] button and select the Excel form that needs to be imported.
- Click [**OK**] button to complete the import operation.



10.4.2. Vehicle Authorization

Function Introduction

Authorize and manage vehicles.

Add

Preconditions for Normal Use of Functions

The administrator has the add permission, and the personnel have license plate registration information.

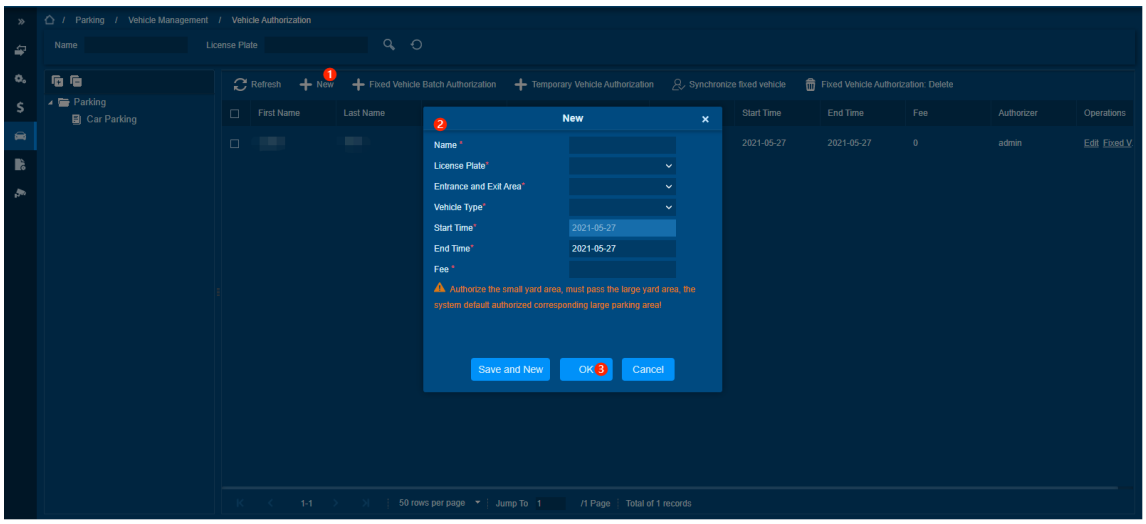
Function Usage Scenarios

Authorize personnel personnel's vehicles.

Feature Trigger Result

Add vehicle authorization information.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in relevant information, all fields are required, field description is as follows:

Name: Choose the name of the personnel.

License Plate: Automatically fills license plate information after selecting personnel.

Entrance and Exit Area: Set the Entrance and Exit Area.

Vehicle Type: Set the Vehicle Definition.

Start Time: Set the Start Time.

End Time: Set the End Time.

Fee: Set the charge amount.

- Click [**OK**] button to complete the add operation.

Fixed Vehicle Batch Authorization

Preconditions for Normal Use of Functions

The administrator has the authority of batch authorization for fixed vehicles.

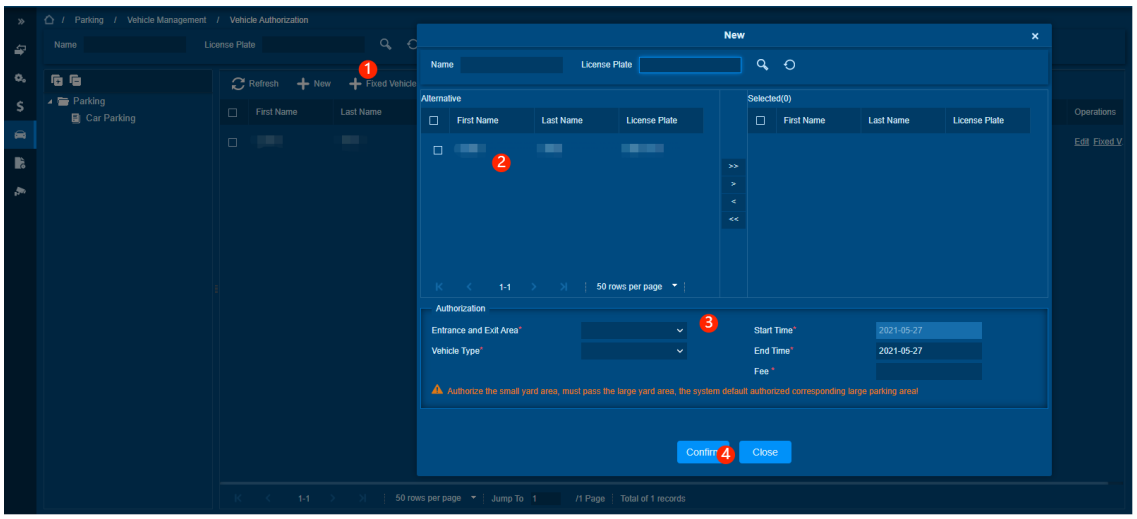
Function Usage Scenarios

It is used for batch authorization of personnel vehicles.

Feature Trigger Result

Batch add personnel license plate authorization.

Steps:-



- Click [**Fixed Vehicle Batch Authorization**] button to pop up the batch add window.
- From the list on the left, select the personnel who need authorization in batches and add them to the list on the right.
- Fill in the relevant information, the field description is as follows:

Entrance and Exit Area: Set Entrance and Exit Area.

Vehicle Type: Set Vehicle Definition.

Start Time: Set the Start time.

End Time: Set the End time.

Fee: Set the charge amount.

- Click [**Confirm**] button to complete the batch fixed car authorization operation.

Temporary Vehicle Authorization

Preconditions for Normal Use of Functions

The administrator has the authority to authorize temporary vehicles and has set entrance and exit area.

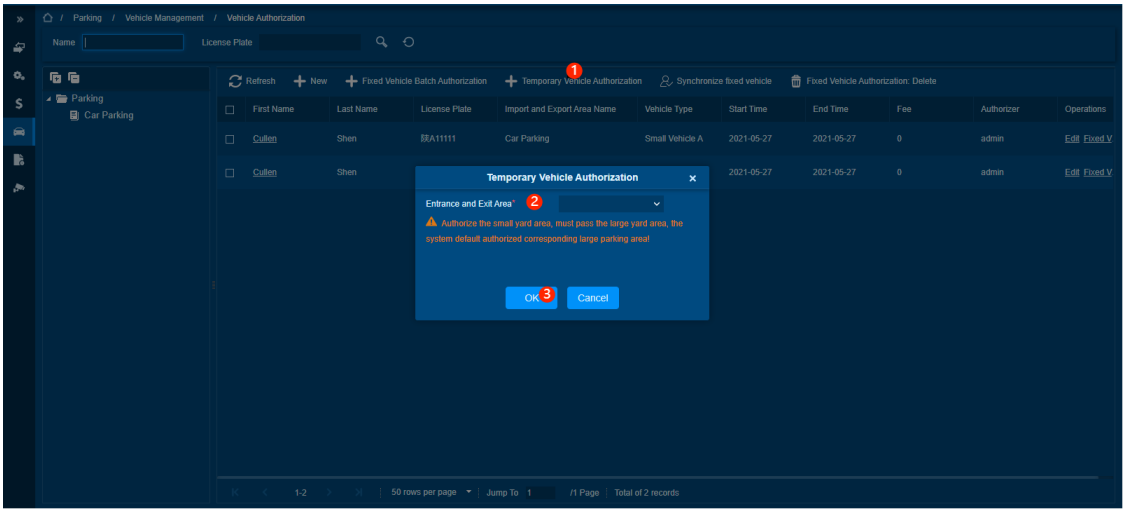
Function Usage Scenarios

Used when temporarily authorizing temporary vehicles.

Feature Trigger Result

Authorize temporary vehicles to enter a certain area.

Steps:-



- Click [**Temporary Vehicle Authorization**] button to pop up the temporary vehicle authorization window.
- Select the temporary vehicle authorization area.
- Click [**OK**] button to complete the temporary vehicle authorization operation.

Synchronize Fixed Vehicle

Preconditions for Normal Use of Functions

The administrator has the permission to synchronize fixed cars.

Function Usage Scenarios

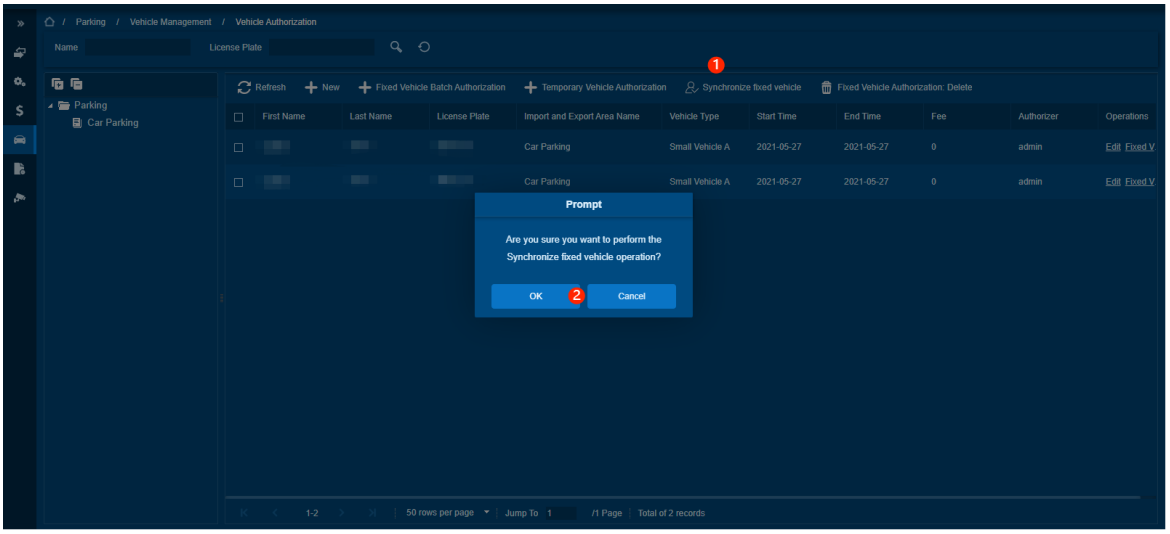
Sync license plate information to the device.

Feature Trigger Result

Synchronize license plate information.

Steps:-

- Click [**Synchronize fixed vehicle**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the synchronization operation.



Unsubscribe

Preconditions for Normal Use of Functions

The administrator has the permission to unsubscribe, and there are data that can be unsubscribed in the list.

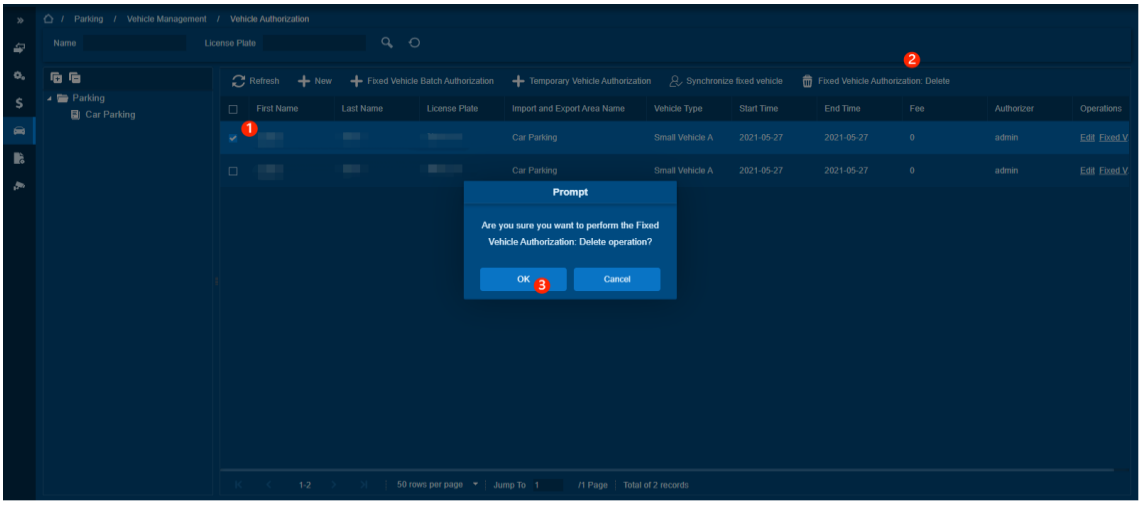
Function Usage Scenarios

Unsubscribe the authorization of the vehicle. After unsubscribed, the vehicle is no longer authorized.

Feature Trigger Result

Unsubscribe checked license plate information.

Steps:-



- Check the data that needs unsubscribed.
- Click [**Fixed Vehicle Authorization**: **Delete**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the unsubscribe operation.

10.4.3. Fixed Vehicle Extension

Function Introduction

For postponement management of fixed vehicles, you can view the start and end time and authorization status of the vehicle authorization period.

Unsubscribe

Preconditions for Normal Use of Functions

The administrator has Unsubscribe permission, and there is data that can be operated in the list.

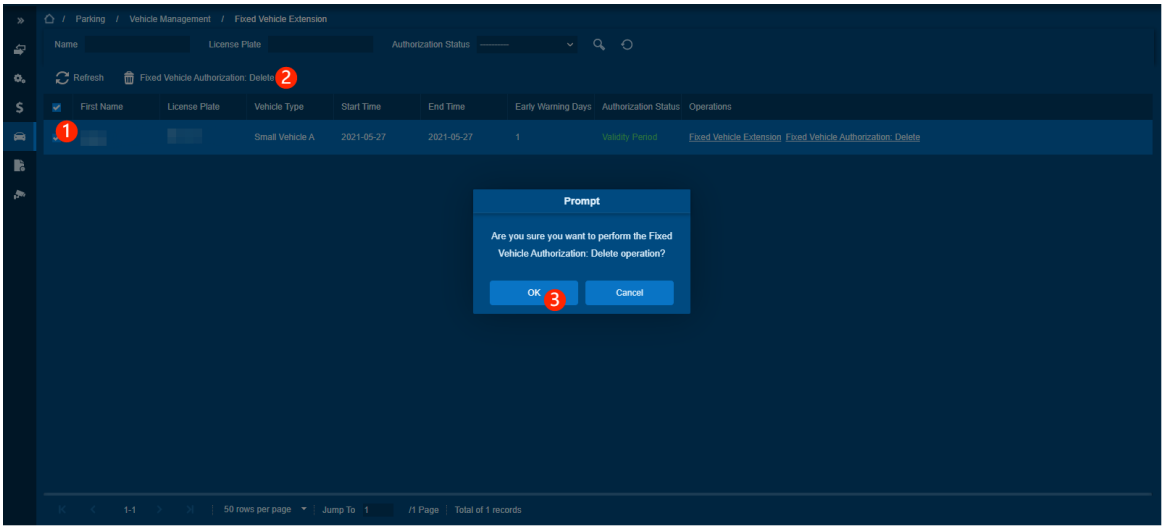
Function Usage Scenarios

The administrator unsubscribes the deferred fixed-vehicle license plate. After unsubscribed, the license plate no longer has the fixed vehicle permission.

Feature Trigger Result

Unsubscribe checked license plate information.

Steps:-



- Check the license plate data that needs to be unsubscribed.
- Click [**Fixed Vehicle Authorization**: **Delete**] button, and a prompt box will pop up.
- Click [**OK**] button to complete the unsubscribe operation.

10.4.4. Block and Allow List Management

Function Introduction

Vehicles on the special list include fire trucks, police cars, and some privileged vehicles that are free of charge. The vehicles on the blocked list refer to those vehicles that are not allowed to enter or leave the parking lot.

Add

Preconditions for Normal Use of Functions

The administrator has the add function permission.

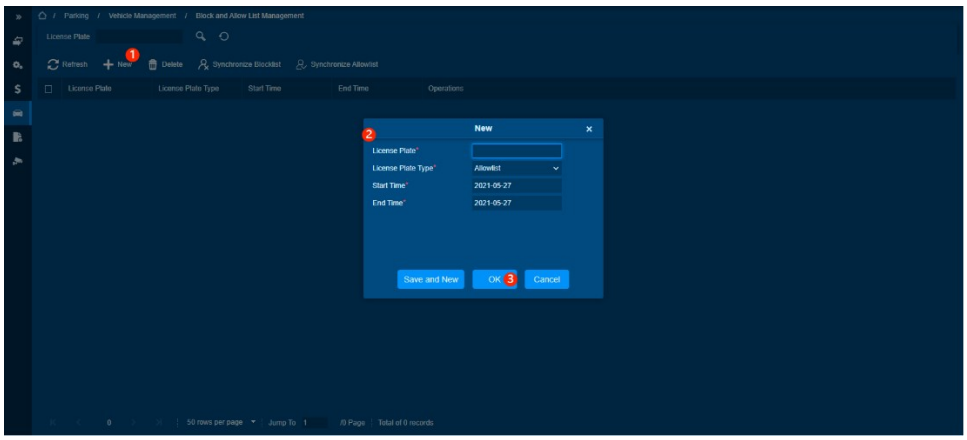
Function Usage Scenarios

The administrator adds to the special vehicle, and when adding, the vehicle can be allowed or prohibited to pass.

Feature Trigger Result

Add special vehicle information.

Steps:-



- Click [**New**] button, and the add window will pop up.
- Fill in relevant information, all fields are required, field description are as follows:

License Plate: Set the added license plate number.

License Plate Type: Select whether the license plate number is a banned list or an allowed list.

Start Time: Set the start time.

End Time: Set the end time.

- Click [**OK**] button to complete the add operation.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and there are data that can be deleted in the list.

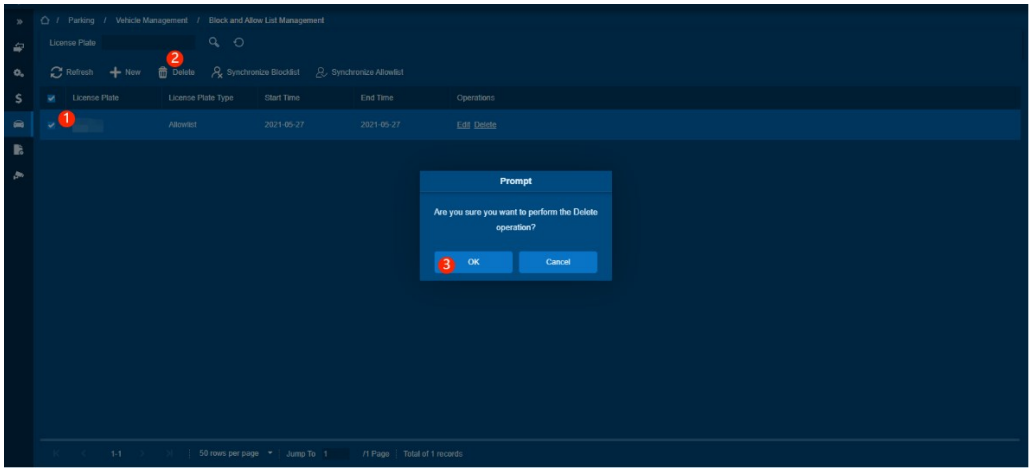
Function Usage Scenarios

The administrator deletes the special vehicle.

Feature Trigger Result

Delete checked special vehicles.

Steps:-



- Select the data that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button in the window and delete operation after finishing.

Synchronization Prohibited List

Preconditions for Normal Use of Functions

The administrator has the permission to synchronize the banned list.

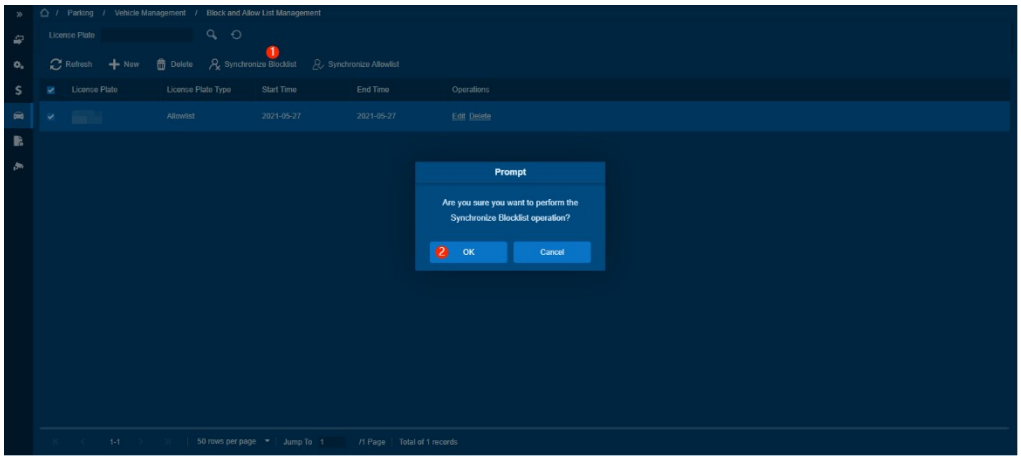
Function Usage Scenarios

The administrator synchronizes the special vehicles in the banned list to the device.

Feature Trigger Result

Synchronization prohibited list.

Steps:-



- Click [**Synchronize Blocklist**] button, and a prompt window will pop up.
- Click [**OK**] button in the prompt box to complete the synchronization prohibited list operation.

Synchronization Allowed List

Preconditions for Normal Use of Functions

The administrator has the permission to synchronize the permission list.

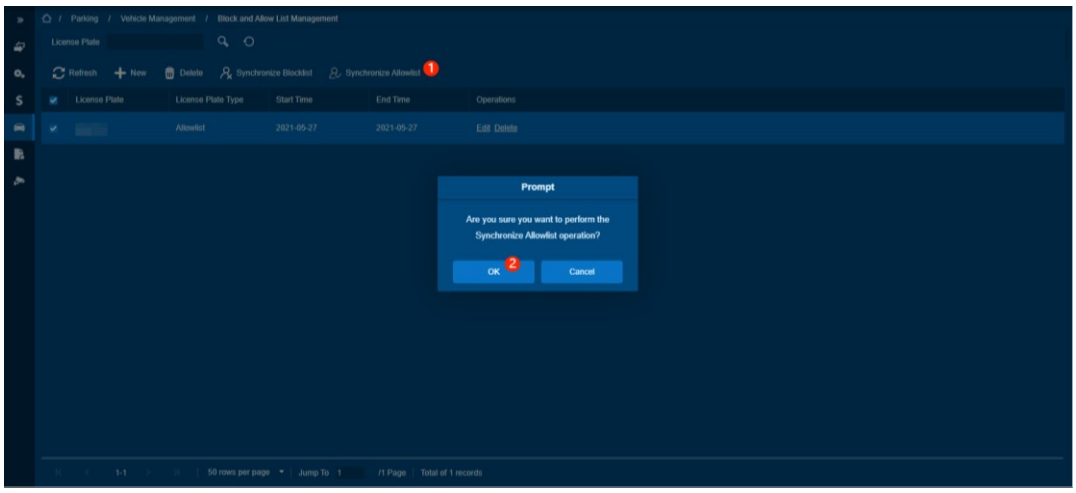
Function Usage Scenarios

The administrator synchronizes the special vehicles in the allowed list to the device.

Feature Trigger Result

Sync allowed list to device.

Steps:-



- Click [**Synchronize Allow list**] button, and a prompt window will pop up.
- Click [**OK**] button in the prompt box to complete the synchronization operation.

10.5. Report Management

Report Management allows you to query all the data of your parking lot, such as vehicle passing records, charging records, and daily and monthly charging details. It can help you to record your every system operation.

Function List

Operations	Description
Vehicle Inside	View, remove, export, and correct license plate information
Entry Record	View, export entry record
Exit Record	View, export exit record
Charge Record	View, export charge record
Expired Vehicle	View, export expired vehicle
Incoming Unusual Vehicles	View, export incoming unusual vehicles
Fixed Vehicle Authorization Record	View, export fixed vehicle authorization record
Device Operation Record	View, export device operation record
Handover Statistics	View, export handover statistics
Daily Income Statistics	View, export daily income statistics
Monthly Income Statistics	View, export monthly income statistics

10.5.1. Vehicle Inside

Function Introduction

This function module provides statistical information of all vehicles in the parking lot.

Remove

Preconditions for Normal Use of Functions

The administrator has the permission to remove the function, and there is vehicle inside data in the list.

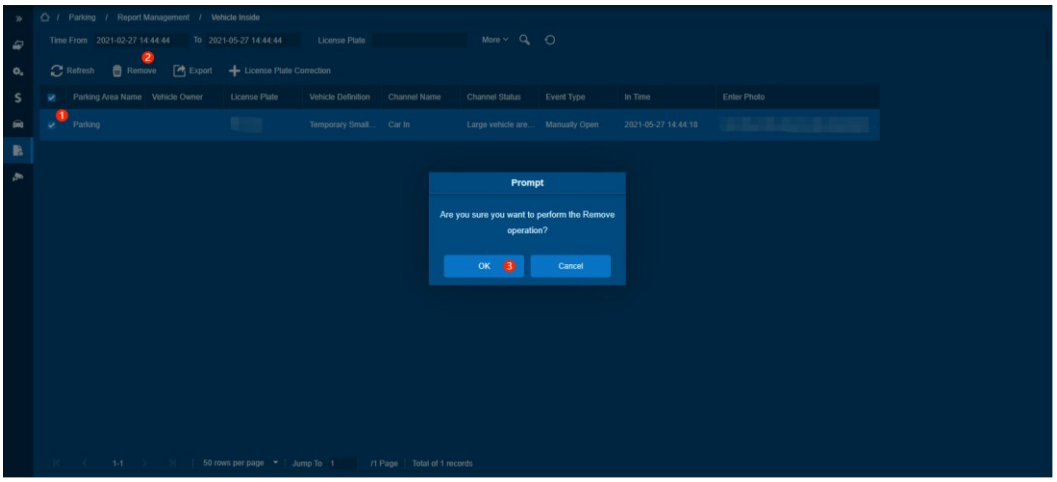
Function Usage Scenarios

The administrator removes the invalid license plate information in the parking lot.

Feature Trigger Result

Remove the checked vehicle.

Steps:-



- Check the vehicles that need to be removed.
- Click [**Remove**] button, and a prompt window will pop up.
- Click [**OK**] button to complete the removal operation.

Export

Preconditions for Normal Use of Functions

The administrator has the export function permission.

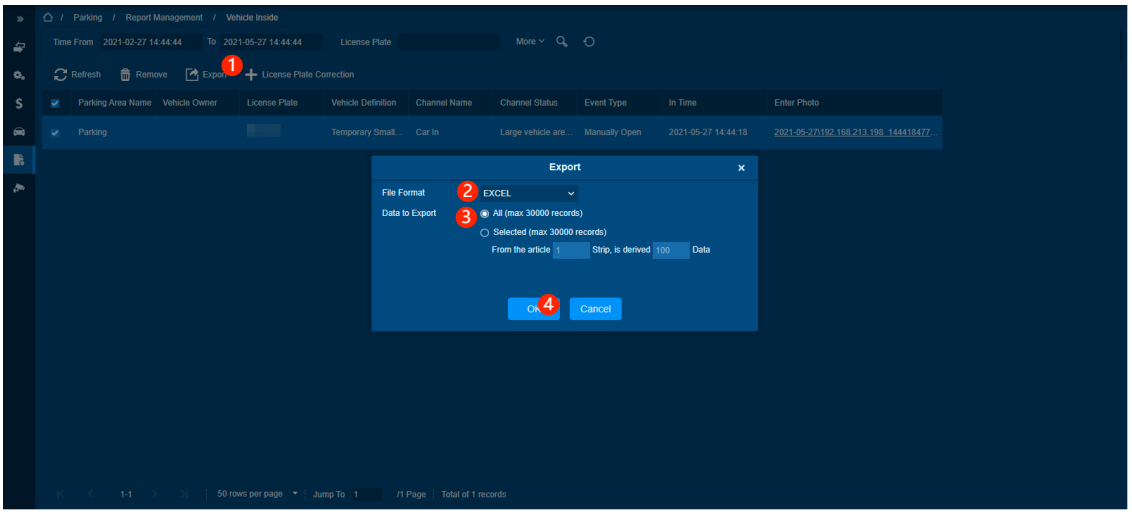
Function Usage Scenarios

Export vehicle inside information from the software to the computer

Feature Trigger Result

Operations	Description
Choose Excel	The format of exported vehicle information is Excel
Choose PDF	The exported vehicle information format is PDF
Choose CSV	The format of the exported vehicle information is CSV
Choose All	Export all vehicle information
Choose selected	Export vehicle information within a certain range

Steps:-



- Click [**Export**] button to pop up the export box.
- Select the format to be exported in the pop-up box.
- Select the range to be exported.
- Click [**OK**] button to finish exporting operations.

License Plate Correction

Preconditions for Normal Use of Functions

The administrator has license plate correction authority.

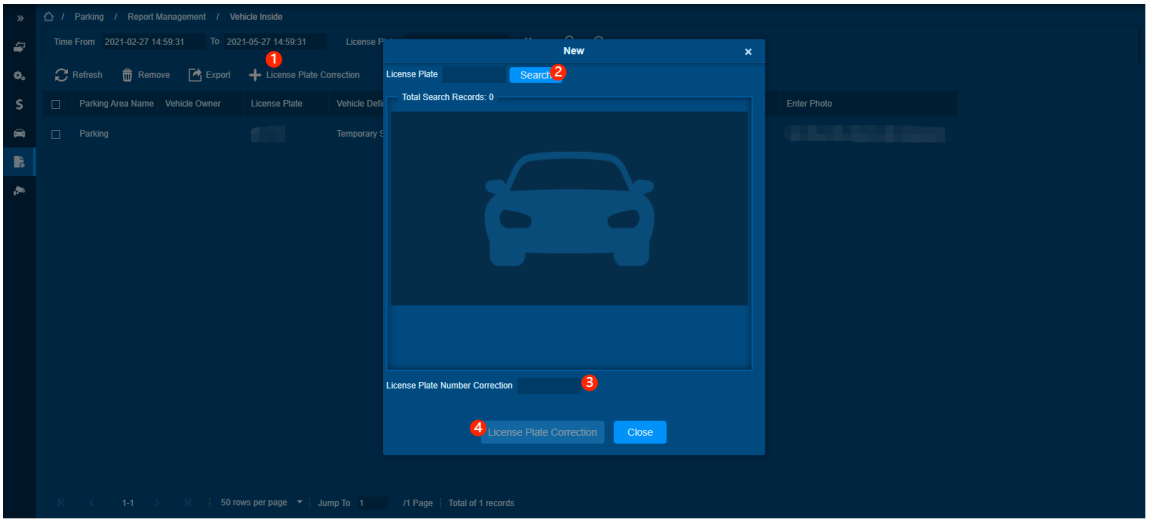
Function Usage Scenarios

When some license plate information is wrong, the license plate can be corrected.

Feature Trigger Result

Correction of license plate information.

Steps:-



- Click [**License Plate Correction**] button, and the license plate correction window will pop up.
- Enter the license plate information and click [**Search**] button.
- Input the corrected license plate.
- Click [**License Plate Correction**] button to complete the verification operation.

10.5.2. Entry Record

Function Introduction

Provide detailed information about vehicles entering the parking lot.

Export

Preconditions for Normal Use of Functions

The administrator has the export function permission.

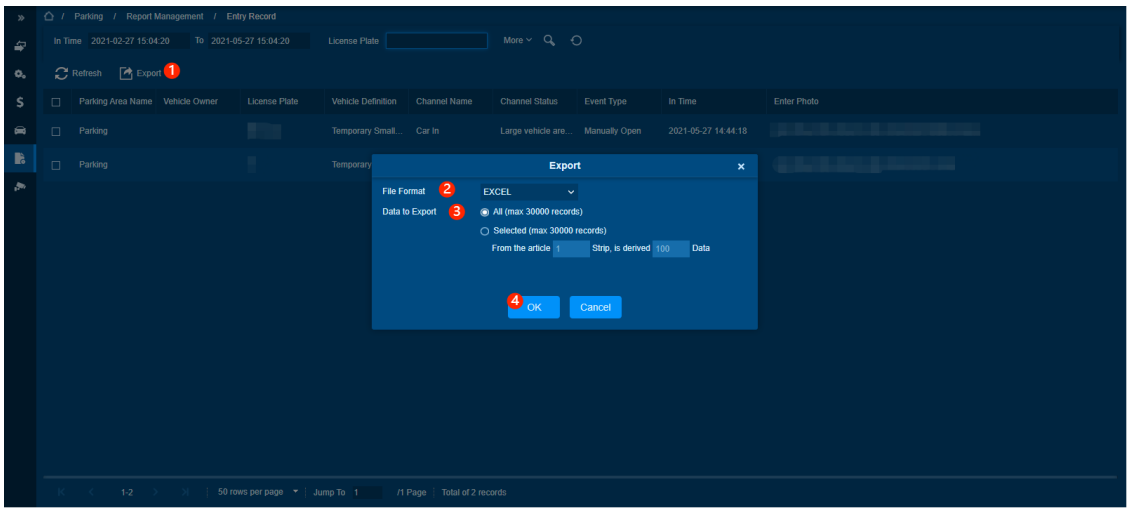
Function Usage Scenarios

Export Entry Record from the software to the computer

Feature Trigger Result

Operations	Description
Choose Excel	The exported entry record format is Excel
Choose PDF	The exported entry record format is PDF
Choose CSV	The exported entry record format is CSV
Choose All	Export all entry record
Choose selected	Export a range of entry record

Steps:-



- Click [**Export**] button to pop up the export box.
- Select the file format to be exported in the pop-up box.
- Select the range to be exported.
- Click [**OK**] button to finish exporting operation.

10.5.3. Exit Record

Function Introduction

Provide detailed information about vehicles leaving the parking lot.

Export

Preconditions for Normal Use of Functions

The administrator has the export function permission.

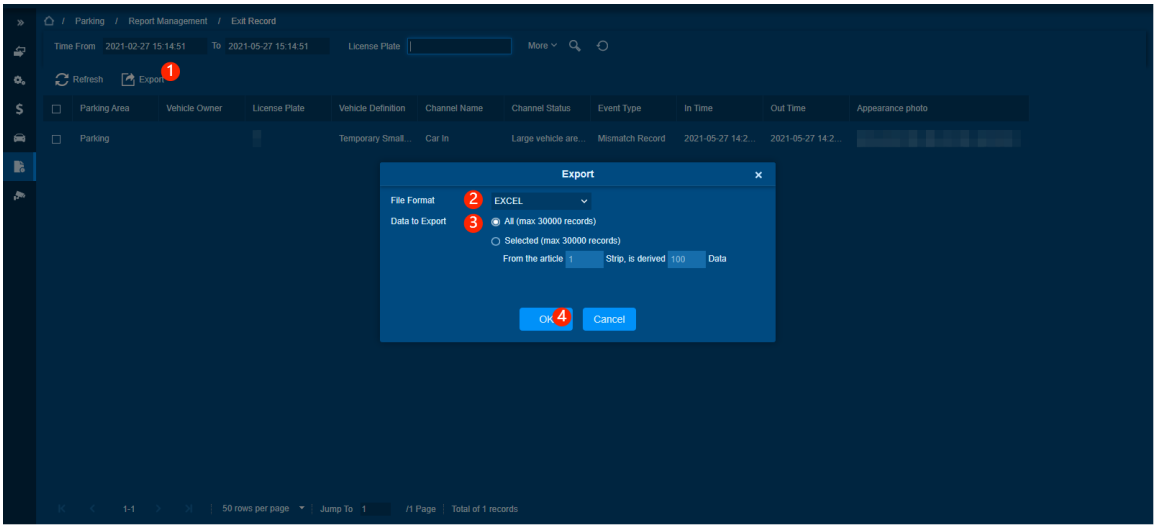
Function Usage Scenarios

Used when the administrator needs to export Exit Record information from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The exported exit record format is Excel
Choose PDF	The exported exit record format is PDF
Choose CSV	The exported exit record format is CSV
Choose All	Export all exit record
Choose selected	Export a range of exit record

Steps:-



- Click [**Export**] button to pop up the export box.
- Select the file format to be exported in the pop-up box.
- Select the range to be exported.
- Click [**OK**] button to finish exporting operations.

10.5.4. Charge Record

Function Introduction

The charge details module provides a report of the charge information of all exported vehicles (fixed vehicles and free temporary vehicles will also generate records with a charge of 0).

Export

Preconditions for Normal Use of Functions

The administrator has export function permissions.

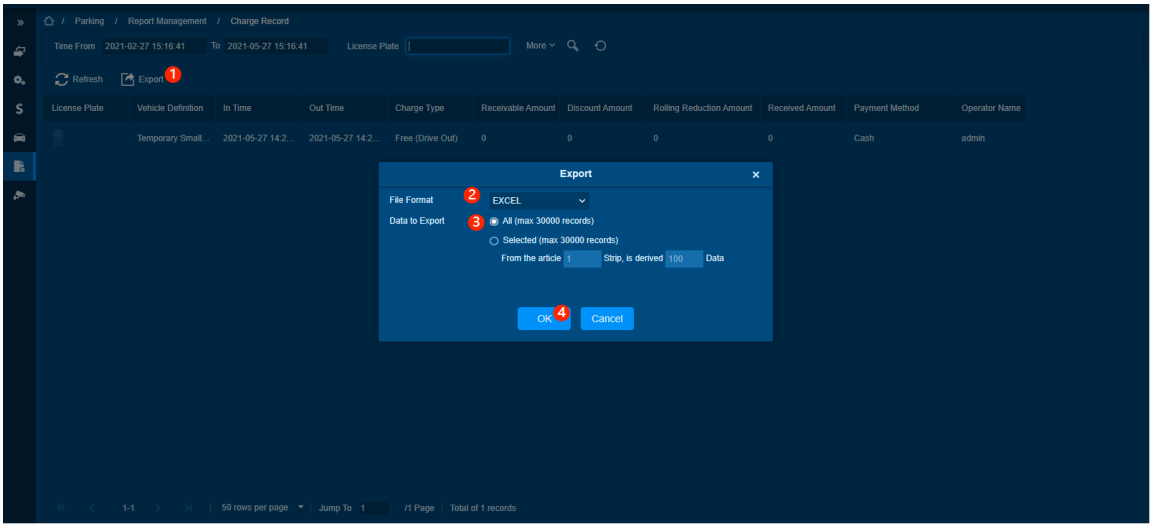
Function Usage Scenarios

The administrator will use it when exporting the charge details from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The format of the exported charge details is Excel
Choose PDF	The format of the exported charge details is PDF
Choose CSV	The format of the exported charge details is CSV
Choose All	Export all charge details
Choose selected	Export charge details within a certain range

Steps:-



- Click [**Export**] button to pop up the Export box.
- Select the file format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operations.

10.5.5. Expired Vehicle

Function Introduction

Show all expired fixed vehicles in the parking lot.

Remove

Preconditions for Normal Use of Functions

The administrator has the permission to remove the function.

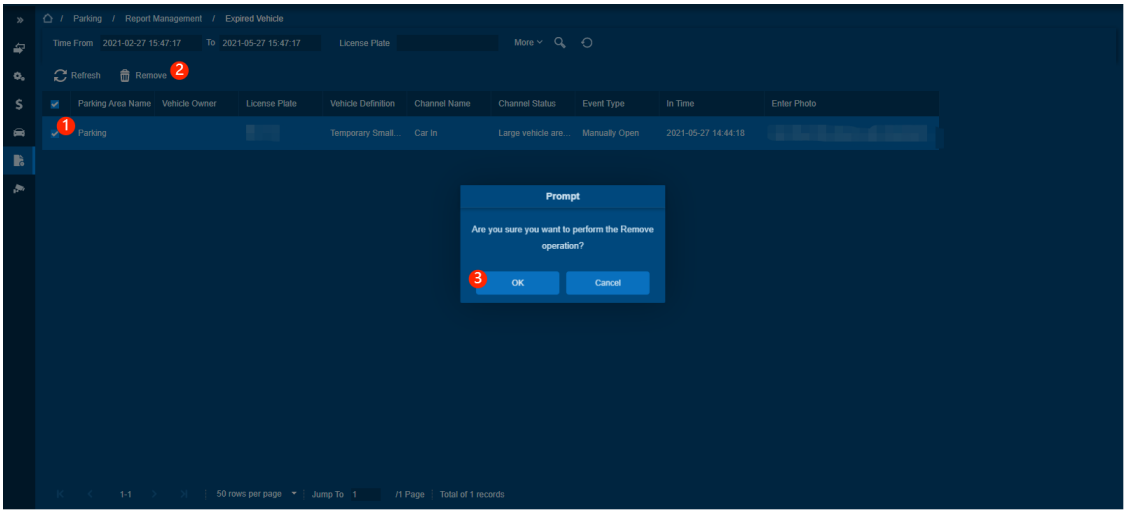
Function Usage Scenarios

The administrator removes the vehicles that stay overtime.

Feature Trigger Result

Remove the vehicles staying in the supermarket.

Steps:-



- Check the license plate data that needs to be removed.
- Click [**Remove**] button, a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the removal of operations.

10.5.6. Incoming Unusual Vehicles

Function Introduction

When the vehicle enters and exits, the abnormal detection status is displayed.

Export

Preconditions for Normal Use of Functions

The administrator has export function permissions.

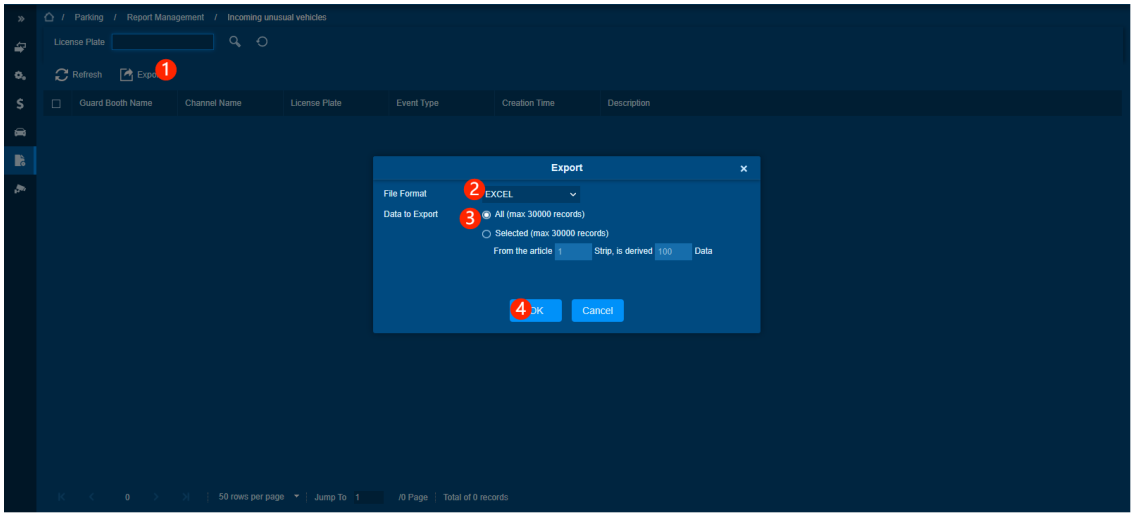
Function Usage Scenarios

Used when the administrator exports the vehicle information from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The format of the exported vehicle information is Excel
Choose PDF	The format of the exported vehicle information is PDF
Choose CSV	The format of the exported vehicle information is CSV
Choose All	Export all vehicle information
Choose Selected	Export vehicle information within a certain range

Steps:-



- Click [**Export**] button to pop up the export box.
- Select the file format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operation.

10.5.7. Fixed Vehicle Authorization Record

Function Introduction

Provide all the details of the vehicle whose license plate has been registered in the system. You can export detailed information as needed.

Export

Preconditions for Normal Use of Functions

The administrator has export function permissions.

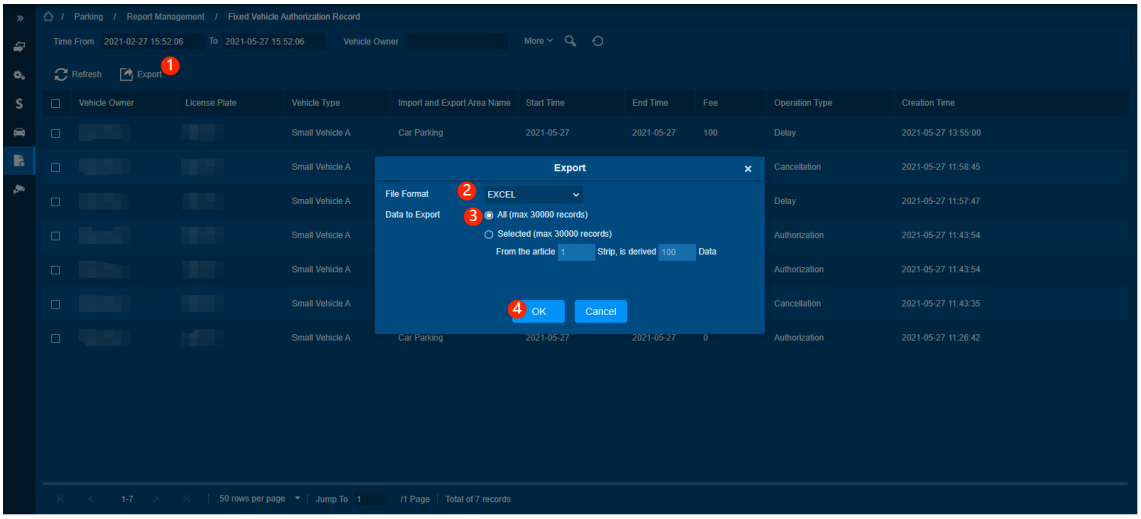
Function Usage Scenarios

It is used when the administrator exports the fixed vehicle authorization record from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The format of the exported authorization record is Excel
Choose PDF	The format of the exported authorization record is PDF
Choose CSV	The format of the exported authorization record is CSV
Choose All	Export all authorization records
Choose selected	Export authorization records within a certain range

Steps:-



- Click [**Export**] button to pop up the export box.
- Select the file format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operation.

10.5.8. Device Operation Record

Function Introduction

Unify the device's operations records for record management.

Delete

Preconditions for Normal Use of Functions

The administrator has the delete function permission, and there are data that can be deleted in the list.

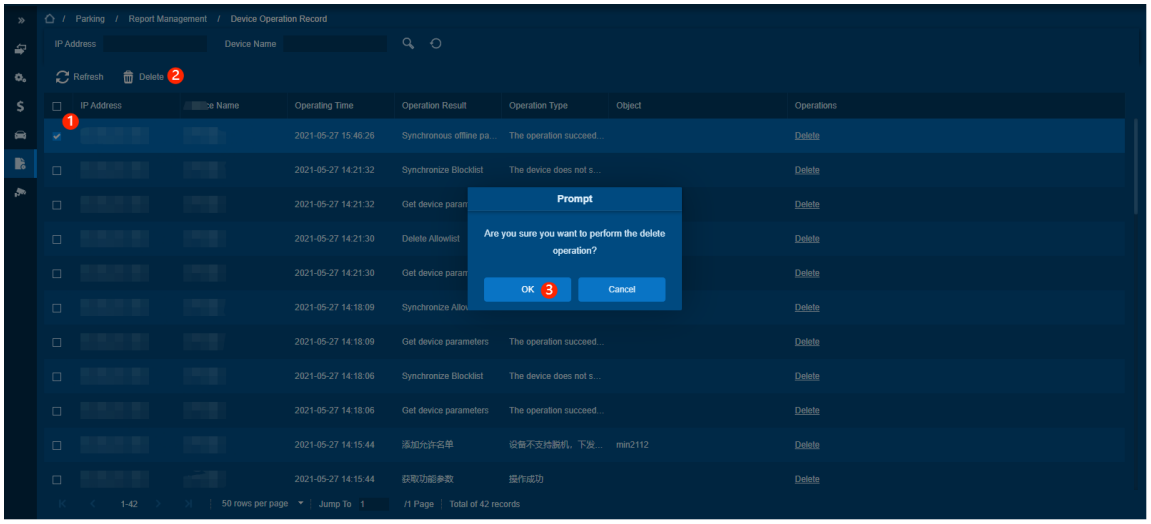
Function Usage Scenarios

Delete redundant device operation record.

Feature Trigger Result

Delete checked record.

Steps:-



- Check the data that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] button to complete delete operations.

10.5.9. Handover Statistics

Function Introduction

The handover record provides a report of the handover record.

Export

Preconditions for Normal Use of Functions

The administrator has export function permissions.

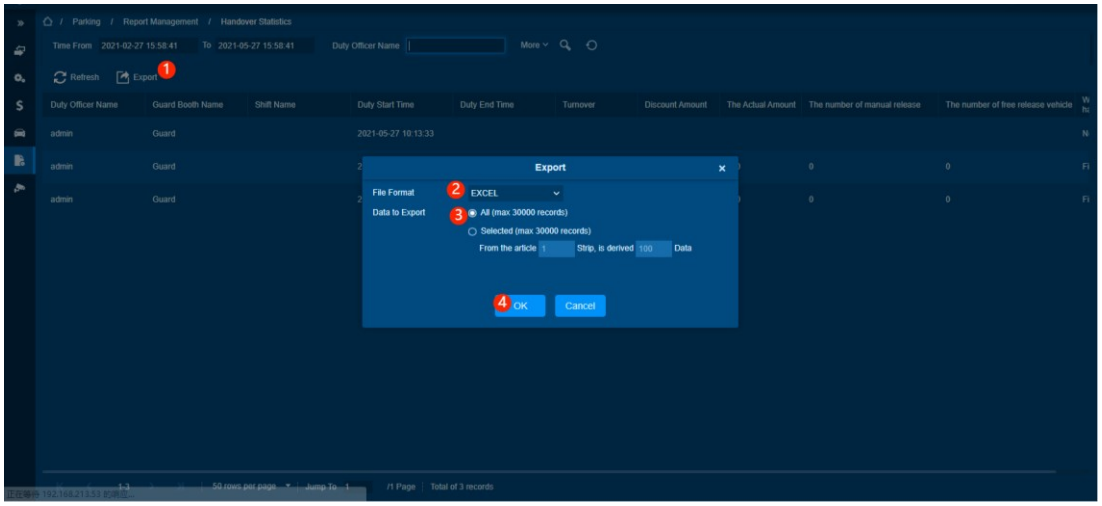
Function Usage Scenarios

Used when the administrator exports handover statistics from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The format of the exported shift information is Excel
Choose PDF	The format of the exported shift information is PDF
Choose CSV	The format of the exported shift information is CSV
Choose All	Export all shift information
Choose selected	Export shift information within a certain range

Steps:-



- Click [**Export**] button to pop up the Export box.
- Select the format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operation.

10.5.10. Daily Income Statistics

Function Introduction

Provides a report on the total daily cost of each Guard Booth for each shift.

Export

Preconditions for Normal Use of Functions、

The administrator has export function permissions.

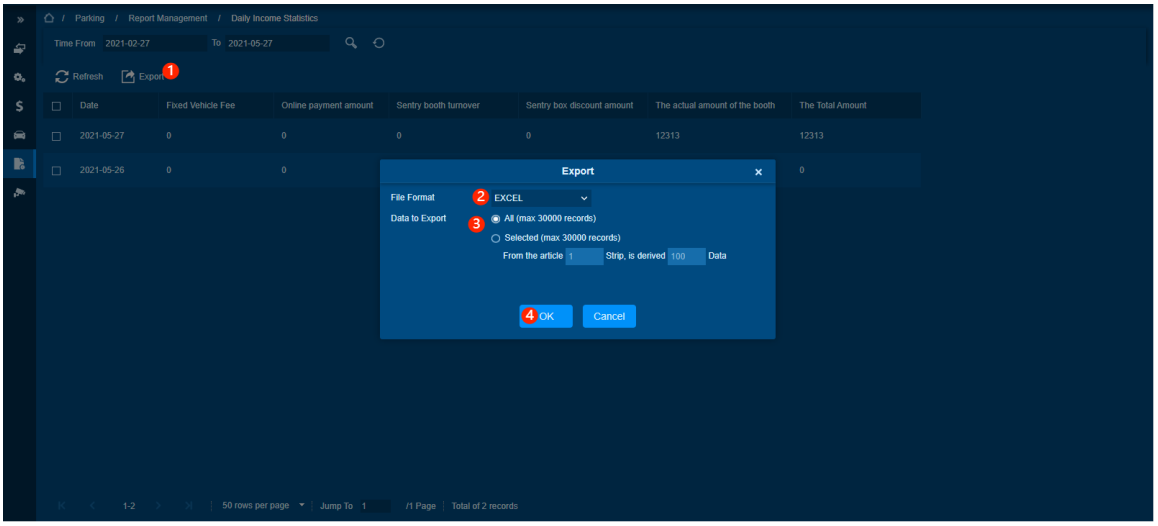
Function Usage Scenarios

Used when the administrator exports the statistical table from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The format of the exported daily income statistics information is Excel
Choose PDF	The format of the exported daily income statistics information is PDF
Choose CSV	The format of the exported daily income statistics information is CSV
Choose All	Export all daily income statistics information
Choose selected	Export daily income statistics information within a certain range

Steps:-



- Click [**Export**] button to pop up the Export box.
- Select the file format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operation.

10.5.11. Monthly Income Statistics

Function Introduction

Export

Preconditions for Normal Use of Functions

The administrator has Export function permissions.

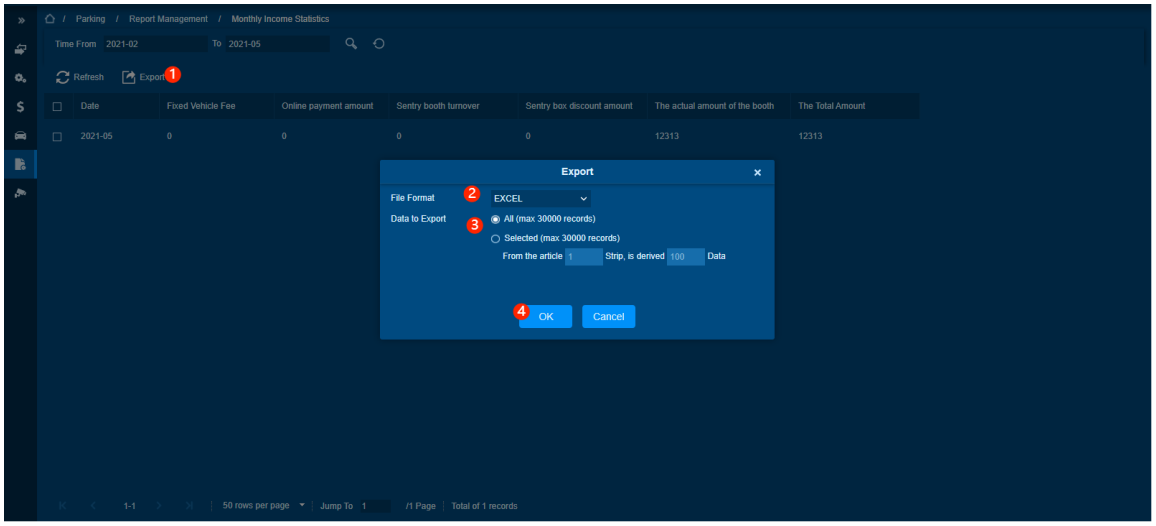
Function Usage Scenarios

Used when the administrator exports the statistical table from the software to the computer.

Feature Trigger Result

Operations	Description
Choose Excel	The exported monthly income statistics information format is Excel
Choose PDF	The exported monthly income statistics information format is PDF
Choose CSV	The exported monthly income statistics information format is CSV
Choose All	Export all monthly income statistics information
Choose selected	Export monthly income statistics information within a certain range

Steps:-



- Click [**Export**] button to pop up the Export box.
- Select the file format that needs Export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete export operation.

10.6. Real-Time Monitoring

Preconditions for Normal Use of Functions

If there is a parking device online, please use Internet Explorer to access this module, because only this browser supports video preview.

Function List

Operations	Description
Guard Booth Monitoring	Guard Booth can be monitored, manual release, shift change, block and allow list management, on-site vehicle query, charge details, limit management operations
Monitoring Room	It can monitor guard booth and remotely open the gate

10.6.1. Sentry Booth Monitoring

Function Introduction

Real-time monitoring provides real-time monitoring data.

Manual Release

Preconditions for Normal Use of Functions

There is a channel that can be released.

Function Usage Scenarios

Manual release can be used when the device cannot be recognized or is offline.

Feature Trigger Result

Manually release vehicles into and out of the field.

Steps:-

- Fill in the license plate information for manual release.
- Select the channel to be released.
- Reasons for choosing manual release.
- Click [**Confirm**] button to complete the manual release of operation.

Shift

Preconditions for Normal Use of Functions

The shift function is turned on in the parking lot settings.

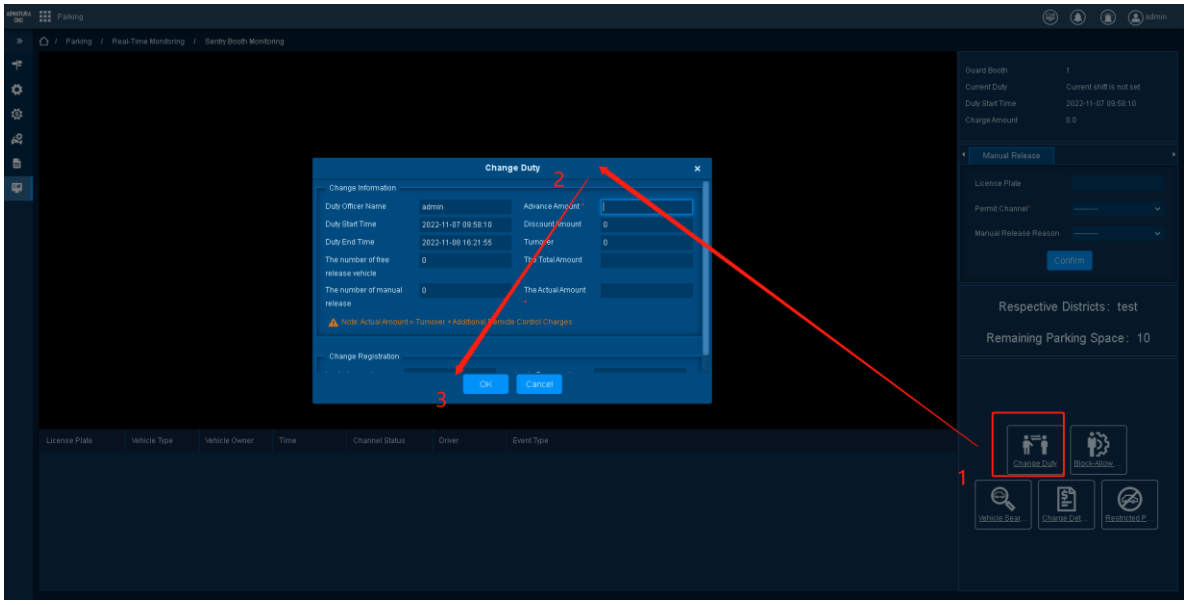
Function Usage Scenarios

When the shift needs to be changed, the shift will be handed over.

Feature Trigger Result

Shift, submit the current shift data to Financial Reconciliation.

Function Operation Progress



- Click [**Change Duty**] button to pop up a window.
- Fill in relevant information.
- Click [**OK**] button to complete the shift.

Block and Allow List Management

Click the [**Block-Allow List Management**] button to pop up the block and allow list management window, the function is consistent with the block and allow list management function.

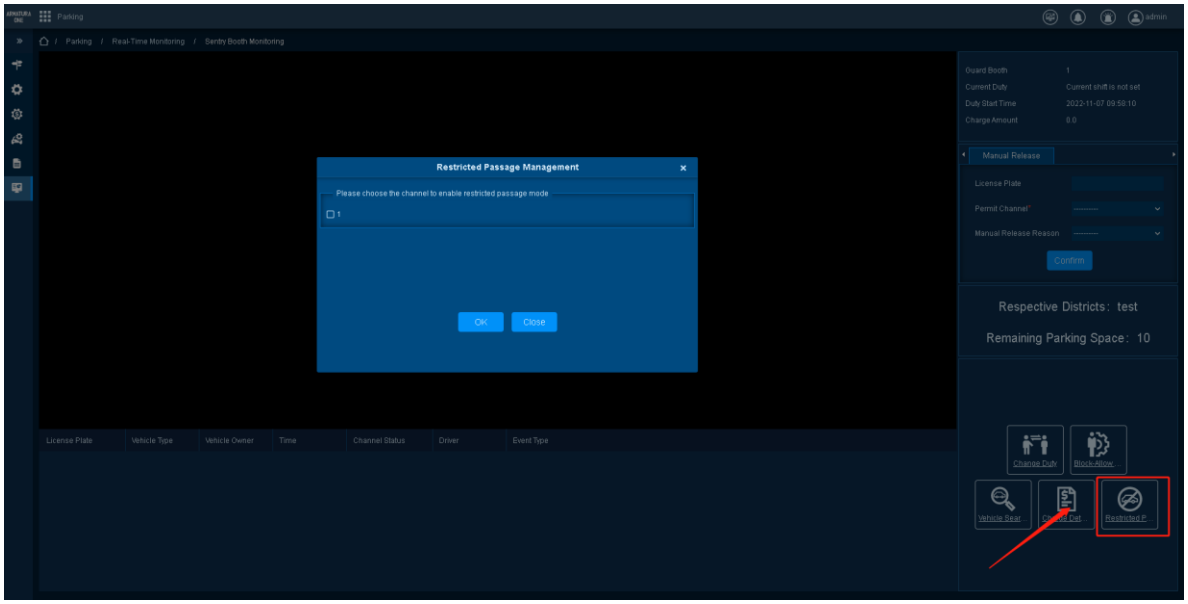
Inquiry of Vehicles in the Venue

Click the [**Vehicle Search**] button to pop up the vehicle search window in the venue, the function is the same as that of vehicle inside.

Charge Details

Click the [**Charge Details**] button to pop up the charge details window, the function is consistent with the charge details.

Limit Line Management



Click [**Restricted Passage Management**] button, a window will pop up, select the channel that needs to be restricted, and click the [**OK**] button to complete the restricted operations.

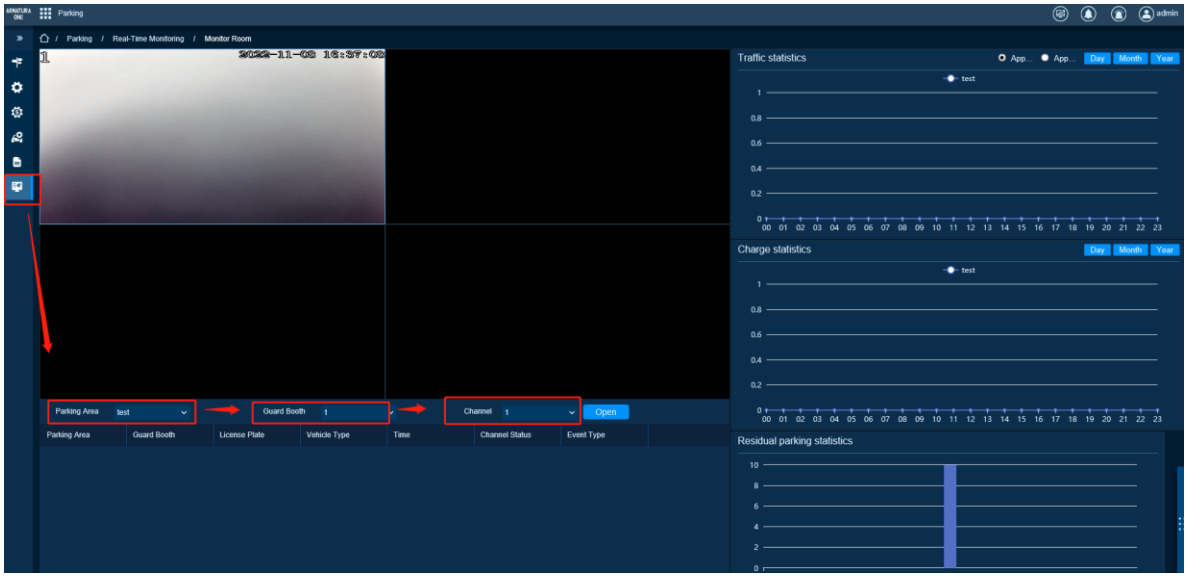
10.6.2. Monitor Room

Function Introduction

In Monitoring Room, you can check video images and entrance and exit information of all guard booths in all parking lots.

Choose **[Real-Time Monitoring]** > **[Monitor Room]**. The Monitoring Room page is displayed as in the following figure.

Select different guard booth or channels to switch the display content.



11. Video Module

The ability to realize video management by integrating and Milestone's Xprotect product. Under this module, you can perform real-time preview and playback of video equipment in authority. You can also set recording schedules, online patrols, and tracking and analysis alarms for people and cars. It is an important functional module for visual security.

11.1. Video Management

Function List

Operations	Descriptions
Video Device	Unified management of Video Device.
Video Preview	It can view the monitoring screen which is connected to the Video Device in real time and can remotely control the PTZ device.
Video Playback	It is possible to replay the recorded content of the camera by searching for the specified time and specifying the camera.
Video Plan	Set the camera device to record regularly and store the video content. The operation flow is Add Video Plan, add cameras in the plan and enable the Video Plan.

11.1.1. Device

Function Description

Unified management of Video Device.

Device List

Preconditions for Normal Use of Function

For third-party integrated , the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

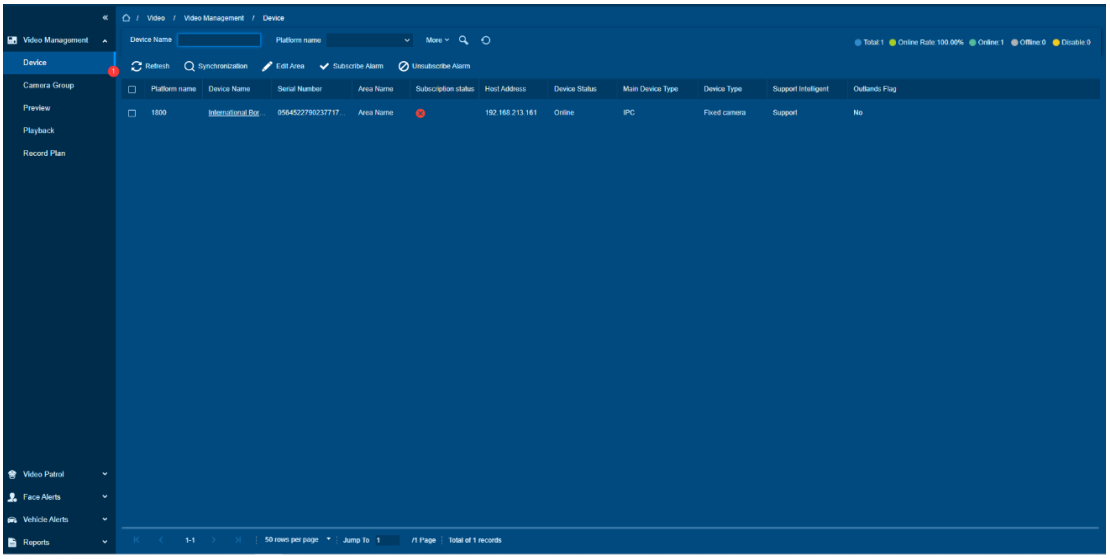
View device information.

Feature Trigger Result

The

Operations	Descriptions
Enter the Page	Check equipment condition

page directly displays the device list data according to the conditions and counts. The status of the device is as follows.



Synchronizing Devices

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

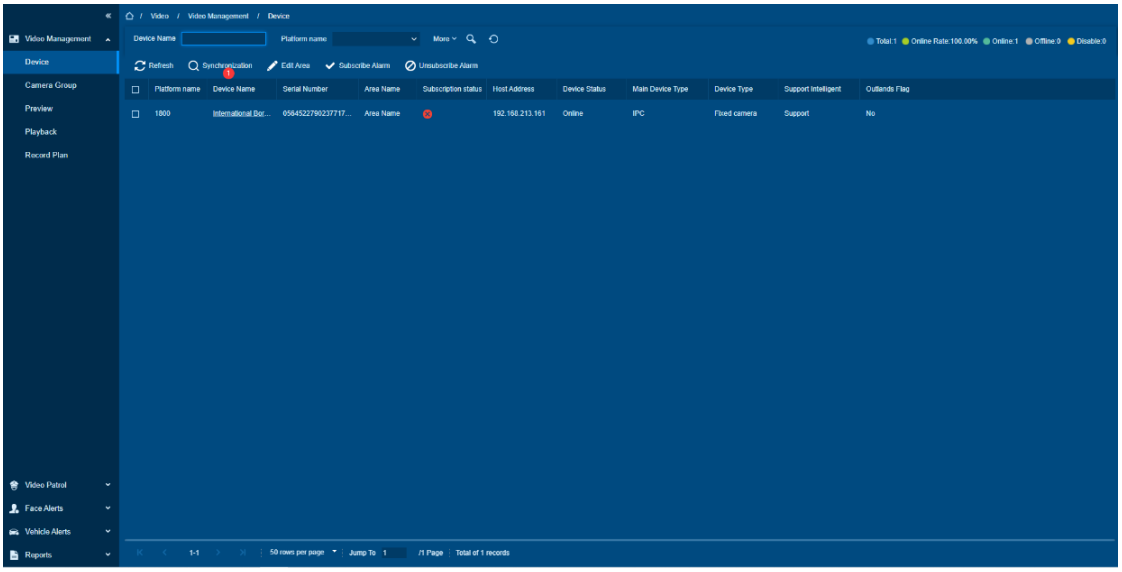
Parameter configuration account permission switch when device data is inconsistent.

Feature Trigger Result

After

Operations	Descriptions
Sync Device	The device data under the account authority will be updated synchronously

completing the parameter configuration, click **[Synchronization]** button, and device list will be generated automatically.



Modify Area

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

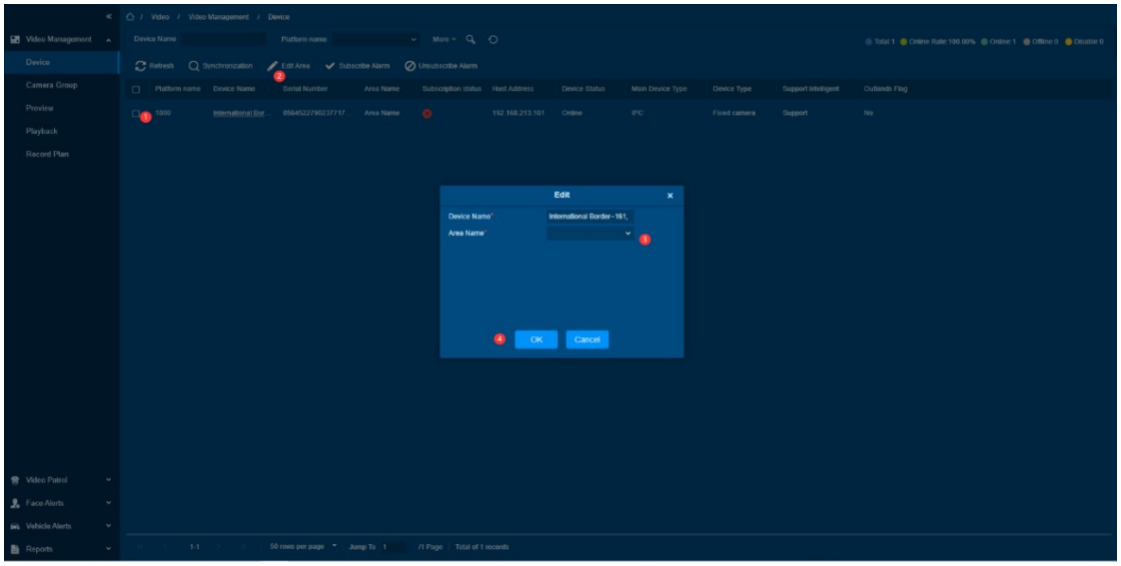
Change the camera's regional permissions.

Feature Trigger Result

Steps:

Operations	Description
Modify Area	Modify the camera's regional permissions

- Check the Video Device of the area that needs to be adjusted and click the [**Edit Area**] button.



Device name: Checked Video Device.

Area Name: Drop down to select the area name, and the area setting refers to the previous area setting.

- Click [**Finish**] to complete the device area adjustment.

Subscribe to alerts

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

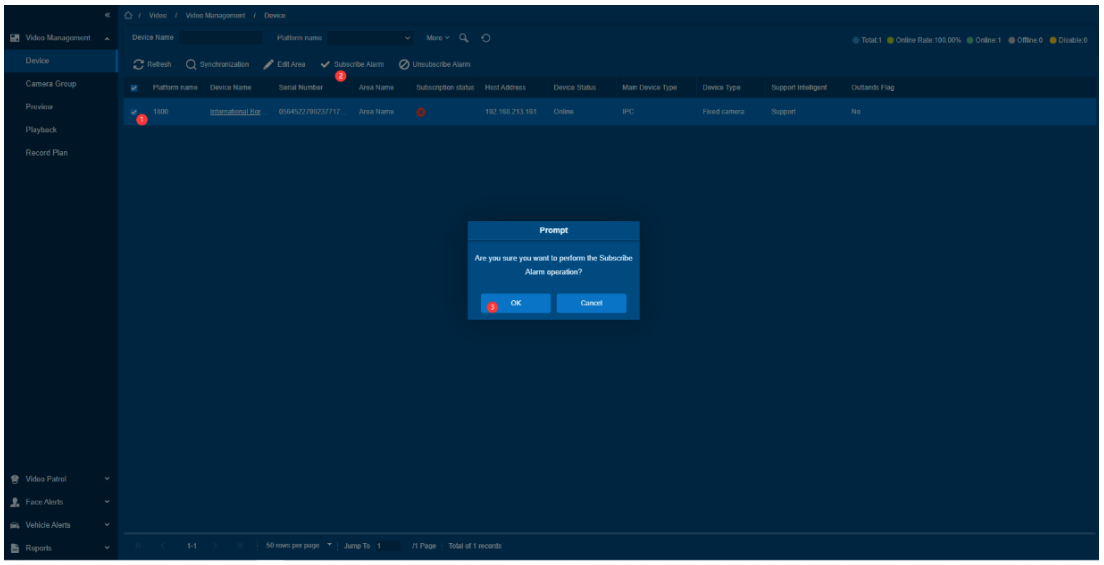
Subscribe to camera alarm data.

Feature Trigger Result

Operations	Descriptions
Subscribe to alerts	Subscribe to camera alarm data

Steps:

- Check the Video Device that needs video alerts and click [**Subscribe Alarm**] button.



- Click [**OK**] to turn on the device video alerts.

Cancel Subscribe to alerts

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

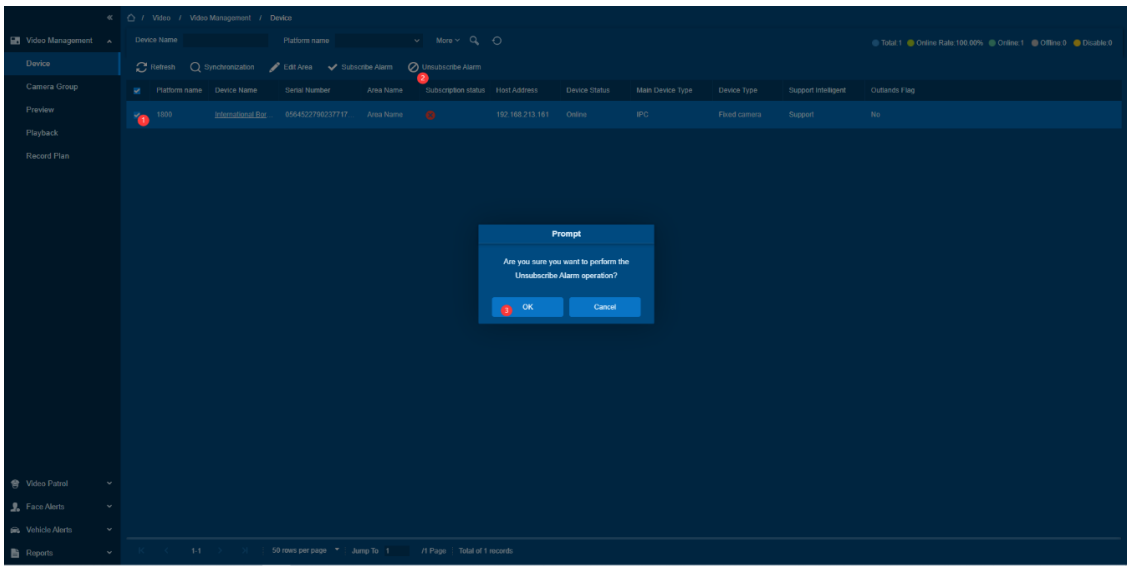
Function Usage Scenarios

Cancel the alarm data of the camera subscription.

Feature Trigger Result

Check the Video Device that needs to remove the video alarm and click the **[Unsubscribe Alarm]** button.

Operations	Descriptions
Cancel Subscribe to alerts	Cancel the alarm data of the camera subscription



Click [**OK**] to close the device video alarm.

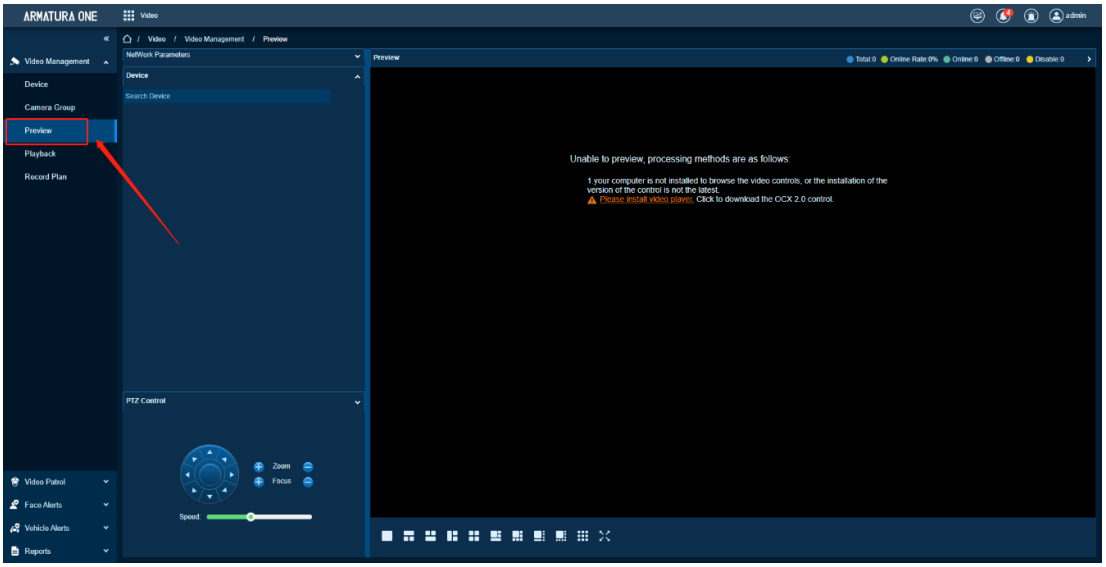
11.1.2. Preview

Function Description

In this menu, you can view the monitoring screen of the connected video equipment in real time and remotely control the PTZ equipment.

Steps:

Click [**Video Management**] > [**Preview**] to view the preview interface: the interface is divided into 4 windows.



Network Parameters

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

For the first time, the video player plug-in must be downloaded, and the browser must be restarted after installation. Only the browser is currently supported.

Function Usage Scenarios

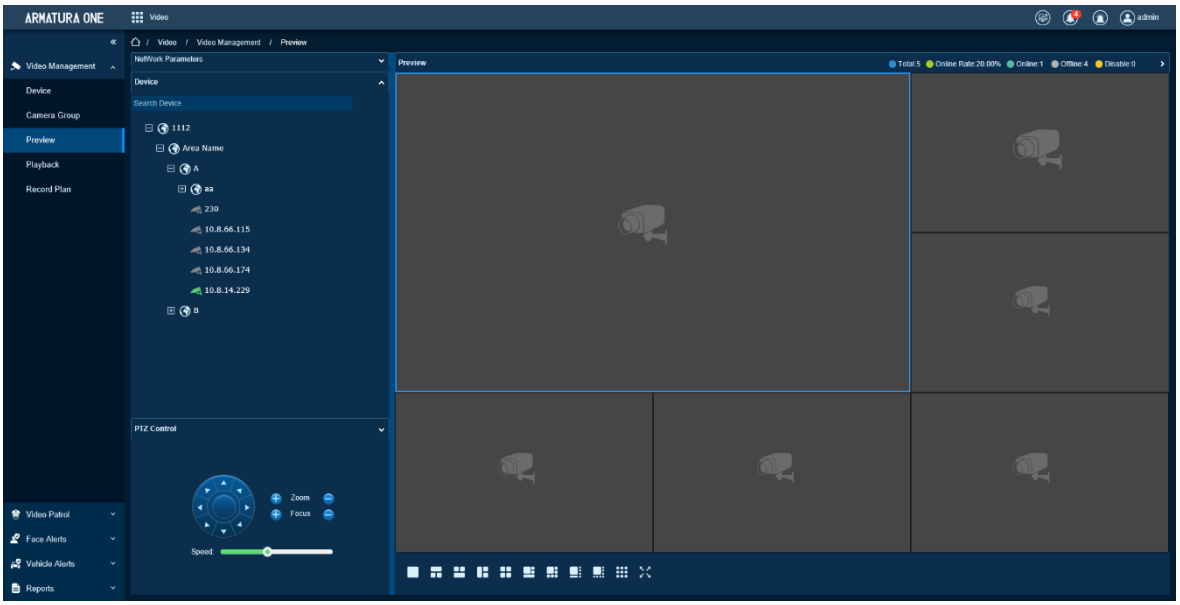
The video cannot be played, you can modify the playback parameters and the network parameters used when playing the video.

Feature Trigger Result

Set

Operations	Description
Modify network parameters	Parameters used for video playback

the parameters of video playback.



Protocol Type: Select the TCP or UDP protocol based on the type of connected device. The TCP protocol is default.

Stream Type: Optional unassigned\mainstream\sub stream1\sub stream2, select according to the type of connected device. The mainstream is used by default.

Device List

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The camera data is synchronized normally.

Function Usage Scenarios

To view the current device information, double-click the device list to preview the device.

Feature Trigger Result

Operations	Description
Double-click the device list	In the Video Preview window, select the pane to play and preview the video.

Device list: Display the device list tree by area. The gray icon indicates that the device is offline; white indicates that the device is online; green indicates the device being previewed; entering the device name in the search box can quickly locate the retrieved device.

PTZ Control Panel

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only supports the IE browser, when the camera is required to play the screen, and the camera needs to support this function.

Function Usage Scenarios

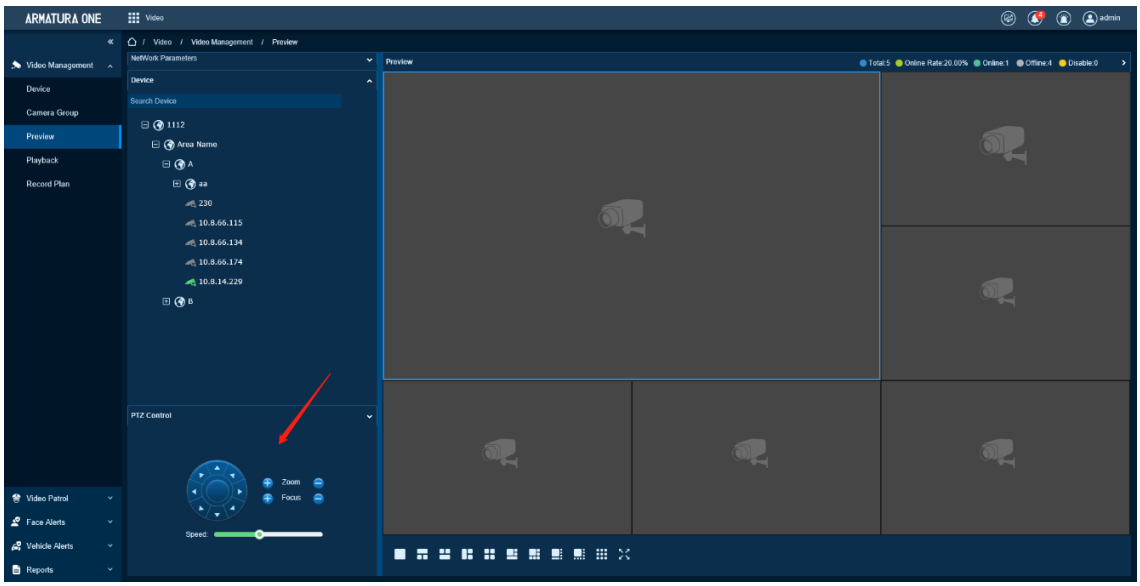
When you need to adjust and move the camera screen, you can control the PTZ.

Feature Trigger Result

Operations	Description
PTZ Control	When the video is playing, make adjustments such as screen movement according to the control.

PTZ control panel:

- Select the camera that supports PTZ control in the preview box on the right and control the camera in the PTZ panel.
- The direction adjustment button allows you to change the camera's viewing angle in 8 different directions.
- The lens adjustment button allows you to zoom in and out the lens distance.
- The focal length adjustment button allows you to adjust the clarity of the lens by zooming in and out.
- The speed bar controls the lens viewing angle's movement speed, which is useful for both large-scale movement and fine-scale fine-tuning.



Device Status Bar

Preconditions for Normal Use of Function

The software runs normally. The account has corresponding operation permissions.

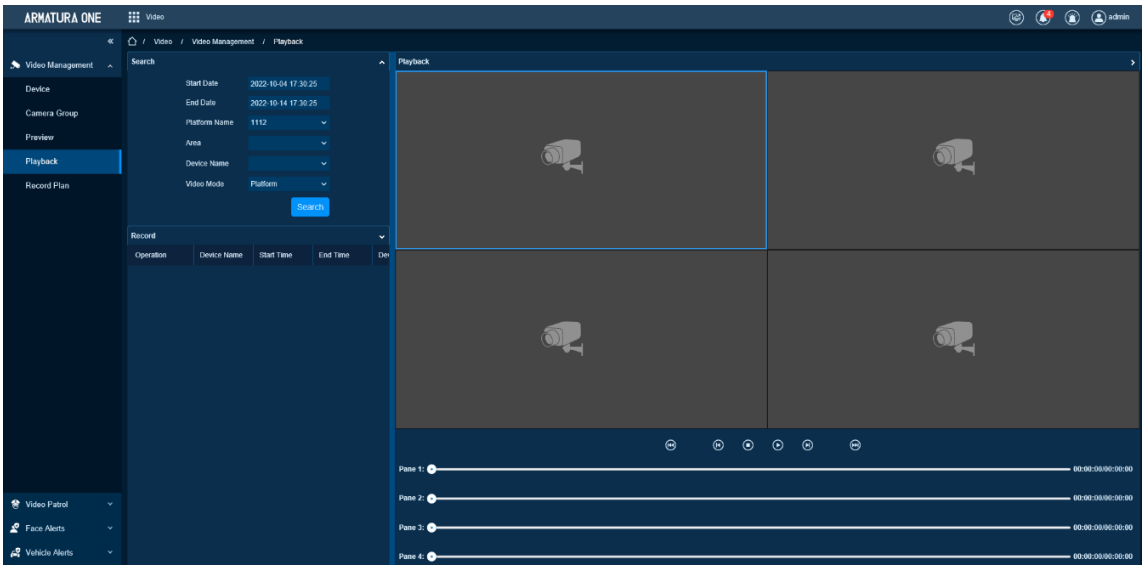
Function Usage Scenarios

Check the online status of the device.

Feature Trigger Result

Operations	Description
Enter the Page	View statistics about the online status of the device.

It displays the basic conditions and statistics of all connected devices currently.



Preview Window

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only supports IE browser, double-click the camera on the device list to play.

Function Usage Scenarios

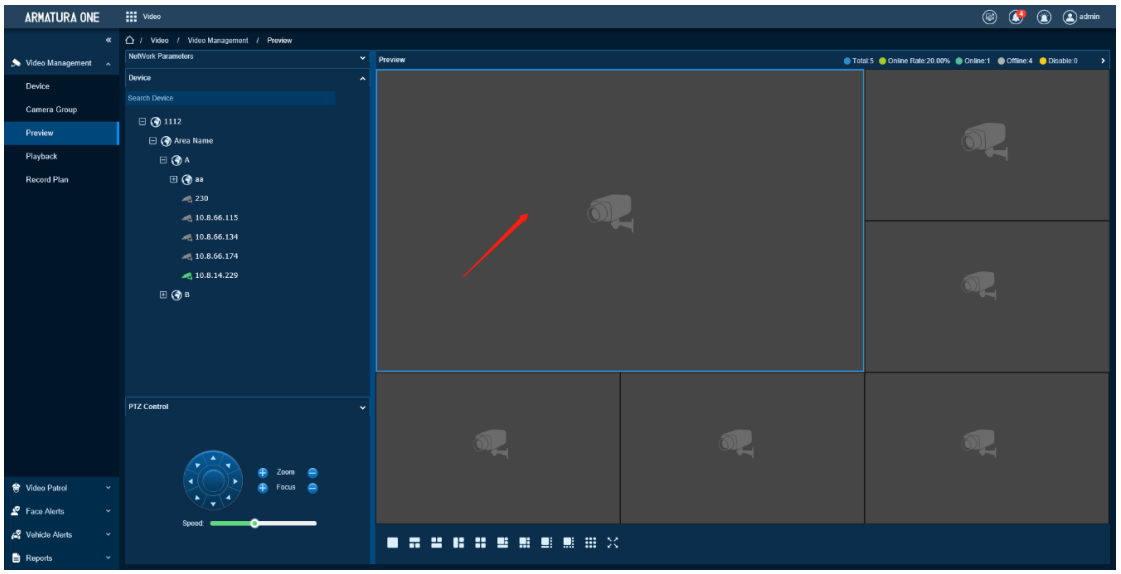
When you need to view the camera screen, you can view and play in multiple windows.

Feature Trigger Result

Operations	Description
Close pane	Video playback stopped
Multi-pane switching	Video playback pane adjustment

Preview window:

- Play and select the camera preview screen.
- Control the number of panes of the picture being played at the same time, support adjustment from 1 to 9 panes.
- Full screen button, full screen display preview window.
- The preview pane supports screen capture, and the PTZ camera can click the PTZ direction adjustment button to control the direction on the playback pane.

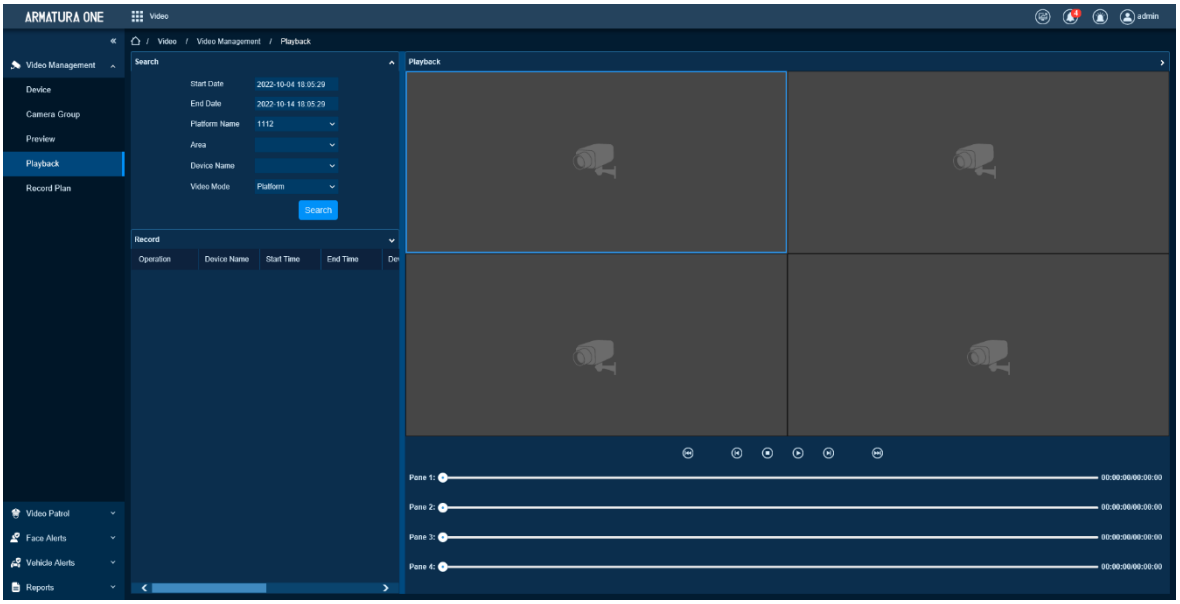


11.1.3. Playback

Function Description

The camera recorded content can be played back by retrieving the recorded video by specifying time and camera under this menu option.

Click [**Video Management**] > [**Playback**] to view the playback interface: It composed of 3 parts.



Search Window

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only the i.e., browser is supported.

Function Usage Scenarios

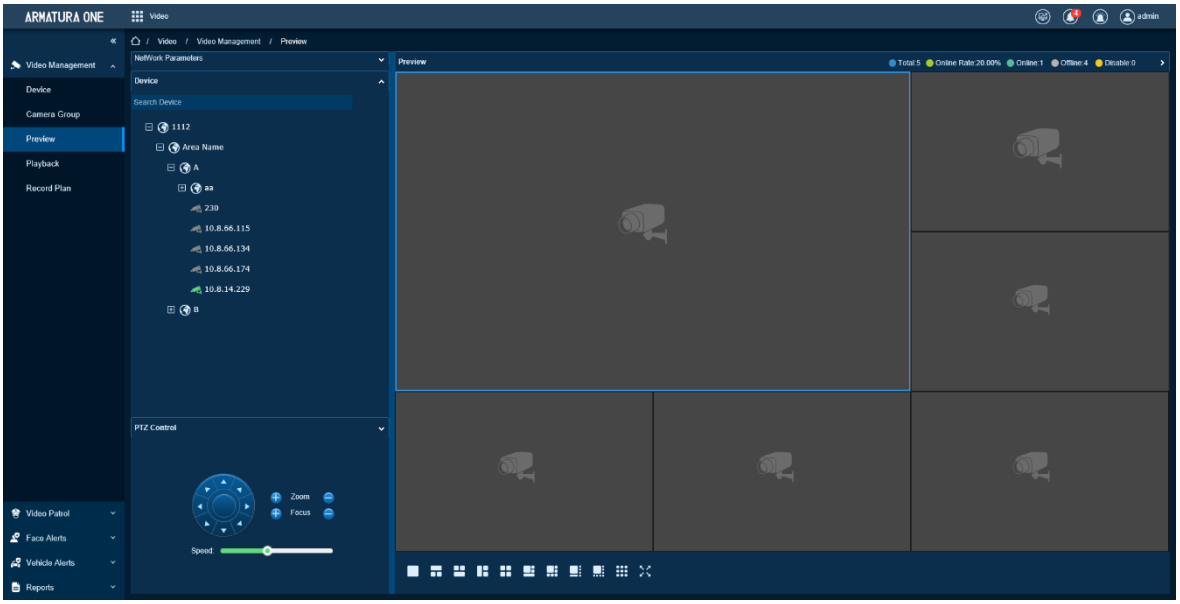
Need to call the video recording and search according to the conditions.

Feature Trigger Result

Operations	Description
Video search	Retrieve the recording data that meets the conditions

Search Window:

- Select the start and end time of the playback video.
- Select the preset camera area to facilitate quick camera search.
- Select the camera name you want to view, support multiple selection and one-key selection.
- The video mode can choose platform video and front-end video content. It is selected according to the video storage mode of the Video Plan. The default is platform video.



- After setting the parameters, click [Search] button, and the search results will be displayed in the video record pane.

Video Recording Pane

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only the i.e., browser is supported.

Function Usage Scenarios

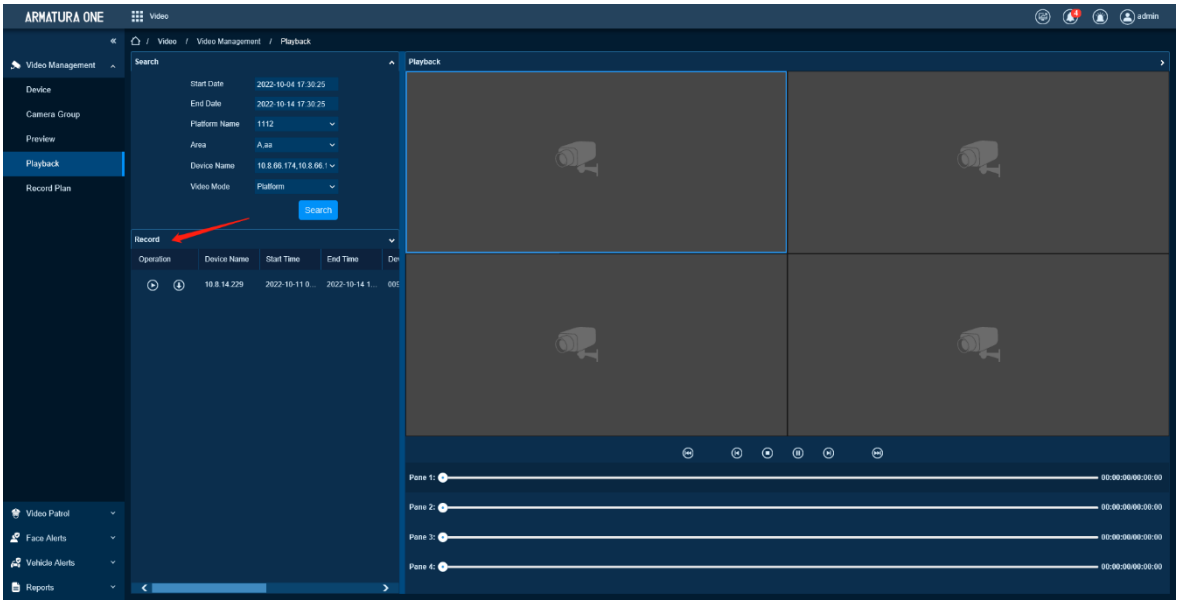
It is necessary to perform playback and video download operations on the retrieved Video Plan.

Feature Trigger Result

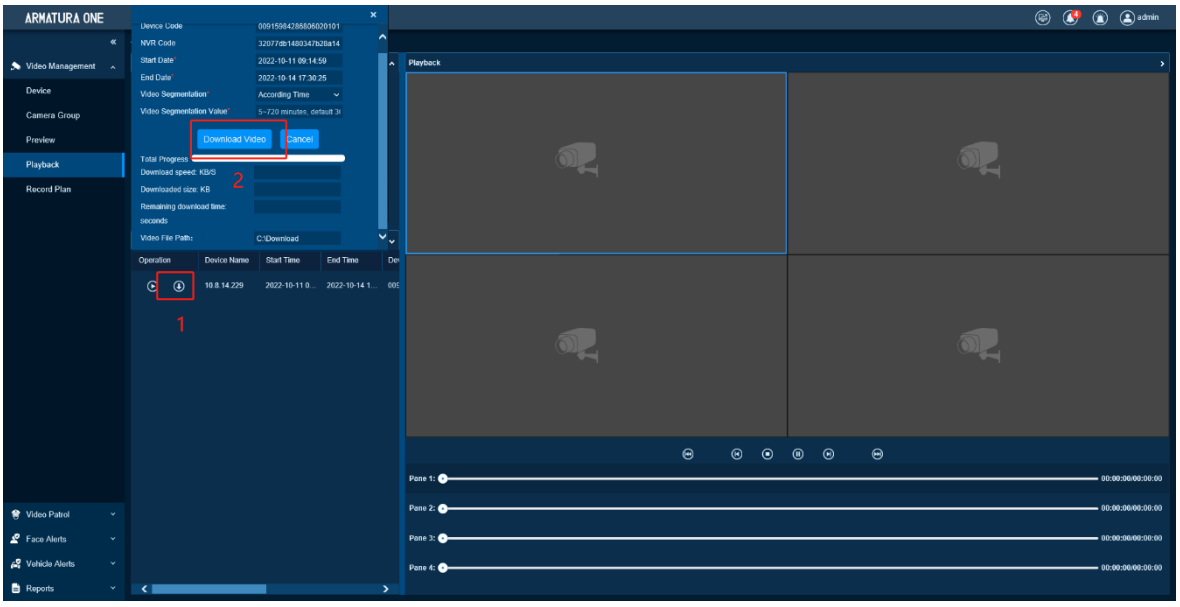
Operations	Description
Video playback	Play back the video recording
Video download	Download the video recording

Video record pane:

- Click **[Search]** button to play the current path record.



- Click **[Download Video]** button, a video download interface will pop up.



Video Download Interface: Its display the basic information of the video which is currently downloaded.

Video Segmentation: The download segmentation mode can be set, and the video can be downloaded according to the length of time. The default download time is 30 minutes, and you can choose from 5 to 720 minutes.

Download videos according to the video storage size, the default download size is 2048MB, 200 to 3072MB is optional.

Click [**Download Video**] button to start the video download, and the download progress will be displayed below playback window.

Video Playback Pane

Preconditions for Normal Use of Function

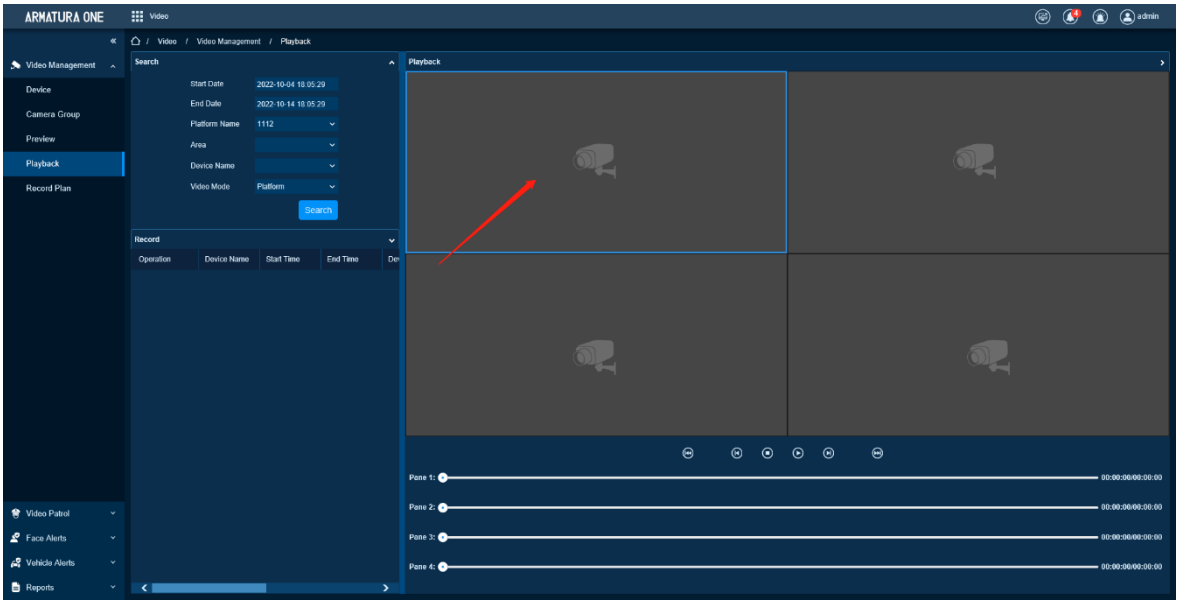
For third-party integrated the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only i.e., browser is supported.

Function Usage Scenarios

Need to control the playback of the video and play in multiple panes.

Feature Trigger Result

Operations	Description
Play control	Control the video screen.



Video Playback Pane: Support 4 channels of video playback at the same time.

Control Par: Control the video playback speed, support slow rewind, and slow forward playback at a minimum of 1/32 times; fast rewind and fast forward playback at a maximum of 32 times; pause video; stop playback.

Progress Bar: Displays the playing time and total time of the current playback video and supports dragging to fast forward and rewind the video playback progress.

11.1.4. Record Plan

Function Description

Set the camera device to record regularly and store the video content. The operation flow is Add Video Plan, add cameras in the plan, and enable the Video Plan.

Video Plan List

View Video Plan data

Preconditions for Normal Use of Function

The software runs normally, and the account has corresponding operation permissions.

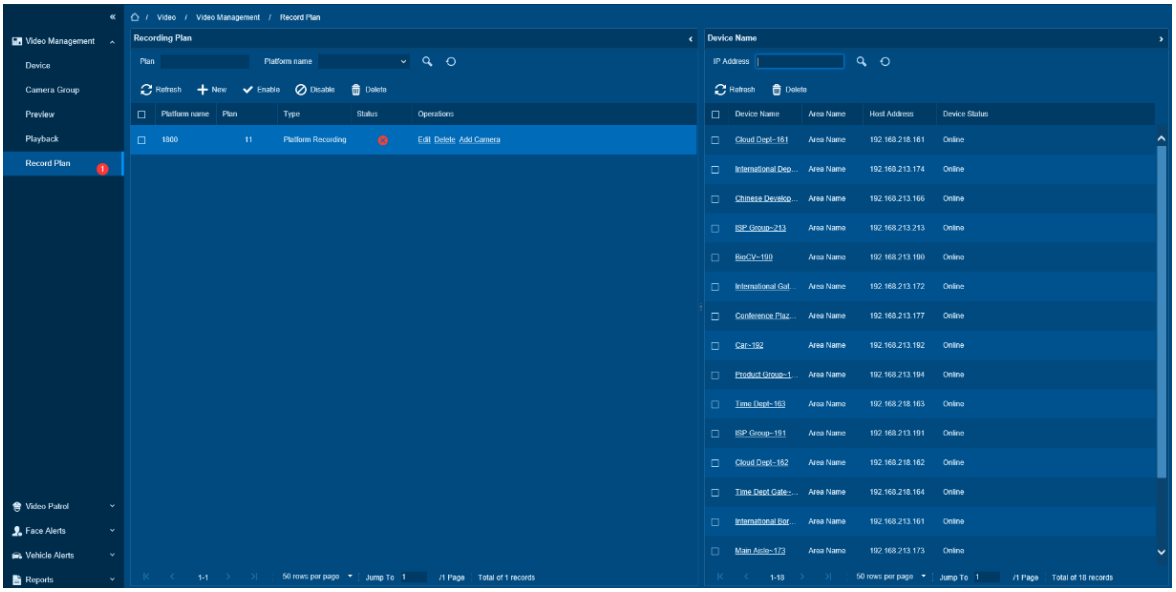
Function Usage Scenarios

Need to check the current situation of the camera to enable the recording function.

Feature Trigger Result

Operations	Description
Enter the Page	Show the current recording plan

Click [**Video Management**] > [**Record Plan**] to view the record plan interface.



Add Video Plan

Preconditions for Normal Use of Function

For third-party integrated , the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

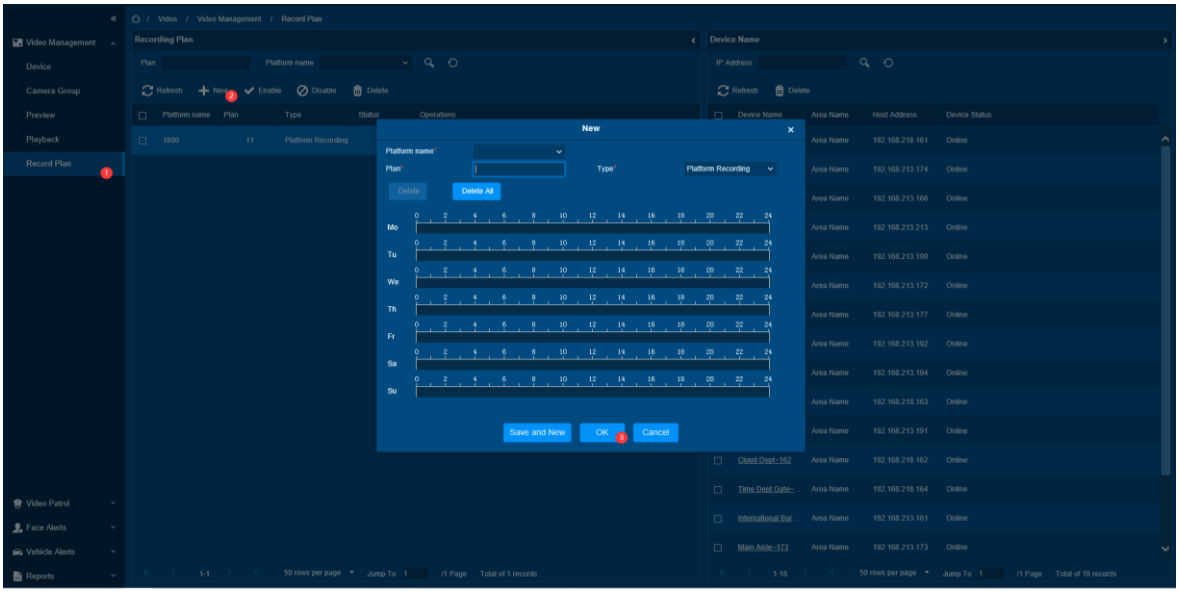
Need to arrange Video Plan for certain cameras in a certain time.

Feature Trigger Result

Click

Operations	Description
Add Video Plan	Set the Video Plan in the Timetable and send the data on the configuration server synchronously

[**Video Management**] > [**Video Plan**] > [**Add**] to enter the Add editing interface:



The fields description are as follows:

Plan Name: Set the name of the Video Plan, which is convenient and quick to find and cannot be repeated.

Storage Type: Optional platform storage, that is, the video is stored in the local server; front-end storage, that is, the video is stored in the camera (device support is required).

Set the Recording Time: Drag on the time bar to select the required recording Timetable and support multiple copies.

Click the [**Save**] button to complete the new plan, and the new plan will be displayed in the plan list.

✍**Note:**

Add plan is disabled by default and needs to be manually enabled

Enable Video Plan

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

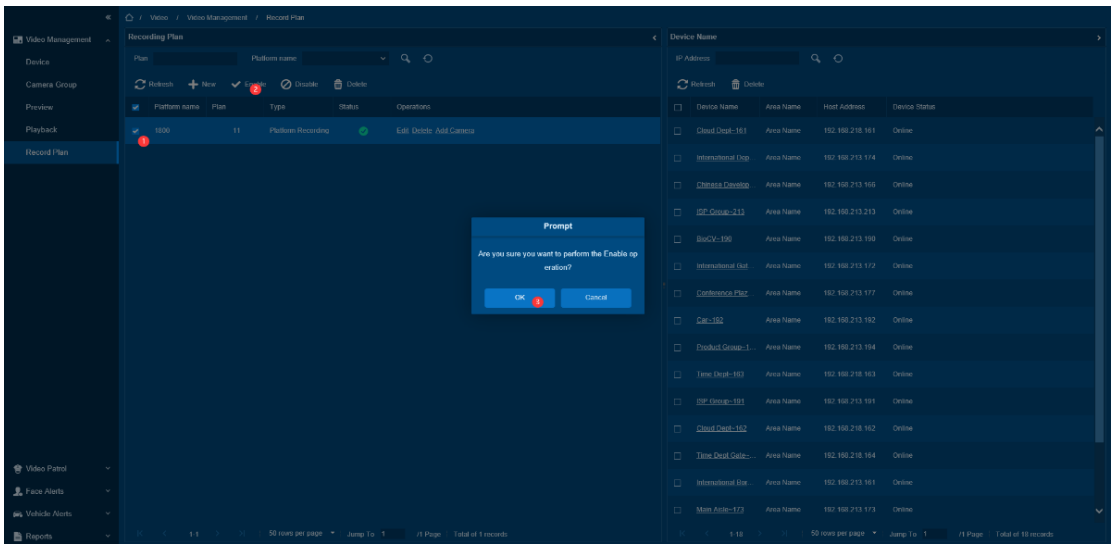
You need to enable the video recording function for the cameras in the Video Plan.

Feature Trigger Result

Operations	Description
Enable Video Plan	The cameras in the Video Plan will start the video recording function according to the set time and synchronously send the data on the configuration server.

Steps:

- Check the Video Plan to be activated in the plan list and click [**Enable**] button.
- Click [**OK**] button to complete the activation.



✍**Note:**

Cannot be activated when the device is offline.

Disable Video Plan

Preconditions for Normal Use of Function

For third-party integrated the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

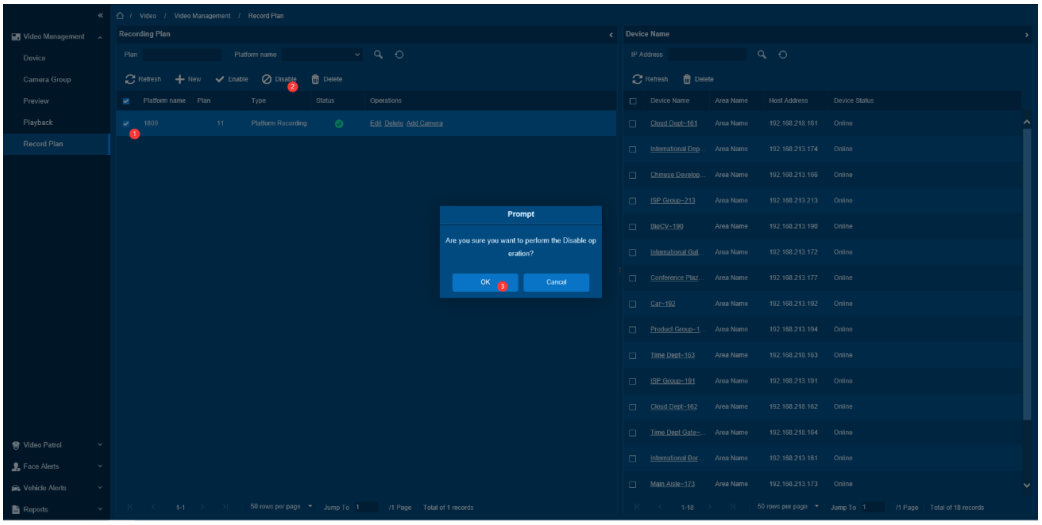
Temporarily stop the Video Plan of the camera within the scheduled time.

Feature Trigger Result

Operations	Description
Disable Video Plan	Stop the execution of the plan and stop the video recording function of the camera and synchronously send the data on the configuration server.

Steps:

- Select the Video Plan that needs to be disabled in the plan list and click [**Disable**] button.
- Click [**OK**] button to complete disabling.



Delete Video Plan

Preconditions for Normal Use of Function

For third-party integrate, the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

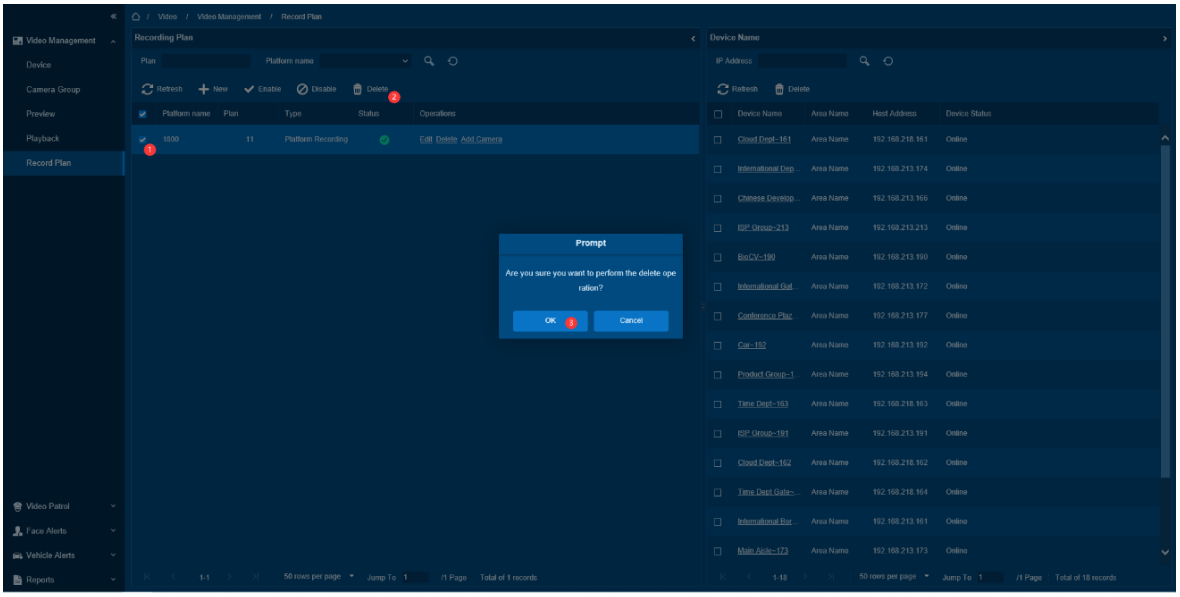
When the Video Plan is discarded and used, the Video Plan can be deleted.

Feature Trigger Result

Operations	Description
Delete Video Plan	Delete Video Plan and synchronize the data on the Delete configuration server.

Steps:

- Check the desired Delete Video Plan and click the [**Delete**] button.
- Click the [**OK**] button to complete Delete.



Modify Video Plan

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. Video Plan is disabled.

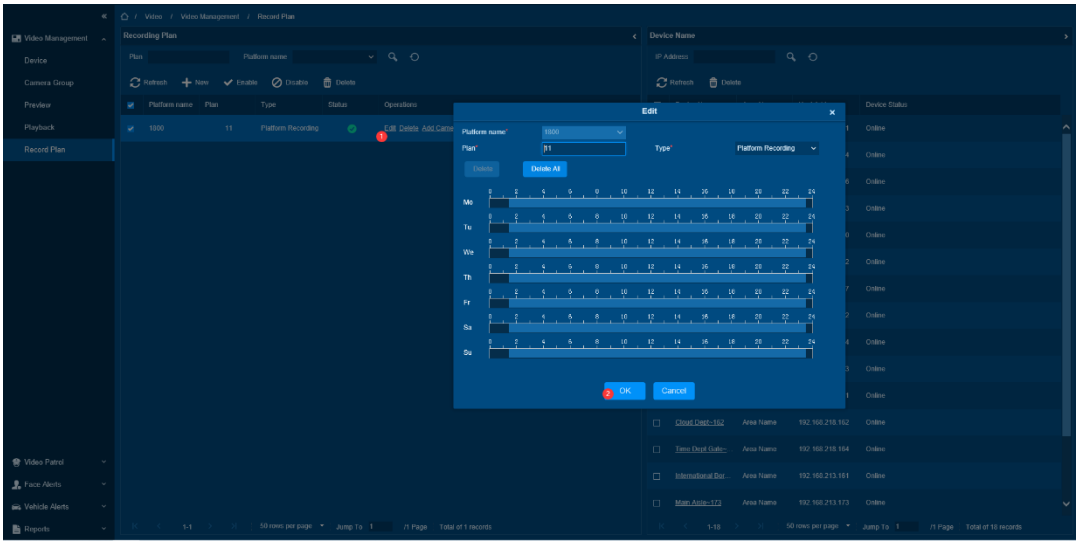
Function Usage Scenarios

Need to modify the time and name of the Video Plan.

Feature Trigger Result

Operations	Description
Modify Video Plan	Rearrange the Video Plan and synchronize the data on the configuration server.

By clicking [**Edit**] on the Video Plan list, the editing page pops up, and you can modify the name and type of the Video Plan.



Camera List in Video Plan

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

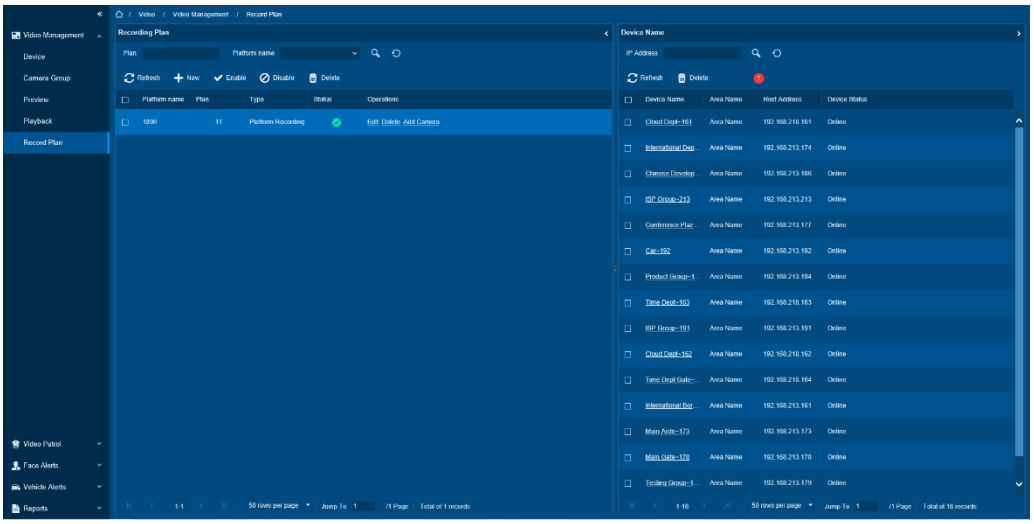
View the camera data in the Video Plan.

Feature Trigger Result

Operations	Description
Click on the Video Plan list	Display the camera data in the Video Plan

Steps:

- Enter the Page, the camera status in the first Video Plan is queried by default.
- You can also view the camera list data in the Video Plan by clicking on the Video Plan list.



Add Camera in Video Plan

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

Function Usage Scenarios

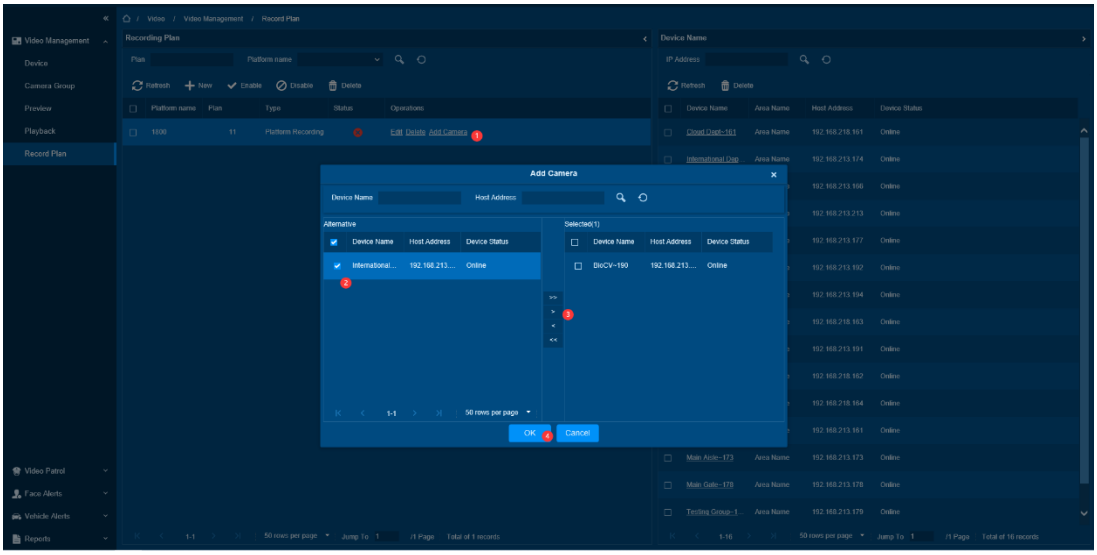
Need to add executed camera data to Video Plan.

Feature Trigger Result

Operations	Description
Add camera data to Video Plan	Add camera data to the Video Plan and synchronize the parameter configuration server to add camera data to the Video Plan.

By clicking [**Add Camera**] on the Video Plan list, the Add Camera window pops up, and you can add and

modify the cameras in the camera group on the window.



Delete Camera in Video Plan

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled.

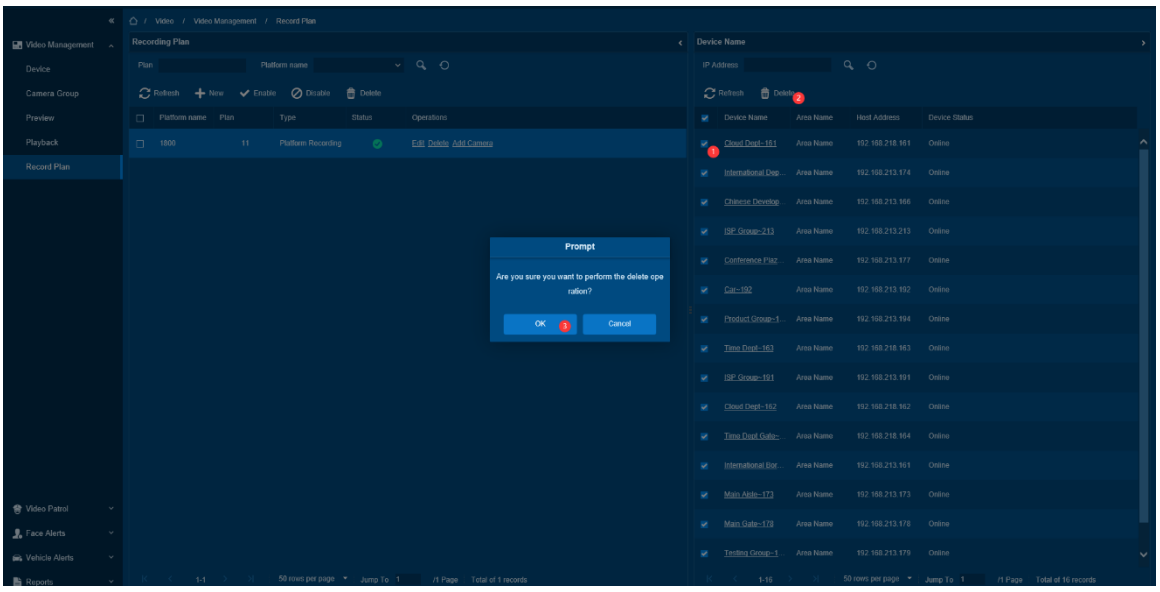
Function Usage Scenarios

When the camera in the Video Plan is discarded and used, the camera data can be deleted.

Feature Trigger Result

Operations	Description
Camera in Delete Video Plan	Cameras in the delete Video Plan and synchronize the parameter configuration server to the cameras in the Delete Video Plan.

On the Video Plan device page, check and select cameras in batches, click [**Delete**] above, and click [**OK**] to delete in batches.



11.2. Video Patrol

In this menu, you can check the punch-in by real-time preview of the camera remotely to achieve the same patrol task as the traditional punch-in effect.

Function List

Operations	Description
Patrol Group	Create a patrol group to add patrol personnel.
Patrol Plan	Assign a patrol plan to the Patrol Group.
Real-Time Patrol	Patrol personnel log in to the patrol account and can perform remote video patrols on this interface.

11.2.1. Patrol Group

Function Description

You can create patrol groups to distinguish between the task of different groups. You need to add patrol personnel in the group.

