User Manual

ZKBio CVAccess

Date: November 2025

Doc Version: 1.1

Software Version: V4.3.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Copyright © 2025 ZKTECO CO., LTD. All rights reserved.

Trademark

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

Disclaimer

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

The contents of this manual must be read as a whole 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 ZKTeco 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 has 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.

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

ZKTeco 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.

ZKTeco 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 ZKTeco has been advised of the possibility of such damages.

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

ZKTeco 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 http://www.zkteco.com.

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

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone   +86 769 - 82109991

Fax   +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques.   With years of experience in the industrialization of biometric verification, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **ZKBio CVAccess software**.

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

Features and parameters with ★ are not available in all devices.

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.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the New User window.
/	Multi-level menus are separated by forwarding slashes. 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.

Contents

1 Introduction

Today, the modern companies' concern for security has rapidly increased. To achieve this, ZKTECO brings you ZKBio CVAccess that helps the customers to integrate the operations of access control and attendance on one platform. The system is divided into four modules, namely: Personnel, Access, Attendance and System Management.

Features:

- It can manage about 2000 personnel data.

- It has a 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 ensure proper feedbacks of data to the management.

Configuration Requirements:

- Dual-core processor with a speed of 2.4GHz or above.

- System Memory of 4GB or above.

- Available space of 10GB or above. We recommend using NTFS hard disk partition as the software installation directory.

- Monitor Resolution of 1024 x 768px or above.

Operating System:

- Supported Operating Systems: Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Window 11 /Windows Server 2008/2013(32/64).

- Supported Database: PostgreSQL.

- Recommended Browser version: IE 11+/Firefox 27+/Chrome 33+/Edge.

1.1 Personnel Module

The Personnel module is used to set the person details and their 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 add the personal information, assign departments, maintain and manage personnel details.

1.2 Access Control Module

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

1.3 Time & Attendance Module

The Attendance Module consists of timetable, shift and schedule management, cross-regional attendance Management. You can also manage other exceptions such as leave, late, overtime etc. At the same time, access control can be configured along with attendance management to generate attendance records.

1.4 Video Intercom Module

The Video Intercom Module can be used in conjunction with door stations, indoor stations, and mobile terminals, as a professional visual communication and access control platform. It can achieve functions such as real-time two-way audio and video calls, remote door unlocking, access permission management, and other security communication features.

1.5 Smart Video Surveillance Module

The Smart Video Surveillance Module can be used in conjunction with NVR, IPC device, as a professional video management platform, it can achieve functions such as preview, playback, video wall display, map configuration, intelligent configuration, video patrol, visual intercom, alarm statistics and reporting, and other management features.

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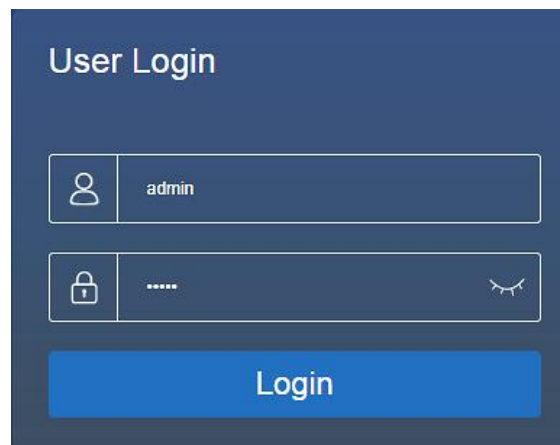
The System Management is primarily used to assign system users and configure the roles of corresponding modules, manage databases such as backup, initialization, and recovery, and set system parameters and manage the system operation logs.

1.7 Service Center Module

This module integrates the device and event logging of the system module. Users can import a map to the map center to view the distribution of monitoring points and alarm sources. When an alarm occurs, users can view the location and surrounding conditions of the alarm source, select a suitable monitoring point, and view video live, playback, and human movement functions.

2   System Operations

2.1 Login

After installing the software, double-click the ZKBio CVAccess icon to open the software. You may also open the recommended browser and enter the IP address and server port in the address bar. The IP address is http://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 **[admin]**, then click **[Login]**. After logging-in for the first time, you need to reset your password.
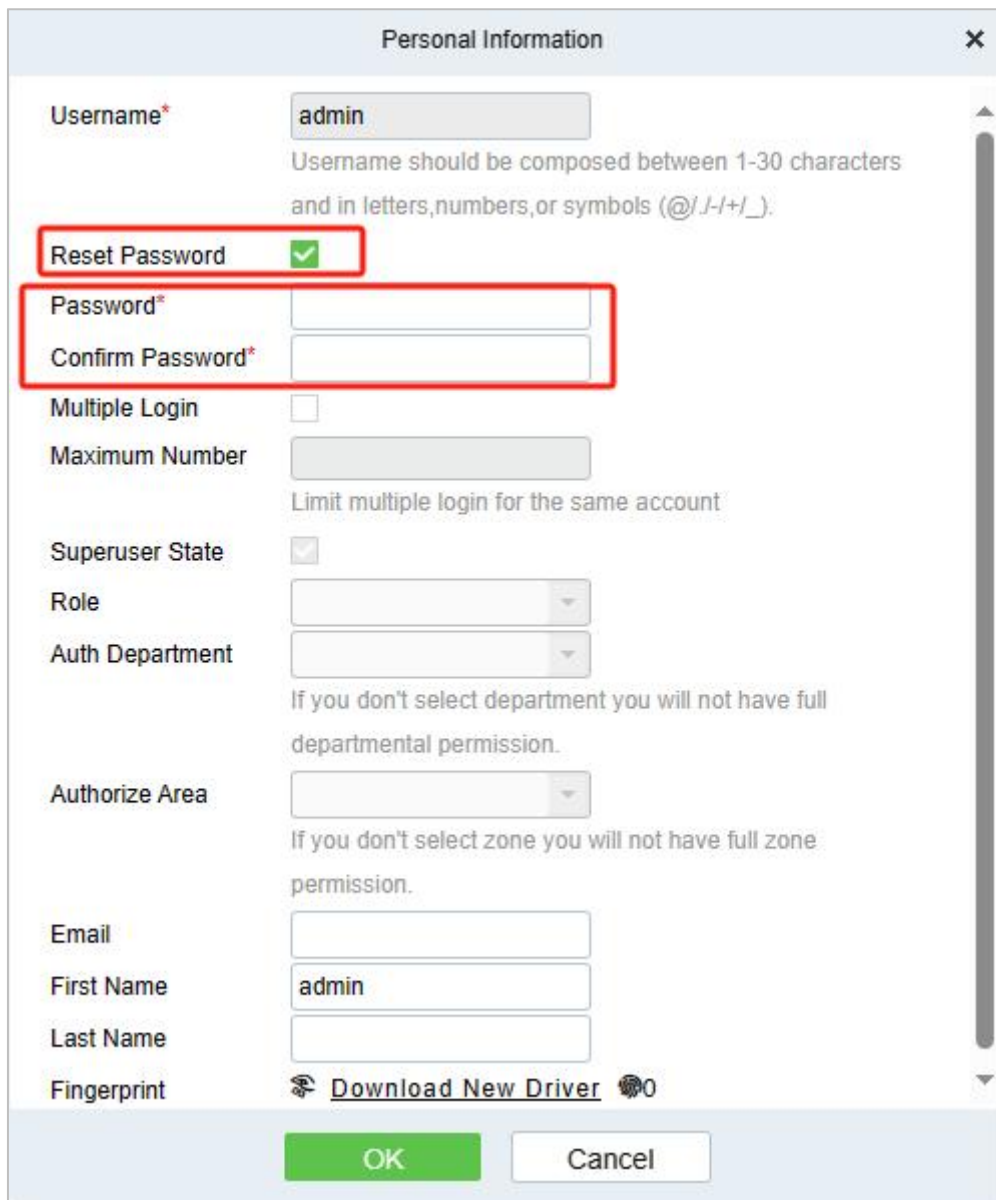
2.2 Activate the System

Please refer the corresponding license activation document.

2.3 Modify Password

You can modify the login password in **[Personal Information]**. Click on the profile picture in the top right corner.

Select the **[Reset Password]** check box to modify the password.

✍**Note:** Both the Superuser and the new user are created by the super user (the default password for the new users is 111111). The username is not case-insensitive, but the password is case-sensitive.

2.4About

Click the **[About]** button ![About icon] on the top right corner of the interface to check all the software version and license information.

2.5Help

Click the **[Help]** button ![Help icon] on the top right corner of the interface to view user manual.

2.6Language

Click the **[Language]** button   on the upper right corner of the interface to switch

the language.

2.7Exit the System

Click the **[Logout]** button   on the upper right corner of the interface to exit the

system.

3 Personnel

You can configure the Personnel Management and Card Management in this module.
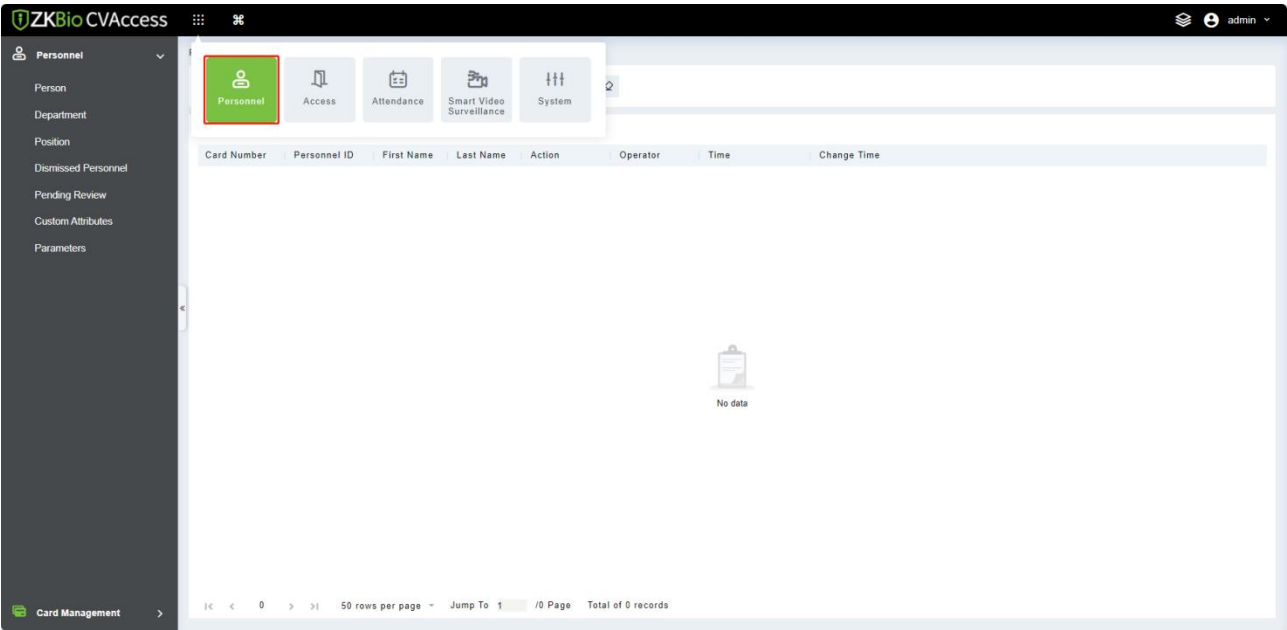
3.1 Personnel Management

The personnel management includes these modules: Personnel, Department, Position, Dismissed Personnel, Pending Review, Custom Attributes, and Parameters.
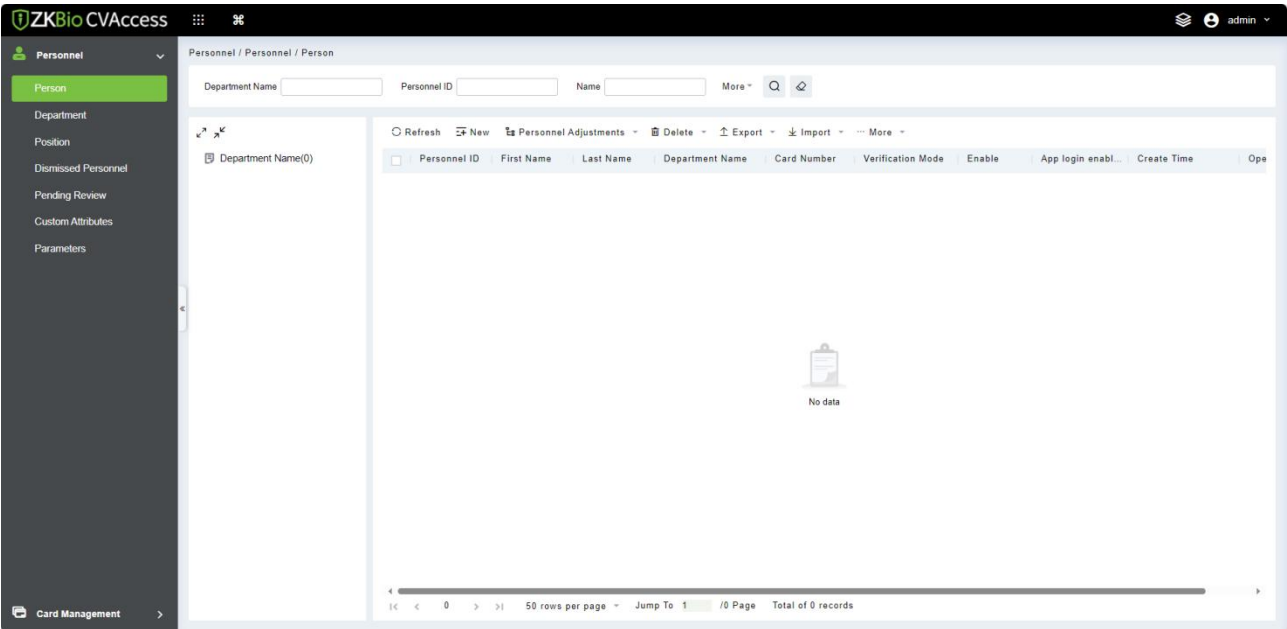
3.1.1 Personnel

By using this management, the user shall register the personnel in the system, or import the personnel information from other software or file 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.

3.1.1.1 Add Personnel

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

Fields are as follows:

•   **Personnel ID:** An ID may consist of up to 9 characters, within the range of 1 to 79999999. It can be configured based on your requirements. The Personnel ID contains only numbers by default but may also include letters.

✎**Notes:**

(1)   When configuring a personnel number, check whether the current device supports the maximum length and whether letters can be used in Personnel ID.

(2)   To edit the settings of the maximum number of characters of each personnel number and whether letters can also be used, click Personnel > Parameters.

•   **Department:** Select from the drop-down menu and click **[OK]**. If the department was not

set previously, only one department named **[Company Name]** will appear.

- **First Name/Last Name:** The maximum number of characters is 50.

- **Gender:** Set the gender of personnel.

- **Mobile Phone:** Enter the phone number of the user.

- **Certificate Type:** There are four types of certificates: ID, Passport, Driver's License and Others.

- **Certificate Number:** Enter the ID number.

- **Birthday:** Input employee's actual birthday.

- **Email:** Input employee's Email ID. The max length is 30.

- **Device Verification Password:** Set password for verifying on the device using personnel accounts. It can only contain up to 6-digits. It cannot be the same with other user's password and the duress password.

- **Card number:** The max length is 10, and it should not be repeated.

- **Personal Photo:** The picture preview function is provided, supporting common picture formats, such as **jpg**, **jpeg**, **bmp**, **png**, **gif,** etc. The best size is 120×140 pixels.

- **Browse:** Click **[Browse]** to select a photo on your local drive to upload.

- **Capture:** Taking photo by camera is allowed when the server is connected with a camera.

- **Register Fingerprint / Finger Vein /Palm /Face:** Enroll the Personnel Fingerprint, Finger Vein, Palm, or Face. To trigger the alarm and send the signal to the system, scan the Duress Fingerprint.
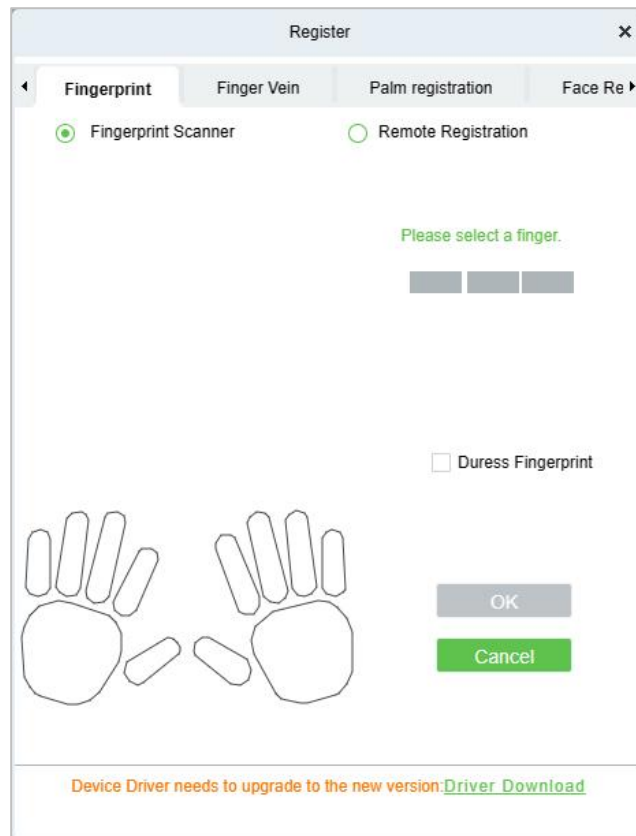
Register Fingerprint:

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

2) Select a fingerprint, press the finger on the sensor three times, then "**Fingerprint registered Successfully**" will be prompted.

3) Click **[OK]** to complete registration.
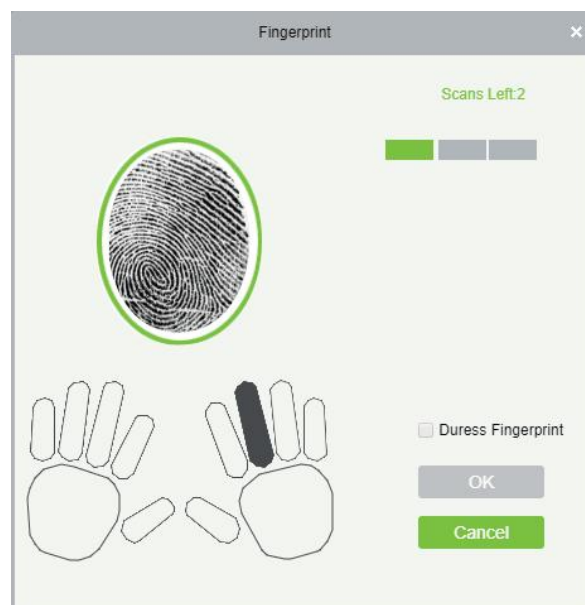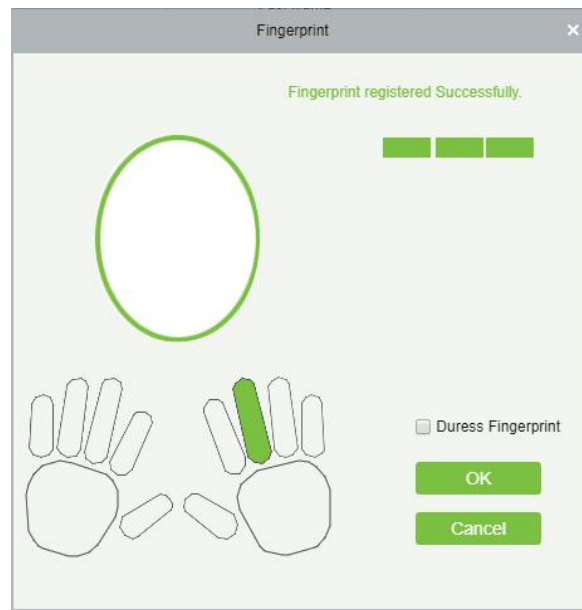
✍Notes:

(1)   Click a fingerprint to delete.

(2)   If you need to register a duress fingerprint, select the **"Duress Fingerprint"** check box.

(3)   If fingerprints are duplicated, **"Don't repeat the fingerprint entry"** will be prompted.

(4)   If the fingerprint sensor driver is not installed, click **[Install driver]** and the system will prompt to download and install the driver.

(5)   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:

  a.   In Internet Explorer, click **[Tools] > [Internet Options] > [Security] > [Credible Sites]**, add http://localhost to the credible sites, then restart the Internet Explorer.

  b.   In Internet Explorer, click **[Tools] > [Internet Options] > [Advanced] > [Reset]** to pop up a dialog of Reset Internet Explorer Settings, click **[Reset]** to confirm; then restart the Internet Explorer (you may try when Point 1 does not help).

  c.   If all the above settings do not work, please execute following operations (take IE11 browser as an example): click **[Tools] > [Internet Options] > [Advanced] > [Security]**, check the option of **"Allow software to run or install even if the signature is ..."**, and remove the select **"Check for server certificate revocation"**, then restart IE.

  d.   If the browser is below IE8, the fingerprint registration page will be different:
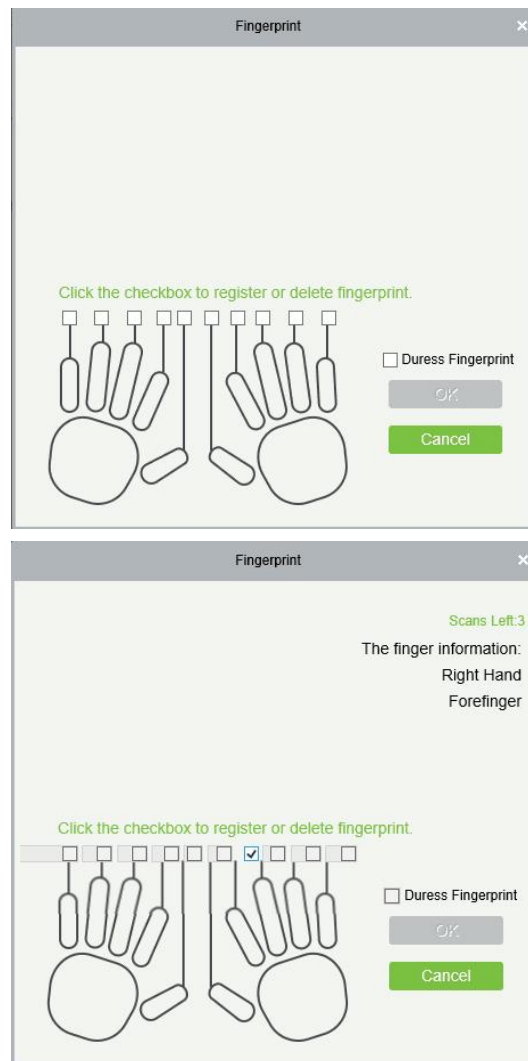
e. The system supports access from the Live20R fingerprint device and the fake fingerprint prevention function.
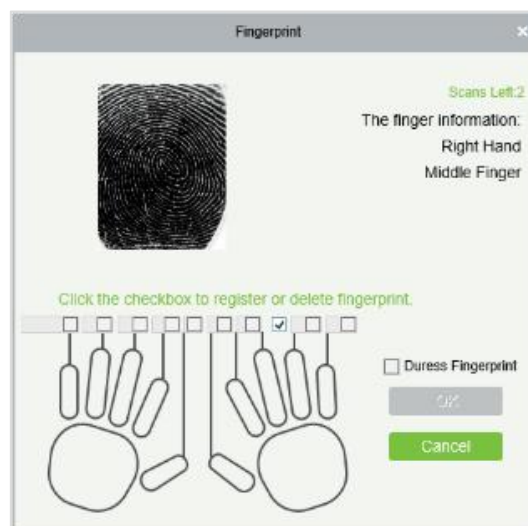
2. Set the Access Control parameters for the personnel. Click **[Access Rule]**.

Fields are as follows:

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

•   **Superuser:** In access controller operation, a super user is not restricted by the regulations on time zones and has extremely high door-opening priority.

•   **Device Operation Role:** It will define the authority level in the device of the user.

•   **Disabled:** Temporarily disable the personnel's access level.

•   **Set Valid Time:** Doors can be set to open only within certain time periods. If the check box is not selected, the door is always active.

 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. Put the cursor on a photo to view details about the personnel.

✍**Notes:**

1) 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 or not. Please upgrade the device to use this function.

2) Not all the devices support the "Set Valid Time" function. Some devices only allow users to set the year, month, and day of the local time. When a user adds a device, the system will notify the user whether the current device supports this function or not. Please upgrade the device to use this function.

3. Click **[Personnel Detail]** to access the details and editing interface and enter information.

4. After entering the information, click **[OK]** to save and exit, the personal details will be displayed in the added list.

3.1.1.2   Edit Personnel

Click **[Personnel] > [Person]**, then select a person, and click **[Edit]**.

3.1.1.3   Delete Personnel

Click **[Personnel] > [Person]**, then select a person, and click **[Delete] > [OK]** to delete.

✍**Note:** All relevant information about the person will be deleted.

3.1.1.4   Adjust Department

1. Click **[Personnel] > [Person]**, then select a person, and click **[Adjust Department]**.

2.   Select from the drop-down list of "New Department".
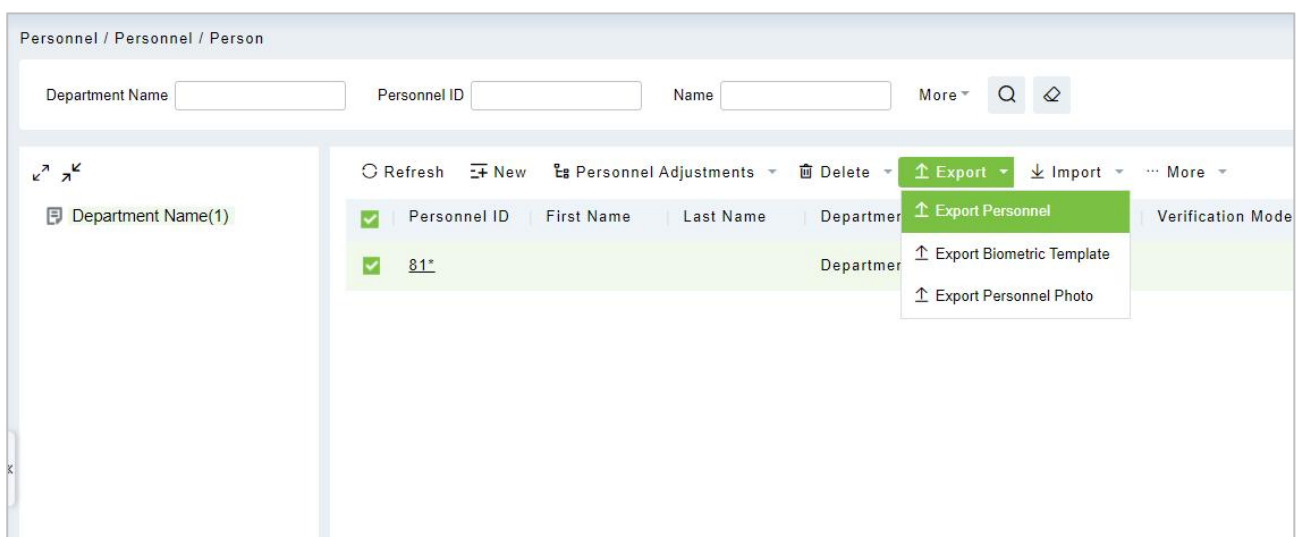
3.   Click **[OK]** to save and exit.

3.1.1.5   Statistics

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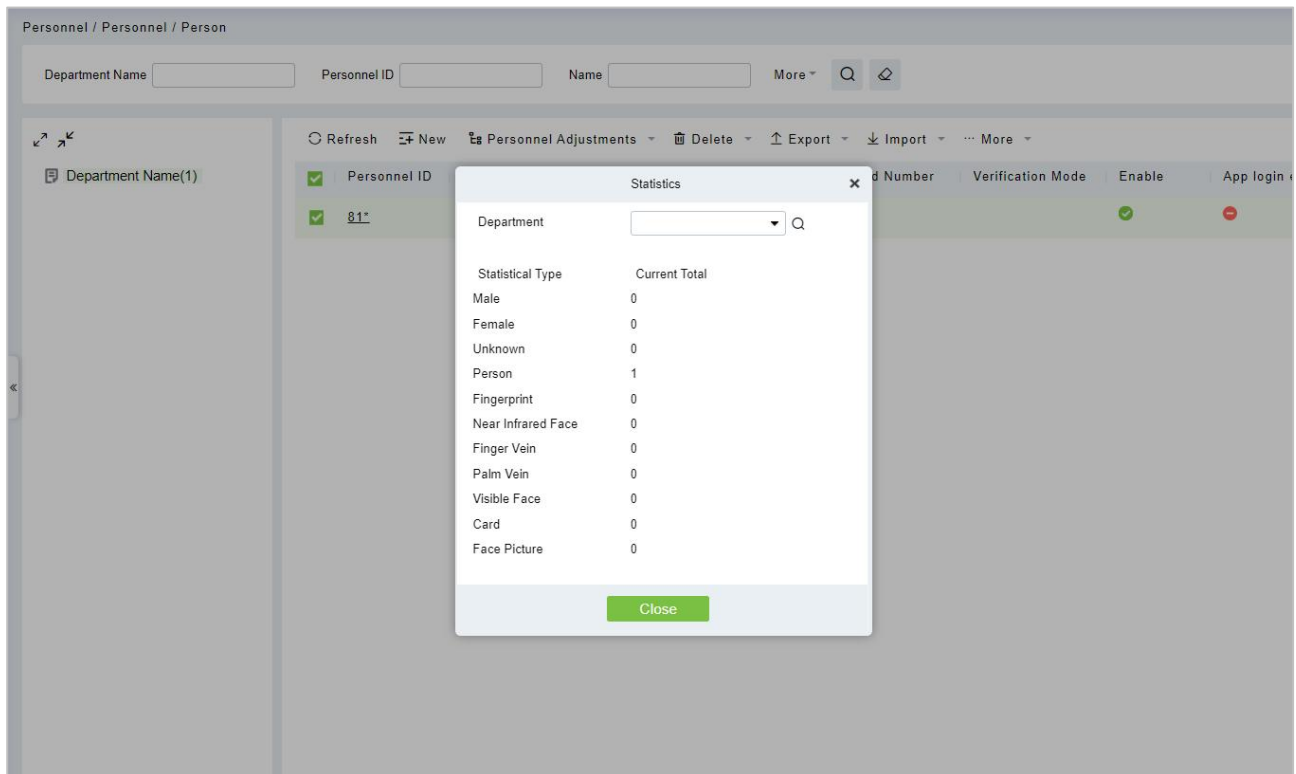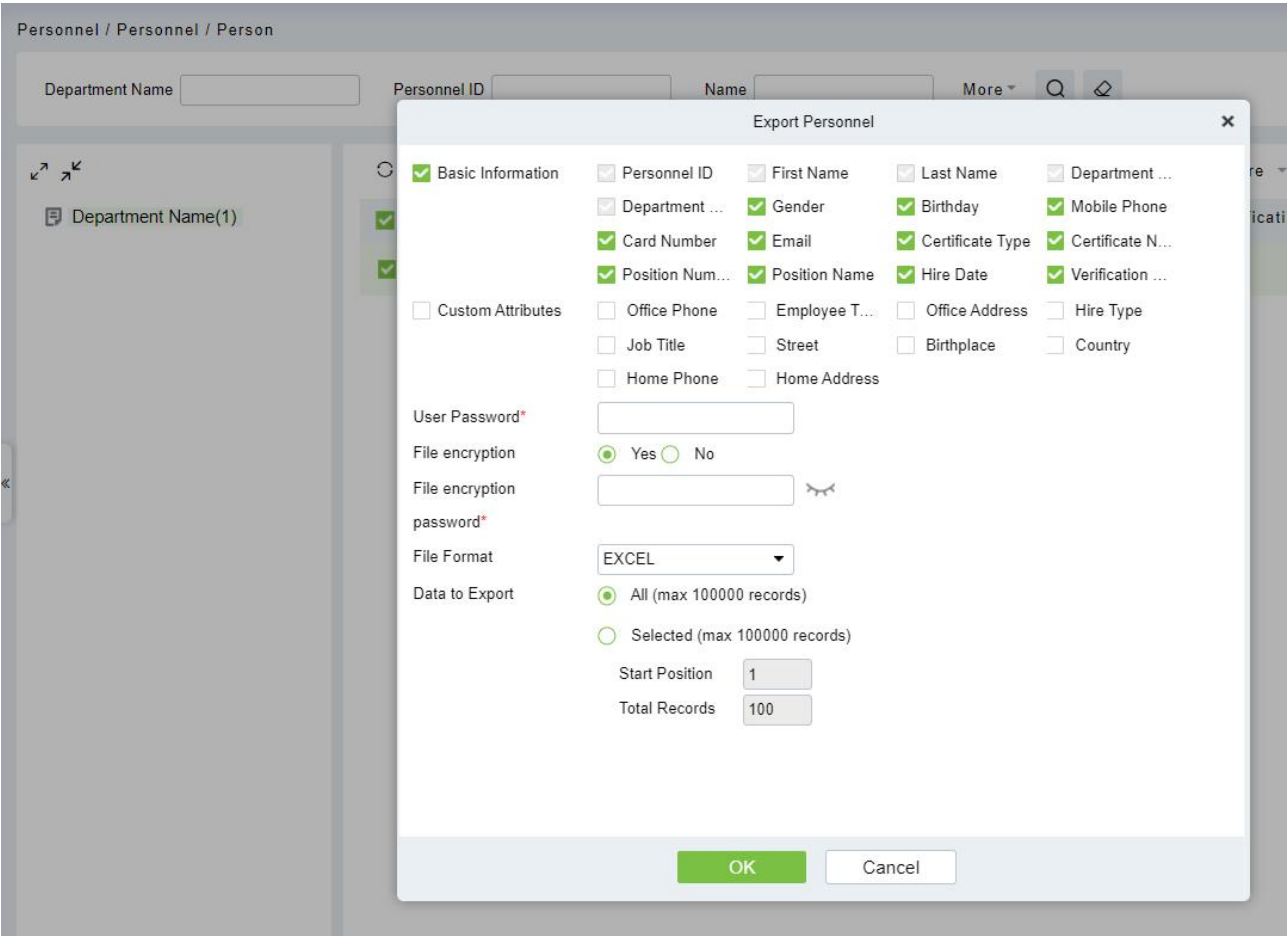

3.1.1.6   Export

Click **[Personnel]> [Person]> [Export]** to export personnel information, personnel biometric templates and personnel photo.
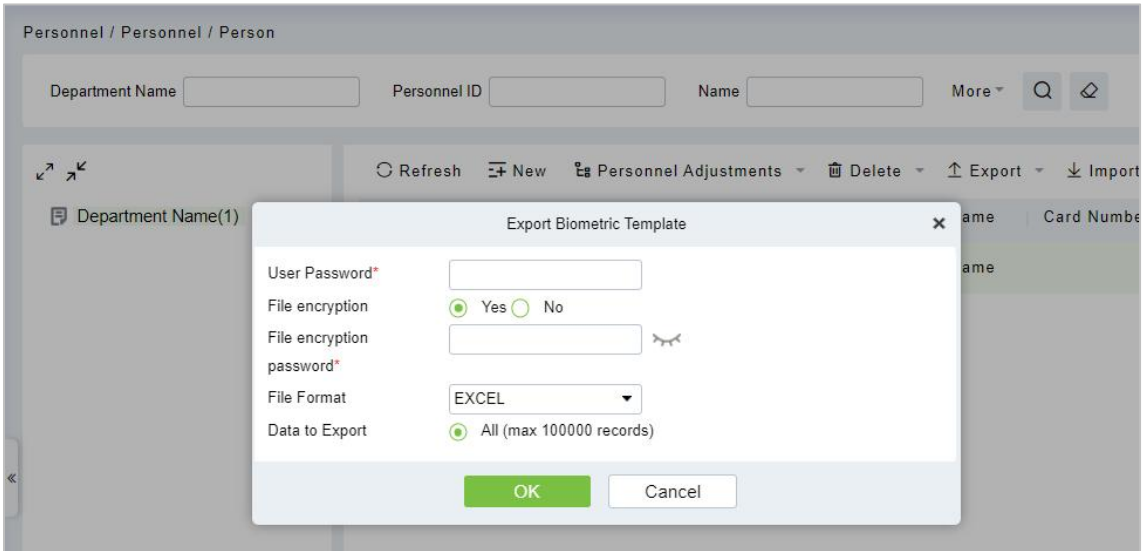
1. Select the type of file and Export mode as required.

2. Export the Biometric Template.

3.   Export Personnel Photo.
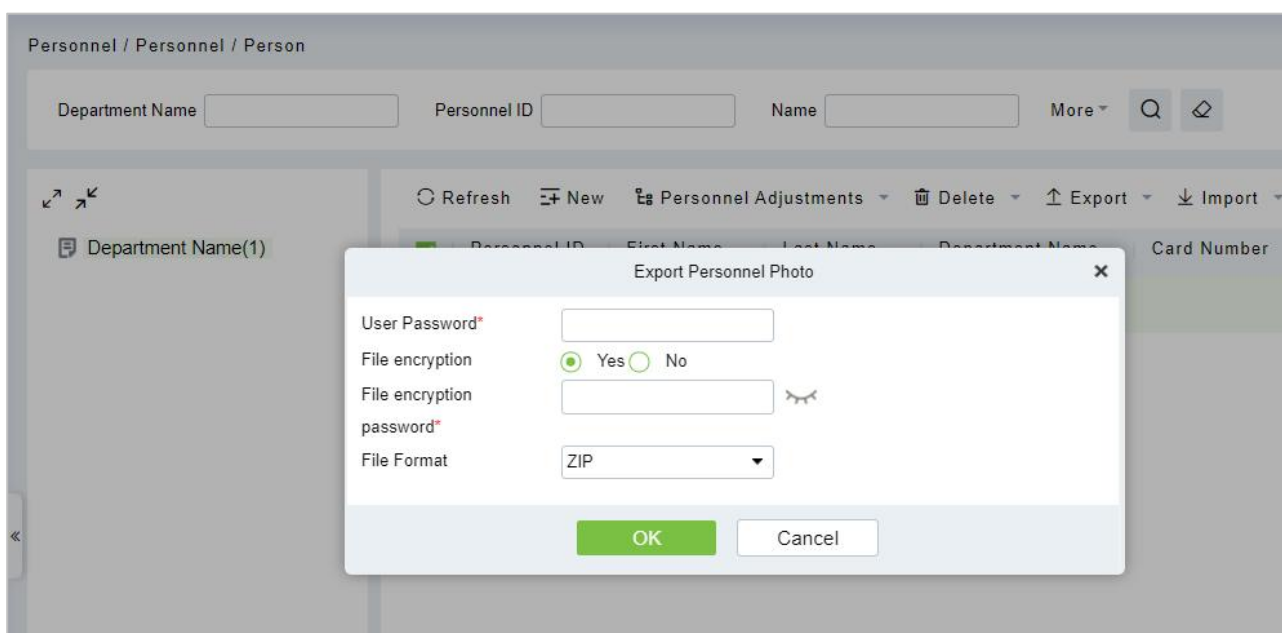
3.1.1.7 Import

Click **[Personnel] > [Person] > [Import]** to import personnel information and personnel biometric templates. It only supports personnel information templates for importing.
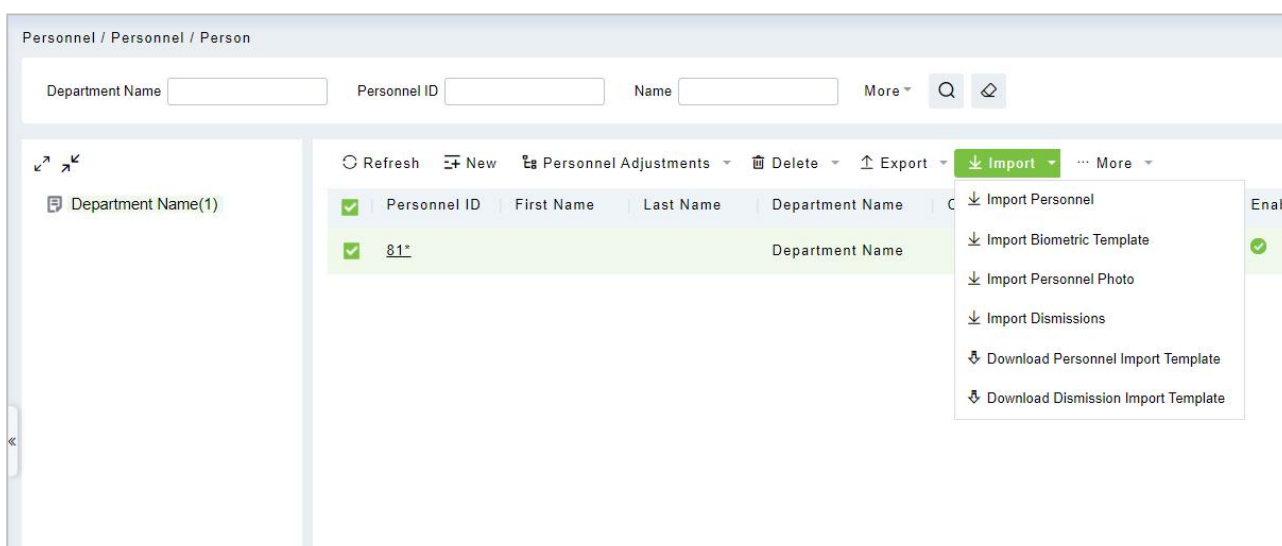
1.   Import Personnel: Select **"Yes"** for **[Update the existed Personnel ID in the system]**, the

original data will be overwritten when the personnel ID is repeated; select **"No"**, the opposite.
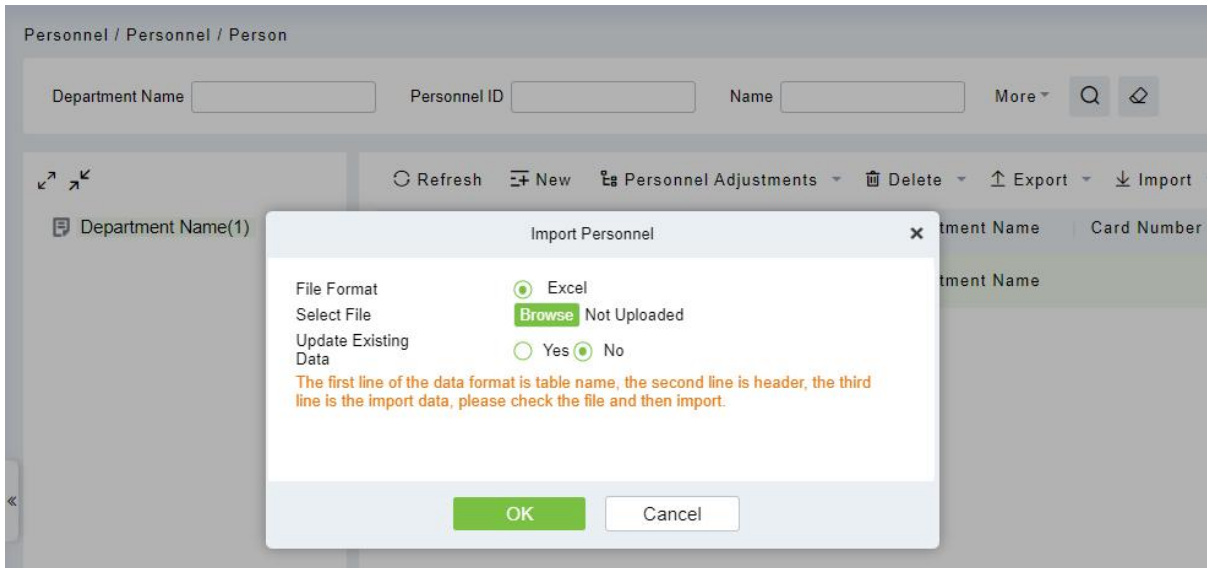
2.   Import Biometric Template.
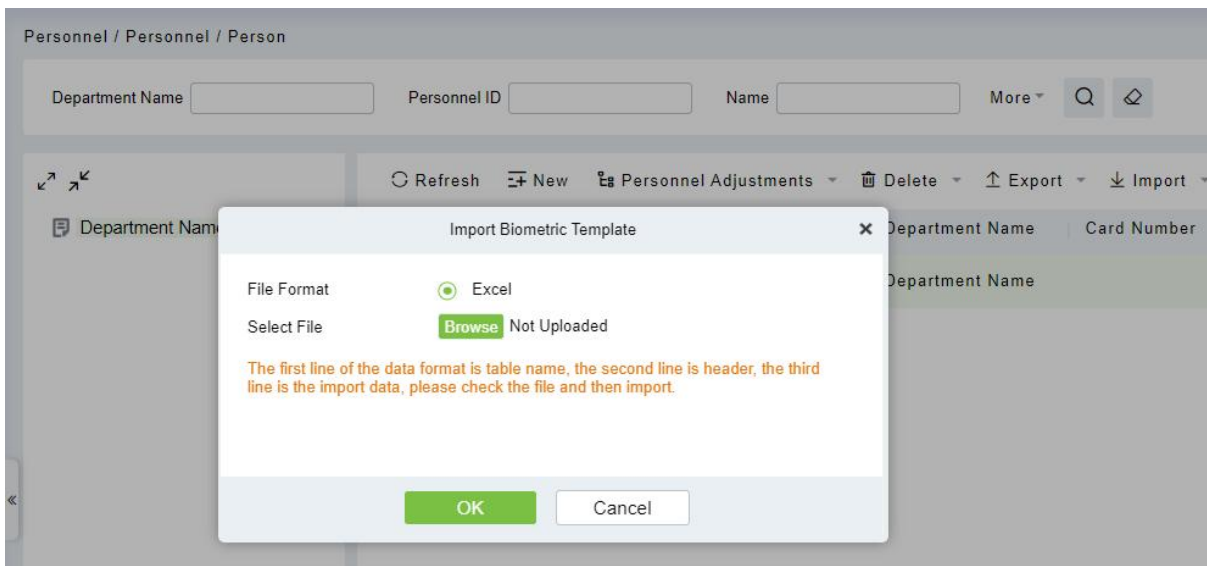
3.   Import Personnel Photo: The personnel photo needs to be named by personnel ID, supporting common picture formats, such as jpg, jpeg, png, gif, etc.
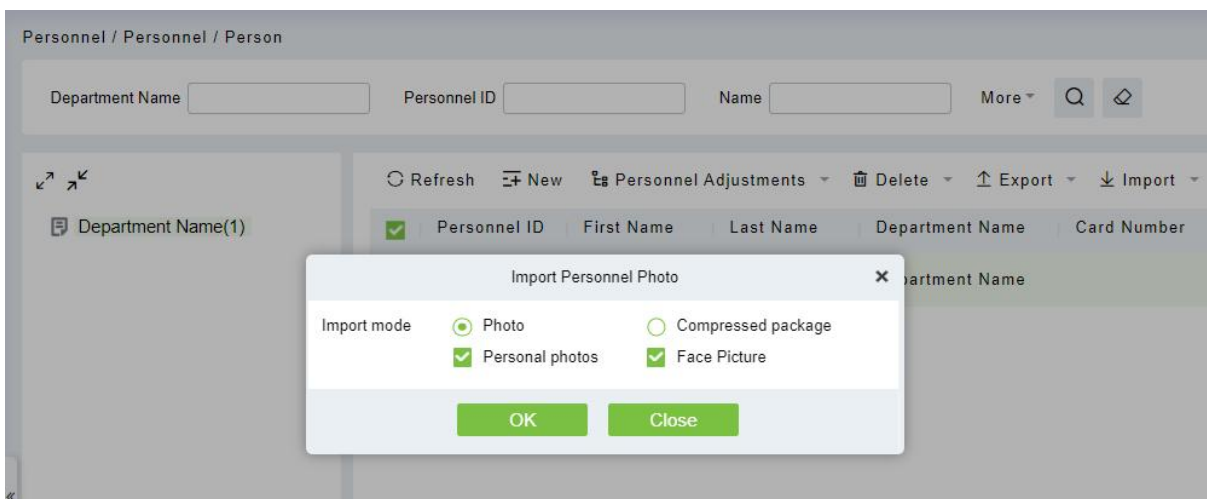
3.1.1.8 More
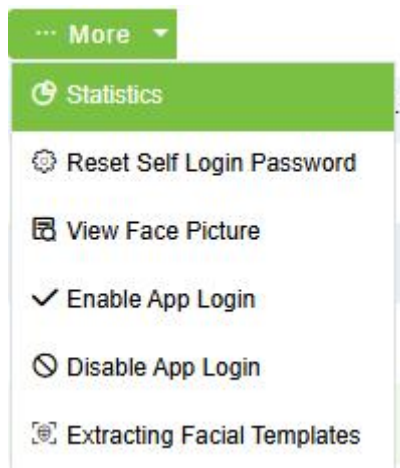
Statistics

Click **Personnel > Person > More**, then select Statistics.

View the number of Person, Male, Female, and the number of Fingerprints, Near Infrared Face, Finger Vein, Palm Vein, Visible Face, Card, and Face Picture.

Reset Self Login Password

Click **Personnel > Person > More**, then select Reset Self Login Password.
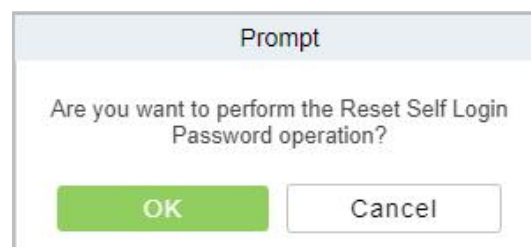
Figure 2- 35 Statistics

View Face Picture (V6.0.0 or above supported)

Click **Personnel > Person > More**, then select View Face Picture.
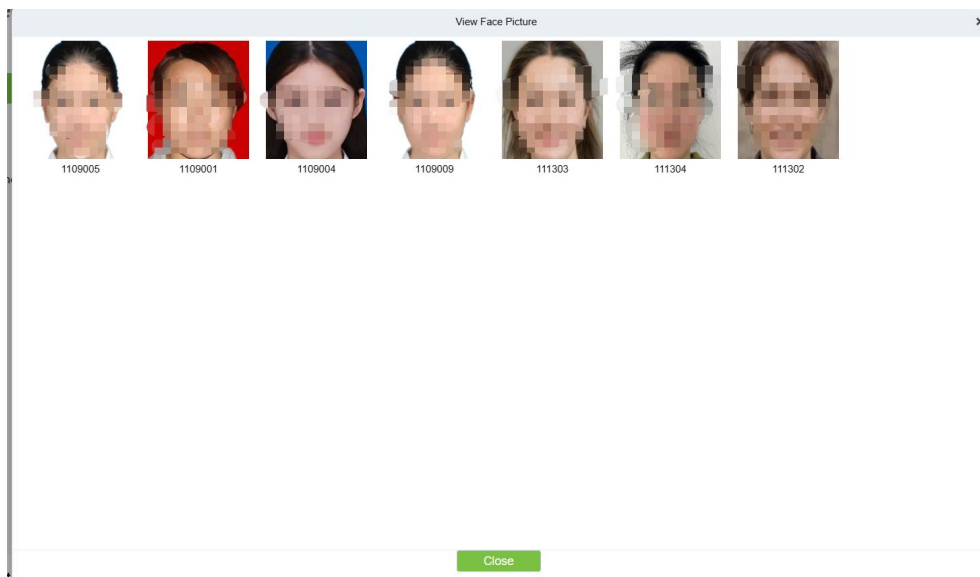
Enable APP Login

Click **Personnel** > **Person** > **More**, then select **Enable app login. Selected** persons will be enabled ZKBio CVSecurity Mobile APP login.When enabling the APP function, an email will be sent to the selected personnel. The email content includes: personnel information, instructions on how to download the ZKBio Zexus APP and how to log in, along with a QR code containing enterprise information for quick scanning and login.
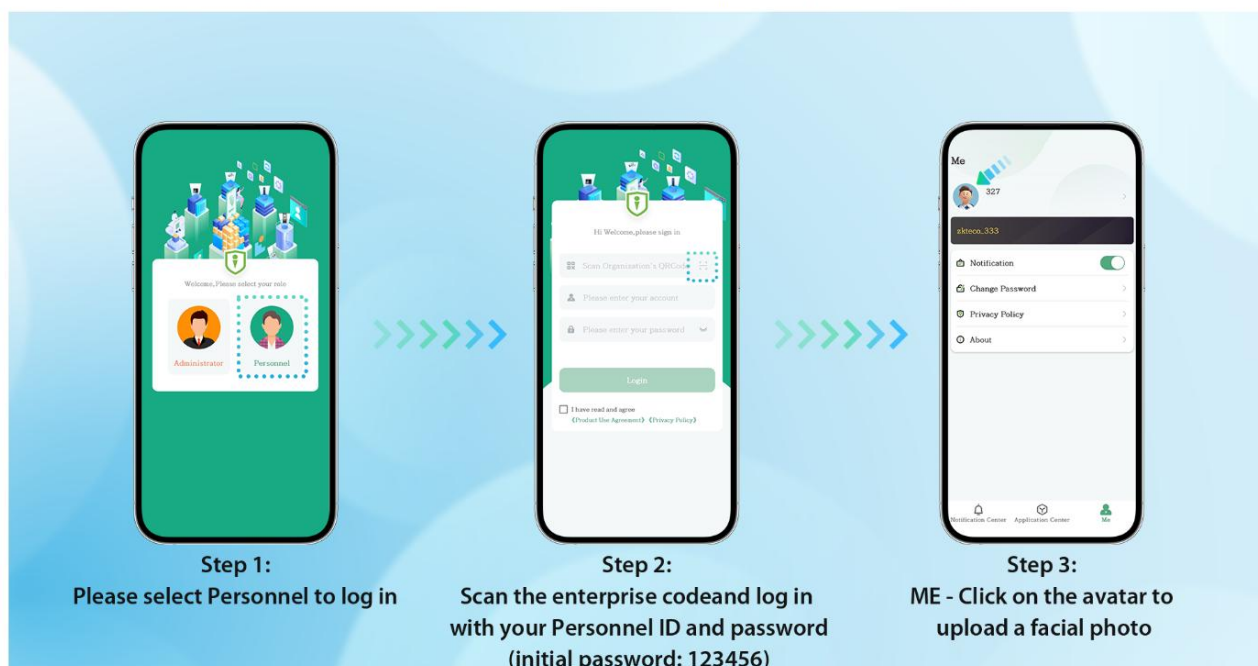
Disable APP Login

Click **Personnel** > **Person** > **More**, then select **Disable app login. Selected** persons will be disabled ZKBio CVSecurity Mobile APP login.
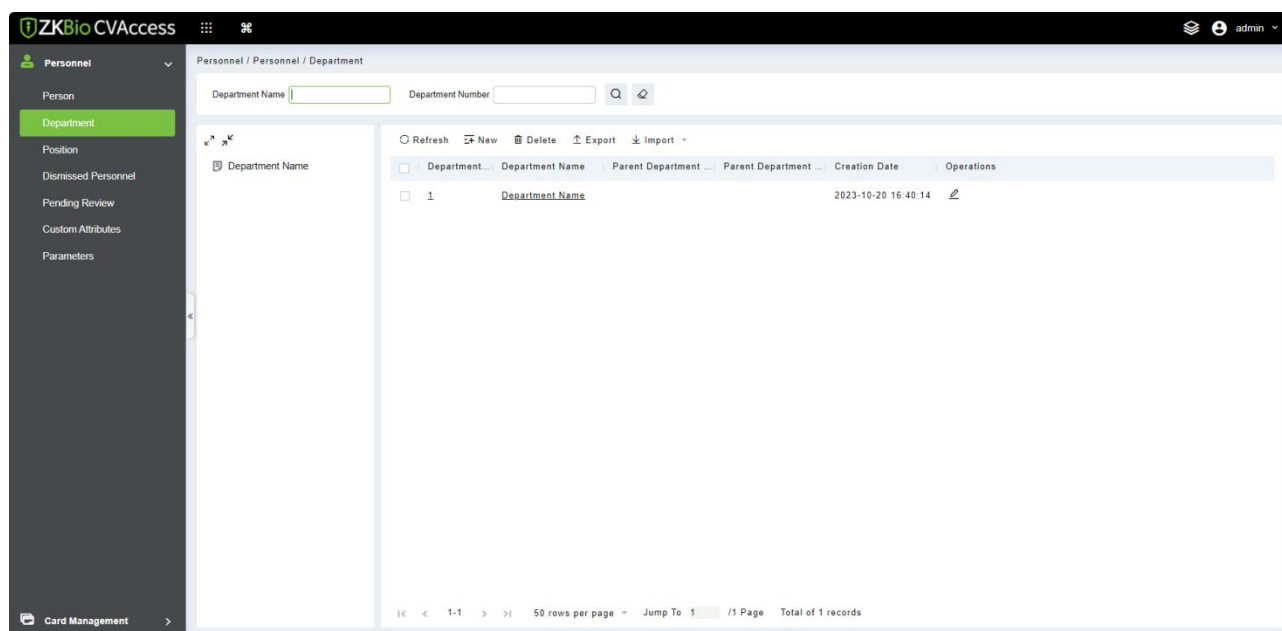
3.1.2 Department

Before managing company personnel, it is required to set a departmental organization chart of the company. Upon the first use of the system, by default it has a primary department named **[General]** and numbered **[1]**. This department can be modified but can't be deleted.

Main functions of Department Management include Add, Edit, Delete, Export and Import Department.

3.1.2.1 Add a Department

1.   Click **[Personnel] > [Personnel Management] > [Department] > [New]**.
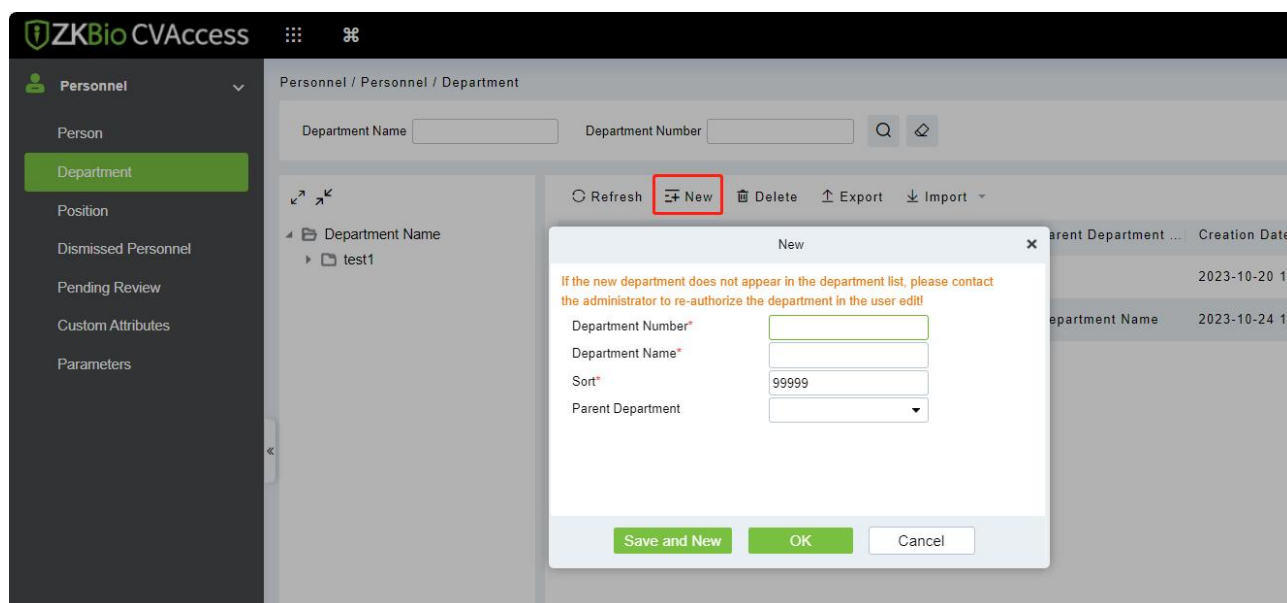
Fields are as followed:

- **Department Number:** Letters and numbers are available. It cannot be identical to the number of other departments. The number shall not exceed 30 digits.

- **Department Name:** Combination of characters up to 100.In case of different levels, the department names can be repeated.

- **Sort:** It is used to set the priority (level) of a department within a parent department. The smaller the number of department sort is, the higher ranks such department has. You can set any number from 1 to 999999.

- **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.

2. After filling the details, you can click **[OK]** to complete adding; or click **[Cancel]** to cancel it or click **[Save and new]** to save and continue adding a new department.

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

3.1.2.2 Edit a Department

Click **[Personnel] > [Personnel] > [Department]**, select a department and click .
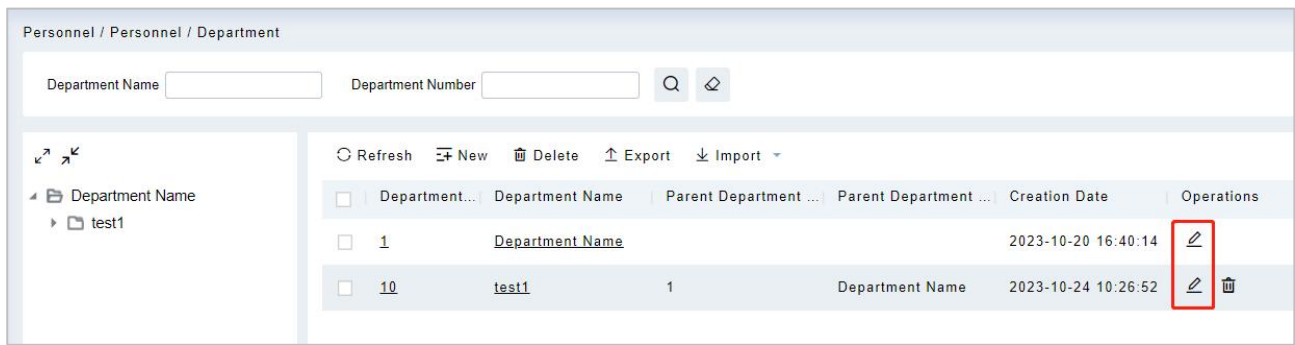
3.1.2.3 Delete a Department

1.   Click **[Personnel] > [Personnel] > [Department]**, select a department and click 🗑.
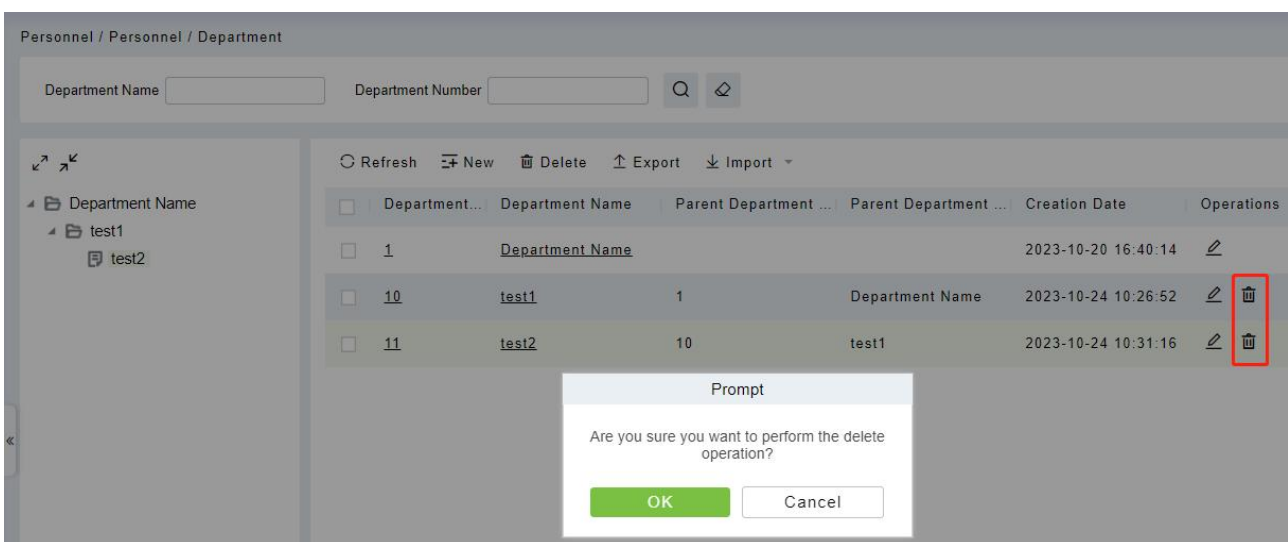
2.   Click **[OK]** to delete.

☞**Note:** If the department has sub-departments or personnel, the department cannot be deleted.

3.1.2.4 Export

1.   Click **[Personnel] > [Department] > [Export]**, the import interface is as follows.
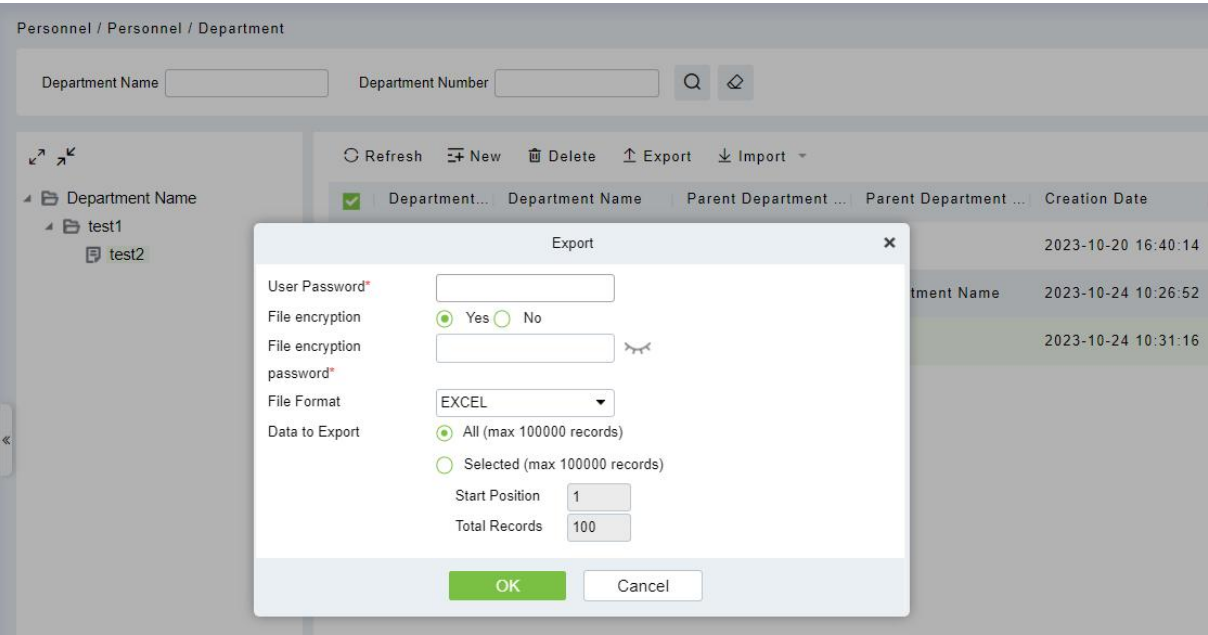
2. It can be exported in EXCEL, PDF, and CSV file format.

<table>
<tr><td colspan="5" align="center">Department</td></tr>
<tr><td>Department Name</td><td>Department Number</td><td>Parent Department Number</td><td>Parent Department Name</td><td>Created Date</td></tr>
<tr><td>ZKTeco</td><td>1</td><td></td><td></td><td>2018-12-21 14:10:08</td></tr>
<tr><td>Marketing Department</td><td>2</td><td>1</td><td>ZKTeco</td><td>2018-12-21 14:10:08</td></tr>
<tr><td>Development Department</td><td>3</td><td>1</td><td>ZKTeco</td><td>2018-12-21 14:10:08</td></tr>
<tr><td>Financial Department</td><td>4</td><td>1</td><td>ZKTeco</td><td>2018-12-21 14:10:08</td></tr>
</table>

3.1.2.5 Import

1. Click **[Personnel] > [Department] > [Import]**, the import interface is as follows:
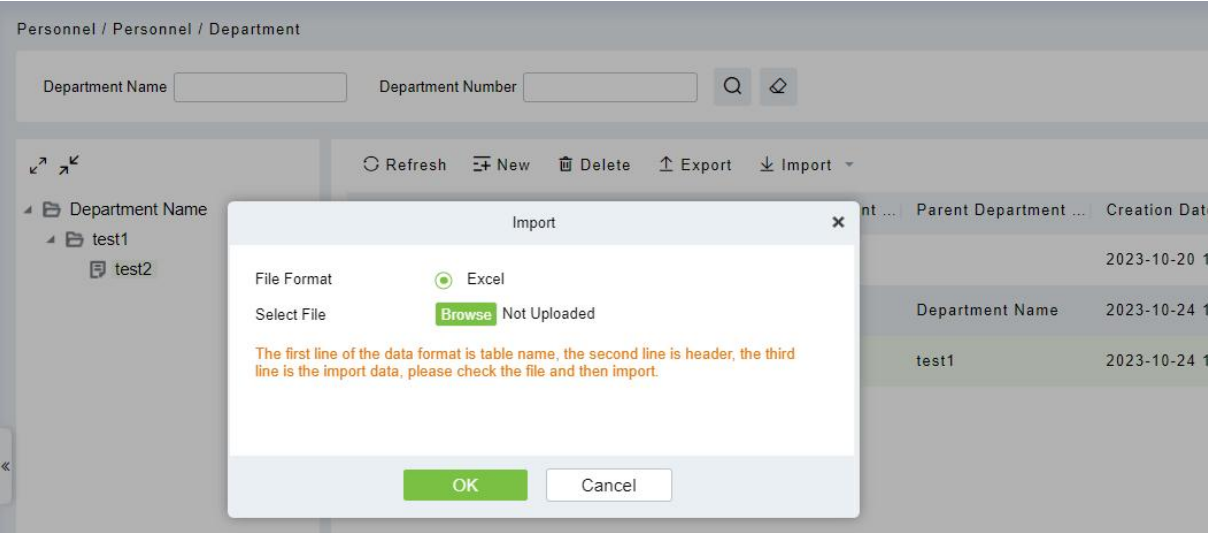
2. Import department information: can import EXCEL, CSV format files.

3. After importing the file, the system will match the imported report field and the data segment field automatically.

3.1.3 Position

Introduces the configuration Steps of manually adding a job in ZKBio CVAccess, and adding a job is used to define the job information of a person.
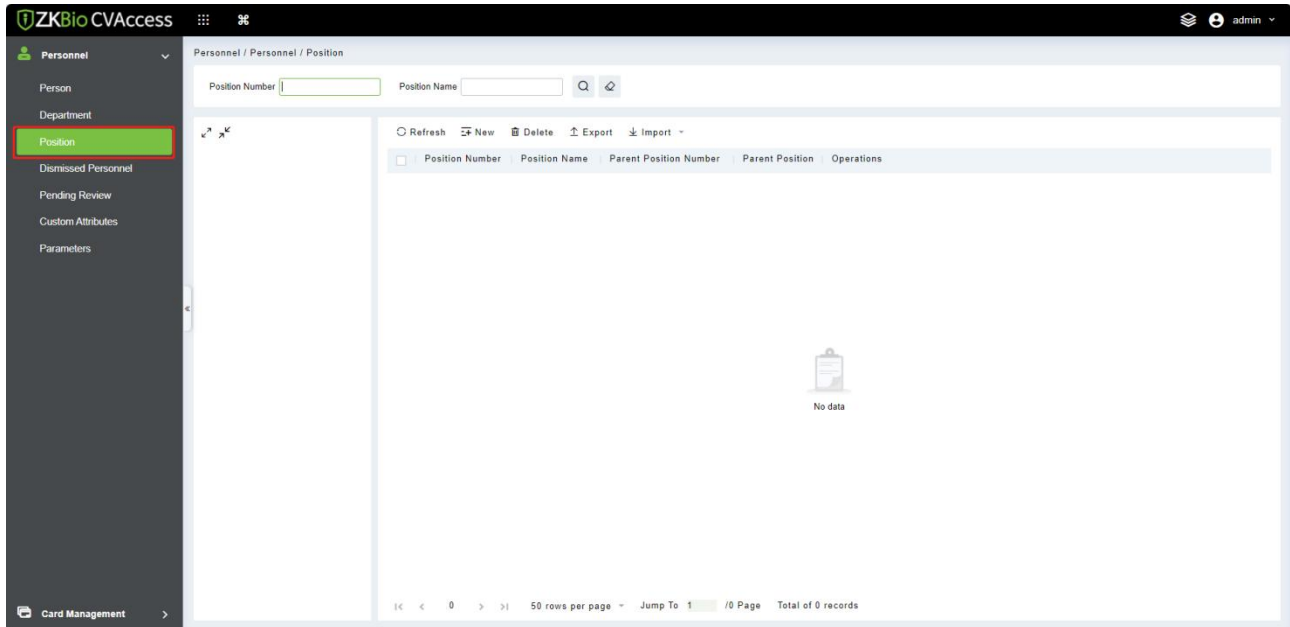
3.1.3.1 Add Position

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

2. On the new job interface, fill in the corresponding parameters according to the adding requirements.
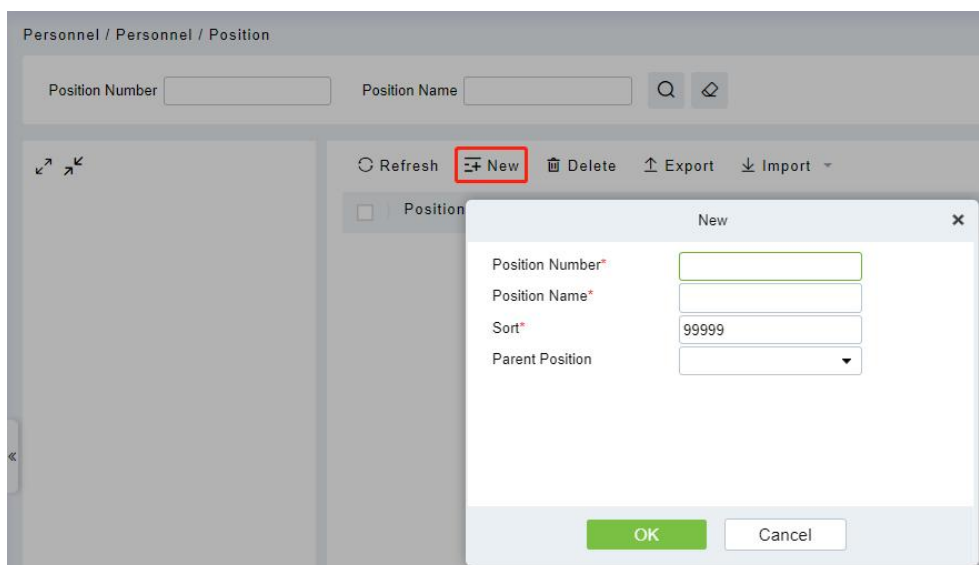
Fields are as followed:

- **Job number:** Customize the job number for easy memory.

- **Job Title:** Customize job title.

- **Sort:** Sort job listings, only numbers are supported.

- **Parent position:** Select the corresponding parent position from the drop-down radio box.
If you need to cancel, click Selected again.

3.1.3.2 Edit

Click **[Personnel] > [Personnel Management] > [Position]**, select a position and click ✏.
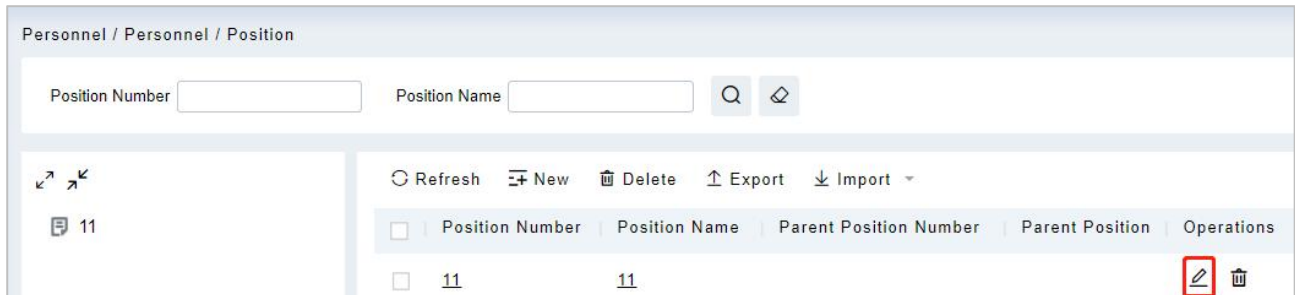
3.1.3.3 Delete

1. Click **[Personnel Management] > [Personnel] > [Position]**, select a position and click 🗑.
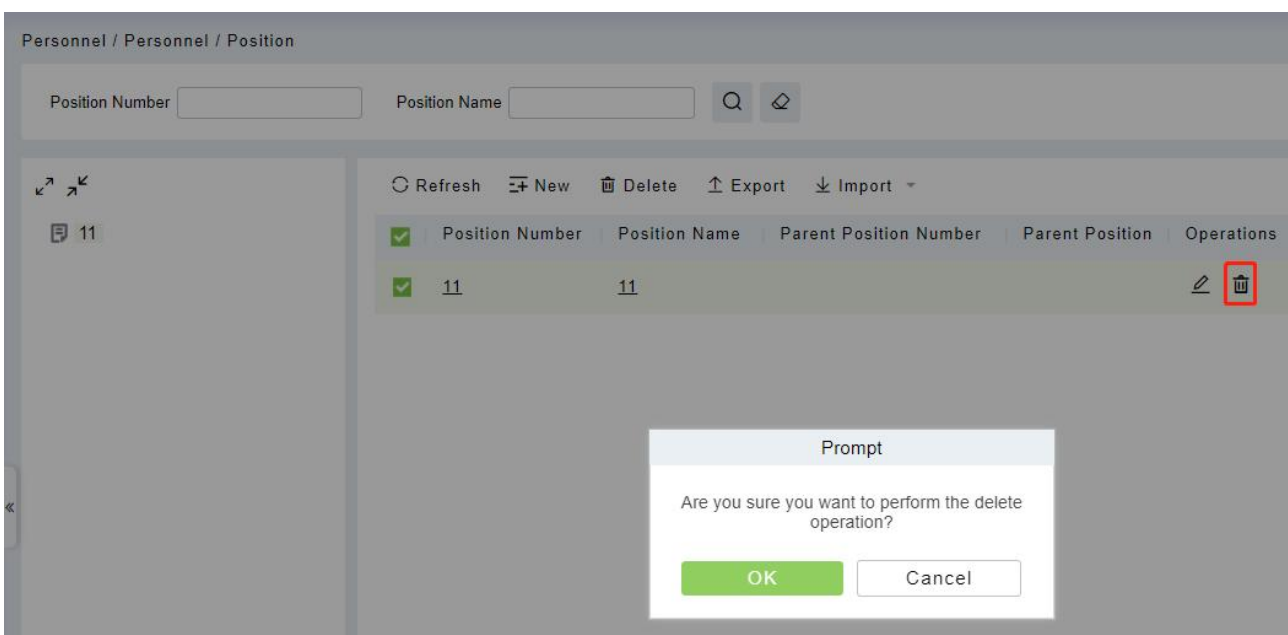
2. Click **[OK]** to delete.

3.1.3.4 Export

1. Click **[Personnel Management] > [Department] > [Position]**, the import interface is as follows.
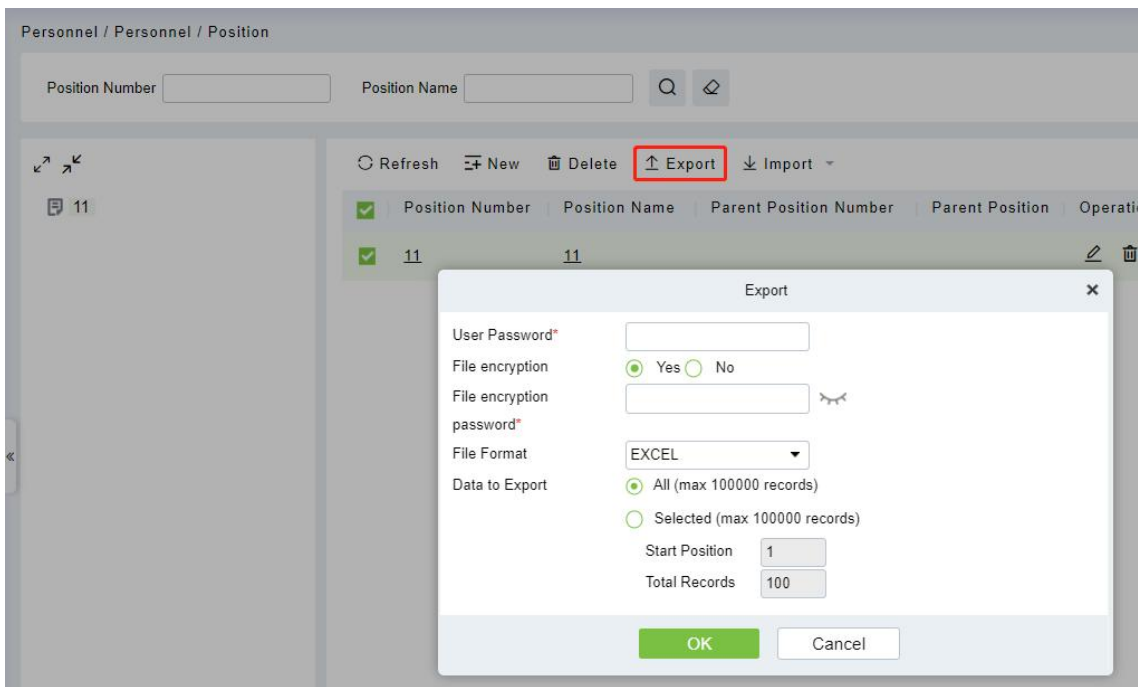
2.   It can be exported in EXCEL, PDF, and CSV file format.

3.1.3.5 Import

1.   Click **[Personnel Management] > [Department] > [Import]**, the import interface is as follows:
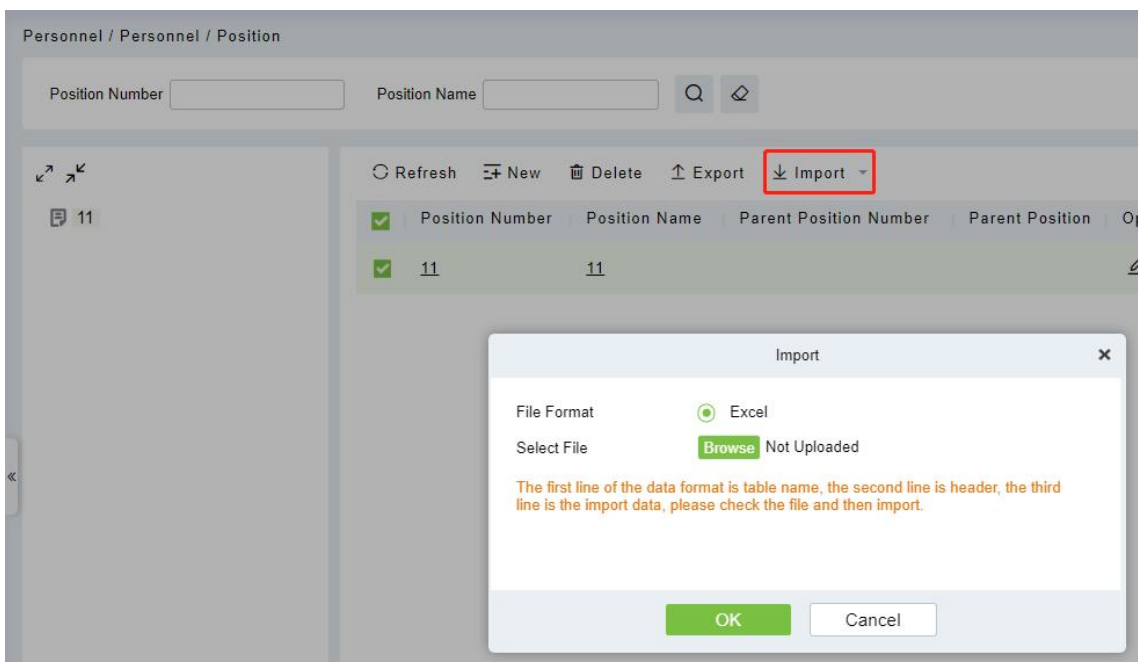

2.   Import department information: can import EXCEL, CSV format files.

3.   After importing the file, the system will match the imported report field and the data segment field automatically.

3.1.4 Dismissed Personnel

This parameter will display the personnel who are not working in company anymore. Once the

person is dismissed, it will be listed.

Click **[Personnel] > [Personnel Management] > [Dismissed Personnel]**.
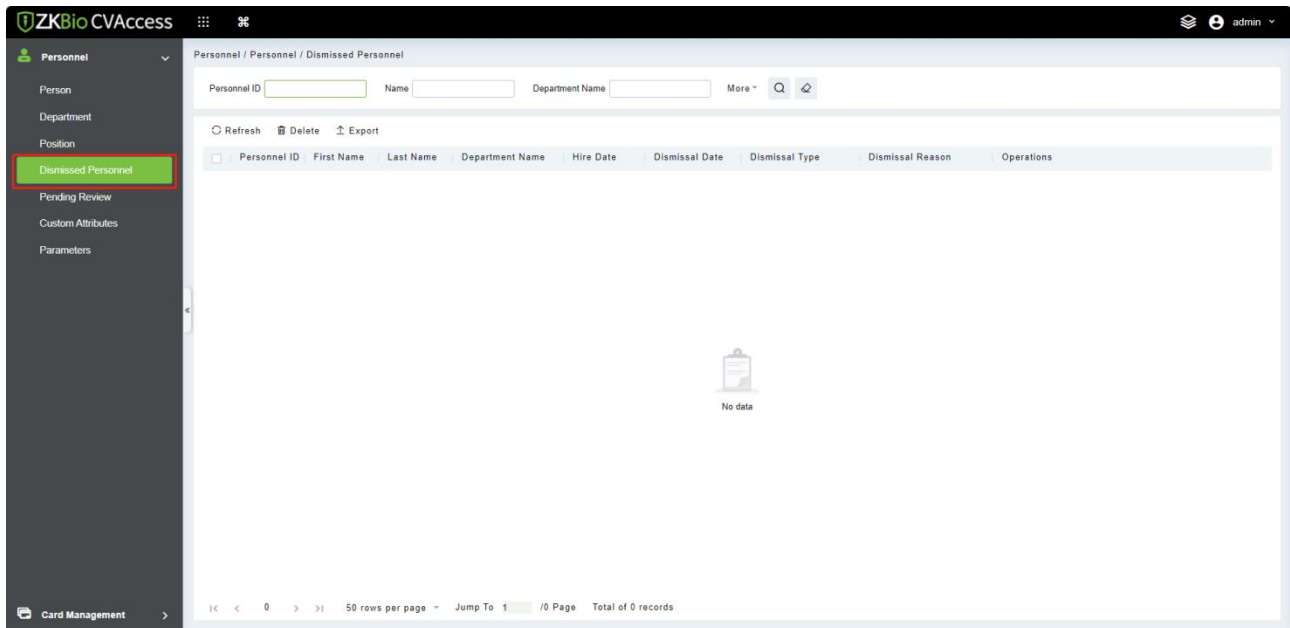
3.1.4.1 Delete

1. Click **[Personnel] > [Personnel Management] > [Dismissed Personnel]**, select a personnel and click 🗑.

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

3.1.4.2 Export

Click **[Personnel] > [Personnel Management] > [Dismissed Personnel]**, it can be exported in EXCEL, PDF, and CSV file format.

3.1.5 Pending Review

Click **[Personnel] > [Personnel Management] > [Pending Review]**.
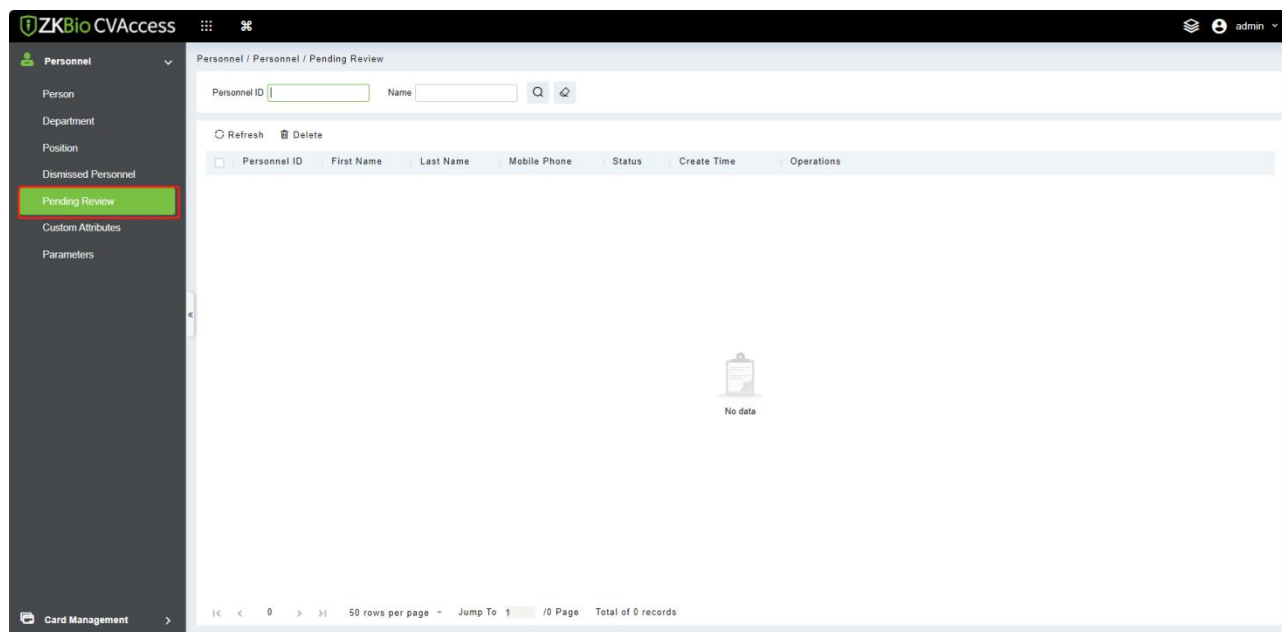
3.1.5.1 Delete

1. Click **[Personnel] > [Personnel Management] > [Pending Review]**, select a review and click
    🗑.

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

3.1.6 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.
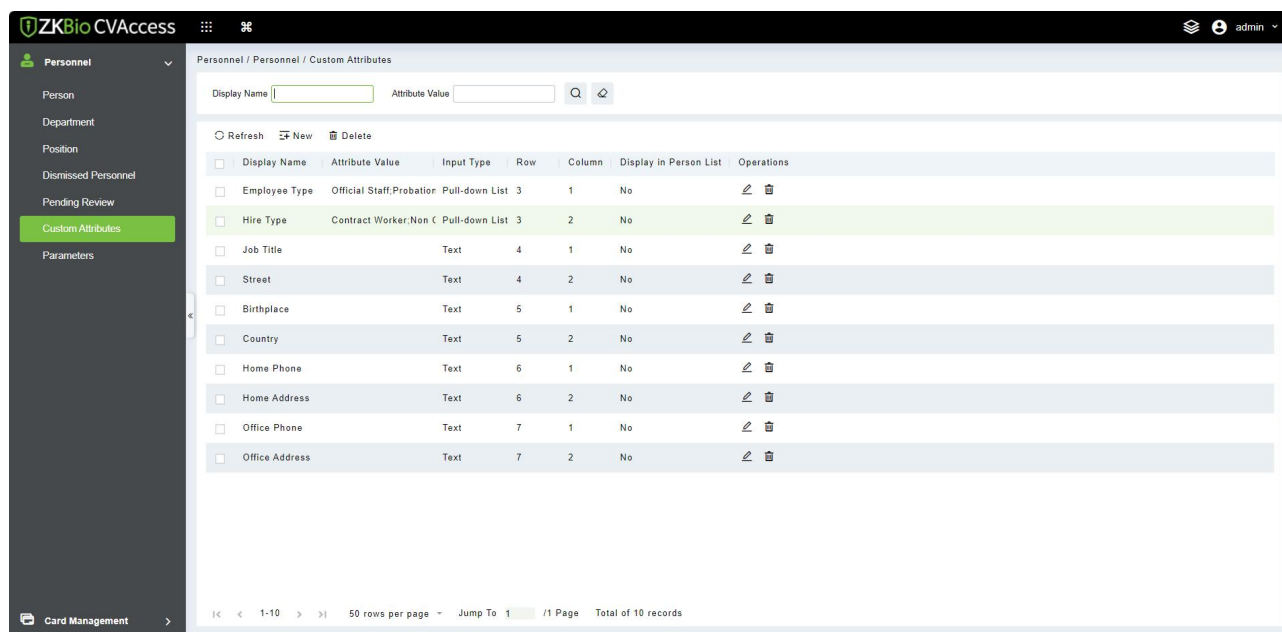
3.1.6.1 New a Custom Attribute

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

Fields are as follows:

- **Display Name:** Must be filled and should not be repeated. Max length is 30.

- **Input Type:** Select the display type from "Pull-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 distinguish 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 can be either 1 or 2, and the row number can only be 3 to 20. 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.

3.1.6.2 Editing a Custom Attribute

Click ✎ to modify the corresponding attributes.

3.1.6.3 Deleting 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.

3.1.7 Parameters

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

2.   You can set the maximum length for a Personnel ID and whether it will support letters or not. If Personnel ID Auto increment is selected as Yes, then while adding personnel, the ID in the field automatically updates to the next succeeding new number.

3.   Set the maximum length (binary number) of the card number that the current system will support.

4.   Set the card format currently used in the system. The card format cannot be switched once it is set up.

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

3.2 Card Management

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

3.2.1 Card

It shows the cards issued in the system with their status.
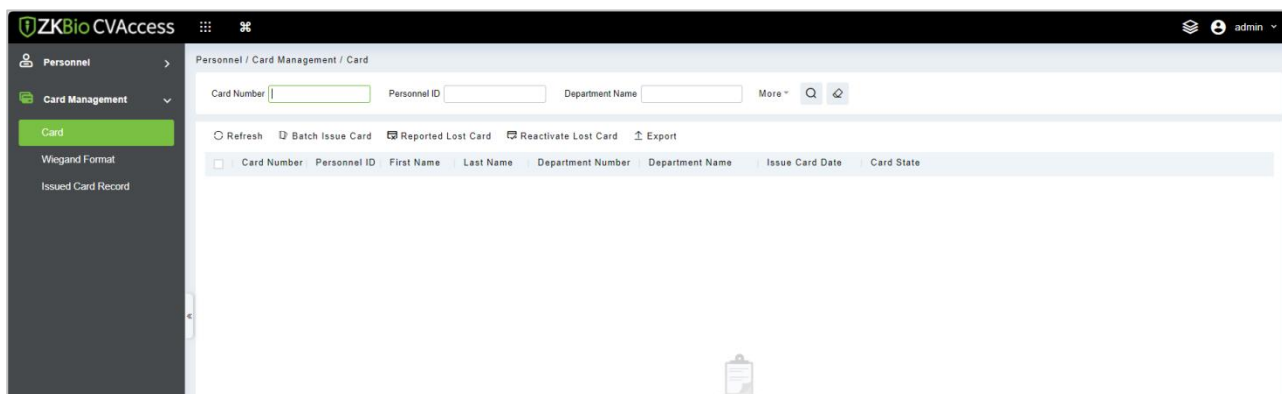
3.2.2 Wiegand Format

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.
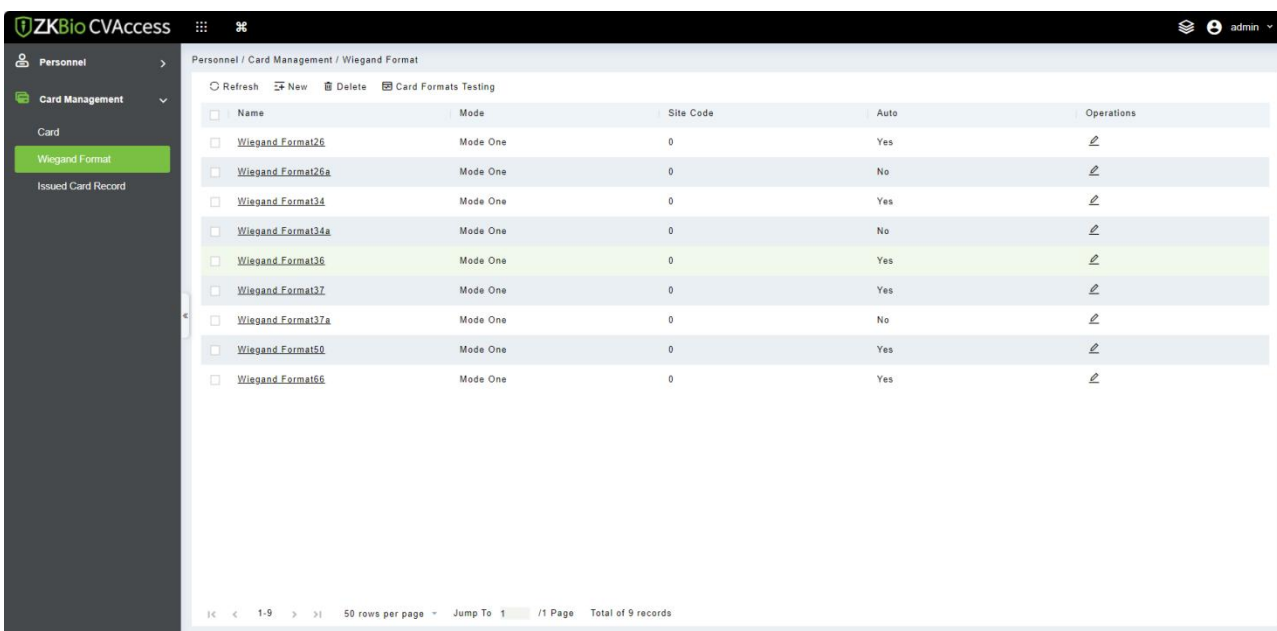
This software supports two modes for adding Wiegand Format, if mode 1 does not meet your setting requirement, you may switch it to mode 2. Take Wiegand Format 37 as an example:

Format Specifying:

"P" indicates Parity Position; "s" indicates Site Code; "c" indicates Cardholder ID; "m" indicates Manufacturer 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 "eeeeeeeeeeeeeeeeeee"; the second parity bits check "ooooooooooooooooooo". Card Check Format can only be set "p, x, m, c, s"; Parity Check Format can only be set "x, b, o, e".

3.2.3 Issue Card Record

It records the life cycle of a card and will display the operations performed on the card.

✎**Note:** The cards and card issuing records of an employee will be deleted altogether when the employee's account is deleted completely.

4   Access Control

The system needs to be connected to an access controller to provide access control functions. To use these functions, the users must install 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 management of the enterprise.
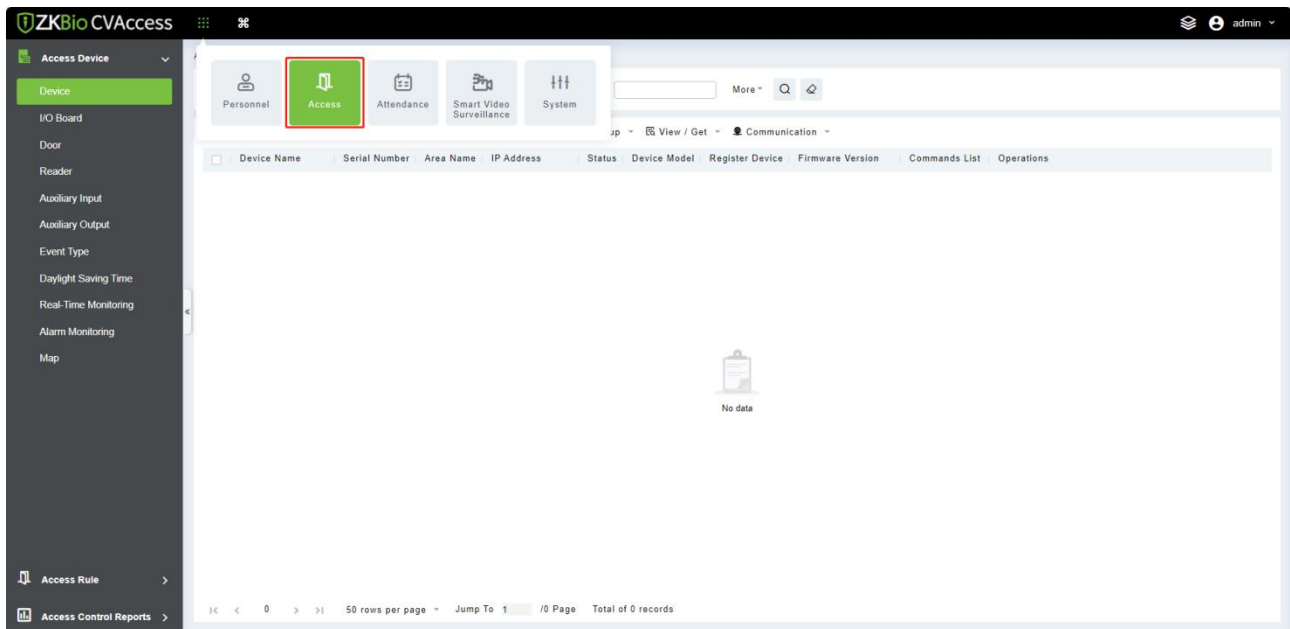
4.1 Device

Add an access device, then set the communication parameters of the connected devices, including system settings and device settings. When communication is successful, you can view here the information of the connected devices, and perform remote monitoring, uploading and downloading, etc.
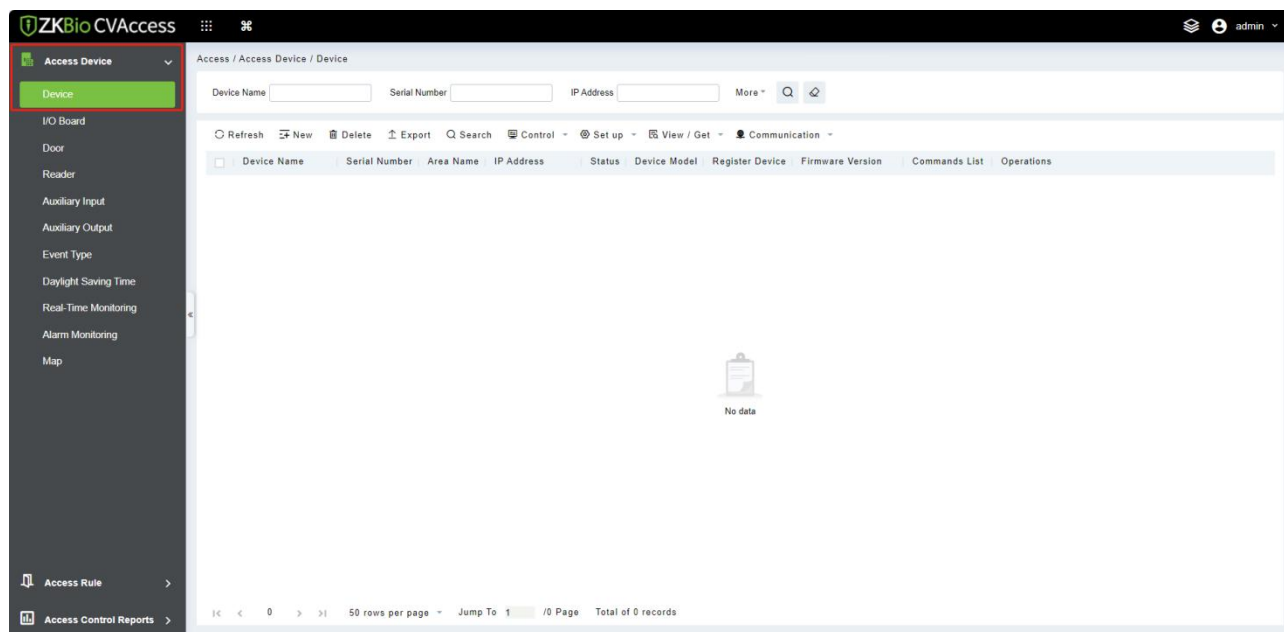
4.1.1 Device

4.1.1.1 Add Device

There are two ways to add Access Devices.

