User Manual

ZKBio CVSecurity

Version: 3.0

Date: January 2026

Software Version: ZKBio CVSecurity_6.7.1_R

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.

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 functions 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 verifications, 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 CVSecurity**.

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

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

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

Table Of Contents

1 Installation and Login

1.1 Operating Environment Requirements

Category	Minimum Requirements
CPU	Core i5 quad-core with a clock speed of 2.8 GHz or higher
RAM	Not less than 8 GB
Hard Disk	500GB minimum (with at least 15GB free space on system disk)
OS	Windows 7/8/8.1/10/11, Windows Server 2008/2012/2016/2019/2022/2025
Graphics Card	Intel integrated graphics, video memory greater than 2.0G (Intel® HD Graphics 530 and above recommended)
Network Card	At least one network card; recommended speed: 1000 Mbps (1 Gbps) or higher
Monitor	At least 21.5 inches, and the best resolution of the monitor is recommended: 1920 * 1080. It is recommended to set the display resolution to 1920 * 1080. Using other resolutions may cause the interface to be abnormal.
Browser	Support Chrome33+ (recommended)/Firefox27+/Explorer11+/Microsoft Edge 89+

Table 1- 1

Instruction:

The number of live channels supported under the minimum configuration requirements:

Resolution	Configuration a (H.264 format)	Configuration a (H.265 format)
CIF (512K)	38	38
4CIF/D1 (2M)	22	22
720P (2M 25fps)	10	10
1080P (4M 25fps)	6	6

Table 1- 2

In the video preview window, you can view the system CPU or memory usage in real time. If the CPU reaches 80%, it is not recommended to increase the video preview window, which will cause the video stream to freeze; if the CPU has reached 80% and the video window does not meet the actual application, the system configuration needs to be improved.

1.2 System Installation

Step 1: Obtain the installation package.

Instruction:

Before installing the software, it is recommended to close the anti-virus software in the system to avoid failing the environment detection. If the antivirus software detects abnormality, you can also choose to ignore it.

After running the application, there will be a few seconds of detection process, please be patient.

Step 2: Right-click the installation package installer, choose to run as an administrator, and the environment detection tool will automatically perform system environment detection. If an abnormality is detected during the installation process, the interface will give a prompt. The user can refer to the prompt information to repair, and re-test after repairing until all the test items are passed before proceeding to the next Step.

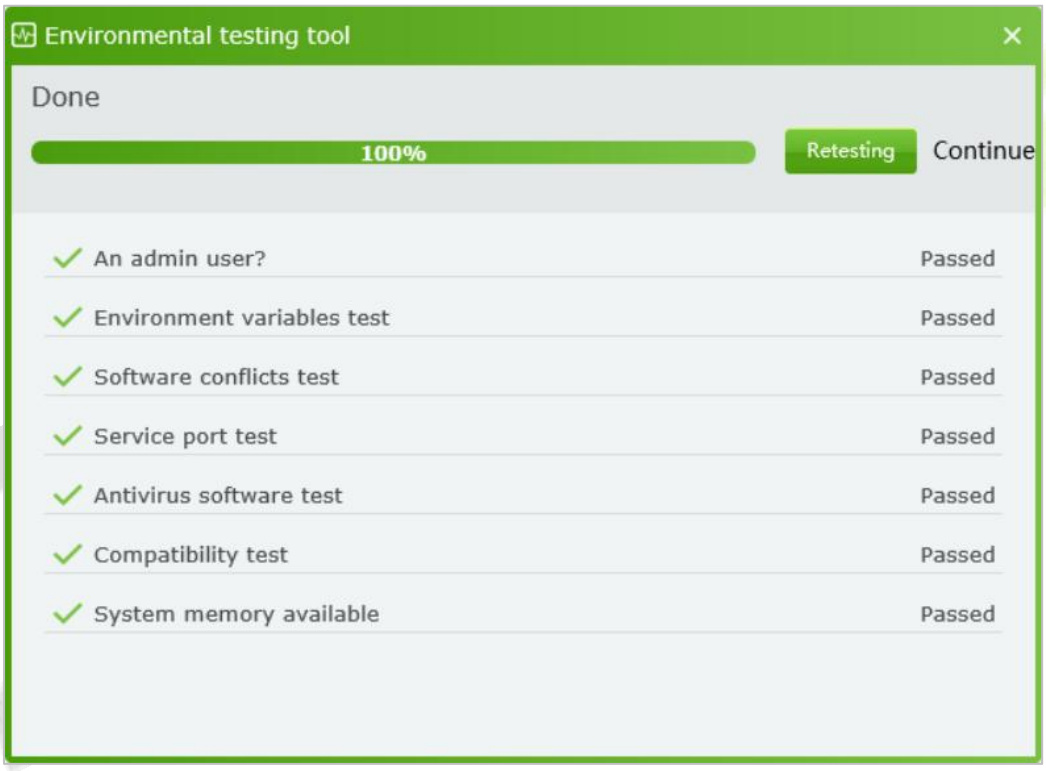


Figure 1- 1

Step 3: If the detection is normal, click **Continue**.

Step 4: Select "I agree to this agreement (A)" and click **Next**.

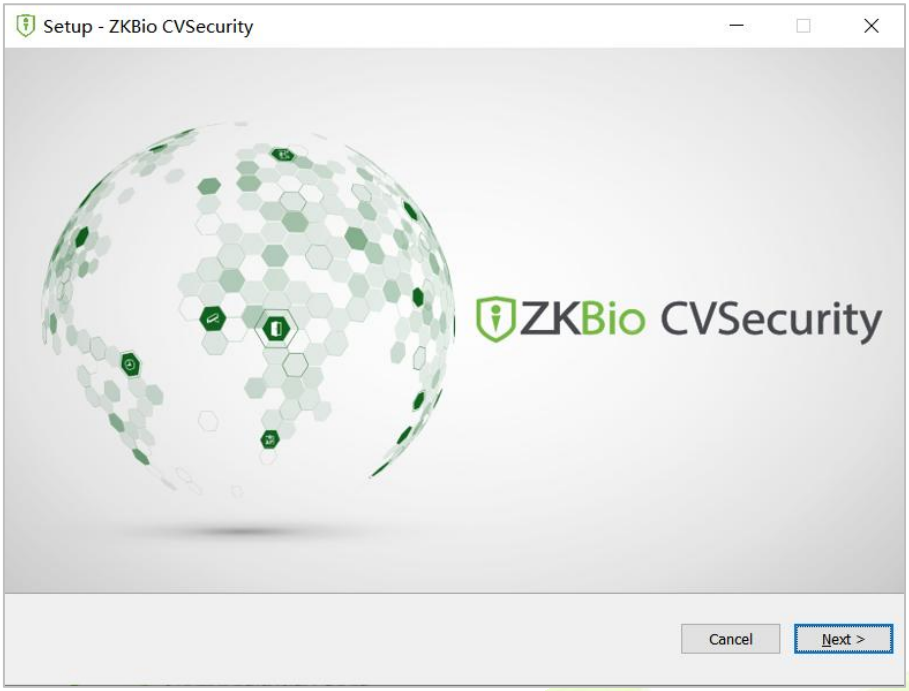


Figure 1- 2

Step 5: After configuring the server port and other parameters, click **Next**.

Instruction:

Default port: 8098

Admin service port: 8088 (default)

HTTPS protocol is enabled by default

Important:

If port 8098 is already in use, manually assign a different port. Avoid conflicts with:

- System reserved ports
- Database port (5442)
- Redis port (6390)
- Web service ports (21, 80)

Firewall:

Check "Add firewall exception to this port" to prevent Windows Firewall from blocking the program.

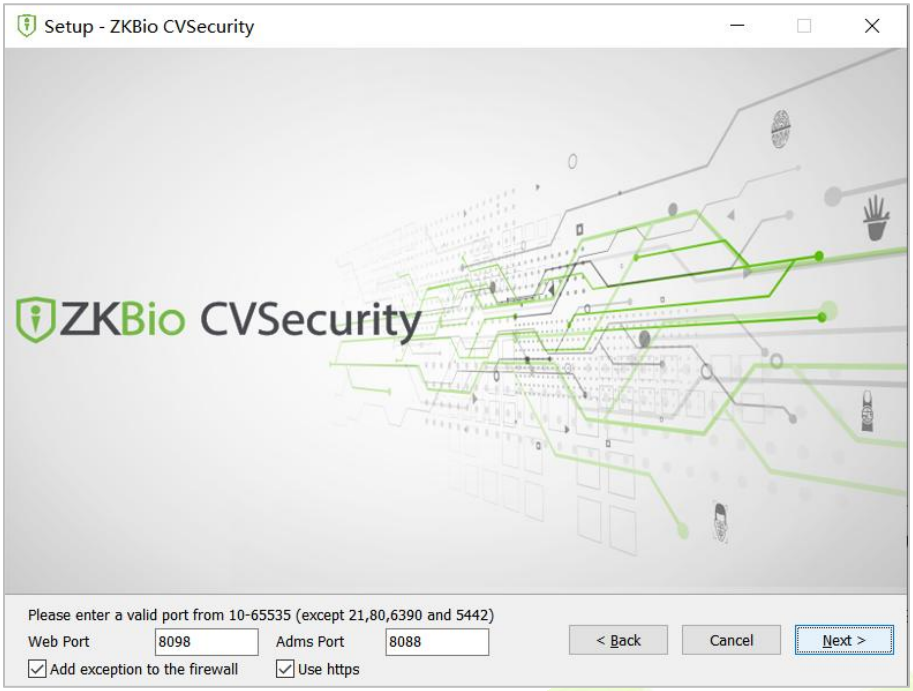


Figure 1- 3

Step 6: After setting the installation directory, click **Next**.

Instruction:

The default installation path is C:\Program Files\ZKBioCVSecurity. You can also click **Browse** to customize the installation path. Please follow the interface prompts to ensure that the selected installation path has enough disk space.

Figure 1- 4

Step 7: After setting the backup file storage path, click **Next**.

Instruction:

The system scans the entire disk by default, locates the drive letter with the largest free space, and creates a new SecurityDBBack folder. You can also click **Browse** to customize the storage path of the

backup file.

Figure 1- 5

Step 8: Select the modules needed for your project, then click **Next**

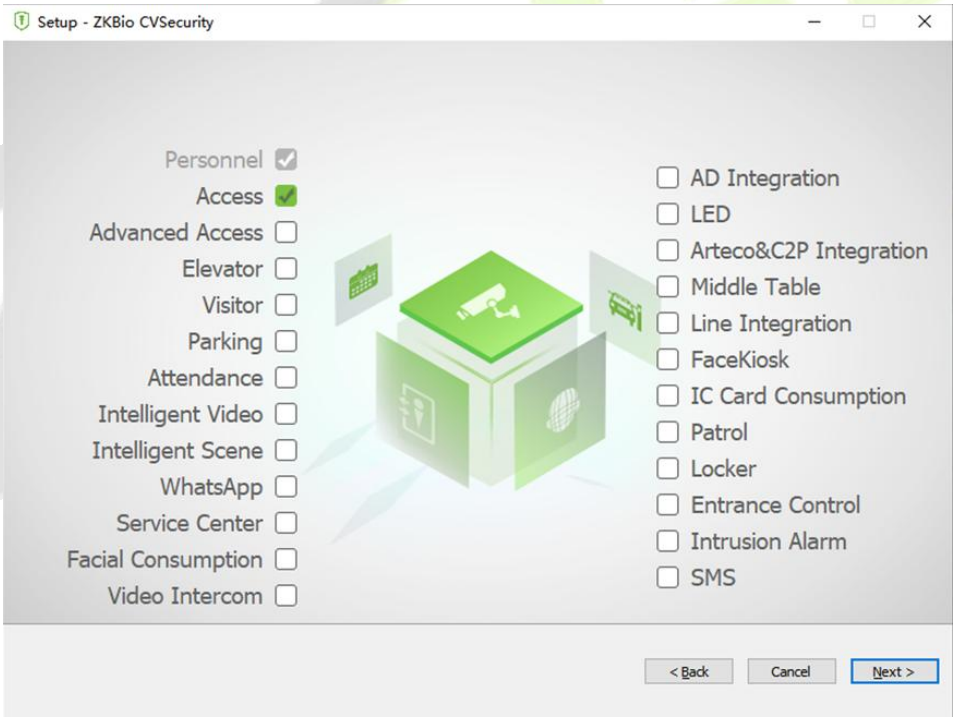


Figure 1- 6

Step 9: After the installation is complete, you will be prompted whether to restart the computer immediately (the default is "Yes"). Click **Finish** to restart the computer to complete the software installation.

Instruction:

After the software installation is complete, it will take a long time (about 2 minutes) for the service to start up. Please wait patiently for the service to start and then complete the operation.

Step 10: Enter the login page as shown in figure below, log in to the system.

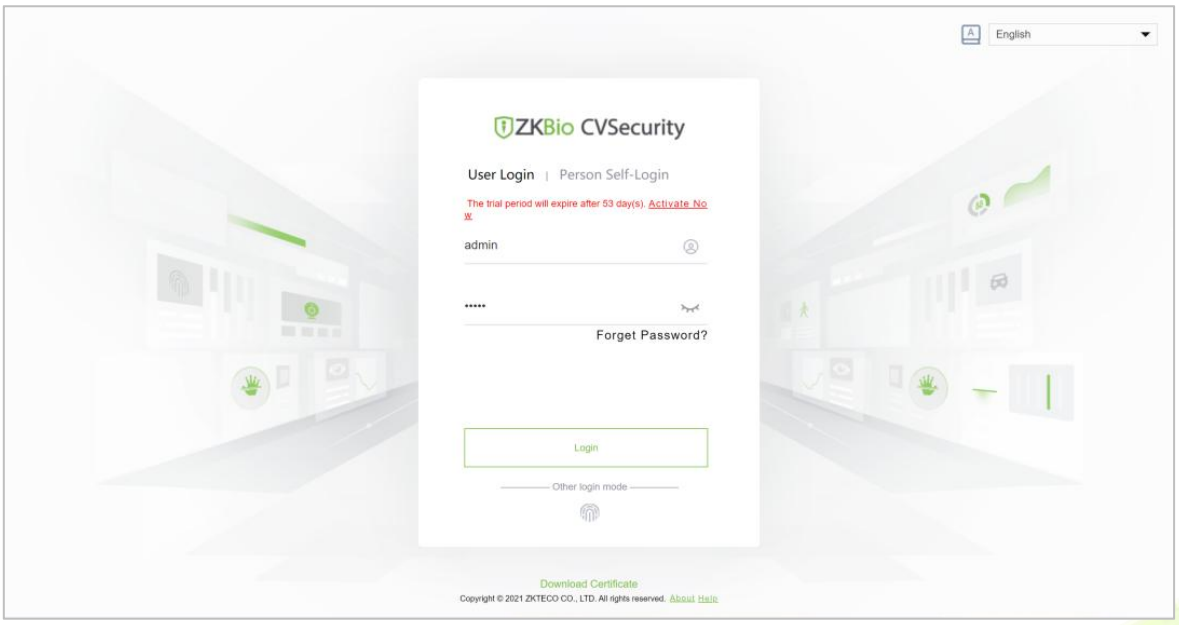


Figure 1- 7

1.3 Self-service License Reset

In general, the software license and the client's server correspond to each other, which means that once a license has been registered, it cannot be used on any other server. However, in special cases, customers may need to perform server migration. For example, if the performance of the original server is too low or if the original server is being damaged, etc., the customer needs to migrate the license to the new server.

At this point, customers can utilize the self-service license reset function, which enables users to reset the license associated with the original server and reactivate it on the new server. This not only enhances the efficiency of license migration but, more importantly, eliminates the need for users to purchase new licenses.

1.3.1 Online Deactivation + Online Activation

● Description:

Deactivate the original server online, and activate the new server online.

● Preconditions:

Both original server and the new server are being connected to the network.

● Steps:

1. Click **Admin > About > Online Deactivation.**

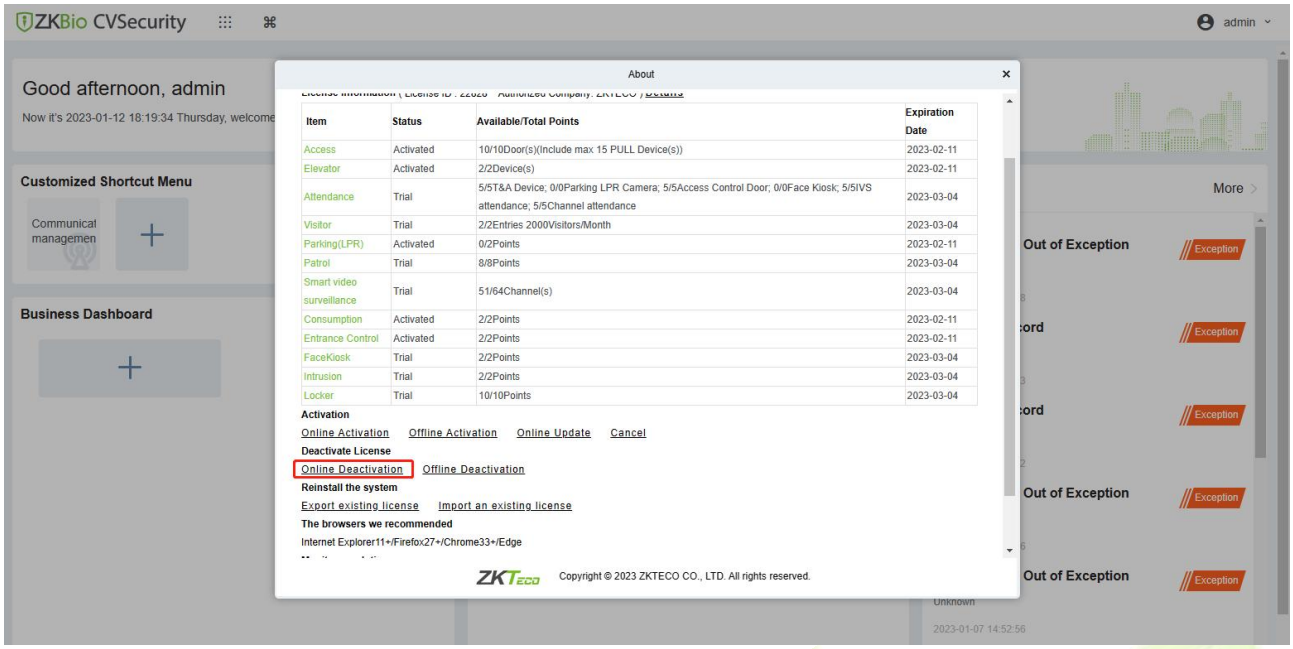


Figure 1- 8 Online Deactivation

2. Click **OK**.

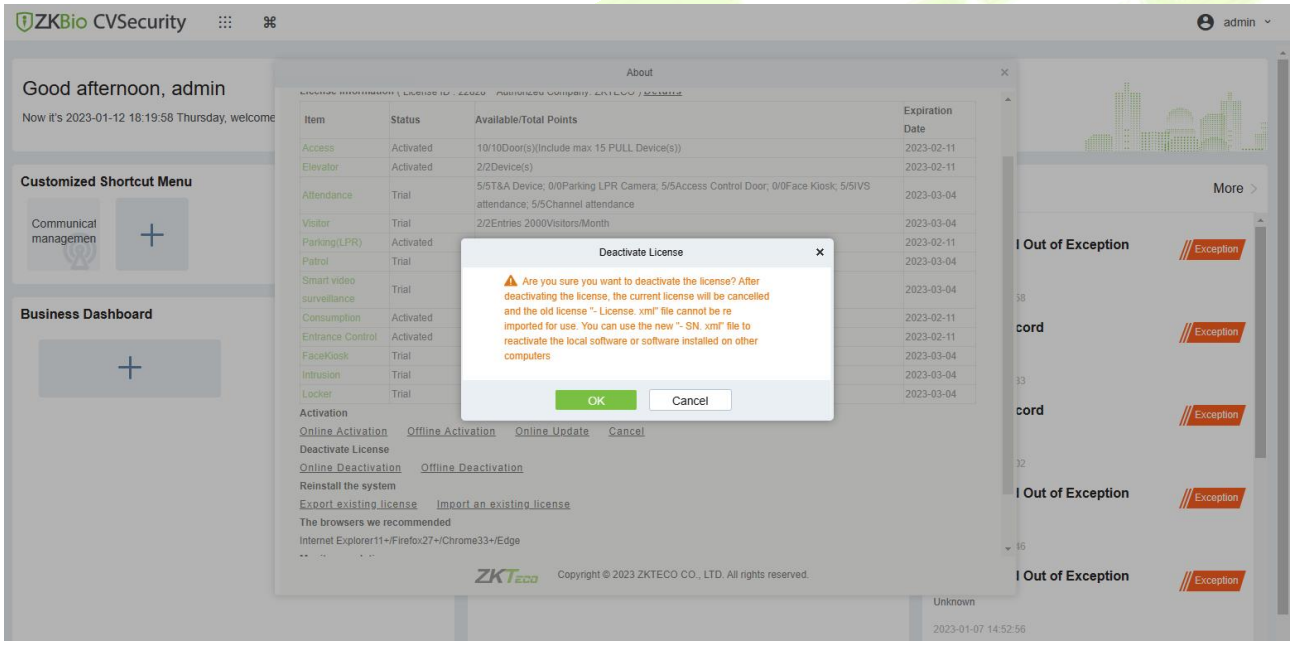


Figure 1- 9 Online Deactivation Confirm.

3. Click **Download**, then a license file with a suffix of SN.xml will be downloaded.

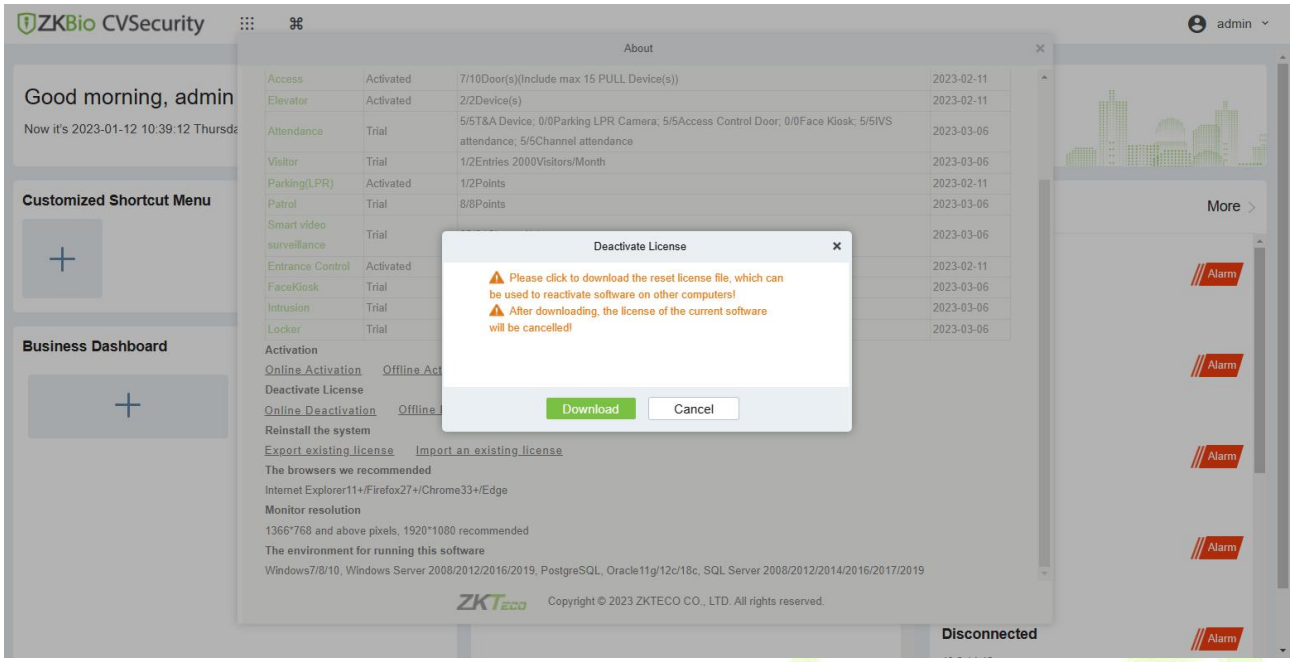
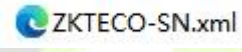


Figure 1- 10 Online Deactivation File Download.

4. Save the license file with a suffix of SN.xml you just downloaded.



5. Log in to a new server.

6. Click **Admin** > **About** > **Online Activation**. Fill in the relevant information, then click on **Browse** to upload the file you got from previous step with the SN.xml suffix

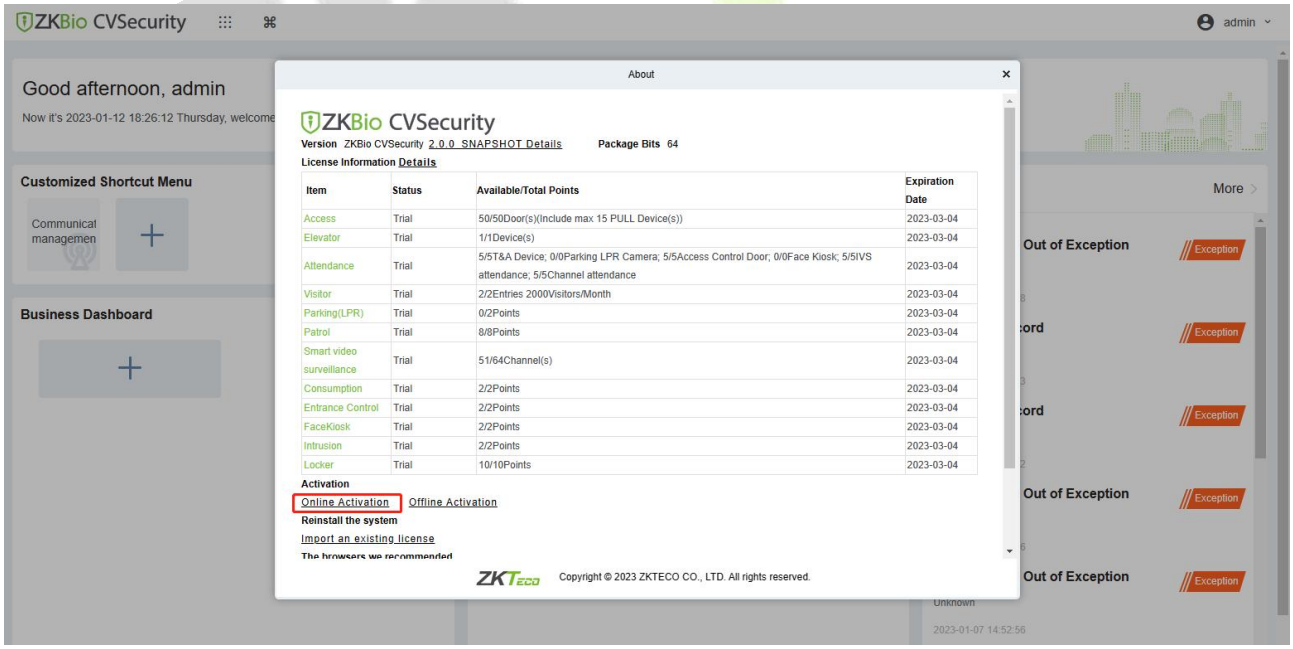


Figure 1- 11 Online Activation

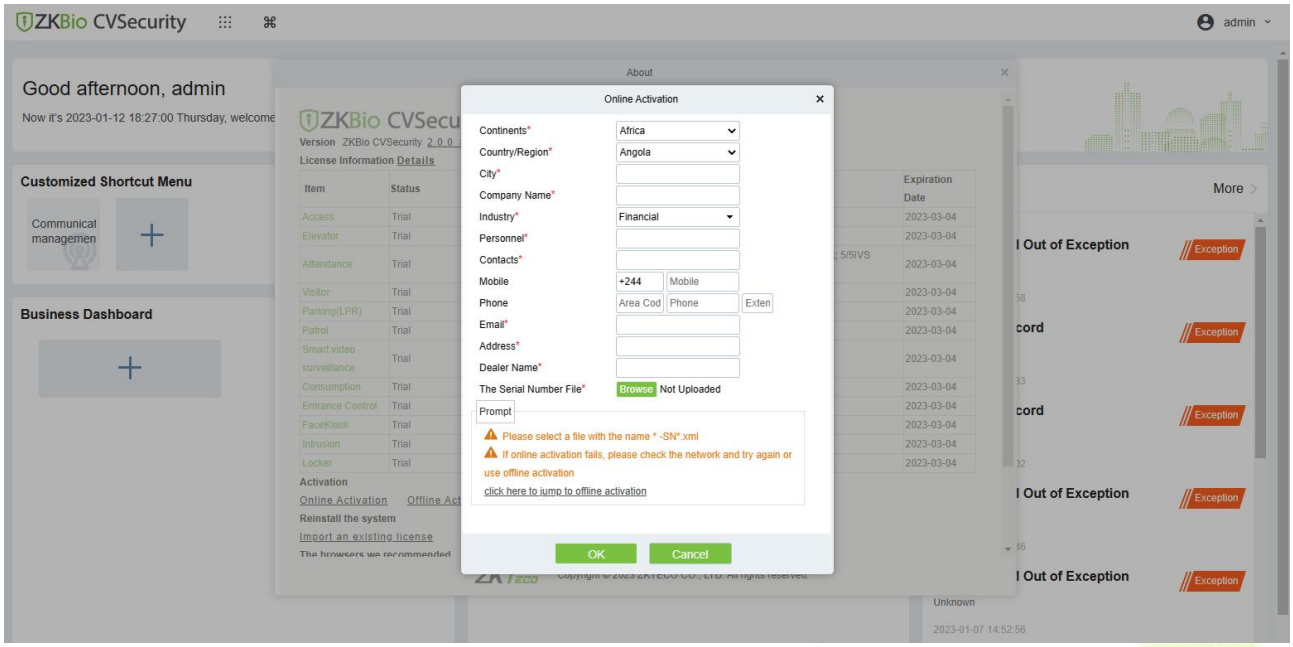


Figure 1- 12 Online Activation Confirm

7. The activation is successful. The following is the successful activation interface:

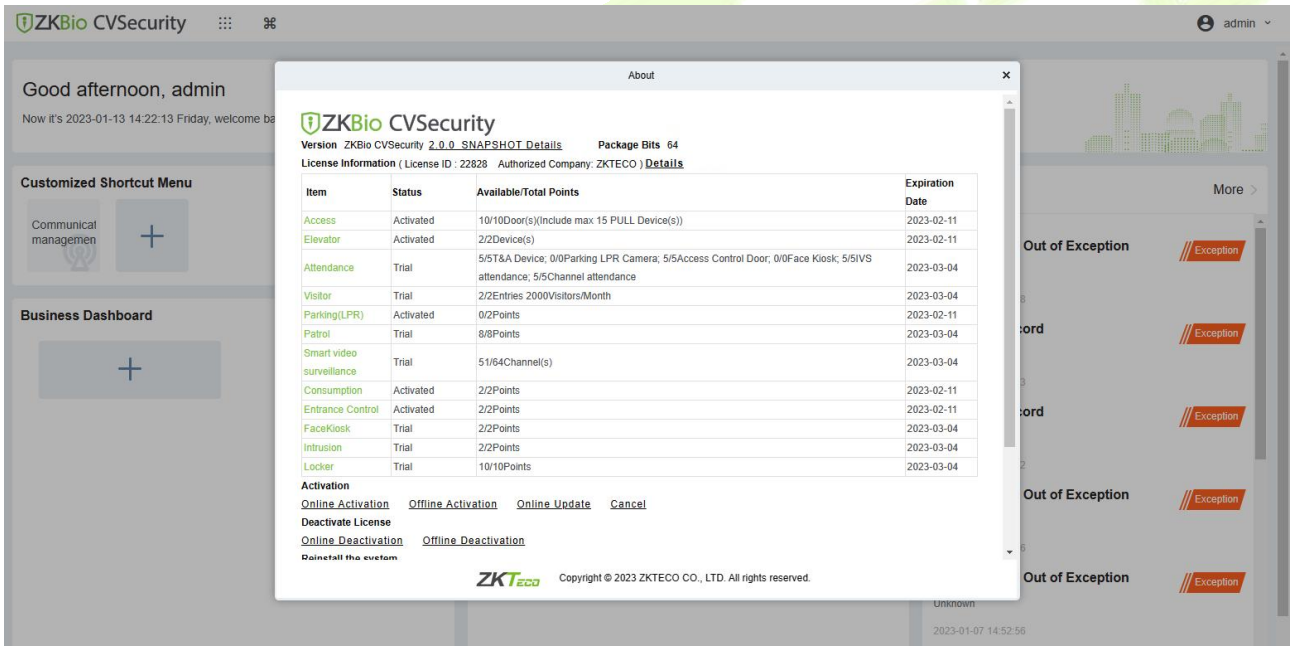


Figure 1- 13 License Activation Succeeded

1.3.2 Offline Deactivation + Online Activation

● Description:

Offline deactivate the original server, and then online, activate the new server.

● Preconditions:

The original server is not connected to the network, while the new server is connected to the network.

● Steps:

1. Click **Admin > About > Offline Deactivation**.

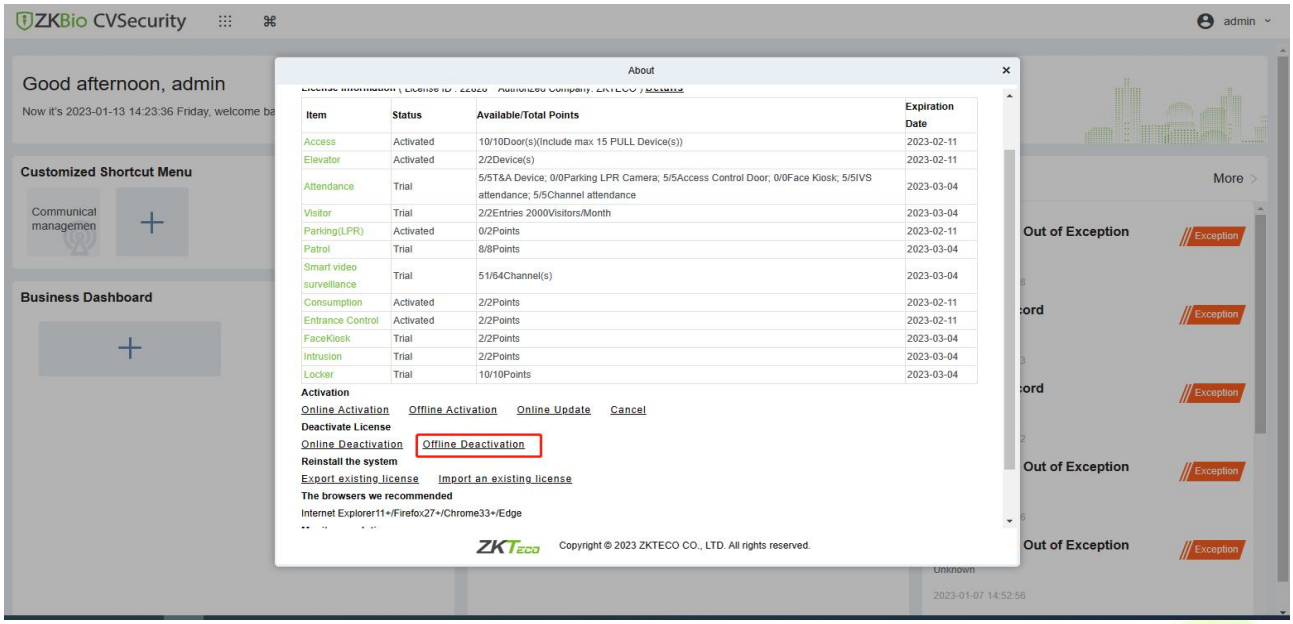


Figure 1- 14 Offline Deactivation

2. Click **OK** .

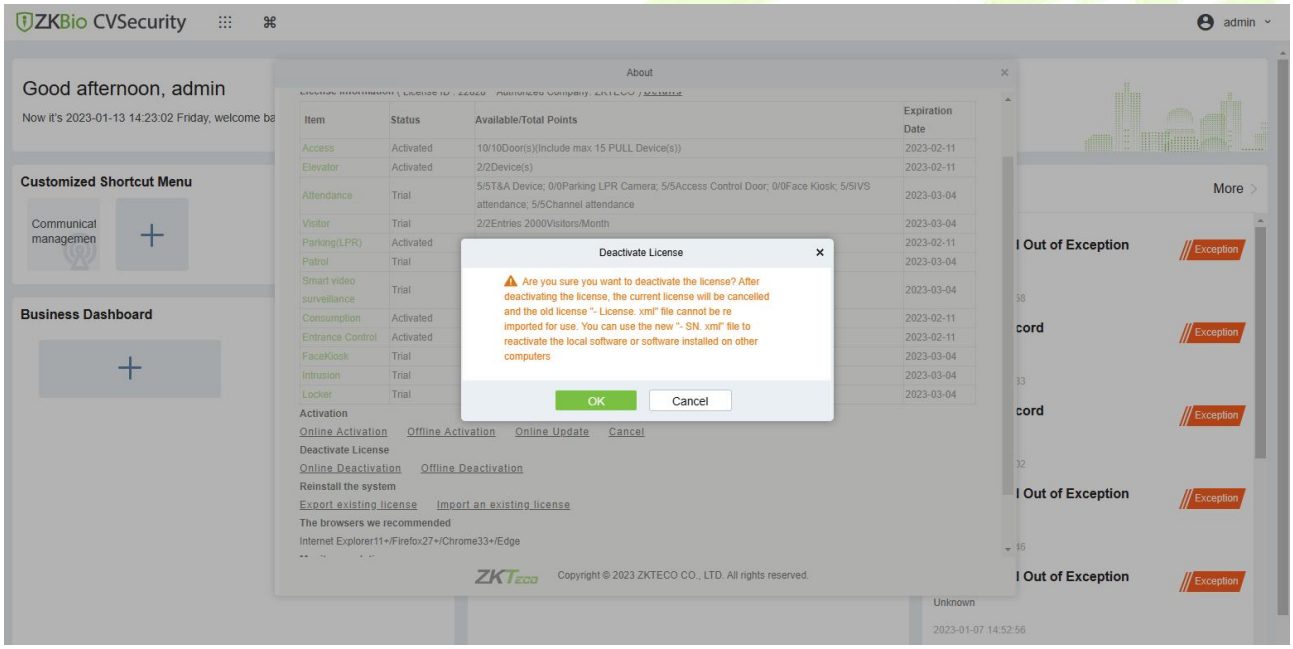


Figure 1- 15 Offline Deactivation Confirm

3. Click **Download**, and then a license file with a suffix of BackActi.xml will be downloaded.

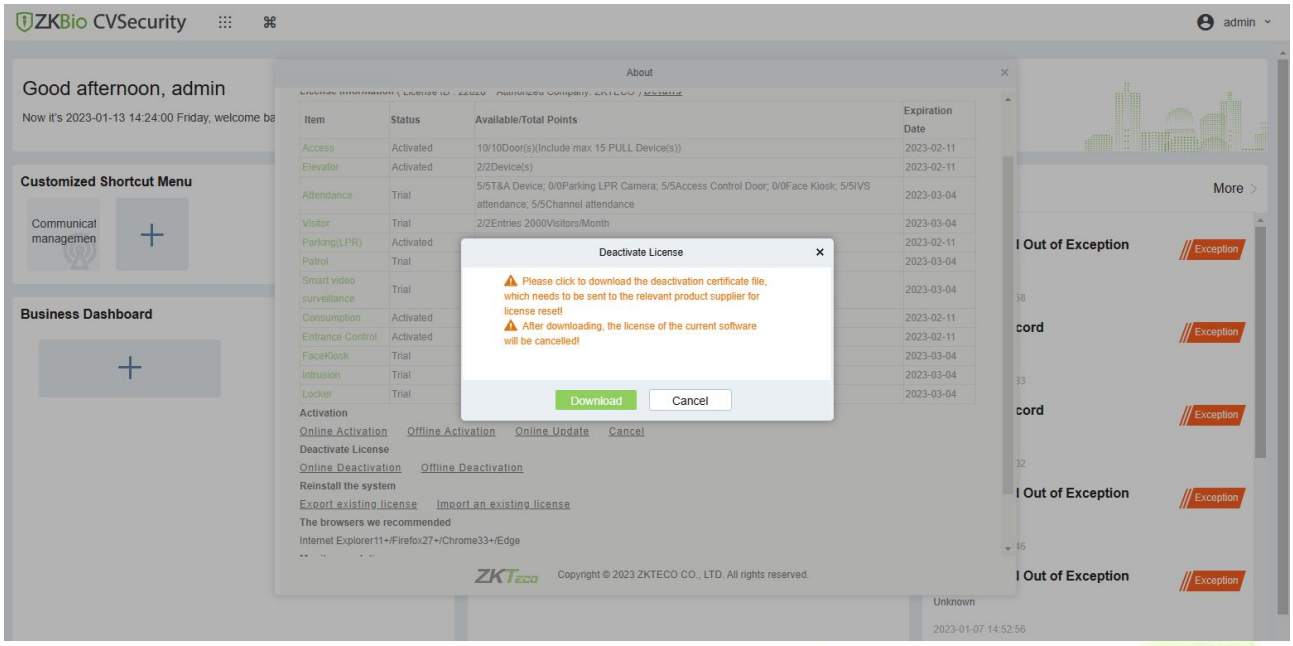
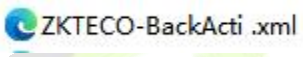


Figure 1- 16 Offline Deactivation File Download

4. Save the license file with a suffix of BackActi.xml that you just downloaded.



5. Open the ZKBio CVSecurity License Deactivate page.

Web Link: [ZKBio CVSecurity License Deactive (zkteco.com)]

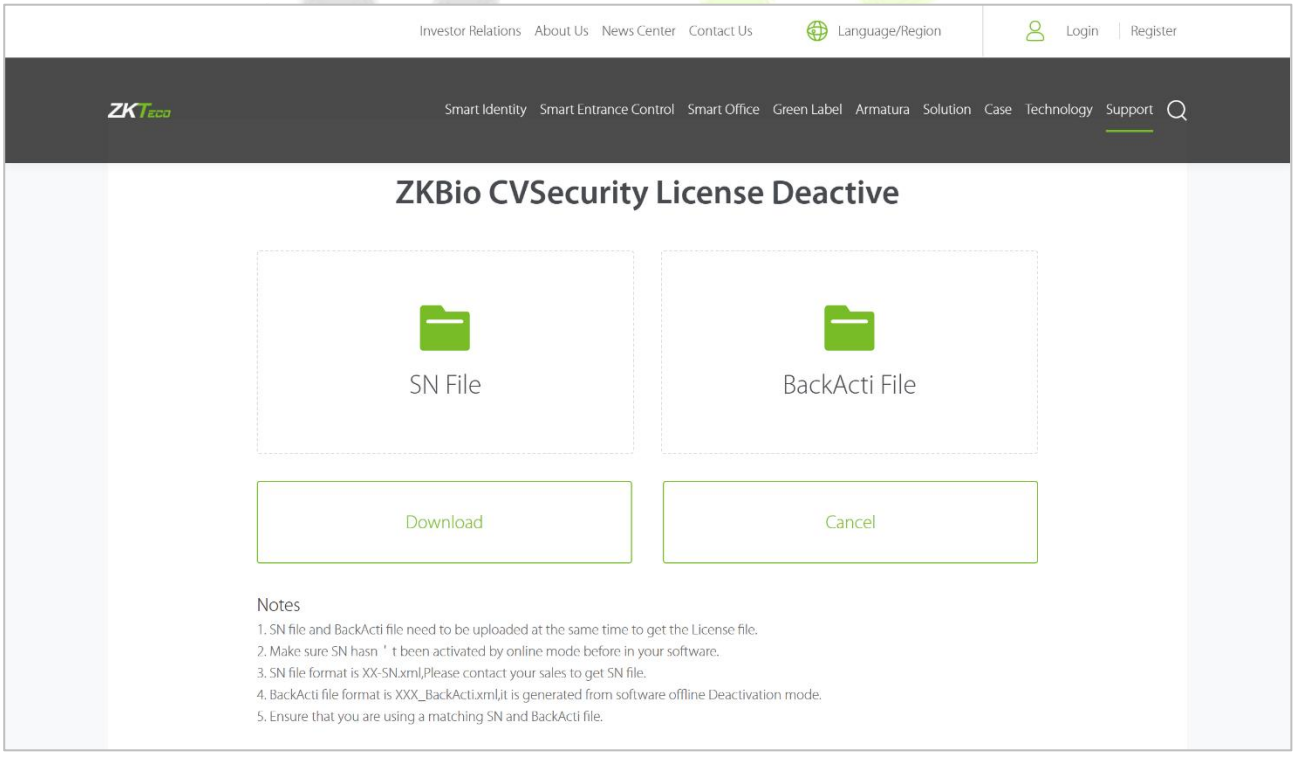


Figure 1- 17

6. Follow the instructions on the page to upload the SN file and the BackActi file downloaded in step 4 in turn.

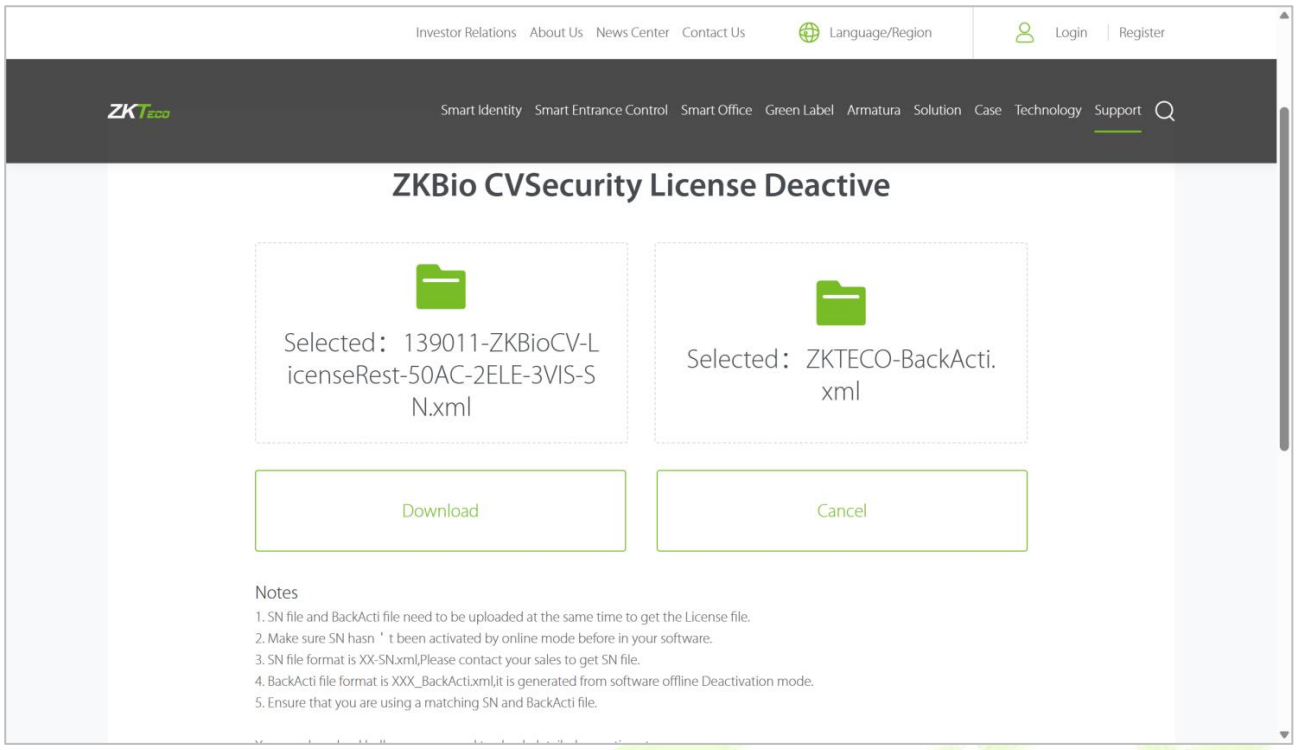


Figure 1- 18

7. Click the Download button to download the activation file.

8. Log in to a new server.

9. Click **Admin > About > Online Activation**. Fill in the relevant information, then click on Browse to upload the file that you just got from previous step with the SN.xml suffix.

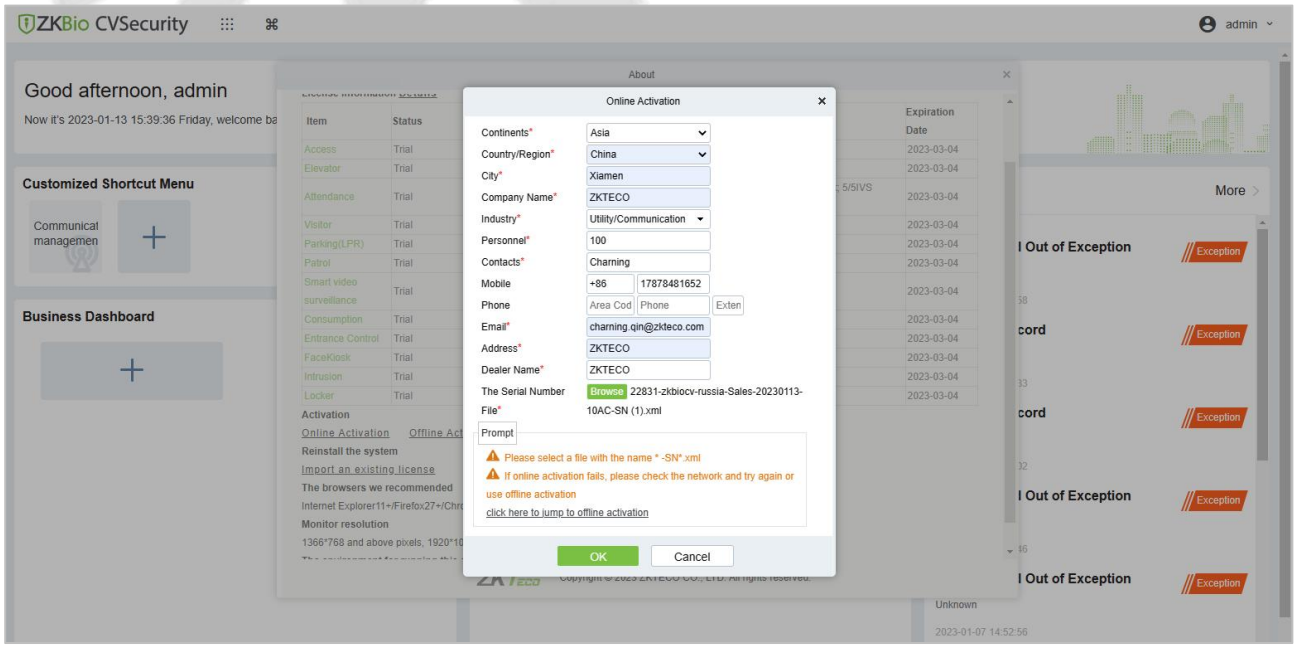


Figure 1- 19 Information Filling and File Uploading

10. The activation is successful. The following is the successful activation interface:

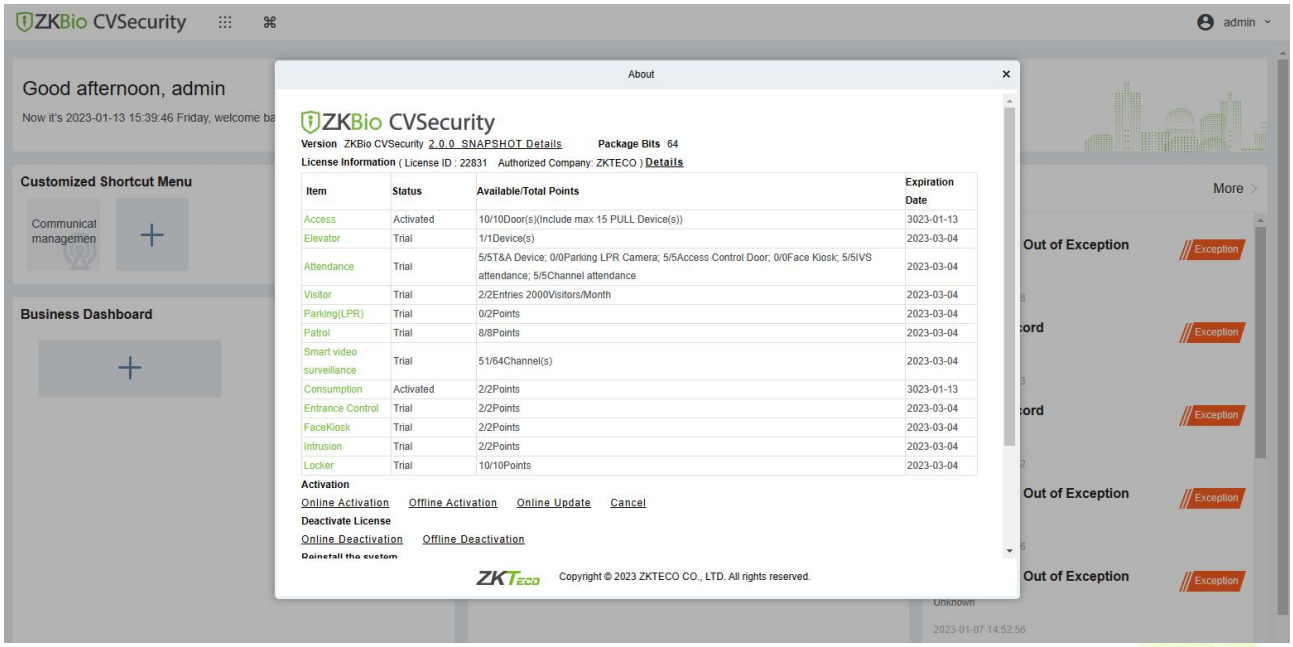


Figure 1- 20 License Activation Succeeded

1.3.3Online Deactivation + Offline Activation

● Description:

Deactivate the original server online, and activate the new server offline.

● Preconditions:

Original server is connected to the network, and the new server is not connected to network.

● Steps:

1. Click Admin > About > Online Deactivation.

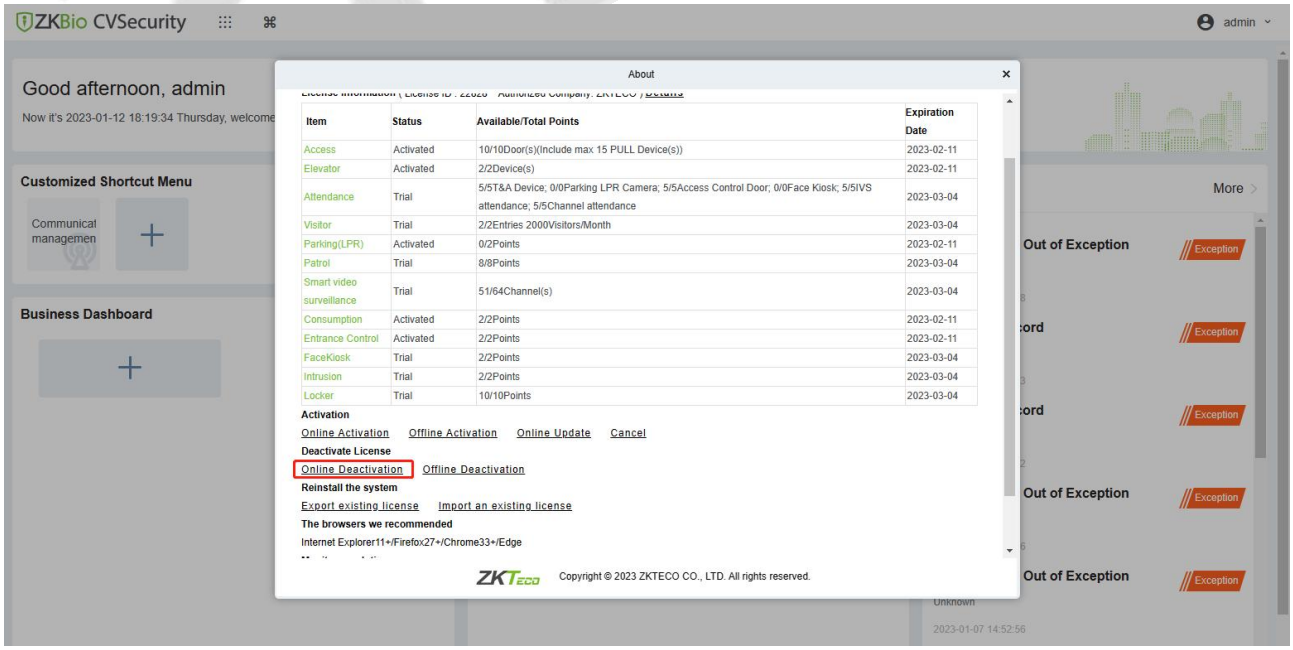


Figure 1- 21 Online Deactivation

2. Click OK.

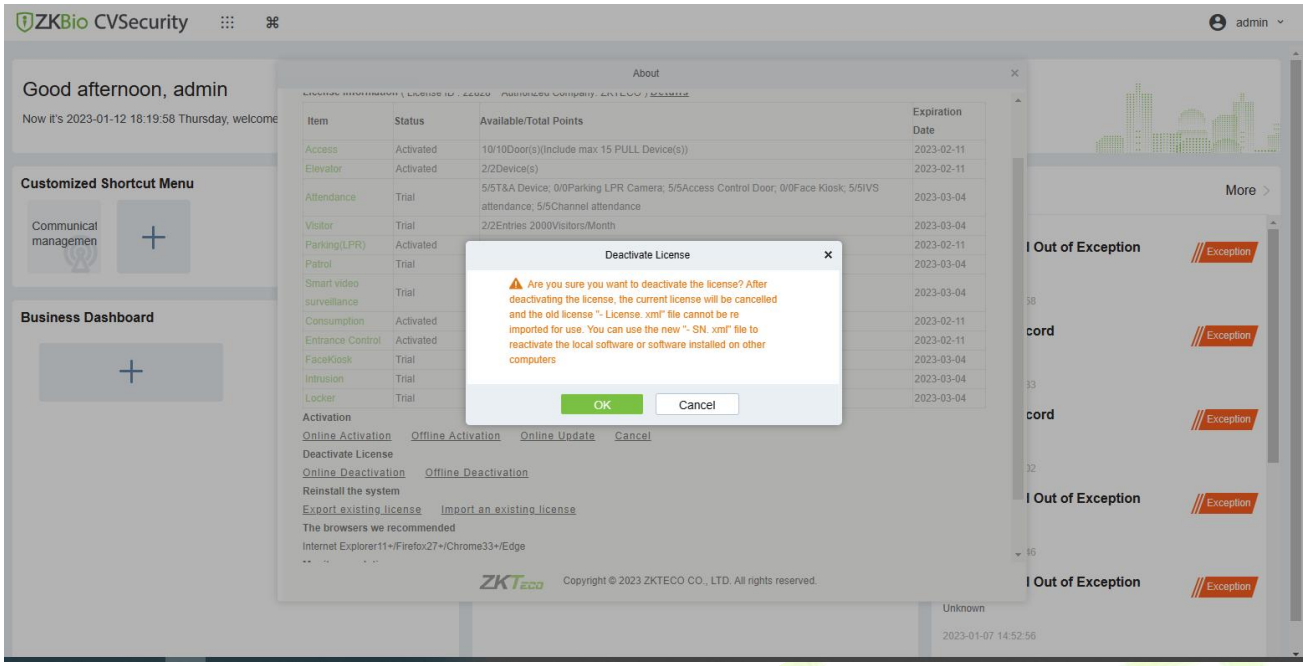


Figure 1- 22 Online Deactivation Confirm

3. Click Download, and then a license file with a suffix of SN.xml will be downloaded.

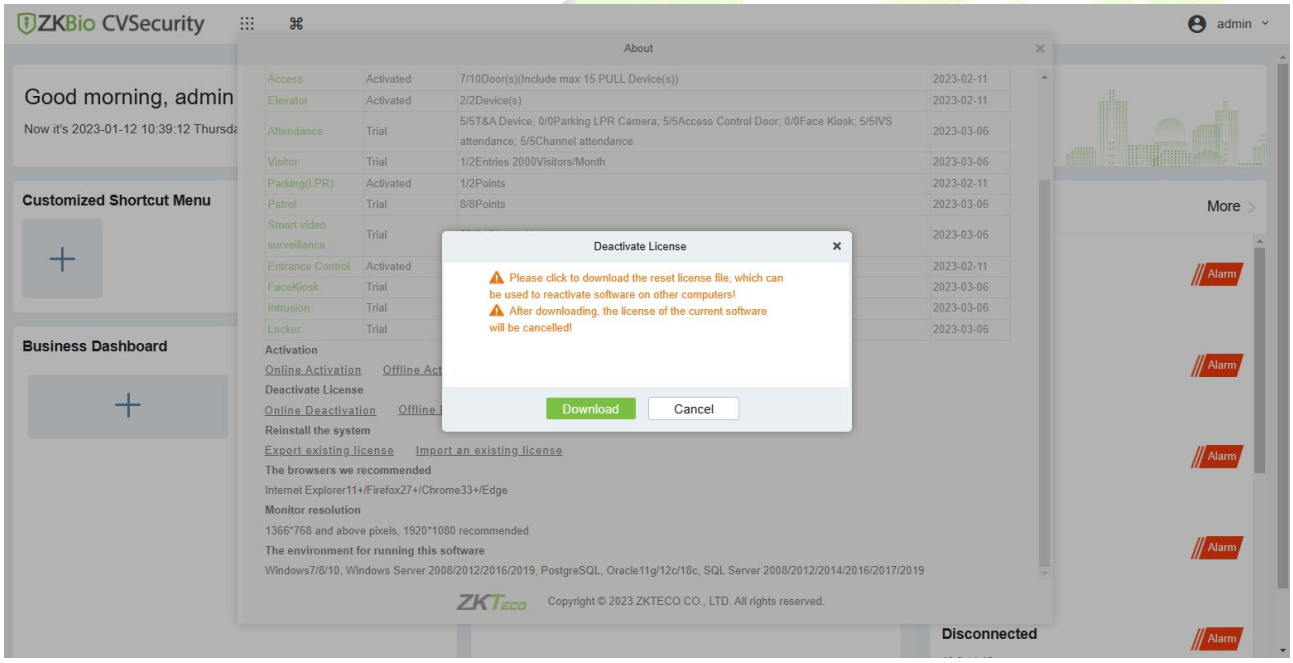
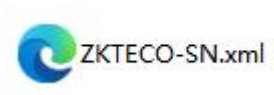


Figure 1- 23 Online Deactivation File Download

4. Save the license file with a suffix of SN.xml you just downloaded.



5. Log in to a new server.

6. Click Admin > About > Offline Activation. Fill in the relevant information, then click Browse to upload the file that you just got from the previous step with the SN.xml suffix.

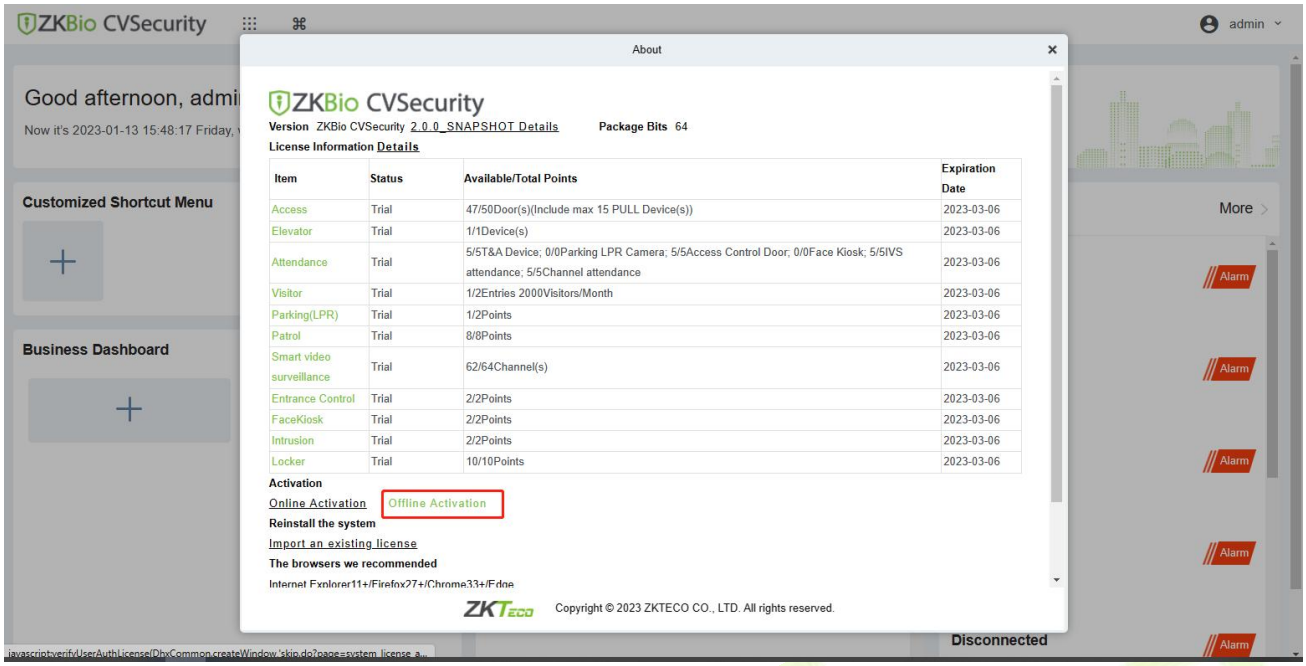


Figure 1- 24 Online Activation

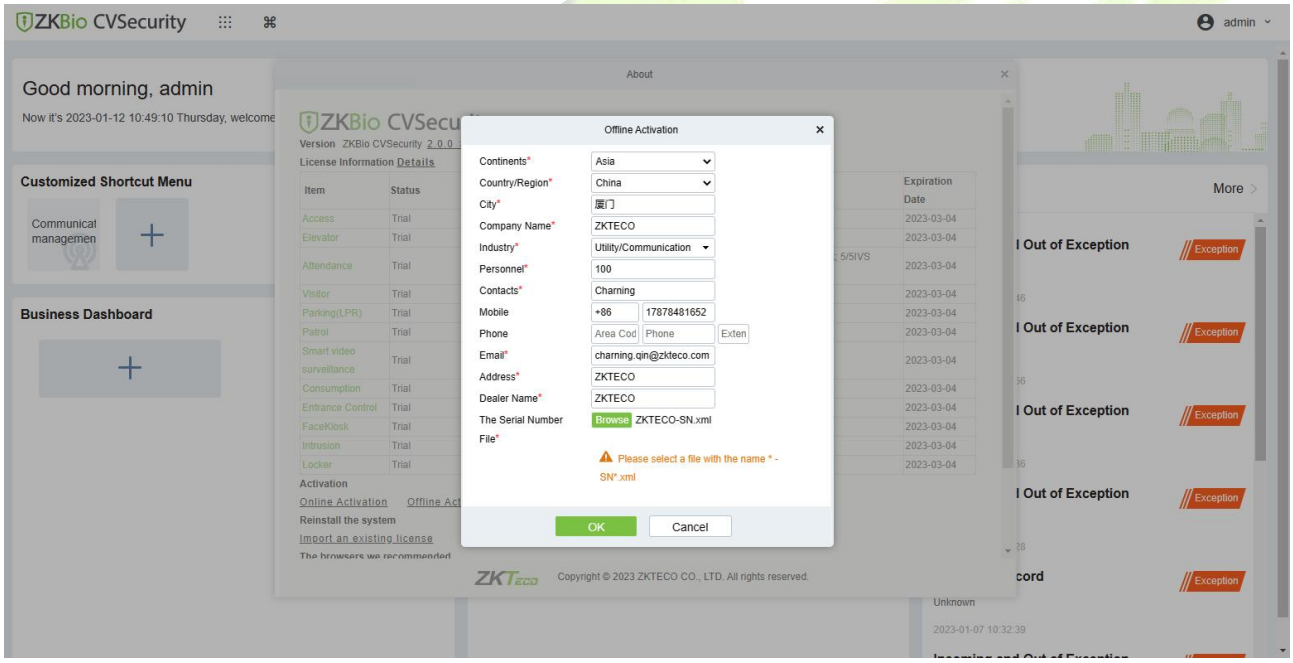


Figure 1- 25 Information Filling and File Uploading

7. Click Download, then a license file with a suffix of upk.xml will be downloaded.

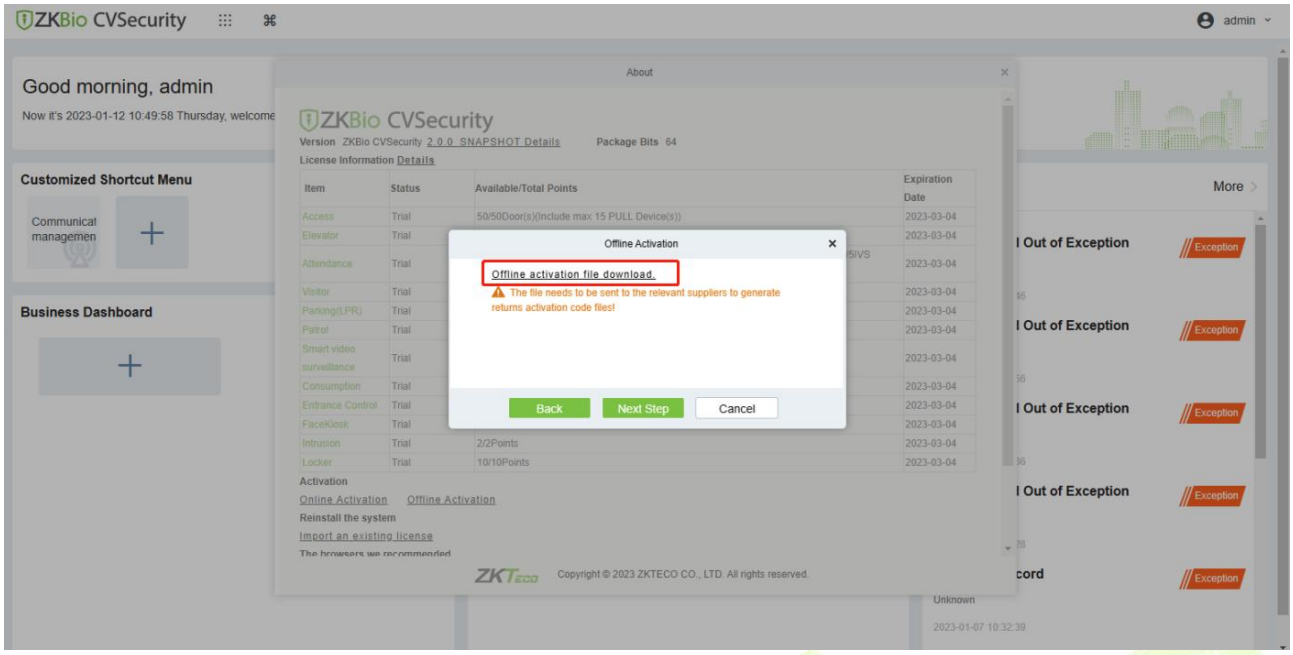


Figure 1- 26 Offline Activation File Download

8. Save the license file with a suffix of upk.xml that you just downloaded.

ZKTECO_lic_upk.xml

9. Go to the website to create the xxx-License.xml file:

Web Link: [ZKBio CVSecurity Offline Activation License (zkteco.com)]

22828-ZKBioCV-HQ-Sales-20230111-[redacted]-2Park-License.xml

10. Back to the the new server, click Admin > About > Offline Activation > Yes, and upload the file that you just got from previous step with the License.xml suffix

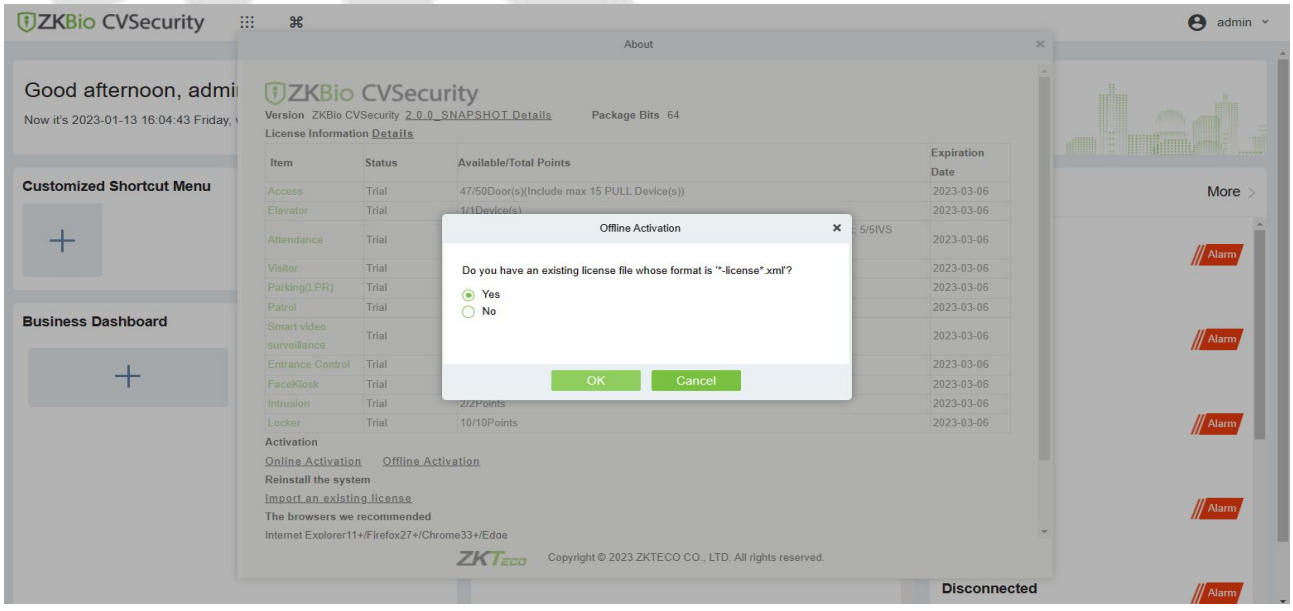


Figure 1- 27 Offline Activation File Upload

11. The activation is successful. The following is the successful activation interface:

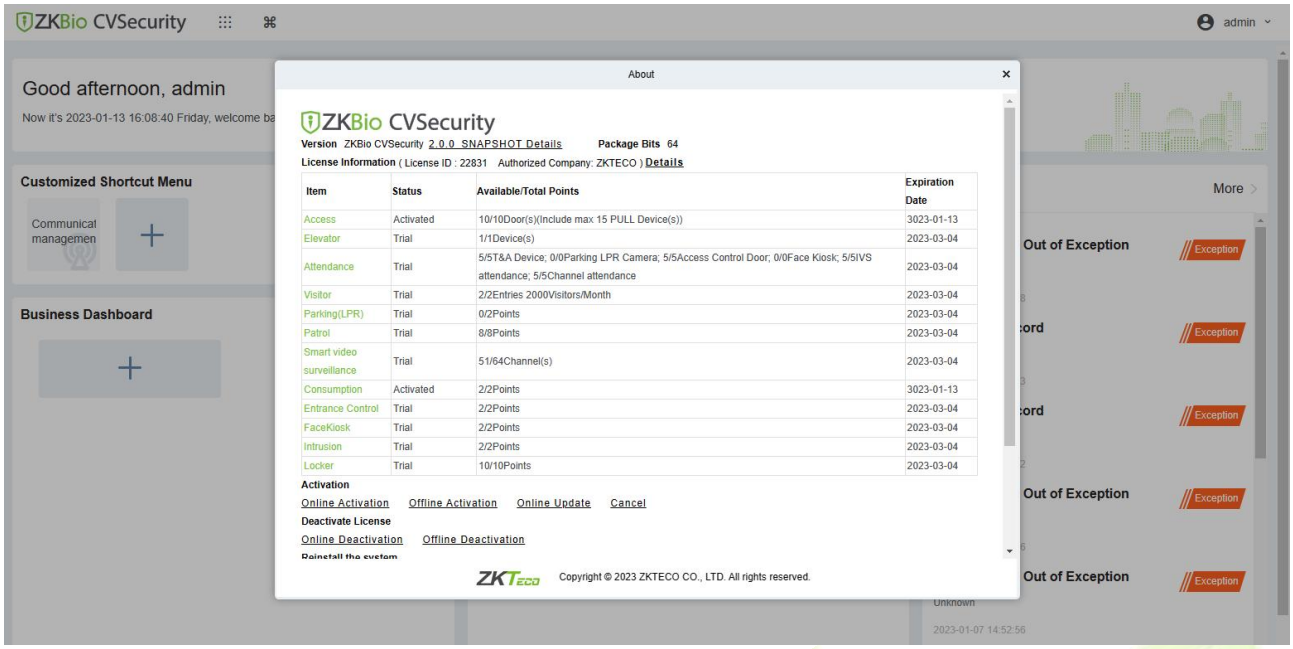


Figure 1- 28 License Activation Succeeded

1.3.4Offline Deactivation + Offline Activation

● Description:

Offline deactivate original server, and then offline activate the new server.

● Preconditions:

Both original server and new server are not connected to the network.

● Steps:

1. Click **Admin > About > Offline Deactivation**.

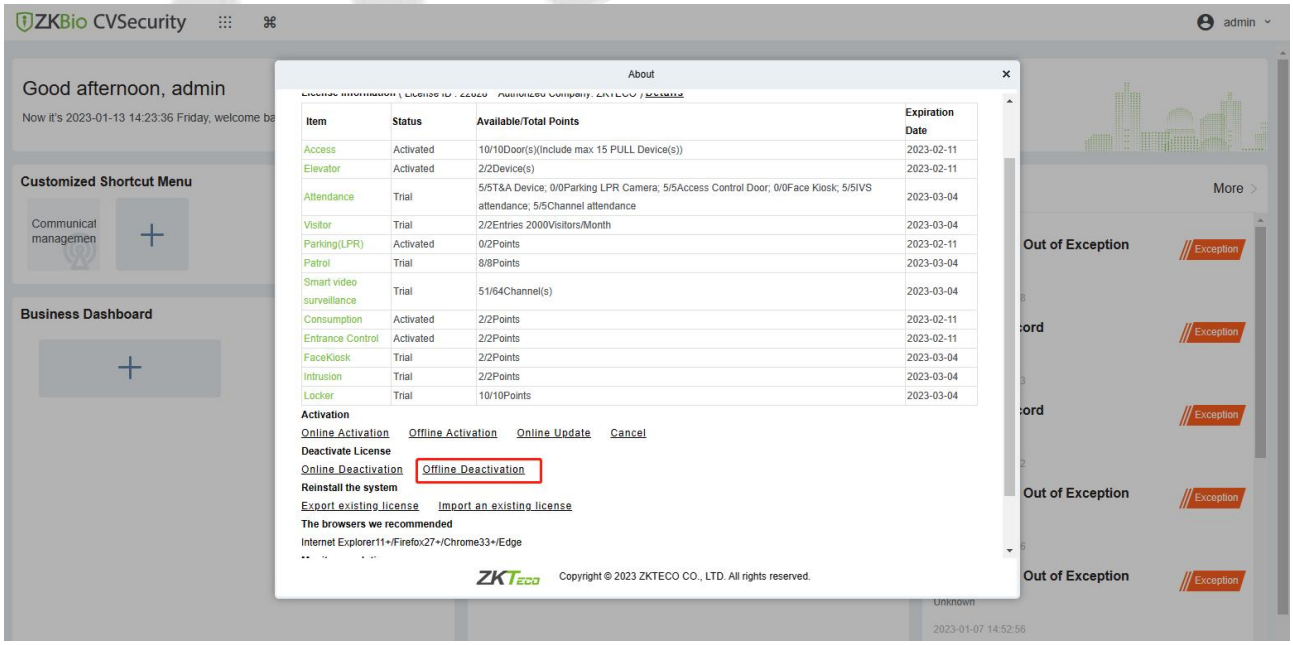


Figure 1- 29 Offline Deactivation

2. Click **OK**.

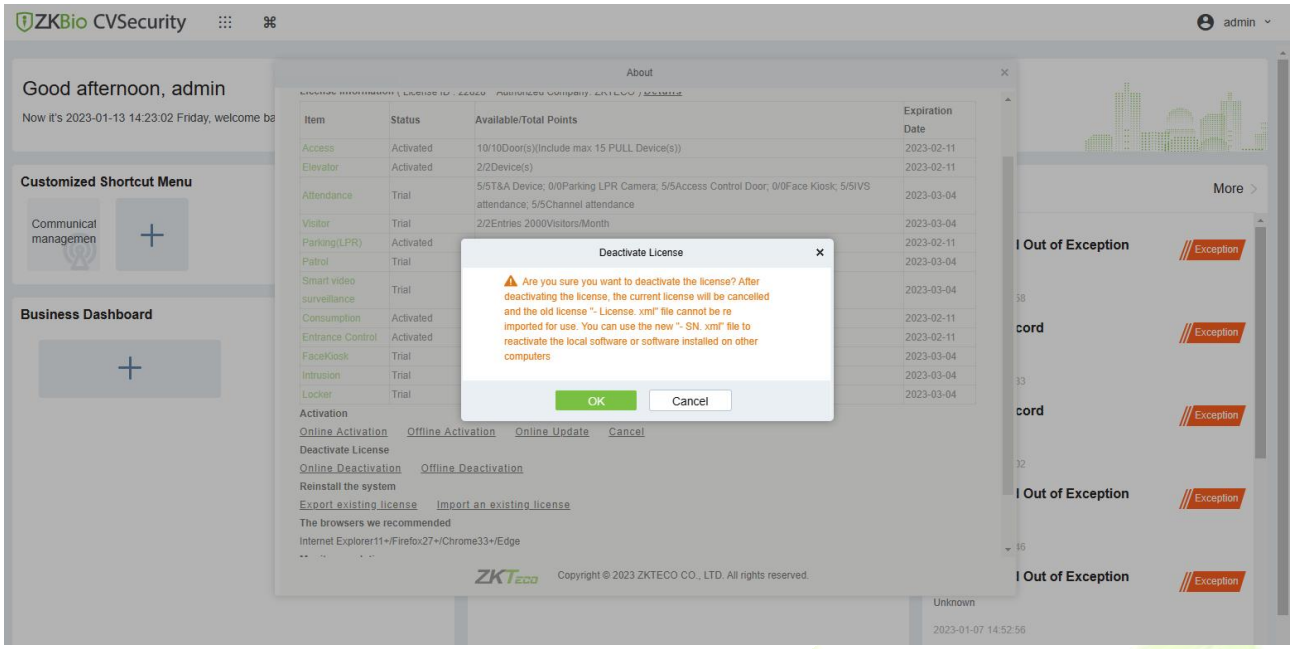


Figure 1- 30 Offline Deactivation Confirm

3. Click **Download**, and then a license file with a suffix of BackActi.xml will be downloaded.

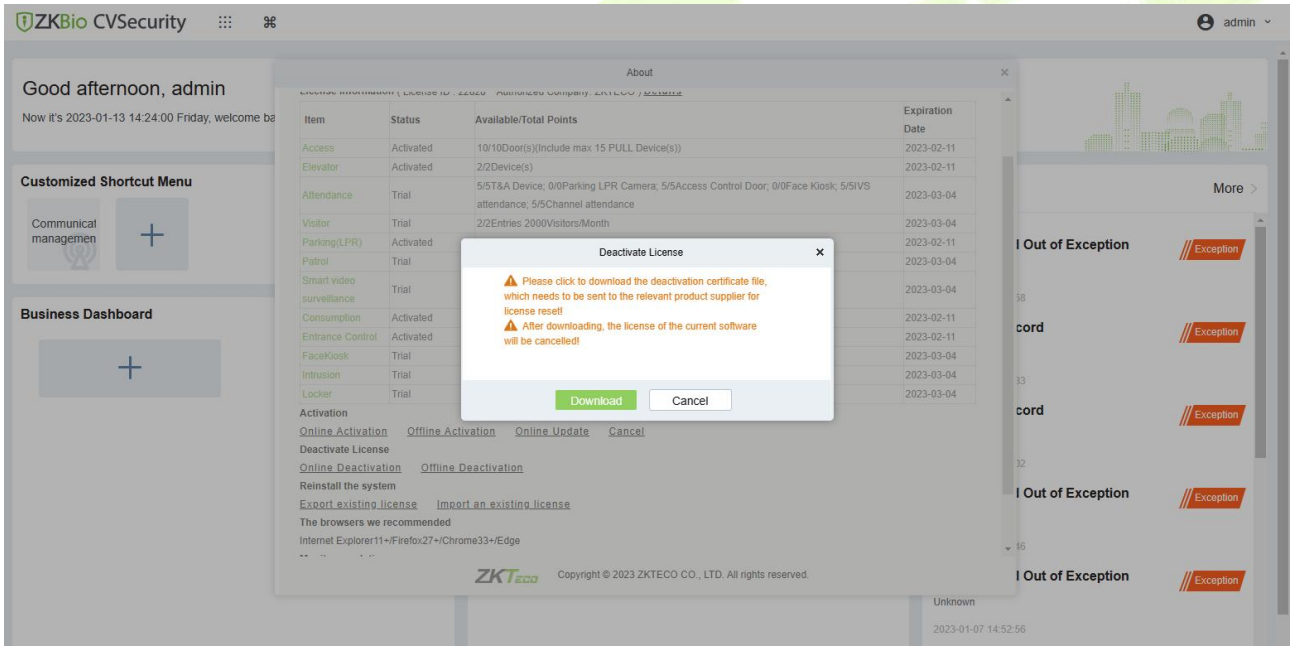
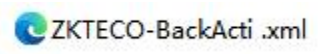


Figure 1- 31 Offline Deactivation File Download

4. Save the license file with a suffix of BackActi.xml you just downloaded.



5. Open the ZKBio CVSecurity License Deactivate page

Web Link: [ZKBio CVSecurity License Deactive (zkteco.com)]

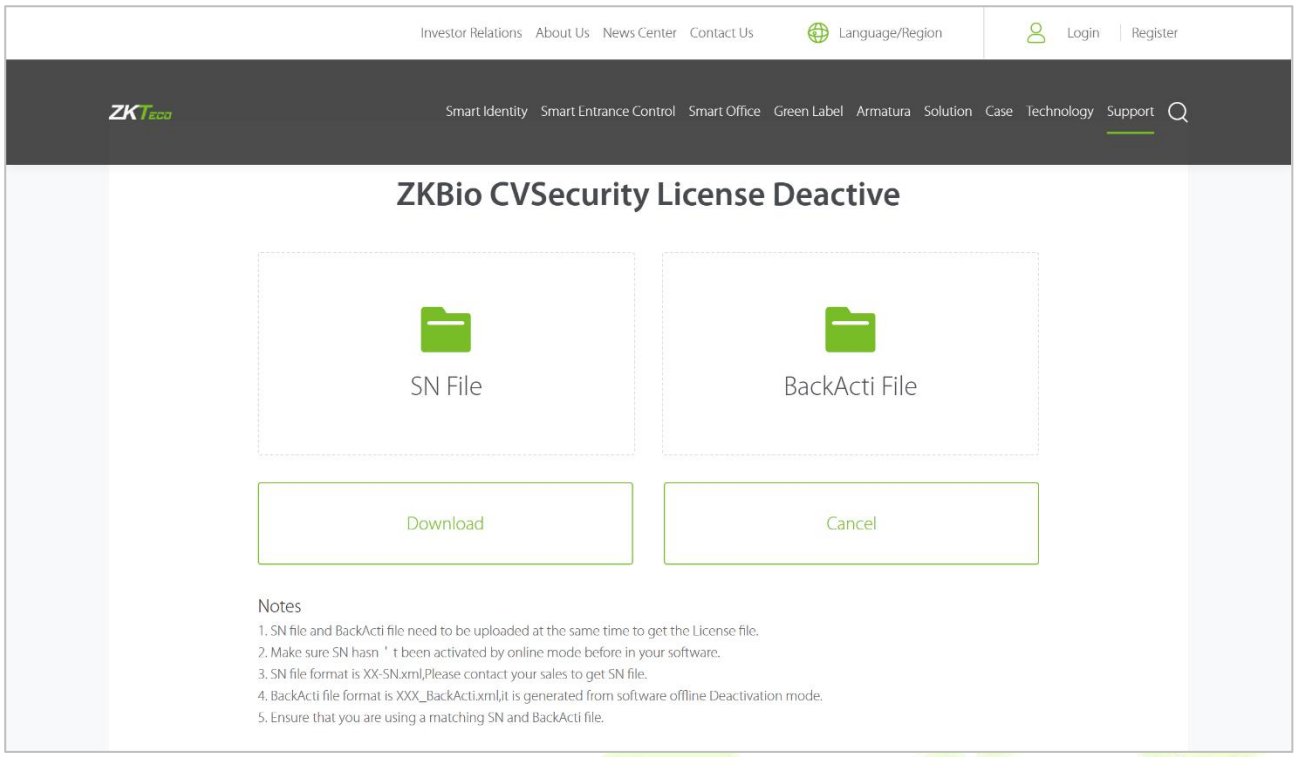


Figure 1- 32

6. Follow the instructions on the page to upload the SN file and BackActi File.

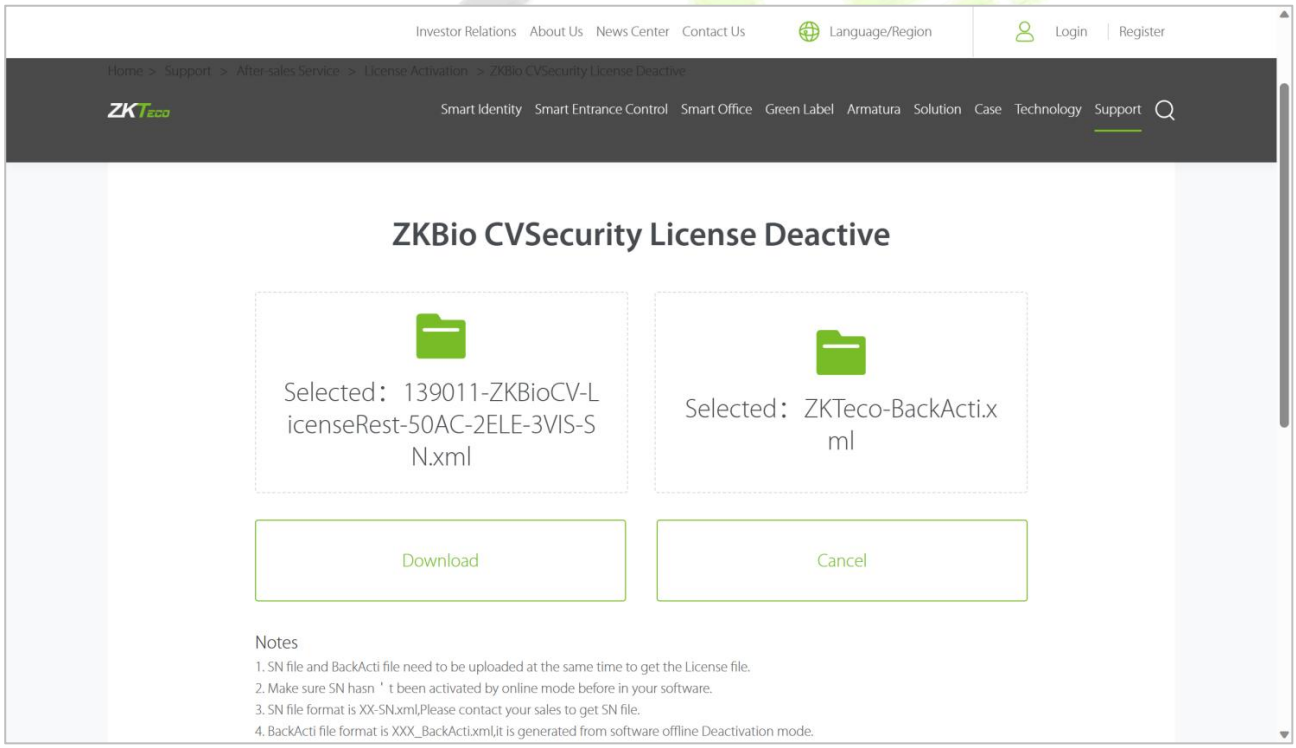


Figure 1- 33

7. Click the **Download** button to download the activation file.

8. Log in to a new server.

9. Click **Admin > About > Offline Activation**. Fill in the relevant information, then click Browse to upload the file that you just got from previous step with the SN.xml suffix.

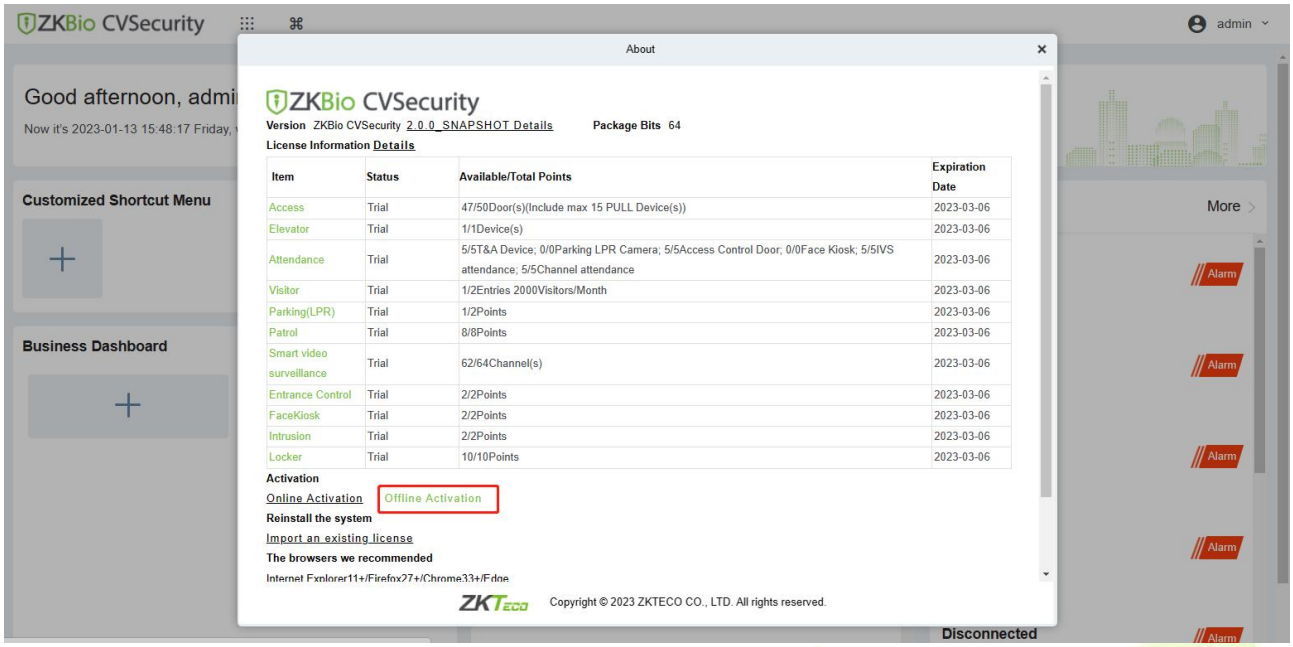


Figure 1- 34 Offline Activation

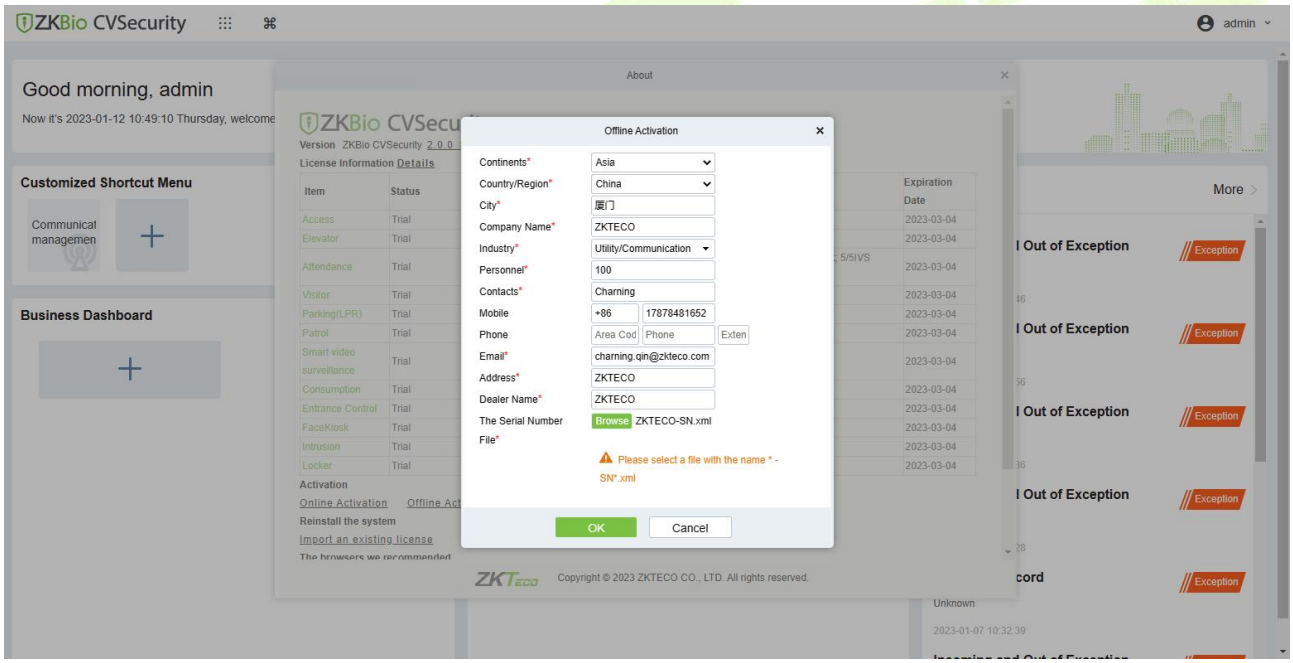


Figure 1- 35 Offline Activation Information Filling

10. Click **Download**, and then a license file with a suffix of upk.xml will be downloaded.

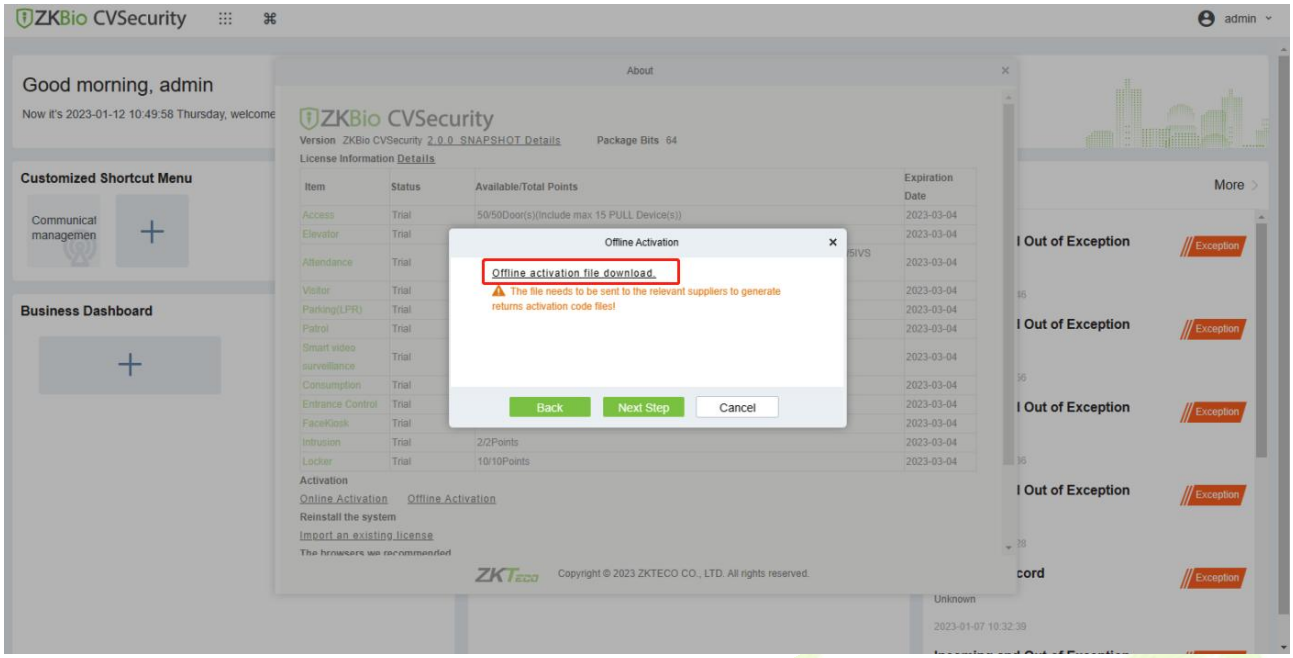
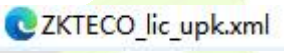


Figure 1- 36 Offline Activation File Download

11. Save the license file with a suffix of upk.xml that you just downloaded.



12. Open the ZKBio CVSecurity Offline Activation License page.

Web Link: [ZKBio CVSecurity Offline Activation License (zkteco.com)]

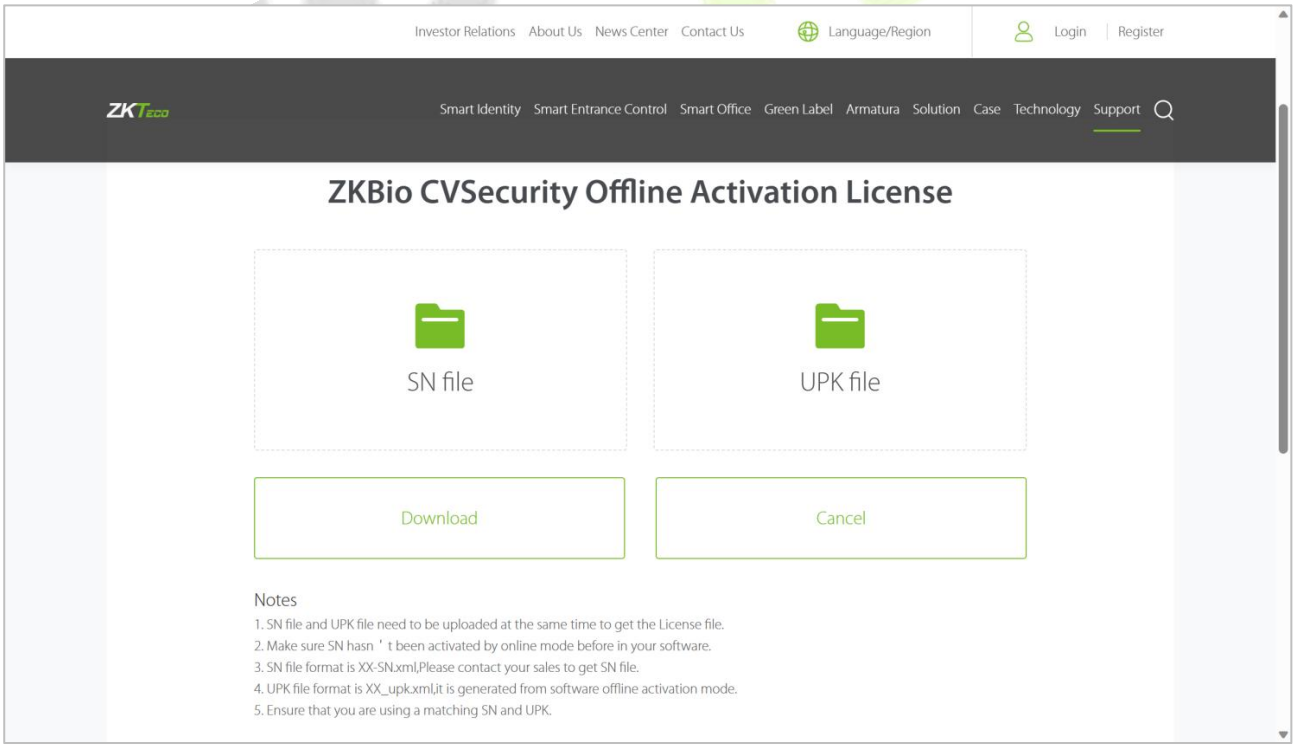


Figure 1- 37

13. Follow the instructions on the page to upload the files downloaded in step 7 and step 11 in turn.

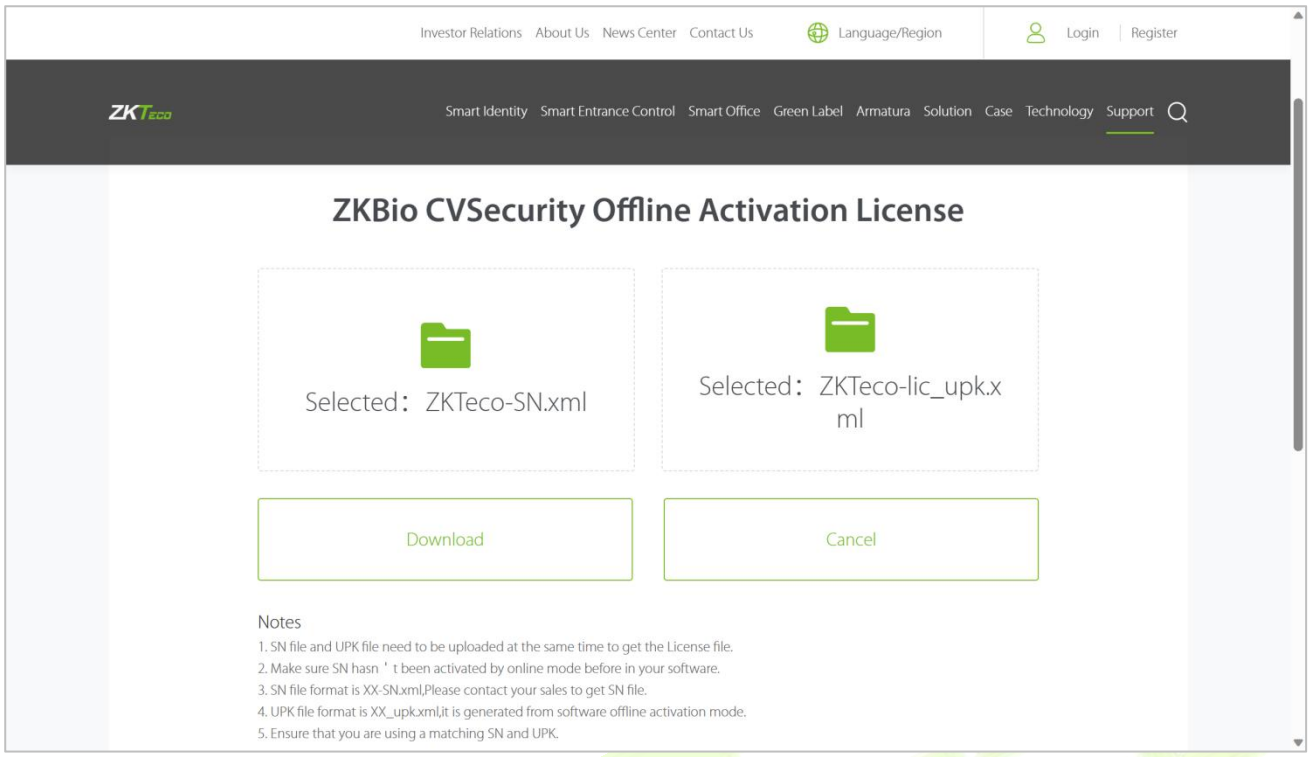
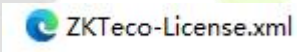


Figure 1- 38

14. Click the **Download** button to download the offline activation file.



15. Back to the the new server, click **Admin > About > Offline Activation > Yes**, and upload the file that you just got from the previous step with the License.xml suffix.

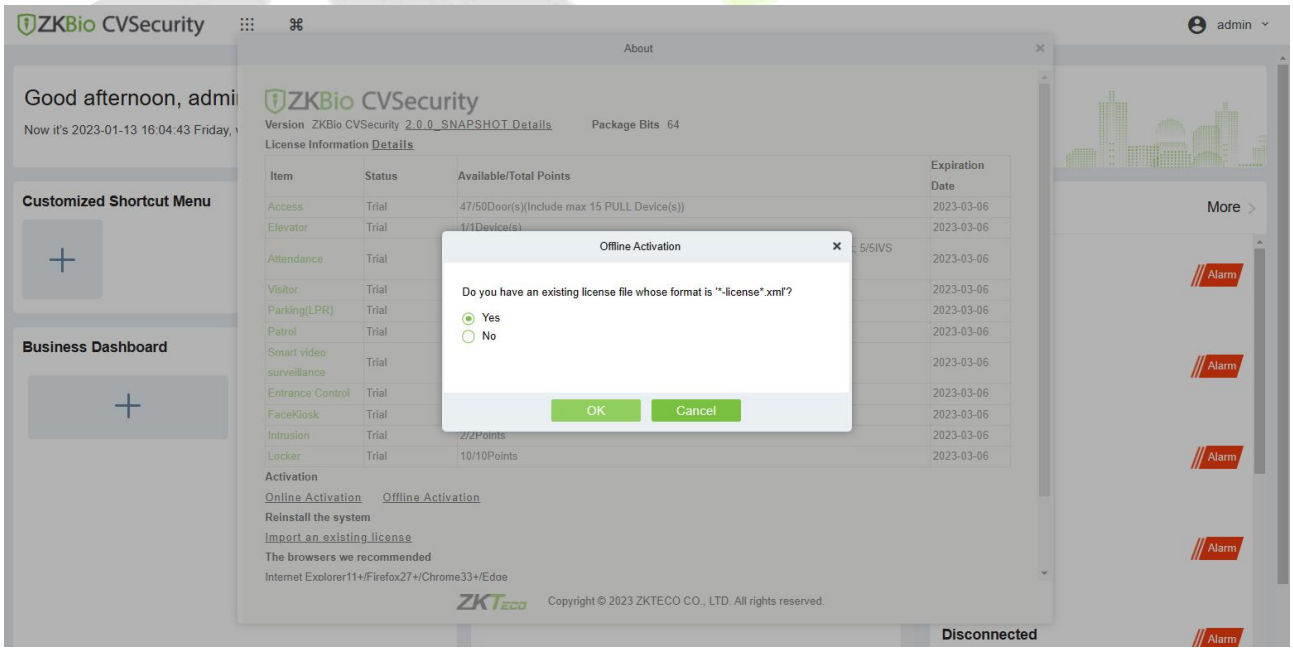


Figure 1- 39 Offline Activation File Download Confirm

16. The activation is successful. The following is the successful activation interface:

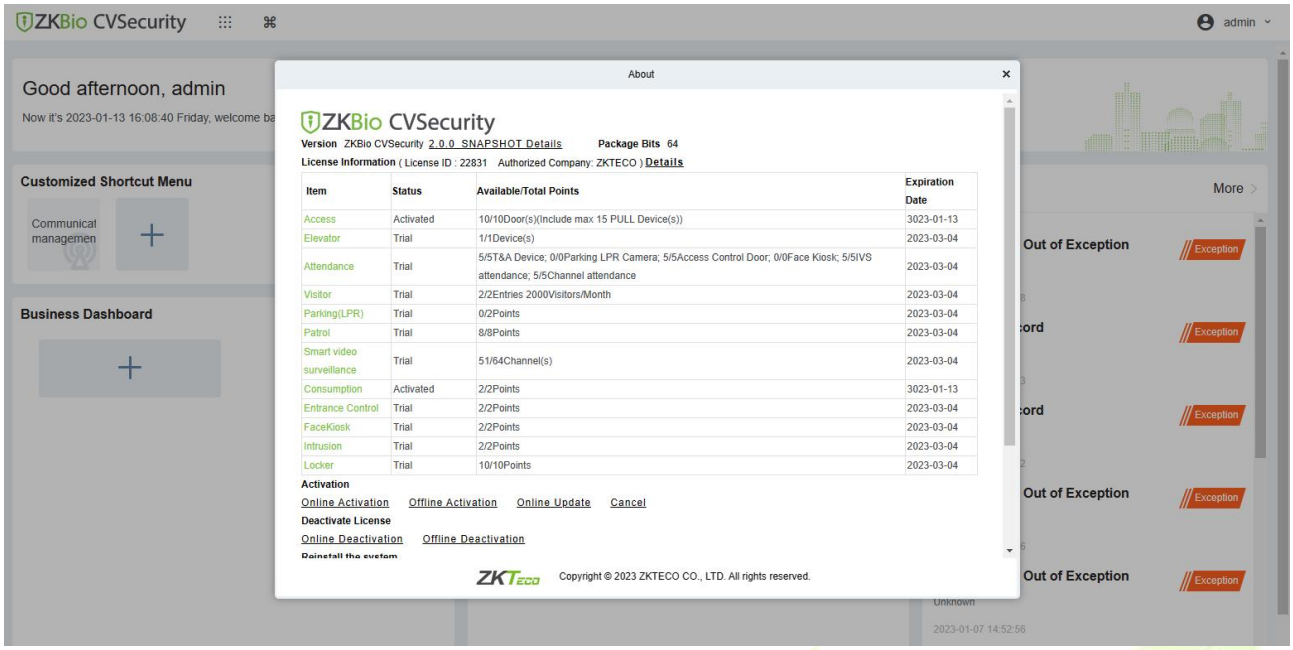


Figure 1- 40 License Activation Succeeded

1.4 Software Homepage Display

The main interface displays the Customized Shortcut Menu, Business Dashboard, Message Notification, Alarm Center and AI Assistant.

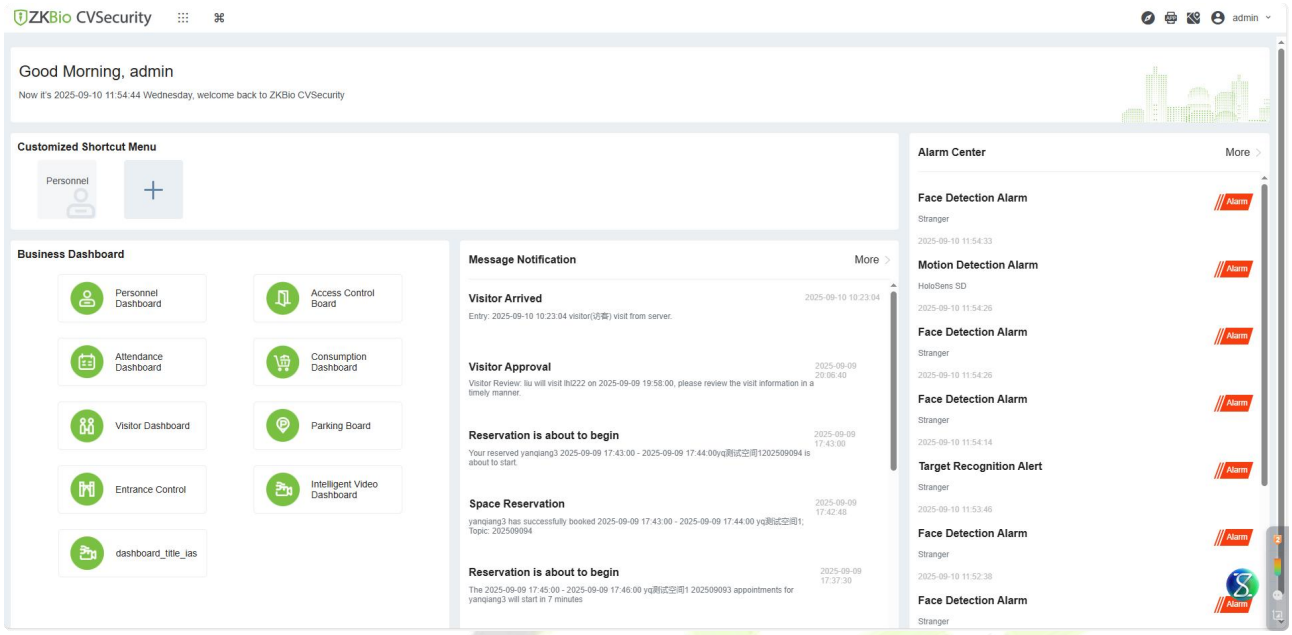


Figure 1- 41 License Activation Succeeded

1.4.1 Customized Shortcut Menu

The customized shortcut menu can be accessed from two locations (as shown in Figure 1-42) to provide quick access to frequently used functions. Users can customize menu items according to their preferences.

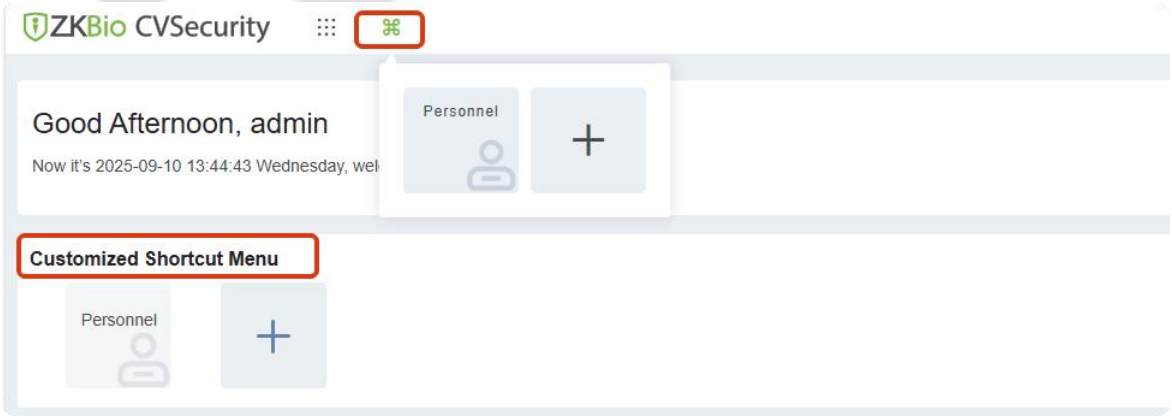


Figure 1- 42 Customized Shortcut Menu

1.4.2 Business Dashboard

Users can add or delete business dashboards according to their actual needs. Clicking on the icons here allows for quick and convenient access to view the business dashboards.

There are a total of 9 business panels, including:Personnel Dashboard,Access Control Board,Attendance Dashboard,Consumption Dashboard,Visitor Dashboard,Parking Board,Entrance Control,Intelligent

Video Dashboard and Intrusion Alarm Dashboard.

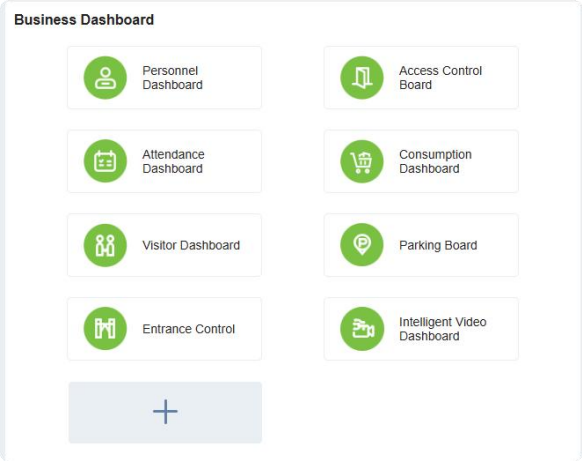


Figure 1- 43 Business Dashboard

1.4.3Message Notification

Here, you can view message notifications for all modules including visitor management, attendance, and space management. Click "**More**" to quickly access the Notification Center.

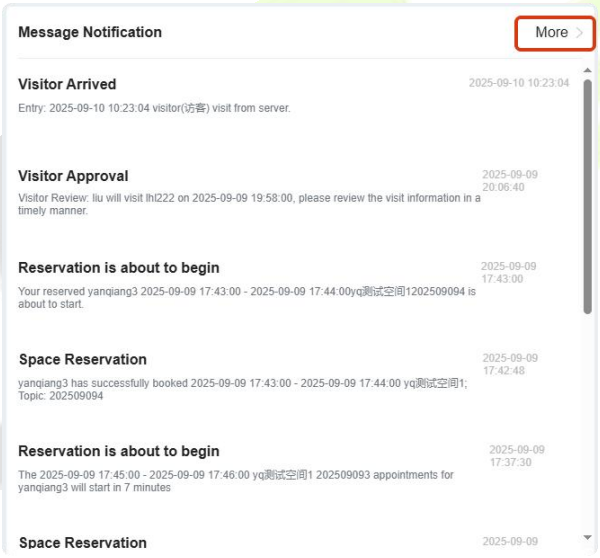


Figure 1- 44 Message Notification

1.4.4Alarm Center

Here, you can view various types of alarm information. Click "**More**" to quickly access the event center.

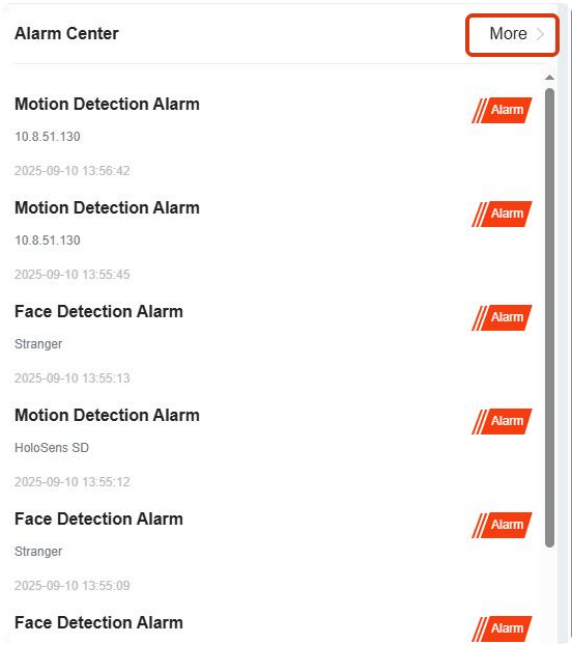
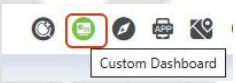


Figure 1- 45 Alarm Center

1.4.5Custom Panel

The Custom Panel allows users to create required data dashboards based on their own needs. It enables different users to view different data panels, with data of each module componentized and customizable via drag-and-drop by users.

Step1: Click the small icon 

of Custom Panel in the upper right corner to access the viewing and configuration interface.

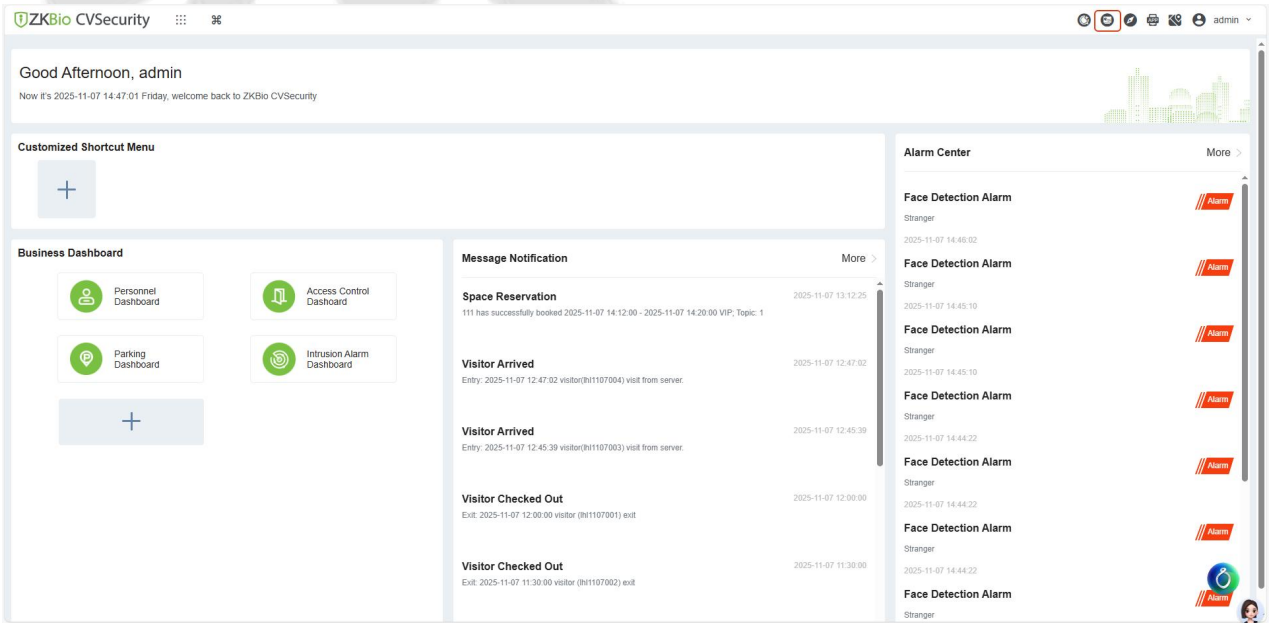


Figure 1- 46 Custom Panel

Step2: On this page, you can view the configured Custom Panels. Click the Add button  to access the configuration interface.

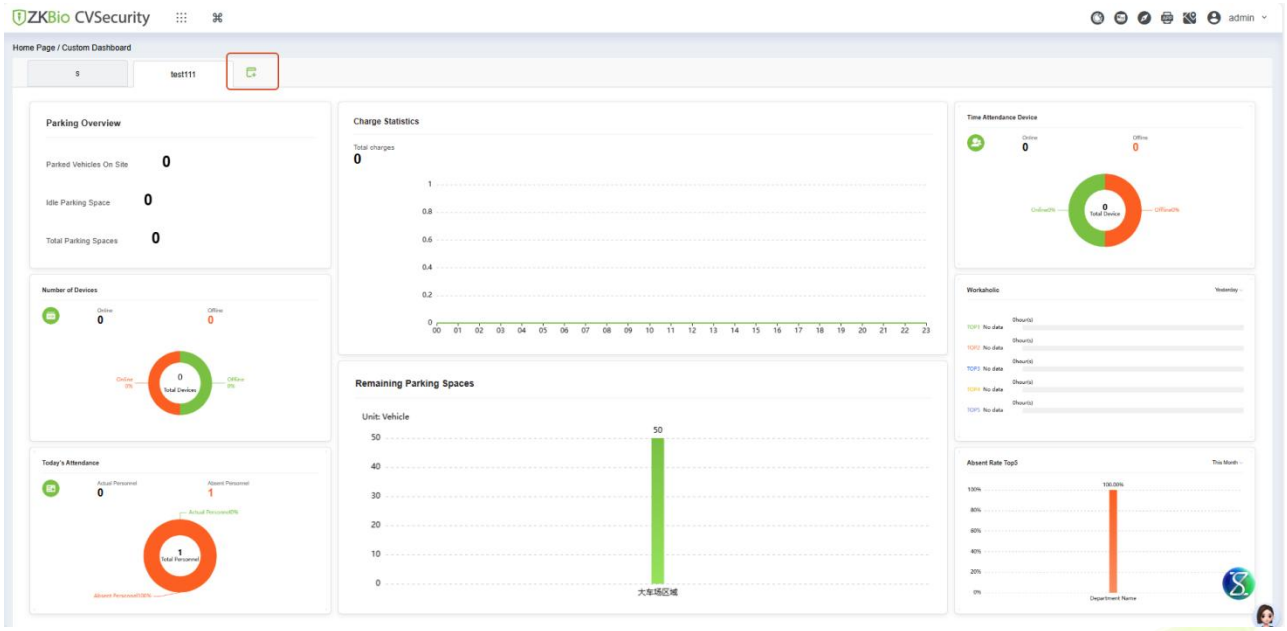


Figure 1- 47 AI Assistant

Step3: On the left side of the configuration interface, you can set the panel name and check whether it is visible to all users. If you select "No", you can further select which users are allowed to view it. Then choose a suitable panel layout to start the configuration.

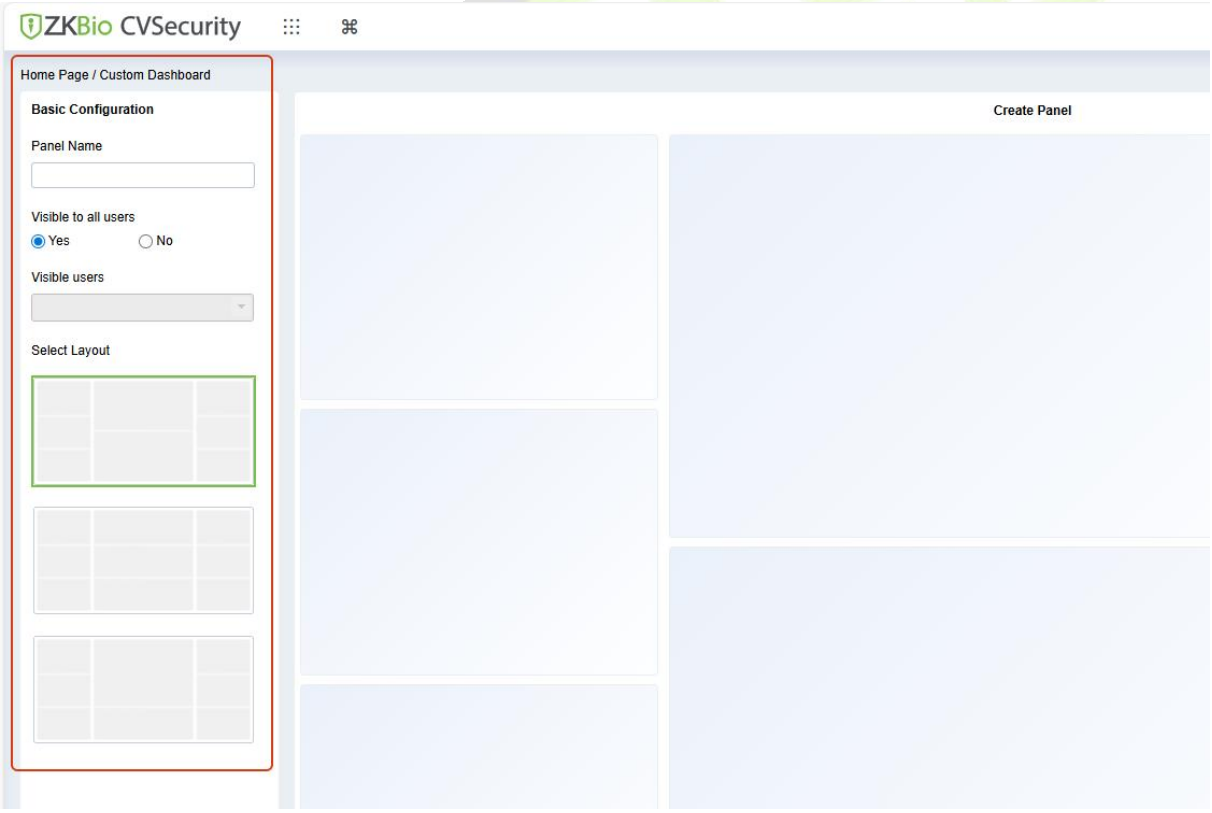


Figure 1- 48 AI Assistant

Step4: On the right side of the configuration interface, components for multiple modules are provided. Users can freely combine them to form a visualized data panel that suits their needs.

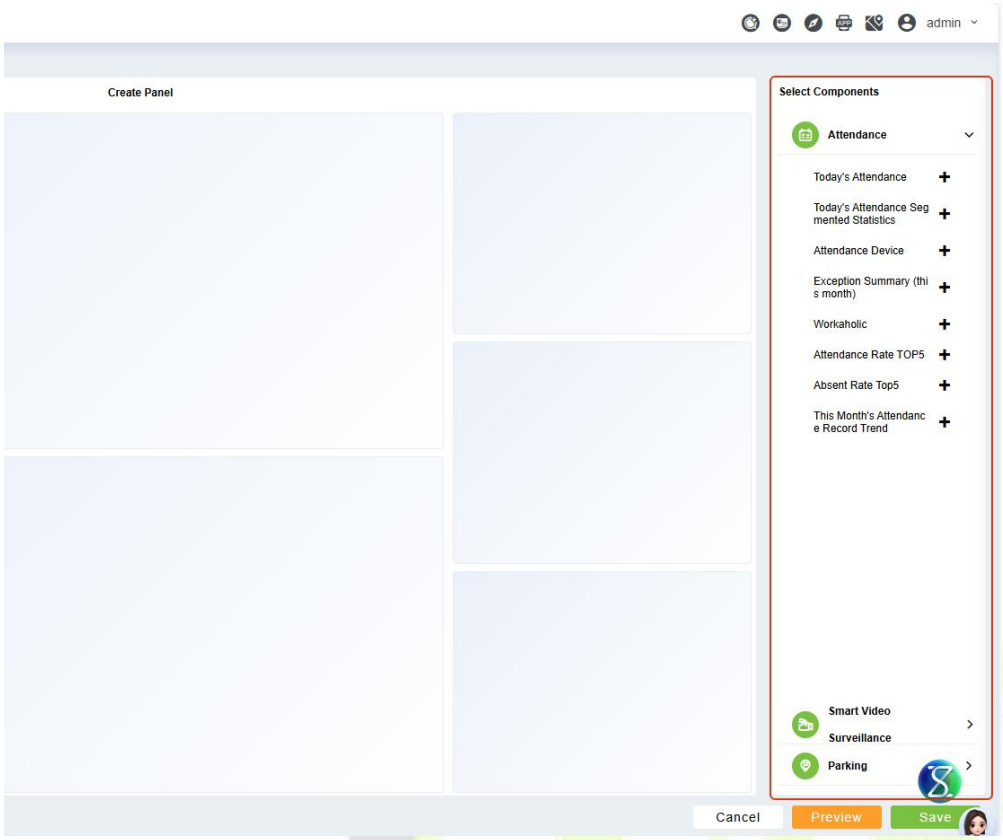


Figure 1- 49 AI Assistant

Users can add components by dragging: click a component on the right and drag it to the desired position in the middle panel to complete the addition.

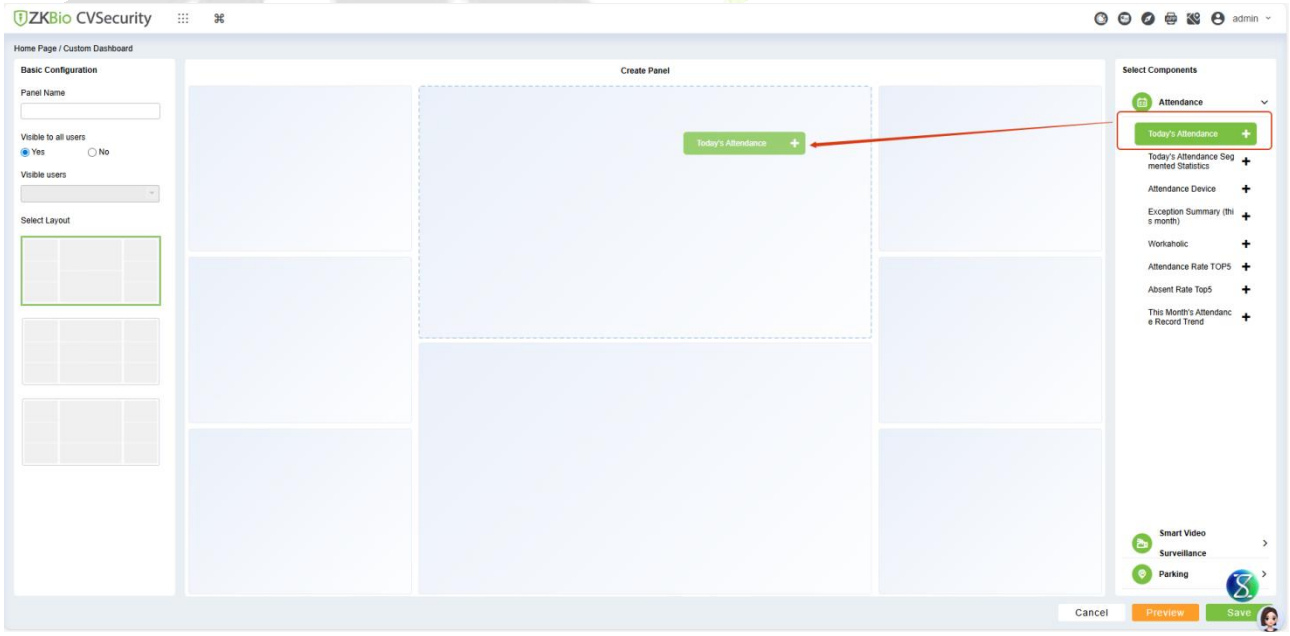


Figure 1- 50 AI Assistant

After completing the addition via dragging, if you want to delete a component and reselect it, you can click the delete button in the upper right corner of the respective component in the middle panel.

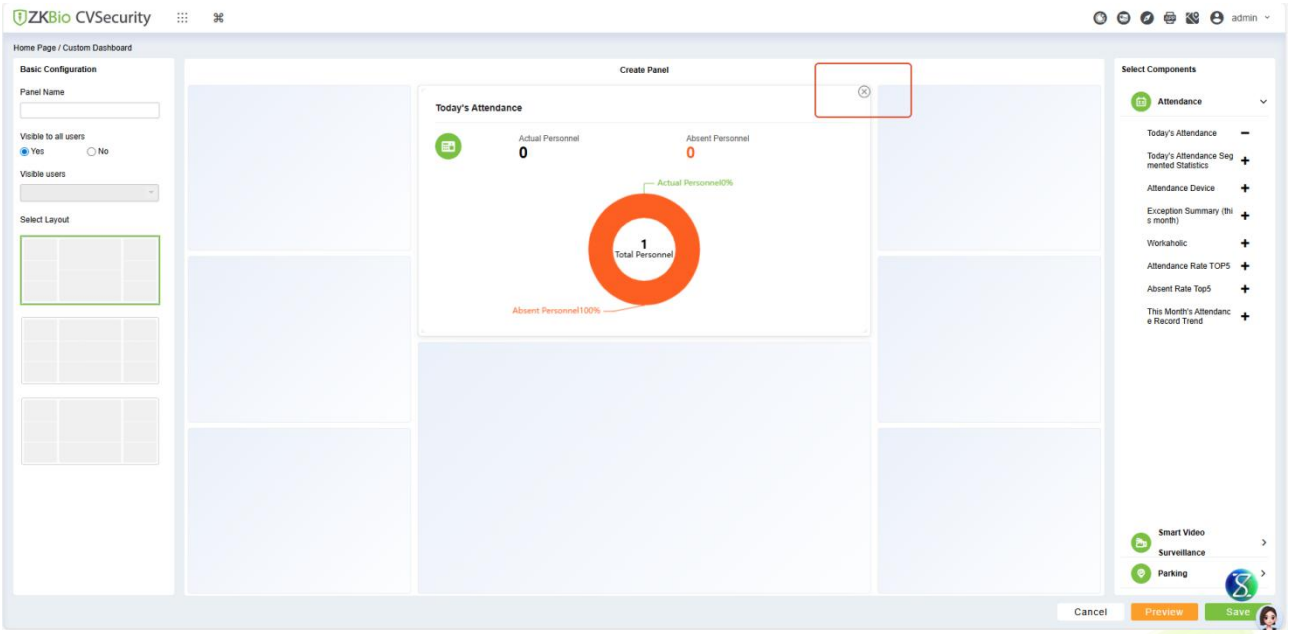


Figure 1- 51 AI Assistant

Step5: After completing the configuration:

Click "Preview" in the lower right corner to preview the panel.

Click "Cancel" to exit the configuration interface.

Click "Save" to save the current Custom Panel.

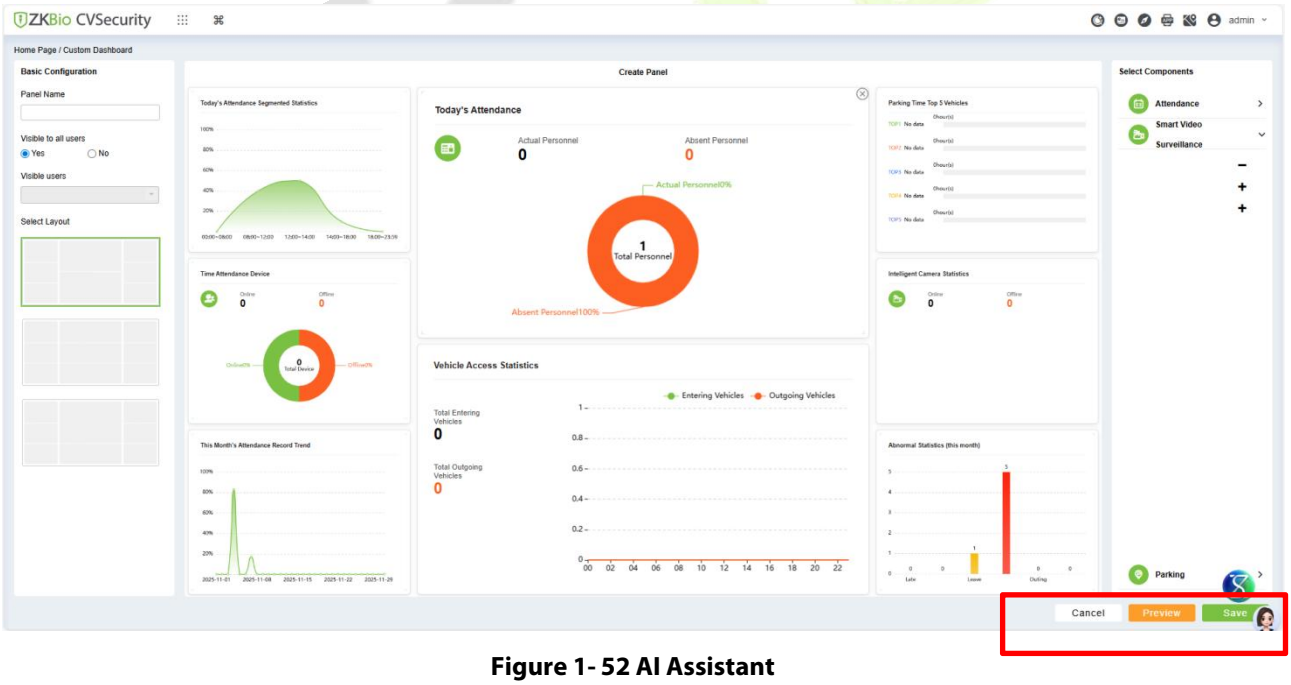


Figure 1- 52 AI Assistant

Step5: For the saved panels:

Users with permission click the Edit button  next to the panel name to reconfigure it.

Users with permission can click the Delete button  to remove the panel; once deleted, it will no longer be visible to all users.

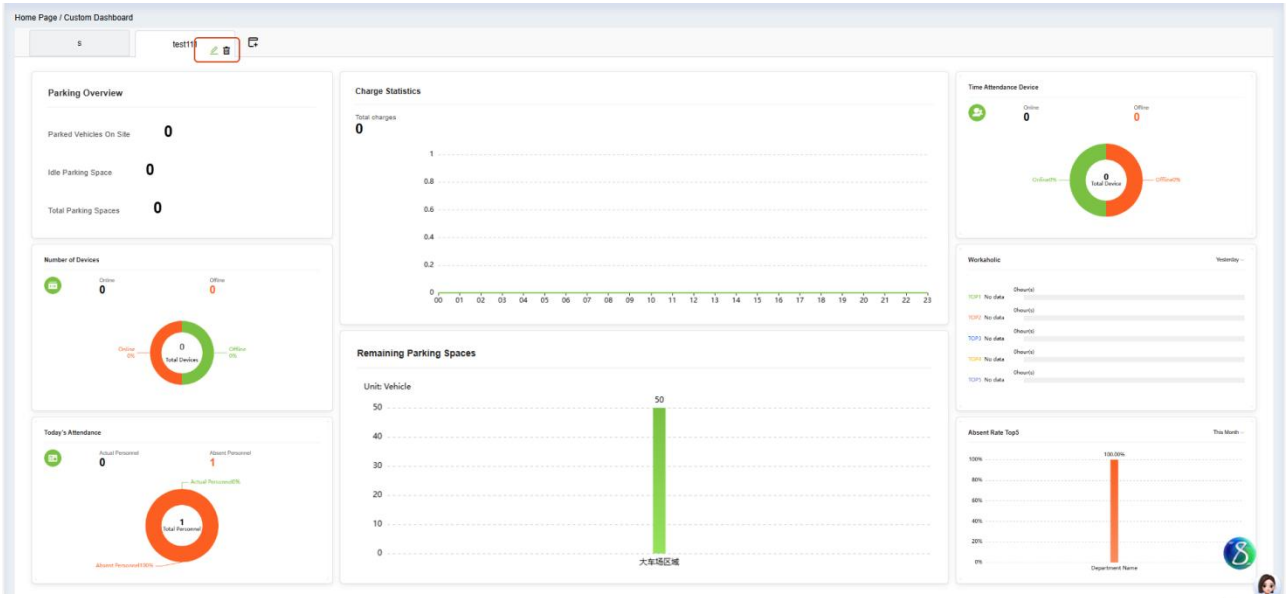


Figure 1- 53 AI Assistant

2 Personnel

Before using the other functions, please configure the personnel system: Personnel and Card Management.

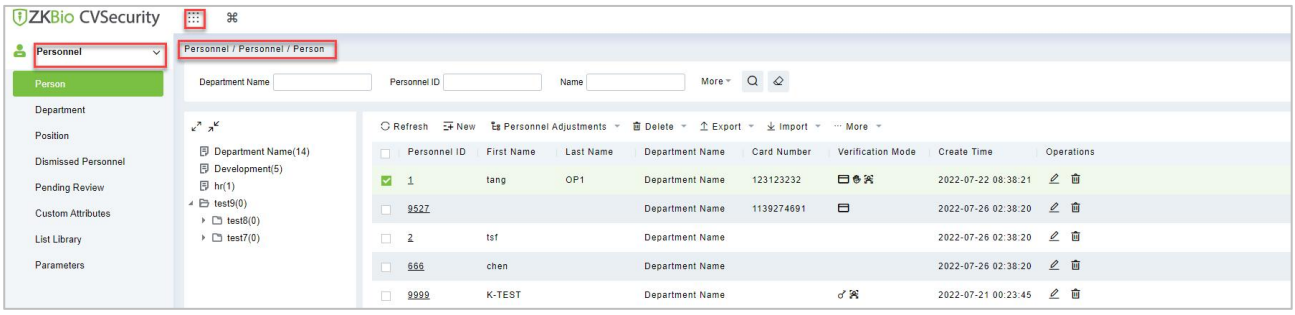


Figure 2- 1 Personnel

2.1 Personnel

Personnel Management includes these modules: Person, Department, Position, Dismissed Personnel, Pending review, Custom Attributes, List Library, and Parameters.

● Operating Procedures:

This operation process is suitable for guiding users how to configure and manage the basic personnel organization after the system is installed.

The flow of personnel organization configuration is shown in figure below.

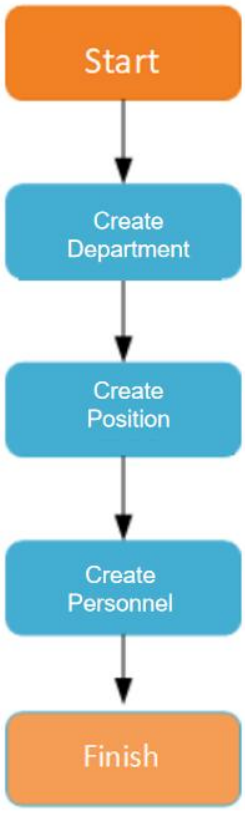


Figure 2- 2 Flowchart of Personnel Configuration

2.1.1Person

When using this management program, the user shall register personnel in the system, or import personnel information from other software or documents into this system.

Main functions of Person include Refresh, Add (New), Personnel Adjustments, Delete, Export, Import, and more.

2.1.1.1Add Personnel (New)

Click **Personnel > Personnel > New**.

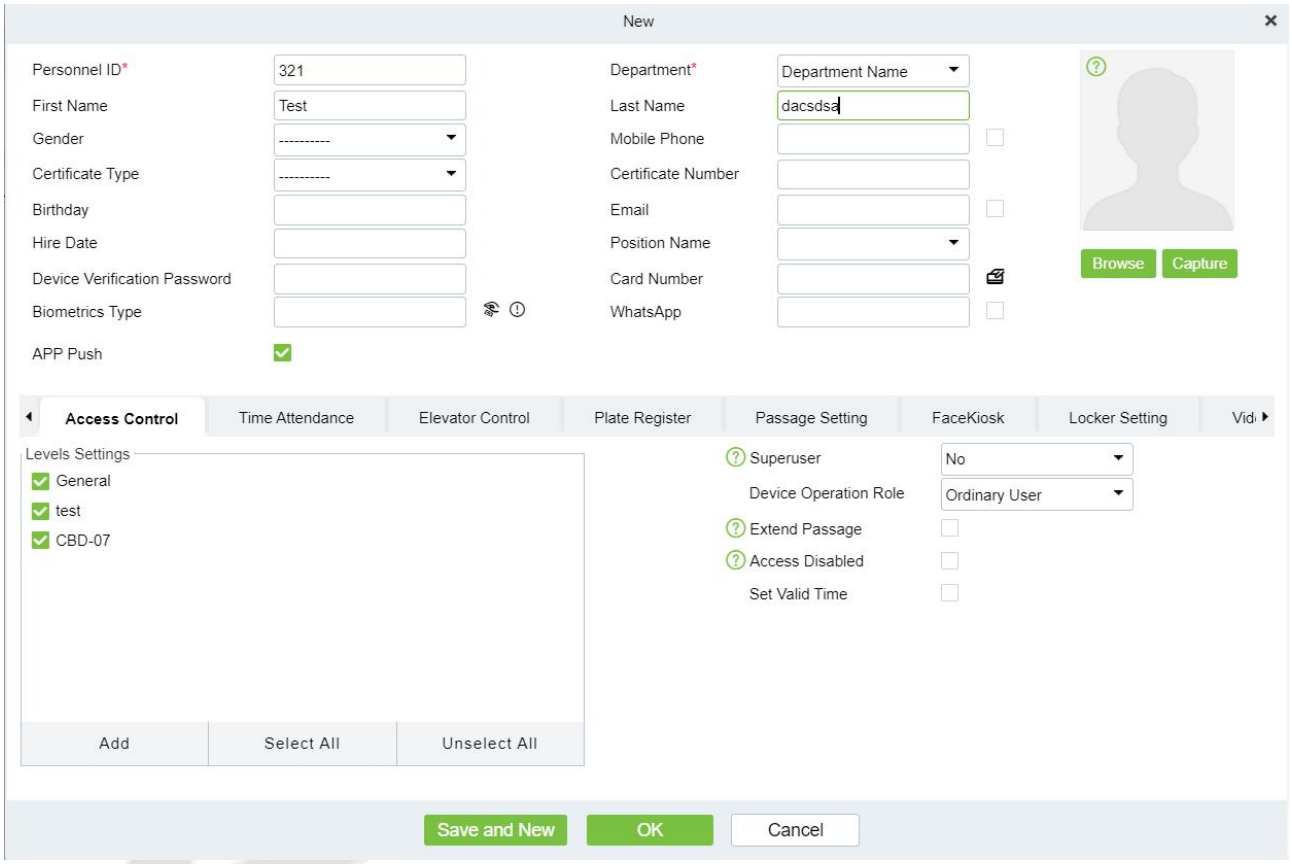


Figure 2- 3 Add Personnel New

● Fields are as follows:

✍**Notes:**(Personnel ID)

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

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

Parameter	Description
Personnel ID	Default maximum support for 9 digits; if you need to support more digits or letters for IDs, please go to the **Parameter** menu to configure.
Department	Select from the pull-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.

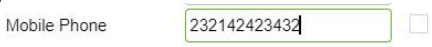
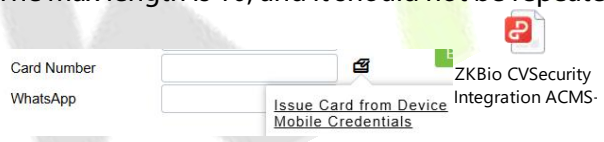
Parameter	Description
Mobile Phone	If you need to send a short message to this person, check the mobile phone box and select the option to send the message. **Modem – SMS**: A modem SMS is a dedicated device that connects to your PC or server, allowing you to send and receive SMS messages. **AWS – SMS**: AWS SMS is a managed service that delivers messages from publishers to subscribers. 
Certificate Type	There are four types of certificates: ID, Passport, Driver License and Others. Select one to upload.
Certificate Number	Enter certificate number.
Birthday	Input employee's actual birthday.
Email	To send an email notification to this person, simply check the box and enter the available email ID of the individual. 
Hire Date	It is the date on which the personnel are appointed. Click to select the date.
Position Name	Set a suitable name for the position. Any character, maximum combination of 100 characters. Position names should not be repeated.
Device Verification Password	Set password for personnel accounts. It can only contain up to 6-digits. If a password exceeds the specified length, the system will truncate it automatically. It cannot be the same with others password and the duress password.
Card Number	The max length is 10, and it should not be repeated.  For more details on Mobile Credentials please refer to the documentation.
Biometric Type	Click on icon to register the person Fingerprints, Finger Vein, Palm, Face registration . Click on icon to view Biometric template details and resgistered person face comparison photos and Plam comparison photos.
WhatsApp	Please enter your WhatsApp account number, and check the box to send WhatsApp messages to this person. 
APP Push	After verification, an app message notification will be sent to this person. 

Table 2- 1 Personnel ID

● Biometric Type:

This part introduces the Steps of personnel biometric registration in ZKBio CVSecurity. The registered biometric data can be used for verification and identification of **Access Control**, attendance, and other equipment.

Biometric registration includes **fingerprint**, **finger vein**, **palm registration** and **face registration**. Since the interfaces of fingerprint registration and finger vein registration are similar, fingerprint registration and palm print registration are used as examples to illustrate the operation process.

● Description:

The server side of the box does not support external "palm meter, finger vein meter" to collect

biometric templates, and the fingerprint reader is only supported by the "Live20R" model.

● Preconditions:

On the computer terminal where the administrator registers the personnel information, connect the fingerprint reader device through the USB port.

● Steps:

Step 1: In the Personnel module, choose **Personnel Management > Person**.

Step 2: Click **Add** with the mouse, and the interface for adding personnel will pop up.

Step 3: On the interface for adding personnel, click the " " button.

Step 4: (Optional) If the driver is not installed, click the icon to pop up the registration and driver download box, download the driver, and complete the installation.

Step 5: After the driver is installed, fingerprint registration can be performed, as shown in figure below.

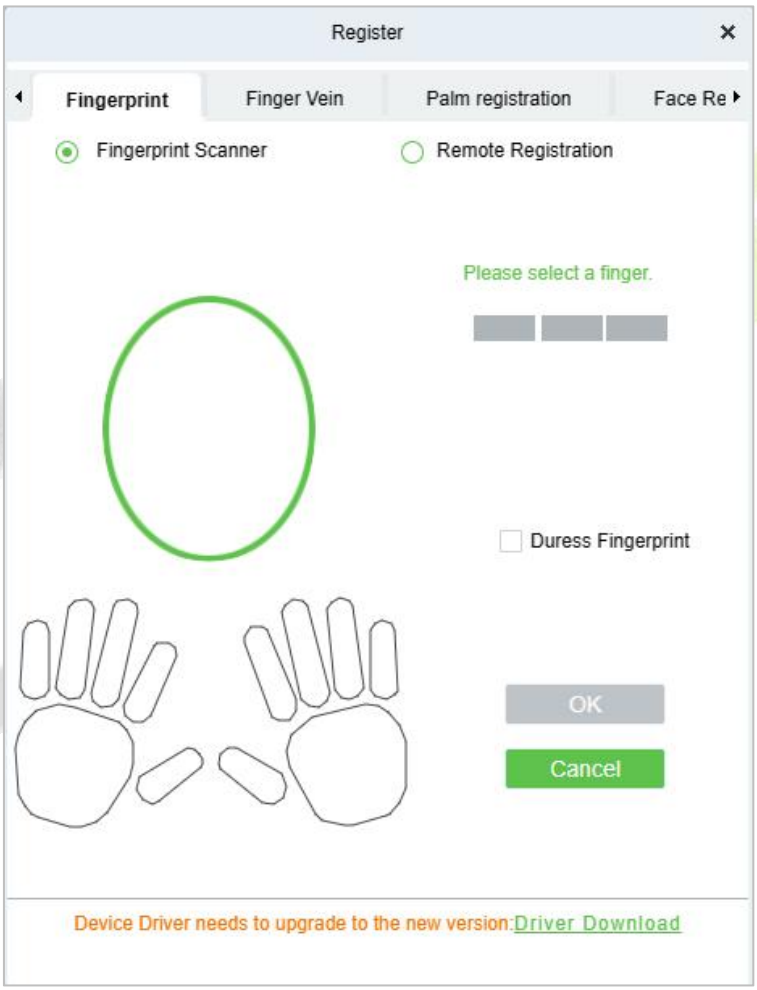


Figure 2- 4 Biometric Type

Step 6: Select the fingers respectively, press the fingerprint on the connected fingerprint reader three times in a row, and the system prompts the fingerprint to be registered successfully.

Step 7: Click **OK** to save and close the fingerprint registration interface.

Details Information:

Click this button to view the details of Biometric Templates or upload a facial photo.

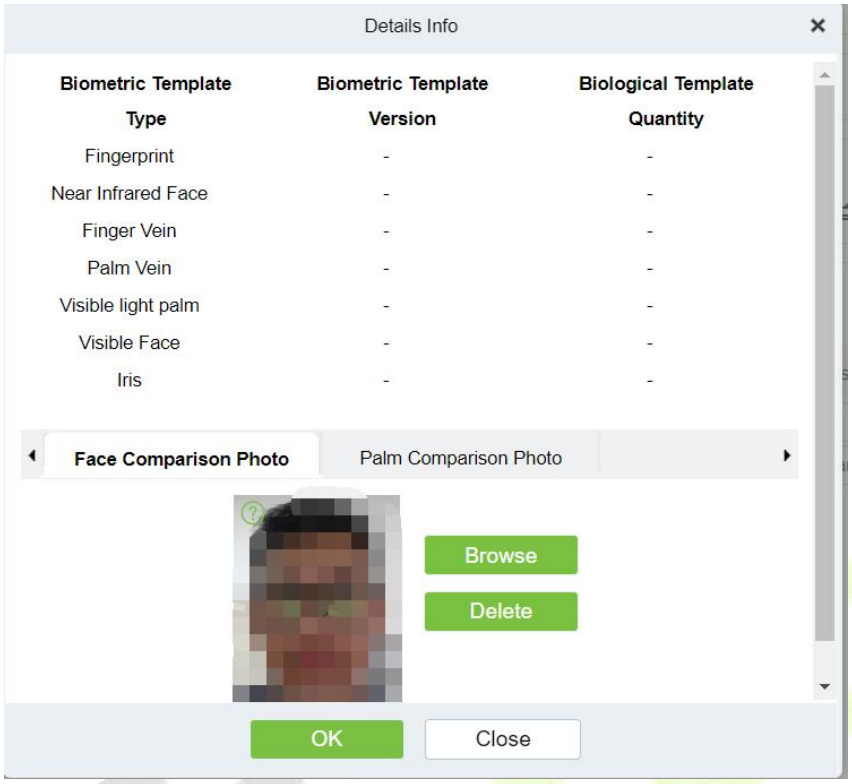


Figure 2- 5 Biometric Details

Face Comparison Photo

Click on **Browse** to upload a facial photo; you can click to view the specifications for the photo.

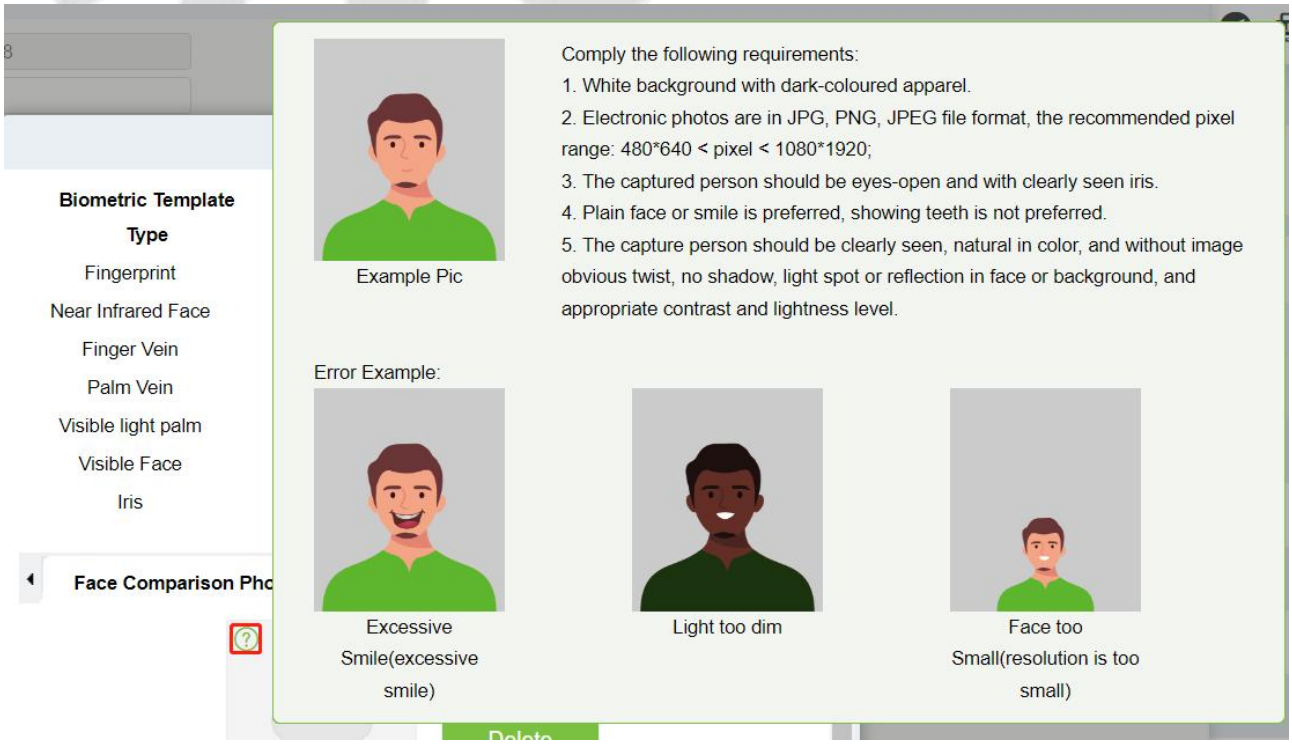


Figure 2- 6 Face Photo

● Access Control:

Click **Access Control** parameter for the personnel.

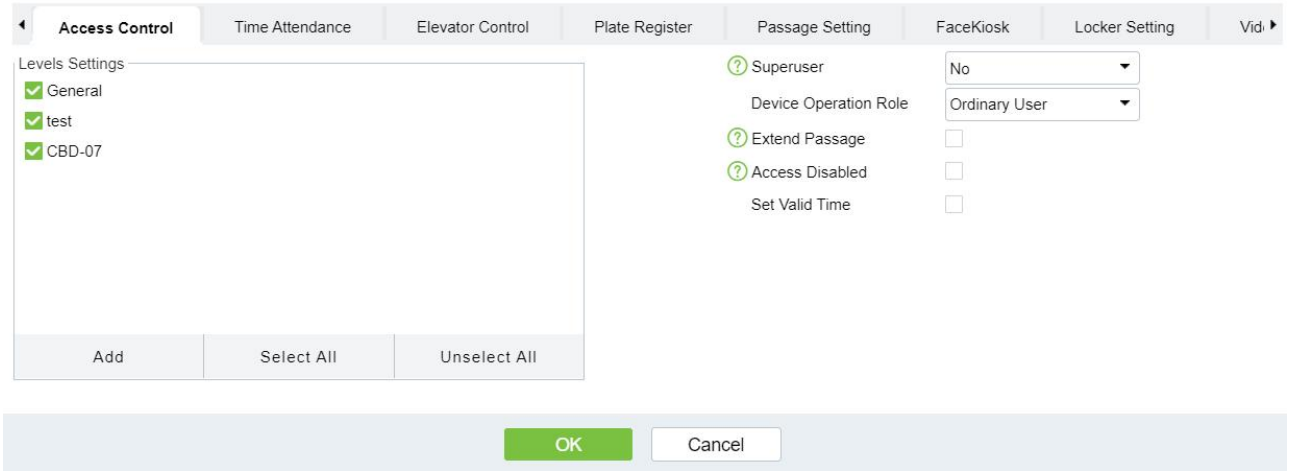


Figure 2- 7 Access Control

Fields are as follows:

Parameter	Description
Level settings	Click **Add,** then set passage rules of special positions in different time zones.
Superuser	In access controller operation, a super user is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door-opening priority.
Device Operation Role	Select administrator to get its levels.
Extend Passage	Extend the waiting time for the personnel through the access points. Suitable for physically challenged or people with other disabilities.
Access Disabled	Temporarily disable the personnel's access level;currently InBio Pro,InBio Pro Plus Controller ,Proface X(ZAM230),SpeedFface V5L(ZAM230).etc supported.
Set Valid Time	Set Temporary access level. Doors can be set to open only within certain time periods. If it is not checked, the time to open the door is always active.

Table 2- 2 Access Control

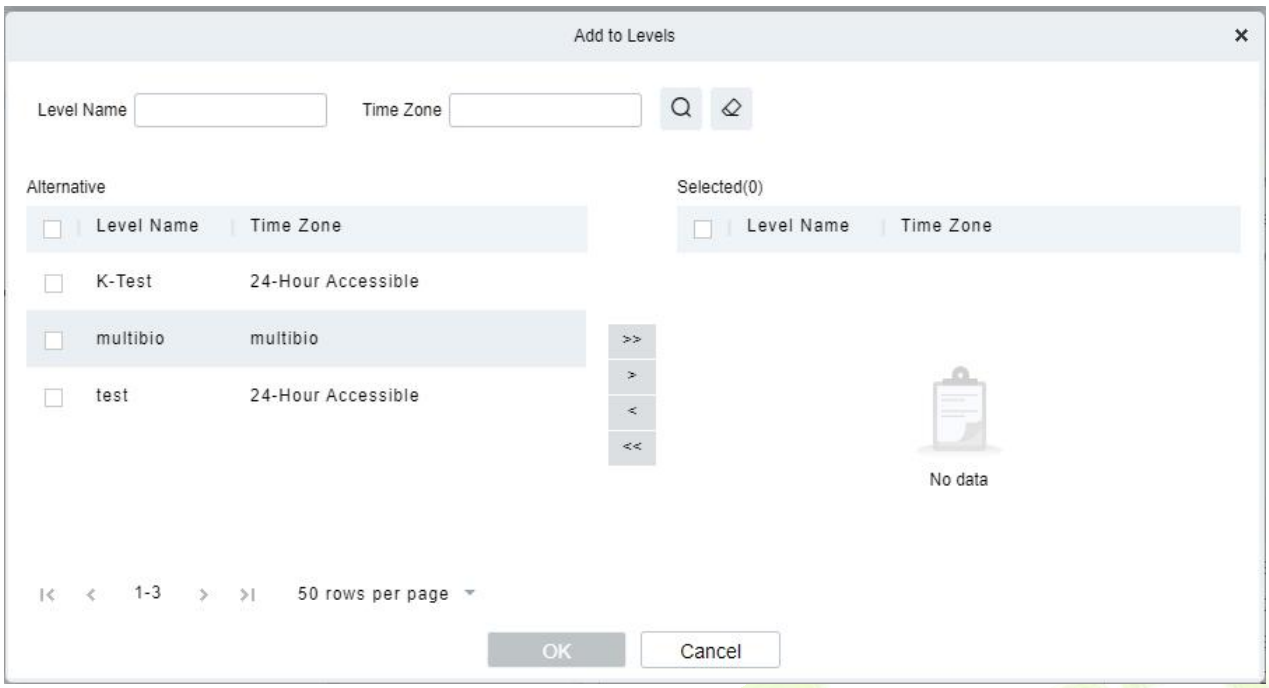


Figure 2- 8 Level Settings

Note:

1. The system will automatically search for the relevant numbers in the departure library during verification.
2. 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.
3. Not all devices support the "Disabled" function. When a user adds a device, the system will notify the user whether the current device supports this function. If the user needs to use this function, please upgrade the device.
4. Not all the devices support the "Set Valid Time" function of setting the hour, minute, and second. Some devices only allow users to set the year, month, and day of the local time. When a user adds a device, the system will notify the user whether the current device support this function. If the user needs to use this function, please upgrade the device.

● Time Attendance:

Set the **Time Attendance** parameter for the personnel.

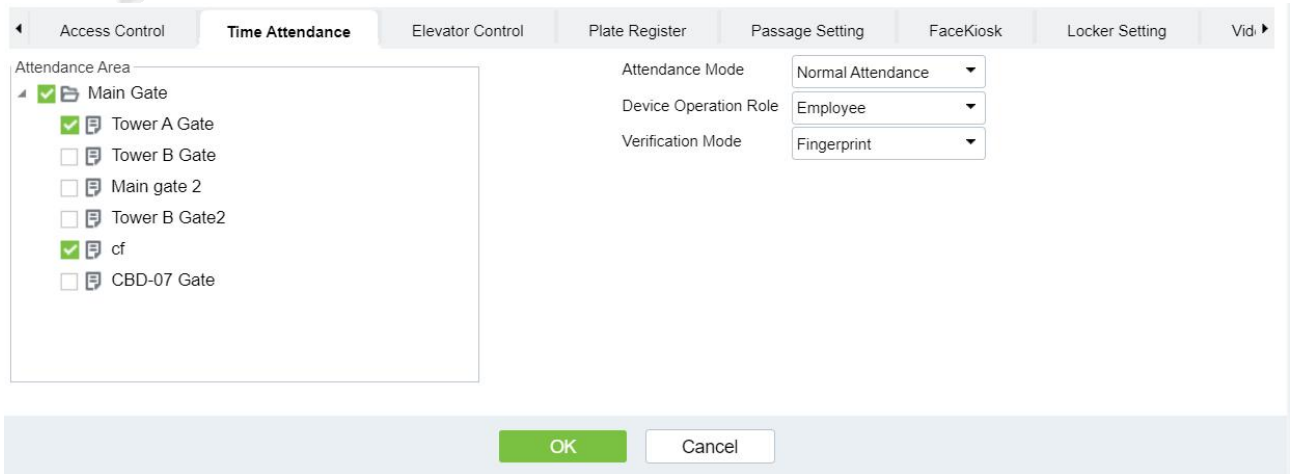


Figure 2- 9 Time Attendance

Fields are as follows:

Parameter	Description
Attendance Mode	You can set the staff attendance area as **Normal Attendance** and **No Punch Required.**
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, **Employee, Enroller, Administrator, and Superuser**
Verification Mode	You can set verification mode as following options: Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.

Table 2- 3 Time Attendance

● Elevator Control:

Click **Elevator Control** and set the Elevator Control parameter for the personnel.

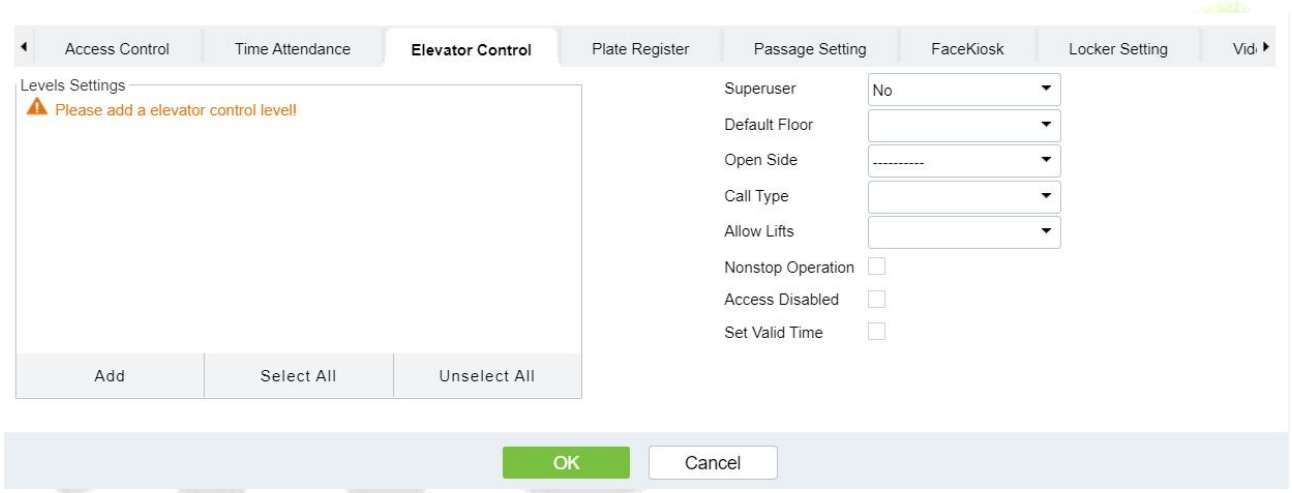


Figure 2- 10 Elevator Control

Fields are as follows:

Parameter	Description
Superuser	In elevator controller operation, a super user is not restricted by the regulations on time zones, holidays and has extremely high door-opening priority.
Default Floor	Select the floor that needs to be reached.
Open Side	Select the elevator door opening direction based on actual conditions.only DCS supported
Call Type	Select different roles based on user permissions.only DCS supported
Allow Lifts	Allowed elevator cars, only supported by KONE; Mitsubishi elevator no supported.
Nonstop Operation	Enabling this option will allow the elevator to directly reach the floor
Access Disabled	Checking the box will disable elevator privileges for that person; currently EC16 control panel and DCS system supported.

Parameter	Description
Set Valid Time	Set Temporary Floor permission. Floor can be set to enable only within certain time periods. If it is not checked, the time to open the door is always active.

Table 2- 4 Elevator Control

✍**Note:** The Elevator level must be set in advance.

● Plate Register:

Click **Plate Register**, set the plate control parameter for the personnel.

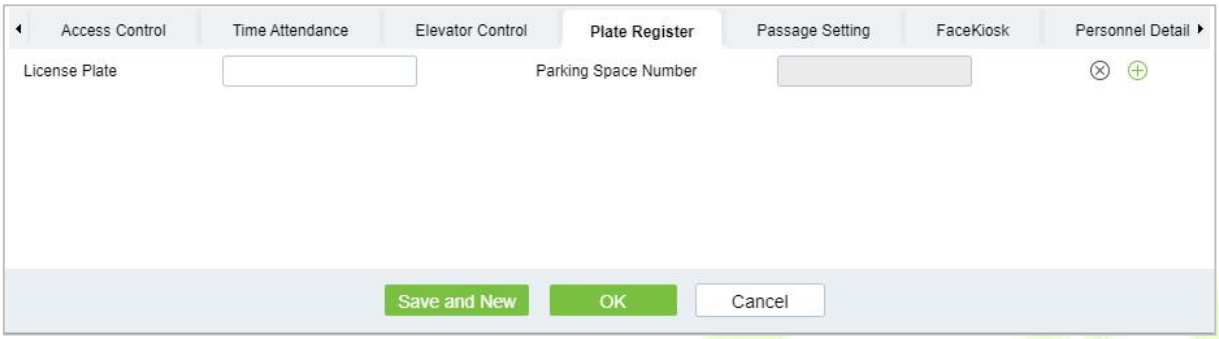


Figure 2- 11 Plate Register

Fields are as follows:

Parameter	Description
License Plate	The user needs to register the license plate.
Parking Space Number	Parking space number corresponding to the vehicle.

Table 2- 5 Plate Register

✍**Note:** Each personnel may register a maximum of 6 license plates.

● Passage Setting:

Click **Passage Setting**, set the Passage Setting parameter for the personnel.

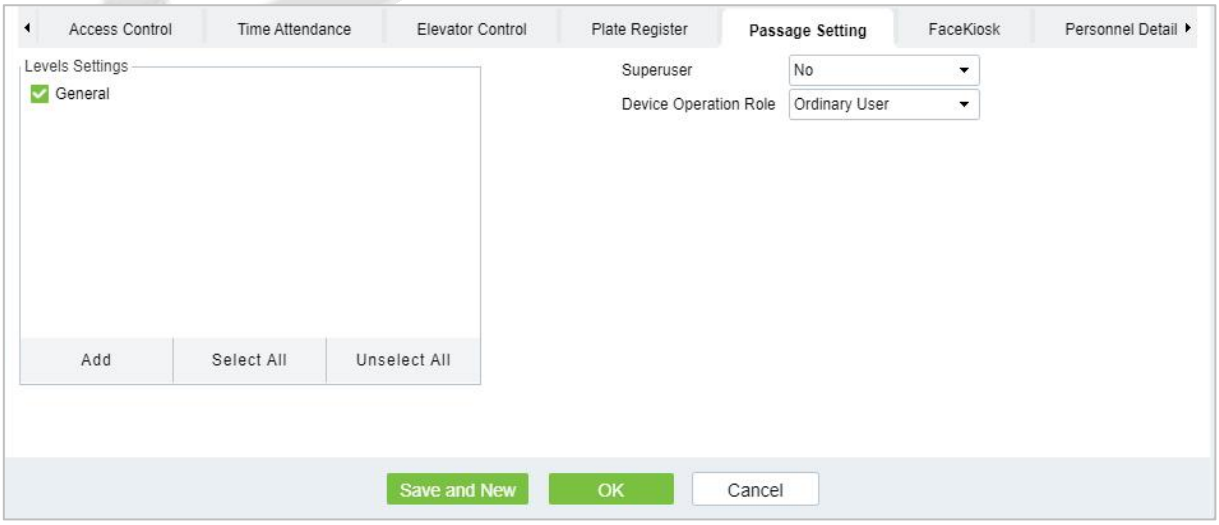


Figure 2- 12 Passage Setting

Fields are as follows:

Parameter	Description
Superuser	Set Superuser as **Yes** or **No** according to requirement.

Parameter	Description
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, **Ordinary User, Administrator**, and **Enroller.**

Table 2- 6 Passage Setting

● Facekiosk:

Click **Facekiosk**, set the Facekiosk parameter for the personnel.

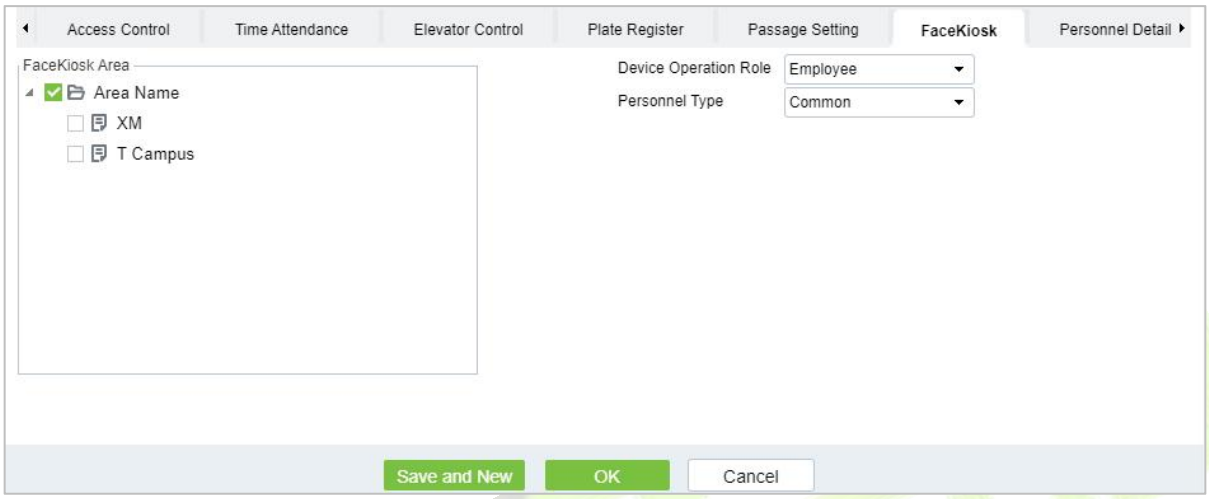


Figure 2- 13 Facekiosk

Fields are as follows:

Parameter	Description
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, employee and Superuser.
Personnel Type	Select type of personnel such as Common, VIP, and Blocklist.

Table 2- 7 Facekiosk

● Locker Setting:

Assigning a cabinet that has a locker number for the personnel.

Click **Locker Setting**, view the locker number for this personnel.

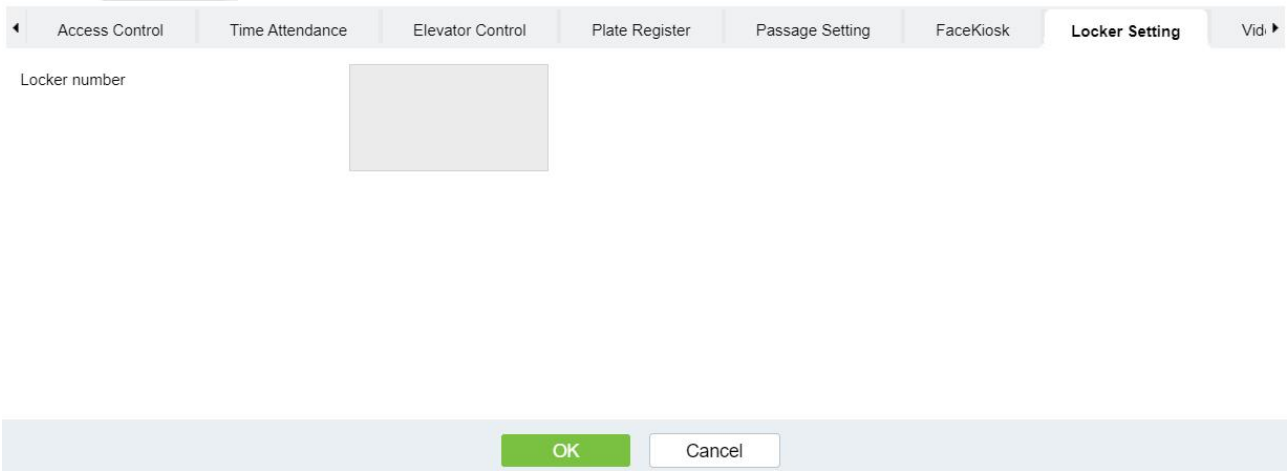


Figure 2- 14 Locker

● Video Intercom Setting:

Assigning extension number to selected person from personnel module, an extension number is a

number or code used within a company or organization to identify different telephone sets.

Click **Video Intercom Setting**,assign a room number or extension number to this person.

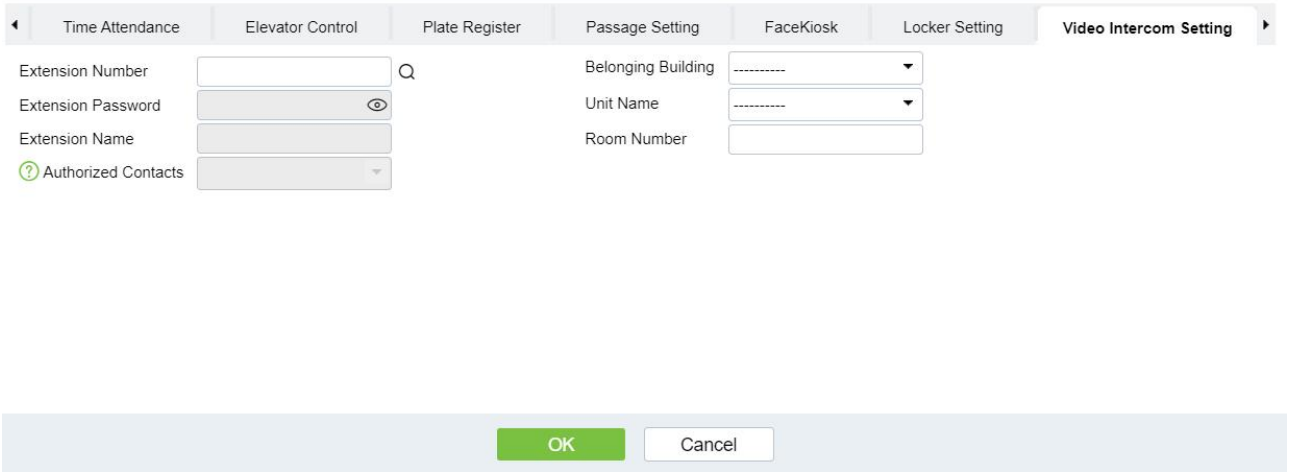


Figure 2- 15 Video Intercom Setting

Fields are as follows:

Parameter	Description
Extension Number	Assign an extension number to this person, click to select.
Extension Password	After selecting the Extension Number, the password will be automatically filled in, but the administrator can also modify it.
Extension Name	After selecting the Extension Number, it will be automatically filled in, and the administrator can also make changes.
Authorized Contacts	You can choose to assign this person to a contact list, which will be displayed in the Mobile APP after assignment.
Belonging Building	The building where the person resides
Unit Name	The unit where the person resides
Room Number	The room number where the person resides

Table 2- 8 Video Intercom

● More Card:

Click **More Card**, the user can register another card for this person.

✍ **Note:** This feature requires the multi-card per person function to be enabled first. The operation method is: go to **Parameters -> Card Setting -> Multiple cards per personnel** and select **Yes**.

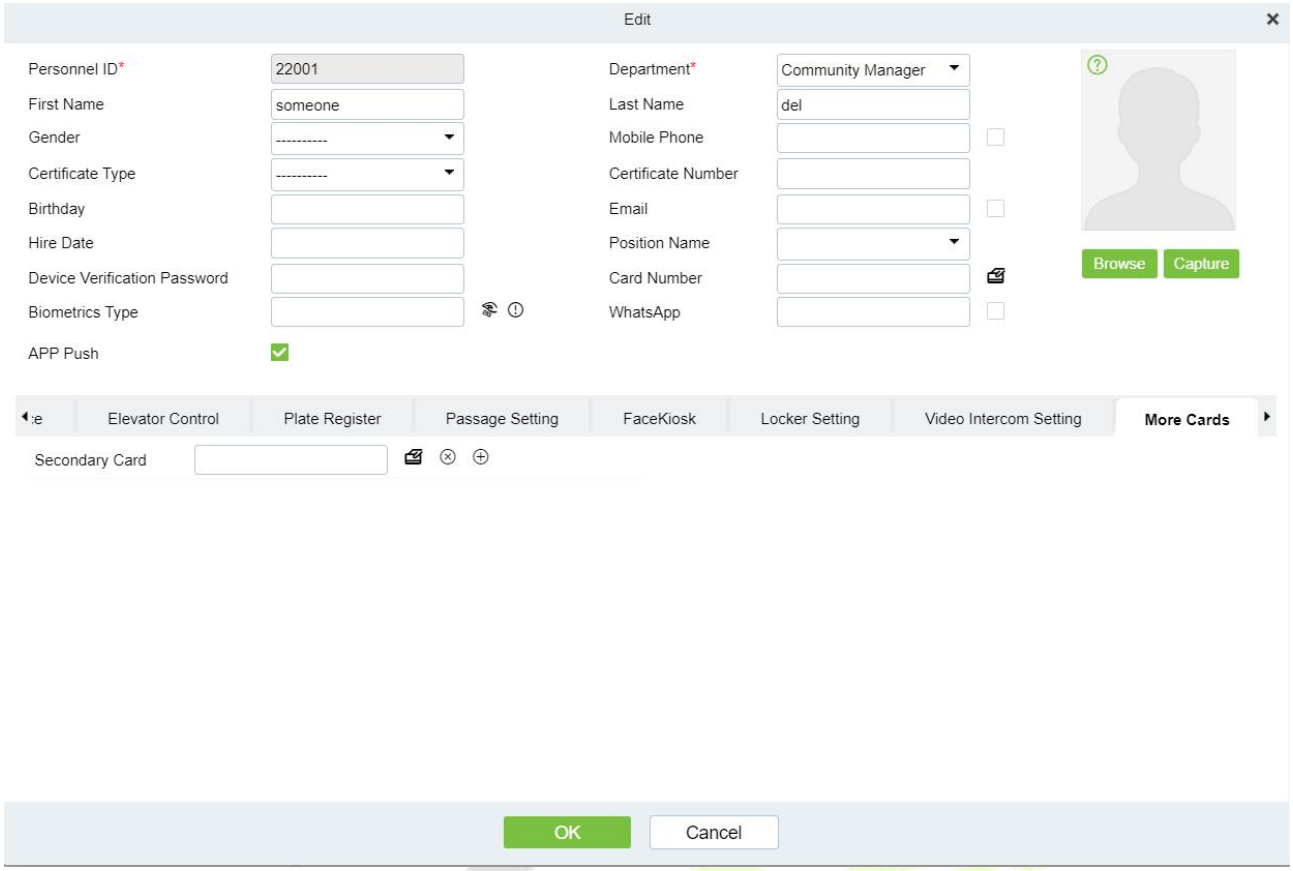


Figure 2- 16 More Card

● Personnel Details:

Click **Personnel Details**, to set the Personnel detail parameter for the personnel.

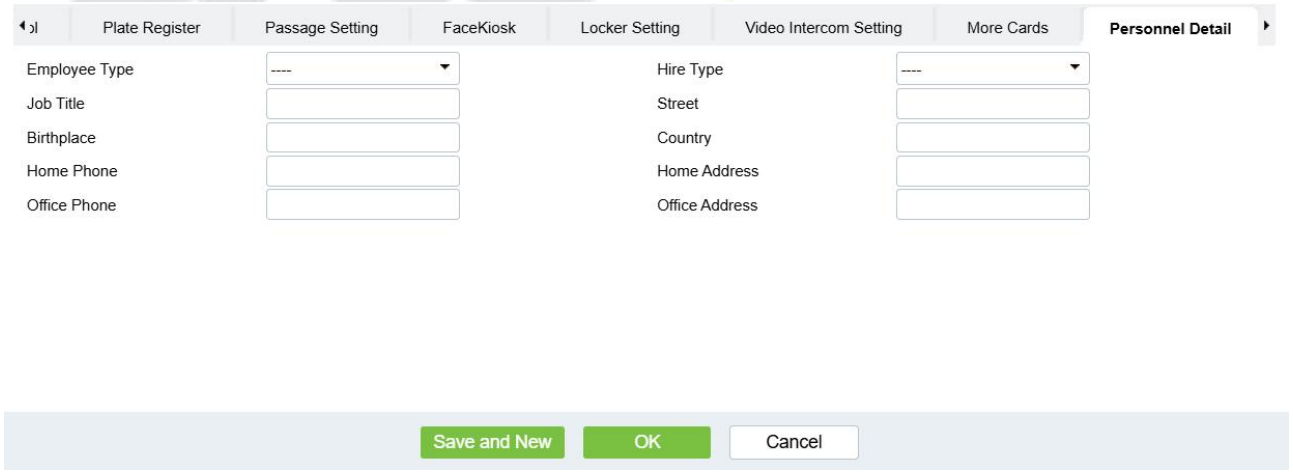


Figure 2- 17 Personnel Details

✍**Note:**If you need to display more fields, you can first add them under the **Custom Attributes** menu.

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

2.1.1.2Personnel Adjustments

Click **Personnel > Person > Personnel Adjustment**.

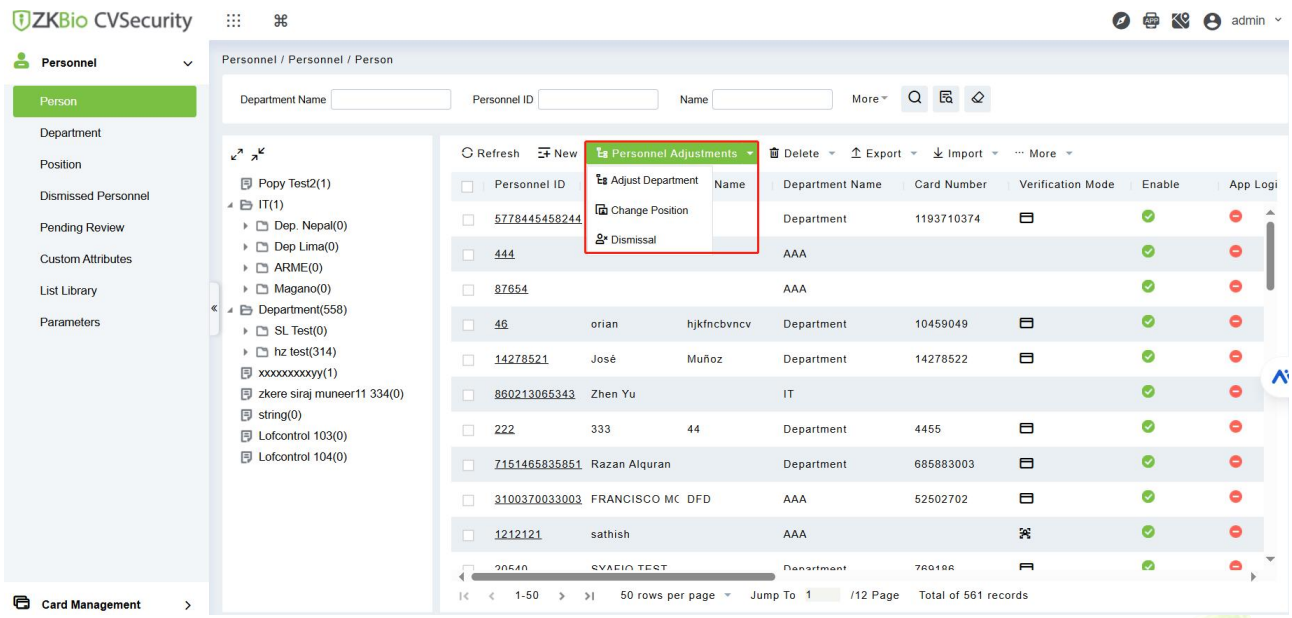


Figure 2- 18 Personnel Adjustment

- **Adjust Department:**

Select the person from the list.Click **Personnel > Person > Personnel Adjustment**, then select **Adjust Department.**

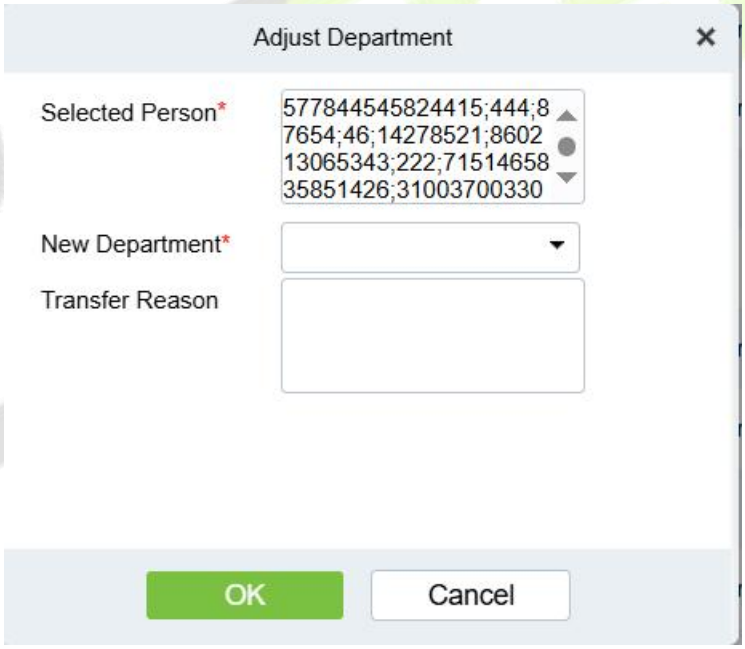


Figure 2- 19 Adjust Department

Fields are as follows:

Parameter	Description
New Department	Select new department from list.
Transfer Reason	Mention the reason for transfer.

Table 2- 9 Adjust Department

- **Change Position:**

Select the person from the list.Click **Personnel > Person > Personnel Adjustment**, then select Change Position.

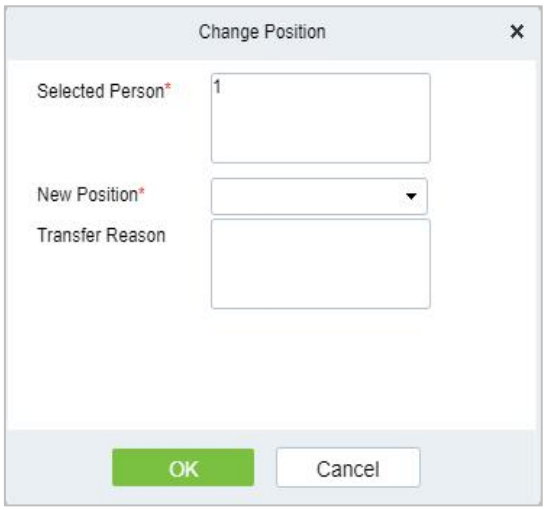


Figure 2- 20 Change Position

Parameter	Description
New Position	Select new Position from list.
Transfer Reason	Mention the reason for transfer.

Table 2- 10 Change Position

● Dismissal:

Select the person from the list.Click **Personnel > Person > Personnel Adjustment**, then select Dismissal.

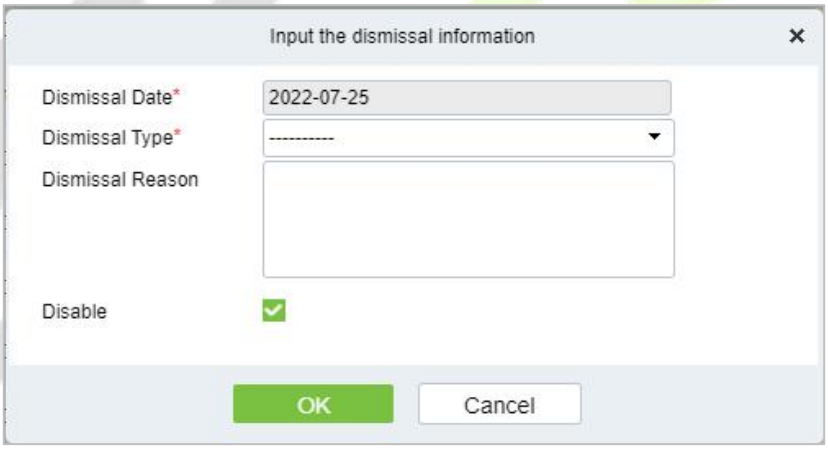


Figure 2- 21 Dismissal

Fields are as follows:

Parameter	Description
Dismissal Date	Select date.
Dismissal Type	Select the type of dismissal from follows, Voluntary Redundancy, Transfer, Dismissed, Resignation.
Dismissal Reason	Mention the reason for Dismissal.

Table 2- 11 Dismissal

2.1.1.3Delete

Click **Personnel > Person**, then select Delete.

● Delete Personnel:

Click **Personnel > Person > Delete**, then select Delete Personnel.

● Delete Biometric Data:

Click **Personnel > Person > Delete**, then select Delete Biometric Data.

2.1.1.4 Export

Click **Personnel > Person**, then select Export.

● Export Personnel:

Click **Personnel > Person > Export**, then select Export Personnel.

Personnel's basic information is all checked (selected), check custom attributes as required.

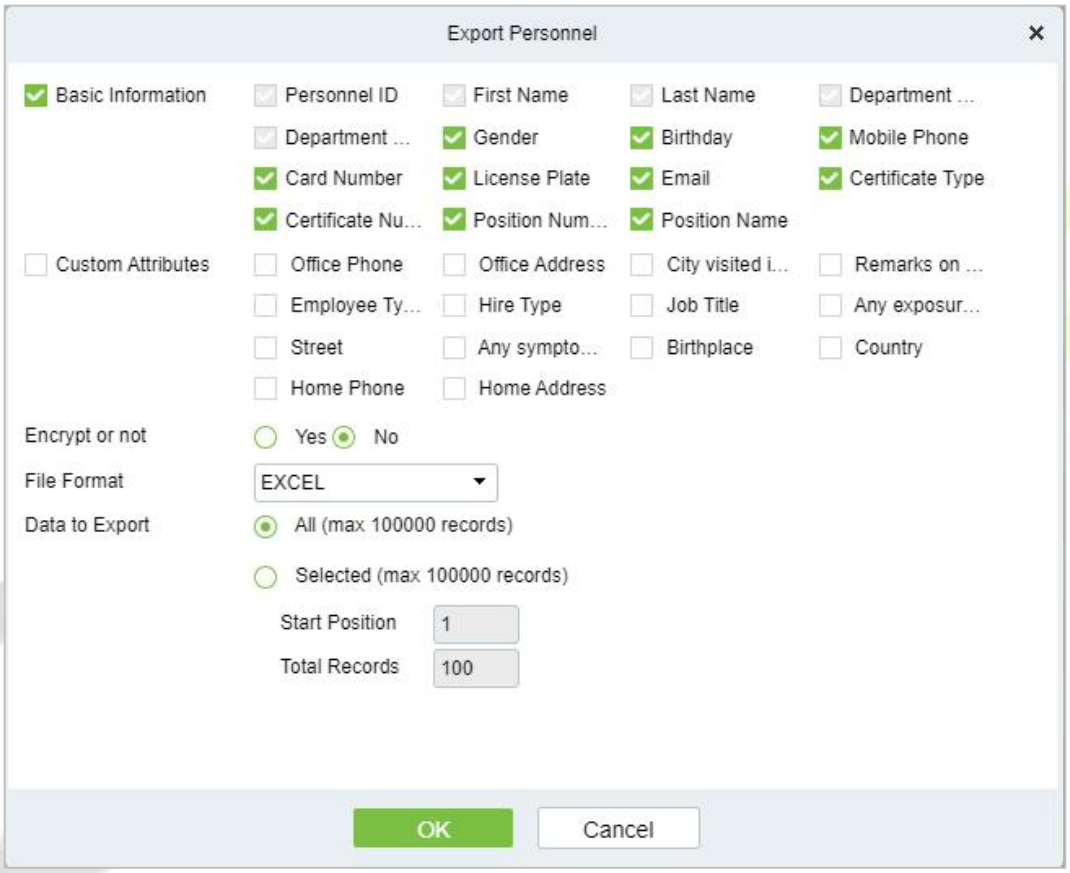
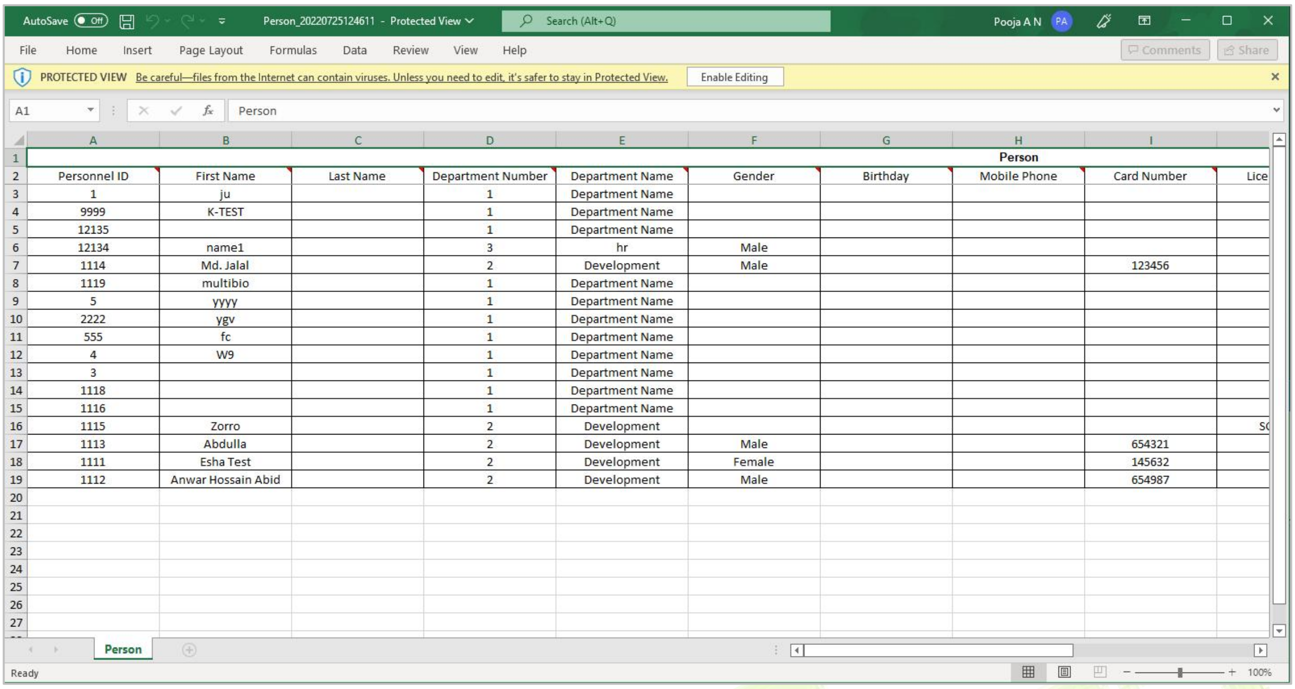


Figure 2- 22 Export Personnel



Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Mobile Phone	Card Number	Lice
1	ju		1	Department Name					
9999	K-TEST		1	Department Name					
12135			1	Department Name					
12134	name1		3	hr	Male				
1114	Md. Jalal		2	Development	Male			123456	
1119	multibio		1	Department Name					
5	yyyy		1	Department Name					
2222	ygv		1	Department Name					
555	fc		1	Department Name					
4	W9		1	Department Name					
3			1	Department Name					
1118			1	Department Name					
1116			1	Department Name					
1115	Zorro		2	Development					S(
1113	Abdulla		2	Development	Male			654321	
1111	Esha Test		2	Development	Female			145632	
1112	Anwar Hossain Abid		2	Development	Male			654987	

Figure 2- 23 Export Personnel

● Export Biometric Template:

Click **Personnel** > **Person** > **Export**, then select Export Biometric Template.