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View patrol group

Feature Trigger Result

Operations	Description

Enter the Page	Show patrol group list

Click the [**Patrol Group**] menu to enter the patrol group page as follows:

Add Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

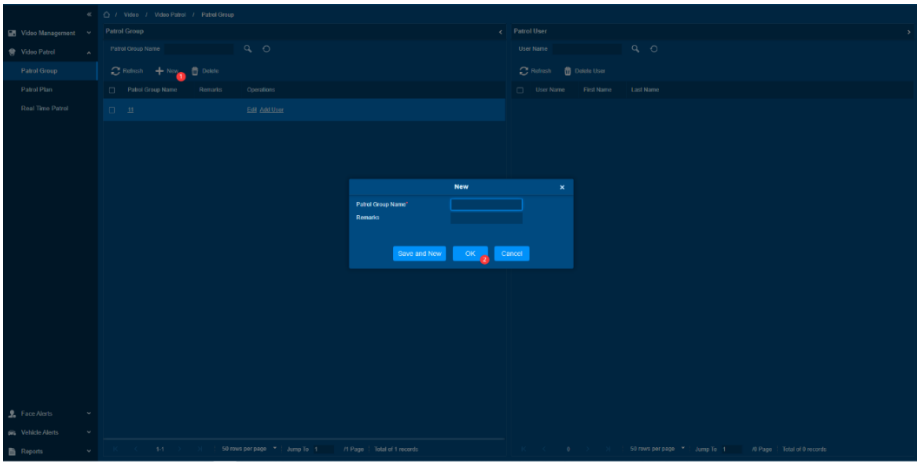
The patrol group needs to be created.

Feature Trigger Result

Operations	Description
Add Patrol Group	Create a patrol group record

Steps:

- Click [**Video Patrol**] > [**Patrol Group**] > [**Add**] to enter the add editing interface.
- Click [**OK**] to add patrol group.



Patrol Group Name: Enter the name of the patrol group for easy search and management. Not repeatable.

Remarks: Enter text remarks of the patrol group

Delete Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Need to delete the abandoned patrol group, delete the abandoned data.

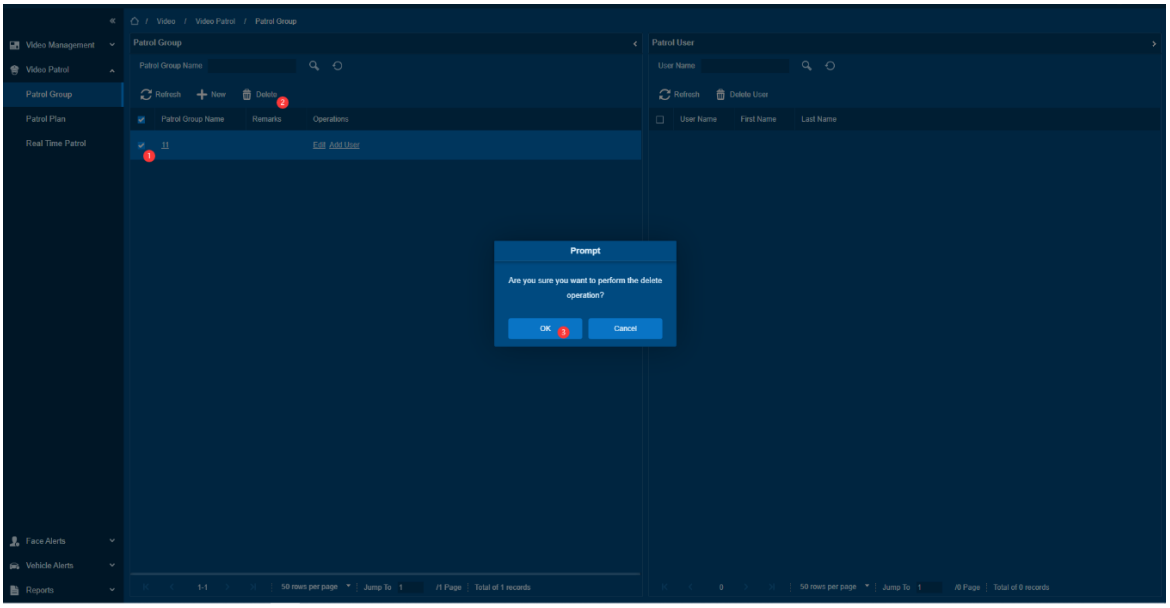
Feature Trigger Result

Operations	Description

Delete Patrol Group	Delete patrol group records

Steps:

- Check the user or user group in the group that needs to be deleted and click [**Delete**] button.
- Click [**OK**] to complete delete.



Edit Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

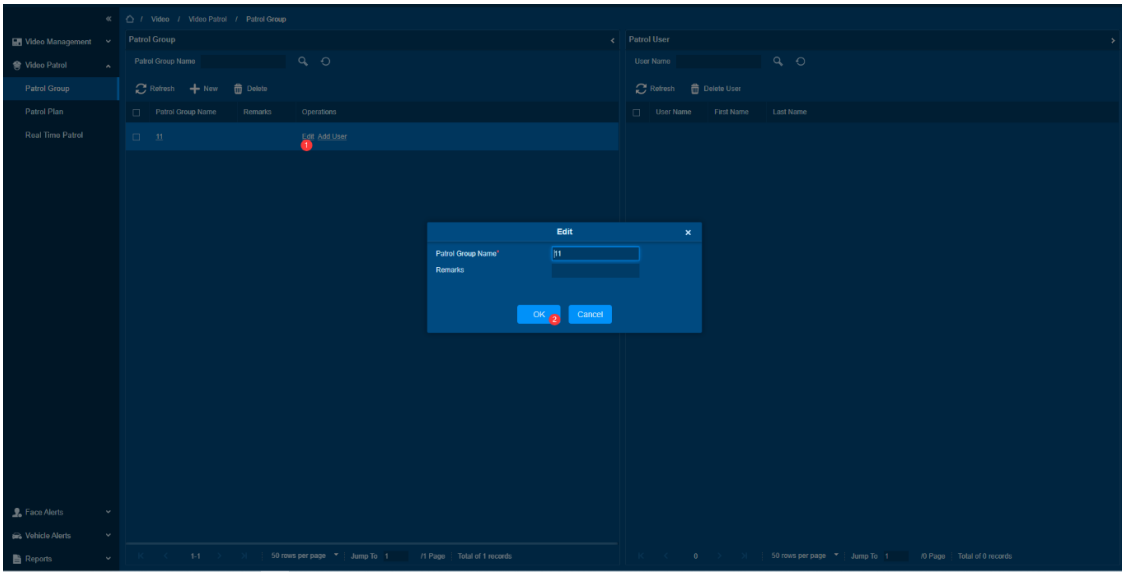
Need to modify the name and content of the patrol group.

Feature Trigger Result

Operations	Description
Edit Patrol Group	Modify the name and content of patrol group

Steps:

- Check the user or user group in the group that needs to be edited and click [**Edit**] button.
- Click [**OK**] to complete edit.



Add User in Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation group.

Function Usage Scenarios

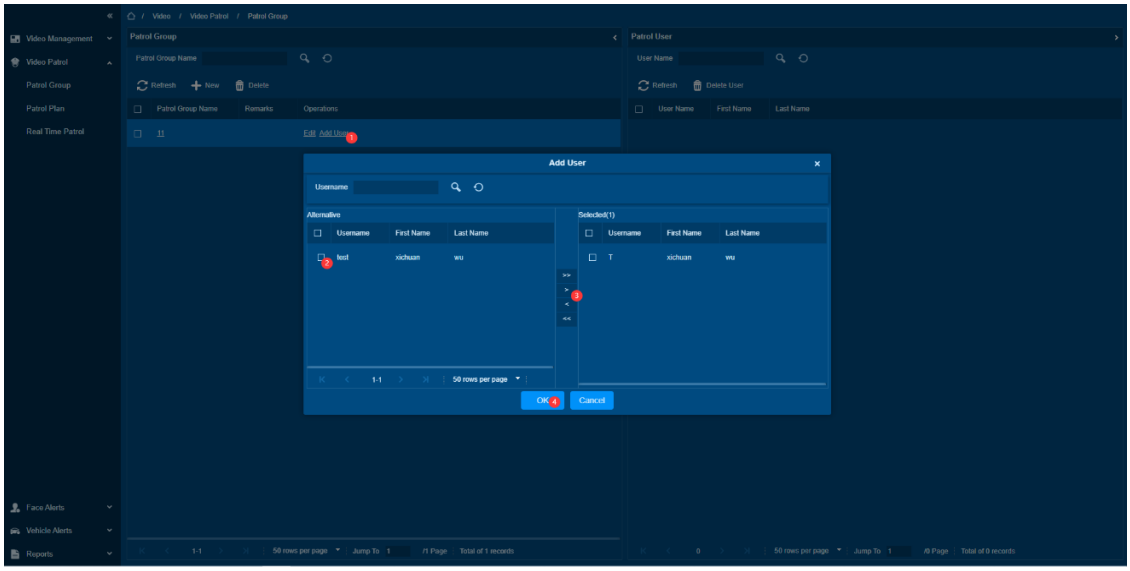
Need to add users to the patrol group.

Feature Trigger Result

Operations	Description
Add Users in Patrol Group	Add users in patrol group

Steps:

- Click [**Add Personnel**] in the list of patrol groups to enter and select to add group members.



- Select the required patrol user, click [**OK**] to complete the addition, and the added user will be displayed in the group member list on the right.

✍**Note:**

The patrol user is the user of the system. Please refer to add user.to add the user of the system.

User List in Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

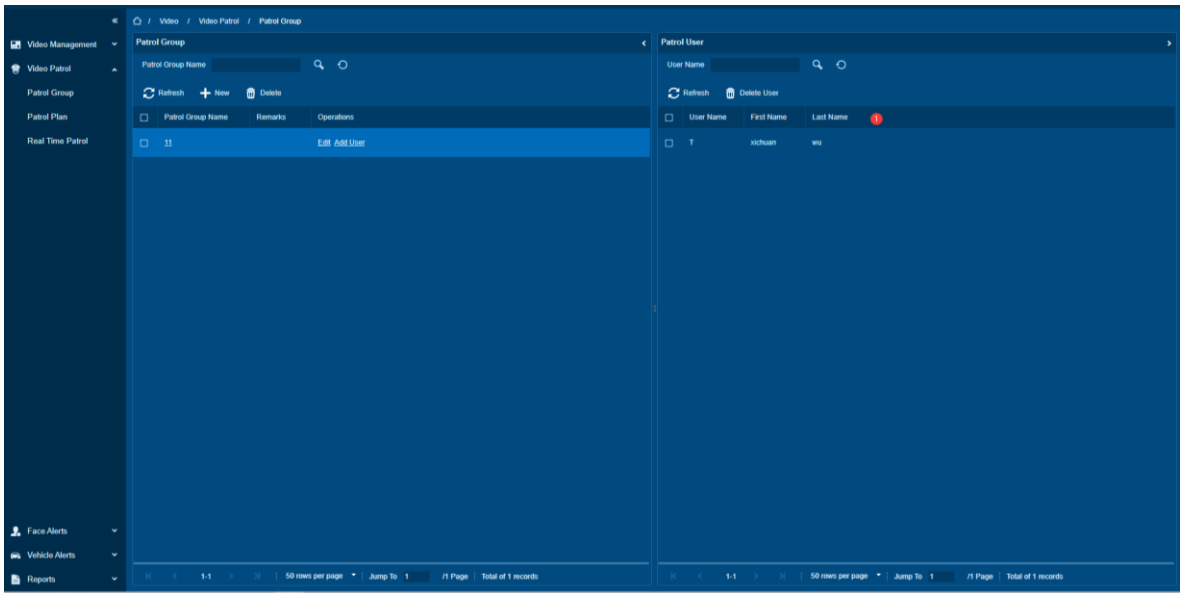
Need to check the users in the patrol group.

Feature Trigger Result

Operations	Description
Enter the Page	Display user data in patrol group

Steps:

- Enter the Page, the user list in patrol group is queried by default.
- You can also view the user list in the patrol group by clicking on the Patrol Group.



Delete User in Patrol Group

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

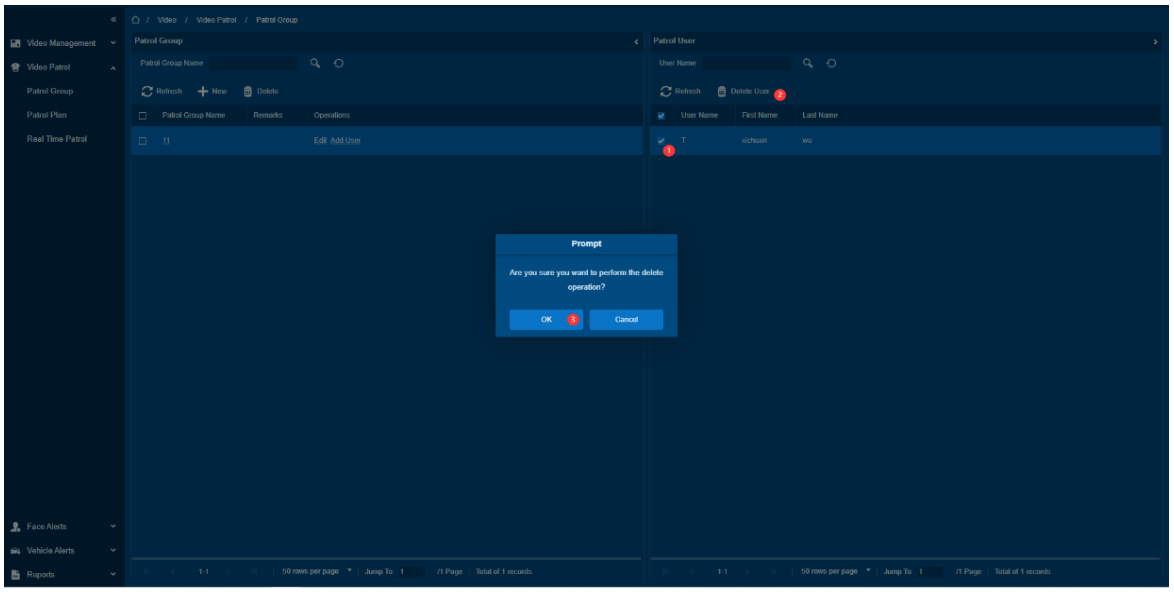
Function Usage Scenarios

Need to delete users in the patrol group.

Feature Trigger Result

Operations	Description
Delete Patrol Group Users	Delete user data in patrol group

Check the user or user group in the group that needs to be deleted and click [**Delete User**] button or the [**Delete**] button.



11.2.2. Patrol Plan

Function Description

Here you can set patrol plan(s) for the patrol groups.

Patrol Plan List

Preconditions for Normal Use of Function

The software runs normally, and the user has the permission of this page.

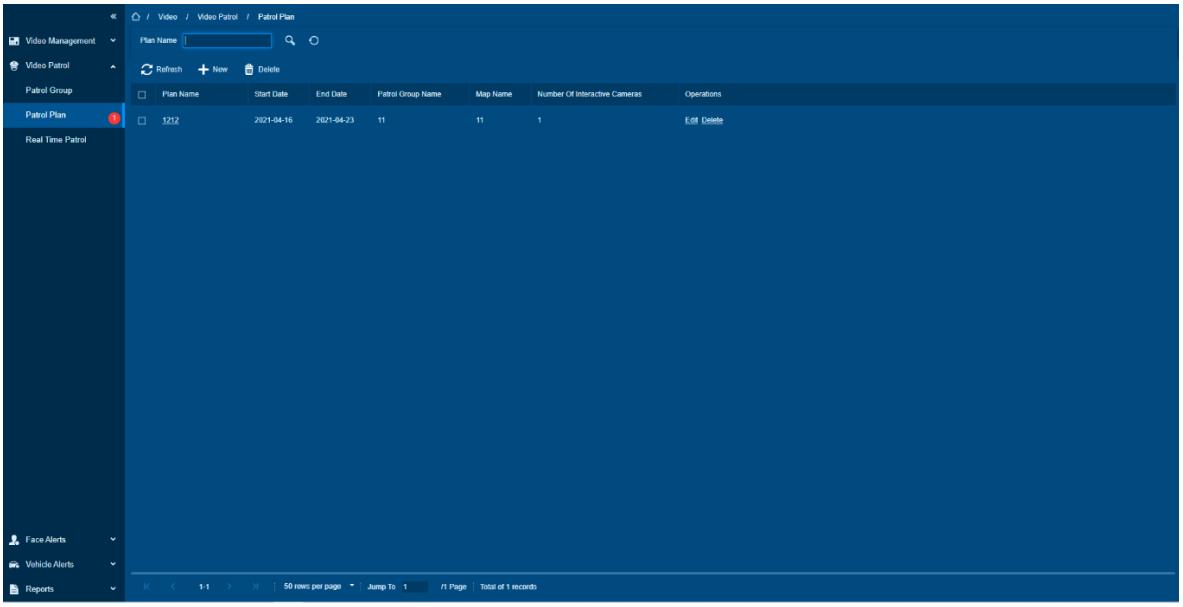
Function Usage Scenarios

Need to view the data list of patrol plan.

Feature Trigger Result

Operations	Description
View Patrol Plan	Display patrol plan data

Click the [**Patrol Plan**] menu to enter the patrol Plan page as follows:



Add Patrol Plan

Preconditions for Normal Use of Function

Need to configure a map and add camera device points.

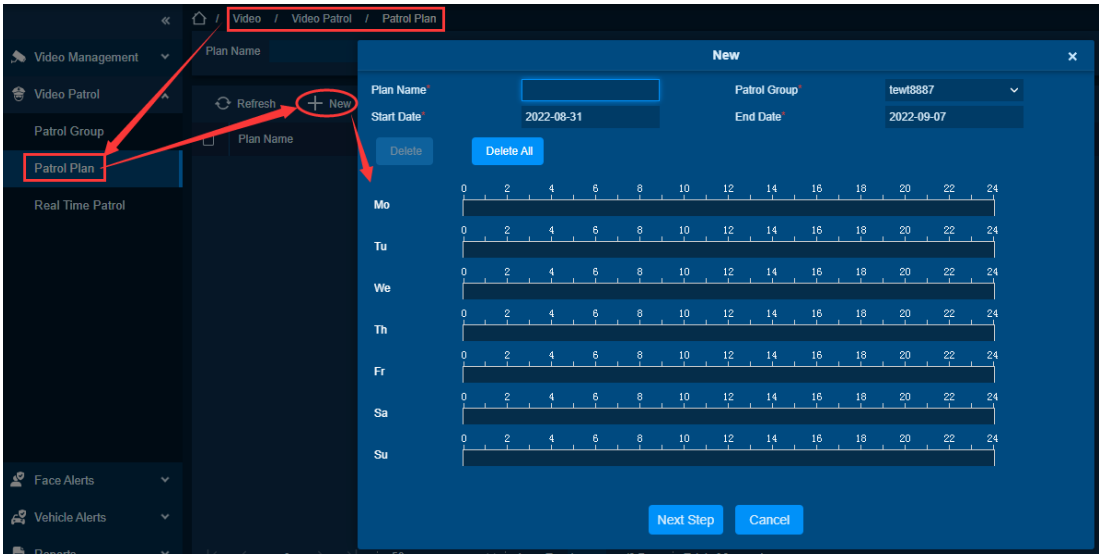
Function Usage Scenarios

Need to view the patrol plan on the map.

Feature Trigger Result

Operations	Description
Add Patrol Plan	Create and add patrol plan

Click [**Video Patrol**] > [**Patrol Plan**] > [**Add**] to enter the add editing interface.



The description is as follows:

Plan Name: Give the plan a name, which is convenient for checking and searching, and it would not be repeated.

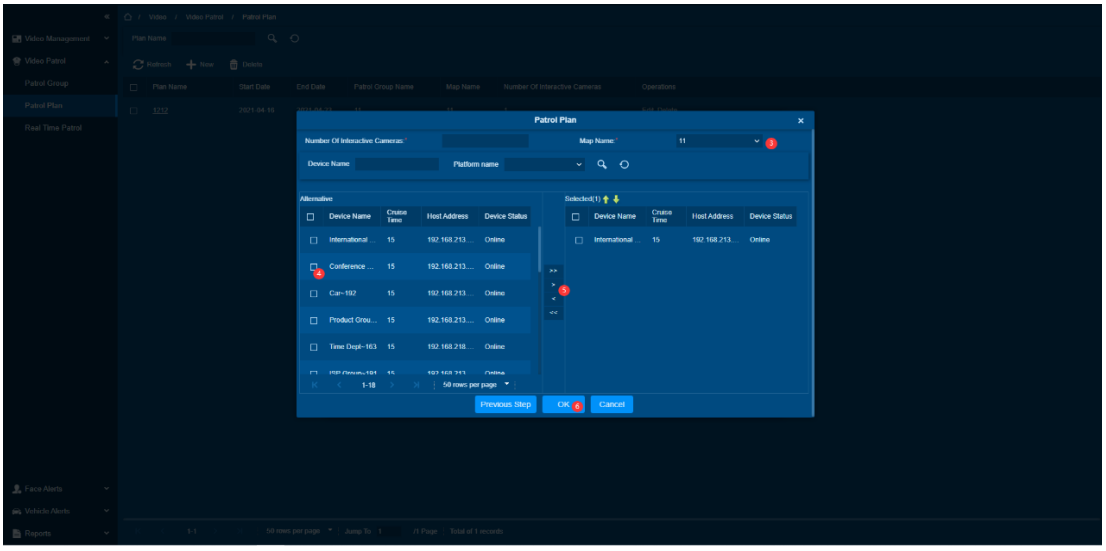
Patrol Group: Optional patrol group that has been created.

Start Date: Set the start date of the patrol, the start date shall not be less than the end date.

End Date: Set the end date of the patrol, the start date shall not be less than the end date.

Patrol Time: Drag on the time bar to select the Timetable that needs to be patrolled, and multiple copies are supported.

After finishing editing this page, click [**Next**] to enter the camera selection interface:



The number of cameras that need to be patrolled: The input value is the number of cameras that need to be clocked during the patrol; (for example, input "5" means that 5 cameras need to be clocked in during a patrol, and the camera that needs to be turned on is the system Randomly generated.), the input value should be less than or equal to the number of candidate cameras.

Map Name: Select the name of the added map. When you select a different map, the device list will display the camera devices that have been added on the different maps.

Camera device list: Add the selected camera to the list on the right, check a single camera device and click [] to adjust the order of the devices during patrol.

Click [**Patrol Duration**] to modify the time the camera needs to patrol to view the video.

✍**Note:**

The camera list only displays camera devices that have been added to the currently selected map. For adding camera devices, please refer to Adding a Camera.

After the setting is completed, click [**OK**] to complete the Add patrol plan.

Edit Patrol Plan

Preconditions for Normal Use of Function

Need to configure a map and add camera device points.

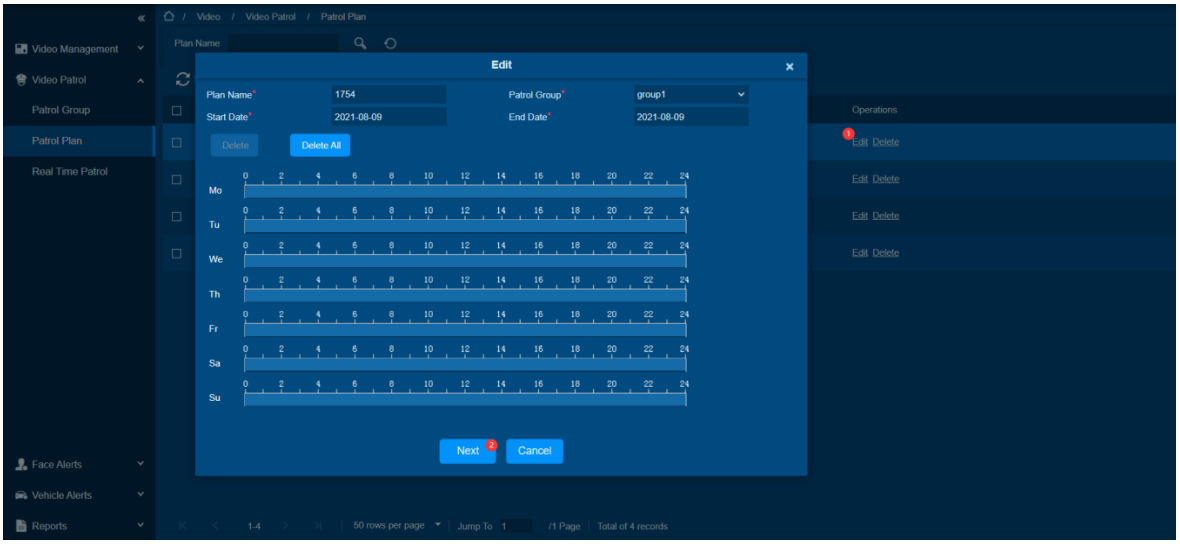
Function Usage Scenarios

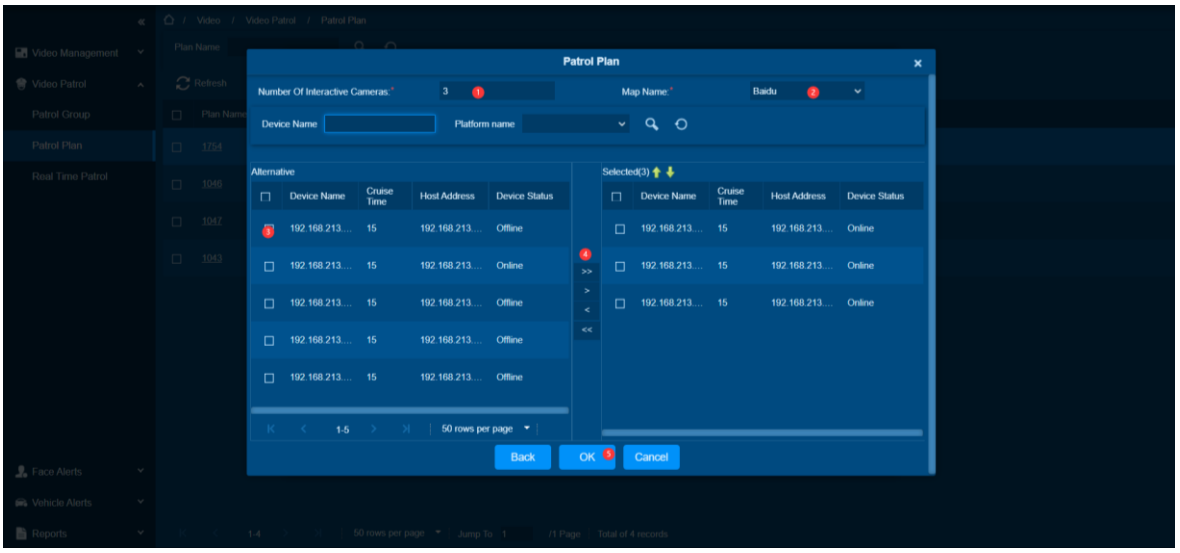
It is necessary to make changes to the created patrol plan.

Feature Trigger Result

Operations	Description
Edit Patrol Plan	Change the content of the patrol plan

Steps:





Delete Patrol Plan

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

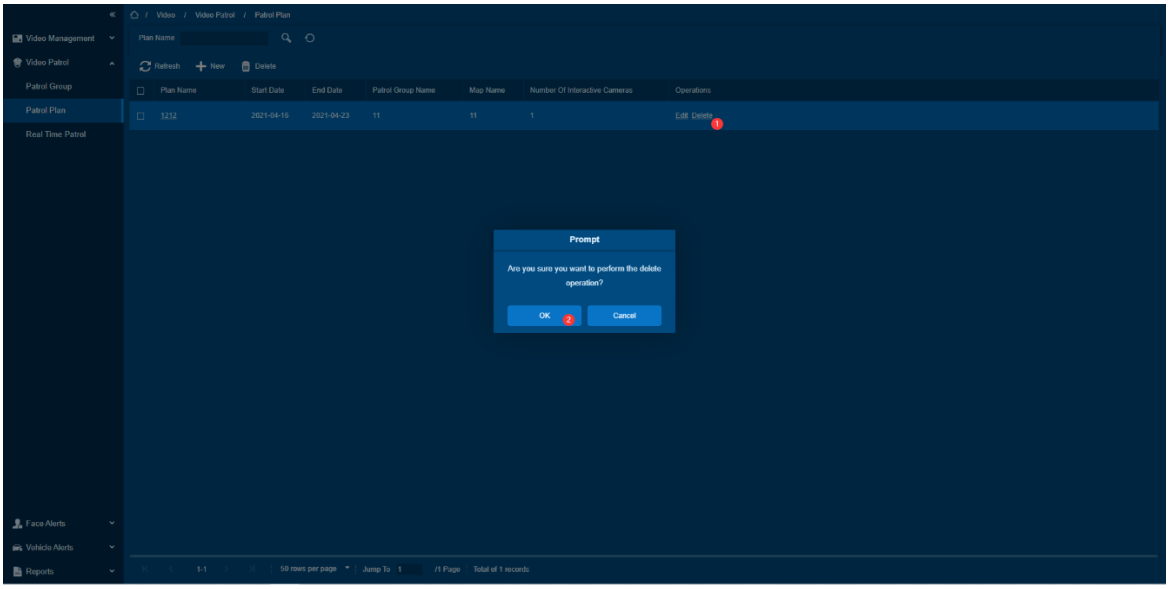
Need to delete the unused patrol plan.

Feature Trigger Result

Operations	Description
Delete Patrol Plan	To delete the patrol plan

Steps:

- Check the need to delete the patrol plan and click [**Delete**].
- Click [**OK**] to delete.



11.2.3. Real-Time Patrol

Function Description

In the Real-time Patrol, you can check all the patrol operations. Online patrols are only available if the patrol stuff logged into the system.

Video Operation

Preconditions for Normal Use of Function

The patrol plan must be set up in advance.

Function Usage Scenarios

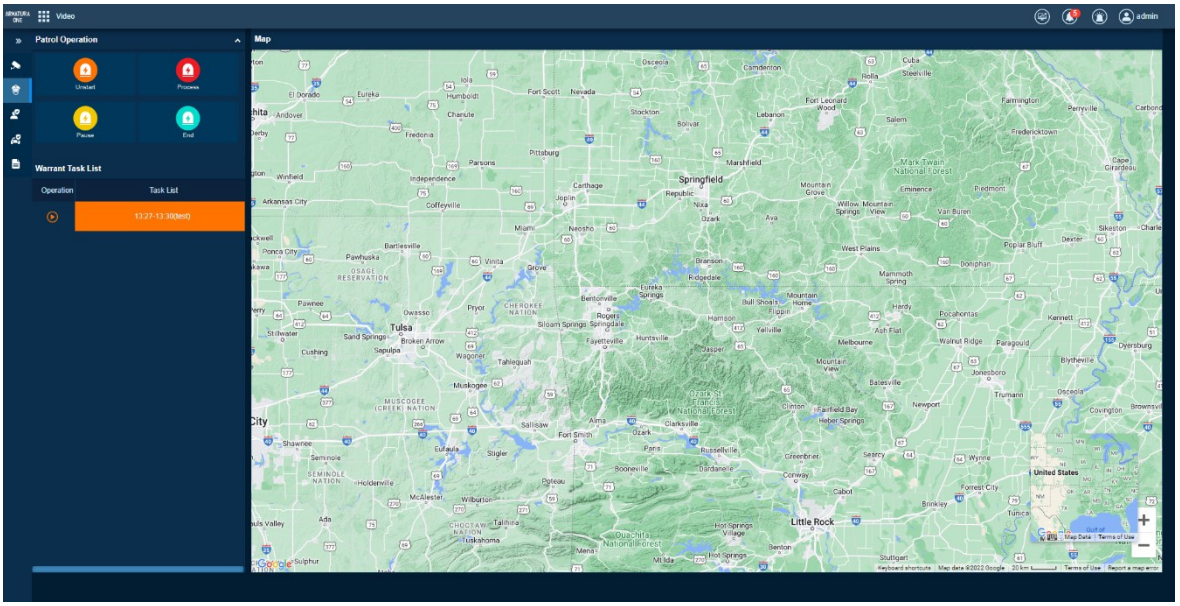
Need to check the classification statistics of the set patrol plan.

Feature Trigger Result

Operations	Description

Click the Corresponding Process Icon	The patrol plan under the corresponding progress is displayed

Patrol Status Display Panel: The patrol states are distinguished by different colors, such as not started, in progress, paused and ended; click different states to switch the task list to display different patrol tasks.



Patrol Task List

Preconditions for Normal Use of Function

The patrol plan created by the data source cannot be executed by the super administrator. It must be a user in the patrol group to execute the plan.

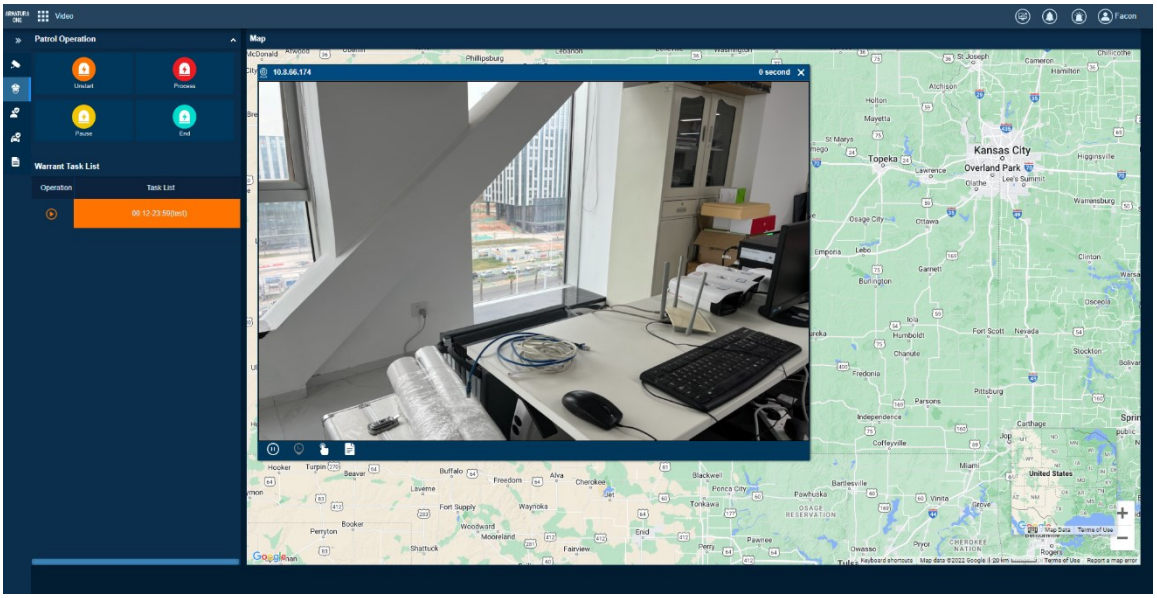
Function Usage Scenarios

Need to view the current patrol mission data.

Feature Trigger Result

Operations	Description
Click to Perform Patrol Mission	A video window pops up on the map page, and the video data is played in sequence.

Task List Panel: Display the task; click [**Patrol**] to start the current patrol.



Map

Preconditions for Normal Use of Function

For third-party integrated, the parameter configuration must be properly connected and enabled. The video player plug-in must be downloaded for the first use, and the browser must be restarted after installation. Currently only the i.e., browser is supported.

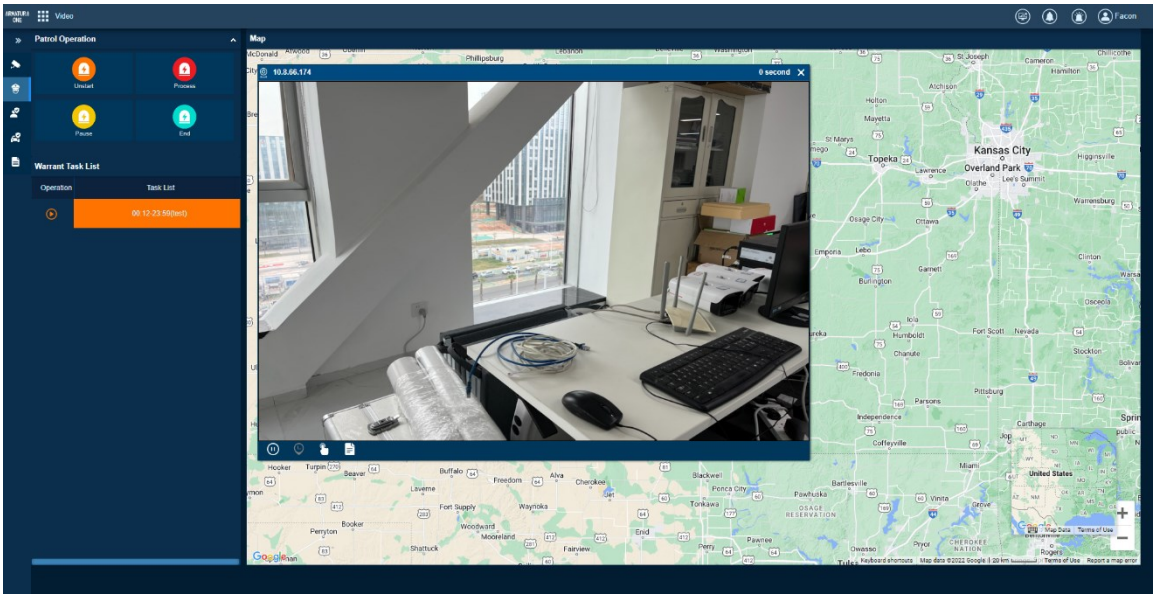
Function Usage Scenarios

It is necessary to perform the patrol plan on the playback device of the patrol plan.

Feature Trigger Result

Operations	Description
Video Play	Carousel processing of the patrol video for 15 seconds

Map Patrol Panel: The map and camera device and the patrol path are displayed. The “red dot” indicates that the current camera is in patrol status.



Video Window: The patrol countdown is displayed in the upper right corner, and the patrol personnel must complete the patrol action within the countdown, and automatically switch to the next patrol camera when the countdown ends.

Pause Button: Pause the current patrol task.

Sign in Button: Sign into the current device. When the button is always bright and flashing, it means that the device needs to sign in. When it is grey, it means no sign in. The sign in setting refers to the patrol plan setting.

Report Alarm Button: When an abnormal situation is found, click this button to report the abnormal situation.

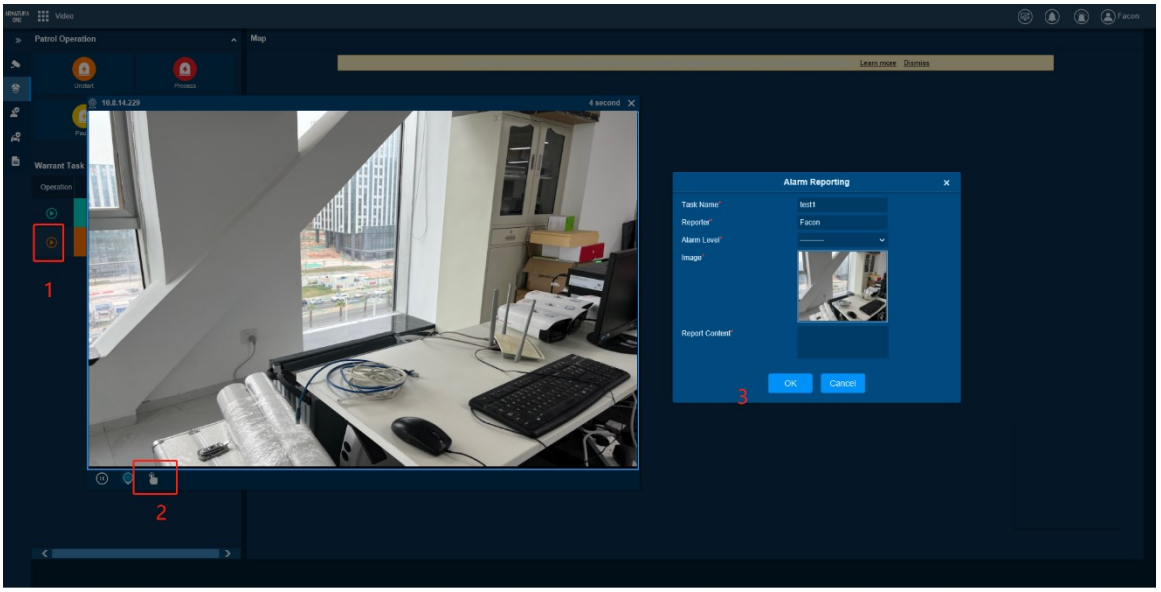
Task Name: Set the name of the current patrol task.

Recording Personnel: The patrol personnel currently logged in.

Alarm Level: You can choose whether the report is important or not, and the record will be synchronized with the alarm center.

Photos: When you click the camera, it will automatically capture the screen or manually click to upload photos.

Report Content: Set the Text remarks.

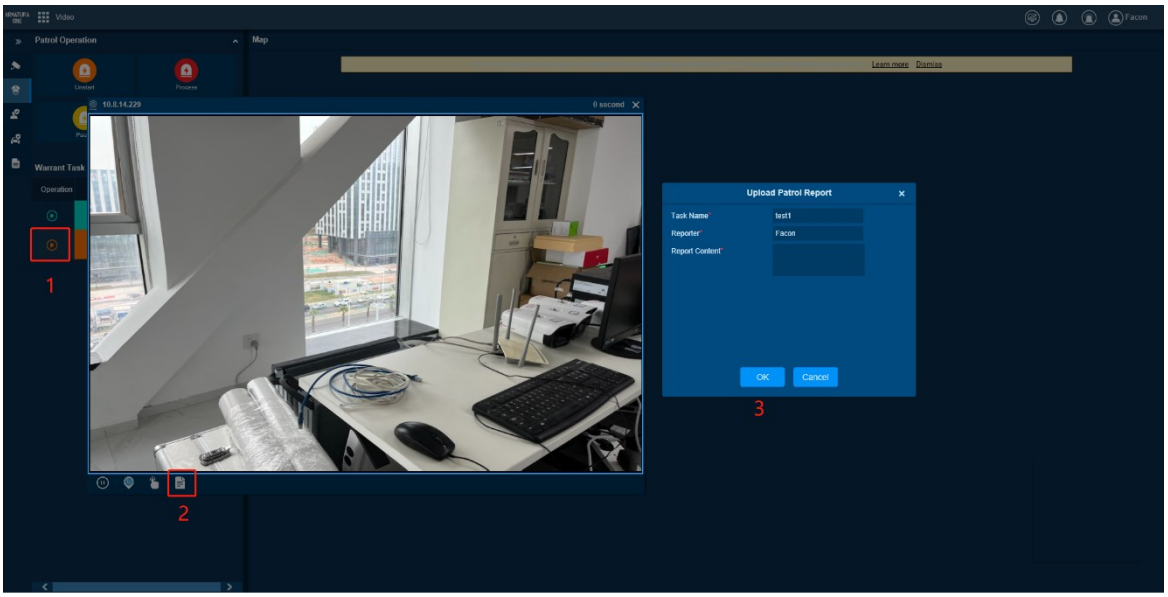


After the video patrol is over, click [**Upload Patrol Report**] button to complete the patrol.

Task Name: Select the name of the current patrol task.

Recording Personnel: Select the patrol personnel currently logged in.

Report Content: Text remarks.



Completed patrol tasks are automatically switched to the completed state in the patrol task list.

11.3. Report

Function List

Operations	Description

Video Event Recording	View the related records of video device snapshots and videos.
Camera Alarm Record	View all video device alarm records, manually add, and export alarm records.
Patrol Report	View the patrol records of the patrol staff.
Patrol Warning	View the police information reported during the patrol.

11.3.1. Video Event Recording

Function Description

In this menu, view related records of video equipment's snapshots and videos.

Video Event Recording List

Preconditions for Normal Use of Function

The equipment has production snapshot data.

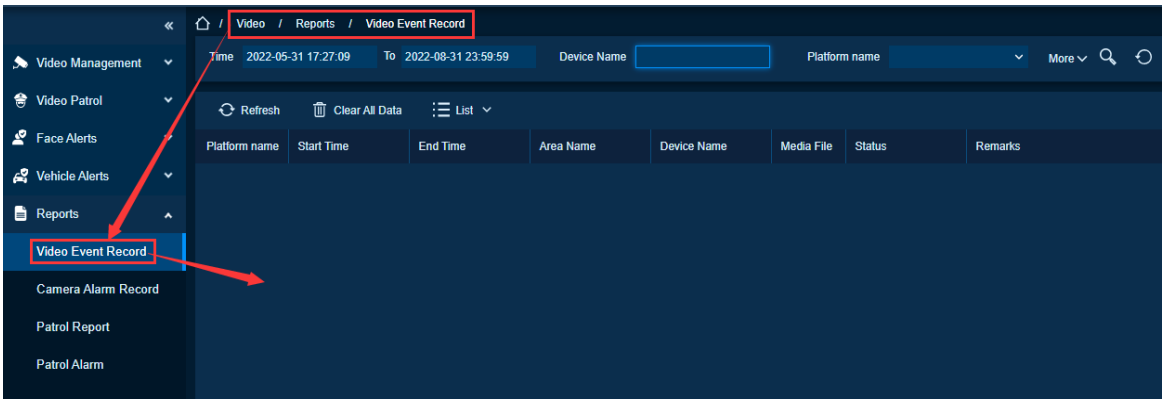
Function Usage Scenarios

Need to query Video Event Recording data.

Feature Trigger Result

Operations	Description
Enter the Page	Display video event recording data.

View the related records of video device snapshots and videos.



Introduction of media file classification:

: Indicates that in the Linkage setting of access control or elevator control, the selected video Linkage type is "Recording". Click to download the video file.

: Indicates that in the Linkage setting of access control or elevator control, the selected video Linkage type is "photograph". Click to preview the image file.

Note:

If you select “Video” and “Photograph” at the same time, two different records will be generated. For the specific setting method, please refer to Linkage setting and Global Linkage above.

11.3.2. Patrol Report

Function Description

View the patrol records of the patrol staff.

Patrol Report

Preconditions for Normal Use of Function

There are patrol records generated.

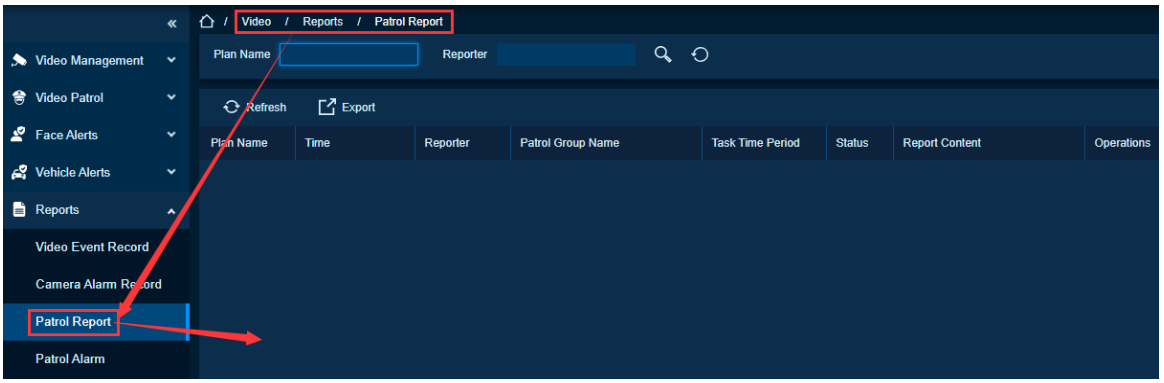
Function Usage Scenarios

Need to query the patrol record data.

Feature Trigger Result

Operations	Description
Enter the Page	Display patrol record data

Click **[Patrol Report]** button to view the detailed information of the patrol personnel



Report information

Check the name of the patrol plan; patrol personnel; belong to the patrol group; patrol plan time; patrol status; patrol remarks and other information.

Capture photos

To view the photo information captured during the patrol, click to view the larger image.

Camera information

Check the patrol time of each camera; the clocking status of the camera, whether to play playback and other information.

Alarm information

View the alarm content and text remarks reported during the patrol process.

11.3.3. Patrol Warning

Function Description

View the police information reported during the patrol.

Patrol Warning

Preconditions for Normal Use of Function

There are patrol warnings.

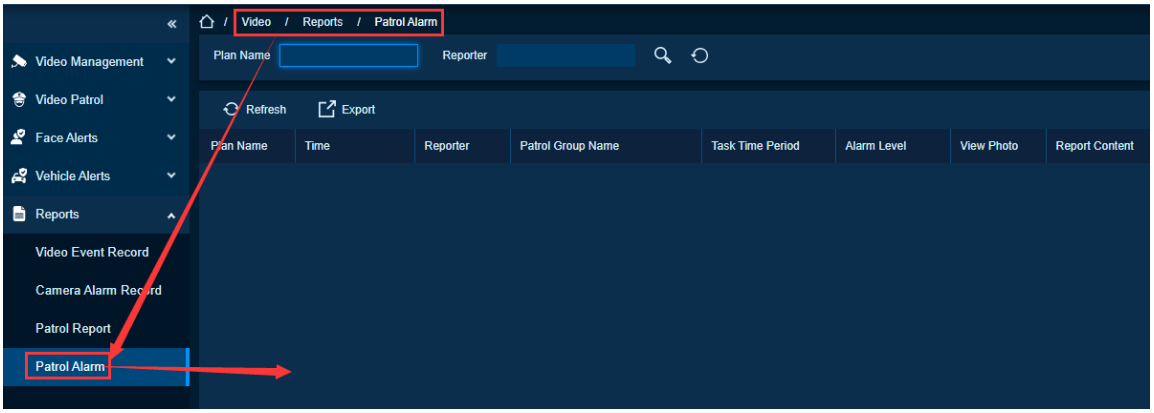
Function Usage Scenarios

Need to query patrol warning data.

Feature Trigger Result

Operations	Description
Enter the Page	Display patrol warning data

Click [ ] button to view the alarm snapshot picture.



12. Office Module

The Office Module is a space management module where you can manage and configure your meeting room, check the status of the meeting room, make reservations, and view the meeting. Once you reserve a meeting room, it will be automatically associated to the corresponding PAD device, and personnel rights will be immediately issued to the PAD for verification.

12.1. Facility Management

Office Management is used to manage corporate public spaces, such as meeting rooms, workstations, etc., to create shared spaces, maintenance reporting and approval procedures, and query space usage records, etc.

Function List

Operations	Description
Meeting Room	Create and manage meeting room
Shared workstation	Create and manage shared workstation

12.1.1. Meeting Room

Function Description

It creates and manage meeting room.

Meeting Room List

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

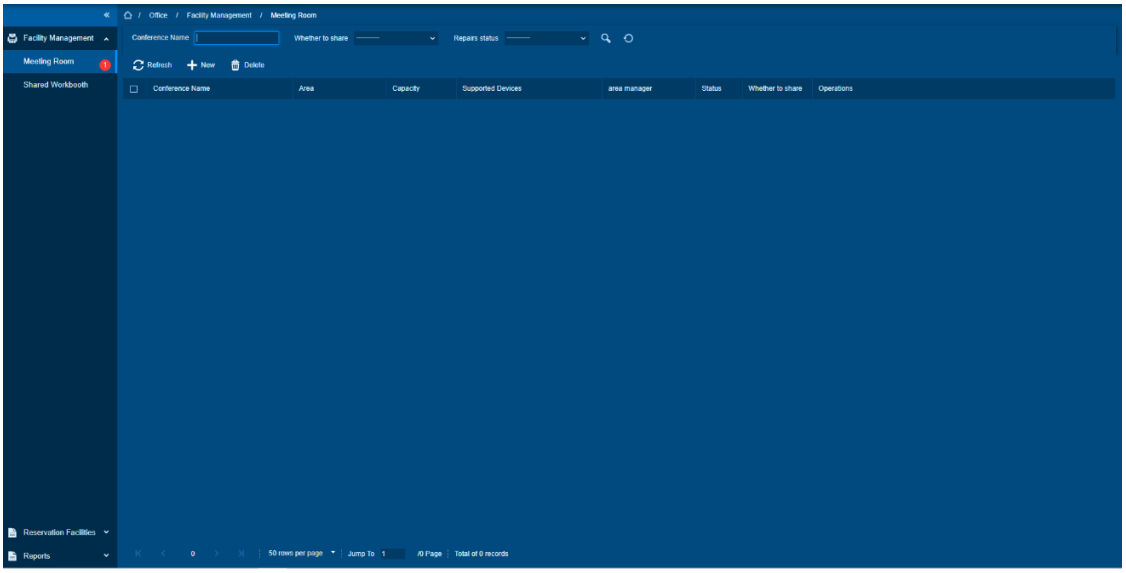
Function Usage Scenarios

View current Meeting Room data.

Feature Trigger Result

Operations	Description
Enter the Page	View meeting room data

Click **[Facility Management] > [Meeting Room]** to view meeting room Interface.



Add Meeting Room

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

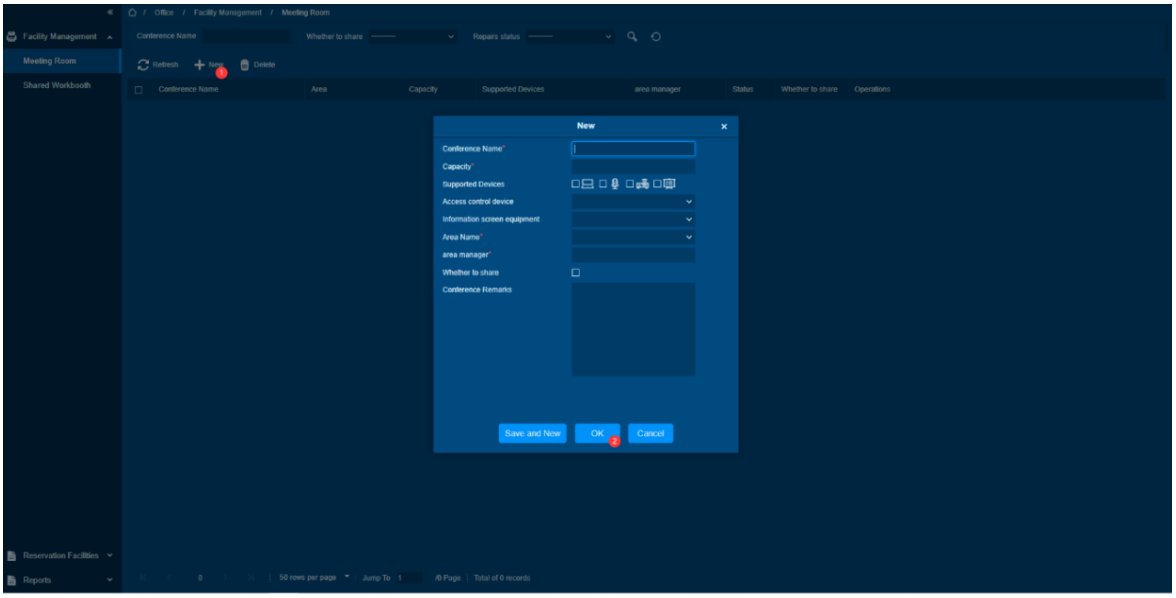
Function Usage Scenarios

Need to create a Meeting Room.

Feature Trigger Result

Operations	Description
Add Meeting Room	Add meeting room

Click **[Meeting Room]** > **[Add]** to enter the Add editing interface.



The description is as follows:

Meeting Room name: Set the name of the Meeting Room for easy reference and cannot be repeated.

Meeting Room Capacity: Set the capacity of the Meeting Room and display the size of the meeting room.

Support equipment: Set the equipment included in the meeting room.

Access control device: Set the access control device of Linkage. When the meeting room is reserved, only the person who made the appointment and the participant has the right to open the door.

Whether to share: Open, visitors can also reserve the meeting room.

Meeting Room remarks: Add text remarks.

Delete Meeting Room

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

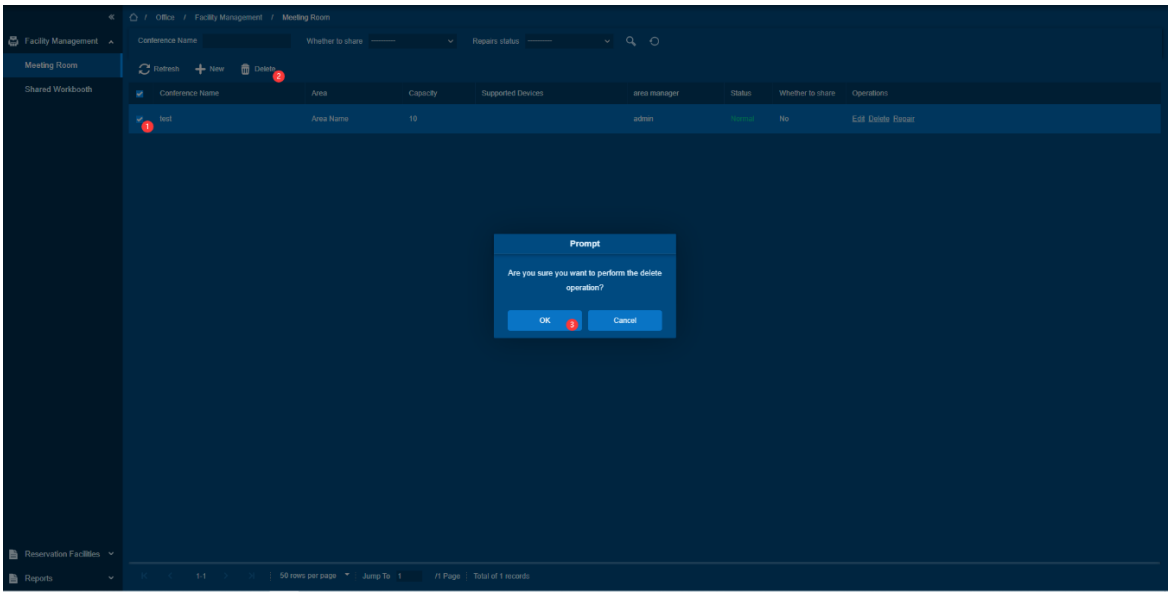
Need to discard a Meeting Room. This Delete the Meeting Room.

Feature Trigger Result

Operations	Description
Delete Meeting Room	Delete corresponding meeting room

Steps:

- Check the meeting room that needs to be deleted, and click the [**Delete**] button:
- Click [**OK**] button to complete the delete meeting room.



Meeting Room Repairs

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

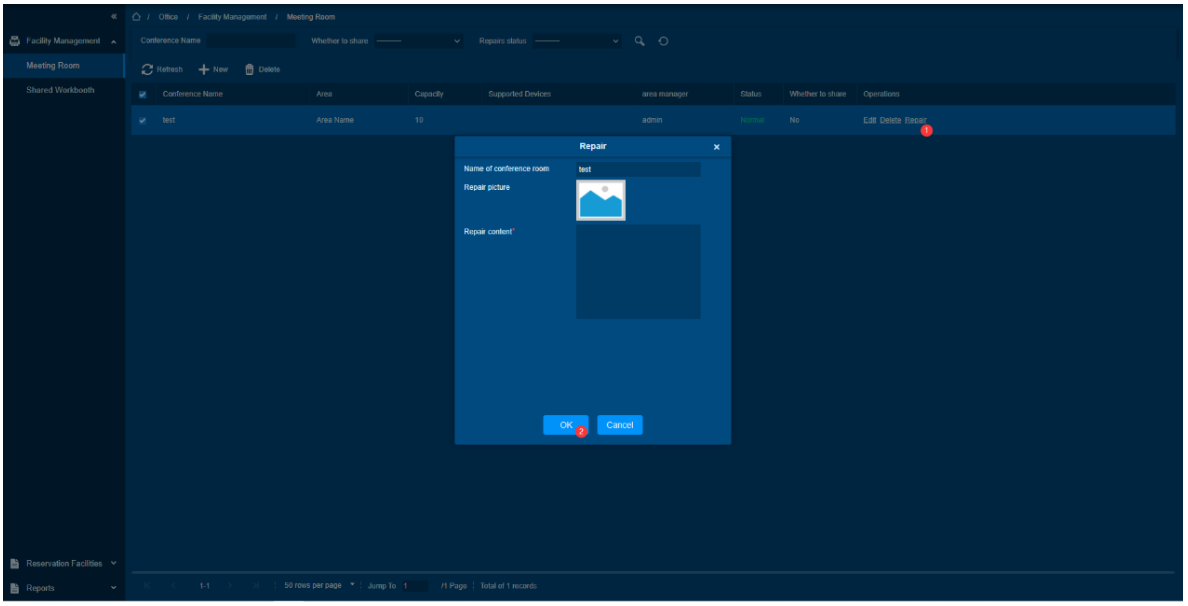
The Meeting Room is out of order and cannot be used.

Feature Trigger Result

Operations	Description
Meeting Room Repair	Report the corresponding meeting room for repairs.

Steps:

- Check the meeting room that needs to be repair and click the [**Repair**] button.
- Click [**OK**] button to complete the repair meeting room.



12.1.2. Shared Workstation

Function Description

When using this management system, you need to register personnel in the system, or import personnel from other software or documents into the system by way of importing, and you can set the authority of the personnel corresponding to the module.

Shared workstation List

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

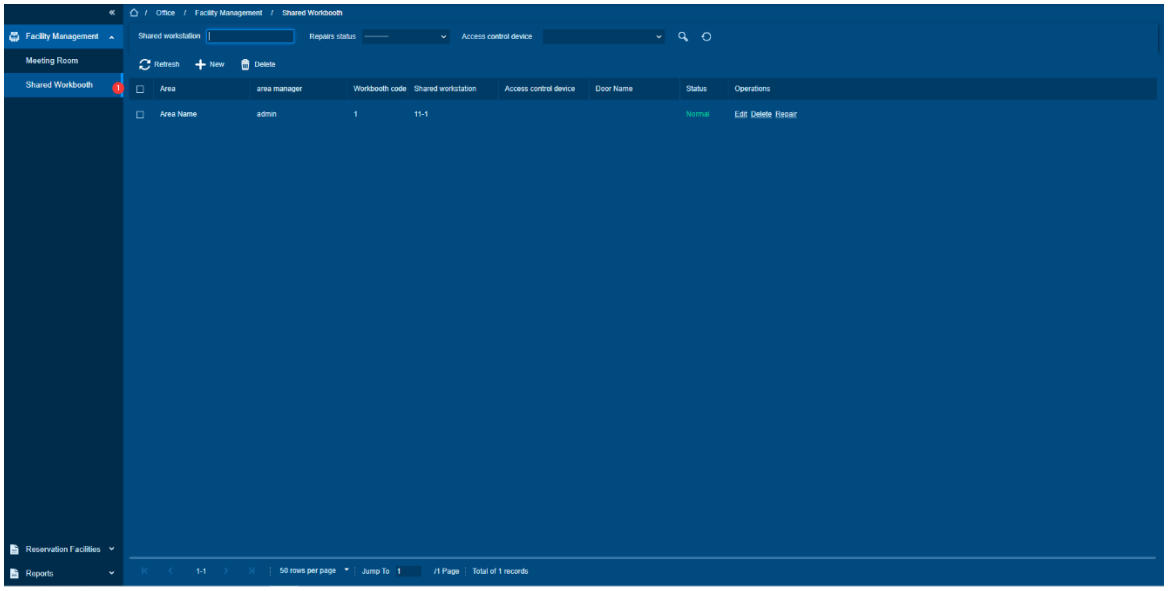
Function Usage Scenarios

View current station data.

Feature Trigger Result

Operations	Description
Enter the Page	View shared workstation data

Click [**Facility Management**] > [**Shared Workstation**] to view shared workstation Interface.



Add Shared Workstation

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

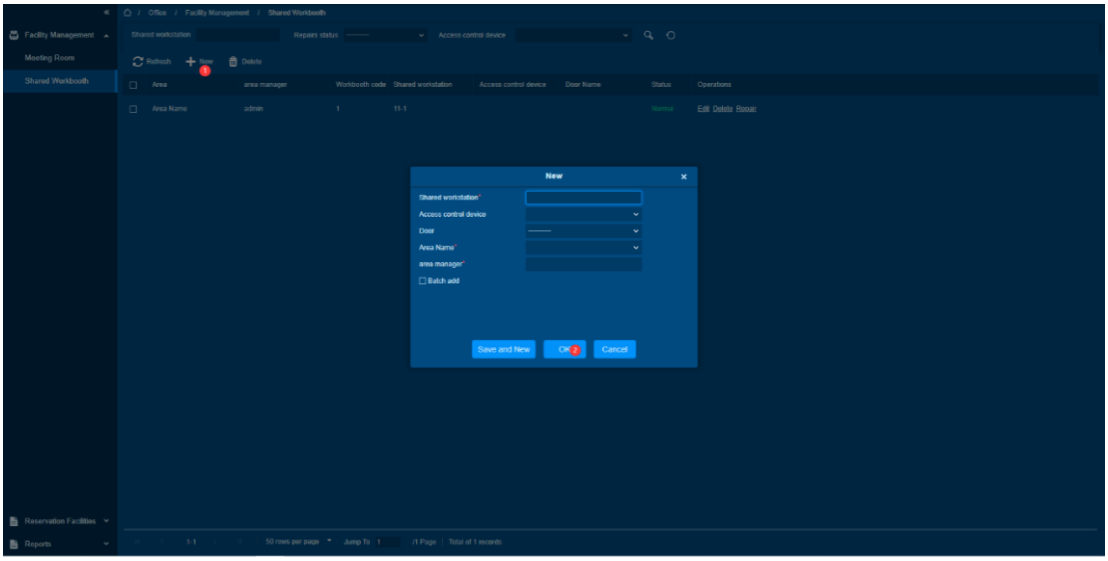
Need to create a shared workstation.

Feature Trigger Result

Operations	Description
Add Shared Workstation	Add a Shared workstation

Steps:

- Click [**New**] to add a new Workstation.
- Click [**OK**] to complete added.



Delete Shared workstation

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

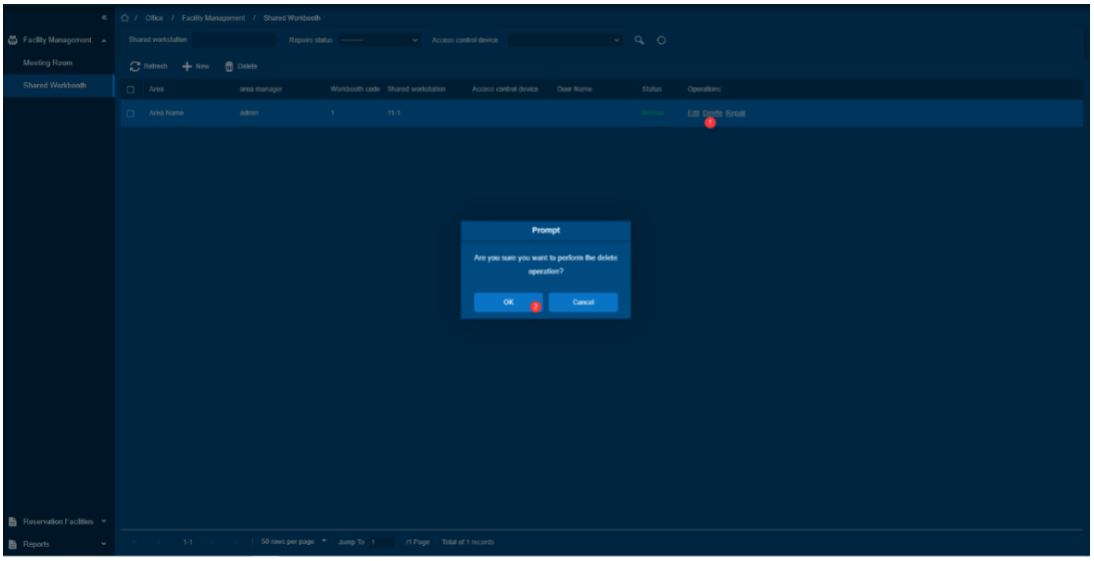
If you need to discard a shared workstation, delete the shared workstation.

Feature Trigger Result

Operations	Description
Delete Shared workstation	Delete station data

Steps:

- Select the area that needs to be deleted, and click the [**Delete**] button, or the [**Delete**] button under operation.
- Click [**OK**] to complete operation**.**



Shared workstation Repairs

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

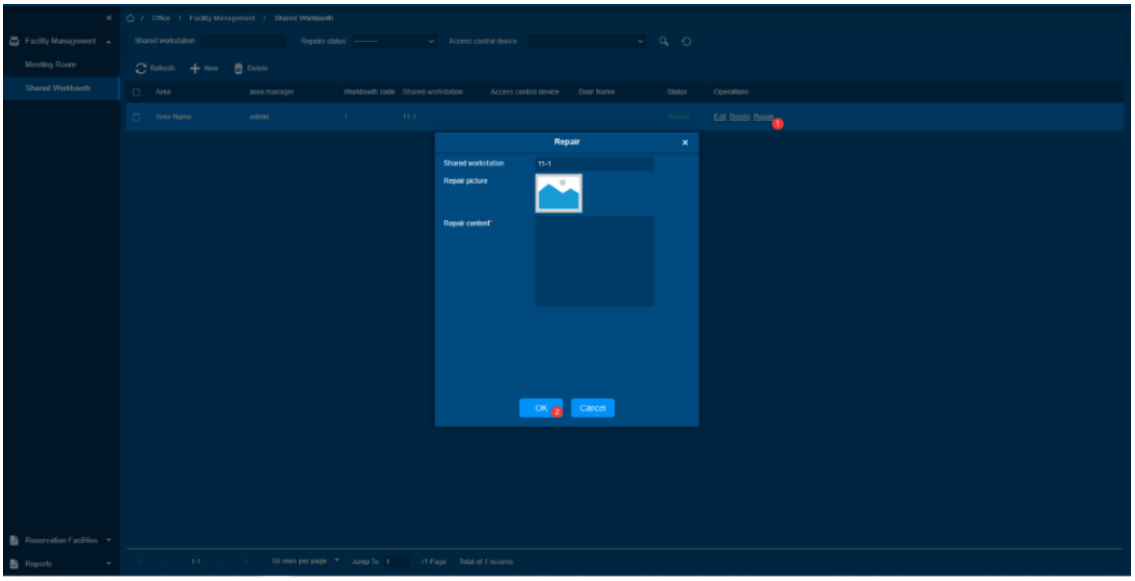
Function Usage Scenarios

The workstation cannot be used if it fails.

Feature Trigger Result

Operations	Description
Workstation repair	Report the corresponding station for repair.

Steps:



12.2. Reservation Facilities

Function List

Operations	Description
Meeting Room Reservation	Check the meeting room reservation status, and make a meeting room reservation

12.2.1. Reserve

Function Description

- Check the meeting room reservation status and make a meeting room reservation.
- Click on the time above and choose to view the meeting room status on different dates.

Meeting Room Reservation List

Preconditions for Normal Use of Function

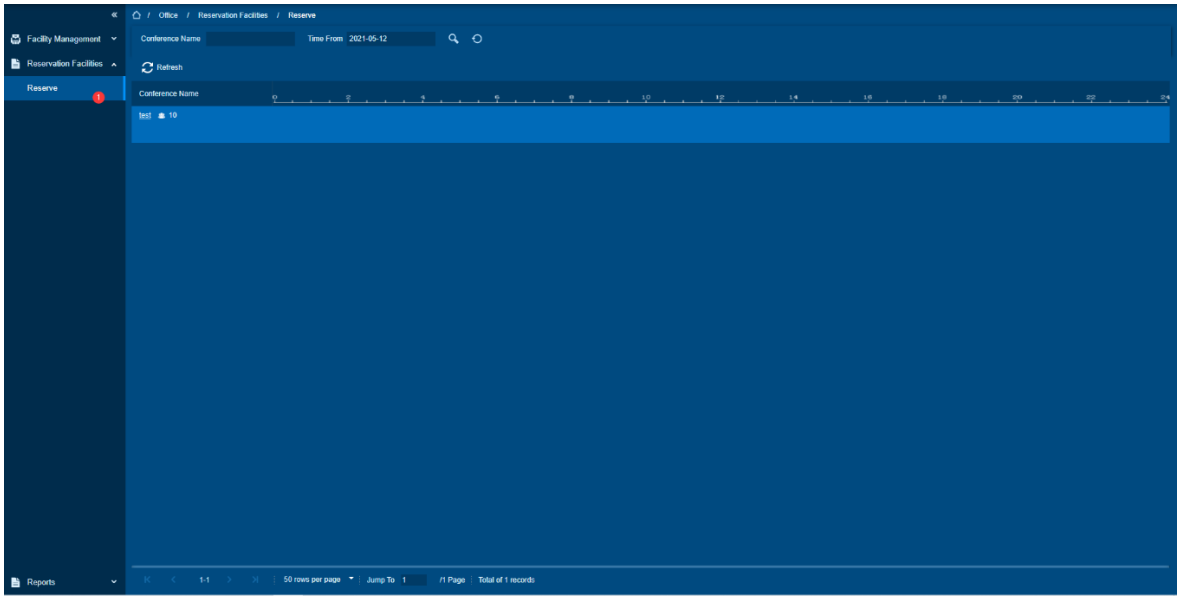
The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

Need to view meeting details.

Feature Trigger Result

Operations	Description
Enter the Page	Show Meeting Room data within the current time



State Description of Meeting Room:

- The Gray status of the scheduled meeting indicates that the meeting has ended or expired.
- The Green status of the scheduled meeting indicates that the meeting has not yet started.
- The Red status of the scheduled meeting indicates that the meeting is in progress.

Meeting Room Reservation

Preconditions for Normal Use of Function

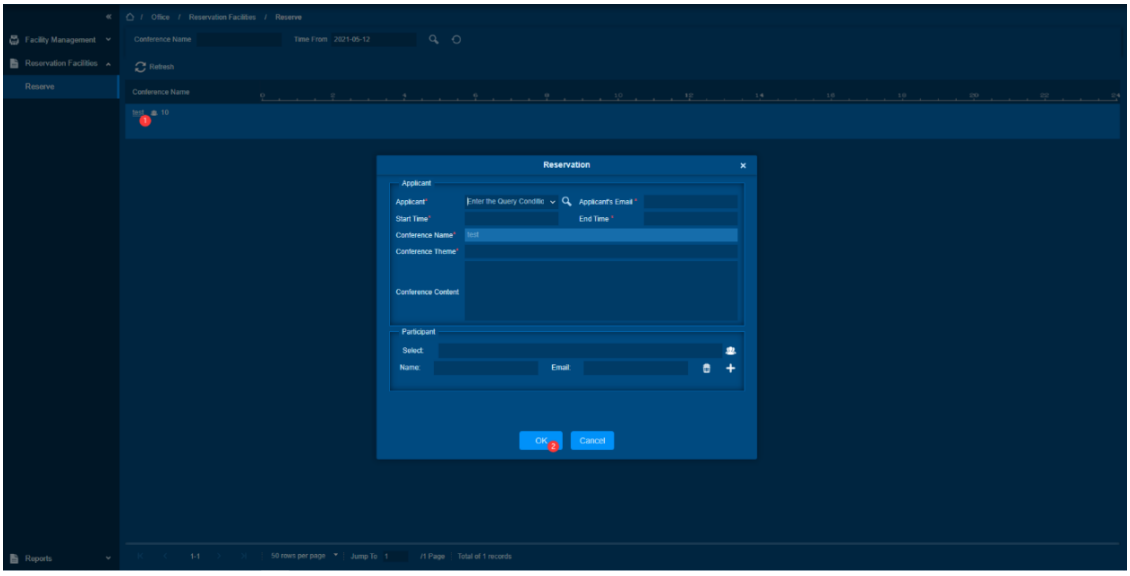
The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

When you need to book a meeting.

Feature Trigger Result

Operations	Description
Meeting Room Reservation	Reservation a meeting



Click the name of the Meeting Room to be reserved and to enter the Meeting Room reservation interface.

The description of each field is as follows:

Appointment person: Appointment person of Meeting Room, support input of personnel ID number to quickly fill in appointment person information.

Reservation person's mailbox: Enter the reservation person's mailbox, and an email notification will be sent after the reservation is successful. When the selected person has set up the mailbox in the personnel, this item will be filled in automatically.

Start time: Set the start time of the scheduled meeting, the start time should be 30 minutes later than the current system time (for example, the current time is 10:00:00, then the scheduled time should be set to the time after 10:30:00), and the start time is not less than the end time.

End time: Set the end time of the scheduled meeting, the start time is not less than the end time.

Meeting Room Name: Display the name of the currently reserved Meeting Room.

Conference subject: Fill in the subject of the conference reservation.

Remarks: Text to remark the content of the meeting.

Participants: Optional personnel and visitors who have been added to participate in the meeting. If the selected participant has set the email information, the system will automatically send the scheduled meeting email.

Manually enter the participant's information, enter the participant's name, and email address below, click to add participant, and click Delete participant.

Meeting Room Reservation Deleted

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

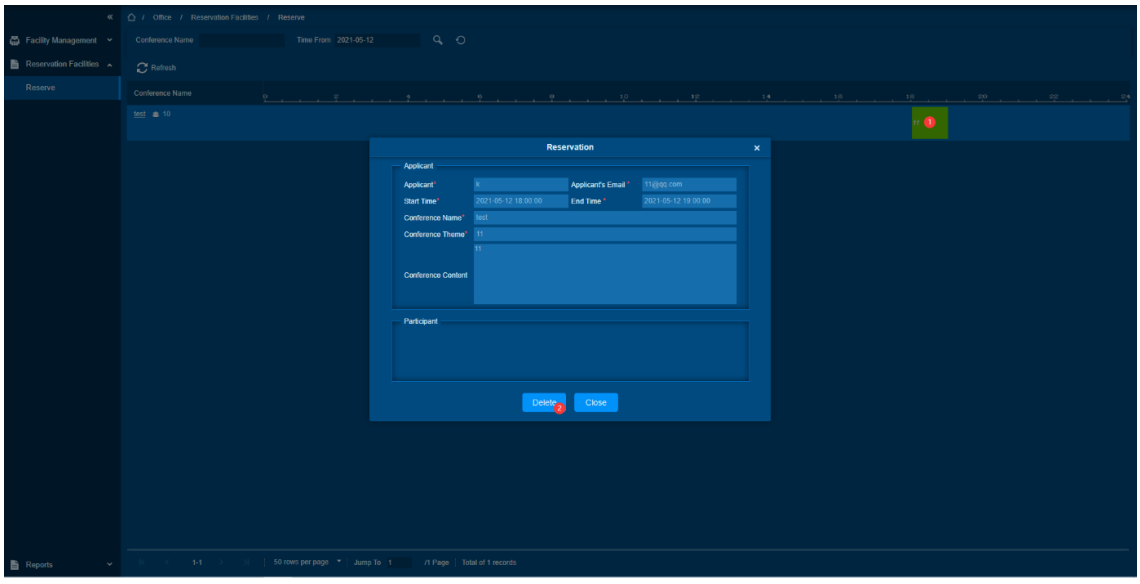
When you need to cancel a meeting.

Feature Trigger Result

Operations	Description
Meeting room reservation cancellation	Cancel a meeting

Steps:

- Click on the scheduled meeting, and the meeting reservation Details interface will pop up.
- Click [**Delete**] button to delete the current scheduled meeting.



✍**Note:**

Expired and started meetings cannot be deleted.

12.3. Reports

Function List

Operations	Description
Meeting Room report	Show Meeting Room statistics
Maintenance Records	Display maintenance records statistics

12.3.1. Report

Function Description

Its shows the statistics of Meeting Room data.

Meeting Room report

Preconditions for Normal Use of Function

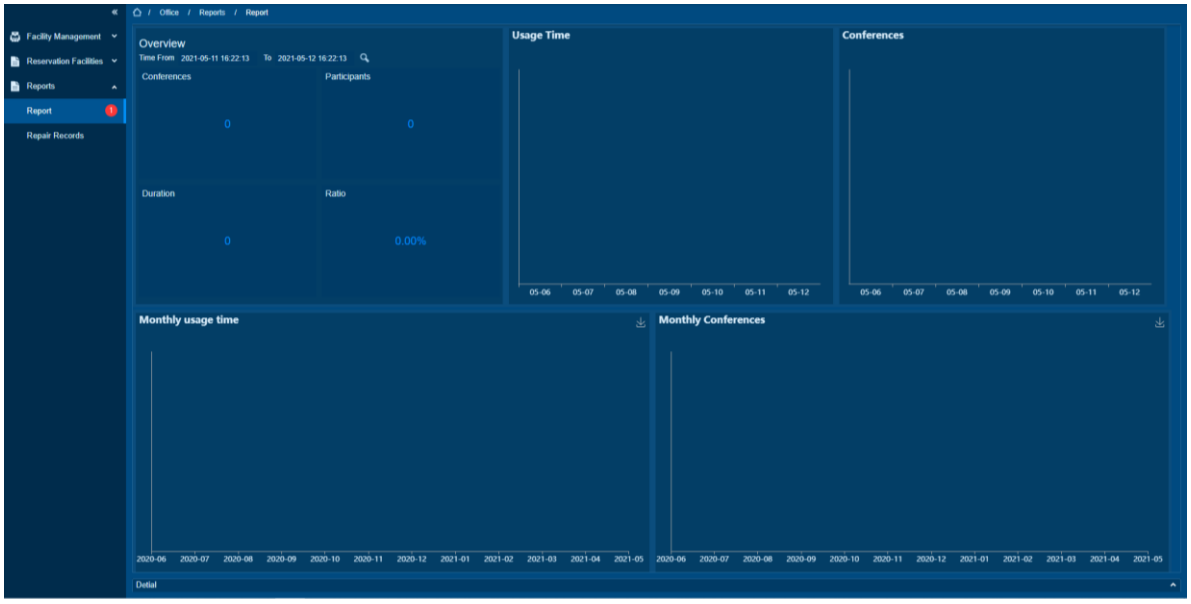
The system is operating normally, and the account has corresponding operation permissions.

Function Usage Scenarios

View meeting room data.

Feature Trigger Result

Operations	Description
Enter the Page	Show meeting room report data



Overview: Display the number of meetings within the set Timetable; the number of participants; the length of

the meeting; the proportion of the number of participants to the total number of participants.

Use time: It display a histogram of the use time of each Meeting Room in the past 7 day.

Number of meetings: A bar graph showing the number of meetings in each Meeting Room in the past 7 days.

Monthly usage time: It display the line graph of the total monthly usage time of each Meeting Room.

Number of monthly meetings: A line graph showing the number of meetings held in each Meeting Room each month.

Click [**Details**] to view the detailed record of the conference reservation.

12.3.2. Repair Records

Function Description

When using this management system, you need to register personnel in the system, or import personnel from other software or documents into the system by way of importing, and you can set the authority of the personnel corresponding to the module.

Maintenance Records List

Preconditions for Normal Use of Function

The system is operating normally, and the account has corresponding operation permissions.

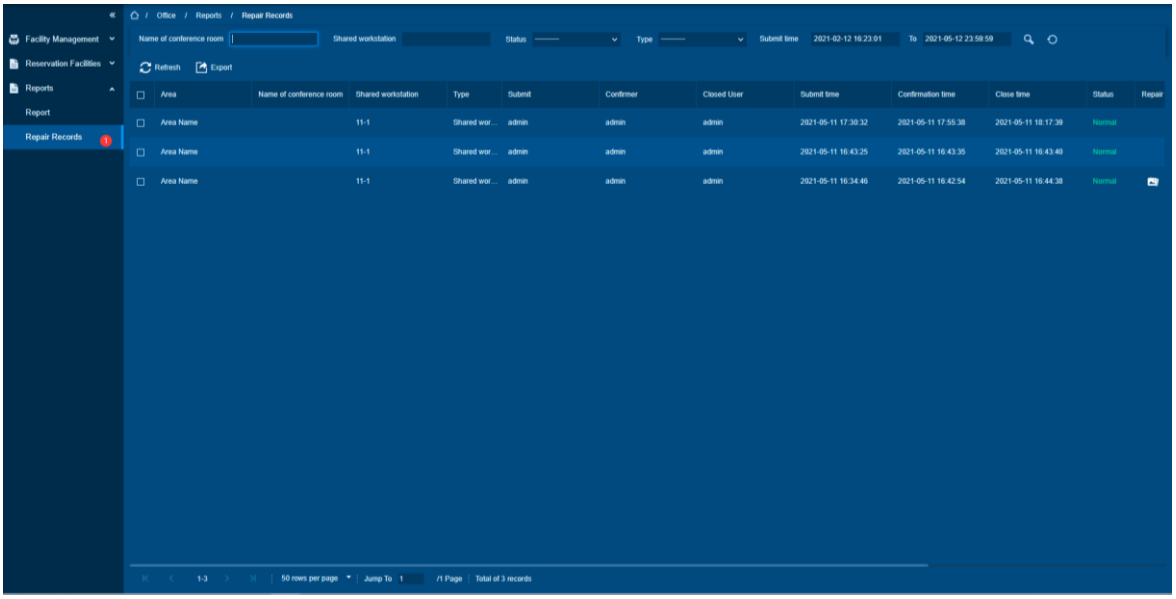
Function Usage Scenarios

Check the repair status.

Feature Trigger Result

Operations	Description
Enter the Page	Display repair report data

Click [**Reports**] > [**Repair Records**] to view repair record Interface.



12.3.3. Online Meeting Records

Online Meeting Room Reservation

Preconditions for Normal Use of Function

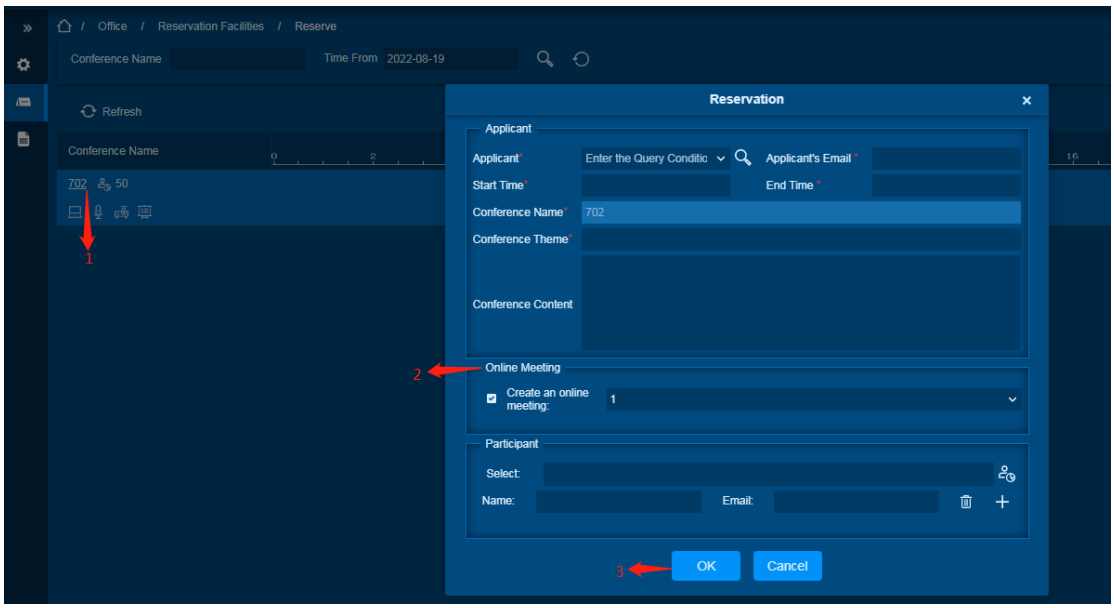
- First, the system must operate normally.
- Second, the account has the necessary operating permissions.
- Third, the system must be connected to the Zoom platform.

Function Usage Scenarios

When you need to book an online meeting.

Feature Trigger Result

Operations	Description
Meeting Room Reservation	Reservation a meeting



Click the name of the Meeting Room to be reserved and to enter the Meeting Room reservation interface.

The description of each field is as follows:

Applicant: Appointment person of Meeting Room, support input of personnel ID number to quickly fill in appointment person information.

Applicant's Email: Enter the reservation person's mailbox, and an email notification will be sent after the reservation is successful. When the selected person has set up the mailbox in the personnel, this item will be filled in automatically.

Start time: Set the start time of the scheduled meeting, the start time should be 30 minutes later than the current system time (for example, the current time is 10:00:00, then the scheduled time should be set to the time after 10:30:00), and the start time is not less than the end time.

End time: Set the end time of the scheduled meeting, the start time is not less than the end time.

Conference Name: Display the name of the currently reserved Meeting Room.

Conference Theme: Fill in the subject of the conference reservation.

Conference Content: Text to remark the content of the meeting.

Online Meeting: Docking between ARMATURA One and Zoom makes it possible to make a conference online.

Participants: Optional personnel and visitors who have been added to participate in the meeting. If the selected participant has set the email information, the system will automatically send the scheduled meeting email.

Manually enter the participant's information, enter the participant's name, and email address below, click  to add participant, and click  Delete participant.

13. Fire Alarm Module

Integrate valid system data to carry out all-round real-time monitoring of fire warning alarms.

13.1. Device

Device Management is used to synchronize the device from the fire alarm host to view and manage the device, view the status of the device in real time, and set the event linkage action between the devices.

Function List

Operations	Description
Device Manager	Simultaneous display of fire alarm data
Equipment Project Manager	Simultaneous display of fire alarm equipment data
Event Group	Simultaneous display of fire alarm event group data
Real-Time Monitoring	Real-time display of fire warning alarm dynamics
Linkage	Simultaneous display of fire alarm linkage status

13.1.1. Device Manager

Function Description

Simultaneous display of fire alarm data.

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

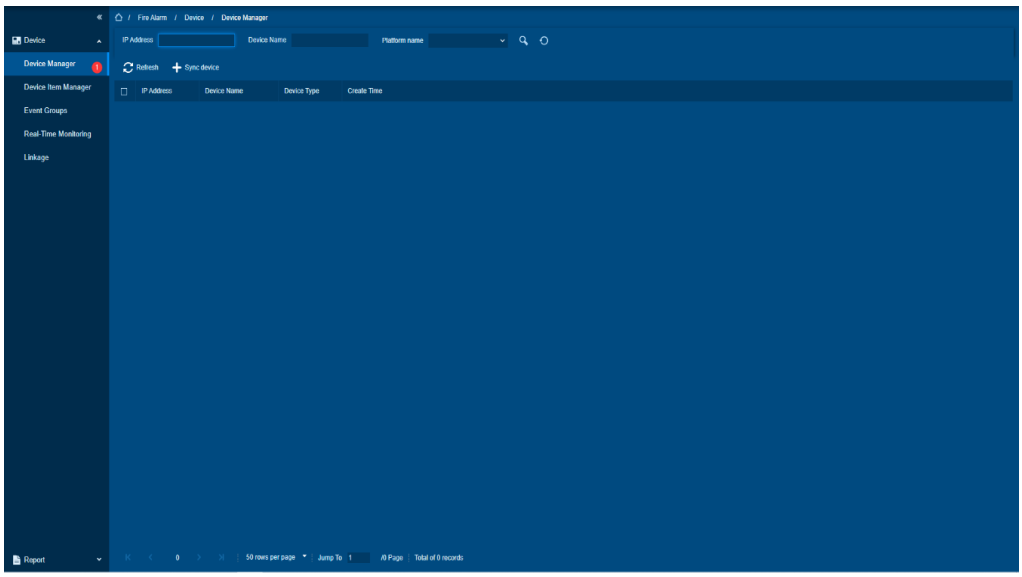
Function Usage Scenarios

Need to view fire alarm device data.

Feature Trigger Result

Operations	Description
Enter the Page	Display fire alarm equipment data

Click [**Fire Alarm Device**] > [**Device Manager**] to access the following page.



Device Manager Synchronization

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

Function Usage Scenarios

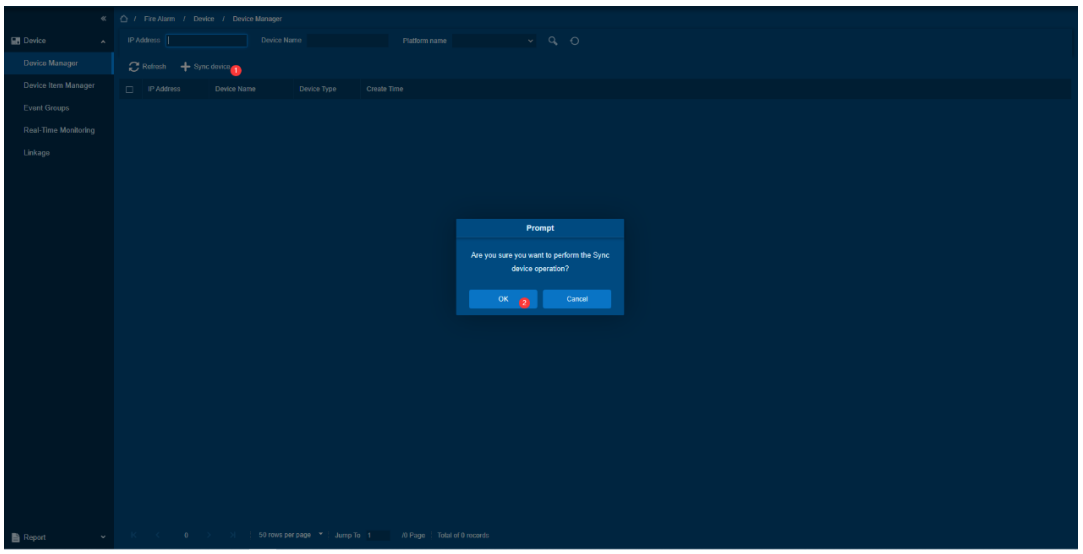
To sync device data.

Feature Trigger Result

Operations	Description
Sync Device Data	The device data are saved in the same way.

Steps:

- Click [**Face Alarm**] > [**Device Manager**] > [**Sync Device**] to sync device data.
- Click [**OK]** to complete operation.



13.1.2. Device Item Manager

Function Description

Simultaneously display of fire alarm data.

Device Project Manager

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

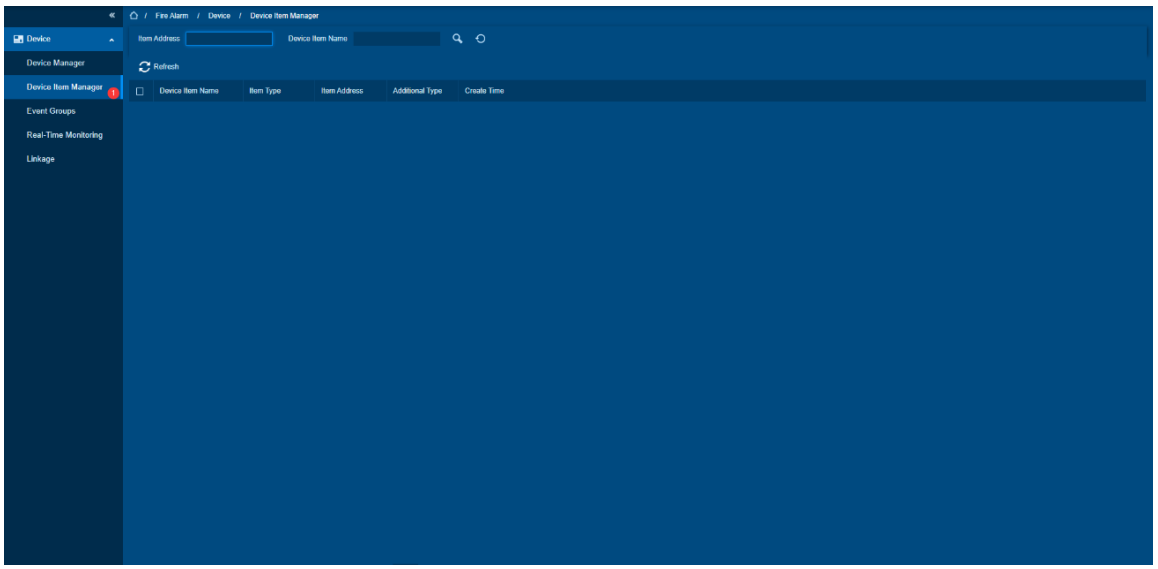
Function Usage Scenarios

It needs to check the status of fire alarm data items.

Feature Trigger Result

Operations	Description
Enter the Page	View fire alarm project data

Click **[Fire Alarm]> [Device] > [Device Item Manager]** to access the following page.



13.1.3. Event Groups

Function Description

Simultaneous display of fire alarm event group data.

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

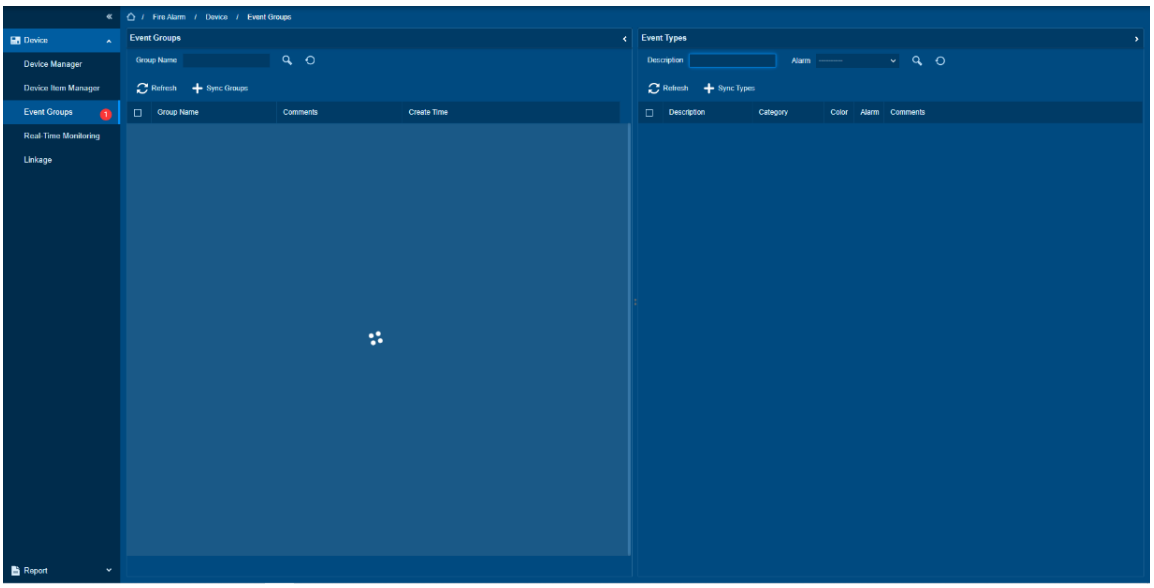
Function Usage Scenarios

It needs to view and display fire alarm event group data.

Feature Trigger Result

Operations	Description
Enter the Page	Display fire event group data

Click **[Fire Alarm]> [Device] > [Event Groups]** to access the following page.



13.1.4. Real-Time Monitoring

Function Description

It displays Real-time fire warning alarm dynamics.

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

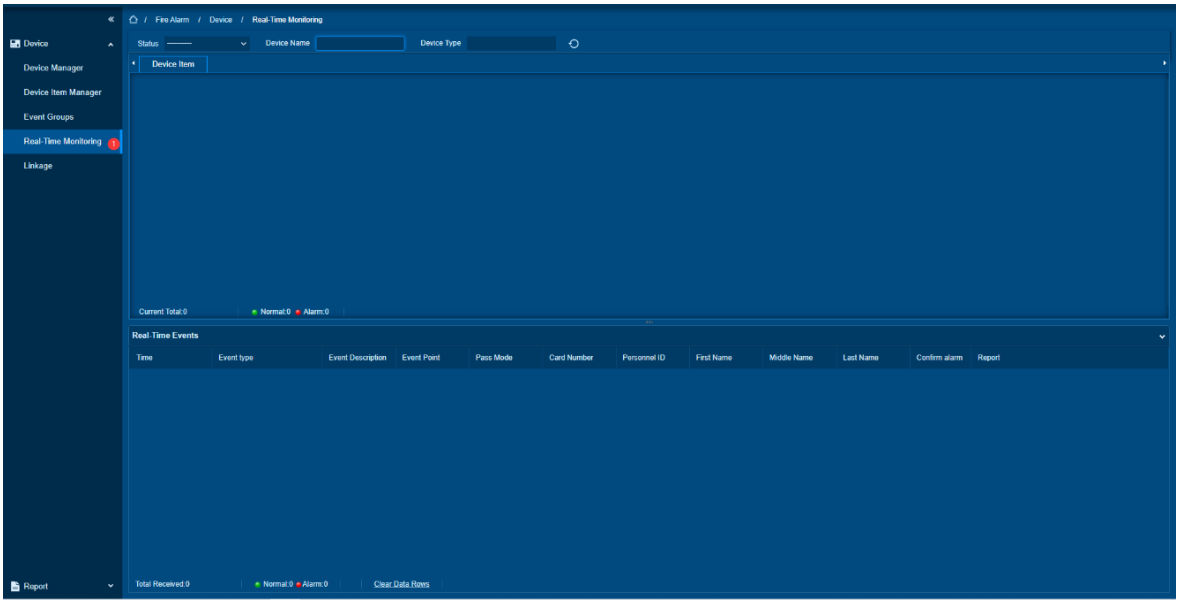
Function Usage Scenarios

Monitoring of the current alarm data page in real-time.

Feature Trigger Result

Operations	Description
Enter the Page	Display current alarm data

Click [**Fire Alarm**]> [**Device**] > [**Real-Time Monitoring**] to access the following page.



13.1.5. Linkage

Function Description

Simultaneously display of fire alarm linkage status.

Linkage List

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

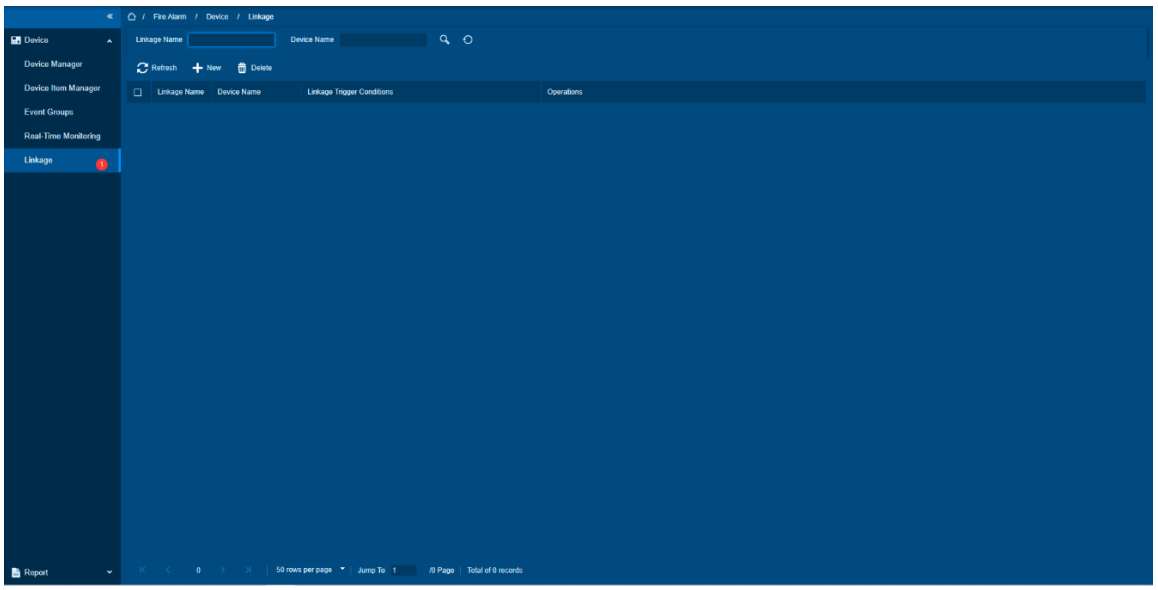
Function Usage Scenarios

To view current Linkage data.

Feature Trigger Result

Operations	Description
Enter the Page	View current Linkage alarm data.

Click **[Fire Alarm]>[Device] > [Linkage]** to access the following page:



13.2. Report

Function List

Operations	Description
Event Type	Simultaneously display fire alarm event type data
Alarm Monitoring	Simultaneously display of fire alarm monitoring data
All Events	Simultaneously display of fire alarm all events data

13.2.1. Event Types

Function Description

Simultaneously display fire alarm event type data.

Event Type List

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

Function Usage Scenarios

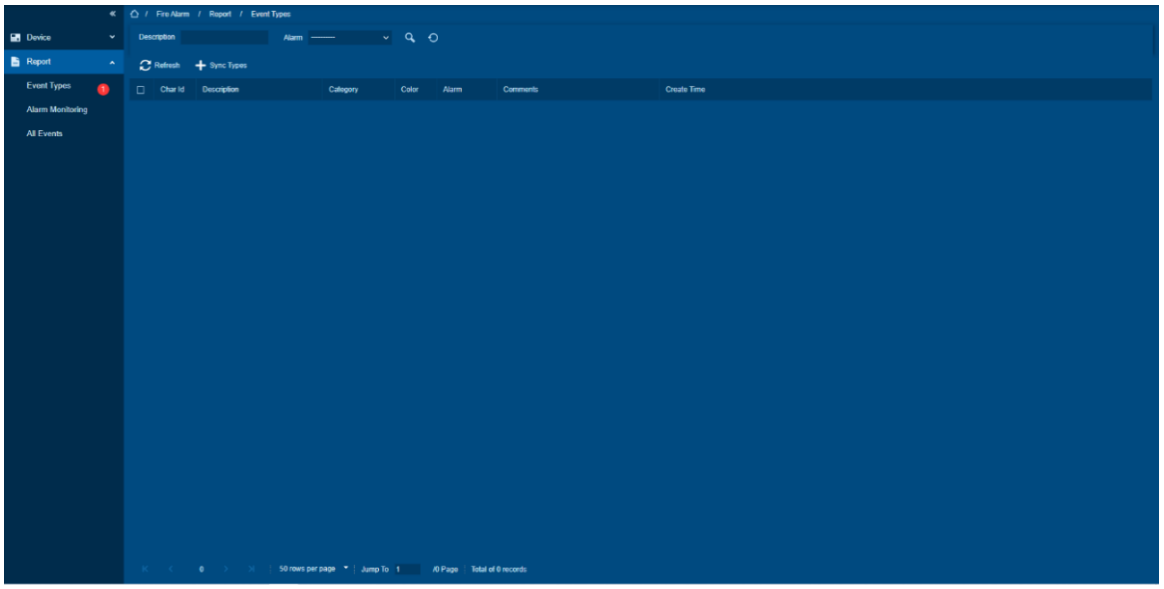
Need to view fire alarm event type data.

Feature Trigger Result

Operations	Description

Enter the Page	Display fire event type data

Click **[Fire Alarm] > [Report] > [Event Types]** to access the following page:



13.2.2. Alarm Monitoring

Function Description

Simultaneously display of fire alarm monitoring data

Alarm Monitoring List

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

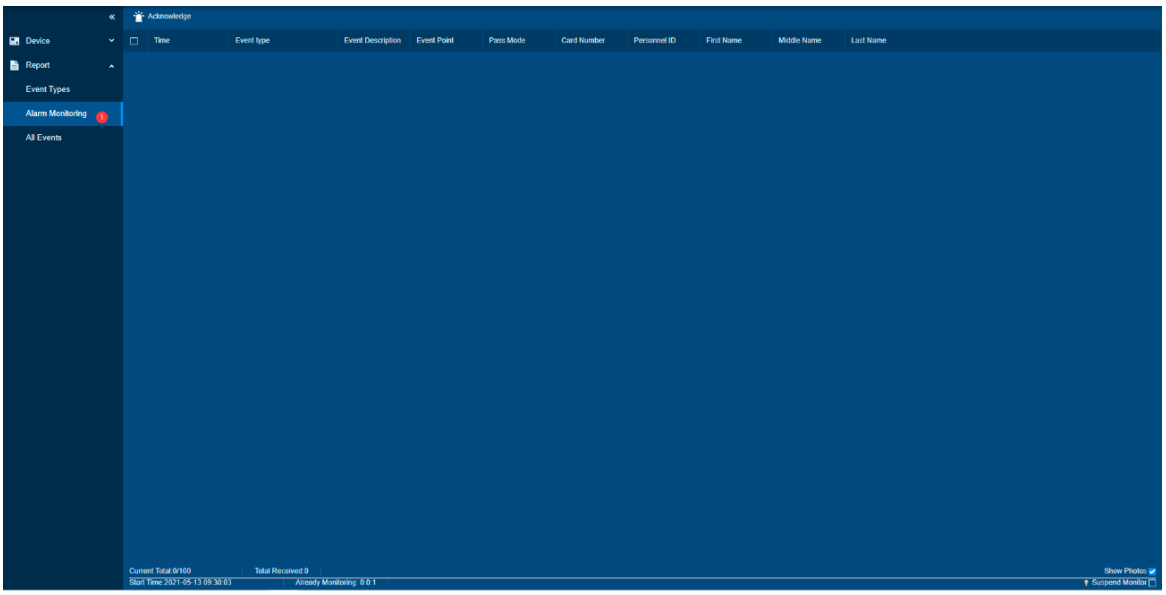
Function Usage Scenarios

Need to view the fire alarm monitoring data.

Feature Trigger Result

Operations	Description
Enter the Page	Display fire alarm monitoring data

Click **[Fire Alarm] > [Report] > [Alarm Monitoring]** to access the following page.



13.2.3. All Events

Function Description

Simultaneously display of fire alarm all events data

All Events List

Preconditions for Normal Use of Function

The system is running normally, and the valid account needs to be configured in the third-party integration module and is in the enabled state.

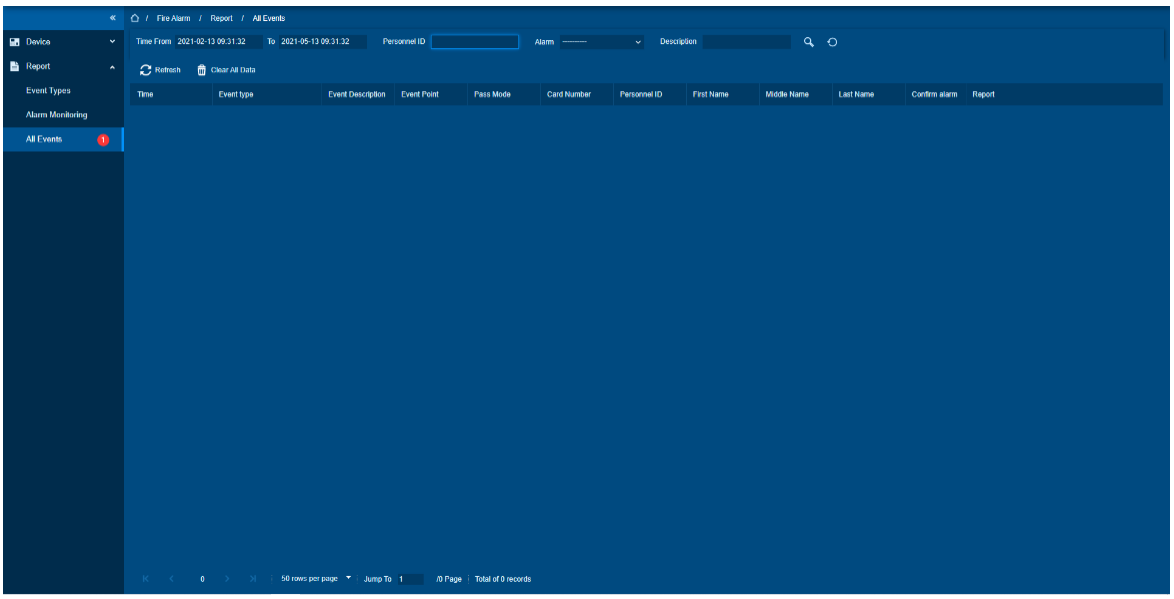
Function Usage Scenarios

Simultaneously display of fire alarm all events data.

Feature Trigger Result

Operations	Description
Enter the Page	Display fire alarm all events data

Click **[Fire Alarm]** > **[Report]** > **[All Events]** to access the following page.



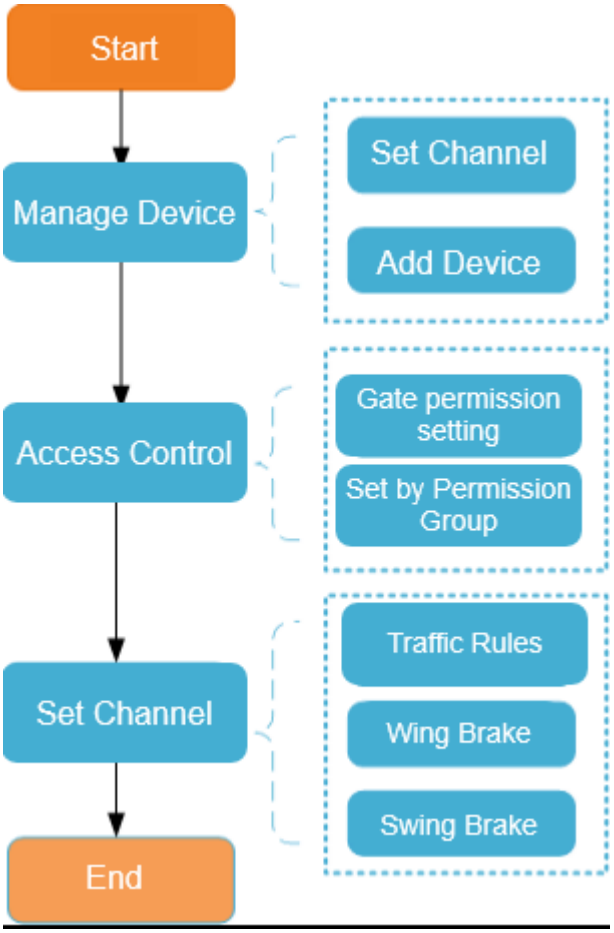
14. Entrance Control

This system connects the gate control board through channel Device (such as TDA integrated machine), and directly controls the relevant parameters of the gate through software, thus controlling the entry and exit of the gate and realizing the automatic management of the gate.

Workflow

Introduce the configuration process of channel service.

The channel business configuration process is shown in below.



14.1. Channel Device

Add channel integrated machine Device, and the integrated machine communicates with the gate control board through RS485 to control the gate.

14.1.1. Passage

Setting the area to which the channel belongs is convenient for users to manage the channel Device in a specific area. After setting the channel, the Device under the channel can be filtered according to the area during real-time monitoring.

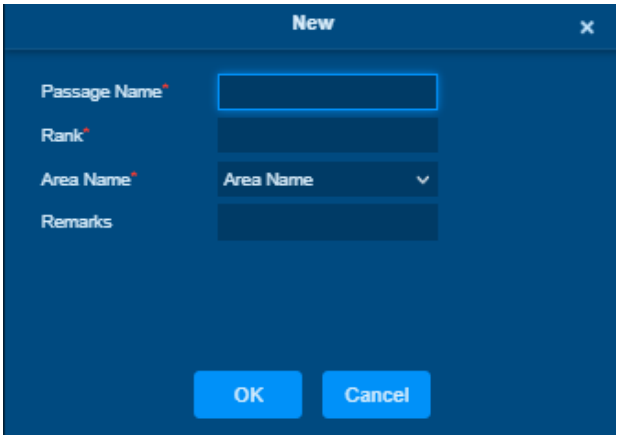
This paper introduces the Steps of creating and configuring channels in software.

To Add Passage (New)

Steps:

Step 1: In the Channels module, select [**Channel Device**]>[**Passage**].

Step 2: In the channel interface, click [**New**] and fill in the relevant parameters, as shown in below. Please refer to table for parameter description.



New Channel Interface

Parameter	How to set
Passage name	Any character, a combination of up to 20 characters, cannot be repeated.
Rank	Only numbers are supported, up to six digits, repeatable. The smaller the ranking, in real-time monitoring, the display will move forward.
Area name	Select the region to which the channel belongs.
Remarks	Any character with a maximum character length of 100.

Description of new channel parameters

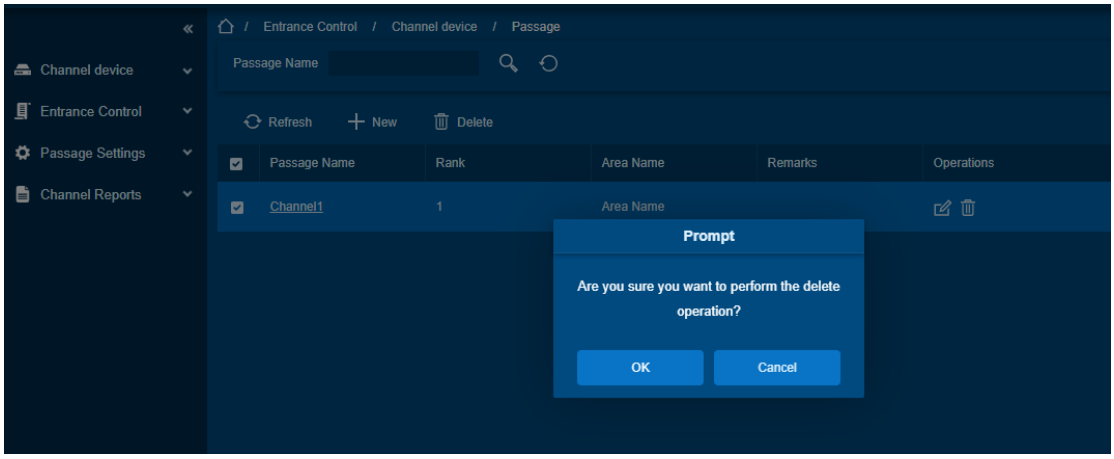
Step 3: Click [**OK**] to complete the channel setting.

Delete Passage

Steps:

Step 1: In the Entrance Control module, select [**Channel Device**] > [**Passage**] and select the template to be deleted.

Step 2: Click [**Delete**] to delete the selected template Click [**OK**] to perform the delete operation.



To Delete Passage

✍**Note:**

The passage cannot be deleted when the device exists.

14.1.2. Device

Searching for Additional Channel Devices (Search)

Introduces the configuration Steps of searching for additional channel devices in software.

Preconditions for Normal Use of Function:

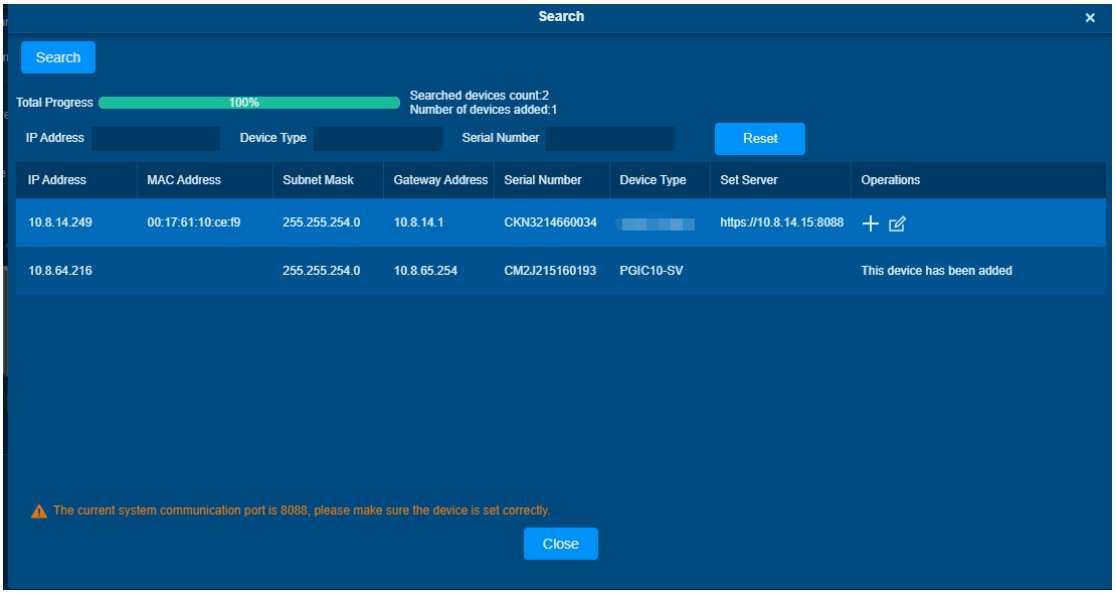
1. Set up IP allocation before adding channel devices.
2. Before searching and adding the device, it is necessary to set the address pointing to the server in advance and set the IP address and port of the current server, that is, the IP address and admins port installed by the current.

Steps:

Step 1: In the Channel module, select [**Channel Device**] >[**Device**].

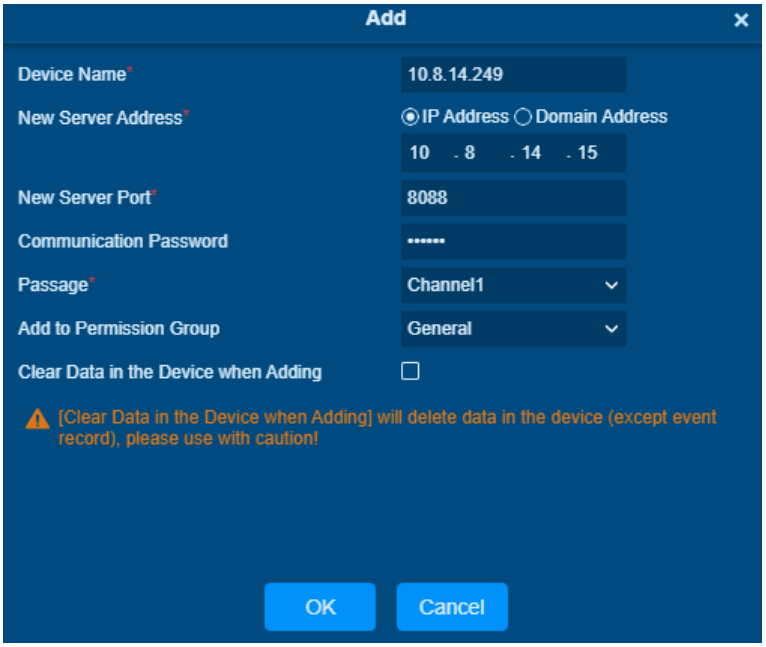
Step 2: In the device interface, click [**Search**] to pop up the search box.

Step 3: Click [**Search**] in the search box to display the channel devices that can be added, as shown in below**.**



Device Search Interface

Step 4: For the channel Device found, click the [**Add**] button in the operation bar to Add the device, and fill in the parameters of device addition, as shown in below. Please refer to table for parameter description.



Device Addition Interface

Parameter	How to set
Device name	Any character, a combination of up to 20 characters, cannot be repeated.

New Server Port	The software is using the ADMS communication port, which is 8088 by default.
Communication Password	The webserver in the backend of the device can be configured for use when interfacing with the software.
Passage	Select the channel to which the device belongs.
Add to Permission Group	Automatically adds the device to the selected permission group.
Clear data in device when adding	When the device is added, the data in the device except the event record is deleted.

Description of device Addition Parameters

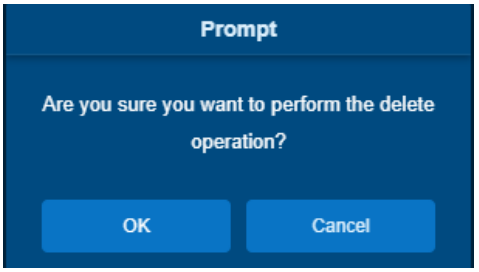
Step 5: Click [**OK**] to complete the addition of channel device.

Delete

Steps:

Step 1: In the [**Entrance Control**], click [Channel Device] > [**Device**] and select device to be deleted.

Step 2: Click [**Delete**] to delete the device.

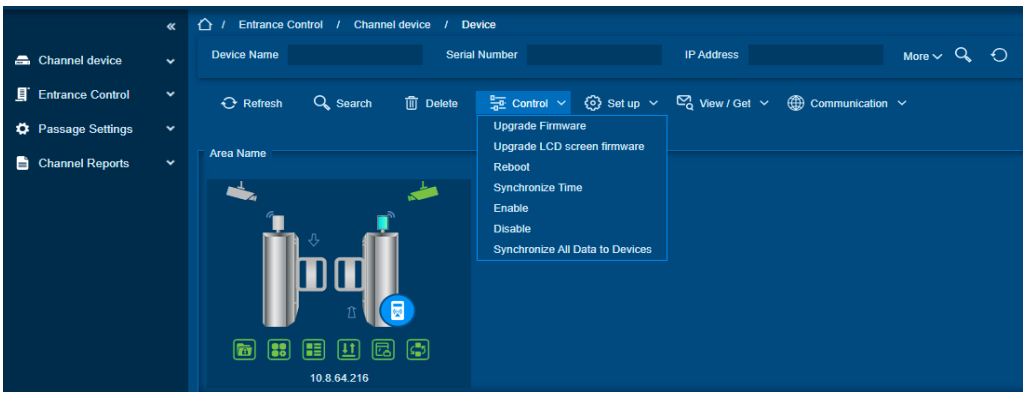


Delete Device

Step 3: Click [**OK**] to perform the delete operation**.**

Control

In this option admin can upgrade firmware and LCD screen firmware. Also, this option helps to reboot the device, enable and disable the devices, and synchronize time and all data.



Device Control Interface

1. **Upgrade Firmware**:

   Select the device to be upgraded and click [**Upgrade Firmware**] to open the setting page. Click [**Browse**], select the firmware upgrade file (file name is emfw.cfg). Click [**Start**] to start upgrading the firmware.

✍**Note:**

Please be cautious while upgrading the firmware. If the firmware has not been updated properly, it may lead to device failure. If you have any queries, please contact the representative or pre-sales technical support team.

2. **Upgrade LCD Screen Firmware:**

   Admin can upgrade LCD screen firmware of device using this option. Select the device to be upgraded and click [**Upgrade LCD Screen Firmware**] to open the settings page. Click [**Browse**] and select the firmware upgrade file. Click [**Start**] to start upgrading the firmware.

3. **Reboot the Device:**

   Admin can send a restart command to the device to automatically restart. Select the device to be reboot and click [**Reboot**] to restart the device.