➢ **Add Device Manually**

1. Click **[Access] > [Device] > [New]** on the Action Menu, the following interface will be shown:
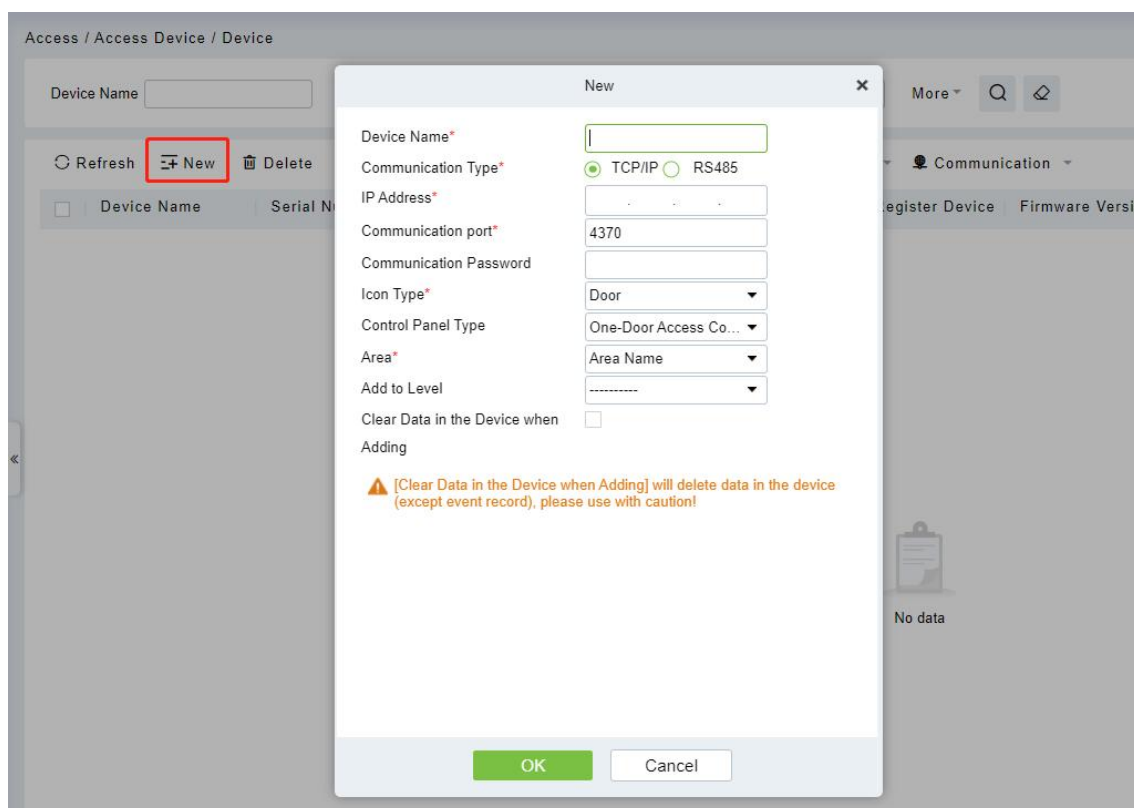
Fields are as follows:

- **Device Name:** Any character, up to a combination of 20 characters.

- **IP Address:** Enter the IP Address of the device.

- **Communication port:** The default value is 4370.

- **Communication Password:** A Password should be a combination of numbers and letters of 6 digits.

✍**Notes:**

(1) You do not need to input this field if it is a new factory device or just completed initialization.

(2) When communication password for the standalone device is set as "0", it means no password. However, in case of access control panel, it means the password is 0.

(3) You need to restart the device after setting the door sensor of the standalone device.

- **Icon Type:** It will set the representation of the device. You can choose as per the kind of device; Door and Flap Barrier.

- **Control Panel Type:** One-door access control panel, two-door access control panel, four-door access control panel, Standalone Device.

- **Area:** Select specific areas of devices. After setting areas, devices (doors) can be filtered by areas upon Real-Time Monitoring.

- **Add to Level:** Automatically add the device to the selected level. The device cannot be automatically added to the selected level if the number of personnel exceeds 5000. You can add personnel after the device is successfully added.

- **Clear Data in the Device when Adding:** If this option is checked, 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 select it.

2. After editing, click **[OK]**, and the system will try to connect the current device.

If it is successfully connected, it will read the corresponding extended parameters of the device.

✍**Note:** When deleting a new device, the software will clear all user information, time zones, holidays, and access control levels settings (including access levels, anti-pass back, interlock settings, linkage settings, etc.) from the device, except the events records (unless the information in the device is unusable, or it is recommended not to delete the device is used to avoid loss of information).

➢ **Add Device by Searching Access Controllers**

1. Click **[Access]** > **[Device]** > **[Search]**, to open the Search interface.
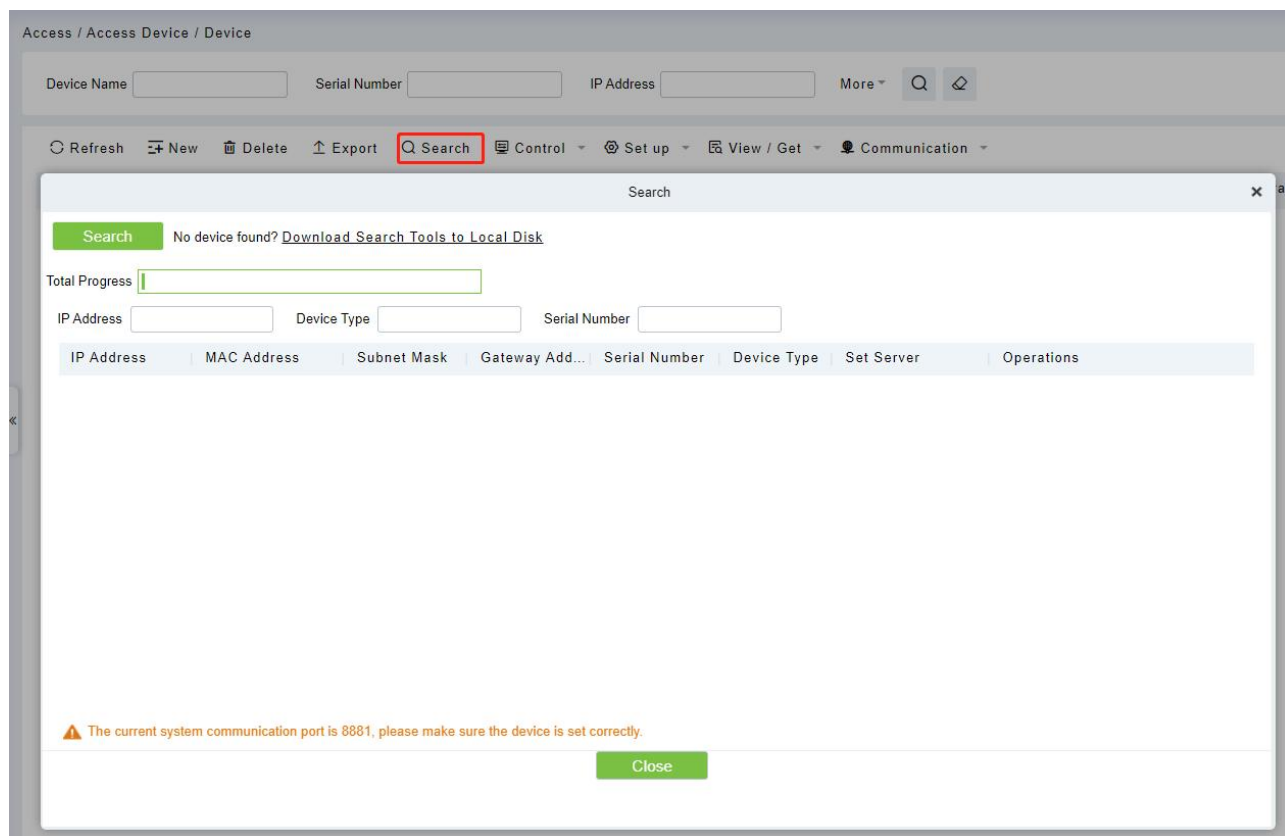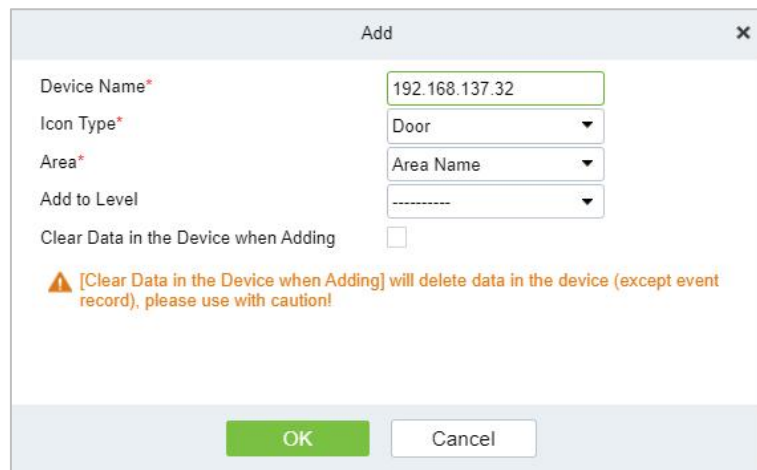
2.   Click **[Search]**, and it will prompt "Searching……".

3.   After the search is complete, the list and the total number of access controllers will be displayed.
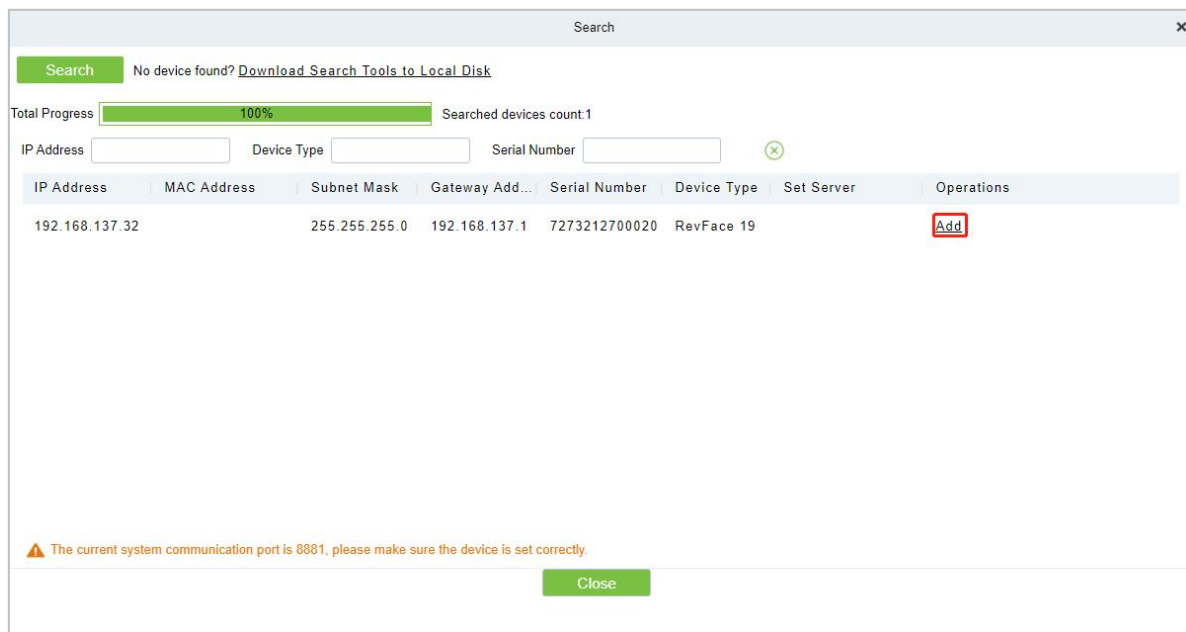
☞ **Note:** UDP broadcast mode will be used to search access devices. This mode cannot perform a cross-Router function. IP address can provide cross-net segment, but it must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.
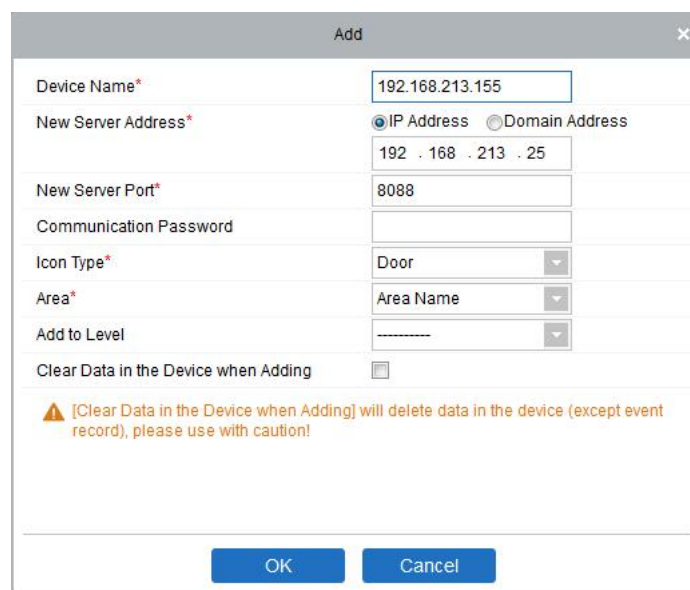
4.   Click on **[Add]** in the search list.

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

- **Clear Data in the Device when Adding:** If this option is selected, after adding device, the system will clear all data in the device (except the event logs).

If the device is a push firmware 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. The device will be added to the software automatically.

- **New Server Address:** To add a device by IP Address or Domain Address, devices can be added to the software by entering the domain address.

- **New Server Port:** Set the access point of system.

- **DNS:** Set a 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.
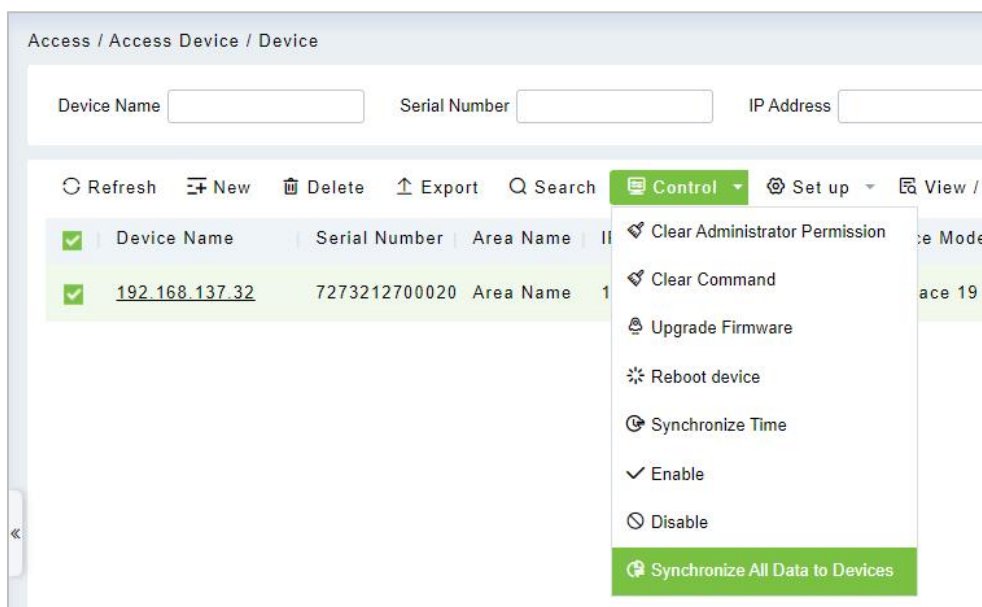
The default IP address of the access device may conflict with the IP of a device on the local network. You can modify its IP address: click **[Modify IP Address]** beside the **[Add]** and a dialog box will pop up in the interface. Enter the new IP address and other parameters (Note: Configure the gateway and IP address in the same net segment).

✍**Note:** Some PUSH devices support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

4.1.2 I/O Board

On the device module, click **[Device]> [I/O Board]> [New]** to add the I/O Board device to the software.
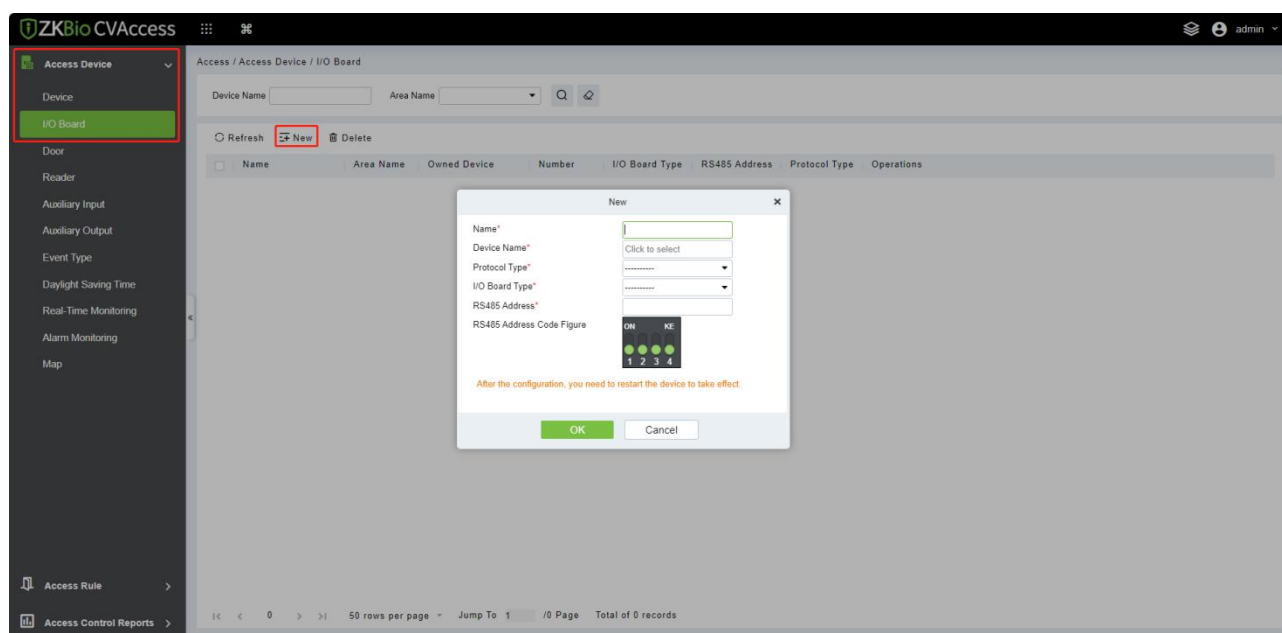
Enter the name of the I/O Board. Select the Device by clicking the Device Name field. The device list

appears as shown below:
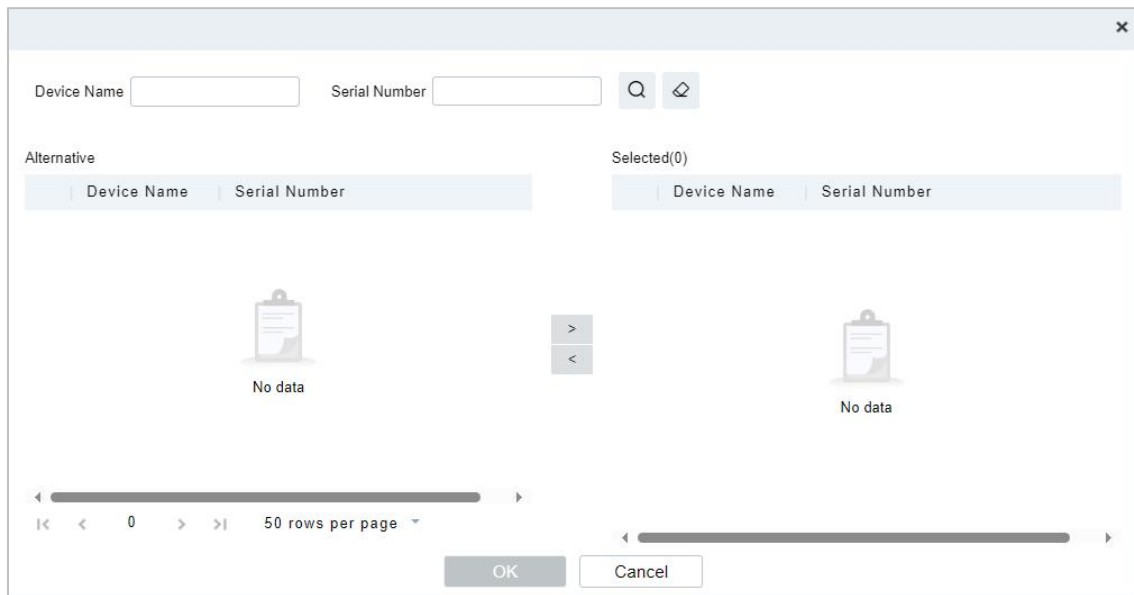
Select the device and click **OK**. Select the I/O Board Type. Set the RS485 Code Address by changing the corresponding button. Click OK to save the details. You can view all the auxiliary inputs in **[Auxiliary Input]** interface.
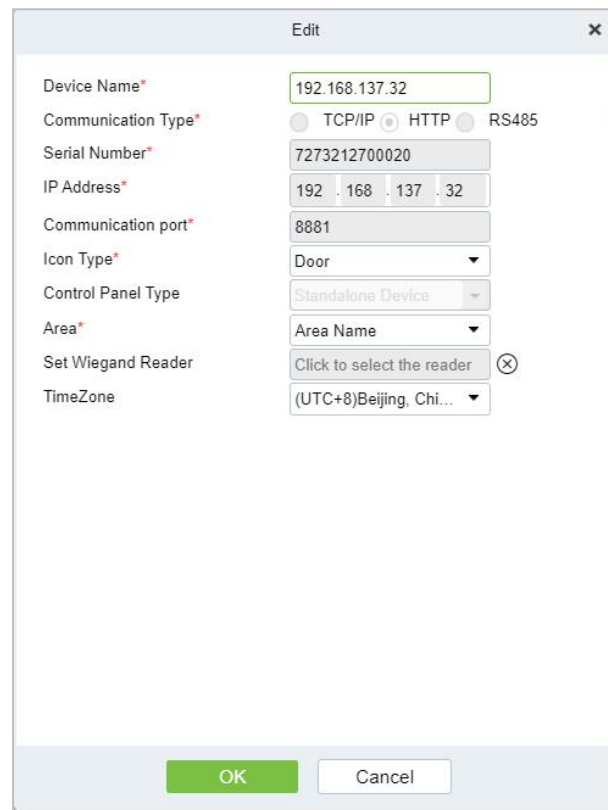
4.1.3 Device Operation

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

4.1.3.1 Edit or Delete a Device

- **Edit:** Click the Device Name or click **[Edit]** to access the edit interface.

- **Delete:** Select the device, click **[Delete]**, and click **[OK]** to delete the device.
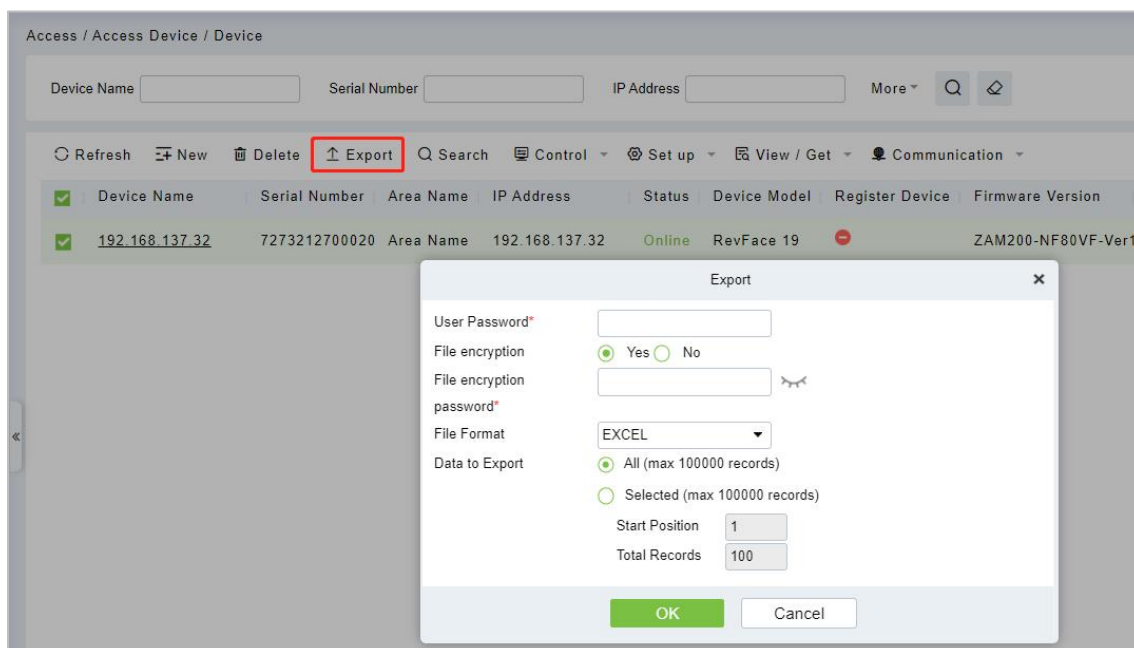
For the details and settings of the above parameters, see Device. Some details cannot be edited. The device Name should be unique and must not be identical to another device.

Control Panel Type cannot be modified. If the type is wrong, users need to manually delete the device and add it again.

4.1.3.2 Export

Device information can be exported in EXCEL, PDF, and CSV file format.

Device										
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Status	Device Model	Register Device	Firmware Version
SpeedFace-V5	CGFE184760043	Area Name	HTTP	Wired	192.168.213.67		Offline	SpeedFace-V5	Yes	1.0.55

4.1.3.3 Clear Administrator Permission

Select the required device, click **[Clear Administrator Permission]** to clear device administrator permissions, and click **[OK]** to finish.
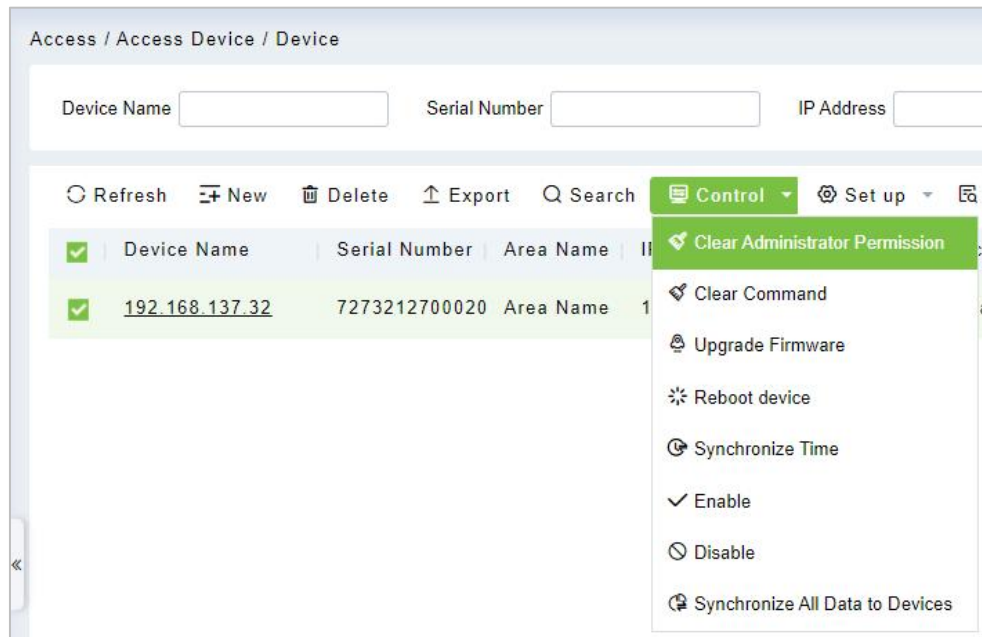
4.1.3.4 Clear Command

Select the required device, click **[Clear Command]** to clear the command being synchronized to the device, and click **[OK]** to finish.
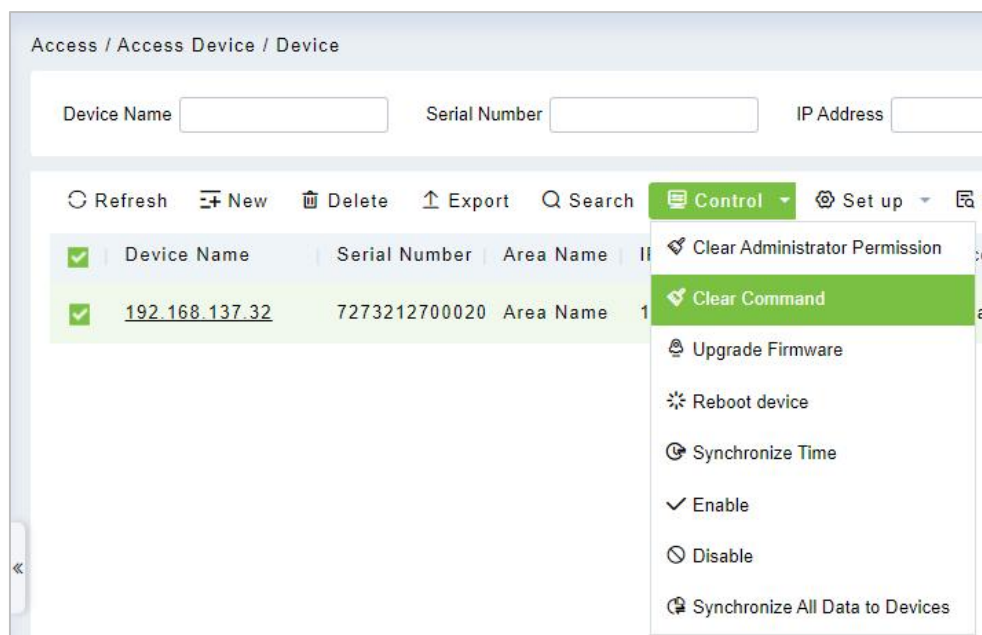
4.1.3.5 Upgrade Firmware

Select the required device that needs to be upgraded, click **[Upgrade firmware]** to enter edit interface, then click **[Choose File]** to select firmware upgrade file (named emfw.cfg) provided by Access software, and click **[OK]** to start upgrading.
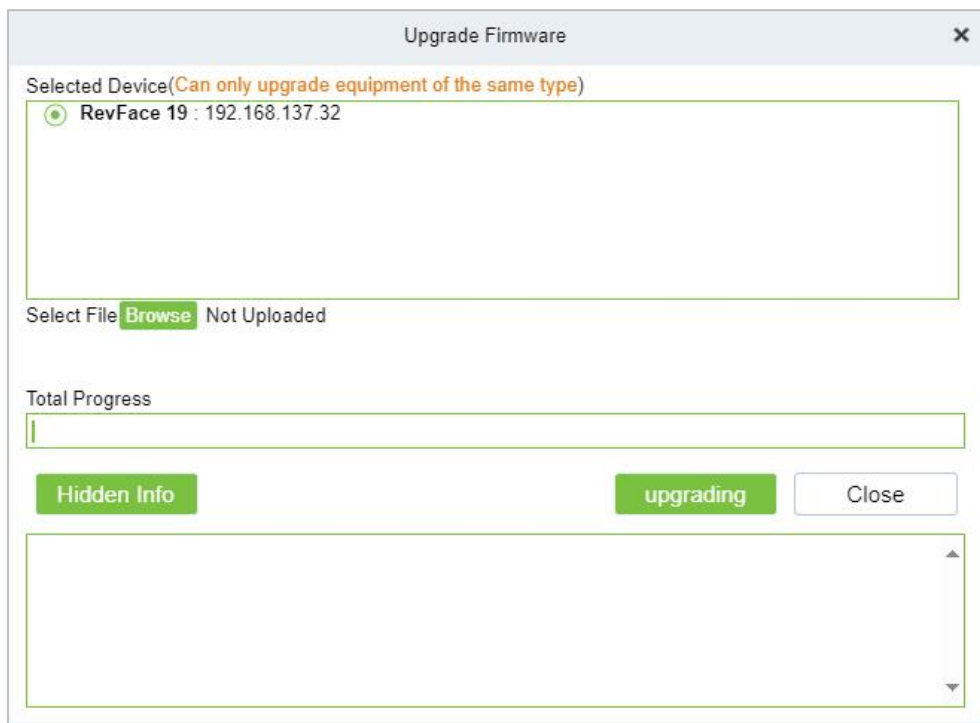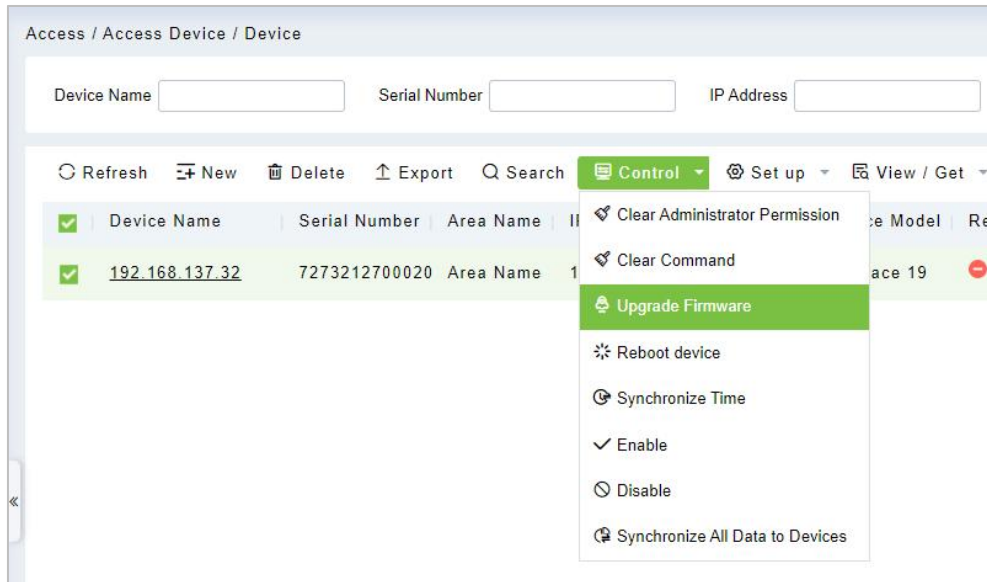
✍ Note: The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware or upgrade it following the instructions of the distributor. The unauthorized upgrade may affect normal operations.

4.1.3.6 Reboot Device

It will reboot the selected device.
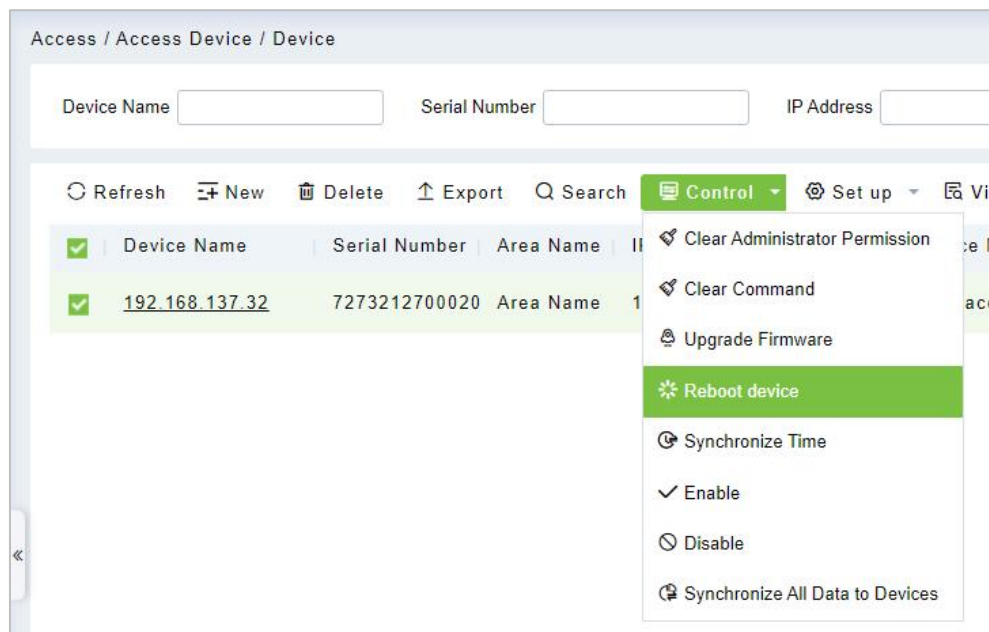
4.1.3.7 Synchronize Time

It will synchronize device time with the server's current time.
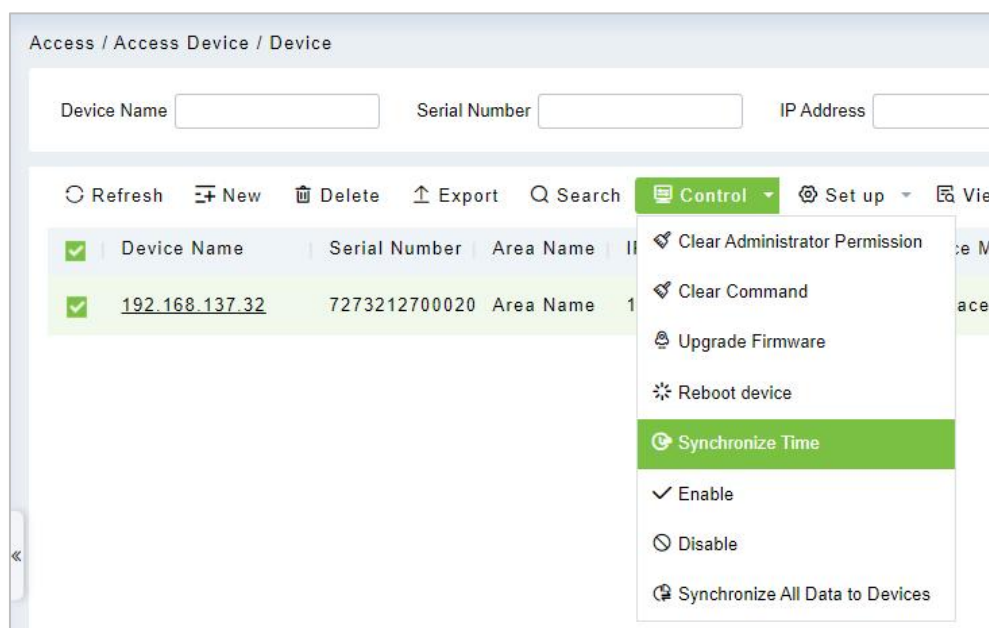
4.1.3.8 Disable/Enable

Select device, click **[Disable/ Enable]** to stop/ start using the device. When communication between the device and the system is interrupted or the device fails, the device may automatically appear in disabled status. After adjusting the local network or device, click **[Enable]** to reconnect the device and restore device communication.
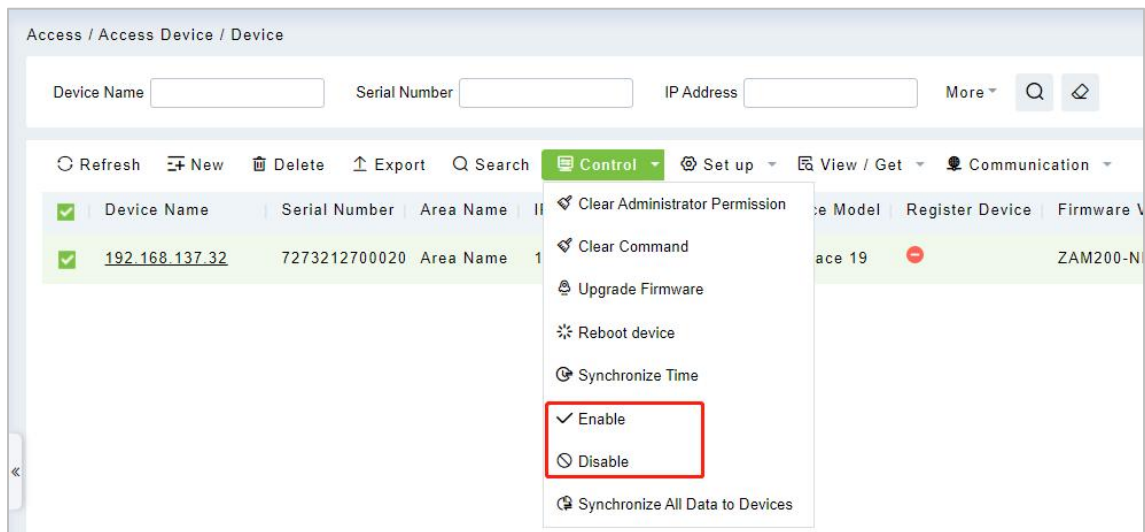
4.1.3.9 Synchronize All Data to Devices

Synchronize data of the system to the device. Select device, click **[Synchronize All Data to Devices]** and click **[OK]** to complete synchronization.
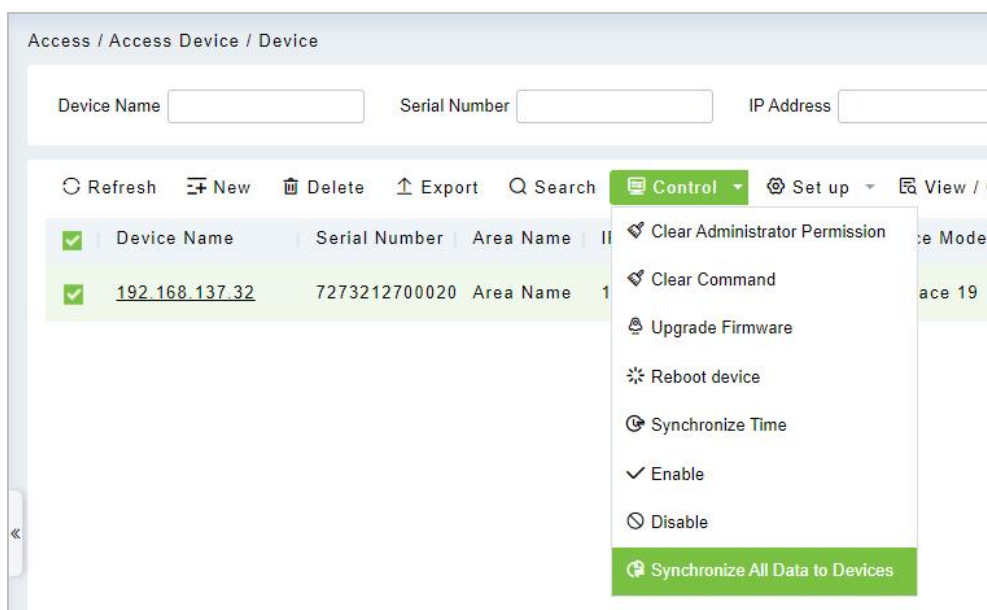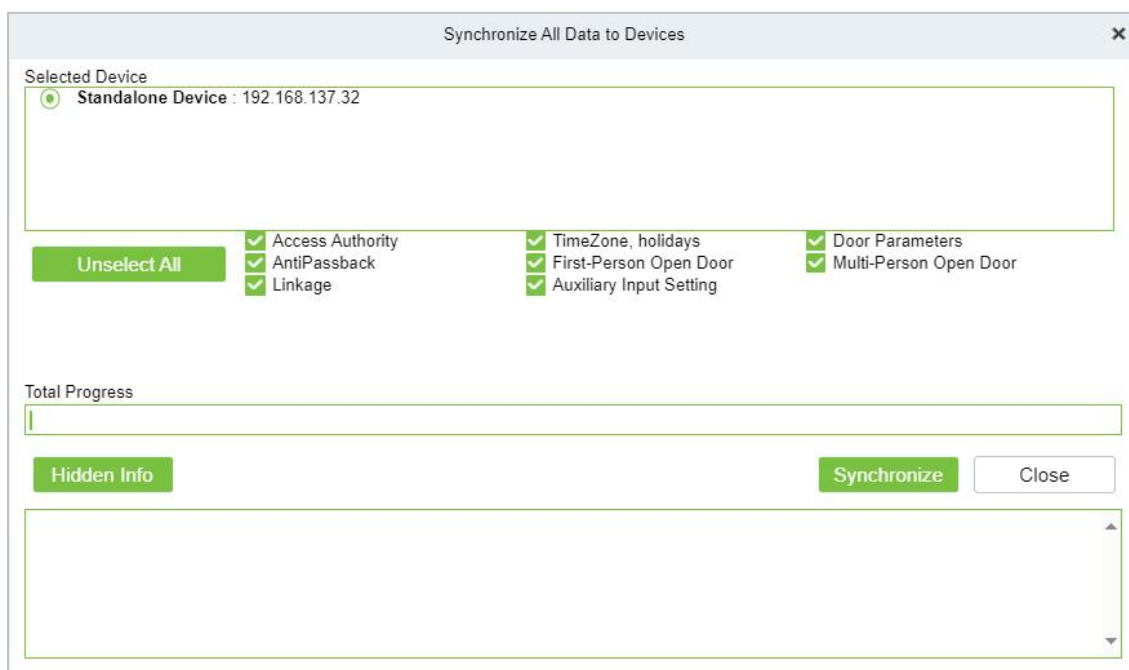
 Note: [Synchronize All Data to Devices] will delete all data in the device first (except transactions), and thus download all settings again. Please keep the internet connection stable and avoid power down situations. If the device is working normally, please use this function with caution. Execute it in rare user situations to avoid impact on normal use of the device.

4.1.3.10 Set Device Time Zone

If the device supports the time zone settings and is not in the same time zone with the server, you need to set the time zone of the device. After setting the time zone, the device will automatically synchronize the time according to the time zone and server time.
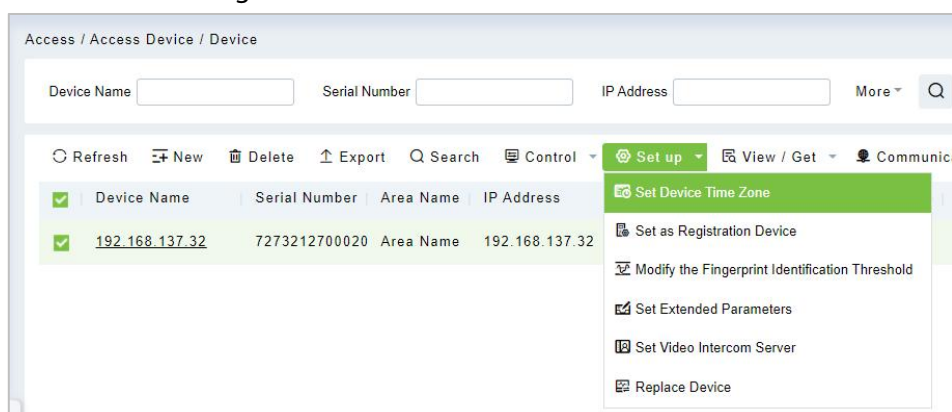
4.1.3.11 Set as Registration Device

Set the registration device only when the standalone device's data such as personnel can automatically upload.
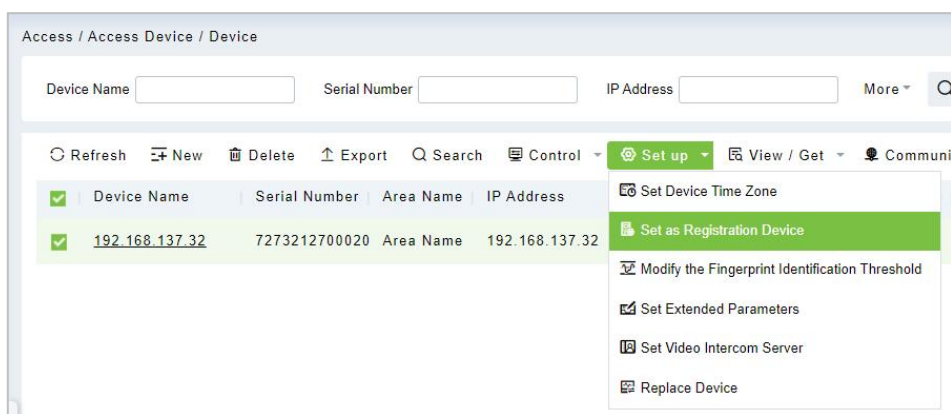
4.1.3.12 Modify the Fingerprint Identification Threshold

✐**Note:** Ensure that the access controller supports fingerprint function.
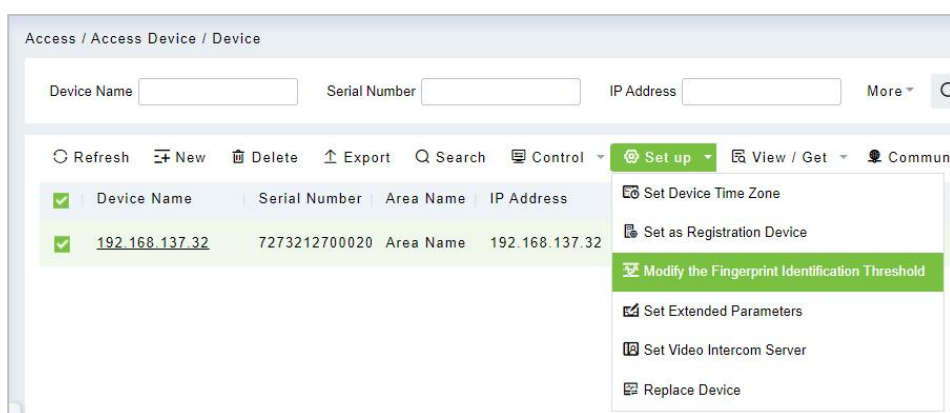
4.1.3.13 Set Video Intercom Server

Configure the address of the video intercom server for the visible light device.
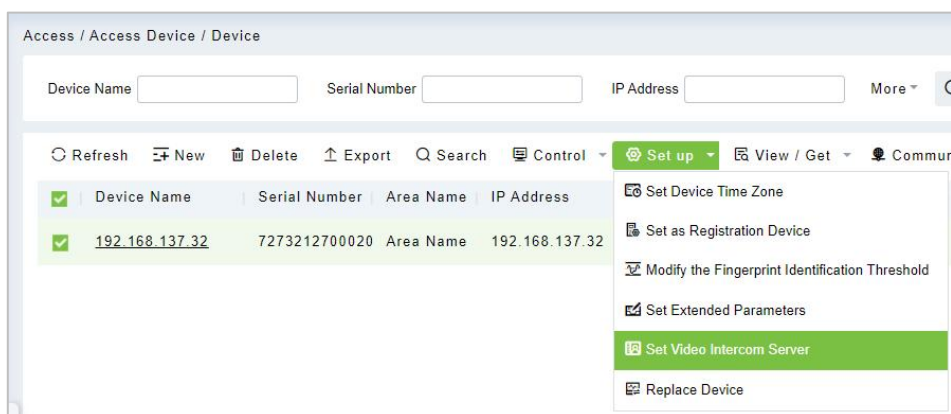
4.1.3.14 Replace Device

Quick device replacement function. When the device is broken, only need to enter the serial number of the new device, you can quickly copy the data of the old device to the new device.

✐ **Note:** Only devices of the same type can be replaced, such as visible light devices can only be replaced with visible light devices, and controllers can only be replaced with new controllers.
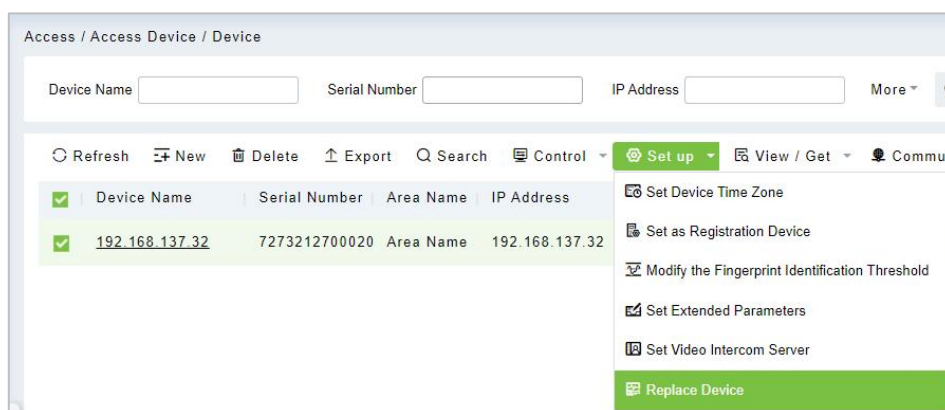
4.1.3.15 Get Device Option

It gets the common parameters of the device. For example, get the firmware version after the device is updated.
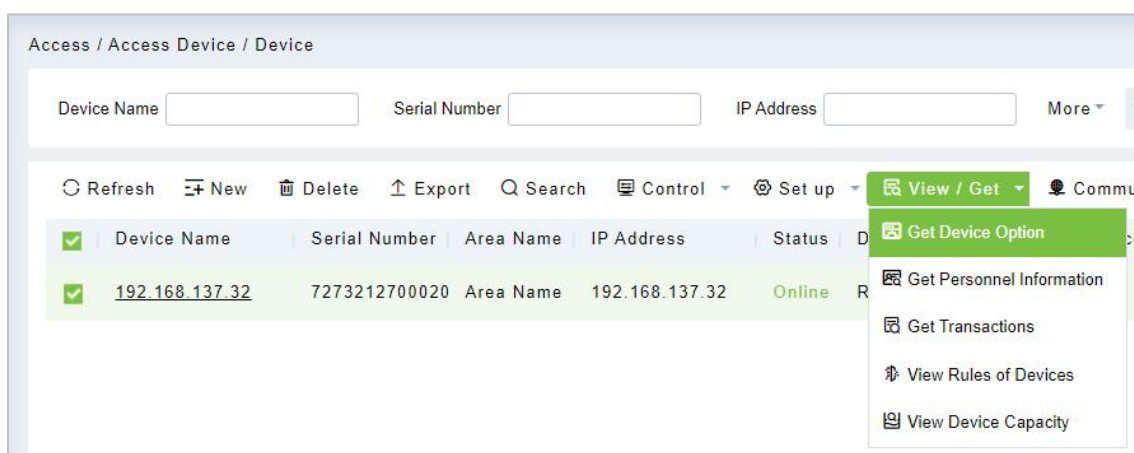
4.1.3.16 Get Personnel Information

Renew the current number of personnel, fingerprints, finger vein and face templates in the device. The final value will be displayed in the device list.
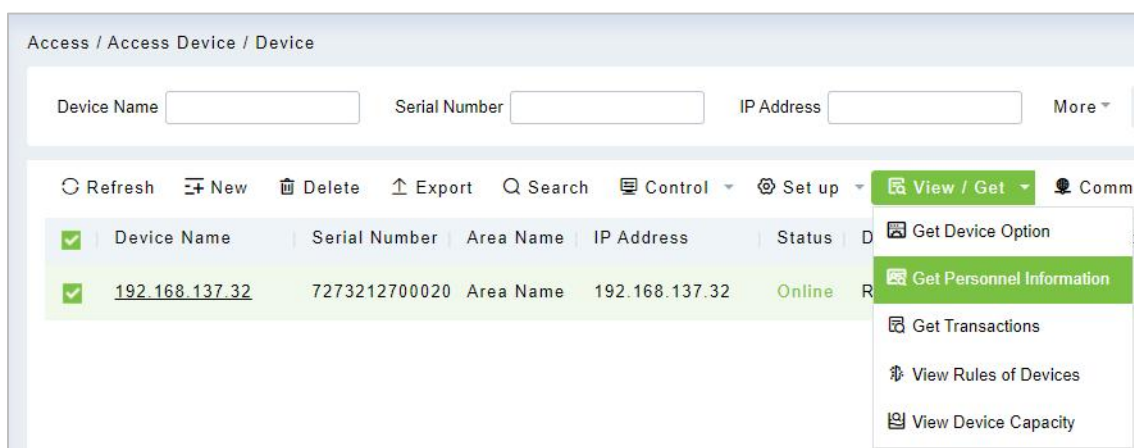
4.1.3.17 Get Transactions

Get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.
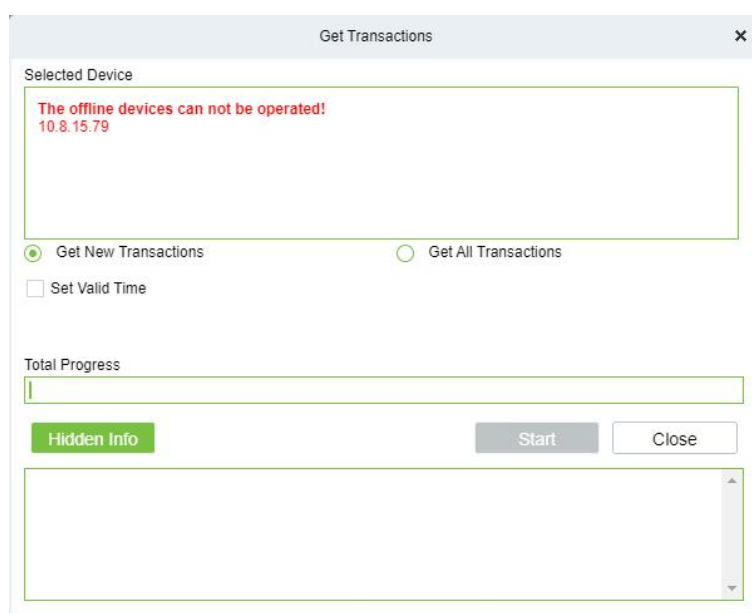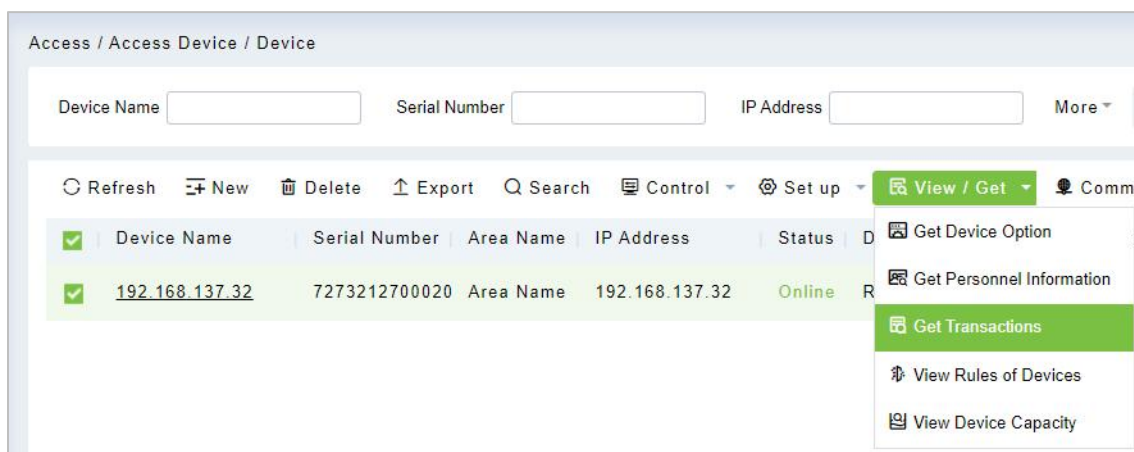
- **Get New Transactions:** The system only gets new transactions since the last collected and recorded transaction. Repeated transactions will not be rewritten.

- **Get All Transactions:** The system will get transactions again. Repeated entries will not be shown twice.

When the network status is healthy and the communication between the system and device is normal, the system will acquire transactions of the device in real-time and save them into the system database. However, when the network is interrupted or communication is interrupted for any reason, and the transactions of the device have not been uploaded into the system in real-time, **[Get Transactions]** can be used to manually acquire transactions of the device. In addition, the system, by default, will automatically acquire transactions of the device at 00:00 on each day.

✎**Note:** Access controller can store up to 100 thousand transactions. When transactions exceed this number, the device will automatically delete the oldest stored transactions (deletes 10 thousand transactions by default).

4.1.3.18 View Rules of Devices

Shows the Access rules in the device.
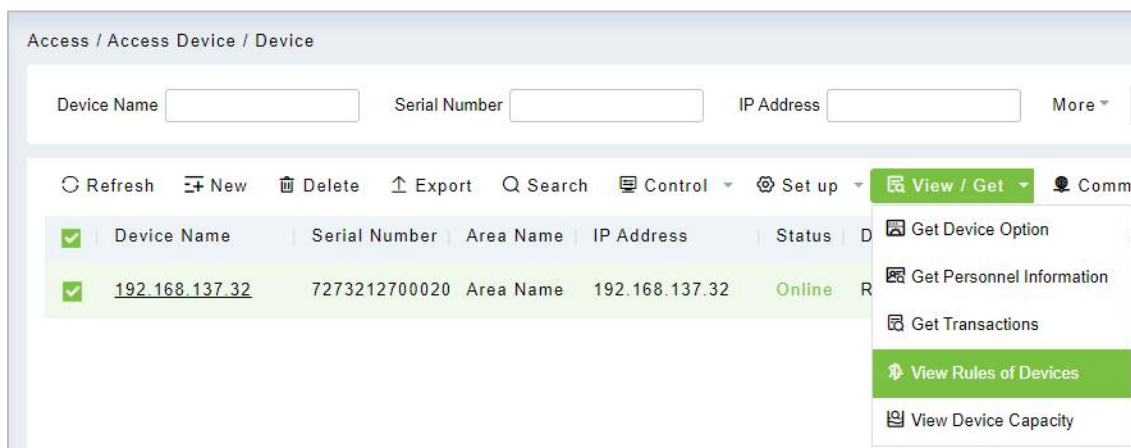
4.1.3.19 View Device Capacity

It checks the capacity of personnel's biometric details in the device.
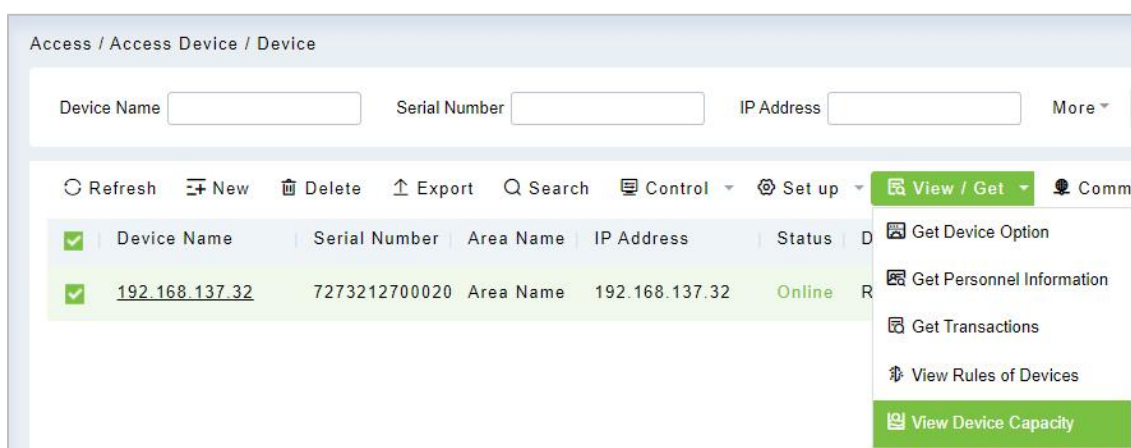
4.1.3.20 Modify IP Address

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 similar to **[Modify IP Address Function]** in <u>Device.</u>
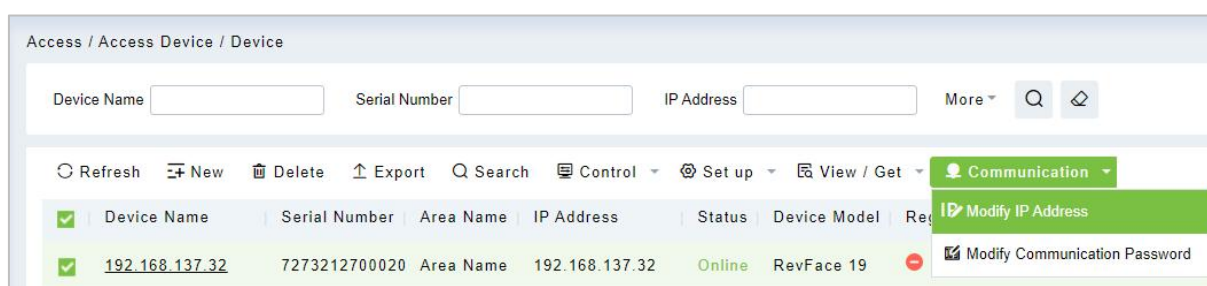
4.1.3.21 Modify Communication Password

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.
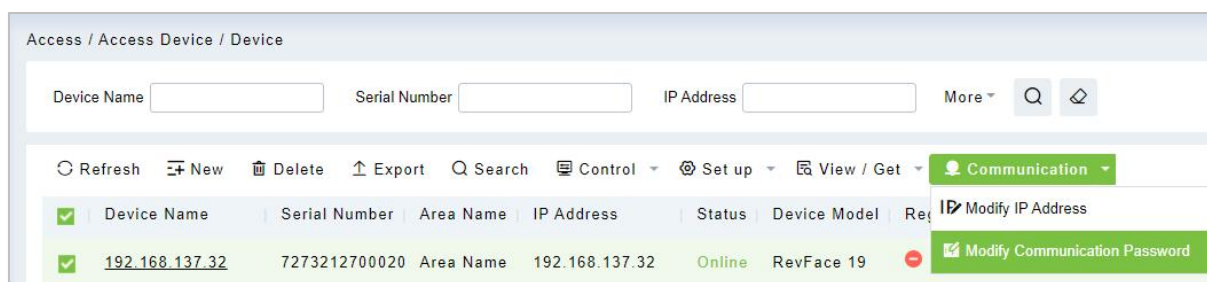
✎Note: A Password should be a combination of numbers and letters of 6 digits.

Users can modify the fingerprint identification thresholds in the devices; it ranges from 35 to 70 and it is 55 by default. The system will read the thresholds from the device. Users can view the threshold devices list. More than one device can be changed by using the Batch operation function.

4.1.4 Doors

1. Click **[Access]** > **[Device]** > **[Door]** to enter Door Management interface (click "Area Name" in the left, the system will automatically filter and display all access devices in this area).
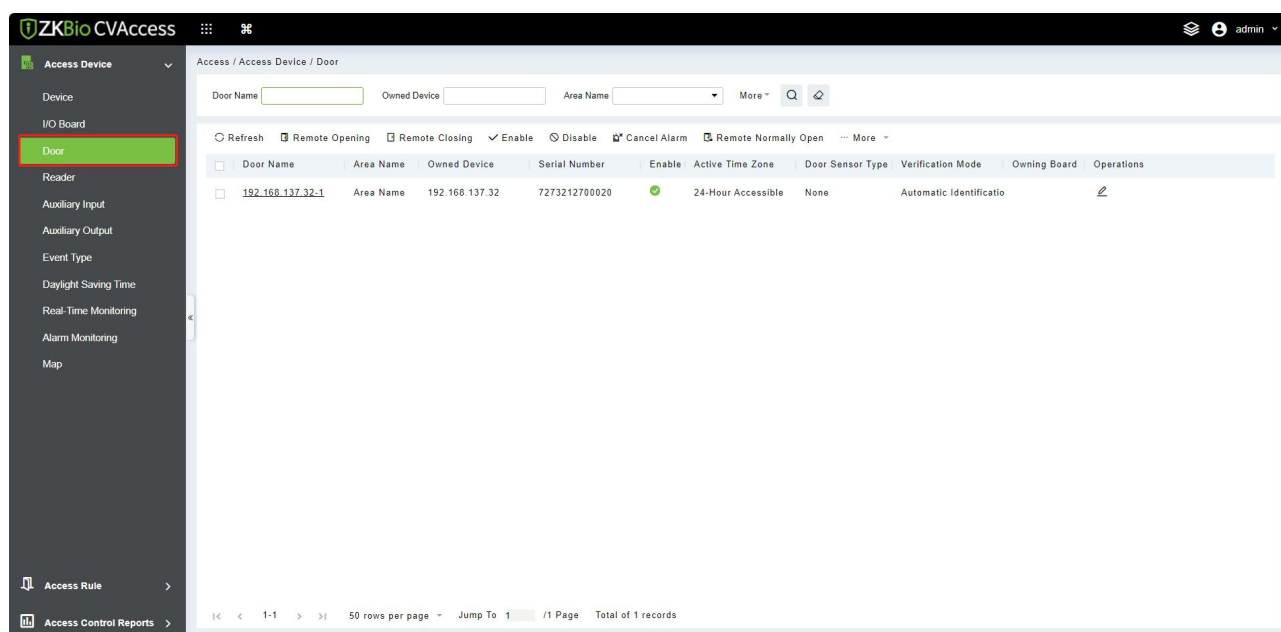
Select the door to be modified, and click the Door Name or ✎ button below the operations tab to open the Edit interface:

Fields are as follows:

- **Device Name:** It can't be edited.

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

✍Note: By default, the suffix number in the Door Name is consistent with the Door Number, but 1/2/3/4 in Anti-Passback and interlock refer to the Door Number, rather than the number following the Door Name, and they are not necessarily related.

- **Door Name:** The default is "device name - door number". The name can be modified as required. Numbers, letters or a combination of both are allowed up to 30 characters.

- **Active Time Zone:** Active Time Zone must be selected, so that the door can be opened and closed normally. A Passage Mode Time Zone must be set within the Active Time Zone.

✍ 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 during 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.

- **Verification Mode:** Identification modes include Automatic Identification, Only fingerprint, Only Pin, Only Password, Pin and Fingerprint, Fingerprint and Password, Pin and Password and Fingerprint, Face, Face and finger, Face and Finger and Password. The default value is Card or Fingerprint. When both Card and Password mode is selected, make sure the door is equipped with a reader that has a keyboard.

- **Lock Open Duration:** It is the time period for which the door remains unlocked after

successful verification. The unit is second (range: 0~254 seconds), and the default value is 5 seconds.

- **Operate Interval:** It is the time-interval between two verifications. The unit is Seconds (range: 0~254 seconds), and the default value is 0 seconds.

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

- **Door Sensor Type:** None (will not detect door sensor), Normally Open, Normally Close. If you have selected as Normally Open or Normally Close, you need to set Door Sensor Delay and decide whether or not Close and Reverse-lock is required. When the door sensor type is set as Normally Open or Normally Close, the default door sensor delay is 15 seconds, and then close and reverse state is enabled.

- **Door Sensor Delay:** It is the delayed duration for the 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: 1~254 seconds). Door Sensor Delay should be greater than the Lock Open Duration.

- **Duress Password, Emergency Password:** Duress means any threats, violence, constraints, or other action used to force someone into doing something against their will. In these situations, input Duress Password (with an authorized card) to open the door. When the door is opened with Duress Password, the alarm is triggered. Upon emergency, the user can use Emergency Password (named Super Password) to open the door. Emergency Password allows normal opening, and it is effective in any time zone and any type of verification mode, usually used for the administrator.

Duress Password Opening (used with an authorized card): 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 plus **[OK]** button, then finally punch legal card. The door opens and triggers the alarm. When Card + Password verify mode is used, please swipe legal card first, then press the password plus **[OK]** button (same as normal opening in card plus password verification mode), the door opens and triggers the alarm.

Emergency Password Opening: 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 Disable Alarm check box to disable the alarm voice in real-time monitoring page.

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

(1) All doors in the current device: Click to apply the above settings to all doors of the current access device.

(2)   All doors in All Control devices: Click to apply the above settings to all doors of all access devices within the current user's level.

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

4.1.5 Reader

1.   Click **[Device]** > **[Reader]** on the Menu, then click on reader name or ✎ button.
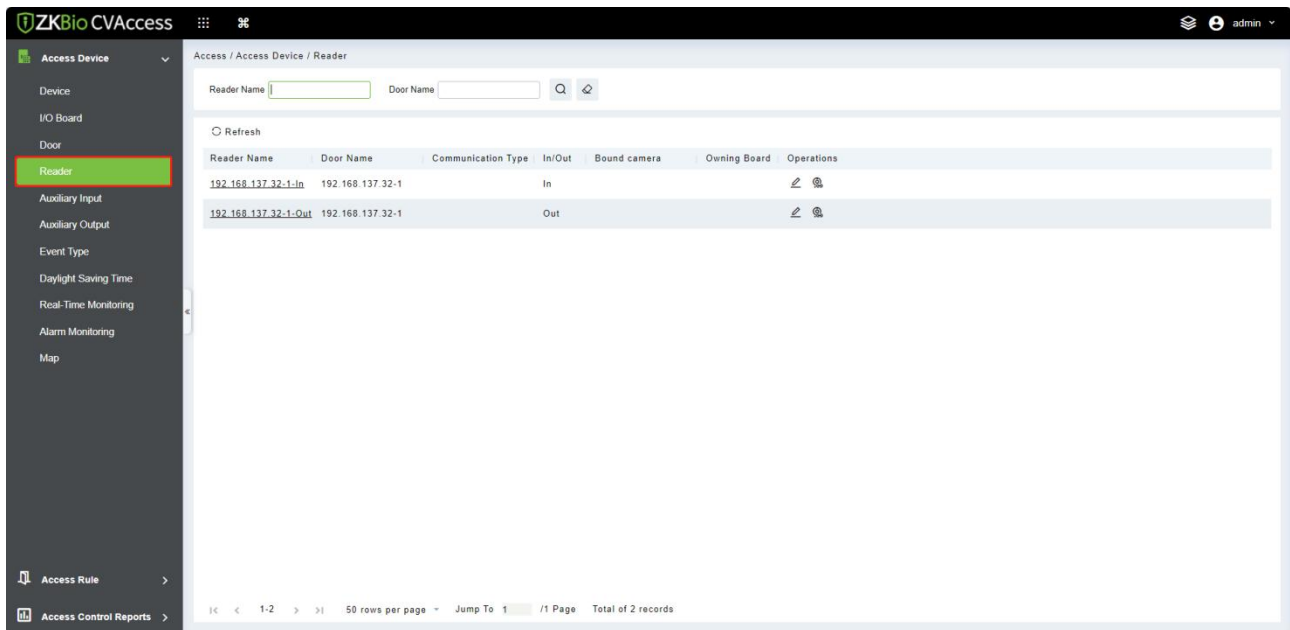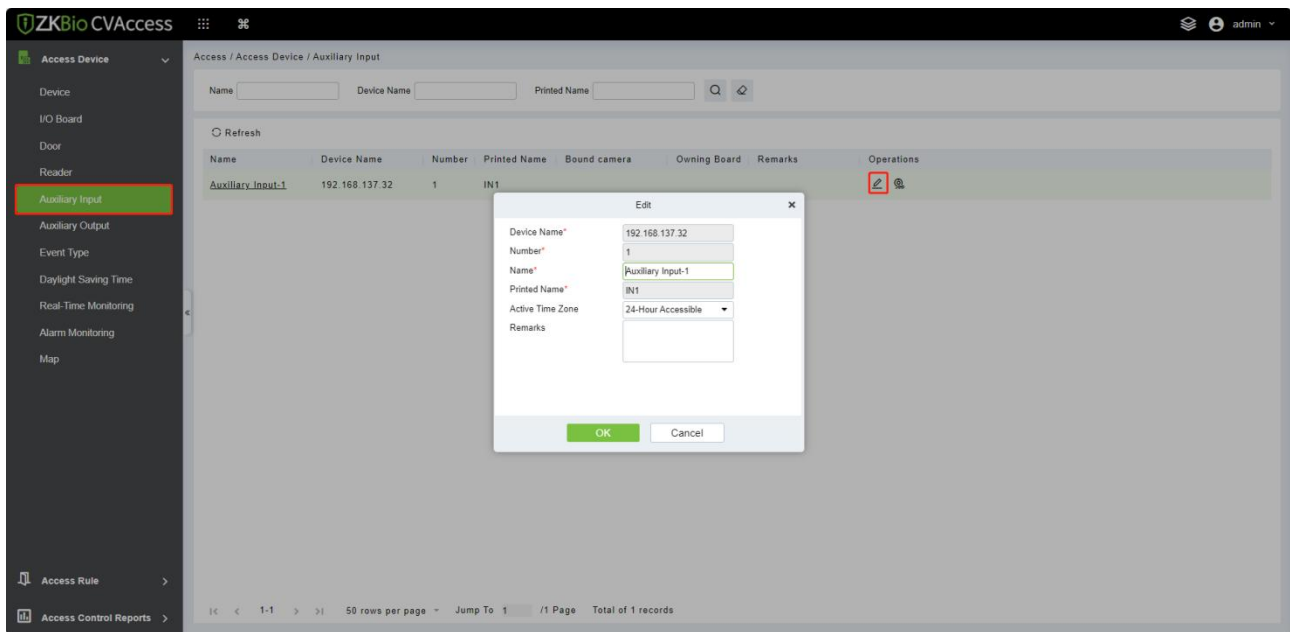

- **Name:** Set the name of the reader displayed on the list page.

4.1.6 Auxiliary Input

It is mainly used to connect devices like infrared sensors, smog sensors, smoke detectors, etc.

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

2.   Click on Name or ✎ button to modify the parameters as shown below:

Fields are as follows:

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

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

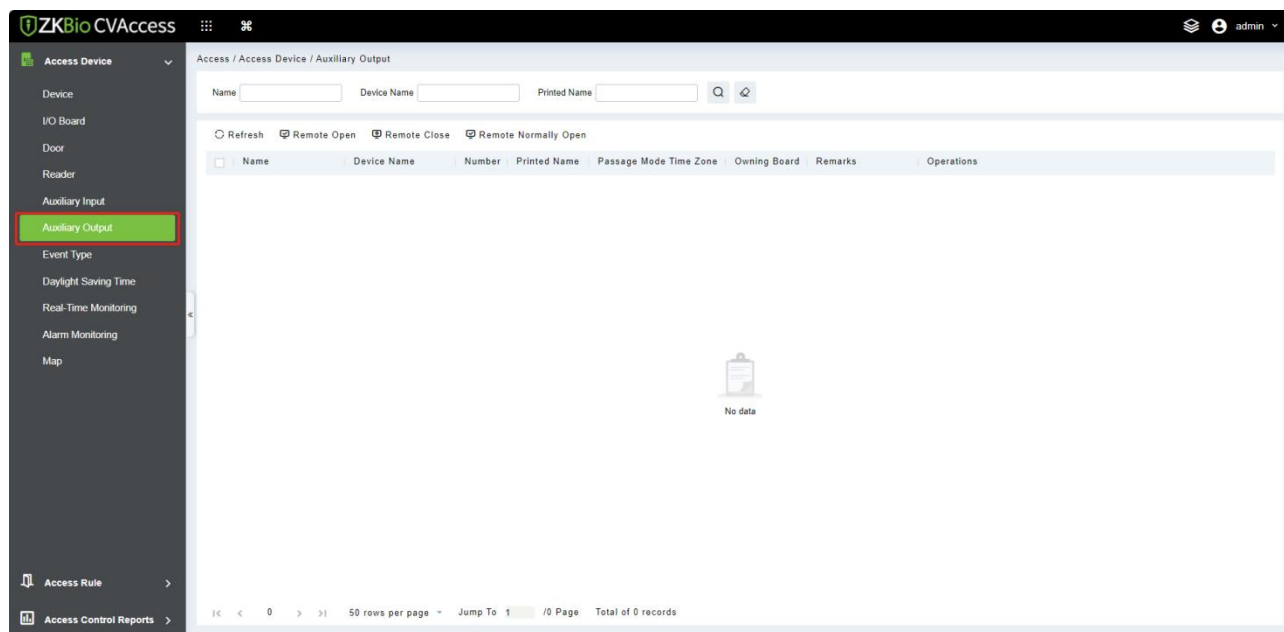- **Active Time Zone:** Auxiliary input will be available only in the specified time segment.

✍**Note:** Only Name can be modified.

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

4.1.7 Auxiliary Output

It is mainly used for alarm output and with active linkage function.

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

2.   Click ✐ button to modify the parameters:

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 normally open or normal close in the selected time zone.

✍**Note:** Only Name, Passage Mode Time Zone and Remarks can be modified.

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

4.1.8 Event Type

It will display the event types of access devices.

1.   Click **[Device]** > **[Event]** to access the following page:
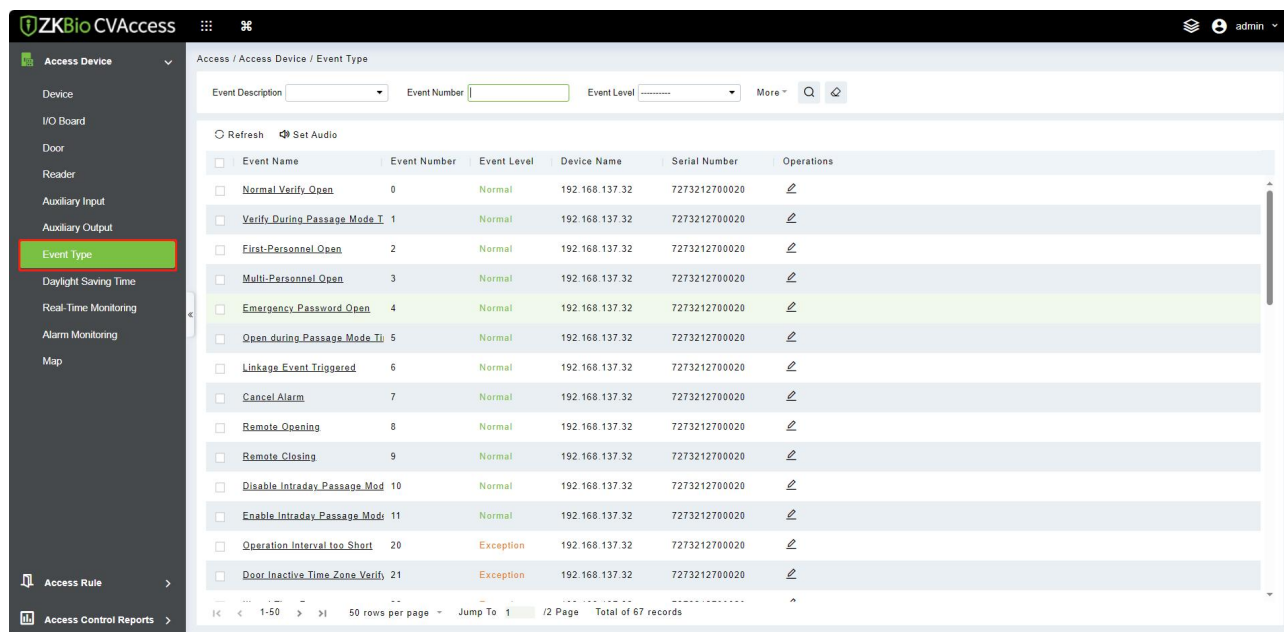
2.   Click **[Edit]** or click on the event type name to edit:
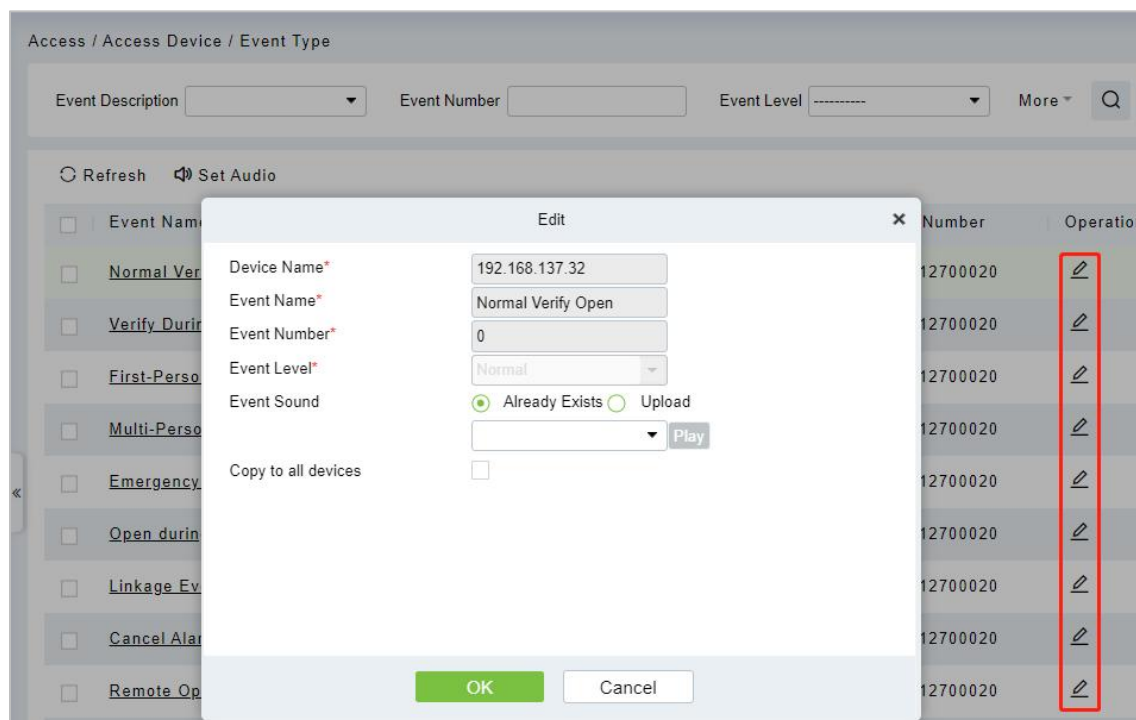
Fields are as follows:

- **Event Level:** Normal, Exception, and Alarm are available.

- **Event Name:** It cannot be modified.

- **Event Sound:** You can set custom sound being played when the event occurs in real-time monitoring.

- **Copy to all devices:** This event will be applied to all current devices within the purview of the same user event number.

➢ **Set Audio**

Same as the event sound. Click **[Set Audio]**:

You can upload audio from your local PC. The file must be in wav or mp3 format, and it must not exceed 10MB.

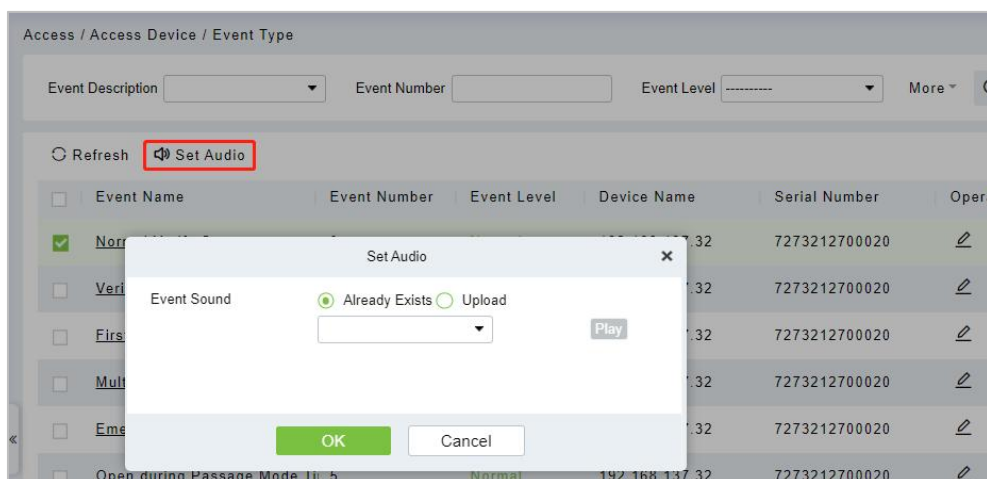For more details about Event Type, please refer to [Access Event Type.](#)

4.1.9 Daylight Saving Time

The Daylight-Saving Time is a function to adjust the official prescribes local time to save energy. The unified time adopted during the implementation is known as the "DST". Typically, regions that use daylight saving time adjusts clocks forward one hour to standard time close to the start of spring in the summer to make people sleep early. It can also help to save energy. In autumn, adjust clocks are adjusted backward to get up early. 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 ahead at (hour) (day) (month) and one hour backward at (hour) (day) (month) if necessary.
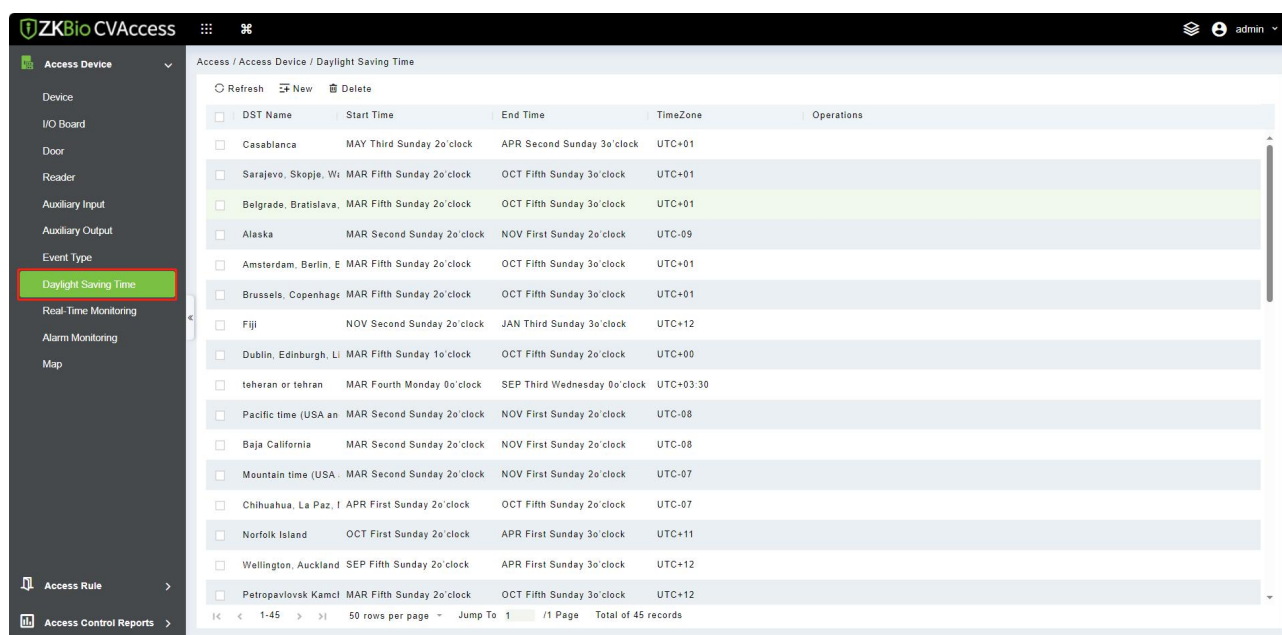
4.1.9.1 Add DST

1.   Click **[Access] > [Device] > [Daylight Saving Time]> [New]**:
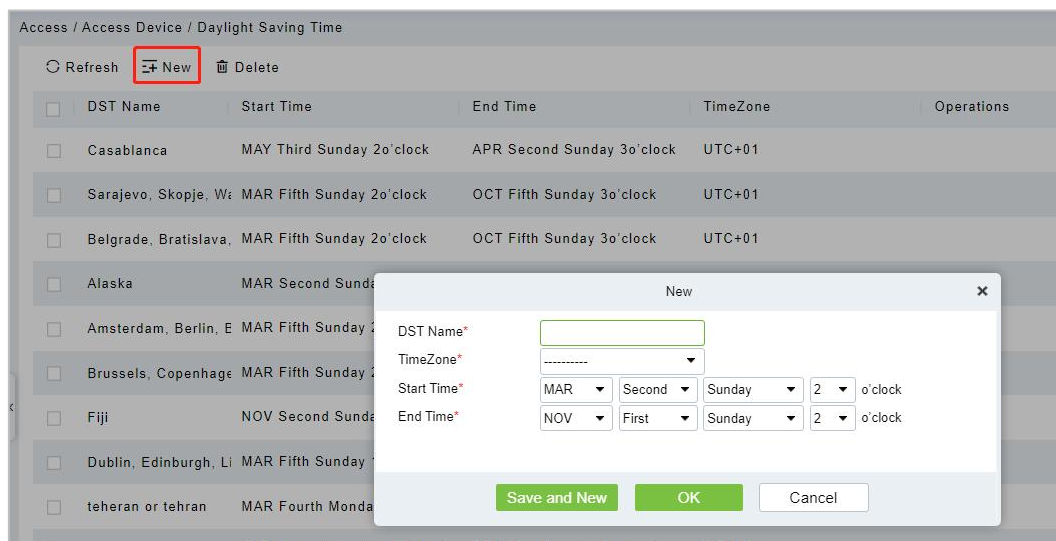
The row fields are as; "Month – Week – Day - Hour" format. For example, if the start time is set as "March – Second –Sunday – 2 o'clock" it means the DST will start from the second Sunday of March at 2 AM. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

4.1.10 Real-Time Monitoring

Click **[Access Device]** > **[Real-Time Monitoring]**.
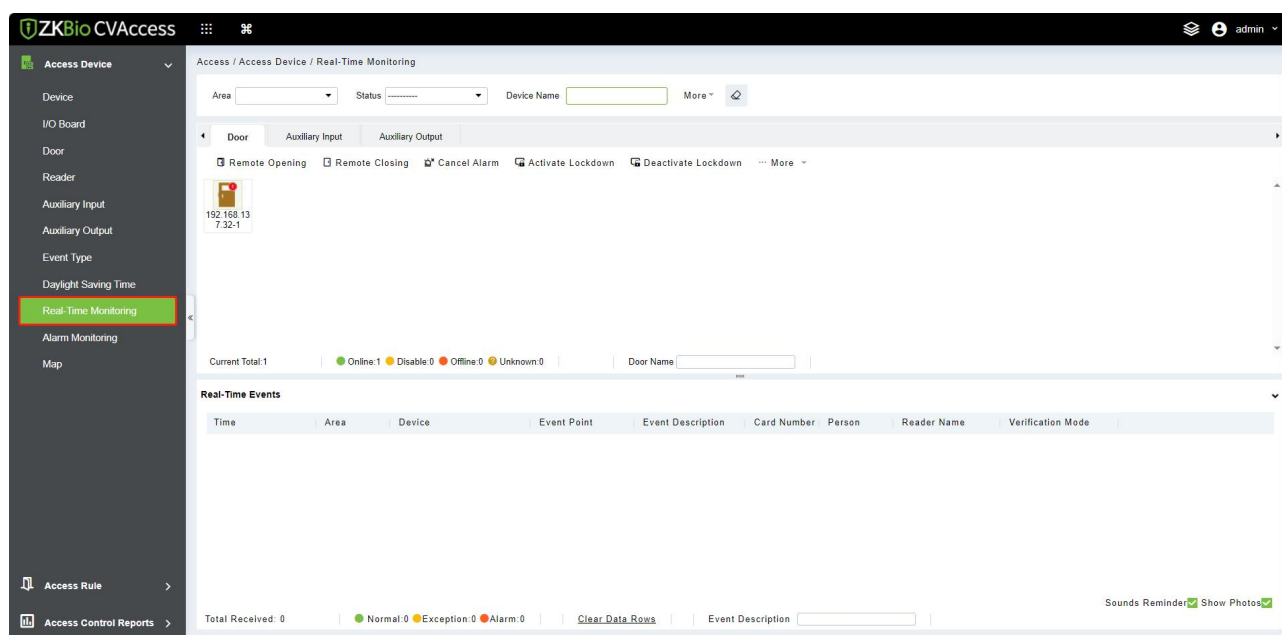
It will monitor the status and real-time events of doors under the access control panels in the system in real-time, including normal events and abnormal events (including alarm events).

The Real-Time Monitoring interface is shown as follows:

Icons	Status	Icons	Status
	Device blocked		Door Offline
	Door sensor not set; relay closed		Door sensor not set; relay opened
	Door sensor not set, and the present firmware does not support current action on the device		
	Online status Door closed; Relay closed		Online status Door closed; Relay opened
	Online status Door closed, and the present firmware does not support current action on the device		
	Online status Door opened; Relay closed		Online status Door opened; Relay opened
	Online status Door opened, and the present firmware does not support current action on the device		
	Door opened alarming; Relay closed		Door opened alarming; Relay opened

|			
🚪	Door opening timeout, Relay closed	🚪	Door opening timeout, Relay opened
🚪	Door opening timeout, and the present firmware does not support current action on the device		
🚪	Door opening timeout, Relay closed/Door Sensor Closed	🚪	Door opening timeout, Relay opened/ Door Sensor Closed
🚪	Door closed alarming; Relay closed	🚪	Door closed alarming; Relay opened
🚪	Door closed alarming, Indicates that the present firmware does not support current action on the device		
🚪	Door sensor not set, Door alarming, Relay closed	🚪	Door sensor unset, Door alarming, Relay opened
🚪	Door opening timeout, Without relay status/Door Sensor Closed	🔒	Door locking

Without relay status, it indicates that the current firmware does not support action on the device.

Different icons represent status as followed:
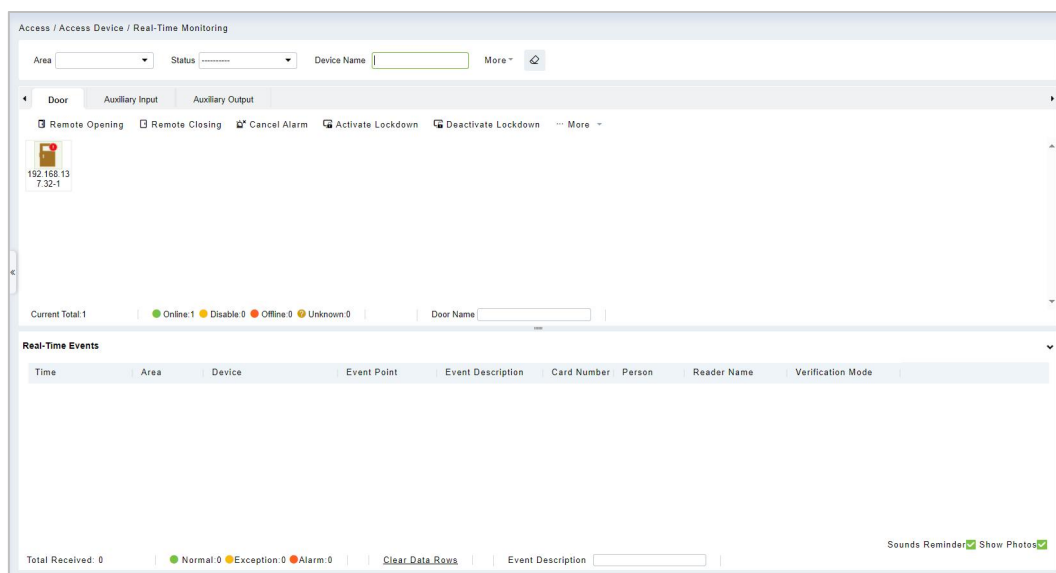
4.1.10.1 Door

- **Remote Opening/Closing:** It can control one door or all doors.

To control a single door, right click over it, and click **[Remote Opening/ Closing]** in the pop-up dialog box. To control all doors, directly click **[Remote Opening/ Closing]** behind Current All.

In the remote opening, the 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 (can be opened at any time).

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]**.

✍**Note:** If **[Remote Opening /Closing]** fails, check whether the devices are disconnected or not. If disconnected, check the network.

• **Cancel the alarm:** Once an alarming door pops-up over the interface, the alarm sound will be played. Alarm cancellation can be done for a single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click **[Remote Opening/ Closing]** on the menu. To control all doors, directly click **[Remote Opening/ Closing]** behind Current All.

✍**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.