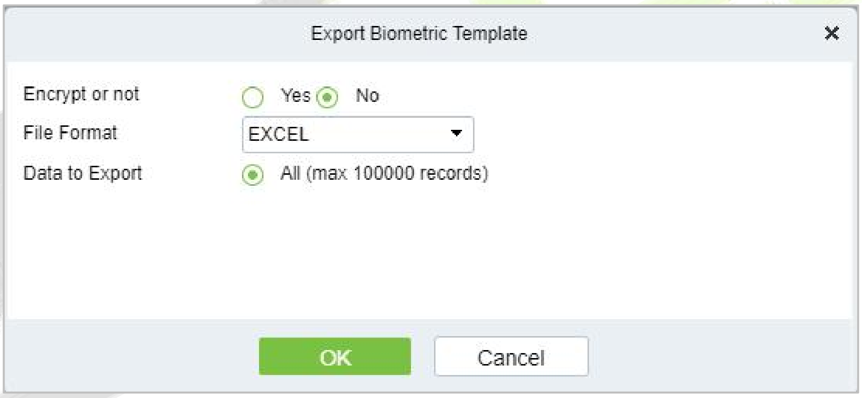
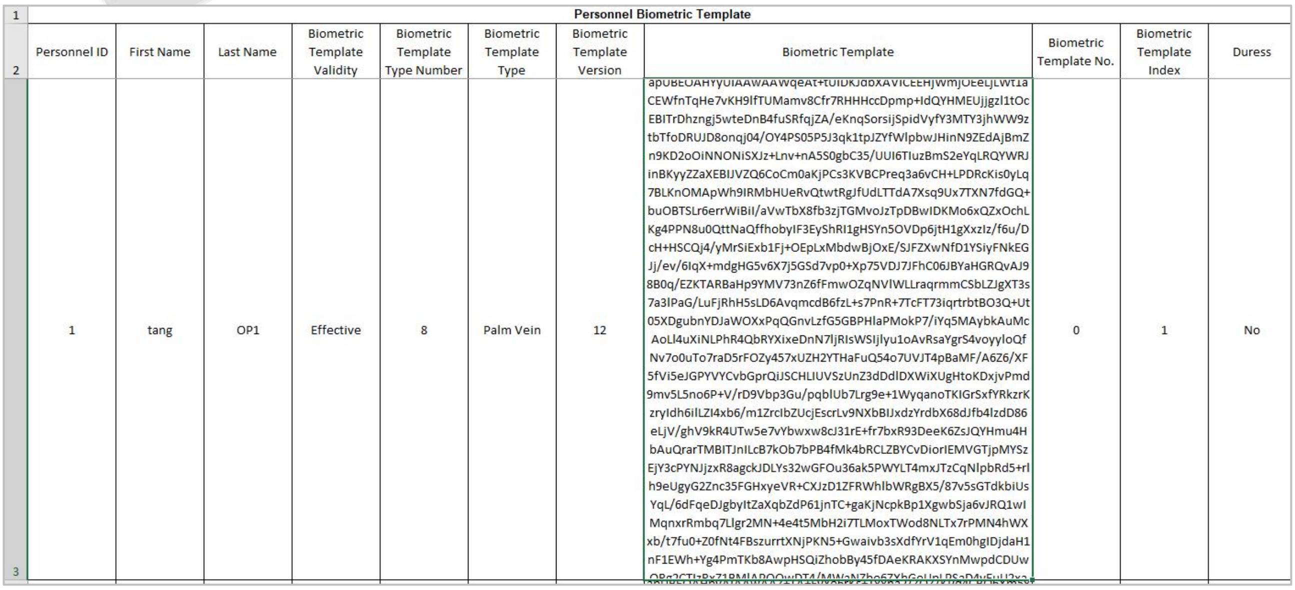


Figure 2- 24 Export Biometric Template



Personnel ID	First Name	Last Name	Biometric Template Validity	Biometric Template Type Number	Biometric Template Type	Biometric Template Version	Biometric Template	Biometric Template No.	Biometric Template Index	Duress
1	tang	OP1	Effective	8	Palm Vein	12	CEWfnTqHe7vKH9lfTUMamv8Cfr7RHHHccDpmp+IdQYHMEUjjgzl1tOcEBITrDhzngj5wteDnB4fuSRfqjZA/eKnqSorsijSpidVyfY3MTY3jhWW9ztbTfoDRUJD8onqj04/OY4PS05P5J3qk1tpJZYfWlpbwJHinN9ZEdAjBmZn9KD2oOiNNONiSXJz+Lnv+nA5S0gbC35/UUI6TIuzBmS2eYqLRQYWRJinBKyyZZaXEBIJVZQ6CoCm0aKjPCs3KVBCPreq3a6vCH+LPDRcKis0yLq7BLKnOMApWh9IRMbHUeRvQtwtRgJfUdLTTdA7Xsq9Ux7TXN7fdGQ+buOBTSLr6errWiBiI/aVwTbX8fb3zjTGMvoJzTpDBwIDKMo6xQZxOchLKg4PPN8u0QttNaQffhobyIF3EyShRI1gHSYn5OVDp6jtH1gXxzIz/f6u/DcH+HSCQj4/yMrSiExb1Fj+OEpLxMbdwBjOxE/SJFZXwNfD1YSiyFNkEGJj/ev/6IqX+mdgHG5v6X7j5GSd7vp0+Xp75VDJ7JFhC06JBYaHGRQvAJ98B0q/EZKTARBaHp9YMV73nZ6fFmwOZqNVlWLLraqrmmCSbLZJgXT3s7a3lPaG/LuFjRhH5sLD6AvqmcdB6fzL+s7PnR+7TcFT73iqrtrbtBO3Q+Ut05XDgubnYDJaWOXxPqQGnvLzfG5GBPHlaPMokP7/iYq5MAybkAuMcAoLl4uXiNLPhR4QbRYXixeDnN7ljRIsWSIjlyu1oAvRsaYgrS4voyyloQfNv7o0uTo7raD5rFOZy457xUZH2YTHaFuQ54o7UVJT4pBaMF/A6Z6/XF5fVi5eJGPYVYCvbGprQiJSCHLIUVSzUnZ3dDdlDXWiXUgHtoKDxjvPmd9mv5L5no6P+V/rD9Vbp3Gu/pqblUb7Lrg9e+1WyqanoTKIGrSxfYRkzrKzryIdh6ilLZI4xb6/m1ZrcIbZUcjEscrLv9NXbBIJxdzYrdbX68dJfb4lzdD86eLjV/ghV9kR4UTw5e7vYbwxw8cJ31rE+fr7bxR93DeeK6ZsJQYHmu4HbAuQrarTMBITJnILcB7kOb7bPB4fMk4bRCLZBYCvDiorIEMVGTjpMYSzEjY3cPYNJjzxR8agckJDLYs32wGFOu36ak5PWYLT4mxJTzCqNlpbRd5+rlh9eUgyG2Znc35FGHxyeVR+CXJzD1ZFRWhlbWRgBX5/87v5sGTdkbiUsYqL/6dFqeDJgbyItZaXqbZdP61jnTC+gaKjNcpkBp1XgwbSja6vJRQ1wIMqnxrRmbq7Llgr2MN+4e4t5MbH2i7TLMoxTWod8NLTx7rPMN4hWXxb/t7fu0+Z0fNt4FBszurrtXNjPKN5+Gwaivb3sXdfYrV1qEm0hgIDjdaH1nF1EWh+Yg4PmTKb8AwpHSQiZhobBy45fDAeKRAKXSYnMwpdCDUw	0	1	No

Figure 2- 25 Export Biometric Template.

● Export Personnel Photo:

Click **Personnel > Person > Export**, then select Export Personnel Photo.

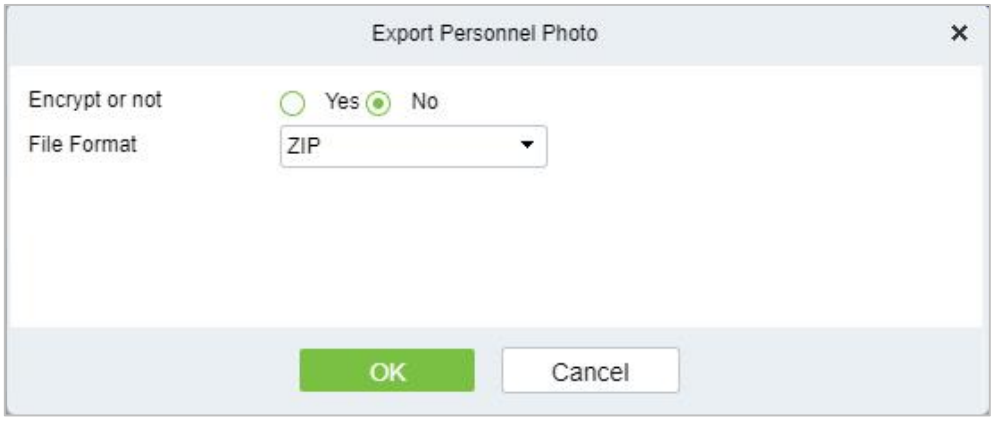


Figure 2- 26 Export Personnel Photo

2.1.1.5Import

Introduce the configuration Steps of manually importing personnel in batches in ZKBio CVSecurity.

It is suitable for scenarios where a large number of personnel information is added. Compared with the manual registration method of individual personnel, the batch import and addition method is faster.

Before adding departments in batches, you need to fill in the template file as required. After filling out the template file, you can import and add departments in batches in the "Department" interface.

● Instruction:

1. The import and addition of personnel includes importing personnel information, personnel biometric template data (optional), and personnel photos (optional), which need to be imported separately.
2. Importing is to pay attention to the uniqueness of the personnel number. When the personnel number is repeated, the result of import and addition will fail.

Import Personnel Information

Before adding people in batches, you need to obtain or fill in a template file as required. After filling in the template file, you can import and add people in batches on the Personnel Management > Personnel interface.

● Steps:

Step 1: In the Personnel module, choose "**Personnel Management > Personnel**".

Step 2: On the personnel interface, select and click the "**Import** > **Download Personnel Import Template**" button, select the parameters to be filled in, and download the template "personnel information template.xls" locally. The parameter selection is shown in Figure 2-21.

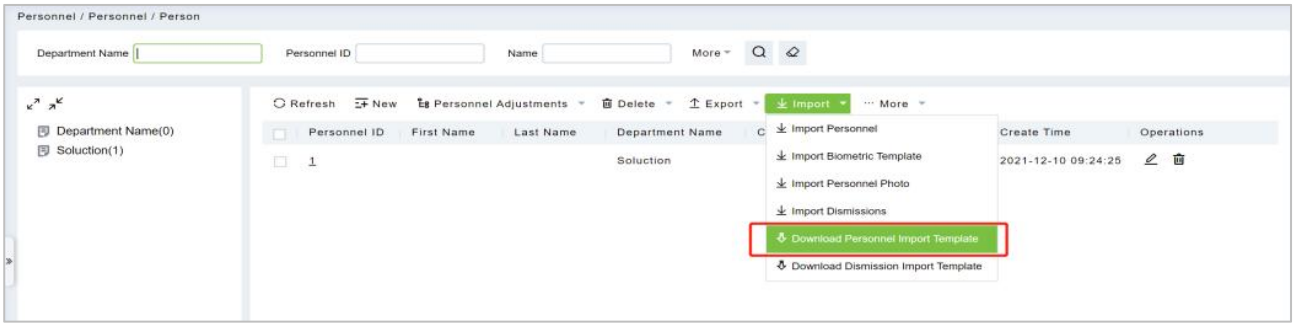


Figure 2- 27 Import Personnel Information Template

Step 3: Open the exported template file "Personnel Information Template.xls" for adding personnel information.

Step 4: In the personnel interface, select and click the "**Import** > **Import Personnel Information**" button; in the **Import Personnel** Interface, click the **Browse** button to import the batch import template into the system, as shown in figure below

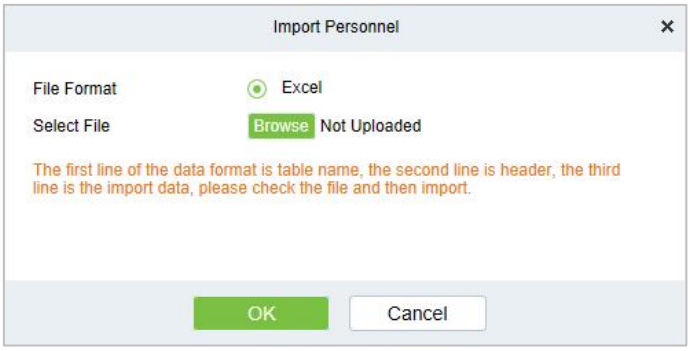


Figure 2- 28 Import Personnel

Step 5: Click **OK**, and the interface displays the result of personnel import and addition.

Step 6: Click **Close** to complete the import and addition of personnel information.

Import Biometric Template

● Preconditions:

1. The system needs to have the basic information files of the personnel in order to support the import of biometric template data.
2. The biometric template data of the current system personnel has been obtained.

● Steps:

Step 1: In the Personnel module, choose "**Personnel Management > Personnel**".

Step 2: On the personnel interface, select and click the "**Import** > **Import Biometric Template Data**" button; in the pop-up import personnel biometric template data interface, click the **Browse** button to import personnel biometric template data into the system in batches, as shown in Figure 2-23 is shown.

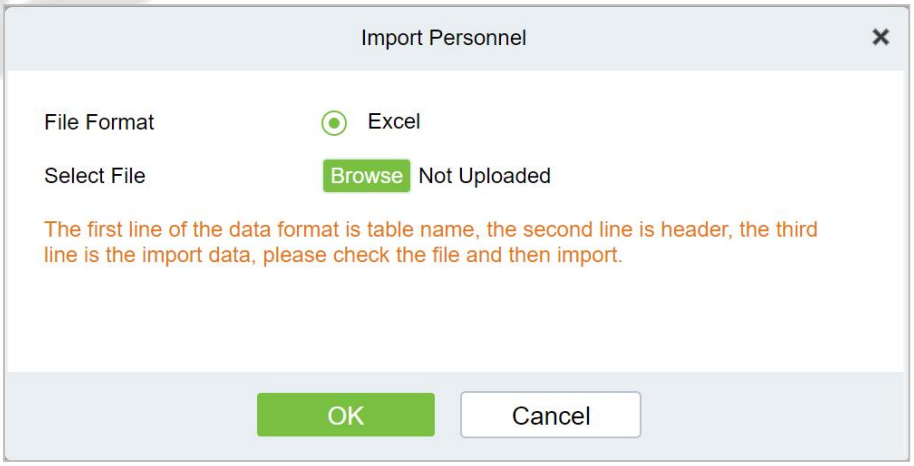


Figure 2- 29 Importing Personnel Biometric Template Data

Step 3: Click **OK**, the interface displays the import and addition results.

Step 4: Click **Close** to complete the import of personnel biometric template data.

Import Personnel Photos

● Preconditions:

1. The system needs to have the basic information files of the personnel in order to support the import of personnel photos.
2. The personnel photos of the current system personnel have been obtained and correctly named according to the personnel number.
3. The photo requirements for personnel are as follows:

Image Format: support .JPEG, .png format.

Image Size: The recommended image size is 35KB~200KB, and the maximum size of a single image is 5MB.

Image Quality: Faces in images are clear and not blurred by lens defocus or face motion. The minimum image depth is an 8-bit grayscale image.

Pixels: The recommended value of face pixels is 200*200, and the distance between the eyes should be greater than or equal to 60 pixels, preferably greater than or equal to 90 pixels.

Brightness and Contrast: The ambient illumination is not less than 300Lux, the image brightness is uniform, the contrast is moderate, and the face has no invisible, no backlight, no reflection, no overexposure, no underexposure and no yin and yang faces.

Attitude: The portrait is upright, looking straight ahead, the horizontal rotation angle of the face should be within ±10°, the elevation angle should be within ±10°, and the tilt angle should be within ±10°.

Blocking: Eyebrows, eyes, mouth, nose and facial contours should not be blocked by bangs, masks, accessories, glasses, etc. The lenses of glasses should be colorless and non-reflective, and the frames of glasses should not be too thick to block human eyes.

Face Area: The face is complete, the outline and facial features are clear, and there is no heavy makeup. The face area of the image should not be processed by PS.

Expression: Natural expression, neutral or smiling (no missing teeth), eyes open naturally, mouth closed naturally, no obvious expressions such as laughter or frown.

● Steps:

Step 1: In the Personnel module, choose “Personnel Management > Personnel”.

Step 2: On the Personnel interface, select and click the "Import > Import Personnel Photo" button, as shown in figure below.

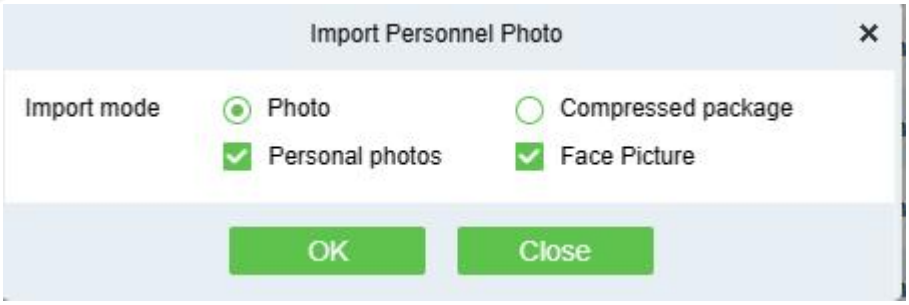


Figure 2- 30 Import Personnel Photos

✍**Note:** If you have selected Face Picture, the pixel of the face photo must be greater than 80,000 pixels, and the face should be centered and well-lit.

Step 3: Optional: upload photos and compressed packages.

Step 4: After selecting the photo method, click **OK** to enter the interface for importing personnel photos, select the photo and click **Start Uploading**.

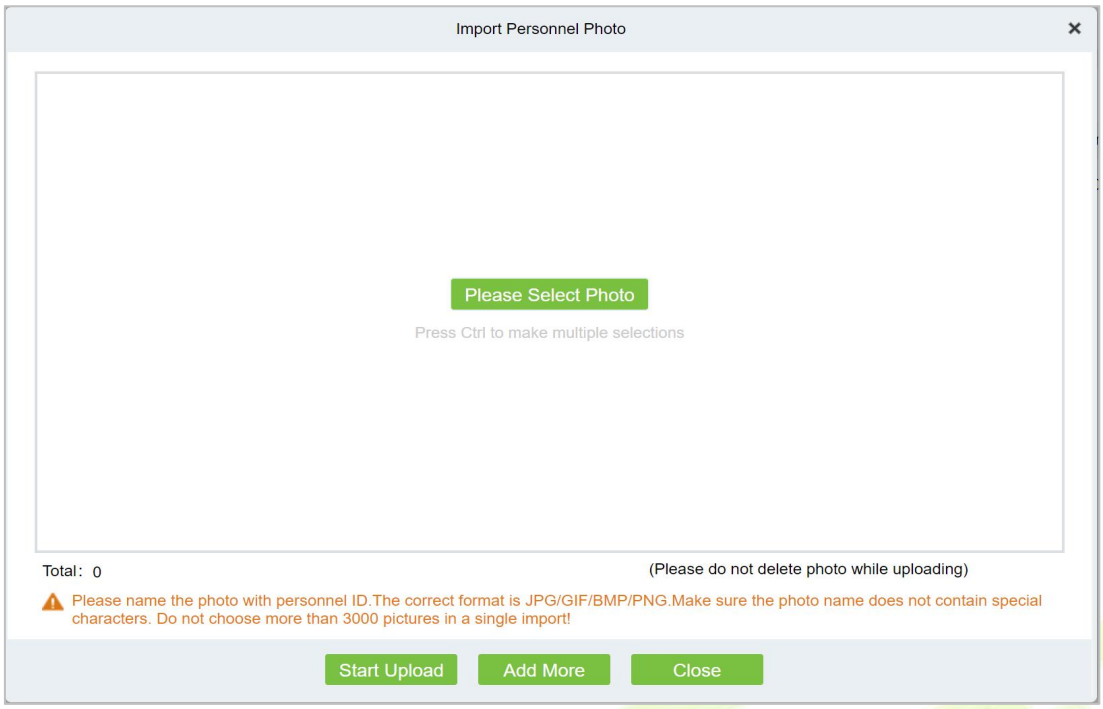


Figure 2- 31 Photos - Importing Personnel Photos

Step 5: After selecting the compression package method, click **OK** to enter the interface of importing personnel photos, click **Browse** to select the file and then click "**Start Uploading**".

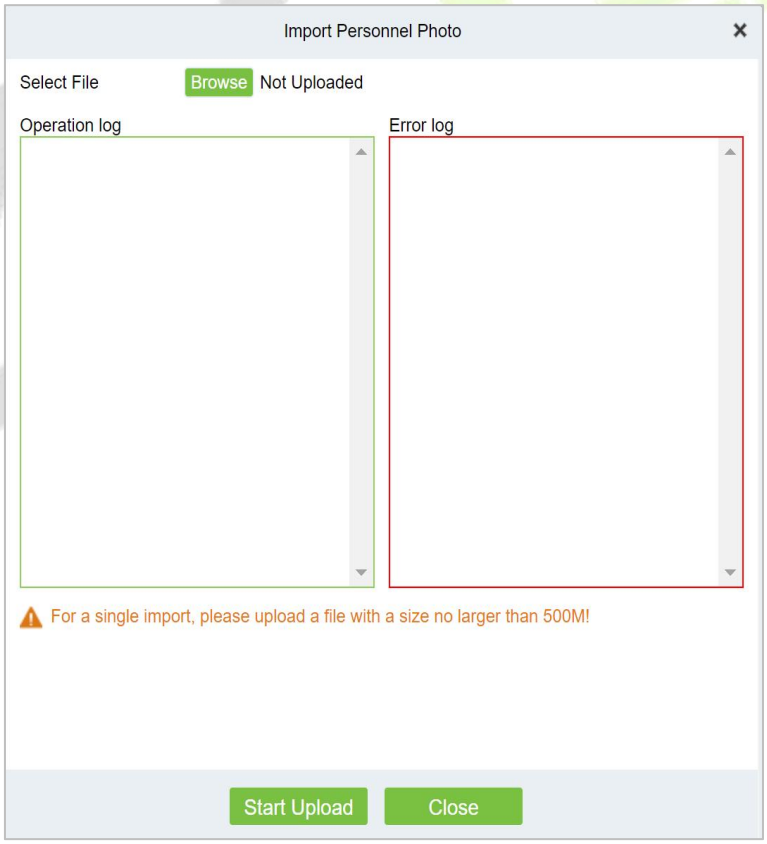


Figure 2- 32 Compressed Package - Importing Personnel Photos

Step 6: After the upload is complete, the interface displays the results of the imported personnel photos.

Step 7: Click **Close** to complete the import and addition of personnel photos.

2.1.1.6More

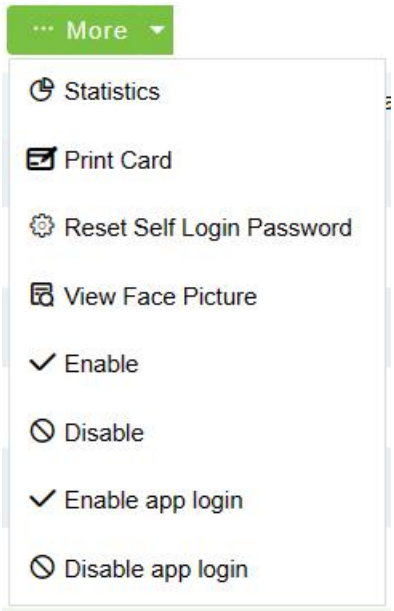


Figure 2- 33 More

Statistics

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

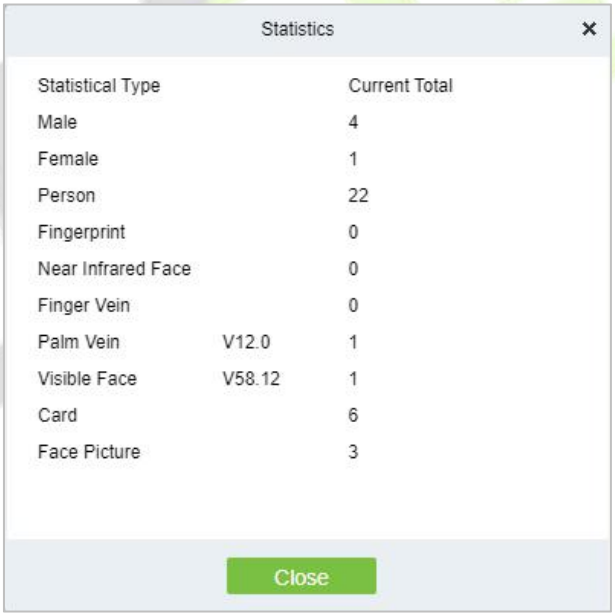


Figure 2- 34 Statistics

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.

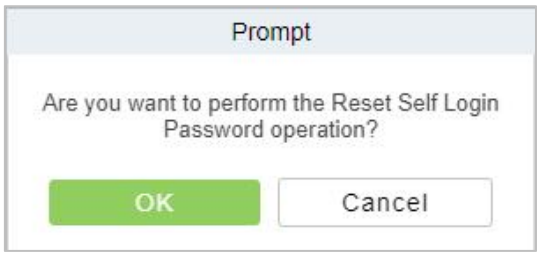


Figure 2- 35 Statistics

View Face Picture (V6.0.0 or above supported)

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

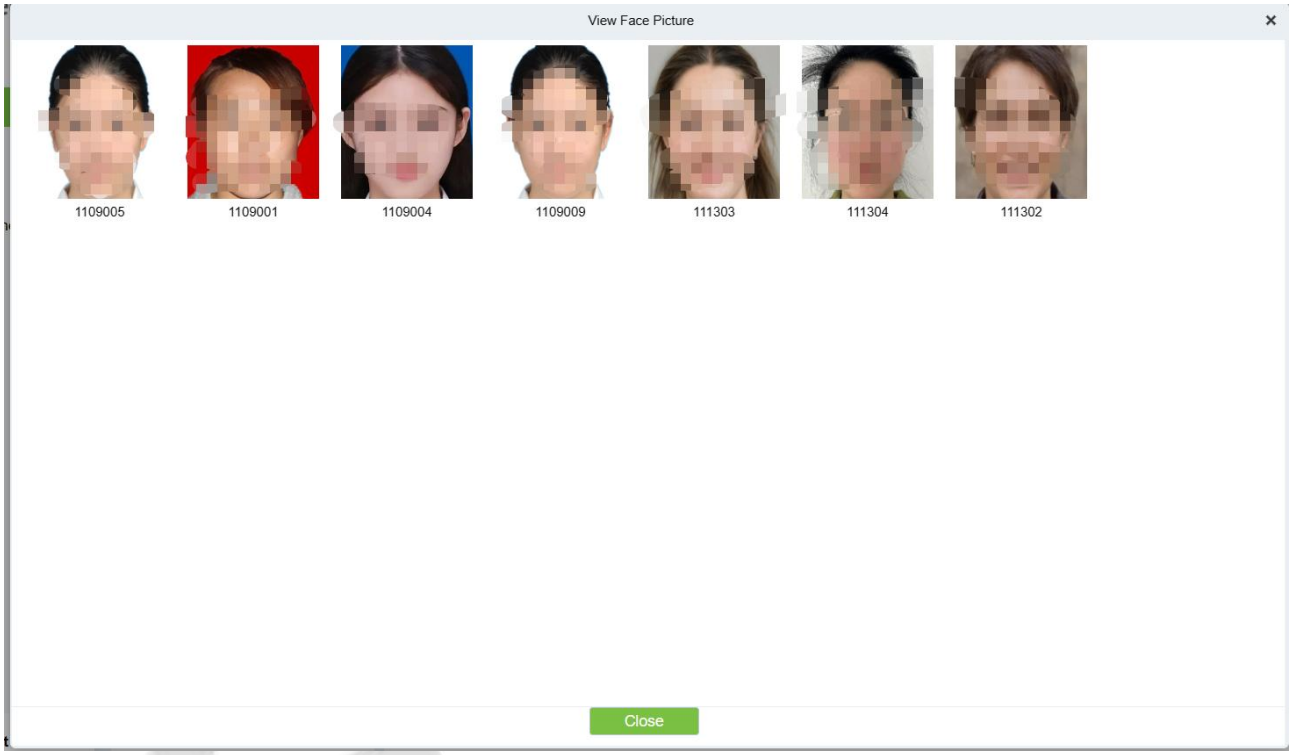


Figure 2- 36

Enable (V6.1.0 or above supported)

Click **Personnel** > **Person** > **More**, then select **Enable. Selected** persons will be enabled.

Disable (V6.1.0 or above supported)

Click **Personnel** > **Person** > **More**, then select **Disable. The** credentials of the selected personnel will be disabled; all the access rights of the selected personnel such as access control, gate barrier, elevator control, locker, etc. will be unavailable, and at the same time will not be able to take attendance, consumption and so on until enabled.

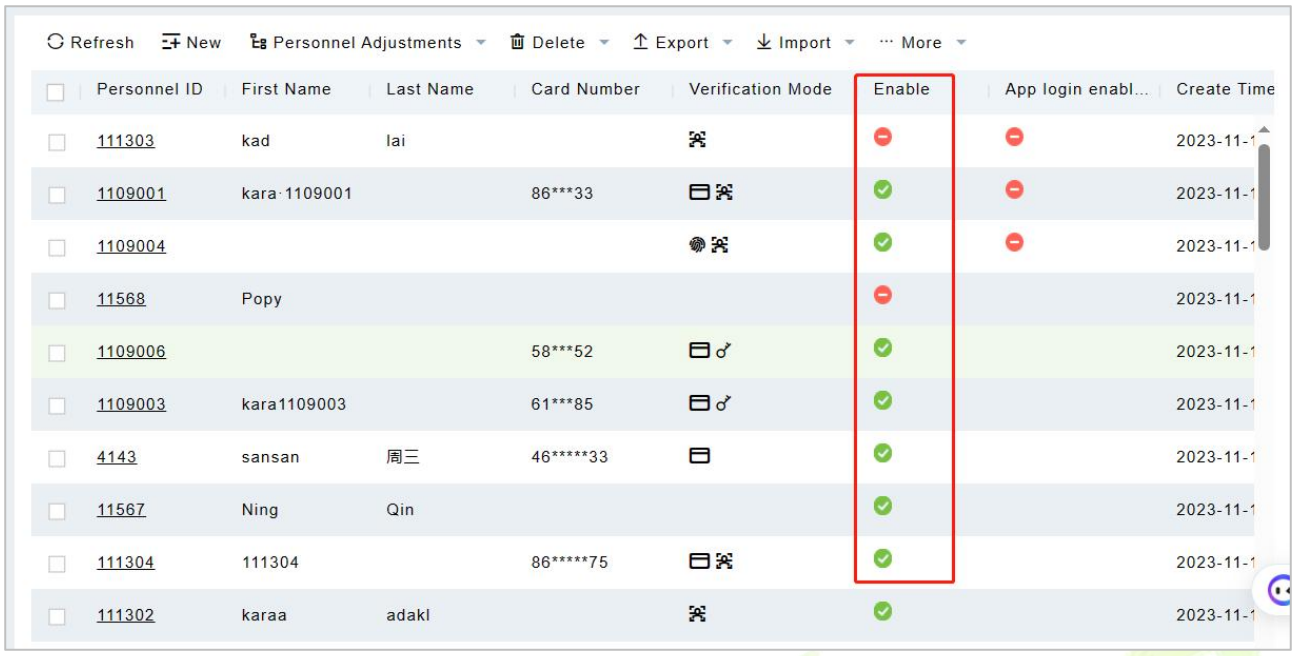


Figure 2- 37

Enable APP Login (V6.1.0 or above supported)

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.

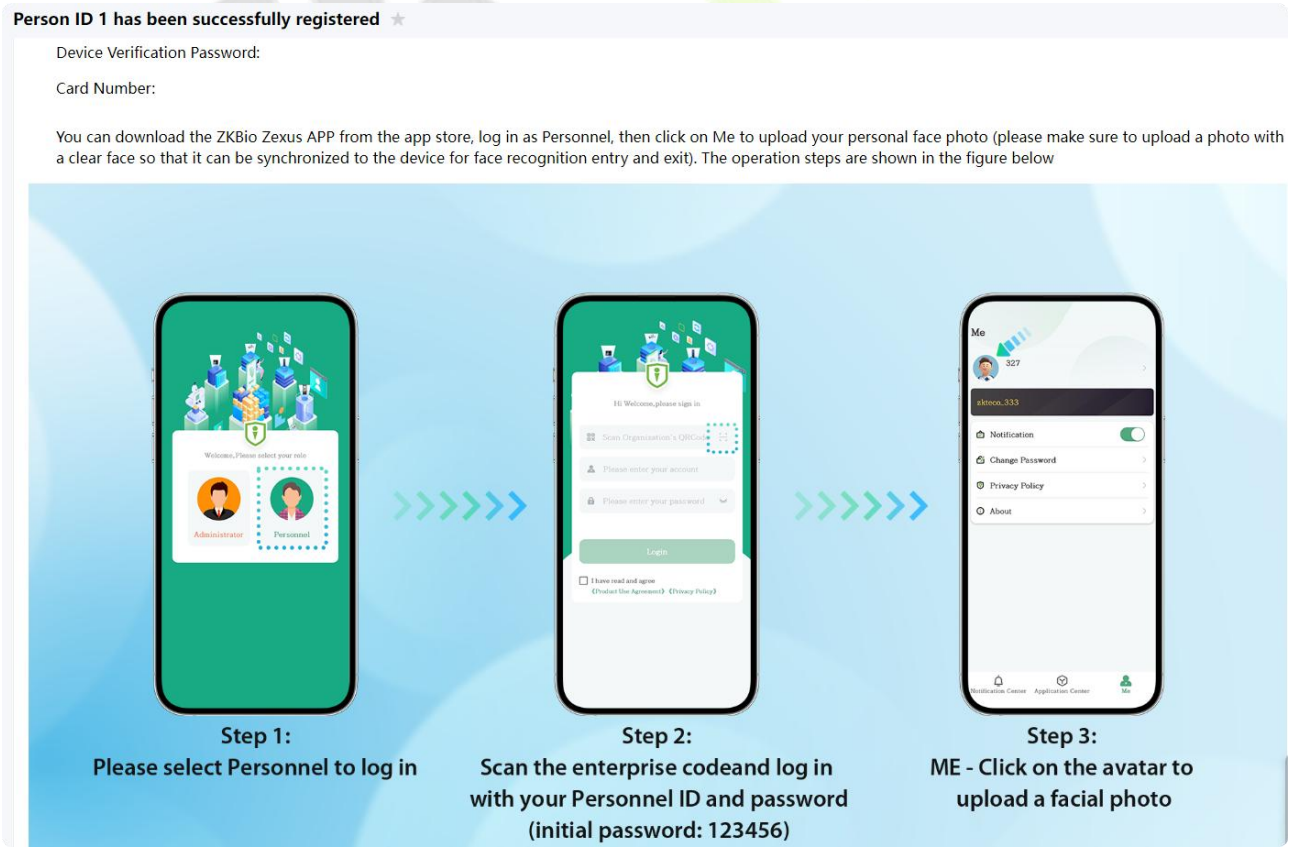


Figure 2- 38

Disable APP Login (V6.1.0 or above supported)

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

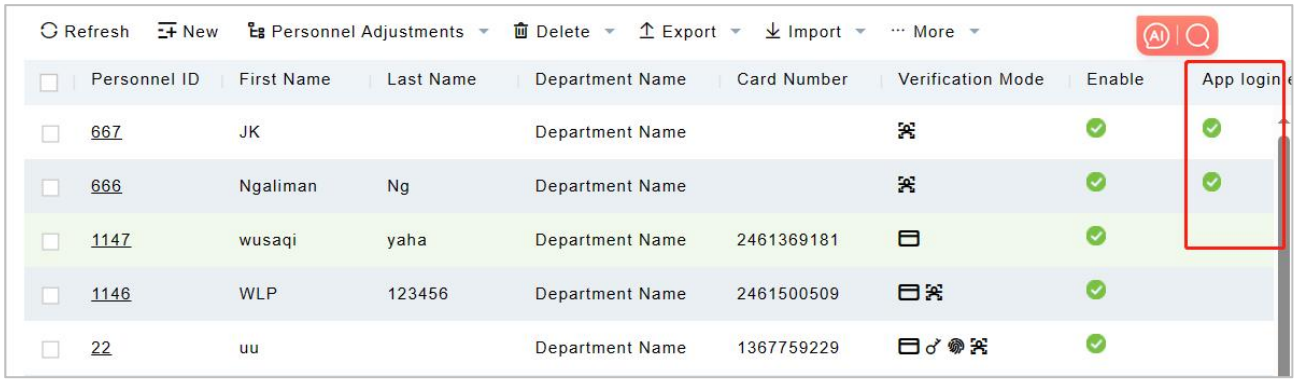


Figure 2- 39

Note: If you need to know how to use the ZKBio CVSecurity APP, please refer to the ZKBio CVSecurity APP.

2.1.2Department

Click **Personnel**, then select 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 (New)**, **Delete**, **Export** and **Import Department.**

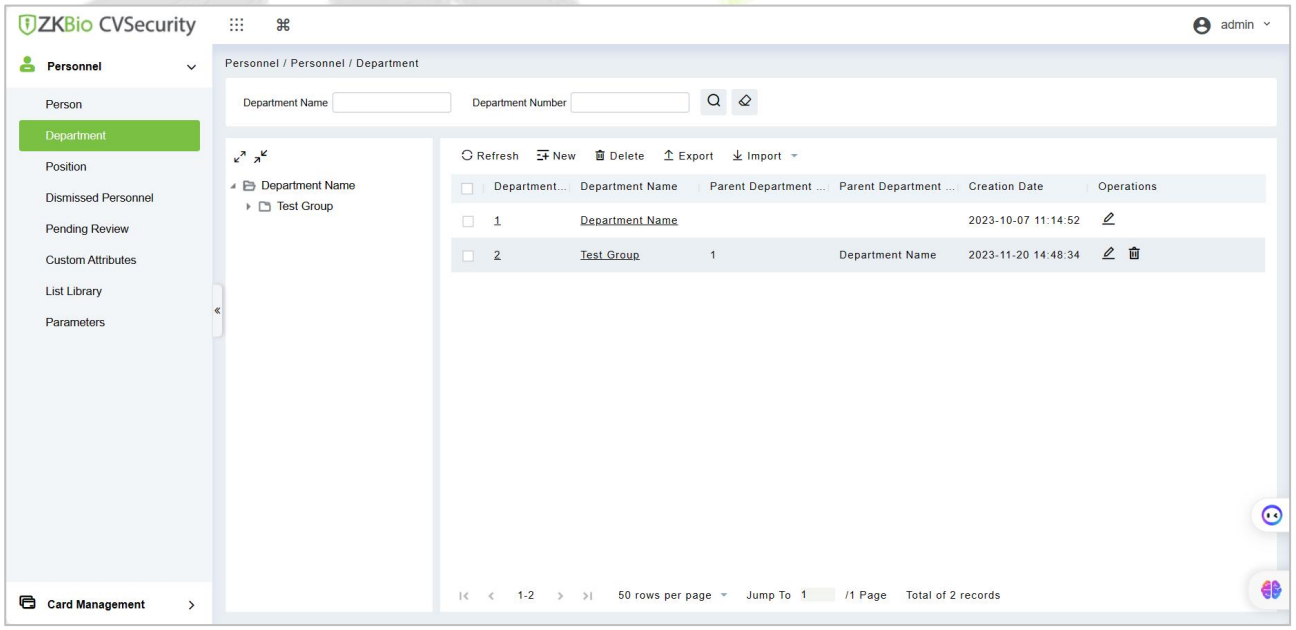


Figure 2- 40

2.1.2.1Add a Department (New)

Introduce the configuration Steps for manually adding a single department in ZKBio CVSecurity.

It is suitable for scenarios where a small number of departmental organizations are added. After most departmental organizations have been created, individual departments can be added individually.

● Steps:

Step 1: In the Personnel module, choose "Personnel Management > Department".

Step 2: Click **Add** with the mouse, and the interface for adding a department will pop up.

Step 3: In the interface of adding a department, fill in the corresponding parameters according to the adding requirements, as shown in figure below. Please refer to Table 2-12 for the description of parameter filling.

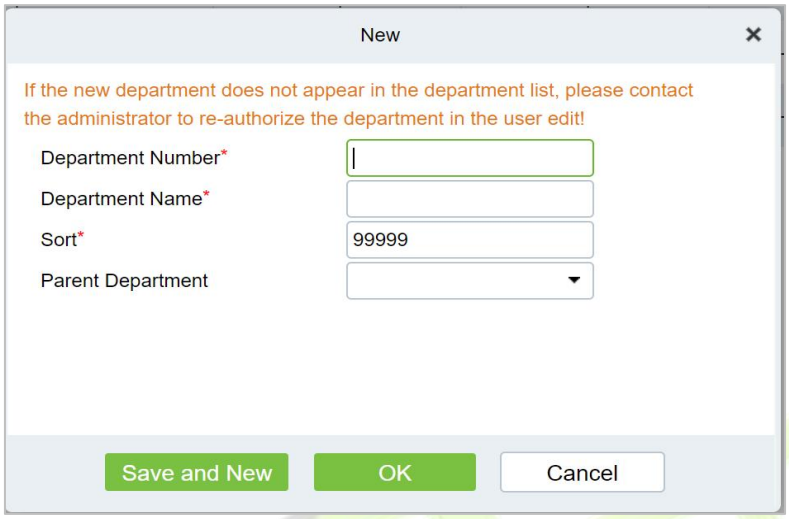


Figure 2- 41 Add Department (New)

● Fields are as follows:

Parameter	Instructions
Department Number	Customize the department number, support letters and numbers.
Department name	Customize the department name.
Sort	Fill in the number of the superior department.
Parent Department	The department name corresponding to the superior department number.

Table 2- 12 Add Department

2.1.2.2Delete

Click **Personnel > Department**, then select Delete.

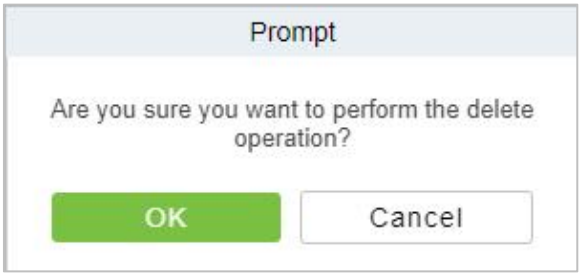


Figure 2- 42 Delete Department

2.1.2.3Export

Click **Personnel > Department**, then select Export.

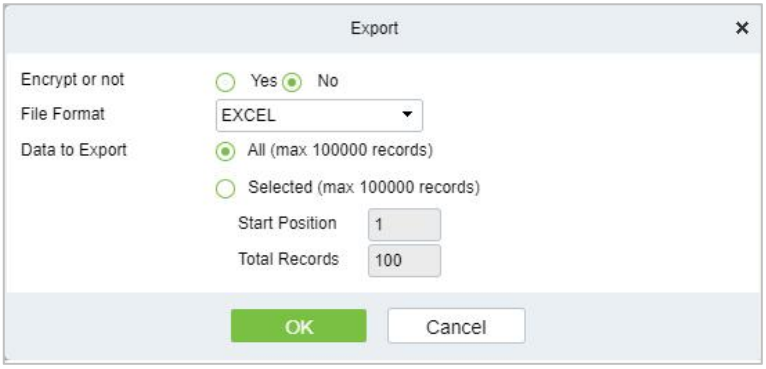


Figure 2- 43 Export Department

2.1.2.4Import

● Import:

Click **Personnel > Department > Import**, then select Import.

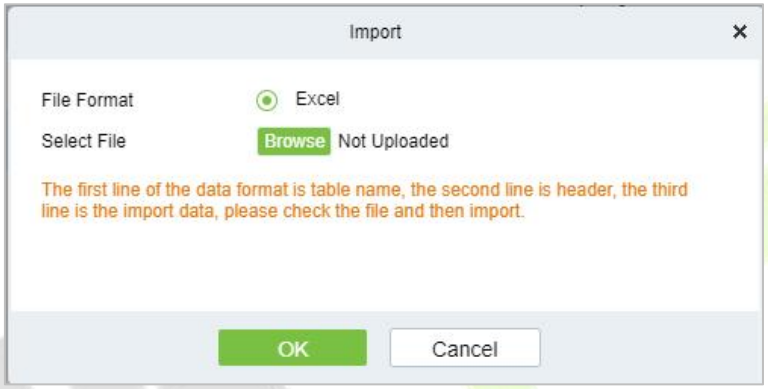


Figure 2- 44 Import Department.

● Download Import Template Department:

Click **Personnel > Department > Import**, then select Download Import Template Department.

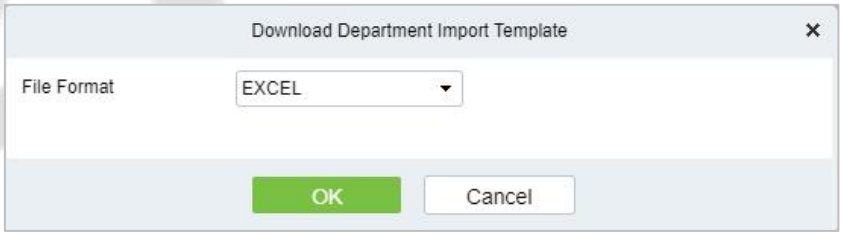


Figure 2- 45 Download Import Template Department

2.1.3Position

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

Click **Personnel**, then select **Position**.

2.1.3.1Add Position

● Steps:

Step 1: In the Personnel >Personnel Management > Position.

Step 2: Click **New (Add Position)**, and the new job interface will pop up.

Step 3: On the new job interface, fill in the corresponding parameters according to the adding requirements, as shown in figure below; please refer to Table 2-13 for parameter filling instructions.

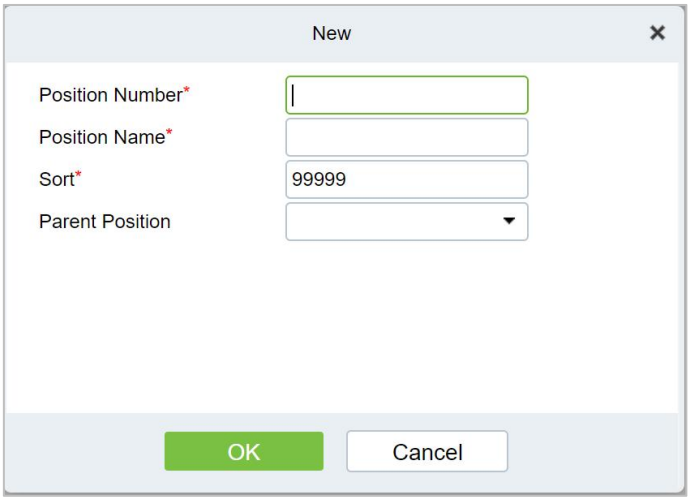


Figure 2- 46 Add Position (New)

● Fields are as follows:

Parameter	Instructions
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.

Table 2- 13 Adding New Position

2.1.3.2Export

Step 1: Click **Personnel** > **Position**, then select Export.

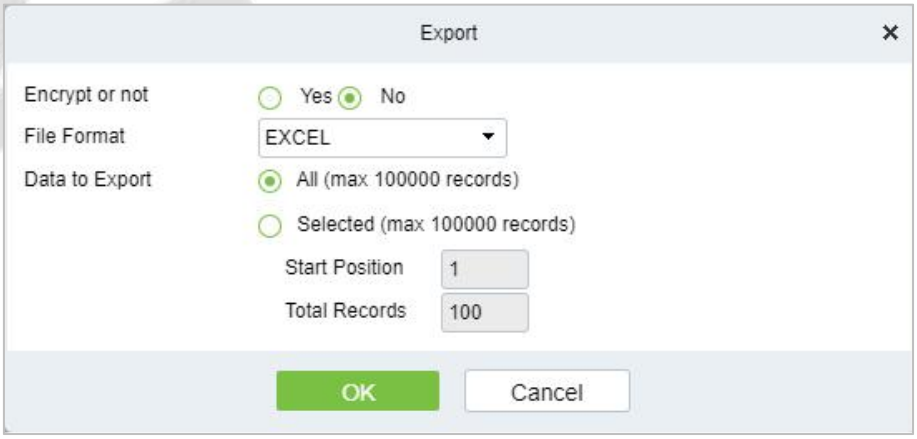


Figure 2- 47 Export Position

Step 2: Click **OK** to save to exit.

2.1.3.3Import

Step 1: Click **Personnel** > **Position** > **Import**, then select Import.

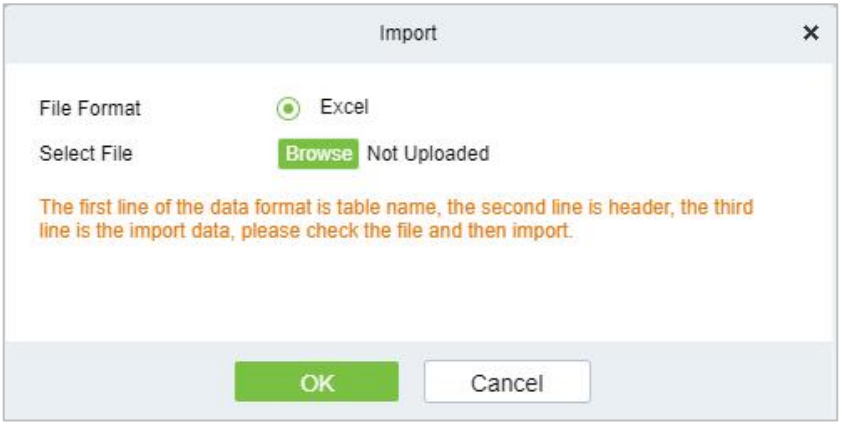


Figure 2- 48 Import Position.

Step 2: Click **OK** to save and exit.

2.1.3.4Delete

Click **Personnel** > **Position**, then click Delete.

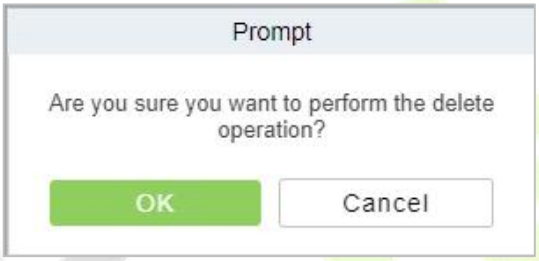


Figure 2- 49 Delete Position

2.1.4Dismissed 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**, then select Dismissed Personnel.

2.1.4.1Delete

Step 1: Click **Personnel** > **Dismissed Personnel**, then select Delete.

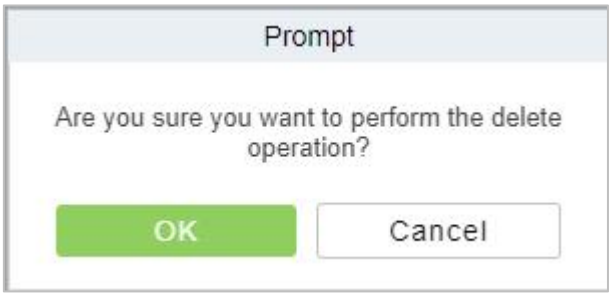


Figure 2- 50 Delete

Step 2: Click **OK** to save and exit.

2.1.4.2Export

Step 1: Click **Personnel** > **Dismissed Personnel**, then select Export.

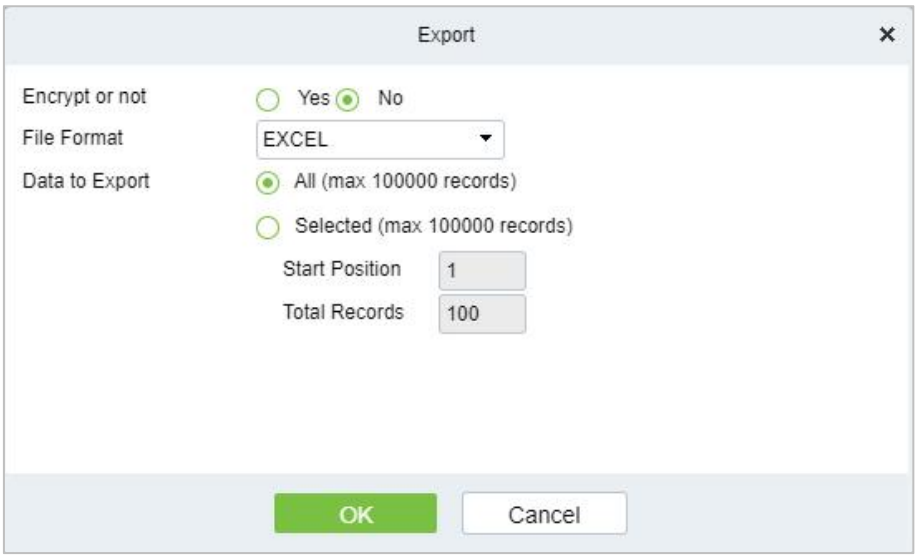


Figure 2- 51 Export

Step 2: Click **OK** to save and exit.

2.1.5Pending Review

2.1.5.1Delete

Step 1: Click **Personnel** > **Pending Review**, then select Delete.

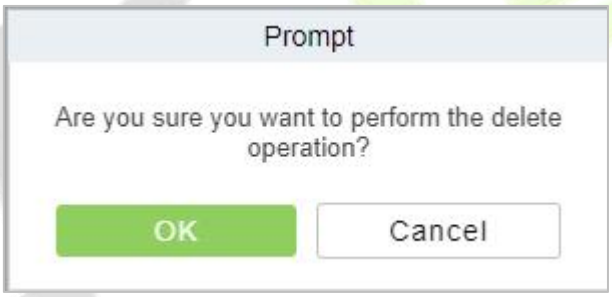


Figure 2- 52 Delete Pending Review

Step 2: Click **OK** to save and exit.

2.1.6Custom 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.

Click **Personnel**, then select Custom Attributes.

2.1.6.1Add Custom Attributes (New)

Step 1: Click **Personnel** > **Custom Attributes**, then select **New** (Custom Attributes).

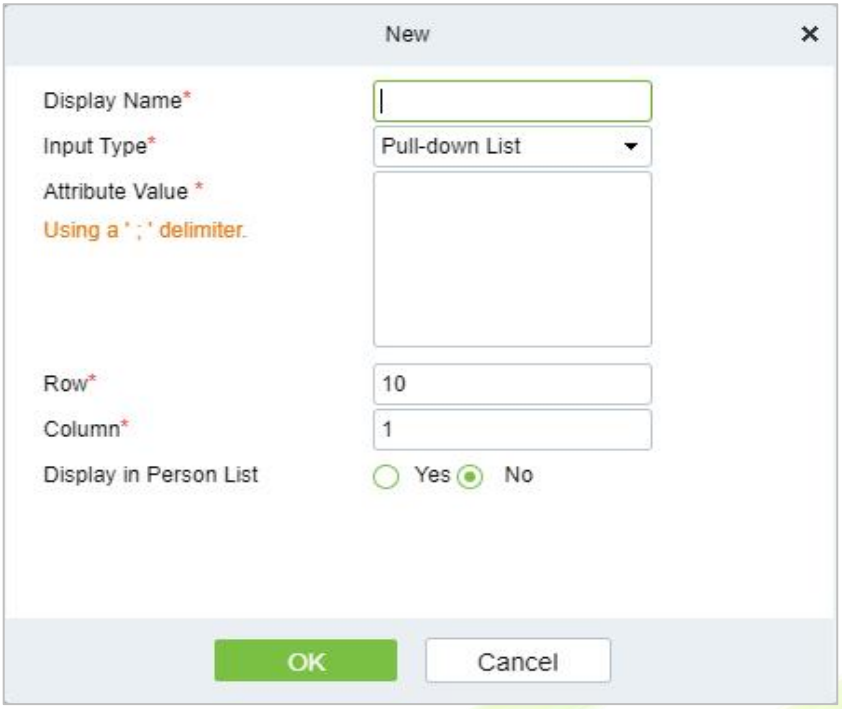


Figure 2- 53 Add Customer Attribute (New)

Fields are as follows:

Parameter	Description
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 cannot exceed 99, and the row number can only be 1 or 2. The combination of the column and row must not be duplicated. As shown in the following figure, Employee Type, is in the first column and first row, and Hire Type is in the first column and second row.

Table 2- 14 Add Customer Attribute (New)

Step 2: Click **OK** to save and exit.

2.1.6.2Delete

Step 1: Click **Personnel > Custom Attributes**, then select Delete.

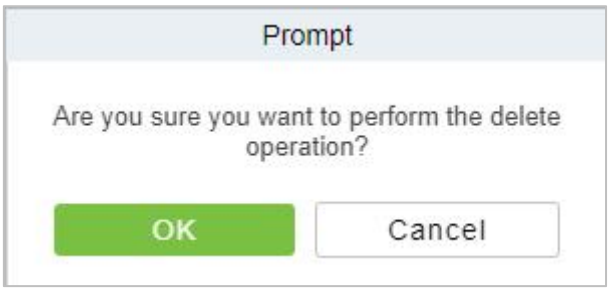


Figure 2- 54 Delete Custom attributes

Step 2: Click **OK** to save and exit.

2.1.7List Library

The list library is mainly used for face matching with face cameras or ZKIVA-Edge.

2.1.7.1Add a List Library (New)

Step 1: Click **Personnel** > **List Library**, then select **New** (List Library).

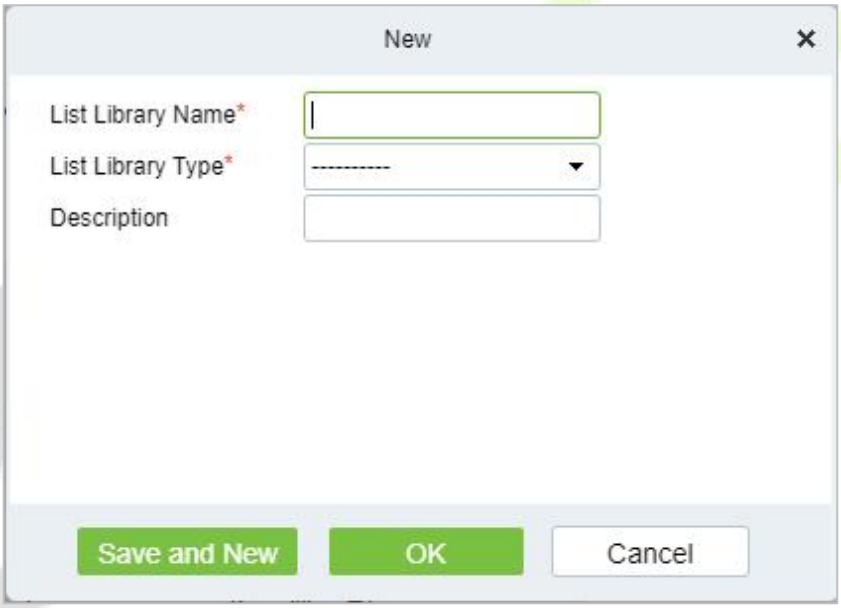


Figure 2- 55 Add List Library (New)

Parameter	Description
List Library Name	The name of list library.
List Library Type	Select type of list library.
Description	Fill Description as required.

Table 2- 15 Add List Library

Step 2: Click **OK** to save and exit.

2.1.7.2Delete

Step 1: Click **Personnel > List Library**, then select Delete.

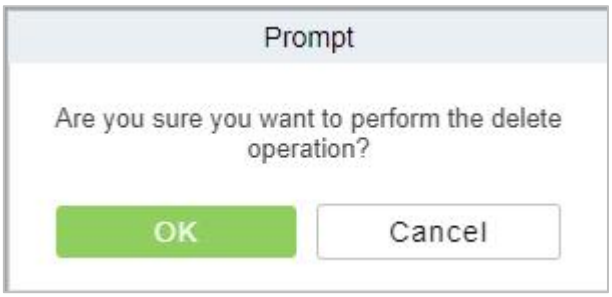


Figure 2- 56 Delete List Library

Step 2: Click **OK** to save and exit.

2.1.8Parameters

In Parameters you can do few settings for options like Personnel ID Setting, Card setting, Pending Personnel Selling, Self-Service registration, Facial Template Extraction Server， and Registration Client.

Click **Personnel > Personnel Management**, then select Parameters.

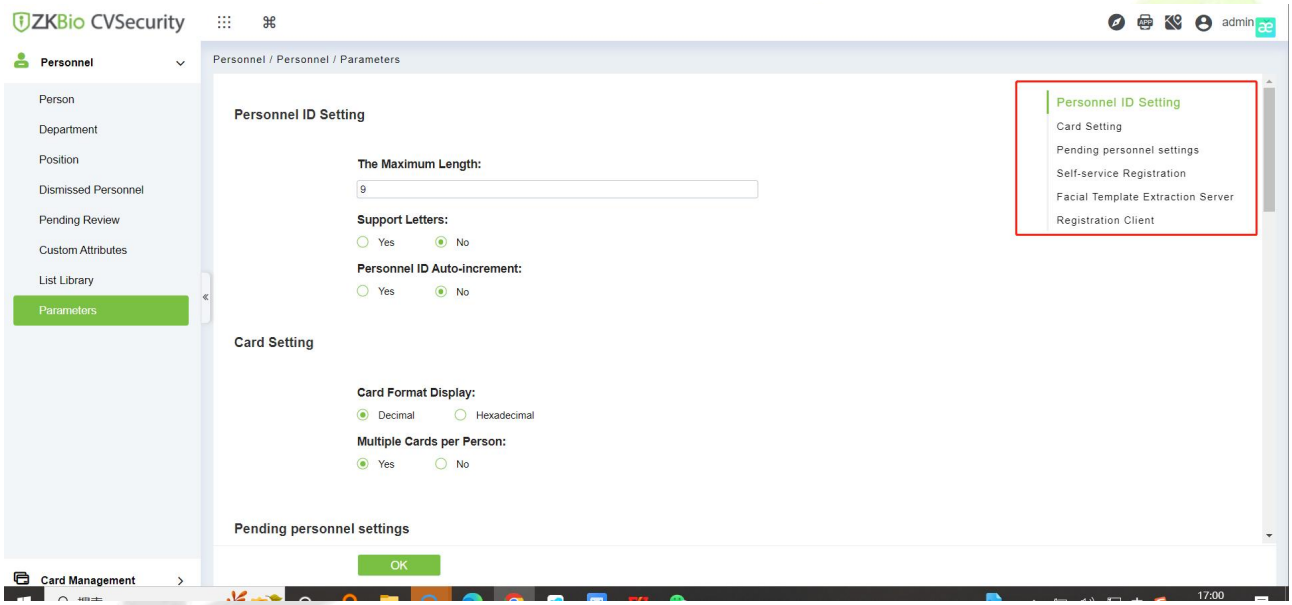


Figure 2- 57 Parameters

2.1.8.1Personnel ID Setting

The maximum length: The Personnel ID supports a maximum length of 23 characters.

Support Letters: When "Yes" is selected, the Personnel ID can include letters.

Personnel ID Auto-increment: When ''Yes'' is selected, the Personnel ID will automatically increment by 1.

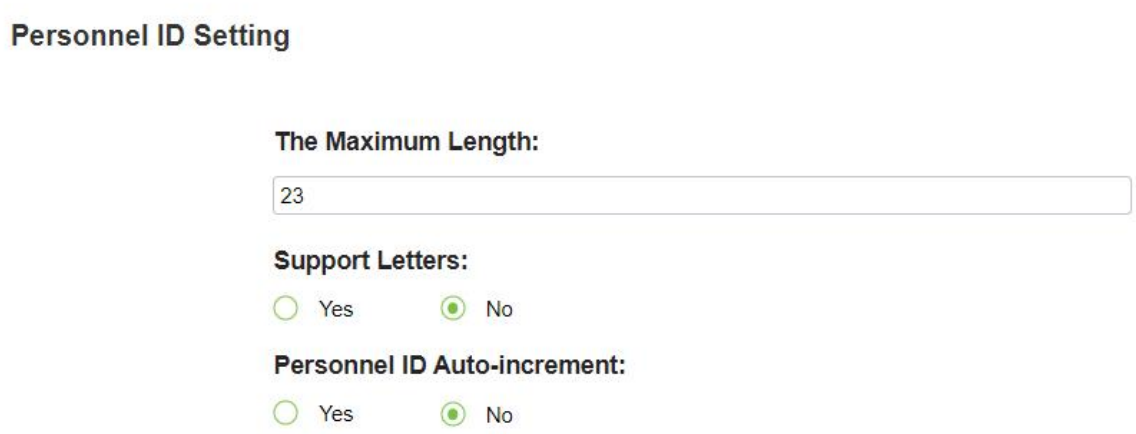


Figure 2- 58 Personnel ID Setting.

2.1.8.2Card Setting

Set **Card Format Display** Select either Decimal or Hexadecimal as the display option.

Multiple Cards per Person: After selecting "Yes," you can register multiple cards for each personnel.

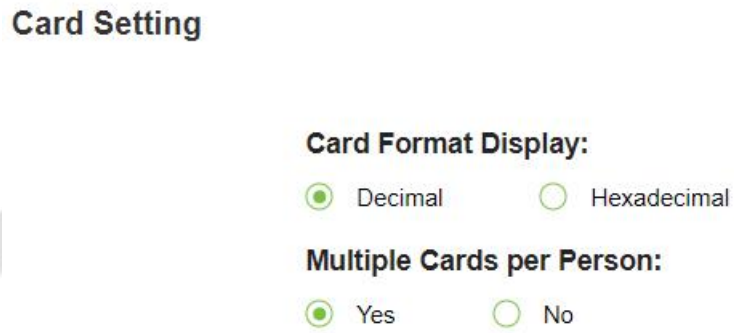


Figure 2- 59 Card Setting

2.1.8.3Pending Personnel Setting

Enable Auto-audit: After selecting **Yes**, the system will automatically approve self-registered personnel.

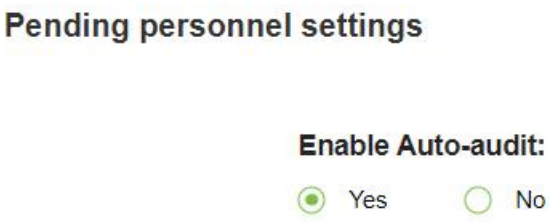


Figure 2- 60 Pending Personnel Selling

2.1.8.4Self Service Registration

Enable Self Registration: After selecting ''Yes'', personnel can scan to self-register their personal information.

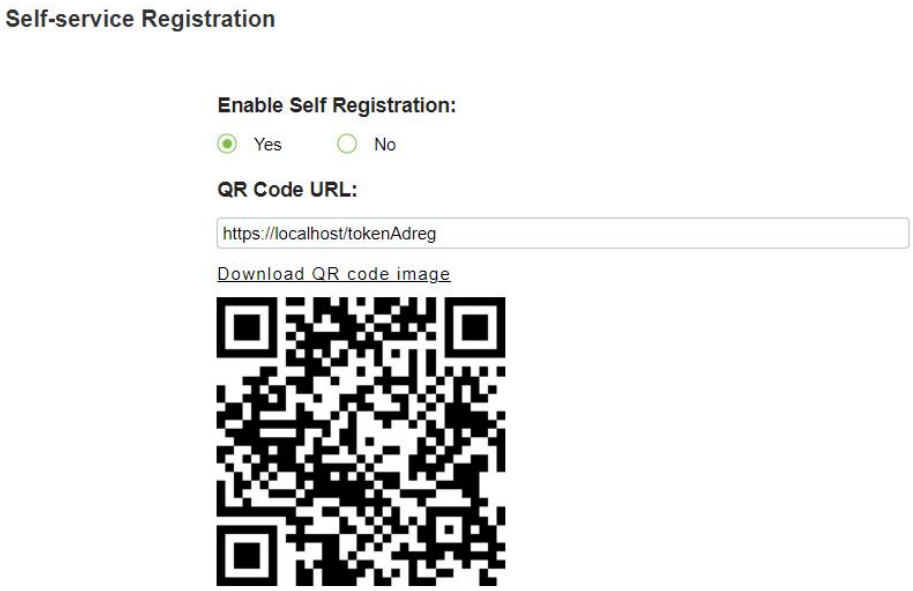


Figure 2- 61 Self Service Registration

2.1.8.5 Personal Sensitive Information Protection

After checking these fields, the corresponding fields under the Personnel menu will be hidden from view.

✍**Note:** In ZKBio CVSecurity version V6.4.0 and later, this feature is adjusted to be configured under the Role menu, allowing for different privacy protections for different user roles.

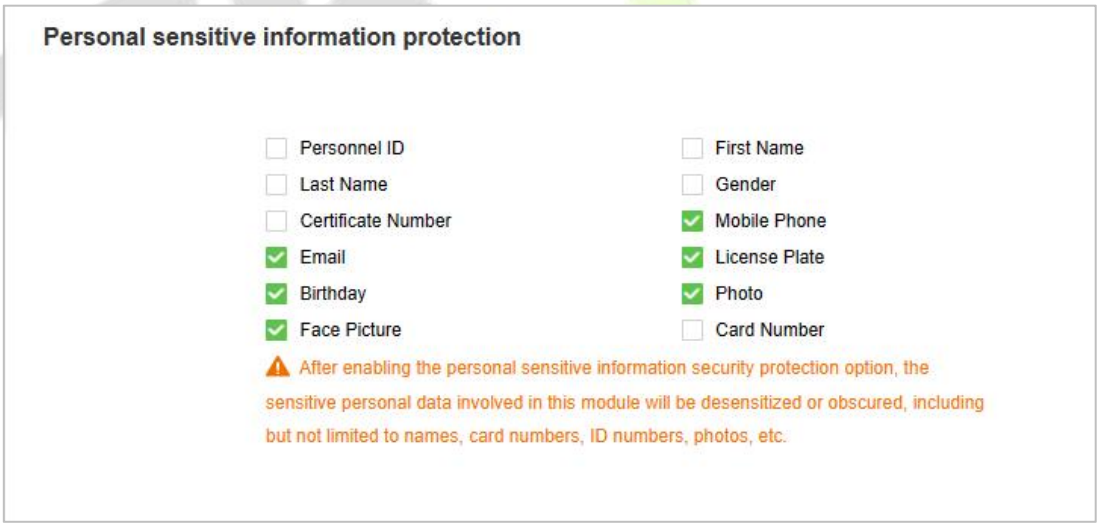


Figure 2- 62 Sensitive Information Protection

2.1.8.6 Facial Template Extraction Server

This feature is applicable to the KF1000 Pro Series. A single KF1000 Pro Reader can be used as an enrollment device. After the enrollment is completed, the facial template can be uploaded to ZKBio CVSecurity and then synchronized for use with the Inbio Pro Plus.

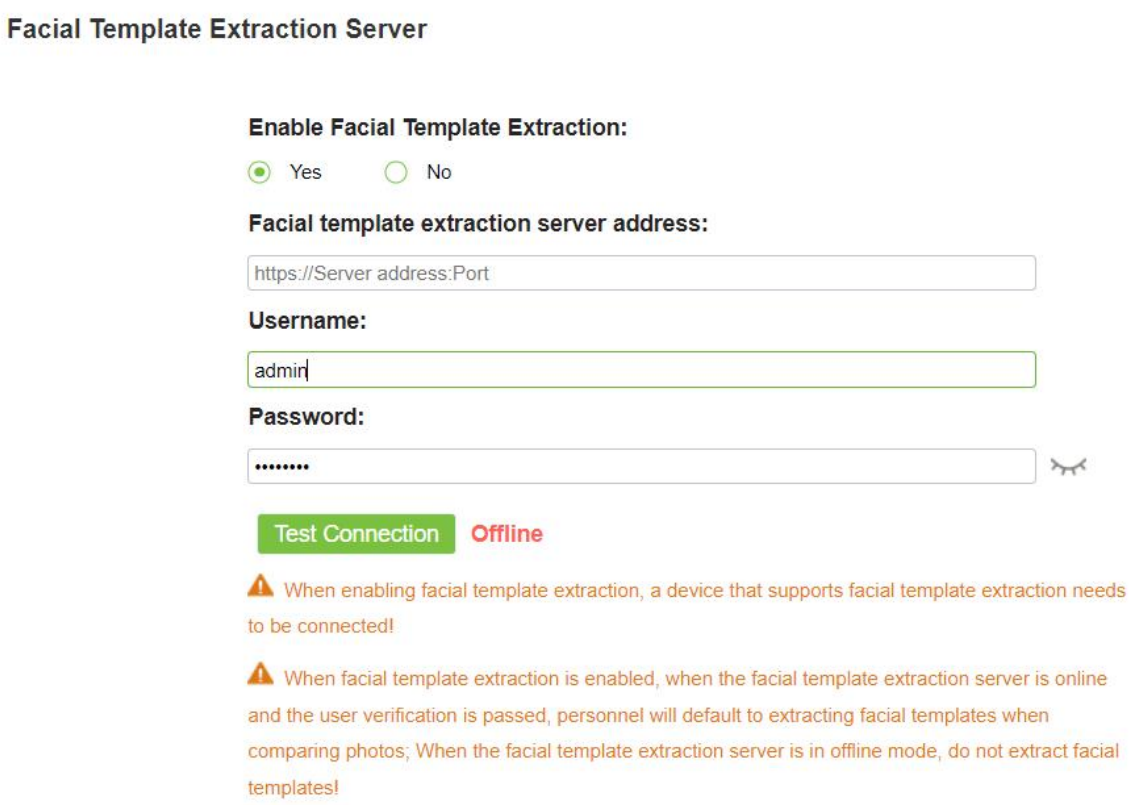


Figure 2- 63 Facial Template Extraction Server

Facial template extraction server address: Enter the server address, the default port number is 8809.

Username: Enter the Webserver user name for the KF1000 Pro series reader.

Password: Enter the Webserver password for the KF1000 Pro series reader.

2.1.8.7Registration Client

●Fields are as follows:

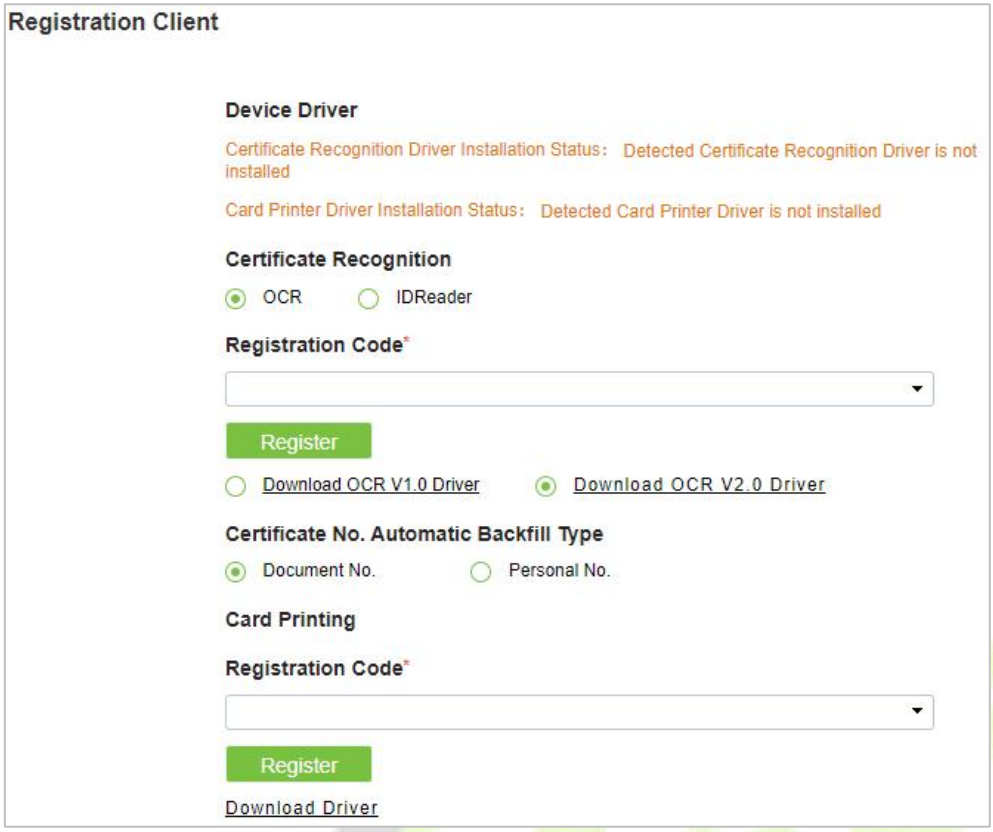


Figure 2- 64 Registration Client

✍Note:

Registration Code: Please make sure you have activated the corresponding license.and then go to **System > Authority Management > Client Register** to got the registration code.

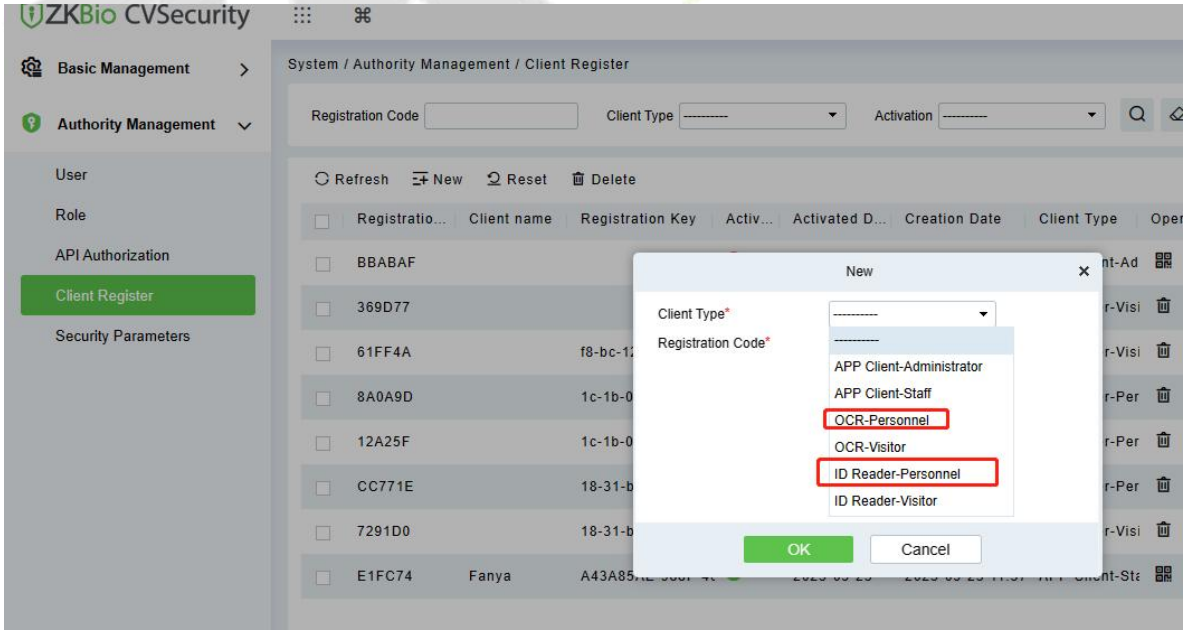


Figure 2- 65 Registration Code

2.2 Card Management

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

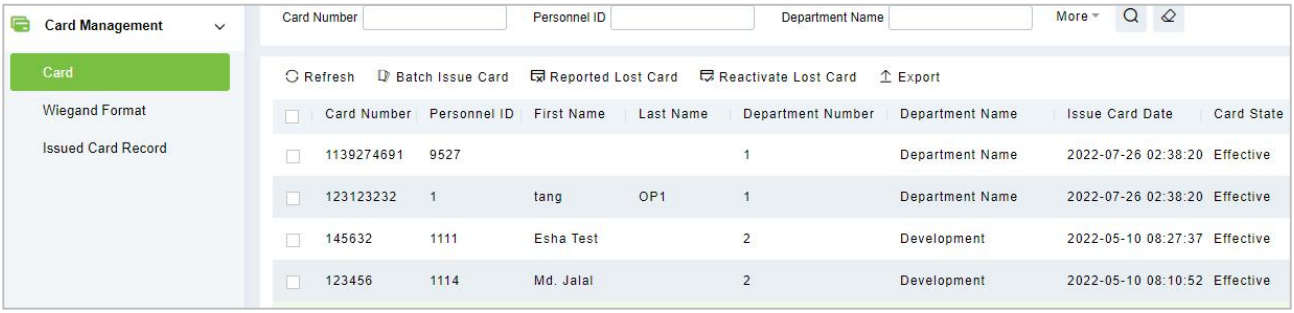


Figure 2- 66 Card Management

2.2.1 Card

2.2.1.1 Batch Issue Card

1. Click **Personnel > Card Management > Card**, then click Batch Issue Card.

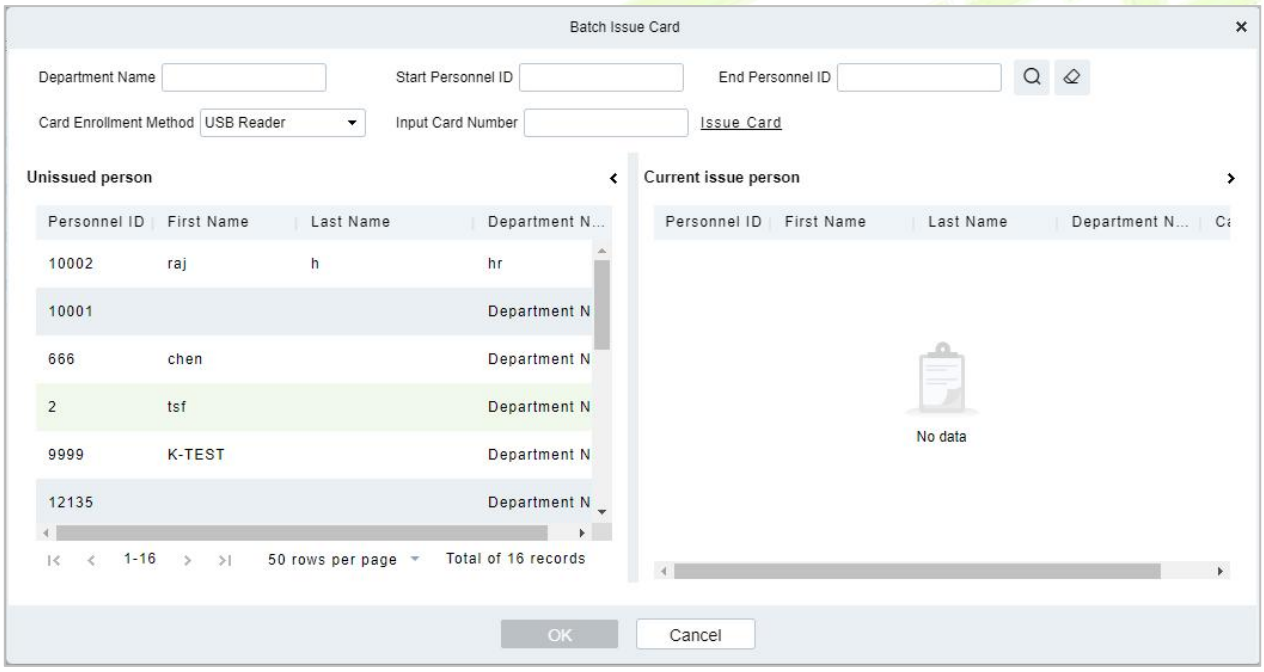


Figure 2- 67 Batch Issue card

2. Fill the fields for Department Name, Start Personnel ID, End Personnel ID, Card Enrollment Method, and Input Card Number.
3. Enter Start and End Personnel No. and click Generate List to generate personnel list and show all personnel without cards within this number series.

✍**Note:** The Start and End Personnel No. only support numbers.

4. Select Card Enrollment Method: Register with a USB Reader or device.

If you want to enroll a card with a USB Reader, you may place the card over the "issue machine" directly. The System will get the card number and issue it to the user in the list on the left.

For the use of device, you need to select the position of punching, click start to read, the system will read the card number automatically, and issue it to the user in the list on the left one by one. After that, click Stop to read.

✍ **Note:** During the Batch Issue Card", system will check whether the card issuer issues card or not, if card has been issued before, the system will prompt "The Card Number has already been issued".

5. Click **OK** to complete card issue and exit.

2.2.1.2 Reported Lost Card

Click **Personnel > Card Management > Card**, then select Reported Lost Card.

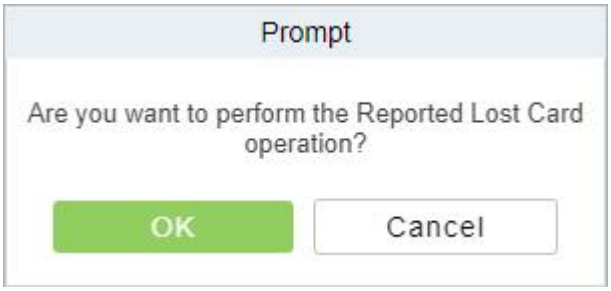


Figure 2- 68 Reported Lost Card

✍ **Note:** Report Lost Card is applicable to all functional modules, not to the offline elevator module. After the report of loss, the status of the card becomes invalid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **Write management card** (**Elevator Device** > **Card** > **Write management card**).

2.2.1.3 Reactive Lost Card

Click **Personnel > Card Management > Card**, then select Reactive Lost Card.

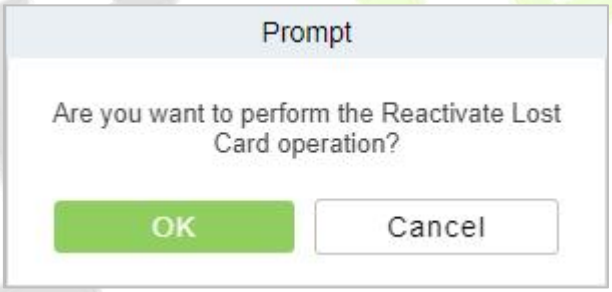


Figure 2- 69 Reactive Lost Card

✍ **Note:** Reactivate Lost Card is applicable to all functional modules, not to the offline elevator module. After reactivating lost card, the status of the card becomes valid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **Write management card** (**Elevator Device** > **Card** > **Write management card**).

2.2.1.4 Export

Step 1: Click **Personnel > Personnel Management > Card Management > Card**, then select Export.

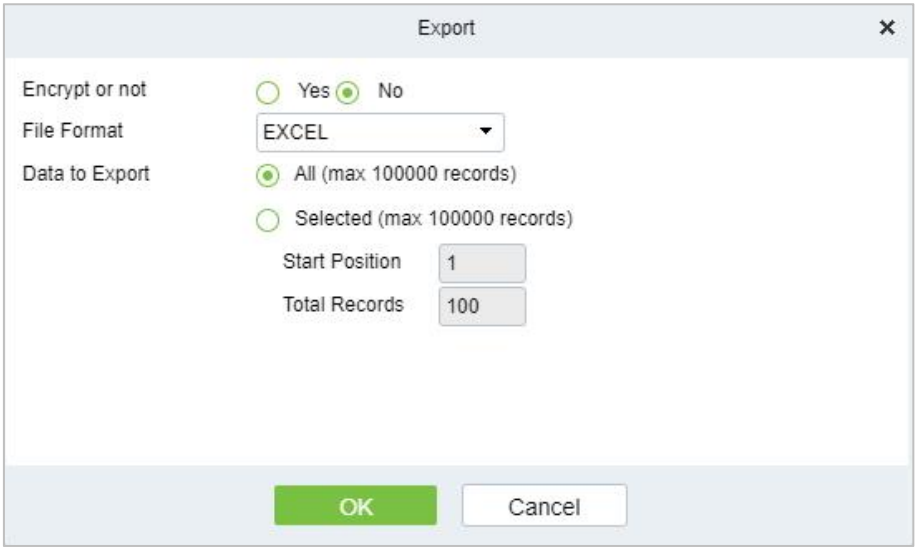


Figure 2- 70 Export

Step 2: Click **OK** to save and exit.

2.2.2Wiegand 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 you needed.

Click **Personnel > Personnel Management > Card Management**, then select Wiegand Format.

2.2.2.1Add Wiegand Format (New)

Click **Personnel > Personnel Management > Card Management > Wiegand format**, then select New (Add Wiegand format).

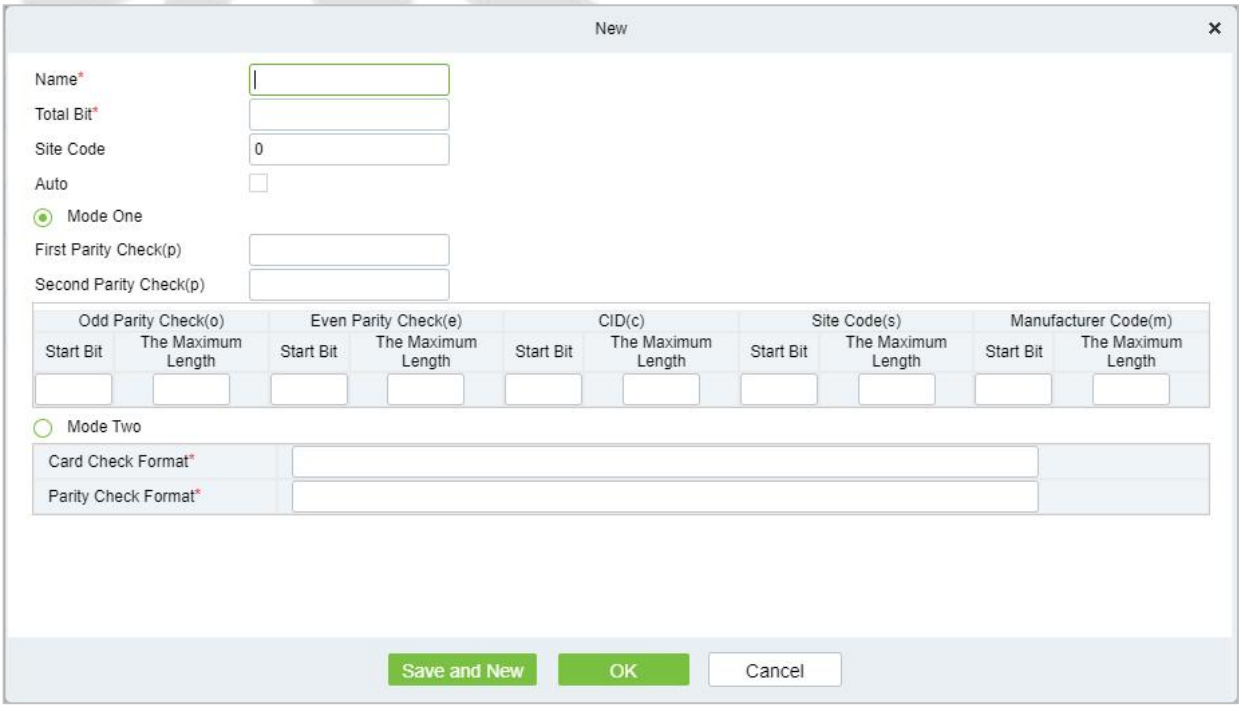


Figure 2- 71 Add Wiegand format (New)

Fields are as follows:

Parameter	Instructions
Name	Enter the Name.
Total Bit	Enter the total bit.
Site Code	Enter the Site code.
Auto	Click if Auto is required.
Mode One	In Mode One Odd Parity Check, Even Parity Check, CID, Site Code, and Manufacturer Code should be set as Start Bit and The Maximum Length.
Mode Two	In Mode Two Card Check format and Parity check Format must be entered.

Table 2- 16 Wiegand Format

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

● Format Specifying:

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

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

✍**Note:**

You can go to **Access > Device > Door ,** select the device and configure the **Wiegand Input Format.**

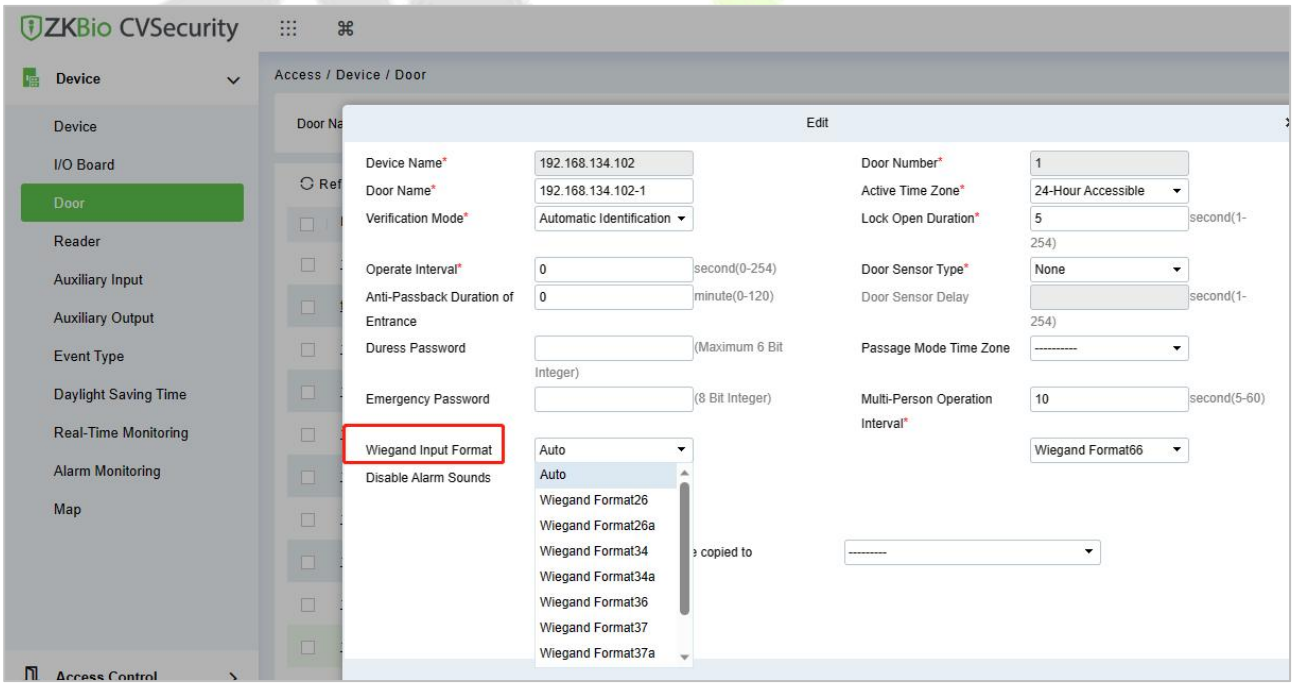


Figure 2- 72 Wiegand Format

2.2.2.2Delete

Click **Personnel > Personnel Management > Card Management > Wiegand Format**, then select Delete.

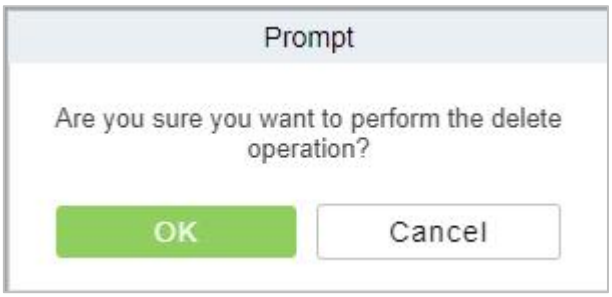


Figure 2- 73 Delete Wiegand Format

2.2.2.3Card Formats Testing

Click **Personnel** > **Personnel Management** > **Card Management** > **Wiegand Format**, then select Card format Testing.

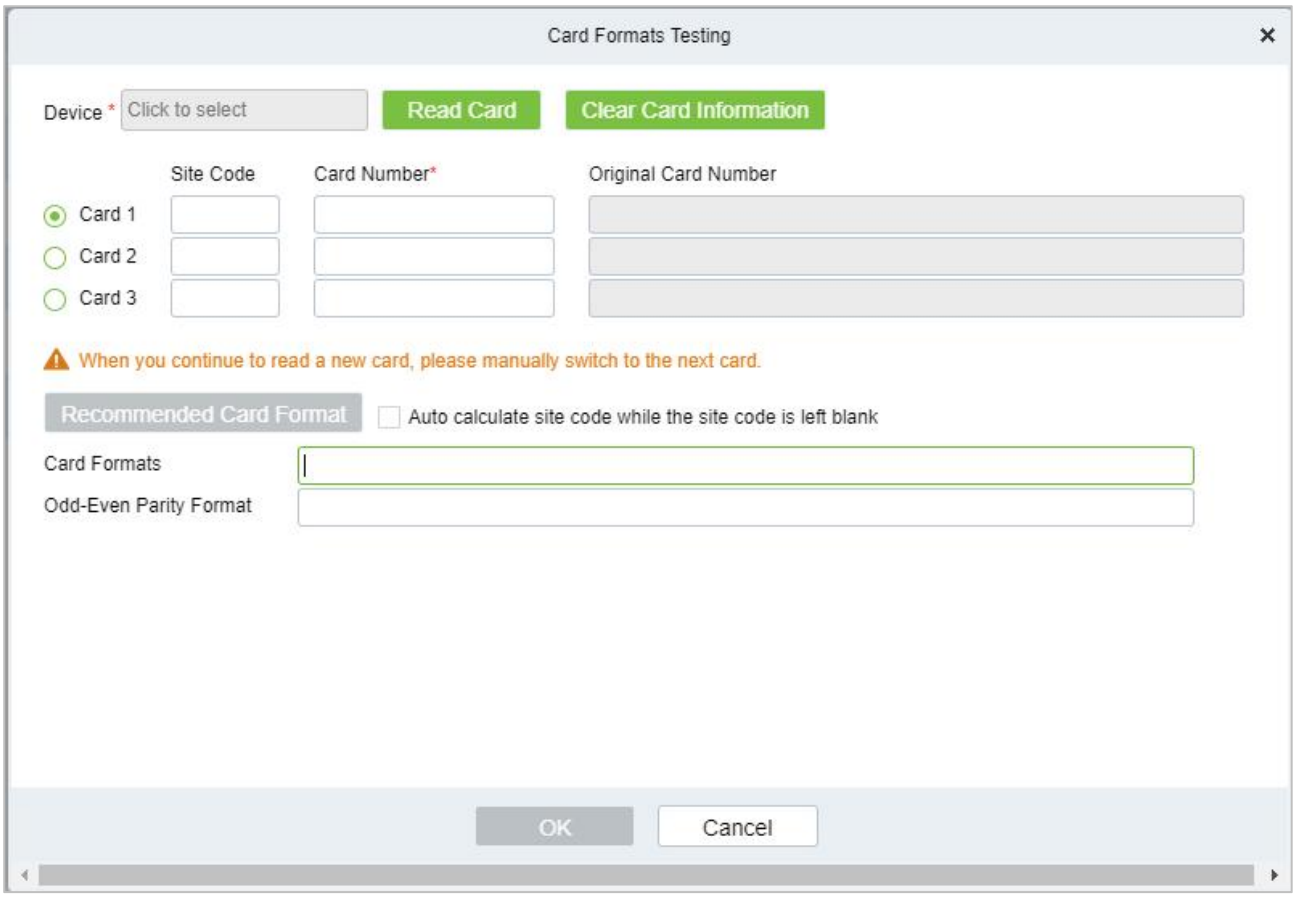


Figure 2- 74 Card Formats Testing

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

Select the device that supports the card format test function, and fill the card number and the site code (optional):

● Steps:

Click **Read Card** and swipe the card on the reader. The original card number will be displayed on the **Original Card Number** text box.

Click **Recommended Card Format** and the recommended Wiegand card format will be displayed below.

Click **Auto calculate site code while the site code is left bank** and the software will calculate the site

code according to the card format and card number.

Click **OK** and the page will jump to the Wiegand format page to save the new Wiegand format.

✍**Note:** The card format testing function is only supported by few devices.

2.2.3Issue Card Record

Click **Personnel > Personnel Management > Card Management**, then select Issue Card Record.

2.2.3.1Export

Step 1: Click Personnel > Personnel Management > Card Management > Issue Card Record, then select Export.

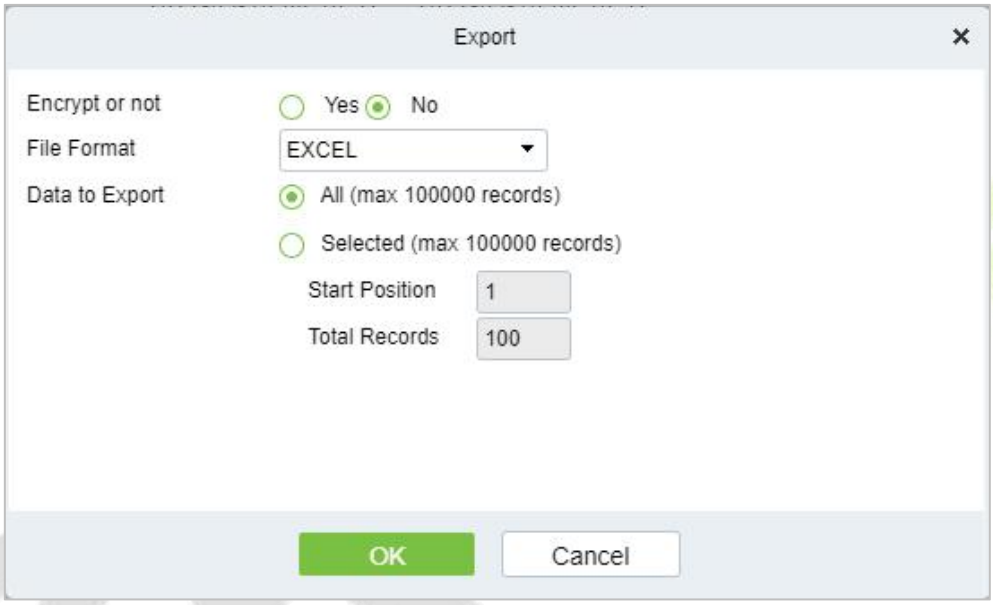


Figure 2- 75 Issue Card Record

Step 2: Click **OK** to save and exit.

3 Access Control

3.1 Operation Scenario

The **Access Control** module is used as the entry and exit management of pedestrians. Through the configuration of access control equipment and permission groups, unified management of entry and exit of people is realized. The most fundamental problem to solve is to control who uses what media to enter and exit which door at what time.

3.2 Operation Process

This section describes the configuration process of the **Access Control** module service.

The **Access Control** module service configuration process is shown in Figure 3-1.

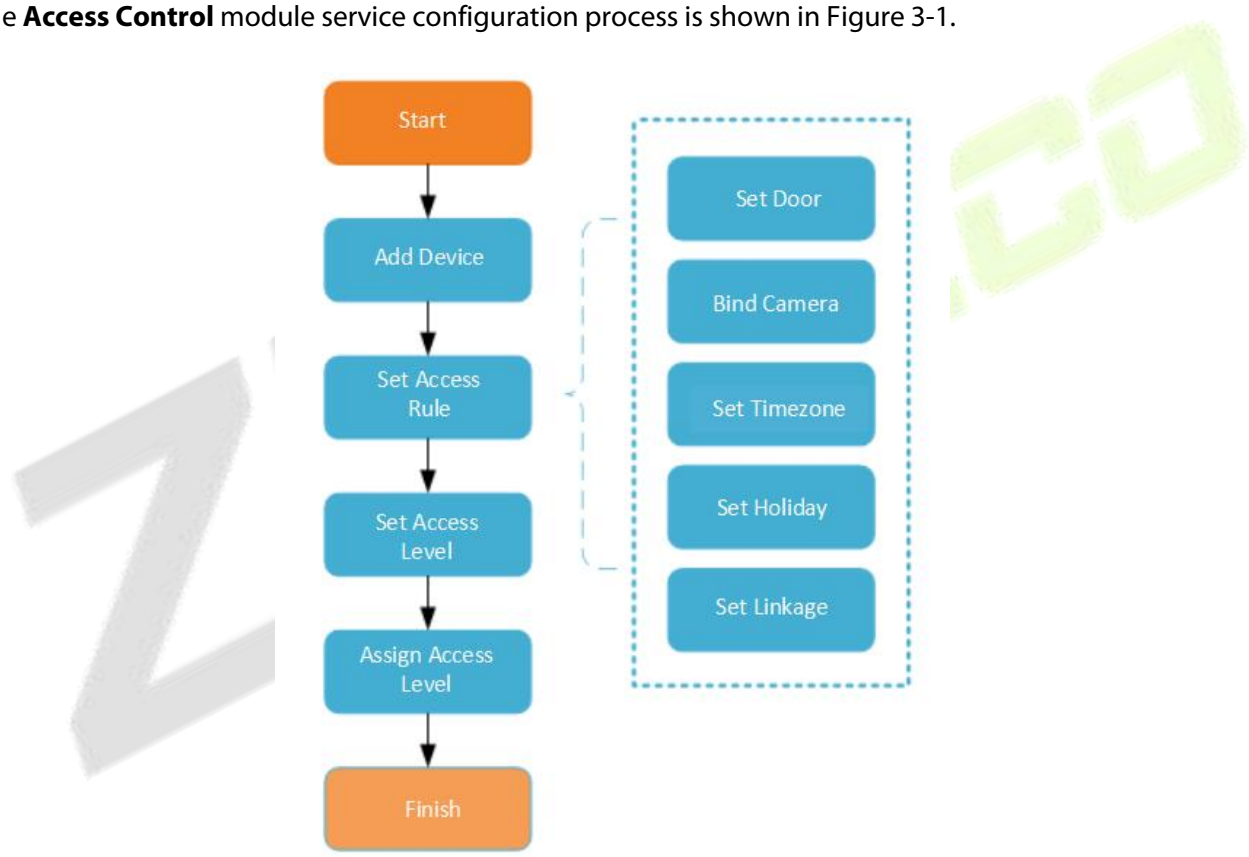


Figure 3- 1 Access Control Configuration Process

3.3 Device Management

3.3.1 Device

Introduce the configuration Steps of searching and adding access control devices in ZKBio CVSecurity.

Through the search method, the access control devices that have been set to point to the server can be found, and the access control devices that have been searched can be added directly, which is convenient to operate.

● Preconditions:

1. Before adding the **Access Control** device, perform IP allocation settings.
2. The device needs to set the server address in advance before searching and adding. The configuration Steps for the server are as follows:

a. In the access control device that has been connected to the power supply and the network, set it directly on the device screen.

b. Select and click "Main Menu > Communication Equipment > Network Management Platform or Cloud Server Settings"

c. Set the IP address and port of the current server, that is, the IP address and port of the current ZKBio CVSecurity server and complete the configuration to the server.

3.3.1.1 Add Devices (New)

● Steps:

Step 1: In the Access Control module, select "Device > Access Control Device".

Step 2: On the device interface, click the “search" button to pop up a search box.

Step 3: Click “start **Search**" in the search box to display the **access control devices** that can be added, as shown in Figure 3-2.

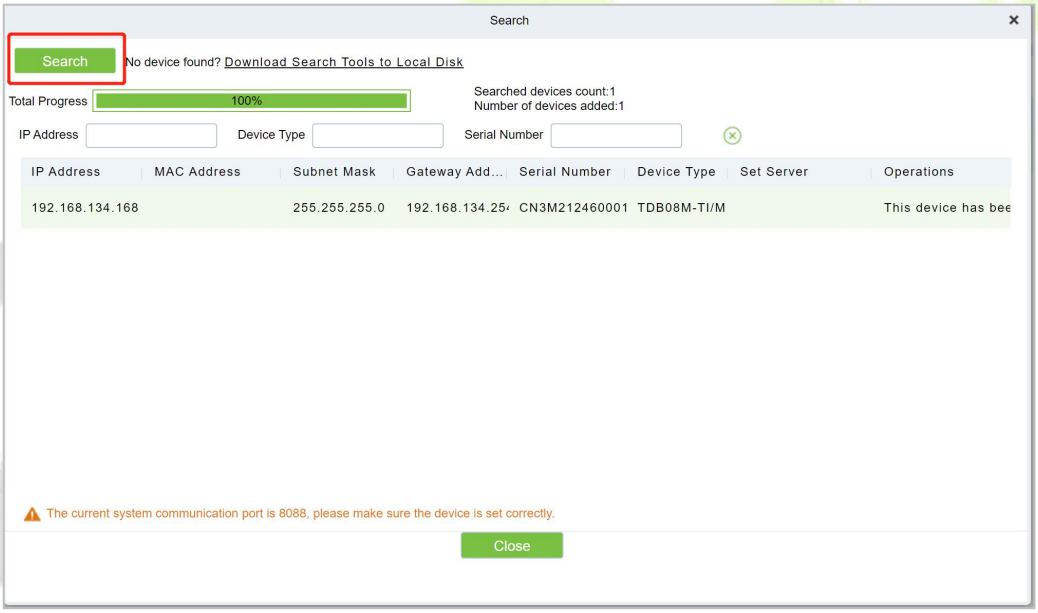


Figure 3- 2 Device Search and Add Interface

Step 4: Optional: Modify the IP address of the **Access Control** device, click "**Modify IP Address**", the device will be restarted after modifying the IP address, and the IP address modification will be completed after the restart.

Step 5: For the searched access control devices, click the **Add** button in the operation bar to add the device; the device addition settings are shown in Figure 3-3, and the parameter settings are described in Table 3-1.

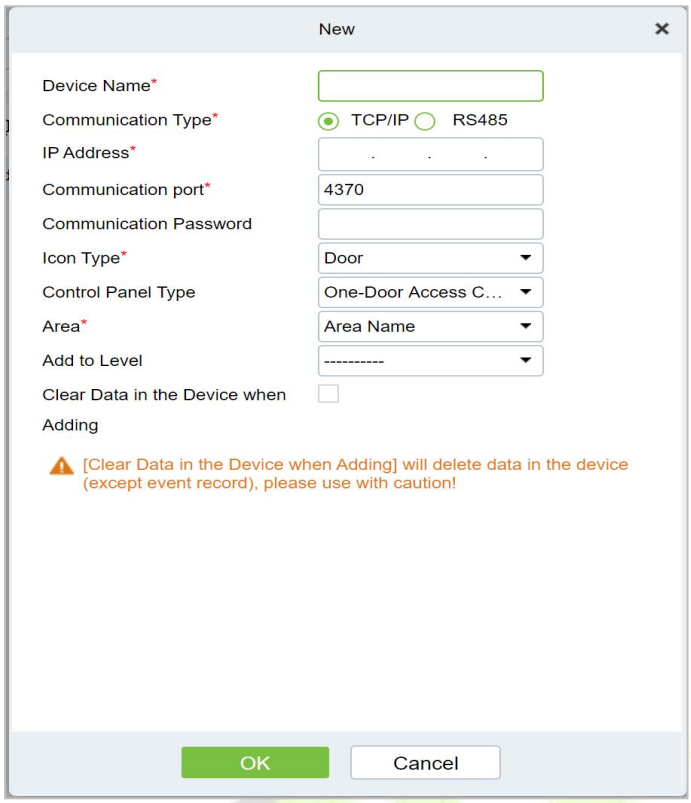


Figure 3- 3 Device Add Interface

Parameter	How to set
Device Name	Customize the name of the device.
New Server Address/Port	Set the IP address and communication port of the system to be used (the default communication port is 8088).
Communication Password	Fill in the communication password of the device. If there is no password, you do not need to fill in it. You can add it only after the verification is successful. For new factory equipment and initialized equipment, the communication password is empty. In order to ensure that the device is not used by others, users can enter the device IP address through the web page to enter the background to customize the device verification password.
Icon Type	Select the icon display type of the real-time monitoring interface: Door,Parking Barrier,Flap Barrier.
Area	Divide the device into regions and select the region to which the device belongs.
Add To Permission Group	The device is automatically added to the selected permission group.
Delete Data From Device When Adding	Set whether the original **Access Control** data in the device will be automatically cleared after the device is added.

Table 3- 1 Parameter setting

Step 6: Click **OK** to complete the operation of adding access control devices. After the operation is completed, the device will restart, and the device will be added after the restart is complete.

Step 7: Click **Close** to close the device search and add interface.

3.3.1.2Delete

Select device, click **Delete**, and click **OK** to delete the device.

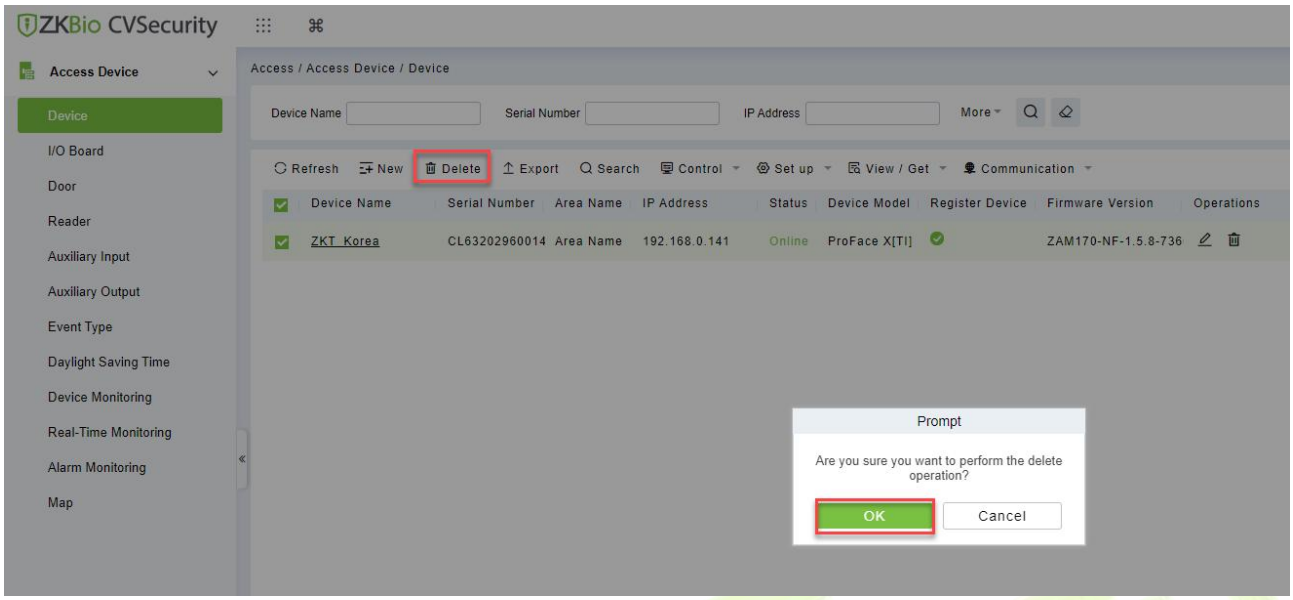


Figure 3- 4 Device Add Interface

3.3.1.3Export

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

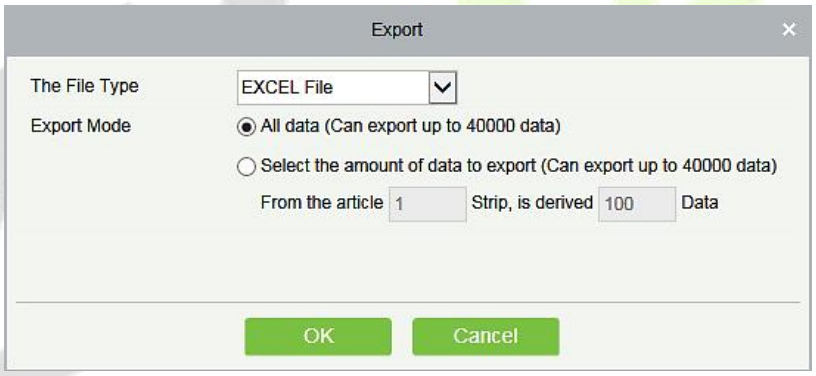


Figure 3- 5 Export

ZKTECO
Device

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

Figure 3- 6 Export

3.3.1.4Control

- **Clear Administration Permission**

This function allows for the online removal of the administrator rights of the device, which is used to solve the problem of forgetting the administrator password.

- **Clear Command**

The command to clear the cache

Upgrade Firmware

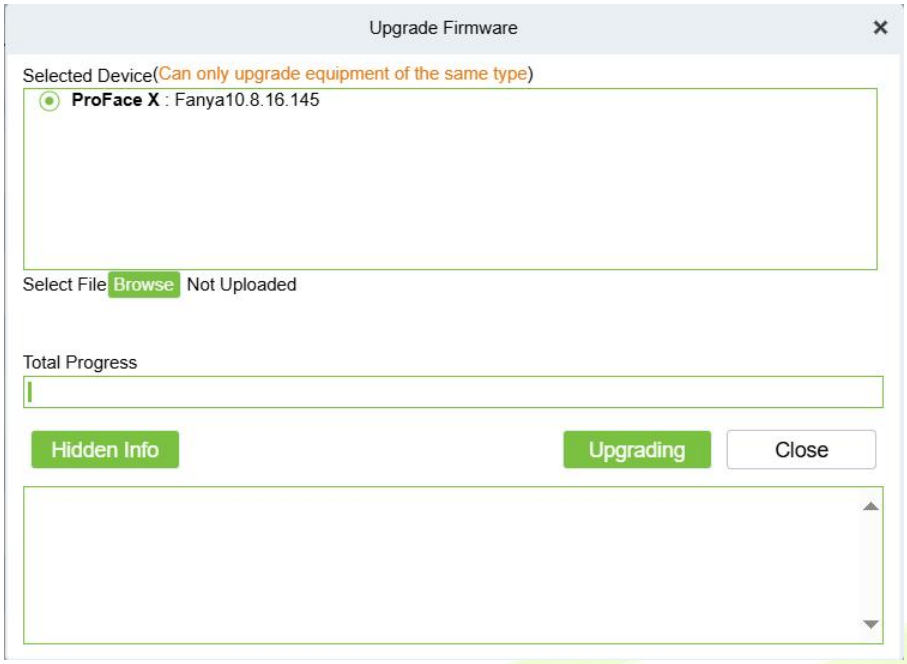


Figure 3- 7 Upgrade Firmware

Tick the device that needs to be upgraded, click **Upgrade firmware** to enter edit interface, then click **Browse** 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. Unauthorized upgrade may affect normal operations.

Reboot Device

It will reboot the selected device.

Synchronize Time

It will synchronize device time with server's current time.

Disable/Enable

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

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.

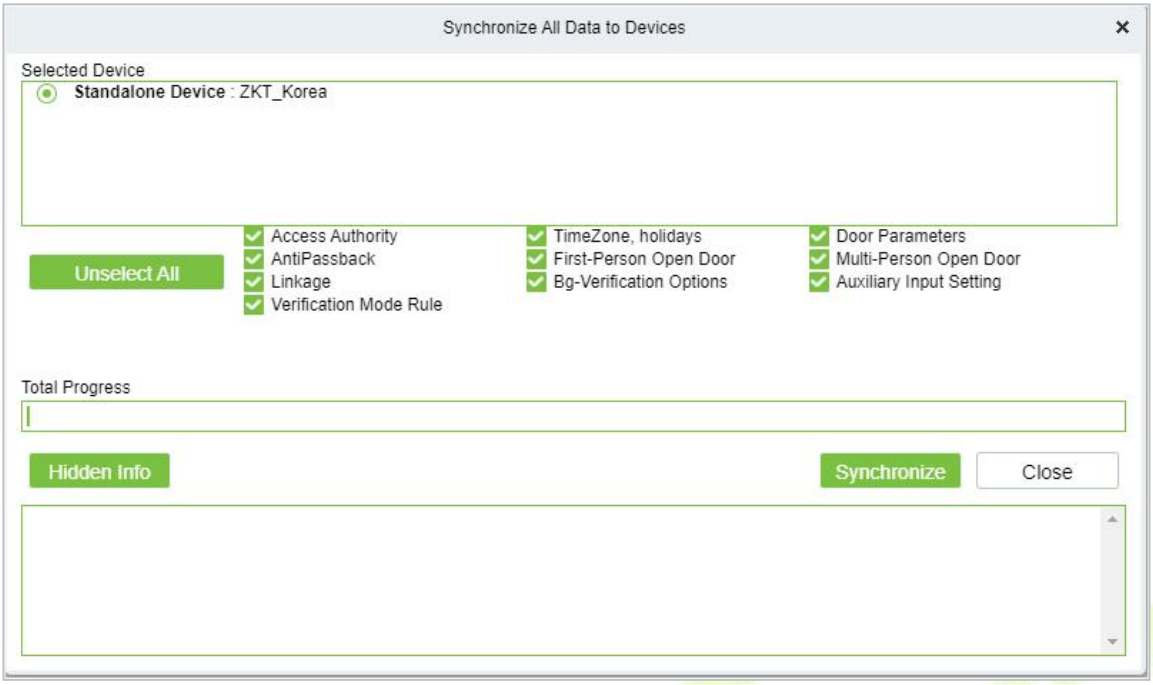


Figure 3- 8 Synchronize All Data to Devices

✍**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.

3.3.1.5Set Up

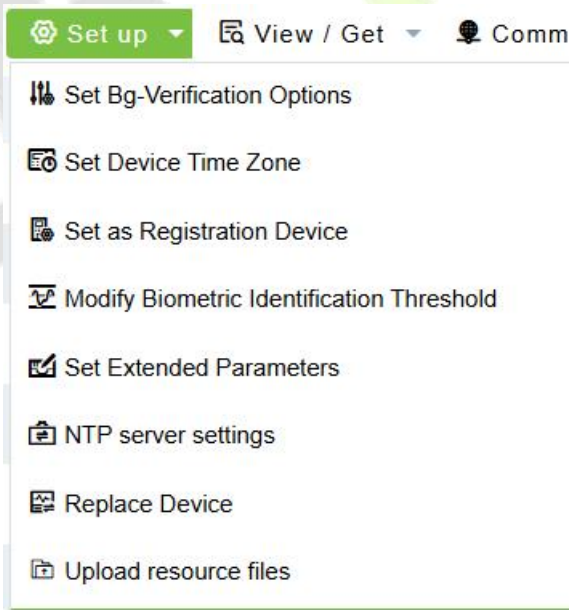


Figure 3- 9 Setup

● Set Background Verification Parameters:

Select the required online device; click **More** > **Set Bg-verification parameters**.

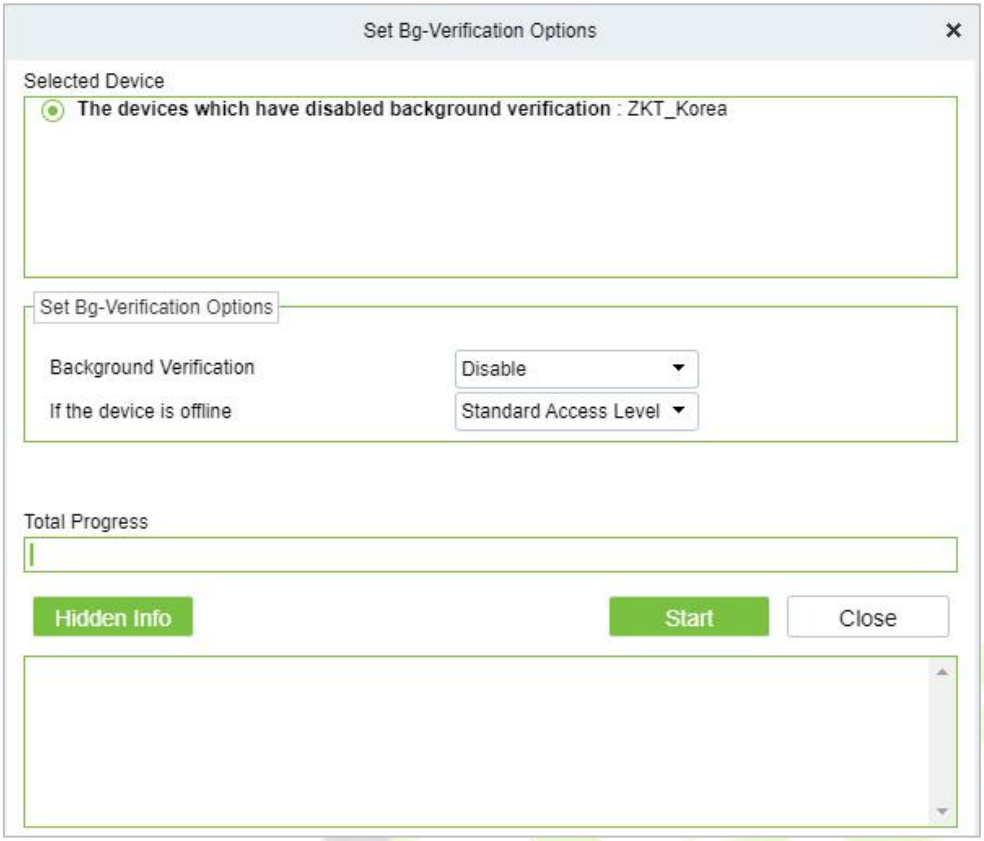


Figure 3- 10 Set Bg-Verification Parameters

Background verification: Enable or Disable Background verification function.

If the device is offline: If the controller is offline, the device has levels of Standard Access Level or Access Denied.

After setting parameters, click **Start** button to issue command to the device setting.

✍ **Note:** If you need advanced access control functions, please enable Background verification, and issue the background verification parameters to the device.

● 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.

Modify the Fingerprint Identification Threshold (Ensure that the access controller supports fingerprint function)

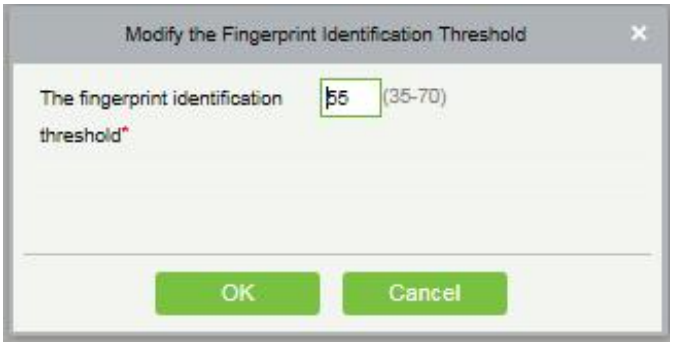


Figure 3- 11 Modify the Fingerprint Identification Threshold

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 thresholds devices list. More than one device can be changed by using Batch operation function.

Set the Registration device

Set the registration device only when the standalone device's data such as personnel can automatically upload.

Figure 3- 12 Set the Registration device

Modify Biometric Identification Threshold

Configure the fingerprint recognition threshold of the device online.

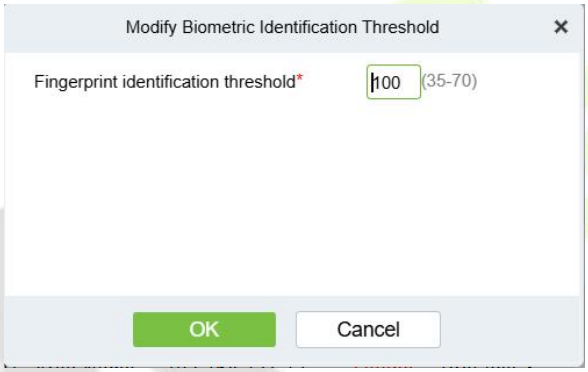


Figure 3- 13 Biometric Threshold

Set Extended Parameters

The relevant parameters of the face recognition device can be configured online.

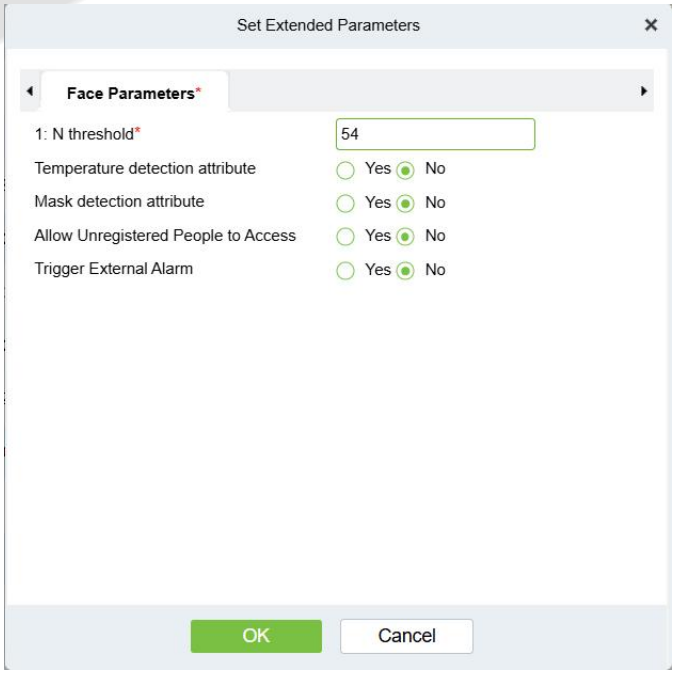


Figure 3- 14 Extended Parameters

If the device does not support face recognition or this parameter, the following prompt will pop up.

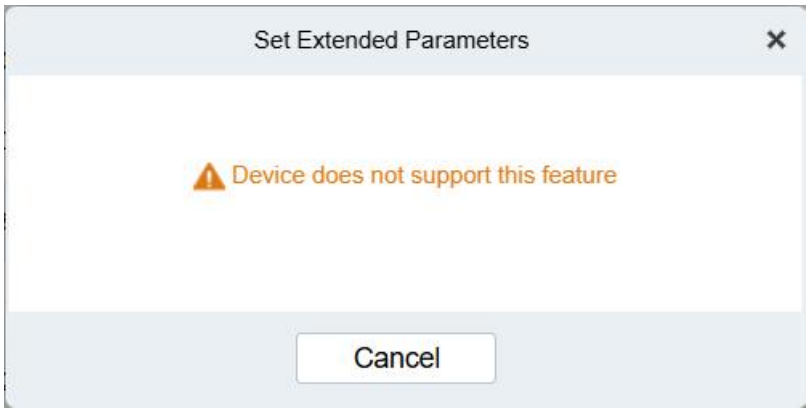


Figure 3- 15 Extended Parameters

● NTP Server Setting

If you need to ensure the accuracy and consistency of time synchronization, you can configure the NTP service here. This function is only supported by the controller .

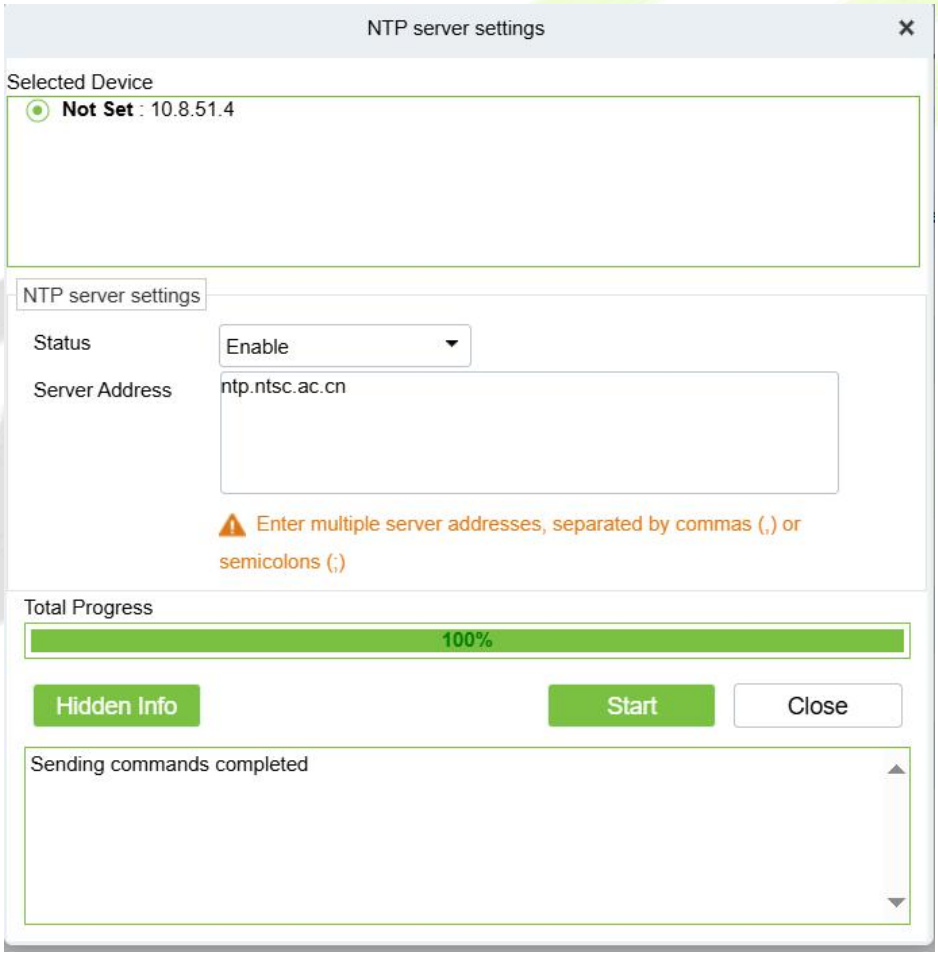


Figure 3- 16 NTP Server

● Device Replacement

Introduce the configuration Steps for replacing access control devices in ZKBio CVSecurity.

When a device is unavailable, we can quickly add a new device and synchronize all configurations from

faulty device to the new device by simply entering the serial number of the replaced device.

Step 1: Go to the **Access** > **Access Device**, select the unavailable device.

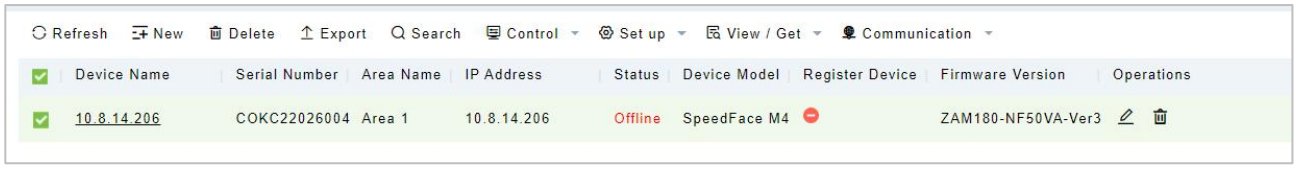


Figure 3- 17 Select the Unavailable Device

Step2: Click **Set up > Replace Device**.

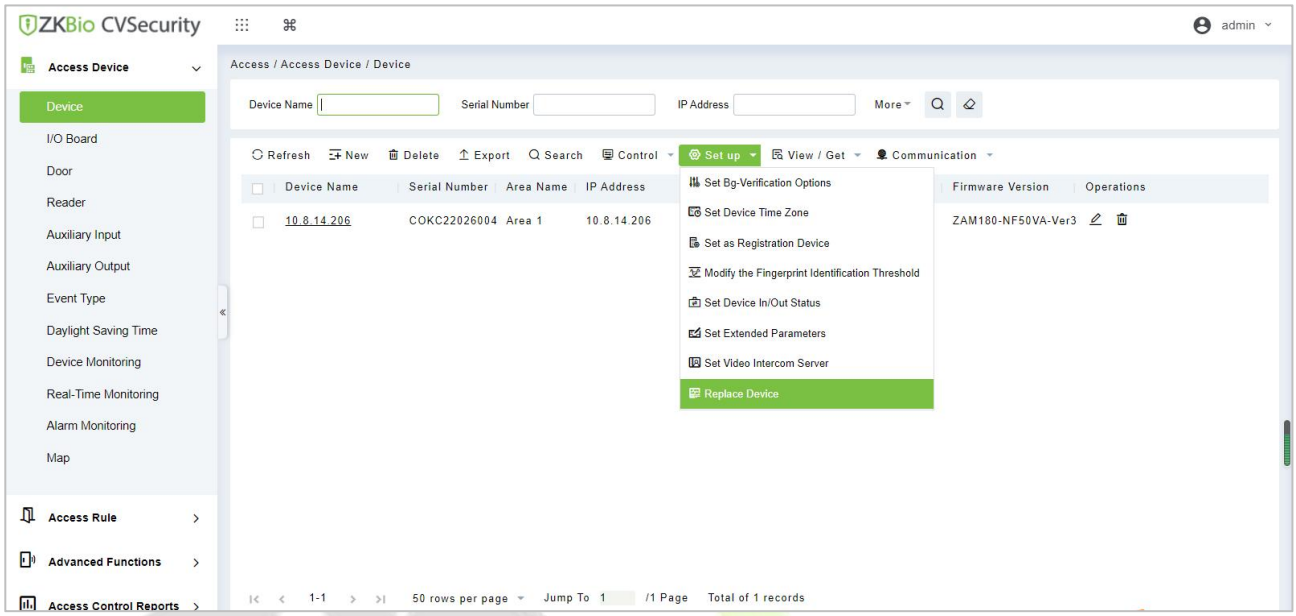


Figure 3- 18 Replace Device

Step 3: Enter the serial number of the new device, then click **OK**.

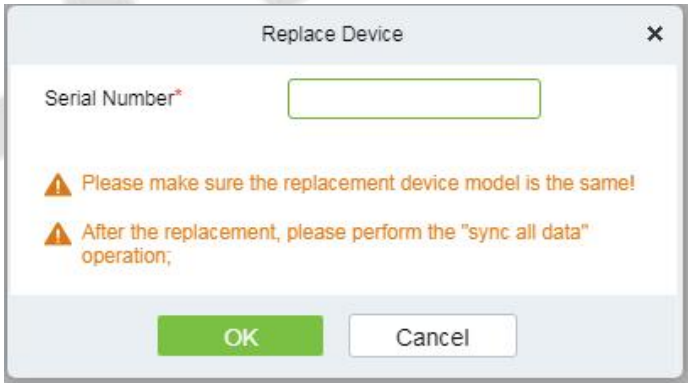


Figure 3- 19 Input the Serial Number

Step 4: Select the new device, then click **Control > Enable**.

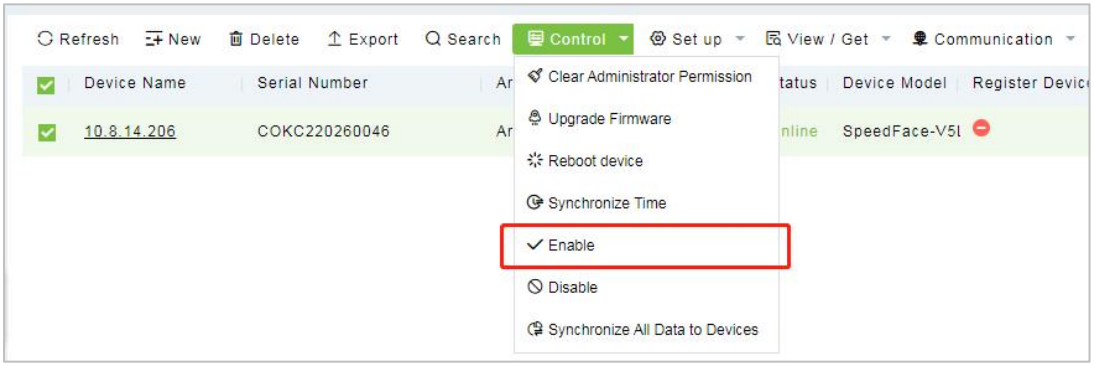


Figure 3- 20 Enable Device

Step 5: Select the new device, then click **Control > Synchronize All Data to Device**.

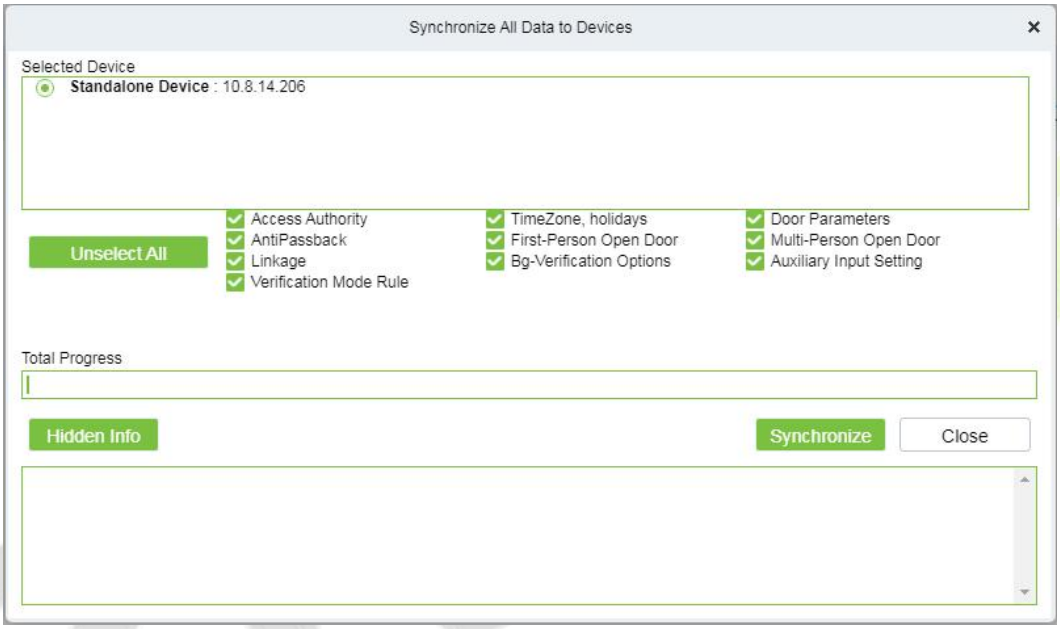


Figure 3- 21 Synchronize Device Data

Note:

1. Before replacement, the device needs to configure the server address and IP allocation.
2. Make sure that the replacement device model is the same.
3. After the replacement, please perform the "sync all data" operation.

Upload Resource File

Upload advertising resources such as device carousel images online. This function is only supported by some Android devices.

3.3.1.6View/ Get

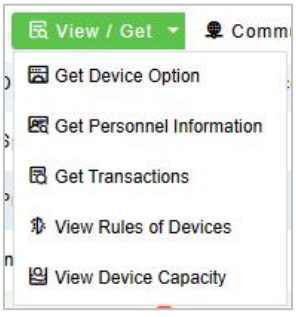


Figure 3- 22 View/Get

Get Device Option

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

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.

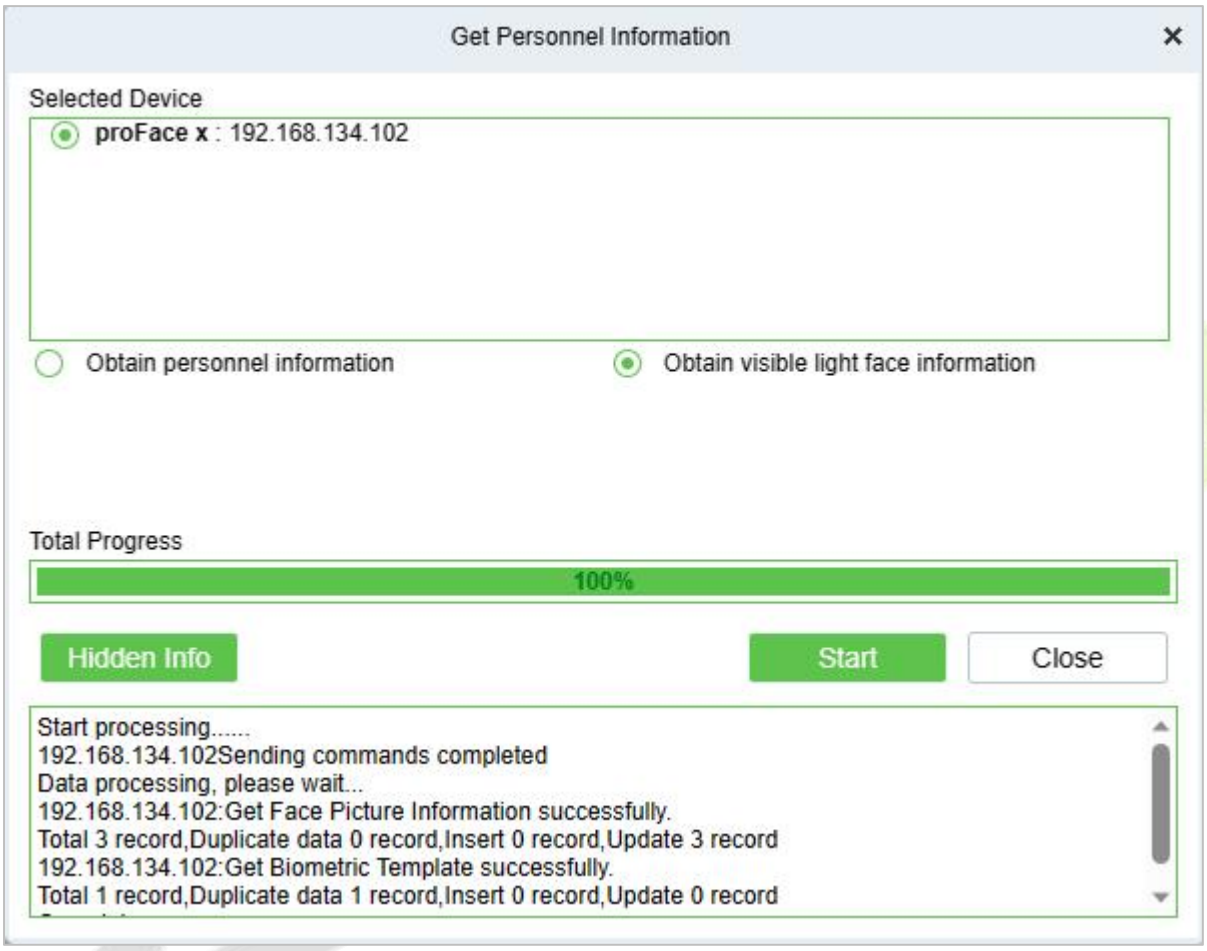


Figure 3- 23 Get Personnel Information

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 reasons, 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 of transactions. When transactions exceed this

number, the device will automatically delete the oldest stored transactions (deletes 10 thousand transactions by default).

View Rules of Devices

Shows the Access rules in the device.

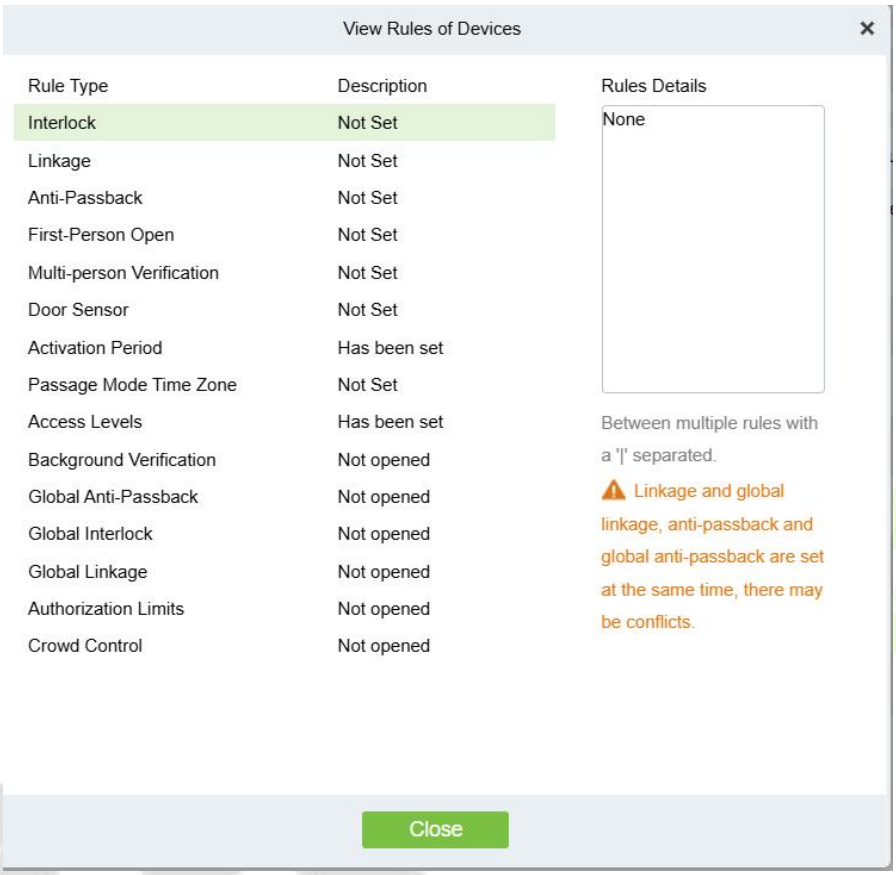


Figure 3- 24 View rules of device

View Device Capacity

It checks the capacity of personnel's biometric details in the device.

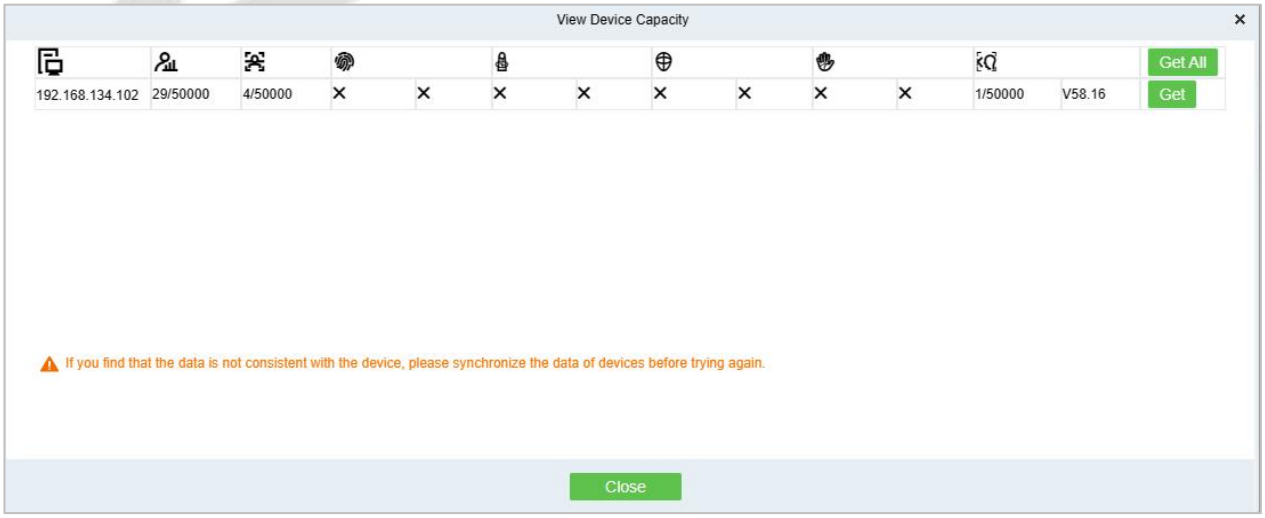


Figure 3- 25 View device capacity

3.3.1.7Communication

Figure 3- 26 Communication

Modify IP Address

Select a device and click **Modify IP address** to open the modification interface. It will obtain a real-time network gateway and subnet mask from the device. (Failed to do so, you cannot modify the IP address). Then enter a new IP address, gateway, and subnet mask. Click **OK** to save and quit. This function is the similar as Modify IP Address Function in Device.

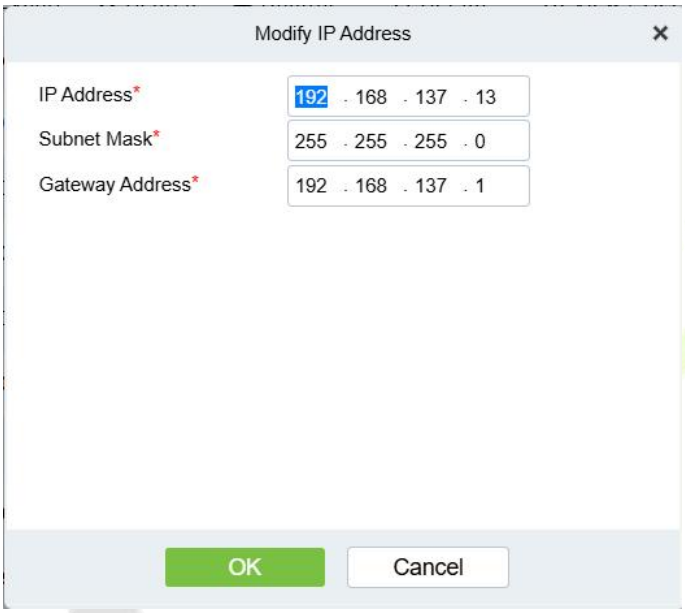


Figure 3- 27 Modify IP Address

Switch Network Connection

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

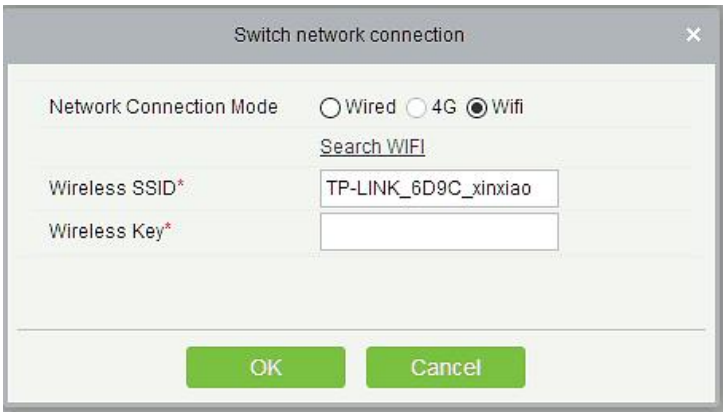


Figure 3- 28 Switch network connection

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

3.3.2I/O Board

By connecting to the I/O expansion board(EX0808), the number of doors can be expanded, and more doors can be operated.

Preconditions

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

Function Usage Scenarios

The current area needs to be expanded with more doors.

Using Trigger Result

One device can control multiple doors.

Operation Steps:

Click **[Access Control Device] > [I/O Expansion Board] > [Add]** to display the new page.

Enter each parameter, click **[OK]** to save the expansion board.

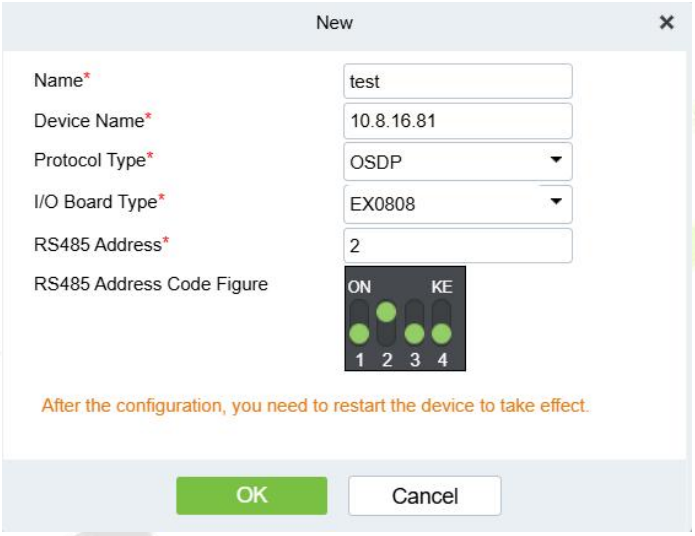


Figure 3- 29 I/O Board

Name: I/O Board Name

Device Name: Select the controller device that needs to be connected to the I/O board.

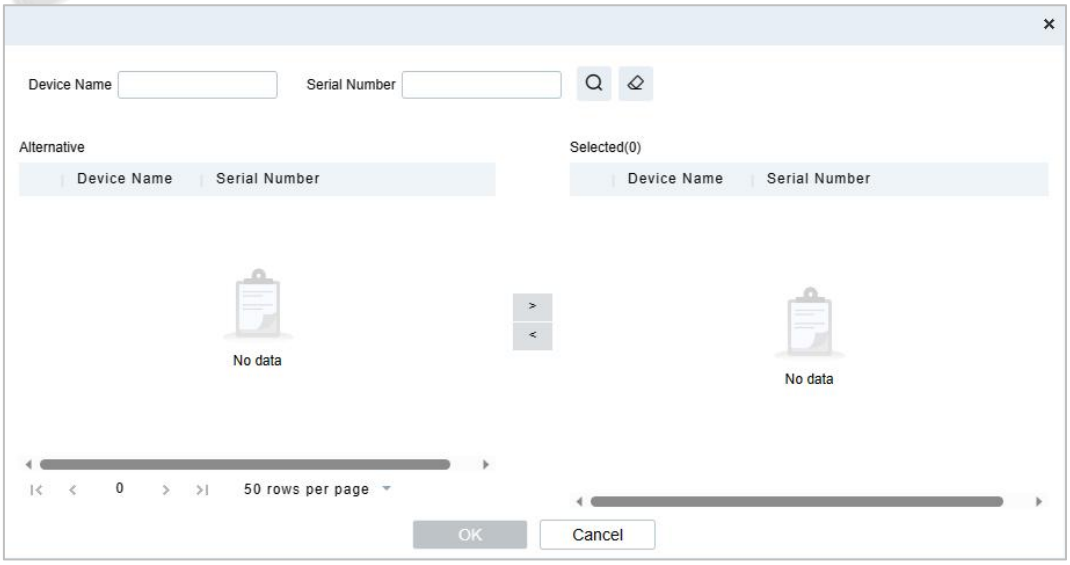


Figure 3- 30 Select Device

Protocol Type: Select the communication protocol for the I/O connection; filter the protocol according to the device selected previously. For example, since Inbio Pro plus supports RS485 and OSDP, options for RS485 and OSDP will appear.

I/O Board Type: Select EX0808.

RS485 Address: RS485 DIP Switch Address.You can enter the numbers(1-15) or click on the coding diagram below to fill it in automatically.

3.3.3Door Setting

The setting of door parameters affects the logic judgment of access control verification. The door parameters support different parameter settings according to the different firmware of the device. The following describes the configuration Steps of the door parameters with one of the devices.

● **Operation Step:**

Step 1: In the Access Control module, select "**Devices > Door**".

Step 2: In the management interface of the door, click the **Edit** button in the door operation bar to pop up the door parameter setting box.

Step 3: In the door parameter setting interface, fill in the corresponding parameters according to the addition requirements, as shown in figure below, please refer to Table 3-2 for parameter filling instructions.

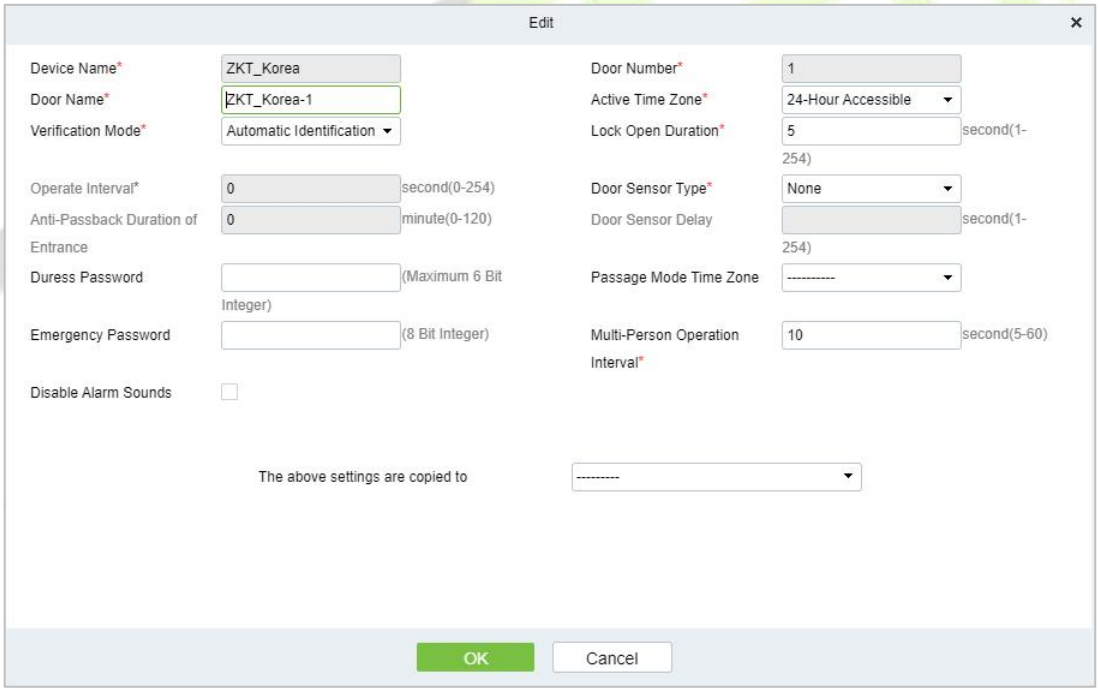


Figure 3- 31 Setting Door Parameters

● **Instructions:**

The firmware of different access control devices supports different door parameters. Set the parameters based on the actual door parameter page. Table 3-4 describes the parameter set for different devices.

Parameter	Setup Instructions
Device Name/Door Number	The basic information about the door is displayed. Reset is not supported.
Name of the Door	Customize the name of the door for easy memory.
Gate Validity Period	Select a period when the gate is valid.

Parameter	Setup Instructions
	Not within the validity period of this door, even if the person has the permission of this door, can not open the door inside.
Verify The Way	Set this parameter to the authentication mode supported by the device.
Lock Drive Duration	Set the time range for unlocking a lock after authentication. For example, if the value is set to 5 seconds, the door can be opened within 5 seconds after the verification. If the door is not opened after 5 seconds, the door will be automatically locked, and the door can be opened only after the verification.
Wiegand Format	Select a Wiegand card format that can be recognized by the door's Wiegand reader. The card format and Settings are different, will not open the door. There are 9 built-in formats in the software, the default is automatic matching wiegand card format, automatic matching can identify a variety of built-in wiegand card format.
Exit Button State	Set the status of the door exit button, locked, not locked. Lock: the door lock does not open after pressing the exit button. Not locked: the door lock is opened after pressing the exit button.
The Exit Button Is Delayed	When the exit button is set to lock, set the delay time of the exit button, that is, the delay time of the inspection door alarm after the exit button is locked.
Operation Interval	Set the interval for Access Control Operation.
Effective Time of Exit Button	Select the time period for setting the exit button.
Magnetic Door Type	Option No, normally open, normally closed, default none.
Behind Closed Doors to Lock	Set whether to lock back after the door is closed.
Magnetic Door Delay	Set the delay for checking the door status sensor after the door is opened. When the door is not "normally open", if it is open, it will start timing, alarm will start after the door magnetic delay time, and alarm will be canceled when the door is closed.
Duration Of Anti-Passback Entry	Set a limit on how long an intelligent entry can take.
Stress The Password	Set up the user to open the door when the threat password. An alarm will be generated when the coerced code opens the door.
Emergency Code	Set a password for the user to use in an emergency. The password is used by the administrator and is valid in any period and authentication mode.
The Door Is Normally Open	Select the time when this door is normally open.
Extended Time of Passage	Set on the basis of the original opening time, additional limit time. Common terms for participants, inconvenient personnel to extend the passage time.
Open Time Delay	Set the time for waiting for the delayed door opening after authentication.
Disable Alarm Reminder	If alarm event occurs on this door, whether there will be alarm sound reminder on the real-time monitoring interface.
Allow Superuser Access When the Door Is Locked	Set whether the super user can verify access when the door is locked.
The Above Settings	To set the door parameters above, the options are all doors of the current device,

Parameter	Setup Instructions
Are Copied To	all doors of all devices.

Table 3- 2 Door Parameters

Step 4: Click **OK** to complete the setting of the door parameters

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 remote opening, user can define the door opening duration (The default is 15s). You can select **Enable Intraday Passage Mode Time Zone** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select **Disable Intraday Passage Mode Time Zone** first, to avoid enabling other normal open time zones to open the door, and then select **Remote Closing**.

✍ **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 is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click **Remote Opening/Closing** in 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.

Activate Lockdown: It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

Deactivate Lockdown: It will unlock a locked door. This function is supported only by certain devices.

3.3.4Reader

This section describes the Step configuration of the Reader binding camera in ZKBio CVSecurity.

● Operation Scenario:

After the camera is bound, if related Settings are set during linkage, the Reader will perform video linkage (capture) once corresponding events occur. The Reader bind cameras in the same way. This section uses the Reader as an example to describe how to bind cameras.

● The Premise Conditions:

A video camera has been added in the **Smart Video Surveillance** module.

● Operation Step:

Step 1: In the access Control module, choose "**Device > Reader**".

Step 2: In the Operation column of the corresponding Reader, click . The bind/unbind camera page is displayed.

Step 3: On the Select Reader screen, set the Reader as required, as shown in figure below

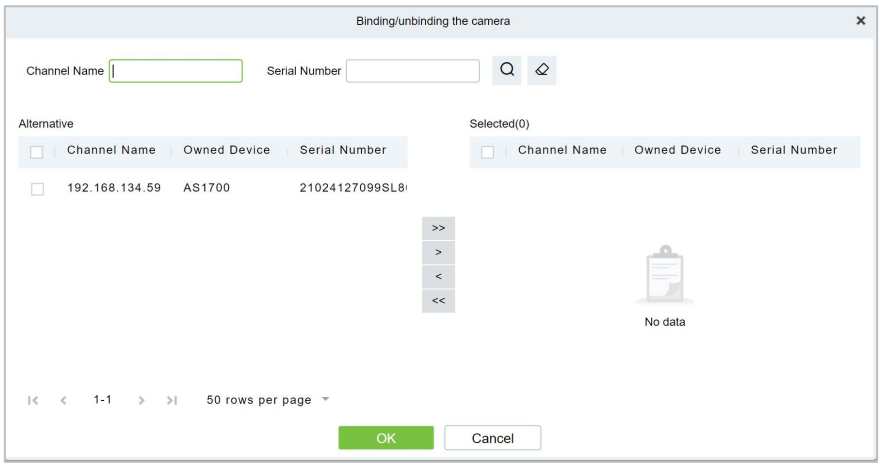


Figure 3- 32 Binding A Camera

Step 4: Click **OK** to bind the camera.

Parameter	How to set
Device Name	Customize the name of the device.
Reader Name	Display the reader's name of the device
Communication Type	Wiegand/RS485, Wiegand, RS485, and Disabled are available. When a communication type is selected, the reader interface on the device will receive data (including card and fingerprint data) for the specified type only
In/Out	Display the in/out of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.

Table 3- 3 Reader Parameters

3.3.5Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

● Operation Step:

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

Step 2: Click on Name or **Edit** to modify the parameters as shown below:

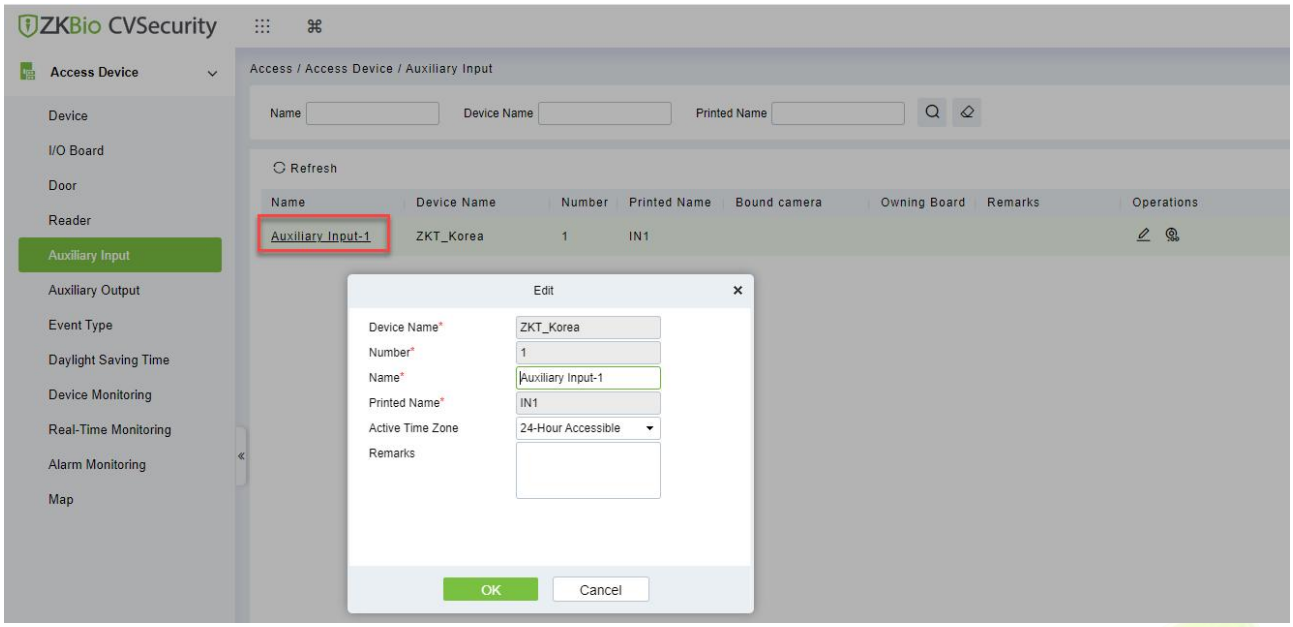


Figure 3- 33 Auxiliary input

Step 3: Click **OK** to save the name and remark and exit.

● Bind/Unbind Camera:

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

✍**Note:** An auxiliary input point can bind more than one channel.

Parameter	How to set
Device Name	Customize the name of the device.
Name	Display the name of the device
Number	Customize the name of the device
Printed Name	Display the input number of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.

Table 3- 4 Auxiliary Input Parameters

3.3.6Auxiliary Output

It is mainly related to alarm and is used when linkage is working.

● Operation Step:

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

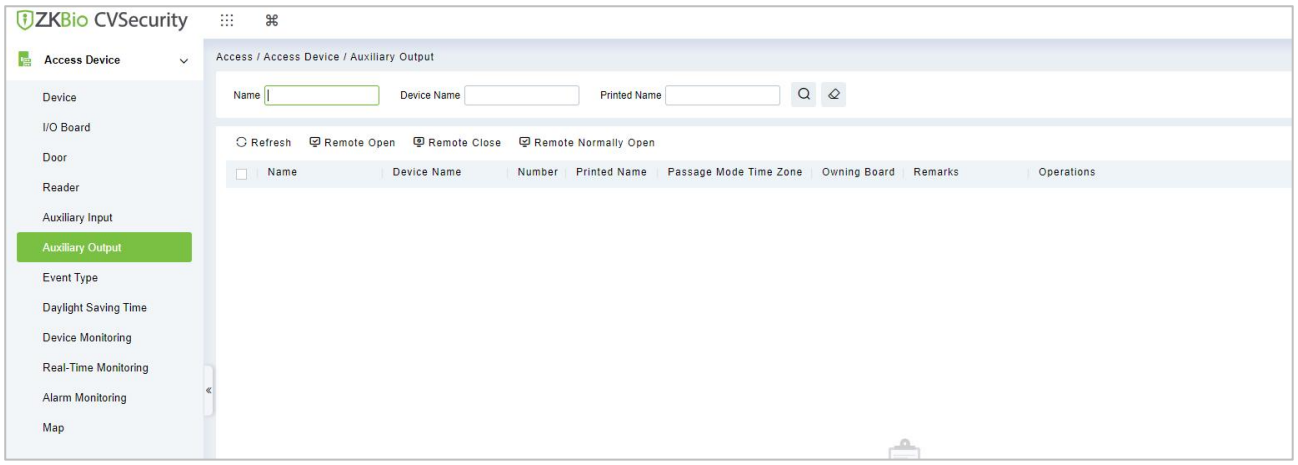


Figure 3- 34 Auxiliary Output

Step 2: Click **Edit** to modify the parameters.

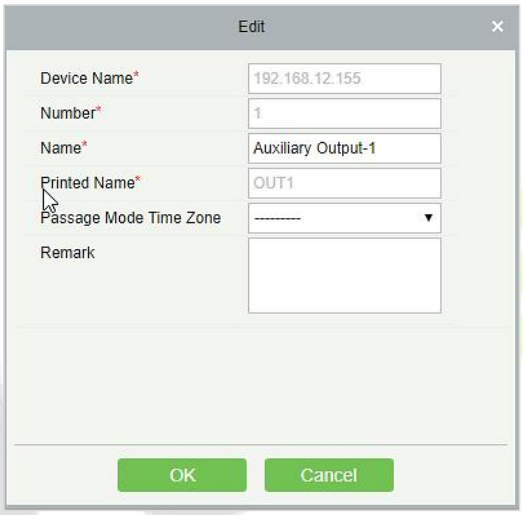


Figure 3- 35 Auxiliary Output Edit

Step 3: Click **OK** to save the name and remark and exit.

3.3.6.1 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.

3.3.6.2 Remote Normally Open

It will set the device as normal open by remote.

Parameter	How to set
Device Name	Customize the name of the device.
Name	Display the name of the device
Number	Customize the name of the device
Printed Name	Display the input number of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.

Table 3- 5 Remote Normally Open Parameter

3.3.7Event Type

It will display the event types of the access devices.

● Operation Step:

Step 1: Click **Access Device** > **Event** to access the following page:

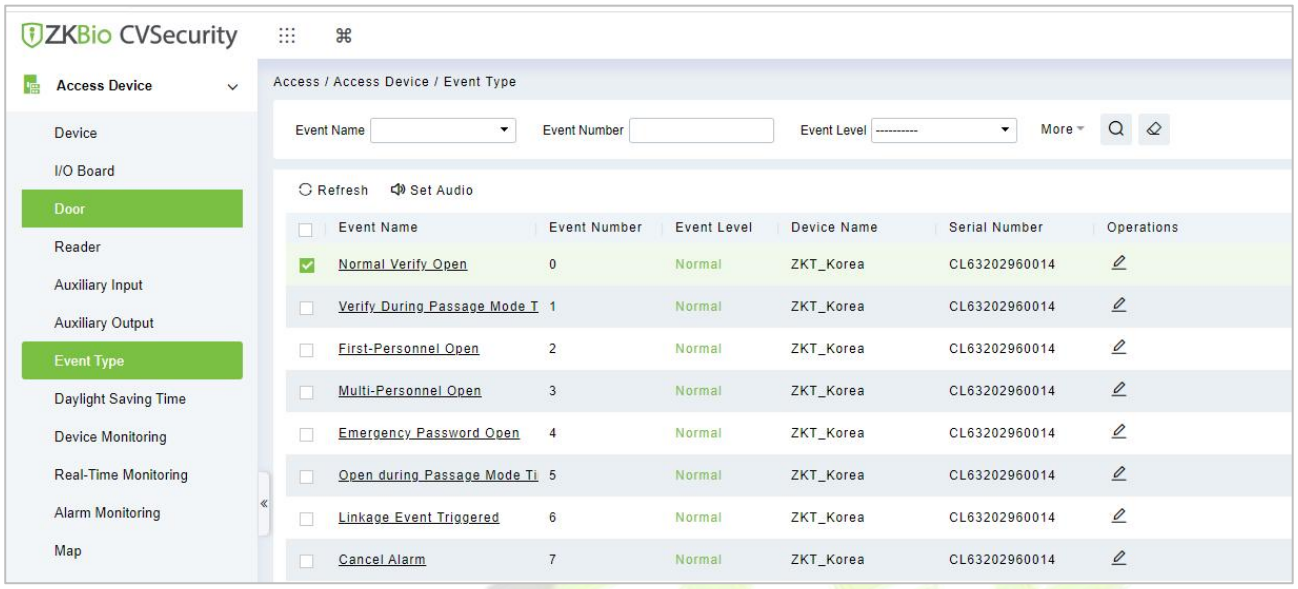


Figure 3- 36 Event Type

Step 2: Click **Edit** or click the event type name to edit.

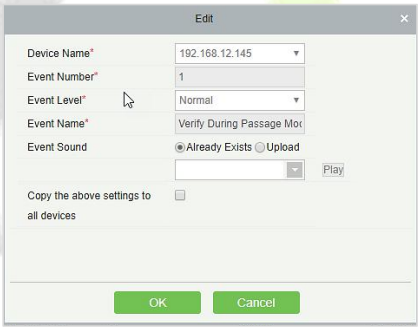


Figure 3- 37 Event Type Edit

3.3.7.1Set Audio

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

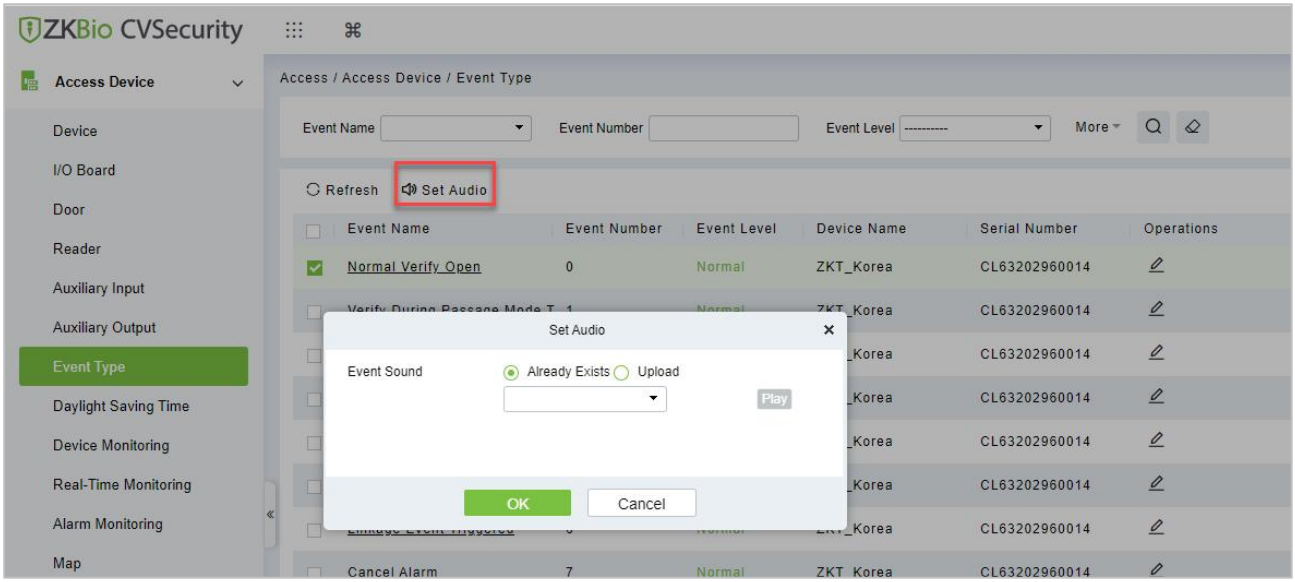


Figure 3- 38 Event Type Set Audio

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

Parameter	How to Set
Event Level	Normal, Exception, and Alarm are available
Event Name	Display the name of the device and it can't be modified.
Device Name	Display the name of the device
Event Number	Display the event number of the device.
Serial Number	Display the serial number of the device

Table 3- 6 Event Parameters

3.3.8 Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. The regulations are different in different countries. At present, nearly 70 countries adopt DST.

To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

3.3.8.1 Add DST (New)

Step 1: Click **Access Device** > **Daylight Saving Time** > **New**.

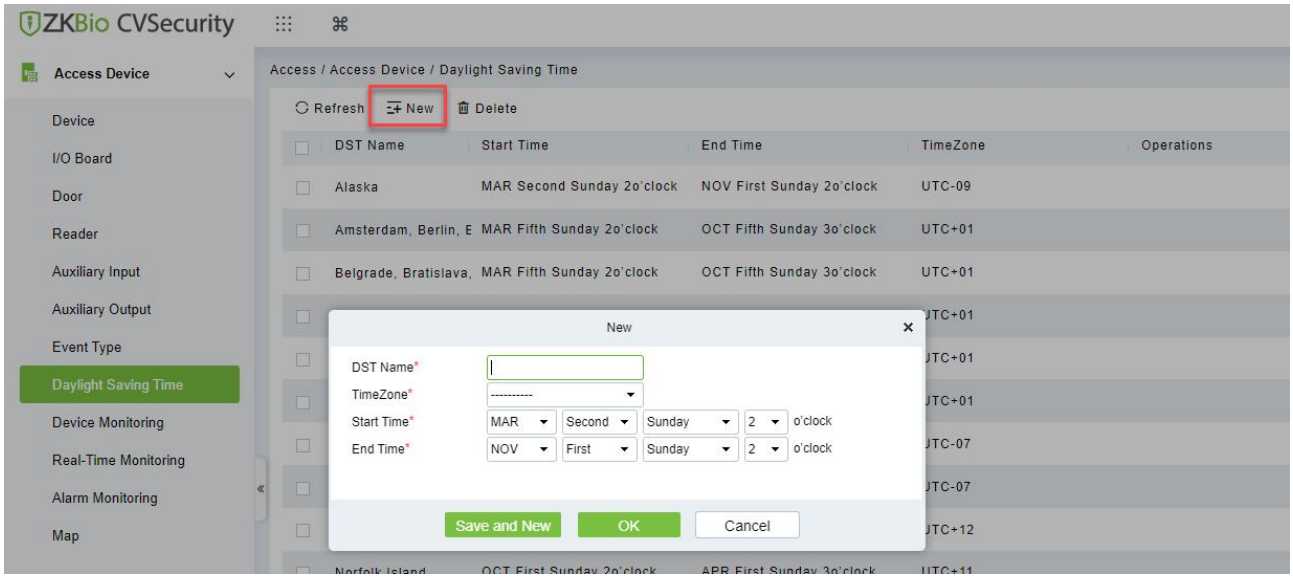


Figure 3- 39 Daylight Saving Mode

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as “second Monday in March, 02:00”. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Parameter	How to set
DST Name	Display the DST name
Start Time	Display the start time of the device
End Time	Display the end time of the device
Time Zone	Display the timezone of the device.

Table 3- 7 Daylight Saving Mode Parameters

3.3.8.2Delete

Select device, click **Delete**, and click **OK** to delete the device.

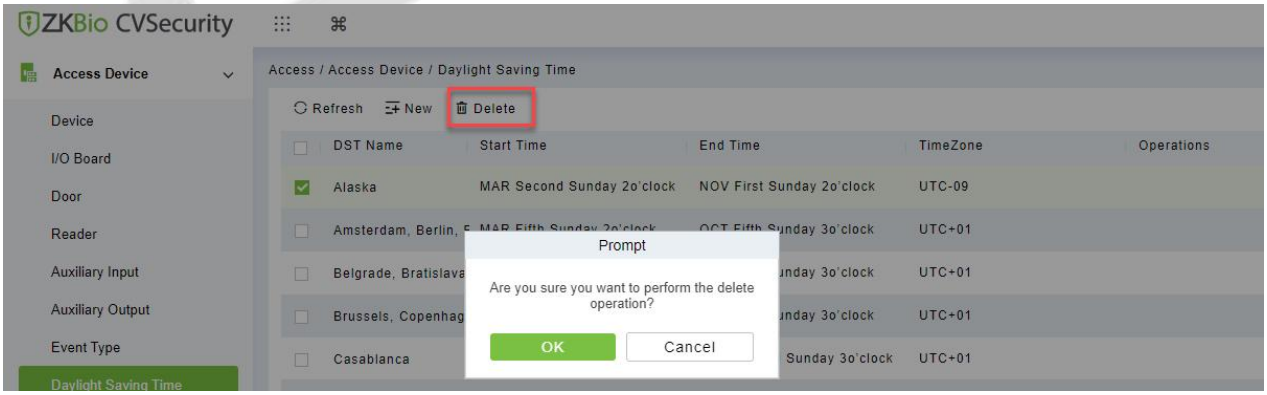


Figure 3- 40 Daylight Saving Mode Delete

3.3.9Real-Time Monitoring

On the real-time management screen, the status of the added device is displayed and the device can be opened or closed. At the same time, the dynamic of real-time events is monitored. If the door opening can be verified and corresponding access control events can be generated, the access control management service configuration is complete.

● **Operation Step:**

Step 1: Check whether the device is online.

In the Access Control module, choose "Access Control Device > Real-time Monitoring".

Check whether the icon status of the added device is online. For details about the icon status, see Table 3-8.

Note: The icons support 3 types, which are:**Door, Parking Barrier, Flap Barrier.**You can go to **Access Module ->Access Device->Device** to select the device, **Edit** for switching.

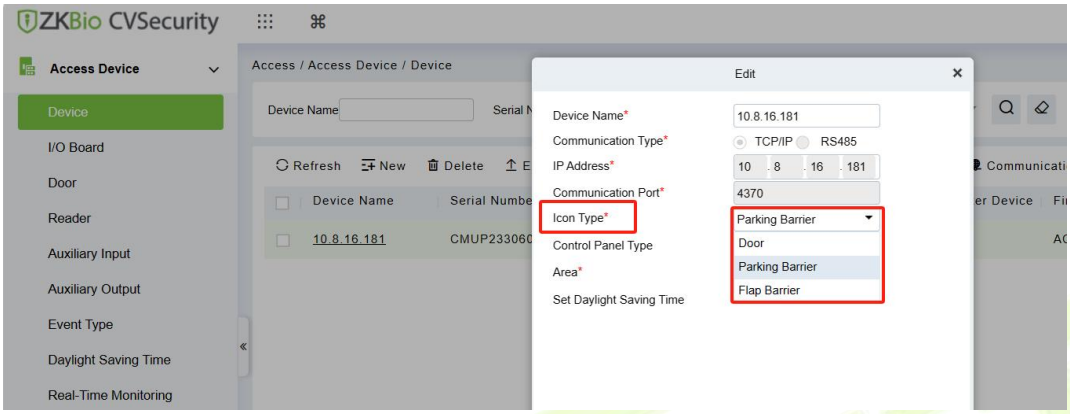


Figure 3- 41 Icon Type

The following table takes Door Icon as an example; the other 2 types(Flap Barrier & Parking Barrier) are only different graphics, but the meaning is the same, you can refer to the following table:

Icon	State	Icon	State
	The device is disabled.		Door offline status
/	No door status sensor, relay off/no relay status	/	Door status sensor not set, relay open/no relay state
/	The door is closed and the relay is off/no relay is in online state	/	The door is closed and the relay is on/no relay
/	On line door open, relay closed/no relay	/	On line door open, relay open/no relay state
	Door opens alarm, relay closes		The door opens to alarm and the relay opens
/	Door opening timeout alarm, relay closed/no relay, door magnetic open	/	Door opening timeout alarm, relay open/no relay, door magnetic open
	Door opening timeout alarm, relay closed/door magnetic closed		Door opening timeout alarm, relay open/door magnetic close

Icon	State	Icon	State
/	Door close alarm, relay off/no relay status	/	Door close alarm, relay open/no relay status
	No door magnetic setting, door alarm, relay closed		No door magnetic setting, door alarm, relay open
	Door opening timeout alarm, no relay/door magnetic closing		The door was locked
	Abnormal communication between the door and the device		
Note: If there is no relay status, the current firmware does not support the "Check relay Status" function.			

Table 3- 8 Description of Door Types

Step 2: Remote opening/closing verification, taking remote opening as an example.

Select the online door device, click "**Remote door opening**", enter the user password in the pop-up security verification, and click **OK**.

On the remote door opening screen, enter the time to open the door and tap **OK**, as shown in figure below.

If "Operation succeeded" is displayed, the remote door opening Operation is complete.

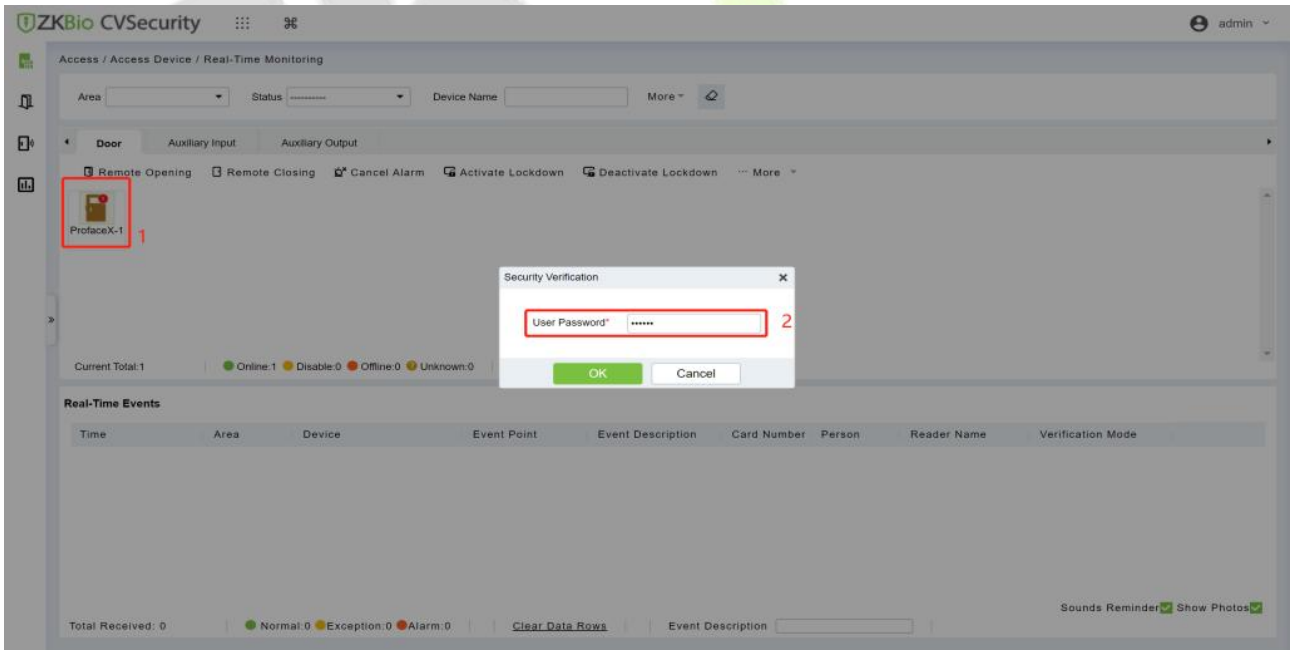


Figure 3- 42 Remote Door Opening

Step 3: Permission to verify.

Verify personnel permissions on added devices.

In the real-time monitoring window, judge whether the personnel permissions are correctly configured according to the event status; If the user has been granted access rights, the real-time access event is a normal verification event, as shown in Figure 3-38, indicating that the access level service is configured.

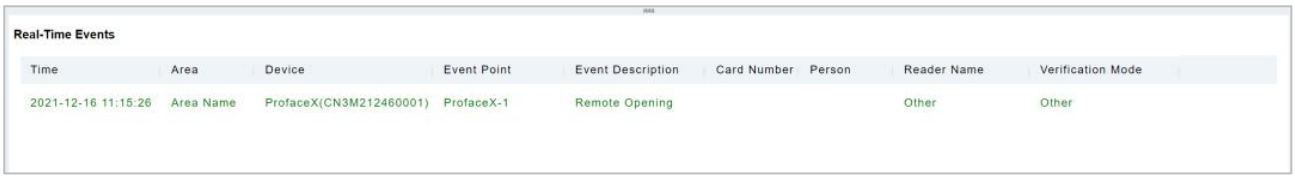


Figure 3- 43 Real-Time Events

3.3.9.1 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 remote opening, user can define the door opening duration (The default is 15s). You can select **Enable Intraday Passage Mode Time Zone** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select **Disable Intraday Passage Mode Time Zone** first, to avoid enabling other normal open time zones to open the door, and then select **Remote Closing**.

✍ **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 is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click **Remote Opening/Closing** in 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.

- **Activate Lockdown**

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices. Super User Swipe to Initiate Lockdown after 3 swipes

- **Deactivate Lockdown**

It will unlock a locked door. This function is supported only by certain devices. Super User Swipe to Initiate disable after 3 swipes

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

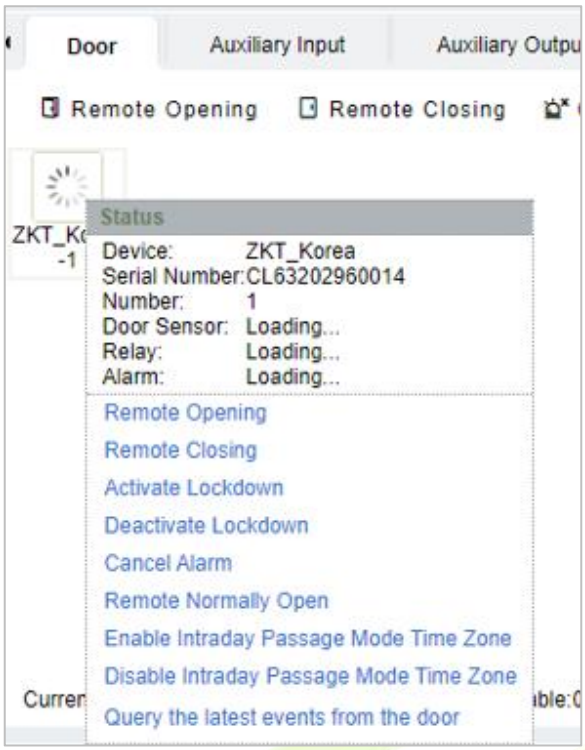


Figure 3- 44 Quick management of doors

- **Personnel Photo Display**

If a Real-Time Monitoring event contains personnel activity, the monitor will display the person photo (if no photo is registered, the monitor will display default photo). The event name, time and date are displayed.

- **Play Audio**

If this option is selected, it plays an audio after an alarming event occurs.

- **Query the Latest Events from The Door**

Click to quickly view the latest events happened 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.

- **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.

The Superuser can initiate lockdown after 3 swipes and deactivate the same after 3 swipes.

3.3.9.2 Auxiliary Input

It monitors current auxiliary input events in real-time.

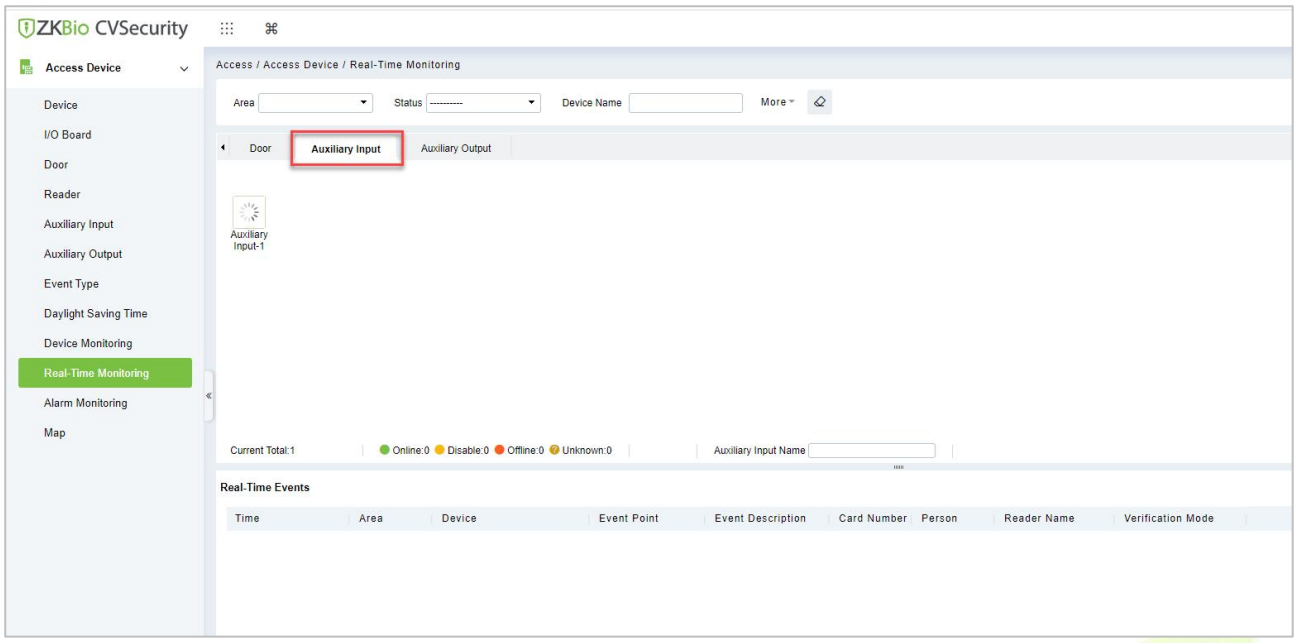


Figure 3- 45 Real Time Monitoring Auxiliary Input

3.3.9.3Auxiliary Output

Here you can perform Remote open, Remote Close, Remote Normally Open.

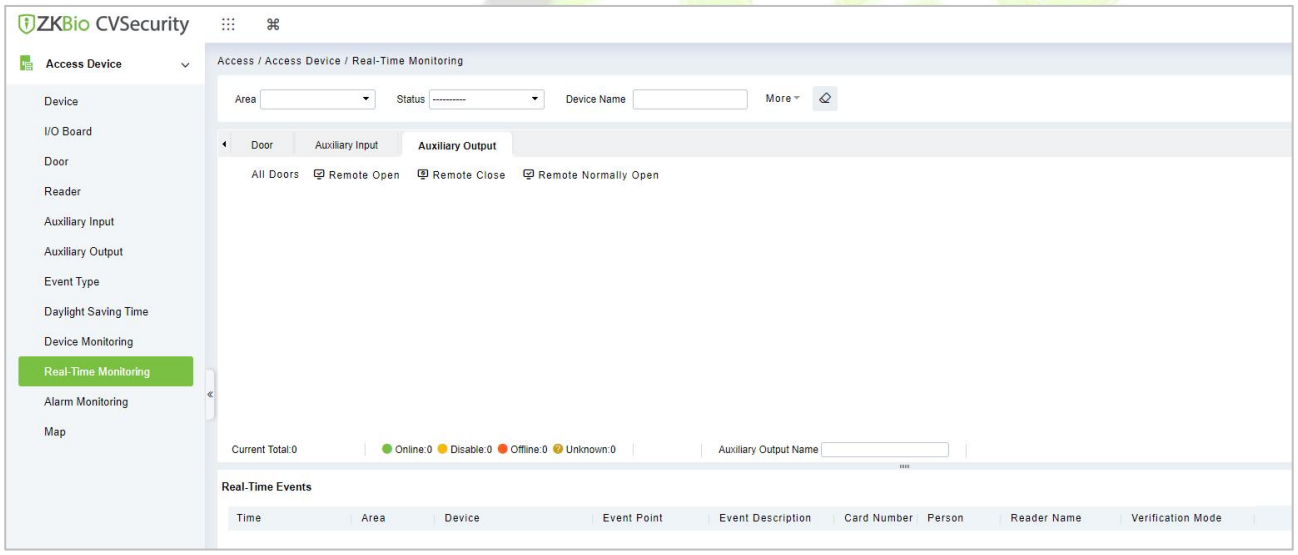


Figure 3- 46 Real Time Monitoring Auxiliary Output

● Monitoring All

By default, the home page displays all doors of the panels within the user's level. User may monitor door(s) by setting the Area, Access Control or Door.

3.3.10Alarm 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

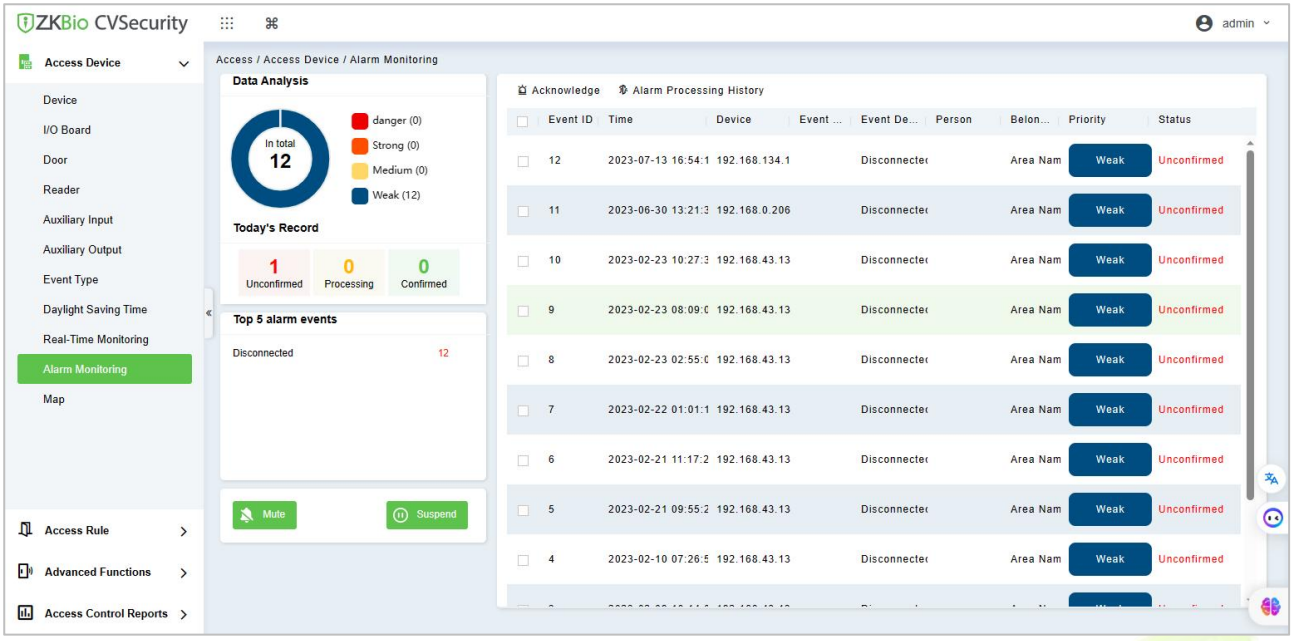


Figure 3- 47 Alarm Monitoring

Note: The current alarm priority is set to the default. If you need to modify it, you can go to the path of **Access -> Access Device -> Alarm Monitoring** to make the adjustment.

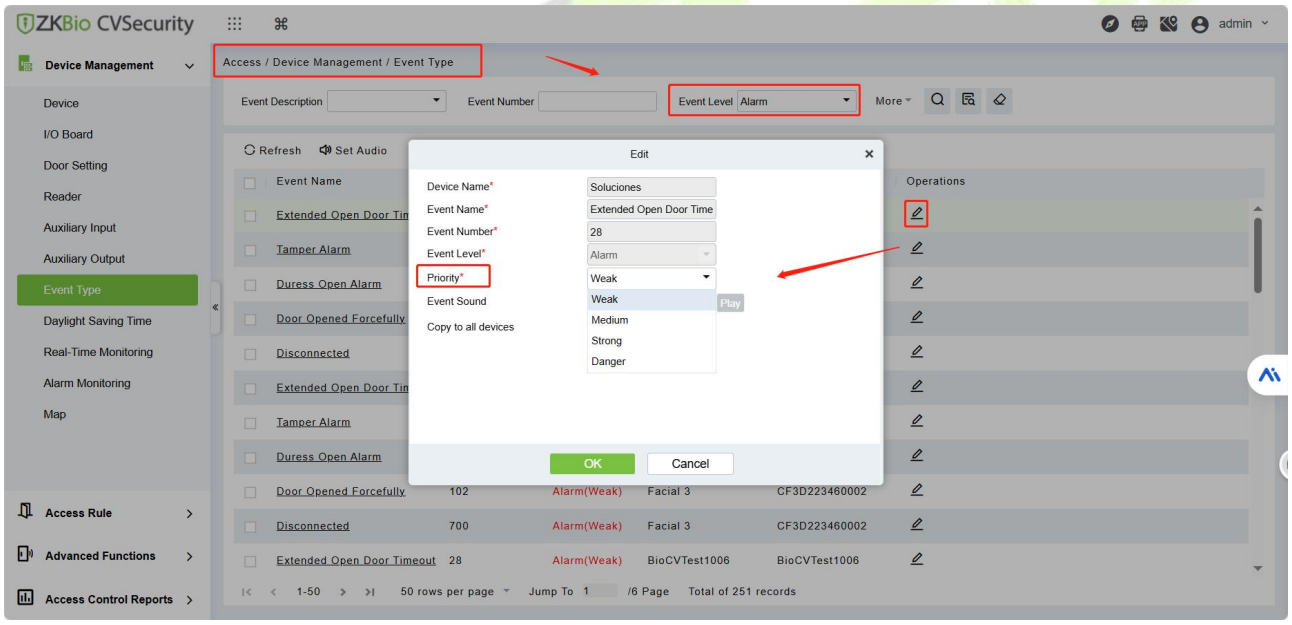


Figure 3- 48 Even Type

3.3.11Map

Click **Access Device** > **Map** > **New** to add a map.

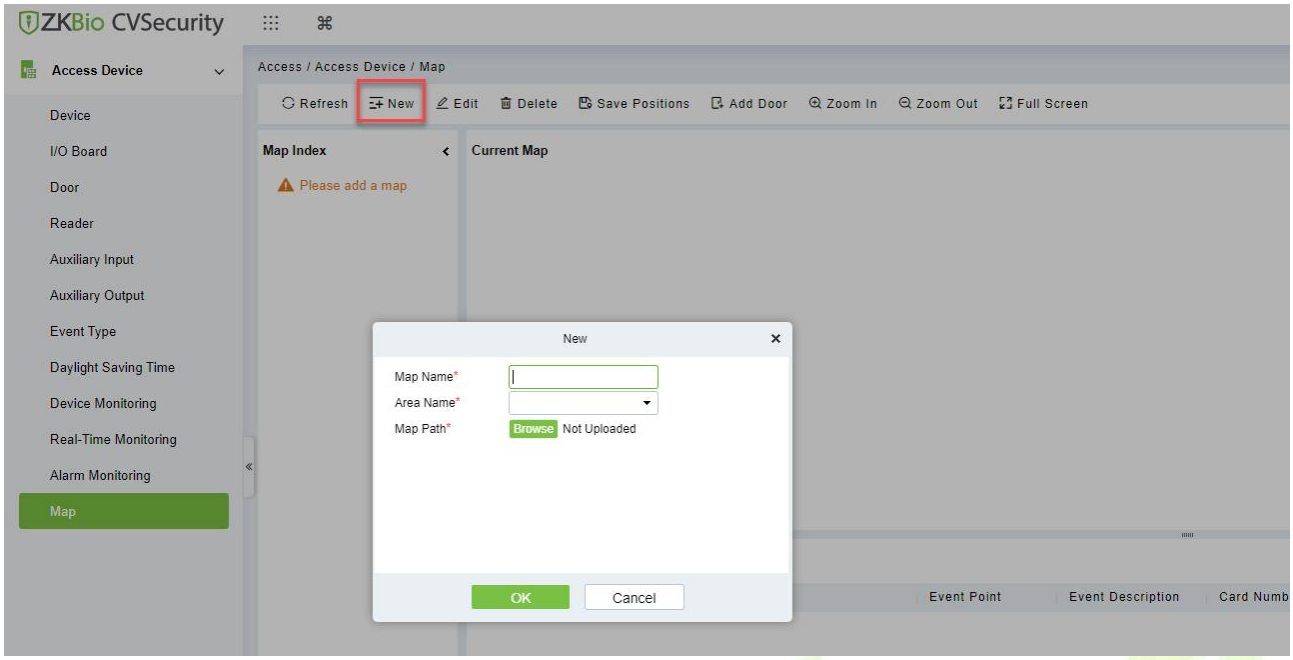


Figure 3- 49 Map

After adding, users can add door on the map, perform zoom-in, zoom-out, etc. If users relocated or modified the map, click **Save Positions** to save. The user can view the new setting at next visit.

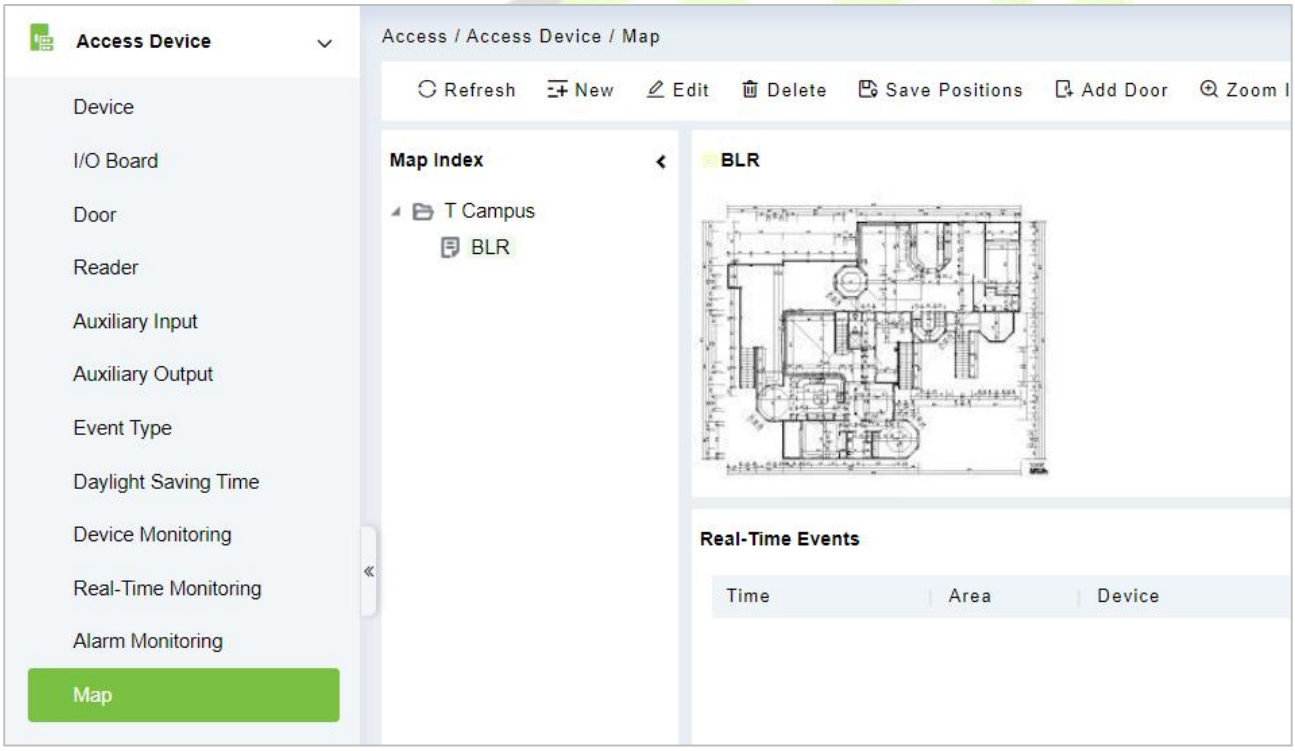


Figure 3- 50 Map Position

3.3.11.1 Add/Delete Map

Users can add or delete a map as needed.

3.3.11.2 Edit Map

Users can edit map name, change 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**).

Add Doors & Cameras

After adding the map, click on "Add doors" and "Add cams" in the toolbar on the right to select devices to add to the map.

Door Operation

If you move the cursor to a door, 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

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.

When an administrator is adding a new user, he can set the user operation rights in role setting, such as Save positions, Add Door, Add Camera, etc.

Note:

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.

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**.

When modifying door icon, especially when users zoomed out the map, the margin for top and left shall not be smaller than 5 pixels, or system will prompt error.