4. **Synchronize Time:**

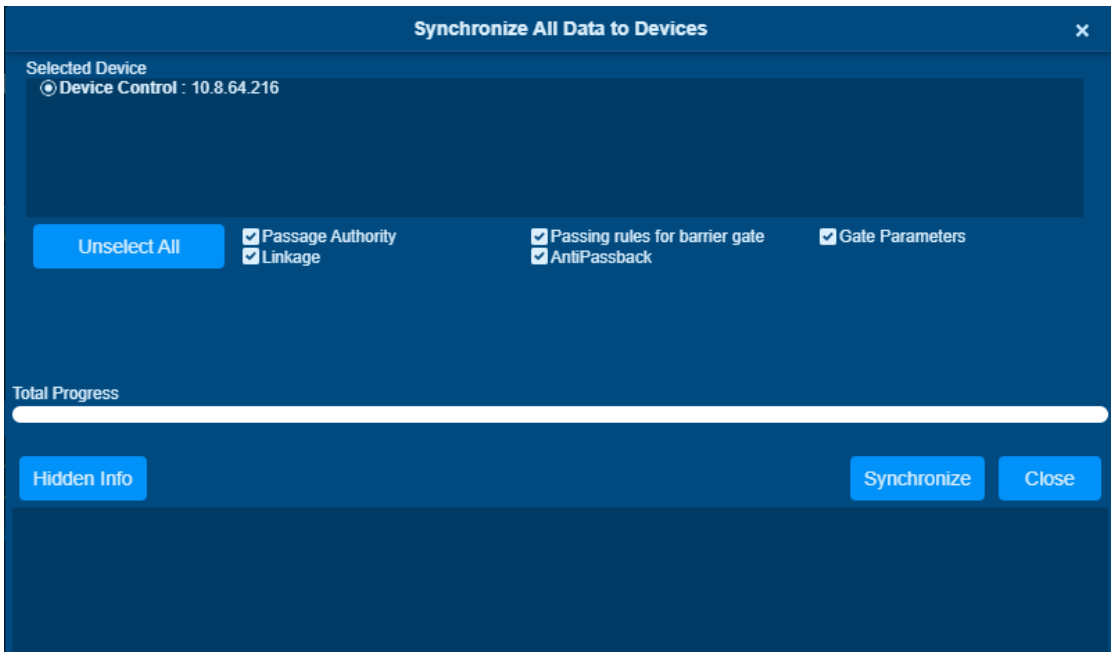
   When the device's time is not accurate, select the device to be synchronized and then click [**Synchronize Time**] to synchronize the server time to the device.

5. **Disable/Enable:**

   Select the device and click [**Disable/Enable**] to stop/start using the device. When communication between the device and the system is interrupted or there is a problem with the device, the device may be automatically displayed as disabled. After adjusting the network or device, click [**Enable**]. The system reconnects to the device, and the communication status of the device is restored.

6. **Synchronize All Data to Devices:**

   This option synchronizes the data in the system to the device. Select the device, click [**Synchronize All Data to Devices**], and click the [**Synchronize**] button to synchronize data.



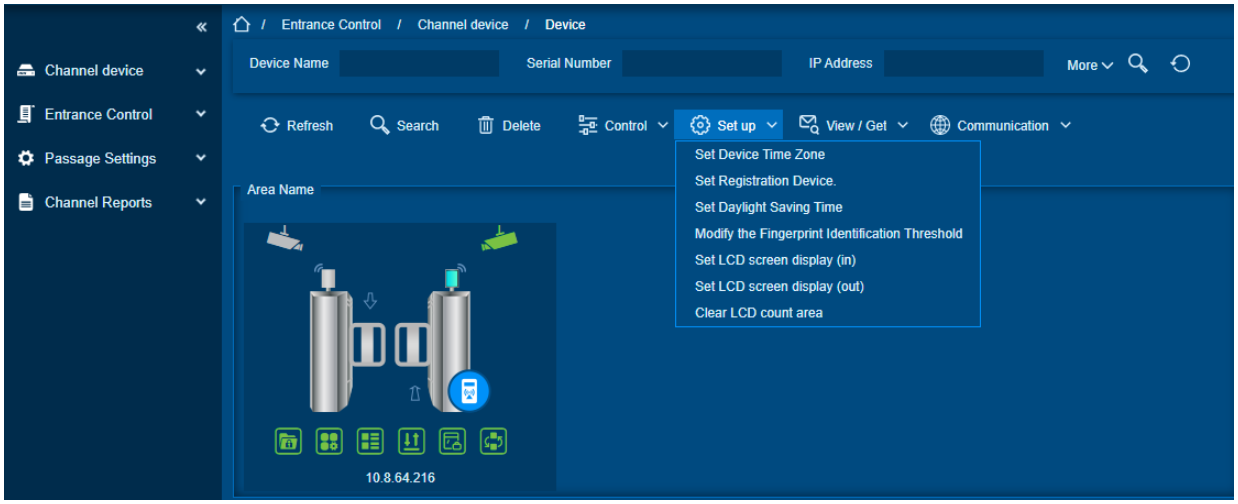
Synchronize All Data to Devices Interface

✍**Note:**

The operation of synchronizing all data will first delete the existing data in the device (excluding event records) and then download all the setting information again. When performing this operation, please try to ensure that the network is unblocked and avoid power failure. When the device is running normally, please use this operation with caution. It is recommended to synchronize the data when the device is unused.

Set up

In this interface help you to set the time zone, registration, daylight saving time, fingerprint identification information and LCD screen display of the selected device.



Set up Options

1. **Set Device Time Zone:**

   Set Device Time Zone allows you to set the accurate time zone if device shows wrong time zone. For

that in **Entrance Control** interface, click [**Channel Device**] > [**Device**] >[**Set-up**], select the device to be set up. Then click [**Set Device Time Zone**] to set up the selected device.

2. **Set Registration Device:**

   The passage standalone device can only automatically upload the personnel and other data entered by the device when the registration device is set. For that in **Entrance Control** interface, click [**Channel Device**] >[**Device**] >[**Set-up**], select the device to be set up. Then click [**Set Registration Device**] to set up the selected device.

3. **Set Daylight Saving Time:**

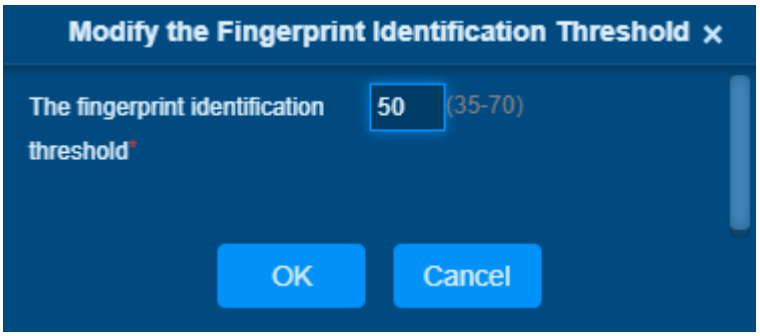
   DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

   In the **Entrance Control** interface, click [**Channel Device**]> [**Device**] > [**Set-up**] and select the device to be set Daylight Saving Time. Then click [**Set Daylight Saving Time**] to set up the selected device.

4. **Modify the Fingerprint Identification Threshold:**

   The user can modify the fingerprint comparison threshold in the device, ranging from 35 to 70, and the factory default value is 55. When a new device is added, the system will read the value from the device, and the user can view the current fingerprint comparison threshold size through the device list (Please make sure the device supports the fingerprint function).

   In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**Set-up**] and select the device to be modify the fingerprint identification. Then click [**Modify the Fingerprint Identification Threshold**] to set up the selected device.



Modify the finger Identification Option

5. **Set LCD Screen Display (In)/(Out):**

   Select the device and set the LCD screen display (in/out). The upper part is the video area 30%, the middle part is the gate channel display area 30%, and the lower part is the picture cycle 40%. Each area can be corresponding to the video and background, The image browsing and clearing operations are confirmed and sent to the LCD screen of the controller for display.

   In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**Set-up**] and select the device to be set LCD screen display. Then click Set [**LCD Screen Display (In)/(Out**)] to set up the selected device.

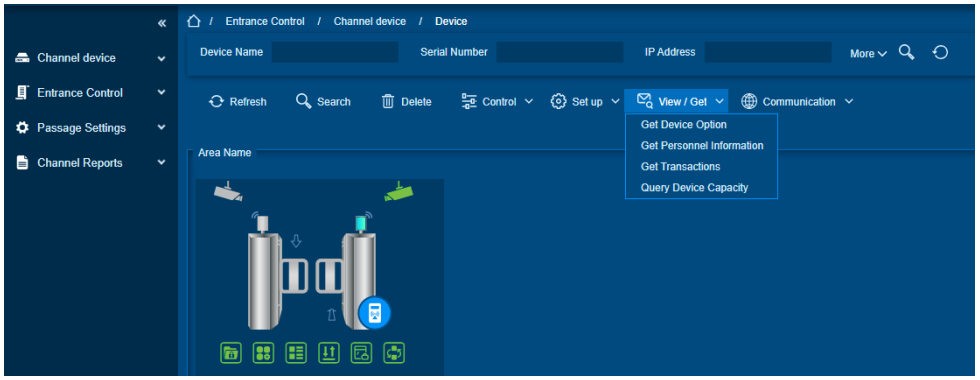
6. **Clear the LCD Counting Area:**

Select the device, clear the middle counting area of the LCD screen, and restart counting.

In the Entrance Control interface, click [**Channel Device**] > [**Device**] > [**Set-up**] and select the device to clear the LCD counting area. Then click [**Clear the LCD Counting Area to clear counting area**] the selected device.

View/ Get

In this interface admin can view device options, personal information, and transaction details.



View/Get Option

1. **Get Device Option:**

   This option allows you to view the common parameters of the device. For example, get the firmware version after the device is updated.

   In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**View/Get**] and select the device to view device options. Then select [**Get Device Option**] to view device options.

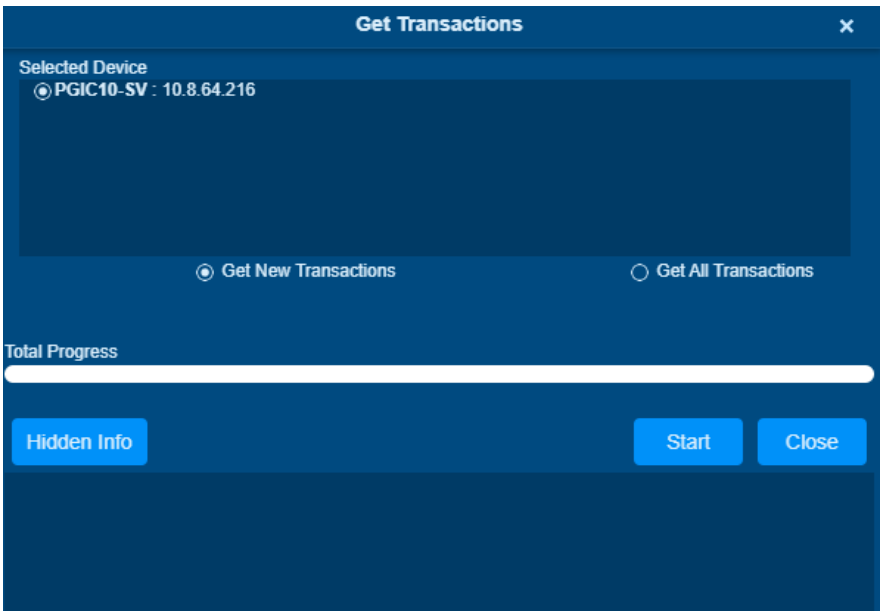
2. **Get Personnel Information:**

   This function obtains the data of Persons, Fingerprints, and Palm prints in the device or obtains the corresponding number.

   In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**View/Get**] and select the device to view personnel information. Then select [**Get Personnel Information**] to view personnel information.

3. **Get Transaction:**

   This function obtains the event records in the device to the system, and the user can choose to obtain new records or all the records. In the **Entrance Control** interface, click [**Channel Device**]> [**Device**] > [**View/Get**] and select the device to get transaction. Then select [**Get Transaction**] to view transaction information.



Get Transactions

When the network is in good condition and the communication between the system and the device is normal, the system will obtain the event record in the device in real-time and saves it in the database. When the communication is interrupted, the event record in the device is not uploaded to the system in real-time. At this time, the user can perform this operation to manually obtain the event records in the device.

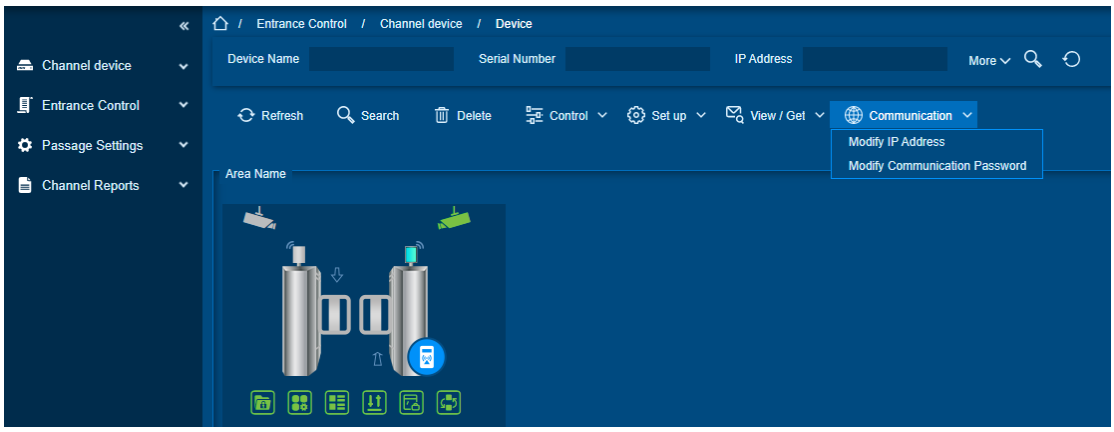
4. **Query Device Capacity:**

   Here, the user can view the capacity information of the device in the software and manually obtain the usage information (person, fingerprint, finger vein, face, palm print) in the device. When the user finds that the information obtained from the software and the device is inconsistent, the user can manually synchronize the data.

   In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**View/Get**] and select the device to view the capacity information of the device. Then select [**Query Device Capacity**] to view the user can view the capacity information of the device in the software and manually obtain the usage information.

Communication

In the **Entrance Control** interface, click [**Channel Device**] > [**Device**] > [**Communication**] to modify IP address and communication password.



Communication Option

1. **Modify IP Address:**

   Select a device and click [**Modify IP address**] to open the modification interface. It will obtain a real-time network gateway and subnet mask from the device. (Failed to do so, you cannot modify the IP address). Then enter a new IP address, gateway, and subnet mask. Click [**OK**] to save and quit. This function is the similar as Modify IP Address Function in Device.

2. **Modify Communication Password:**

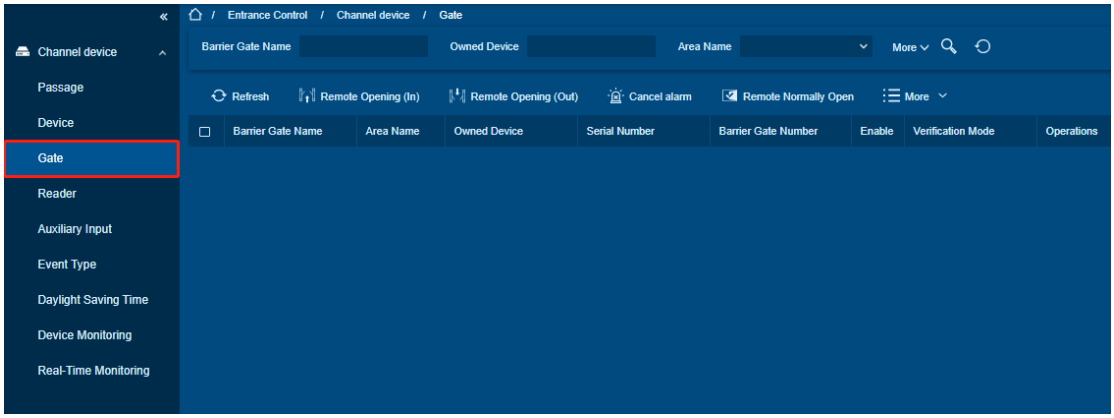
   Select a device and click [**Modify Communication Password**] to open the modification interface The system will ask for the old communication password before modifying it. After verification, input the new password twice, and click [**OK**] to modify the communication password.

✍**Note:**

Communication passwords shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password settings can improve the device's security. It is recommended to set communication passwords for each device.

14.1.3. Gate

In the **Entrance Control** module, select [**Channel Device**] > [**Gate**].



Channel Device Gate

Remote Gate Opening (in)/(out)

In the **Entrance Control** interface, click [**Channel Device**] > [**Gate**] interface allows the user to control one gate or all gates. To control a single gate right-click over it and click [**Remote Opening (In/Out**)] in the pop-up dialog box. To control all gates, directly click [**Remote Opening (In/Out**)] behind Current All.

Cancel the Alarm

Once an alarm door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for a single gate or all gates.

In the **Entrance Control** interface, click [**Channel Device**] > [**Gate**] and select the alarm gate to be modified. Then click [**Cancel the Alarm**] to cancel the alarm.

✍**Note:**

If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

Remote Normally Open

It will set the gate as normal open by remote.

In the **Entrance Control** interface, click [**Channel Device**] > [**Gate**] and select the gate to be set as normal open. Then click [**Remote Normal Open**] to set the gate as normal open by remote.

More Options

In the **Entrance Control** interface, click [**Channel Device**] > [**Gate**] >[**More**] to activate the door lockdown status (remote lock and unlock).

1. **Remote Lock:**

   It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

2. **Remote Unlock:**

   It will unlock a locked door. This function is supported only by certain devices.

3. **Enable / Disable Intraday Passage Mode Time Zone:**

   In remote opening, user can define the door opening duration (The default is 15s). You can select [**Enable Intraday Passage Mode Time Zone**] to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

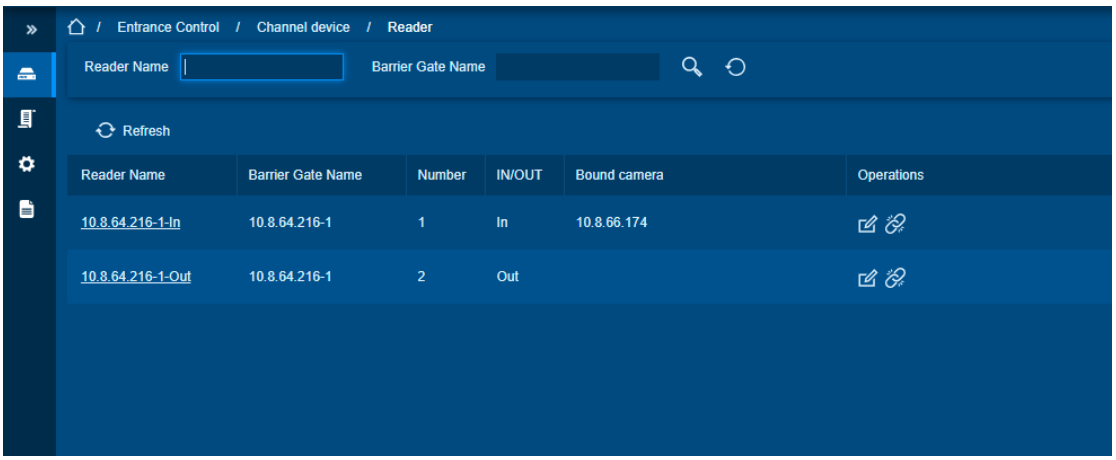
   To close a door, select [**Disable Intraday Passage Mode Time Zone**] first, to avoid enabling other normal open time zones to open the door, and then select [**Remote Closing**].

14.1.4. Reader

Each Entry device has a reader, user can view the reader information in this interface.

Steps:

Click [**Entrance Control**] > [**Channel Device**] > [**Reader**] to view the reader information such as reader name, barrier gate name, bound camera, and it in/out details.

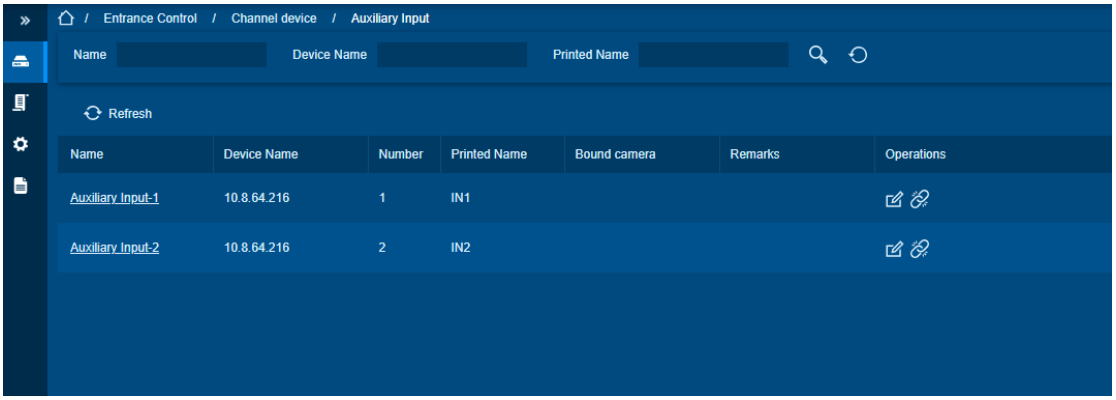


Reader Interface

14.1.5. Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

Click [**Entrance Control**] > [**Channel Device**] > [**Auxiliary Input**], to access below shown interface.



Reader Interface

Bind/Unbind Camera

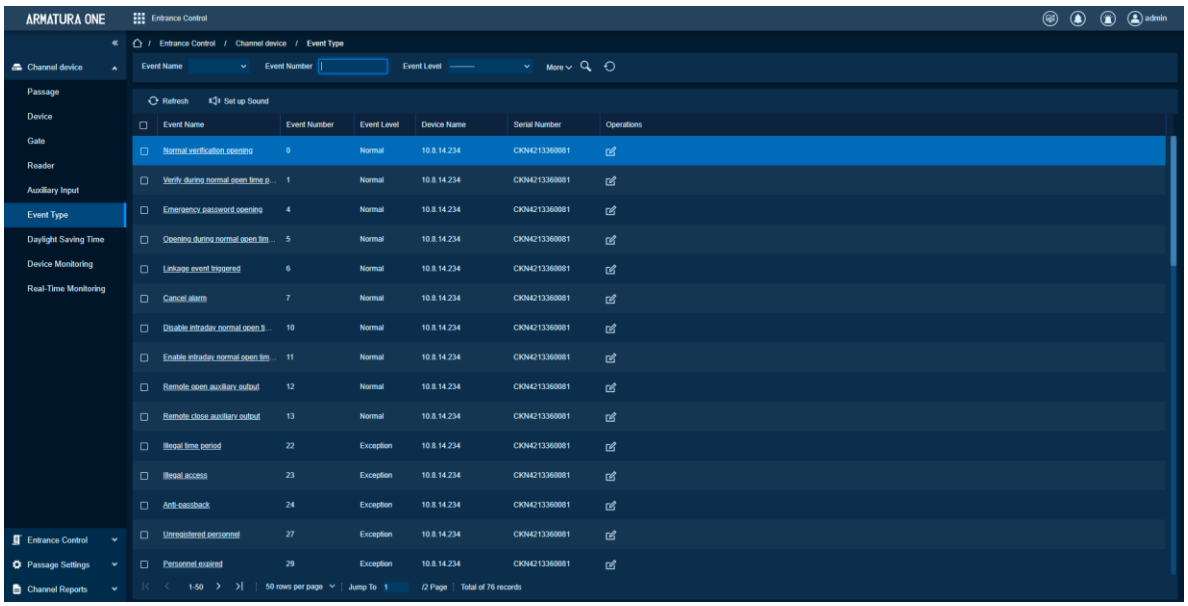
Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos, or screenshots) once there is a corresponding event occurs. For this, the interaction setting in Linkage or in Global Linkage should be done before.

✍**Note:**

An auxiliary input point can bind more than one channel.

14.1.6. Event Type

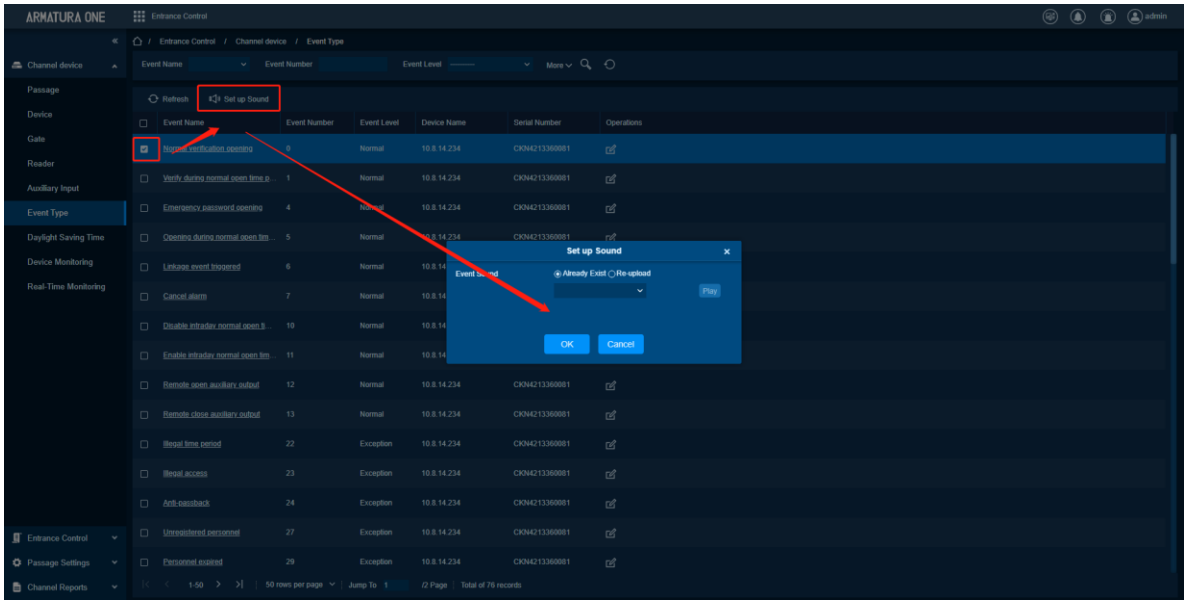
The Event Type is mainly used to display various event types included in the channel device. Click [**Entrance Control**] > [**Channel Device**] > [**Event Type**], and the following interface appears.



Event Type

Set the sound

Here, the user can set the event sound. First, select the event to be set sound and then click [**Set up Sound**] on the page.



Event Type

The audio file can be uploaded locally. The file must be in wav or mp3 format, and the size cannot exceed 10MB.

14.1.7. Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save

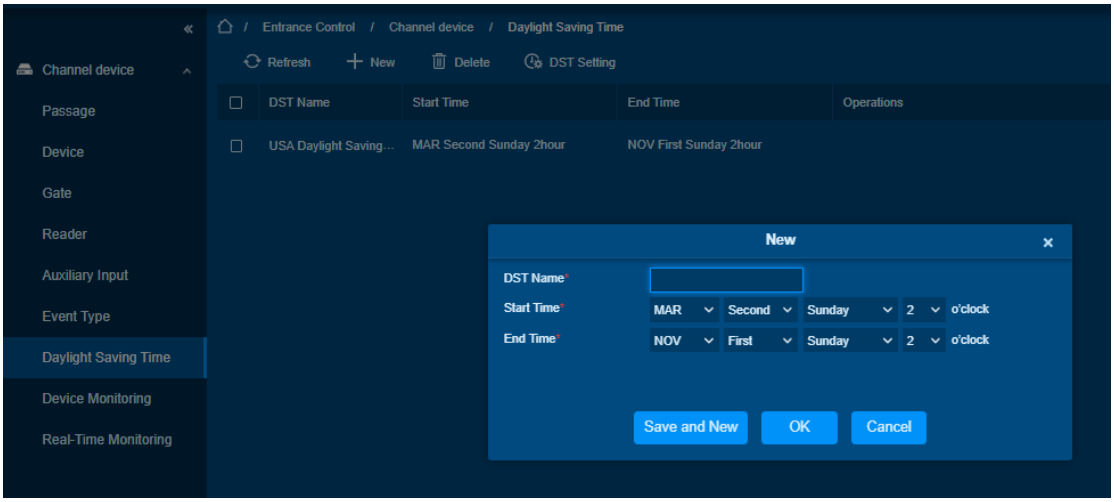
energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. The regulations are different in different countries. At present, nearly 70 countries adopt DST.

To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

Add DST (New)

Step:

Step 1: Click [**Entrance Control**] > [**Channel Device**] > [**Daylight saving Time**] > [**New**].



Daylight Saving Mode

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as “second Monday in March, 02:00”. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Parameter	How to set
DST Name	Any character, a combination of up to 20 characters, cannot be repeated.
Start and End Time	Enter the start and end time. Set as Month-Weeks-week hour: minute format.

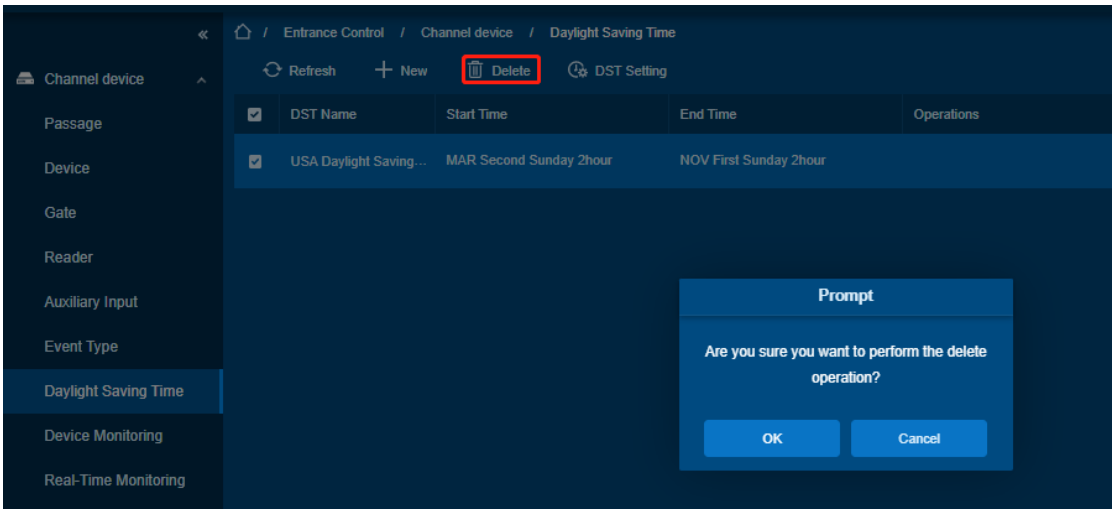
Description of New DST Parameters

Delete

Steps:

Step 1: Click [Entrance Control] > [Channel Device] > [Daylight saving Time] and select DST information to be delete.

Step 2: Click [**Delete**] and click [**OK**] to delete the DST.



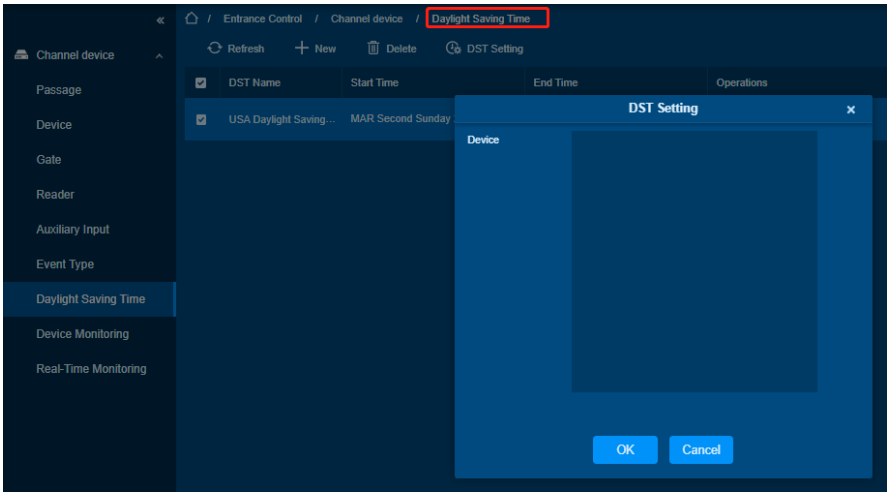
Daylight Saving Mode Delete

DST Setting

Steps:

Step 1: Click [Entrance Control] > [Channel Device] > [Daylight Saving Time] and select DST information to be modify.

Step 2: Click [**DST Setting**] and select device from the appeared window.

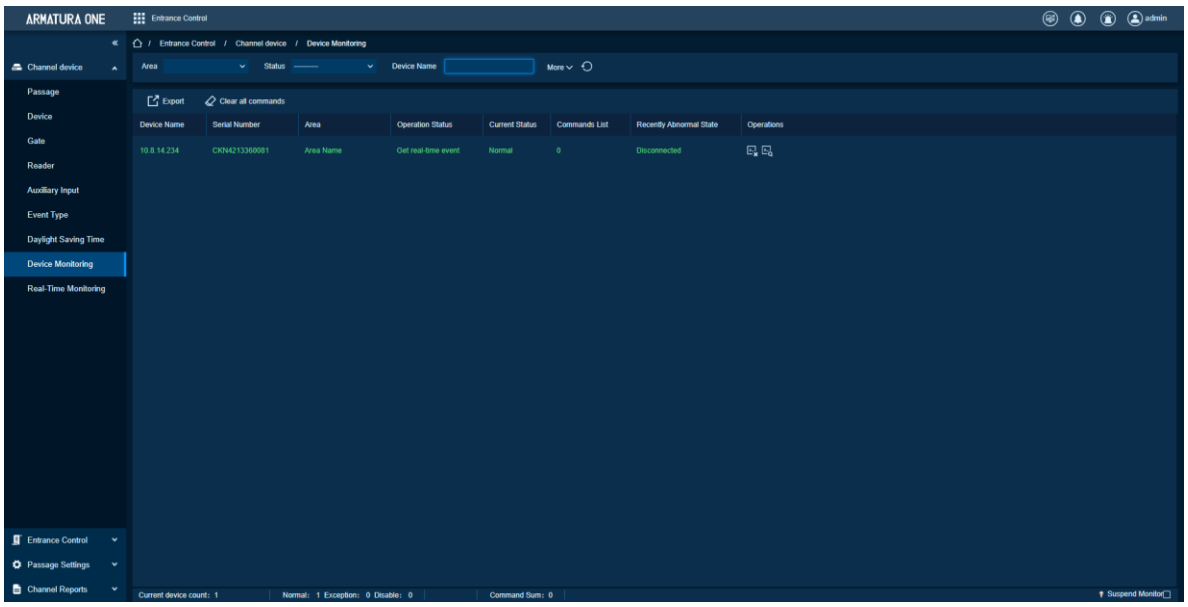


DST Setting

Step 3: Click [**OK**] to save the settings.

14.1.8. Device Monitoring

By default, it monitors all devices within the current user's level. You may click [**Entrance Control**] > [**Channel Device**] > [**Device Monitoring**] to view a list of operation information of devices: Device Name, Serial No., Area, Operation Status, Current status, Commands List, and Related Operation.

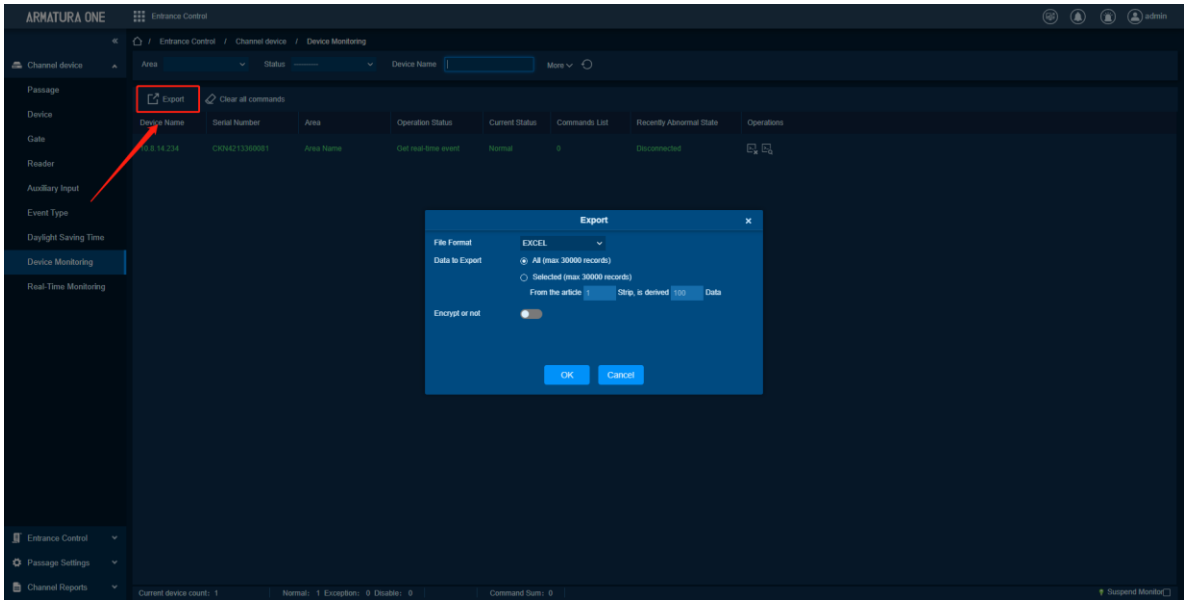


Device monitoring interface

Export

Device commands can be exported in EXCEL, PDF, CSV file format.

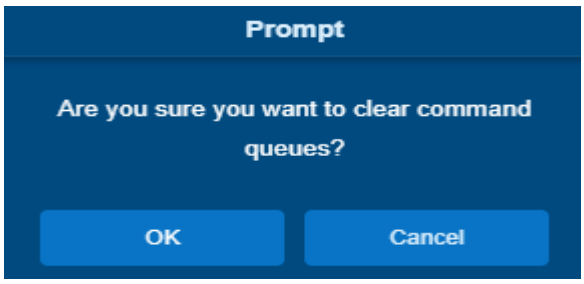
Click [**Entrance Control**] > [**Channel Device**] > [**Device Monitoring**] > [**Export**] to export the device commands.



Device monitoring Export Option

Clear All Command

This option allows the users to clear the unwanted command. Click [**Entrance Control**] > [**Channel Device**] > [**Device Monitoring**] and select the commands to be delete. Click [**Clear All Command**] in operations column.



Device monitoring Clear command

14.1.9. Real-Time Monitoring

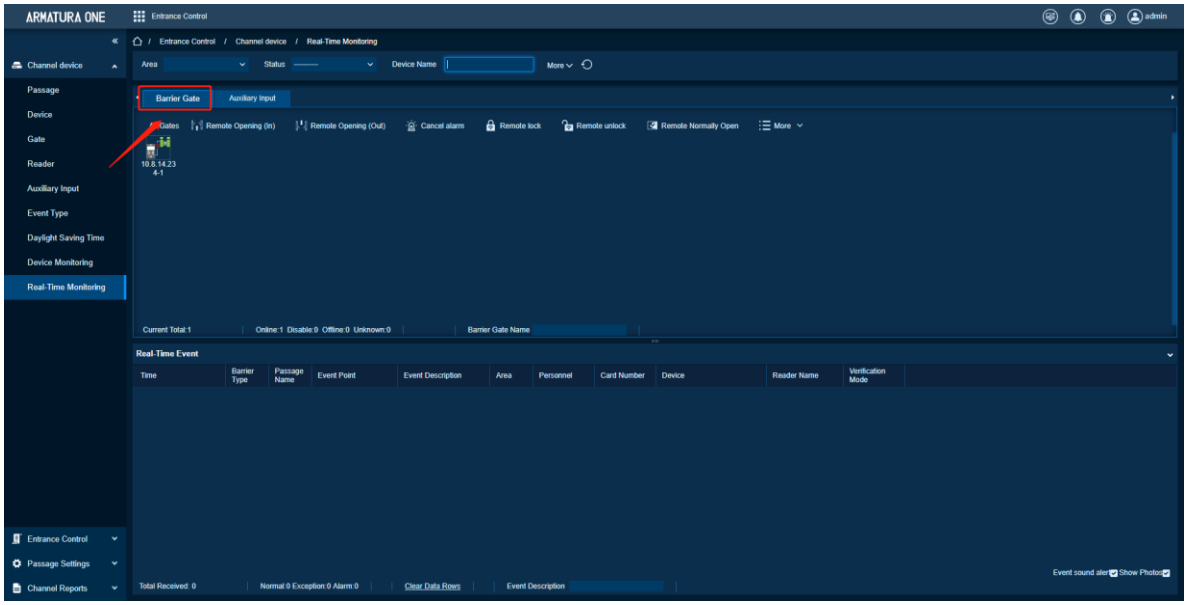
On the real-time management screen, the status of the added device is displayed, and the device can be opened or closed. At the same time, the dynamic of real-time events is monitored. If the gate opening can be verified and corresponding access control events can be generated, the access control management service configuration is complete.

Remote Gate Opening (in)/(out)

In the **Entrance Control** interface, click [**Channel Device**] > [**Real Time Monitoring**] interface allows the user to control one gate or all gates.

Steps:

Step 1: Check whether the device is online. Check whether the icon status of the added device is online. Click [**Barrier Gate**] to check and modify the real-time status of the added devices.



Barrier Gate Option in Real-Time Monitoring Interface

Step 2: Remote opening in/out verification, taking remote opening in as an example. Select the online barrier gate device, click [**Remote opening in**], enter the user password in the pop-up security verification, and click [**OK**].

On the remote door opening screen, enter the time to open the door and tap [**OK**]. If Operation succeeded in is displayed, the remote door opening Operation is complete.

Cancel the alarm

In the **Entrance Control** interface, click [**Channel Device**] > [**Real Time Monitoring**] interface and select the alarm gate to be modified. Then click [**Cancel the Alarm]** to cancel the alarm.

✍**Note:**

If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

Remote Lock

In the **Entrance Control** interface, click Channel Device > Real-Time Monitoring and select the barrier to modify the lock status Then click Remote Lock to activate the door lockdown status (remote lock and unlock).

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by **certain devices.**

Remote Unlock

In the **Entrance Control** interface, click [**Channel Device**] > [**Real-Time Monitoring**] and select the barrier to modify the lock status Then click [**Remote Unlock**] to activate the door lockdown status (remote lock and unlock).

It will unlock a locked door. This function is supported only by certain devices.

Remote Normally Open

It will set the gate as normal open by remote.

In the **Entrance Control** interface, click [**Channel Device**] > [**Real Time Monitoring**] and select the gate to be set as normal open. Then click [**Remote Normal Open**] to set the gate as normal open by remote.

More Options

In the **Entrance Control** interface, click [**Channel Device**] > [**Real-Time Monitoring**] >[**More**] to activate the door lockdown status (remote lock and unlock).

Enable / Disable Intraday Passage Mode Time Zone

In remote opening, user can define the door opening duration (The default is 15s). You can select [**Enable Intraday Passage Mode Time Zone**] to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select [**Disable Intraday Passage Mode Time Zone**] first, to avoid enabling other normal open time zones to open the door, and then select [**Remote Closing**].

Auxiliary Input

In this interface, the user can identify real-time connected sensor devices such as infrared sensors or smog sensors.

To view the list of real-time connected devices, click [**Entrance Control**] **> [Channel Device] > [Real-Time Monitoring**] and select [**Auxiliary Inputs**].

14.2. Entrance Control

By setting the gate authority group and assigning it to the corresponding personnel, the gate authority of the personnel can be controlled. At the same time, it is also possible to set the response rules to the gate through Anti-Passback and linkage, to meet the requirements of different entry and exit scenarios.

14.2.1. Barrier Gate Permission Group

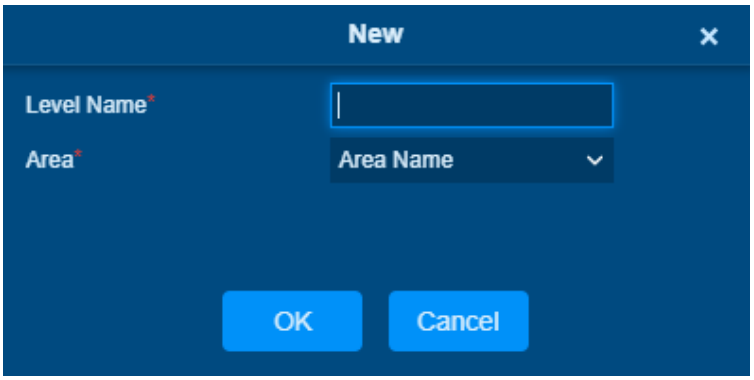
Gates added to the system should be set in the form of permission groups. Set the corresponding permission group, add gates to the permission group, and define the area where the permission group belongs.

To Add Gate Permission (New)

Steps:

Step 1: In the [**Entrance Control**] module, select [**Entrance Control**] > [**Barrier Gate Permission Group**]. In the barrier gate permission group interface, click [**New**] in the left column of the mouse to pop up the gate permission group adding interface.

Step2: In the **New** interface of gate permission group, set the corresponding content according to the new requirements, as shown in below. Please refer to table for parameter filling instructions.



Add Gate Permission Group Interface

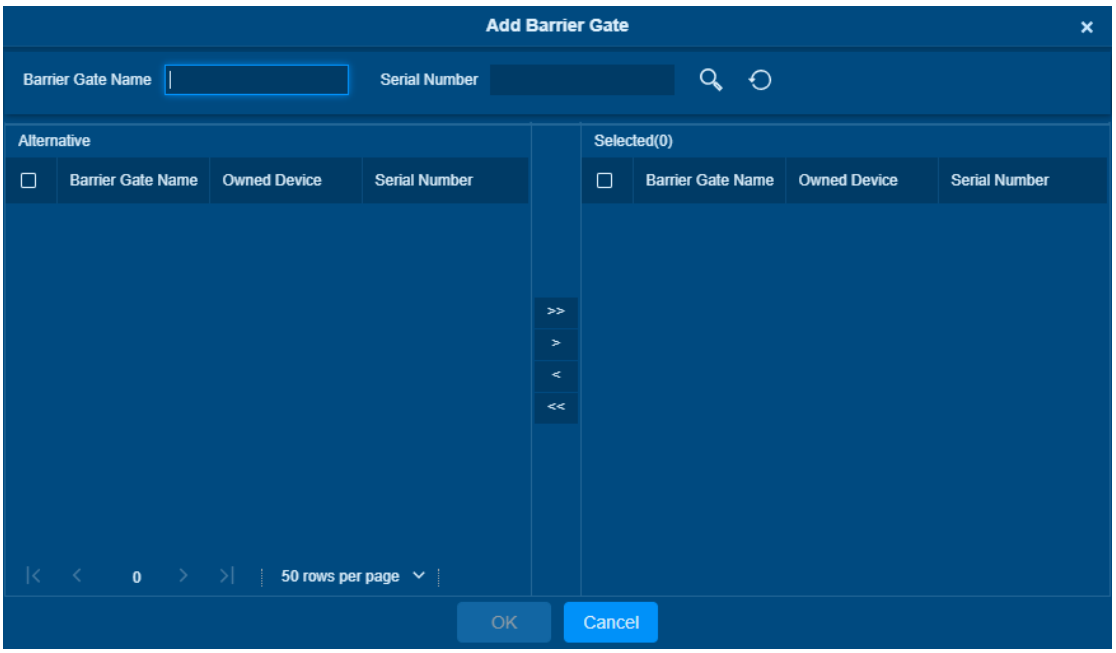
Parameter	How to set
Level Name	Any character, a combination of up to 20 characters, cannot be repeated.
Area	Permission groups belong to a zone to which users assigned permissions can manage permission groups under the zone.

Description of Added Gate Permission Parameters

Step 3: Click [**OK**] to complete the configuration of the access level.

Step 4: In the gate permission group interface, click [**Add Barrier Gate**] icon on the right side of the

created gate permission group, and the interface of selecting Add Gate will pop up, and the corresponding gate will be added according to the requirements, as shown in below.



Adding Gate Interface

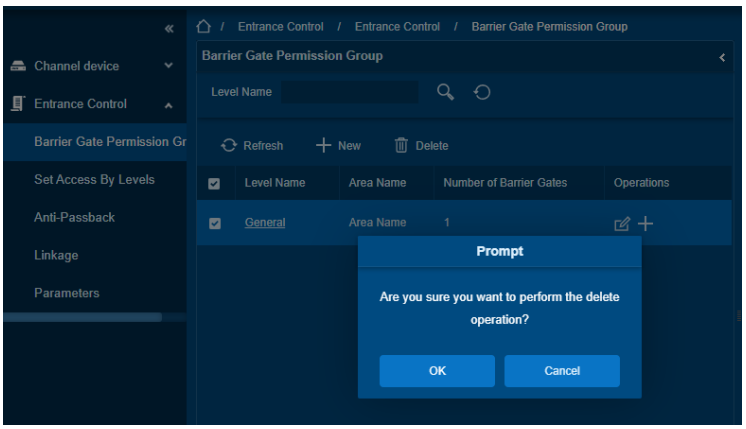
Step 5: Click [**OK**] to complete the setting of gate permissions.

Delete

Steps:

Step 1: Click [**Entrance Control**] > [**Entrance Control**] > [**Barrier Gate Permission Group**] and select gate permission group to be delete.

Step 2: Click [**Delete**] and click [**OK**] to delete gate permission group.



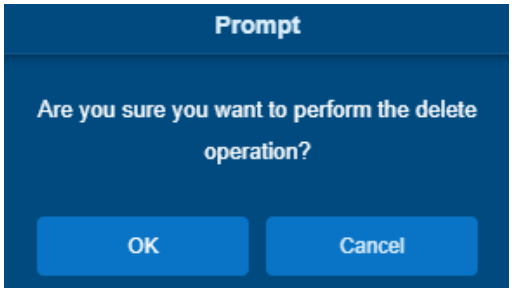
Deleting Gate Interface

Delete Barrier Gate

Steps:

Step 1: Click [**Entrance Control**] > [**Entrance Control**] > [**Barrier Gate Permission Group**] and select barrier gate name to be delete.

Step 2: Click [**Delete**] and click [**OK**] to delete barrier gate from the group.



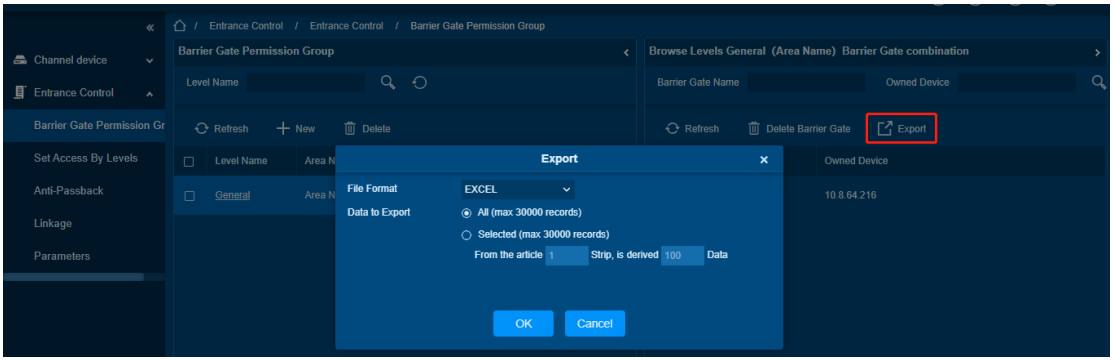
Delete Barrier Gate

Export

You can export barrier gate details into an Excel, PDF, or CSV file. See the figure below.

Steps:

Step 1: In [**Entrance Control**] > [**Entrance Control**] > [**Barrier Gate Permission Group**] > [**Export**] to export the barrier gate records to Excel sheet or PDF or CSV. Enter the User password in the prompt.



Export Interface

Step 2: Select the file format and click [**OK**].

14.2.2. Set Access By Levels

Assign the added gate permission group to the person.

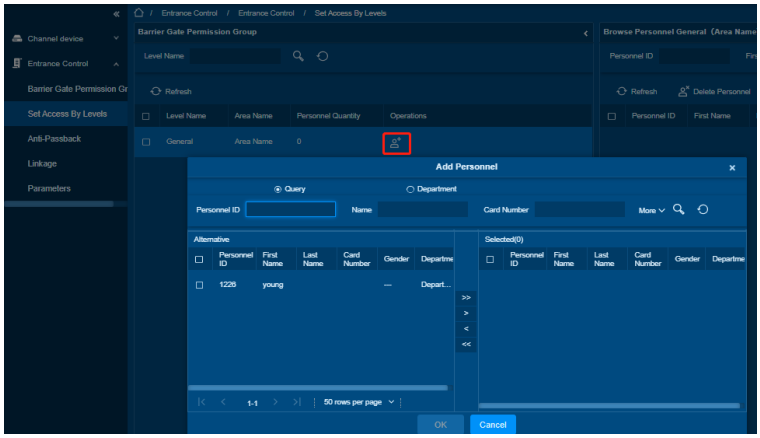
Introduces the operation Steps of allocating personnel authority according to authority group in software.

Add Person

Steps:

Step 1: In the **Entrance Control** module, click [**Entrance Control**] > [**Set Access By Levels**].

Step 2: Click [**Add Person**] icon in the operation bar of the corresponding permission group to open the interface of adding person. Select the corresponding person as needed, as shown in below.



Add Person Option

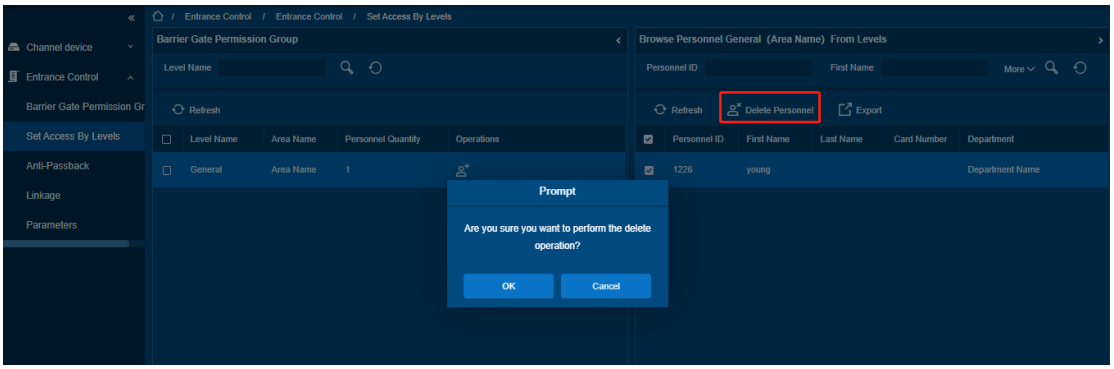
Step 3: Click [**OK**] to complete the assignment of personnel permissions.

Delete Personnel

Steps:

Step 1: Click [**Entrance Control**] > [**Entrance Control**] > [**Set Access By Levels**] and select person to be delete.

Step 2: Click [**Delete Personnel**] and click [**OK**] to delete barrier gate from the group.



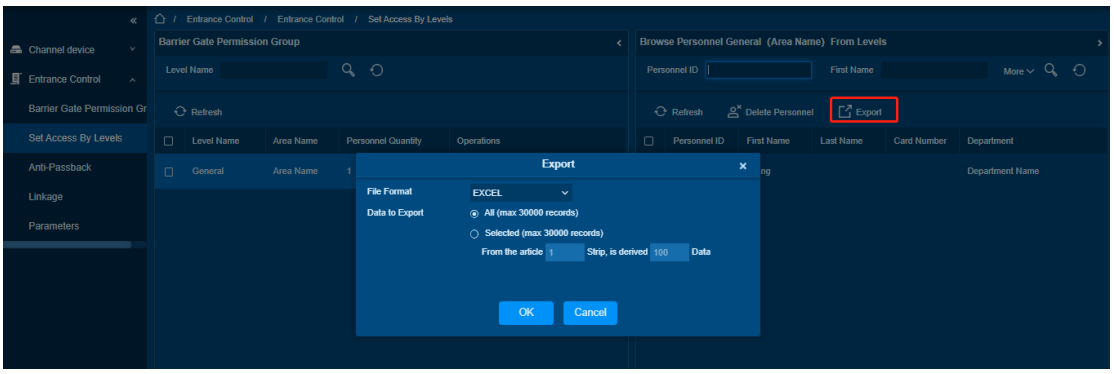
Delete Person

Export

You can export barrier gate details into an Excel, PDF, or CSV file. See figure below.

Steps:

Step 1: In [**Entrance Control**] > [**Entrance Control**] > [**Set Access by Levels**] > [**Export**] to export the persons records to Excel sheet or PDF or CSV. Enter the User password in the prompt.



Export Interface

Step 2: Select the file format and click [**OK**].

14.2.3. Anti-Passback

At present, it supports Anti-Passback in and out. On some occasions, people who require card swiping verification must swipe their cards from another channel when they come in from one channel, and the card swiping records must be strictly corresponding to one entry and one exit. Users can use this function when they enable it in settings, which is generally used in special units, scientific research, bank vaults and other occasions.

To Add Anti-Passback

This paper introduces the configuration Steps of adding Anti-Passback effect in.

Steps:

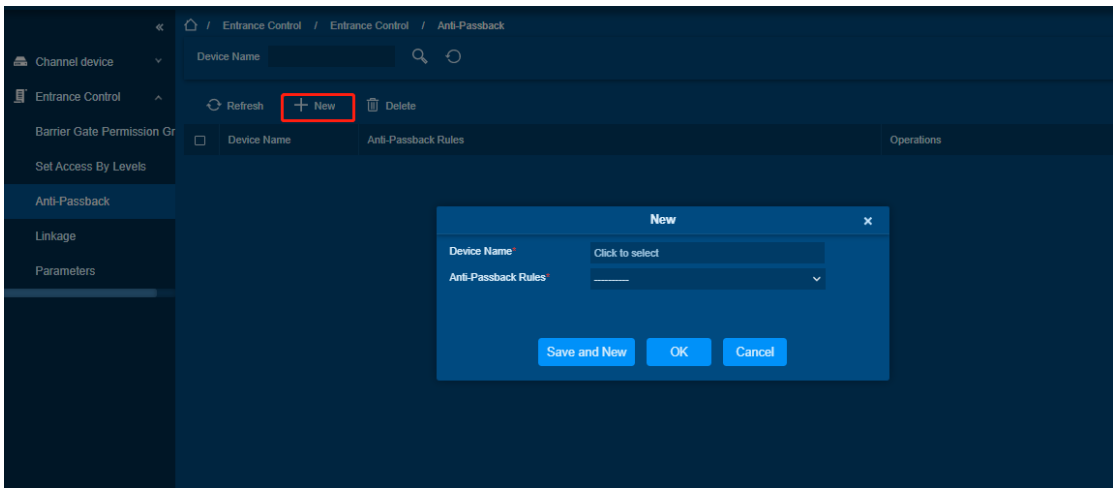
Step 1: In the **Entrance Control** module, select [**Entrance Control**] > [**Anti-Passback**] and Click **New**.

Step 2: Select the specified device.

Description

When adding Anti-Passback, you can't see the device that has been set up in Anti-Passback in the device list. After deleting the set Anti-Passback information, the device returns to the device list. Anti-Passback settings of all-in-one machine: Anti-Passback, Anti-Passback and Anti-Passback.

Step 3: Select the Anti-Passback rule and click [**OK**] to complete the setting, as shown in below. The newly added Anti-Passback settings are displayed in the list of selected Anti-Passback rules.



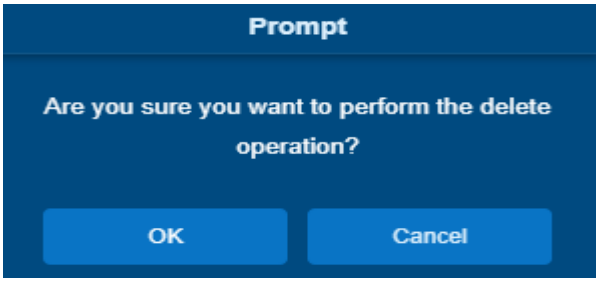
Add Anti-Passback Interface

Delete

Steps:

Step 1: Click [**Entrance Control**] > [**Entrance Control**] > [**Anti-Passback**] and select device name to be delete.

Step 2: Click [**Delete**] and click [**OK**] to delete Anti-passback from the group.



Delete Anti-Passback

14.2.4. Linkage

After a specific event is triggered at a certain input point in the channel system, a linkage action will be generated at the specified output point to control the events such as verification opening, alarm and anomaly in the system, which will be displayed in the corresponding event list monitored.

Precondition:

You must do the following steps before linking new configurations:

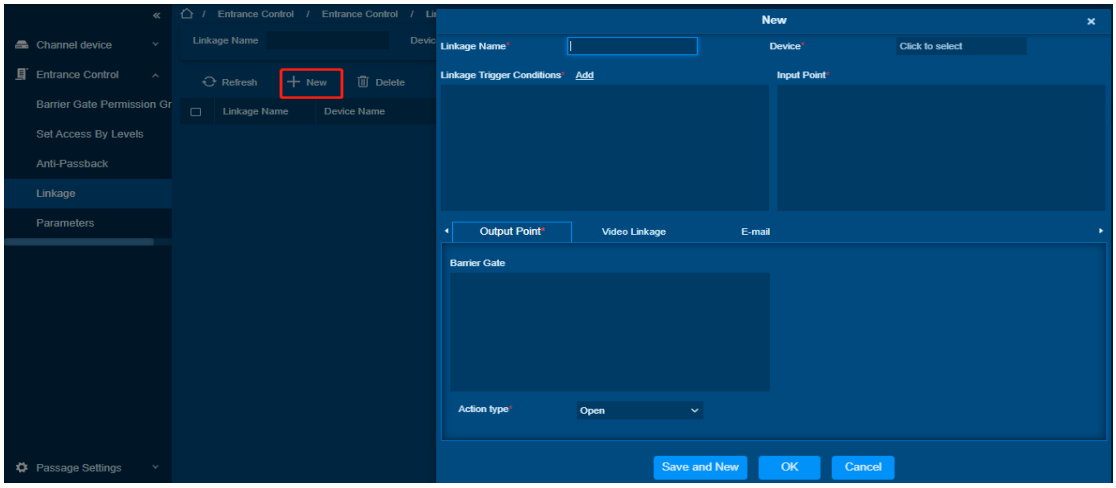
1. Gate device, input point, output point, read head binding camera add settings.
2. Mailbox parameter configuration.

Add Linkage

Steps:

Step 1: In the **Entrance Control** module, select [**Entrance Control**] > [**Linkage**].

Step 2 : In the linkage setting interface, select and click the [**New**] button to fill in the corresponding parameters, as shown in below. Please refer to table for linkage parameters.



New Linkage Interface

Parameter	Description
Linkage name	Custom setting linkage name for easy reference.
Device	Customize and select the added access control device.
Linkage trigger Conditions	Select the condition under which the linkage operation is triggered, that is, the type of event generated by the selected device.
Input point	Select the input point to set the device input.
Output point	Select the output point to set the output of the device.
Action Type	Choose to set up linkage action, including device operation of output point, video linkage and mail. Refer to Table 14-5 for configuration description of the three modes.

Description of New Linkage Parameters

Parameter	How to set
Output point operation	Set the action type of output point: closed, open and normally open. Sets the delay time if the output point action is on.
Video linkage	Pop-up video, display duration: check the pop-up video in the real-time monitoring interface and set the pop-up duration.

Parameter	How to set
	Video recording and video recording duration: Check to record and set the video recording duration. Capture: Set whether the linkage action takes pictures: If you take pictures, you also need to set whether it pops up in the real-time monitoring interface and the display time.
E-Mail	Set the email address of the received linkage content when the linkage event occurs.

Explanation of Output Action Parameters

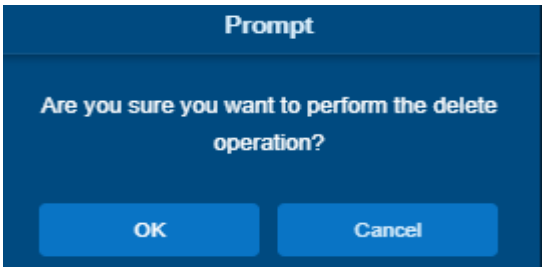
Step 3: Click [**OK**] to complete the linkage configuration.

Delete

Steps:

Step 1: Click [**Entrance Control**] > [**Entrance Control**]> [**Linkage**] and select the linkage name to be delete.

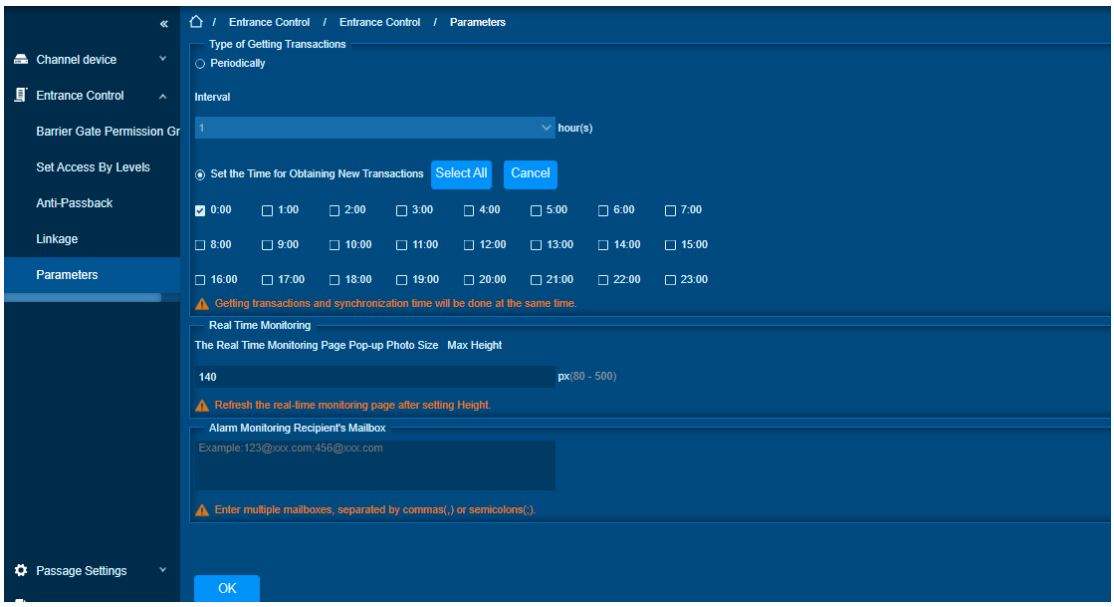
Step 2: Click [**Delete**] and click [**OK**] to delete linkage.



Delete Linkage

14.2.5. Parameters

Click [**Entrance Control**] > [**Entrance Control**]> [**Parameter**] to enter the parameter setting interface.



Add Parameters

Type of Getting Transactions

1. **Periodically:**

   Start from the setting and efficient time, the system attempts to download new transactions every time interval.

2. **Set the Time for Obtaining New Transactions:**

   The selected Time is up, the system will attempt to download new transactions automatically.

3. **The Real Time Monitoring Page Pop-up Staff Photo Size:**

   When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

4. **Alarm Monitoring Recipient Mailbox:**

   The system will send email to alarm monitoring recipient's mailbox if there is any event.

14.3. Passage Settings

Software can directly manage the gate function by maintaining the gate traffic rules (control time period and traffic mode) and setting the gate parameters appropriate to the gate.

14.3.1. Barrier gate passing Rules

Set the passage time and passage mode of the gate, so that the gate can set different entry and exit passage modes in different time periods. It can be applied to flap Barrier and swing Barrier.

Add Barrier Gate Passing Rules

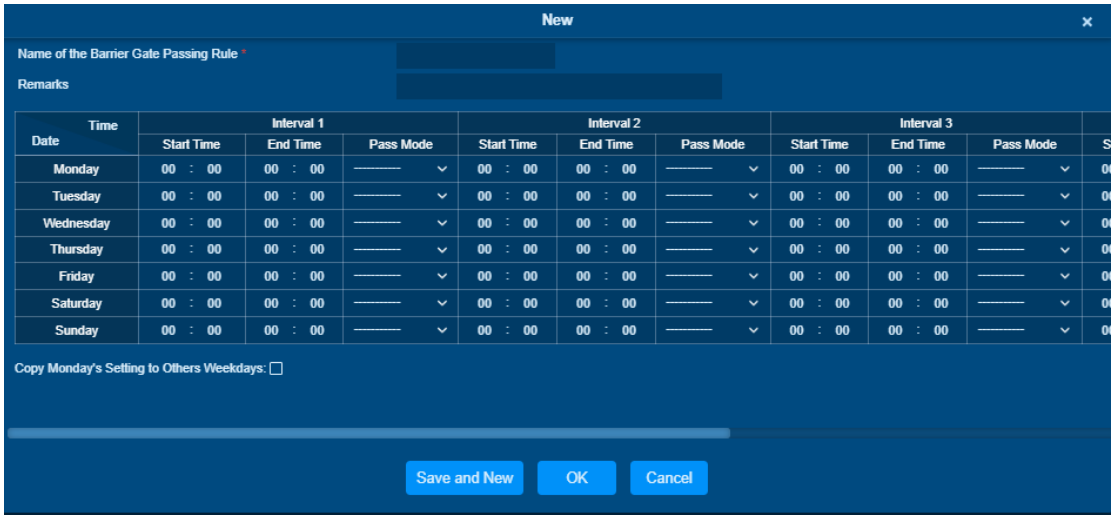
This section describes the steps for configuring gate traffic rules in Software.

Steps:

Step 1: In the **Entrance Control** module, select [**Passage Settings**] > [**Barrier Gate Passing Rules**].

Step 2: Click [**New**] and the interface for adding gate traffic rules will pop up.

Step 3: In the new interface, set the corresponding contents according to the new requirements, as shown in below. Please refer to table for parameter setting instructions.



Interface of Adding Gate Traffic Rules

Parameter	How to set
Name of the Barrier Gate Passing Rules	Any character, up to 30 characters.
Remarks	The explanation of the current period and the main application occasions shall consist of 5 0 characters at most.
Time interval	A gate passage rule contains up to 5 intervals in a week.
Time Interval-Start/End time	Set the start and end time in each time interval.
Pass Mode	Set the traffic mode in each time interval and select it from drop-down. There are 10 traffic modes by default: "Two-way controlled", "free entry and exit controlled", "controlled entry and exit free", "two-way freedom", "forbidden entry and exit controlled", "forbidden entry and exit free entry", "free entry and exit forbidden entry", "two-way

	prohibition", "remote normal opening".
Copy Monday time to other working days	You can quickly copy Monday settings to other workdays.

Parameter Description of Gate Traffic Rules

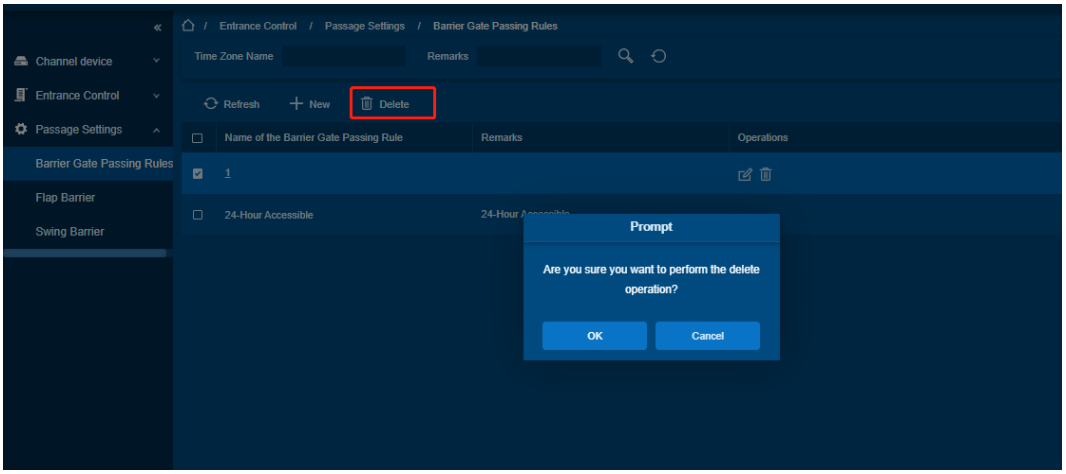
Step 4: Click [**OK**] to complete the addition of the gate traffic rules.

Delete Passage

Steps:

Step 1: In the **Entrance Control** module, select [**Passage Settings**] > **[Barrier Gate Passing Rules**]. and select the rule to be deleted.

Step 2: Click [**Delete**] to delete the selected rule.



To Delete Barrier Gate Passage Rule

Step 3: Click [**OK**] to perform the delete operation.

14.3.2. Flap Barrier

This section describes the steps for parameter configuring of Wing Barrier in Software.

Steps:

Step 1: In the **Entrance Control** module, select [**Passage Settings**] > [**Flap Barrier**].

Step 2: In the flap Barrier interface, click the [**Edit**] button under the name or operation of the flap Barrier to enter the flap Barrier parameter editing interface.

Step 3: Click [**OK**] to complete the configuration of flap Barrier parameters.

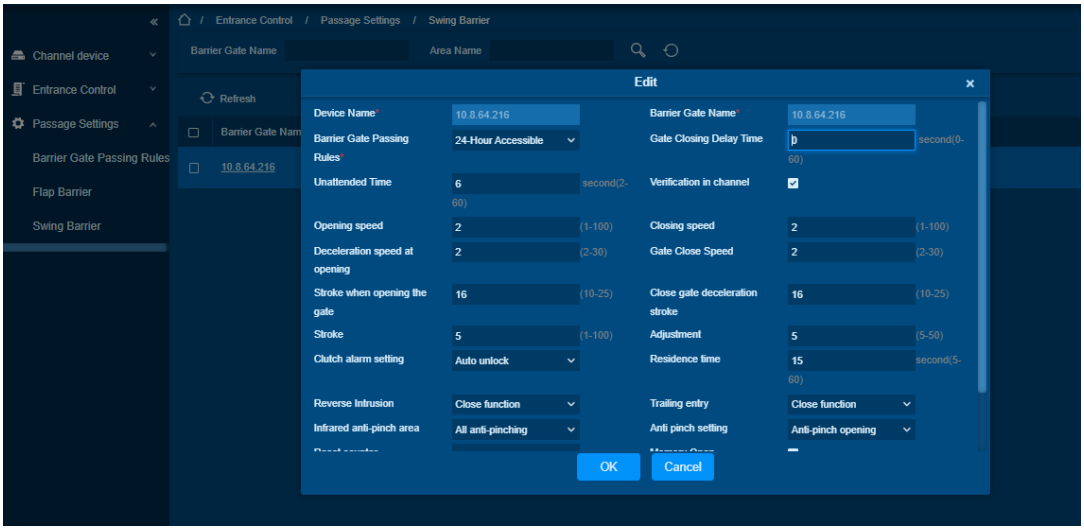
14.3.3. Swing Barrier

This section describes the steps for parameter configuring of swing Barrier in Software.

Steps:

Step 1: In the **Entrance Control** module, select [**Passage Settings**] > [**Swing Barrier**].

Step 2: In the swinging interface, click the [**Edit**] button under the swinging name or operation to enter the swinging parameter editing interface, as shown in below.



Swing Barrier Parameter Configuration Interface

Step 3: Click [**OK**] to complete the configuration of wing Barrier parameters.

The devices PGIC supports:

Device Name	Remark
SBT2011S	Only use as Access controller
SBT2022S	Only use as Access controller
SBTL7011	Only use as Access controller
SBTL7022	Only use as Access controller
SBTL9000	Access controller and turnstile gates controller.
SBTL9011	Access controller and turnstile gates controller.
SBTL9022	Access controller and turnstile gates controller.
SBTL9200	Access controller and turnstile gates controller.

SBTL9211	Access controller and turnstile gates controller.
SBTL9222	Access controller and turnstile gates controller.
Mars Pro-S1000	Access controller and turnstile gates controller.
Mars Pro-S1011	Access controller and turnstile gates controller.
Mars Pro-S1022	Access controller and turnstile gates controller.
Mars Pro-S1200	Access controller and turnstile gates controller.
Mars Pro-S1211	Access controller and turnstile gates controller.
Mars Pro-S1222	Access controller and turnstile gates controller.
Mars Pro-F1011	Only use as Access controller
Mars Pro-F1022	Only use as Access controller
MarsPro-F1211	Only use as Access controller
Mars Pro-F1222	Only use as Access controller
Mars-B1011	Only use as Access controller
Mars-B1022	Only use as Access controller
Mars-B1211	Only use as Access controller
Mars-B1222	Only use as Access controller
Mars-S1011	Only use as Access controller
Mars-S1022	Only use as Access controller
Mars-S1211	Only use as Access controller
Mars-S1222	Only use as Access controller
Mars-F1011	Only use as Access controller
Mars-F1022	Only use as Access controller
Mars-F1211	Only use as Access controller

Mars-F1222	Only use as Access controller

Description of Swing Barrier Parameters

14.4. Channel Reports

In the Channel report, you can query the All Transactions, Today's Access Records, Person's Last Access Location, and All Exception Events. You can choose to export all or export records after querying.

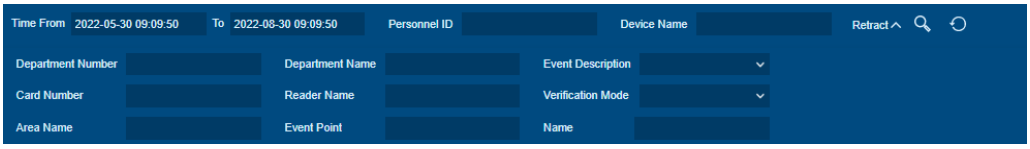
14.4.1. All Transactions

This section describes the steps for configuring of more report, export and clearing all transaction report.

Steps:

Step 1: In the Entrance Control module, select [Channel Reports]> [All Transactions].

Step 2: In the All Records interface, fill in the corresponding query information and click the [**More**] symbol to complete the query of all record tables, as shown in below

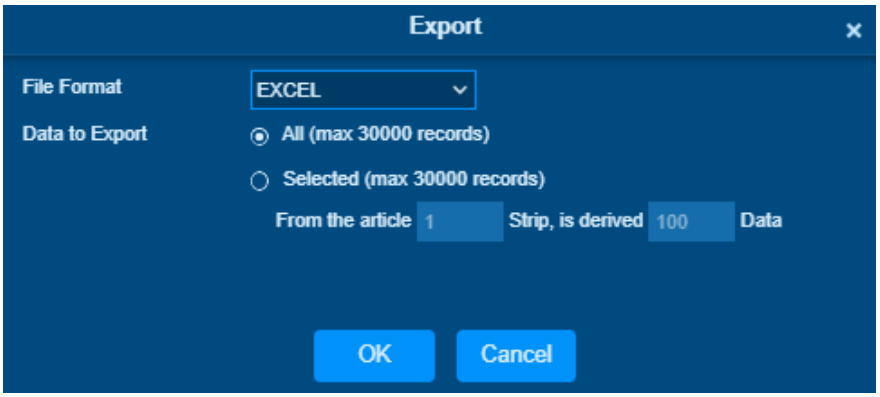


All Transactions

Export

Steps:

Step 1: In the full record interface, click [**Export**], enter the user password in the pop-up security verification, and click [**OK**]. Select whether to encrypt and export the file format, and Click [**OK**], as shown in below.

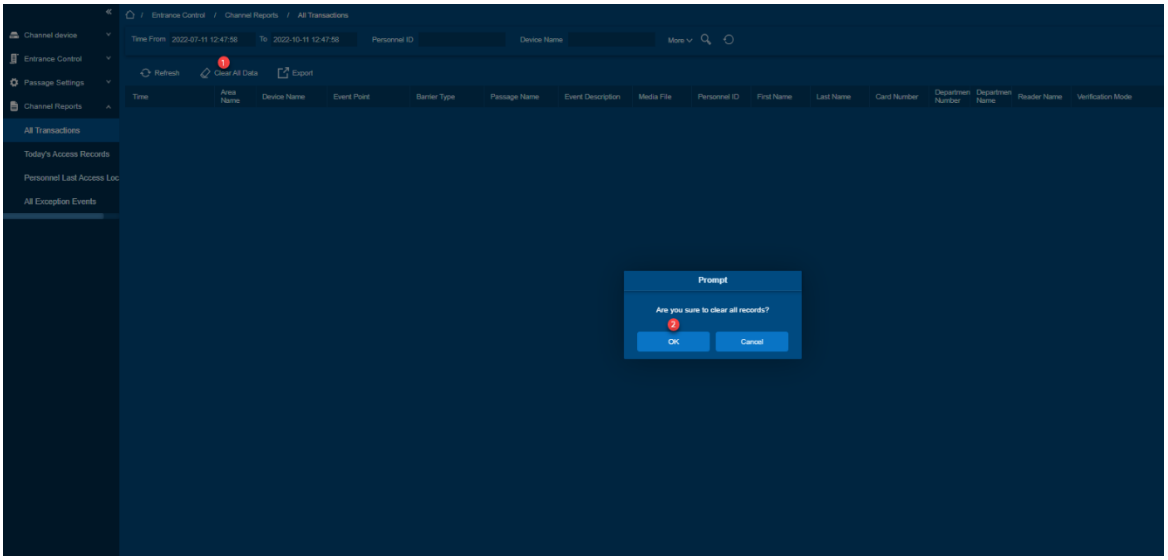


Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

Clear All Data

Click [**Clear All Data**] to pop up prompt, click [**OK**] to clear all transection reports.



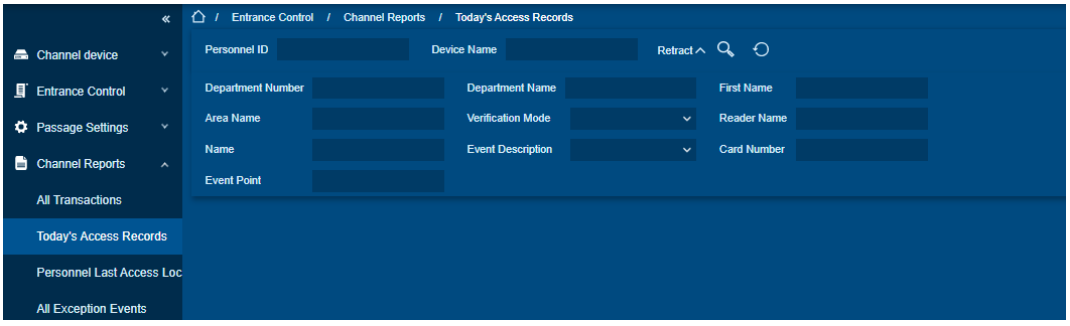
14.4.2. Today's Access Records

The access records for today are displayed in this option.

Steps:

Step 1: In the **Entrance Control** module, select [**Channel Reports**] > [**Today's Access Record**].

Step 2: In Today's Access Record interface, fill in the corresponding query information and click the [**More]** symbol to complete the query of access record tables, as shown in below.

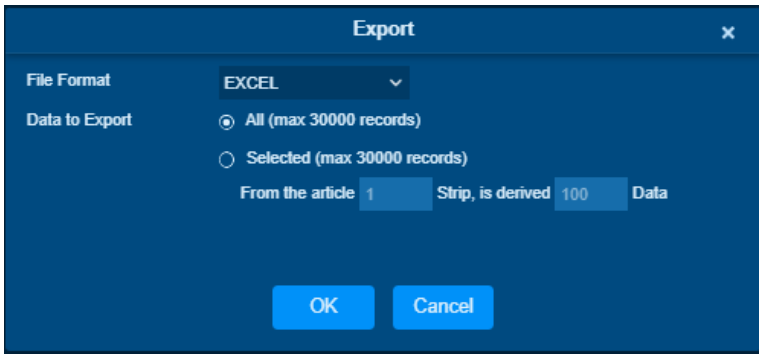


Today's Access Record

Export

Steps:

Step 1: In the access record interface, click [**Export**], enter the user password in the pop-up security verification, and click [**OK**]. Select whether to encrypt and export the file format, and Click [**OK**], as shown in below.

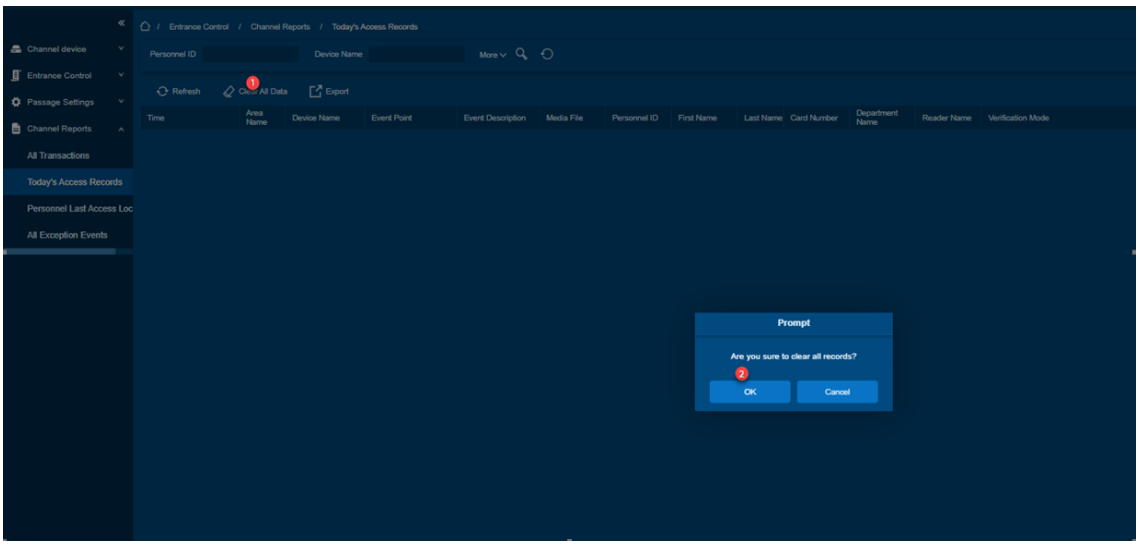


Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

Clear All Data

Click [**Clear All Data**] to pop up prompt, click [**OK**] to clear all access records.



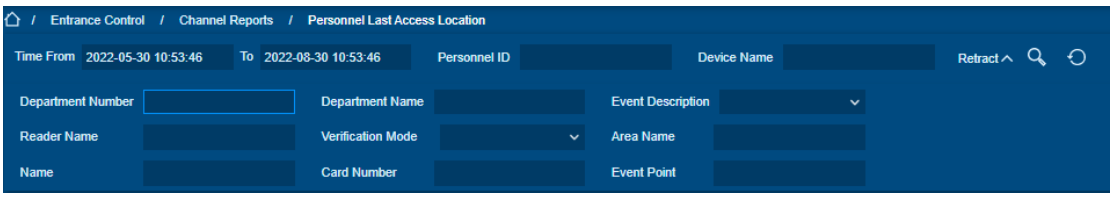
14.4.3. Personnel Last Access Location

Displays the last location visited by persons with access rights. It is convenient for users to quickly locate the location of personnel.

Steps:

Step 1: In the **Entrance Control** module, select [**Channel Reports**] > [**Personnel Last Access Location**].

Step 2: In Personnel Last Access Location interface, fill in the corresponding query information and click the [**More**] symbol to complete the query of access record tables, as shown in below.

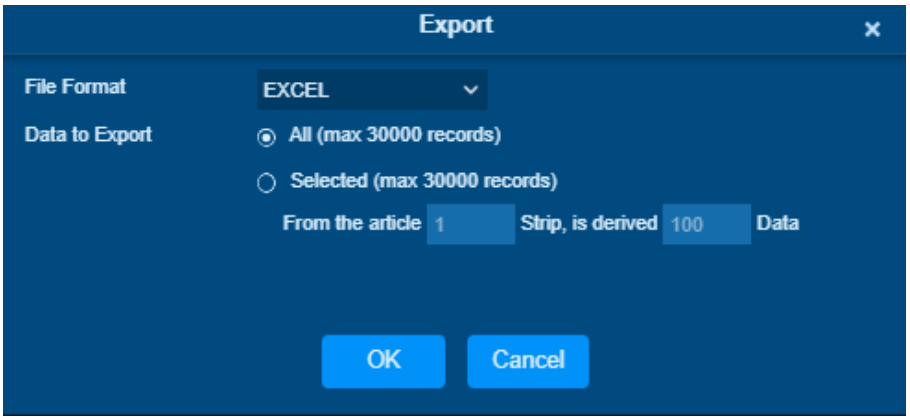


Today's Access Record

Export

Steps:

Step 1: In the access location interface, click [**Export**], enter the user password in the pop-up security verification, and click [**OK**]. Select whether to encrypt and export the file format, and Click [**OK**], as shown in below.

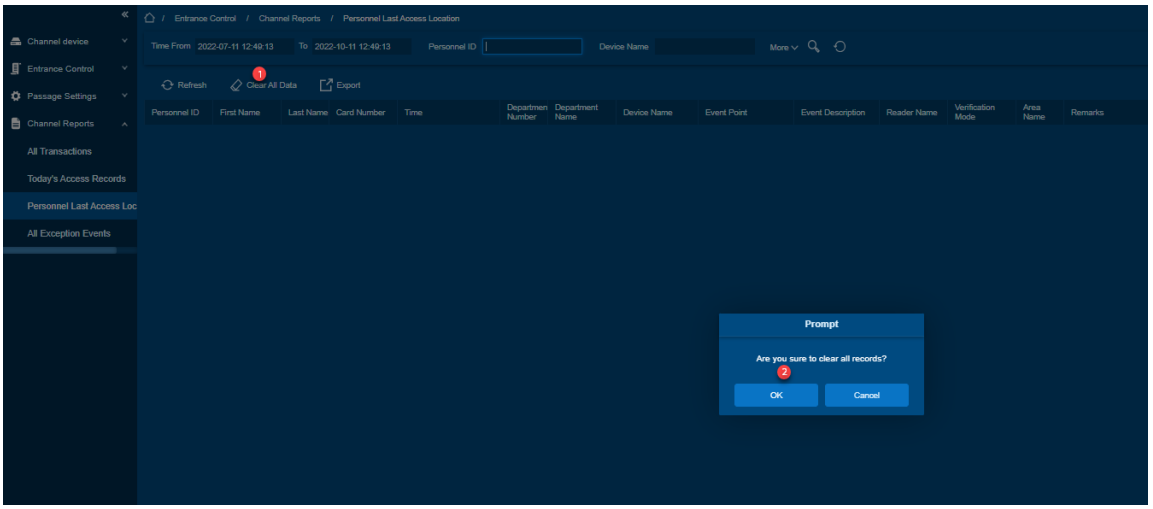


Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

Clear All Data

Click [**Clear All Data**] to pop up prompt, click [**OK**] to clear all personal last access location data.



14.4.4. All Exception Events

Click [**Channel Report**] > [**All Exception Events**] to view the abnormal events (including alarm events) such as unregistered persons, illegal entry, gate opening timeout, and failure to connect to the server under specified conditions (including alarm events).

Steps:

Step 1: In the **Entrance Control** module, select [**Channel Reports**] > [**All Exception Events**].

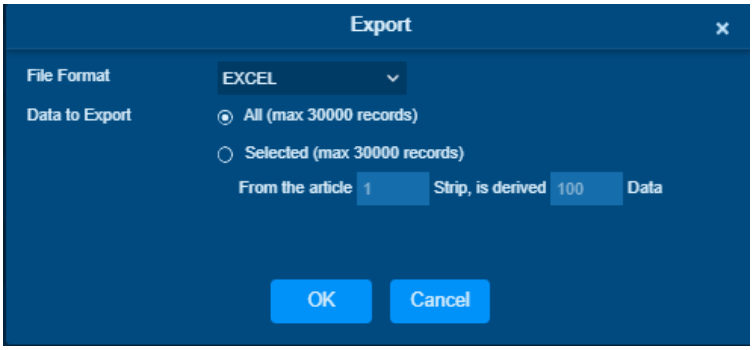
Step 2: In All Exception Events interface, fill in the corresponding query information and click the **[More]** symbol to complete the query of access record tables, as shown in below.

All Exception Events

Export

Steps:

Step 1: In the All-Exception Events interface, click [**Export**], enter the user password in the pop-up security verification, and click [**OK**]. Select whether to encrypt and export the file format, and Click [**OK**], as shown in below.

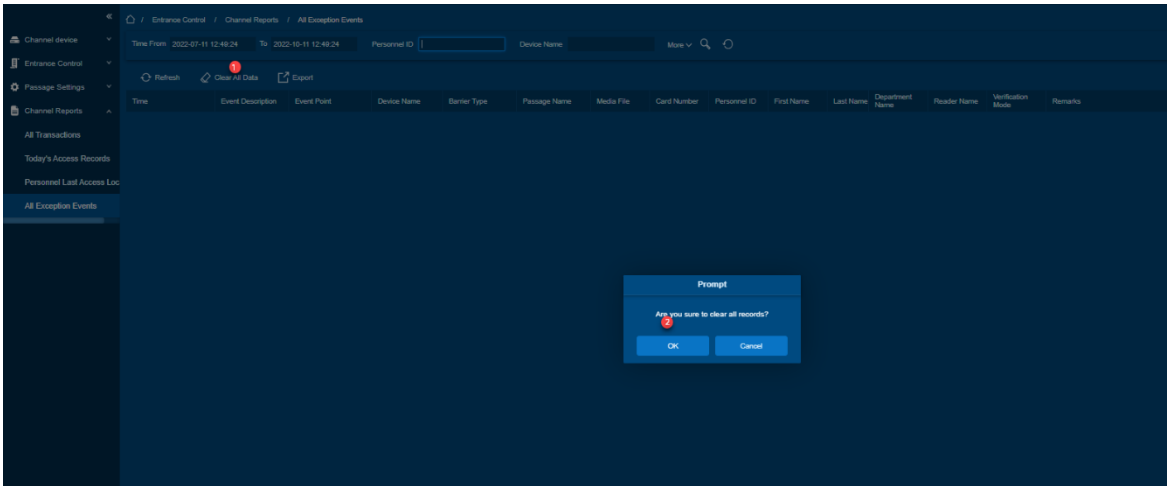


Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

Clear All Data

Click [**Clear All Data**] to pop up prompt, click [**OK**] to clear all exception events.



15. FaceKiosk Module

As a large-screen media display device, the FaceKiosk can display advertisement announcement information through the FaceKiosk and can use as an identification device for non-inductive attendance and personnel monitoring. The FaceKiosk module connects to the FaceKiosk device, allowing you to configure the FaceKiosk area personnel as and the FaceKiosk displays advertising resources, etc.

15.1. FaceKiosk Device

Function Description

It manages the system FaceKiosk device, supports operations such as adding device, delete after searching, setting the FaceKiosk Device Status, and obtaining FaceKiosk Device Data.

Function List

Operations	Description
Device	FaceKiosk device can delete, search, enable, disable, restart, synchronize software data to Device, and send QR code address, get device parameters, view device parameters, re-upload data, get designated personnel data, clear device command, clear Verify photo, clear verification record operation.
Set by Region	Synchronize personnel in the area, add Personnel, and delete personnel in the area
Set by Personnel	Add area and delete area by person

15.1.1. Device

FaceKiosk device can delete, search, enable, disable, restart, synchronize software data to Device, and send QR code address, get device parameters, view device parameters, re-upload data, get designated personnel data, clear device command, clear Verify photo, clear verification record operation.

Searching Device

Preconditions for Normal Use of Function

The FaceKiosk Device needs to set the service address, service port and communication port first.

Function Usage Scenarios

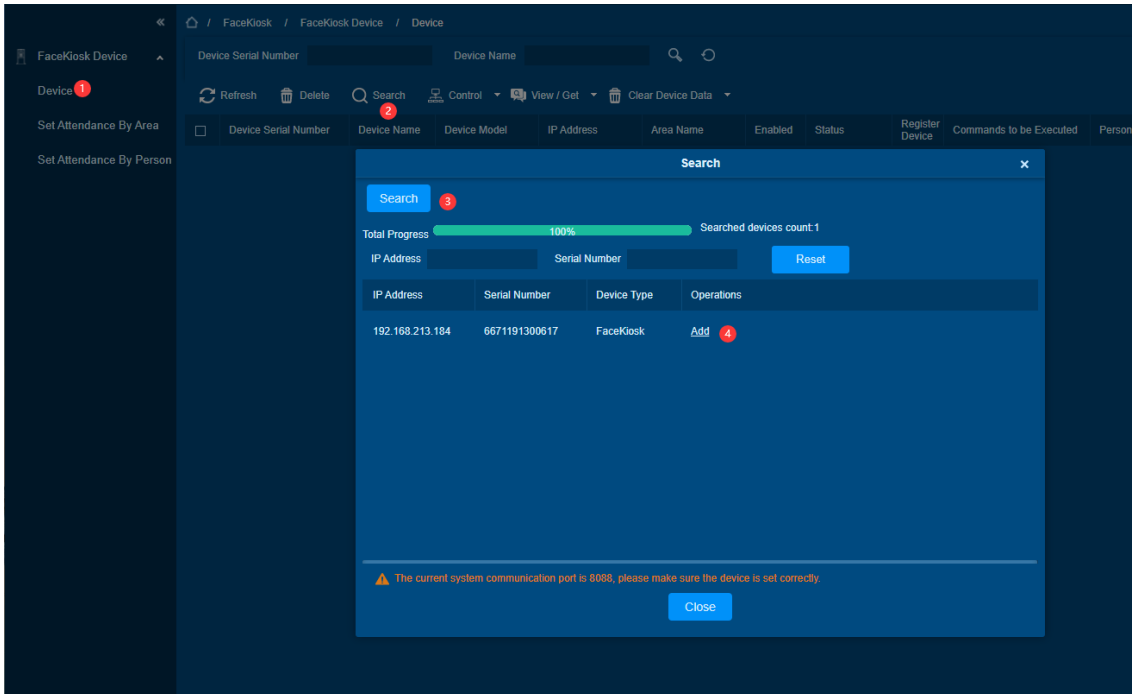
It is used to search software data of the device.

Feature Trigger Result

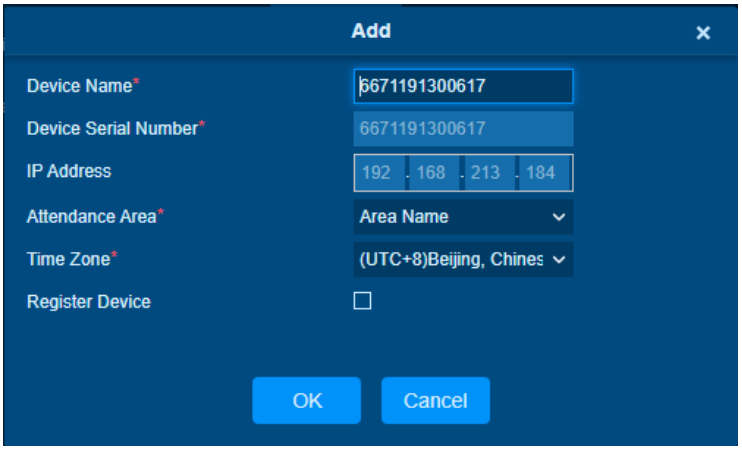
Add elevator control device information, able to operate device.

Steps:

Click [**Device**] > [**Search**] then search window will pop up as shown in figure.



Select the Device to be added and click the [**Add**] button to enter the add editing interface.



Device Name: Set the Device Name.

Device Serial Number: It display the serial number of the Device on the FaceKiosk.

IP Address: It display the IP Address of the Device on the FaceKiosk.

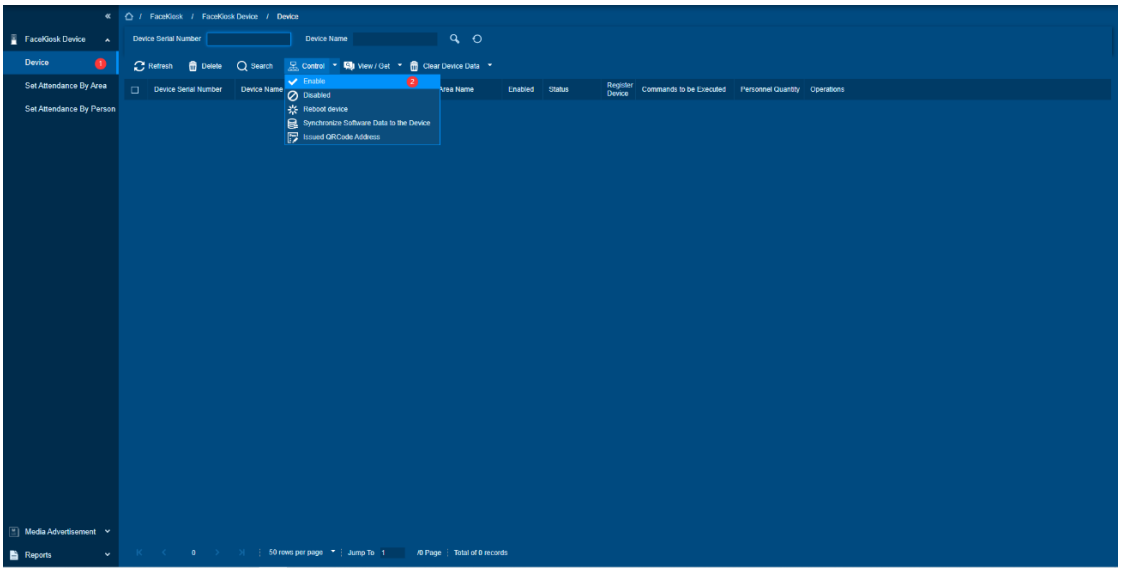
Attendance Area: Select the area of the FaceKiosk Device.

Time Zone: Select the Time Zone of the FaceKiosk Device.

Register Device: Check the FaceKiosk Device as the Registration Machine.

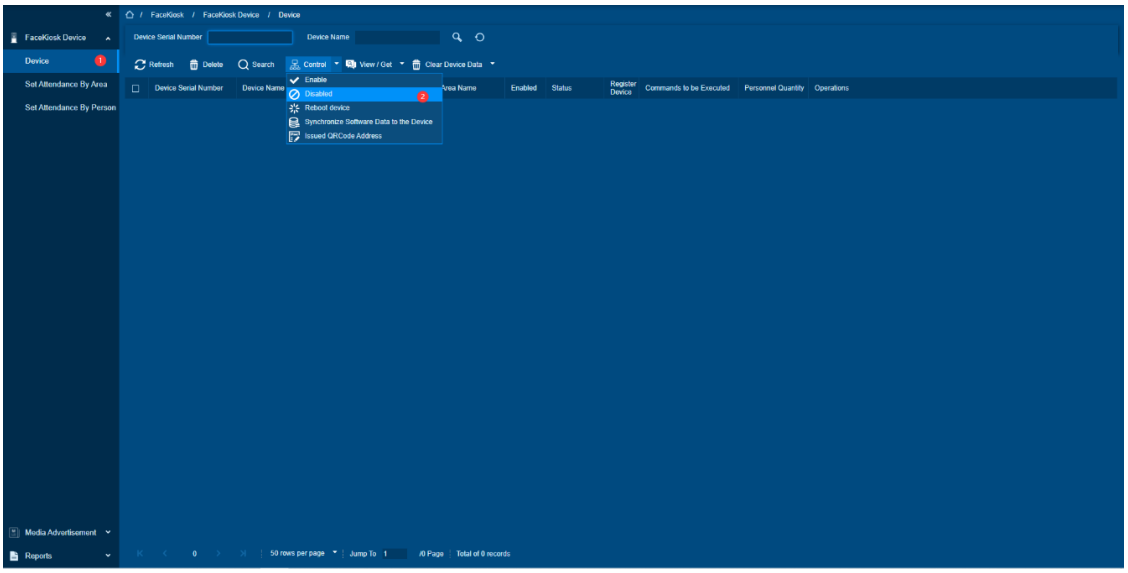
Enable

Check the FaceKiosk Device that needs to be enabled, click the [**Device Control**] button, and select **[Enable]**.



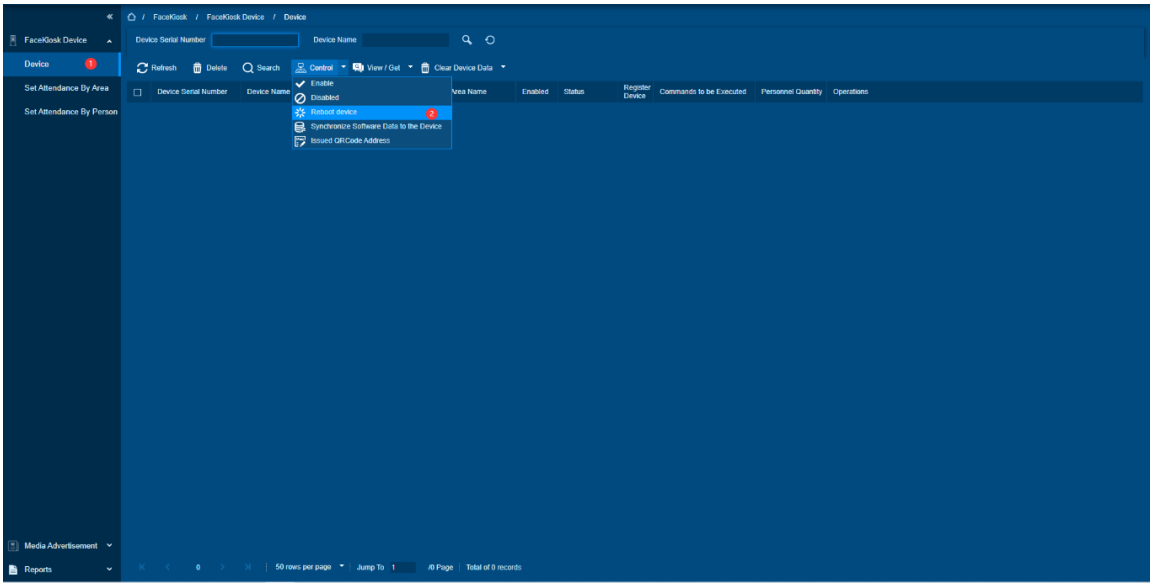
Disable

Check the FaceKiosk Device that needs to be disabled, click the **[Device Control]** button, and select **[Disable]**.



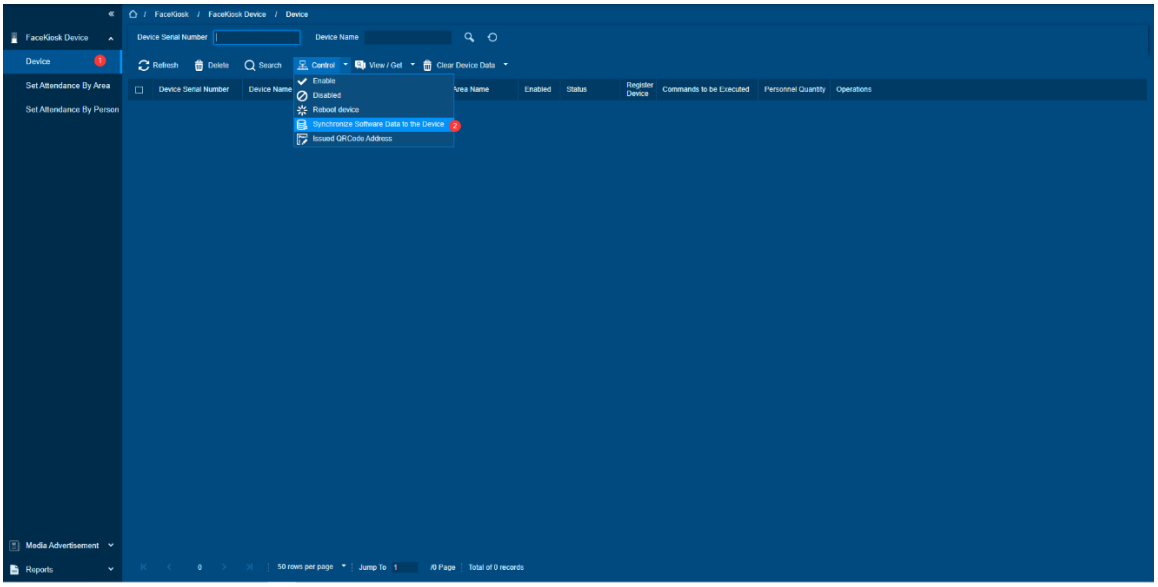
Restart Device

Check the FaceKiosk Device that needs to be restarted, click the [**Device Control**] button, and select to restart the FaceKiosk Device. The device needs to be restarted to restart the device.



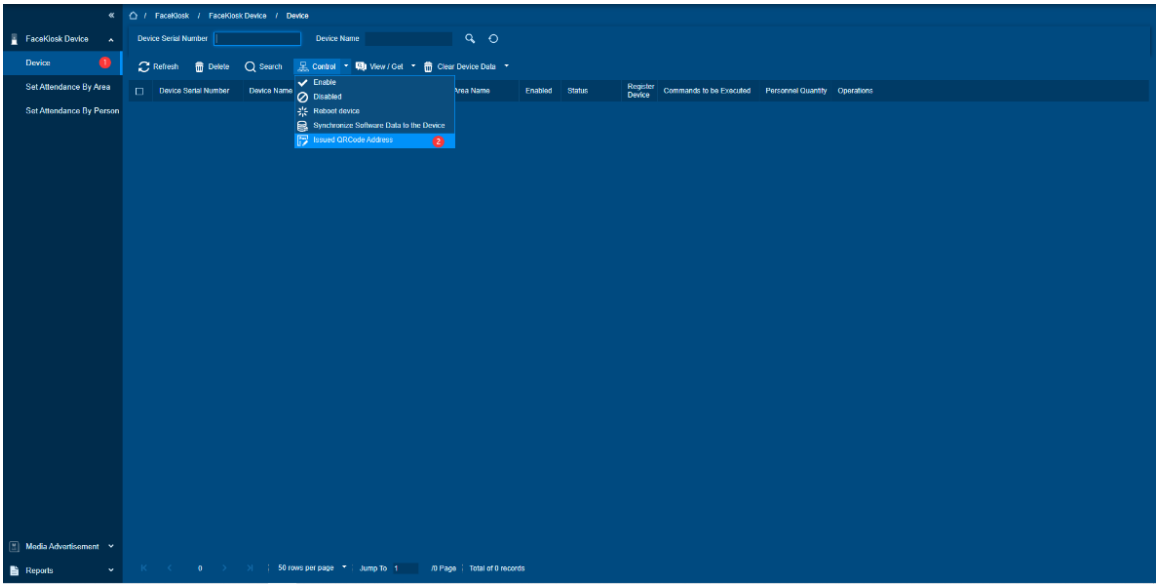
Synchronize software data to Device

Check the FaceKiosk Device that needs to be Synchronized, click the [Device Control] button, and click to synchronize software data to the FaceKiosk Device.



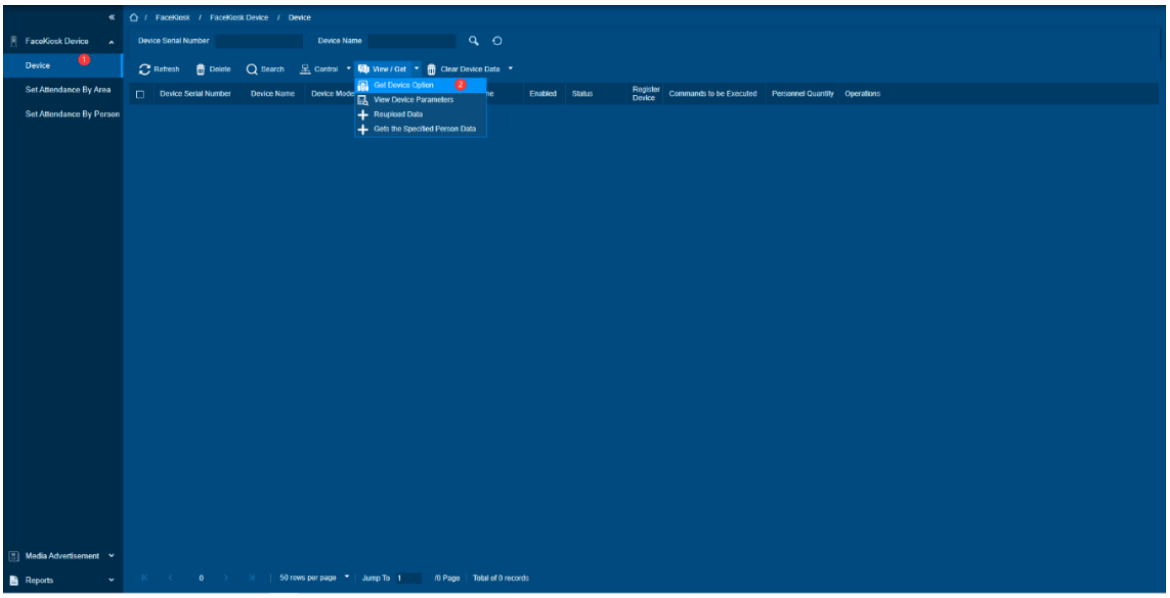
Synchronize software data to Device

Check the FaceKiosk Device that needs to send the QR code URL, click the [**Device Control**] button, select the QR Code Address to be sent to the FaceKiosk Device, fill in the URL of the QR Code, and click [**OK**].



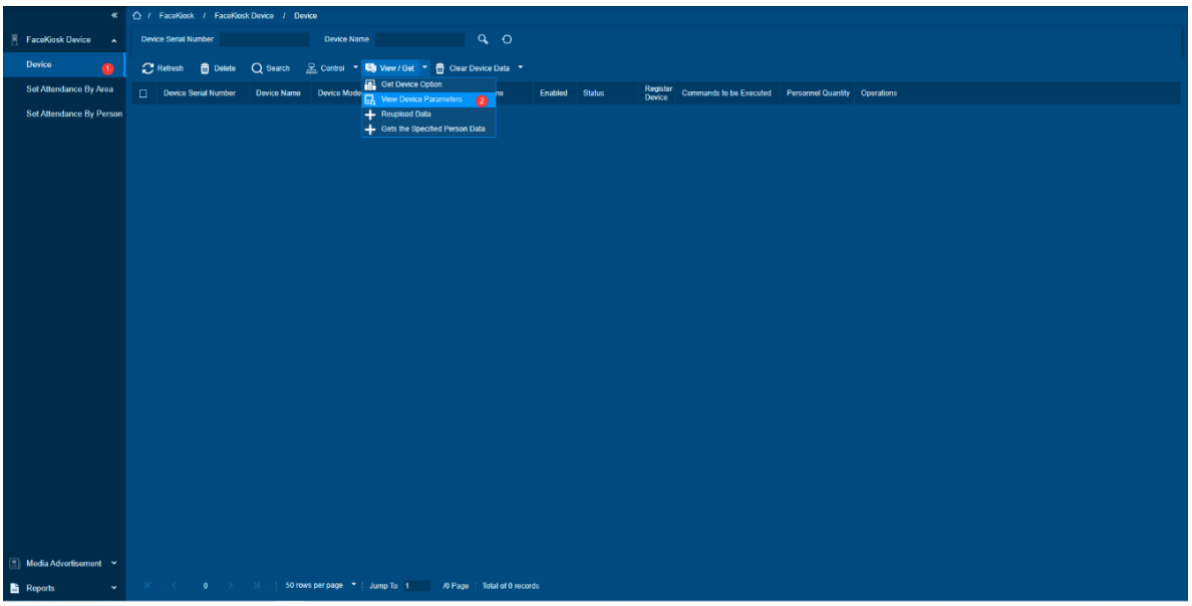
Get Device parameters

Check the FaceKiosk Device that needs to get Parameters, click the [**View and Get**] button, select get Device Parameters, and click [**OK**] to get the FaceKiosk Device Parameters.



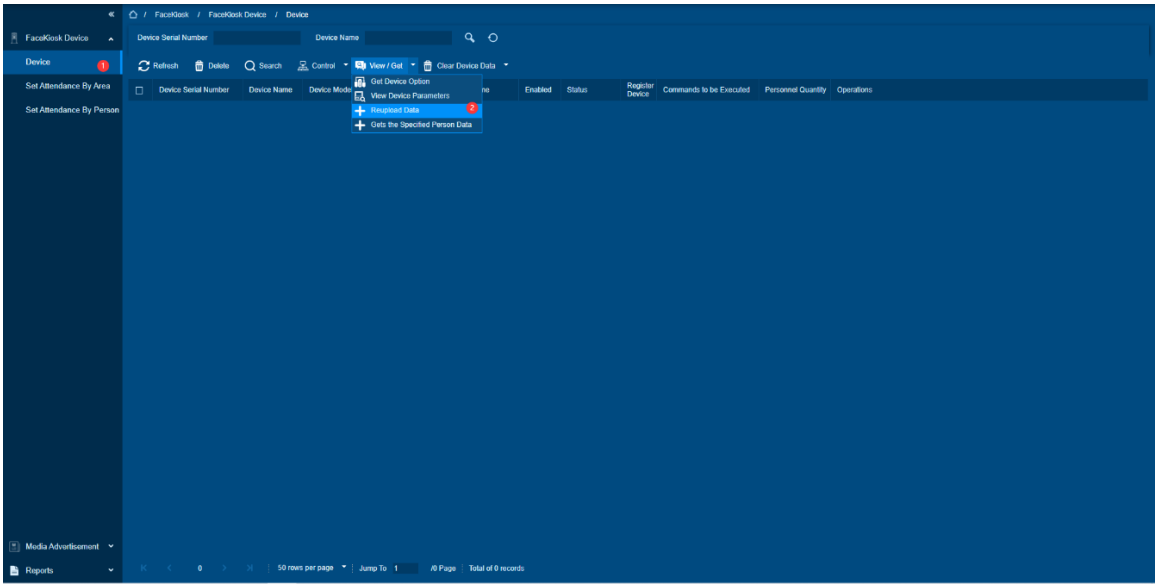
View Device Parameters

Check the FaceKiosk Device that needs to view the Device Parameters, click the [**View and Get**] button, and select View Device Parameters to display the Device Parameter Information.



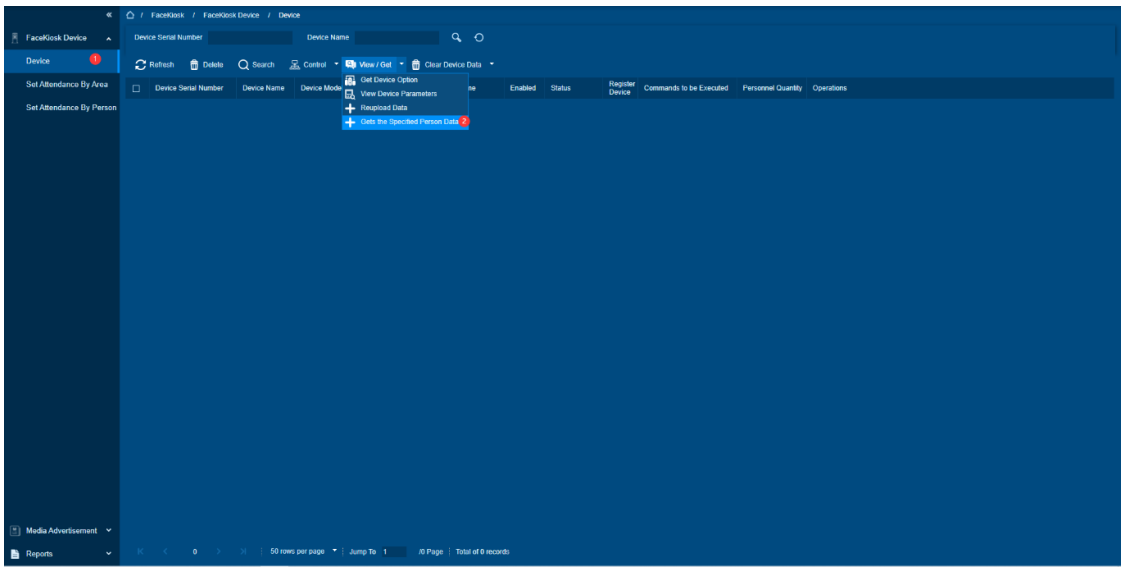
Re-upload Data

Check the FaceKiosk Device that needs to Re-upload data, click the [**View and Get**] button, and select Re-upload data. In the pop-up information box, you can choose to upload verification records, personnel information, and personnel photos as needed.



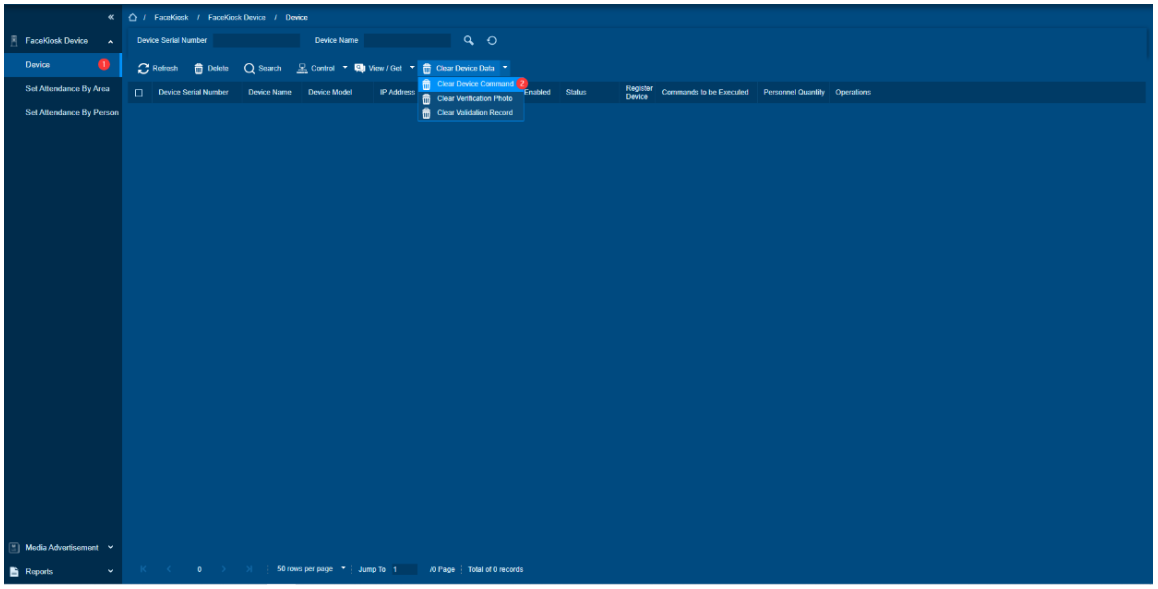
Obtain Designated Personnel Data

Check the FaceKiosk Device that needs to Re-upload data, click the **[View and Get]** button, select to obtain the specified personnel data, and enter the personnel number in the pop-up information box. If there are multiple personnel numbers, separate them with commas.



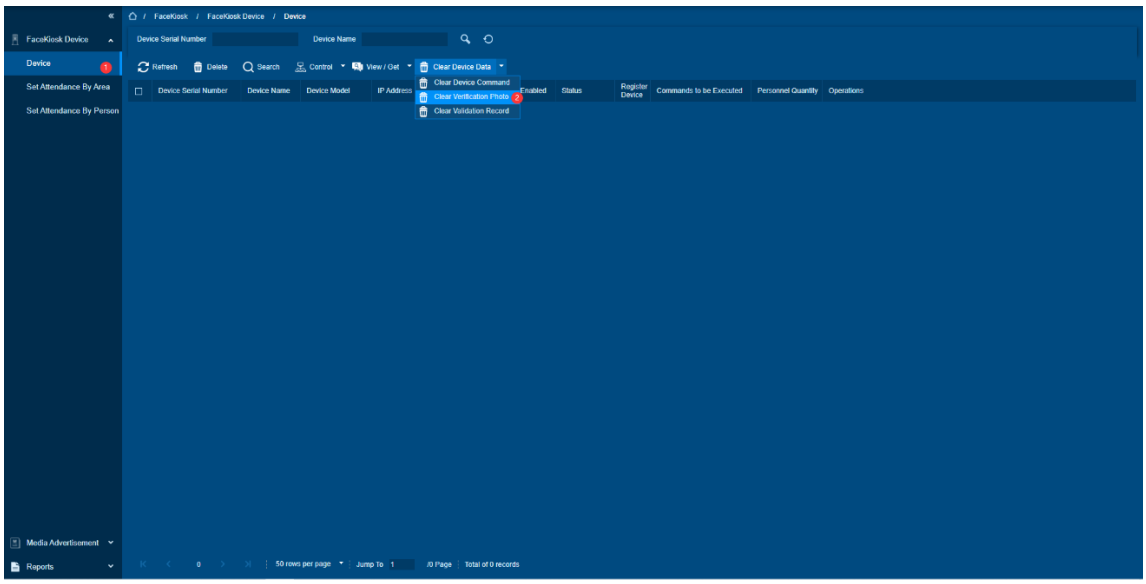
Clear Device Command

Check the FaceKiosk Device that needs to clear the Device Command, click the **[Clear Device Data]** button, and select the clear device command to clear the device command.



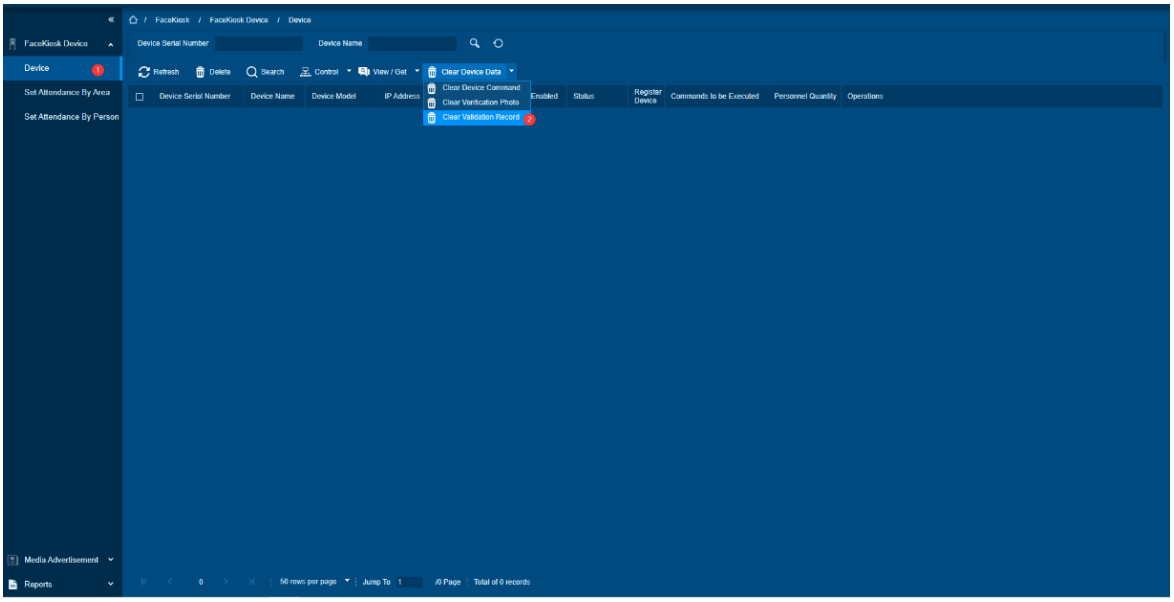
Clear Verification Photos

Check the FaceKiosk Device that needs to clear the verification photos, click the [**Clear Device Data**] button, and select Clear Verification Photos to clear the verification photos in the device.



Clear verification records

Check the FaceKiosk Device that needs to clear the verification record, click the **[Clear Device Data]** button, and select Clear Verification Record to clear the verification record in the device.



15.1.2. Set Attendance By Area

Preconditions for Normal Use of Function

Add FaceKiosk device.