➢ **Quick Management of Doors**

If you move the cursor over a door's icon; you can perform the above-explained operations in a quick way. In addition, you can query the latest events from the door.
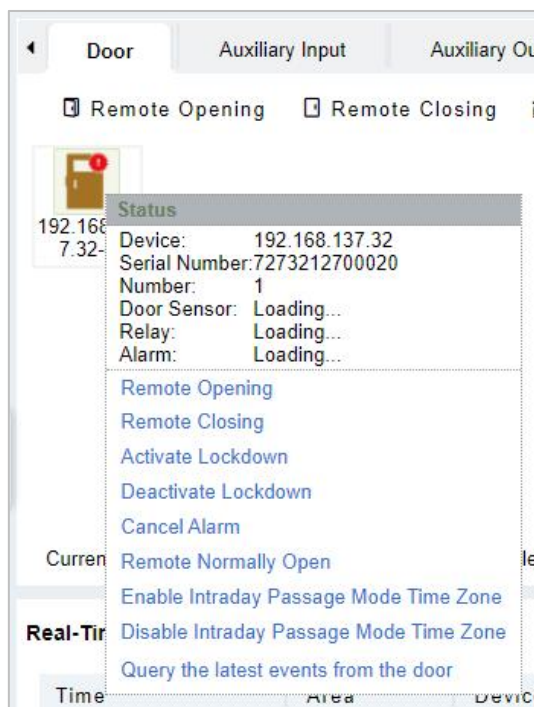

• **Query the latest events from the door:** Click to quickly view the current events on the door.

• **Issue card to person:** If you swap an unregistered card, a record with a card number will pop-up in real-time monitoring interface. Right click that card number, and a menu will pop-out.

Click "Issue card to person", to assign that card to one person.

➢ **Multiple selection**

You can select multiple doors at the same time to perform operations such as remote opening, remote closing, canceling alarm, etc. Double-click the door icon to edit the door properties.
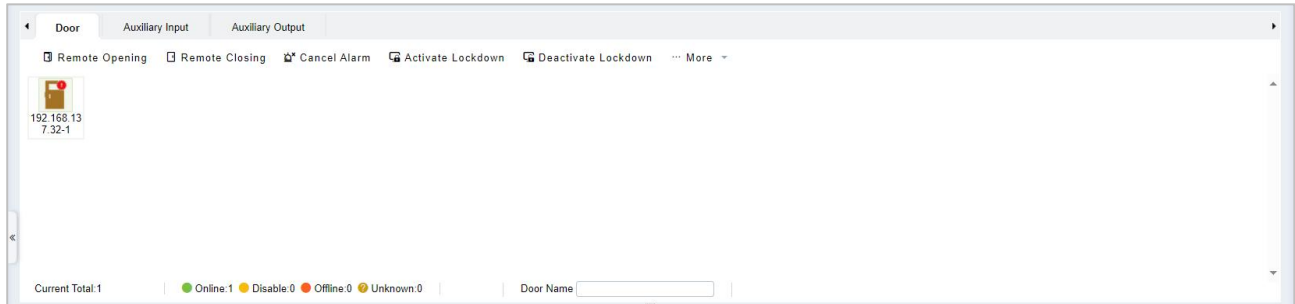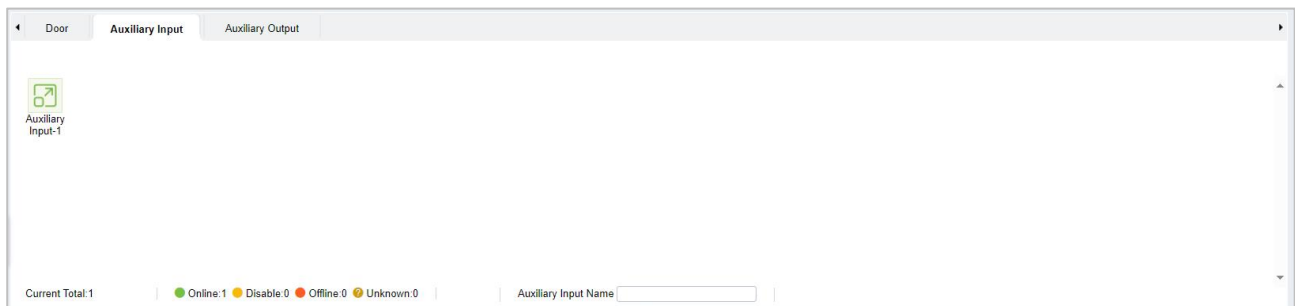

➢ **Event monitoring**

The system will automatically acquire records of devices being monitored (by default, display 200 records), including normal and abnormal access control events (including alarm events). Normal events will appear in green; alarm events will appear in red; other abnormal events will appear in orange.

4.1.10.2 Auxiliary Input

It monitors current auxiliary input events in real-time.

4.1.10.3 Auxiliary Output

Here you can perform Remote open, Remote Close, Remote Normally Open.
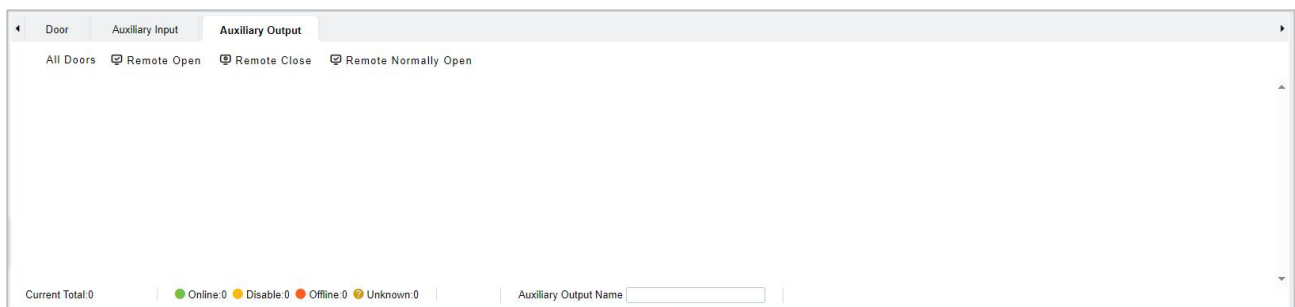
4.1.11 Alarm Monitoring

It monitors the alarm events of the doors. The alarm will be raised in case of abnormalities such as Tamper, Passback, etc. The alarms raised by the doors will be displayed in this page. The Alarm details consist of the Time, Device Name, Event Point, Description of the event, Person responsible for the alarm and the corresponding reader name.
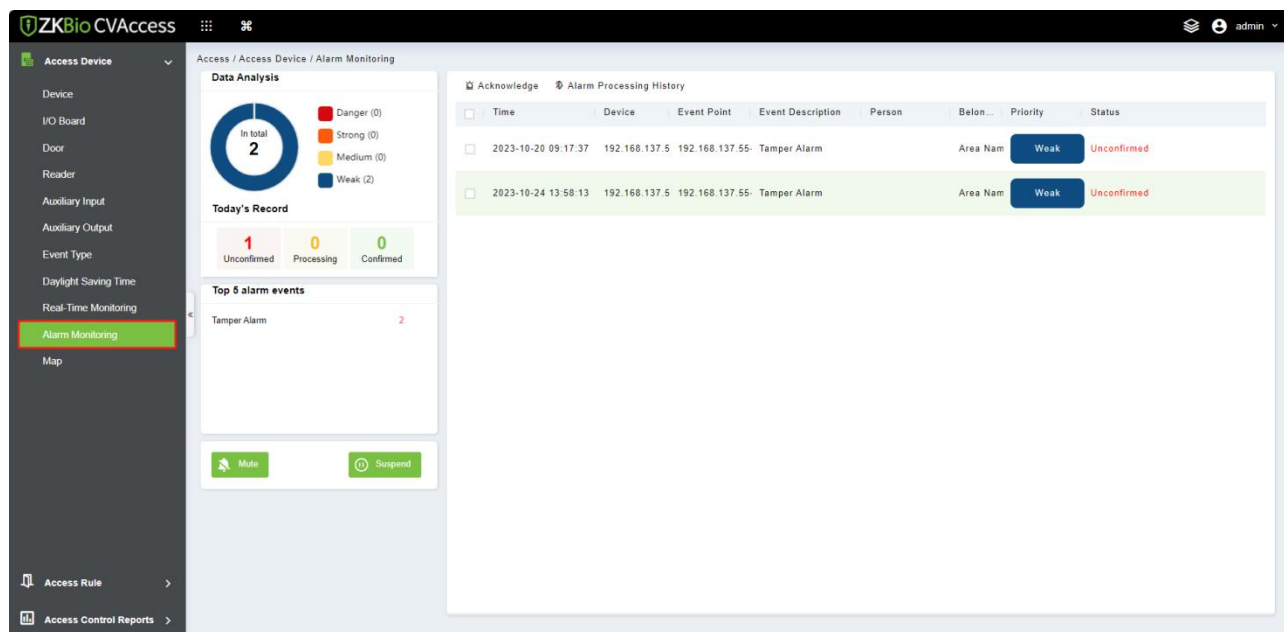
Note: If the firmware version of the device supports, the Event Description will pop-up, or else only "Alarm" will be displayed in Event Description without any details.

Select the Alarm and click **[Acknowledge]** to respond to the Alarm.
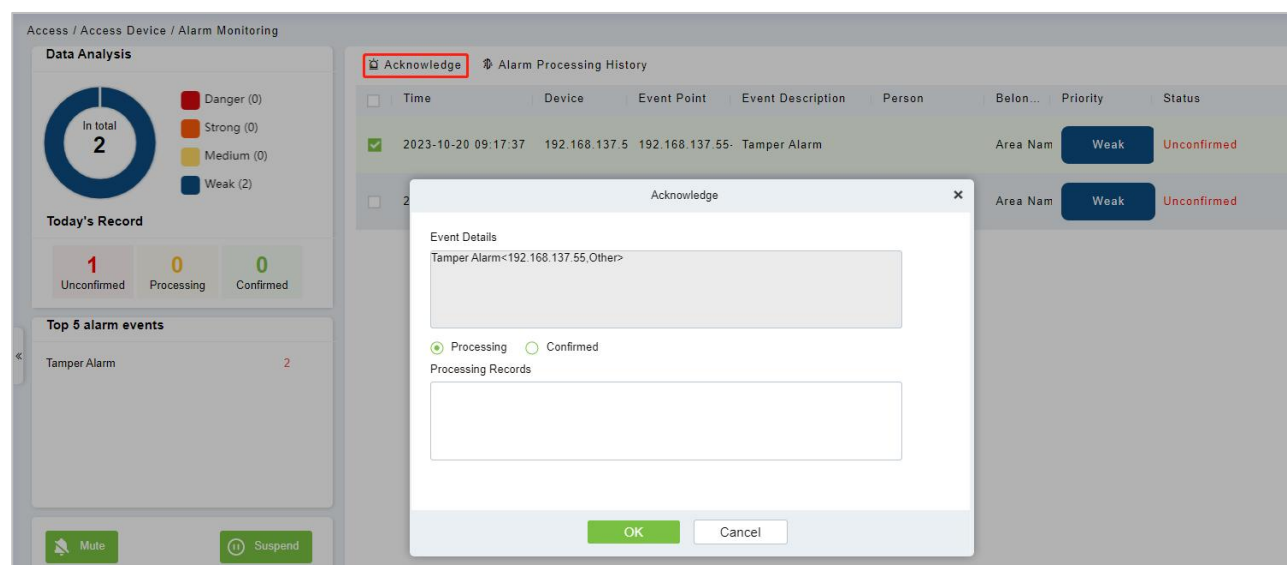
Note: When a door has multiple alarm states, it will display just one alarm type description in the descending severity order, the order are as follows: tamper-resistant alarm > duress alarm (password

+ fingerprint) > duress password or fingerprint alarm > unexpected opening alarm > opening timeout alarm > device disconnects alarm.

4.1.12 Map

Click **[Access Device]** > **[Map]** > **[New]** to add a map.
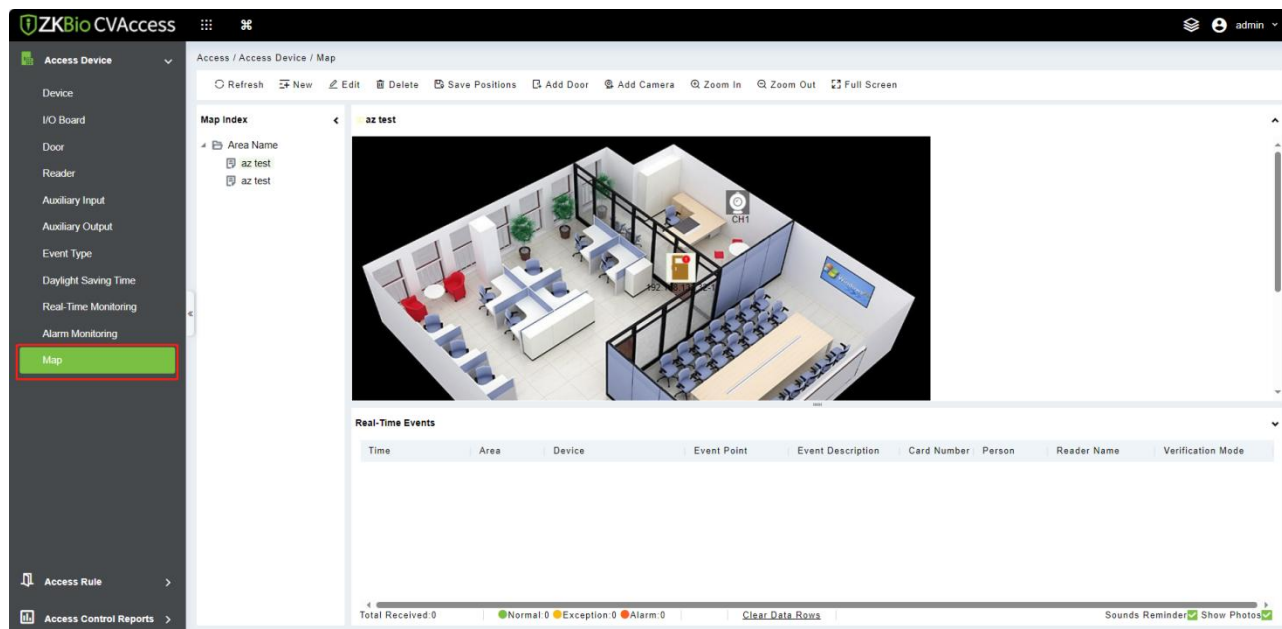
After adding, users can add a door on the map; perform zoom-in, zoom-out, etc. If users relocated some sections or modified the map, click **[Save Positions]** to save. The user can view the new setting after re-opening the Map interface.

- **Add / Delete Map:** Users can add or delete a map as needed.

- **Edit Map:** Users can edit map name, change the map or the area it belongs to.

- **Adjust map (includes door):** Users can add a door on the map or delete an existing one (right click the door icon, and select **[Delete Door]**), or adjust the map or position(s) of the door or camera icons (by dragging the door or camera icons), adjust the size of the map (click **[Zoom in]** or **[Zoom out]** or click **[Full Screen]**).

- **Door operation:** If you move the cursor over a door icon, the system will automatically filter and displays the operation according to the door status. Users can do remotely open/close doors, cancel alarms, etc.

- **Levels 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.

✎**Notes:**

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 the door icon, especially when users zoomed out the map, the margin for top and left shall not be smaller than 5 pixels, or the 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 the screen and the settings of browsers.

4.2 Access Rule Management

4.2.1 Time Zones

It sets usage time of a door; the reader can only be used only during a valid time period of certain doors. 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 period cannot be modified and deleted. The user can add new Time Zones as required.
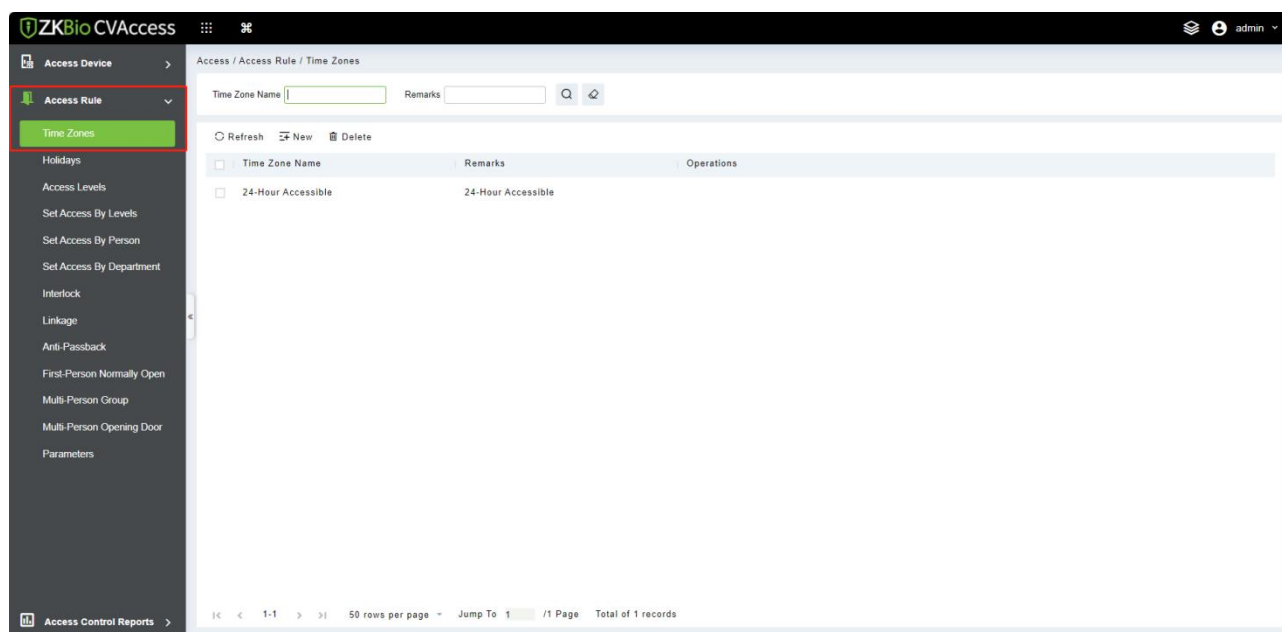
➢ **Add Access Control Time Zone**

1. Click **[Access Rule] > [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.

✎**Note:** Detailed description of the current time zone, including an 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 times 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 purposes. The holiday type is optional. If the user does not enter one, the system will use the default value.

- **Copy on Monday's setting on others weekdays:** Select the check box to copy the settings of Monday to other weekdays.

2. After setting, click **[OK]** to save, and it will display in the list.

➢ **Modify Access Control Time Zones**

- **Edit:** Click the ✎ button in the **Operation** module to enter the edit interface. After editing, click **[OK]** to save.

- **Delete:** Click the 🗑 button in the **Operation** module, 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 select the check boxes one or more time zones in the list and click the **[Delete]** button over the list, then click **[OK]** to delete, or click **[Cancel]** to cancel the operation.

4.2.2 Holidays

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**
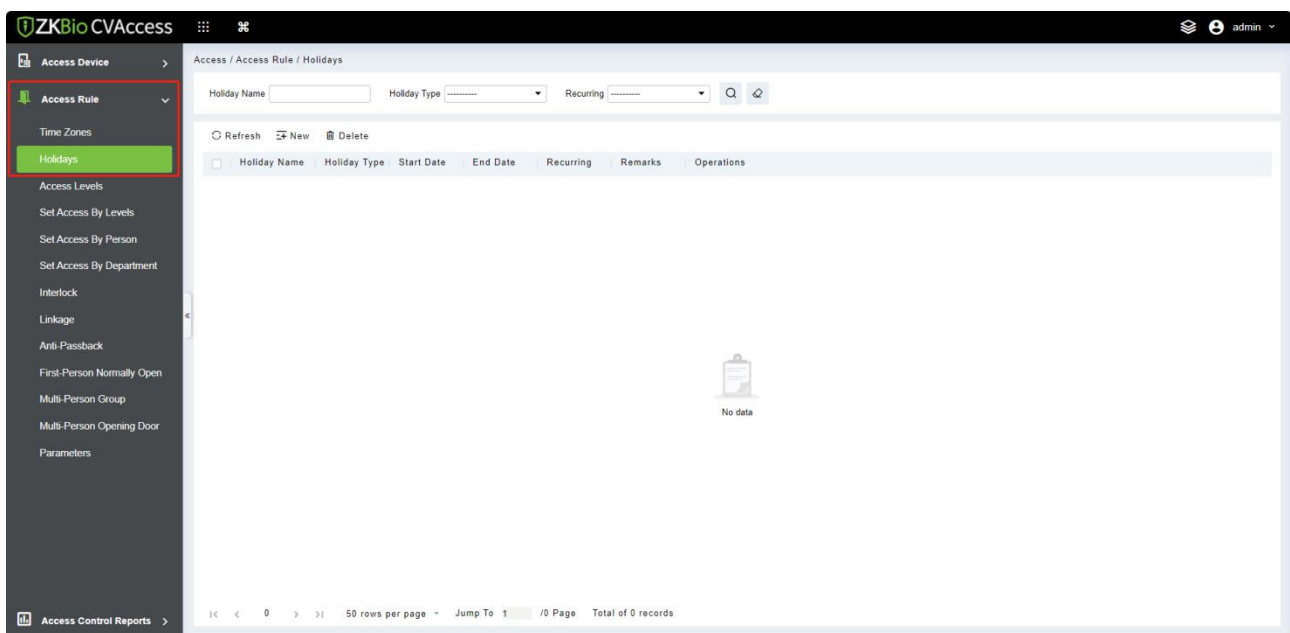
1. Click **[Access Rule] > [Holidays] > [New]** to enter edit interface.

Fields are as follows:

- **Holiday Name:** Any character, up to a combination of 30 characters.

- **Holiday Type:** Holiday Type 1/2/3, as explained in <u>Holiday</u>. 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 is 2019-01-01. 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 is used when the holiday repeats on the same date every year. The default is No. For example, the Near Year's Day is on January 1 each year and can be set as Yes. Some festival date changes every year, so it cannot be set a repeated and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2019, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Tuesday, but the Access Control Time of Holiday Type 1.

2. After editing, click **[OK]** button to save, and it will display on the holiday list.

➢ **Modify**

Click Holiday Name or 🖉 button under Operations to enter the edit interface. After modification, click **[OK]** to save and quit.

➢ **Delete**

In the access control holiday list, click 🗑 button under Operations. Click **[OK]** to delete or click **[Cancel]** to cancel the operation. An Access Control Holiday in use cannot be deleted.

4.2.3 Access Levels

Access levels indicate that one or several selected doors can be opened by verification of a combination of the different persons within a certain time zone. The combination of the different persons set in the Personnel Access Level option.

➢ **Add**
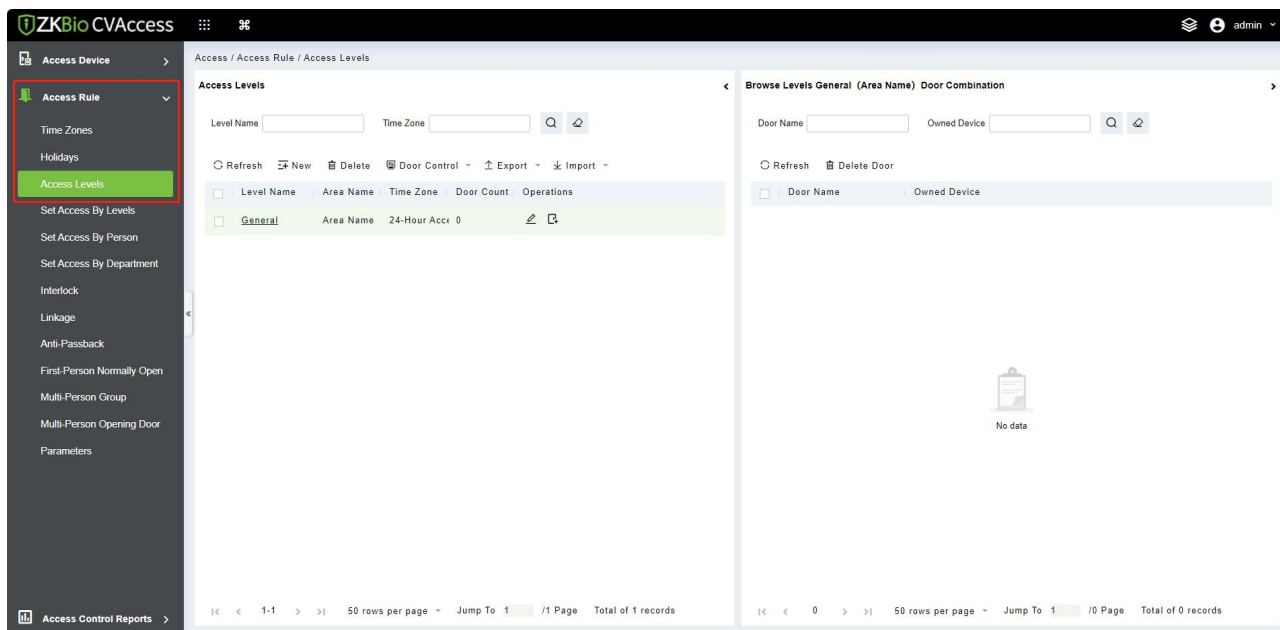
1. Click **[Access Rule]** > **[Access Levels]** > **[New]** to enter the Add Levels editing interface.
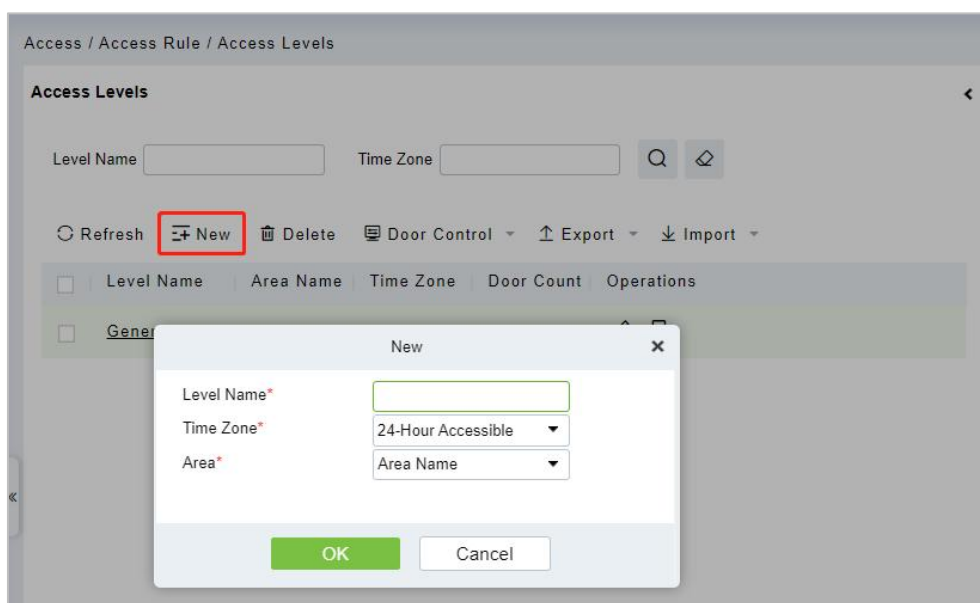
2. Set each parameter: Level Name (must not be the same as other level names), Time Zone.

3. Click **[OK]** and then the system prompts "Immediately add doors to the current Access Control Level", click **[OK]** to add doors, or you can click **[Cancel]** to return the access levels list. The added access level will be displayed in the list.

✎**Note:** Different doors of different panels can be selected and added to an access level.

➢ **Door Control**

Click **[Access Rule]** > **[Access Levels]**, and choose the access level, click door control, the operation will affect all the doors of this access level.
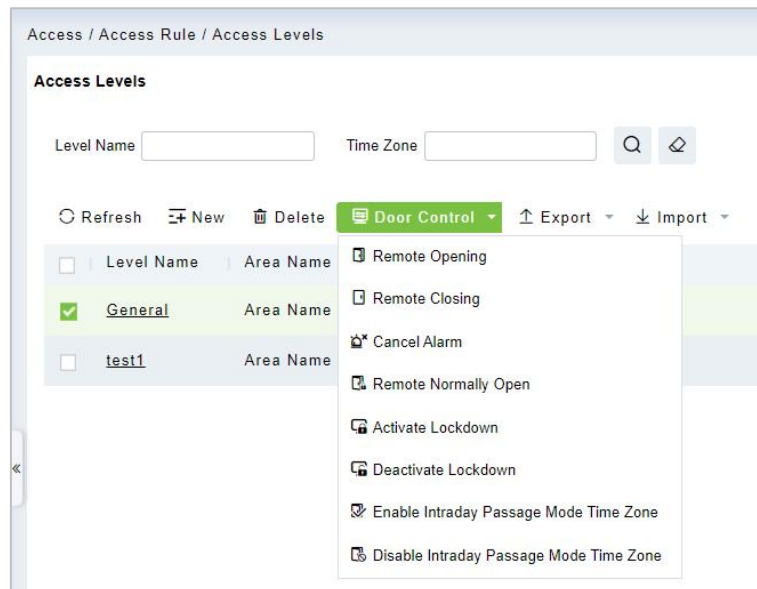
4.2.4 Set Access by Levels

➢ **Add/Delete Person for Levels**

1. Click **[Access Rule]** > **[Access Levels]** > **[Set Access by Levels]** to enter the edit interface, then select an Access level in the list on the left, personnel having the right of opening doors in this access level will be displayed in the list on the right.
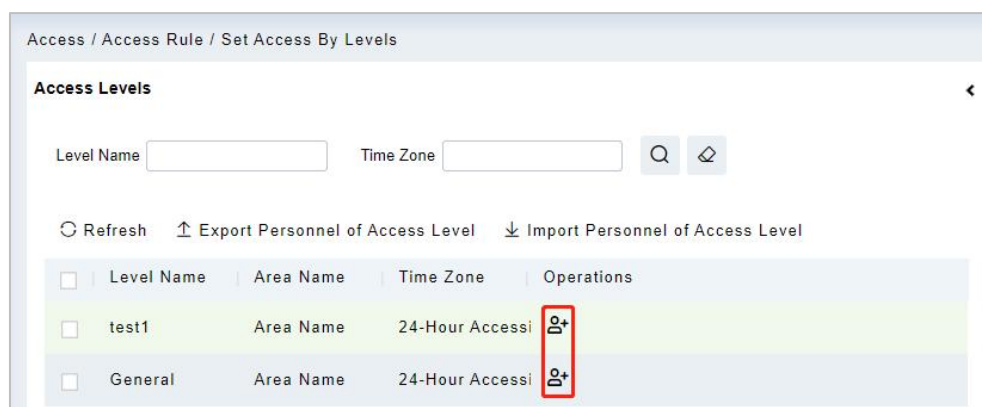
2. In the left list, click 👤⁺ under Operations to pop up the Add Personnel box; select personnel (multiple) and click ＞ to move to the selected list on the right, then click **[OK]** to save and exit.
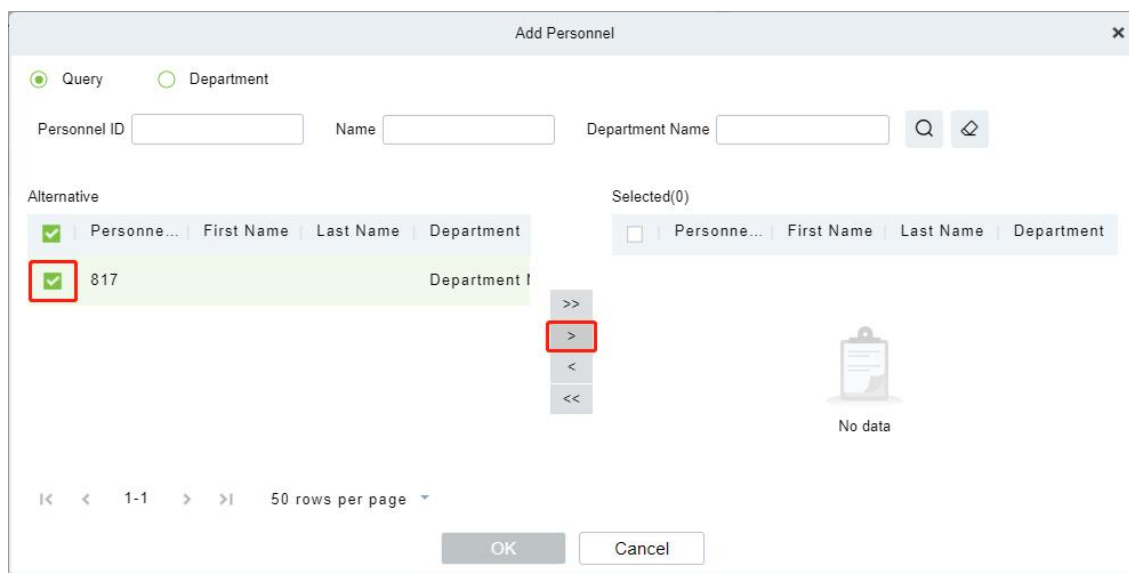
3. Click the level to view the personnel on the list on the right. Select personnel and click **[Delete Personnel]** above the list on the right, then click **[OK]** to delete.

4.2.5 Set Access by Person

Add selected personnel to selected access levels or delete selected personnel from the access levels.
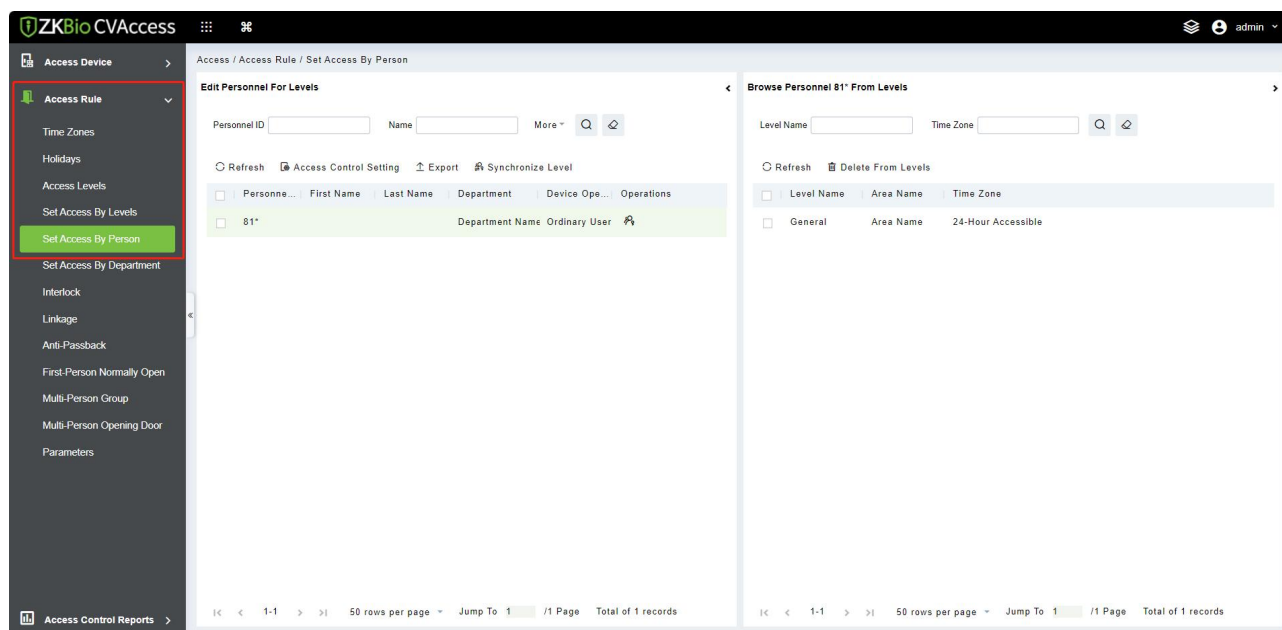
➢ **Add/Delete levels for Selected Personnel**

1. Click **[Access Rule]** > **[Access Levels]** > **[Set Access by Person]**, click Employee to view the levels in the list on the right.

2. Click button in the **Operations** module 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.
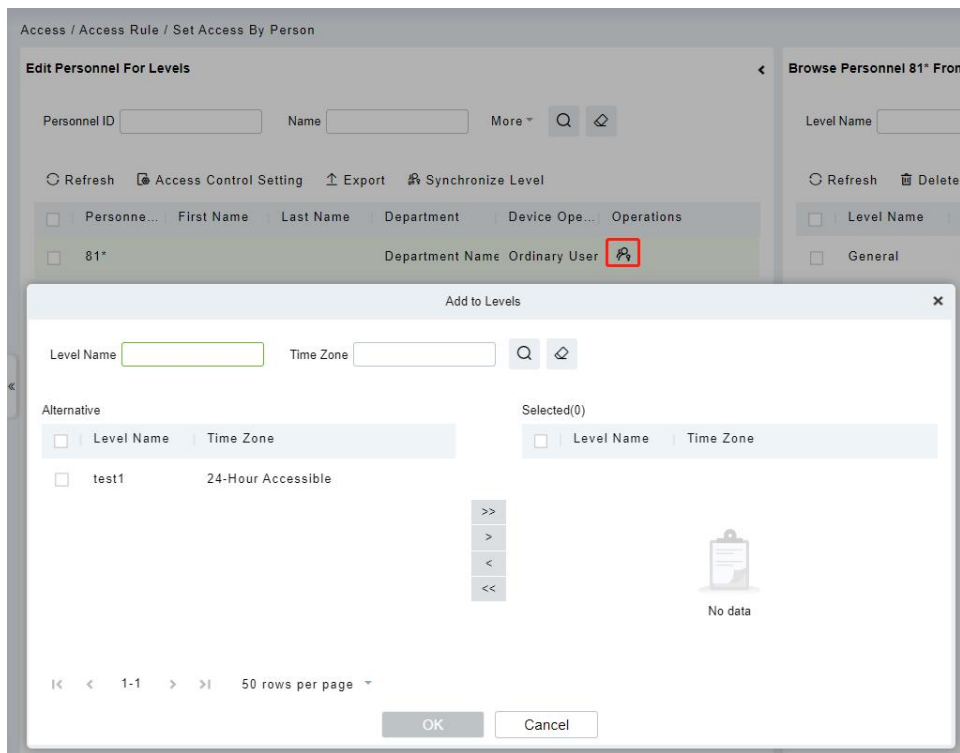
3. Select Level (multiple) in the right list and click **[Delete from levels]** above the list, then click **[OK]** to delete the selected levels.

➢ **Setting Access Control for Selected Personnel**

1. Select a person in the list on the left and click **[Access Control Setting]**.
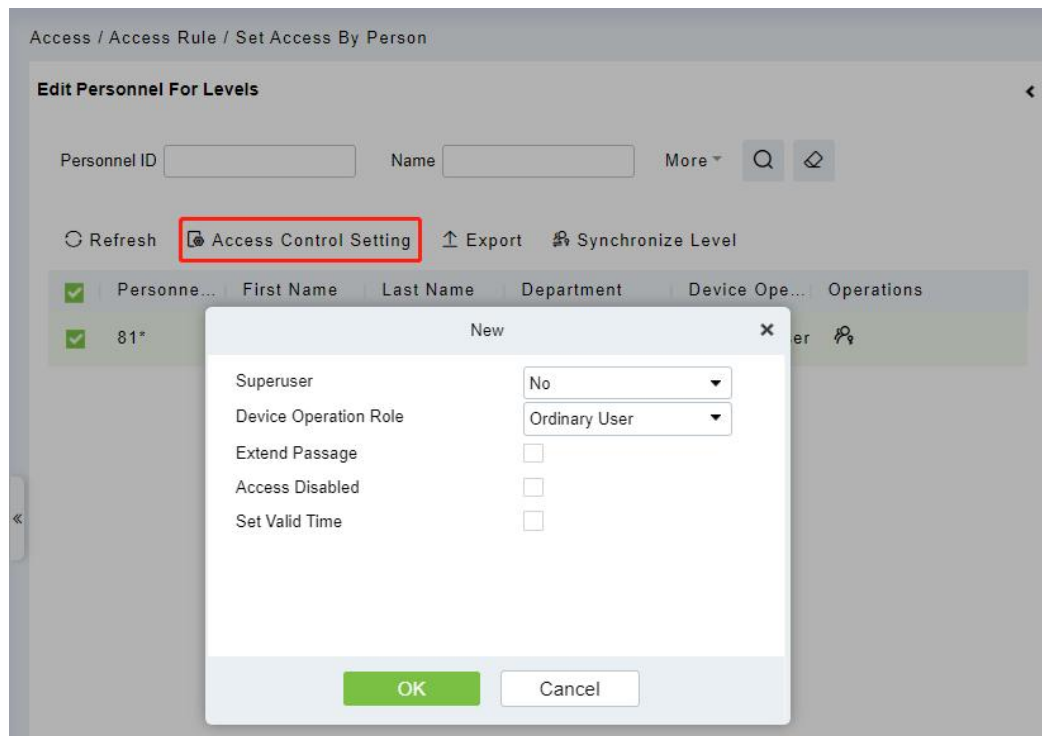
2. If required, set access control parameters and then click **[OK]** to save the settings.

3. Now you need to add levels to the personnel.
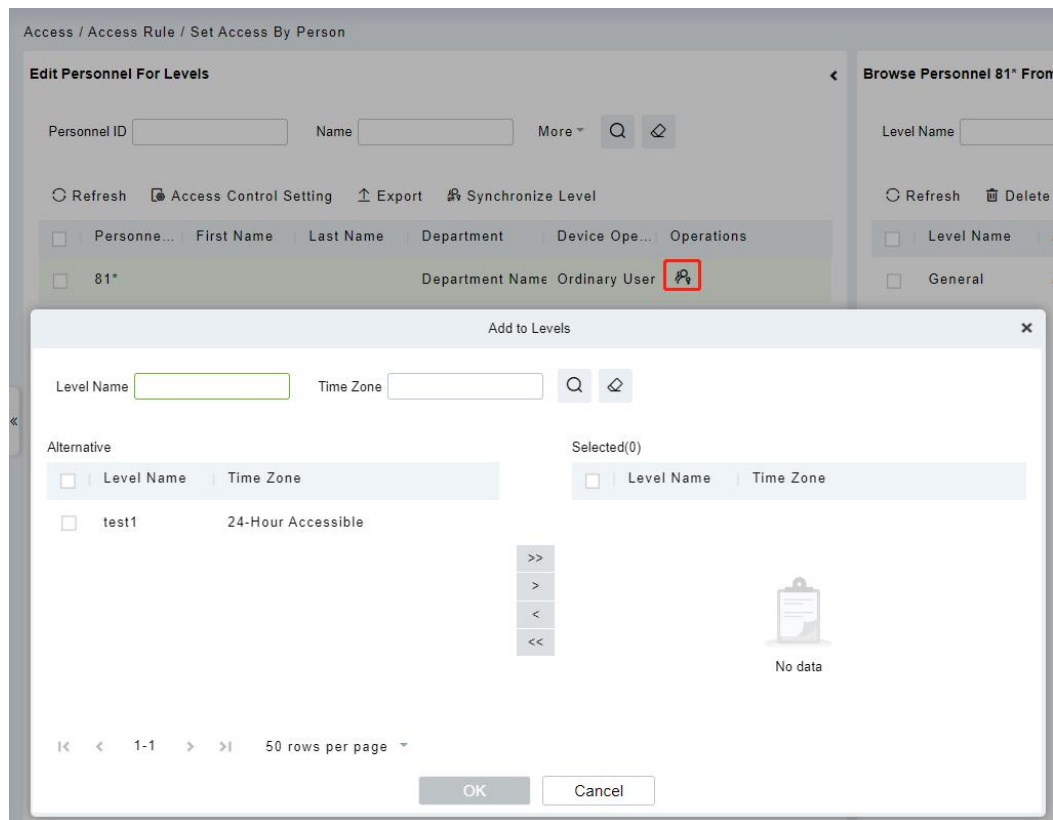
4.   After selecting the required level(s), click **OK** to save and exit.

4.2.6 Set Access by Department

You can add the selected department to the selected access levels or delete the selected department from the access levels. The access to the personnel in the department will be changed.
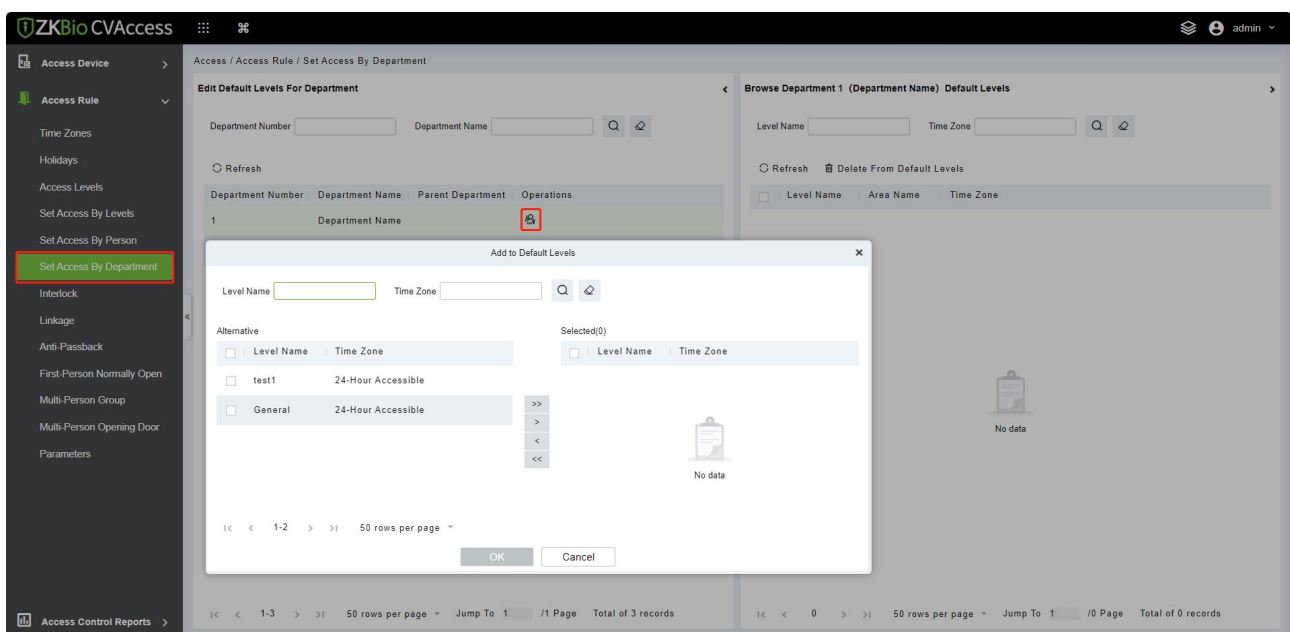
4.2.7 Interlock

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.

Before setting the interlock, please ensure that the access controller is connected with the door sensor, which has been set as NC or NO state.

➢ **Add Interlock**

1. Click **[Access Rule]**> **[Interlock]** > **[New]** to enter the edit interface.
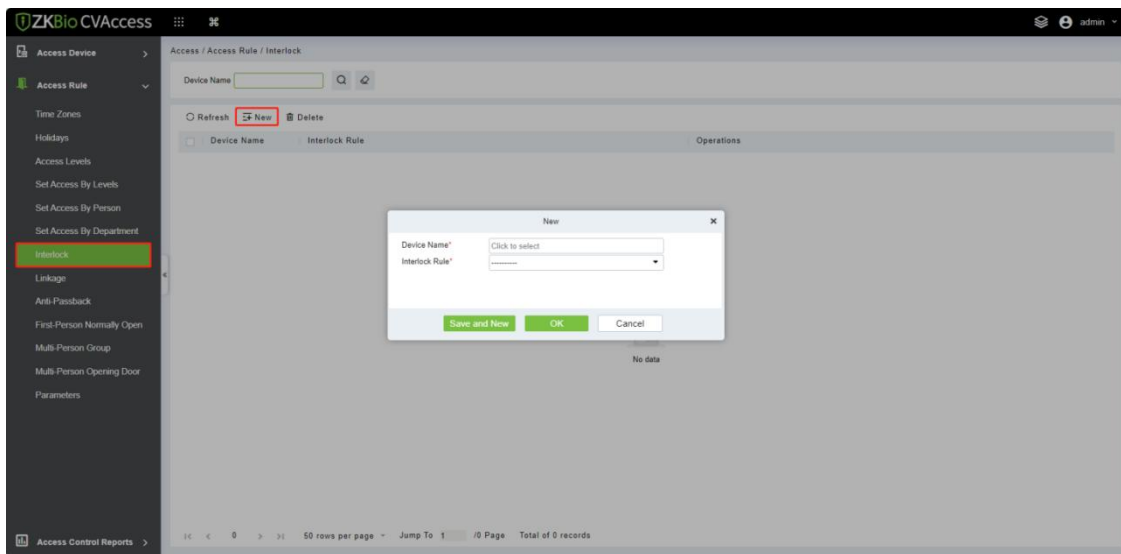
2. Select the required Device. When users are adding devices, interlocked devices cannot be seen in the drop-down list. After deleting established interlock information, the corresponding device will return to the drop-down list. Interlock setting will vary with the number of doors controlled by selected devices:

    •   A one-door control panel has no interlock settings.

    •   A two-door control panel: 1-2 two-door interlock settings.

    •   A four-door control panel: 1-2 two-door interlock; 3-4 two-door interlock; 1-2-3 three-door interlock; 1-2-3-4 four-door interlock.

3. Select Interlock Rule, select an item, and then click **[OK]** to complete. The newly added interlock settings will be shown in the list.

✎**Note:** During editing, the device cannot be modified, but the interlock settings can be modified. If the interlock settings are not required for the device anymore, the interlock setting record can be deleted. If users delete a device record, its interlock setting record, if any, will be deleted.

4.2.8 Linkage

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 setting**

1. Click **[Access Rule] > [Linkage] > [New]**.
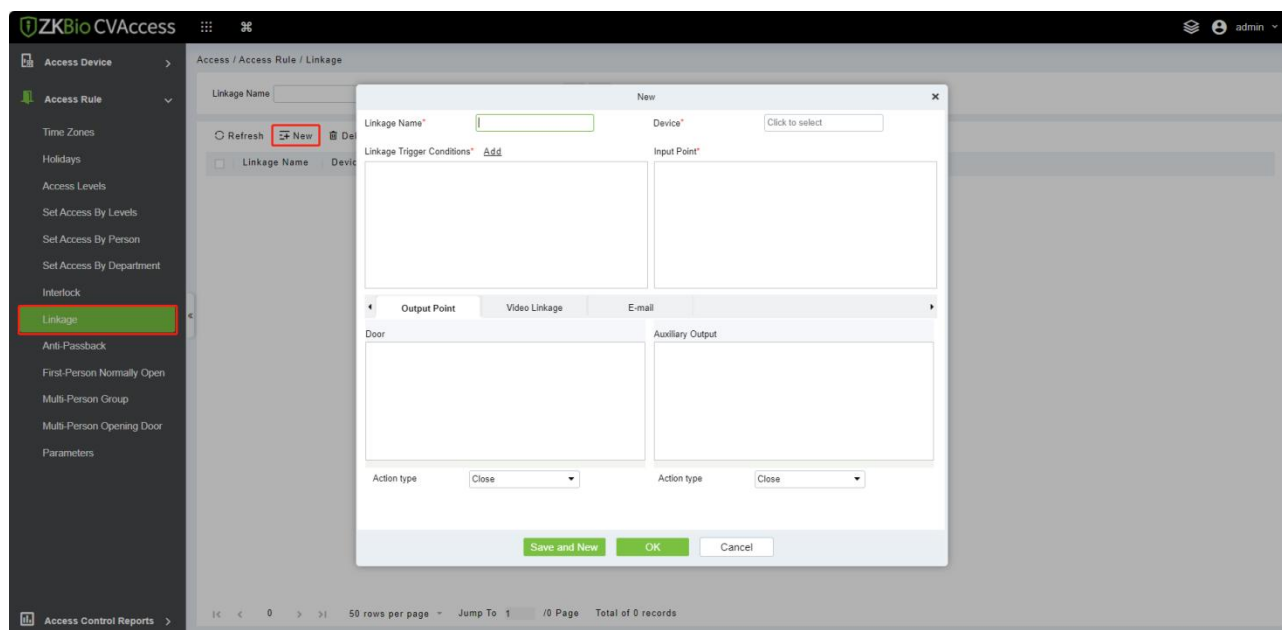
2. Enter the linkage name, select a linkage device, linkage trigger conditions, input point, output point, and then set linkage action, video linkage and other parameters.

3. After selecting devices, corresponding linkage settings will be displayed. The System will first judge whether the device is successfully connected and reads 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:
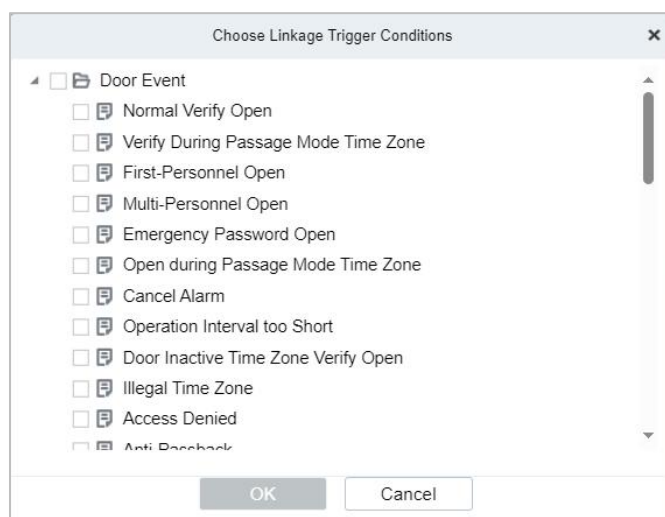
✎ **Note:** Linkage Trigger Conditions contain Door Event and Auxiliary Input Event. And "Fail to connect server", "Recover connection", "and Device connection off" will be filtered from Door Event.

The fields are as follows:

- **Linkage Name:** Set a linkage name.

- **Linkage Trigger Conditions:** It contains trigger conditions for Door and Auxiliary input. These conditions trigger the event type of selected device. All events could be a trigger condition.

- **Input Point:** Select appropriate triggering input point (the specific input point please refers to specific device parameters).

- **Output Point:** Select required output point (the specific output point please refers to specific device parameters).

- **Action Type:** Close, Open, Normal Open. The default is Close. To open, delay time or Normal Open shall be set.

4. Select the Input Point and Output Point, Linkage Action, and Email Address.

5. It's supported to set video linkage, used with VMS Module, for more details please refer VMS module.

The fields are as follows:

- **Pop Up Video:** Select pop-up video on the real-time monitoring screen and set the pop-up duration.

- **Video (new):** Set the time of the video linkage, set the time before event and after the event.

- **Capture:** Set linkage action whether to take a photo, if a photo is taken, you also need to set whether to pop up on the real-time monitoring interface and the display duration.

6. After editing, click **[OK]** to save and quit, then the added linkage setting will be shown on the list.

For example, if users select Normal Punching Open Door as a trigger condition, and the input point is Door 1, the output point is Lock 1, action type is Open, and the delay is 60 seconds. 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 seconds.

✍**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 condition are the same, and the system has a 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 condition are the same, and the system has linkage setting record where the input point is 'Any', it will not permit the user to add (or edit) a linkage setting record where the input point is a specific door or auxiliary input.

In addition, the same linkage setting at the input point and output point are not allowed. The same device permits consecutive logical linkage settings. The system allows setting several trigger conditions for a linkage setting at a time.

4.2.9 Anti-Passback

Currently, Anti-Passback settings support in and out Anti-Passback. On some special occasions, it is required that the cardholders who entered from a door 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 Settings**

1. Click **[Access Rule]** > **[Anti-Passback]** > **[New]** to show the edit interface:
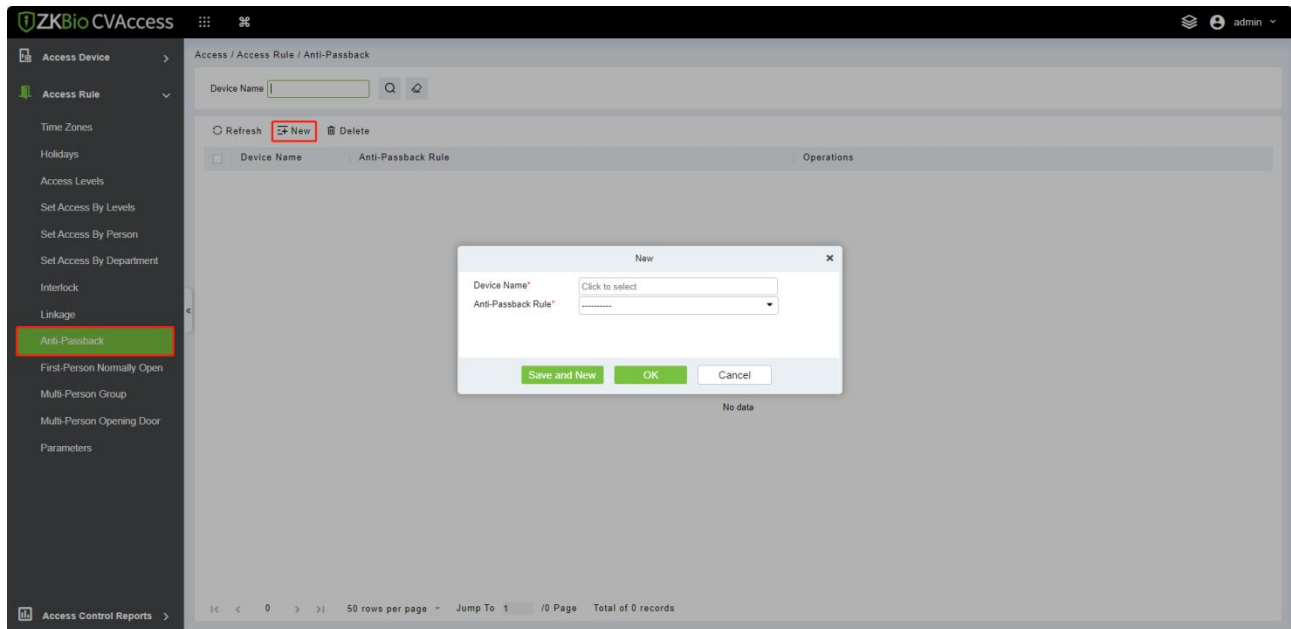
2. Select the required device(s). When adding Anti-Passback Rules, devices with Anti-Passback settings cannot be seen in the drop-down list. When deleting established Anti-Passback information, the corresponding device will appear in the drop-down list again. The settings vary with the number of doors controlled by the device.

    • Anti-Passback settings of a one-door control panel: Anti-Passback between door readers.

    • Anti-Passback settings of a two-door control panel: Anti-Passback between readers of door 1; Anti-Passback between readers of door 2; Anti-Passback between door 1 and door 2.

    • Anti-Passback settings of a four-door control panel: Anti-Passback of door 1 and door 2; Anti-Passback of door 3 and door 4; Anti-Passback of door 1/2 and door ¾; Anti-Passback of door 1 and door 2/3; Anti-Passback of door 1 and door 2/3/4; Anti-Passback between readers of door 1/2/ 3/ 4.

    ✍ **Note:** The door reader mentioned above includes Wiegand reader that is connected with access controller and Indio reader. The single and two door-controller with Wiegand reader includes out and in the 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, an odd number is for in reader, an even number is for our reader.

3. Select Anti-Passback Rule, and select one item, click **[OK]** to complete, and then the added

Anti-Passback settings will be shown in the list.

✍**Note:** When editing, you cannot modify the device, but can modify Anti-Passback settings. If Anti-Passback setting is not required for the device any more, the Anti-Passback setting record can be deleted. When you delete a device, its Anti-Passback setting record, if any, will be deleted.

4.2.10 First-Person Normally Open

This function helps to keep the door open for a specific time interval after the first verification by assigned personnel.

During a specified interval, If the first verification is by a person having First-Person Normally Open level access, then 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 a successful addition, assigned personnel can open the door. You can browse and delete the personnel on the right side of the interface.

Operation steps are as follows:

1. Click **[Access Rule]** > **[First-Person Normally Open]** > **[New]**, select Door Name and Passage Mode Time, and click **[OK]** to save the settings.
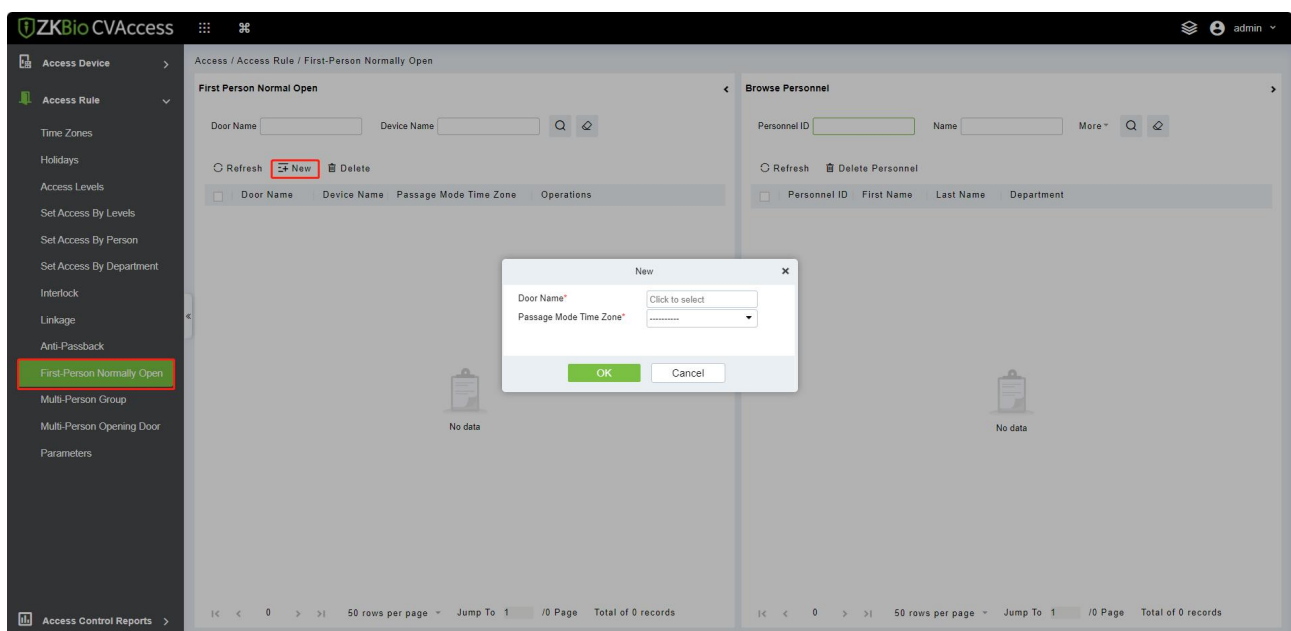
2. Click 😄 button in the Operation module to add personnel having First-Person Normally Open

level (this person must have access control level), then click **[OK]** to save.
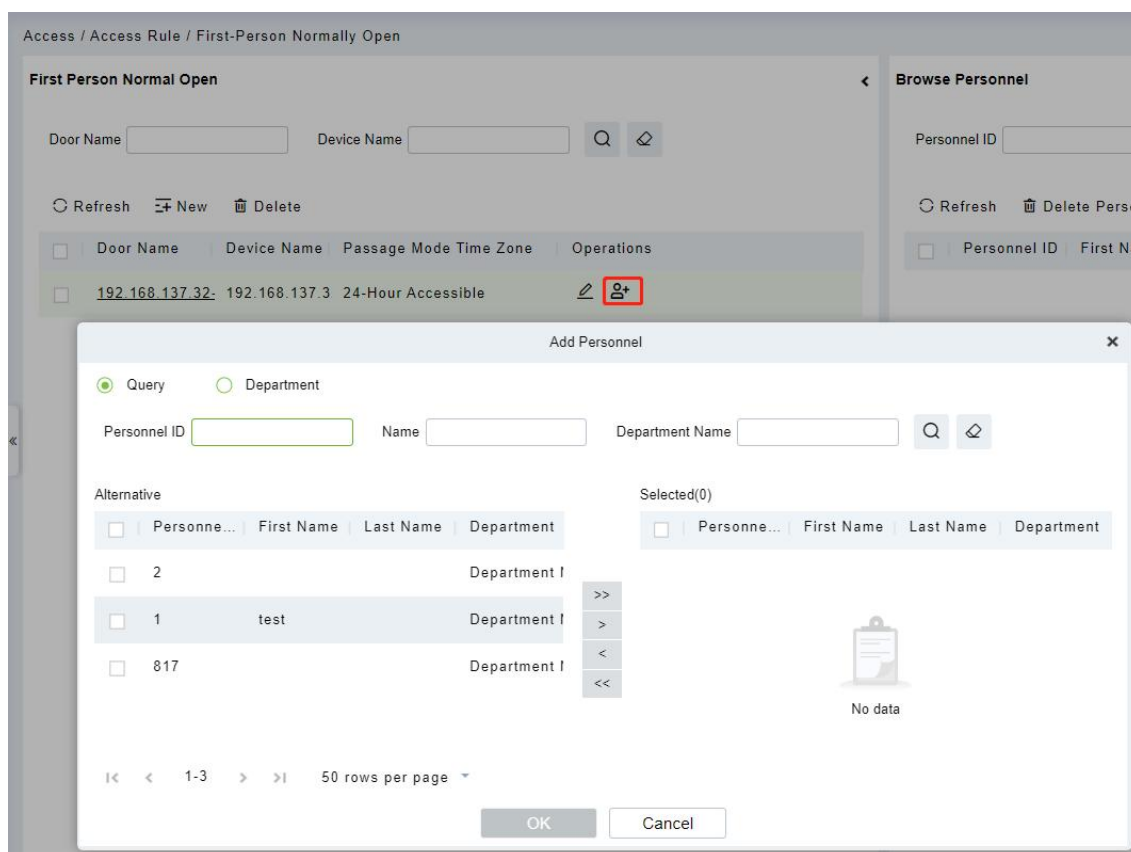
4.2.11 Multi-Person Group

The door will open only after the consecutive verification of multiple people. Any person verifying outside of this combination (even if the person belongs to any other valid combination) will interrupt the procedure and you need to wait for 10 seconds to restart verification. The door cannot be opened by verifying using just one of the combinations.

1. Click **[Access Rule]** > **[Multi-Person Group]** > **[New]** to access the following edit interface:
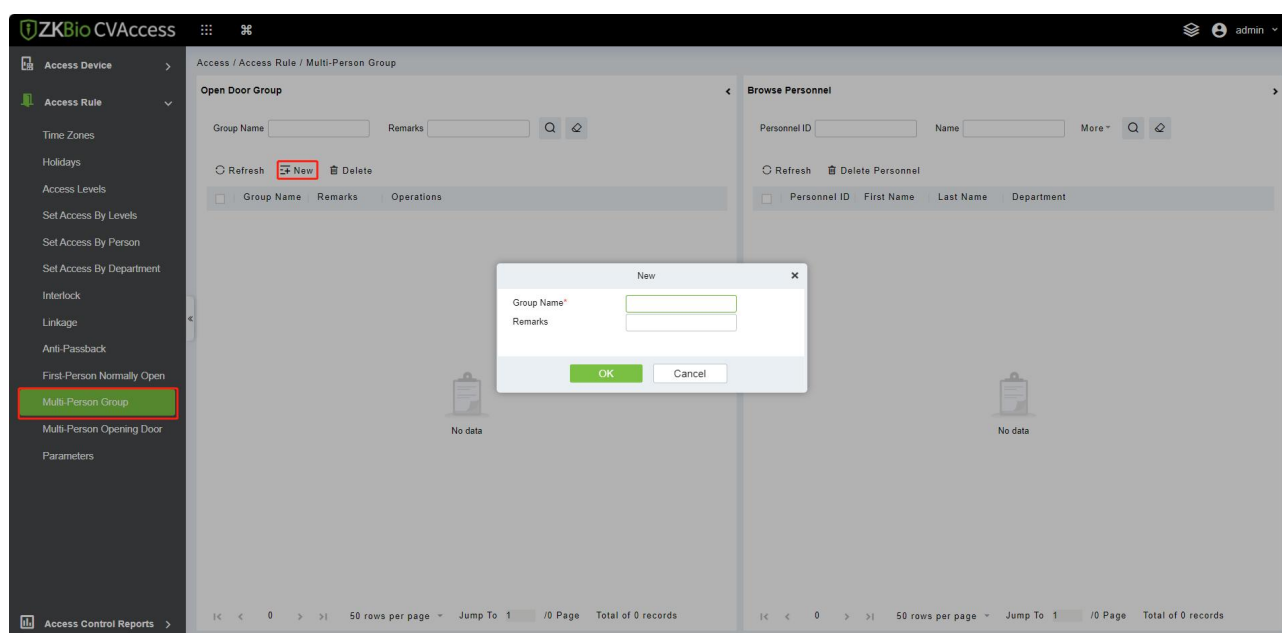
- **Group name:** Any combination of up to 30 characters that cannot be identical to an existing group name.

  After editing, click **[OK]** to save and return. The added Multi-Person Personnel Group will appear in the list.

2. Click 🙎⁺ button in the Operation module to add personnel to the group.

3. After selecting and adding personnel, click **[OK]** to save and return.

✐**Note:** A person can only be a part of only one group.

4.2.12 Multi-Person Opening Door

Set levels for personnel in Multi-Person Personnel Group.

It is a combination of the personnel in one or more Multi-Person Personnel Groups. 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 door 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.

➢ **Multi-Person Opening Door Settings**

1. Click **[Access Rule] > [Multi-Person Opening Door] > [New]**:
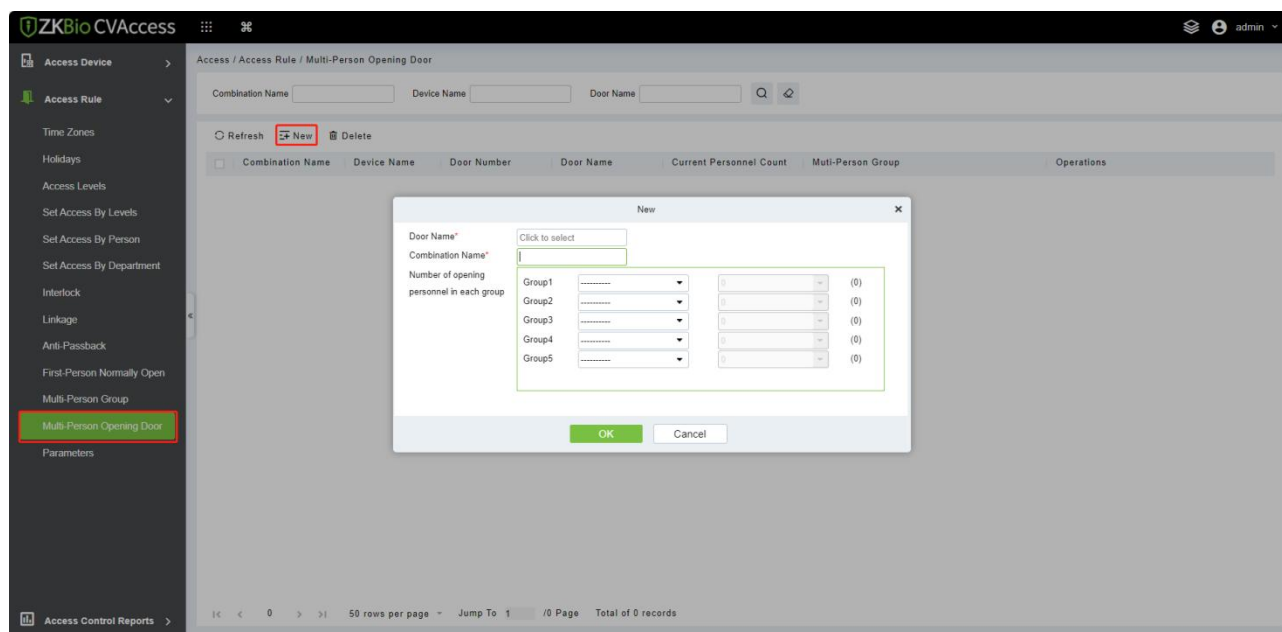
2. The maximum number of Multi-Person Opening Door people for combined door opening is 5. The numbers in the brackets show the current actual number of people in a group. Select the number of people for combined door opening in a group and click **[OK]** to complete.

✍ **Note:** The default 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 it.

4.2.13 Parameters

Click **[Access Rule]** > **[Parameters]** to enter the parameter setting interface:
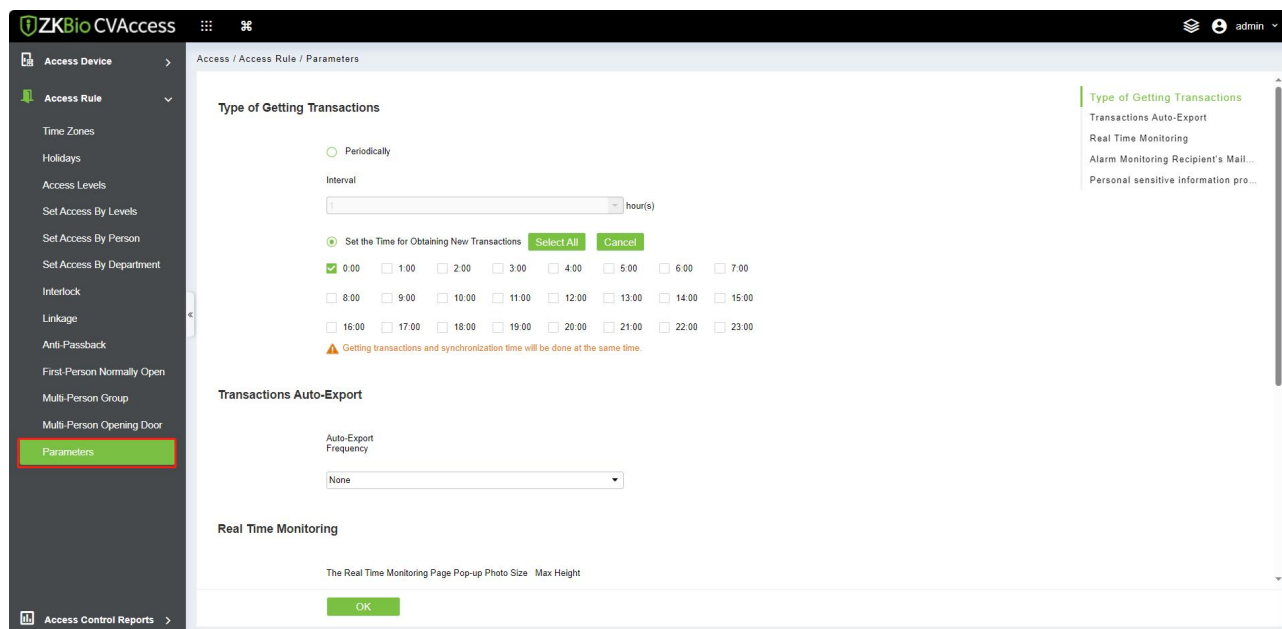
➢ **Type of Getting Transactions**

Periodically

The system will download new transactions at the selected time interval.

Set the Time for Obtaining New Transactions

The system will download new transactions automatically at the selected time instances.

➢ **Transactions Auto-Export**

Auto-Export Frequency

It supports to set the Auto-Export Frequency by Day or Month. When the Auto-Export frequency is set by day, you have to set the Hour and minute.
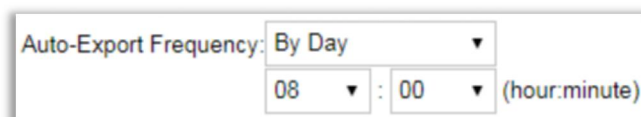
When the Auto-Export frequency is set to month, you have to select whether to export on the first day of the month or on a particular date.

Export Mode

It supports to export the Monthly Transactions or All Data. At a time, the device can export 30000 data.

Recipient's Mailbox

Set the Recipient's Mailbox.

➢ **The Real Time Monitoring**

You can select the checkbox accordingly.

If the display photo is selected, the real-time monitoring page will display the personnel photo during an access control event. You can set the quality of the image as required; the more px value will give a clearer photo.

Alarm Monitoring Recipient Mailbox: The system will send emails to alarm monitoring recipient's mailbox if there is any event.

4.3 Access Reports

Includes "All transactions", "Events from Today", "All Exception Events" and so on. You can export after the query.

You can generate statistics of relevant device data from reports, including card verification information, door operation information, and normal punching information, etc.

About the Normal and abnormal event please refer to Real-Time Monitoring for details.

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 an emergency password to open doors

will include only password verification mode.

4.3.1 All Transactions

Because the data quantity of access control event records is more, you can view access control events as a specified condition when querying. By default, the system displays the latest three months' transactions. Click **[Reports]** > **[All Transactions]** to view all transactions:

- • **Media File:** You can view or download the photos and videos.

- • **Clear All Data:** Click **[Clear All Data]** to pop up prompt and click **[OK]** to clear all transactions.

- • **Export:** You can export all transactions in Excel, PDF, and CSV format.

4.3.2 Events from Today

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, and CSV format.

4.3.3 All Exception Events

Click **[Reports]** > **[All Exception Events]** to view exception events in specified condition. The options are the same as those of **[All Transactions]**.
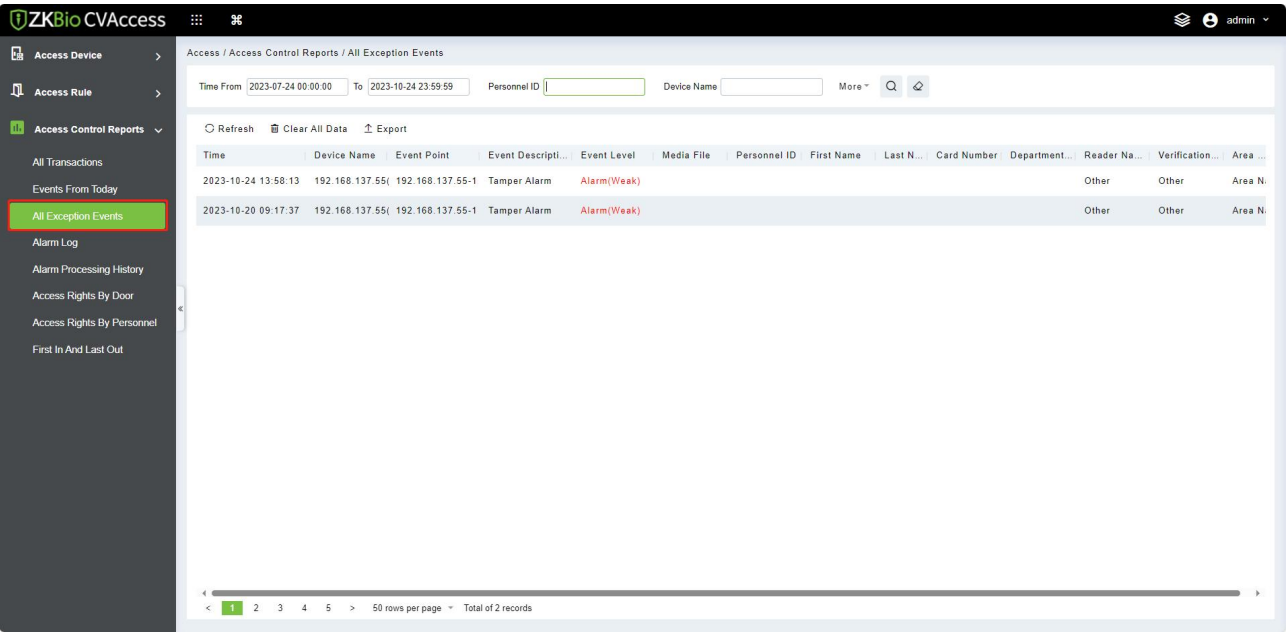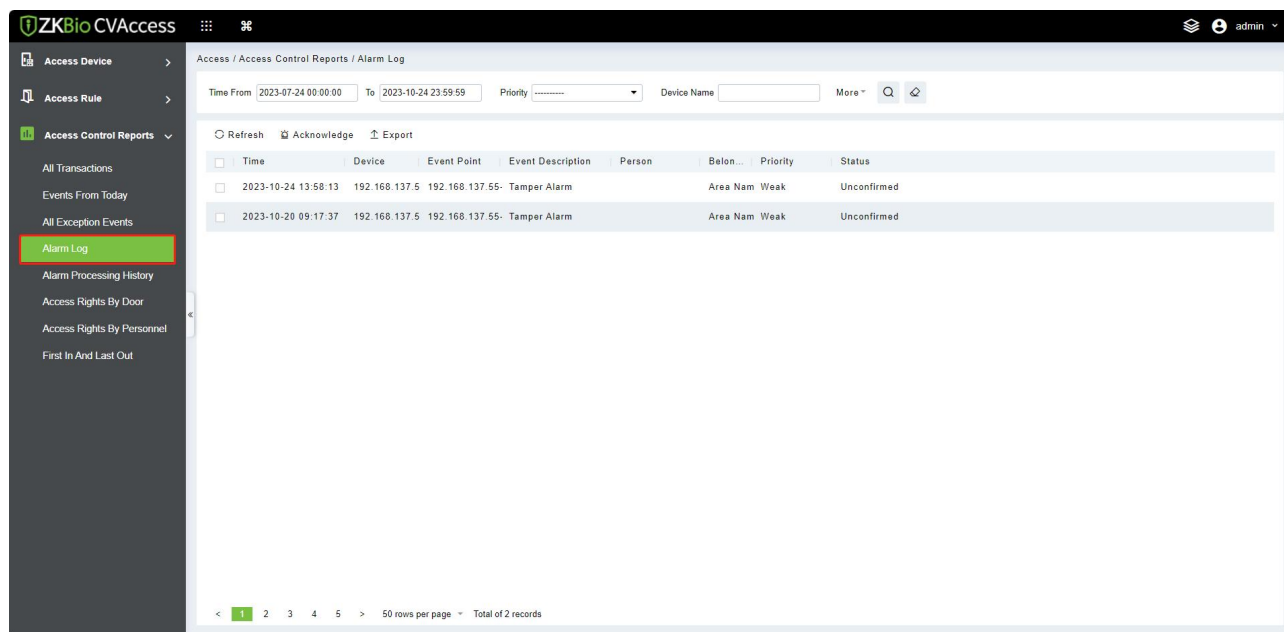
- **Clear All Data:** Click **[Clear All Data]** to pop up prompt, and then click **[OK]** to clear all exception events.

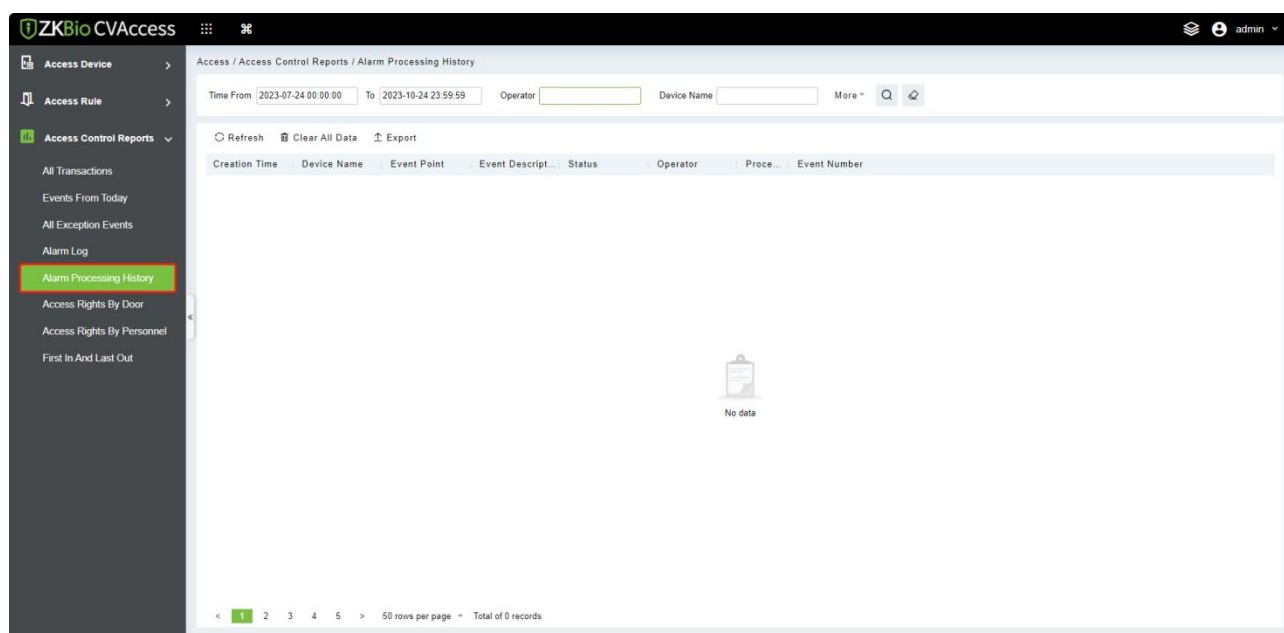- **Export:** You can export all exception events in Excel, PDF, and CSV format.

4.3.4 Alarm Log

Click **[Reports]** > **[Alarm Log]** to view historical statement in **Alarm Monitoring**.

4.3.5 Alarm Processing History

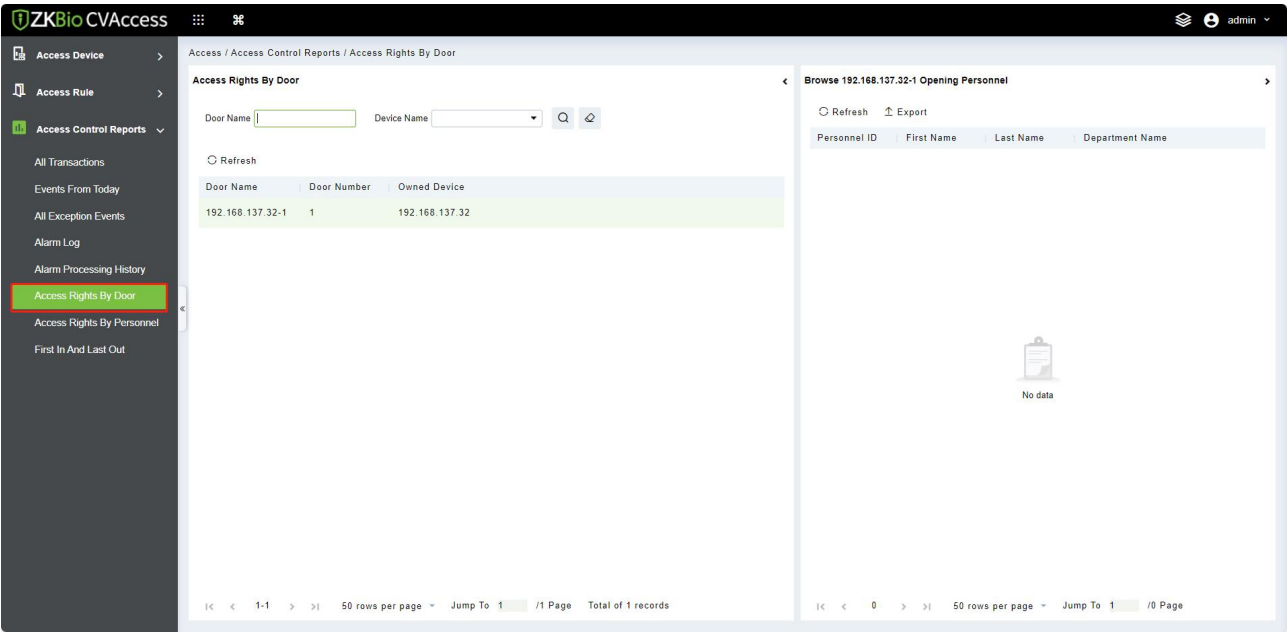Click **[Reports]** > **[Alarm Processing History]** to view reports of processing records in **Alarm Monitoring**.

4.3.6 Access Rights by Door

View related access levels by the door. Click **[Reports]** > **[Access Rights by Door]**, the data list on 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.

You can export all the personnel having access levels to the door data in Excel, PDF, and CSV format.

4.3.7 Access Rights by Personnel

View related access levels by personnel.

Click **[Reports]** > **[Access Rights by Personnel]**, the data list on 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.
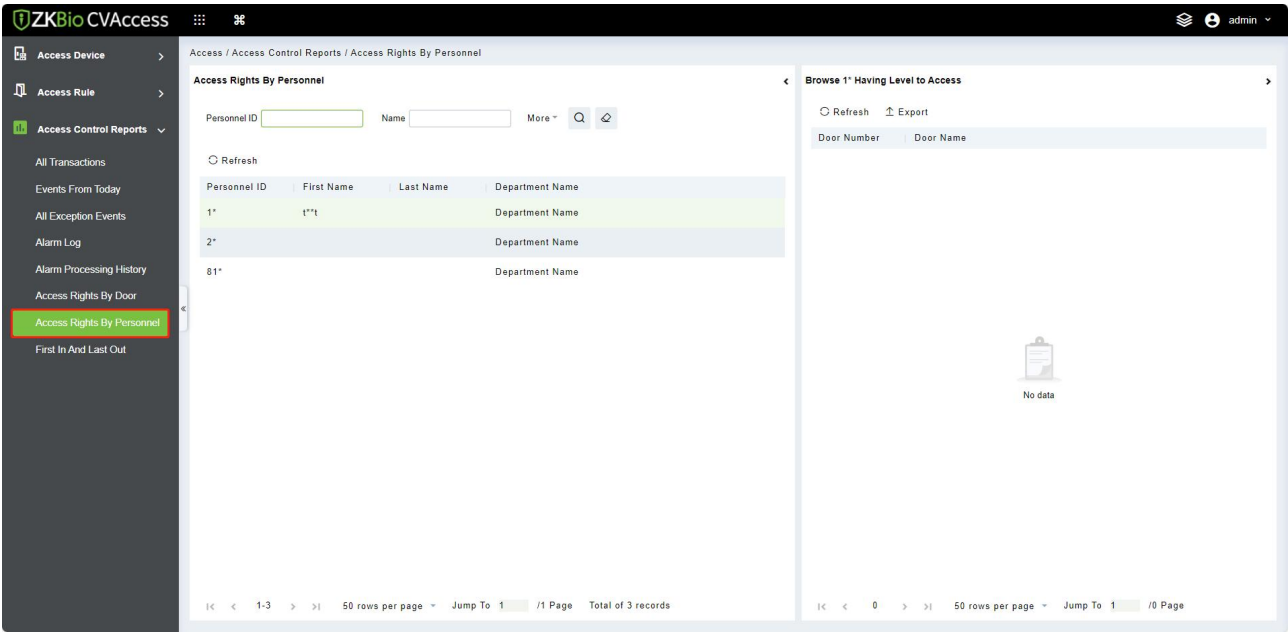
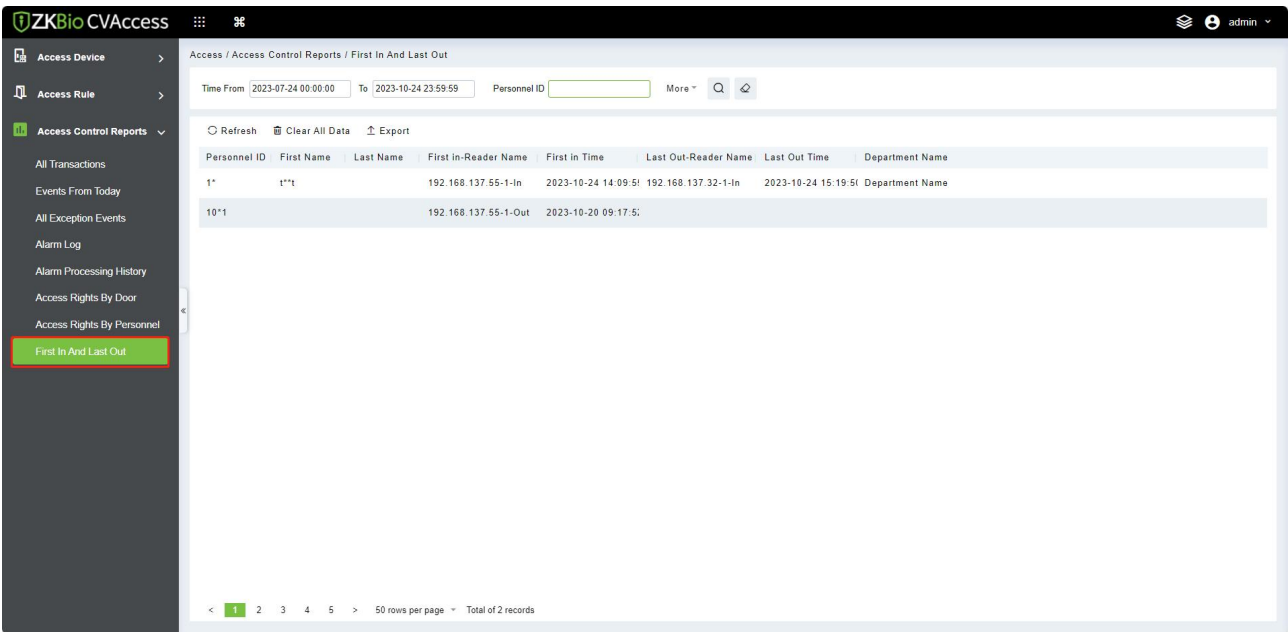You can export all the door information in Excel, PDF, and CSV format.

4.3.8 First in and Last out

Click **[Reports]** > **[First in and Last out]** to view report of first entry and last exit, used to quickly screen out the first entry and last exit of the day.

5   Time & Attendance Management

To help companies perform information-based attendance management, this software implements automatic collection, statistics, and query of employee attendance data. This improves the management of human resources and facilitates the check-in of employees. This software enables the management personnel to collect statistics and check the employee attendance and enables the management department to query and appraise the attendance of all departments, thus allowing enterprises to accurately acquire the employee attendance data.
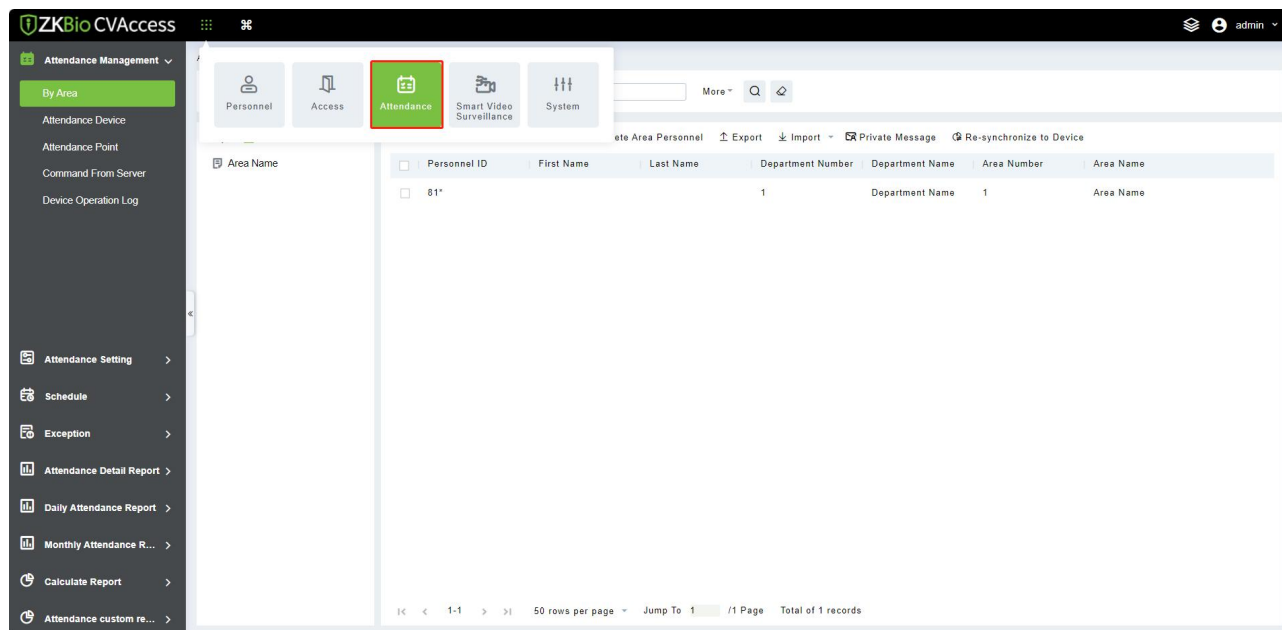
5.1 Attendance Management

This function includes adding a device, adding area and assigning it to the personnel. Set the communication parameters of the device. The system can communicate with the device properly only when communication parameters are configured correctly, including the parameter settings in the system and the device. After successful communication, you can view the information on the connected device and can perform remote monitoring of the device/upload and download.

5.1.1   Set Attendance by Area

Area is a concept of space that facilitates the management of devices in a specific area.

In this system, area setting is a process of dividing devices by zone. A prominent feature of "Area" is to allow the system to automatically manage the employee information on devices. According to requirements, areas can be allocated to devices (one device can belong to one area only), and employees can be allocated to one or more areas.

5.1.1.1 Add/Delete Personnel for A Specified Area

1. Click **[Attendance Management]**> **[By Area]**, click a certain area of left side, the system will display the personnel on the right side.
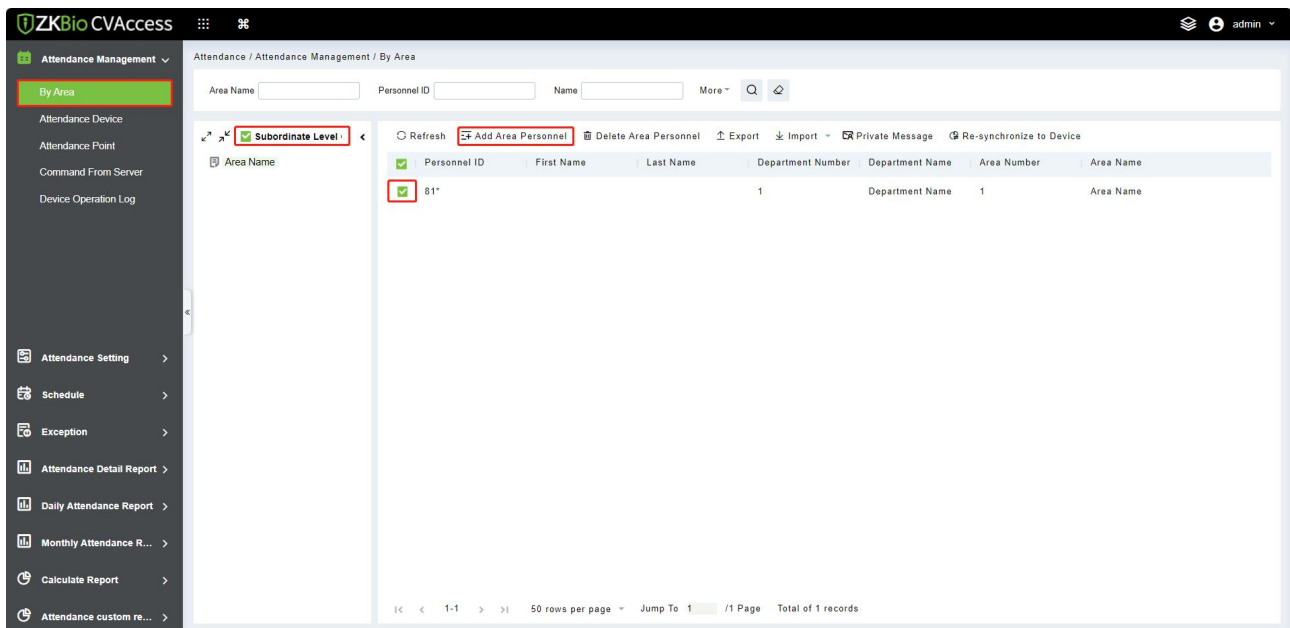
2. Click **[Add Area Personnel]** under the list on the left to pop up the Add Person page. Select the person to the right list and click **[OK]** to complete it.
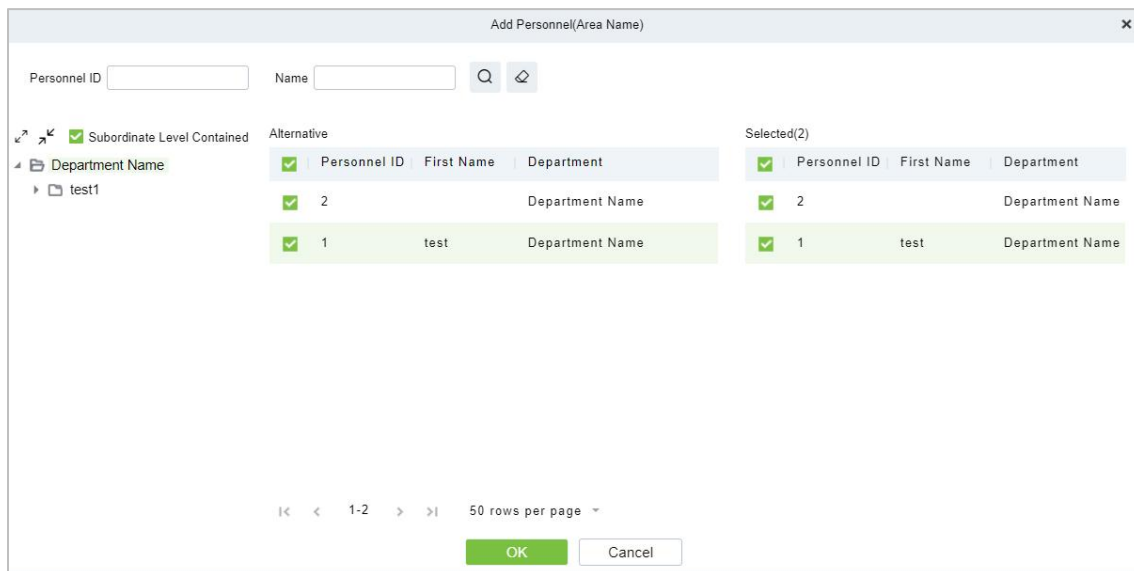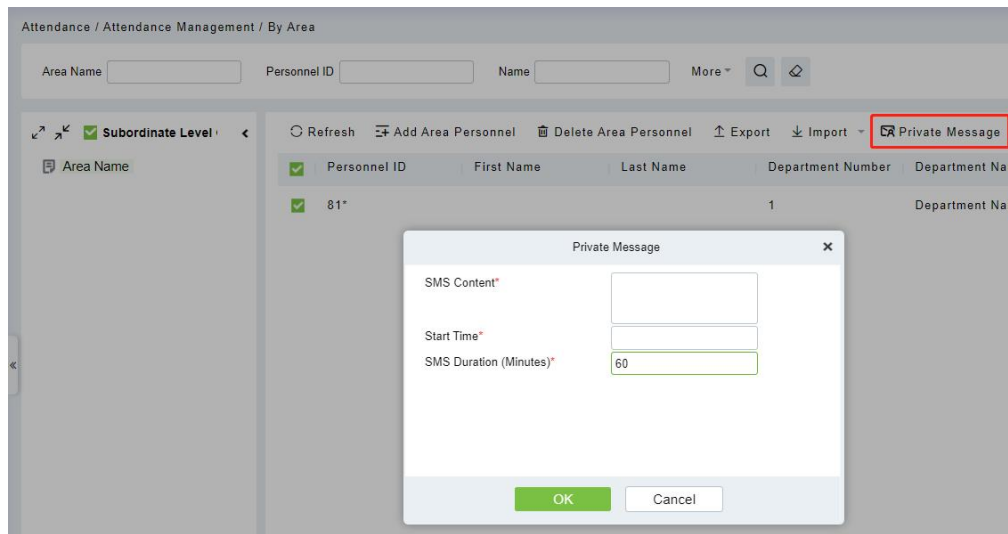

3. To delete a person in the area, select the person on the right side and click **[Delete Area Personnel]** to delete the person from the area.