Users are recommended to add a map size under 1120 * 380 pixels. If several clients access the same server, the display effect will be different according to resolutions of screen and the settings of browsers.

3.4 Access Rule

Access control rules are the core logic control part of access control, including time period settings, linkage settings, etc.

3.4.1Timezone

In **Access Control** Module, time period is a very important basic concept, which is used to set the use time of the door and specify that **Access Control** is available in the valid time period.

This section describes how to configure Step to manually add a time range in ZKBio CVSecurity.

3.4.1.1Add (New)

● Operation Step:

Step 1: In the access Control module, choose “Access Rule > Time zone”.

Step 2: Click **New**, the interface for adding time segments is displayed.

Step 3: The time segment page is added. Set the content based on the new requirements, as shown in figure below. For parameter Settings, see Table 3-9.

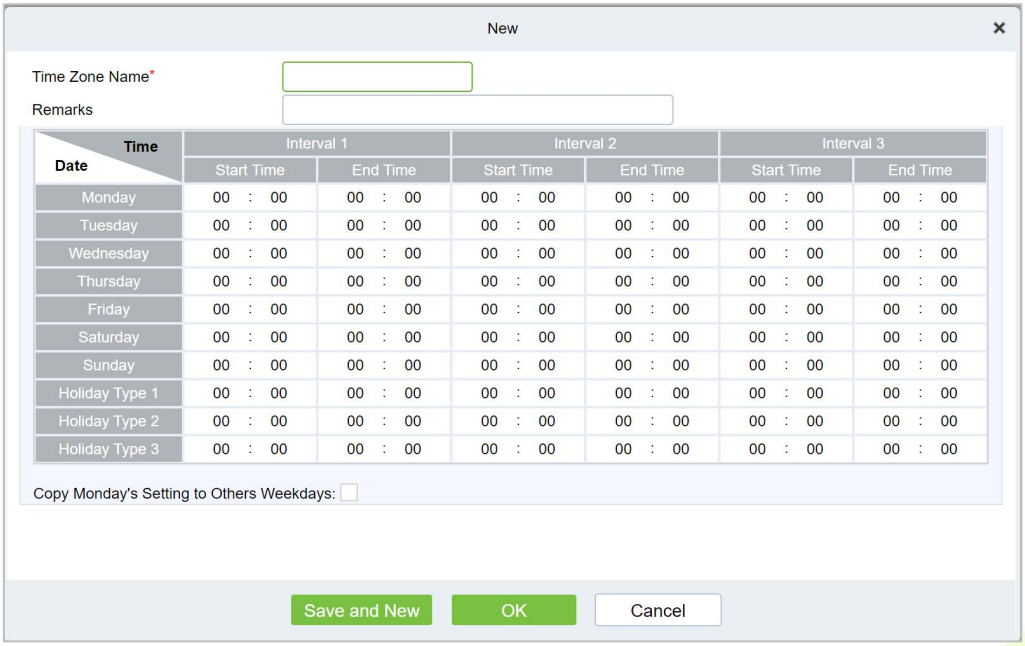


Figure 3- 51 Adding A Time Range

Parameter	How to set up
Schedule Name	You can set a time range name for easy memory.
Note	Remarks Description of user-defined Settings.
Time interval	Set the start time and end time for each time range. The time period includes one week and three holiday-type time periods.
Copy Monday's time to other weekdays	You can quickly copy your Monday Settings to other weekdays.

Table 3- 9 Parameters to Be Added in The Time Range

Step 4: Click **OK** to finish adding the time range.

3.4.1.2Delete

Select time zone name, click **Delete**, and click **OK** to delete the time zone.

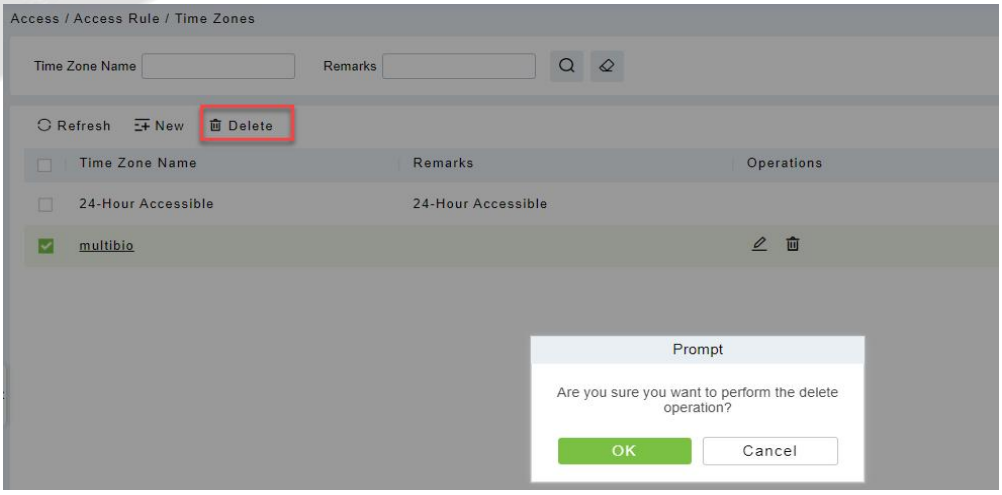


Figure 3- 52 Time Zone Delete

3.4.2Holiday

The access control time on holidays may be different from that on weekdays. To facilitate Operation, the system supports separate access control time on holidays.

This section describes how to manually add a holiday Step in ZKBio CVSecurity.

3.4.2.1Add (New)

● Operation Step:

Step 1: In the Access Control module, choose "**Access Rule > Holidays**".

Step 2: Click **New**, the page for adding holidays is displayed.

Step 3: When a page is added during holidays, set the content as required, as shown in figure below. For parameter Settings, see Table 3-10.

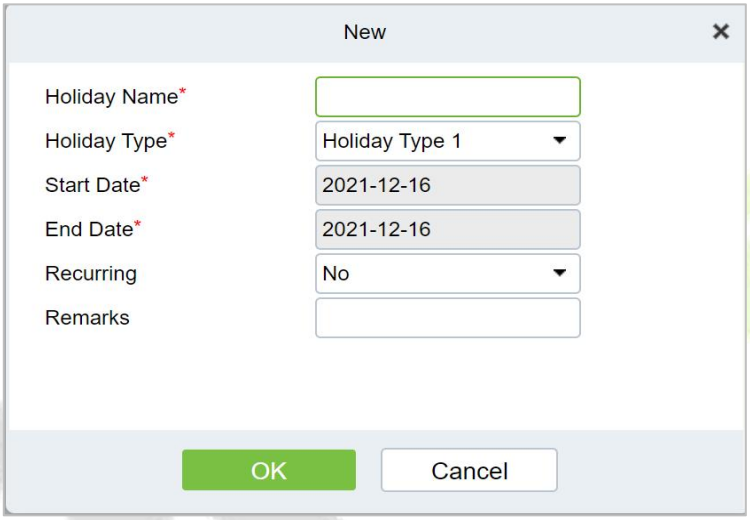


Figure 3- 53 Adding Holidays

Parameter	How to set up
Holiday Name	You can set holiday names for easy memory.
Type of Holidays	The holiday type can be: Holiday type 1, Holiday type 2, holiday type 3. Set holiday type to time Range.
Start time/End time	Set the holiday time range.
According to the annual circulation	Set whether this holiday cycle by year: yes, no. For example, if New Year's Day is January 1, set this parameter to Yes.Mother's Day falls on the second Sunday in May. If the date is uncertain, set it to No.
Note	Custom Settings description.

Table 3- 10 Parameters for Adding Holidays

Step 4: Click **OK** to finish adding the holiday.

3.4.2.2Delete

Select holiday, click **Delete**, and click **OK** to delete the holiday.

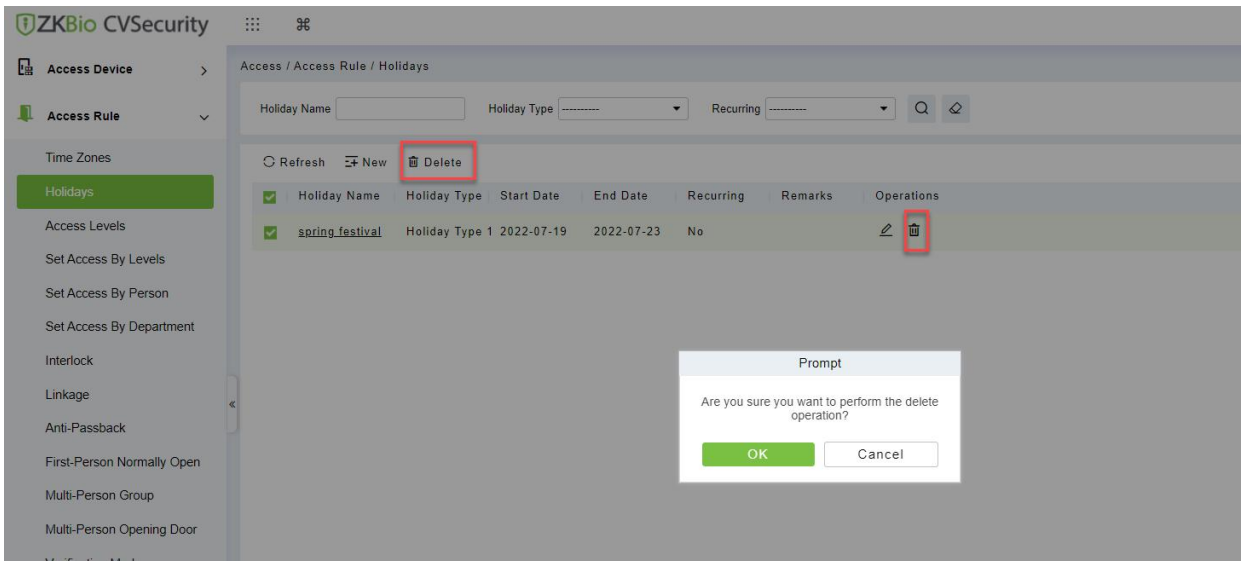


Figure 3- 54 Holiday Delete

3.4.2.3Import

Step 1: Select and click the "**Download Import Template**" button,download the template "Holiday Template.xls" locally.

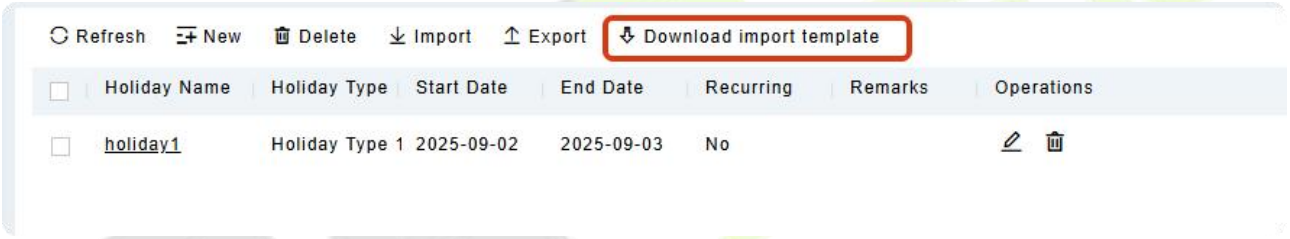
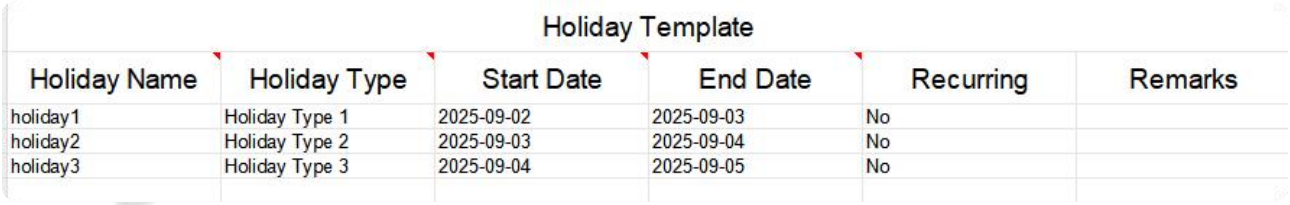


Figure 3- 55 Download Import Template

Step 2: Open the exported template file "Holiday Template.xls" for adding holiday information.



Holiday Template

Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
holiday2	Holiday Type 2	2025-09-03	2025-09-04	No	
holiday3	Holiday Type 3	2025-09-04	2025-09-05	No	

Figure 3- 56 Import Template

Step 4: Select and click the "**Import**" button; click the "**Browse**" button to import the batch import template into the system and click OK, as shown in figure below.

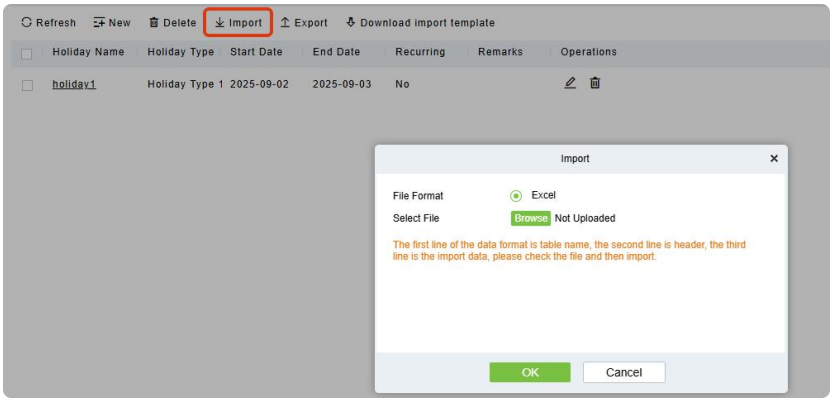


Figure 3- 57 Import

3.4.2.4Export

Click the "**Export**" and set the relevant parameters.

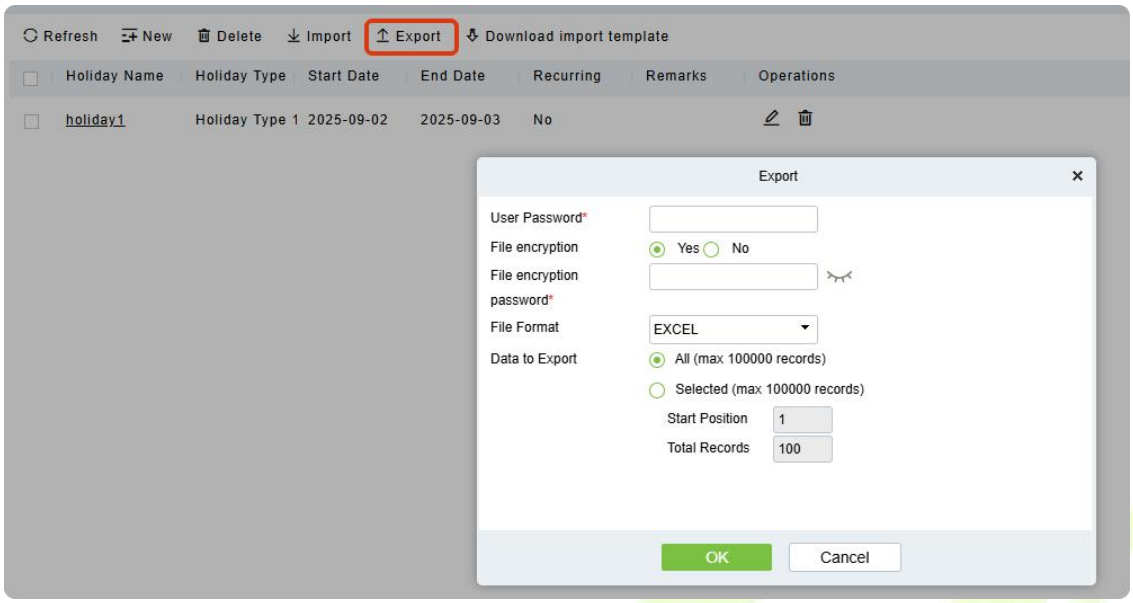


Figure 3- 58 Export

	Holidays					
2	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
3	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
4						

Figure 3- 59 Export

3.4.3Access Level

Access level groups define groups and categories of internal doors to facilitate subsequent permission assignment operations.

Setting operations include creating access level groups and adding doors to access level groups.

3.4.3.1Add (New)

This section describes how to create Step for Access Control groups in ZKBio CVSecurity.

● Operation Step:

Step 1: In the Access Control module, choose "**Access Rule > Access Level**".

Step 2: Click **New** in the left column, and the page for adding access level groups is displayed.

Step 3: On the page for adding access level groups, set parameters based on the new requirements, as shown in figure below. For parameter Settings, see Table 3-11.

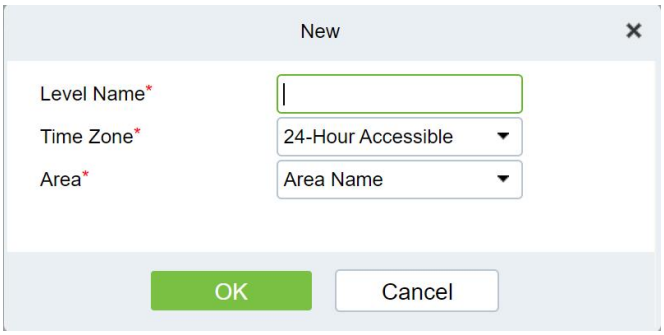


Figure 3- 60 Adding Access Level Groups

Parameter	How to set up
Permission Group Name	You can customize the name of the access level group for easy query.
Access Control Period	Select the configured access time range to define the valid access time range for this permission group.
Area	Select the configured area from **System > System Management > Area Settings** and define the area to which the Access Control group belongs.

Table 3- 11 Description of Access Control Right Groups

Step 4: Click **OK** to finish configuring the access control right group.

3.4.3.2Add Door

This topic describes how to add Operation Step to the door of the created access level group in ZKBio CVSecurity.

● Operation Step:

Step 1: In the Access Control module, choose "**Access Rule > Access level>Add Door**".

Step 2: Click **"Add Door"**, and the page for selecting a door is displayed. add a door as required, as shown in figure below.

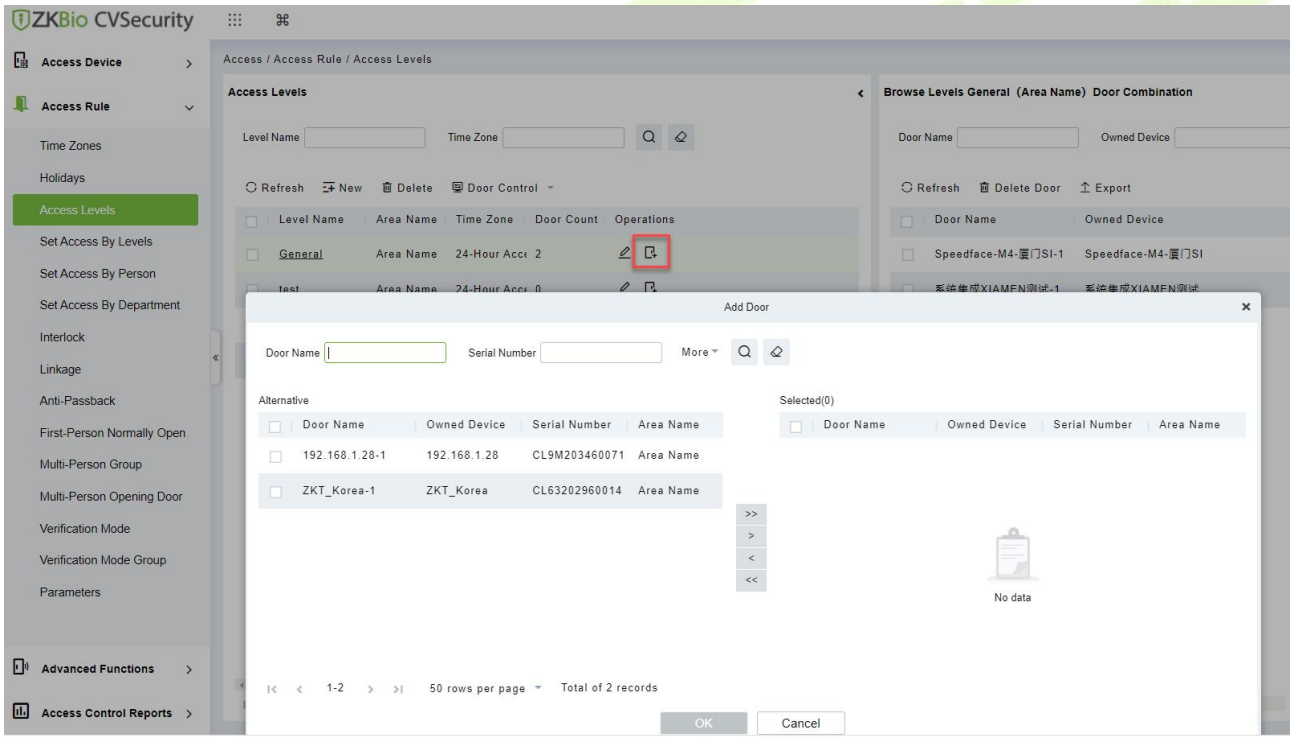


Figure 3- 61 Adding Access Level Groups Add Doors

Step 3: Click **OK** to finish configuring the door for the access control right group.

3.4.3.3Door Control

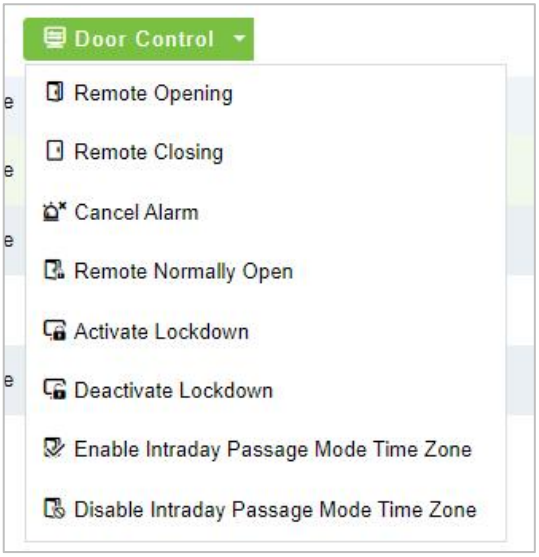


Figure 3- 62 Door Control

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 remote opening, user can define the door opening duration (The default is 15s). You can select **Enable Intraday Passage Mode Time Zone** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select **Disable Intraday Passage Mode Time Zone** first, to avoid enabling other normal open time zones to open the door, and then select **Remote Closing**.

✍ **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 is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click **Remote Opening/Closing** in 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.

Activate Lockdown

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices. Super User Swipe to Initiate Lockdown after 3 swipes

Deactivate Lockdown

It will unlock a locked door. This function is supported only by certain devices. Super User Swipe to Initiate disable after 3 swipes.

3.4.3.4Import or Export Access Level

Step 1: Export and fill in Access Level Template:

In the **Access Module**, click **Access Rule** > **Access Levels** > **Export** > **Export Access Level**, then fill in the Access levels information.

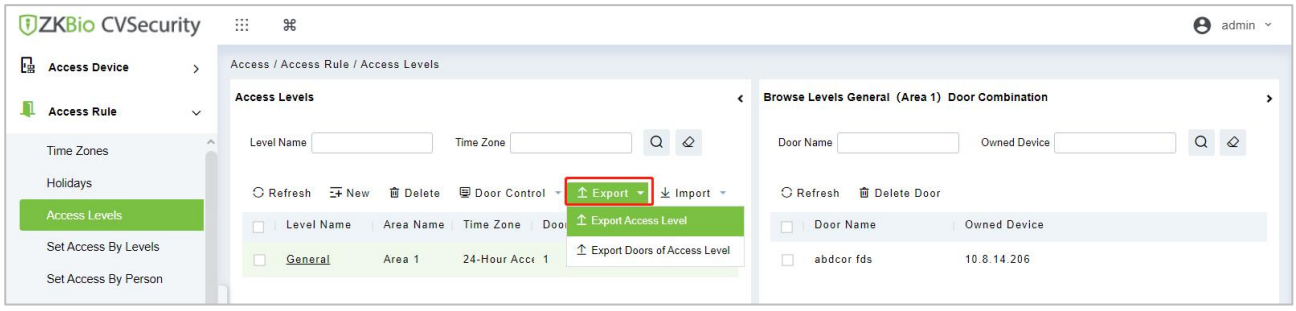


Figure 3- 63 Export Access Level Template

Access Levels		
Level Name	Area Name	Time Zone
Level 1	Area 1	Time Zone 1
Level 2	Area 2	Time Zone 1
Level 3	Area 3	Time Zone 1
Level 4	Area 4	Time Zone 1
Level 5	Area 5	Time Zone 1

Figure 3- 64 Fill in Access Level Template

Note: The Level name can be customized. The Area Name can be set from **System** > **System Management** > **Area Settings**, the Time Zone can be set from **Access** > **Access Rule** > **Time Zones**.

Step 2: Export the Doors of Access Level Template:

In the **Access Module**, click **Access Rule** > **Access Levels** > **Export** > **Export Doors of Access Level**, 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**.

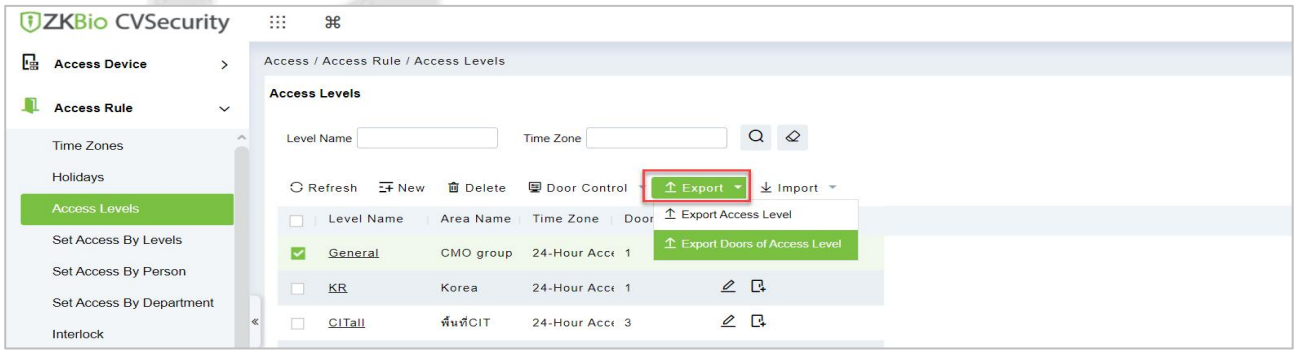


Figure 3- 65 Export the Access Level Template 1

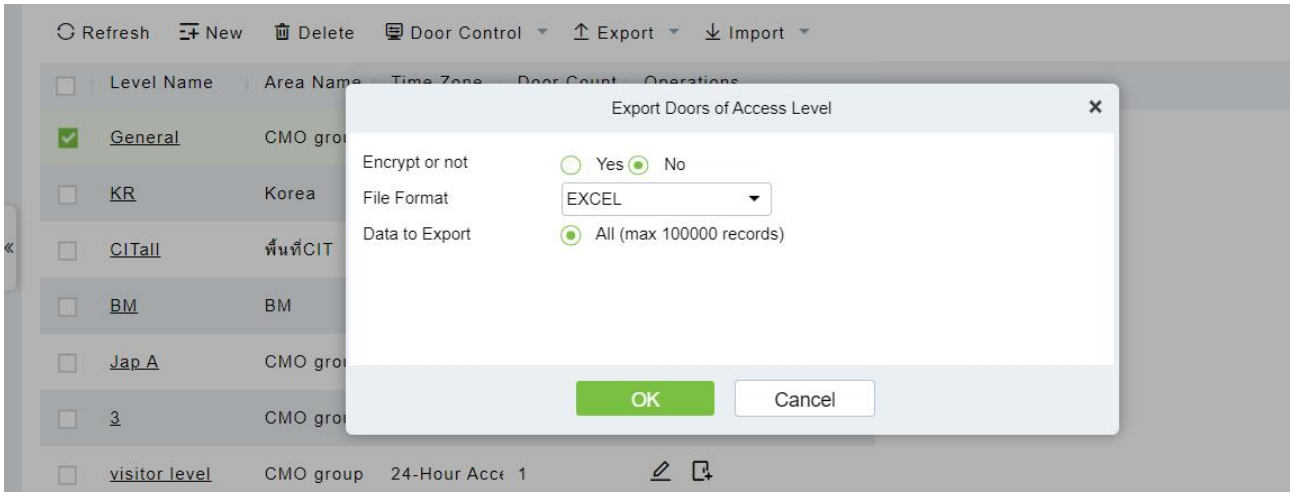


Figure 3- 66 Export the Access Level Template 2

Step 3: Import the Access Level Template:

In the **Access** module, click **Access Rule** > **Access Levels** > **Import** > **Import Access Level**, and click **Browser** to upload the Access Level Template.

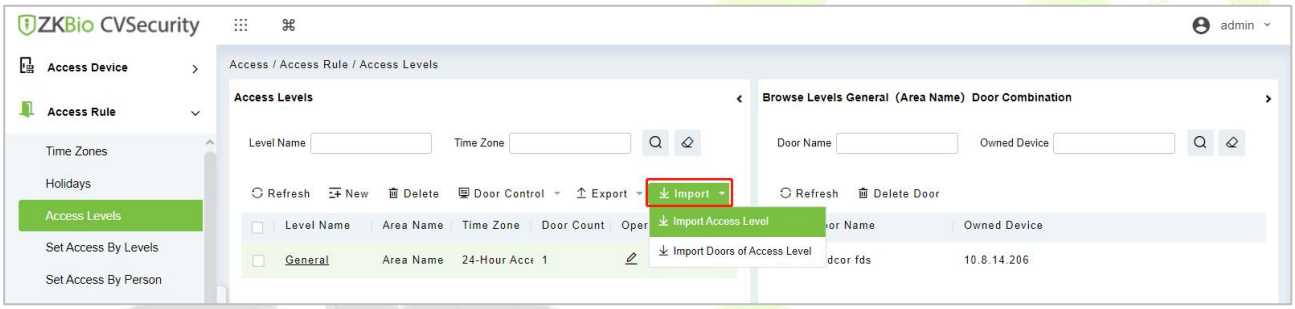


Figure 3- 67 Import the Access Level Template 1

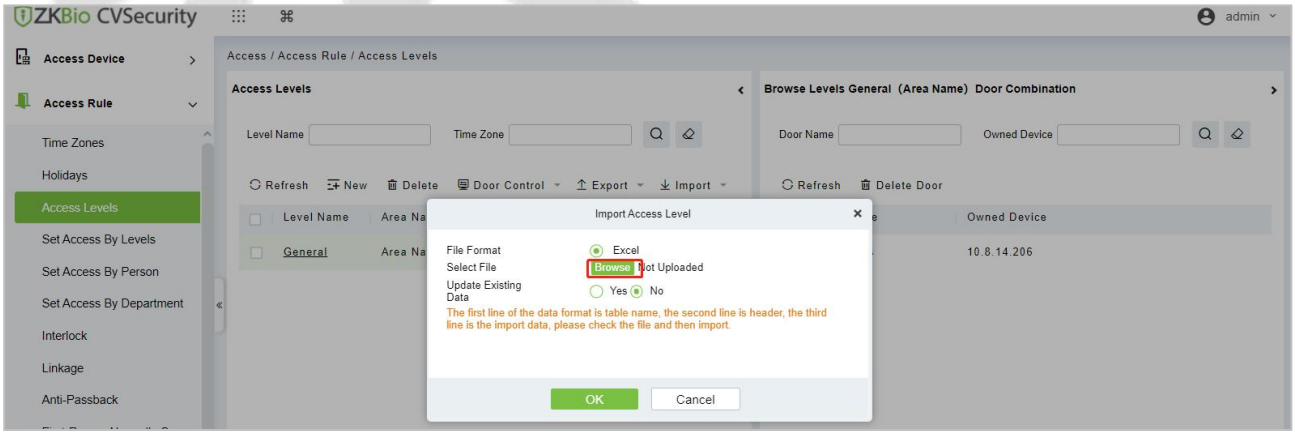


Figure 3- 68 Import the Access Level Template 2

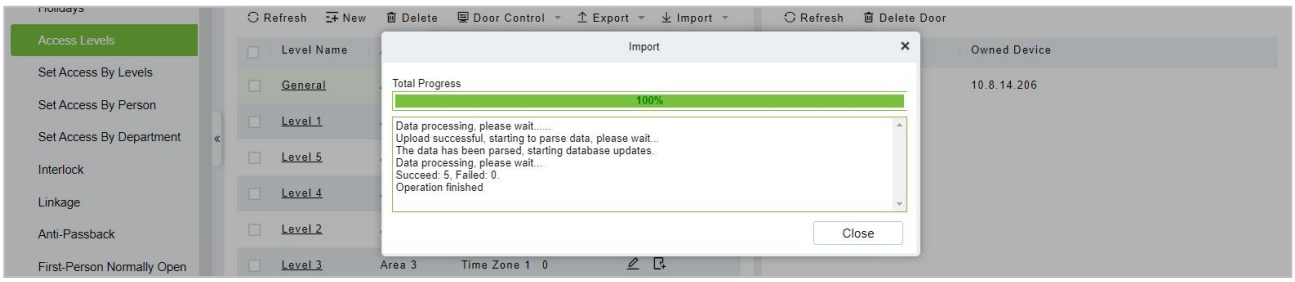


Figure 3- 69 Import the Access Level Template 3

Step 4: After the upload is successful, we can view the uploaded level as the following figure.

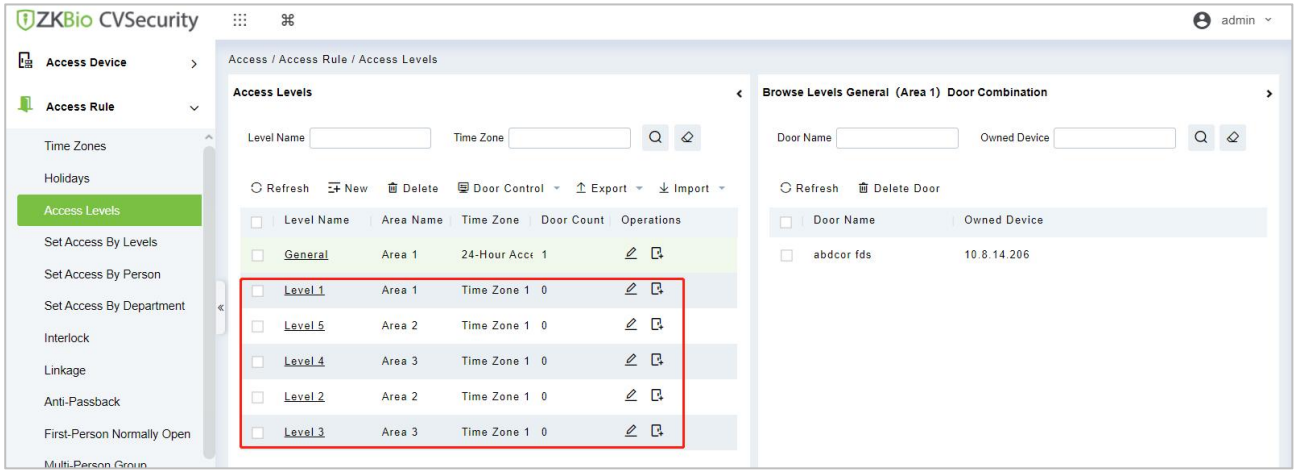


Figure 3- 70 Import the Access Level Template 4

Step 5: Import the Doors of Access Level Template:

In the Access module, click **Access Rule** > Access Levels > **Import** > **Import Doors of Access Level**, and click Browser to upload the Access Level Template.

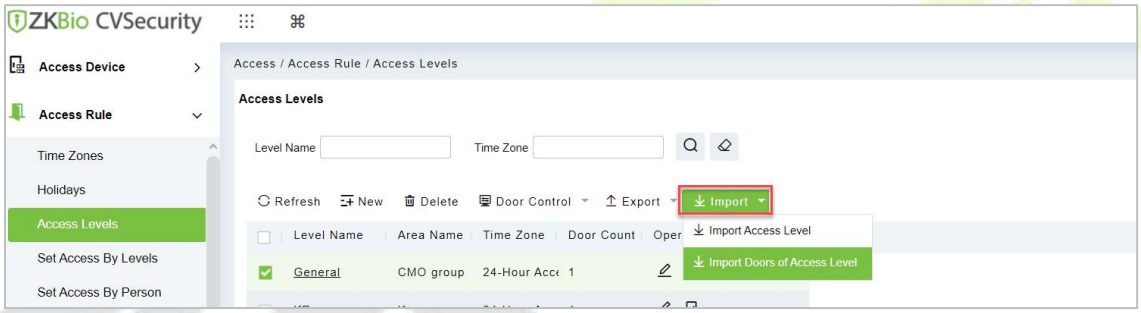


Figure 3- 71 Import the Doors of Access Level Template 1

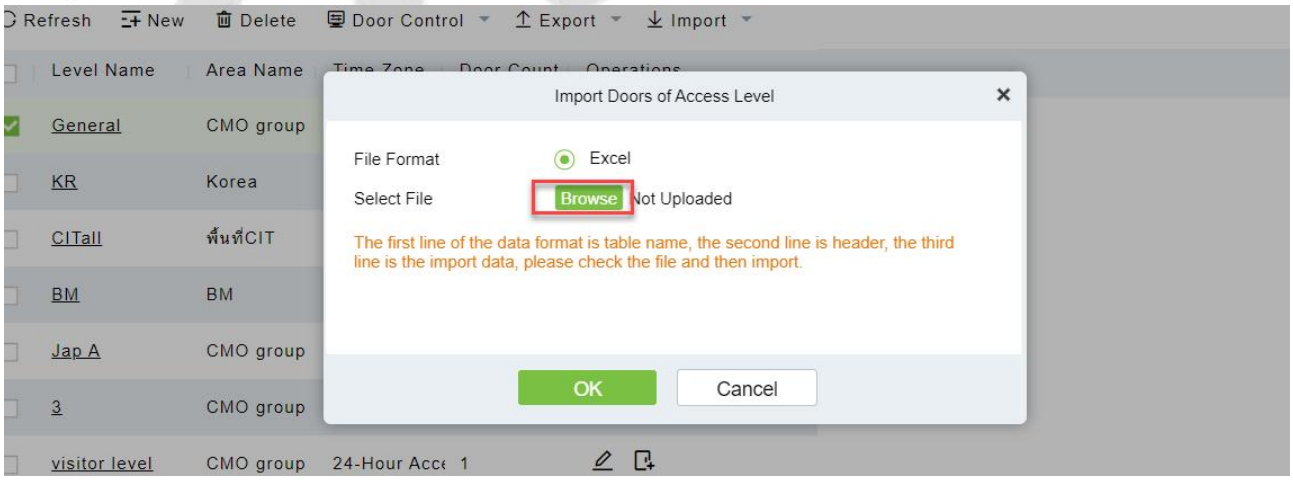


Figure 3- 72 Import the Doors of Access Level Template 2

Step 6: After the upload is successful, we can view the uploaded level as the following figure.

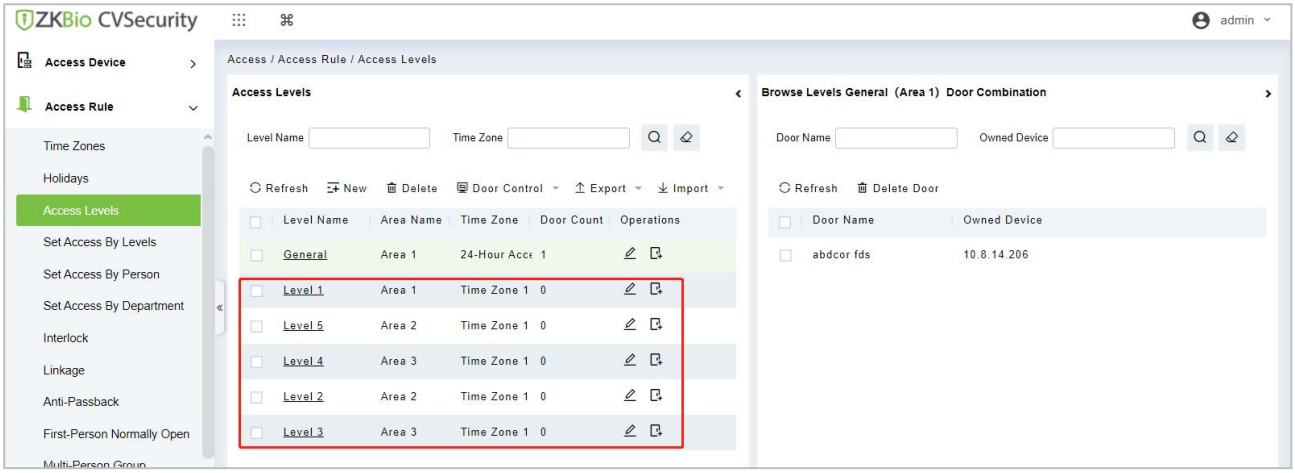


Figure 3- 73 Import the Doors of Access Level Template 3

3.4.4Set Access By Level

Permission assignment Manages the access level of personnel. After permission assignment, personnel can verify the door opening Operation.

You can assign user rights by user group or assign user rights by user group.

3.4.4.1Assign Personnel Rights by Permission Group

Assigning personnel permissions by permission group is used to define a set of open-door personnel for a permission group.

Describes Operation Step that assigns staff permissions by permission group in ZKBio CVSecurity.

●Operation Step:

Step 1: In the Access Control module, choose "**Access Rule>Set Access by Levels**".

Step 2: In the Operation column of the corresponding permission group, tap "**Add Personnel**". The Add personnel page is displayed. Select personnel as required, as shown in figure below.

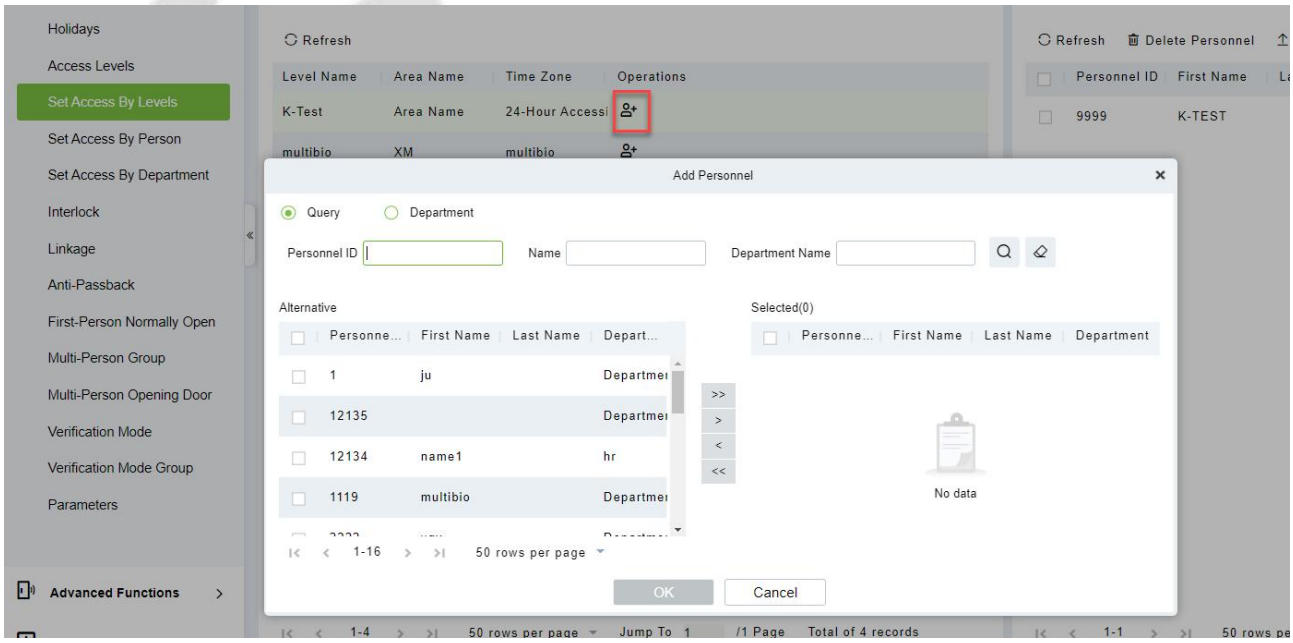


Figure 3- 74 Assigning Rights to Users by Rights Group

Step 3: Click **OK** to complete the assignment of personnel permissions.

3.4.4.2Delete Personnel

Select personnel ID, click **Delete**, and click **OK** to delete the personnel ID.

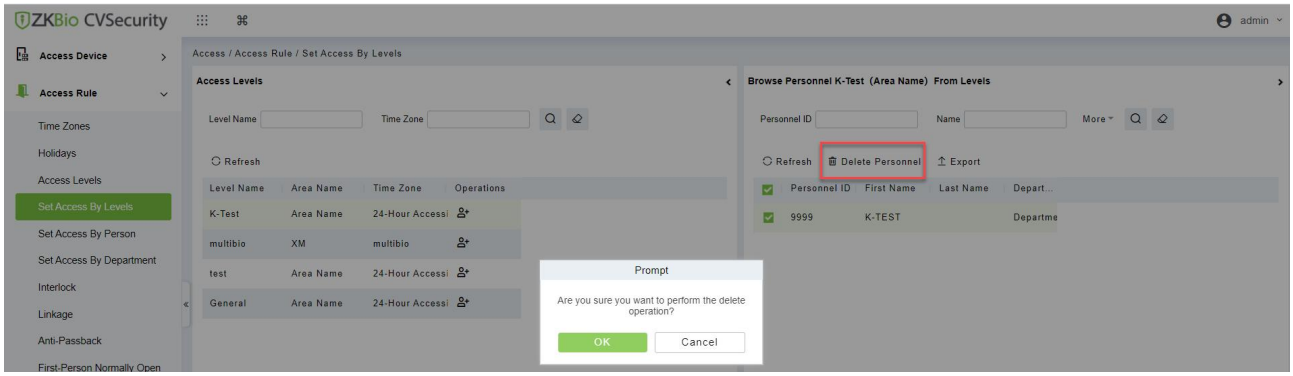


Figure 3- 75 Delete Personnel

3.4.4.3Export

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

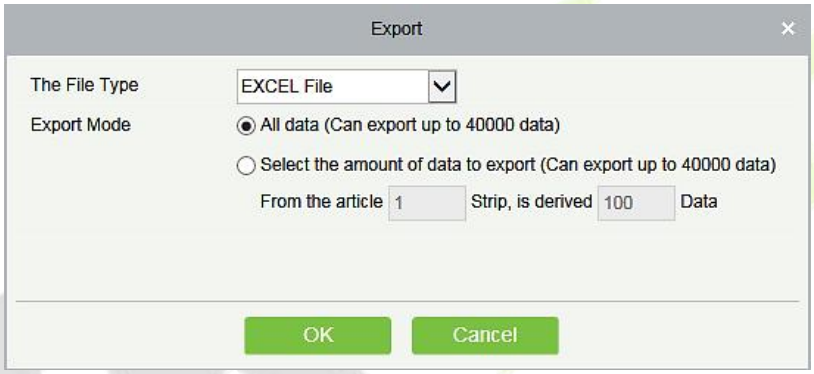
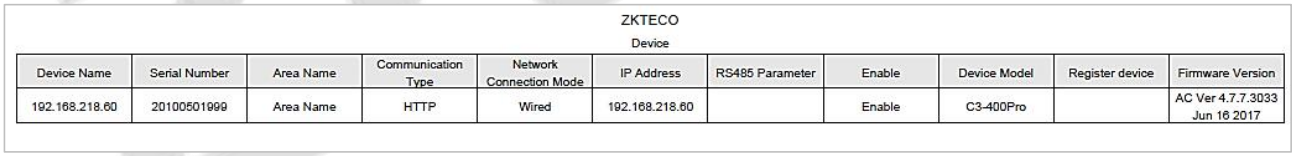


Figure 3- 76 Export



ZKTECO
Device

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

Figure 3- 77 Set Access level Allocation Export

3.4.5Set Access By Person

Assigning access level groups by person A permission set is used to define the access level set of a person.

This section describes Operation Step that assigns access control group permissions by person in ZKBio CVSecurity.

3.4.5.1Access Control Setting

● Operation Step:

Step 1: In the Access Control module, choose "**Access Control > Settings by Personnel**".

Step 2: In the Operation column of the Access Control group, click **"Add Access Control Group**". The page for adding access control groups is displayed. Select the Access Control group as required.

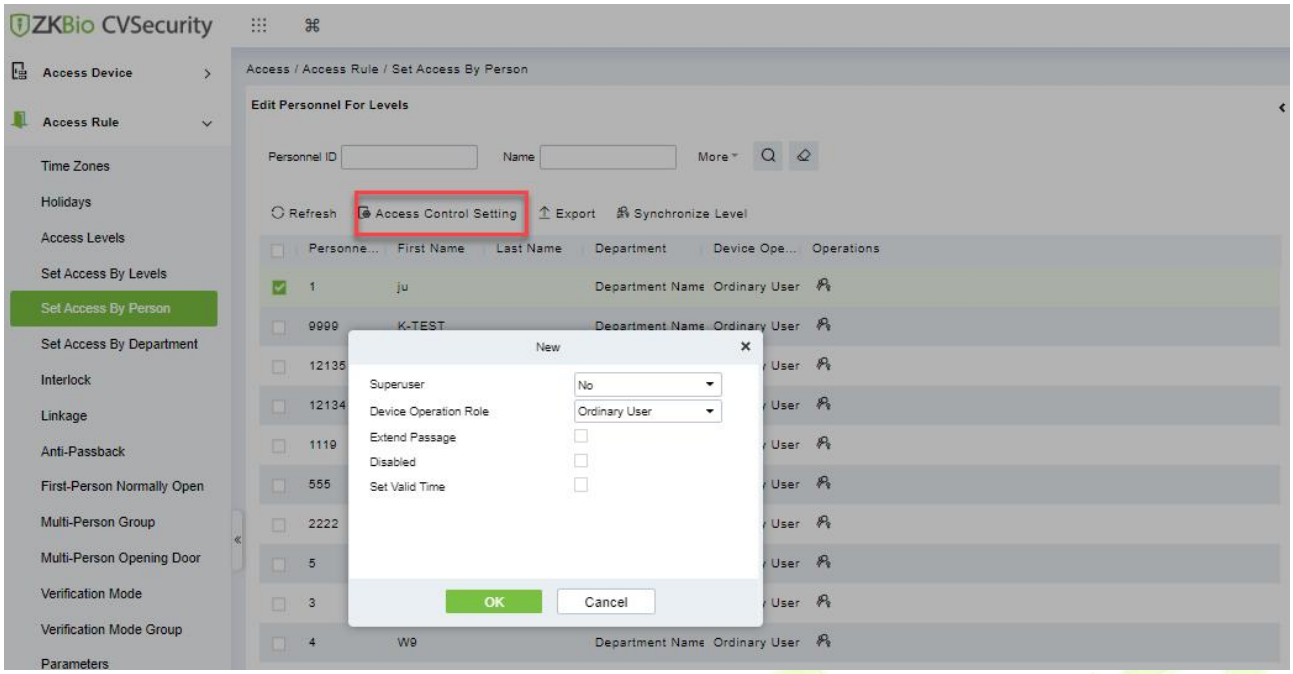


Figure 3- 78 Assigning Rights Groups by User

Step 3: Click **OK** to complete the assignment of personnel permissions.

3.4.5.2Add Level

Permission assignment Manages the access level of personnel. After permission assignment, personnel can verify the door opening Operation.

You can assign user rights by user group or assign user rights by user group.

Assign Personnel Rights by Permission Level

Assigning personnel permissions by permission group is used to define a set of open-door personnel for a permission group.

Describes Operation Step that assigns staff permissions by permission group in ZKBio CVSecurity.

●Operation Step:

Step 1: In the Access Control module, choose "**Access Rule>Set Access by Levels**".

Step 2: In the Operation column of the corresponding permission group, tap "**Add Levels**". The Add level page is displayed. Select personnel as required.

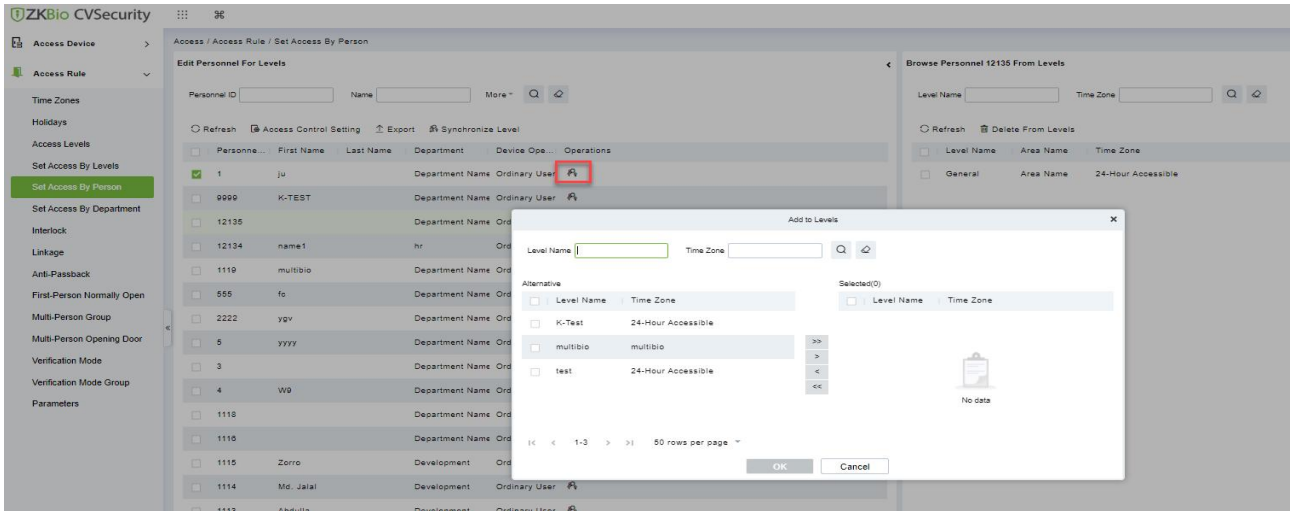


Figure 3- 79 Assigning Rights to Users by Rights Group

Step 3: Click **OK** to complete the assignment of level permissions.

3.4.5.3Delete from Level

Select level name, click **Delete**, and click **OK** to delete the level name.

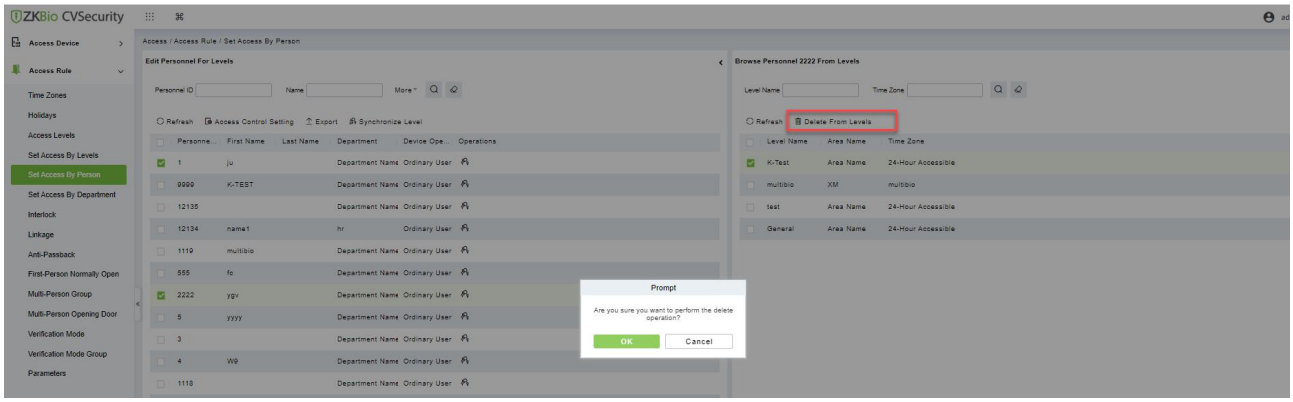


Figure 3- 80 Access Level Group by Person Delete

3.4.5.4Export

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

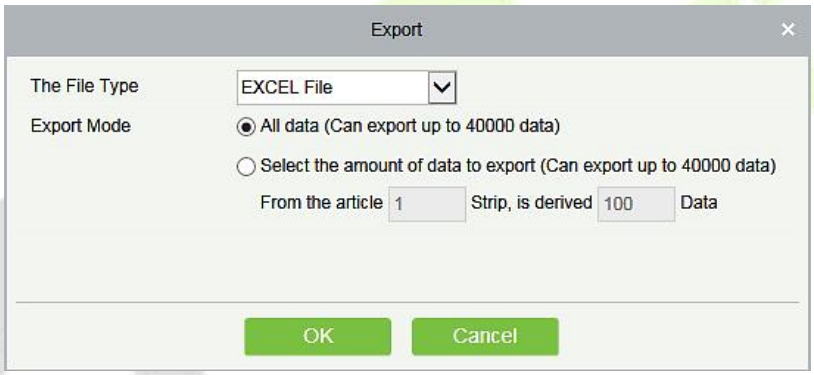


Figure 3- 81 Export

ZKTECO
Device

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

Figure 3- 82 Access Level Group by person Export

3.4.5.5Synchronize Level

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

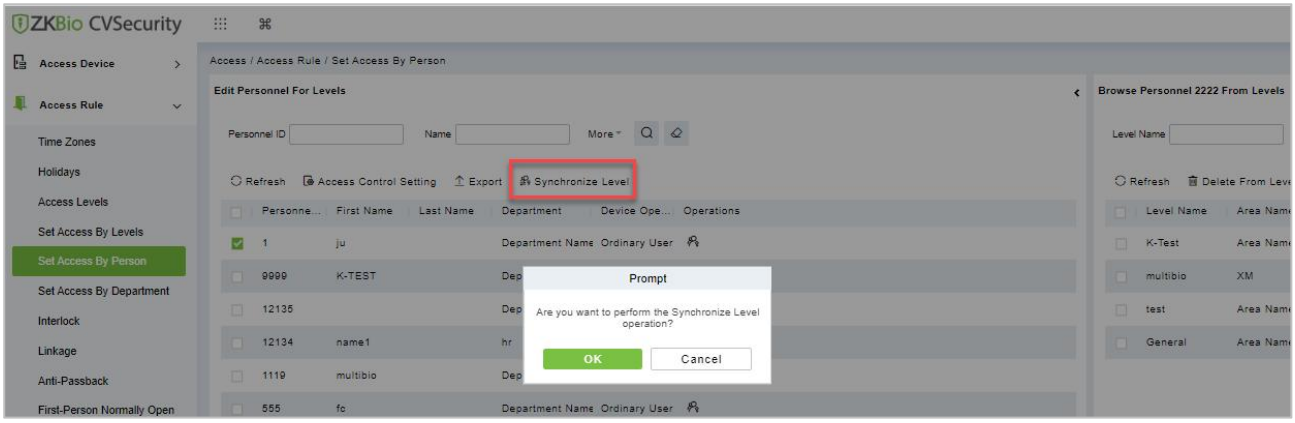


Figure 3- 83 Synchronize Level

3.4.6Set Access By Department

The access level group assigned by department defines the set of access levels for the personnel in the department.

This section describes Operation Step that assigns Access Control group permissions by person in ZKBio CVSecurity.

● Operation Step:

Step 1: In the Access Control module, choose "**Access Control > Set by department**".

Step 2: In the Operation column of the Access Control group, click **"Add Access Control Group"**. The page for adding Access Control groups is displayed. Select the Access Control group as required.

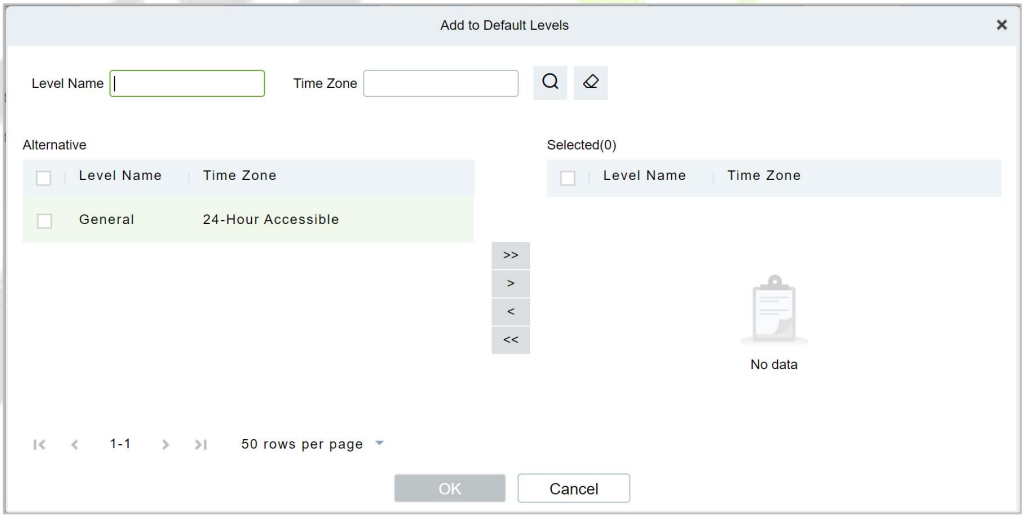


Figure 3- 84 Assigning Rights Groups by Department

Step 3: Click **OK** to complete the assignment of department permissions.

3.4.6.1Add Default Level

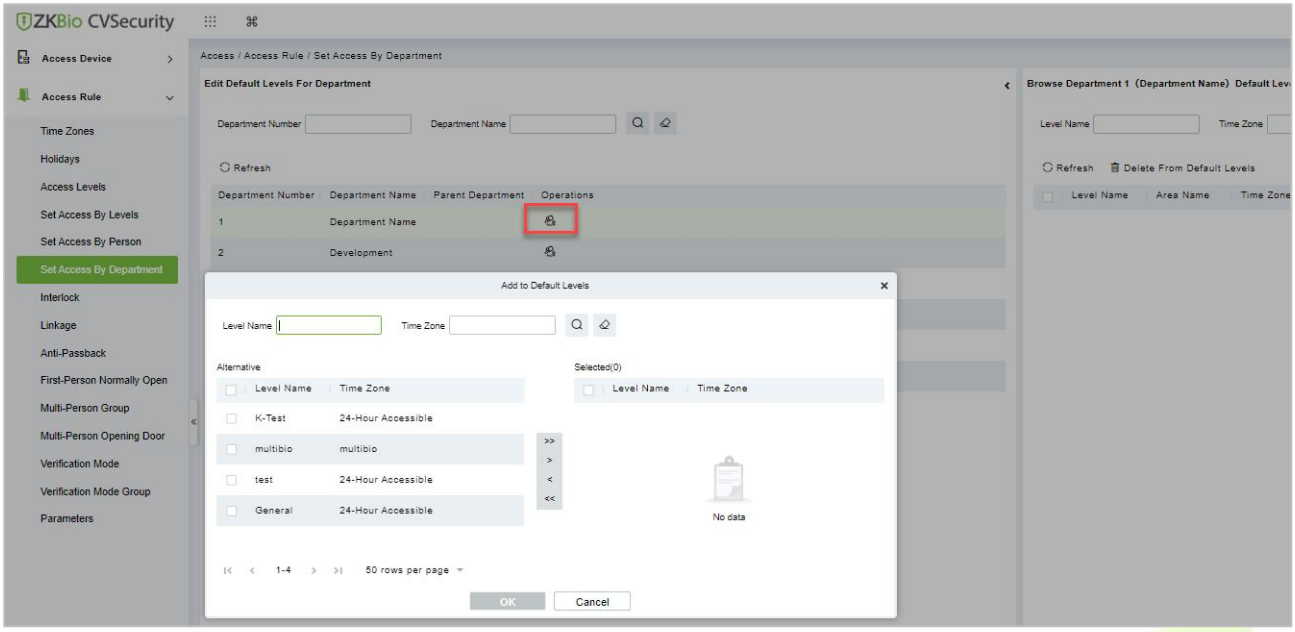


Figure 3- 85 Add Default Level Groups by Department

3.4.6.2 Delete Default Level

Select delete default level name, click **Delete**, and click **OK** to delete the default level name.

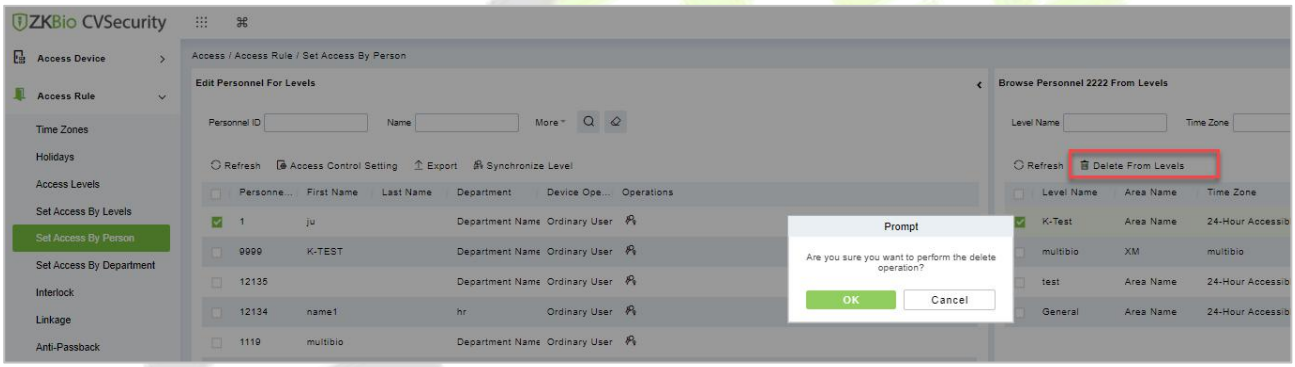


Figure 3- 86 Delete Rights Groups by Department

3.4.7 Interlock

Set interlock control between two or more doors on the access controller device: To verify the opening of a door, ensure that all other doors interlocked with the door are closed; otherwise, the door cannot be opened.

This section describes the Step of adding interlock effect in ZKBio CVSecurity.

● The Premise Conditions:

The door opening/closing state monitoring is realized by detecting the door magnetic state. Therefore, interlock function requirements:

1. The door status sensor at the device end must be correctly installed
2. In door setting on the software side, the status of the door status sensor must be set to normally open or normally closed (based on the actual installation).

3.4.7.1 Add (New)

● **Operation Step:**

Step 1: In the Access Control module, choose "**Access Control > Interlock**" and click New.

Step 2: Select the specified device.

Instructions:

When you add a device for which interlock has been configured, the device cannot be found in the drop-down list. After the configured interlock information is deleted, the device is returned to the drop-down list.

Interlock Settings vary with the number of doors controlled by the device:

Single-door controller: no interlock setting

Dual door controller: 1-2 two door interlock Settings

Four-door controller: 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, 1-2-3-4 four-door interlock, 1-2 and 3-4 door interlock

Step 3: Select the interlock rule, and click **OK** to complete the settings, as shown in figure below. The new interlock Settings are displayed in the list.

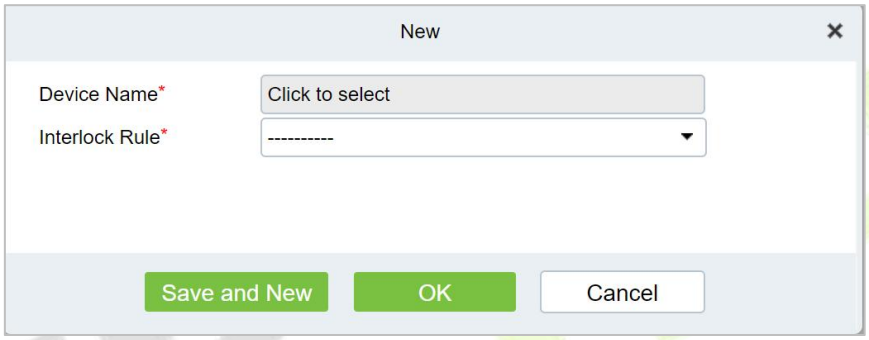


Figure 3- 87 Adding Interlock Configuration

Parameter	How to set up
Device Name	You can customize the name of the Device
Interlock Rule	Select the configured interlock rule.

Table 3- 12 Description of interlock

3.4.7.2Delete

Select interlock, click **Delete**, and click **OK** to delete the interlock.

3.4.8Linkage

The use method and scenario of linkage are flexible. After a specific event is triggered by an input point in the **Access Control** system, a linkage action will be generated at the specified output point to control events such as verification opening, alarm and abnormality in the system.

This section describes how to add Step to the linkage effect in ZKBio CVSecurity.

Add (New)

● **The Premise Conditions:**

Before adding a linkage configuration, perform the following operations:

Step 1: Add Settings for binding cameras to access control devices, input points, output points, and readers.

Step 2: Optional: In the **System Management** module, choose "**System Management > Mail**

Management" to set the sender server. The Step of setting the sender server is as follows:

In the System Management module, choose 'system Management > Mail Management".

Click "**Sender Server Settings**" to pop up the sender server Settings interface.

On the Sender server Settings screen, set parameters as required, as shown in figure below. For parameter Settings, see Table 3-13.

After setting, click "**Test connection**" to receive the email, indicating that the test has passed.

Step 3: Click **OK** to finish setting email parameters.

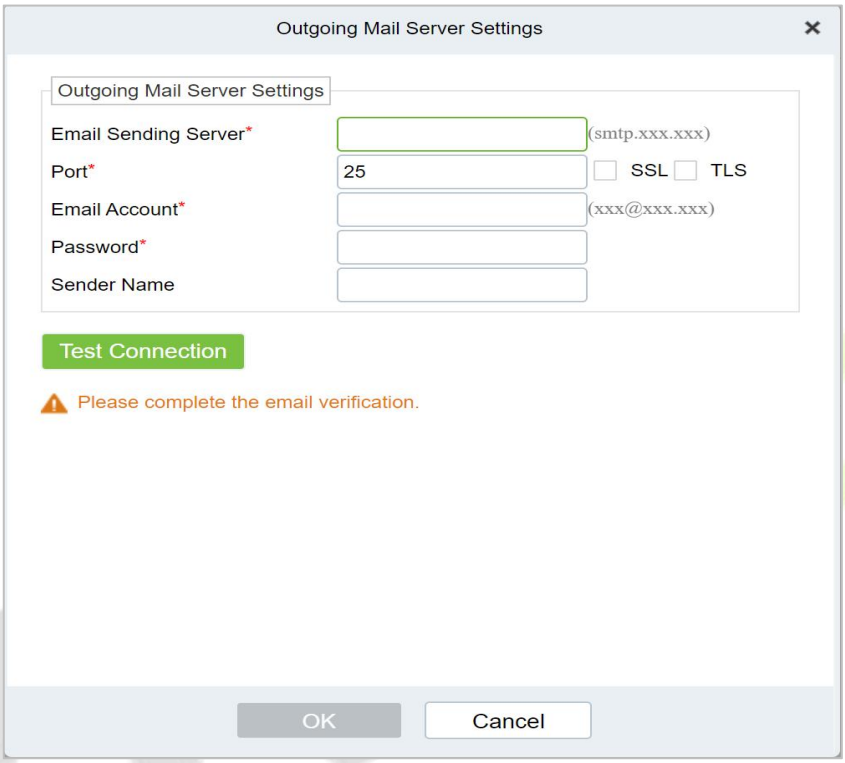


Figure 3- 88 Mailbox Parameters

Parameter	How to set up
Email server address/port	You can customize the email server address and port. The email products that provide the SMTP server can be used.
Email username and password	Enter the user's name and password for the mailbox.
Name of sender	Sets the name of the sender on the received message.

Table 3- 13 Mailbox Management Parameters

● **Operation Step:**

Step 1: In the Access Control module, choose "**Access Control > Linkage**".

Step 2: On the linkage setting screen, click **Add**, as shown in figure below. Table 3-14 and Table 3-15 refer to the linkage parameters.

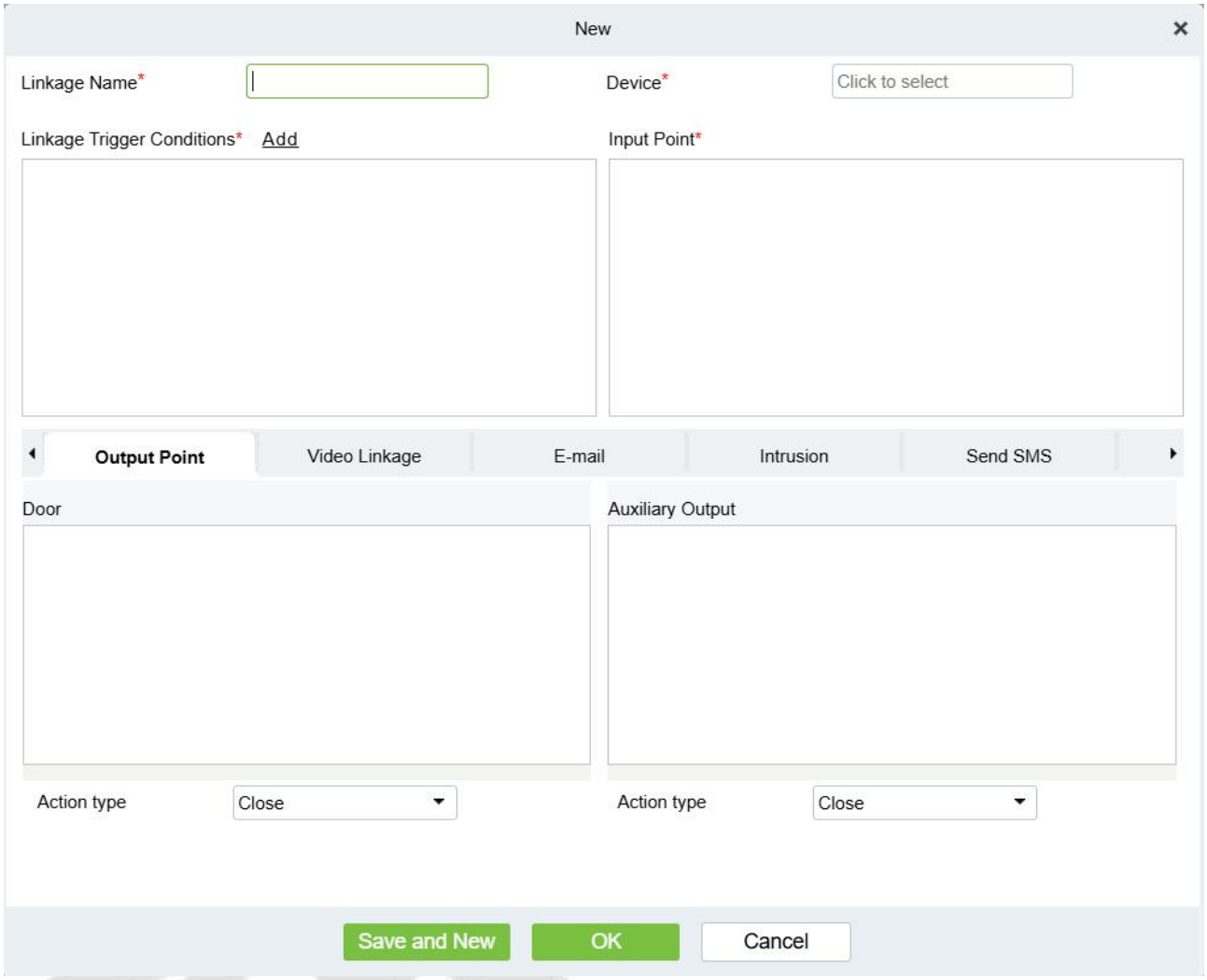


Figure 3- 89 New Linkage Configuration

Parameter	How to set up
Linkage Name	You can customize the linkage name for easy query.
Device	Custom Select an added access control device.
Linkage Departure Condition	Select the condition triggered by the linkage Operation, that is, the event type generated by the selected device.
Input Point	Select the input point to set device input.
Output Point	Select the output point to set device output.
Linkage Action Setting	You can set the linkage action, including Operation, video linkage, and email. Table 3-3 describes the configurations of the three modes.

Table 3- 14 New Linkage Parameters

Parameter	How to set up
The Output Point of Operation	Set the output action type: close, open, normally open. Sets the delay time if the output action is on.
Video Linkage	Pop-up video and display duration: Select pop-up video on the real-time monitoring screen and set the pop-up duration. Video recording and Video Duration: Select Video recording to set the video duration. Capture: Set linkage action whether to take a photo: If a photo is taken, you also

Parameter	How to set up
	need to set whether to pop up on the real-time monitoring interface and the display duration.
E -Mail	Set the email address that receives the linkage content when a linkage event occurs.
Intrusion	Configure the action of arming an area after an event is triggered
Send SMS	Configure the recipient of the SMS when the event is triggered
Line	Configure the recipient of the Line when the event is triggered
WhatsApp	Configure the recipient of the WhatsApp when the event is triggered

Table 3- 15 Setting Linkage Actions

Step 3: Click **OK** to complete the linkage configuration.

3.4.8.1 Delete

Select linkage, click **Delete**, and click **OK** to delete the linkage.

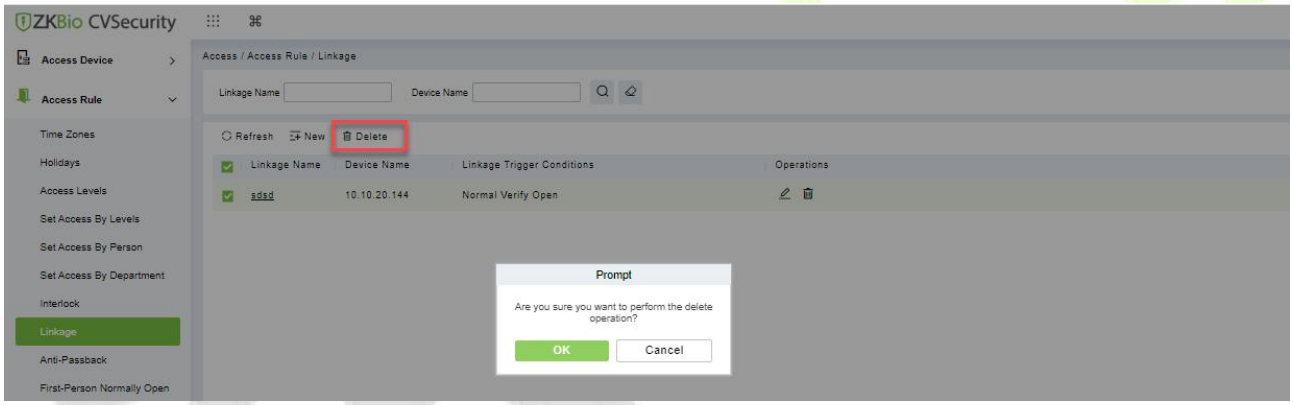


Figure 3- 90 Adding Interlock Configuration

3.4.9 Anti-Passback

Some occasions require the personnel that brush card to verify, brush card to come in from a door must brush card to go out from another door, brush card record must enter a strict correspondence. This function can be used when users enable it in the settings. It is generally used in special units, scientific research, bank vaults and other occasions.

This section describes the Step of adding the Anti-Passback effect in ZKBio CVSecurity.

3.4.9.1 Add (New)

● **Operation Step:**

Step 1: In the Access Control module, choose "**Access Control > Anti-Passback**" and click New.

Step 2: Select the specified device.

Instructions:

When you add an Anti-Passback device, the configured Anti-Passback device is not displayed in the device list. After the antisubmarine information is deleted, the device returns to the device list.

The Anti-Passback setting varies with the number of gates controlled by the equipment:

Anti-Passback setting of single door controller: Anti-Passback between readers

Two controllers: door 1 Anti-Passback between readers, door 2 Anti-Passback between readers, door 1

and door 2 Anti-Passback

Four door controllers: door 1 and door 2 Anti-Passback, door 3 and door 4 Anti-Passback, door 1/ door 2 and door 3/ door 4 Anti-Passback, door 1 and door 2/ door 3/ door 4 Anti-Passback, door 1 and door 2/ door 3/ door 4 Anti-Passback, door 1/ door 2/ door 3/ door 4 Anti-Passback reader

Step 3: Select the Anti-Passback rule and click **OK** to complete the settings. The new Anti-Passback Settings are displayed in the list.

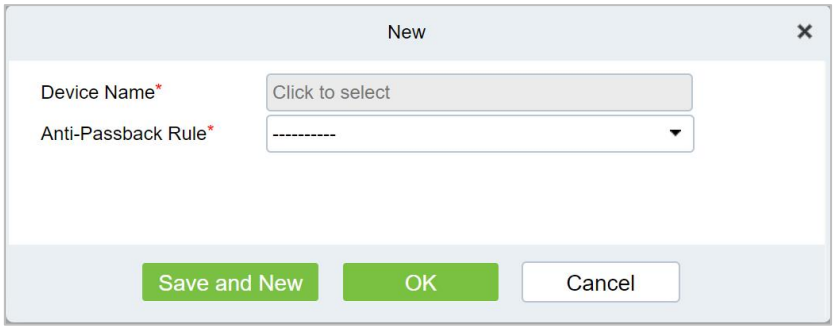


Figure 3- 91 Adding the Anti-Passback Configuration

3.4.9.2Delete

Select device, click **Delete**, and click **OK** to delete the device.

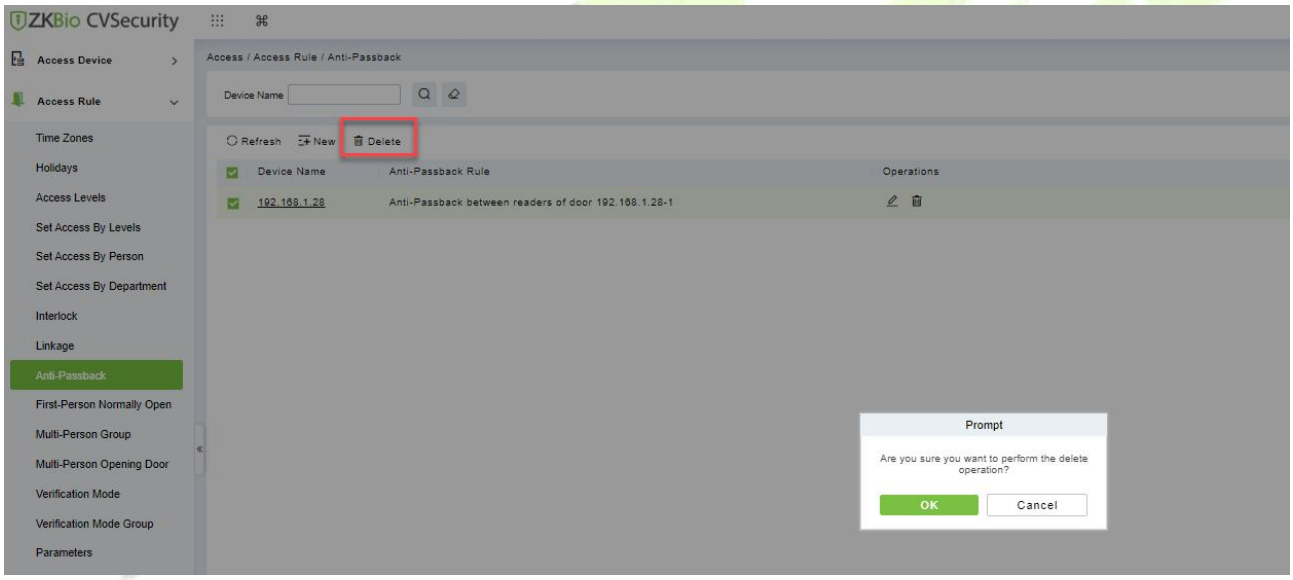


Figure 3- 92 Anti-Passback Delete

3.4.10First-Person Open

In the specified period, after the verification of the first person with normally open permission, the door normally open, the end of the valid period of the door automatically closed.

This section describes how to add Step in ZKBio CVSecurity.

● **The Premise Conditions:**

The time range has been set for the Access Control module.

3.4.10.1Add (New)

● Operation Step:

Step 1: In the Access Control module, choose "**Access Control > First person normally Open**" and click New.

Step 2: Select the specified device, add Settings for the specified door, and select the normally open time period, and click **OK**, as shown in figure below.

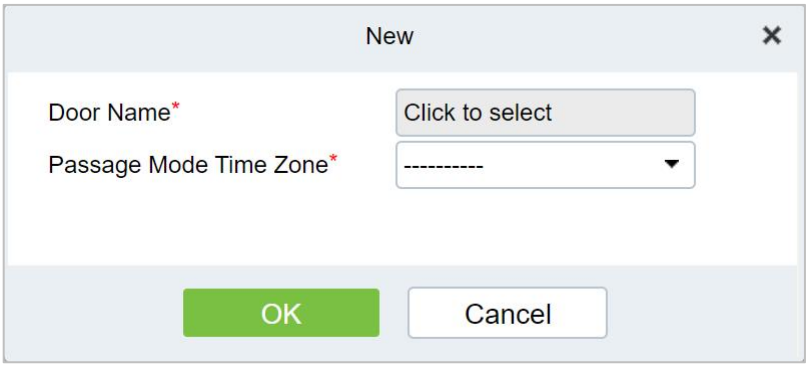


Figure 3- 93 Configuring the First Person to Open the Door

Step 3: Click "**Add People**" on the interface of "**Opening of the first person**". After adding people, click **OK** to complete the setting of "opening of the first person".

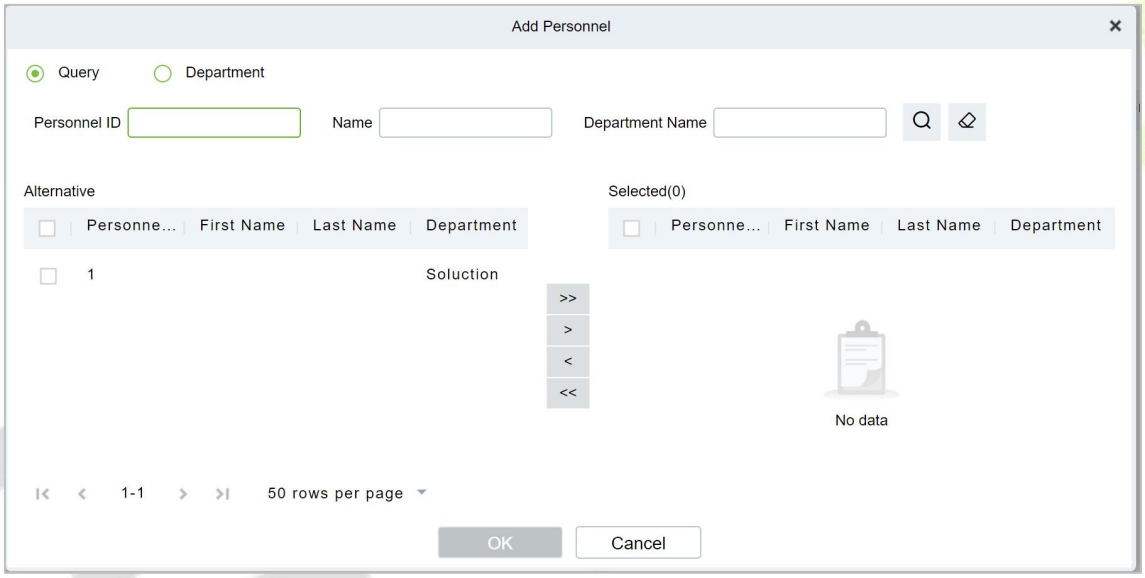


Figure 3- 94 Adding A First Person Normally Open Person Configuration

3.4.10.2Delete

Select personnel ID, click **Delete**, and click **OK** to delete the personnel ID.

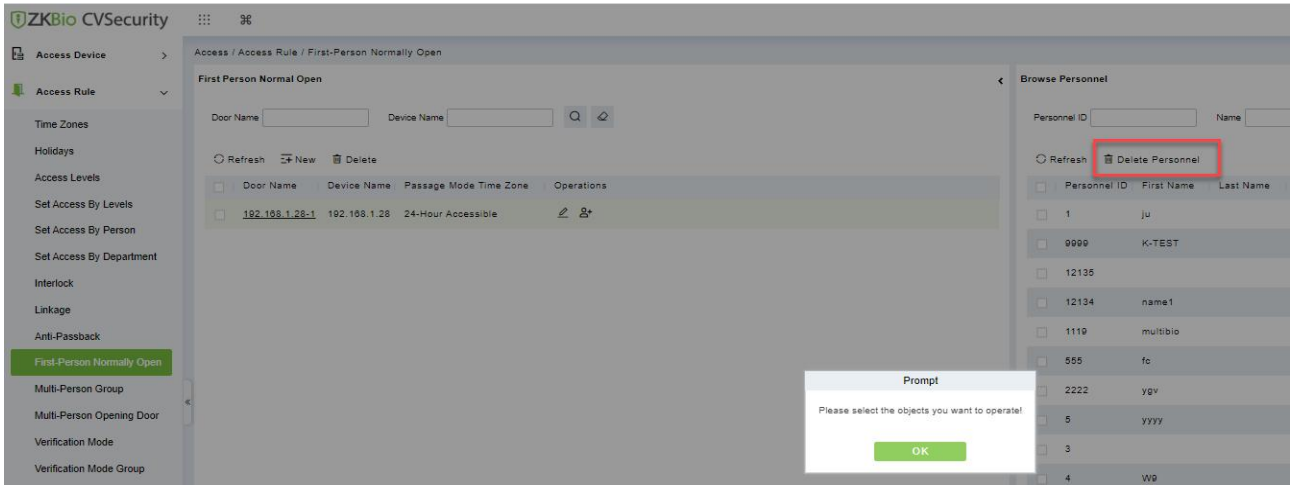


Figure 3- 95 Delete Person Normally Open Person Configuration

3.4.11 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 other valid combination) will interrupt the procedure and you need to wait 10 seconds to restart verification. It will not open by verification by only one of the combinations.

3.4.11.1 Add (New)

Step 1: Click **Access Rule** > **Multi-Person Group** > **New** to access the following edit interface:

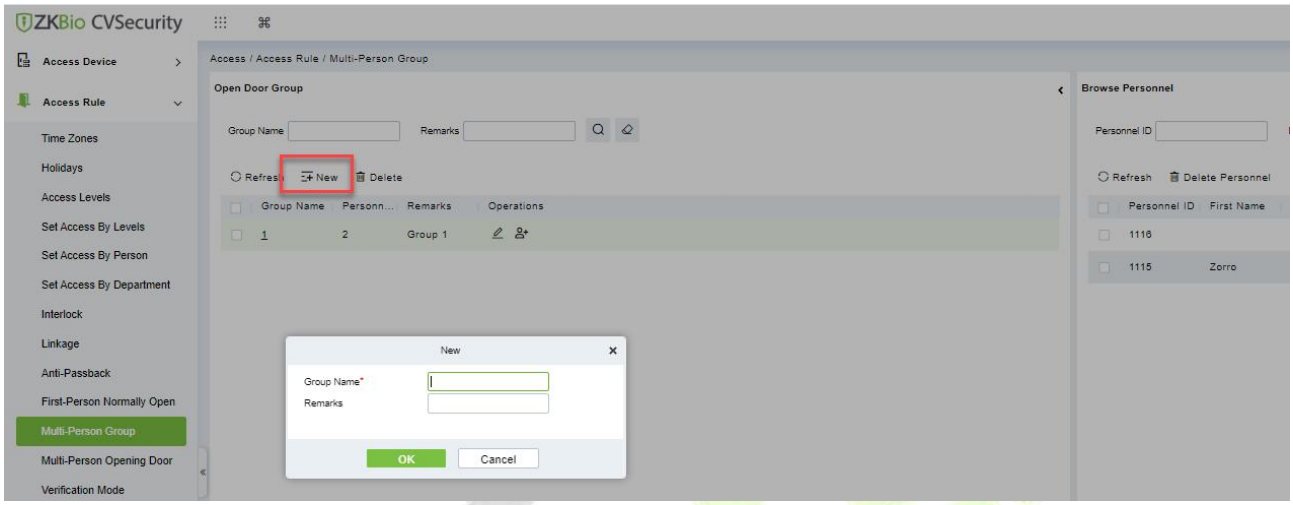


Figure 3- 96 Adding A Multi-Person Group

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.

Step 2: Click **Add personnel** under Related Operations to add personnel to the group.

Step 3: After selecting and adding personnel, click **OK** to save and return.

✍**Note:** A person can only be grouped into one group.

3.4.11.2 Edit

Click **Access Rule** > **Multi-Person Group** > **Edit** after selecting the required section in the interface.

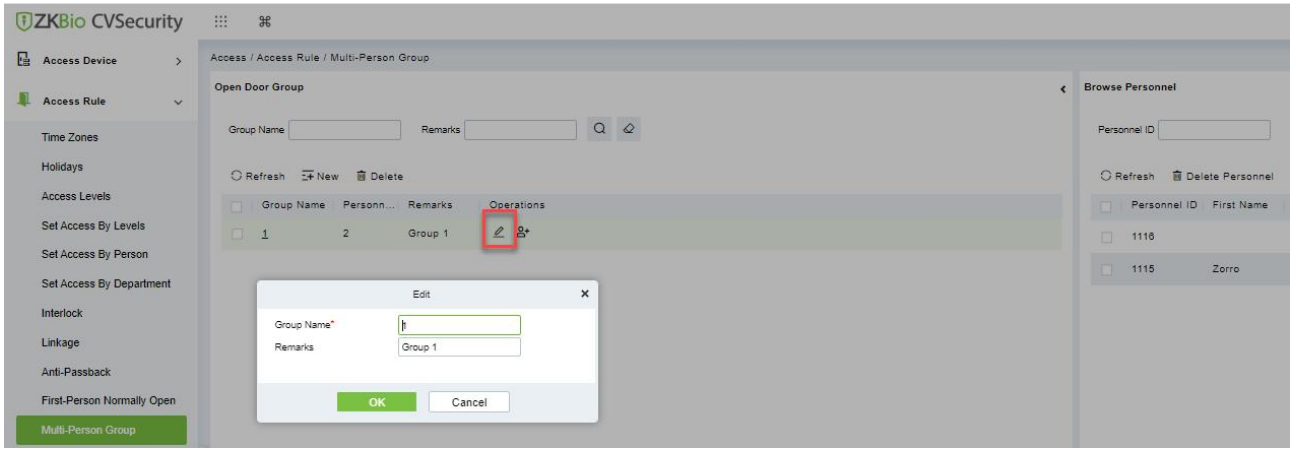


Figure 3- 97 Edit Multi-Person Group

3.4.11.3Add Personnel

Click **Access Rule** > **Multi-Person Group** > **Add Personnel** after selecting the required section in the interface.

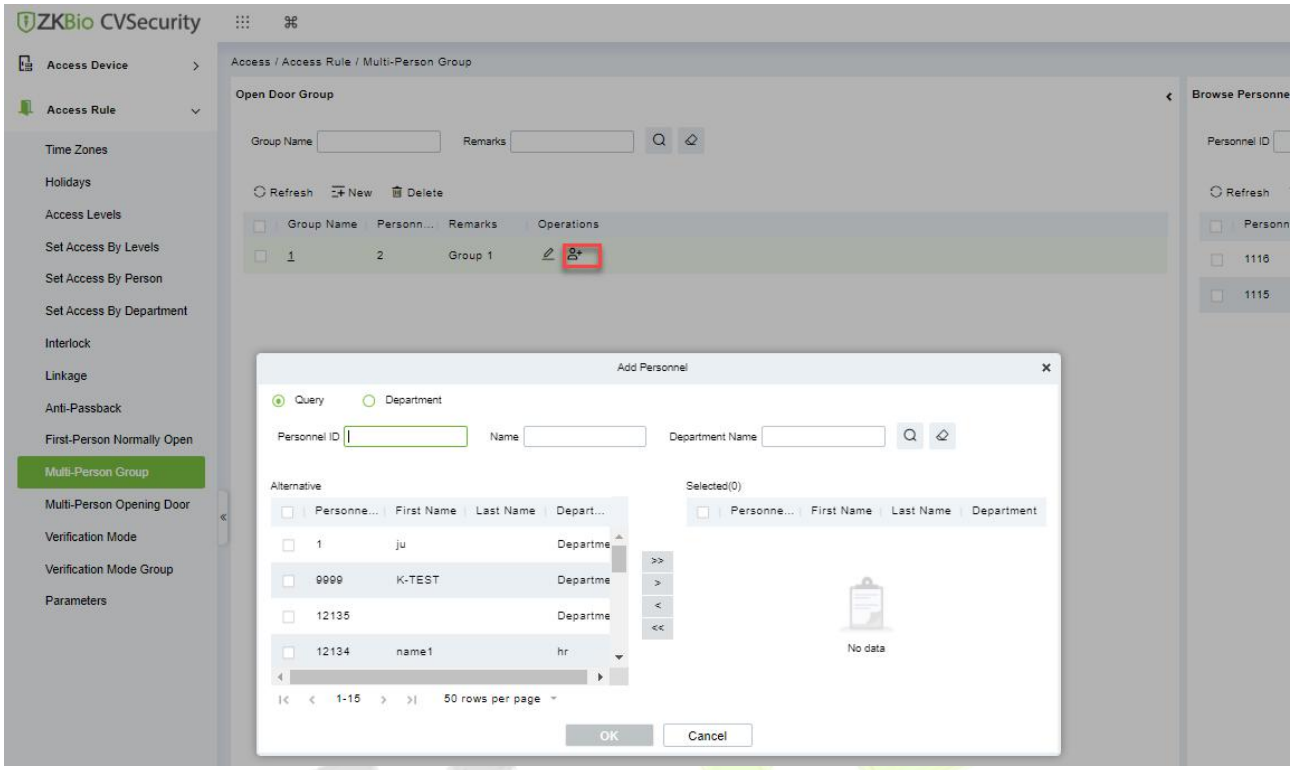


Figure 3- 98 Adding A personnel for Multi-Person Group

3.4.11.4Delete

Click **Access Rule** > **Multi-person group** > **Delete** after selecting the required section in the interface.

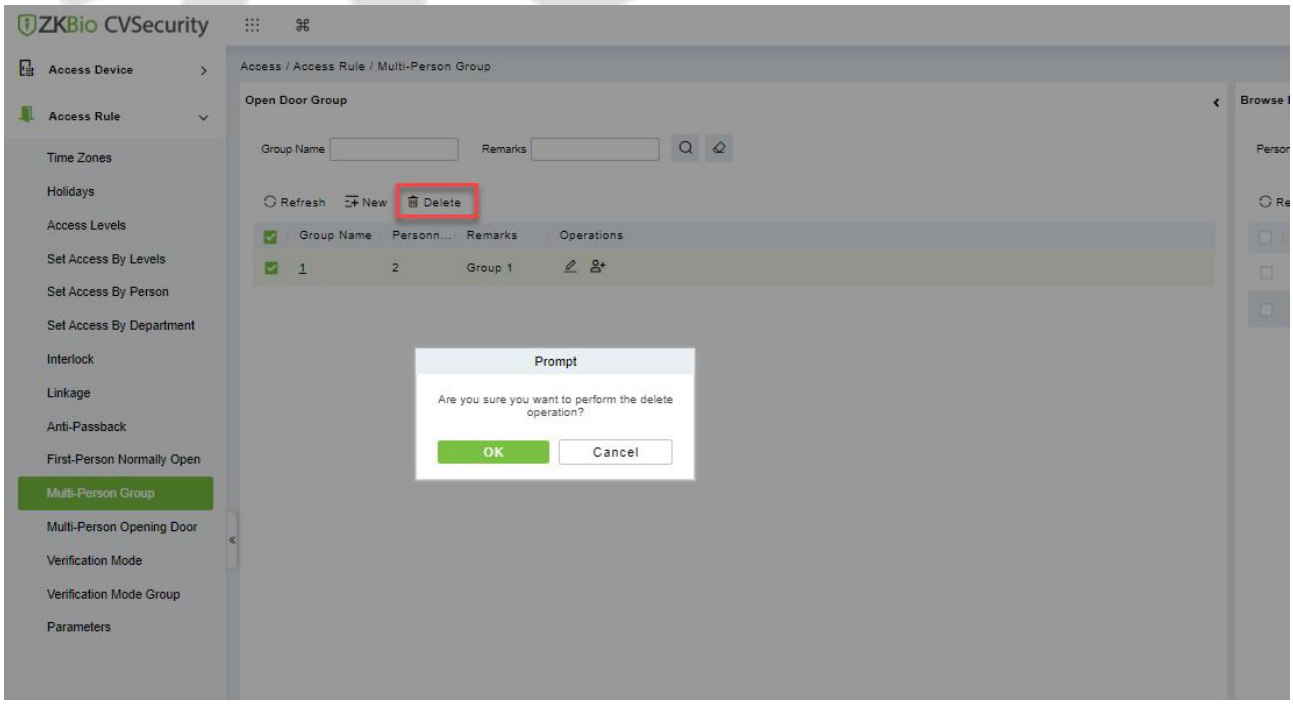


Figure 3- 94 Delete A Multi-Person Group

3.4.12Multi-Person Verification

In a specific scenario, it is necessary for more than one person to be present at the same time to verify their identity before they can open the door through permission verification.

● **Instructions:**

1. In an application scenario where, multiple users are required to verify their identities before opening the door, the authentication process is limited to N (no more than 5) by grouping people into groups.
2. In practice, if all the personnel to be verified are of the same type or level, it can be verified by multiple people in a single group. If there are different categories or levels of personnel, you can set a certain number of personnel in each group to achieve verification.
3. Before the multi-party door verification rule is reached, if the verification fails during the process, wait 10 seconds for the verification again.

3.4.12.1 Add (New)

Step 1: In the **Access Control** module, choose "**Access Rule > Multiple Door Opening Personnel Group**" and click **New**. After filling in the corresponding parameters, click **OK** to save the settings.

Step 2: Click "**Add Personnel**" on the right of the list of created multi-person door opening personnel, select the personnel to be added to the group in the pop-up function, and click **OK** to save the settings.

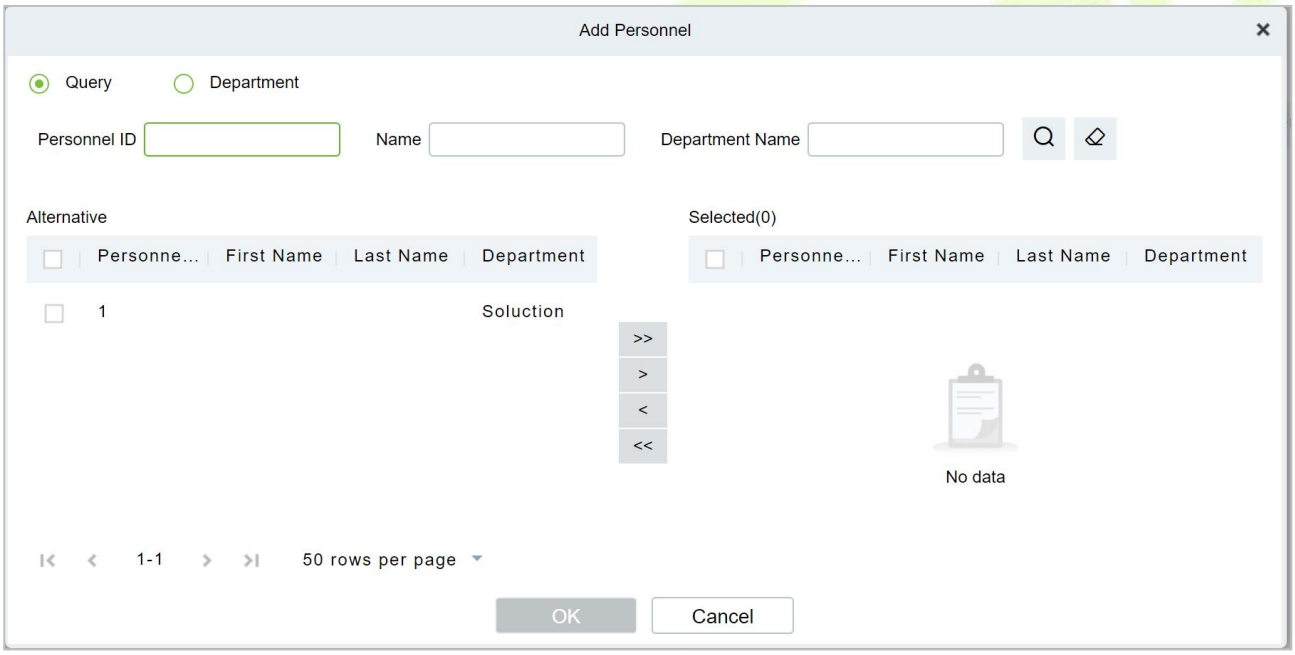


Figure 3- 100 Adding Multiple Door Openers

Step 3: In the multi-person door opening interface, click **Add**, set permissions for multi-person door opening personnel group.

Step 4: On the page for adding multiple door users, select the specified door, group information for multiple door users, and the number of verification personnel for each group, and click **OK** to save the settings.

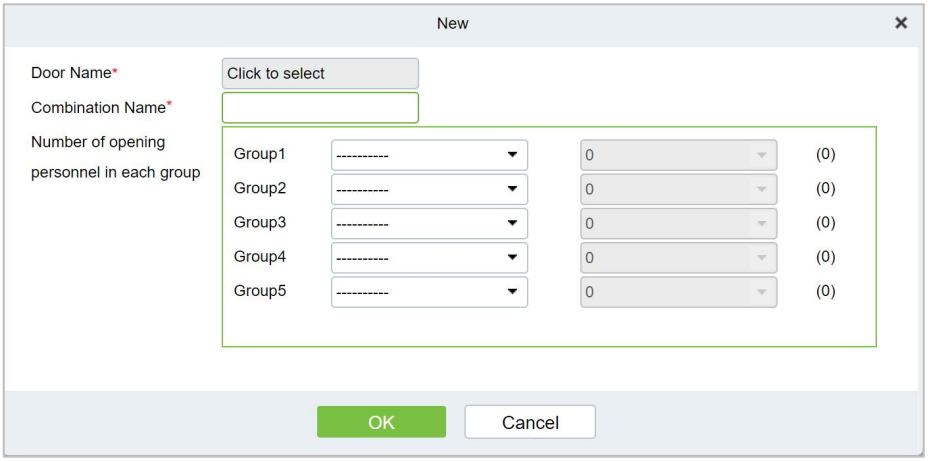


Figure 3- 101 Adding Multiple Door Openers

Step 5: In the **Access Control** module, choose "**Access Rule > Authentication Mode Rule**" and click **Add** to set the access control authentication rule for the corresponding period.

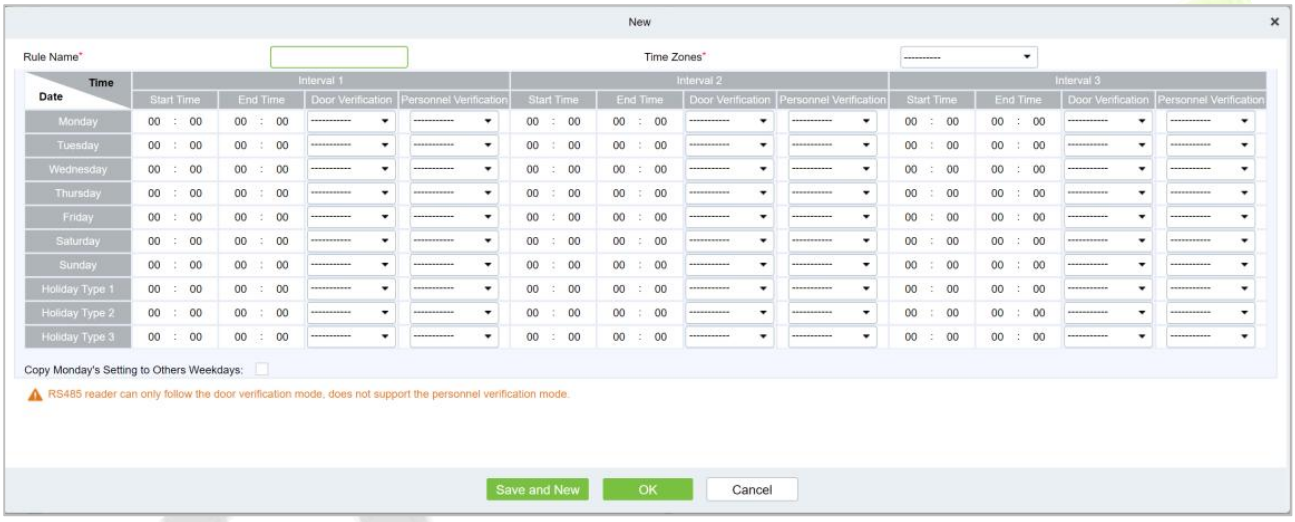


Figure 3- 102 Delete A Multi-Person Group

Step 6: Click **Add Door** on the right of the created authentication mode rule, select a door, and set the authentication mode rule for the door.

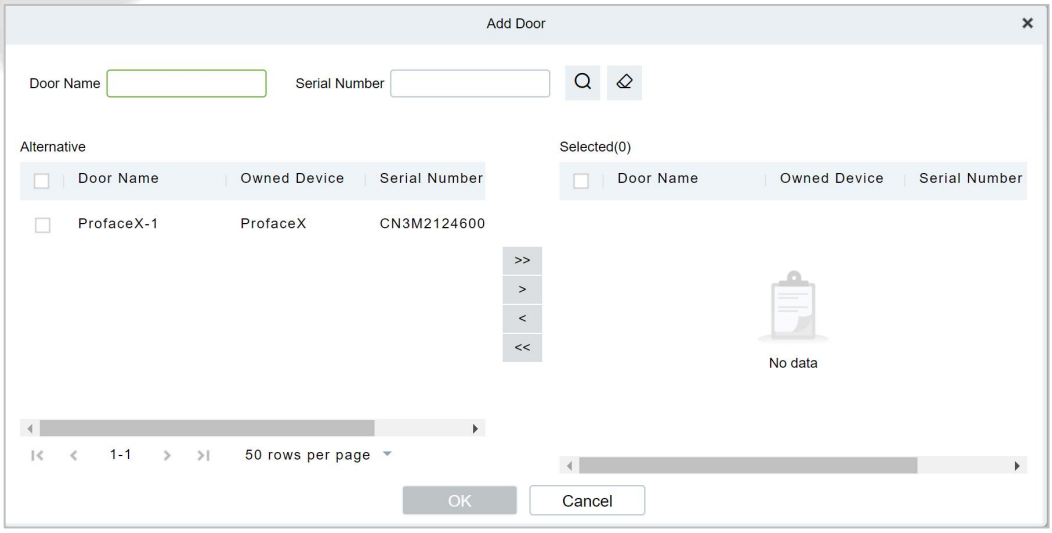


Figure 3- 103 Verification Rule Configuration for Adding Multiple Door Openers

Step 7: click **OK** to save the settings.

3.4.12.2Delete

Click **Access Rule** > **Multi-person opening door** > **Delete** after selecting the required section in the interface.

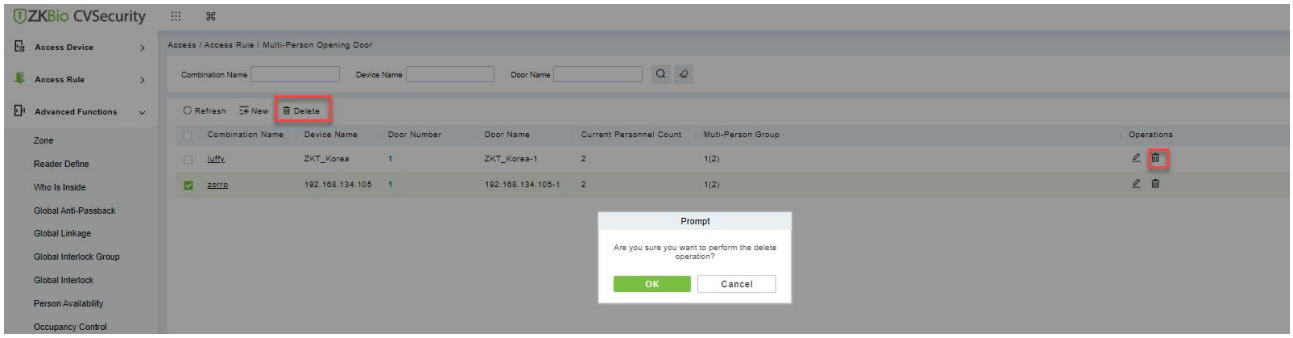


Figure 3- 104 Delete A Multi-Person Group

3.4.13Open Door Duration

Set different door opening durations based on personnel.

Applicable Scenarios: Logistics warehouses, parking facilities, factory workshops, and other environments with varying operational requirements.

Example: loading and unloading operations can be assigned longer durations (e.g., 60 seconds) to accommodate forklifts or multiple personnel, while standard access uses shorter durations (e.g., 10 - 15 seconds).

Step: Enter Access → Access Rule → Open Door Duration, click "New" to add personnel, select the corresponding door, and configure the opening duration for both the door and the personnel. As shown in the figure below, click "OK" to save and exit.

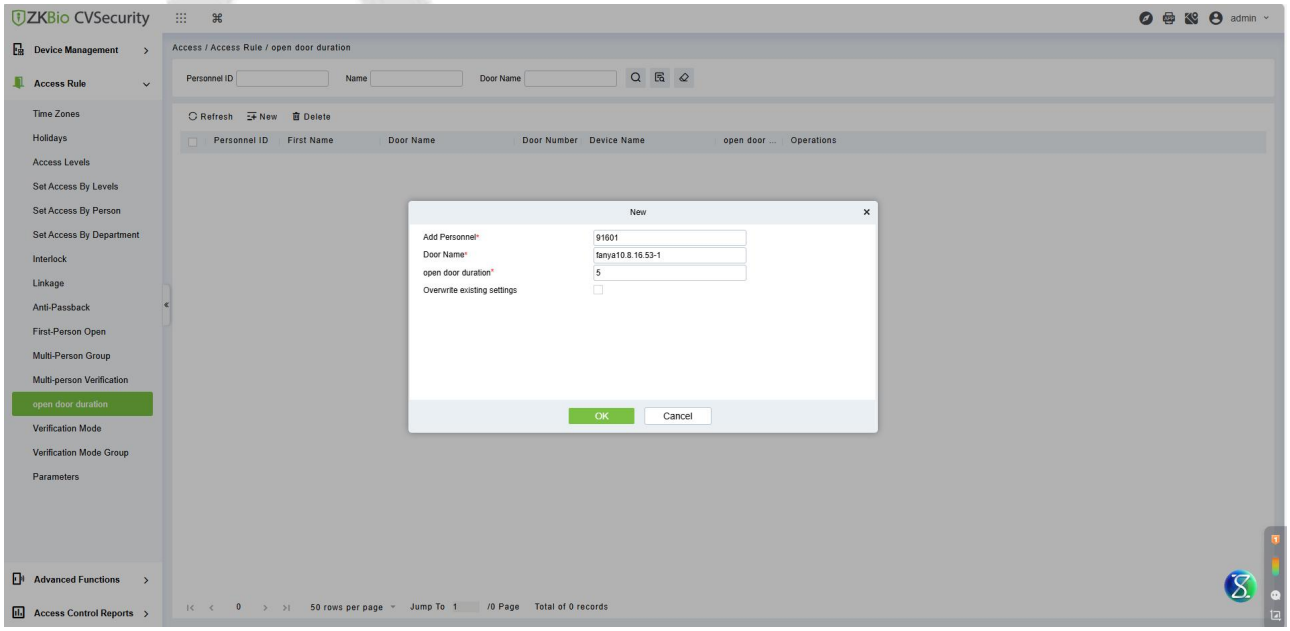


Figure 3- 105 Open Door Duration

3.4.14Verification Mode

You can set verification modes for doors and personnel separately in a specified time segment.

3.4.14.1New

Step 1: Click **Access Rule** > **Verification Mode** > **New** to go to the page for adding a verification mode rule.

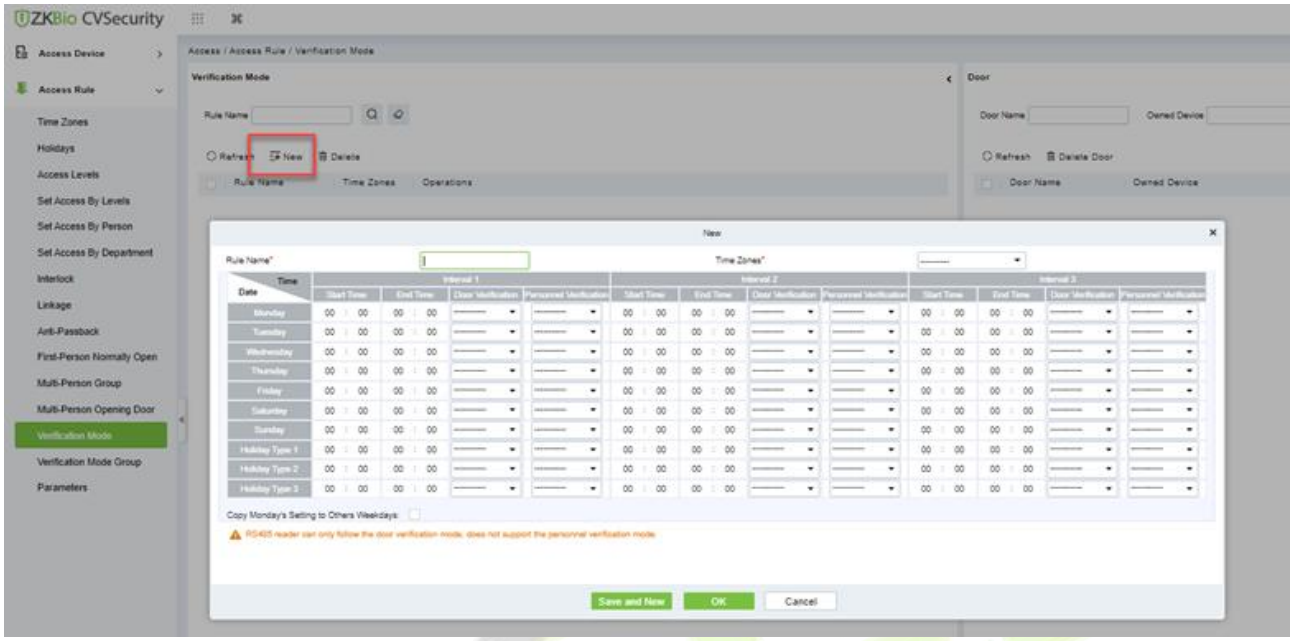


Figure 3- 106 Add Verification mode

Step 2: Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.

Step 3: Click **OK** to finish the setting.

On the list page, you can add or delete doors in the verification mode rule.

3.4.14.2Verification Mode Group

You can set verification modes for doors and personnel separately in a specified time segment.

● Steps:

Step 1: Click **Access Rule** > **Verification Mode** > **New** to go to the page for adding a verification mode rule.

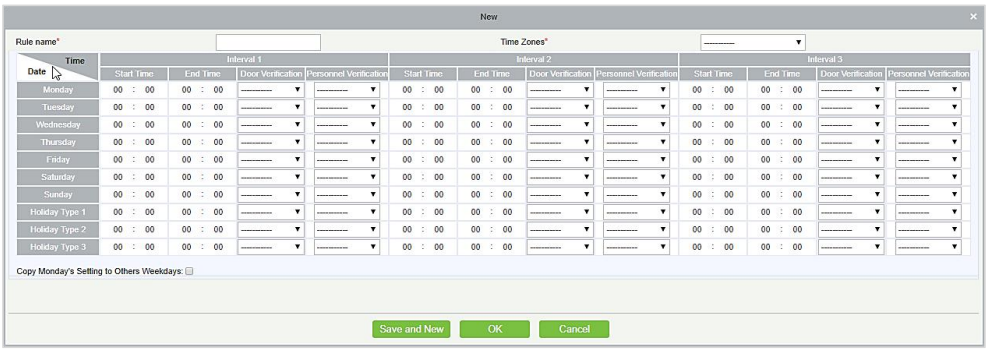


Figure 3- 107 Add Verification mode Group

Step 2: Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.

Step 3: Click OK to finish the setting.

On the list page, you can add or delete doors in the verification mode rule.

Note: If a rule includes the verification mode for personnel, you cannot select doors with the RS485 readers when adding doors. You can modify only the configuration on the reader setting page before adding doors.

● Verification Mode Group:

Set appropriate personnel for configured verification mode rule.

3.4.15 Parameters

Click **Access Rule** > **Parameters** to enter the parameter setting interface:

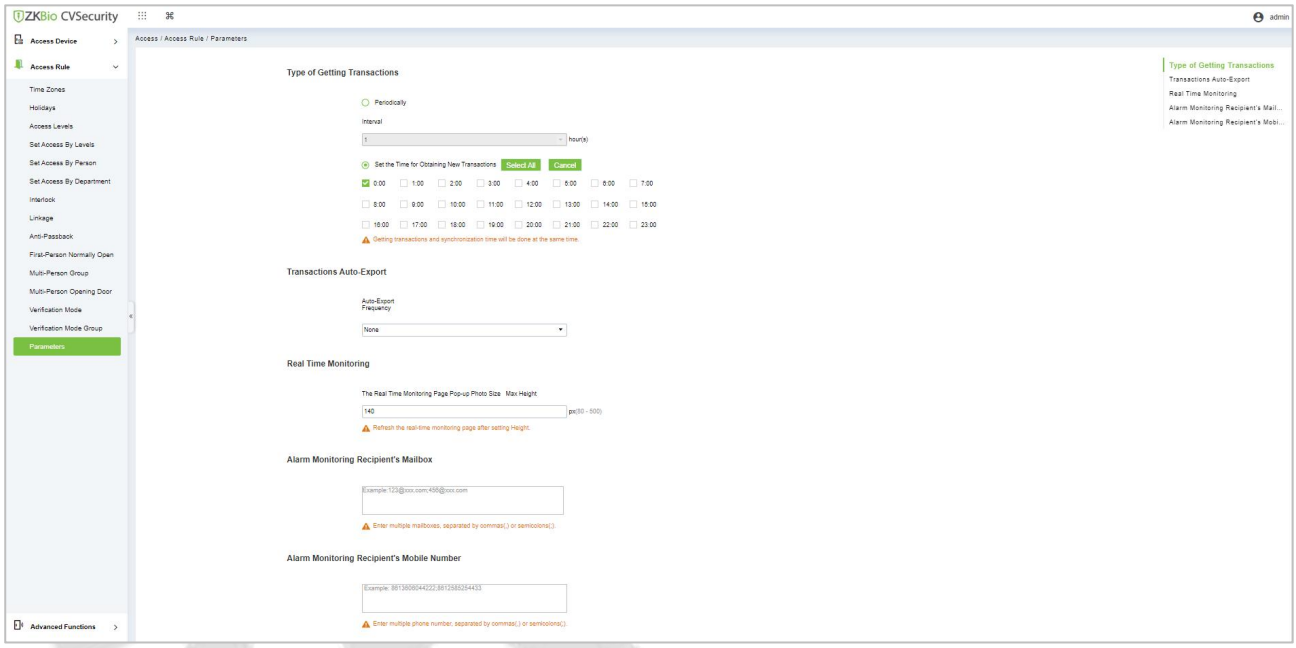


Figure 3- 108 Add Parameters

● Type of Getting Transactions:

Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Set the Time for Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

Transaction Auto-Export

The user can choose the export frequency and the data to be exported each time. If the export frequency is selected as **"By day"**, you must set the time to export the data. You must also select the mode of export. It can be daily transactions or all the system data (30000 data units can be sent at a time. We can customize the data that we need to export from custom report 1 and custom report 2.

If the export frequency is selected as **"By Month"**, you must select the day to export the data. It can be the first day of the month or you can specify any particular date. Then select the export frequency as Daily Data or all System data. Finally, add the recipient's mail address to send the transaction data.

Figure 3- 109 Transaction Auto Export

The Real Time Monitoring Page Pop-up Staff Photo Size

When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

Figure 3- 110 Real Time Monitoring

Alarm Monitoring Recipient Mailbox

The system will send email to alarm monitoring recipient's mailbox if there is any event.

Figure 3- 111 Alarm Monitoring Recipient Mailbox

Alarm Monitoring Recipient Mobile Number

The system will send alarm monitoring recipients to mobile, if there is any event.

Figure 3- 112 Alarm Monitoring Recipient Mobile Number

3.5 Advanced Functions

Advanced access control is optional. You must obtain permission to activate the advanced access control.

In addition to the global linkage function, enable the background authentication function first.

The access control area must be defined when advanced functions such as global Anti-Passback are used.

3.5.1 Area Definition

Divide areas and define access control areas. The access control area is reserved for advanced access control but not for system management.

This section describes Step in ZKBio CVSecurity to add an access control area.

3.5.1.1 Add (New)

● **Operation Step:**

Step 1: In the Access Control module, choose "**Advanced function > Area Definition**" and click New.

Step 2: On the page that is displayed, set related parameters, and click **OK**.

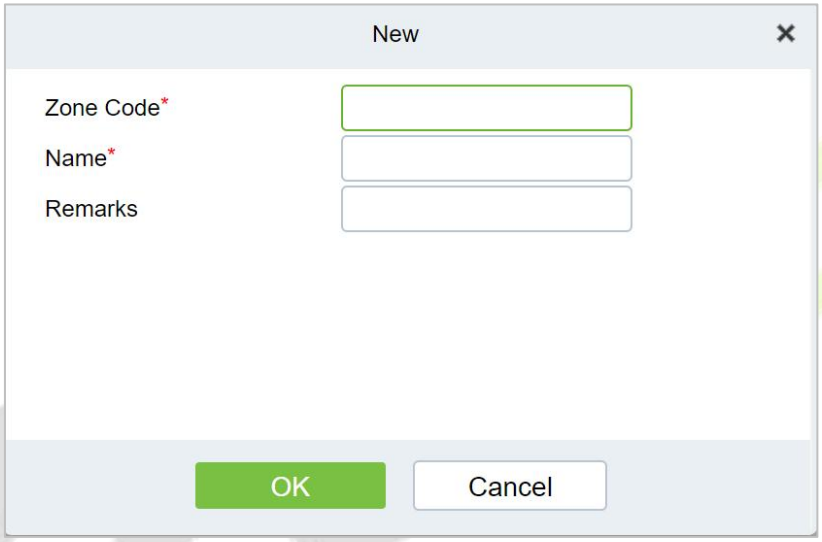


Figure 3- 113 Page for Adding Access Control Areas

3.5.1.2 Delete

Click **Advanced function** > **Area Definition** > **Delete** after selecting the required section in the interface.

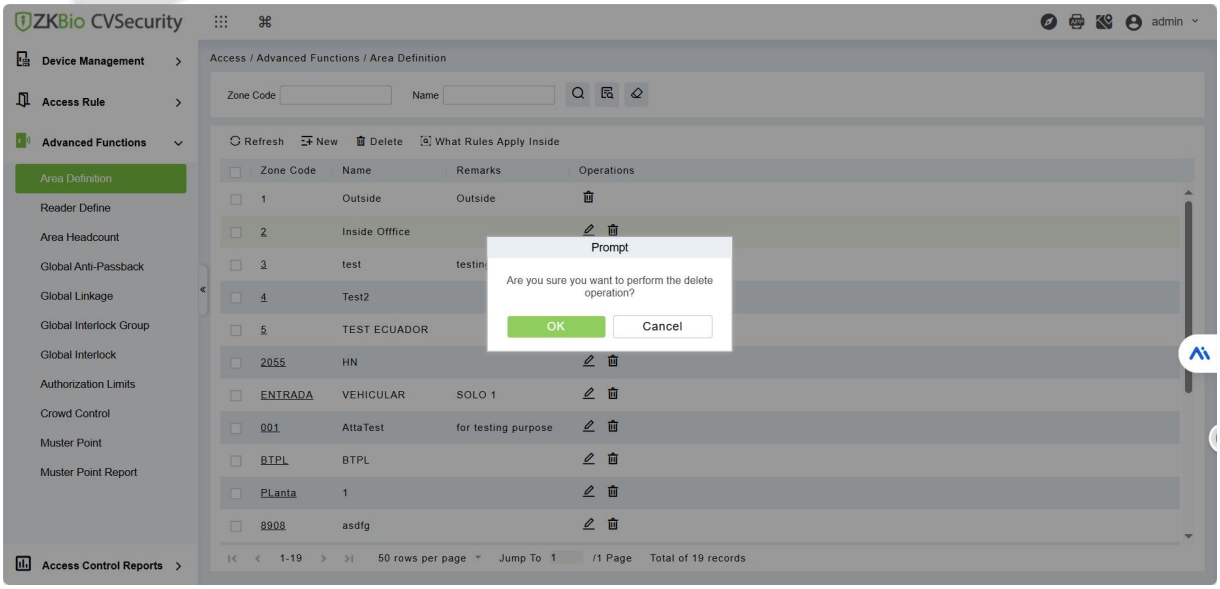


Figure 3- 114 Delete Access Control Areas

3.5.1.3What Rules Apply Inside

Click **What rules inside** after selecting the required section in the interface we can check the rules are applied for the particular zone.

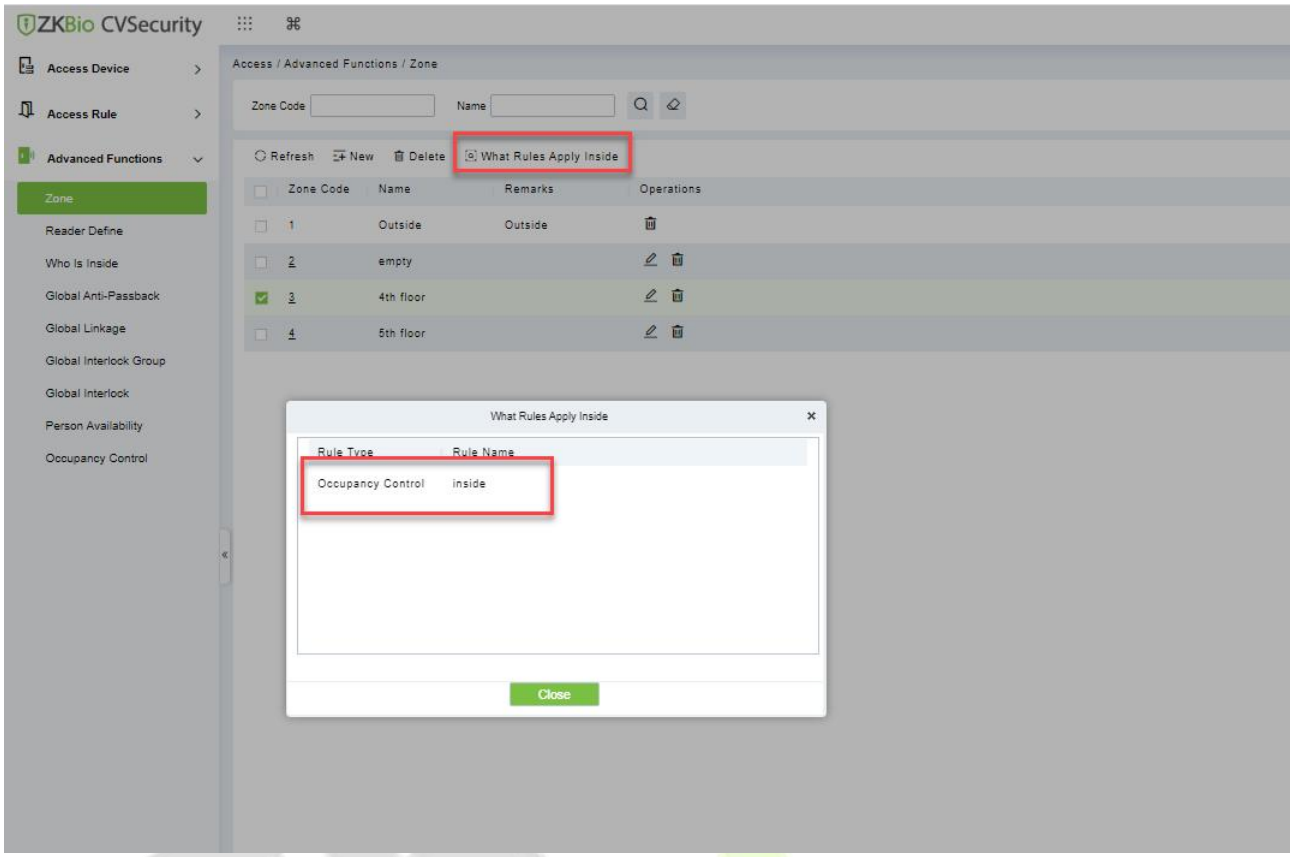


Figure 3- 115 What Rules Apply Inside

3.5.2Reader Define

This function is configured based on the access control area. To use the global Anti-Passback function, you must define the reader.

This section describes the Step of adding a Reader definition in ZKBio CVSecurity.

3.5.2.1Add (New)

●Operation Step:

Step 1: In the Access Control module, choose " **Advanced function > Reader Define**" and click New.

Step 2: On the page that is displayed, set related parameters and click **OK**.

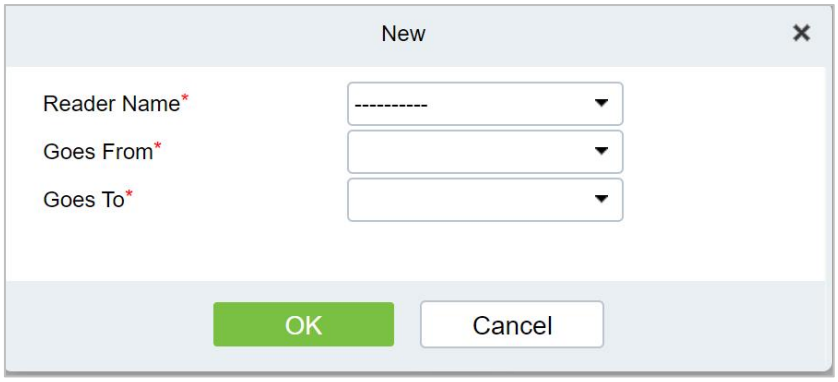


Figure 3- 116 Page for Adding a Reader

3.5.2.2Batch New

Step 1: Click **Advanced Functions > Reader Define > Batch New** to enter the batch add interface:

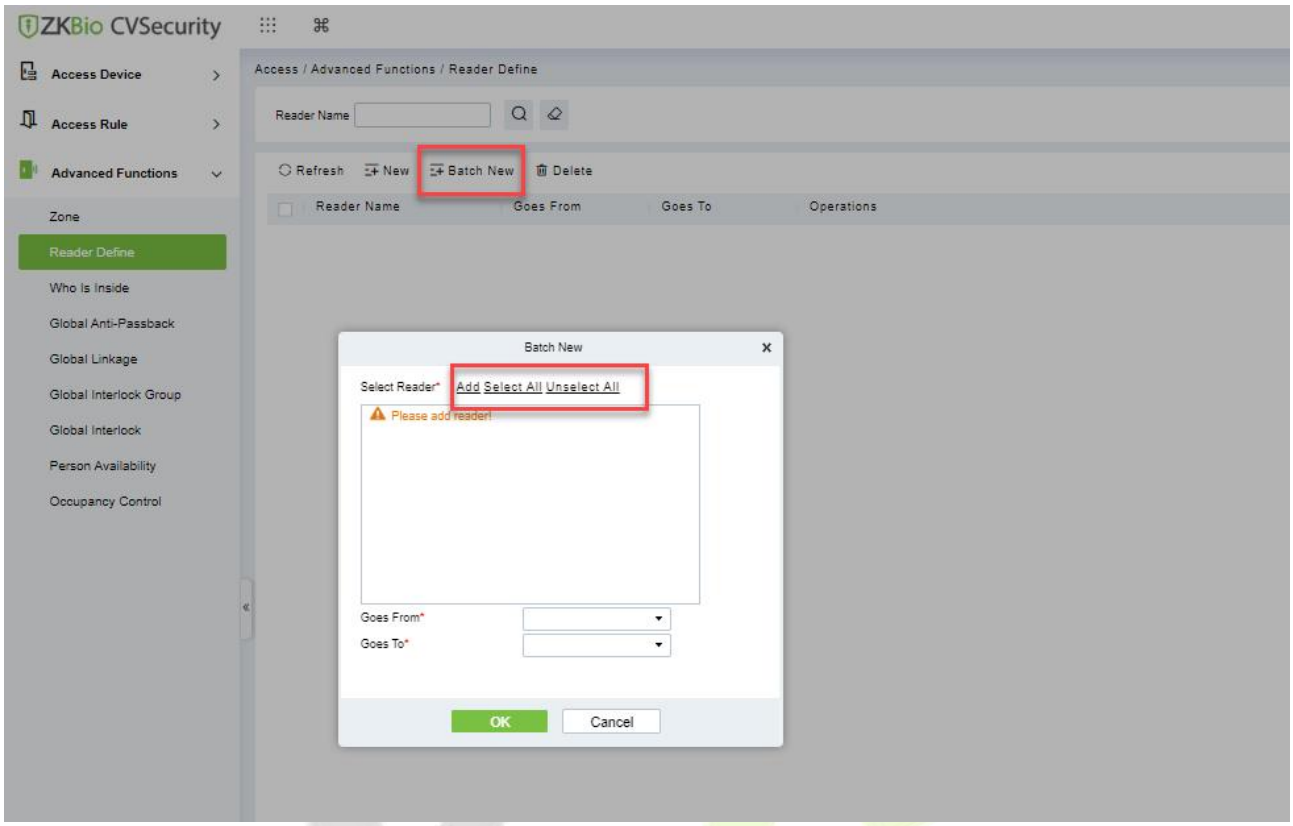


Figure 3- 117 Batch New

Step 2: Click **Add**, select Reader(s) and move towards right and click **OK**.

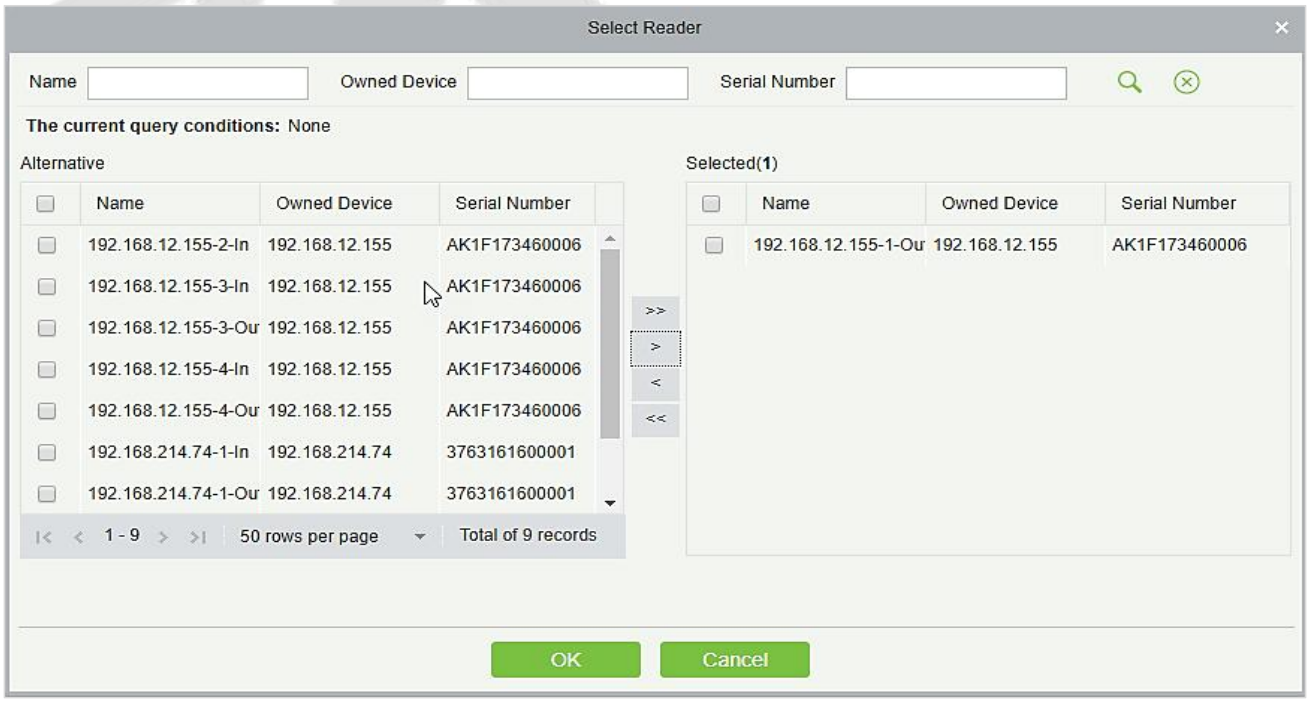


Figure 3- 118 Add Reader Define

Step 3: Set Goes from and Goes to as required and press **OK**.

3.5.2.3Delete

In the **Access > Advanced Functions > Reader Define**, click **Delete** button under Operations. Click **OK** to delete.

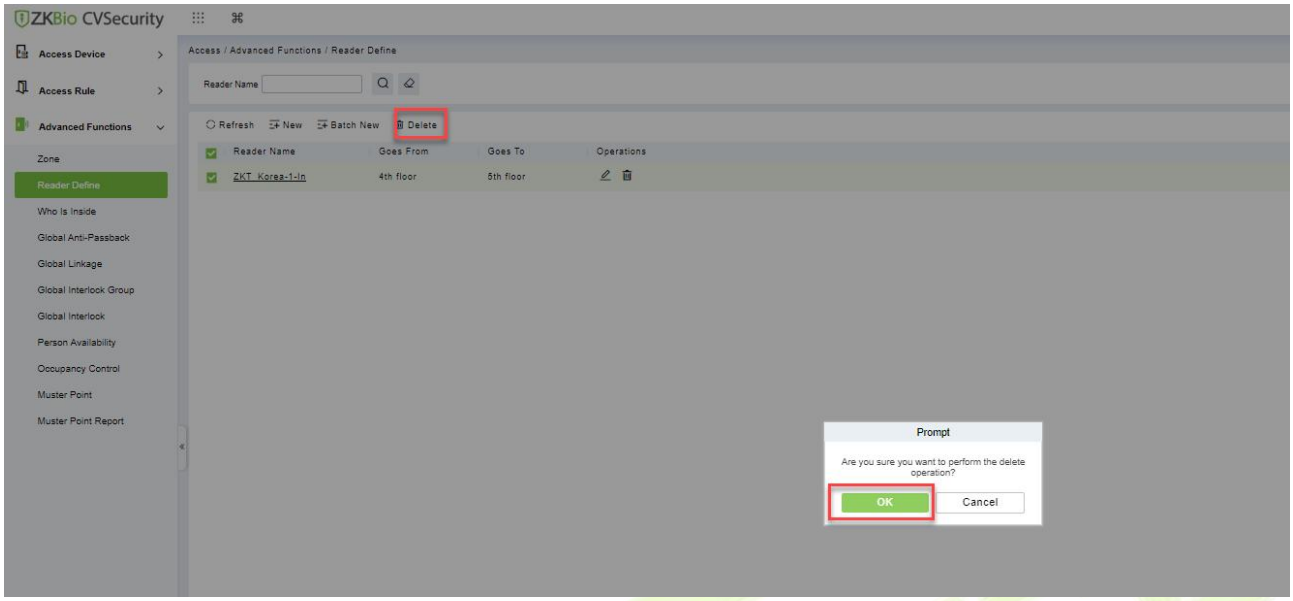


Figure 3- 119 Delete Reader Define

3.5.3Area Headcount

After entering the access control area, users can use this function to view the personnel in the access control area. You can choose the access control area tree to view the personnel in the corresponding access control area.

This section describes how to view the Steps of people in a region in ZKBio CVSecurity.

● **Operation Step:**

Step 1: In the Access Control module, choose "**Advanced Function >Area Headcount**".

Step 2: On the page for viewing personnel in a region, you can select the area on the left to view and delete personnel in the area, as shown in figure below.

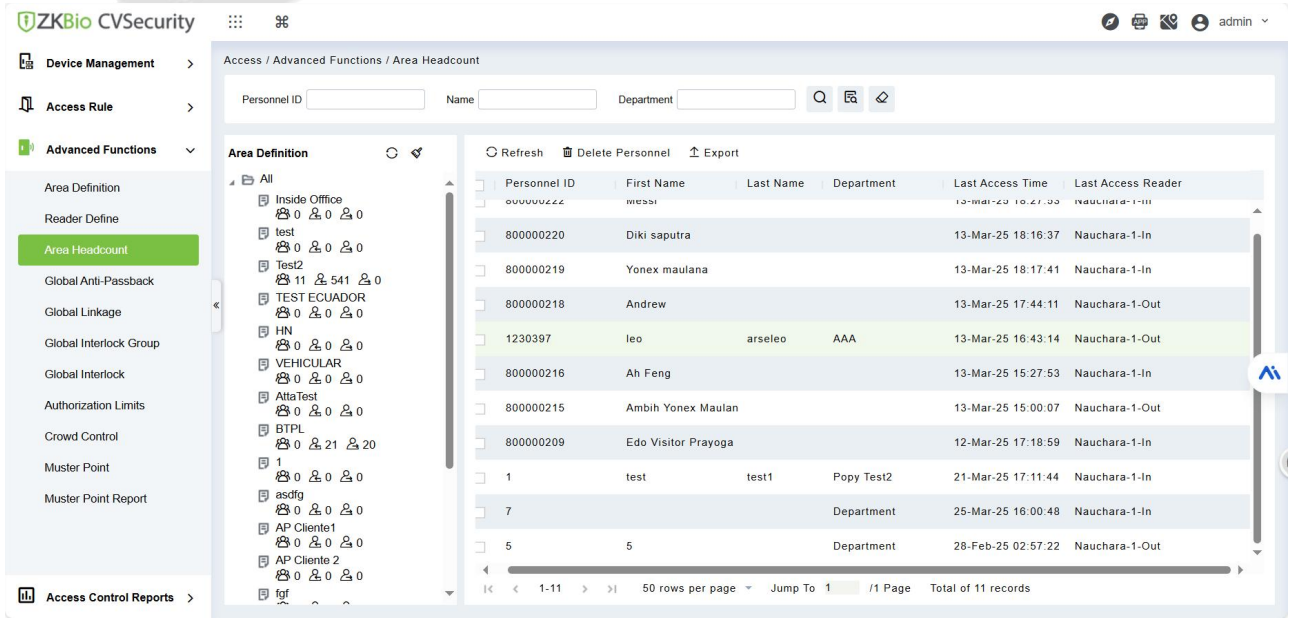


Figure 3- 120 View Area Personnel Page

3.5.3.1Delete Personnel

Select personnel ID, click **Delete**, and click **OK** to delete the level name.

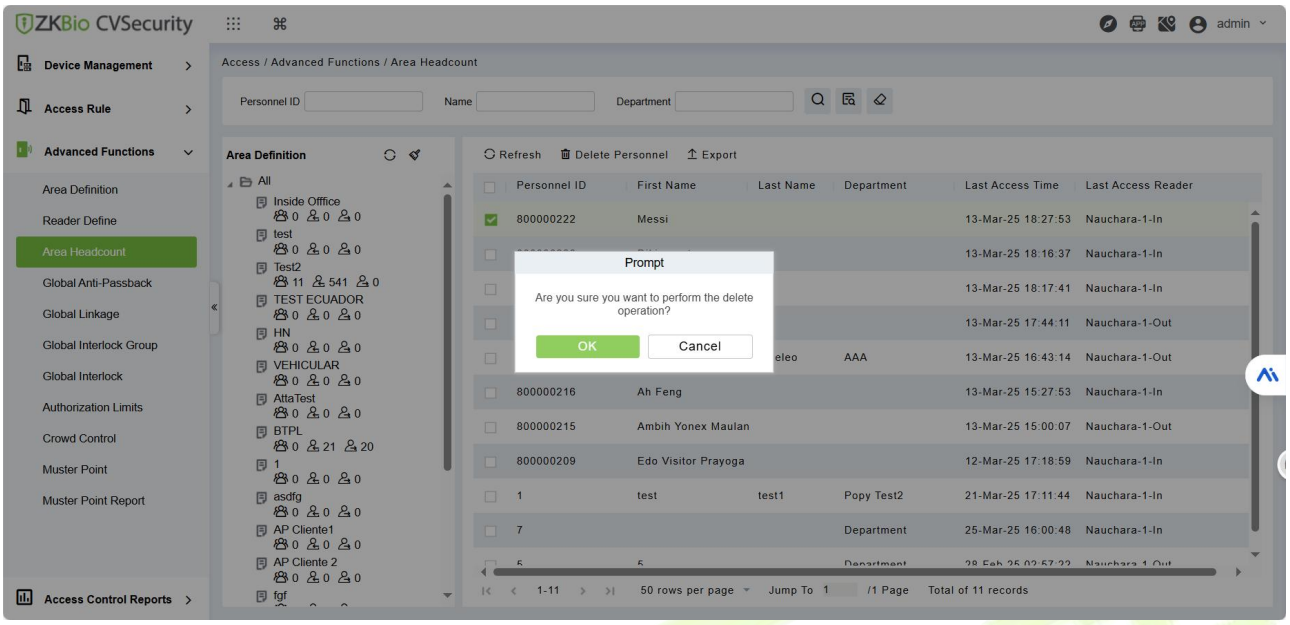


Figure 3- 121 Delete Area Headcount

3.5.3.2Export

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

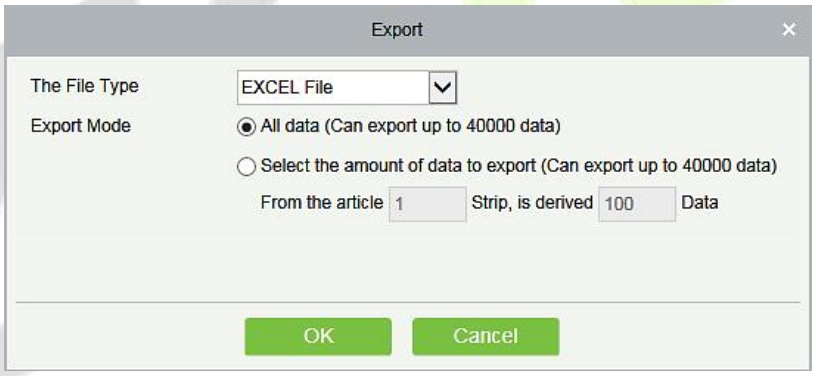
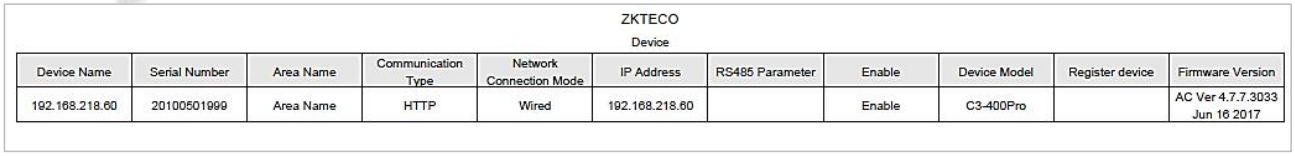


Figure 3- 122 Export



ZKTECO

Device

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

Figure 3- 123 Export Area Headcount

3.5.4Global Anti-Passback

Global Anti-Passback Settings can be carried out across devices, and only push devices support global Anti-Passback functions. This function supports logical Anti-Passback, timed Anti-Passback and timed logical Anti-Passback, and can be configured for specific personnel.

This section describes the Step configuration of global Anti-Passback in ZKBio CVSecurity.

● The Premise Condition:

1. Background authentication has been enabled on the device.

2. Set the access control area and reader definition.

3.5.4.1 Add (New)

● Operation Step:

Step 1: In the Access Control module, choose "**Advanced Access Control > Global Anti-Passback**" and Click New.

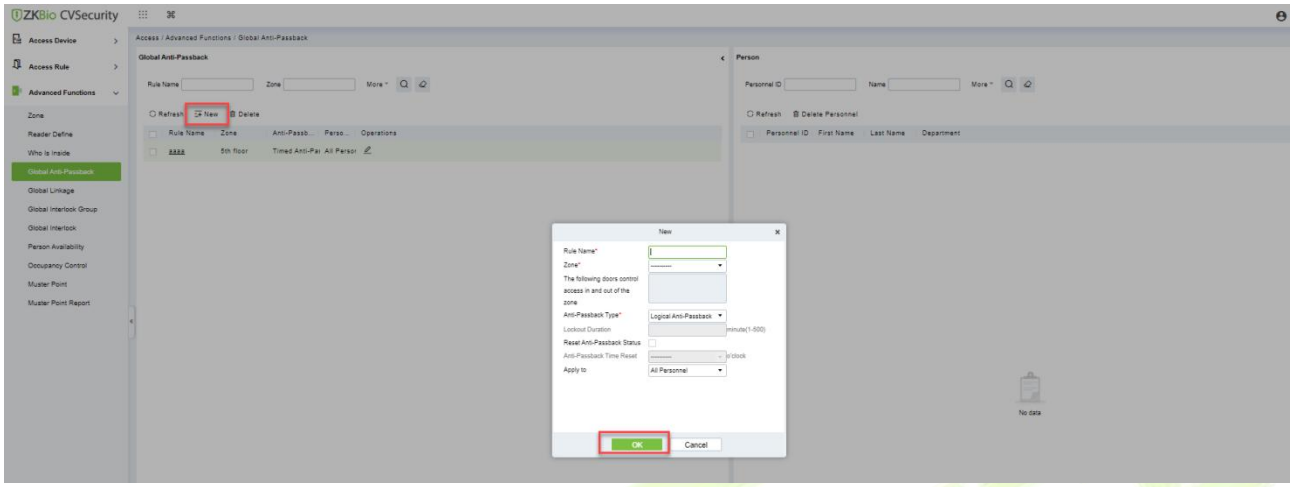


Figure 3- 124 Add Global Anti-Passback

Step 2: On the page for adding global Anti-Passback Settings, set related parameters and click **OK**, as shown in figure below. For parameter description, see Table 3-16.

Parameter	Description
Rule Name	The value can contain a maximum of 30 characters.
Entrance Guard Area	Select an option from the access control area drop-down list box.
The Door List Controls Access to The Access Control Area	The corresponding door information is displayed. The same gate shall not be used to control two independent Anti-Passback boundaries.
Anti-Passback Type	It contains three types of Anti-Passback: logic Anti-Passback, timing Anti-Passback and timing logic Anti-Passback. instructions Logical Anti-Passback: strictly follow the "one in, one out" rule in the Anti-Passback area, otherwise the verification will not open Timed Anti-Passback: A user can enter the Anti-Passback area only once within a specified period of time. After the specified period expires, the user's status will be cleared and the user can enter the Anti-Passback area again Timed logical Anti-Passback: the user can open the door normally only after following the exit and entry rules of logical Anti-Passback.Timing logic antisubmarine is only used in abnormal situations. For example: if the logical Anti-Passback time is set and the personnel follows others out, the personnel cannot swipe the card machine within the set locking time. The Anti-Passback state will be reset after the set locking time, and the traffic can continue.
The Locking Time	You can set the locking period only when you select timing Anti-Passback or logic Anti-Passback type.
Reset Global Anti-Passback Status	Clear the Anti-Passback status of personnel in the system and restore the initialization status.

Parameter	Description
Reset Anti-Passback Time	The reset time can be selected only when reset global Anti-Passback status is selected. When it is time to reset Anti-Passback, the system will automatically clear the Anti-Passback status of all personnel in the access control area.
Applied	All personnel, selected personnel, except selected personnel three types: instructions All personnel: This type can only be edited. Personnel selection is not supported Selected Personnel: If you select this type, you can add personnel. This Anti-Passback type takes effect only for these personnel. Personnel other than selected: Select this type, add personnel, this Anti-Passback type will only take effect for personnel other than selected.

Table 3- 16 Global Anti-Passback Settings

3.5.4.2Delete

In the **Access > Advanced Functions > Global Anti-Pass**, click **Delete** button under Operations. Click **OK** to delete.

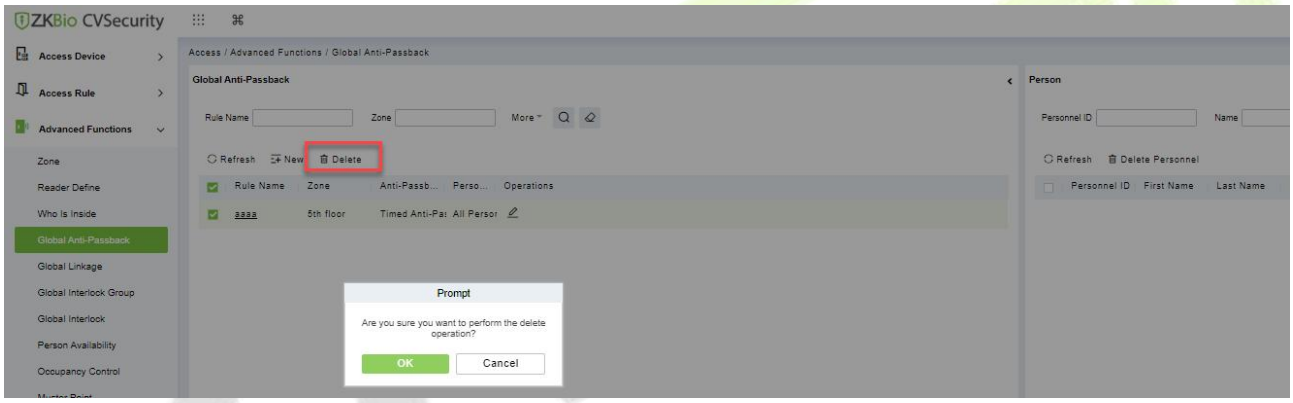


Figure 3- 125 Delete Global Anti-Passback

3.5.5Global Linkage

The global linkage function can be set across devices. Only the push device supports the global linkage function

This section describes how to configure Step for global linkage in ZKBio CVSecurity.

3.5.5.1Add (New)

● Operation Step:

Step 1: In the Access Control module, choose "**Advanced Function > Global Linkage**" and Click New.

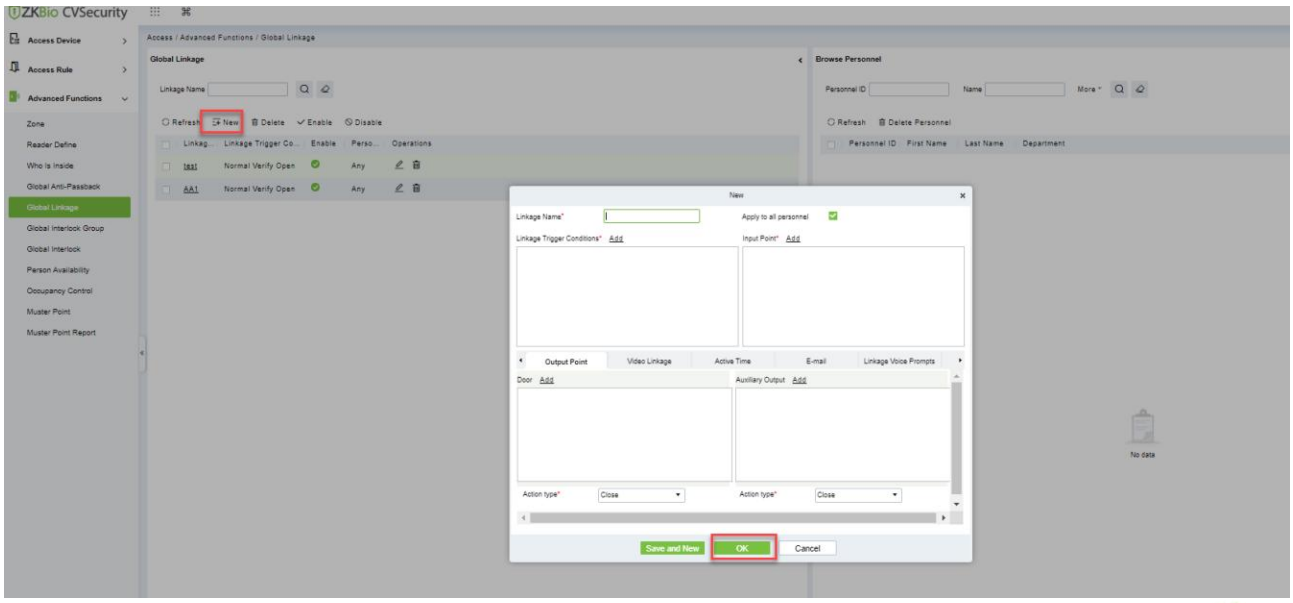


Figure 3- 126 Add Global Linkage

Step 2: On the page for adding global linkage, set related parameters and tap **OK**, as shown in figure below. Table 3-17 describes the parameter description to complete global linkage Settings.

Parameter	Operation Instructions
Linkage Name	You can customize the linkage name for easy query.
It Works for Everyone	After this parameter is selected, the linkage Settings take effect on all personnel.
Linkage Trigger Condition	Select the condition triggered by the linkage Operation, that is, the event type generated by the selected device.
Input Point	Select the input point to set device input.
Dots	Select the output point to set device output. Set the output action type: close, open, normally open. Sets the delay time if the output action is on.
Video Linkage	Pop-up video and display duration: Select pop-up video on the real-time monitoring screen and set the pop-up duration. Video recording and Video Duration: Select Video recording to set the video duration. 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.
Valid Time	The reset time can be selected only when reset global Anti-Passback status is selected When it is time to reset Anti-Passback, the system will automatically clear the Anti-Passback status of all personnel in the access control area.
Mail	Set the email address that receives the linkage content when a linkage event occurs

Table 3- 17 lobal Linkage Parameters

Apply to all personnel: If this option is selected, this linkage setting is effective for all personnel.

Active Time: Set the active time of the linkage setting.

Step 3: Choose Global Linkage trigger conditions, the input point (System will filter devices according to the choice in first step) and the output point, Set up linkage action. For more details about these parameters, please refer to Linkage Setting.

Note: You can select multiple Door Events, but "Fail to connect server", "Recover connection" and "Device connection off" will be filtered automatically from Door Event.

Step 4: Click **OK** to save and quit. The added Global Linkage will display in the list.

3.5.5.2Delete

In the **Access > Advanced Functions > Global Linkage**, click **Delete** button under Operations. Click **OK** to delete.

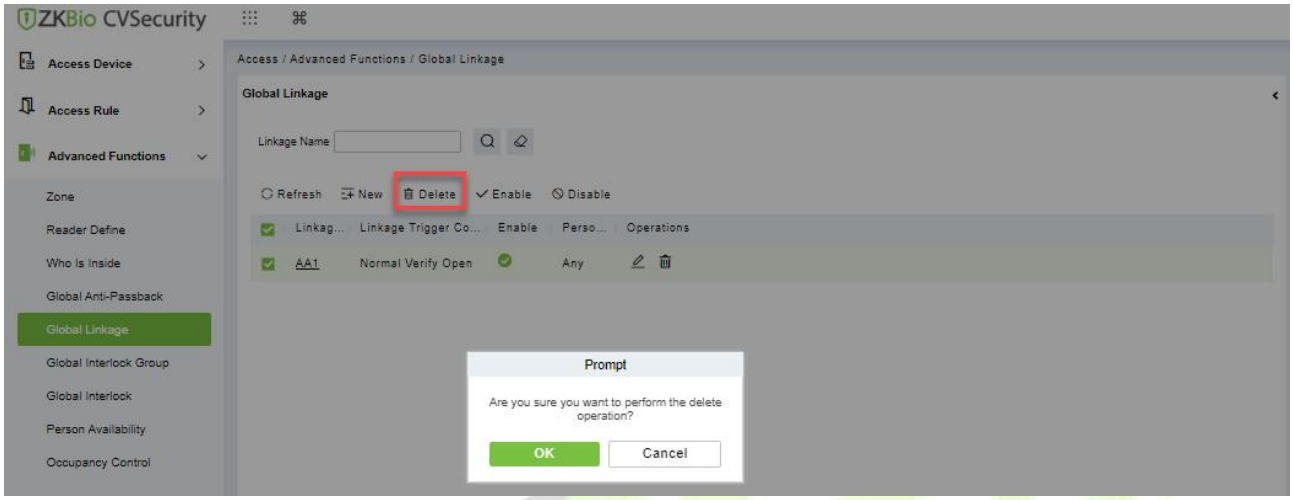


Figure 3- 127 Delete Global Linkage

3.5.5.3Enable

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).

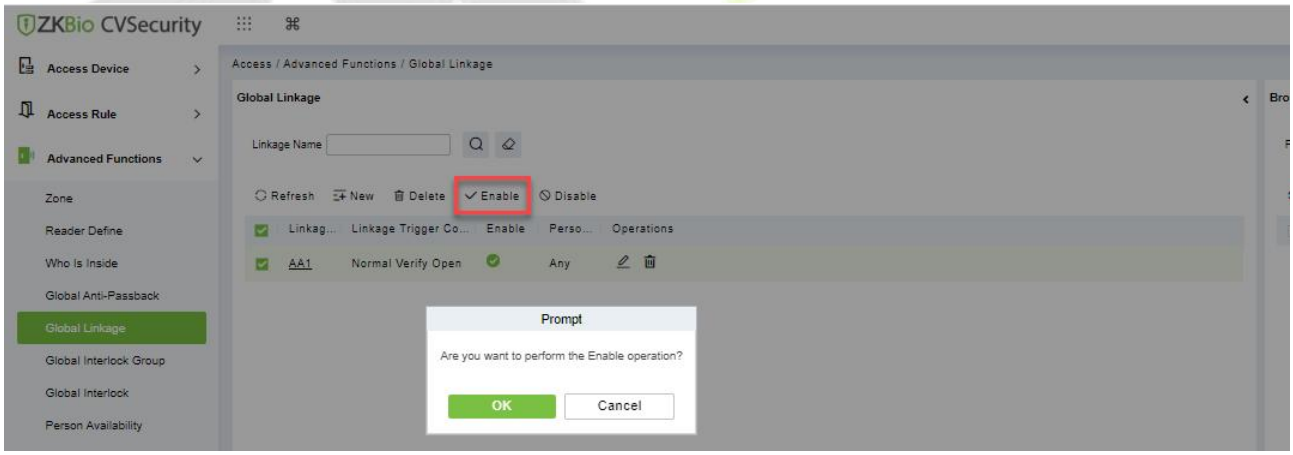


Figure 3- 128 Enable Global Linkage

3.5.5.4Disable

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

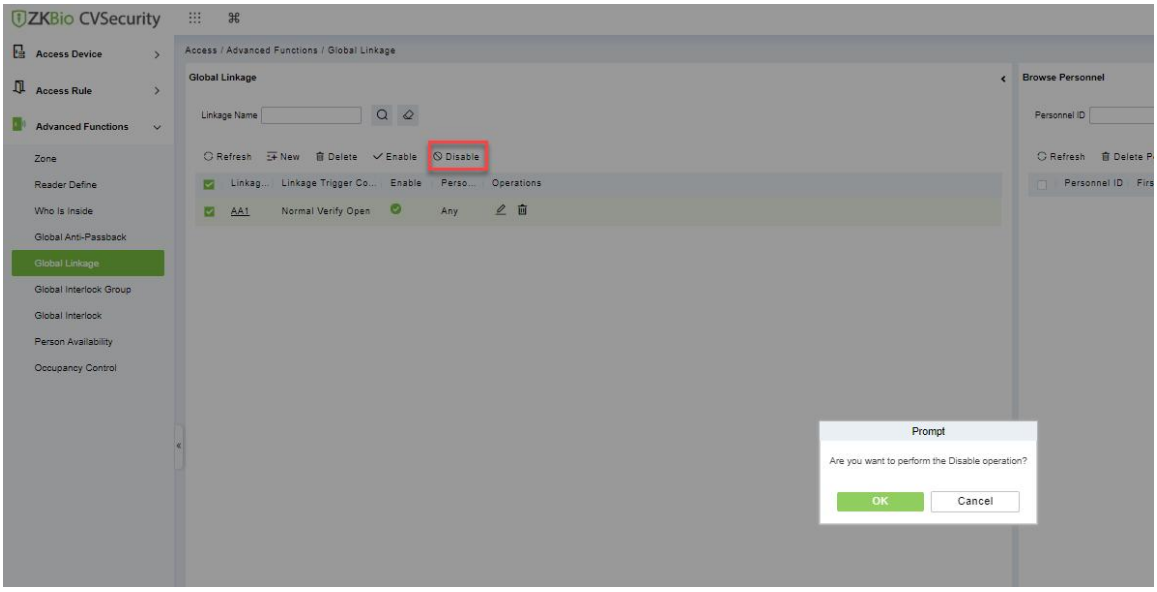


Figure 3- 129 Disable Global Linkage

3.5.6Global Interlock Group

Global interlocking the global interlocking function can be set across devices. Only the push device supports global interlocking. By setting the global interlock group to group doors, you can set global interlock.

This section describes the Step configuration of global interlock in ZKBio CVSecurity.

● The Premise Condition:

Background authentication has been enabled on the device.

3.5.6.1Add (New)

● Operation Step:

Step 1: In the Access Control module, choose "**Advanced Access Control** > **Global Interlock Group**" and Click New.

Step 2: On the page for adding a global interlock group, set related parameters and Click **OK**, as shown in figure below.

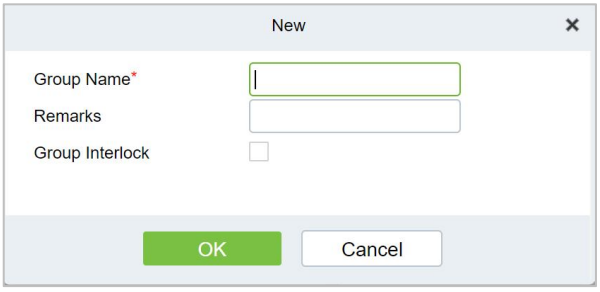


Figure 3- 130 Global Interlock Group Settings Screen

Parameter	How to set up
Group Name	Any combination of up to 30 characters that cannot be identical to an existing group name
Group Interlock	Select the configured interlock rule.

Table 3-18 Description of Advance Global Interlock

Step 3: On the global interlock group page, tap Add Door next to the configured group name on the left, as shown in figure below.

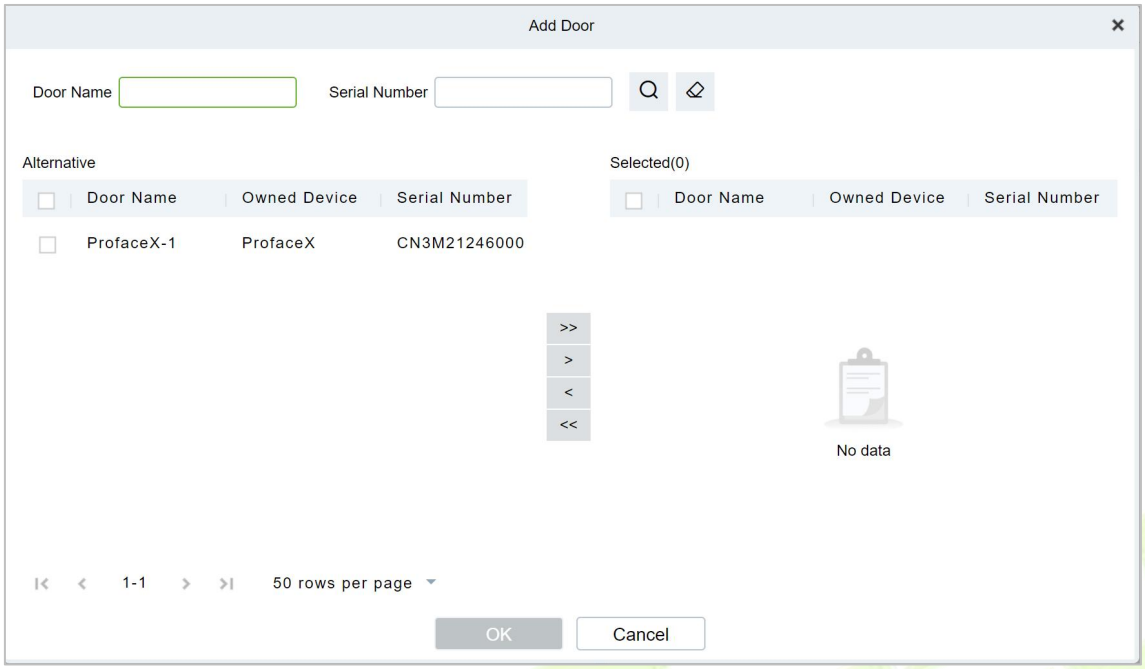


Figure 3- 131 Adding A Door to A Global Interlock Group

3.5.6.2Delete

In the **Access > Advanced Functions > Global Interlock Group**, click **Delete** button under Operations. Click **OK** to delete.

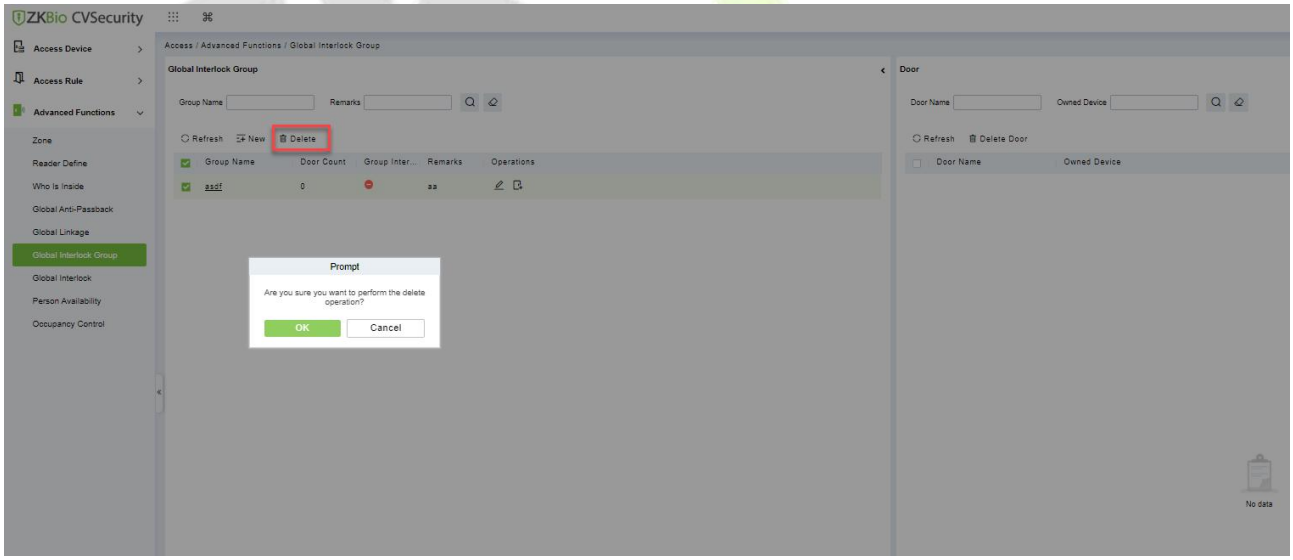


Figure 3- 132 Delete A Door to A Global Interlock Group

3.5.7Global Interlock

3.5.7.1Add (New)

Step 1: In the Access Control module, choose "**Advanced Access Control > Global Interlock**" and Click New.

On the page for adding global interlock, set related parameters and Click **OK**, for example

Step 2: The global interlock name is set.

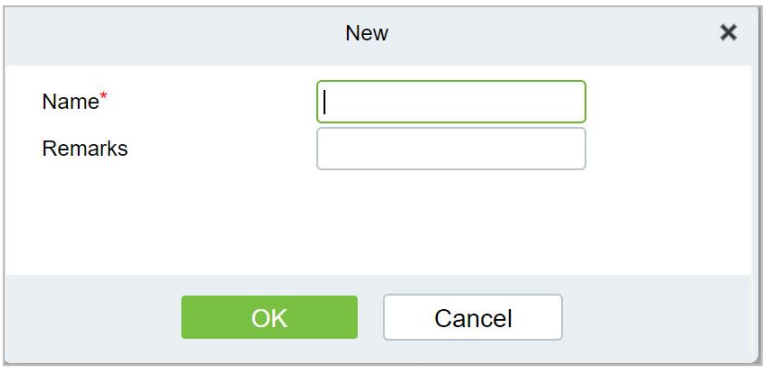


Figure 3- 133 Global Interlock Settings Screen

Parameter	How to set up
Name	Any combination of up to 30 characters that cannot be identical to an existing name
Remark	Select the configured interlock rule.

Table 3- 18 Description of Access Control Right Groups

Step 3: On the global interlock screen, click **Add** Group next to the configured global interlock on the left, as shown in figure below.

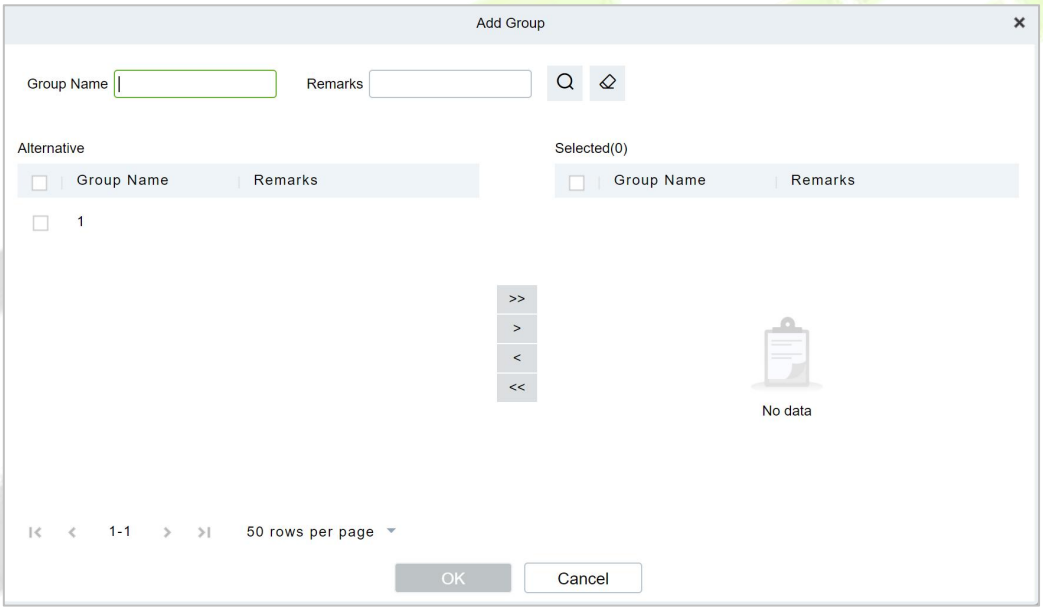


Figure 3- 134 Page for Adding Global Interlock Groups

3.5.7.2Delete

In the **Access** > **Advanced Functions** > **Global Interlock**, click **Delete** button under Operations. Click **OK** to delete.

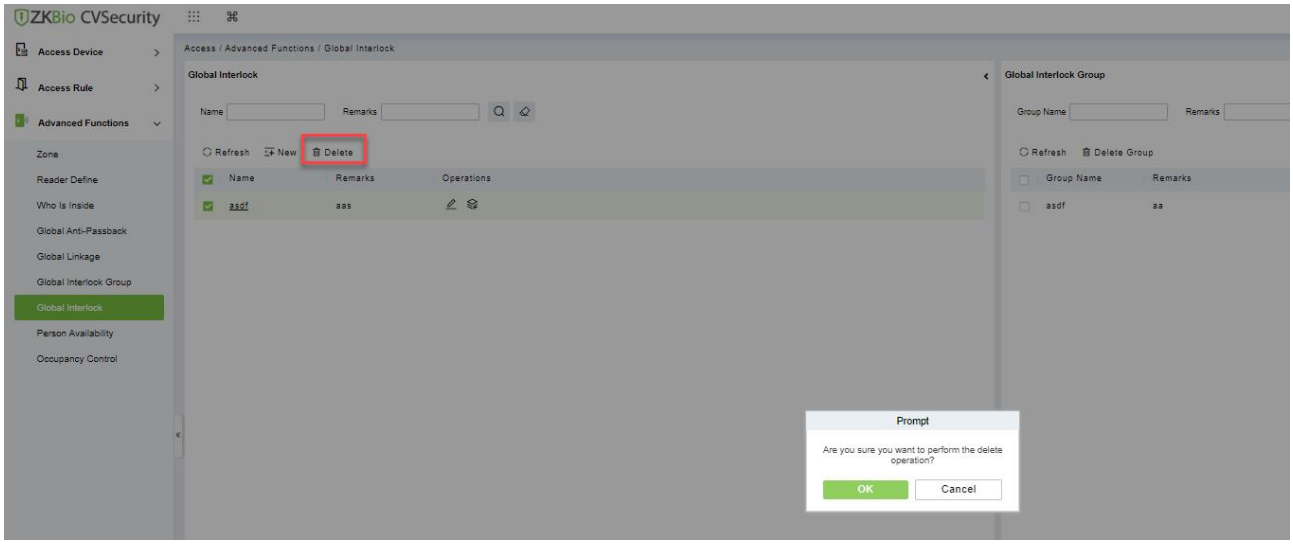


Figure 3- 135 Page for Adding Global Interlock Groups

3.5.8Authorization Limits

It is used to restrict the expiration date, the number of days after the first use, and the number of times the user passes the specified advanced access control area.

- **The Premise Condition:**

1. Background authentication has been enabled on the device
2. Set the access control area and reader definition.

3.5.8.1Add (New)

- Operation Step:

Step 1: In the Access Control module, choose "**Advanced Functions>Authorization Limits**, and Click **New**.

Step 2: On the **Access Control Area Properties** page, set related parameters and Click **OK**.

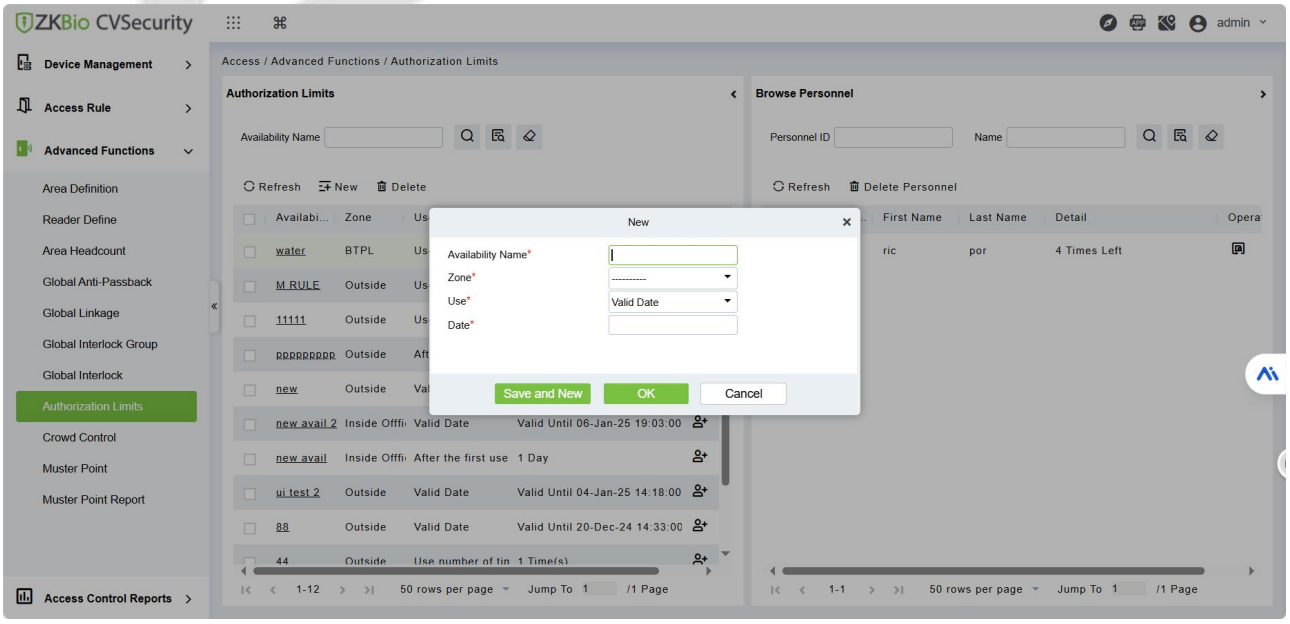


Figure 3- 136 Page for Setting Access Area Properties

Step 3: In the properties of the **access control area** that has been set, click **Add** Personnel on the left

to add the corresponding personnel, and Click **OK**.

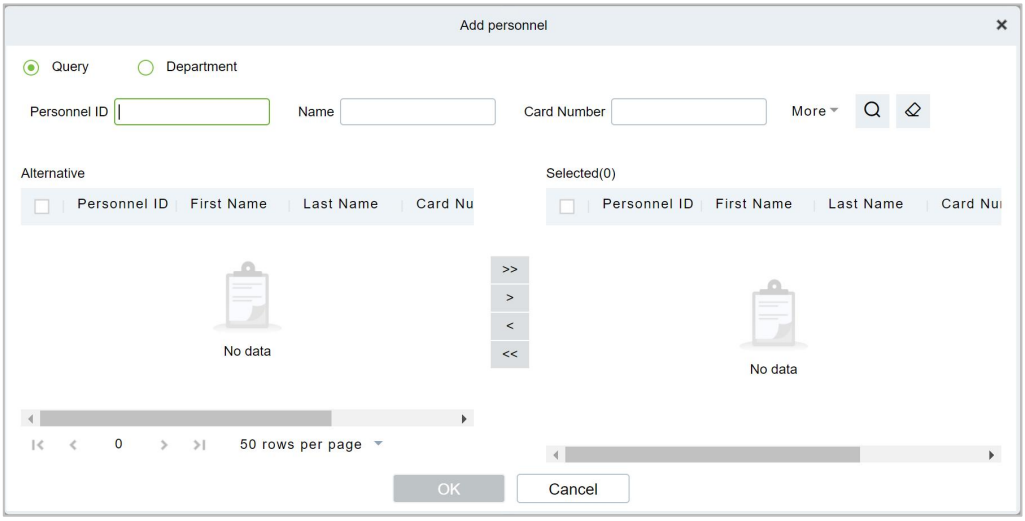


Figure 3- 137 Personnel Availability Add Personnel Settings Screen

Step 4: On the personnel validity screen, tap **Add**, set related parameters, and tap **OK**.

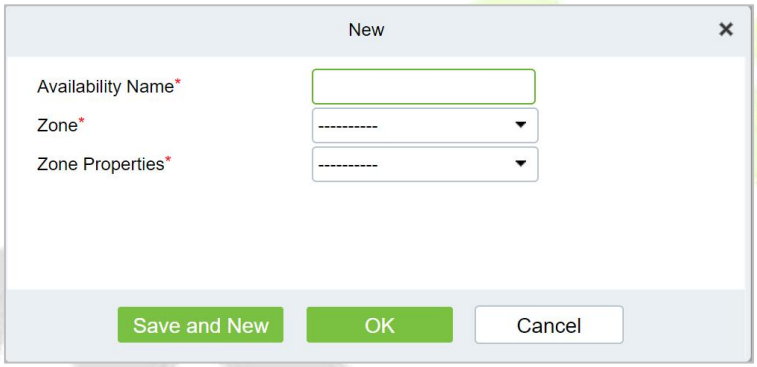


Figure 3- 138 Personnel Validity Setting Screen

3.5.8.2Delete

In the **Access > Advanced Functions > Personnel Availability**, click **Delete** button under Operations. Click **OK** to delete.

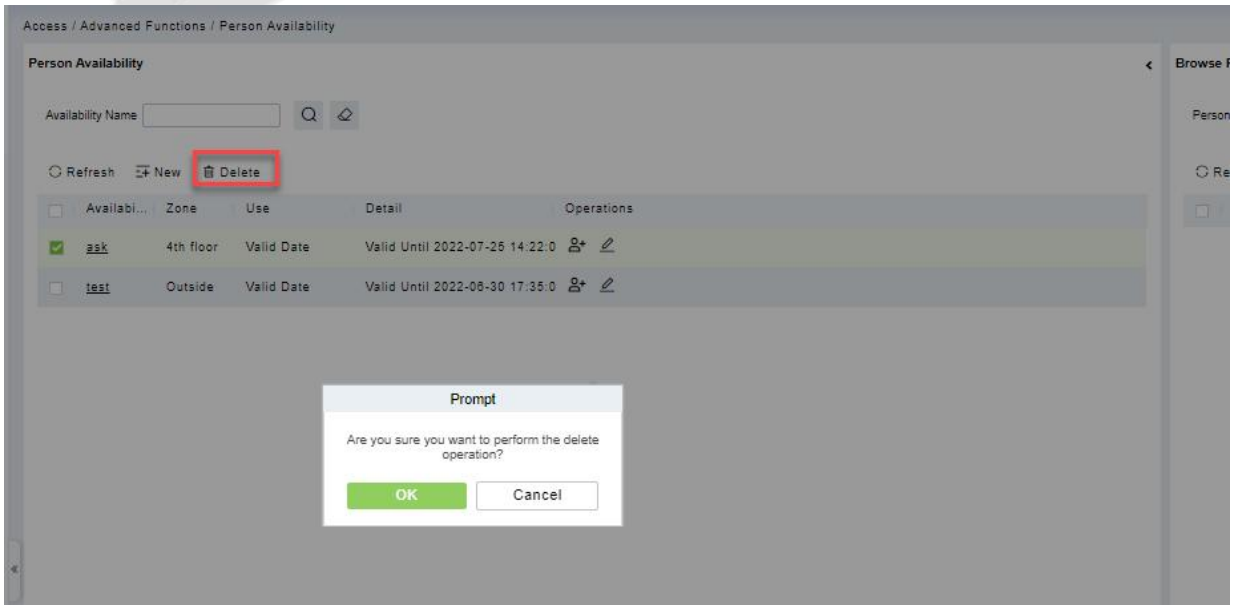


Figure 3- 139 Delete Personnel Validity Setting

3.5.9Crowd Control

Control the maximum/minimum capacity of the area in the Advanced Access Control.

This section describes the Step configuration for population control in ZKBio CVSecurity.

●The Premise Condition

1. Background authentication has been enabled on the device.
2. Set the access control area and reader definition.

3.5.9.1Add (New)

●Operation Step

Step 1: In the Access Control module, choose "A**dvanced Function> Crowd Control**" and Click **New**.

Step 2: On the Add Person control screen, set related parameters and click **OK**.

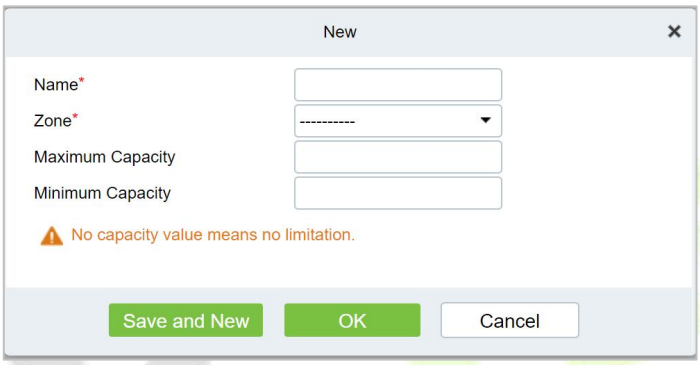


Figure 3- 140 Configuring the People Counting Function

3.5.9.2Delete

In the **Access** > **Advanced Functions** > **Crowd Control**, click **Delete** button under Operations. Click **OK** to delete.

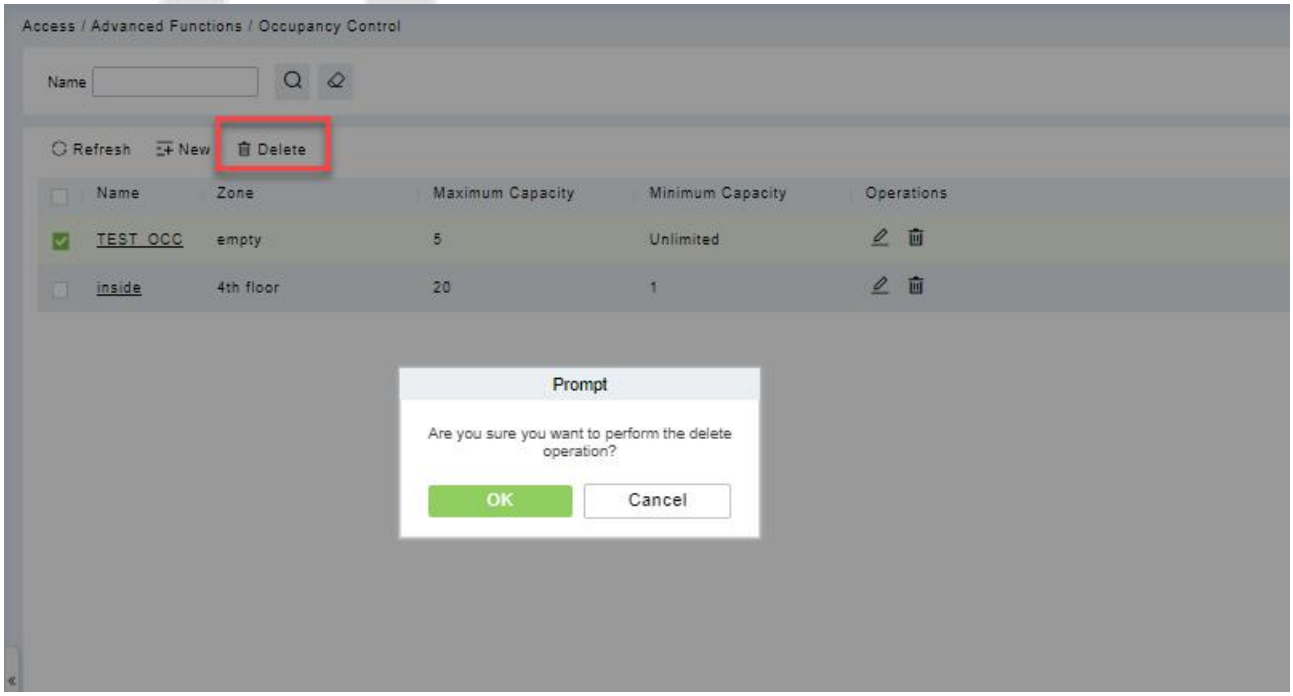


Figure 3- 141 Delete Configuring the People Counting Function

3.5.10Muster Point

Note : The V6.6.0 version has been updated and moved to the Scene Center module. For more details, please refer to Emergency Evacuation.

Designate the access control device of a certain place as the Muster Point. When an emergency event (such as a fire alarm) occurs, the linkage triggers the activation of the Muster Point to open the door, and the AC Device is used to count the escape of personnel, and quickly identify the escaped personnel and dangerous personnel.

3.5.10.1Add (New)

Select the access control devices as the equipment of Muster Point, and assign the corresponding department.

Note: The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

● Operation Steps:

Step 1: Set device as Muster Point, go to "**Access Control > Advanced Functions > Muster Point > New**".

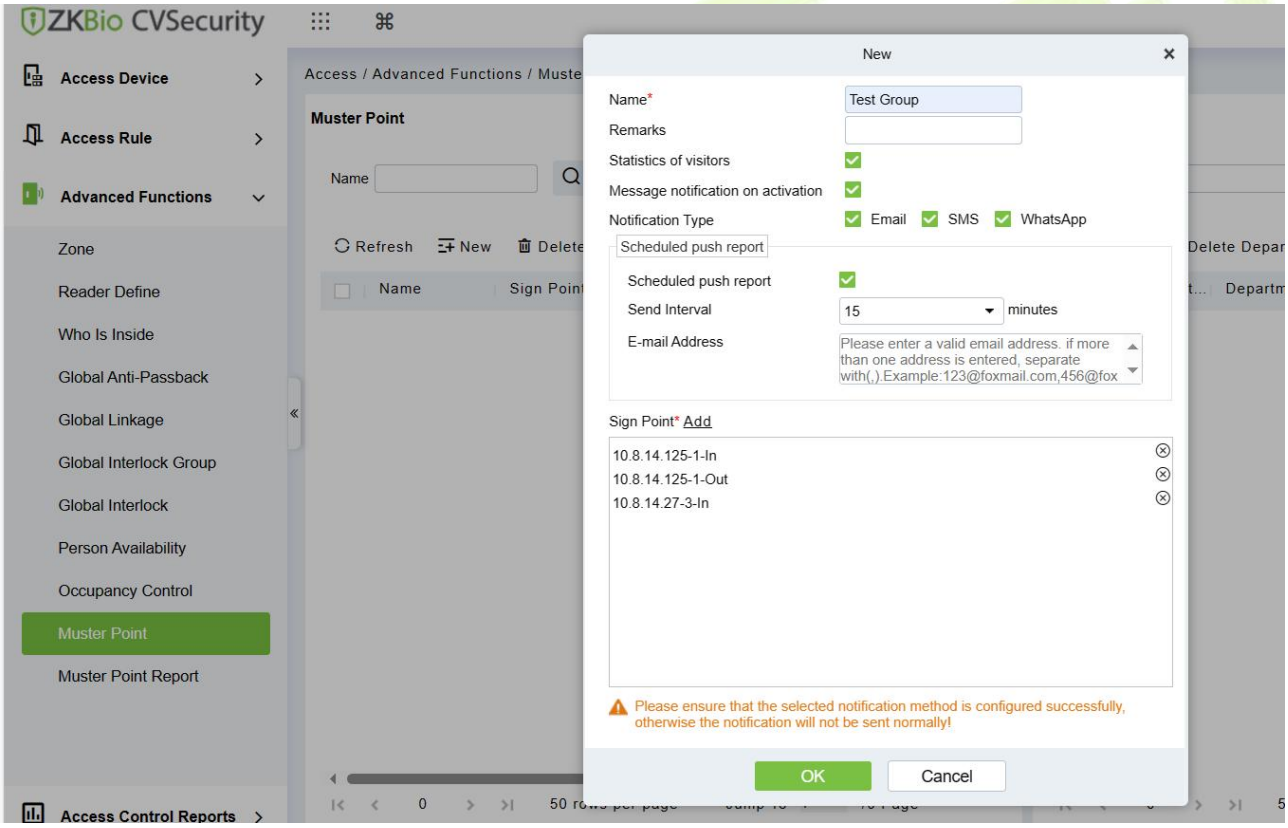


Figure 3- 142 Sign Point

Name: the name of Muster Point.

Remarks: Description of Muster Point.

Statistics of visitors: Enabling visitor statistics will notify visitors when a muster point is activated and count all visitors who have not checked out. (V6.1.0_R or above supported)

Message Notification on Activation: When enabled, the system will automatically send a muster notification to personnel when Muster Point is activated.

Notification Type: When enabled message notification, you can choose the sending method, there are

3 method: Email, SMS, WhatsApp.

Scheduled Push Report: Once enabled, the system will send mustering reports to the administrator at regular intervals (within a set period) when muster point is activated.

Email Address: Administrator email address for receiving mustering reports.

Step 2: Click add department to the point.

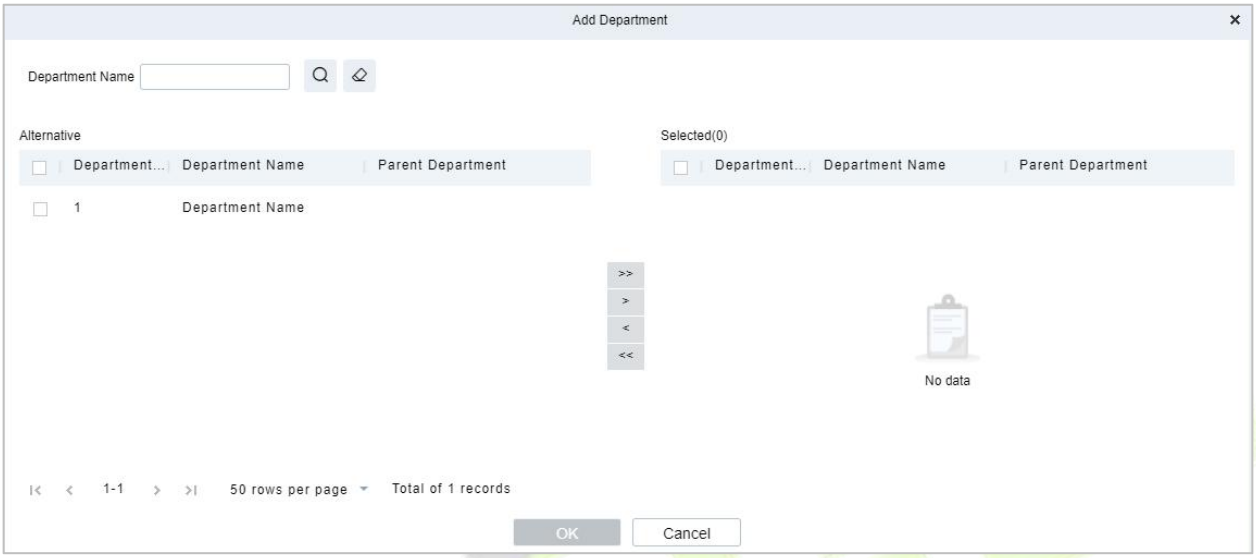


Figure 3- 143 Add Department

Step 3: Set Global Linkage: set Linkage Trigger Conditions and Input Point, Select Muster Point as an output action.

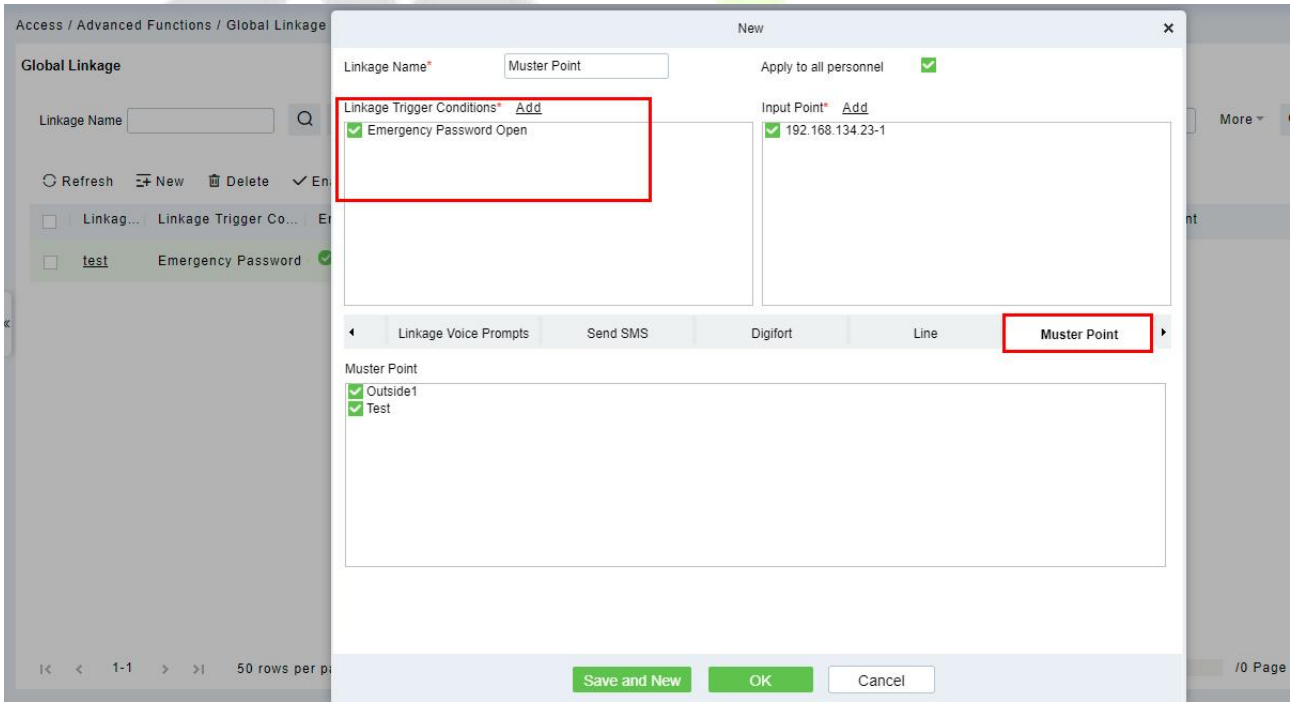


Figure 3- 144 Global Linkage

Note: Before you use global linkage, you must confirm that your device has enable background authentication.

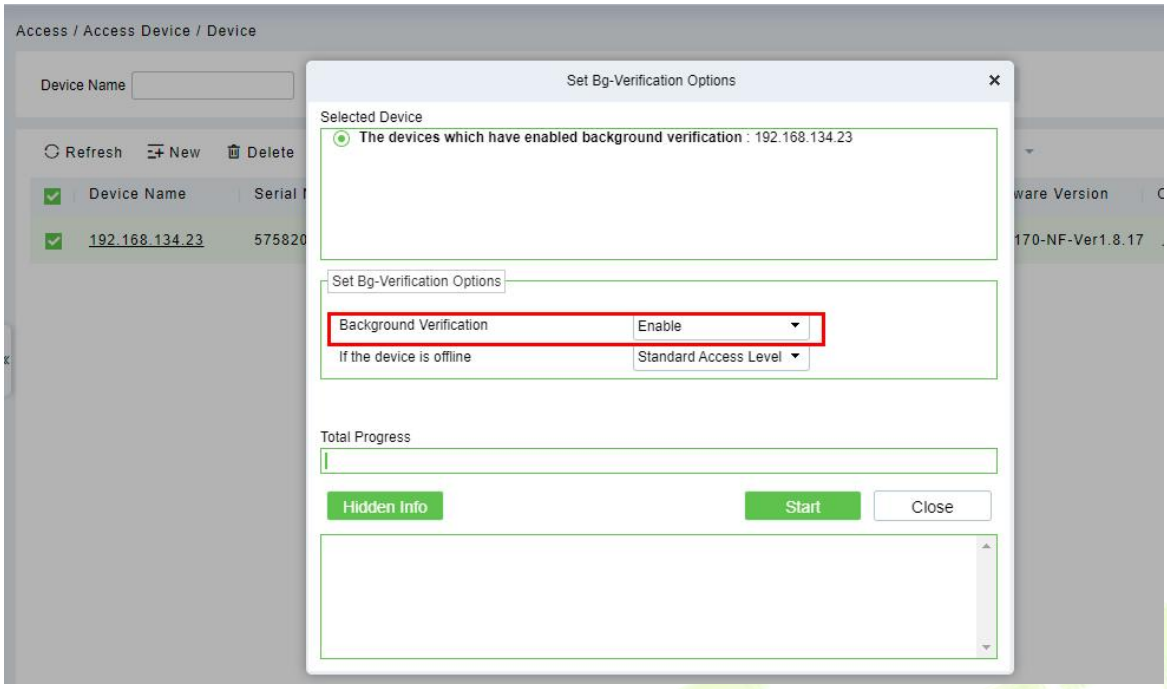


Figure 3- 145 Enable Bg-Verification Options.

3.5.10.2Activated

When the linkage event is triggered, the door is opened remotely.and the Muster Point would be activated.