Function Usage Scenarios

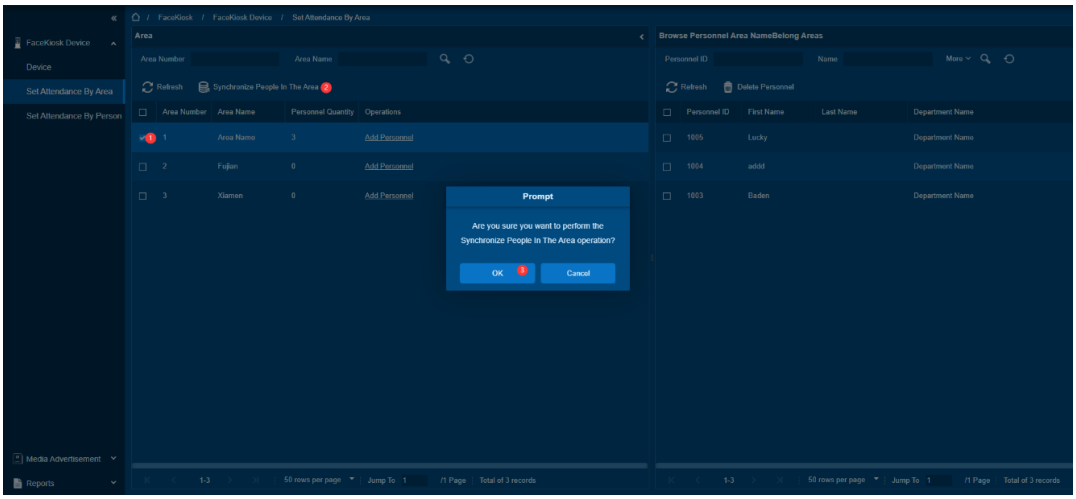
It used to synchronize people in the area.

Feature Trigger Result

People in the area are synchronized to the FaceKiosk device.

Steps:

- Select an area and click [**Synchronize People in The Area**].
- Click [**OK**] to sync these people to FaceKiosk device.



15.1.3. Set Attendance By Person

Preconditions for Normal Use of Function

Add FaceKiosk device.

Function Usage Scenarios

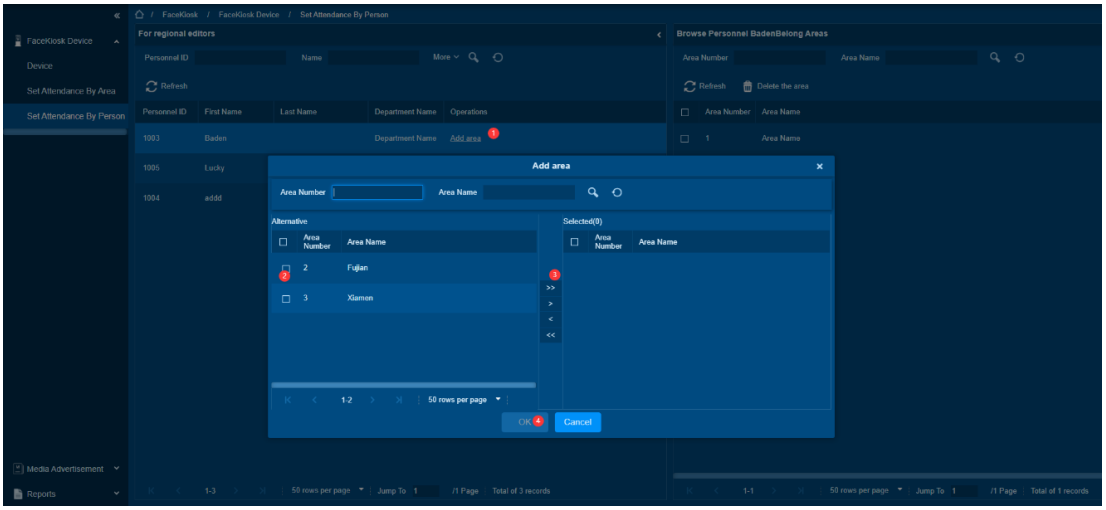
It used to synchronize people in the area.

Feature Trigger Result

Synchronized people in the area to the FaceKiosk device.

Steps:

- Select a person and click [**Add Area**].
- Choose an area for people to add.



15.2. Media Advertising

Media Advertising used to add and manage advertising resources for your FaceKiosk devices.

Function List

Operation	Description
Advertisement Resources	View the image or video data of local resources and external resources of advertisements
Advertisement Settings	Check advertising settings on the setting FaceKiosk.

15.2.1. Advertising Resources

Function Description

View the image or video data of local resources and external resources of advertisements.

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

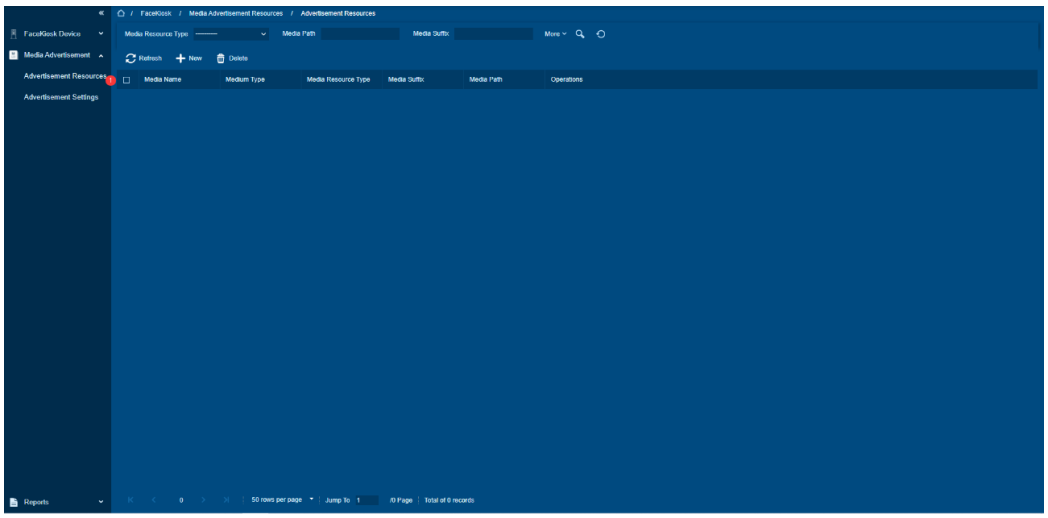
Function Usage Scenarios

Need to view Advertising Resources data on the software.

Feature Trigger Result

Display Advertising Resources data on the software.

Click [**Advertising Resources**] menu to enter the advertising resources list.



Add Advertising Resources

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

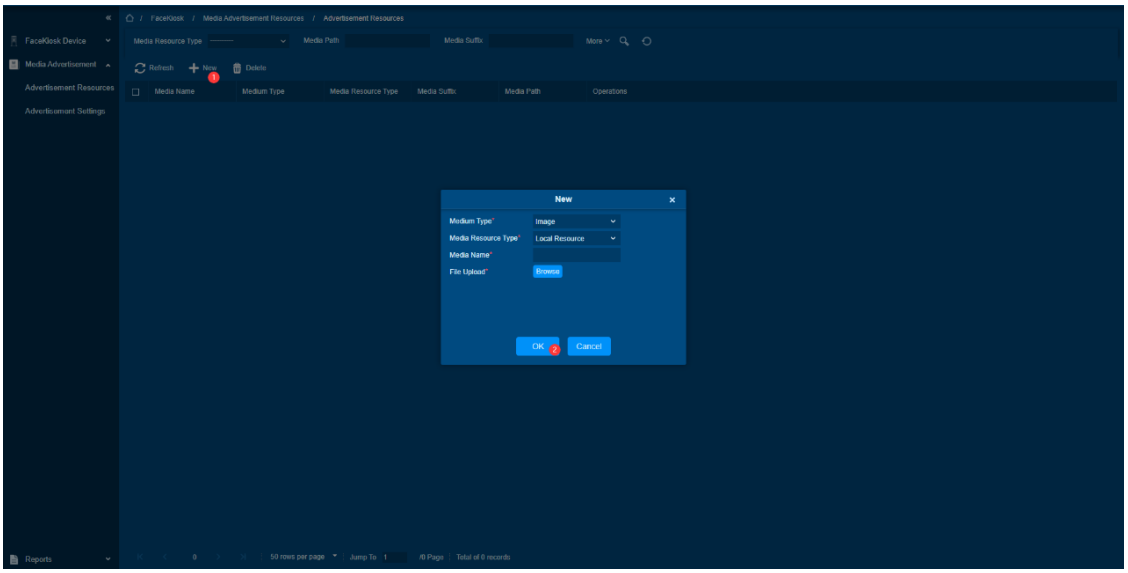
Need to add new Advertising Resources to the software

Feature Trigger Result

On the software, a new Advertising Resources was created.

Steps:

- Click [**Media Advertising**] > [**Advertising Resources**] > [**Add**] to enter the add advertising Resource's interface.
- Click [**OK**] to upload the media file.



Resource Type: Optional picture/video.

Source of Resources: Optional local resources/external links.

Media Resource Name: Set the name of the media resource file.

File Upload: Select the local file to upload.

External link: link to an external file.

Delete Advertising Resources

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

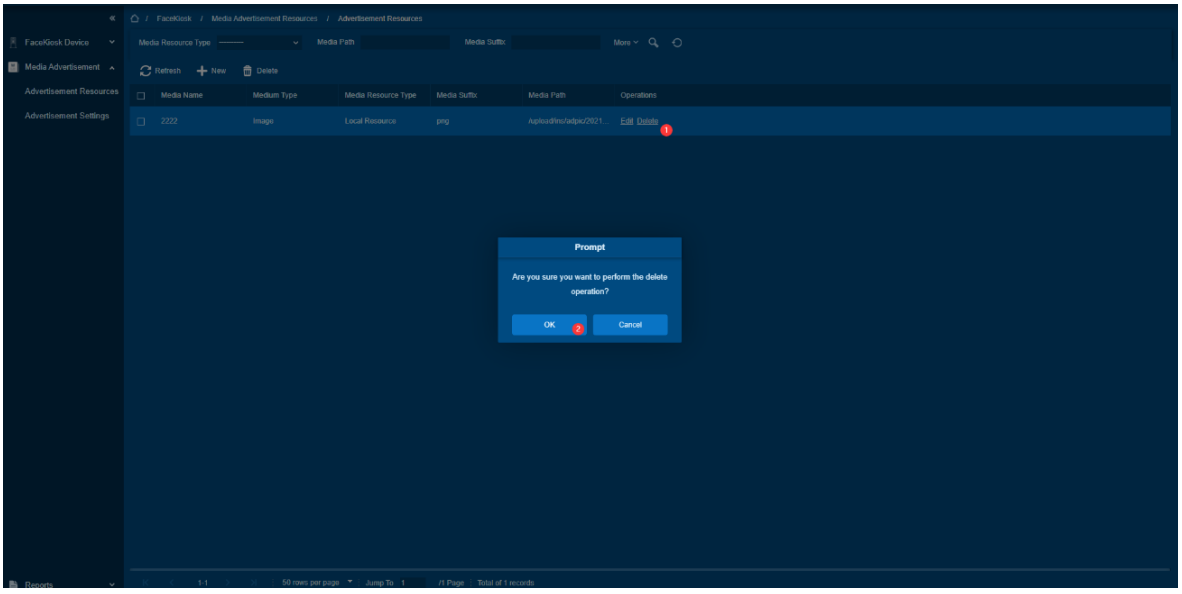
Need to delete the abandoned Advertising Resources.

Feature Trigger Result

On the software, a piece of Advertising Resources data was removed.

Steps:

- Select the media files that need to be deleted, and click [**Delete**] button, or click the [**Delete**] button under Operation
- Click [**OK**] to delete the media file.



15.2.2. Advertisement Settings

Function Description

Check advertisement settings on the setting FaceKiosk.

Preconditions for Normal Use of Function

The software is running normally, and the FaceKiosk Device is connected normally.

Function Usage Scenarios

Need to set up the advertisement page of the FaceKiosk.

Feature Trigger Result

Modify the Advertisement Settings of the FaceKiosk on the software, and at the same time issue a command to the FaceKiosk device to modify the Advertising Resources data on the FaceKiosk.

Function Operation Steps

Add Information Ad Settings

Preconditions for Normal Use of Function

The software is running normally, and the FaceKiosk device is connected normally.

Function Usage Scenarios

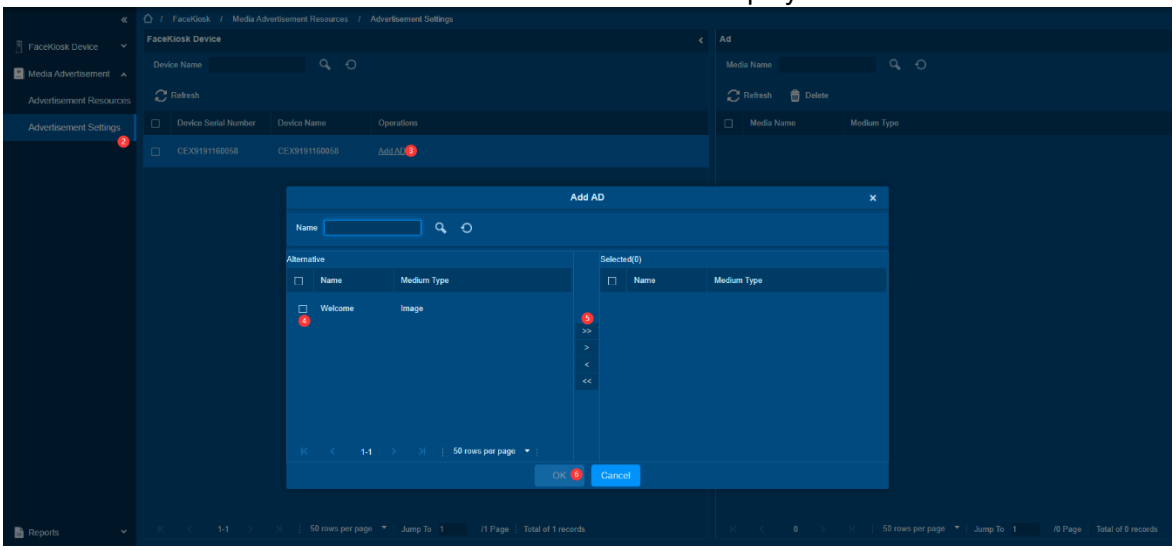
Need to set up the advertisement page of the FaceKiosk.

Feature Trigger Result

Modify the ad settings of the FaceKiosk on the software, and at the same time issue a command to the FaceKiosk device to modify the advertising resources data on the FaceKiosk.

Add Ads

- Select the FaceKiosk device that needs to add advertisements and click the [**Add Advertisement**] button under operation to enter the list of selected advertisements.
- Select the desired advertisement content, add it to the right, and click [**Confirm**] to complete the advertisement addition. The added advertisement will be displayed in the advertisement list on the right.



Delete FaceKiosk Ad Settings

Preconditions for Normal Use of Function

The software is running normally, and the FaceKiosk device is connected normally.

Function Usage Scenarios

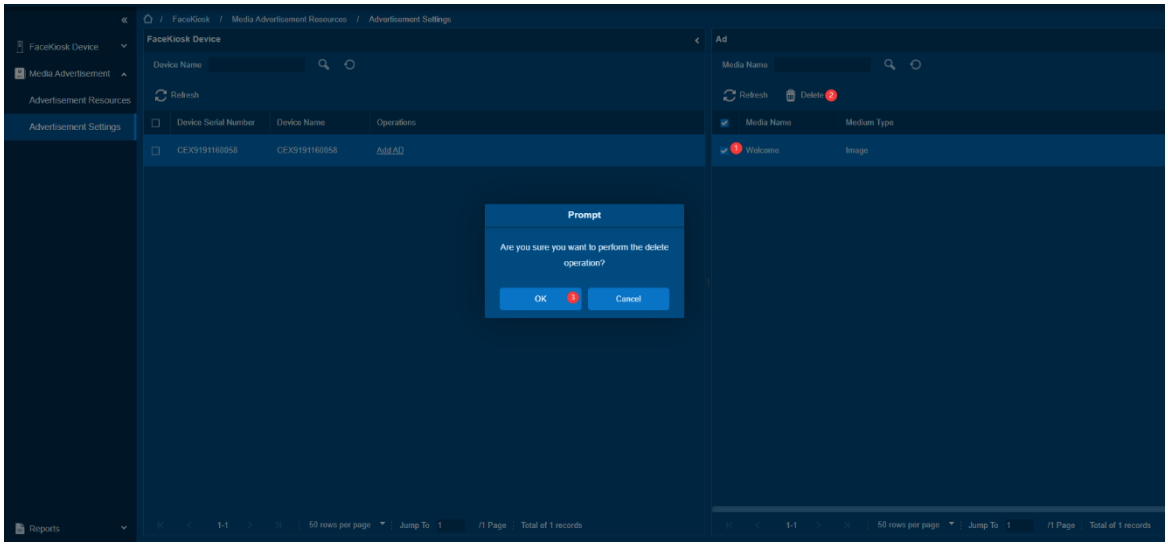
Need to set up the advertisement page of the FaceKiosk.

Feature Trigger Result

Modify the advertisement settings of the FaceKiosk on the software, and at the same time issue a command to the FaceKiosk Device to modify the advertising resources data on the FaceKiosk.

Delete Ads

In the list of ads on the right, select the ad and click [Delete] to remove the ad content added by device.



15.3. Report

Function List

Operations	Description
Verification Record	You can view the verification record of each department personnel's face verification on the FaceKiosk device according to the time.

15.4. Verification Record

Function Description

On the FaceKiosk device, you can view the verification record of each department personnel's face verification according to the time.

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

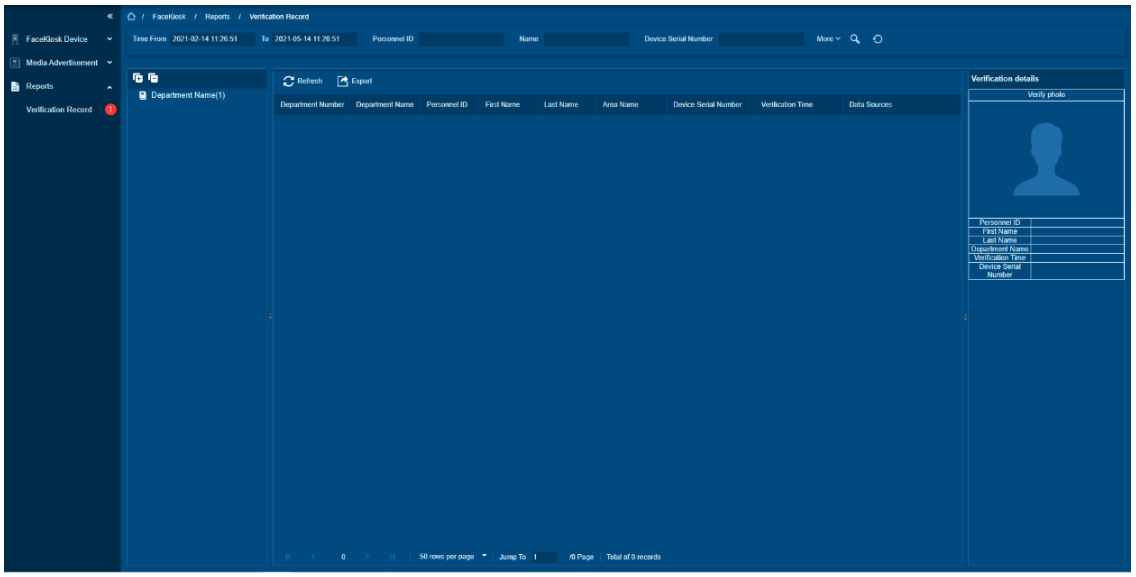
Function Usage Scenarios

It is necessary to check the Verification Record of each department personnel's face verification on the FaceKiosk device.

Feature Trigger Result

It displays the Verification Record of the FaceKiosk device to verify the face.

Enter the Page to view Verification Record information



16. Temperature Detection

The temperature measurement module is designed to be able to know the basic temperature status of visitors or personnel in a timely manner. The health information of all people is managed.

16.1. Temperature

Function List

Operations	Description
Real-time Monitoring	Real-time display of personnel's temperature records, abnormal temperature records, and non-wearing masks.
Parameters	Set the threshold and unit of body temperature.

16.2. Real-Time Monitoring

Prerequisites for normal function use

Administrators have real-time monitoring privileges, access control module has added access control devices with temperature measurement, personnel and visitors are in the personnel pool, and all have the appropriate access control privilege groups.

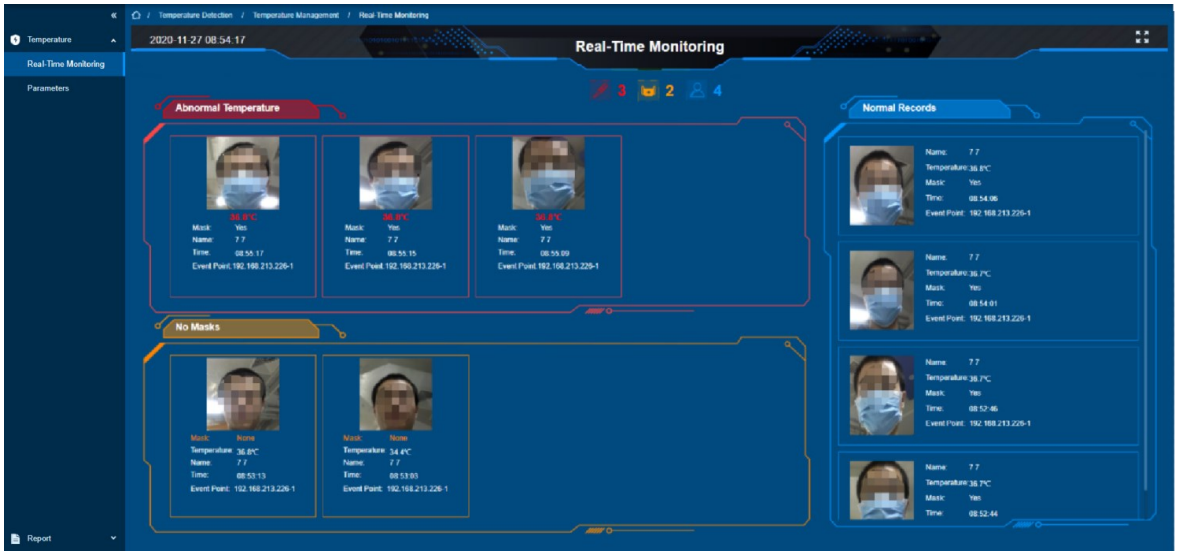
Function usage scenarios

After adding the access control device with temperature measurement function, synchronize the data, and face verification and body temperature measurement will be performed when a person is going to pass.

Trigger results

Display personnel's temperature records, abnormal temperature records, and non-wearing masks.

Click [**Temperature**] > [**Real-Time Monitoring**] to access the following page:



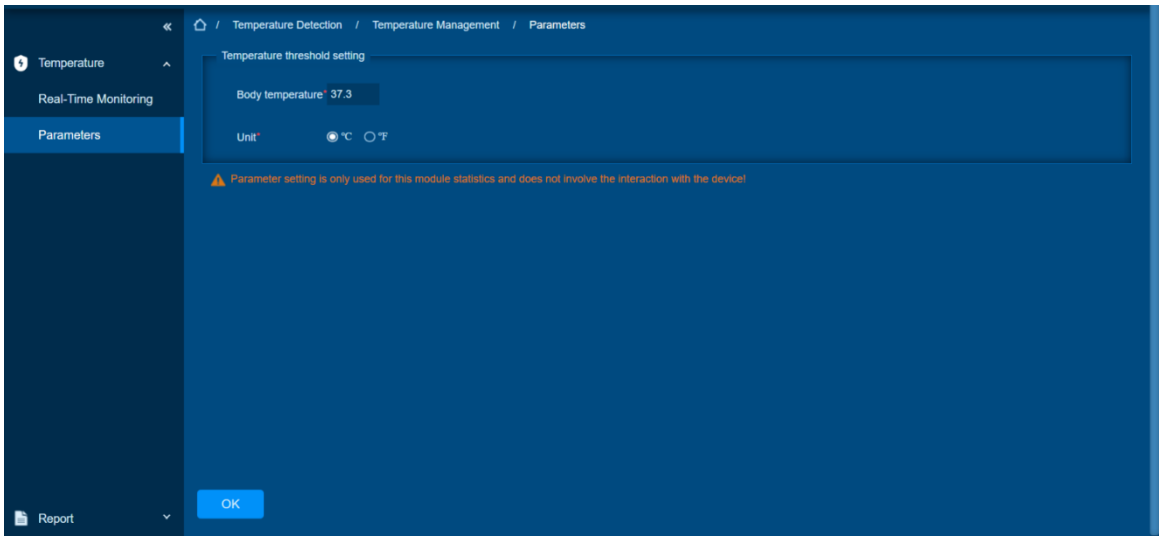
16.2.1. Parameters

It allows the user to set the body temperature threshold which determines the category to which the recorded temperature falls-in i.e., Abnormal Temperature or Normal Temperature. For example, assume that the threshold temperature is set to 37.30C. If the recorded temperature is 370C, it will be saved as “Normal Temperature” and if the recorded temperature is 380C, it will be saved as “Abnormal Temperature”. The temperature unit can also be chosen between 0C or 0F.

Function description

Set the threshold and unit when the device detects the body temperature.

Click [**Temperature**] > [**Parameters**] to access the following page:



Field Description:

Temperature threshold setting: Set the normal body temperature and body temperature unit.

✍**Note:**

After setting the body temperature threshold, the Real-Time Monitoring Page will refresh, and the persons will be categorized according to the new threshold temperature.

The value is rounded off to one decimal place.

16.3. Report

Function List

Operations	Description
Statistics Panel for Registered Personnel	Display the temperature status of registered persons
Temperature Raw Record	Display and export the temperature record table
Individual Temperature Record	Display and export the detailed information of human body temperature
Abnormal Temperature Record	Display, export, and query abnormal personnel body temperature information
Departmental Daily Statistic	Displaying and exporting personnel temperature information from departmental statistics
Monthly Statistics	Graphical presentation of event statistics

16.3.1. Statistics Panel for Registered Personnel

Function description

Display the temperature status of registered persons.

Temperature Raw Record

Export

Prerequisites for normal function use

Administrators have export privileges.

Function usage scenarios

Exporting record table information from software.

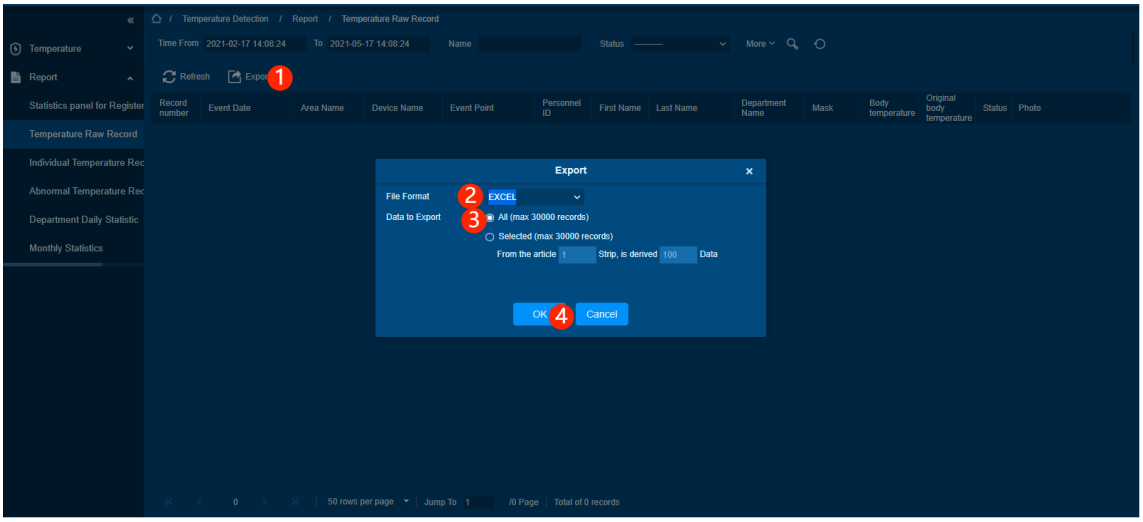
Trigger results

Operations	Description
Select EXCEL	Export the record table to EXCEL format
Select PDF	Export the record table to PDF format
Select CSV	Export the record table to CSV format

Select all data	Export all data from the record table
Select the amount of data to export	Exporting some data from the record table

Steps:

1. Click [**Export**] button and a pop-up window will appear.
- Select the file format to be exported.
- Select the range to be exported.
- Click [**OK**] to complete the export operation.



16.3.2. Temperature Raw Record

Prerequisites for normal function use

The administrator has access to the query function and the relevant data is available in the list.

Function usage scenarios

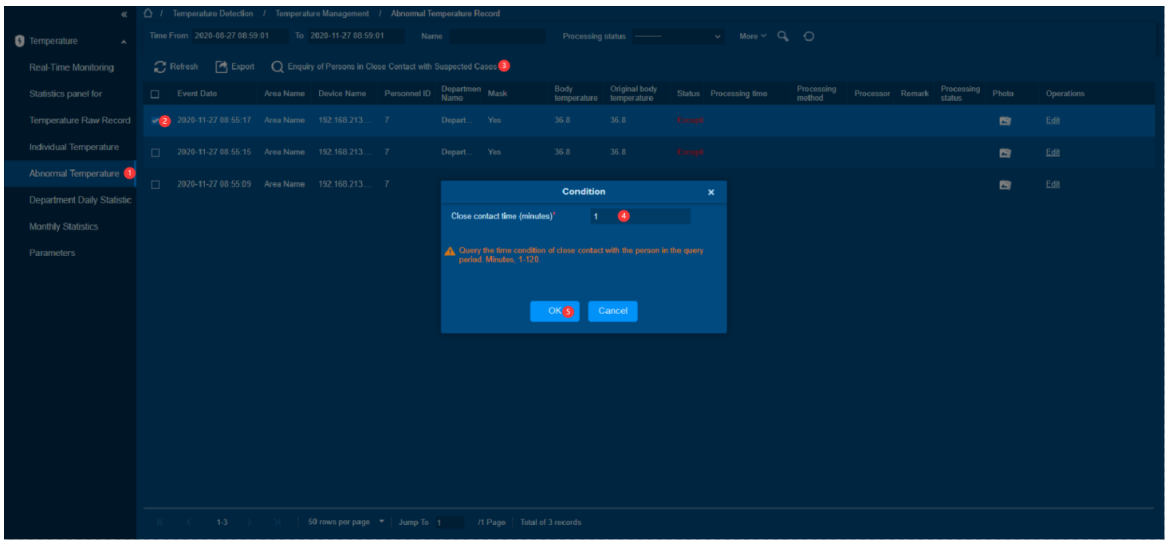
When someone is a suspected case, it is necessary to find people who have had close contact with that person for investigation and prevention and control.

Trigger results

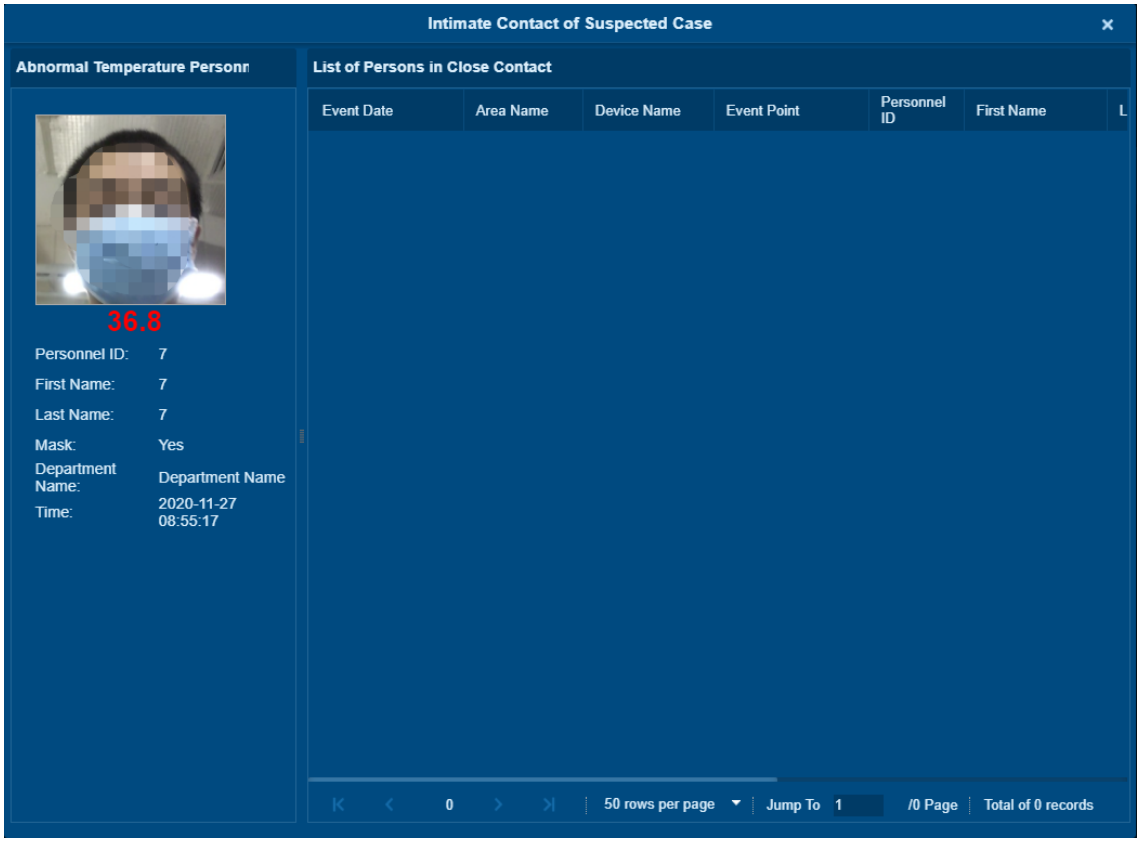
Query information on people who are in close contact with suspected cases.

Steps:

- Select an exception record and click [**Enquiry of Persons in Close Contact with Suspected Cases**] button.



- Set contact time, the records will be filtered and displayed as follows.



16.3.3. Individual Temperature Record

Export

Prerequisites for normal function use

Administrators have export privileges.

Function usage scenarios

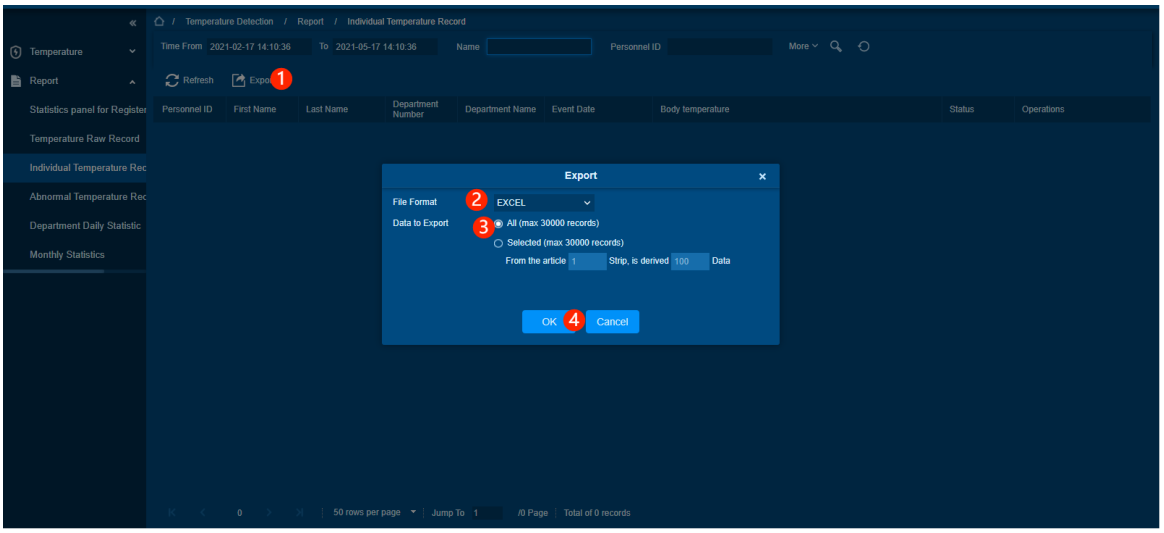
Exporting personnel temperature details from software.

Trigger results

Operations	Description
Select EXCEL	Export personnel temperature details to EXCEL format
Select PDF	Export personnel temperature details to PDF format
Select CSV	Export personnel temperature details to CSV format
Select all data	Export all data of the person's temperature detail information
Select the amount of data to export	Exporting part of the data of the person's temperature detail information

Steps:

- Click on the [**Export**] button and a pop-up window will appear.
- Select the file format to be exported.
- Select the range to be exported.
- Click [**OK**] to complete the export operation.



16.3.4. Abnormal Temperature Record

Export

Prerequisites for normal function use

Administrators have export privileges.

Function usage scenarios

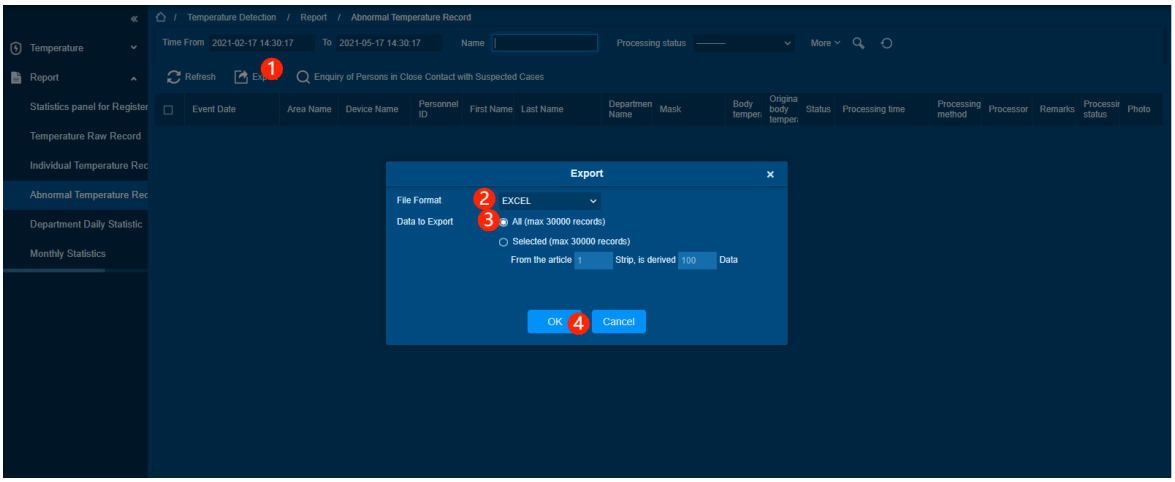
Exporting record table information from software.

Trigger results

Operations	Description
Select EXCEL	Export the record table to EXCEL format
Select PDF	Export the record table to PDF format
Select CSV	Export the record table to CSV format
Select all data	Export all data from the record table
Select the amount of data to export	Exporting some data from the record table

Steps:

- Click [**Export**] button and a pop-up window will appear.
- Select the file format to be exported.
- Select the range to be exported.
- Click [**OK**] to complete the export operation.



16.3.5. Department Daily Statistic

Export

Prerequisites for normal function use

Administrators have export privileges.

Function usage scenarios

Exporting statistical report information from software.

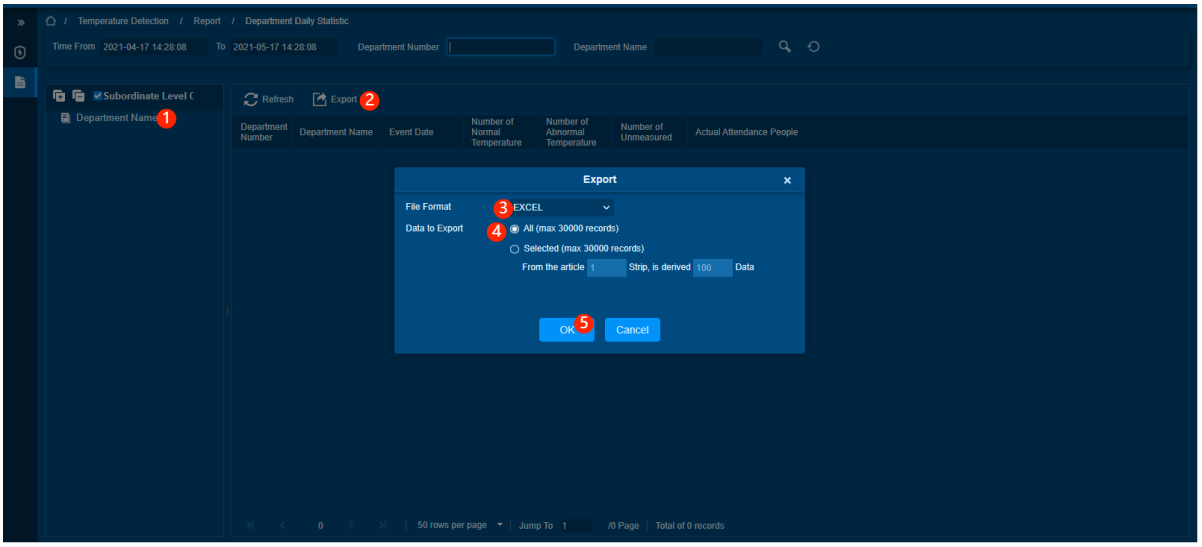
Trigger results

Operations	Description
Select EXCEL	Export statistical report information to EXCEL format
Select PDF	Export statistical report information to PDF format
Select CSV	Export statistical report information to CSV format

Select all data	Exporting all data for statistical report information
Select the amount of data to export	Exporting partial data for statistical report information

Steps:

- Select the department to be viewed.
- Click on the [**Export**] button and a pop-up window will appear.
- Select the file format to be exported.
- Select the range to be exported.
- Click [**OK**] to complete the export operation.



16.3.6. Monthly Statistic

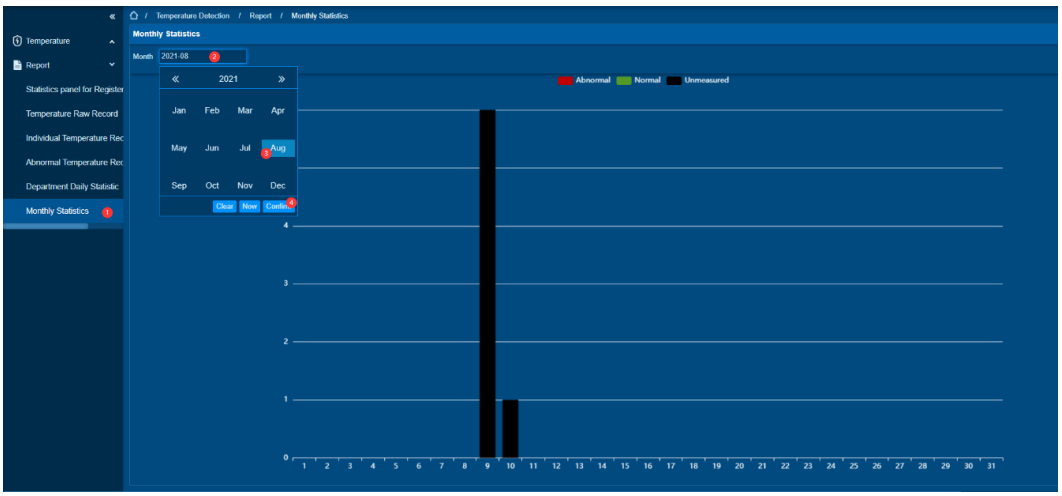
Check the temperature measurement of the month.

Function description

Graphical presentation of event statistics.

Steps:

- Select time when you want to run a query.



17. Defence

In this module, you can group tag management for all personnel in your system, including employees, visitors, strangers, and their vehicles, and use a unified portal to synchronize personnel and vehicle data between the tag group you define and the third-party platform. For example, sync to the IVS platform.

In addition, we have also made some interesting applications here. The Target Alert function uses the devices of each module to follow the tag group people or vehicles you define and can notify and remind you when these people or vehicles appear. These can be Any equipment currently connected to the system will greatly enhance your regional security control; the area Occupancy Control function can achieve accurate population control in the area through access control and camera device to ensure that the number of people in the area is within your setting, these functions will better assist you in the management of regional security.

17.1. Tags

Function List

Operations	Description
Personnel Tags Group	Classify personnel into groups for management, and synchronize these groups with third-party platforms
Vehicle in System	Store and display all vehicle information in the system
Vehicle Tags Group	Classify Vehicle into groups for management, and synchronize these groups with third-party platforms
Strangers	Manage and add system strangers

17.1.1. Personnel Tags Group

Function Description

Use this function to tags group all the people in the system, including employees, visitors, and strangers. The people in the tags group will have common attributes, and they will be available for you to choose and manage in the following smart scenario applications. The tag group can also be synchronized and updated with the third-party platform for the personnel information in the group to ensure that the personnel information on platforms is consistent.

Default List

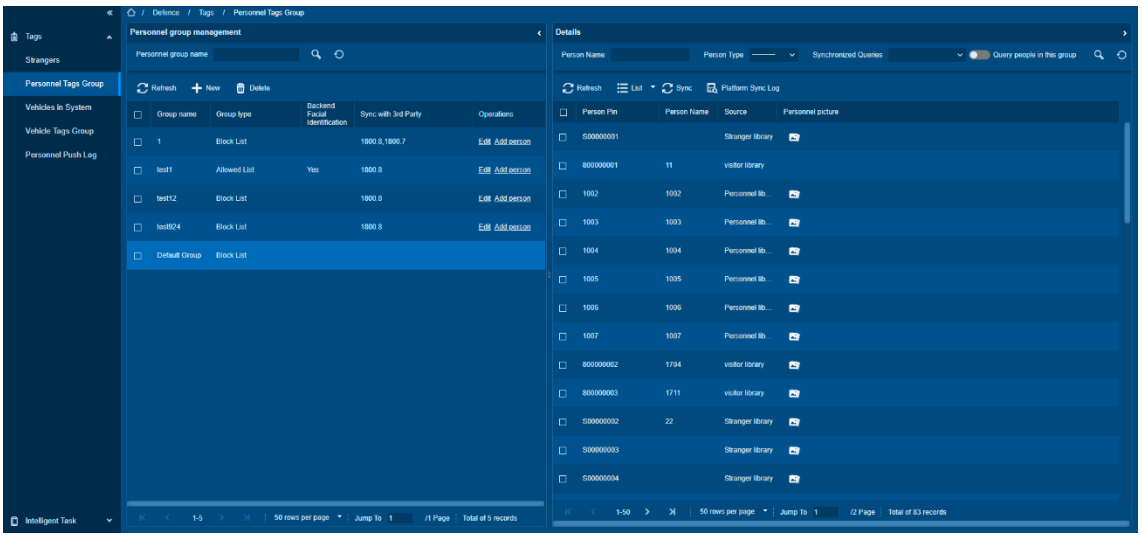
Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

The system default library will be created automatically. When the system is installed, it will include all

personnel information in the system, including personnel, historical visitors, and strangers. Unlike the newly added personnel tag group, it is not allowed to be edited or deleted. When you create a third-party platform, you can check the system default library for personnel synchronization.



New Personnel Tags Group

Preconditions for Normal Use of Function

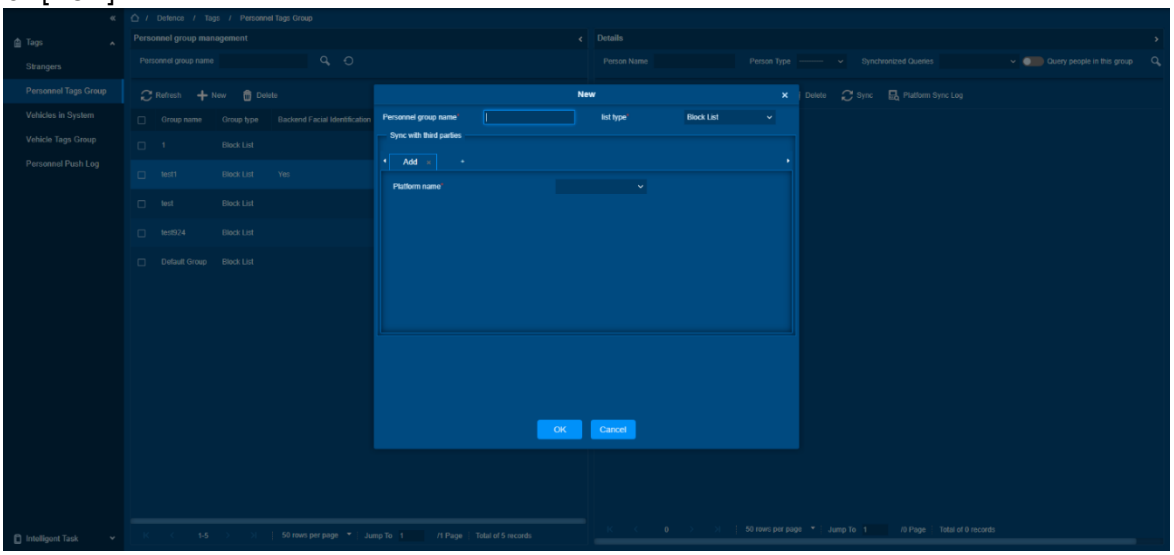
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

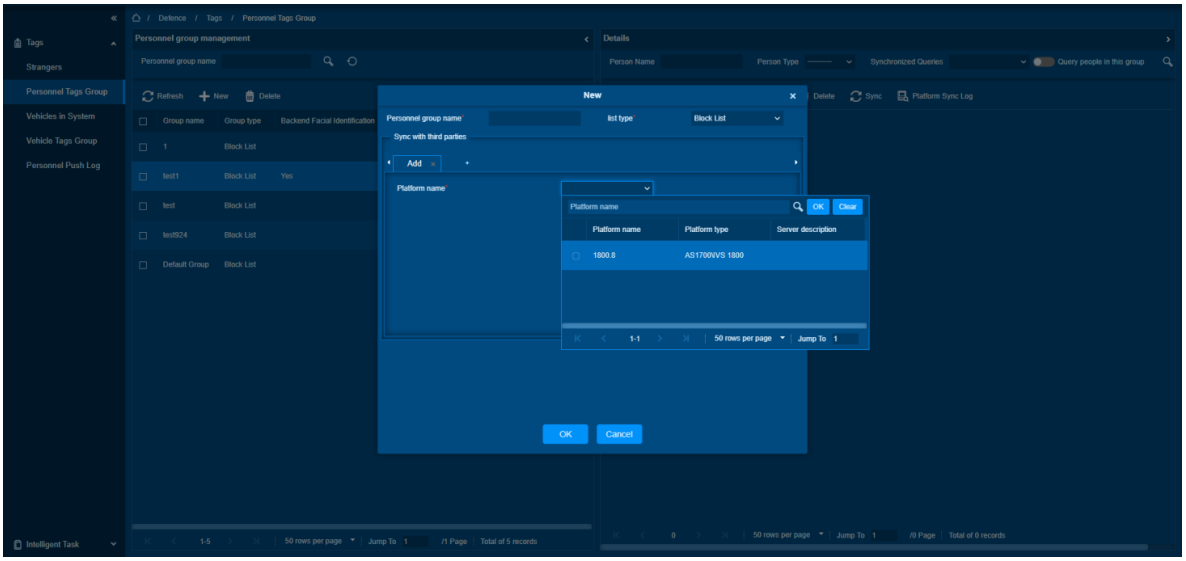
Create a new tag group

Steps:

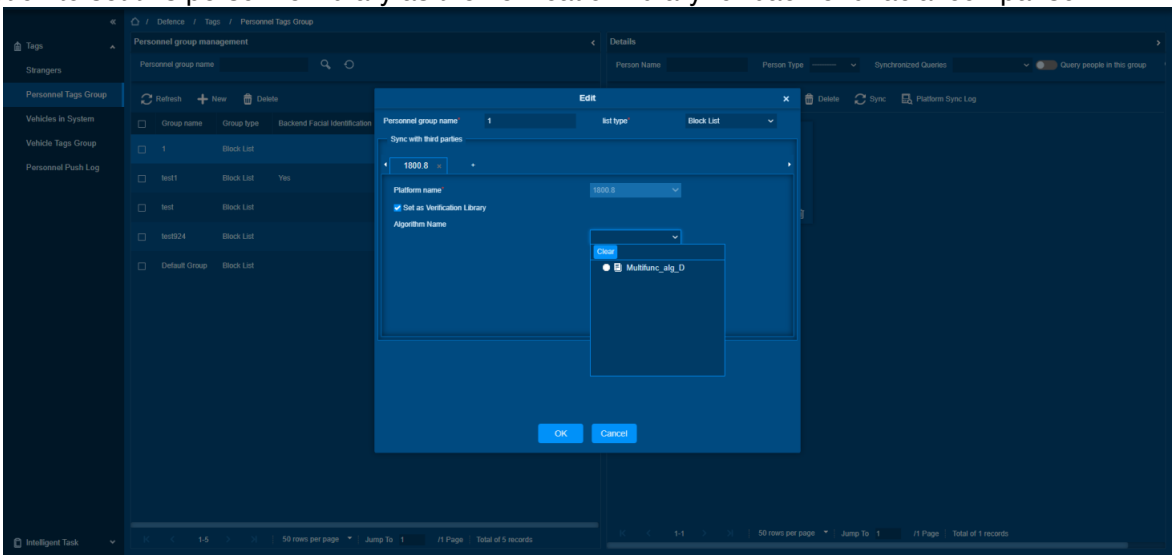
1. Click [**New**].



2. Set tag group name and type.
3. Set whether to synchronize to a third-party platform, choose the name of the bound third-party platform.



4. When the third-party platform to be bound is the IVS type, you can check the Set as verification library option to set this personnel library as the verification library for back-end facial comparison.



Click [**OK**] to complete the create operation, meanwhile, a library will be created synchronously on the bound platform. After that, every personnel added to this library will be automatically synchronized to the bound third-party platform (optional).

Add Personnel

Preconditions for Normal Use of Function

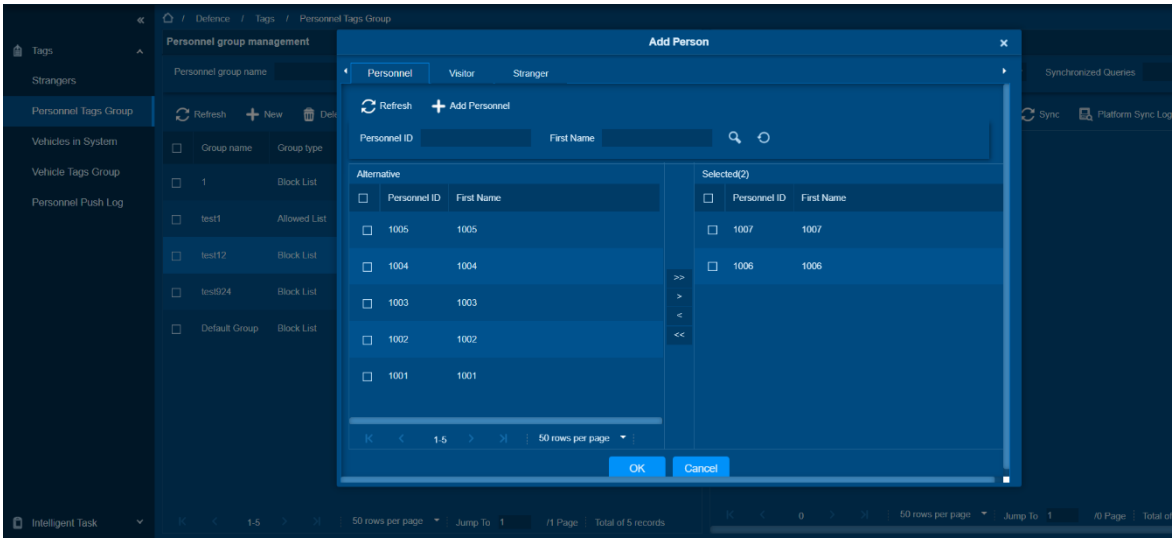
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Add people to the tag group

Steps:

1. Click [**Add Person**].



2. Choose and select the personnel category.
3. Move them to the right.
4. Click **[OK]** to complete add personnel.

Delete

Preconditions for Normal Use of Function

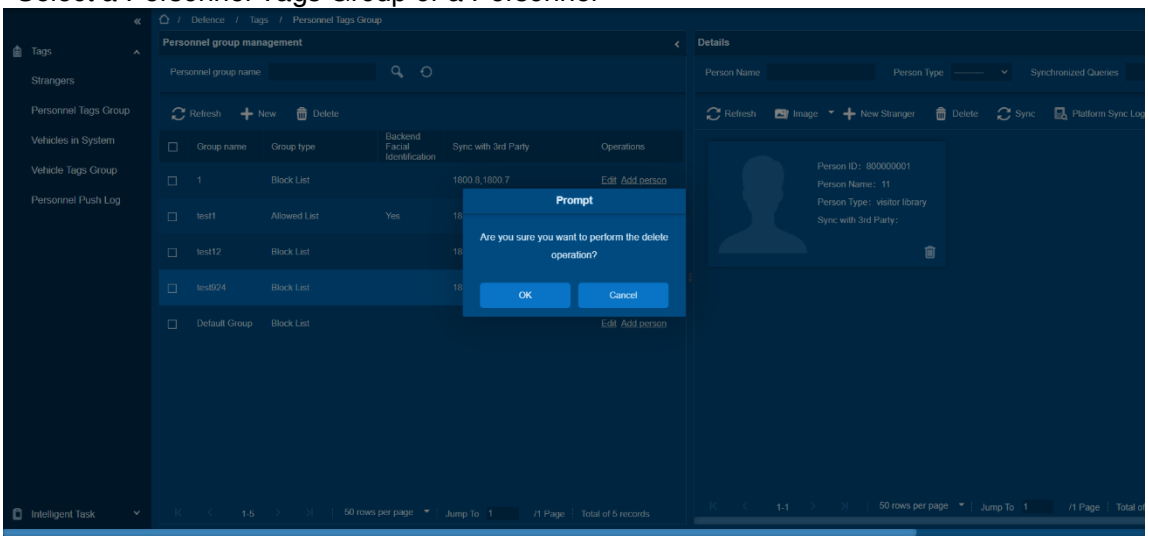
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Delete a person tag group, or delete a person in the group

Steps:

1. Select a Personnel Tags Group or a Personnel



2. Click [**Delete**] in the tool bar or operations.
3. Click [**OK**] to complete the operation of deleting a person tag group or person.

Re-synchronized

Preconditions for Normal Use of Function

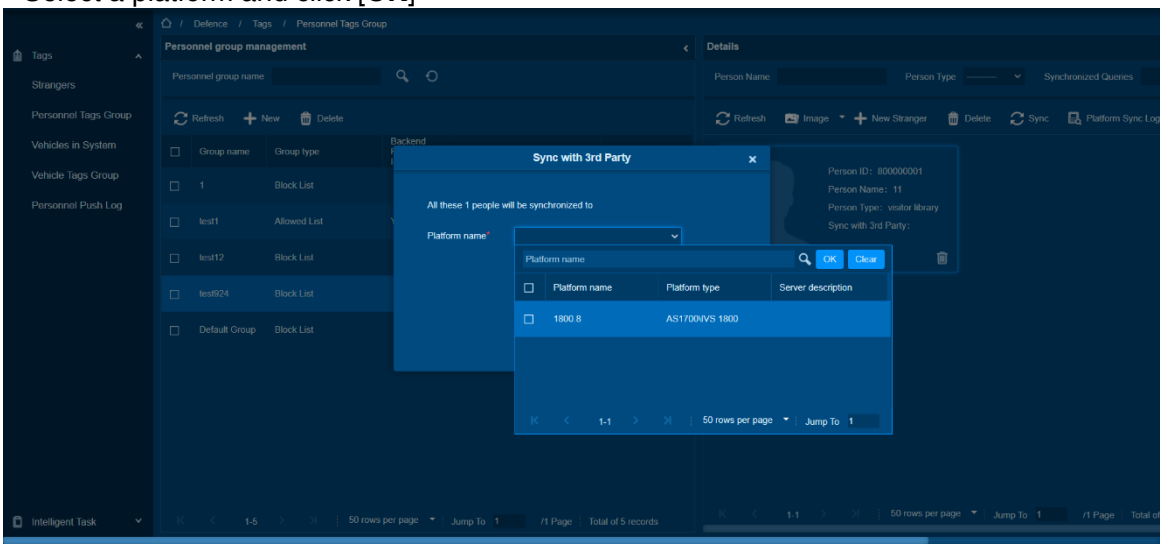
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

When part of the personnel synchronization fails, you can use this function to manually synchronize the personnel again.

Steps:

1. Select a Personnel
2. Click [**Sync**] in the toolbar
3. Select a platform and click [**OK**]



17.1.2. Vehicles in System

Function Description

In this function, all the vehicles entered in the system will be included and their affiliation will be displayed, it contains the vehicles of personnel and visitors and is connected to the parking module.

New

Preconditions for Normal Use of Function

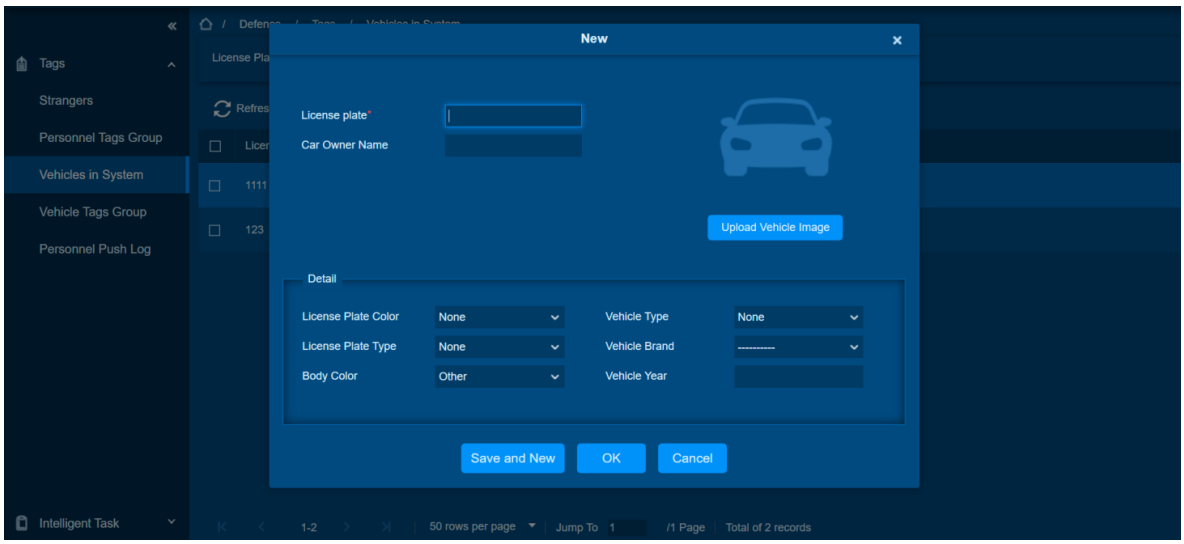
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Create a new system vehicle and associate them with a person.

Steps:

1. Click [**New**].



2. Input Vehicle detail.
3. Click [**OK**] to complete adding.

17.1.3. Vehicle Tags Group

Function Description

Use this function to group all the vehicles in the system for tags management. The vehicles in the tag group will have common attributes, and they will be available for you to choose and use in the following smart scenario applications. You can also synchronize and update the vehicle information in the group with the third-party platform to ensure that the vehicle information on platforms is consistent.

New

Preconditions for Normal Use of Function

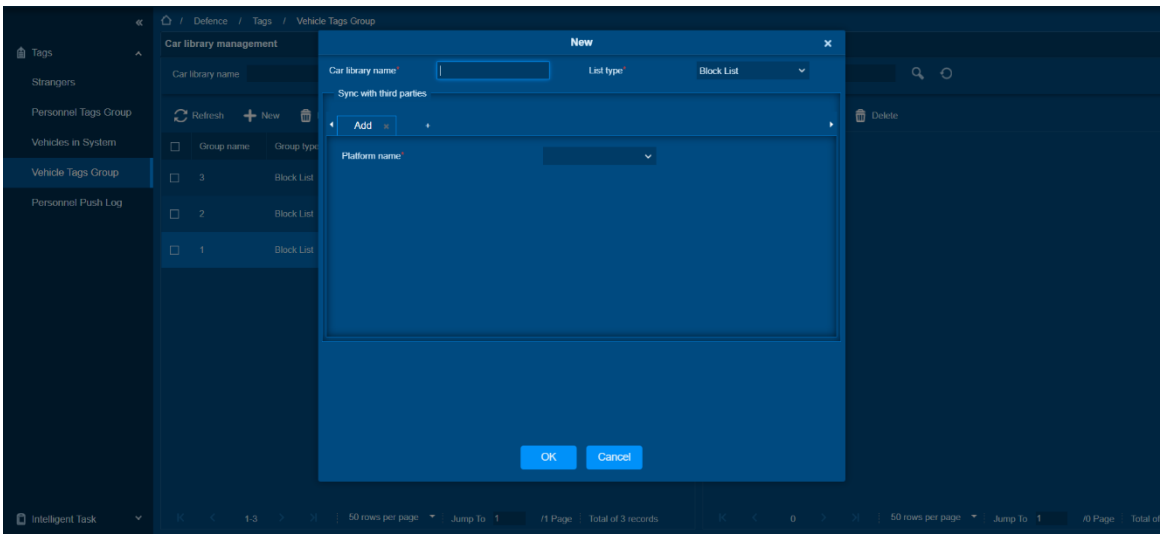
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

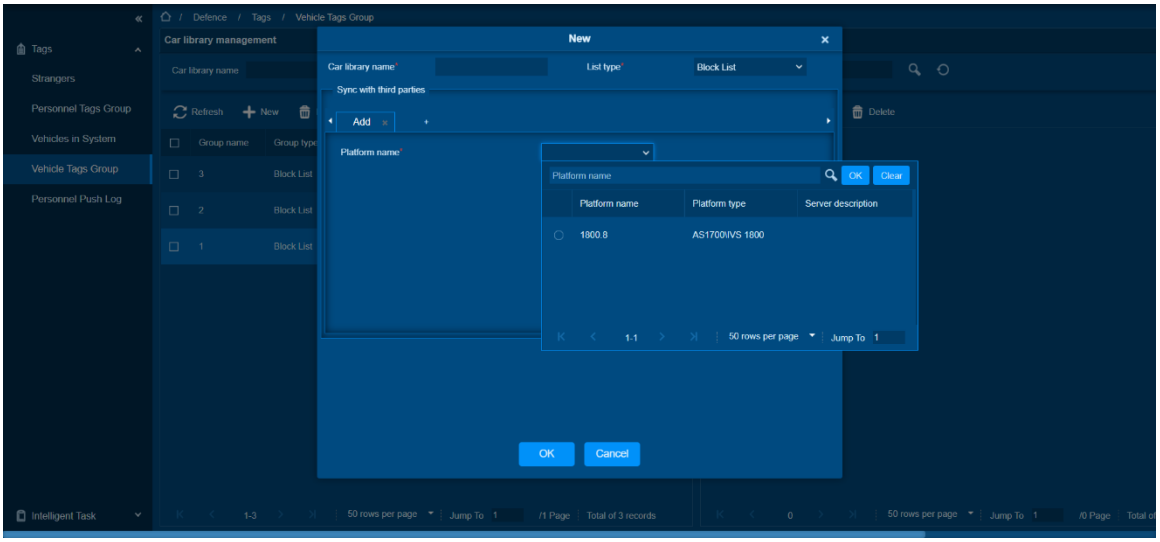
Create a vehicle tags group.

Steps:

1. Click [**New**].



2. Set tags group name and type.
3. Set whether to synchronize to a third-party platform and select the name of the bound third-party platform.



Click [**OK**] to complete the create operation. Meanwhile, a vehicle library will be created synchronously on the bound platform. After that, every vehicle added to this library will be automatically synchronized to the bound third-party platform (optional).

Add Vehicles

Preconditions for Normal Use of Function

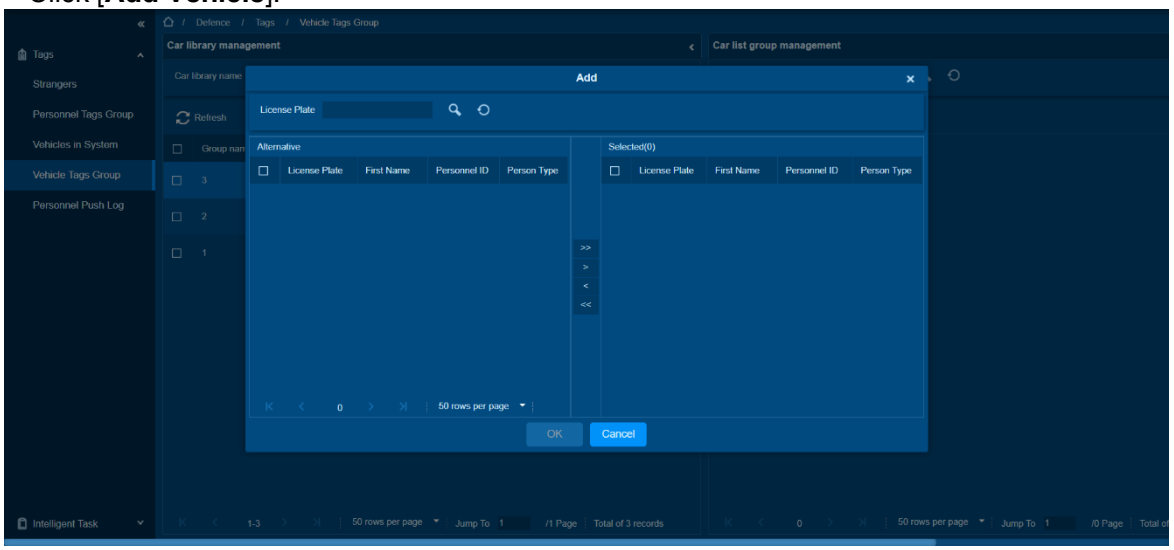
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Add a system vehicle to the vehicle tag group

Steps:

1. Click [**Add Vehicle**].



2. Choose and select the Vehicles.
3. Move them to the right.
4. Click [**OK**] to complete the adding.

Delete

Preconditions for Normal Use of Function

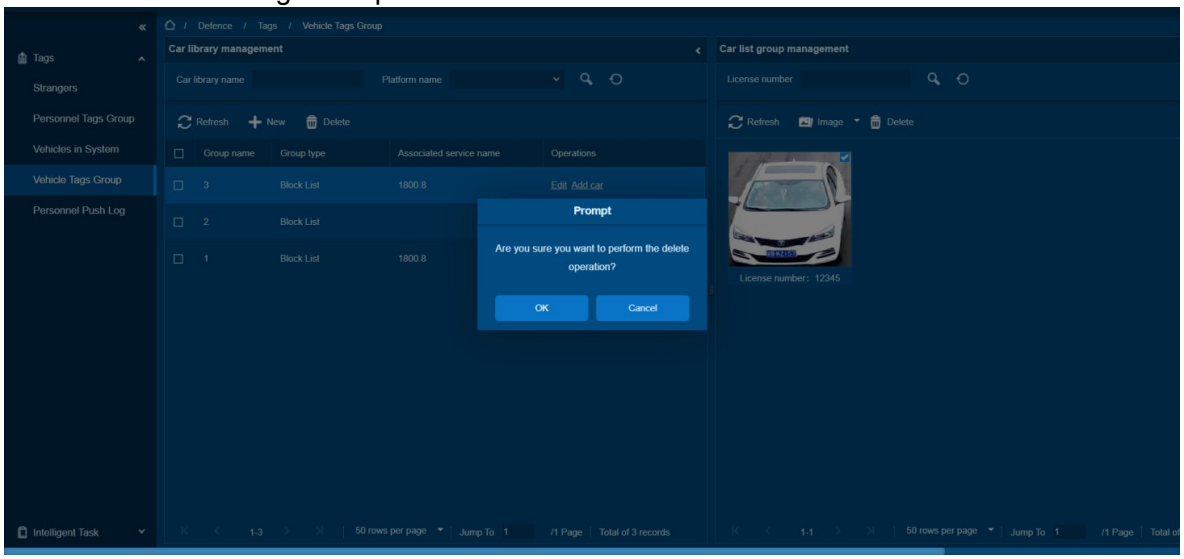
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Delete a vehicle tag group or delete a vehicle in the group.

Steps:

1. Select a Vehicle Tags Group.



2. Click [**Delete**] in the tool bar or operations.

3. Click [**OK**] to complete the delete the vehicle tag group or the vehicle.

Re-synchronized

Preconditions for Normal Use of Function

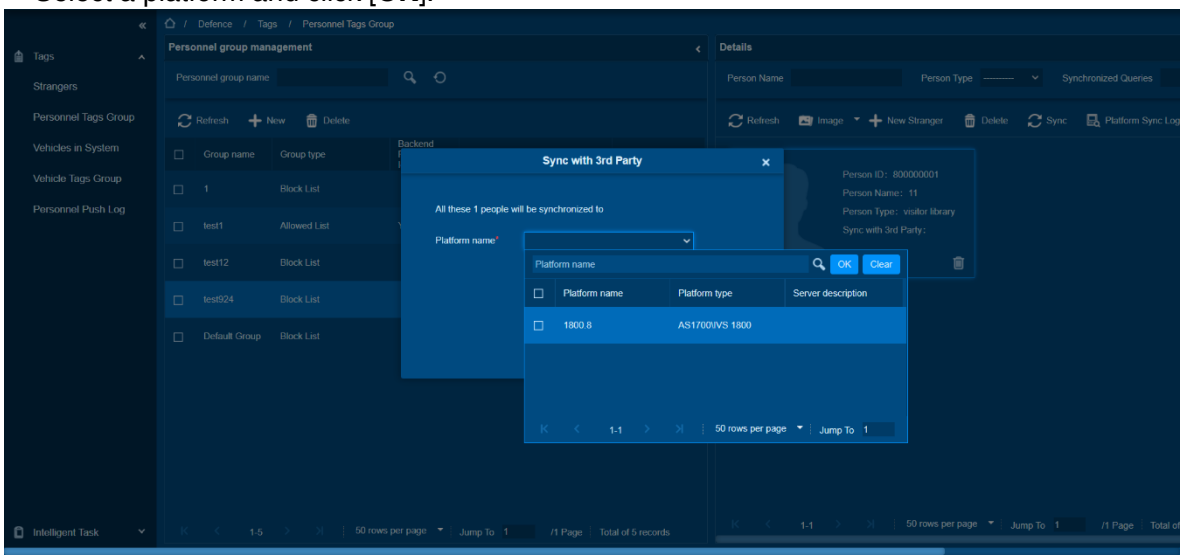
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

When part of the vehicle synchronization fails, you can use this function to manually re-synchronize the vehicle.

Steps:

1. Select a Vehicle.
2. Click [**Sync**] in the toolbar.
3. Select a platform and click [**OK**].



17.1.4. Strangers

Function Description

Use this feature to create and manage strangers in your system.

New

Preconditions for Normal Use of Function

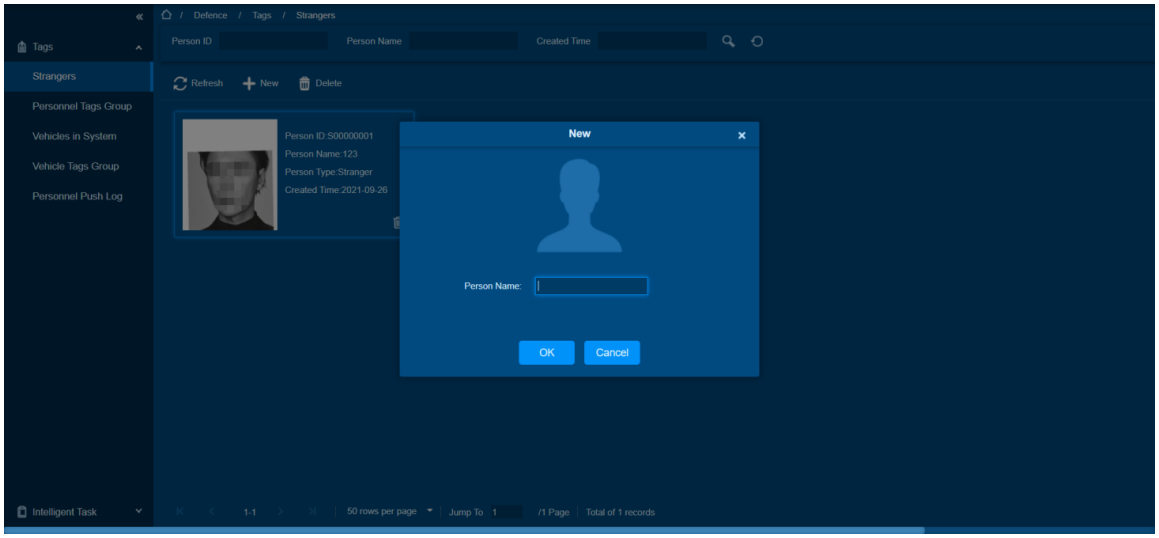
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Create a stranger.

Steps:

1. Click [**New**].



Click [**OK**] to complete the stranger adding.

17.2. Intelligent Task

Function List

Operations	Description
Target Alerts	Use full-module devices to keep an eye on your defined tag group of people or vehicles and be able to generate notifications and alerts on the presence of those people or vehicles
Occupancy Control	Control the number of people in the area with video and access control devices

17.2.1. Target Alerts

Function Description

Use this function to create an alert task, set the Tags group above mention as a target, once those people or vehicle presence, you be able to receive an alarm notification in Alarm Center, and keep it record in report. Alarm can be trigger by Access, Attendance, Elevator, Visitor, Parking, Video and FaceKiosk Module.

New

Preconditions for Normal Use of Function

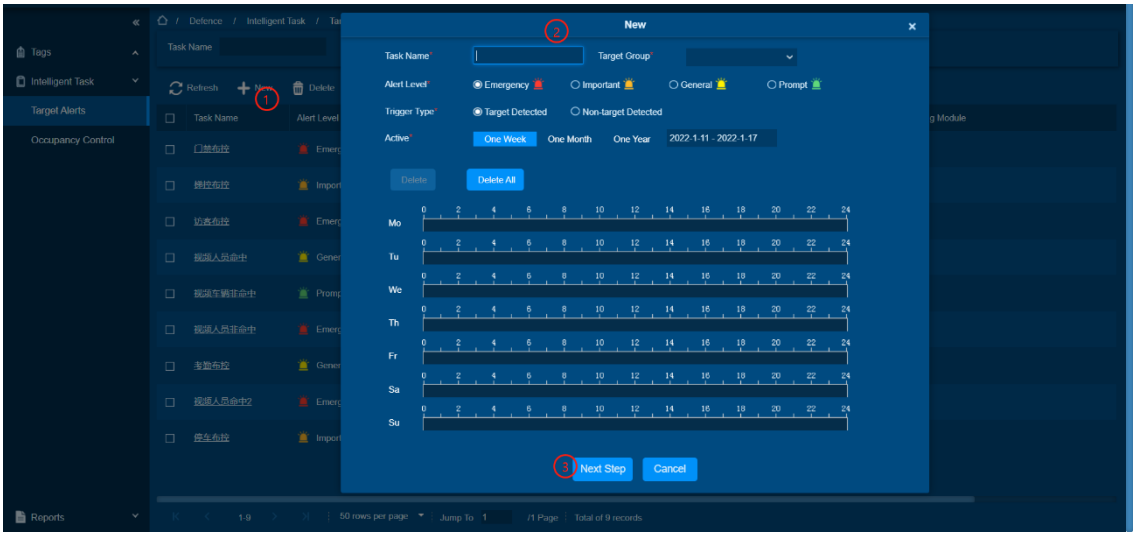
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

Create a target alert task.

Steps:

1. Click [**New**].



Set parameters of the task, and the fields are explained as follows:

Task Name: Set alert task name.

Target Group: Select groups been set in above Personnel Tags Group or Vehicle Tags Group.

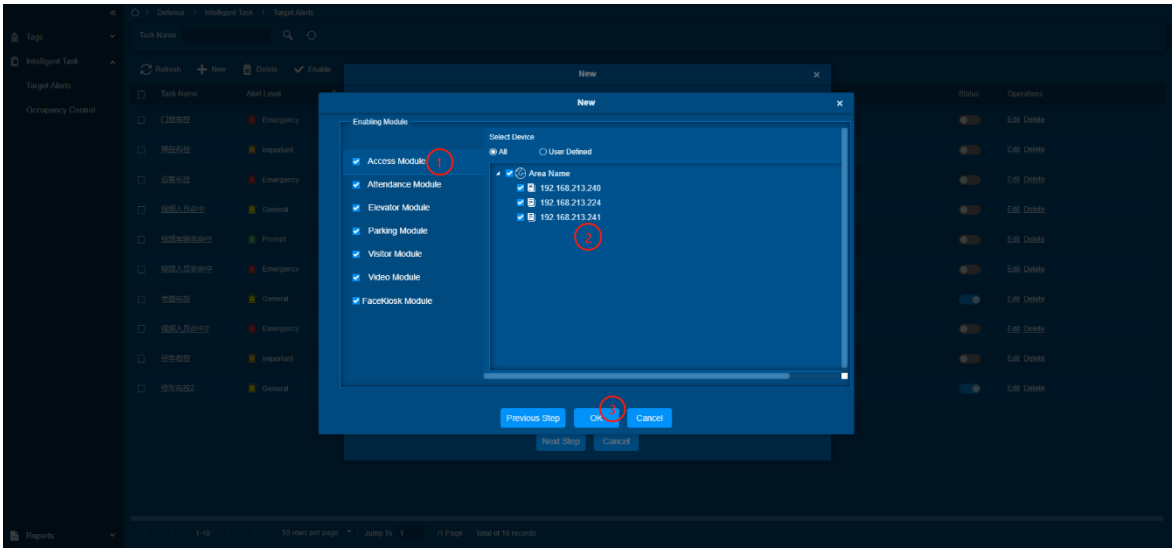
Alert Level: Set trigger alarm notification level.

Trigger Type: Optional Target detected (When the target in selected group appears will be triggered alarm) or non-target detected (Trigger an alarm when the target is not in the selected group).

Active: Set task active time period.

Daily Active Time: set daily active time during above active time period.

2. Then click [**Next Step**].



Select active module and device when person record in these selected devices will be trigger alarm.

3. Click [**OK**] to finish the setup and enable the task.

Edit

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Target alert task was disabled.

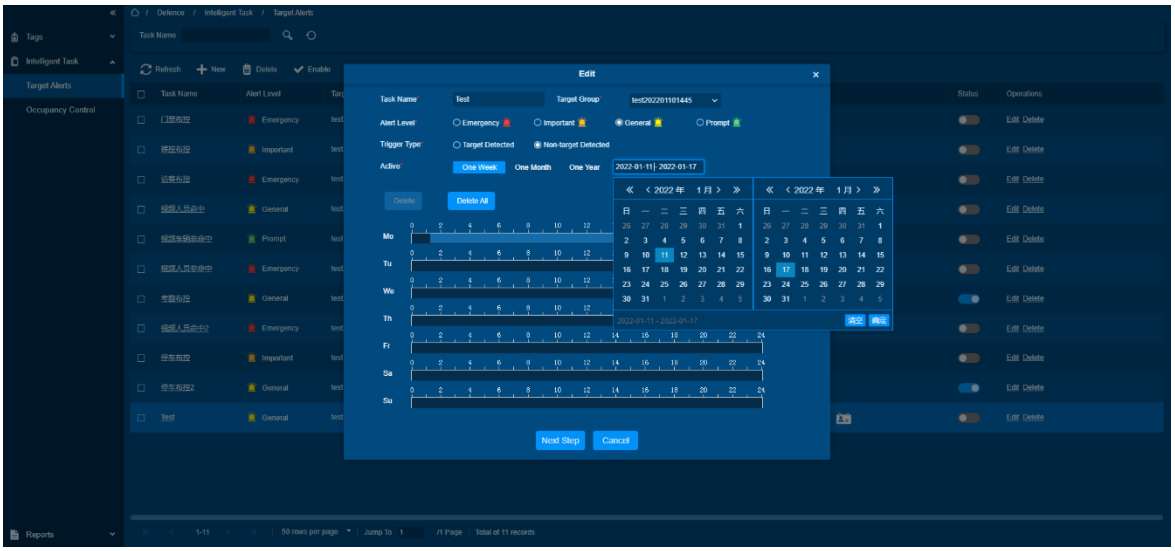
Function usage scenarios

Edit a target alert task.

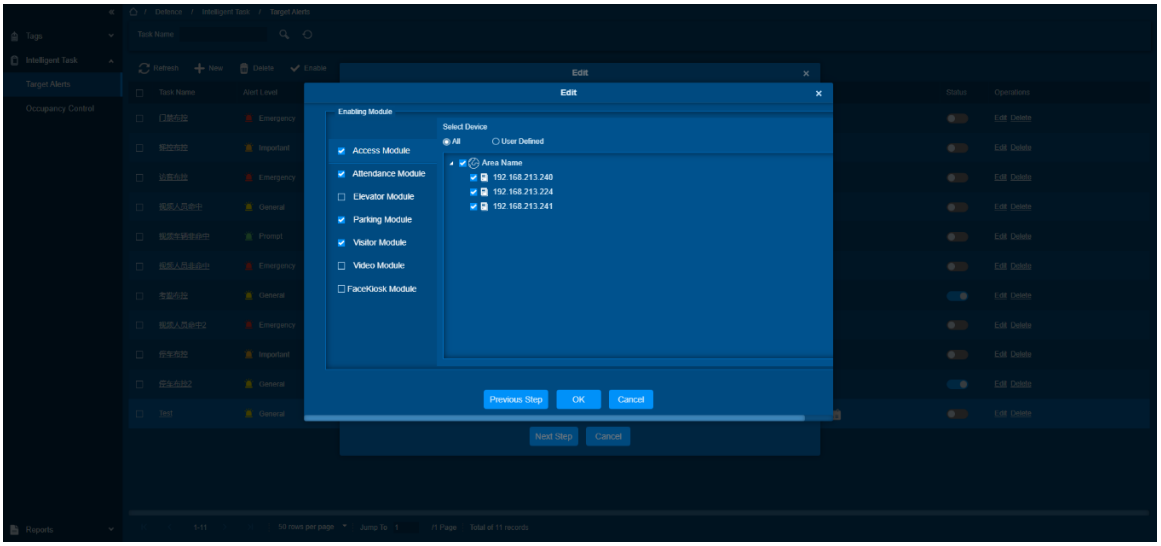
Steps:

1. Click the task name or click [**Edit**] in operation.

2. Change Active time period and click [**Next Step**].



3. Change the enable module and device and click [**OK**] to save edit.



Enable/Disabled

Preconditions for Normal Use of Function

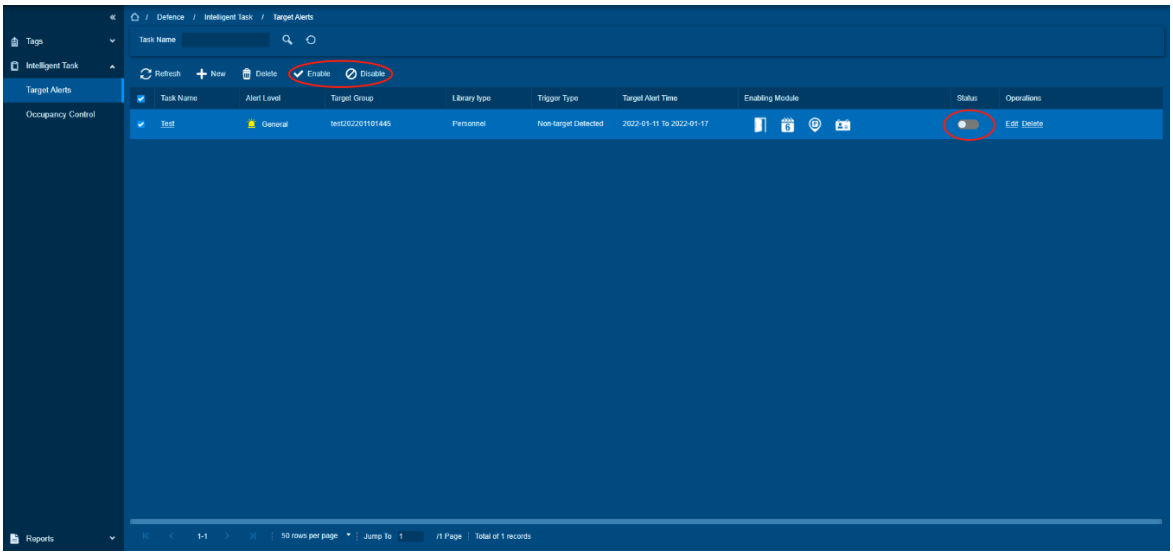
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

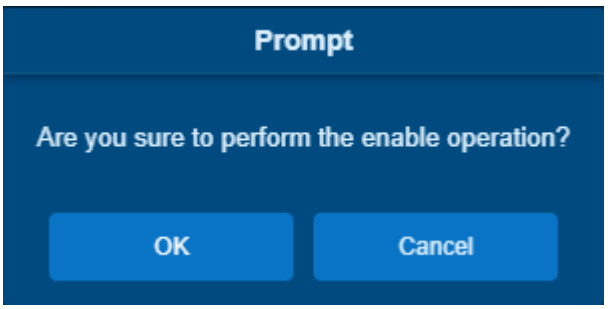
Enable/Disabled a target alert task.

Steps:

1. Select alert task and click [**Enable/Disabled**] in the tool bar or in the Status.



2. Click [**OK**] to confirm Enable/Disabled task.



3. Disabled task will not generate any new alarm records.

Delete

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

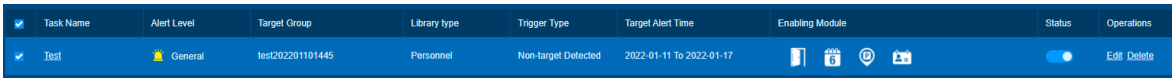
Operation task was disabled.

Function usage scenarios

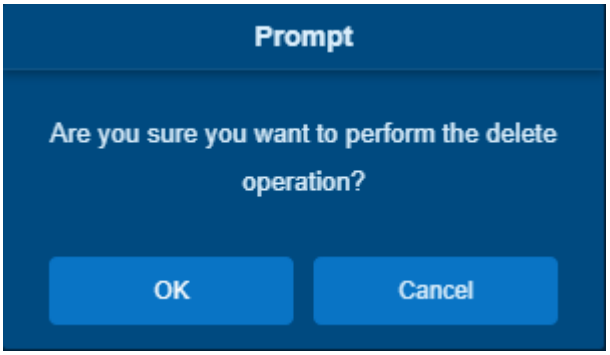
Delete an existed target alert task.

Steps:

1. Select task and click [Delete] in the tool bar or in the operation.



2. Click [OK] to confirm delete task operation.



17.2.2. Occupancy Control

Function Description

Use this function to create and control the number of people in an area, set the capacity of the area, and restrict all or some people from entering when the maximum number of people is reached.

New

Preconditions for Normal Use of Function

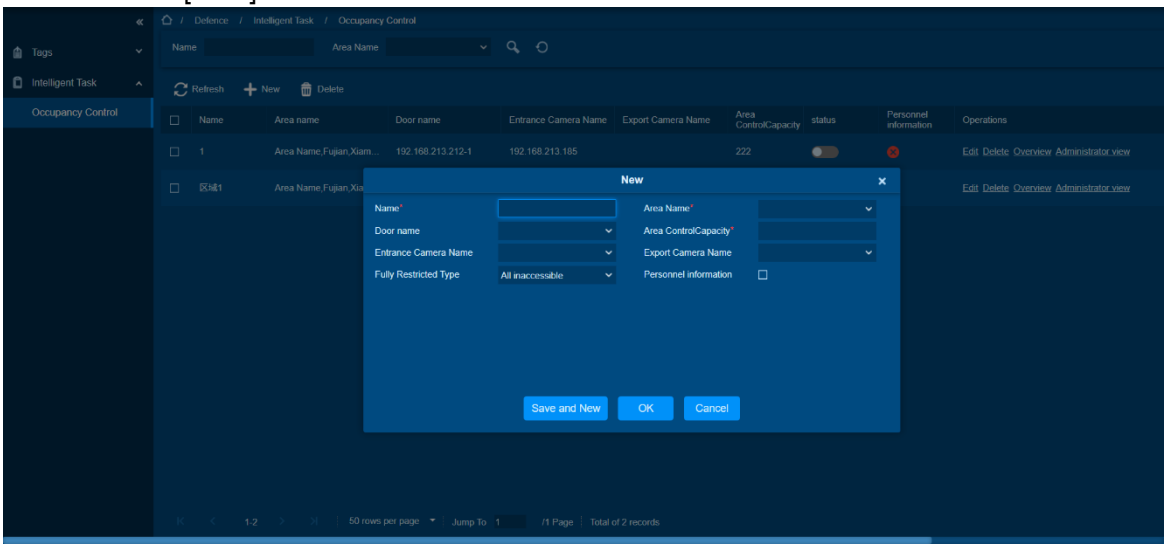
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

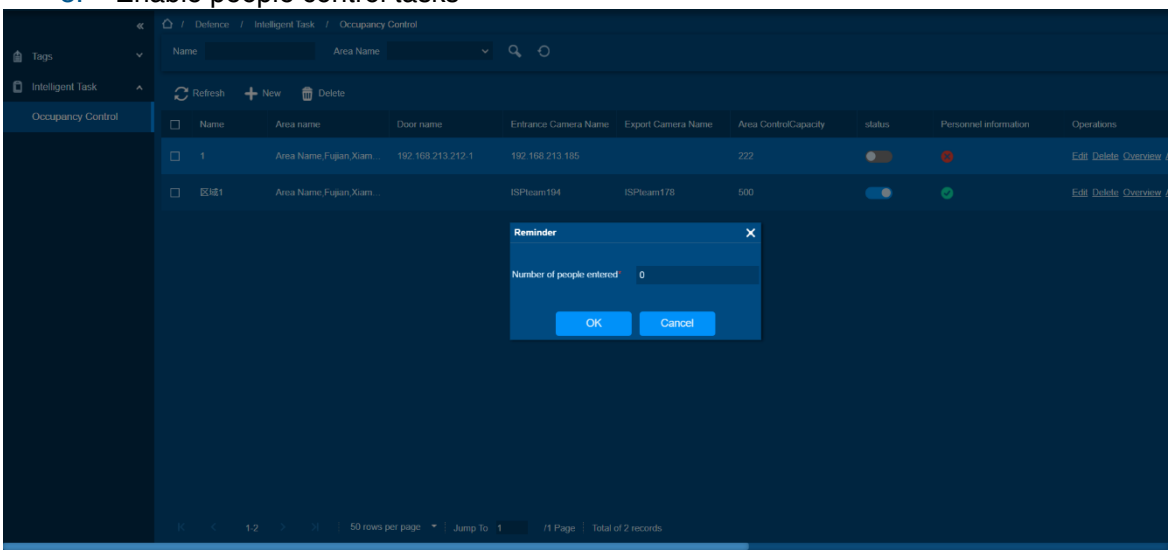
Create an occupancy control.

Steps:

1. Click [**New**].



2. Configure the parameters of the occupancy control
3. Enable people control tasks



Overview

Preconditions for Normal Use of Function

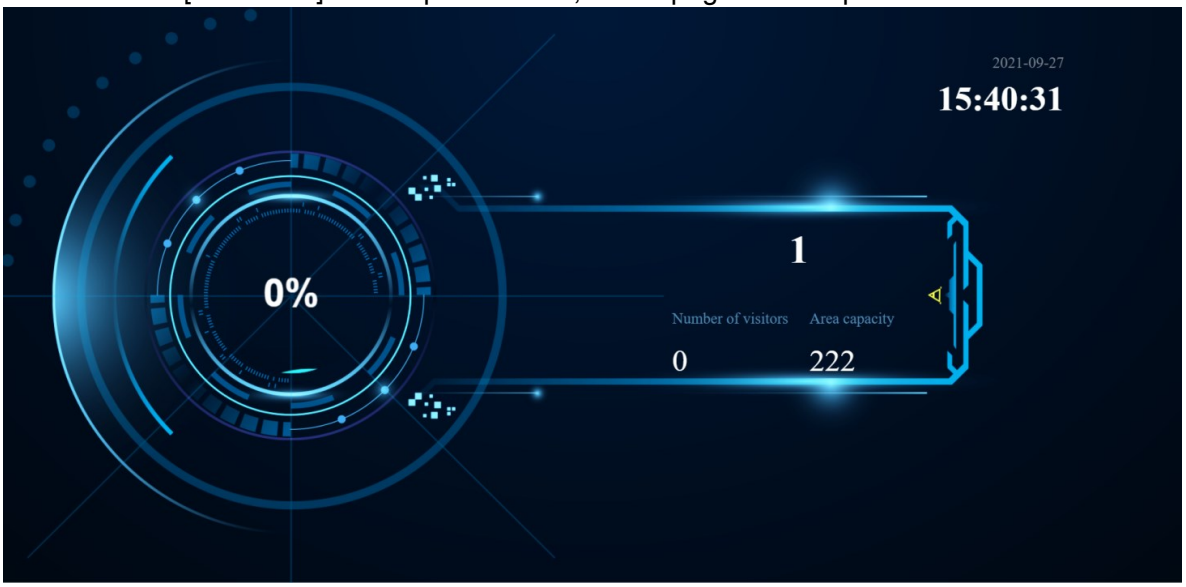
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

External large screen to display the number of people in the area to control the real-time situation.

Steps:

1. Click [**Overview**] in the operation bar, a new page will be open.



Administrator view

Preconditions for Normal Use of Function

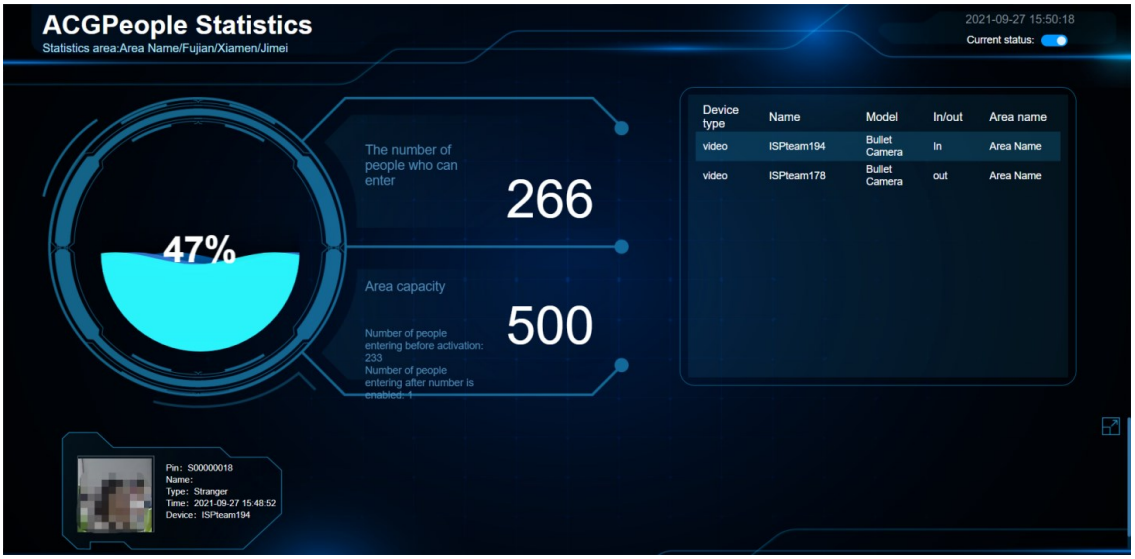
The software runs normally, and the account has the corresponding operation authority.

Function usage scenarios

For the administrator to monitor, can display the number of people in the area and personnel details.

Steps:

1. Click [**Administrator View**] in the operation bar, a new page will be open.



17.2.3. Muster Point

Designate the access control device of a certain place as the Muster Point. When an emergency event (such as a fire alarm) occurs, the linkage triggers the activation of the Muster Point to open the door, and the AC Device is used to count the escape of personnel, and quickly identify the escaped personnel and dangerous personnel.

Add Muster Point:

Select the access control devices as the equipment of Muster Point and assign the corresponding department.

✍**Note:**

The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

Steps:

Step 1: Set device as Muster Point, go to [**Defence**] > [**Intelligent Task**] > [**Muster Point**] > [**New: Sign device to the point**].

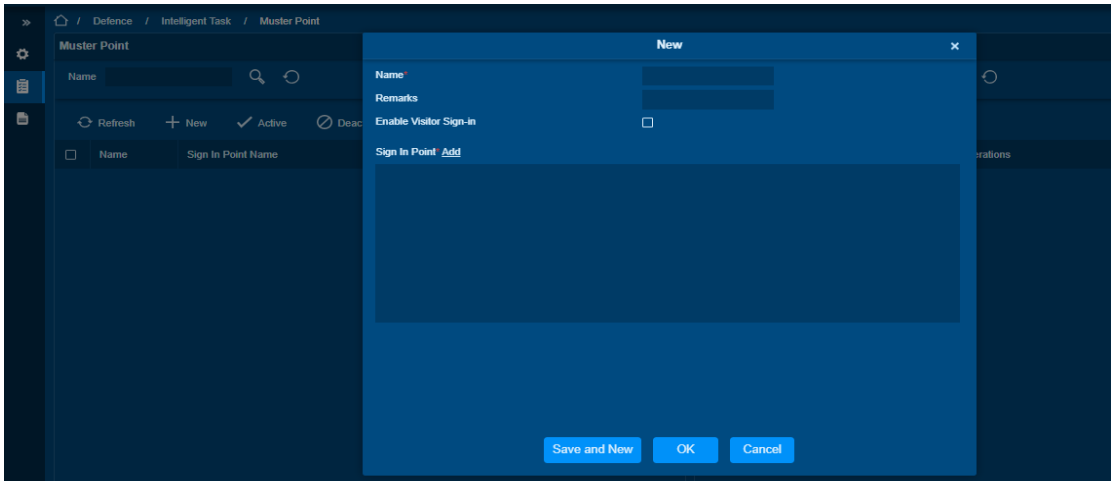


Figure-1-Sign Point

Step 2: Click [...] > [**Set Access by Department**] add department to the point.

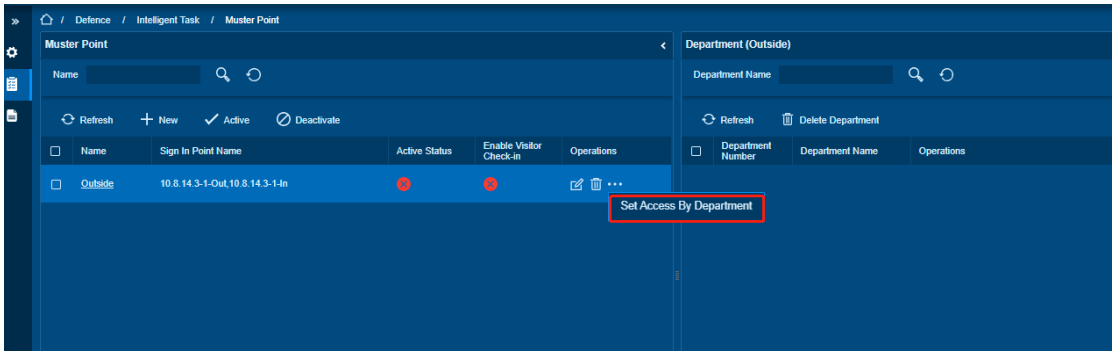


Figure-2-Add Department

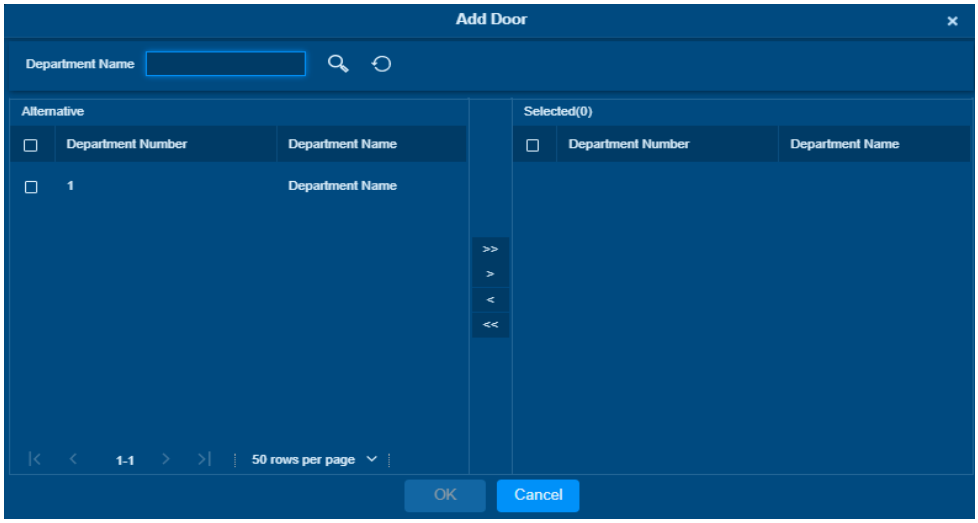


Figure-3-Add Department

Step 3: Set Global Linkage: set Linkage Trigger Conditions and Input Point, select Muster Point as an output action.

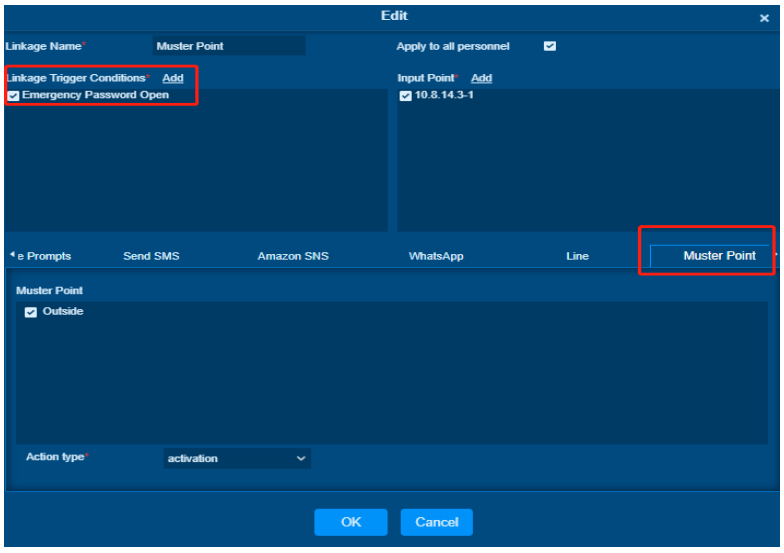


Figure-4-Global Linkage

Note:

Before you use global linkage, you must confirm that your device has enable background authentication.

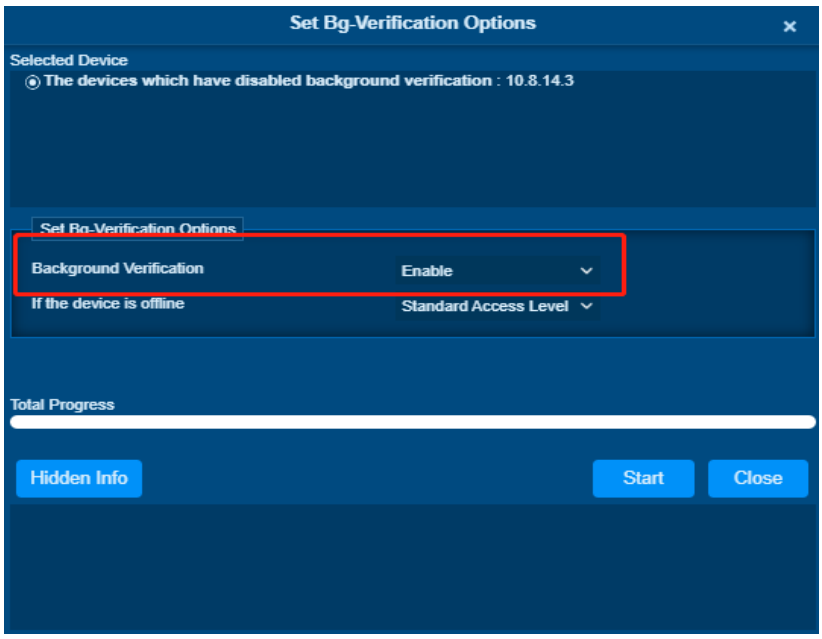


Figure-5-Enable BG-Verification Options

Activated

✍**Note:**

There are two methods to activate the muster point: manual activation and automatically activation through global linkage.

Manual Activation

Steps:

Step 1: Select a muster point and click [**Active**] in the tool bar.

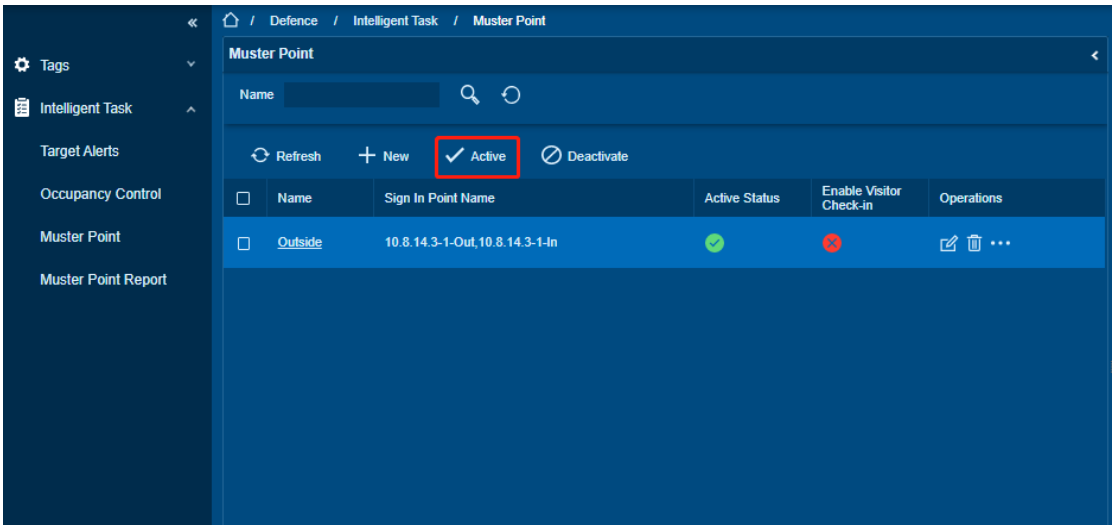


Figure-6-Active

Step 2: Click [**OK**] to confirm Active the muster point.

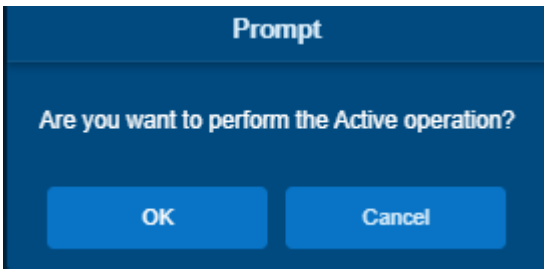


Figure-7-Active-OK

Automatically Activation Through Global Linkage:

When the linkage event is triggered, the door is remotely opened, and the Muster Point would be activated.

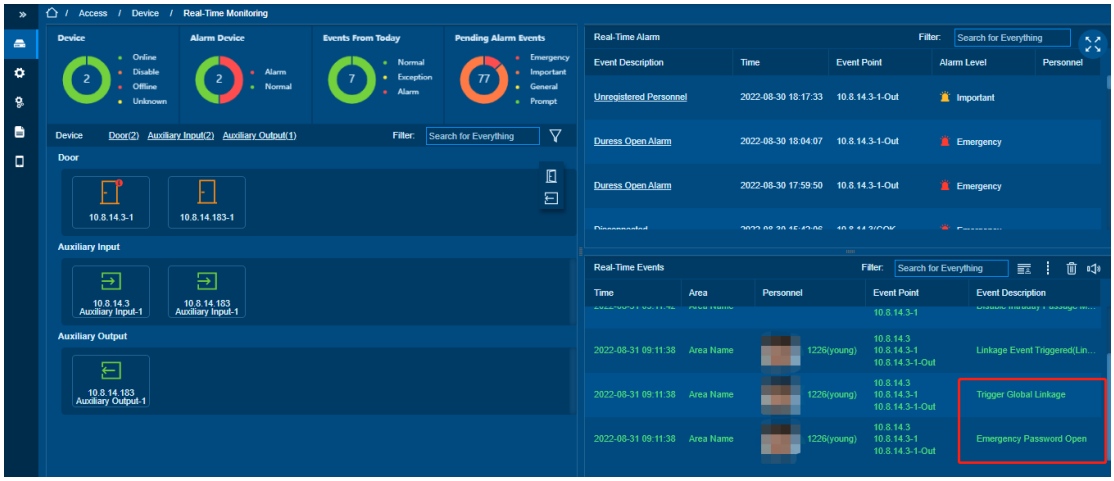


Figure-8-Real-Time Monitoring

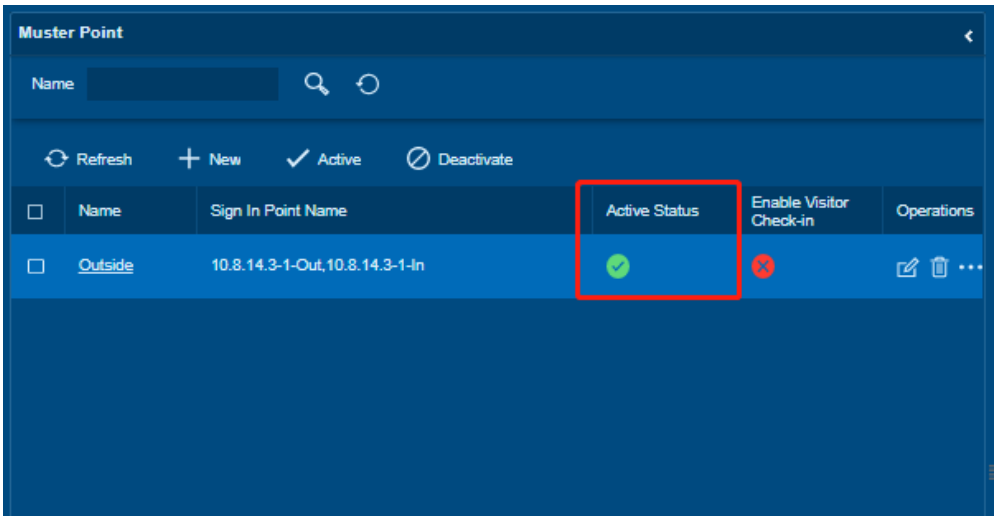


Figure-9-Muster Point

✍**Note:**

When the muter point is activated, user information will be synchronized to the device, people in the binding department will change to “Danger”.

Delete:

In the [**Defence**] > [**Intelligent Task**] > [**Muster Point**], click button under Operations. Click [**OK**] to delete.

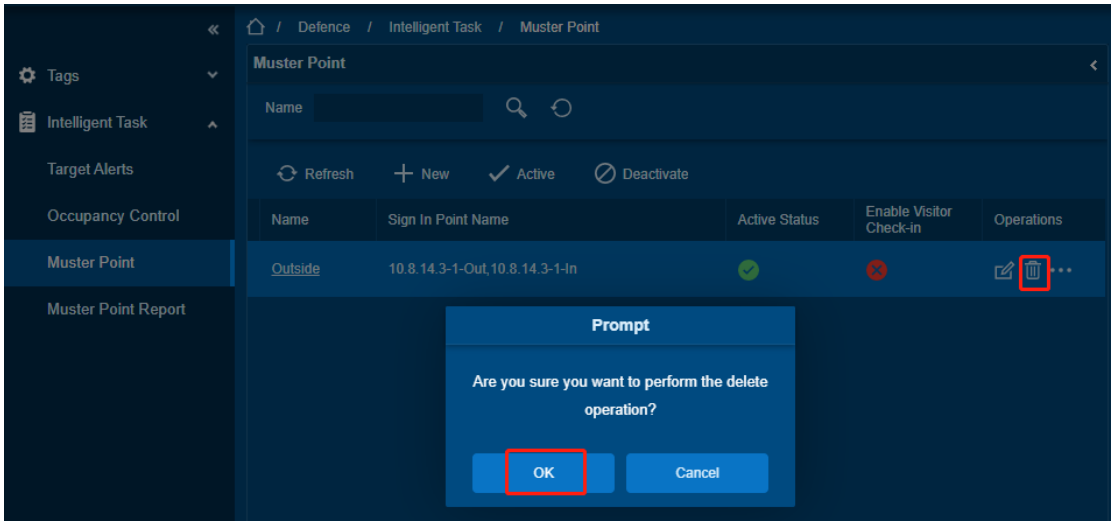


Figure-10-Delete Muster Point

Deactivate:

In the [**Defence**] > [**Intelligent Task**] > [**Muster Point**], click [**Deactivate**] button under Operations. Click [**OK**] to deactivate.

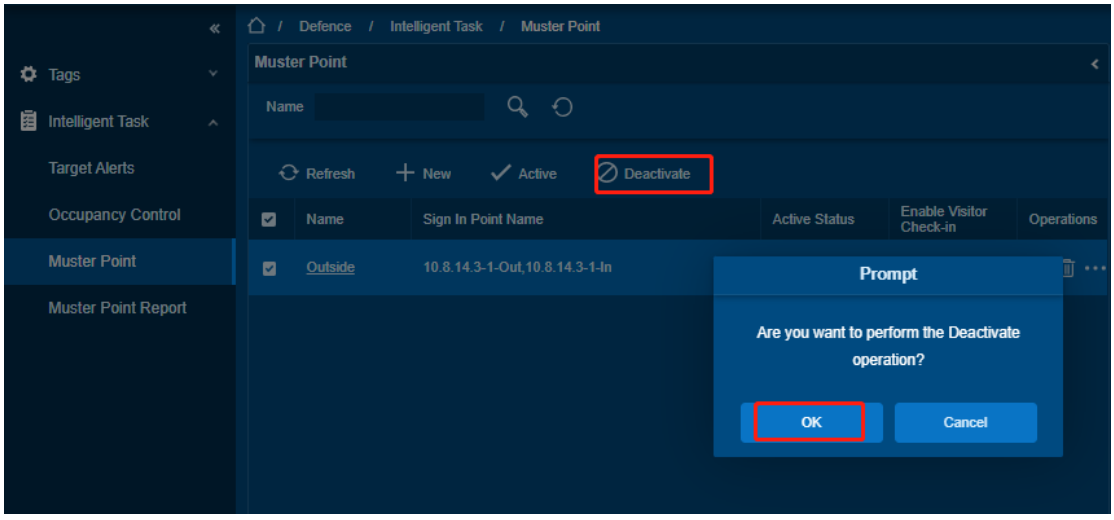


Figure-11-Cancel Muster Point

17.2.4. Muster Point Report

Select the access control devices as the equipment of Muster Point and assign the corresponding department.

✍**Note:**

The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

Step:

Step 1: Set device as Muster Point setting, go to [**Defence**] > [**Intelligent Task**] > [**Muster Point Report**], select [**Muster Point Name**].

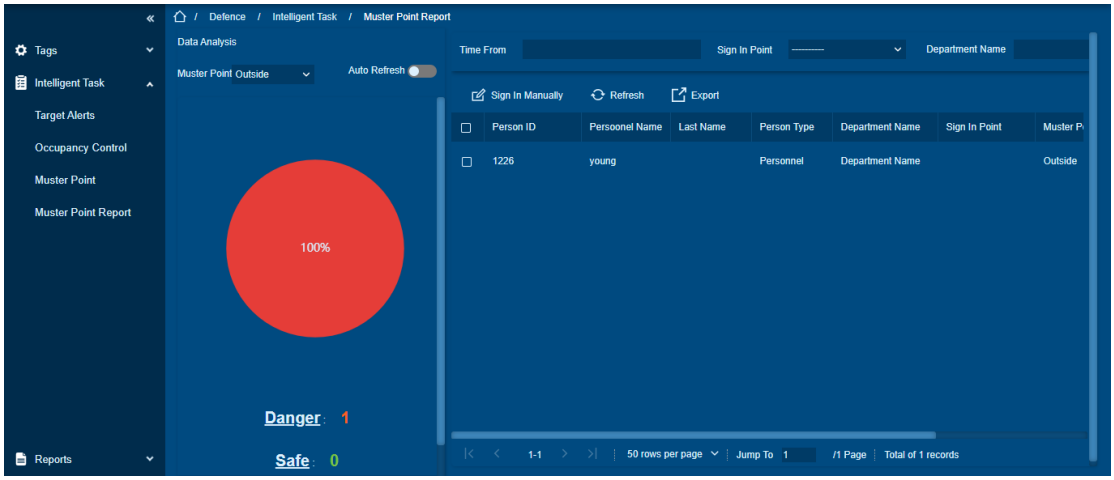


Figure-12-Check the Report

Sign In Manually:

✍**Note:**

There are two sign-in modes: one is that users sign in through the verification of device, and the other is that administrators help users sign in manually.

If a user is not verified on the device, the administrator can sign in manually: Select [**Sign in Manually**], as shown in the figure below.

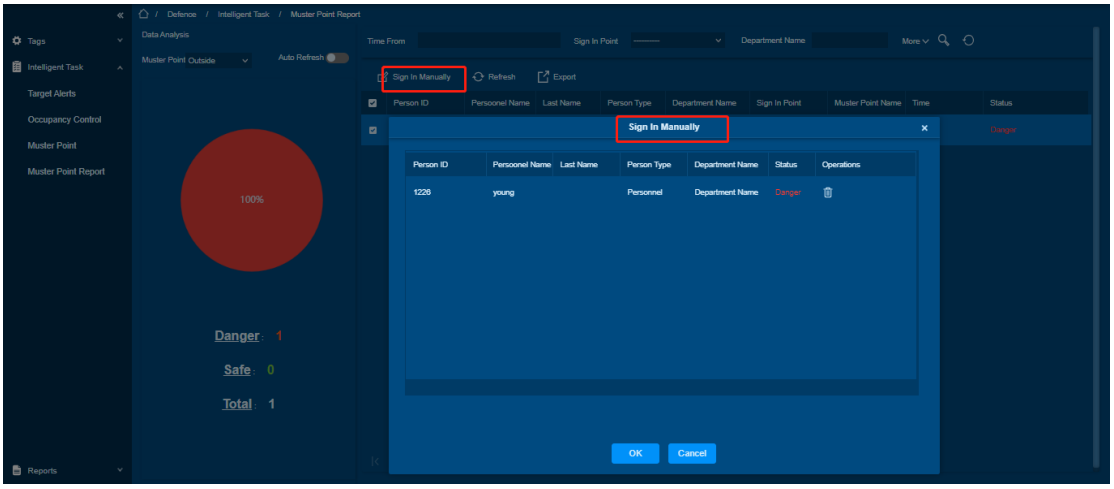


Figure-13-Sign in Manually

After finishing the sign-in, check the Statues will change to “Safe”.

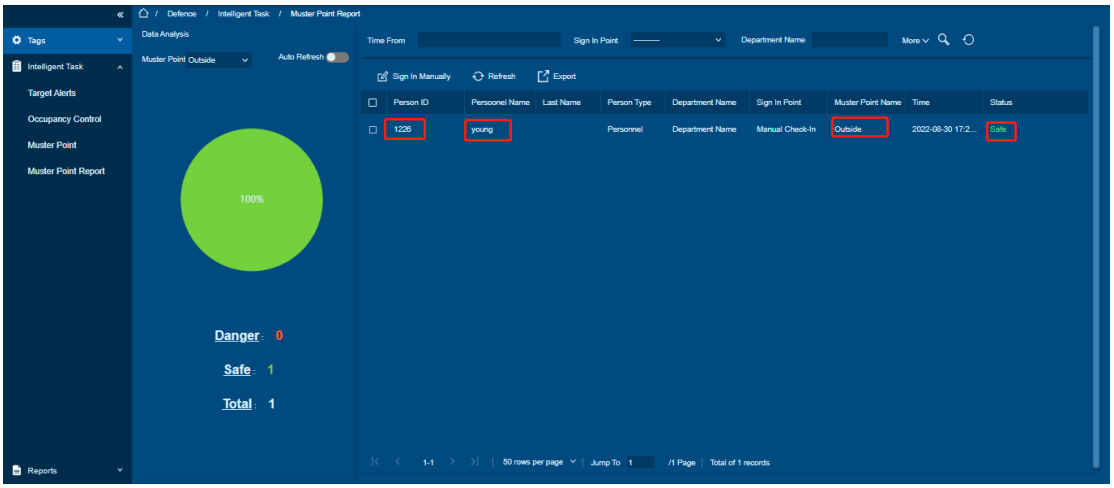


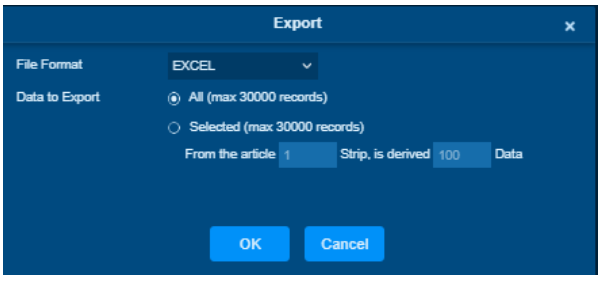
Figure-14-Sign in Manually

✍**Note:**

If it is verified on the device, the Statues will change to "safe."

Export:

Click [**Export**], select the file format to export, and Click [**OK**].



Muster Point Report

Person ID	Persoonel Name	Last Name	Person Type	Department Name	Sign In Point	Muster Point Name	Time	Status
1226	young		Personnel	Department Name	defence_master_point_report_manual_checkIn	Outside	2022-08-30 17:25:22	Safe

Figure-15-Export

17.3. Reports

Function List

Operations	Description
Alarm Reports	Store and view alarm records generated by Target Alerts

17.3.1. Alarm Reports

Function Description

Use this function to view Target Alerts task alarm records.