5.1.1.2 Private Message

This feature can display a short message to someone regularly (device should support).

Select personnel and click **[Private Message]**. The setting interface as follows:

After the setting is completed, click **[OK]**. After swipe cards successfully on the device, the device will send short message to this person. For example, the message like "Happy Birthday to you", to strengthen the interaction between the company and employees.

**The fields are described below:**

Short Message: The message displayed on the time and attendance device, which supports input 40 characters.

Start Time: The start time to display private short messages.

Short Message Duration (minutes): Shows the duration of the private short message after a successful check-in.

5.1.1.3 Re-synchronize Data to the Device

Synchronize personnel data from the system to the device. Select a device of a certain area, click **[Re-synchronize to Device]**, and click the **[OK]** button to synchronize the data, so that personnel can verify on the time attendance device in the area:
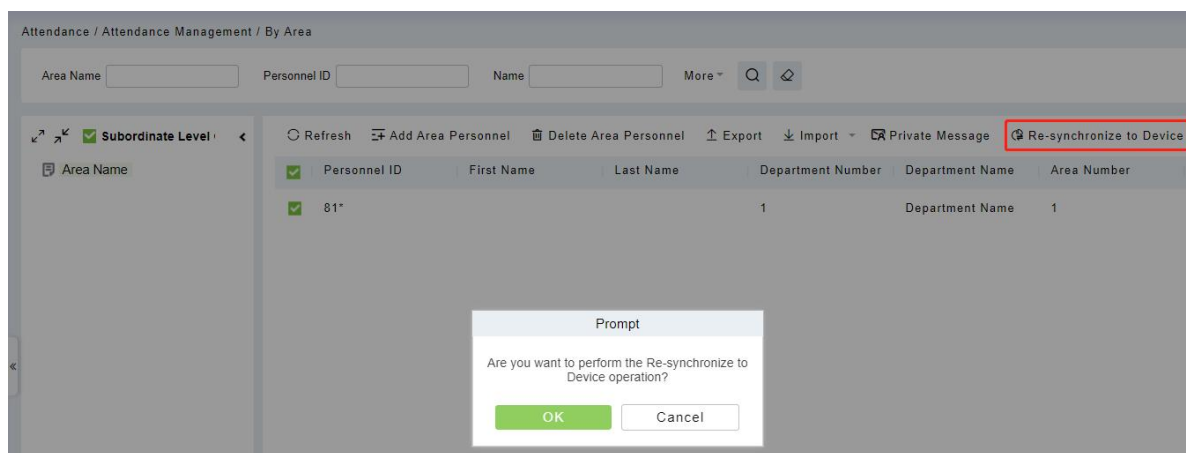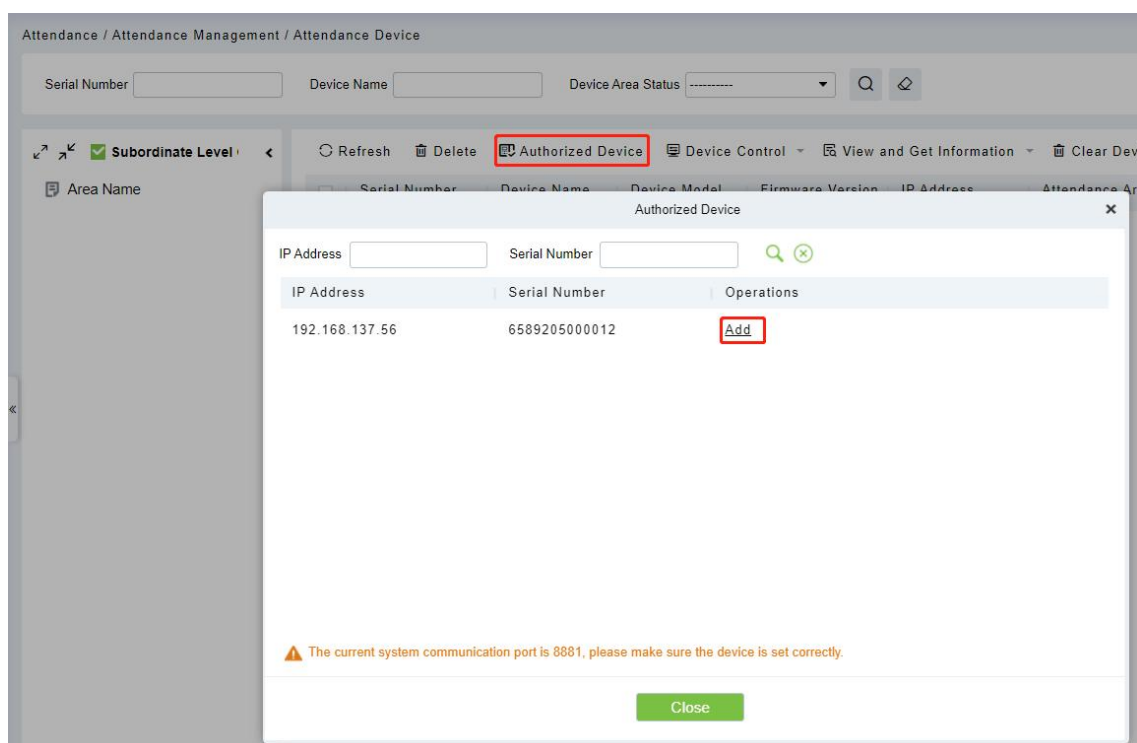
5.1.2 Attendance Device

After a time and attendance device is added to the software, the user can search device, edit, delete, device control, view and get information, clear device data, view commands, etc.
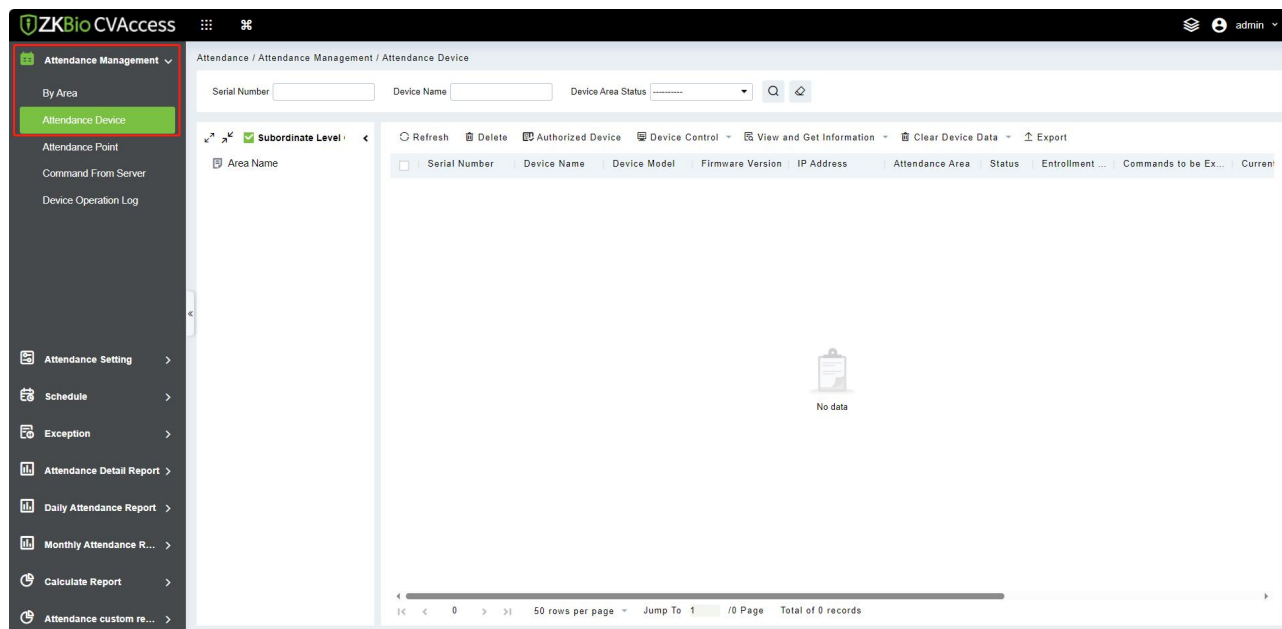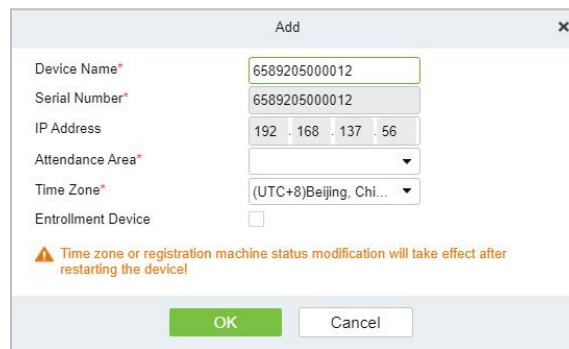

5.1.2.1 Authorized Device

1. Click **[Attendance Management]** > **[Attendance Device]** > **[Authorized Device]**, as follows:

2. Click **[Add]** to pop up the device edit interface. After the information is filled in, click **[OK]** to complete operation, and click **[Cancel]** to cancel the edit operation.

Fields are as follows:

- **Device Name:** Time and attendance device name, any character up to 20.

- **Device Serial Number:** Attendance device serial number.

- **IP Address:** The IP address of the attendance device.

- **Attendance Area:** The equipment for regional division, to achieve regional data management.

- **Time Zone:** Time and attendance at different time zones.

- **Enrollment Device:** If not selected, the user data uploaded by the device will not be processed (the attendance record of the device will not be checked). If checked, the user data uploaded by the device will be processed.

✍ **Note:** Before adding devices to the software, users need to set the communication IP and address of time attendance device.

5.1.2.2　Edit Device

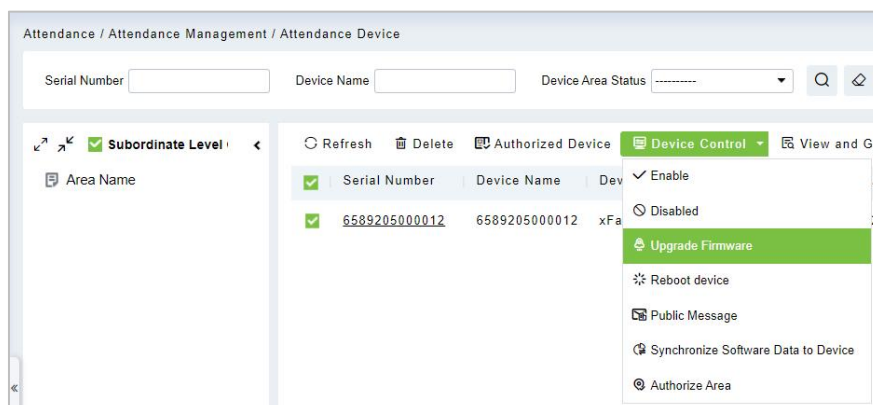Select the device and click ✑ button, to modify device information.

5.1.2.3　Delete

Select the device and click **[Delete]** to remove the device and its information.

5.1.2.4　Refresh

Click **[Refresh]** to update the device list status information.

5.1.2.5 Device Control

➢ **Enable**

After the device is enabled, the upload and download of data are enabled normally. (When the device is enabled, users can choose whether it is a registration device or not).

➢ **Disable**

After the device is disabled, the device is not allowed to upload and send data.

➢ **Upgrade Firmware**

Select the required device that needs to be upgraded, click **[Upgrade firmware]** to enter edit interface, then click **[Choose File]** to select firmware upgrade file (named emfw.cfg) provided by Access software, and click **[OK]** to start upgrading.
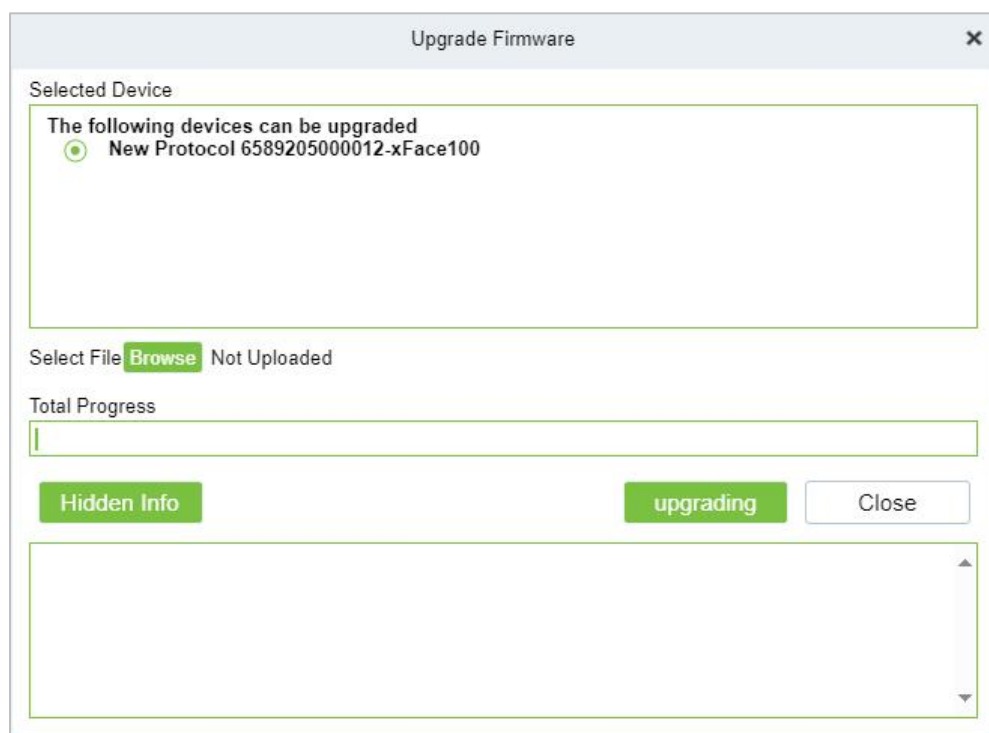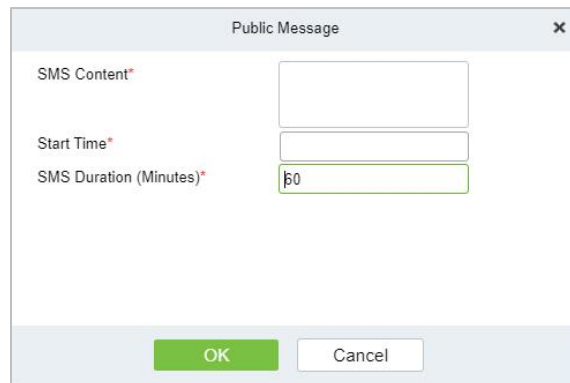

➢ **Reboot Device**

Select the device you want to restart; the software sends a reboot command and restarts the device.

➢ **Public Message**
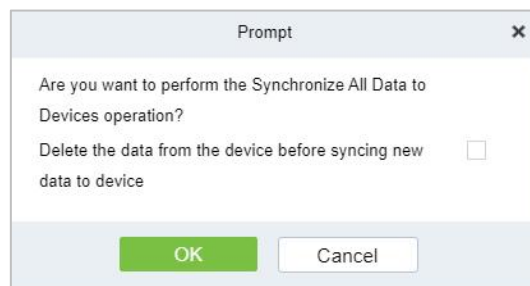
You can set the public messages in the device so that the device can display short messages on the page (Not all the devices support this function).
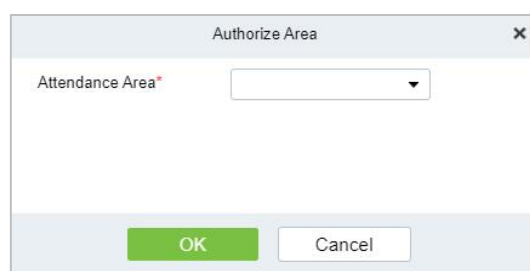

➢ **Synchronize software data to the device**

Select the device to be synchronized and send the corresponding device area data in the software to the device.

➢ **Authorize Area**

It can reach certain areas within a period of time after being authenticated.

5.1.2.6 View and Get Information

> ➢ **Get Device Option**

Select the device of which you want to get information, click Get software to send command, get the device related parameters, such as: serial number, IP address, device model, firmware version number, etc.

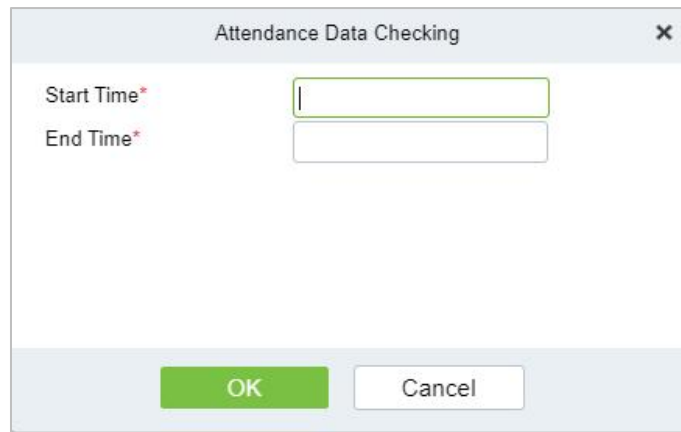> ➢ **View Device Parameters**

After clicking **[View Device Parameters]**, the page will navigate automatically to the device commands page in the system management module to show command queries.

> ➢ **Attendance Data Checking**
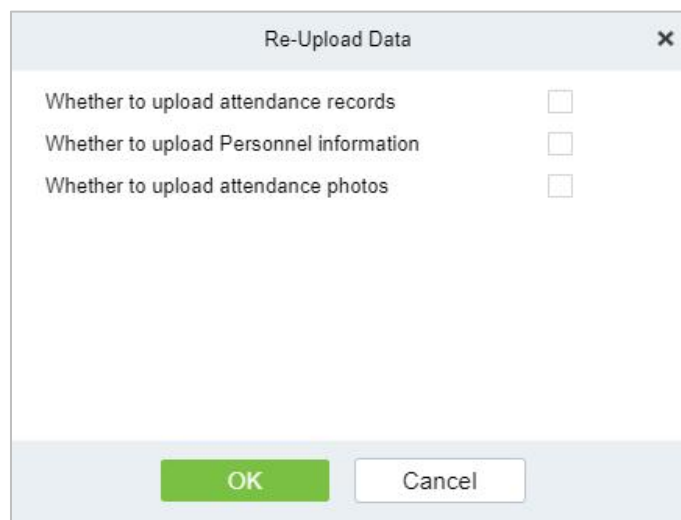
Select the device to proofread data, select the proofing date, the software issues a command to proofread the software and device attendance data.

> ➢ **Re-upload Data**

Select the device in which you want to upload data. Click to enter the check box to upload the data type: attendance record/attendance photo, click the confirmation to get such information again from the device.

> ➢ **Get the Specified Personnel Data**

Select the device from the list and click Get the Specified personnel data.

Enter the desired person numbers separated by a comma and click **[OK]**.

5.1.2.7 Clear Device Data
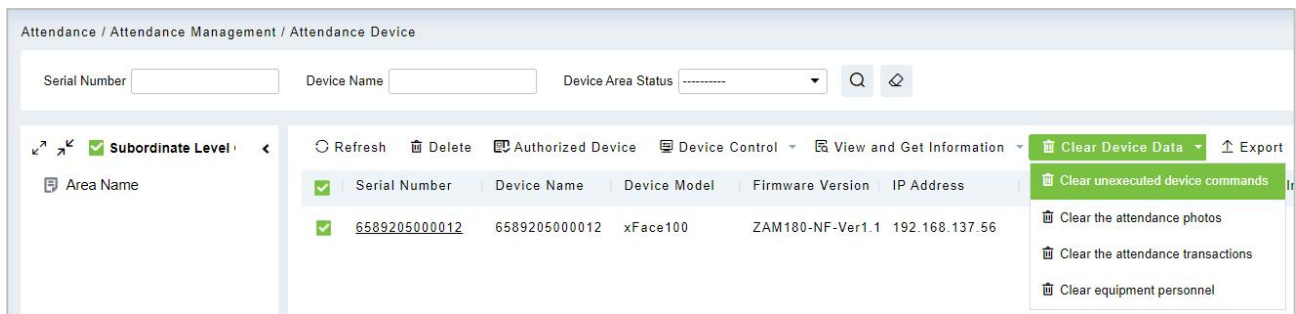
➢ **Clear Unexecuted Device Commands**

Select the device to be cleared. It clears the operation command issued by the software in the setting.

➢ **Clear the attendance photos**

Select the device. This function will clear all the attendance photo records from the device.
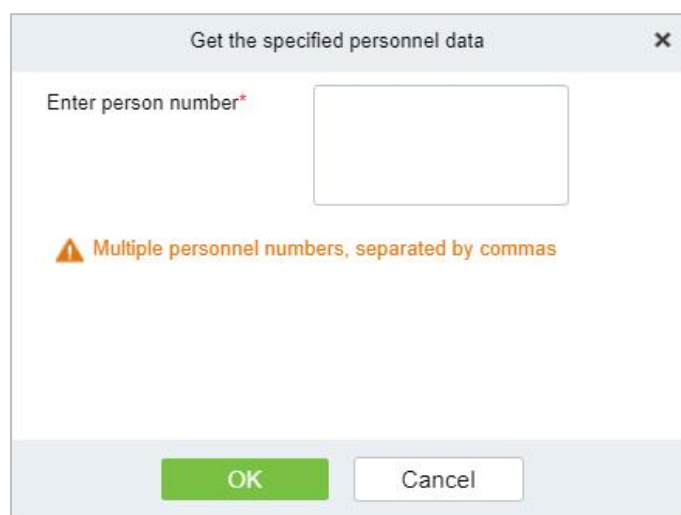
➢ **Clear the attendance transactions**

Select the device. This function will clear all the attendance data records from the device.

➢ **Clear equipment Personnel**

This function will clear all the equipment personnel records from the device.

5.1.2.8 Export

Device information can be exported in EXCEL, PDF, and CSV file format.
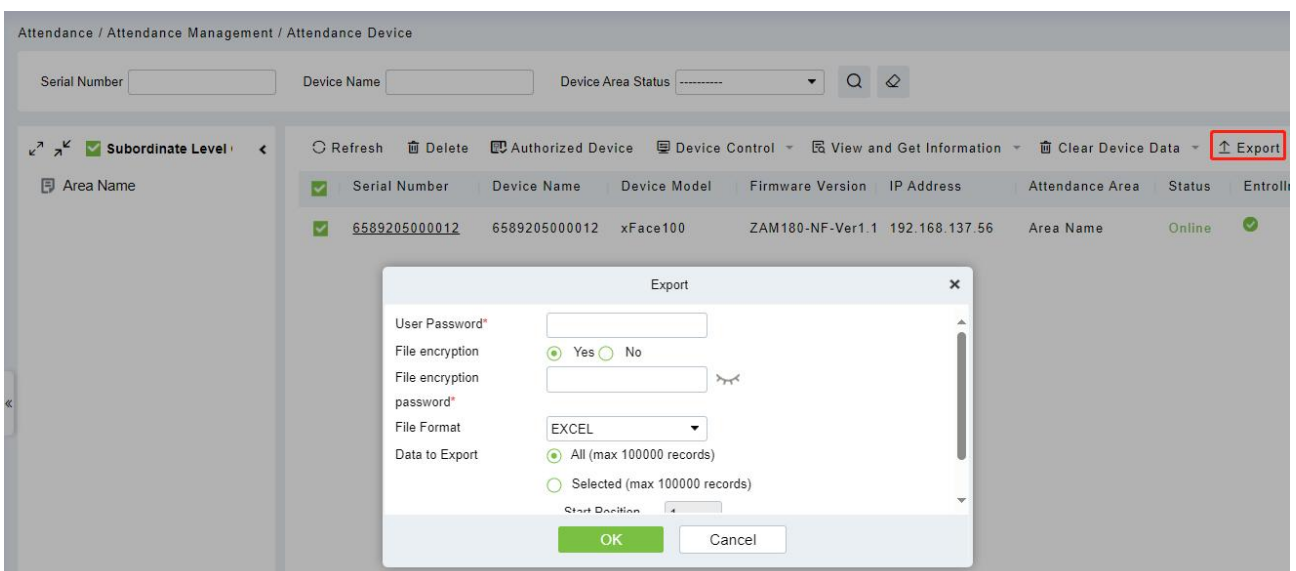
5.1.3 Attendance Point

The system supports setting access control as the attendance point. After setting the access device

as an attendance point, its access records will be transferred to the attendance system in real time as punch records.
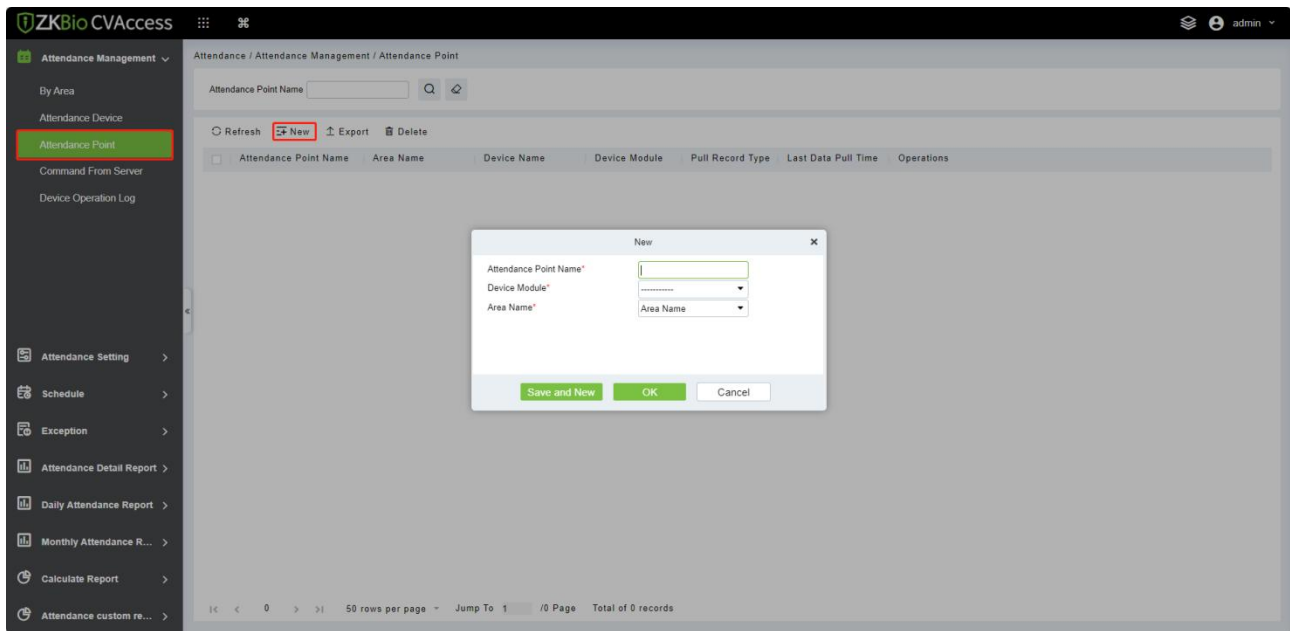
5.1.4 Command from Server
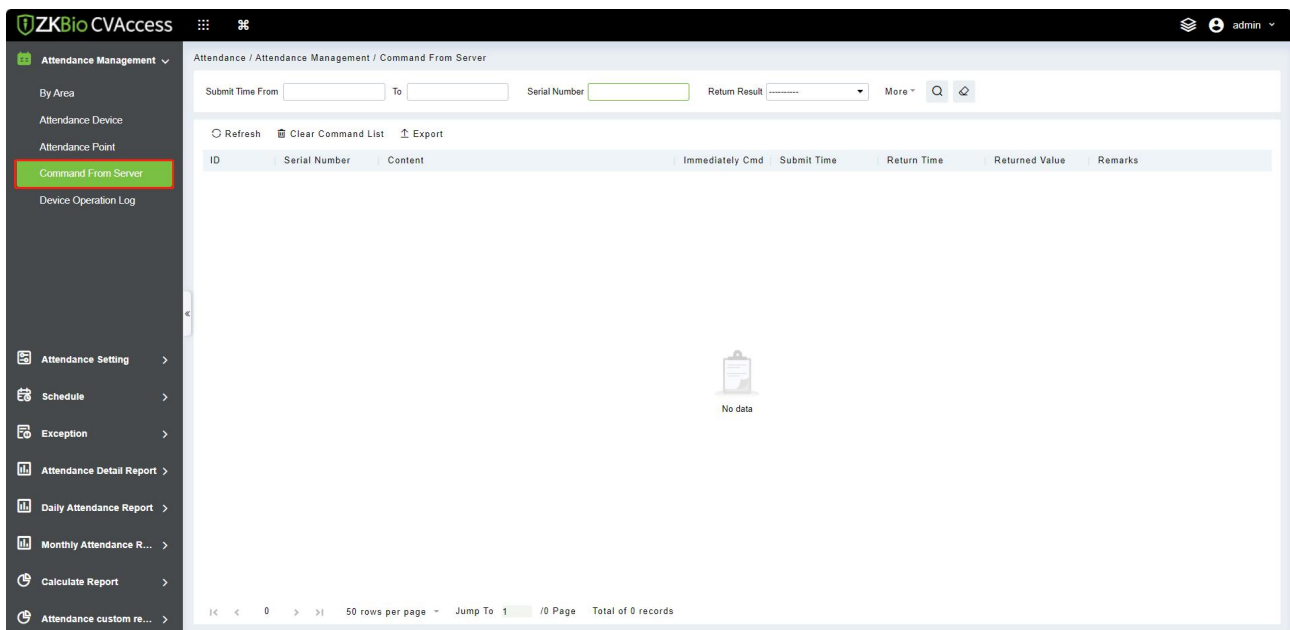
5.1.5 Device Operation Log

Click **[Attendance Management]**> **[Device Operation Log]** to display the operation logs of the attendance device in the area.
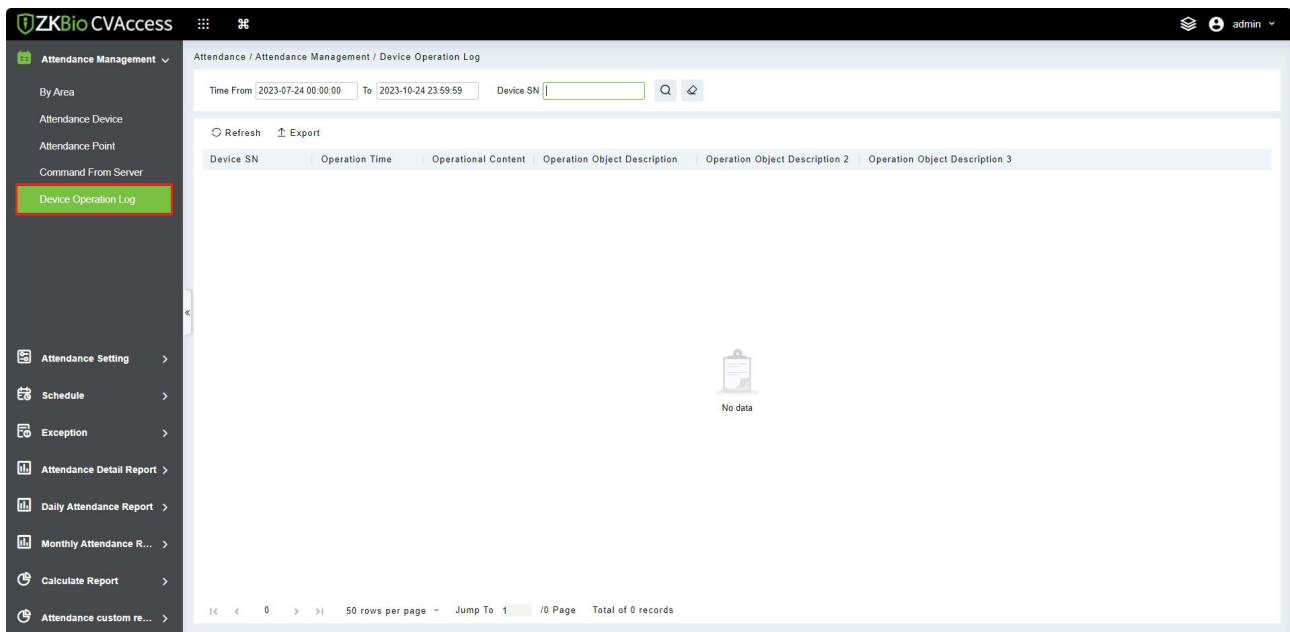
5.2 Attendance Setting

5.2.1 Attendance Rules

Since the attendance system of the company is different, the user needs to manually set the attendance parameters to ensure the accuracy of the final attendance calculation. The attendance rule setting is a way to show the company's attendance system.

Click **[Attendance] > [Attendance Setting] > [Attendance Rules]**.

5.2.1.1 Basic Rule Setting

Check-in Rule:

- Earliest Principle: By default, it takes the first check-in within the valid time zone.

- Closest Principle: It will take the closet check-in within the valid time zone.

Check-out Rule:

- Late Principle: By default, it takes the last punch card record within the range of valid attendance range.

- Closest Principle: It takes the punch card record closest to the closing time within the range of valid attendance).

Attendance calculation result when the shift cross-day:

- The first day: The effective working hours of the second day is counted to the first day;

- The second day: The effective working hours of the first day is counted to the second day.

Overtime Statistics: Yes (default), No; the first overtime switch for statistics, if set to No, overtime will not be calculated.

Intelligent Matching Shift Rule: Longest Working duration, Least abnormal (default). The longest working duration will calculate each shift respectively to obtain the most effective longest time shift. The Least abnormal will consider the shift which has a minimum number of exceptions (such as late, leave early, etc.).

Late & Early Leave Counted as Absent: No (default) Yes refers to that if it is late or early leave, then the time period is recorded as an absence.

Missing Check-In count as: If no sign-in or no sign-out record is incomplete, the priority is the highest, then no late arrival, early leave, absenteeism and validity will be counted When missing Check-In is counted as late, if no Check-In, it will be counted as being late for N minutes. If the absence of sign-in or sign-out is recorded as absenteeism, the length of absenteeism is equal to the length of working hours minus the length of late and early leave.

Missing Check-Out count as: If no sign-in or no sign-out record is incomplete, the priority is the highest, then no late arrival, early leave. Absenteeism and validity will be counted When missing Check-Out is counted as early leave, if no Check-Out, it will be counted as leaving early for N minutes.

The minimum time period should be greater than (minimum 10 minutes):120 (default); Range: 10-999; Required.

The maximum time period should be less than (maximum 1440 minutes): 600 (default); Range: 10-1440; Required.

Exact digits of the decimal point: 1 (default), 2.

5.2.1.2 Non-Leave Calculation Setting

Minimum Unit: Calculate the smallest unit of this arix.

Rounding Control:

- Down (discard): discard the decimal part, as long as the integer.

- Rounding: If the first decimal place is greater than 5, the integer will be added with 1, otherwise, the integer will be taken.

- Up (carry): With decimal, discard decimal, integer plus 1.

Report Display Symbol: Symbols for associated report presentation.

5.2.1.3 Annual Leave Balance Setting

Annual Leave Clearing and Issuing Date: Set the annual leave clearing date.

Annual Leave Rule: Set annual leave days according to length of service, which can be added by symbols.

5.2.1.4 Other Rules

Attendance Photo: After enabling the option, the sensitive personal data involved in this module will be desensitized or obscured.

Enable Real Time Roll Call: Turn on the real-time roll call function, and the sign-in status of personnel will be displayed in the "sign-in Table" under the report.

Whether to enable employee self-service login: The frequency of setting attendance points to obtain records includes (10 seconds/time, 20 seconds/time, 30 seconds/time, 1 minute/time ~ 8 minutes/time).

5.2.2 Holiday

Click **[Attendance] > [Attendance Setting] > [Holiday]** to manually adding holidays in.

5.2.2.1 Adding

1. In the function menu, click **[Attendance Setting]** > **[Holiday]** > **[New]**, the following page is displayed:
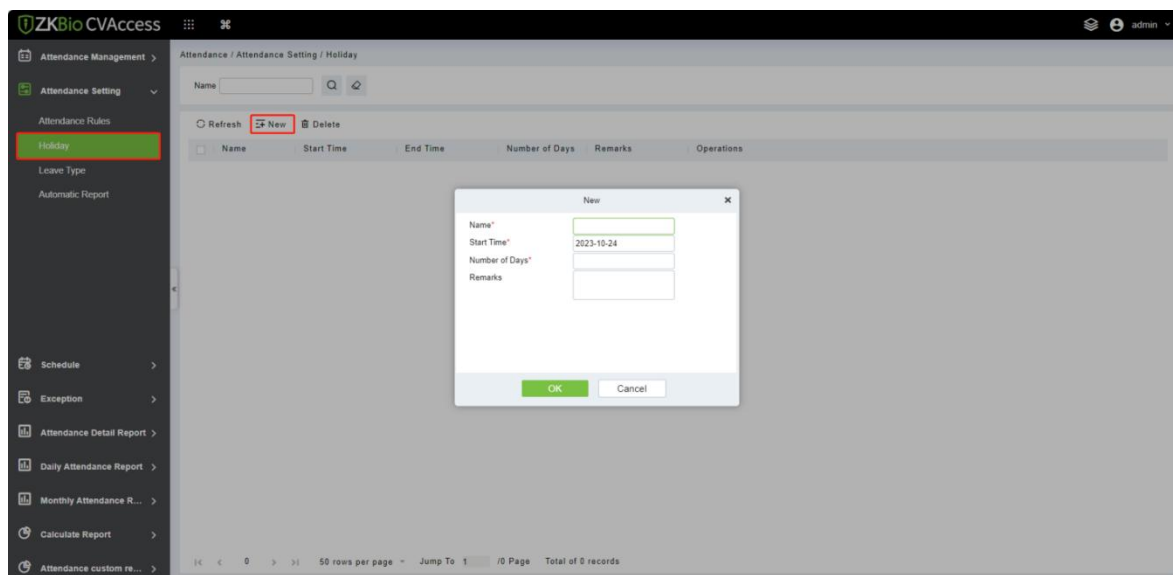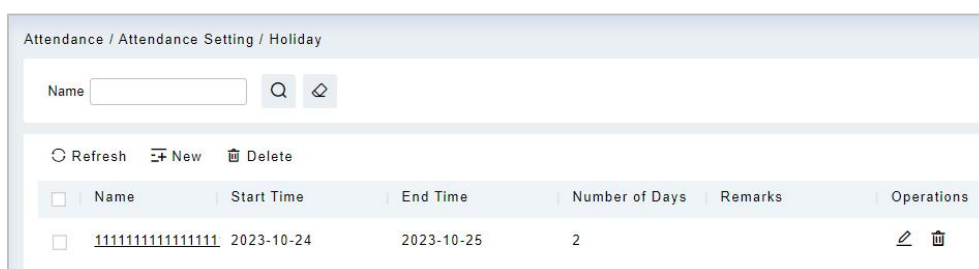
2.	After the information is entered, click **[OK]** to finish new addition, click **[Cancel]** to cancel new addition.

Field Description:

- **Name:** Required.

- **Start time:** Holiday start date, the format is date and time.

- **Number of Days:** The duration of the holiday, character length 2, required.

- **Remarks:** Character length 50.

5.2.2.2 Edit

Select holiday which need to be edited and click ✎ button beside holiday information.

5.2.2.3 Delete

Select the Holiday which need to be deleted and click 🗑 button.

5.2.3 Leave Type

There are 9 leave types by default, editable, but not allowed to be deleted: user-defined leave type can be extended.

Click **[Attendance] > [Attendance Setting] > [Leave Type]**.

5.2.3.1 Adding

1. In the menu, click **[Attendance Setting]** > **[Leave Type]** > **[New]**, the following page is displayed:
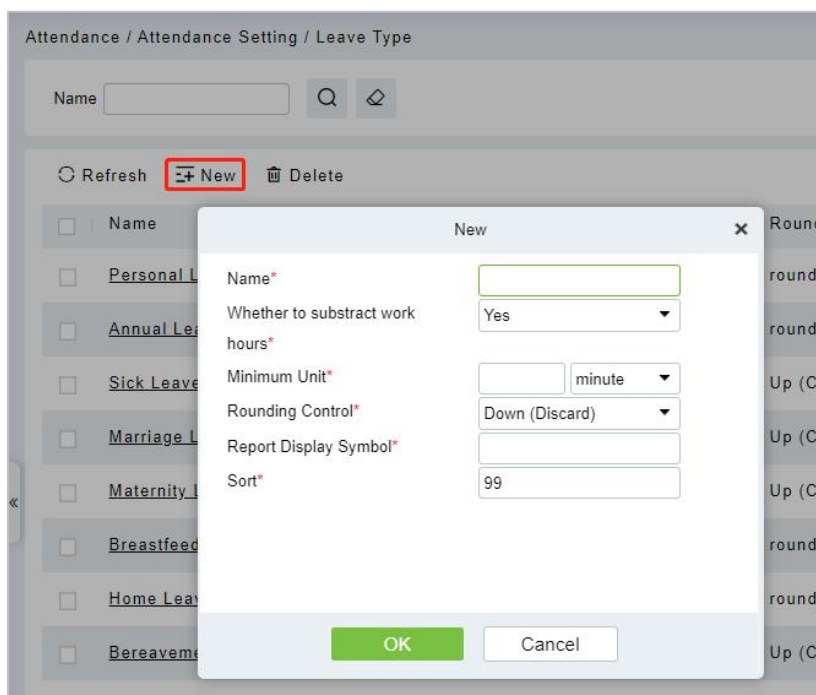
2. After the information is entered, click **[OK]** to finish new addition, click **[Cancel]** to cancel new addition.
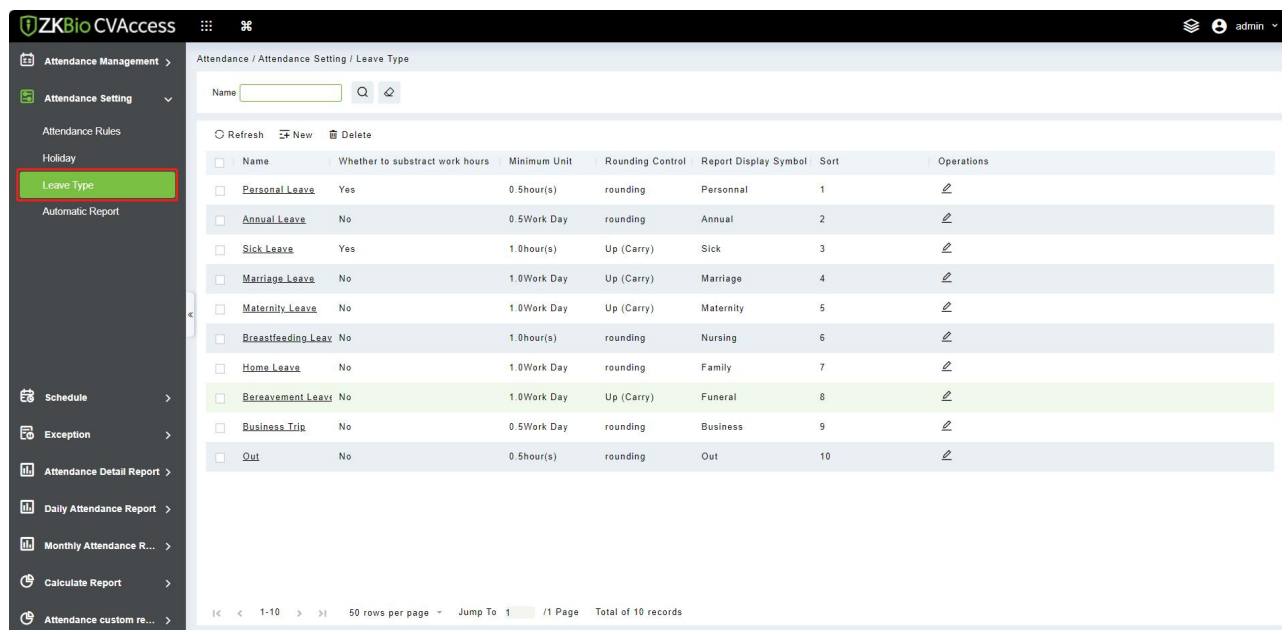
3. The default system has 9 kinds of leave type, Casual leave, Marriage Leave, Maternity Leave, Sick Leave, Annual Leave, Home Leave, Bereavement Leave, Breastfeeding Leave, custom. We can edit these leave type but cannot delete it.

5.2.3.2 Edit

Select the leave type and click ✎ button to edit.

Field Description:

- **Name:** Required, maximum character length is 30.

- **Whether to subtract work hours:** Set whether to deduct the length of work for the leave of this leave. For example, maternity leave / marriage leave / annual leave are statutory holidays without deducting the length of work.

- **hours:**

  - **Minimum Unit:** Calculate the smallest unit for this alias.

  - **Rounding Control:** Down (discard): discard the decimal part, as long as the integer; Rounding: If the first decimal place is greater than 5, the integer will be added with 1, otherwise, the integer will be taken; Up (carry): There are decimals, decimals are discarded, integers are added by 1.

- **Report Display Symbol:** Symbols for the presentation of the associated report.

- **Sort:** Sort job listings, only numbers are supported.

5.2.3.3 Delete

Select the leave type and click **[Delete]** to delete.

5.2.4 Automatic Report

Automatic report supports the function to package the report into an attachment at a fixed time point (daily or monthly) and send the attachment via email to be designated personnel or ftp server.

1. In the function menu, click **[Attendance Setting]** > **[Automatic Report]** > **[New]**, the following page is displayed:
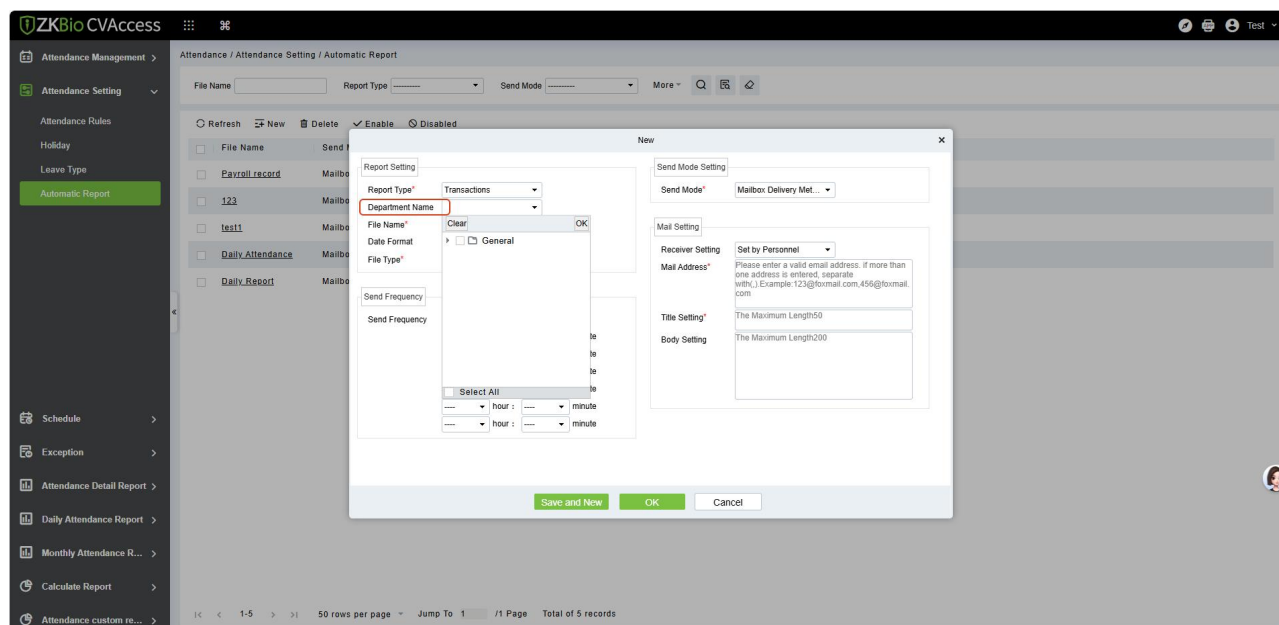
2. In the Report Setting section.

    Report Type: Select the desired choice from "Transactions" or "Daily Attendance". The report will be according to the selected type. Transactions will give the details related to the device with Attendance area and time of the personnel. Daily attendance will give the attendance details of the personnel.

    Department Name: you can select the department name. After selection, only the attendance records of the selected department will be pushed to the recipients.

    File Name: Consists of 3 parts: custom file name + year, month, day, hour, minute and second, such as (Department of the original records of the test section 201706271143).

A. The first field is for the custom file name.

B. The second field contains two option for the format of the date: yyyyMMdd and yyyy-MM-dd.

C. The third field contains the hour, minute and second format: Currently it supports HHmmss.

    Data Format: Select the format of the date.

    File Type: Currently it supports TXT.

3. In the Send Frequency section, set frequency for the mail delivery. The frequency has two options; By day and By month. If you have selected "By day", then you can set a maximum of 6 interval in a day (only once per hour) at which the mail delivery will start.

A. It can only be set in increasing order of time.

B. The minute set in the first-time interval will be same for all other five intervals.

    If you have selected as "By month", then you have 3 options to choose from; first is "last day of the month", second is first day of the month and the third is any specific date.

4. Send Mode: Choose a delivery method.

5. Mail setting: Set the details of receiver mail.

➢   **Receiver settings:**

Set the receiver as per below options:

- ⊠ Set by Personnel: Enter the E-mail address in text box, and if more than one email is there, then put ":" to separate the e-mails.

- ⊠ Set by Department: Select a department from the department hierarchy,

- ⊠ Set by Area: Select an attendance area from the area hierarchy,

➤ **Mail address:** Enter a valid mail address. The maximum length is 50 characters.

➤ **Title setting:** It refers to subject of the mail. The maximum length is 50 characters.

➤ **Body settings:** Write the text accordingly. The maximum length is 255 characters.

6. Make sure the sender mail settings are already defined.

7. Once all the details are filled, click **[OK]** to finish.

5.3 Schedule

5.3.1 Timetable

This function is used to set the time zone that will be used in the attendance calculation and configuring the information of each parameter with the minimum unit set. For example, allow late / early leave time, whether it is necessary to Check-in / Check-out, set the time range of Check-in / Check-out, overtime setting and so on.

Before setting the shift, you should set all possible time segments, that is, time zone setting. Set the shift before scheduling, setting the attendance rules in the settings will be significant.

Click **[Attendance]** > **[Schedule]** > **[Timetable]** to enter the time zone page:
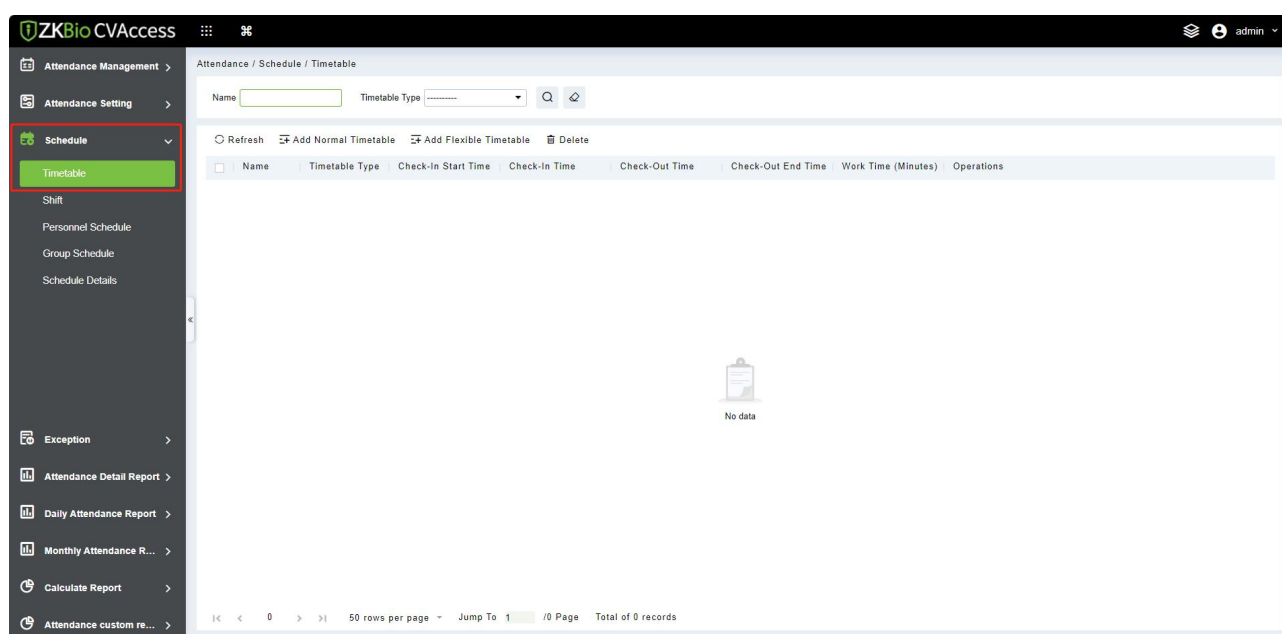
5.3.1.1 Add Normal Timetable

This paper introduces the configuration Steps of adding normal time period to the regular shift

configuration of VAORIDA.

1.   Click **[Add Normal Timetable]**.

2.   Configure the time period information in the **Add Normal Time** Period window.

Field Description:

• **Before/After work:** Set the valid range of check-in/check-out for this time period, and the check-in/check-out records outside this range are invalid records. The valid sign-in time after going to work and the valid sign-out time before going off work cannot overlap, which must be filled in.

• **Allow Late/Allow Early/Leave(Minutes):** Refers to how long it is allowed to be late and leave early within the specified time points for going to and from work, and the minutes allowed to be late and leave early must be within the valid time range of sign-in and sign-out before they can take effect.

• **Must Check-In/Check-Out** In the selected time range, set whether you must sign in and sign out when going to and from work.

• **Auto Deduct Break Time:** When used for attendance calculation, whether to subtract the number of minutes defined by inter-segment deduction for this time period.

• Start counting overtime before/after N minutes from work/work, with the shortest overtime minutes and the maximum overtime hours limited: Select whether to record the verification records before and after work as overtime.

5.3.1.2   Add Flexible Timetable

1.   Click **[Add Flexible Timetable]**.

2.   Configure the time period information in the **Add Flexible Time** Period window.

5.3.1.3 Delete

Click **[Delete]** or click on the 🗑 icon to delete the required Timetable type from the list.

5.3.2 Shift

Shift is composed of one or more timetable period(s) in accordance with a certain order and cycle of sequence. It is set as default shift for staffs. To get staff attendance, first we must set the shift.

Click **[Attendance]** > **[Schedule]** > **[Shift]** to enter the main menu of shift as shown below. The search function can be convenient for shift inquiry. The list shows all shifts of the current system. The time period details list shows the details of the time period of the shift in the form of a chart.
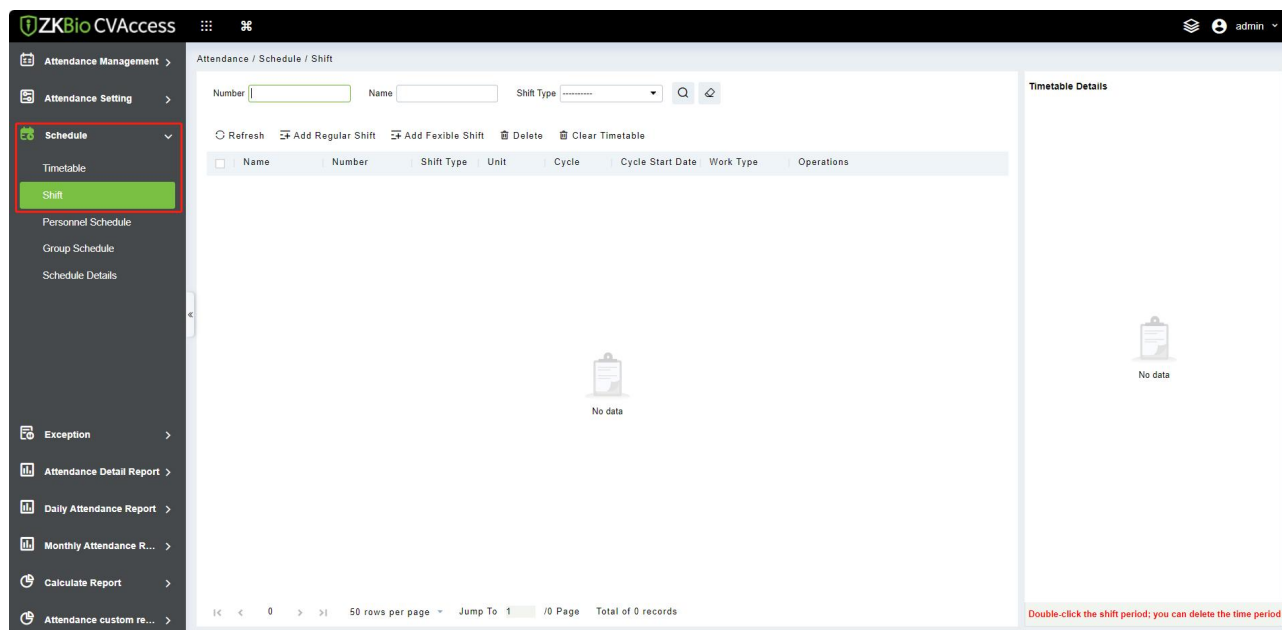
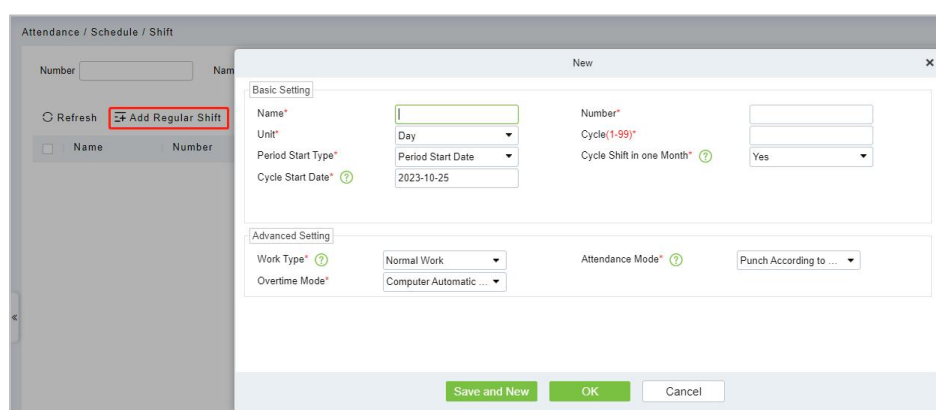### 5.3.2.1 Add Regular Shift

1.   Click **[Attendance] > [Schedule] > [Shift] > [Add Regular Shift]**.

2.   Configure the shift information in the **Add Regular Shift** window.

Field Description:

•   **Unit:** Set the unit of the cycle, and the default is "day". There are three types of units: Day, Week, Month.

•   **Period:** Defines the number of cycles of a shift, and the cycle of the shift = cycle number * units.

   1)   If the unit is "day", the range is 1 to 99.

   2)   If the unit is "week", the range is 1 to 15.

   3)   If the unit is "month", the range is 1 to 12.

•   **Period starting type:** This field is displayed only when the cycle unit is Day, Description:

   1)   It is not displayed when the units are "week" and "month".

   2)   There is cycle start date and scheduling start date, and the default is cycle start date.

3)   If you select Scheduling Start Date, the start date when scheduling is the first day of the cycle.

- **Period start date:** This field is displayed only when the cycle start type is Cycle Start Date. Define the start date of the shift, and the date before the start date is not affected by the shift. The default system start date is the current system date.

- Work Type:

1)   Normal work: This shift is a normal work shift

2)   Overtime on rest days: This shift is overtime on rest days

3)   Overtime on holidays: This shift is overtime on holidays.

- Attendance mode:

1)   Swipe the card normally according to the shift: the default item of the system, and punch in normally according to the punch in.

2)   Brush a valid card once a day: only need to brush the card once in the swiping interval defined by the time period within one day, even if it is normal to punch in.

3)   Punch-in-free: Setting this shift can avoid punch-in.

- Overtime mode:

1)   Computer automatic calculation: It is connected with "whether the delay counts overtime" in the time period. When "whether the delay counts overtime" is "no", the delayed overtime is not calculated, and the overtime time of the overtime bill is not calculated at the same time.

2)   Overtime must be applied: delayed overtime is not calculated, only the overtime order shall prevail; When the signing-back time is less than the end time of overtime, the overtime time is not calculated.

3)   Not counting overtime: overtime hours are not counted for delayed overtime or overtime application.

5.3.2.2 Add Flexible Shift

1.   Click **[Attendance] > [Schedule] > [Shift] > [Add Flexible Shift]**.

2.   Configure the shift information in the **Add Flexible Shift** window.
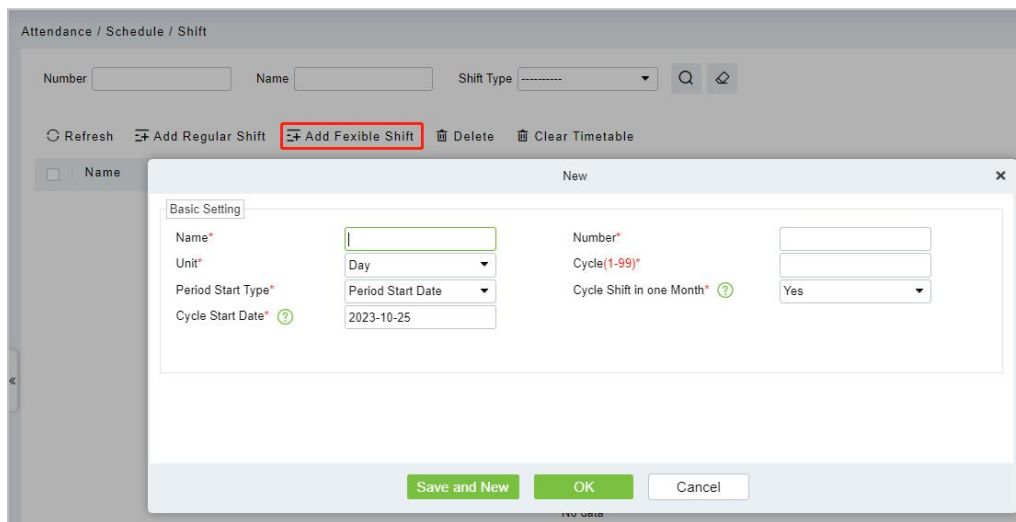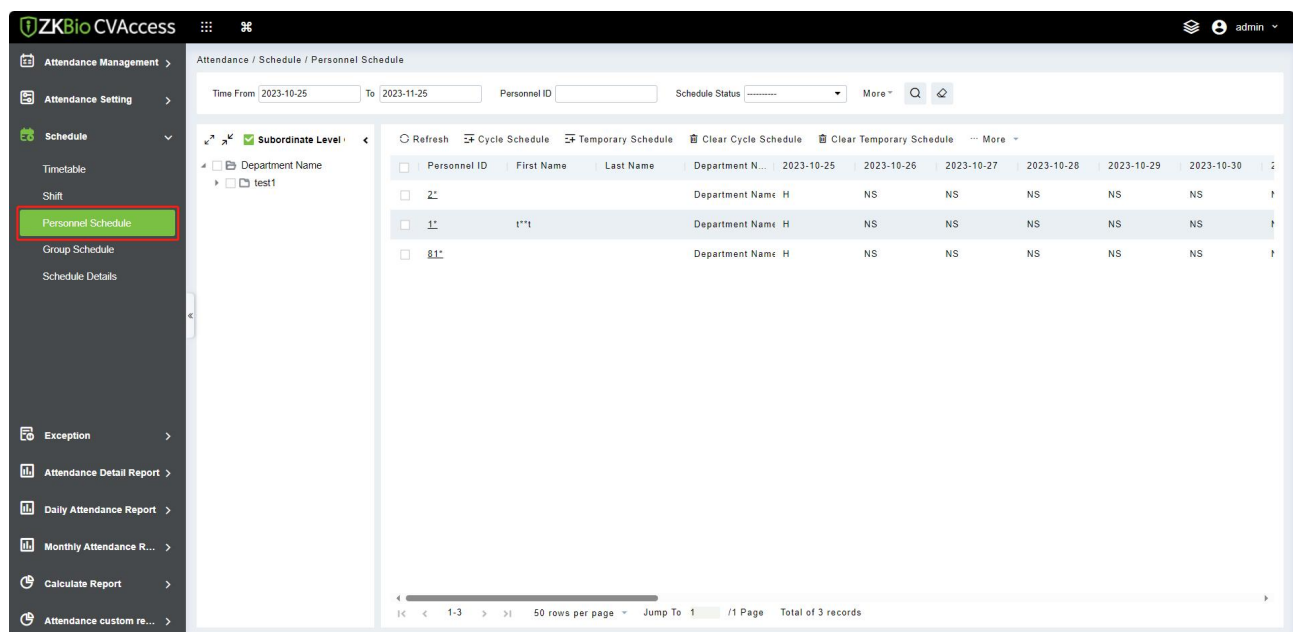
5.3.2.3 Delete

Click **[Delete]** or click on the 🗑 icon to delete the required Shift type from the list.
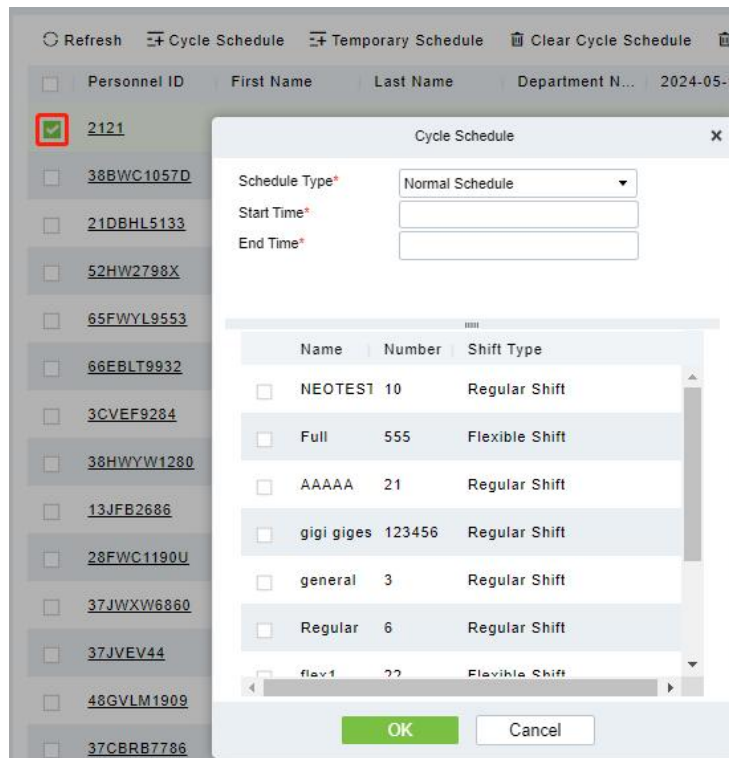
5.3.3 Personnel Schedule

Personnel scheduling operations is completely same as group scheduling, but when scheduling personnel, the object of choice is personnel at the top left corner of the interface.

5.3.3.1 Cycle Schedule

1. Click **[Attendance]** > **[Schedule]** > **[Personnel Schedule]** > **[Cycle Schedule]**.

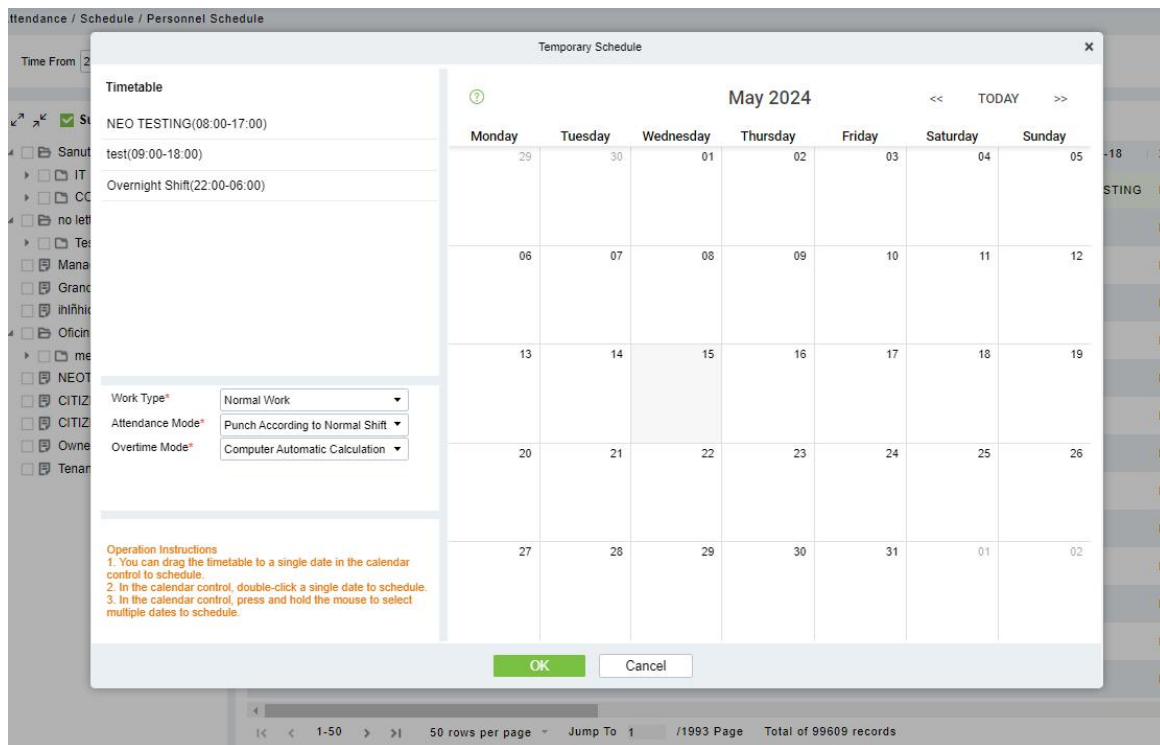2. Configure the Schedule information in the **Cycle Schedule** interface.

Field Description:

- **Schedule Type:**

    1) Normal Shift Scheduling: Only one shift can be selected for normal shift scheduling

    2) Smart scheduling: Smart scheduling can select multiple shifts. Select smart scheduling, and the software will automatically judge the most suitable shift according to the punch-in record for attendance calculation.

- **Start Time/End Time:** Set which date segment the schedule works on.

- **Select Shift:** Select the shift to use for scheduling.

5.3.3.2 Temporary Schedule

1. Select a personnel and click **[Attendance] > [Schedule] > [Personnel Schedule] > [Temporary Schedule]**.

2. Configure the Schedule information in the **Temporary Schedule** interface.

Field Description:

- Work Type:

  1) Normal work: This shift is a normal work shift.

  2) Overtime Time OT: This shift is overtime on rest days.

  3) Holiday OT: This shift is overtime on holidays.

- Attendance Mode:

  1) Punch According to Normal Switch: the default item of the system, and punch in normally according to the punch in

  2) Punch Once at any Time in a Day: only need to brush the card once in the swiping interval defined by the time period within one day, even if it is normal to punch in.

  3) No Punch Required: Setting this shift can avoid swiping cards.

- Overtime Mode:

  1) Computer Automatic Calculation: It is connected with "whether the delay counts overtime" in the time period. When "whether the delay counts overtime" is "no", the delayed overtime is not calculated, and the overtime time of the overtime bill is not calculated at the same time.

  2) Overtime must be applied for: delayed overtime is not calculated, only the overtime order shall prevail; When the signing-back time is less than the end time of overtime, the overtime time is not calculated.

  3) Not Calculated as Overtime: overtime hours are not counted for delayed overtime or overtime application.
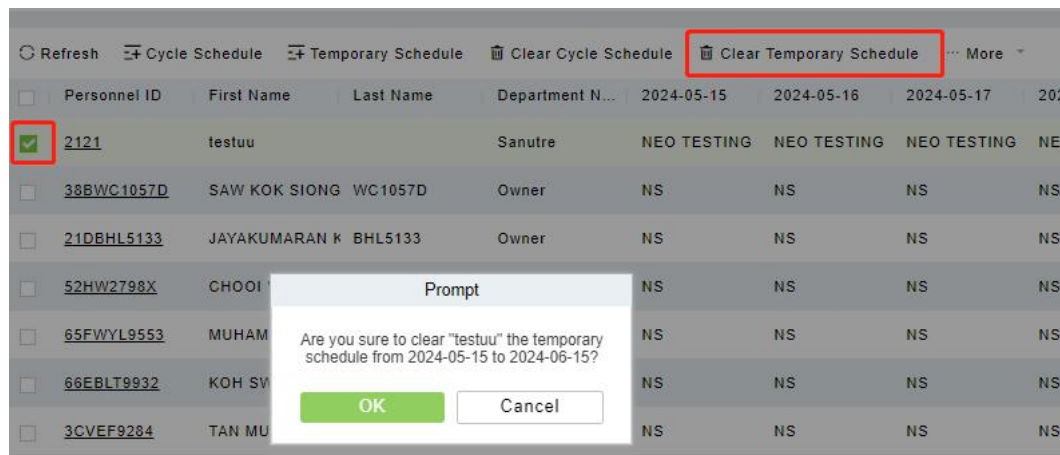
5.3.3.3 Clear Cycle Schedule

Select a personnel and click **[Attendance] > [Schedule] > [Personnel Schedule] > [Clear Cycle Schedule]** to clear the cycle schedule.
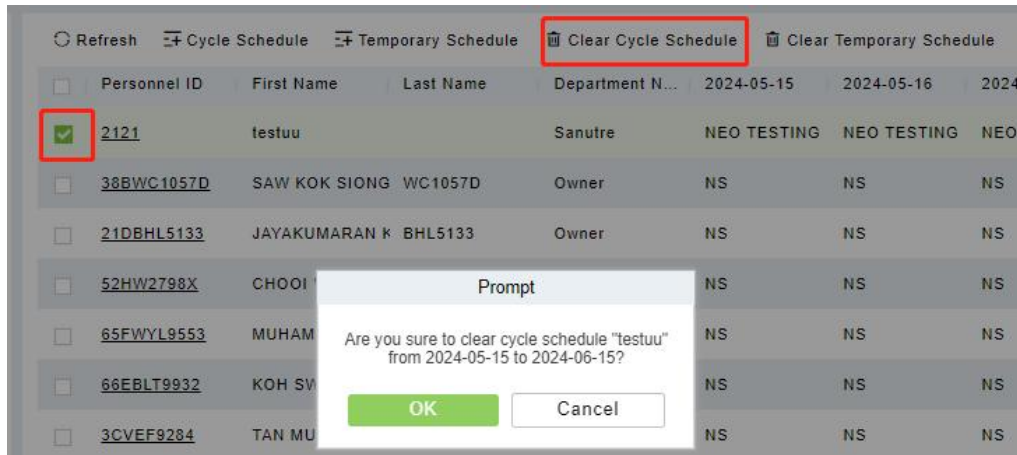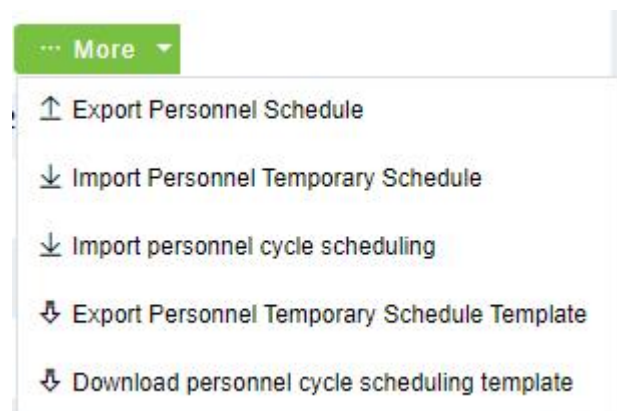

5.3.3.4 Clear Temporary Schedule

Select a personnel and click **[Attendance] > [Schedule] > [Personnel Schedule]] > [Clear Temporary Schedule]** to clear the temporary schedule.
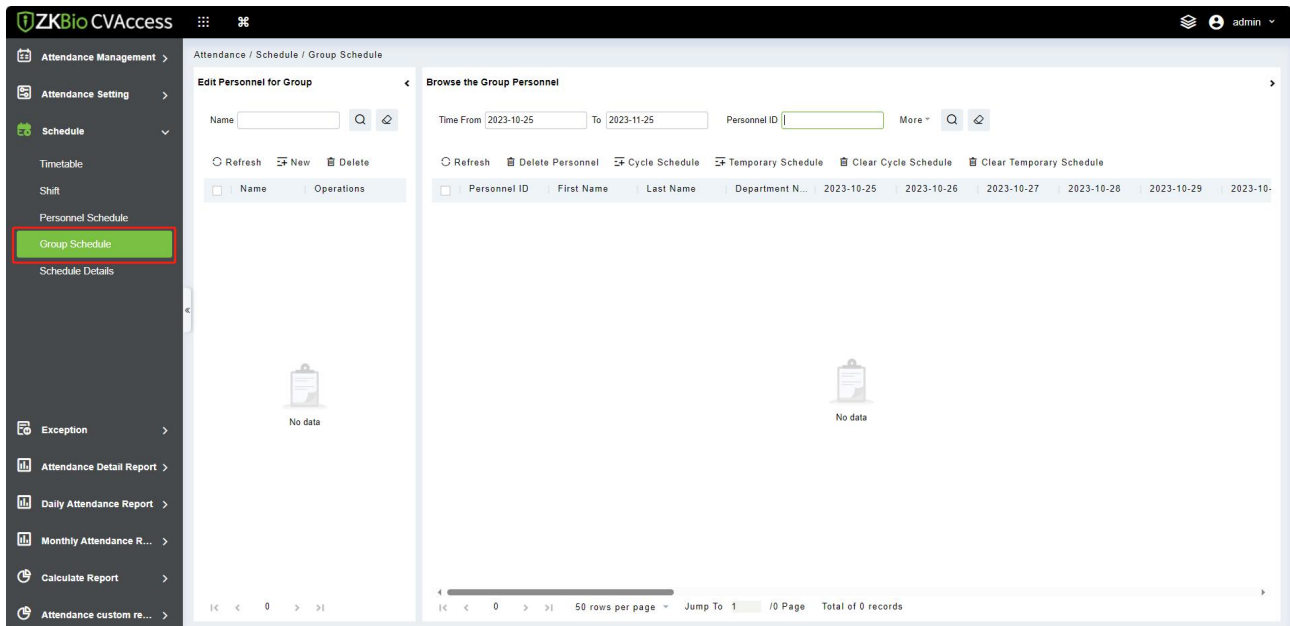

5.3.3.5 More (New)

1.   Click **[Attendance] > [Schedule] > [Personnel Schedule] > [More]** to export/import/download schedule.

5.3.4 Group Schedule

Grouping scheduling means grouping people, and then scheduling people in batches by grouping.

This paper introduces the configuration Steps of grouping cycle scheduling in.

5.3.4.1 Edit Personnel for Group

➢ **New**

1. Click **[Attendance] > [Schedule] > [Group Schedule] > [New]**.

2. Configure the Group information in the **Group Schedule** interface.
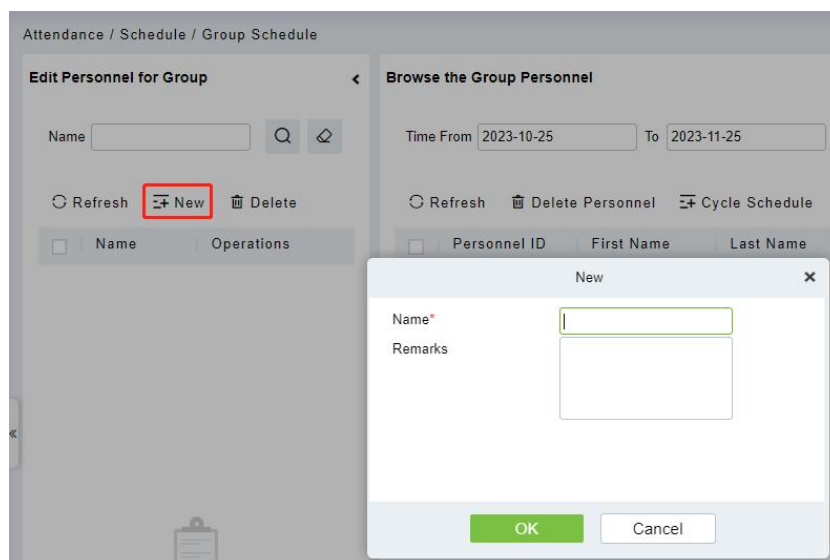
Field Description:

- **Name:** Cannot contain special symbols, period name cannot be duplicated, length is 30 characters, required.

• **Remarks:** Mentioning comments.

➢ **Delete**

Click **[Delete]** to delete the required group from the list.

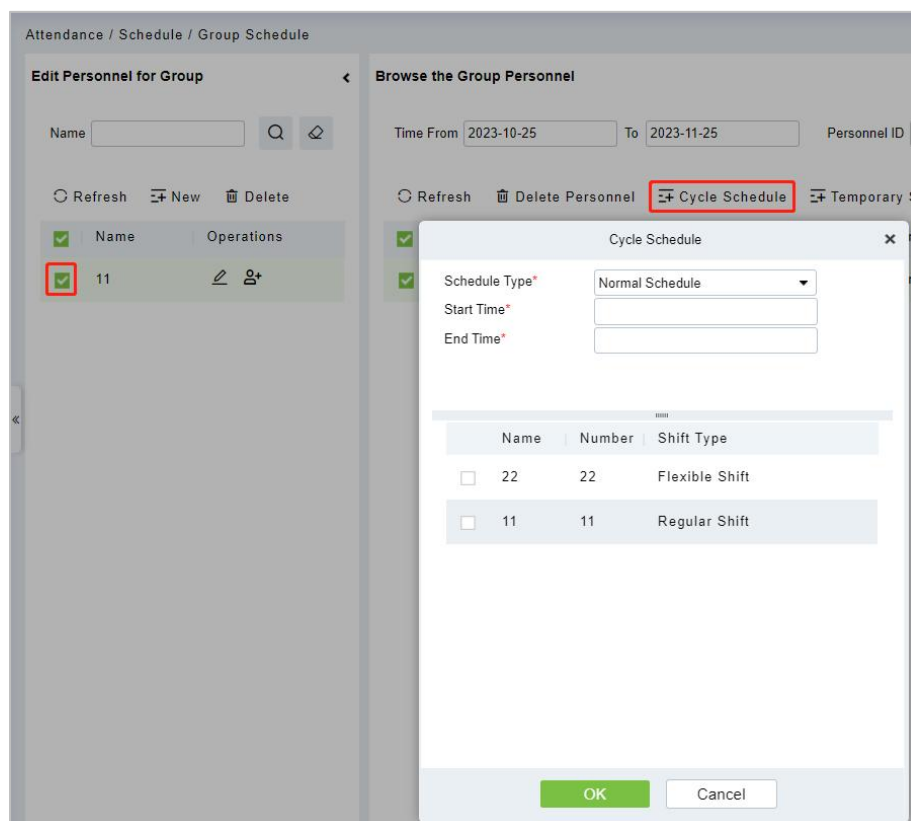### 5.3.4.2 Browse the Group Personnel

➢ **Delete Personnel**

Click **[Attendance] > [Schedule] > [Group Schedule] > [Delete Personnel]** to delete the required person from the list.
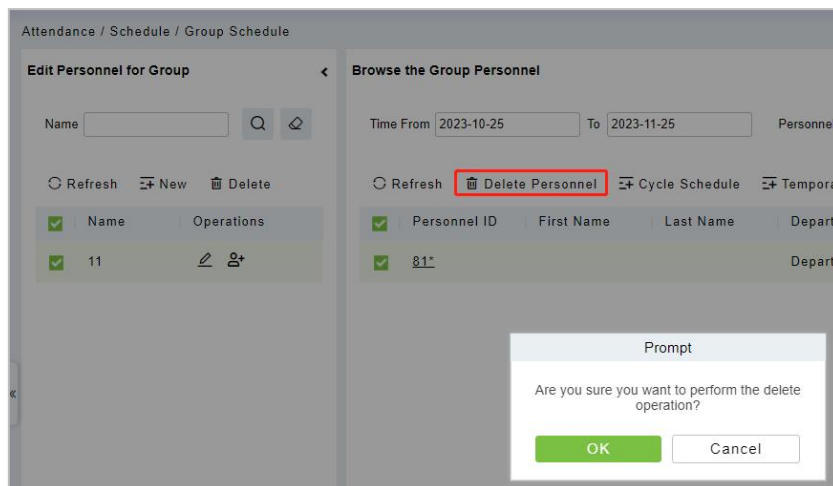
➢ **Cycle Schedule**

1. Select a group and click **[Attendance] > [Schedule] > [Group Schedule] > [Cycle Schedule]**.

2. Configure the Schedule information in the **Cycle Schedule** interface.

Field Description:

- **Schedule Type:**

  Normal Shift Scheduling: Only one shift can be selected for normal shift scheduling

  Intelligent scheduling: Intelligent scheduling can select multiple shifts. Select intelligent scheduling, and the software will automatically judge the most suitable shift according to the punch-in record for attendance calculation.

- **Start Time/End Time:** Set which date segment the schedule works on.

- **Select Shift:** Select the shift to use for scheduling.

➢ **Temporary Schedule**

1. Select a group and click **[Attendance] > [Schedule] > [Group Schedule] > [Temporary Schedule]**.

2. Configure the Schedule information in the **Temporary Schedule** interface.


Field Description:

- Work Type:

  1) Normal work: This shift is a normal work shift.

  2) Overtime Time OT: This shift is overtime on rest days.

  3) Holiday OT: This shift is overtime on holidays.

- Attendance Mode:

  1) Punch According to Normal Switch: the default item of the system, and punch in normally according to the punch in

2) Punch Once at any Time in a Day: only need to brush the card once in the swiping interval defined by the time period within one day, even if it is normal to punch in.

3) No Punch Required: Setting this shift can avoid swiping cards.

• Overtime Mode:

1) Computer Automatic calculation: It is connected with "whether the delay counts overtime" in the time period. When "whether the delay counts overtime" is "no", the delayed overtime is not calculated, and the overtime time of the overtime bill is not calculated at the same time.

2) Overtime must be applied for: delayed overtime is not calculated, only the overtime order shall prevail; When the signing-back time is less than the end time of overtime, the overtime time is not calculated.

3) Not Calculated as Overtime: overtime hours are not counted for delayed overtime or overtime application.

➢ **Clear Cycle Schedule**

Select a group and click **[Attendance] > [Schedule] > [Group Schedule] > [Clear Cycle Schedule]** to clear the cycle schedule for all personnel under the group.
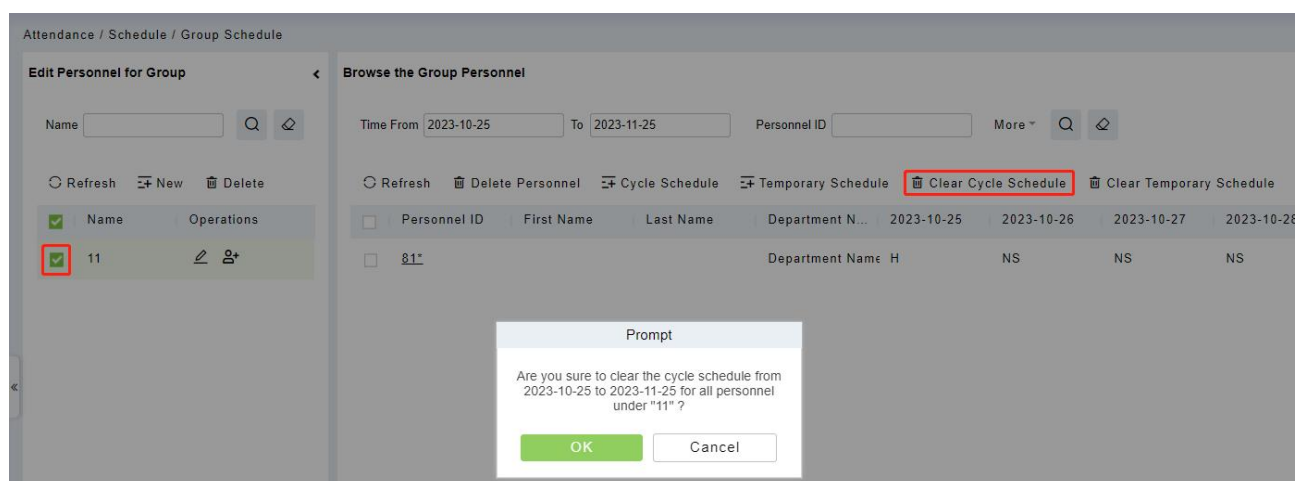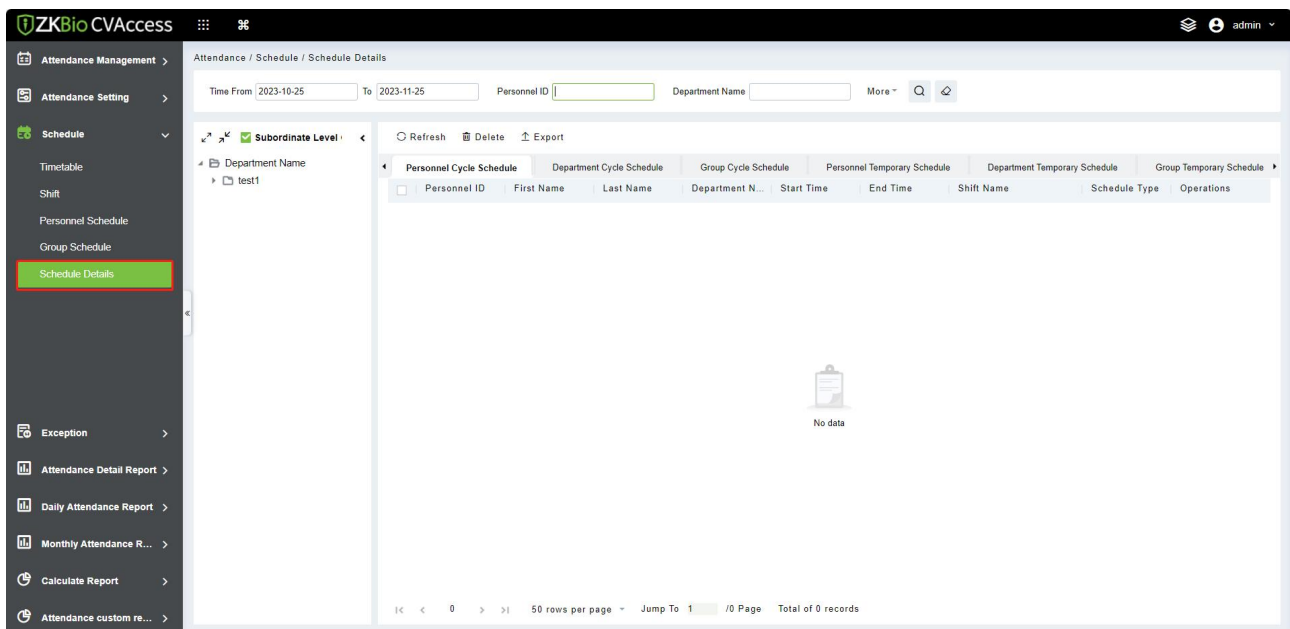

➢ **Clear Temporary Schedule**

Select a group and click **[Attendance] > [Schedule] > [Group Schedule] > [Clear Temporary Schedule]** to clear the temporary schedule for all personnel under the group.
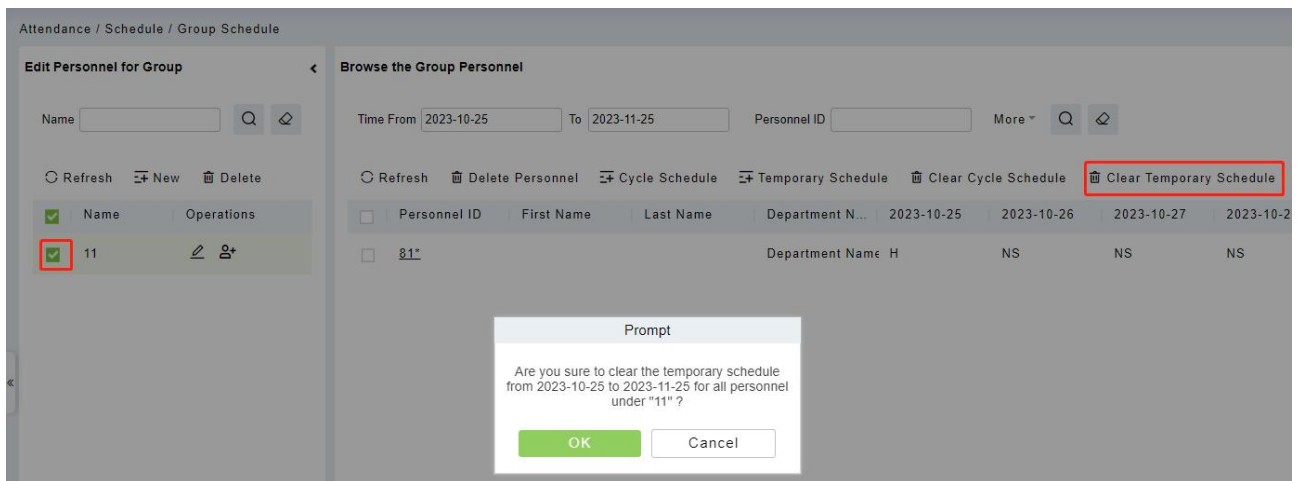
5.3.5 Schedule Details

Click **[Attendance] > [Schedule] > [Schedule Details]**, after setting the attendance time period and shift, you can schedule the personnel.
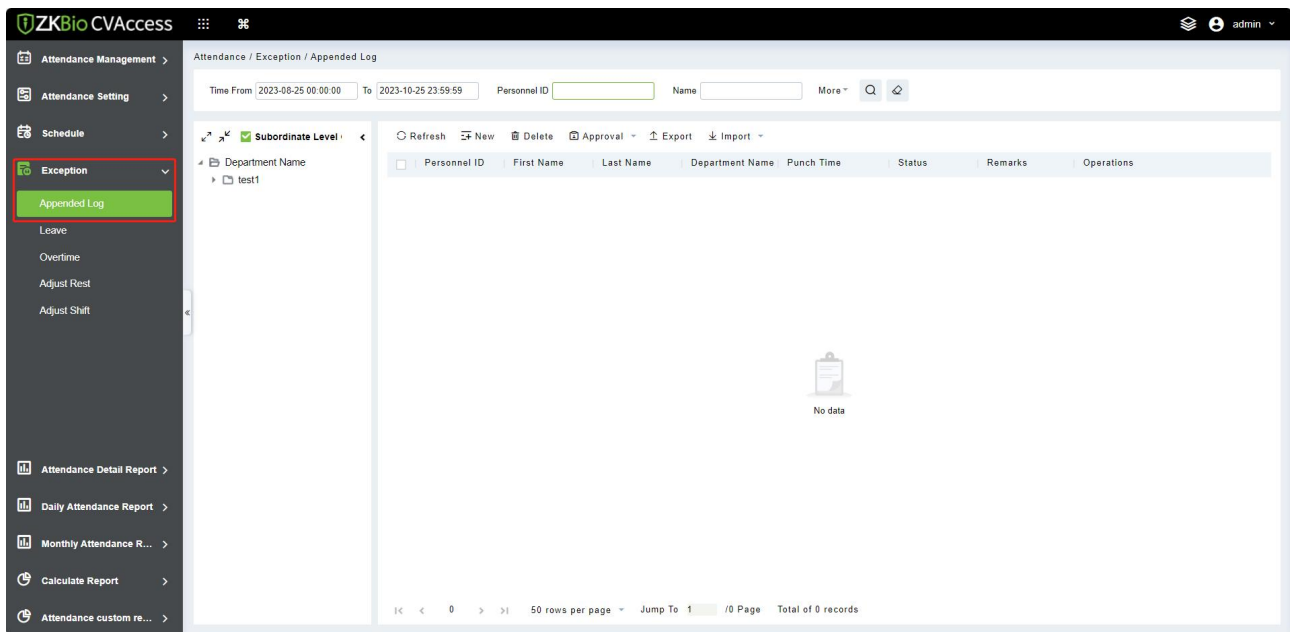

## 5.4 Exception

5.4.1 Appended Log

In the case of personnel going out on business or forgetting to punch in, the manual supplementary recording of attendance records in the attendance report is called supplementary signing card, which is generally summarized and entered by the management personnel according to the attendance results and the attendance system of the enterprise after the attendance cycle ends.

Click **[Attendance] > [Exception] > [Appended Log]**.

> ➢ **New**

1. Click **[Exception] > [Appended Log] > [New]**:
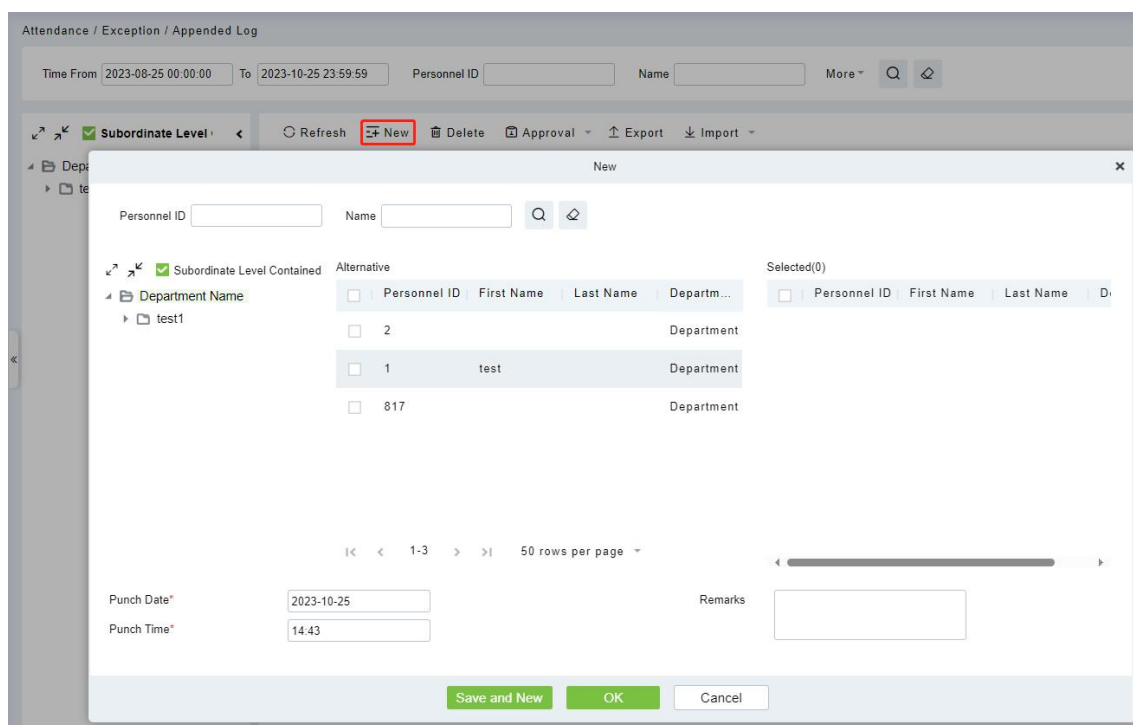
Fields are as follows:

• **Personnel:** Select the required personnel for an appended receipt, multiple choices are available.

• **Punch Data/Time:** Set the date and time of punch.

• **Remarks:** Enter the reason for an appended receipt, the max length is 50.
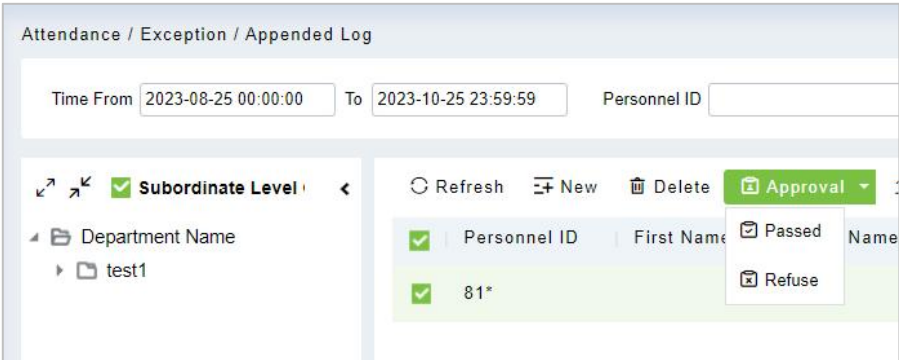
2. After filling the information, click **[OK]** to save and exit, the appended receipt will be displayed in the added list.