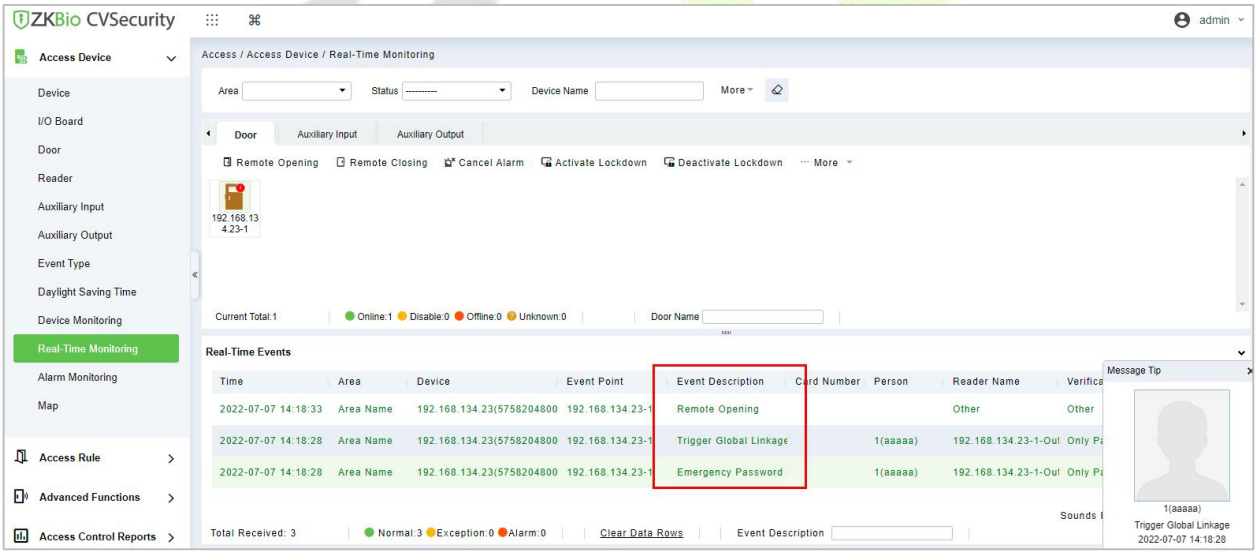


Figure 3- 146 Real-Time Monitoring

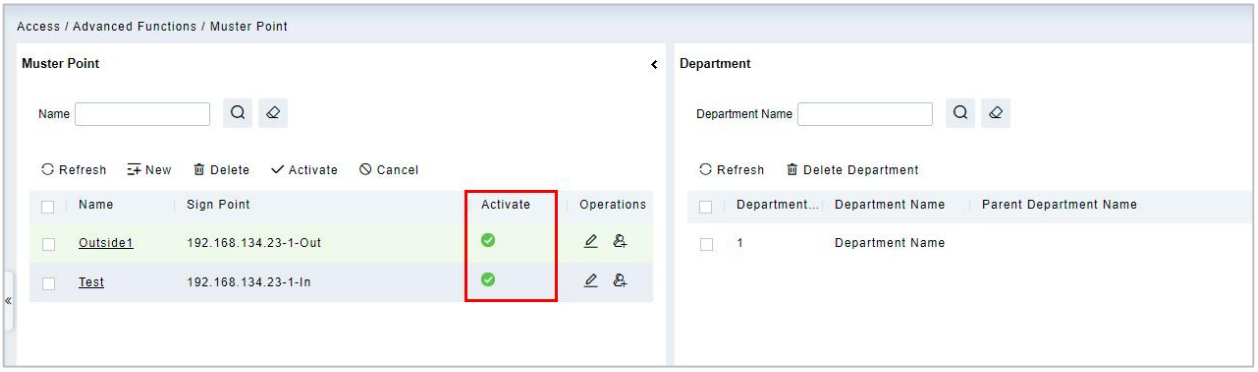


Figure 3- 147 Muster Point

3.5.10.3Delete

In the **Access > Advanced Functions > Muster Point**, click **Delete** button under Operations. Click **OK** to delete.

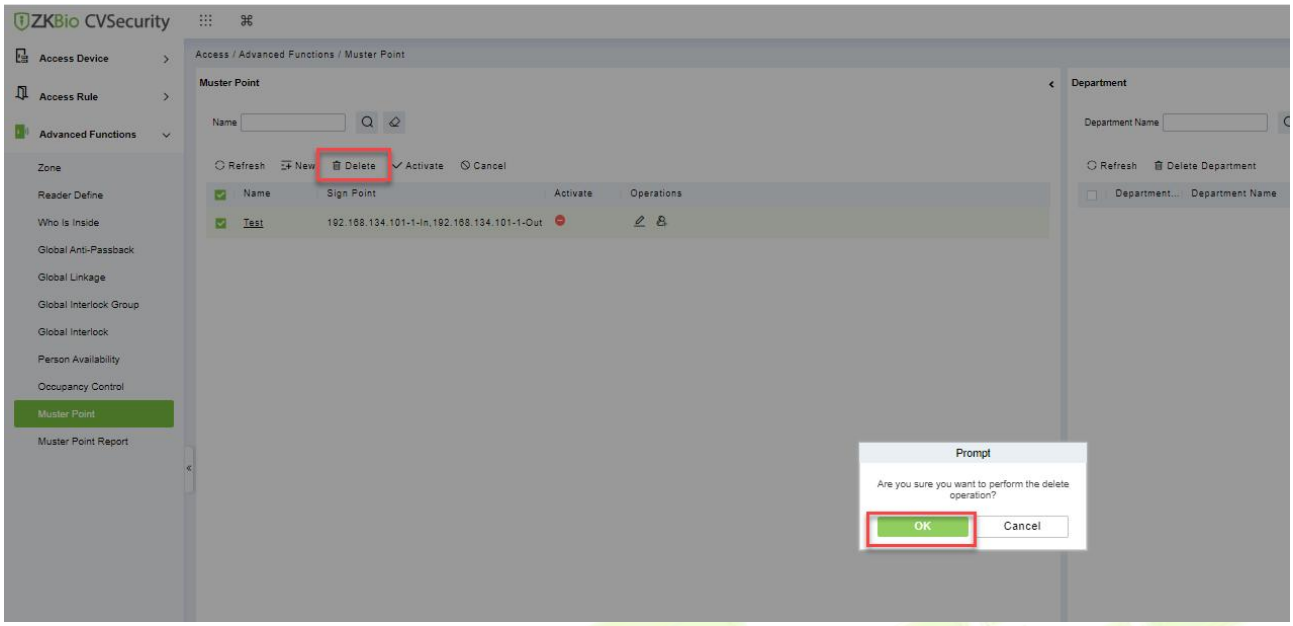


Figure 3- 148 Delete Muster Point

3.5.10.4Cancel

In the **Access > Advanced Functions > Muster Point**, click **Cancel** button under Operations. Click **OK** to cancel.

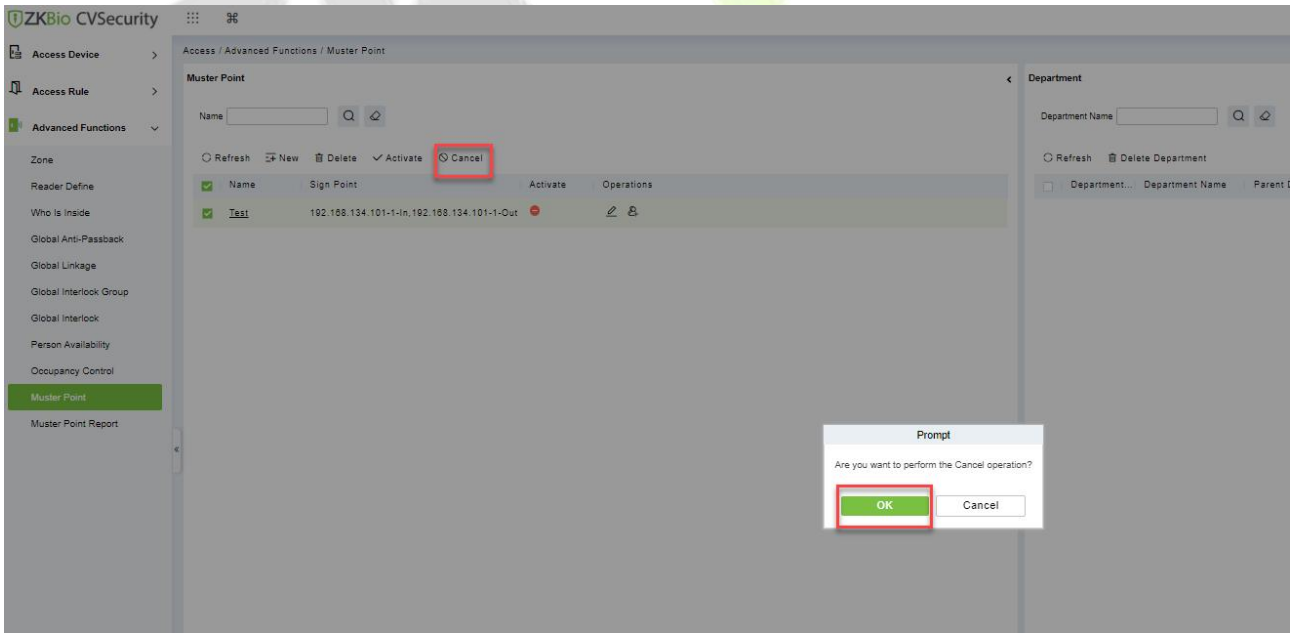


Figure 3- 149 Cancel Muster Point

3.5.11 Muster Point Report

Note : The V6.6.0 version has been updated and moved to the Scene Center module. For more details, please refer to Emergency Evacuation.

Note: The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

● Operation Steps:

Step 1: Go to "**Access Control > Advanced Functions > Muster Point Report**".

You can select a muster point ,and click to genera the report.

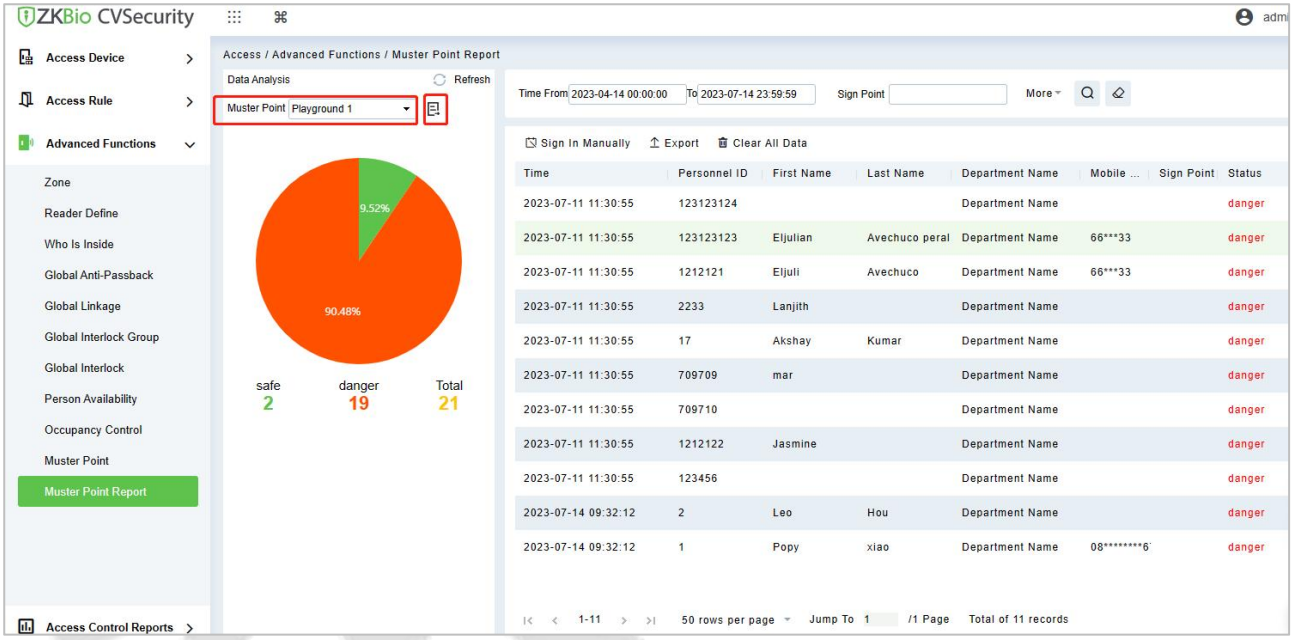


Figure 3- 150 Check the Report

3.5.11.1 Sign In Manually

If someone is not verified on the device, the administrator can manually sign in: Select **Sign in Manually**, see the picture below.

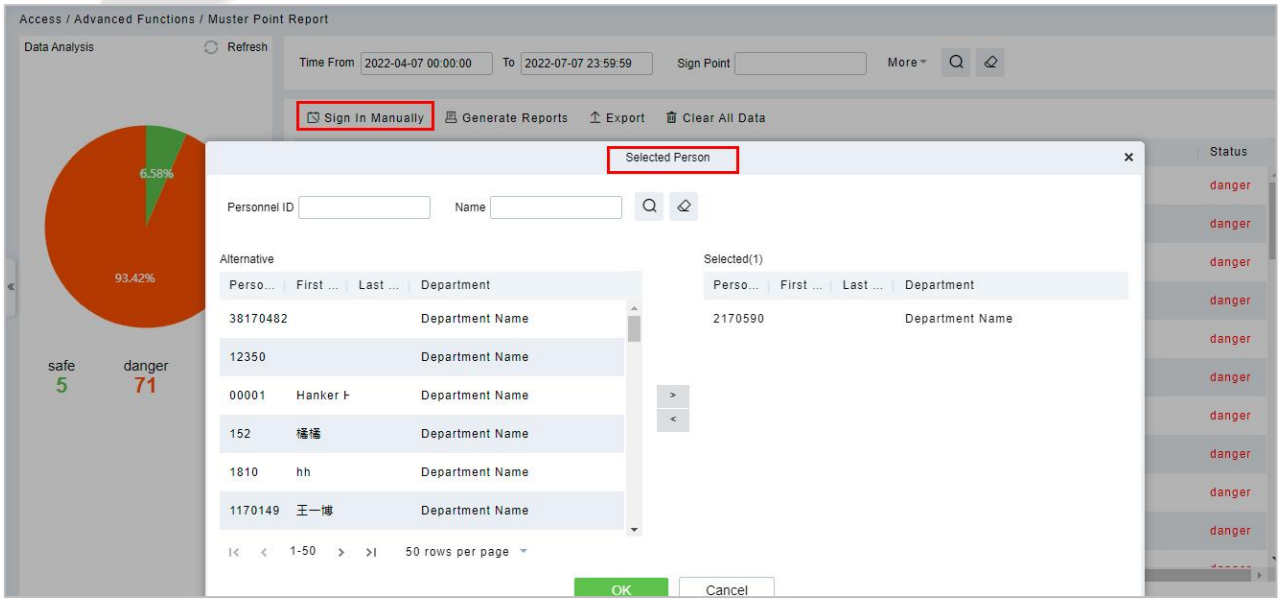


Figure 3- 151 Sign in Manually

Check the statues will change to “safe”.

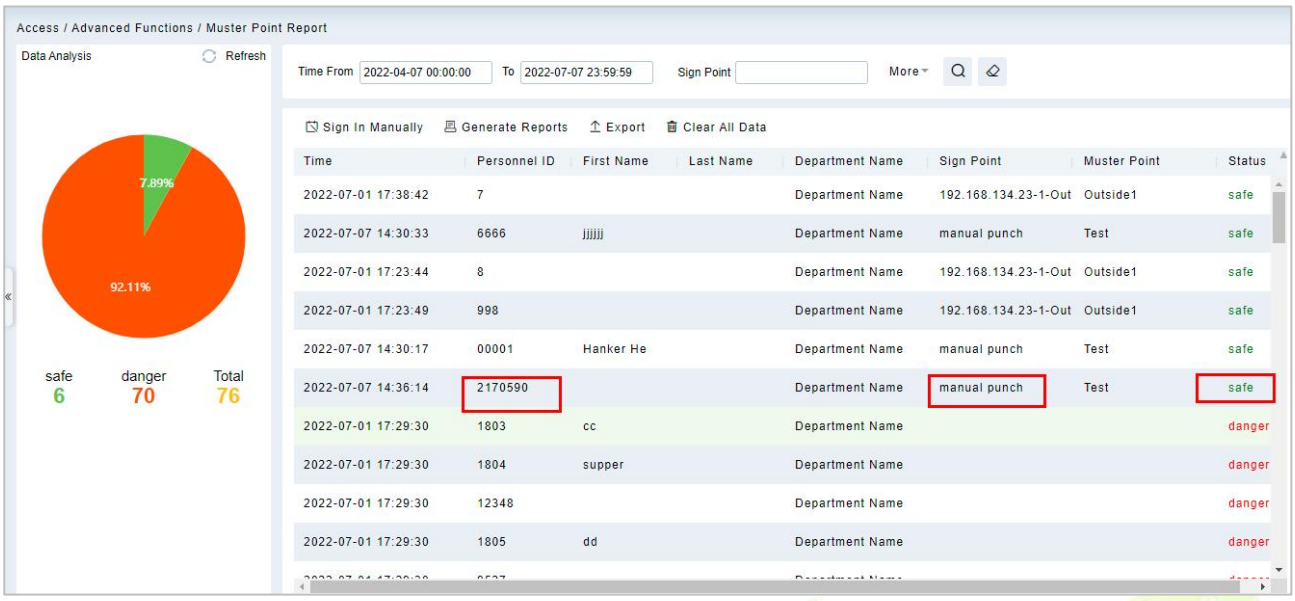


Figure 3- 152 Sign in Manually

3.5.11.2Export

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**.

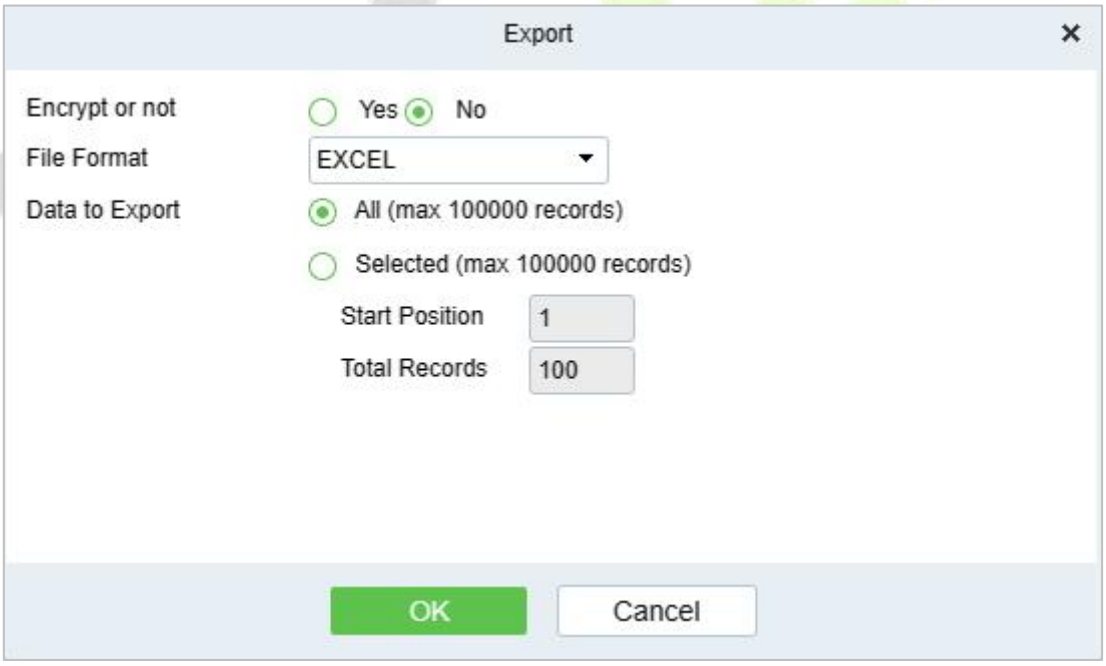


Figure 3- 153 Export

Muster Point Report

Time	Personnel ID	First Name	Last Name	Department Name	Mobile Phone	Sign Point	Status
2023-07-11 11:30:55	123123124			Department Name			danger
2023-07-11 11:30:55	123123123	Eljulian	Avechuco peral	Department Name	6622333		danger
2023-07-11 11:30:55	1212121	Eljuli	Avechuco	Department Name	6622333		danger
2023-07-11 11:30:55	2233	Lanjith		Department Name			danger
2023-07-11 11:30:55	17	Akshay	Kumar	Department Name			danger
2023-07-11 11:30:55	709709	mar		Department Name			danger
2023-07-11 11:30:55	709710			Department Name			danger
2023-07-11 11:30:55	1212122	Jasmine		Department Name			danger
2023-07-11 11:30:55	123456			Department Name			danger
2023-07-14 09:32:12	2	Leo	Hou	Department Name			danger
2023-07-14 09:32:12	1	Popy	xiao	Department Name	086134342567		danger

Figure 3- 154 Report

3.5.11.3 Clear All Data

In the **Access > Advanced Functions > Muster Point Setting**, click **Clear All Data** button under Operations. Click **OK** to clear all data.

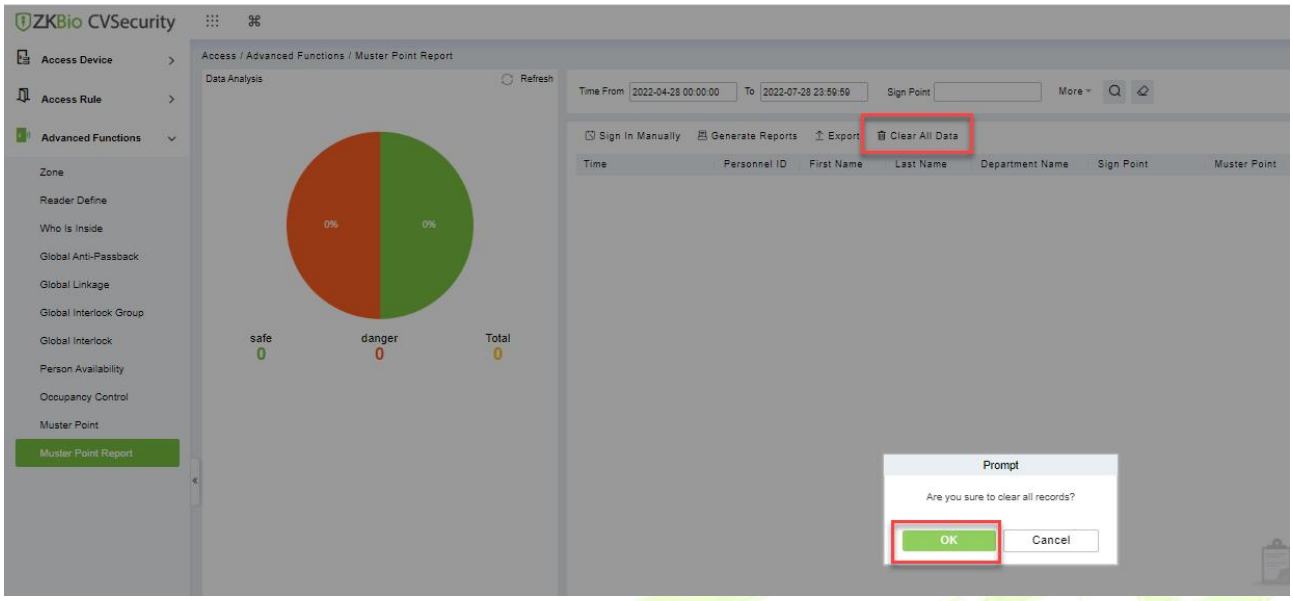


Figure 3- 155 Clear All Data

3.6 Access Control Reports

In the access control report, you can query all access control records, including All records, Today's Access records, All abnormal records, door query, personnel query and Personnel access records reports.You can export all records or query records.

This section describes the Step for querying and exporting reports in ZKBio CVSecurity.

3.6.1 All Transactions

● Operation Step

Step 1: In the Access Control module, choose "**Access Control Report > All Records**".

Step 2: On the All Records interface, fill in the corresponding query information and click the "search" symbol to complete the query of all records, as shown in figure below.

Figure 3- 156 Report Query Page

3.6.1.1 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**.

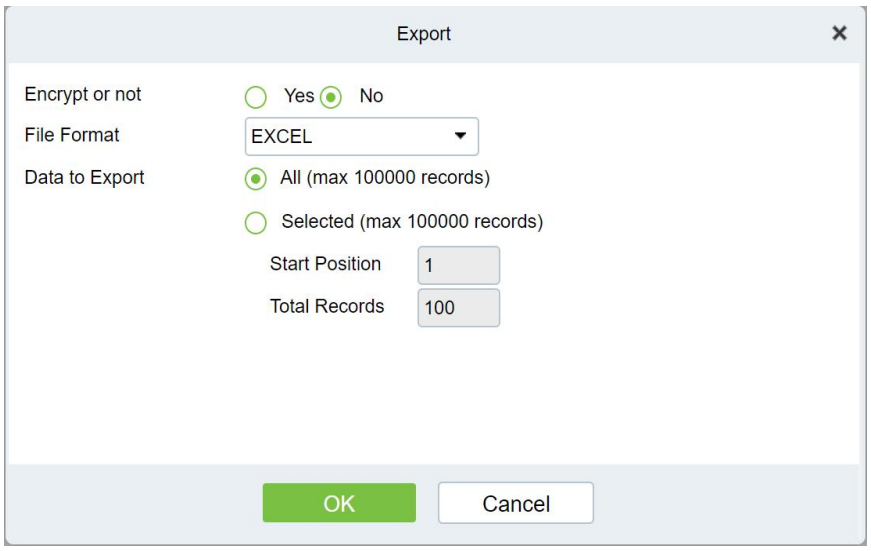
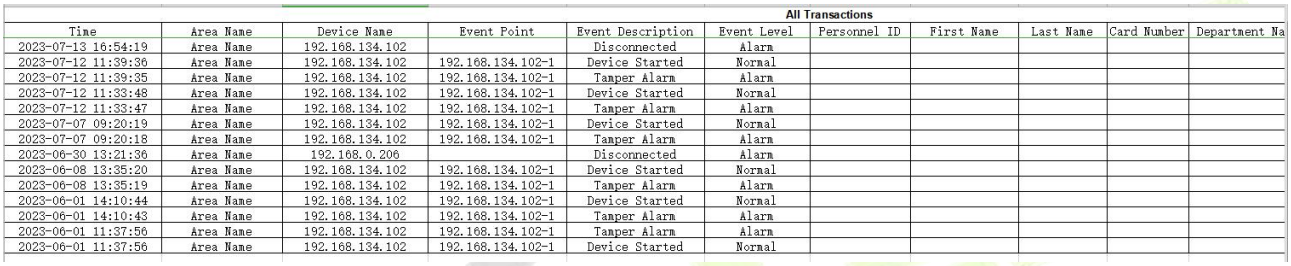


Figure 3- 157 Report Export



All Transactions

Time	Area Name	Device Name	Event Point	Event Description	Event Level	Personnel ID	First Name	Last Name	Card Number	Department Na
2023-07-13 16:54:19	Area Name	192.168.134.102		Disconnected	Alarm					
2023-07-12 11:39:36	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					
2023-07-12 11:39:35	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-07-12 11:33:48	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					
2023-07-12 11:33:47	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-07-07 09:20:19	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					
2023-07-07 09:20:18	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-06-30 13:21:36	Area Name	192.168.0.206		Disconnected	Alarm					
2023-06-08 13:35:20	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					
2023-06-08 13:35:19	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-06-01 14:10:44	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					
2023-06-01 14:10:43	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-06-01 11:37:56	Area Name	192.168.134.102	192.168.134.102-1	Tamper Alarm	Alarm					
2023-06-01 11:37:56	Area Name	192.168.134.102	192.168.134.102-1	Device Started	Normal					

Figure 3- 158 Report Export

3.6.2Events From Today

Check out the system record today.

Click **Access Control Reports** > **Events from Today** to view today's records. You can export all events from today in Excel, PDF, CSV format.

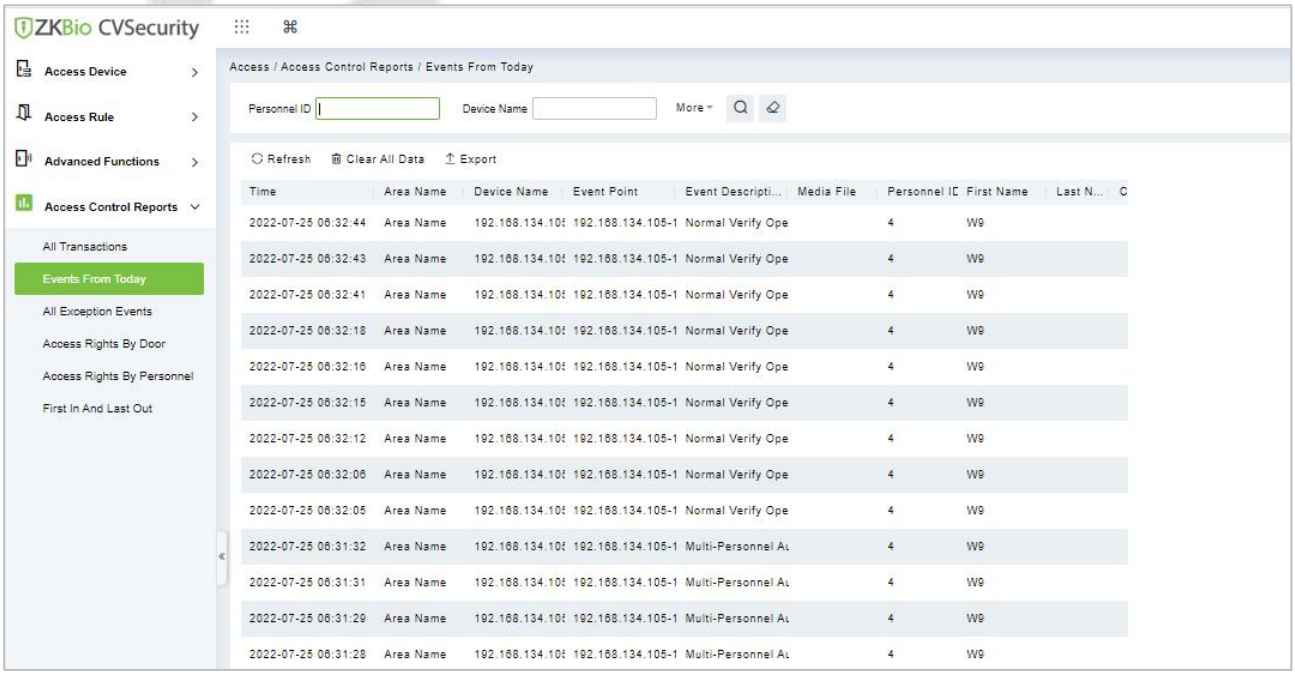


Figure 3- 159 Event from Today

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**.

ZKTECO

Events From Today

Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name	Remark
2017-12-15 18:29:02	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:59	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:45	13260079	5	Necol	Ye	Marketing Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:41	13260079	5	Necol	Ye	Marketing Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:38	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:35	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:23	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:20	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:17	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:13	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:06	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:01	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:23:52	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:16	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:12	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:02	6155266	2	Lucky	Tan	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:22:21	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:20:24	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	

Created on: 2017-12-15 18:36:55

Created from ZKBioSecurity software. All rights reserved. 1/30

Figure 3- 160 Report Export Page

Clear All Data: Click **Clear All Data** to pop up prompt, and then click **OK** to clear all events from today.

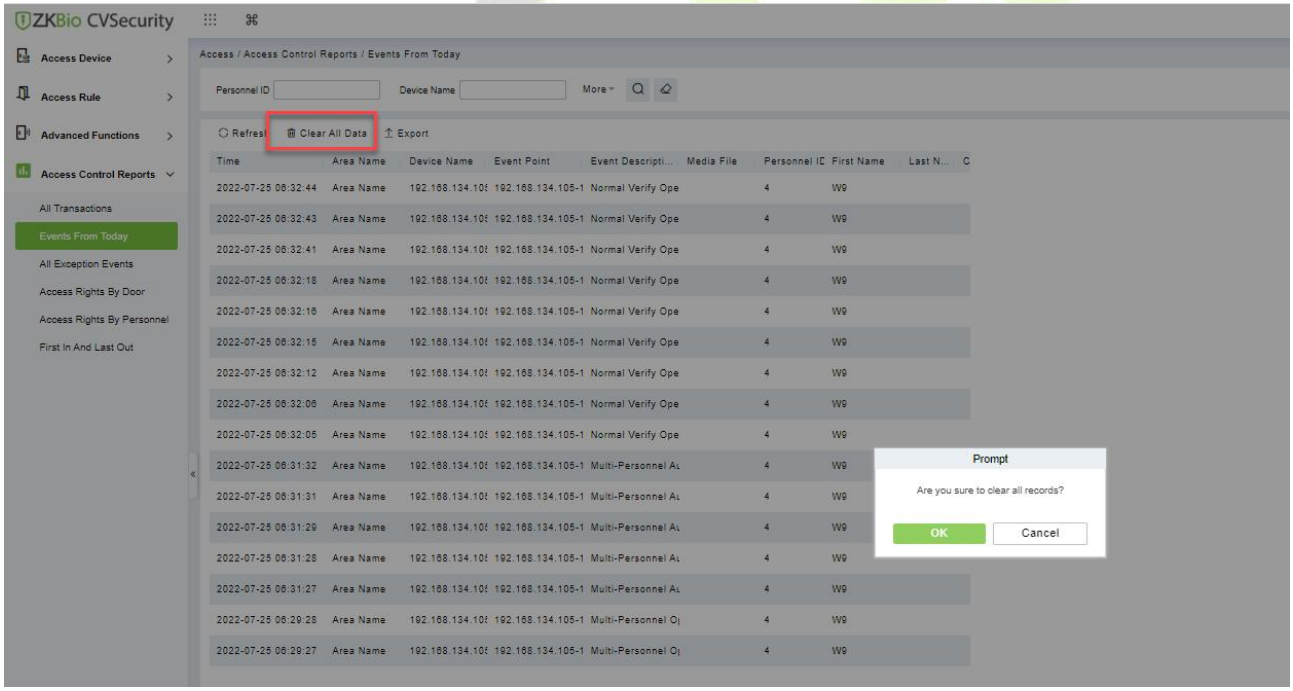


Figure 3- 161 Events Clear All Data

3.6.3All Exception Events

Click **Access Control Reports** > **All Exception Events** to view exception events in specified condition. The options are same as those of **All Transactions**.

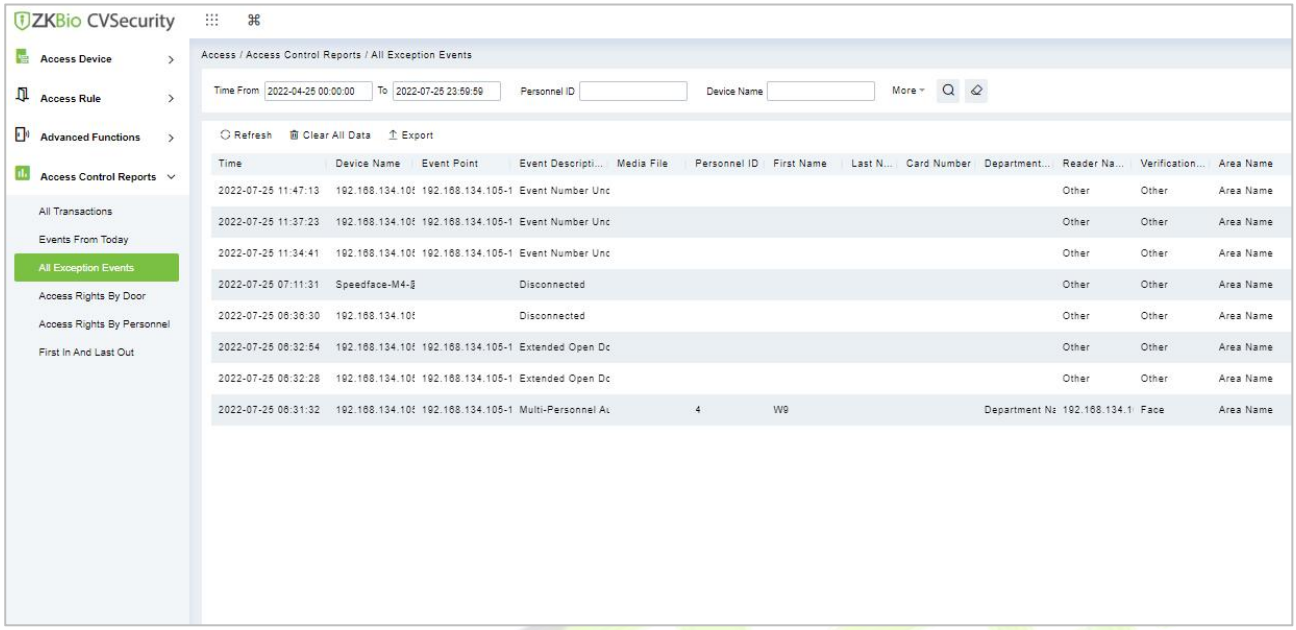


Figure 3- 162 All Exception events

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, CSV format.

ZKTECO

All Exception Events

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Time	Event Description	Event Point	Device Name	Card Number	Personnel ID	First Name	Last Name	Area Name	Department Name	Reader Name	Verification Mode	Remark
2017-12-15 17:43:03	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 17:42:41	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 17:35:27	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:35:17	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:35:06	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:34:00	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:52	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:43	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:35	Operation Interval too Short	192.168.218.60-2	192.168.218.60					Area Name		192.168.218.60-2-In	Other	
2017-12-15 16:33:14	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:06:54	Can not connect to server		192.168.218.60					Area Name		Other	Other	
2017-12-15 13:50:17	Disconnected		192.168.218.60					Area Name		Other	Other	
2017-12-15 11:53:45	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:41:04	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:19:45	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:19:37	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:05:50	Anti-Passback	192.168.218.60-1	192.168.218.60	9505930	800000005	Bill	Fang	Area Name	Visitor	192.168.218.60-1-In	Only Card	
2017-12-15 11:05:	Anti-Passback	192.168.218.60-1	192.168.218.60	13260079	800000004	Tom	Lee	Area Name	Visitor	192.168.218.60-1-	Only Card	

Created on: 2017-12-15 18:37:19

1/3

Figure 3- 163 All Exception Events Export

3.6.4Alarm Log

View all the alarm logs and be able to make remarks.

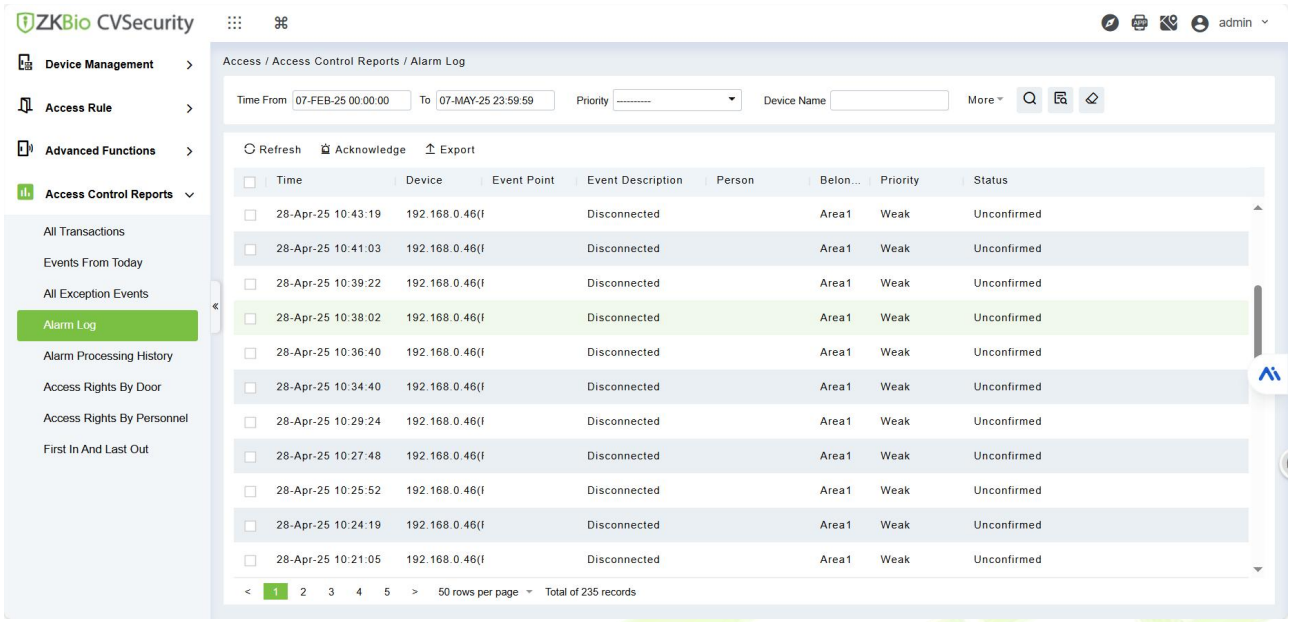


Figure 3- 164 Alarm Log

3.6.5Access Rights By Door

View related access levels by door. Click **Access Control Reports** > **Access Rights by Door**, the data list in the left side shows all doors in the system, select a door, the personnel having access levels to the door will be displayed on the right data list.

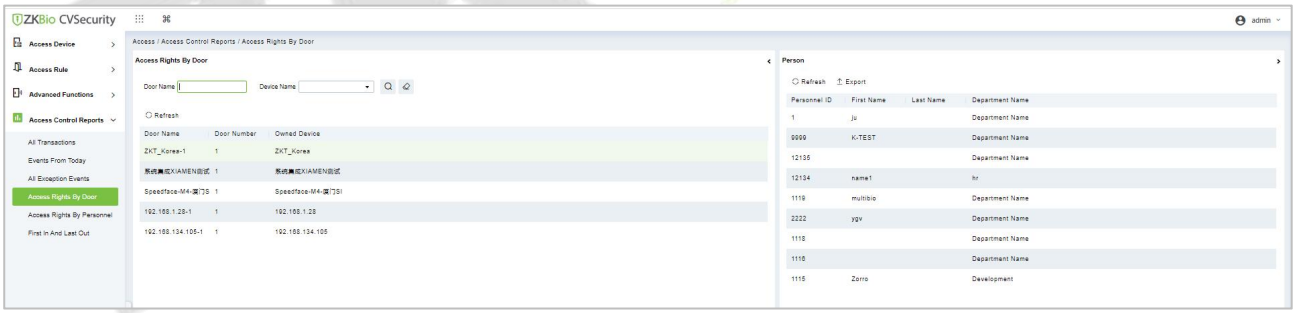


Figure 3- 165 Access Right by Door

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

ZKTECO

192.168.218.60-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
4	Berry	Cao	General
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
7	Jacky	Xiang	General
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department

Figure 3- 166 Access Right by Door Export Page

3.6.6Access Rights By Personnel

View related access levels by door or personnel.

Click **Access Control Reports** > **Access Rights by Personnel**, the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

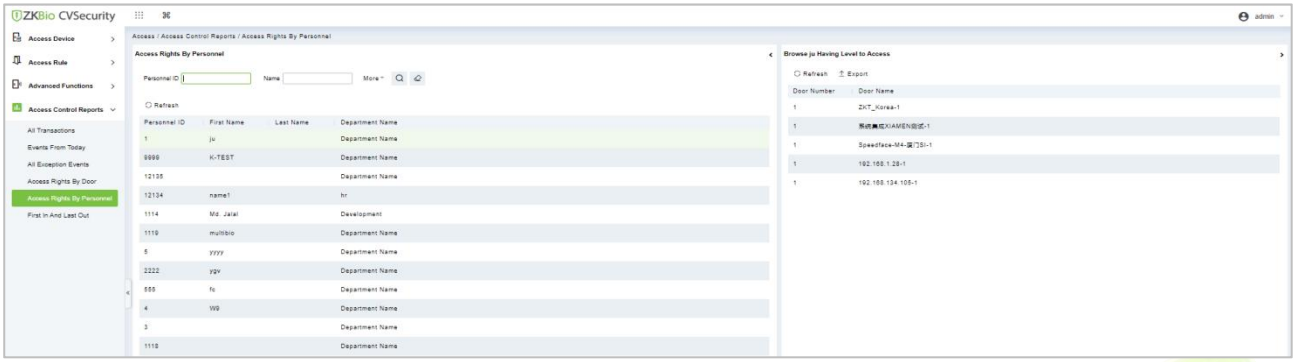


Figure 3- 167 Access Right by Personnel

You can export all the door information in Excel, PDF, CSV format.

ZKTECO

6(Amber) Having Level to Access

Door Number	Door Name
1	192.168.218.60-1
2	192.168.218.60-2
3	192.168.218.60-3
4	192.168.218.60-4

Figure 3- 168 Access Right by Personnel Export Page

3.6.7First In and Last Out

Click **Access Control Reports** > **First in And Last Out** to view the First and the Last time interval.

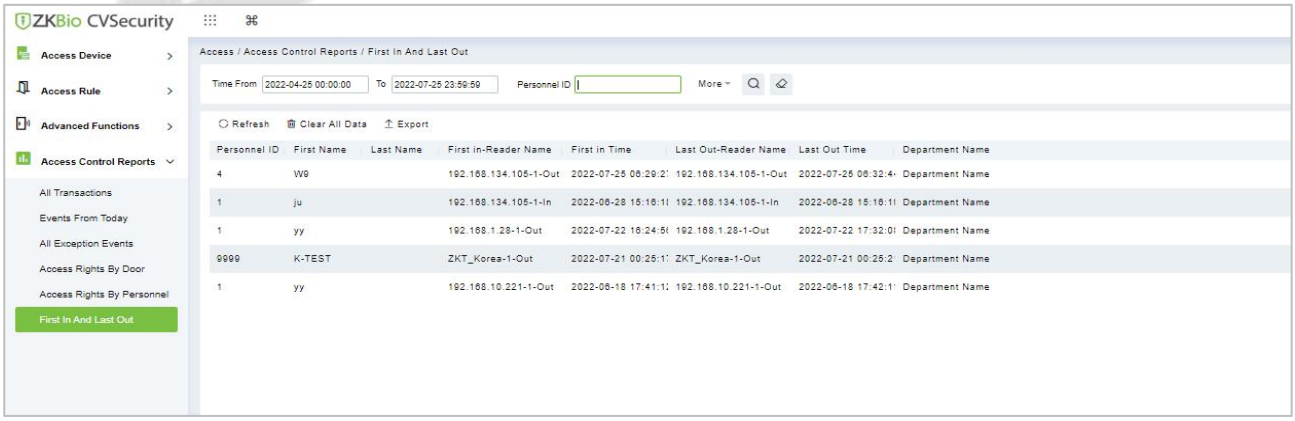


Figure 3- 169 Access Right by Door Export Page

3.6.7.1Clear All Data

In the Access > Advanced Control Reports > First in and Last Out, click **Clear All Data** button under Operations. Click **OK** to clear all data.

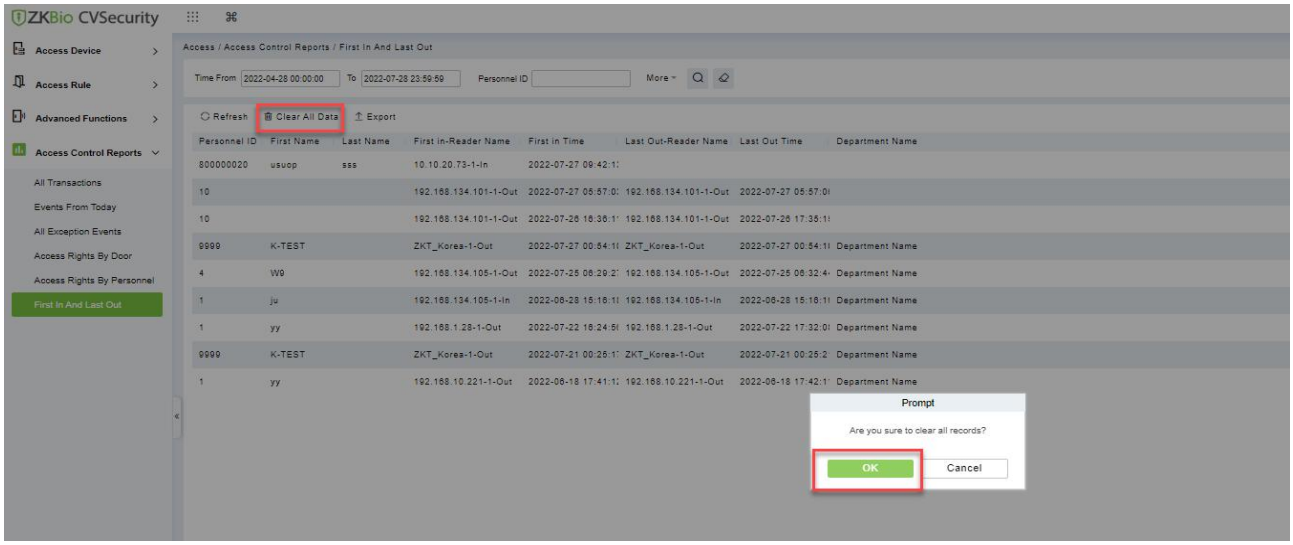


Figure 3- 170 Clear All Data

4 Video Intercom

4.1 Basic Management

This section describes how to make basic settings in ZKBio CVSecurity.

4.1.1 Building

4.1.1.1 Add Building

Operation Step:

Step 1: In the Video Intercom module, choose "**Basic Management > Building**".

Step 2: Click **New**, the page for adding buildings will be displayed.

Step 3: On the page where buildings are added, configure the necessary content as shown in the figure below. Also, adjust the parameter settings as indicated in the same figure.

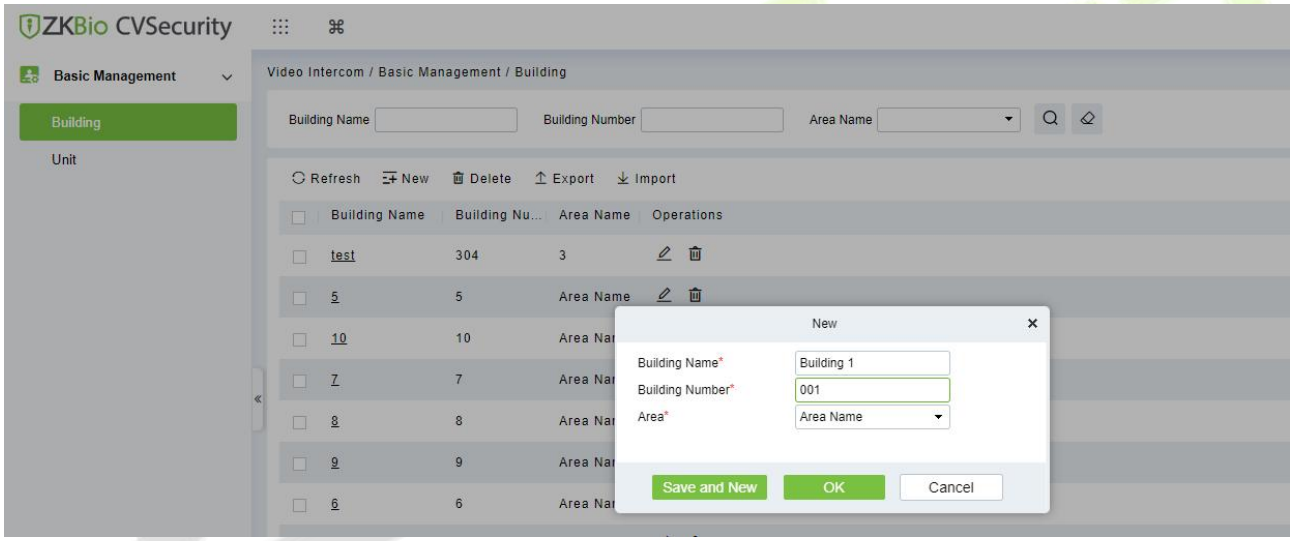


Figure 4- 1 Building Add Interface

Parameter	Description
Building Name	Enter the name of the building.
Building Number	Enter the number of the building.
Area	Select the area name.

Table 4- 1

4.1.1.2 Delete

Select the Building, click **Delete**, and then, click **OK** to delete the building.

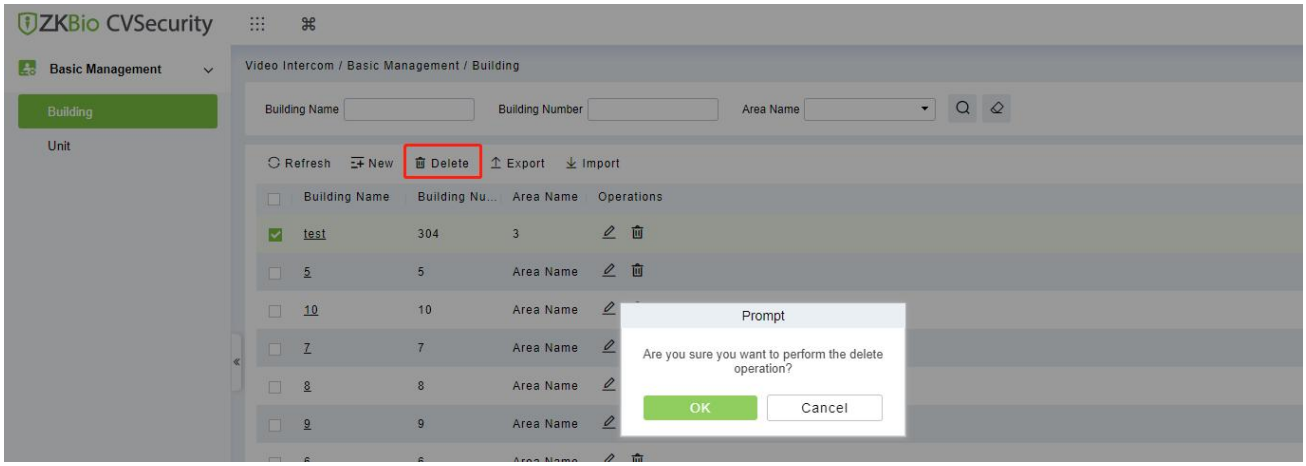


Figure 4- 2 Delete Building

4.1.1.3Edit

Select the Building, click **Edit**, and then, click **OK** after editing the building details.

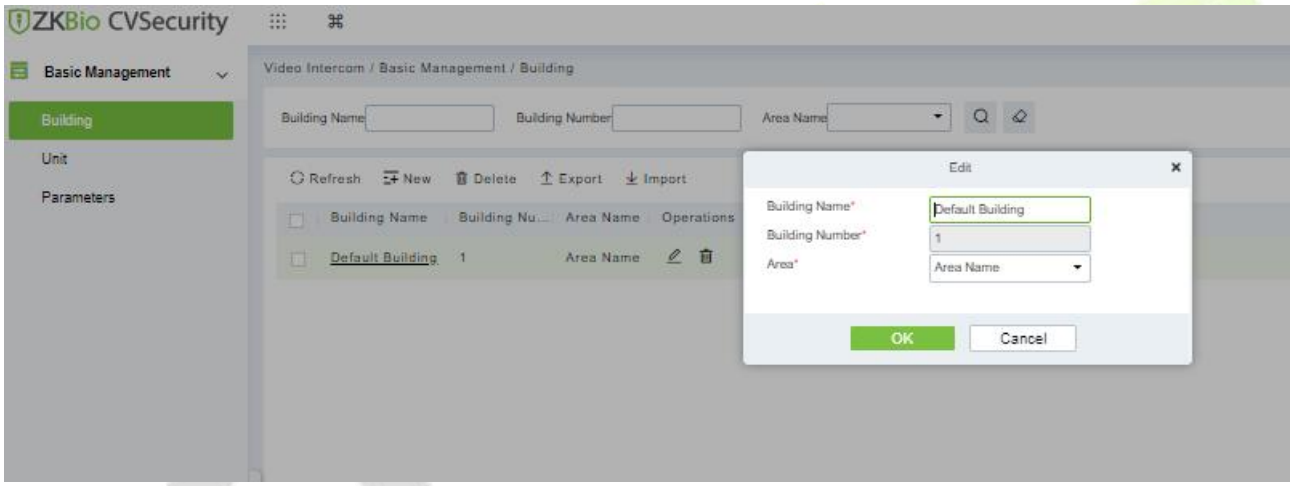


Figure 4- 3

4.1.1.4Import

Batch import floor data based on the provided template.

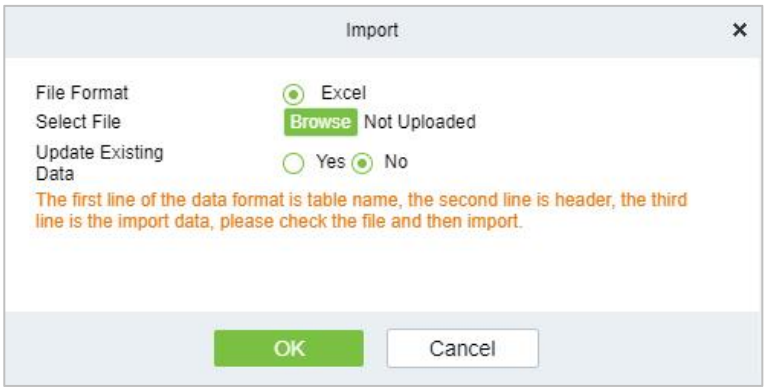


Figure 4- 4 Import

4.1.1.5Export

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

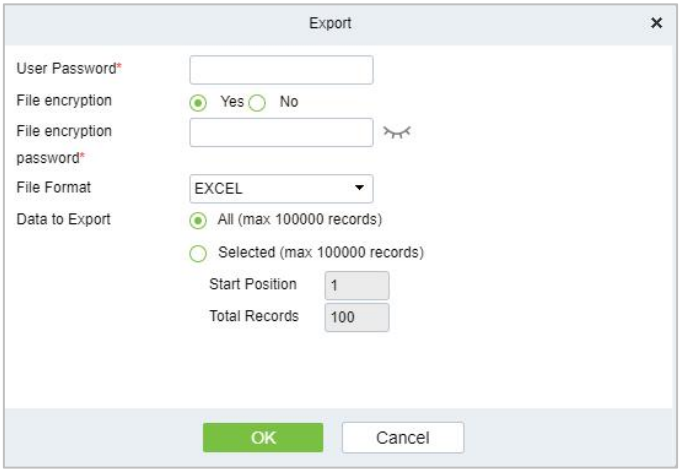


Figure 4- 5 Export

4.1.2Unit

4.1.2.1Add Unit

Operation Step:

Step 1: In the Video Intercom module, choose "**Basic Management > Unit**".

Step 2: Click **New**, the page for adding units will be displayed.

Step 3: On the page for adding units, set the required content as shown in the figure below.

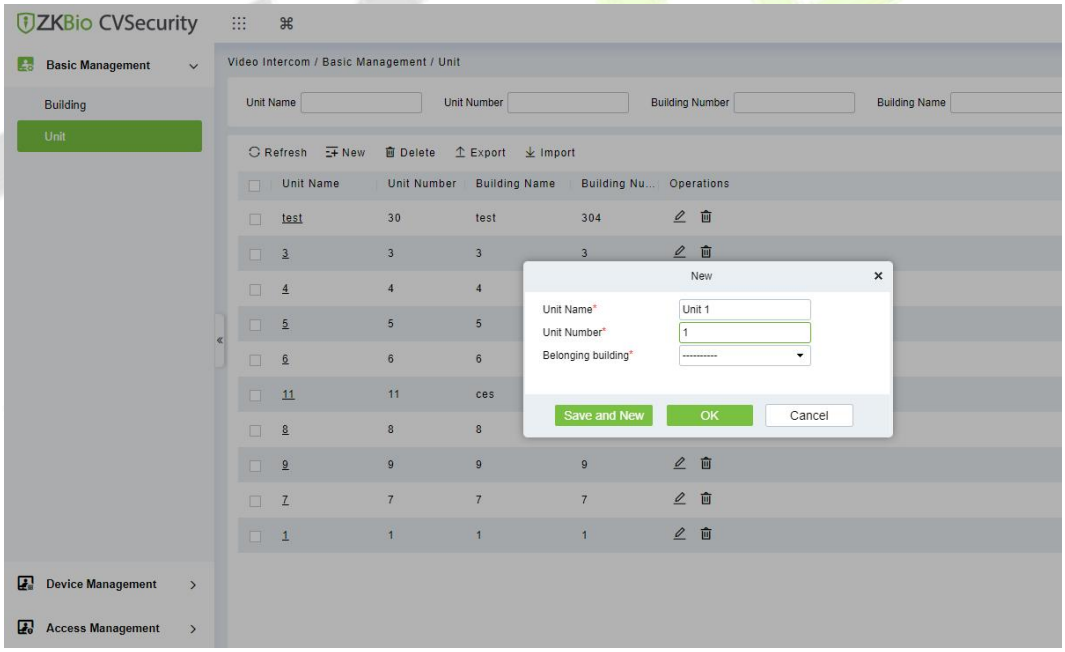


Figure 4- 6 Unit Add Interface

Parameter	Description
Unit Name	Enter the name of the unit.
Unit Number	Enter the unit number.
Belonging Building	Select the belonging building.

Table 4- 2

4.1.2.2Delete

Select Unit, click **Delete**, and click **OK** to delete the unit.

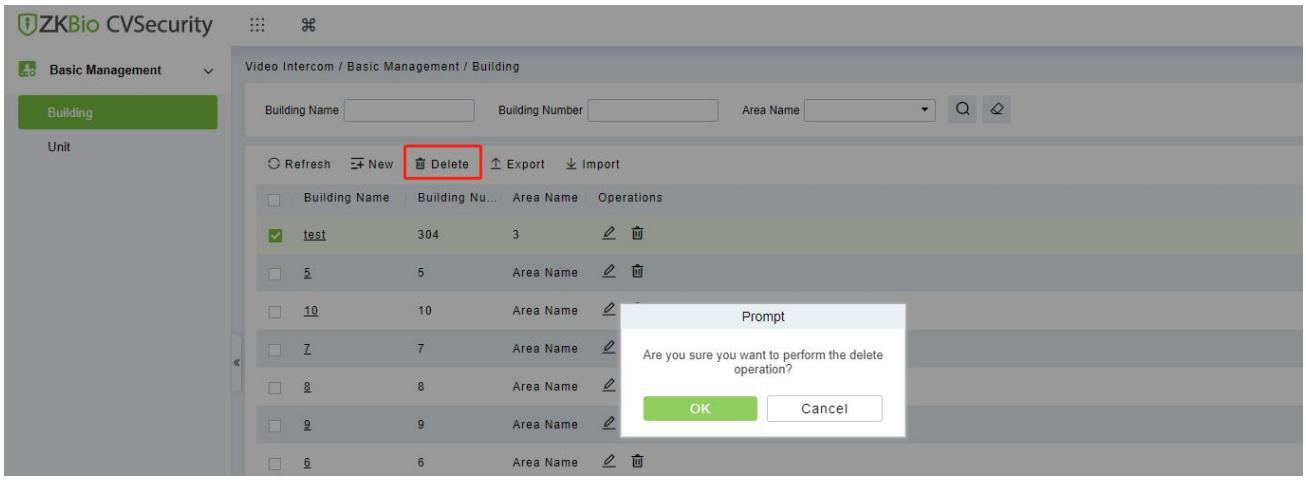


Figure 4- 7 Unit Delete

4.1.2.3Edit

Select Unit, click **Edit**, and then click **OK** after editing the unit details.

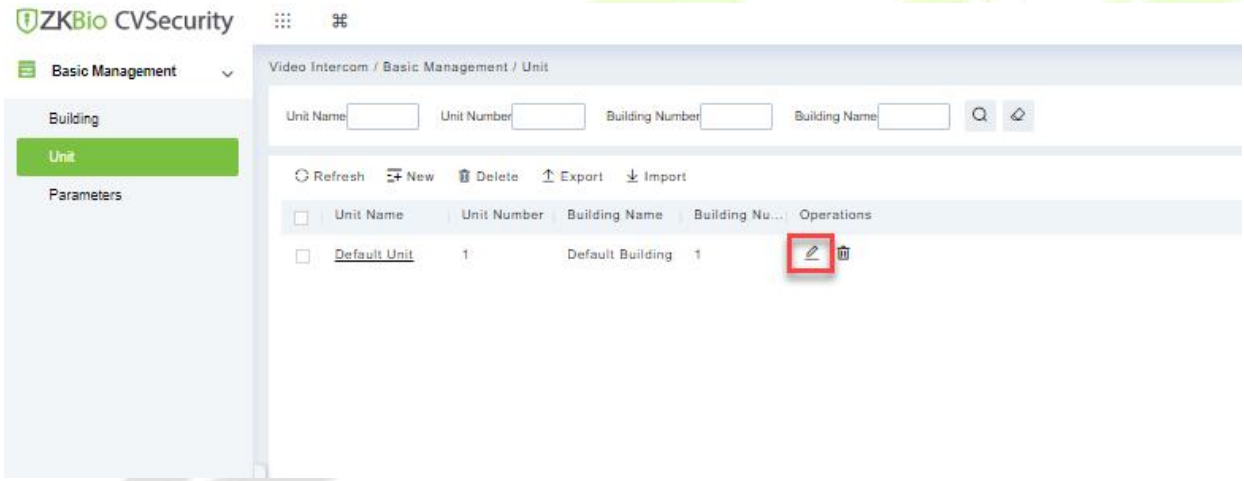


Figure 4- 8

4.1.2.4Export

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

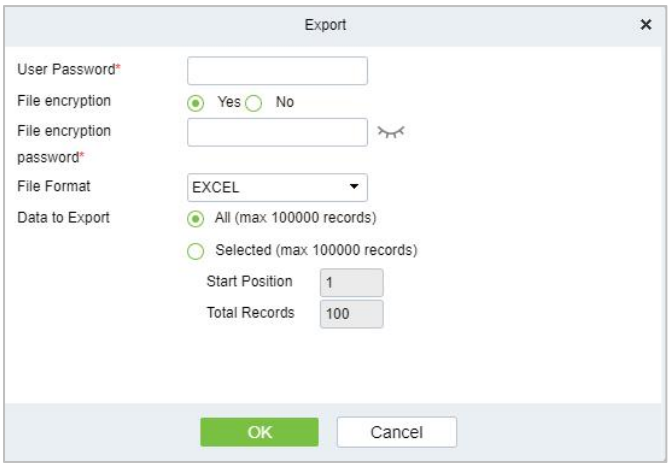


Figure 4- 9 Export

4.1.2.5Import

Batch import floor data according to the added template.

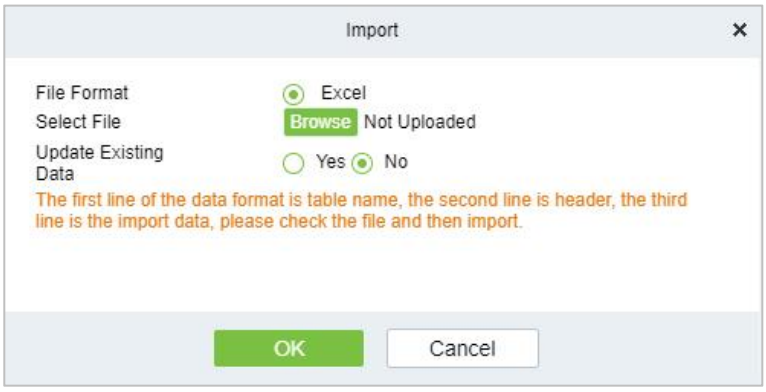


Figure 4- 10 Import

4.1.3Parameter

This menu is used for configuring DTMF,APP Call Number Type and SIP Service Mode.

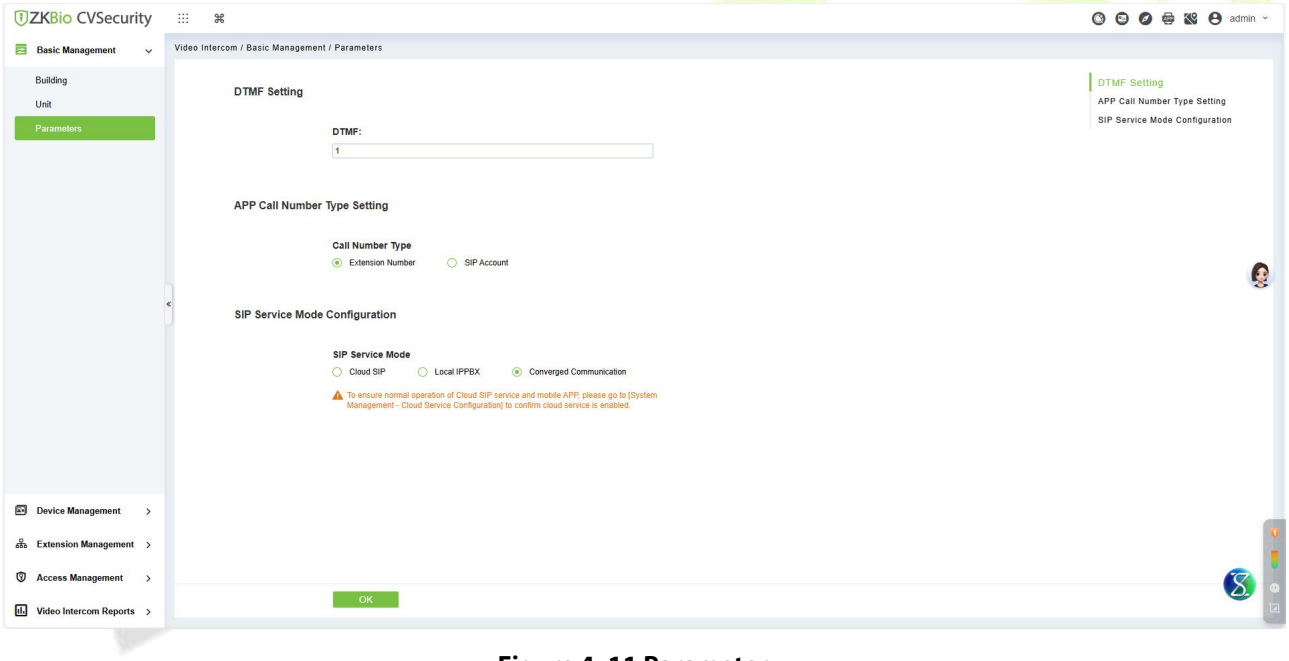


Figure 4- 11 Parameter

● DTMF

DTMF (Dual-Tone Multi-Frequency) is a telephone communication technology used to send 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.

● APP Call Type

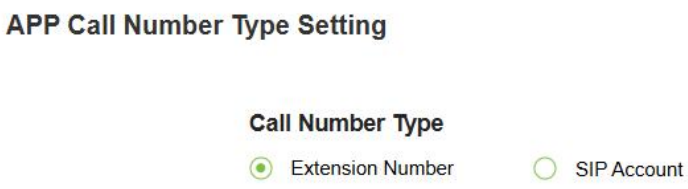


Figure 4- 12 App Call Type

It is used to configure the call type of the APP, and the extension number or SIP account can be selected.

Result Verification

For example, if the extension number is selected, only the extension number can be entered for dialing when the APP makes a call. If the SIP account is entered, the APP will prompt that the extension number does not exist.

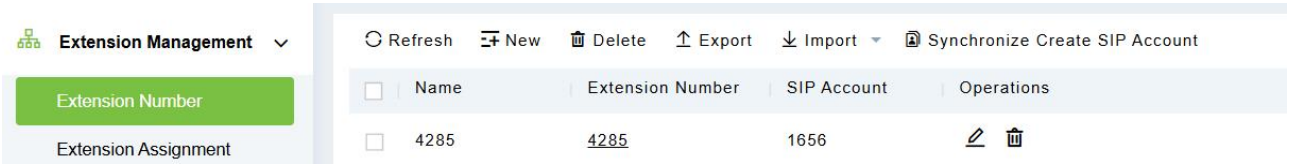


Figure 4- 13 Result Verification

As shown in the following figure, if a SIP account is entered in the APP, a prompt will be displayed saying "The extension number does not exist.

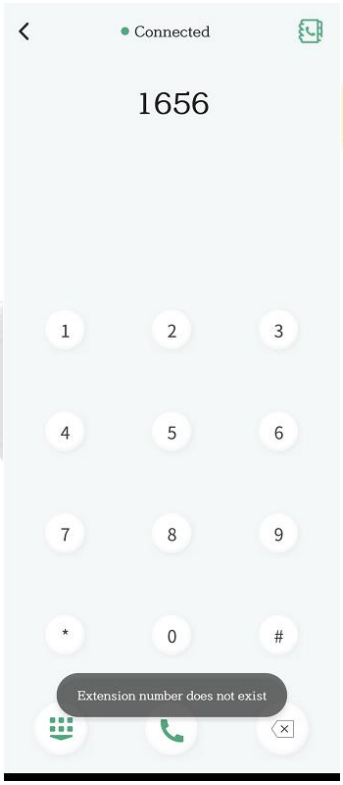


Figure 4- 14 Result Verification

SIP Service Mode

Figure 4- 15 SIP Service Mode

The system supports three SIP service modes. Select the mode that best suits your deployment requirements:

- Cloud SIP: When this mode is selected, the system will adopt cloud - based SIP service. Through Cloud SIP, users can enjoy convenient remote communication services and can seamlessly connect with other devices and services that support Cloud SIP.
- Local IP PBX: When this mode is selected, the system will use the locally deployed IP PBX to manage and process SIP communications. This is suitable for environments requiring local storage and management of communication data. Scenarios with limited or restricted internet connectivity and deployments with tight restrictions on data location and ownership.
- Converged Communication: This mode integrates multiple communication methods to realize the integration of functions such as voice, video, and instant messaging. When the converged communication mode is selected, users can perform diversified communication operations on a unified platform, improving communication efficiency and experience.

Note: Cloud service must be enabled. Navigate to System Management > Cloud Service Configuration to enable cloud services before using Cloud SIP mode or the mobile APP.

4.2 Device Management

4.2.1 DNK Device Operation Guide

DNK Type :the devices supported by this type include:

- Outdoor unit: VEX-B21L, VEX-B21A, VEX-B24L, VEX-B24A, VEX-B25L
- Indoor unit:VT07-B22L,VT07-B26L-W,VT10-B21A,VT10-B21L

4.2.1.1 Add Devices

Step 1: Go to **Video Intercom > Device Management > Device**.

Step 2: Click **New**, the interface for adding a device will be displayed.

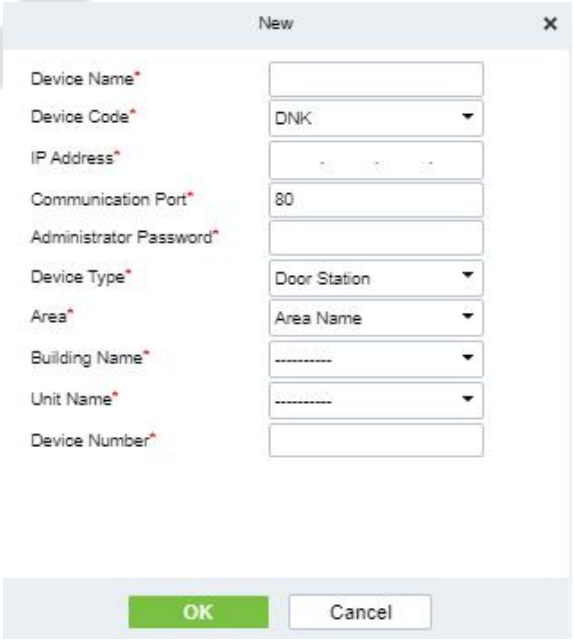


Figure 4- 16 Device Add Interface

Step 3:Manufacture: please select **DNK**.Please add the corresponding parameters.

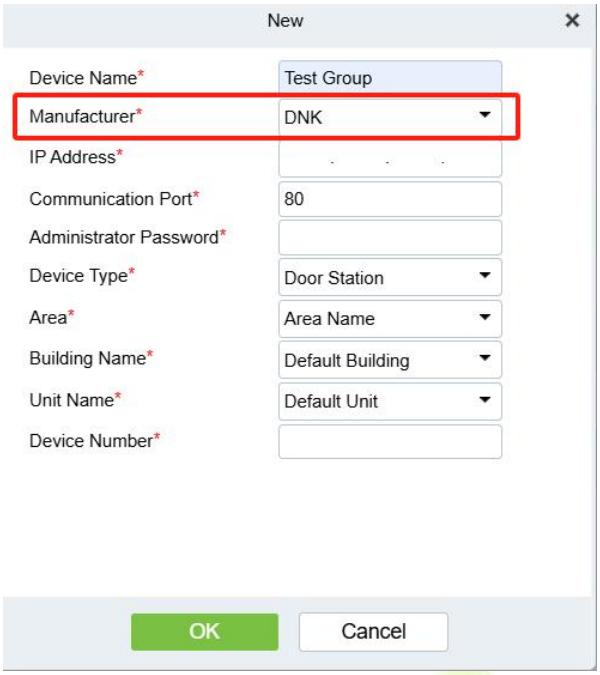


Figure 4- 17 Device Add Interface

Parameter	How to set
Device Name	Customize the name of the device.
Device Code	Select the device code.
IP Address	Fill in the IP address of **Video Intercom** device.
Communication Port	Enter the communication port number of the device.
Username	Enter the username of the device.
Administrator Password	Fill in the administrator password.
External Network Address	Enter the external address of the device.
Transport Protocol	Select the transport protocol of the device.
Device Type	• Select the device type you want to add, support to select outer station, outdoor station, doorbell station and indoor Station. • If select **Outer Station**, you should choose the device area and choose whether to enable the unit number. • If select **Door Station**, you should choose device area, Building and unit. • If select **Doorbell Station**, you should choose area, building, unit and room. • If select **Indoor Station**, you should choose area, building, unit and room, and fill in the Sync Code.
Area	Divide the device into regions and select the region to which the device belongs.
Building	Please first configure the building where the device is located in the "Building" settings.

Unit Name	Please first configure the unit where the device is located in the "**Unit**" settings.
Device Number	Customize the number of the device.

Table 4- 3 Parameter setting

4.2.1.2Delete

Step 1: On the Device interface, select the required Device from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

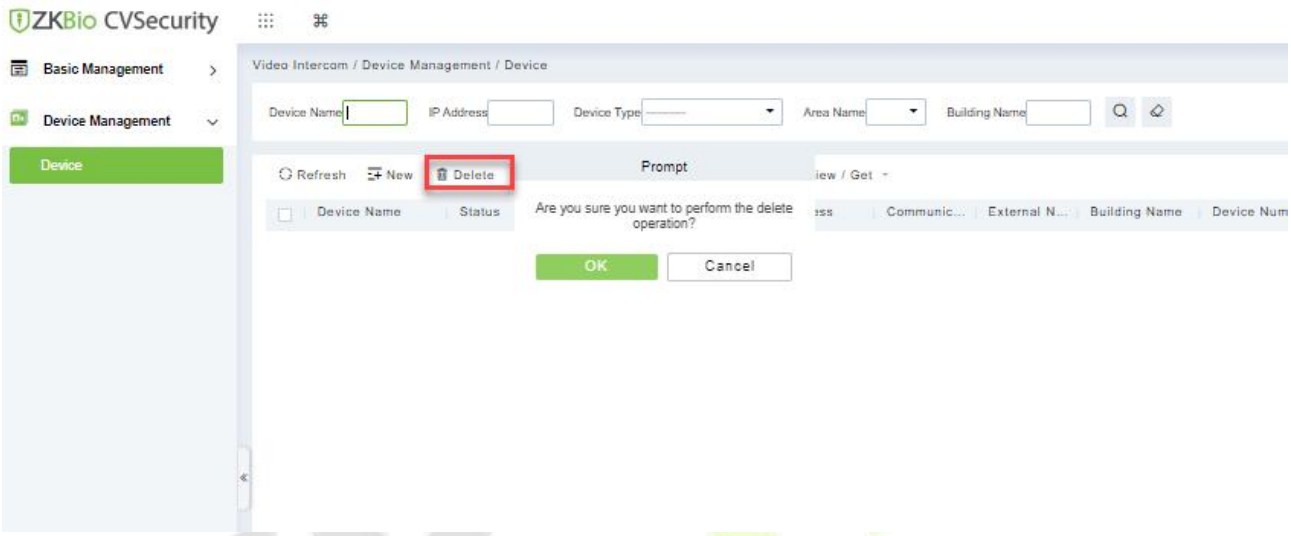


Figure 4- 18 Device Delete Interface

4.2.1.3Export

You can export all transactions in Excel, PDF, CSV format.

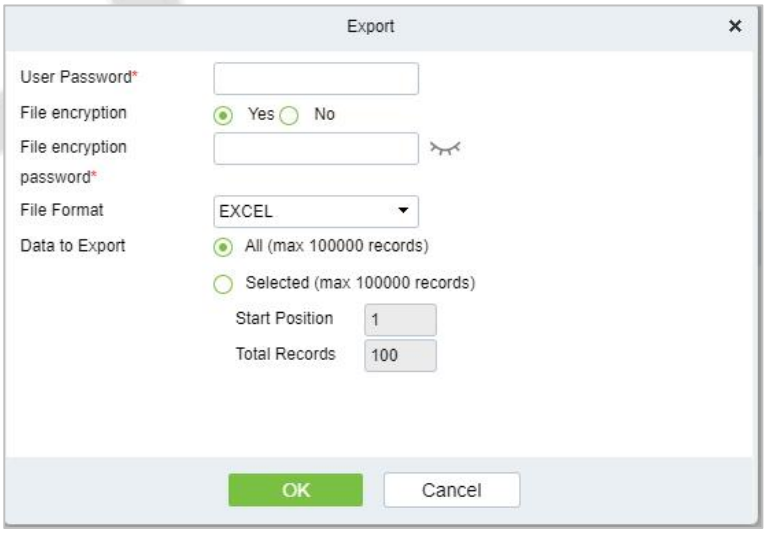


Figure 4- 19 Export video intercom Configuration Flow

4.2.1.4Import

If you need to add DNK Device in bulk, you can use the Import function.

Step 1: Click on **Import -> Download Import Template**, select the parameters to be filled in, and download the template "Video Intercom Device Information Template.xls" locally.

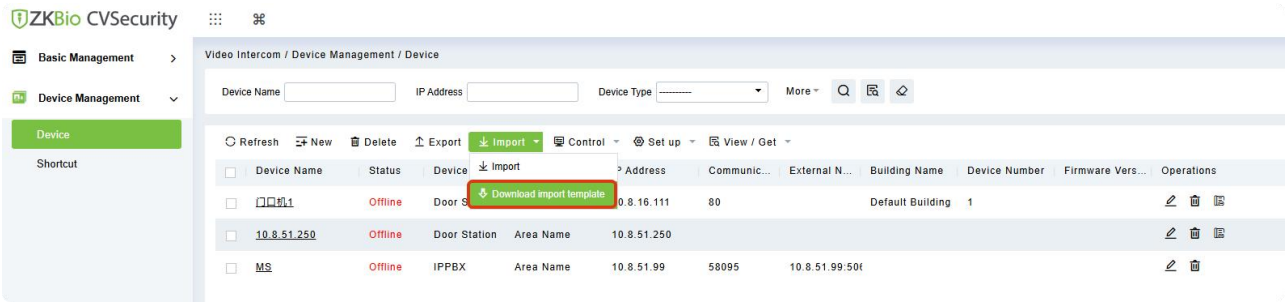


Figure 4- 20 Device Import Interface

Step 2: Fill in the device-related information according to the table notes as required.

Video Intercom Device Information Template

Device Name	Device Type	IP Address	ministrator Passw	Area Name	Device Number	Building Name	Unit Name	Sync Code
SC	0	10.8.16.111	Admin123	Area Name	0	Default Building	Default Unit	111
JH	3	10.8.51.250	Admin124	Area Name	1	Default Building	Default Unit	111
JS	3	10.8.51.99	Admin125	Area Name	2	Default Building	Default Unit	111
MK	3	10.8.51.77	Admin126	Area Name	0	Default Building	Default Unit	111

Figure 4- 21

Note: When downloading and importing the template to fill in the information, be sure to carefully check the table annotations and fill in the data as required by the annotations.Click on the small red triangle in the upper right corner of the table to view the annotation content.

Step 3: Click on **Import -> Import**, then click **Browse** to select the import template, and click **OK** to start the bulk import process.

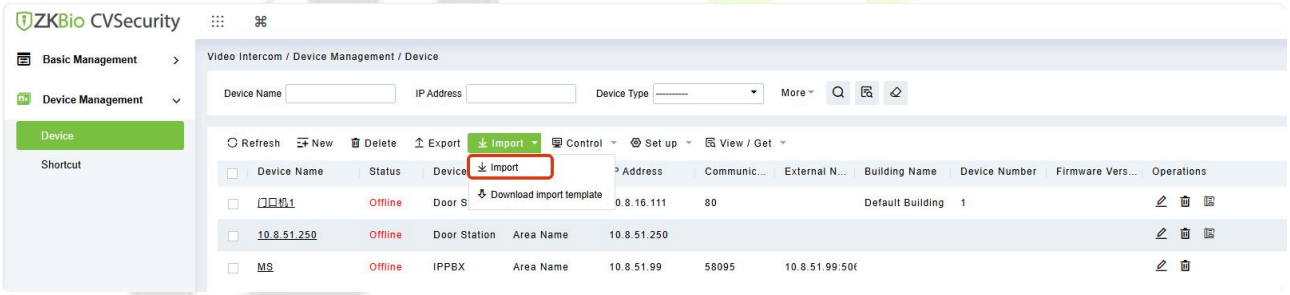


Figure 4- 22 Device Import Interface

4.2.1.5Control

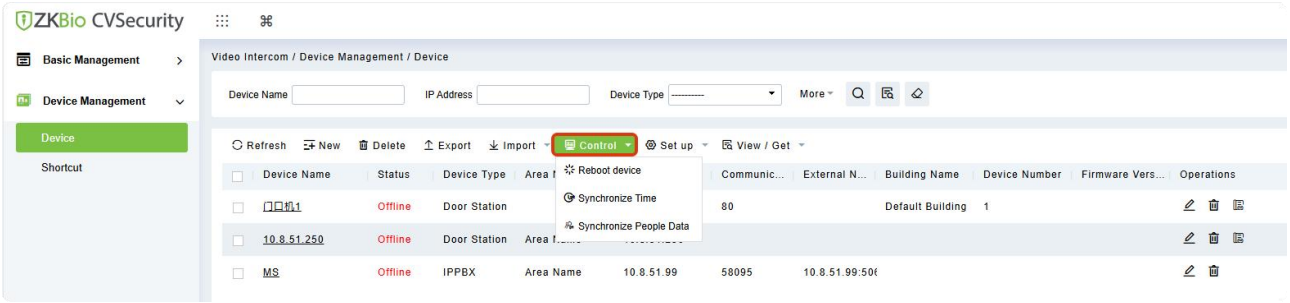


Figure 4- 23 Device Control Interface

- Reboot Device

It will reboot the selected device.

- Synchronize Time

It will synchronize device time with 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.

4.2.1.6 Set up

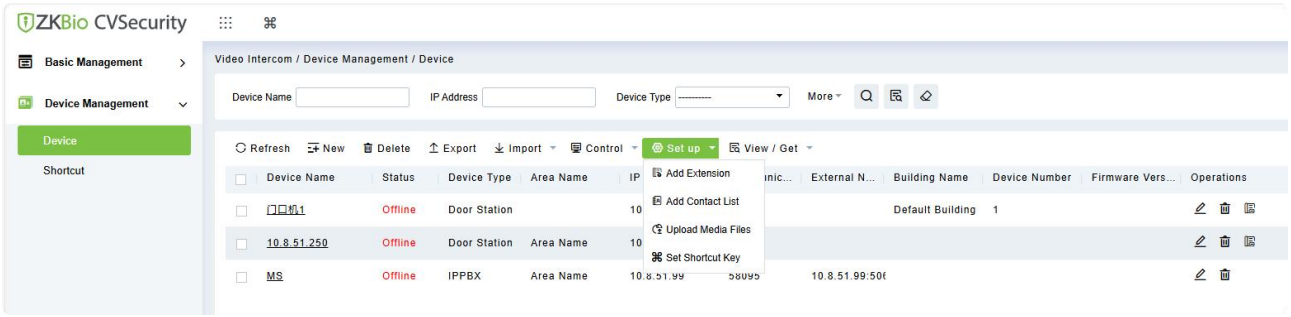


Figure 4- 24 Device

● Add Extension

It will add the extension for the device.

● Add Contact List

It will add the contact list to the device.

● Upload Media Files

Click to upload the media files for the device.

● Set Shortcut Key

Click to set a shortcut for the device.

4.2.1.7 View/Get

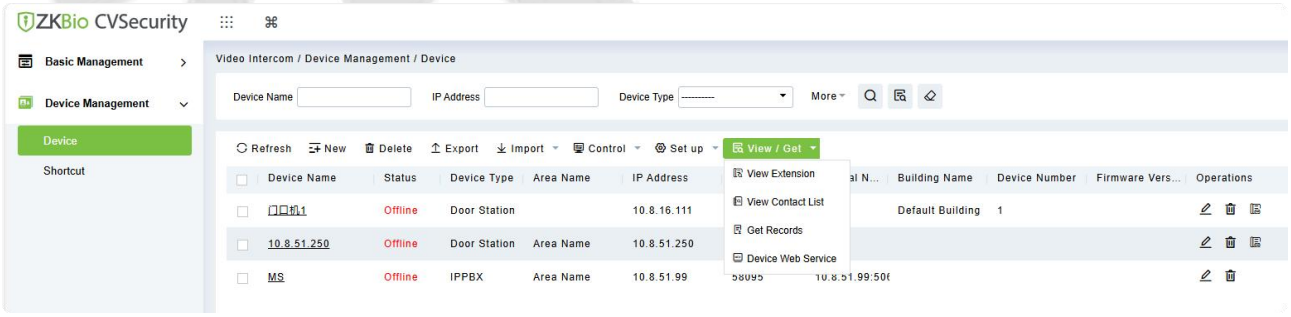


Figure 4- 25 Device

● View Extension

Select device and click View Extension to get the device extension data.

● View Contact List

Select device and click View Contact List to get the device contacts details.

Select device and click get records to get the device data.

● Device Web Service

Select device and click Device Web Service to get the web service details of the device.

4.2.2 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 do not wish to purchase IPBX server hardware, you can also subscribe to our cloud SIP. The following steps mainly illustrate the operational instructions for the GDS PBX service.

● GDS Device

Step 1: Go to **Video Intercom > Device Management > Device**.

Step 2: Click **New**, the interface for adding a device will be displayed.

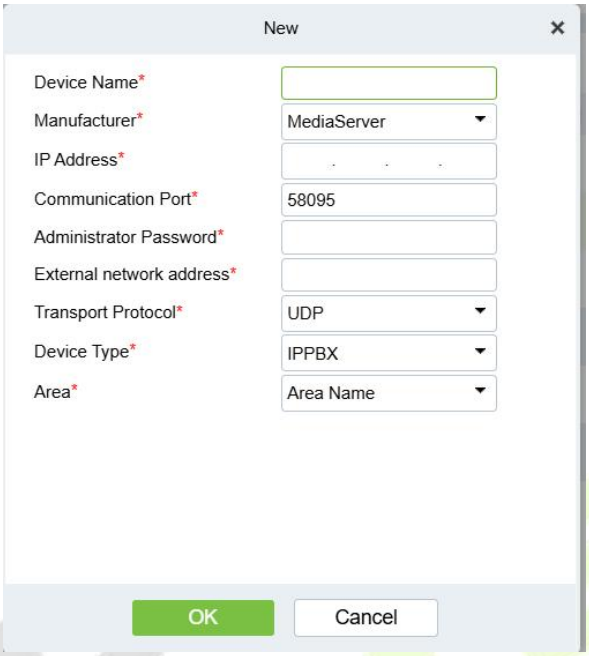


Figure 4- 26 Device Add Interface

Step 3:Manufacture :please select the brand.and add update corresponding parameters.

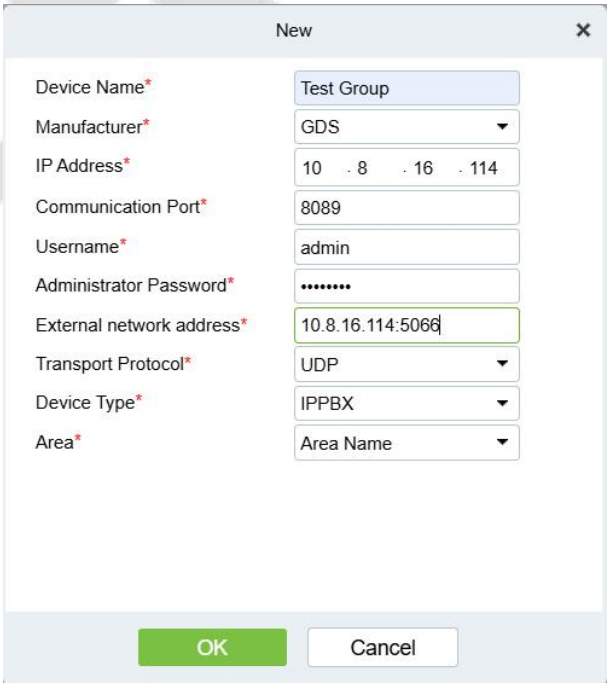


Figure 4- 27 GDS Parameter

Parameter	How to set
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**.
User Name	The user name 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	Area in which the PBX server is located

Table 4- 4 GDS Parameter

4.2.3Shortcut

Enter Video Intercom → Device Management → Shortcut. Here, you can add or delete shortcut keys.

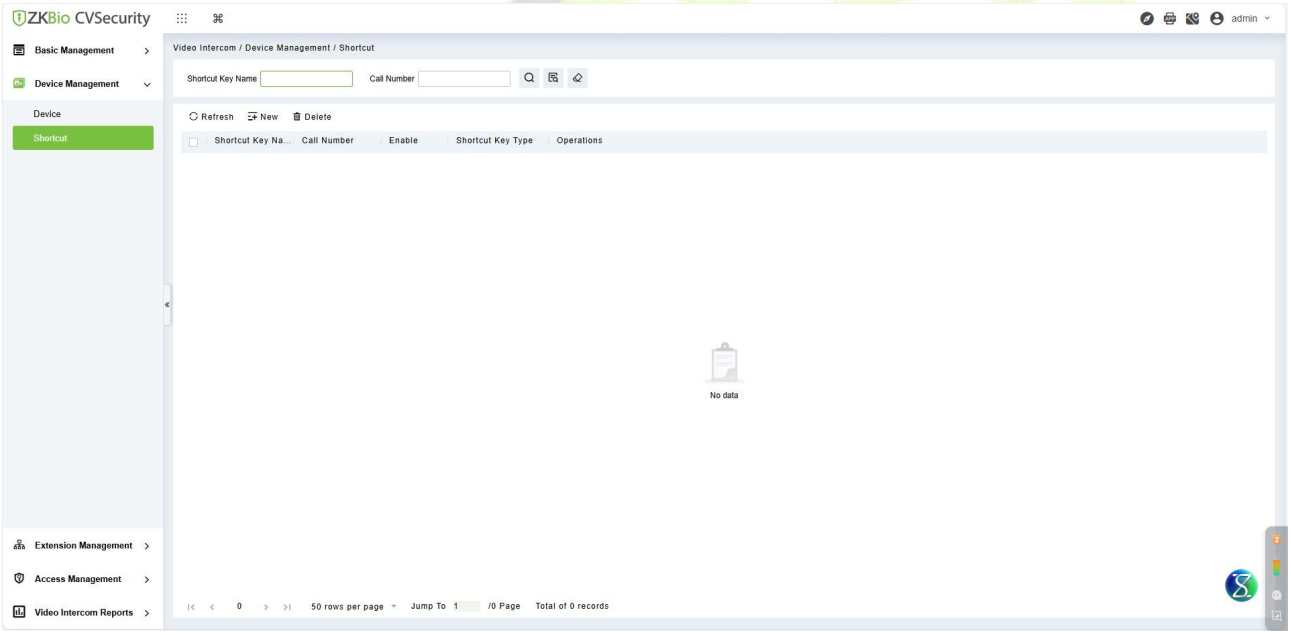


Figure 4- 28 Shortcut

Note: Currently, this function only supports ZKTECO access control devices and does not support DNK devices.

Step1: Click "New", fill in the Shortcut Key Name and the Call Number (if the SIP Service Mode is Cloud Sip, fill in the sip account; if the SIP Service Mode is Local IPPBX, fill in the extension number), check whether to enable it, and select the binding type as Normal user or Admin.

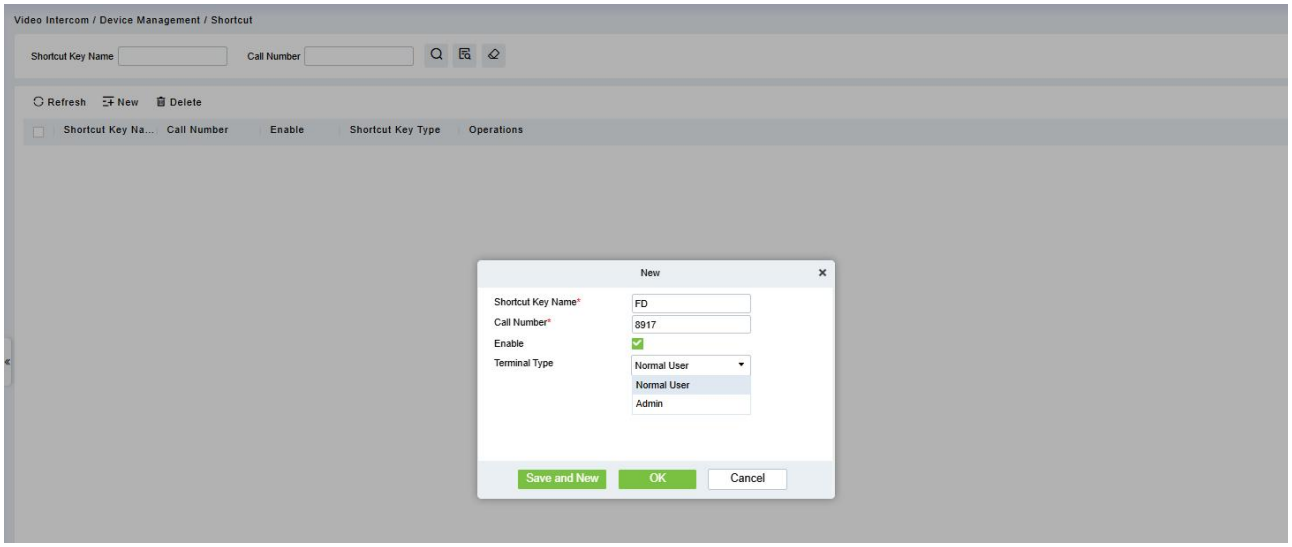


Figure 4- 29

Step 2: After adding the shortcut keys, go to Video Intercom → Device Management → Device, select the device, and then click "Set up" → "Set Shortcut Key".

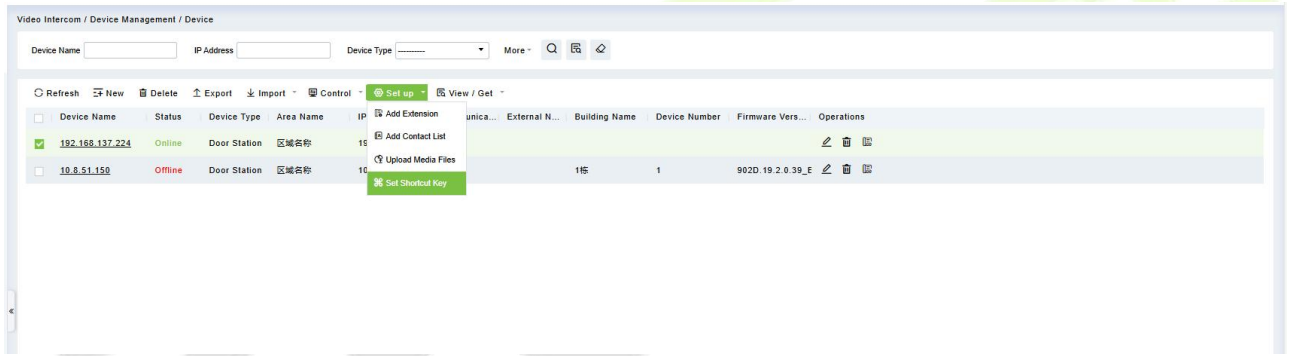


Figure 4- 30

Step 3: Click "Add Shortcut Key".

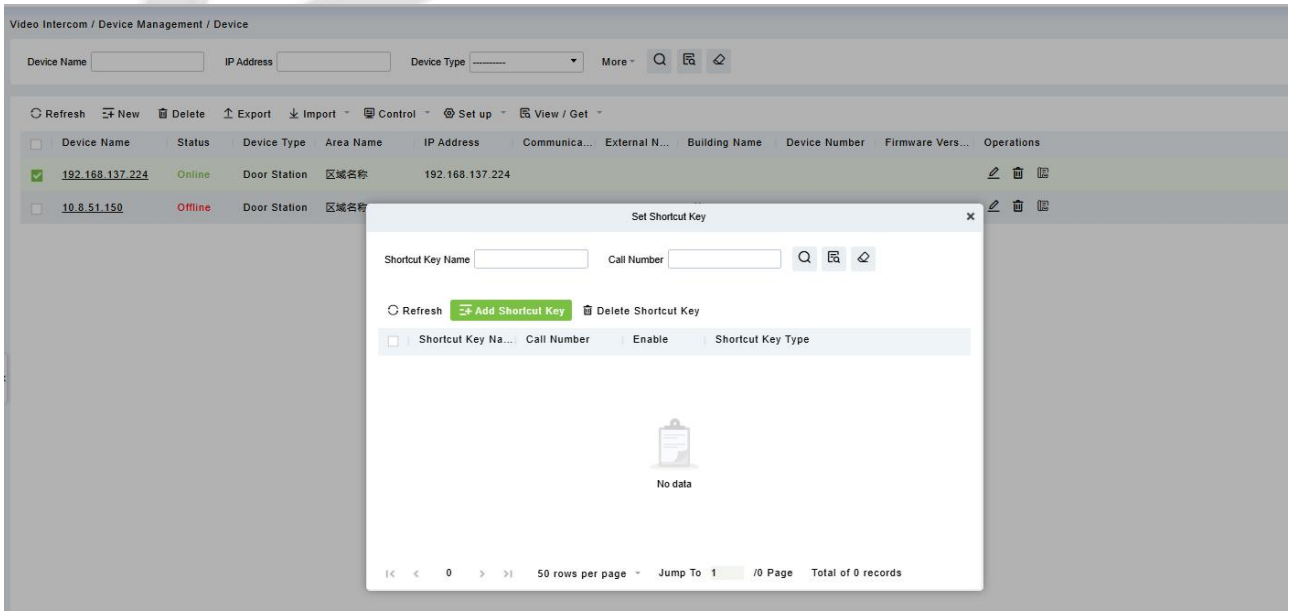


Figure 4- 31

Step 4: Move the shortcut key you want to add to the right side and click "OK" to complete the operation.

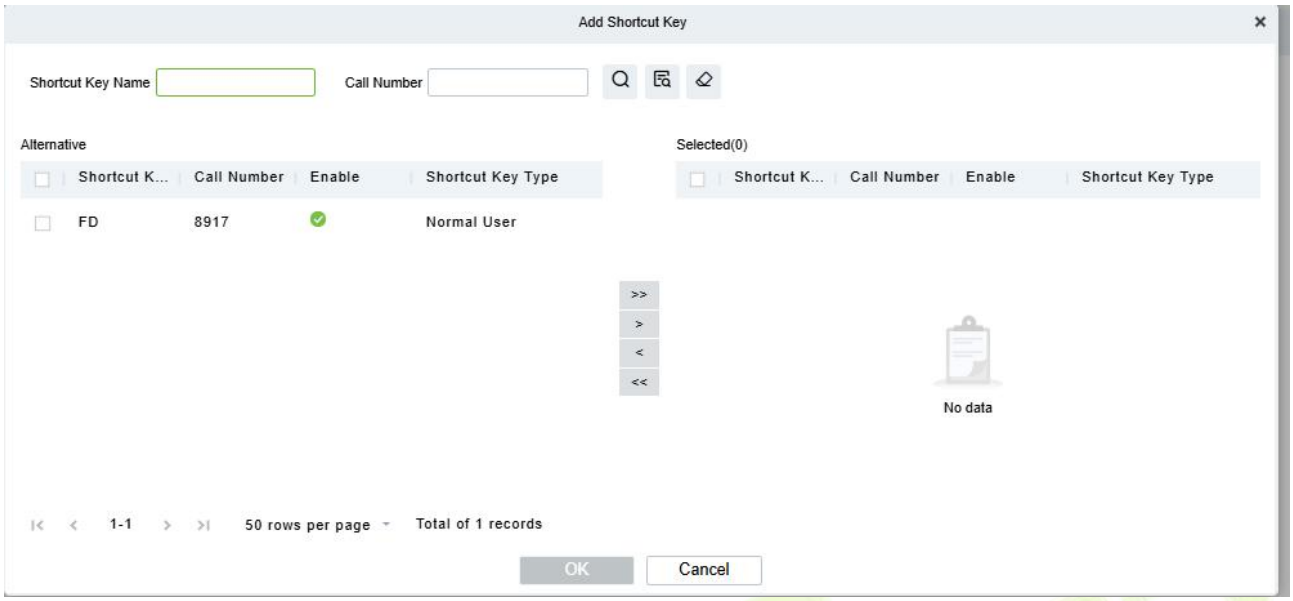


Figure 4- 32

After adding the shortcut key, go to the intercom Settings →SIP Settings → Call Shortcut key Settings of the access control door machine. You can view the newly added shortcut key. Click the "Doorbell" button on the device's home page to enter the intercom page, and you can call through the shortcut key.

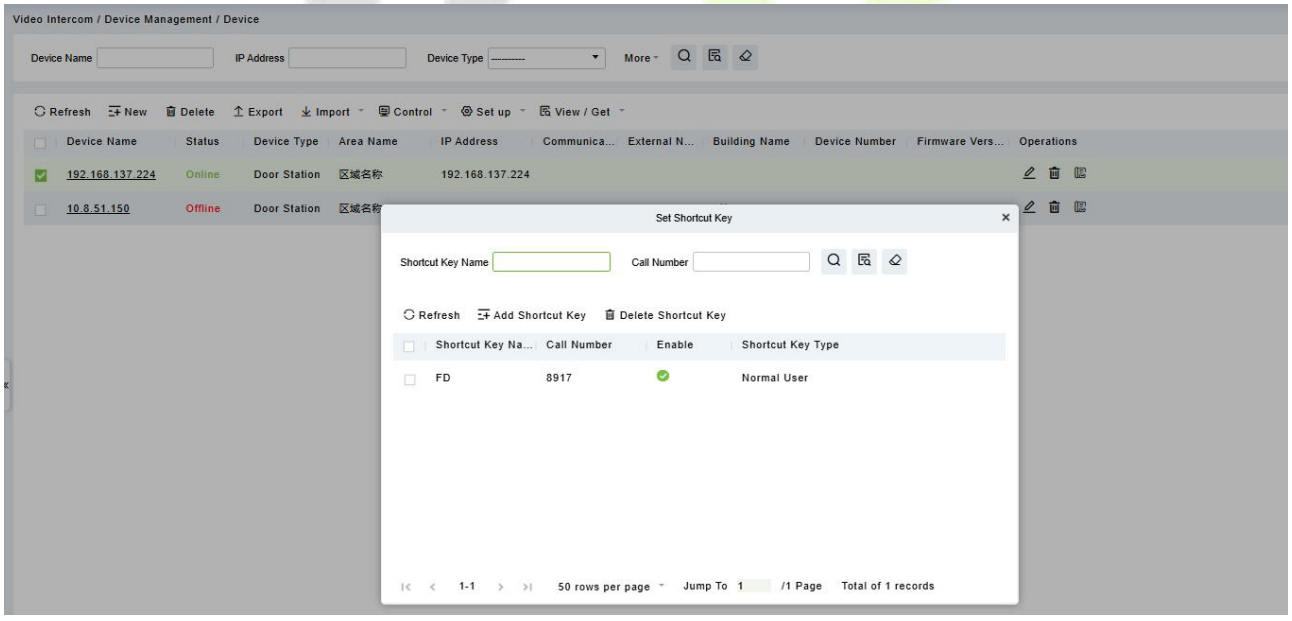


Figure 4- 33

After checking the shortcut key, click "Delete Shortcut Key" to delete the shortcut key. The access control door will delete it simultaneously.

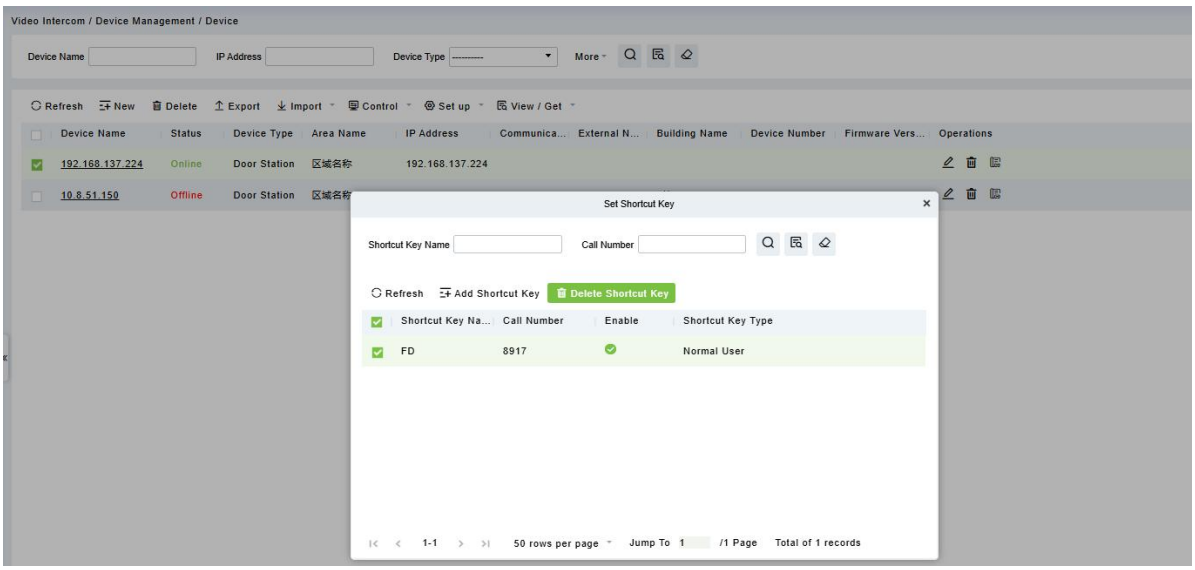


Figure 4- 34

4.3 Extension Management

This menu is used for managing and assigning extension numbers.

Prerequisite

ZKBio CVSecurity supports two types of SIP servers:

- PBX Server: For addition and operation methods, please refer to IPBX Device Operation Guide
- Cloud SIP: Enable Cloud Sip ,please refer to Cloud Setting

4.3.1 Extension Number

Usually used for internal telephone systems, an extension number is a number or code used within a company or organization to identify different telephone sets.

4.3.1.1 New

Click on **"New"** to add a single extension number. If you need to add in bulk, please use the "Import" function.

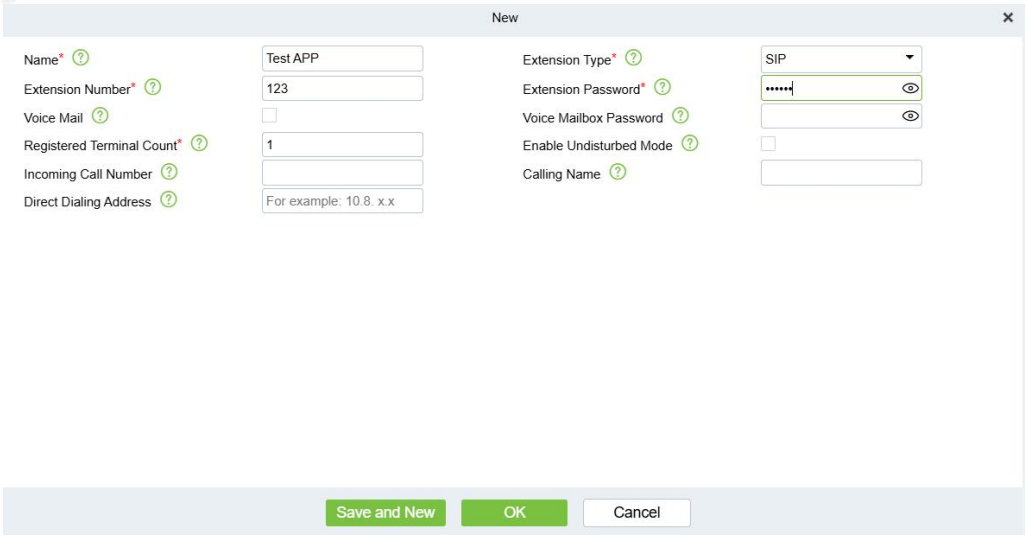


Figure 4- 35 New Extension Number

Parameter	How to set
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.

Table 4- 5 Parameter

Result Verification

After clicking "OK", the created extension number and SIP account will be automatically displayed in the list. The SIP account is hidden by default, and you can right-click on the table header and tick the option.

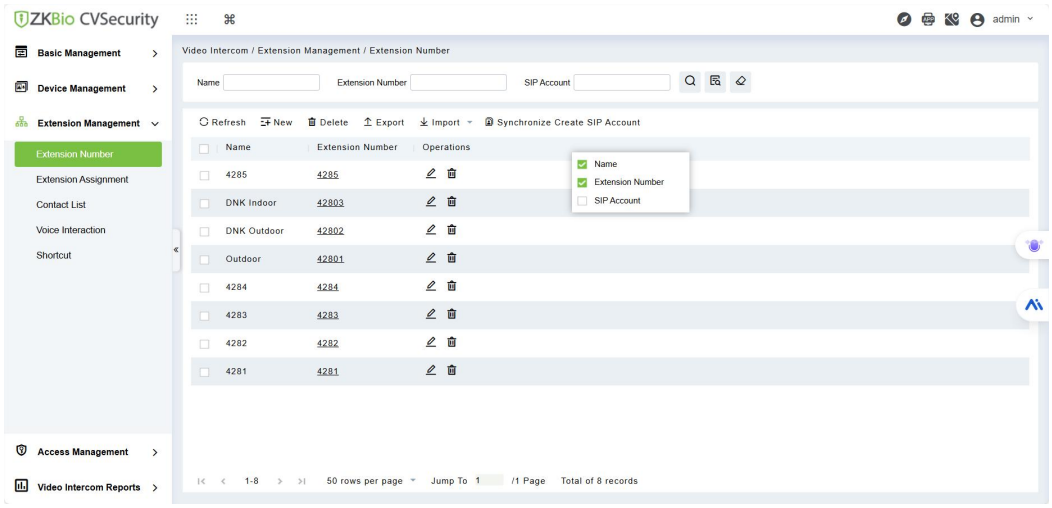


Figure 4- 36 Result Verification

4.3.1.2Delete

Select one or more extension numbers from the list, then click "**Delete**", a dialog box will appear as shown below:

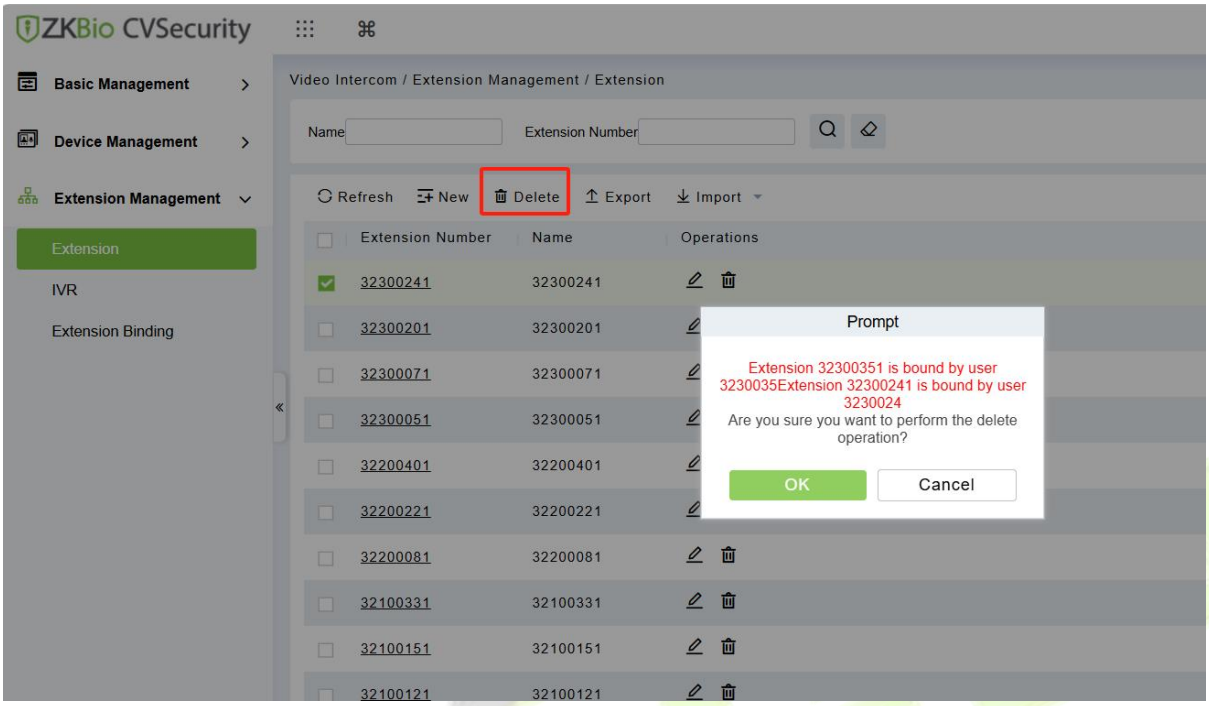


Figure 4- 37 Delete Extension Number

Clicking **OK** will result in the deletion of the selected extension number.

4.3.1.3Import

If you need to add extension numbers in bulk, you can use the Import function.

Step 1: Download the import template by clicking **Import -> import** template.

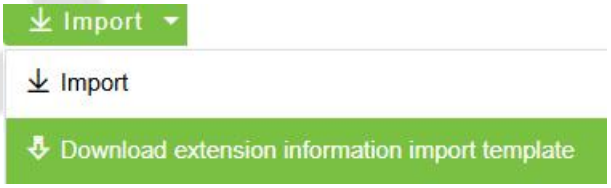


Figure 4- 38 Import Extension Number

Step 2: Fill in the information into the import template.

Extension Information Template

Extension Number	Name	Direct Dial Address	Calling Number	Calling Name
400	Popy Xiao			Popy Xiao
401	Lambert Chen			Lambert Chen
402	Leo Hou			Leo Hou
403	sfsfd			sfsfd
404	fsfds			fsfds
405	fsfsf			fsfsf
406	fsfsf			fsfsf
407	fsfsf			fsfsf
408	fsfsdfd			fsfsdfd
409	fssdfds			fssdfds
410	fsfsdfd3w			fsfsdfd3w
411	fsfsw			fsfsw
412	fsfsf1			fsfsf1
413	afsfdsf			afsfdsf
414	wdsfsfs			wdsfsfs

Figure 4- 39 Import Extension Number

Step 3: Click on **Import -> Import,** then click Browse to select the import template, and click OK to start the bulk import process.

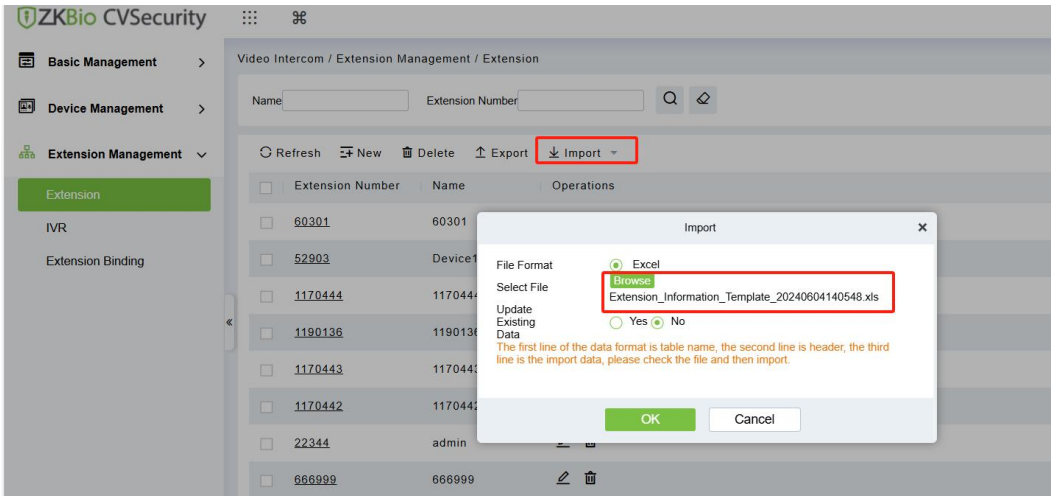


Figure 4- 40 Import Extension Number

Once the progress reaches 100%, you will be prompted with the results of the import, as shown in the figure below.

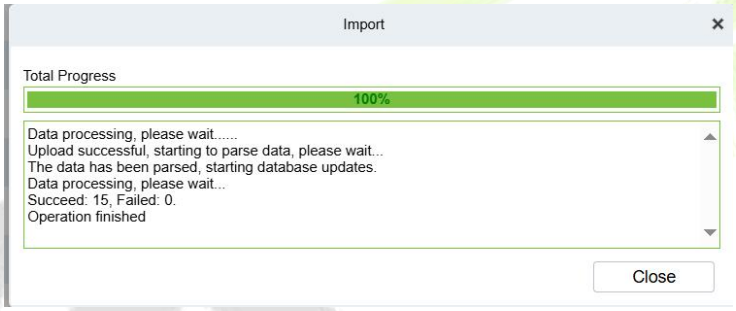


Figure 4- 41 Progress

4.3.1.4Export

Export the relevant information of the extension numbers.

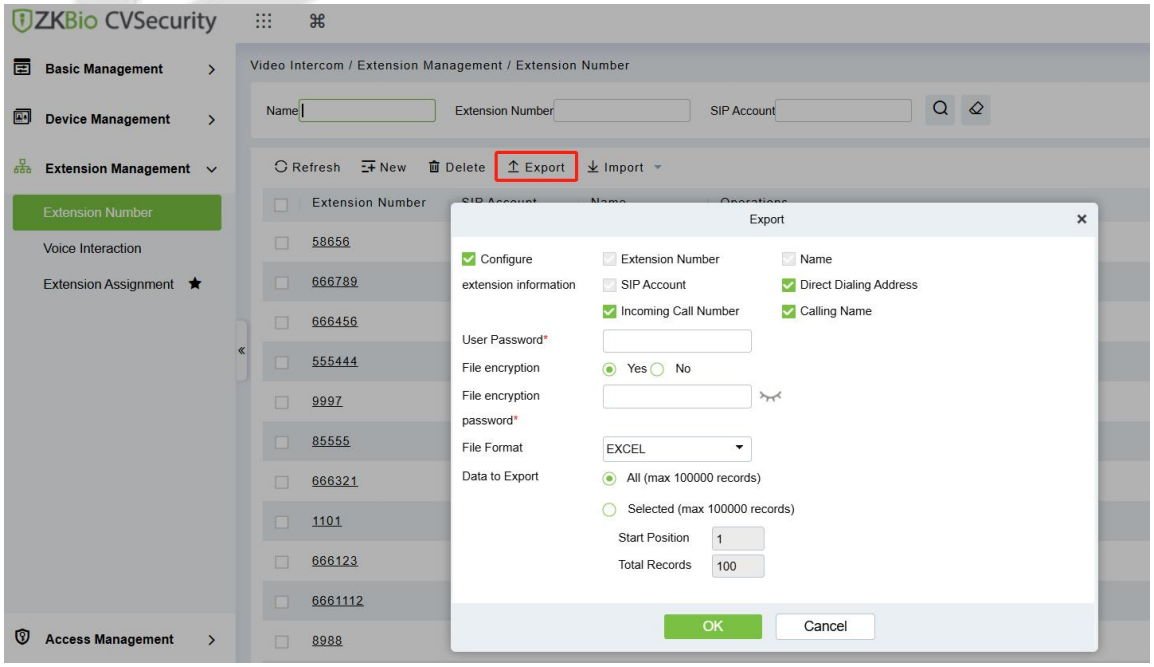


Figure 4- 42 Export Extension Number

4.3.2Extension Assignment

This feature is designed to assign extension numbers to devices, personnel, and system users that have been added to ZKBio CVSecurity.

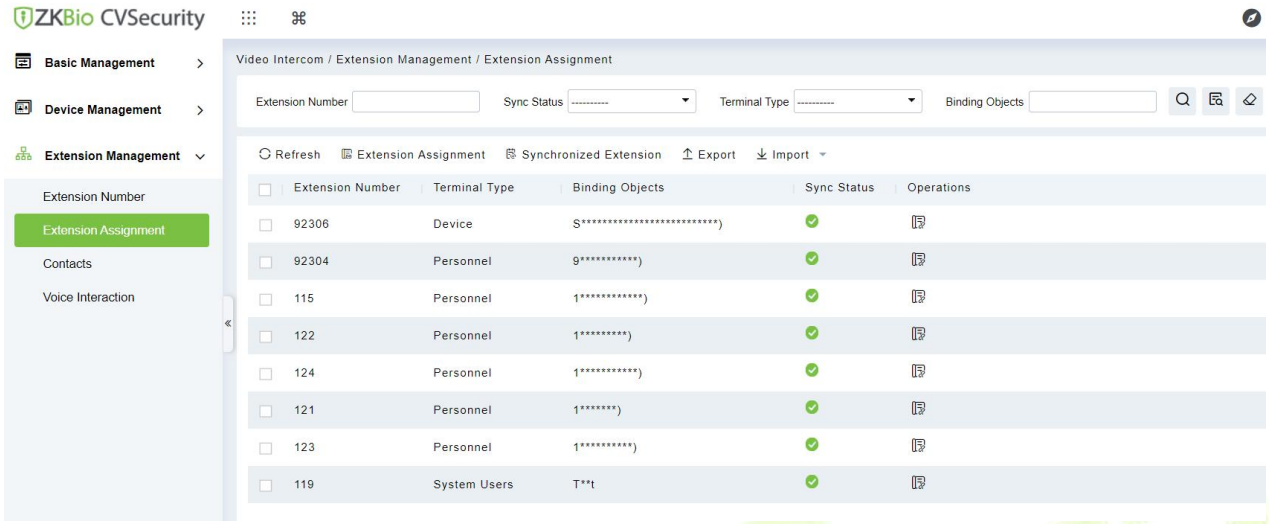


Figure 4- 43 Extension Assignment

4.3.2.1Extension Number Assignment

4.3.2.1.1 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.You can refer to the hardware suggestion list for the required firmware versions.

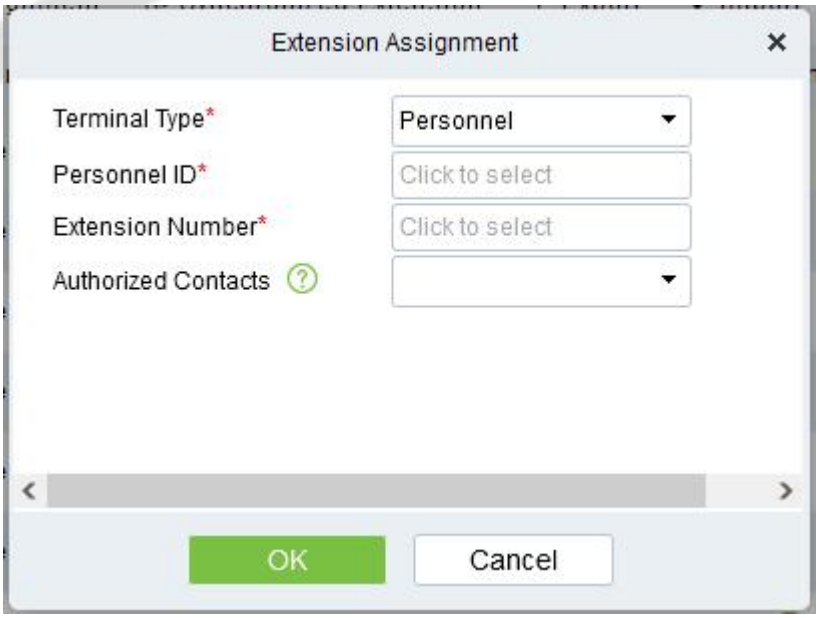


Figure 4- 44 Device

Result Verification

In the device's visual intercom interface, under **"Account,"** you can see that the SIP server and account information have been automatically written in, as shown in the figure below.

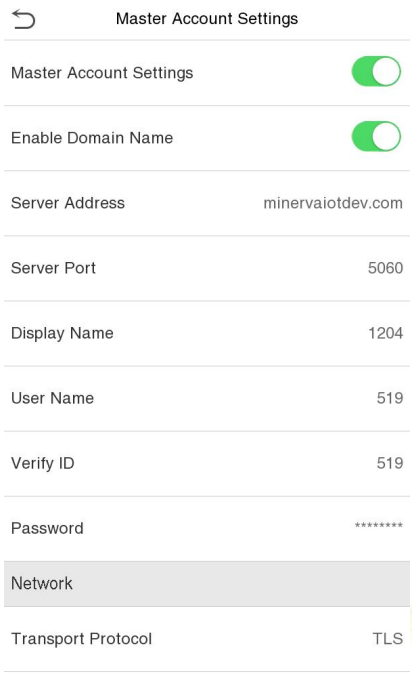


Figure 4- 45 Device Account

4.3.2.1.2 Assigning Accounts to Personnel (App)

Terminal Type: Select "Personnel" as the Binding Type;

Personnel ID: Choose 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.

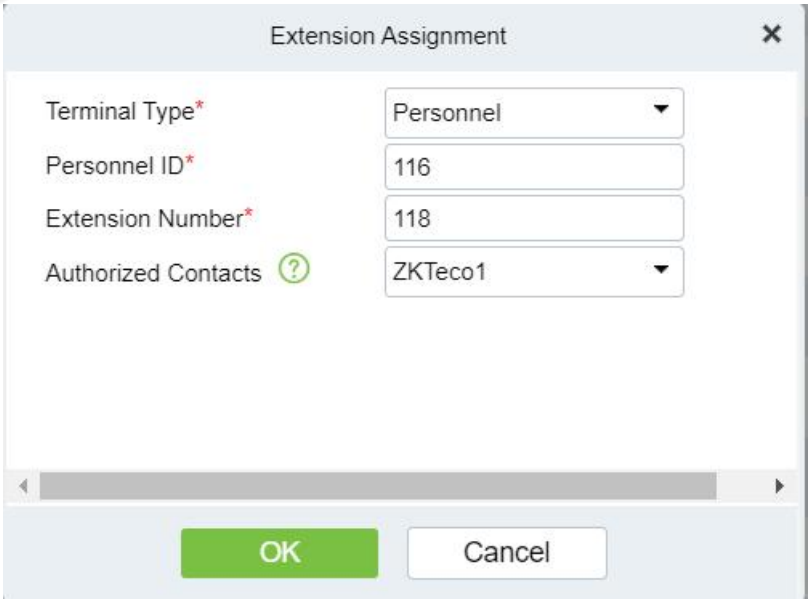


Figure 4- 46 Personnel

If the personnel has already enabled APP Login, then after logging in to the APP, they can directly use the APP for visual intercom communication.

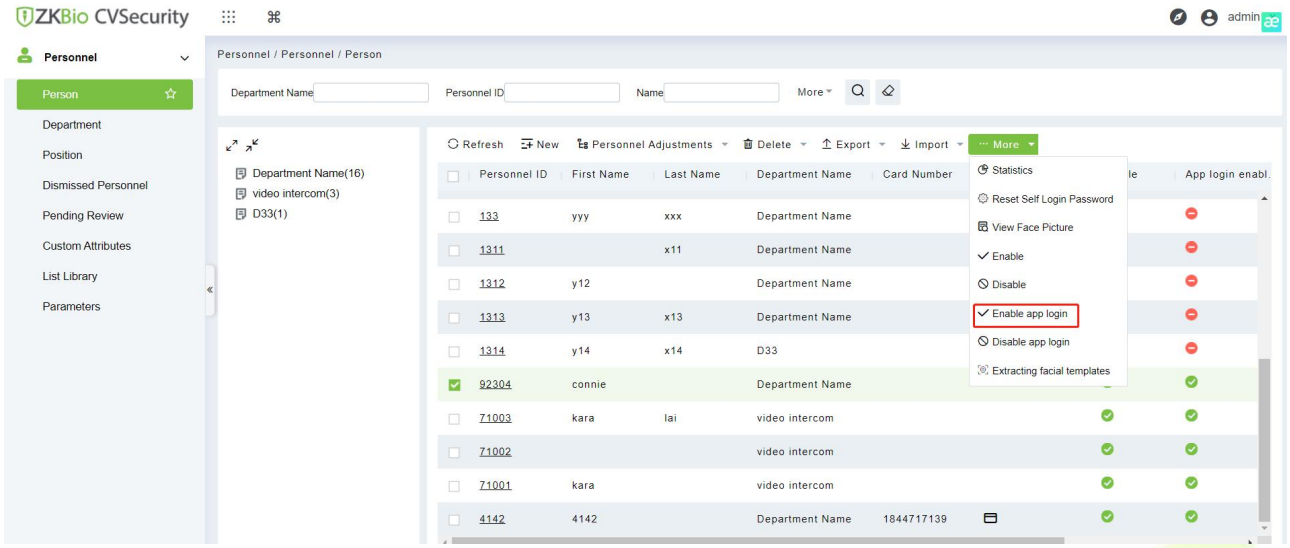


Figure 4- 47 Enabled APP Login

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 has not been assigned an extension number, entering the application will prompt "You have not been assigned an extension number, please contact the administrator."

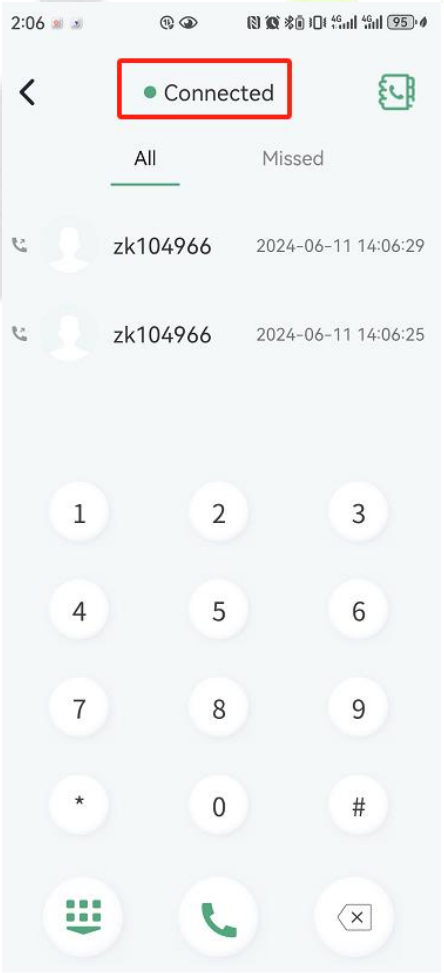


Figure 4- 48

4.3.2.1.3 Assigning Accounts to System User (App)

Terminal Type: Select "System User";

User Name: 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.

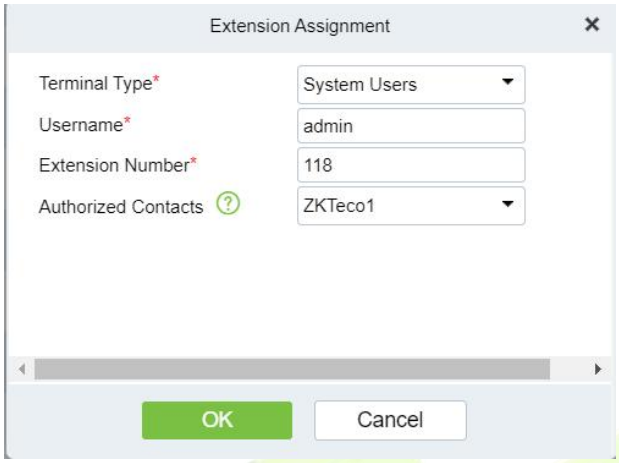


Figure 4- 49

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."

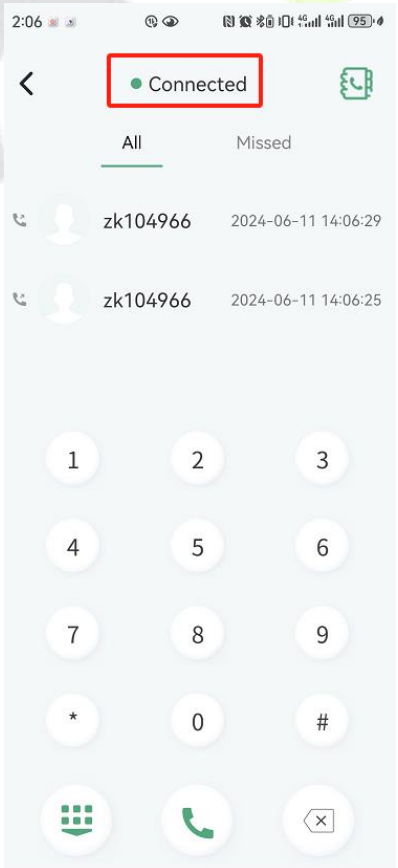


Figure 4- 50

4.3.2.2Synchronized 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 APP. If the synchronization is interrupted or not successful, you can also click on "Synchronize Extension" to resynchronize.

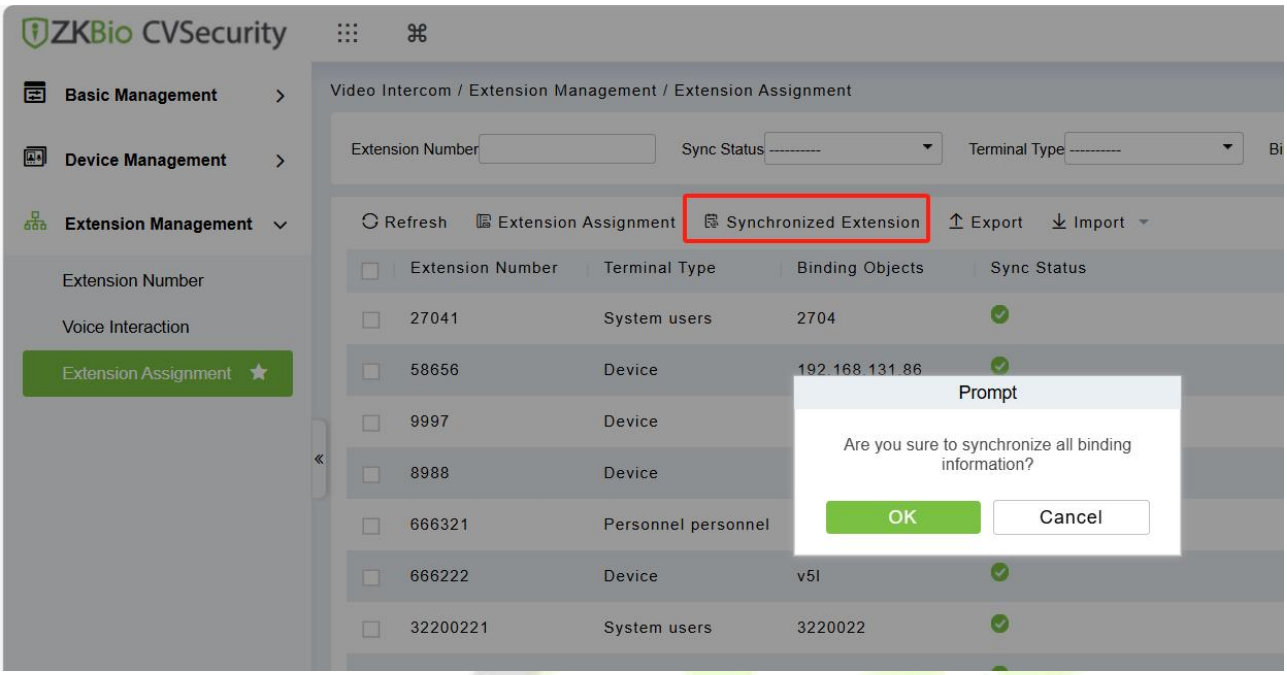


Figure 4- 51 Synchronize Extension

4.3.2.3Import

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 and enter the details.

Extension binding information template

Extension Number	Terminal Type	Binding Objects
101	Personnel	101
102	Personnel	102
103	Personnel	103
104	System User	Test
105	Device	105

Figure 4- 52

Step 2: Download the import template by clicking **Import -> import** template.

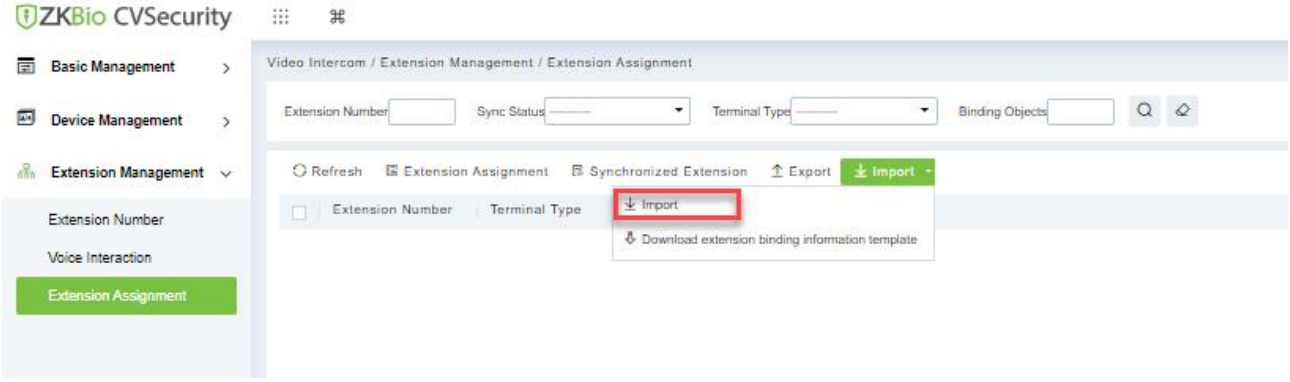


Figure 4- 53

Step 3: Click on **Import -> Import,** then click Browse to select the import template, and click **OK** to start the bulk import process.

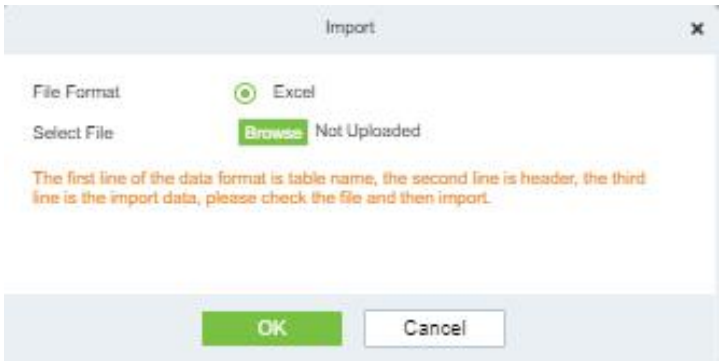


Figure 4- 54

4.3.2.4Export

Export the relevant information of the extension assignment.

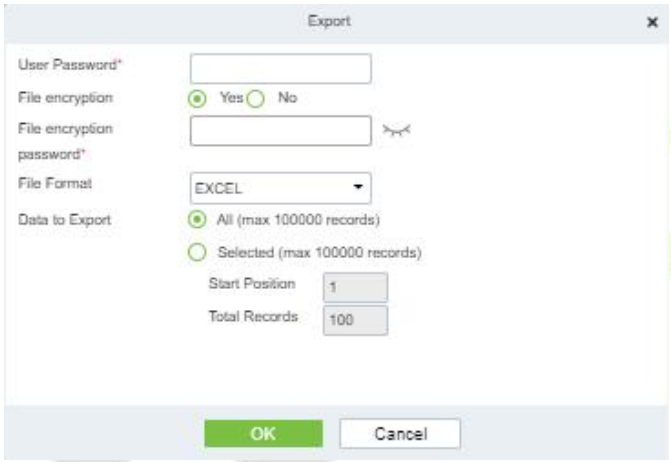


Figure 4- 55

4.3.2.5Unbinding Extension

Click  button,This will unbind the extension number from its current association.

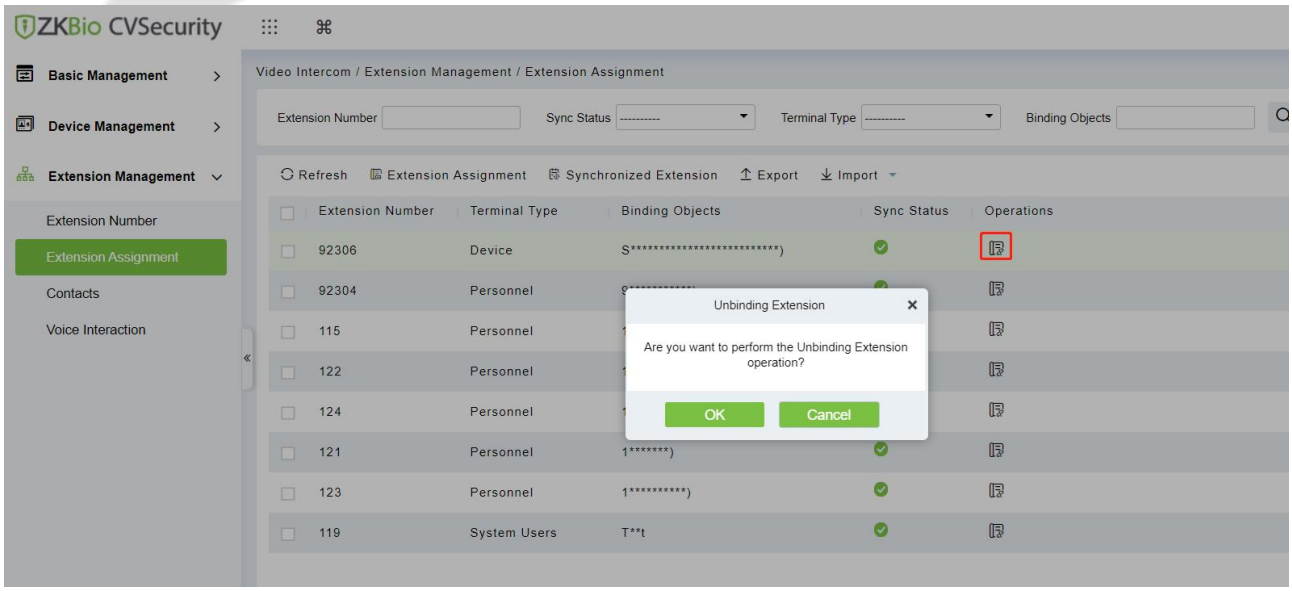


Figure 4- 56

4.3.3Contact List

User can create a contact list and assign it to devices or the app.

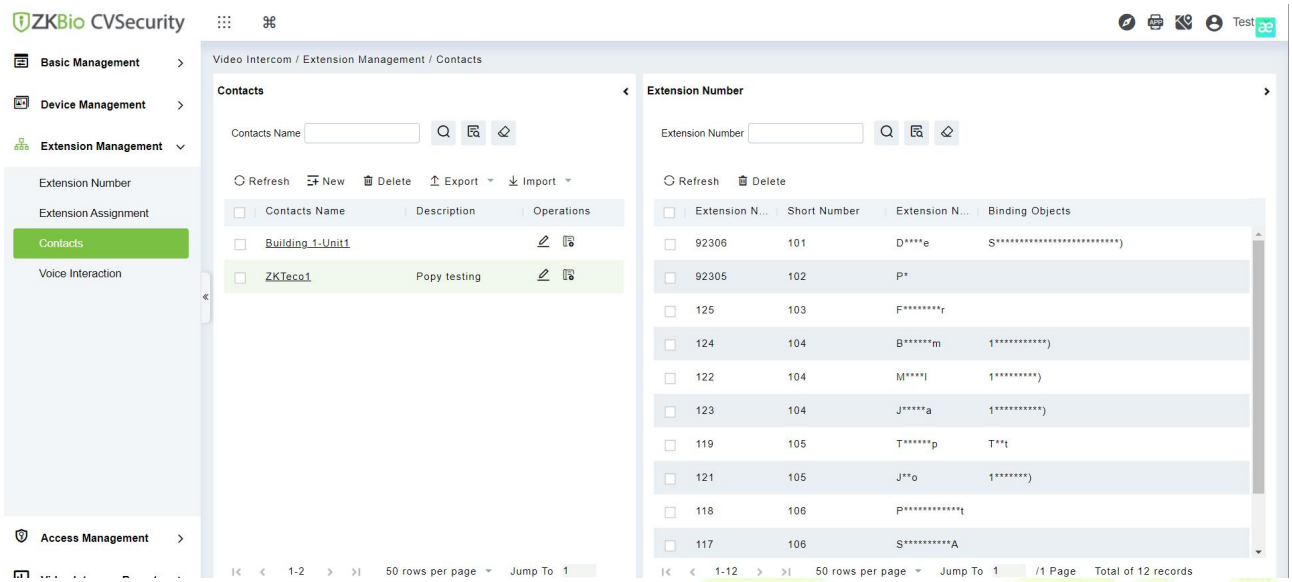


Figure 4- 57

4.3.3.1New

Click the **New** to create a new contact list.

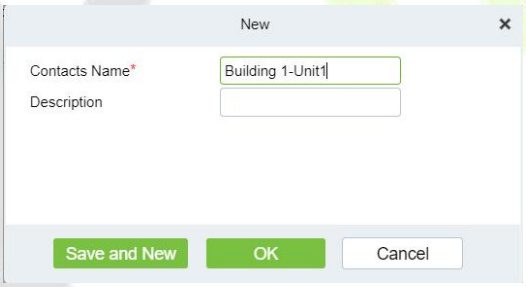


Figure 4- 58

4.3.3.2Add Extension

Click on the icon to add an extension number to the contact list, as shown in the image below:

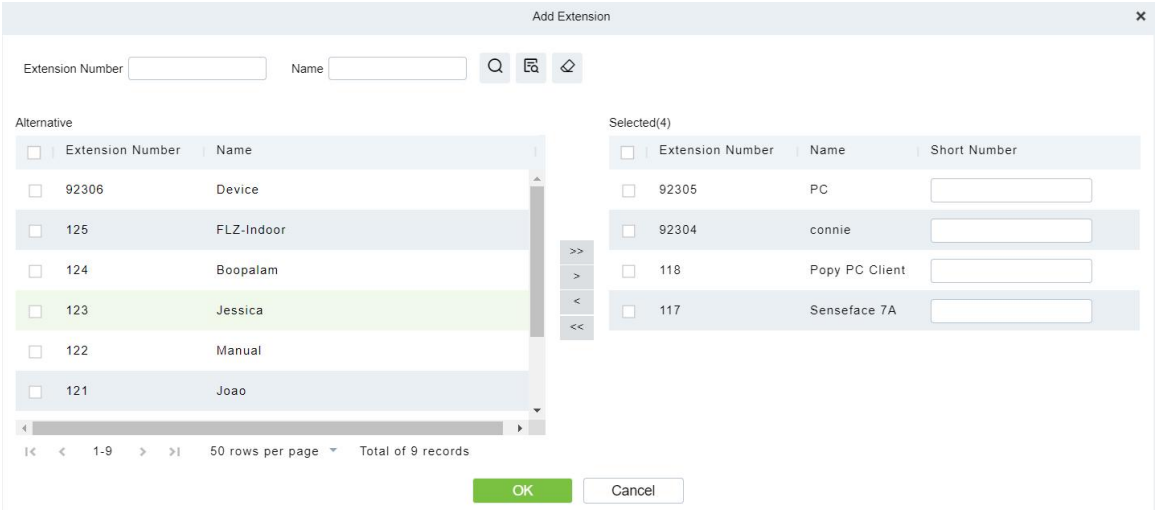


Figure 4- 59

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 CVSecurity 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.

4.3.3.3Delete

Click **Delete** to remove the contact list.

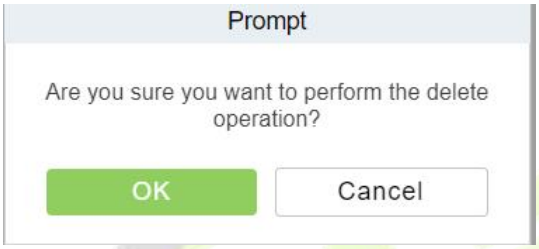


Figure 4- 60

4.3.3.4Export

Click **Export** to export the contact list.

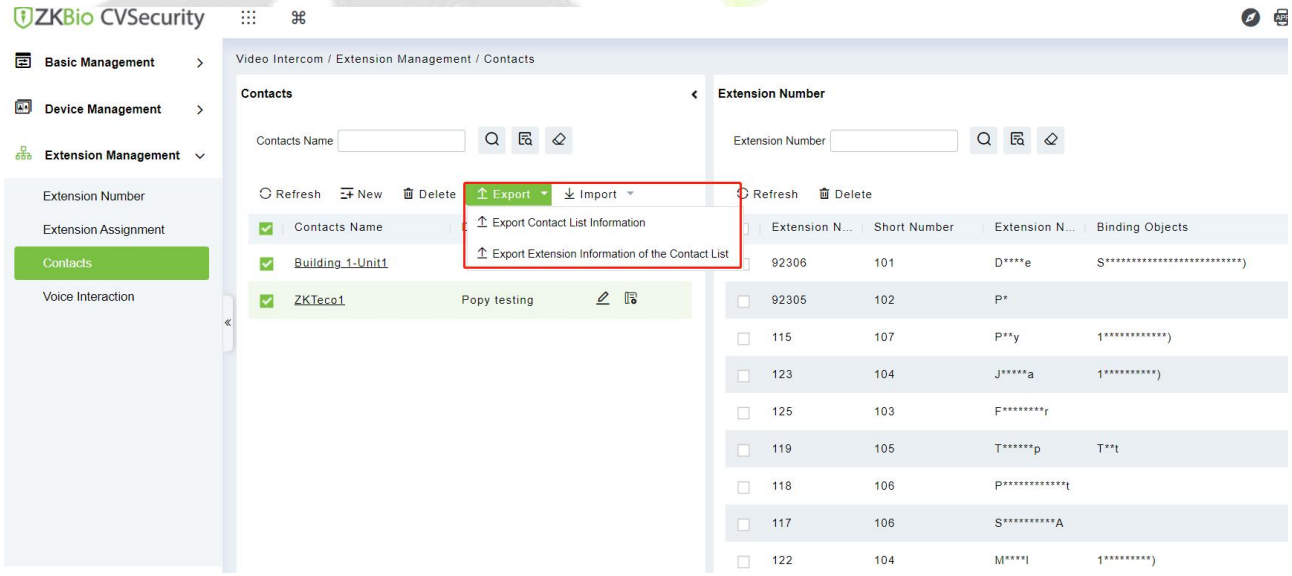


Figure 4- 61

● Export Contact List Information

Contacts	
Contacts Name	Description
Building 1-Unit1	
ZKTeco1	Popy testing

Figure 4- 62

● 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)

Figure 4- 63

4.3.3.5Import

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.

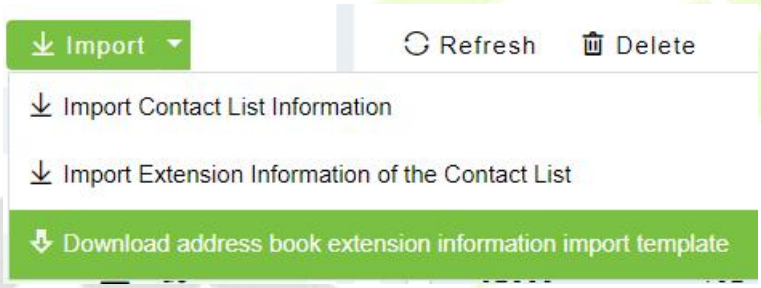


Figure 4- 64

4.3.4Voice 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 CVSecurity 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.)

4.3.4.1New

Click on **Video Intercom -> Extension Management ->Voice Interaction page**, and click on New to display the window as shown in the figure below.

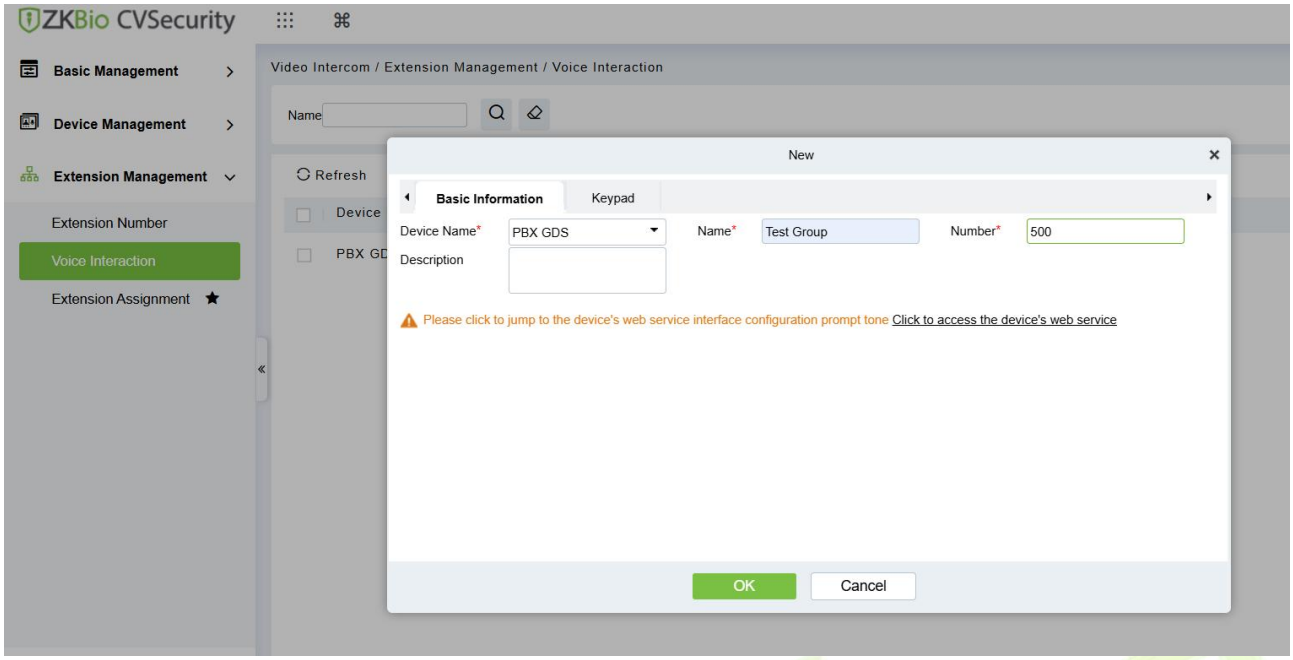


Figure 4- 65 Voice Interaction

● Basic Information

The PBX Server's IVR feature basic information configuration, with field explanations as follows:

Parameter	How to set
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

Table 4- 6 Parameter

● Keypad

Configure the purpose and actions intended to be achieved by the IVR.

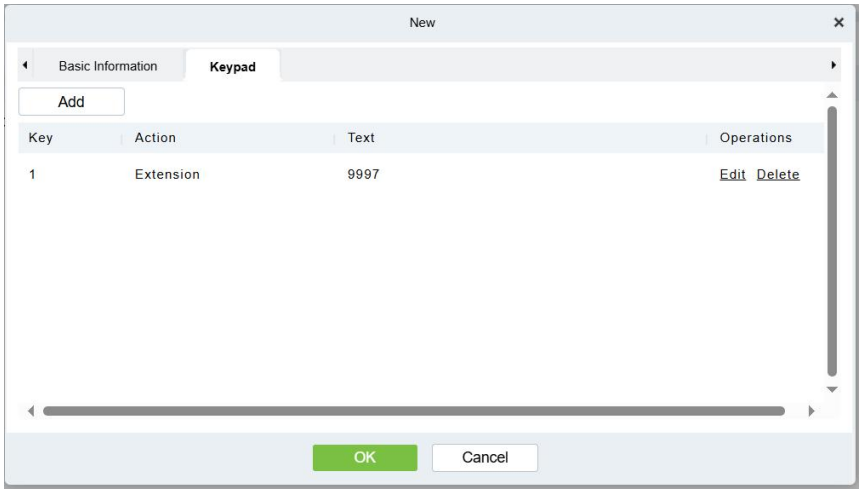


Figure 4- 66 Keypad

Click "**Add**" to begin the configuration.

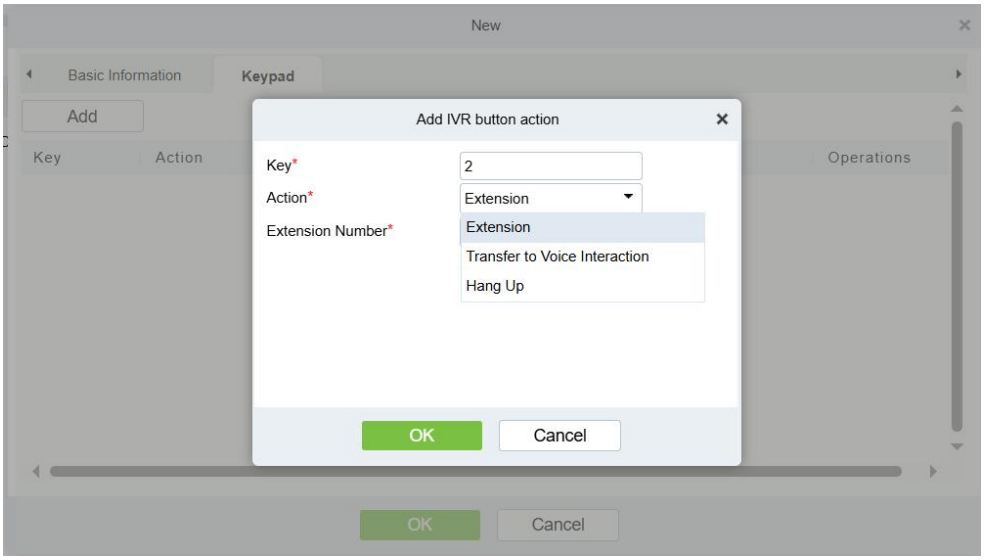


Figure 4- 67

Parameter	How to set
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.

Table 4- 7 Parameter

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:

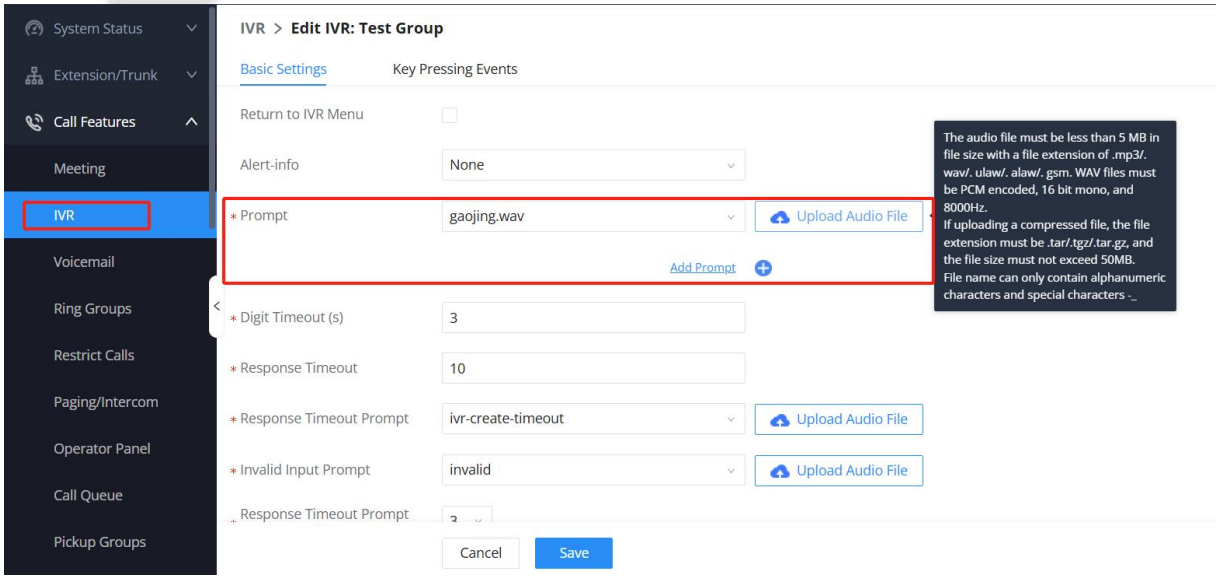


Figure 4- 68 IVR

1. Access Control Linkage

Go to **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.

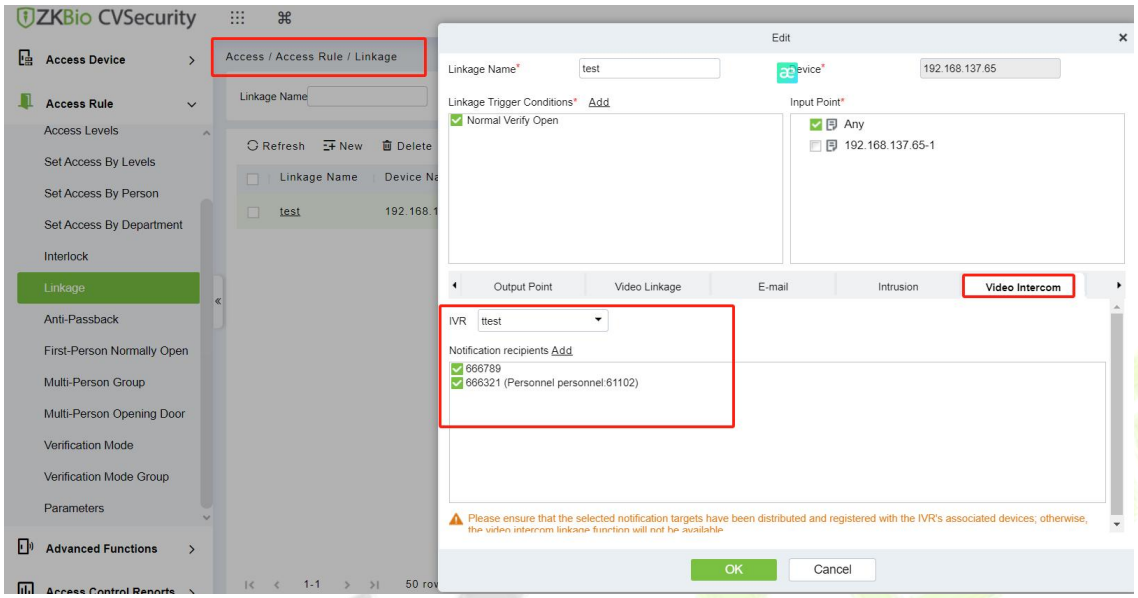


Figure 4- 69 Access Control Linkage

4.3.4.2Obtain IVR

Go to Video Intercom -> Extension Management ->Voice Interaction page, and click on Open IVR the window as shown in the figure below:

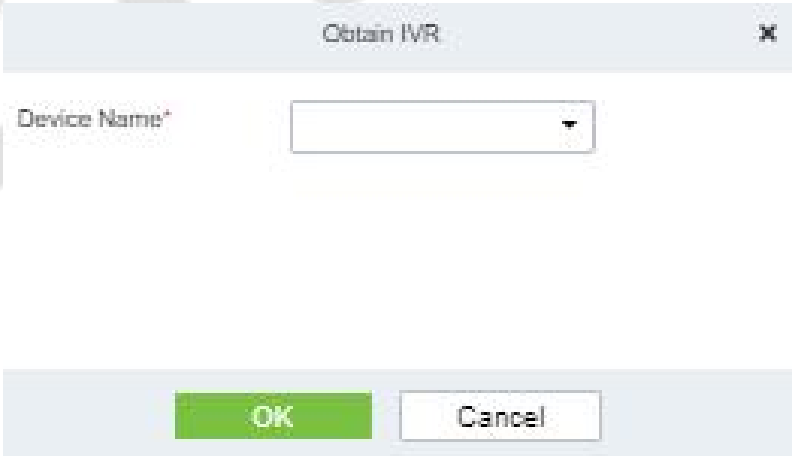


Figure 4- 70 Obtain IVR

Parameter	How to set
Device Name	Enter the name of the device.

Table 4- 8 Parameter

4.4 Access Management

This menu is solely used for configuring and synchronizing access permissions for personnel entering and exiting for **DNK** device types.

4.4.1 Access Control Group

Access control group define groups and categories of video intercom to facilitate subsequent permission assignment operations.

Setting operations include creating access level groups and adding doors to access level groups.

4.4.1.1 Add Group

This section describes how to create Step for Access Control groups in the module of Video Intercom.

● Operation Step:

Step 1: In the Video Intercom module, choose "**Access Management > Access Control Group**".

Step 2: Click **New** in the left column, 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 figure below.

Figure 4- 71 Adding Access Control Groups

Parameter	How to set
Level name	Customize the name of the access control groups.
Description	Add description as needed.

Table 4- 9 Description of Access Control Right Groups

Step 4: Click **OK** to finish configuring the access control right group.

4.4.1.2 Add Device

● Operation Step:

Step 1: In 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 figure below.

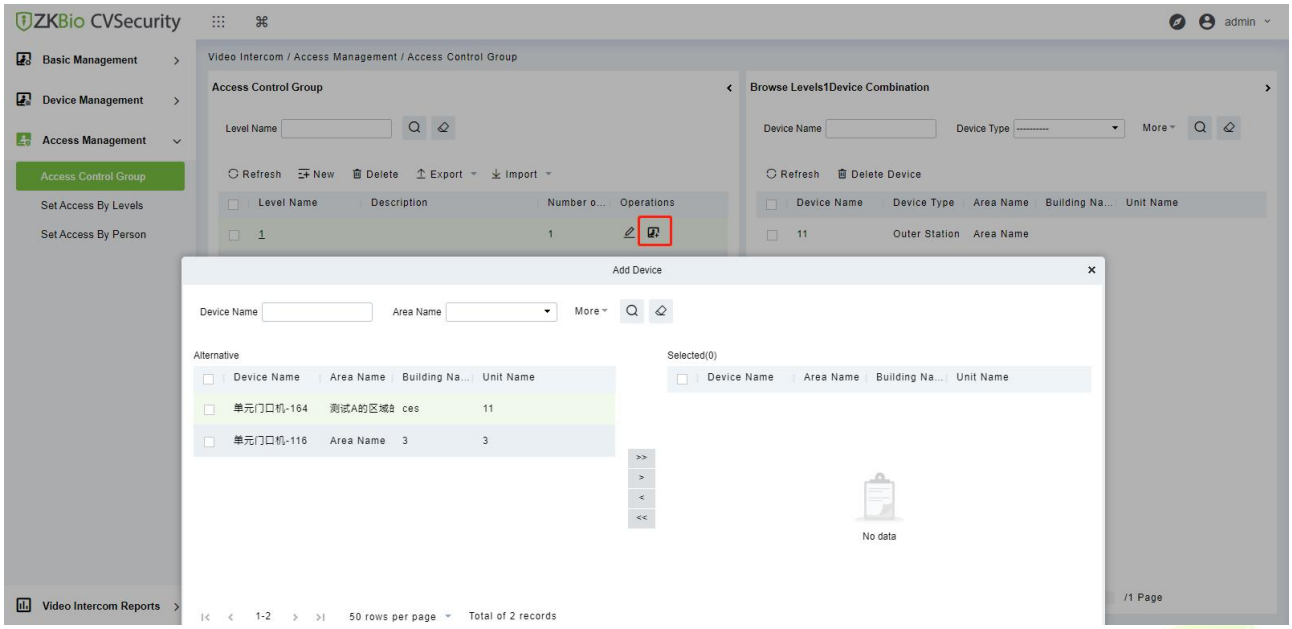


Figure 4- 72 Adding Access Control Groups Add Devices

Step 3: Click **OK** to finish configuring the device for the video intercom right group.

Parameter	How to set
Device Name	Enter the name of the device.
Area Name	Enter the name of the Area.

Table 4- 10 Parameter

4.4.1.3Delete Devices

Select delete device, click **Delete**, and click **OK** to delete device.

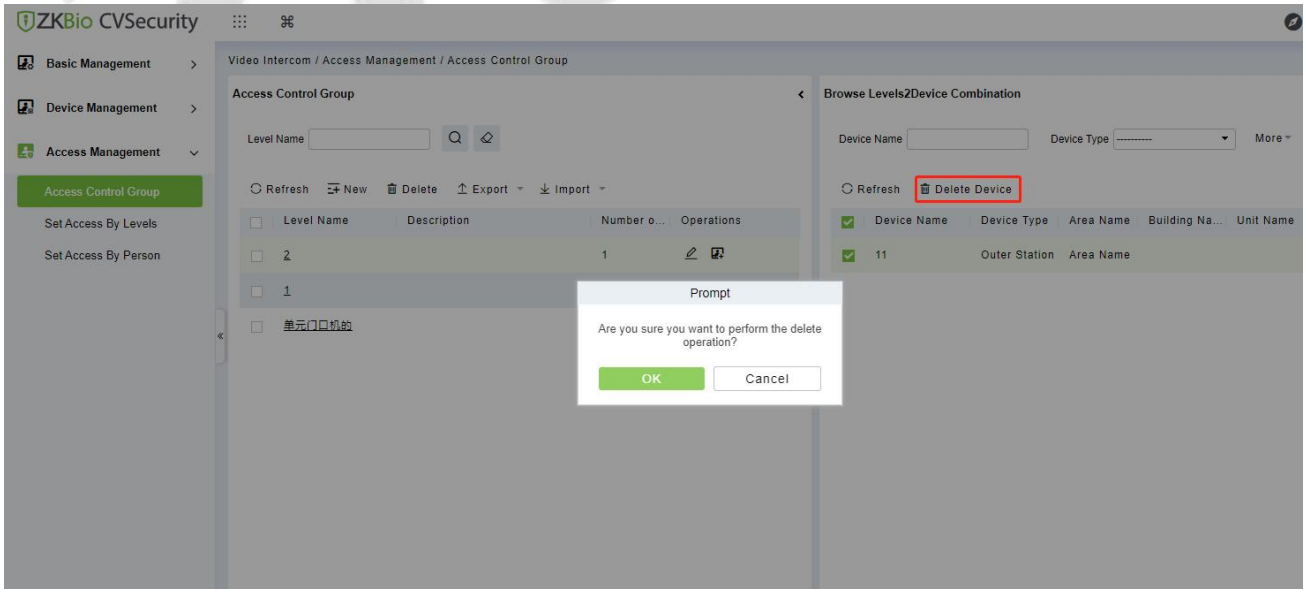


Figure 4- 73 Delete Device

4.4.1.4Export / Import

Export the permission group information of 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**.

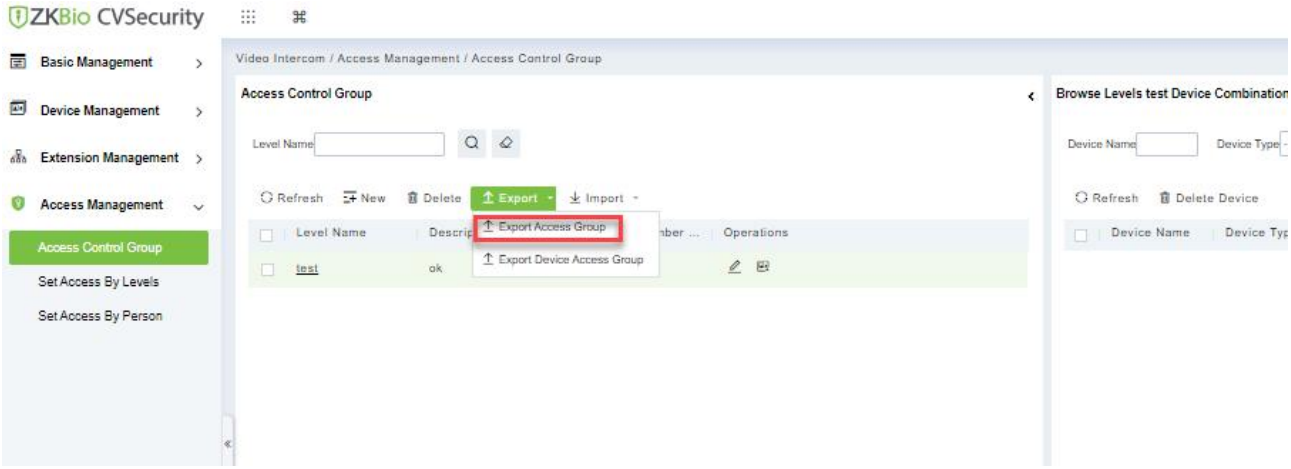


Figure 4- 74 Export Access Group 1

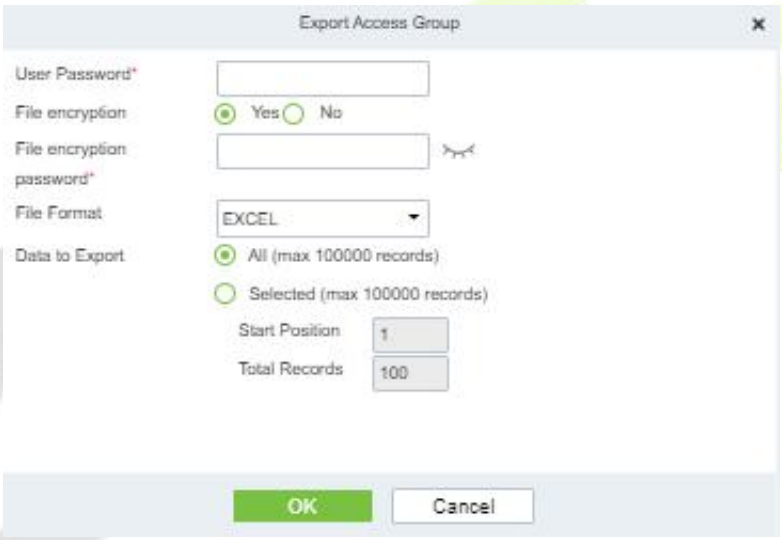


Figure 4- 75 Export the Access Group Template 2

Export the device Access groupof Access Control Template:

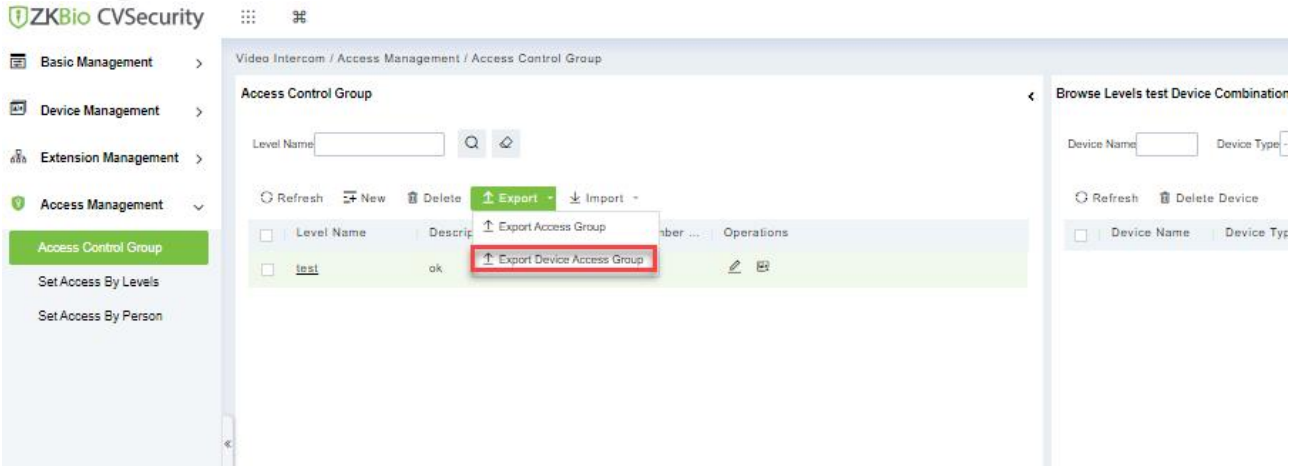


Figure 4- 76 Export the device access group Template 1

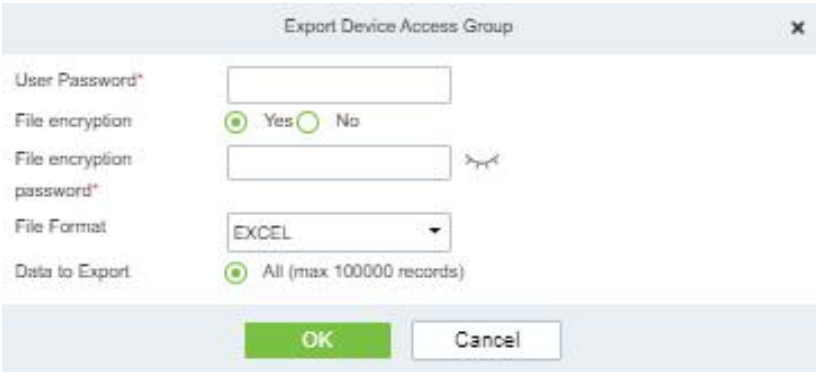


Figure 4- 77 Export the device access groupTemplate2

4.4.2Set Access By Levels

This section describes Operation Step that set access by levels in the module of video intercom in ZKBio CVSecurity.

4.4.2.1Add Personnel

●Operation Step:

Step 1: In the Video Intercom module, choose "**Access Management**>**Set Access by Levels**"

Step 2: In the Operation column of the corresponding permission group, click "**Add Personnel**". The Add

Personnel page is displayed. Select personnel as required.

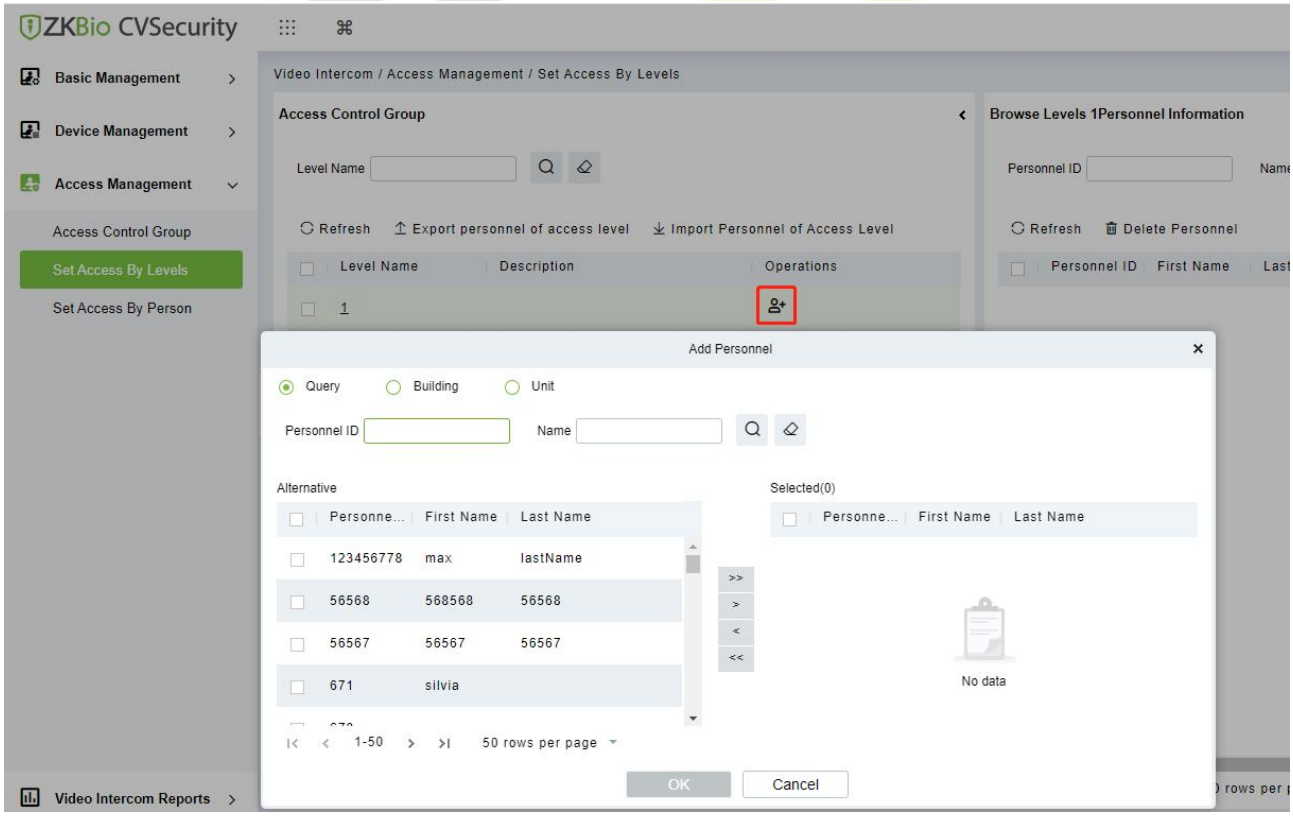


Figure 4- 78 The Interface of Add Personnel When Set Access by Level

Step 3: Click **OK** to complete the assignment of personnel add.

Parameter	How to set
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.

Table 4- 11 Parameter

4.4.2.2Export Personnel of Access Level

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**.

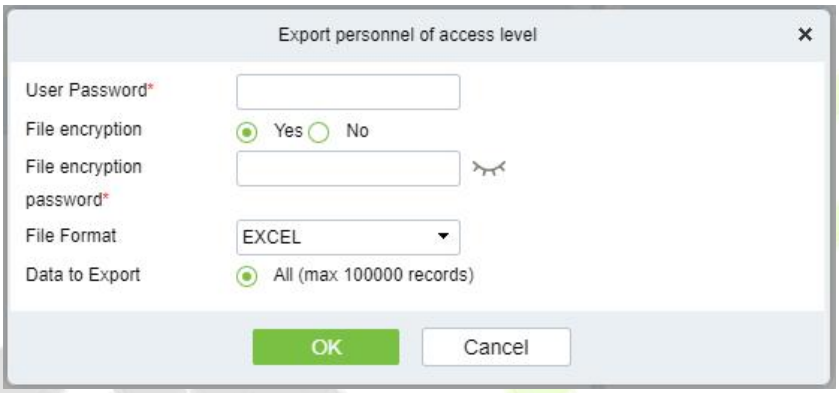


Figure 4- 79 Export the Personnel of Access Level

4.4.2.3Import Personnel of Access Level

Click **Import** and then click **Browse** to select a file from the stored location. Finally, click **OK**.

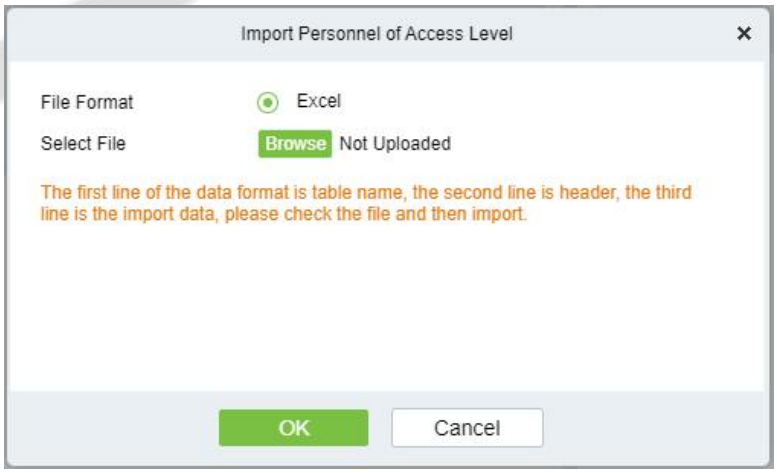


Figure 4- 80 Import the Personnel of Access Level

4.4.2.4 Delete Personnel

Select delete personnel, click **Delete**, and click **OK** to delete personnel.

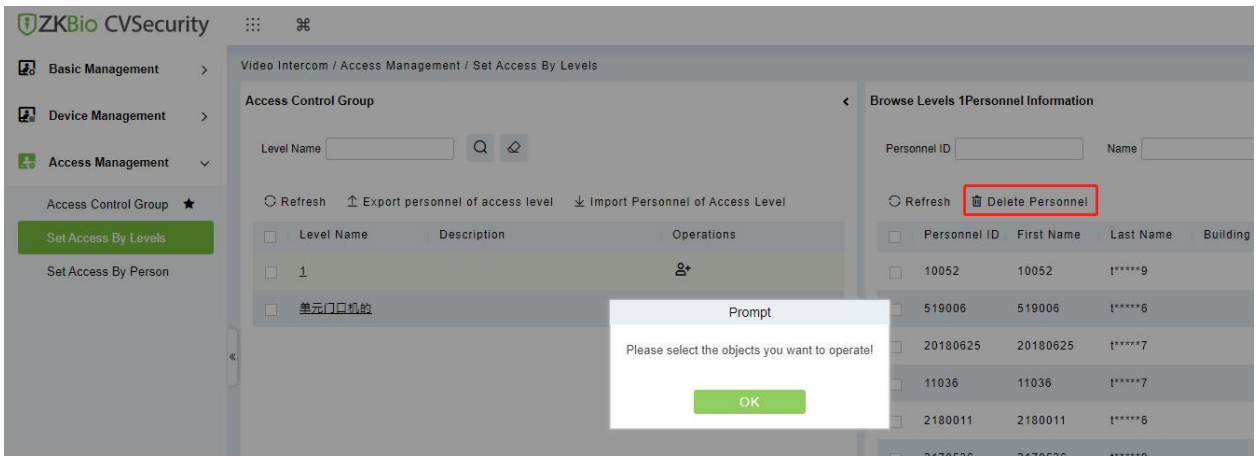


Figure 4- 81 Delete Personnel

4.4.3Set Access By Person

This section describes Operation Step that set access by person in the module of video intercom in ZKBio CVSecurity.

4.4.3.1Add Personnel

Operation Step:

Step 1: In the Video Intercom module, choose **Access Management>Set Access by Person**.

Step 2: In the Operation column of the corresponding permission group, click "**Add to Levels**". The Add level page will be displayed. Select level as required.

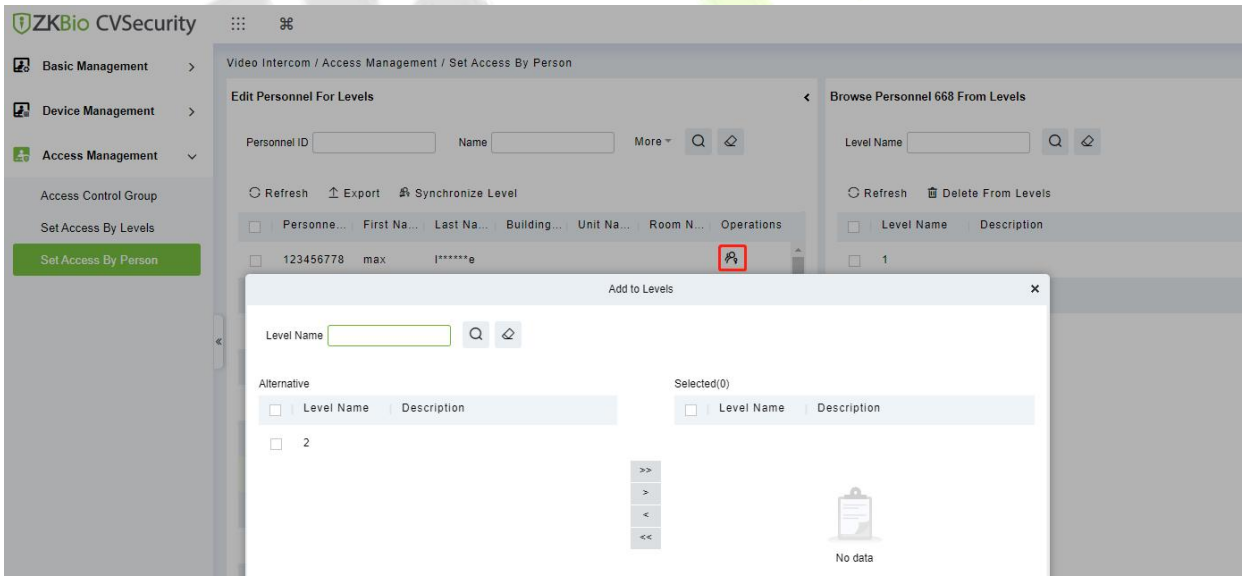


Figure 4- 82 The Interface of Add Level When Set Access by Personnel

Step 3: Click **OK** to complete the assignment of personnel add.

Parameter	How to set
Level Name	Enter the name of the level for the person.

Table 4- 12 Parameter

4.4.3.2Export

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**.

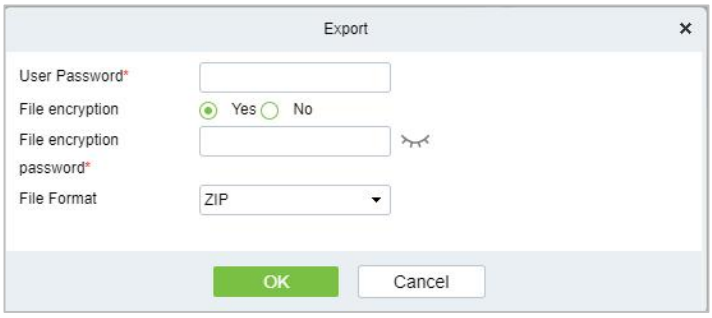


Figure 4- 83 Export the Access Level of Personnel

4.4.3.3Synchronize Access Level

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

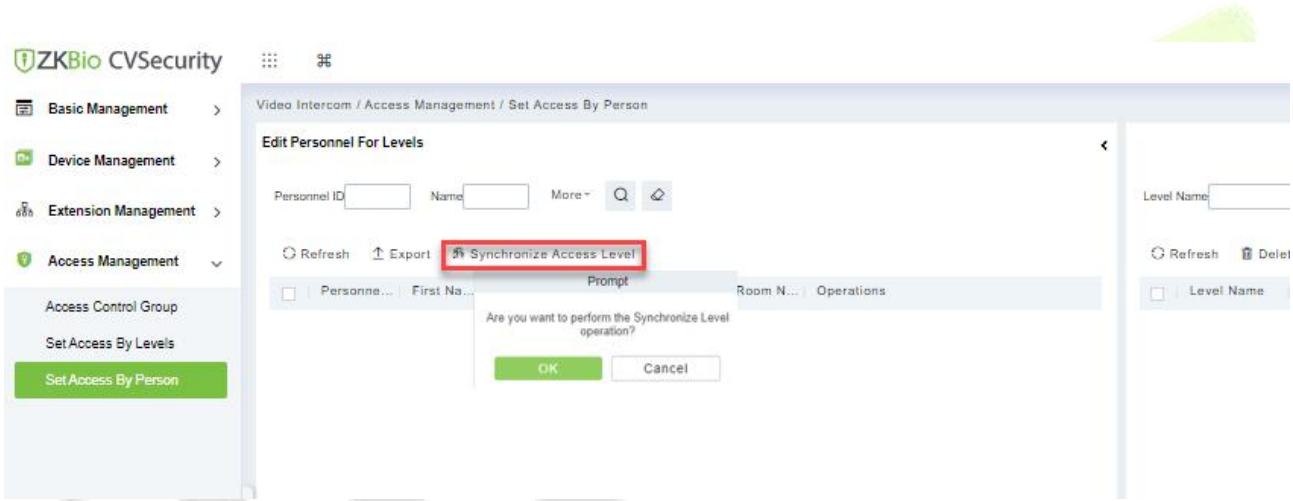


Figure 4- 84 Synchronize Access Level

4.4.3.4Delete from Levels

Select delete level, click **Delete**, and click **OK** to delete level.

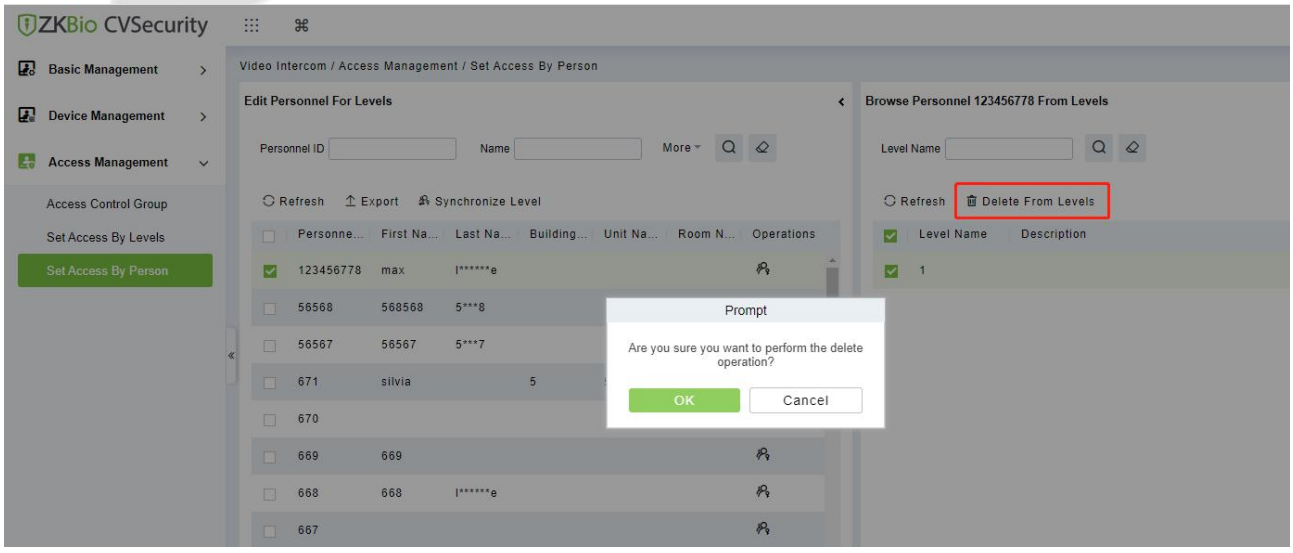


Figure 4- 85 Delete level

4.5 Video Intercom Reports

In the video intercom report, you can query all video intercom records, which includ 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 CVSecurity.

4.5.1Call Records

4.5.1.1Record Query

●Operation Step:

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.

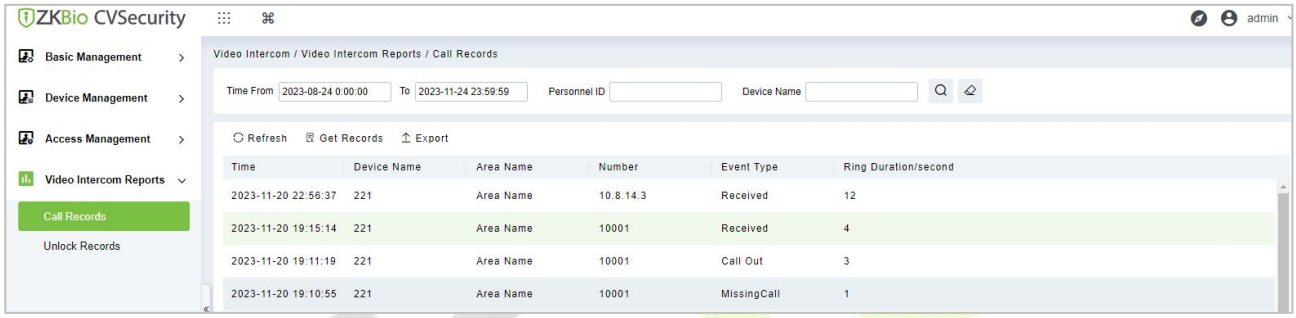


Figure 4- 86 Report Query Page

4.5.1.2Get Records

●Operation Step:

Step 1: In 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.

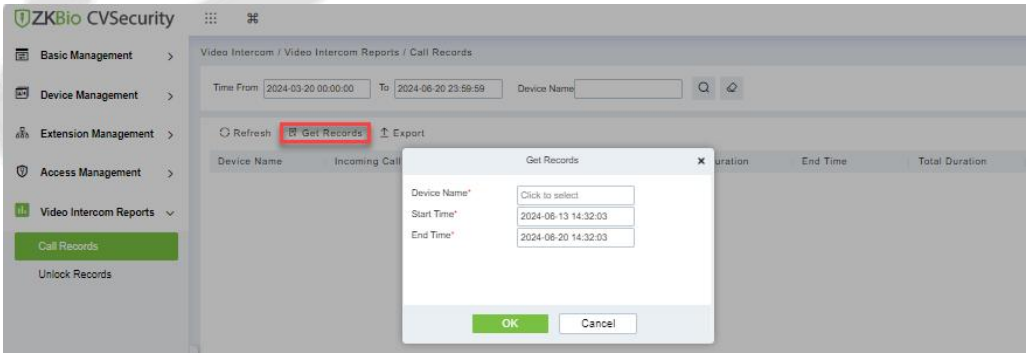


Figure 4- 87 Get Records Page 1

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.

Table 4- 13 Parameter

Step3: On the Select device interface, select the device you need, as shown in figure below.

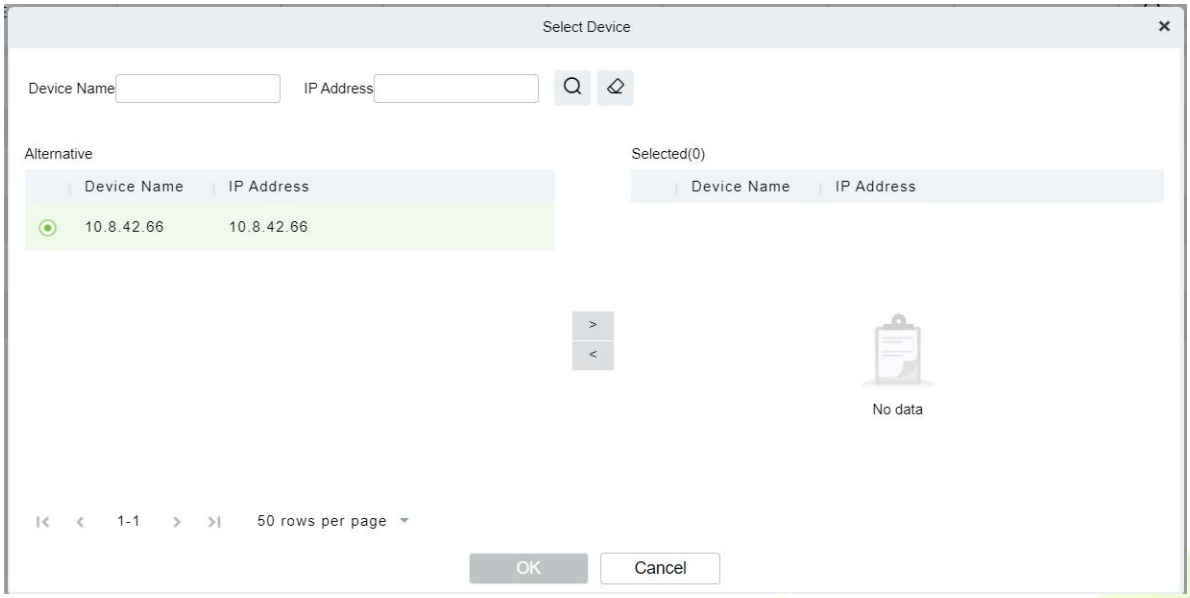


Figure 4- 88 Get Records Page 2

Step 4: Click **OK** to complete the complete acquisition of device records.

4.5.1.3Export

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**.

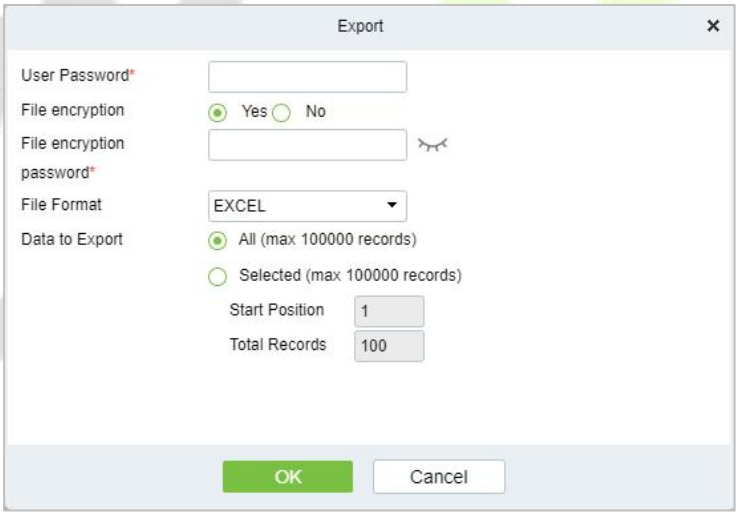


Figure 4- 89 Report Export

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

Figure 4- 90 Call Report Export

4.5.2Unlock Records

4.5.2.1Record Query

● Operation Step:

Step 1: In 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.

Figure 4- 91 Report Query Page

4.5.2.2Get Records

● Operation Step:

Step 1: In 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.

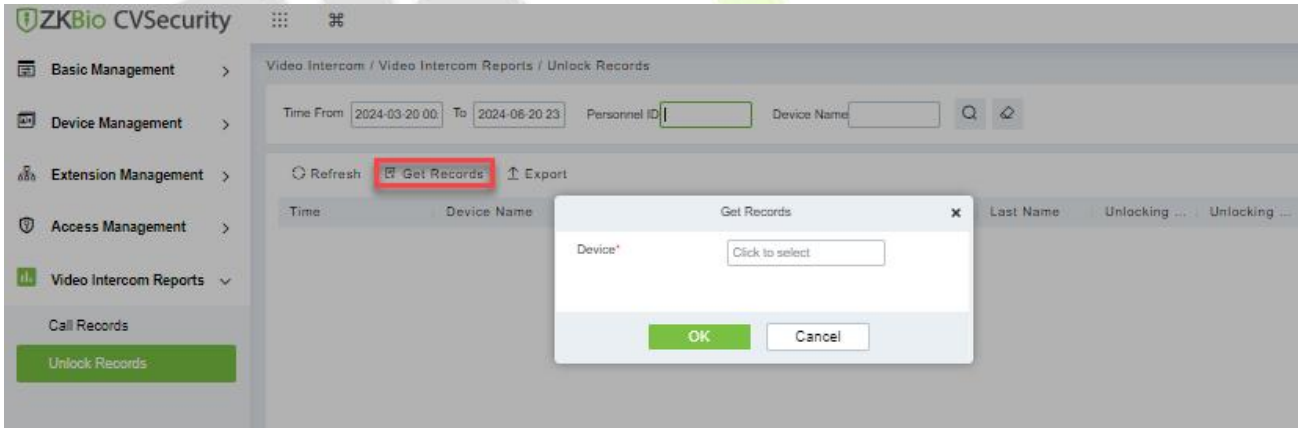


Figure 4- 92 Get Records Page 1

Parameter	Description
Device Name	Select the name of the device.

Table 4- 14 Parameter

Step 3: On the Select device interface, select the device you need, as shown in figure below.

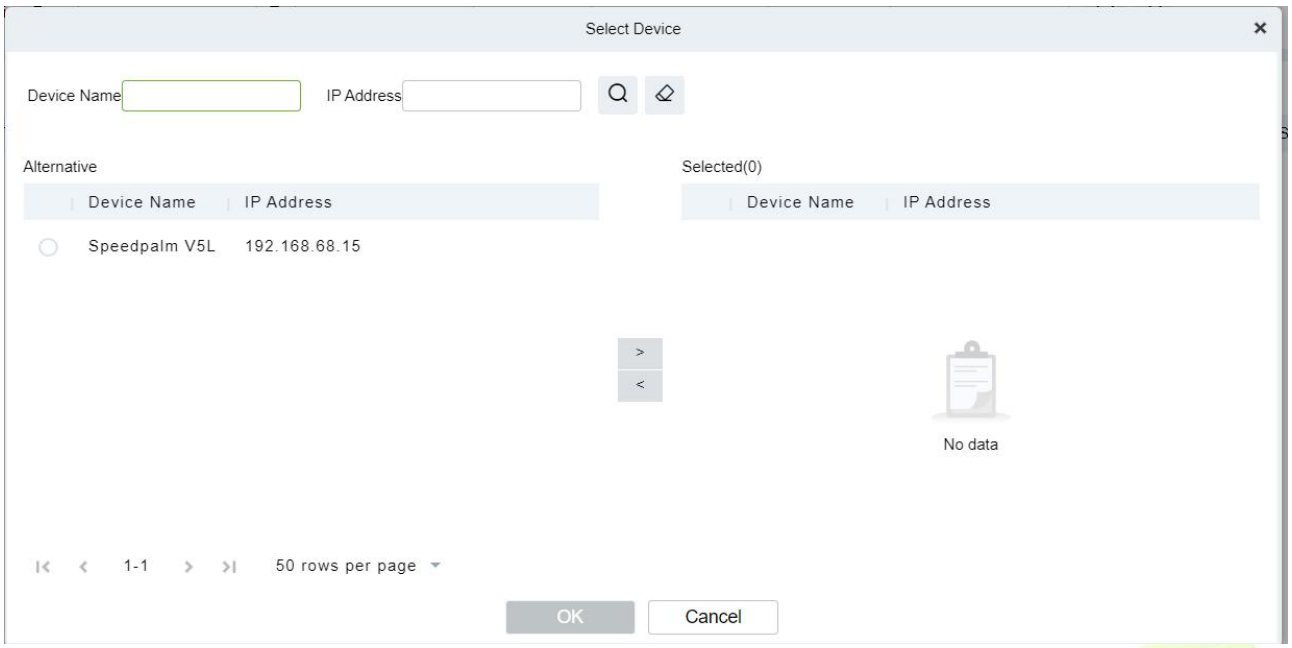


Figure 4- 93 Get Records Page 2

Step 4: Click **OK** to complete the complete acquisition of unlock records.