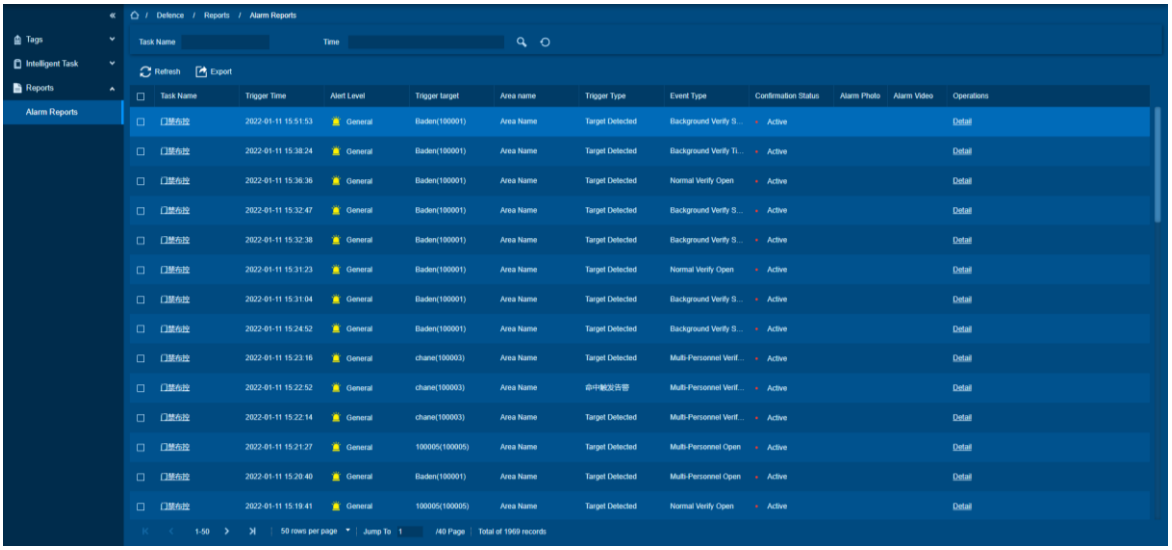
Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

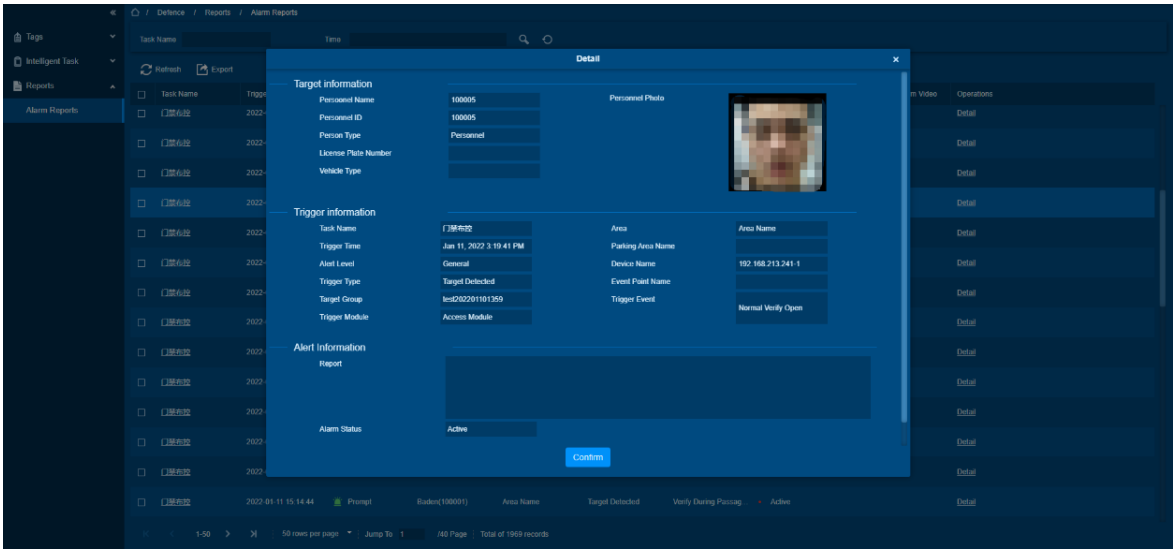
Function usage scenarios

Review an alarm record.

Steps:



1. Click [**Detail**] to view alarm detail.



18. Building Automation

The Building Automation enable the administrator to manage the building more intelligently, conveniently, and simply. The purpose is to improve occupant comfort and utility life, efficient operation of building systems, reduce energy consumption and operating costs and automatic centralized improve control lighting and temperature, etc. Now we can support common brands sensors, such as Honeywell, Johnson Controls and so on.

Module Function List

Functions	Descriptions
Gateway	Gateway devices add, delete, view.
Terminal	Terminal delete, edit, add, search, view and configure terminal attribute.
Attribute Monitoring	The administrator monitors the terminal equipment in real time according to the classification of the terminal or the subsystem.
Regulation Center	Setting a linkage rule. After a specific event is triggered by an input point in the regulation center, a linkage action will be generated at a specific output point to device such as Email, monitor, access, and SMS.
Events Report	Display all alarm report.
Regulation Report	Display all linkage report.
Subsystem	Categorize the device terminal.
Icon Library	Upload, search, delete and view icon.

18.1. Device

Function Description

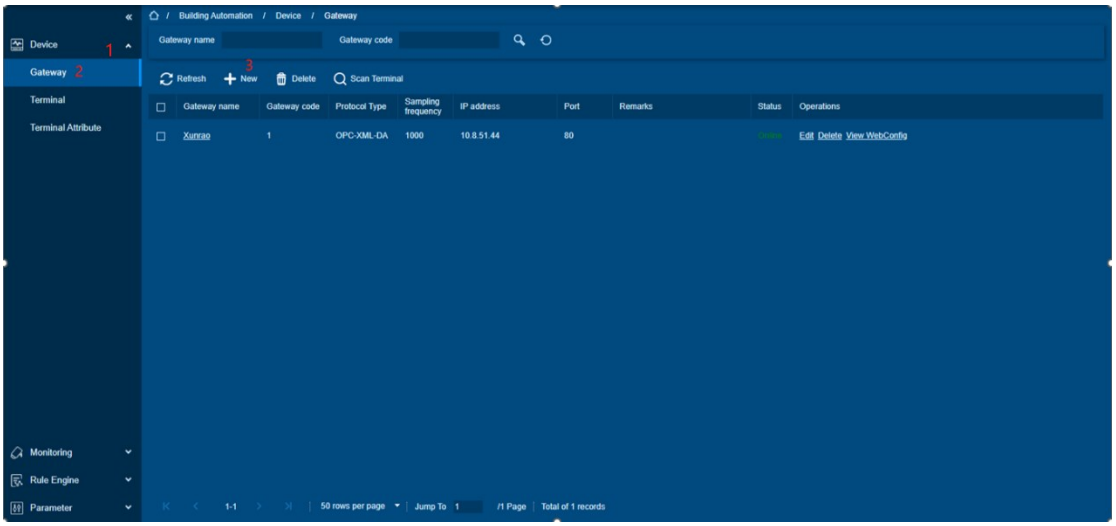
Device management, support adding, deleting, setting device status, obtaining, and viewing device parameters and records. Devices include gateway and terminal.

18.1.1. Gateway

When using the building automation program, the user first need to add a gateway to the system. The protocol types currently supported by our system are OPC-XML-DA. The main functions of Gateway Management include Add, Edit, Delete, scan terminal.

Add gateway

1. Click **[Building Automation]** >**[Device]** >**[Gateway]** > **[New]**



2. On the New interface, enter Gateway name, Gateway code, Protocol Type and the other details displaying in the below image.
3. Click OK and save the settings.

✍**Note:**

- The protocol types currently supported by our system are OPC-XML-DA.
- The time frame for sampling frequency within 1000ms to 2000ms.

Search gateway

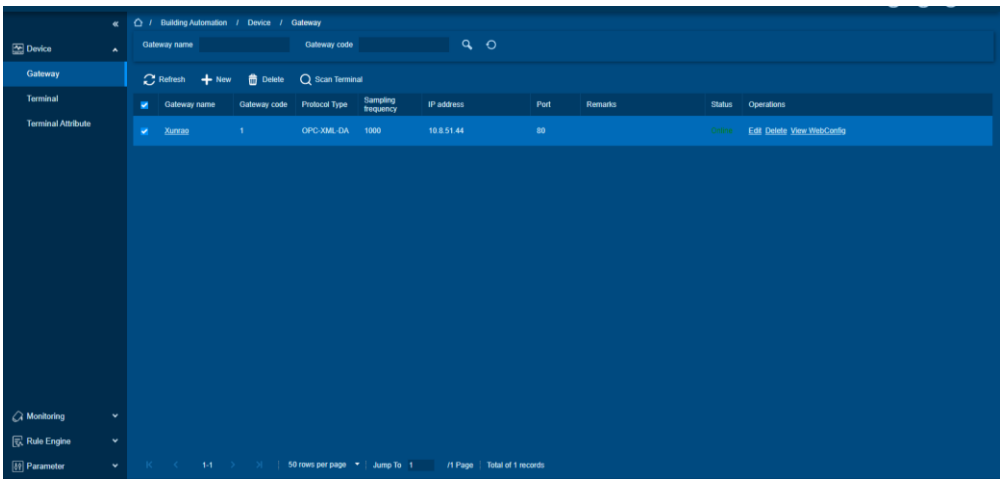
- Click [Gateway name] or [Gateway code] then enter Gateway name or Gateway code to search target.

✍**Note:**

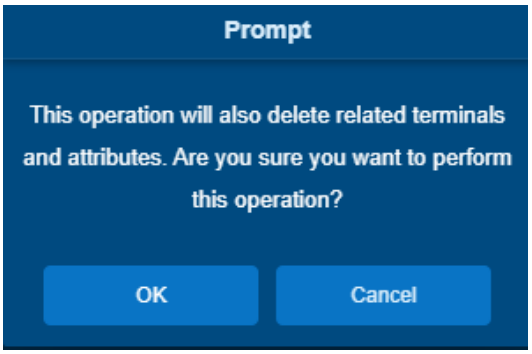
- System is support fuzzy search.

Delete gateway

1. Click **[Device]** > **[Gateway]**, then select the gateway.



2. Click **[Delete]** > **[OK]**

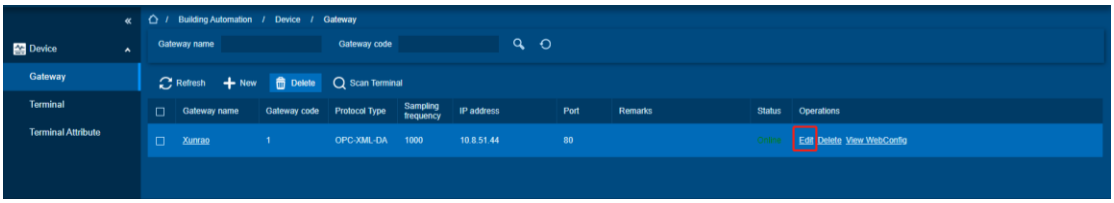


✍**Note:**

- All relevant information about the gateway will be deleted.
- If the gateway cannot be deleted, it may be occupied

Edit gateway

- Click **[Device]** > **[Gateway]**. Then select the desired gateway and click **[Edit]**.



✍**Note:**

- After the gateway has been added, the user can edit the parameters of the gateway in the interface, such as IP address, Gateway name, Sampling frequency, Ports.

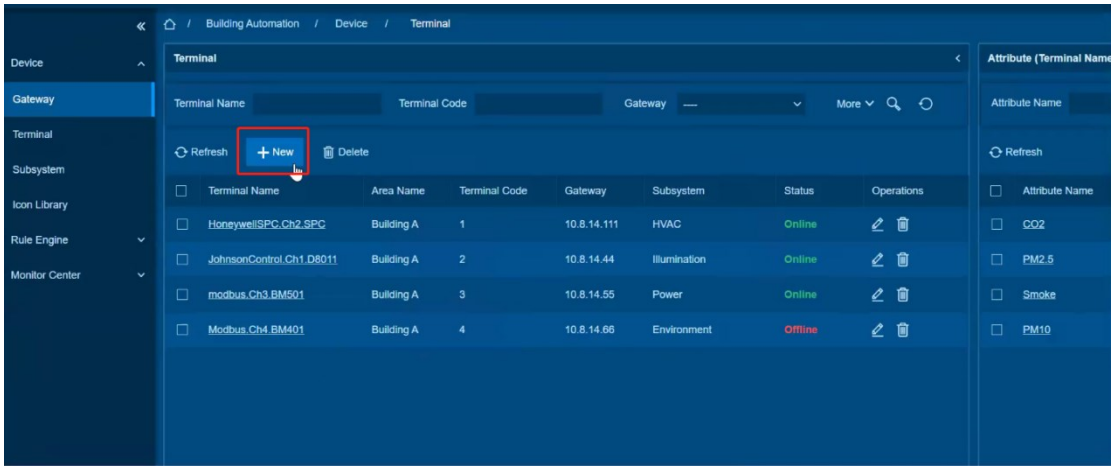
18.1.2. Terminal

After adding the gateway, the user needs to add a terminal device to collect some parameter, such as carbon dioxide concentration, temperature, whether the light is off or on and so on. Our system supports

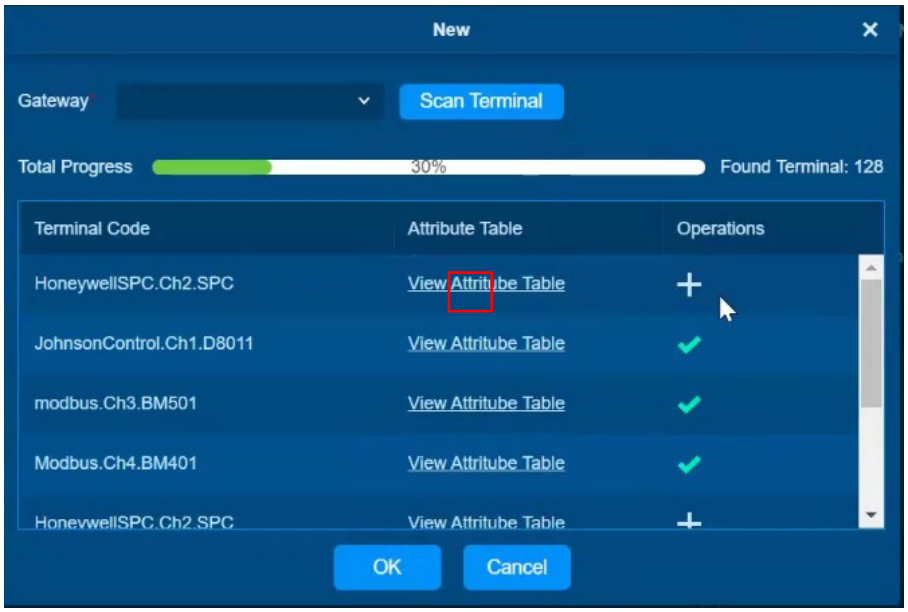
terminal equipment from most manufacturers on the market, for example, Honeywell, Bosch, Johnson Controls, Siemens, etc.

Add Terminal

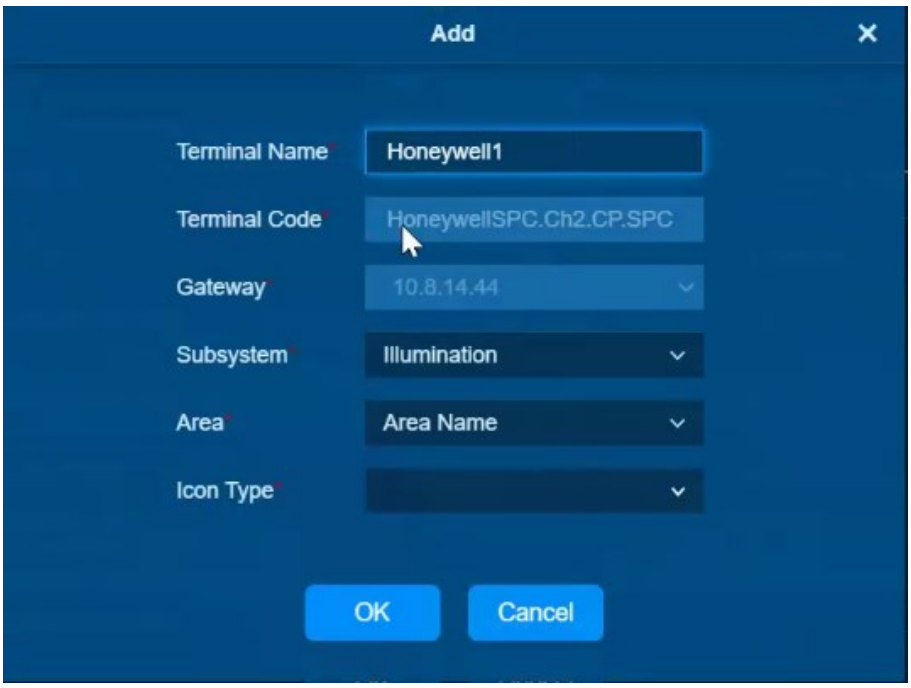
1. Click **[Building Automation]** >**[Device]** >**[Terminal]** > **[New]**



2. Click **[Gateway]** Then choose the gateway and click Scan Terminal.
3. Choose the gateway you need, then click OK.
4. Then choose the terminal and click plus.



5. Enter Terminal name, Terminal Code, Gateway, Subsystem, Area, and Icon Type, then click OK and save the settings.

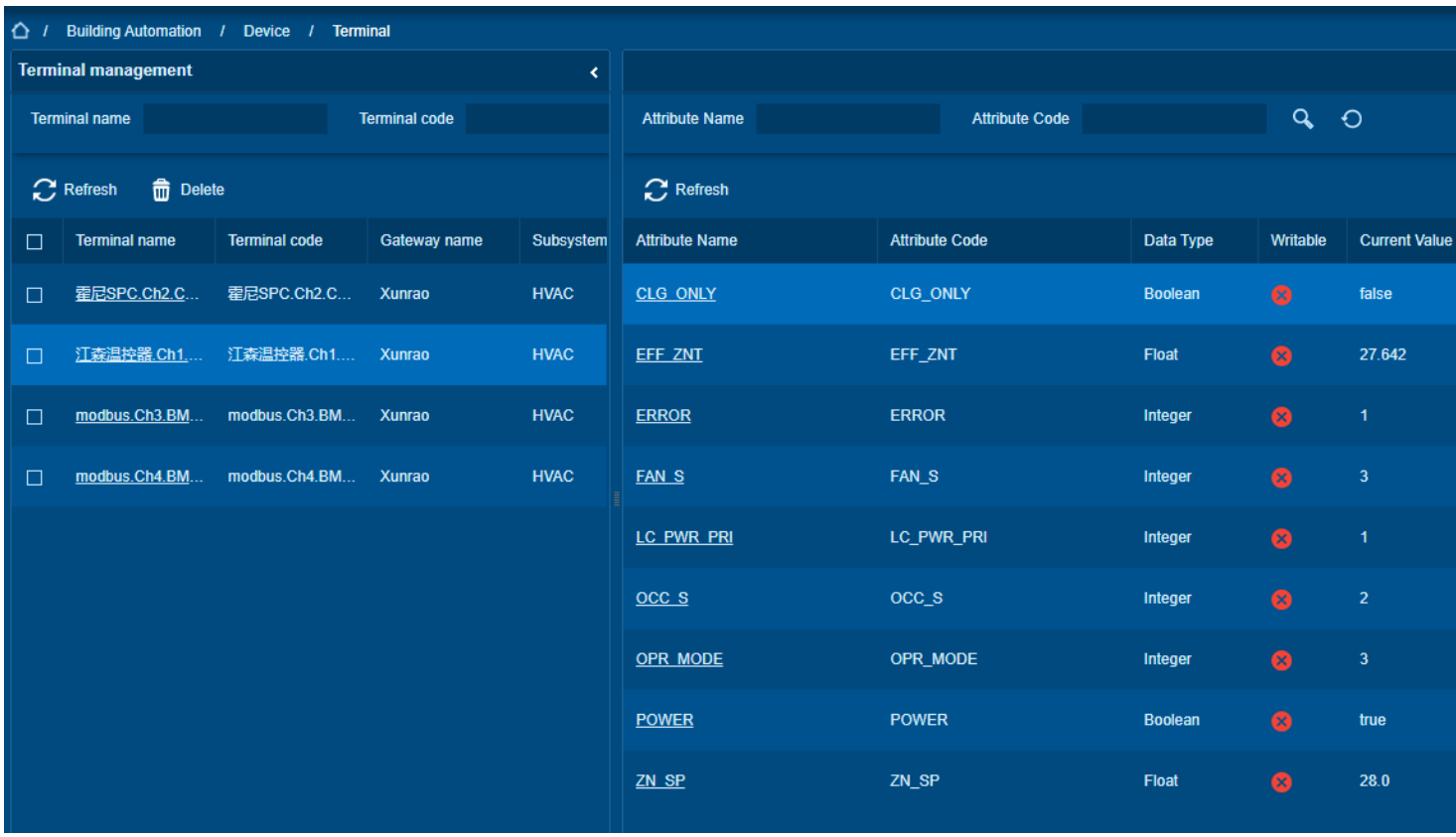


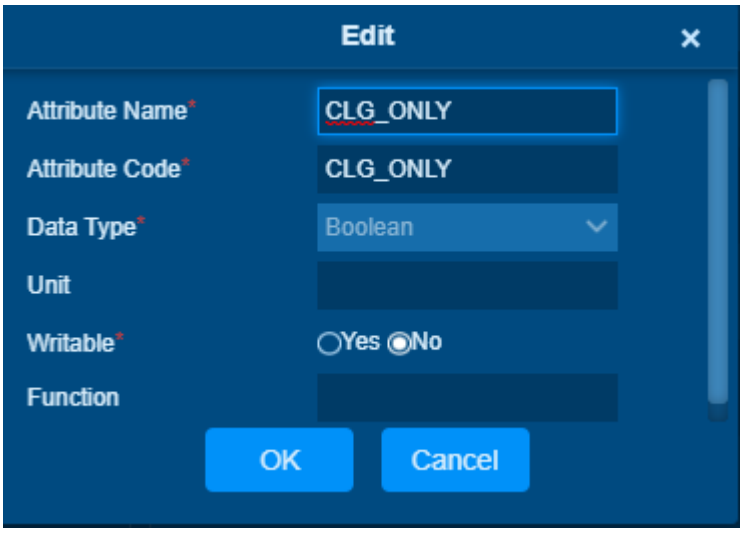
✍**Note:**

1. The administrator should ensure terminal device has been matched with the gateway.
2. User could preview which parameters the sensor can obtain such as smoke, pm2.5 through view terminal attribute.
3. Ordinary users can only see authorized area devices.

Preview Terminal Attribute

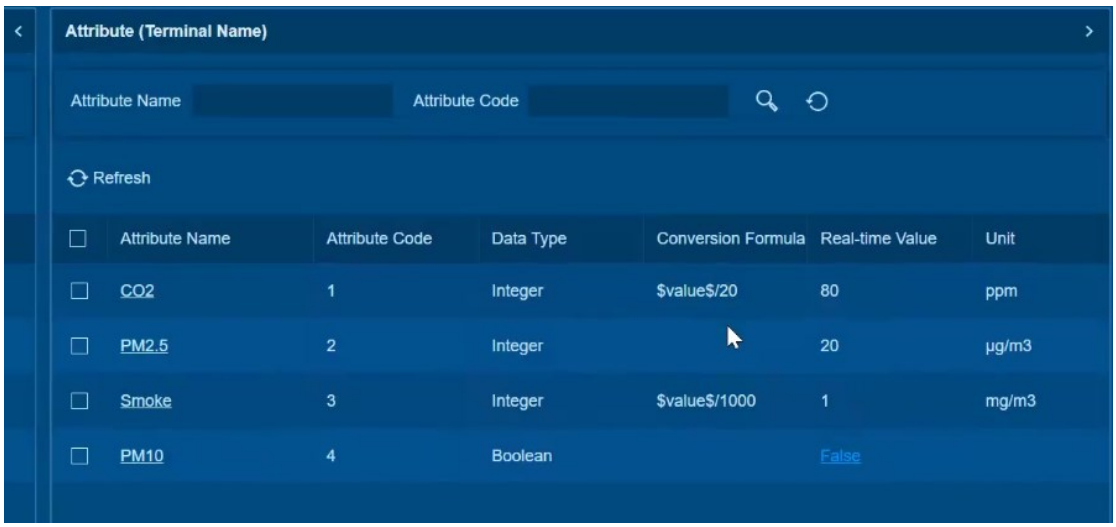
On the interface, users can click on different terminal devices to preview the properties corresponding and set terminal attribute.





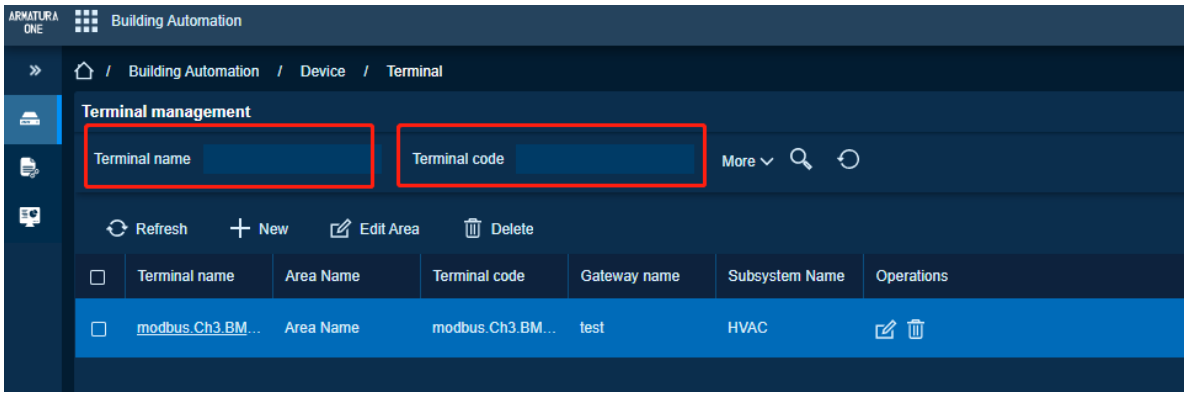
✍**Note:**

- Terminal attribute can be set by user such as data type, conversion formula, unit and so on.



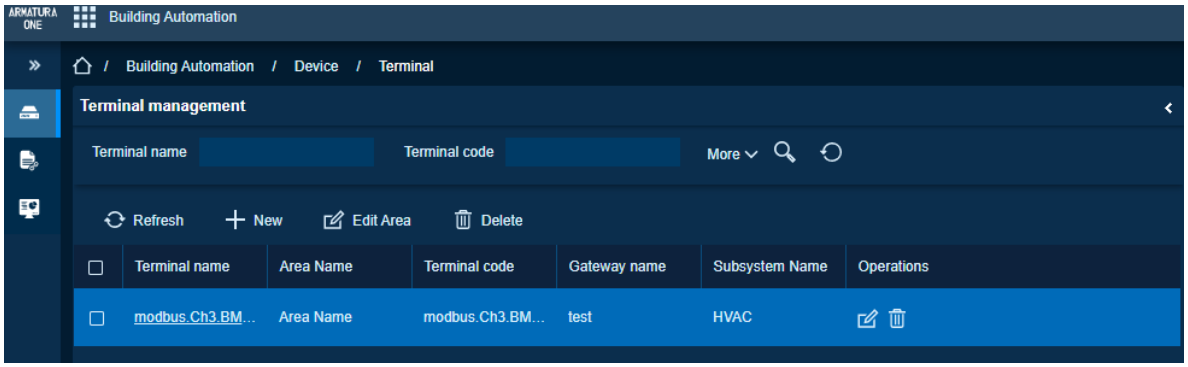
Search Terminal

- Click **[Terminal name]**, **[Terminal code]** or **[Gateway name]** then enter Terminal name, Terminal code or Gateway name to search target.

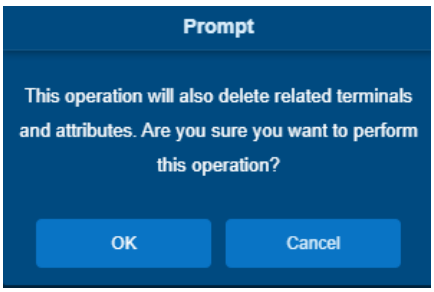


Delete Terminal

1. Click **[Device]** > **[Terminal]**, then select the Terminal



2. Click [Delete] > [OK]

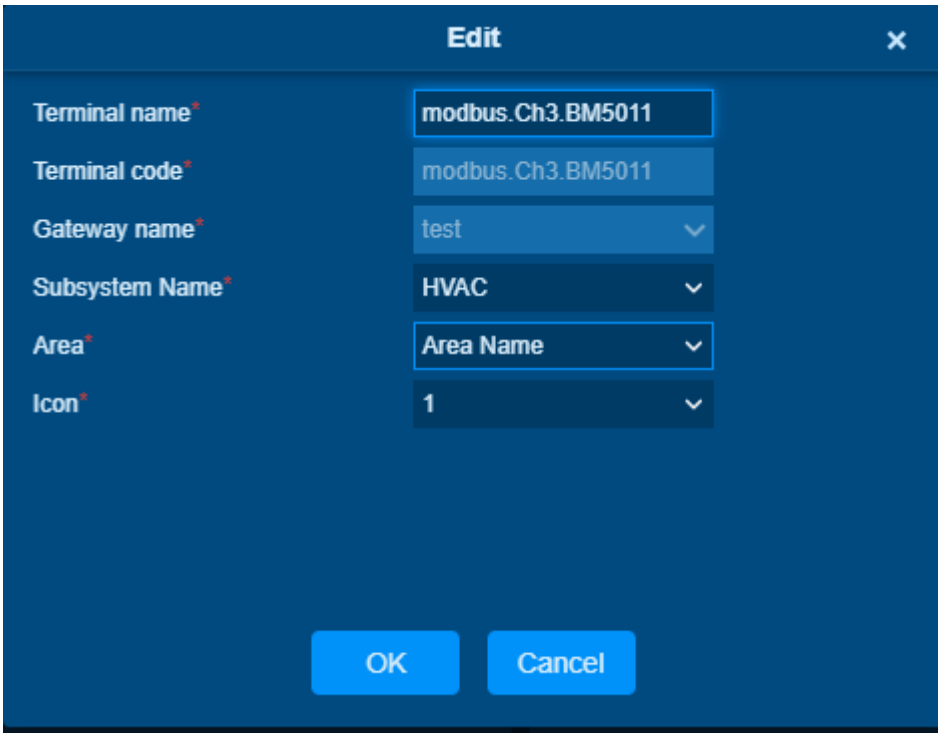


✍**Note:**

- All relevant information about the gateway will be deleted.
- If the gateway cannot be deleted, it may be occupied
- System is support fuzzy search.

Edit gateway

Click on the device name to edit then click OK and save the settings.

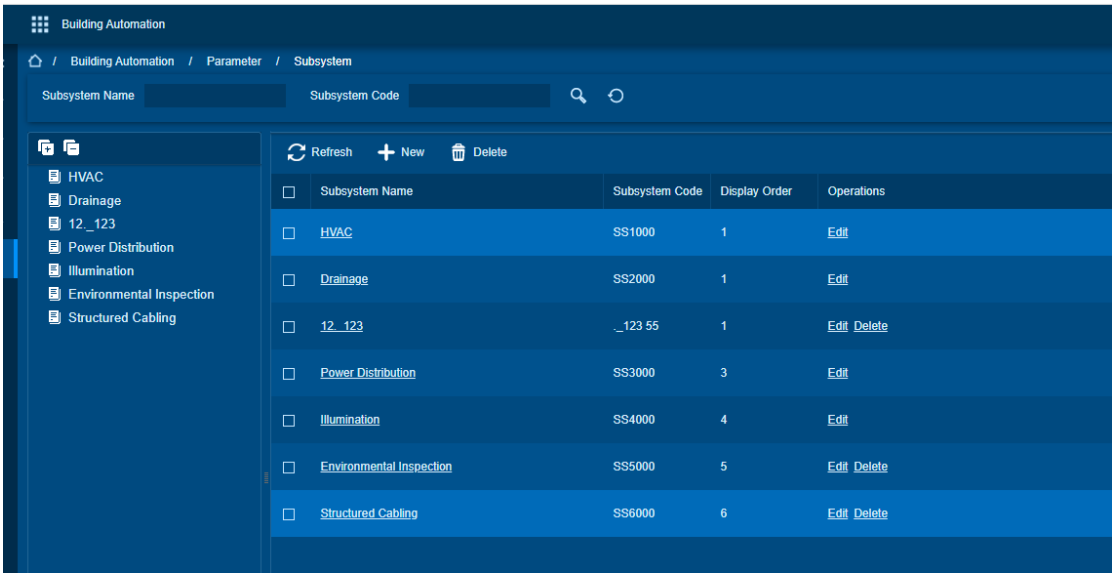


18.1.3. Subsystem

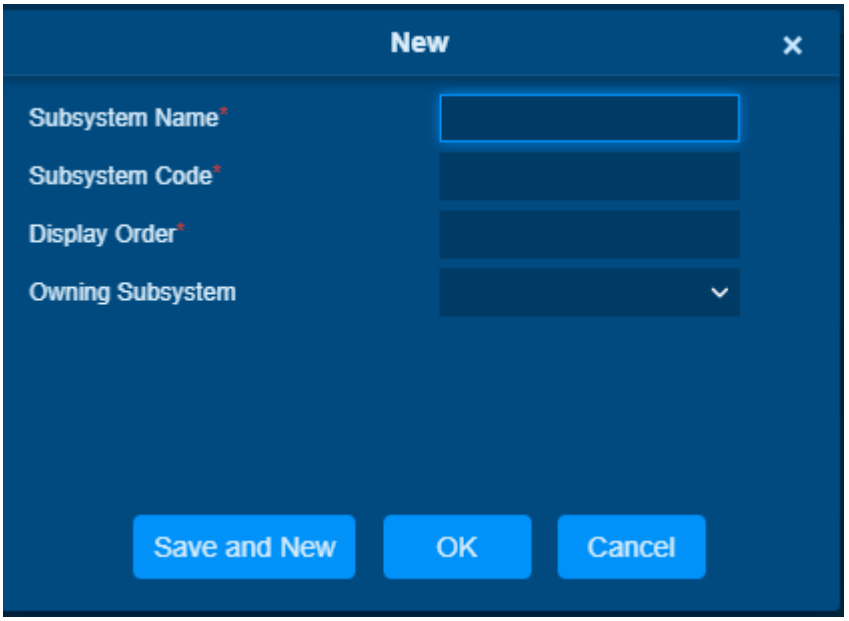
The subsystem is to classify the terminal which can help user find the terminal quickly. Administrator is able add, delete, edit, search and view subsystem.

Add subsystem

1. Click [Parameter] >[Subsystem]> [New]



2. Enter subsystem name, subsystem code, display order and owning system.



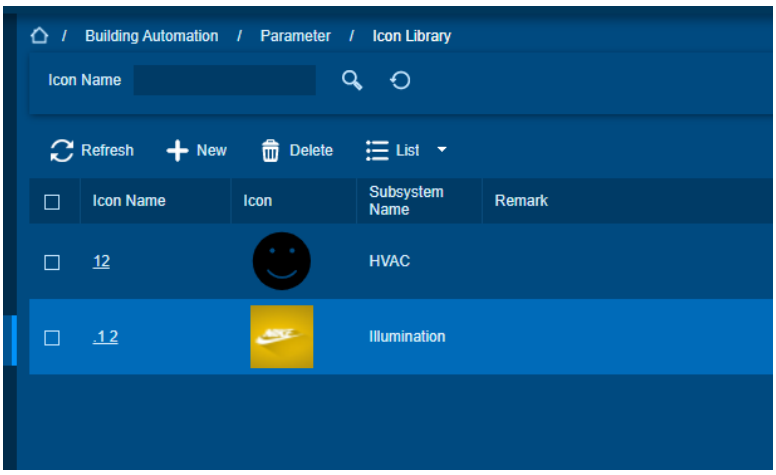
Click [Save and New] or [OK] save the settings.

18.1.4. Icon Library

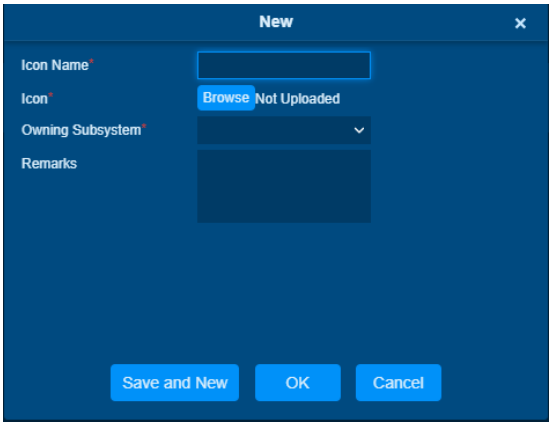
User can upload, search, delete and view icon in the library. And administrator need some icons to define terminal properties which can help user comprehend terminal attribute quickly.

Add icon

1. Click [Parameter] >[Icon Library]> [New]



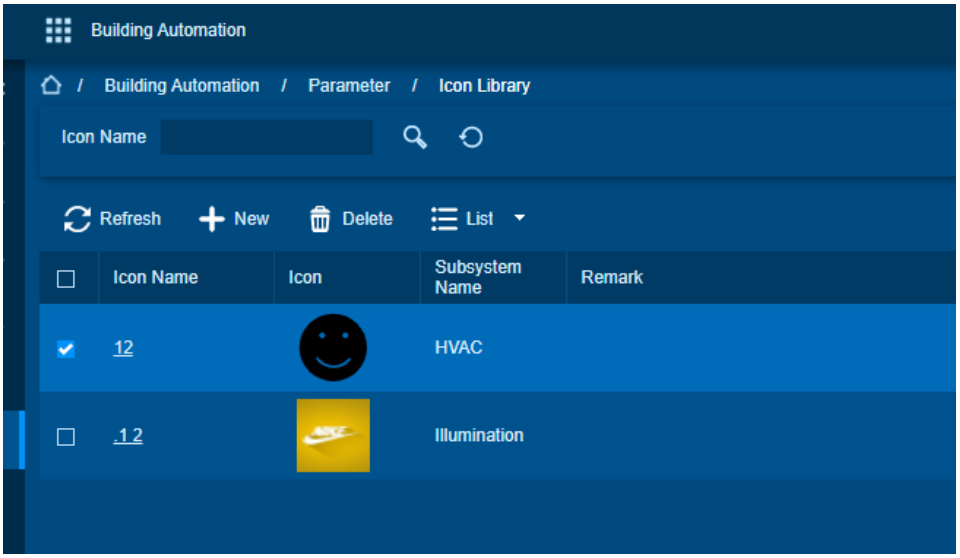
2. Enter icon name, upload icon and choose owning subsystem.



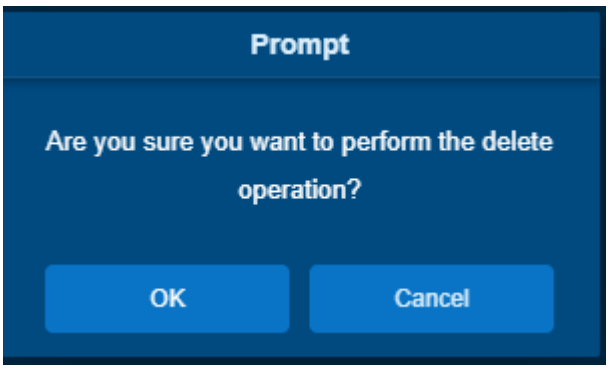
3. Click OK and save the settings.

Delete icon

1. Click [Parameter] >[Icon Library], then select the icon.

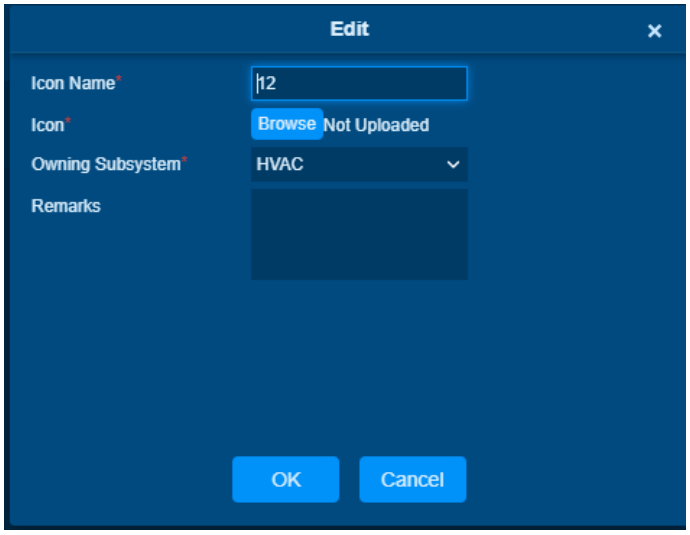


2. Click [Delete]> [OK]



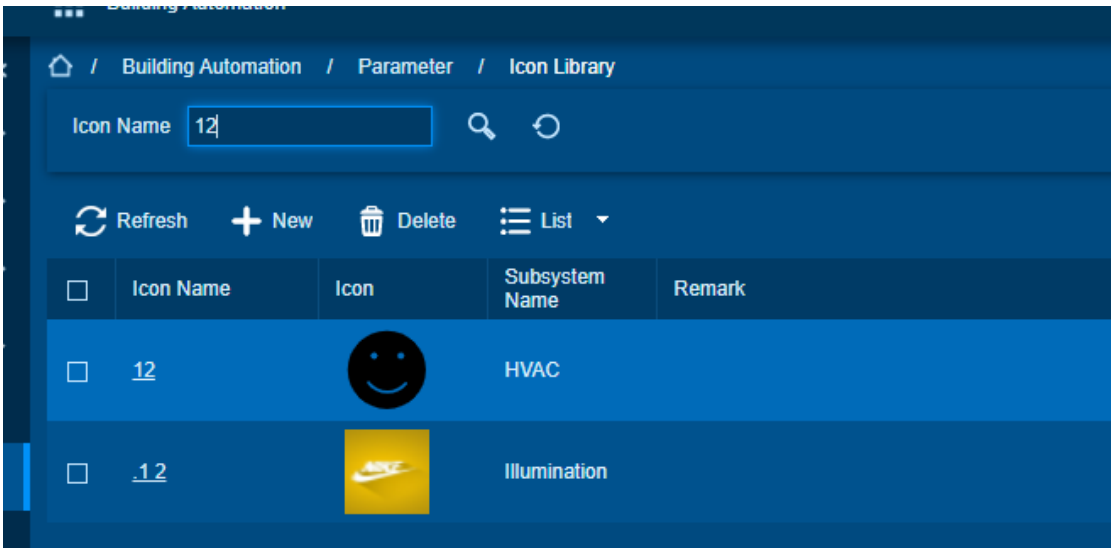
Edit icon

1. Click [Parameter] > [Icon Library], then click the icon name.
2. User can edit icon name, re-upload icon and reselect owning subsystem.



Search icon

1. Click [Parameter] > [Icon Library]
2. Enter icon name to search target.



Note:

- System is support fuzzy search.

18.2. Rule Engine

Function Description

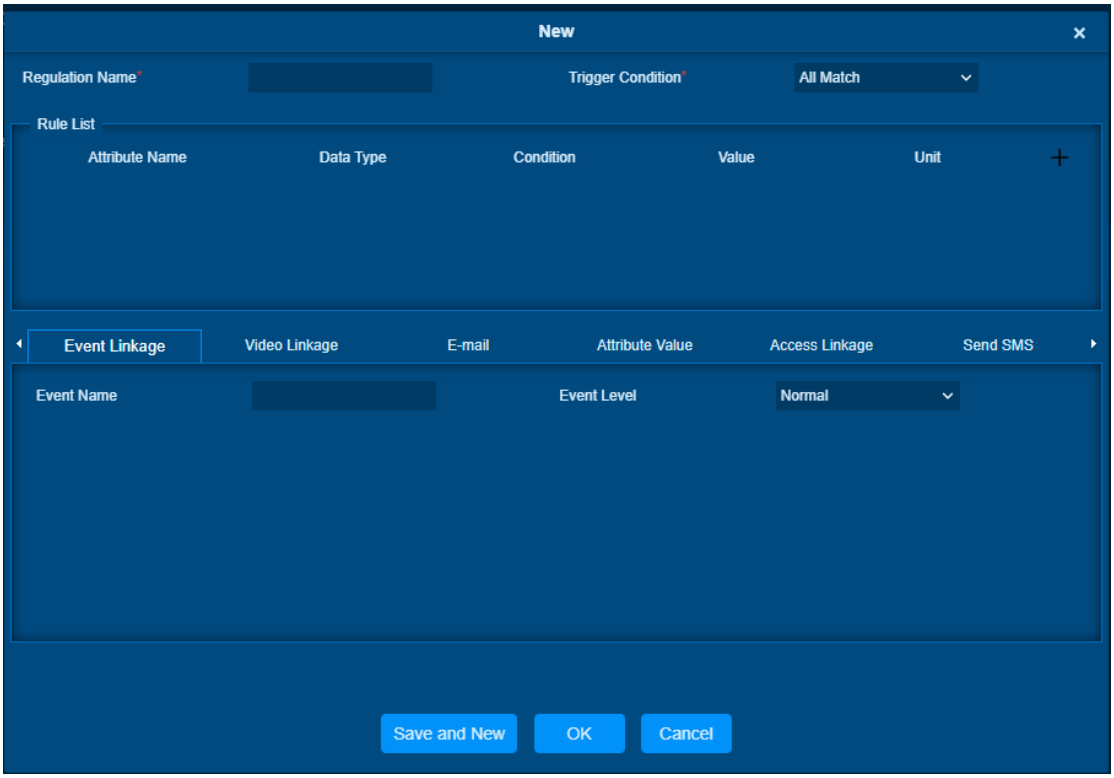
Rule engines provide a platform for user to create various linkage rule and view event and regulation report in rule engine.

18.2.1. Regulation Center

Regulation Center is equivalent to linkage, when an event is triggered at an input point of the terminal, a linkage action will occur at the specified output point, such as send email and SMS, linkage access control and video and list them in the corresponding monitoring view.

Add regulation

1. Click **[Building Automation]** > **[Rule Engine]**> **[Regulation Center]** > **[New]**
2. On the New interface, enter Regulation Name, choose Trigger Condition, create new rules, and set output point.
3. Click OK and save the settings.

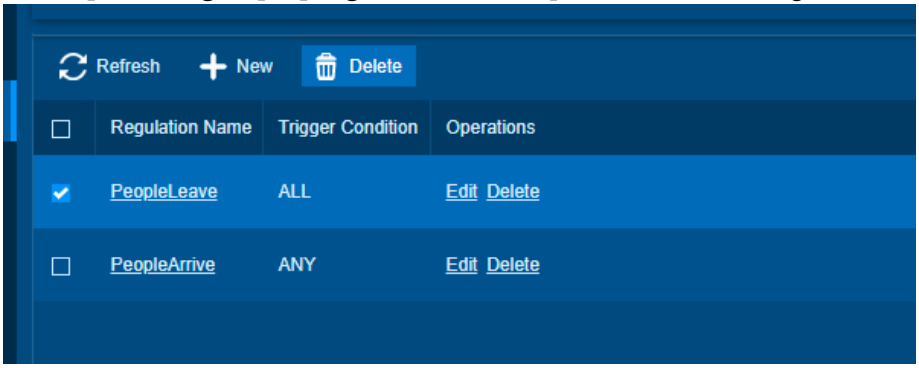


✍**Note:**

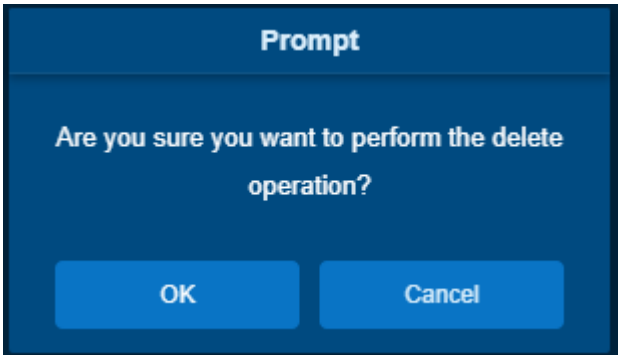
- Trigger condition is divided into two types. One type is linkage will not be triggered until all conditions are met. The other type is linkage will be triggered if at least one condition is met.
- Rules can be created, delete, edit by user.

Delete regulation

1. Click **[Rule Engine]** > **[Regulation Center]**, then select the regulation.

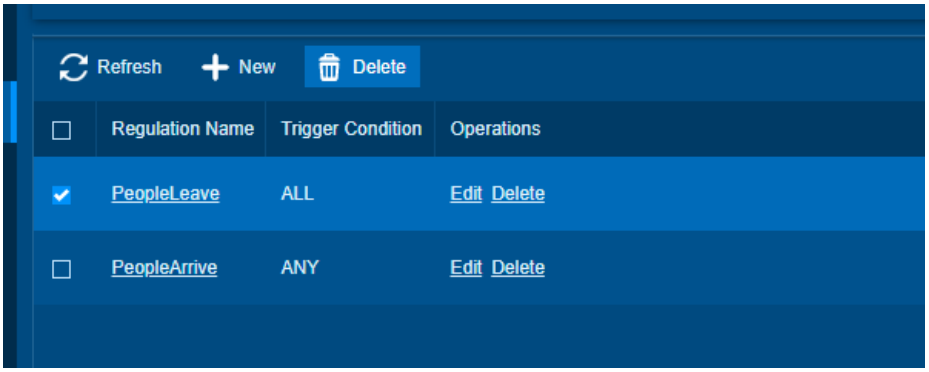


2. Click **[Delete]**> **[OK]**

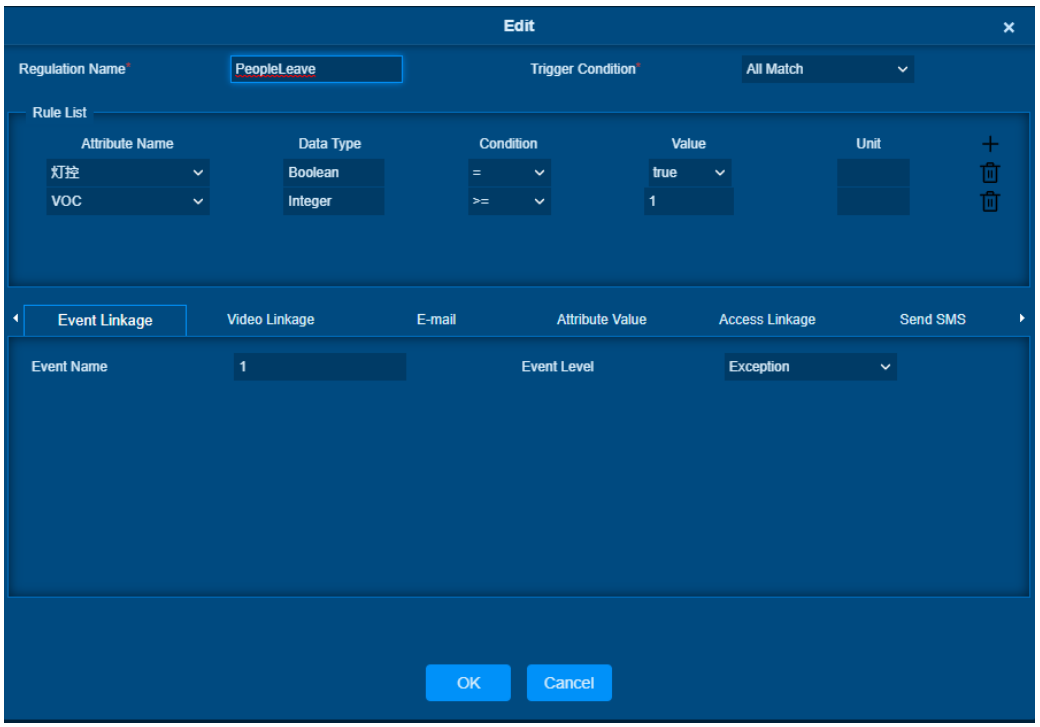


Edit regulation

1. Click **[Rule Engine]** > **[Regulation Center]**, then select the regulation.

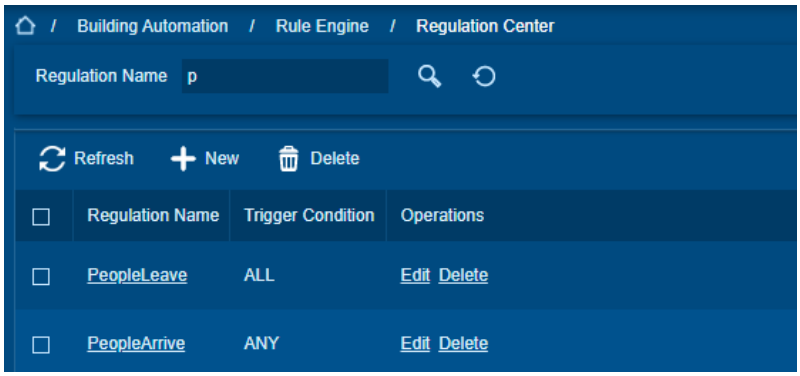


2. Click **[Edit]**> **[OK]**



Search regulation

1. Click **[Rule Engine]** > **[Regulation Center]**
2. Enter regulation name to search target

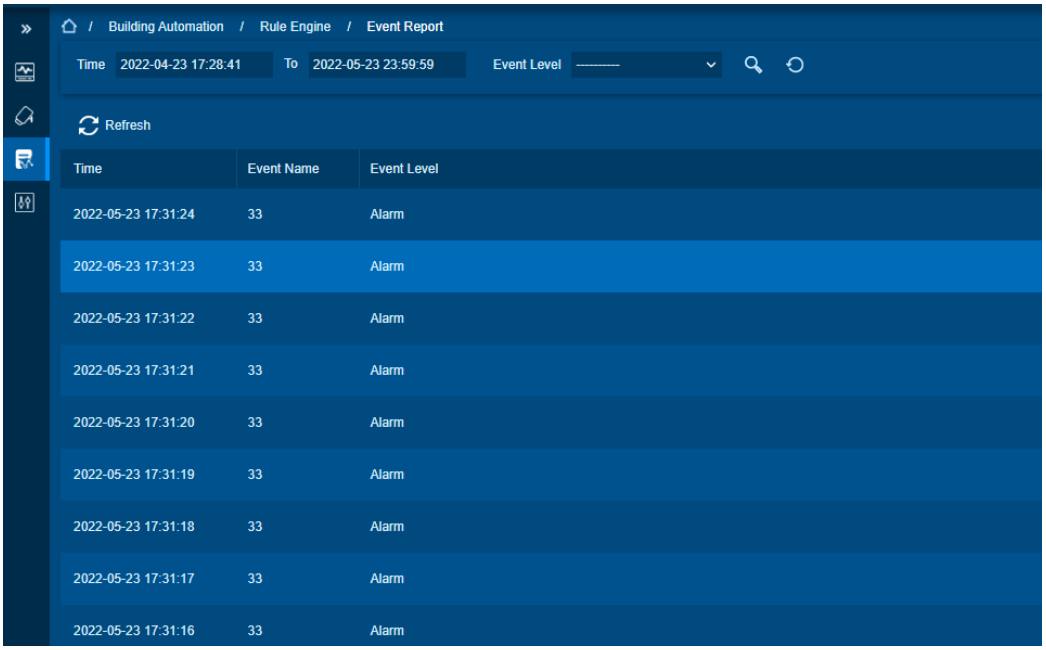


✍**Note:**

- System is support fuzzy search.

18.2.2. Event Report

All event linkage records will be saved in Event Report. And it displays event occur time, event name and event level.

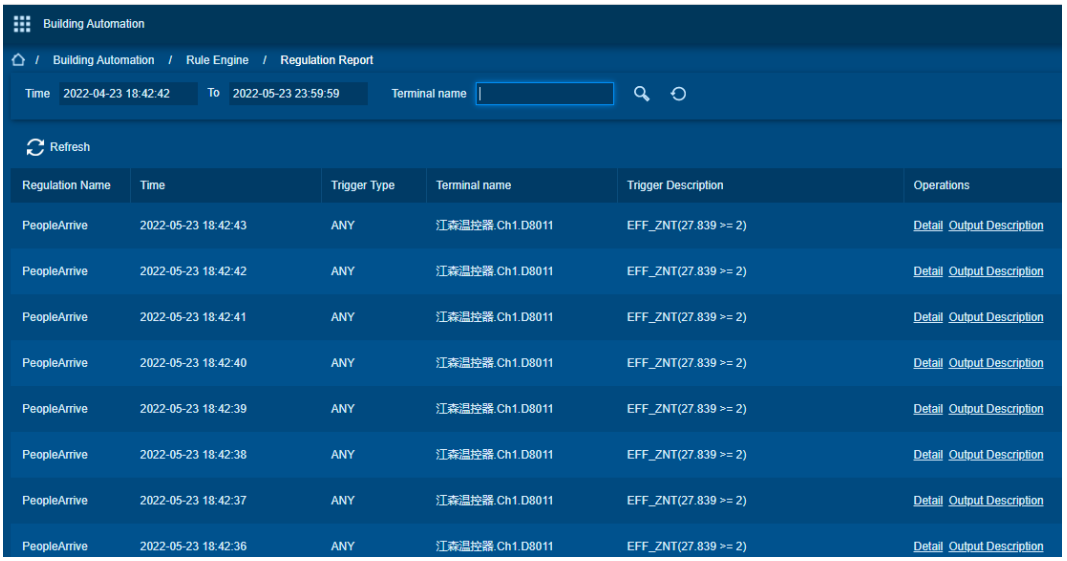


✍**Note:**

- According to the time frame and event level, user is able to filter out target events.
- Event level are divided into normal, exception and alarm, which is defined by user.

18.2.3. Regulation Report

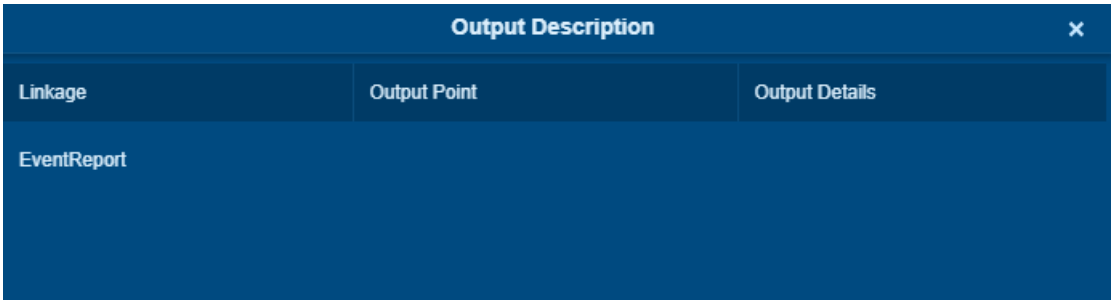
The regulation report displays the record of the terminal itself linking itself. And it displays event regulation name, time, trigger type, terminal name, trigger description and operation.



✍**Note:**

- According to the time frame and terminal name, user is able to search for the regulation name.

- System is support fuzzy search.
- Detail and output description can be previewed by user in the system.



18.3. Monitoring

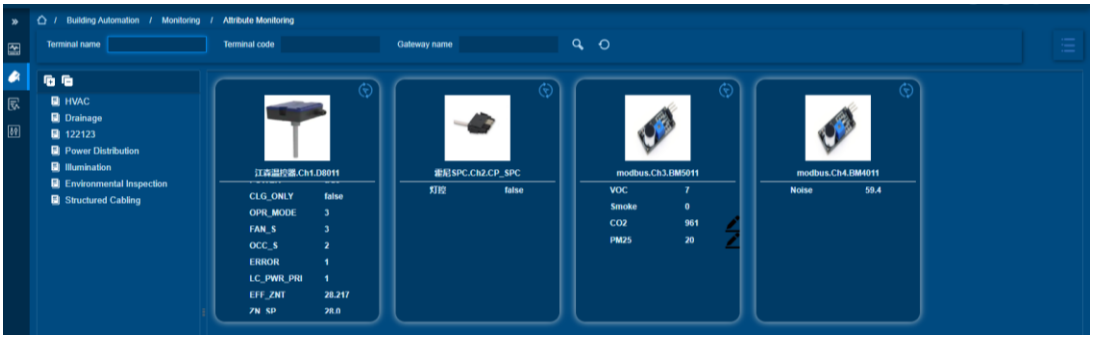
Function Description

It is convenience for administrator monitoring device attribute in real time.

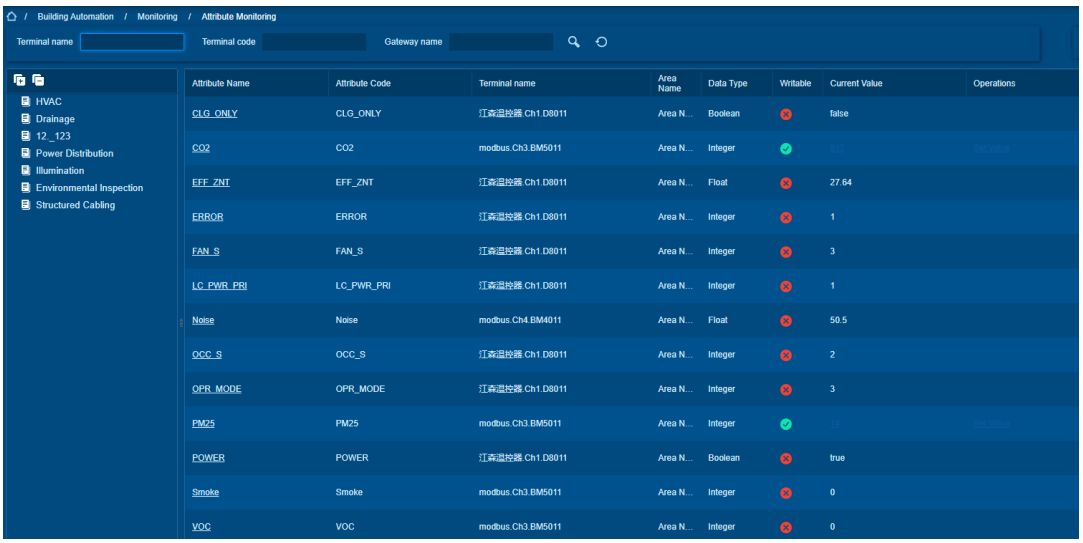
18.3.1. Attribute Monitoring

The interface is clearly display terminal real-time attribute monitoring. According to terminal or subsystem, user can preview real-time attribute monitoring.

1. According to terminal



2. According to subsystem



19. Intrusion Alarm

Intrusion Alarm are mainly applied to places where people cannot control in real time such as some dangerous places which need boundary control. For example, when someone or animal intruders are found in some restricted areas, corresponding alarms will be generated, essentially to ensure the safety of the area.

Key Words Description

Keywords	Description
Partition	A space, such as a front door, floor, or hallway, can assign multiple Points.
Point	It is the connection port between the front-end detector and the alarm control panel and is the smallest spatial unit that can distinguish alarm event
Bypass	Points that are Service Bypassed cannot produce Extra Point events
Unbypass	Points that are Service Bypassed can produce Extra Point events

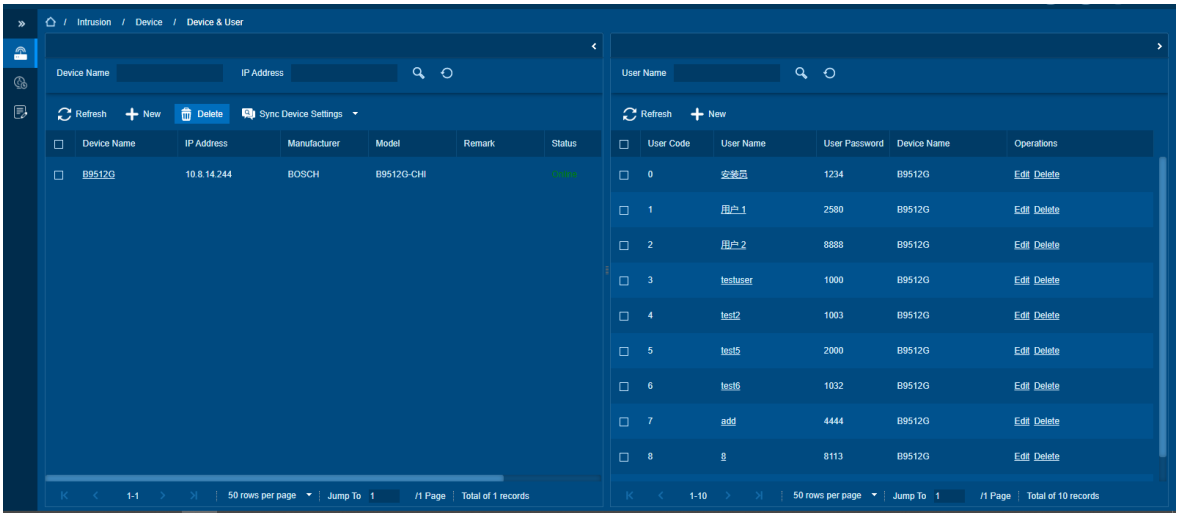
19.1. Device

Device includes Panel/ Partition/ Point/ Output and some of the alarm linkage of the intrusion alarm panels.

19.1.1. Device & User

The left part is device management, the right part is user management.

If you select a device on the left, the user list of the device will display on the right.



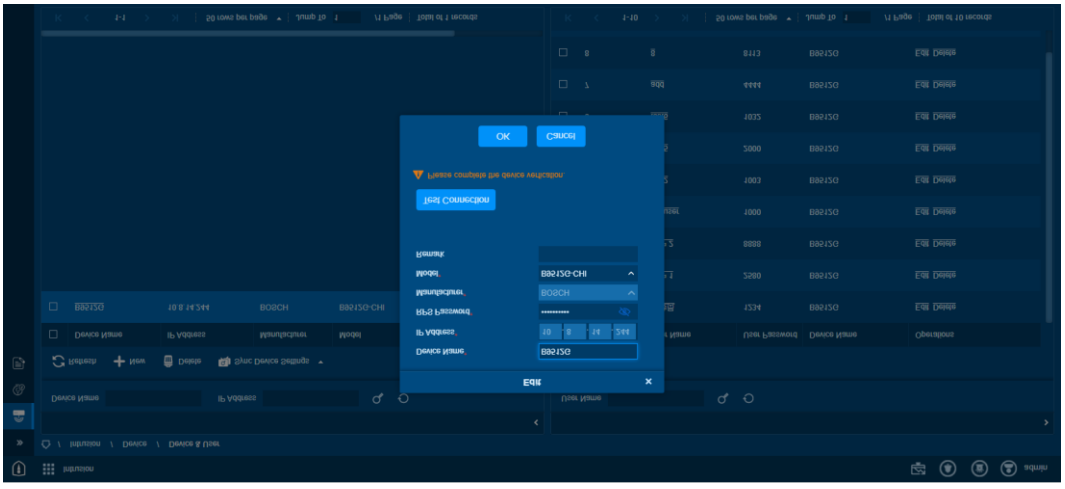
Add Device

- Click **[New]** button to add a new device.
- Fill in the following device information: Device Name, IP Address, RPS Password, Manufacturer, Model, Remark.

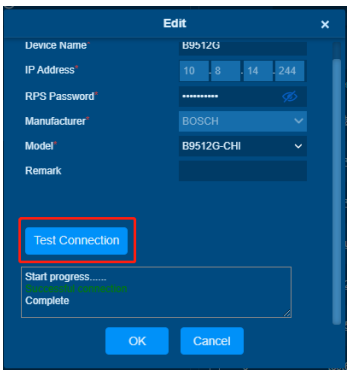
✍Note:

Currently only support Bosch B series and C series to connect intrusion alarm panels.

Series	Model
Bosch B Series	B6512/B5512/B4512/B3512
Bosch G Series	B9512G/B8512G

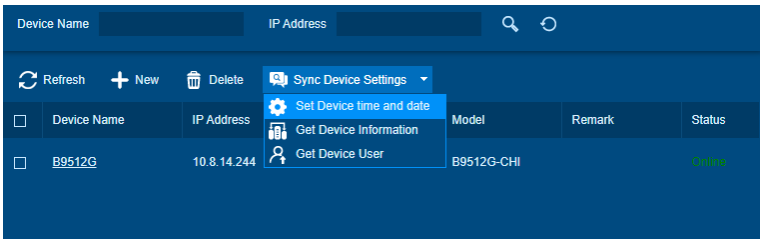


- Click **[Test Connection]** and try to connect the device.



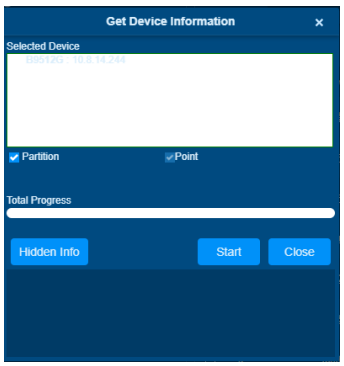
- Click **[OK]** button to complete operations.

Device operations

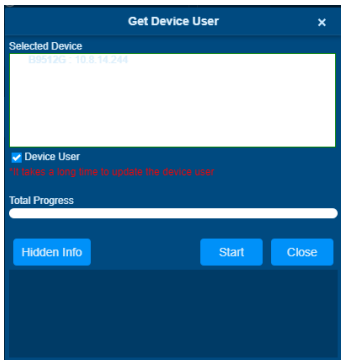


Set Device time and Date: Synchronize the device time, you can also select the Partition and the Point in the device.

Get Device Information: Get the Device information or get the Partition or Point.



Get Device User:



Add User

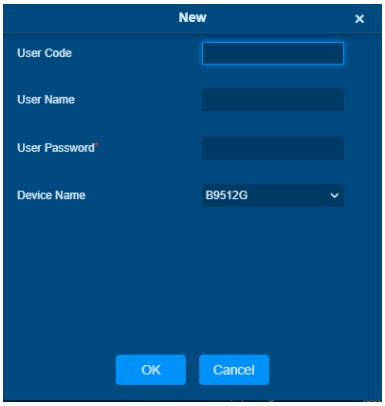
User is someone who has a password to input on keypad to enable some function or configure panels.

keypad

(The keypad can perform operations on the partitions and points)

If the device is normal, you can Add Users.

- Click **[New]** and fill in the following user information.



✍**Note:**

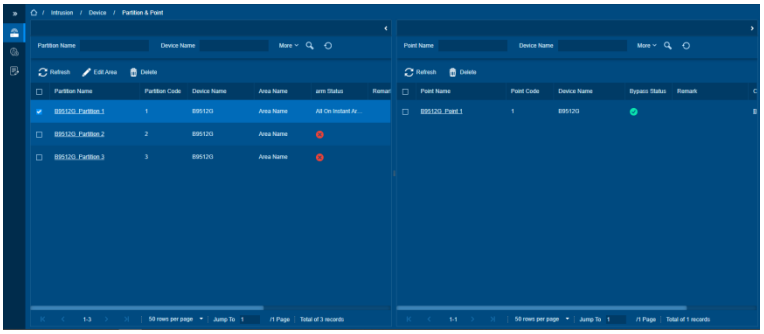
The user code and the username cannot duplicate

19.1.2. Partition & Point

A Partition can contain multiple points. A license can control the number of points. If the number of points exceeds the license limit, the license will alert you that the license is insufficient.

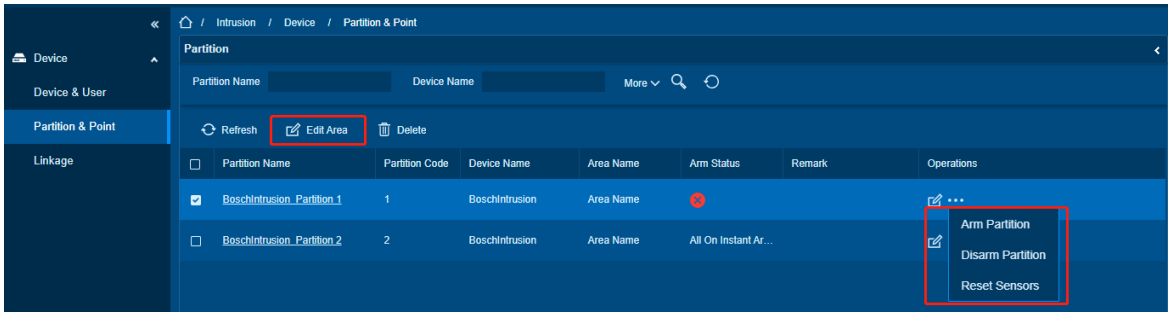
The left part is partition list, the right part is the corresponding point list.

The Partitions and Points obtained by the device display here. The Partition on the left and the Point corresponding to each Partition display on the right. A panel can correspond to multiple partitions.

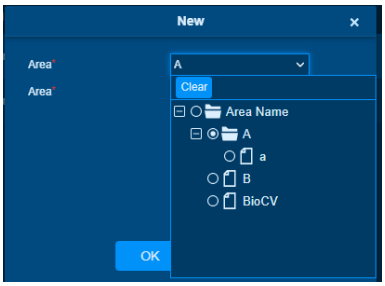


Partition

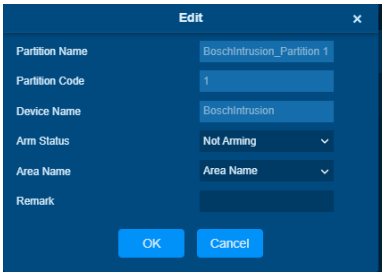
We can do a few operations to Partition, including **[Edit Area], [Edit], [Arm Partition], [Disarm Partition], [Reset Sensors],**



Edit Area: Click  to select the partition area.

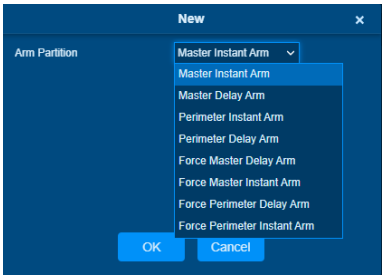


Edit: Click  to edit the device information, including changing the Arm Status, the Area Name and editing the remark.



Arm Partition: To set out the partition, when an event occurs, the panel generates an alarm, or a no alarm

based on the deployment.

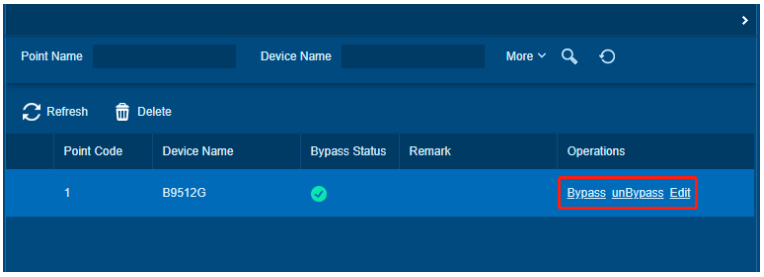


Disarm Partition: Disabled the arm partition setting.

Reset Sensors: In case of alarm or failure, the sensor must be reset to restore normal state.

Point

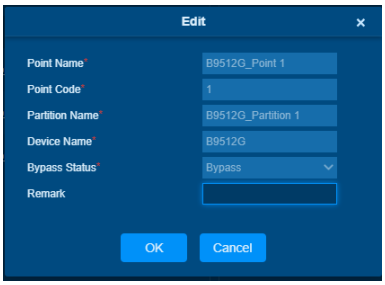
We can do a few operations to Point, including:



Bypass: Disable the Point within a defense cycle.

UnBypass: Cancel Bypass, the Point return to normal status.

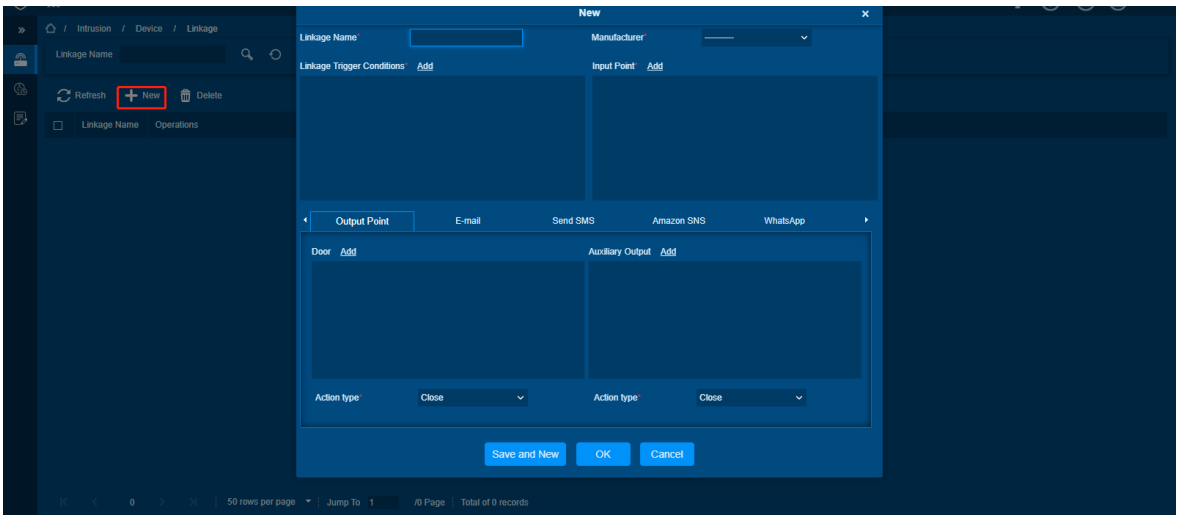
Edit: View some parameters of Point and edit the Remarks.



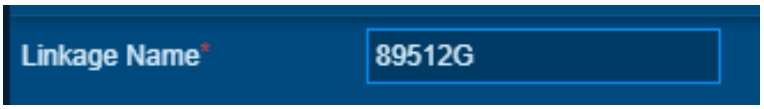
19.1.3. Linkage

Some intrusion events can be linked to other modules, currently can be linked to access control, and the message center.

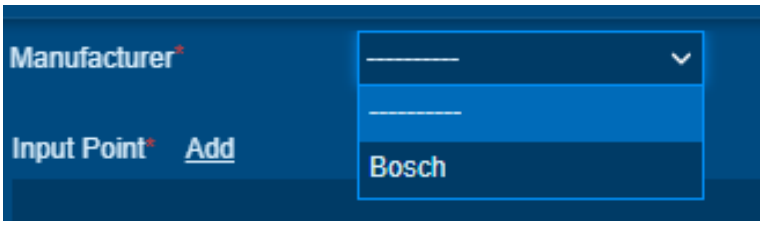
Click **[+New]** and fill in the following linkage information.



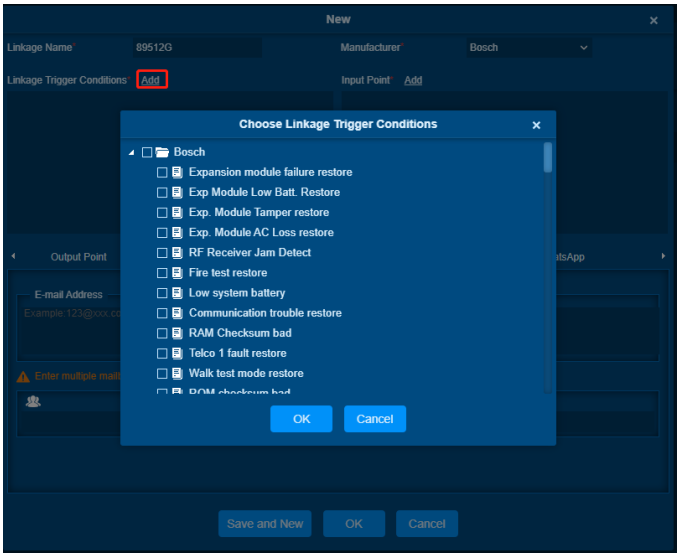
Linkage Name: Edit as required



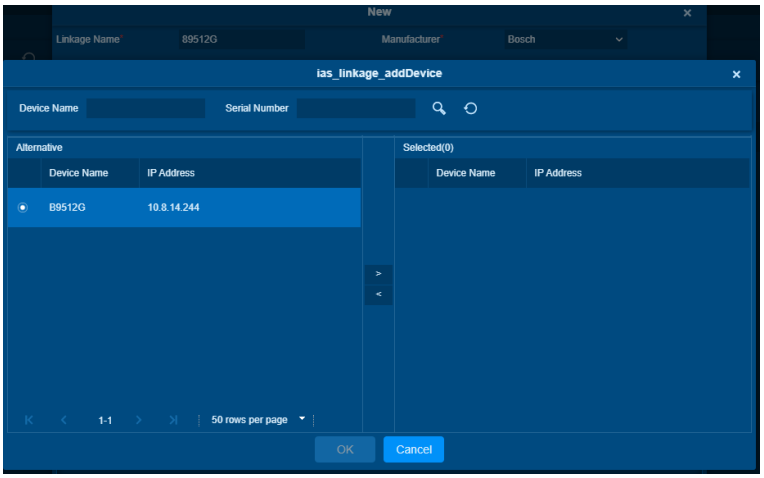
Manufacturer: Currently supported Bosch



Linkage Trigger Conditions: Click Add to select. Linkage occurs when the related events are generated.



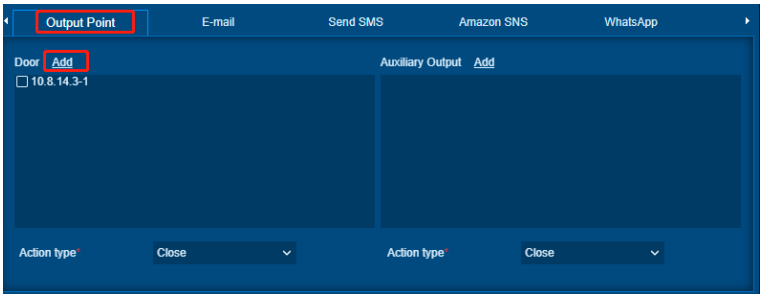
Input Point: Click Add to select and click > to confirm.



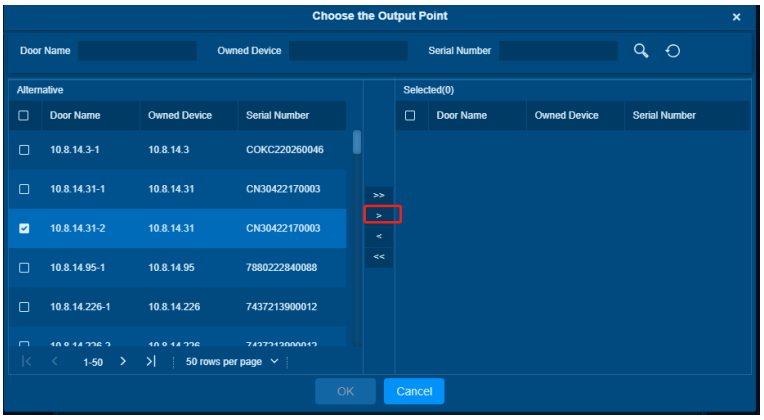
Output Point: It can add a Door or Auxiliary Output device for linkage.

Add a door

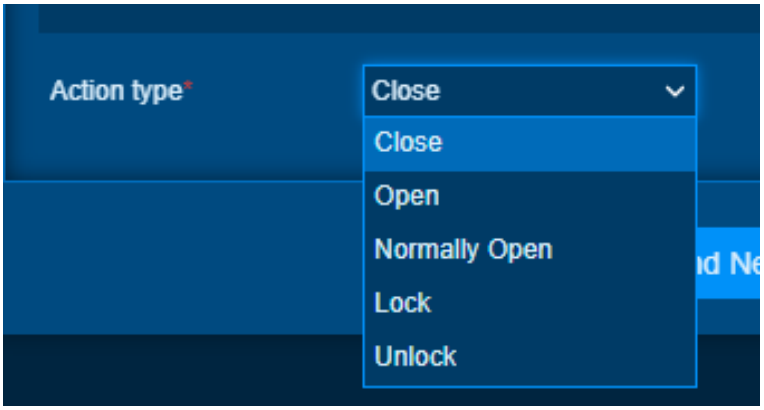
Step 1: Click [**Add**] to add a door device.



Step 2: Select a door device, and click > to add it, then click [**OK**]

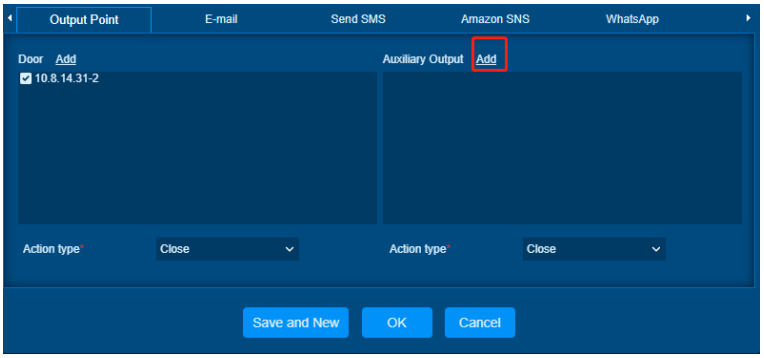


Step 3: Set the door Action type, you can choose **[Close]**, **[Open]**, **[Normally Open]**, **[Locked]**, or **[Unlocked]**.

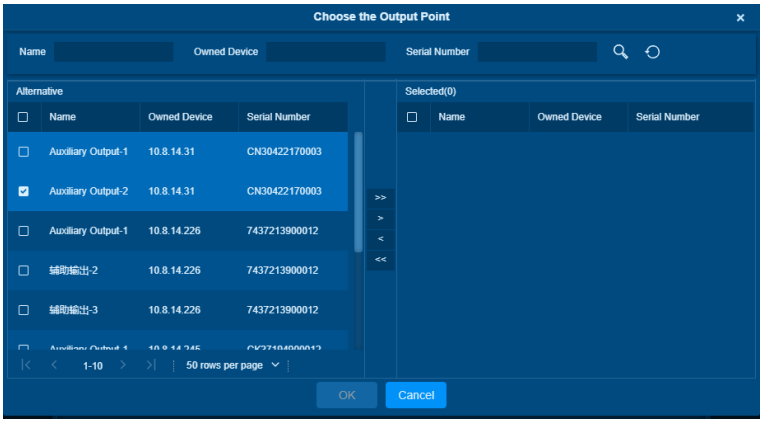


Add an Auxiliary Output

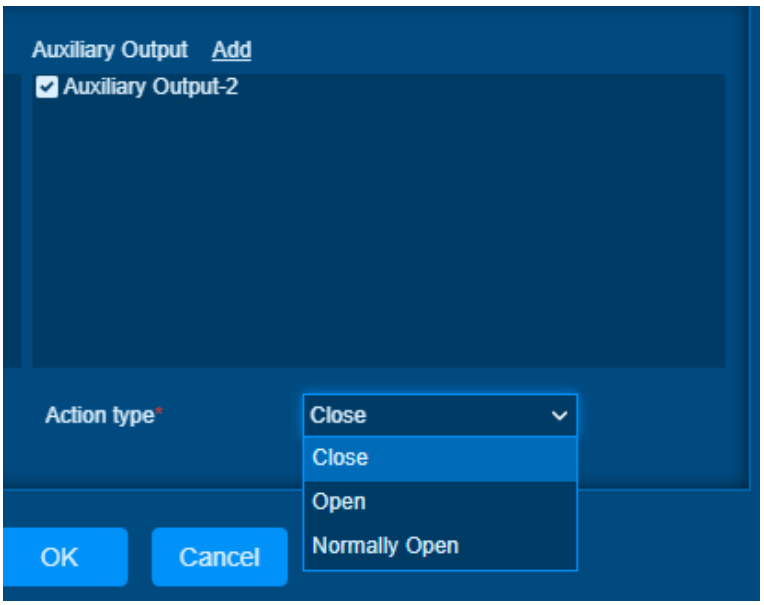
Step 1: Click [**Add**] to add an Auxiliary Output



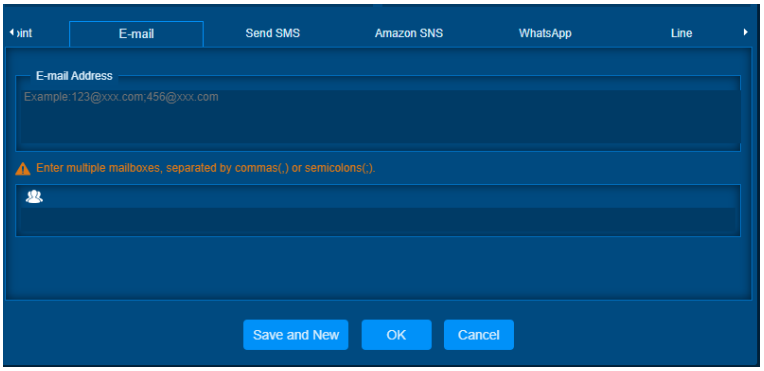
Step 2: Select a door Auxiliary Output device, and click > to add it, then click [**OK**]



Step 3: Set the Auxiliary Output Action type, you can choose **[Close]**, **[Open]**, **[Normally Open]**, **[Locked]**, or **[Unlocked]**.



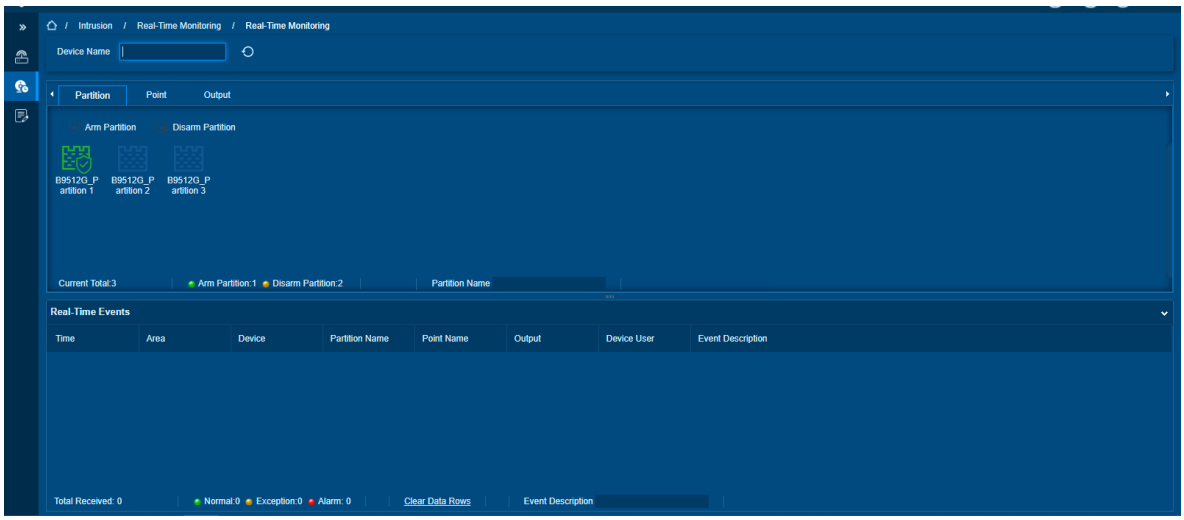
Email, Send SMS, Amazon SNS, WhatsApp, Line: It can also link with the message center, when an alarm is generated, a notification is sent through the linked communication mode.



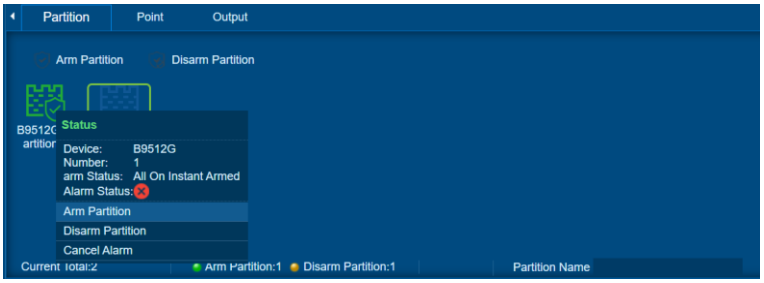
19.2. Real-Time Monitoring

Real-time monitoring Monitors alarm events and events generated by alarm devices in real time.

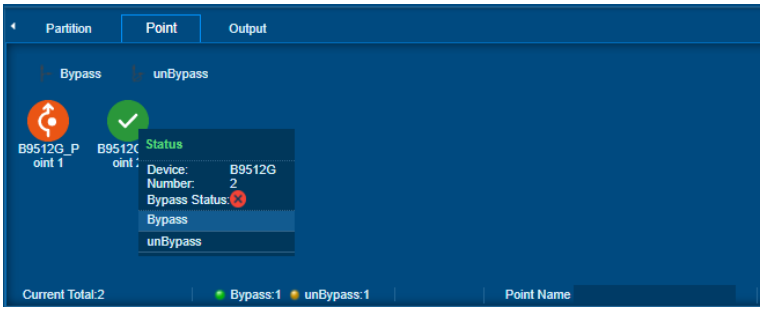
It can display the status of each partition (such as alarm/no alarm) and quickly set out the Partition, Point, Output.



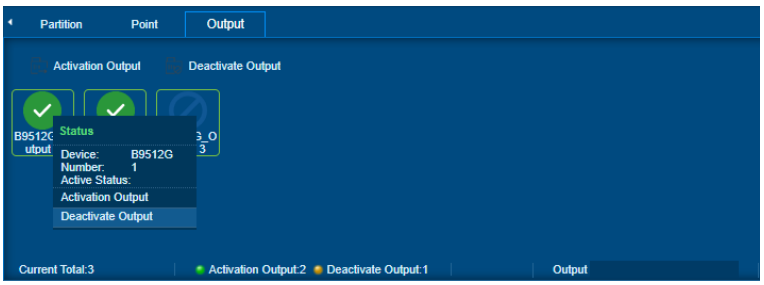
Partition: We can view the device status by placing the mouse cursor on the device. The green indicates the device is All on Instant Armed, and the Gray indicates the device is not armed. We can also select the partition and operate it quickly, such as Arm Partition, Disarm Partition, Cancel Alarm.



Point: We can view the Point status. The green indicates the Point is on Bypass, the yellow indicates the Point is on UnBypass. We can also click on the point and operate it quickly, such as Bypass, Unbypass.



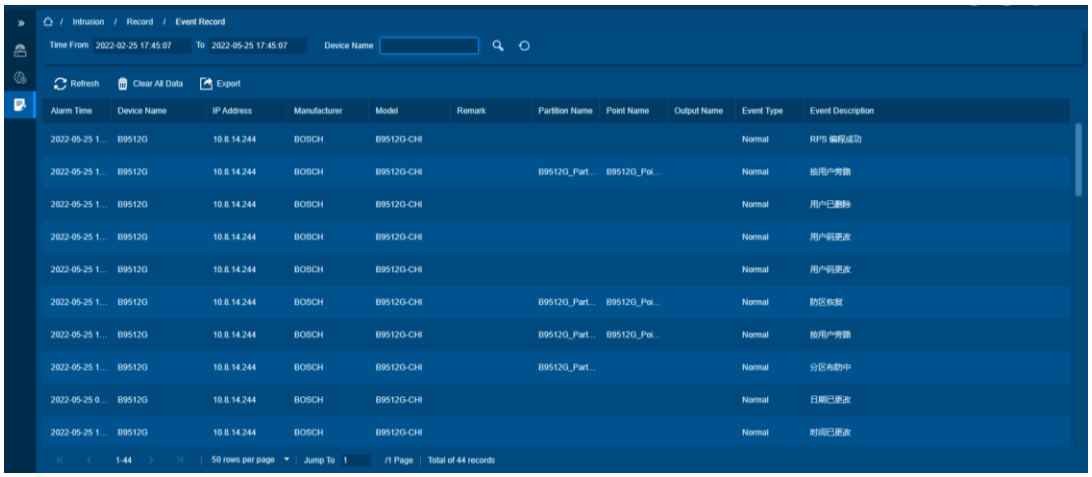
Output: We can view the state of Alarm Panel Outputs. We can also click on the point and operate it quickly, such as Activate Output and Deactivate Output.



19.3. Record

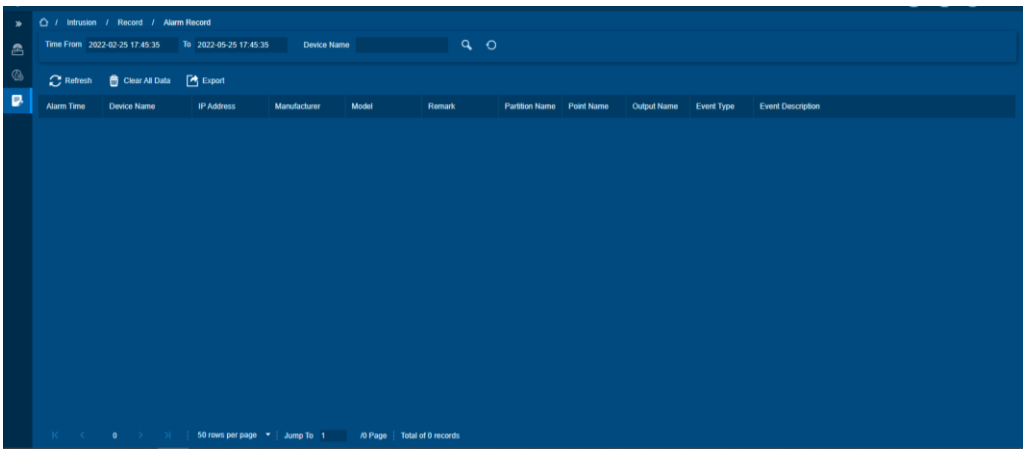
19.3.1. Event Record

It contains all of the event records, not just the alarm records, but also some of the action logs, like Reset Sensor.



19.3.2. Alarm Record

It contains all of the alarm records.



20. Data Monitor

It contains data analysis center for each module, including statistics of basic type of reports, data analysis of reports, etc. Through the statistical charts, the situation of each event can be visualized, and the contents of the charts can be further analyzed.

20.1. Data Chart

Function List

Functions	Description
Data Chart	View, export, download, and close chart-related data for access control, visitor, office, personnel, video, and system modules

20.1.1. Base Chart

Function Description

You can view the chart data of access control, visitor, office, personnel, video, system modules, graphically display the data in the form of charts, by clicking on the event list on the left or right, the chart of the corresponding event will be displayed, and can export and download, close the data of each chart.

Access Chart

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]** on the Action Menu, the following interface will be shown:

Overview: The charts in the overview are the more important and generalized data charts for the entire access control module and include the following charts:

1. Device type statistics: statistics on the various device types added to the access control module.

2. Regional equipment statistics: statistics on the type of equipment between regions.

3. Usage module statistics: statistics on the devices added to the access control module are used in other modules.

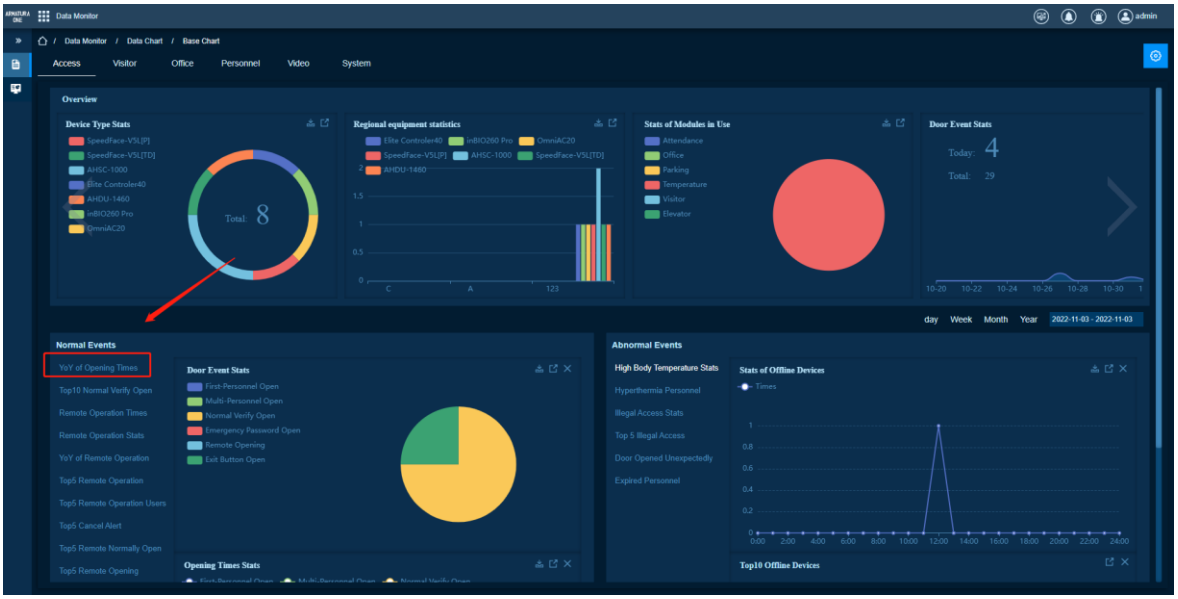
4. Door open event statistics: statistics on the last 15 days of open doors.

5. Remote operation statistics: statistics of the last 15 days of remote operations.

Normal Events: Normal events can be selected by the time control for day, week, month, year, or the normal access control event data graph for the corresponding Timetable.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]** > **[YoY of Opening Times]** on the Action Menu, the chart will be displayed at the top of the normal class of events, before the chart is moved down, the rest of the chart function is the same, as shown in the figure:



1. Door opening event statistics: the proportion of each door opening event in the Timetable, including normal verification to open the door, the first person to open the door, multiple people to open the door, the door button to open the door, the emergency password to open the door, remote door opening.

2. Door opening statistics: statistics on the number of individual doors opening events during the Timetable.

3. The number of openings: statistics of this Timetable and the previous Timetable, the number of openings compared.

4. Top5 door open device: statistics of the current Timetable open the door number of the top five equipment information.

5. Top5 for low-frequency door opening statistics of the current Timetable to open the door ranked in the top five devices information.

6. Normal verification of door opening statistics on the frequency of normal verification of door opening in the current Timetable.

7. Normal verification of open door top10: statistics of the current Timetable of the normal verification of the top 10 devices open door information.

8. Number of remote operations: Statistics on the total number of remote operations in the current Timetable, including remote open, remote close, remote lock, remote open, remote unlock.

9. Remote operation statistics: statistics on the percentage of remote operations in the current Timetable.

10. Remote Operation Comparison: Statistics on the number of remote operations in the current Timetable compared to the number of remote operations in the previous Timetable.

11. Remote operation top5: Statistics on the top five devices for remote operation in the current Timetable.

12. Remote operation user top5: statistics of the top five remote operation system users in the current Timetable.

13. Top5 cancelled alarms: Statistics on the top five devices with the highest number of cancelled alarms in the current Timetable.

14. Top5 remote Normally open: statistics of the top five remote Normally open devices in the current Timetable.

15. Top5 remote door opening statistics of the current Timetable, the number of remote doors opening the top five devices information.

16. Regional equipment alarms & handling statistics: statistics on the number of equipment alarms in the current Timetable and the number of alarms handled by system personnel.

17. Top10 permission group configuration: statistics of the greatest number of permission groups configured in the current Timetable device information.

18. Unauthorized devices: Statistics on devices that are not configured with permission groups in the current Timetable.

Abnormal Events: The abnormal events can be selected by the time control for the day, week, month, year, or the abnormal access control event data graph for the corresponding Timetable, including the following.

1. Offline statistics: count the total number of times the device is offline during the current Timetable.

2. Top10 offline: statistics of the top ten offline devices in the current Timetable, the most offline times can be recommended for maintenance or regular maintenance and other processing.

3. Excessive temperature statistics: statistics of excessive temperature in the current Timetable.

4. Overheated persons: statistics on persons with high body temperature in the current Timetable.

5. Illegal access statistics: statistics of illegal access within the current Timetable.

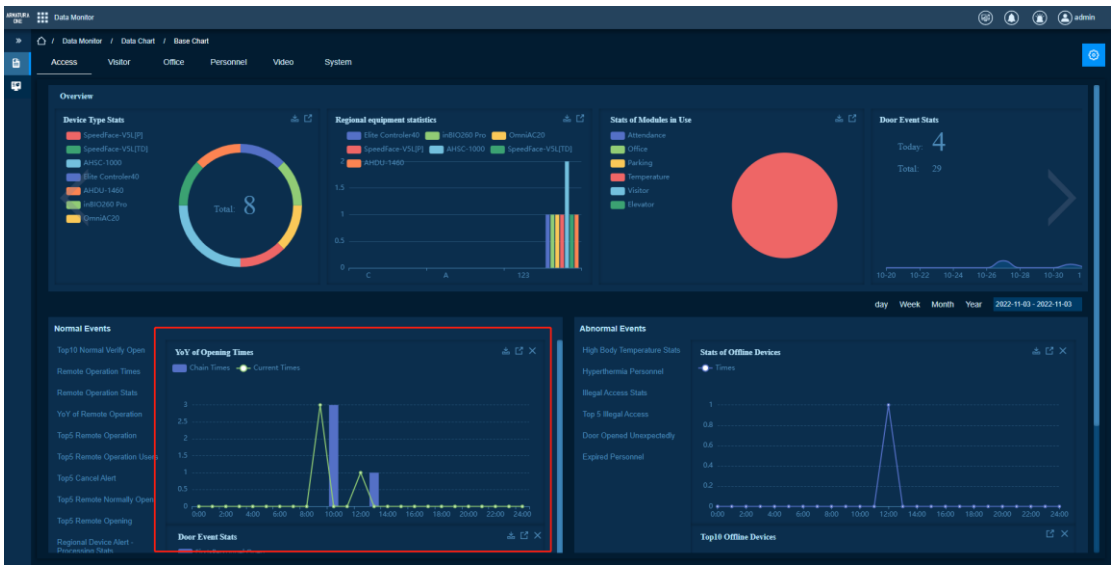
6. Top5 illegal access: statistics of the current Timetable illegal access to the top five people information situation.

7. Door accidentally opened: statistics on the number of accidental openings of the device during the current Timetable.

8. Expired personnel: statistics of the current Timetable has passed the expiration date of the personnel information, convenient for the administrator to deal with.

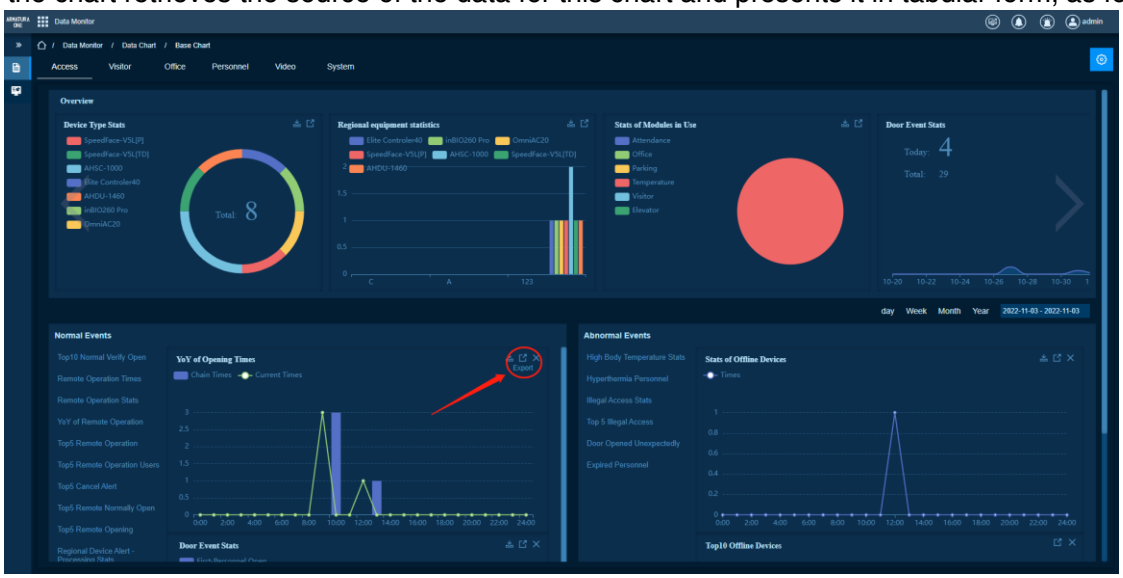
Close Chart

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]** > **[YoY of Opening Times],** the following interface will be shown:



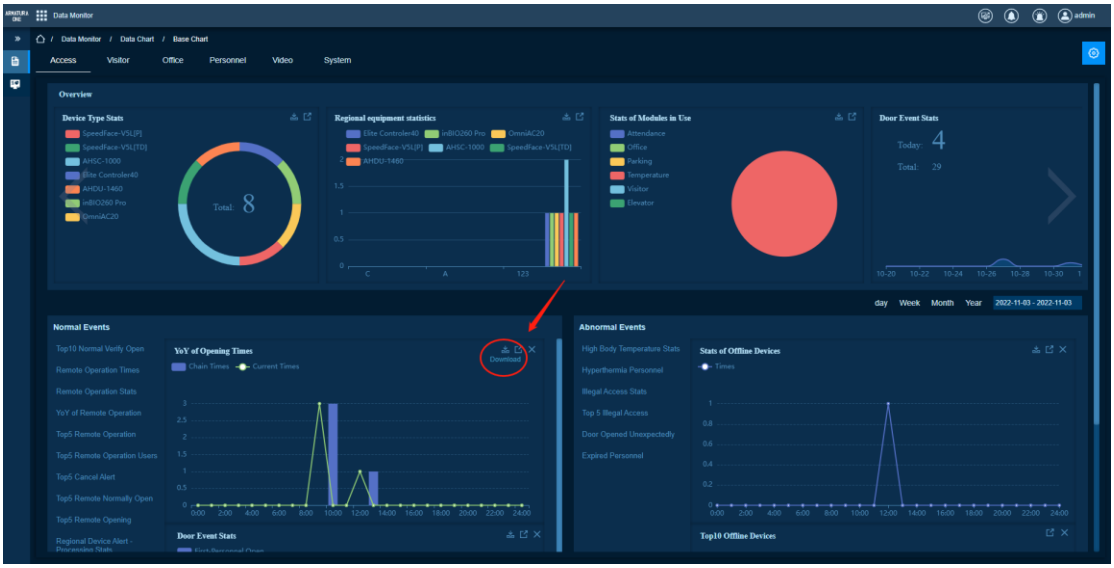
Export

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Access]** > **[YoY of Opening Times]** The Export button in the chart retrieves the source of the data for this chart and presents it in tabular form, as follows.



Download

- Click **[Data Monitor]** > **[Data Chart]** > **[Access]** > **[YoY of Opening Times]** the download button in the chart will allow this chart to be downloaded in PNG format, as shown in the figure.



Visitor Chart

Preconditions for Normal Use of Function

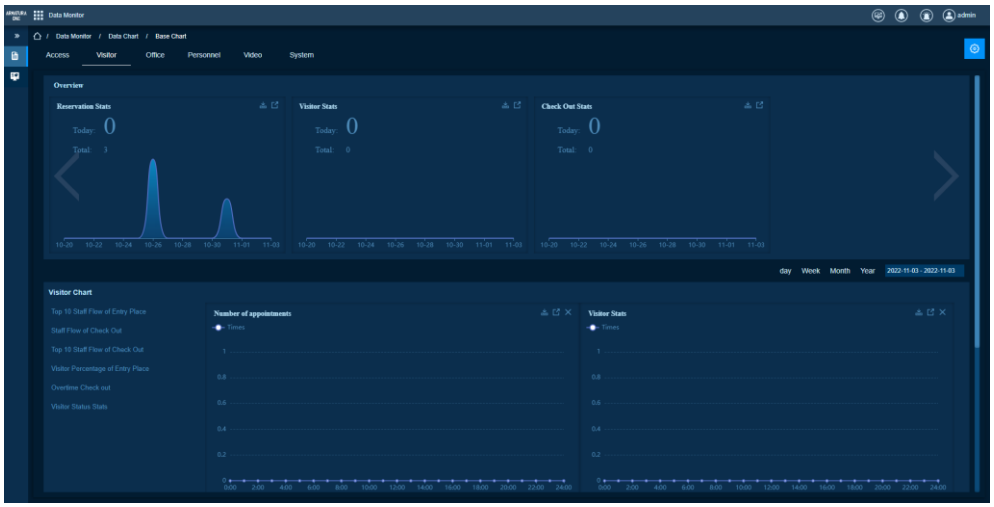
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Visitor]** on the Action Menu, the following interface will be shown:



Overview: The charts in the overview are the more important and generalized data charts for the entire visitor module, including the following charts.

1. Reservation statistics: statistics on the number of reservations within the last 15 days and today.

2. Visitor statistics: statistics on the number of visitors in the last 15 days and today.

3. Sign-Out Statistics: Statistics on the number of sign-outs in the last 15 days and today.

Visitor Chart: Visitor charts can be selected via time controls for daily, weekly, monthly, yearly, or corresponding Timetable visitor event data charts, including the following:

1. Number of appointments: Statistics on the number of appointments made by visitors during the Timetable.

2. **Visitor statistics:** statistics on the number of visitors during the Timetable.

3. Top 10 Host: information on the top 10 Host in the statistical Timetable.

4. Registration location traffic: statistics on the number of registrants at the registration location during the Timetable.

5. Top 10 registered locations in terms of visitor traffic: information on the top 10 registered locations in terms of number of visitors during the statistical Timetable.

6. Sign-out location traffic: statistics on the number of people signing out during the Timetable.

7. Top 10 sign-out locations in terms of traffic flow: the top 10 sign-out locations in terms of number of sign-outs during the Timetable.

8. Sign out timeout personnel: statistics of the system sign out timeout personnel information within the Timetable.

9. Visitor status statistics: statistics on the number of registered persons, signed-out persons and remaining unsigned-out persons during the Timetable.

Office Chart

Preconditions for Normal Use of Function

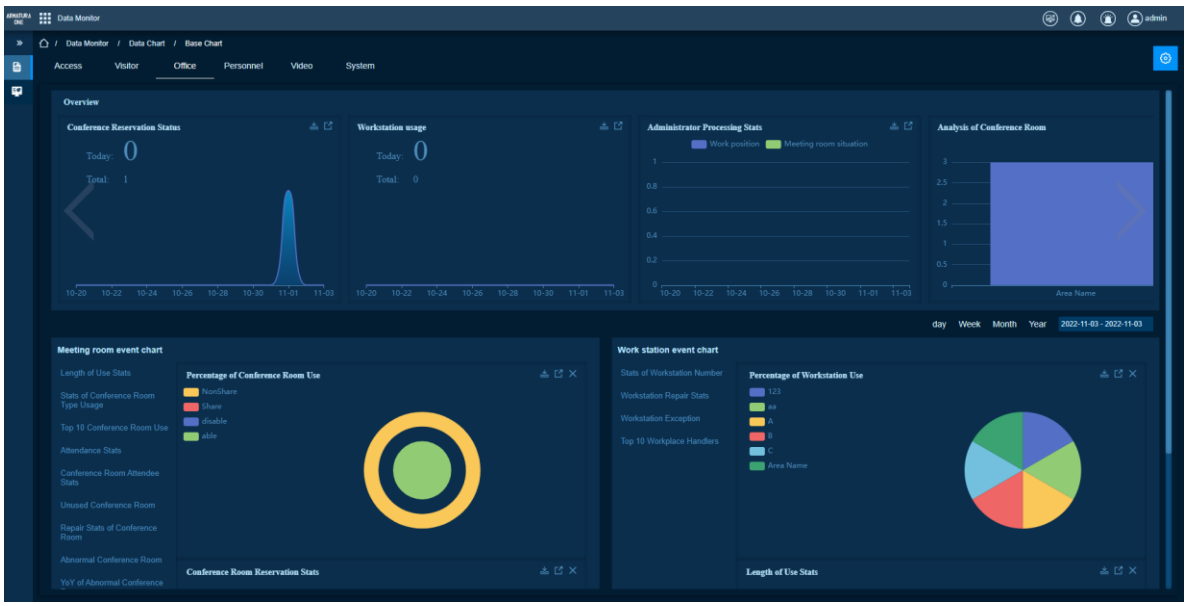
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Office]** on the Action Menu, the following interface will be shown:



Overview: The charts in the overview are important and general data charts for the entire office module, including the following charts：

1. Meeting reservation situation: Count the number of meeting rooms reserved in the last 15 days and today.

2. Station usage: statistics the usage of stations in the last 15 days and today, and the usage is counted once from the beginning of occupation.

3. Manager processing statistics: statistics on the comparison between the processing of repair reports in the conference room and the processing of repair reports by the station area administrators.

4. Conference room statistics: count the number of regional conferences rooms.

5. Station statistics: count the number of regional stations.

Meeting room event Chart: The meeting room event chart can be used to select the day, week, month, year, or the meeting room event data chart in the corresponding Timetable through the time control, including the following content:

1. Proportion of meeting room usage: count the number of available/unavailable meeting rooms, and the number of shared/non-shared meeting rooms.

2. Conference room reservation statistics: count the number of reservations of each conference room within the Timetable.

3. Usage time statistics: the usage time of each meeting room in the Timetable (the day is not counted, the usage starts from the beginning of the week, and the usage starts from the occupation).

4. Conference room type usage statistics: statistics on the usage time of shared/non-shared conference rooms during the statistical Timetable (not counting days, starting on a weekly basis).

5. Top 10 meeting room usage: list of the top ten meeting rooms used in the statistical Timetable.

6. Participants statistics: the number of participants during the statistical Timetable (participants plus reservations).

7. Conference room participant statistics: the number of participants in the conference room during the statistical Timetable.

8. Unused meeting rooms: list information of unused meeting rooms during the statistical Timetable.

9. Conference room repair report statistics: the number of meeting room repair reports during the statistical Timetable.

10. Timetable repair report statistics: statistics of the repair report status of each conference room during the Timetable.

11. Abnormal meeting rooms: information about meeting rooms that are in repair or maintenance within the statistical Timetable.

12. Abnormal meeting rooms: the total number of repairs reported for meeting rooms during the statistical Timetable and the ring ratio of the total number of repairs to the previous time;;

13. Top10 repair request handlers: the top ten administrators who processed the meeting room repair requests during the statistical Timetable.

Workstation event Chart: The station event chart can be used to select the day, week, month, year, or the station event data chart in the corresponding Timetable through the time control, including the following content:

1. Proportion of station usage: the number of station usage in each area during the statistical Timetable (counted once from the start of activation).

2. Usage time statistics: statistics on the usage time of stations in the Timetable (calculated once from the beginning of occupation).

3. Usage time statistics: statistics on the usage time of stations in the Timetable (calculated once from the beginning of occupation).

4. Station repair statistics: count the number of station repair requests during the statistical Timetable.

5. Abnormal workstations: information about workstations that are in repair or maintenance within the statistical Timetable.

6. Top 10 of the workstation repair application handlers: information about the top ten administrators in the number of processing times after the workstation repair application within the statistical Timetable.

Personnel Chart

Preconditions for Normal Use of Function

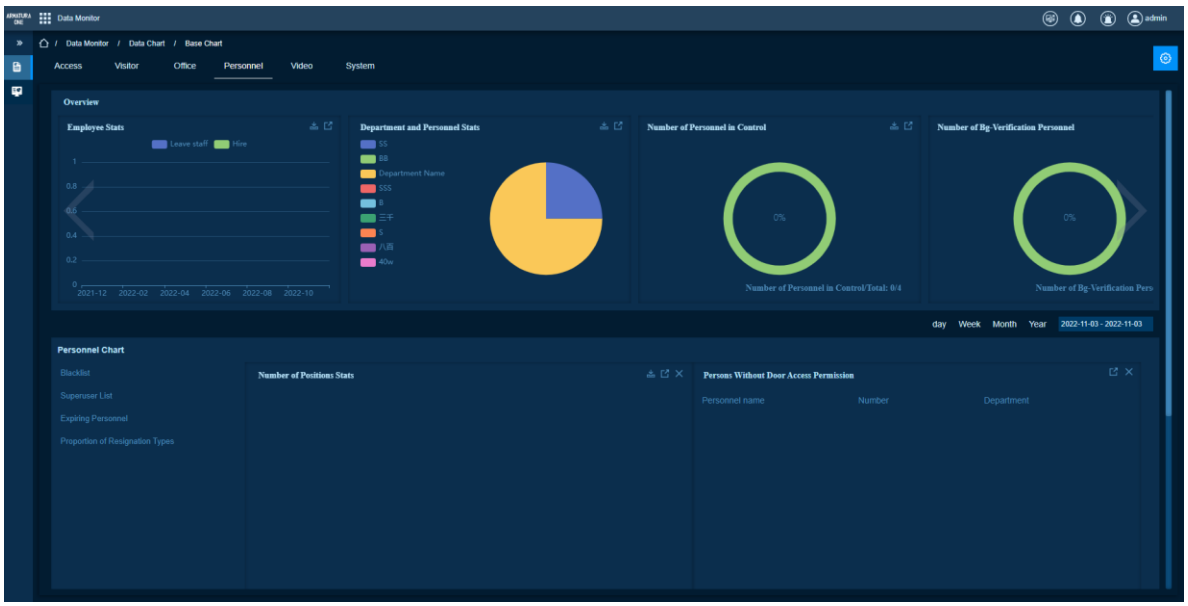
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Personnel]** on the Action Menu, the following interface will be shown:



Overview: The charts in the overview are important and general data charts for the entire personnel module, including the following charts:

1. Statistics of recruited and resigned personnel: Statistics on the number of recruits and resigned within the last month.

2. Department and population statistics: statistics on the proportion of people in each department.

3. Number of deployed controls: the number of deployed controls accounted for the total number of people.

4. Number of background verifiers: Statistics support the number of background verifiers in the total number of people.

5. Proportion of men and women by age group: Statistics on the proportion of men and women by age group.

6. Employee's working age ratio: the ratio of men to women of different working ages.

Personnel Chart: Personnel event chart can be selected through the time control day, week, month, year, or the personnel event data chart in the corresponding Timetable, including the following content:

1. Number of positions statistics: statistics of the number of people in each position within the Timetable.

2. Persons without a card: information of persons without an authorized card number during the statistical Timetable.

3. Persons without photos: information of persons without face avatars in the statistical Timetable.

4. Banned persons: information of persons on the banned list during the statistical Timetable.

5. Super user list: Super user personnel information during the statistical Timetable.

6. Persons who are about to expire: the list of personnel who are about to expire (within five days) within the statistical Timetable, sorted down in order of the most recent expiration time.

7. Proportion of resignation types: the proportion of the number of resignation types in the statistical period, including resignation, dismissal, transfer, and self-resignation.

8. Persons without access control authority: information of persons without access control authority within the statistical Timetable.

Video Chart

Preconditions for Normal Use of Function

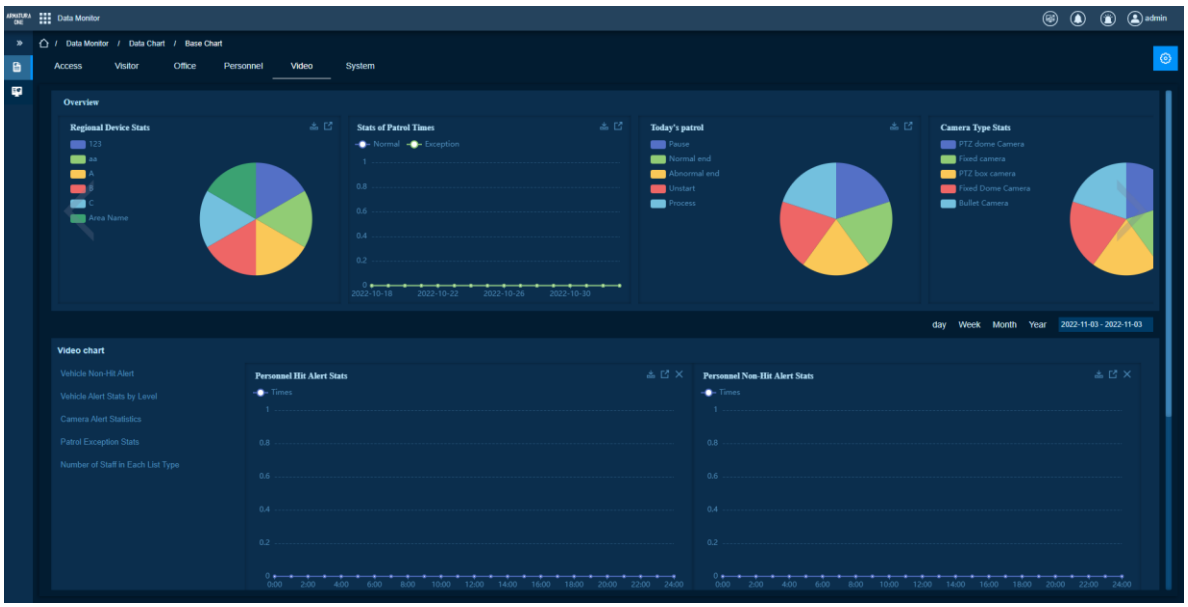
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Monitor]** > **[Data Chart]** > **[Base Chart]** > **[Video]** on the Action Menu, the following interface will be shown:



Overview: The charts in the overview are important and general data charts for the data of the entire video module, including the following charts:

1. Regional equipment statistics: count the amount of equipment in each area.

2. Statistics of the number of patrols: count the number of video patrols within 15 days (not including today).

3. Today's patrol situation: statistics on today's patrol status, including not started, in progress, suspended, normal end, abnormal end.

4. Camera type: count the number of each camera type.

5. Personnel and vehicle alarm statistics: count the number of personnel hit/non-hit and vehicle hit/non-hit alarms.

Video Chart: The video event chart can be used to select the day, week, month, year, or the video event data chart in the corresponding Timetable through the time control, including the following content:

1. Personnel hit alarm statistics: the number of personnel hit alarms in the statistical Timetable.

2. Personnel non-hit alarm statistics: the number of personnel non-hit alarms in the statistical Timetable.

3. Alarm statistics for personnel of various levels: the number of alarms of each alarm level during the statistical Timetable.

4. Vehicle hit alarm: the number of vehicles hit alarms in the statistical Timetable.

5. Vehicle non-hit alarm: the number of vehicle non-hit alarms in the statistical Timetable.

6. Vehicle alarm statistics of each level: statistics of the number of vehicle alarms of each alarm level within the Timetable.

7. Camera alarm statistics: statistics of the number of times of each alarm type in the statistical Timetable.

8. Statistics of abnormal patrols: the number of times of no patrol, patrol alarm, and patrol not clocked in during the statistical Timetable.

9. Times of each type of list: the number of people of each type of list during the statistical Timetable (banned list, allowed list, red list).