> ➤ **Delete**

1. Click **[Exception] > [Appended Log] > [Delete]**:

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

> ➤ **Approval**

1. Click **[Exception]** > **[Appended Log]**, select a personnel information and click **[Approval]**.

2. Click [Passed] or [Refuse].

> ➤ **Export**

You can export selected appended receipt data in Excel, PDF, and CSV file format.

				ZKTECO Appended Receipt			
Personnel ID	First Name	Last Name	Department Number	Department Name	Punch Time	Remark	Operation Time
1	Jerry	Wang	1	General	2017-12-15 08:40:00		2017-12-15 16:40:51
2	Lucky	Tan	3	Development Department	2017-12-15 08:40:00		2017-12-15 16:40:51
2940	Sherry	Yang	hotel	Hotel	2017-12-15 08:40:00		2017-12-15 16:40:51
3	Leo	Hou	4	Financial Department	2017-12-15 08:40:00		2017-12-15 16:40:51
4	Berry	Cao	1	General	2017-12-15 08:40:00		2017-12-15 16:40:51
5	Necol	Ye	2	Marketing Department	2017-12-15 09:50:00		2017-12-15 16:51:00
6	Amber	Lin	4	Financial Department	2017-12-15 09:50:00		2017-12-15 16:51:00
7	Jacky	Xiang	1	General	2017-12-15 09:50:00		2017-12-15 16:51:00

5.4.2 Leave

Personnel may need to leave at different circumstances. They can apply and the leave will be displayed here:

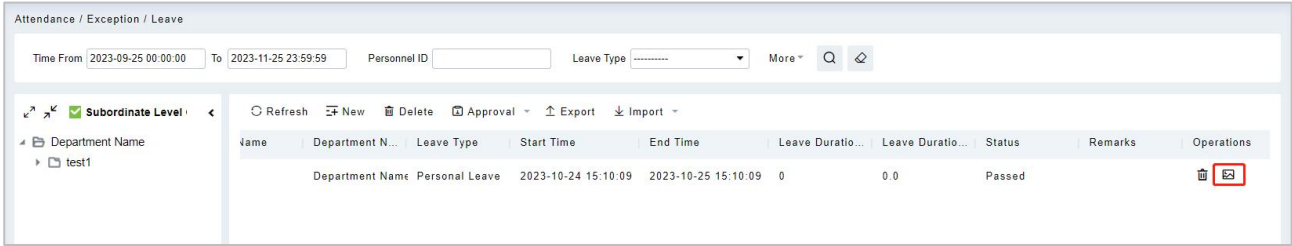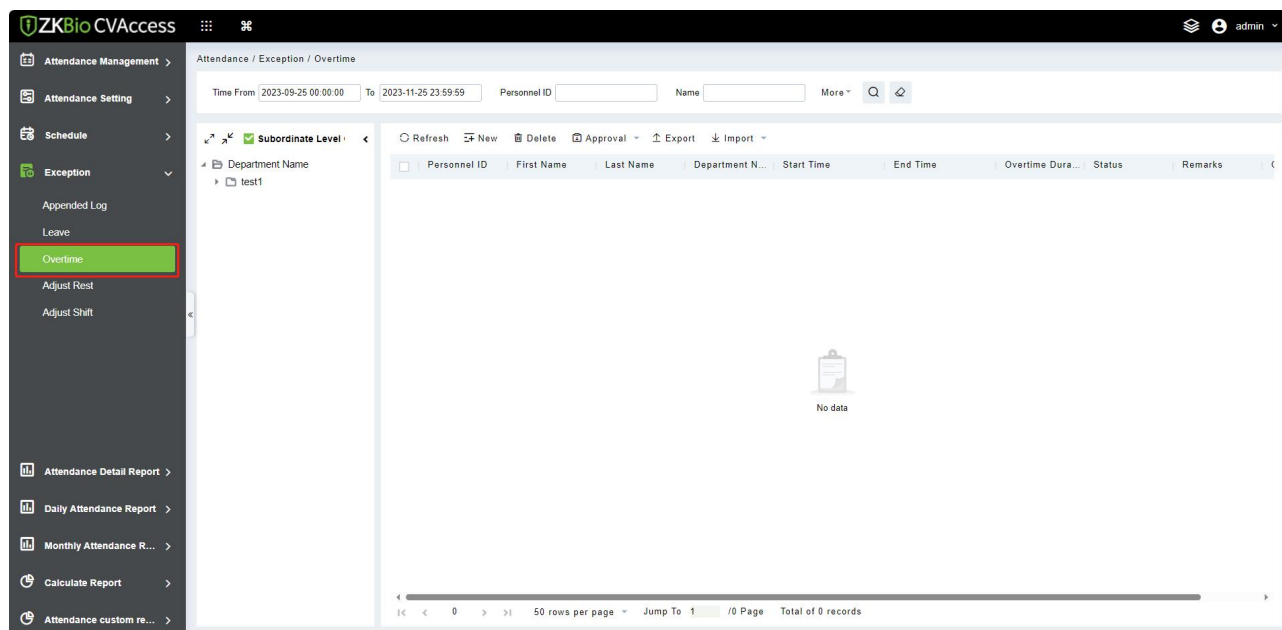Click **[Attendance] > [Exception] > [Leave]**.

> ➤ **New**
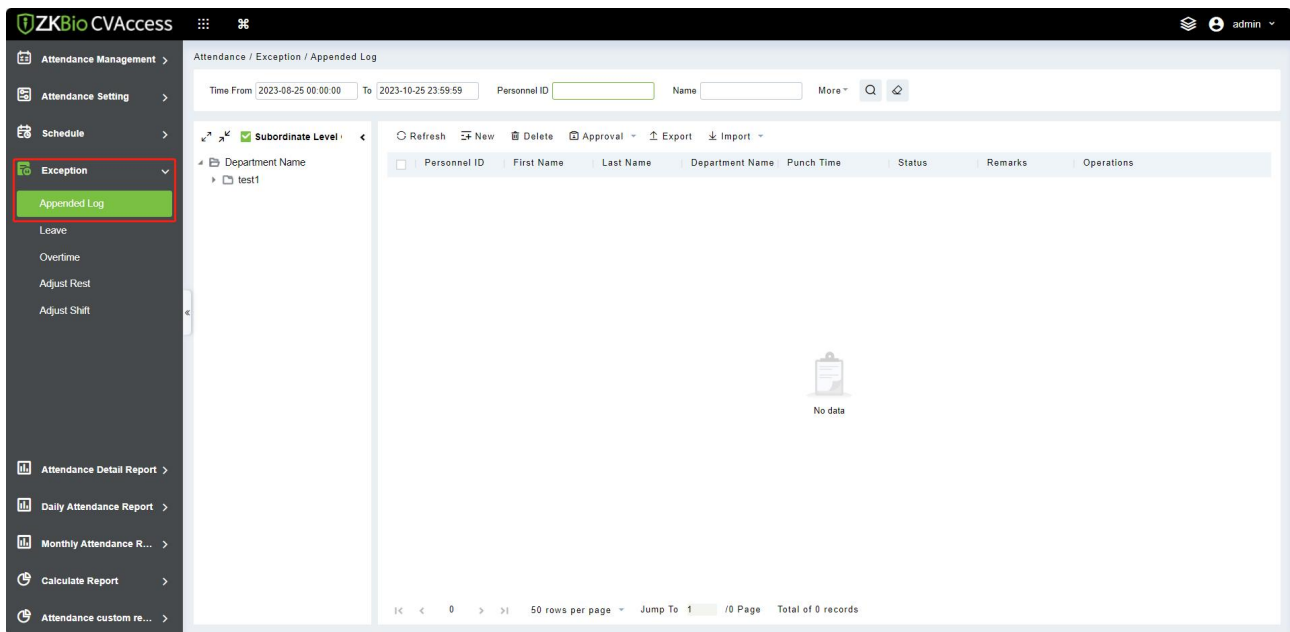
1. Click **[Exception] > [Leave] > [New]**:
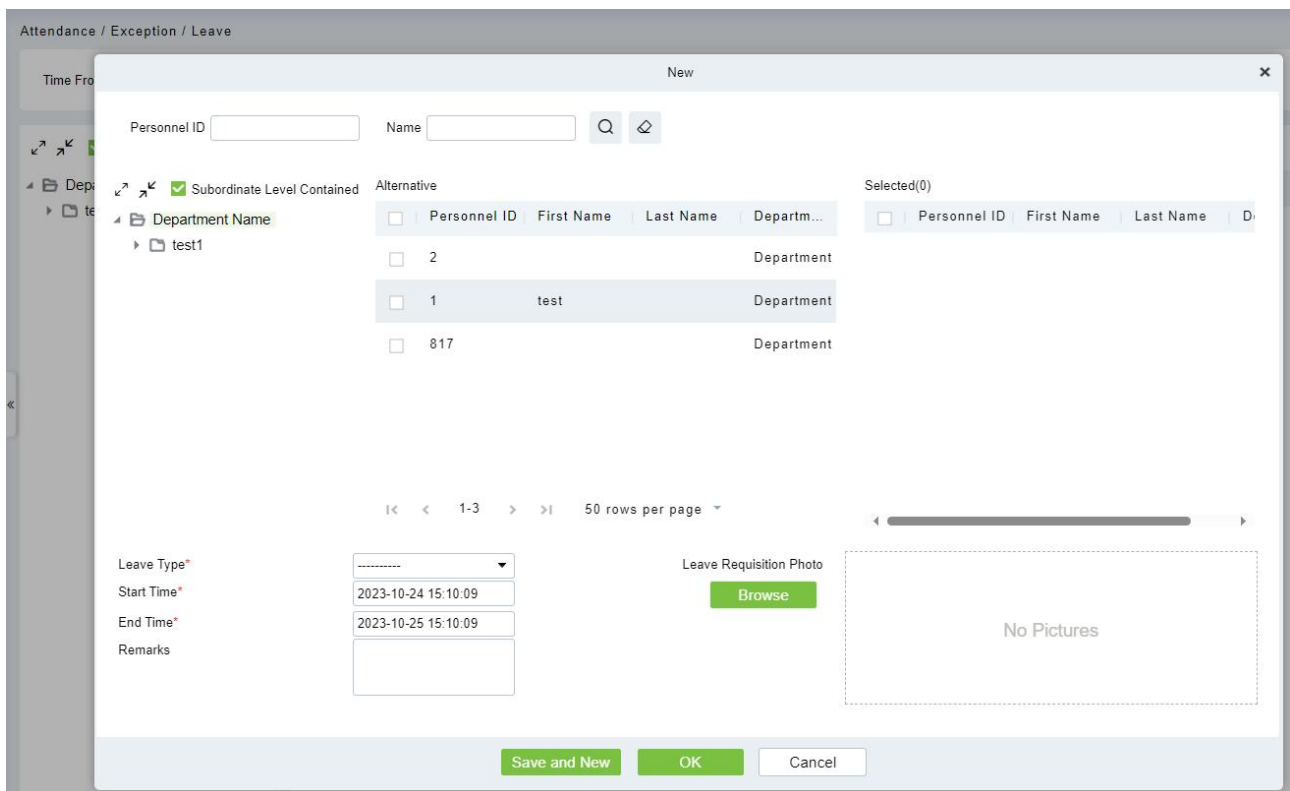
Fields are as follows:

- **Personnel:** Select the required personnel, multiple choice is available.

- **Leave Type:** Set the type of leave.

- **Start Time:** Start time of the leave.

- **End Time:** End time of the leave.

- **Remarks:** Enter the reason for leave, the max length is 50.

- **Leave Requisition Photo:** Upload photo of supporting document for the leave request.

2. After filling the information, click **[OK]** to save and exit, the leave information will be displayed in the added list. Click ![icon] button at the end of each line to view the leave requisition photo.

➢ **Delete**

1. Click **[Exception]** > **[Leave]**, select a personnel information and click **[Delete]**.

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

➢ **Approval**

1. Click **[Exception]** > **[Leave]**, select a personnel information and click **[Approval]**.

2. Click **[Passed]** or **[Refuse]**.
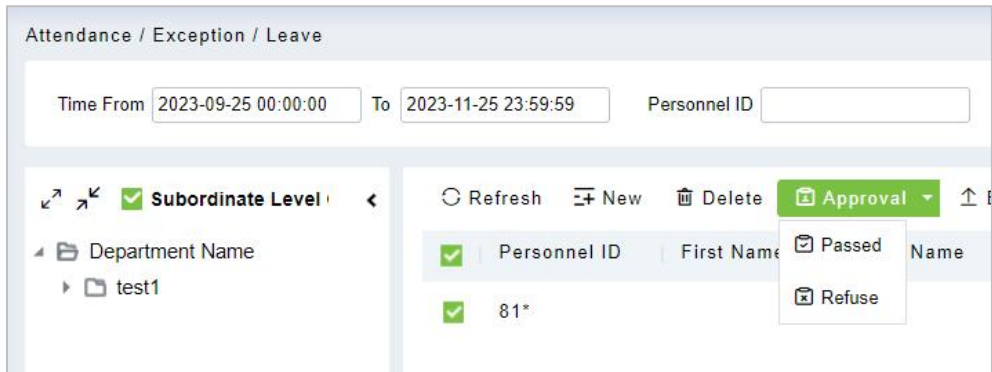
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

ZKTECO
Leave

Personnel ID	First Name	Last Name	Department Number	Department Name	Leave Type	Start Time	End Time	Remark	Operation Time
1	Jerry	Wang	1	General	Casual Leave	2017-12-15 16:36:07	2017-12-15 16:36:07		2017-12-15 16:36:17
3	Leo	Hou	4	Financial Department	Marriage Leave	2017-12-15 18:38:48	2017-12-15 18:38:48		2017-12-15 18:38:53
5	Necol	Ye	2	Marketing Department	Annual Leave	2017-12-15 16:36:19	2017-12-15 16:36:19		2017-12-15 16:36:27
6	Amber	Lin	4	Financial Department	Sick Leave	2017-12-15 18:38:54	2017-12-15 18:38:54		2017-12-15 18:39:00
9	Lilian	Mei	3	Development Department	Breastfeeding Leave	2017-12-15 18:39:02	2017-12-15 18:39:02		2017-12-15 18:39:10

5.4.3 Overtime

Click **[Attendance]** > **[Exception]** > **[Overtime]**.

➢ **New**

1.   Click **[Exception] > [Overtime] > [New]**:
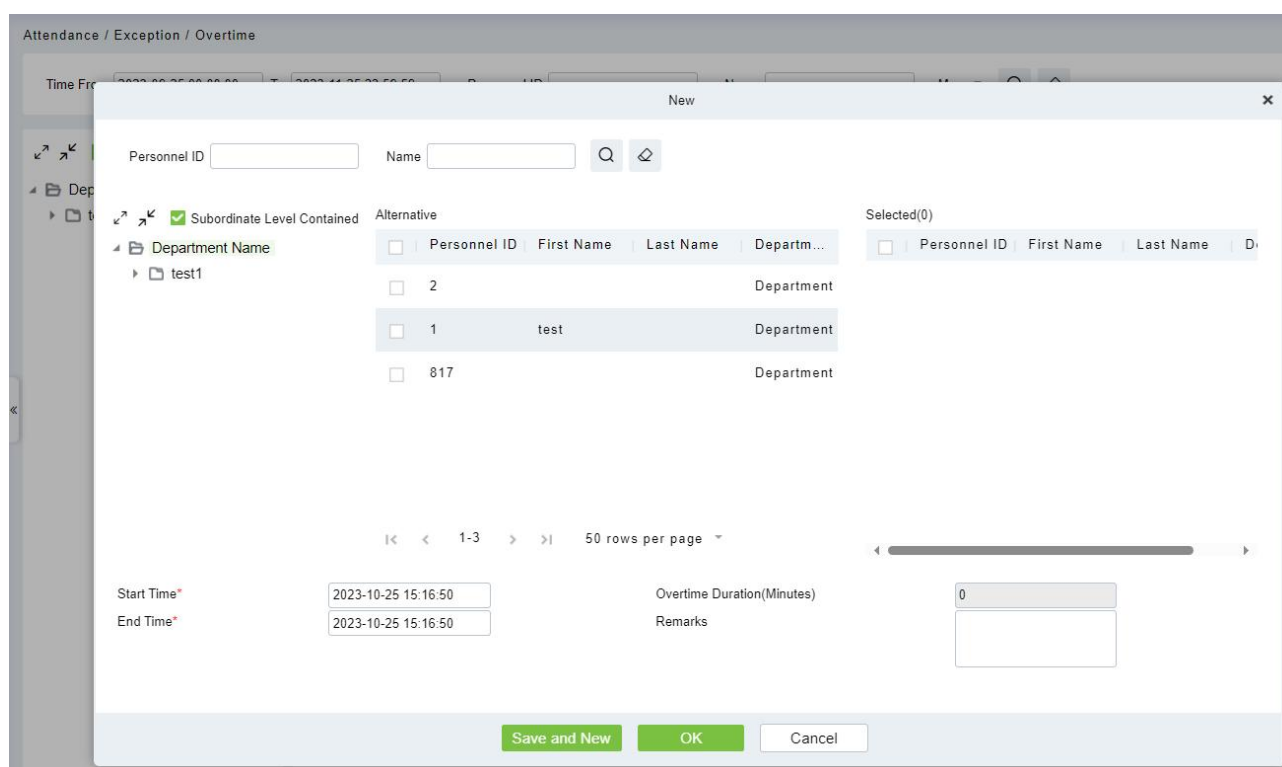
Fields are as follows:

•   **Personnel:** Select the required personnel for overtime, multiple choices are available.

•   **Start Time:** Start time of overtime.

•   **End Time:** End time of overtime.

•   **Overtime Duration:** It is automatically calculated based on the start/end time and cannot exceed one day.

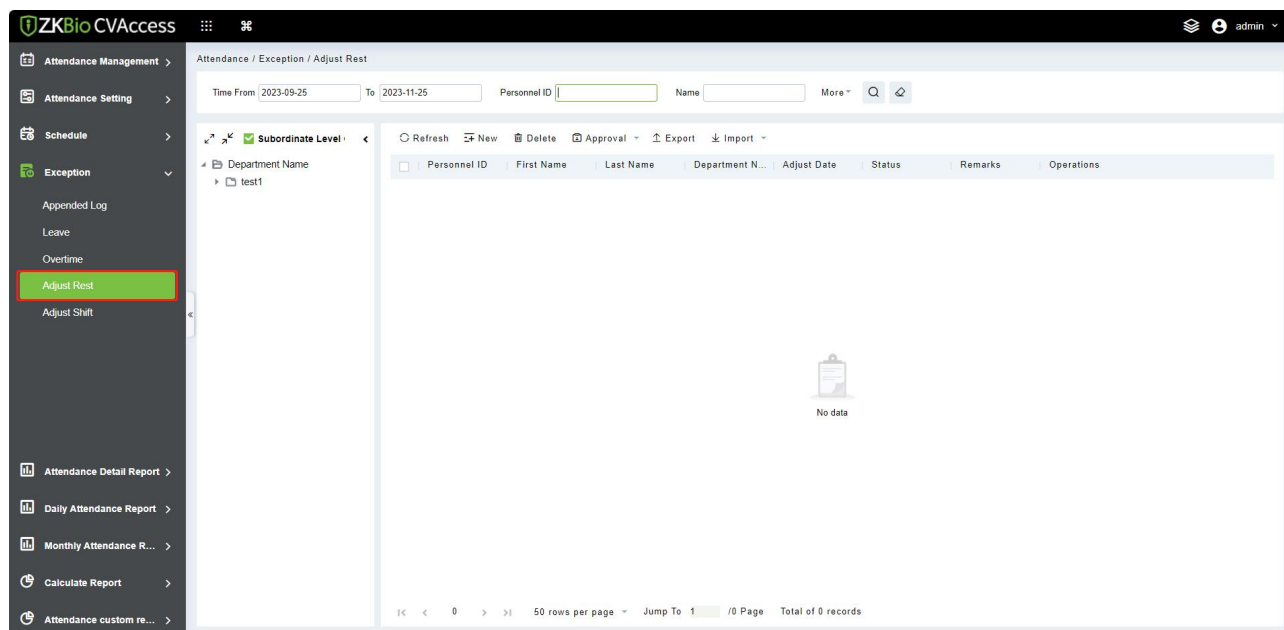•   **Remarks:** Enter the description of overtime, the max length is 50.

2.   After filling the information, click **[OK]** to save and exit, the overtime information will be displayed in the added list.

➢   **Delete**

1.   Click **[Exception]** > **[Overtime]**, select an personnel information and click **[Delete]**.

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

➢   **Approval**

1.   Click **[Exception]** > **[Overtime]**, select a personnel information and click **[Approval]**.

2.   Click **[Passed]** or **[Refuse]**.
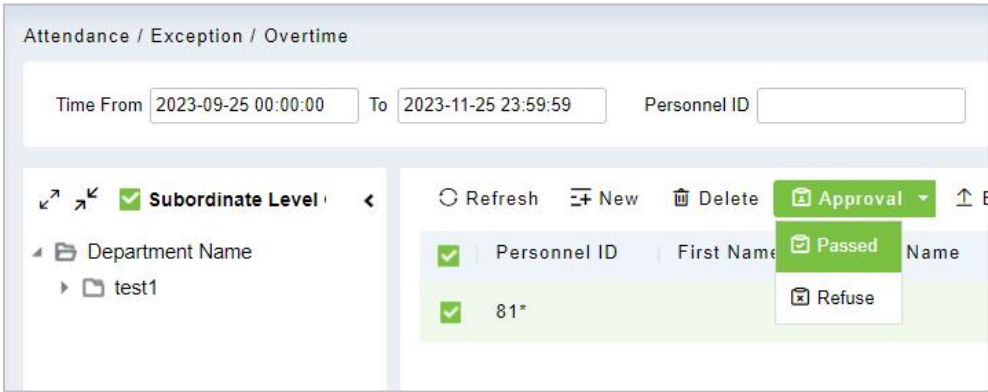
➢   **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

ZKTECO									
Overtime									
Personnel ID	First Name	Last Name	Department Number	Department Name	OT Type	Start Time	End Time	Remark	Operation Time
3	Leo	Hou	4	Financial Department	Normal OT	2017-12-15 16:37: 34	2017-12-15 16:37: 34		2017-12-15 16:37: 37
5	Necol	Ye	2	Marketing Department	Normal OT	2017-12-18 11:44: 03	2017-12-18 11:44: 03	Finish Project	2017-12-18 11:44: 28

5.4.4 Adjust Rest

Click **[Attendance]** > **[Exception]** > **[Adjust Rest]**.

> ➢ **New**

1. Click **[Exception] > [Adjust Rest] > [New]**:
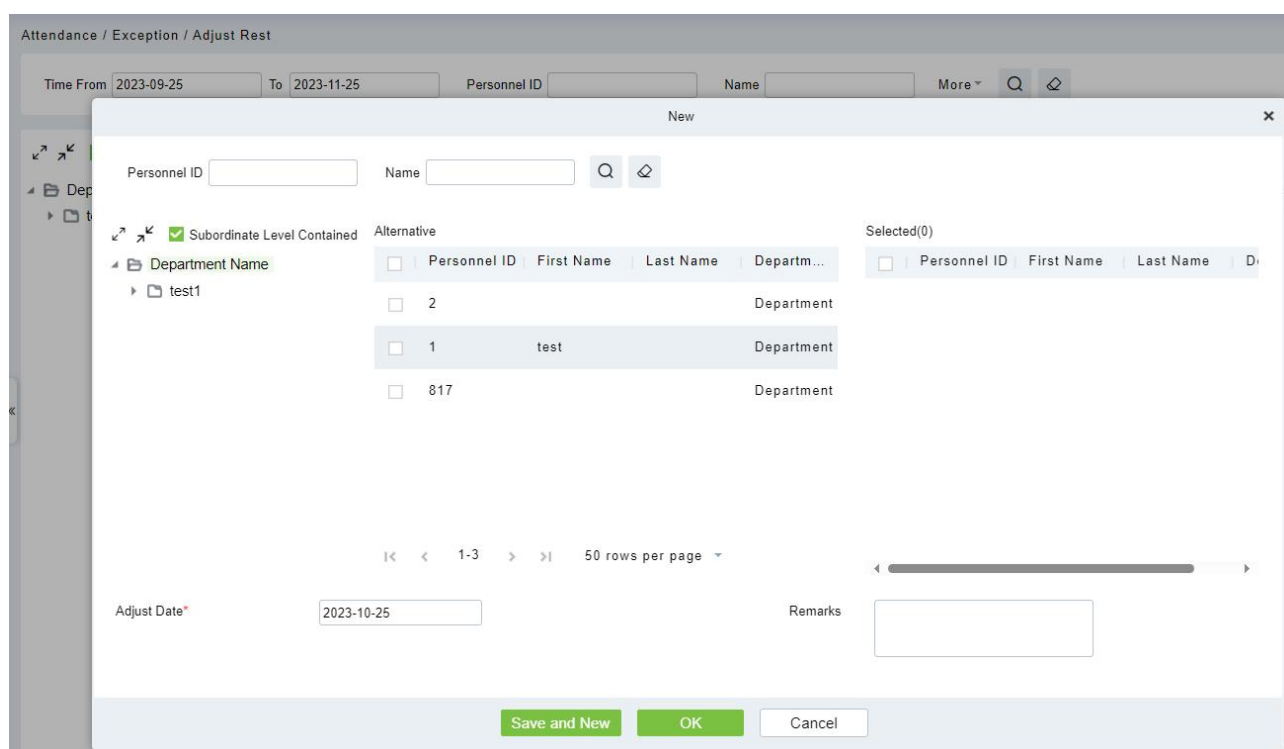
Fields are as follows:

•   **Adjust Date:** The date and time of adjustment.

•   **Remarks:** Enter the reason to adjusting and append the max length is 50.

2. After filling the information, click **[OK]** to save and exit, the adjust and append information will be displayed in the added list.

> ➢ **Delete**

1. Click **[Exception]** > **[Adjust Rest]**, select a personnel information and click **[Delete]**.

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

➢   **Approval**

1. Click **[Exception]** > **[Adjust Rest]**, select a personnel information and click **[Approval]**.

2. Click **[Passed]** or **[Refuse]**.

➢   **Export**

You can export selected leave data in Excel, PDF, and CSV file format.
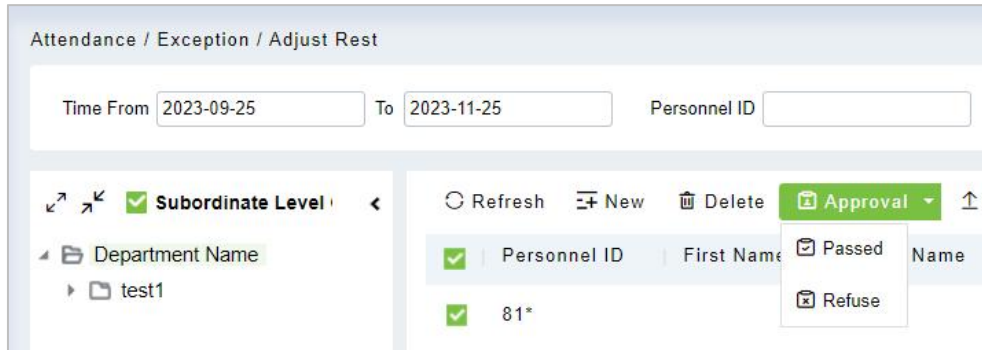
Personnel ID	First Name	Last Name	Department Number	Department Name	Adjust Type	Adjust Date	Schedule Name	Remark	Operation Time
				ZKTECO					
				Adjust and Append					
1	Jerry	Wang	1	General	Append Attendance	2017-12-18	Day Shift	123	2017-12-18 13:54:54
2	Lucky	Tan	3	Development Department	Append Attendance	2017-12-18	Flexible	456	2017-12-18 13:55:40
9	Lilian	Mei	3	Development Department	Adjust Rest	2017-12-18		adjust rest	2017-12-18 11:45:02

5.4.5 Adjust Shift

Click **[Attendance]** > **[Exception]** > **[Adjust Shift]**.
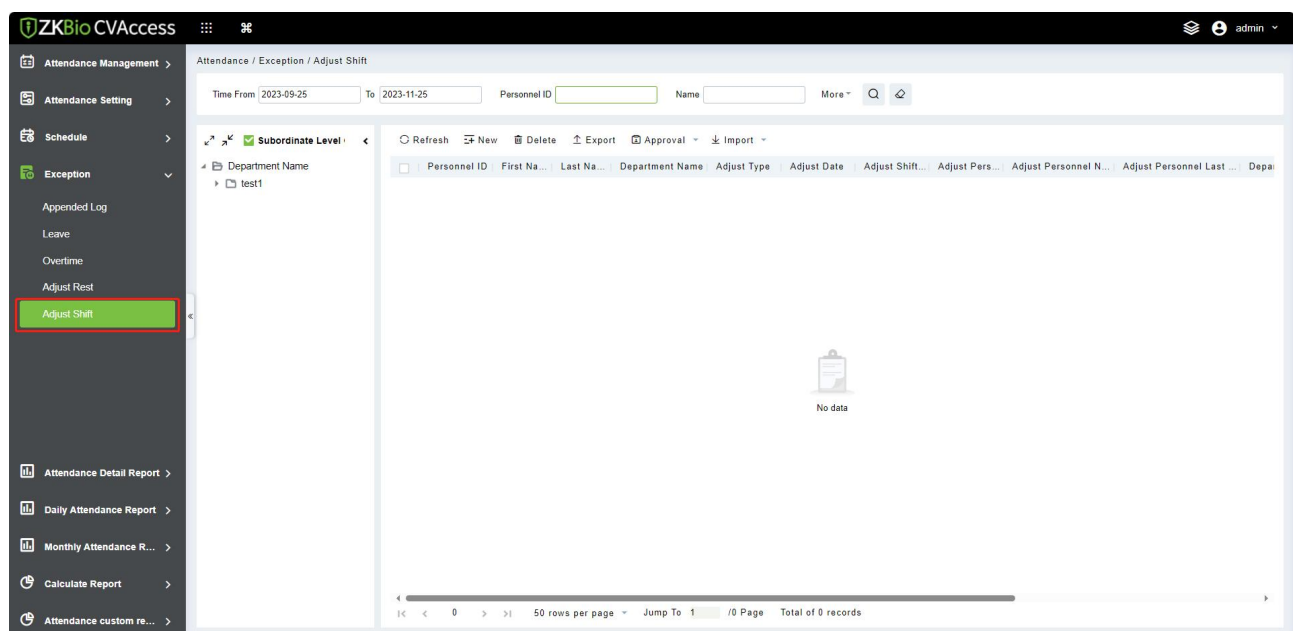
➢   **New**

1. Click **[Exception]** > **[Adjust Shift]** > **[New]**:

2. Adjust Type is divided into three shifts:

1) Adjust the personnel shift on the same day: It will adjust one personnel's shift on the same day.

- **Personnel ID:** The max length is 32. (Fill the correct ID. After you enter the ID and click on the next field, the Name and Department are automatically filled.)

- **First Name:** Obtained automatically based on Personnel ID.

- **Department Name:** Obtained automatically based on Personnel ID.

- **Adjust Date:** The date and time of adjustment.

- **Adjust Shift Name:** Choose an adjust shift.

- **Remarks:** Enter the description of adjusting shift, the max length is 50.

2) Adjust the personnel shift in other days: It will adjust one personnel's shift in different days.

- **Personnel ID:** The max length is 32. (Fill the correct ID. After you enter the ID and click on the next field, the Name and Department are automatically filled.)

- **First Name:** Obtained automatically based on Personnel ID.

- **Department Name:** Obtained automatically based on Personnel ID.

- **Adjust Date:** The date and time of adjustment.

- **Remarks:** Enter the description of adjusting shift, the max length is 50.

3) Two-people exchange: It will exchange shifts of two people on different days.

- **Personnel ID:** The max length is 32. (Fill the correct ID; after you enter the ID and click on the next field, the Name and Department are automatically filled.)

- **First Name:** Obtained automatically based on Personnel ID.

- **Department Name:** Obtained automatically based on Personnel ID.

- **Adjust Personnel ID:** ID number of the adjust personnel. The max length is 32. (Fill the correct ID; after you enter the ID and click on the next field, the Name and Department are automatically filled.)

- **Adjust Personnel Name:** Obtained automatically based on Personnel ID.

- **Adjust Department Name:** Obtained automatically based on Personnel ID.

- **Adjust Date:** The date and time of adjustment.

- **Remarks:** Enter the description of adjusting shift, the max length is 50.

3. After filling in the information, click **[OK]** to save and exit, the adjust shift information will be

displayed in the added list.

➢ **Approval**

1. Click **[Exception]** > **[Adjust Shift]**, select a personnel information and click **[Approval]**.

2. Click **[Passed]** or **[Refuse]**.
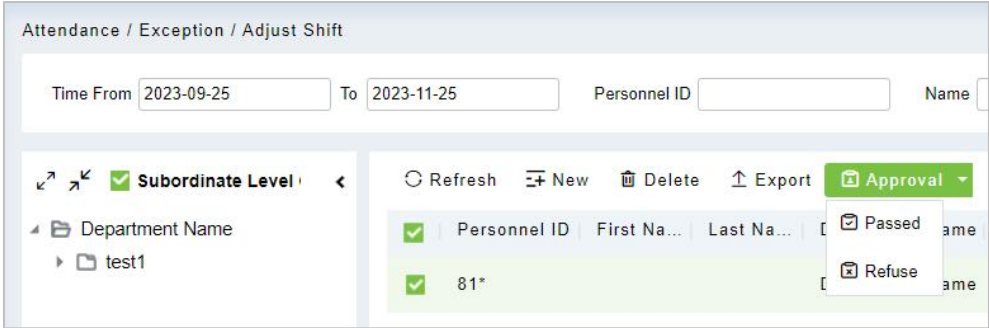
➢ **Export**

You can export selected adjust shift data in Excel, PDF, CSV file format.

							ZKTECO							
							Adjust Shift							
Personnel ID	First Name	Last Name	Department Number	Department Name	Adjust Type	Adjust Date	Personnel ID	Adjust Personnel Name	Adjust Personnel Last Name	Department Number	Department Name	Adjust Date	Remark	Operation Time
3	Leo	Hou	4	Financial Department	Adjust the personal shift in other days	2017-12-18						2017-12-18		2017-12-18 13:56:27
4	Berry	Cao	1	General	Adjust the personal shift in the same day	2017-12-18							Change to flexible	2017-12-18 14:00:27
5	Necol	Ye	2	Marketing Department	Two people exchange	2017-12-18	8	Glori	Liu	2	Marketing Department	2017-12-18	exchange	2017-12-18 14:02:21

5.5 Attendance Detail Report

5.5.1 Manual Calculation

In the Attendance Report, you can view the clock-in record of a person and check whether the attendance status of the person is correct through attendance calculation. If it is correct, it means that the attendance business configuration is completed.

Click **[Attendance]** > **[Attendance Detail Report]** > **[Manual Calculate]**.
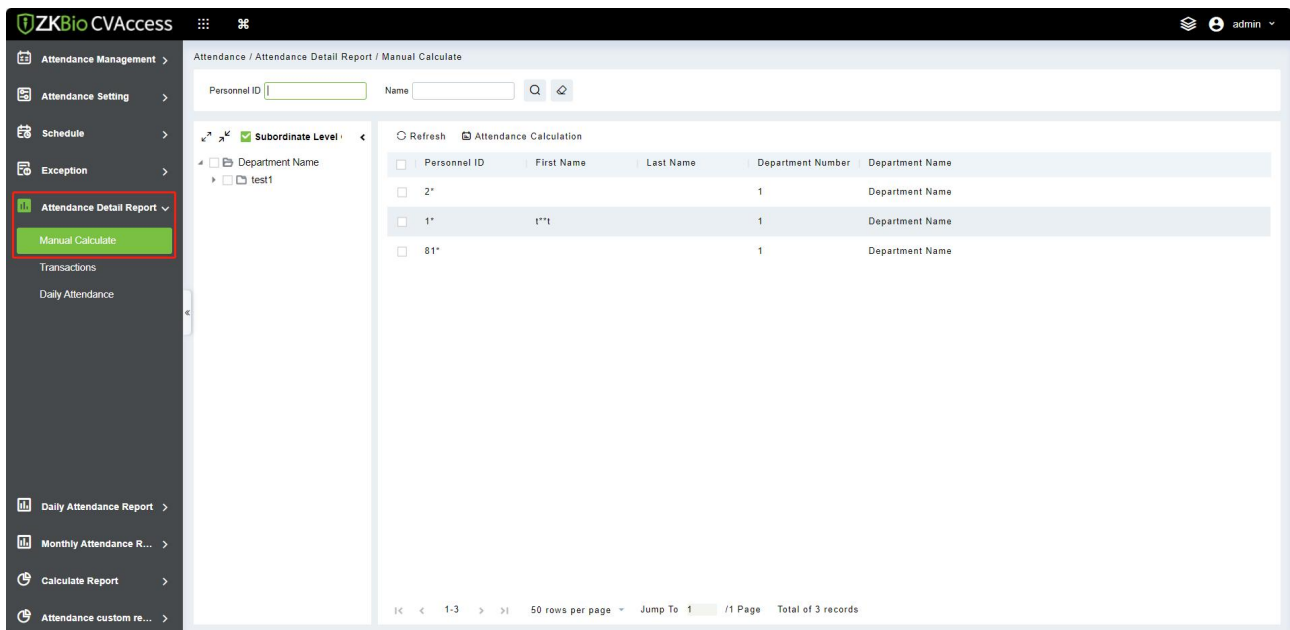
1. Check the person who needs to perform attendance calculation, and click **[Attendance Calculation]**.
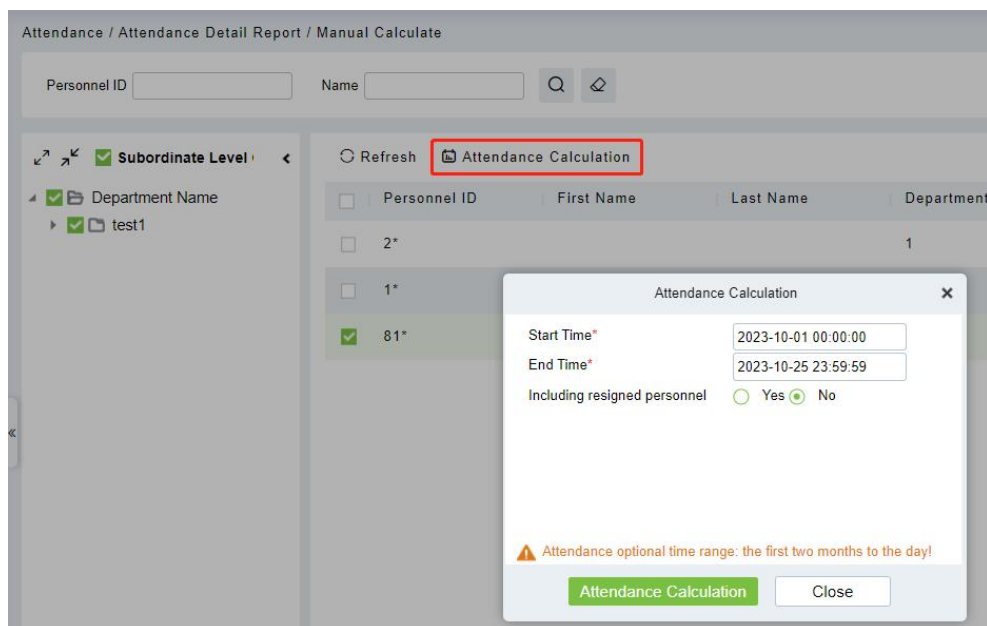
2. Configure the attendance calculation information, and click **[Attendance Calculation]**.
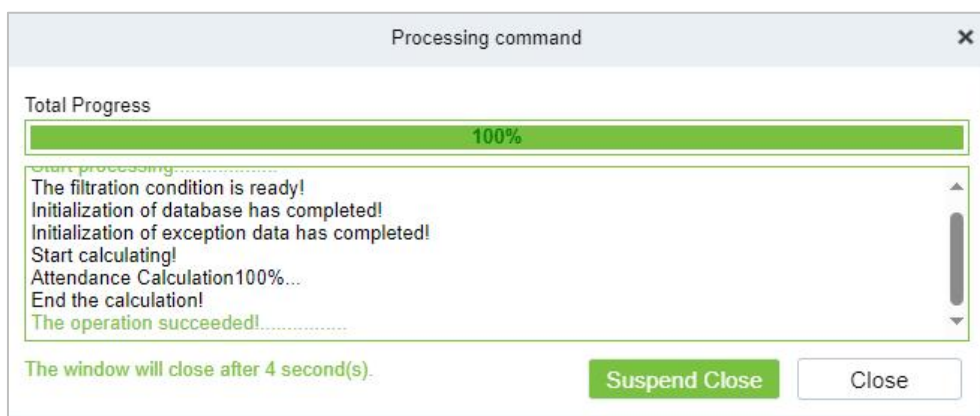
3. After the calculation is completed, you can view related reports.

5.5.2 Transaction

Attendance records of all employees will be displayed on this interface, including the attendance record of uploaded attendance transactions. The record of the normal punch on the device will be uploaded to the software as the original record. When a particular data is selected, the details will be displayed on the right side of the page.

Click **[Attendance] > [Attendance Detail Report] > [Transaction]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

➢ **Import U Disk Records**

The "Import U disk record" feature allows you to import the device data (including access control, parking, Facekiosk, Video records) to the transaction table.

➢ **Synchronize Attendance Records**

The access control records can be synchronized to attendance records through this function. Select the start time and end time to import, check the attendance point list and click **[OK]**.
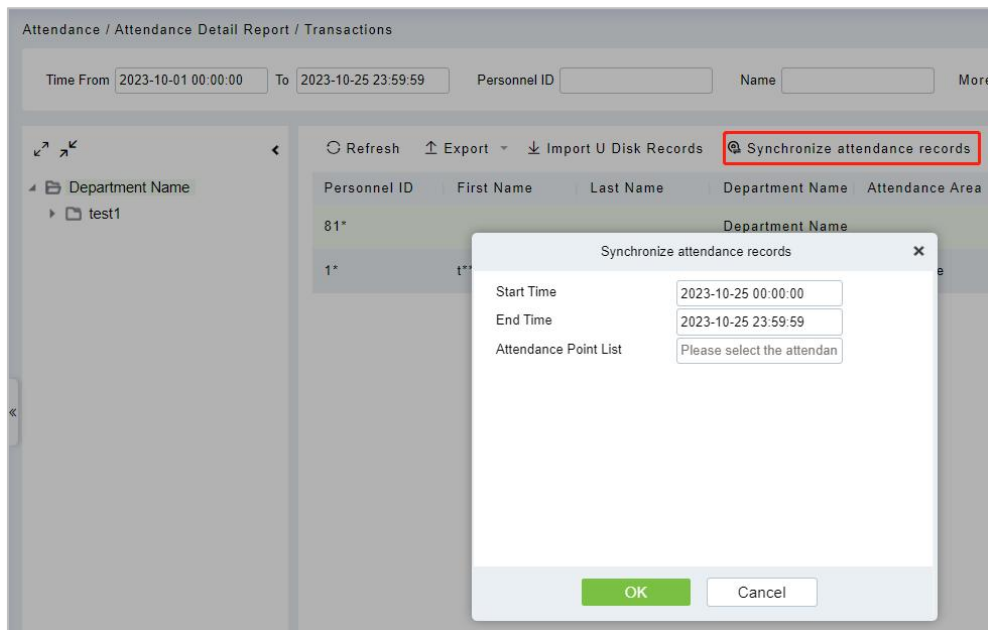
5.5.3 Daily Attendance

The table shows personnel's daily attendance status, punch time, the early leaving time, the latest time, the detailed punch time during the selected period.

Click **[Attendance] > [Attendance Detail Report] > [Daily Attendance]**.
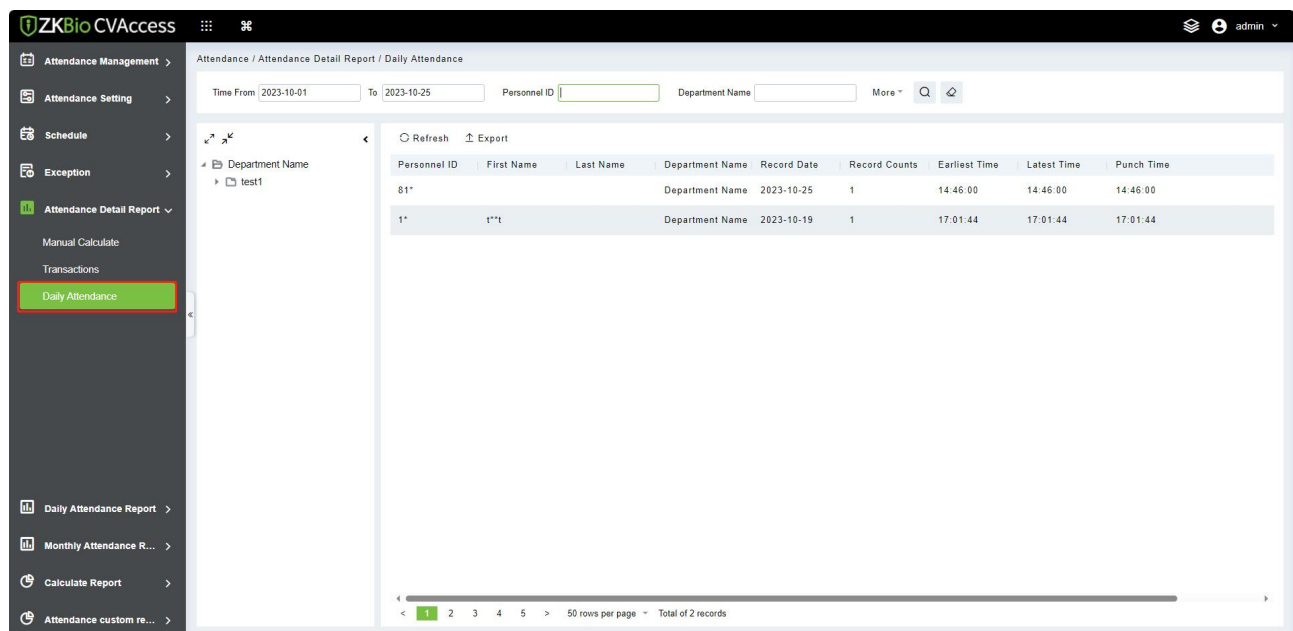
> ➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6 Daily Attendance Report

5.6.1 Daily Report

This function is used to get the daily report within the specified range of date and time attendance details of personnel, including attendance, late arrival, early leaving, overtime and so on.

Click **[Attendance]** > **[Daily Attendance Report]** > **[Daily Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.2 Work Time Report

This will be the total effective time of this shift. It is automatically set by the system as per the Check-in/out details.

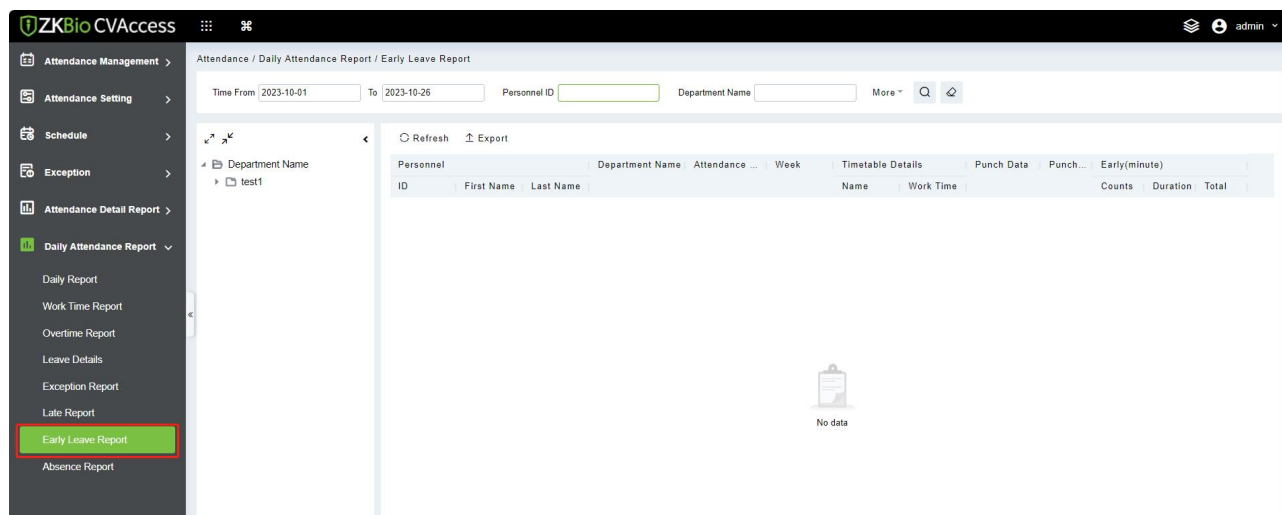Click **[Attendance]** > **[Daily Attendance Report]** > **[Work Time Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.3 Overtime Report

This function is used to get the overtime report within the specified range of date and time attendance details of personnel.

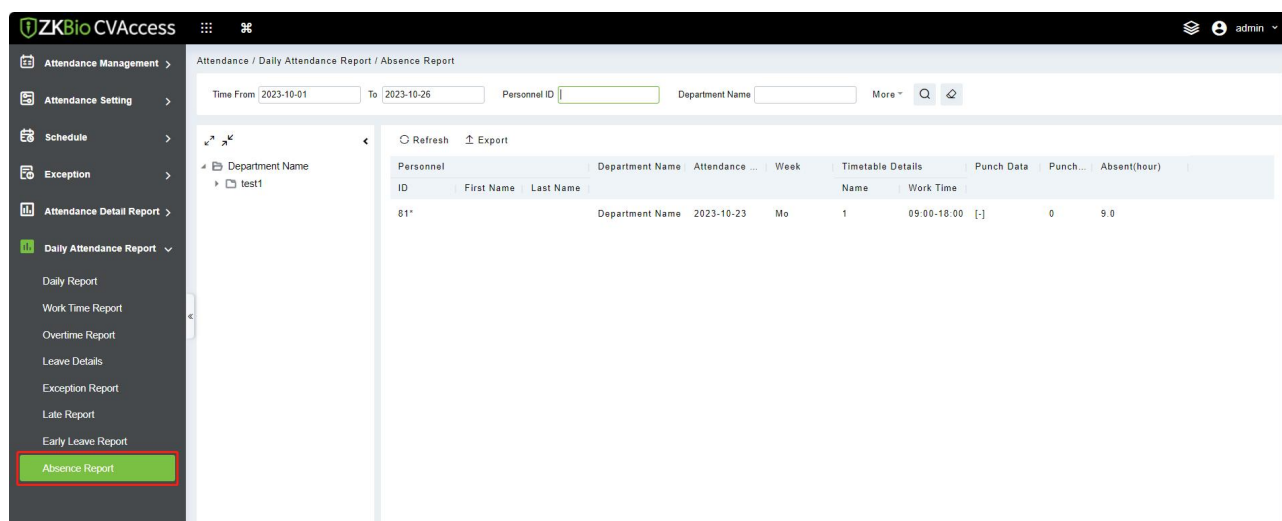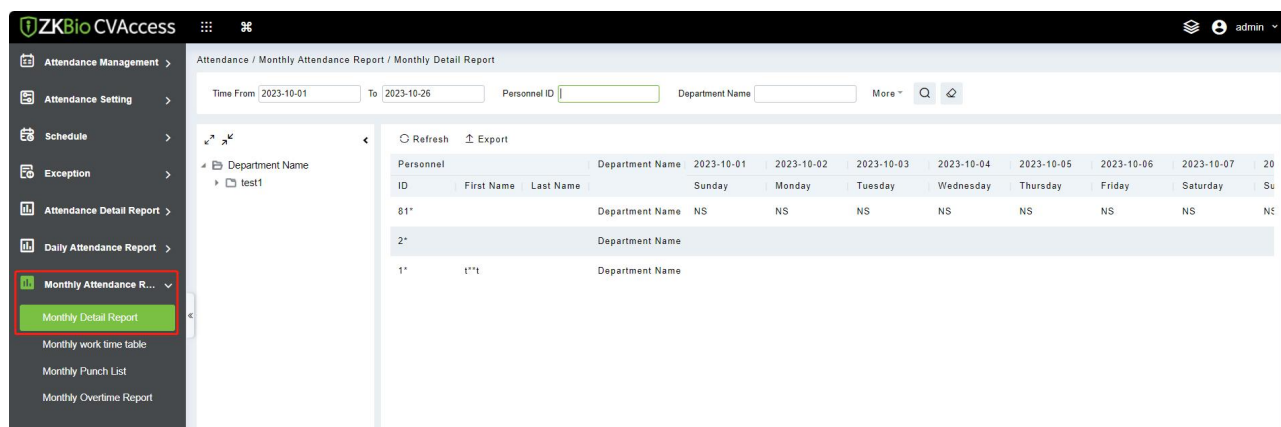Click **[Attendance] > [Daily Attendance Report] > [Overtime Report]**.
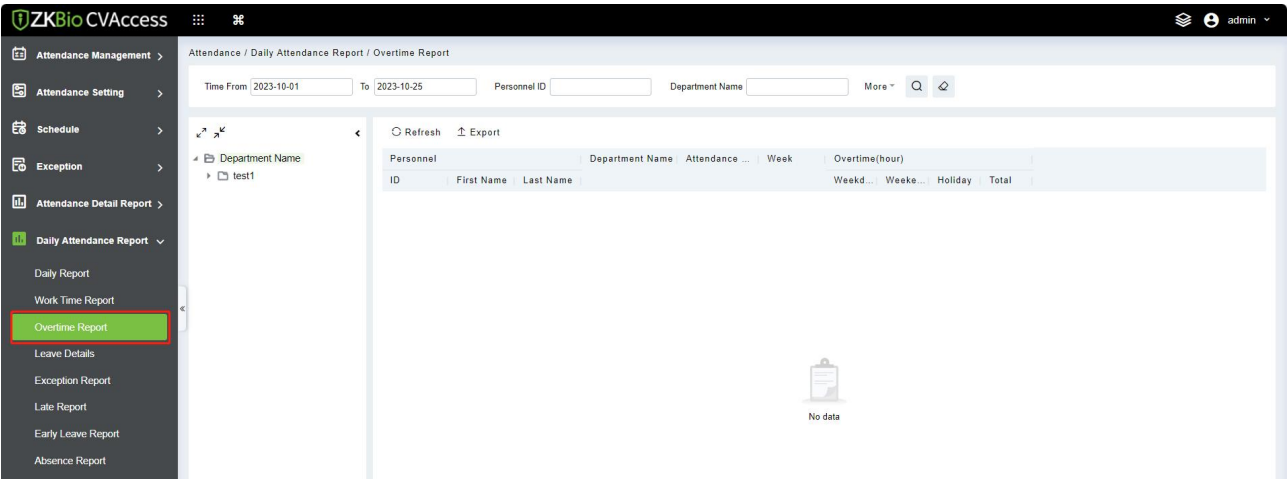
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.4 Leave Details

Personnel may need leave at different circumstances. They can apply and the leave will be displayed here.

Click **[Attendance] > [Daily Attendance Report] > [Leave Details]**.
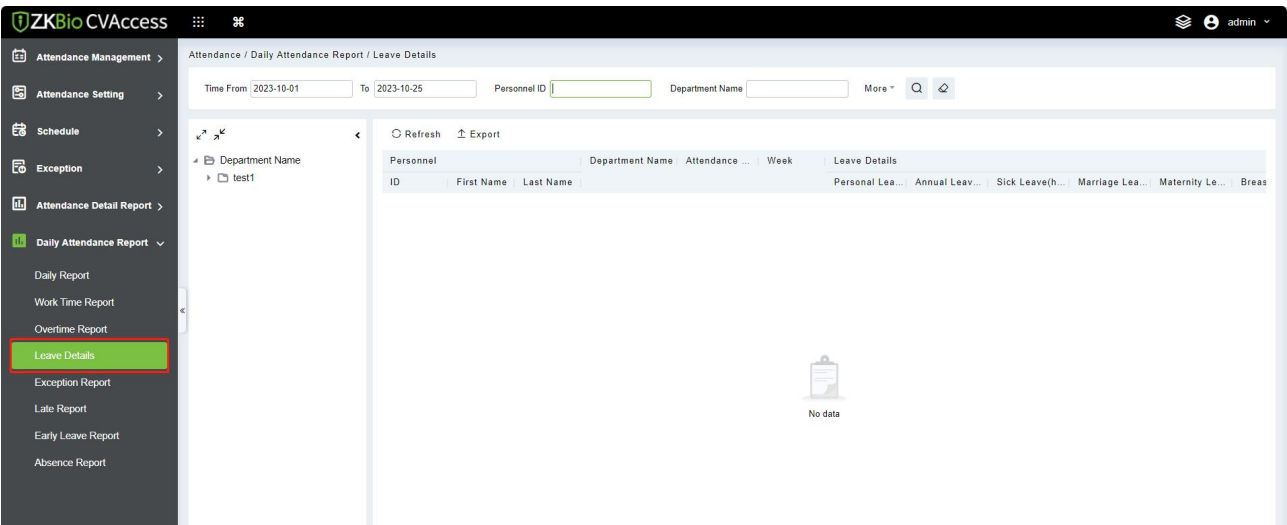
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.5 Exception Report

This function is used to get the exception report within the specified range of date and time attendance details of personnel.

Click **[Attendance] > [Daily Attendance Report] > [Exception Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.6 Late Report

This function is used to get the late report within the specified range of date and time attendance details of personnel.

Click **[Attendance] > [Daily Attendance Report] > [Late Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.7 Early Leave Report

This function is used to get the early leave report within the specified range of date and time attendance details of personnel.

Click **[Attendance] > [Daily Attendance Report] > [Early Leave Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.6.8 Absence Report

This function is used to get the absence report within the specified range of date and time attendance details of personnel.

Click **[Attendance] > [Daily Attendance Report] > [Absence Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.7 Monthly Attendance Report

5.7.1 Monthly Detail Report

This function will automatically give the report for a selected month on a daily basis. The report includes attendance status and characters, and summarizes the actual attendance time, absence, leave, business trips and outings in the month.

Click **[Attendance] > [Monthly Attendance Report] > [Monthly Detail Report]**.

The attendance status is displayed as per following priority at the bottom of the interface.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.7.2 Monthly Work Time Table

This function will automatically give the report for a selected month on a daily work time.

Click **[Attendance] > [Monthly Attendance Report] > [Monthly work time table]**.
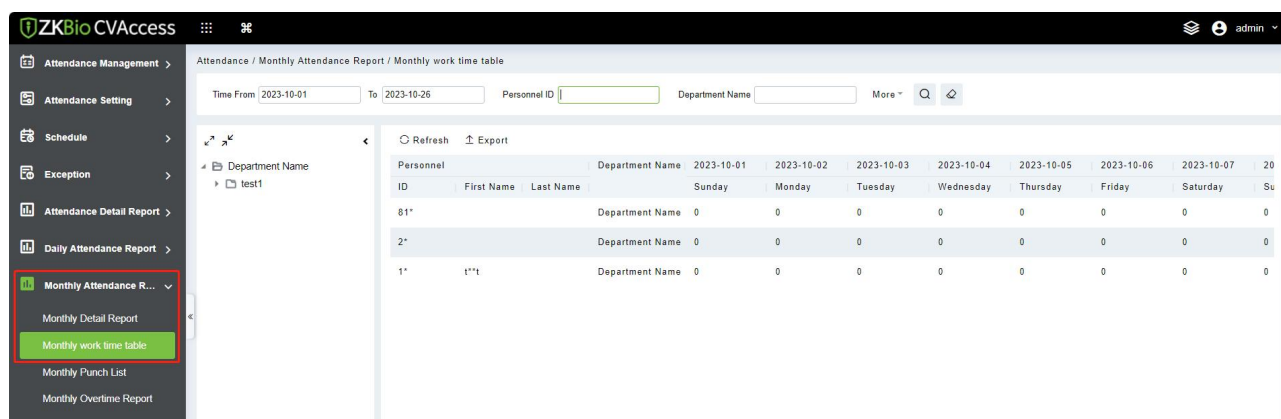
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.7.3 Monthly Punch List

This function will automatically give the report for a selected month on daily punch list.

Click **[Attendance] > [Monthly Attendance Report] > [Monthly Punch List]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.7.4 Monthly Overtime Report

This function will automatically give the report for a selected month on daily overtime.

Click **[Attendance] > [Monthly Attendance Report] > [Monthly Overtime Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8 <u>Calculate Report</u>

5.8.1 Monthly Staff Report

This function will give details for a selected month. The details include personnel attendance summary status and detailed information, including attendance, late, leaving early, etc.

Click **[Attendance]** > **[Calculate Report]** > **[Monthly Staff Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8.2 Employee Overtime Summary

This function is used to get the overtime summary report within the specified range of date and time attendance details of personnel.

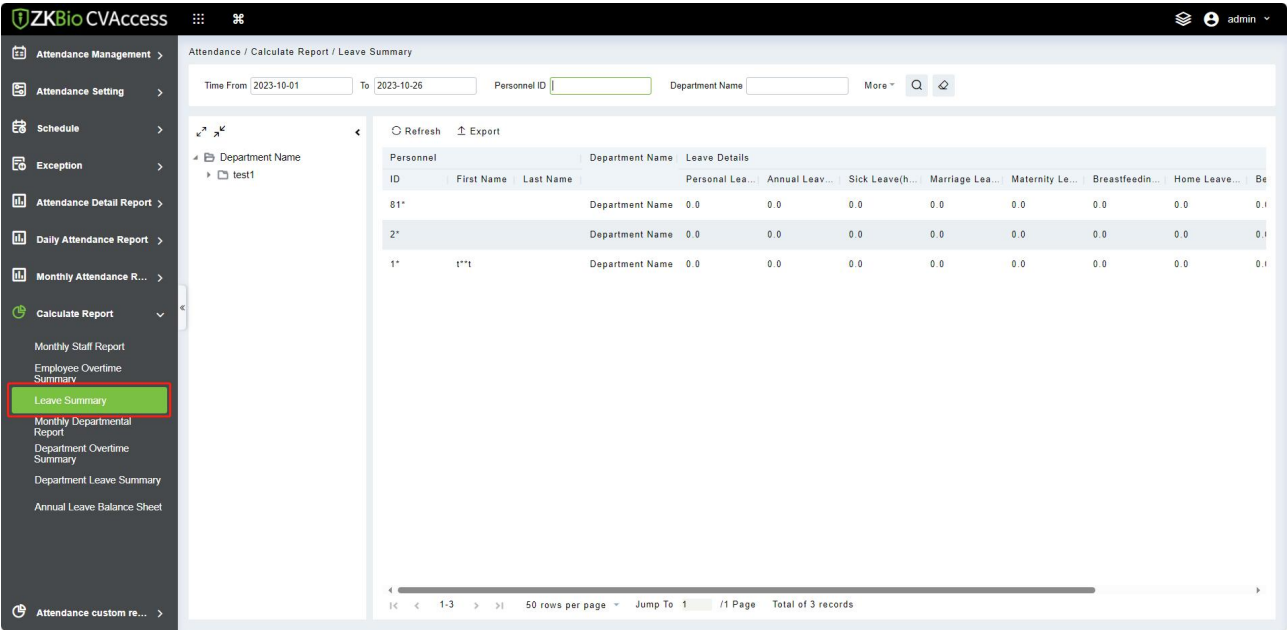Click **[Attendance]** > **[Calculate Report]** > **[Employee Overtime Summary]**.
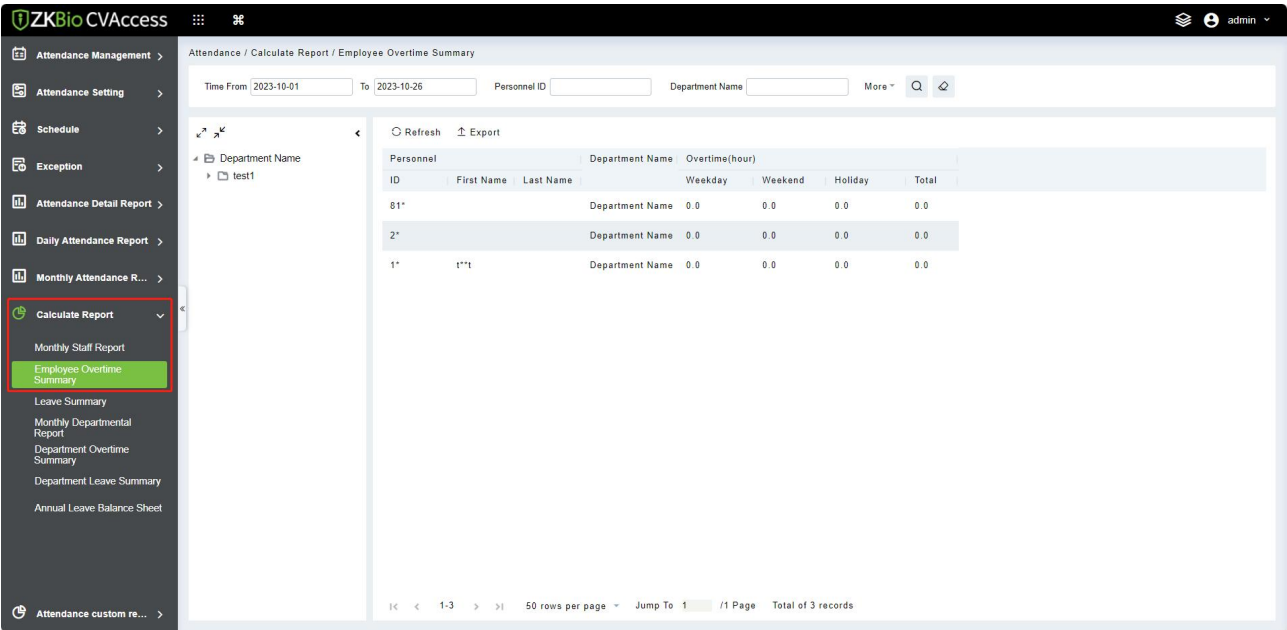
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8.3 Leave Summary

The report summarizes the valid time for all valid leave records, leave type, within the selected date range. Select the time range from which you want to view the leave record.

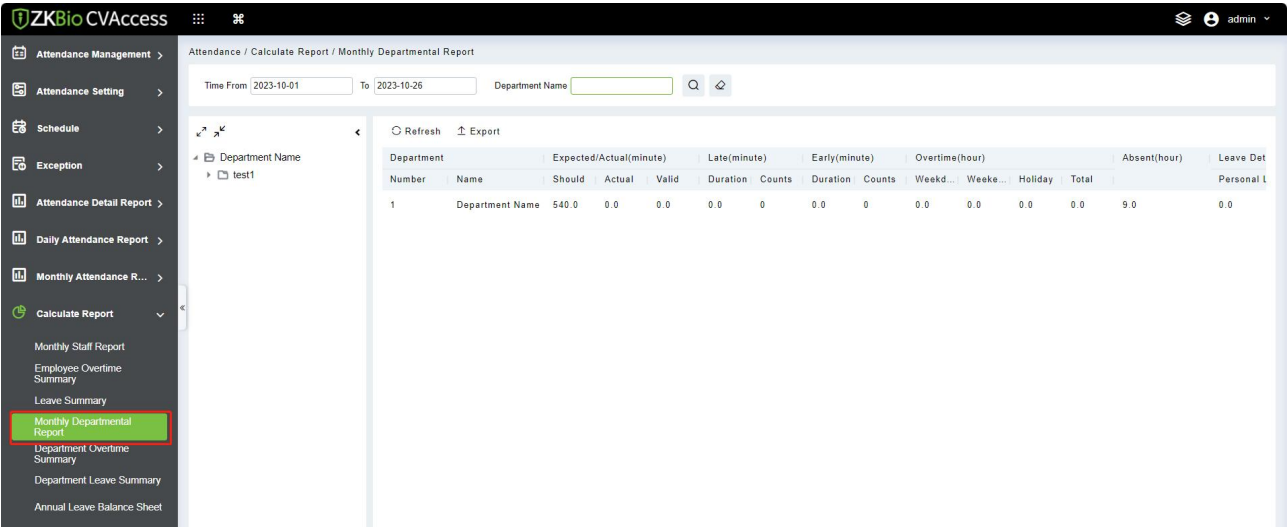Click **[Attendance] > [Calculate Report] > [Leave Summary]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

ZKTECO
Leave Summary

Personnel ID	First Name	Last Name	Department Number	Department Name	Leave Type Statistics
1	Jerry	Wang	1	General	Casual Leave(1) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(0) Bereavement Leave(0) Breastfeeding Leave(0) Custom (0)
5	Necol	Ye	2	Marketing Department	Casual Leave(0) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(1) Bereavement Leave(0) Breastfeeding Leave(0) Custom (0)
9	Lilian	Mei	3	Development Department	Casual Leave(0) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(0) Bereavement Leave(0) Breastfeeding Leave(1) Custom (0)
3	Leo	Hou	4	Financial Department	Casual Leave(0) Marriage Leave(1) Maternity Leave(0) Sick Leave(0) Annual Leave(0)

Created on: 2017-12-15 18:39:22

Created from ZKBioSecurity software. All rights reserved.   1/2

5.8.4 Monthly Departmental Report

This function is used to get the monthly detail record of all departments. Details include details of all personnel in the department, attendance, late, leaving early, and so on.

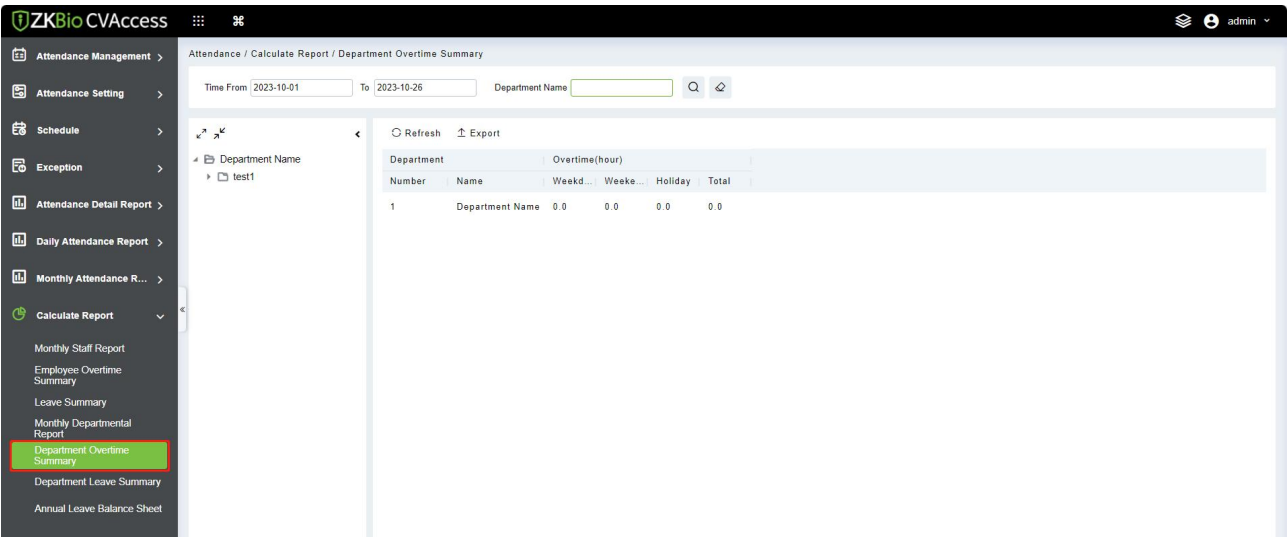Click **[Attendance] > [Calculate Report] > [Monthly Departmental Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8.5 Departmental Overtime Summary

This function is used to get the departmental overtime summary report within the specified range of date and time attendance details of personnel.

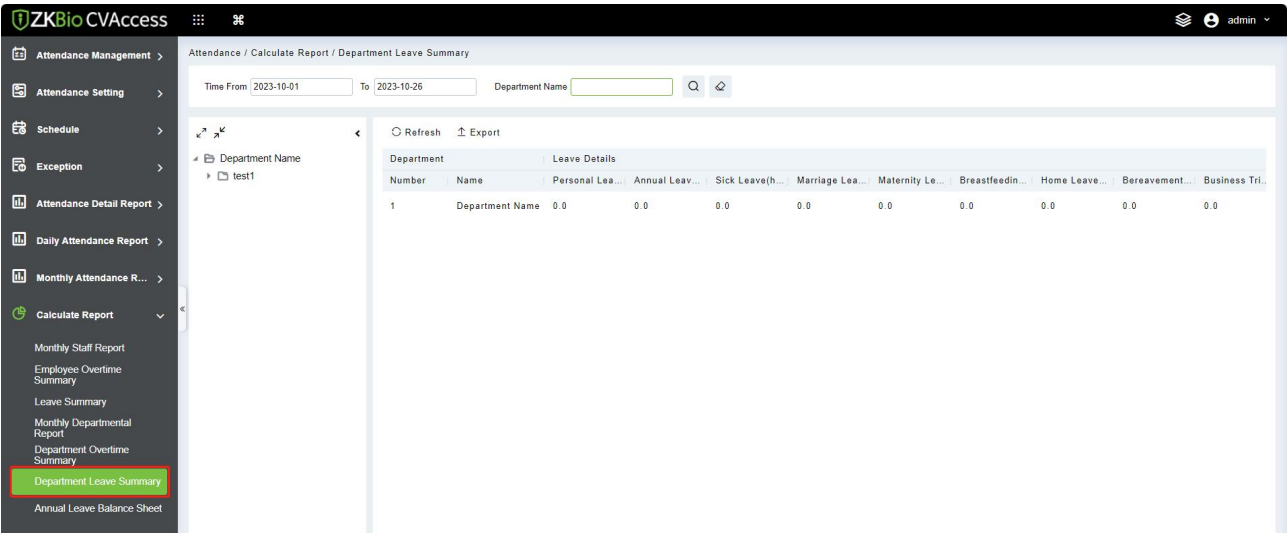Click **[Attendance] > [Calculate Report] > [Departmental Overtime Summary]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8.6 Departmental Leave Summary

This function is used to get the monthly detail record of all departments. Details include details of all personnel in the department, attendance, late, leaving early, and so on.

Click **[Attendance] > [Calculate Report] > [Monthly Departmental Report]**.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.8.7 Annual Leave Balance Sheet

This function is used to get the annual leave balance sheet of personnel.

Click **[Attendance] > [Calculate Report] > [Annual Leave Balance Sheet]**.
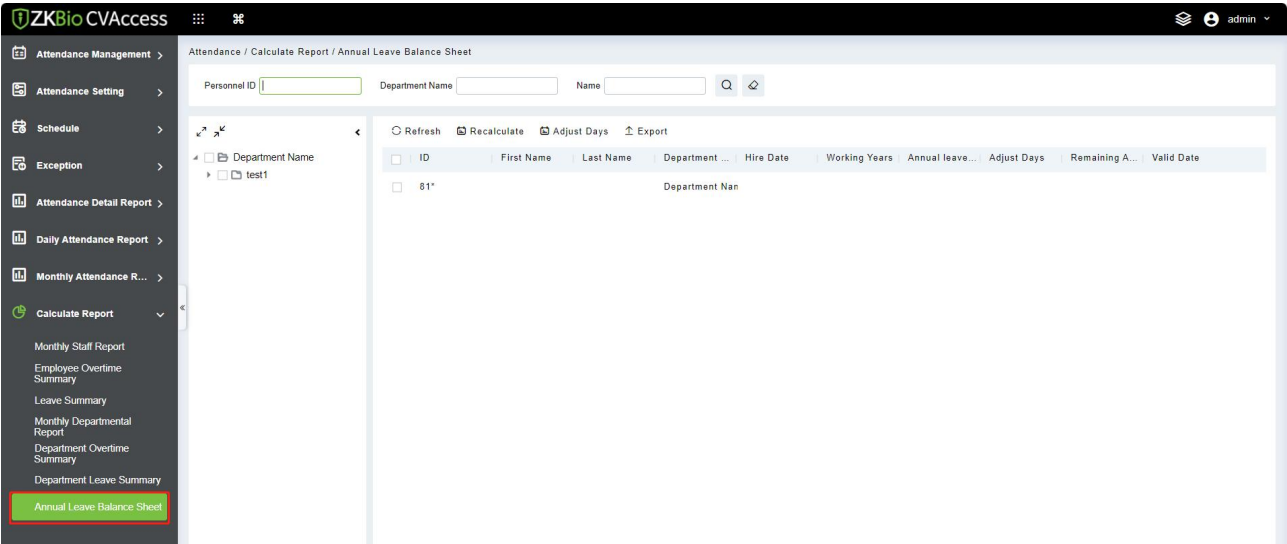
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

5.9 Attendance Custom Report

5.9.1 Attendance Custom Report

This function is used to get the custom attendance report, you can select the report content according to your needs.

Click **[Attendance] > [Attendance Custom Report] > [Attendance Custom Report]**.
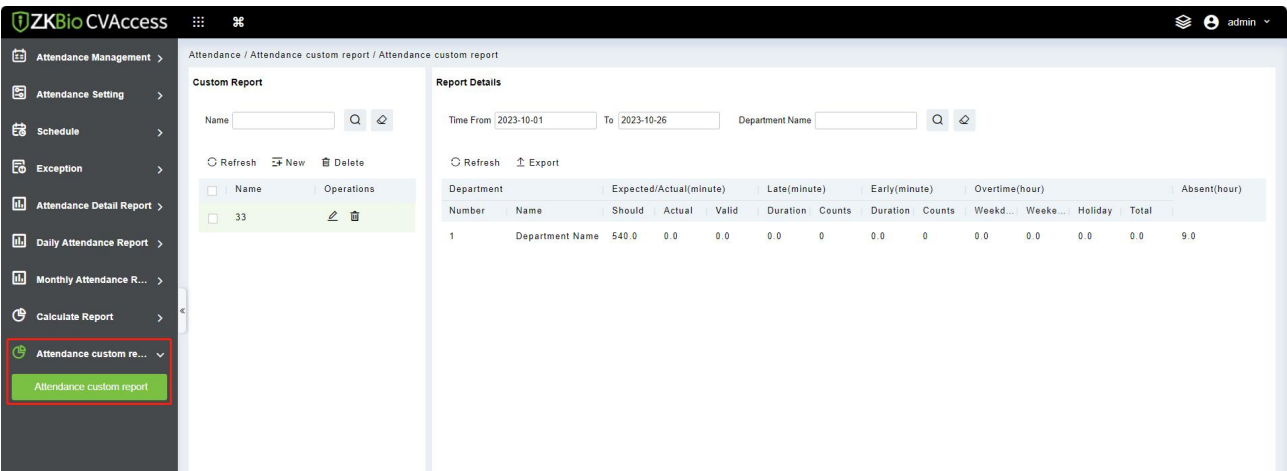
➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

6 Smart Video Surveillance

6.1 Device Management (New)

6.1.1 Device

This operation is used to instruct users how to connect NVR to the platform and cameras, so that the platform can manage the connected devices uniformly, such as viewing the live and video recordings of cameras.

Click **[Smart Video Surveillance]** > **[Device Management > [Device]**.
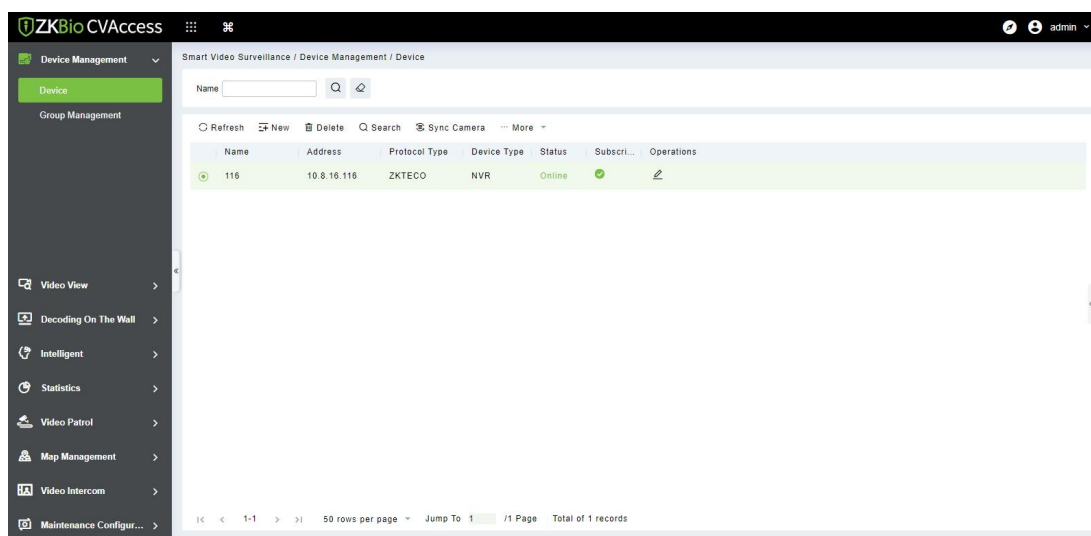
6.1.1.1 Adding Devices

Maximum supports 1024 video channels, support 64 channels preview and 16 channels real-time playback simultaneously.

1.   Click **[New]** under the main device list to display the adding interface.

There are 5 types you can select (ZKTECO/ONVIF/ZKIVA-Edge T1/ZKIVA-Edge X1/TPLink). If the purchased device is ZKNVR, select "ZKNVR" for the type.

Field Description:

- **Type:** Select the device type.

- **Name:** Customize the device name.

- **Address:** Configure the device address. The format is: xxx.xxx.xxx.xxx, for example: 192.168. 6.5.

- **Port:** Configure the device port.ZKNVR default is 8081.

- **Username and Password:** The NVR's user name and password.

✎**Note:**

- For ZKNVR, the default account is (admin, 12345678)

- For ZKIVA-Edge T1, the default account is(hxgk, hxgk1234)

- If you need to configure intelligent functions, visit the ZKIVA-Edge T1 Web side.

2.   Click **[OK]**.

6.1.1.2 Delete

Click **[Smart Video Surveillance] > [Device Management > [Device]**, then select **[Delete]**.

6.1.1.3 Search

Click **[Smart Video Surveillance] > [Device Management > [Device]**, you can select your device type and click **Search** to search NVR or IPC.
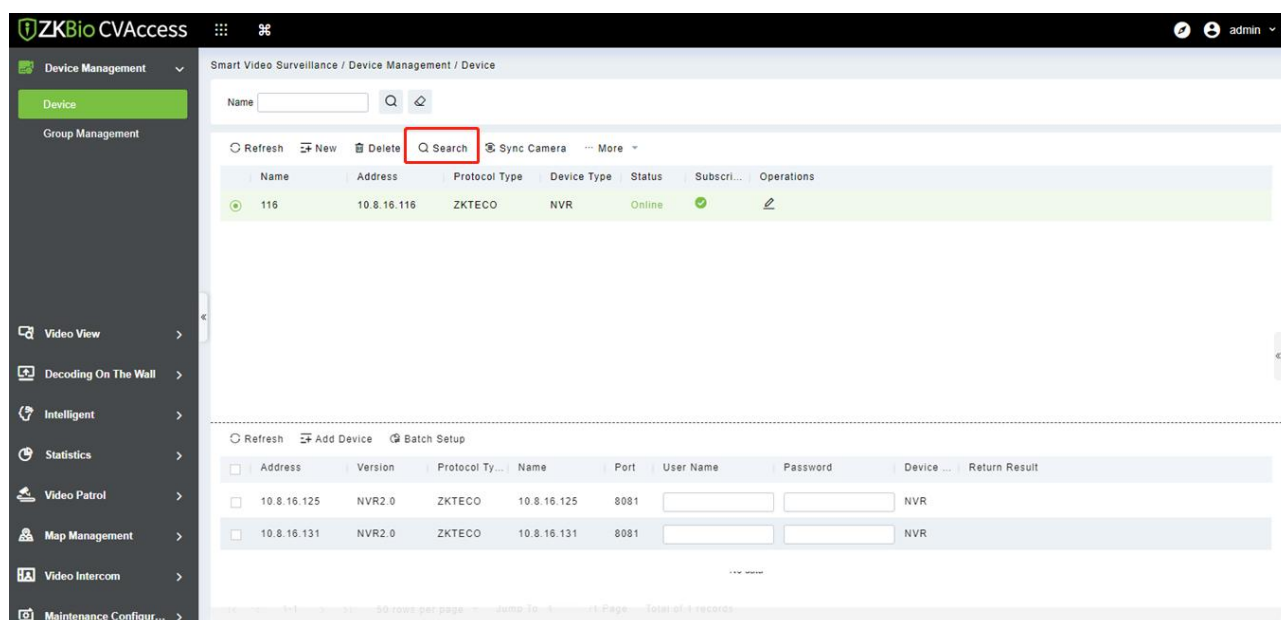
➢   **Refresh**

Click **[Refresh]** to refresh interface.

➢   **Add Device**

Select the searched device to add.

➢ **Batch Setup**

Batch fill the password of the device

6.1.1.4 Sync Camera

Click **[Smart Video Surveillance] > [Device Management] > [Device]**, then click **[Sync Camera]**.

6.1.1.5 Batch Sync Library

Step1: Enter Smart Video Surveillance → Device Management → Device, and click "Batch Sync Library".
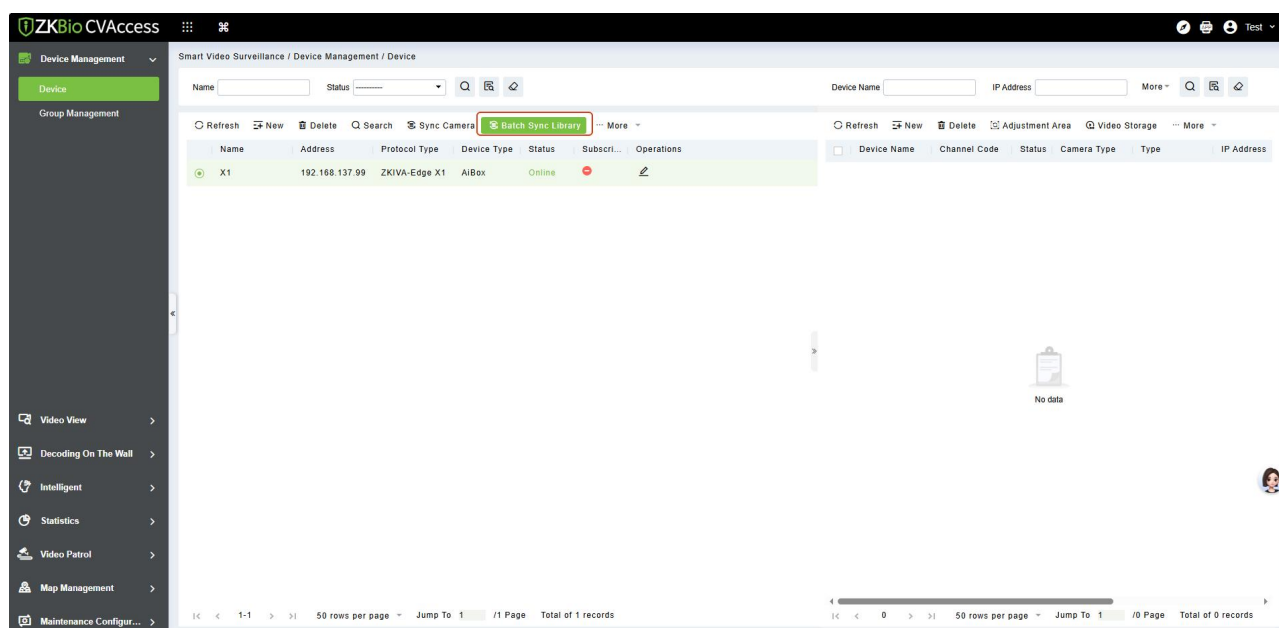
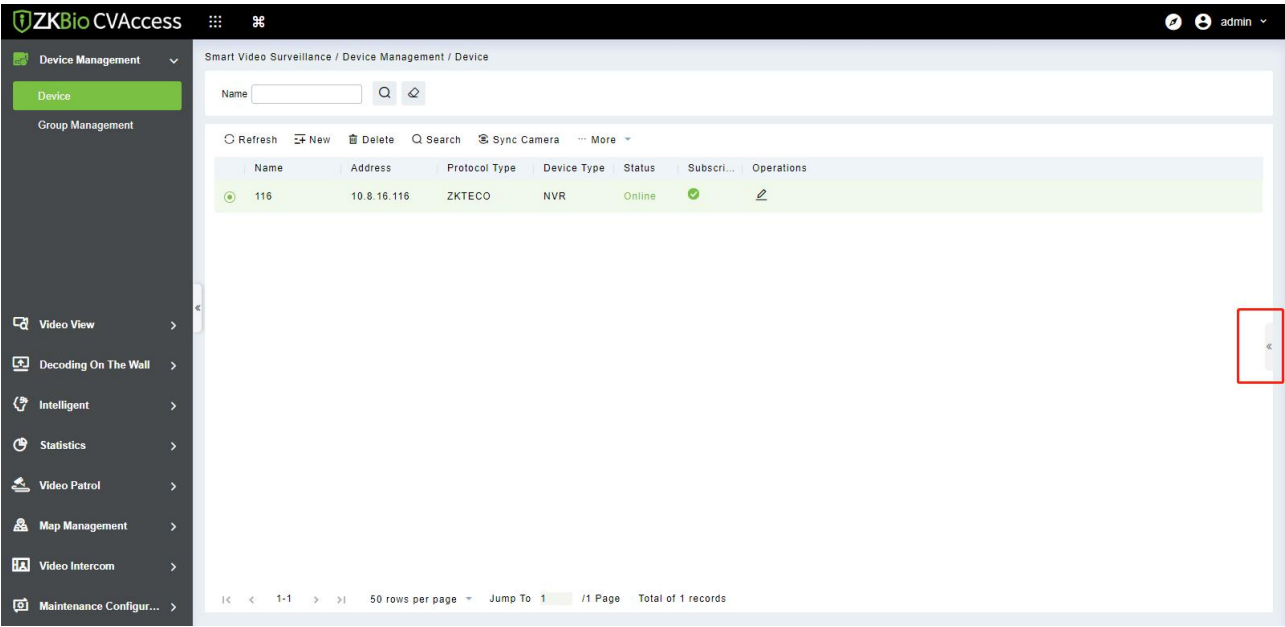**Step2:** Select the list you want to synchronize and move it to the right,and click "Next Step".
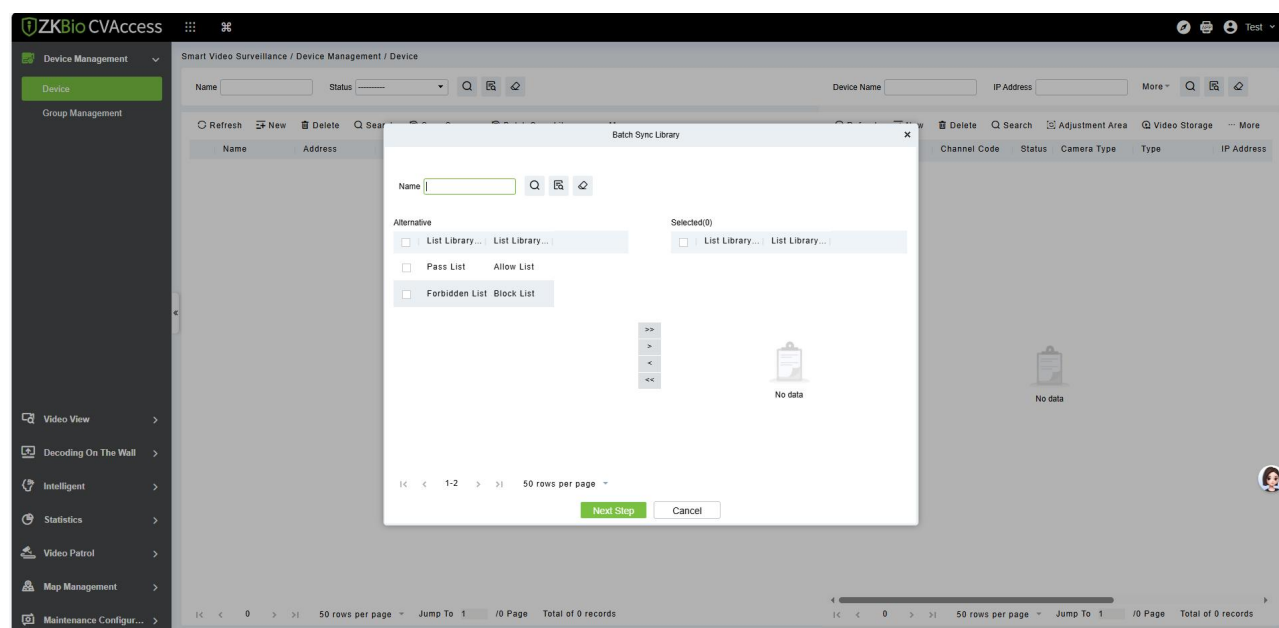
Step3: Select the devices for which you want to synchronize the list (multiple can be checked at once), move them to the right, and click "OK" to complete the list library synchronization.
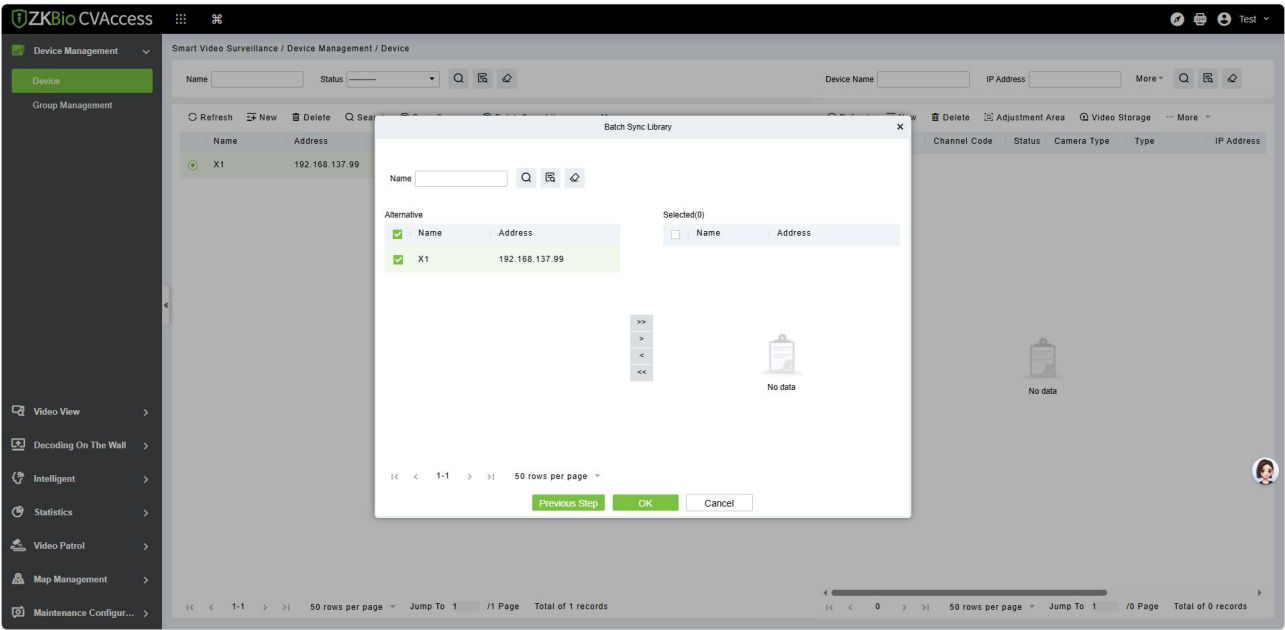
Data will start to be imported automatically until the operation completion prompt is given.

6.1.1.6 Add IPC to NVR

Click this icon ⟨⟨ to extend the page for adding cameras.

> ➤ **New**

Click **[New]** to add camera to NVR.

> ➤ **Delete**

Click to delete the camera.
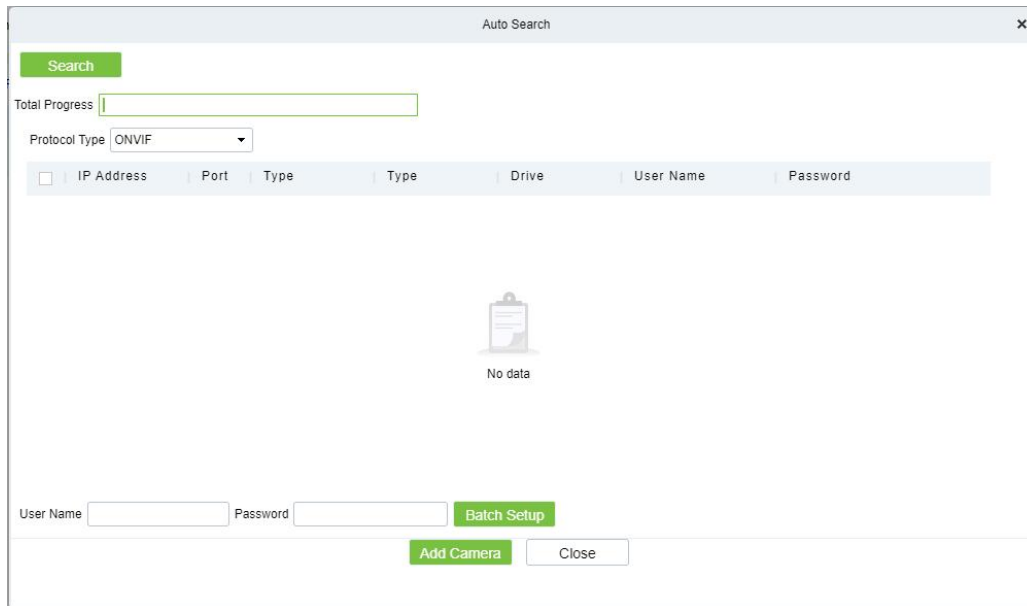
> ➤ **Search**
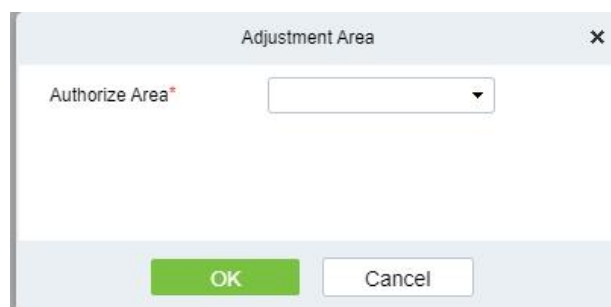
Click search to add camera devices to NVR.
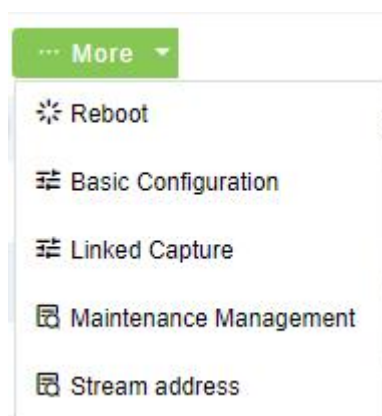
➢ **Adjustment Area**

Select the camera device and adjust the authorization area of the device.

➢ **Reboot**

Click to reboot camera.

➢ **Basic Configuration**

Configure camera information.

> ➢ **Linked Capture**

Capture photos of camera.
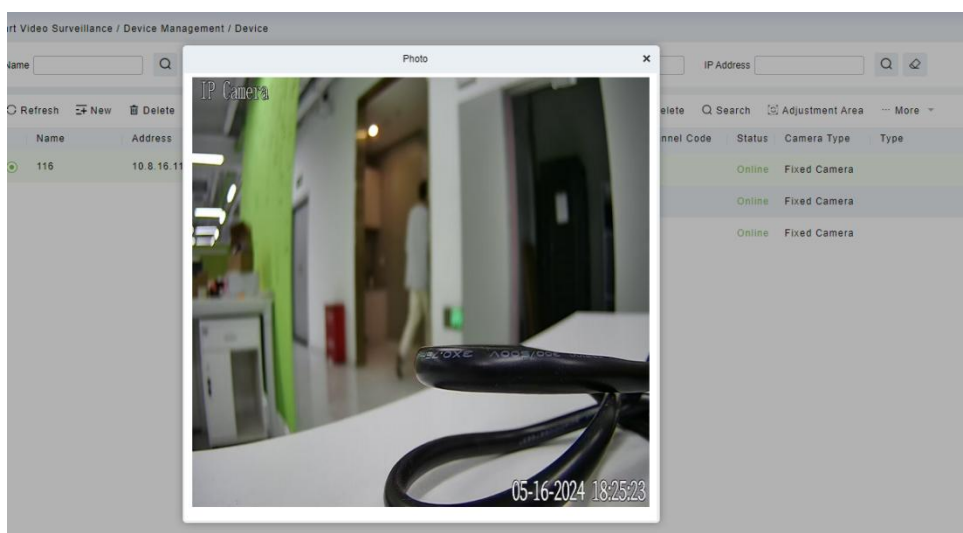
> ➢ **Maintenance Management**

Click to enter the web interface of the device.

> ➢ **Stream address**

Click to view the device's stream address.