4.5.2.3Export

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.

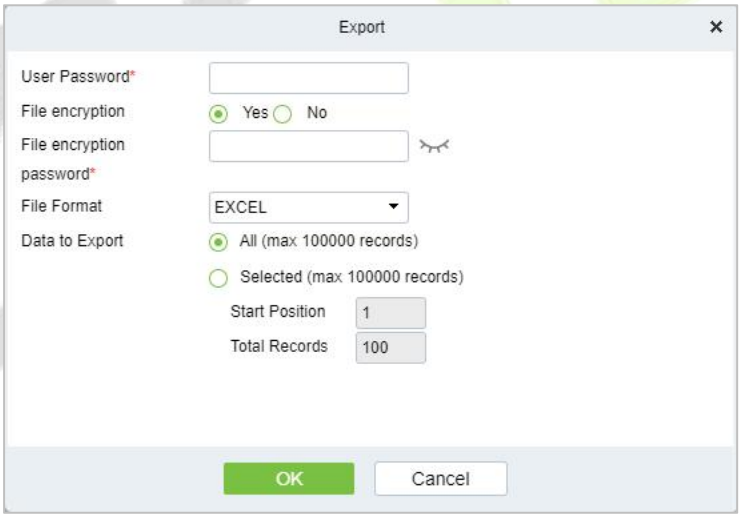


Figure 4- 94 Report Export

	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

Figure 4- 95 Unlock Report Export

5 Smart Video Surveillance

5.1 Device Management

The Smart Video Surveillance module supports controlling manufacturer brands. ZKTeco devices are supported by default and do not require license control, while other devices require corresponding licenses.

5.1.1 Device (Add Device)

● Scene Description:

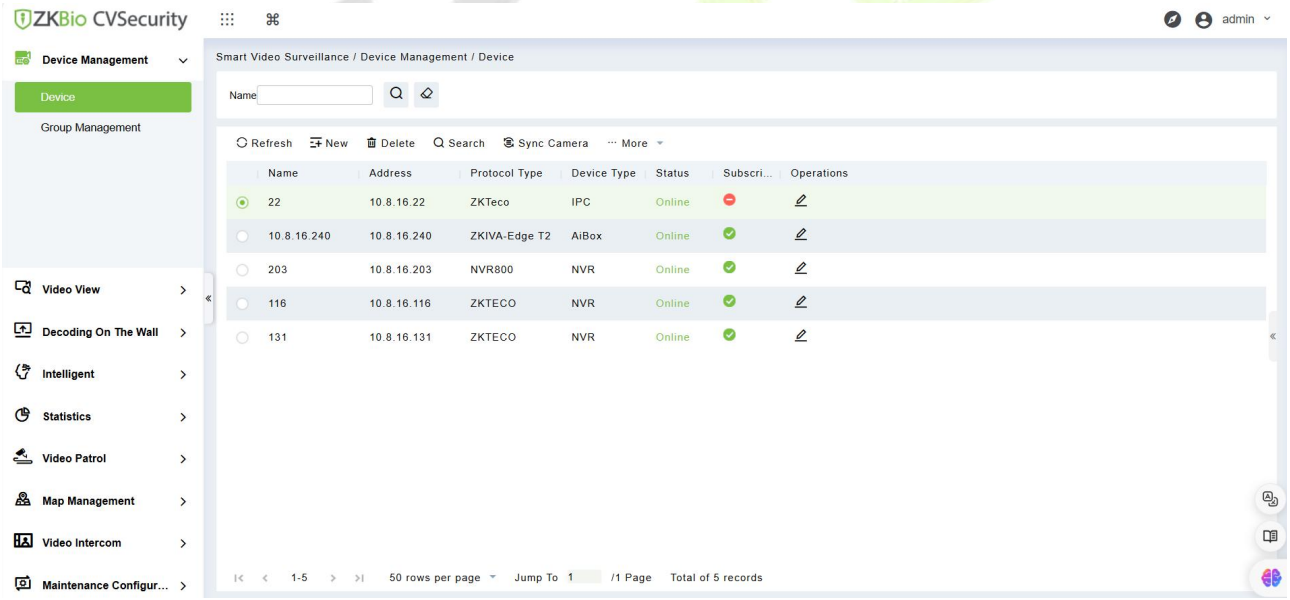
This operation is used to instruct users how to connect NVR to the platform and cameras, so that the platform can manage the connected devices uniformly, such as viewing the live and video recordings of cameras.

5.1.1.1 Manual Add NVR

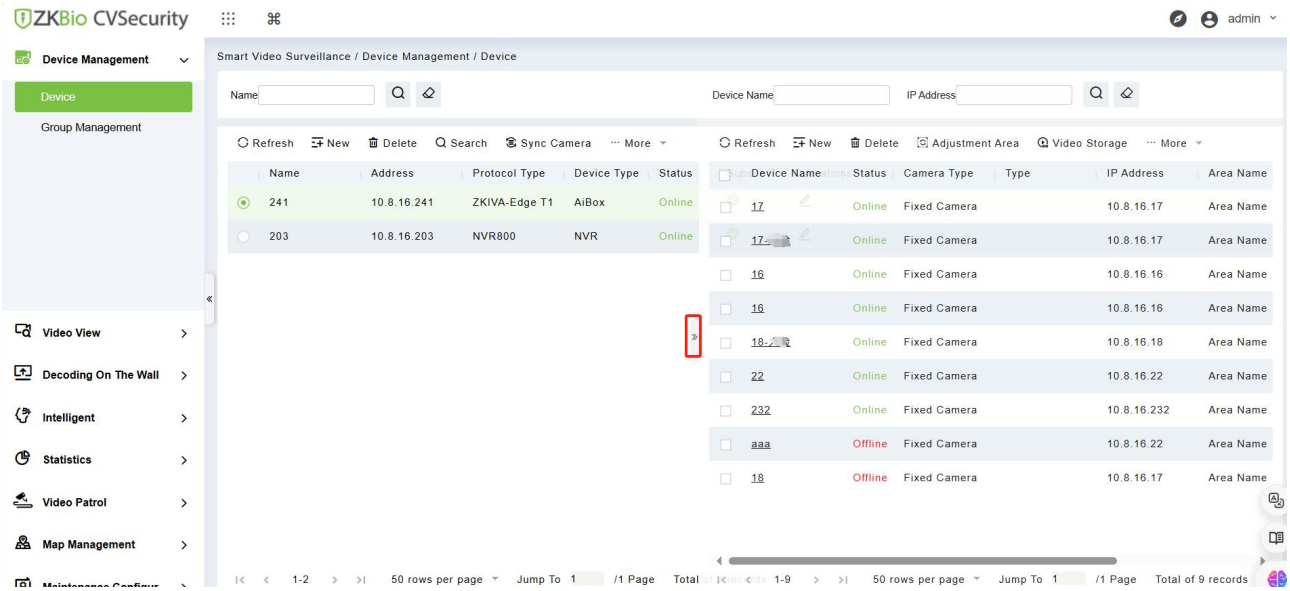
Maximum supports 1024 video channels, support 64 channels preview and 16 channels real-time playback simultaneously.

● Operating Steps:

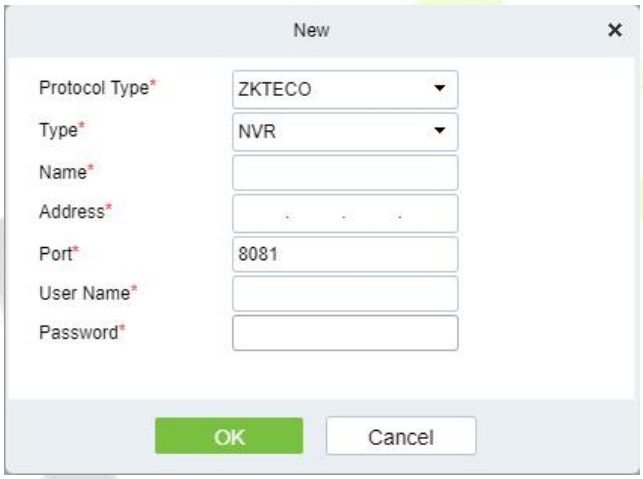
Step 1: Under the Smart Video Surveillance module, select **Device Management** > **Device**.



Note: The default page only shows the master device, if you want to see the cameras added to the master device, please click the icon « on the far right side to see them.



Step 2: Click **New** under the main device list to display the adding interface as shown in figure below, and the description of each parameter is shown in Table 4-1.



● Scene Description:

There are 8 types you can select(ZKTECO/ZKIVA-Edge T1/ZKIVA-Edge X1/NVR800/IVS1800/TD NVR3000/ONVIF/TPLink). If the purchased device is ZKNVR, select "NVR" for the type. If you want to add ZKIPC, click Type and select “IPC”.

Parameters/Buttons	Description
Type	Select the device type.
Protocol Type	Select the type of protocol.
Name	Customize the device name.
Port	Configure the device port.ZKNVR default is 8081.
Address	Configure the device address. The format is: xxx.xxx.xxx.xxx, for example: 192.168. 6.5
Username & Password	The NVR’S user name and password. Note: For ZKNVR, the default account is (admin,123456) ForIVS1800, you should to login the web page to add a new account.

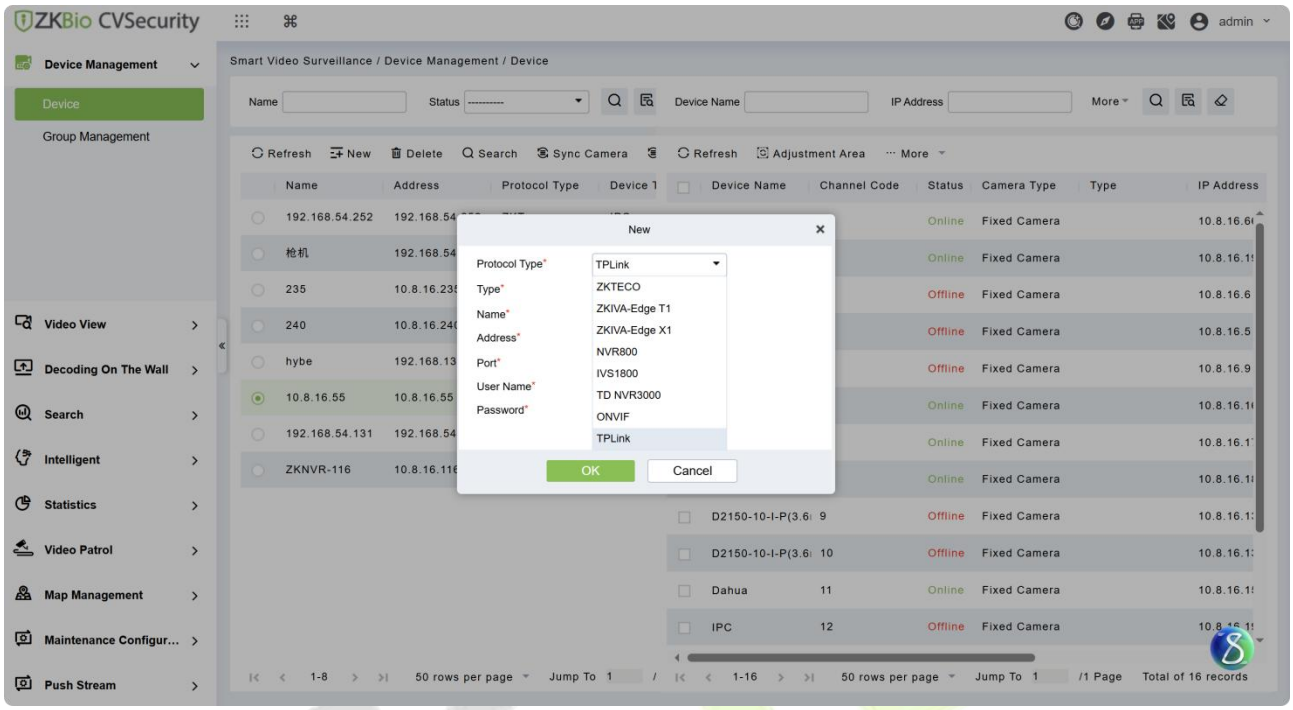
Table 5- 1 Adding Device Parameters or Function Description

Step 3: Click **OK**.

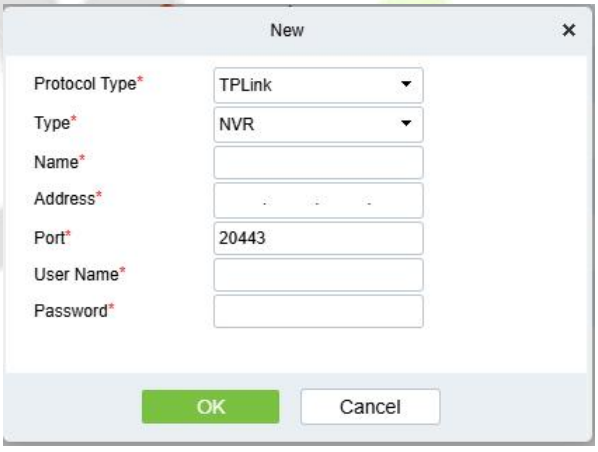
Integrated with TP-Link NVR to enable preview, playback, intelligent alert display, and alarm linkage.

- Operating Steps:

Step1: Enter Smart Video Surveillance → Device Management → Device,Click "New" under the main device list to display the adding interface as shown in figure below.



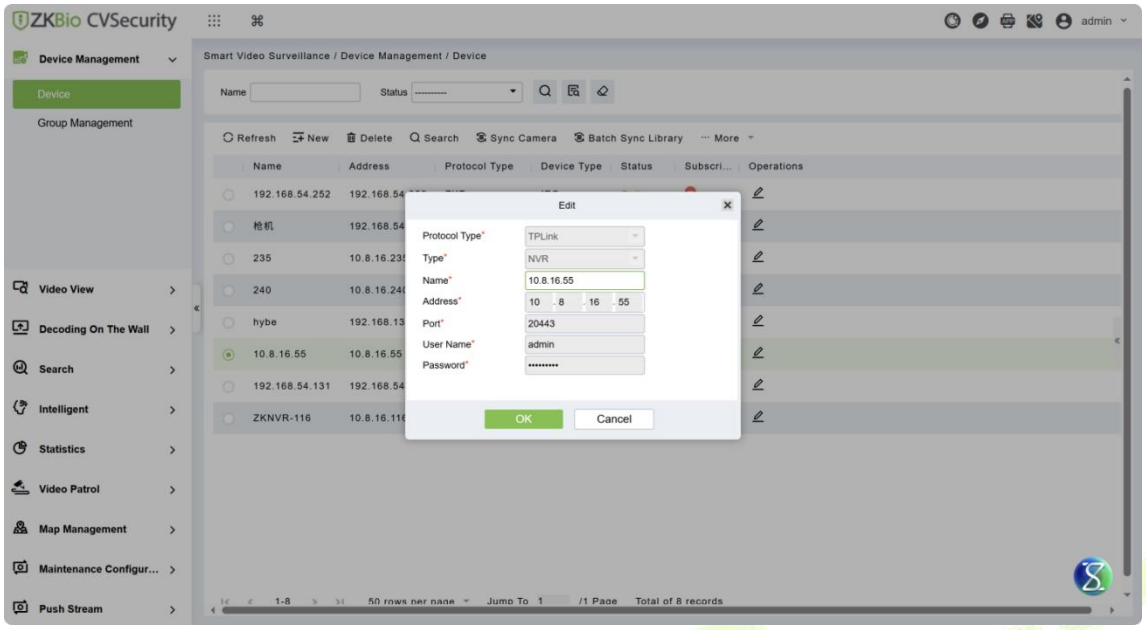
Step2: You can choose NVR devices based on the TP-Link protocol.



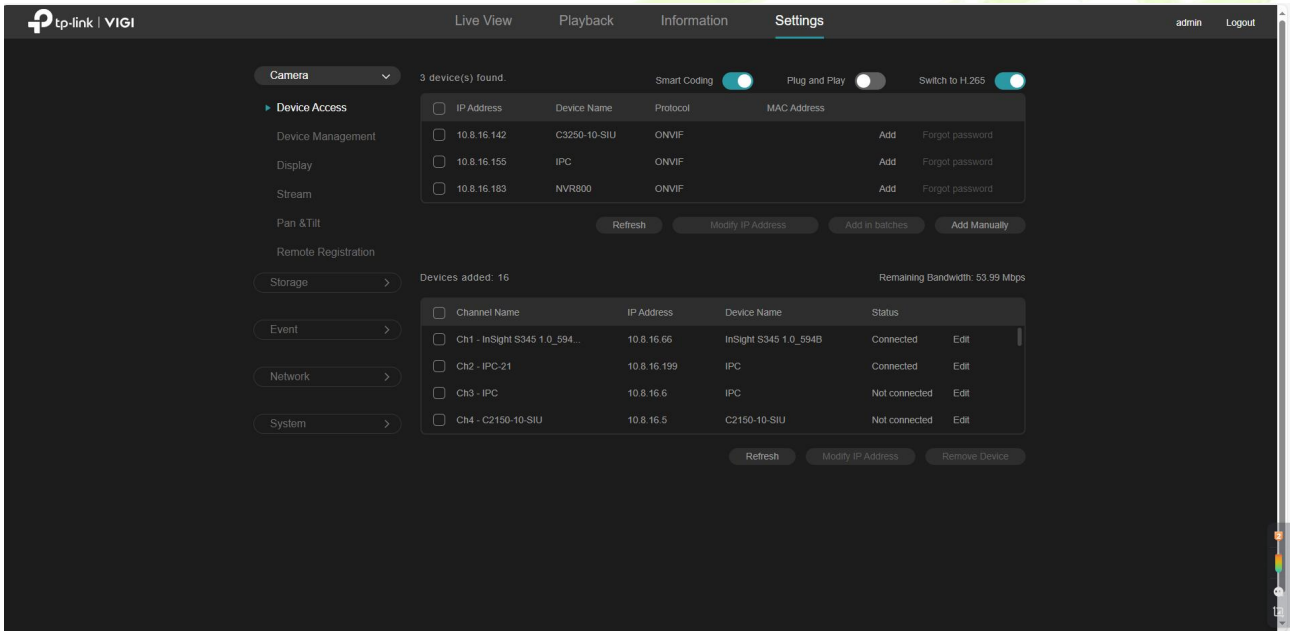
The description of each parameter is shown in Table.

Parameters/Buttons	Description
Type	Select the device type.
Protocol Type	Select the type of protocol.
Name	Customize the device name.
Port	Configure the device port.TPLink NVR default is 20443.
Address	Configure the device address. The format is: xxx.xxx.xxx.xxx, for example: 192.168. 6.5
Username & Password	The NVR'S user name and password.

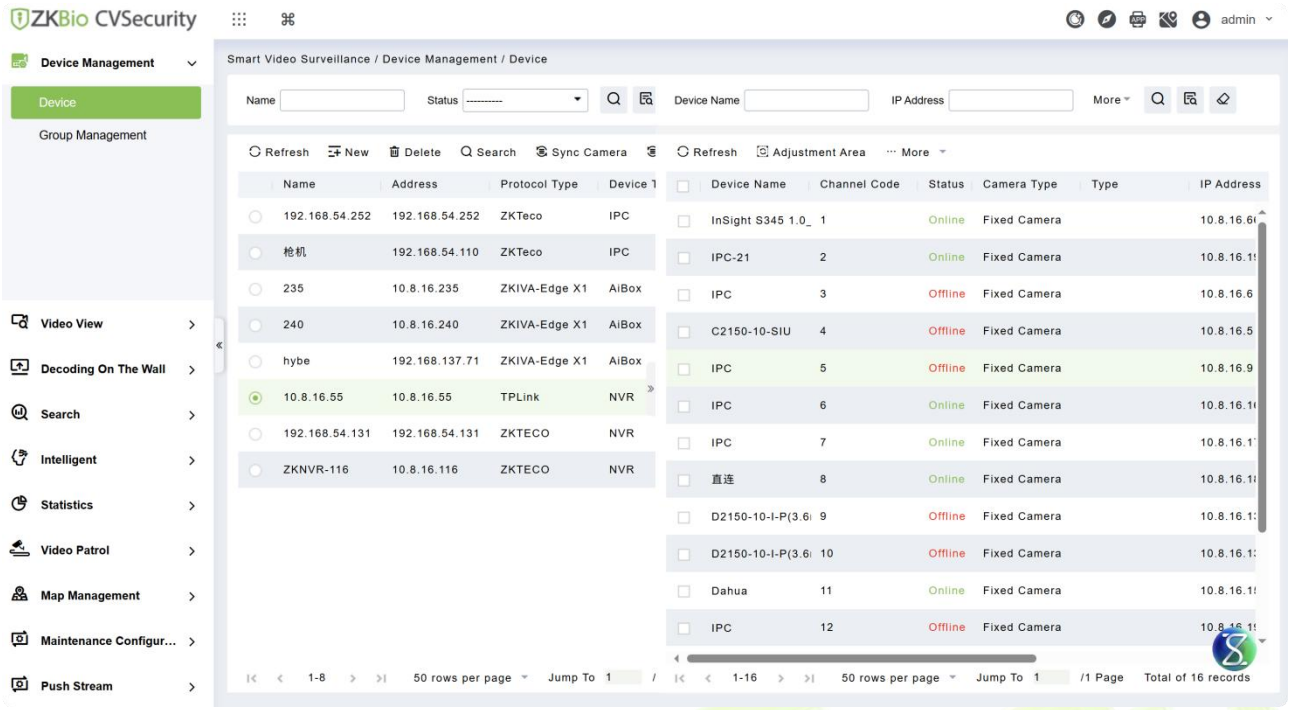
Step 3: Click **OK**.



Step 4: Add IPCs on the NVR client.



The software interface will automatically synchronize the added camera devices.

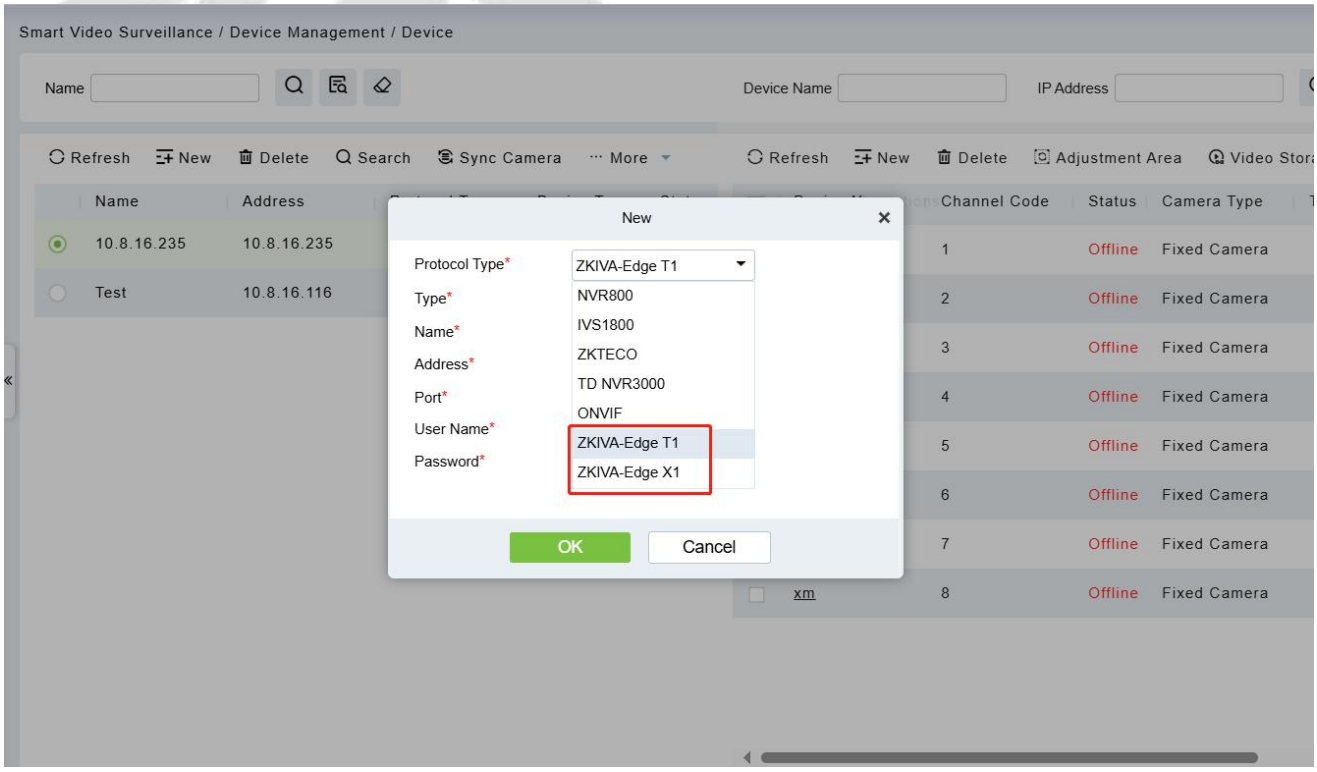


5.1.1.2Manual Add ZKIVA-Edge

To add a ZIVA-Edge T1/X1, click 'New.' Currently, the ZKIVA-Edge T1/X1 device only supports adding devices through this method and does not support adding devices via search.

Operation Steps

Step 1: Go to S**mart Video Surveillance > Device Management > Device**, and click New. Select your device model; if the device is a ZKIVA-Edge T1, choose that model.

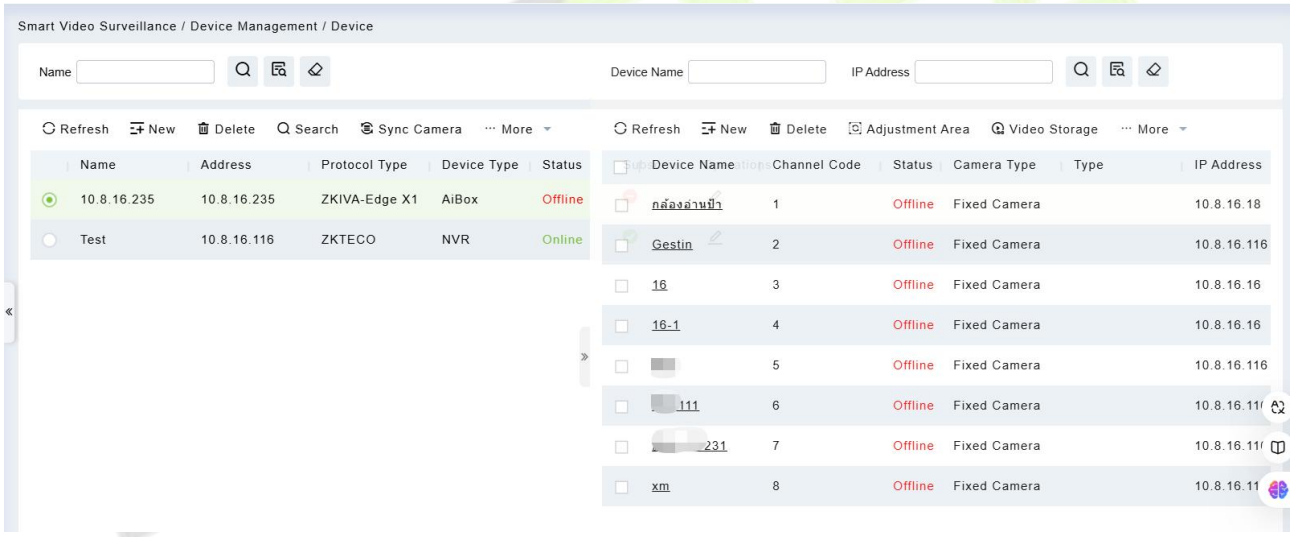


The table below provides a description of the parameters:

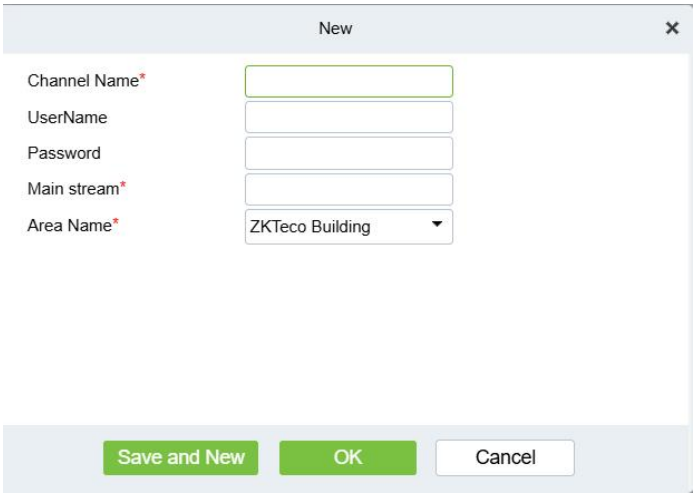
Parameter	Description
Protocol Type	Select the protocol type to be added: ZKIVA-Edge T1/X1.
Type	Select the type of device to be added: The default type for ZKIVA-Edge T1/X1 is AiBox.
Name	Customize the device name.
Address	Configure the device address. The format is: xxx.xxx.xxx.xxx, for example: 192.168.6.5.
Port	Configure the device port: The default port value is "80".
Username	The username and password for logging into the Web of the ZKIVA-Edge T1/X1 device.
Password	

Step 2: Add the camera to the ZKIVA-Edge.

Select ZKIVA-Edge from the list, and then click « on the expand/collapse window.



Step3: Click **New** to add a new camera to ZKIVA-Edge.



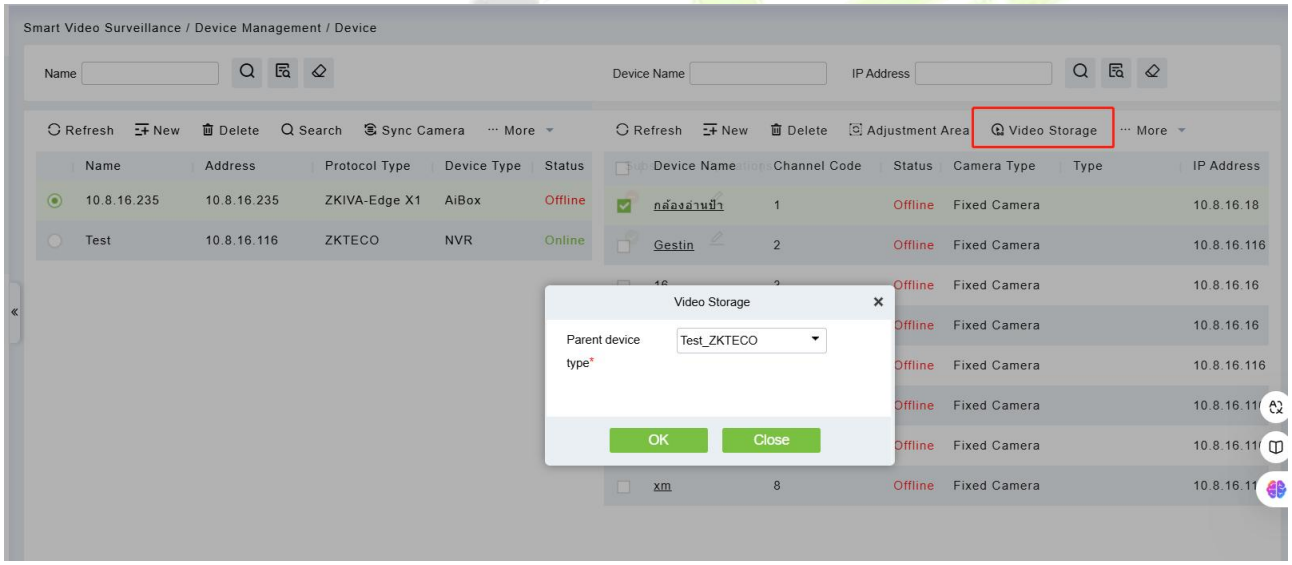
Parameter Description is as follows in the table:

Parameter	Description
Channel Name	Distinguish channels by setting camera names.
User Name	The IP address of the connected device (this address must be unique).
Password	Obtain the corresponding main stream after logging into the channel.
Main Stream	RTSP url of the camera for this channel.
Area Name	Select the area where the device is located.

● Video Storage

ZKIVA-Edge supports only algorithmic analysis and has no storage capability, you can bind the camera to an NVR by clicking **Video Storage**. This enables video playback and quickly integrates the camera with the NVR.

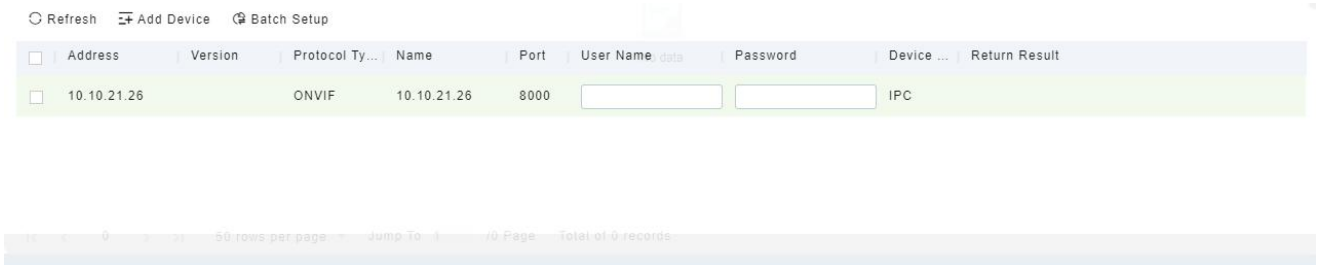
Note: If a camera is added to both ZKIVA-Edge and an NVR, it will consume license channel counts on both devices. For example, if a camera is already added to ZKNVR1 and then also added to ZKIVA-Edge X1, it will use 2 license channels.



5.1.1.3 Search to add NVR devices

Click Smart Video Surveillance > Device Management > Device.

Note: Search is not supported for IVS1800/TD NVR3000.

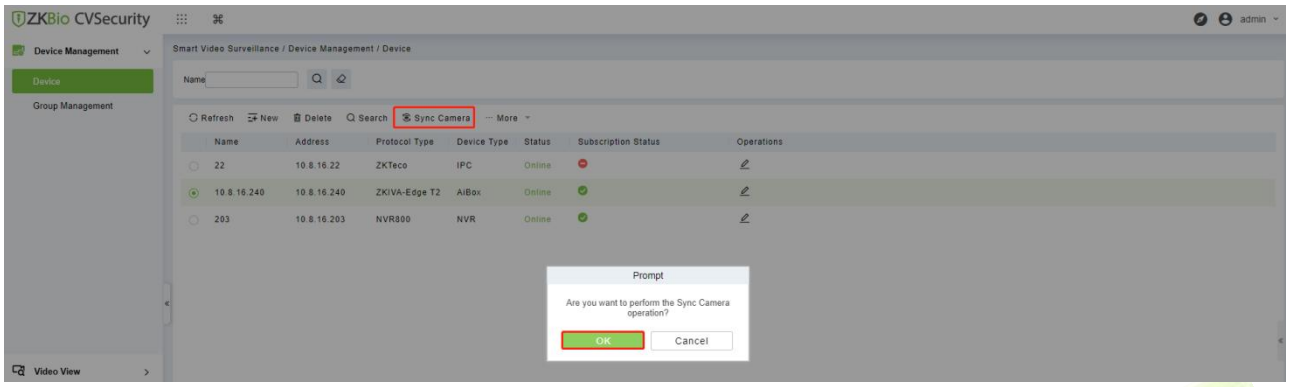


5.1.1.4Delete

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

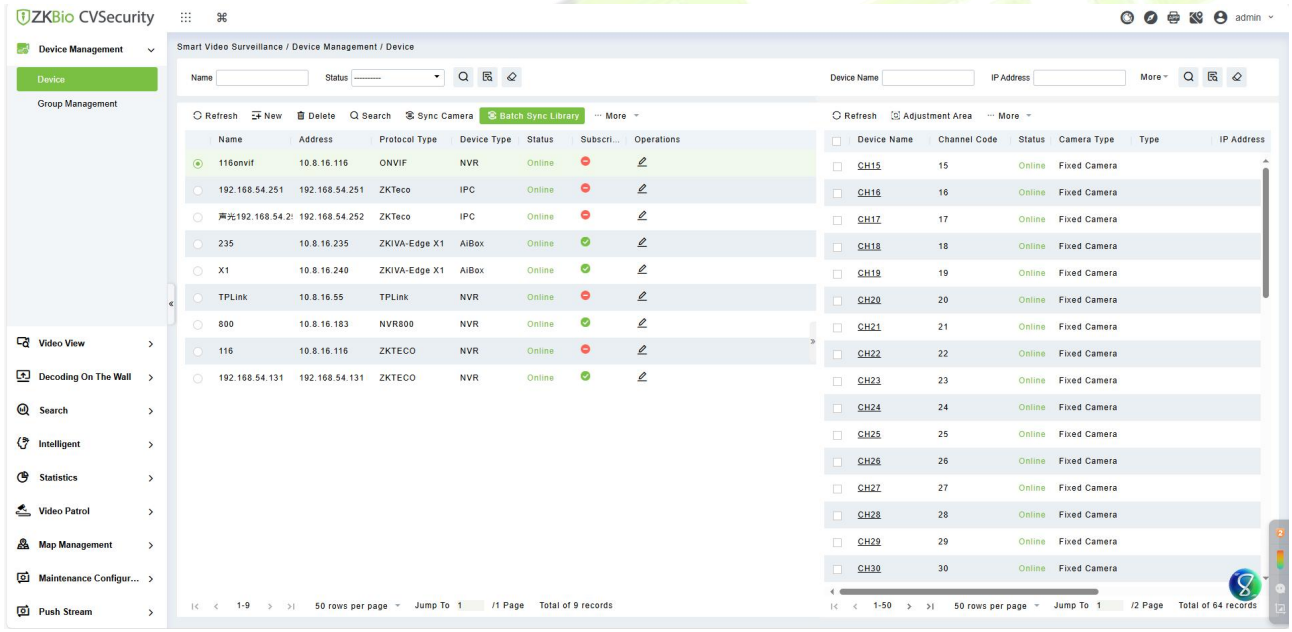
5.1.1.5Sync Camera

Click **Smart Video Surveillance > Device Management > Device**, then select Sync Camera.

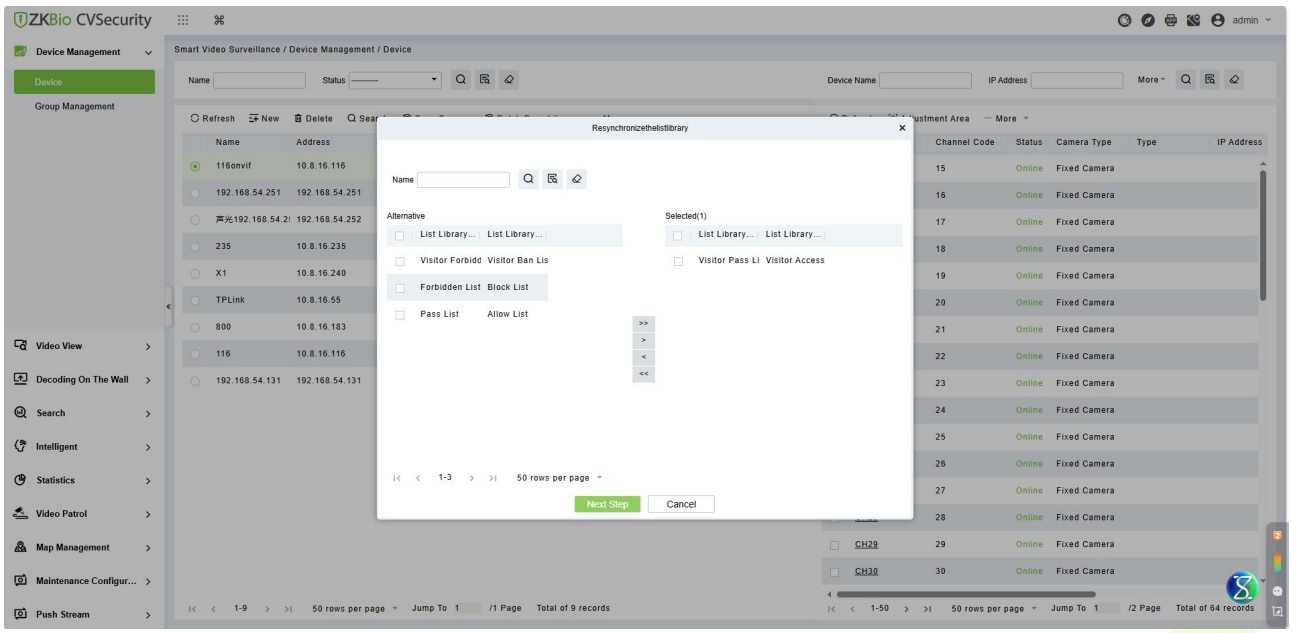


5.1.1.6Batch Sync Library

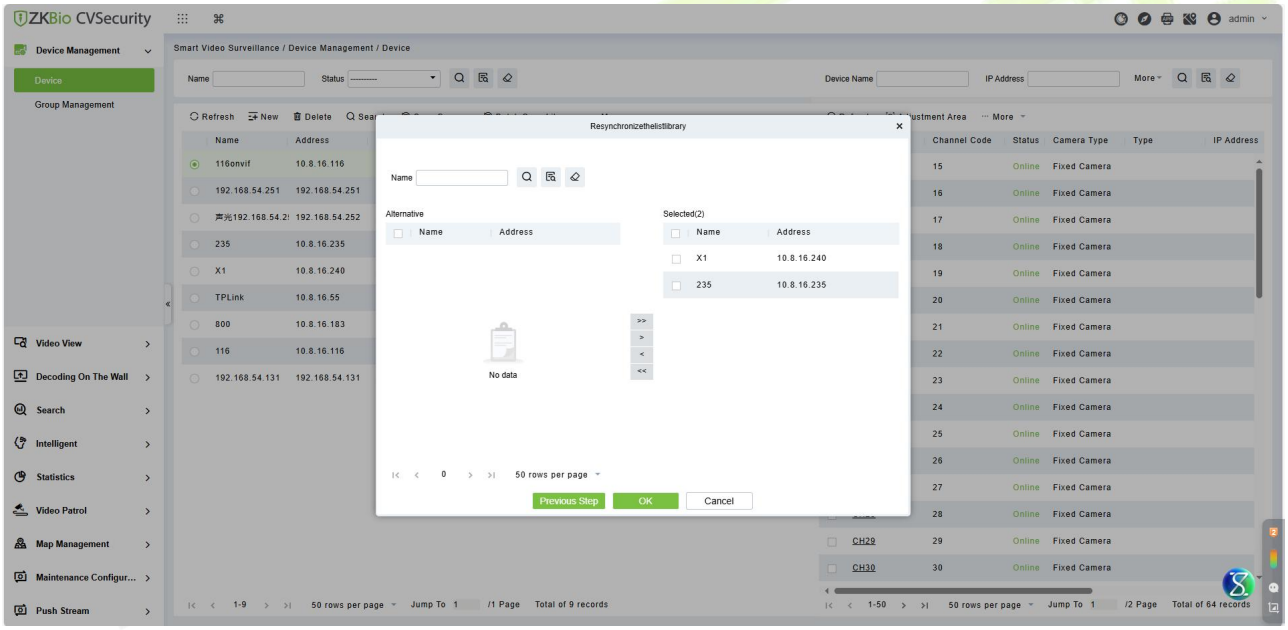
Step 1: Click **Smart Video Surveillance > Device Management > Device,** and click "Batch Sync Library".



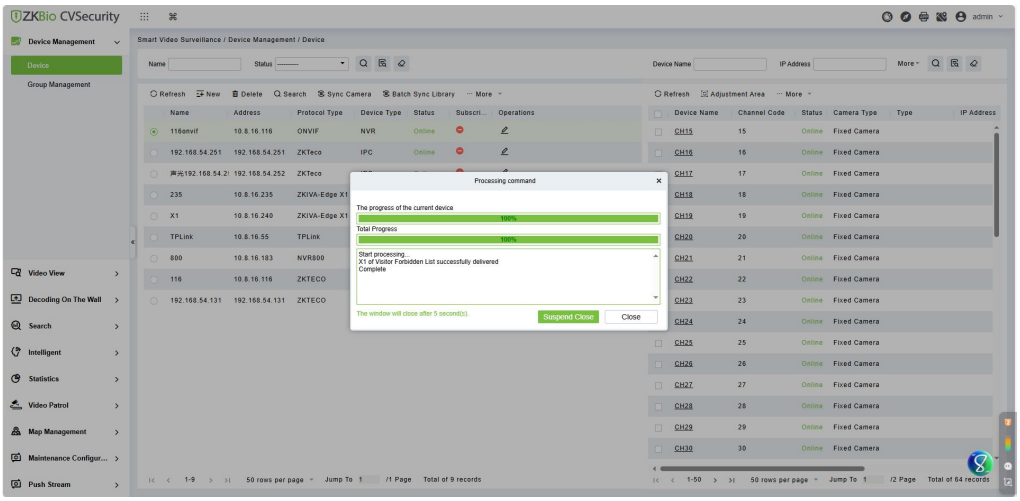
Step2: Select the list you want to synchronize and move it to the right,and click "Next Step".



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.



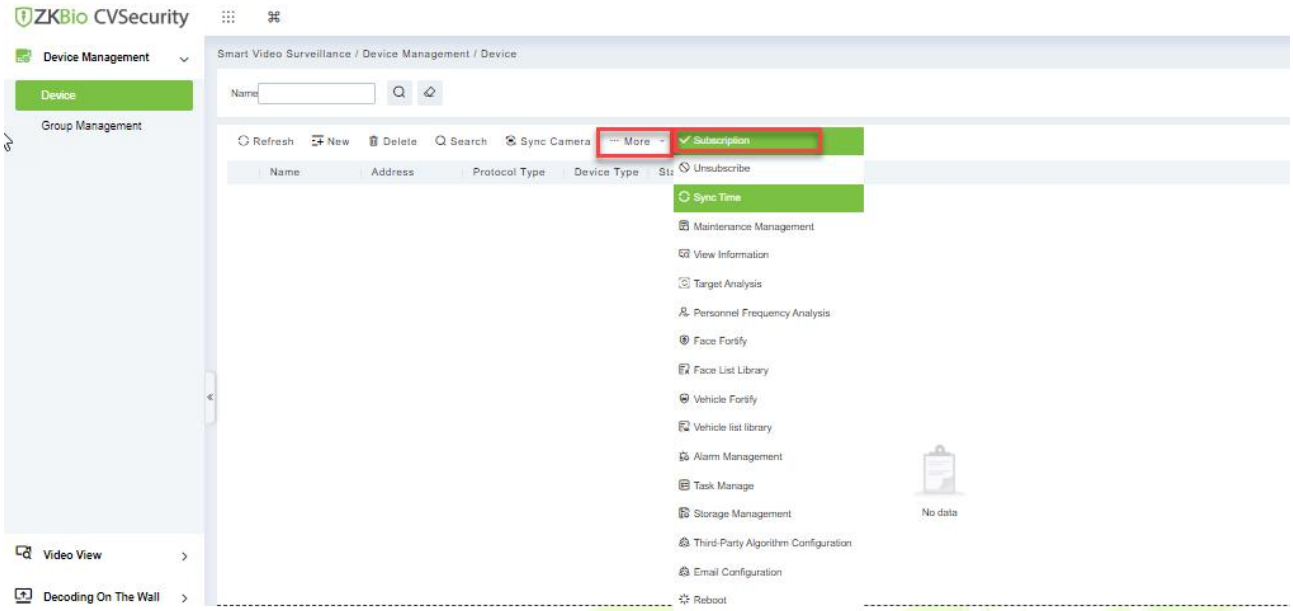
Data will start to be imported automatically until the operation completion prompt is given.



5.1.1.7Subscription

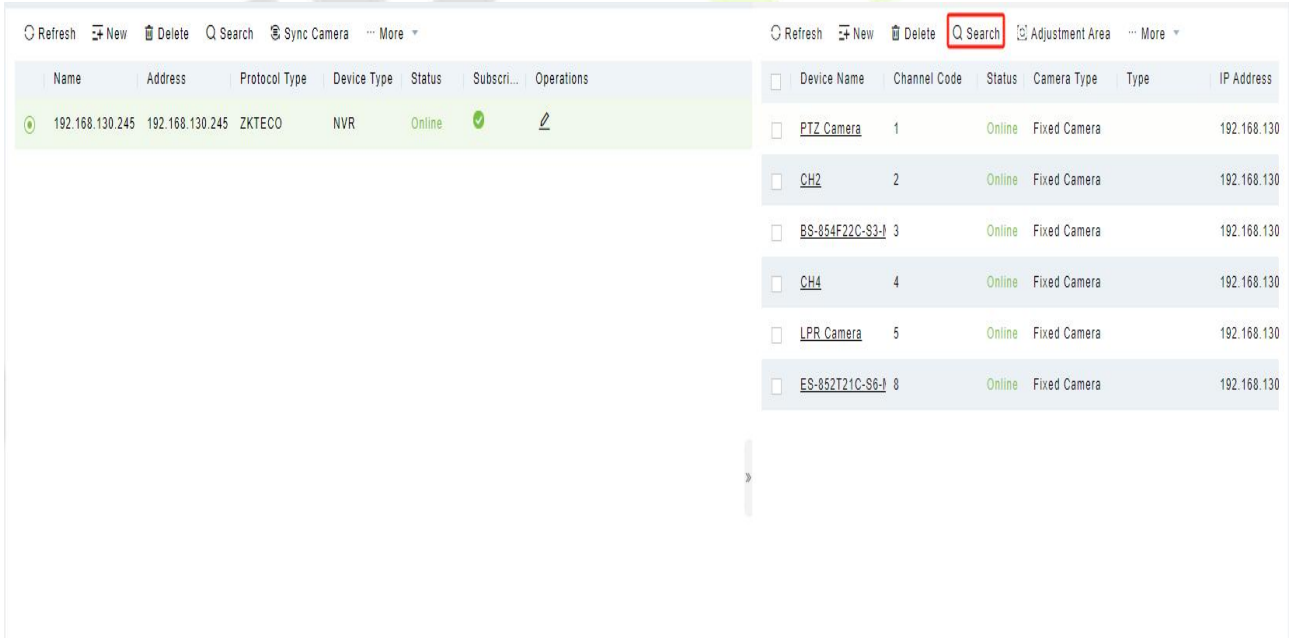
Click **Smart Video Surveillance > Device Management > Device, then click More > Subscription**.

The NVR will only push alerts to ZKBio CVSecurity after Subscription.



5.1.1.8Add Camera

Step 1: In the **Smart Video Surveillance** module, select "**Device Management > Device**".Select a NVR device, then click the "**Search**" button on the right.



Step2: Search for cameras by IP address.

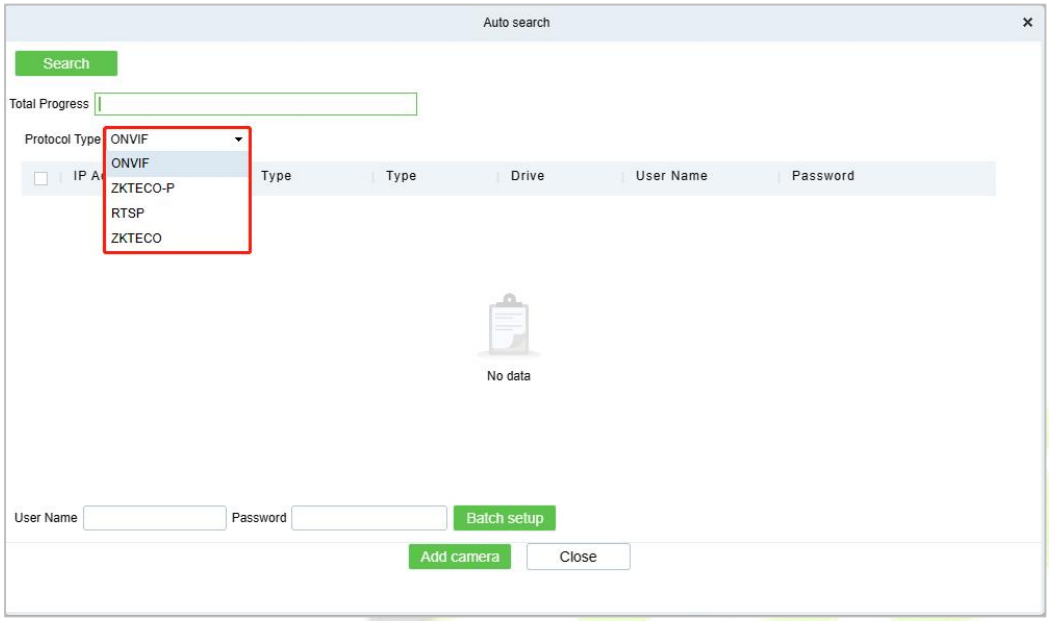
In the search interface, select the protocol type, that is, the protocol type ZKTeco-P, Rtsp, ZKTeco or ONVIF (recommended to use ZKTeco) connected to the camera.

Instruction:

1. Protocol type supports the selection of zkteco-P, Rtsp, zkteco and ONVIF protocols. (Recommended to use zkteco).
2. Using ZKTECO protocol access, all functions can be used normally.

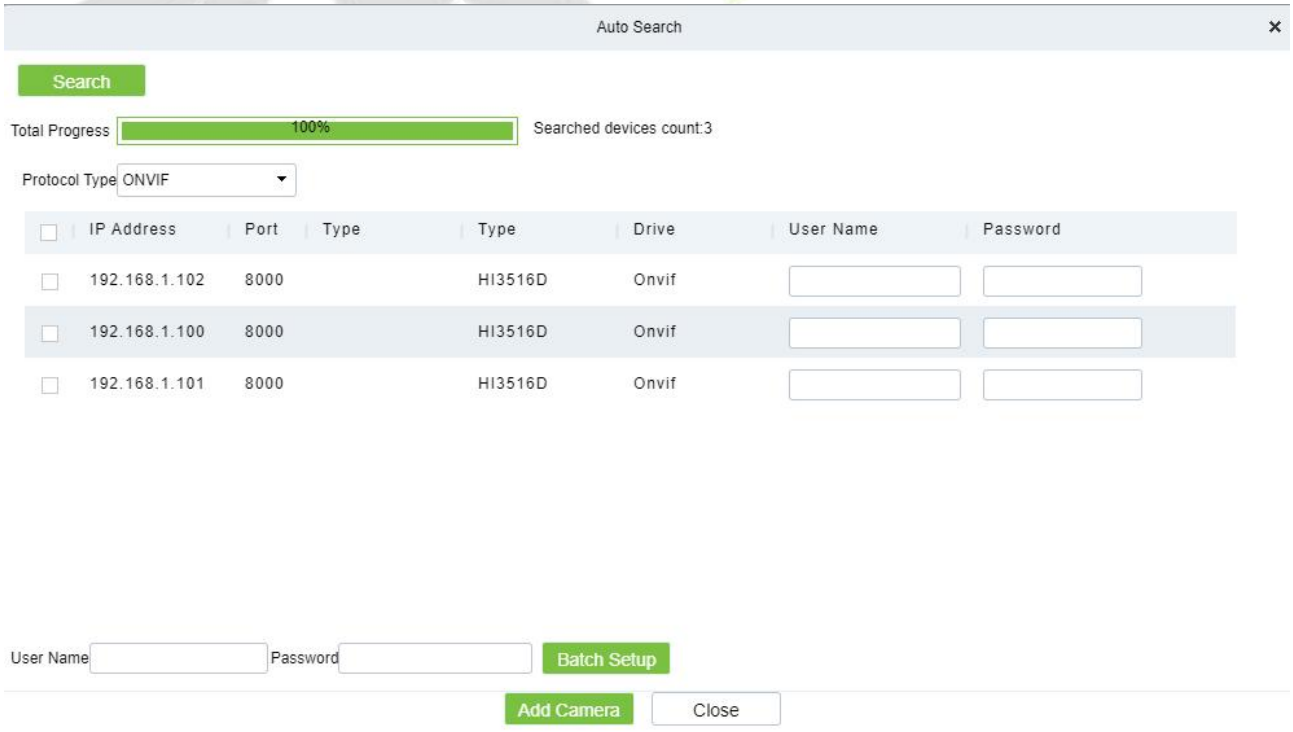
3. The ONVIF protocol is used to access, and the IPC parameter configuration except "camera" and "image parameter" does not take effect.
4. Using ZKTECO-P, Rtsp, protocol access, PTZ control cannot be used, and IPC parameter configuration does not take effect.

Click **Search** to start searching for online cameras.



Step 4: Account verification.

For the searched cameras, directly check the cameras in the camera list, and then perform account verification (the account number and password are the camera's registered user name and password), as shown in figure below, and parameter descriptions are shown in Table.



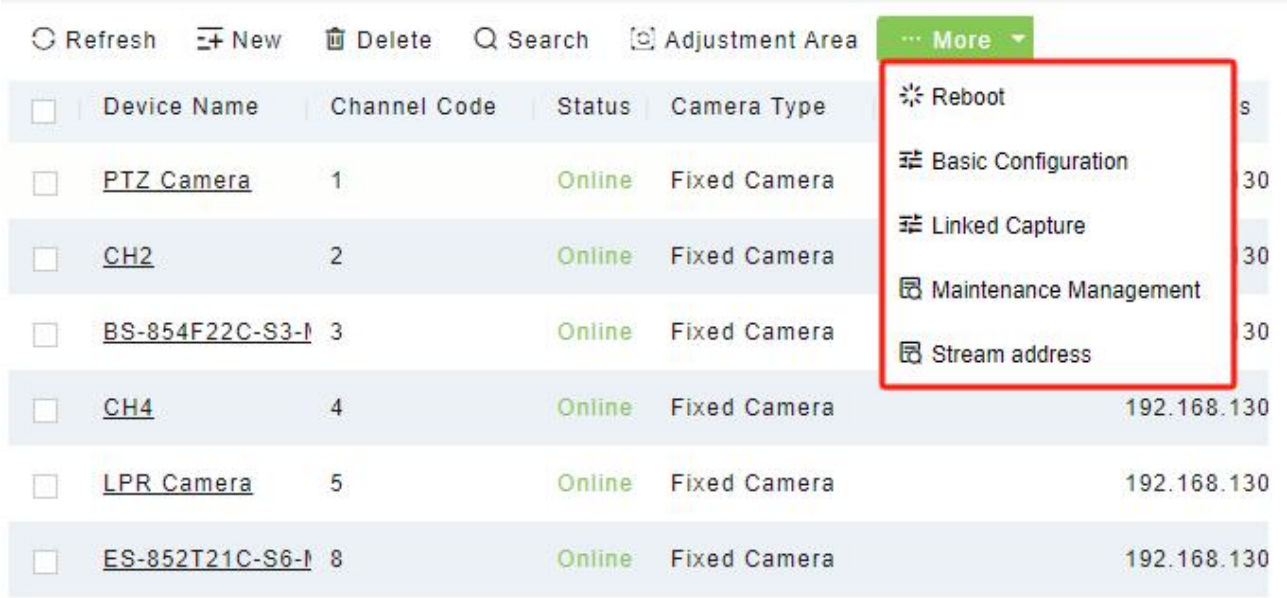
Parameter	Parameter Description
Port	Through zkteco-p, rtsp, zkteco, onvif protocols, the default port is 80.
Account Password	The registered username and password of the camera. If all cameras to be added have the same registered username and the same registered password, you can also use the username and password at the bottom of the search list for batch verification.

Step 5: Close the pop-up window to complete the search and addition of cameras.

Step 6: The subsequent configuration is shown in Table.

Scenes	Configure
New/Delete	Click New : Manually add a camera. Click Delete : Select one or more cameras to delete.
Adjustment Area	Under the **Camera Device** tab, you can select single or multiple cameras, and then click the Adjustment Area button to adjust the area to which the cameras belong.

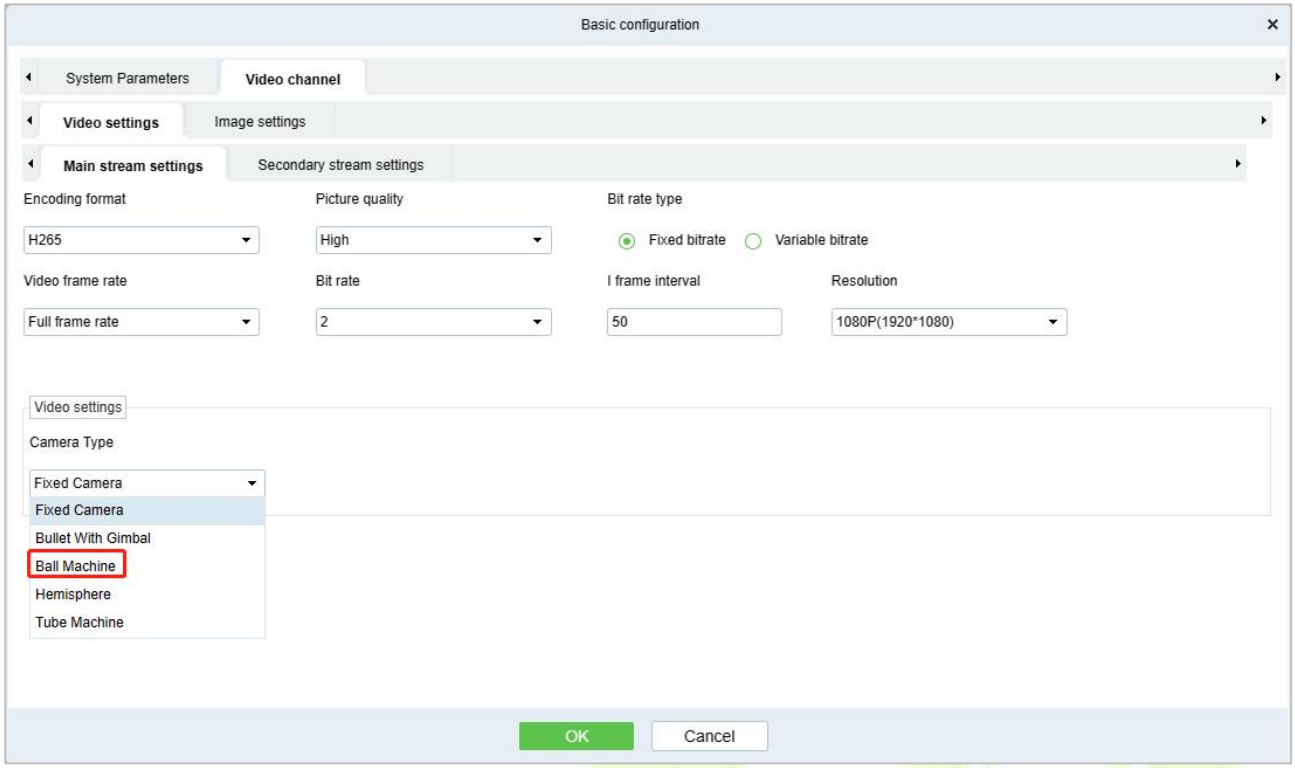
Step 7: Parameter Setup: Click **More** to get more operation.



Reboot: Restart the camera.

Basic Configuration: Basic camera parameters configuration, including encoding format, image quality, bit rate, pixels, etc.

Note: If the added camera is PTZ, you need to switch the camera type to **Ball Machine** in this page below.



5.1.2Group Management

Click **Smart Video Surveillance > Device Management > Group Management**.

5.1.2.1New

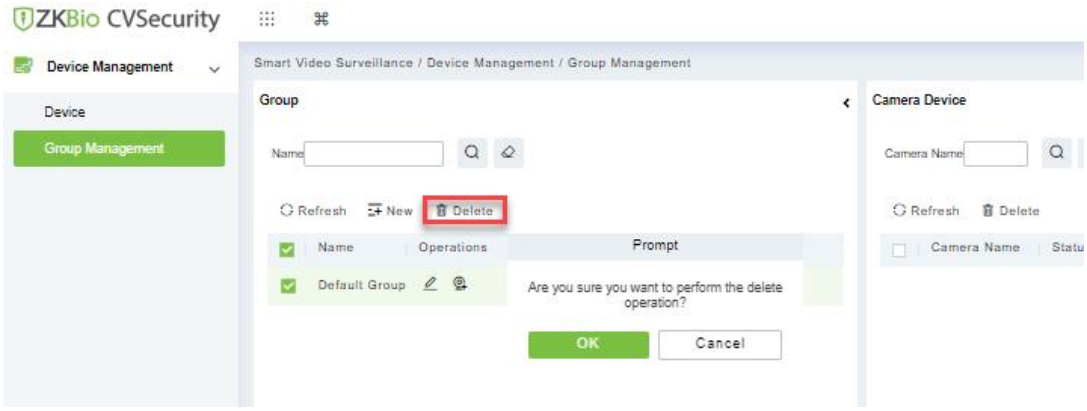
Click Smart Video Surveillance > Device Management > Group Management, then select New.

Parameters	Description
Name	Enter the name of the group.

Click **OK** to save and exit.

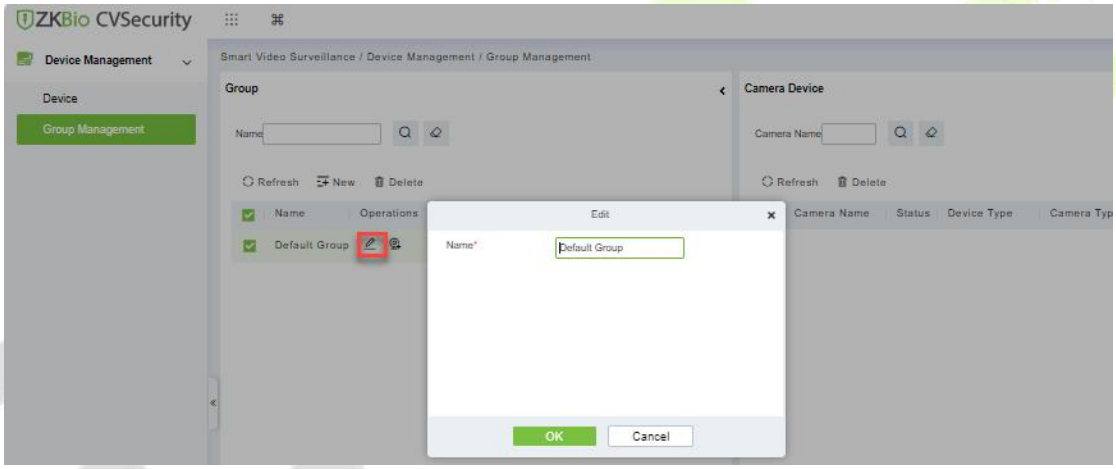
5.1.2.2Delete

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



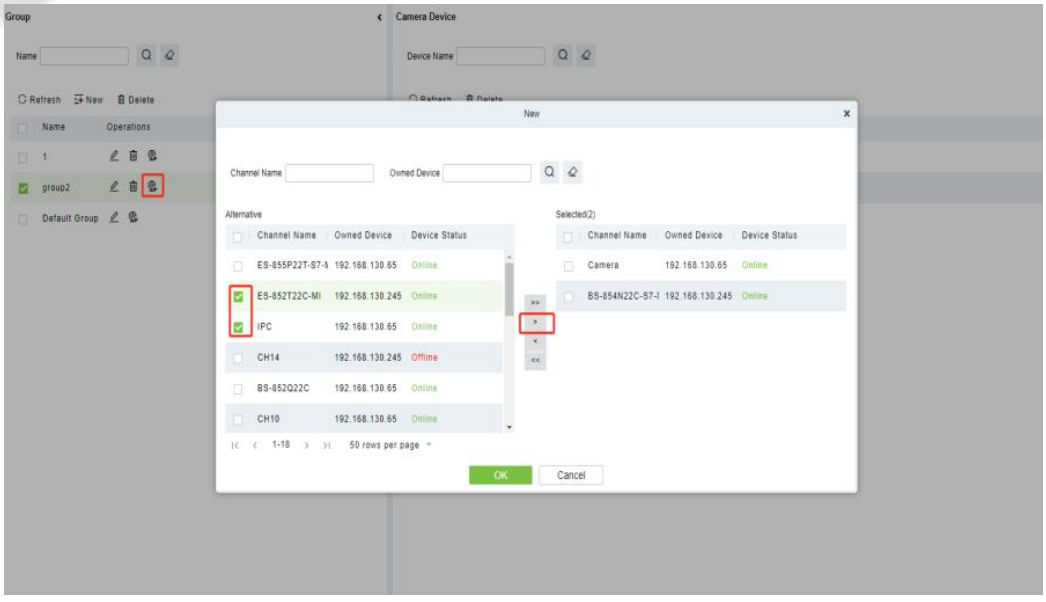
5.1.2.3Edit

Click **Smart Video Surveillance > Device Management > Group Management**, then click on the Edit icon to edit the required details.



5.1.2.4Add Camera to Group

Click **Smart Video Surveillance > Device Management > Group Management**, then select Add Camera.



5.2 Video View

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

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

5.2.1Video Preview

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

You can review recorded videos here.

5.2.1.1Live Preview

● Description:

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:

Step 1: In the Smart Video Surveillance module, select **Video View > Video Preview**.

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

Description:

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 become unstreamlined.

● Live preview of group camera:

Step 1: In the Smart Video Surveillance module, select "**Device Management > Grouping Management**" to group the cameras.

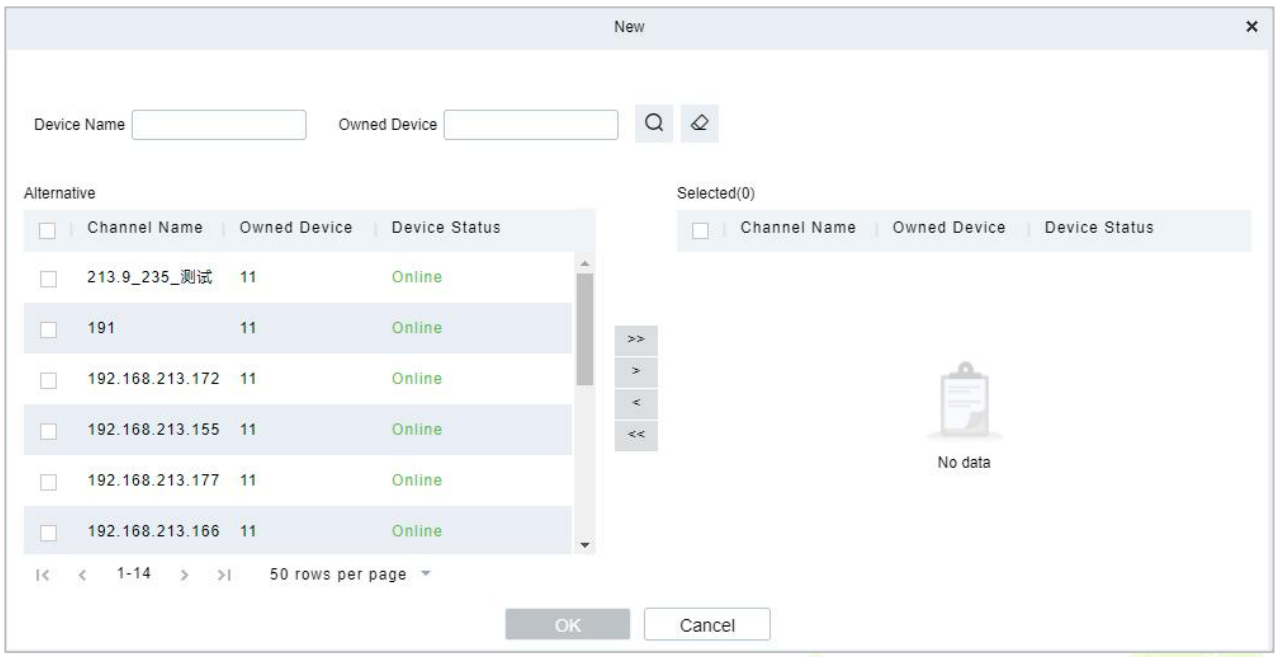
Step 2: Click **Add** in the grouping list, enter the grouping name, and click "Confirm" to complete the addition of camera grouping.

Step 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.

Step 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.

Description:

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.



5.2.1.2Video Preview

●Operation scenario:

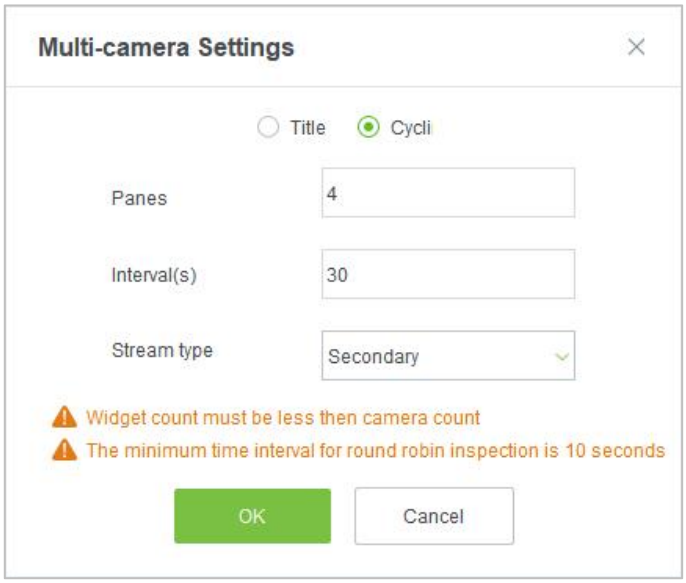
Using the round patrol function, the user can switch the live pictures monitored by multiple cameras regularly. For example, there are multiple cameras in a scene, and the live situation of all cameras cannot be displayed on a live split screen interface. The administrator can automatically switch the 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.

●Operating Steps:

Step 1: In the **Smart Video Surveillance** module, select Video View > Video Preview.

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

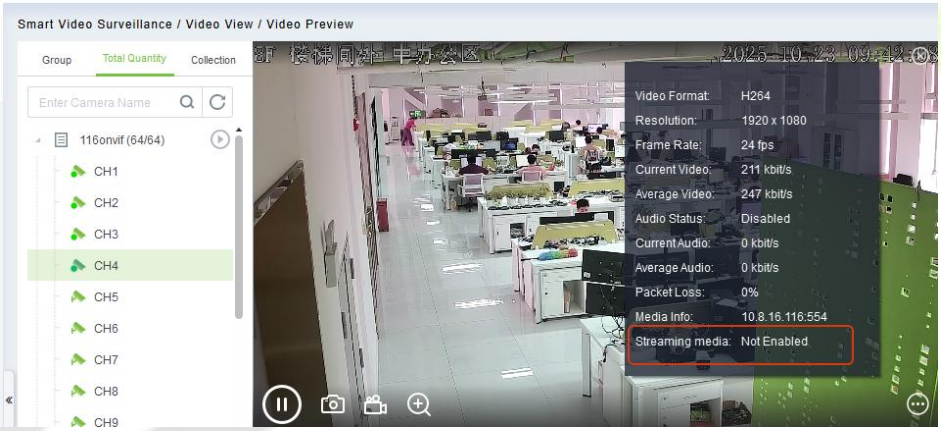
Step 3: Click "Round Tour" to open the round tour setting window and configure round tour information, as shown in figure below, and the parameter description is shown in Table.



Parameter	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	• Main code stream: large code stream, high definition, and high bandwidth occupation. • Auxiliary code stream: The code stream is small, the definition is low, and the bandwidth is small. Description: When there is bandwidth limitation, it is recommended to select secondary code stream.

Step 4: Click **OK** to start the round tour.

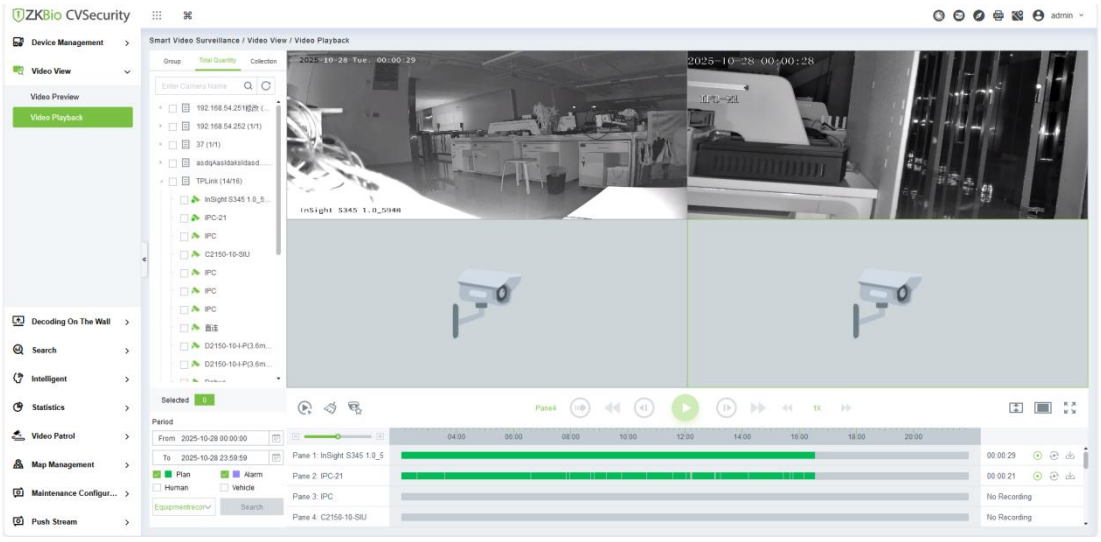
Step 5: End the round and click the toolbar below to close all screens.



You can check whether the current playback is streaming media during video preview.

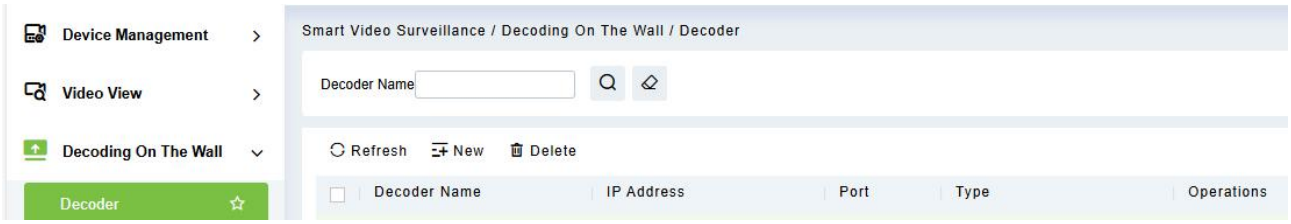
5.2.2Video Playback

Click Smart Video Surveillance > Video View > Video Playback.



5.3 Decoding On the Wall

Click **Smart Video Surveillance > Decoding on The Wall**.

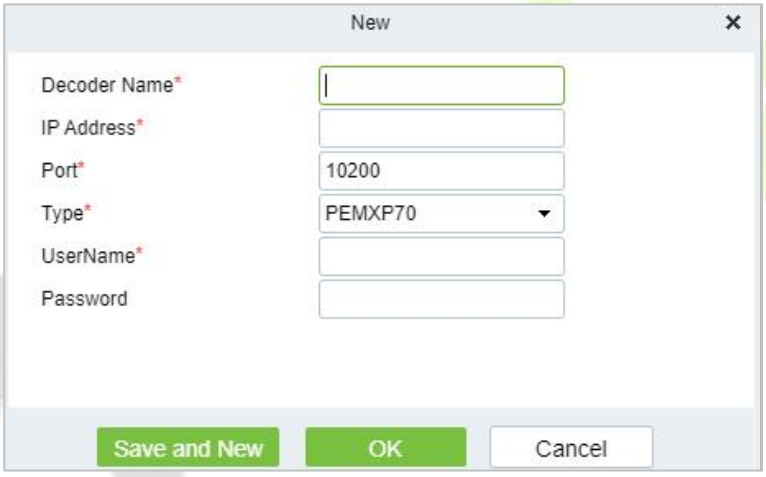


5.3.1Decoder

Click **Smart Video Surveillance > Decoding on the wall > Decoder**.

5.3.1.1New (Add Decoder)

Click **Smart Video Surveillance > Decoding on The Wall**, then select New.



Parameter	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

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

5.3.2TV Wall

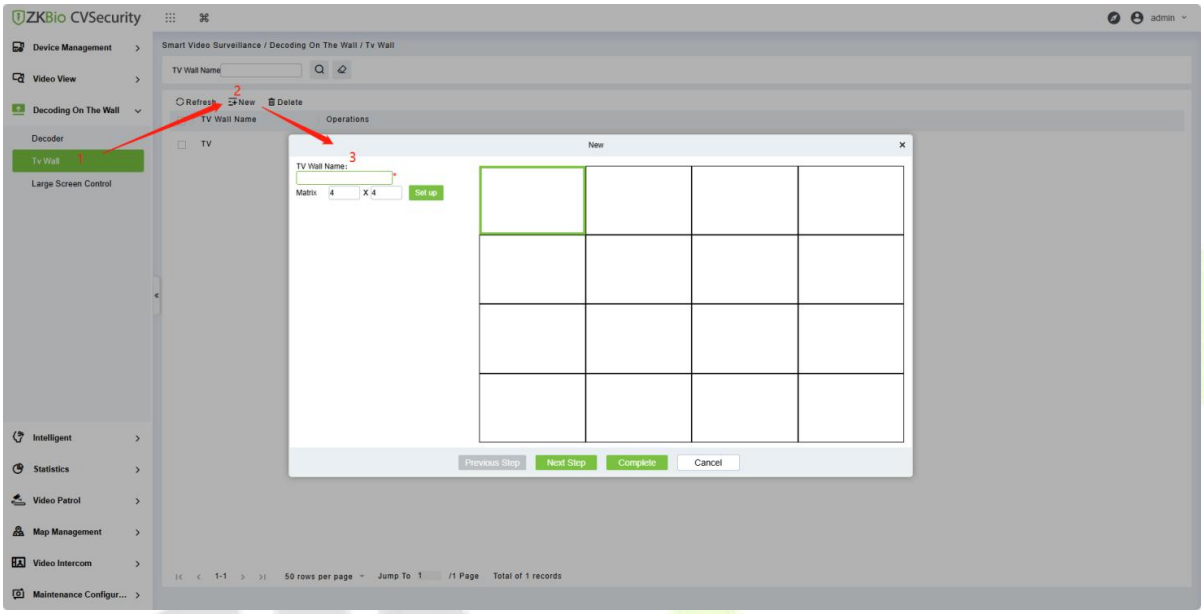
Click **Smart Video Surveillance > Decoding on the wall > TV Wall**.

5.3.2.1New (Create TV Wall)

Click **Smart Video Surveillance > Decoding on the wall > TV Wall**, then select New (Create TV Wall).

Step 1: In the Smart Video Surveillance module, select "**Decoding Wall > TV Wall**".

Step 2: Click **Add** to enter the "**Add TV Wall**" page, as shown in figure below



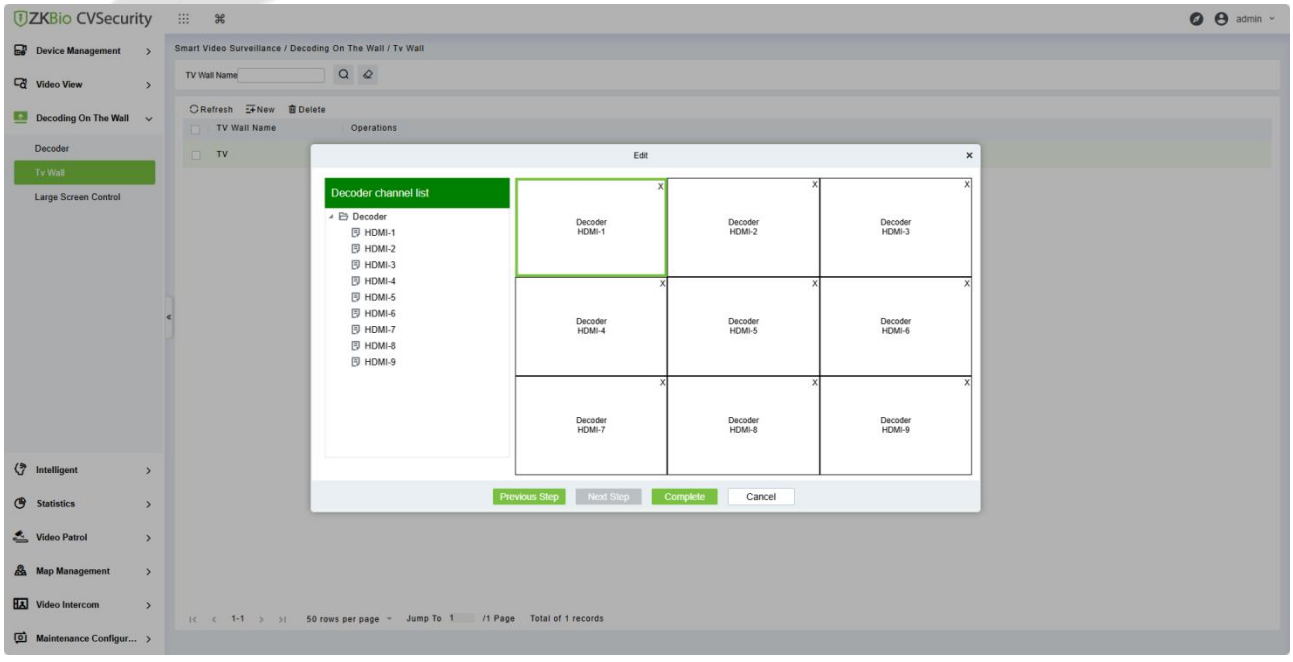
Step 3: Enter a custom TV Wall Name.

Step 4: In the Matrix Settings box, customize the number of rows and list of input layouts, and click **Settings** to apply the layout.

Description:

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

Step 5: Click next to enter the TV wall binding decoder interface, as shown in figure below.



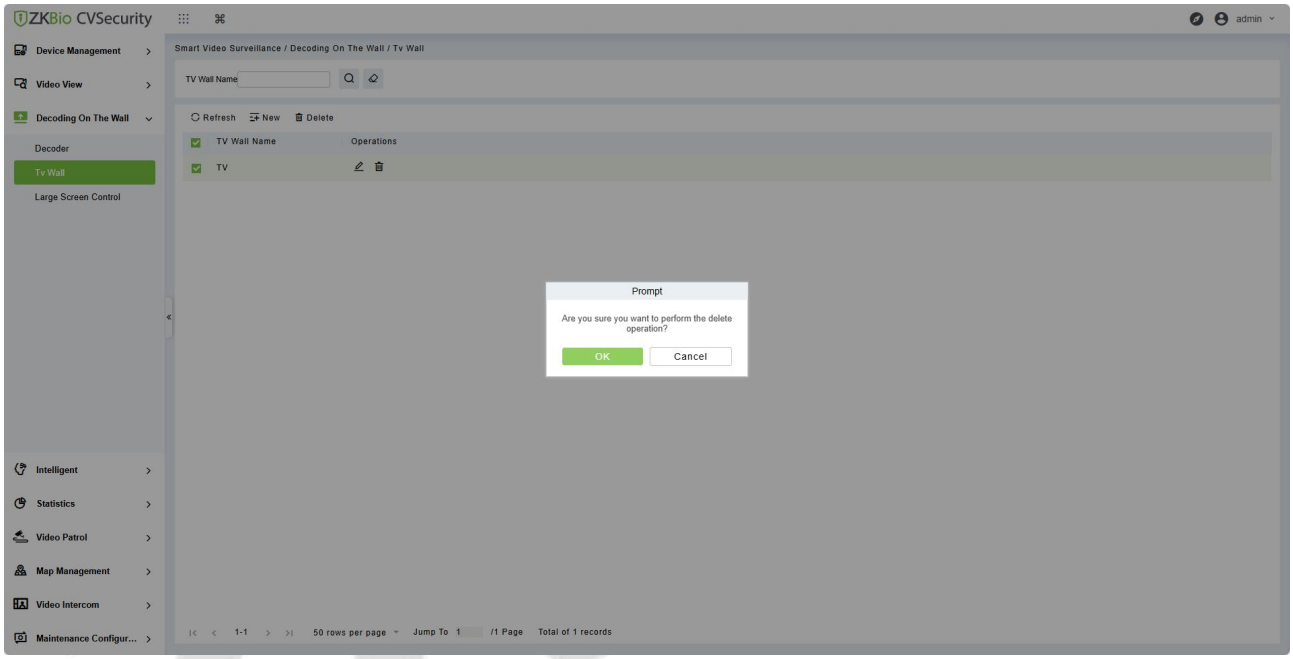
Step 6: Select the TV wall pane to which you want to add a decoder channel, and then click **Decoder Channel** on the left to complete the binding.

Parameter	Description
TV Wall Name	Enter the TV wall name.

Step 7: Click **Finish** to finish adding the TV wall.

5.3.2.2Delete

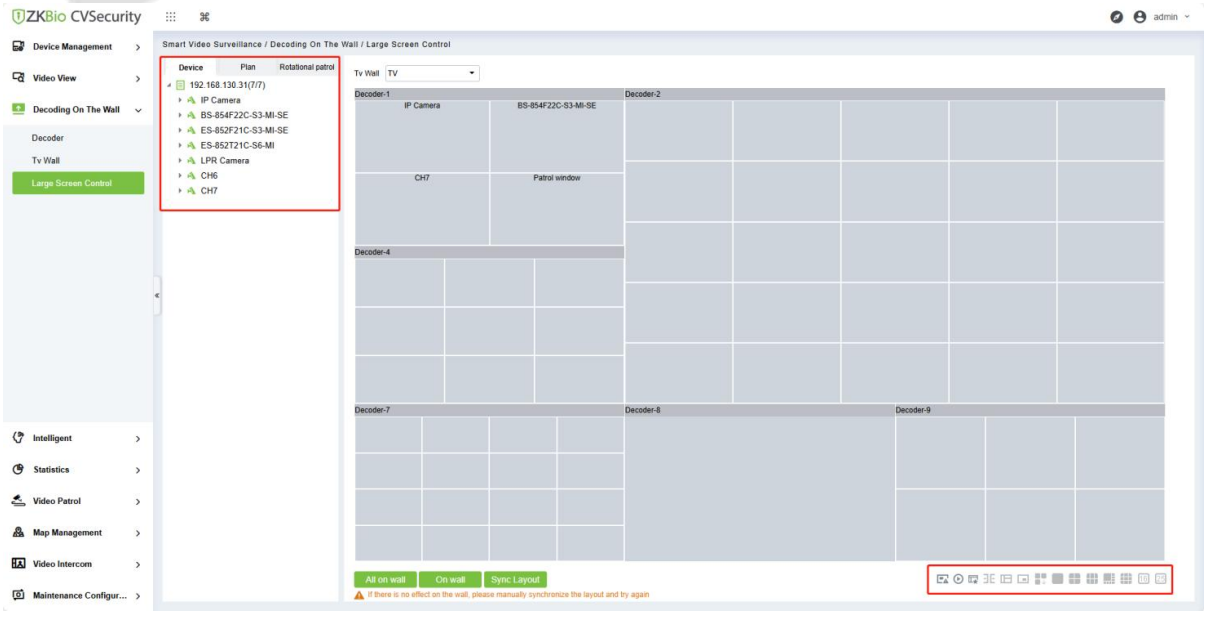
Click **Smart Video Surveillance > Decoding on The Wall > TV Wall**, then select Delete.



5.3.3Large Screen Control

5.3.3.1Device

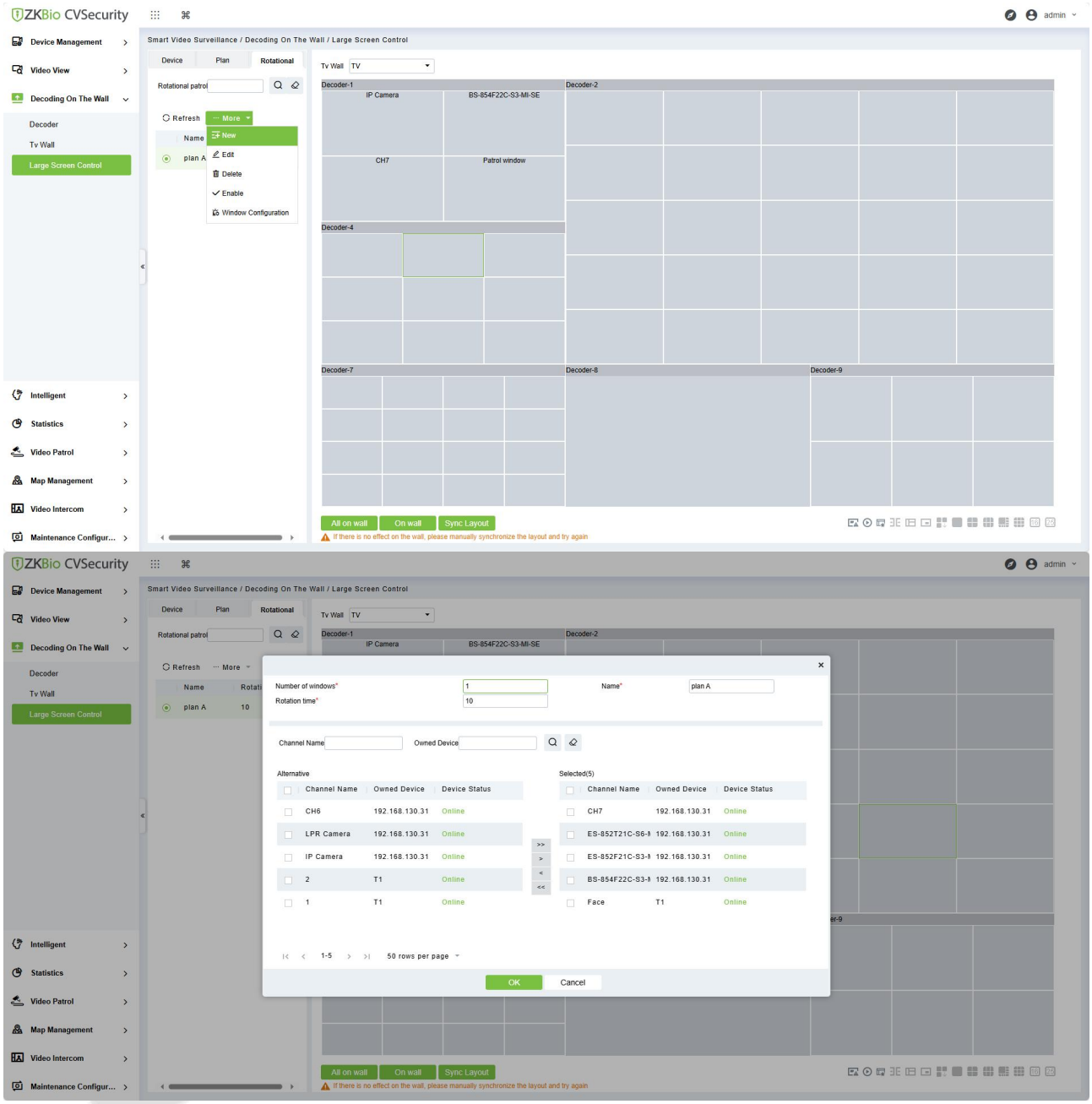
Click **Smart Video Surveillance > Decoding on the wall > Large Screen Control**.



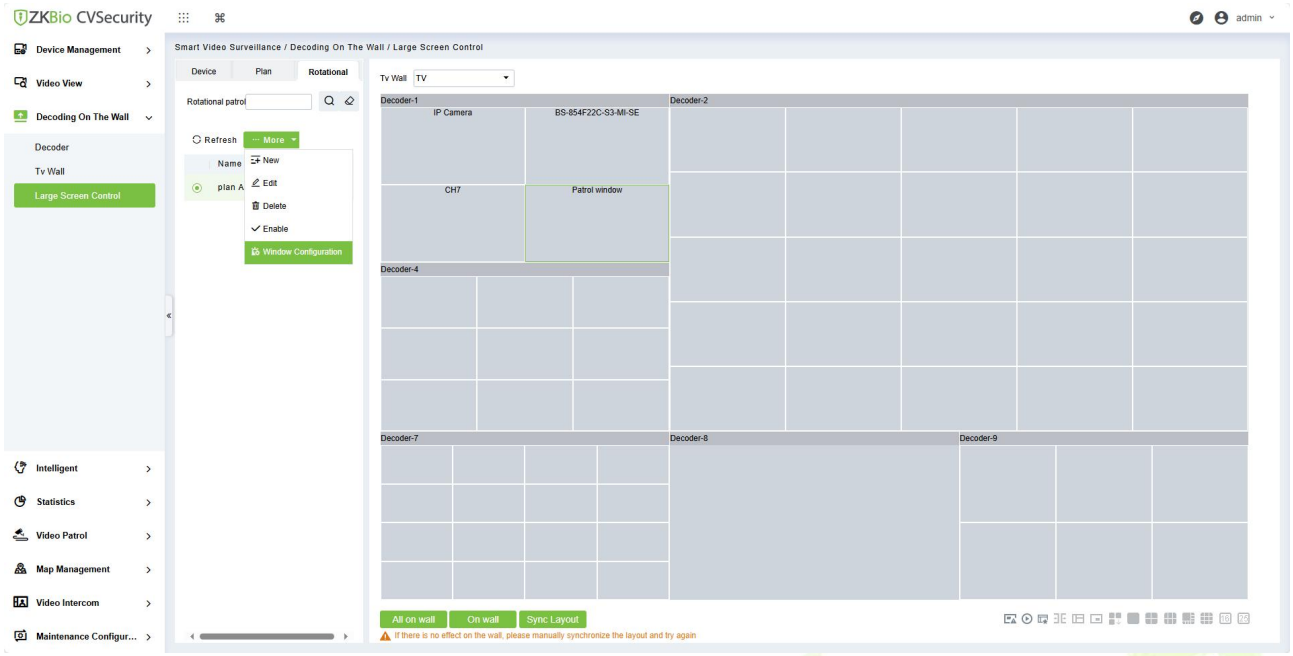
Icon	Parameter	Description
	Alarm Setup	Select a screen to show the events of linked alarms.
	Video Preview	Previewing the current screen.
	Collection of Plan	Join the list of collection profiles.
	Merged screen	Merge multiple scattered screens into one.
	Split Screen	Separate the merged screens.
	Floating 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.
	9 Split Screen	9 Split Screen.
	16 Split Screen	16 Split Screen.
	25 Split Screen	25 Split Screen.

5.3.3.2Rotational Patrol

Step 1: Click **More** > **New,** Enter the number of Windows, Name and Rotation Time, and select the channel to play, and click OK.



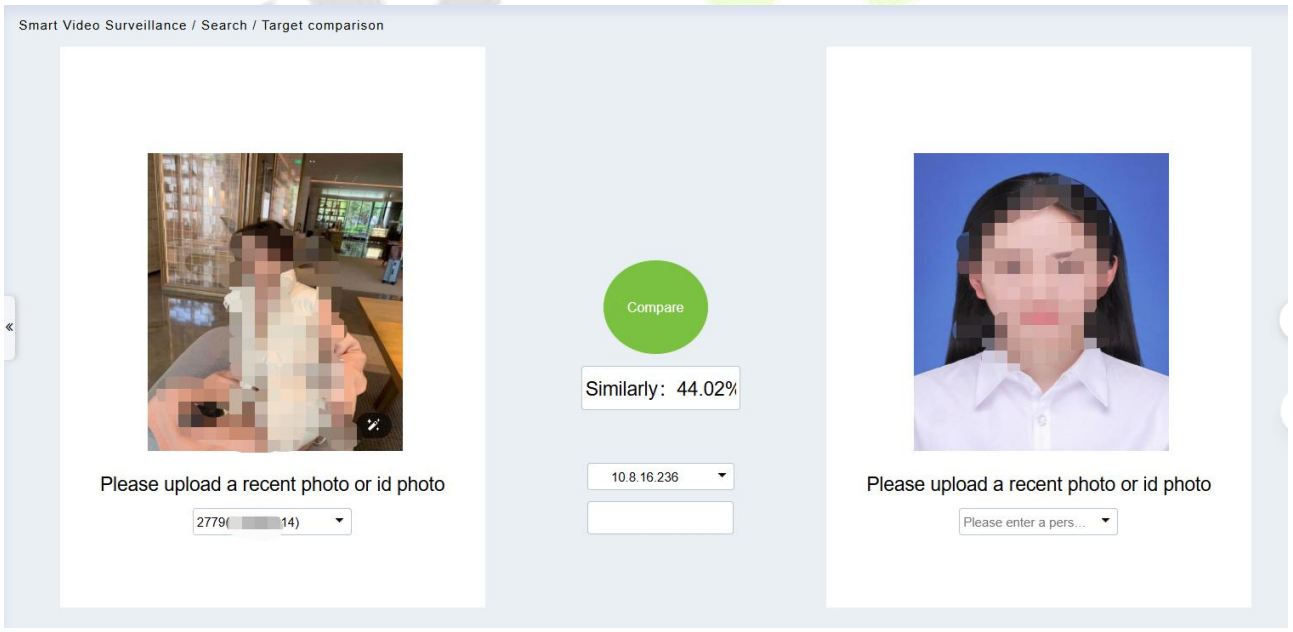
Step 2: Select windows, and click **More > Window Configuration > Enable**.



5.4 Search

Its function is to use face recognition technology to compare the people in two photos (recent photos or ID photos) by uploading them, and determine whether they are the same person.

Note: Currently, this function is only supported by ZKIVA - Edge T1/X1.

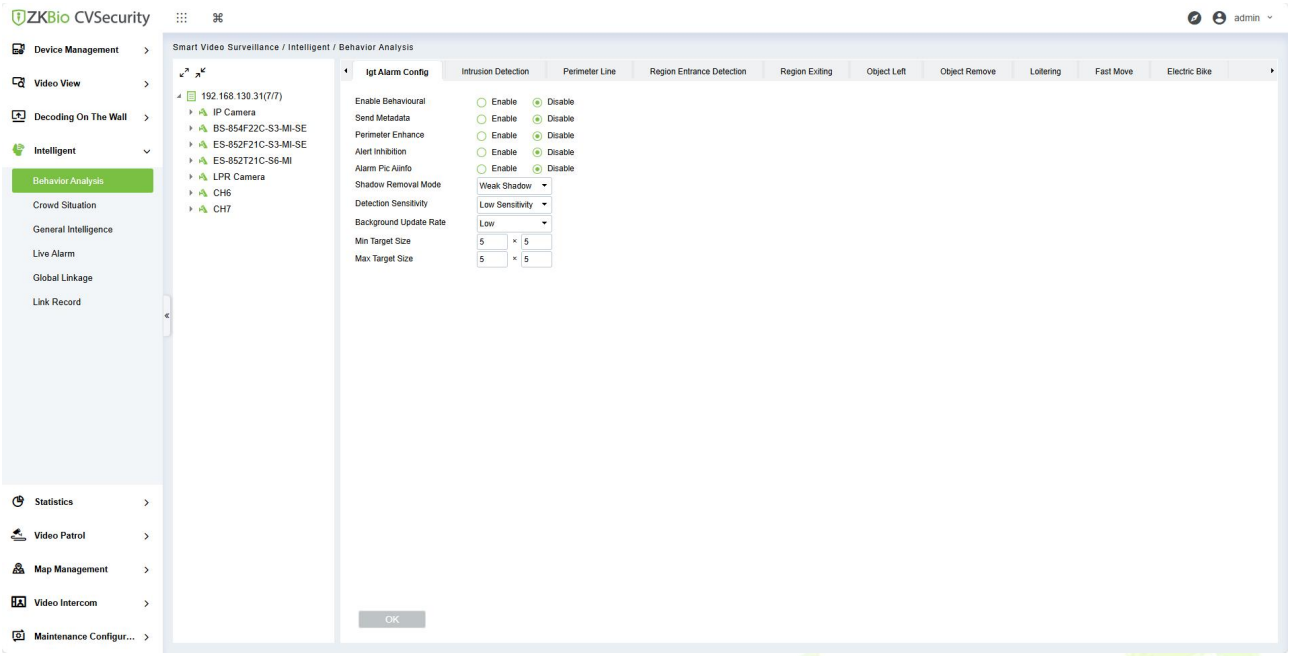


5.5 Intelligent

5.5.1 Behavior Analysis

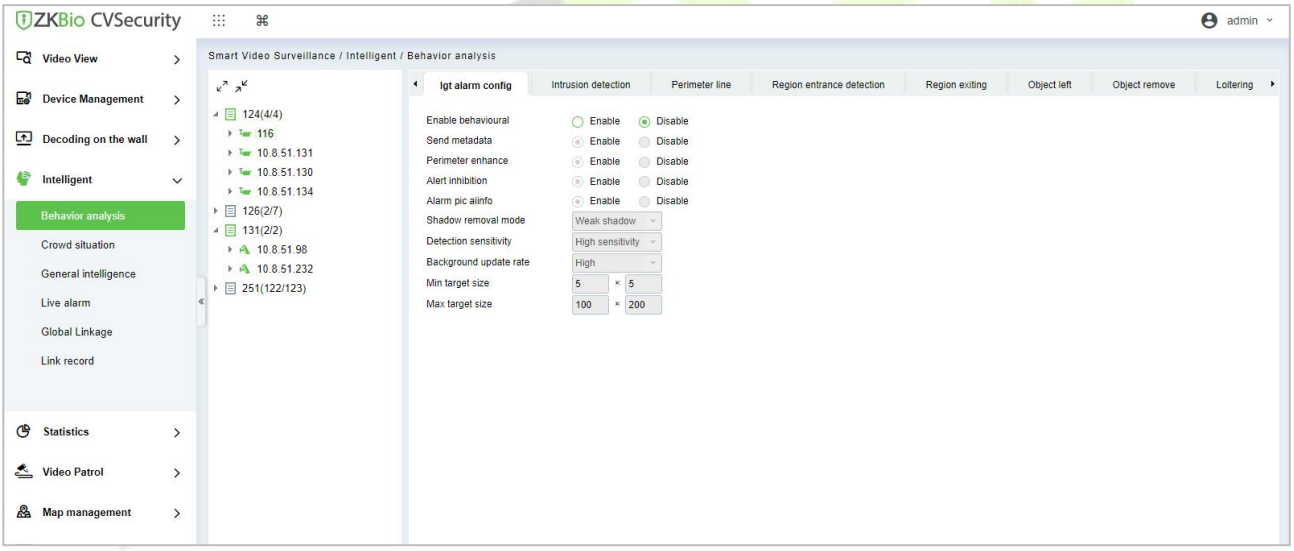
Configuration of intelligent functions for behavioral analysis using front-end cameras by ZKBio CVSecurity.

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

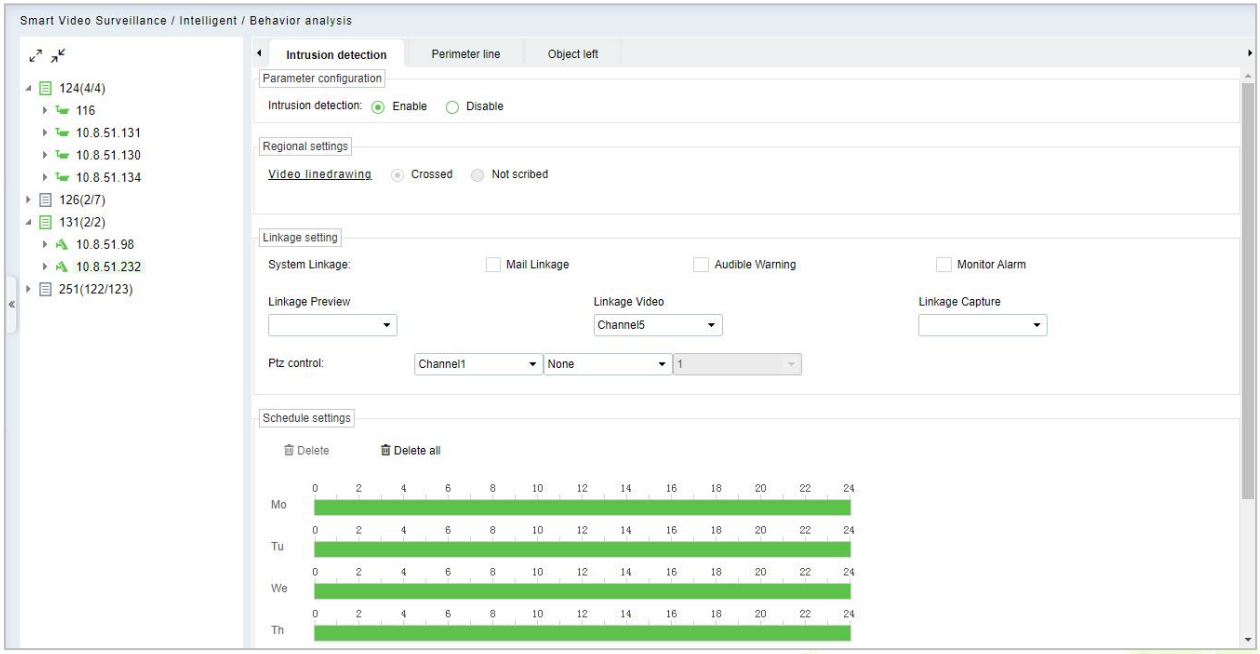


Step 1: Select the camera on the left and the software will automatically switch to the menu of smart features supported by that camera.

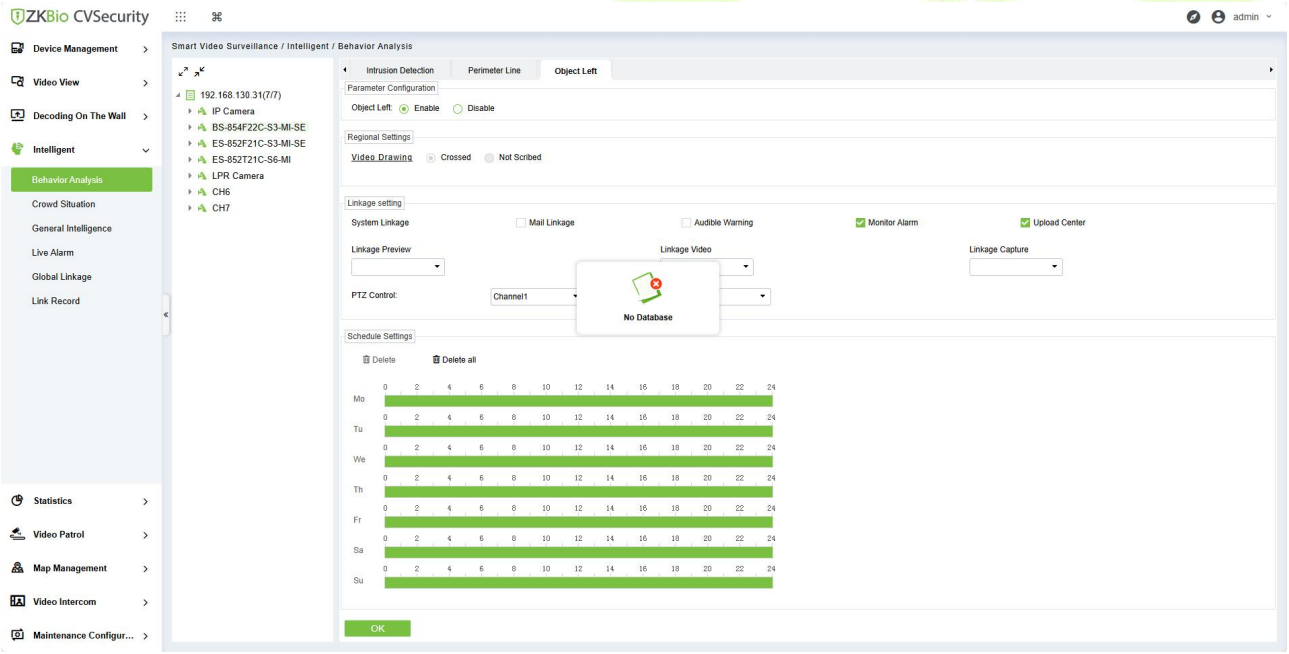
1) If it's Holowits branch device, after click, the page shown as below:



2) If it's ZKBio Sense device, after click, the page shown as below:



3) If the camera does not support intelligent functions, after click, the page shown as below: No database.

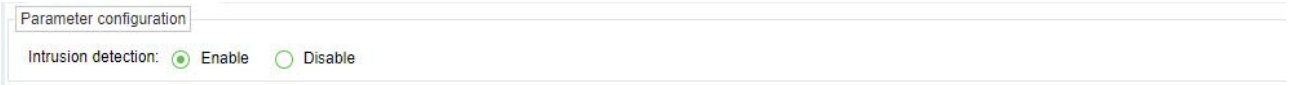


The following mainly explains the intelligent function configuration of ZKBio Sense series.

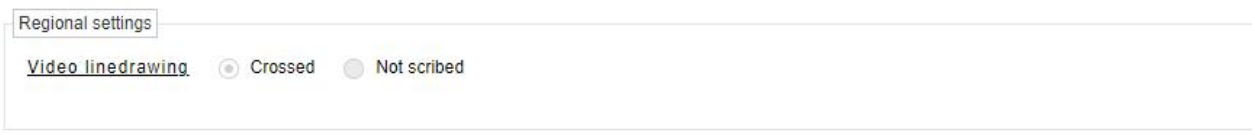
5.5.1.1 Intrusion Detection

Parameter Configuration

Configure to enable intrusion detection.



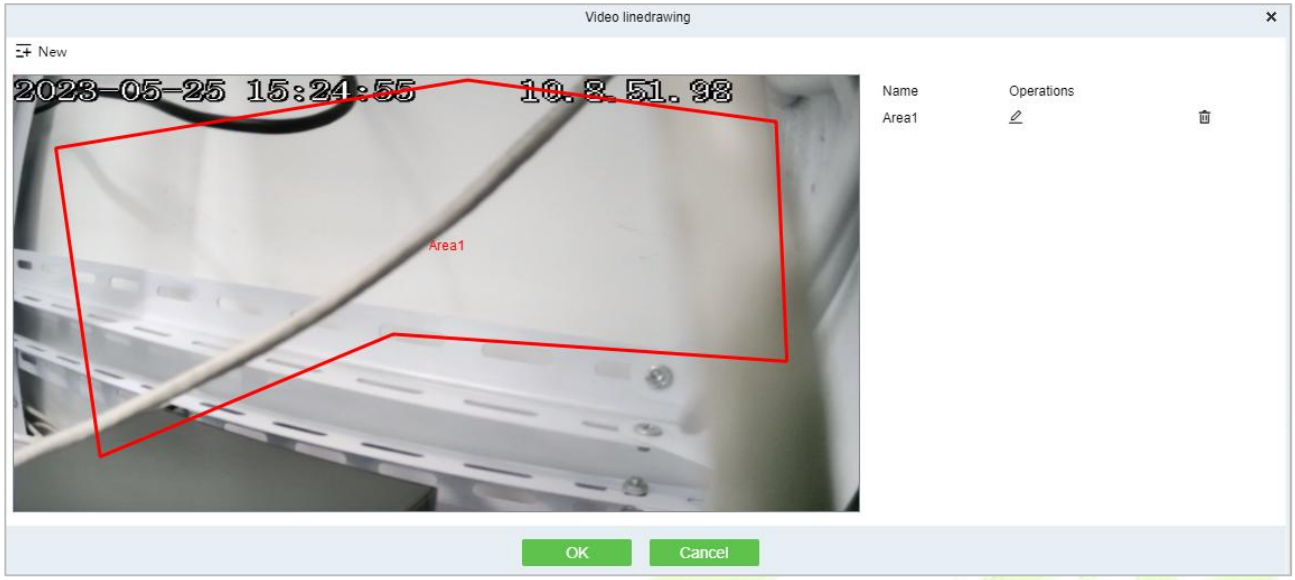
Regional Settings



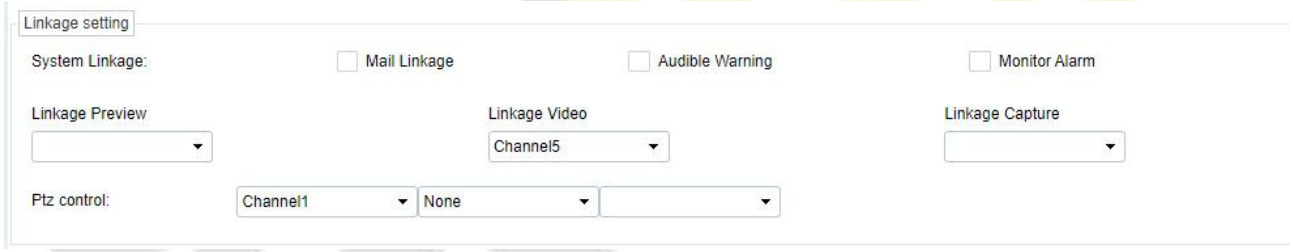
Crossed: Indicates that a line is currently drawn for this smart feature.

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

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

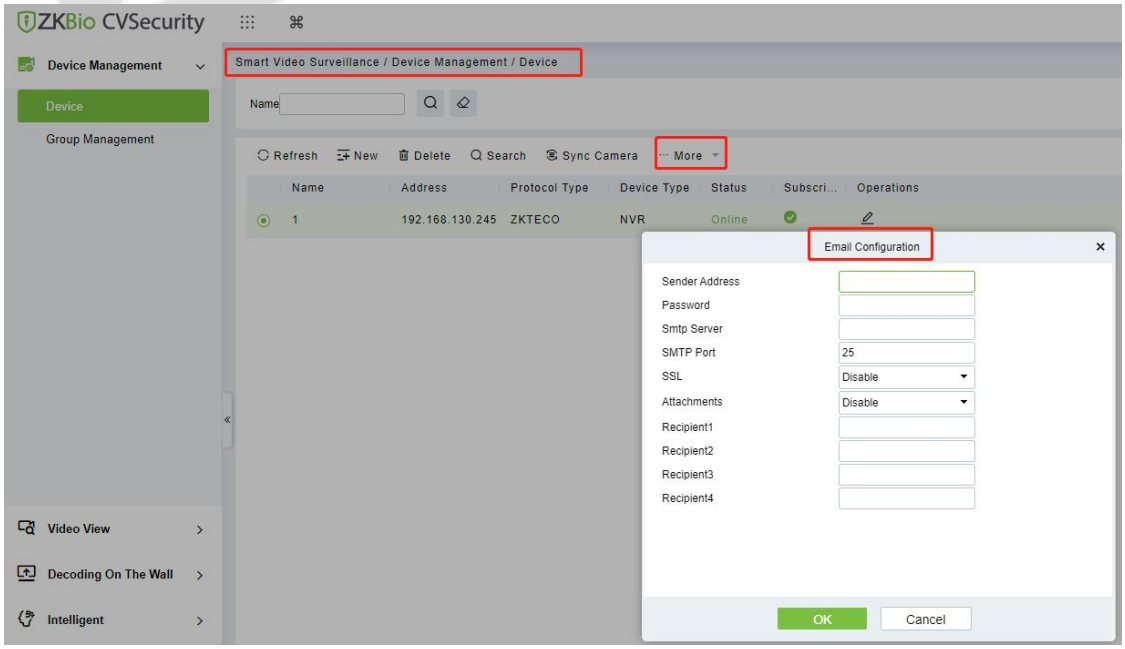


Linkage Setting



System Linkage:

a. Mail Linkage: After select the mail linkage, you need to go to Smart Video Surveillance > Device Management > Device, select the NVR. Click More>Email configuration, to set the sending server and recipient address.



b. Audible Warning: NVR's buzzer alarm.

c. Monitor Alarm: Display alarm information in the NVR.

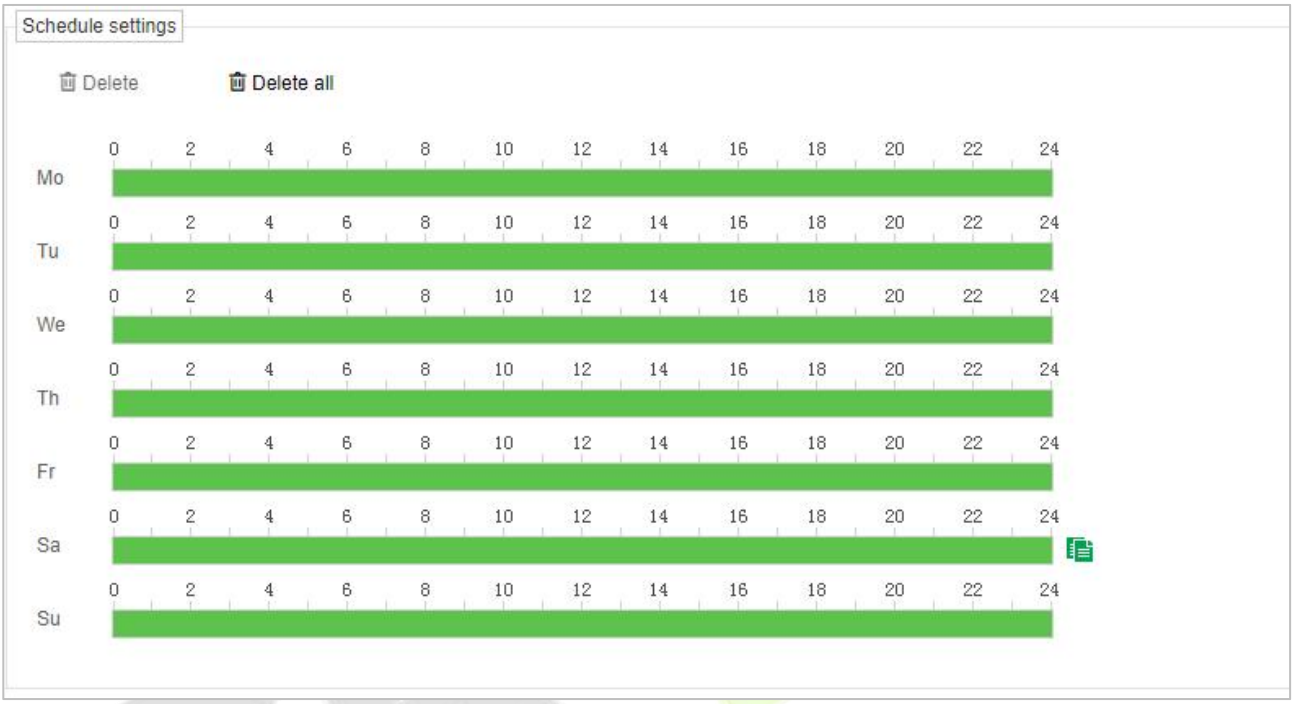
d. Linkage Preview: A preview of the linked camera is displayed in the NVR.

e. Linkage Record: Linkage to record.

f. Linkage Capture: Linkage to snapshot.

g. PTZ Control: The linkage PTZ executes the preset point and trajectory line.

Schedule Settings:



After configuring all the above functions, click **Save.**

5.5.1.2Perimeter Line

Please refer to Intrusion Detection setup.

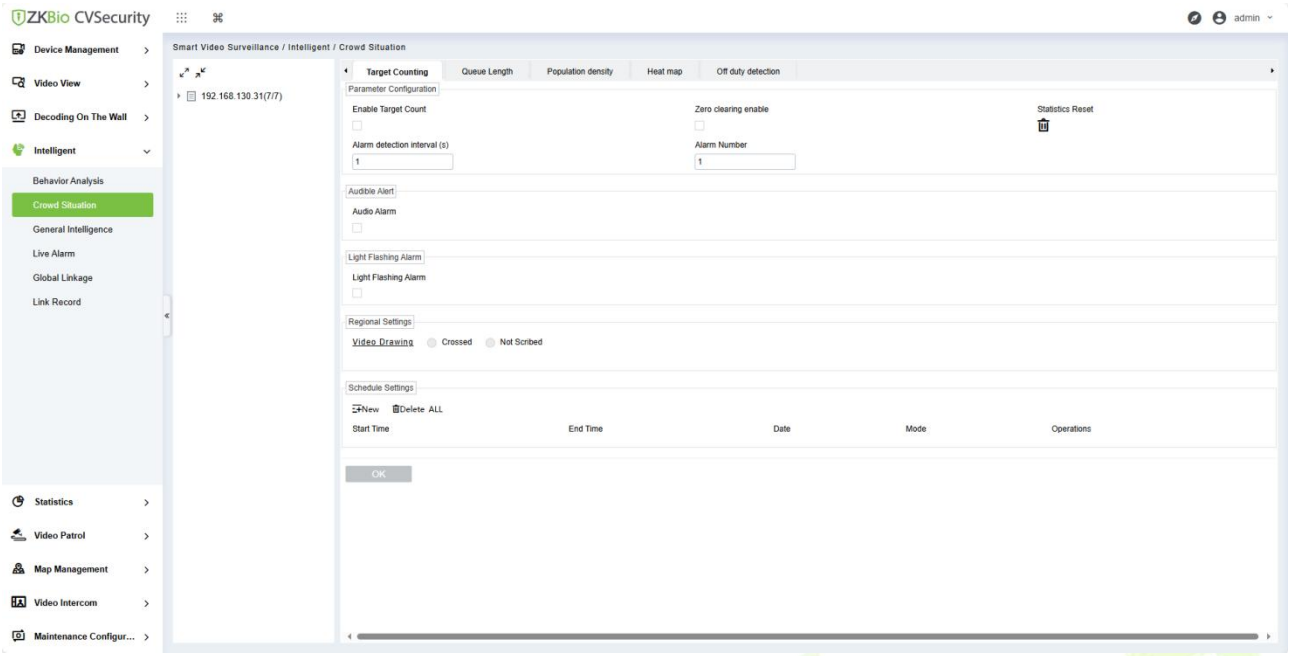
5.5.1.3Object Left

Please refer to Intrusion Detection setup.

5.5.2Crowd Situation

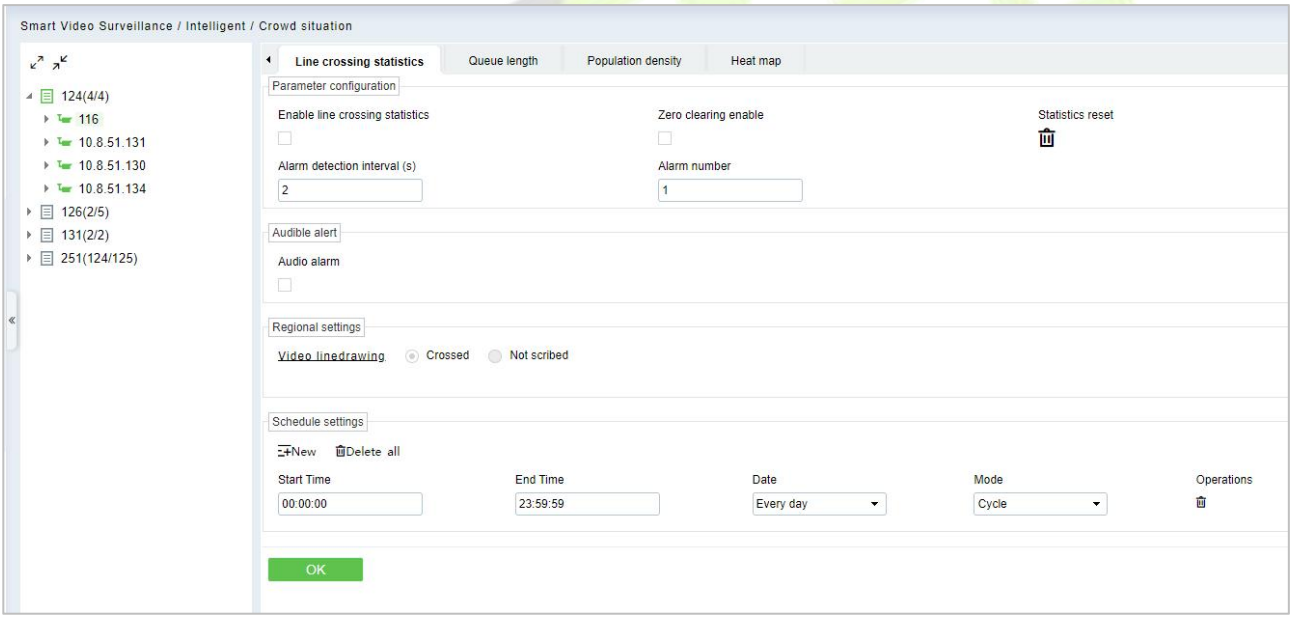
Configuration of intelligent functions for crowd situation of front-end cameras by ZKBio CVSecurity.

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

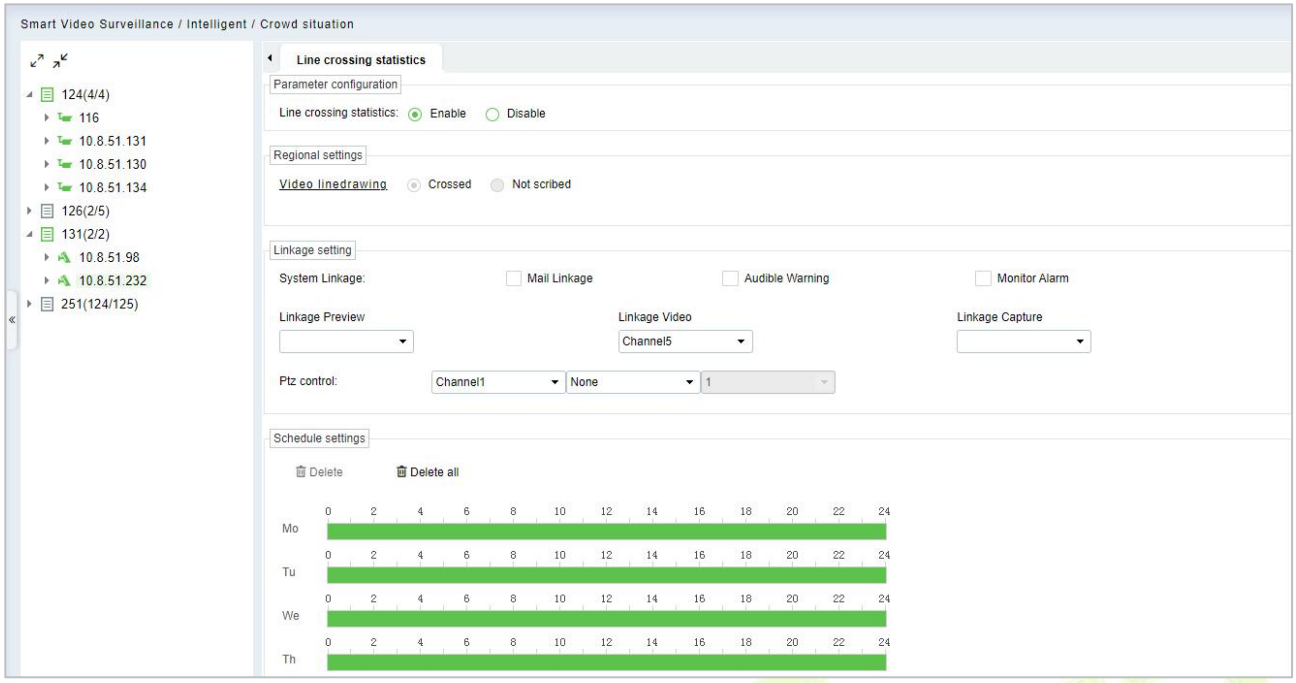


Step 1: Select the camera on the left and the software will automatically switch to the menu of smart features supported by that camera.

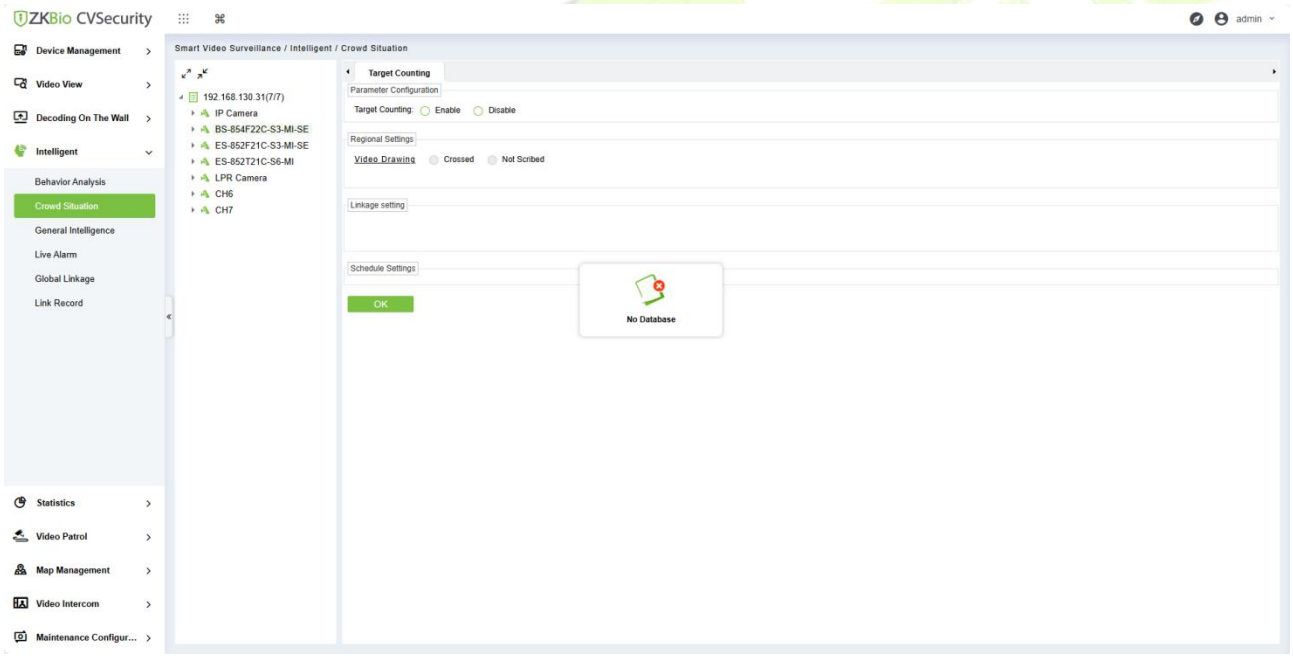
1) If it's Holowits branch device, after click, the page shown as below:



2) If it's ZKBio Sense device, after click , the page shown as below:



3) If the camera does not support intelligent functions, then after click, the page shown as below: No database.



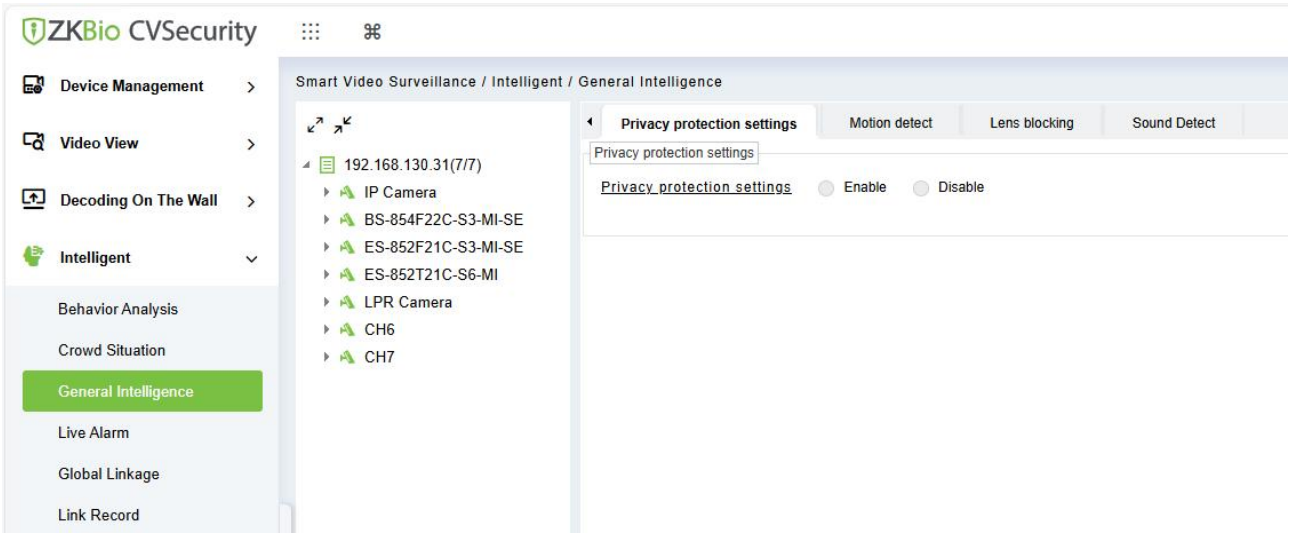
5.5.2.1 Line Crossing Statistics

Please refer to Intrusion Detection setup.

5.5.3 General Intelligence

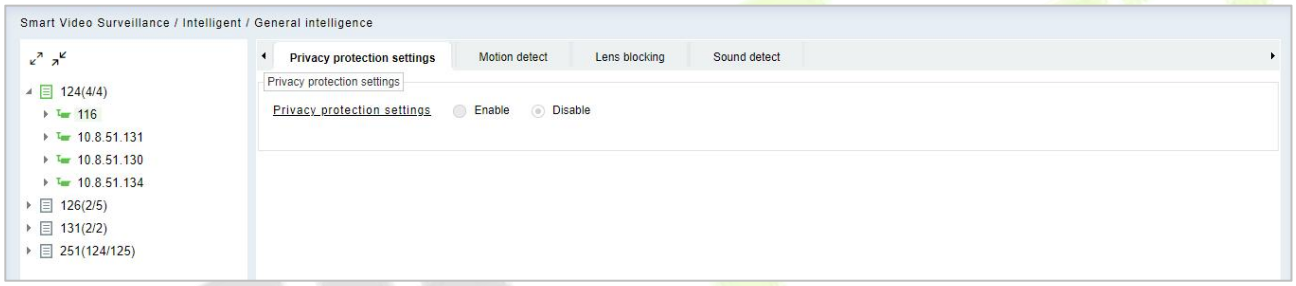
Configuration of general intelligence functions for front-end cameras by ZKBio CVSecurity.

Note: The default interface is part of Holowits' functionality. Different cameras have different intelligences, selecting the camera on the left will display the intelligences according to what the camera has to offer.

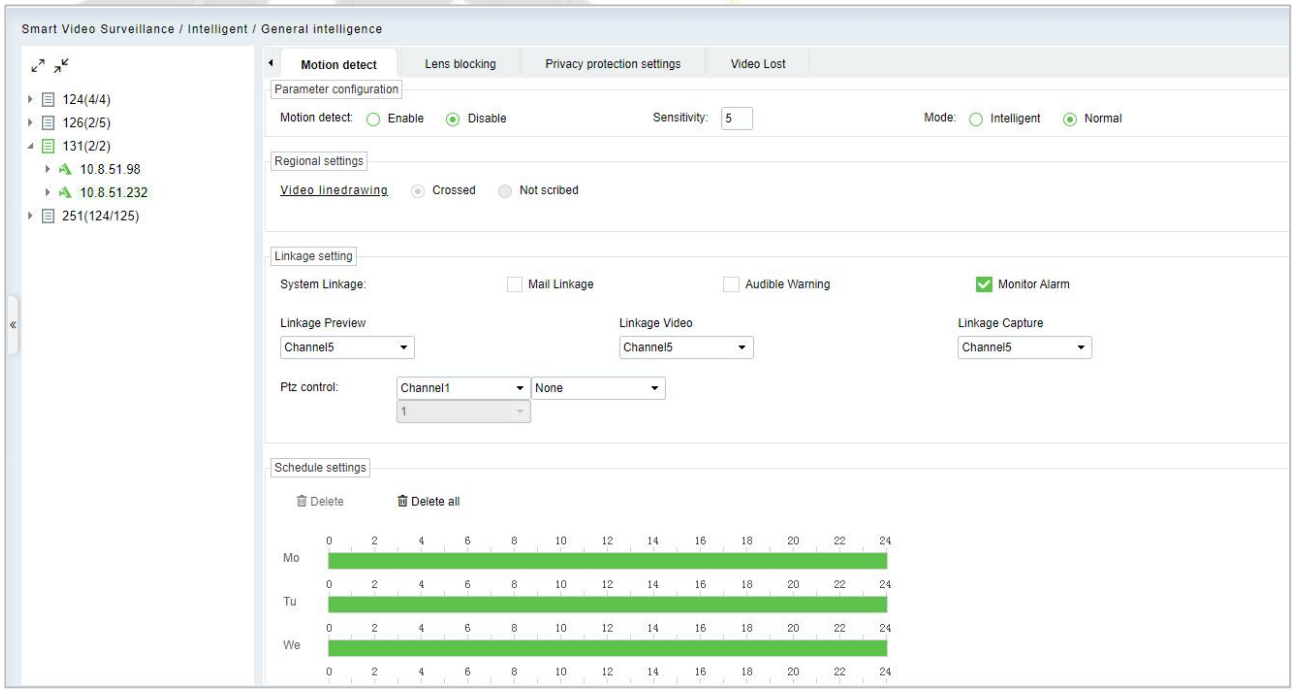


Step 1: Select the camera on the left and the software will automatically switch to the menu of smart features supported by that camera.

1) If it's Holowits branch device, after click, the page shown as below:



2) If it's ZKBio Sense device, after click, the page shown as below:



5.5.3.1 Motion Detection

Please refer to Intrusion Detection setup.

Parameter Configuration:

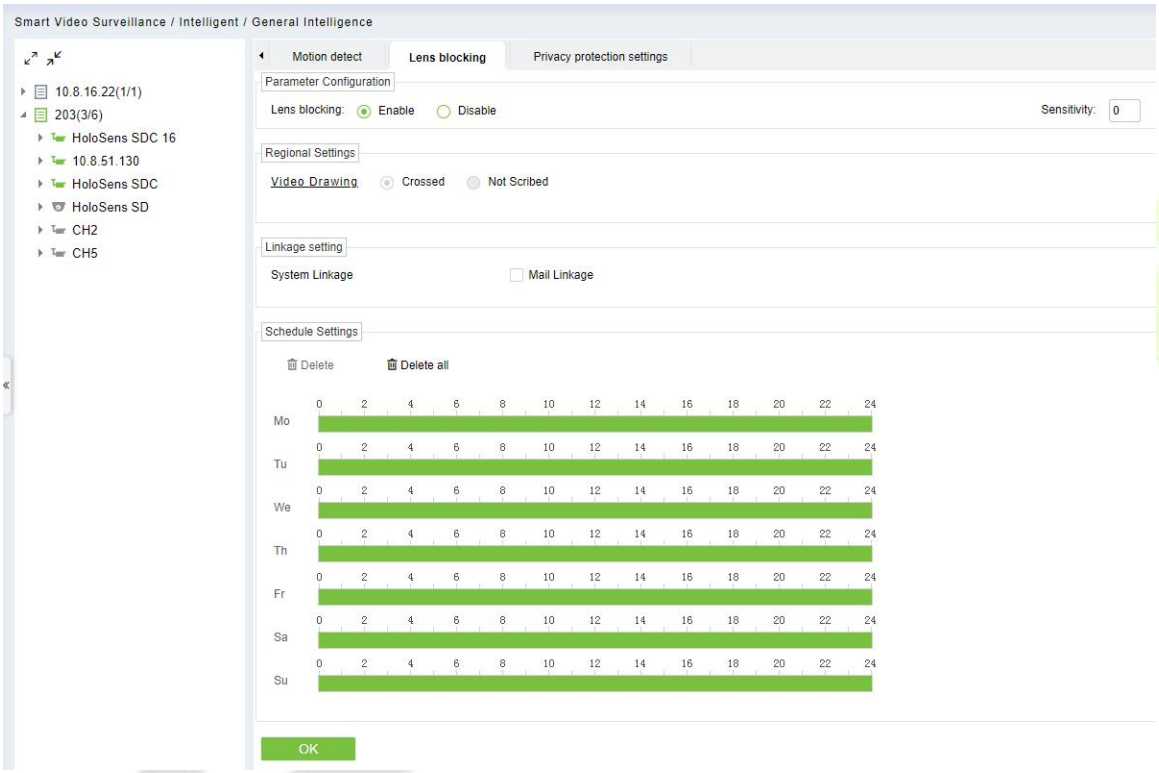
Sensitivity: Detection sensitivity.

Mode: Intelligent: Can distinguish between human or vehicles.

Normal: No distinction between human and vehicles.

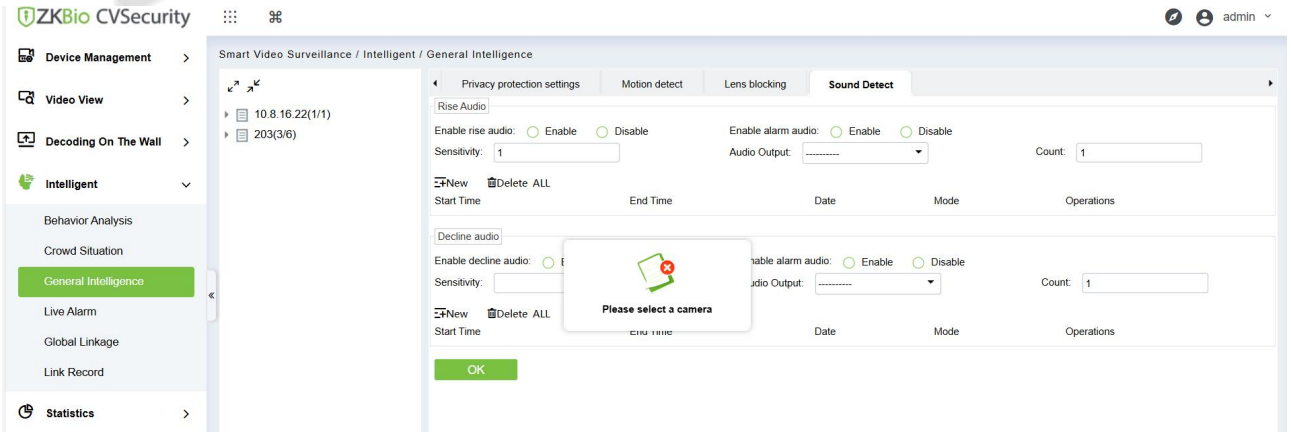
5.5.3.2Lens Blocking

Lens Obstruction Alarm; after clicking **Enable** button to enable, please click **Video Drawing** to configure the detection area.



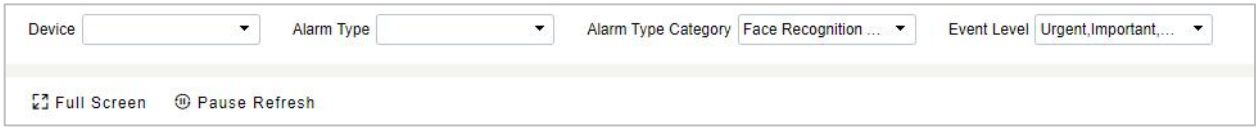
5.5.3.3Sound Detect

Sound diagnostics; this feature is only available with Holowits Camera.



5.5.4Live Alarm

Real-time video alarm monitoring.



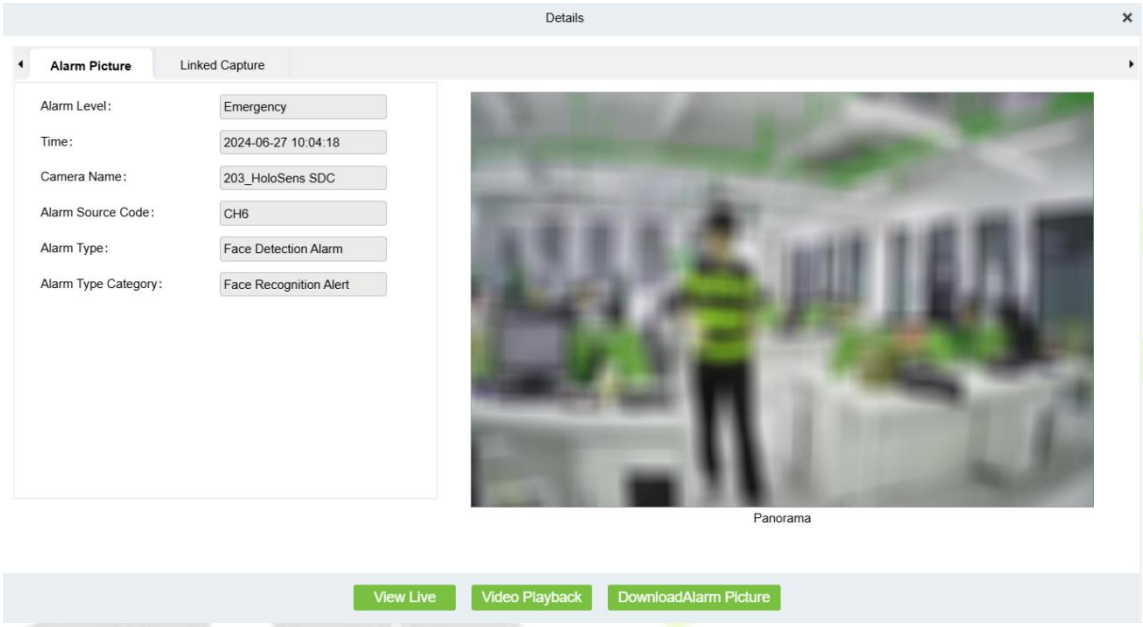
Full Screen

View the video in the full screen.

Pause Alarm

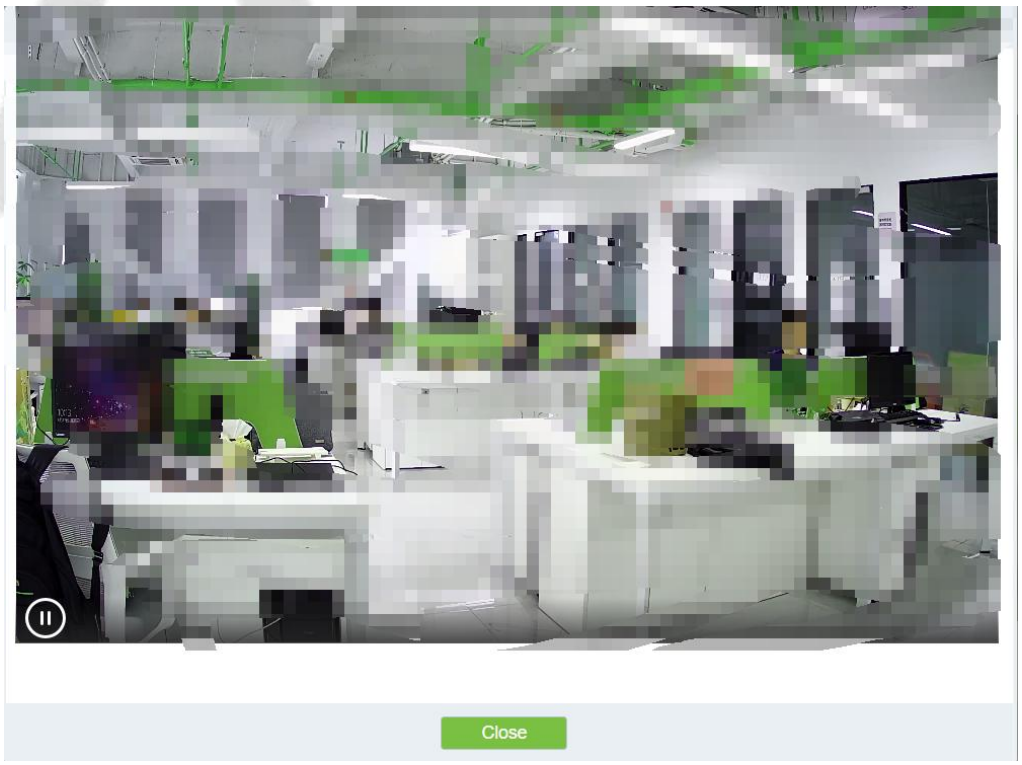
This function will help you to pause the alarm.

Double-click the alarm card to view the alarm details, as shown in the figure below.



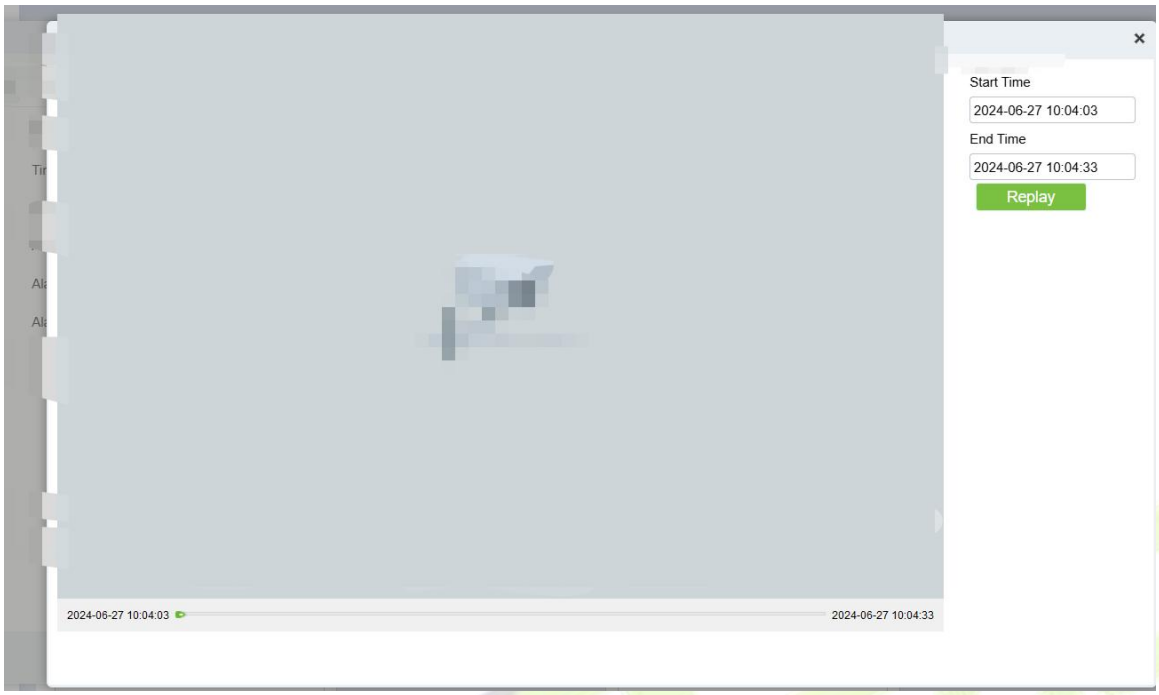
●View Live

Click on the **Live View** button to view the live video.



● Video Playback

Click the **Video Playback** button to view the alarm playback in real time.

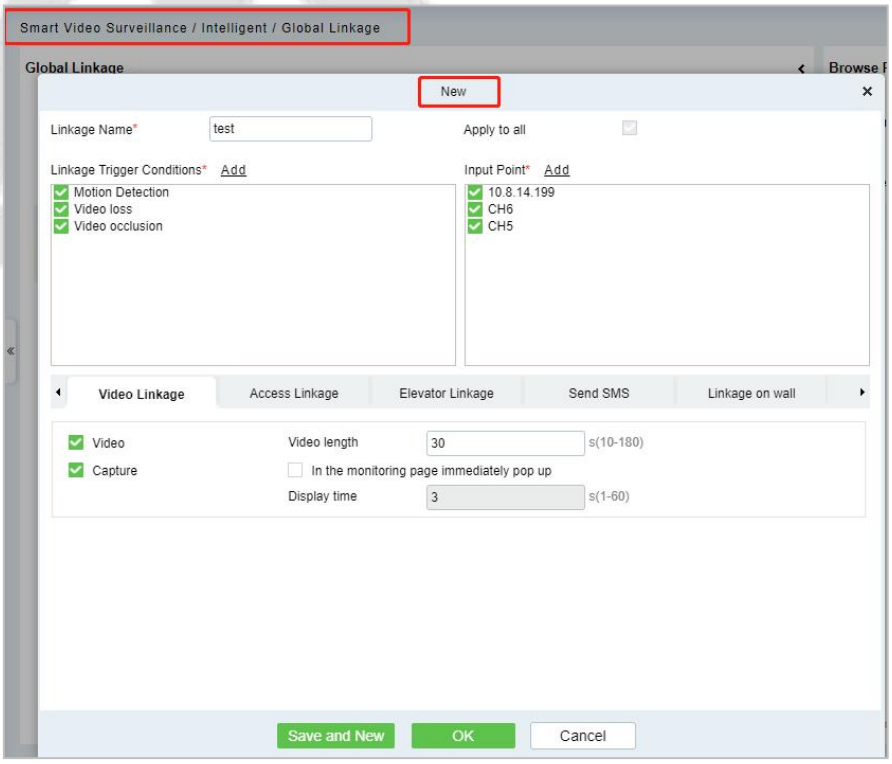


● Download Alarm Picture

Click **Download Alarm Picture** and the browser will download the picture automatically.

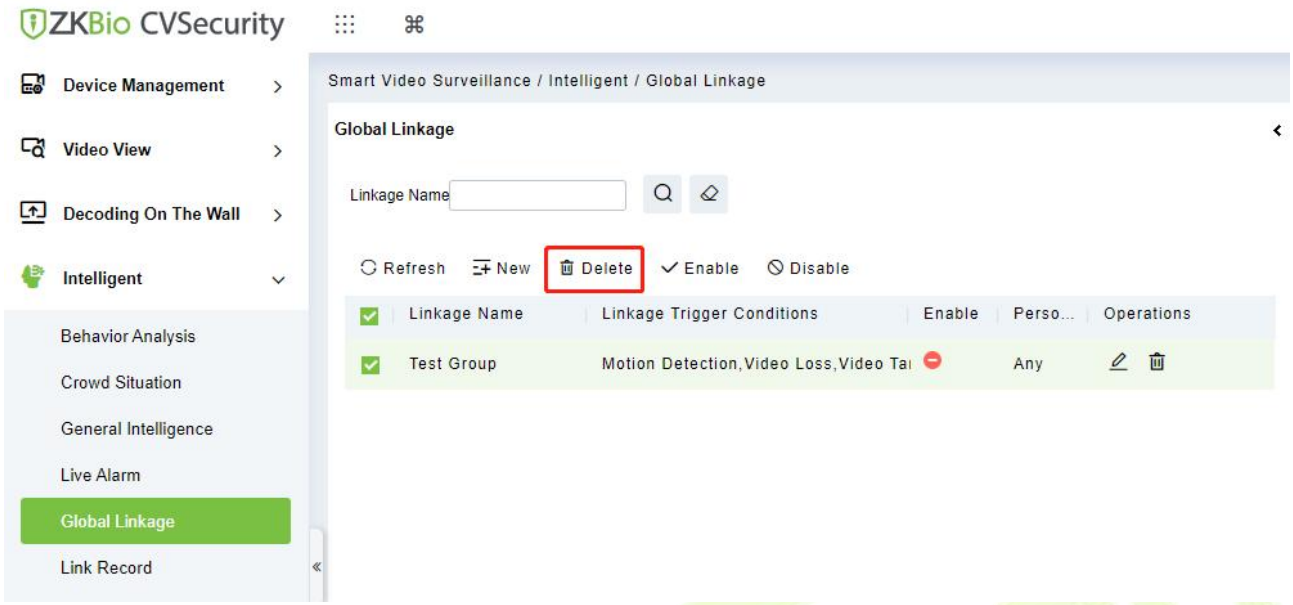
5.5.5 Global Linkage

Go to **Smart Video Surveillance** > **Intelligent** > **Global Linkage**, click New to set the video linkage.



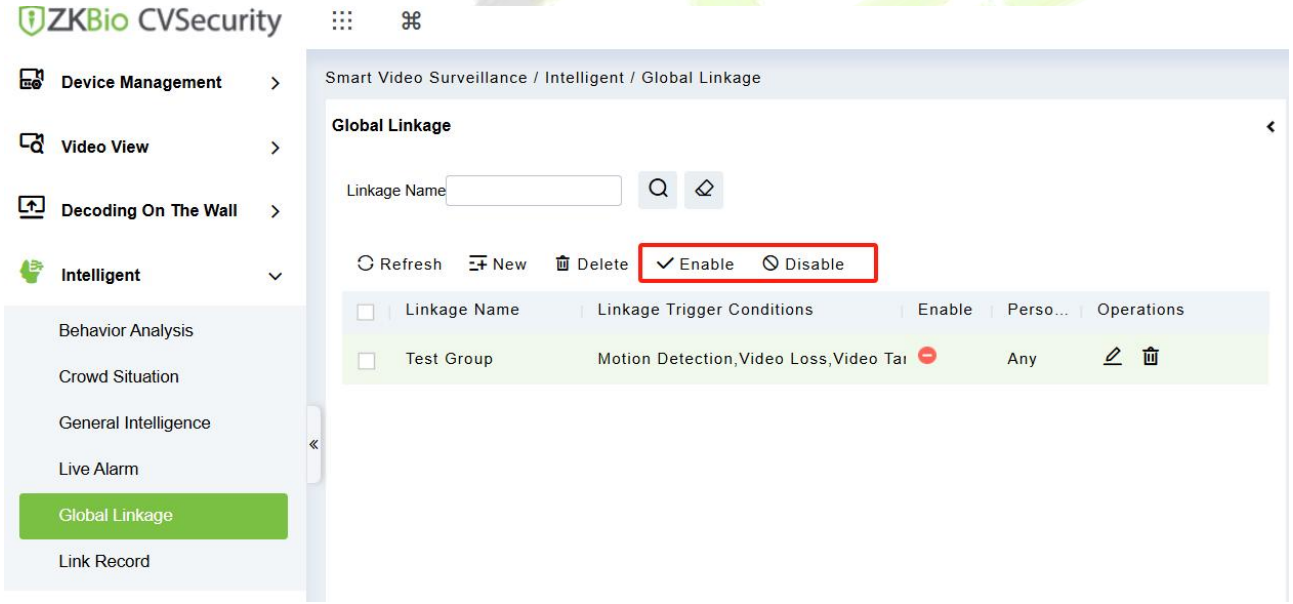
5.5.5.1Delete

Select the **Linkage Name**, click **Delete**, and click **OK** to delete the linkage details.



5.5.5.2Enable/Disable

Select the **Linkage Name**, click **enable/disable** to either enable or disable the linkage details.

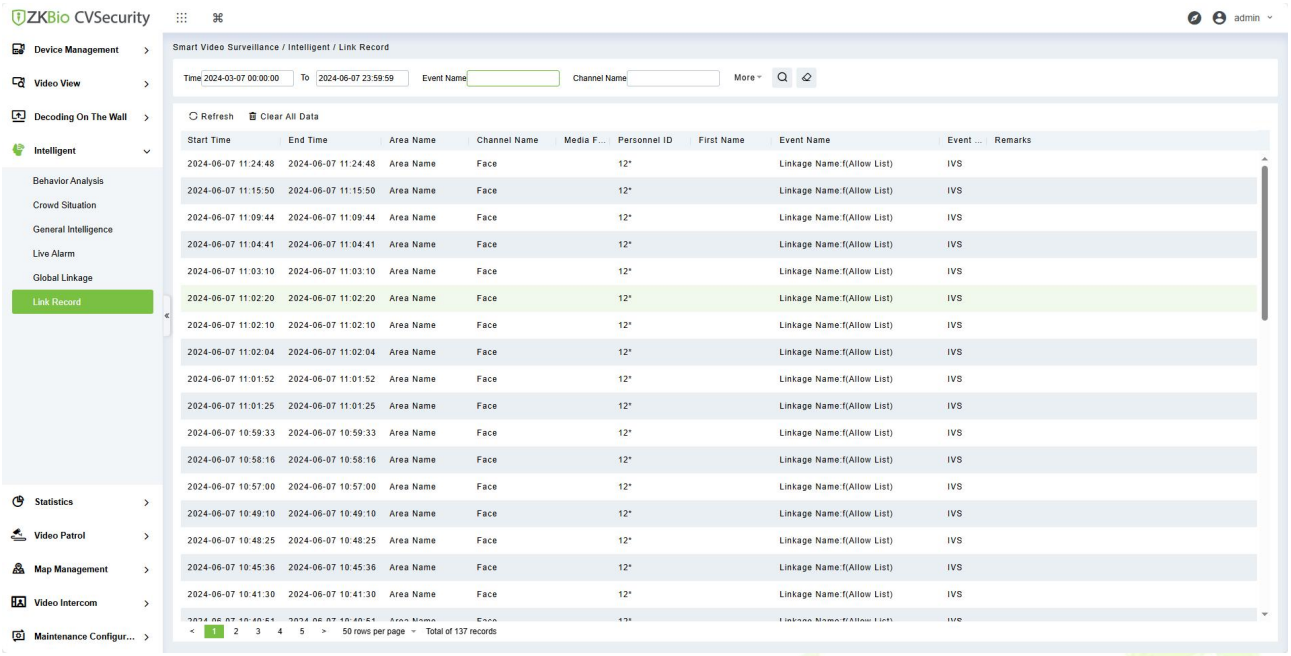


5.5.6Link Record

5.5.6.1Clear All Data

● Operating Steps:

Step 1: Click **Intelligent > Link Records > Clear All Data** to view clear all records:



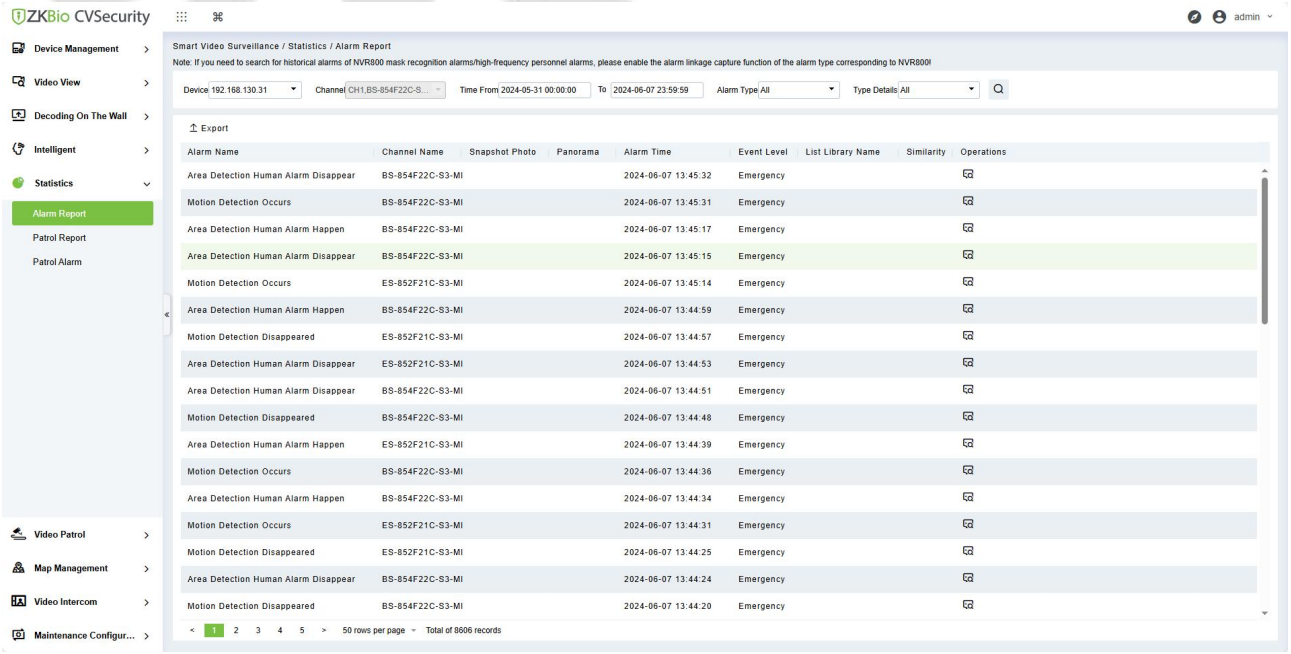
Step 2: Click **Clear All Data** to pop up prompt and click **OK** to clear all records.

5.6 Statistics

5.6.1 Alarm Report

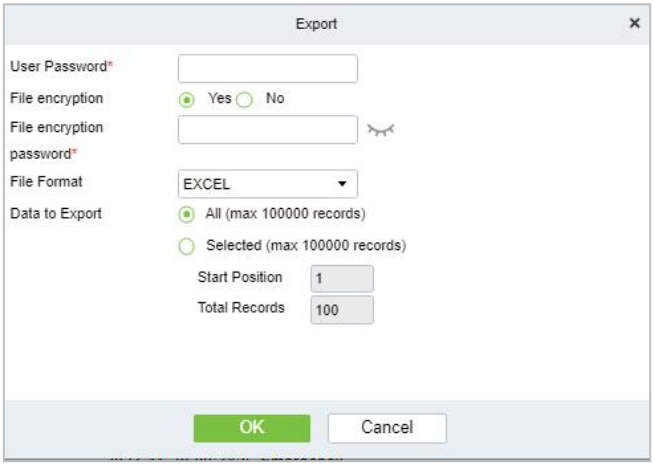
Click **Statistics** > **Alarm Report** then select Alarm Type.

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.



5.6.1.1 Export

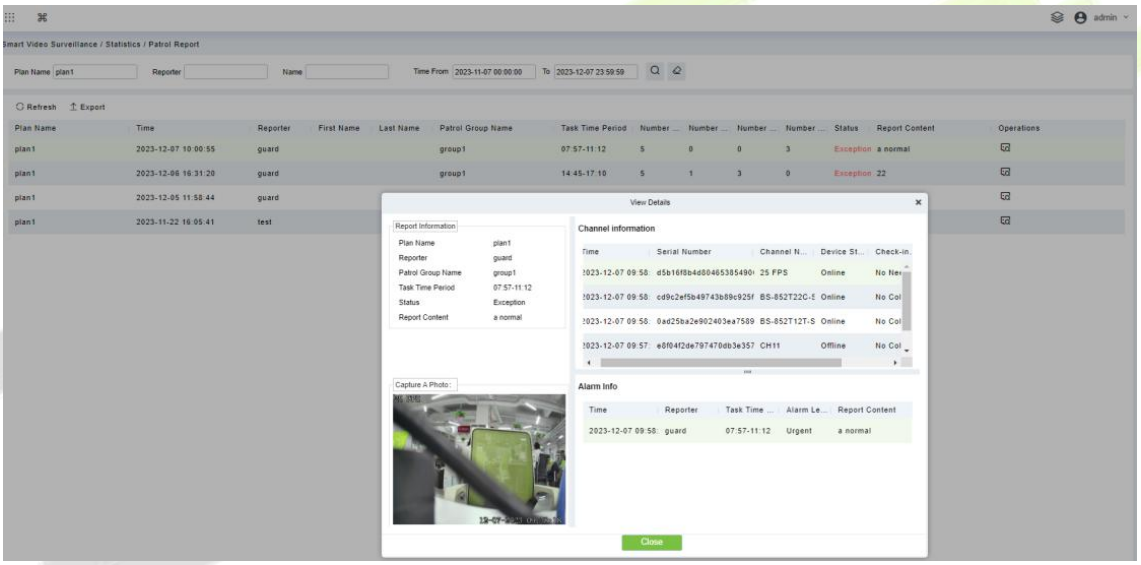
Export selected personal information in the area; need enter user password and file encryption; you can export Excel, PDF, CSV or TXT format; Export up to 10000 pieces of data at once.



5.6.2Patrol Report

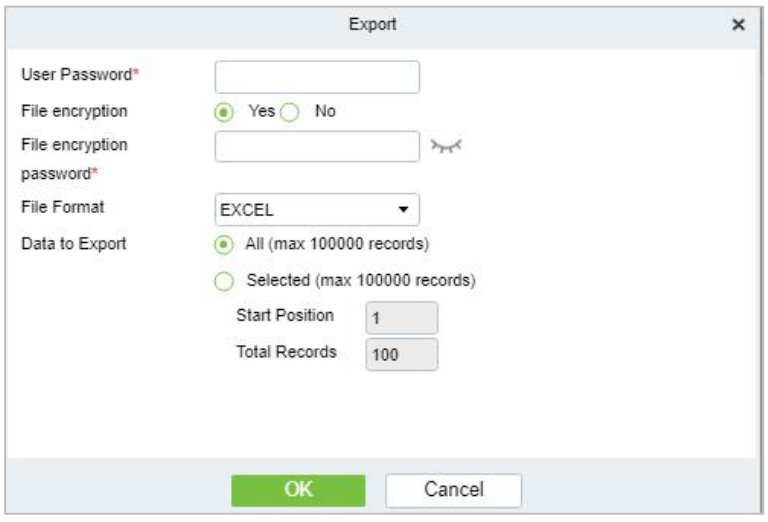
Click Statistics > Patrol Report, then select Plan Name.

In this module, by viewing detailed details, you can see the corresponding channel camera serial number and abnormal captured images.



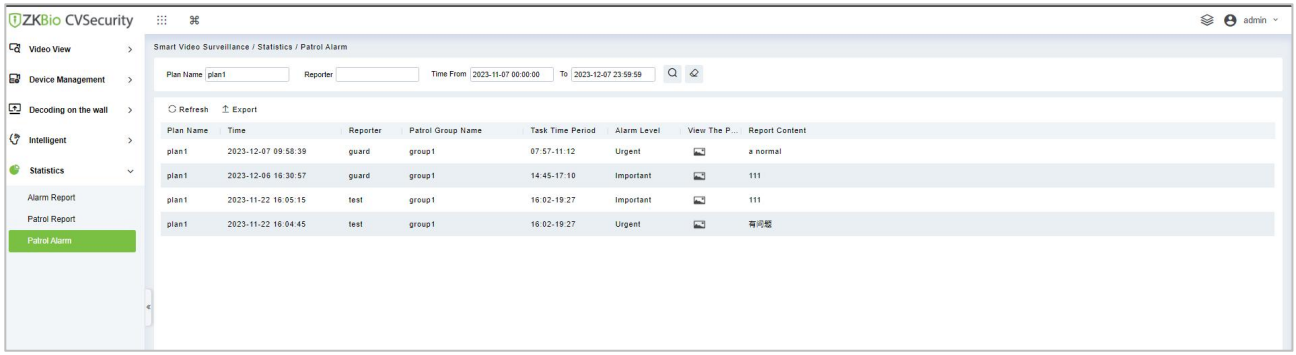
5.6.2.1Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.



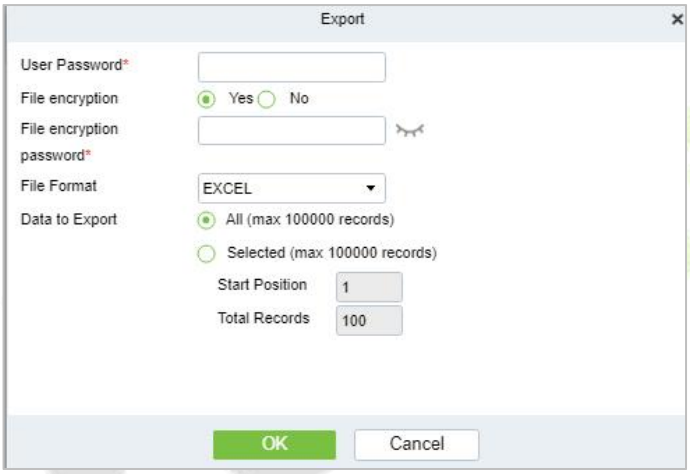
5.6.3 Patrol Alarm

Click **Statistics** > **Patrol Alarm**, then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.



5.6.3.1 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.



5.7 Video Patrol

Click **Video Patrol** > **Patrol Group**.

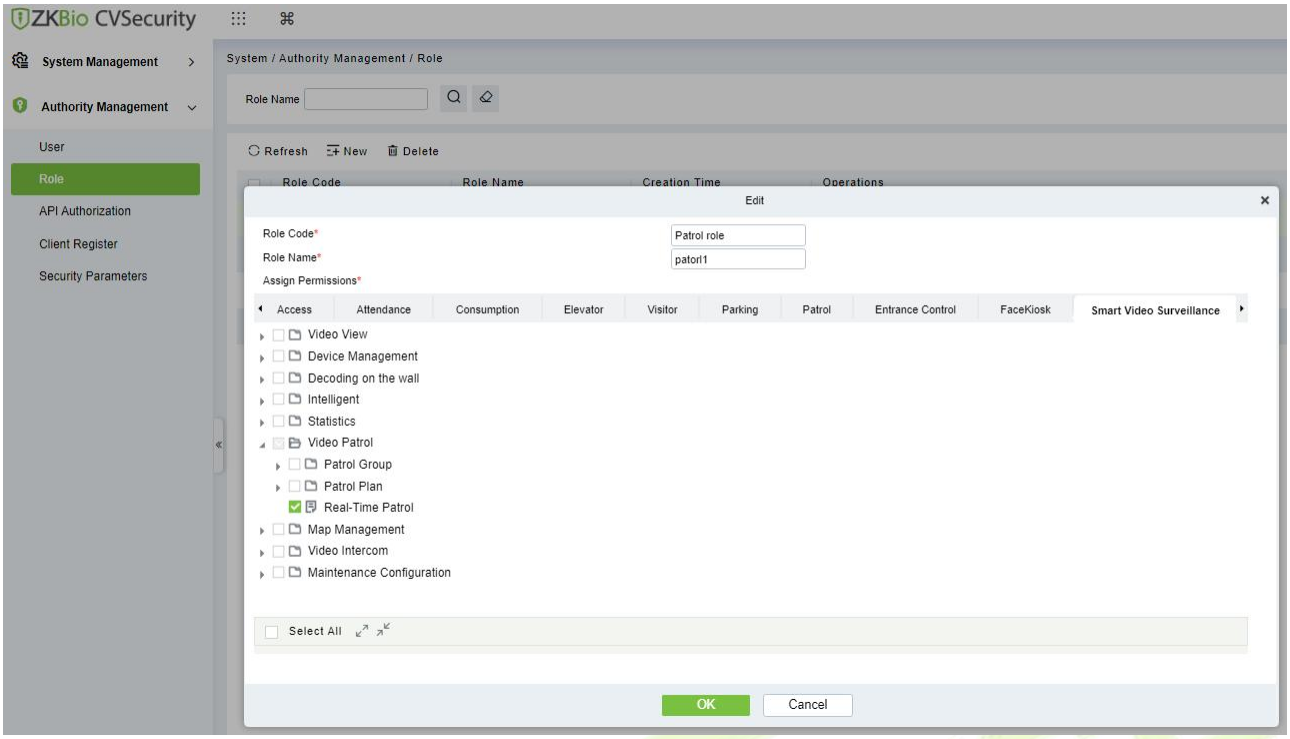
On the preset path, you can check the punch-in by a real-time preview of the camera remotely to achieve the same patrol task as the traditional punch-in effect.

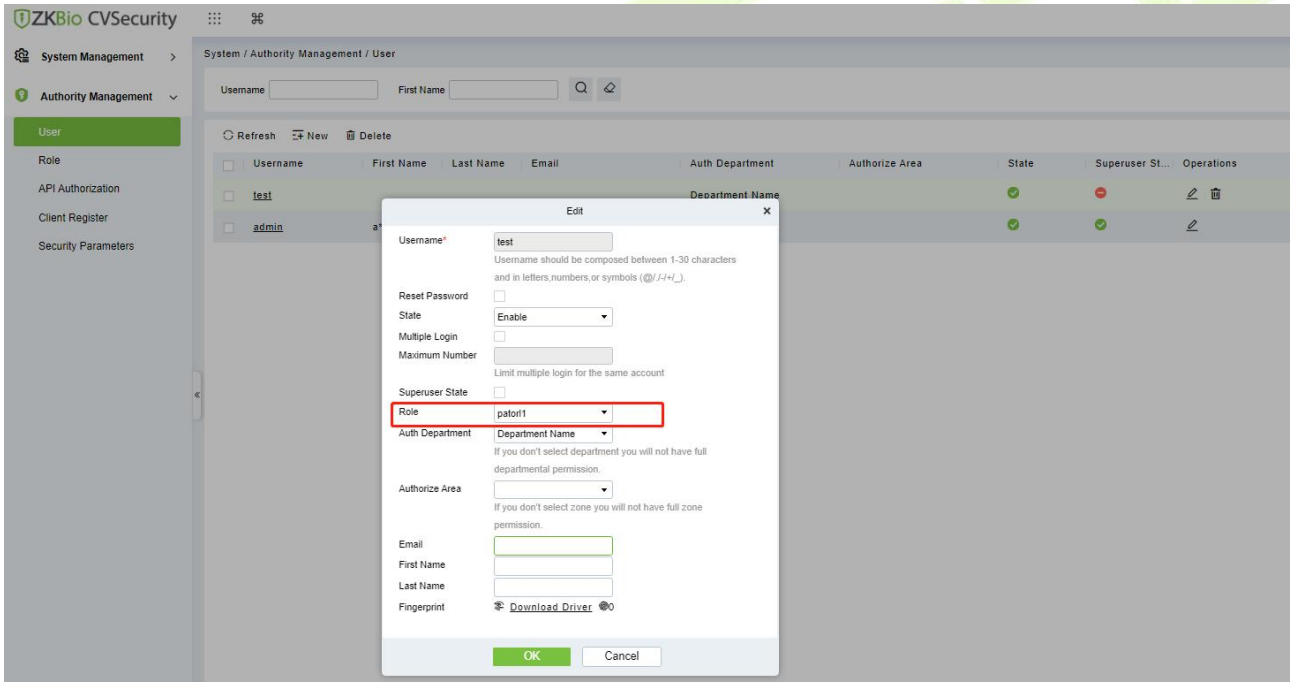
5.7.1 Patrol Group

Create a patrol group to add patrol personnel.

Note:

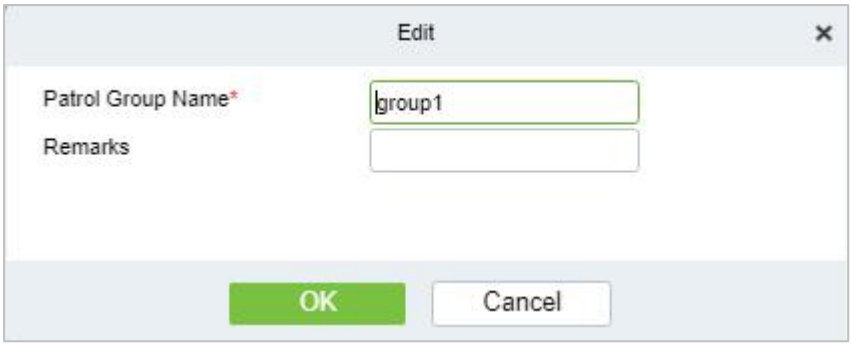
1. Please go to System >Authority Management >Role to add the role group, Assign video patrol permissions.
2. Create the System user and add in the patrol role.





5.7.1.1 New

Click **Video Patrol> patrol group> New** to enter the new editing interface:

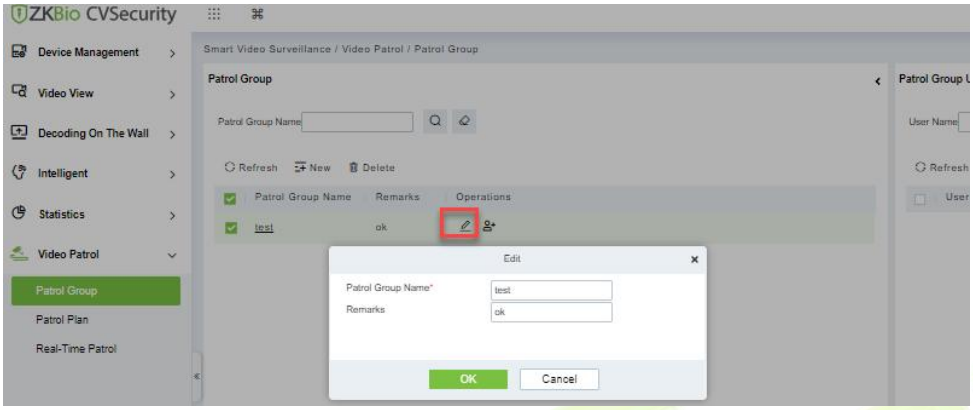


Patrol Group Name: Enter the name of the patrol group for easy searching and management non-repeatable.

Remarks: Text notes of the patrol group.

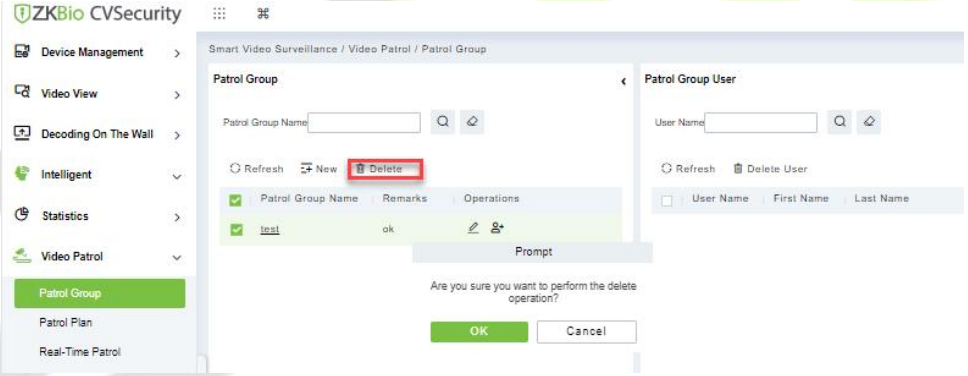
5.7.1.2Edit

Select the edit patrol group name and click edit icon button to edit the required details and click "OK" to submit.



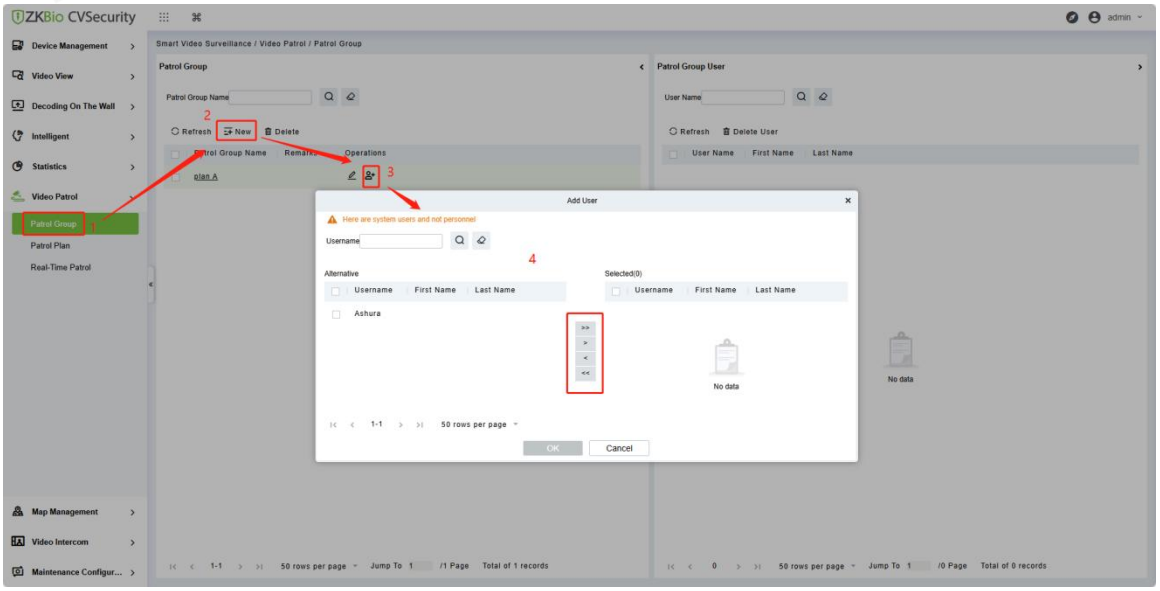
5.7.1.3Delete User

Select the Username and click this button to delete it.



5.7.1.4Add Patrol Group User

In the patrol group list, click Add User to enter and select to add group members.

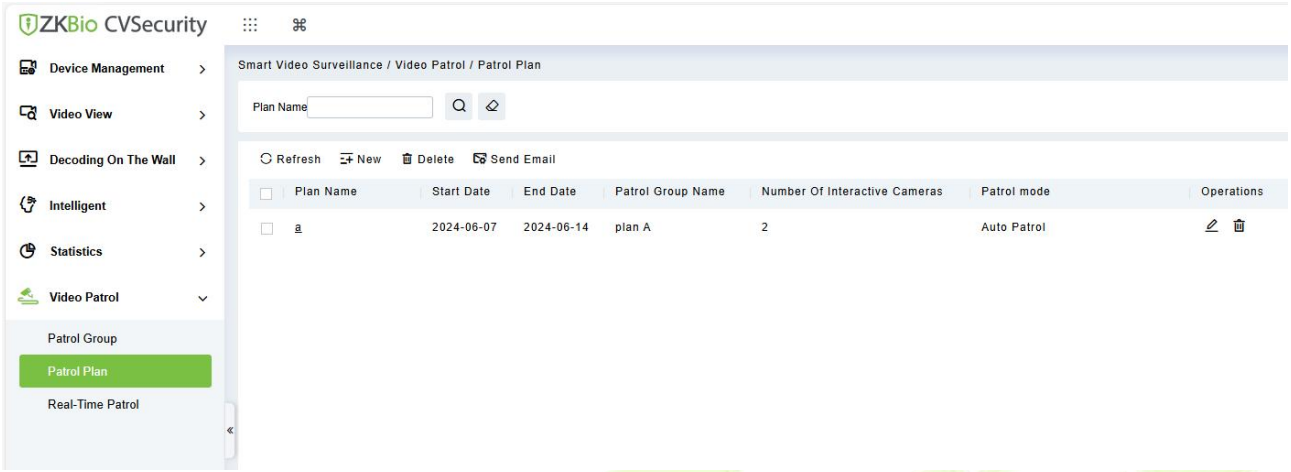


Select the required patrol users and click the OK button to complete the addition. The added users will be displayed in the group member list on the right.

Note: Patrol users are users of the system. For adding users to the system, please refer to Adding Users.

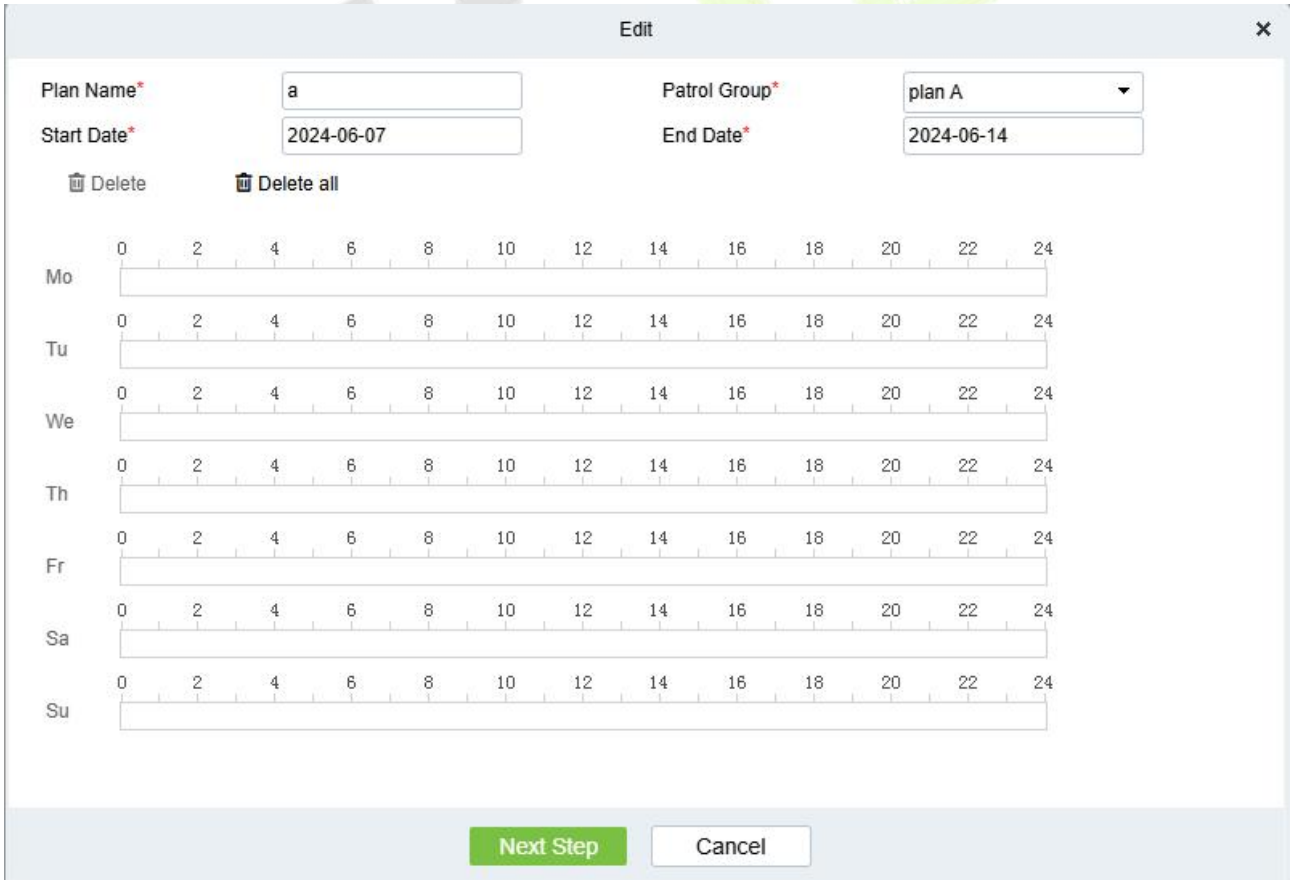
5.7.2Patrol Plan

Set a patrol plan for the patrol team.



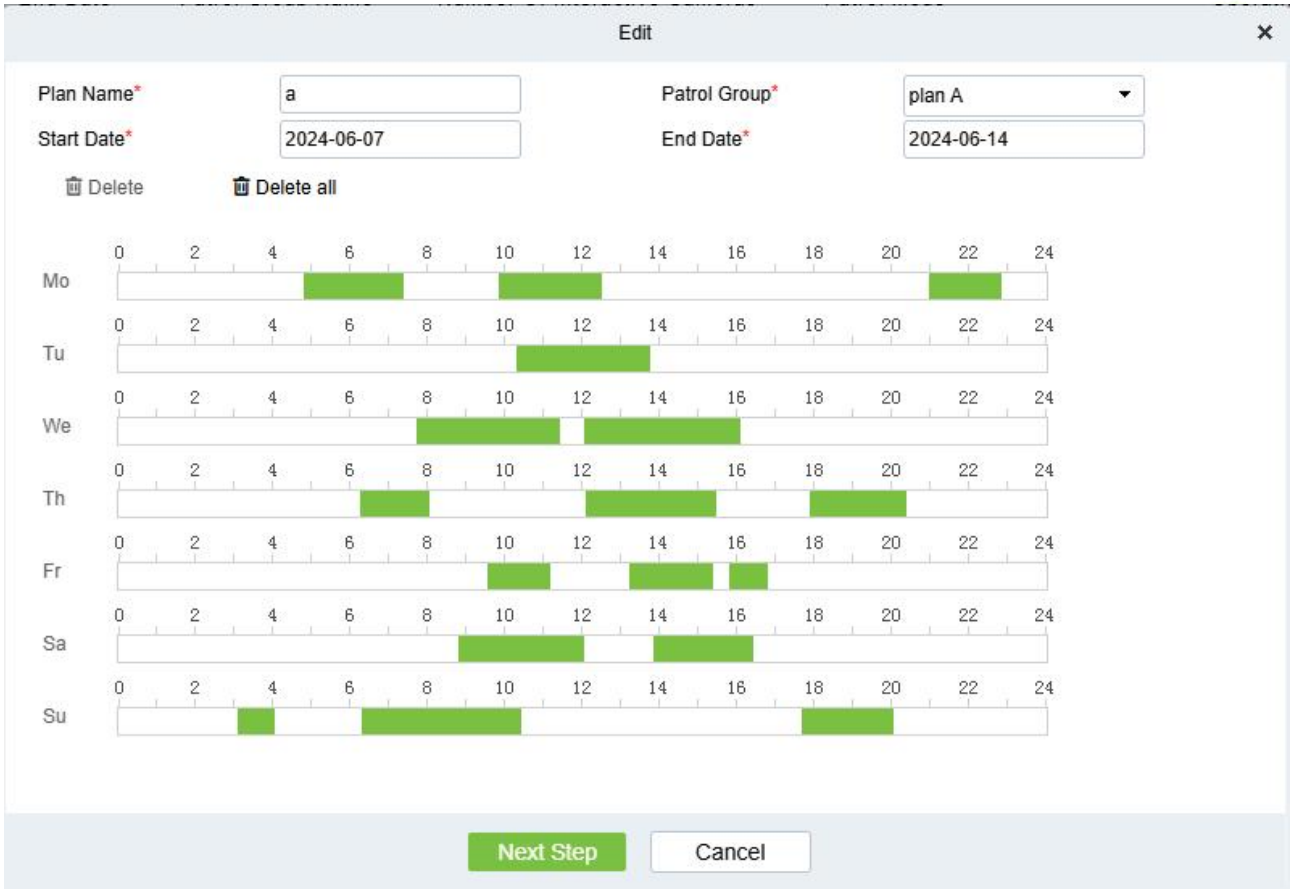
5.7.2.1New

Click **Video Patrol**> **Patrol Plan**> **New** to enter the new editing interface:

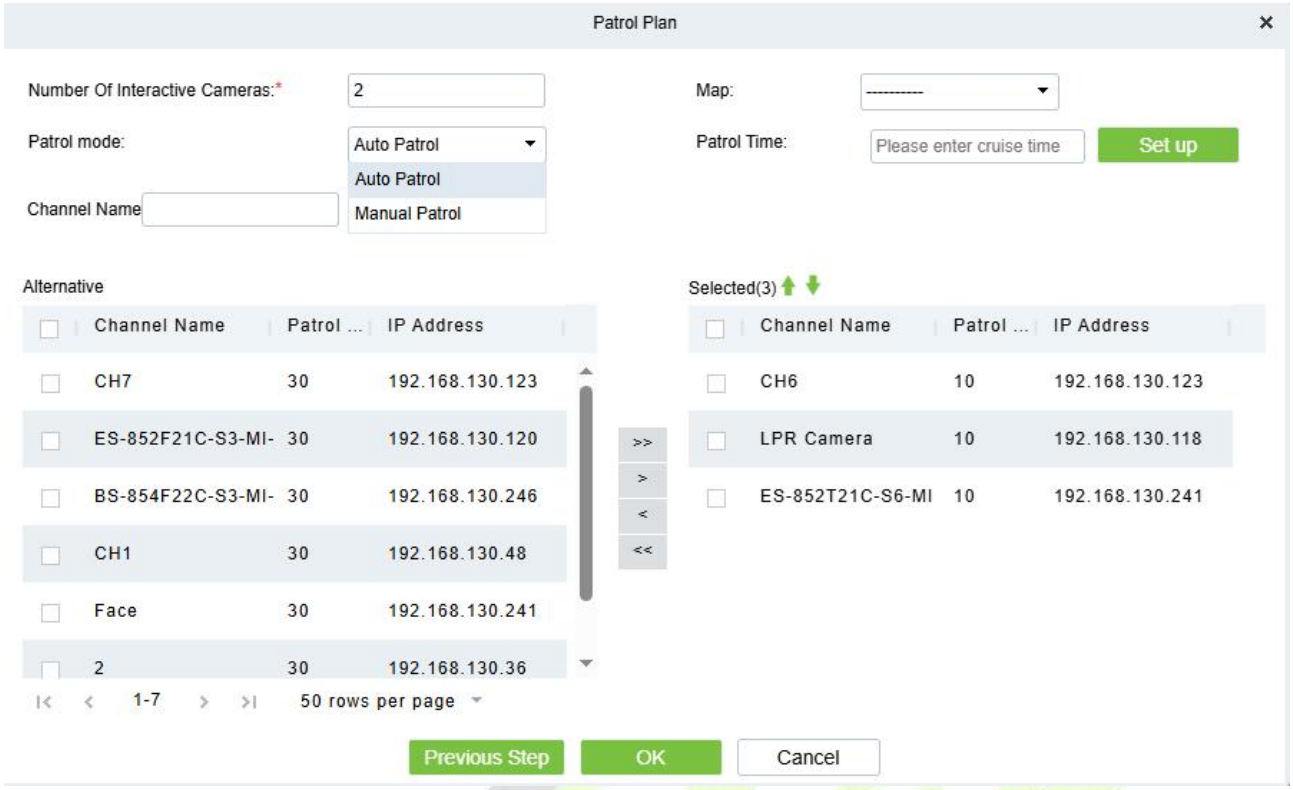


● The fields are described as follows:

Parameters	Instructions
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.



After editing this page, click Next to enter the camera selection interface:



Number of interactive Cameras: Set the number of cameras that need to be chick-in, (like "3" means that Chick-in must be completed on 3 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.

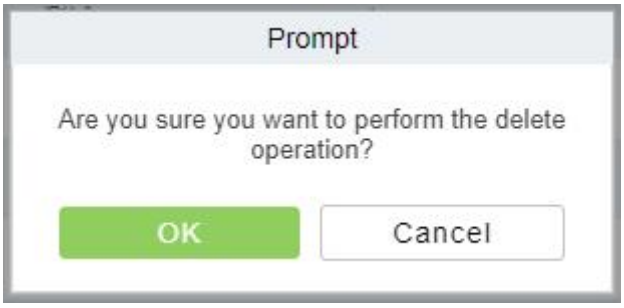
Note:

(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.The path is Service Center> Map Center>Map Config.

5.7.2.2Delete

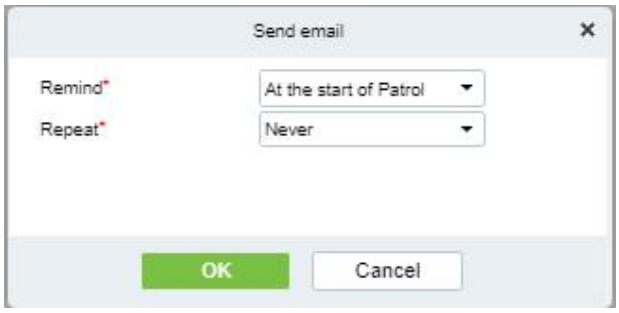
Select the Patrol Plan to be deleted and click the **Delete** button



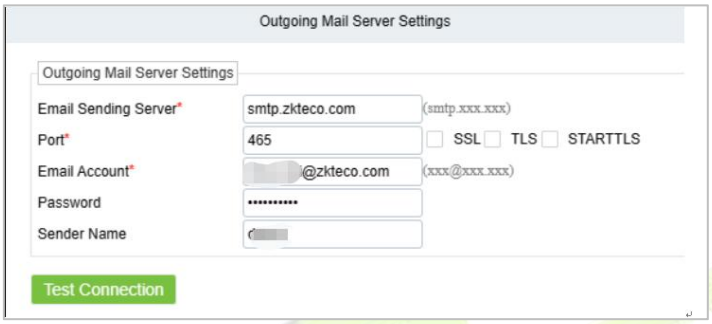
Note: Ongoing or pause plans cannot be deleted, please complete the plan first.

5.7.2.3Send Email

Select Send email button, set remind information and repetitions.

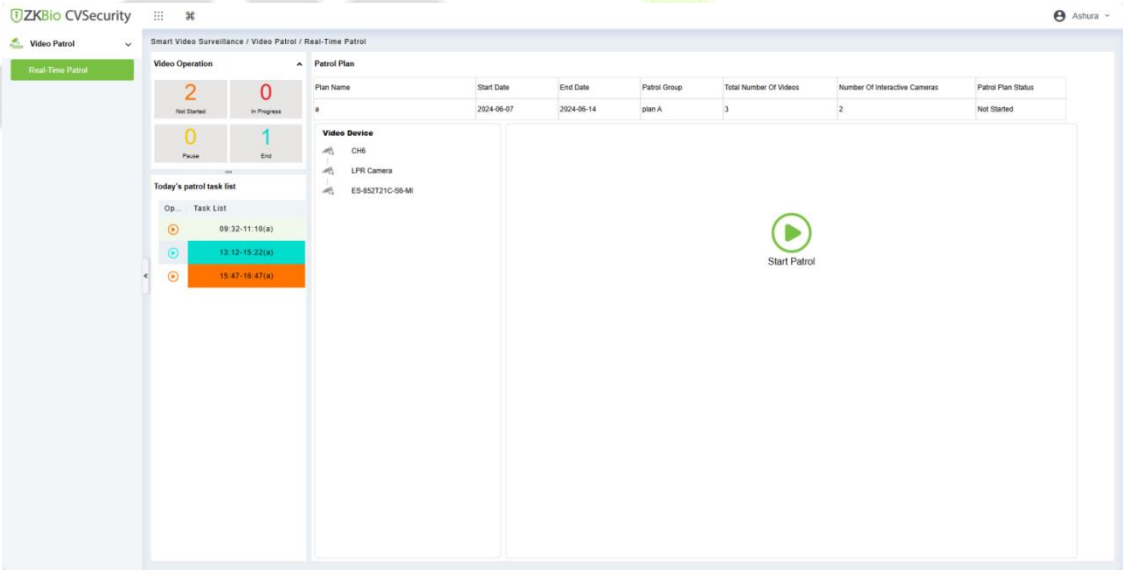


Note: Email outgoing configuration requires System Management ->Email configuration ->Outgoing Mail Server Settings.



5.7.3Real-Time Patrol

Click **Video Patrol** > **Real-time Patrol,** Online patrols are only available if the patrolman is logged into the system.



- Video Operation:

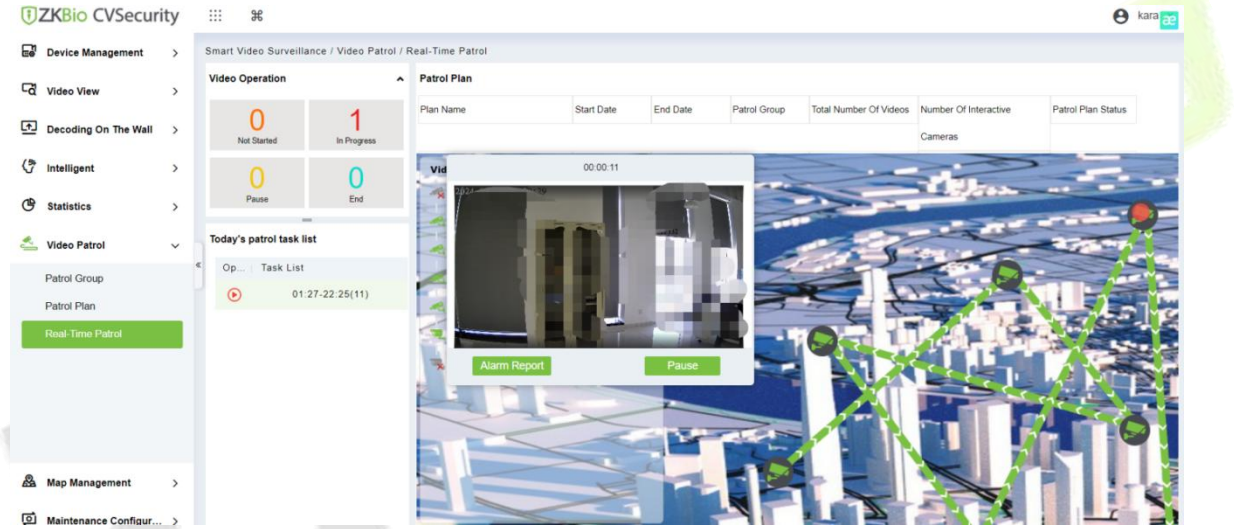
View different states of the Patrol plan.