System Chart

Preconditions for Normal Use of Function

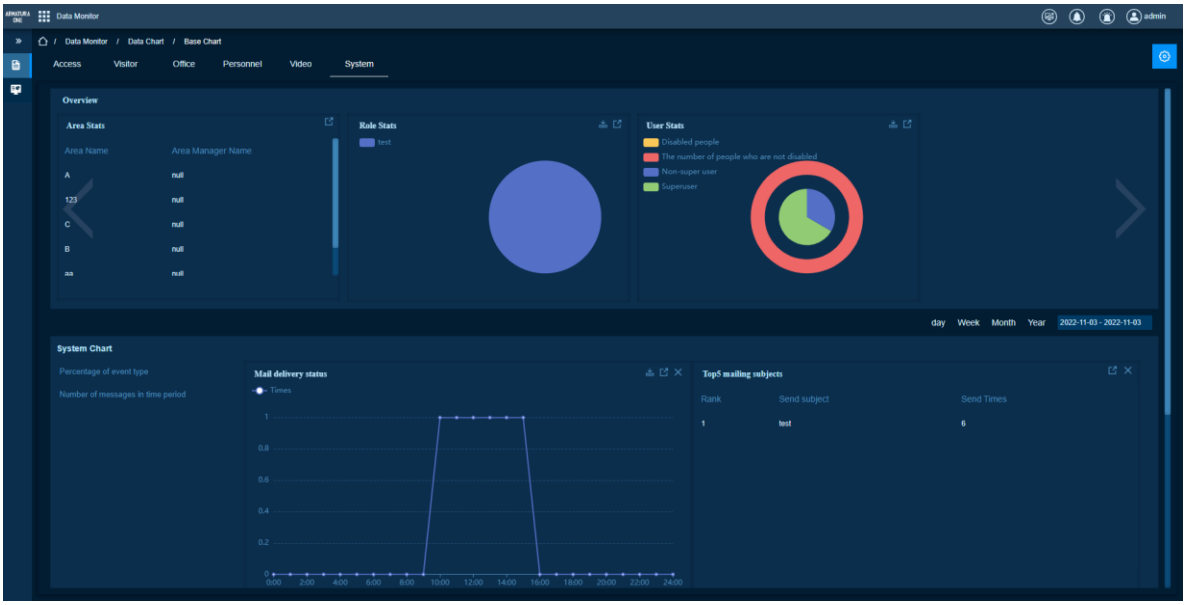
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

Administrators or users, need to view the overall data situation of the corresponding module.

Steps:

- Click **[Data Center]** > **[Data Chart]** > **[Base Chart]** > **[System]** on the Action Menu, the following interface will be shown:



Overview: The charts in the overview are important and general data charts for the data of the entire system module, including the following charts:

1. Regional statistics: statistics of all the regions of the system module and the corresponding regional administrators.

2. System role: Count the types of system roles and the number of corresponding personnel.

3. System user statistics: statistics on the number of disabled/non-disabled, super users/non-super users.

System Chart: The system event chart can select the day, week, month, year, or the system event data chart in the corresponding Timetable through the time control, including the following content:

1. Mail delivery status: count the number of mails sent during the Timetable.

2. Top 5 email subject: Top five email subject information in the statistical Timetable.

3. Proportion of platform types used: the number of platforms used during the statistical Timetable.

4. Message status: the number of each message status corresponding to the statistical Timetable.

5. Proportion of event types: Statistics of the event types of each module in the Timetable, click on a different module to display the event type of the corresponding module.

6. Number of messages in Timetable: the number of system messages of each module in the statistical Timetable.

20.2. Function Chart

Function List

Functions	Description
Alarm Management	Display system alarm information in real time in the form of charts

20.2.1. Alarm Management

Function Description

View a variety of alarms and alarm details including access control alarms, face alert alarm, vehicle alert alarm, intrusion detection, tripwire detection, loitering detection, area entry detection, area exit detection, and fast movement detection, and perform alarm processing operations.

Overview

Preconditions for Normal Use of Function

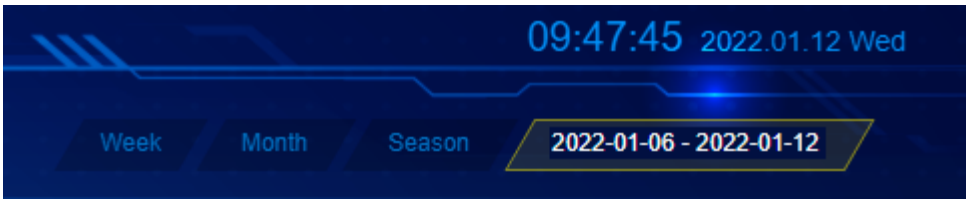
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View all types of alarms in real time.

Time Range

Select a different display time period to set different time range in every chart.



Could be set time period by Week, Month, Season or user defined.

Alarm Trend

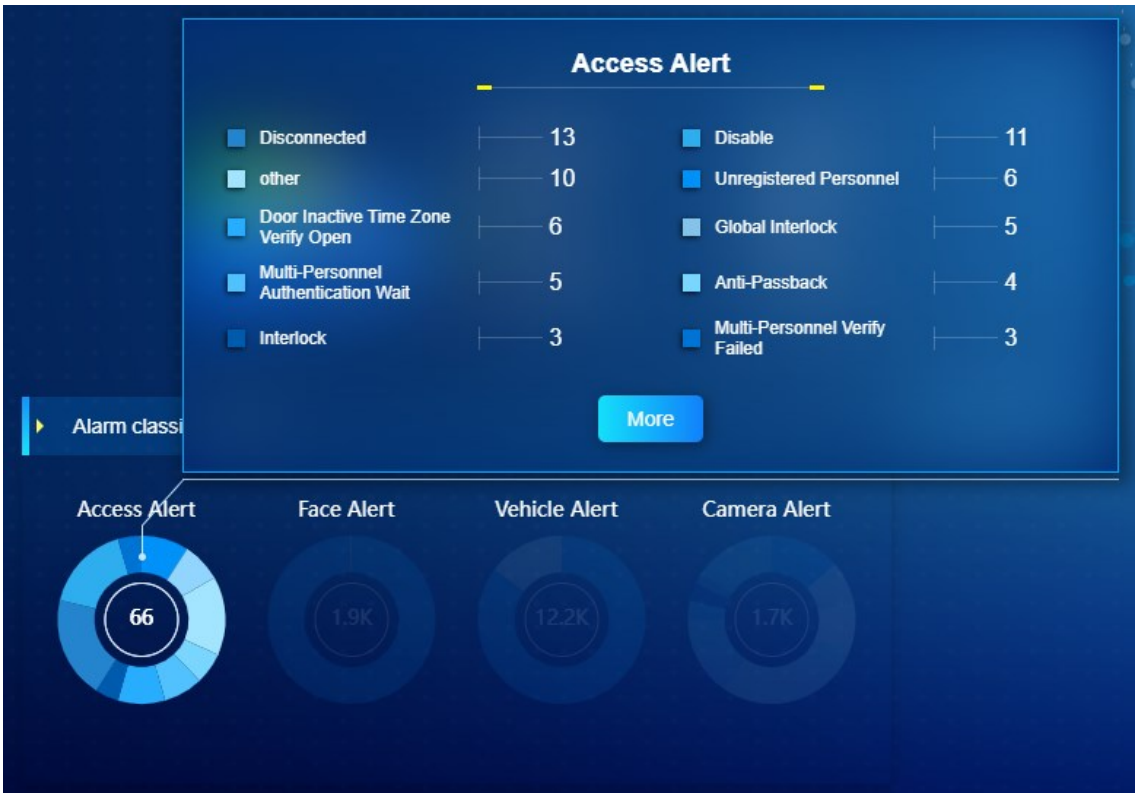
View the trend graph of alarms by different levels over time range.

Alarm Type Statistics

Shows the number and percentage of different types of alarms compared

Alarm Classification Statistics

Displays the number of different types of alarms, move in to see the components of each alarm trigger event and their number.

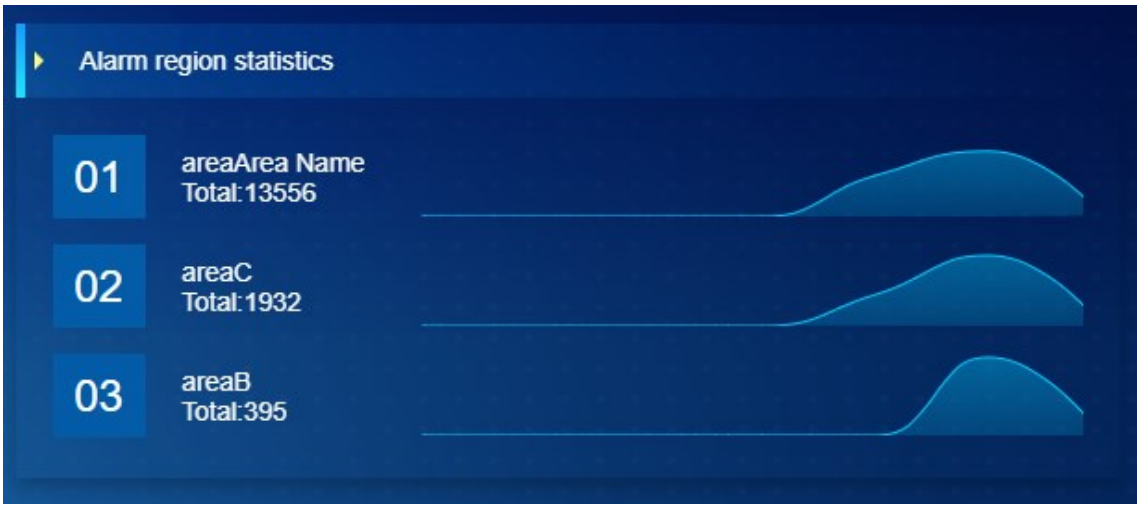


Total Alarm

Displays the total number of alerts generated, pending, and processed.

Alarm Region Statistics

View the distribution of the number of alarms in each area of the system.

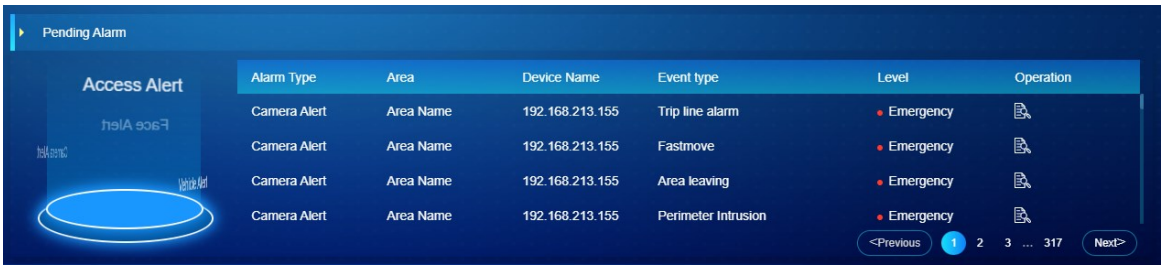


Alarm Rank Statistics

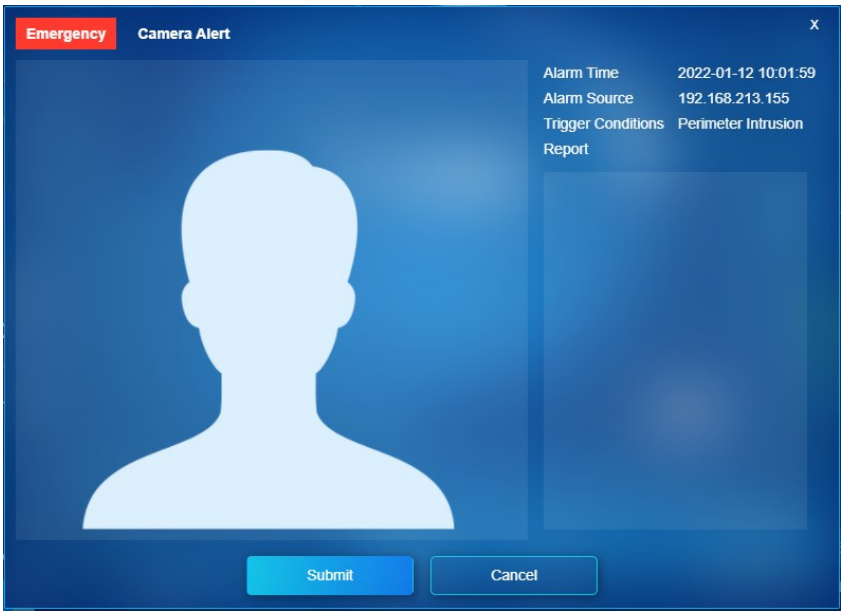
Displays the number of alarms of different levels.

Pending Alarms

View pending alarms and alarm details.



Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



Access Alert

Preconditions for Normal Use of Function

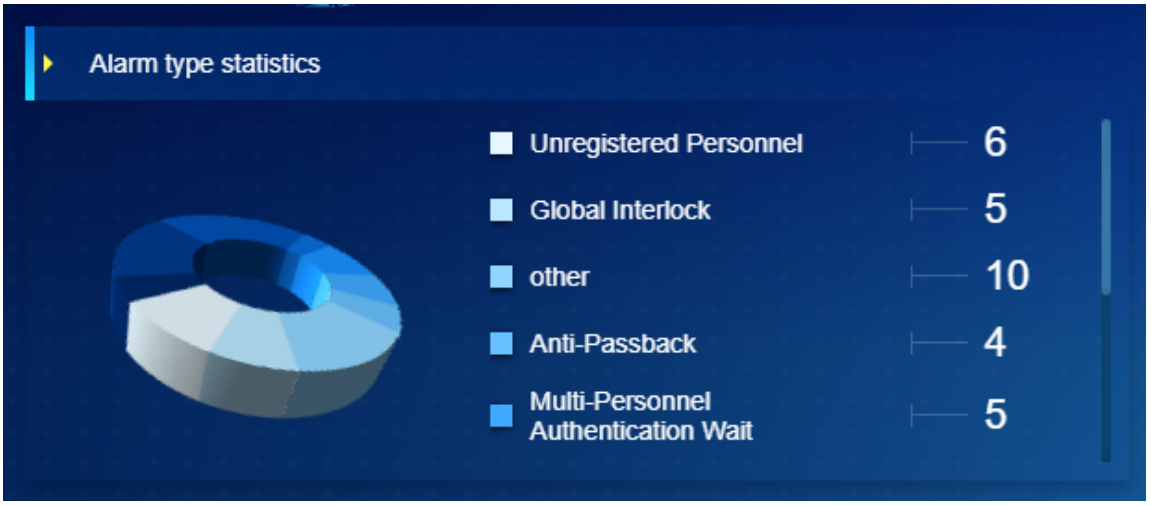
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View Access alarms in real time.

Alarm Type Statistics

View the composition and quantity of access alarm types.

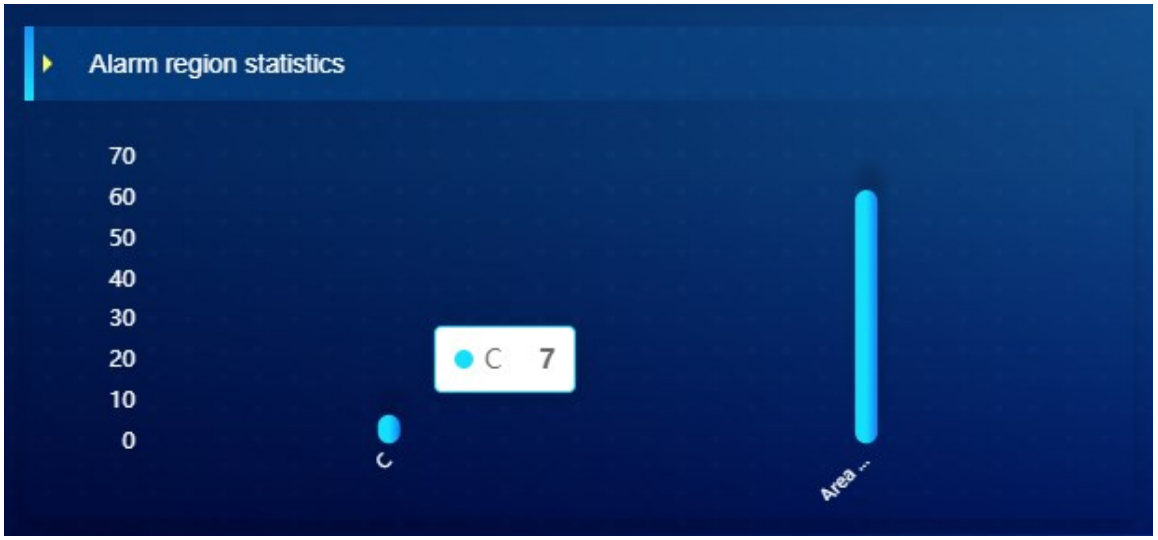


Alarm Rank Statistics

Display the number distribution of each alarm level of the access control.

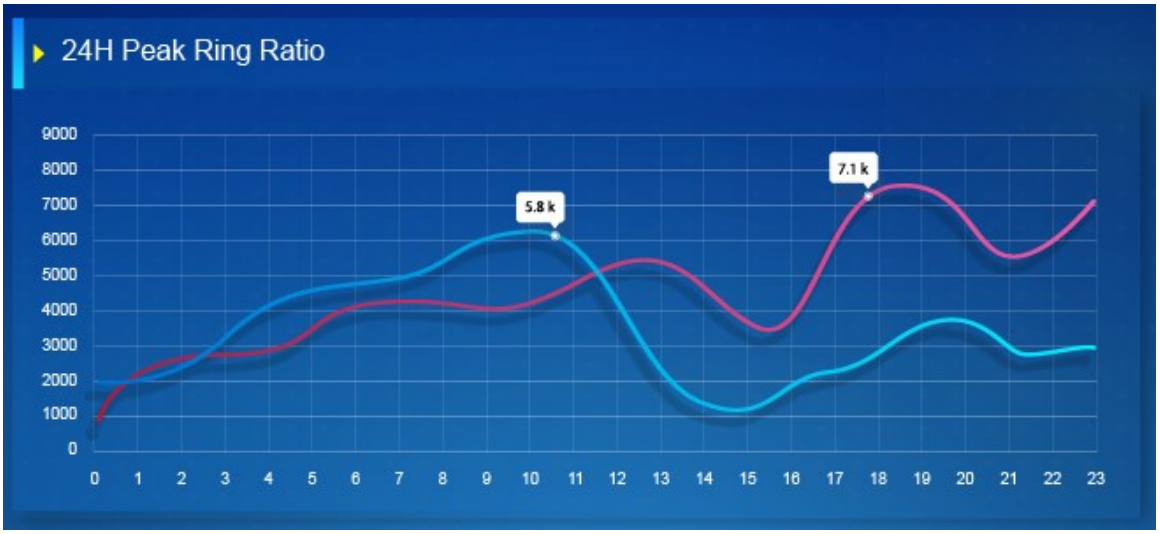
Alarm Region Statistics

Display the number of access alarms in different areas of the system.



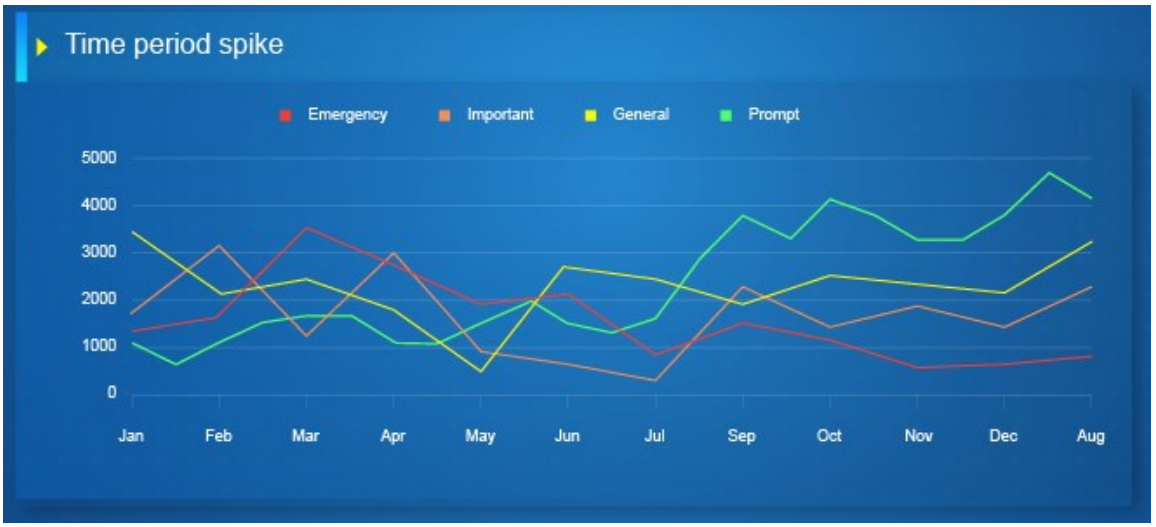
24H Peak Ring Ratio

A graph comparing the number of alerts per hour over a period of time.



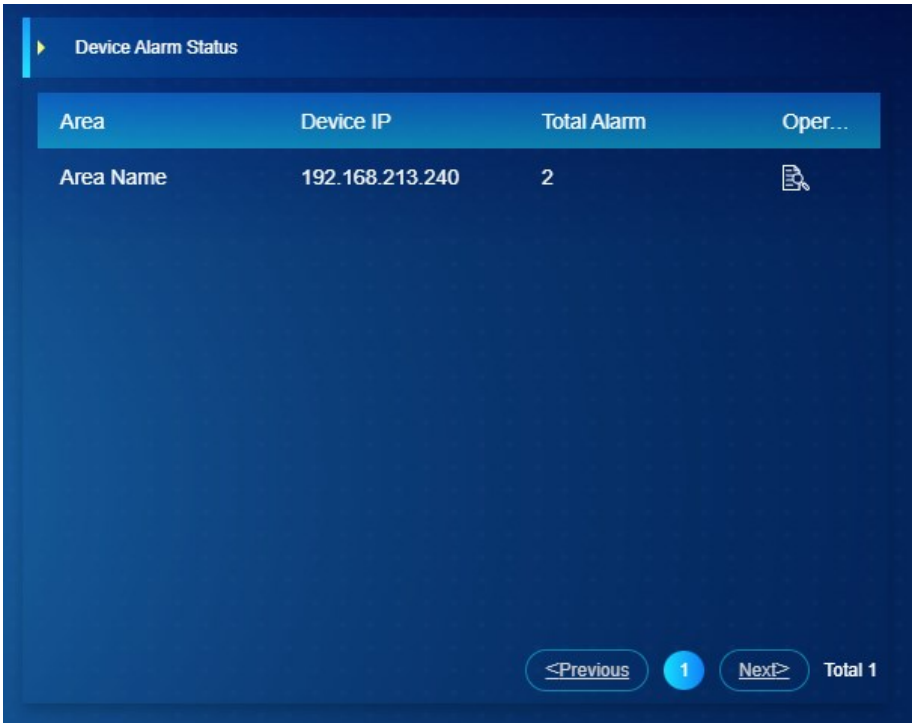
Time Period Peak

A graph comparing different access alarm levels over a period of time.

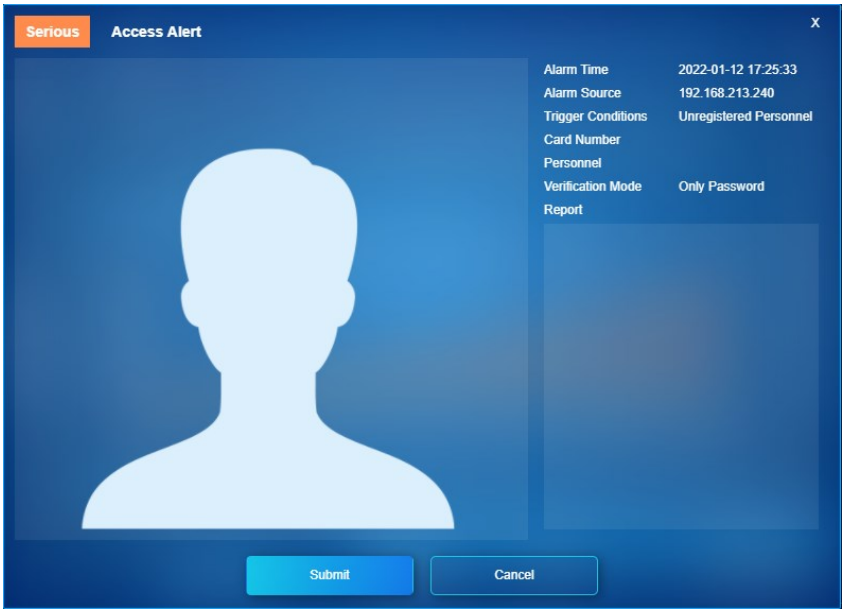


Device Alarm Condition

View access alarm status, quantity, and details of the device.

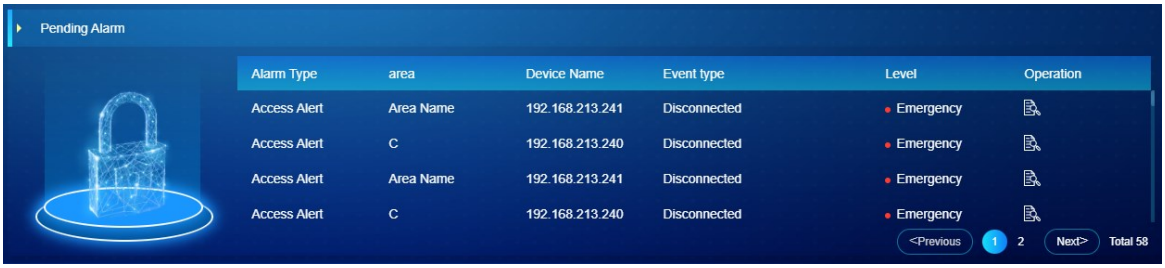


Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.

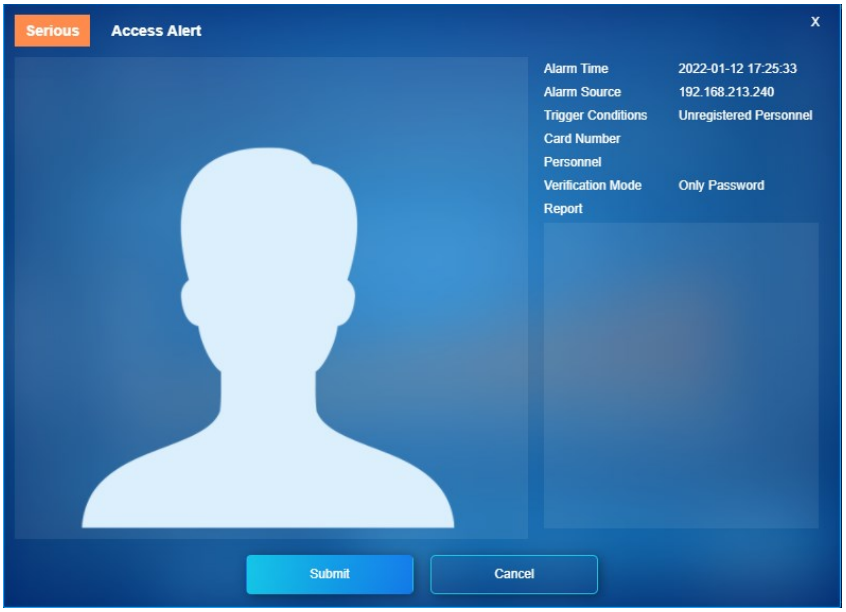


Pending Alarm

View pending access alarm status and details.



Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



Face Alert

Preconditions for Normal Use of Function

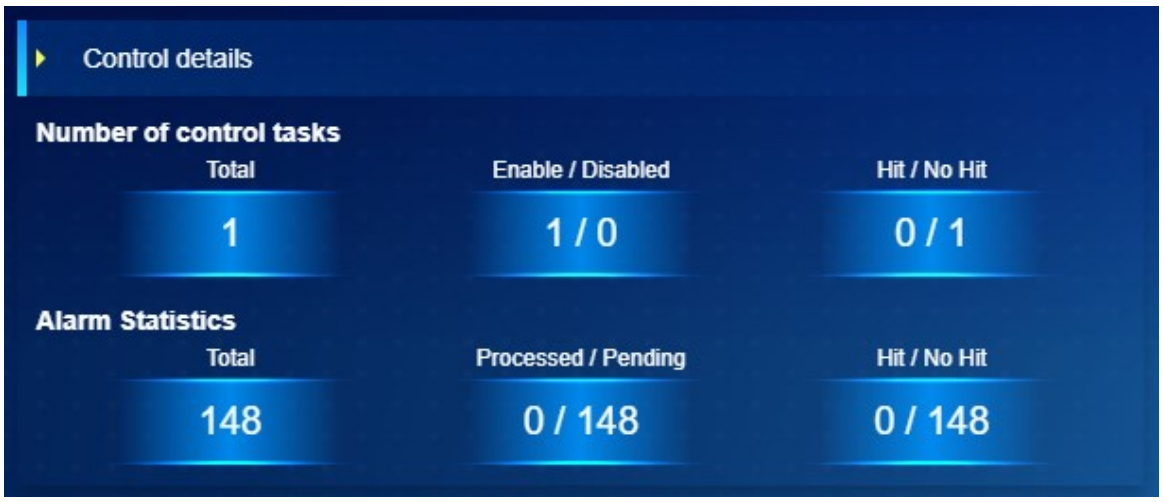
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View Face alert alarms in real time.

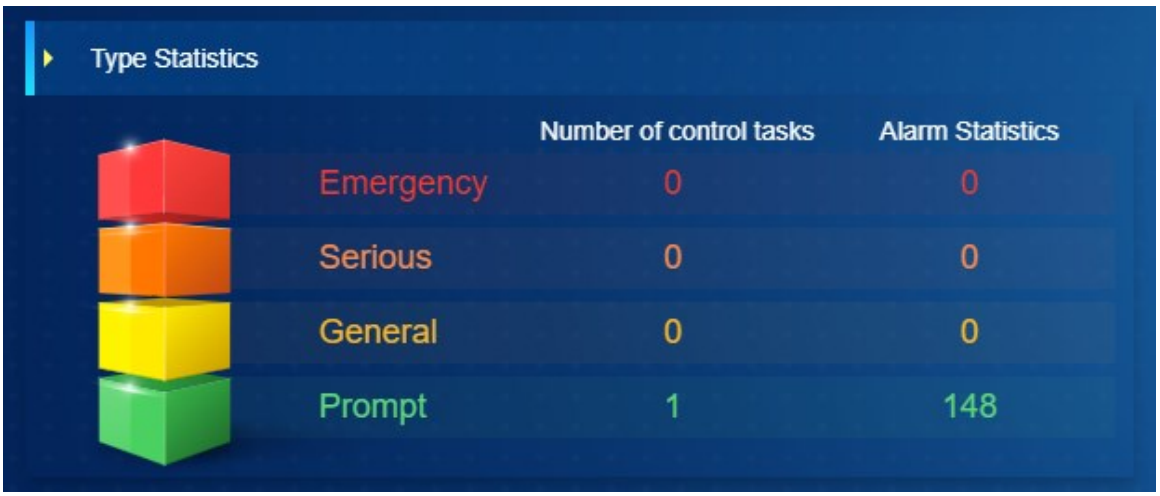
Control Details

Display the data situation of Face Alert and alarms that has been generated.



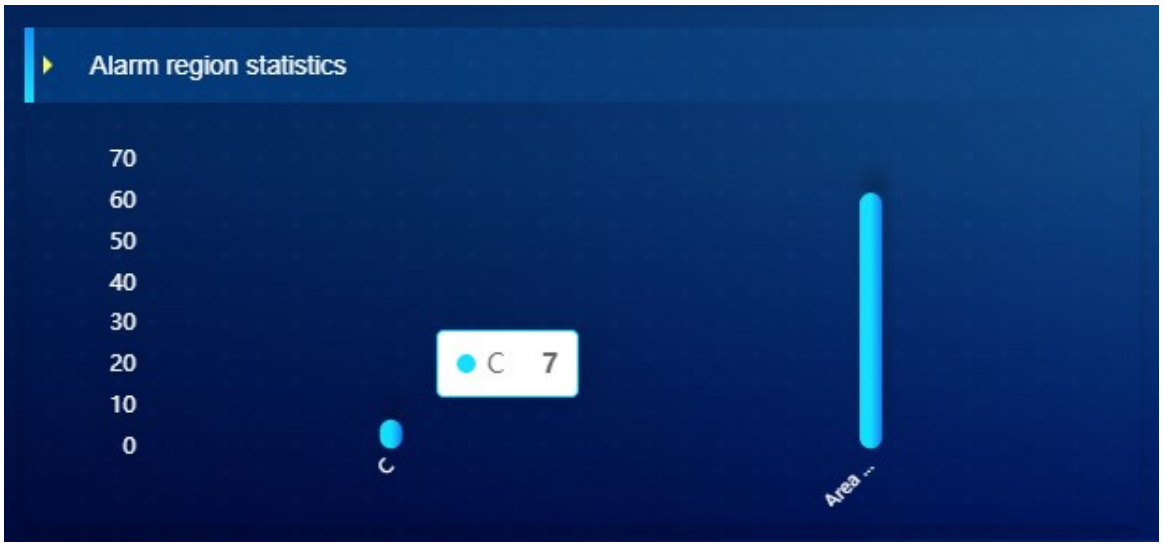
Type Statistics

Displays the number of alarms that have been set for each level of Face Alert and the number of alarms generated by each level.



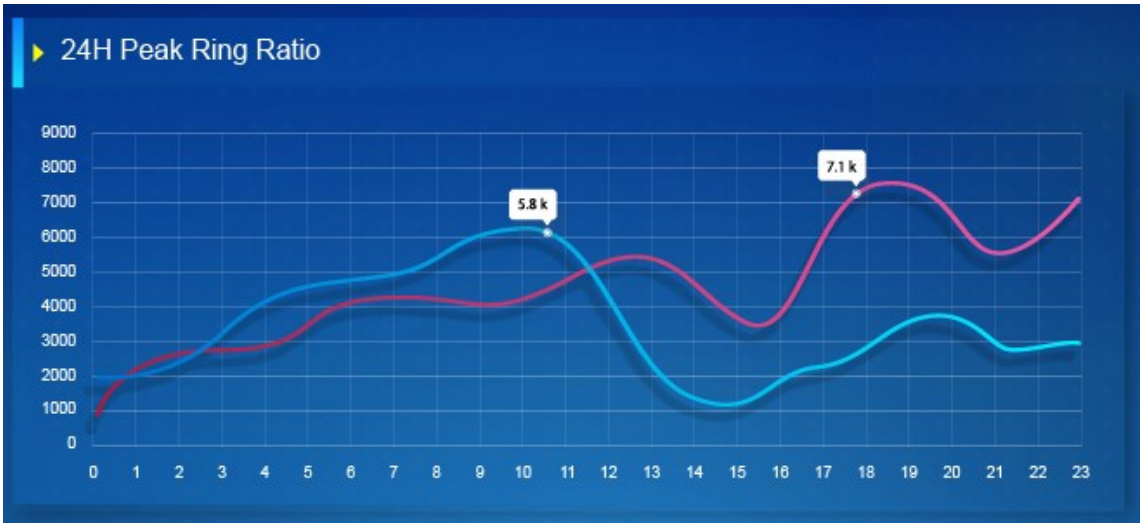
Region Statistics

Display the number of face alert alarms in different areas of the system.



24H Peak Ring Ratio

A graph comparing the number of alerts per hour over a period of time.

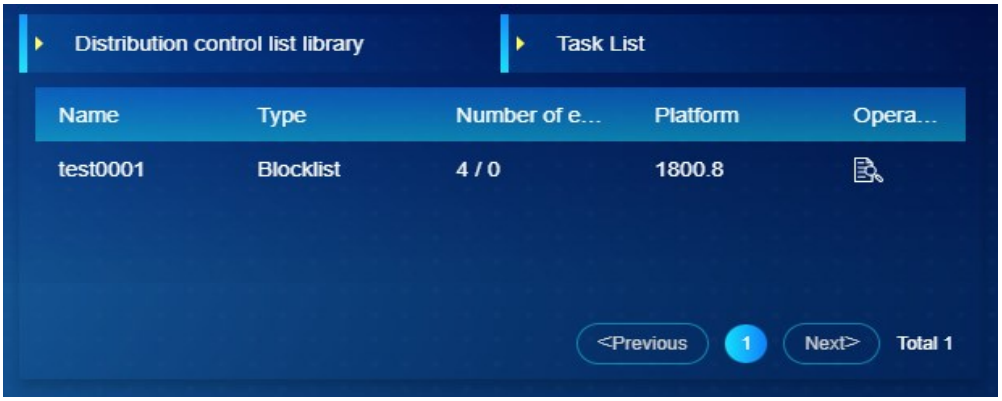


Time Period Peak

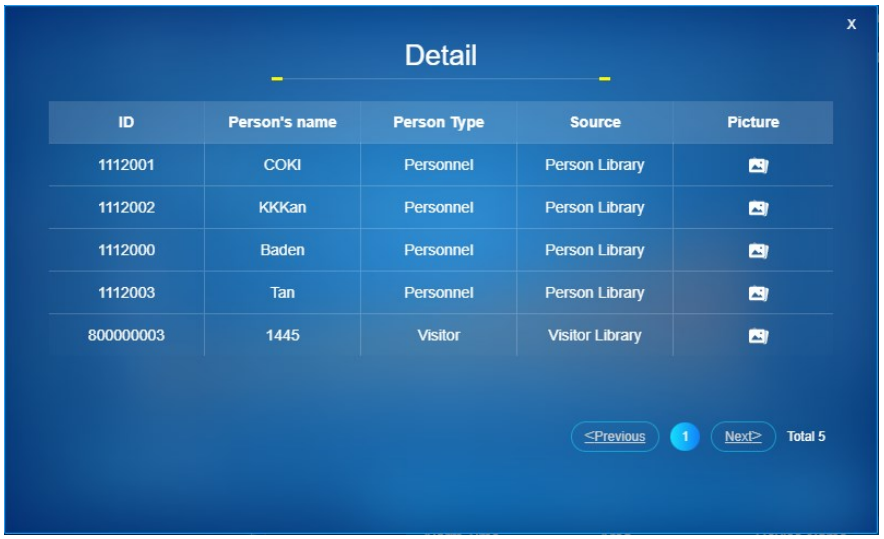
A graph comparing different face alert alarm levels over a period of time.

Distribution Control List Library

Display the face alert list library and the details of the list personnel that have been deployed.

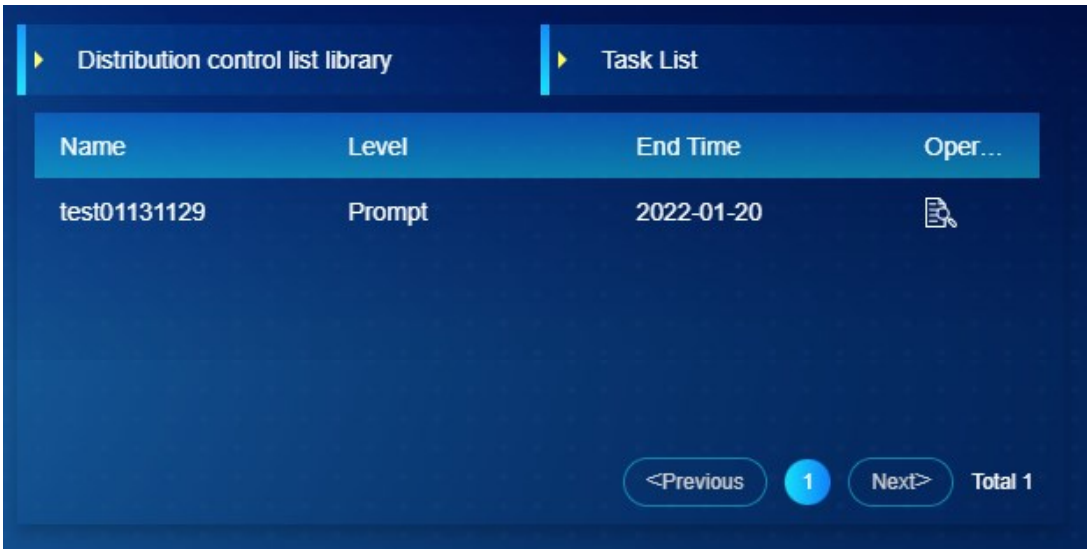


Click [**Detail**] to view the composition of the library.



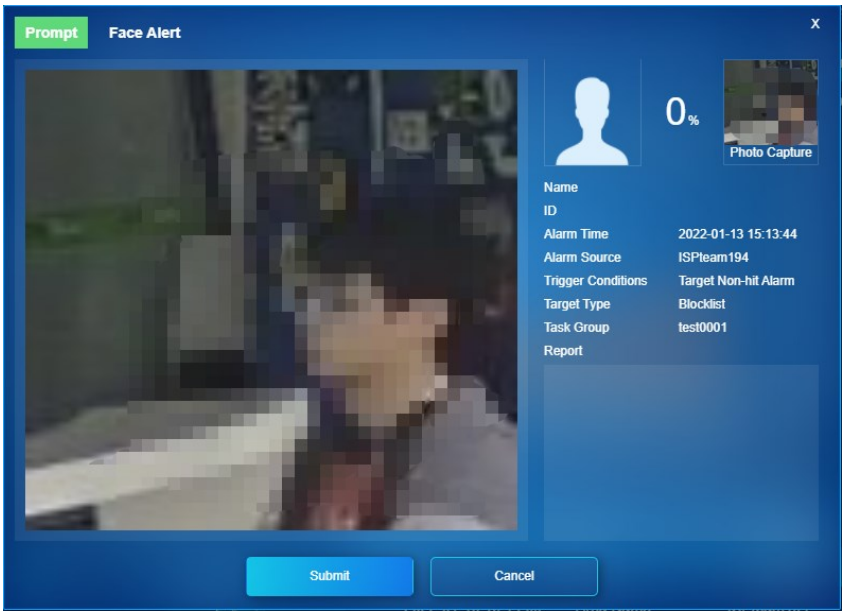
Task List

View the face alert task, and task details and the historical alarm records.



Click [**Detail**] to view Task detail and history alarm records.

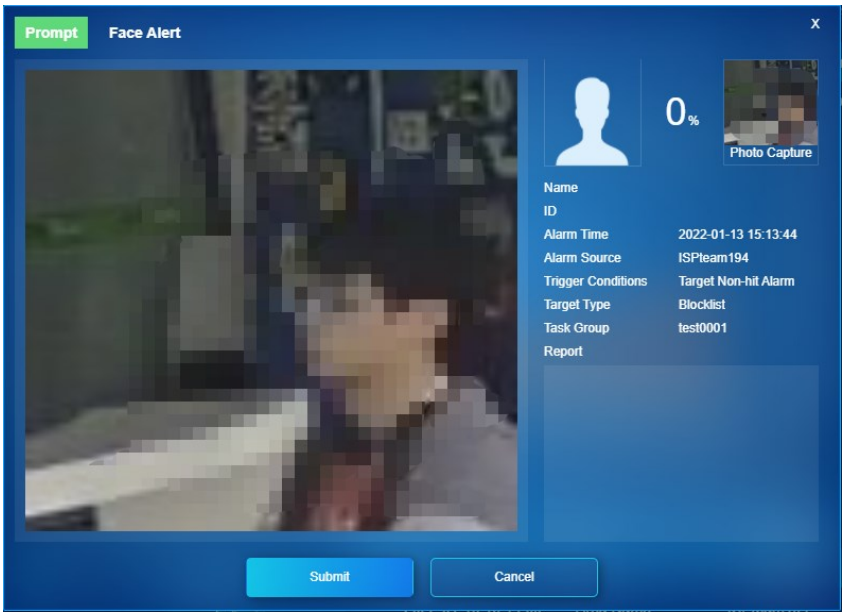
Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



Pending Alarm

View pending face alert alarm status and details.

Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



Vehicle Alert

Preconditions for Normal Use of Function

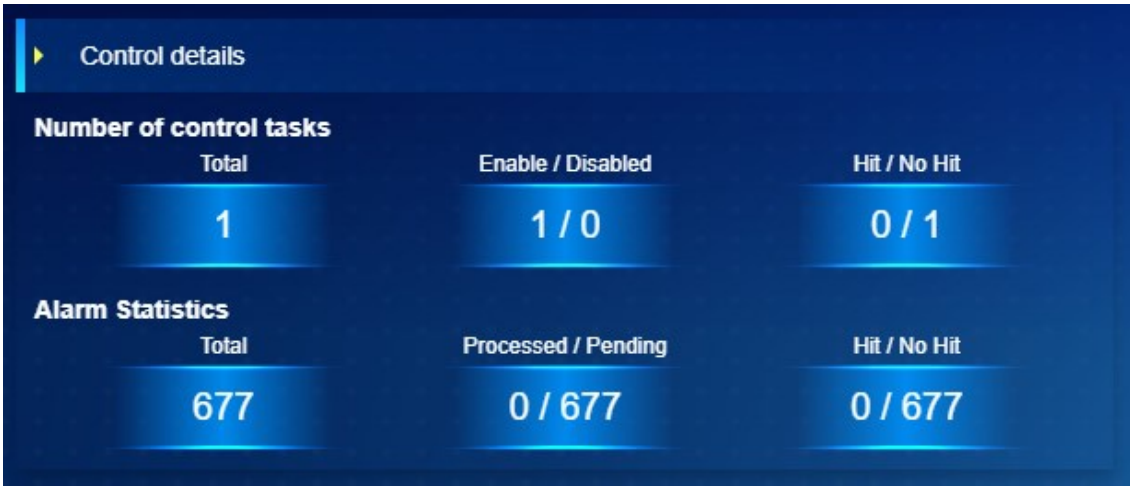
The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View vehicle alert alarms in real time.

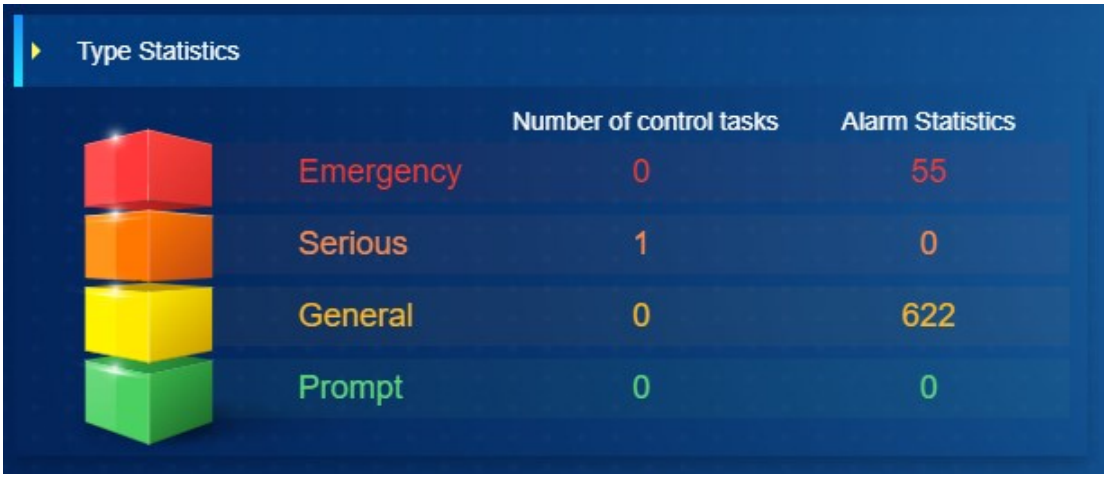
Control Details

Display the data situation of Vehicle Alert and alarms that has been generated.



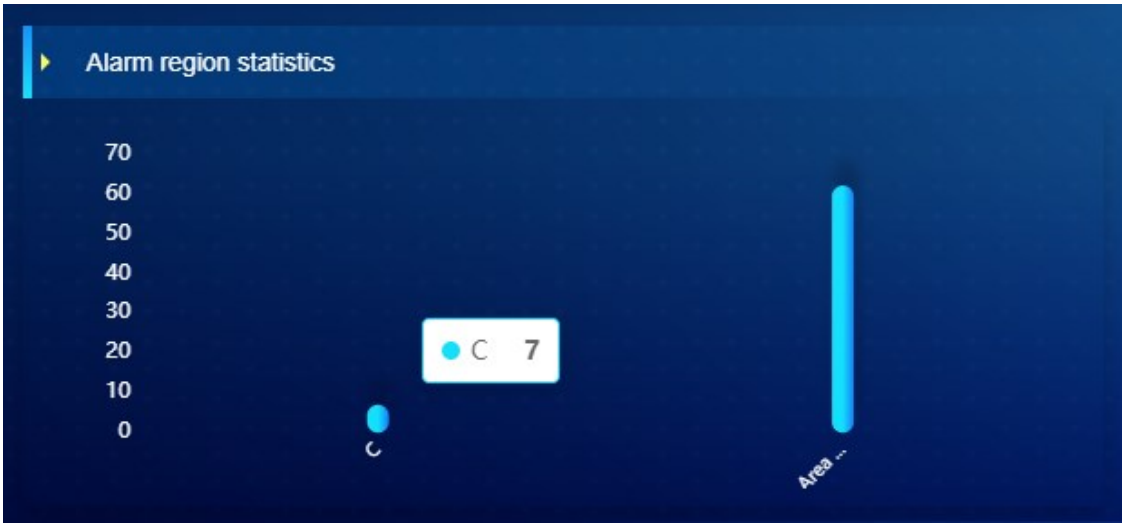
Type Statistics

Displays the number of alarms that have been set for each level of Vehicle Alert and the number of alarms generated by each level.



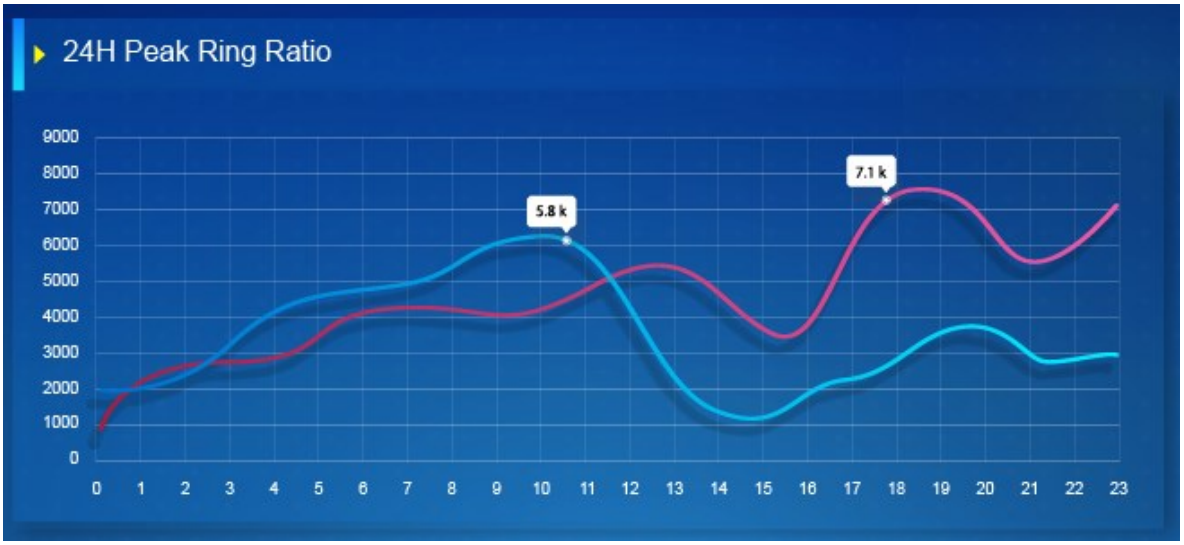
Region Statistics

Display the number of Vehicle alert alarms in different areas of the system.



24H Peak Ring Ratio

A graph comparing the number of alerts per hour over a period of time.

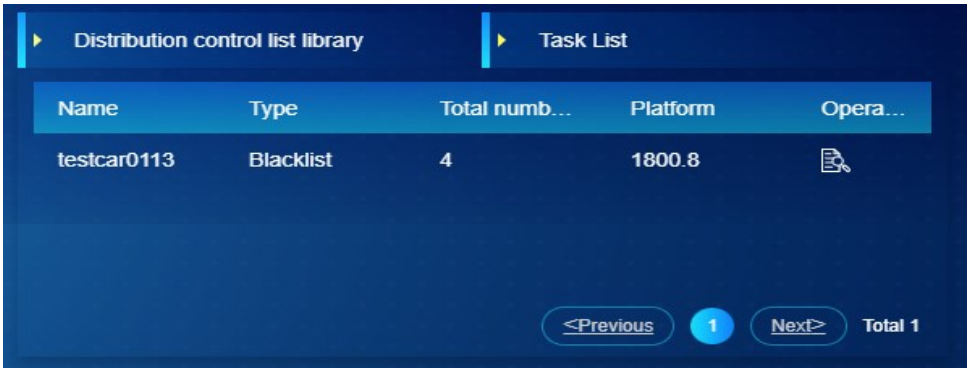


Time Period Peak

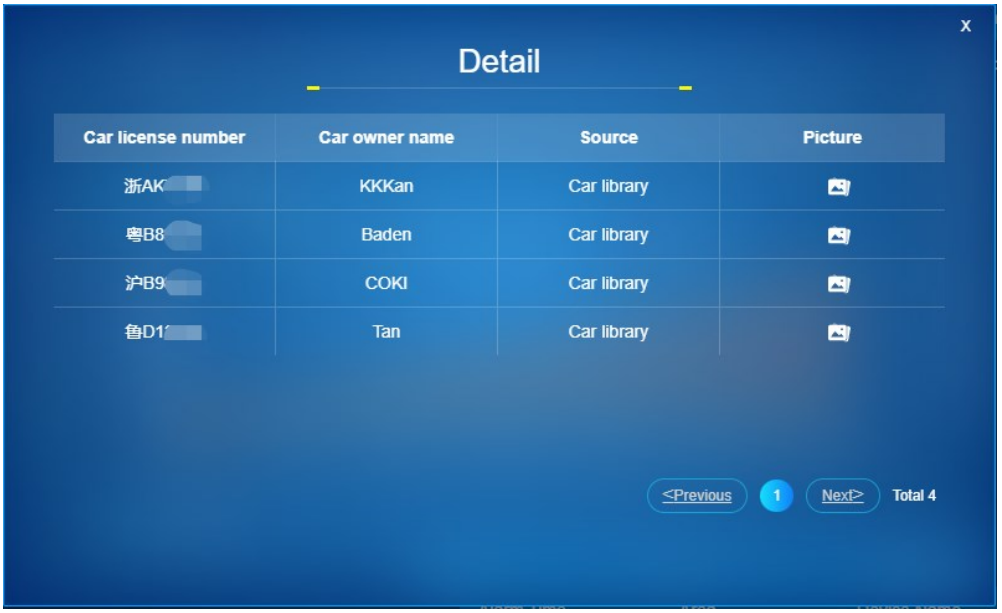
A graph comparing different face alert alarm levels over a period of time.

Distribution Control List Library

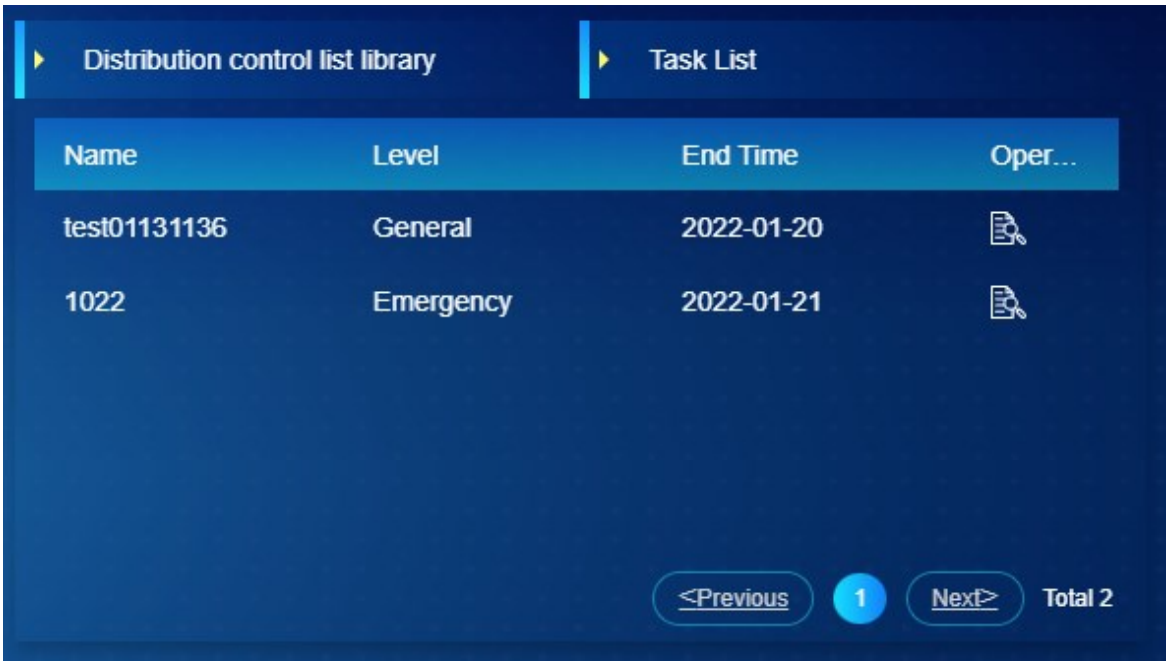
Display the vehicle alert list library and the details of the list personnel that have been deployed.



Click [**Detail**] to view the composition of the library.

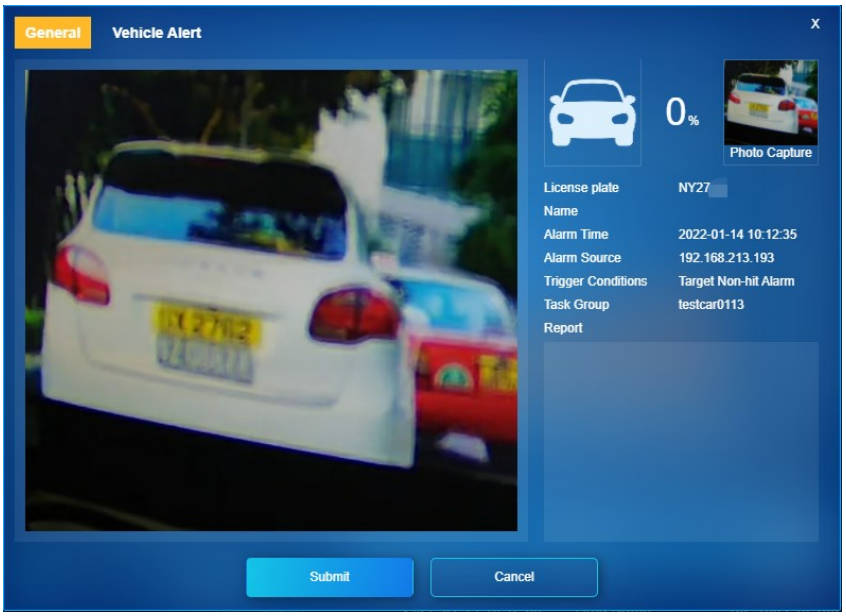


Task List



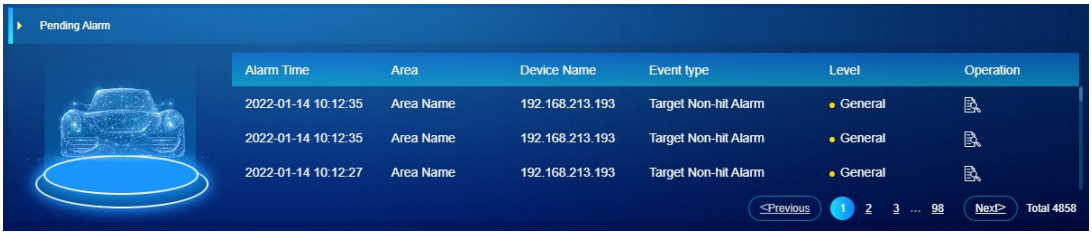
Click [**Detail**] to view Task detail and history alarm records.

Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.

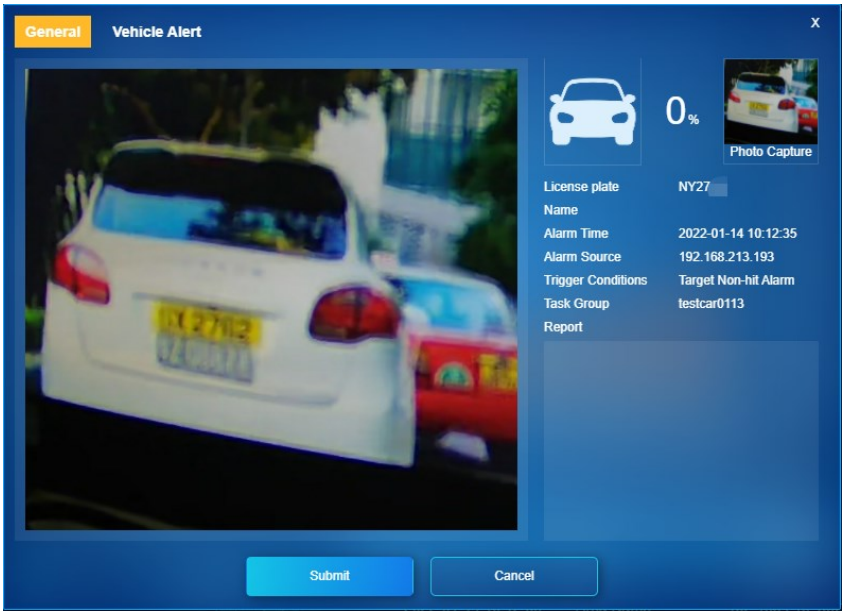


Pending Alarm

View pending vehicle alert alarm status and details.



Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



Camera Alert

Preconditions for Normal Use of Function

The software runs normally, and the account has the corresponding operation authority.

Function Usage Scenarios

View camera alert alarms in real time.

Total Number of Cameras

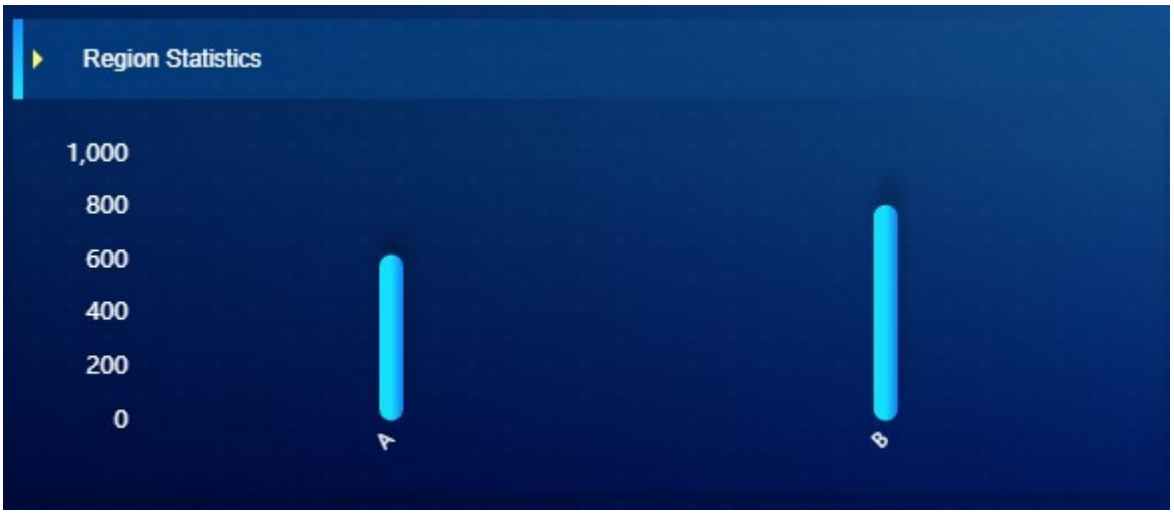
View the total number of cameras and the number of subscriptions used as alerts and the number of idle.

Type Statistics

Displays the distribution of the number of generated camera alarms of different levels.

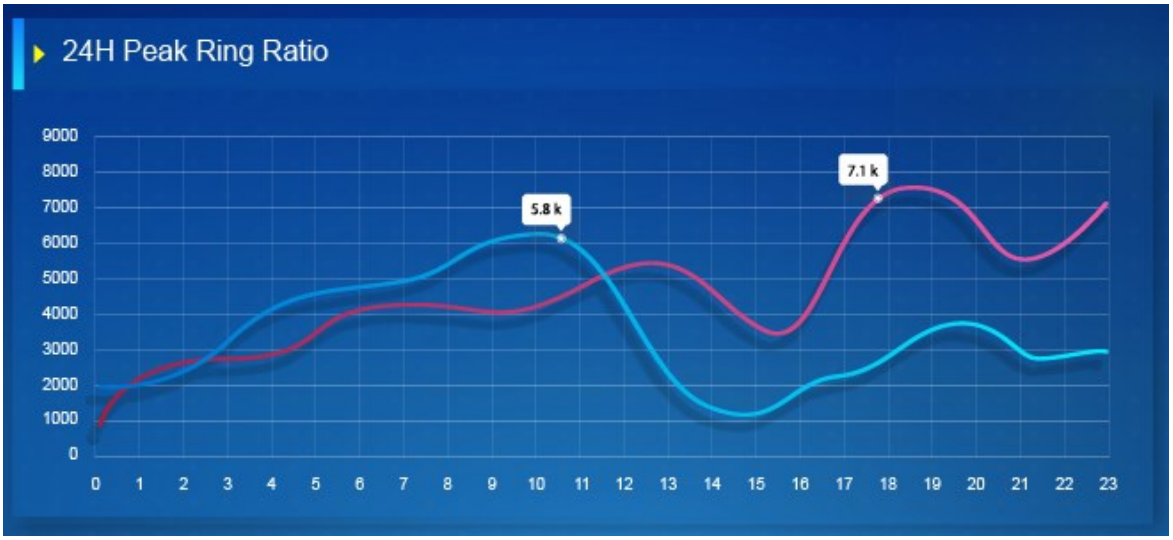
Region Statistics

Display the number of camera alarms in different areas of the system.



24H Peak Ring Ratio

A graph comparing the number of alerts per hour over a period of time.



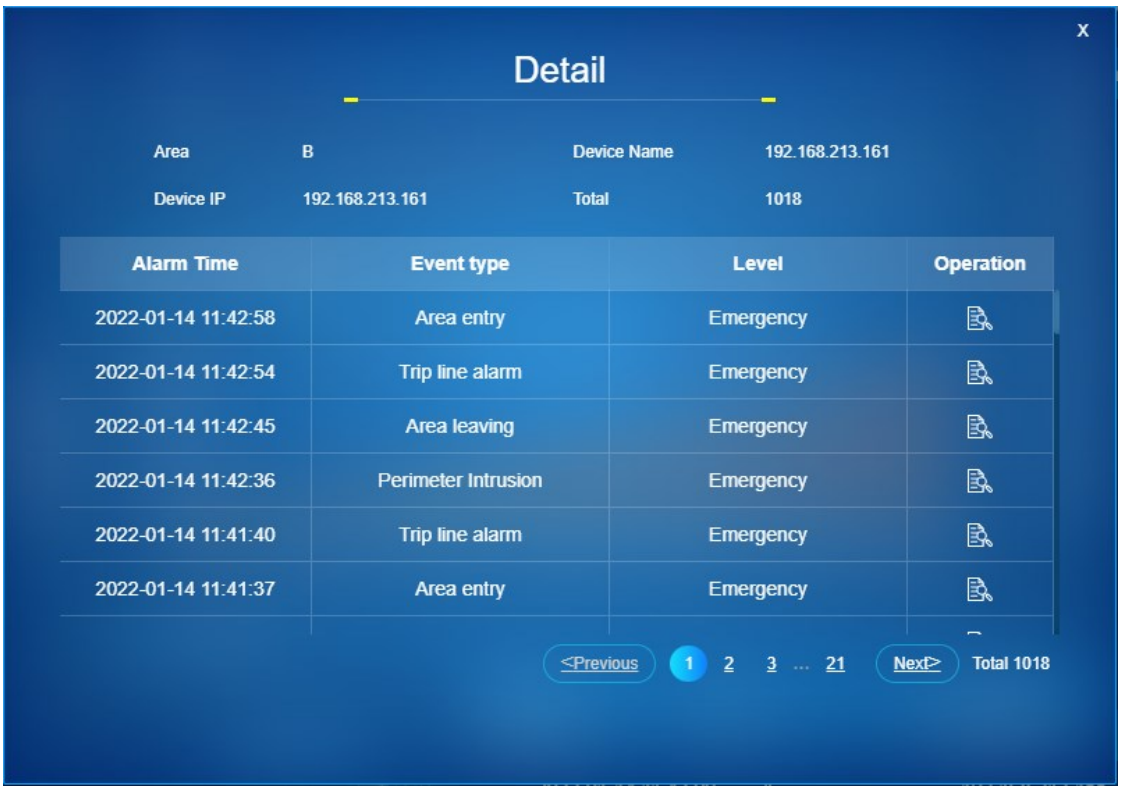
Time Period Spike

A graph comparing different face alert alarm levels over a period of time.

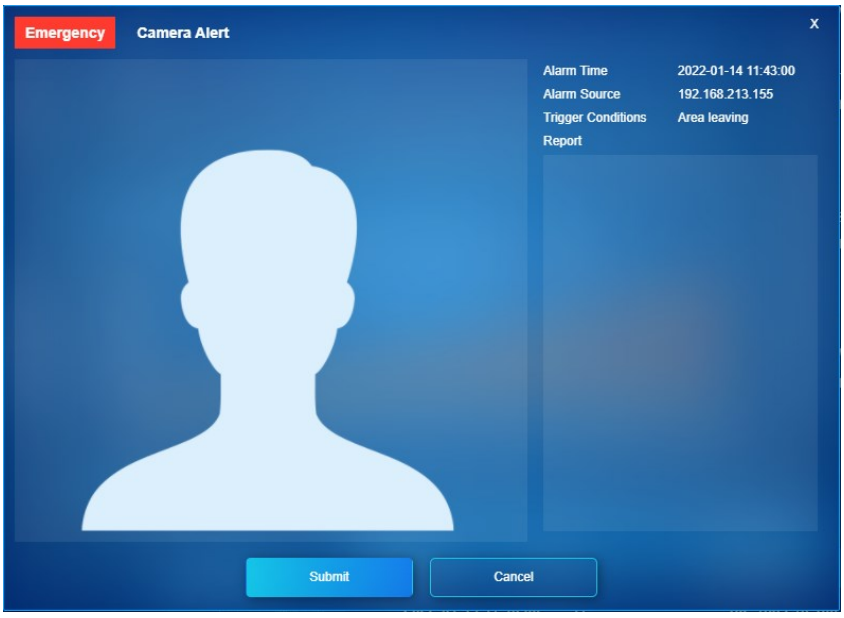
Device Alarm Status

Display the generated alarm devices and their alarm numbers and view the alarm details of the device.

Click [**Detail**] to view device detail and alarm records.

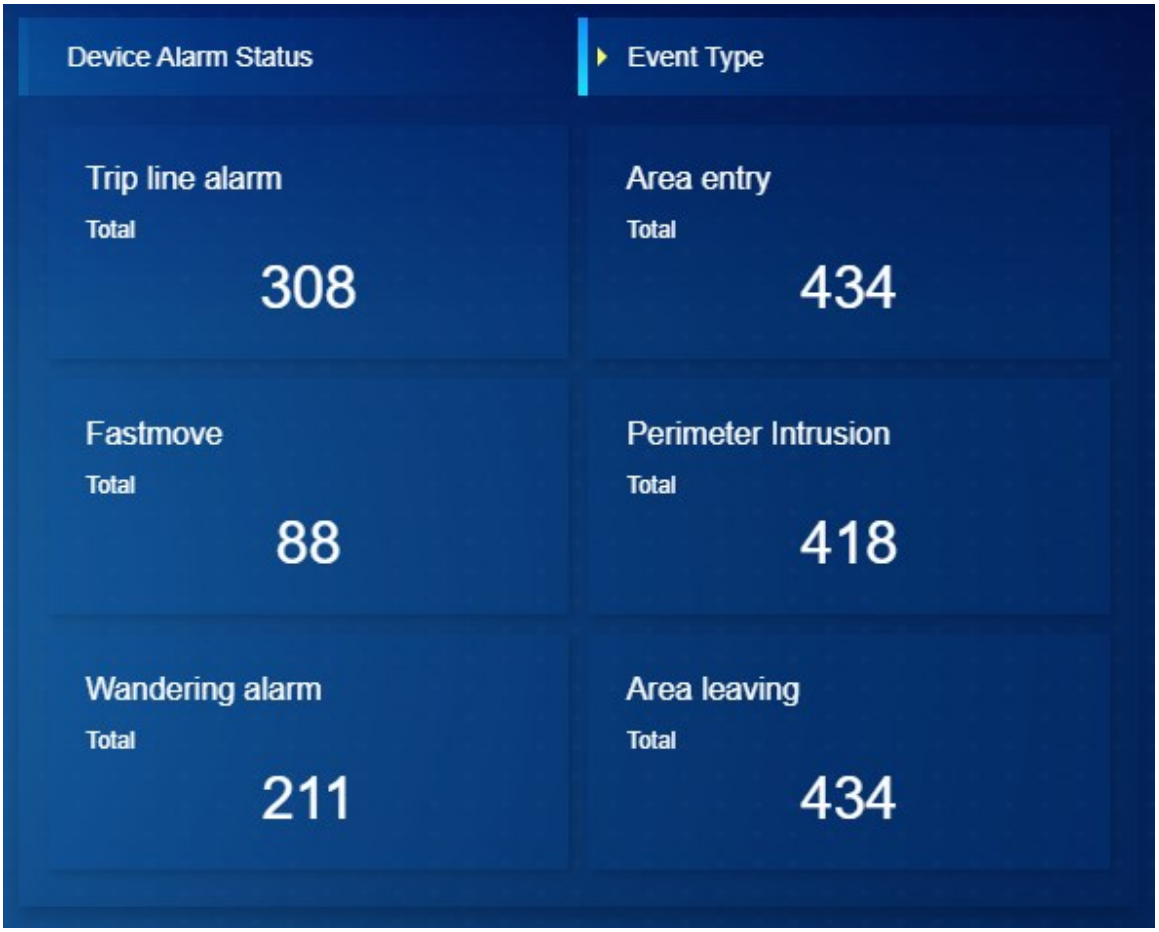


Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



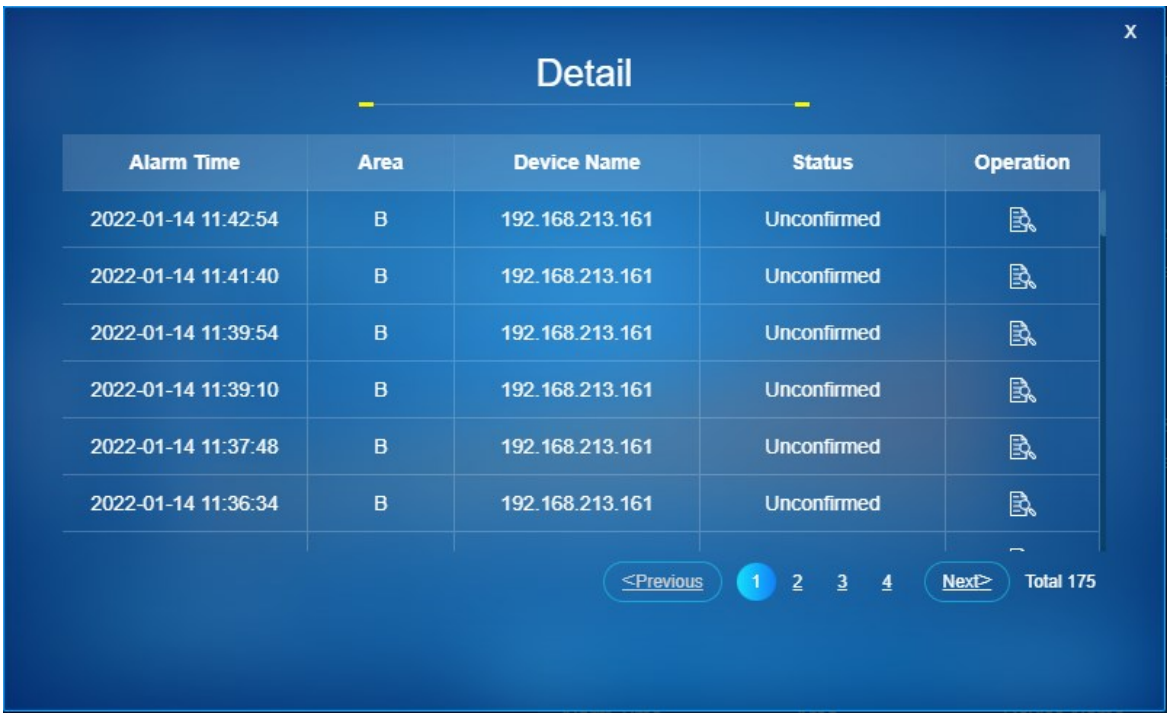
Event Type

View the number of different camera alarm events and alarm details.

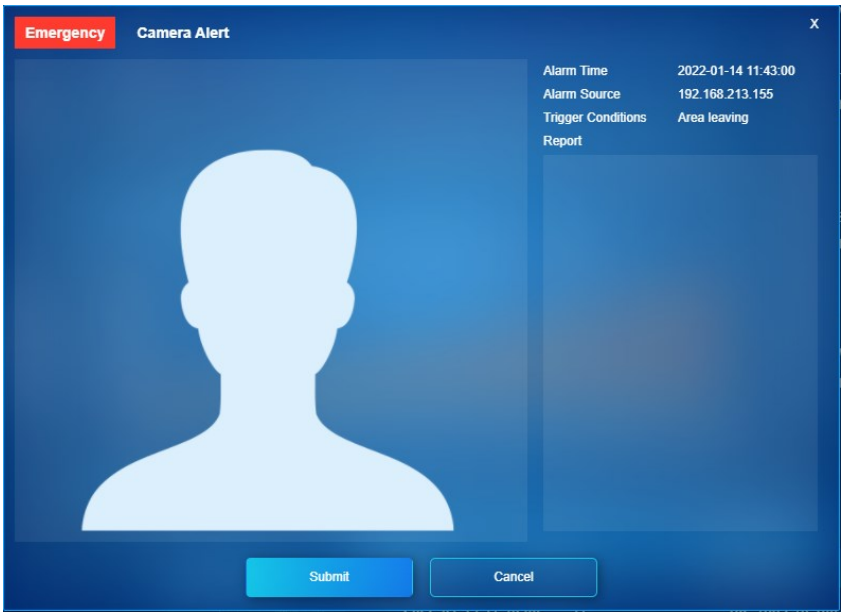


Click on an event to view the distribution of the number of different regions.

Click [**Detail**] to view the details of the alarms in the area.

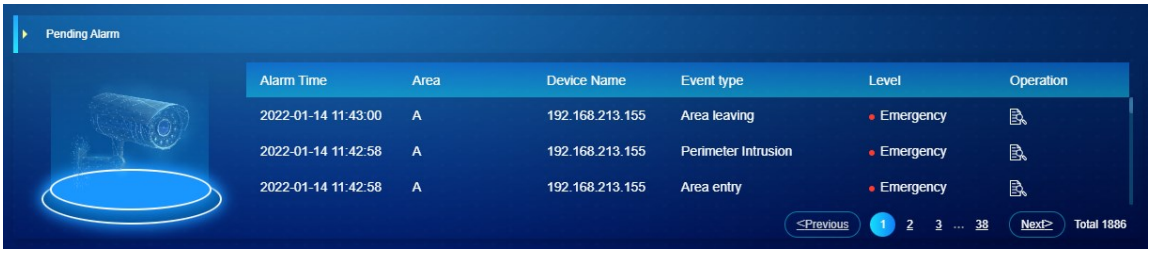


Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.

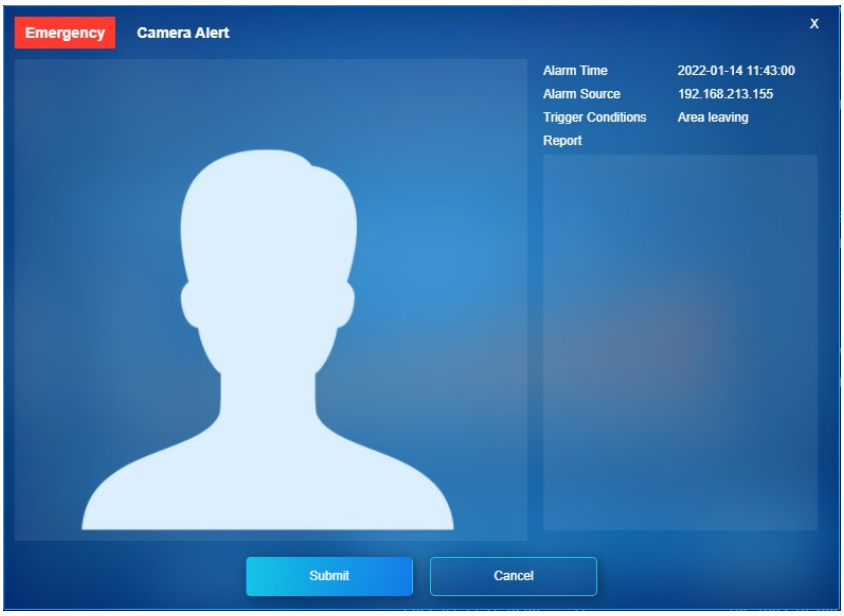


Pending Alarm

View pending camera alarm status and details.



Click [**Detail**] to view alarm detail and make a text content and click [**Submit**] to confirm an alarm.



21. System Management

System settings mainly include assigning system users (such as company management users, registrars, and access control administrators) and configuring the roles of the corresponding modules, managing the database, setting system parameters, and view operation logs, etc.

21.1. Basic Management

Function List

Operation	Description
Operation Log	All operation logs are displayed on this page.
Database Management	The database can be refreshed, backed up and scheduled as required.
Regional Settings	Area is a spatial concept that allows users to manage devices in a specific area.
Department	Operate the department of personnel to better divide the personnel.
Mail Management	Set up email sending server information.
Data Dictionary	The user can find the meaning of the error code and self-check the software error.
Data Cleaning	Data cleaning is to save the storage space of the server and prevent the data stored by the server from being too large.
Audio File	Audio file on the management software.
Data Migration	When the software is upgraded from the old version to the new version, the old version of data can be transferred to the new version.
Type of Certificate	Type of certificate supported by the management system.
Print Template	View and edit the employee card print template.
System Monitoring	Check the server load usage.

21.1.1. Operation Log

Function Description

All operation logs are displayed on this page. You can query specific logs based on conditions.

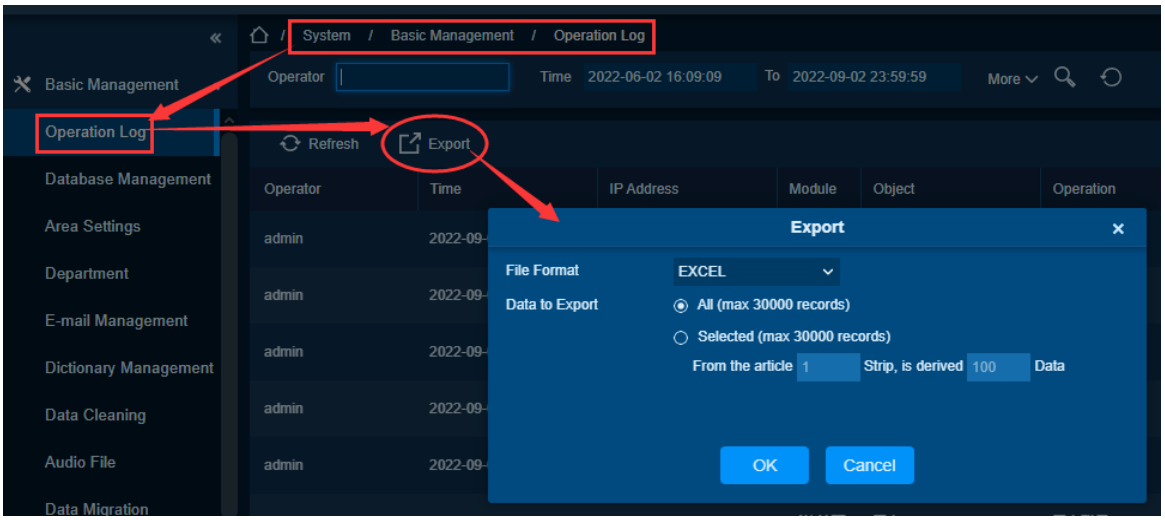
Export

Preconditions for Normal Use of Function

The administrator has export function permissions.

Function Usage Scenarios

It is used when the data of the list needs to be exported to EXCEL, PDF, CSV, and other formats.



21.1.2. Database Management

Function Description

All historical operation logs related to database backup are displayed on this page. Your database can be refreshed, backed up and scheduled as required.

Immediate Backup

Preconditions for Normal Use of Function

The administrator has the authority for the immediate backup function and has the ability to set up an FTP server.

Function Usage Scenarios

Perform manual backup of the database of the local area network and data recovery operations of manual backup.

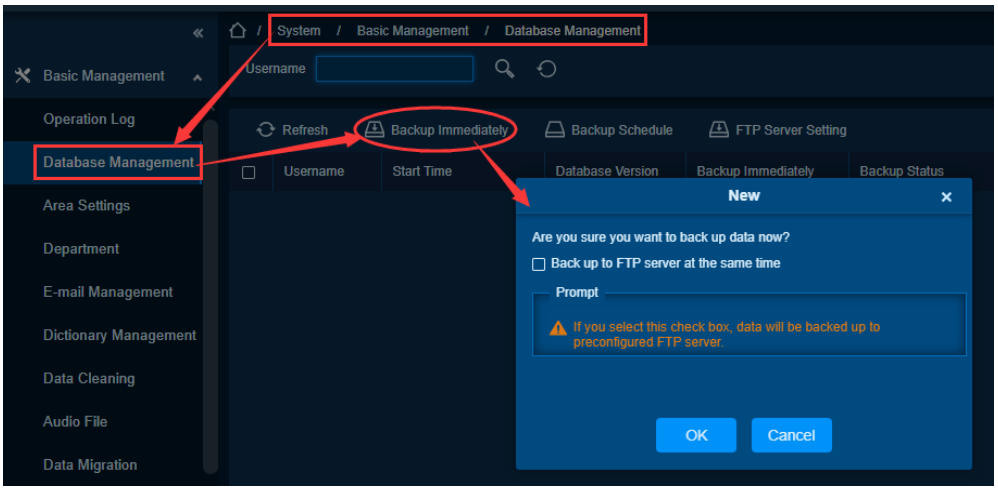
Feature Trigger Result

The database is successfully backed up, and the backup data is successfully restored.

Steps:

- Click [**Backup Immediately**], a pop-up window will pop up.
- Check whether it needs to be assigned to the FTP server.

- Click [**OK**] to complete the database backup operation.



Scheduled Backup

Preconditions for Normal Use of Function

The administrator has the authority to schedule backups.

Function Usage Scenarios

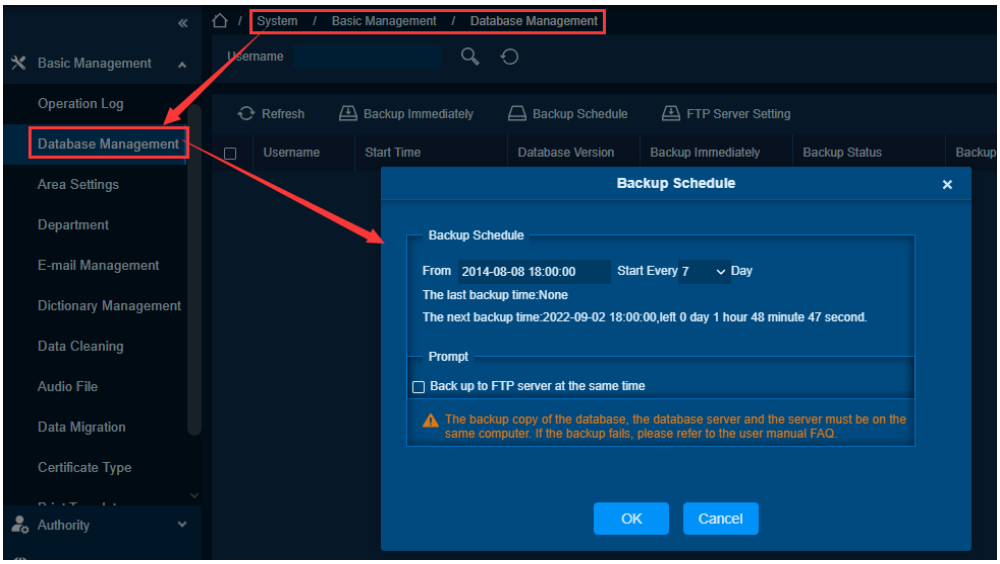
You can set how often the backup is required.

Feature Trigger Result

Back up according to the set time.

Step:

- Click [**Backup Schedule**] button to pop up a window.
- Set the time when the backup needs to be scheduled.
- Check whether you need to synchronize to the FTP server.
- Click [**OK**] button to complete the planned backup operation.



FTP Server Settings

Preconditions for Normal Use of Function

The administrator has the authority to set up the FTP server.

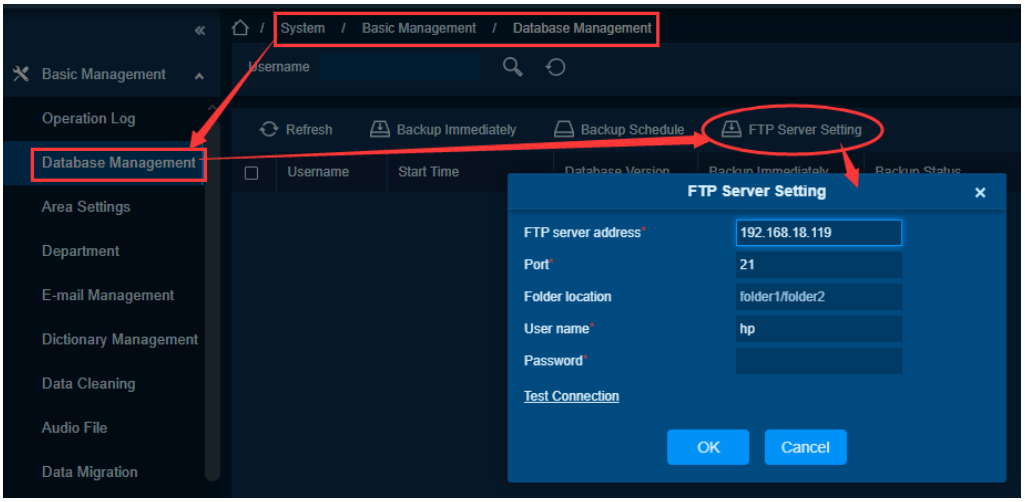
Function Usage Scenarios

When you need to back up the database, you must first set up an FTP server.

Feature Trigger Result

Set up FTP server as a precondition for other functions.

Steps:



- Click [**FTP Server Setting**] button, a window will pop up.
- Fill in the relevant information, the items marked with * are required, and the fields are explained as follows:

FTP Server Address: Set the address of the FTP server.

Port: Set the port number

Folder Location: Set the address after the database backup.

Username: Set the username.

Password: Set the password

- Click [**OK**] button to complete the FTP setting operation.

21.1.3. Area Setting

Function Description

Area is a spatial concept that allows users to manage devices in a specific area. After setting the area, you can filter the device (door) by area according to real-time monitoring.

Add

Preconditions for Normal Use of Function

The administrator has the add area permission.

Function Usage Scenarios

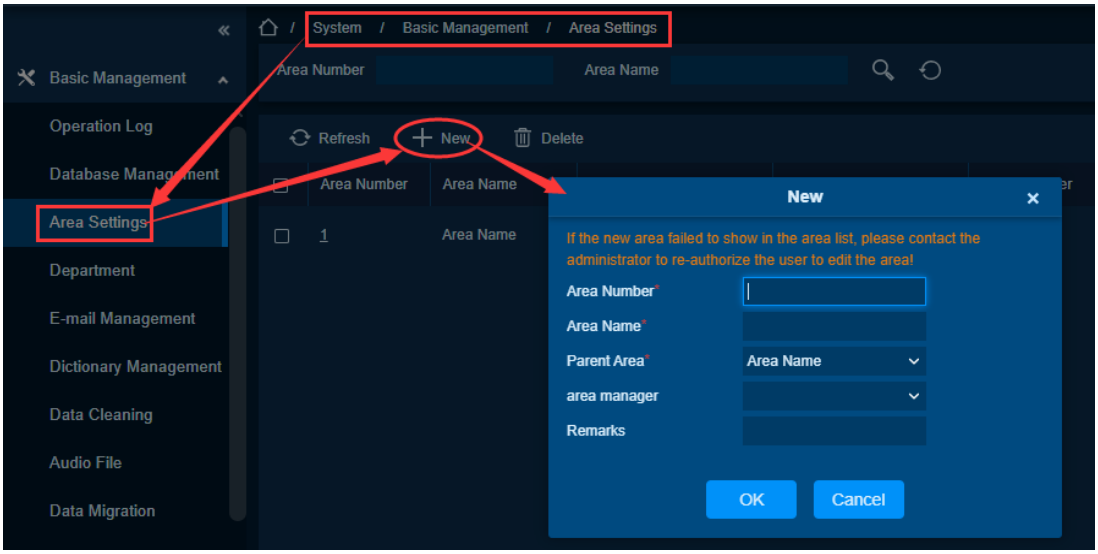
Use when you need to divide the area or manage the area more effectively.

Feature Trigger Result

Add an area.

Steps:

- Click [**New**] button to pop up a window.



- Fill in the relevant information, the items marked with * are required, and the fields are explained as follows:

Area Number: Give add area settings a number, the number must be unique.

Area Name: Give add area settings a name, the name must be unique.

Parent Area: The parent area of the add area.

Area Manager: the administrator who sets the area.

Remarks: Set the remark information in the add area.

- Click [OK] button to complete the add operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there are areas that can be deleted in the list, and the areas that need to be deleted are not associated with other information.

Function Usage Scenarios

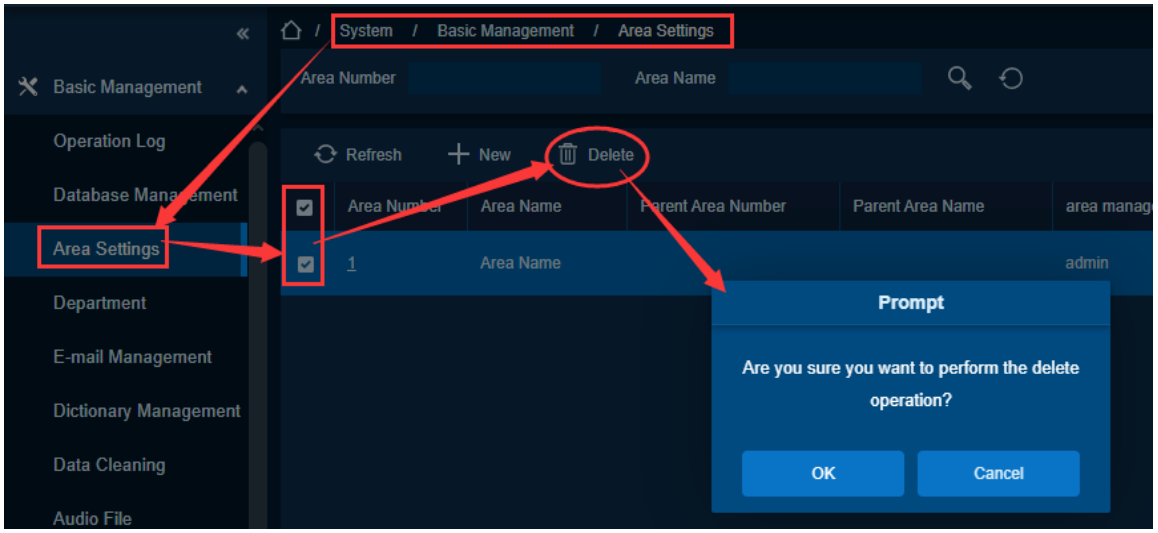
Used when a certain area is not needed, or this area has expired.

Feature Trigger Result

Delete the checked area.

Steps:

- Select the area that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.
- Click [**OK**] in the prompt box to complete the delete operation.



21.1.4. Department

Function Description

Operate the department of personnel to better divide the personnel.

Add

Preconditions for Normal Use of Function

The administrator has the add department permission, and the department name and department number must be unique.

Function Usage Scenarios

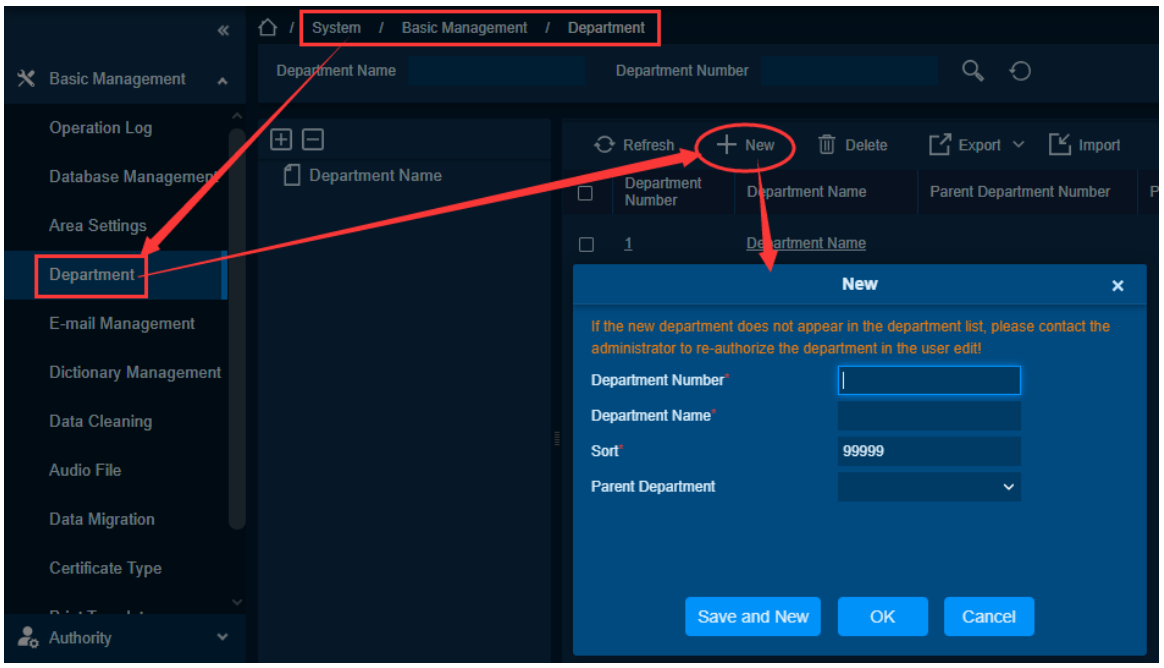
To better manage the staff, divide the staff into different parts, you need to add the corresponding department.

Feature Trigger Result

Add a department.

Steps:

- Click [**New**] button a new window will pop up.



- Fill in the relevant information in the pop-up window. Items marked with * are required. The fields are described as follows:

Department Number: Set the department number, the number must be unique.

Department Name: Set the department name, the name must be unique.

Sort: Set the sort of department.

Parent Department: Set the parent department of the department.

- Click [OK] button to complete the add operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there are data that can be deleted in the list.

Function Usage Scenarios

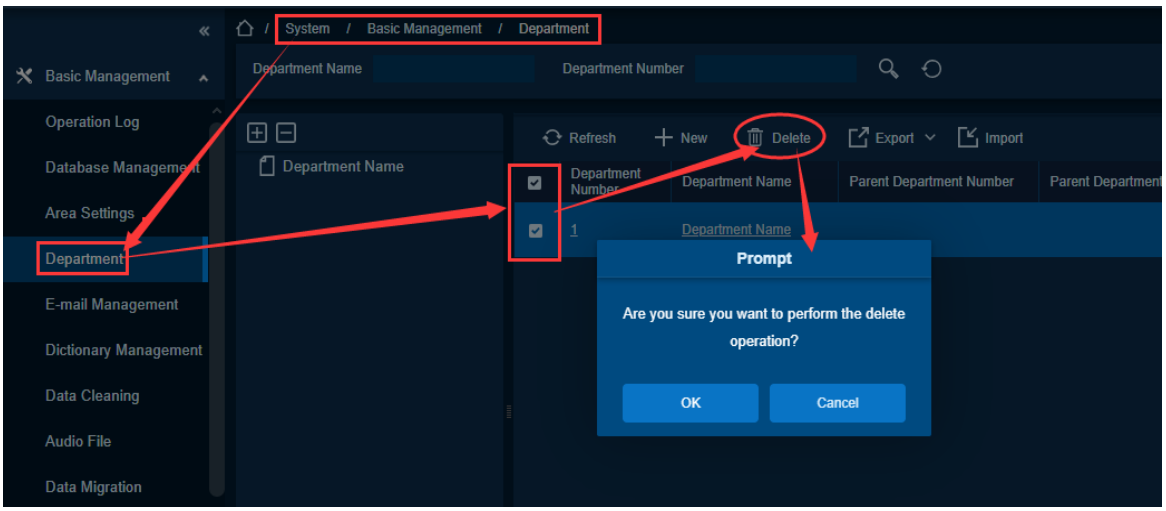
Delete redundant or unused departments.

Feature Trigger Result

Delete the selected department.

Steps:

- Select the department that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete operation.



Export Department Information

Preconditions for Normal Use of Function

The administrator has the right to export department information.

Function Usage Scenarios

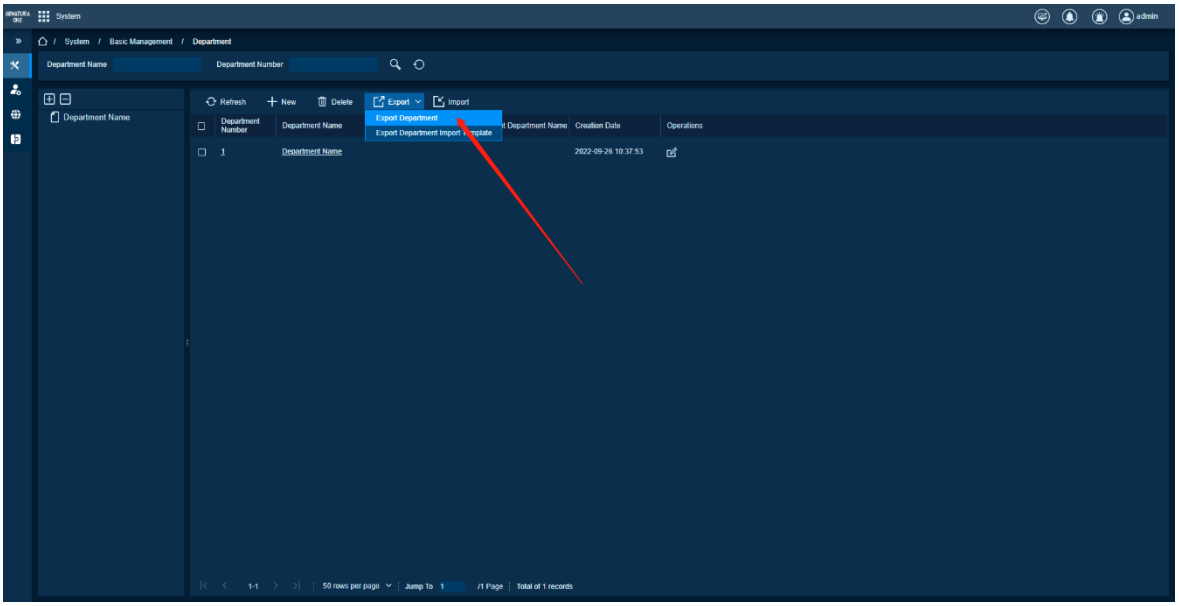
Export the department information on the software to the computer.

Feature Trigger Result

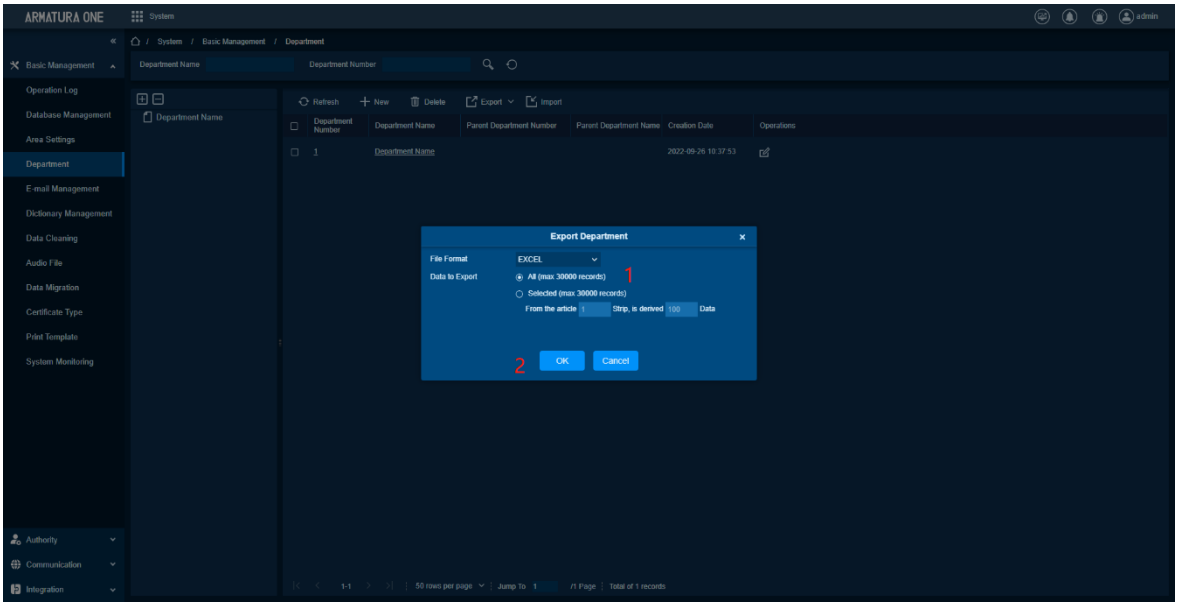
Operations	Description
Select Excel	Export department information to EXCEL format
Select PDF	Export Department information to PDF format
Select CSV	Export Department information to CSV format
Select All Data	All data of export department information
Select the amount of Data Export	Partial data of export department information

Steps:

- Select the department that needs to be exported.
- Click [**Export**] drop-down box.
- Select [**Export Department**] in the drop-down box, and a window will pop up.



- Select the File Format.
- Select the Data Range.
- Click [**OK**] to complete the export department information operation.



Export Department Template

Preconditions for Normal Use of Function

The administrator has the export department template permission.

Function Usage Scenarios

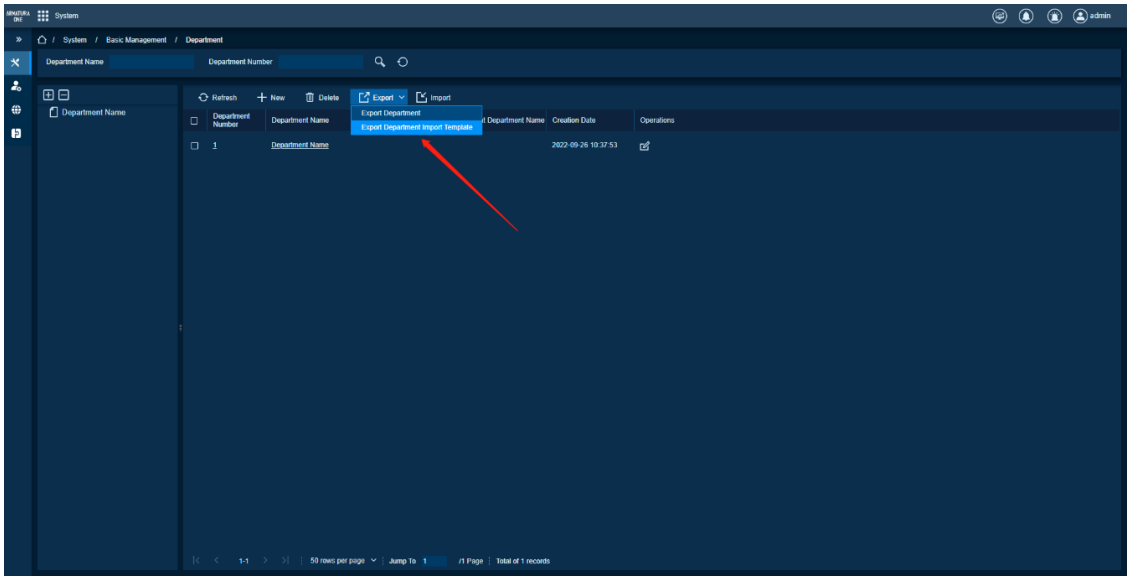
When you need to import the department in the EXCEL format, you need to use the department's EXCEL template.

Feature Trigger Result

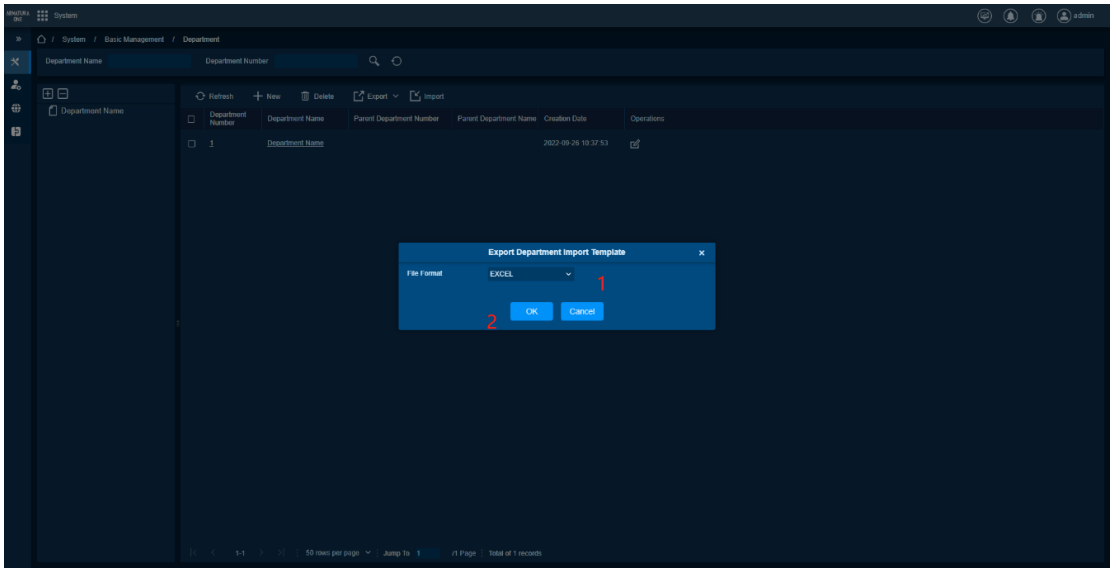
Export the department template to EXCEL format.

Steps:

- Click [**Export**] drop-down box.
- Select [**Download Department Import Template**] in the drop-down box.



- Select format as EXCEL format.
- Click [**OK**] button to complete the export department template operation.



Import

Preconditions for Normal Use of Function

The administrator has the import function permission, and the imported template is the export department template.

Function Usage Scenarios

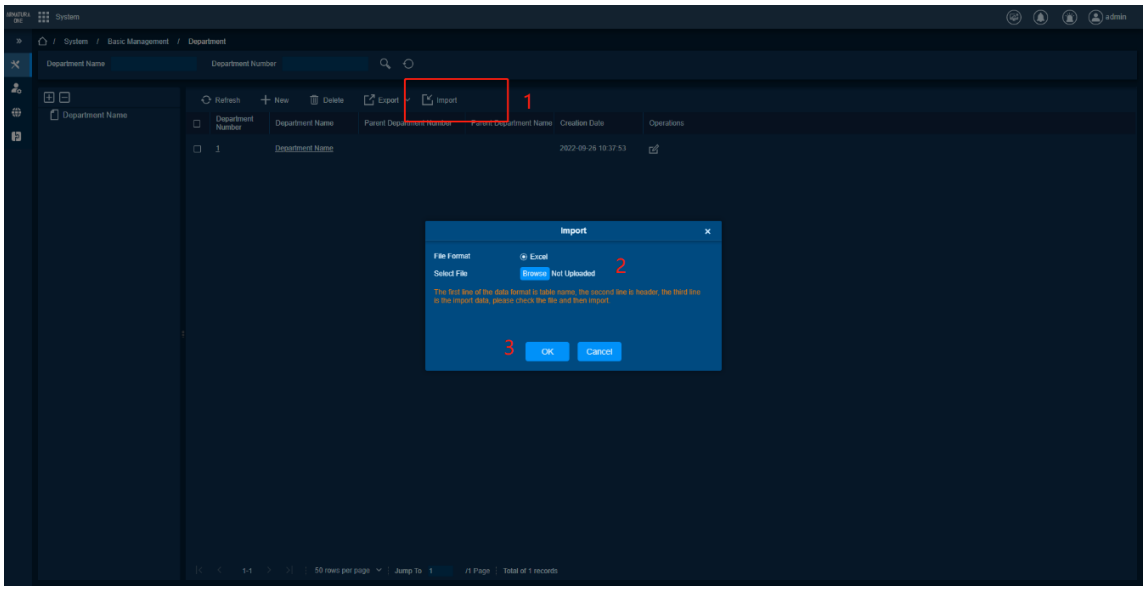
Import the Departments written in EXCEL forms into the software.

Feature Trigger Result

Import the data in the EXCEL form into the software.

Steps:

- Click [**Import**] button to pop up a window.
- Click [**Browse**] button in the pop-up window and select the template to be imported.
- Click [**OK**] button to complete the import operation.



21.1.5. E-mail Management

Function Description

Set up email sending server information. Before sending an email, you need to select prompt template and linkage, and display all the sending information.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there is information that can be deleted in the list.

Function Usage Scenarios

When unused information appears, check delete.

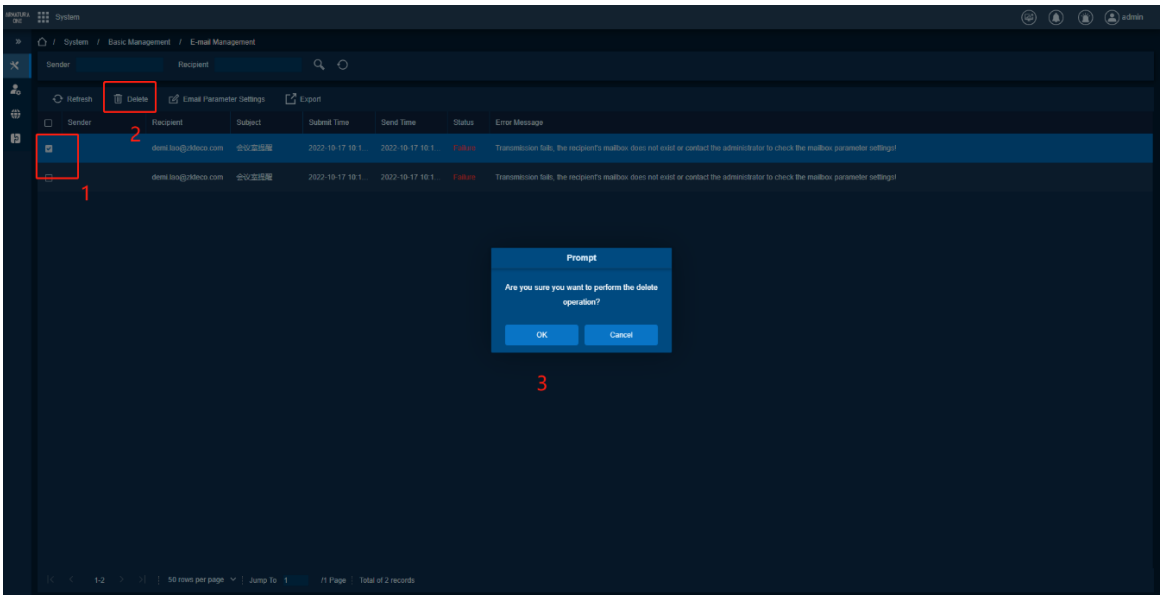
Feature Trigger Result

Delete the checked information.

Steps:

- Select the information that needs to be deleted.
- Click [**Delete**] button, and a prompt window will pop up.

- Click [**OK**] in the prompt window to complete the delete operation.



Email Parameters Setting

Preconditions for Normal Use of Function

The administrator has the mailbox parameters setting permission.

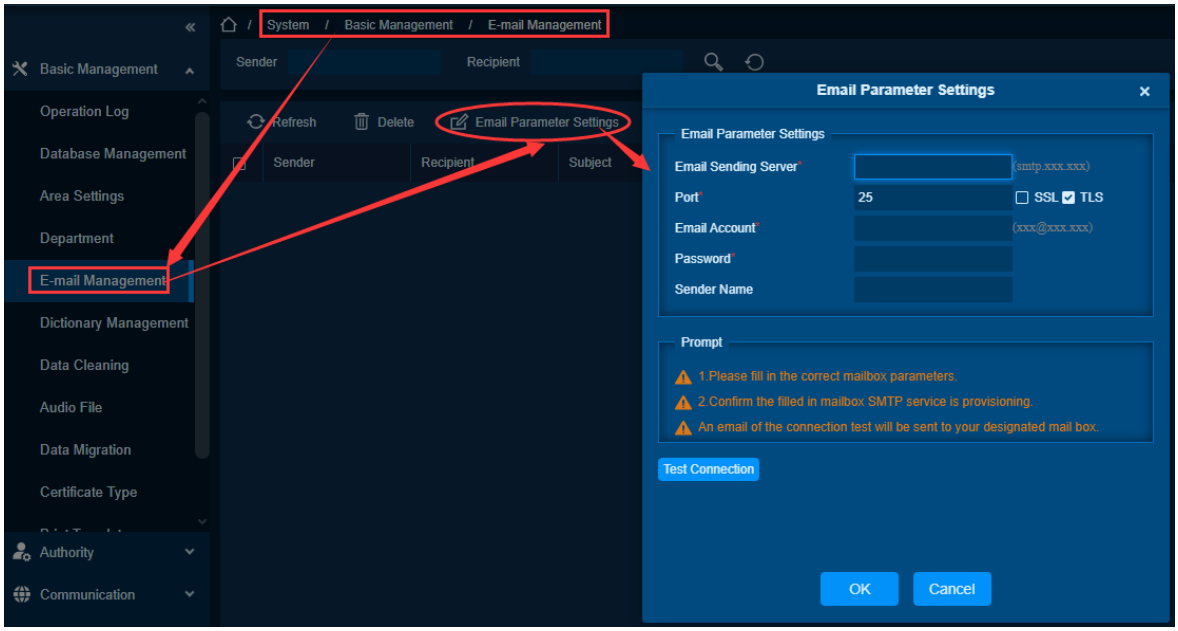
Function Usage Scenarios

When you want to send mail, you must first set the mailbox parameters before you can send the mail successfully.

Feature Trigger Result

After the configuration is successful, the send mail function can be used.

Steps:



- Click [**Email Parameter Settings**], and a pop-up window will pop up.
- Fill in the relevant parameters. Items marked with * are required.
- After filling in the information, click the [**Test Connection**] button. If successful appears, it means the setting is successful, and a test email will be sent to the set email address.
- Click [**OK**] to complete the mailbox parameters setting operation.

The fields are explained as follows:

Email Sending Server: Set the email sending server address.

Port: Set the mail server port number

Email Account: The address of the sender's mailbox

Password: The password of the sender's email address

Sender Name: Set the name of the sender.

Export

Preconditions for Normal Use of Function

The administrator has the export function authority.

Function Usage Scenarios

It is used when it is necessary to export the mail information on the software to the computer for operation.

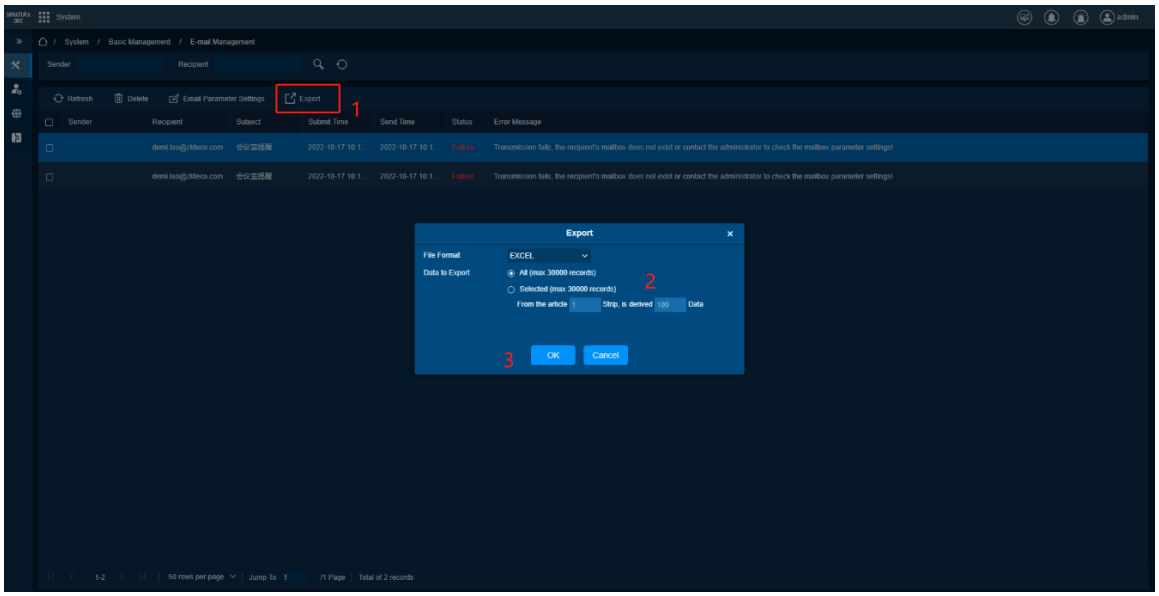
Feature Trigger Result

Operations	Description
Select Excel	Export the mail information to EXCEL format

Select PDF	Export email information to PDF format
Select CSV	Export the email information to CSV format
Select all data	Export all data of the mail message
Select the amount of data export	Partial data of export mail information

Steps:

- Click [**Export**] button, a window will pop up.
- Select the File Format.
- Select the data range that needs to be exported.
- Click [**OK**] to complete the Export mail information operation.

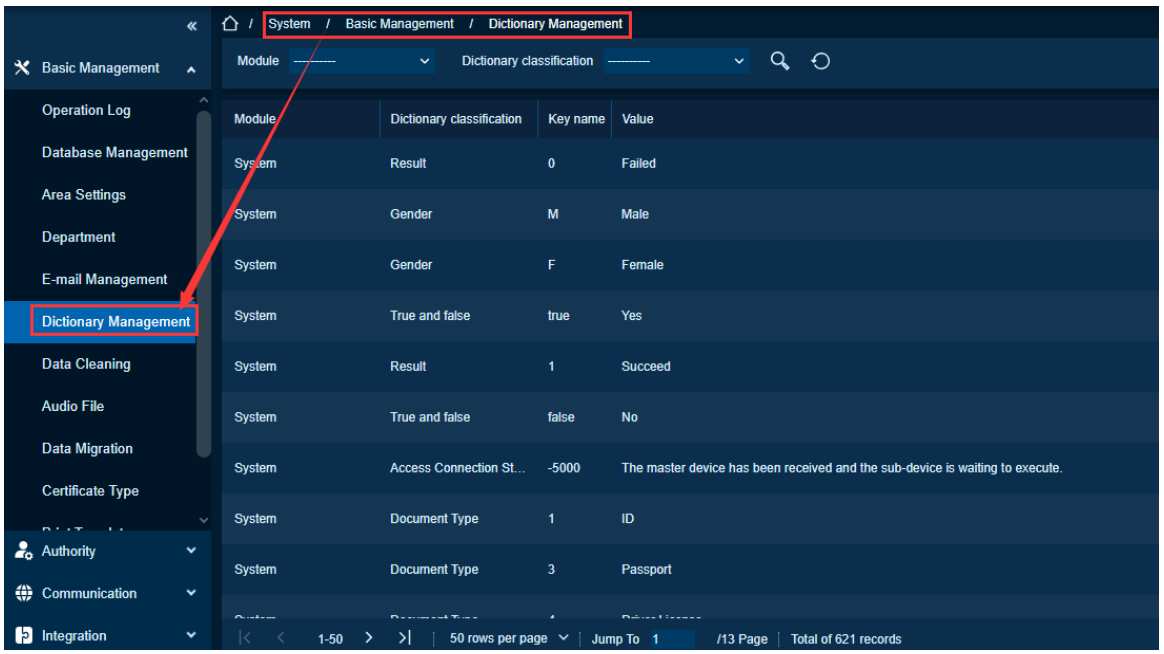


21.1.6. Data Dictionary

Function Description

Data dictionary management function, the user can find the meaning of the error code and self-check the software error.

Interface Display

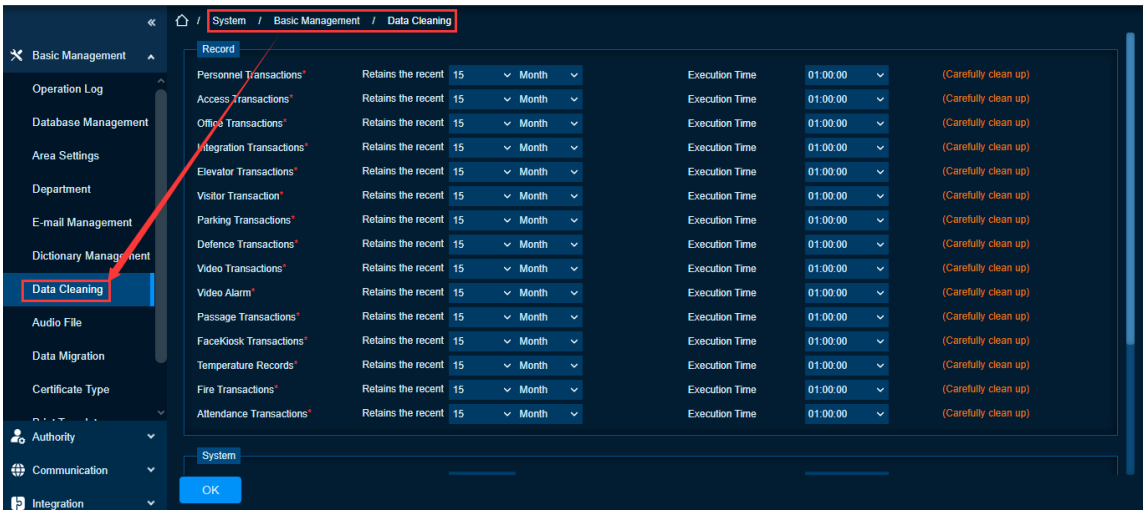


21.1.7. Data Cleaning

Function Description

Data cleaning is to save storage space and prevent the data stored by the server from being too large.

Interface Display



21.1.8. Audio File

Function Description

Audio file on the management software, used for the access control module or sent to the corresponding Device to provide voice support.

Add

Preconditions for Normal Use of Function

The administrator has the add function authority, and the file format selected during add must be MP3 or WAV format.