6.1.2 Group Management

Click **[Smart Video Surveillance]** > **[Device Management]** > **[Group Management]**.
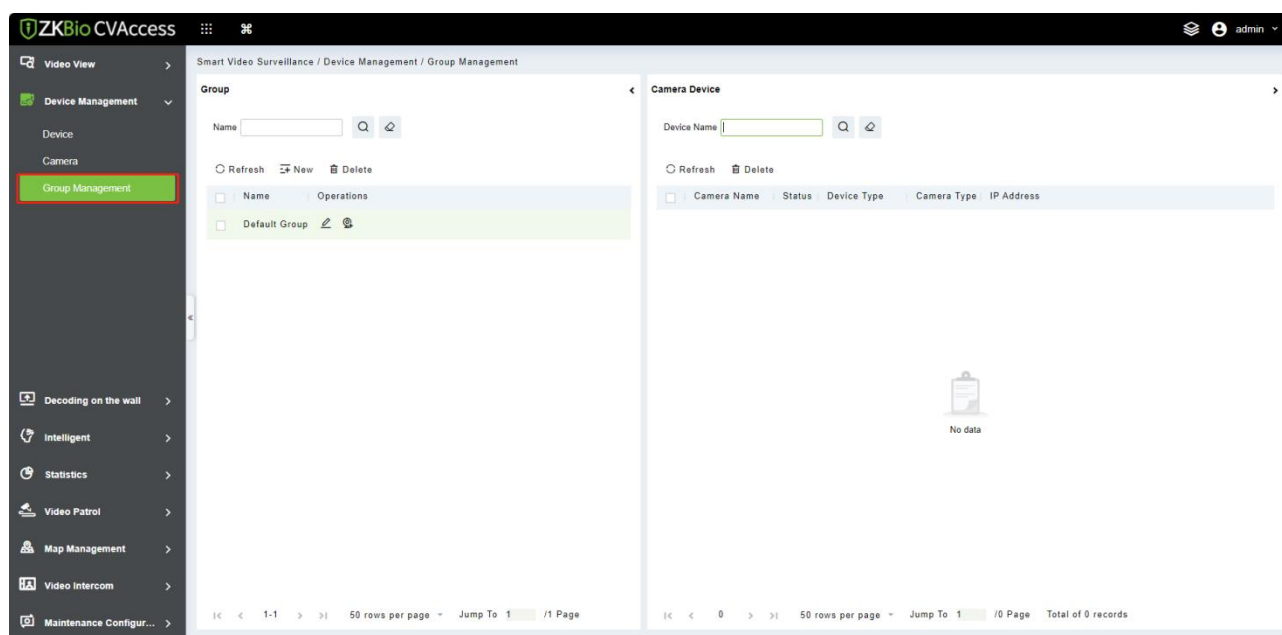
6.1.2.1 New

1. Click **[Smart Video Surveillance] > [Device Management] > [Group Management]**, then click **[New]**.
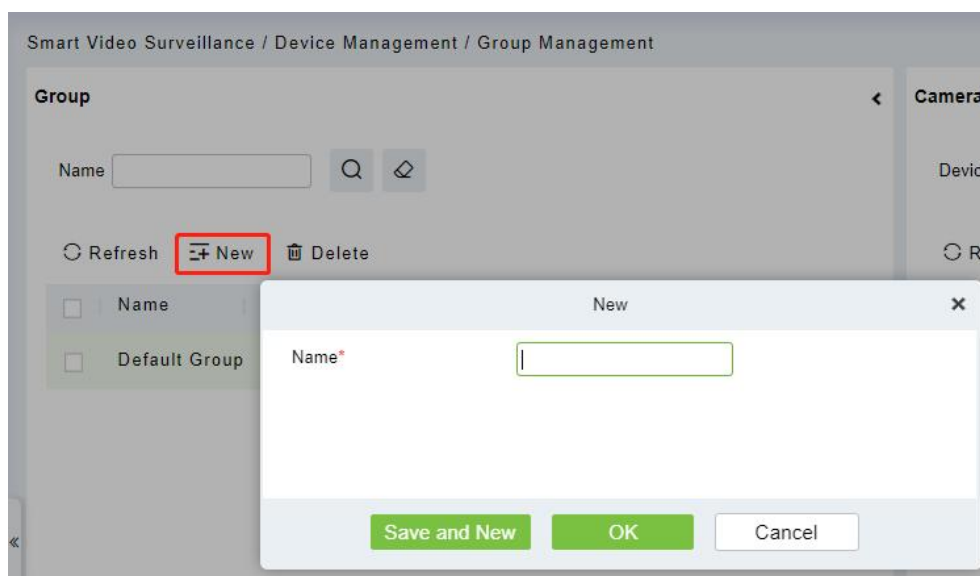
2. Click **[OK]** to save and exit.

6.1.2.2 Delete

Click **[Smart Video Surveillance] > [Device Management] > [Group Management],** then click **[Delete]**.

6.2 Video View

Click **[Smart Video Surveillance] > [Video View].**

In this module you can access the videos as **Video Preview** and **Video Playback**.

6.2.1 Video Preview

Click **[Smart Video Surveillance] > [Video View] > [Video Preview]**.

You can review recorded videos here.

6.2.1.1 Live Preview

When applying video monitoring products, please strictly comply with the applicable laws and regulations for the application and maintenance of video monitoring, recording, snapping and other services. It is forbidden for enterprises or individuals to install monitoring device in office areas, monitor employees" behaviors, or use video monitoring device to snoop on other people's privacy for illegal purposes.

➢ **Single camera live preview**

1. Click [Smart Video Surveillance] > [Video View] > [Video Preview].

2. In Full Devices, double-click the online camera to the live playback pane to open live preview.

✎**Note:** During live preview, please do not overlap the windows, interfaces, or dialog boxes of other programs on the window that opens live, otherwise it may cause live screen or video playback to be unsmooth.

➢ **Live preview of group camera**

1. Click [Smart Video Surveillance] > [Device Management] > [Grouping Management].

2. Click **[Add]** in the grouping list, enter the grouping name, and click "Confirm" to complete the addition of camera grouping.

3. Select the newly created camera group and click **[Add Camera]** on the right side. Double-click the camera in the new interface that pops up, and click **[OK]** to add it to the grouping, as shown in figure below.

4. In **Intelligent** module, select **[Video View] > [Video Preview]**, and in "**Grouping Devices**", double-click the online camera to the live playback pane to open the live preview.

✎**Note:** During live preview, please do not overlap the windows, interfaces, or dialog boxes of other programs on the window that opens live, otherwise it may cause live screen or video playback to be unsmooth.
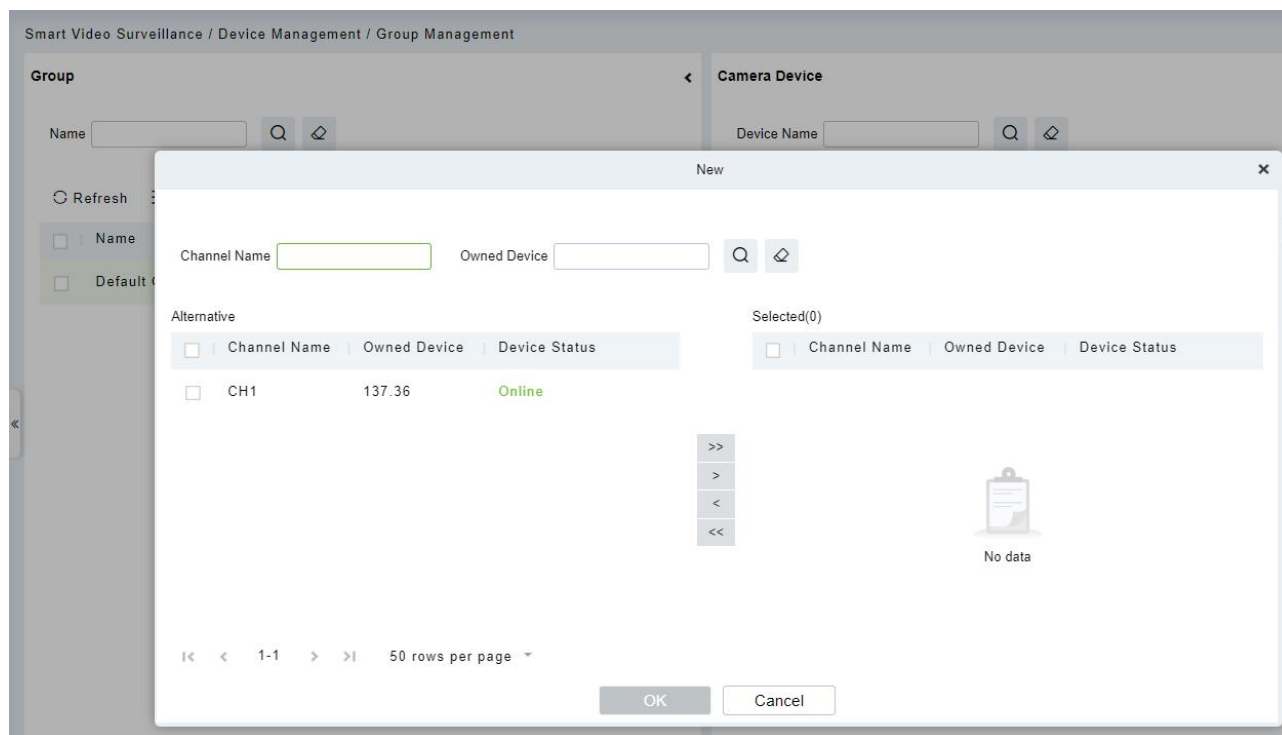
6.2.1.2 Video Preview

Using the round patrol function, the user can switch the live pictures monitored by multiple cameras regularly. For example, there are multiple cameras in a scene, and the live situation of all cameras cannot be displayed on a live split screen interface. The administrator can automatically switch the cameras of a scene to monitor the live situation every 30 seconds by using the round patrol function and realize the live browsing of all cameras in batches and time periods.

1. Click **[Smart Video Surveillance] > [Video View] > [Video Preview]**.

2. Under the list of grouped devices or full devices, click " " on the right to pop up the "Multiple Camera Operation Settings" page.

3. Click **[Round Tour]** to open the round tour setting window and configure round tour information.

Field Description:

- **Window number:** The number of round-robin windows must be less than the number of round-robin cameras.

- **Time interval (seconds):** Set the camera rotation picture residence time under the selected main device.

- **Stream type:**

    1) Main code stream: large code stream, high definition, and high bandwidth occupation.

    2) Auxiliary code stream: The code stream is small, the definition is low, and the bandwidth is small.

    3) Description: When there is bandwidth limitation, it is recommended to select secondary code stream.

4. Click **[OK]** to start the round tour.

5. End the round and click the toolbar ✄ below to close all screens.

➢ **Fast Target Search**

Screenshot for quick target search during preview or replay:

When security guards view real-time surveillance or playback video and find a suspicious person in the screen, they can zoom in on that person and take a screenshot to support quick "target search" to jump to target search and person track mapping.

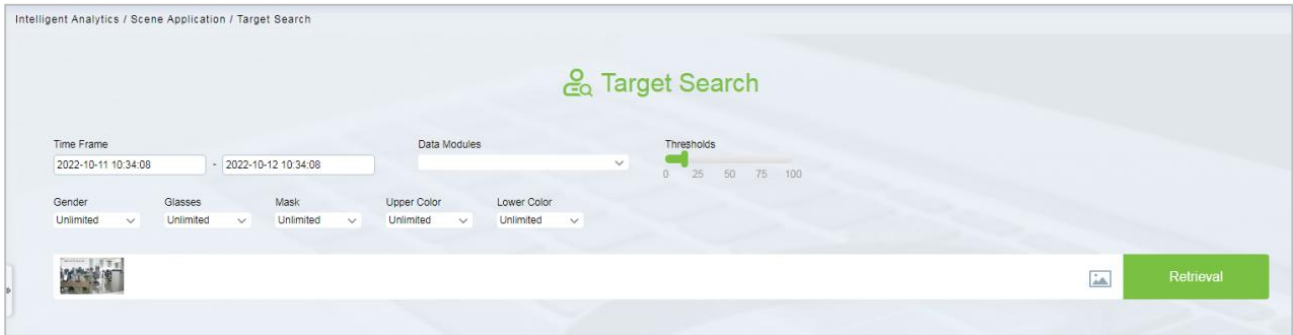1. Go to the **[Smart Video Surveillance] > [Video Preview]**, click 📷 to snap a screenshot.
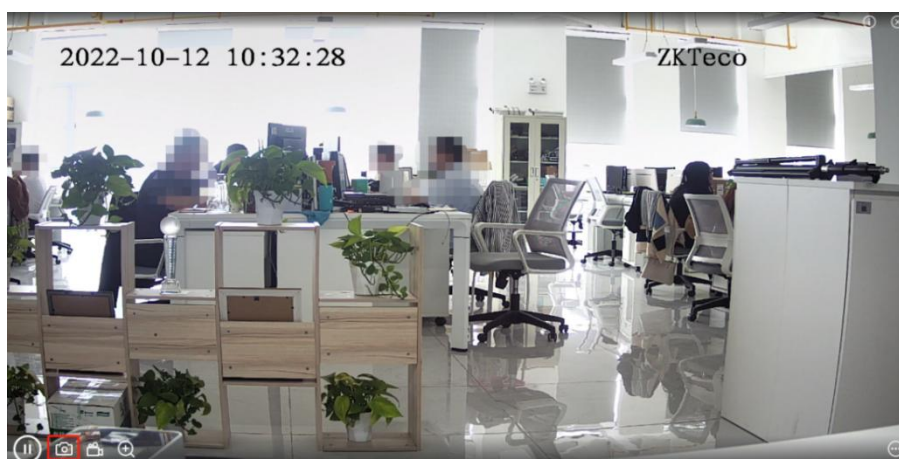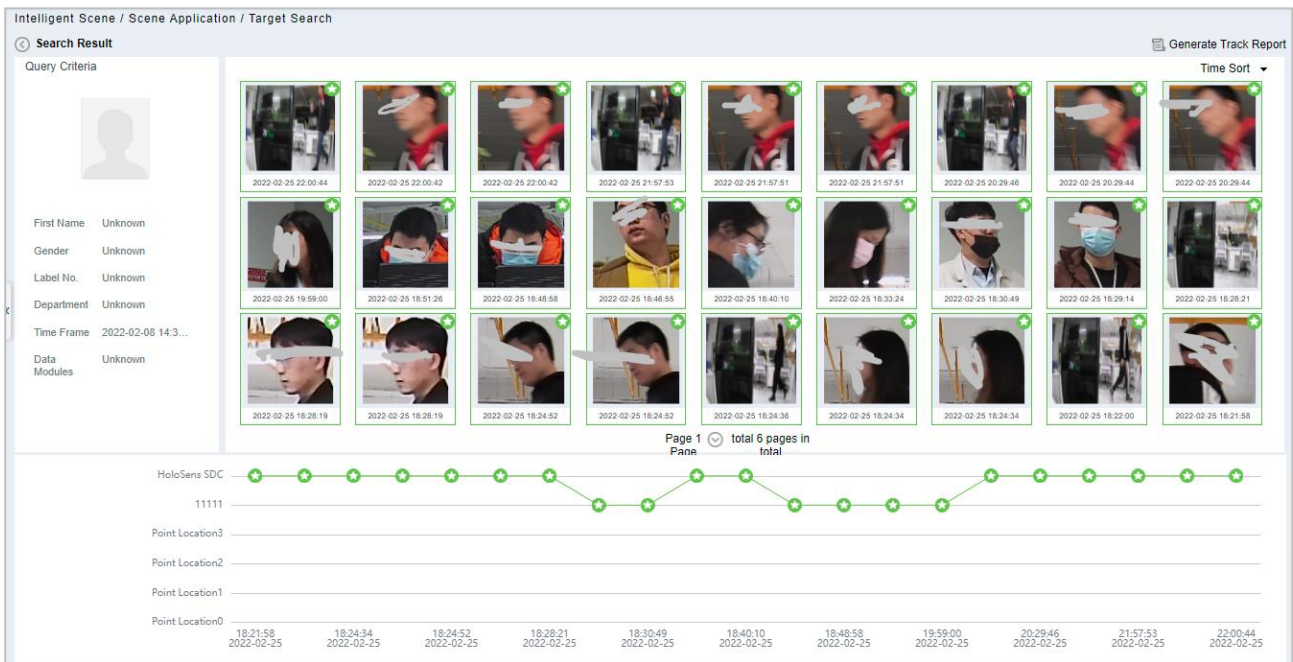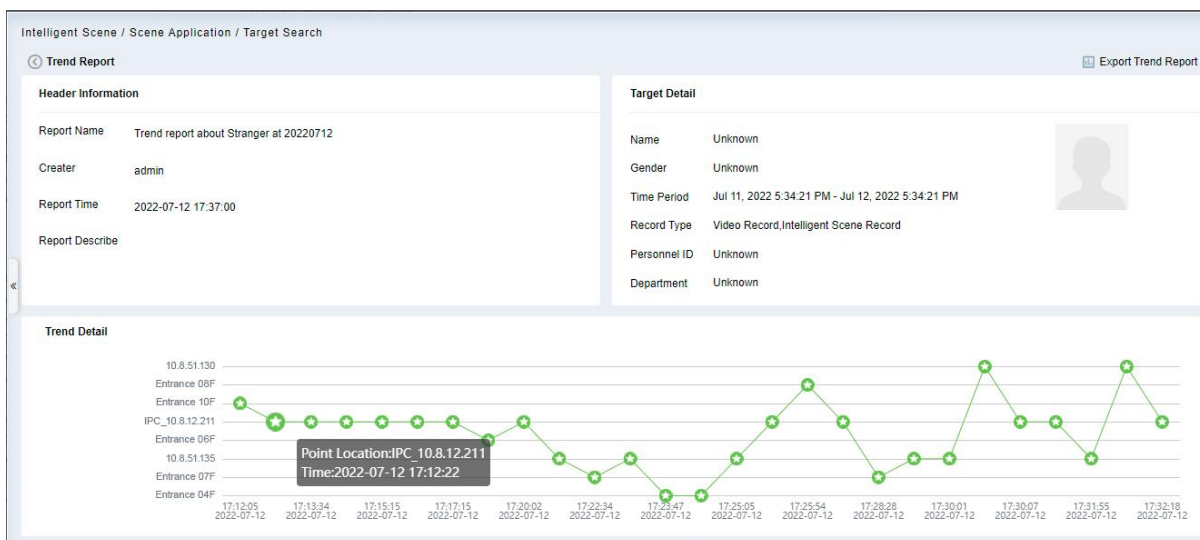

2. Then click **[Target search]**.
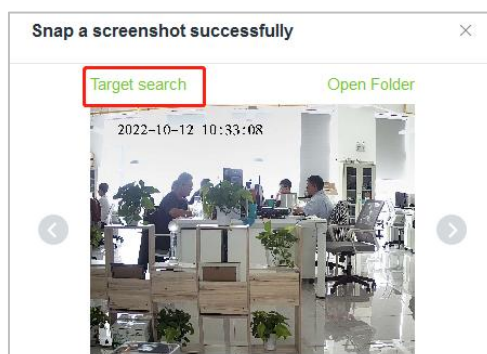
3.   Next click **[Retrieval]**.

4.   After the retrieval, the retrieval results appear.

5.   In the retrieval result, you can click Generate Trend Report in the upper right corner of the interface to export the trend report in PDF format, as shown in figure below.
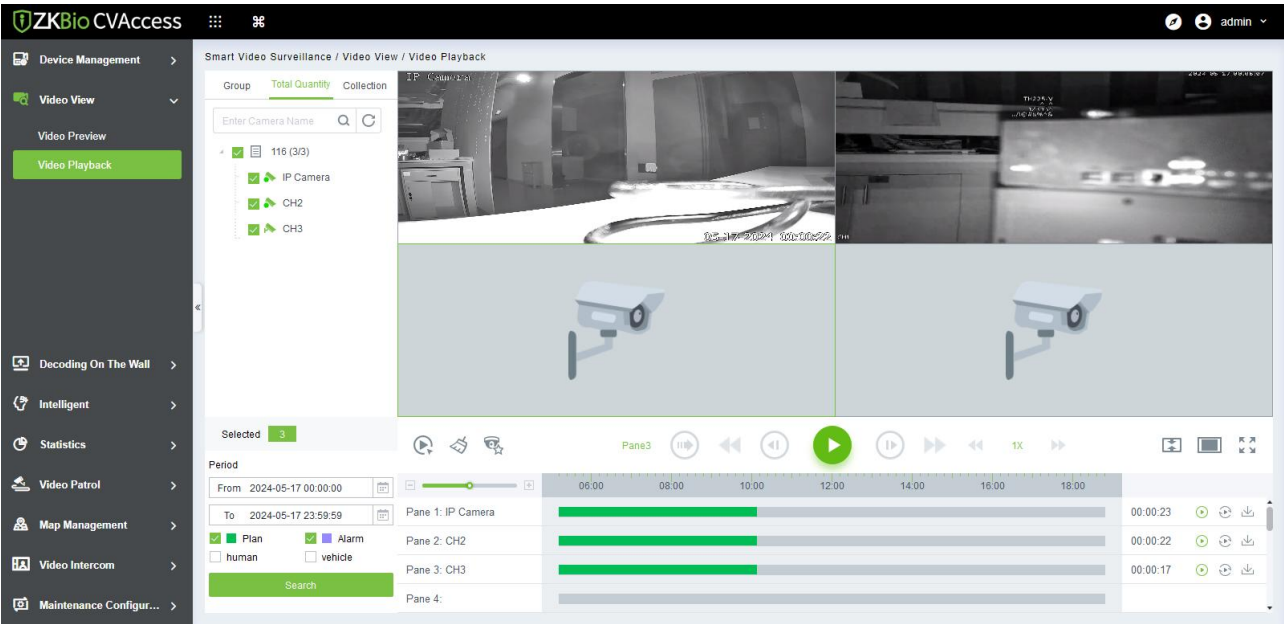
6.2.2 Video Playback

Click **[Smart Video Surveillance] > [Video View] > [Video Playback]**.

6.3 Decoding On the Wall

6.3.1 Decoder

Click **[Smart Video Surveillance] > [Decoding on the wall] > [Decoder]**.
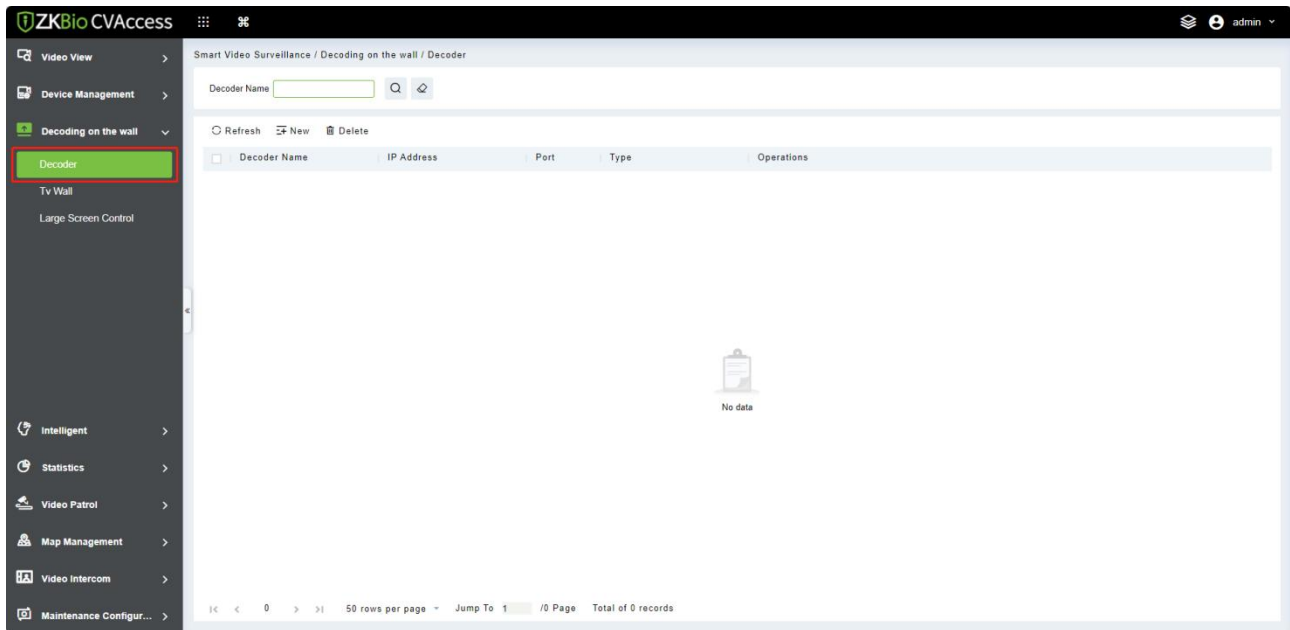
6.3.1.1 Add Decoder

1. Click **[New]**.

Field Description:

- **Decoder Name:** Custom decoder name.

- **IP Address:** IP Address of the decoder.

- **Port:** Default port 10200.

- **Type:** Select the device model to access the decoder. Support PEMXP70 and DEC6109

decoder access.

- • **Username:** Enter the business username.

- • **Password:** Enter the business password.

2. Click **[OK]** to save and exit, or click **[Save and New]** to continue.

6.3.1.2 Delete

Click **[Smart Video Surveillance] > [Decoding on the wall] > [Decoder]**, then click **[Delete]**.
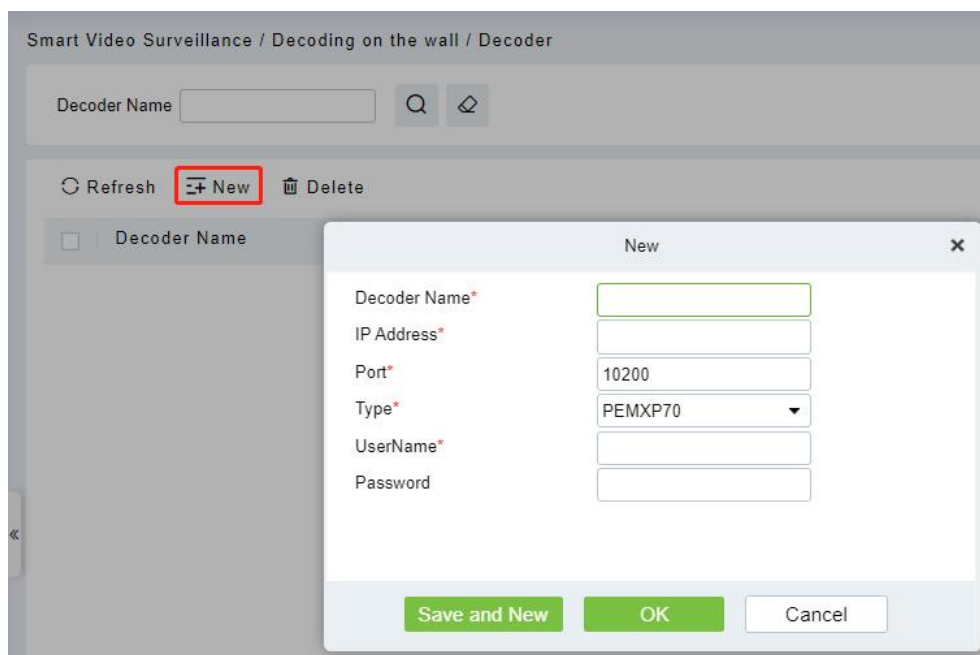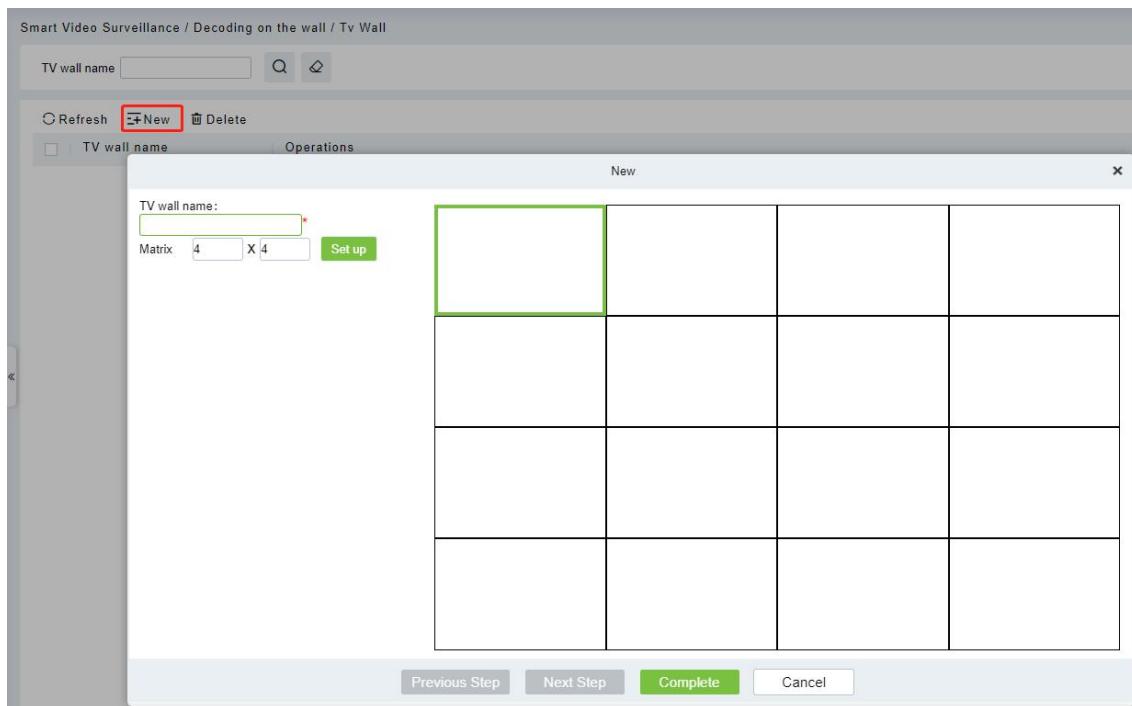
6.3.2 TV Wall

Click **[Smart Video Surveillance] > [Decoding on the wall] > [TV Wall]**.
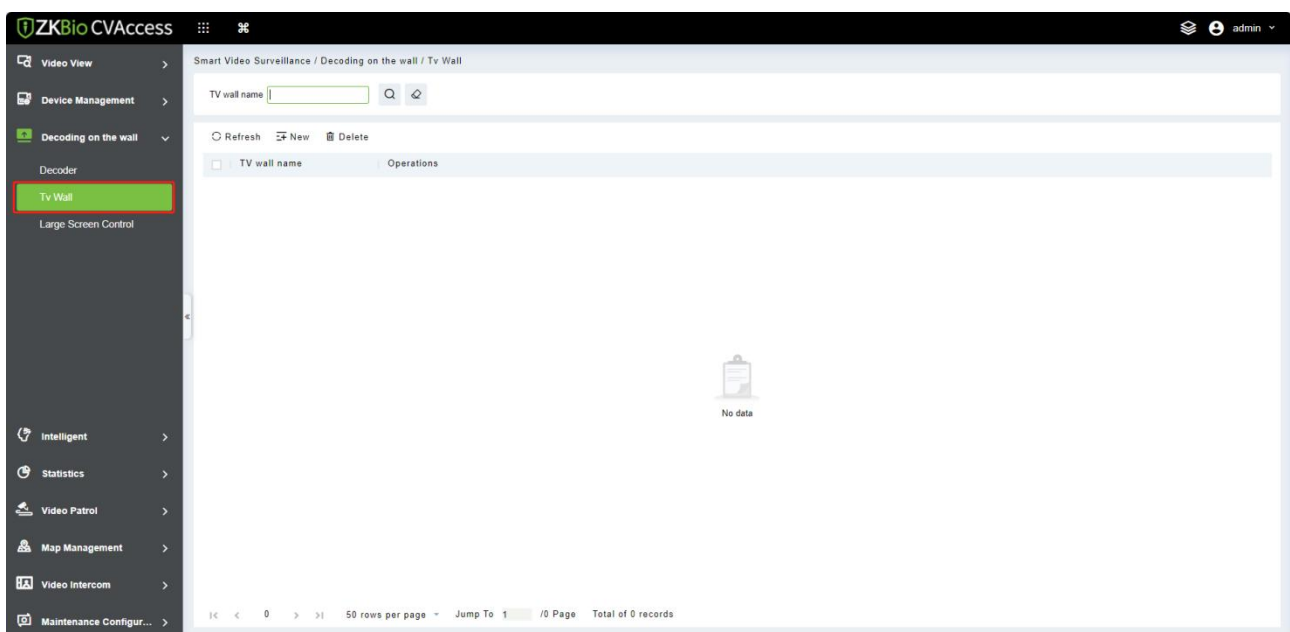
6.3.2.1 Create TV Wall

1. Click **[Smart Video Surveillance] > [Decoding on the wall] > [TV Wall]**, then click **[New (Create TV Wall)]**.

2.   Enter a custom TV Wall Name.

3.   In the Matrix Settings box, customize the number of rows and list of input layouts, and click **[Set up]** to apply the layout.

✍**Note:** Matrix Layout pane settings, supporting a minimum of 1 * 1 and a maximum of 8 * 8.

4.   Click next to enter the TV wall binding decoder interface, as shown in figure below.
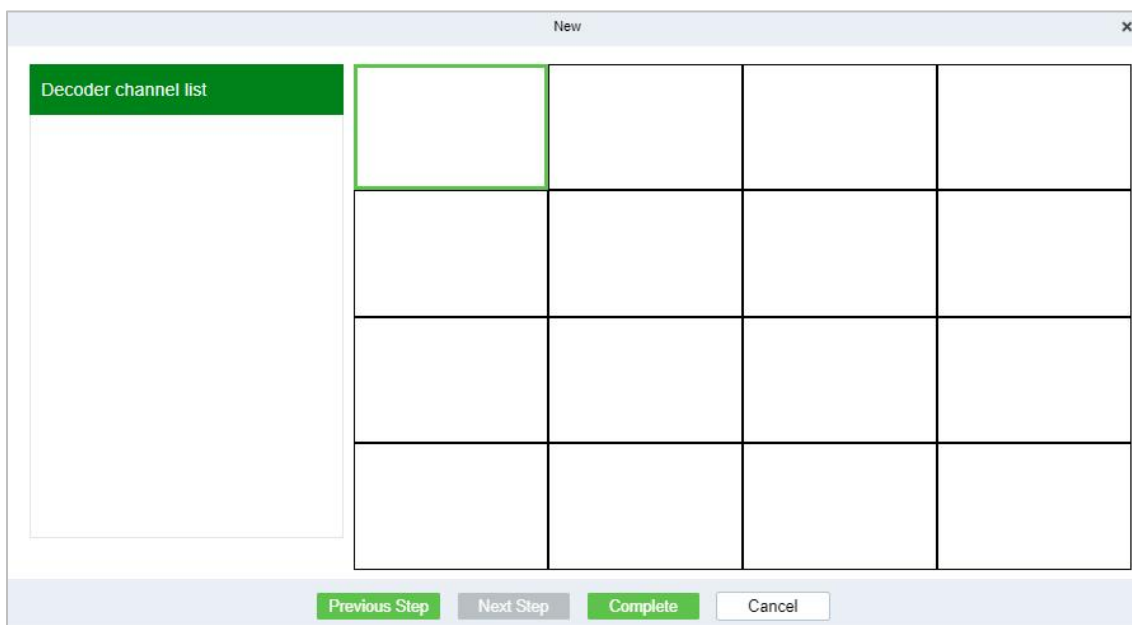
5.   Select the TV wall pane to which you want to add a decoder channel, and then click **[Decoder Channel]** on the left to complete the binding.

6.   Click **Finish]** to finish adding the TV wall.

6.3.3 Large Screen Control

Click **[Smart Video Surveillance] > [Decoding on the wall] > [Large Screen Control].**
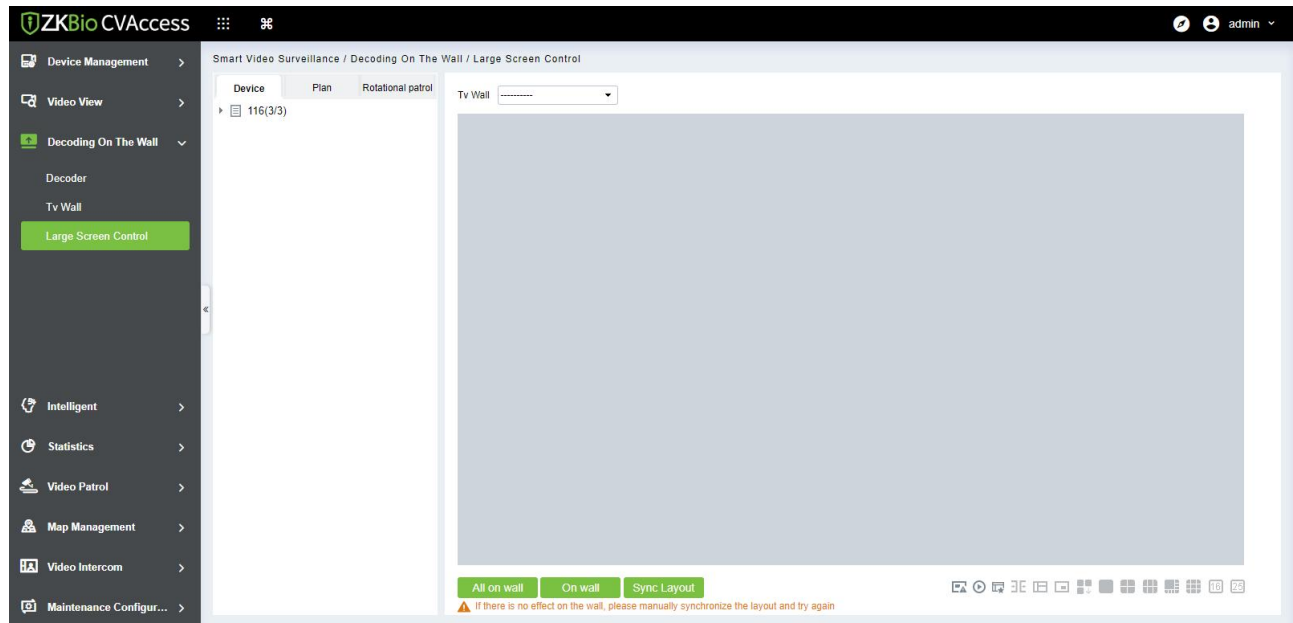
Icon	Parameter	Description
	Alarm Setup	Select a screen to show the events of linked alarms
	Video Preview	Previewing the current screen
	Collection of Plan	Join the list of collection profiles
	Merged screen	Merge multiple scattered screens into one
	Split Screen	Separate the merged screens
	Floating Window	Floating screen window
	Down Wall	End on the wall
	1 Split Screen	1 Split Screen
	4 Split Screen	4 Split Screen
	8 Split Screen	8 Split Screen

Icon	Parameter	Description
⊞	9 Split Screen	9 Split Screen
16	16 Split Screen	16 Split Screen
25	25 Split Screen	25 Split Screen

6.3.3.1 Plan

Click this icon 🖼 to save current patrol settings to **[Plan]**.
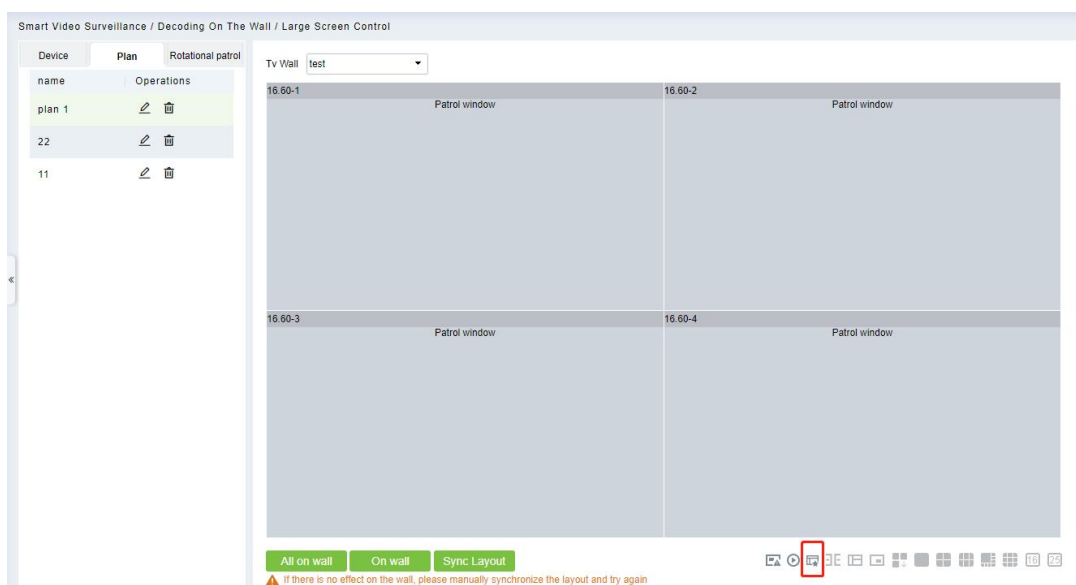
6.3.3.2 Rotational patrol (New)
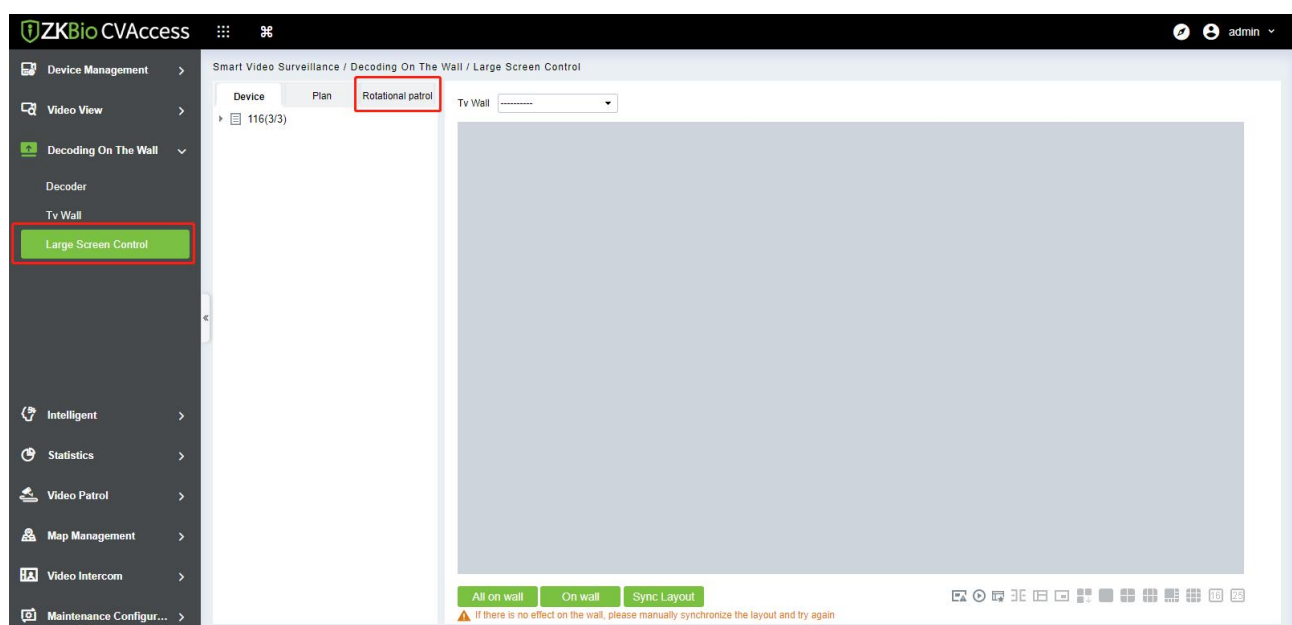
1.   Click **[Smart Video Surveillance]** > **[Decoding on the wall]** > **[Large Screen Control]**>**[TV

Wall] to select a TV.

2.   Select a window, click **[Smart Video Surveillance]>[Decoding on the wall] > [Large Screen Control]>[Rotational patrol]>[more]>[Window Configuration]** to add configure patrol window.

3.   Click **[Smart Video Surveillance]>[Decoding on the wall] > [Large Screen Control]>[Rotational patrol]>[more]>[New]** to add a new video rotational patrol.
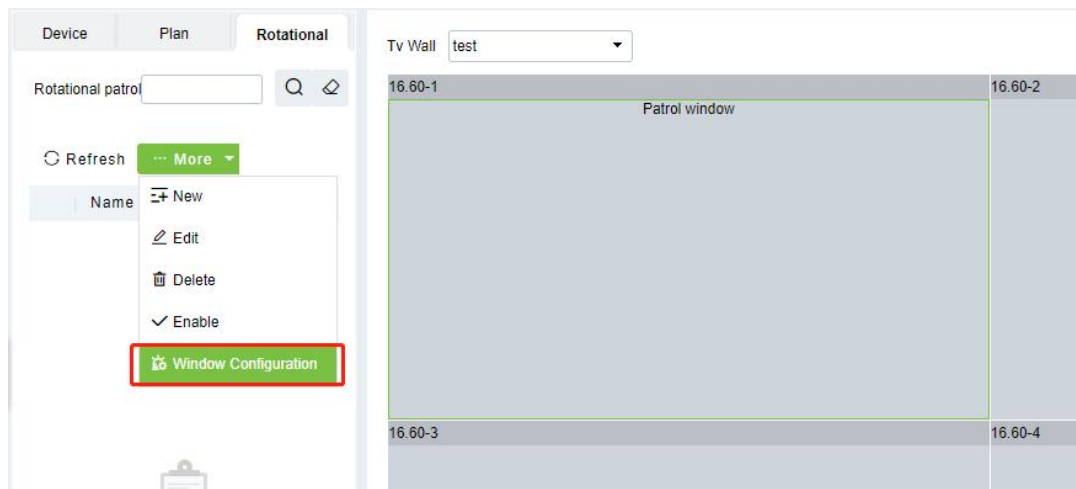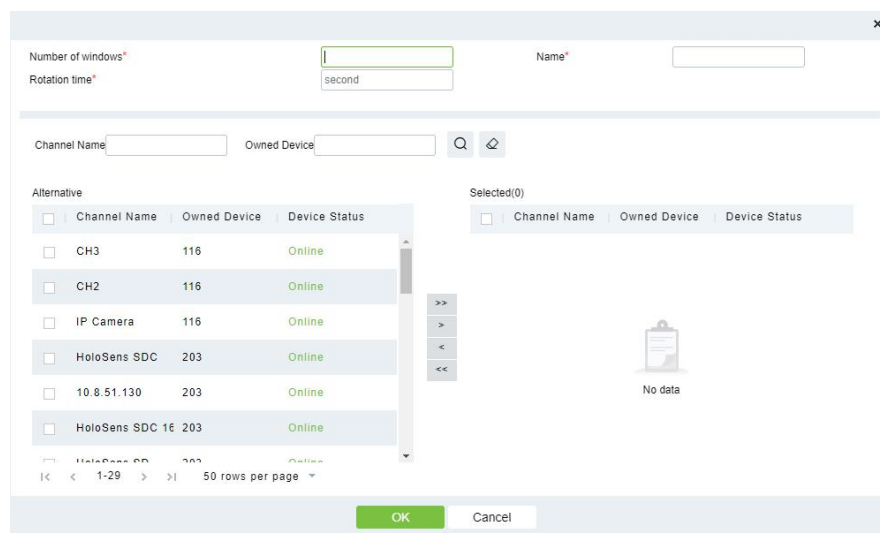

-   **Number of windows:** Number and name of this rotational patrol plan.

✍ **Note:** When configuring the number of polling windows, the number of windows filled in should be consistent with the actual number of windows.

For example:

As shown in the following figure, we have configured 4 patrol windows, so we should fill in 4 in the **Number of Windows.**
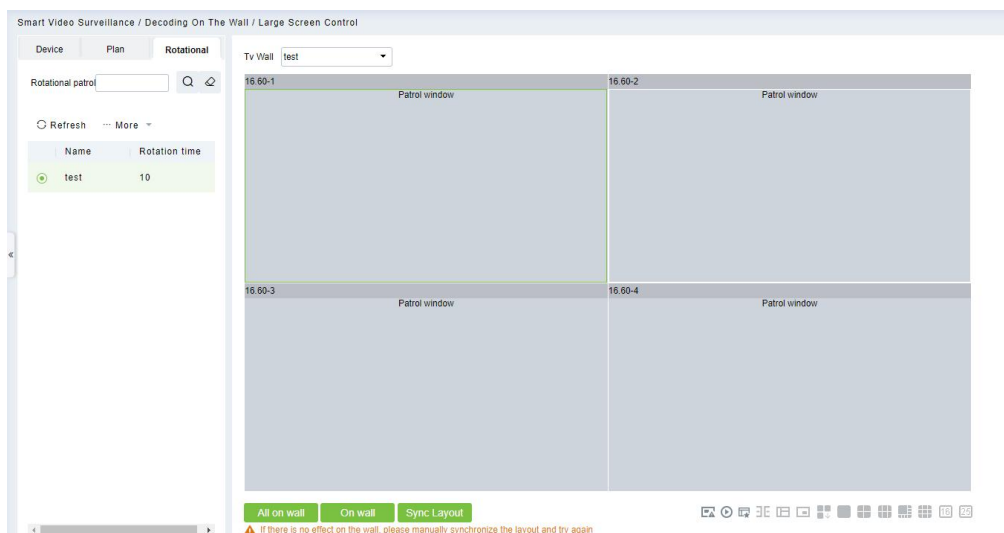
- **Name:** Rotation name.

- **Rotation time(second):** The duration of camera rotation patrol

4.   Click **[Smart Video Surveillance]>[Decoding on the wall] > [Large Screen Control]>[Rotational patrol]>[more]>[Enable]** to add a new video rotational patrol.
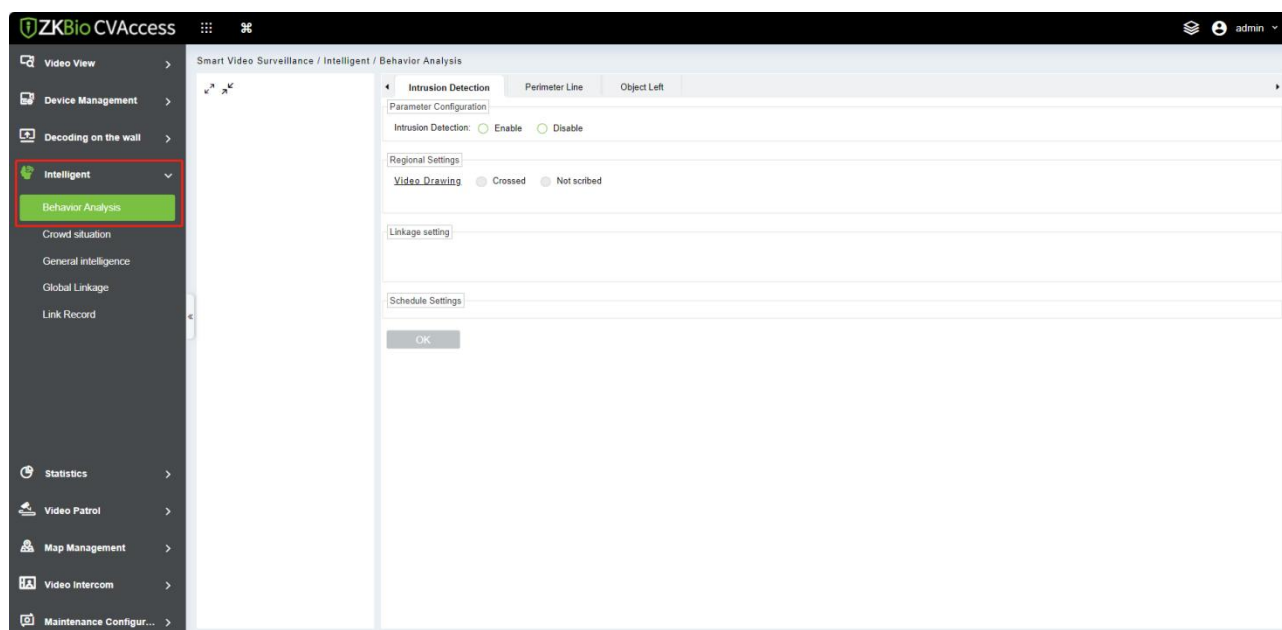
6.4 Intelligent

6.4.1 Behavior Analysis

Configuration of intelligent functions for behavioral analysis of front-end cameras by ZKBio CVAccess.

✍**Note:** The default interface is part of Holowits' functionality.

Click **[Smart Video Surveillance] > [Intelligent] > [Behavior Analysis].**

➢ **Parameter Configuration**

Configure to enable intrusion detection.

➢ **Regional Settings**

- **Crossed**: Indicates that a line is currently drawn for this smart feature.

- **Not Scribed**: Indicates that a line is currently not drawn for this smart feature.

Click **[Video Link Drawing]**, draw the detection area.

6.4.2 Crowd Situation

Configuration of intelligent functions for crowd situation of front-end cameras by ZKBio CVAccess.

✍**Note:** The default interface is part of Holowits' functionality.

Click **[Smart Video Surveillance] > [Intelligent] > [Crowd Situation]**.

6.4.3 General Intelligence

Configuration of general intelligence functions of front-end cameras by ZKBio CVAccess.

✏**Note:** The default interface is part of Holowits' functionality.

Click **[Smart Video Surveillance] > [Intelligent] > [General Intelligence]**.
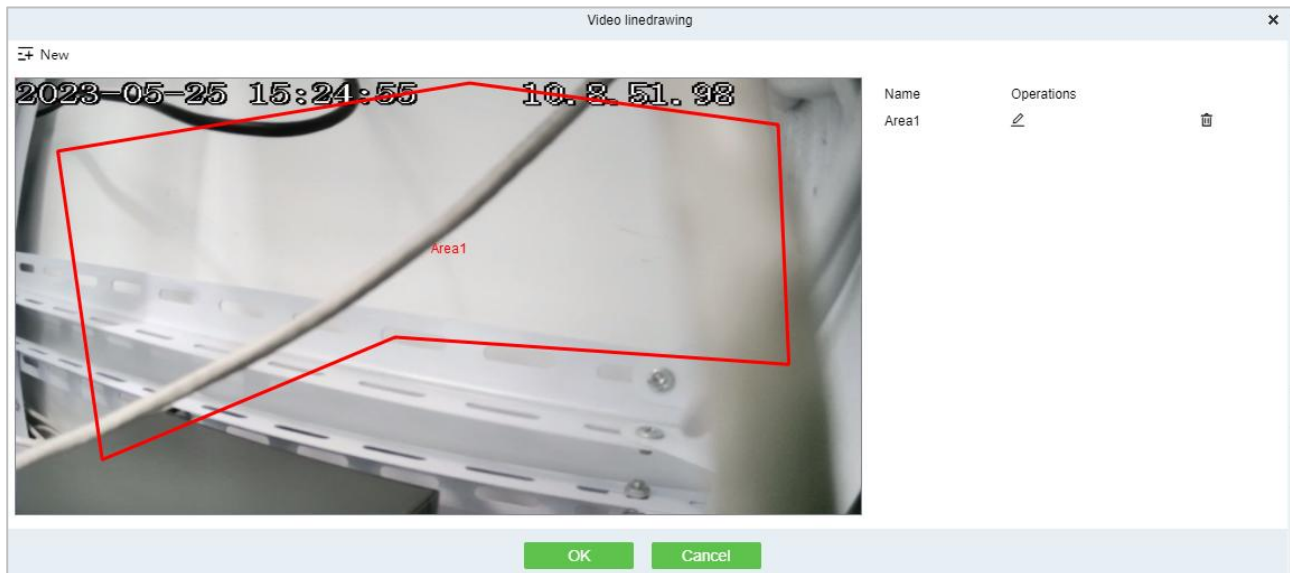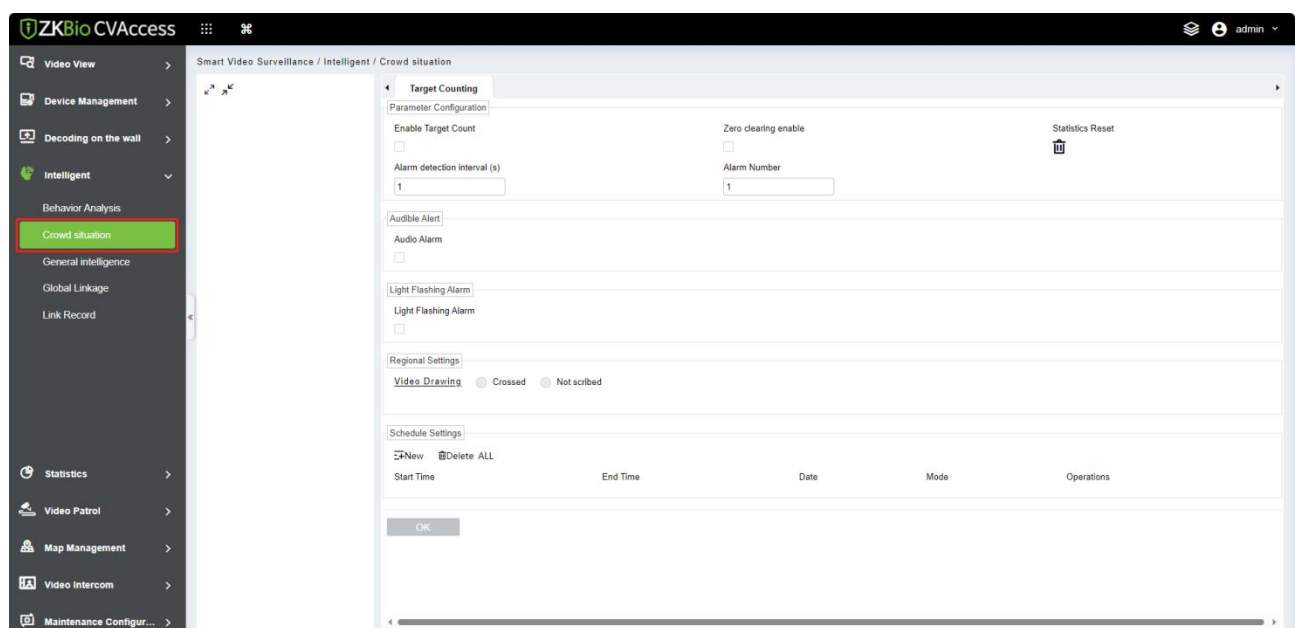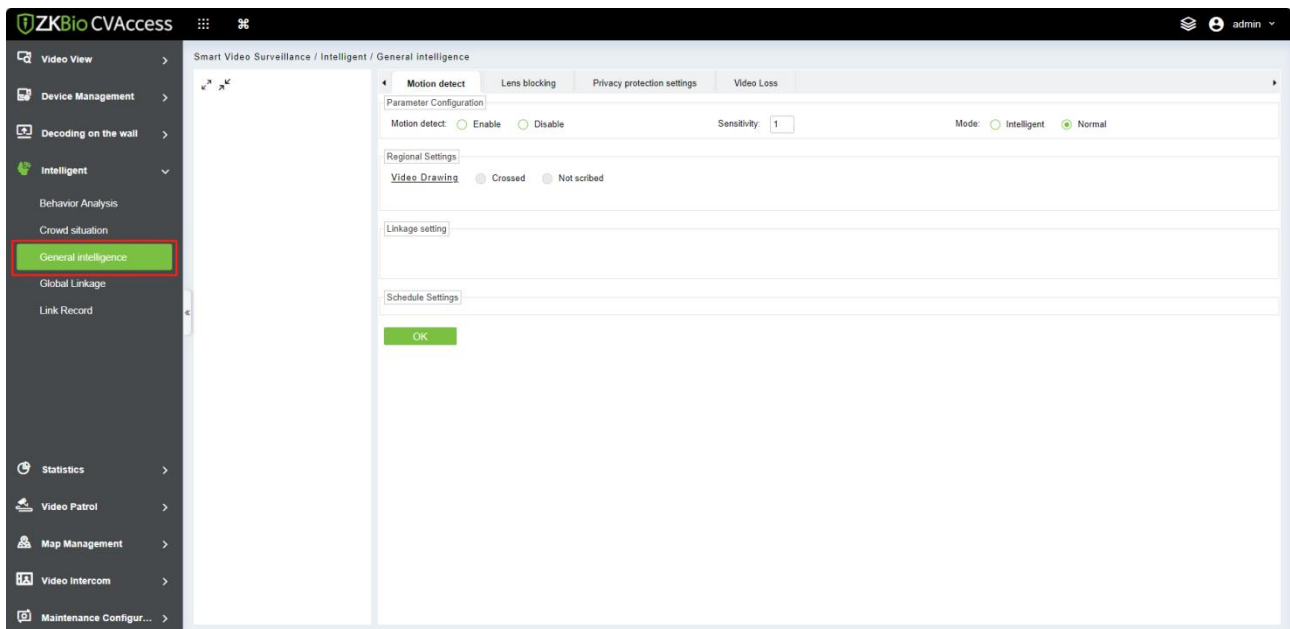

➢ **Parameter Configuration**

- **Sensitivity**: Detection sensitivity.

- **Mode:**

    1) **Intelligent**: Can distinguish between people or vehicles.

    2) **Normal:**   No distinction between people and vehicles.

6.4.4 Global Linkage

Click **[Smart Video Surveillance] > [Intelligent] > [Global Linkage]**.
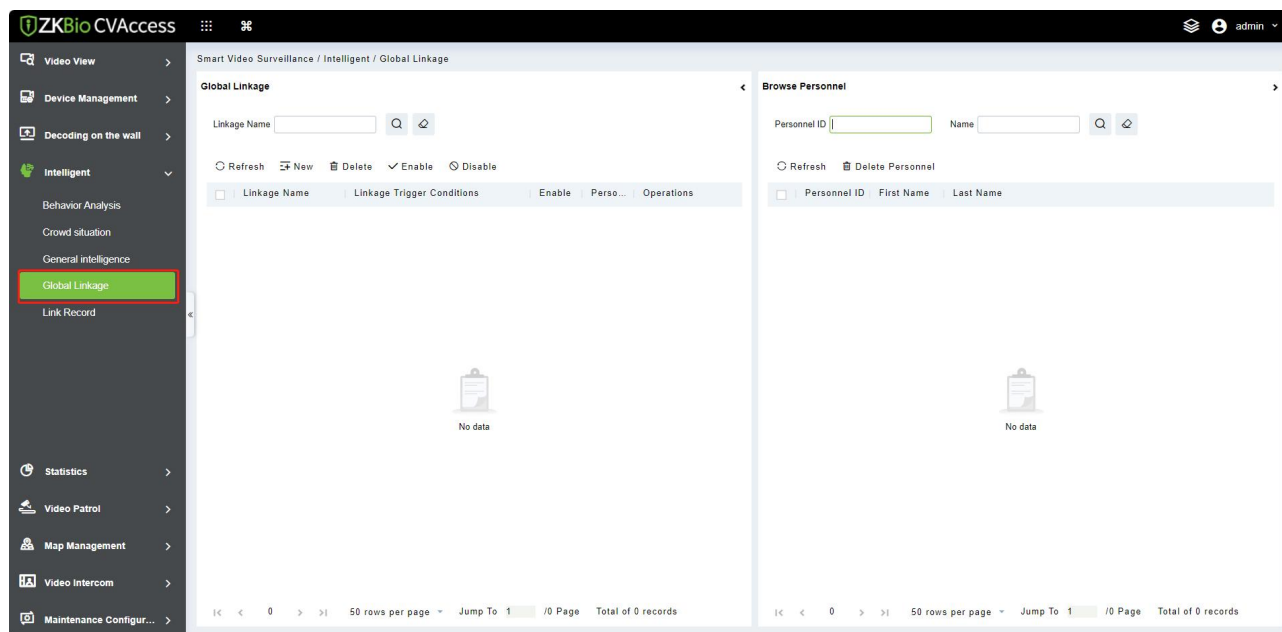
6.4.5 Link Record

Click **[Smart Video Surveillance] > [Intelligent] > [Link Record]**.

➢ **Clear All Data**

Click **[Clear All Data]** to pop up prompt and click **[OK]** to clear all records.

6.5 Statistics

6.5.1 Alarm Report

In this module, you can access the data for the type of personnel or person can select the start time and end time the serial number of the video channel, and different alarm types to filter the report.
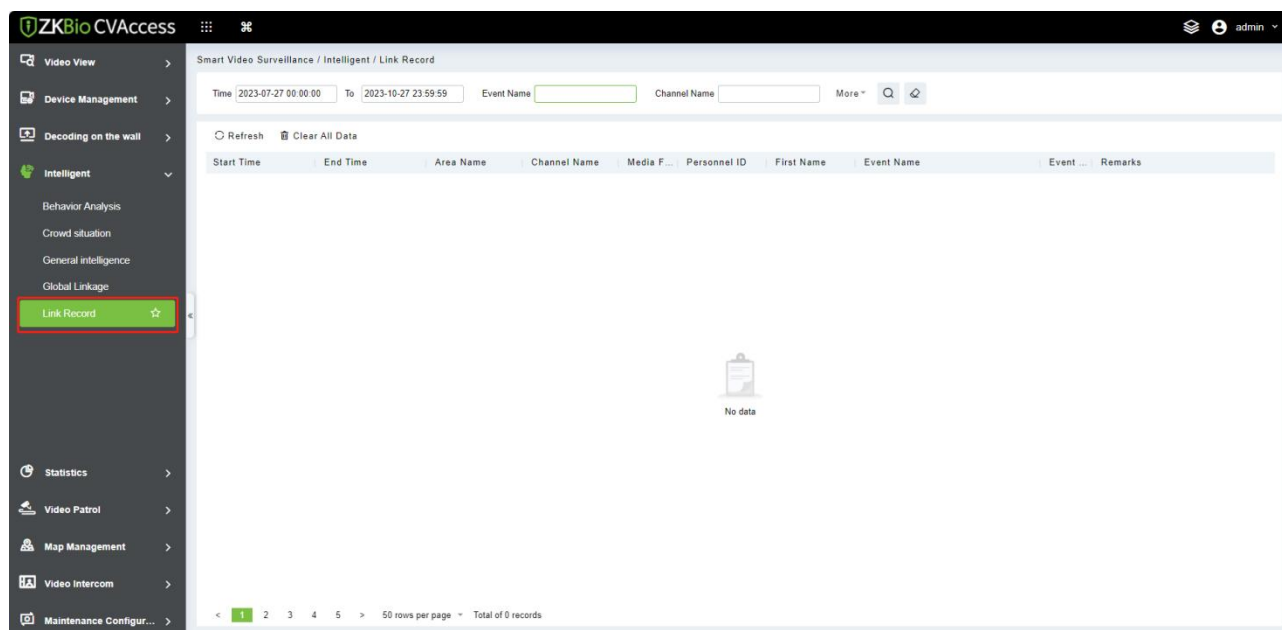
Click **[Smart Video Surveillance] > [Statistics] > [Alarm Report]**.
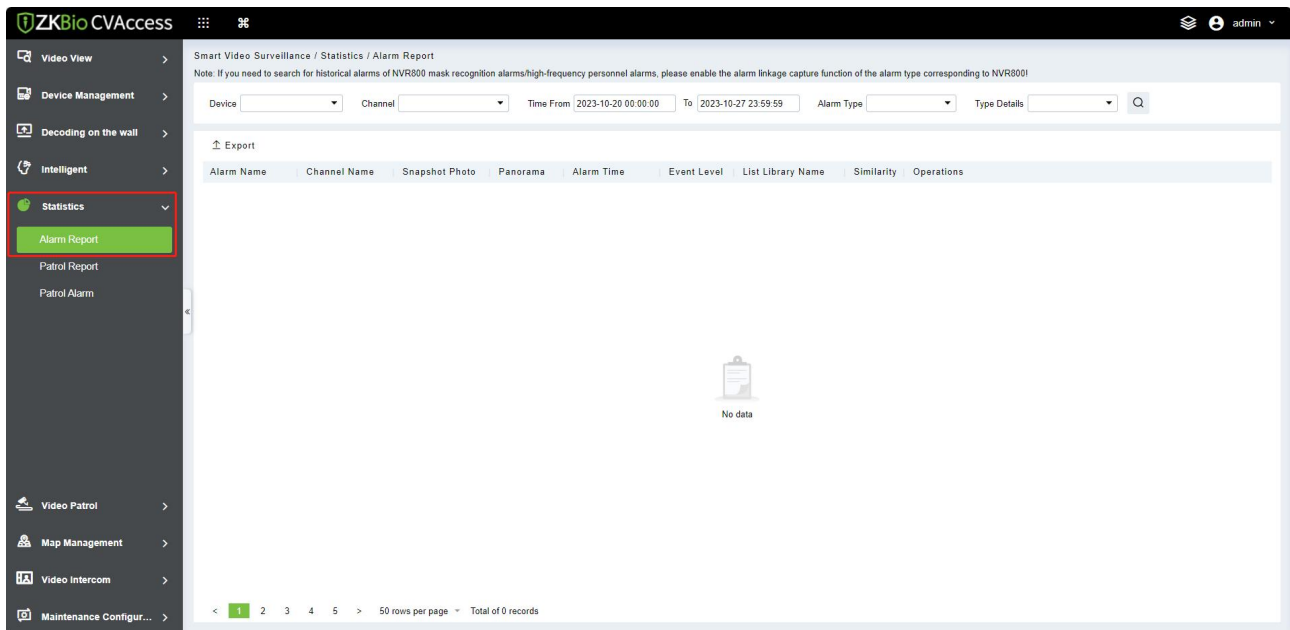
6.5.2 Patrol Report

In this module, you can access the data for the type of personnel or person as dd, aa, vip, or VIP, Forbidden list, pass list, and Stranger to get data to follow the options.

Click **[Smart Video Surveillance] > [Statistics] > [Patrol Report]**.

6.5.3 Patrol Alarm

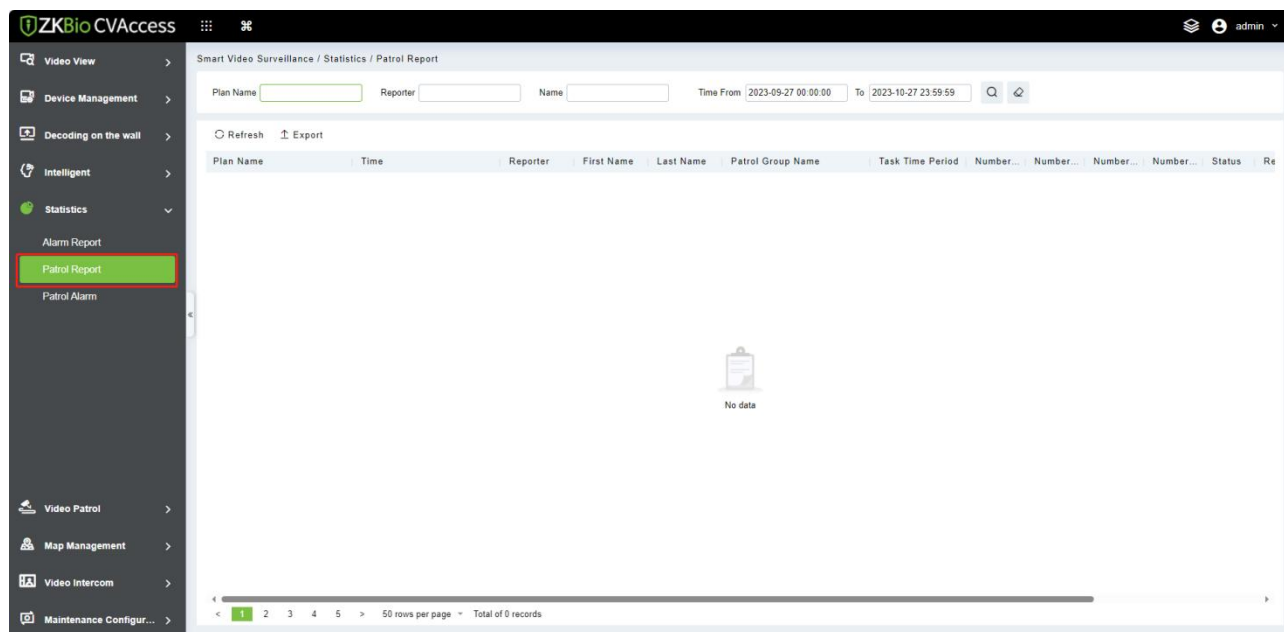In this module, you can access the data for the type of personnel or person as dd, aa, vip, or VIP, Forbidden list, pass list, and Stranger to get data to follow the options.

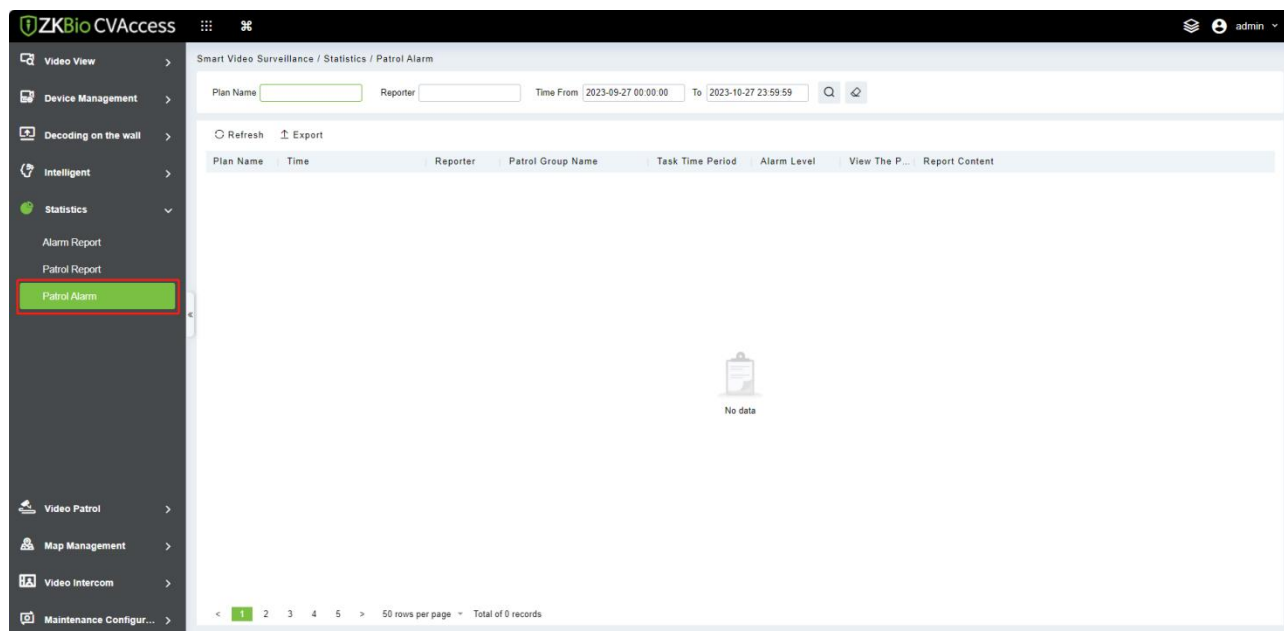Click **[Smart Video Surveillance] > [Statistics] > [Patrol Alarm]**.

6.6 Video Patrol

On the preset path, you can check the punch-in by a real-time preview of the camera remotely to achieve the same patrol task as the traditional punch-in effect.

6.6.1 Patrol Group

Create a patrol group to add patrol personnel.

Click **[Smart Video Surveillance] > [Video Patrol] > [Patrol Group]**.
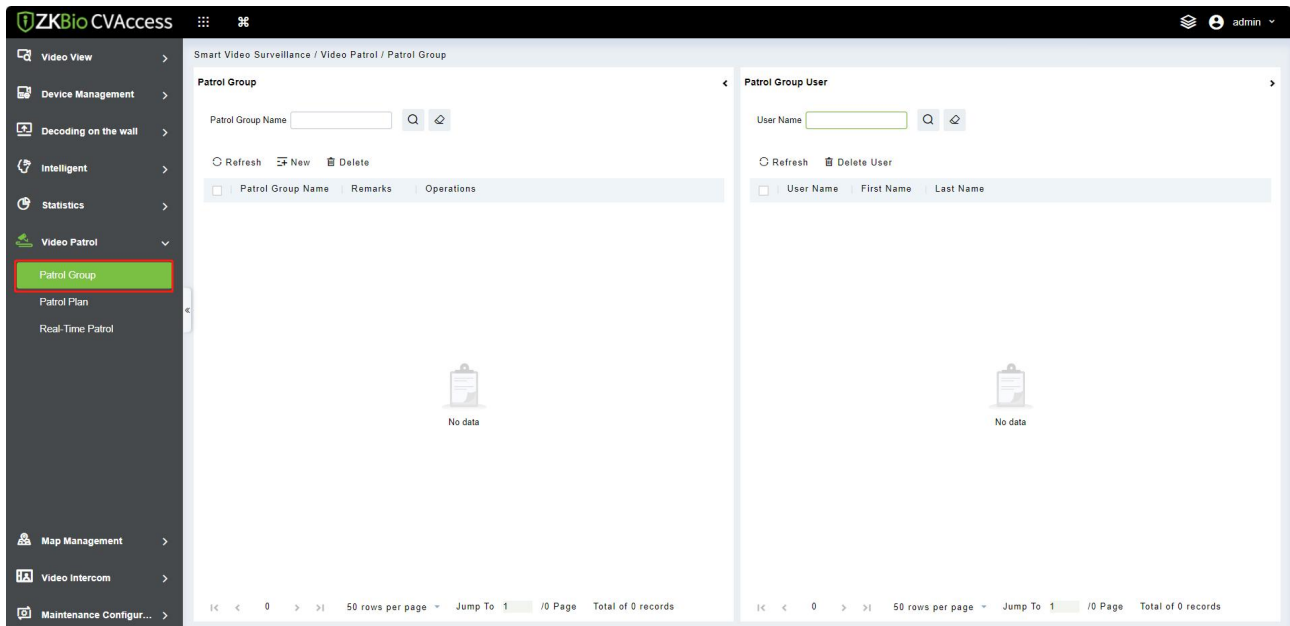
6.6.1.1 Add Patrol Group

Click **[New]**.

Field Description:

- **Patrol Group Name:** Enter the name of the patrol group for easy searching and management non-repeatable.

- **Remarks:** Text notes of the patrol group.

6.6.1.2 Add Patrol Group User

In the patrol group list, click 👤+ button to enter and select to add group members.

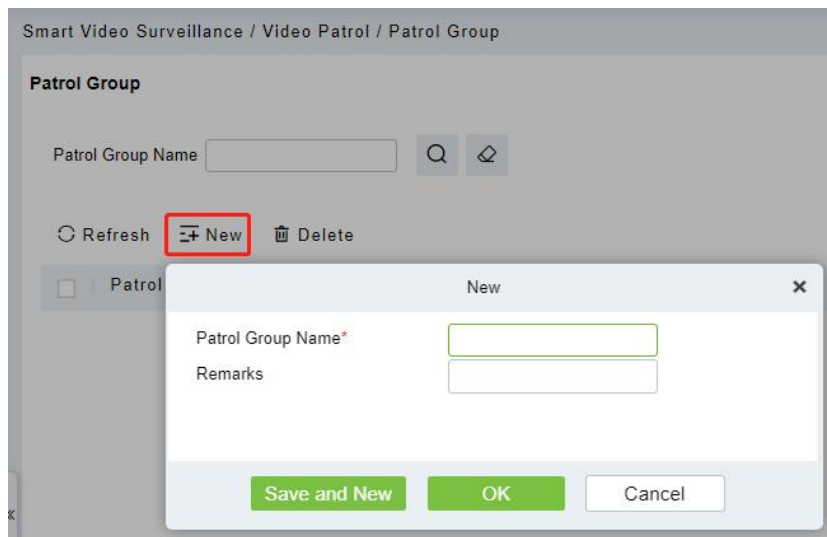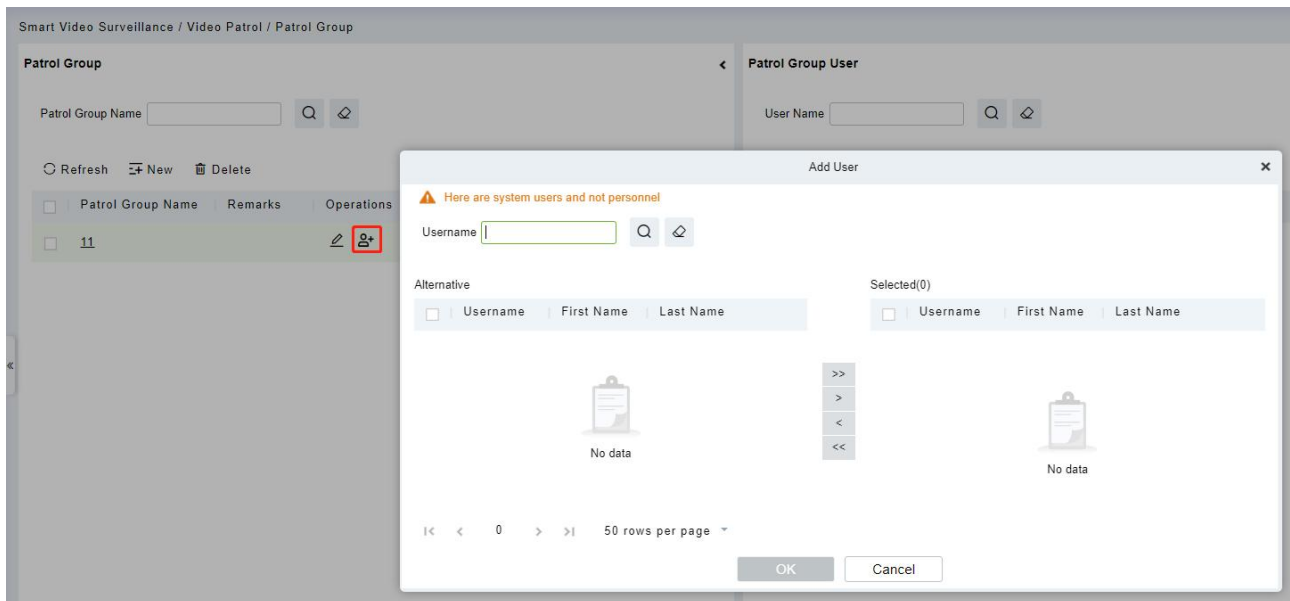Select the required patrol users and click the **[OK]** button to complete the addition. The added users will be displayed in the group member list on the right.

✎**Note:** Patrol users are users of the system. For adding users to the system, please refer to Adding Users.

6.6.2 Patrol Plan

Set a patrol plan for the patrol team.

Click **[Smart Video Surveillance] > [Video Patrol] > [Patrol Plan]**.
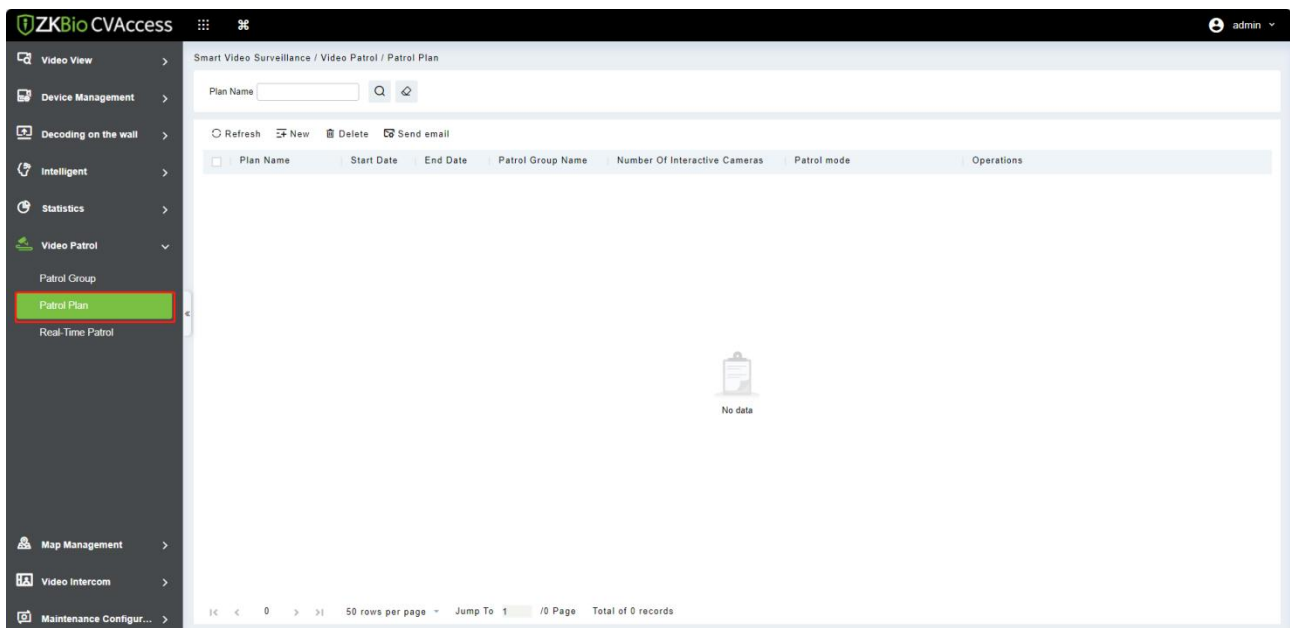
6.6.2.1 Add Patrol Plan

1.   Click **[New]**.

Field Description:

- **Plan Name:** Give the plan a name, make it easy to view and find, not repeatable.

- **Patrol Group:** Optional created patrol group.

- **Start Date:** Set the start date of the patrol. The start date must not be less than the end date.

- **End Date:** Set the end date of the patrol. The start date must not be less than the end date.

- **Patrol Time:** Drag the time bar to select the time period that needs to be patrolled. Multiple copies are supported.

2.   After editing this page, click **[Next]** to enter the camera selection interface.

Field Description:

- **Number of interactive Cameras:** Set the number of cameras that need to be chick-in, (like "5" means that Chick-in must be completed on 5 cameras during this patrol plan, this number must be less than or equal to the number of cameras you have chosen)

- **Channel Name:** Search the channel

- **Device List:** Select the equipment on the map that needs to be patrolled. The device list shows only the devices that have been added to the current map, if you want to add a device, go to Device Add

- **Map:** Select the map that needs to be patrolled.

✎**Note:**

1) You can set the length of time you need to watch each camera by clicking on the cruise time, which is 30 seconds by default.

2) The camera used in the patrol plan needs to be added in the center of the map.
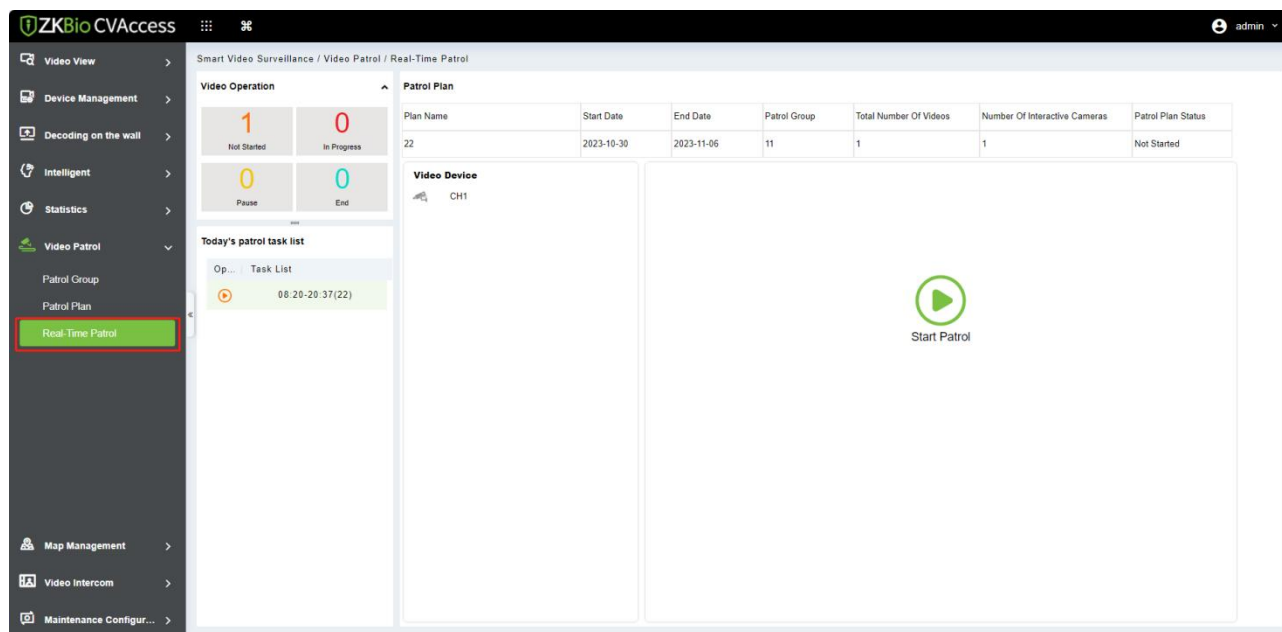
6.6.2.2 Delete

Select the Patrol Plan to be deleted and click the **[Delete]** button.

✎**Note:** Ongoing or pause plans cannot be deleted, please complete the plan first.

6.6.3 Real-Time Patrol

Click **[Smart Video Surveillance] > [Video Patrol] > [Patrol Plan]**. Online patrols are only available if the patrolman is logged into the system.

➢ **Video Operation**

View different states of the Patrol plan.

➢ **Today's Patrol Task List**

Displaying the patrol plan, click to patrol.

➢ **Patrol Plan**

After clicking **[Start Patrol]**, the video patrol will start. The map will display all cameras on the patrol route, as shown in the figure below:

✍**Note:**

1) You need to add a camera in the center of the map in advance.

2) The camera points in the list are connected on the map to form a patrol route.

3) A red dot on a camera indicates a camera on patrol.

➢ **Patrol Window**

When the camera is patrolling, the floating window on the map will display real-time images.

6.7 Map Management

Click **[Smart Video Surveillance] > [Map Management]**. Click **[New]** to add a E-map, then you can click **[Add Camera].** Add the cameras to the map, then adjust the position and **[Save position]**.
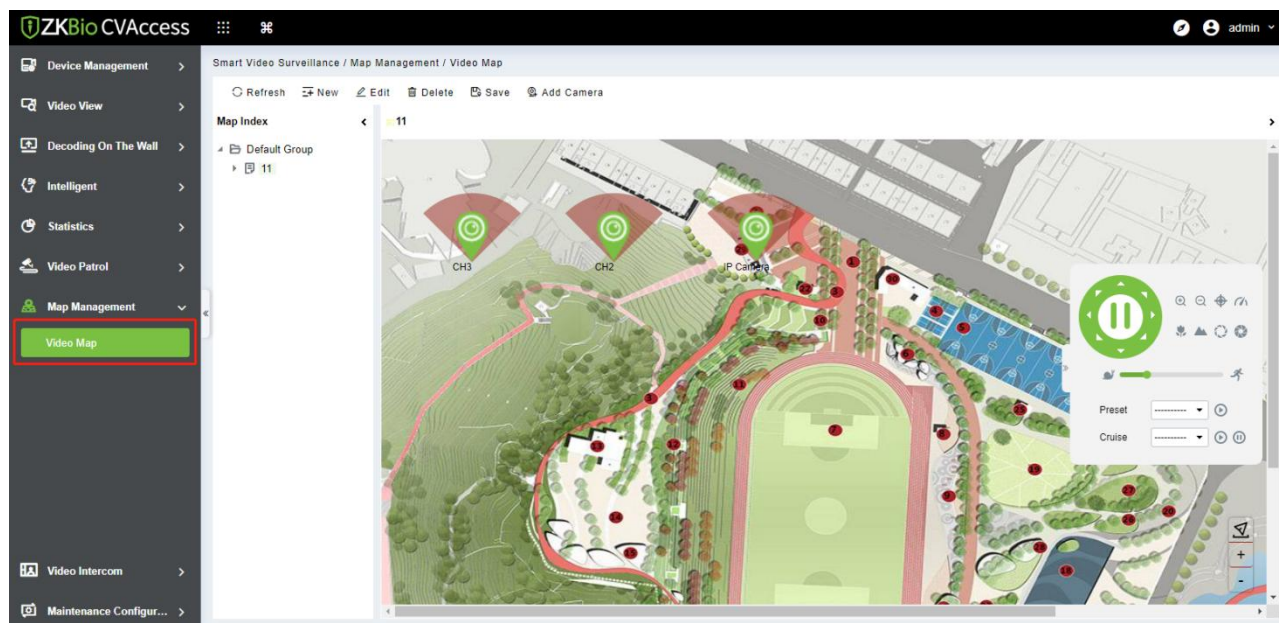
Meanwhile, the camera can be controlled through pan tilt.

6.8 Maintenance Configuration

6.8.1 Developer Log

Click **[Smart Video Surveillance] > [Maintenance Configuration] > [Developer Log]**, then click **[One-Click Collection]** to download all system logs and system information.
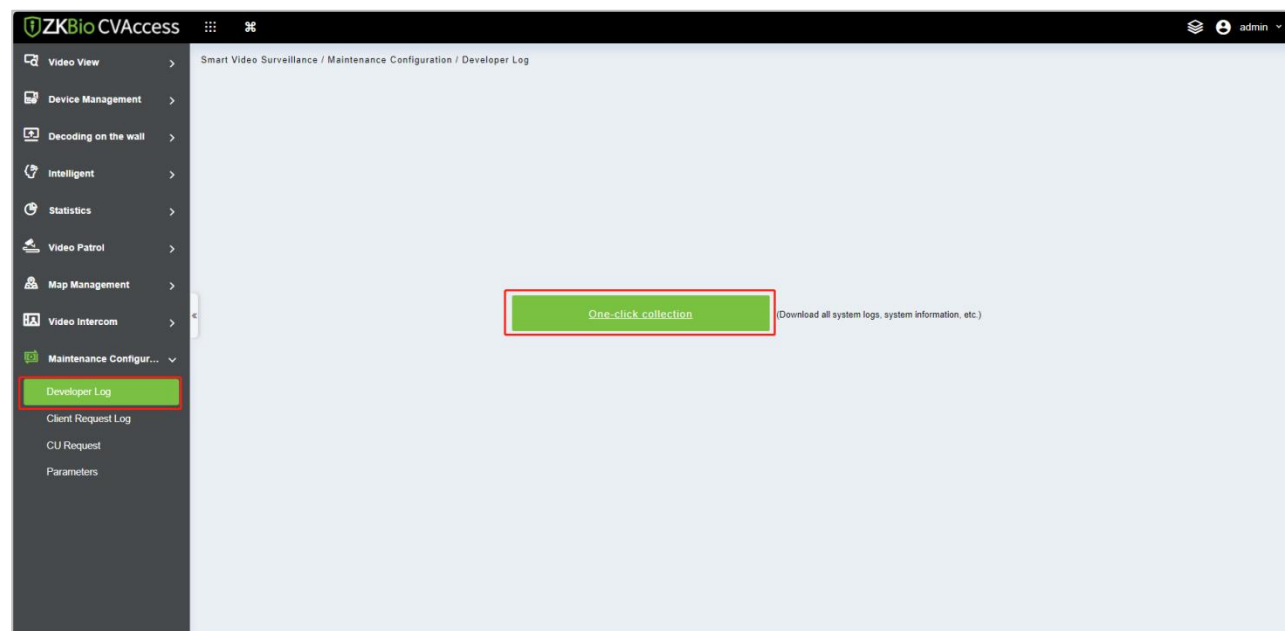
6.8.2 Client Request Log

Click **[Smart Video Surveillance] > [Maintenance Configuration] > [Client Request Log]**.
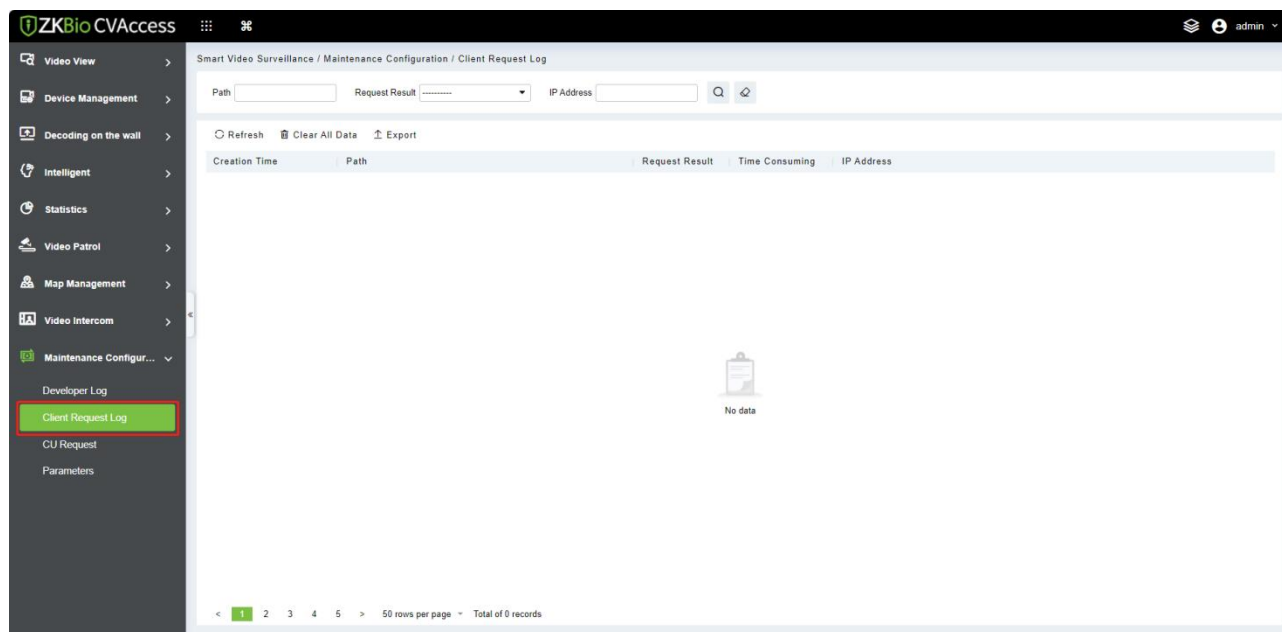
➢ **Clear All Data**

Click **[Clear All Data]** to pop up the prompt and click **[OK]** to clear all data operations.

➢ **Export**

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

6.8.3 CU Request

Click **[Smart Video Surveillance] > [Maintenance Configuration] > [CU Request]**.
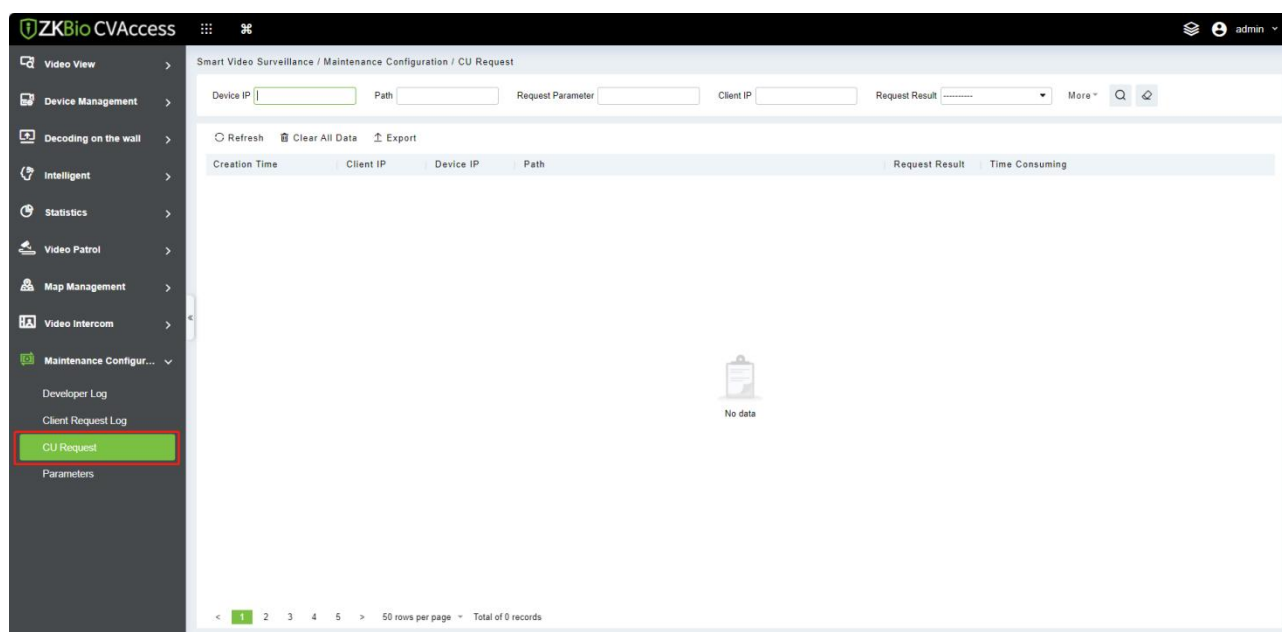
➢ **Clear All Data**

Click **[Clear All Data]** to pop up the prompt and click **[OK]** to clear all data operations.

➢ **Export**

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

6.8.4 Parameters

Click **[Smart Video Surveillance] > [Maintenance Configuration] > [Parameters]**. Set up all the settings, then click **[OK]**.
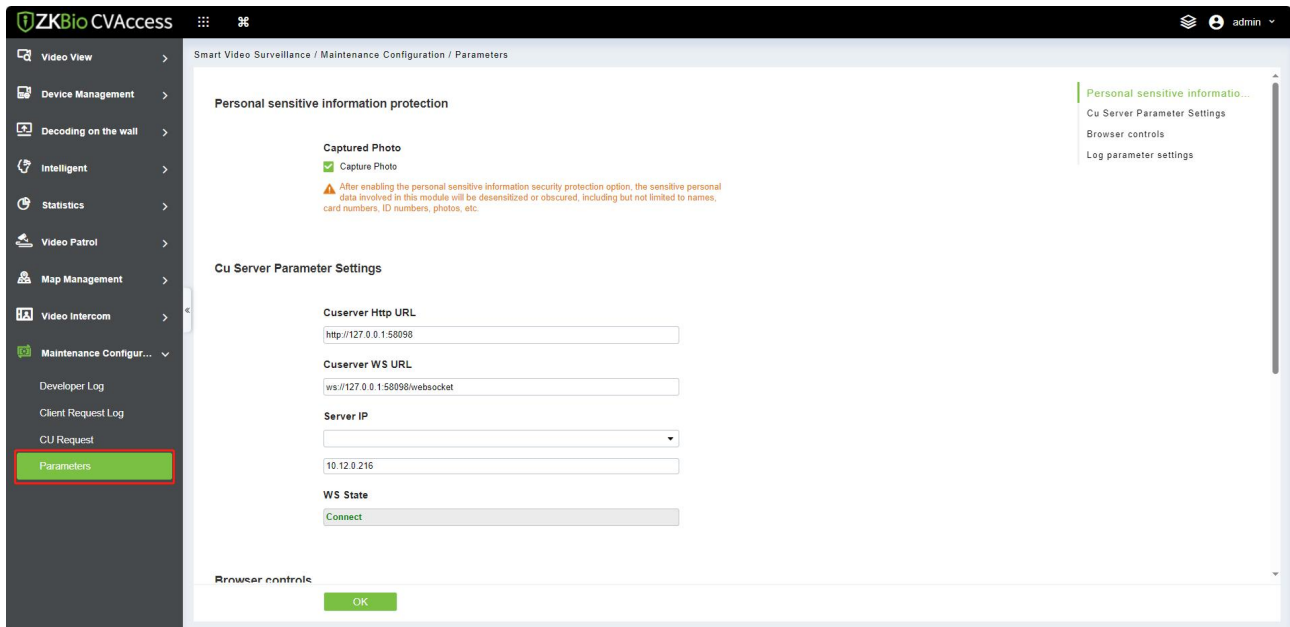
Field Description:

- **CU Server Parameter Settings:** Set Up CU server HTTP URL and WS URL and enter Server IP address then can view WS state.