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:

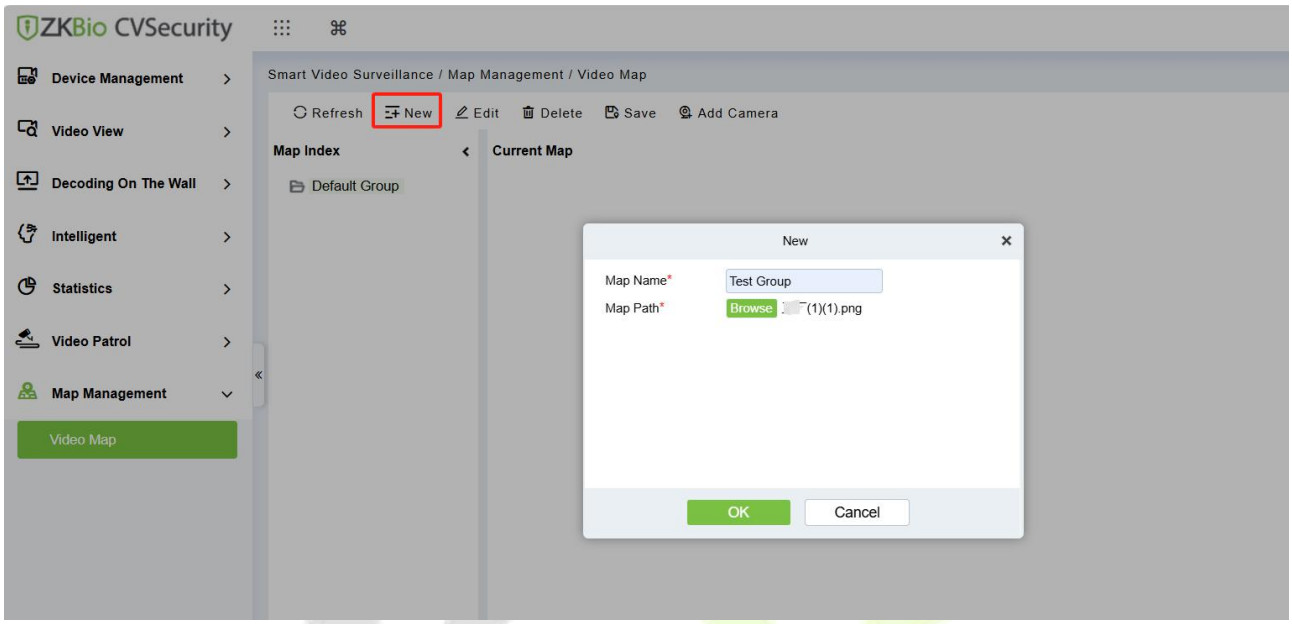
When the camera is patrolling, the floating window on the map will display real-time images.

5.8 Map Management

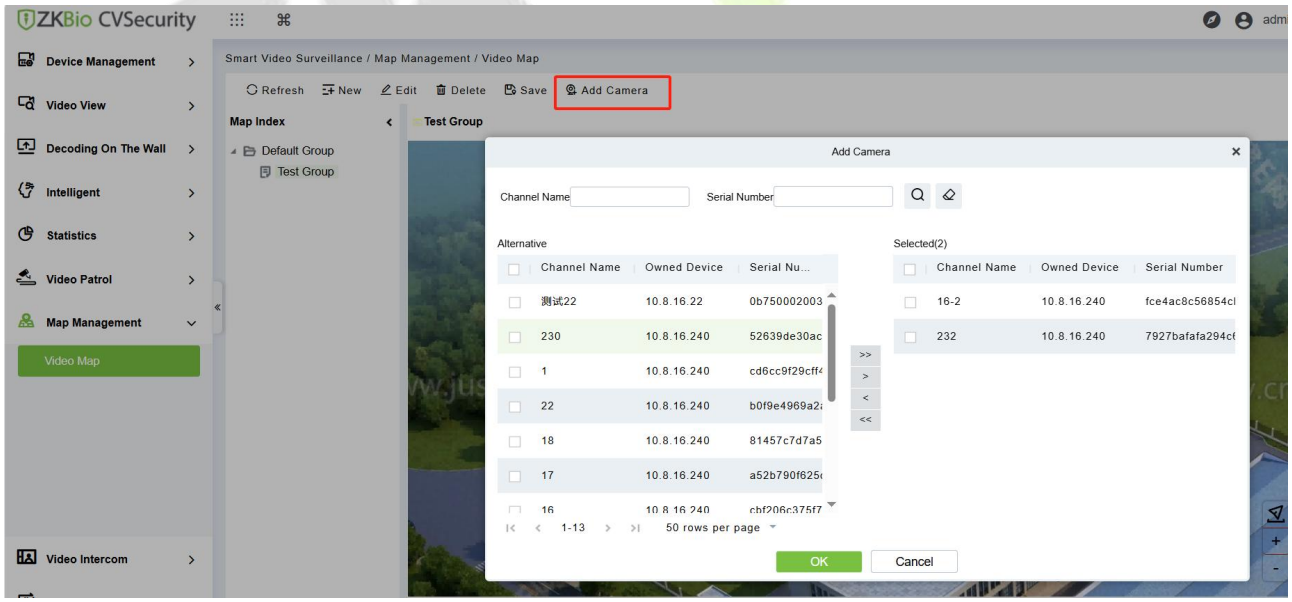
5.8.1 Video Map

5.8.1.1 New/ Add Camera

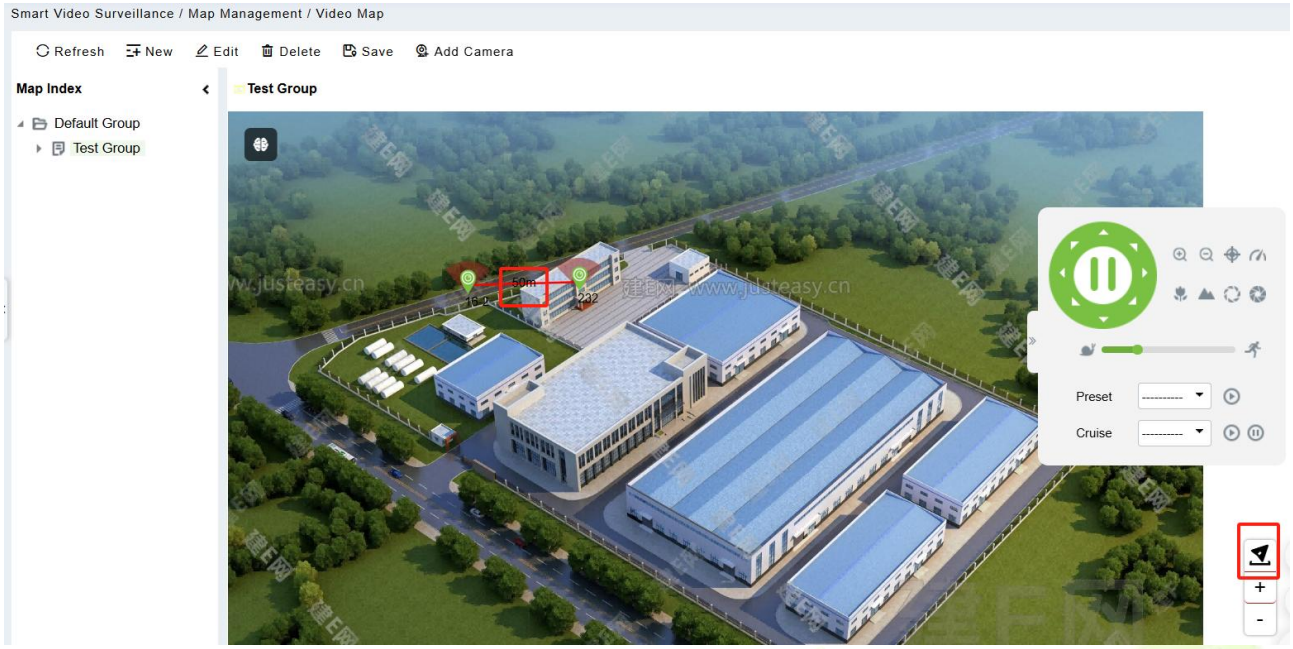
Click **Map Management** > **Video Map**. Click New to add a E-map.



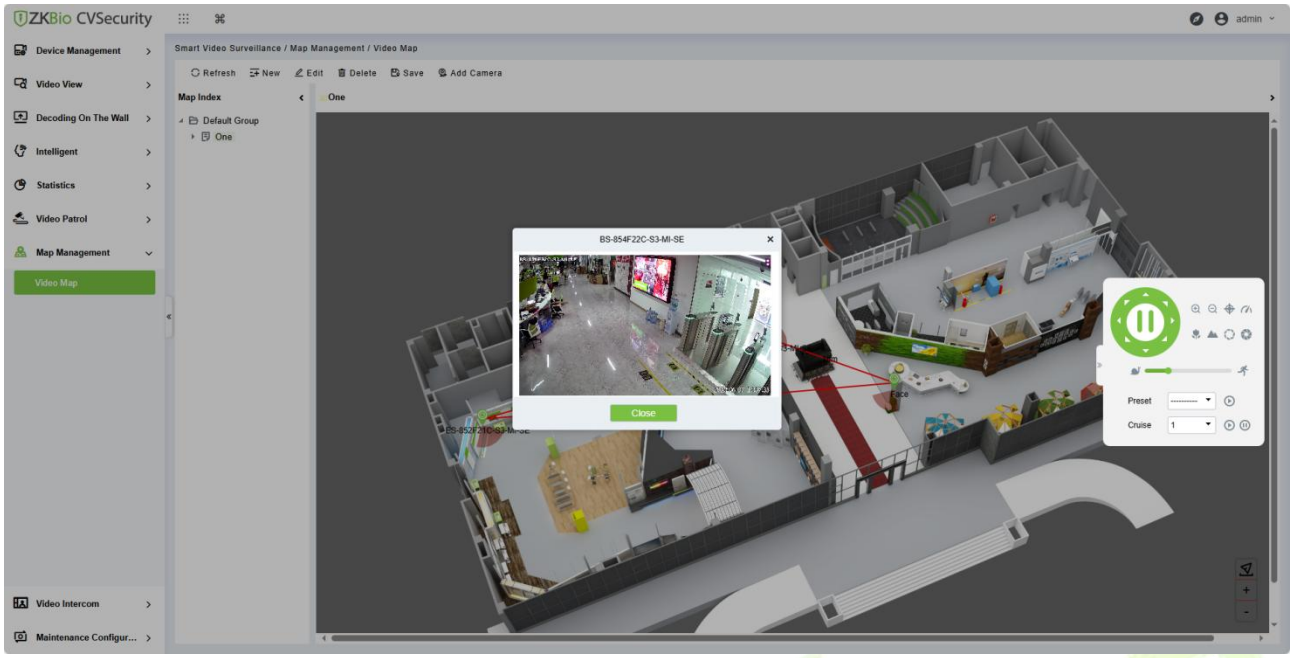
Then you can click **Add Camera.** Add the cameras to the map.



Adjust the position and **Save position.** Click  button and select camera can dimension distance.

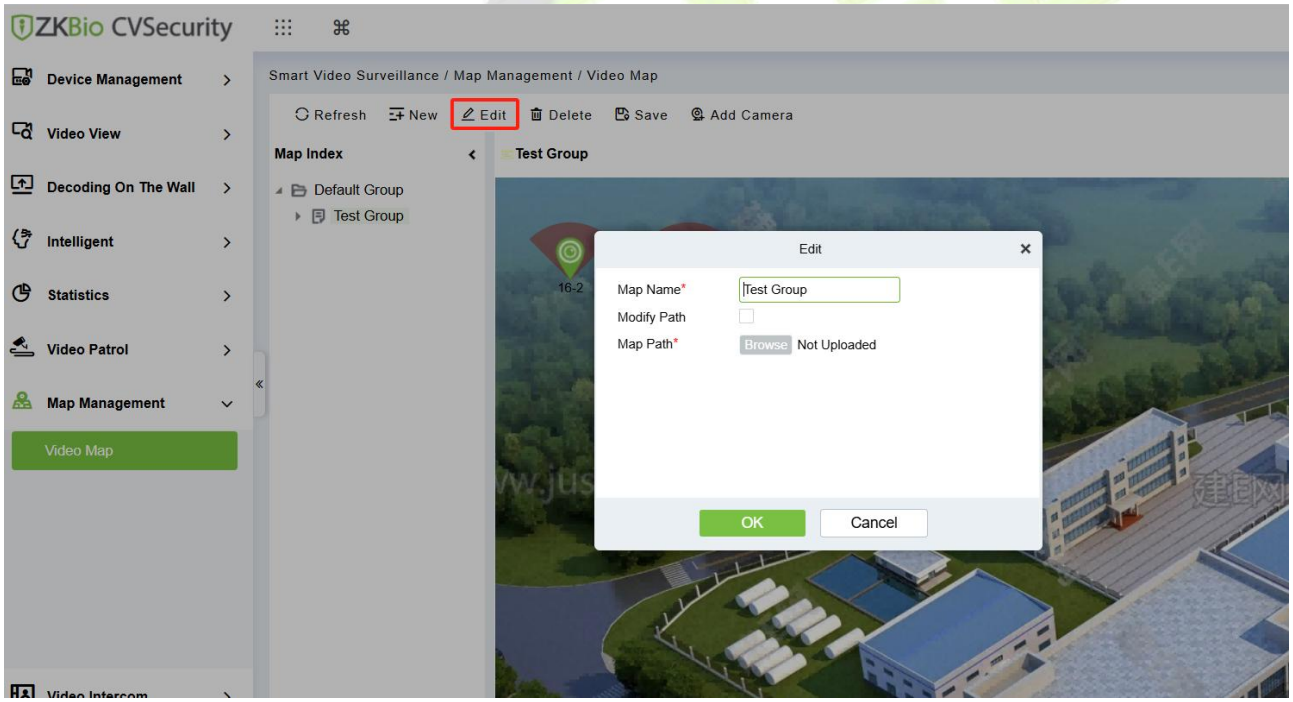


The map will be displayed as follows:



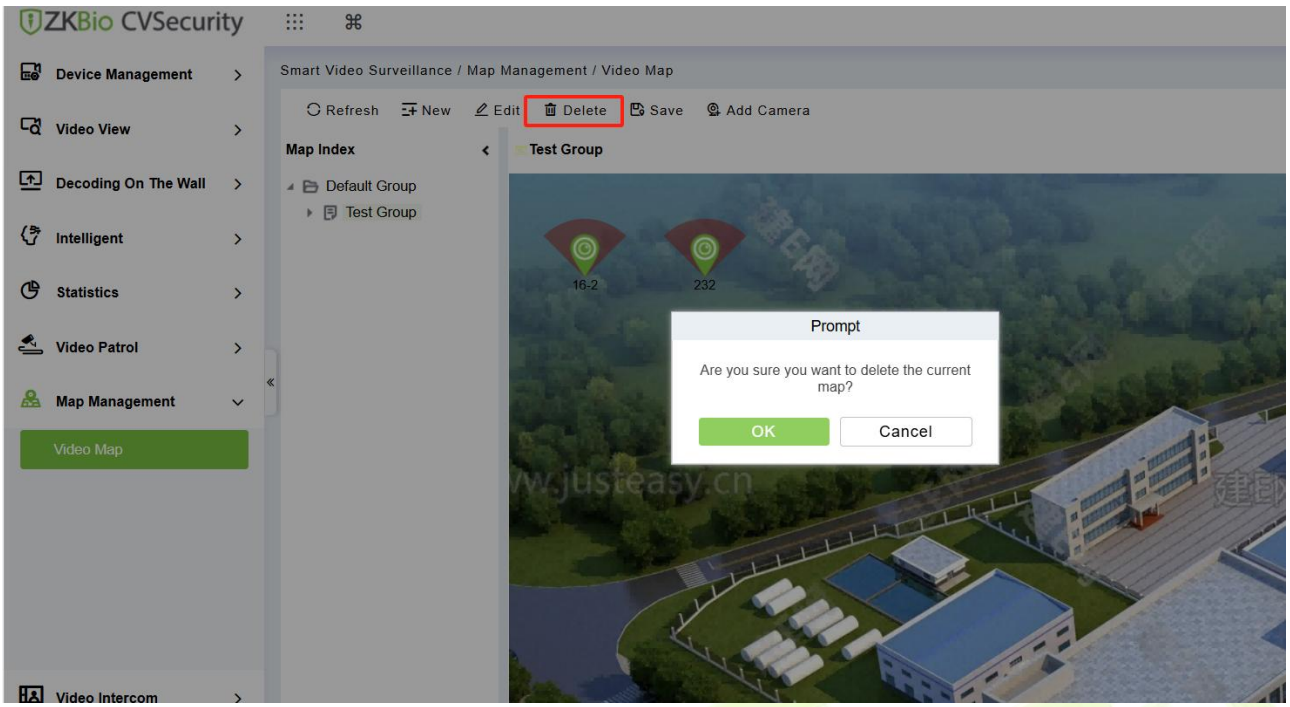
5.8.1.2Edit

Click **Map Management > Video Map**, select the map details and then click on the **Edit** icon to edit the required details.



5.8.1.3Delete

Click **Map Management > Video Map** , select the map details and then click on **Delete** to delete the required details.

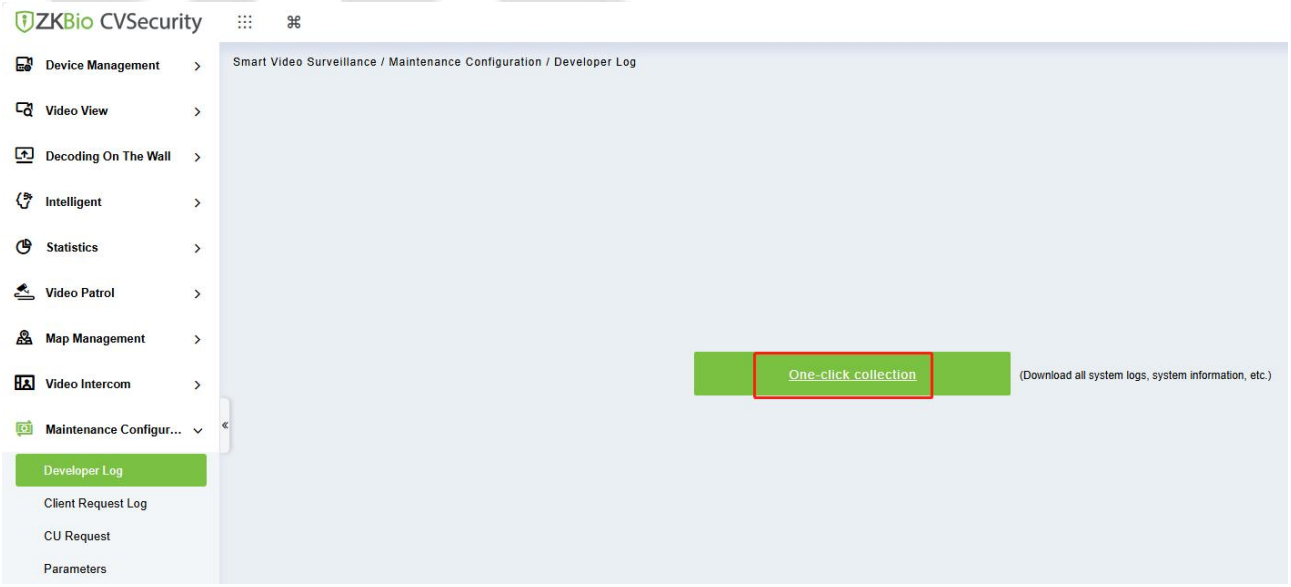


5.9 Maintenance Configuration

5.9.1 Developer Log

Click Intelligent Video > Maintenance Configuration> Developer Log, then select One-Click Collection.

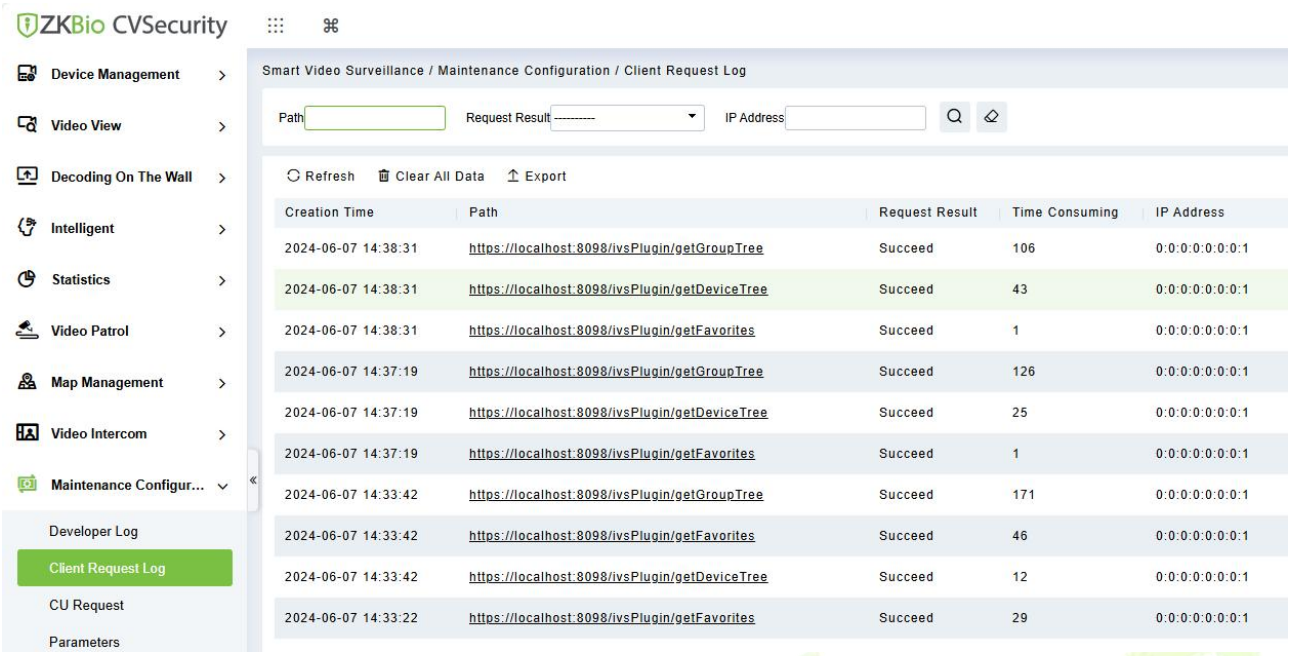
Users can download all system logs and system information to get Click on the **One-Click Collection** option.



5.9.2 Client Request Log

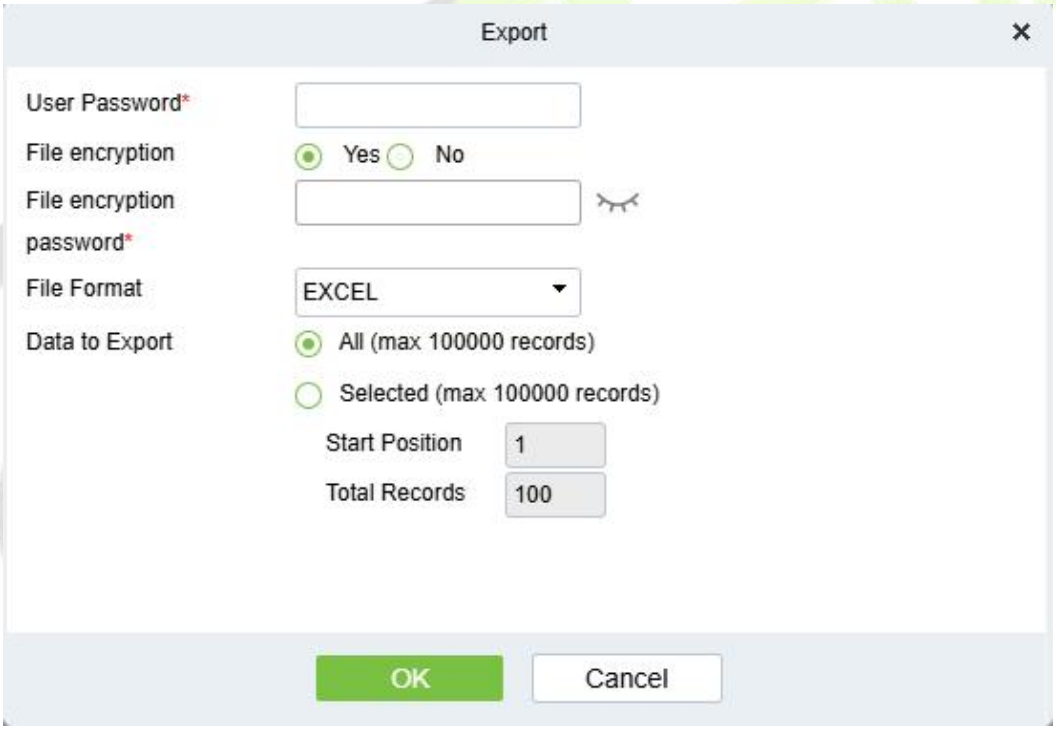
5.9.2.1 Clear All Data

Click **Clear All Data** to pop up the prompt and click **OK** to clear all Data Operations.



5.9.2.2 Export

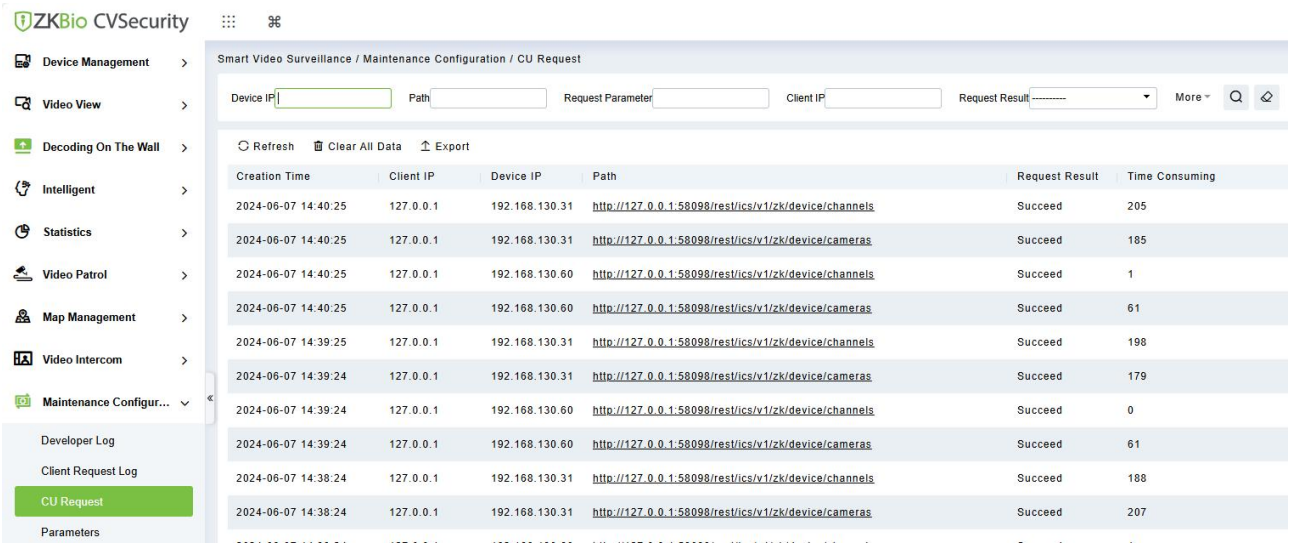
Export selected personnel information in the area; you can export Excel, PDF, CSV format.



5.9.3 CU Request

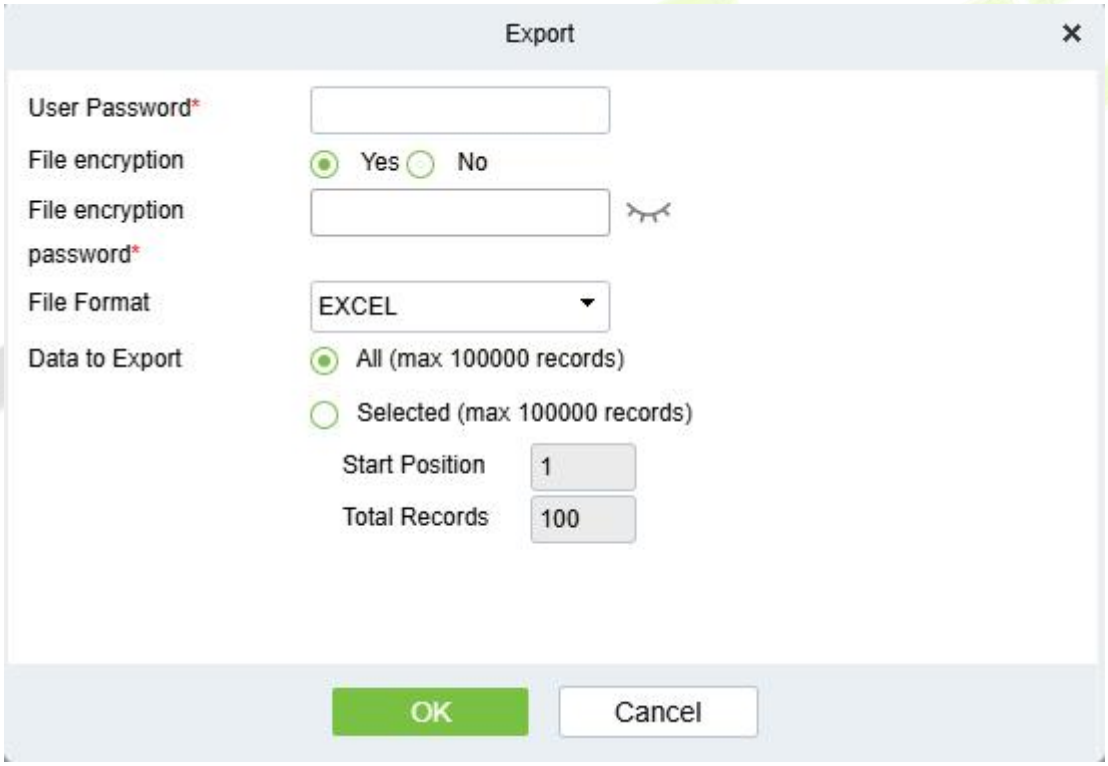
5.9.3.1 Clear All Data

Click **Clear All Data** to pop up the prompt and click **OK** to clear all Data Operations.



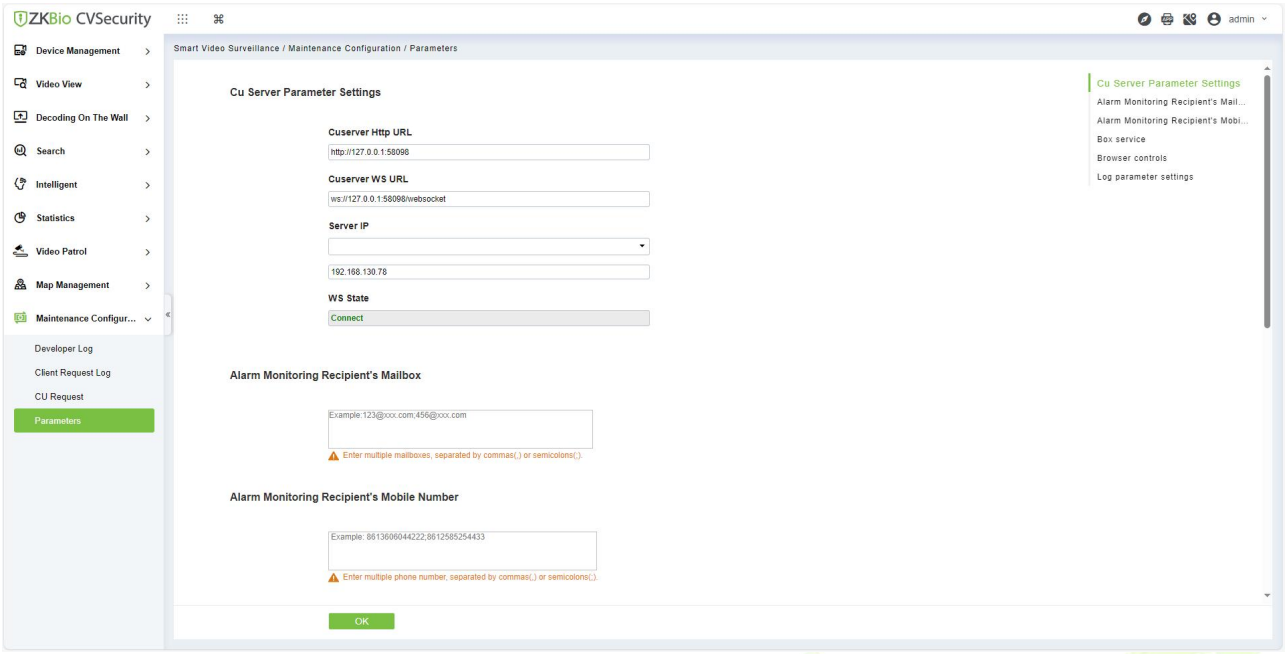
5.9.3.2Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.



5.9.4Parameters

Click Intelligent Video > Parameters, then Set up all the settings, then Click OK.



Parameters	Instructions
CU Server Parameter Settings	Set Up CU server HTTP Url and WS Url and enter Server IP address then can view WS state.
Alarm Monitoring Recipient's Mailbox	Set the email address to receive alarm.
Alarm Monitoring Recipient's Mobile Number	Set the Mobile Number to receive alarm.
Box service	Whether to receive the alarm of the box and select the terminal to receive the stranger's track.
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.

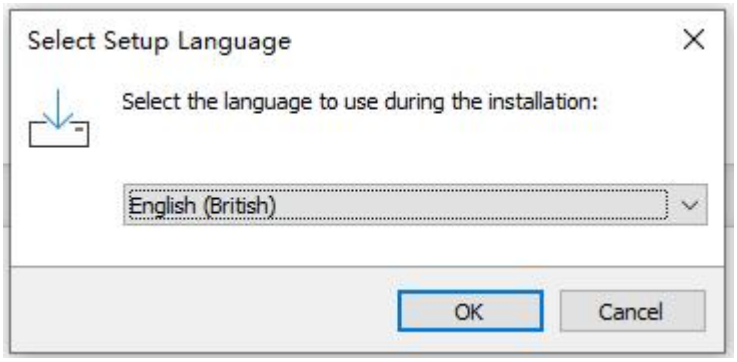
5.10 ZKBio Video Client

5.10.1 Installing the Client

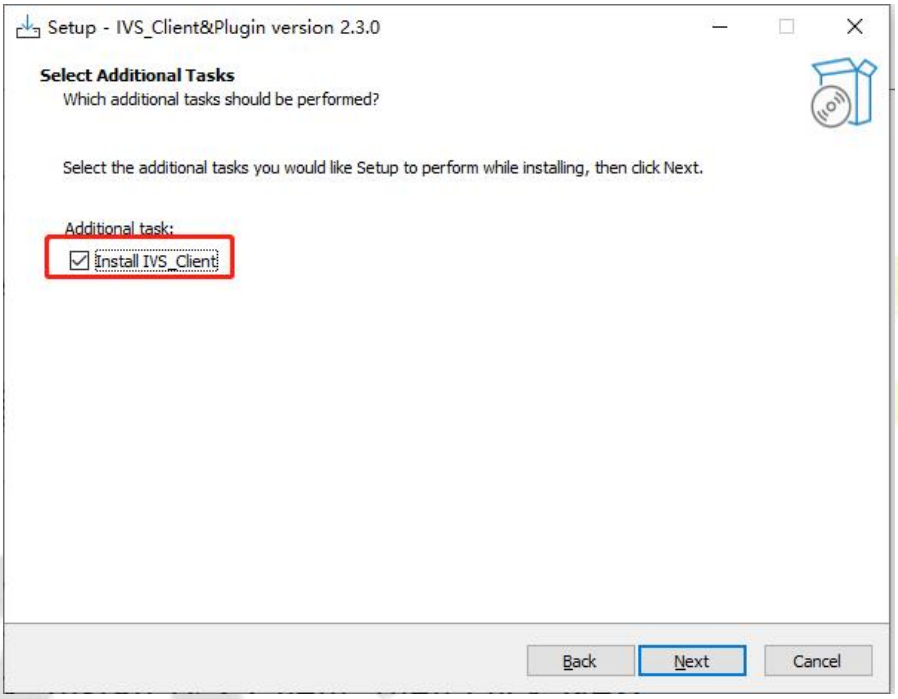
● Operating Steps:

Step 1: Click Install package to proceed to the installation process.

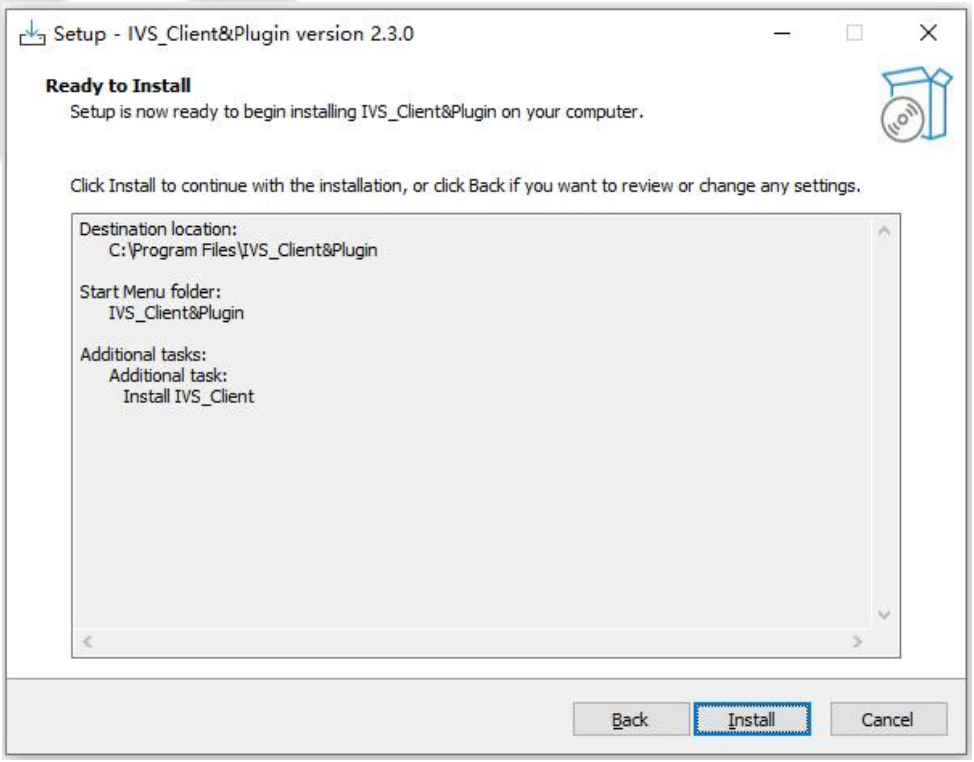
Step 2: Select the language to use during the installation,and click **OK**.



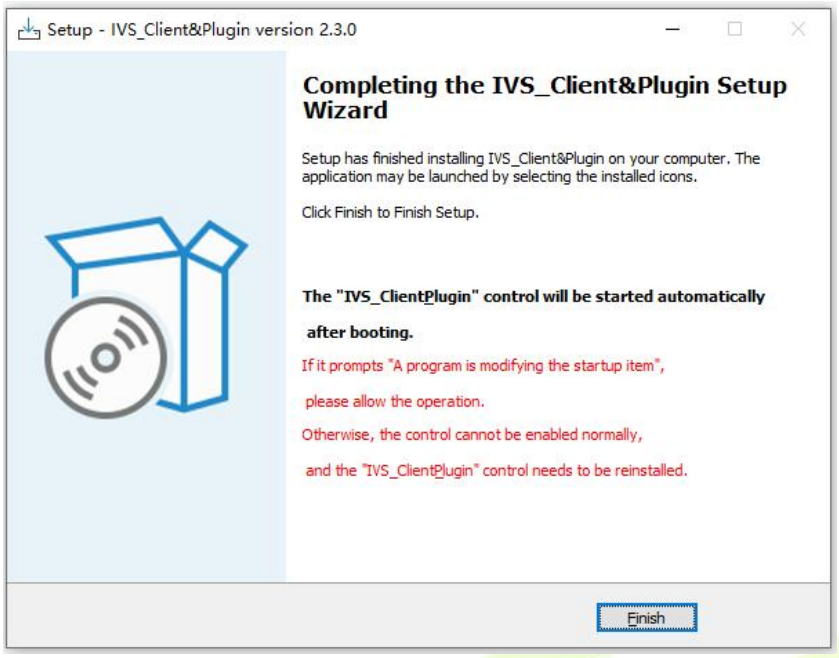
Step 3: Select the additional task 'Install IVS_Client', then click **Next**.



Step 4: Click **Install** to continue with the installation.



Step 5: Click **Finish** to complete the installation process.



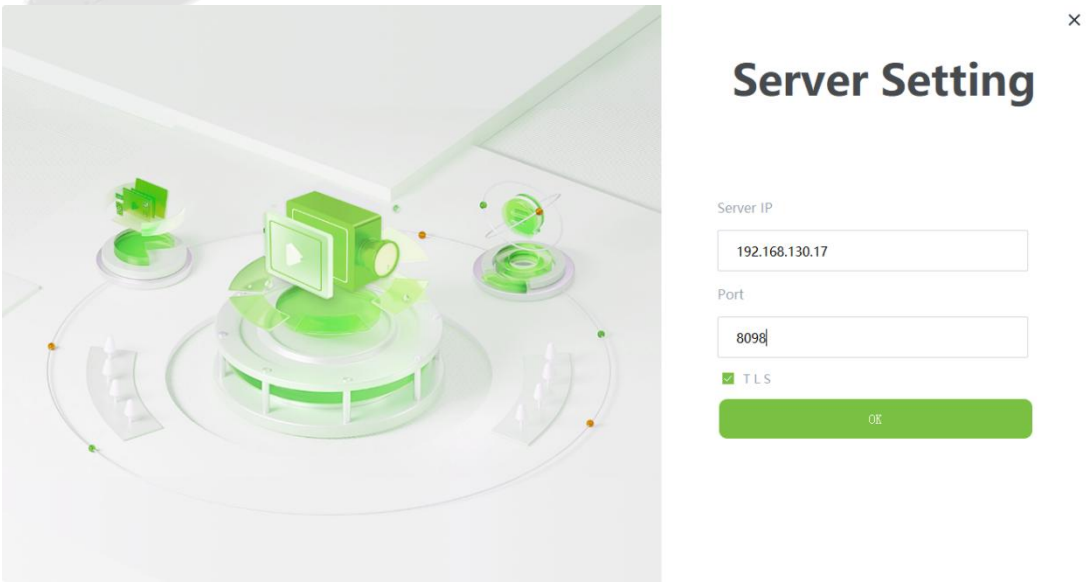
5.10.2Configuration And Use

5.10.2.1Login

●Operating Steps:

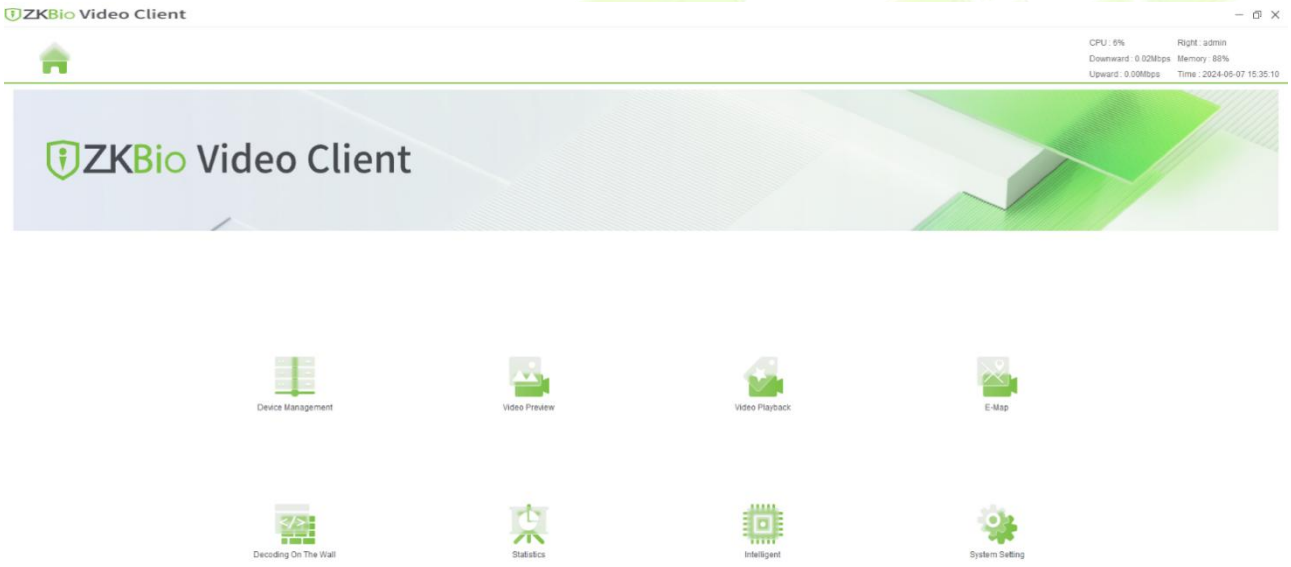
Step 1: Click the icon of the client to access the client login page.

Step 2: Click **Server Setting** and Configure ZKBioCV Security's server IP and port,enable **TLS** and click **OK**.



Step 3: Select the language of the client,enter ZKBioCV Security's username and password,then click **Login**.

5.10.2.2Homepage



5.10.2.3Device Management

Please refer to 5.1 setup.

5.10.2.4Video Preview

Please refer to **5.2** setup.

5.10.2.5Video Playback

Please refer to **5.2** setup.

5.10.2.6E-Map

Please refer to 5.8 setup.

5.10.2.7Decoding On The Wall

Please refer to **5.3** setup.

5.10.2.8Statistics

Please refer to 5.6 setup.

5.10.2.9Intelligent

Please refer to 5.5 setup.

5.10.2.10System Setting

Please refer to **5.9** setup.

6 Time & Attendance

6.1 Operation Scenario

Attendance, also known as time management, carries out attendance function operations such as scheduling for employees, and helps enterprises effectively collect attendance data of employees, enter abnormal attendance data, and calculate attendance results.

6.2 Operation Flow

Introduce the configuration process of attendance management business.

The attendance management business configuration process is shown in figure below.

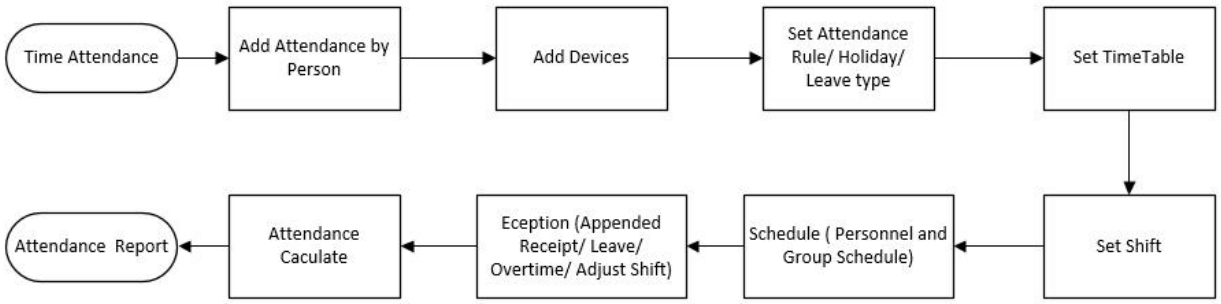


Figure 6- 1 Attendance Configuration Process

6.3 Attendance Management

6.3.1 Personnel Verification Method

Administrators can modify attendance verification methods for staff members.

select multiple staff members, click **"Verification Method Setting"** and choose the appropriate verification method for the selected individuals.

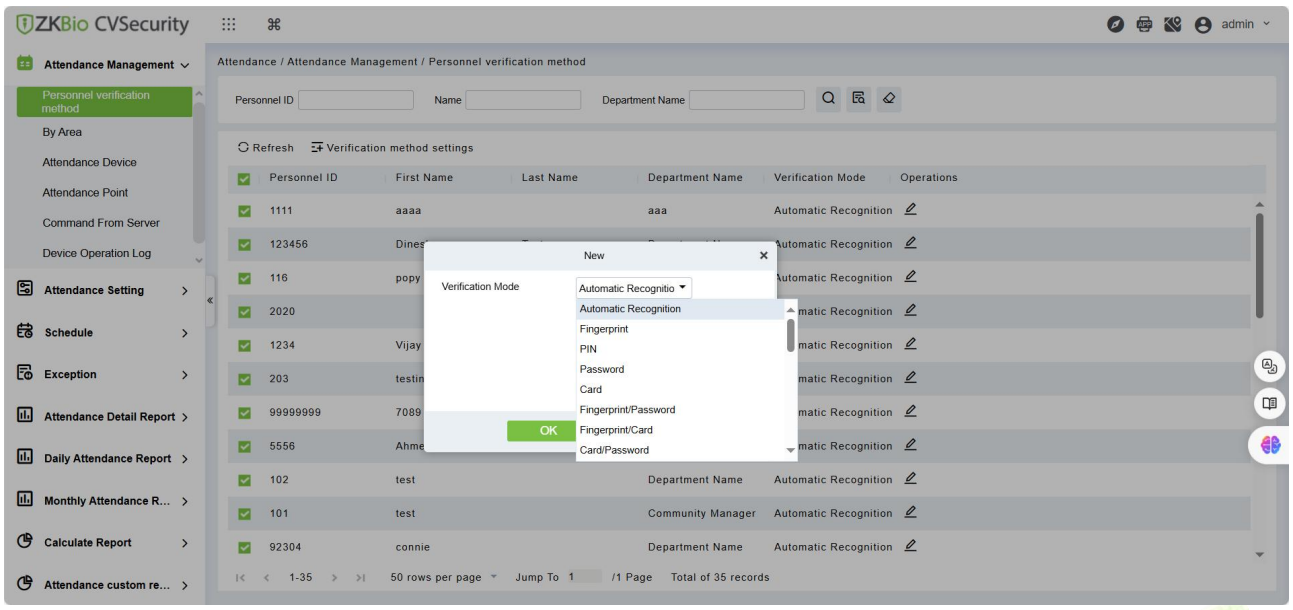


Figure 6- 2 Verification Method

6.3.2By Area

This action is used to define which persons in the Attendance area can be attended. Only those who are added to the area can be attended.

This part introduces the configuration Steps of manually setting regional attendance personnel in.

6.3.2.1Add Area Personnel

●Operating Steps:

Step 1: In **Attendance** module, select "Attendance Management > Setting Personnel by Region", select the region to be set in the list on the left, and then click "Add Regional Personnel" on the right.

Step 2: Add personnel information in the pop-up Add Personnel window, as shown in figure below.

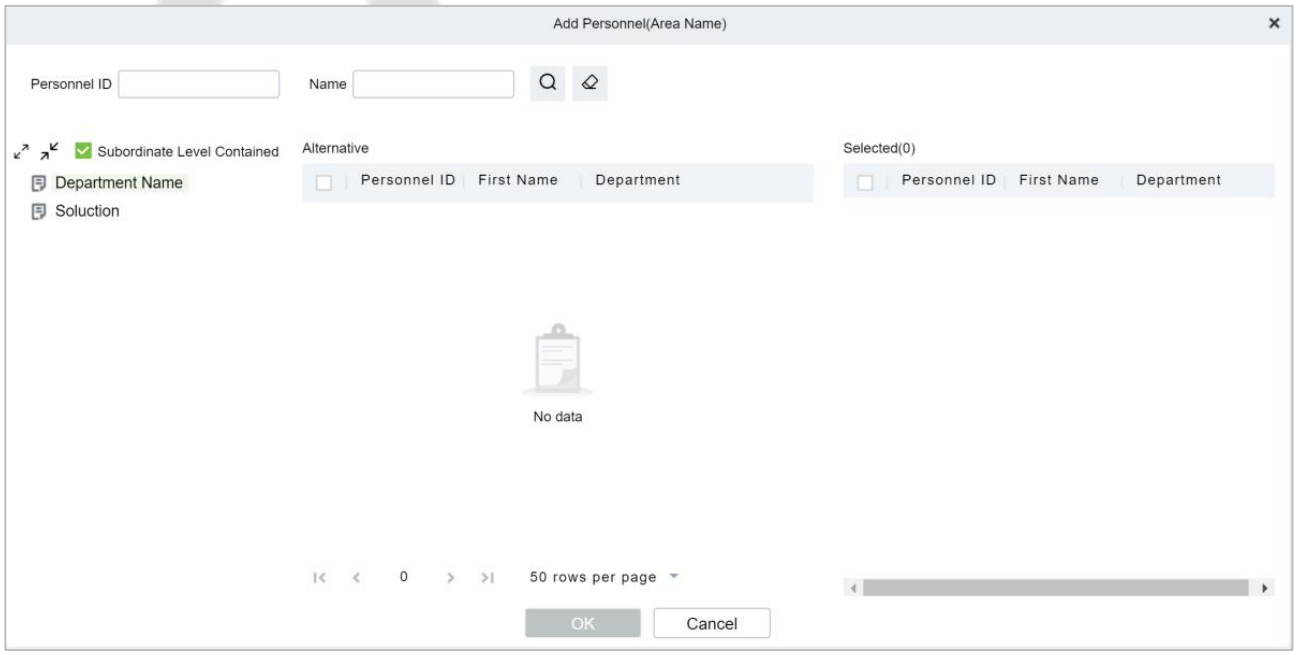


Figure 6- 3 Add by Area

Step 3: Click **OK** to complete the configuration of adding attendance personnel in the area.

6.3.2.2Delete Area Personnel

Step 1: On the **Area** interface, select the required ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected ID.

Step 3: Click **Delete**, to ensure and delete the selected ID from the list.

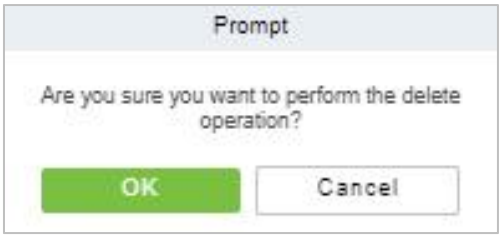


Figure 6- 4 Deleting People

6.3.2.3Export

You can export all transactions in Excel, PDF, CSV format.

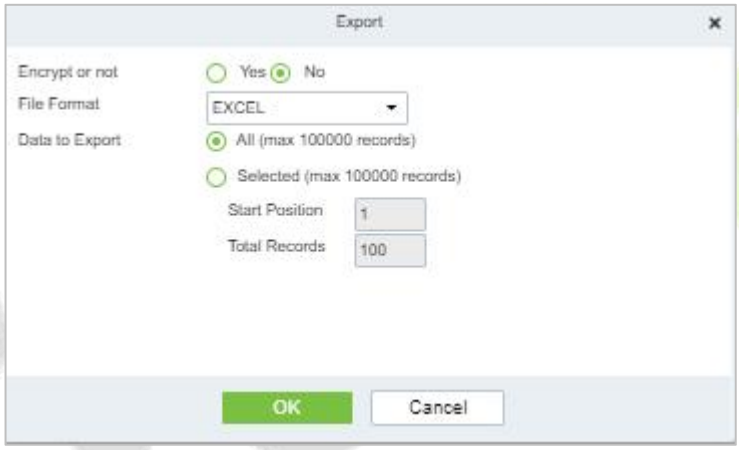


Figure 6- 5 Export People

6.3.2.4Import

You can import all transactions in Excel, PDF, CSV format.

● Import Area Personnel:

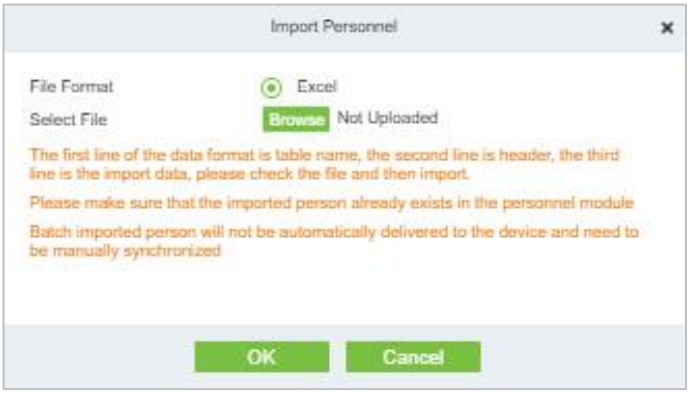


Figure 6- 6 Adding People Import Area

● Import and Delete Area Personnel:

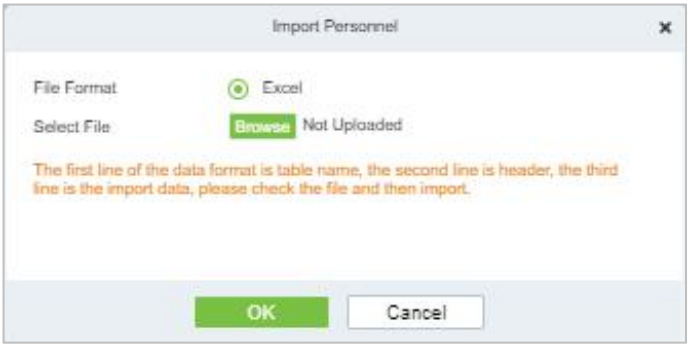


Figure 6- 7 Import Personnel

● Download Import Template:

You can download the entire file in Excel, PDF, CSV format.

6.3.2.5 Private Message

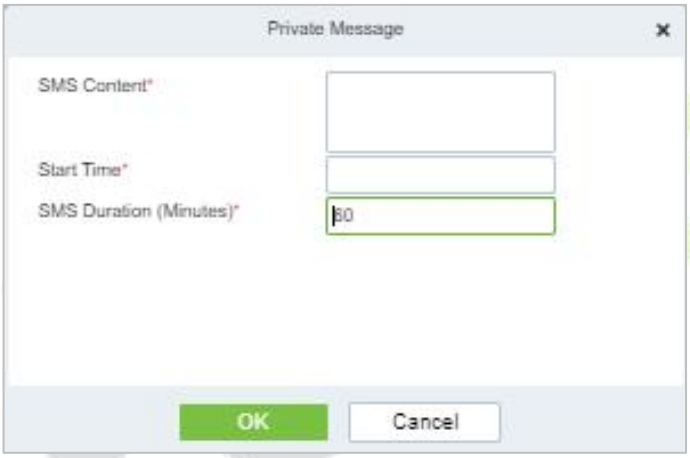


Figure 6- 8 Private Message

6.3.3 Attendance Device

This part introduces adding attendance device and setting communication parameters of connecting device, including the settings in the system and attendance device. After successful communication, you can view the information of connected devices, monitor the machines remotely, synchronize data and other operations.

Use Attendance Machine as Attendance Data Source.

● Precondition:

You need to set up the communication of the device first:

1. Open "Communication Settings > Network Settings" on the attendance device and configure the device network information in the pop-up "Network Settings" window.
2. Open "Communication Settings > Cloud Service Settings" and configure cloud server information in the pop-up "Cloud Server Settings" window.

6.3.3.1 Authorized Device

This part introduces the configuration Steps of adding attendance device in by authorization.

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Management > Attendance Device**, and click

"Authorized device".

Step 2: In the **Authorized Devices** window that pops up, add attendance devices, as shown in figure below.

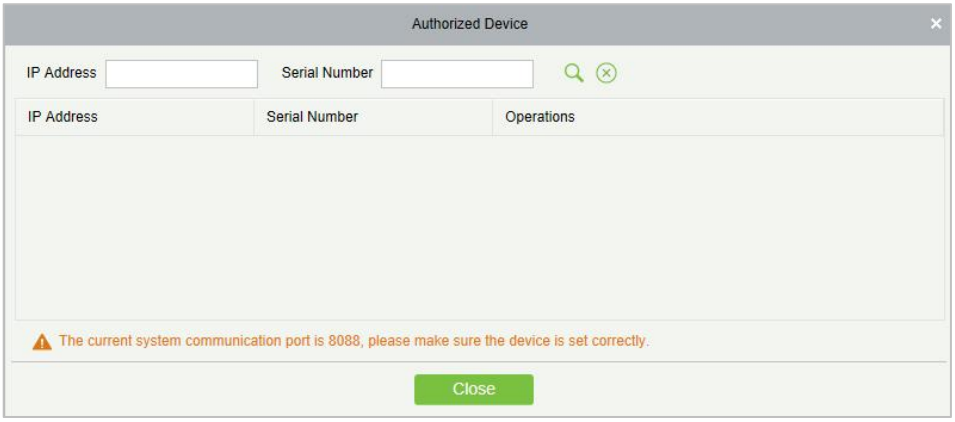


Figure 6- 9 Device Authorization Add Interface

Step 3: In the **Add** window that pops up, configure the device information, as shown in figure below and the key parameters are described in Table 6-1.

Figure 6- 10 Adding Device Setup Interface

Parameter	Description
Attendance Area	The device is divided into regions to realize the management of regional data.
Whether To Register the Machine	If it is not checked, the user data uploaded by the device will not be processed (if the attendance record of the device is checked or not, it will be processed); Check, and the user data uploaded by the device will be processed.

Table 6- 1 Description of Key Parameters.

6.3.3.2Delete

Step 1: On the **Device** interface, select the required Device Name from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

6.3.3.3Device Control

Upgrade Firmware

Tick the device that needs to be upgraded, click **Upgrade firmware** to enter edit interface, then click

Browse 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. Unauthorized upgrade may affect normal operations.

Reboot Device

It will reboot the selected device.

Public Message

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

Disable/Enable

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

Synchronize Software 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.

Authorize Area

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

6.3.3.4View and Get Information

Get Device Option

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

Get the specified personnel data

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.

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

To re-upload the data from the device.

View Device Parameters

To view the parameters and the specification of the device.

6.3.3.5Clear Device Data

Clear unexecuted device commands

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

Clear the attendance photos

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.

6.3.4Attendance Point

This part introduces the configuration Steps of using **Access Control /parking/facekiosk/passage/ smart video surveillance** machine as attendance data source in.

6.3.4.1New

●Operating Steps:

Step 1: In the Attendance module, select Attendance Management > Attendance Points, and click New.

Step 2: Add **Access Control** attendance points in the pop-up **Add** window, as shown in figure below. Please refer to Table 6-2 for explanations of key parameters.

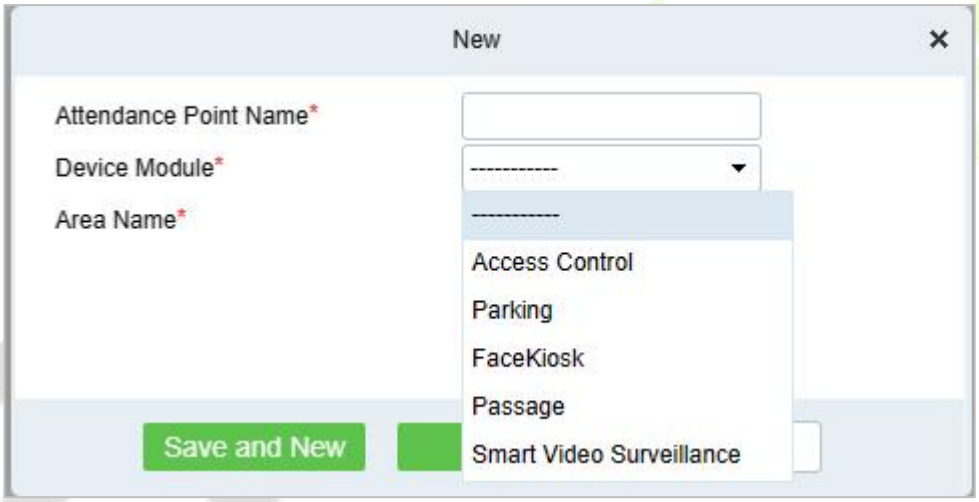


Figure 6- 11 Adding Attendance Point Interface

Parameter	Description
Device Module	Device module for setting attendance record source.
Area Name	The area to which the device belongs.
Door List	You need to set the door corresponding to the attendance record source.

Table 6- 2 Parameter Description

Step 3: Click **OK**.

Step 4: Select "Detailed Report > Original Record Table" and click Synchronous Attendance Point Record.

Step 5: Select the time node and attendance point to be synchronized in the pop-up **Synchronize Attendance Point Record** window, as shown in figure below.

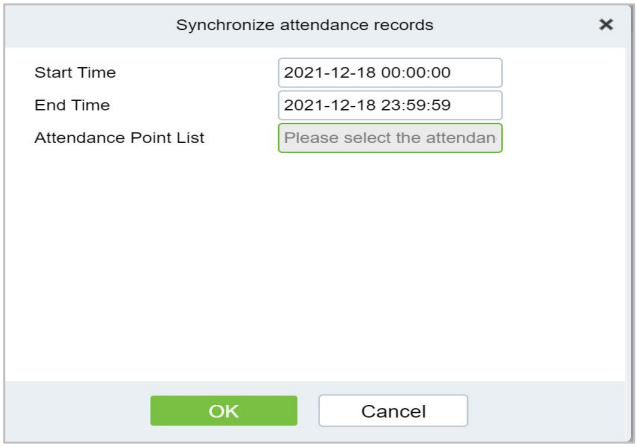


Figure 6- 12 Record of Synchronized Attendance Points

Step 6: Click **OK**.

6.3.4.2Export

You can export all transactions in Excel, PDF, CSV format.

6.3.4.3Delete

Step 1: On the **Attendance Point** interface, select the required Attendance Point Name from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Attendance Point.

Step 3: Click **Delete**, to ensure and delete the selected Attendance Point from the list.

6.3.5Mobile Check In Range

This menu is used to configure the check-in range for mobile attendance by setting up geofences to define valid check-in areas, ensuring the accuracy of attendance data.

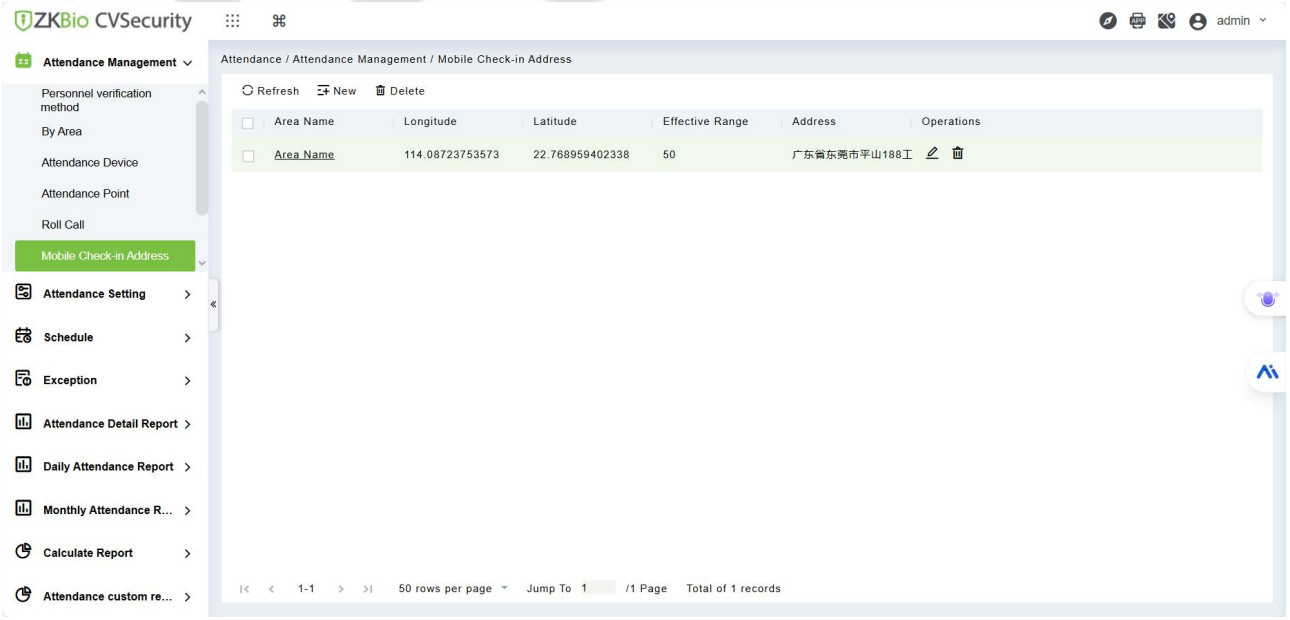


Figure 6- 13 Mobile Check In Range

6.3.5.1New

Click "New" to add a new attendance range.

Note: Currently, only Baidu Maps is supported, and users are not allowed to input latitude and

longitude or specific addresses by themselves. If you want to use this function, it is recommended that users allow the browser to access the location and obtain the detailed current location through the browser. It is shown as follows:

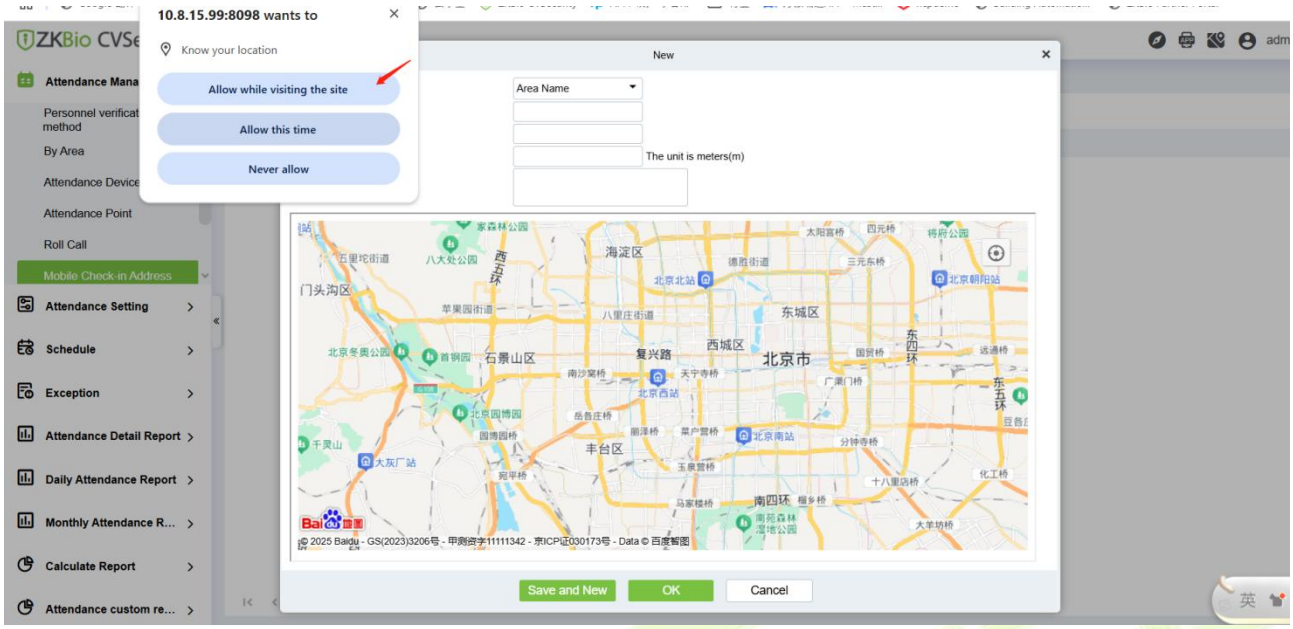


Figure 6- 14 Add a new attendance range

You can also try clicking on Baidu Maps to select an appropriate location. If you need to return to the current location, you can click on "Return to Current Location".

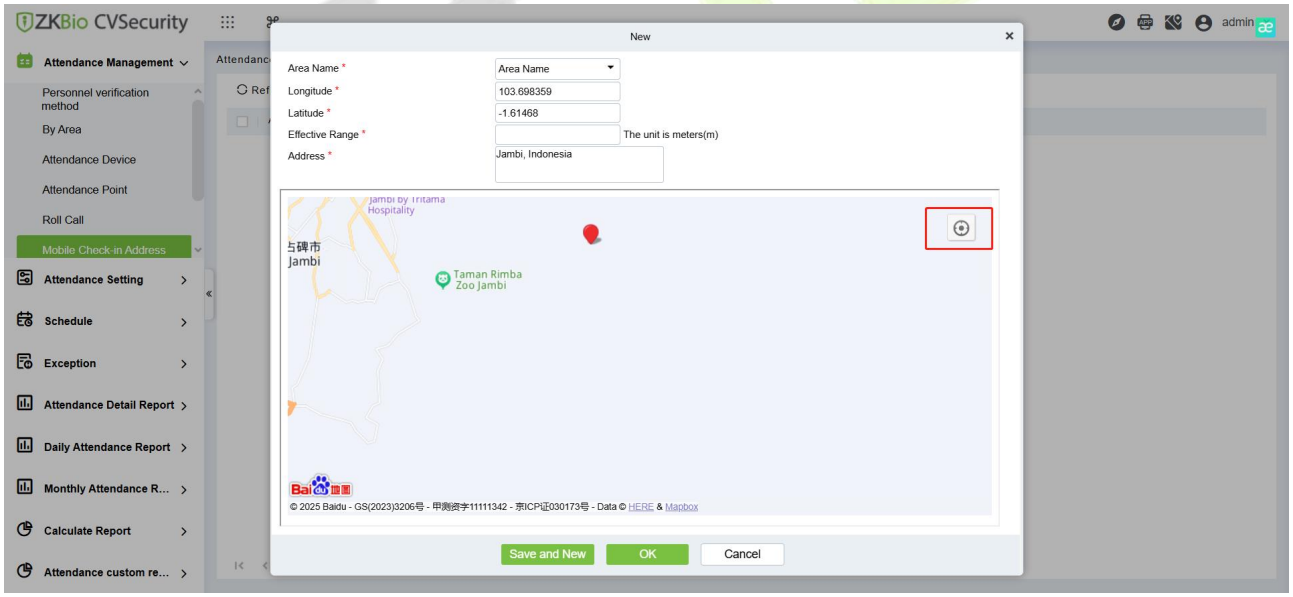


Figure 6- 15

6.3.6Device Command

6.3.6.1Clear Command List

Step 1: You can clear command as required. Click **Clear Command** after selecting the corresponding ID.

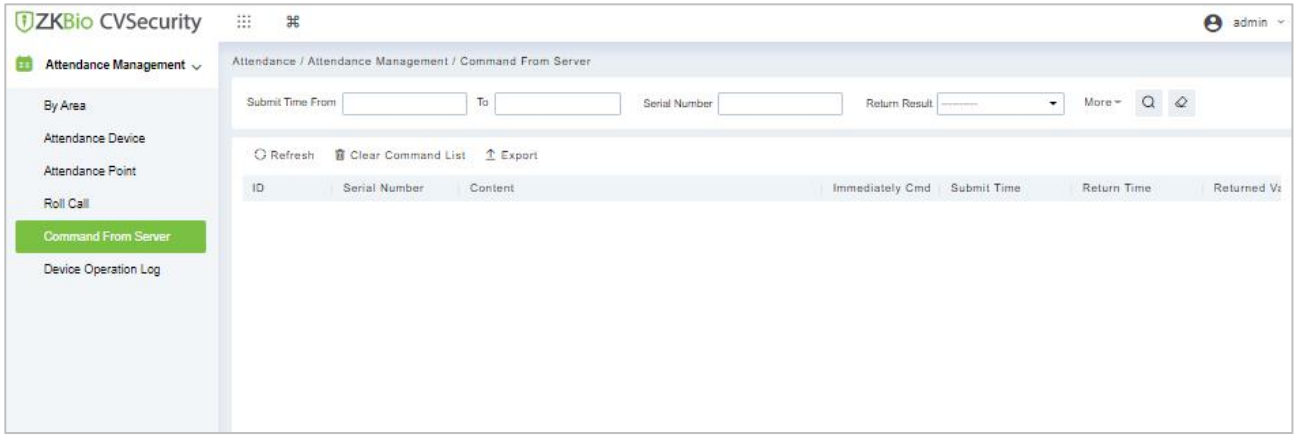


Figure 6- 16 Roll Call Clear Command List

6.3.6.2 Export

You can export all transactions in Excel, PDF, CSV format.

6.3.7 Device Operation Log

For 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.

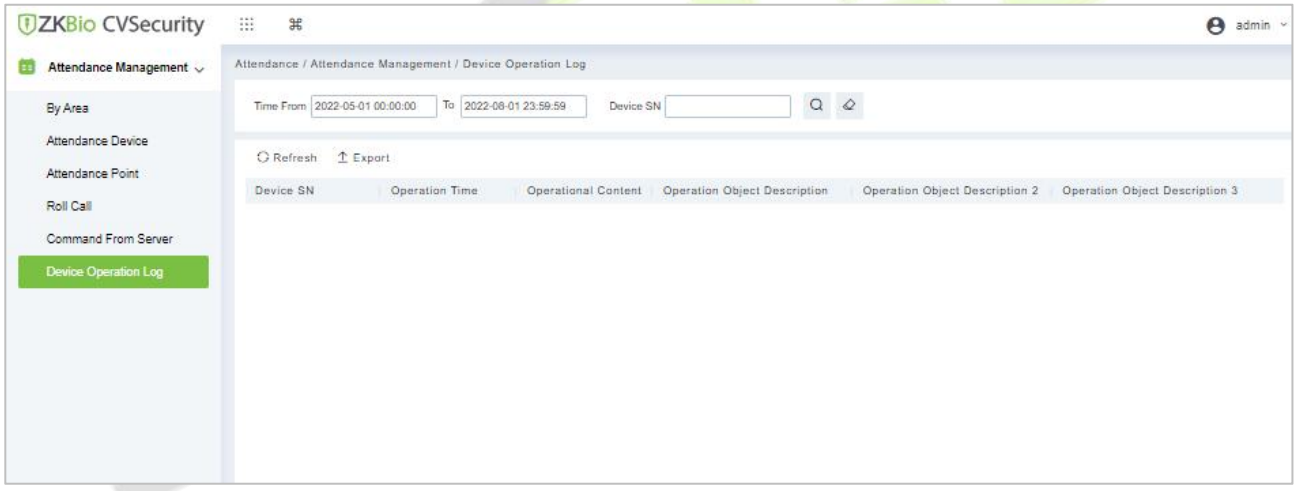


Figure 6- 17 Device operation Log

6.3.7.1 Export

You can export all transactions in Excel, PDF, CSV format.

6.4 Attendance Setting

Attendance settings affect attendance results, is the core of attendance calculation logic, including attendance rules settings, holiday settings, fake settings.

6.4.1 Attendance Rule Setting

Because the attendance system is different in each company, it is necessary to manually set attendance rules to ensure the accuracy of the final attendance calculation. The setting of attendance rules is the main way to reflect the attendance system of enterprises.

This part introduces the configuration Steps of attendance rules in.

6.4.1.1 Basic Rule Setting

● Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in figure below, and the basic rule parameter description is shown in Table 6-3.

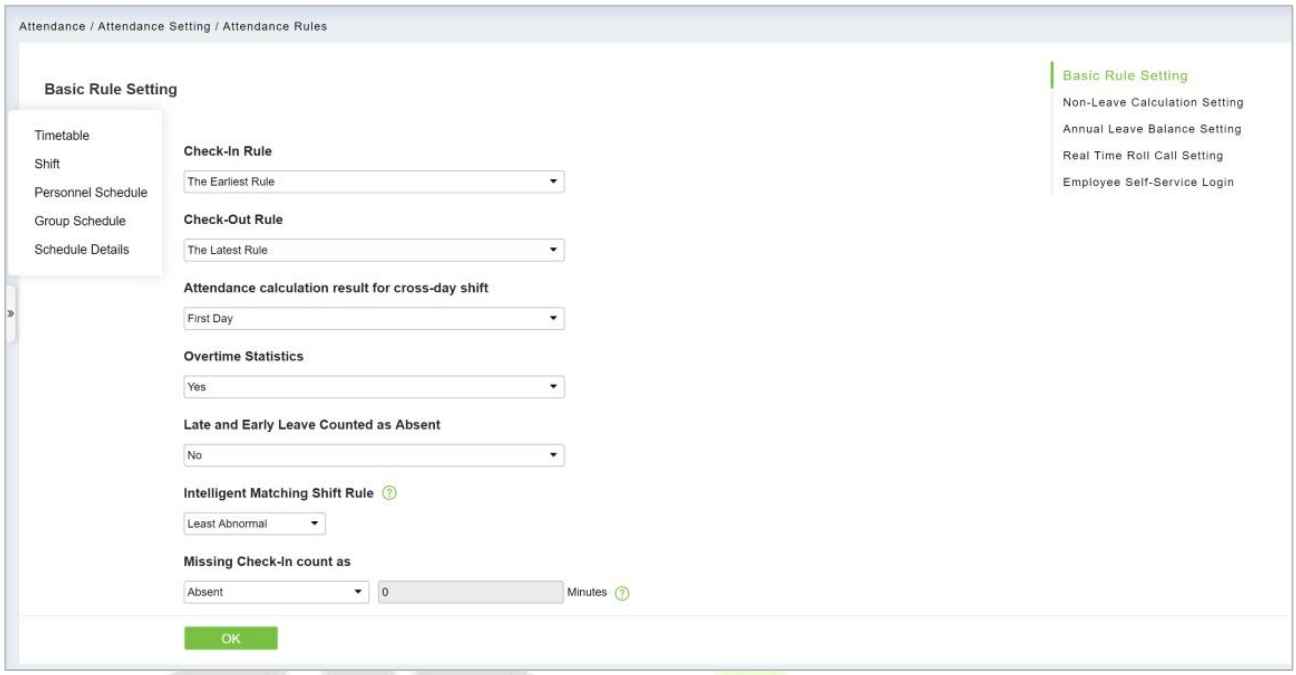


Figure 6- 18 Attendance Rules

6.4.1.2 Non-Leave Calculation Setting

● Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Non-Leave Calculation Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in figure below, and the Non-Leave Calculation description is shown in Table 6-3.

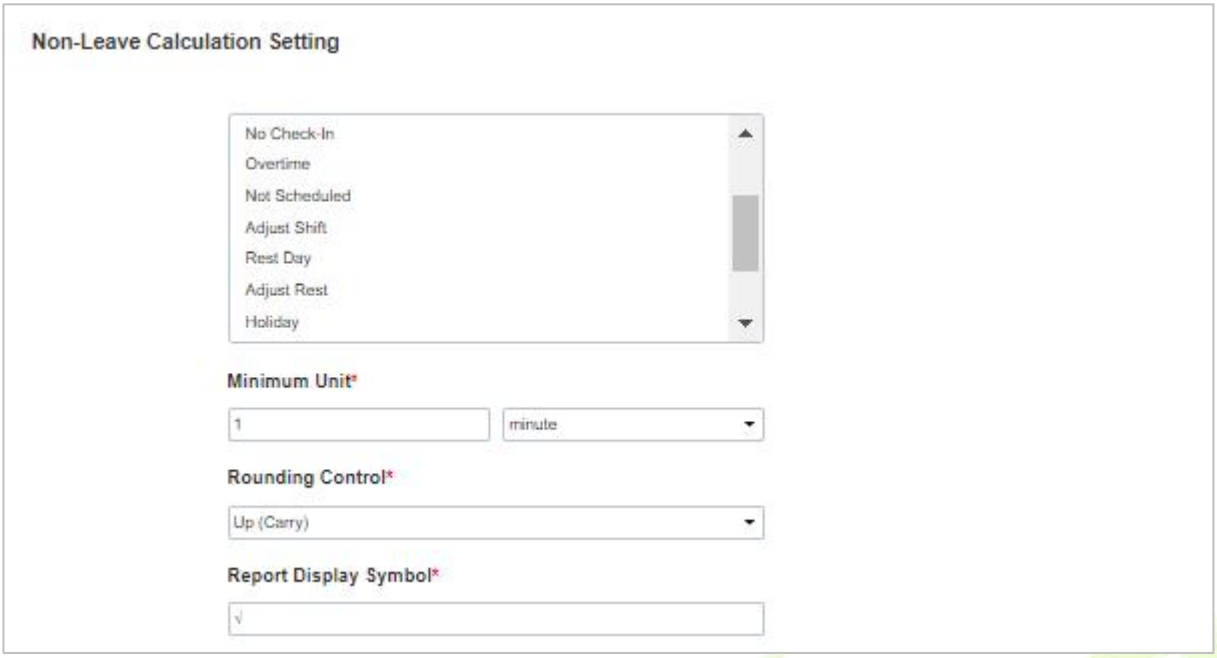


Figure 6- 19 Attendance Rules Settings

6.4.1.3Annual Leave Balance Setting

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Settings > Attendance Rules>Annual Leave Balance Setting**.

Step 2: In the **Attendance Rule** interface, fill in the attendance rules as required, as shown in figure below, and the Annual Leave Balance description is shown in Table 6-3.

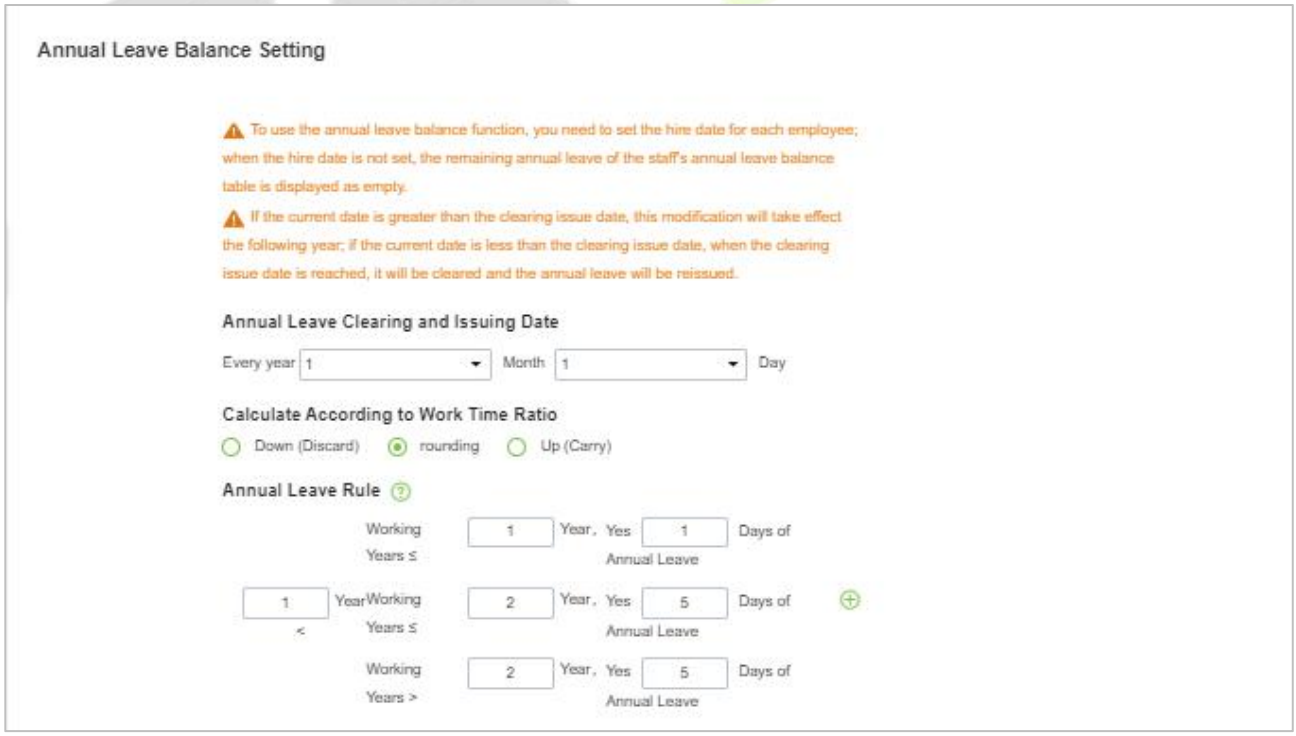


Figure 6- 20 Annual Leave balance Setting

6.4.1.4Real Time Roll Call Setting

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Settings > Attendance Rules>Real Time Roll Call Setting**.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in figure below, and the Real Time Roll Call description is shown in Table 6-3.

Figure 6- 21 Roll Call Real Time

6.4.1.5Employee Self-Service Login

●Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Employee Self Service Login Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in figure below, and the Employee Self Service Login description is shown in Table 6-3.

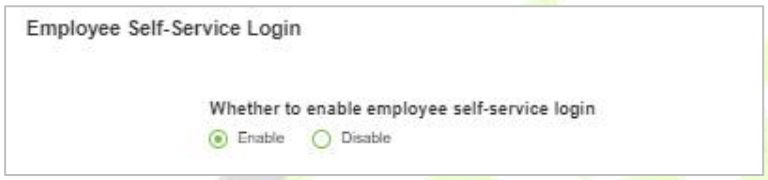


Figure 6- 22 Roll Call Real Time

Parameter	Specific Parameters	Description
Basic Rule	Work check-in and card collection rules	• The earliest (by default, the first punch-in record is taken within the valid card taking range) • Nearby (take the clock-in record closest to working hours within the valid card-taking range).
	Rules for sign-out and card collection after get off work	• Latest (by default, the last punch-in record is taken within the valid card taking range) • Nearby (take the clock-in record closest to the attendance checking time within the valid card-taking range).
	The shortest attendance period should be greater than (10 minutes)	120 (default); Range: 10 to 999; Required
	The longest attendance period should be less than (1440 minutes)	600 (default); Range: 10 to 1440; Required
	The shift time period spans days, and the attendance calculation results	• On the first day, if there is a cross-day, count the working hours in the effective shift on the second day to the first day. • On the second day, if there is a cross-day, the working hours in the effective shift on the first day are counted to the second day.

Parameter	Specific Parameters		Description
	Being late and leaving early is absenteeism		• No (default) • If yes, there are cases of being late and leaving early, and this period is recorded as absenteeism.
	Statistical overtime		• Yes (default) • No; If the first switch of overtime statistics is set to No, overtime will not be calculated.
	Minimum overtime time per time (minutes)		This parameter is applied to overtime rule duration statistics. If overtime duration is less than the set minimum overtime duration, it will not be reflected in attendance statistics.
	Exact number of decimal points		1 (default), 2.
	Failure to sign in is recorded as		Three ways: • Absence • Be late • Incomplete Description: • When you are late, you should set the number of minutes you are late. • Absence and incompleteness are not valid attendance, but absence is absenteeism and incompleteness is absenteeism. Statistics attendance by setting basic rules in monthly detailed reports and other related reports.
	Unsigned refund as		Three ways: • Absence • Be late • Incomplete Description • When you are late, you should set the number of minutes you are late. • Absence and incompleteness are not valid attendance, but absence is absenteeism and incompleteness is absenteeism. Statistics attendance by setting basic rules in monthly detailed reports and other related reports.
Non-Pseudo Class Calculation Settings	Set up various states of non-fake classes (including being late, leaving early,	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

<table>
<tr><th>Parameter</th><th colspan="2">Specific Parameters</th><th colspan="2">Description</th></tr>
<tr><td></td><td rowspan="2">not signing in, etc.)</td><td></td><td colspan="2">integer will be added with 1, otherwise, the integer will be taken.
• Up (carry): With decimal, discard decimal, integer plus 1</td></tr>
<tr><td>Report presentation on symbol</td><td colspan="2">Symbols for associated report presentation</td></tr>
<tr><td rowspan="3">Setting of Annual Leave Balance</td><td colspan="2">Annual leave cleared and issued date</td><td>Set the annual leave clearing date</td><td rowspan="3">Description
• Using the annual leave balance function requires setting the entry time for each person; When the induction time is not set, the remaining annual leave in the personnel annual leave balance table is displayed as blank.
• If the current date is greater than the clearing and issuing date, the revised content will take effect the following year; If the current date is less than the zero-clearing issue date, the annual leave will be cleared and reissued when the zero-clearing issue date is reached.
For example
Sam San joined the company on September 1 last year
Setting of annual leave balance
The clearing and issuing date is January 1 of each year; According to the proportion of work rounded calculation; There are 3 days" annual leave when the length of service is less than or equal to 1 year, and 5 days" annual leave when the length of service is less than or equal to 3 years
Annual leave entitlement calculation
It enjoyed 4/12 x3 = 1.0 days from September 01 to December 31 last year
This year's 01-01 to 12-31 enjoys 4.0 days (this year's 01-01 to 08-31 enjoys 8/12 x3 = 2.0 days + this year's 09-01 to 12-31 enjoys 4/12 x5 ≈ 2. 0 days)</td></tr>
<tr><td colspan="2">Calculated according to the proportion of working hours</td><td>There are three ways to calculate the proportional duration:
• 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</td></tr>
<tr><td colspan="2">Rules of annual leave duration</td><td>Set annual leave days according to length of service, which can be added by symbols</td></tr>
</table>

Parameter	Specific Parameters	Description
Real-Time Roll Call Setting	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.	
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).	

Table 6- 3 Description of Basic Rule Parameters

6.4.2Holidays

This part introduces the configuration Steps of manually adding holidays in.

6.4.2.1New

● Operating Steps:

Step 1: In the **Attendance** module, select "Attendance Settings > Holidays" and click **New**.

Step 2: Configure holiday information in the pop-up **Add** window.

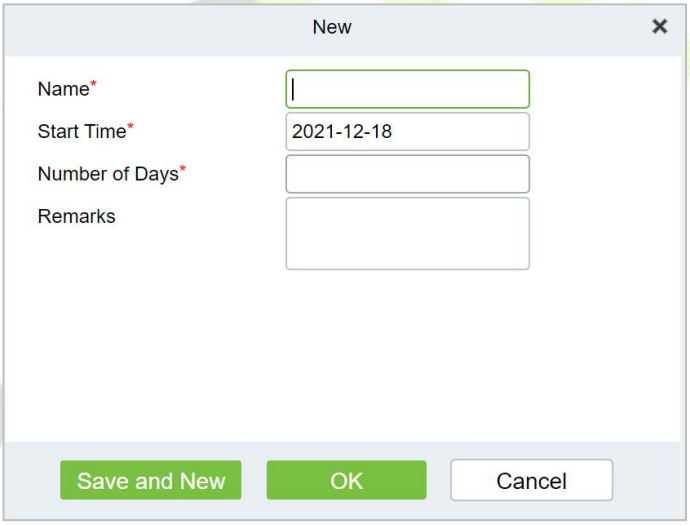


Figure 6- 23 New Holidays

Step 3: Click OK.

6.4.2.2Delete

Step 1: On the **Holiday** interface, select the required Holiday Name from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Holiday list.

Step 3: Click **Delete**, to ensure and delete the selected Holiday from the list.

6.4.2.3Export

Click the "**Export**" and set the relevant parameters.

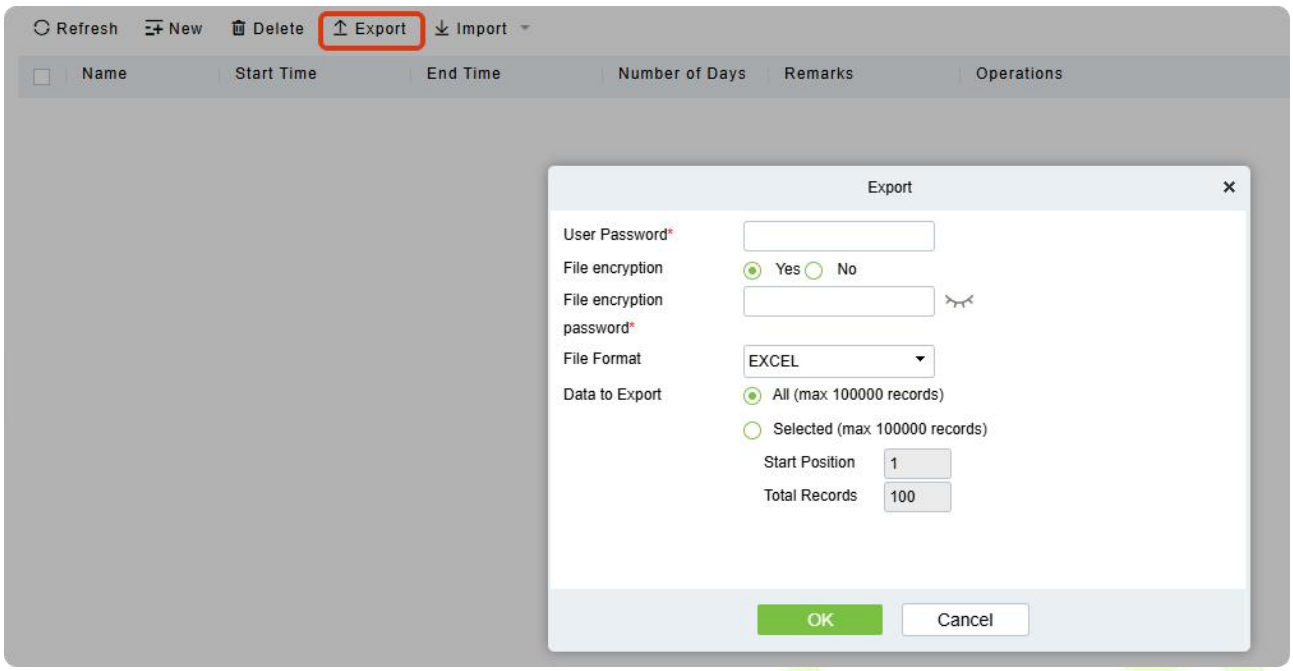


Figure 6- 24 Export Holidays

	Holiday				
1					
2	Name	Start Time	End Time	Number of Days	Remarks
3	holiday1	2025-09-09	2025-09-15	7	
4					

Figure 6- 25

6.4.2.4Import

Step 1: Select and click the "**Import->Download Import Template**" button,download the template "Holiday Template.xls" locally.

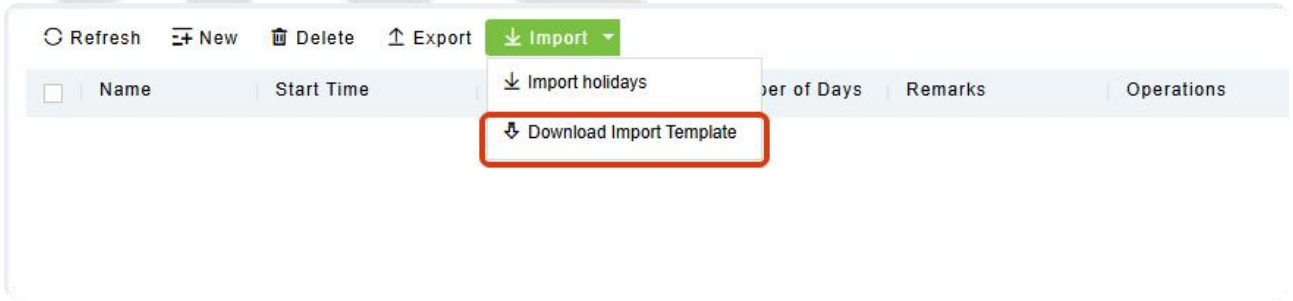


Figure 6- 26 Import Holidays

Step 2: Open the exported template file "Holiday.xls" for adding holiday information.

Holiday			
Name	Start Time	Number of Days	Remarks
holiday1	2025-09-09	2025-09-15	7
holiday2	2025-09-10	2025-09-16	8
holiday3	2025-09-11	2025-09-17	9

Figure 6- 27

Step 3: Select and click the "**Import**" button; click the "**Browse**" button to import the batch import template into the system and click OK, as shown in figure below.

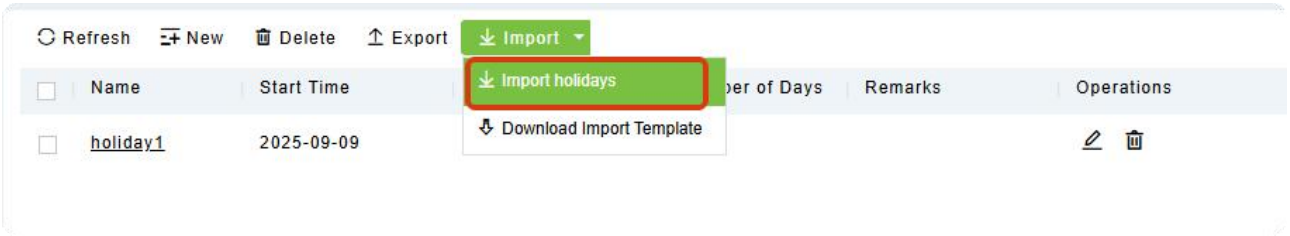


Figure 6- 28 Import Holidays

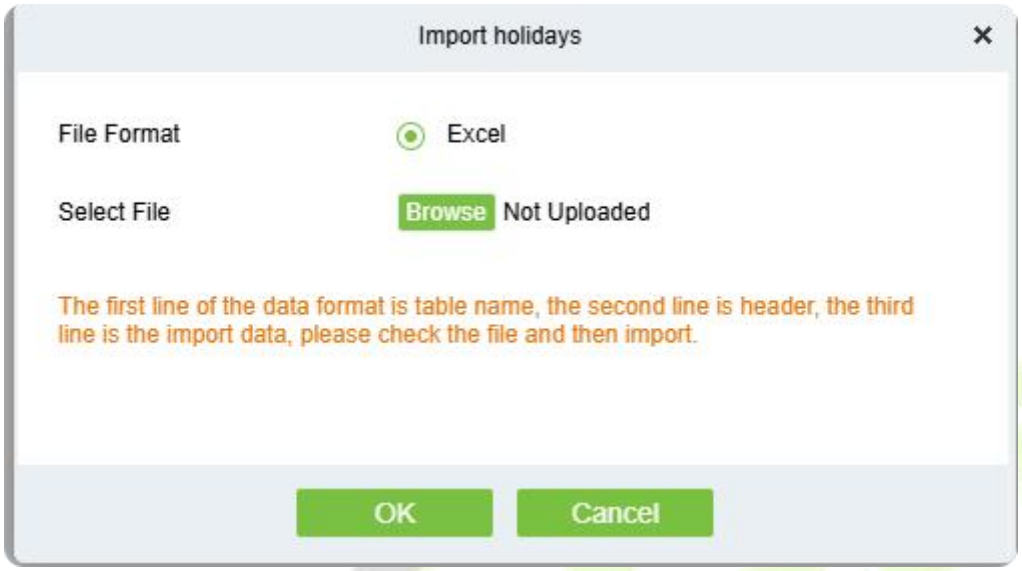


Figure 6- 29

6.4.3Leave Type

This part introduces the configuration Steps of adding Leave Type.

6.4.3.1New

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Settings > Leave Type** and click Add.

Step 2: Configure fake information in the pop-up **Add** window, as shown in figure below. Please refer to Table 6-4 for explanations of key parameters.

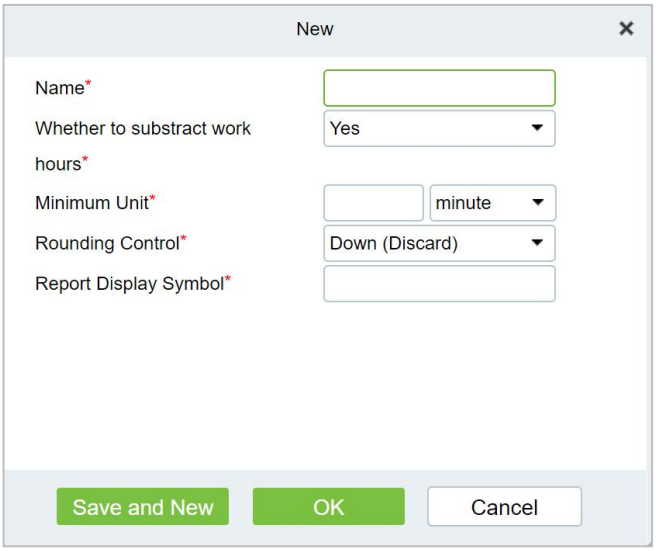


Figure 6- 30 New Leave Type

Parameter	Description
Name	Character length 30, required.
Whether To Deduct Working Hours	Whether the working hours should be deducted for setting this kind of leave, for example, maternity leave/marriage leave/annual leave are all legal holidays, and the working hours are not deducted.
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 Presentation Symbol	Symbols for the presentation of the associated report.

Table 6- 4 Description of Key Parameters

Step 3: Click **OK**.

6.4.3.2Delete

Step 1: In the **Leave Type** interface, select the required Leave from the list.

Step 2: Click **Delete** or click on the  icon.to delete the required Leave from the list.

Step 3: Click **Delete**, to ensure and delete the selected Leave from the list.

6.4.4Automatic Report

The Automatic reporting feature helps you to send the reports to the designated person at the specified time.

6.4.4.1New

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Settings > Automatic Report** and click New.

Step 2: Click to **New** to configure all the details.

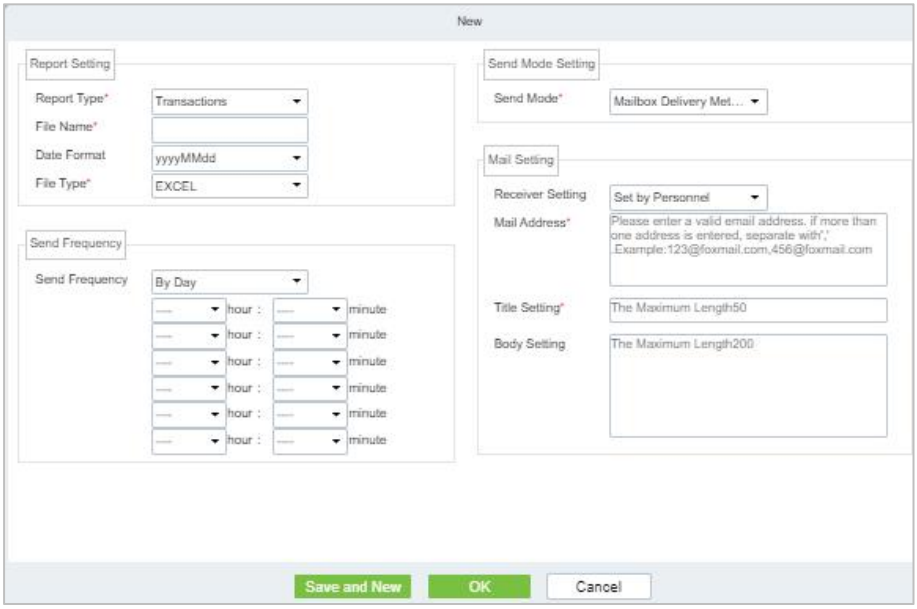


Figure 6- 31 Automatic Report

6.4.4.2Delete

Step 1: In the **Automatic Report** interface, select the required File from the list.

Step 2: Click **Delete** or click on the icon.to delete the required File from the list.

Step 3: Click **Delete**, to ensure and delete the selected File from the list.

6.4.4.3Enable/Disabled

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

6.4.5Process Settings

To achieve the approval function, it is necessary to maintain the relationship between positions at all levels in the personnel module and assign them to the corresponding personnel. Then setup the approval process for different process types and different positions.

6.4.5.1New

● Operating Steps:

Step 1: In the Attendance module, select **Attendance Settings > Process Settings** and click New.

Step 2: Click to **New** to configure all the details.

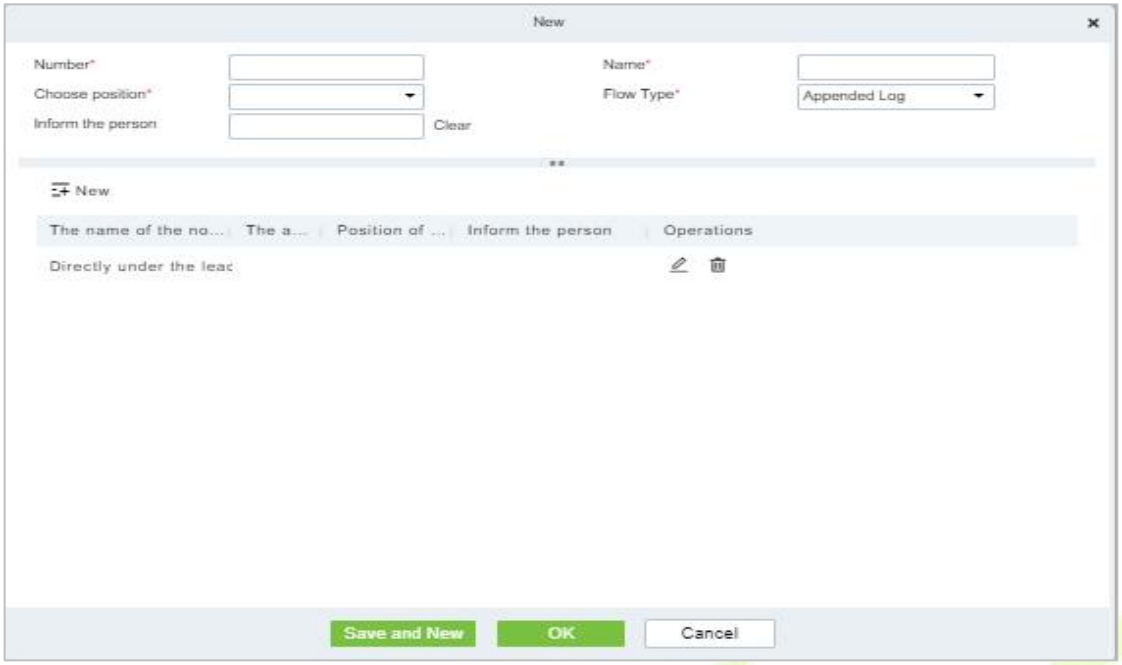


Figure 6- 32 Processing Setting

6.4.5.2Enable/Disabled

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

6.5 Regular Shift Setting Schedule

Regular shifts can choose one or more normal time periods to form a regular shift according to laws. Regular shifts are often used in regular occasions, such as office buildings, governments, banks, etc.

6.5.1Timetable

6.5.1.1Add Normal Timetable

This part introduces the configuration Steps of adding normal time period to the regular shift configuration of VAORIDA.

● Operating Steps:

Step 1: In the Attendance module, select **Schedule Management > Time Period** and click Add Normal Time Period.

Step 2: Configure the time period information in the **Add Normal Time** Period window, as shown in figure below. Please refer to Table 6-5 for the explanation of key parameters.

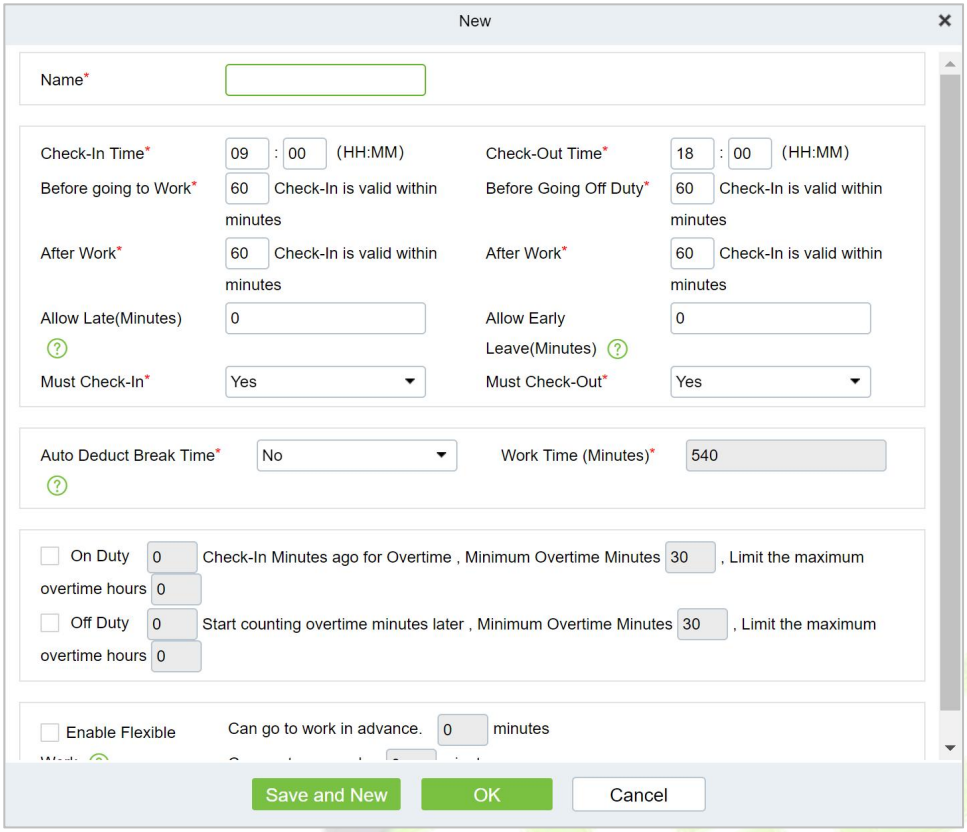


Figure 6- 33 New Time Period

Parameter	Description
Before/after work, 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.
Minutes allowed to be late/leave early	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.
You must sign in/return	In the selected time range, set whether you must sign in and sign out when going to and from work.
Whether it is deducted between segments	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.

Parameter	Description
Enable flexible hours to work	It refers to the flexible working parameter that people who go to work early can get off work early and people who work at night need to get off work late. When checked, you need to set the number of minutes that can be advanced/delayed, and it must be within the valid sign-in/sign-out time range.

Table 6- 5 Description of Key Parameters

Step 3: Click **OK**.

6.5.1.2Add Flexible Timetable

● Operating Steps:

Step 1: In the Attendance module, select **Schedule Management > Time Period** and click Add Flexible Timetable.

Step 2: Configure the time period information in the **Add Flexible Timetable** window.

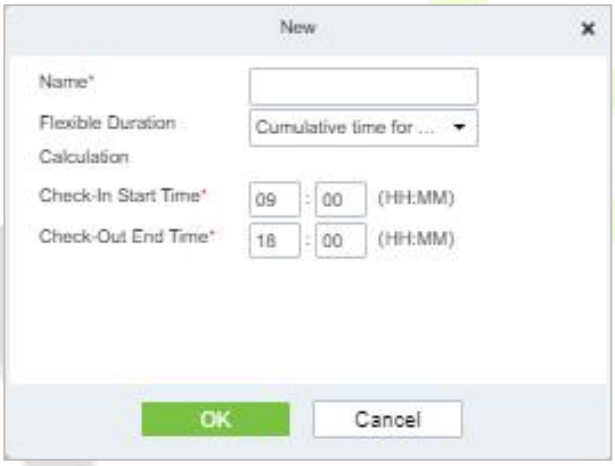


Figure 6- 34 Adding Flexible Time Table

6.5.1.3Delete

Step 1: In the **Timetable** interface, select the required Type from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Timetable Type from the list.

Step 3: Click **Delete**, to ensure and delete the selected Type from the list.

6.5.1.4Add Regular Shift

● Operating Steps:

Step 1: In the Attendance module, select '**Schedule Management > Shift**" and click "Add Regular Shift".

Step 2: Configure shift information in the "Add Regular Shift" window, as shown in figure below. Please refer to Table 6-6 for explanation of key parameters.

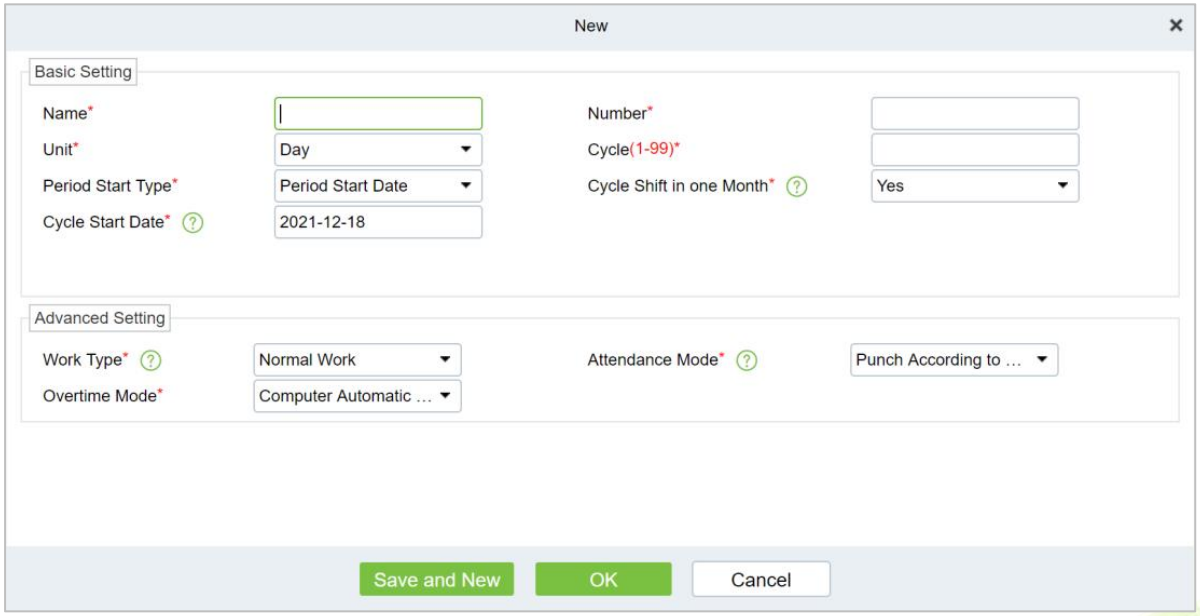


Figure 6- 35 New Shift

Parameter	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. • If the unit is "day", the range is 1 to 99. • If the unit is "week", the range is 1 to 15. • 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 • It is not displayed when the units are "week" and "month". • There is cycle start date and scheduling start date, and the default is cycle start date. • 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.
Type of work	• Normal work: This shift is a normal work shift • Overtime on rest days: This shift is overtime on rest days • Overtime on holidays: This shift is overtime on holidays.
Attendance mode	• Swipe the card normally according to the shift: the default item of the system, and punch in normally according to the punch in.

Parameter	Description
	• 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. • Punch-in-free: Setting this shift can avoid punch-in.
Overtime mode	• 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. • 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. • Not counting overtime: overtime hours are not counted for delayed overtime or overtime application.

Table 6- 6 Description of Key Parameters

Step 3: Click **OK**.

6.5.1.5Add Flexible Shift

Step 1: In the shift interface, click **Set Time Period** under the operation bar of the added regular shift, and configure the time period information in the pop-up **Set Time Period** window.

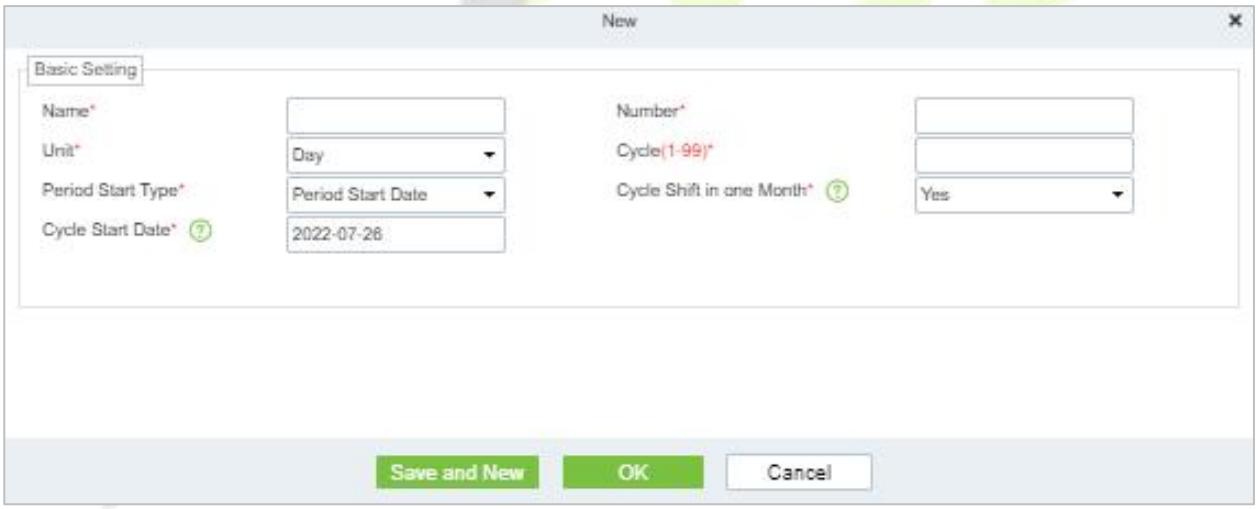


Figure 6- 36 Adding Flexible Shift

6.5.1.6Delete

Step 1: In the **Shift** interface, select the required Shift Type from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Shift Type from the list.

Step 3: Click **Delete**, to ensure and delete the selected Shift Type from the list.

6.5.1.7Clear Timetable

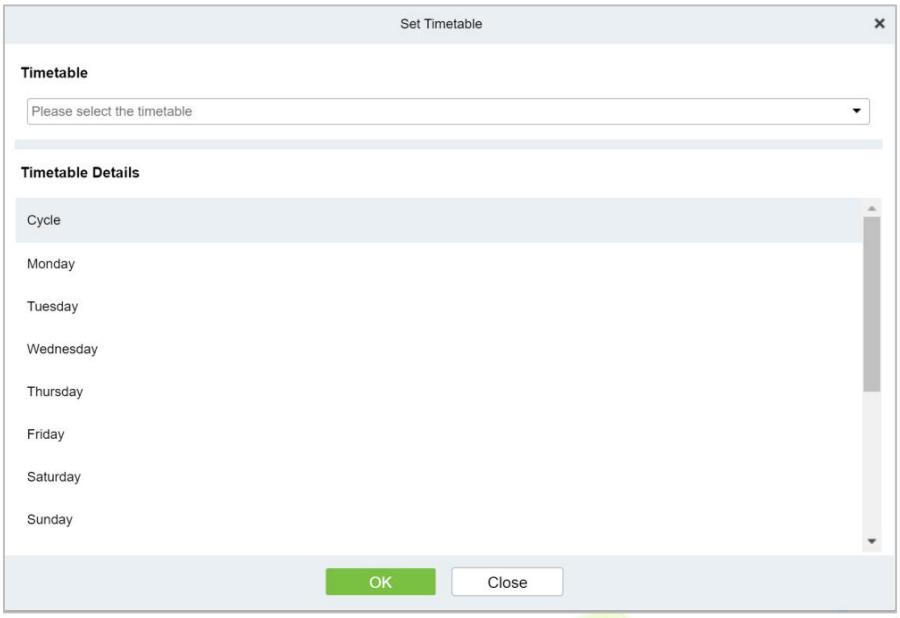


Figure 6- 37 Adding Time Periods

Step 6: Click **OK** to complete the addition of time period, and the specific time period is displayed in the time period details on the right.

6.5.2Personnel 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.

6.5.2.1Cycle Schedule

Step 1: In the Attendance module, select **Schedule Management** > **Personnel Schedule** and click Cycle Schedule.

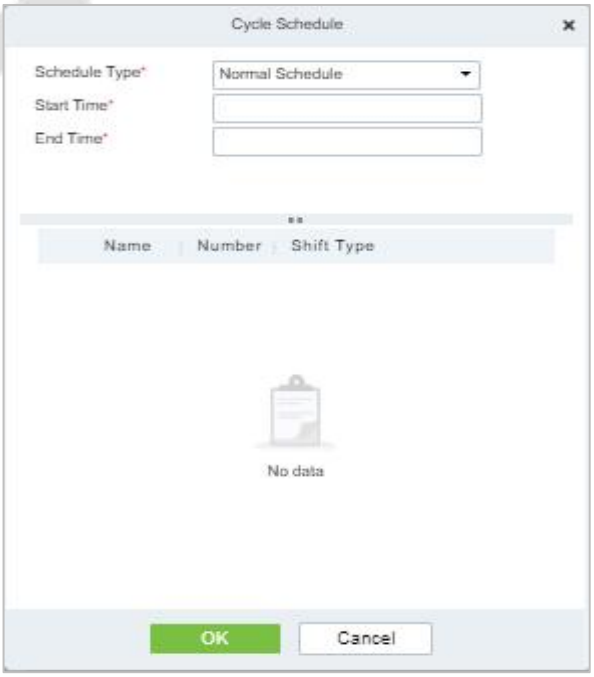


Figure 6- 38 Adding Personnel Schedule

6.5.2.2Temporary Schedule

Step 1: In the Attendance module, select **Schedule Management** > **Personnel Schedule** and click Temporary Schedule.

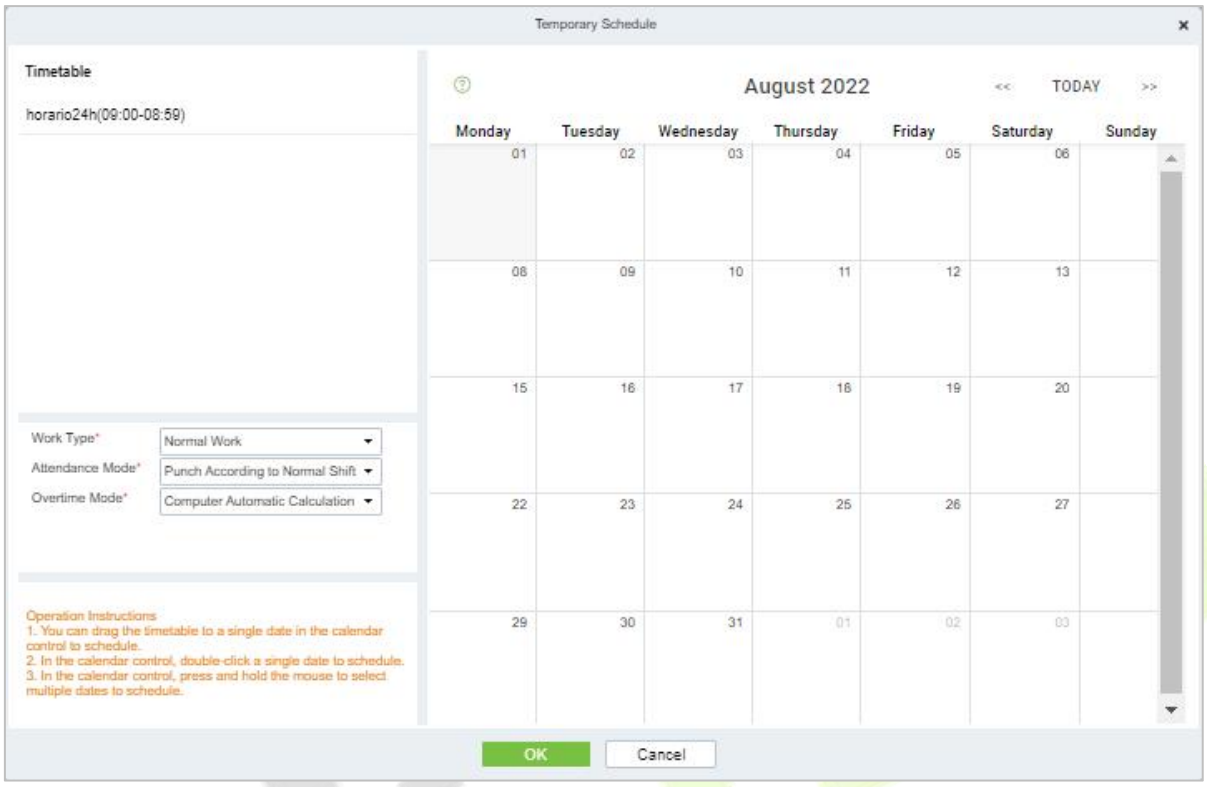


Figure 6- 39 Adding Temporary Schedule

6.5.2.3Clear Cycle Schedule

Step 1: In the **Attendance** module, select **Schedule Management** > **Personnel Schedule** and then click on the Personnel ID that you want to delete, and click **Clear Cycle Schedule**.

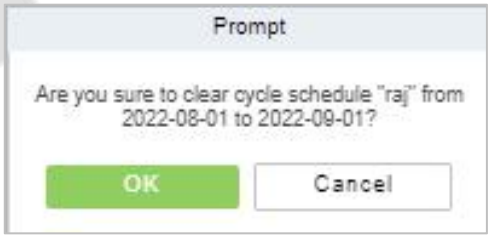


Figure 6- 40 Clear cycle schedule

6.5.2.4Clear Temporary Schedule

Step 1: In the **Attendance** module, select **Schedule Management** > **Personnel Schedule** and then click on the Personnel ID that you want to delete, and click **Clear Temporary Schedule**.

Figure 6- 41 Clear Temporary Schedule

6.5.3Group Schedule

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

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

6.5.3.1Edit Personnel for Group

New

Step 1: In the Attendance module, select **Schedule> Group Schedule** and click New.

Step 2: Configure the Schedule Name in the **Group Schedule** interface.

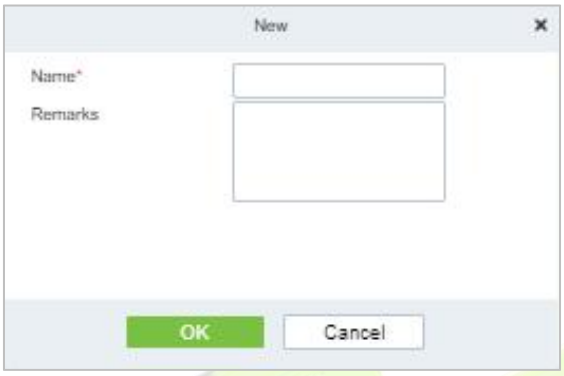


Figure 6- 42 Adding Elastic Time Period

Parameter	Description
Name	Can not contain special symbols, period name can not be duplicated, length is 30 characters, required.
Remarks	Mentioning comments.

Table 6- 7 Description of Key Parameters

Step 3: Click **OK**.

Delete

Step 1: In the **Schedule** interface, select the required Shift Type from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Shift Type from the list.

Step 3: Click **Delete**, to ensure and delete the selected Shift Type from the list.

6.5.3.2Browse the Group Personnel

Delete Personnel

Step 1: In the **Schedule** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

Cycle Schedule

Step 1: In the **Attendance** module, select **Scheduling Management > Personnel Scheduling**, check the personnel under the department that needs scheduling or the designated personnel, and click "Periodic Scheduling".

Step 2: Configure scheduling information in the pop-up **Cycle Scheduling** window, as shown in figure below. Please refer to Table 6-8 for parameter description.

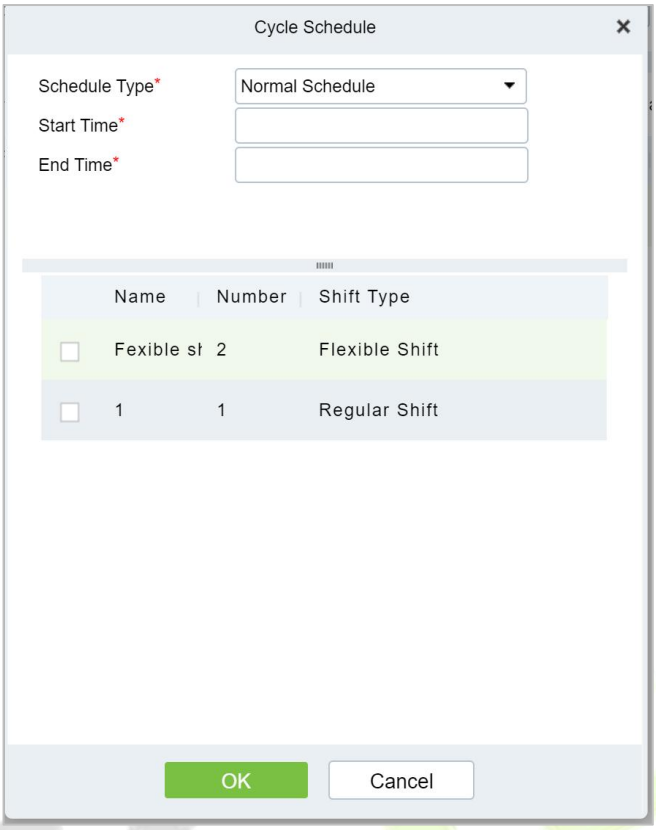


Figure 6- 43 Cycle Scheduling

Parameter	Description
Scheduling 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.

Table 6- 8 Description of Key Parameters of Cycle Scheduling

Step 3: Click **OK** to complete the configuration of personnel cycle scheduling.

Temporary Schedule

Step 1: In the **Attendance** module, select 's**cheduling Management > Personnel Scheduling**", check the personnel under the department that needs scheduling or the designated personnel, and click "Periodic Scheduling".

Step 2: Configure scheduling information in the pop-up **Temporary Schedule** window, as shown in figure below. Please refer to Table 6-9 for parameter description.

Step 3: Click **OK** to complete the configuration of temporary personnel scheduling

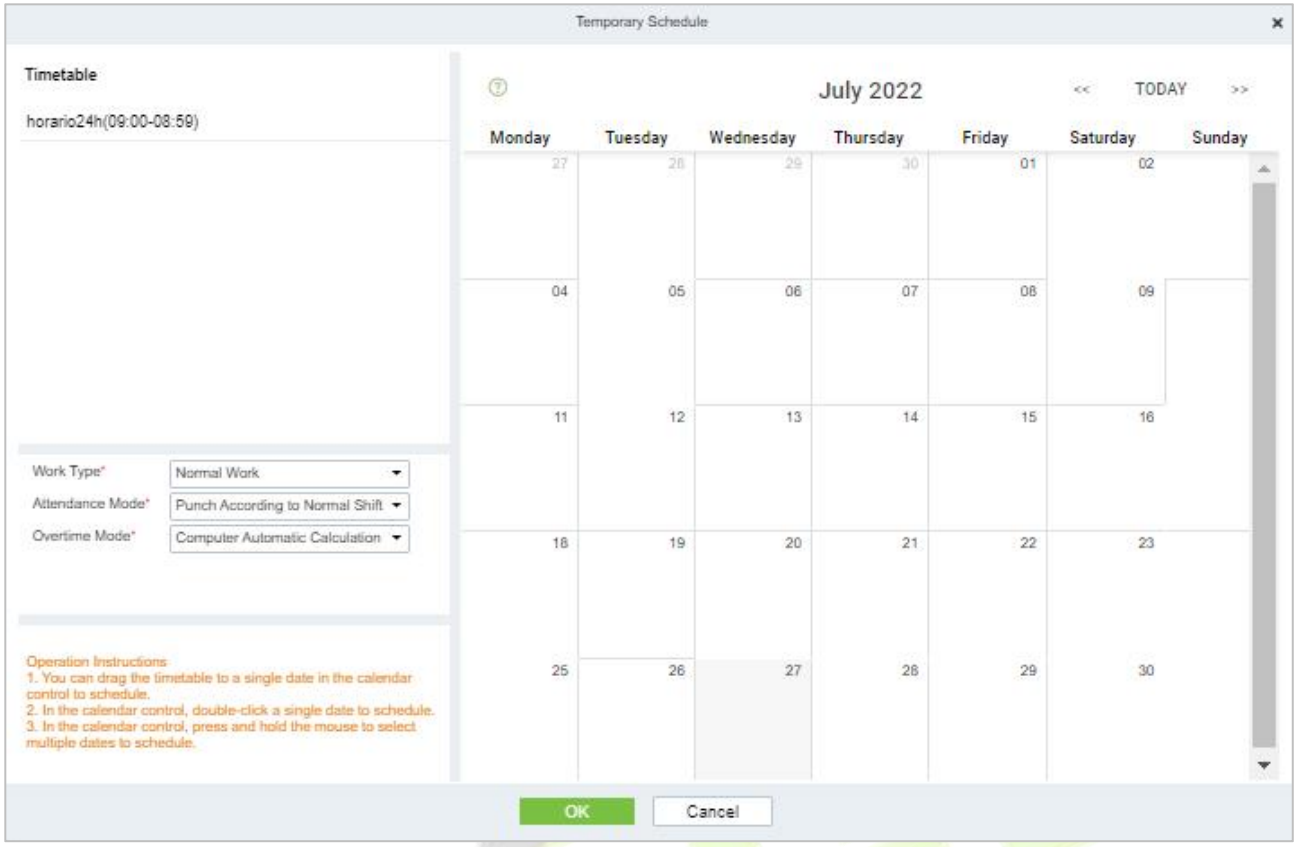


Figure 6- 44 Group Temporary schedule

Parameter	Description
Type of Work	• Normal work: This shift is a normal work shift. • Overtime on rest days: This shift is overtime on rest days. • Overtime on holidays: This shift is overtime on holidays.
Attendance Mode	• Swipe the card normally according to the shift: the default item of the system, and punch in normally according to the punch in • 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. • Punch-in-free: Setting this shift can avoid swiping cards.
Overtime Mode	• 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. • 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. • Not counting overtime: overtime hours are not counted for delayed overtime or overtime application.

Table 6- 9 Description of Key Parameters of Temporary Scheduling

Clear Cycle Schedule

Step 1: In the **Attendance** module, select **Scheduling Management > Personnel Scheduling**, check the personnel under the department that needs scheduling or the designated personnel, and click **Periodic Scheduling**.

Step 2: Configure scheduling information in the pop-up **Clear Cycle Schedule** window.

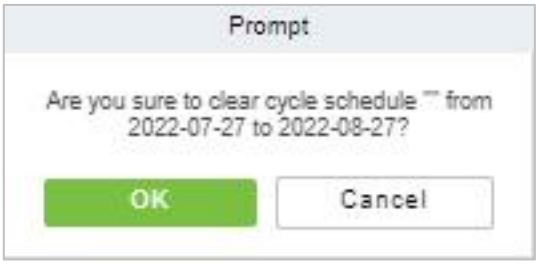


Figure 6- 45 Group Clear cycle Schedule

6.5.4Schedule Details

After setting the attendance time period and shift, you can schedule the personnel.

6.5.4.1Delete

Step 1: In the **Schedule** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.5.4.2Export

You can export all transactions in Excel, PDF, CSV format

6.6 Exception

6.6.1Manual Check - in

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.

6.6.1.1New

● Operating Steps:

Step 1: In the Attendance module, select **Exception Management > Manual Check - in** and click Add.

Step 2: Configure the card replacement information in the pop-up **Add** window, first select the "Department" where the person to be resigned is located, then select the person to be resigned, and finally enter the date and time of the card replacement.

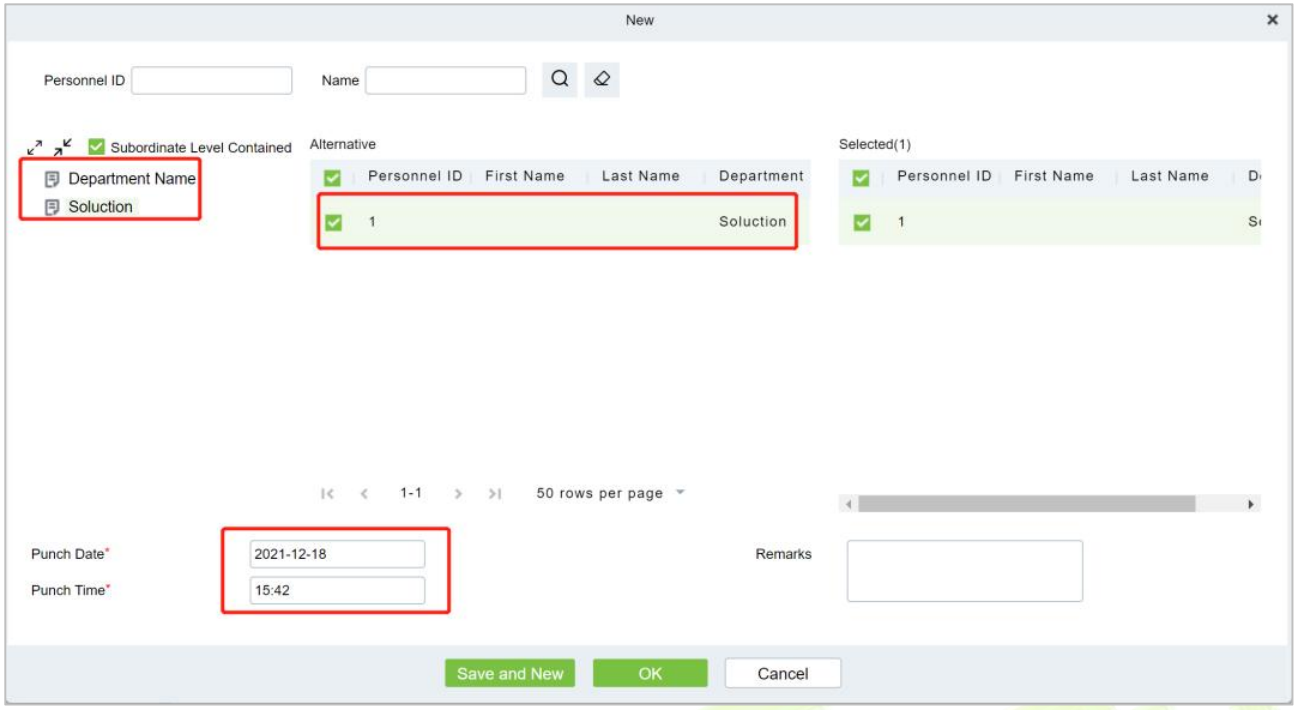


Figure 6- 46 Replacement Card

Step 3: Click **OK**.

6.6.1.2Delete

Step 1: In the **Appended Log** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.1.3Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.1.4Export

You can export all logs in Excel, PDF, CSV format.

6.6.1.5Import

You can import all logs in Excel, PDF, CSV format.

6.6.2Leave

When encountering special circumstances, people may need to take time off for different reasons, and hope that the time off can be displayed in the system statistics.

6.6.2.1New

● Operating Steps:

Step 1: In the Attendance module, select **Exception Management > Leave** and click New.

Step 2: Configure the leave form information in the pop-up **Add** window, first select the "Department"

where the person to take leave is located, then select the leave person, finally enter the leave time, and optionally upload the leave attachment.

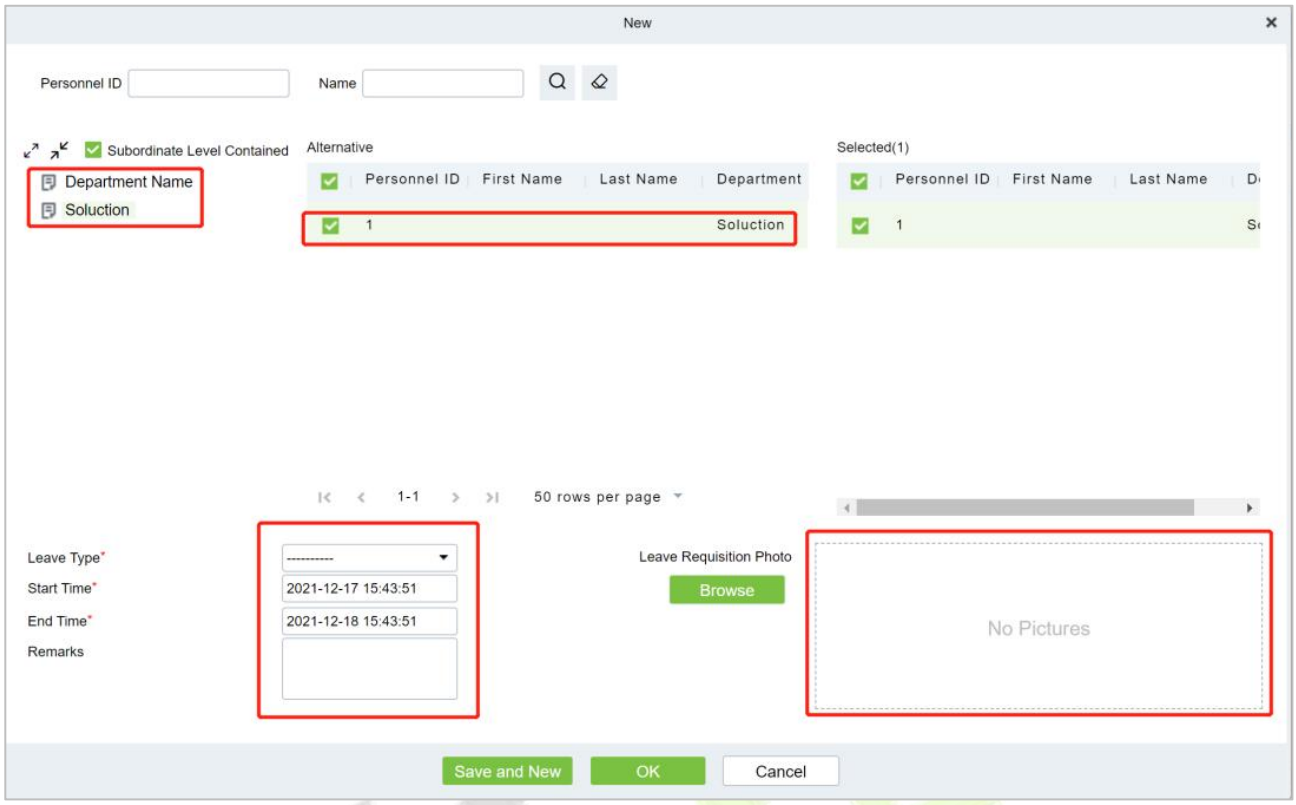


Figure 6- 47 Leave Request Form

Step 3: Click **OK**.

6.6.2.2Delete

Step 1: In the **Leave** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.2.3Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.2.4Export

You can export all logs in Excel, PDF, CSV format.

6.6.2.5Import

You can import all logs in Excel, PDF, CSV format.

6.6.3Overtime

6.6.3.1New

Step 1: In the Attendance module, select **Exception Management > Overtime** and click New.

Step 2: Configure overtime form information in the pop-up **Add** window, first select the "Department"

where the person to work overtime is located, then select the overtime person, and finally enter overtime hours.

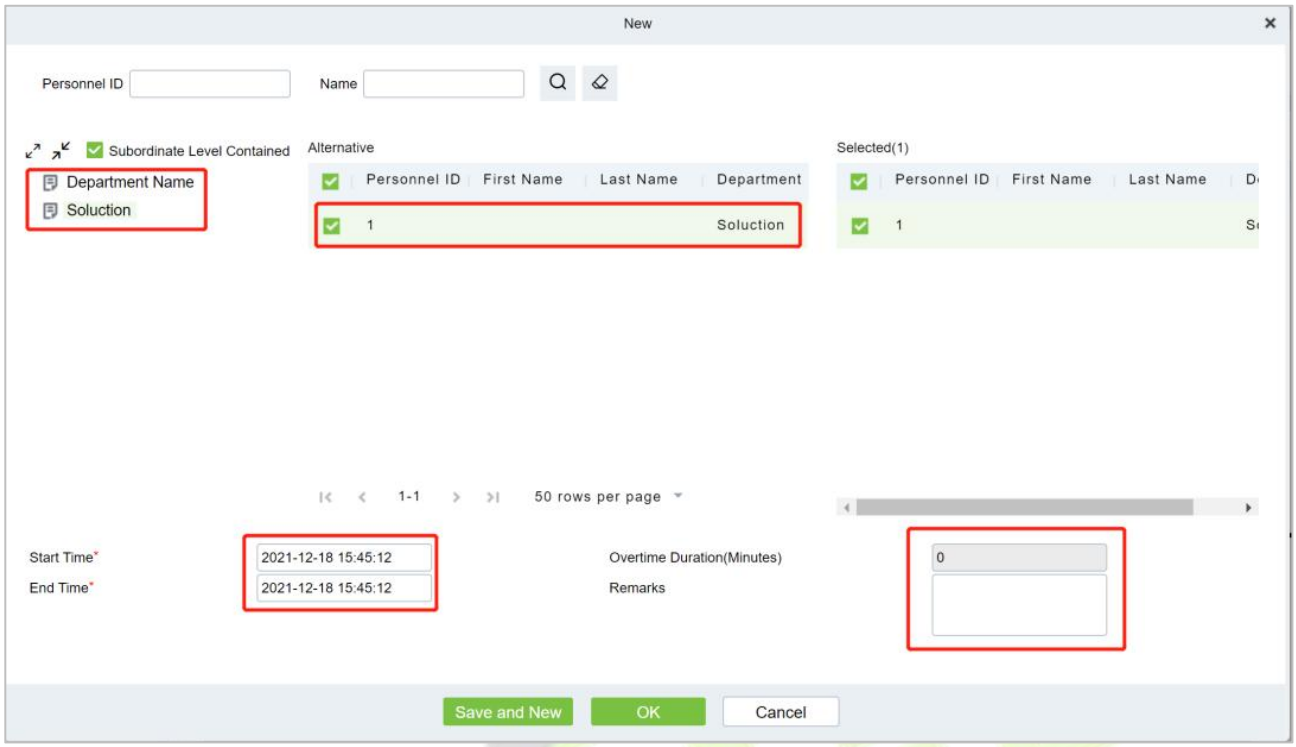


Figure 6- 48 Overtime Form

Step 3: Click **OK**.

6.6.3.2Delete

Step 1: In the **Overtime** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.3.3Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.3.4Export

You can export all logs in Excel, PDF, CSV format.

6.6.3.5Import

You can import all logs in Excel, PDF, CSV format.

6.6.4Adjust Rest

6.6.4.1New

●Operating Steps:

Step 1: In the Attendance module, select **Exception Management > Leave Adjustment** and click New.

Step 2: In the pop-up **Add** window, configure the information of the leave adjustment form, first select

the "Department" of the person to be transferred, then select the person to be transferred, and finally enter the leave adjustment time.

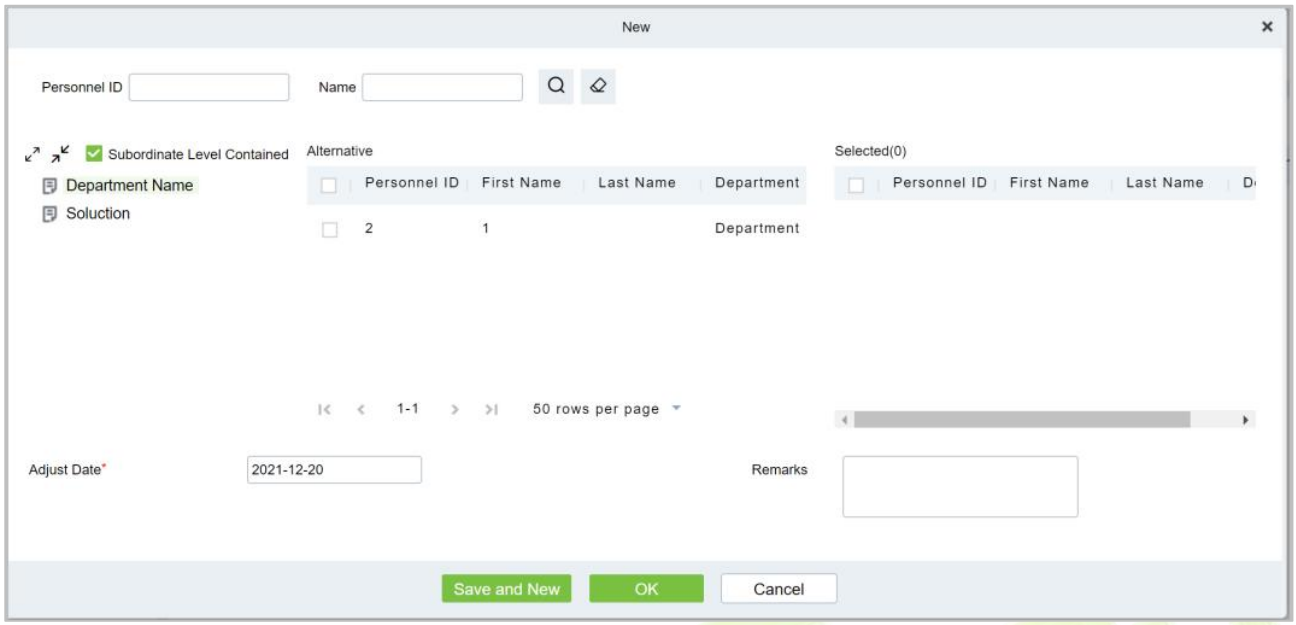


Figure 6- 49 Leave Adjustment Form

Step 3: Click **OK**.

6.6.4.2Delete

Step 1: In the **Adjust Rest** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.4.3Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.4.4Export

You can export all logs in Excel, PDF, CSV format.

6.6.4.5Import

You can import all logs in Excel, PDF, CSV format.

6.6.5Shift Adjustment

6.6.5.1New

●Operating Steps:

Step 1: In the Attendance module, select **Exception Management > Shift Adjustment** and click New.

Step 2: In the pop-up **Add** window, configure the shift adjustment list information, first enter the shift adjustment "Personnel Number", then select "shift Adjustment Date", and finally select "shift Adjustment Name".

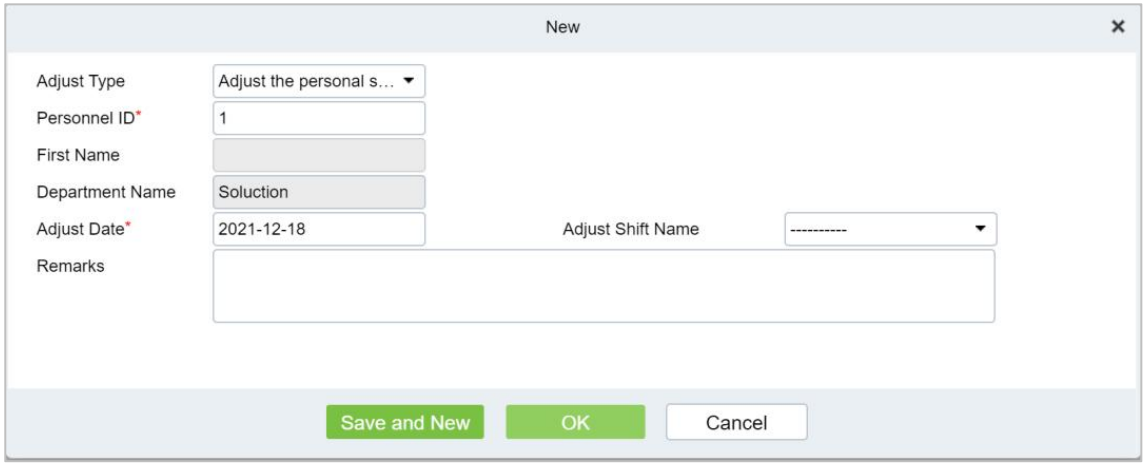


Figure 6- 50 Leave Adjustment Form

Step 3: Click **OK**.

6.6.5.2 Delete

Step 1: In the **Adjust Shift** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.5.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.5.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.5.5 Import

You can import all logs in Excel, PDF, CSV format.

6.7 Attendance Detail Report

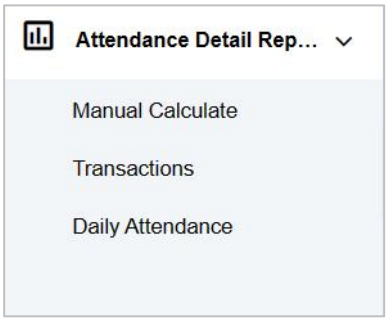


Figure 6- 51

6.7.1 Manual Calculate

In the Attendance Report, you can review an individual's clock-in record and verify their attendance

status through attendance calculation. If the status is accurate, it indicates that the attendance business configuration is complete.

● Operating Steps:

Step 1: In **Attendance** Module, select **Detailed Report > Manual Calculation**, check the person who needs to perform attendance calculation, and click **Attendance Calculation**.

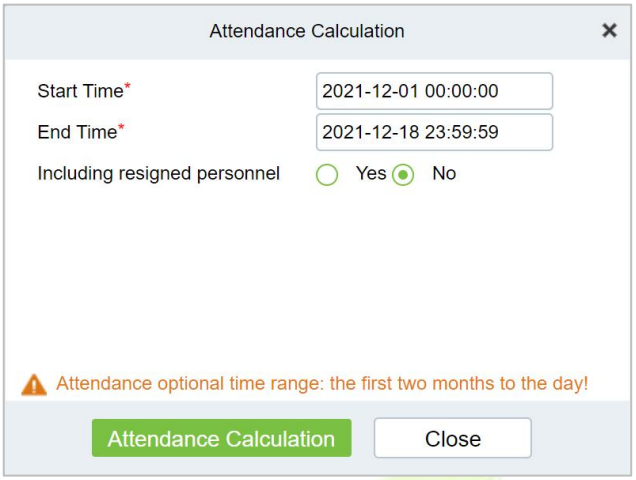


Figure 6- 52 Manual Calculation

6.7.2Transactions

This interface will display attendance records for all employees, including those from uploaded attendance transactions. The original record for a normal punch on the device will be uploaded to the software. When a specific data point is selected, its details will be shown on the right side of the page.

● Operating Steps:

Step 1: In the Attendance module, select **Detailed Report > Transaction**.

Step 2: In the original record table interface, fill in the corresponding query information, and click the **Query** symbol to complete the query of all record tables.

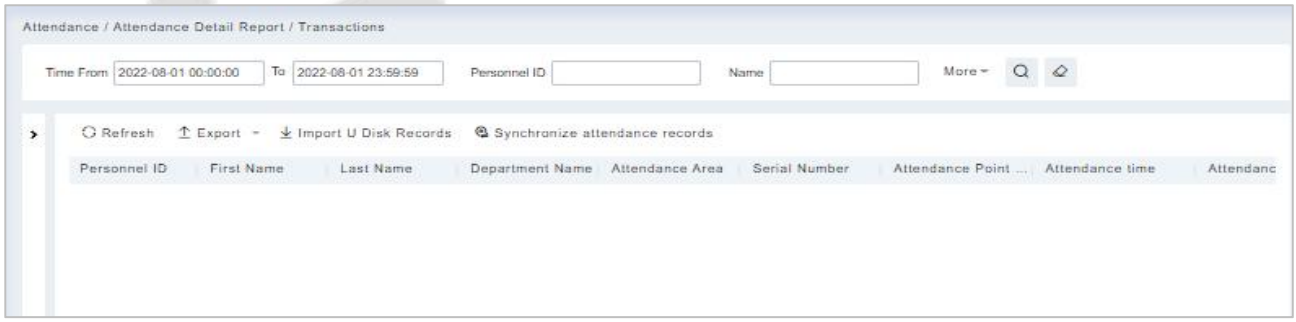


Figure 6- 53 Report Query Interface

Export:

Step 1: In the original record table interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

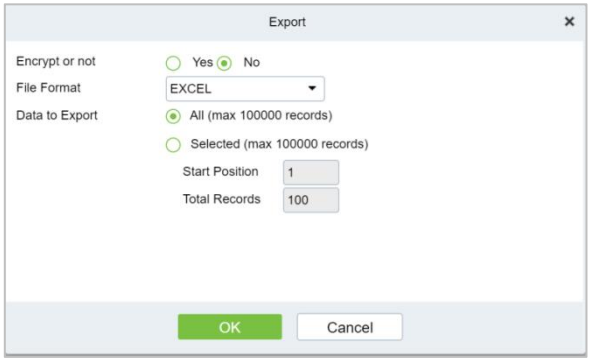


Figure 6- 54 Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

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**.

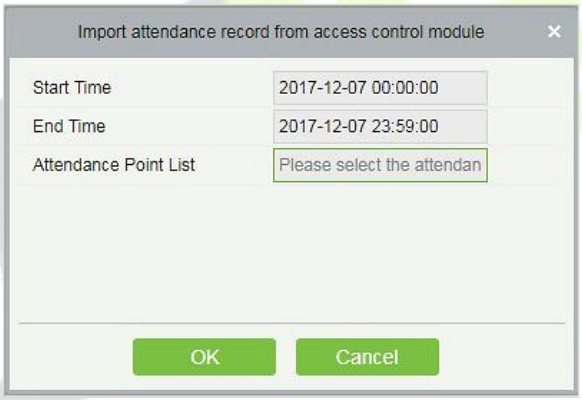


Figure 6- 55 Synchronize Attendance Records

6.7.3Daily 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.

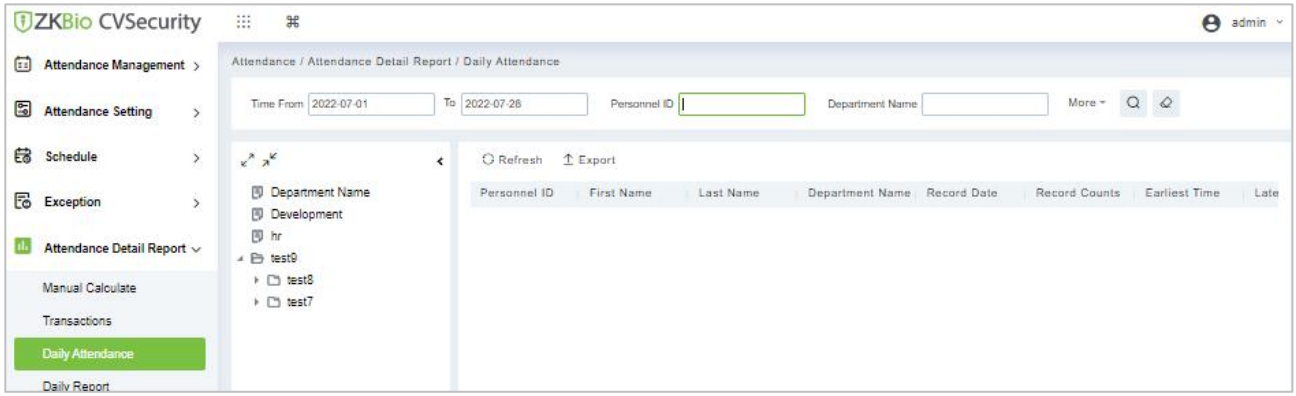


Figure 6- 56 Daily Attendance

6.8 Daily Attendance Report

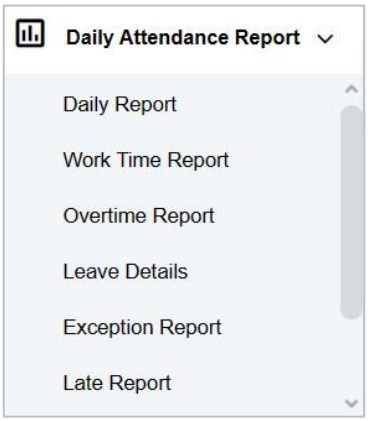


Figure 6- 57 Daily Attendance Report Interface

6.8.1 Daily Report

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.

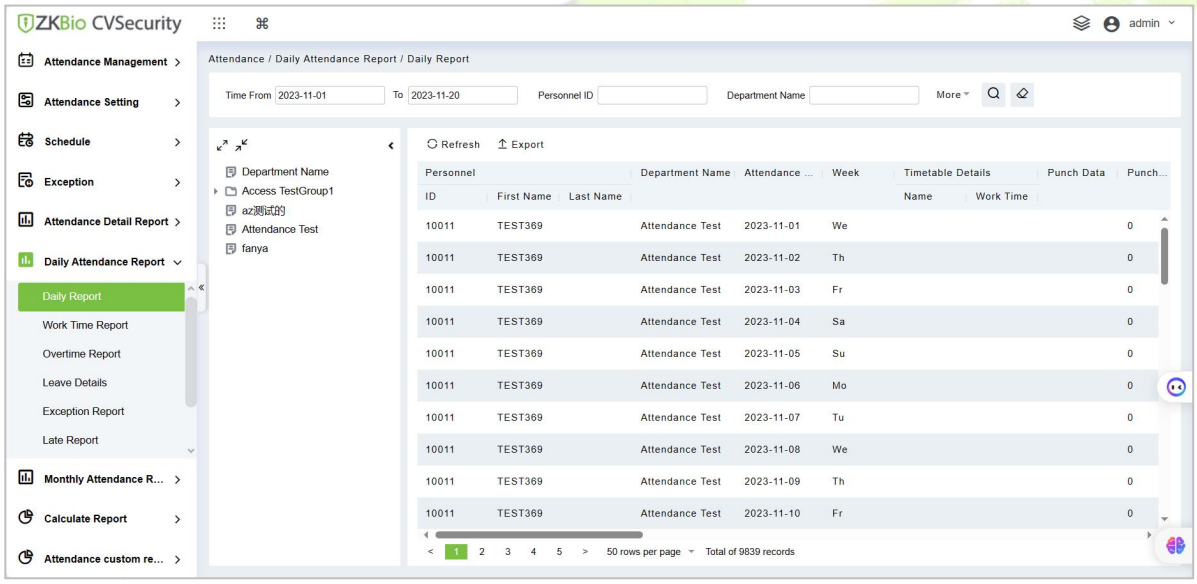


Figure 6- 58 Daily Report Interface

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

Figure 6- 59 Report Export Interface

6.8.2Work Time Report

These interfaces display the personnel's work data, including actual work time and overtime data, and allow for the export of the data.

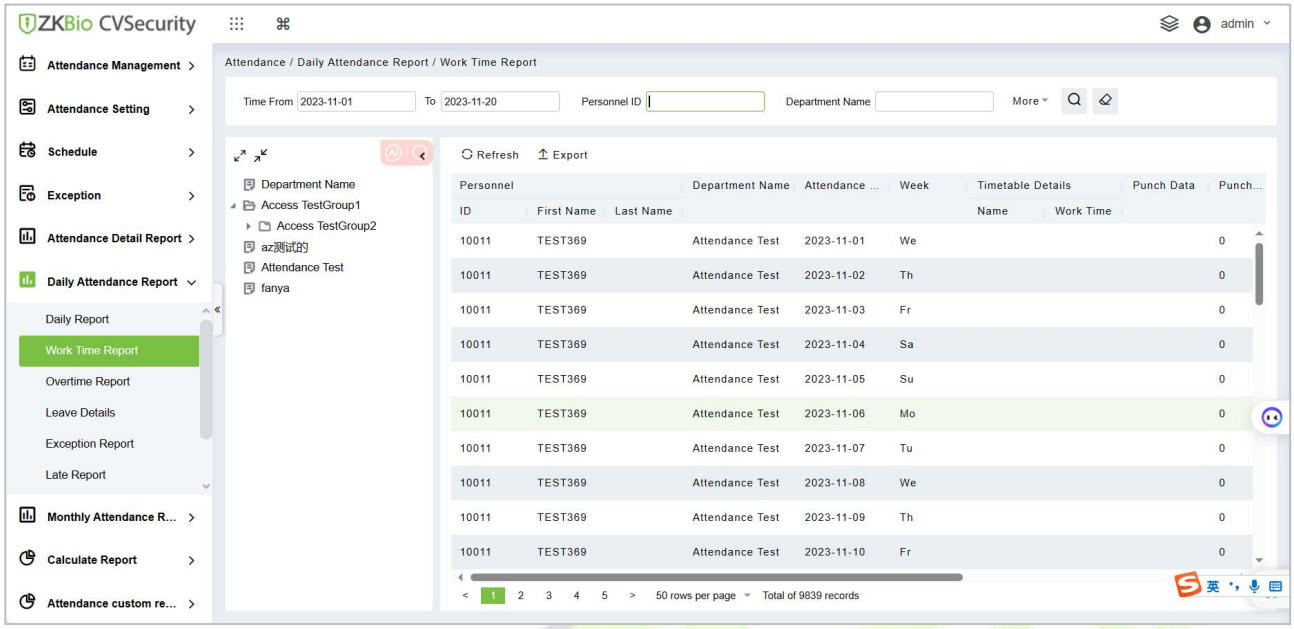


Figure 6- 60 Work Time Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

Work Time Report

Personnel			epartment Nam	ttendance Dat	Week	Timetable Details		Punch Data	Punch Counts	Expected/Actual(minute)			Overtime(hour)			
ID	First Name	Last Name				Name	Work Time			Should	Actual	Valid	Weekday	Weekend	Holiday	Total
10011	TEST369		Attendance	2023-11-01	We				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-02	Th				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-03	Fr				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-04	Sa				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-05	Su				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-06	Mo				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-07	Tu				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-08	We				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-09	Th				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-10	Fr				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-11	Sa				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-12	Su				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-13	Mo				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-14	Tu				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-15	We				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-16	Th				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-17	Fr				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-18	Sa				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
10011	TEST369		Attendance	2023-11-19	Su				0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Figure 6- 61 Report Export Interface

6.8.3Overtime Report

The Overtime report interface displays the overtime work hours of the personnel and allows for the export of the details.

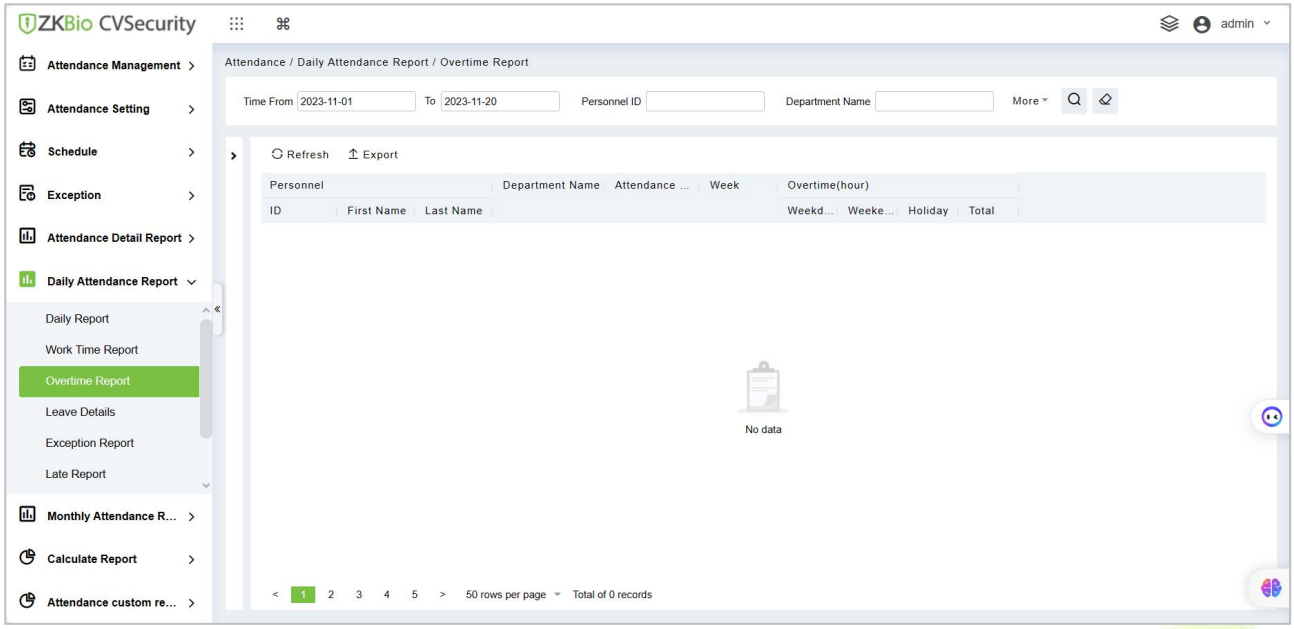


Figure 6- 62 Overtime Report Interface

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.8.4 Leave Details

Personnel can apply for leave, and the requests will be displayed here.

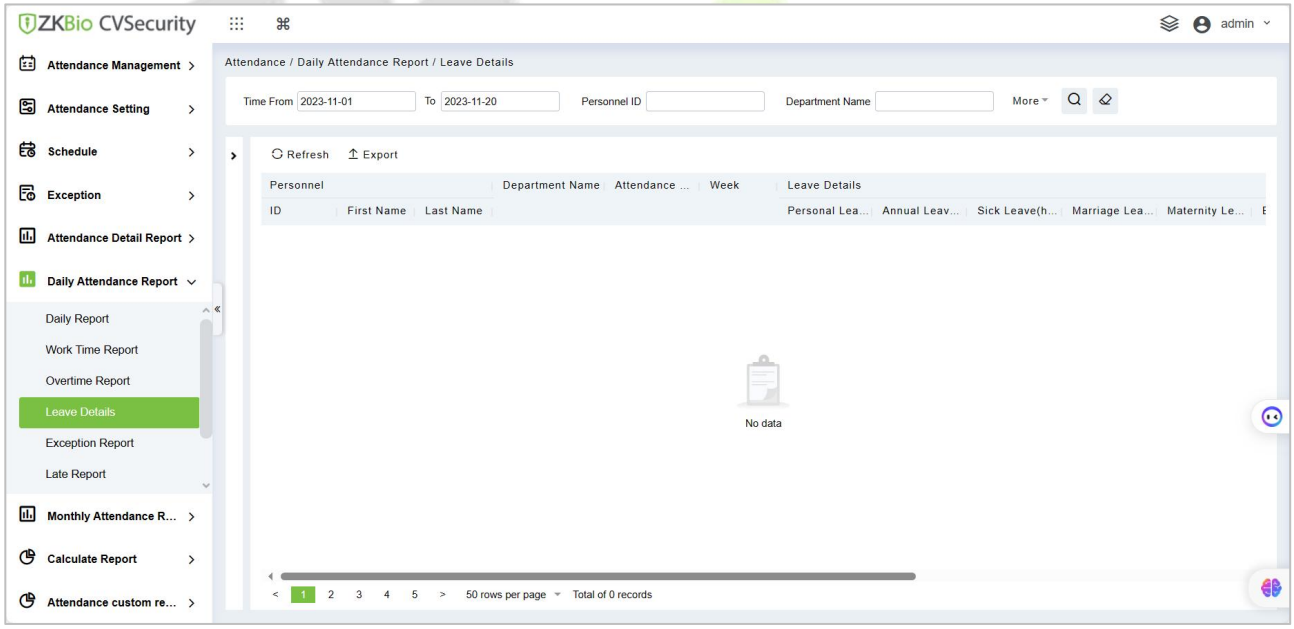


Figure 6- 63 Leave Details Interface

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.8.5 Exception Report

It displays all the attendance exceptions like misses in and out punches.

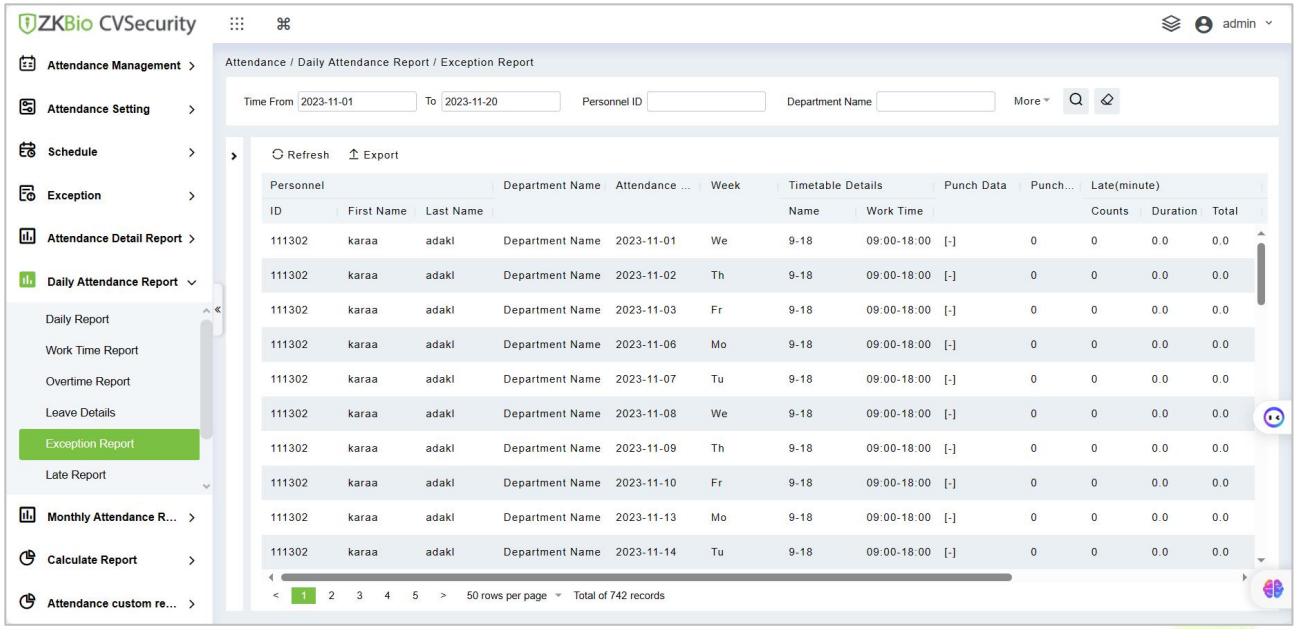
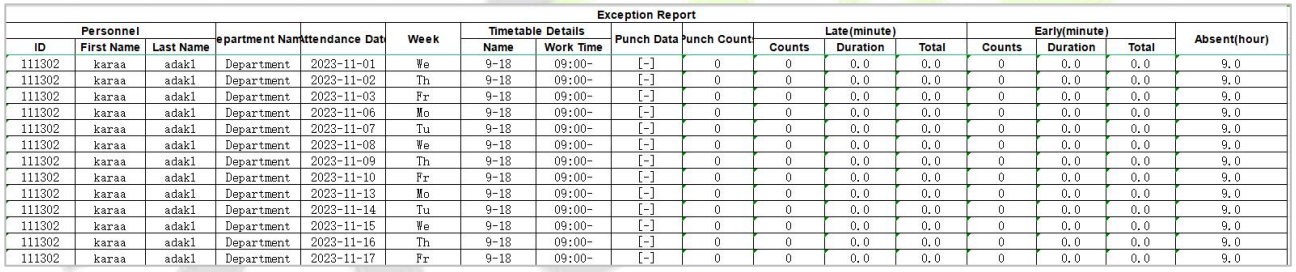


Figure 6- 64 Exception Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.



Exception Report

Personnel			epartment Nam	ttendance Dat	Week	Timetable Details		Punch Data	Punch Count	Late(minute)			Early(minute)			Absent(hour)
ID	First Name	Last Name				Name	Work Time			Counts	Duration	Total	Counts	Duration	Total	
111302	karaa	adakl	Department	2023-11-01	We	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-02	Th	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-03	Fr	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-06	Mo	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-07	Tu	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-08	We	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-09	Th	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-10	Fr	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-13	Mo	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-14	Tu	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-15	We	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-16	Th	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0
111302	karaa	adakl	Department	2023-11-17	Fr	9-18	09:00-	[-]	0	0	0.0	0.0	0	0.0	0.0	9.0

Figure 6- 65 Report Export Interface

6.8.6 Late Report

The list displays the late arrival time of the employees.

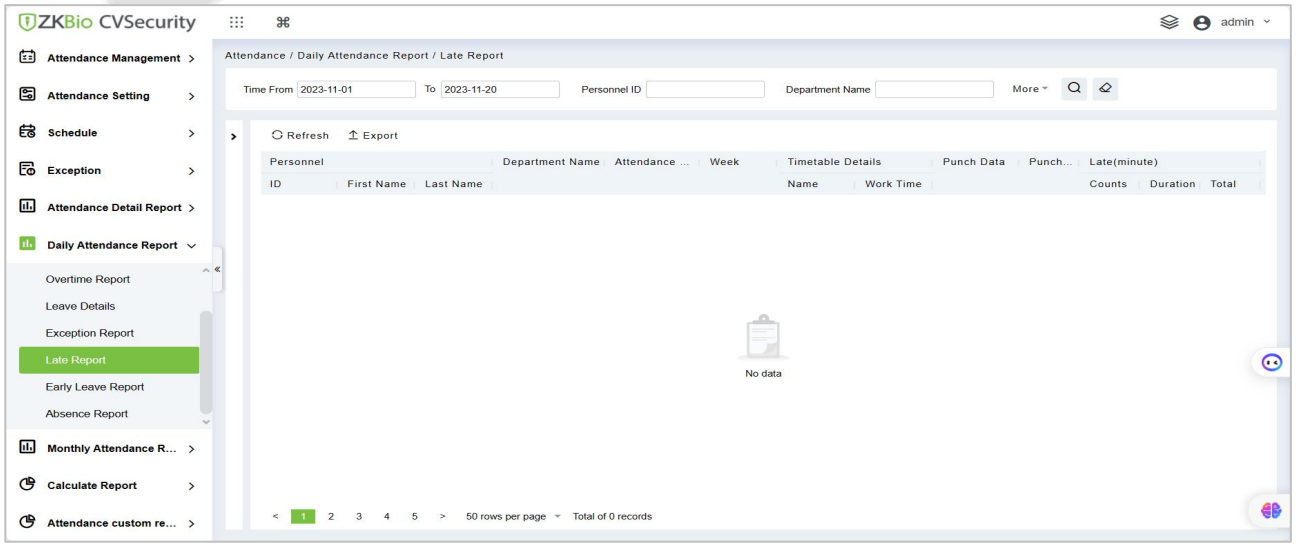


Figure 6- 66 Late Report Interface

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.8.7Early Leave Report

The list shows the time of the early leave of the employees.

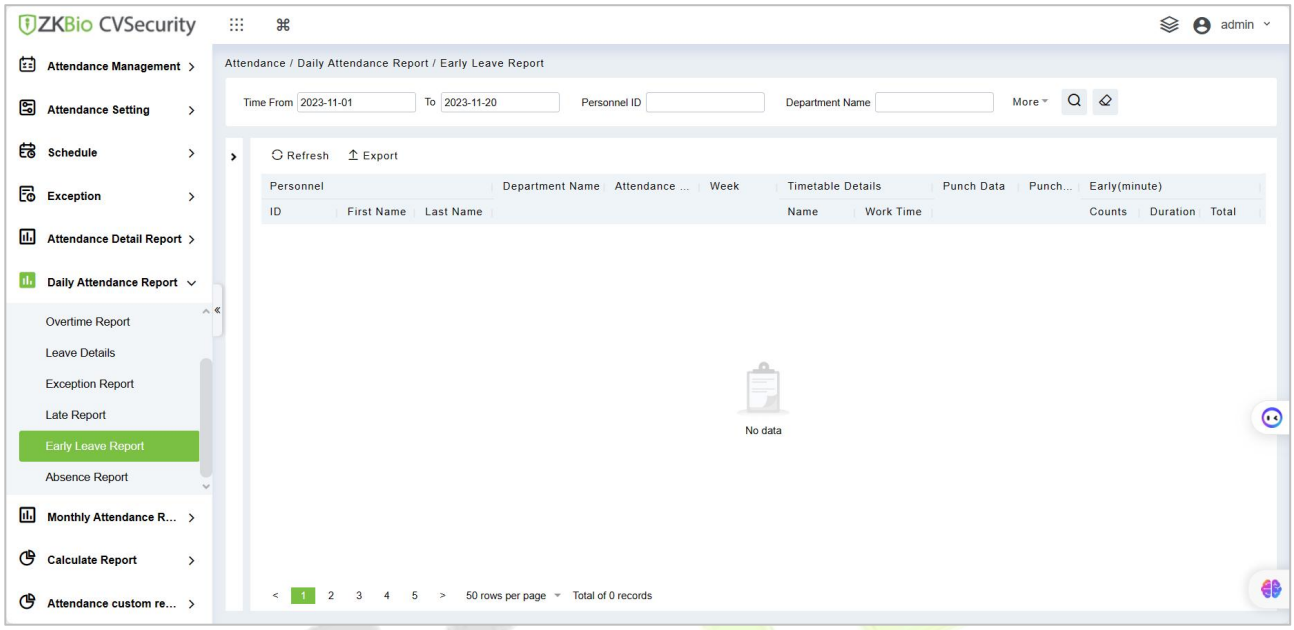


Figure 6- 67

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.8.8 Absence Report

The list displays the late arrival, early leave, and absent details of the employees.

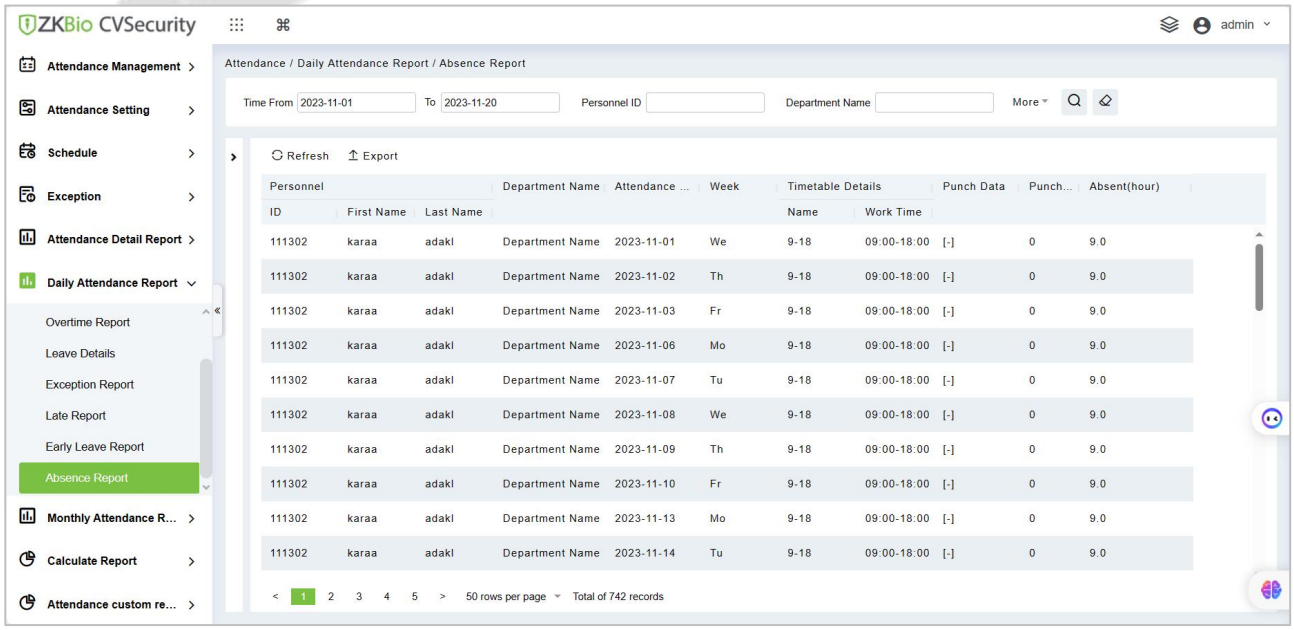


Figure 6- 68 Absence Report Interface

Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.9 Monthly Attendance Report

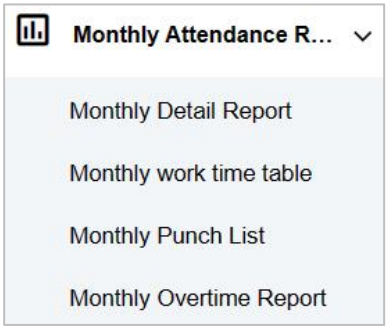


Figure 6- 69

6.9.1 Monthly Detail Report

The Monthly Detail Report is used to analyse the entire attendance of all the employees in that month. It includes Present hours, Absent hours, Holidays, Weekly-off and shifts so on

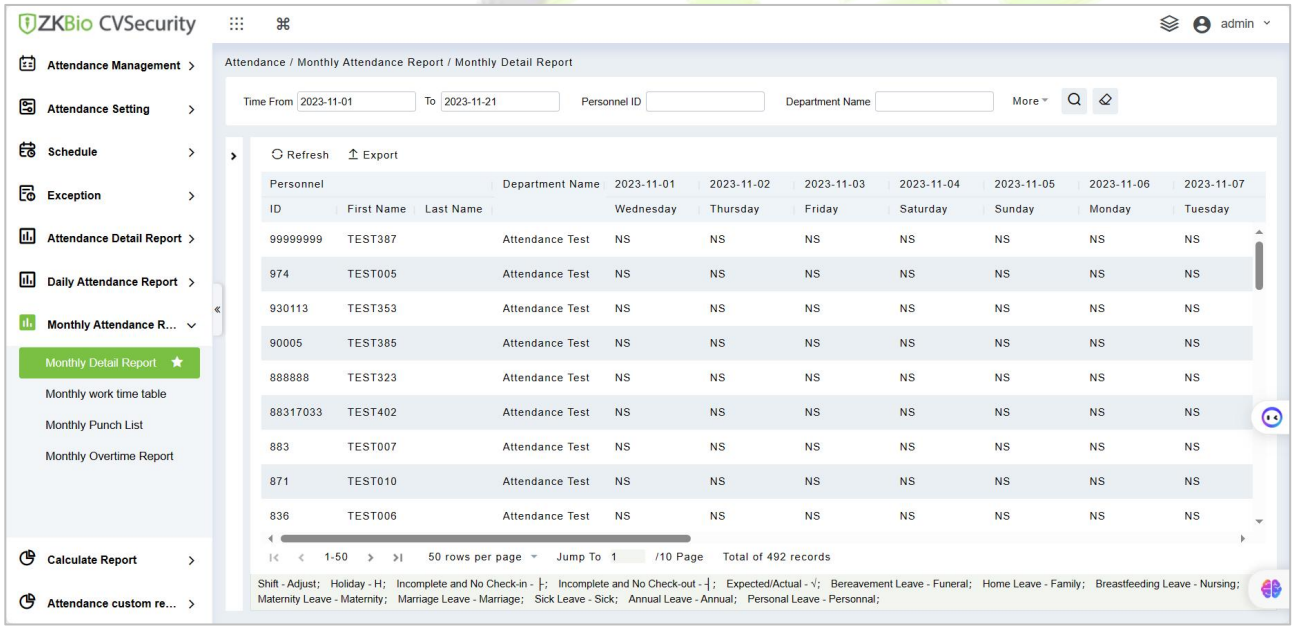


Figure 6- 70 Monthly Detail Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

Monthly Detail Report

Personnel			Department Name	2023-11-01	2023-11-02	2023-11-03	2023-11-04	2023-11-05	2023-11-06	2023-11-07	2023-11-08	2023-11-09	2(
ID	First Name	Last Name		Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	
99999999	TEST387		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
974	TEST005		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
930113	TEST353		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
90005	TEST385		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
888888	TEST323		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
88317033	TEST402		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
883	TEST007		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
871	TEST010		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
836	TEST006		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
80233	TEST008		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
8023	TEST009		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
7777777	TEST350		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
7658	TEST352		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	
67890	TEST347		Attendance Test	NS	NS	NS	NS	NS	NS	NS	NS	NS	

Figure 6- 71 Monthly Details Report

6.9.2Monthly Work Time

The monthly work time report gives the details of attendance status, Clock-in time, Clock-out time and the total worked hours.

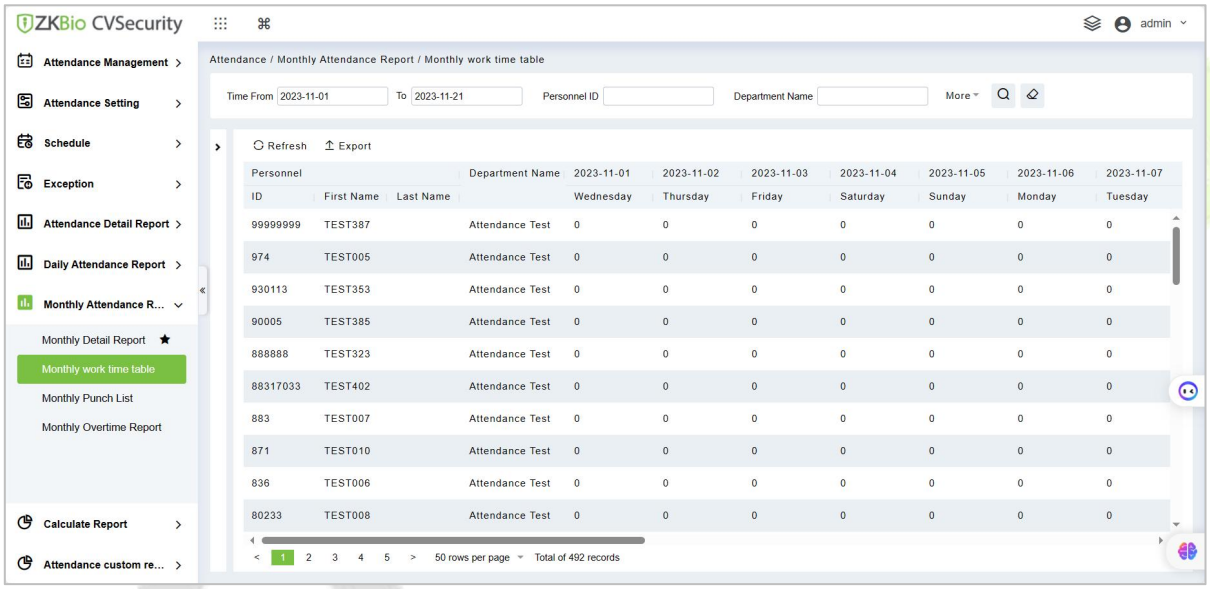


Figure 6- 72 Monthly Work Time Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

Monthly work time table

Personnel			epartment Nar	2023-11-01	2023-11-02	2023-11-03	2023-11-04	2023-11-05	2023-11-06	2023-11-07	2023-11-08	2023-11-09	2023-11-10	2023-11-11	2023-11-12
ID	First Name	Last Name		Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
99999999	TEST387		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
974	TEST005		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
930113	TEST353		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
90005	TEST385		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
888888	TEST323		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
88317033	TEST402		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
883	TEST007		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
871	TEST010		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
836	TEST006		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
80233	TEST008		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
8023	TEST009		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
7777777	TEST350		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
7658	TEST352		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
67890	TEST347		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
6666666	TEST391		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
6629	TEST115		Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60061			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60060			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60059			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60058			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60057			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60056			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60055			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60054			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60053			Attendance	0	0	0	0	0	0	0	0	0	0	0	0
60052			Attendance	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6- 73 Export Report Interface

6.9.3Monthly Punch List

The monthly punch Report displays the attendance details namely Status, Clock-in, Clock-out, Early Leave, Late coming, assigned to each employee.

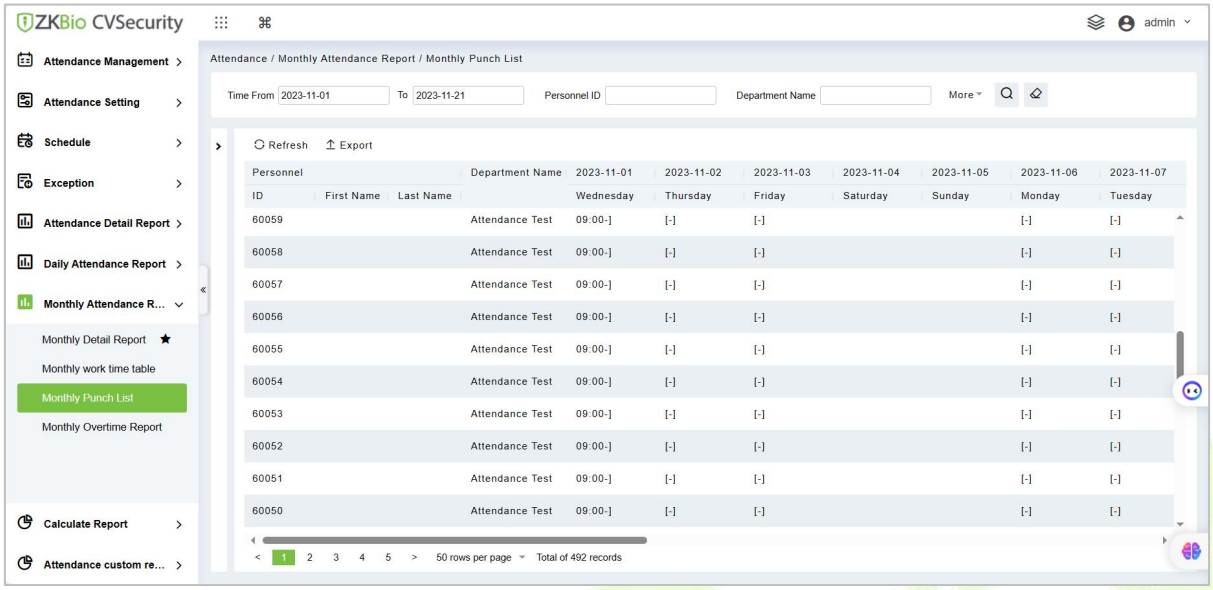


Figure 6- 74 monthly Punch Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

Monthly Punch List																				
Personnel				2023-11-01	2023-11-02	2023-11-03	2023-11-04	2023-11-05	2023-11-06	2023-11-07	2023-11-08	2023-11-09	2023-11-10	2023-11-11	2023-11-12	2023-11-13	2023-11-14	2023-11-15
ID	First Name	Last Name		Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday
99999999	TEST387		Attendanc															
974	TEST005		Attendanc															
930113	TEST353		Attendanc															
90005	TEST385		Attendanc															
888888	TEST323		Attendanc															
88317033	TEST402		Attendanc															

Figure 6- 75 Export Report Interface

6.9.4Monthly Overtime Report

The Overtime Summary Report displays the overtime hours worked by the employees.

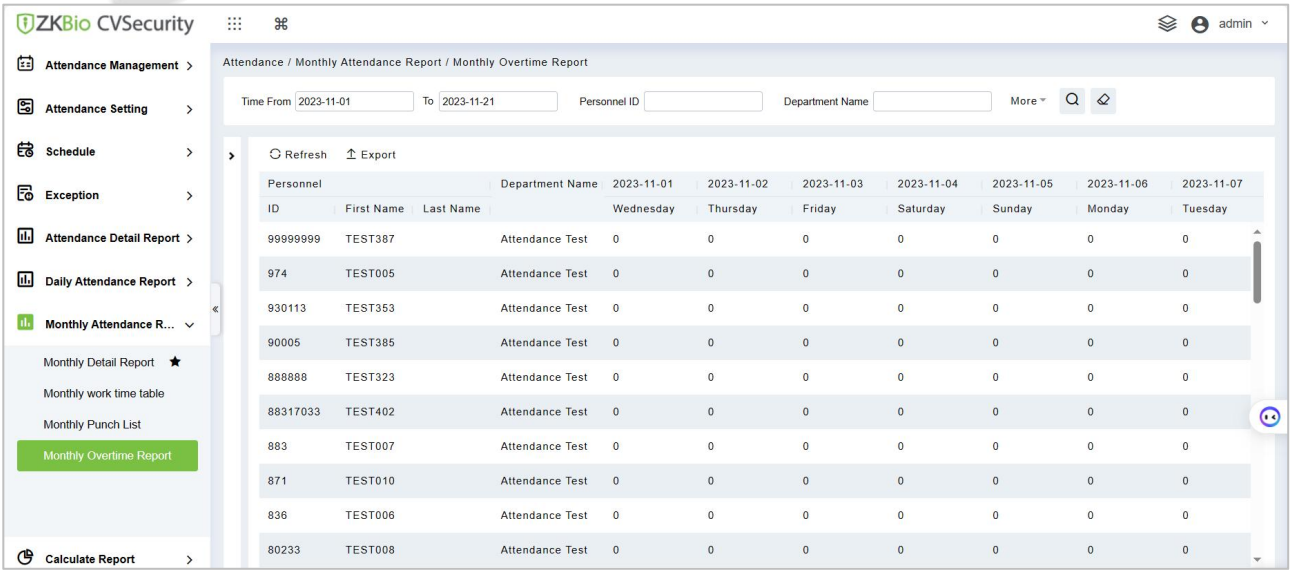
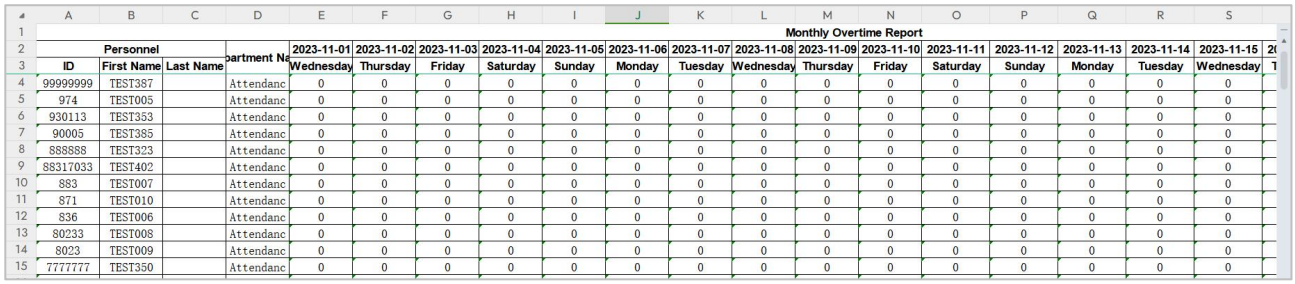


Figure 6- 76 Monthly Overtime Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Monthly Overtime Report																		
2	Personnel			Department Name	2023-11-01	2023-11-02	2023-11-03	2023-11-04	2023-11-05	2023-11-06	2023-11-07	2023-11-08	2023-11-09	2023-11-10	2023-11-11	2023-11-12	2023-11-13	2023-11-14	2023-11-15
3	ID	First Name	Last Name		Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday	Wednesday
4	99999999	TEST387		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	974	TEST005		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	930113	TEST353		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	90005	TEST385		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	888888	TEST323		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	88317033	TEST402		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	883	TEST007		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	871	TEST010		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	836	TEST006		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	80233	TEST008		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	8023	TEST009		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	7777777	TEST350		Attendanc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 6- 77 Export Report Interface

6.10 Calculate Report

6.10.1 Monthly Staff Report

The Attendance Status Summary report is used to analyse the entire attendance status of all the employees in that month. It includes Present hours, Absent hours, Holidays, Weekly-off and so on.

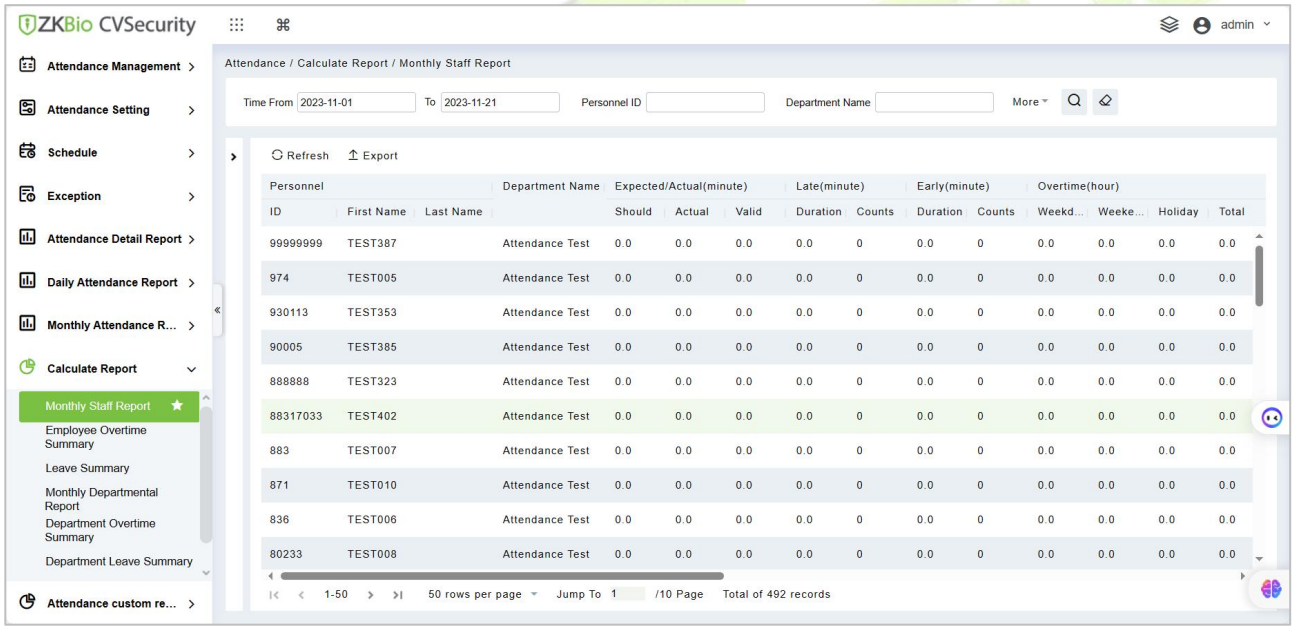
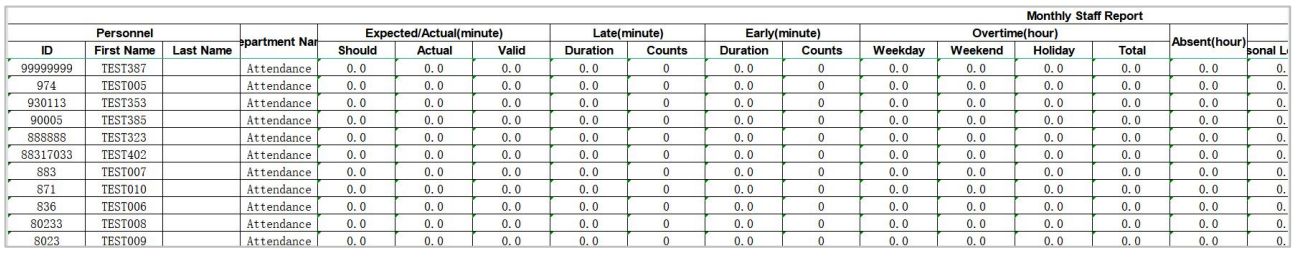


Figure 6- 78 Monthly Staff Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.



Monthly Staff Report																		
Personnel			Department Name	Expected/Actual(minute)			Late(minute)		Early(minute)		Overtime(hour)				Absent(hour)	
ID	First Name	Last Name		Should	Actual	Valid	Duration	Counts	Duration	Counts	Weekday	Weekend	Holiday	Total		
99999999	TEST387		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
974	TEST005		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
930113	TEST353		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
90005	TEST385		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
888888	TEST323		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
88317033	TEST402		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
883	TEST007		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
871	TEST010		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
836	TEST006		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
80233	TEST008		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.
8023	TEST009		Attendance	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0	0.0	0.0	0.

Figure 6- 79 Export Report Interface

6.10.2Employee Overtime Summary

The Overtime Summary Report displays the overtime hours worked by the employees.