Function Usage Scenarios

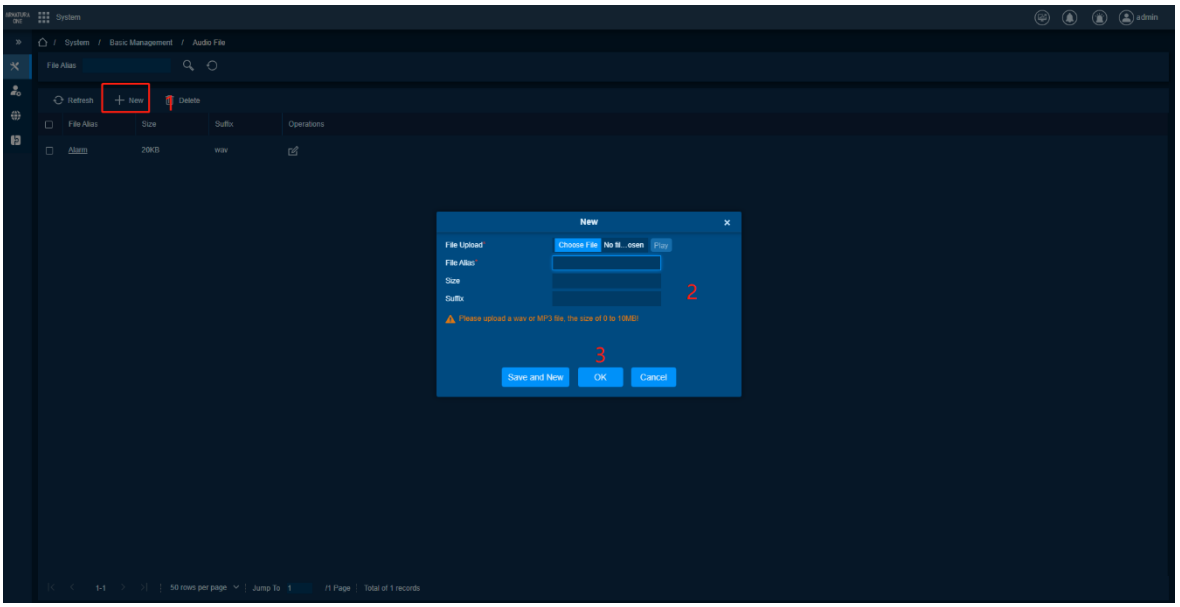
Use when you need to add voice prompts to Device or access control module.

Feature Trigger Result

Add audio file.

Steps:

- Click [**New**] button to pop up a window.
- Fill in the relevant information, the items marked with * are required.
- Click [**OK**] button to complete the add operation.



The fields are explained as follows:

File Upload: Select the audio file to be uploaded.

File Alias: Set the file name.

Size: Set the file size.

Suffix: Set the file suffix.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function authority, and there are data that can be deleted in the list (except the initialization data), and the data that needs to be deleted is not used by other modules.

Function Usage Scenarios

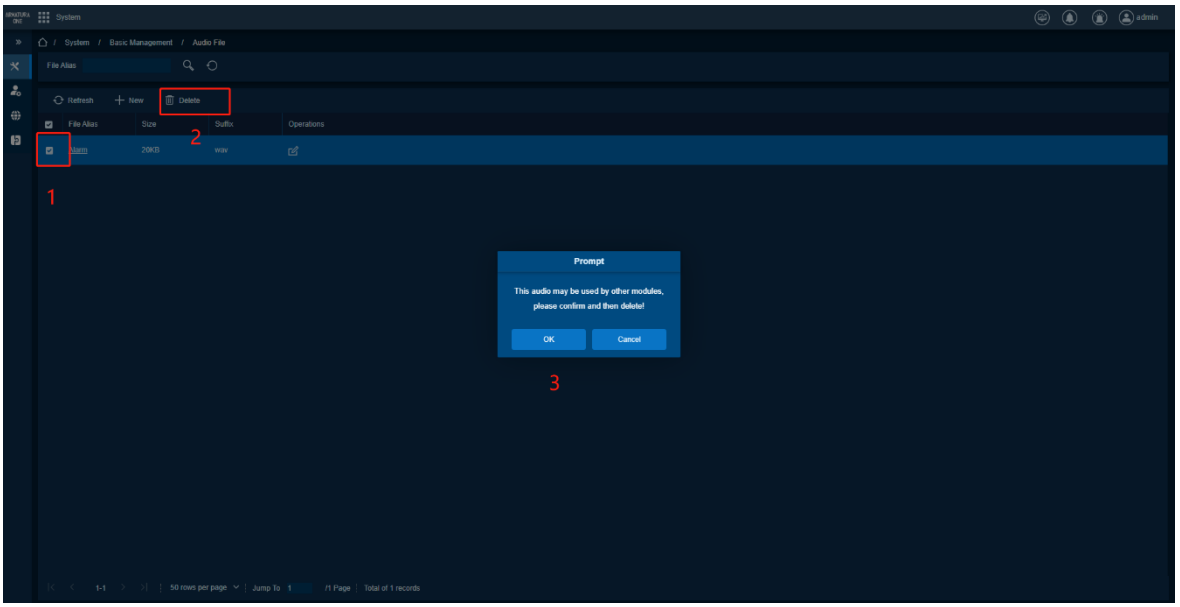
When there are redundant or unused audio file in the list, you can use the delete function to delete.

Feature Trigger Result

Delete the checked audio file.

Steps:

- Check the audio File that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] to complete the delete audio File operation.



21.1.9. Data Migration

Function Description

When the software is upgraded from the old version to the new version, the old version of data can be transferred to the new version.

Preconditions for Normal Use of Function

The administrator has data migration permission.

Function Usage Scenarios

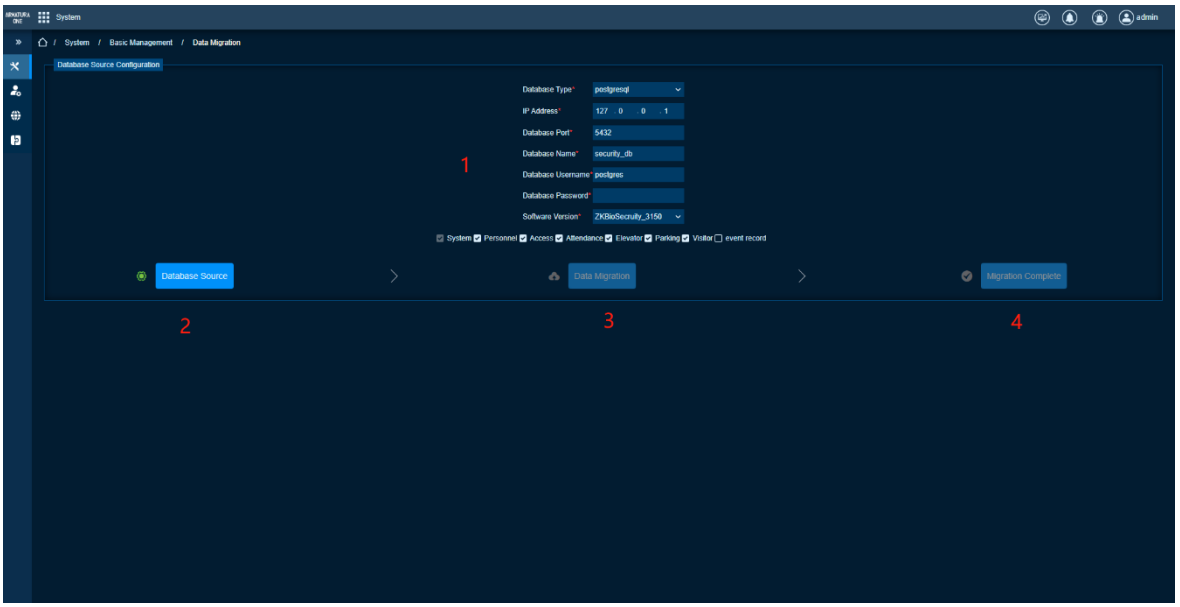
When the software is upgraded from the old version to the new version, the old version of data can be transferred to the new version.

Feature Trigger Result

The data is migrated to the set database.

Steps:

- Fill in the relevant information, all information is required,
- Click [**Database Source**] button.
- Click [**Data Migration**] button.
- Click [**Migration Complete**] button to migrate data.



The fields are explained as follows:

Database Type: Set the Database type.

IP Address: Set the Database IP address.

Database Post: Set the Database port number.

Database Name: Set the Database name.

Database Username: Set the Database username.

Database Password: Set the Database password.

Software Version: Set the Software version.

21.1.10. Certificate Type

Function Description

Type of certificate supported by the management system.

Add

Preconditions for Normal Use of Function

The administrator has the add type of certificate permission.

Function Usage Scenarios

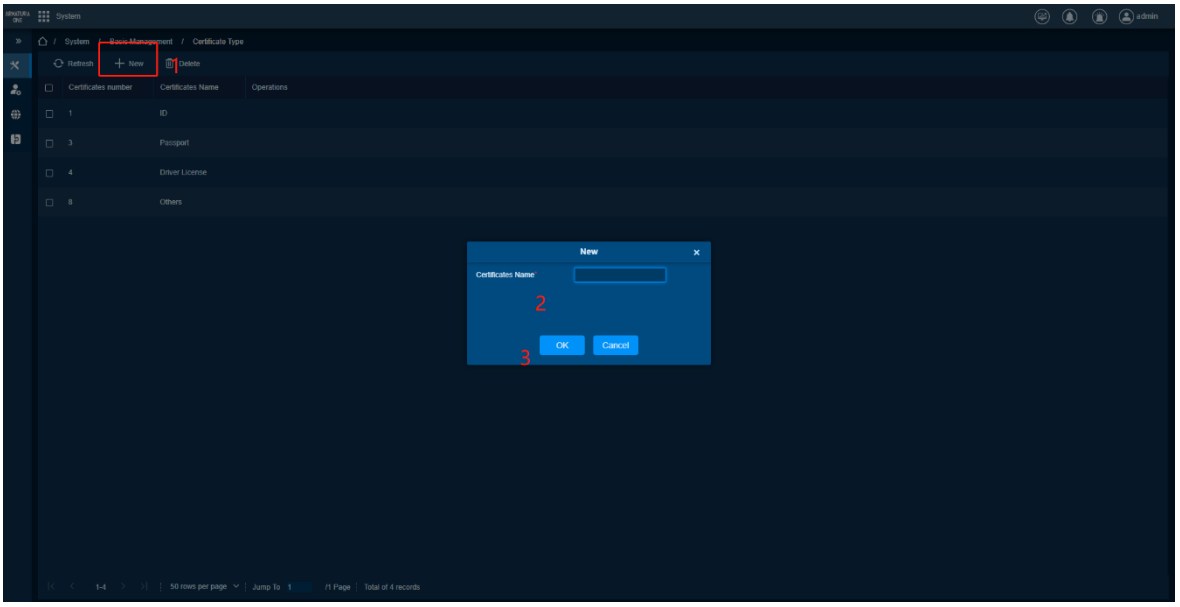
Use when you need to add a type of certificate to meet some specific conditions.

Feature Trigger Result

Add a type of certificate.

Steps:

- Click [**New**] button to pop up a window.
- Fill in the name of the type of certificate of add.
- Click [**OK**] button to complete add.



Delete

Preconditions for Normal Use of Function

The administrator has the delete type of certificate permission, and there are data in the list except for the initialization data.

Function Usage Scenarios

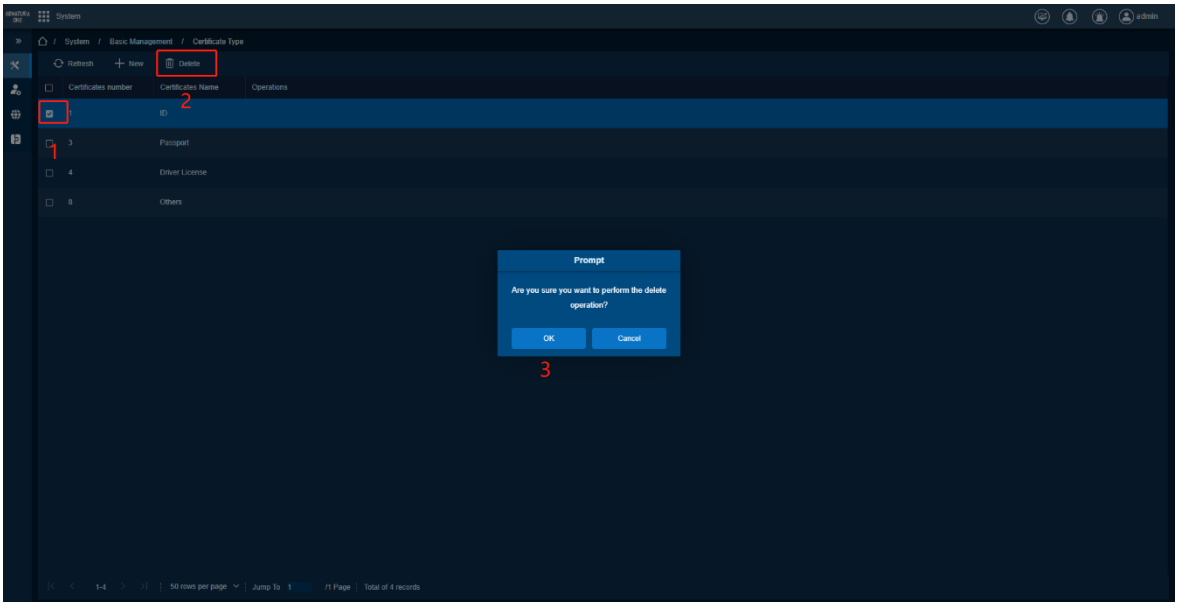
Use when you need to delete the extra type of certificate.

Feature Trigger Result

Delete type of certificate。

Steps:

- Check the type of certificate that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] in the prompt box to complete the delete type of certificate operation.



21.1.11. Print Template

Function Description

View and edit the employee card print template.

Add

Preconditions for Normal Use of Function

The administrator has the add print template permission.

Function Usage Scenarios

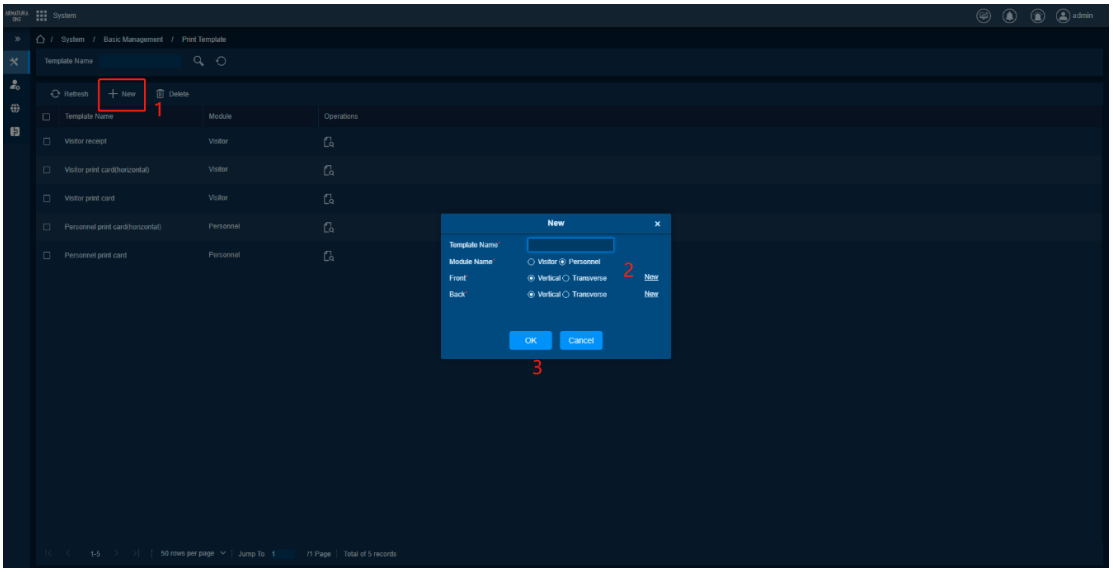
Use when you need to add a print template.

Feature Trigger Result

Add a print template.

Steps:

- Click [**New**] button a window will pop up.
- Fill the relevant information.
- Click [**OK**] to complete the add operation.



Delete

Preconditions for Normal Use of Function

The administrator has the delete print Template permission, and there are print templates that can be deleted in the list.

Function Usage Scenarios

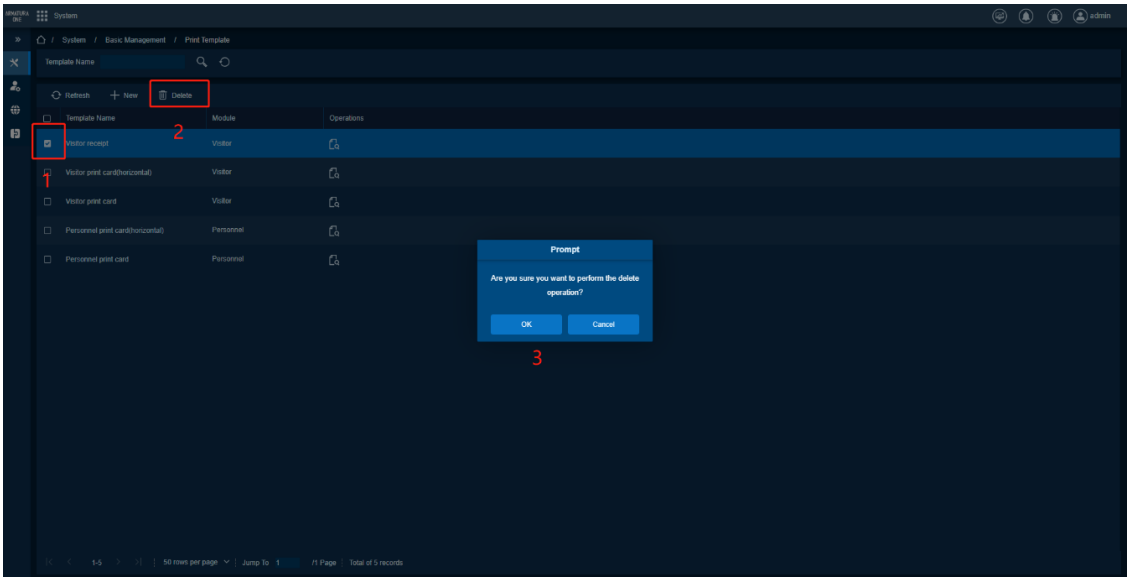
Delete redundant, unused print template.

Feature Trigger Result

Delete print template.

Steps:

- Select the Print Template that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete print template operation.

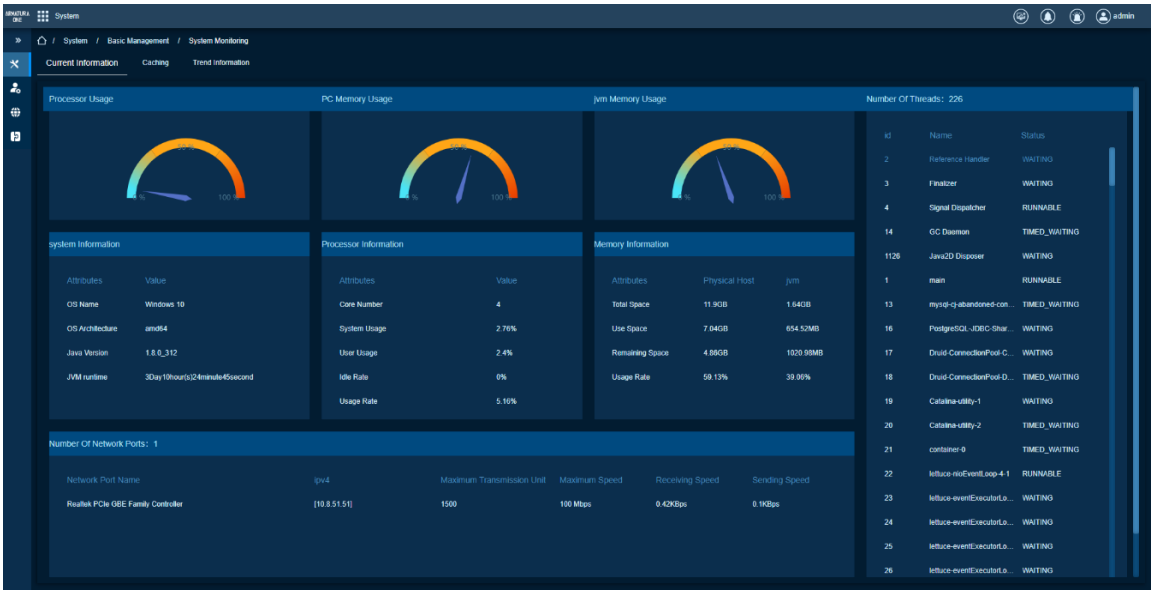


21.1.12. System Monitoring

Function Description

Check the server load usage.

Function Page Display



21.2. Authority Management

Use this function to manage your ARMATURA One system administrator account, use roles and permissions.

- Perform third-party API authorization management.

- Set the security configuration parameters of the system.

Function List

Operations	Description
User	Add, delete user in the system
Character	Add and delete character in the system and edit permission of character
API Authorization	Add, delete, browse API
Client Authorization	Add, reset, delete client Authorization
Security Settings	Set system security properties

21.2.1. User

Function Description

Add a new user in the system and set the level for this user.

Add

Preconditions for Normal Use of Function

The administrator has the add user permission, and the username of Add must be unique.

Function Usage Scenarios

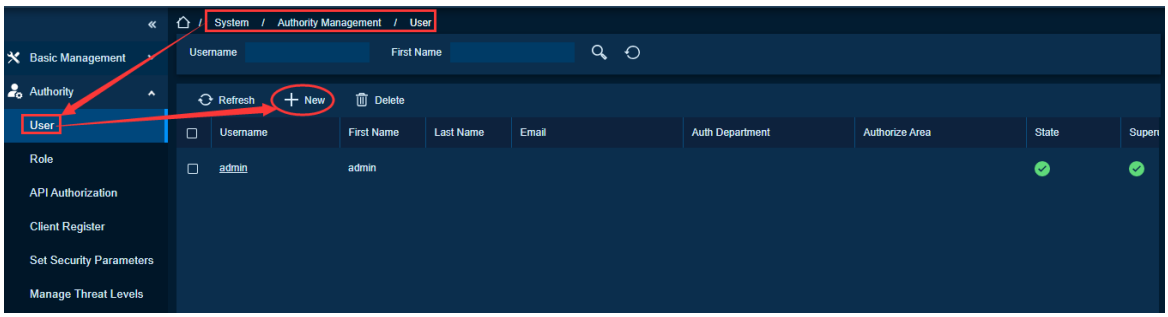
Used for adding user to the system.

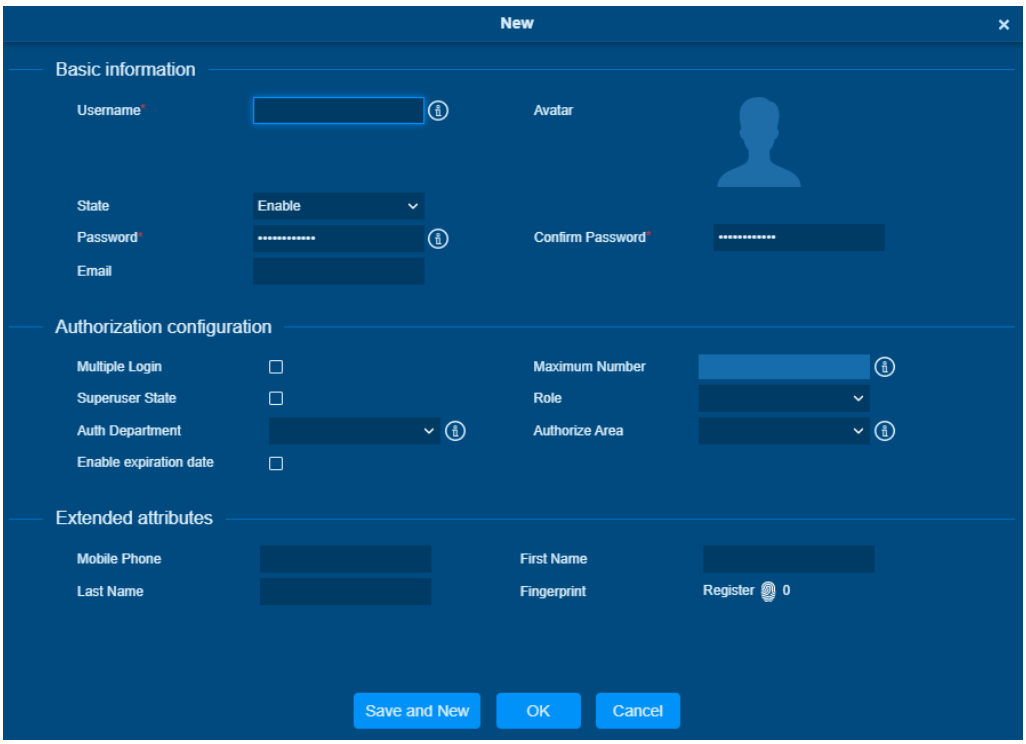
Feature Trigger Result

Add user to the system.

Steps:

- Click [**New**] button, and the add window will pop up.





- Fill in the relevant information, the items marked with * are required, and the fields are explained as follows:

Avatar: Set user avatar, click on the avatar to browse, and select the avatar.

Username: Set the username.

Password: Set the user password, the default is **Changeme_123**

Confirm Password: Confirm the set password again.

State: Set the state of the user.

Email: Set the user mailbox, user could use this email to reset password.

Multiple Login: After selecting, you can set the number of User logins at the same time.

Maximum Number: Limit the number of users who log in at the same time.

Superuser State: Super User State, when checked, the user is a super administrator.

Role: Set the character of the user.

Auth Department: Set the authorization department of the user.

Authorize Area: Set the authorization area of the user.

Enable expiration date: Set account expiration date, and the user will be expired and cannot login after the time period you selected.

Mobile Phone: Set the user mobile phone number.

First Name: Fill in the name of the user.

Last Name: Fill in the last name of the user.

Fingerprint: Click [**Registration**] to register the user fingerprint.

- Click [OK] to complete the add user operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there are data that can be deleted in the list (except the initialization data)

Function Usage Scenarios

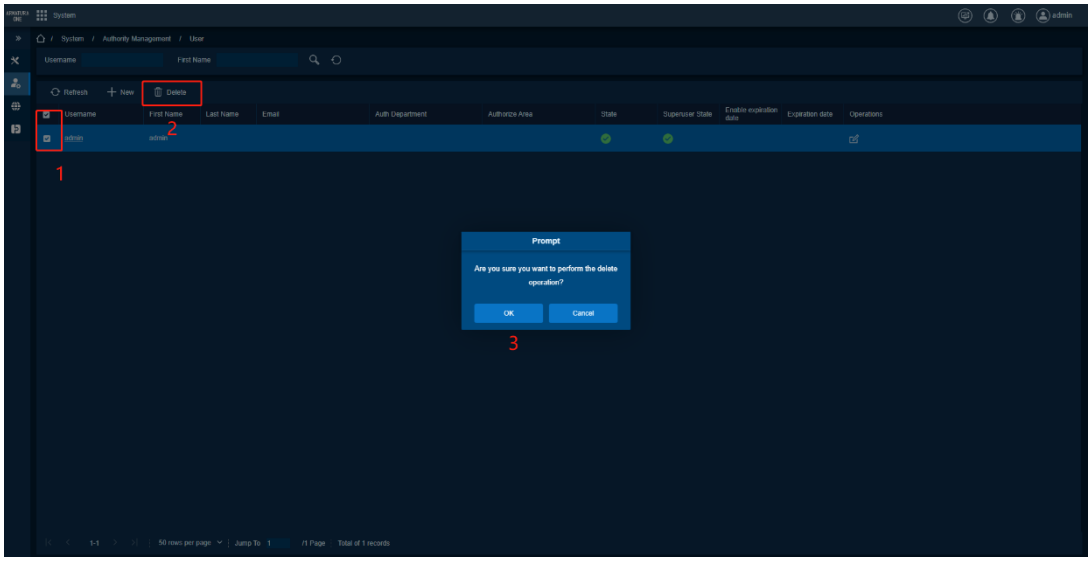
Delete redundant, unused, and invalid users.

Feature Trigger Result

Delete the checked user.

Steps:

- Select the user who needs to delete.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete user operation.



21.2.2. Character

Function Description

Add and delete character in the system and edit permission of character.

Add

Preconditions for Normal Use of Function

The administrator has the add character permission, and the add character number must be unique.

Function Usage Scenarios

It is used when the Character in the current list cannot meet some conditions.

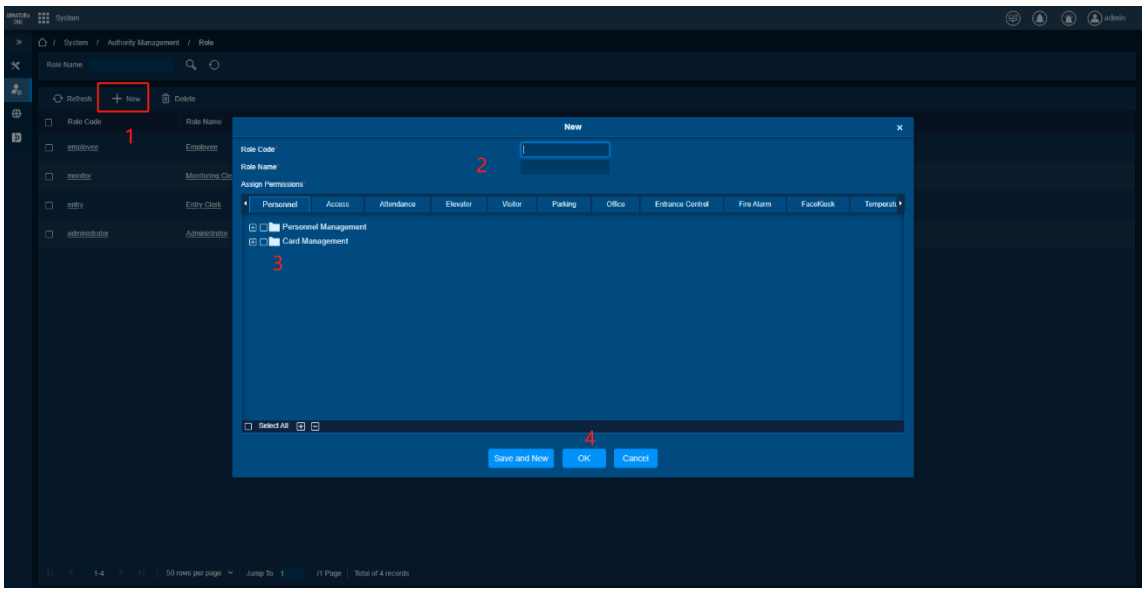
Feature Trigger Result

Add a character.

Step:

- Click [**New**] button, and the add window will pop up.

Fill in the relevant information, all information is required, the fields are explained as follows:



Role Code: Set the number of the character.

Role Name: Set the name you think.

- Assign permissions, check the required permissions, and assign permissions to character.
- Click [**OK**] to complete the add character operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete character permission, and there are characters that can be deleted in the list (except for initializing the character).

Function Usage Scenarios

Delete redundant and unnecessary characters.

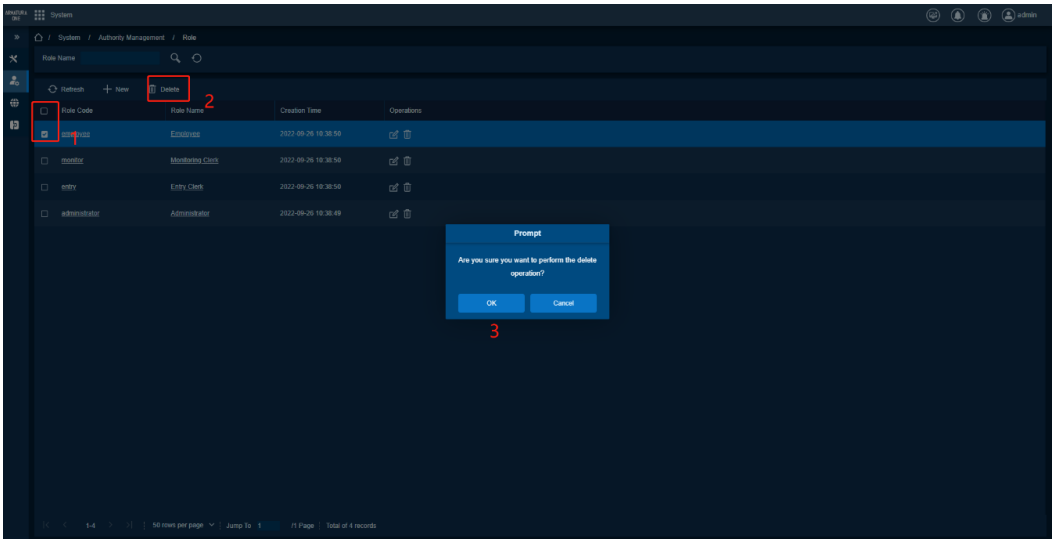
Feature Trigger Result

Delete the selected character.

Steps:

- Select the character that needs to be deleted.

- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete character operation.



21.2.3. API authorization

Function Description

Add, delete, browse API.

Add

Preconditions for Normal Use of Function

The administrator has the add API permission, and API authorization is activated within the license.

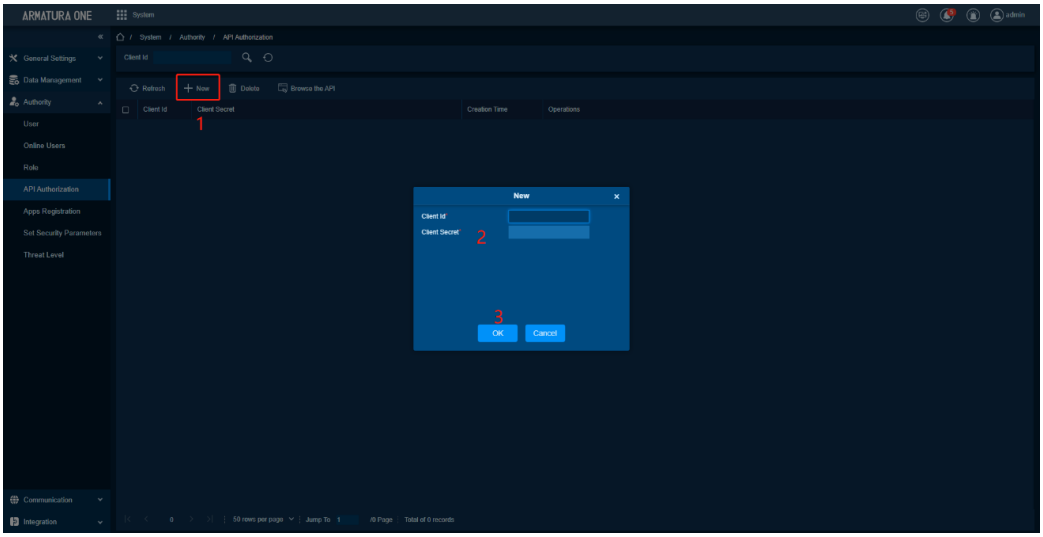
Function Usage Scenarios

Use when you need to add a new API authorization.

Feature Trigger Result

Add API authorization.

Steps:



- Click [**New**] button, and the add window will pop up.
- Fill in the relevant information. All fields are required. Field descriptions are as follows:

Client ID: Enter the client ID.

Client Secret: The client secret automatically generated based on the client ID.

- Click [**OK**] to complete the add operation.

Delete

Preconditions for Normal Use of Function

The administrator has the delete permission, and there is information that can be deleted in the list.

Function Usage Scenarios

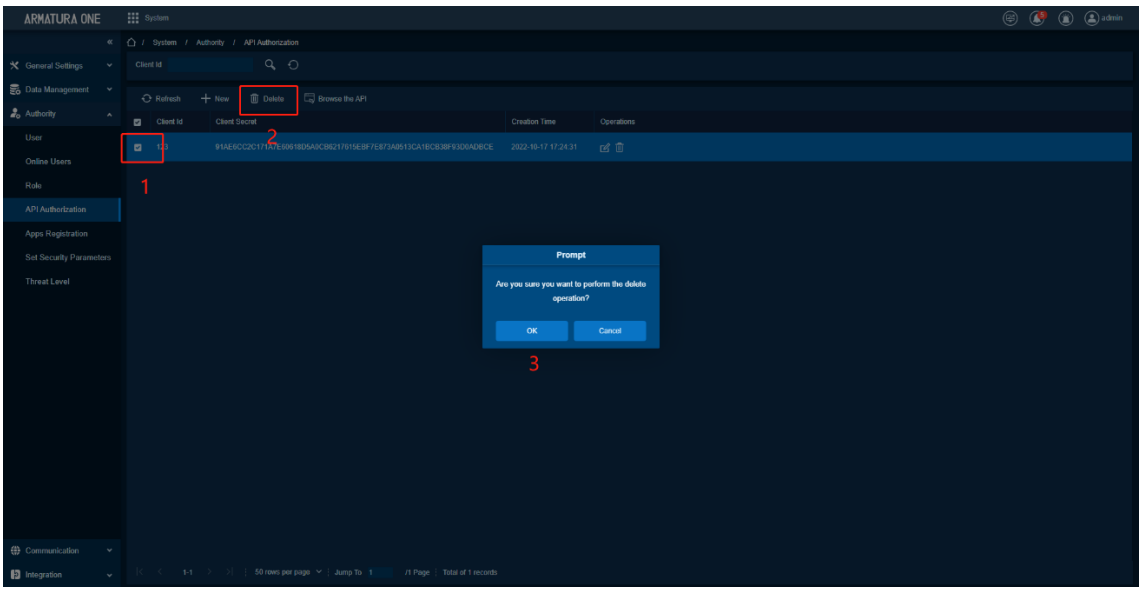
Delete redundant and invalid client API.

Feature Trigger Result

Delete the checked API.

Steps:

- Select the information that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the operation.



Browse API

Preconditions for Normal Use of Function

The administrator has the permission to browse the API, and there are client API data in the list.

Function Usage Scenarios

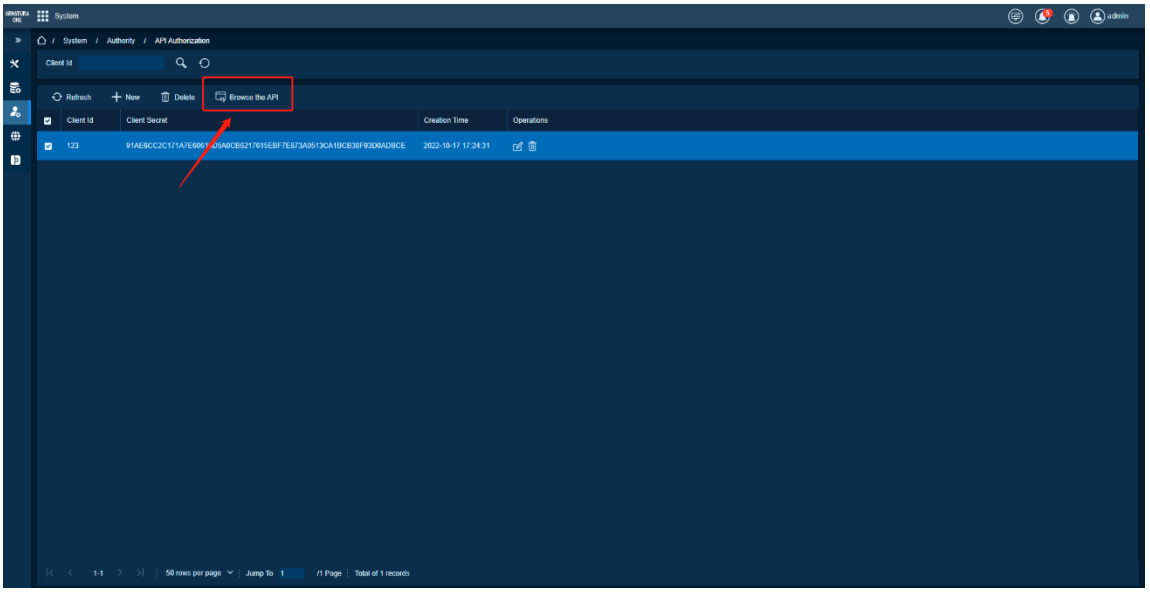
When you need to know the API interface on the software, you can browse the API.

Feature Trigger Result

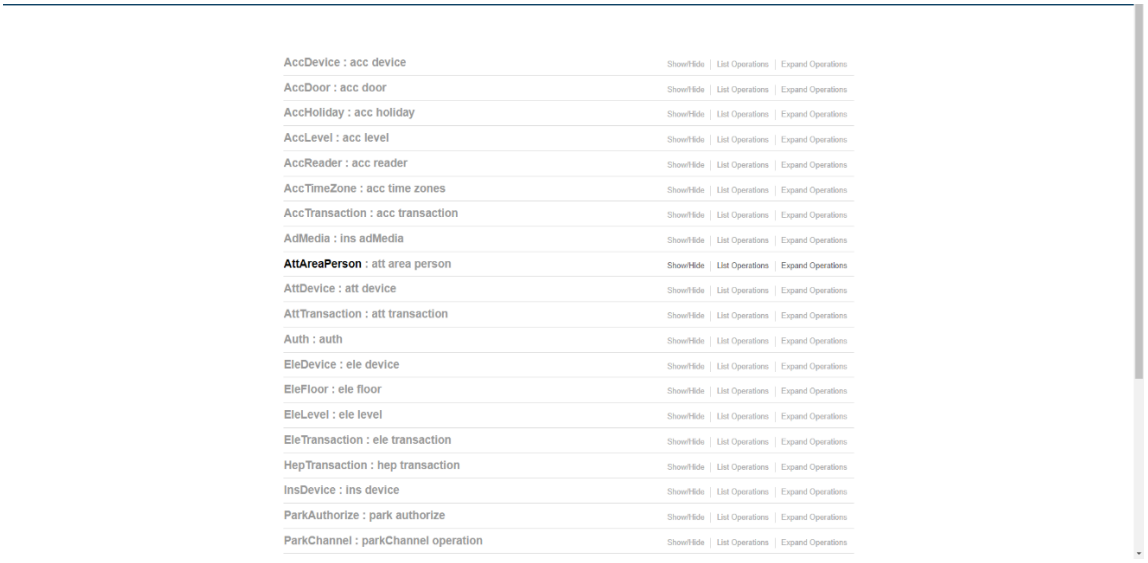
Browse the API on the software.

Steps:

- Click [**Browse the API**].



Click on the page to be redirected and the API of the module to be found.



21.2.4. Client Authorization

Function Description

You can add client types to the system and generate registration codes for the client registration of each module function. The number of customers allowed is controlled by the number of allowed points.

Add

Preconditions for Normal Use of Function

The administrator has the add client authorization permission, and there are module points that can be used in the license.

Function Usage Scenarios

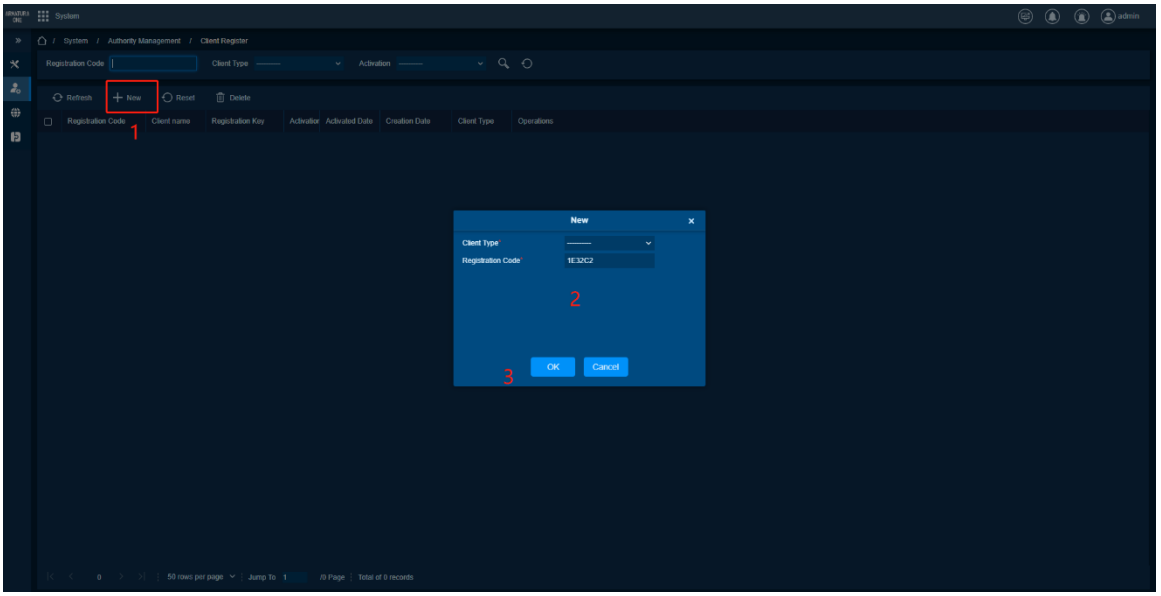
To use module functions normally, the corresponding device needs to be added.

Feature Trigger Result

Add client authorization.

Steps:

- Click [**New**] button, and the Add window will pop up.
- Select the client type to be added.
- Click [**OK**] to complete the add operation.



Reset

Preconditions for Normal Use of Function

The administrator has the reset function authority.

Function Usage Scenarios

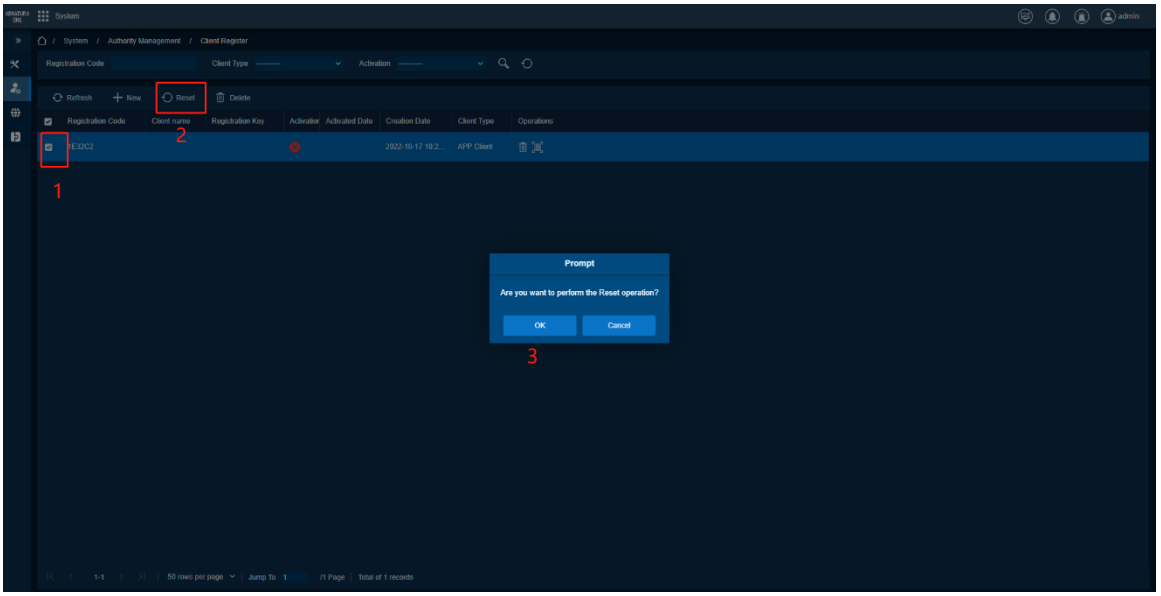
To be used when the client is reset.

Feature Trigger Result

Reset the selected client.

Steps:

- Select the clients that need to be reset.
- Click [**Reset**] button, a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the reset operation.



Delete

Preconditions for Normal Use of Function

The administrator has the delete client permission.

Function Usage Scenarios

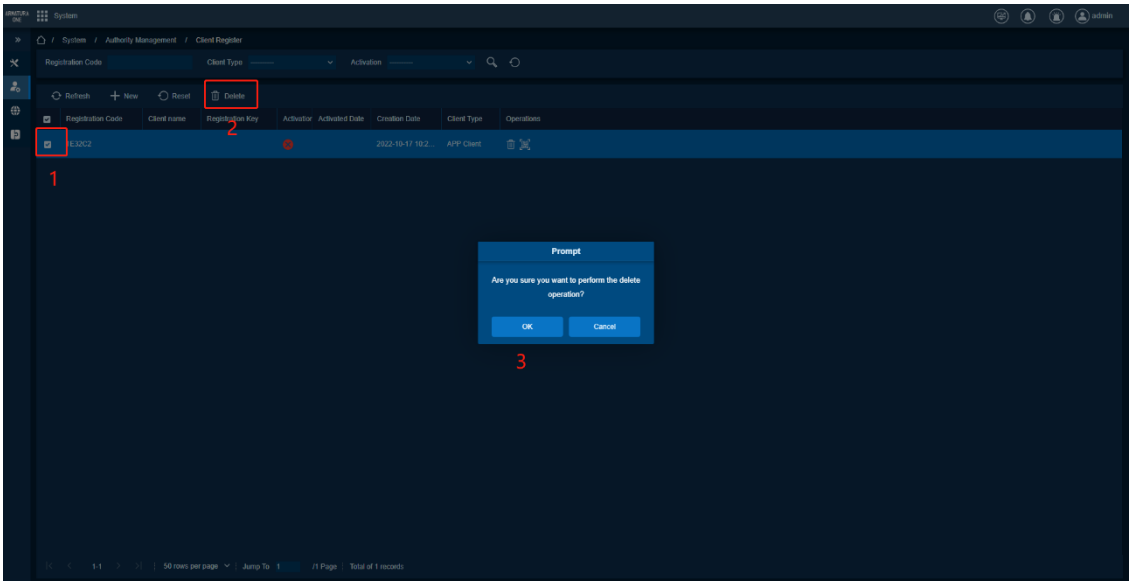
You can delete the client when it is not needed, or the client is redundant.

Feature Trigger Result

Delete the selected client.

Steps:

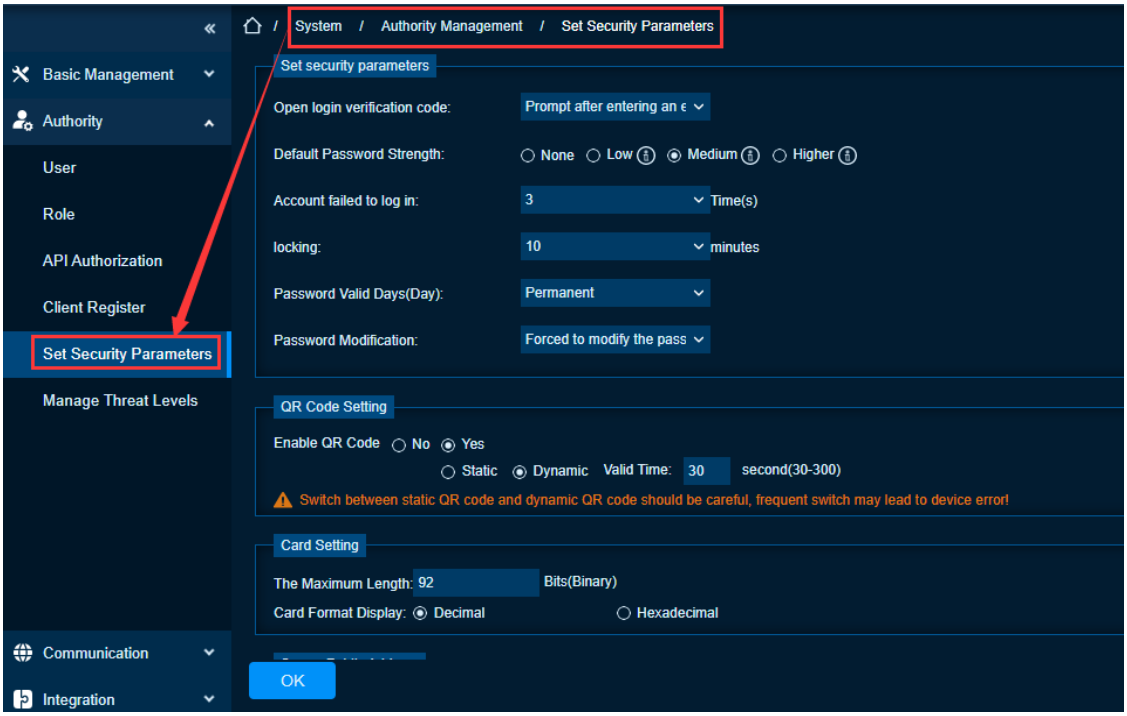
- Select the client that needs delete.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the delete client operation.



21.2.5. Security Settings

Function Description

Set the security attributes of the login system.



Field Description

Open login verification code： Login verification code settings, you can set the method of opening the verification code when logging in.

Default Password Strength： Set the minimum strength of the password.

Account failed to log in： Lock after setting the maximum number of failed logins attempt for User.

Locking： Set the login lock event.

Password Valid Days (Day)： Set the password validity period.

Password Modification： Set the initial password modification strategy.

Enable QR Code： Set whether to turn on the QR code, and whether the QR code is static or dynamic after it turns on.

Maximum Card Length: Set the maximum length (binary number) of the Card number that the current system will support.

Card Format: Set the card format currently used in the system. The card format cannot switch once it is set up.

21.2.6. Threat Level

Preconditions for Normal Use of Function

Need to set **Personnel Threat Level** and **Access Level Threat Level** first.

Set Personnel Threat Level

Set Access Level Threat Level

Function Usage Scenarios

Threat Level is a restricted access control for specific scenarios, such as Threat, Rob, Fire …

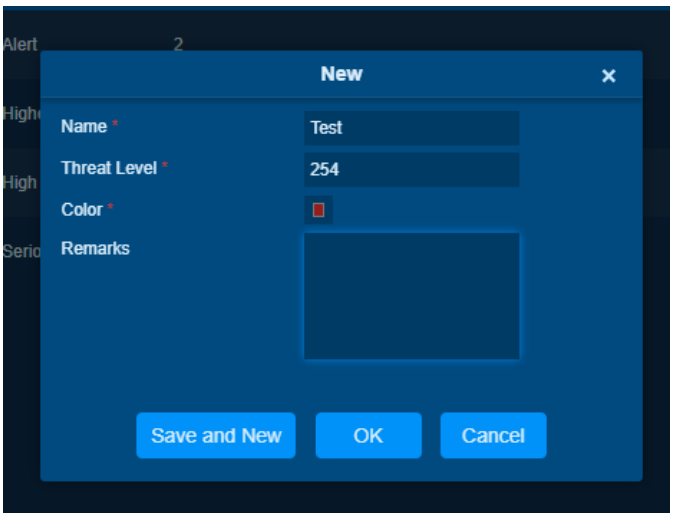
Admin will design some threat level for person and doors.

Feature Trigger Result

Delete the selected client.

Steps:

Add Threat Level

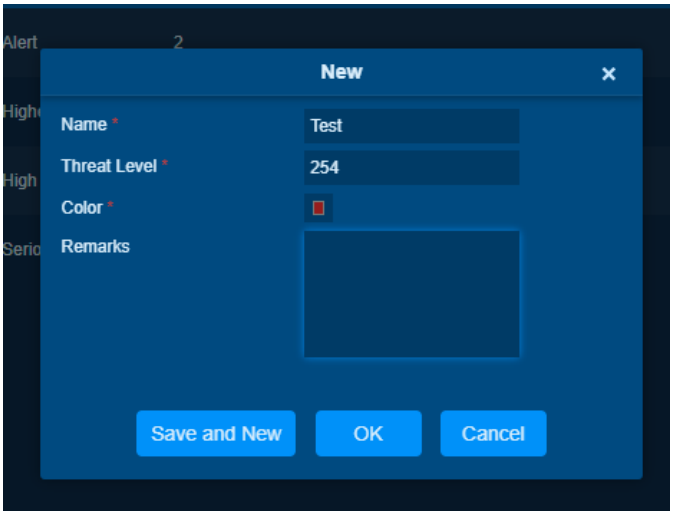


Name: Name for clarify which level it is

Threat Level: Code for threat level, range from 1 to 254

Color: Support all color

Edit Threat Level

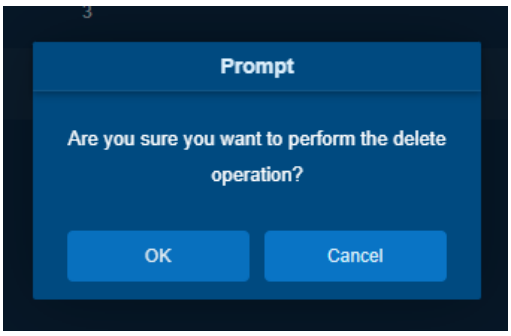


Name: Name for clarify which level it is

Threat Level: This code is not allowed to change when edit.

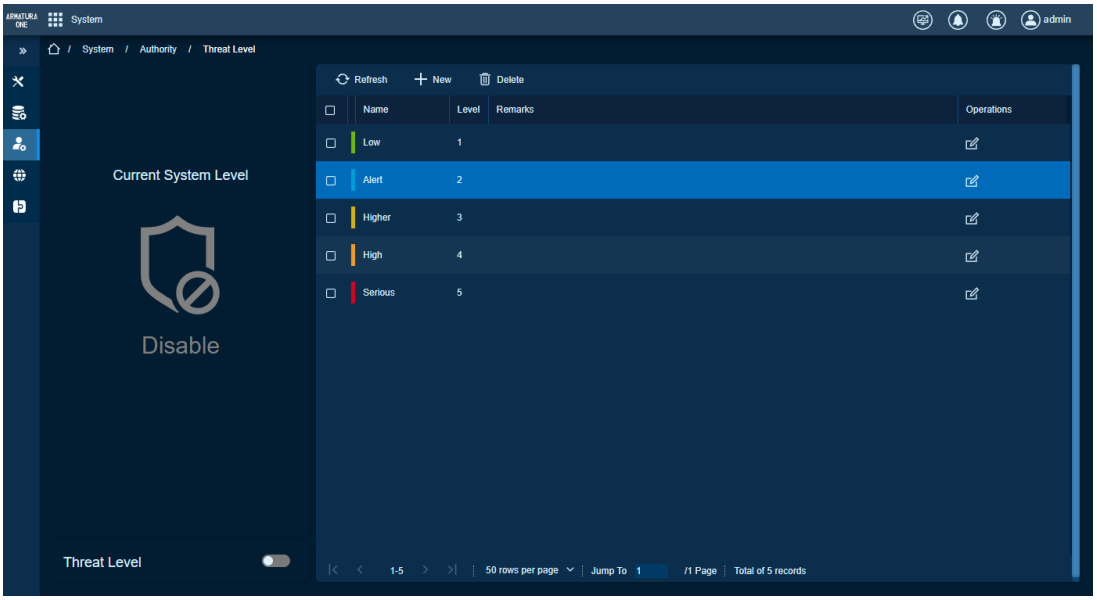
Color: Support all color

Delete Threat Level



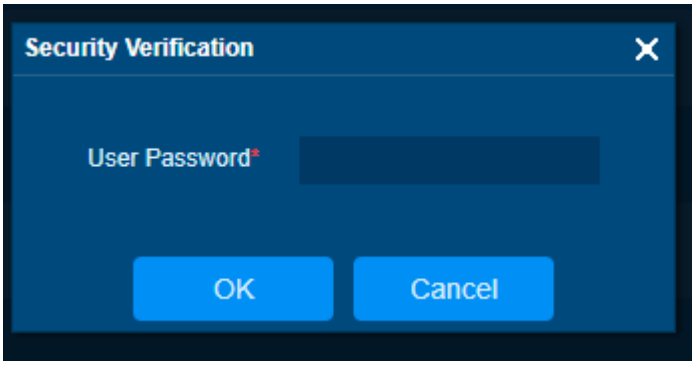
Switch Threat Level

- Visit **[System] -> [Authority Management] -> [Manage Threat Levels]**

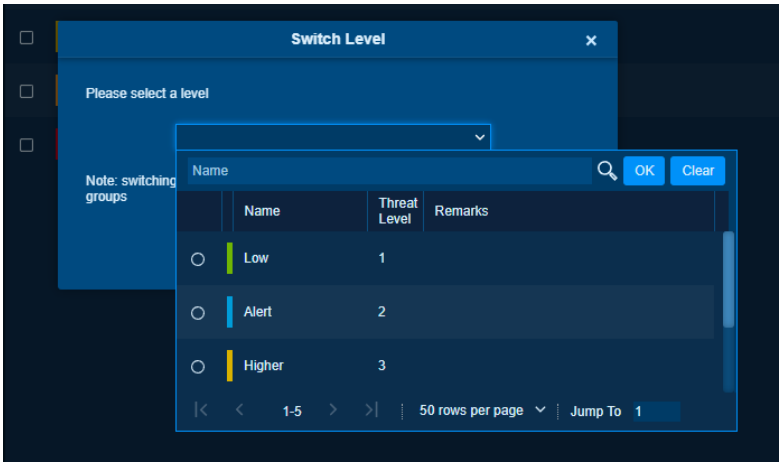


- Enable **Threat Level**

- Security Verification



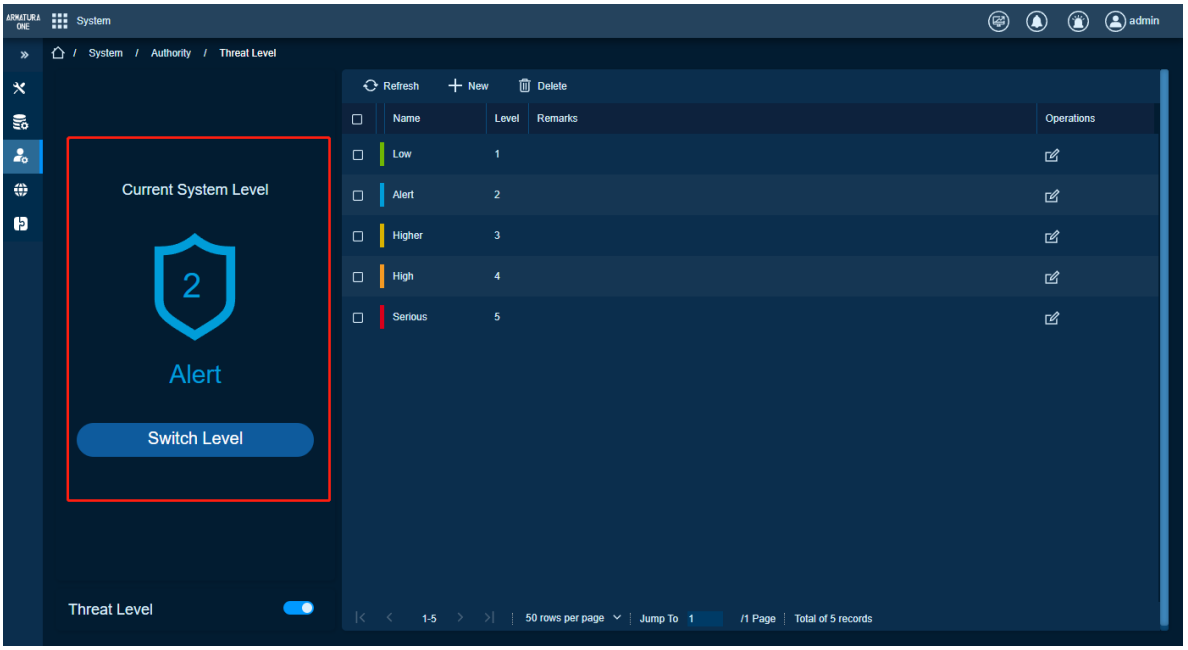
- Switch **System Threat Level**



✍**Note:**

Switching system threat level may result in invalidation of some users and access groups

After selected, system threat level will show on left



21.3. Communication

View the communication commands of software and hardware devices, view the list of communication devices, and monitor the communication port and network status.

Function List

Operations	Description
Device Commands	Clear, export server issued command

Communication Device	View authorized device
Communication Monitoring	Set up ADMS communication

21.3.1. Device Commands

Function Description

Record all operations performed on the software.

Preconditions for Normal Use of Function

The administrator has the authority to clear the command table and there is data in the table.

Function Usage Scenarios

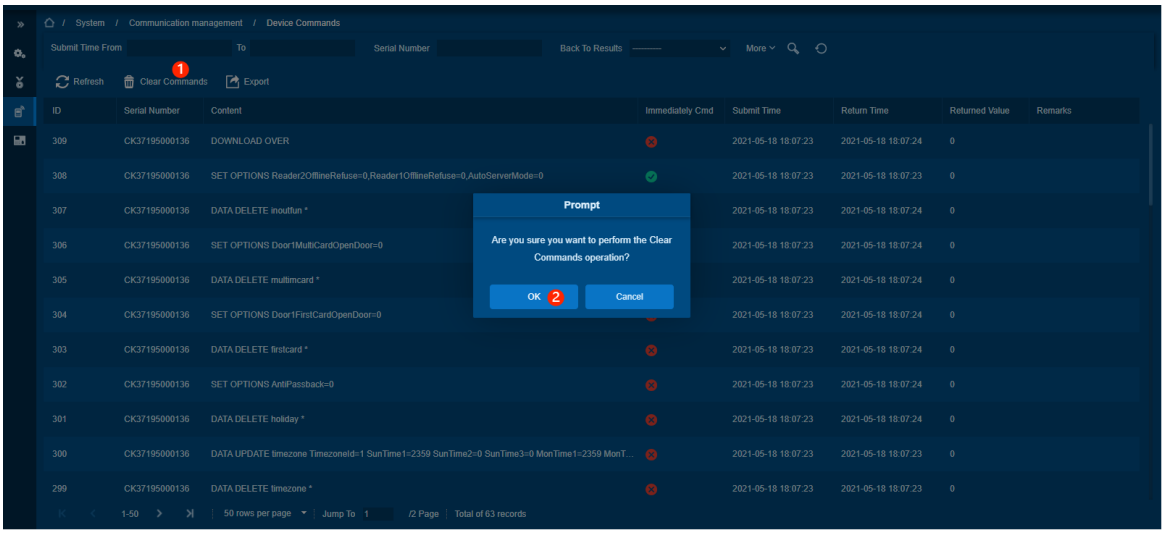
It used when there is too much data in the table.

Feature Trigger Result

Delete all data in the table.

Steps:

- Click [**Clear Commands**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the operation of clearing the command list.



Export

Preconditions for Normal Use of Function

The administrator has the export function authority.

Function Usage Scenarios

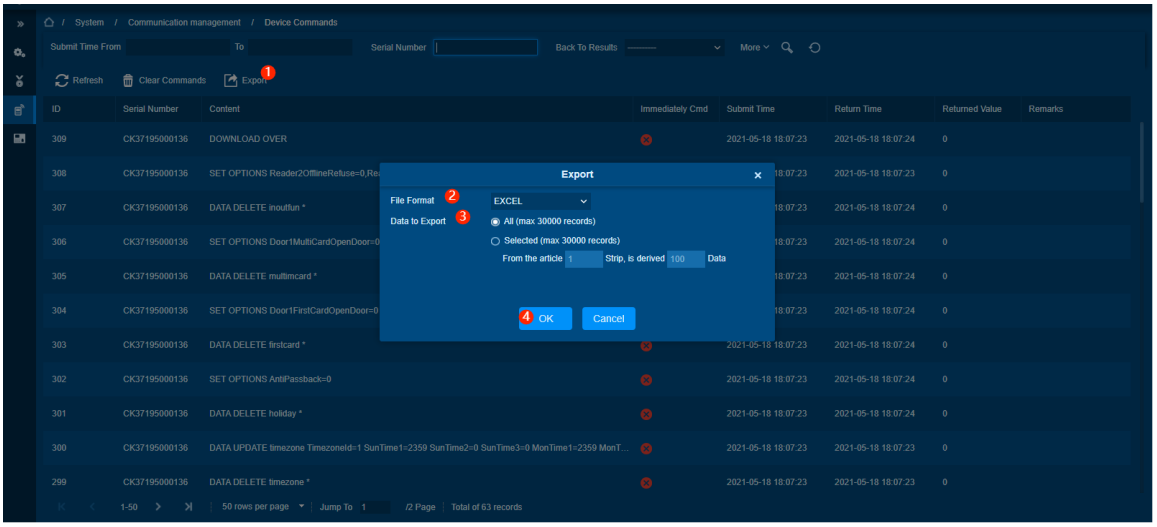
Export the data on the software to the computer.

Feature Trigger Result

Operations	Description
Select Excel	Exported document format is Excel
Select PDF	Exported document format is PDF
Select CSV	Exported document format is CSV
Select All	Export all log information
Select Selected	Export log information within a certain range

Steps:

- Click [**Export**] button, a window will pop up.
- Select the file format.
- Select the data range that needs to be exported.
- Click [**OK**] to complete the export operation.



21.3.2. Communication Device

Function Description

Check the authorized device.

Preconditions for Normal Use of Function

The administrator has the permission to view authorized devices.

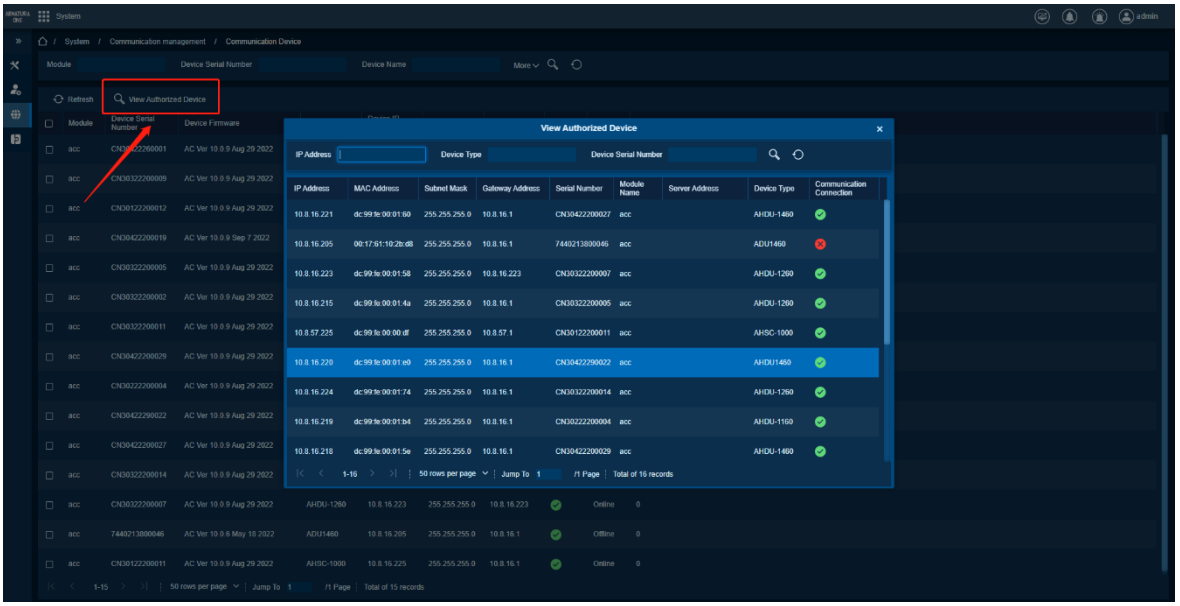
Function Usage Scenarios

View authorized device.

Feature Trigger Result

View authorized device.

Click [**View Authorized Device**] button, and you can view the authorized device in the pop-up list.



21.3.3. Communication Monitoring

Function Description

Check the ADMS communication port of the current server, and check whether the server's Internet connection is normal.

Preconditions for Normal Use of Function

The administrator has the permission to view ADMS communication port.

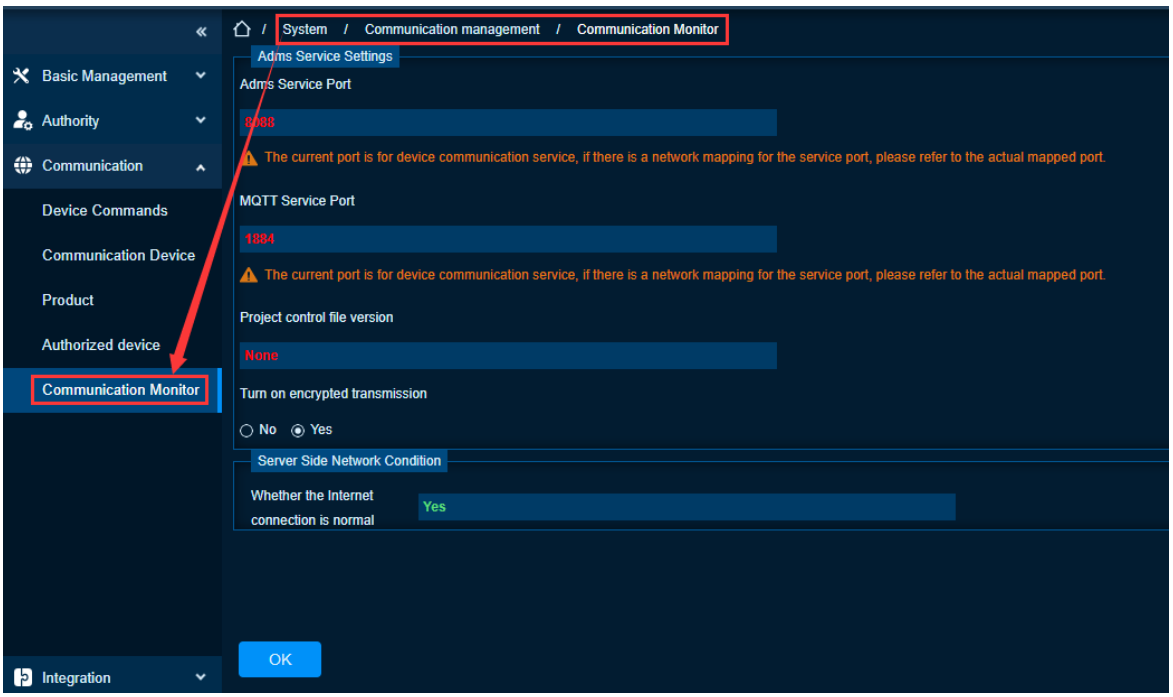
Function Usage Scenarios

View ADMS communication port.

Feature Trigger Result

View ADMS communication port.

Click [**Communication Monitoring**] to access the following page:



Field Description

ADMS Service Port: View the service port number of ADMS.

Whether the Internet connection is normal: Check whether the current Internet link is normal.

21.4. Integration

To manage the docking configuration between ARMATURA One and third-party systems. Enable and monitor third-party docking platforms.

- View the content of messages sent by the system.
- Query the content of the message notification in the system.
- Docking with Microsoft AD system.

Function List

Operations	Description
Platform Connections	Add, enable, disable platform
Message Management	Delete, export message
System Message	View export system message
AD Management	You can access shared personnel data

21.4.1. Platform Connection

Function Description

Add a platform to cooperate with the software.

Add

Preconditions for Normal Use of Function

The administrator has the add permission, and the license can have the license points of the corresponding module.

Function Usage Scenarios

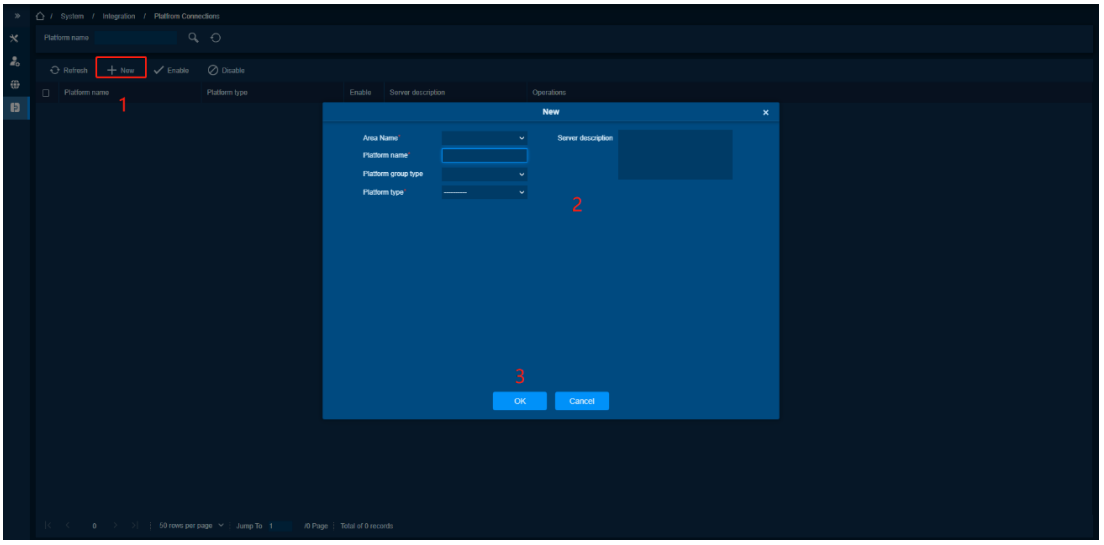
When a function needs to be used on other platforms, it can be added.

Feature Trigger Result

Add a platform.

Steps:

- Click [**New**] button, and the Add window will pop up.



- Fill in and select relevant information.

The field descriptions are as follows:

Parameter	How to set
Area Name	Select the area name.
Platform Name	Set the name of the platform
Platform Group Type	Select the platform group type
Platform Type	Select the platform type.
Server Description	Add server description

- Click **[OK]** to complete the Add operation.

Add Zoom Platform

Preconditions for Normal Use of Function

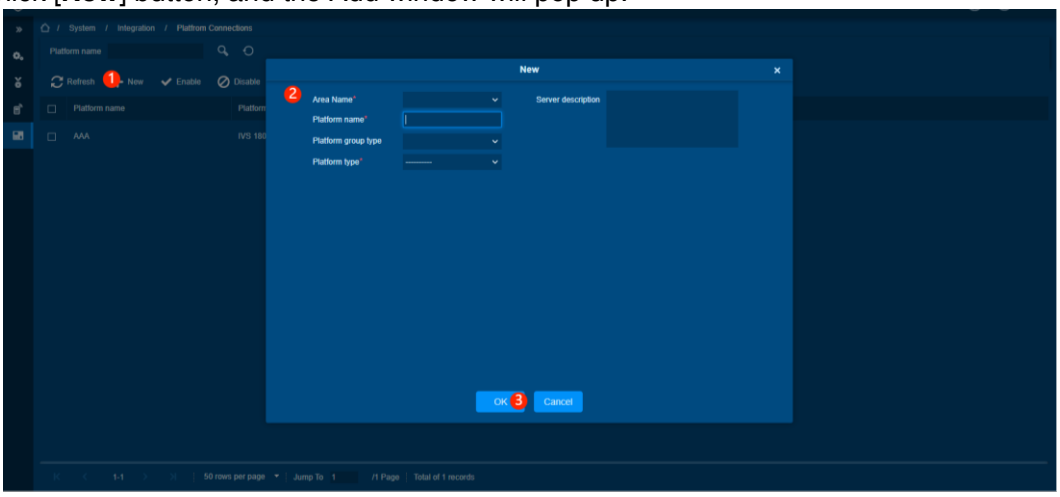
The administrator must organize an online meeting.

Function Usage Scenarios

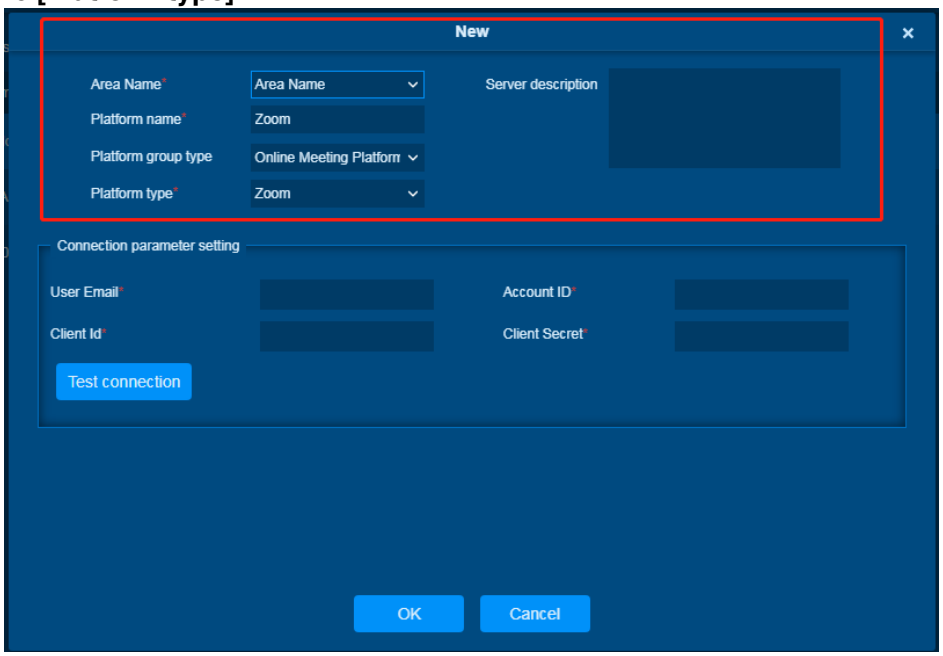
It is used to reduce the meeting costs and increase work efficiencies.

Steps:

1. Click [**New**] button, and the Add window will pop up.

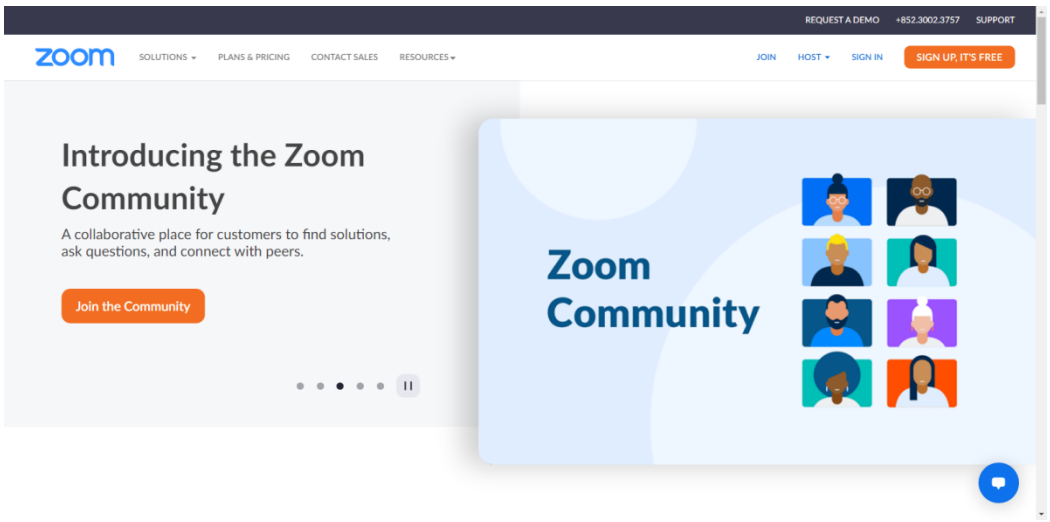


2. Fill in the information and select **[Online Meeting Platform]** in the **[Platform group type]**, then choose the **[Zoom]** in the **[Platform type]**.

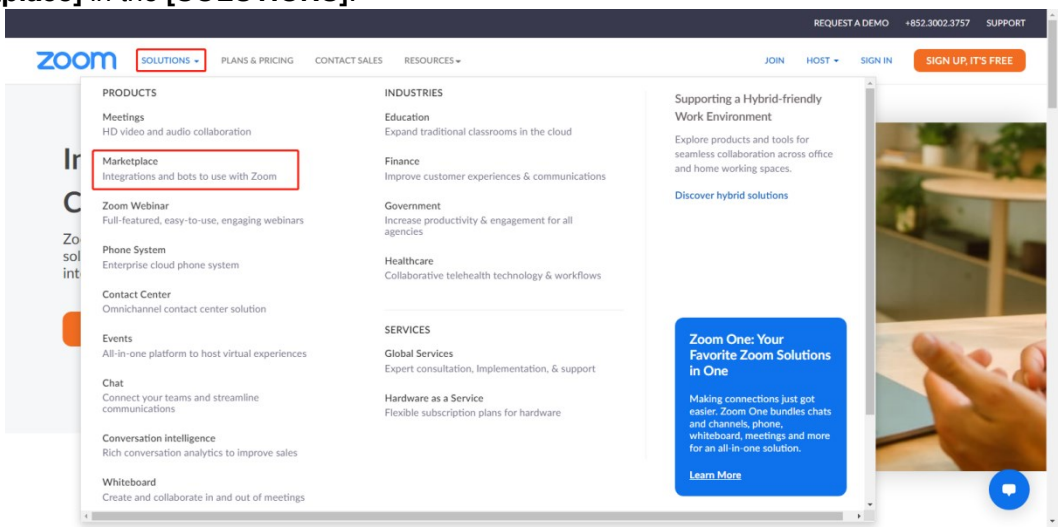


3. Configure the connection parameter setting as follows:

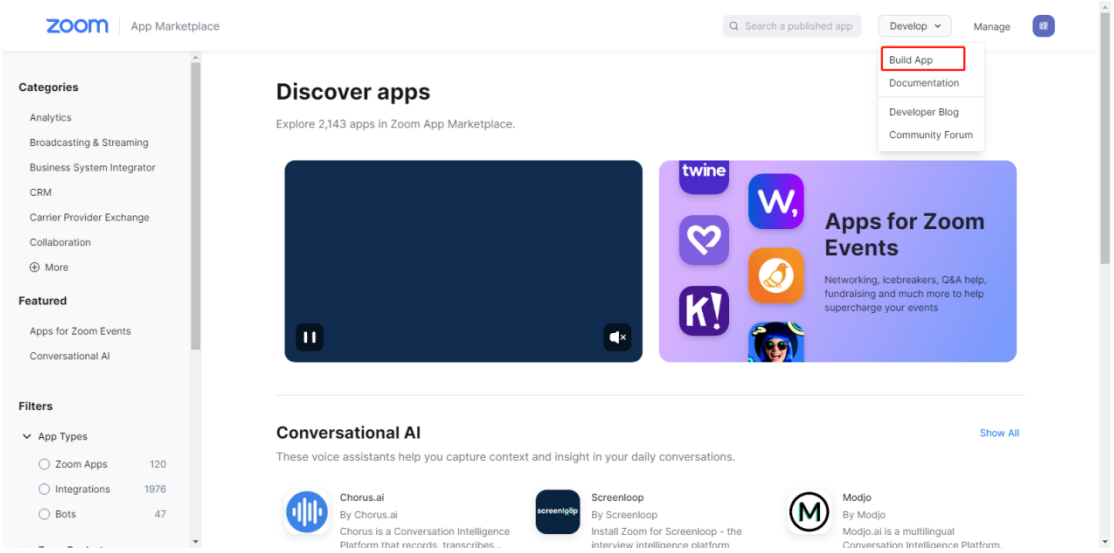
- Log in to Zoom official website: https://zoom.us/.



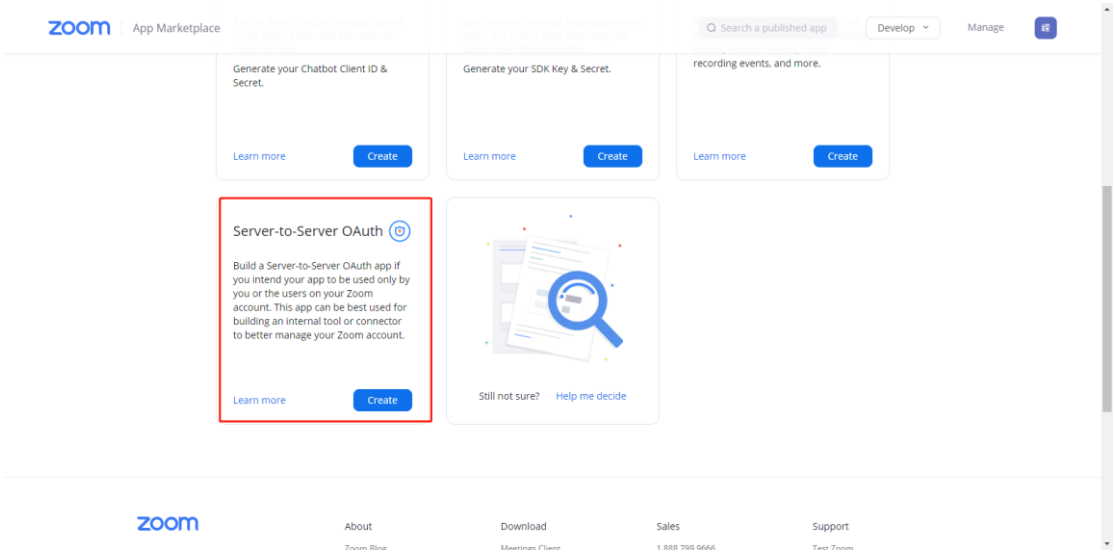
- Click **[Marketplace]** in the **[SOLUTIONS]**.



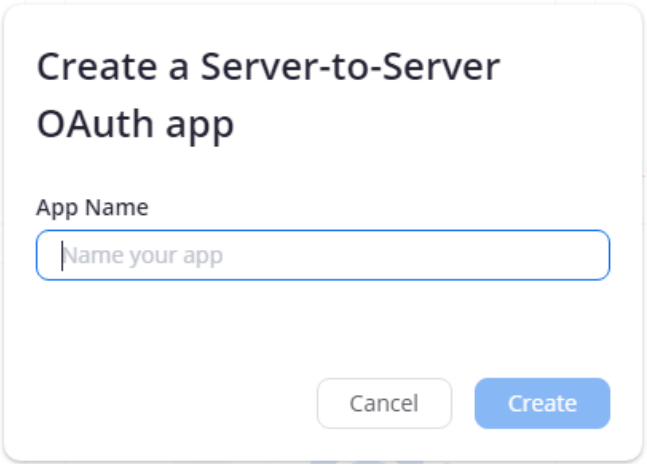
- Click **[Build App in the Develop]**.



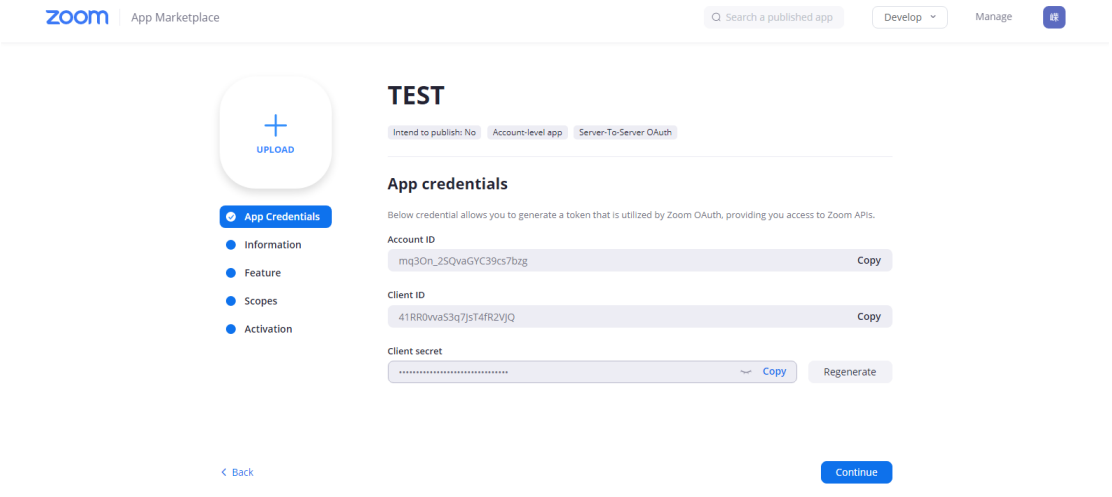
- Create Server-to-Server OAuth.



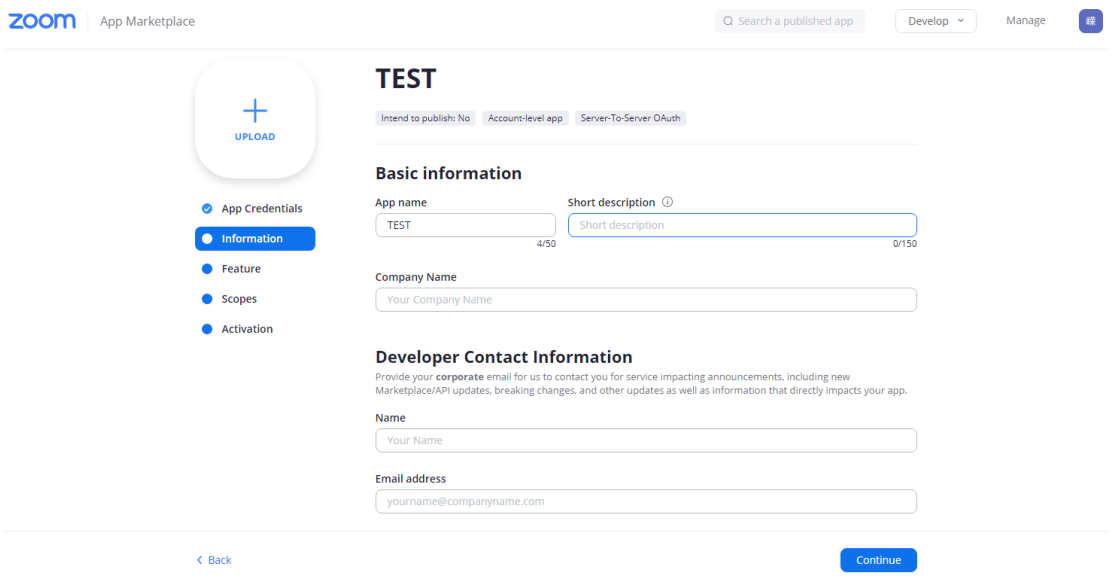
- Input the App name then click **[Create]**.



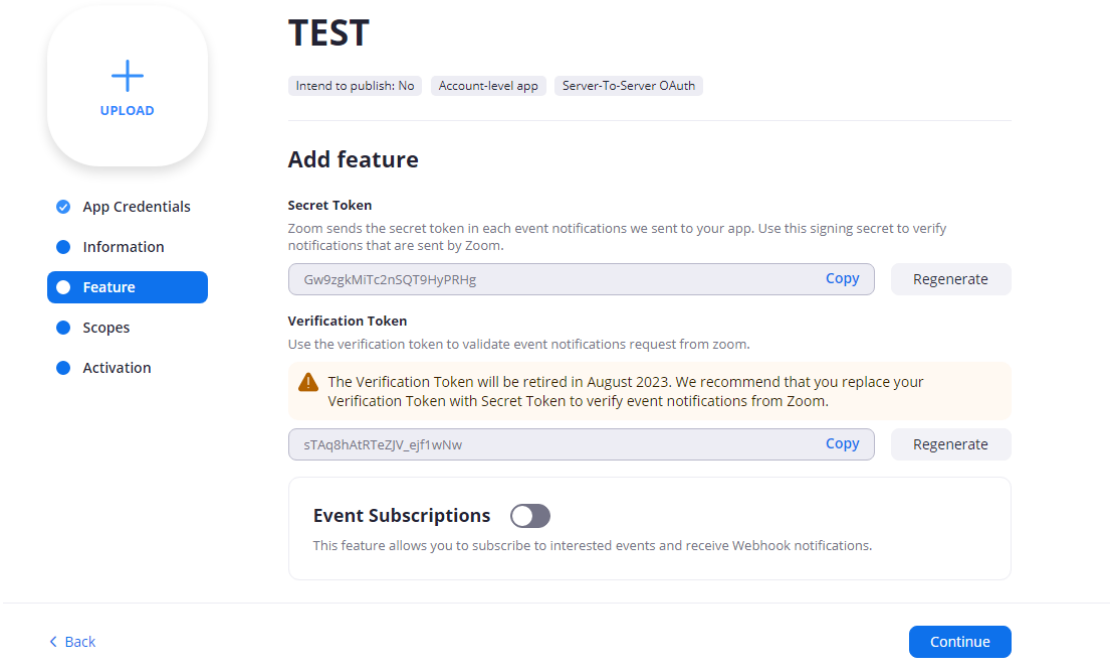
- Then will skip ahead to API configuration, click **[Continue]** skip to next step.



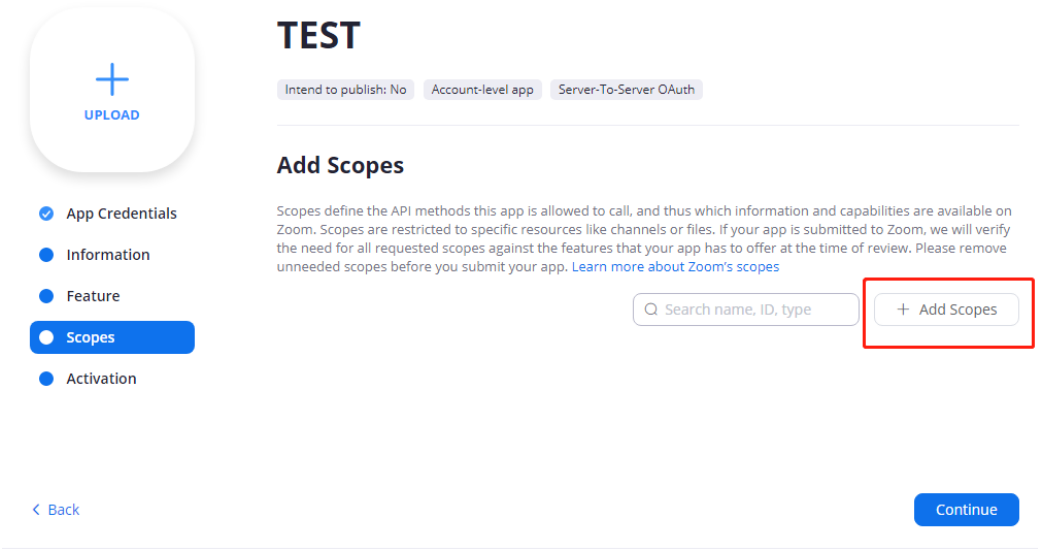
- Enter the basic information and developer contact information.



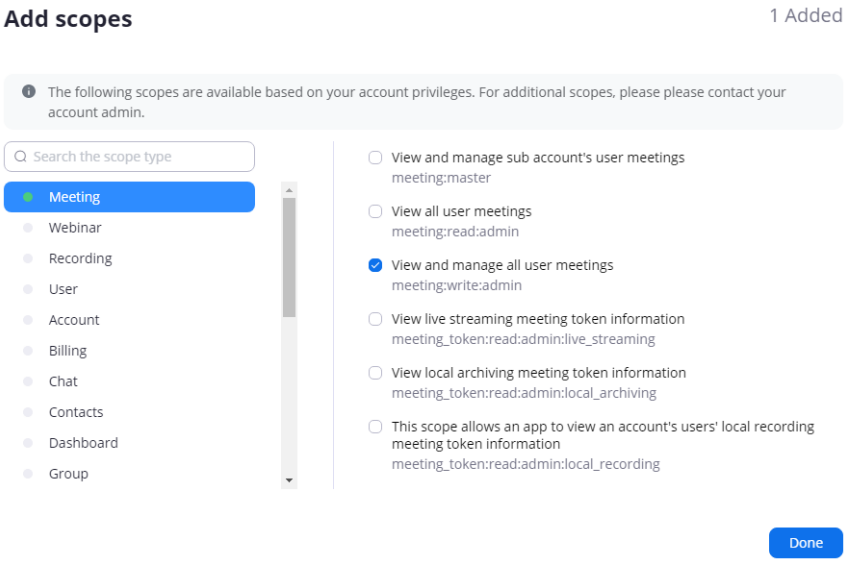
- Feature configuration is default, then click **[Continue]**.

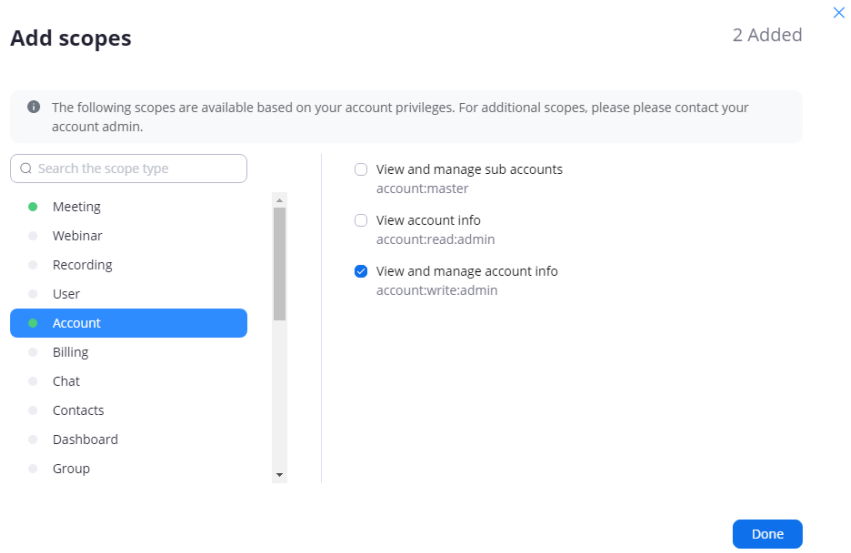


- Click **[Add Scopes]** to configure the scope.

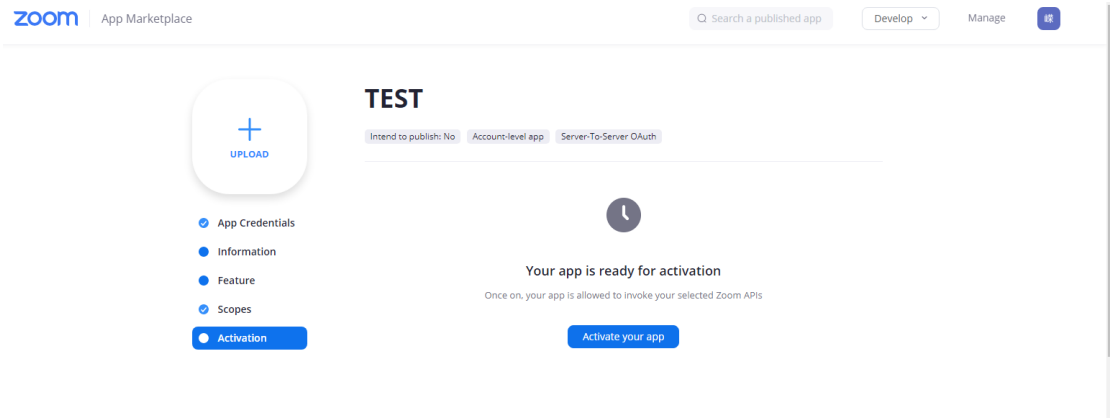


- Add [**View and manage account info**] and [**View and manage all user meetings**], then click **[Done]**, finally click **[Continue]**.

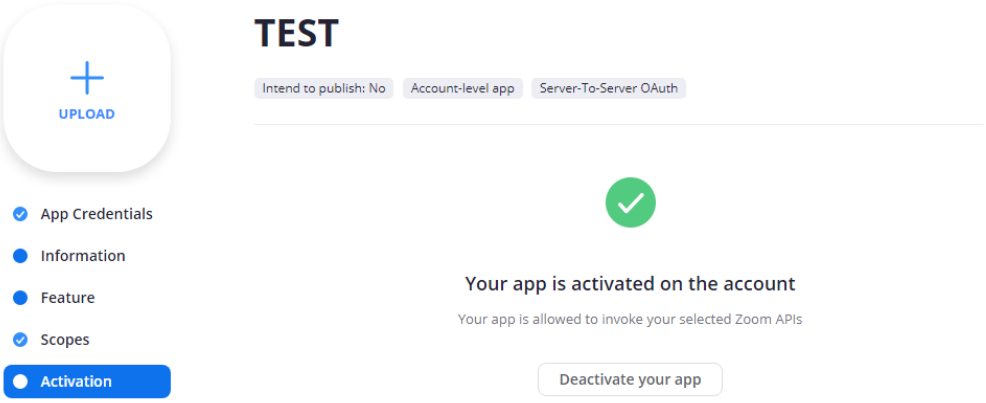




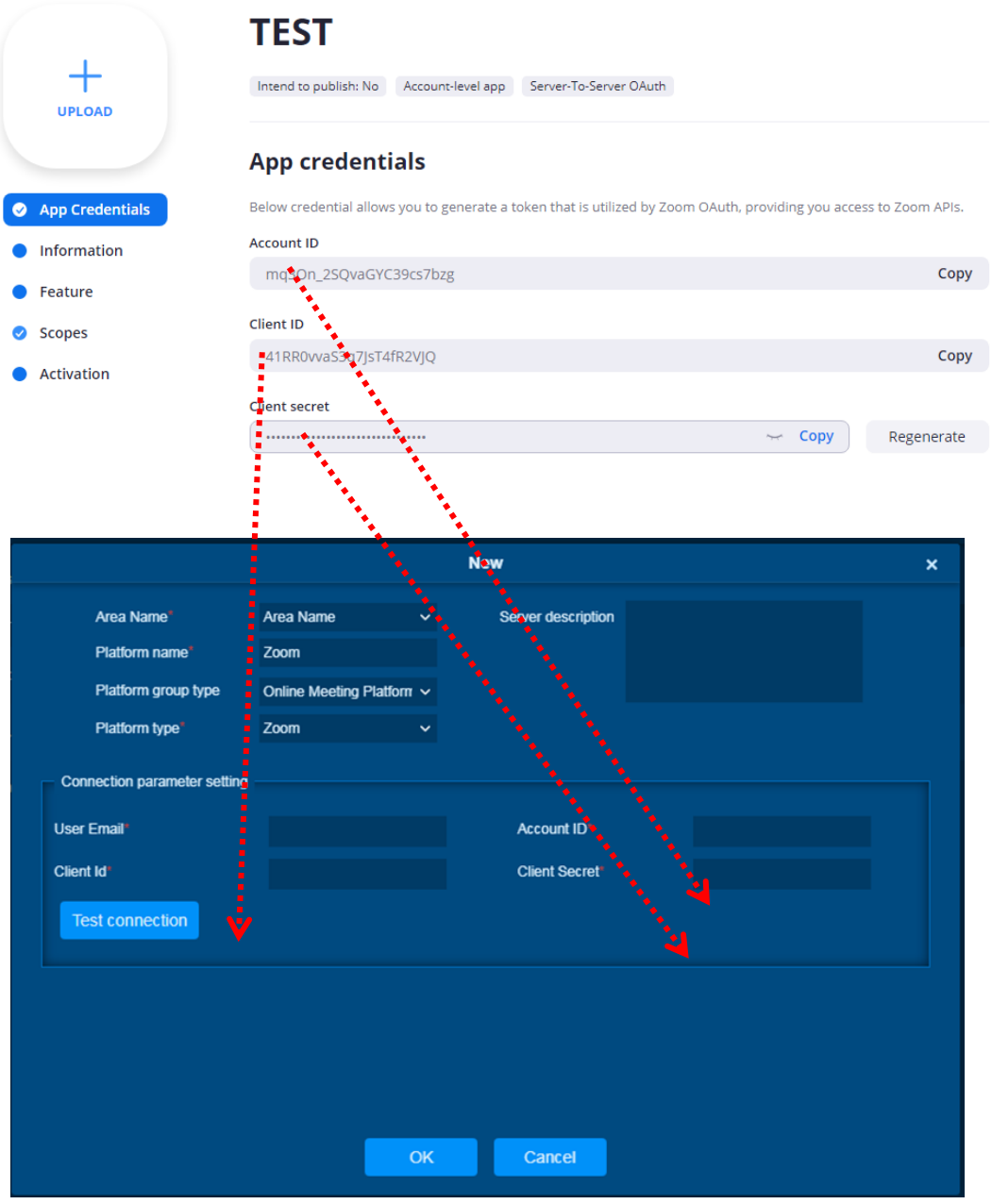
- Next click **[Activate your app]** to complete the configuration.



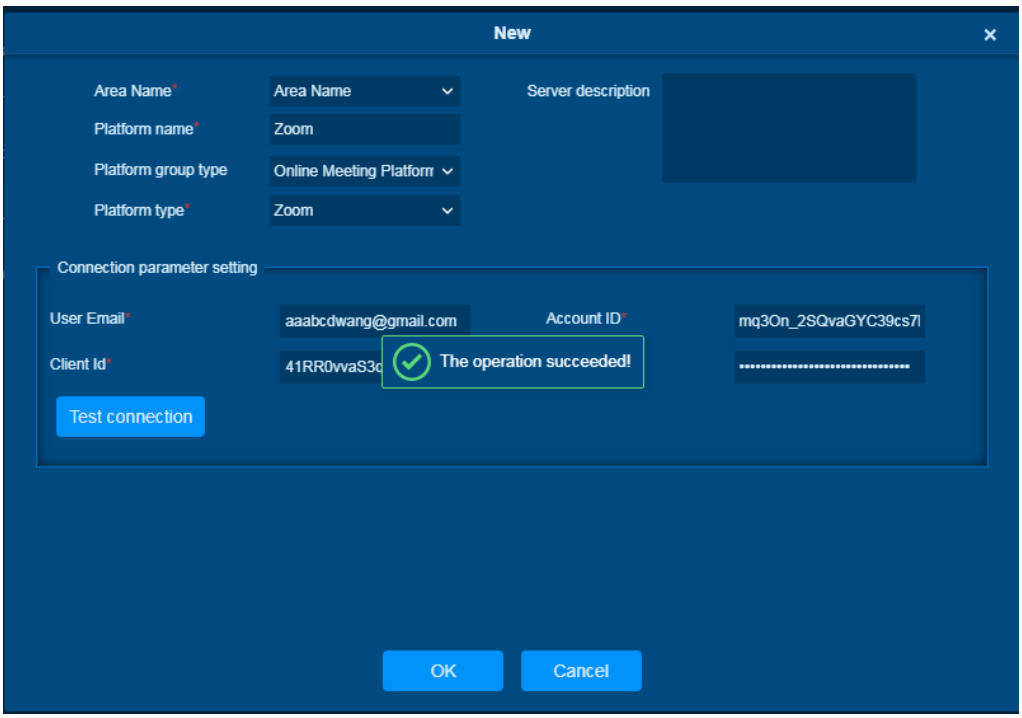
- When the prompt “Your app is activated on the account” appears, it indicates that the Zoom connection parameter configuration has been successful.



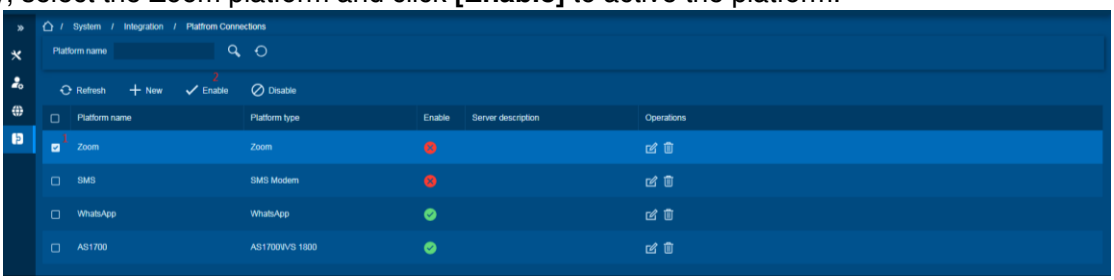
4. Skip to **[App credentials]** and then put in the appropriate parameters in the Armatura One platform connection. The **[User Email]** is the same as the one used to sign up with Zoom. And the Account ID, Client Id, and Client Secret are derived from the **[App credentials]**.



5. After filling in the relevant parameters, click **[Test connection]**, if it appears “The operation successful” means platform connection is successful, vice versa.



6. Click **[OK]**
7. Finally, select the Zoom platform and click **[Enable]** to active the platform.



Enable

Preconditions for Normal Use of Function

The administrator has the permission to enable the function, and data in the list can be modified.

Function Usage Scenarios

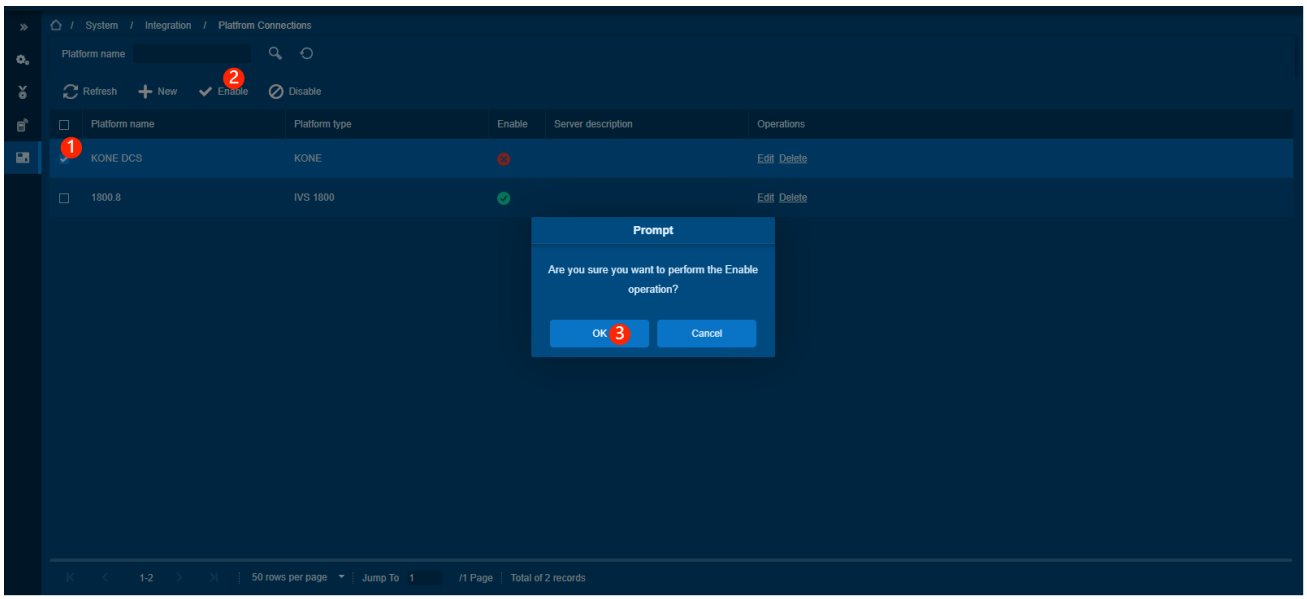
When you need to use a certain platform, and this platform is disabled, you can enable the platform.

Feature Trigger Result

Enable the checked platform for other module functions.

Steps:

- Check the platform that needs to be started.
- Click [**Enable**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the activation operation.



Disable

Preconditions for Normal Use of Function

The administrator has the permission to disable functions, and the list includes platform information that can be modified.

Function Usage Scenarios

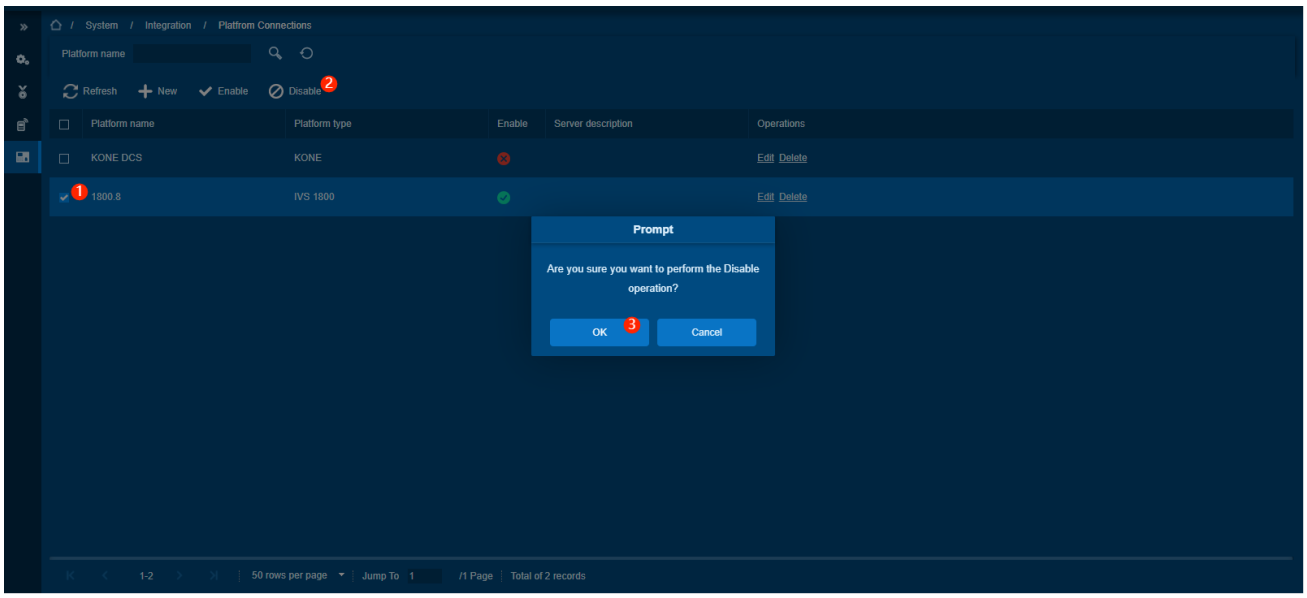
When you don't need to use a certain platform for the time being, you can disable.

Feature Trigger Result

Disable the checked platforms.

Steps:

- Check the platforms that need to be disabled.
- Click [**Disable**] button, a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the disabling operation.



21.4.2. Messages Management

Function Description

It Integrate messages sent by third-party messaging platforms.

Delete

Preconditions for Normal Use of Function

The administrator has the delete function permission, and there is information that can be deleted in the list.

Function Usage Scenarios

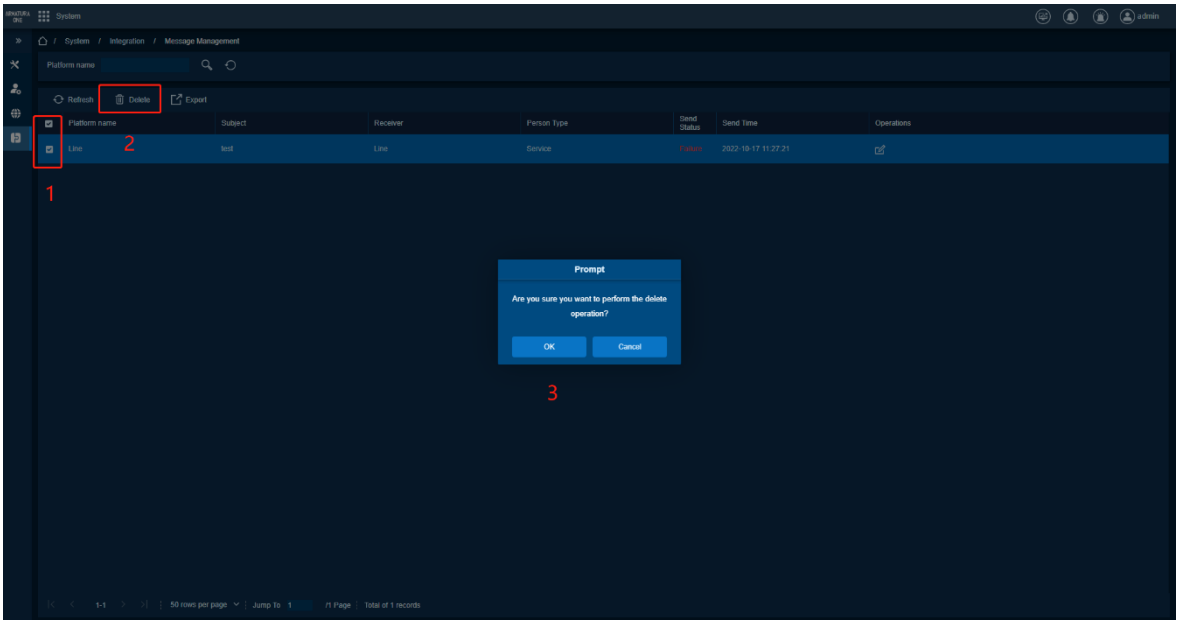
Delete unnecessary or expired data.

Feature Trigger Result

Delete the checked data.

Steps:

- Check the information that needs to be deleted.
- Click [**Delete**] button, and a prompt box will pop up.
- Click [**OK**] button in the prompt box to complete the Delete operation.



Export

Preconditions for Normal Use of Function

The administrator has the export function authority, and there is data in the list.

Function Usage Scenarios

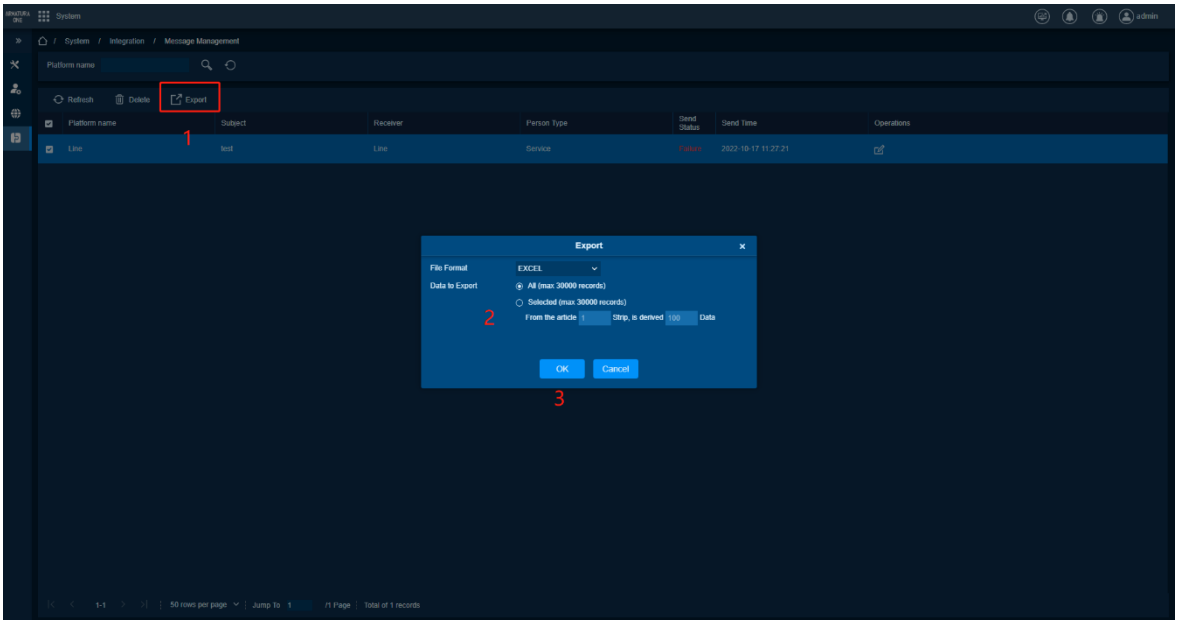
Export the information on the software to the computer.

Feature Trigger Result

Operations	Description
Select Excel	Export the message to EXCEL format
Select PDF	Export the message to PDF format
Select CSV	Export the message to CSV format
Select All Data	Export all data of the message
Select the Amount of Data Export	Export partial data of the message

Steps:

- Click [**Export**] button to pop up the Export box.
- Select the file format that needs to export in the pop-up box.
- Select the scope of export.
- Click [**OK**] button to complete the Export operation.



21.4.3. System Message

Function Description

It stores all system messages.

Export

Preconditions for Normal Use of Function

The administrator has the export function authority, and there is data in the list.

Function Usage Scenarios

Export the data on the software to the computer.

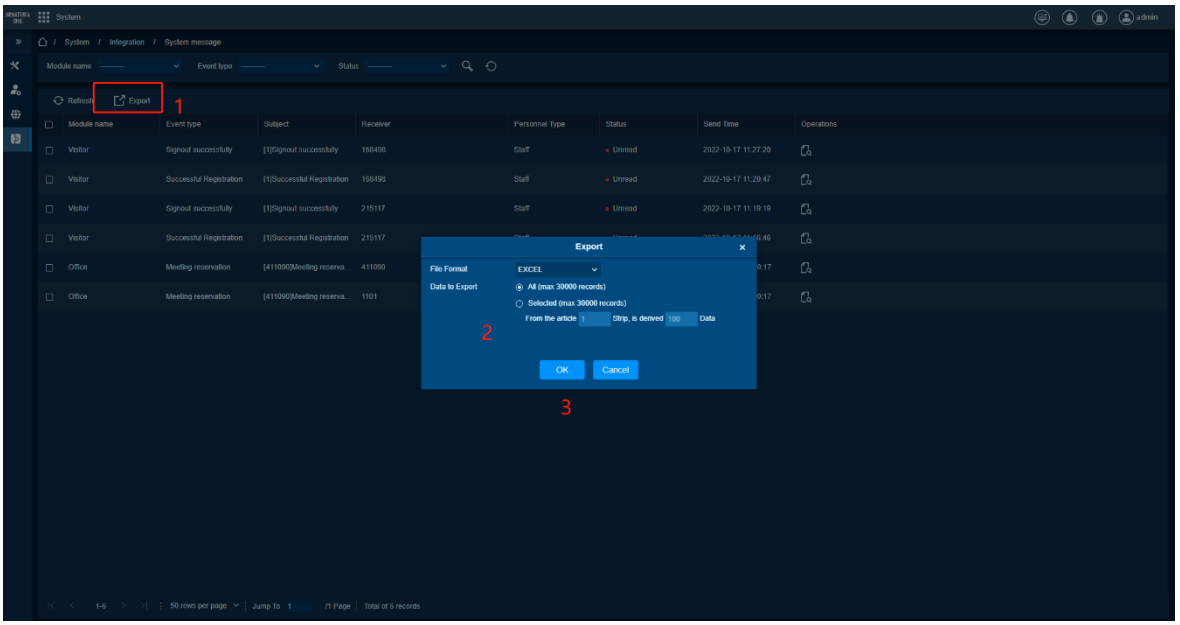
Feature Trigger Result

Operations	Description
Select Excel	Convert system message export to EXCEL format
Select PDF	Convert system message export to PDF format
Select CSV	Convert system message export to CSV format
Select All Data	Export all data of system message
Select the Amount of Data Export	Export partial data of system message

Steps:

- Click [**Export**] button to pop up the Export box.
- Select the file format that needs to export in the pop-up box.
- Select the scope of export.

- Click [**OK**] button to complete the Export operation.