- **Browser Controls:** Set up the File Storage location and change and restore the path

- **Log Parameter Settings:** Set Up the debug log and Access log, and select Yes/No.

7 Video Intercom

7.1 Basic Management

This module describes how to configure basic settings in ZKBio CVAccess.

7.1.1 Building

7.1.1.1 Add Building

To perform the following steps, to add a building:

Step 1: On the Video Intercom module, click on "**Basic Management > Building**".

Step 2: Click on the **New**, and the page for adding a building will be displayed.

Step 3: On the page for adding buildings, configure the required details as shown in the figure below, and adjust the parameter settings as indicated in the same figure.
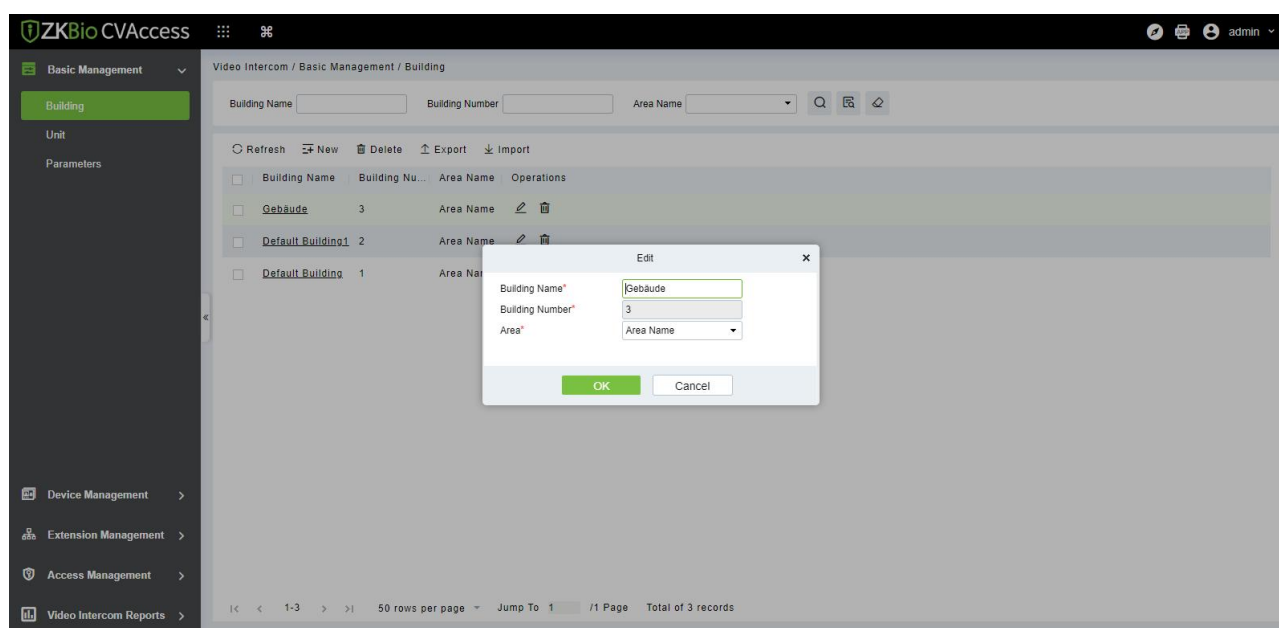
Parameter	Description
Building Name	Enter the name of the building.
Building Number	Enter the number of the building.
Area	Select the area name.

7.1.1.2 Delete

On the Building interface, select the building, click on the **Delete**, then a confirmation pop-up, and click **OK** again to confirm and permanently remove the selected building from the list.

7.1.1.3 Edit

The edit function allows users to modify existing building details within the application.

Select the Building, click on **Edit**, and then, click **OK** after modifying the building details.

7.1.1.4 Import

Import floor data in batches using the provided template.

7.1.1.5 Export

Device information can be exported in EXCEL, PDF, CSV file format.

7.1.2 Unit
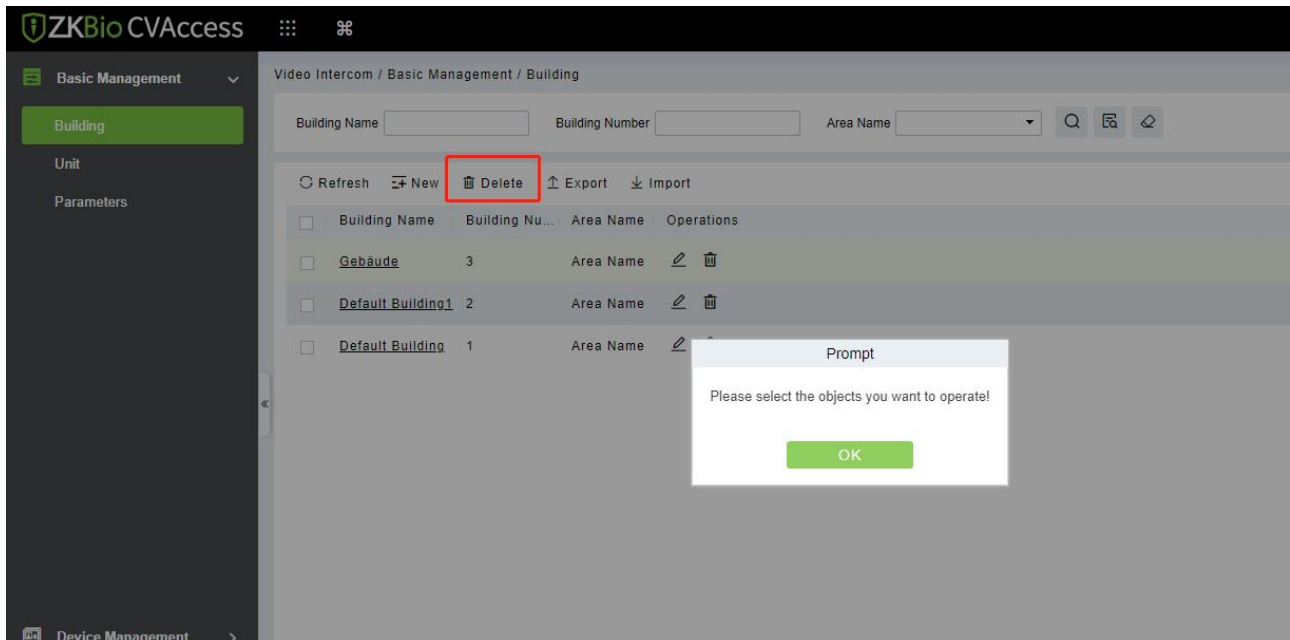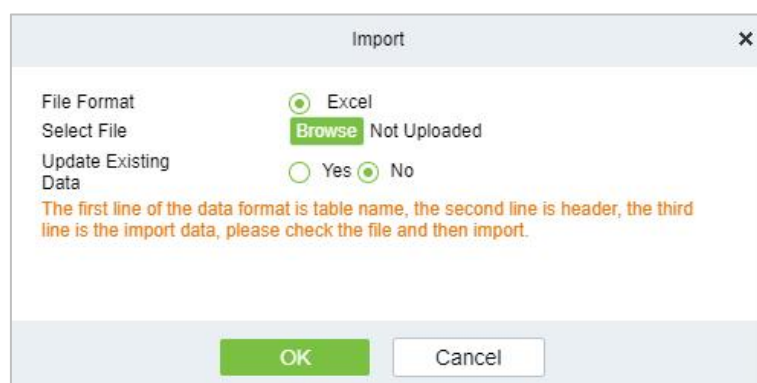
7.1.2.1 Add Unit

To perform the following steps, to add a unit:

Step 1: On the Video Intercom module, click on "**Basic Management > Unit**".

Step 2: Click on the **New**, and the page for adding a unit will be displayed.

Step 3: On the page for adding units, set the required content as shown in the figure below.

Parameter	Description
Unit Name	Enter the name of the unit.
Unit Number	Enter the unit number.

Parameter	Description
Belonging Building	Select the belonging building.

7.1.2.2 Delete

The Delete function allows the user to remove existing units from the application.

On the unit interface, select the unit then click **Delete**. A confirmation pop-up will appear, click **OK** to confirm and permanently remove the selected unit from the list.
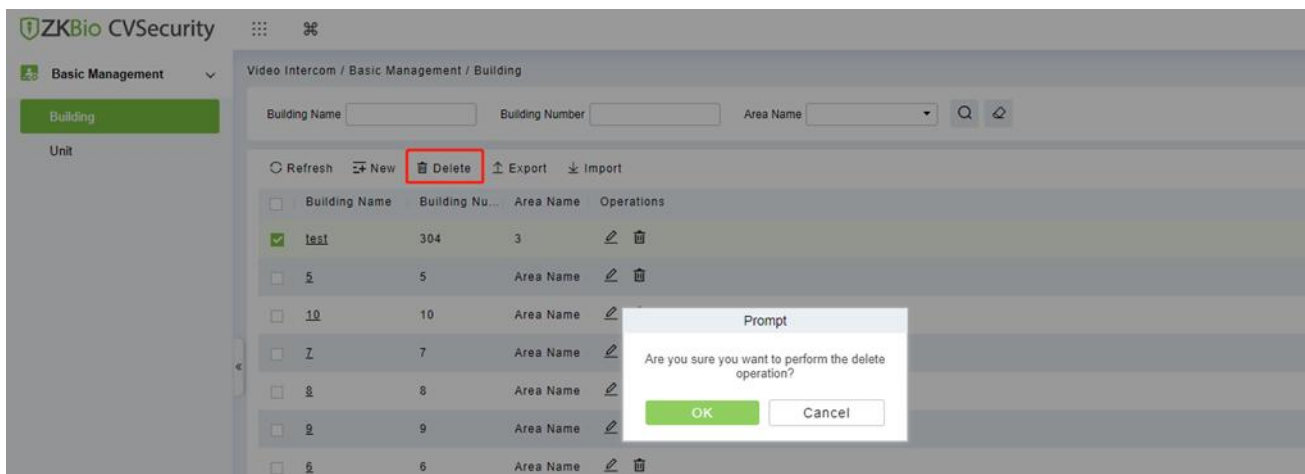
7.1.2.3 Edit

The edit function allows users to modify existing unit details within the application.

Select Unit, click **Edit**, and then click **OK** after modifying the unit details.

7.1.2.4 Export

Device information can be exported in EXCEL, PDF, CSV file format.

7.1.2.5 Import

Import floor data in batches using the provided template.

7.1.3 Parameter

This menu is used for configuring DTMF.

DTMF (Dual-Tone Multi-Frequency) is a telephone communication technology for sending signals through telephone key presses. After configuring DTMF in this menu, the command will be synchronized with the connected devices and apps. This synchronization is used to match the door-opening command between the app and the device, facilitating direct door opening via the app.
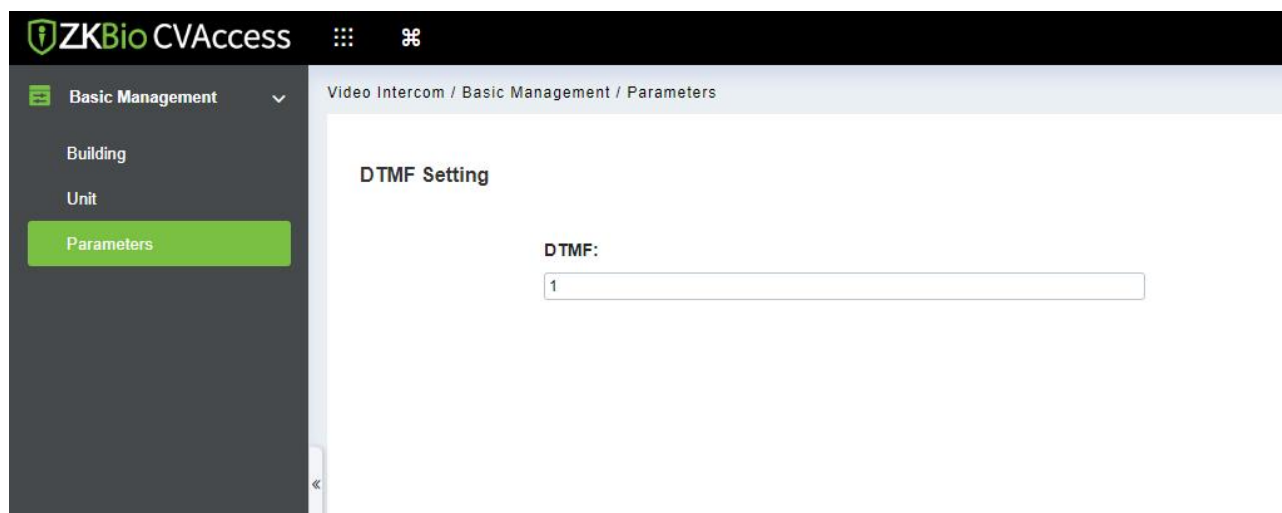
The "SIP Service Mode" option in System → Cloud Settings has been hidden.

A new "SIP Service Mode" option has been added to Video Intercom → Parameters .
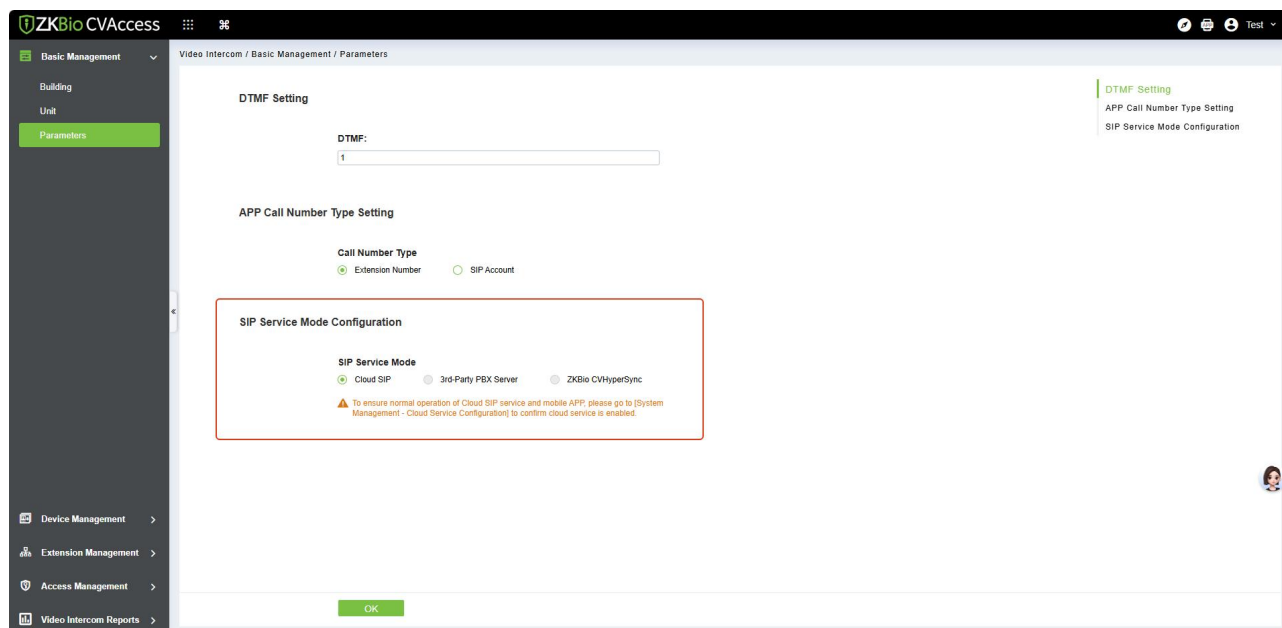
7.2 Device Management

7.2.1 Device Operation Guide

7.2.1.1   Add Devices

To perform the following steps, to add a device:

Step 1: Click on **Access Module > Device > Device**.

Step 2: Click **New** to add a device, for more detailed operations, please refer to chapter 4.1.1.

Step 3: After adding devices in the Access module, the support video intercom will automatically

sync with the Video Intercom module. Currently supported device models include SenseFace 7A/7B and SpeedPalm V5L.
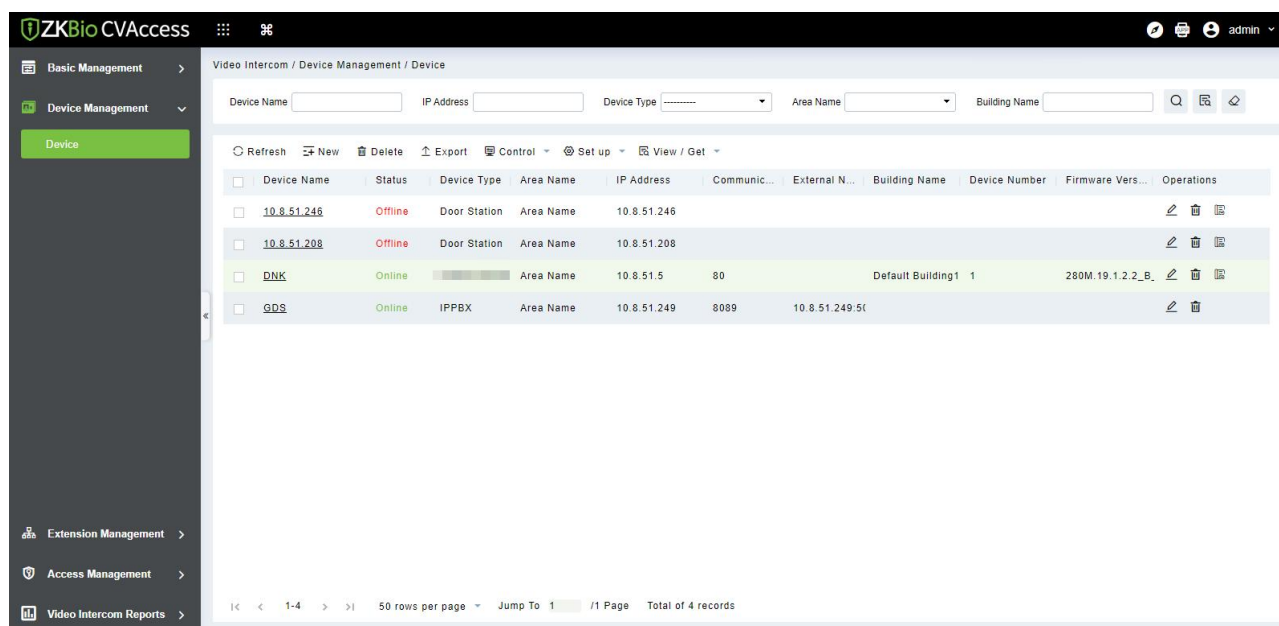
7.2.1.2 Delete
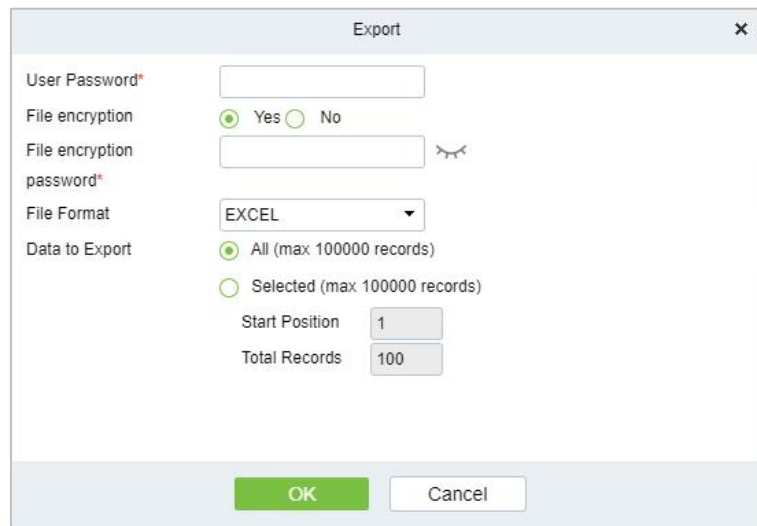
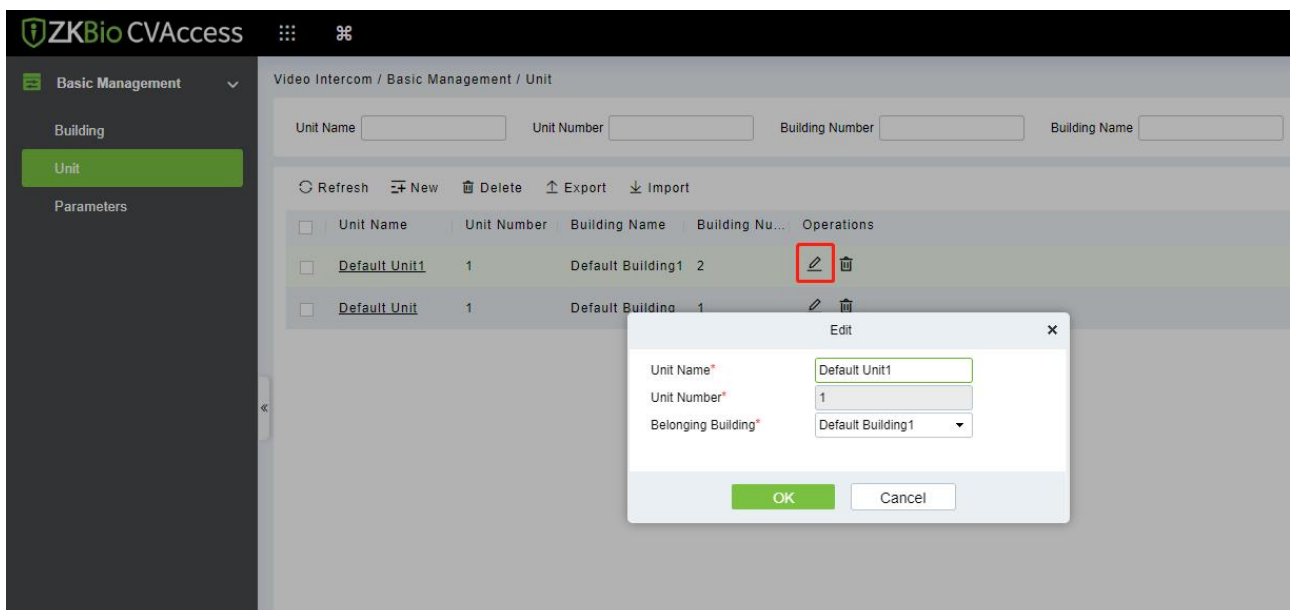The Delete function allows the user to remove existing devices from the application.

On the device interface, select the Device then click **Delete**. A confirmation pop-up will appear, then click **OK** to confirm and permanently remove the selected device from the list.
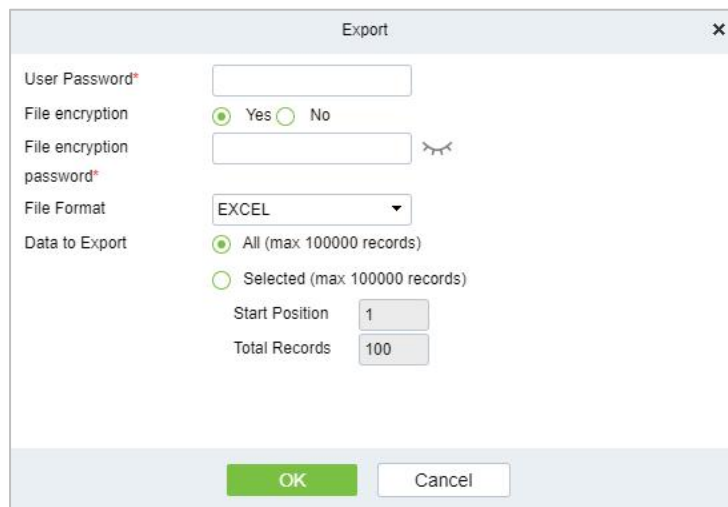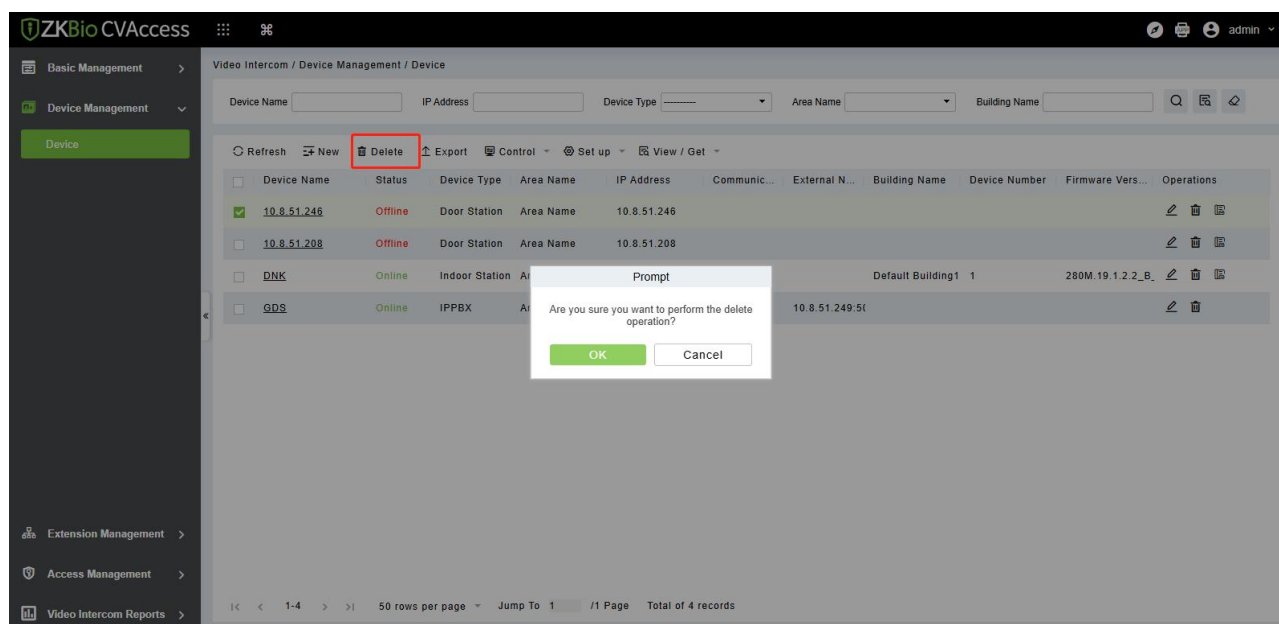

7.2.1.3 Export

Device information can be exported for all transactions in Excel, PDF, and CSV format.

7.2.1.4 Control

● Reboot Device

It will reboot the selected device.

● Synchronize Time

It will synchronize device time with the server's current time.

● Synchronize People Data

Synchronize data of the system to the device. Select device, click **Synchronize People Data** and click
OK to complete synchronization

7.2.1.5 Set up

● Add Extension

It will add the extension for the device.

● Add Address Book

It will add the address book to the device.

● Upload Media Files

Click to upload the media files for the device.

7.2.1.6 View/Get

● View Extension

Select the device and click View Extension to get the device extension data.

● View Address Book

Select the device and click View Address Book to access the device address details.

● Get Record

Select a device and click Get Records to access the device data.

● Device Web Service

Select a device and click Device Web Service to get the web service details of the device.

7.2.2 IPBX Device Operation Guide

This device type is used to assign SIP accounts to devices and the APP for SIP protocol-based video intercom applications. Before using this feature, you need to purchase a GDS PBX server from ZKTeco. If you prefer not to purchase IPBX server hardware, you can subscribe to our cloud SIP. The following steps provided operational instructions for the GDS PBX service.

● GDS Device

To perform the following steps, to add a GDS device:

Step 1: Click on the **Video Intercom > Device Management > Device**.

Step 2: Click **New**, and the page for adding a GDS Device will be displayed.

Step 3: Manufacture: Select **GDS** and add the corresponding parameters.

Parameter	Description
Device Name	Customize the name of the server.
IP Address	Fill in the IP address of **PBX Server**.
Communication Port	Fill in the Port of **PBX Server**.
Username	The username of PBX Server.
Administrator Password	Fill in the administrator password.
External Network Address	The address of the actual SIP communication (The port number is the default UDP port for SIP services).
Transport Protocol	Transport protocol for SIP, default is UDP.
Device Type	Device type, default is IPBX
Area	The area in which the PBX server is located

7.3 Access Management

This menu is used only for configuring and synchronizing access permissions for personnel entering and exiting for **DNK** device types.

7.3.1   Access Control Group

Access control groups define groups and categories of video intercom to facilitate subsequent permission assignment operations.

Setting operations includes creating access-level groups and adding doors to access-level groups.

7.3.1.1   Add Group

This section describes how to create steps for Access Control groups in the module of Video Intercom.

To perform the following steps, to add a group:

Step 1: On the Video Intercom module, choose "**Access Management > Access Control Group**".

Step 2: Click **New**, and the page for adding access control groups will be displayed.

Step 3: On the page for adding access control groups, set parameters based on the new requirements, as shown in the figure below.

Parameter	Description
Level name	Customize the name of the access control groups.
Description	Add description as needed.

Step 4: Click **OK** to finish configuring the access control right group.

7.3.1.2   Add Device

To perform the following steps, add a device:

Step 1: On the Video Intercom module, choose "**Access Management > Access Control Group>Add Device**".

Step 2: Click "**Add Device**", and the page for selecting a door will be displayed. Add a door as required, as shown in the figure below.
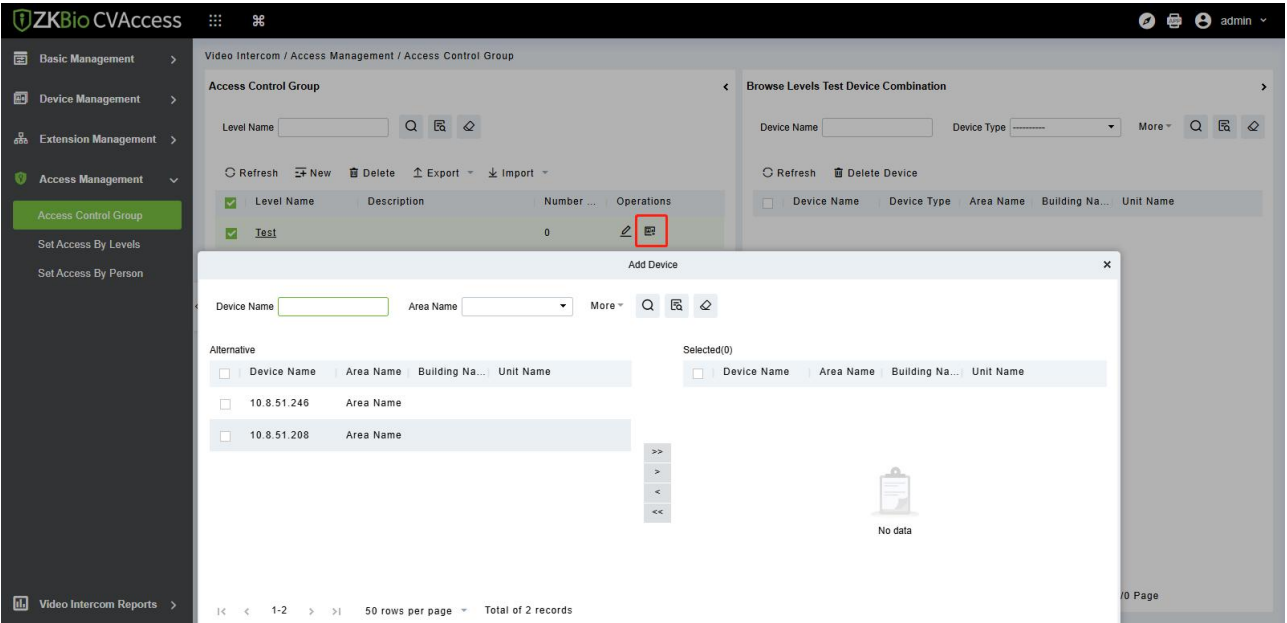
Step 3: Click **OK** to finish configuring the device for the video intercom right group.

Parameter	Description
Device Name	Enter the name of the device.
Area Name	Enter the name of the Area.

7.3.1.3 Delete Devices

The Delete function allows the user to remove existing devices from the application.

Select the device then click **Delete Device**. A confirmation pop-up, click **OK** to confirm and permanently remove the selected device from the list.
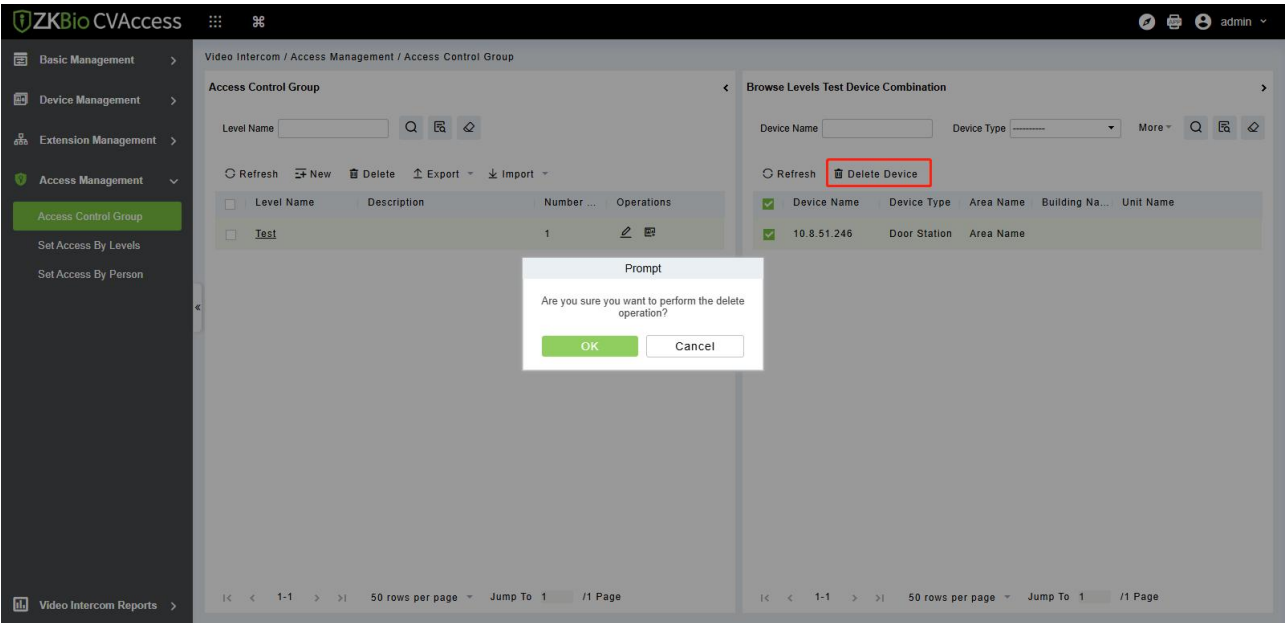
7.3.1.4 Export / Import

Export the permission group information of the Access Control Template:

In the Video Intercom Module, click **Access Management** > **Access Control Group**>**Export**>**Export Access Group**", then You can export doors of access level in Excel file format. Enter the user password in the displayed security verification dialog box and click **OK**. Select whether to encrypt the file and the file format to export, and Click **OK**.
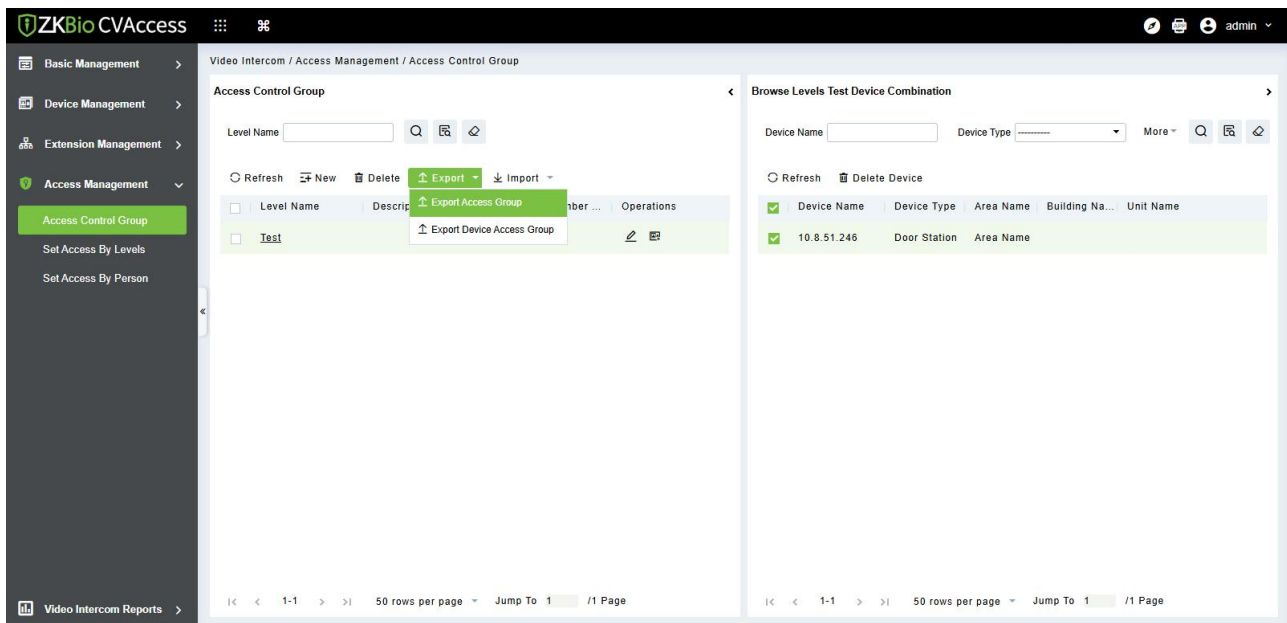
Export the device Access group of Access Control Template:
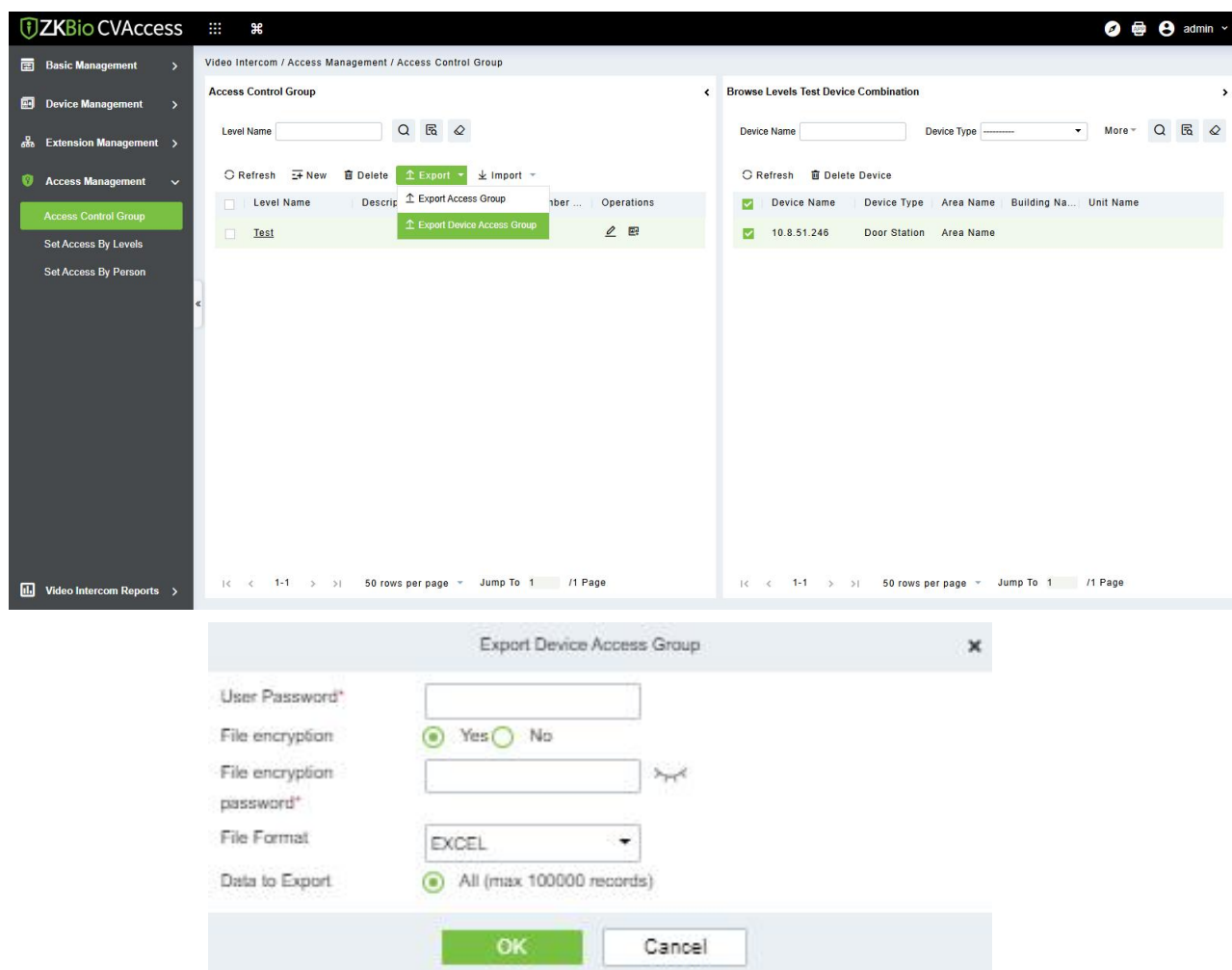
7.3.2 Set Access by Levels

This section describes the operation step that sets access by levels in the module of video intercom in ZKBio CVAccess.

7.3.2.1 Add Personnel

To perform the following steps to add personnel:

Step 1: On the Video Intercom module, choose "**Access Management**＞**Set Access by Levels** "

Step 2: Under the operation column of the corresponding permission group, click "**Add Personnel**". Then Add personnel page is displayed. Select personnel as required.
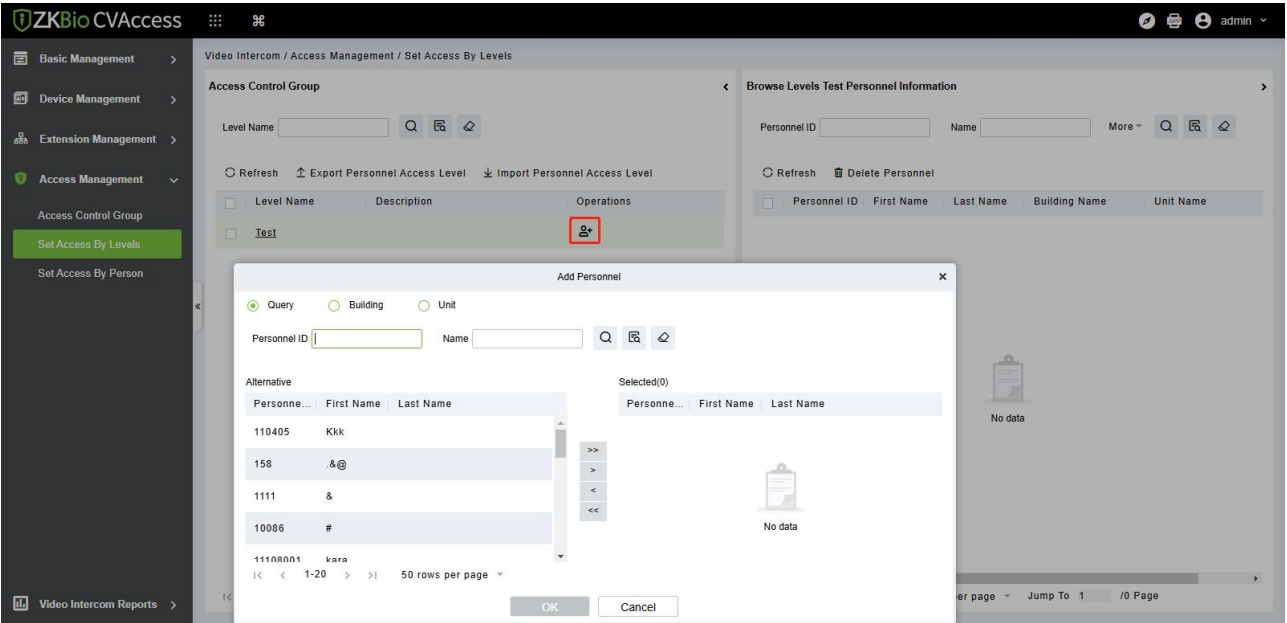
Step 3: Click **OK** to complete the assignment of personnel add.

Parameter	Description
Personnel ID	Enter the personnel ID.
Name	Enter the name of the person.
Building Name	Select the building name.
Unit Name	Select the unit name.

7.3.2.2 Export Personnel of Access Level

Click **Export**, enter the user password in the displayed security verification dialog box, and Click **OK**. Then choose whether to encrypt the file and the file format to export and click **OK**.
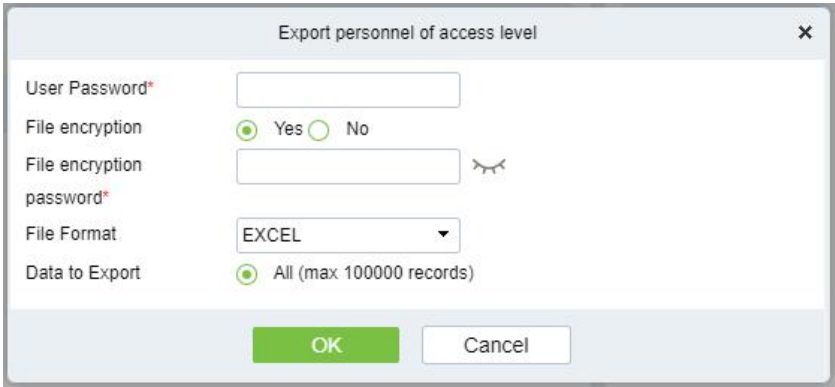
7.3.2.3 Import Personnel of Access Level

Click **Import** and then click **Browse** to select a file from the stored location. Finally, click **OK**.
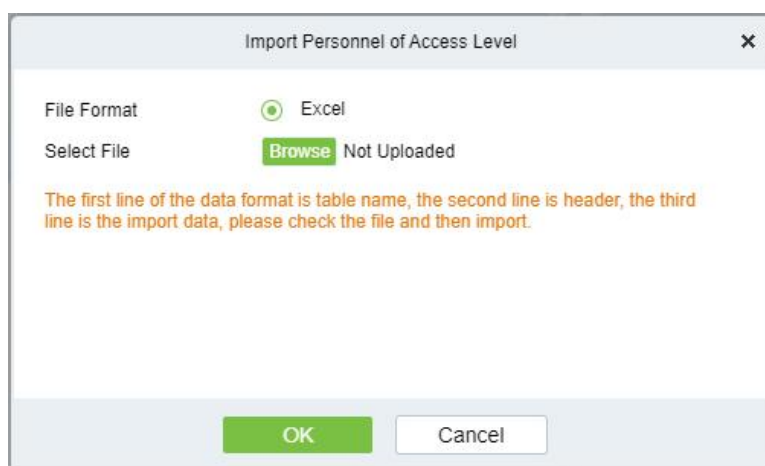
7.3.2.4 Delete Personnel

The Delete function allows the user to remove existing personnel from the application.

On the **Set Access By Level** interface, select the personnel then click **Delete**. A confirmation pop-up will appear, then click **OK** to confirm and permanently remove the selected personnel from the list.
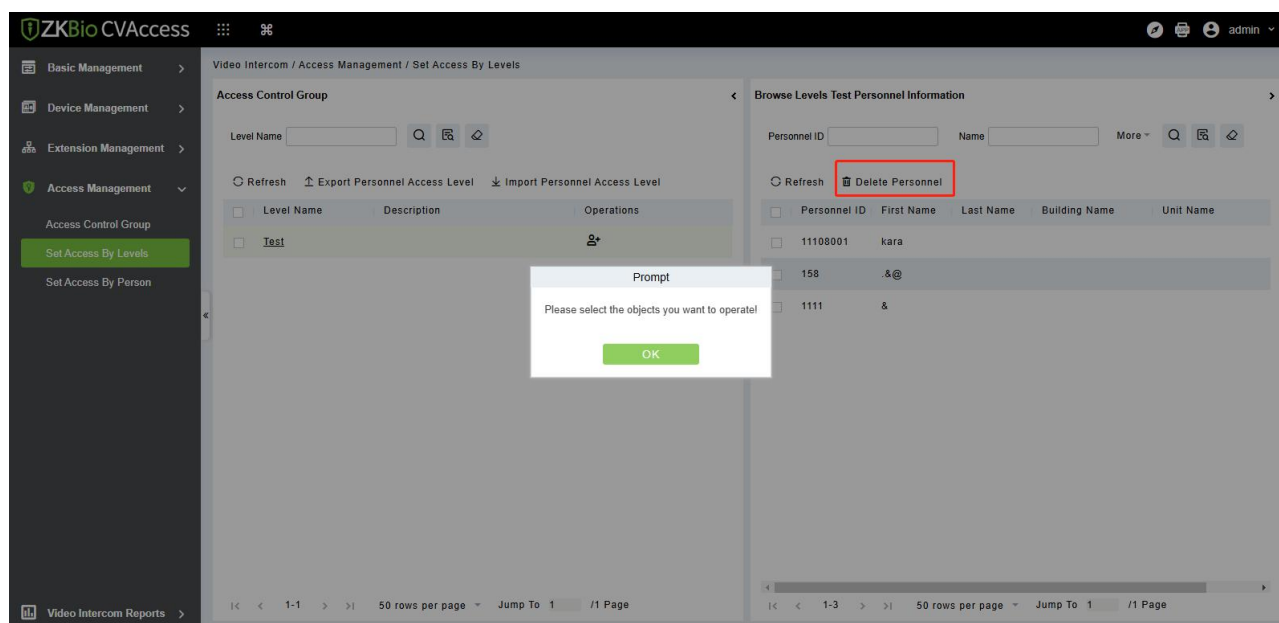
7.3.3 Set Access by Person

This section describes the operation step that set access by the person in the module of video intercom in ZKBio CVAccess.

7.3.3.1 Add Personnel

To perform the following steps, to add personnel:

Step 1: On the Video Intercom module, choose **Access Management>Set Access by Person**.

Step 2: Under the operation column of the corresponding permission group, click "**Add to Levels**".

The Add level page will be displayed. Select the level as required.


Step 3: Click **OK** to complete the assignment of personnel add.

Parameter	Description
Level Name	Enter the name of the level for the person.

7.3.3.2 Export

Click **Export**, enter the user password in the displayed security verification dialog box, and Click **OK**. Then choose whether to encrypt the file and the file format to export and click **OK**.
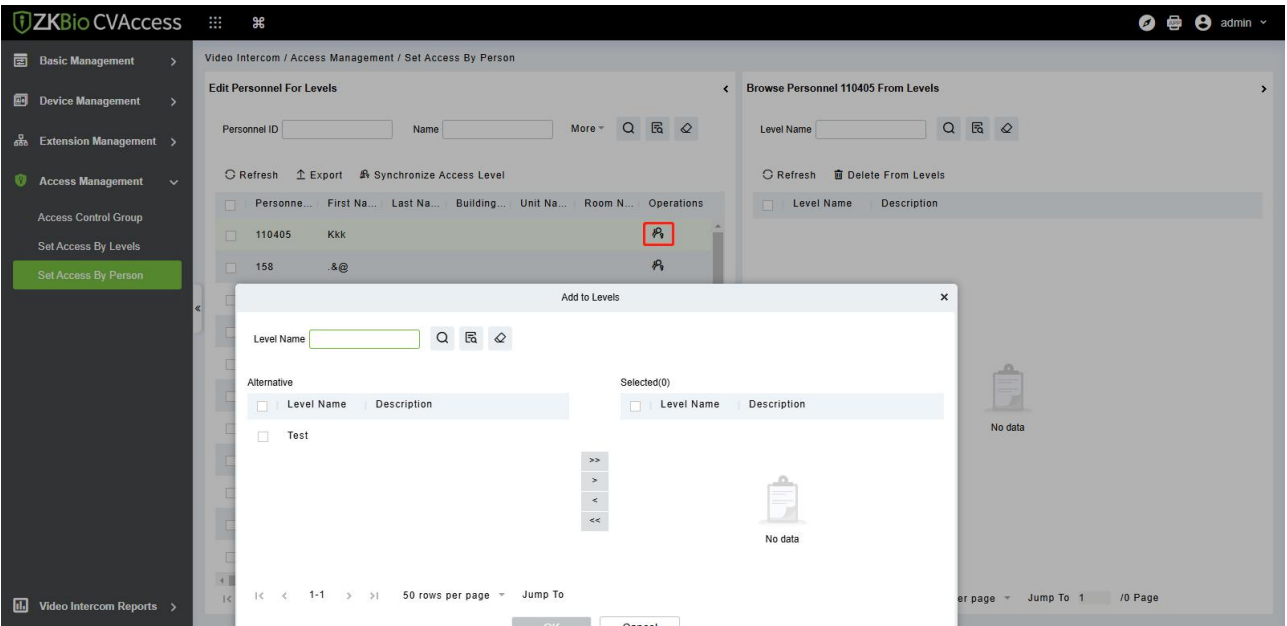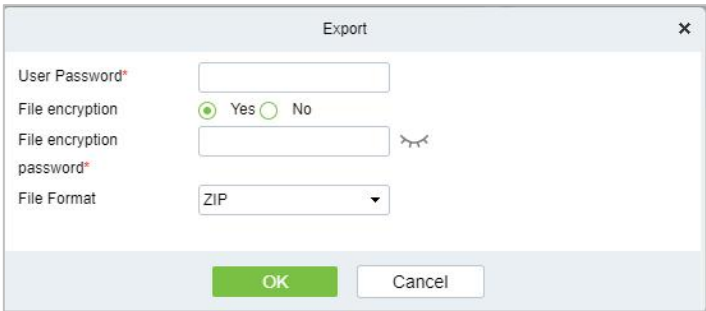

7.3.3.3 Synchronize Access Level

Select the level to be synchronized and send the corresponding device area data in the software to the device.

7.3.3.4 Delete from Levels

The Delete function allows the user to remove existing levels from the application.

On the **Set Access By Person** interface, select the personnel then click **Delete**. A confirmation pop-up will appear, then click **OK** to confirm and permanently remove the selected personnel from the list.
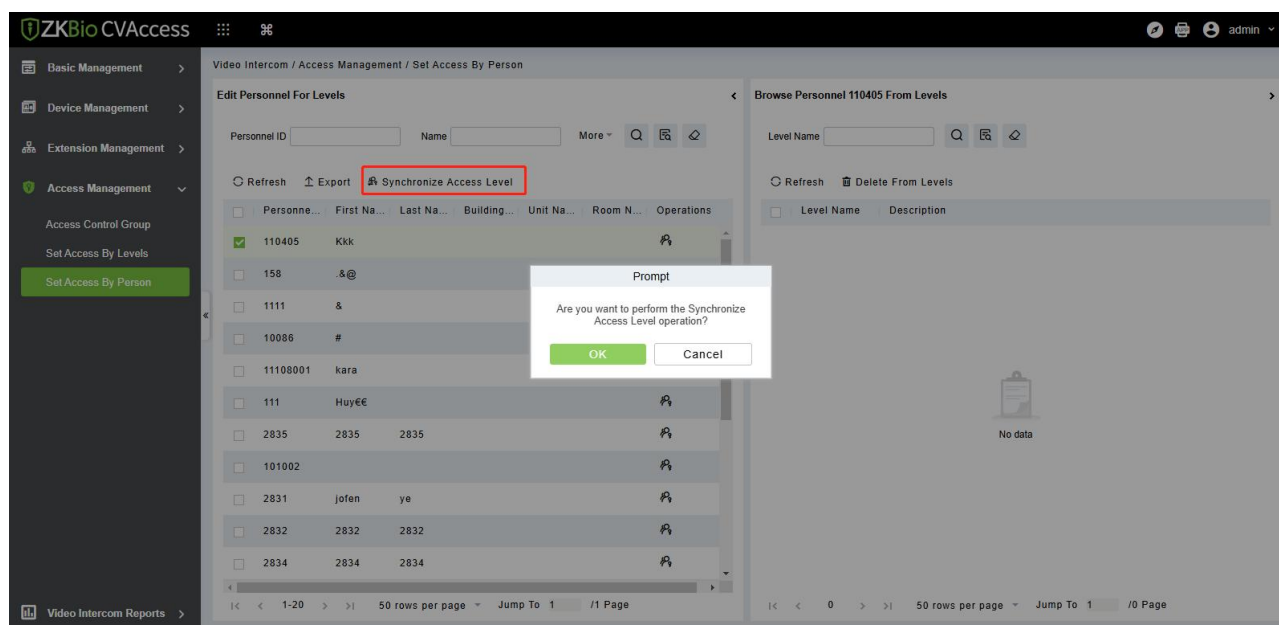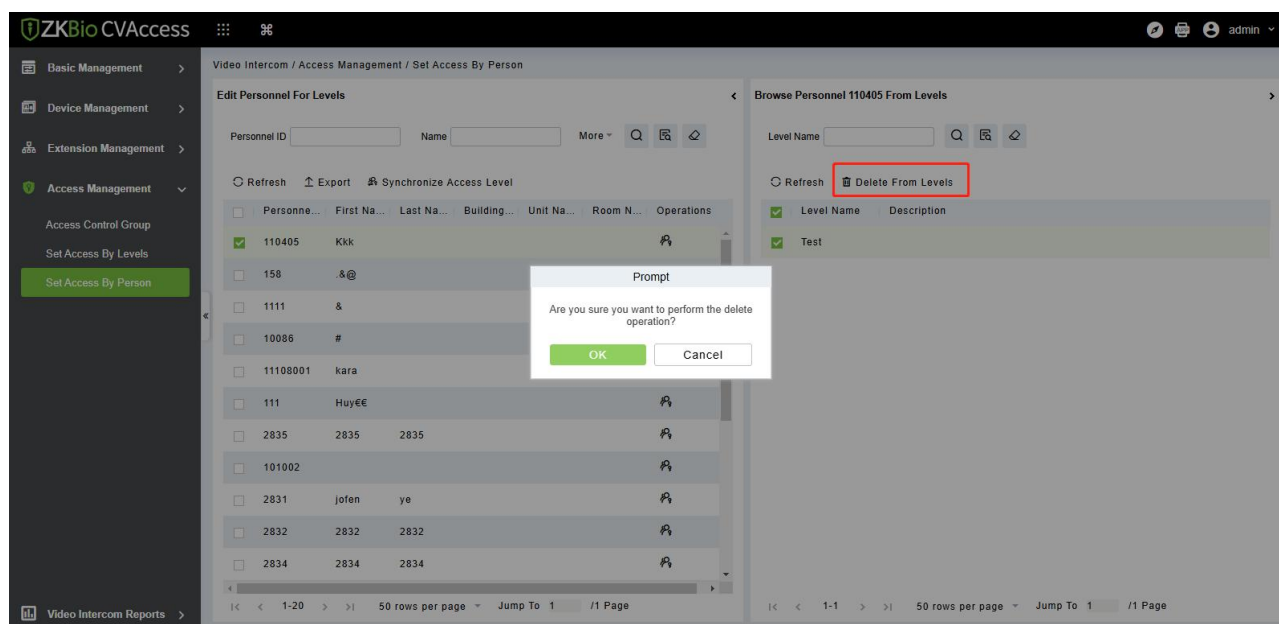

7.4 Extension Management

This module is used for managing and assigning extension numbers.

Prerequisite

ZKBio CVAccess supports two types of SIP servers:

- PBX Server: For addition and operation methods, please refer to <u>IPBX Device Operation Guide.</u>

- Cloud SIP: Enable Cloud Sip ,please refer to Cloud Setting.

7.4.1 Extension Number

An extension number is a code or number used within a company or organization to identify individual telephone sets, typically in internal telephone systems.

7.4.1.1 New

Click on **"New"** to add a single extension number. To add multiple extensions at once, use the "Import" function.

Parameter	Description
Name	Customize the extension name
Extension Type	Default communication type for SIP
Extension Number	Customize the extension number; for example, the number for Room 401, Unit 2, Building 1 can be defined as 12401 for easy internal recognition
Extension Password	Password for the extension
Voice Mail	Enable voicemail, this parameter is only valid for PBX servers
Voice Mailbox Password	The voicemail password for this extension, this parameter is only valid for PBX servers

Enable Undisturbed Mode	Enable the Do Not Disturb mode to ignore all incoming calls, this parameter is only valid for PBX servers
Incoming Calling Number	Caller ID number
Calling Name	Caller ID name
Direct Dialing Address	Intranet point-to-point call device IP; enter the IP here, and the call will be made to the direct dial address first; if the direct dial address is unreachable, then the call will be made through SIP; dual protection, effectively avoiding communication issues in case of network interruption or SIP server downtime.

7.4.1.2 Delete

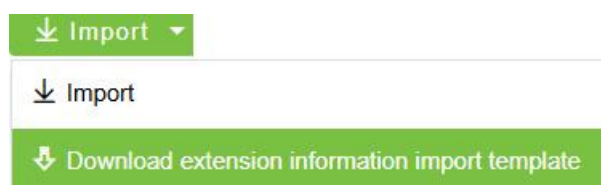On the **Extension Numbers** interface, select the extension name then click **Delete**. A confirmation pop-up will appear, then click **OK** to confirm and permanently remove the selected extension name from the list.
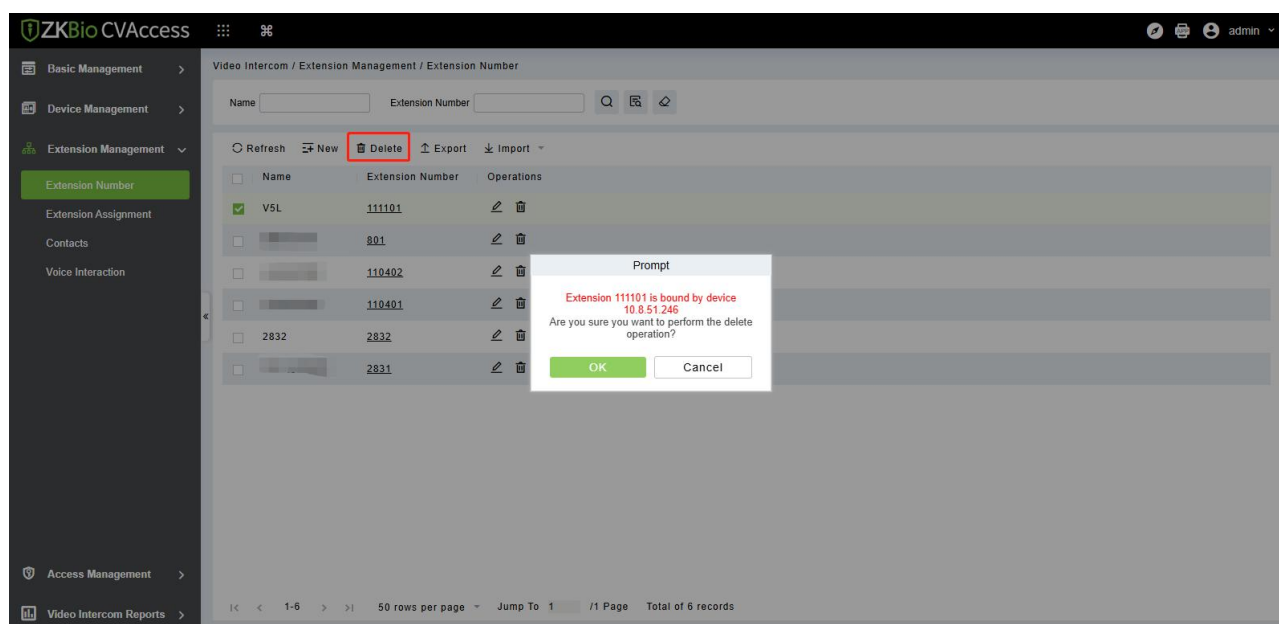
7.4.1.3 Import

User need to add extension numbers in bulk, user can use the Import function.

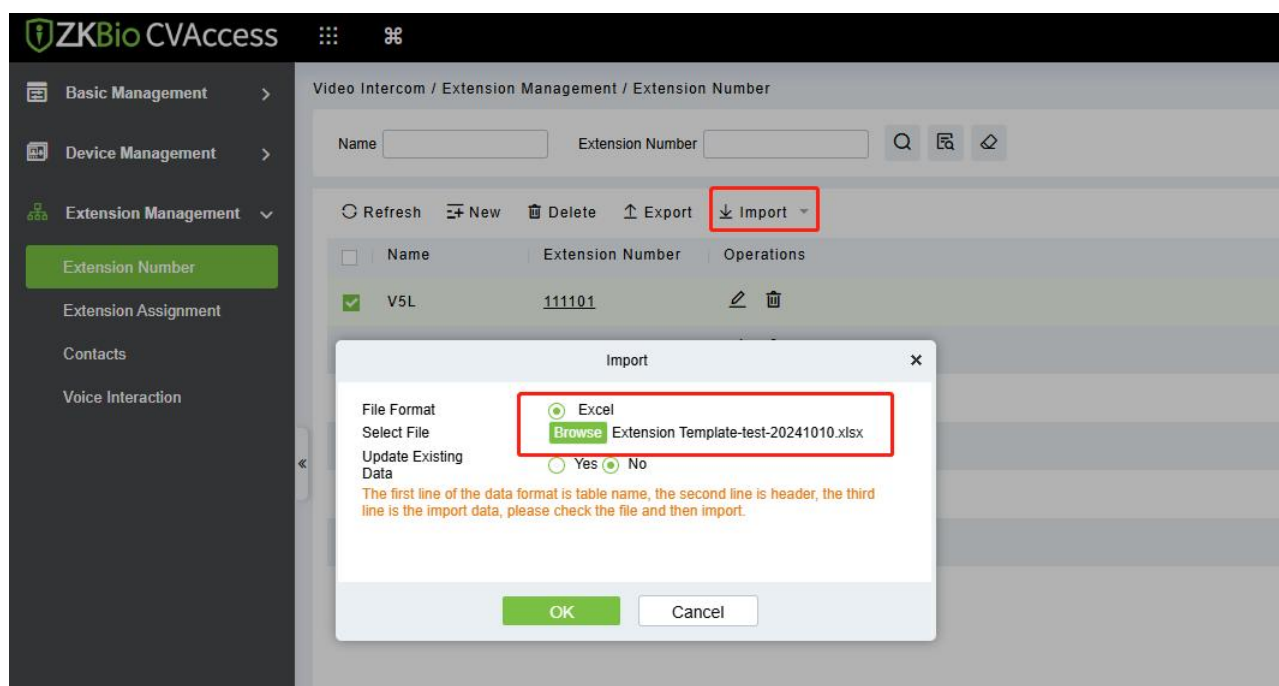**Step 1:** Download the import template by clicking **Import -> Import** template.

Step 2: Fill in the information into the import template.

Step 3: Click on **Import,** then click Browse to select the import template, and click **OK** to start the bulk import process.

Once the progress reaches 100%, user will be prompted with the results of the import, as shown in the figure below.
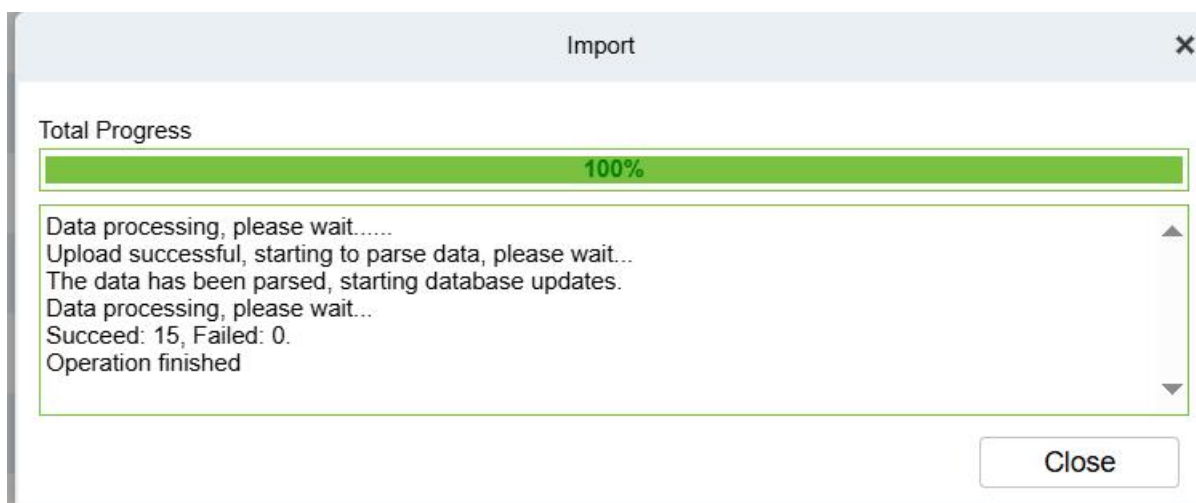
7.4.1.4 Export

Export the relevant information of the extension numbers.

7.4.2 Extension Assignment

This feature is designed to assign extension numbers to devices, personnel, and system users added to ZKBio CVAccess.
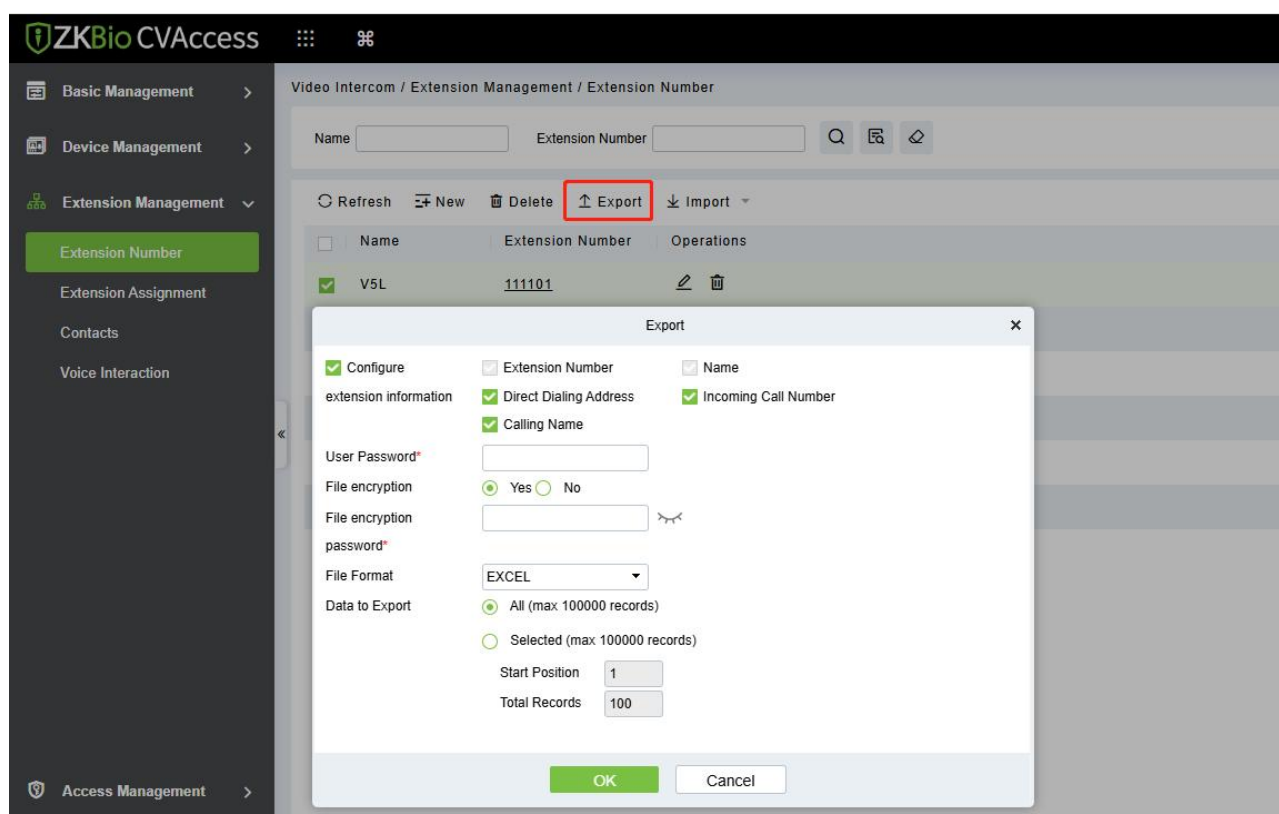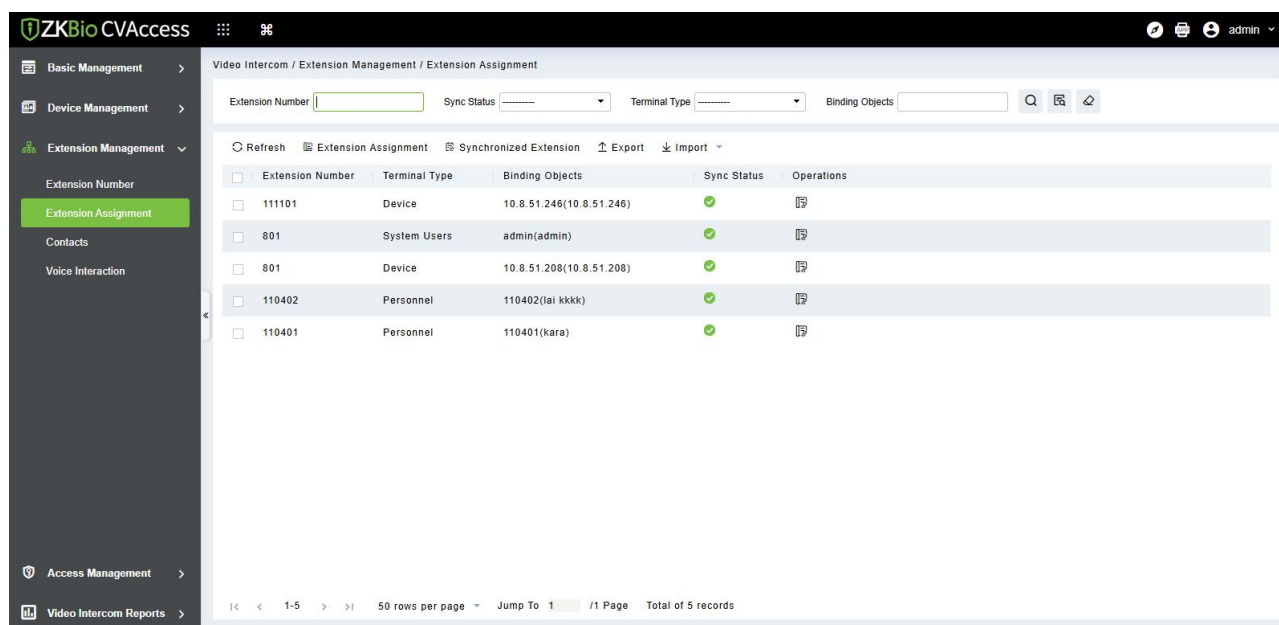
7.4.2.1 Extension Number Assignment

7.4.2.1.1 Assign Accounts to Devices

Select the Terminal Type from the drop-down list the as **Personnel, System users, Device**, then select the Personnel ID for the device you wish to bind, and select the Extension Number. The account information will be automatically synchronized to the device, eliminating the need for users to manually configure the address on the device.

Authorized Contacts: Assign the selected contact list to the device, enabling it to dial the short numbers or extension numbers within that contact list.

Note: SenseFace/SpeedPalm /DNK devices require a firmware upgrade to support the contact list functionality. User can refer to the hardware suggestion list for the required firmware versions.

Result Verification

In the device's visual intercom interface, under **"Account,"** the user can see that the SIP server and account information have been automatically written in, as shown in the figure below.
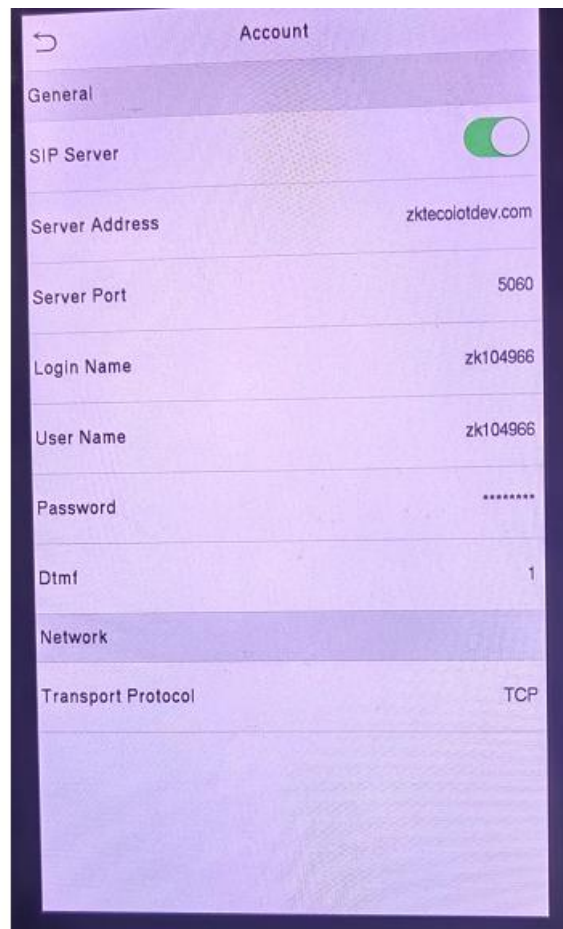
7.4.2.1.2   Assigning Accounts to Personnel (App)
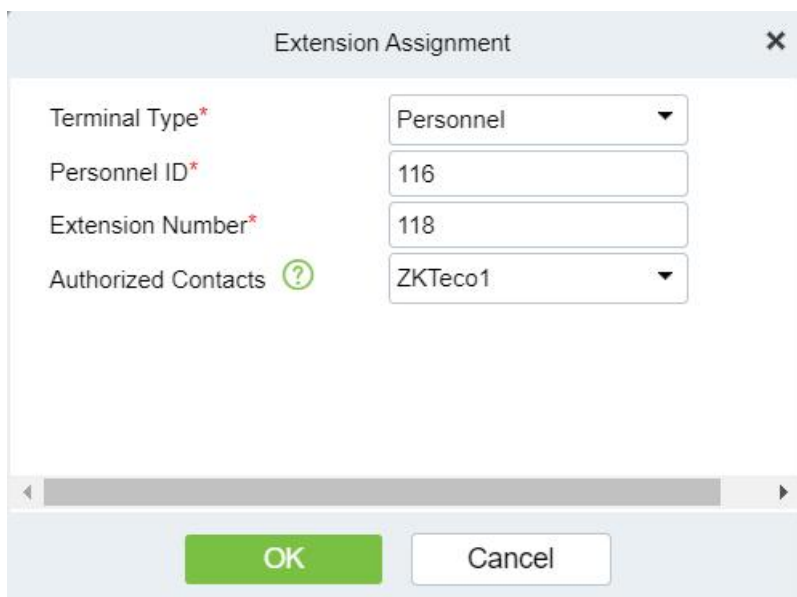
Terminal Type: Select "Personnel" as the Binding Type;

Personnel ID: Select the Personnel ID for the individual to whom you want to assign the account.

Extension Number: Select the extension number in the Extension Number field.

Authorized Contacts: After selecting the contact list, the contacts in that list will be automatically synced to the APP.
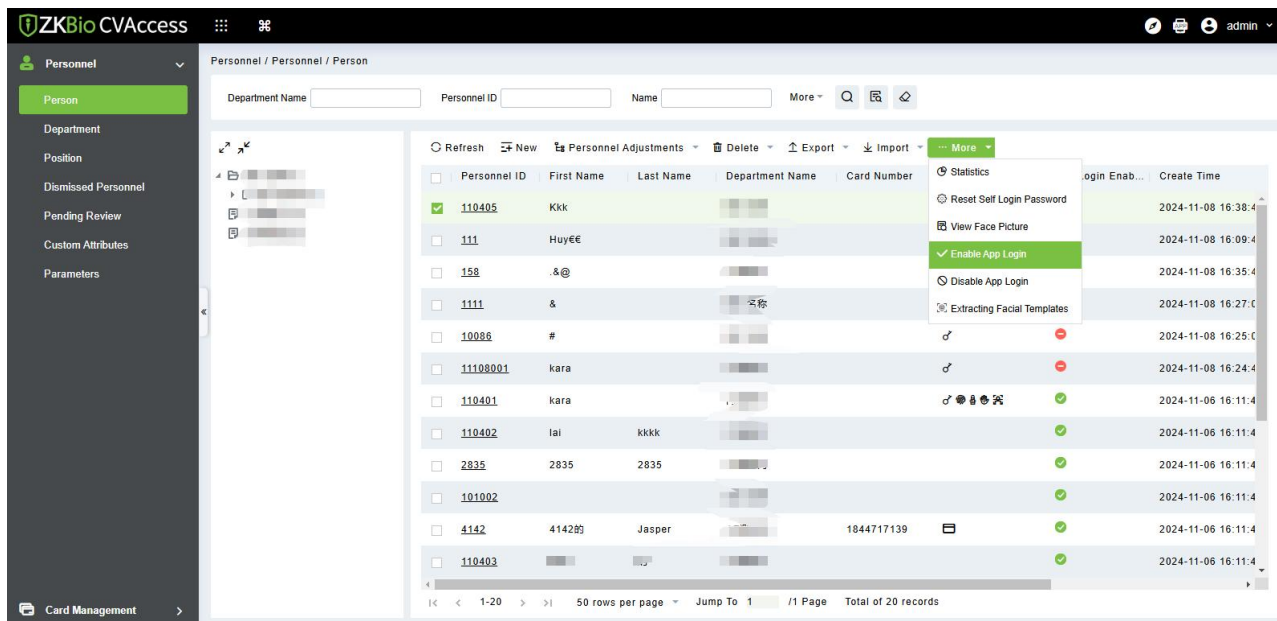
Once the personnel enable APP Login, they can log in and immediately use the APP for visual intercom communication.

Result Verification:

After the personnel logs into the APP and enters the Video Call application, the interface status will display as "**Connected**"; if the personnel have not been assigned an extension number, entering the application will prompt "You have not been assigned an extension number, please contact the administrator."
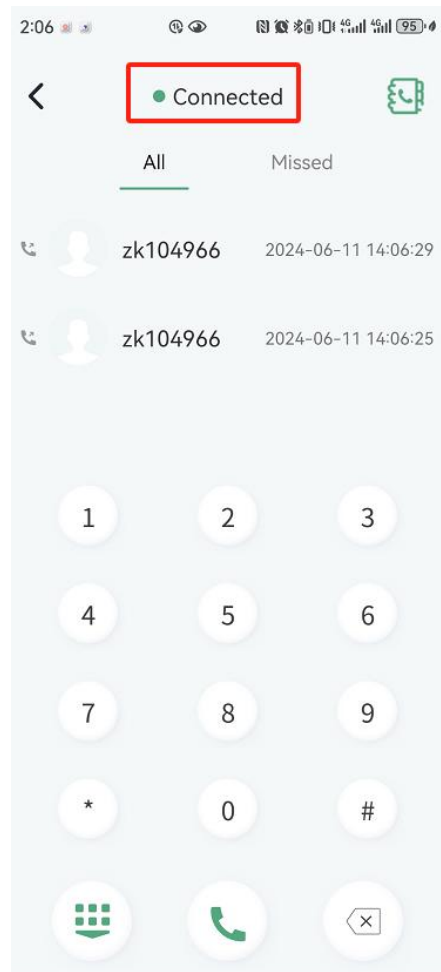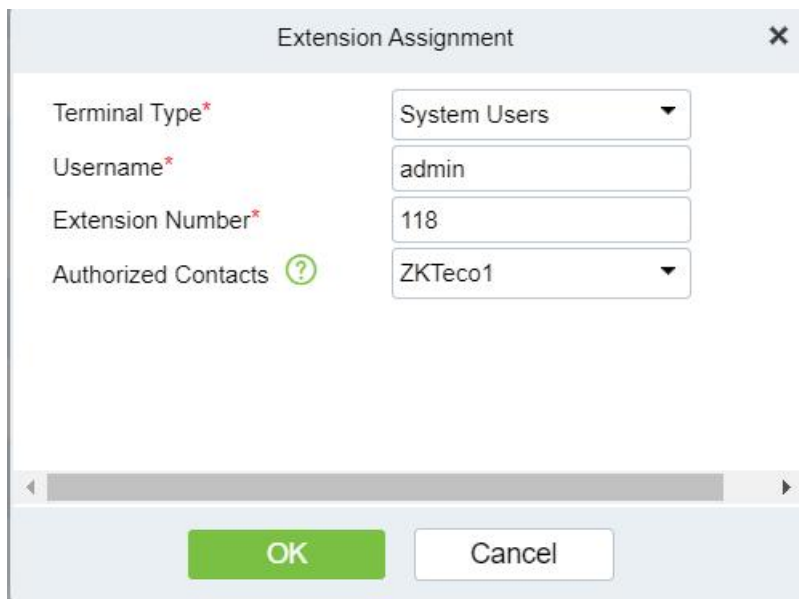
7.4.2.1.3   Assigning Accounts to System User (App)

Terminal Type: Select "System User".

Username: Choose the system user to whom the account needs to be assigned.

Extension Number: Select the extension number.

Authorized Contacts: Assign the contact list to the system user; after the assignment, the system user can view contacts and make calls through the APP.

Result Verification:

After logging into the APP, upon entering the Video Call application, the interface status will display as "**Connected**"; if no extension number has been assigned, the application will prompt with "You have not been assigned an extension number, please contact the super administrator."
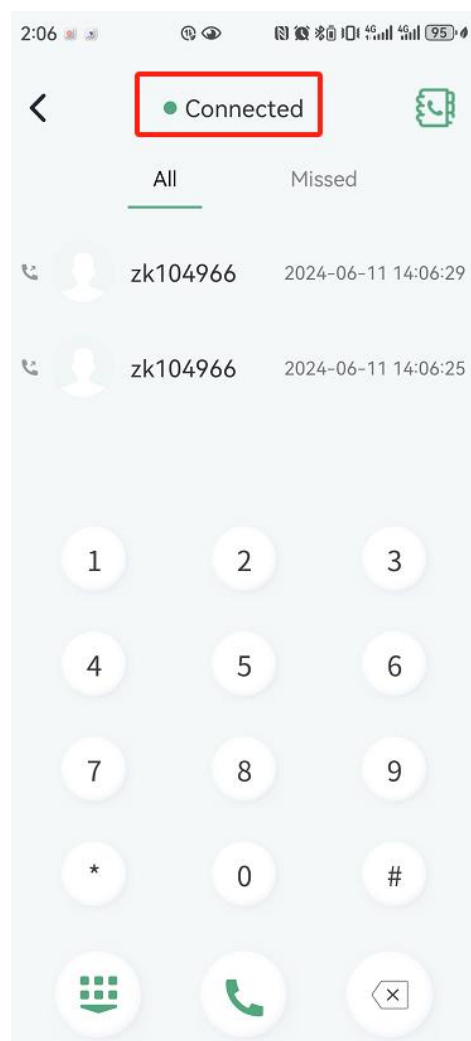
7.4.2.2 Synchronized Extension

Following the aforementioned steps to assign extension numbers to devices, personnel, and system users, the system will automatically synchronize the data to the devices or APPs. If the synchronization is interrupted or not successful, you can also click on "Synchronize Extension" to resynchronize.
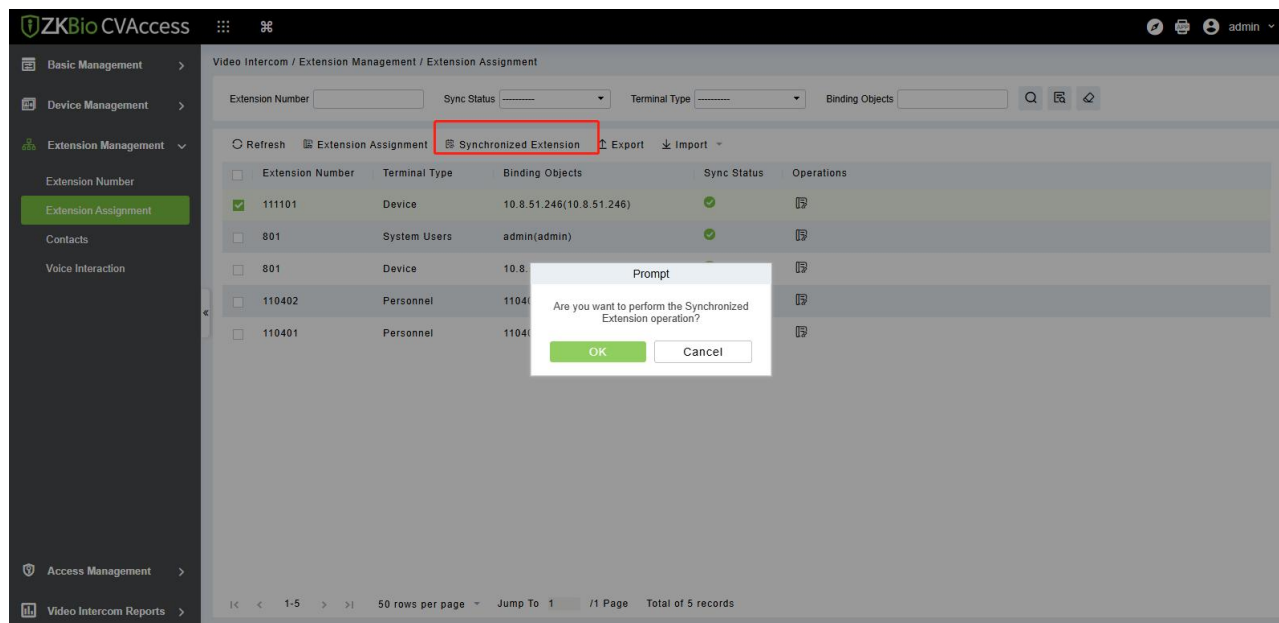
7.4.2.3 Import

If you need to add extension numbers in bulk, you can use the Import function.

Step 1: Click on **Import -> Download extension information import template**, then enter the details.

Step 2: Download the import template by clicking **Import -> import** template.

Step 3: Click on **Import,** then click Browse to select the import template, and click **OK** to start the bulk import process.

7.4.2.4 Export

Export the relevant information for the extension assignment.
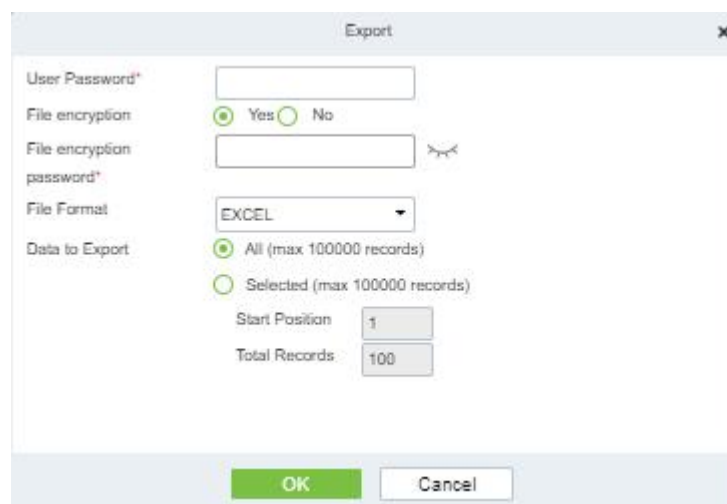
7.4.2.5 Unbinding Extension

Click on the [icon], to unbind the extension number from its current association.
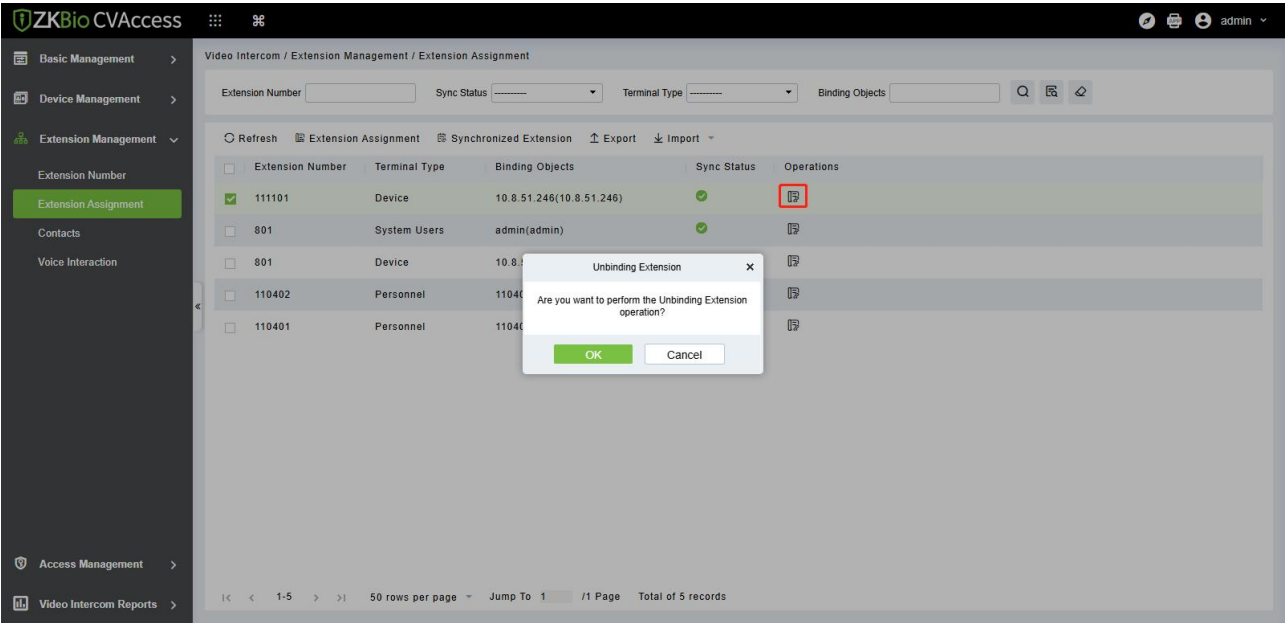
7.4.3 Contact List

User can create a contact list and assign it to devices or the app.
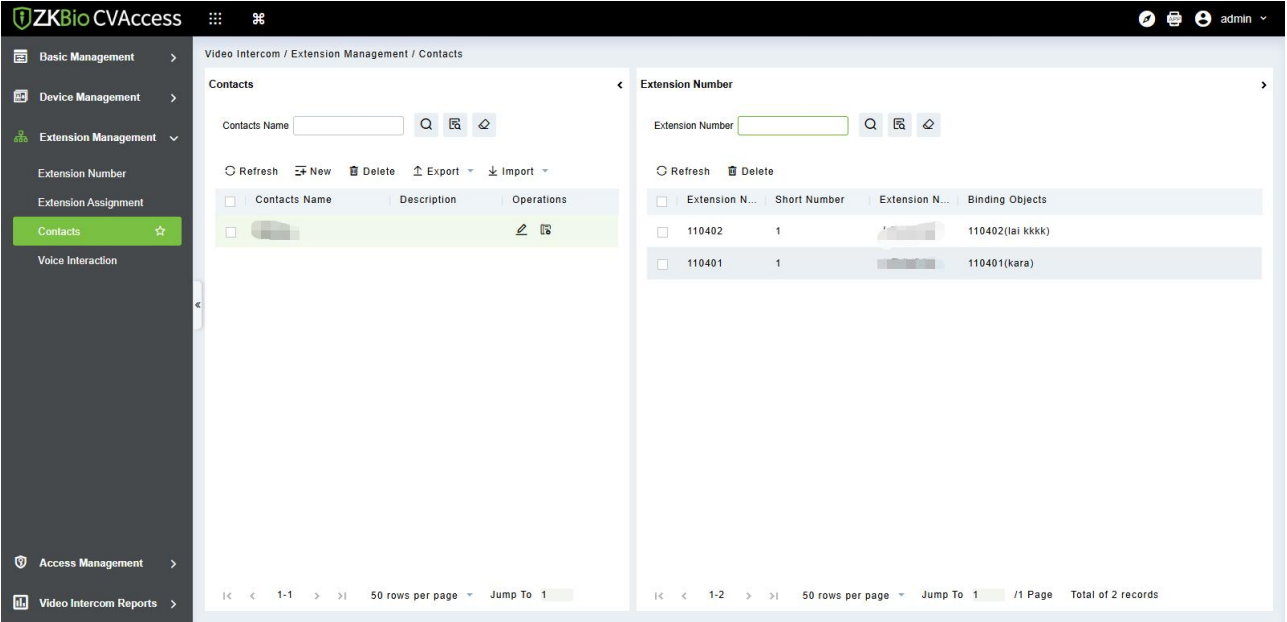
7.4.3.1 Create a New Contact

Click the **New** to create a new contact list.

7.4.3.2 Add Extension

Click on the icon to add an extension number to the contact list, as shown in the image below:

After selection, the right sidebar allows you to edit and customize the **Short Number**.

Short Number: Users can customize it, and Short Numbers can be duplicated. For example, if there are 4 members in the engineering maintenance team (4 extension numbers), to facilitate answering calls, they can all define their Short Number as 101. When this contact list is synchronized to the device or extension numbers, dialing 101 from the device will ring all 4 members of the engineering maintenance team.

Note:

1. The ZKBio CVAccess APP (ZKBio Zexus) supports this contact list feature. SenseFace/SpeedPalm devices need a firmware upgrade to support it.

2. After creating a contact list, you can assign it to individuals, system users, or devices in the Extension Assignment section.

7.4.3.3 Delete

Click **Delete** to remove the contact list.
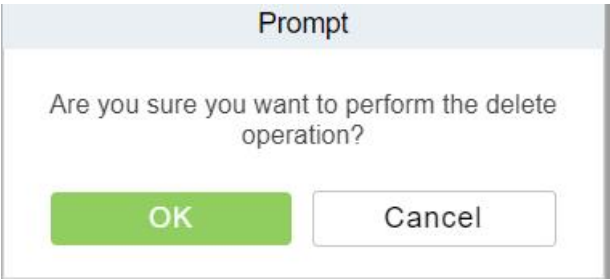
7.4.3.4 Export

Click **Export** to export the contact list.
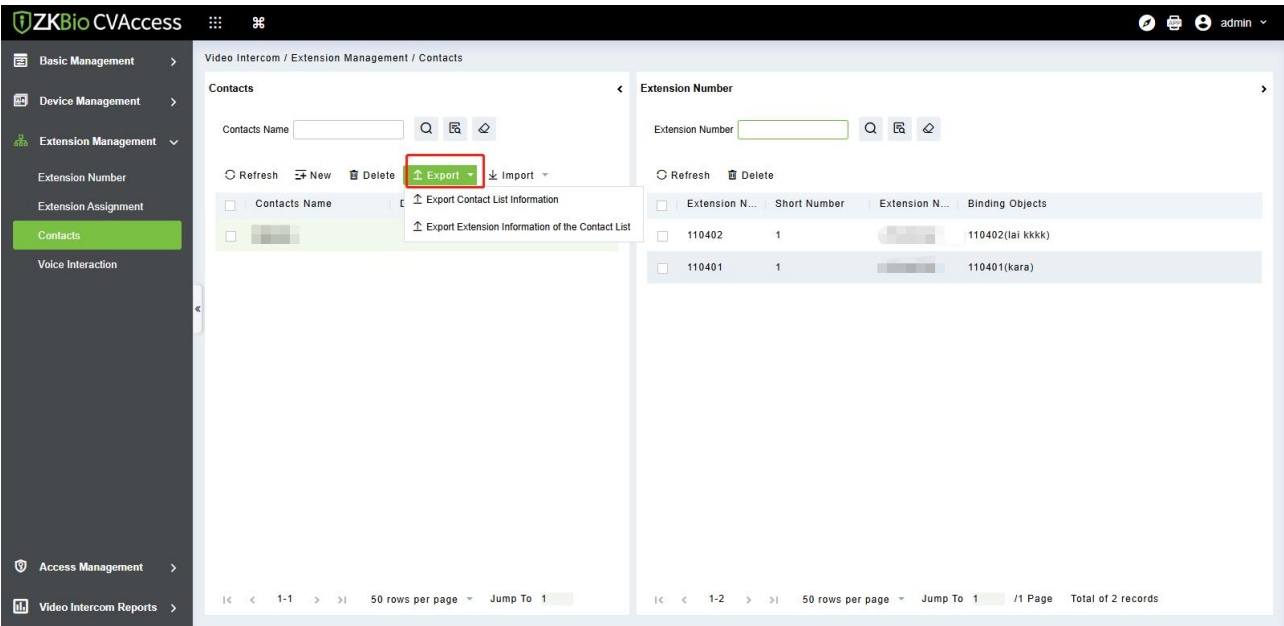
● Export Contact List Information

Contacts	
Contacts Name	Description
Building 1-Unit1	
ZKTeco1	Popy testing

● Export Extension Information of the Contact List

Video intercom address book extension information				
Contacts Name	Extension Number	Short Number	Extension Name	Binding Objects
ZKTeco1	92306	101	Device	Senseface 7A(192.168.137.60)
ZKTeco1	92305	102	PC	
ZKTeco1	115	107	Popy	115(Popy xiao)
ZKTeco1	123	104	Jessica	111(Jessica)
ZKTeco1	125	103	FLZ-Indoor	
ZKTeco1	119	105	Test app	Test
ZKTeco1	118	106	Popy PC Client	
ZKTeco1	117	106	Senseface 7A	
ZKTeco1	122	104	Manual	112(Manuel)
ZKTeco1	116	107	Speedpalm V5L	
ZKTeco1	124	104	Boopalam	114(Boopalan)
ZKTeco1	121	105	Joao	113(Joao)

7.4.3.5 Import

Click **"Import"** to import a contact list.