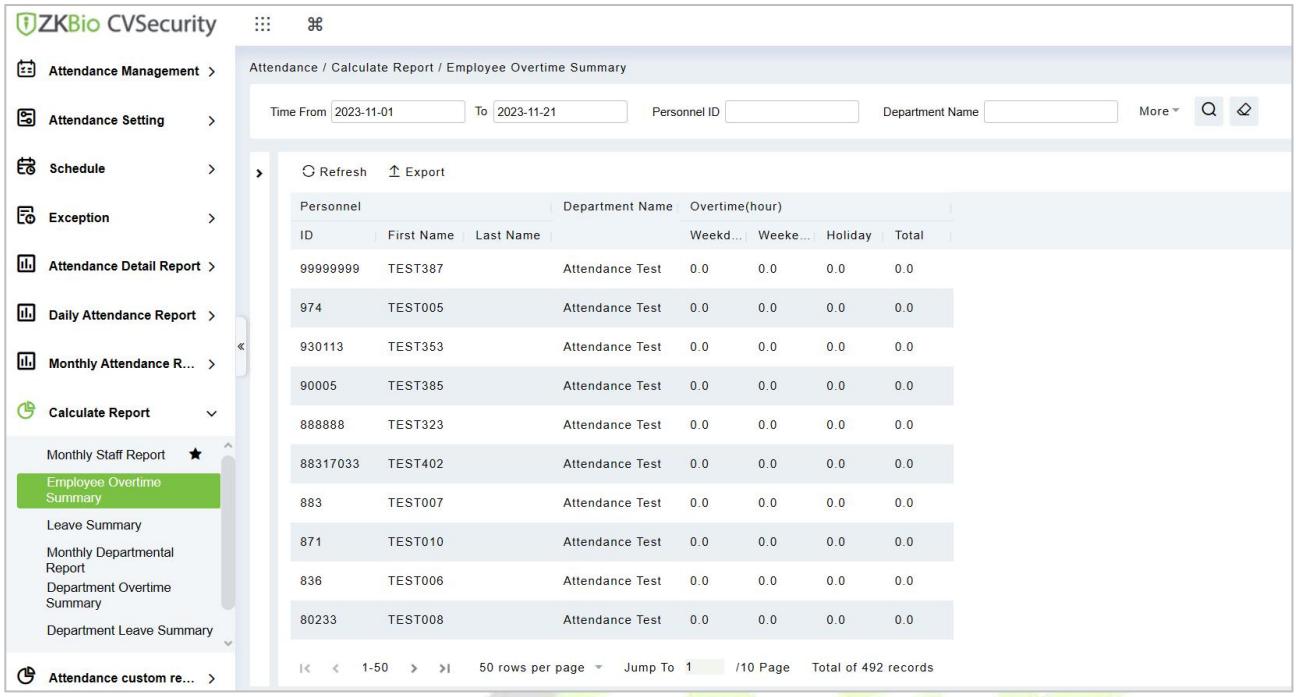


Figure 6- 80 Employee Overtime Summary Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.10.3Leave Summary

The leave summary displays the total leaves taken by the employees. It includes sick leave, casual leave, parental leave, annual leave, compassionate leave, and more. The procedure to view the leave summary is the same as the Employee Summary

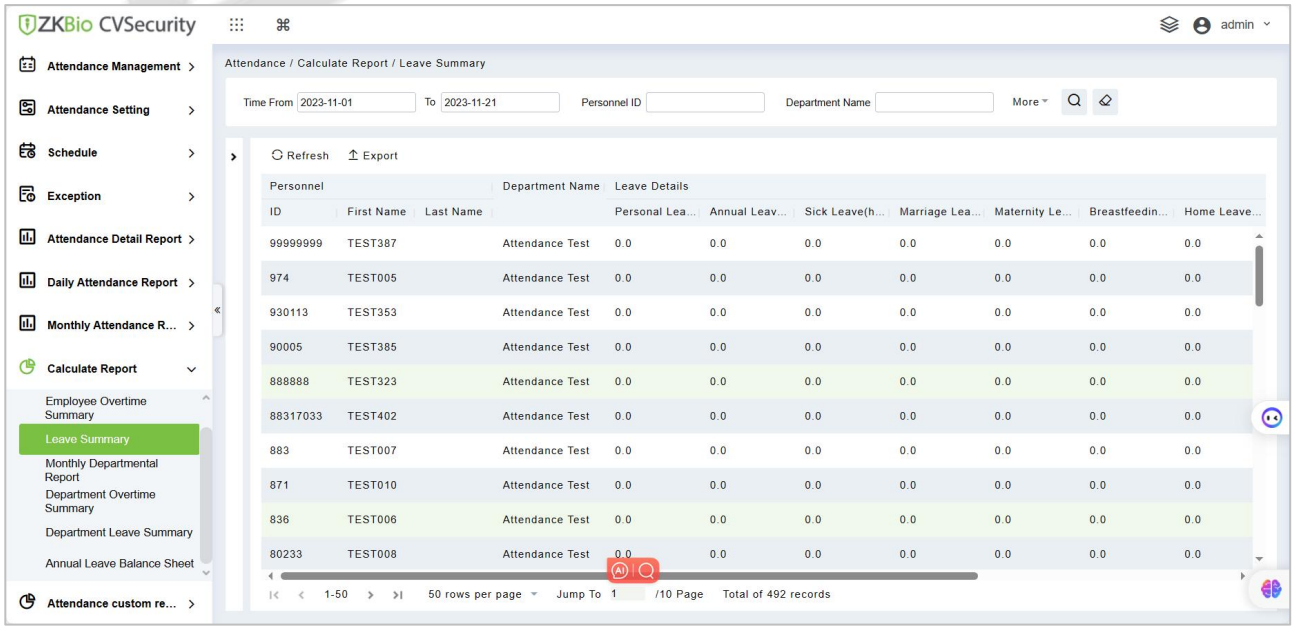


Figure 6- 81 Leave Summary Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.10.4Monthly Department Report

The Department Summary displays all the data of a department including the number of employees, late arrivals, leaves, absents, and more(count). The procedure to view the department summary is the same as the Employee Summary.

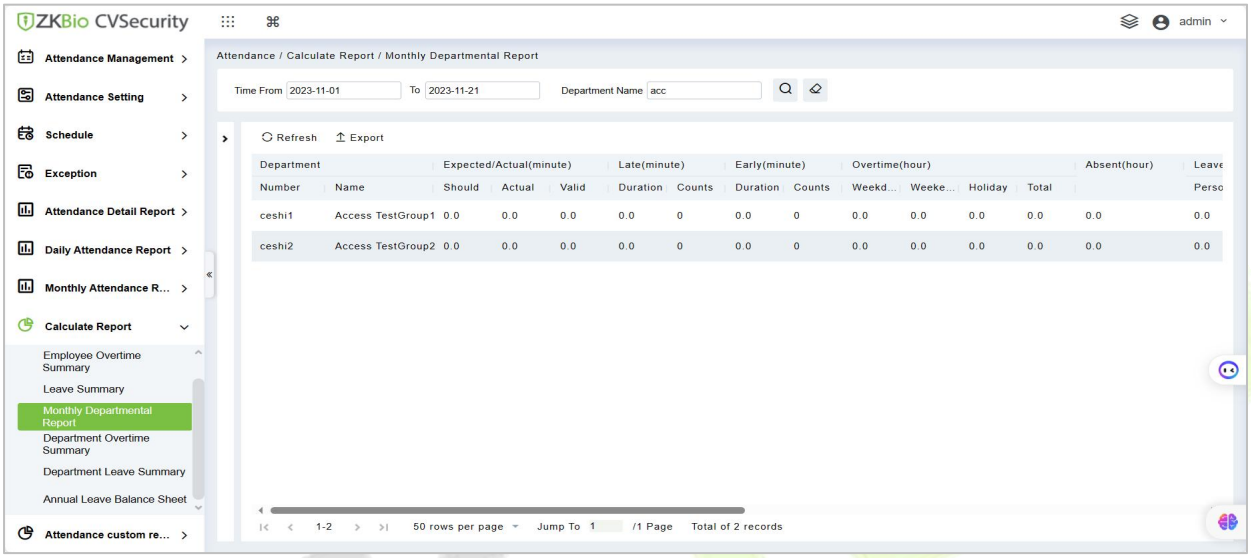


Figure 6- 82 Monthly Department Summary Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.10.5Department Overtime Summary

The Overtime Summary Report displays the overtime hours worked by the employees in a department.

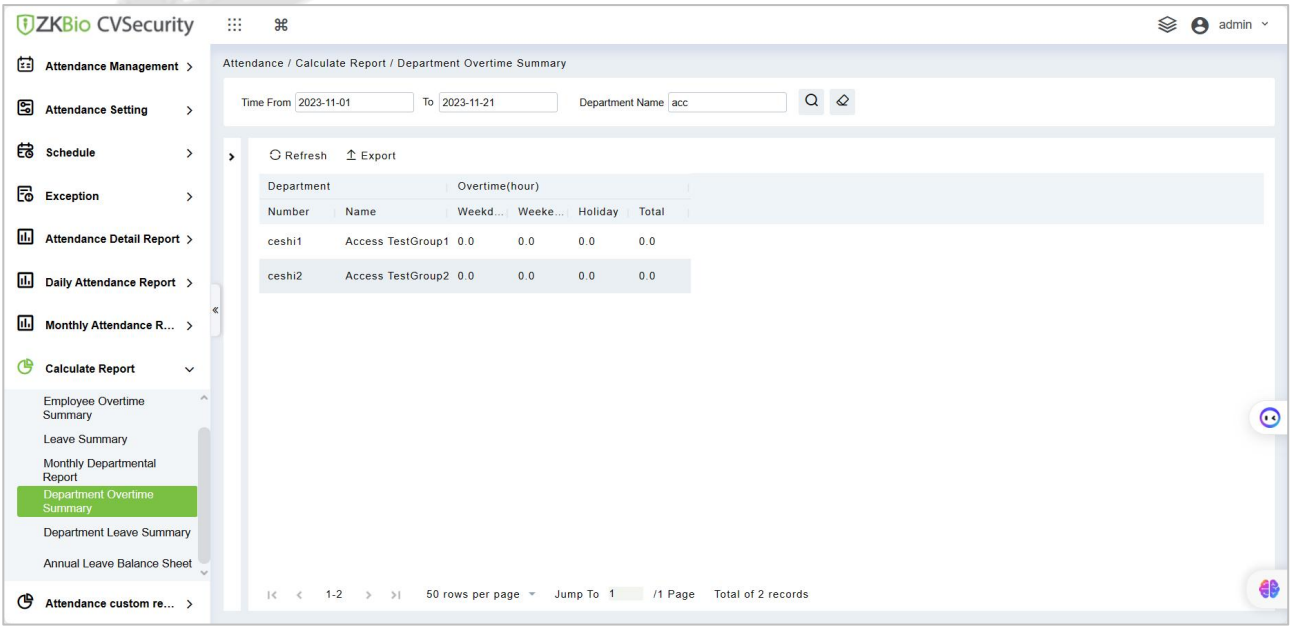


Figure 6- 83 Department Overtime Summary Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.10.6 Department Leave Summary

The department leave summary displays the total leaves taken by the employees in a department. It includes sick leave, casual leave, parental leave, annual leave, compassionate leave, and more.

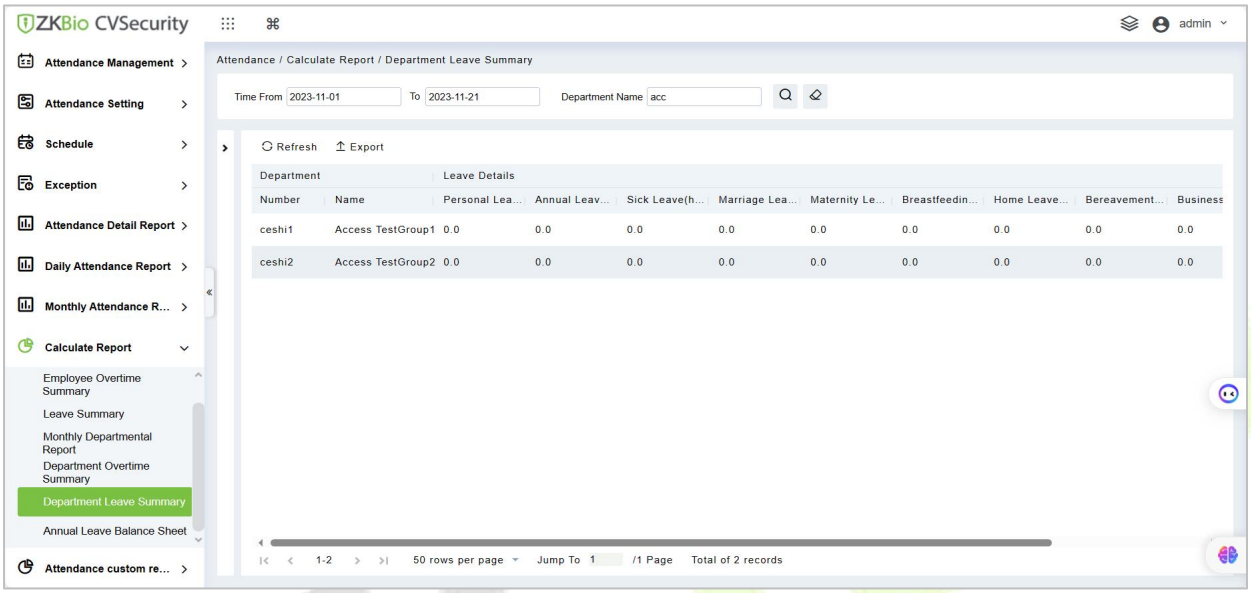


Figure 6- 84 Department Leave Summary Report Interface

● Export:

Click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

6.10.7 Annual Leave Balance Sheet

The Yearly Summary displays all the data of the employee including the number of late arrivals, leaves, absents, and working (count).

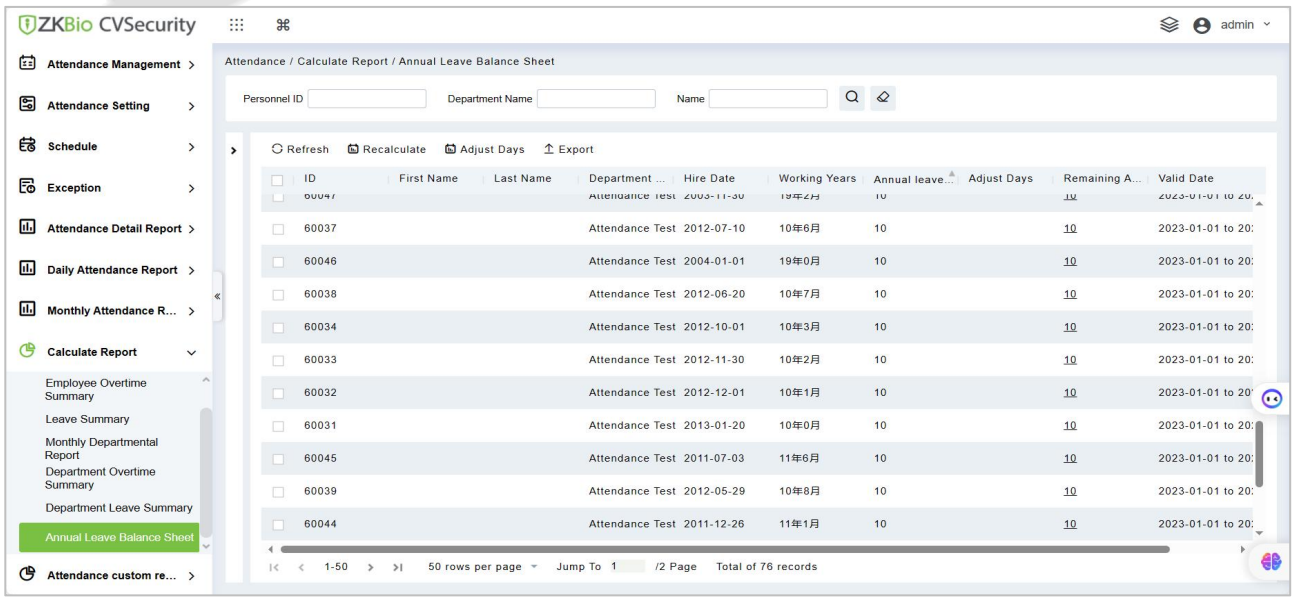


Figure 6- 85 Annual Leave Balance Summary Report Interface

6.11 Attendance Custom Report

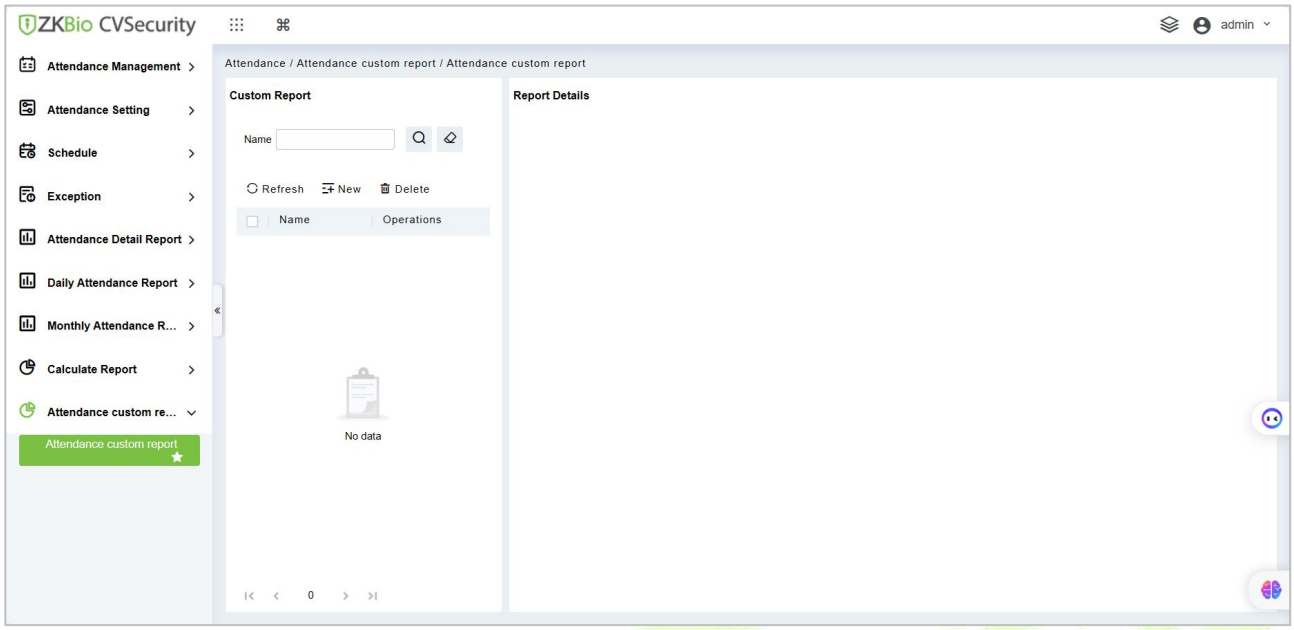


Figure 6- 86

6.11.1 New

1. Go to Attendance > Attendance Custom Report, click New.

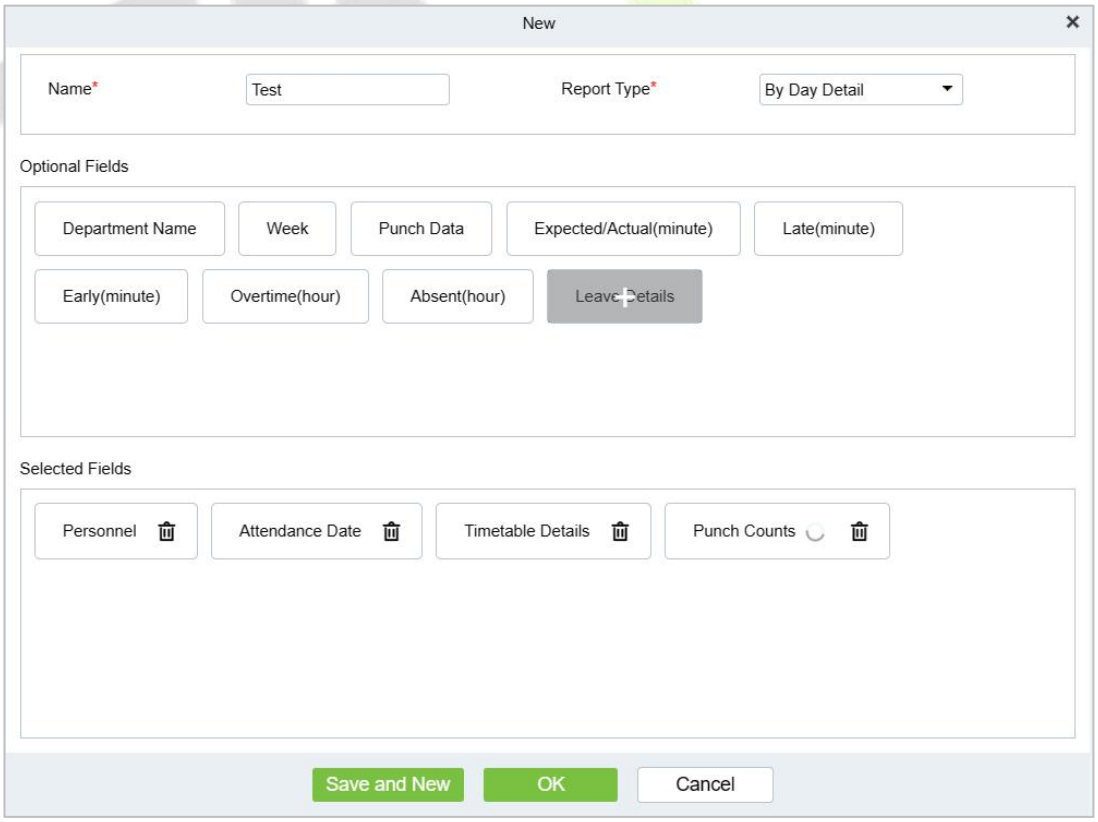


Figure 6- 87

Name: The name of your customized report.

Report Type: There are 3 types, Summary by Dept, Summary by Person, By Day Detail. Optional fields

vary by type.

2. After saving, you can view and export the custom report.

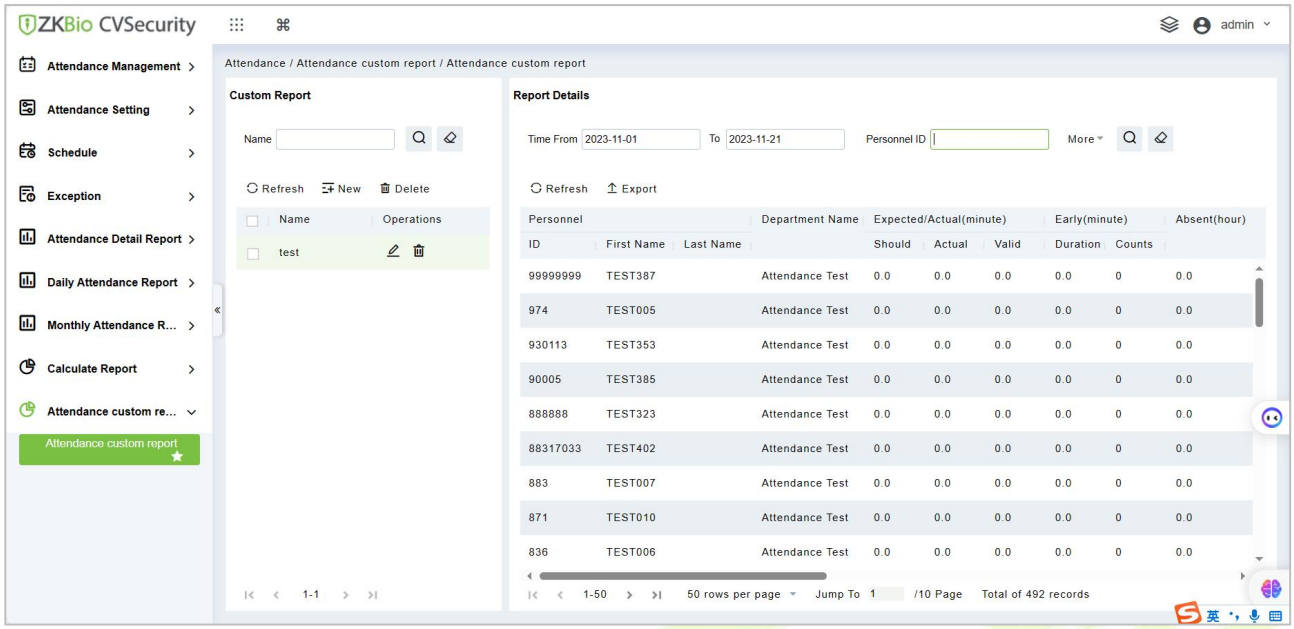


Figure 6- 88

7 Parking

7.1 Operation Scenario

In modern parking lot management, vehicle management is an important aspect, especially for special parking lots, parks and communities, it is required to strictly manage all kinds of vehicles in real time, strictly monitor their entry and exit time, and register and identify all kinds of vehicles (including internal vehicles and external vehicles). In a large-scale field, there are many vehicles coming in and out. For example, every vehicle must be judged manually, which is time-consuming and not conducive to management and inquiry, and the security work is difficult and inefficient. In order to improve this management mode, which is not commensurate with modern parking lots, residential areas, etc., It is necessary to realize the authorization and intelligence of vehicle management as soon as possible, and manage it in the form of computer network, so as to monitor and manage all the vehicles at the entrance and exit effectively and accurately. It is required that the system provide corresponding application software to realize the high efficiency and intelligence of parking lot management.

7.2 Operation Flow

This part introduces the configuration process of parking management business.

The parking management business configuration process is shown in figure below.

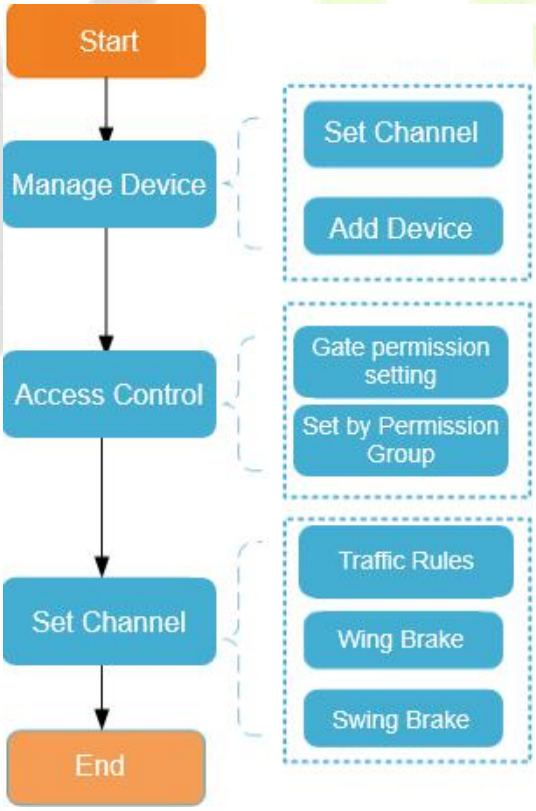


Figure 7- 1 Parking Configuration Flow

7.3 Basic Parking Management

7.3.1 Parking Lot Settings

This part introduces the public parameters of the parking lot under.

● Operating Steps:

Step 1: In the Parking module", select "Parking Basic Management > Parking Settings".

Step 2: In the Parking setting interface, as shown in figure below, fill in relevant parameters. Please refer to Table 7-1for parameters.

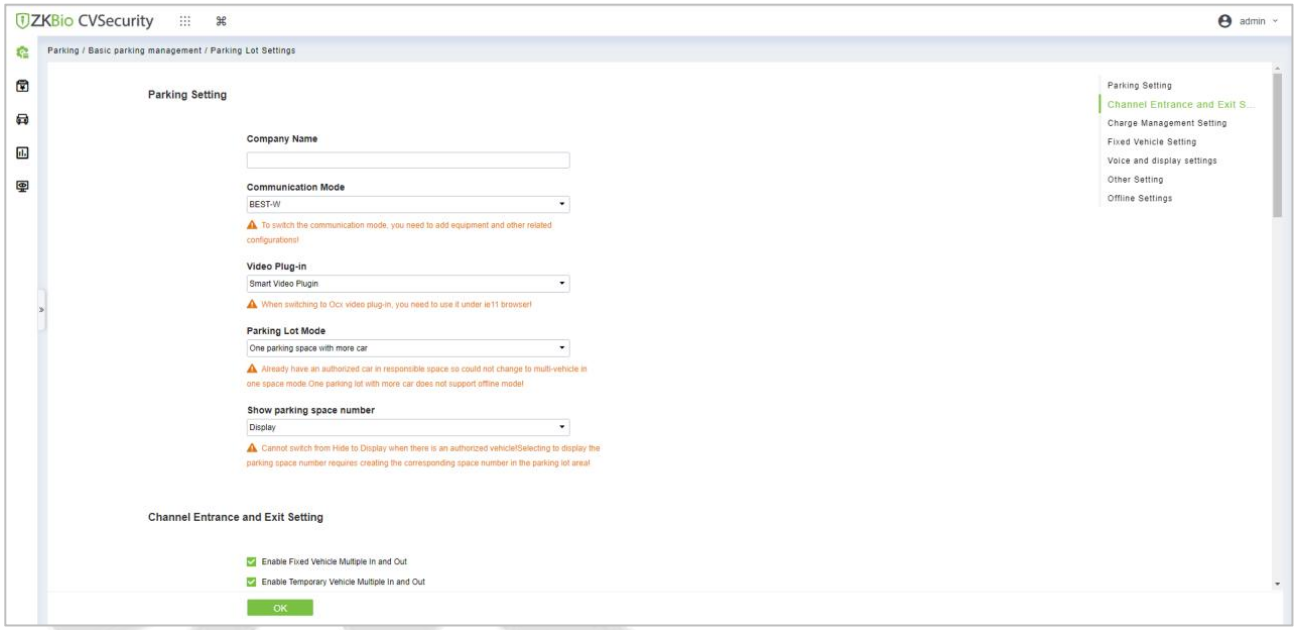


Figure 7- 2 Parking Parameter Setting Interface

Parameter	Specific Parameters	Parameter Description
Parking Setting	Company Name	You can customize the Parking company name, which can be displayed in the billing receipt.
	Communication Mode	Selection according to the communication protocol of the device.The module is compatible with both HTTP and BEST protocols, allowing devices using these two protocols to operate simultaneously.
	Parking Lot Mode	• One Parking Space with one car: means that only one fixed car can be authorized in one parking space at present. • One Parking Space with more car: a parking space that allows multiple fixed cars to be authorized.
	Display Parking Space Number	You can choose whether to display the parking space number or not, and you can specify a certain parking space number.
	Real Time Preview	The number of videos that can be displayed on the Real

Parameter	Specific Parameters	Parameter Description
	Channel Count	Time Monitoring page can be switched from 4/6/8/12/16.
Entrance and Exit Lane Setting	Enable the fixed or temporary vehicles are multiple In and out.	Allow the fixed or Temporary vehicles to the parking area and vehicles are multiple in and out.
	Matching Precision of Entrance and Exit	Vehicles are allowed by exact match and 5 or 6digits registration numbers to the entrance and exit area of the parking.
	Special license plate contains characters	Enter the special license plates contains characters wherever required.
	Duplicate license plate waiting time	In Duplicate license plate waiting time Mention the timings of single channel mode and normal mode
Charge Management Settings	Enable the fixed car charging standard	If the fixed car charging standard has been set in advance, check this setting, and when the fixed car is authorized and postponed, it will be implemented according to this charging standard; If it is not checked, you can only manually enter the extension time and amount.
	Print the charge receipt	If the receipt printer is set and connected, the corresponding receipt will be printed when the charge is successful.
	Enable consumption discounts	Set the "Discount Strategy" in advance and then check the Enable Consumption Discount System, and the consumption discount will be carried out.
	Unmatched processing mode	There are two existing ways to deal with mismatches: "free release" and "opening the gate after charging fees"; Manual release is to open the gate directly, and when the gate is opened after charging, a charge confirmation box will pop up during manual release (only for temporary vehicles).
	Synchronize data to the cloud	After opening, offline parking data will be uploaded to the cloud platform synchronously.
Fixed Vehicle Setting	Statistic parking space of fixed car	• If it is checked, the number of cars will not be deducted after authorization, and the number of cars will be counted in real time when vehicles enter and leave the field. • If it is not checked, the number of fixed cars will be deducted after authorization.
	Enable fixed vehicles to switch to temporary	• If this option is checked, the fixed car will be automatically converted into a temporary car after it expires, and the charge will be made according to the

Parameter	Specific Parameters	Parameter Description
	vehicles	temporary charging method. • If it is not checked, this option will require manual release for the fixed car to come out when it expires.
	Warning days for fixed vehicles	If the warning days are set to 5 days, it is necessary to prompt the vehicles to postpone the fixed vehicles when entering and leaving the field within 5 days.
Voice And Display Settings	Enable external display	Checking this parameter will display the relevant parking data on the external display.
	The entrance shows the remaining parking spaces	Display the remaining parking spaces at the entrance of the parking lot.
	Statistics of car Parking area parking spaces in car Parking area	The statistics of the number of cars in the corresponding booth in the big Parking area include the number of cars in the small Parking area.
	Vehicle entry and exit broadcast license plate	If this parameter is checked, the license plate will be broadcast when the vehicle enters and exits.
	Display color	Set the display color of parking machine.
Ticket Dispenser setting	Enable Ticket Dispenser	The Ticket Dispenser parameters can only be configured after the Ticket Dispenser setting is enabled.
	Enable QR code	After enabling this feature, a QR code will be printed on the ticket.
	Enable Print License Plate	Record the license plate numbers captured by the LPRC300 device, so that if a parking ticket is lost, the license plate number can be used to query and pay the fee.
	Paperless Automatic Opening	After activation, the Ticket Dispenser will automatically open the gate to allow passage when it runs out of paper.
	Virtual License Plate	Enter the content for the virtual license plate here.
	Time of delayed ticket issuance(second)*	Set the ticket dispensing delay time here.
	Ticket Header	Enter the header content for the ticket here.
	Ticket Tail	Enter the tail content for the ticket here.
Other Settings	Maximum vehicle stay	Set the maximum stay time of on-site vehicles. If the on-site

Parameter	Specific Parameters	Parameter Description
	time	vehicles have not left after this time, the records of on-site vehicles will be displayed in the "On-site Stay Timeout Vehicles" report.
	Save days of snapshot photos	Set snapshot photos saved more than the set number of days photos will be automatically deleted, if you do not want to delete snapshot photos will change the parameter set to 0 days.
	Snapshot Save Path	You can customize the path where photos are saved.

Table 7- 1 Description of Parking Parameters

Step 3: After setting the parameters, Click **OK**.

7.3.2Device

For 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.

7.3.2.1Edit or Delete a Device

Step 1: Click Device Name or click **Edit** to access the edit interface.

Step 2: Select device, click **Delete**, and click **OK** to delete the device.

7.3.2.2Reboot Device

It will reboot the selected device.

7.3.2.3Synchronize Time

It will synchronize time with server's current time.

7.3.2.4Get Device Parameters

Click Get Device Parameters Users can get device parameters which is they need from the system.

7.3.2.5Delete Device Command

Click Delete Device command, to delete the selected device command' data.

7.3.2.6Get Device Version

Click Device version to get selected device version.

7.3.3Parking Area

This part introduces the Step configuration of and Parking area.

7.3.3.1Add New

Operating Steps:

Step 1: In the Parking module, select **Parking Basic Management > Parking Area**.

Step 2: In the **Parking Area** interface, click **Add New** and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-2 for parameter description.

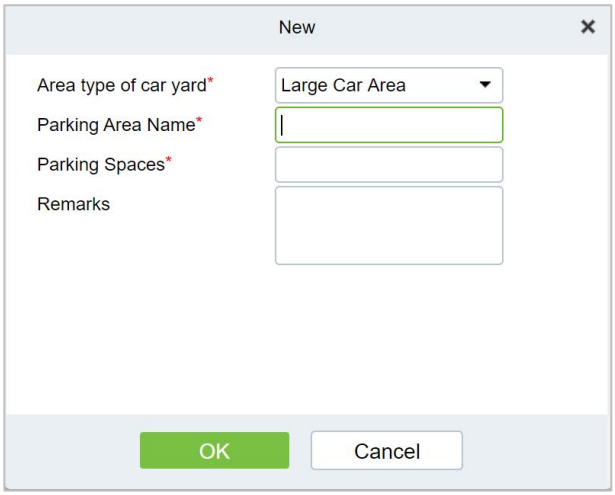


Figure 7- 3 New Interface in Parking Area

Parameter	Description
Type Of Parking Area	Set whether the current Parking area is a big Parking or a small Parking.
Name Of Parking Area	The name of the Parking area cannot be duplicated.
Parking Spaces	Set total number of parking spaces in this area.
Remarks	Text description.

Table 7- 2 Parameter Description of Parking Area

Step 3: Click **OK** to complete the setting of the Parking area.

7.3.3.2Edit

Click a parking area name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

7.3.3.3Delete

Select one or more parking areas and click **Delete** at the upper part of the list and click **OK** to delete the selected parking areas. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single parking area.

7.3.3.4Refresh

Click **Refresh** at the upper part of the list to load new parking areas.

7.3.4Entrance And Exit Area

This part introduces the Step configuration of parking entrance and exit area.

7.3.4.1Add New

Operating Steps:

Step 1: In the Parking module, select "**Parking Basic Management > Entrance and Exit Area**".

Step2: In the interface of Entrance and Exit Area, click **Add New** and fill in relevant parameters, as shown in figure below. Please refer to Table 7-3 for parameter description.

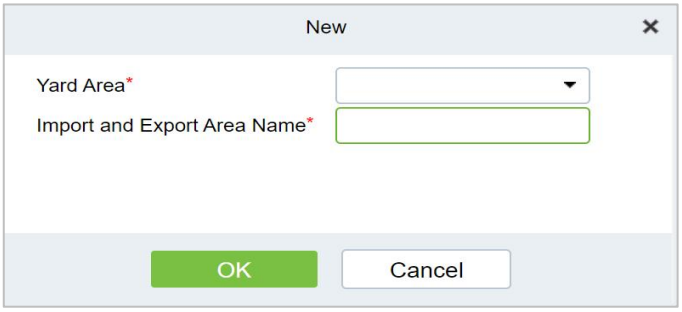


Figure 7- 4 Add Interface of Entrance and Exit Area

Parameter	Description
Parking Area	The name of Entrance and Exit Area cannot be duplicated.
Name Of Entrance and Exit Area	The Parking area to which the Entrance and Exit Area belongs.

Table 7- 3 Description of Parameters of Entrance and Exit Area

Step 3: Click **OK** to complete the setting of Entrance and Exit Area.

7.3.4.2Edit

Click an entrance and exit area name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

7.3.4.3Delete

Select one or more entrance and exit areas and click **Delete** at the upper part of the list and click **OK** to delete the selected entrance and exit areas. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single entrance and exit area.

7.3.4.4Refresh

Click **Refresh** at the upper part of the list to load new entrance and exit areas.

7.3.5Booth

This part introduces the Step configuration of ZKBio CVSecurity Guard Booth. After the configuration is completed, you can check and monitor the Guard Booth interface and operate the gate opening.

7.3.5.1Add New

Operating Steps:

Step 1: In the Parking module, select "**Parking Basic Management > Guard Booth**".

Step 2: In the **Guard Booth** interface, click **Add New** and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-4 for parameter description.

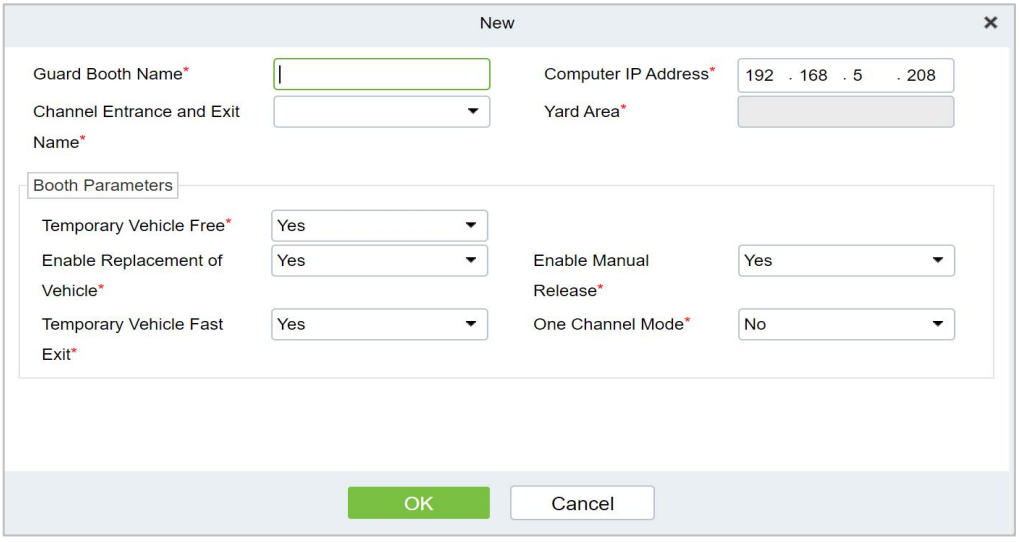


Figure 7- 5 Added Guard Booth Interface

Parameter	Description
Name of Guard Booth	Set the name of the booth.
Guard Booth Computer IP	When the booth mode is browser, the IP address of the booth needs to be set.
Guard Booth Mode	There are two modes of Guard Booth: • Browser: You need to set the IP of the booth computer • Platform: Automatically generate platform registration code
Platform Registration Code	When the booth mode is a platform, it is automatically generated for CS booth registration.
Name Of Entrance and Exit Area	Entrance and Exit Area to which the booth belongs.
Parking Area	After selecting the Entrance and Exit Area, the information of the parking lot area will be read, which is read-only.
Allow Temporary Cars Free of Charge	Set whether the temporary car is free or not, check the interface of opening the billing result of the temporary car, and there will be a "Free" button to allow the temporary car to be free.
Enable Replacement Models	Set whether the replacement vehicle is enabled or not and check the temporary vehicle charging result interface to change the temporary vehicle type of the vehicle. Different vehicle types have different charging standards, so the charging result will also change.
Enable Manual Clearance	Set whether to enable manual release. After checking Enable, you can manually control the gate to open for vehicle release.

Parameter	Description
Temporary Cars Come Out Quickly	Set whether to enable the temporary car to come out quickly. If the temporary car does not incur parking fees after checking the enable, the billing result confirmation interface will not pop up, and the gate will be opened and released directly.
Single Channel Mode	Set whether to enable the single channel mode. After checking Enable, the previous channel of the current scene application can be used for both entry and exit. However, in terms of logical settings, it is recommended to establish different logical channels to bind different IPC devices.

Table 7- 4 Parameter Description of Guard Booth

7.3.5.2Edit

Click a guard booth name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

7.3.5.3Delete

Select one or more guard booths and click **Delete** at the upper part of the list and click **OK** to delete the selected guard booths. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single guard booth.

7.3.5.4Refresh

Click **Refresh** at the upper part of the list to load new guard booths.

7.3.6Lane

This part introduces the configuration of relevant Steps of parking passage.

7.3.6.1Add New

Operating Steps:

Step 1: In the Parking module, select **Basic Parking Management > Lane**.

Step 2: Click **Add New** in the lane interface and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-5 for parameter description.

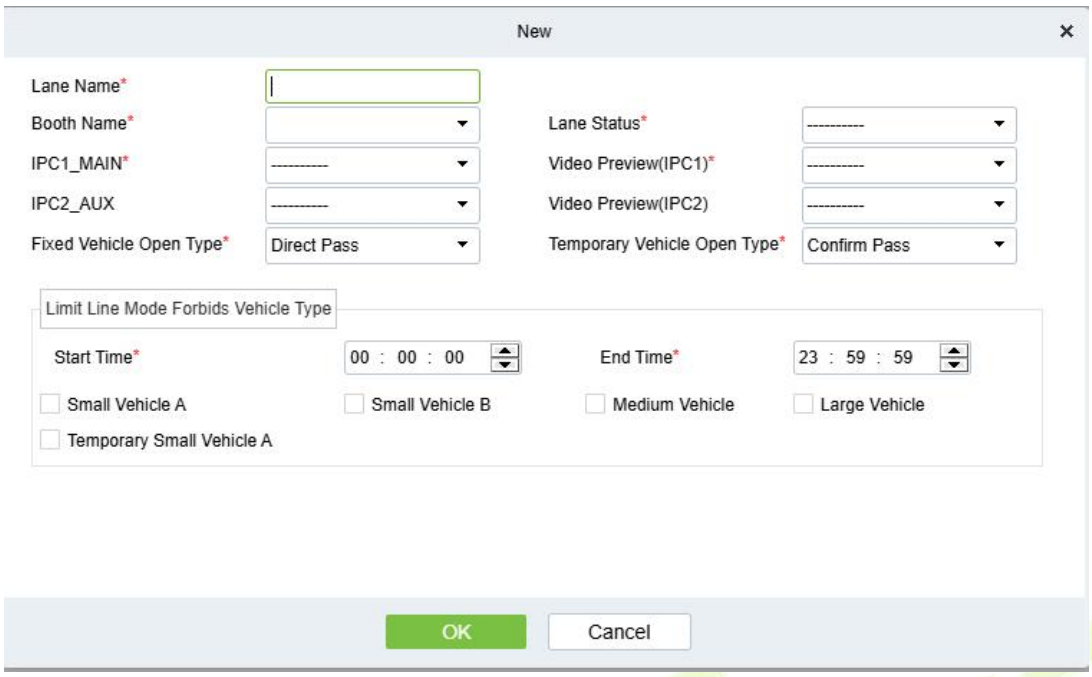


Figure 7- 6 New Channel Interface

Parameter	Description
Lane Name	You can customize the lane name here
Booth Name	Select the corresponding booth
Lane Status	Select the lane properties of the entrance and exit of the corresponding booth entrance and exit area
IPC1_MAIN*	The IP address of device 1, and the corresponding video port position is the monitoring position where the device is located
IPC2_AUX	The IP address of device 2, and the corresponding video port position is the monitoring position where the device is located
Fixed Vehicle Open Type*	Direct release (open the gate directly after identifying the license plate) Confirm the release (pop up the confirmation box and click the button manually to open the gate)
Temporary Vehicle Open Type*	Pick up and release (open the gate directly after identifying the license plate) Confirm the release (pop up the confirmation box and click the button manually to open the gate)
Limit Line Mode Forbids Vehicle Type	You can set the start time and end time, check the vehicle types that are prohibited from passing here, and multiple selections are allowed.

Table 7- 5 Description of Channel Parameters

Step 3: Click **OK** to complete the channel setting.

● The association between TBM and LPR:

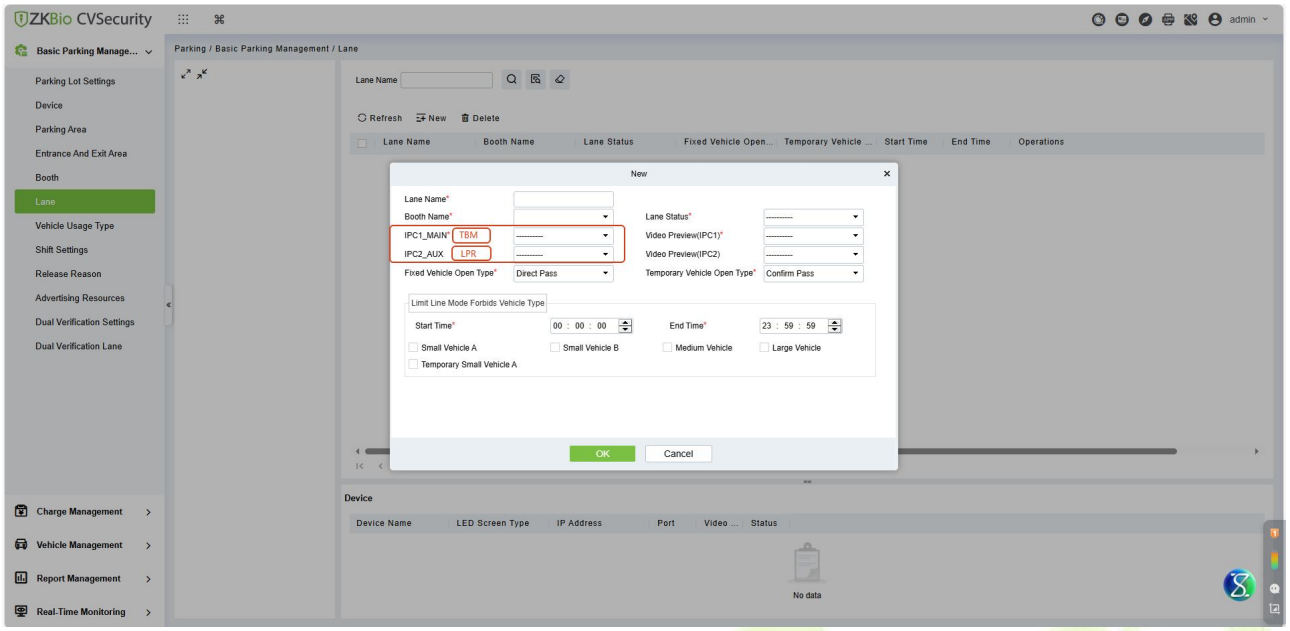


Figure 7- 7 Lane

■ Entrance TBM+LPR

No virtual license plate is set: The prefix defaults to VP. Set virtual license plate: The prefix is the set letter

Enable license plate printing: The license plate number will be displayed on the receipt. If the license plate printing is not enabled, the license plate number will not be displayed on the receipt

Temporary vehicle: Entry → LPR recognition → Ticket collection (auxiliary license plate recognition includes license plate recognition and photo recognition); LPR not recognized (The auxiliary license plate is a system-generated license plate)

Fixed vehicle: Entry → LPR recognition → Card swiping (auxiliary license plate recognition includes license plate recognition and photo recognition); LPR not identified (no processing)

Central payment: Enter the receipt or license plate → Normal billing

Scan the TBM code at the payment exit → Open the gate

■ Export TBM+LPR

Temporary vehicle: Exit → LPR recognition → Ticket scanning (Auxiliary license plate recognition includes license plate recognition and photo recognition)

Fixed vehicle: Exit → LPR recognition → Swipe card (Auxiliary license plate recognition includes license plate recognition and photo recognition)

7.3.6.2 Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.3.6.3 Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single channel.

7.3.6.4Refresh

Click **Refresh** at the upper part of the list to load new channels.

7.3.7Vehicle Usage Type

This part introduces the configuration of related Steps of vehicle definition.

7.3.7.1Add New

Operating Steps:

Step 1: In the Parking module, select **Parking Basic Management > Vehicle Definition**.

Step 2: Click **Add New** in the vehicle definition interface and fill in the relevant parameters, as shown in figure below. Please refer to table below for parameter description.

Parameter	Description
Vehicle Definition	Select the corresponding. vehicle
Vehicle Type	Vehicle type of the charging standard
Status	Select the vehicle status enable or disable
Remarks	Text description

Table 7- 6 Description of vehicle definition Parameters

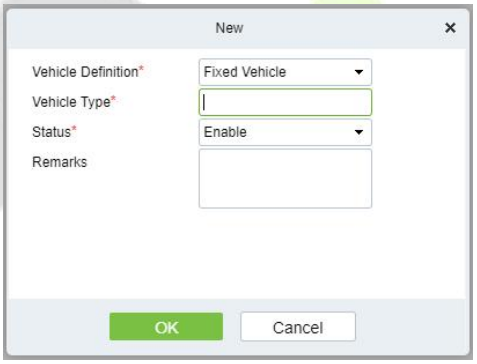


Figure 7- 8 New vehicle definition

7.3.7.2Editing the Vehicle Type

Step 1: Click a vehicle type name or **Edit** in the operation column. The Edit page is displayed.

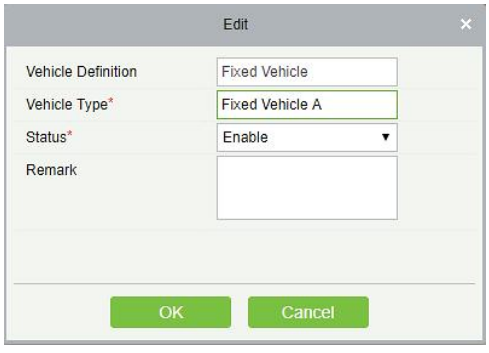


Figure 7- 9 Edit vehicle Type

Step 2: Set Vehicle Type, select a Status, and enter the vehicle type description in Remark.

Step 3: Click **OK** to save and exit.

7.3.7.3Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a vehicle definition.

7.3.7.4Refresh

Click **Refresh** at the upper part of the list to load new vehicle definitions.

7.3.8Shift Settings

This part introduces the configuration of related Steps of parking shift.

7.3.8.1Add New

Operating Steps:

Step 1: In the Parking module, select "**Parking Basic Management > Shift Setting**".

Step 2: In the **Shift Setting** interface, click **Add New** to fill in relevant parameters, as shown in figure below. Please refer to Table below for parameter description.

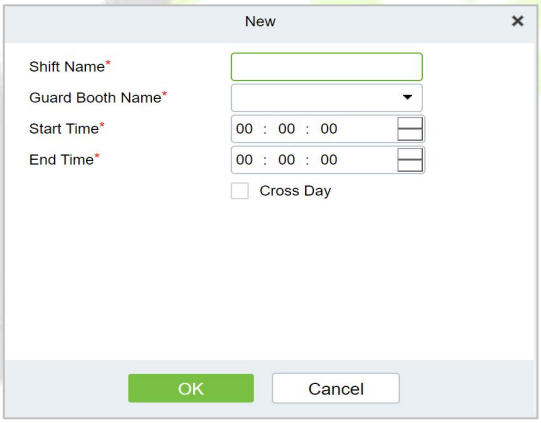


Figure 7- 10 New Shift Interface

Parameter	Description
Shift name	Distinguish the difference between shifts by setting the device name
Name of Guard Booth	Distinguish the differences between booths by setting device names
Start time	Select the time when the shift starts
End time	Select the time when the shift ends
Across the sky	Is the shift time set across days

Table 7- 7 Shift Parameter Description

Step 3: Click **OK** to complete the setting of adding shift settings.

7.3.8.2Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.3.8.3Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a shift setting.

7.3.8.4Refresh

Click **Refresh** at the upper part of the list to load new shift settings.

7.3.9Release Reason

A manual release reason must be selected when the manual release function is used on the online monitoring page.

7.3.9.1Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Basic Management > Manual Release Reason.

Step 2: In the **Manual Release Reason** interface, click **Add New** to fill in relevant parameters, as shown in figure below. Please refer to Table 7-8 for parameter description.

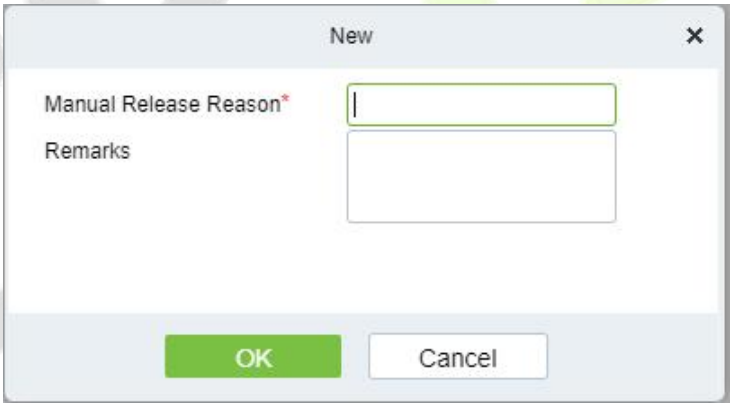


Figure 7- 11 New Manual Release Reason Interface

Parameter	Description
Shift Name	Distinguish the difference between shifts by setting the device name
Name Of Guard Booth	Distinguish the differences between booths by setting device names
Start Time	Select the time when the shift starts
End Time	Select the time when the shift ends
Across the Sky	Is the shift time set across days

Table 7- 8 Manual Release Reason parameter description

7.3.9.2Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.3.9.3Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a manual release reason.

7.3.9.4Refresh

Click **Refresh** at the upper part of the list to load new Manual Release Reason.

7.3.10Dual Verification Settings

The dual verification feature combines access control data with license plate recognition, allowing the barrier to open only when both the driver and the license plate information match, providing enhanced security. When a vehicle enters the reading range, the LPR camera scans and identifies the license plate. Simultaneously, the driver must swipe a card or verify their identity via facial recognition/fingerprint on the access control device. If both the license plate number and the driver's identification results match the data in the database, the parking barrier will lift to grant access. Otherwise, entry will be denied.

Enable the **"Enable Parking Lot verification"** option under the menu:**Parking > Basic Parking Mana gement >Double Verification Setting.**

Note: *The dual verification feature can only be activated after configuring the binding relationship between the access control device and LPR (License Plate Recognition) in 7.3.11Dual Verification Lane*

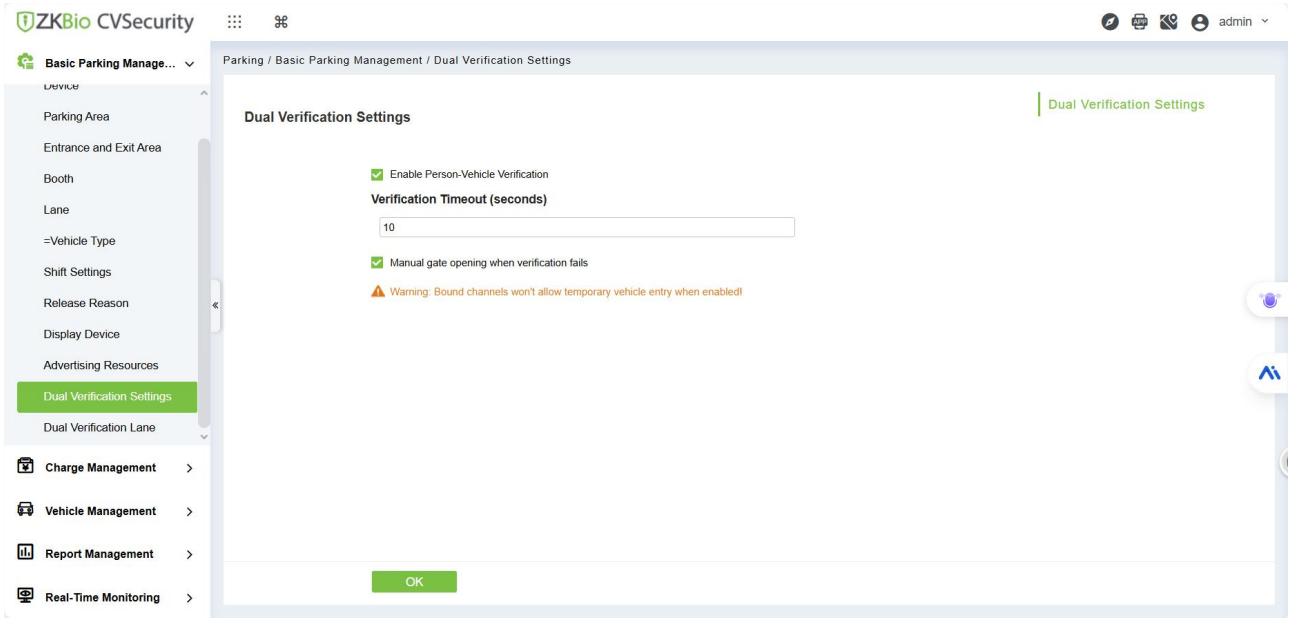


Figure 7- 12 Dual Verification Setting

The explanation of the corresponding parameters is as follows in the table:

Parameter	Description
Enable Parking Lot Verification	Configures whether to enable the dual verification feature for parking and access control.
Verification Timeout	Sets the timeout duration for verification between parking and access control devices (10-255 seconds).
Enable Manual Gate Opening Upon Dual Verification Failure	Configures whether to allow manual gate opening if dual verification fails.

Table 7- 9 Dual Verification Parameter Description

7.3.11 Dual Verification Lane

Under this menu, you can bind the access control device and LPR (License Plate Recognition) within the same channel.

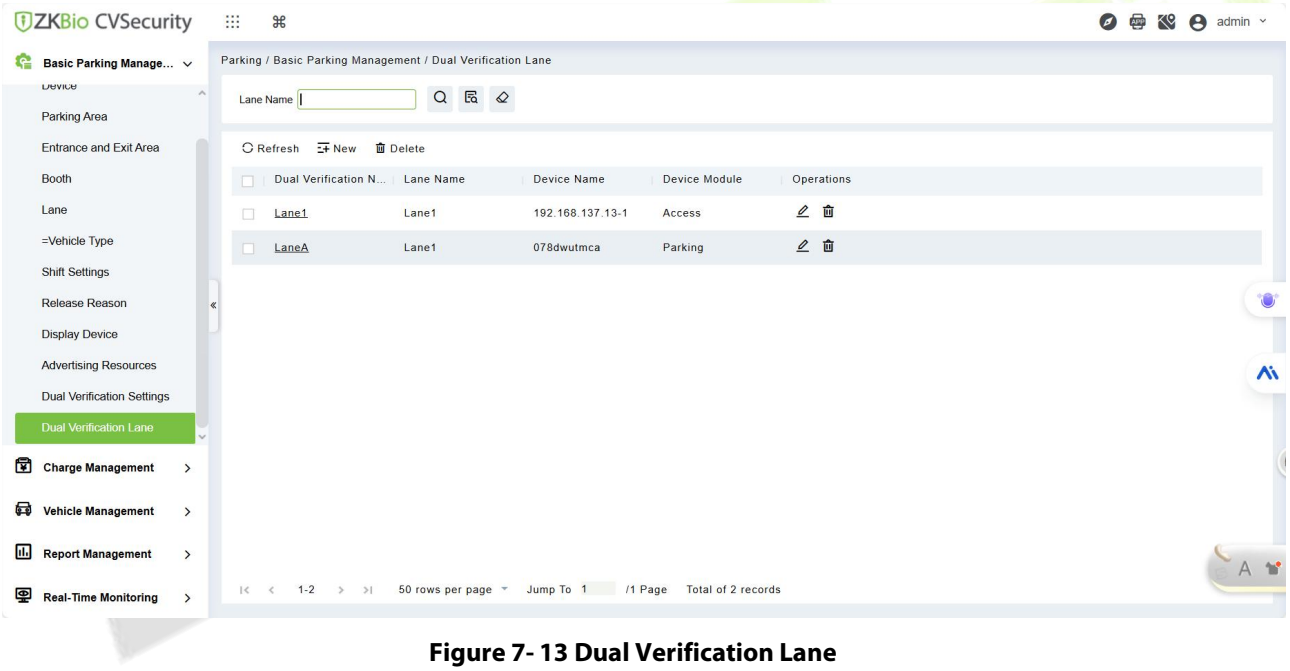


Figure 7- 13 Dual Verification Lane

Under **Parking > Basic Parking Management > Double Verification Lane**, click **New** and select the device from either the access control or parking module.

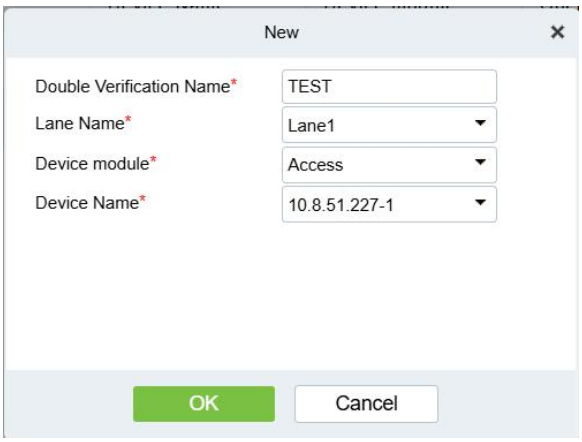


Figure 7- 14 New Dual Verification

Note: *When selecting the access control device for a lane for the first time, you must repeat the operation—choose the* ***same lane*** *again and then select the LPR (License Plate Recognition) device from the parking module. This binds the access control and parking devices to the same lane.*

Verification Result:

- If both license plate recognition and personnel verification on the access control device are completed **within the set time range**, the software will log a "Normal Gate Opening" record.
- If verification occurs **beyond the set time range**, the system will display the error prompt: **"Dual Verification Timeout."**

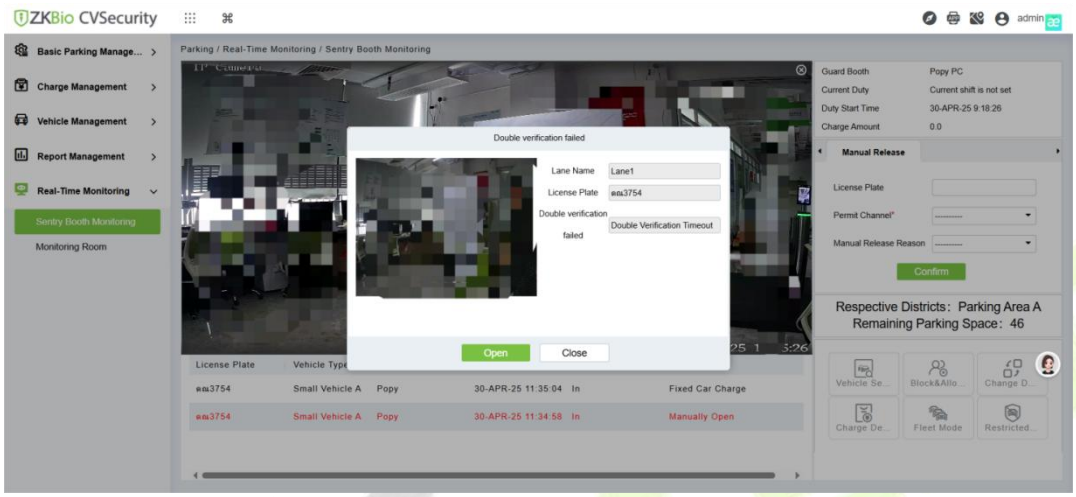


Figure 7- 15 Dual Verification Result

7.4 Charge Management

This part introduces the related configuration of parking charge management, mainly setting the charging rules of various car types in the parking lot and the discount strategy of merchants.

7.4.1 Auth Vehicle Fee Rules

This part introduces the operation Steps of periodic charging rules for fixed cars in.

7.4.1.1 Add New

Operating Steps:

Step 1: In the Parking module, select "**Charge Management > Fixed Car Charge Rules**"

Step 2: In the fixed car charging rules interface, click **Add New** and fill in the corresponding parameters, as shown in figure below. Please refer to Table 7-10 for parameter description.

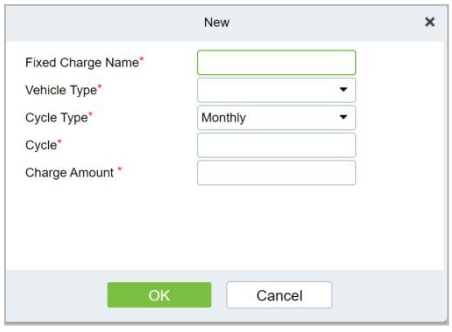


Figure 7- 16 Fixed Car Charge Rules Interface

Parameter	Description
Name of Fixed Car Charge	Set the name of the charging standard for fixed cars, which cannot be repeated.
Car Type	Select the car type corresponding to the fixed car charging standard, and each car type can only be set once.
Periodic Type	Fixed car charging cycle type, monthly/daily.
Period	Set the cycle time, that is, the effective time of the fixed car.
Amount	Set the amount charged.

Table 7- 10 Parameter Description of Fixed Car Charging Rules

7.4.1.2Edit

Click a fixed charge name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.4.1.3Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single fixed vehicle charge.

7.4.1.4Refresh

Click **Refresh** at the upper part of the list to load new fixed vehicle charge.

7.4.2Temp Vehicle Fee Rules

This part introduces the Step configuration of temporary car charging rules in.

7.4.2.1Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Charge Management > Temporary Car Charge Rules".

Step 2: In the Temporary Car Charge Rules interface, click **Add New.**and fill in the corresponding parameters, as shown in figure below. Please refer to Table 7-11 for parameter description.

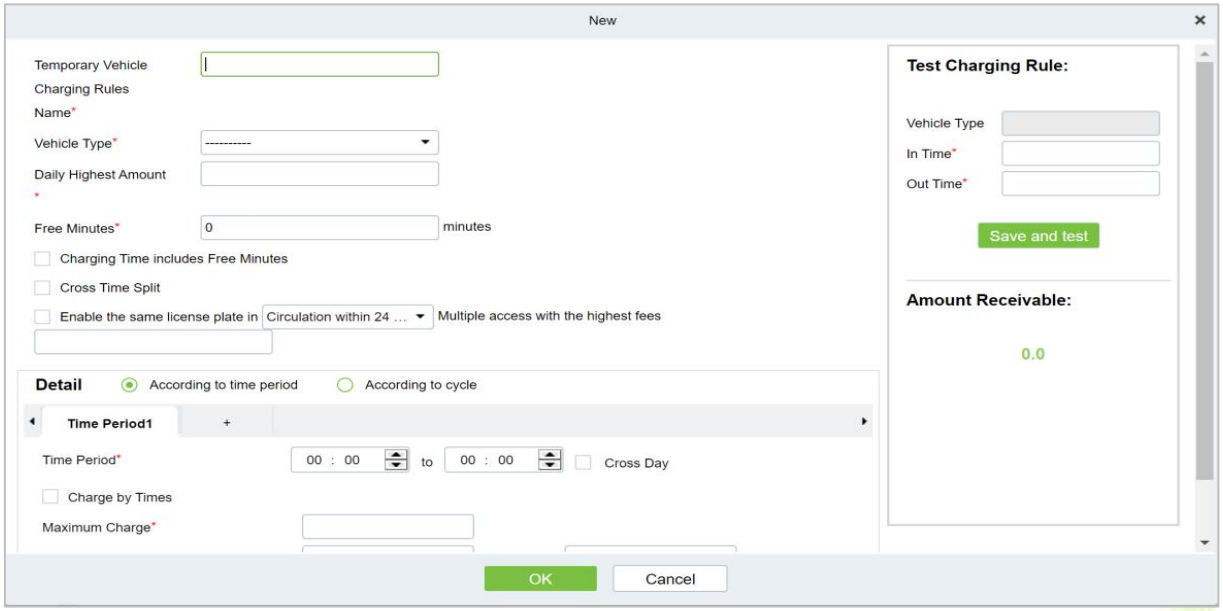


Figure 7- 17 Temporary Car Charge Rules Interface

Parameter	Description
Temporary Vehicles Charging Rules Name	Set the name of temporary car charging rule, which cannot be duplicated.
Vehicle Type	Select the vehicle type corresponding to the charging standard.
Daily Highest Amount	The maximum charge within one day (for example, 10 yuan per hour, 240 yuan for a full day; If the maximum charge amount for the whole day is set to 100 yuan, just charge 100 yuan).
Free Minutes	There is no charge for parking time within this value range.
Charging Time Includes Free Minutes	• Check this item, assuming that the free minute is 30 minutes, and the parking time is 31 minutes. If the parking time exceeds the free minute, the parking time will be charged according to 31 minutes at this time. • If this item is not checked, assuming that the free minute is 30 minutes and the parking time is 31 minutes, if it exceeds the free minute, the parking time at this time is 1 minute (31 minutes minus 30 minutes).
Cross Time Splitting	Suppose that the charge for period 1 is set at 1 yuan every 15 minutes from 9:00 to 10:00, the charge for period 2 is set at 10 yuan every 15 minutes from 10:00 to 11:00, and the parking time is from 9:43 to 10:30. • If this item is not checked, 1 yuan will be charged from 9:43 to 9:58, and if it is only two minutes and less than 15 minutes from 9:58 to 10:00, it will be supplemented from 10:00 to 10:13, then charged according to time period 2 from 10:13 to 10:28, and so on. • If this item is checked, 1 yuan will be charged from 9:43 to 9:58, only two minutes will be less than 15 minutes from 9:58 to 10:00, 1 yuan will be charged according to time period 1, time period 2 will

Parameter	Description
	be charged from 10:00 to 10:15, and so on.
Enable The Same License Plate to Enter and Leave the Maximum Charge for Multiple Times in A Cycle of 24 Hours (24 Hours on Natural Days)	That is, rolling charges. If the accumulated fees for the same license plate entering and leaving the parking lot for many times exceed this value, no fees will be charged within the set period. The cycle can be set as 24 hours on a natural day or 24 hours on a cycle: 24 hours on a natural day refers to 0:00-24: 00; Cycle 24 hours refers to the time from the admission time to the next day.
By Time Period	• Time period: Set the charging standards for different time periods, and check the cross-day, but to ensure that the cumulative sum of all time periods is 24 hours, multiple time periods can be added, and the time periods remain continuous. • Charge by time: If this item is checked, the first time charge, the amount of unit time charge cannot be filled in, only the highest charge is charged, and the fee set in "Maximum Charge" is charged every time; If this item is not checked, the fee will be charged according to the first time charge, and the remaining time exceeding the first time charge setting will be charged according to the unit time; If the first time charge is not set, the charge will be charged directly according to the unit time, and the unit minute must be a multiple of 15. If the charge exceeds the charge set in the "Maximum Charge", it will be charged according to the maximum charge amount. • First time charge: Set the first time within how many minutes, the amount of charge. • Maximum charge: the maximum amount of charge in the setting period. • Charge amount per unit time: Set the charge amount for how many minutes in this time period.
Periodically	• Cycle: From the admission time, the next 1440 minutes (24 hours) can be divided into multiple cycle charging standards. • Charge by time: set whether to charge by time in the cycle. After checking, you can only set the maximum charge amount in the cycle, but you cannot set the charge amount per unit time. • Maximum charge: the maximum amount of charge in the setting period. • Charge amount per unit time: Set the charge amount for how many minutes within the minutes of the cycle.

Table 7- 11 Parameter Description of Temporary Car Charging Rules

7.4.2.2Edit

Click a temporary charge name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.4.2.3Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single temporary vehicle charge.

7.4.2.4Refresh

Click **Refresh** at the upper part of the list to load new temporary vehicle charge.

7.4.3Overtime Fee Rules

This part introduces the operation Steps of charging rules when vehicles time out in.

7.4.3.1Add New

Operating Steps:

Step 1: In the Parking module, select **Parking Charge Management > Overtime Charge Rules**.

Step 2: In the **Overtime Charge** Rule interface, click **Add New** and fill in the corresponding parameters, as shown in figure below. Please refer to Table 7-12 for parameter description.

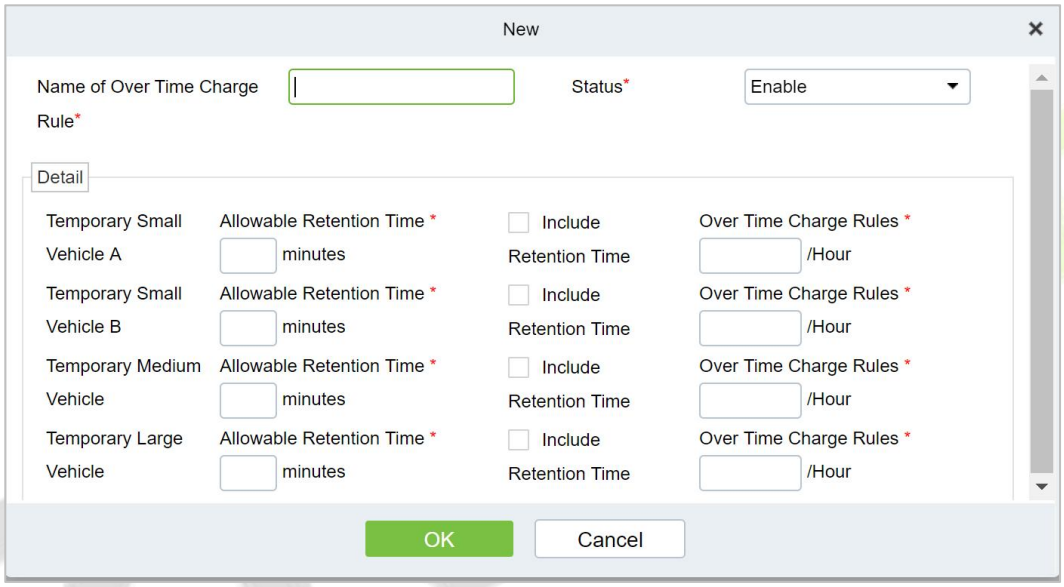


Figure 7- 18 Interface of Timeout Charging Rules

Parameter	Description
Overtime Charge Standard	Set the name of timeout charging standard, which cannot be duplicated.
Status	Select whether to enable the charging standard.
Detailed Settings	Set the allowed detention time of each temporary vehicle type after the central payment and the charging standard after exceeding the time.
Allowable Residence Time	The detention time allowed in the garage after the central payment; In case of overtime, you need to charge again.
Including Residence Time	Assume that the allowed detention time is 30 minutes, and the detention time is 31 minutes after payment. If this item is checked, it will be charged according to the timeout of 31 minutes; If this item is not checked, it will be charged according to the timeout of 1 minute.

Parameter	Description
Overtime Charging Rules	The billing standard for exceeding the allowable residence time.

Table 7- 12 Parameter Description of Overtime Charge Rules

7.4.3.2Edit

Click a name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.4.3.3Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a time charging rules.

7.4.3.4Refresh

Click **Refresh** at the upper part of the list to load new over time charging rules.

7.4.4Discount Strategy

This part introduces the Step configuration of parking discount strategy for parking discount.

7.4.4.1Add New

Operating Steps:

Step 1: In the Parking module, select **Parking Charge Management > Discount Strategy**.

Step 2: In the discount policy interface, click **Add New** and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-13 for parameter description.

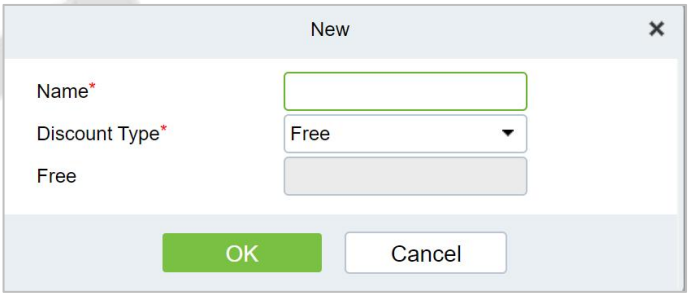


Figure 7- 19 New Discount Policy Interface

Parameter	Description
Policy Name	Set the name of discount policy, which cannot be duplicated.
Discount Type	Select the discount type: • Free, no charge. • The amount of reduction and exemption, the cost is directly deducted from the fixed amount. • Reduce minutes, subtract minutes from parking time and then charge.

Parameter	Description
	• Percentage of reduction and exemption, percentage of expense deduction.
Amount of Relief	At present, the discount type is reduction amount, and the corresponding field name is reduction amount; If it is another type, it corresponds to the corresponding unit. When the discount type is free, this item is not filled in.

Table 7- 13 Discount Strategy Parameter Description

7.4.4.2Edit

Click a name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

7.4.4.3Delete

Select one or more discount policies and click **Delete** at the upper part of the list and click **OK** to delete the selected discount policies. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single discount strategy.

7.4.4.4Refresh

Click **Refresh** at the upper part of the list to load new discount policies.

7.4.5Business Management

This part introduces the operation Steps of merchant management in.

7.4.5.1Add New

Operating Steps:

Step 1: In the Parking module, select "**Parking Charge Management > Business Management** ".

Step 2: In the **Business Management** interface, click **Add New** fill in the corresponding parameters, as shown in figure below. Please refer to Table 7-14 for parameter description.

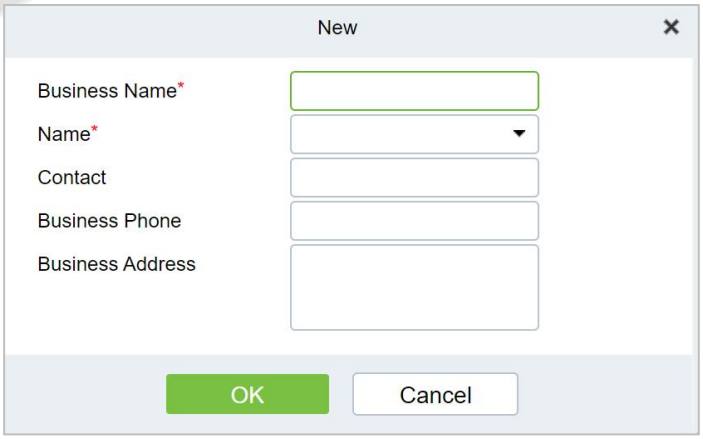


Figure 7- 20 Business Management New Interface

Parameter	Description
Merchant Name	Set the merchant's name, which cannot be duplicated.

Parameter	Description
Discount Method	Choose a discount strategy.
Contact Person	Set up merchant contacts.
Merchant Telephone Number	Set the contact number of the merchant.
Merchant Address	Set the merchant contact address.

Table 7- 14 Description of Business Management Parameters

7.4.5.2Edit

Click a name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.4.5.3Delete

Select one or more vendors and click **Delete** at the upper part of the list and click **OK** to delete the selected vendors. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single vendor.

7.4.5.4Refresh

Click **Refresh** at the upper part of the list to load new vendors.

7.4.6Financial Reconciliation

This part introduces the operation Steps of accounting reconciliation in.

Operating Steps:

Step 1: In the Parking module, select "**Parking Charge Management > Financial Reconciliation**".

Step 2: In the account reconciliation interface, click **Reconciliation**, as shown in figure below. Please refer to Table 7-15 for parameter description

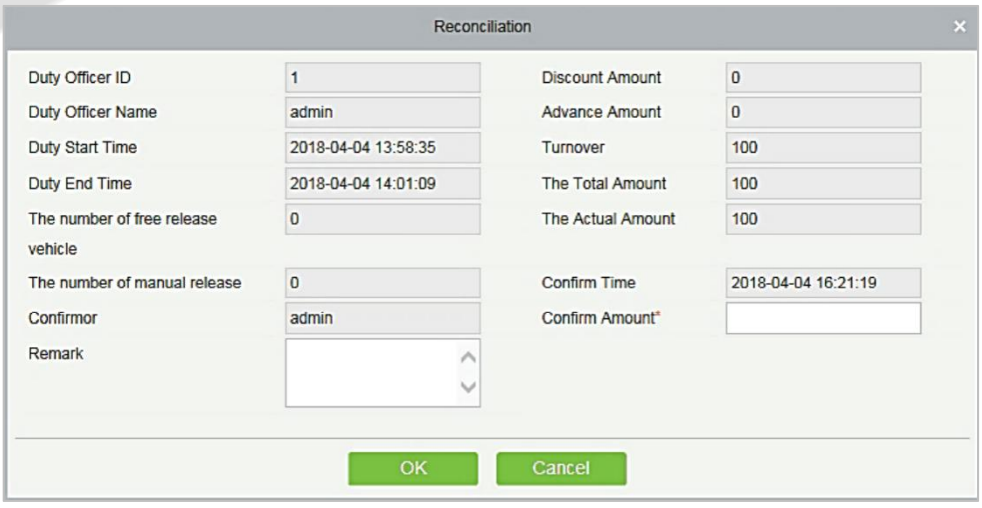


Figure 7- 21 Accounting Reconciliation New Interface

Parameter	Description
Duty Officer Name	Duty officer name
Duty Officer Id	Duty officer ID
Duty Starts Time	Duty starts time
Duty End Time	Duty end time
The Number of Free Release Vehicle	Number of vehicles released free of charge
The Number of Manual Releases	Number of vehicles released manually
Confirmor	Reconciliation personnel
Advance Amount	Amount prepaid to the guard booth (for changes).
Turnover	Paid amount
The Total Amount	Advance amount + Turnover
The Actual Amount	Amount entered by the duty officer during the shift change.
Confirm Time:	Current time
Confirm Amount:	Amount confirmed by the reconciliation personnel
Remark	Remark to be added.

Table 7- 15 Parameter Description of Accounting Reconciliation

7.5 Vehicle Management

7.5.1 License Plate Registration

This part introduces the operation Steps of License. Plate Registration.

7.5.1.1 Add New

Operating Steps:

Step 1: In the Parking module, select "**Vehicle Management > License Plate Registration** ".

Step 2: In the License. Plate Registration interface, click **Add New**, as shown in figure below. Please refer to Table 7-16 for parameter description

Figure 7- 22 License Plate Registration New Interface

Parameter	Description
Name	Enter the person's name
License Plate	License Plate numbers to be added for registration

Table 7- 16 Parameter Description of License Plate Registration

7.5.1.2Edit

Click **Edit** at the end of each line or click the corresponding Personnel ID and modify personnel license plate registration information in the Edit dialog box.

7.5.1.3Delete

Select one or more license plate registration information and click **Delete** at the upper part of the list and click **OK** to delete the selected registration information. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single registration information.

7.5.1.4Download License Plate Import Template

This function will help you to download the licence plate import template.

A	B
License Plate Import Template	
Personnel ID	License plate number (multiple license plates, separated)

Figure 7- 23 License Plate Download Template

7.5.1.5License Plate Import

This function will help you to upload the licence plate import template.

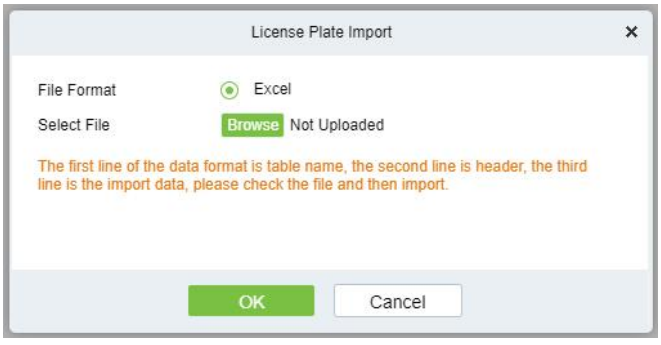


Figure 7- 24 License Plate Registration Import Interface

7.5.2Vehicle Authorization

This part introduces the configuration of vehicle authorization Steps in. Only authorized vehicles can normally use the parking module process.

7.5.2.1Add New

Operating Steps:

Step 1: In the Parking module, select **Vehicle Management > Vehicle Authorization**.

Step 2: Click **Add** and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-17 for parameter description.

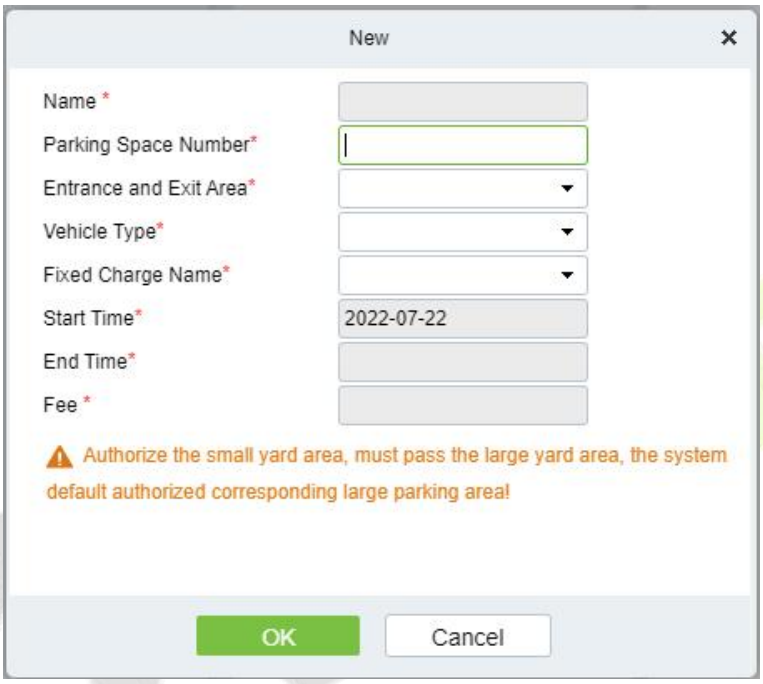


Figure 7- 25 Vehicle Authorization Interface

Parameter	Description
Name	In the input box, enter one or more characters contained in the name or number of the owner, and you can find the owner vaguely.
Parking Space Number	Enter the total number of parking spaces in this area
Entrance And Exit Area	Set the Entrance and Exit Area where this license plate can pass. After selecting the parking space number, filter and only display the Entrance and Exit Area of the parking lot area to which the parking space number belongs.
Car Type	Select the vehicle type to which the vehicle belongs.
Fixed Charge Name	Unique name of a fixed vehicle charge
Start Time/End Time	Refers to the time/deadline for authorizing the license plate to take effect. If the fixed car charging standard is enabled, this parameter is filled in by default.

Parameter	Description
Amount Collected	Record the fees charged for this authorization; If the fixed car charging standard is enabled, this parameter is filled in by default.

Table 7- 17 Description of Vehicle Authorization Parameters

Step 3: Click **OK** to complete the setting of vehicle authorization.

7.5.2.2Fixed vehicle Batch Authorization

On the Vehicle Management page, click Fixed vehicle Batch Authorization. The Fixed vehicle Batch Authorization page is displayed as in the following figure:

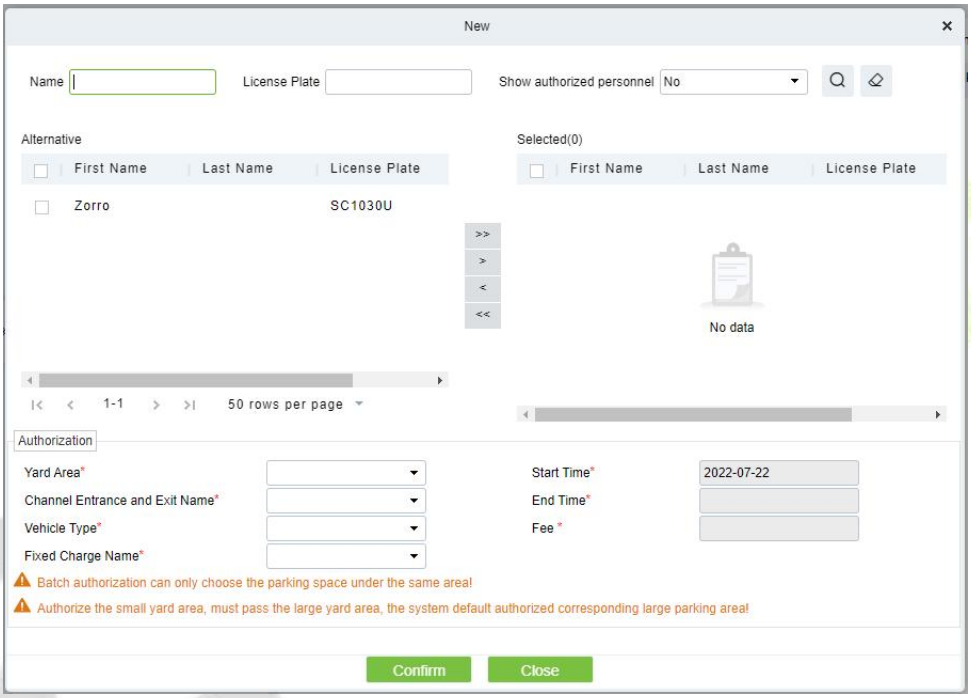


Figure 7- 26 Fixed vehicle Batch Authorization New Interface

Select one or more license plates to be authorized from the list on the left. Click > in the middle to add the license plate to the list on the right. Enter the vehicle type, entrance, and exit area, fee, start time and end time in the Authorization area, and click OK to save the information and authorize fixed vehicles in batches.

7.5.2.3Temporary Vehicle Authorization

On the **Vehicle Management** page, click **Temporary Vehicle Authorization,** the Temporary Vehicle Authorization page is displayed as shown in the following figure. Only the entrance and exit areas to be authorized need to be selected.

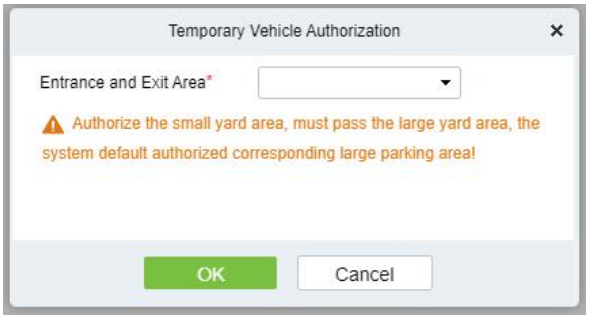


Figure 7- 27 Temporary vehicle Authorization Interface

7.5.2.4Fixed Vehicle Authorization: Delete

Select multiple check boxes in the first column of the license plate list and click Delete to cancel license plates in batches or click Delete at the end of each line to cancel a single license plate.

7.5.2.5Export

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

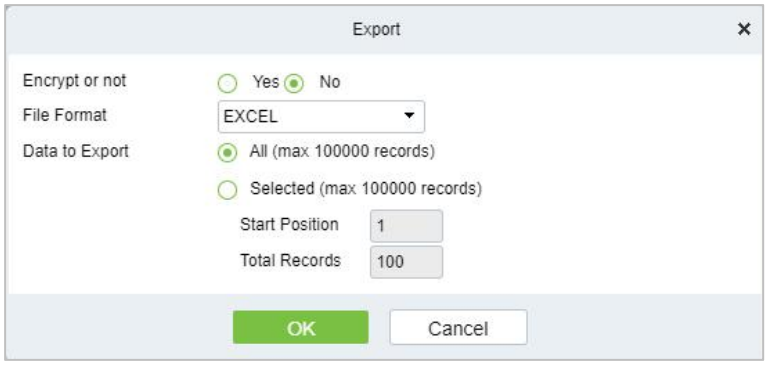


Figure 7- 28 Fixed vehicle Authorization Export

7.5.3Vehicle Extension

7.5.3.1Fixed Vehicle Authorization: Delete

Select multiple check boxes in the first column of the license plate list and click **Delete** to cancel license plates in batches or click **Delete** at the end of each line to cancel a single license plate.

7.5.3.2Batch Extension

Select a fixed license plate for which the valid time needs to be extended and click **Batch Extension** at the end of a fixed license plate. The **Batch Extension** page is displayed.

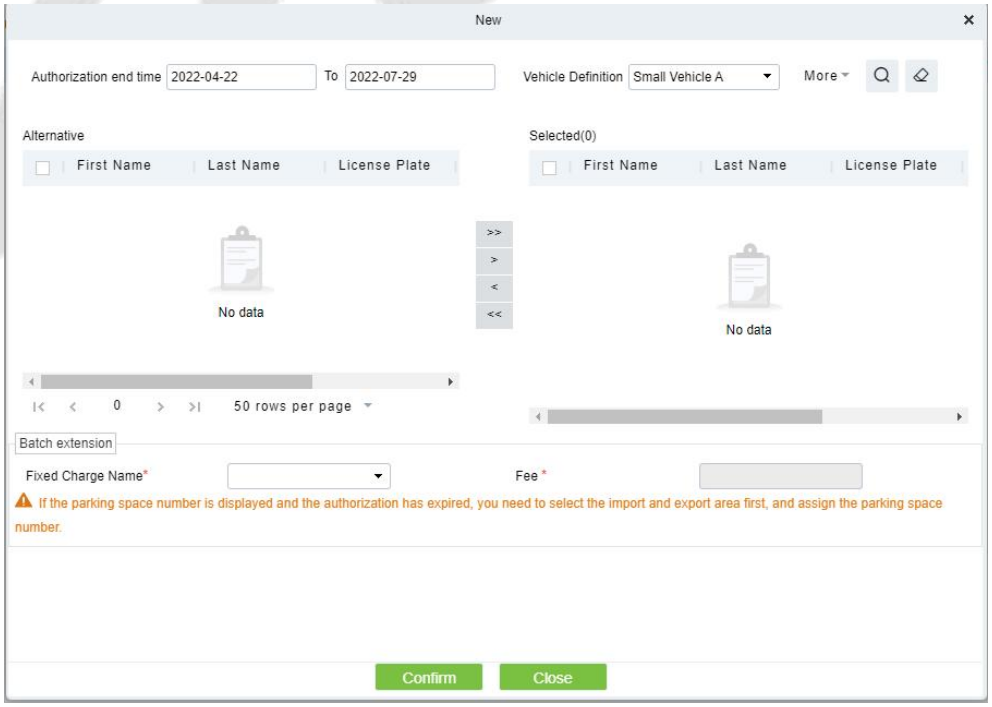


Figure 7- 29 Fixed vehicle Authorization Batch Extension

Set Extended Deadline and Fee. Click OK to save and exit.

7.5.4Allow & Disable List Management

7.5.4.1Add New

● Operating Steps:

Step 1: In the Parking module, select **Vehicle Management > Block&Allow List Management**.

Step 2: Click **Add New** and fill in the relevant parameters, as shown in figure below. Please refer to Table 7-18 for parameter description.

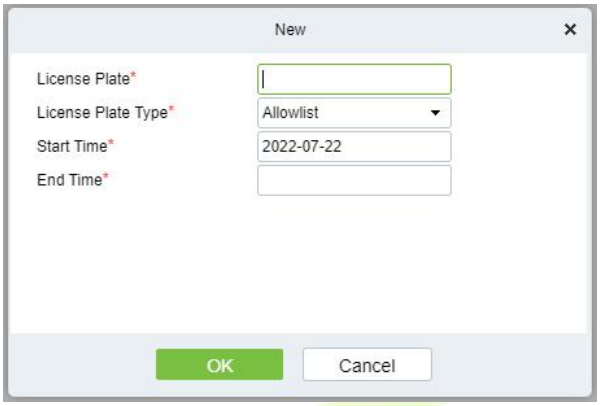


Figure 7- 30 Block&Allow List Management New Interface

Parameter	Description
License Plate	License plate numbers to be added to the blocklist or allowlist
License Plate Type	The value can be block list or allowlist
Start Time/End Time	Time when the allowlist takes effect & expires (This parameter is not available for the blocklist).

Table 7- 18 Description of Block&Allow List Management Parameters

7.5.4.2Edit

Click a **license plate** number or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

7.5.4.3Delete

Select one or more license plate numbers and click **Delete** at the upper part of the list and click **O**K to delete the selected license plate numbers. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single license plate number.

7.5.4.4Refresh

Click **Refresh** at the upper part of the list to load the latest blocklist and Allowlist.

7.5.4.5Synchronize Blocklist

Click **Synchronize Blocklist,** click **OK** to synchronize all blocklists, click **Cancel** to cancel.

When the device is off-line, the device will automatically synchronize blocklist and broadcast voice. It should be noted that the device must be equipped with an SD card.

7.5.4.6Synchronize Allowlist

Click **Synchronize Allowlist,** click **OK** to synchronize all Allowlists, click **Cancel** to cancel.

When the device is off-line, the device will identify the Allowlist synchronized and automatically open the gate. It should be noted that the device must be equipped with an SD card.

7.6 Report Management

7.6.1Vehicle Inside

7.6.1.1Remove

Remove from Device function lets you to remove or eliminate the transmitted Work Codes from the Device.

7.6.1.2Export

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

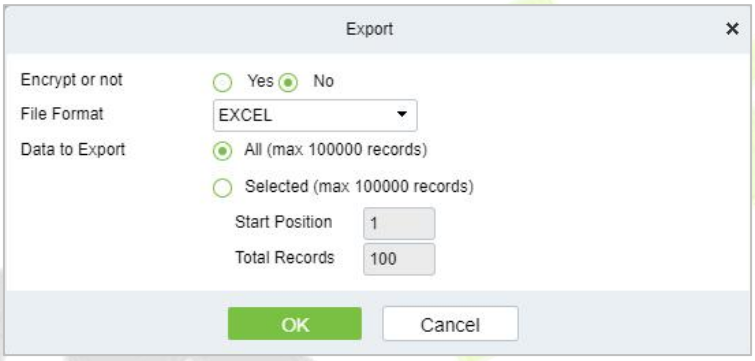


Figure 7- 31 vehicle Inside Export Interface

7.6.1.3License Plate Correction

Make modifications of the License Plate Number.

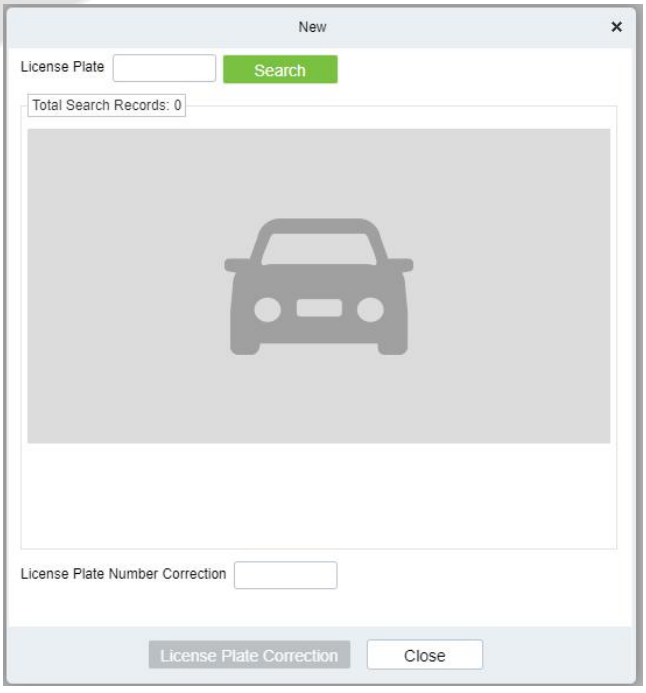


Figure 7- 32 License Plate Correction

7.6.2Entry Record

It will provide the details of the vehicle which entered into the parking.

Click **Report Management** > **Entry Record**. Select the desired time period, vehicle owner and license plate number, and click to query Entry records. Click **More** to query based on other conditions.

7.6.2.1Export

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

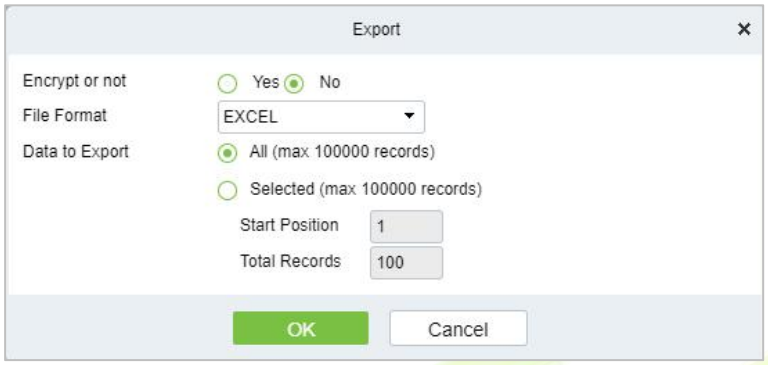


Figure 7- 33 Entry Record of Export Interface

7.6.3Exit Record

It will provide the details of the vehicle which exited out of the parking.

Click **Report Management** > **Exit Record**. Select the desired time period, vehicle owner and license plate number, and click to query Exit records. Click **More** to query based on other conditions.

7.6.3.1Export

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

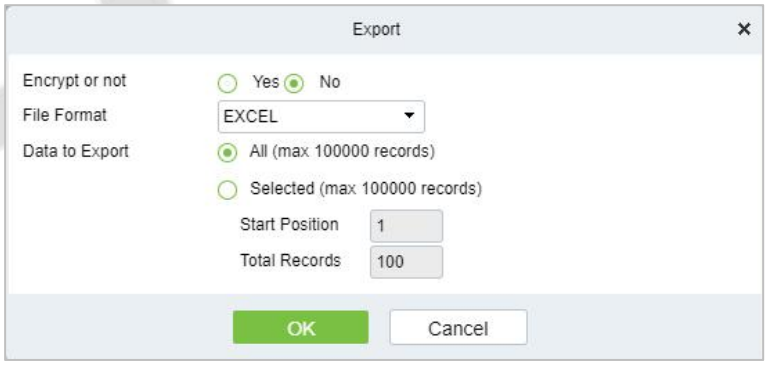


Figure 7- 34 Exit Record of Export Interface

7.6.4Charge Record

The Charge Record Details module provides reports of charging information of all exit vehicles (records with fee of 0 are also generated for fixed vehicles and charging-free temporary vehicles).

7.6.4.1Export

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

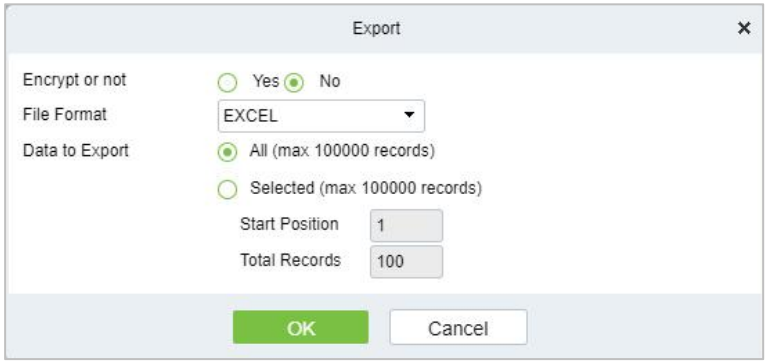


Figure 7- 35 Export interface for Charge Record

Choose **Report Management** > **Charge Details**. Select the desired time period and operator name and click \ to query charging details. Click **More** to query based on other conditions. The page is shown in the following figure.

7.6.5Expired Vehicle

7.6.5.1Incoming Unusual Vehicles

It will provide the details of the vehicle which incoming unusually of the parking.

Click **Report Management** > **Incoming Unusual Vehicles**. Select the desired time period, vehicle owner and license plate number, and click to query Exit records. Click **More** to query based on other conditions.

7.6.5.2Export

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

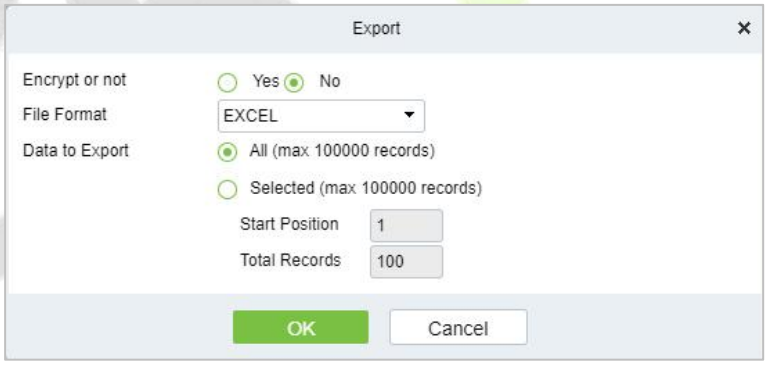


Figure 7- 36 Incoming Unusual Vehicles of Export Interface

7.6.6Authorized Vehicle Records

It will provide the details of the vehicle which fixed authorization records of the parking.

Click **Report Management** > **Fixed vehicle Authorization Record**. Select the desired time period, vehicle owner and license plate number, and click to query Exit records. Click **More** to query based on other conditions.

7.6.6.1Export

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

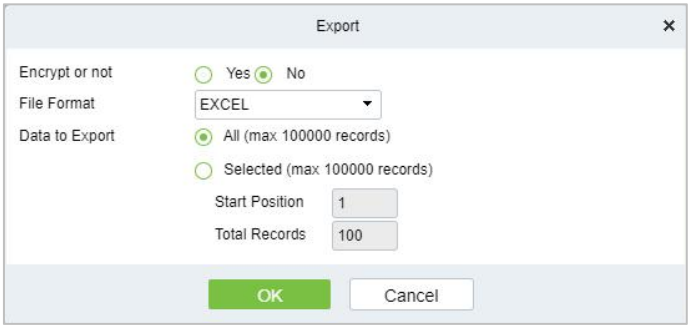


Figure 7- 37 Fixed vehicle Authorization Record of Export Interface

7.6.7Device Operation Records

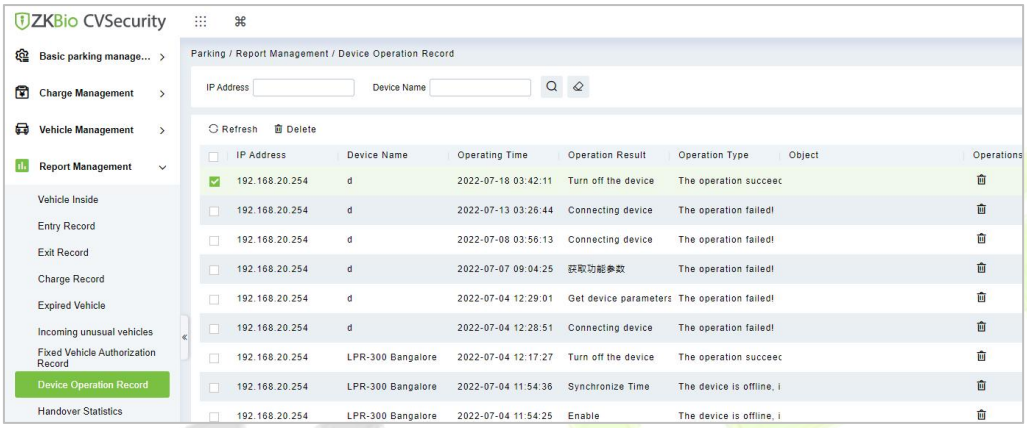


Figure 7- 38 Device Operation Record Interface

7.6.7.1Delete

Select one or more device operation record and click **Delete** at the upper part of the list and click **OK** to delete the selected device operation record. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single device operation record.

7.6.8Handover Statistics

The Handover Record provides reports of handover records.

Choose **Report Management** > **Handover Statistics.** Select the desired time period and operator name and click **** to query handover records. Click **More** to query based on other conditions. The page is shown in the following figure.

7.6.8.1Export

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

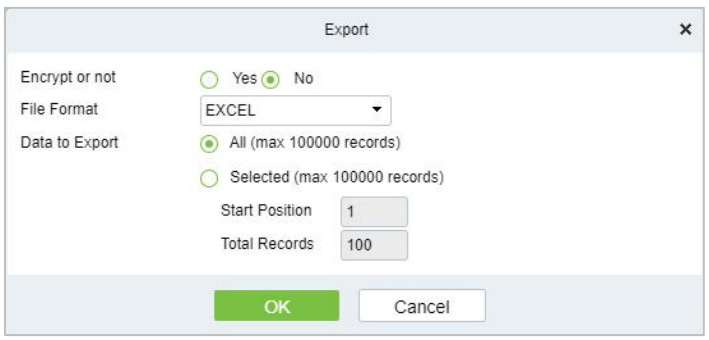


Figure 7- 39 Hand Over Statistics of Export Interface

7.6.9Daily Income Statistics

The Daily Report provides reports of the total amount of charges per day for each shift in each duty guard booth.

Choose **Report Management > Daily Reports**. Select the desired time period and click **** to query the total amount of charges for each shift in each duty guard booth. The page is shown in the following figure.

7.6.9.1Export

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

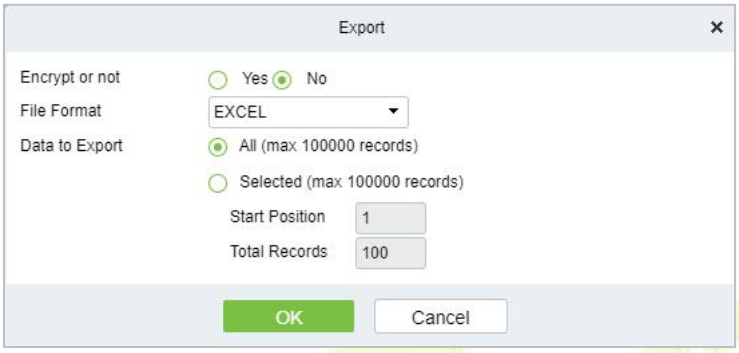


Figure 7- 40 Daily Income Statistics of Export Interface

7.6.10Monthly Income Statistics

The Monthly Report provides statistics of parking fees for each day of the month.

Choose **Report Management > Monthly Reports**. Select the desired time period and click **1A** to query the parking fees the page is shown in the following figure.

7.6.10.1Export

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

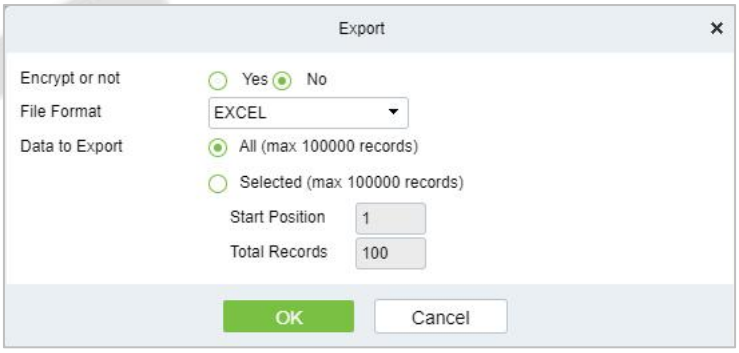


Figure 7- 41 Export Interface of Monthly Income Statistics

7.7 Real-Time Monitoring

This part introduces the configuration of real-time monitoring in parking module and can view the monitoring dynamics in real time in this interface.

7.7.1Booth Monitoring

This part introduces that the configuration of monitoring related information can be viewed in the

booth monitoring interface in, and the administrator can view the monitoring dynamics in the booth monitoring interface.

● Operating Steps:

Step 1: In the Parking module, click "**Parking Real-time Monitoring > Sentry Booth Monitoring**".

Step 2: In the booth monitoring interface, you can view related monitoring videos and events, as shown in figure below.

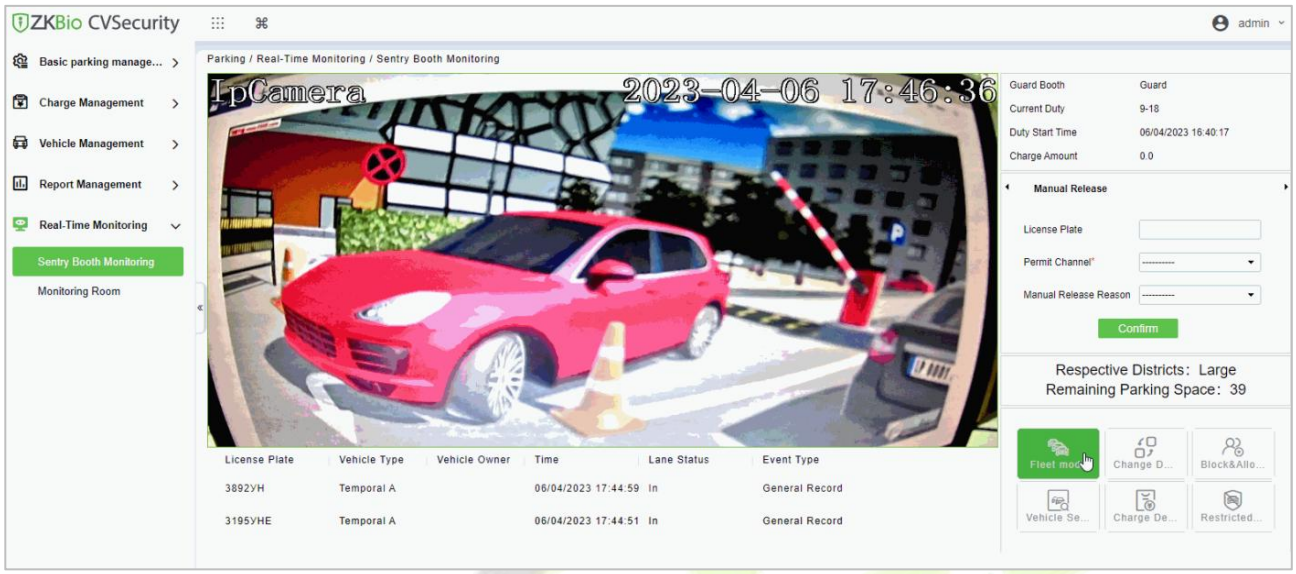


Figure 7- 42 Guard Booth Monitoring Interface

7.7.1.1 Manual Release

This part introduces the manual release function of Guard Booth monitoring, and the administrator can operate the vehicle release in this interface.

● Operating Steps:

Step 1: In the Parking module, click "**Parking Real-time Monitoring > Box Monitoring > Manual Release**".

Step 2: Under manual release, the administrator can operate vehicle release here, and when the vehicle is not recognized, manual release can be performed, as shown in figure below.

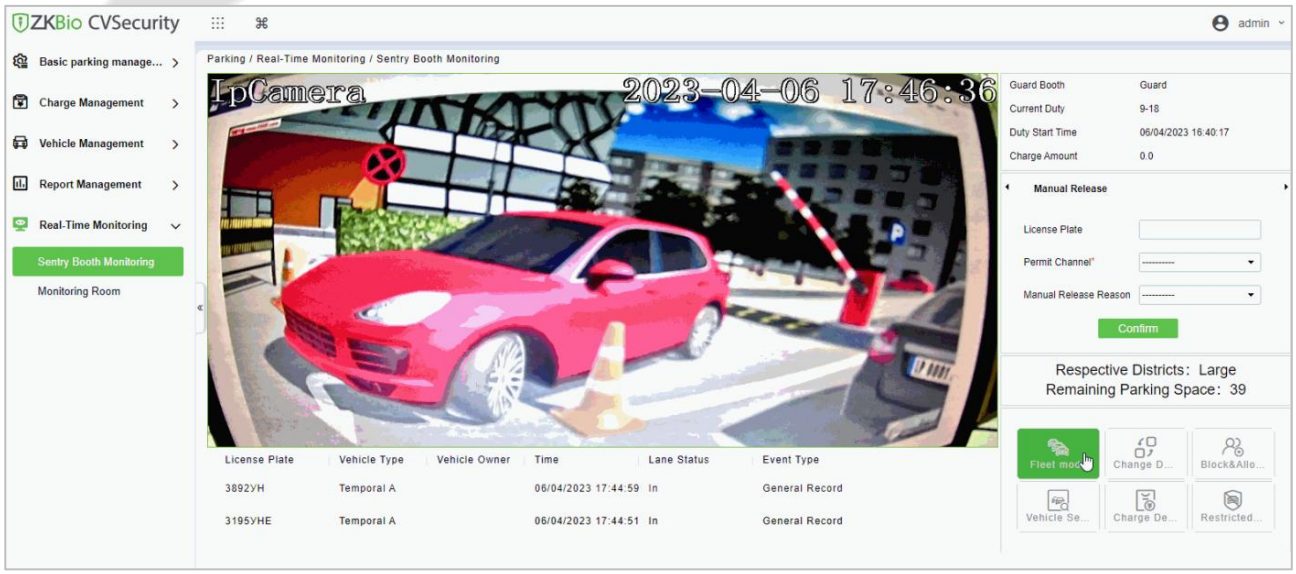


Figure 7- 43 Manual Pass Interface

7.7.1.2Change Shifts

This part introduces the information configuration of personnel shift change in, where you can view the data information of shift change handover when exchanging shifts.

● Operating Steps:

Step 1: In the Parking module, click "**Parking Box Monitoring > Shift Change**".

Step 2: Set the relevant shift information, as shown in figure below, and refer to Table 7-19 for parameter description.

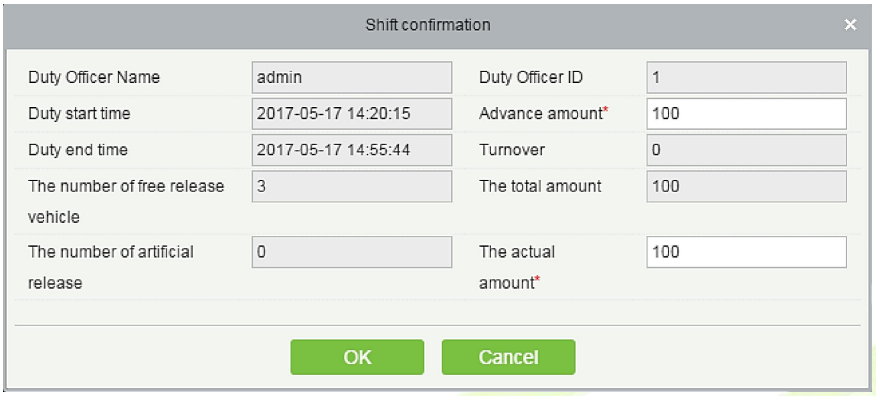


Figure 7- 44 Shift Change Interface

Parameter	Description
Name of Duty Officer	Show the name of the person on duty
Working Hours	Show the working hours of the personnel on duty
attendance Checking Hours	Display the attendance checking time of the attendant
Number of Vehicles Released Free of Charge	Number of vehicles allowed to be released free of charge
Number of Manual Switches	Number of times of manual release through manual gate opening
Advance Amount	Such as reserve amount, such as reserve for change
Preferential Amount	Amount of parking discount
Turnover	Business amount generated by parking lot charges
Total Amount	Total amount of car park revenue
Actual Amount	Actual amount of parking lot income (net income)

Table 7- 19 Description of Shift Change Parameters

Step 3: Enter the account number and password of the shift changer.

Step 4: Click **OK** to complete the setting of booth shift change.

7.7.2Monitoring Room

This part introduces that the configuration of monitoring related information can be viewed in the monitoring room interface in, and the administrator can view the monitoring dynamics in the monitoring room interface.

●Operating Steps:

Step 1: In the Parking module, click "**Parking Real-Time Monitoring > Monitor Room**".

Step 2: You can view relevant monitoring videos and data statistics in the monitoring room interface, as shown in figure below.

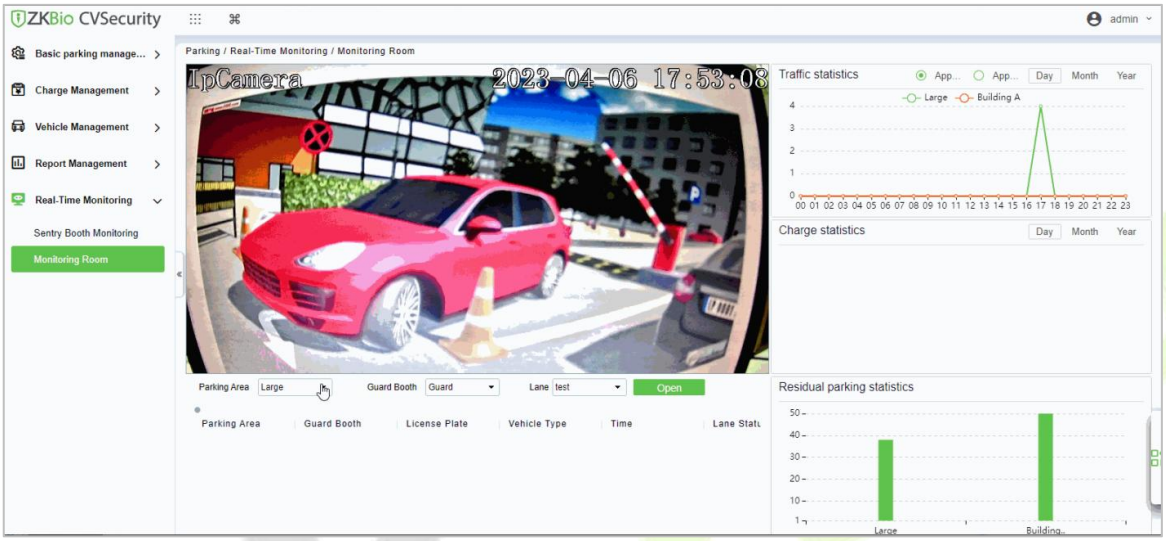


Figure 7- 45 Monitoring Room Interface

7.7.2.1Manual Barrier Opening

This part introduces the Step configuration that the administrator can open the Barrier manually, which can be used to open the Barrier manually when the vehicle is not recognized.

●Operating Steps:

Step 1: In the Parking module, click "**Parking Real-time Monitoring > Monitor Room**".

Step 2: In the monitor room interface, click "Open Gate-Enter License Plate Number-Confirm Open Gate", as shown in figure below.

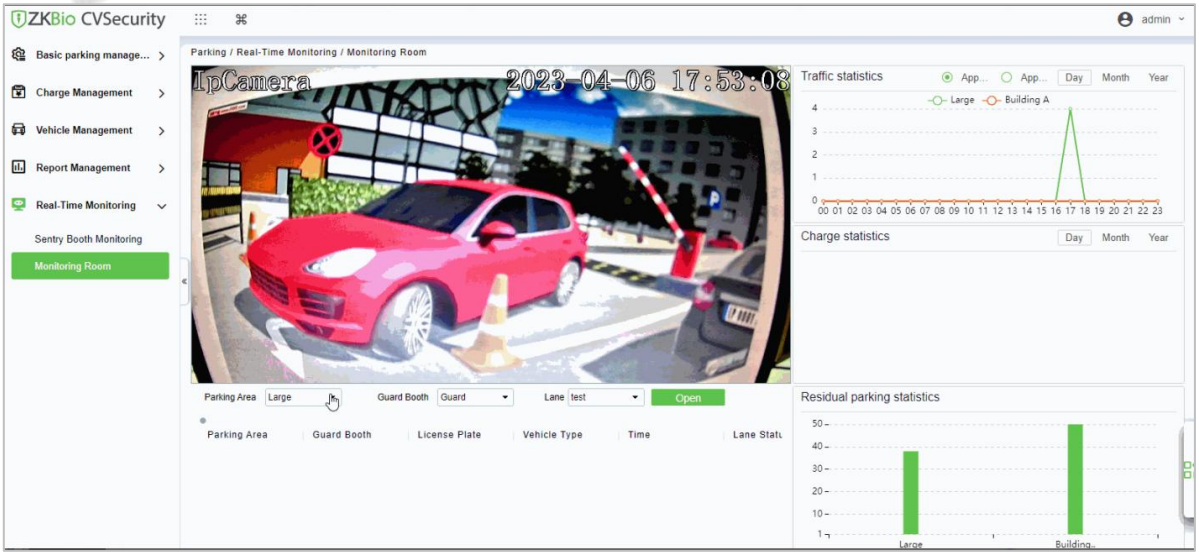


Figure 7- 46 Switch Interface

7.8 Ticket Dispenser Management

A parking lot ticket dispenser is a form of gate that allows pedestrians to pass through a designated area one at a time. They are typically installed in parking areas that are unattended.

7.8.1 Authorized Products (BEST-W Protocol)

Obtain Best-W protocol secret key and upload it to the ticket dispenser for authorization binding.

● Operation:

Step 1: Click **System > Communication Management > Product > New**, Add a product.

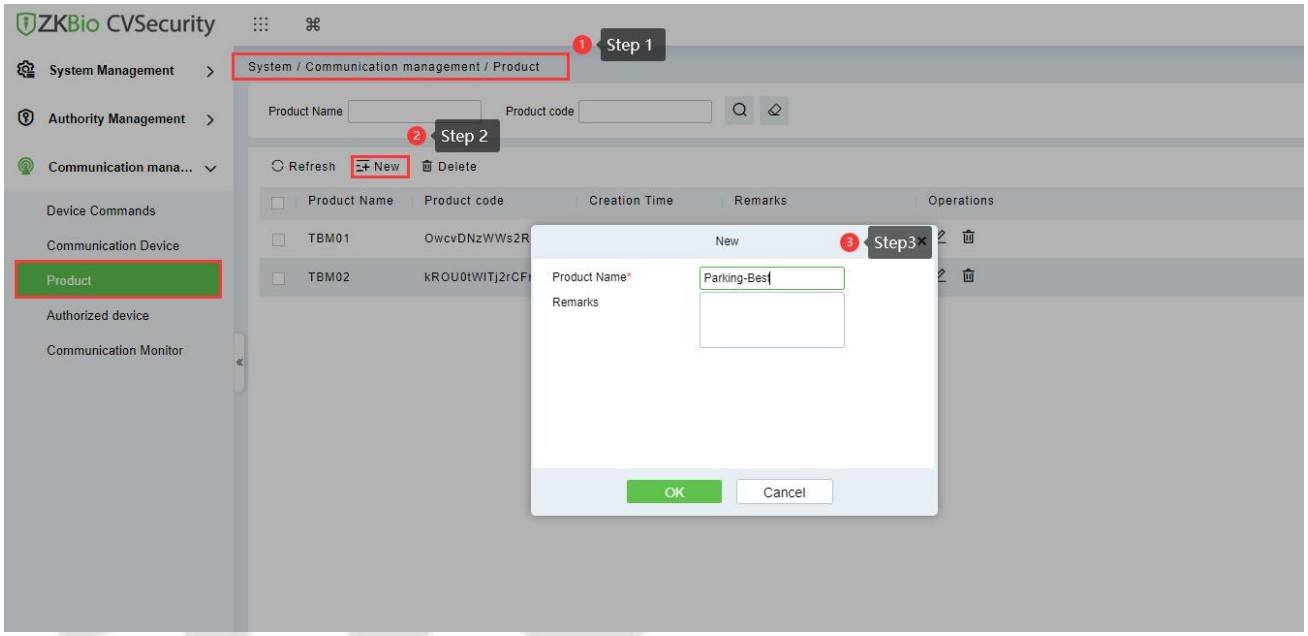


Figure 7- 47 Add a product

Step 2: Click **System > Communication Management > Authorized device > New**, enter the device serial number to generate the secret key.

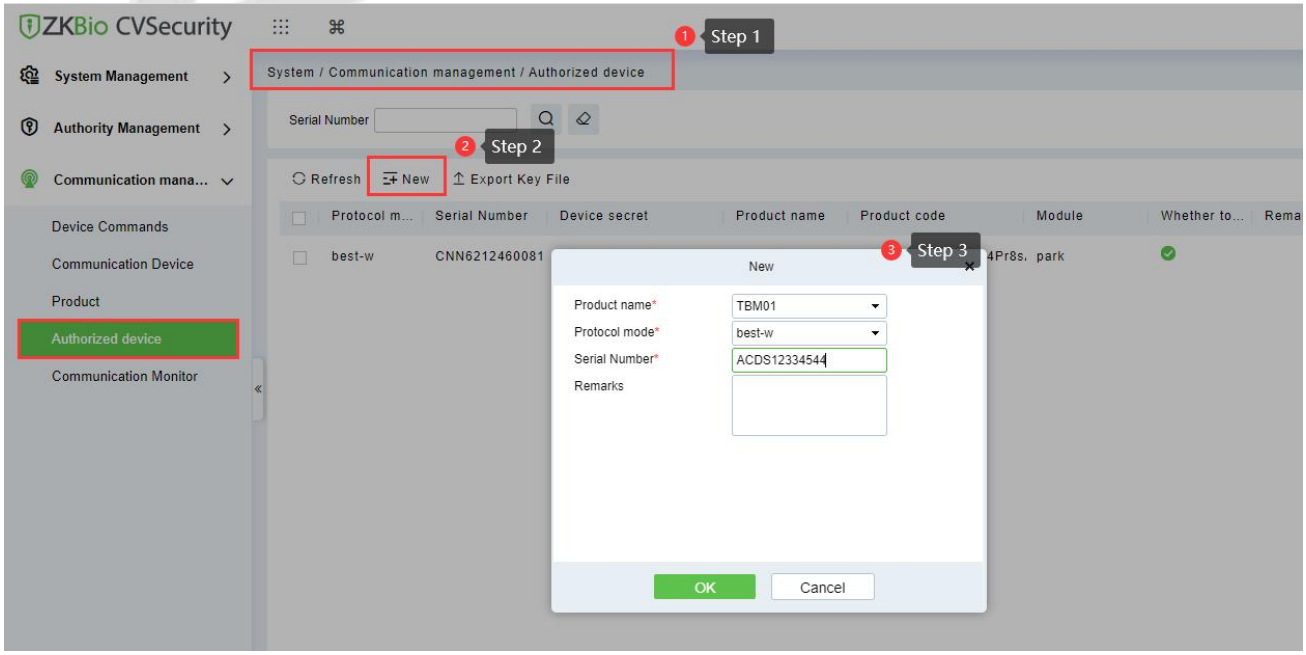


Figure 7- 48 Authorized Device

Select the product, click **Export Key File**, enter the activation time and click **Export.**

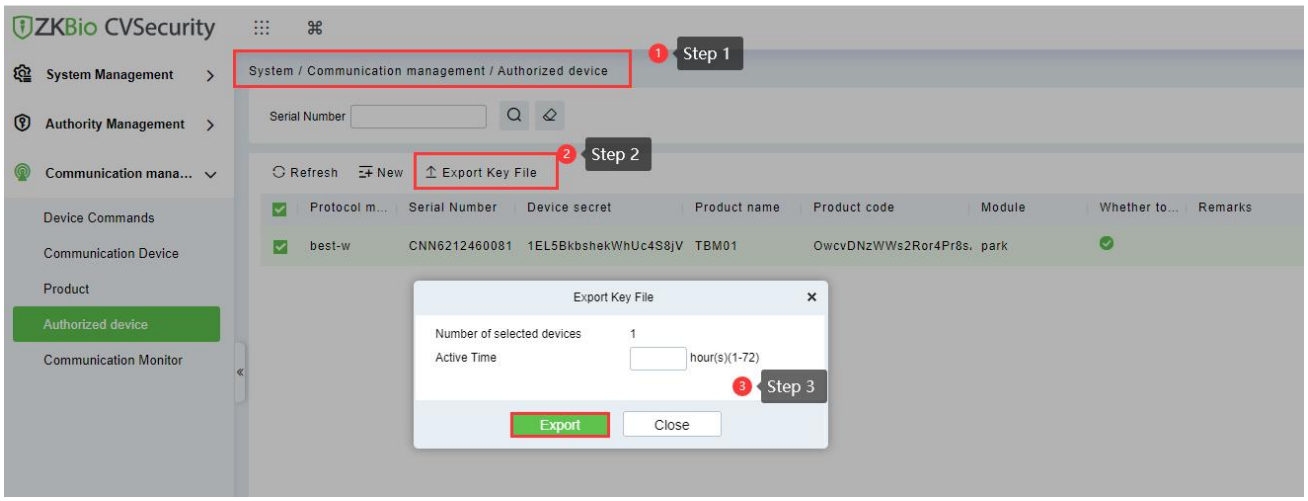


Figure 7- 49 Export Key File

Active Time: The secret key activation time range, after that, the secret key cannot be used again.

Step 3: Login in TBM01 web page, click Setup > Comm Configuration > Best Configuration and Enable Best.

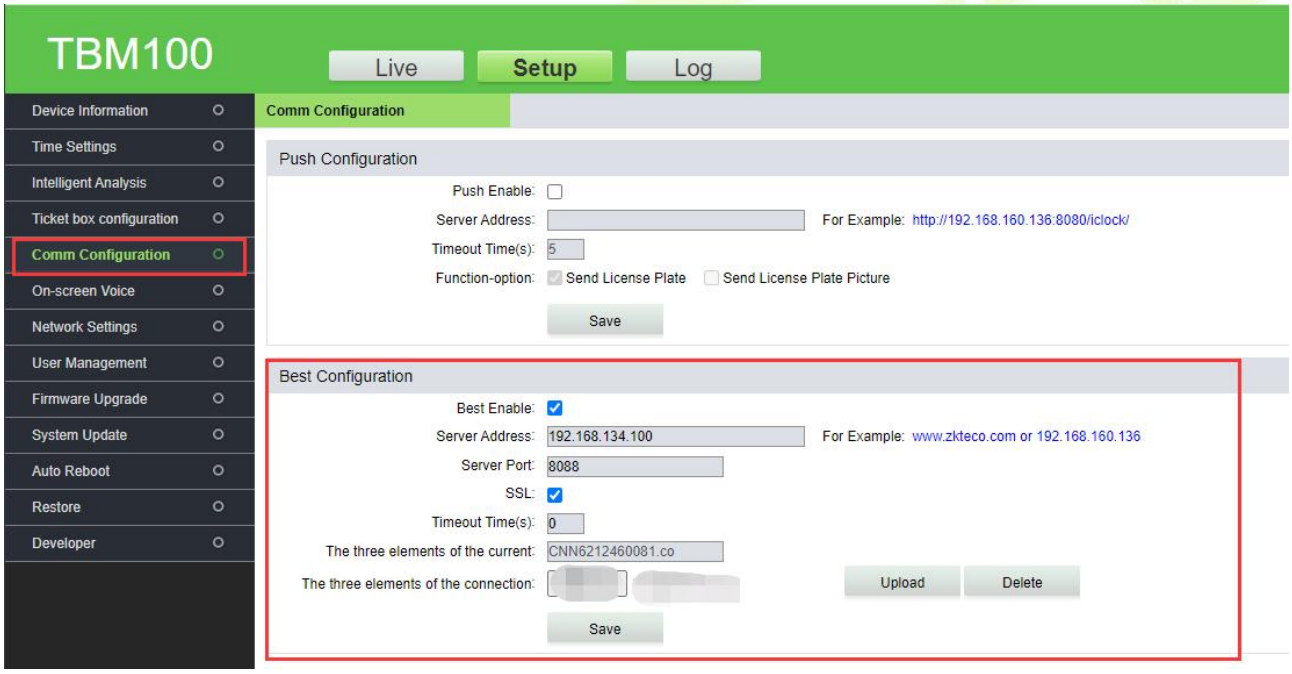


Figure 7- 50 TBM01 Web Page

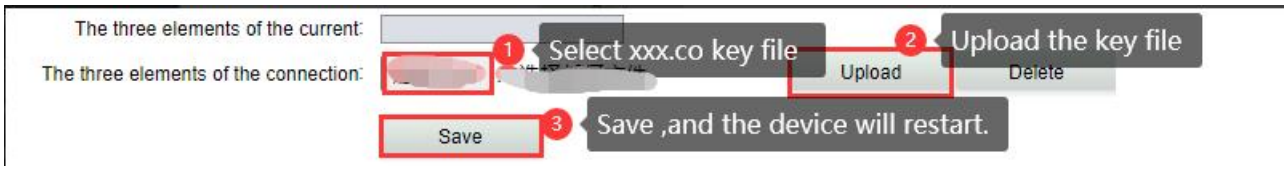


Figure 7- 51 Import Key File

Fields are as follows:

Parameter	Description
Server Address	Server address of the connected ZKBio CVSecurity .
Server Port	The port for the device to communicate with ZKBio CVSecurity,

Parameter	Description
	default is 8088.
SSL	Whether the ZKBio CVSecurity server is encrypted or not, and if it is HTTPS then Enable SSL.
Timeout Time(s)	Communication timeout connection time.
The three elements of the current	The secret key exported from ZKBio CVSecurity and decompressed; the key format is "SNXXXXX.co"
The three elements of the connection	Select the Key of "SN.co", click Upload, then **Save** and the device will restart.

Table 7- 20 Comm setting

Note: The firmware of ticket dispenser should be higher than" V9.2.4.20221223.16 ".

7.8.2Set Parking Parameter

Enabling BEST protocol and ticket dispenser for ZKBio CVSecurity.

Step 1: Go to ZKBio CVSecurity Parking Module, click **Parking > Basic Parking Management > Parking Lot Setting >Communication Mode**, select BEST-W.

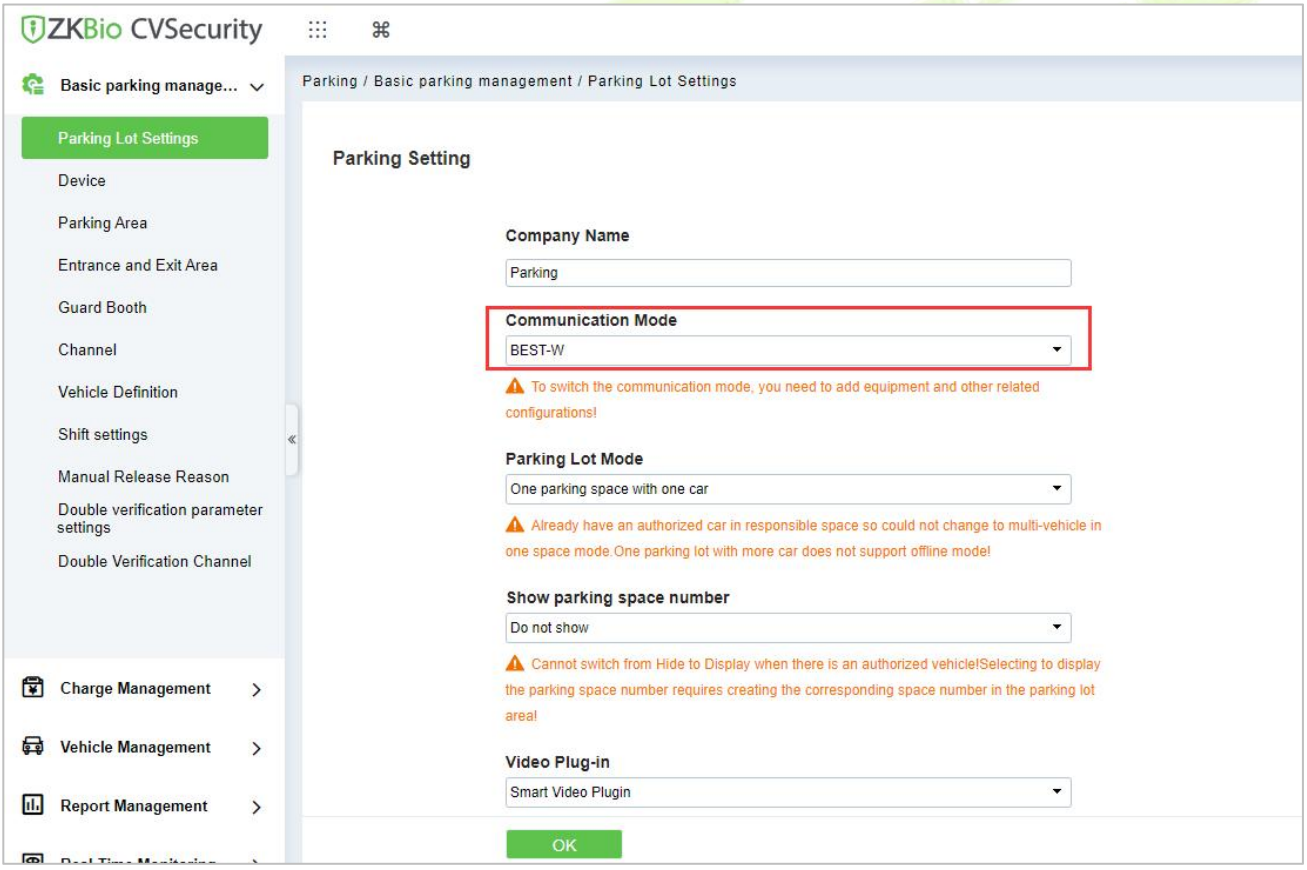


Figure 7- 52 Enable BEST-W

7.8.2.1Entrance and Exit Lane Setting

Click **Parking > Basic Parking Management > Parking Lot Setting> Entrance and Exit Lane Setting > Enable Ticket box**.

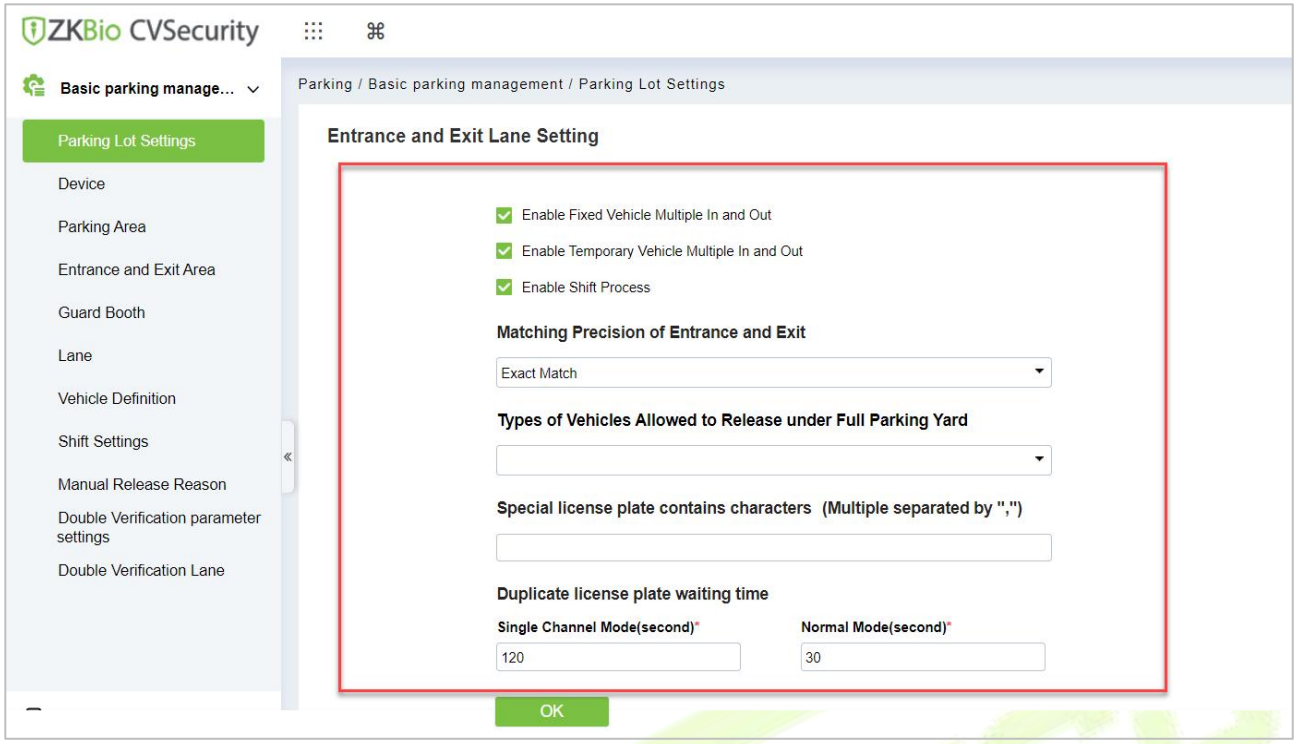


Figure 7- 53

Fields are as follows:

Parameter	Description	Parameter
Entrance and Exit Lane Setting	Enable the fixed or temporary vehicles are multiple In and out.	Allow the fixed or Temporary vehicles to the parking area and vehicles are multiple in and out.
	Matching Precision of Entrance and Exit	vehicles are allowed by exact match and 5 or 6digits registration numbers to the entrance and exit area of the parking.
	Types of Vehicles Allowed to Release under Full parking Yard	vehicles are allowed like small size, larger or medium vehicle.
	Special license plate contains characters	Enter the special license plates contains characters wherever required.
	Duplicate license plate waiting time	In Duplicate license plate waiting time Mention the timings of single channel mode and normal mode

Table 7- 21

7.8.2.2Charge Management Setting

Click P**arking > Basic Parking Management > Parking Lot Setting> Charge Management Setting > Enable Ticket box**.

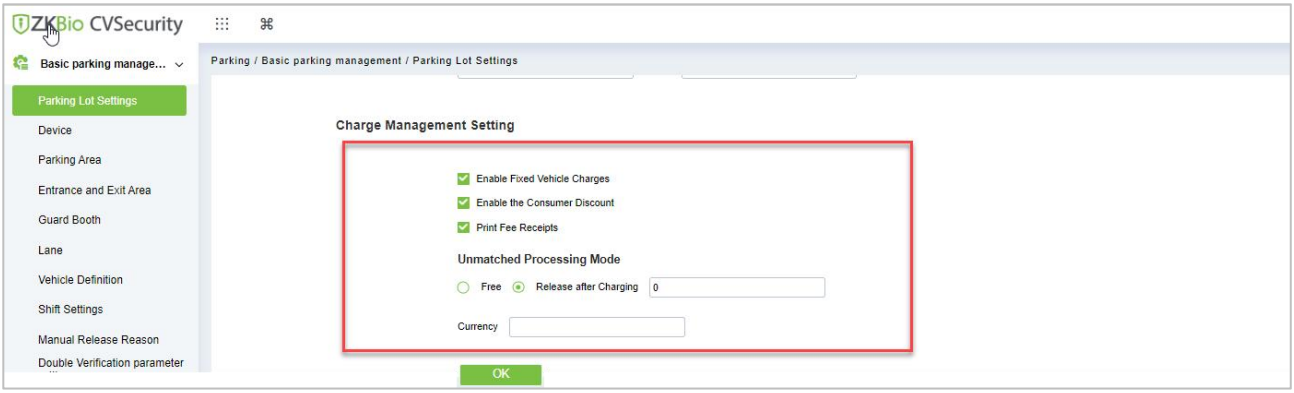


Figure 7- 54

Fields are as follows:

Parameter	Specific Parameters	Parameter Description
Charge Management Settings	Enable the fixed Vehicle charges	If the fixed vehicle charging standard has been set in advance, check this setting, and when the fixed vehicle is authorized and postponed, it will be implemented according to this charging standard; If it is not checked, you can only manually enter the extension time and amount.
	Print the fee receipt	If the receipt printer is set and connected, the corresponding receipt will be printed when the charge is successful.
	Enable consumption discounts	Set the "Discount Strategy" in advance and then check the Enable Consumption Discount System, and the consumption discount will be carried out.
	Unmatched processing mode	There are two existing ways to deal with mismatches: "free release" and "opening the gate after charging fees"; Manual release is to open the gate directly, and when the gate is opened after charging, a charge confirmation box will pop up during manual release (only for temporary vehicles).

Table 7- 22

7.8.2.3Fixed Vehicle Setting

Click **Parking > Basic Parking Management > Parking Lot Setting> Fixed Vehicle Setting > Enable Ticket box**.

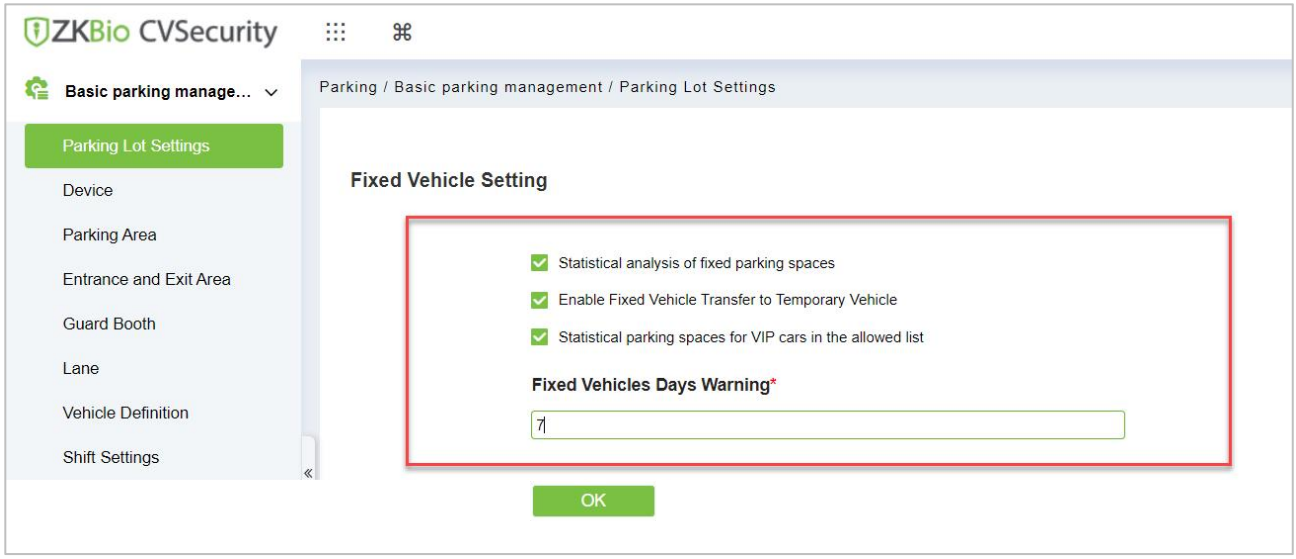


Figure 7- 55

Fields are as follows:

Parameter	Specific Parameters	**Parameter Description**
Fixed Vehicle Setting	Statistical analysis of fixed parking spaces	If it is checked, the number of vehicles will not be deducted after authorization, and the number of vehicles will be counted in real time when vehicles enter and leave the field.If it is not checked, the number of fixed vehicles will be deducted after authorization.
	Enable fixed vehicle transfer to temporary vehicles	If this option is checked, the fixed vehicles will be automatically converted into a temporary vehicles after it expires, and the charge will be made according to the temporary charging method. If it is not checked, this option will require manual release for the fixed vehicles to come out when it expires.
	Statistical parking spaces for VIP cars in the allowed list	Only for VIP vehicles to park in the allowed specific area space.
	Warning days for fixed vehicles	If the warning days are set to 5 days, it is necessary to prompt the vehicles to postpone the fixed vehicles when entering and leaving the field within 5 days.

Table 7- 23

7.8.2.4Voice and Display Setting

Click **Parking > Basic Parking Management > Parking Lot Setting> Voice and Display Setting > Enable Ticket box**.

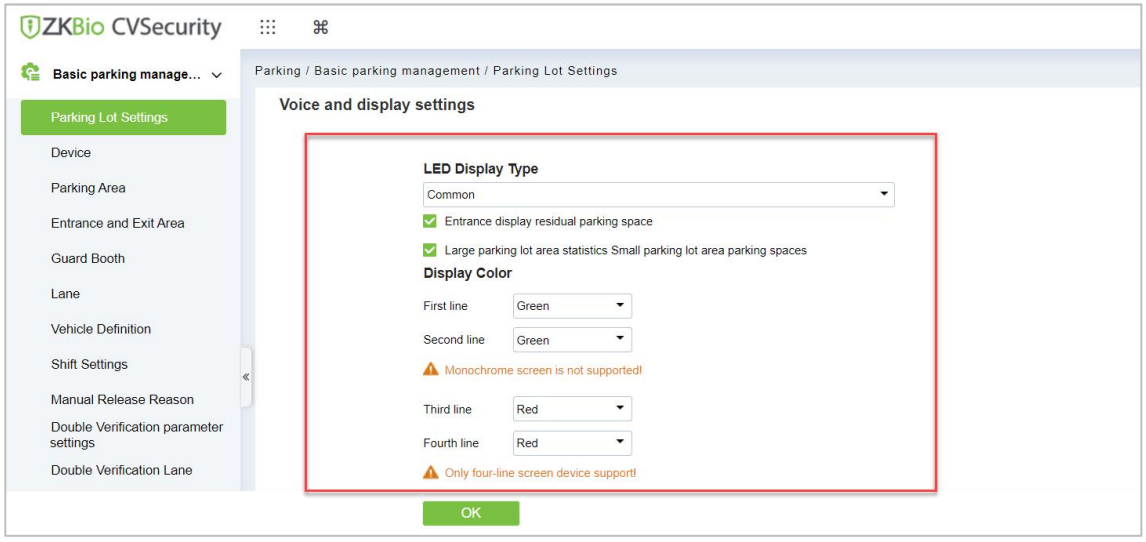


Figure 7- 56

Fields are as follows:

Parameter	Specific Parameters	**Parameter Description**
Voice and display settings	The entrance shows the remaining parking spaces	Display the remaining parking spaces at the entrance of the parking lot.
	Statistics of car Parking area parking spaces in car Parking area	The statistics of the number of cars in the corresponding booth in the big Parking area include the number of cars in the small Parking area.
	Display color	Set the display color of parking machine.

Table 7- 24

Click **Parking > Basic Parking Management > Parking Lot Setting> Ticket Dispenser setting > Enable Ticket box**.

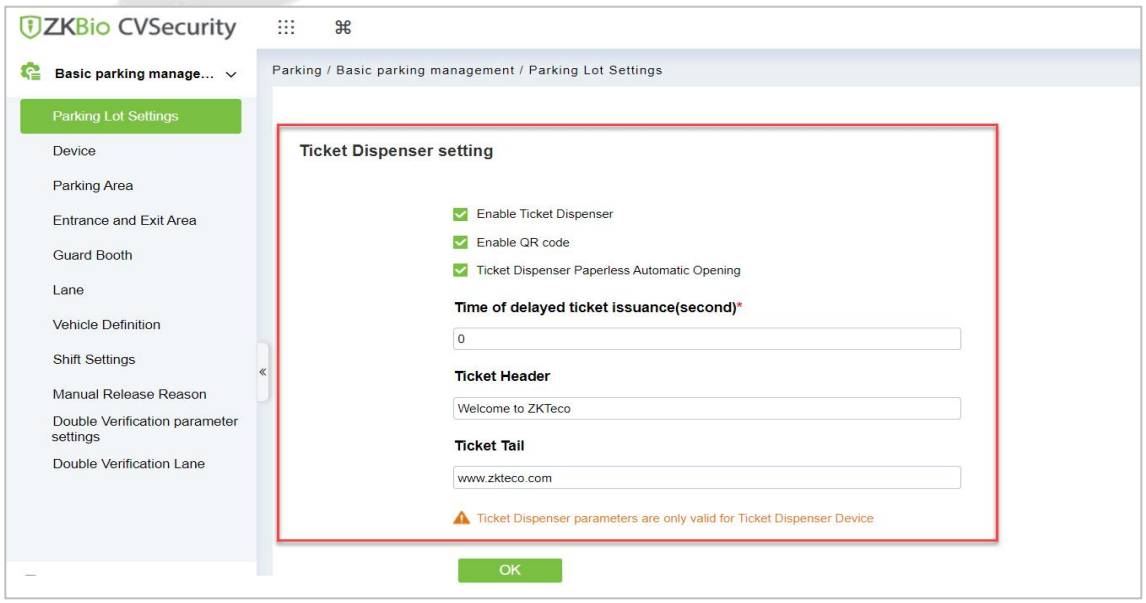


Figure 7- 57 Enable Ticket Dispenser

Fields are as follows:

Parameter	Specific Parameters	Parameter Description
Ticket Dispenser Settings	Enable Ticket Dispenser	Enable the platform's ticket dispenser function.
	Enable QR Code	Enable QR Code function. Print barcode if unchecked.
	Ticket Dispenser Paperless Automatic Opening	After setting, if there is no printing paper in the ticket dispenser, the barrier will open.
	Time of delayed ticket issuance(second)	Ticket dispenser delays printing after the vehicle is detected.
	Ticket Header	What is displayed in the header of the ticket.
	Ticket Tail	What is displayed in the tail of the ticket.

Table 7- 25 Enable Ticket Dispenser

7.8.2.5Protection of Personal Sensitive Information

Click **Parking > Basic Parking Management > Parking Lot Setting> Protection of Personal Sensitive Information > Enable Ticket box**.

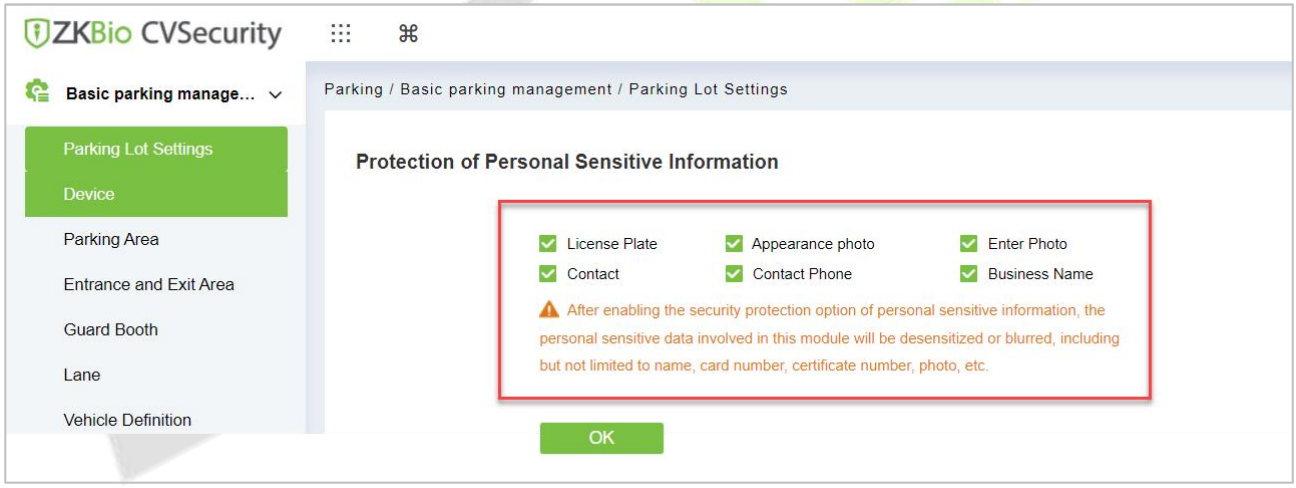


Figure 7- 58

Fields are as follows:

Parameter	Specific Parameters	Parameter Description
Protection of personal sensitive information	Enable personal sensitive information	Enable the License Plate, Appearance photo, Enter photo, Contact/phone, Business Name, for security protection.

Table 7- 26 Parameter

7.8.2.6Other Setting

Click **Parking > Basic Parking Management > Parking Lot Setting> Other Setting > Enable Ticket box**.

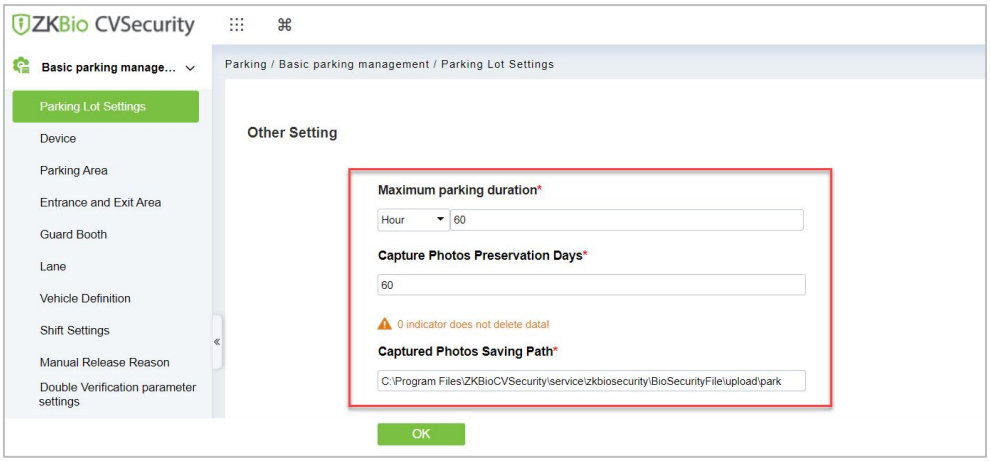


Figure 7- 59

Fields are as follows:

Parameter	Specific Parameters	Parameter Description
Other Settings	Maximum parking duration	Set the maximum stay time of on-site vehicles. If the on-site vehicles have not left after this time, the records of on-site vehicles will be displayed in the "On-site Stay Timeout Vehicles" report.
	save days of captured photos	Set captured photos saved more than the set number of days photos will be automatically deleted, if you do not want to delete captured photos will change the parameter set to 0 days.
	captured photos Saving Path	You can customize the path where photos are saved.

Table 7- 27

7.8.2.7Offline Setting

Click **Parking > Basic Parking Management > Parking Lot Setting> Offline Setting > Enable Lifeline Mode**.

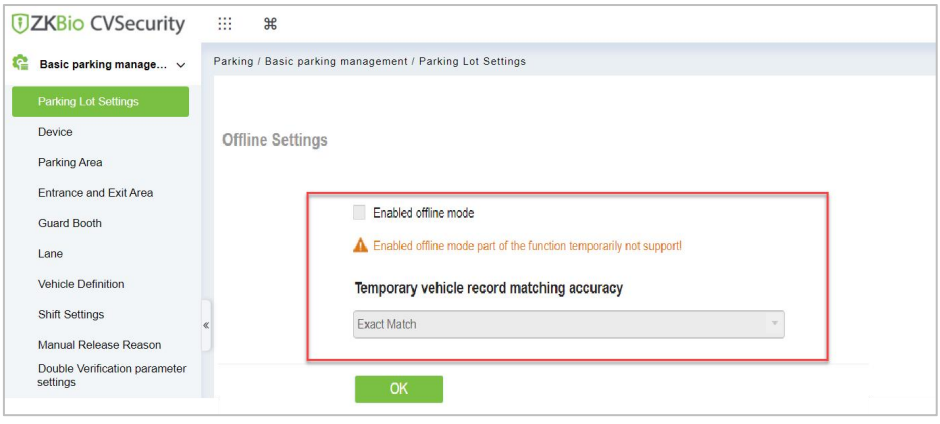


Figure 7- 60

Fields are as follows:

Parameter	Specific Parameters	Parameter Description
Offline Setting	Enable offline mode	Enable the License Plate, Appearance photo, Enter photo, Contact/phone, Business Name, for security protection.
	Temporary vehicle record matching	vehicles are allowed by exact match and 5 or 6digits registration numbers to the entrance and exit area of the parking.

Table 7- 28

7.8.3Add Ticket Dispenser

Add ticket dispenser to ZKBio CVSecurity.

7.8.3.1Search

Click **Parking > Basic Parking Management > Device >Search**, search and add the ticket dispenser.

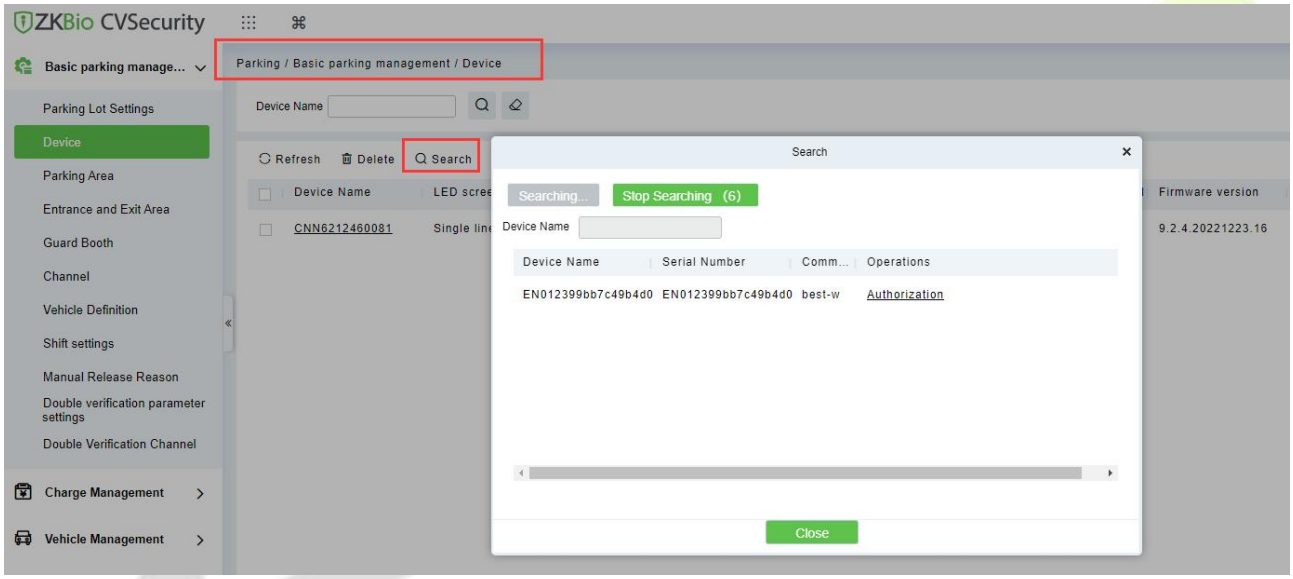


Figure 7- 61 Search device

After searching, click **Authorization**.

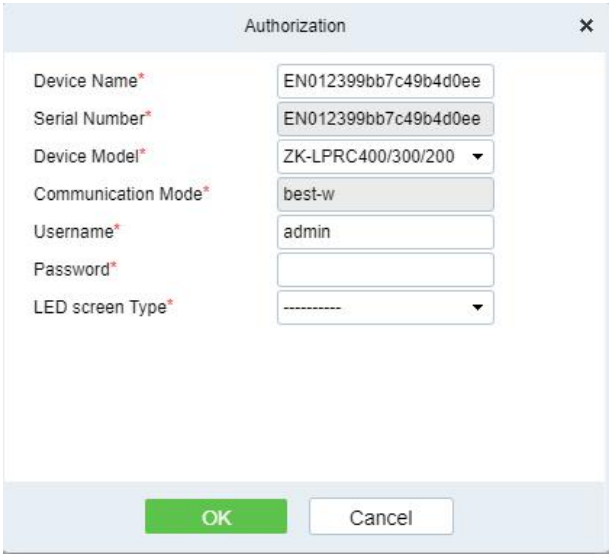


Figure 7- 62 Add device

Fields are as follows:

Parameter	Description
Device Name	The name of your ticket dispenser device
Serial Number	The serial number of devices
Device Model	Select ZK-TBM100
Communication Mode	Use BEST-W Protocol.
Username	Login name, default is admin.
Password	Login password, the default is 123456
LED Screen Type	Types of LED screens for ticket dispenser.

Table 7- 29 Add device

7.8.3.2Add New

Operating Steps:

Step 1: In the Parking module, select **Parking Basic Management > Device**.

Step 2: In the **Device** interface, click **Add New** and fill in the relevant parameters, as shown in figure below.

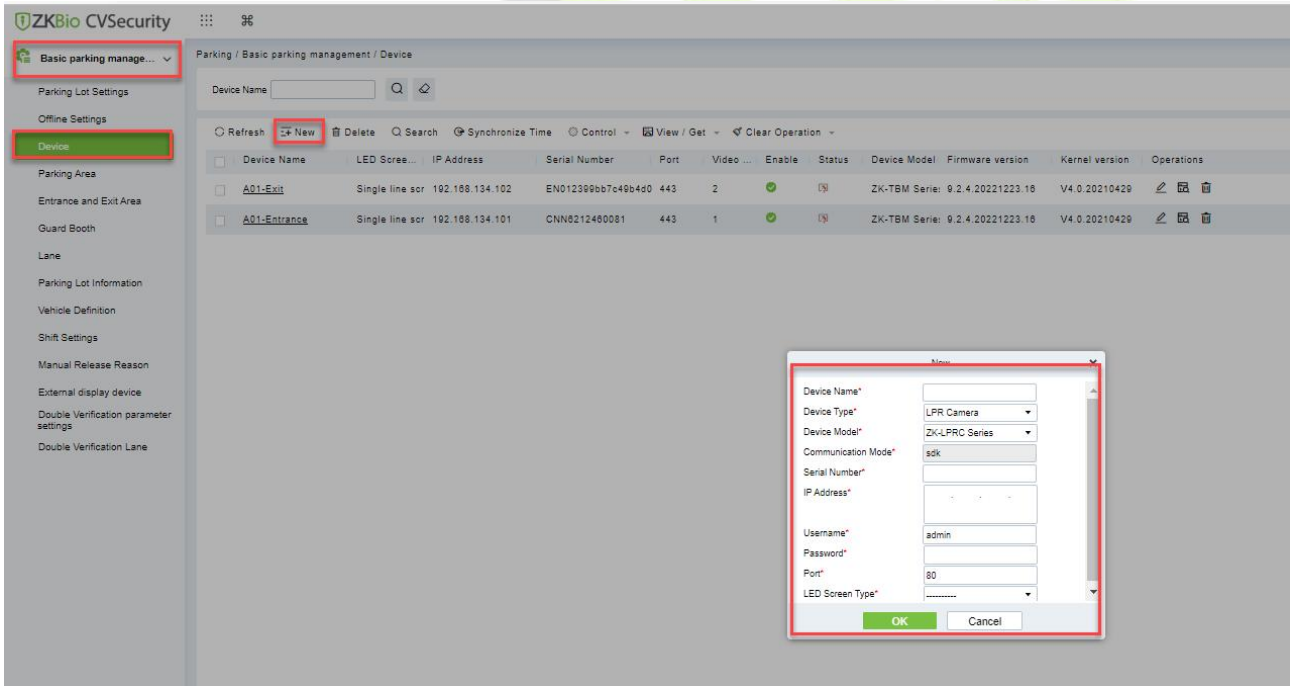


Figure 7- 63

Fields are as follows:

Parameter	Description
Device Name	The name of your ticket dispenser device
Device Type	The type of the device.
Serial Number	The serial number of devices
Device Model	Select ZK-TBM100

Parameter	Description
Communication Mode	Use BEST-W Protocol.
IP Address	The IP address of your device.
Username	Login name, default is admin.
Password	Login password, the default is 123456
LED Screen Type	Types of LED screens for ticket dispenser.

Table 7- 30

Step 3: Click **OK** to complete the setting of the Parking area.

7.8.3.3Refresh

Refresh the current page.

7.8.3.4Delete

Select **device**, click **Delete**, and click **OK** to delete the device.

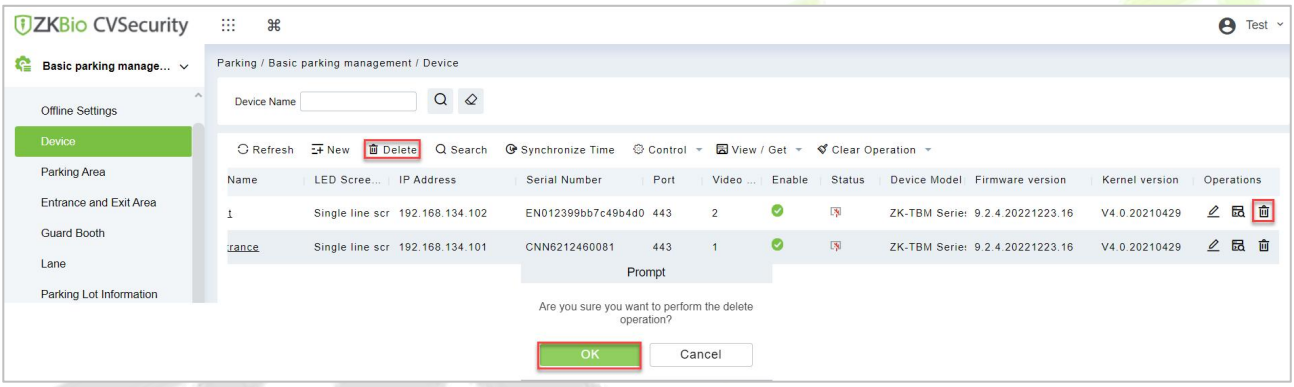


Figure 7- 64 Delete device

7.8.3.5Synchronize Time

It will synchronize device time with server's current time.

7.8.3.6Control

Reboot Device: After clicking on it, the device will restart.

7.8.3.7View/Get

Get device parameters: Get the device parameters, such as IP Address, and video port, etc.

Get device version: Get the firmware version of device.

7.8.3.8Clear Operation

Clear blocklist: Clear blocklisted license plates.

Clear allowlist: Clear allowlist license plates.

Clear fixed vehicle: Clear the fixed vehicle.

7.8.3.9Operations

: Edit the selected device.

: View all commands for the device.

: Delete the selected device.

7.8.4Lane Setting

Preconditions: Refer to 9 Parking Module to configure the parking area, entrance and exit area, guard booth.

Operation Step

Step 1: Click **Parking > Basic parking management > Lane.** Add the ticket dispenser device to the channel.

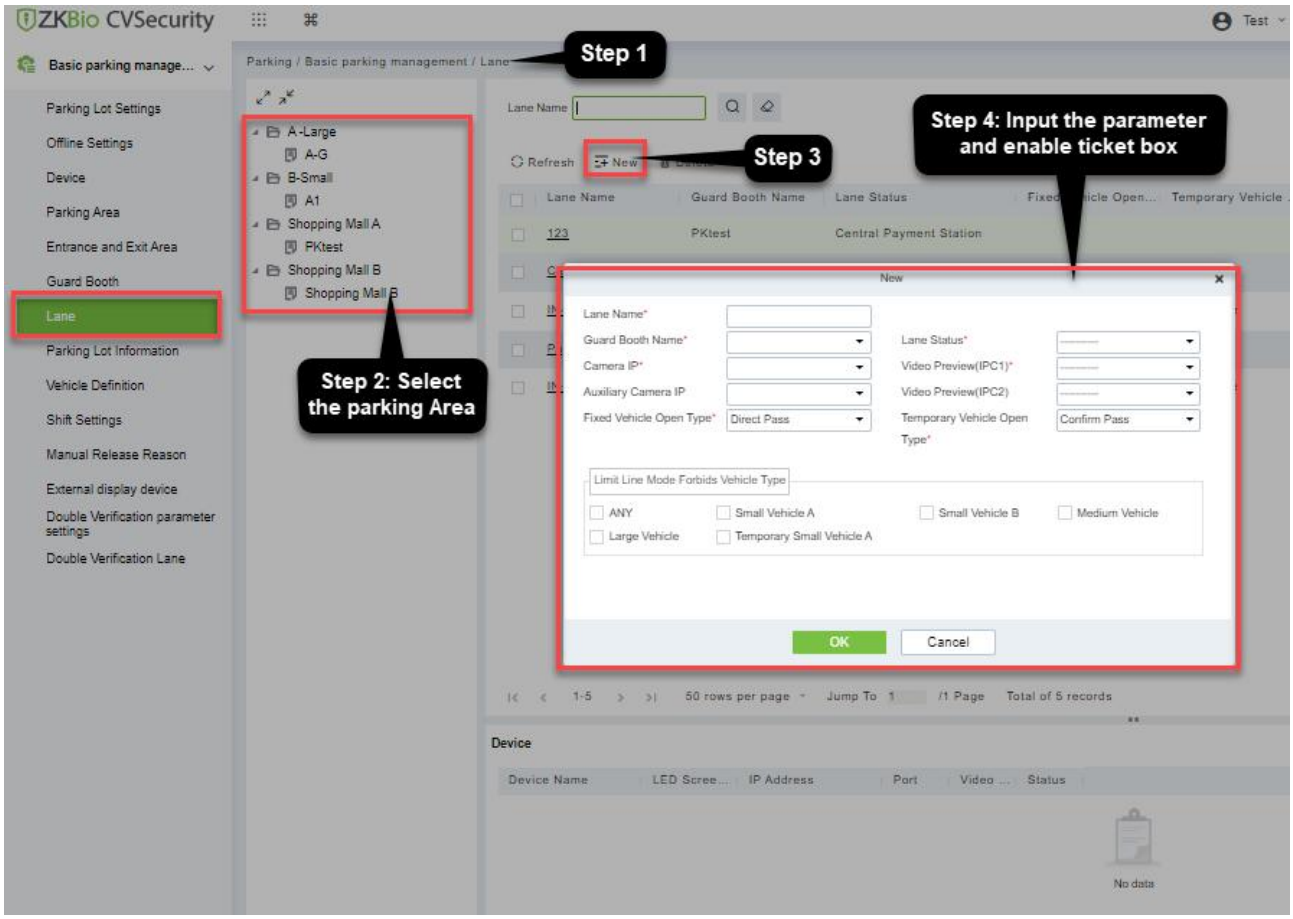


Figure 7- 65 Add channel

Fields are as follows:

Parameter	Description
Lane Name	You can customize the lane name here
Guard Both Name	Select the corresponding booth
Lane Status	Select the channel properties of the entrance and exit of the corresponding booth entrance and exit area
Camera IP	The ip address of device 1, and the corresponding video port position is the monitoring position where the device is located
Auxiliary Camera IP	The ip address of device 2, and the corresponding video port position is the monitoring position where the device is located

Parameter	Description
Video Preview Windows (IPC)	Windows for real-time monitoring of booth
Fixed Vehicle Open Type	Direct pass: card identification successfully opens the barrier. Confirm pass: after successful card identification, booth confirmation is required before opening the door
Temporary Vehicle Open Type	Direct pass: after Printing ticket open the barrier. Confirm pass: if the temporary vehicle need to charged, select "Confirm pass"

Table 7- 31 Lane Setting

Step 3: Click **OK** to complete the lane setting.

7.8.4.1 Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

7.8.4.2 Delete

Select one or more channels and click Delete at the upper part of the list and click OK to delete the selected channels. Click Cancel to cancel the operation or click Delete in the operation column to delete a single channel.

7.8.5 Vehicle Authorization

7.8.5.1 Fixed Vehicle Authorization

Vehicles for internal personnel in the case of using the ticket box, vehicles of internal personnel must swipe their cards to enter and exit.

Operation Steps:

Step 1: Click **Personnel** > **Personnel** > **Person** > **New**, add a new person, register card and license plate.

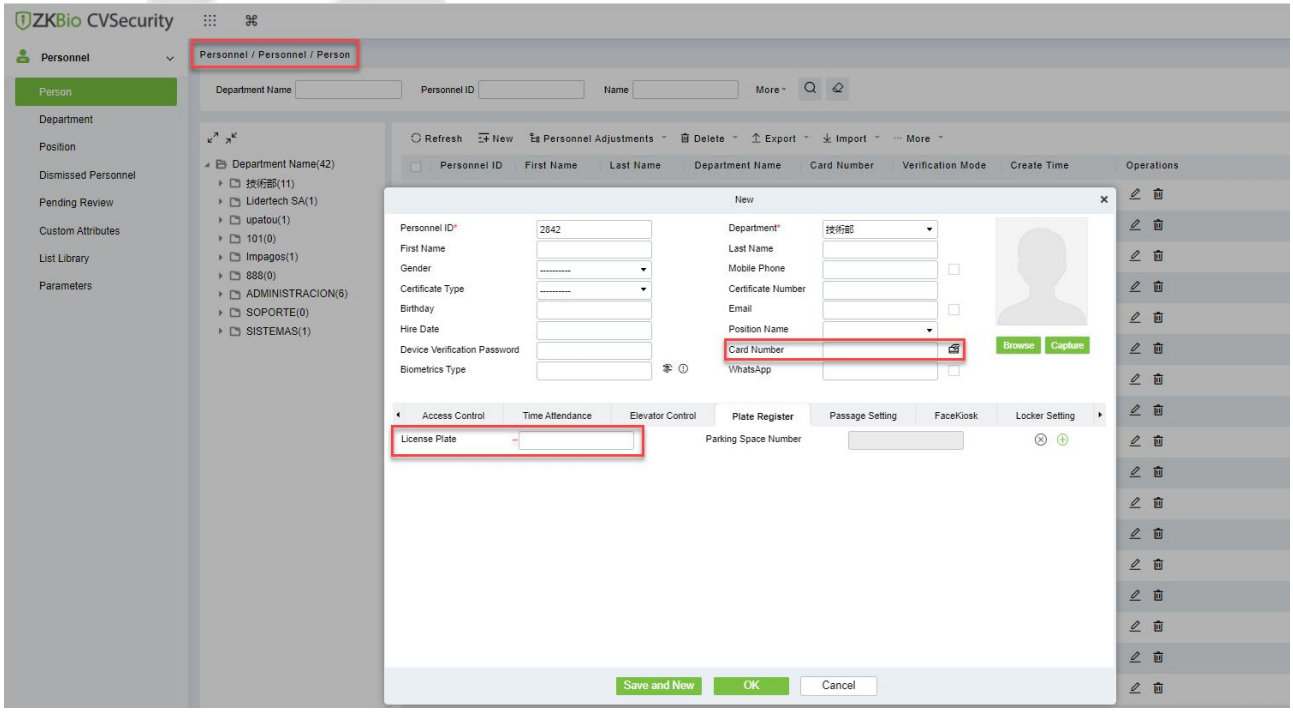


Figure 7- 66 Add personnel

Step 2: Click **Parking > Vehicle Management > Vehicle Authorization> Fixed Vehicle Batch Authorization**, select the personnel and authorization.

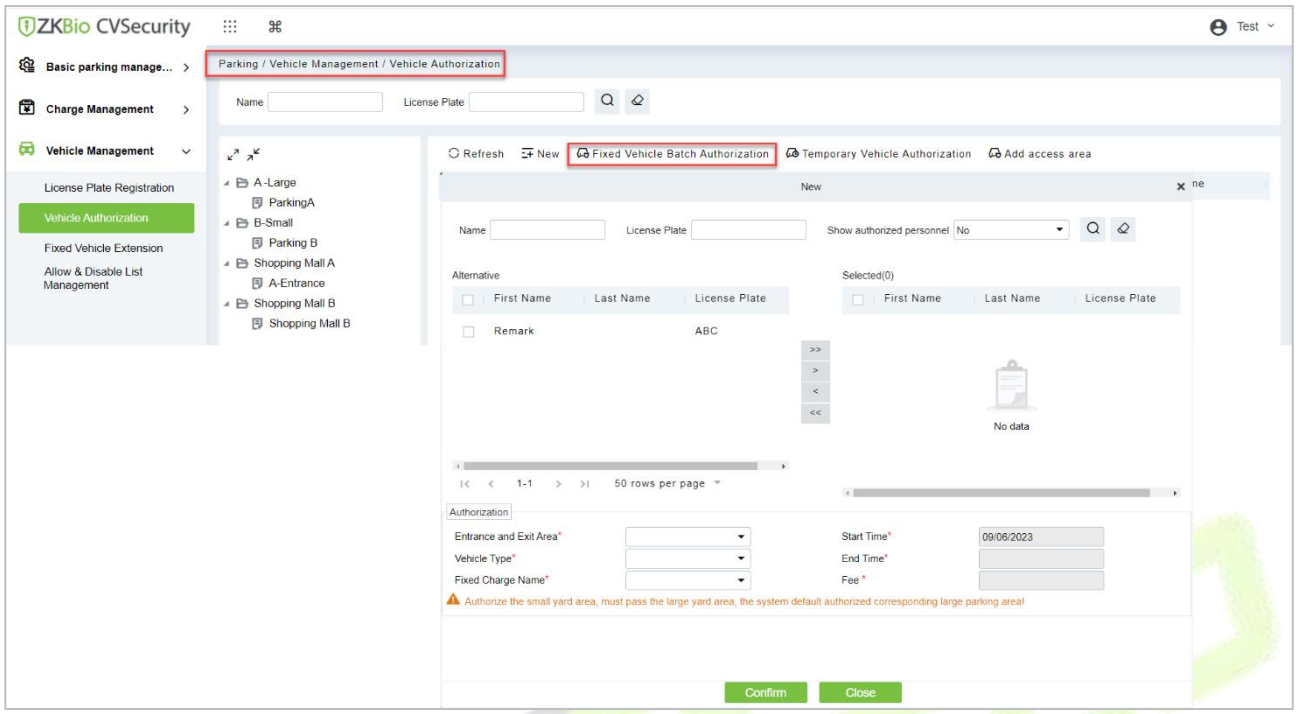


Figure 7- 67 Fixed vehicle Batch Authorization

Step 3: Successfully authorized vehicles will be displayed in the list.

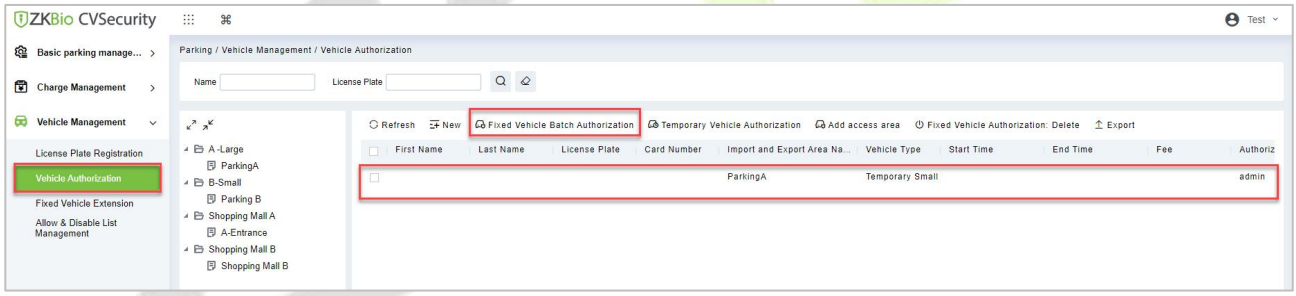


Figure 7- 68 Authorization list

7.8.5.2Temporary Vehicle Authorization

Temporary cars print tickets at the entrance ticket dispenser and exit after scanning the QR code and charging.

Operation Step:

Step 1: Click **Parking > Vehicle Management > Vehicle Authorization> Temporary Vehicle Authorization**. Authorize access areas for temporary vehicles.

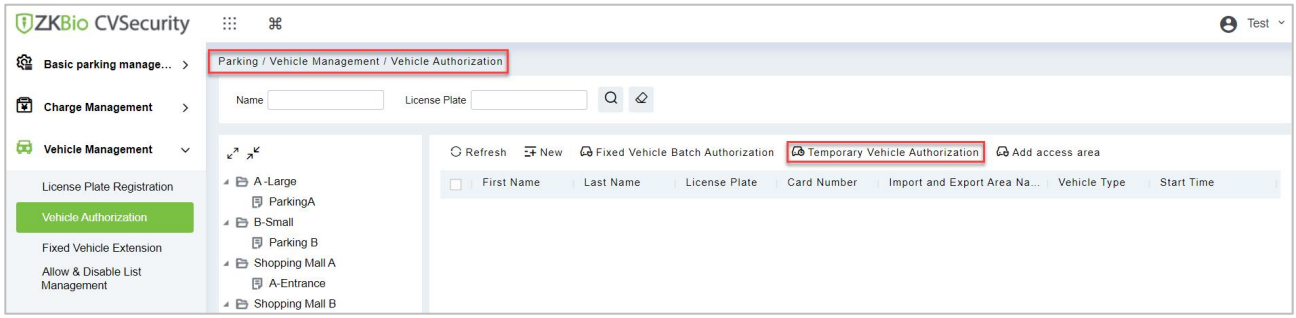


Figure 7- 69 Temporary Vehicle Authorization

Step 2: Successfully authorized vehicles will be displayed in the list.

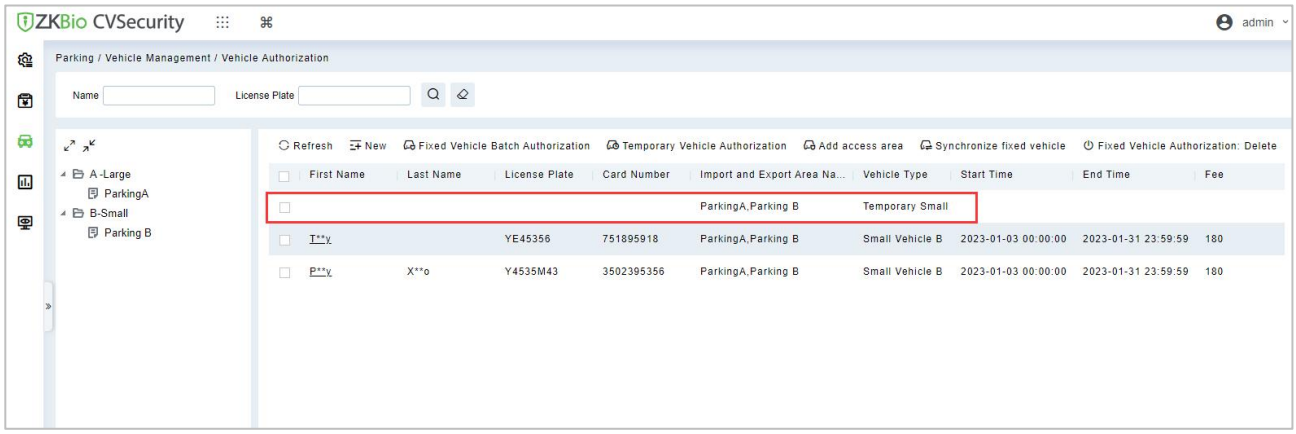


Figure 7- 70 Authorization list

7.8.6 Result Verification

7.8.6.1 Vehicle Entrance

Click Parking > Real-time Monitoring > Sentry Booth Monitoring, to check the vehicle access events.

Fixed Vehicle: Fixed vehicle swipe card on the ticket dispenser to enter, the booth real-time monitoring can view the record.

Temporary Vehicle: The vehicle sensor detects the vehicle and activates the ticket dispenser, the temporary vehicle enters after printing the ticket.

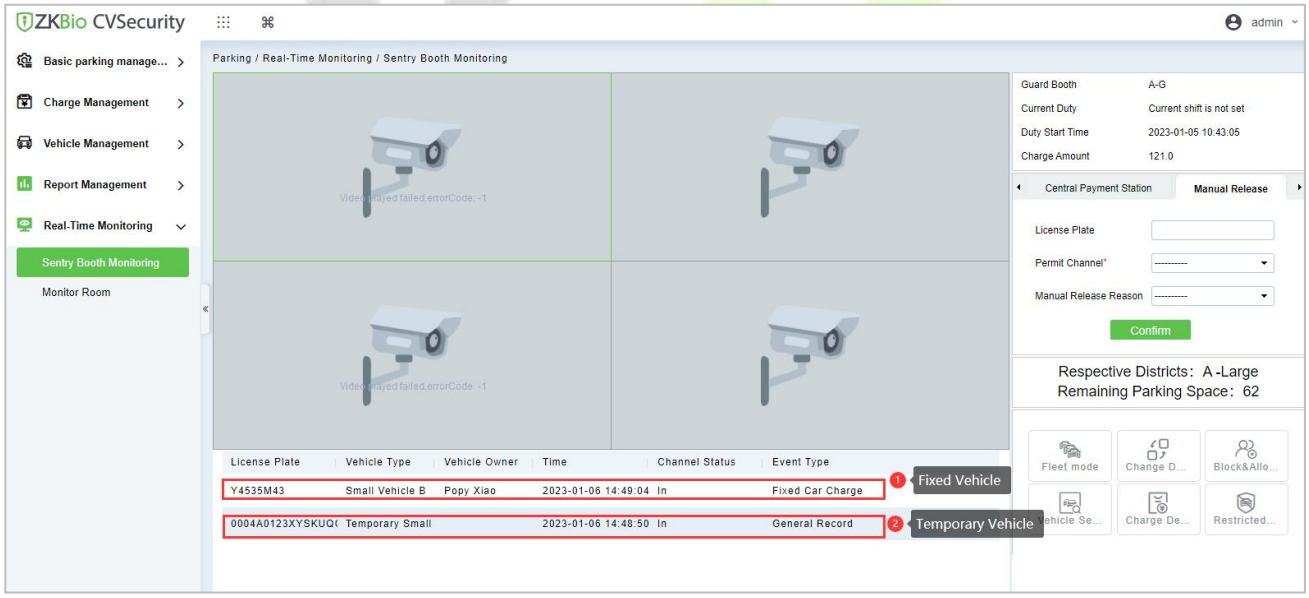


Figure 7- 71 Vehicle Entrance

7.8.6.2 Vehicle Exit

Click Parking > Real-time Monitoring > Sentry Booth Monitoring, to check the vehicle access events.

Fixed Vehicle: Fixed vehicle swipe card on the ticket dispenser to exit, the booth real-time monitoring can view the record.

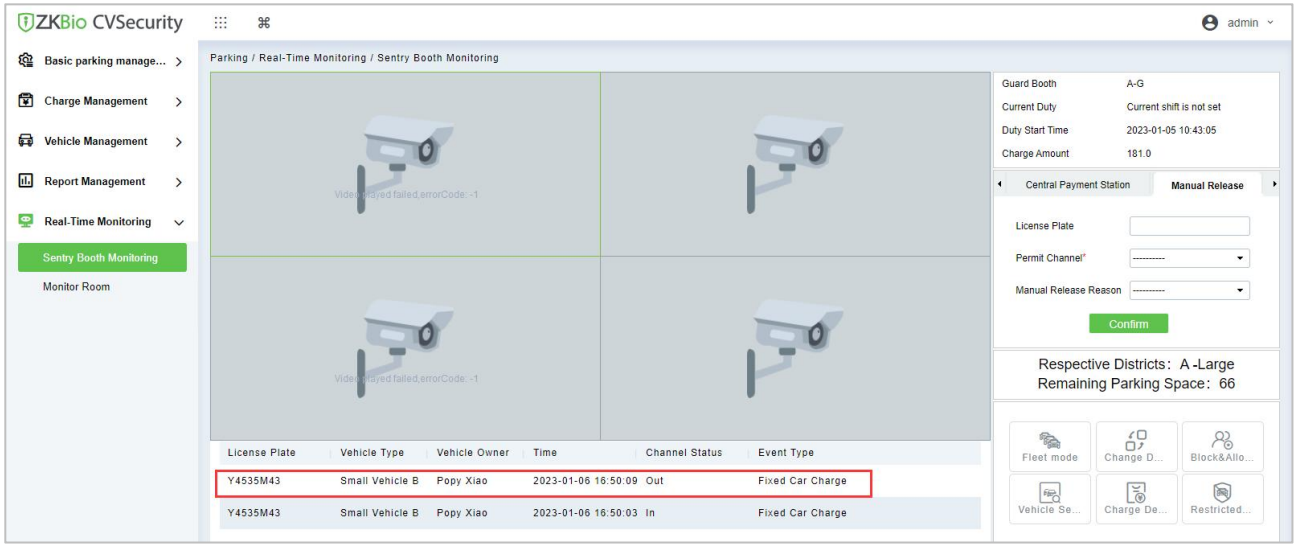


Figure 7- 72 Sentry Booth Monitoring

Temporary Vehicle: At the exit, after the ticket box scans the QR code, the system starts billing, check the picture below;

After charging, you can click **print the bills** or **open** the barrier.

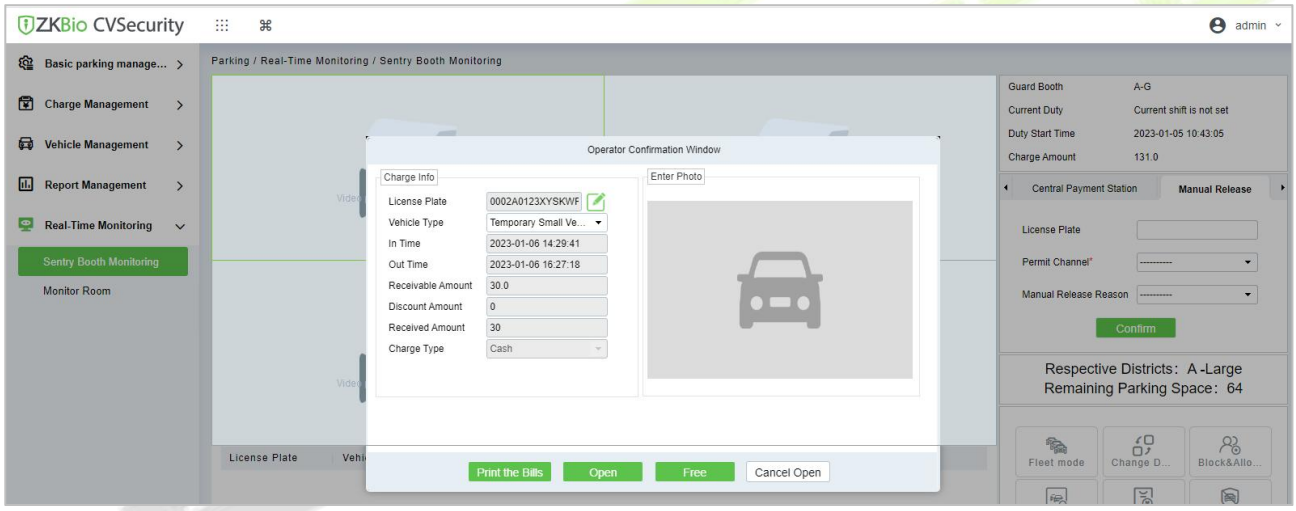


Figure 7- 73 Sentry Booth Monitoring

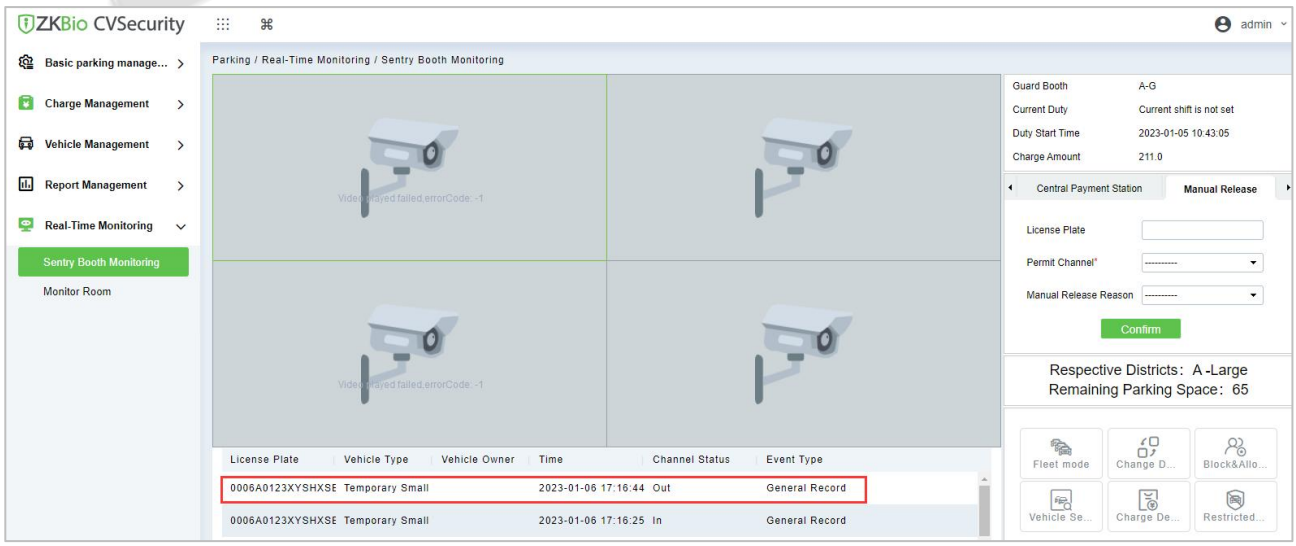


Figure 7- 74 Sentry Booth Monitoring

7.8.7Central Payment Station

When the exit is far from the post, the central payment station can be activated; when charging at the station, the vehicle can stay for a period before leaving the site.

● Operation Step:

Step 1: Click **Parking > Basic Parking Management > Lane > New**, add a channel and set to “Central Payment Station“.

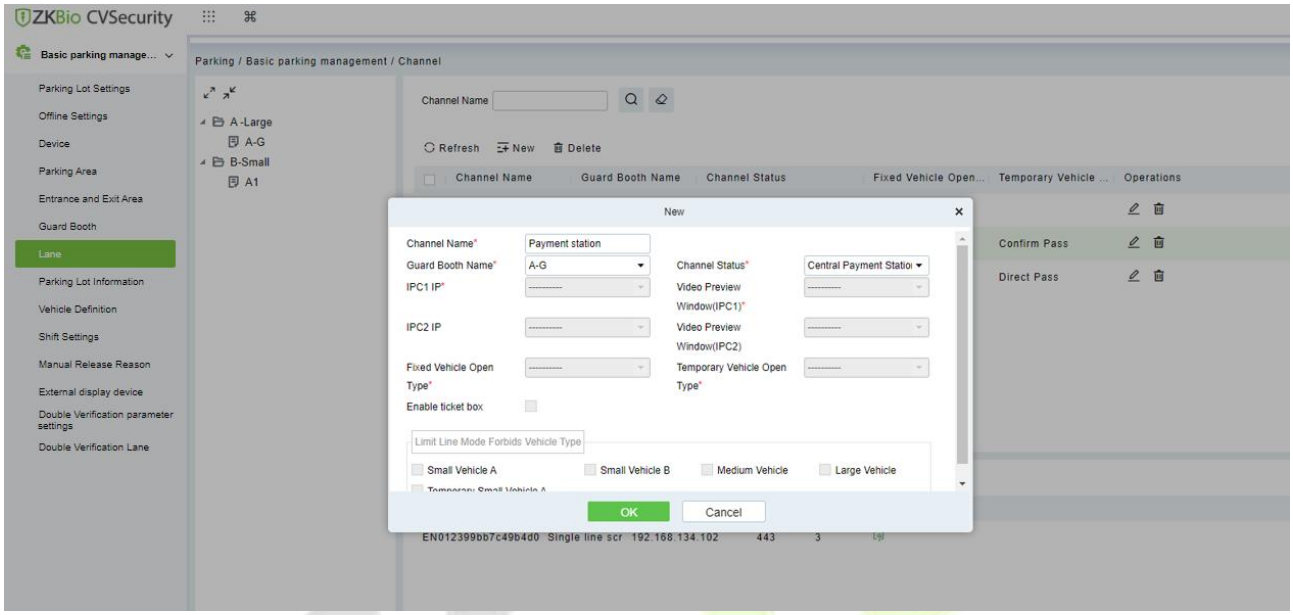


Figure 7- 75 Channel Setting (1)

Step 2: Click **Parking > Basic Parking Management > Lane > New**, add a channel and set to “Central Payment Exit“.

When charging at the central payment station, you need to exit at this designated "central payment exit".

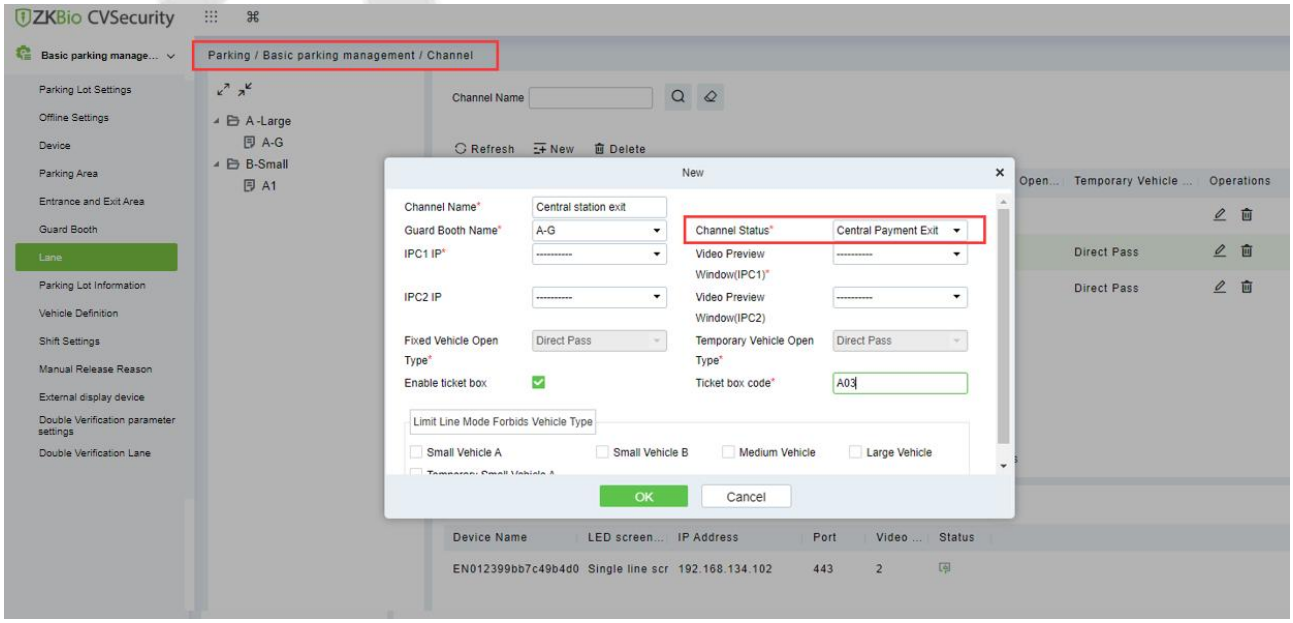


Figure 7- 76 Channel Setting (2)

Step 3: Click **Parking > Charge Management > Overtime Charge Rules > New**, New vehicle overstay charge rule.

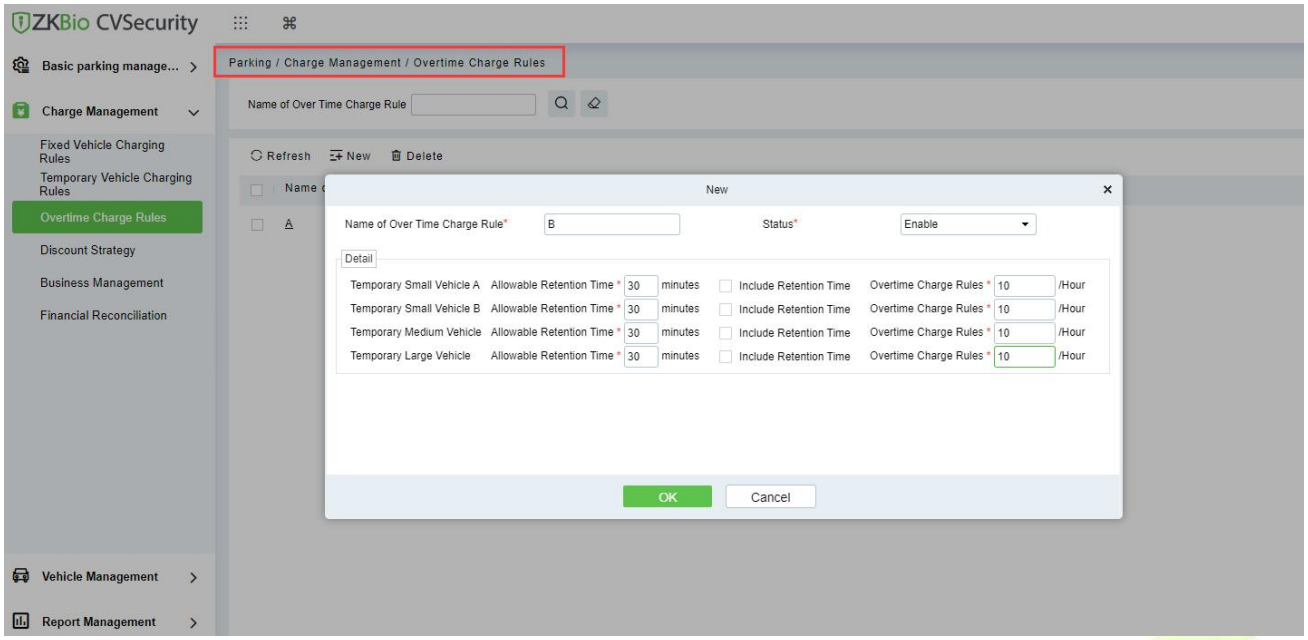


Figure 7- 77 Overstay rule

Edit : Edit the selected device.

Delete : Delete the selected device.

Step 4: Click **Parking > Real-time Monitoring > Sentry Booth Monitoring**.

When the vehicle arrives at the central payment station, the administrator uses Barcode Scanner to scan the entrance QR code and the system starts billing.