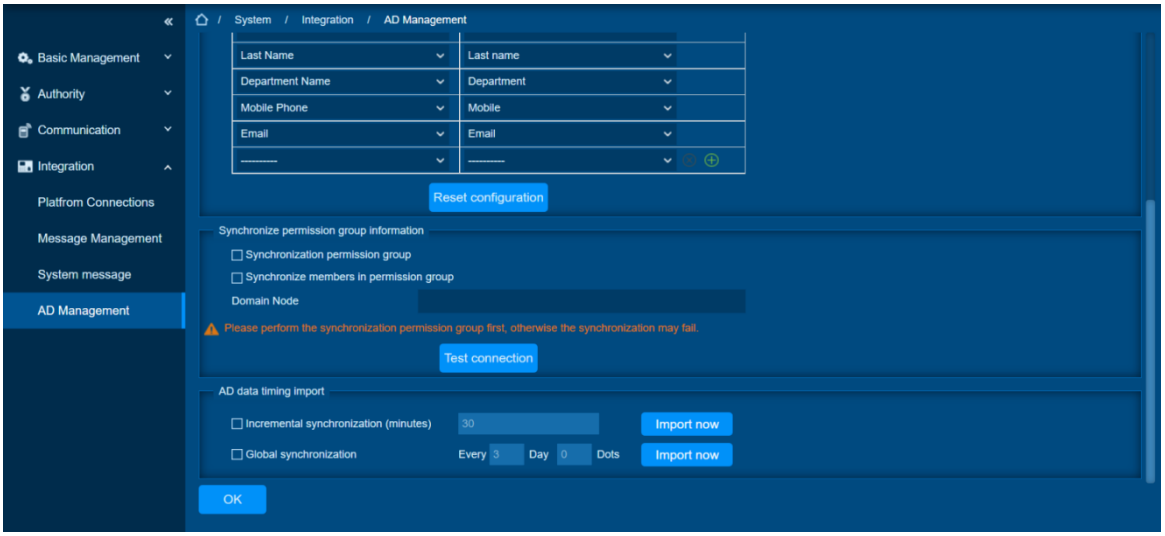


21.4.4. AD Management

Function Description

You can access shared personnel data.

Click [**System Integration**] > [**ADD Management**] to access the following page.



Field Descriptions:

Server Address: Set the server address.

Username: Set the username.

Password: Set the password

Domain Node: Set up domain nodes.

AD Field Setting: AD field settings

Synchronization Permission Group: After checking, synchronize permission group.

Synchronize Members in Permission Group: After checking, the members in the permission group will be synchronized.

Domain Node: Set access level domain node.

Incremental Synchronization (minutes): Set the time for AD incremental synchronization.

Global Synchronization: Set the time for global synchronization.

21.4.5. Map Configuration

Function Description

Before using the electronic map, the user needs to add the map first. After the addition is successful, the user can add doors on the map, zoom in and out the map (and the doors on the map). After the user changes the location of the map or icon, the current settings can be saved through **[**Save Location**]**, so that when you visit again, you can see the status of the previous settings, and the user can see the real-time events of the door on the map.

New Map

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

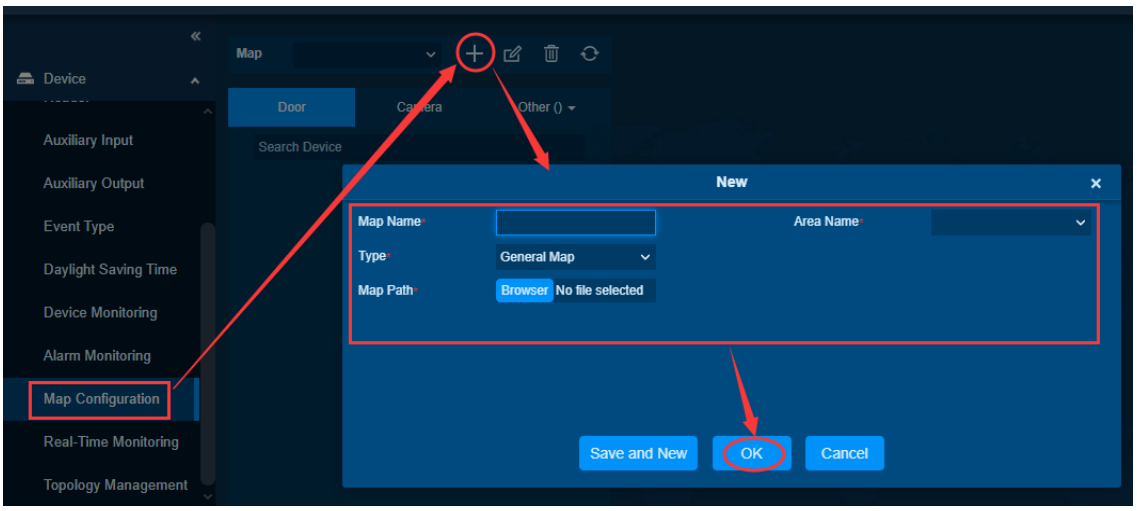
Need to perform map configuration operations on specific areas.

Feature Trigger Result

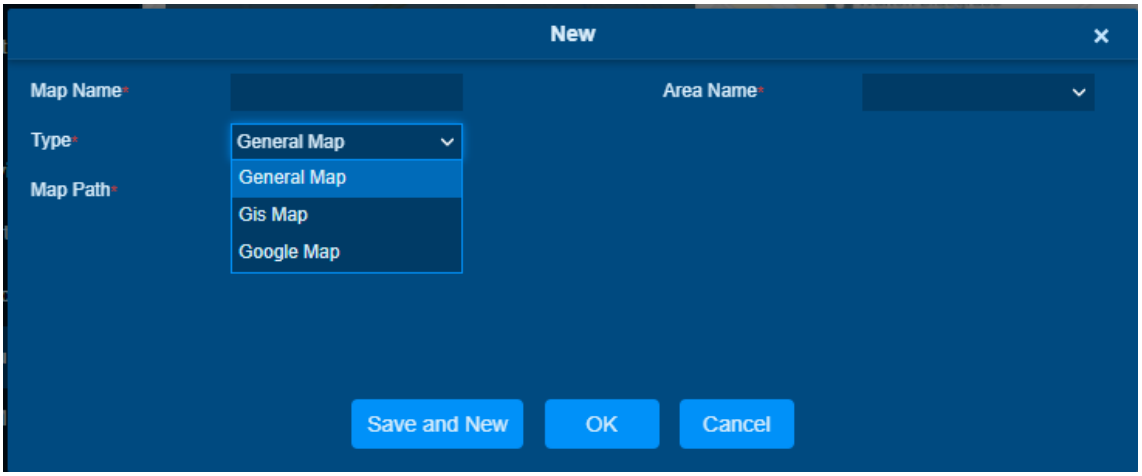
Add a new map, including name, map type, path, area name, etc.

Steps:

- Click **[Access]** > **[Device]** > **[Map Configuration]** > **[** **]** on the Action Menu, the following interface will be shown:



Currently supports 3 map types, select the proper map type.



General Map

Upload your local image as a map, support JPG\PNG type format.

GIS Map

Supported by Supermap, contact your local dealer to get full setting parameter, it may charge and supported by 'Supermap' company.

Google Maps

Supported by Google Cloud Platform, users self-register and billing for the service on Google Cloud Platform to obtain the KEY for connection.

Authority Control

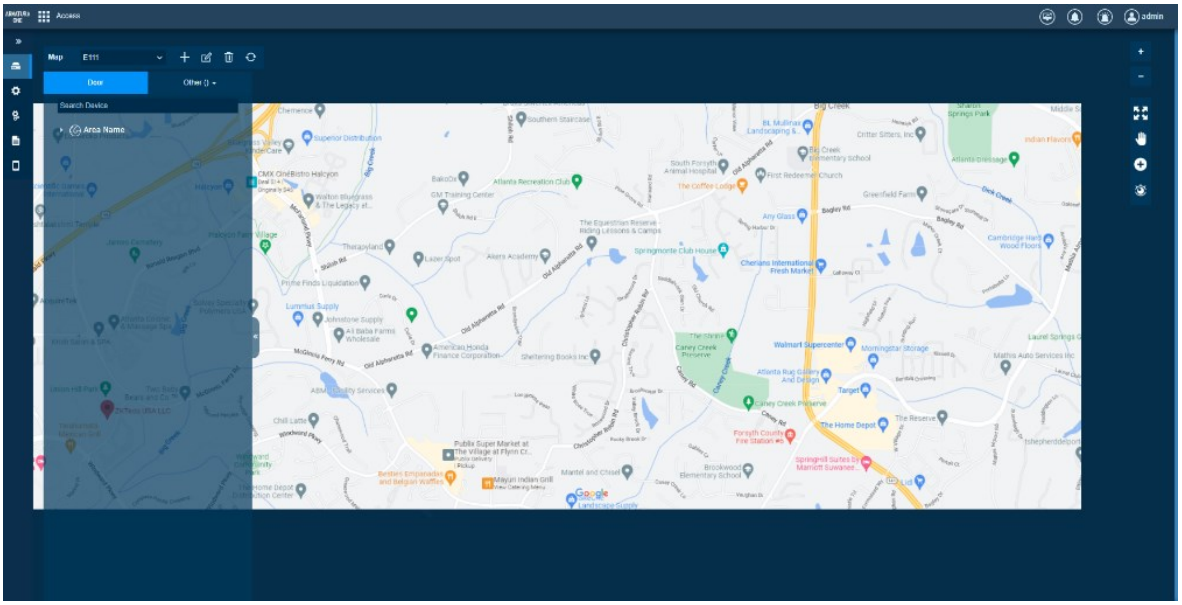
1. Users need to select the relevant area for the map when adding levels. The area will be relevant to the user access levels, users can only view or manage the map within levels. If the relevant area of a map is modified, all doors on the map will be cleared. Users need to add the doors manually again.
2. When an administrator is adding a new user, he can set the user operation rights in role setting, such as save positions, Add Door, Add Camera, etc.

✍**Note:**

1. In Map Modification, users can choose to modify the map name but not the path. Users only need to check the box to activate the modification option.
2. The system supports adding multi doors at the same time. After adding the doors, users need to set the door position on the map and click **[Save].**
3. When modifying door icon, especially when users zoomed out the map, the margin for top and left shall not be smaller than 5 pixels, or system will prompt error.
4. Users are recommended to add a map size under 1120 * 380 pixels. If several clients access the same server, the display effect will be different according to resolutions of screen and the settings of browsers.
5. GIS Map data is provided by your GIS provider.
6. Google Map key is provided by Google, register in Google, or contact your local dealer

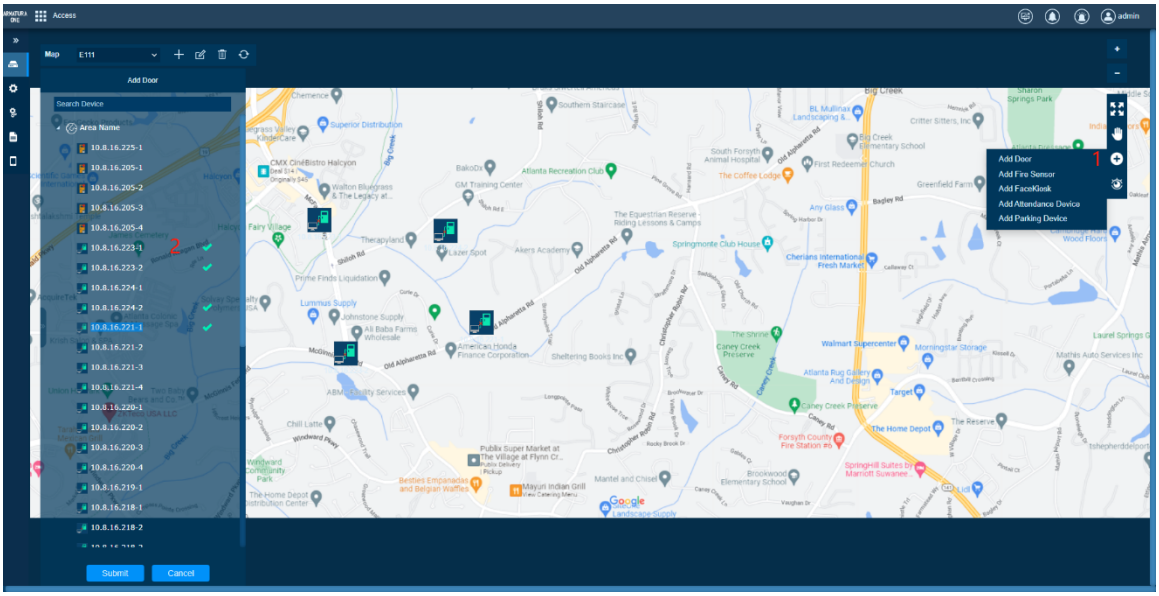
Adjust Map

Use the mouse scroller or the "**+**" "**-**" sign in the toolbar in the upper right corner to zoom in and out the map, using [] icon to adjusting the proper view height, and click [**Finish**] to lock, so that the view height will be locked at the current set, and every time the map is loaded in will be like this.



Add Devices

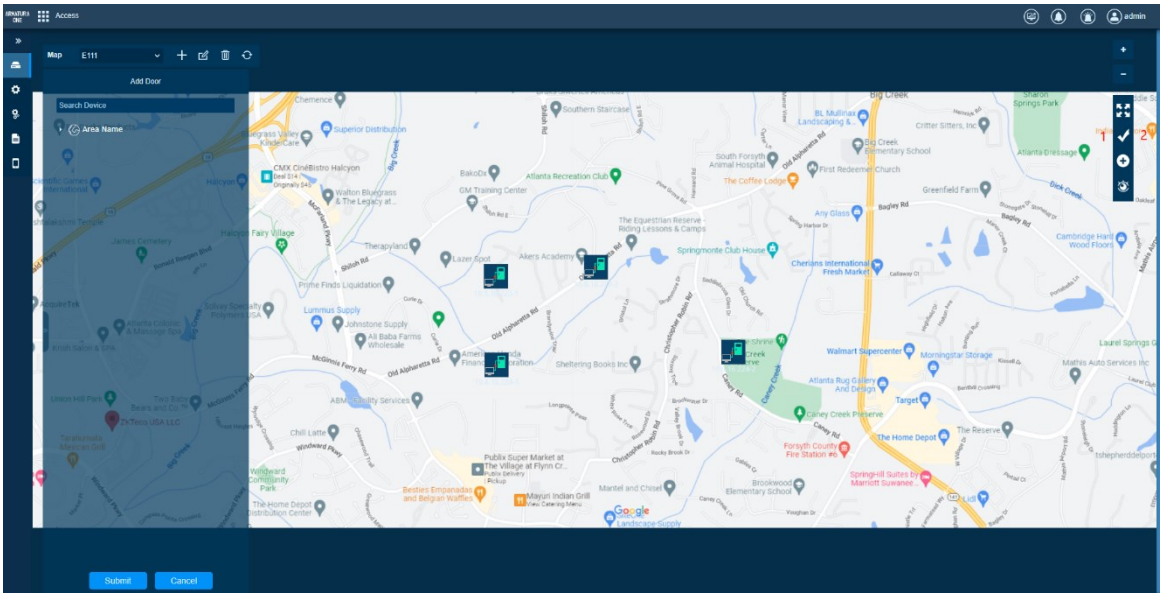
Using [] icon to add device to the map, Doors\ Cameras\ Fire Sensor\ FaceKiosk\ Attendance Device\ Parking Device could be added to the map.



Click the icon and select Add Door, the left window will list the area devices for selection, drag them to the map, and finally click the submit button in the list to complete the confirmation.

Change Device Location

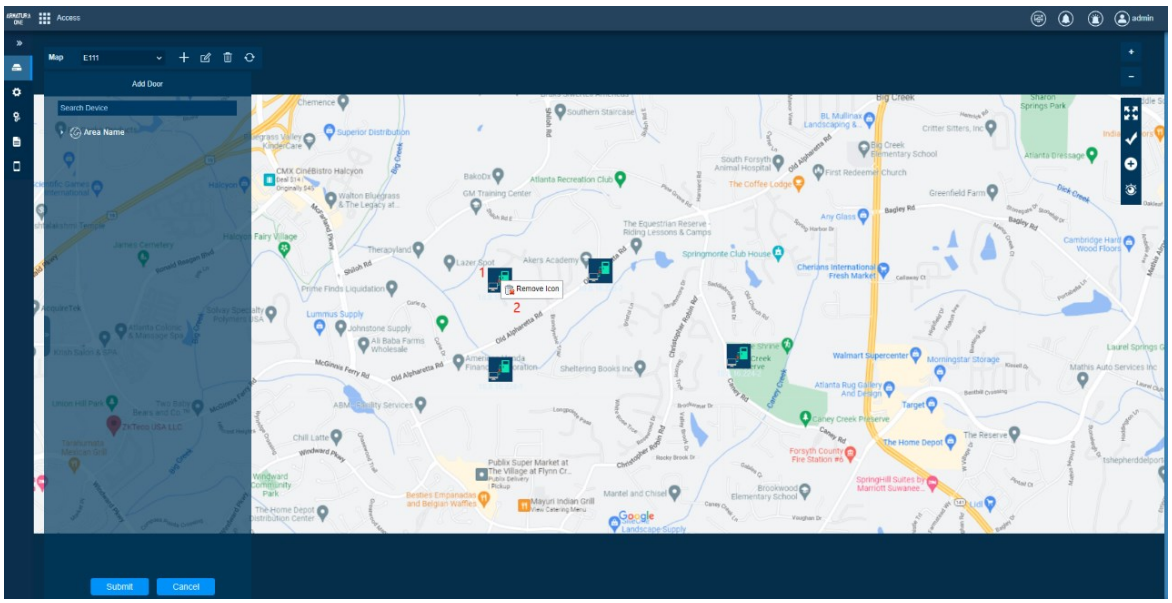
Using [ ] icon to change the current location of the device on the map.



Click the button and drag the device icon on the map to wherever you want and finally click the button again to confirm operation.

Remove the Device

Right-click the icon of the device that needs to be removed on the map and select remove.



Edit Map Parameters

Preconditions for Normal Use of Function

Log in to the system with the current account and have the authority.

Function Usage Scenarios

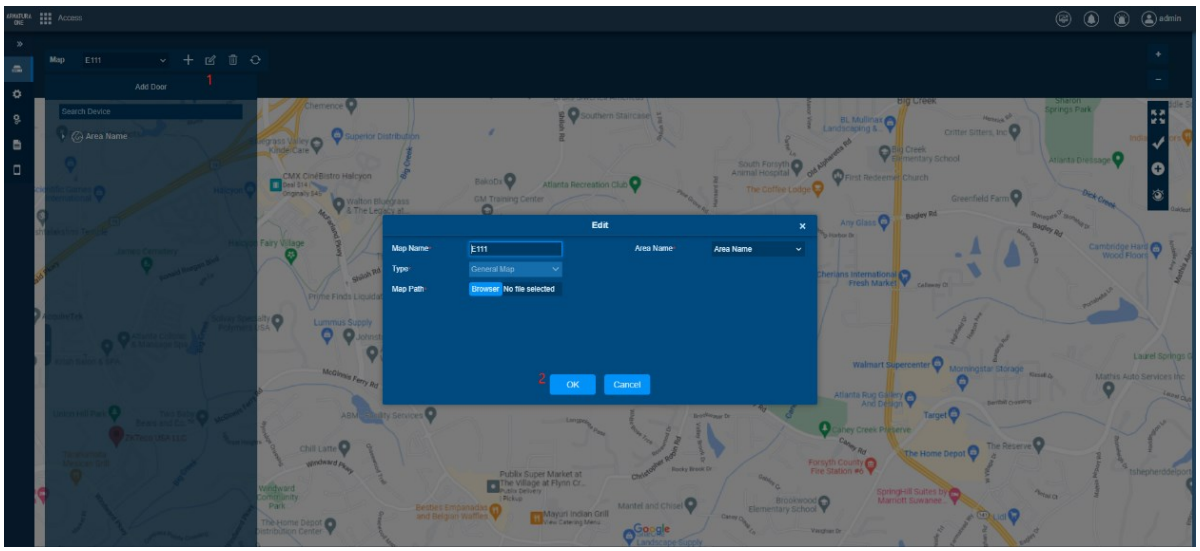
Need to modify the configuration of some doors and cameras in a specific area.

Feature Trigger Result

You can modify the added map, the name, secret key, center point coordinates, etc.

Steps:

- Click **[Access] > [Device] > [Map Configuration] > [ ]** on the Action Menu, the following interface will be shown.



After editing, you can operate the map. For details, check **[Adding Map]**.

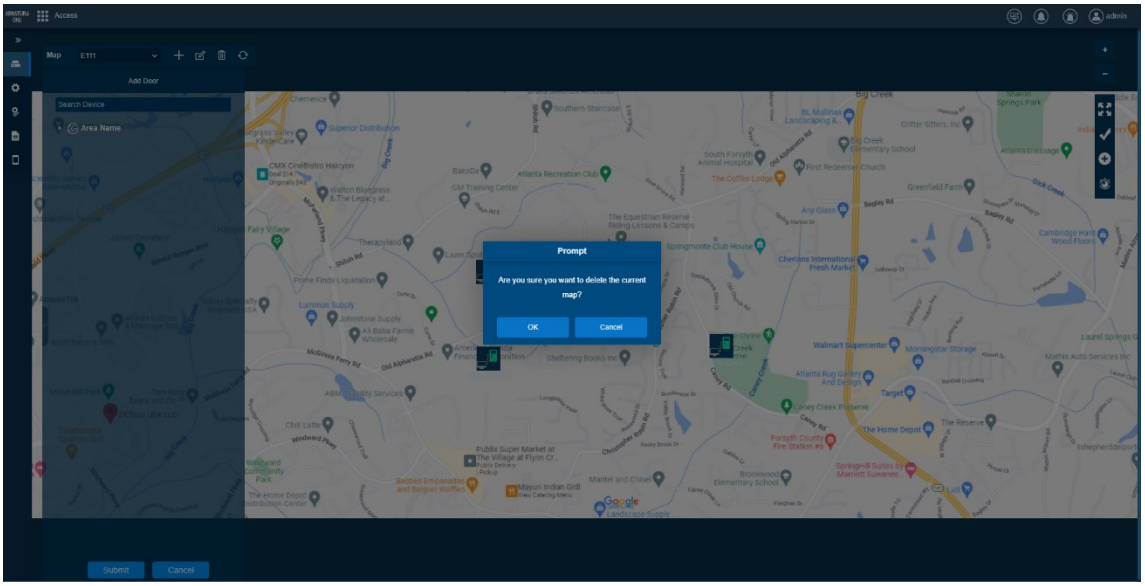
Delete Map

Feature Trigger Result

Delete the map and the devices on the map.

Steps:

- Click **[Access]** > **[Device]** > **[Map Configuration]** > **[ ]** on the Action Menu, the following interface will be shown. Click **[OK]** and the map is deleted.



22. FAQs

Q: How to use a card issuer?

A: Connect the card issuer to PC through USB port, and then select individual personnel card issue or batch card issue. Move the cursor to the card number input box, and punch the card on the card issuer, then the card number will be automatically shown in the input box.

Q: What is the use of role setting?

A: Role setting has the following uses: 1. To set unified level for the same type of users newly added, just directly select this role when adding users; 2. When setting system reminder and determine which roles can be viewed.

Q: How to operate if I want to set accounts for all personnel of the Company's Financial Department?

A: First, create a new role in system setting and configure the functions to be used for this role. Then add a user, set user information, and select the user's role, thus adding a new account. For other accounts, do the same.

Q: In Windows Server 2003, why the IE browser displayed error when access the system, how to solve it?

A: This problem occurs because that Server 2003 has [Security Configuration Option] settings. If you want to access the system, please configure it as follows: click Start - Control Panel - Add or Remove Program, select [Add and remove Windows components] in the interface and click [Internet Explorer Enhanced Security Configuration] option, cancel the tick before it. Then click [Next] to remove it from the system. Open the system again the browser will access the system properly.

Q: If backing up or restoring the database fails, the possible reason?

A:

Backup fails: Please check the system environment variables, please go to [Properties] > [Advanced] to set the environment variables as "C:\Program Files\ArmaturaOne\service\zkpostgre\bin". "C:\Program Files" is the system installation path, you can modify by your actual situation.

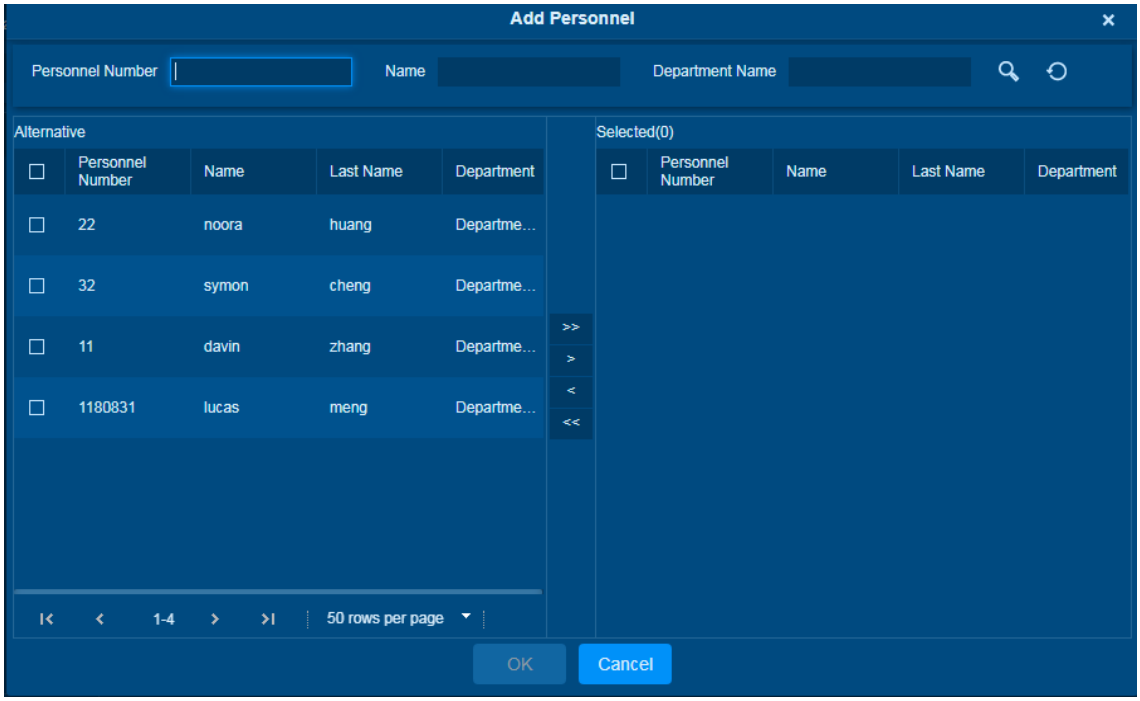
Restore fails: There are several reasons: The system version is too high or too low, or the database has been damaged, you need to follow the prompts to change the system version or repair the system, re-install the database.

23. Appendices

23.1. Common Operations

Select Personnel

The selected personnel page in the system is as below:

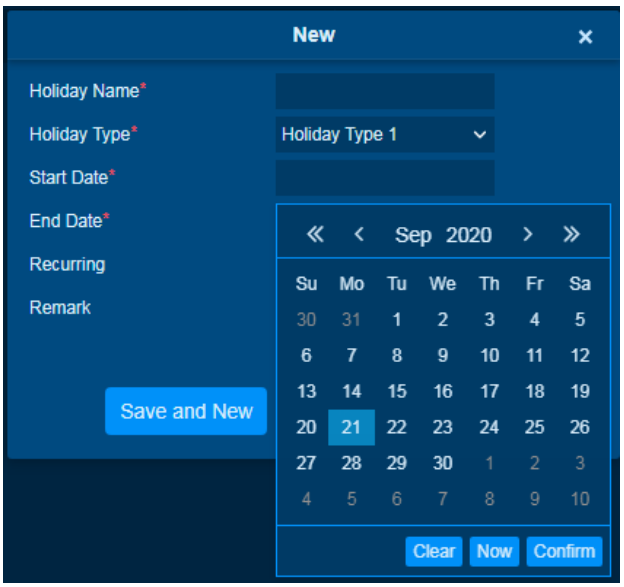


You can select the personnel from list generated, or you can also click **[More]** to filter by gender or department.

Click > to move the selected personnel in to the selected lists. If you want to cancel the movement, click <.

Set Date and Time

Click the date and time box:

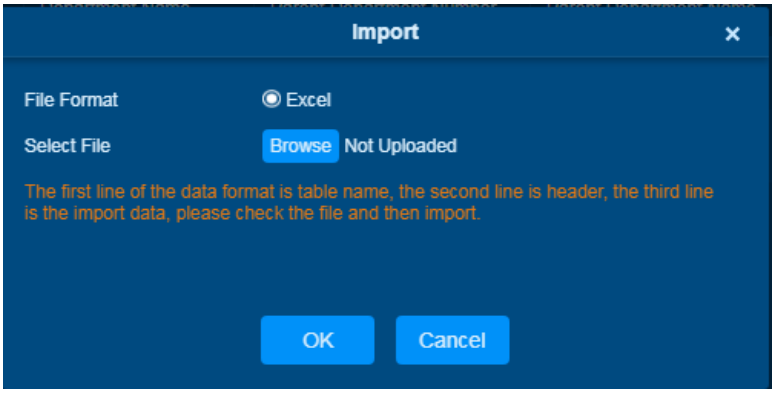


Click on the Year to select by clicking or . Click the Month and Date to select directly.

Import (take the Department list importing as an example)

If there is a personnel file in your computer, you can Import it into the system.

1) Click [**Import**].



Fields are as follows:

File Format: Select the file format as Excel.

Select File: Chose the file to be imported.

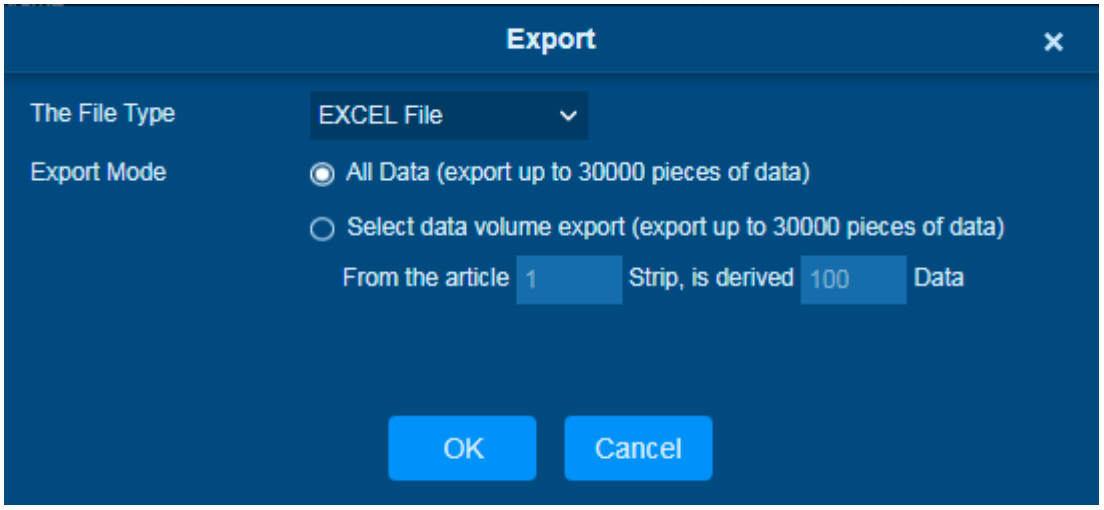
2) Click **[OK]** to import.

✍**Note:**

- When importing department table, department name and department number must not be empty, the parent department can be empty. Duplicated number does not affect the operation, it can be modified manually.
- When importing personnel table, personnel number is required. If the personnel number already exists in the database, it will not be imported.

Export (take the personnel list exporting as an example)

1) Click [**Export**].



2) Select the file format and export mode to be exported. Click [**OK**].

3) You can view the file in your local drive.

✍**Note:**

10000 records are allowed to export by default, you can manually input as required.

23.2. Access Event Type

23.2.1. Normal Events

Normal Punch Opening: In **[Only Card]** verification mode, the person having open door levels punch card at valid Timetable, open the door, and trigger the normal event.

Normal Press Fingerprint Opening: In **[Only Fingerprint]** or **[Card or Fingerprint]** verification mode, the person having open door levels press fingerprint at valid time, the door is opened, and trigger the normal event.

Card and Fingerprint Opening: In **[Card and Fingerprint]** verification mode, the person having the open permission, punch the card and press the fingerprint at the valid time, and the door is opened, and trigger the normal event.

Exit button Open: press the exit button to open the door within the door valid time zone and trigger this normal event.

Trigger the exit button (locked): indicates the normal event triggered by pressing the exit button when the exit button is locked.

Punch during Normal Open Time Zone: At the normal open period (set normal open period for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission punch effective card at the opened door to trigger this normal event.

Press Fingerprint during Normal Open Time Zone: At the normal open period (set normal open period

for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission press the effective fingerprint at the opened door to trigger this normal event.

First-Person Normally Open (Punch Card): In **[Only Card]** verification mode, the person having first-person normally open permission, punch at the setting first-person normally open time (the door is closed) and trigger the normal event.

First-Person Normally Open (Press Fingerprint): In **[Only Fingerprint]** or **[Card plus Fingerprint]** verification mode, the person having first-person normally open permission, press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

First-Person Normally Open (Card plus Fingerprint): In **[Card plus Fingerprint]** verification mode, the person having first-person normally open permission, punch the card and press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

Normal Open Time Zone Over: After the normal open time zone over, the door will close automatically.

Remote Normal Opening: When set the door state to normal open in the remote opening operation, this normal event is triggered.

Cancel Normal Open: When punch the valid card or use remote opening function to cancel the current door normal open state, this normal event is triggered.

Disable Intraday Passage Mode Time Zone: In door normal open state, punch effective card for five times (must be the same user) or select **[Disable Intraday Passage Mode Time Zone]** in remote closing operation, and this normal event is triggered.

Enable Intraday Passage Mode Time Zone: If the intraday passage mode time zone is disabled, punch effective card for five times (must be the same user) or select **[Enable Intraday Passage Mode Time Zone]** in remote opening operation, and this normal event is triggered.

Multi-Person Opening Door (Punching): In **[Only Card]** verification mode, multi-Person combination can be used to open the door. After the last card is verified, the system triggers this normal event.

Multi-Person Opening Door (Press Fingerprint): In **[Only Fingerprint]** or **[Card plus Fingerprint]** verification mode, multi-Person combination can be used to open the door. After the last fingerprint is verified, the system triggers this normal event.

Multi-Person Opening Door (Card plus Fingerprint): In **[Card plus Fingerprint]** verification mode, multi-Person combination can be used to open the door. After the last card plus fingerprint is verified, the system triggers this normal event.

Emergency Password Opening Door: Emergency password (also known as super password) set for the current door can be used for door open. This normal event will be triggered after the emergency password is verified.

Opening Door during Normal Open Time Zone: If the current door is set a normally open period, the door will open automatically after the setting start time has expired, and this normal event will be triggered.

Linkage Event Triggered: After linkage configuration takes effect, this normal event will be triggered.

Cancel Alarm: When the user cancels the alarm of corresponding door successfully, this normal event will be triggered.

Remote Opening: When the user opens a door by **[Remote Opening]** successfully, this normal event will

be triggered.

Remote Closing: When the user closes a door by **[Remote Closing]** successfully, this normal event will be triggered.

Open Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Open for Action Type, this normal event will be triggered when the linkage setting takes effect.

Close Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Close for Action Type, or closes the opened auxiliary output by **[Door Setting]** > **[Close Auxiliary Output]**, this normal event will be triggered.

Door Opened Correctly: When the door sensor detects the door has been properly opened, triggering this normal event.

Door Closed Correctly: When the door sensor detects the door has been properly closed, triggering this normal event.

Auxiliary Input Point Disconnected: Will be triggered auxiliary input point is disconnected.

Auxiliary Input Point Shorted: When the auxiliary input point short circuit, trigger this normal event.

Device Start: Will be triggered if device starts (This event of PULL devices will not appear in real-time monitoring and can be viewed only in event records of reports).

23.2.2. Abnormal Events

Too Short Punch Interval: When the interval between two punching is less than the set time interval, this abnormal event will be triggered.

Too Short Fingerprint Pressing Interval: When the interval between two fingerprints pressing is less than the set time interval, this abnormal event will be triggered.

Door Inactive Time Zone (Punch Card): In [Only Card] verification mode, if the user having the door open permission punch but not at door effective period, this abnormal event will be triggered.

Door Inactive Time Zone (Press Fingerprint): If the user having the door open permission, press the fingerprint but not at the door effective time, this abnormal event will be triggered.

Door Inactive Time Zone (Exit Button): If the user having the door open permission, press exit button but not at the effective period, this abnormal event will be triggered.

Illegal Time Zone: If the user with the permission of opening the door, punches during the invalid time zone, this abnormal event will be triggered.

Illegal Access: If the registered card without the permission of current door is punched to open the door, this abnormal event will be triggered.

Anti-Passback: When the anti-pass back takes effect, this abnormal event will be triggered.

Interlock: When the interlocking rules take effect, this abnormal event will be triggered.

Multi-Person Verification (Punching): When Multi-Person combination opens the door, the card verification before the last one (whether verified or not), this abnormal event will be triggered.

Multi-Person Verification (Press Fingerprint): In [Only Fingerprint] or [Card or Fingerprint] verification mode, When Multi-Person combination opens the door, the fingerprint verification before the last one (whether verified or not), this abnormal event will be triggered.

Unregistered Card: If the current card is not registered in the system, this abnormal event will be triggered.

Unregistered Fingerprint: If the current fingerprint is not registered or it is registered but not synchronized with the system, this abnormal event will be triggered.

Opening Door Timeout: If the door sensor detects that it is expired the delay time after opened, if not close the door, this abnormal event will be triggered.

Card Expired: If the person with the door access level, punches after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Fingerprint Expired: If the person with the door access permission, presses fingerprint after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Password Error: If using [Card plus Password] verification mode, duress password or emergency password to open door, this abnormal event will be triggered.

Failed to Close door during Normal Open Time Zone: If the current door is in normal open state, but the user cannot close it by [Remote Closing], this abnormal event will be triggered.

Verification Mode Error: If the user opening door mode is inconsistent with that set for current door, this abnormal event will be triggered.

Background Verification Failed: If the background verification fails, this abnormal event will be triggered.

Background Verification Success: If the background verification succeeds, this abnormal event will be triggered.

Background Verification Timeout: If no background verification result is returned in the specified period, this abnormal event will be triggered.

Multi-Person Verification Failed: When Multi-Person combination opens the door, the verification is failed, and triggers this abnormal event.

23.2.3. Alarm Events

Duress Password Opening Door: Use the duress password of current door for verifying successfully and trigger this alarm event.

Duress Fingerprint Opening Door: Use the duress fingerprint of current door for verifying successfully and trigger this alarm event.

Duress Opening Door Alarm: Use the duress password or duress fingerprint set for current door for verifying successfully and trigger this alarm event.

Opened Accidentally: Except all normal events, if the door sensor detects that the door is opened, and this alarm event will be triggered.

Door-open timeout: This alarm event is triggered when the opened door is not locked at closing door time.

Tamper-Resistant Alarm: This alarm event will be triggered when AIO device is tampered.

Server Connection Failed: This alarm event will be triggered when the device is disconnected from the server.

Mains power down: Inbio5 series controller events, external power down.

Battery power down: Inbio5 series controller event, built-in battery power-down.

Invalid card alarm: Alarm event trigger when invalid card swiping five consecutively.

✍**Note:**

The user can customize the level of each event (Normal, Abnormal, and Alarm).

23.3. Elevator Event Type

23.3.1. Normal Events

Normal Punch Open: This normal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card and passed the verification.

Punch during passage mode time zone: This normal event is triggered if a valid card is punched after a user with the floor opening right sets the Normally Open periods for a specific floor or sets the floor to the Normally Open state through the remote opening floor operation.

Open during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific floor or sets the floor to the Normally Open state through the remote opening floor operation.

Remote release: This normal event is triggered if a user remotely releases a button successfully.

Remote locking: This normal event is triggered if a user remotely locks a button successfully.

Disable intraday passage mode time zone: This normal event is triggered if a user performs this operation on the Remotely Release Button page when a floor is in Normally Open state.

Enable intraday passage mode time zone: This normal event is triggered if the user performs this operation on the Remotely Lock Button page when the Normally Open periods of the floor are prohibited on the day.

Normal fingerprint open: This normal event is triggered if a user with the button releasing right presses his/her fingerprint in the "Card or fingerprint" verification mode and the verification is passed.

Press fingerprint during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific door or sets the door to the Normally Open state through the remote opening door operation.

Passage mode time zone over: When the preset Normally Open period arrives, the button is automatically locked.

Remote normal opening: This normal event is triggered if a user selects the continuously releasing button to set the button in continuously released state on the page for remotely opening the floor.

Device started: This normal event is trigger upon startup of the device. (This event will not appear in the

real-time monitoring and can only be viewed through the event records in the report.)

Password open: This normal event is triggered if a user with the button releasing right presses the password in the "Password only" or "Card or fingerprint" verification mode and the verification is passed.

Superuser open buttons: This normal event is triggered if the super user remotely releases a button successfully.

Start the fire floor: Release all buttons in the case of emergency so that users can select floors.

Superuser close buttons: This normal event is triggered if the super user remotely closes floors (locks the buttons) successfully.

Enable elevator control button: Restart the elevator control function.

Disable elevator control button: Temporarily disable the elevator control function.

Auxiliary input disconnected: This normal event is triggered if the auxiliary input point is disconnected.

Auxiliary input shorted: This normal event is triggered if the auxiliary input point is short circuited.

23.3.2. Abnormal Events

Operate interval too short: This abnormal event is triggered if the actual interval between two times of card punching is smaller than the interval that is set for this floor.

Press fingerprint interval too short: This abnormal event is triggered if the actual interval between two times of fingerprint pressing is smaller than the interval that is set for this floor.

Button inactive time zone (punch card): This abnormal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card beyond the effective periods.

Illegal time zone: This abnormal event is triggered if a user with the floor opening right punches his/her card beyond the effective periods.

Access denied: This abnormal event is triggered if a registered card is punched before the elevator control right of the current floor is set for this card.

Disabled card: This event is triggered if the current card number is not registered in the system yet.

Card expired: This event is triggered if a person, for whom the elevator control effective time is set, punches his/her card beyond the elevator control effective periods and verification fails.

Fingerprint expired: This event is triggered if a person, for whom the elevator control effective time is set, presses his/her fingerprint beyond the elevator control effective periods and verification fails.

Password error: This event is triggered if the verification mode is associated with the password and the password verification fails.

Disabled fingerprint: This event is triggered if the current fingerprint is not registered in the system or has been registered but not synchronized to the device.

Button inactive time zone (press fingerprint): This abnormal event is triggered if a user with the floor opening right presses his/her fingerprint beyond the effective periods of the floor.

Failed to close during passage mode time zone: This abnormal event is triggered if the current floor is in Normally Open state and the button cannot be locked by performing the Remotely Locking Button operation.

Wiegand format error: This abnormal event is triggered if a card is punched and the Wiegand format of this card is incorrectly set.

✍**Note:**

User can self-define the level of each event (normal, abnormal and alarm).

23.4. End user License Agreement

Important Note:

This end-user license agreement (hereinafter referred to as the “Agreement”) is entered into by you (individual, company, or any other entity) and ARMATURA LLC (hereinafter referred to as “ARMATURA”) on the use of this Software (refer to Article 1.1 for definition).

You must be of legal age in your country to view and enter into this Agreement. If you are under legal age, a guardian must enter into this Agreement in your place.

Read this Agreement carefully before using any ARMATURA software or downloading any updates for this Software. By using any ARMATURA software or downloading any updates for this Software, you will be deemed to have accepted all these terms of this Agreement. If you do not accept the terms of this Agreement, do not use any ARMATURA software or download any updates to this Software. You can view this Agreement at any time by visiting the ARMATURA official website (http://www.armatura.us).

I. General Provisions

(I) The “Software” referred to in this Agreement is defined as:

1. Software modules provided to you with ARMATURA equipment, including but not limited to code, other embedded software, documents, interfaces, content, fonts, and any other data protected by the copyright of ARMATURA and its licensors.

2. Updates or upgrades to the Software defined in Article 1.1.1. This does not include updates or upgrade to open-source software modules defined in Article 1.2

(II) ARMATURA software and/or its updates or upgrades may contain software modules that are protected by third-party copyright or contain open-source licenses (hereinafter referred to as “open-source software modules”). These open-source software modules are indicated by the Software’s license information, which displays the license applicable to each module. When using these open-source software modules, you will be subject to the terms and conditions of their individual licenses. This Agreement does not affect any of your rights and obligations under such licenses. If there is any conflict between the licensing provisions outlined in this Agreement with an open-source software module license, the open-source license will prevail.

(III) Unless otherwise specified, the defined Software is bound to the terms of this Agreement, regardless of whether it is stored in read-only memory, any other media, any other form, or in an online location authorized by ARMATURA.

II. End-User License

Subject to the terms and conditions of this Agreement, you have the right to use this Software in a limited, non-exclusive manner (as defined in Article 1.1). This Software may not be sold, transferred, or used for any other commercial purpose.

III. Specific Use Restrictions

(I) Without the express consent of ARMATURA, you may not use its technology or intellectual property to develop software or design, develop, manufacture, sell, or grant licenses for third-party software/accessories associated with ARMATURA software.

(II) You may not distribute or provide this Software to third-parties over a network available to multiple devices or clients at the same time.

(III) Without the written consent of ARMATURA, you may not sell, rent, lease, lend, sublicense, or distribute this Software in full or part to any third-party. However, you may permanently transfer the license to this Software in full, along with the associated ARMATURA equipment, provided that:

1. The transfer must include the ARMATURA equipment and all associated ARMATURA software.

2. You may not store any backups of any ARMATURA software, in full or in part.

3. The party receiving the ARMATURA equipment and software has read and accepted all the terms and conditions of this Agreement.

(IV) Unless expressly permitted, you shall not and shall not allow any other party to copy, reverse engineer, decompile, disassemble, or create derivatives of the Software. You shall not and shall not allow any other party to export the source code from, decode, or modify this Software; any service provided by this Software; or any part thereof.

(V) You agree not to use this Software and its related updates to engage in the following actions:

1. Copy or use any part of this Software outside the scope of this Agreement.

2. Provision of this Software to any third-party in full or in part (including but not limited to the applications, services, code, and source code contained within this service) without the written consent of ARMATURA.

3. Use of this Software in a deceptive manner or for deceptive purposes.

4. Deletion of any copyright notices or prompts contained within this Software.

5. Attempts to destroy, bypass, modify, invalidate, or evade any digital copyright management system related to this Software and/or its integral components.

6. Any other improper or illegal behavior.

(VI) Before saving or copying this Software, you must first obtain authorization from the relevant copyright holder in your country or region. The copy functionality provided by this ARMATURA Software is limited to copying files without copyrights, files for which you have a copyright, or files for which you have obtained authorization or legal permissions to copy. You understand that the ownership and intellectual property rights of any files displayed, stored, or accessed through this Software belong to their respective copyright holders. These files may be subject to copyright laws, other intellectual property laws and treaties, or third-party terms of use. Unless otherwise specified, this Agreement does not grant you any rights to, nor the continued use of such files.

(VII) You agree to comply with all applicable laws and regulations of the country/region in which this Software is stored or being used (including but not limited to the laws of the country/region in which you reside, or download/use this Software from).

IV. All Rights Reserved

ARMATURA and its licensors reserve all rights and entitlements to this Software, including any other rights not expressly granted to you in this Agreement.

V. Privacy Policy

The ARMATURA Privacy Policy (hereinafter referred to as the “Privacy Policy”) provides information related to the data collected by ARMATURA, and how it utilizes such data. During your use of this Software, ARMATURA will collect data in accordance with the provisions of this Agreement and its Privacy Policy.

VI. Use of Data

(I) You agree that ARMATURA and its affiliates/licensors may collect data from your Software to improve its provision of services and products to you. By default, we do not actively collect data from your software, and we may only collect personal data upon your instructions and in compliance with data protection laws.In order to facilitate ARMATURA's provision of software updates, upgrades, product support, and other product services, you agree that ARMATURA and its affiliates/licensors may collect system and application data from your Software. This includes your software name, system and application version, region and language settings, software version, software identification data, network service provider, and IP address. All data is anonymized before collection and processing.

(II) During your use of this Software, collected data may be processed or transmitted to ARMATURA offices, affiliates, or licensors outside your country/region of residence. As such, your data may be transferred to or accessed from jurisdictions outside the country/region in which you are using ARMATURA products or services. These jurisdictions may have differing data protection laws, and may not offer the same protections. ARMATURA warrants that your data will be protected at an adequate level in accordance with all applicable laws and regulations.

(III) ARMATURA will only retain your data within the period of time necessary for the purposes outlined in this Agreement and Privacy Policy, unless longer retention is permitted or required by law. ARMATURA warrants that it will take all appropriate technical and organizational measures to prevent unauthorized access or disclosure of data. You understand, however, that no measures can guarantee absolute security.

VII. Software Updates

ARMATURA may provide you with software updates, though you understand it is under no obligation to do so. Unless accompanied by a separate end-user license agreement, any updates provided by ARMATURA for this Software shall be subject to this Agreement. By deciding not to download updates provided by ARMATURA, you understand and accept that you may be subjecting yourself to serious security risks, and that the Software may become unstable or unusable. Some software functionality may only be available in certain versions. It is recommended to keep the Software up-to-date to ensure the best possible user experience.

VIII. Termination and Continued Validity

(I) This Agreement shall take effect from the day you install this Software. You may terminate this Agreement at any time by permanently deleting, destroying, or returning this Software, including all backup copies and related materials provided by ARMATURA. All corresponding costs shall be borne by you. If you fail to comply with any its terms or conditions outlined in this Agreement, ARMATURA or its licensors have the right to terminate this Agreement at any time and without prior notice. After this Agreement is terminated, you must immediately cease using this Software and delete all related software and materials that have been copied to and/or installed on your ARMATURA equipment or computer.

(II) Articles 6, 9, 10, 11, 12, 14, and 15 shall continue to be effective even after the termination of this Agreement.

IX. Disclaimer

(I) You accept that this Software is provided to you “as is” without any express or implied warranty, and to the maximum extent permitted by applicable laws, ARMATURA and its licensors/affiliates or copyright holders do not provide any express or implied warrants or guarantees. This includes but is not limited to guarantees regarding merchantability, quality, suitability, accuracy, confidentiality, and non-infringement of third-party rights. Neither ARMATURA nor any other party guarantees that the functionality of this Software is suitable to your requirements, nor that its operation will be uninterrupted or without error. By opting to use this Software to obtain a specific result, all responsibilities and risks associated with its install and use shall be borne by you.

(II) Installing this Software may affect the availability of third-party software, applications, or services. ARMATURA does not guarantee that the functions or services contained within this Software will meet your requirements, nor does it guarantee that the Software and its services will be without error, lack bugs, or provide continuous and lasting services. Furthermore, ARMATURA does not guarantee that this Software will be compatible with any third-party software or service.

(III) You understand that ARMATURA’s software and services are not suitable for certain applications, including but not limited to operation of nuclear energy facilities, aircraft navigation and communication systems, air traffic control systems, and life support or weapon systems. Errors or time delays in ARMATURA software in these situations may lead to personal injury, death, or serious physical and environmental damage.

X. Limitation of liability

(I) ARMATURA does not assume any responsibility for problems that may result from the misuse or unauthorized modification of the Software.

(II) To the extent not expressly prohibited by applicable laws, ARMATURA and its employees, licensors, and affiliates are not liable for the compensation of any profit loss, sales loss, data loss, cost of purchasing alternative goods or services, property damage, personal injury, business interruption, business information loss; or any special direct, indirect, incidental, economic, punitive, or ancillary damages regardless of theory of liability (contract, tort, negligence, or other), even if they were aware of the possibility of such damages. Certain jurisdictions do not allow the limitation of liability for personal injury, incidental, or consequential damages. As such, these limitations may not apply to you.

(III) The total damages for which ARMATURA may be liable to you shall not exceed the price you paid for the purchase of its equipment/software (excluding cases of personal injury or death due to negligence by ARMATURA, subject to applicable laws and regulations).

(IV) The laws of certain countries/regions do not allow Agreements to exclude or limit certain warrants, guarantees, or liabilities. If these laws apply to you, some or all of the limitations outlined in this Article may

not apply to you. No provision outlined in this Agreement affects your legal rights as a consumer, and these rights cannot be modified or waived through your acceptance of this Agreement.

XI. Technical Support

ARMATURA has no obligation to provide you with any technical support services for this Software outside of those required by law. No verbal and written information or advice given by a ARMATURA authorized representative shall constitute a warranty. Should ARMATURA software or services prove defective, you assume the entire cost of all necessary repairs or corrections.

XII. Export Control

Unless otherwise authorized by applicable laws and relevant regulations in ARMATURA's resident jurisdiction, you may not use, export, or re-export ARMATURA software.

XIII. Contact Method

If you have any questions, comments, or suggestions, you may contact ARMATURA at (470) 816-1970 by phone or info@armatura.us by email.

XIV. Dispute Resolution and Applicable Law

The verification, interpretation, modification, performance, and dispute resolution of this Agreement is governed by the laws of the state of Georgia, without regard to conflict of law provisions. You accept that this Agreement will be considered to have been signed in Atlanta, GA. In the event of any dispute concerning the content or performance of this Agreement, both parties shall endeavor to resolve the dispute through amicable negotiation. If the dispute cannot be resolve through amicable negotiation, either party may submit the dispute to the people's court with jurisdiction over the location this Agreement was signed for litigation.

XV. Entire Agreement

This Agreement constitutes the entire agreement between you and ARMATURA in regards to the use of this Software, and will replace any previous agreement between you and ARMATURA in regards to the aforementioned. You may be subject to other applicable terms and conditions during use or purchase of open-source software, third-party content, or other services from ARMATURA.

23.5. Personal Information Protection and Privacy Policy

This Policy only applies to ARMATURA ONE products or services of ARMATURA ONE, including ARMATURA ONE Server, ARMATURA ONE Mobile APP.

Last update: February 2022

If you have any question, comment or suggestion, please contact us via the following means:

Email: info@armatura.us

Biometric Privacy Notice:

This software application allows customers to store and manage biometric data associated with registered individuals interacting with the software and connected biometric devices.

Note that a person's biometric data is considered as personal identification information. As such, a person's biometric data is protected under the governing laws of the country and state/province wherever the person's biometric data is recorded. Prior to customers operating the software, customers should first ensure they have the legal right to record their users' biometric data. Customers intending to store & match their users' biometric data should first inform their users of the customer's intention and gain their users' permission prior to enrolling their users' biometric data in the software.

This Policy will help you understand the following:

- Personal information collection rules
- How we protect your personal information
- Your rights
- How we handle personal information of minors
- How this Policy is updated
- How to contact us

ARMATURA LLC and its affiliates (hereinafter referred to "ARMATURA", or "Company" or "We") understands the importance of personal data and will do everything possible to protect your personal information. We are committed to preserving your trust in us by protecting your personal information based on the following principles: responsibility in accordance with authority, purpose specification, informed consent, minimal necessary, security safeguard, subject participation, openness and transparency, etc. ARMATURA also commits to protect your personal information by implementing appropriate security measures in accordance with industry accepted security standards.

Before using any products (or services), please read this Policy carefully and make sure you have fully understood and agreed to this Policy. By using any products or services, you acknowledge that you have fully understood and agreed to this Policy.

Definitions

1.ARMATURA ONE Services refers to services developed and operated by the ARMATURA ONE platform to improve the management of ARMATURA ONE modules, including personnel, access control, elevator (DCS), visitors, building automation, intrusion, video and system management.

These services can be deployed in the cloud as well as on local servers, including websites, products, offline software, and mobile devices (apps).

2.ARMATURA ONE Service Provider refers to ARMATURA, the company that developed and provides ARMATURA ONE services.

3.Personal Information refers to information recorded electronically or otherwise that can be used alone or in combination with other information to identify the identity and activities of a particular natural person. Such information includes name, mobile phone number, ID number, email address, personal biometric information (e.g., face, fingerprint, palm information), employment information (employee number), corporate information (corporate name and business identification number), and personal information of children under age 14 (inclusive).

4.Personal Information Controller refers to an organization or individual that has the authority to determine the purpose and manner of handling personal information. The personal information controllers referred to in this agreement are corporate/organizational users of ARMATURA ONE products.

5.Local Server refers to the enterprise/organization which allocates and authorizes access to and use of computers or devices on which ARMATURA ONE product are installed. That is, the enterprise/organization controls the personal information and data stored on the local server.

I. Personal information collection rules

(1) Which of your personal information will be collected by us

We will collect and use your personal information for the following purposes:

1.To Help You Activate ARMATURA ONE Services.

To register and activate these services, you must provide basic information such as your continents, country/region, city, company name, industry, personal contacts, mobile phone, email address and dealer name, so that we can provide you with services related.

2.Providing You With ARMATURA ONE Services.

1) Information Provided by You

In using our services, you may provide feedback to help us better understand your experience and needs, so as to better improve our services.

2) Information We Collect During Your Use of the Service

To provide you with services, pages, and search results that better meet your needs; understand product suitability; and identify any issues with your account, we will collect information about the products and/or services you use, along with how you use them. This information includes:

Device Information: We receive and record information about the device you are using (e.g., device model, operating system version, device settings, unique device identifier, and other hardware and software characteristics), the location of the device (e.g., IP address, GPS location information, Wi-Fi connections, Bluetooth, and base stations that can provide relevant information) based on the specific permissions you granted during the installation and use of the software.

Log Information: When you use products or services provided by our website or client end, we will automatically collect detailed use information of our services and save them as relevant web logs. For example, your search and query content, IP address, browser type, language used, date and time of visit, and the records of webpages visited.

Separate device and log information cannot be used to identify particular natural person.

If we combine such non-personal information with other information to identify a specific natural person, or use this information in combination with personal information, such non-personal information will be treated as personal information during the combined use. We will anonymize and de-identify such personal information unless we obtain your authorization or are otherwise required by laws and regulations.

When you contact us, we may save your communication or call records, content, or contact information to better help you solve the problem, contact you in the future, or to help us solve related problems.

3. Security

To prevent, detect, and investigate fraud, infringement, breach of security, unlawfulness, or violations of agreements, policies, or rules with us and/or our partners, we may collect or integrate your user information, service usage information, device information, log information, and information that we and/or our partners have obtained your authorization to share or that is shared under the law.

If we cease to operate ARMATURA ONE services, we will promptly cease the continued collection of information about you and your employees and visitors, and will delete or anonymize your personal information in our possession.

(2) How we use your personal information

Your information is collected to provide you with services, and to improve the quality of those services. To this end, we will use your information for the following purposes:

1. To provide you with ARMATURA ONE products or services, and to maintain, improve, and optimize these services and your user experience.

2. To prevent, discover, and investigate fraud, infringement, acts endangering security, violations of laws and our agreements, policies, or rules, and to protect you, other users, or the public, along with us and our legitimate rights and interests, we may use or integrate your user information, service use information, device information, log information and information that was obtained by us, our partners, or shared under the law to comprehensively determine risks of your account and transactions, verify identities, detect and prevent security incidents, and take the necessary recording, auditing, analyzing, and disposing measures according to relevant laws.

3. We may process your information or combine it with information from other services for the purpose of providing you with a more personalized service, such as to recommend content that may be of interest to you, including but not limited to sending you information about ARMATURA ONE services, presenting you with personalized third-party promotions through the system, or sharing information with ARMATURA ONE partners with your consent so that they may send you information about their products and services.

(3) How we use Cookies and similar technologies

1. Cookies

Cookies and similar technologies are widely used in the Internet. To ensure the smooth operation of our website, we will store a small data file named Cookie in your computer or mobile device. A Cookie typically contains identifiers, site names, and some numbers and characters. With the Cookie, our website can store your preference and other data. We will not use Cookies for any other purpose than that specified in this Policy. You may manage the Cookie according to your own preference or delete it. You may choose to delete all Cookies saved in your computer, and most of the web browsers have a feature to block the Cookies. But if you do this, you will need to change the user settings each time you visit our website.

2. Other similar technologies

In addition to Cookies, we will also use other similar technologies such as website beacons and pixel tags on our website to help us understand your preference for products or services and improve our customer service.

(4) How we share, transfer and disclose your personal information

1. Share

Without your explicit consent, we will not share your personal information with any other company, organization and individual.

We may share your personal information with an external institution if required by laws and regulations or government authorities.

2. Transfer

We will not transfer your personal information to any other company, organization or individual, except under the following circumstances:

a) Transfer with your explicit consent: with your explicit consent, we will transfer your personal information to other parties;

b) If any merger, acquisition or bankruptcy process involves transfer of your personal information, we will request the new company or organization in possession of your personal information to continue to be bound by the personal information protection policy, or we will request the new company or organization to seek your permission again.

3. Public disclosure

We will only disclose your personal information in the following circumstances:

a) With your explicit consent;

b) Law-based disclosure: we may disclose your personal information in cases where such disclosure is required by laws, legal proceedings, litigation or government authorities, including in cases:

- Related to personal information controller's performance of obligations prescribed by laws and regulations;
- Directly related to national security or national defense security;
- Directly related to public safety, public health or vital public interests;
- Directly related to crime investigation, prosecution, trial and judgment execution;
- Where such disclosure is necessary for protecting the vital legitimate interests such as life and property of the subject of personal information or any other individual while it is difficult to obtain the consent therefrom;
- Where the personal information involved is disclosed to the public by the subject itself;

- Where such disclosure is necessary for signing and performing the contract concerned according to the requirements of the subject of personal information;
- Where the personal information is collected from legally and publicly disclosed information, such as legal news reports and publicized government information;
- Where such disclosure is necessary for maintaining safe and stable operation of the products/services provided, such as identification or disposal of failures of products/services;
- Where the personal information controller is a news agency and such disclosure is necessary for legal news reporting;
- Where the personal information controller is an academic research institute, and such disclosure is necessary for statistics or academic research in the public interest, and the personal information contained in the results of academic research or description provided externally is de-identified.

Please note that according to law, sharing, transferring or disclosing personal information does not include the scenario in which personal information is de-identified in such a way that the recipient of such information cannot restore the information or re-identify the subject of personal information before it is shared, transferred, or disclosed. As a result, we may store or process such information without notifying you or obtaining your consent.

II. How we protect your personal information

If you are an administrator of an enterprise organization, we will not collect personal information submitted by individual users under your enterprise/organization when you use ARMATURA ONE. For personal information leakage problems, you should look for your company/organization. Relevant data is collected and stored in a software database of your enterprise/organization. Enterprise/organizational control data may include:

(1) Your position, subordinate department, public mailbox account, office phone number and other information assigned to you by your enterprise/organization, and as you to complete enterprise/organization activities asked to provide or produce fingerprint features, facial features,palm features, face images, personal information such as location, and consumption records, visitor information, etc.

(2) Other data submitted by enterprise/organization users containing your personal information (including employment information, contact information, personal identity information, etc.).

You understand and agree that the enterprise/organization is the controller of the aforesaid enterprise data, and the operation, management and use of the aforesaid services and the processing of your personal information/data by the enterprise/organization has nothing to do with the ARMATURA ONE team. The enterprise/organization shall ensure that the express consent of the individual users of ARMATURA ONE has been obtained in advance. Only end user information necessary for enterprise operation and management is collected, and end users are fully informed of the purpose, scope and usage of relevant data collection.

(3) Information provided to us by third parties:

We will collect information about you from other users when they perform operations related to you. We may also obtain your personal data from affiliated companies of ARMATURA ONE, cooperative third parties or other legal means. For example, in order to protect your legitimate rights and interests, prevent fraud, gambling and other risks, and maintain the safe and stable operation of ARMATURA ONE services, we need to obtain the user identification information.

(4) Despite our security measures, the Internet environment is not 100% safe. Please be aware that there is no "perfect security measure" on the Internet, but we will try our best to ensure safety of your information.

III. Your rights

In accordance with U.S. laws, regulations, standards, and established practices of other countries and jurisdictions, we will protect your rights to:

(1) Access your personal information

You have the right to access your personal information, unless otherwise provided by laws and regulations. You may access your personal information by contacting your enterprise/organization administrator.

For other personal information generated during your use of our products or services, if you want to exercise your right to access your personal data, please send an email to your enterprise/organization administrator.

(2) Correct your personal information

Upon noticing any of your personal information we processed is wrong, you have the right to request us to make corrections. You may submit the request via means listed in Item "(1) Access your personal information".

(3) Delete your personal information

In the following cases, you may request your enterprise/organization to delete your personal information:

1. The enterprise/organization process your personal information in violation of laws and regulations;
2. The enterprise/organization collect or use your personal information without your consent;
3. The enterprise/organization process personal information in violation of the agreement with you;
4. You can no longer use our products or services, or you want to canceled your account;

In circumstances prescribed by applicable laws, you have the right to revoke your consent to your enterprise/organization processing of your personal data at any time. However, the cancellation will have no bearing on the legality and effectiveness of your personal data that your enterprise/organization previously processed with your consent, or other appropriate legitimacy.

(4) Respond to your request

To safeguard security, you may need to provide a request in writing or otherwise prove your identity. Your enterprise/organization may ask you to provide proof of your identity before processing your request.

You enterprise/organization may not respond to your request in the following circumstances:

1. The request is related to personal information controller’s performance of obligations prescribed by laws and regulations;
2. The request is directly related to national security or national defense security;
3. The request is directly related to public safety, public health or vital public interests;
4. The request is directly related to crime investigation, prosecution, trial and judgment execution;
5. The personal information controller has sufficient evidence that the subject of personal information is subjectively malicious or abusing his/her rights;
6. Not responding to the request is for protecting the vital legitimate interests such as life and property of the subject of personal information or any other individual, while it is difficult to obtain the consent therefrom;
7. Responding to request of the subject of personal information will bring serious damage to the legitimate rights and interests of the subject or any other individual or organization; or

8. The request involves trade secrets.

IV. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

V. How this Policy is updated

Our personal information protection and privacy policy is subject to change from time to time.

Without your explicit consent, we will not cut your rights you are entitled to under this Policy. We will post any change to this Policy on our website.

For major changes, we will also provide a more prominent notification (for some services, we will send notice via email, stating the particulars of changes to this Policy).

Major changes referred to in this Policy include, but are not limited to:

1. Major changes of our service model, such as change of purpose, type or way of use of personal information;

2. Major changes in ownership structure or organizational structure, such as changes caused by business adjustment, bankruptcy, merger and acquisition;

3. Change of the party with which we share personal information or to which we transfer or disclose personal information;

4. Major changes in your rights of participating in the handling of personal information or the way you exercise such rights;

5. Changes of the department responsible for personal information security, or of the contact information or of the channel for filing a complaint;

We will also archive the previous versions of this Policy for your reference.

VI. How to contact us

If you have any question, comment or suggestion about this Policy, please send an email to info@armatura.us. Normally, we will reply within 30 days. More contact information is available on our website (http://www.armatura.us).

23.6. Create a PWAs APP

Browser Requirements

Microsoft Edge Browser

Version Requirements

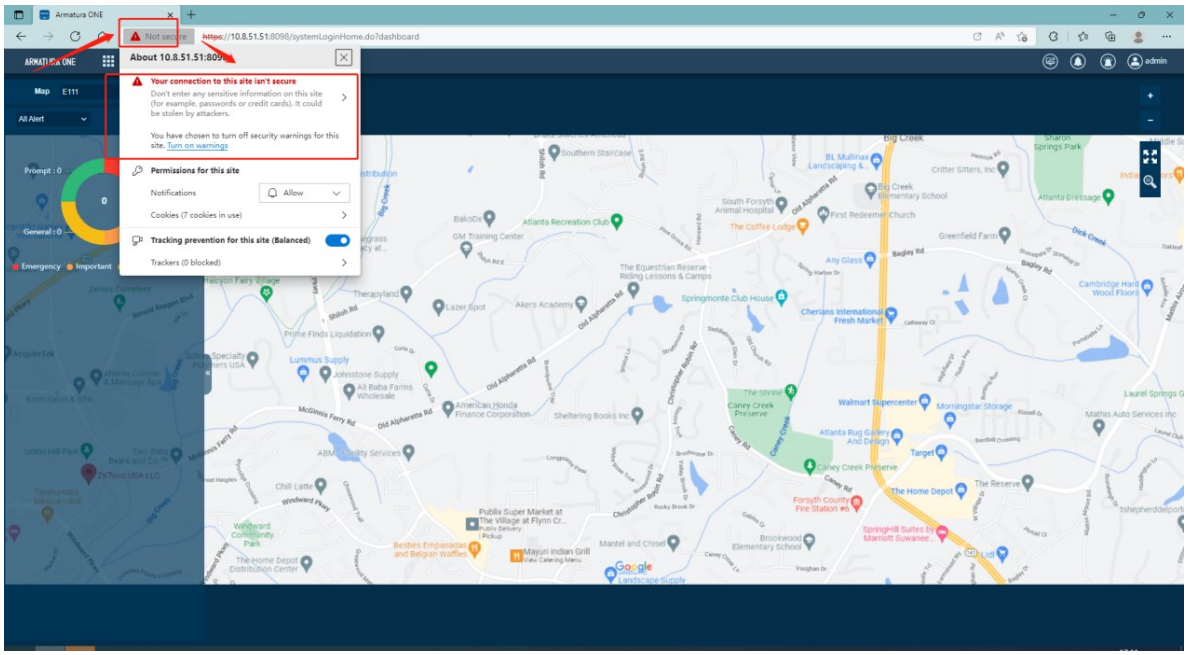
Latest than 88.0.705.53

23.6.1. Install PWAs

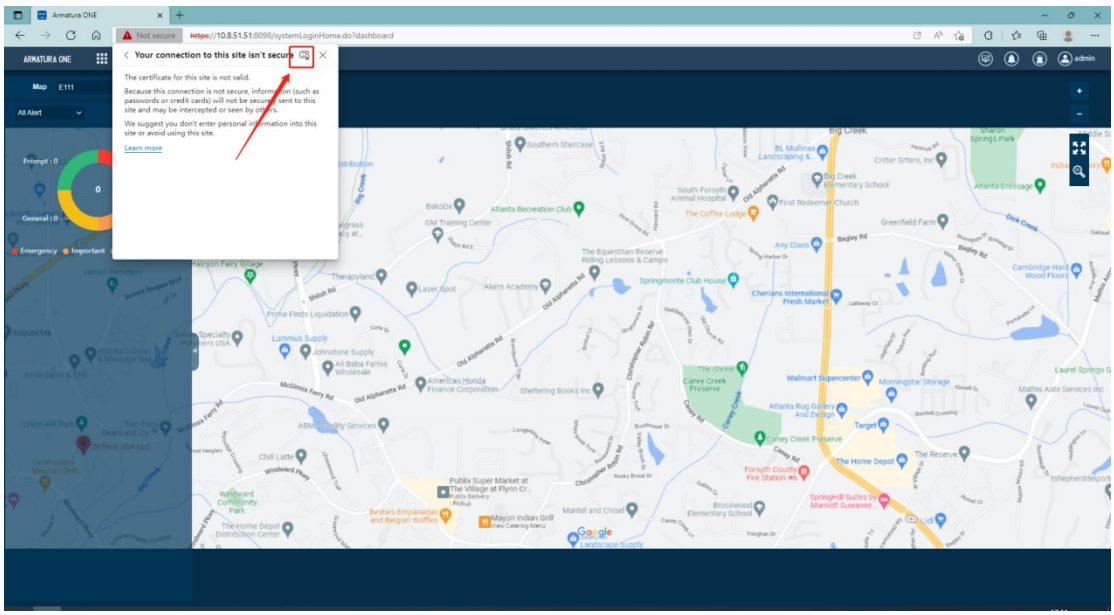
Step：

1. Click the ‘Not secure’ warning next to the URL.

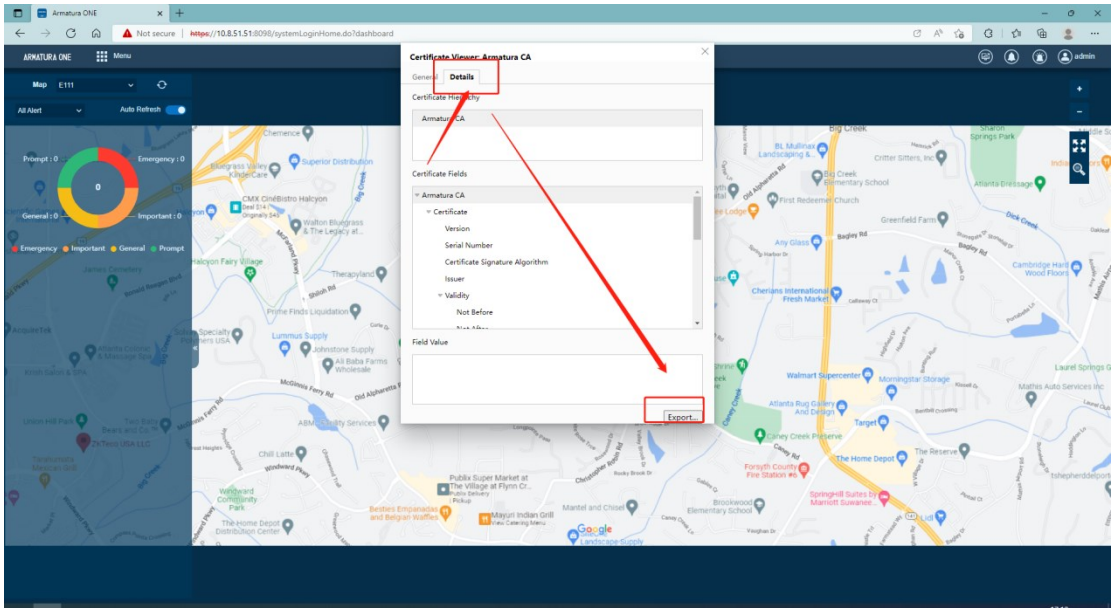
2. Click the ‘Your connection to this site is not secure’



3. Click the certificate’s icon.



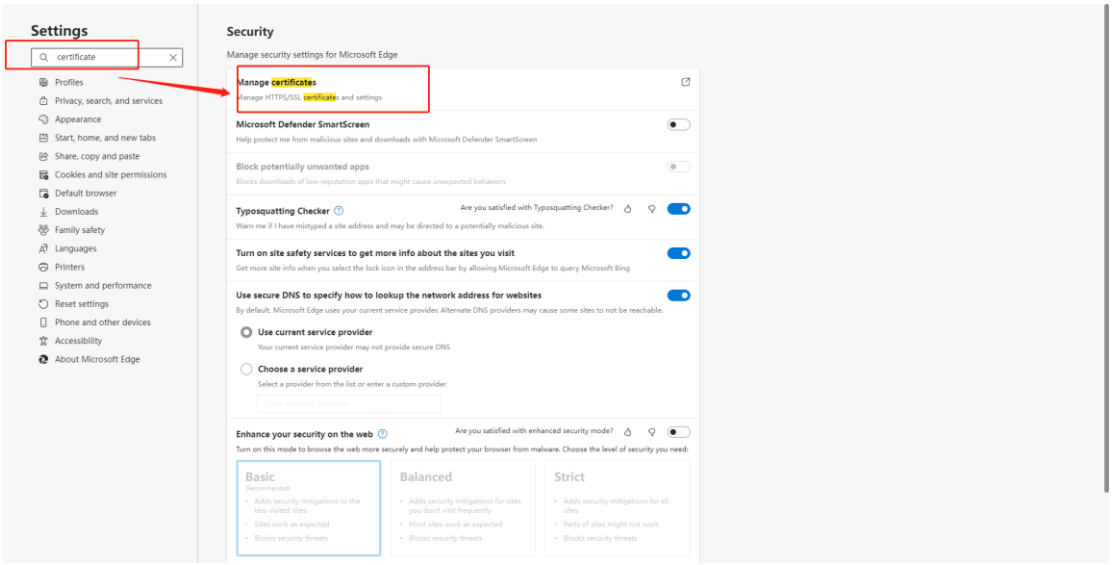
4. Select ‘Details’ and click ‘Export’ to save the certificate to your computer.



5. Open your browser.

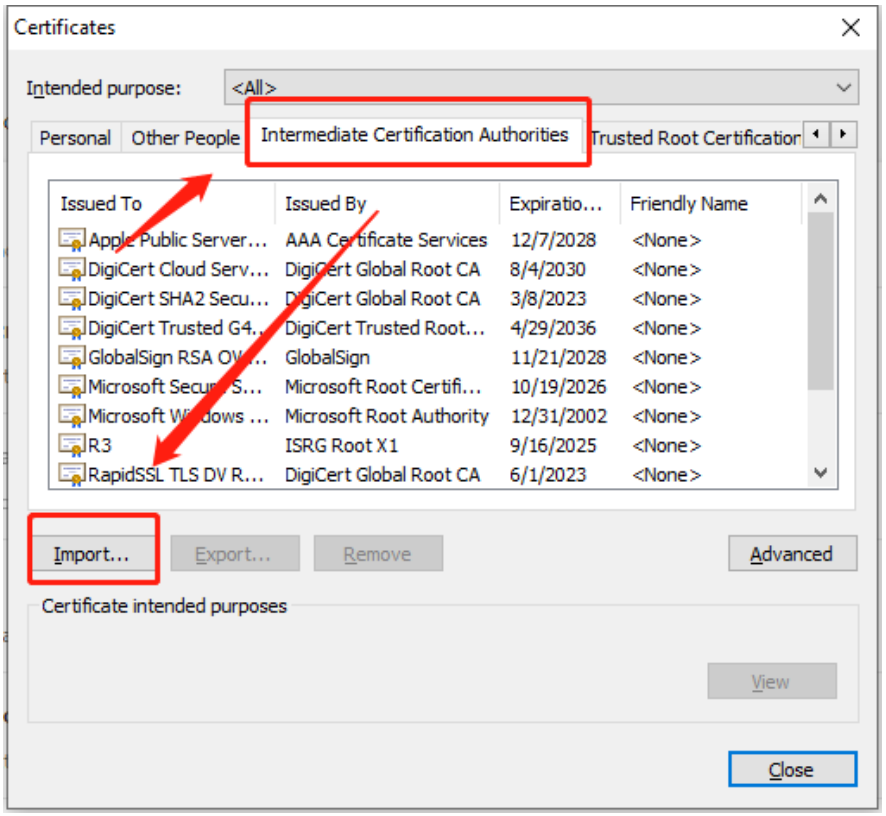
6. Click the ‘Settings’ and search for ‘Certificates’

7. Click the ‘Manage Certificates’

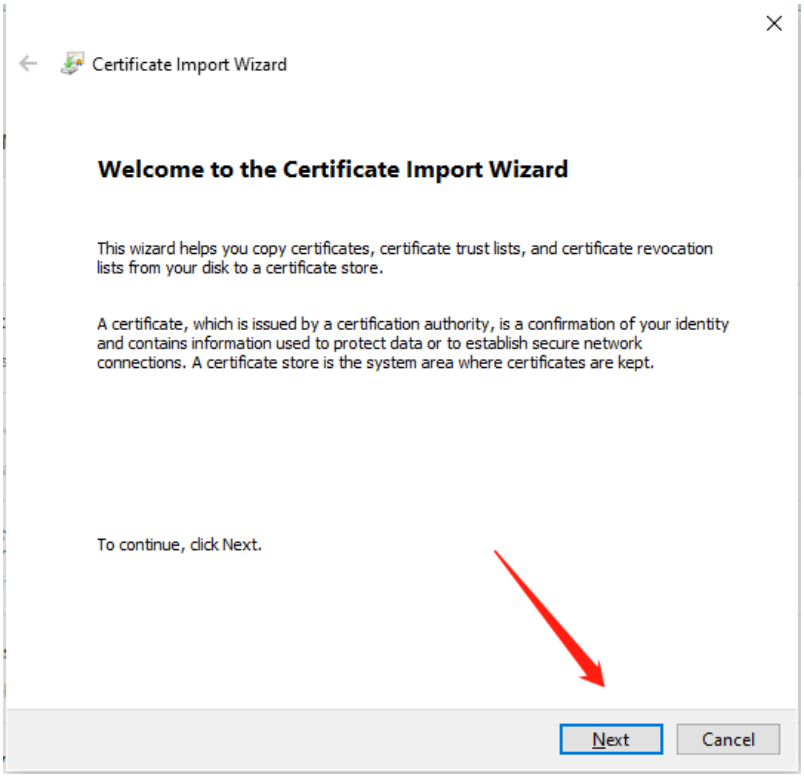


8. Click the ‘Intermediate Certification Authorities’

9. Click ‘Import’

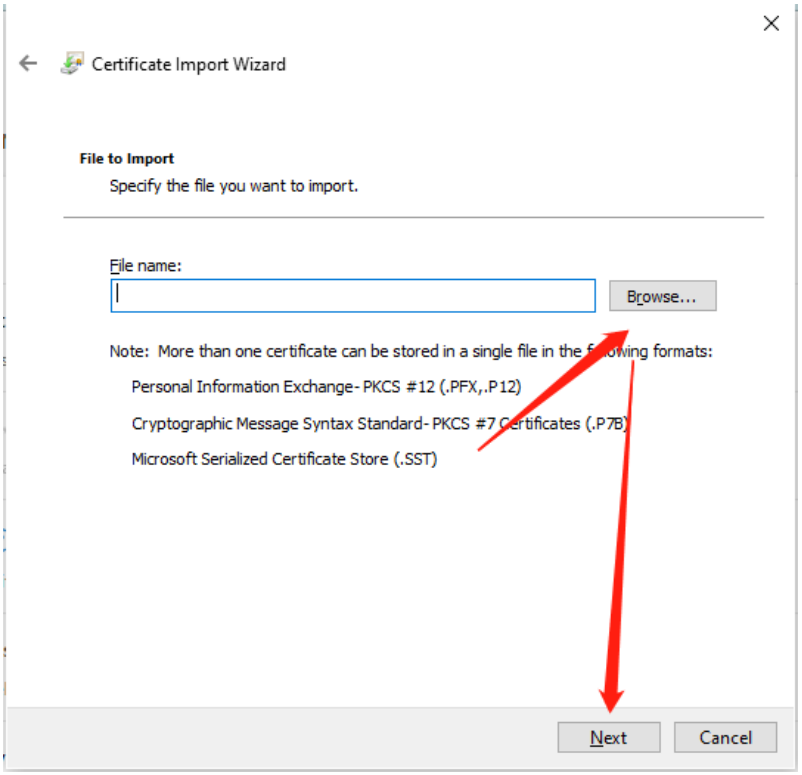


10. Select “Next”

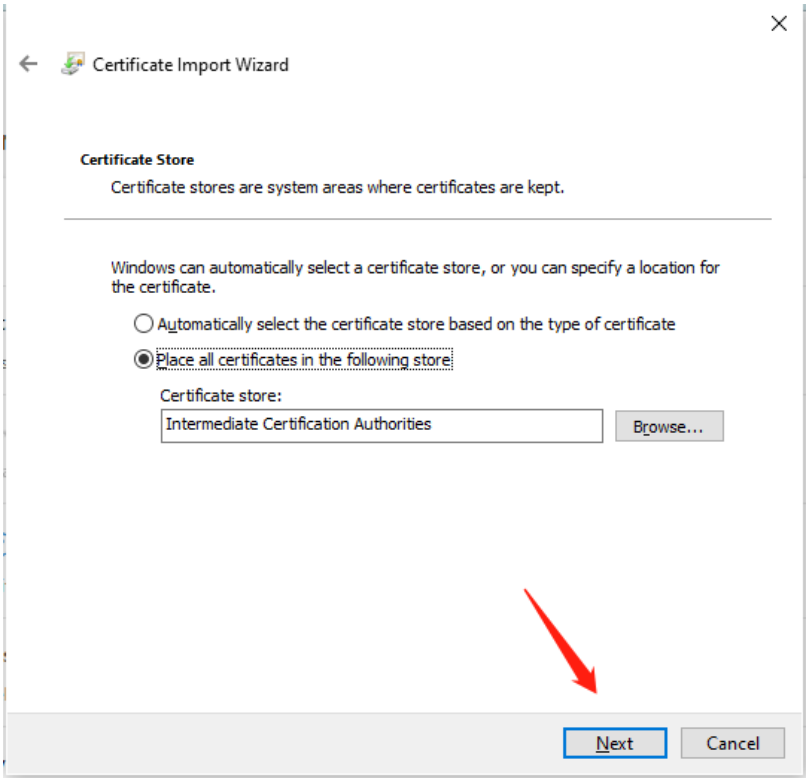


11. Click ‘Browse’ and select the address where you downloaded the certificate.

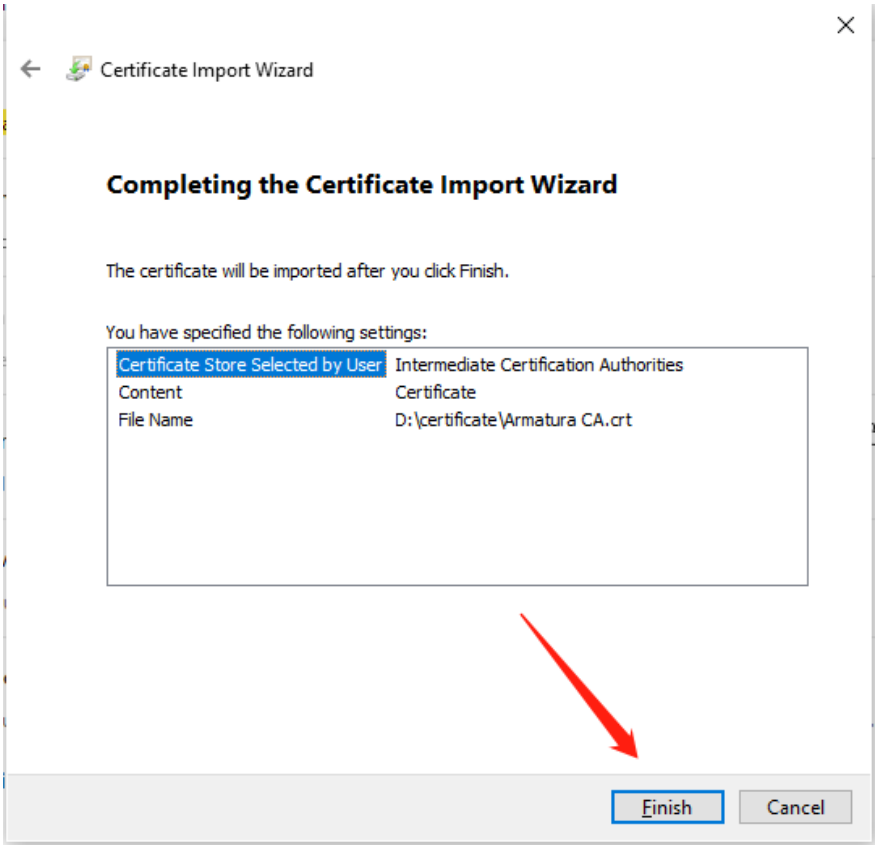
12. Select ‘Next’



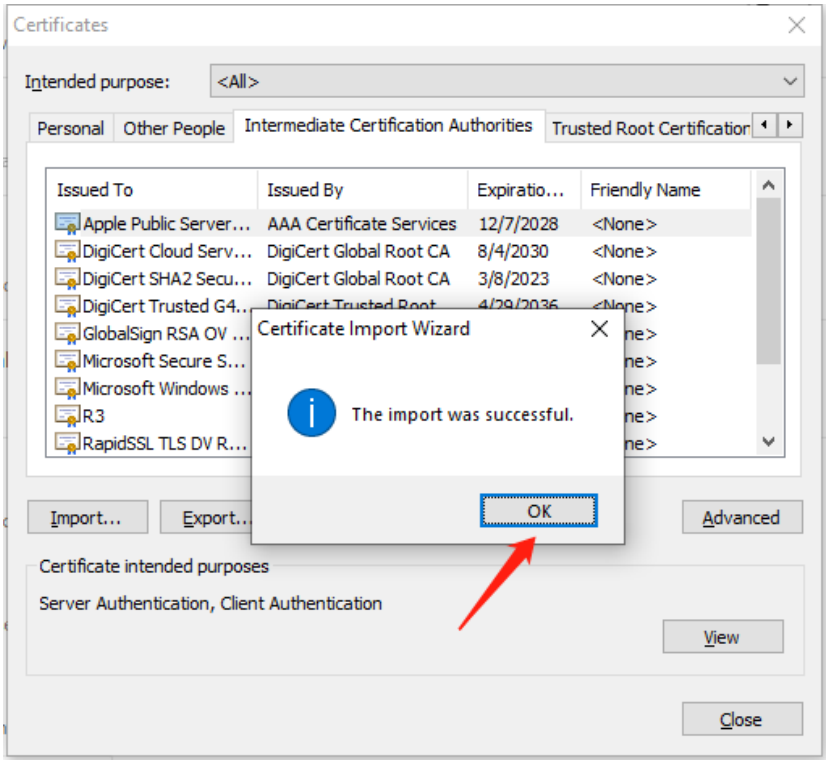
13. Select ‘Next’



14. Click ‘Finish’

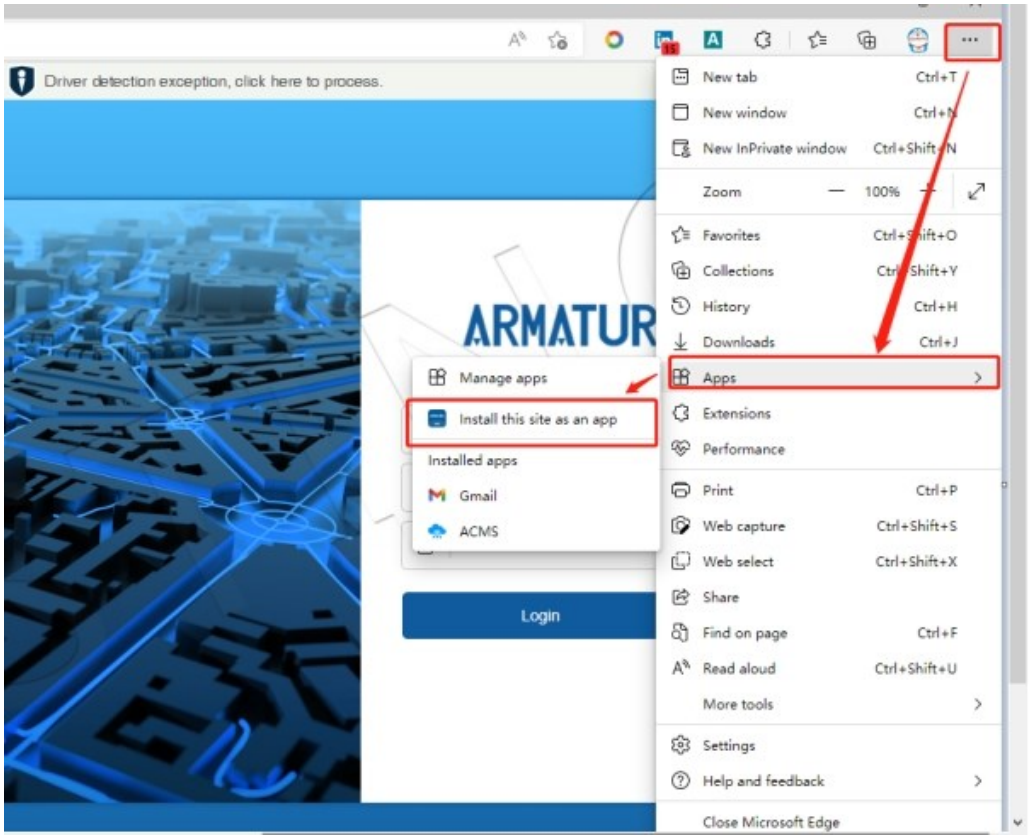


15. The certificate import was successful.

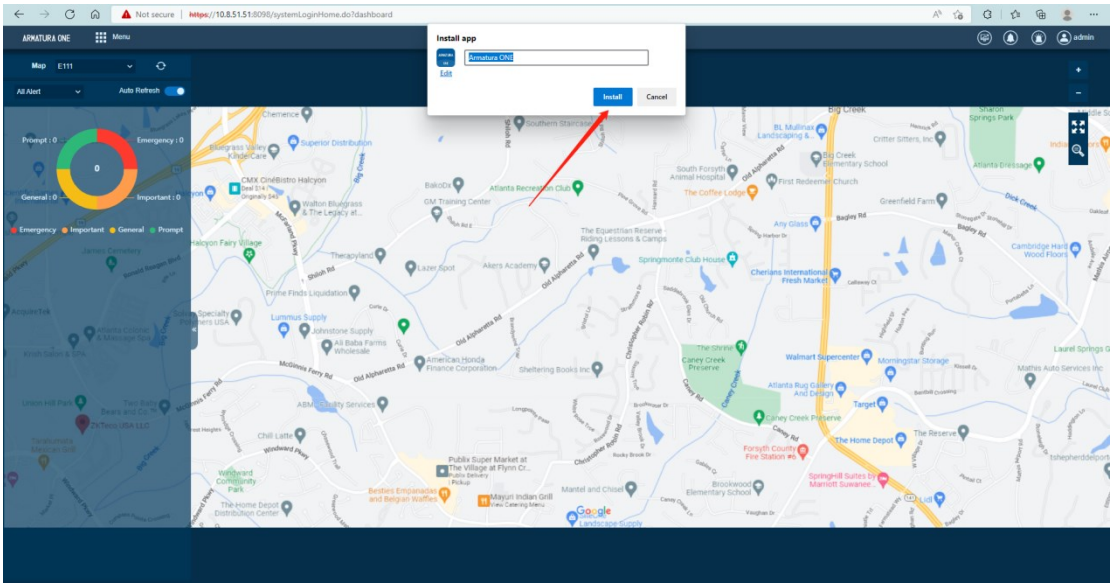


16. Select ‘apps’ in your browser’s settings.

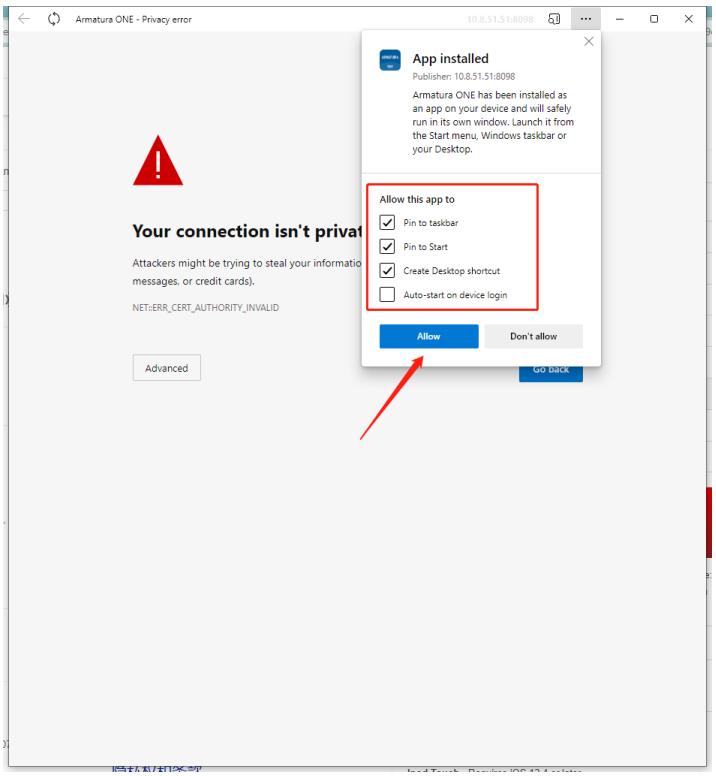
17. Click the ‘Install this site as an app’



18. Click install.

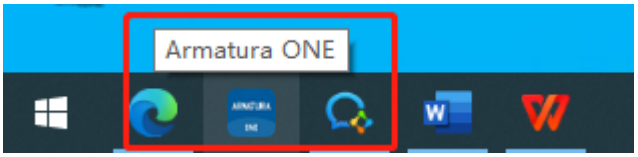


19. After the installation is successful, make the relevant settings for the app.

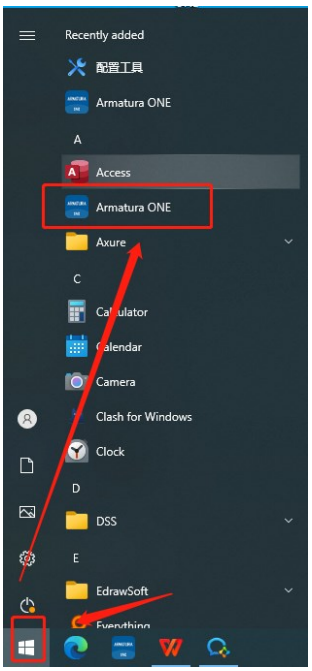


The software settings are as follows:

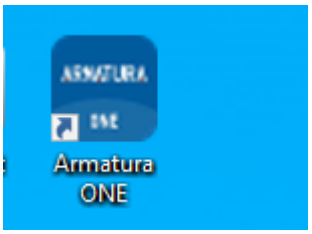
(1) Pin to taskbar.



(2) Pin to start.



(3) Create Desktop shortcut.



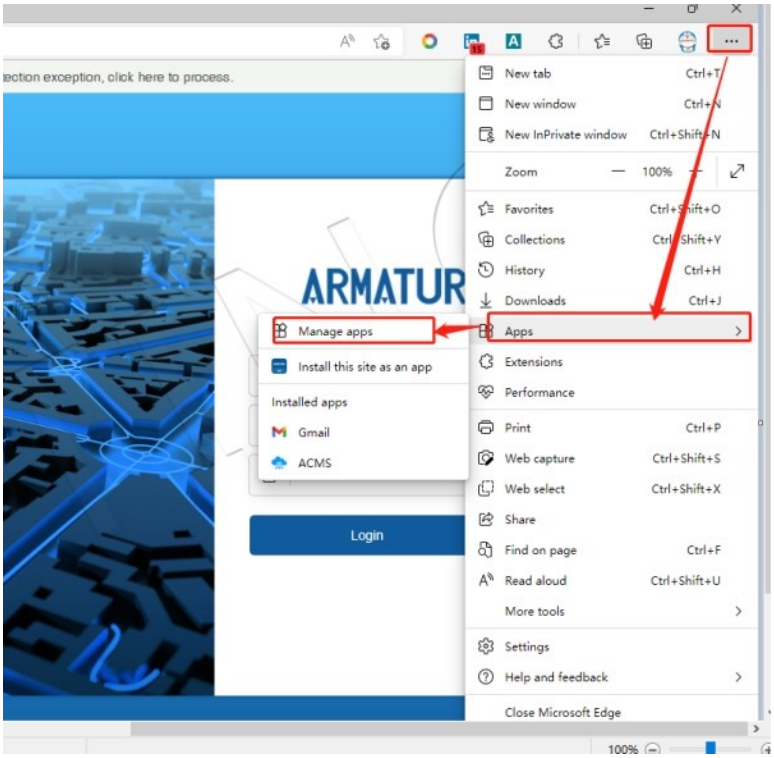
(4) Auto-start on device login.

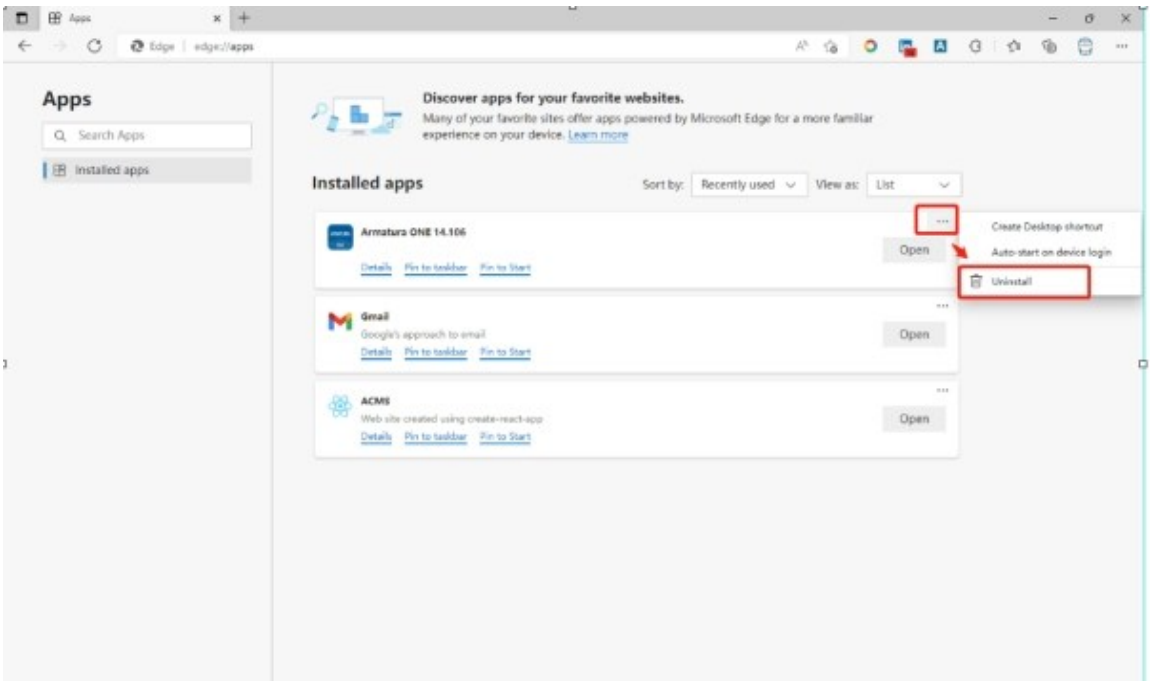
The software opens automatically after booting.

20. Finish.

Click on the steps below to open the software.

23.6.2. Uninstall Application





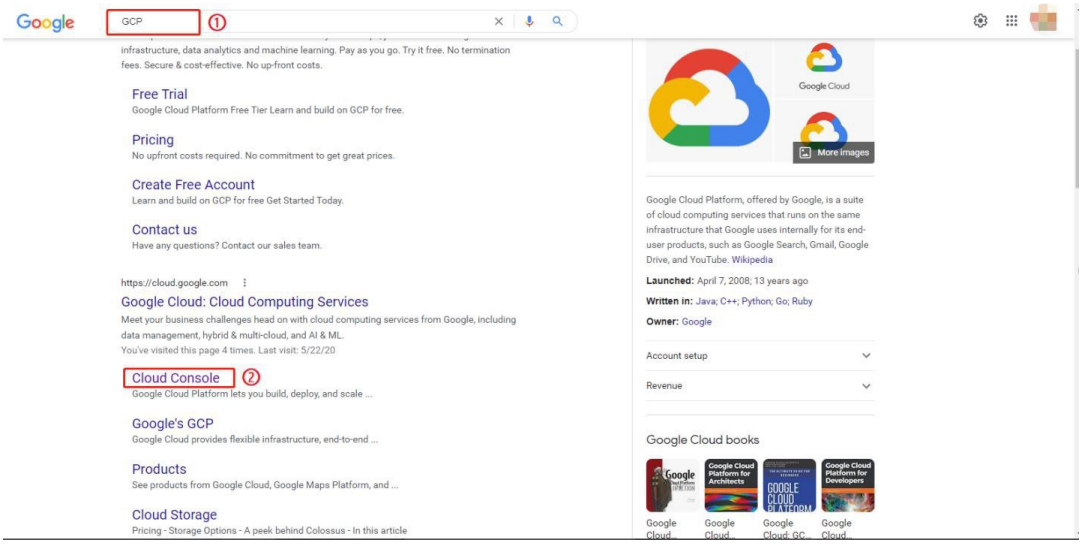
23.7. How to get Google Maps API Key

Precondition:

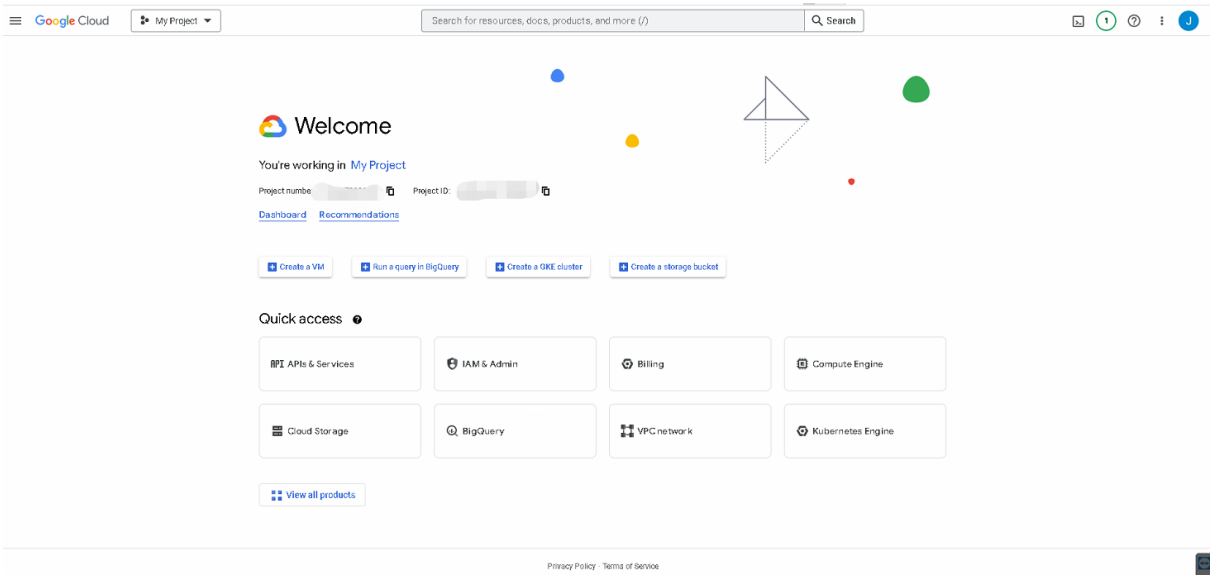
An international credit card is needed, such as MasterCard or VISA, and bonded to Billing.

Step：

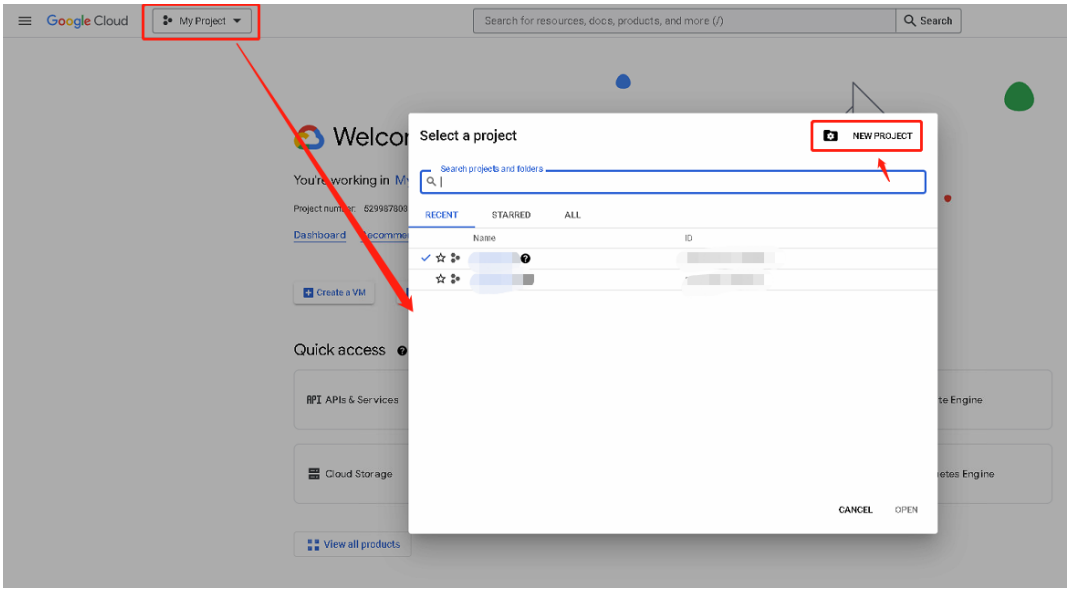
1. Use browser to visit https://console.cloud.google.com/ or search ‘GCP’ in google to get link.

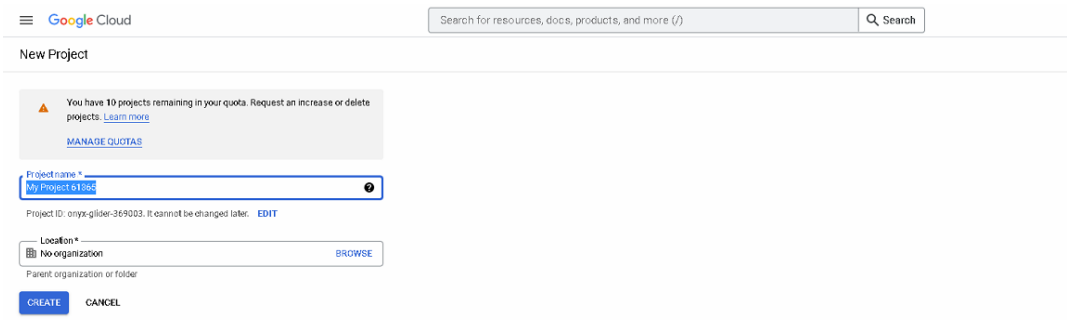


2. Login in your Gmail account.

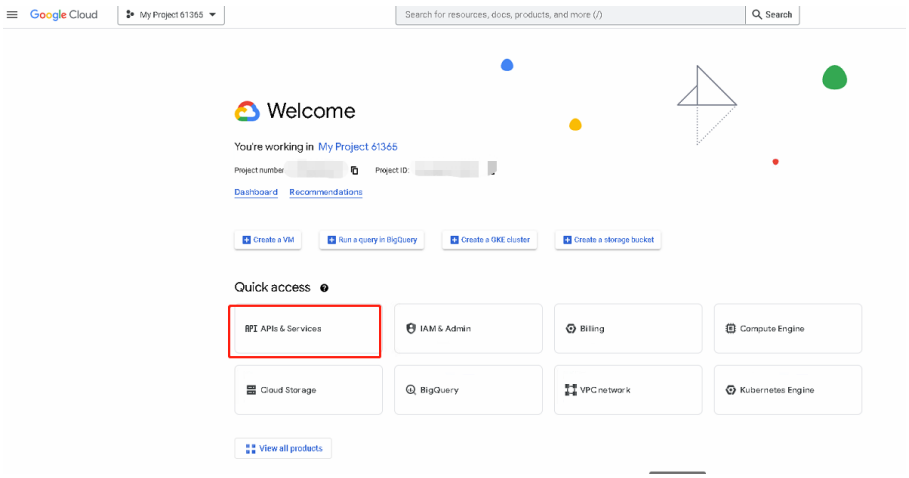


3. Create a new project as shown in the figure below.

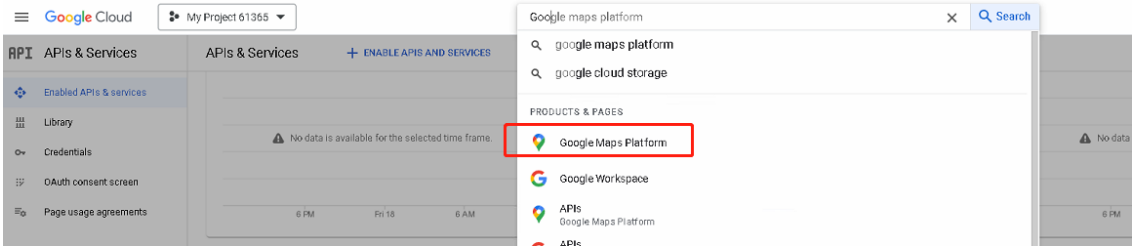




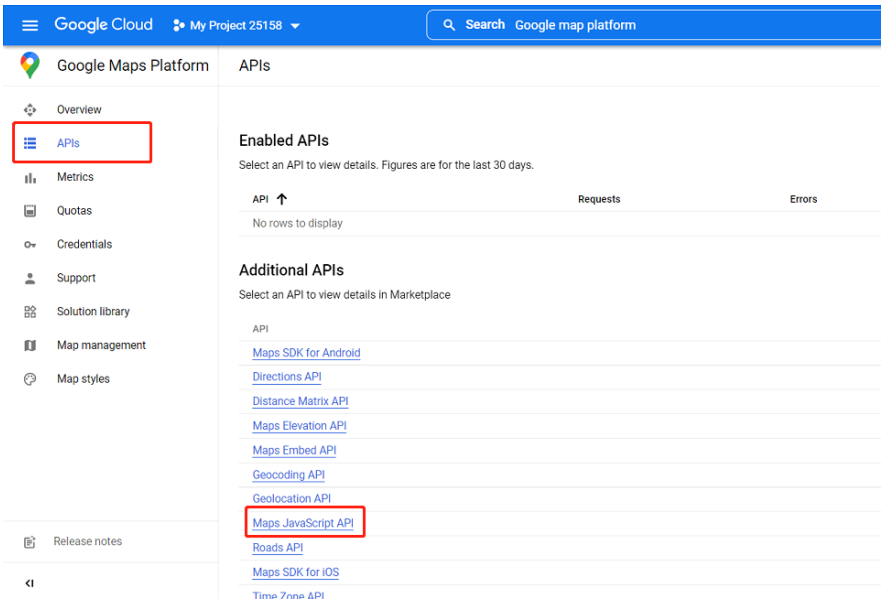
4. After creating, find **APIs &Services** in **Quick Access**



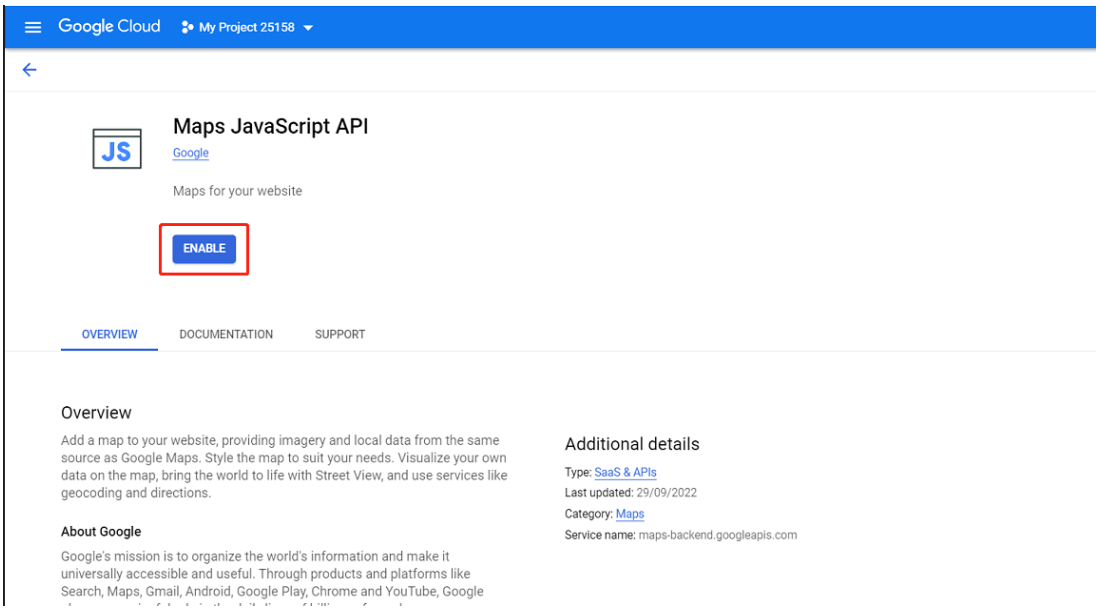
5. Search **Google Maps Platform** in header search bar



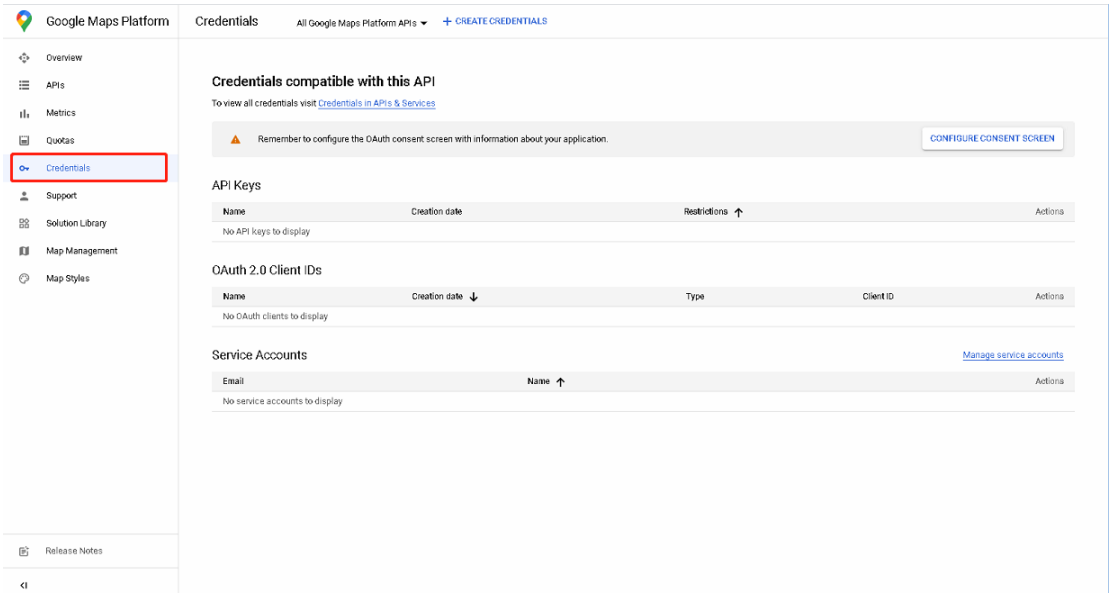
6. Click APIs on the left menu, select Maps JavaScript API



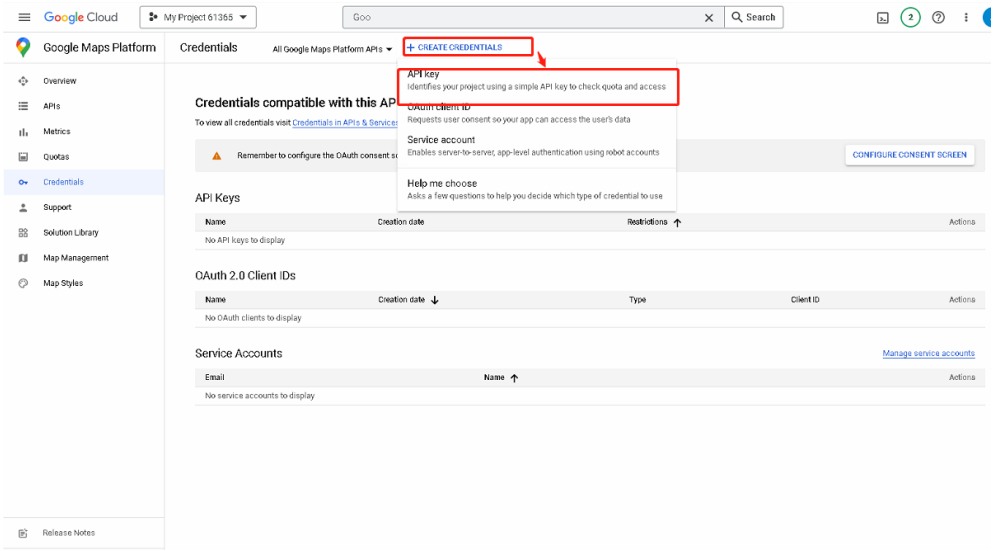
7. Click **Enable**



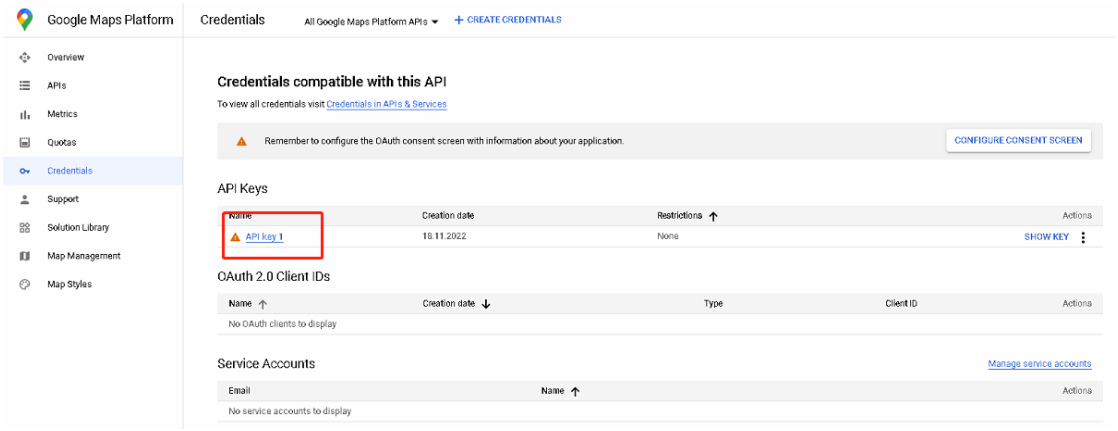
8. Back to previous page and find **Credential** in left menu



9. Click **Create Credential**, select **API Key**

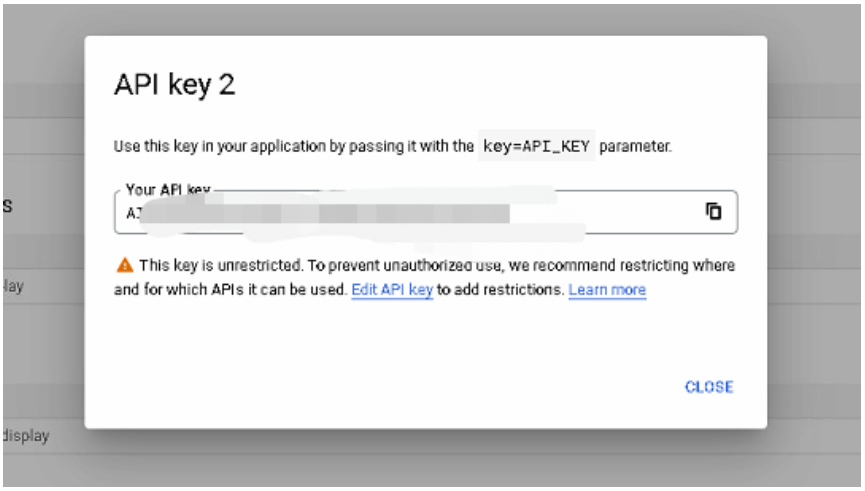


10. After Created, there will be an API Key show in table

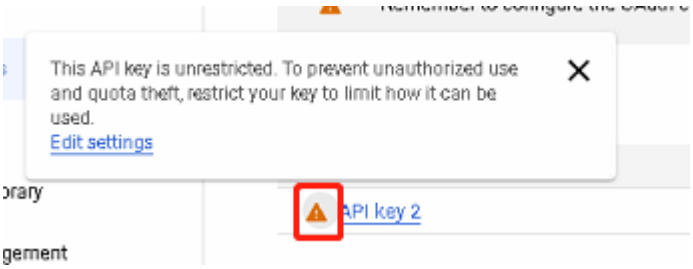


11. Click **Show Key**

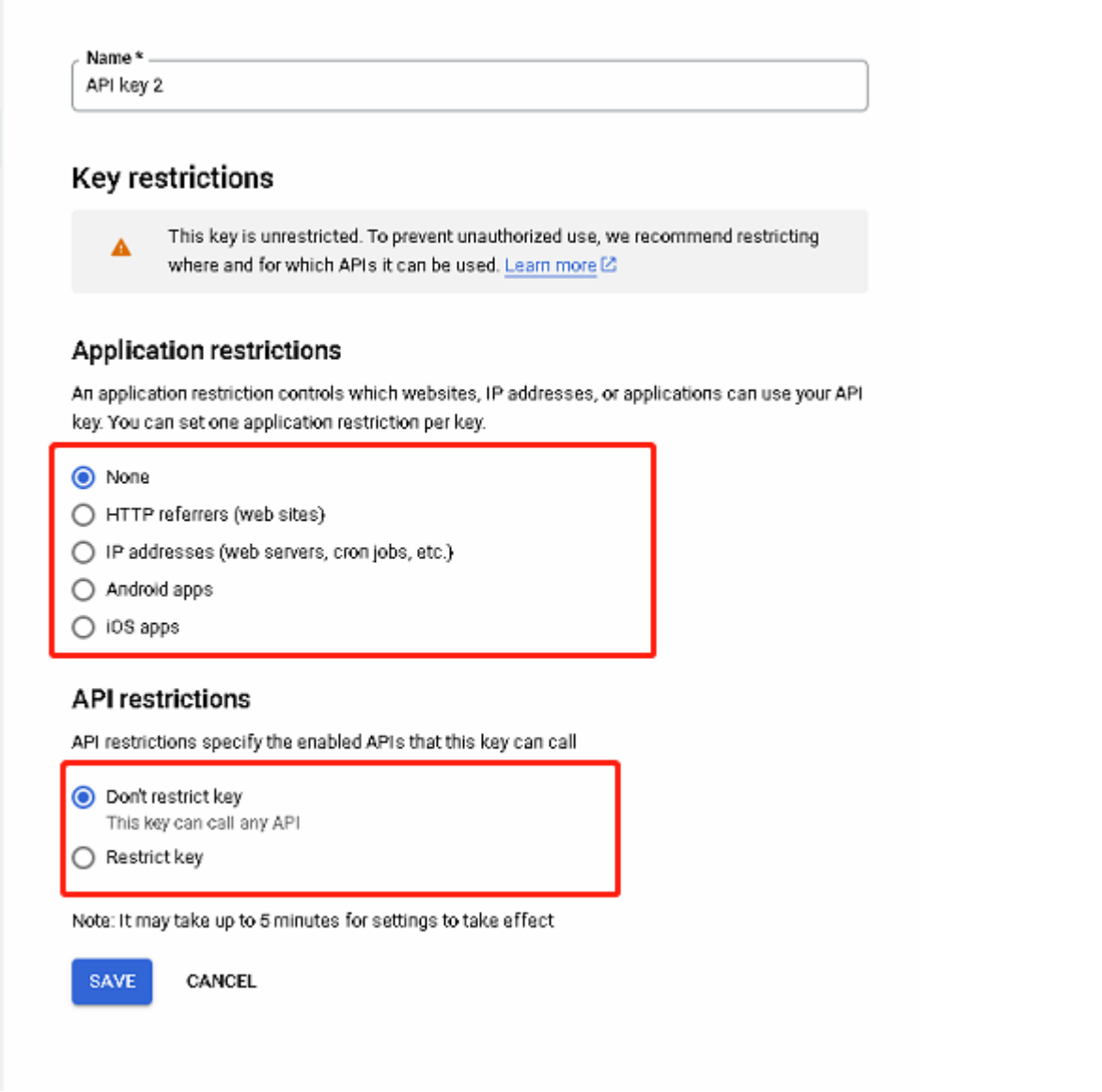
12. Check **API Key**



13. Check Alert, click **Edit Settings**



14. Select **Application restrictions** refer from your deployment and select **API Restrictions**



15. Click Save

ARMATURA

ARMATURA LLC www.armatura.us E-mail:sales@armatura.us