You can download the import template and then proceed with the import based on the requirements of the template.
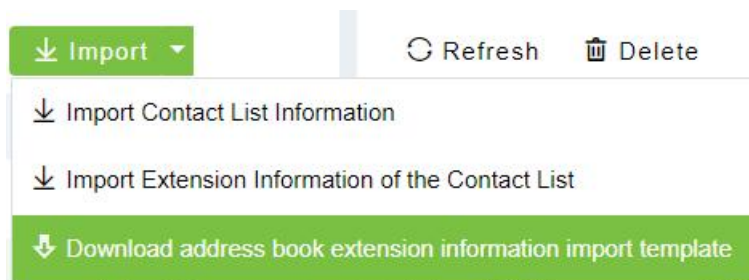
7.4.4 Voice Interaction

IVR (Interactive Voice Response) is a telephone service technology that allows users to interact with an automated telephone system through telephone key presses or voice commands; this feature is only available with PBX Server.

This feature can be used for two major applications: Access Control linkage to video intercom; and IVR Intelligent Voice Interaction.

1. Intelligent Voice Interaction

The IVR system can improve service efficiency, reduce labor costs, and provide users with uninterrupted service 24 hours a day. For example: Suppose the user has configured the IVR extension number to 10086 and has pre-configured the voice guidance content, then the user can dial 10086 via the app, and the guidance content will be played automatically; the user can press buttons according to the guidance, such as pressing 1 to call customer service, pressing 5 to hang up, etc. (Currently, the ZKBio CVAccess Mobile App does not support retrieving keyboard input during the call process, the next version will support it; the current version can be used in conjunction with the indoor unit.)

7.4.4.1 Create a New Voice Interaction

Click on **Video Intercom -> Extension Management ->Voice Interaction page**, it will enter into the voice interaction interface then click on New to display the window as shown in the figure below.
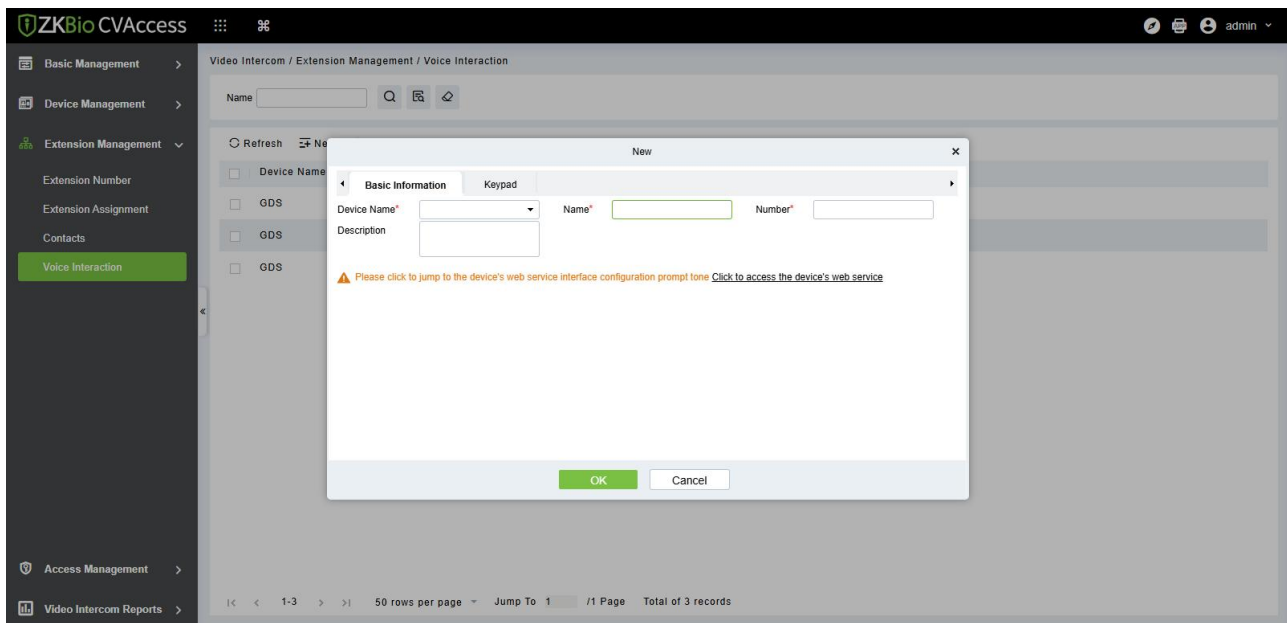
● Basic Information

The PBX Server's IVR feature basic information configuration, with field explanations as follows:

Parameter	Description
Device Name	Select PBX Server
Name	Custom Name: Name this voice interaction
Number	Configure IVR Extension: Set the extension number for the IVR
Description	Description: Provide a description for this IVR

● Keypad

Configure the purpose and actions intended to be achieved by the IVR.

Click "**Add**" to begin the configuration.

Parameter	Description
Key	Keyboard values: 1-9, *, #
Action	A total of 3 actions are supported: Extension: Dial an extension number. After selecting this option, you can further choose the extension number.

	Transfer to Voice Interaction: Transfer to another IVR. After selecting this option, you can further choose the IVR number. Hang Up: End the call.

Note: To ensure the normal use of the IVR function, after you have completed the configuration of the above content, you must go to the PBX's Web-IVR page to find the IVR you just saved and edit it to upload the required voice files, as shown in the figure below:

2.   Access Control Linkage

Click on **Access > Access Rule > Linkage,** and click on "**New**" to start configuring the linkage. In the output actions, you can find Video Intercom. You can select the IVR and the extension number you wish to call.

After the configuration is complete, when the triggering conditions are met, the system will automatically call the specified extension number and play the IVR voice, preventing security personnel from missing emergency alerts.

7.4.4.2 Obtain IVR

Click on **Video Intercom -> Extension Management ->Voice Interaction** page, and click on Open IVR the window as shown in the figure below:

Obtain IVR	✕
Device Name*	▼

OK   Cancel

Parameter	Description
Device Name	Enter the name of the device.

7.5 Video Intercom Reports

In the video intercom report, you can query all video intercom records, which include call records and unlock records. You have the option to export all records or query specific records. This section describes the Step for querying and exporting reports in ZKBio CVAccess.

7.5.1 Call Records

7.5.1.1 Record Query

To perform the following steps to get the call records:

Step 1: In the Video Intercom module, choose "**Video Intercom Report** > **Call Records**".

Step 2: On the call Records interface, fill in the corresponding query information and click the icon

to complete the query of all records, as shown in figure below.
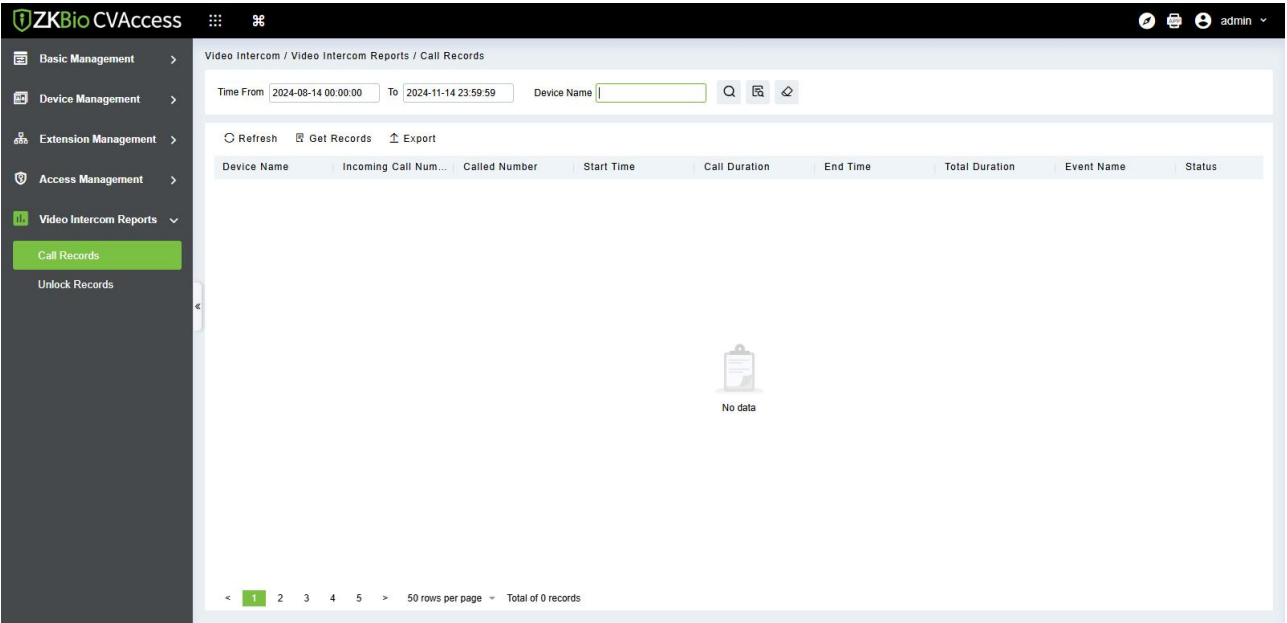
7.5.1.2 Get Records

To perform the following steps to get the records:

Step 1: On the Video Intercom module, choose "**Video Intercom Report > Call Records > Get Records**".

Step 2: On the Get Records interface, select the indoor station, as shown in figure below.
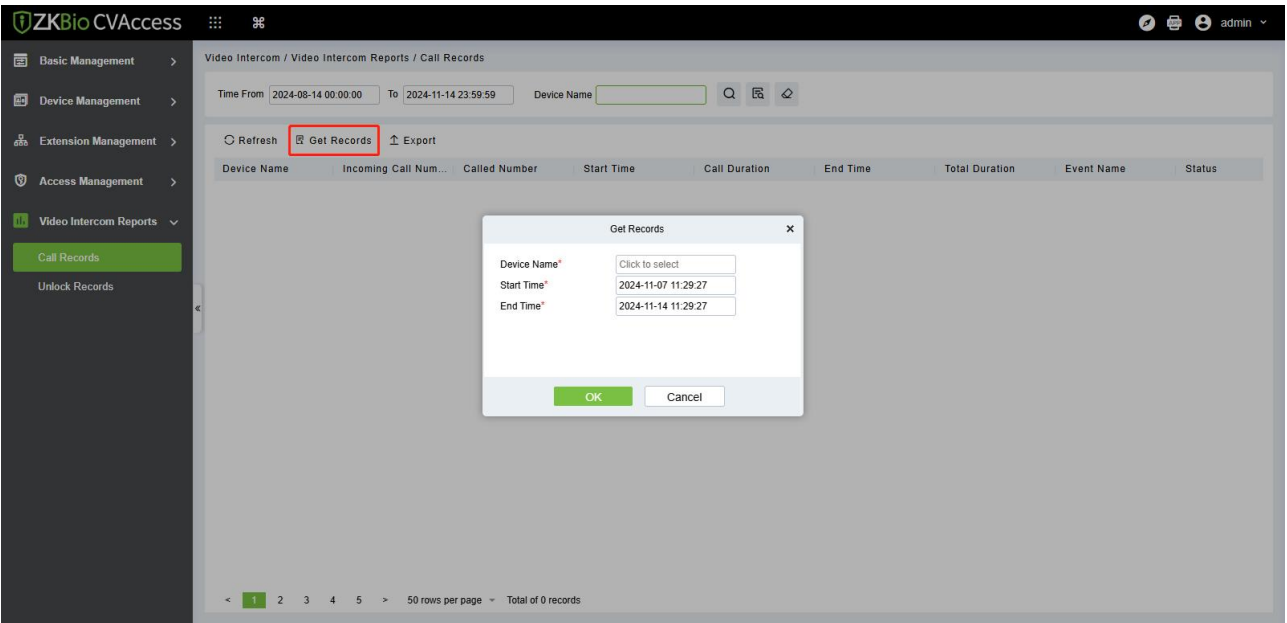
Parameter	Description
Device Name	Select the name of the device.
Start Time	Enter the start time of the device.
End Time	Enter the end time of the device.

Step3: On the Select device interface, select the device you need, as shown in figure below.

| Select Device | ✕ |

Device Name [   ]   IP Address [   ]   🔍   ⬦

Alternative   Selected(0)

	Device Name	IP Address		Device Name	IP Address
⊙	10.8.42.66	10.8.42.66			

>
<

No data

|< ‹ 1-1 › >| 50 rows per page ▾

OK   Cancel

Step 4: Click **OK** to complete the complete acquisition of device records.

7.5.1.3 Export

Click **Export**, enter the user password in the displayed security verification dialog box, and click **OK**. Select whether to encrypt the file and the file format to export and click **OK**.

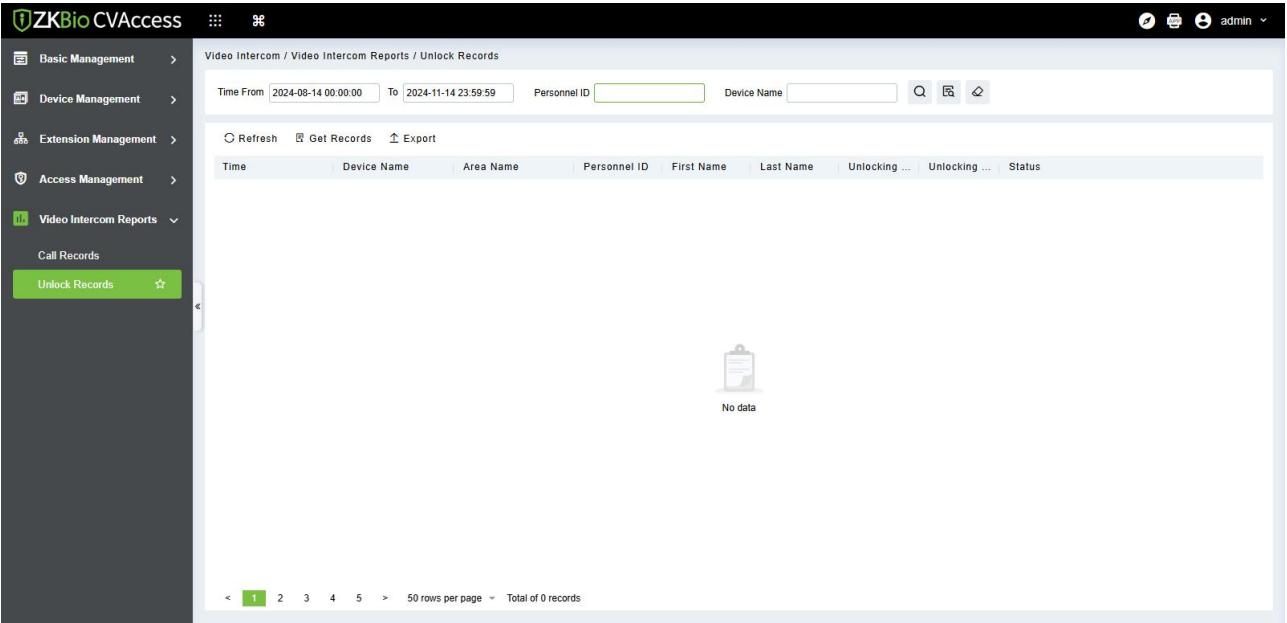| Call Records					
Time	Device Name	Area Name	Number	Event Type	Ring Duration/second
2023-11-20 22:56:37	221	Area Name	10.8.14.3		12
2023-11-20 19:15:14	221	Area Name	10001		4
2023-11-20 19:11:19	221	Area Name	10001		3
2023-11-20 19:10:55	221	Area Name	10001		1
2023-11-20 19:09:56	221	Area Name	10001		5
2023-11-20 19:09:46	221	Area Name	10001		4
2023-11-20 19:07:27	221	Area Name	10001		5
2023-11-20 17:44:48	221	Area Name	10.8.14.3		4
2023-11-20 16:13:06	221	Area Name	10.8.14.3		4
2023-11-16 19:54:01	221	Area Name	10001		2
2023-11-16 19:53:52	221	Area Name	10001		3
2023-11-16 19:52:23	221	Area Name	2010008		0
2023-11-16 19:51:49	221	Area Name	2010008		0
2023-11-16 19:51:33	221	Area Name	2010008		0

7.5.2 Unlock Records

7.5.2.1 Record Query

To perform the following steps to view the query of all records:

Step 1: On the Video Intercom module, choose "**Video Intercom Report** > **Unlock Records**".

Step 2: On the unlock Records interface, fill in the corresponding query information and click the

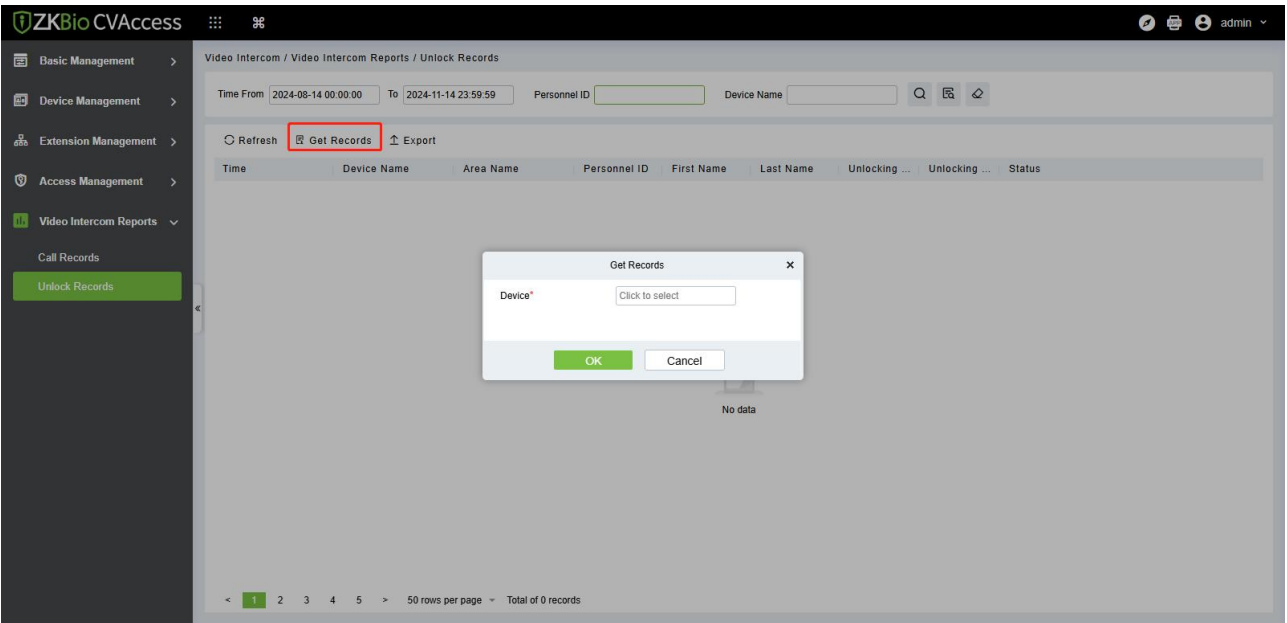icon   to complete the query of all records, as shown in figure below.

7.5.2.2 Get Records

To perform the following steps to view the query of all records:

Step 1: On the Video Intercom module, choose "**Video Intercom Report > Unlock Records > Get Records**".

Step 2: On the Get Records interface, select the indoor station, as shown in figure below.

Parameter	Description
Device Name	Select the name of the device.

Step 3: On the Select device interface, select the device you need, as shown in figure below.

Step 4: Click **OK** to complete the complete acquisition of unlock records.

7.5.2.3 Export

Click **Export**, enter the user password in the displayed security verification dialog box, and click **OK**. Select whether to encrypt the file and the file format to export and click **OK**.

| ▲	A	B	C	D	E	F	G	H
1				Unlock Records				
2	Time	Device Name	Personnel ID	First Name	Last Name	Unlock Method	Number	Status
3	2023-11-23 14:30:46	-164				Password	0000	Succeed
4	2023-11-23 14:30:43	-164				Password	789	
5	2023-11-23 14:30:39	-164				Password	0000	Succeed
6	2023-11-23 14:29:02	-164				Password	0000	Succeed
7	2023-11-23 14:28:58	-164				Password	9999	
8	2023-11-23 14:28:52	-164				Password	99	
9	2023-11-23 14:28:49	-164				Password	0000	Succeed
10	2023-11-22 17:40:54	-164				Password	0000	Succeed
11	2023-11-22 08:57:44	-116				Face		
12	2023-11-22 08:57:13	-116				Face		
13	2023-11-22 07:02:27	-116				Face		
14	2023-11-22 07:00:39	-116				Face		
15	2023-11-22 07:00:17	-116				Face		
16	2023-11-22 06:47:40	116				Face		
17	2023-11-21 09:37:00	16				Face		
18	2023-11-21 09:35:36	16				Face		
19	2023-11-20 22:37:26	64				Password	123456	
20	2023-11-20 22:37:08	64				Password	11	
21	2023-11-20 19:08:09	64				Password	0000	Succeed
22	2023-11-20 19:08:05	64				Password	0000	Succeed
23	2023-11-20 19:06:09	64				Password	0000	Succeed

8   System

System settings primarily include assigning system users (such as company management user, administrator, and access control administrator) and configuring the roles of corresponding modules, managing database, setting system parameters, and view operation logs, etc.
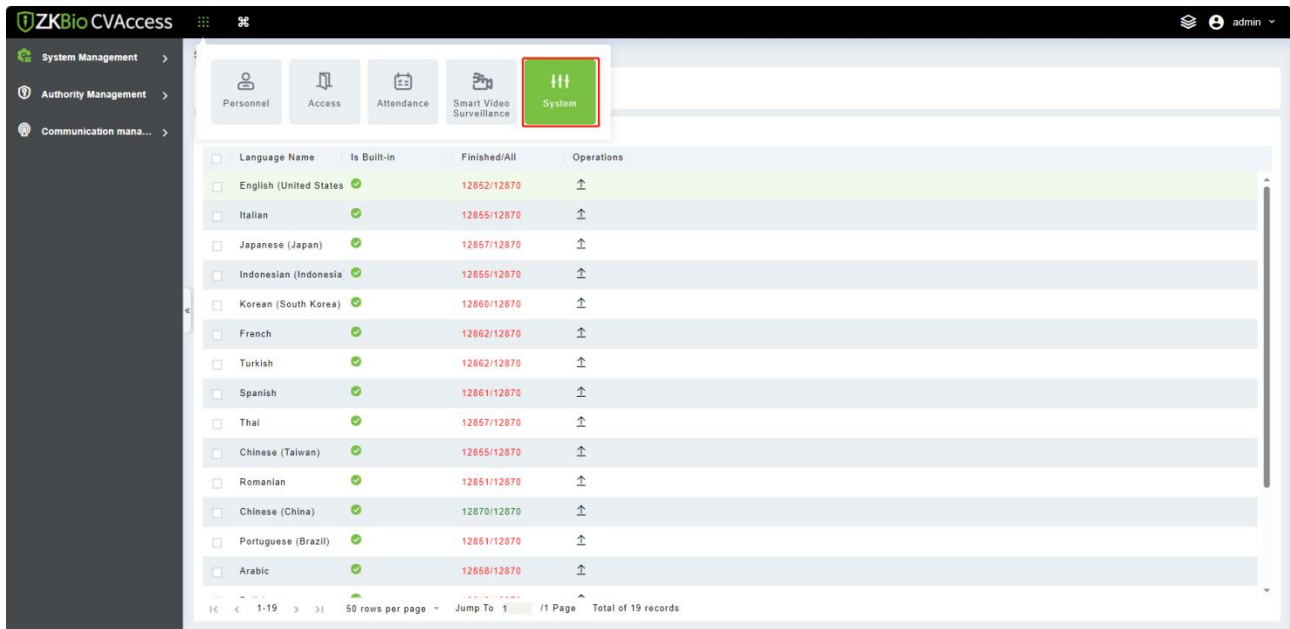
8.1 System Management

8.1.1   Operation Logs

Click **[System]** > **[System Management]** > **[Operation Log]**.
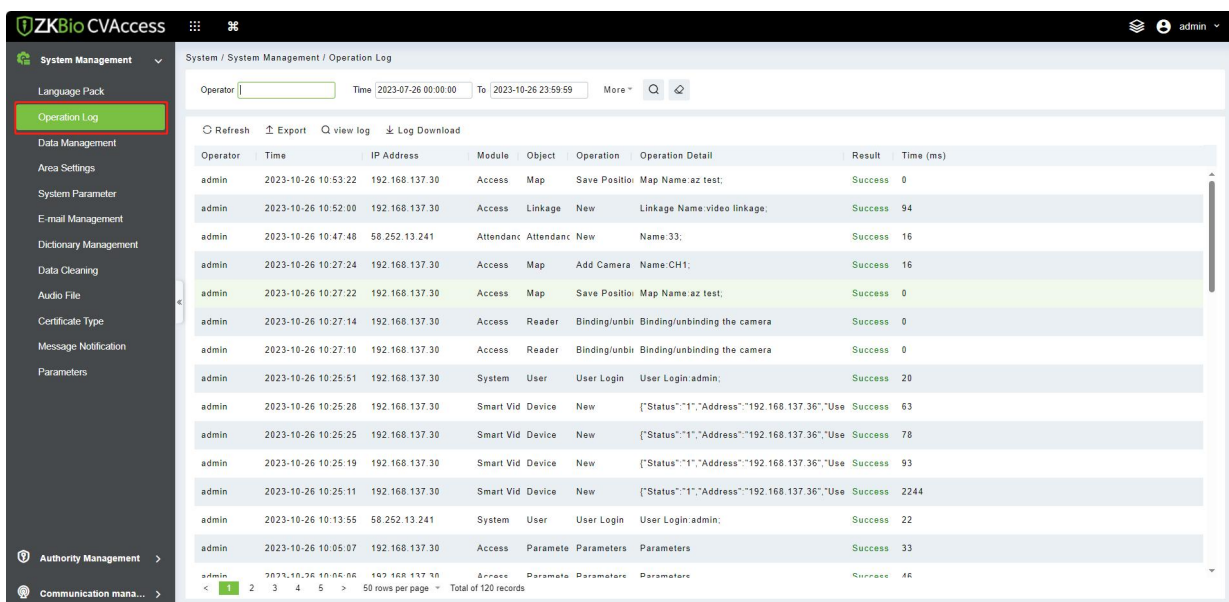
All operation logs are displayed on this page. You can query specific logs by conditions.

➢ **Export**

You can export selected leave data in Excel, PDF, and CSV file format.

8.1.2 Database Management

Click **[System]** > **[System Management]** > **[Database Management]**.

History of database backup operation logs is displayed in this page. You can refresh, backup and schedule backup database as required.
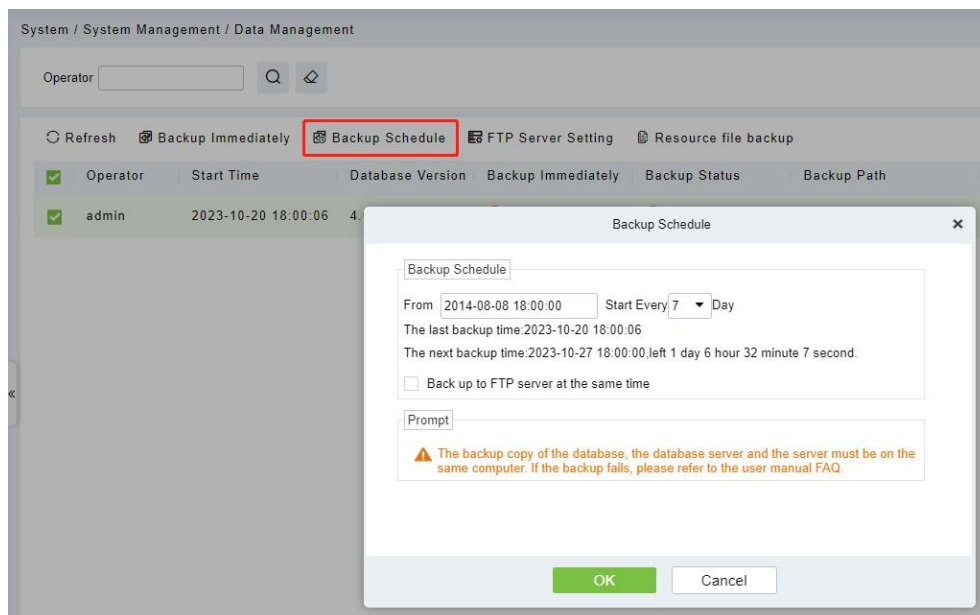
➢ **Backup Immediately**

Backup database to the path set in installation right now.

✍**Note:** The default backup path for the system is the path selected during the software installation. For details, refer to <u>ZKBio CVAccess Installation Guide</u>.
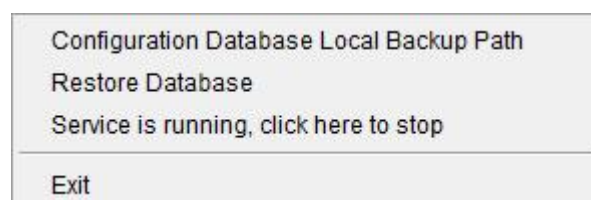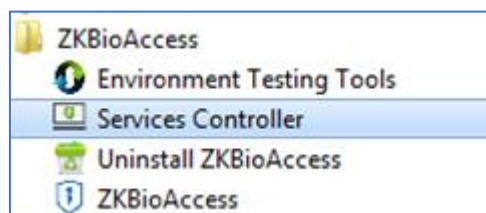
➢ **Backup Schedule**

Click **[Backup Schedule]**.

Set the start time, set interval between two automatic backups, click **[OK]**.

➢ **Restore Database**

1. Click the start menu of the PC > **[All Programs]** > **[ZKBio CVAccess]** > Then run "Services Controller", and you can find out the icon of "Services Controller" in Taskbar as follow, right click that icon, then left click "Restore Database".

2. In the popup window, click **[Browse]** to choose the backup file to restore the database.

✍ **Note:** Before restoring a database, it is recommended that you back up the current database to avoid data loss.
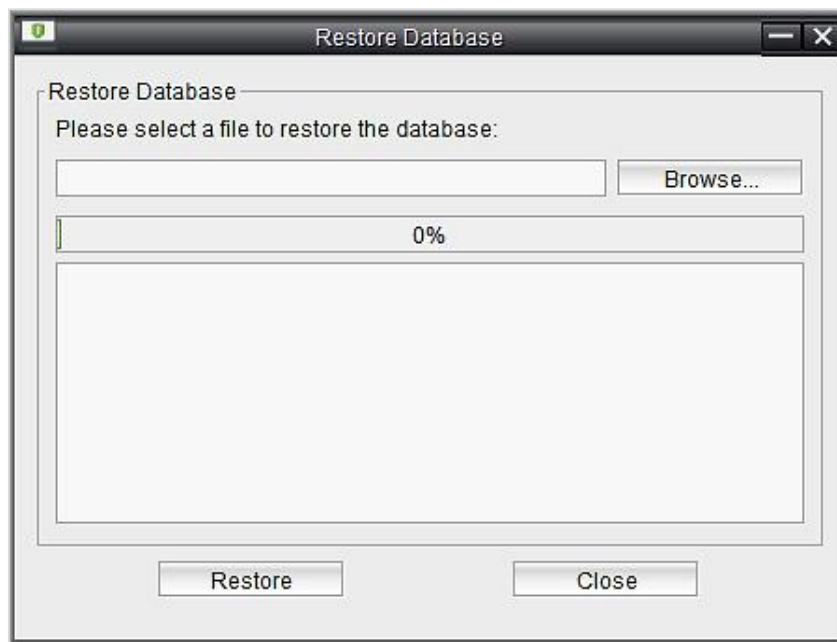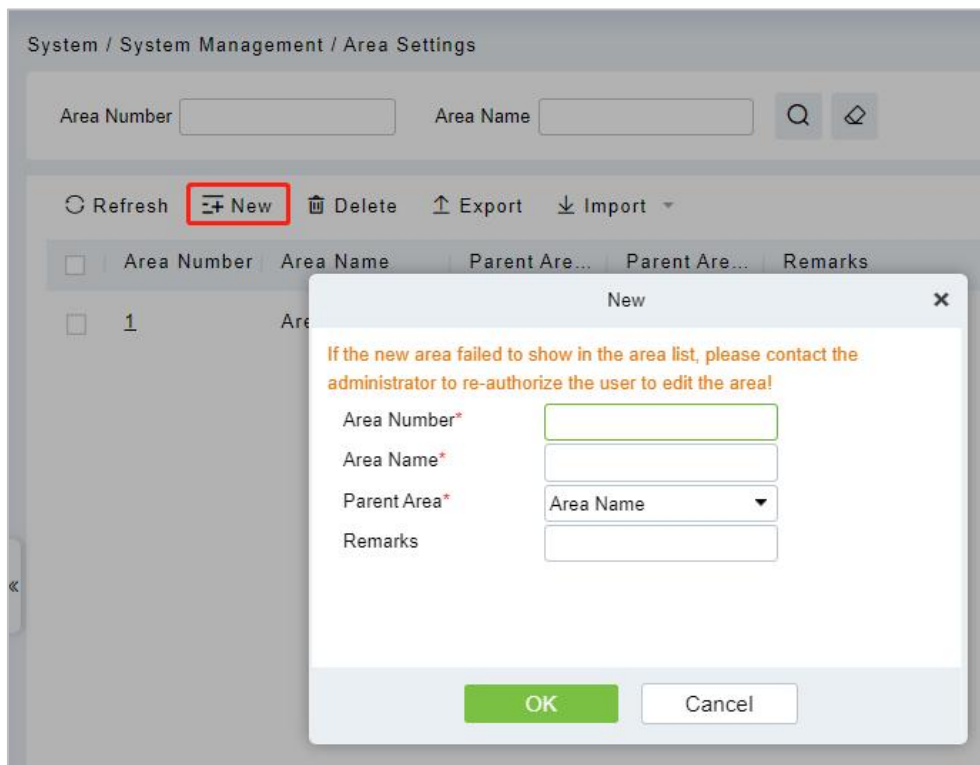
8.1.3 Area Settings

Area is a spatial concept which enables the user to manage devices in a specific area. After area setting, devices (doors) can be filtered by area upon real-time monitoring.

Click **[System]** > **[System Management]** > **[Area Settings]**. The system, by default, has an area named "Area Name" and numbered "1".
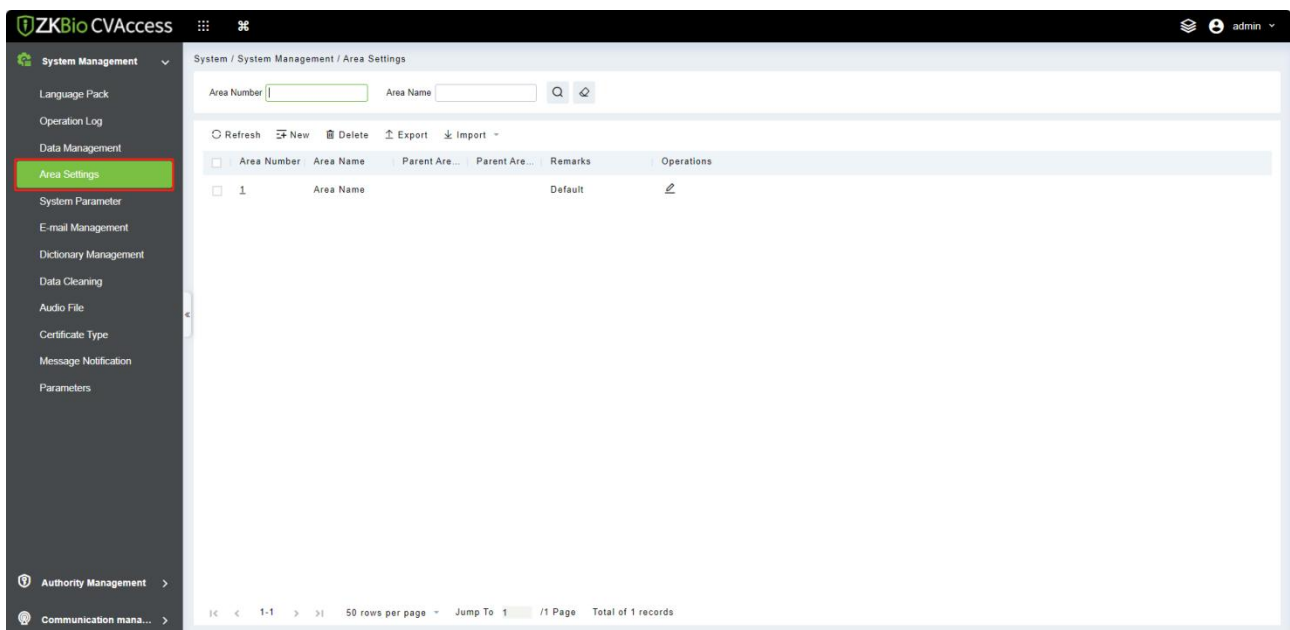
➢ **Add an Area**

1.   Click **[New]**.

Fields are as follows:

- **Area Number:** It must be unique.

- **Area Name:** Any characters with a length of less than 30.

- **Parent Area:** Determine the area structure of the system.

2. Click **[OK]** to finish adding.
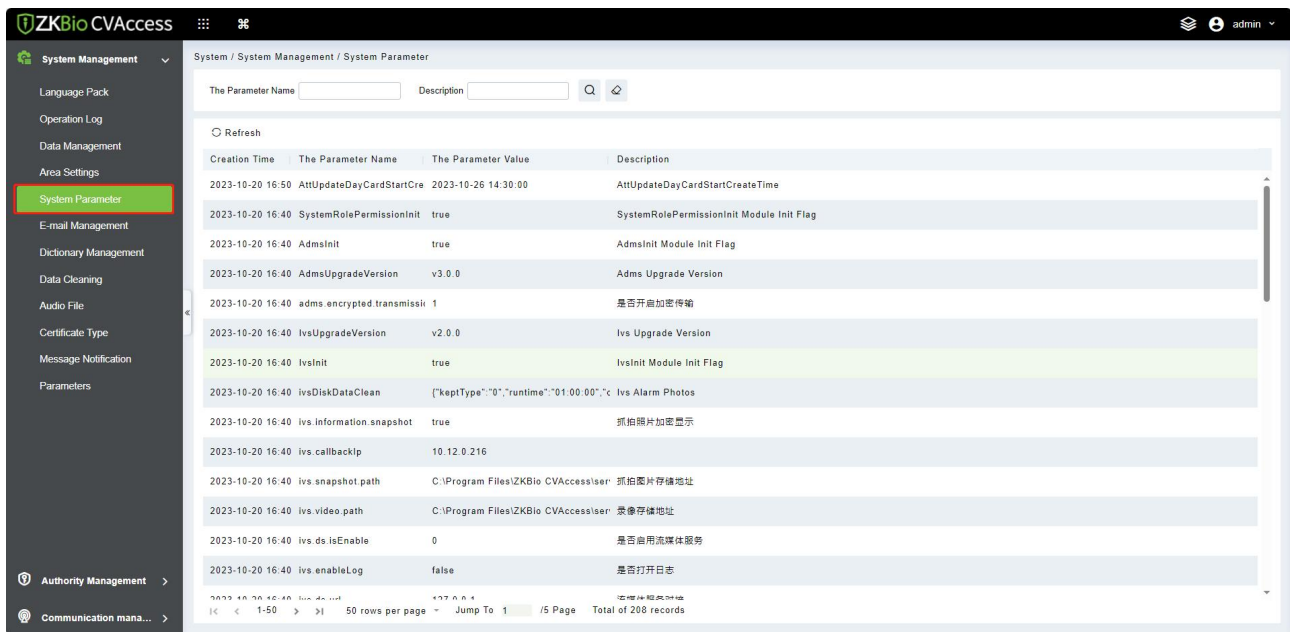
➢ **Edit/Delete an Area**

Click **[Edit]** or **[Delete]** as required.

8.1.4 System Parameter

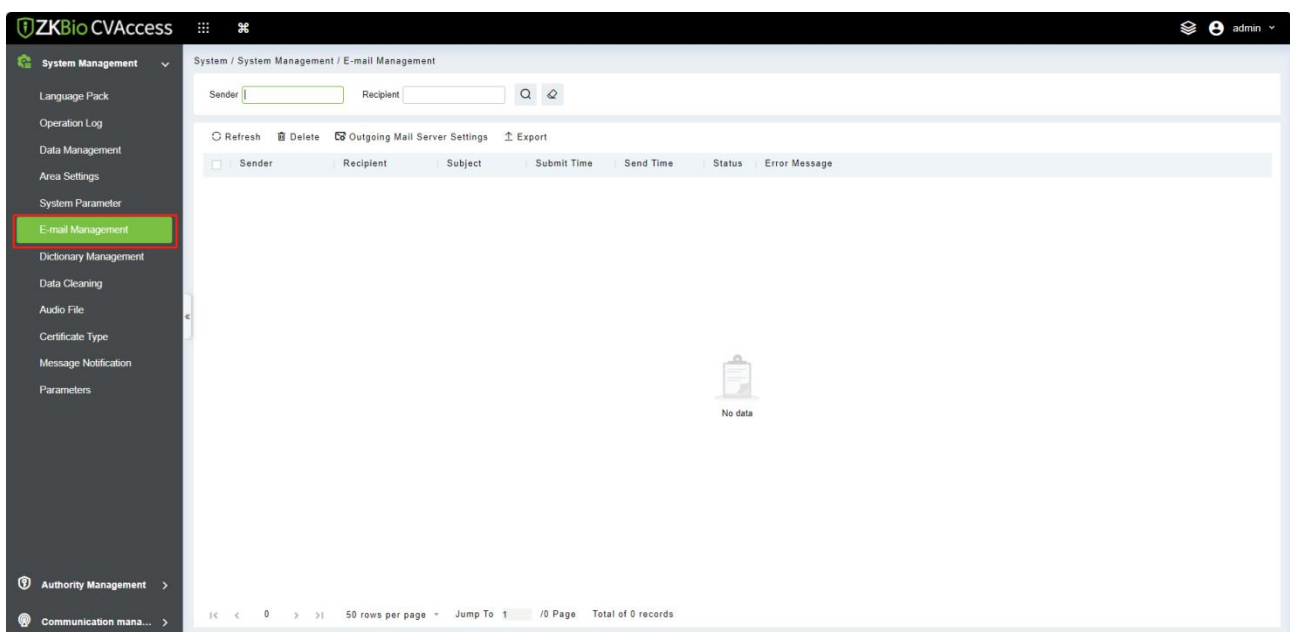This function is used to view parameters that have been created.

Click **[System]** > **[System Management]** > **[System Parameter]**.
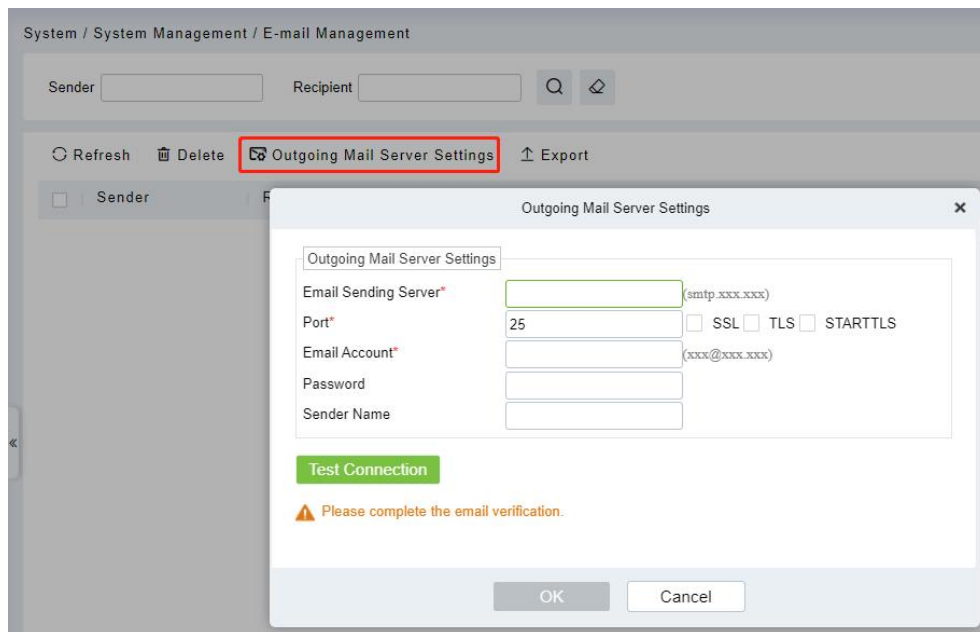
8.1.5 E-mail Management

Set the email sending server information. The recipient Email should be set in Linkage

Click **[System]** > **[System Management]** > **[Email Management]**.

➢ **Outgoing Mail Server Settings**

Click **[Outgoing Mail Server Settings]**.

🖎 **Note:** The domain name of E-mail address and E-mail sending server must be identical. For example, if the Email address is: test@gmail.com, then the E-mail sending sever must be: smtp.gmail.com.

8.1.6 Dictionary Management

Data dictionary management function, users can find the meaning of error code and self-check software errors.

Click **[System]** > **[System Management]** > **[Dictionary Management]**.
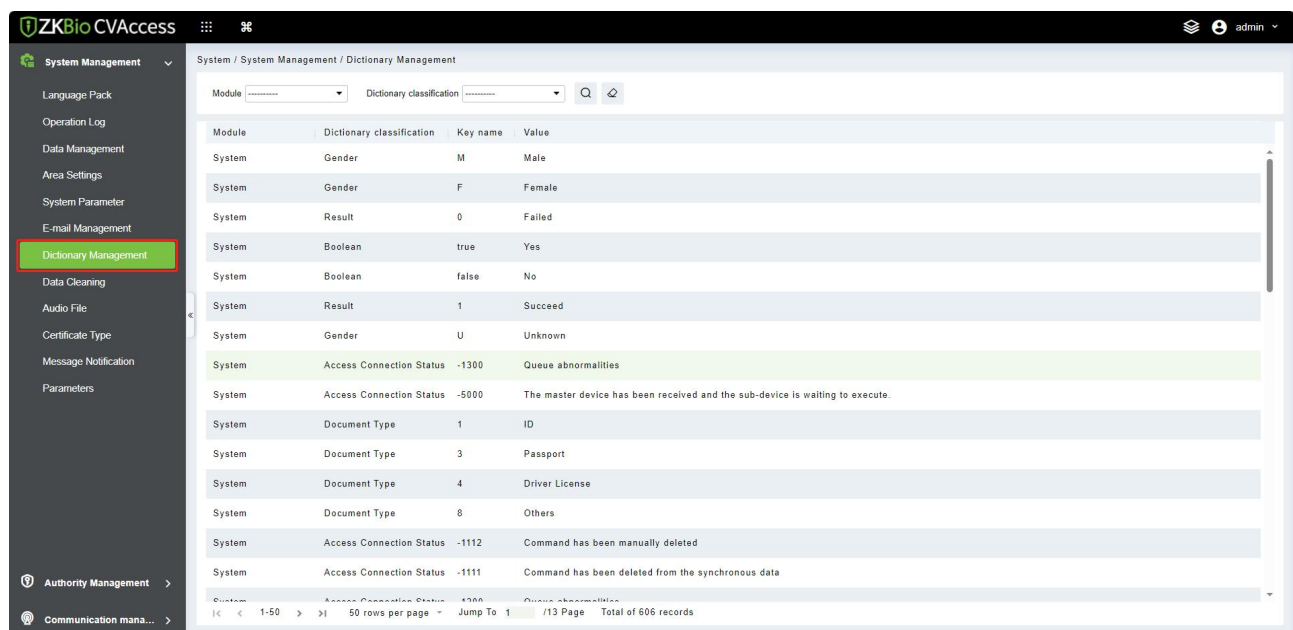
8.1.7 Data Cleaning

The data cleaning time settings are available to set. The data volume increases with the use of the system. To save the storage space on the disks, you need to periodically clean old data generated by the system.

Click [**System**] > [**System Management**] > [**Data Cleaning**].

8.1.7.1 Record

This option helps you to set the frequency of retain the recent data of the access transaction, attendance transaction, elevator transactions and visitor transactions etc.

8.1.7.2 Disk Space Cleanup

In this option you can set the frequency of the retains the recent and also clean up the selecyted days data.

8.1.7.3 System

This option helps you to clean up the system operation log, device commands and database backup file.

8.1.8 Audio File

Click **[System]** > **[System Management]** > **[Audio File]**.

➢ **New**

1. Click **[New]**.
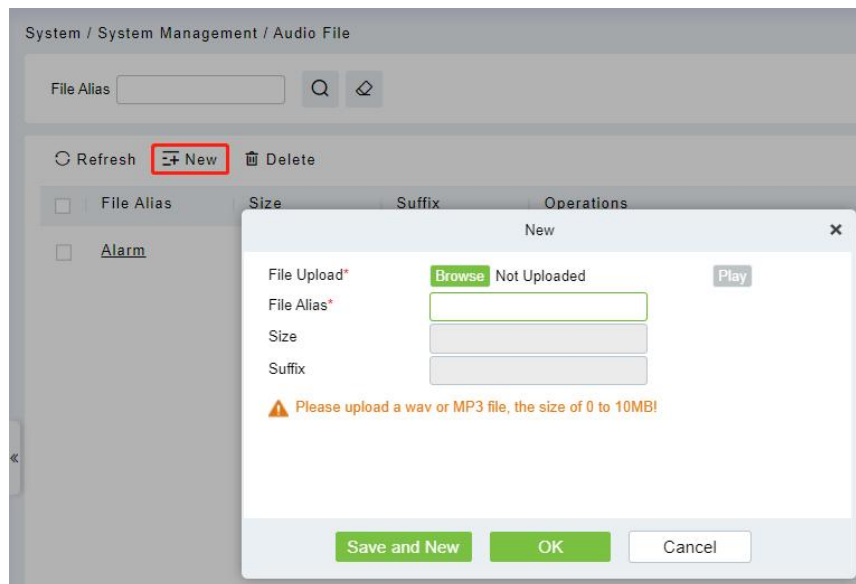
Fields are as follows:

- **File Alias (Name):** Enter the file name. Any character, up to 30 characters.

- **Size:** After uploading the file, the file size is automatically generated.

- **Suffix:** After uploading the file, the suffix of the file is automatically generated.

2. Click **[OK]** to finish adding.

✍ **Note:** You can upload a sound from the local. The file must be in wav or mp3 format, and it must not exceed 10MB.

8.1.9 Certificate Type

The system initializes 9 certificate types. User can add the required certificate type for personnel and visitor registration.

Click **[System]** > **[System Management]** > **[Certificate Type]**.
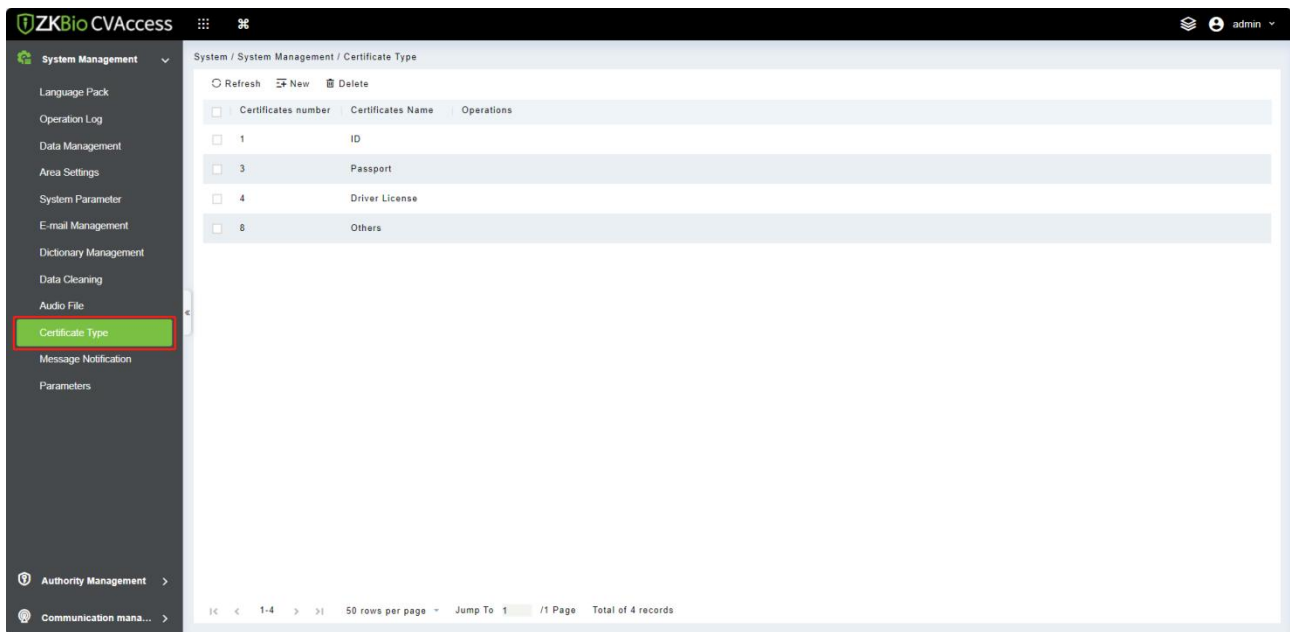
8.1.10 Message Notification

This function is used to open/close the event notification of access and attendance transaction.

Click [**System**] > [**System Management**] > [**Message Notification**].
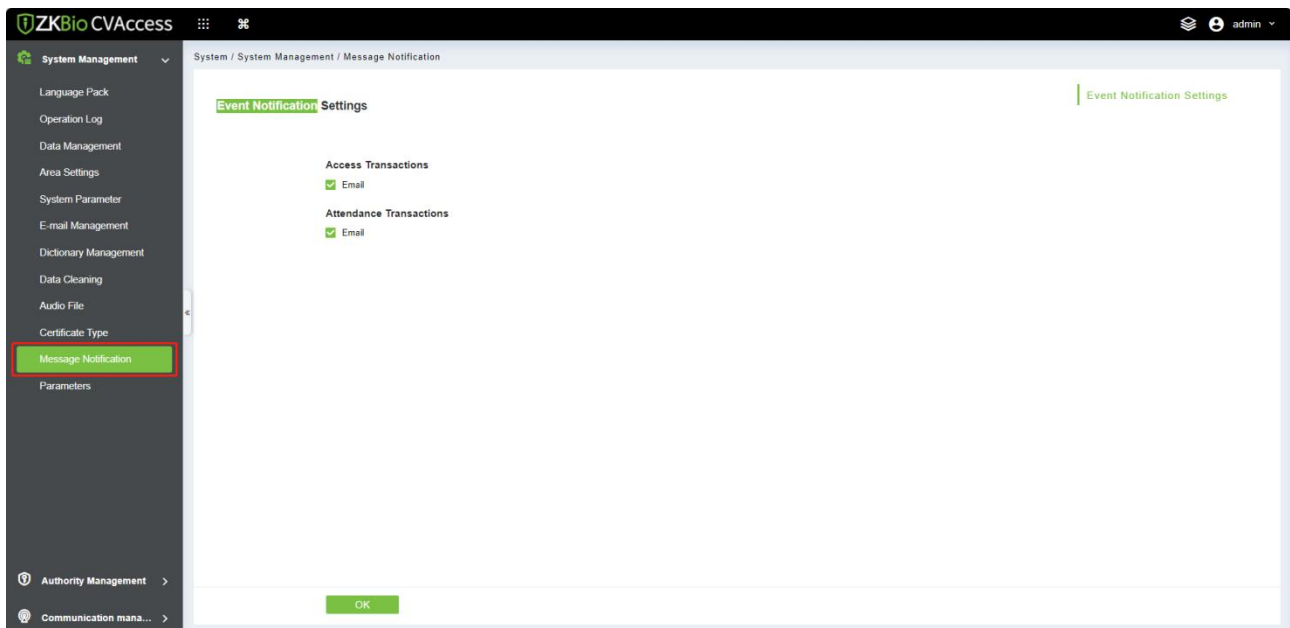
8.1.11 Parameters

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

8.1.11.1 QR Code Setting

1. Enable QR code, select "**YES**" or "**NO**" for Enable the QR code

2. Enable QR code If YES select "**YES** > **Static**". It will be fixed the QR information same manner for

the rest of time.

3.   Enable QR code If YES select "**YES**> **Dynamic** > **Valid Time**". It will generate new QR code every
      30 seconds.

8.1.11.2 Video Watermark

This option helps you to add watermark and tile to your videos.

8.1.11.3 Personal Sensitive Information Protection

After enabling the personal sensitive information security protection option, the sensitive personal
data involved in this module will be desensitized or obscured, including but not limited to names,
card numbers, ID numbers, photos, etc.

8.1.11.4 Privacy Policy

Click **[View]** to view the privacy policy.

8.2 Authority Management

8.2.1 User

Add new users and implement levels for the user in the system.

Click **[System]** > **[Authority Management]** > **[User]**.
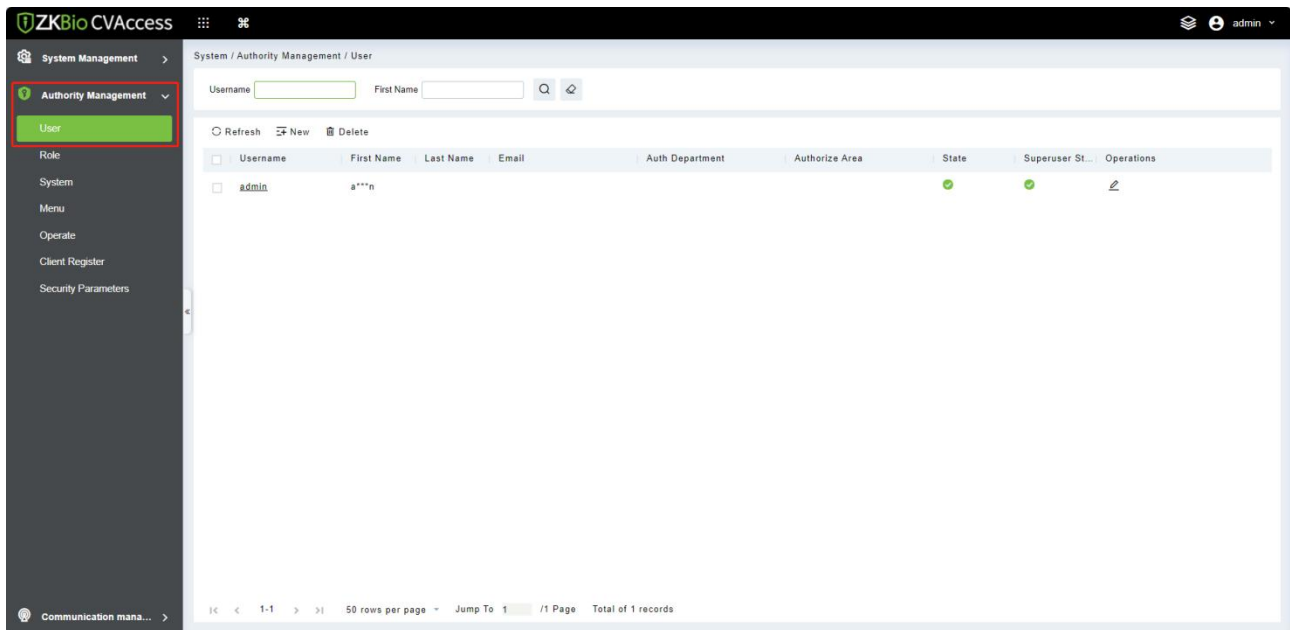
➢ **New**

1. Click **[System] > [Authority Management] > [User] > [New]**.
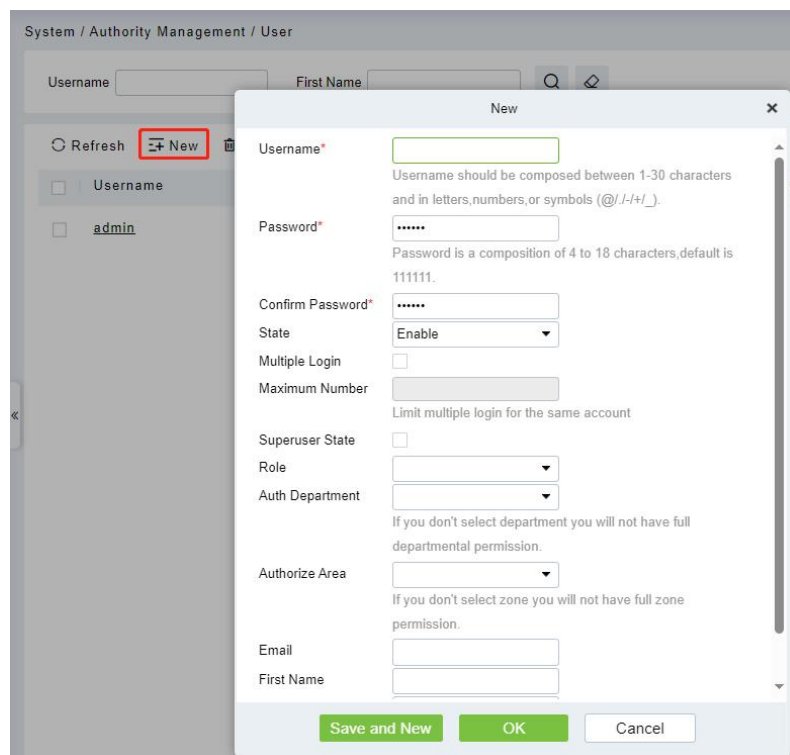
Fields are as follows:

- **Username:** Any characters within a length of 30.

- **Password:** The length must be more than 4 digits and less than 18 digits. The default password is 111111.

- **State:** Enable or disable the user to operate the system.

- **Super User State:** Enable or disable the user to have the super user's levels.

- **Role:** You need to define the role as explained in Role.

- **Auth Department:** If no department is selected, then the user will have all department rights by default.

- **Authorize Area:** No area selected means the user possesses all area rights by default.

- **Email:** Type your email in the correct format.

- **First Name:** Type your initials.

2. After editing, click **[OK]** to complete user adding, and the user will be shown in the list.

8.2.2 Role

When using the system, the super user needs to assign different levels to new users. To avoid setting users one by one, you can set roles with specific levels in role management and assign appropriate roles to users when adding users. A super user has all the levels, can assign rights to new users and set corresponding roles (levels) according to requirements.

Click **[System]** > **[Authority Management]** > **[Role]**.
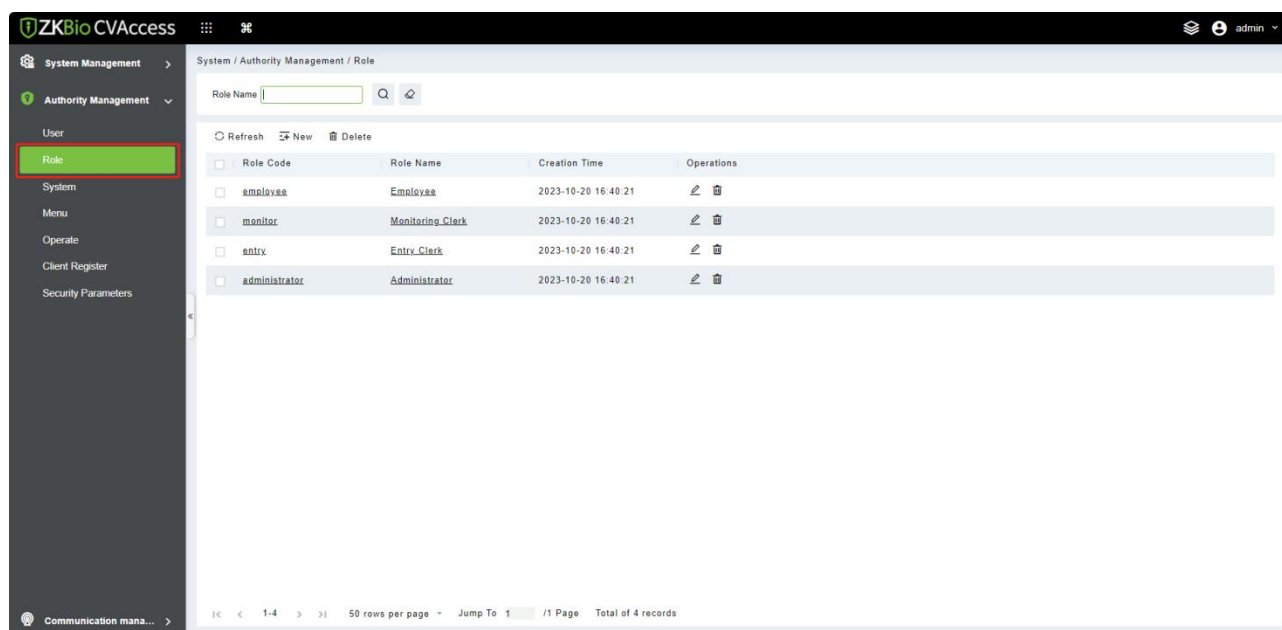
1. Click **[System] > [Authority Management] > [Role] > [New]**.

2.   Set the name and assign permissions for the role.
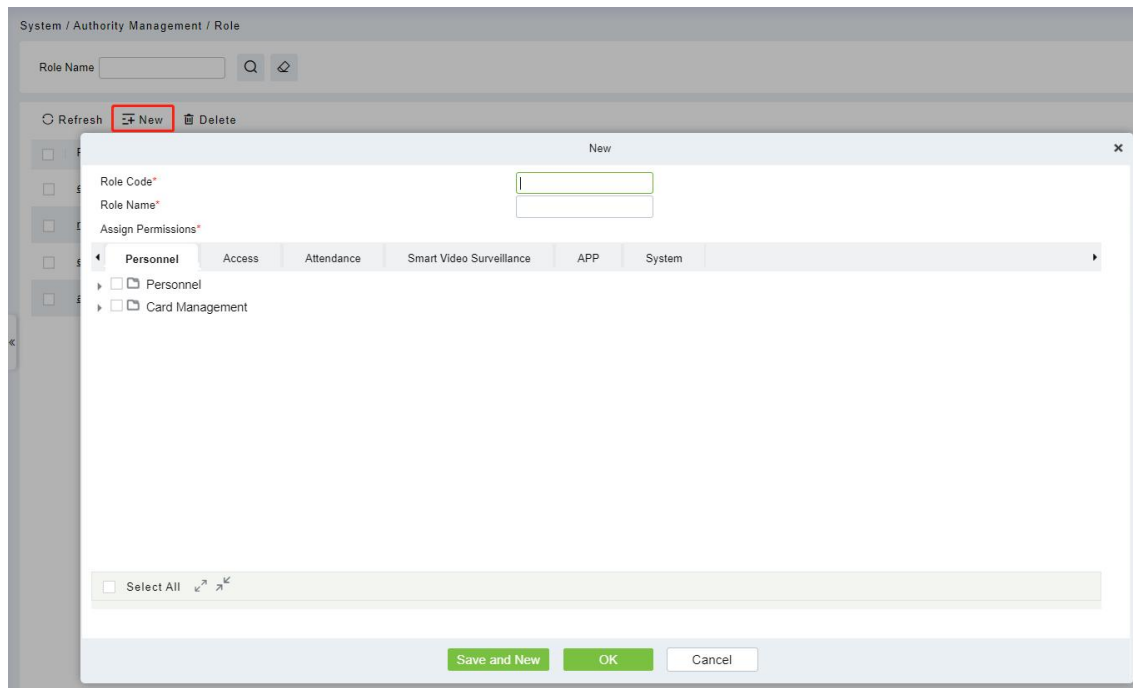
3.   Click **[OK]** to save.

8.2.3 Client Register

You can add client types for the system and generate registration codes for client registrations of each module function. The number of allowed clients is controlled by the number of allowed points.

Click **[System]** > **[Authority Management]** > **[Client Register]**.

➢   **New**
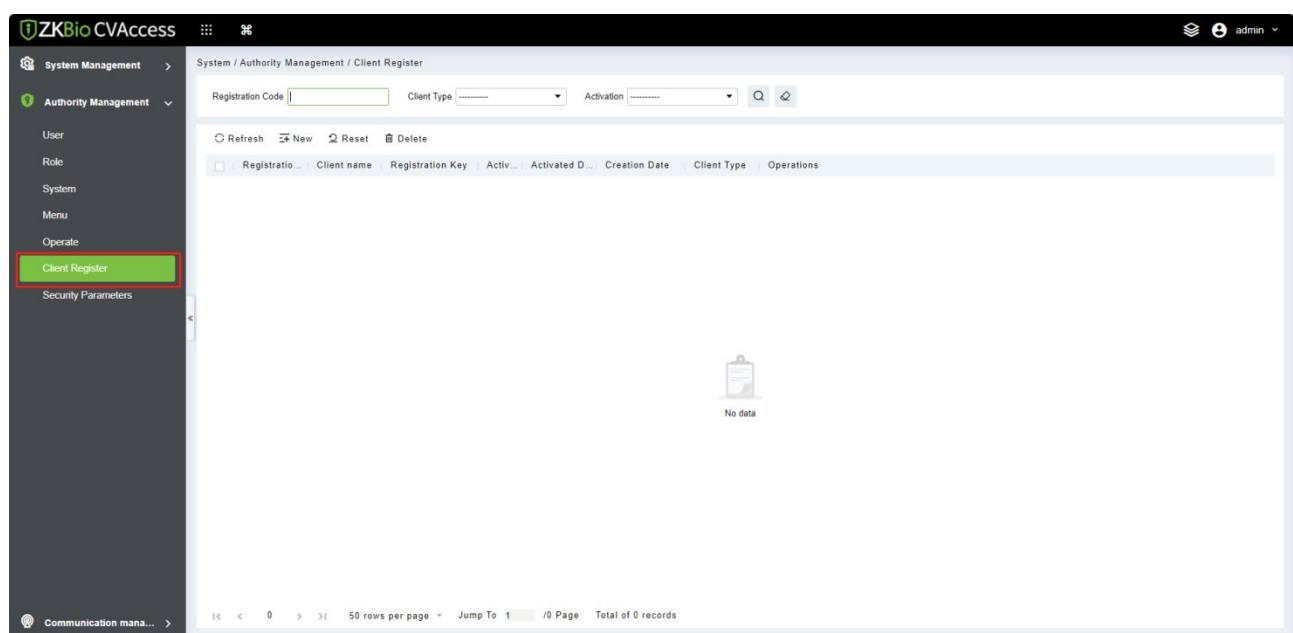
1.   Click **[New]**.
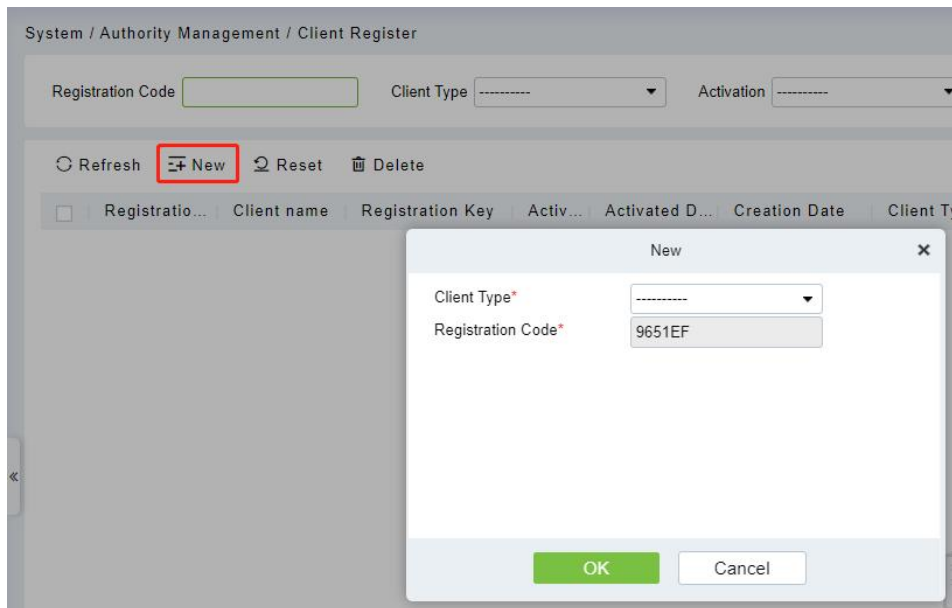
Fields are as follows:

- **Client Type:** The value can be APP Client, OCR-Personnel, OCR-Visitor, ID Reader-Personnel, ID Reader-Visitor or Signature- Visitor, Card Printing- Personnel, Card Printing-Visitor.

- **Registration Code:** The registration code for APP Client is used under Network Settings on the APP login page and that for Print Card-Personnel is used under Parameter Settings > Client Registration. Only new registration codes added on the server are authorized and one registration code can be used by only one client.

2. Click **[OK]** to finish adding.

8.2.4 Security Parameters

Click **[System]** > **[Authority Management]** > **[Security Parameters]**.
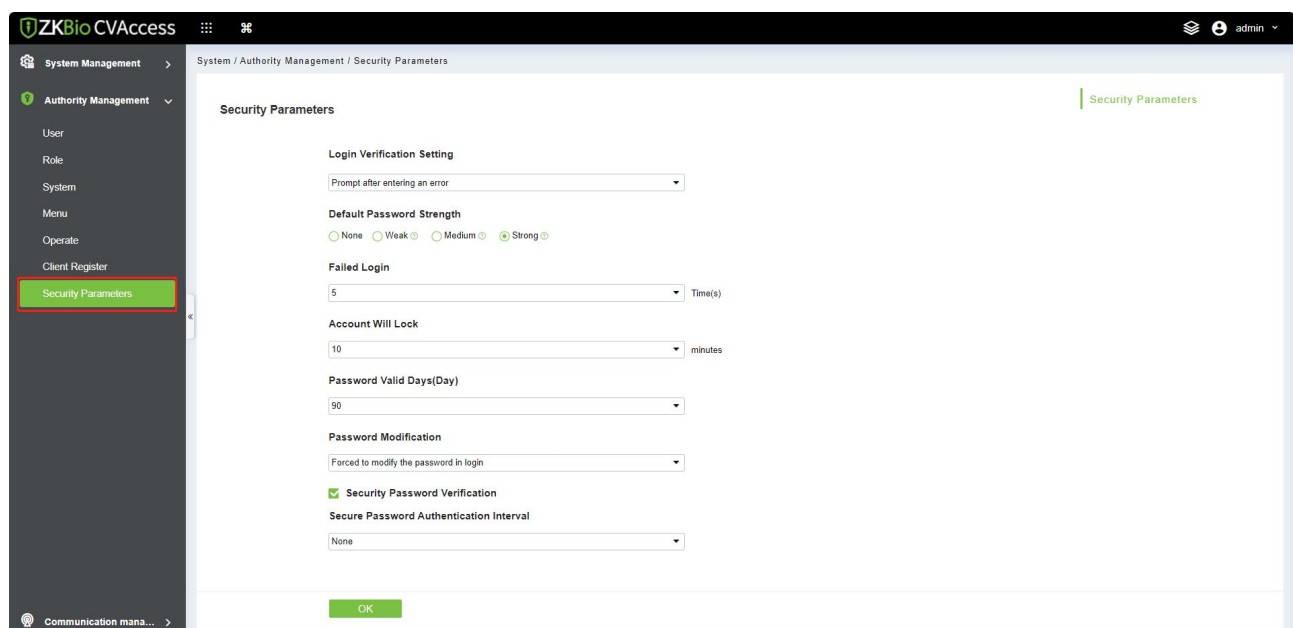
➢ **Login Verification Code Setting**

It includes None, always prompt verification code, Prompt after entering an error.

- **Do not open verification code:** The system allows no verification code

- **Open verification code:** Users must fill in the verification code when logging in to the software.

- **Open after input error:** The system will pop-up a verification box after filling in the wrong Username and password.

➢ **Password Strength Setting**

- **Weak:** The passwords that can be used must contain at least 8 characters and contain at least 2 of the following types: numbers, lowercase letters, uppercase letters, and special characters.

- **Medium:** The passwords that can be used must contain at least 8 characters and contain at least 2 of the following types: numbers, lowercase letters, uppercase letters, and special characters, as well as numbers and lowercase letters or only numbers and uppercase letters.

- **Strong:** The passwords that can be used must contain at least 8 characters and contain at least 3 of the following types: numbers, lowercase letters, uppercase letters, and special characters.

➢ **Account Will Lock**

The account will be locked if user fails to login the system as per the software setting. For example, if the system allows user fill in wrong username and password for 2 times. The system will be locked for 10 minutes after exceeding 2 times of operation.

➢ **Password Valid Day (s)**

Users can set the validity as 30 days, 60 days or permanent. If password gets expired, user cannot login to the system.

➢ **Password Modification**

There are 2 options that user can set. Not mandatory and forced to modify the next time you login.

- **Not mandatory:** The system does not need to modify the initial password.

- **Forced to modify the next time you login:** It is compulsory to modify the initial password after the second login.

➢ **Secure Password Authentication Interval**

Minimum password authentication interval.

8.3 Communication Management

8.3.1 Device Commands

Click **[System]** > **[Communication]** > **[Device commands]**, the commands lists will be displayed.
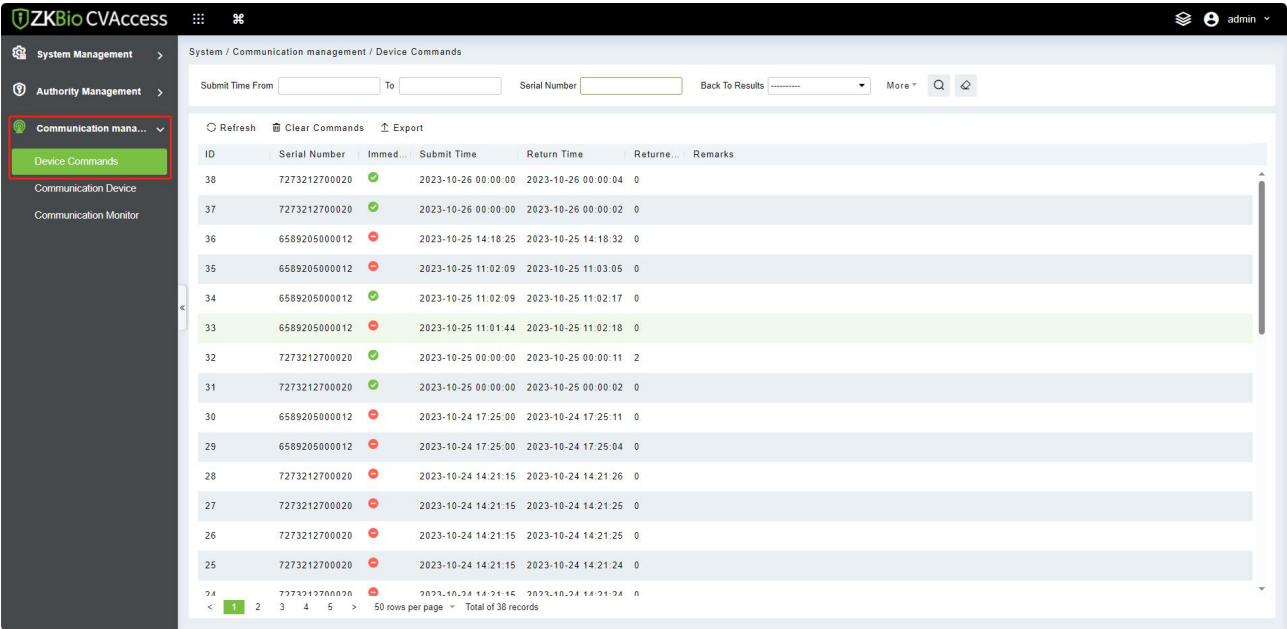
If the returned value is more than or equal to 0, the command is successfully issued. If the returned value is less than 0, the command failed.

➢ **Clear Commands**

Clear the command lists.

➢ **Export**

Export the command lists to local host. You can export to an Excel file. See the following figure.

			Device Commands			
ID	Serial Number	Content	Immediately Cmd	Submit Time	Return Time	Returned Value
1504	20100501999	DATA UPDATE userauthorize Pin=2AuthorizeTi mezoneId=1Auth orizeDoorId=1 Pin=1AuthorizeTi mezoneId=1Auth orizeDoorId=1 ...	false	2017-12-18 10:51:15	2017-12-18 10:51:21	0

8.3.2 Communication Device

Click **[System]** > **[Communication]** > **[Communication Device]**, you can view all equipment information and communication in the system. Detailed information such as accessed module, serial number, firmware version, IP address, communication status, and command execution can be viewed.
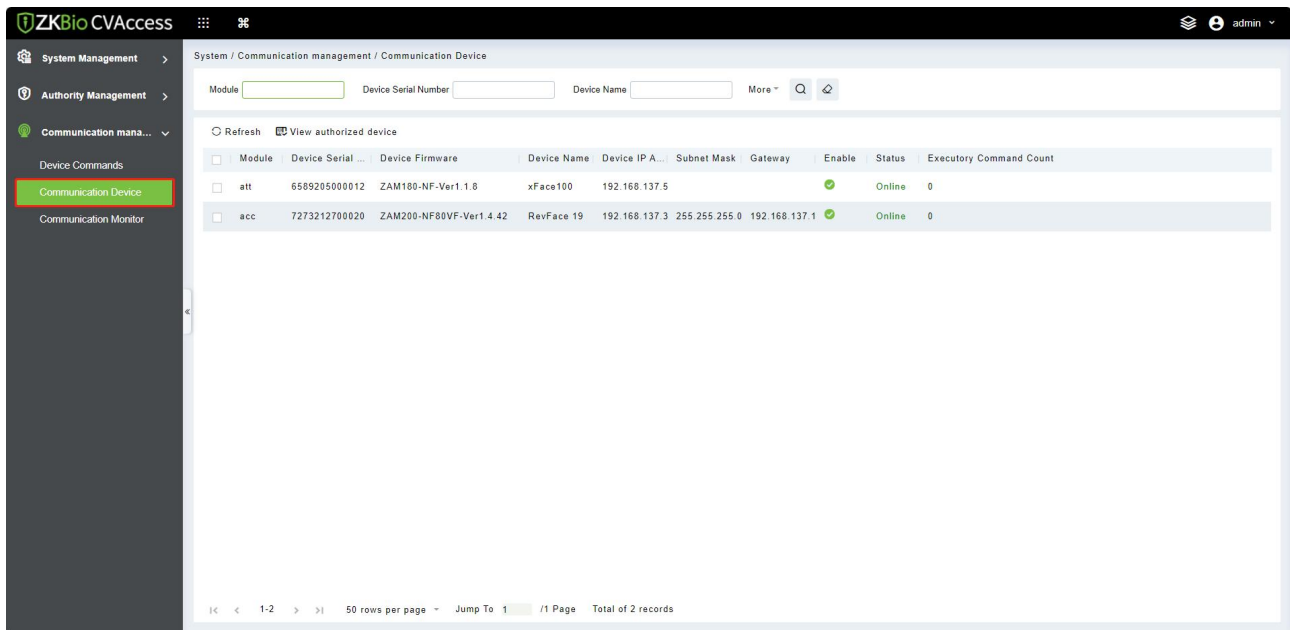
8.3.3 Communication Monitor

Click **[System]** > **[Communication]** > **[Communication Monitor]**, the device service port and its details will be displayed:
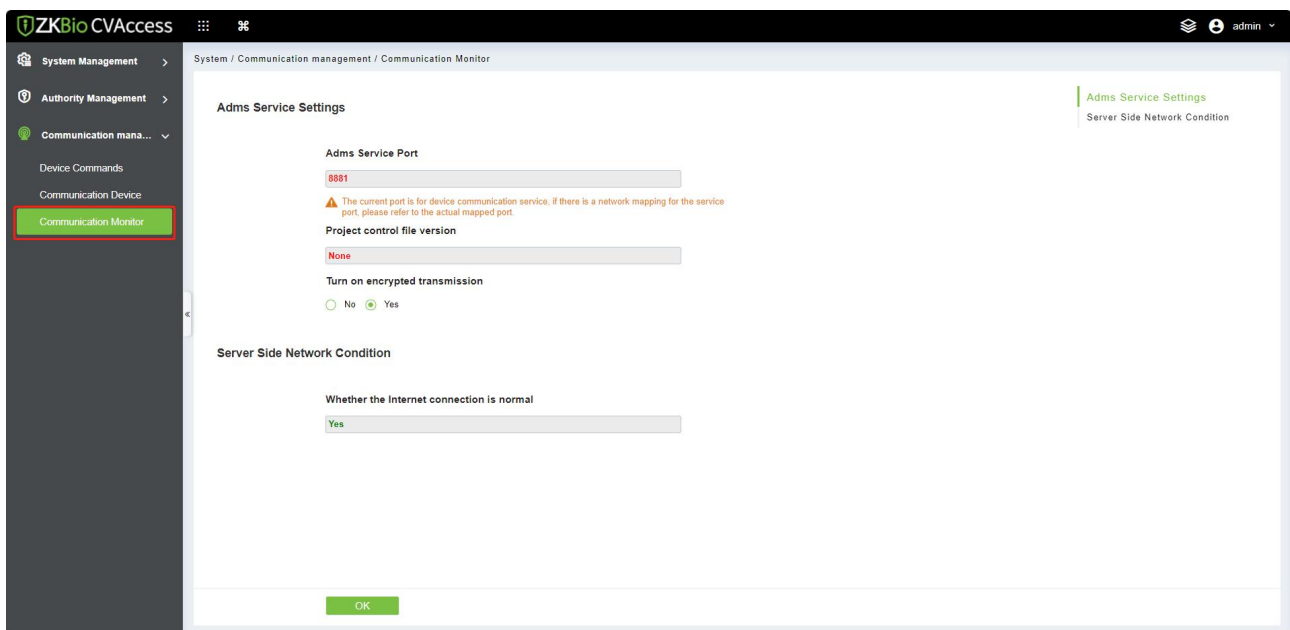
✍**Note:** While installing ZKBio CVAccess, you need to put port number properly.
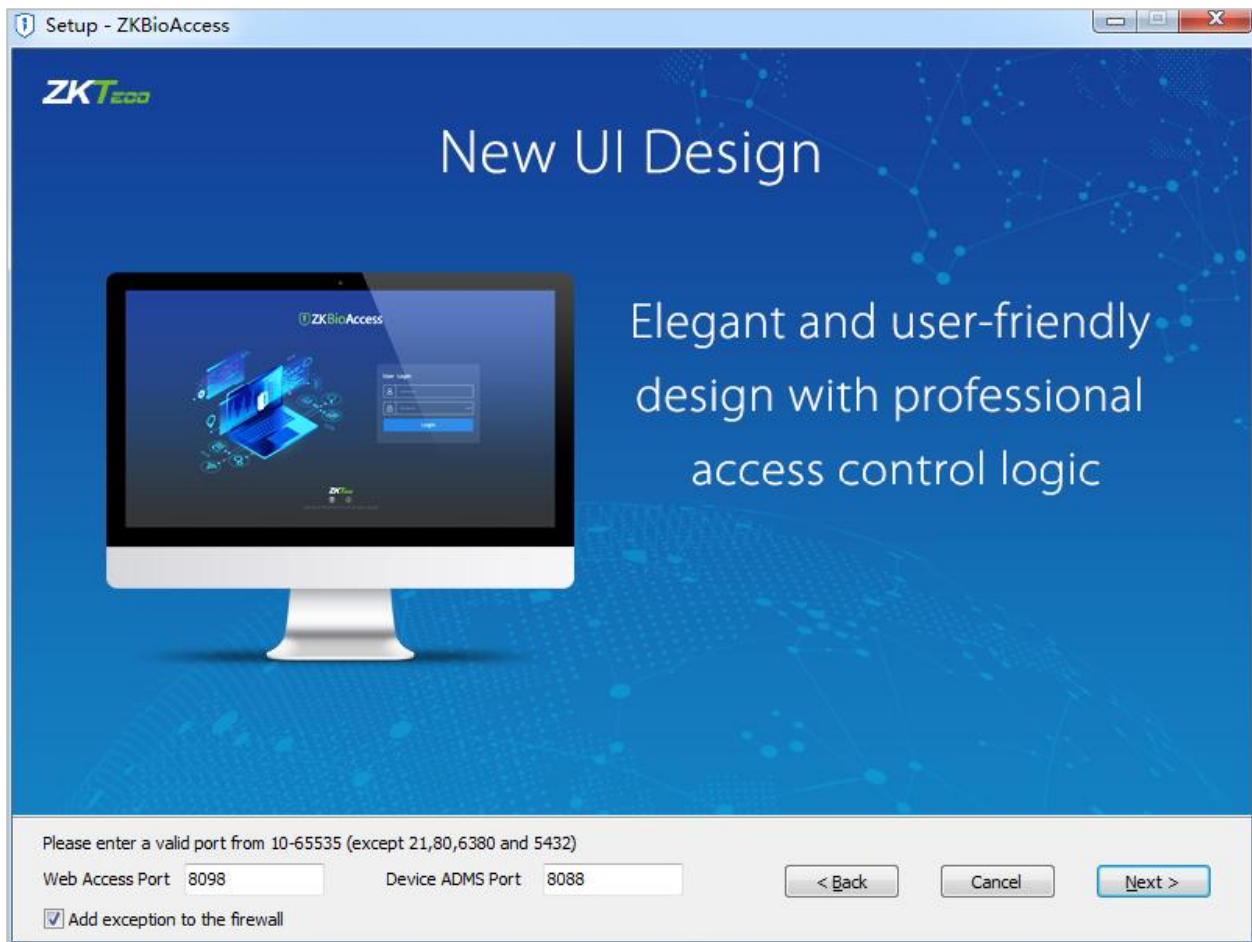
ADMS port is used to connect to the device and the web access port is used to access the website.
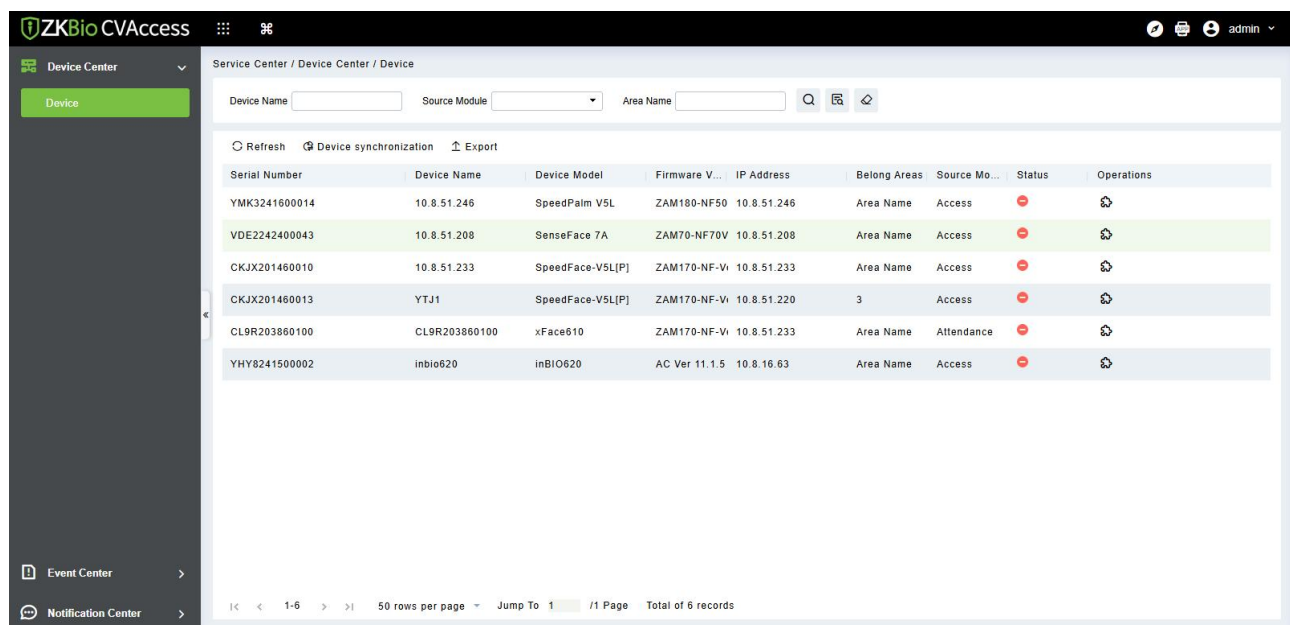
9   Service Center

This module integrates the device and event logging of the system module. Users can import a map to the map center to view the distribution of monitoring points and alarm sources. When an alarm occurs, users can view the location and surrounding conditions of the alarm source, select a suitable monitoring point, and view video live, playback, and human movement functions.

9.1 Device Center

9.1.1 Device

Devices added to the access control and video module are displayed on the screen, and basic device information is displayed, as shown in figure below.

- Device Synchronization:

Synchronize data of the system to the device. Select device, click Synchronize Data to Devices and click OK to complete synchronization.

✍**Note:** Synchronize Data to Devices will delete all data in the device first (except transactions), and thus download all settings again. Please keep the internet connection stable and avoid power down situations. If the device is working normally, please use this function with caution. Execute it in rare user situations to avoid impact on normal use of the device.

9.2 Event Center

Through the definition of the event level and type, it makes the level prompt for the record generated under real-time monitoring.

9.2.1 The Event Type

The software contains event types by default. You cannot add new event types. You can customize the level of the event type.

This section describes how to modify step.

Modify Event Type

To perform the following steps to modify event type:

Step 1: On the Service Center module, choose **Event Center > Event Type**.

Step 2: On the **Event Type** page, select the event type to be modified and click **Event Level**. The Event Level dialog box is displayed.
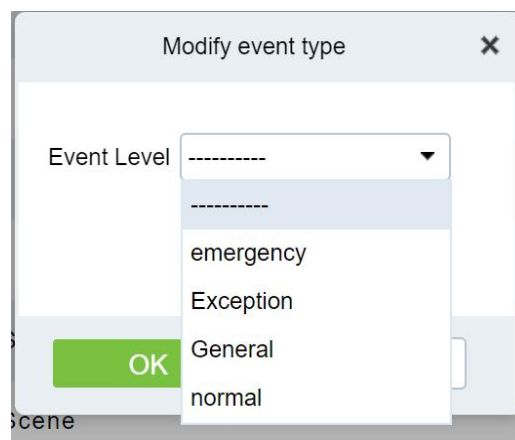
Step 3: After selecting the desired level, Click **OK** to complete changing the event type level.

9.2.2 The Event Record

This screen records all events generated on the platform, as shown in figure below:

In the event record list, after selecting multiple events and clicking Confirm, enter the confirmation details and save. The processing status of the selected events will then change to "Confirmed".
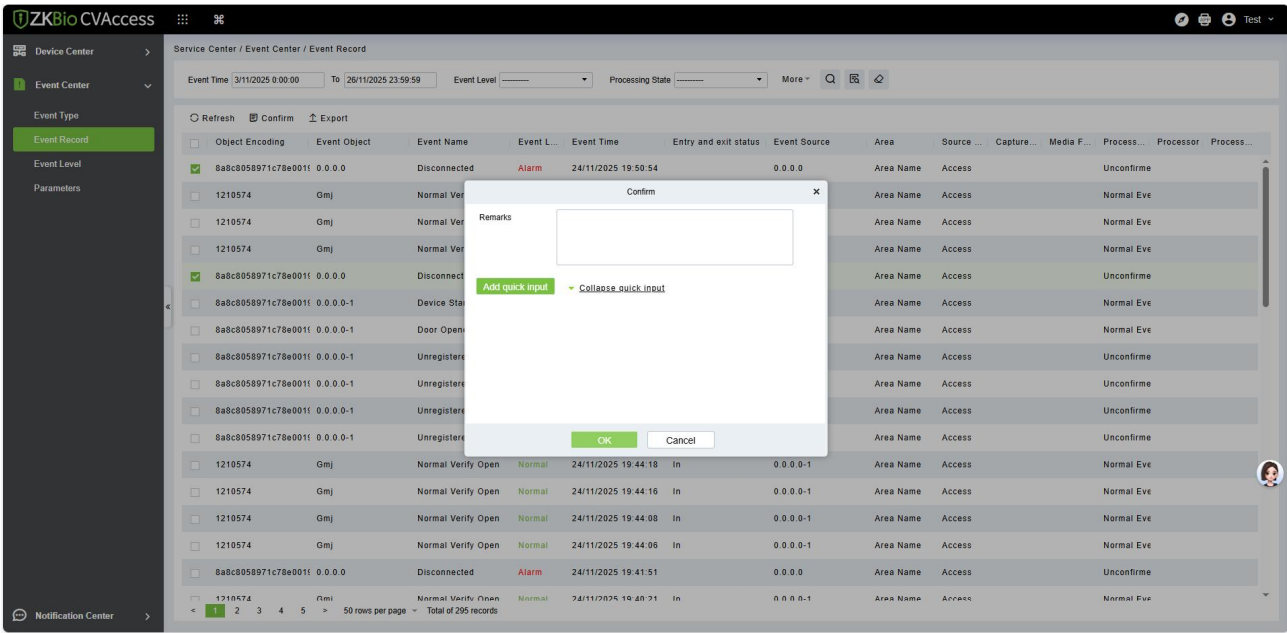
9.3 Notification Center

● Notification Record

This interface records the notification reminding events generated by the attendance and visitor module.
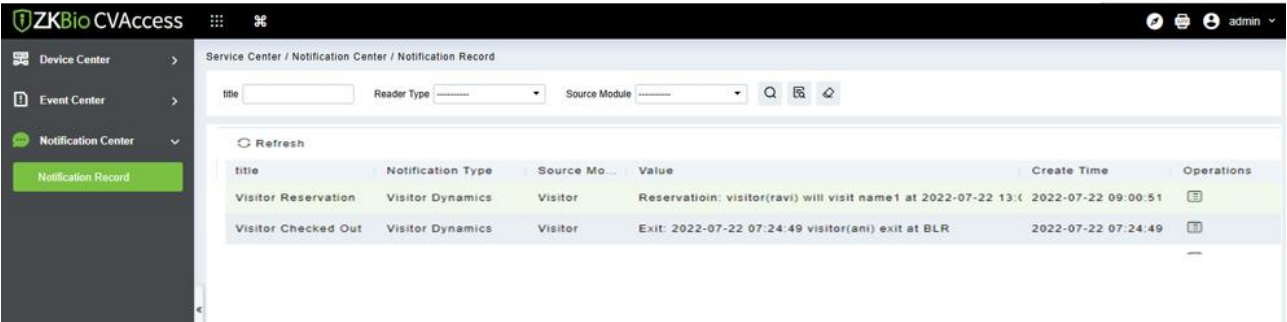
FAQs

Q: How to use a card issuer?

A: Connect the card issuer to the PC through USB port, and then click 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. 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 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, clear the checkbox. 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\ZKBio CVAccess\Main Resource\postgresql\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.

END-USER LICENSE AGREEMENT

Important information - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between Sketch and you (either an individual or a single entity). The **SOFTWARE PRODUCT** includes the Software application, associated media, printed materials, and online or electronic documentation. By installing, copying, or otherwise using the Software Product, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the Software Product.

SOFTWARE PRODUCT LICENSE

The Software Product is protected by copyright laws and international copyright agreements, as well as other intellectual property laws and agreements. The Software Product is licensed and cannot be sold by any third party.

1.   GRANT OF LICENSE

This EULA grants you the following rights:

Installation and Use: You may install the software in an unlimited number of systems.

Replication and Distribution: You may distribute the software to an unlimited number of systems; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. The Software Product may be distributed as a standalone product or can be included in your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Limitations on Deconstruction, Decompilation, and Disassembly

You may not deconstruct, decompile, or disassemble the Software Product, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components

The software product is licensed as a single product. Its components may not be separated for use on more than one system.

Software Transfer

You may permanently transfer your ownership, provided the recipient agrees to the terms of this EULA.

Termination

Without prejudice to any other rights, ZKTeco may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such a case, you must destroy all copies of the Software Product and all of its components.

Distribution

The Software Product may not be sold or be included in a product or package which intends to receive benefits through the inclusion of the Software Product. The Software Product may be

included in any free or non-profit packages or products.

3. COPYRIGHT

All titles and copyrights in and to the Software Product(including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the Software Product), the accompanying printed materials, and any copies of the Software Product are owned by ZKTeco. The Software Product is protected by copyright laws and international agreements. Therefore, you must treat the Software Product like any other copyrighted material except that you may install the Software Product on a single system provided you keep the original solely for backup or archival purposes.

LIMITED WARRANTY

NO WARRANTIES

ZKTeco expressly disclaims any warranty for the Software Product. The Software Product and any related documentation are provided "as it is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or no infringement. The entire risk arising out of use or performance of the Software Product remains with you.

NO LIABILITY FOR DAMAGES

In no event, ZKTeco shall be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if ZKTeco has advised of the possibility of such damages.

Acknowledgment of Agreement

I have carefully read and understood this Agreement, ZKTeco Ltd.,'s Privacy Policy Statement.

If YOU ACCEPT the terms of this Agreement:

I acknowledge and understand that by accepting this agreement, I have to abide by the terms and conditions to use the Software Product to ensure smooth function. I also acknowledge that ZKTeco can terminate the License Agreement if I don't comply with the terms and conditions.

IF YOU DO NOT ACCEPT the terms of this Agreement.

I acknowledge and understand that by refusing to accept these terms, I have rejected this license agreement and therefore have no legal right to install, use, or copy this Product or the Licensed Software that it incorporates.