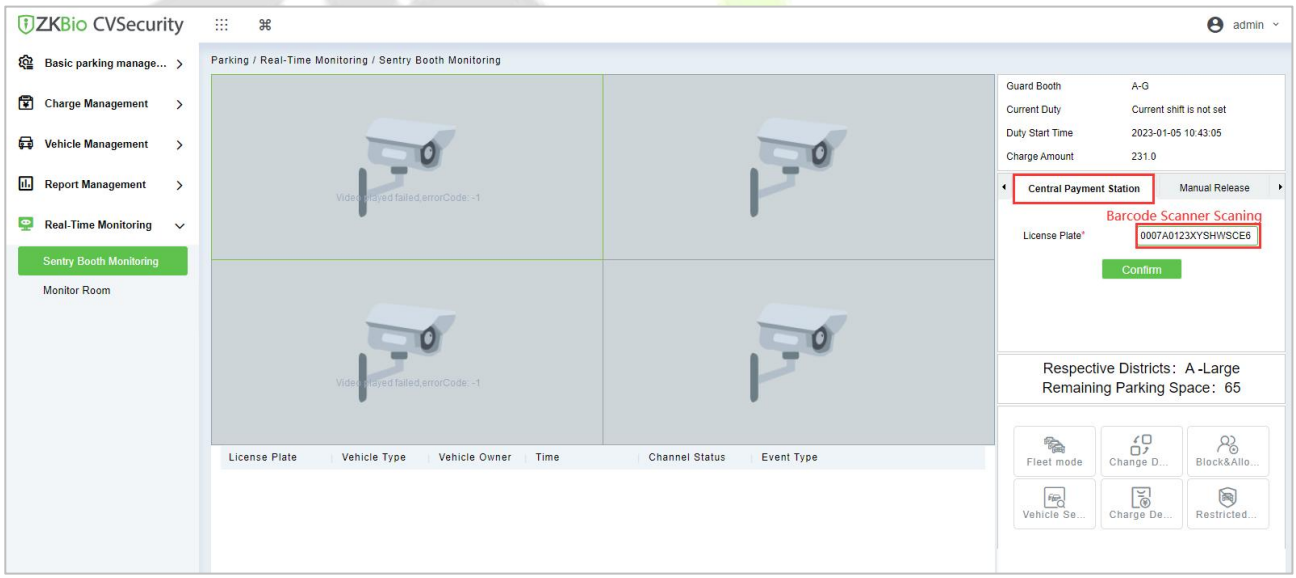


Figure 7- 78 Overstay Rule

After click **Confirm**, the charge window will pop up, after paid,you can click **Print the bills** or **Charge**.

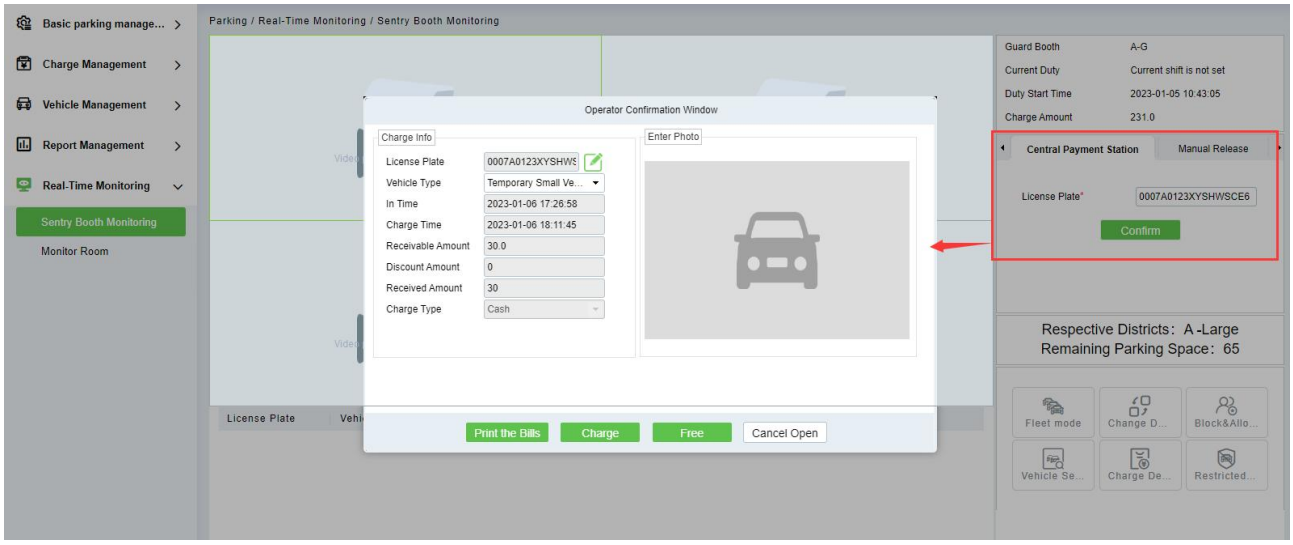


Figure 7- 79 Overstay Rule (2)

After successful payment, the vehicle can continue to stay or exit, overtime stay is charged according to the set rules.

When the time limit is exceeded, ZKBio CVSecurity will prompt "Please go to the central payment station to pay for the overtime stay" when the ticket dispenser at the central payment exit is scanning.

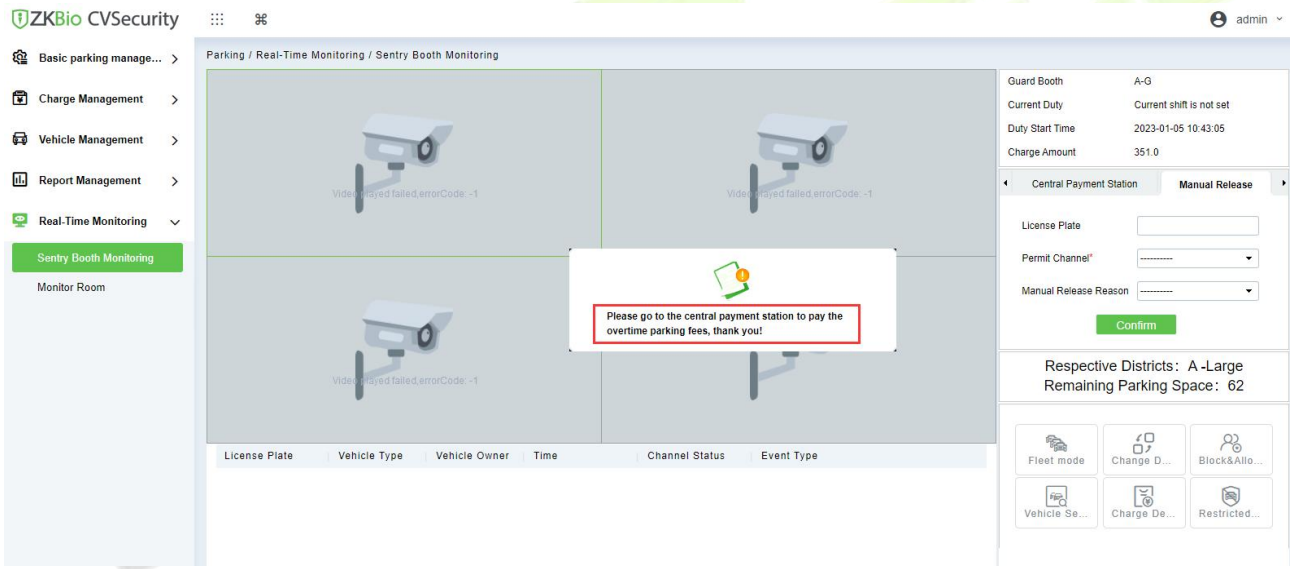
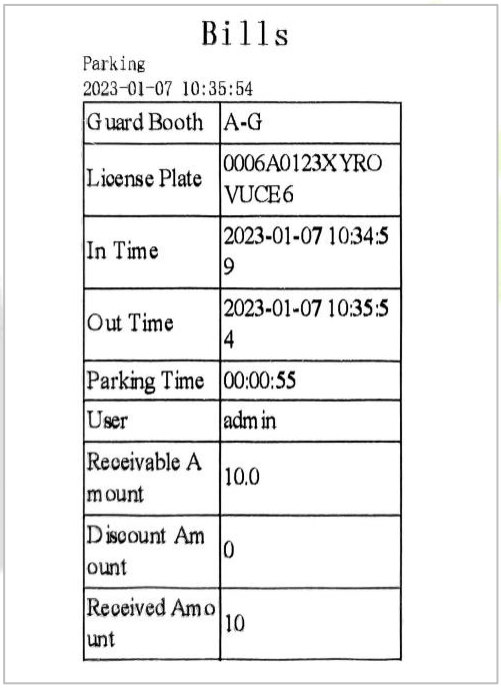


Figure 7- 80 Overstay Fee

7.8.8Annex 1

Figure 7- 81 Bar code Ticket

Figure 7- 82 QR code Ticket



Bills

Parking

2023-01-07 10:35:54

Guard Booth	A-G
License Plate	0006A0123XYRO VUCE6
In Time	2023-01-07 10:34:59
Out Time	2023-01-07 10:35:54
Parking Time	00:00:55
User	admin
Receivable Amount	10.0
Discount Amount	0
Received Amount	10

Figure 7- 83 Receipts printed at the central payment station

8 Visitor Management

8.1 Operation Scenario

By registering visitor's certificates, photos and other effective ways, and issuing corresponding Access Control/Elevator control/passage/witness authority, visitors can be managed safely and efficiently.

8.2 Operation Flow

Introduces the configuration process of visitor management business.

The business configuration process of the visitor management business is shown configure below.

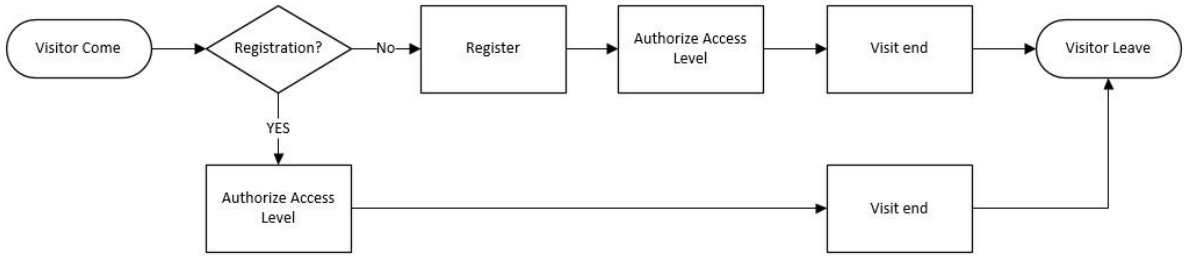


Figure 8- 1 Visitor Configuration Process

8.3 Visitor Registration

The visitor process includes two steps: identity registration and check-in. Since these typically occur simultaneously, this manual combines them under "Visitor Registration" for simplicity.

8.3.1 Visitor Check-in

8.3.1.1 Visitor Check-in

There are three ways to register visitors:

①Self-service Facekiosk

Visitors can Check-in directly on Facekiosk

②Front Desk PC

Visitors Check-in at the front desk computer

③Auto to Check-in

The system can automatically check in by setting it on the software side, or check in after verification at designated access, parking, and entrance control devices.

1.PC-Side Registration (Direct Registration)

This part introduces the configuration Steps of PC registration (Direct registration).

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Registration > Visitor Check-in**.

Step 2: In the Visitor Check-in interface, click **Visitor Check-in** to enter the registration interface for visitor registration, as shown in figure below.

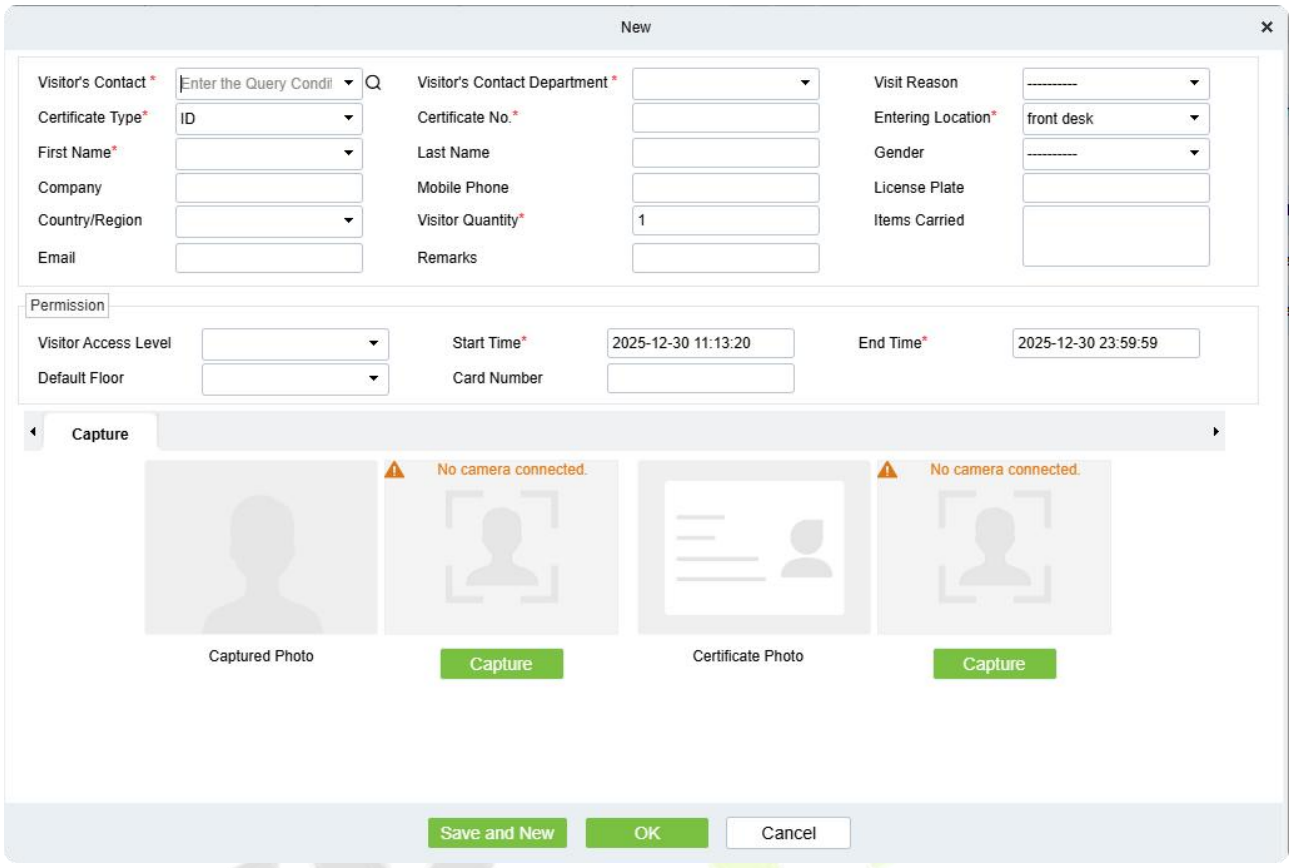


Figure 8- 2 Direct Register Visitor Interface

Parameter	Description
Visitor's Contact	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visitor's Contact Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the **Visit Reason** of **Basic Management**.
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
Entering Location	Select the entry place for the visitor. You can add an entry place in the **Entry Place** of **Basic Management**.

Parameter	Description
First Name	Enter the first name of the visitor.
Visitor Quantity	Enter the number of visitors.
Start and End Time	Enter the start and end times of the visit.
Capture	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click **Capture** to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 8- 1 Description of Parameters of Visitor Check-in

2.PC Registration (Register after making a reservation in advance)

This part introduces the configuration Steps of Registration through the Visitor Reservation.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Reservation**.

Step 2: In the visitor reservation interface, click **New** to complete the reservation registration before visitors visit, as shown in figure below.

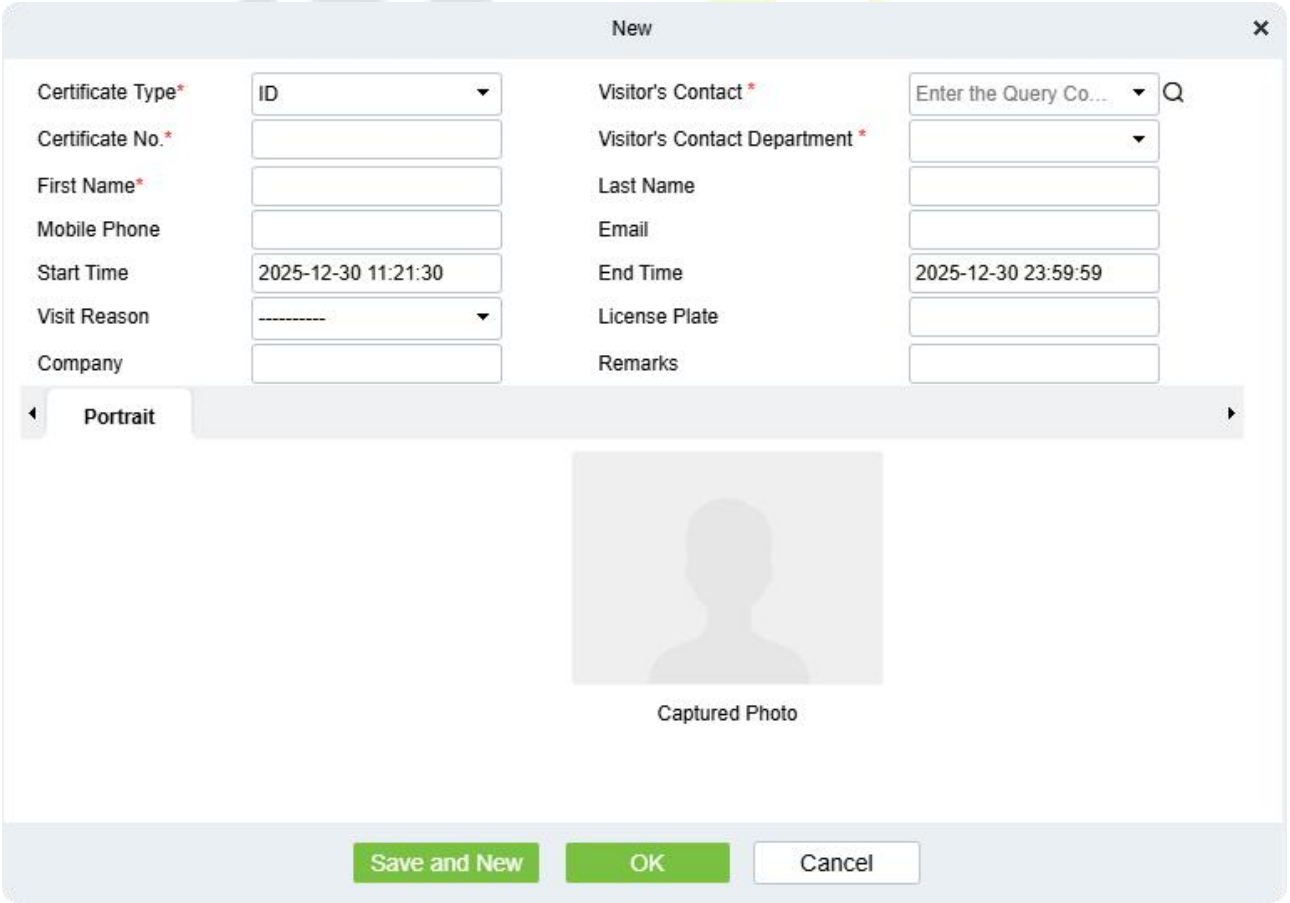


Figure 8- 3 Reservation Interface

Parameter	Description
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
Visitor's Contact	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visitor's Contact Department	Select the department the visitor will visit.
First Name	Enter the first name of the visitor.
Start and End Time	Enter the start and end times of the visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the **Visit Reason** of **Basic Management**.
Portrait	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click **Capture** to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 8- 2 Description of Parameters Reservation

Step 3: Select **Visitor Registration** > **Visitor Check-in** > **Visitor Check-in** to enter the registration interface for visitor registration. Enter the **First Name** to directly obtain the ID number, thus displaying the visitor information of reservation registration, then select the visitor authority, and click **OK** to complete the visit registration, as shown in figure below.

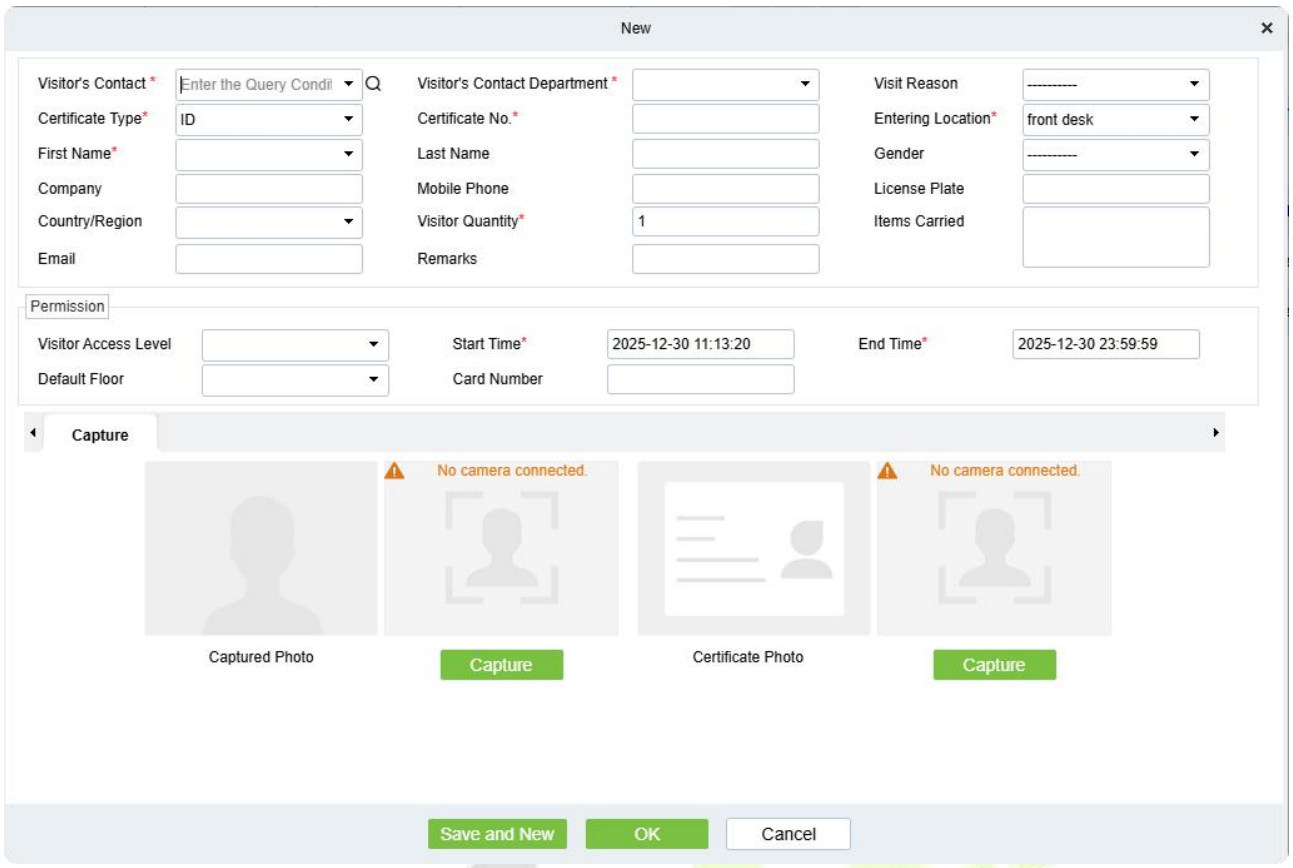


Figure 8- 4 Second Generation Identity Registration Interface

Notes:

For different browsers, the contents of tips are different, the actual browser display prevails, just choose the shared camera, and allow the system to access the camera.

If the entry place supports a network camera, scanner, high camera, it will not pop up this tip.

You can select card number, fingerprint, password, or code scanning for registration (set in the parameter setting).

8.3.1.2Check Out

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Registration > Visitor Check-out**.

Step 2: In the Visitor Check-in interface, click **Check Out** to enter the registration interface for visitor Check Out, as shown in figure below.

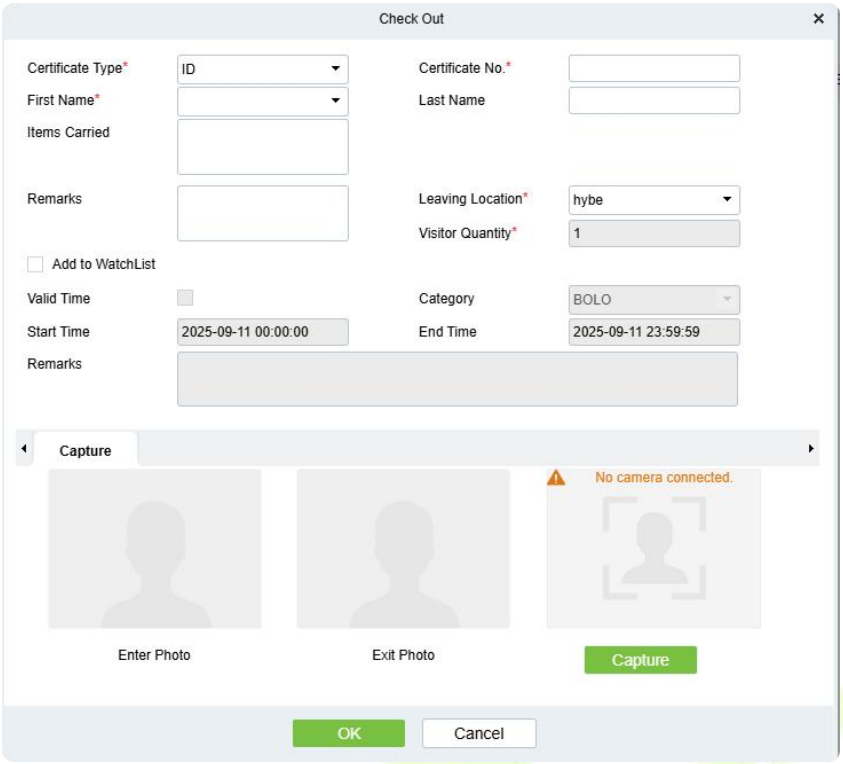


Figure 8- 5 Check Out

Parameter	Description
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Leaving Location	Select the exit location for visitors after the visit concludes.
Visitor Quantity	Enter the number of visitors.
Add to WatchList	Choose whether to add the visitor to the monitoring list.
Valid Time	Choose whether to customize the monitoring duration.
Category	Select the monitoring type.
Start and End Time	Enter the start and end times of the watchlist.
Personnel Details	Enter the personnel details.

Parameter	Description
Capture	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click **Capture** to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 8- 4 Description of Parameters

8.3.1.3Visitor Cloning

Application scenario: Similar to an entourage copying some information from the previous person, visitors only need to show their credentials and snap photos to complete the registration. It mainly includes the following attributes: Host, visit department, visit reason, Entrance, company, country, visitor level, start time, end time.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Registration > Visitor Check-in**.

Step 2: In the visitor registration interface, click **Visitor Cloning** to enter the registration interface for visitor cloning.

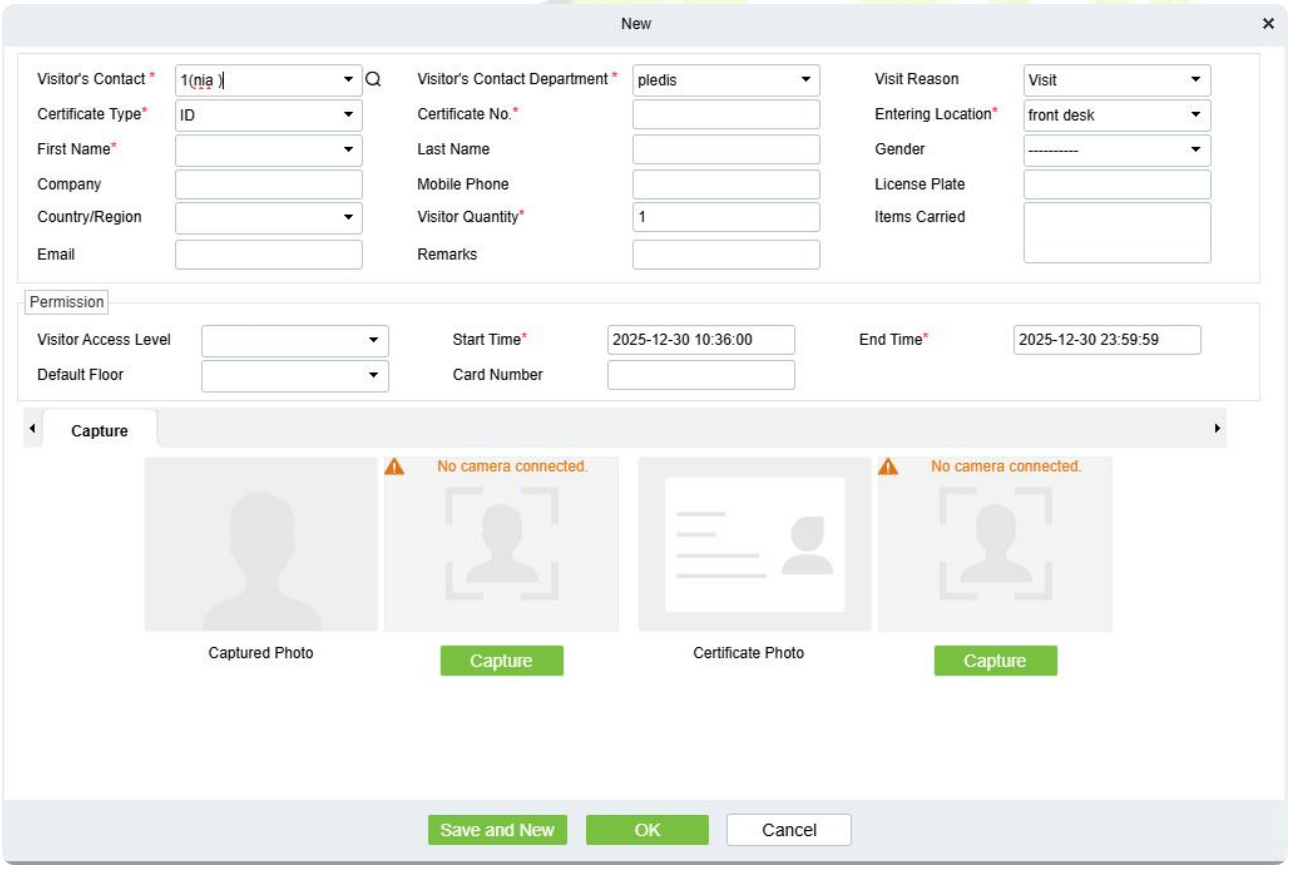


Figure 8- 6 Visitor Cloning interface

8.3.1.4Batch

Batch option will help you to do multiple check-in and check-out at a time.

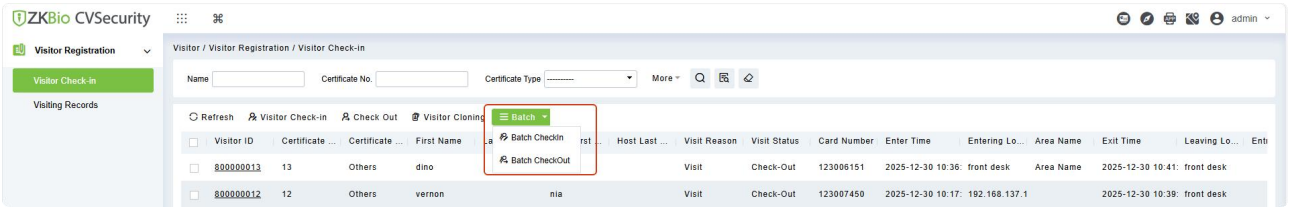


Figure 8- 7 Batch Interface

1.Batch Check-in

Batch Check-in option will help you to do multiple check-in at a time. For that you need to create a reservation for the visitors. Then you can be able to see details in the **Batch Check in** option for multiple check-ins at a time.

● Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation > Visitor Reservation**. In the reservation interface, click **New** to complete the reservation registration.

Step 2: In the **Visitor** module, select **Visitor Registration > Visitor Check-in**.

Step 3: In the Visitor Check-in interface, select the visitor to do the check-in and click **Batch > Batch check in** to do multiple check-in of visitors at a time.

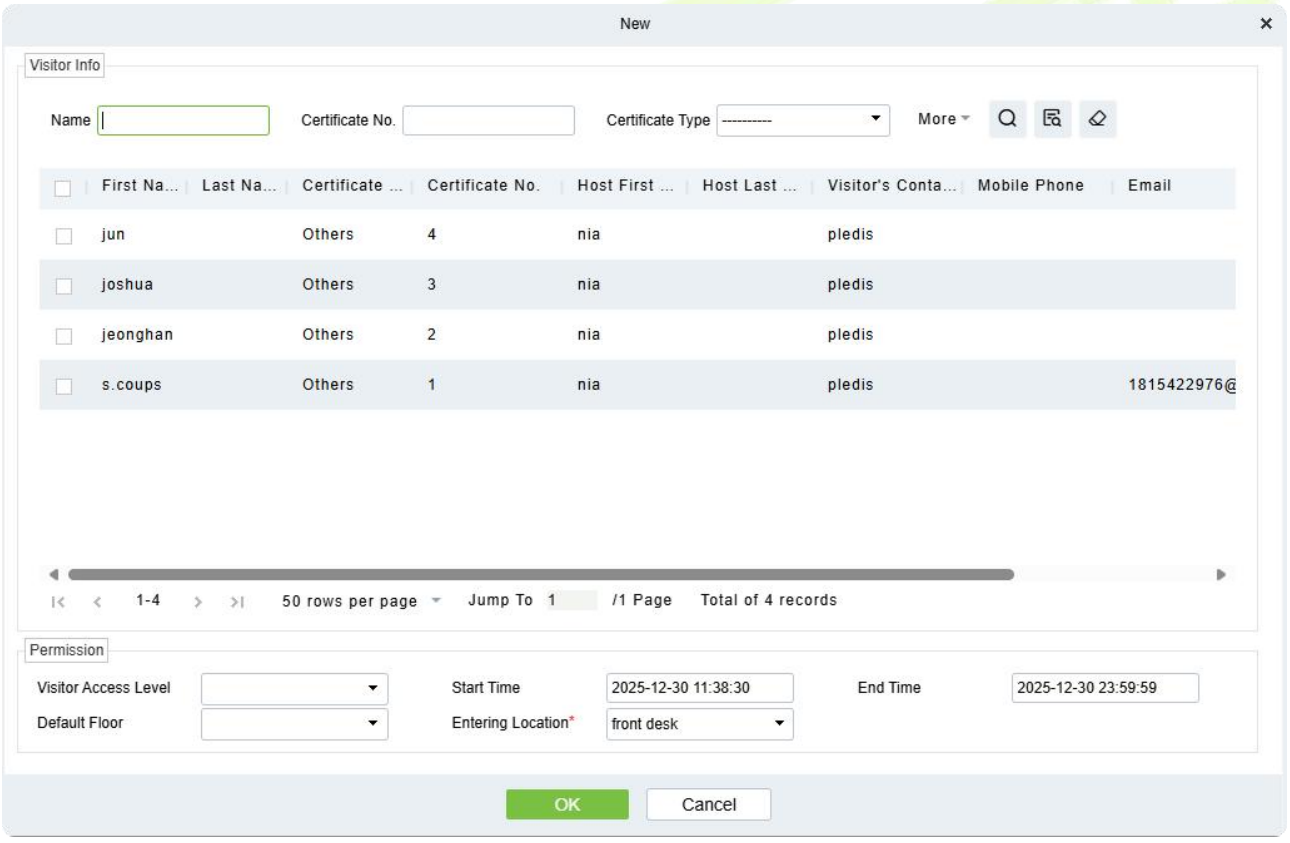


Figure 8- 8 Batch Check in interface

Step 3: Click **OK** to check in the selected visitors.

2.Batch Check Out

Batch check out option will help you to do multiple check out of visitors at a time.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Registration > Visitor Check-in**.

Step 2: In the Visitor Check-in interface, select the visitor to do the check out and click **Batch > Batch**

checkout to do multiple checkouts of visitors at a time.

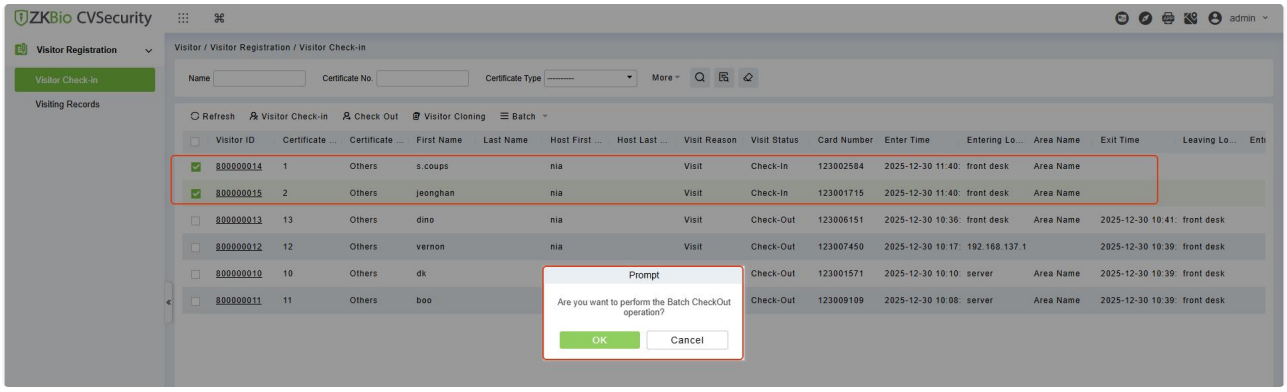


Figure 8- 9 Batch Check out interface

Step 3: Click **OK** to check-out the selected visitors.

8.3.2Visitor Records

Visitor Records interface provides the complete details about the registered visitors such as Visitor Code, First Name, Last Name, Certificate Type, Certificate No., Company etc. You can delete, disable or enable and export the selected visitor.The user login interface only displays visitor records from the department(s) authorized for the user.

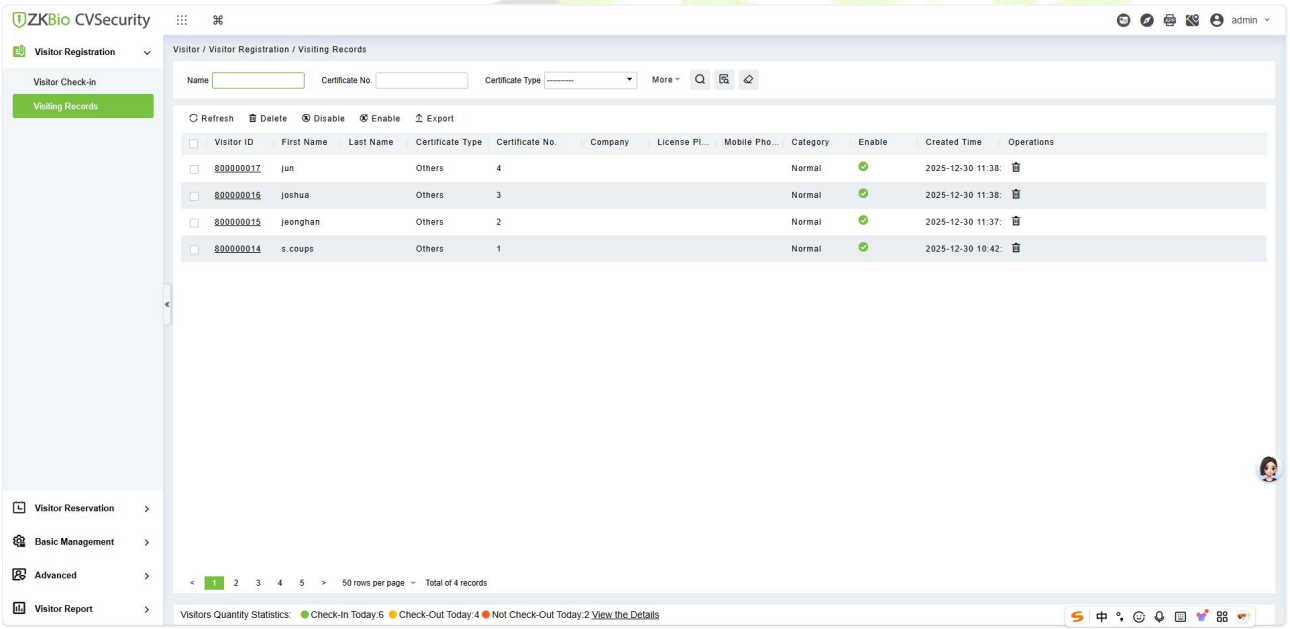


Figure 8- 10 Visitor Interface

8.3.2.1Delete

In **Visitor** module click **Visitor Registration** > **Visiting Records**, select a visitor, and click **Delete**.

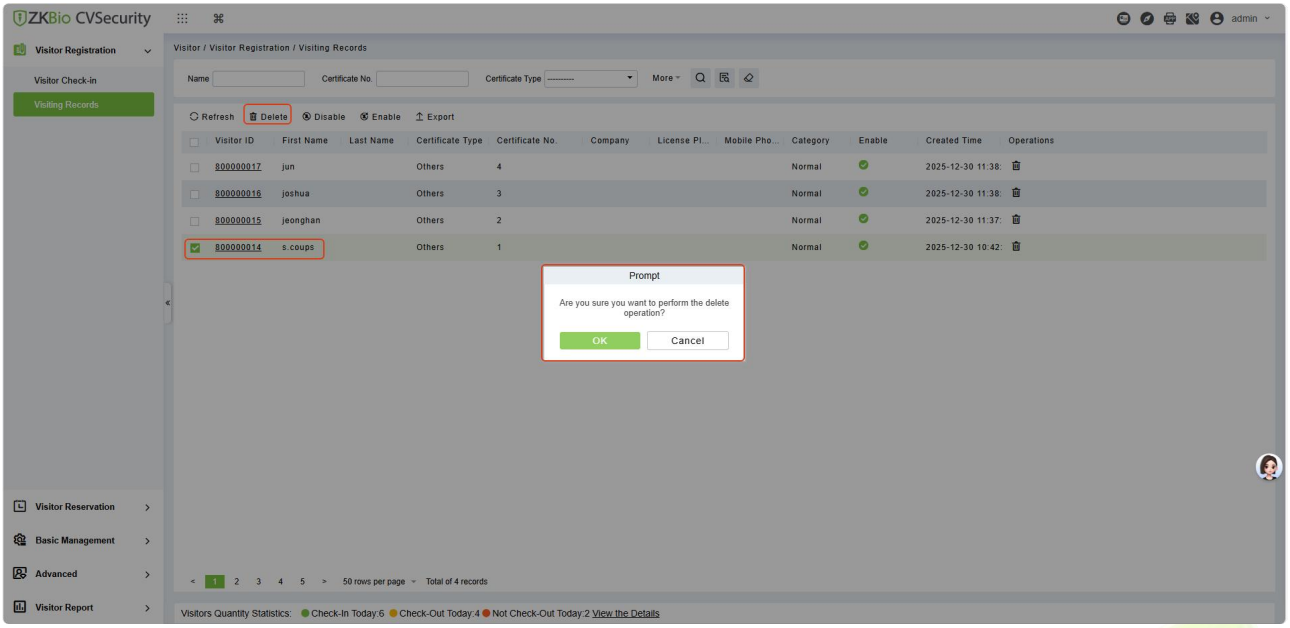


Figure 8- 11 Deleting Visitor

Click **OK** to delete the selected visitor.

8.3.2.2Disable

In **Visitor** module Click **Visitor Registration** > **Visiting Records**, select a visitor, and click **Disable**.

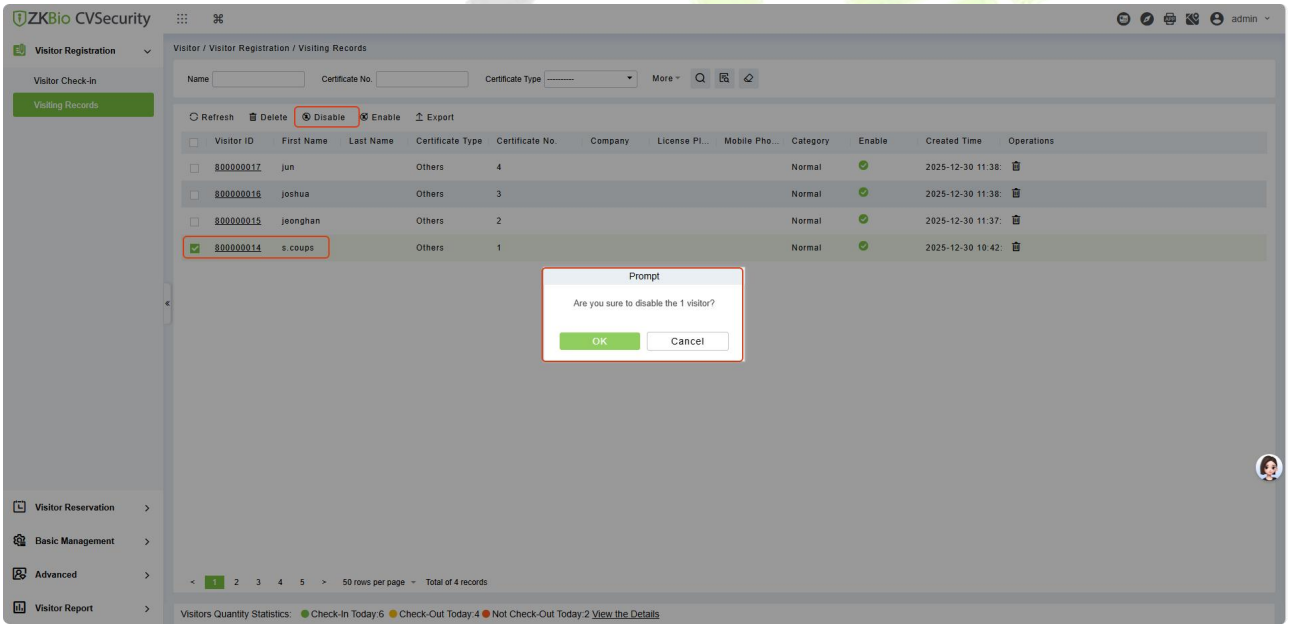


Figure 8- 12 Disabling Visitor

Click **OK** to block the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor is blocked.

8.3.2.3Enable

In **Visitor** module click **Visitor Registration** > **Visiting Records**, select a blocked visitor, and click **Enable**.

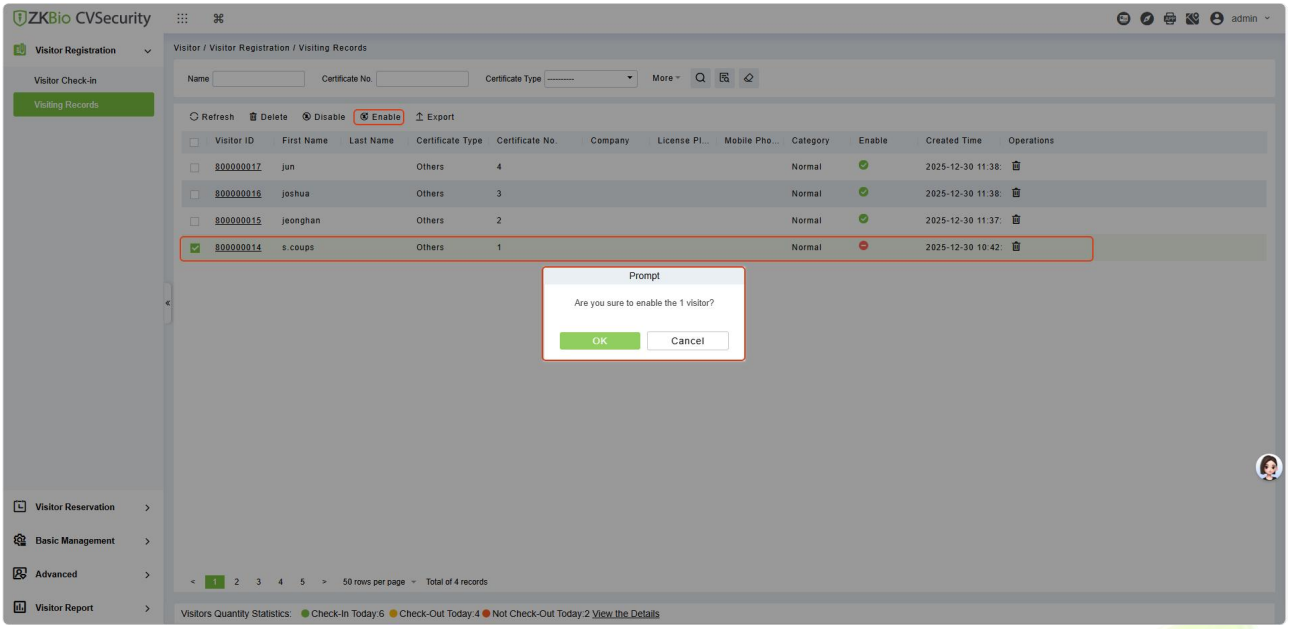


Figure 8- 13 Enabling Visitor

Click **OK** to enable the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor is enabled.

8.3.2.4Export

You can export visitor details into an Excel, PDF, or CSV file. See the following figure.

●Operating Steps:

Step 1: In **Visitor** module click **Visitor Registration > Visiting Records > Export** to export the visitor records to Excel or PDF or CSV or TXT. Enter the User password in the prompt.You can also choose to encrypt the exported file and select the range of output data.

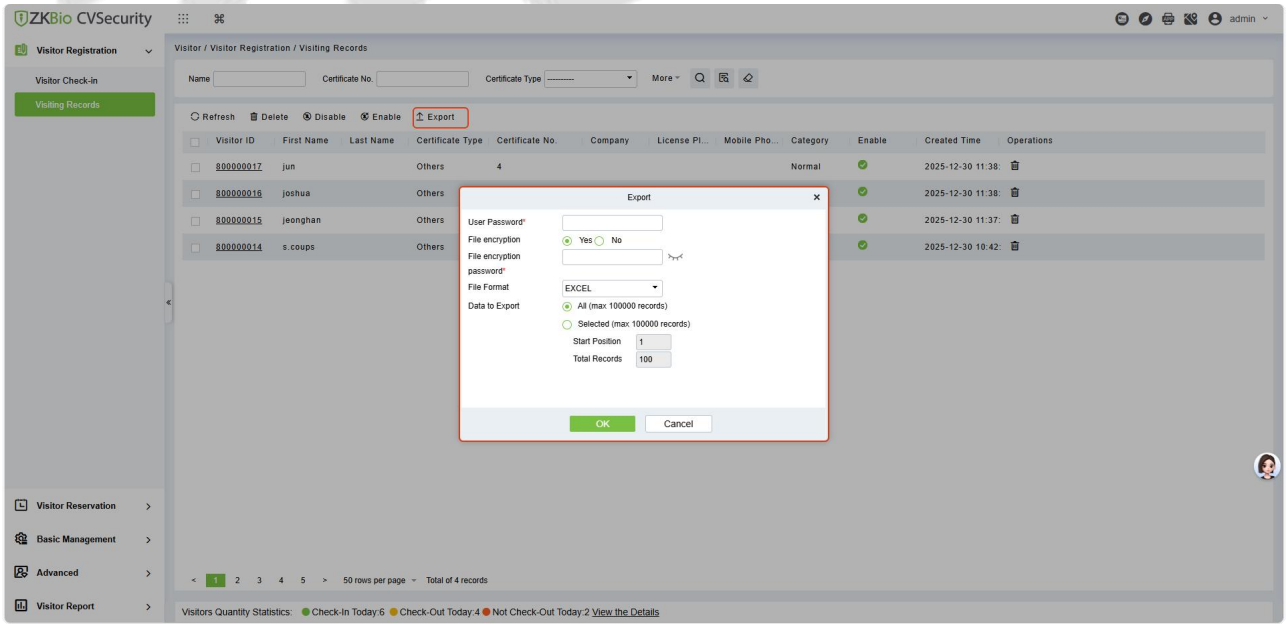


Figure 8- 14 Export Interface

Step 2: click **OK**.

8.4 Visitor Reservation

8.4.1 Visitor Reservation

Visitor Reservation helps you to do reservations before the visitor's visit.

8.4.1.1 New

Creating new Reservations for Visitors.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Reservation**.

Step 2: In the reservation interface, click **New** to complete the reservation registration before the visitor's visit.

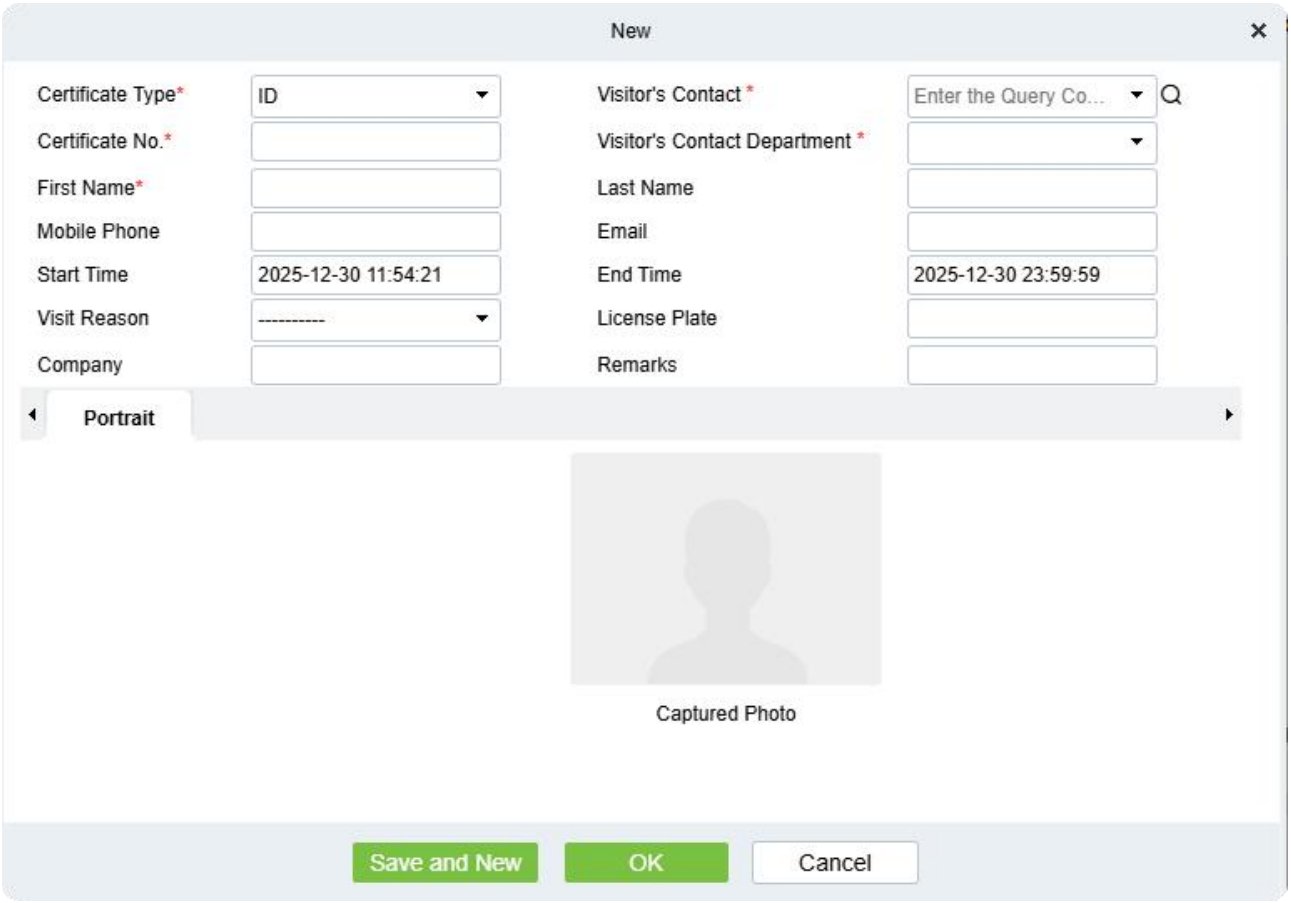


Figure 8- 15 Reservation Interface

Parameter	Description
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.

Parameter	Description
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
Visitor's Contact	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visitor's Contact Department	Select the department the visitor will visit.
First Name	Enter the first name of the visitor.
Start and End Time	Enter the start and end times of the visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the **Visit Reason** of **Basic Management**.
Portrait	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click **Capture** to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 8- 6 Description of Parameters of Adding a Visitor Reservation

After the reservation visitors can complete the visit registration using Visitor Check-in option.

8.4.1.2Delete

In the **Visitor** module, select **Visitor Reservation > Visitor Reservation,** select a visitor reservation and click **Delete**.

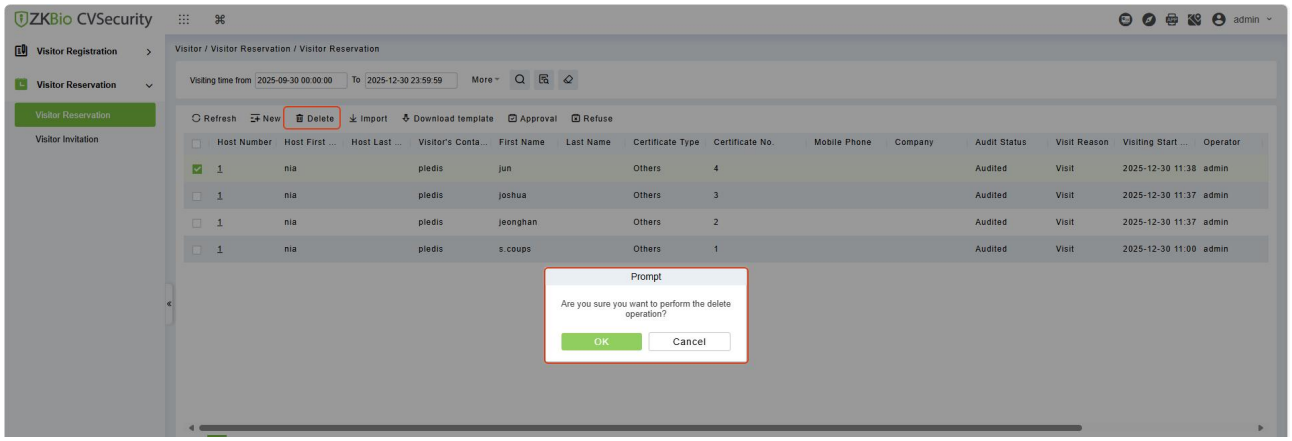


Figure 8- 16 Deleting Visitor Reservation

Click **OK** to delete the selected visitor reservation.

8.4.1.3Import

You can import visitor reservation details into the software as in Excel format. See the following Figure.

● Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation > Visitor Reservation,** click **Import**.

Step 2: Click the **Browse** button to import the visitor reservation template data .You can download the template from the software by clicking **Download Template** into the system, as shown in figure below.

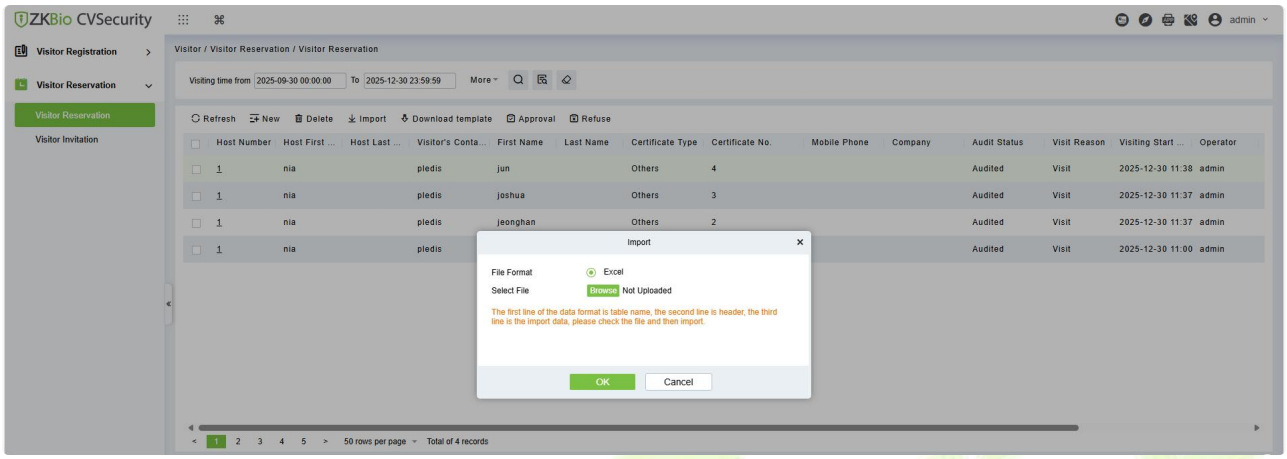


Figure 8- 17 Import Visitor Reservation

Step 3: Click **OK**, and the interface displays the result of importing and adding visitor reservations.

Step 4: Click **Close** to complete the import and addition of visitor reservations.

8.4.1.4Download Template

You can download template visitor reservation details into the software as in Excel format.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Reservation,** click **Download template**.

Step 2: Click **OK**, and the interface displays the result of importing and adding visitor reservations.

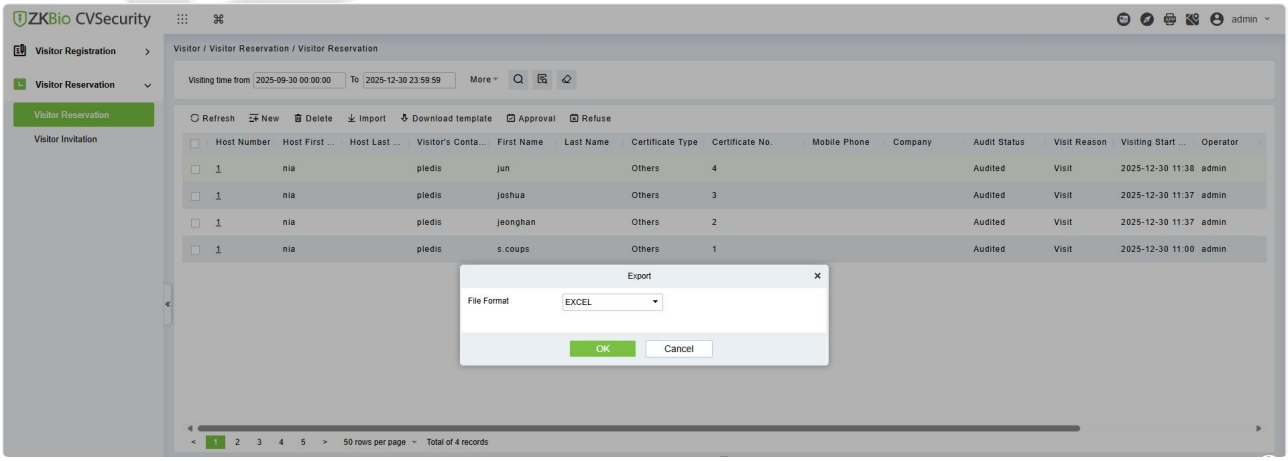


Figure 8- 18 Import Visitor Reservation

8.4.1.5Approval

Allow the administrator to review the employee's self-reservation visitors.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Reservation > Approval**.

Step 2: In the **Reservation** interface, select the visitor to be reviewed and click **Approval** to review the visitor.

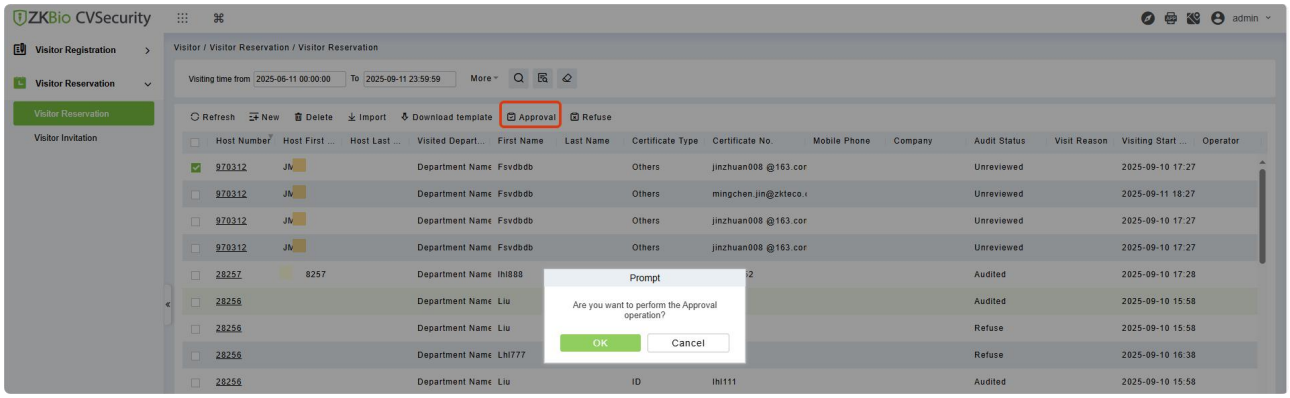


Figure 8- 19 Approval Visitor Reservation

Step 3: Click **OK** to perform the review operation.

8.4.1.6Refuse

Allow the administrator to block the employee's self-reservation visitors.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Reservation > Refuse**.

Step 2: In the **Reservation** interface, select the visitor to be reviewed and click **Refuse** to block the visitor.

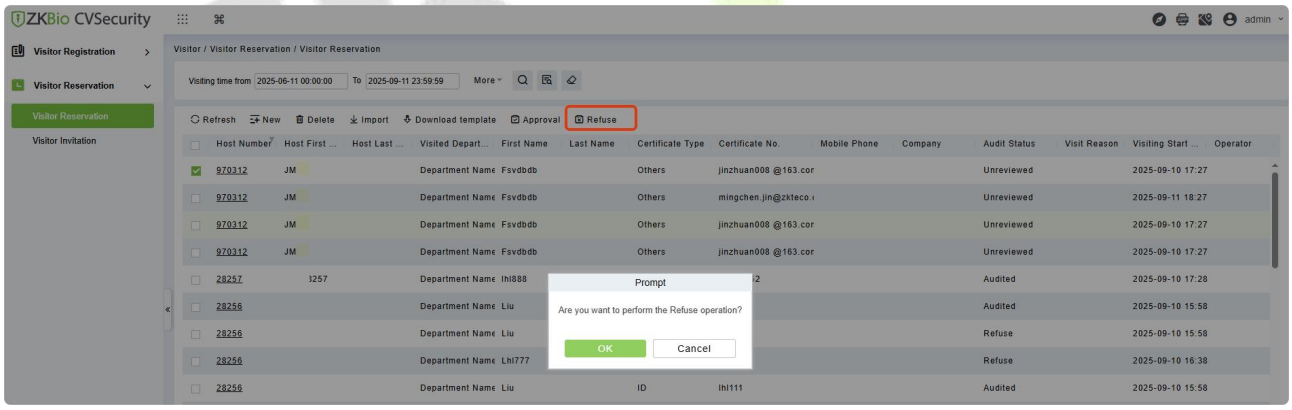


Figure 8- 20 Refuse Visitor Reservation

Step 3: Click **OK** to perform the refuse operation.

8.4.2Visitor Invitation

8.4.2.1New

You can send invitations to the needed visitors by using this option.

● Operating Steps:

Step 1: In the Visitor module, select **Visitor Reservation > Visitor Invitation**.

Step 2: In the **Invite** interface, click **New** to send the invitation to the visitors and the details as shown in figure below.

Step 3: Click **OK** to send the invitation.

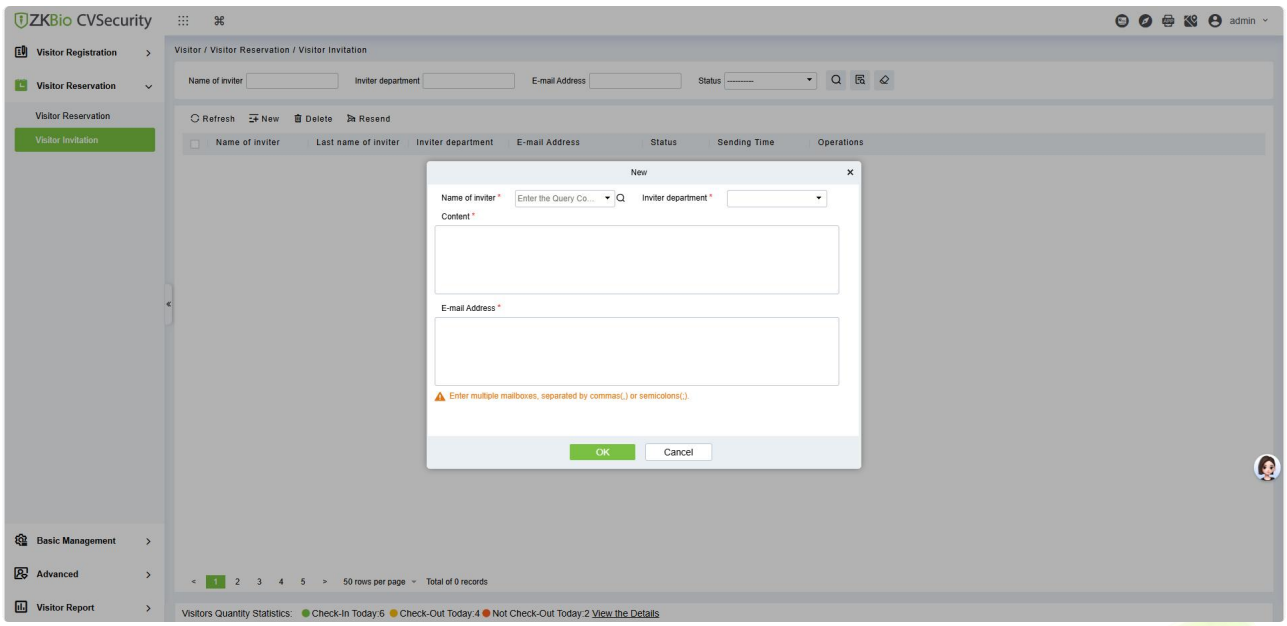


Figure 8- 21 Invite Interface

Parameter	Description
Name of the Inviter	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Inviter Department	Select the department of the inviter.
Content	Enter the content or reason of the invitation.
Email Address	Enter the Email address.

Table 8- 7 Description of Parameters of Invite Visitors

● Results Validation:

Visitors will receive an email and can scan the QR code to complete the appointment.

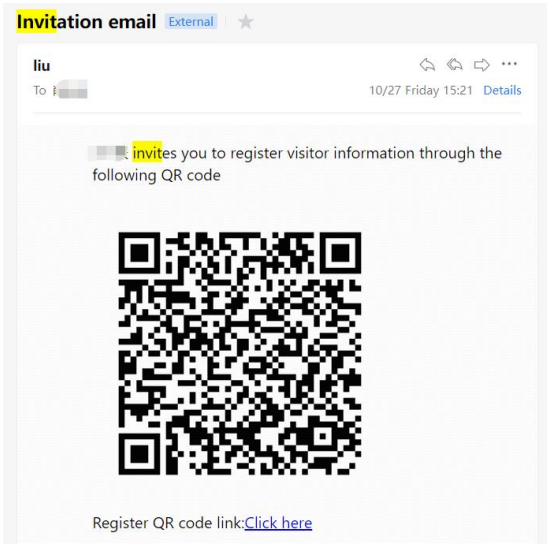


Figure 8- 23 Invitation Email

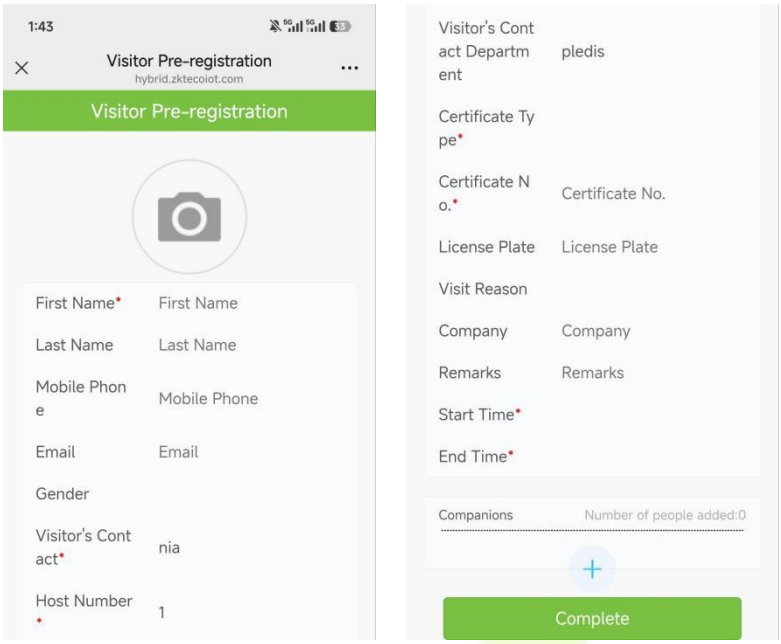


Figure 8- 23 Visitor Pre -registration page

8.4.2.2Delete

To delete the visitor invitations.

● Operating Steps:

Step 1: In Visitor module click **Visitor Reservation > Visitor Invitation**.

Step 2: In the invite interface select the invitation to be deleted and click **Delete**.

Step 3: Click **OK** to delete the invitation.

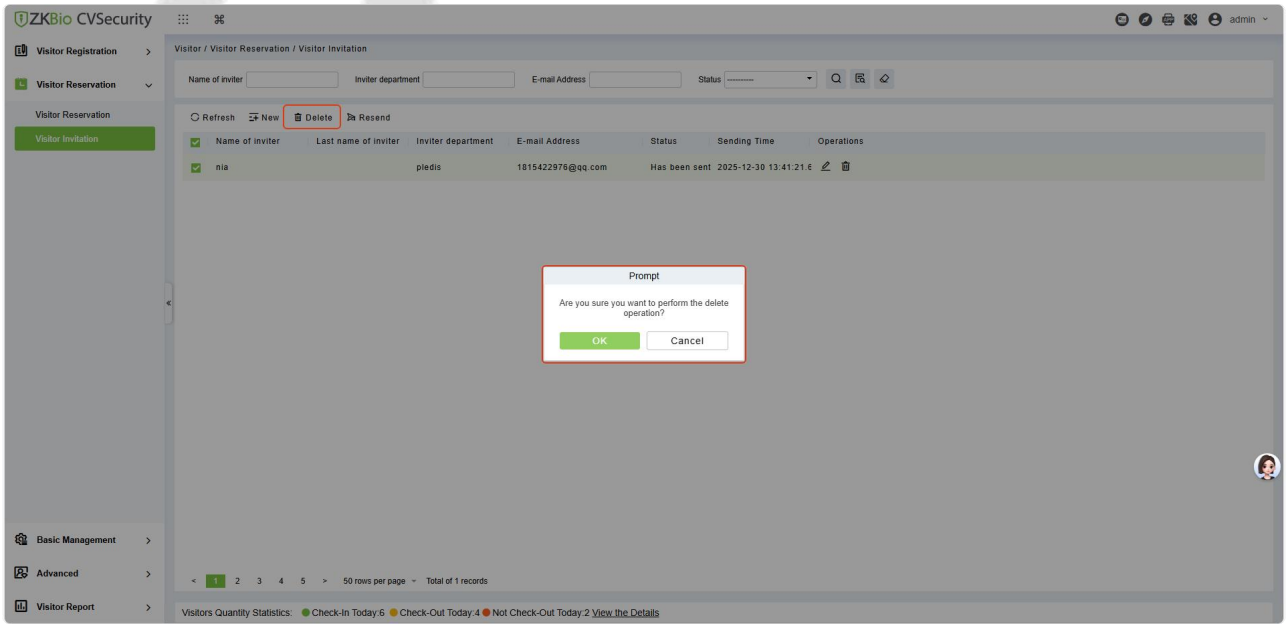


Figure 8- 24 Delete Invitations

8.4.2.3 Resend

To Resend the visitor invitations.

● Operating Steps:

Step 1: In Visitor module click **Visitor Reservation > Visitor Invitation**.

Step 2: In the invite interface select the invitation to be resend and click **Resend**.

Step 3: Click **OK** to resend the invitation.

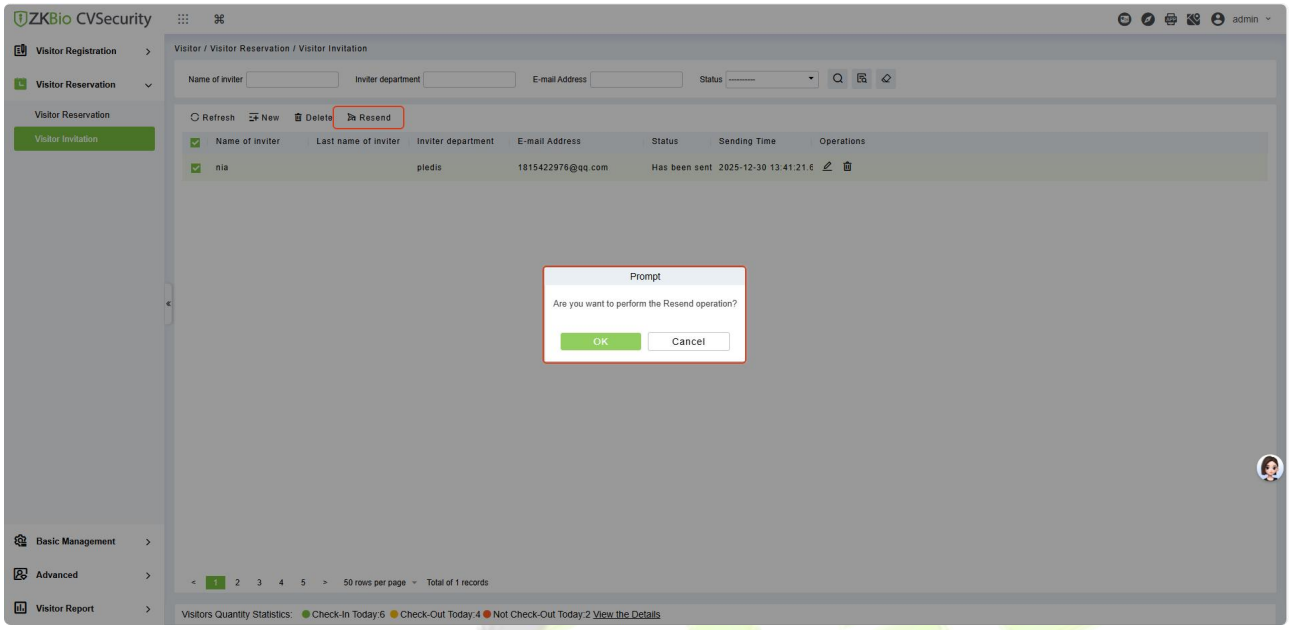


Figure 8- 25 Resend Invitations

8.4.3 Respondent Self-Approval

Optimize the visitor process, after sending the visitor invitation email, ZKBio CVSecurity will send an audit email to the host. The host can complete the operation of "Review or Reject" by clicking on the audit link of the email, then quickly complete the review.

● Set the Outgoing Mail Server Settings:

Step 1: In System Management module, click **Email Management > Outgoing Mail Server Settings**:

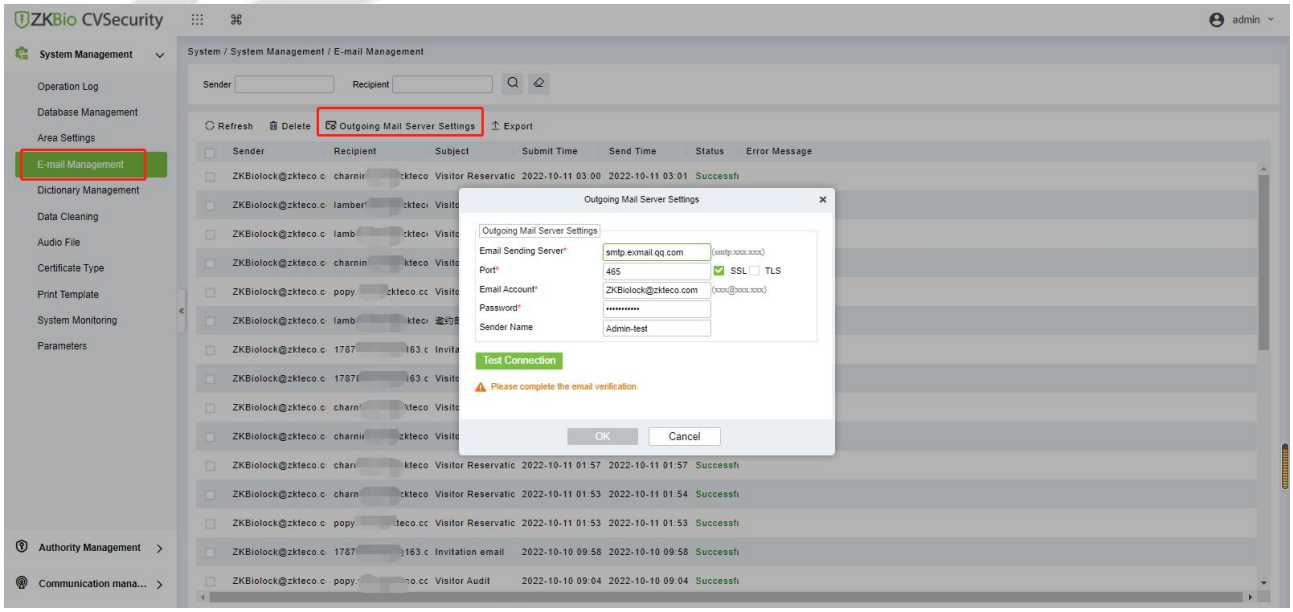


Figure 8- 26 Outgoing Mail Server Settings

Step 2: Set the Outgoing Mail Server Settings as Table below.

Parameter	How to set up
Email server address/port	You can customize the email server address and port. The email products that provide the SMTP server can be used
Email username and password	Enter the user's name and password for the mailbox.
Name of sender	Sets the name of the sender on the received message.

Table 8- 8 Outgoing Mail Server Settings

Step 3: After setting, click **Test Connection** to receive the email, indicating that the test has passed.

Step 4: Click **OK** to finish setting email parameters.

✍**Note:** The domain name of E-mail address and E-mail sending server must be identical. For example, the Email address is test@gmail.com, and the E-mail sending server must be smtp.gmail.com.

● Set Visitor Parameters:

Step 1: In Visitor module, Click **Basic Management > Parameters**.

Step 2: Select **No** for the **Enable automatic review of guest appointments,** so that the visitors' reservations need to be approved.

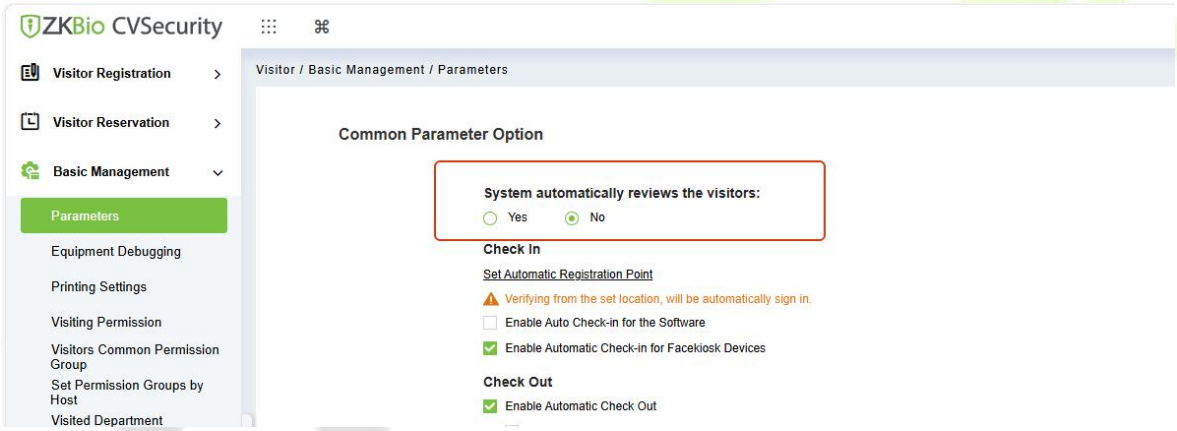


Figure 8- 27 Disable System automatically reviews the visitors

Select **"Yes"** for **"Enable Cloud Visitor Registration URL"** so that visitors can make self-service appointments via QR codes or links.

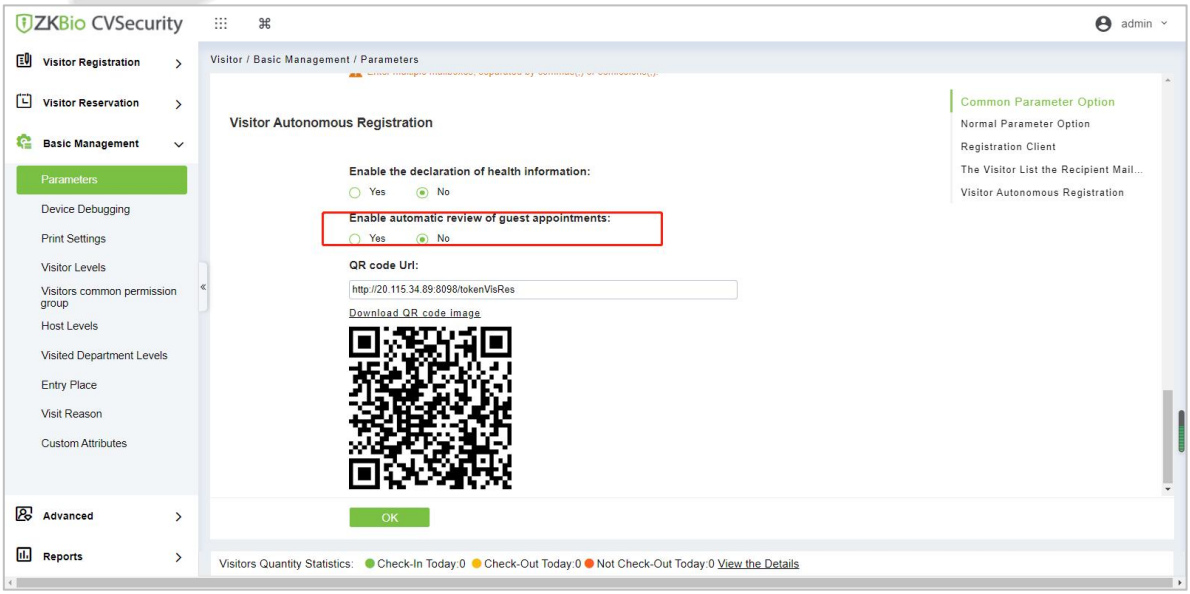


Figure 8- 28 Enable Cloud Visitor Registration URL

● Respondent Self-Approval:

When a visitor submits registration information, host will receive a review email as shown below:

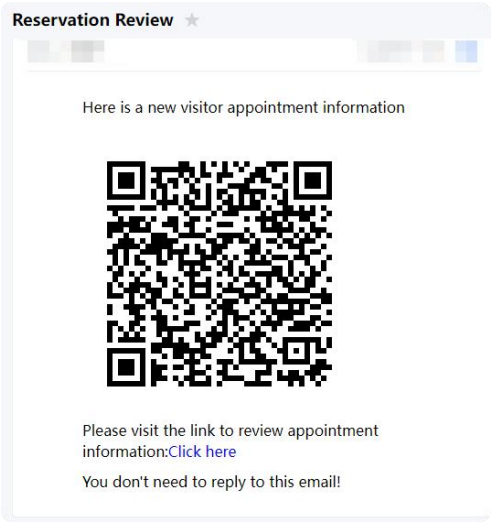


Figure 8- 29 Reservation Review

Scan the QR code or click the link to enter the review interface.Click **Review** if you agree to make an appointment.Click **Refuse** if you refuse the appointment.

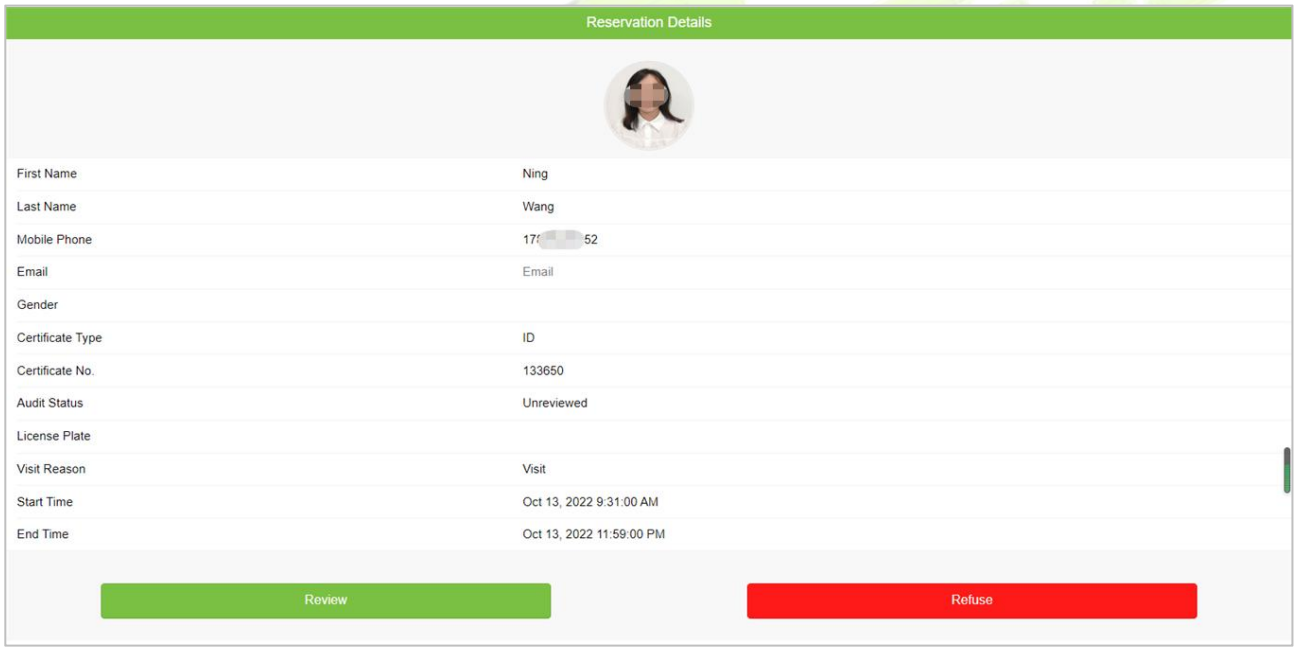


Figure 8- 30 Visitor Reservation Audit

8.5 Basic Management

8.5.1 Parameters

In **Visitor** module Click **Basic Management** > **Parameters** to set the parameters.

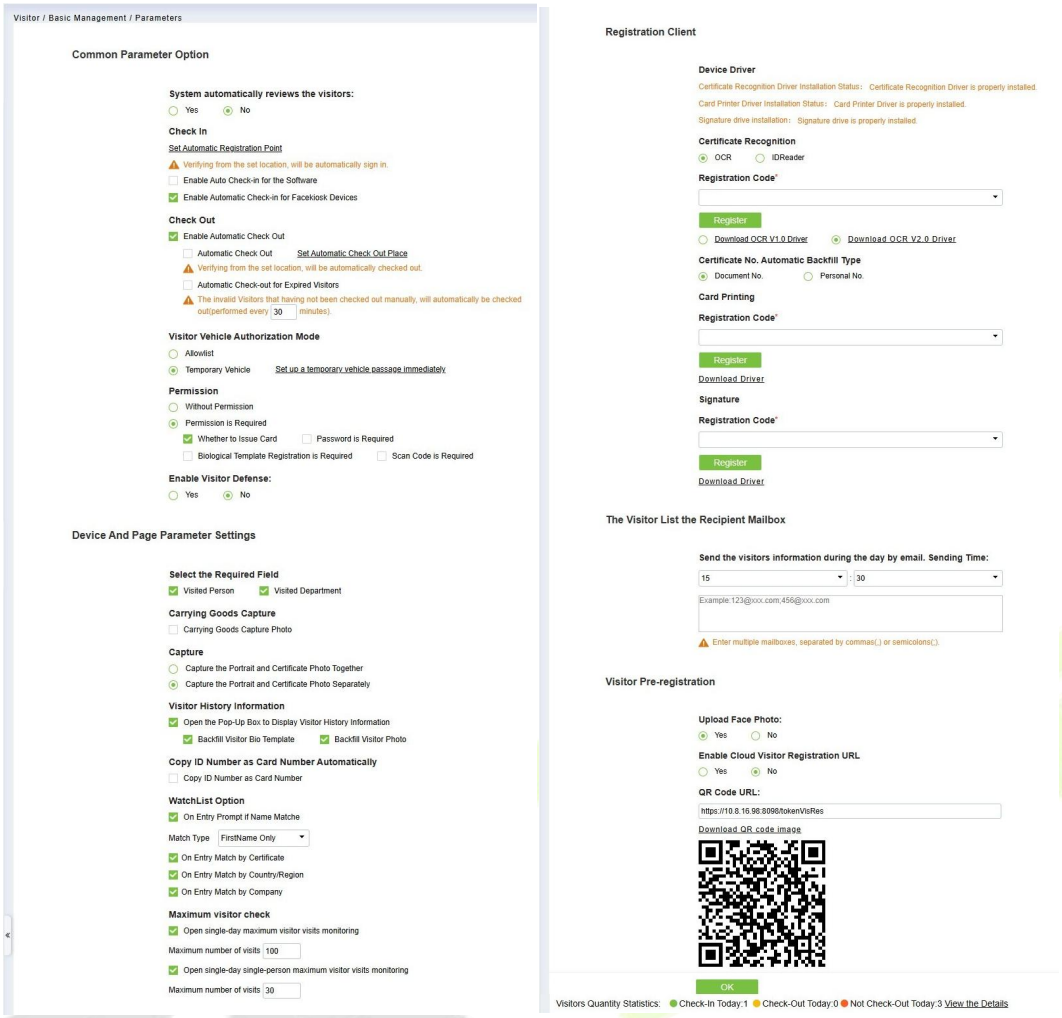


Figure 8- 31 Parameter

- Common Parameter Option:
  - **System automatically reviews the visitors:**After selecting "Yes," the system automatically approves the visitor's reservation information.
  - **Check In:**
  - **Set Automatic Registration Point:** Click to designate access control devices, entrance gates, or parking equipment as registration points. Visitors can self-register and gain immediate access at these designated locations upon arrival.

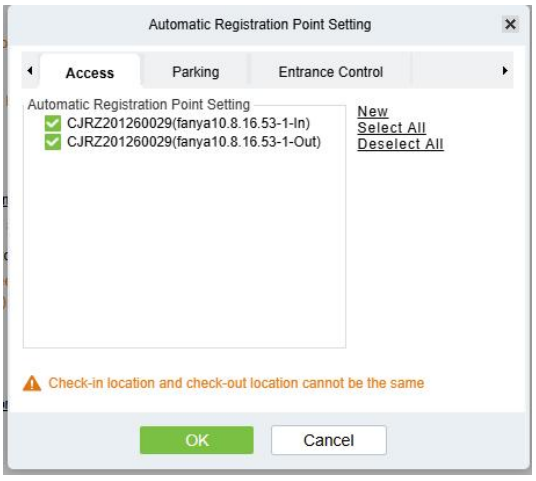


Figure 8- 32 Auto Check-in Point

- **Enable Auto Check-in for the Software:** After activation, it will automatically change the visitor's visit status to Check-in 5 minutes before their scheduled arrival time.
- **Enable Automatic Check-in for Facekiosk Devices:** When activated, visitors will be automatically checked in after registering at the visitor terminal.

If a visitor checks in at an automatic check-in point or a Facekiosk visitor machine, the linked DCS can automatically grant the visitor the floor access permissions of the person they are visiting.

- **Check Out:**

- **Enable Check Out:**When enabled, you can perform a manual check-out operation on the software; when disabled, there is no check-out button.
- **Set Automatic Check Out Place:**Setting automatic sign-out place means specifying some readers as the auto sign-out place. Click Set Automatic Check Out Place. Then click OK to finish.

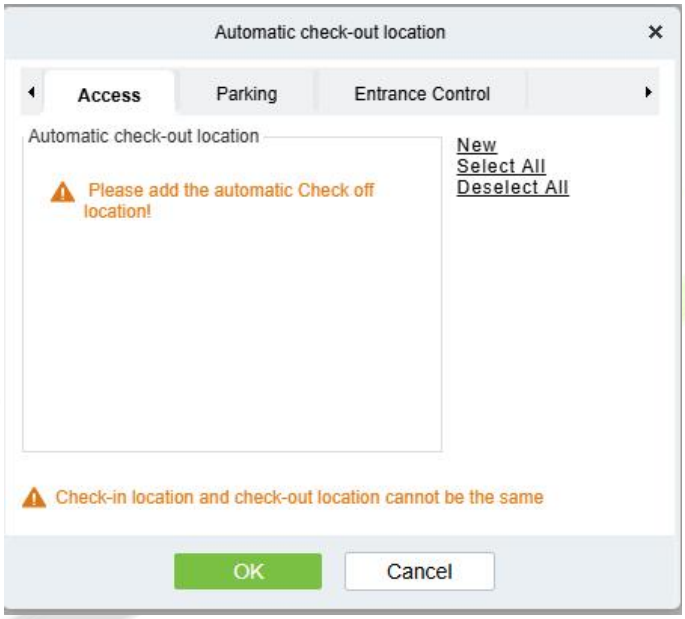


Figure 8- 33 Automatic Exit Place

- **Automatic Check-out for Expired Visitors:** Expired visitors who have not been manually signed out will be automatically signed out after a specified interval.

- **Visitor Vehicle Authorized Mode:**Define the attributes of visitor vehicles, with options for temporary vehicles or the allowed list. Different vehicle attributes need to comply with the vehicle management rules of the Parking module.It is also possible to select a temporary vehicle passage for temporary vehicles.

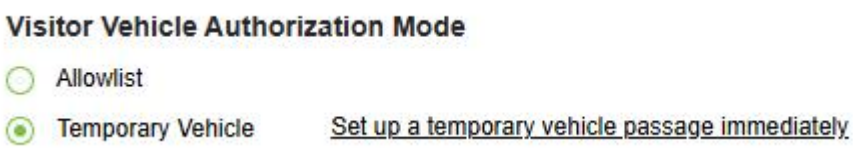


Figure 8- 34 Visitor Vehicle Authorized Mode

- **Permission:**

- **Without permission :**There is no need to grant access control permissions to visitors.

- **Permission is required:**Grant access control permissions to visitors, and further select the method for visitor verification as shown below.

  Whether to Issue Card: Whether to issue card for the visitor.

  Password is required: If selected, it will make password mandatory.

  Biological Template Registration is Required: Whether to register the fingerprint/palm/finger vein for the visitor.

  Scan Code is Required: If selected, it will code scan mandatory.

- **Enable Visitor Defense:** If "**Yes**" is selected, the visitor's registered information will be automatically added to the allowed list database for camera recognition.

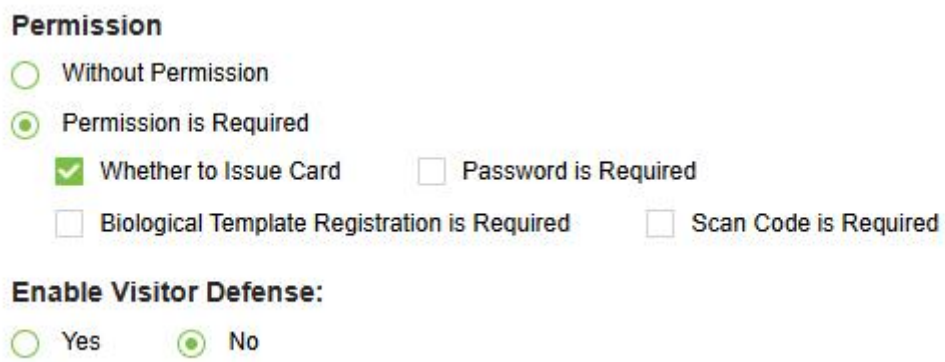


Figure 8- 35 Permission

- Device and Page Parameter Setting:
  - **Select the Required Field:** You can set whether the Host (Personnel) and visited departments would be required in the registration page and the reservation page.
  - **Carrying Goods Capture:**When enabled, visitors will be required to take photos of the goods, upload them, and save them during registration.

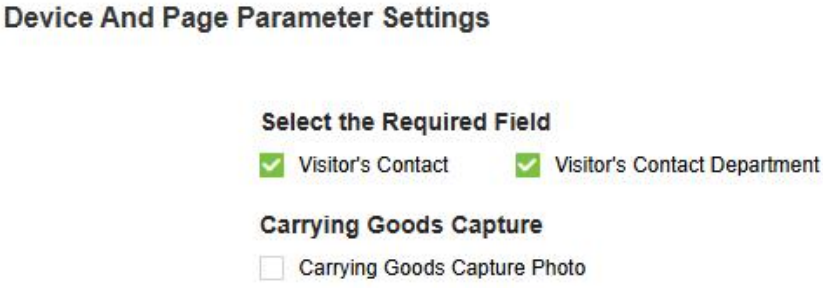


Figure 8- 36 Device and Page Parameter Setting

- **Capture:** Whether to capture the portrait and certificate photo simultaneously during visitor registration.

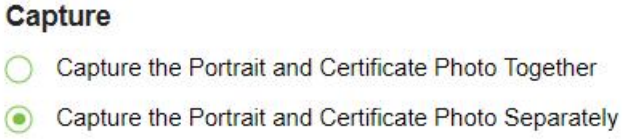


Figure 8- 37 Capture

- **Visitor History Information:** You can select the display parameters of the visitor history. Selecting the Open the Pop-Up Box to Display Visitor History Information check box displays the visitor information with photo and fingerprint of the visitor (These two will be auto-selected).

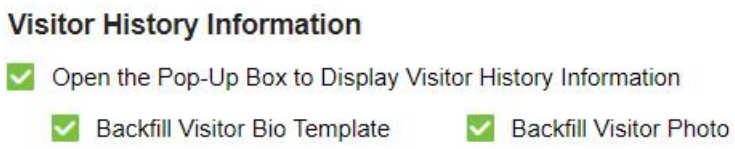


Figure 8- 38 Visitor History Information

- **Copy ID Number as Card Number Automatically:** Enable this if you want to use the same ID number as the Card number.

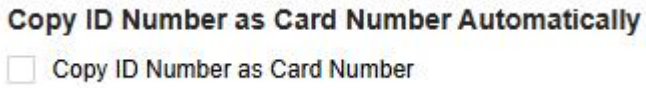


Figure 8- 39 Copy ID Number as Card Number Automatically

- **Watch List Option:** Select the matching rules for the Watch List. If a match is successfully made according to the set rules, a reminder will be given for the Watch List after the reception desk registers the visitor.The optional matching rules are shown in the figure below.

Figure 8- 40 Watch List Option

- **Maximum visitor check:** You can define the parameters to limit the number of visitors and the number of visit times.

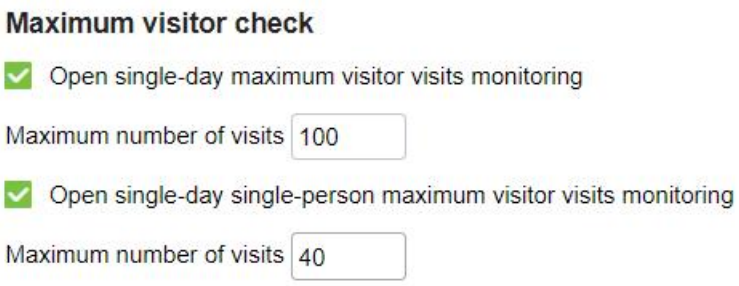


Figure 8- 41 Maximum visitor check

Note: When the number of visitors reaches the default upper limit set on the day, a prompt will pop up when entering the registration page.

●Registration Client(This feature requires activation of the relevant license):

Step 1: If there is no driver installed in the system, the **Download Driver** link is displayed. Click the link to download and install the driver.

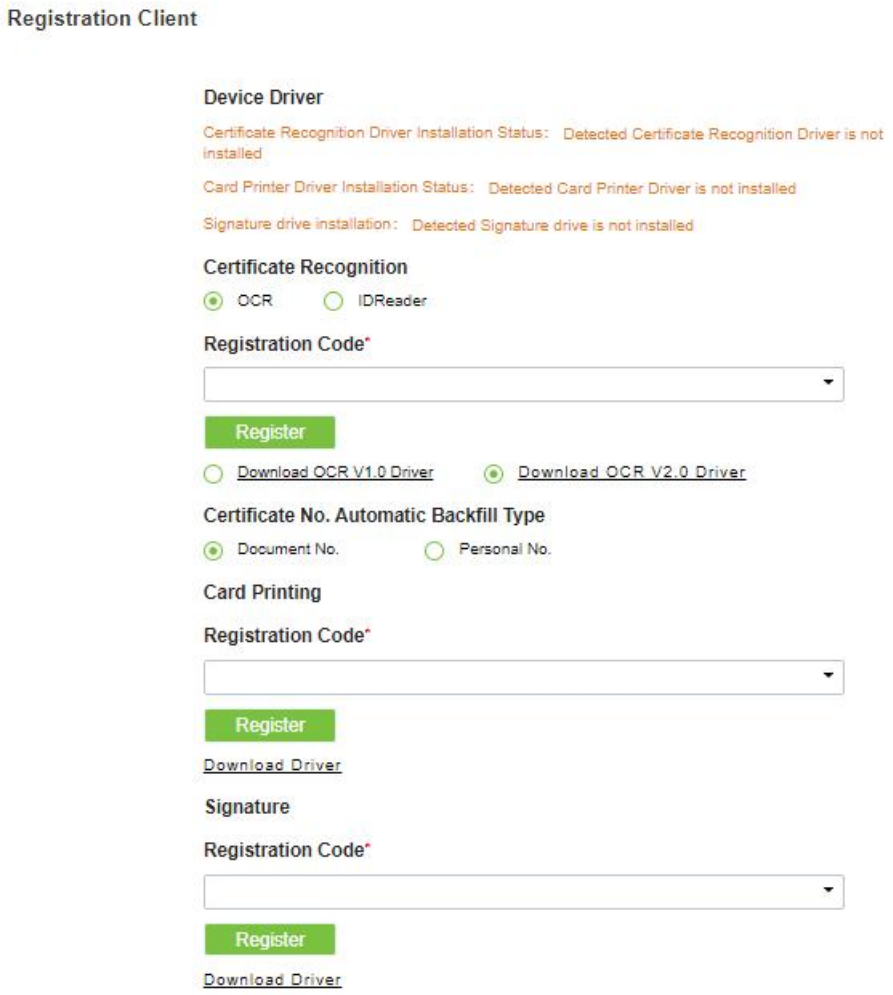


Figure 8- 42 Registration Client

Step 2: Enter the corresponding registration code and click **Register**.

Note: The Registration code can only be obtained after purchasing the corresponding license. After activating the license, you can check it at **System** > **Authority Management** > **Client Register** to view the **registration code.**

●The Visitor List the Recipient Mailbox:

Configure the recipient's mailbox and the time for system to send the list of visitors.

Figure 8- 43 Visitor List the Recipient Mailbox

●Visitor Pre-registration:

Visitors can use the self-service registration link. If you have already installed and activated the ZKBio CVConnect Client, you can click on "use cloud visitor link," and it will automatically fill in the cloud

visitor link.

Note: You can download the ZKBio CVConnect Client and enable cloud settings under System -> System Management -> Cloud Settings.

Figure 8- 44 Visitor Pre-registration

8.5.2Equipment Debugging

Equipment Debugging option will provide information about Entry Place, Print installation, Device Driver installation, and USB Camera.

In **Visitor** module Click **Basic Management** > **Equipment Debugging** to know about the current location details (including IP address), Printer-driver installation information, device driver installation, calibrate the scanners, and USB camera information.

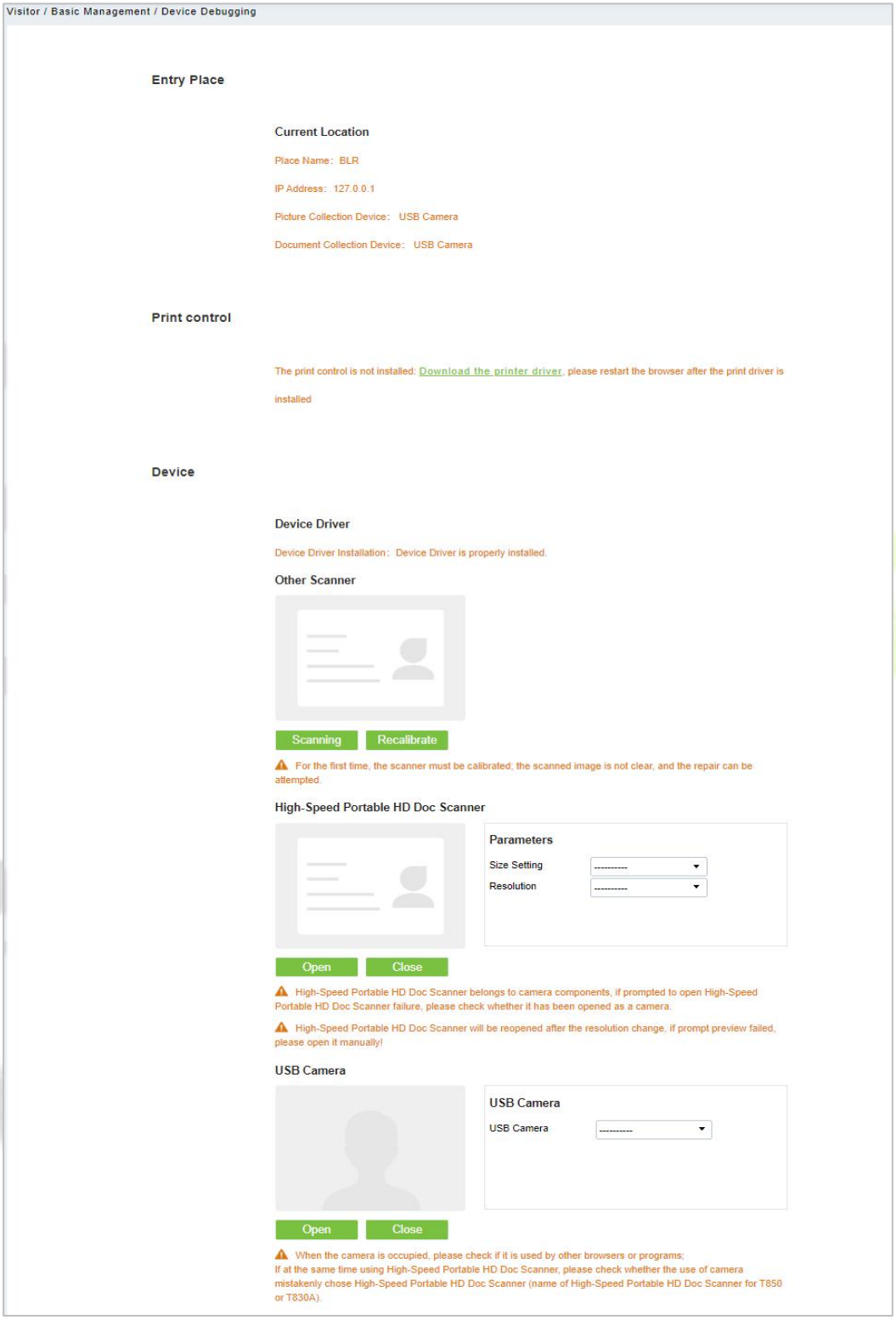


Figure 8- 45 Device Debugging Interface

Parameter	Description
Visitor Registration Point	Displays the information of the current entry place, such as the name of the entry place, IP, Mode of picture/document collection.
Print Control	It shows the Printer-driver installation information

Parameter	Description
Device	Display device driver installation, you can debug, calibrate the scanner. Set the High-Speed Portable HD Doc Scanner parameters, and information of USB camera. (IE browser does not display USB device debugging).

Table 8- 10 Description of Parameters of Device Debugging

8.5.3Print Settings

In **Visitor** module Click **Basic Management** > **Print Setting** to go to the printer settings.

● Global Settings (Receipt Printer):

Select **Receipt Printer** to set the global setting of the printer.

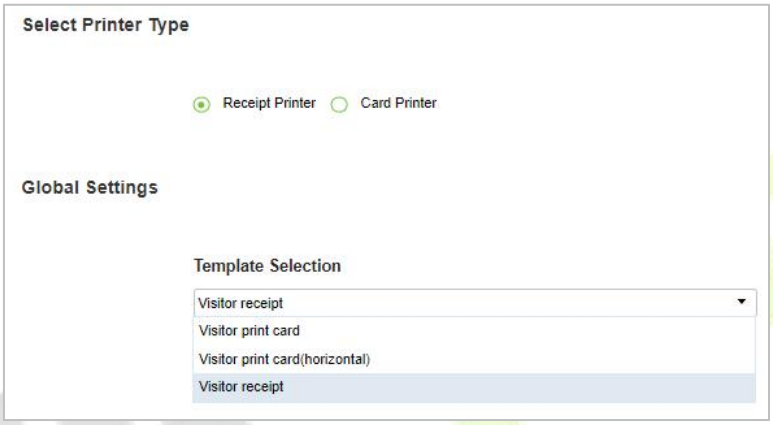


Figure 8- 46 Global Settings of Printer

Parameter	Description
Template Selection	Select a template to print the template, if the template does not meet the print content, you can add or edit the template (the default template cannot be edited, deleted). Available Templates are Visitor Receipt, Visitor Print Card and Visitor Print Card (Horizontal).

Table 8- 11 Description of Parameters of Printer Setting

● Local Settings (Receipt Printer):

You can set the options for the printer, the type of paper to be printed, or the custom paper size, and view the effect by clicking Print Preview / Direct Print. At last, you can save the current setting for the printout of the visitor badge.

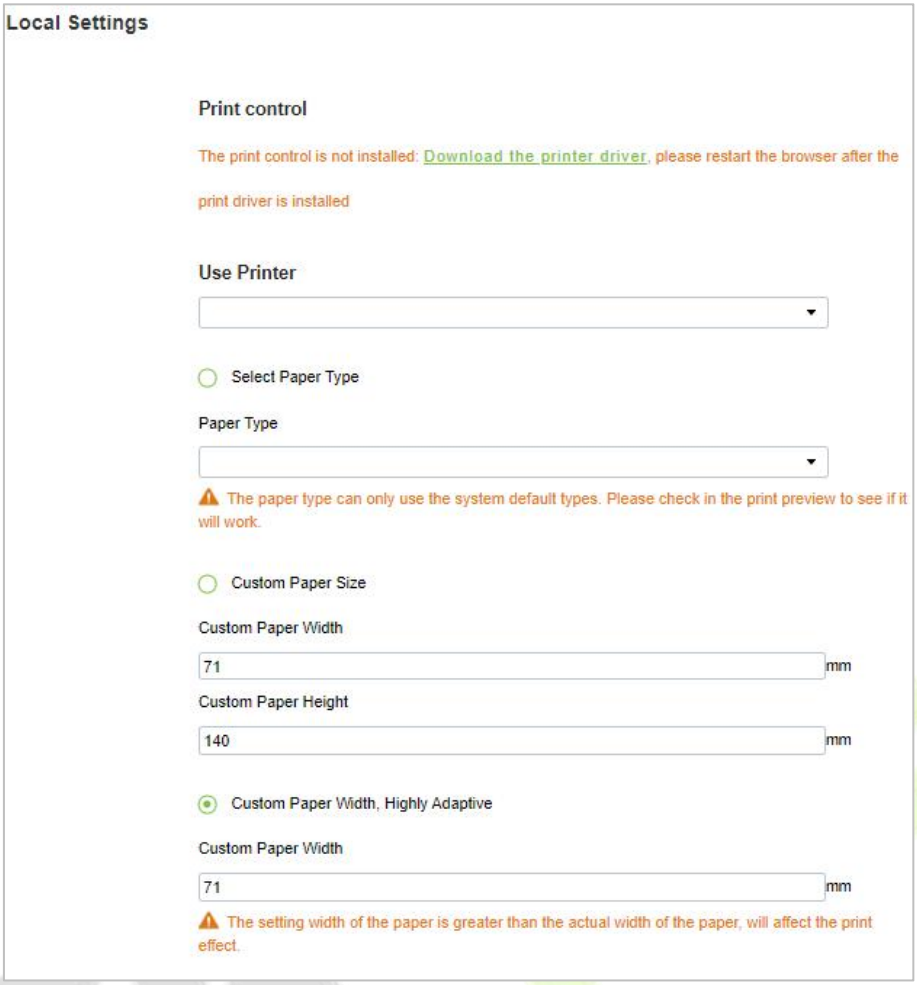


Figure 8- 47 Local Settings of Printer

Parameter	Description
Use Printer	Select the printers from the available list of printers.
Paper Type	Select the Paper Type
Custom Paper Size	You can customize the paper size like paper height and width.

Table 8- 12 Description of Parameters of Local Settings of Printer

● Card Printing:

In the parameter setting interface, you can set the parameters of card. Initially, define the template (refer to personnel card printing), and then set the card printing function. If the automatic card printing is selected, printer connection is required. After the visitor registration is completed, user can print the card directly.

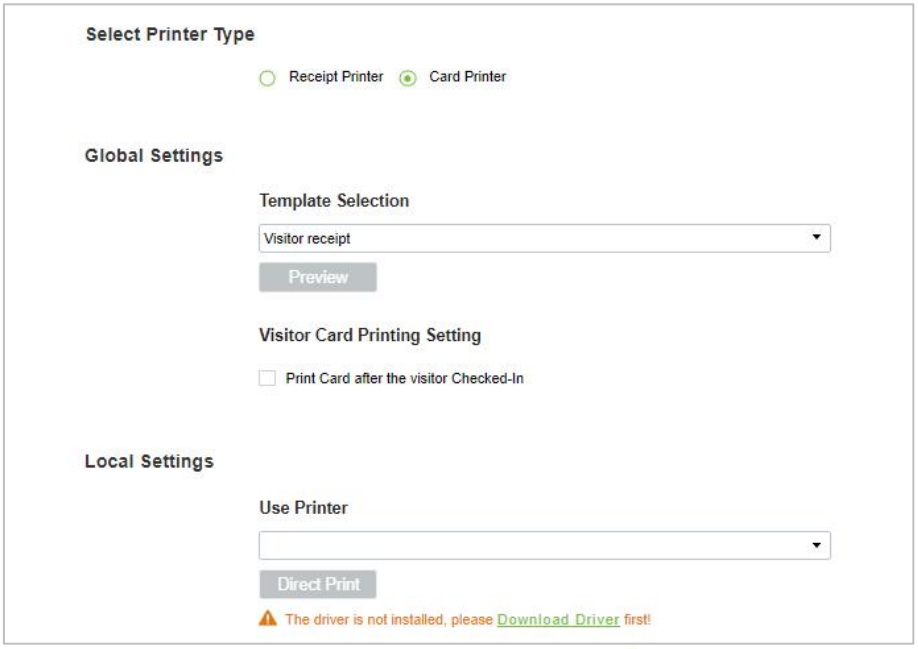


Figure 8- 48 Printer Setting of Card Printer

Parameter	Description
Template Selection	Select a template to print the template, if the template does not meet the print content, you can add or edit the template (the default template cannot be edited, deleted). Available Templates are Visitor Receipt, Visitor Print Card and Visitor Print Card (Horizontal).
Visitor Card Printing Setting	Select the visitor card printing settings (like after visitor check in)
Use Printer	Select the printer from the available list of printers.

Table 8- 13 Description of Parameters of Printer Setting of Card Printer

8.5.4Visiting Permission

Pre-configure visitors' access permissions for access control, elevator control, and passage.

Note: First configure permissions in the access control, elevator control, and passage modules.

Once configured, permissions can be:

- Assigned during visitor registration, or

manually added in the visitor permission group interface after registration.

- Permissions are automatically revoked when visitors check out.

To access: Visitor interface > **Basic Management** > **Visiting Permission**.

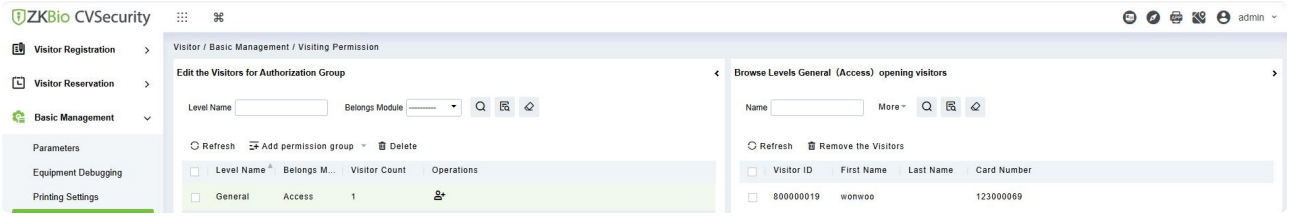


Figure 8- 49 Visitor Level Interface

8.5.4.1Add Permission Group

In this option you can give access, elevators, and entrance control permissions to the visitors.

Add Access Levels

To add Access Levels.

●Operating Steps:

Step 1: In the Visitor Module, click **Basic Management** > **Visiting Permission** > **Add Access Levels.**

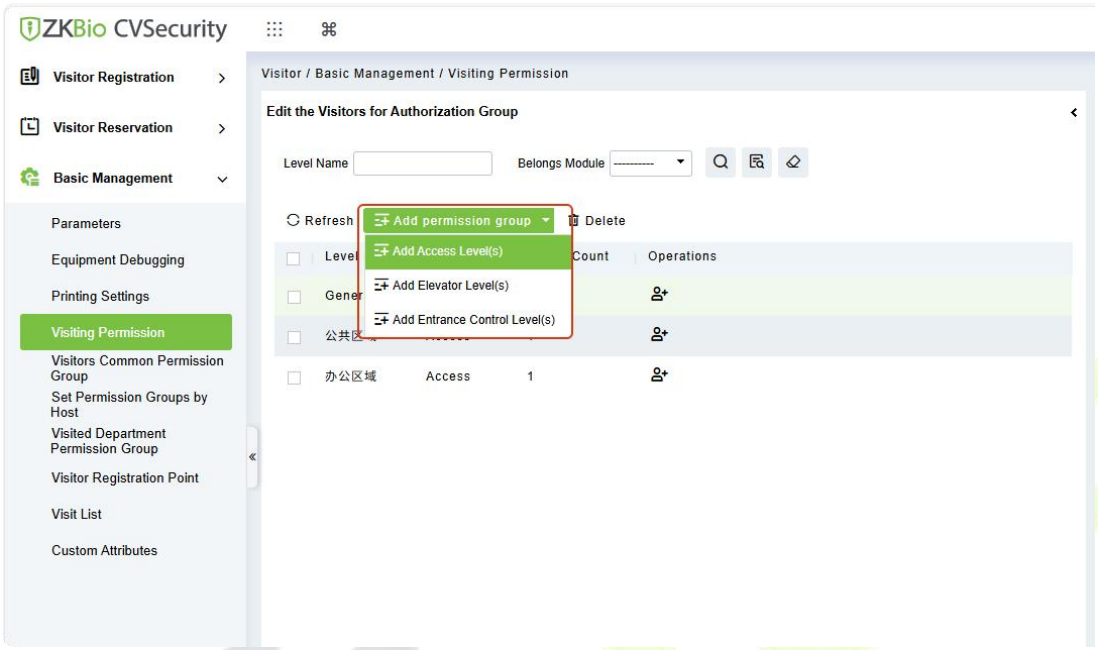


Figure 8- 50 Add Access Level Interface

Step 2: Select one or more access levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

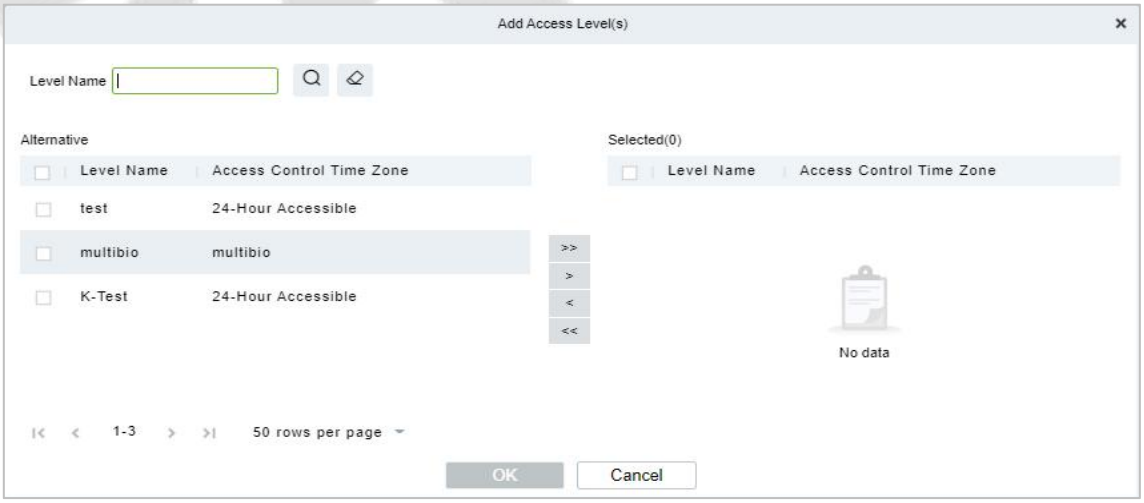


Figure 8- 51 Add Access Level Interface

Step 3: In the **Visitor** module, select **Visitor Registration** > **Visitor Check-in** interface, and click **Visitor Check-in** to assign personnel visitor permissions.

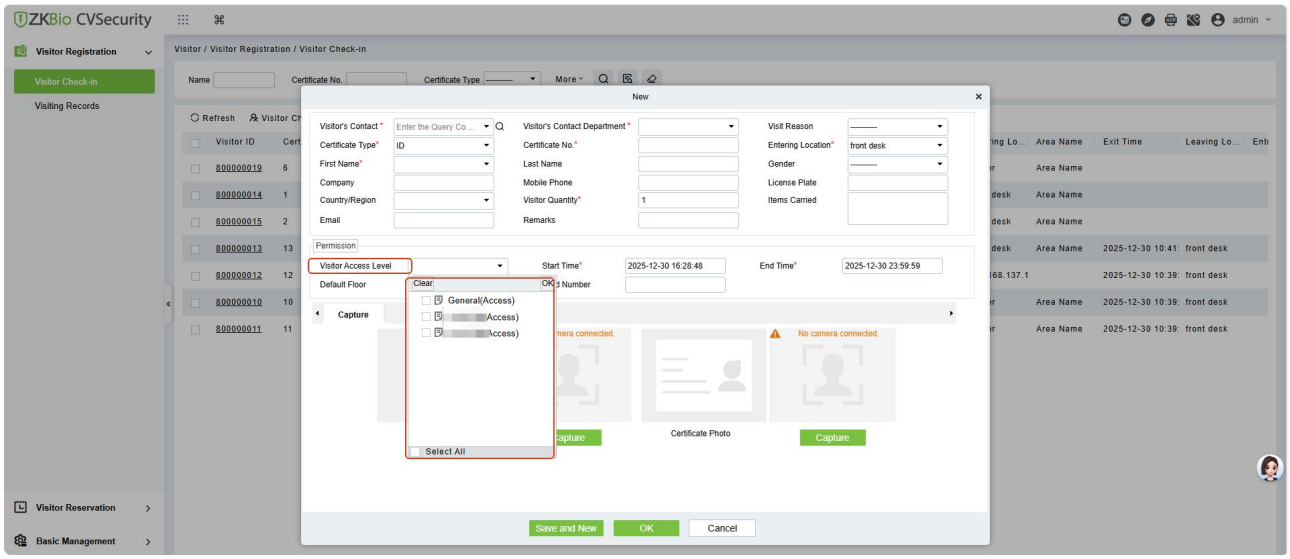


Figure 8- 52 Visitor Add Visitor Permission Interface

Add Elevator Levels

To add Elevator Levels.

● Operating Steps:

Step 1: In the Visitor Module, click **Basic Management** > **Visiting Permission** > **Add Elevator Levels**.

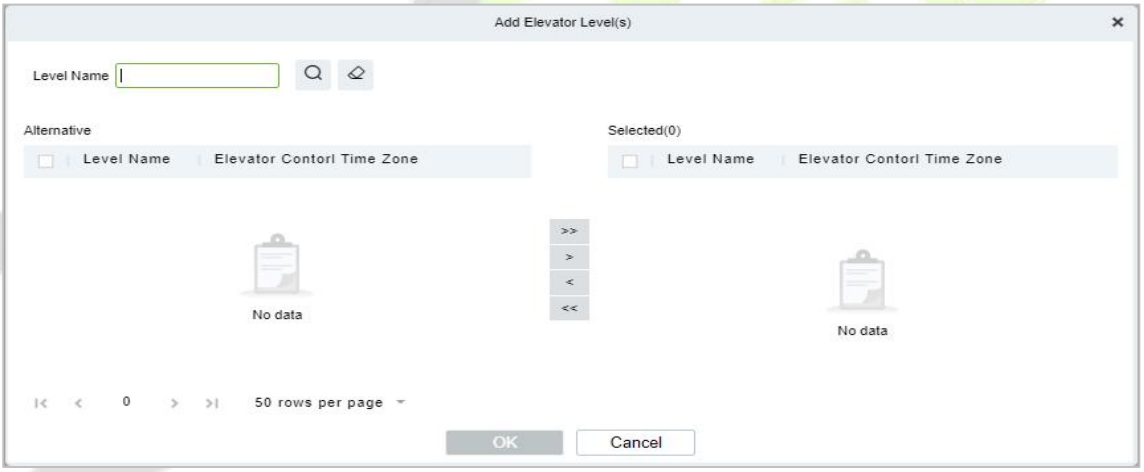


Figure 8- 53 Add Elevator Level Interface

Step 2: Select one or more elevator levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

Step 3: Allocate the elevator levels for the visitor when registering.(It is the same as the operation steps for access control permissions)

Add Entrance Control Level

To add Entrance Control Levels.

● Operating Steps:

Step 1: In the Visitor Module, click **Basic Management** > **Visiting Permission** > **Add Entrance Control Level**

Step 2: Select one or more entrance control levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

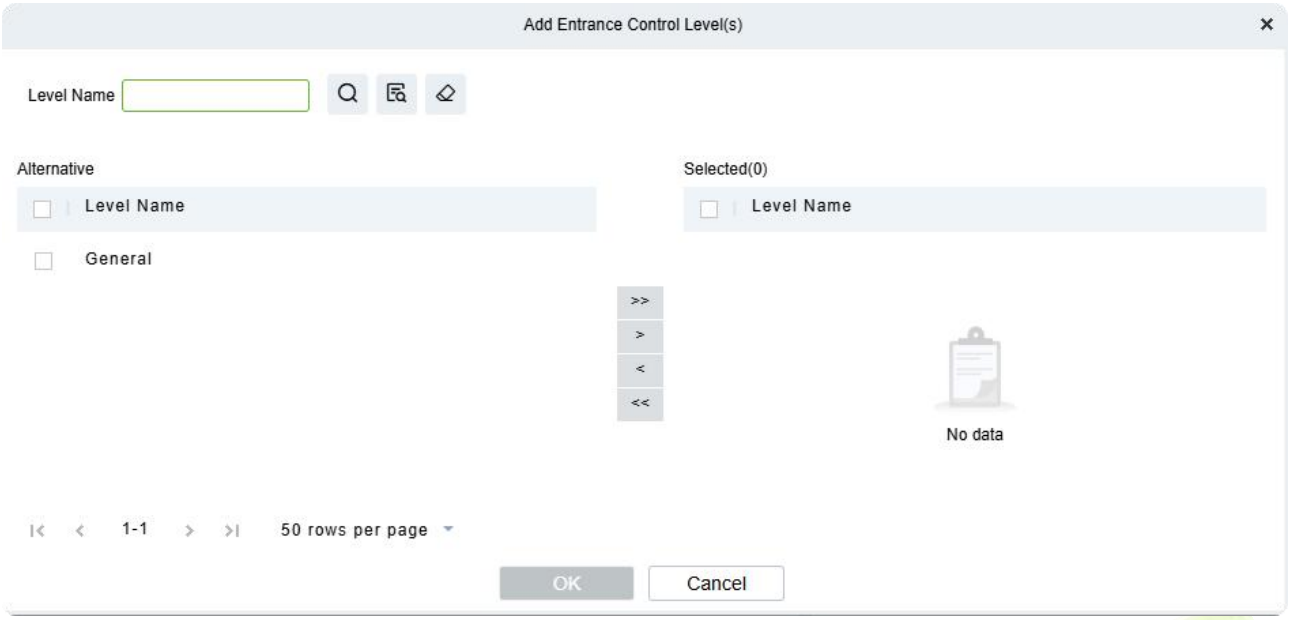


Figure 8- 54 Add Entrance Control Level Interface

Step 3: Allocate the entrance control levels for the visitor when registering.(It is the same as the operation steps for access control permissions)

8.5.4.2Delete

In the **Visitor** module, click **Basic Management** > **Visiting Permission**, select a visitor level and click **Delete** to delete the visitor level.

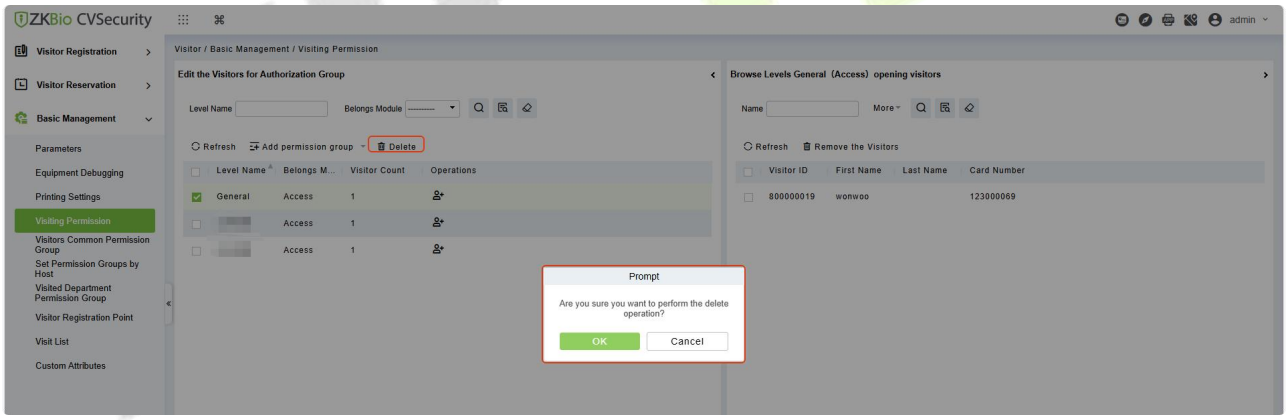


Figure 8- 55 Delete Level Interface

Click **OK** to perform the delete operation.

8.5.4.3Add Visitors to Levels (Browse Level)

Adding visitors to levels.

● Operating Steps

Step 1: In the Visitor module, click **Basic Management** > **Visiting Permission**.

Step 2: Select the permission group, click on the icon under the operation categories.

Step 3: Select one or more visitors, click > or >> to move into the Selected menu. Click **OK**.

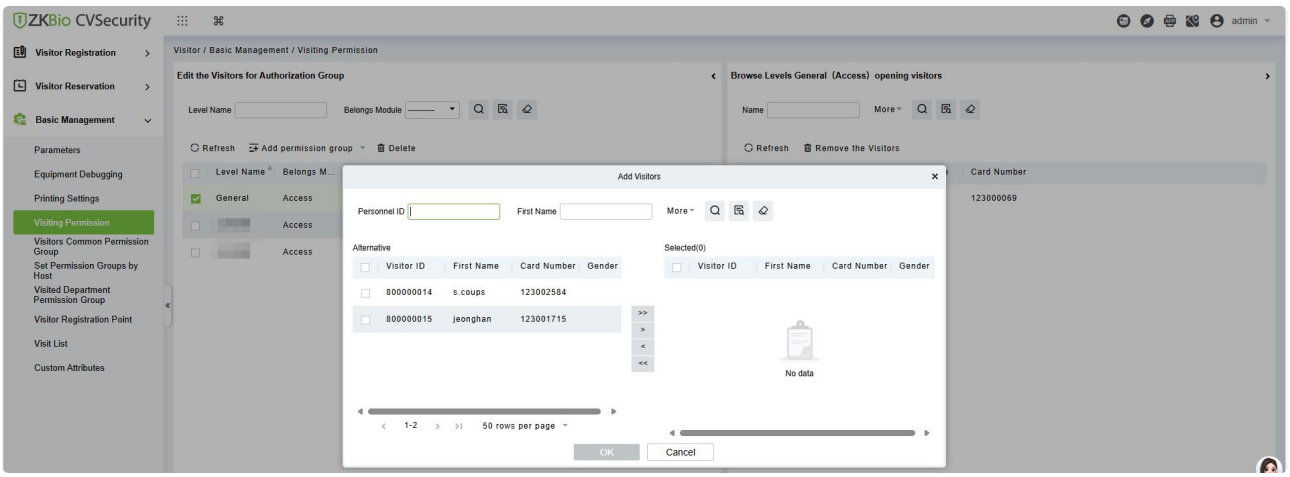


Figure 8- 56 Add Visitor Interface

Step 4: After clicking **OK** the processing window will appear like figure below shows below**.**

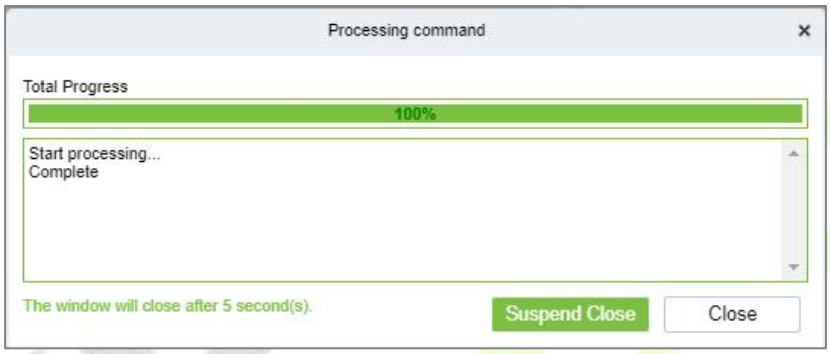


Figure 8- 57 Processing Command Interface

8.5.4.4Remove the Visitors from Browse Level

Removing the visitors from the levels.

●Operating Steps:

Step 1: In the Visitor Module, click **Basic Management** > **Visiting Permission**.

Steps 2: Select the visitor to be deleted, Click **Remove the Visitor** as shown in figure below.

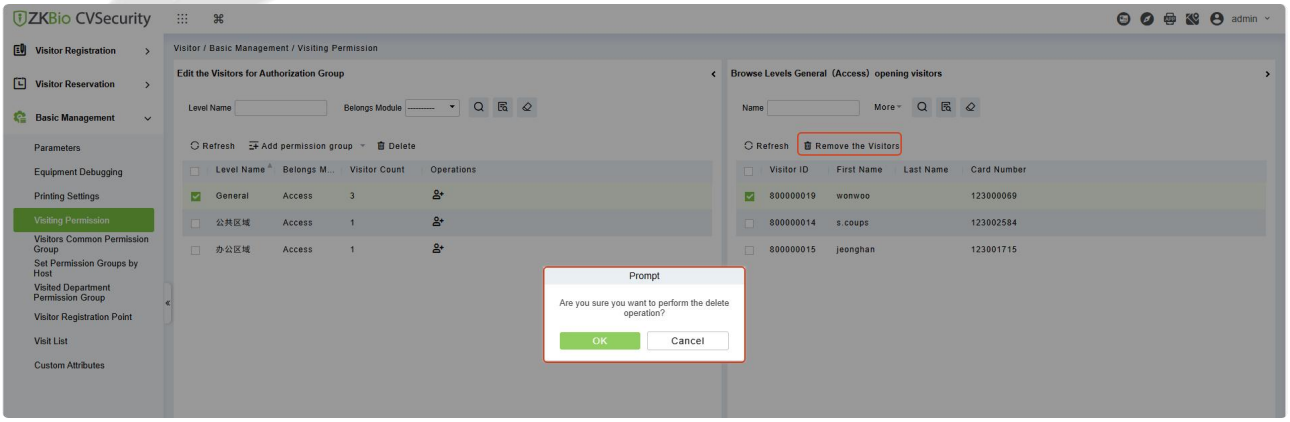


Figure 8- 58 Remove Visitors from Browse Level

Step 3: Click **OK** to perform the delete operation.

8.5.5Visitor Common Permission Group

After a visitor's reservation is approved, they will be automatically added to the Visitor Common Permission Group. The validity period of this permission group will cover from 00:0 0:00 on the day the visit starts to 23:59:59 on the day the visit ends, ensuring that the permission is valid throughout the entire visit period.Even if the visitor arrives before the start time of the visit, they can use the permissions in the Visitor Comm on Permission Group to verify and pass through; even if the visitor has not checked out after the end time of the visit, they can still use the permissions in the Visitor Common Permission Group to verify and pass through. Due to the above functional characteristics, it is mainly used for access permission management of gate entrances and exits as well as public areas (such as the first-floor lobby, first-floor elevators, and other public areas with **lower security levels**).

Designated devices such as access control systems, parking systems, and passageways serve as automatic check-in points. When visitors arrive at these designated devices, they can obtain access permissions and complete registration.

Note: The Visitor Common Permission Group is usualy used in conjunction with the automatic check. in point function. If the automatic check-in function is configured in the parameters, please be sure to configure the Visitor Common Permission Group at the same time.

8.5.5.1Add Permission Group

Add Access Level

To add Access Level Group

● Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Visitor Common Permission Group**.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Access Level**, and then add the corresponding permissions.

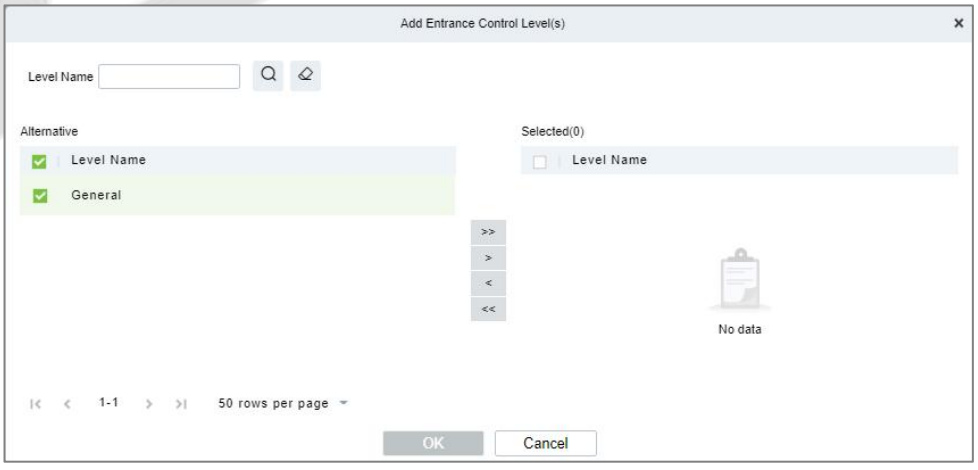


Figure 8- 59 Visitor Permission Group Adding Interface

Select one or more access levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

Add Elevator Level

To add Access Level Group

●Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Visitor Common Permission Group**.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Elevator Level**, and then add the corresponding permissions.

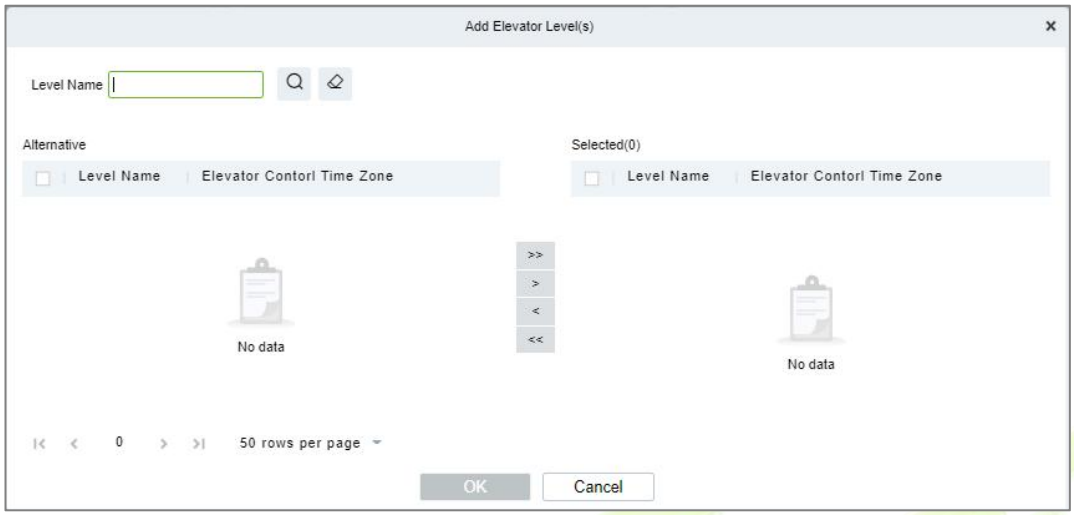


Figure 8- 60 Visitor Permission Group Adding Interface

Select one or more elevator levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

Add Entrance Control Level

To add Access Level Group.

●Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Visitor Common Permission Group**.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Entrance Control Level**, and then add the corresponding permissions.

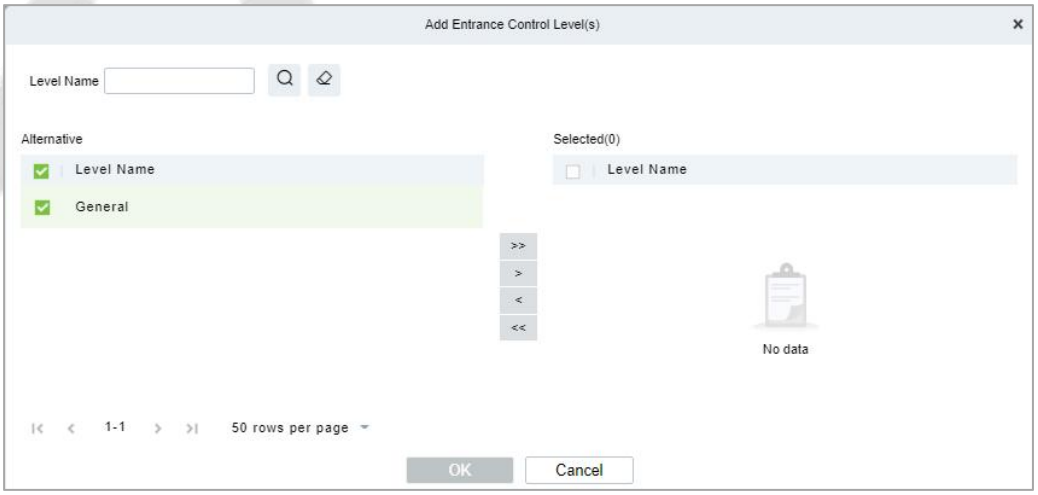


Figure 8- 61 Visitor Permission Group Adding Interface

Select one or more entrance control levels, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their names.

8.5.5.2Delete

In the **Visitor Module,** click **Basic Management** > **Visitor Common Permission Group**, select a visitor

level and click **Delete** to delete the visitor level.

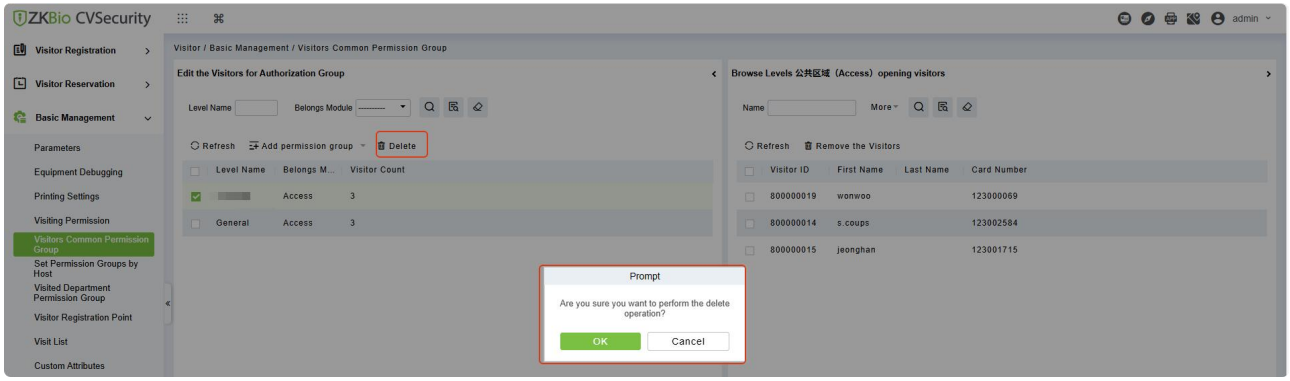


Figure 8- 62 Delete Level Interface

Click **OK** to perform the delete operation.

8.5.5.3Remove Visitors from Browse Level

●Operating Steps:

Step 1: In the Visitor Module, click **Basic Management > Visitor Common Permission Group.**

Step 2: Select the visitor details to be deleted, Click **Remove the Visitor**.

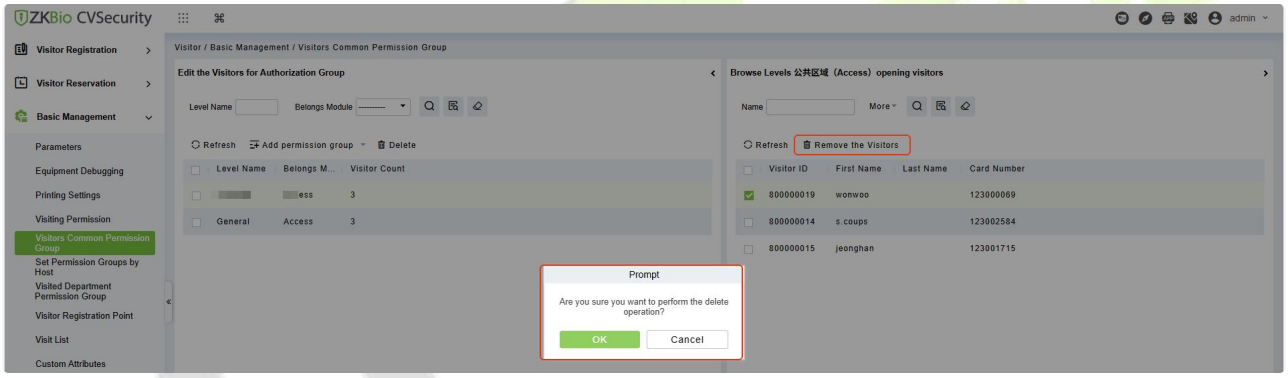


Figure 8- 63 Remove Visitors from Browse Level

Step 3: Click **OK** to perform the delete operation.

8.5.6Set Permission Groups by Host

Configure this function so that when a visitor registers, they are automatically granted the permissions of the person being visited, and these permissions are automatically revoked when the visitor check out.

8.5.6.1New

This part introduces the configuration steps of Set Permission Groups by Host.

●Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Set Permission Groups by Host**.

Step 2: In the Set Permission Groups by Host interface, click **New** to add interviewee.

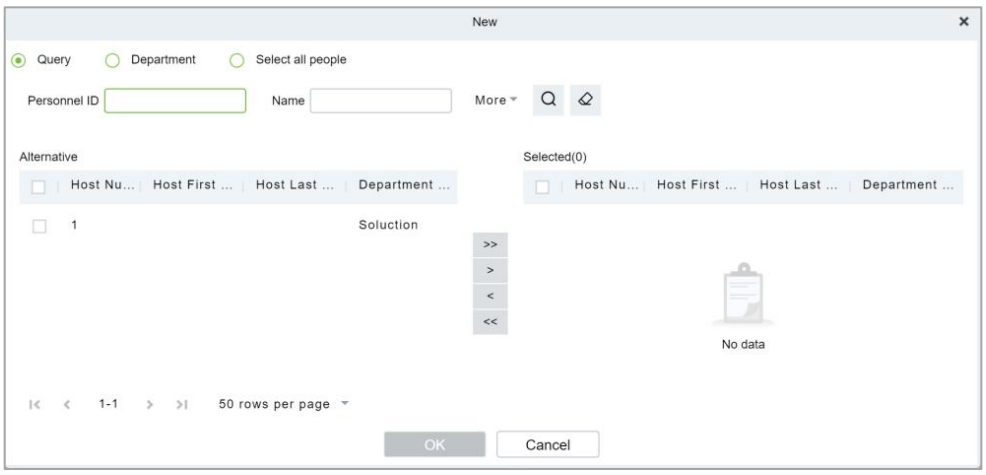


Figure 8- 64 New Interface for Interviewee

Step 3: After the new information is successfully added, click **Add Visited Levels** under operations. After the respondent adds the corresponding permissions, this permission group will be distributed to the visitor when the visitor registers, and the visitor will have the permissions possessed by this permission group.

Note: Only after configuring the permission group in the visiting permission can it appear in the list here for selection.

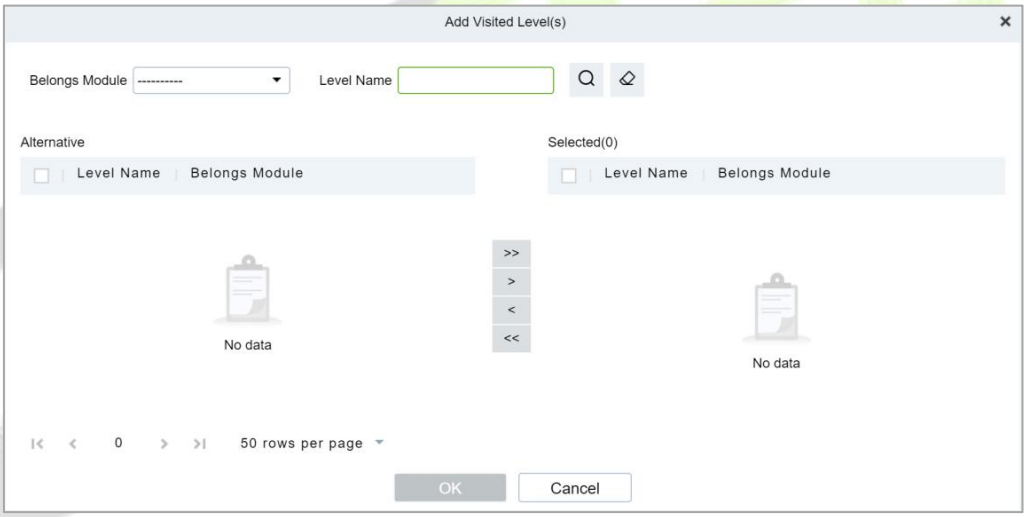


Figure 8- 65 Add Visitor Permissions Interface

8.5.6.2Delete

In the **Visitor** module**,** click **Basic Management > Set Permission Groups by Host**, select a Host and click **Delete** to delete the Host level.

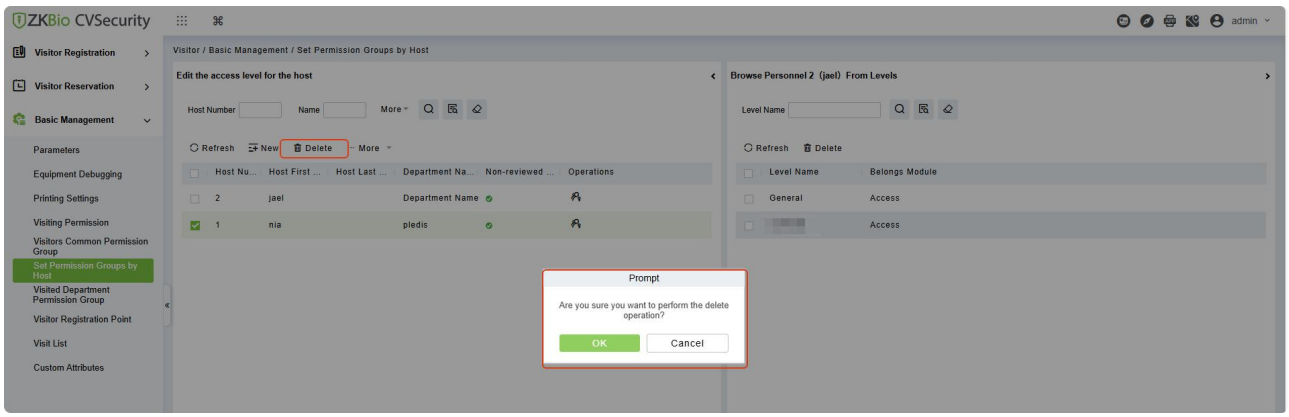


Figure 8- 66 Delete Level Interface

Click **OK** to perform the delete operation.

8.5.6.3More

8.5.6.3.1 Non-reviewed Visitors

Authorize the interviewee with the functional permission of invitation without review.

● Operating Steps:

Step 1: In the **Visitor** module, click **Basic Management > Set Permission Groups by Host**, select Interviewee.

Step 2: Click **More > Non-reviewed Visitors** and select **Yes** or **No** from the drop-down list as shown in figure below.

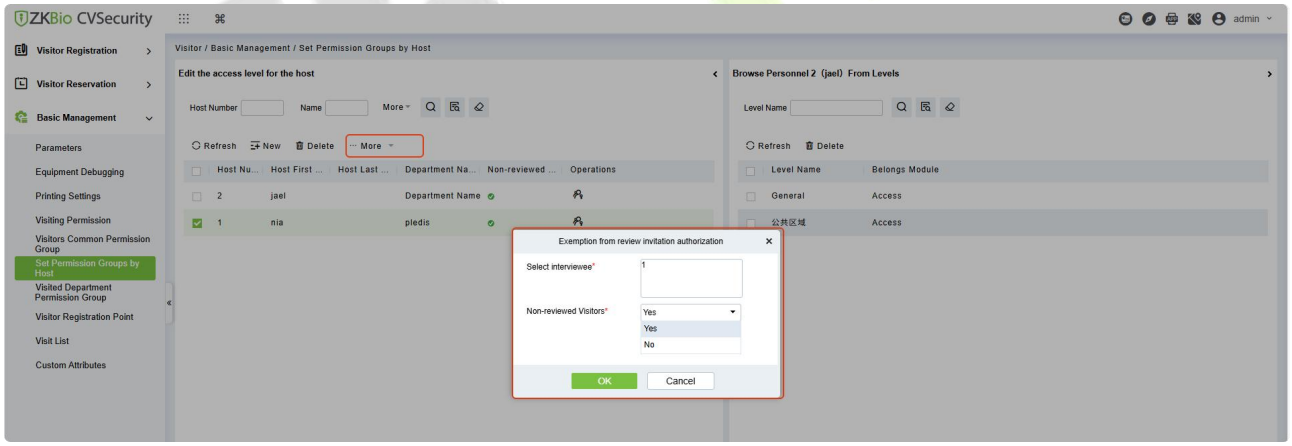


Figure 8- 67 Authorized Exemption Invitation Interface

Step 3: Click **OK** to send authorized exemption invitation to the interviewee.

8.5.6.3.2 Batch Add Visited Permission Groups

After selecting multiple interviewees, click **More** > **Batch Add Visited Permission Groups**.Select one or more permission groups, click > or >> to move into the Selected menu. Click **OK**.Permission groups can be queried and filtered by their belongs module and names.

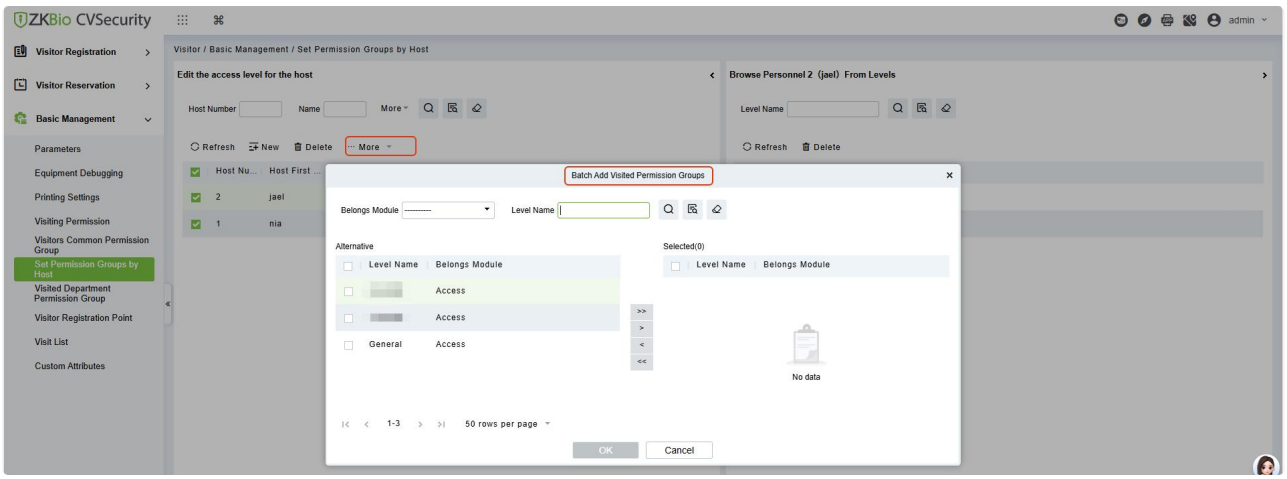


Figure 8- 68 Batch Add Visited Permission Groups

8.5.6.4Remove Visited Host Level from Browse Level (Delete)

● Operating Steps:

Step 1: In the Visitor module, click **Basic Management** > **Set Permission Groups by Host**.

Step 2: Select the visited level details to be deleted, click **Delete**.

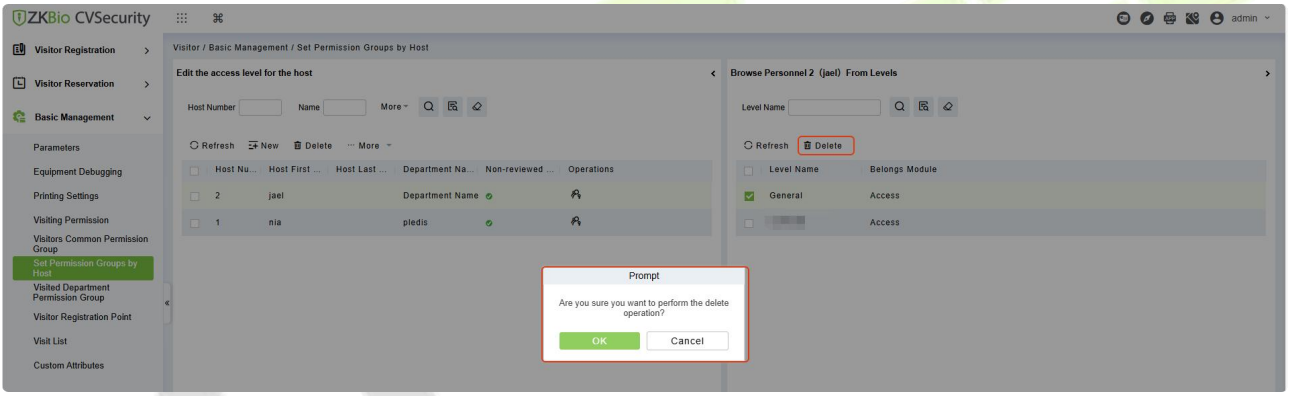


Figure 8- 69 Remove Visited Level from Browse Level

Step 3: Click **OK** to perform the delete operation.

8.5.7Visited Department Permission Group

Configure this function to automatically grant the visitor the permissions of the visited person's department upon visitor registration, and automatically revoke these permissions when the visitor signs out.

8.5.7.1New

● Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Visited Department Permission Group**.

Step 2: In the Visited Department Permission Group interface, click **New** to add the visited department.

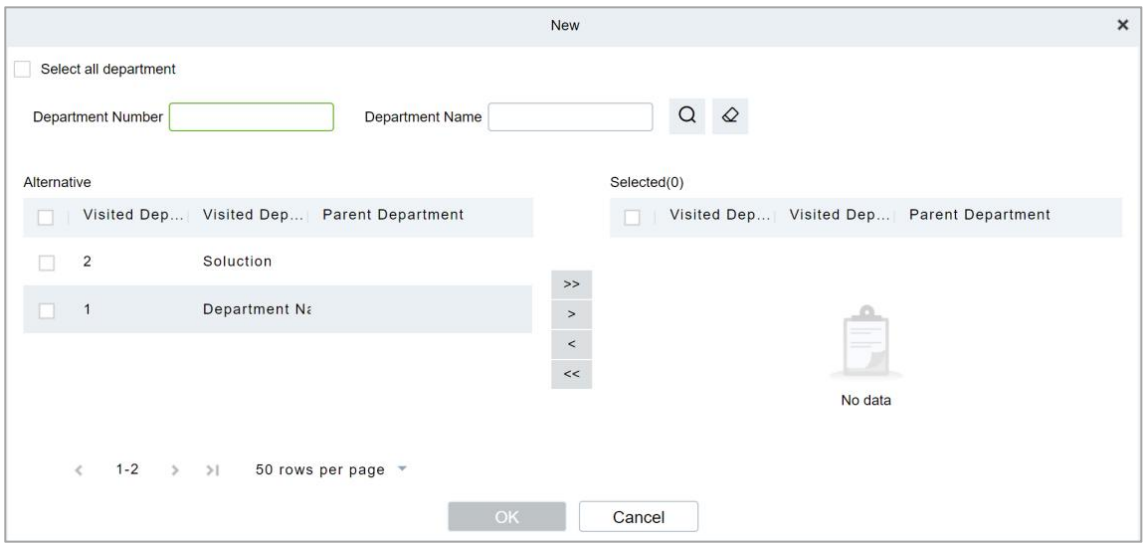


Figure 8- 70 Add Department Interface

Step 3: In the interface of editing permission group for visited department, click **Add Visited Level** under Operation. After adding the corresponding permission, when the visitor registers, this permission group will be distributed to the visitor, and the visitor will have the permission of this permission group.

Note: Only after configuring the permission group in the visiting permission can it appear in the list here for selection.

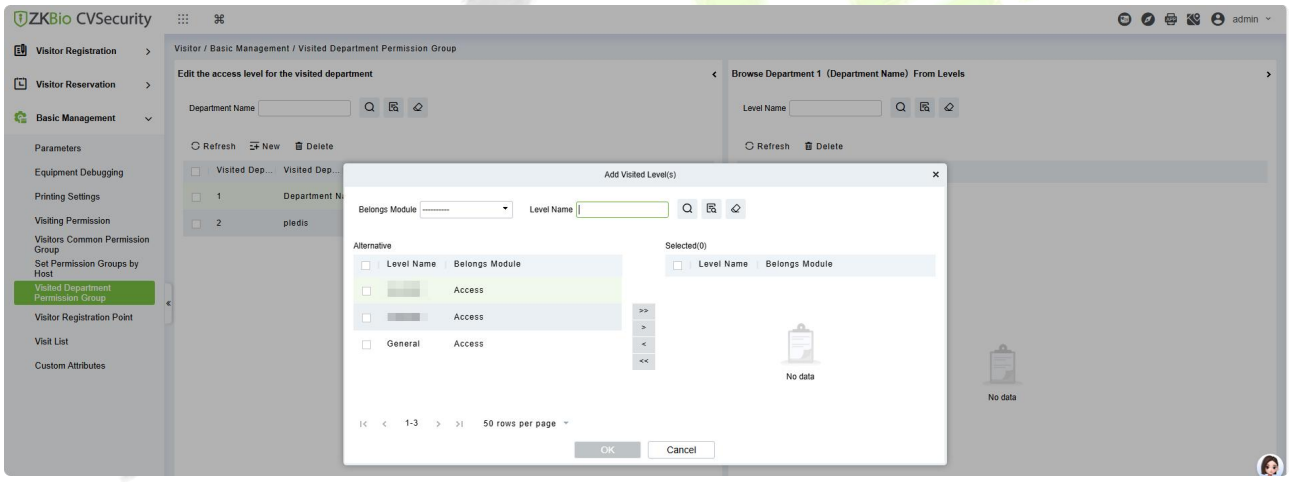


Figure 8- 71 Add Department Permission Interface

8.5.7.2Delete

In the **Visitor** module, click **Basic Management** > **Visited Department Permission Group**, select a visited department and click **Delete** to delete the Department Permission Group.

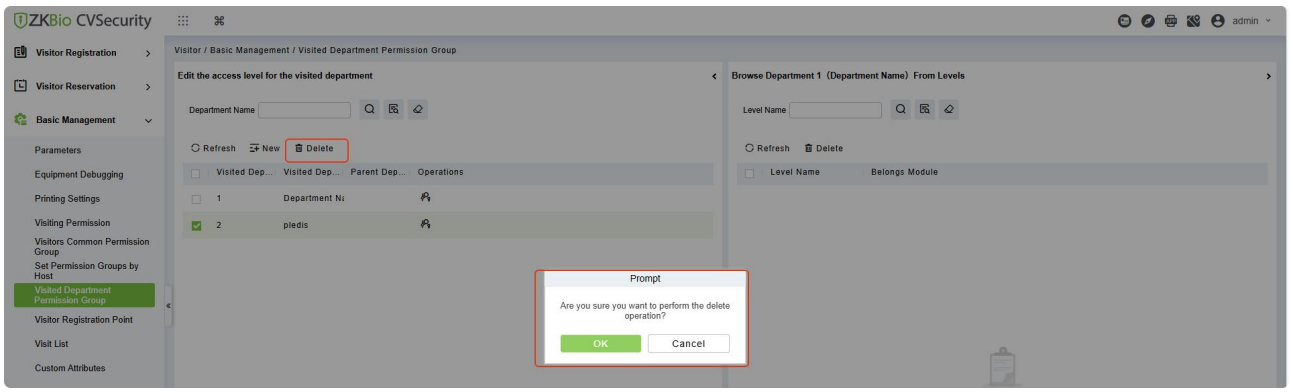


Figure 8- 72 Delete Visited Department Interface

Click **OK** to perform the delete operation.

8.5.7.3Remove Visited Department Level from Browse Level (Delete)

●Operating Steps

Step 1: In the Visitor module, click **Basic Management > Visited Department Permission Group.**

Steps 2: Select the Level details to be deleted, click **Delete**.

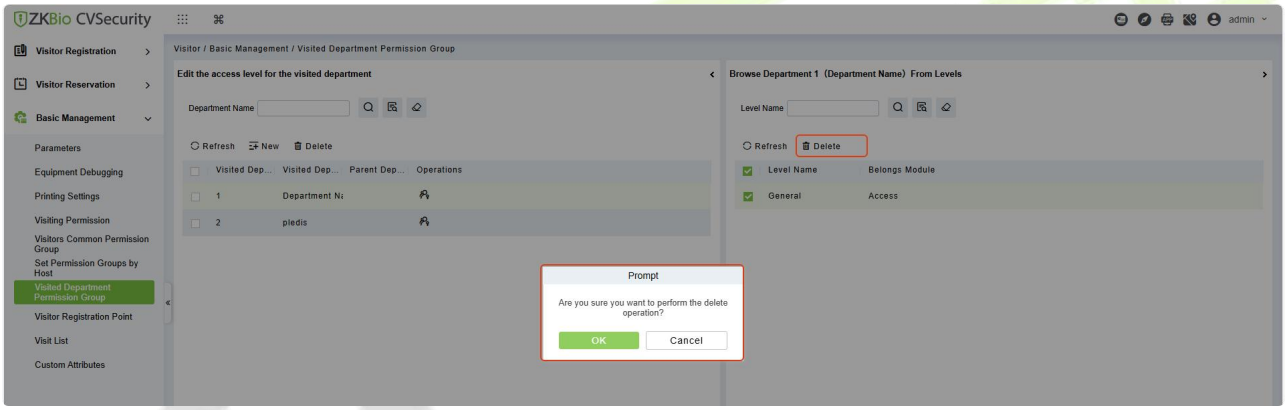


Figure 8- 73 Remove Visited Level from Browse Level

Step 3: Click **OK** to perform the delete operation.

8.5.8Visitor Registration Point

Only the registered platform (including PC platform and visitor plane) can register and sign off visitors.

This interface displays a list of all registered places in the visitor system. Displays fields such as enlistment location name, IP address, area name, and so on.

8.5.8.1New

Introduces the configuration steps of registering locations in ZKBio CVSecurity.

1.Ordinary Computer

●Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Visitor Registration Point**.

Step 2: In the Visitor Registration Point interface, click **New** and select **Ordinary Computer** as the visitor machine type, as shown in figure below. Please refer to Table below for parameter description.

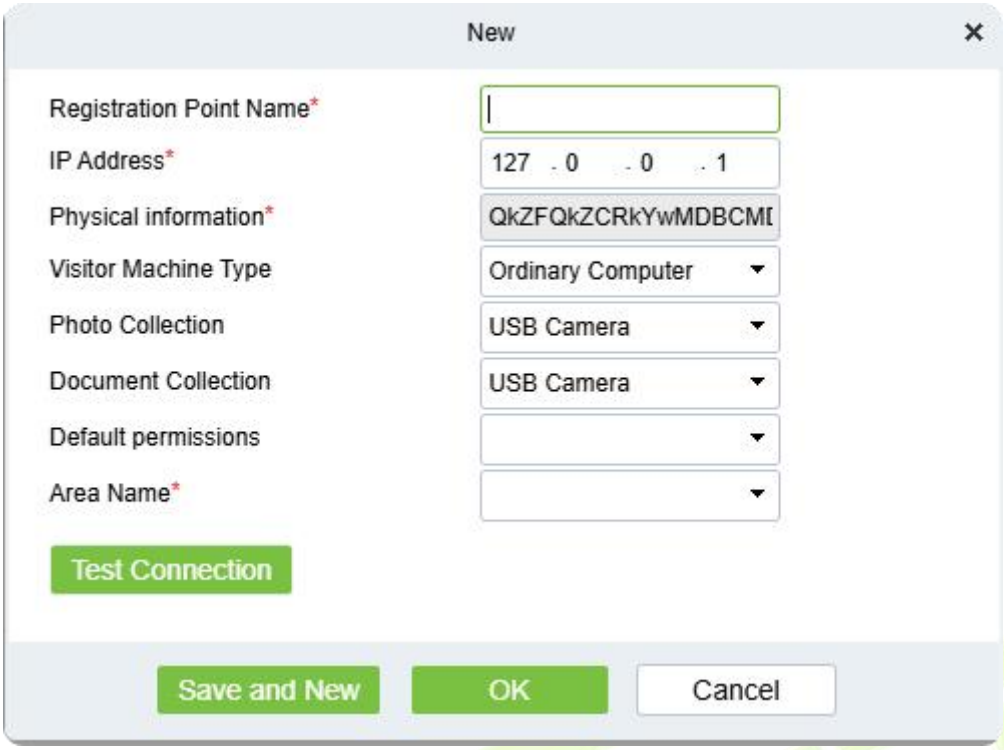


Figure 8- 74 Ordinary Computer Entry Place Interface

Parameter	Description
Registration Point Name	Any character, no more than 50, not repeatable.
IP Address	Register the IP address of the computer used by the platform of visitor information and read the IP address of the local computer by default, which can be edited.
Physical Information	The physical information of the computer used by the platform for registering visitor information is automatically filled in by default and cannot be edited.
Visitor Machine Type	By default, it is an ordinary computer. When connecting the visitor machine, select the visitor machine type: FaceKiosk.
Photo Collection	Select the type of camera installed by customers, which is divided into USB camera, webcam, and dual-camera altimeter. Description: The server side of the box does not currently support external "dual camera high camera".
Document Collection	Select the certificate collection equipment installed by customers, which is divided into USB camera, High-Speed Portable HD Doc Scanner,scanner and Dual Camera High-Speed Portable HD Doc Scanner. Description: The box server does not support external "altimeter, scanner and dual-camera altimeter" for the time being.

Parameter	Description
Default Permissions	Select the default access rights for visitors registered at this level of location.
Area Name	Add the name of the area to which the registration place belongs, and the visiting registration record of each registration place will be filtered according to the area of the registration place

Table 8- 14 Description of Entry Place Parameters

2.FaceKiosk

●Operating Steps:

Step 1: In the Visitor module, select **Basic Management > Entry Place**.

Step 2: In the registration location interface,click **New** and select **FaceKiosk** as the visitor machine type, as shown in figure below. Please refer to Table below for parameter description.

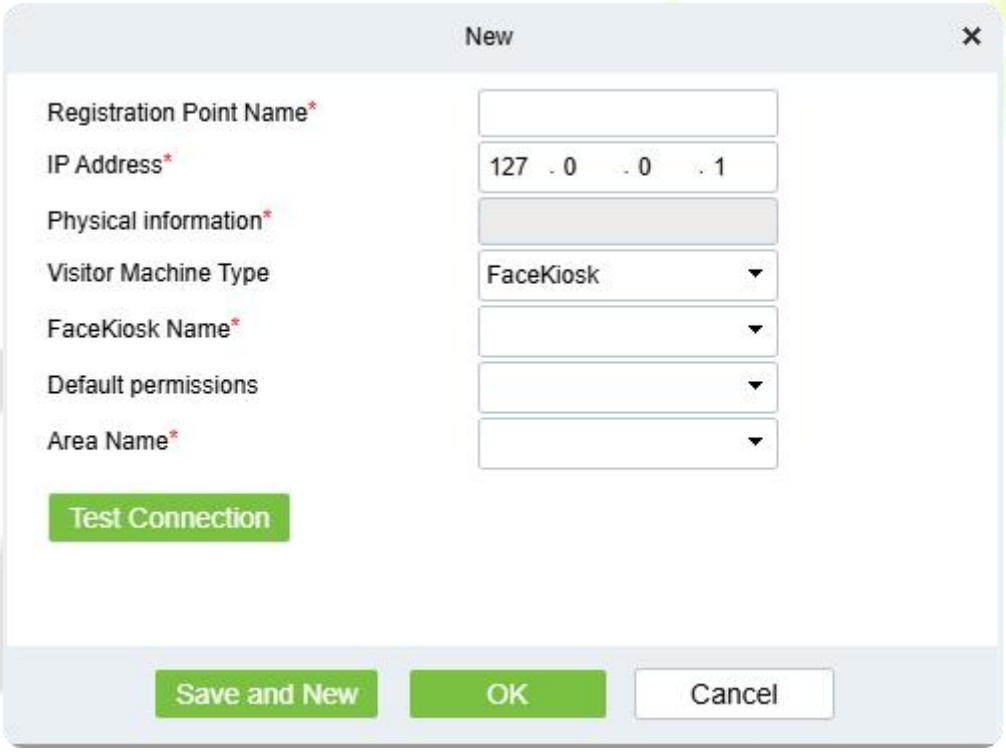


Figure 8- 75 Interface of Visiting Passenger Airline Entry Place

Parameter	Description
Registration Point Name	Any character, no more than 50, cannot repeat.
IP Address	Register the IP address of the computer used by the platform of visitor information and read the IP address of the local computer by default, which can be edited.
Physical Information	The physical information of the computer used by the platform for registering visitor information is automatically filled in by default and cannot be edited.

Parameter	Description
Visitor Machine Type	By default, it is an ordinary computer. When connecting the visitor machine, select the visitor machine type: FaceKiosk.
FaceKiosk Name	Select the name of the FaceKiosk.
Default Permissions	Select the default access rights for visitors registered at this level of location.
Area Name	Add the name of the area to which the registration place belongs, and the visiting registration record of each registration place will be filtered according to the area of the registration place

Table 8- 15 Description of Registration Location Parameters

8.5.8.2Delete

●Operation Steps:

Step 1: In the Visitor Module, click **Basic Management > Visitor Registration Point**, select the place name to be deleted.

Step 2: Click **Delete** to delete the selected place.

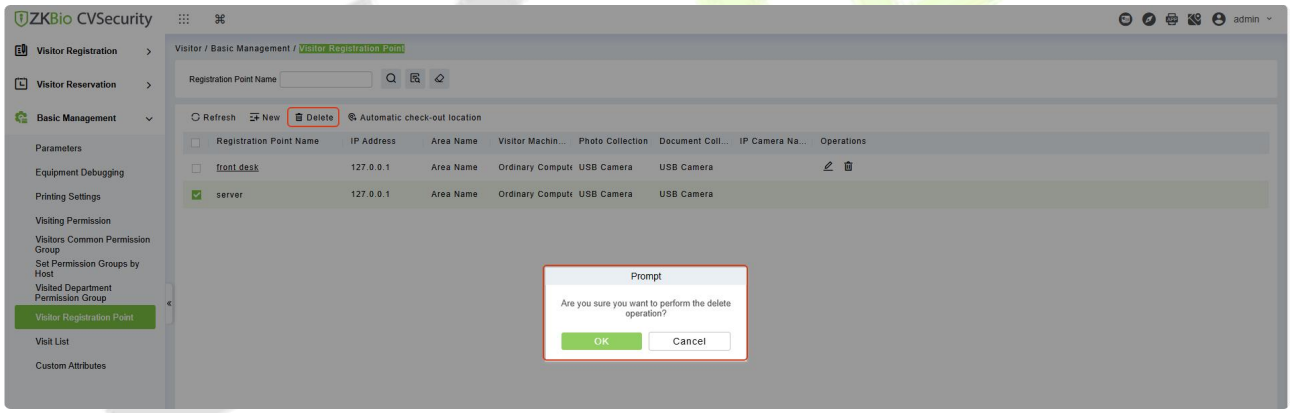


Figure 8- 76 Interface of Visiting Passenger Airline Entry Place

Step 3: Click **OK** to perform the delete operation.

8.5.8.3Automatic Check-out location

●Operation Steps:

Step 1: In the Visitor Module, click **Basic Management > Visitor Registration Point**, click **Automatic Check-out location**.

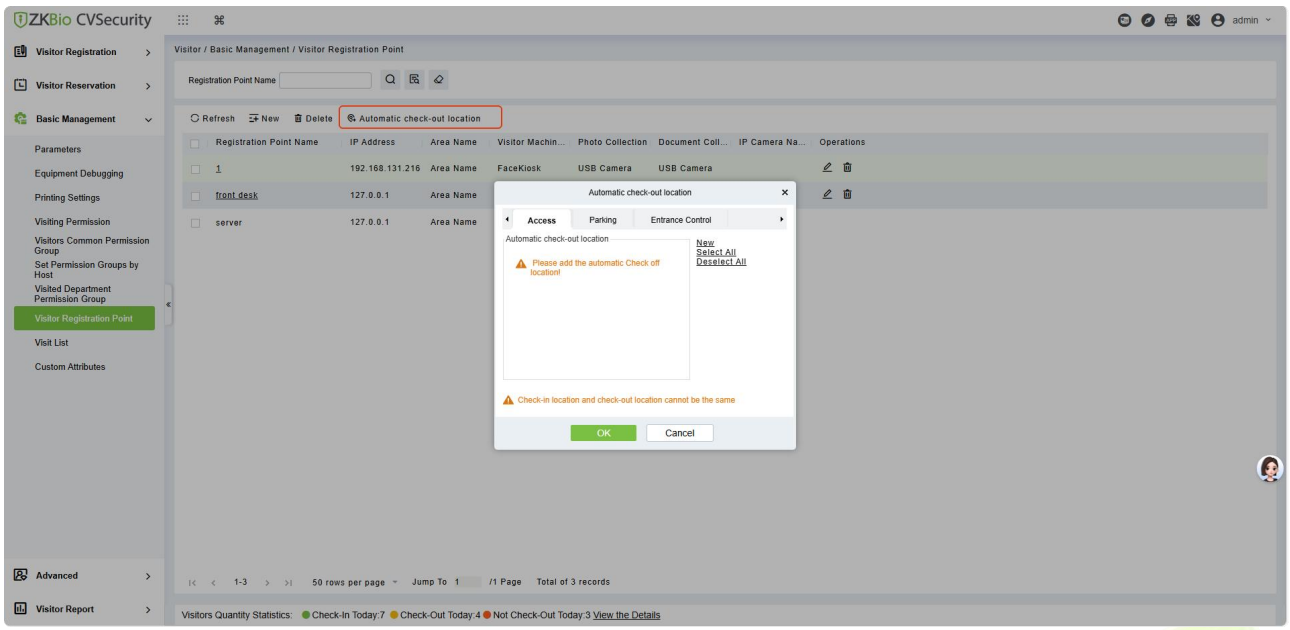


Figure 8- 77 Automatic Exit Place Interface

Step 2: Click **New** to add place as automatic check-out place and select the place reader name (Device place) from the appeared window. Click **OK** to save the data.

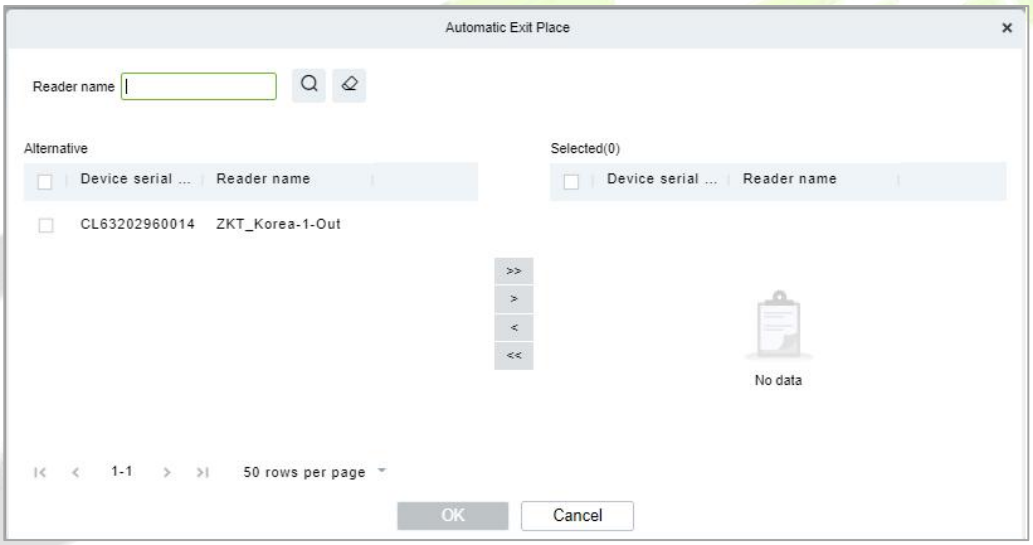


Figure 8- 78 Add Place as Automatic Exit Place

Step 3: Select the place to be set as automatic check-out place and click **OK**.

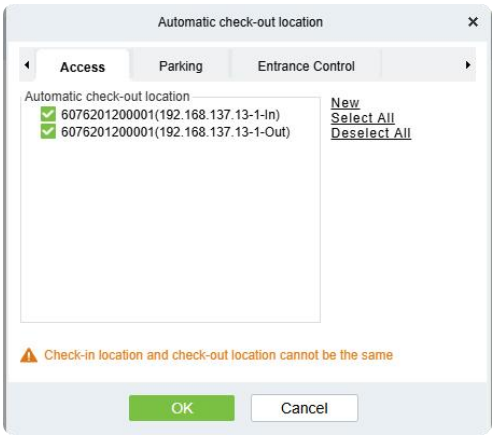


Figure 8- 79 Select Place as Automatic Exit Place

8.5.9Visit List

You can Add, Delete or Edit visit reason in this interface, so that you can select either from them at the entry registration page.

8.5.9.1New

● Operation Steps:

Step 1: In the Visitor module, click **Basic Management > Visit List> New**.

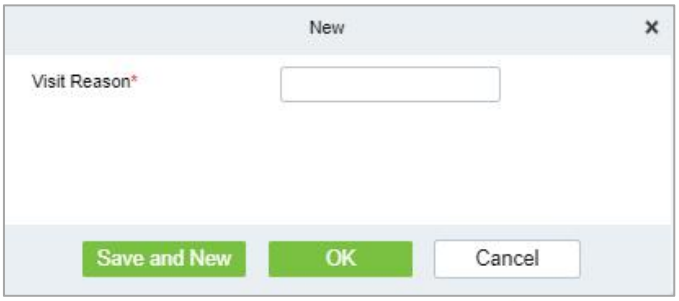


Figure 8- 80 Add Place as Automatic Exit Place

Step 2: Click **OK** to finish.

8.5.9.2Delete

● Operation Steps:

Step 1: In the **Visitor** module, click **Basic Management > Visit List**, select visit reason to be deleted.

Step 2: Click **Delete** to delete the selected visit reason.

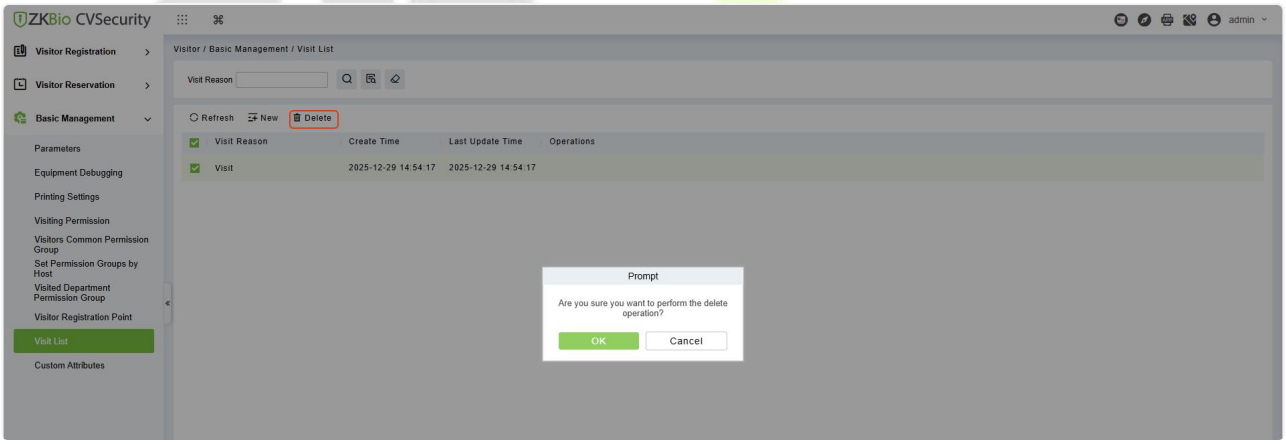


Figure 8- 81 Delete Visit Reason

Step 3: Click **OK** to perform the delete operation.

8.5.10Custom Attributes

If you want to add or delete a specific field on the registration page, then you can use this function.

8.5.10.1New

In this interface you can add any specific field on the registration page.

● Operation Steps:

Step 1: In the **Visitor Module**, click **Basic Management > Custom Attributes**, click **New** to add a specific field on the registration page.

Step 2: Enter the Attribute name, select the field type as Pull down, Multiple Choice, Single Choice or Text.

If you select any of the type except Text, then you have to mention the attribute value(s). Use a semicolon to separate the values. Enter Row and Column as required and choose Yes or No according with requirement.

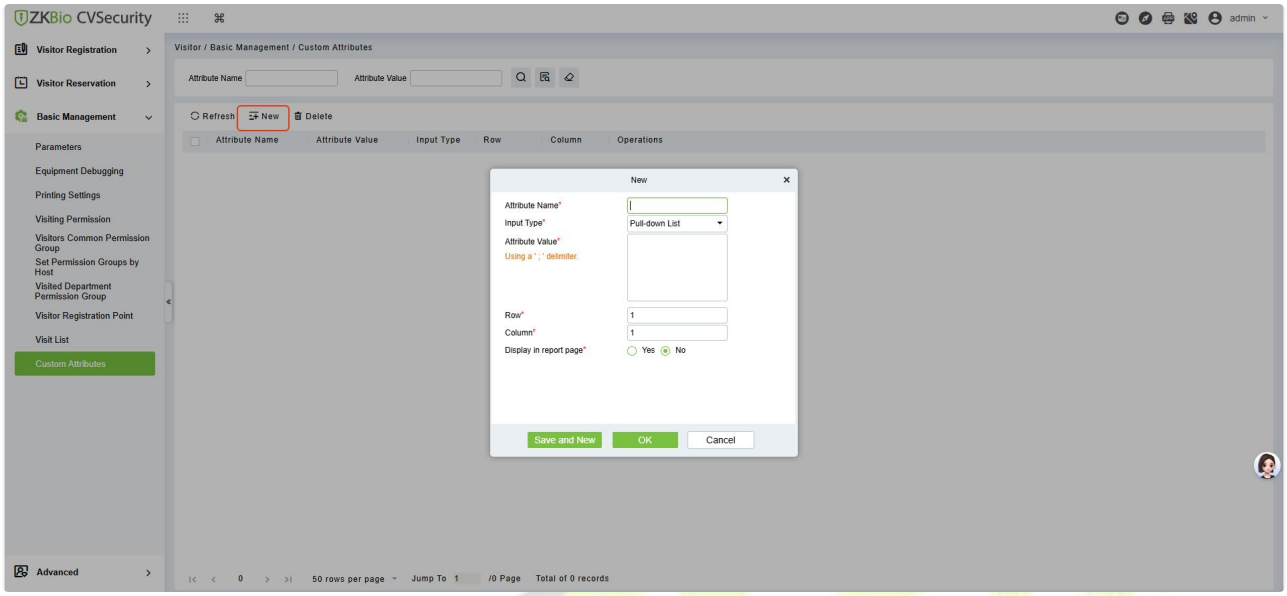


Figure 8- 82 Custom Attributes Interface

Step 3: Click **OK** to add the attribute.

Parameter	Description
Attribute Name	Enter the attribute name.
Input Type	Select the input type from the drop-down list such as Pull down, Multiple Choice, Single Choice or Text.
Attribute Value	Enter the attribute value. n attribute has multiple values, you can separate them with a semicolon. If you select text as input type of the attribute, then no need to add the attribute value.
Row	Enter the row number as required.
Column	Enter the column number as required.
Display in report page	If an attribute should be displayed on report pages, select **Yes**. Otherwise select **No.**

Table 8- 16 Description of Entry Place Parameters

8.5.10.2Delete Custom Attributes

To delete customized attributes.

● Operation Steps:

Step 1: In the **Visitor** module, click **Basic Management** > **Custom Attributes** and select the attribute to be deleted.

Step 2: Click **Delete** to delete a specific field on the registration page.

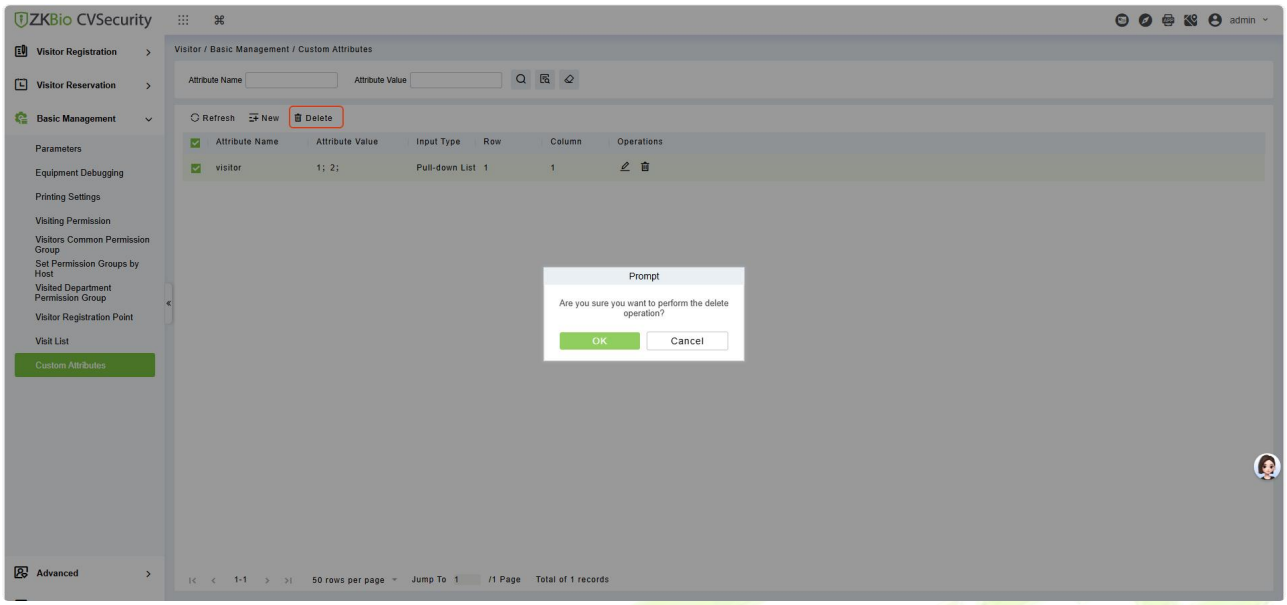


Figure 8- 83 To Delete Custom Attribute

Step 3: Click **OK** to perform the delete operation.

8.6 Advanced

8.6.1 Category

This interface allows you to add or delete the visitor category.

8.6.1.1 To Add New Visitor Category

● Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Category** and click **New** to add a new category.

Step 2: Enter the type of category and remarks as shown in figure below.

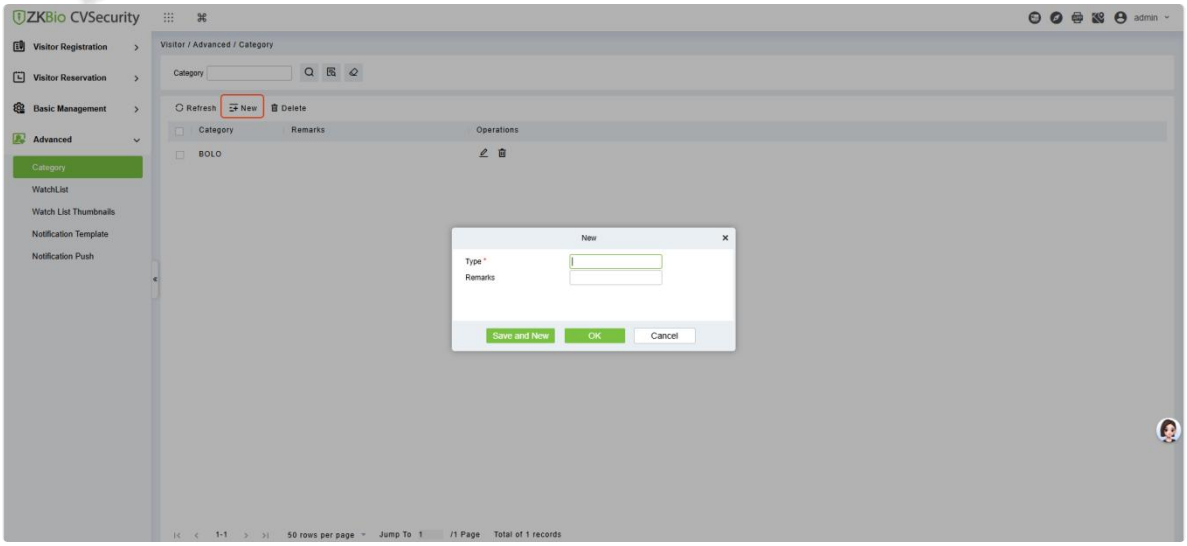


Figure 8- 84 Category Interface

Step 3: Click **OK** to save the data.

Parameter	Description
Type	Enter the type of category.
Remarks	Enter the remarks about the category (Optional).

Table 8- 17 Description of Category Parameters

8.6.1.2To Delete Category

● Operation Steps:

Step 1: In the **Visitor** module, click **Advanced > Category** and select the category to be deleted.

Step 2: Click **Delete** and then click **OK** to perform the delete operation.

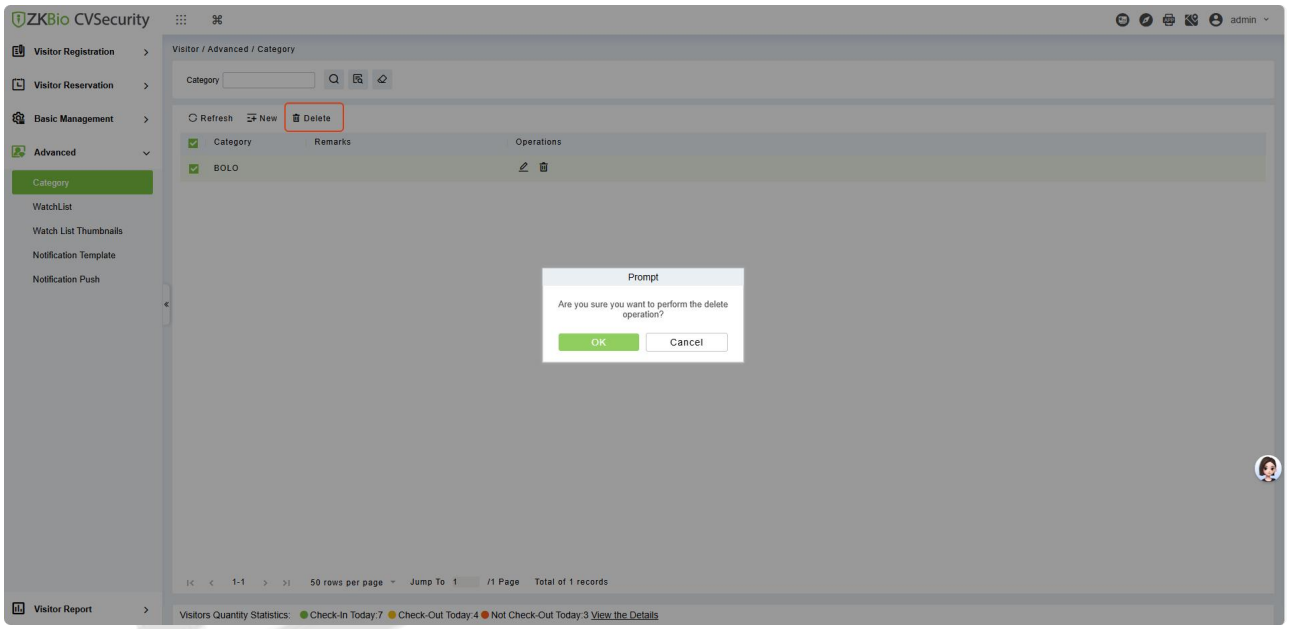


Figure 8- 85 To Delete Category

8.6.2WatchList

Watch List interface displays the list of visitor information, and you can Add, Delete, Enable, or Disable the visitors.

8.6.2.1New

Step 1: In the **Visitor** module, click **Advanced > WatchList** and click **New** to add visitor.

Step 2: Enter the Visitor details such as Type, Full Name, Category, Certificate Type and Certificate Number.

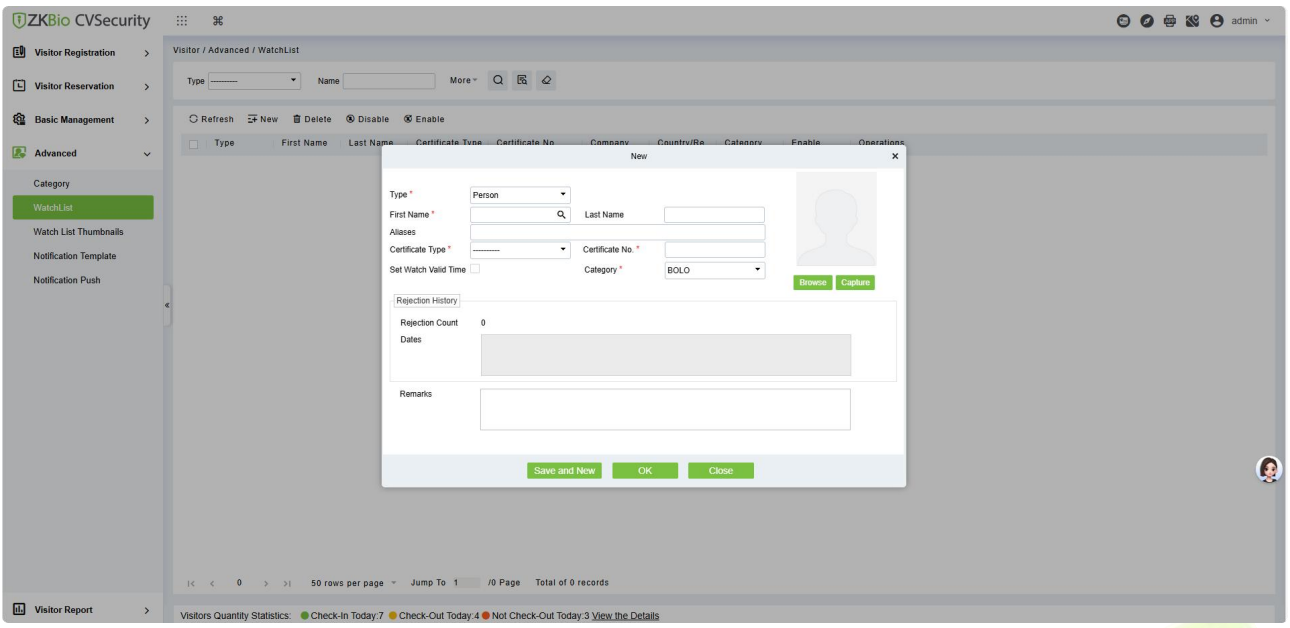


Figure 8- 86 Watchlist Interface

Step 3: Click **Save and New** to save the details.

Parameter	Description
Type	Select type from the drop-down list; Available types are Person, Company, Category/Country.
First and Last Name	Select visitor name using search icon. If you selected company as type, then enter the company name.
Aliases	You can enter the more familiar name of visitor if it needed.
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
Category	Select the visitor category from the drop-down list.
Set Watch Time	You can set watch time for the selected visitor by clicking on the check box. Then enter the Start Date and end Date.
Rejection counts and Dates	Displays how many times the business rejected the visitor and rejected dates.

Table 8- 18 Description of WatchList Parameters

8.6.2.2Delete WatchList

● Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **WatchList** and select the visitor watch list to be deleted.

Step 2: Click **Delete** to delete the selected watch list.

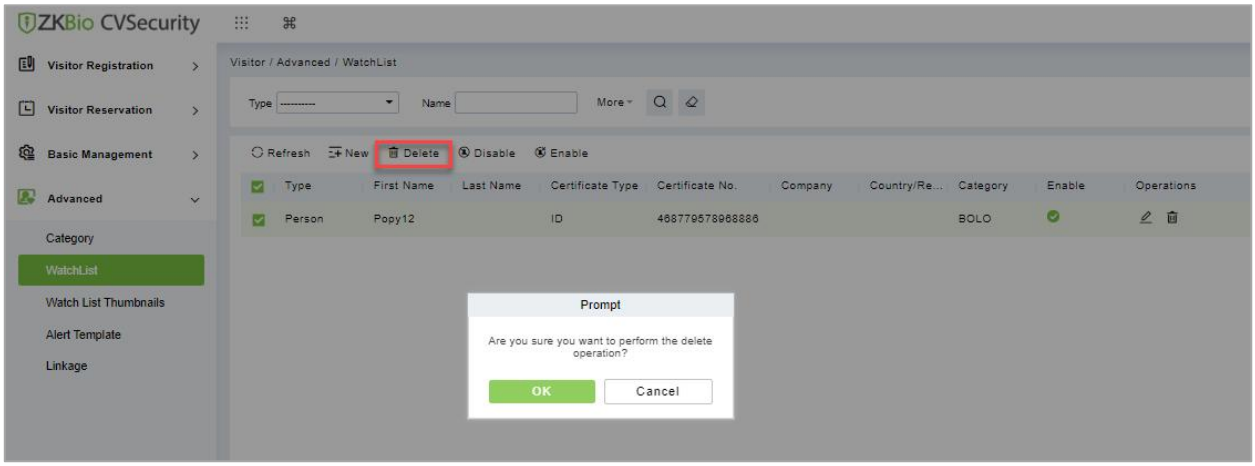


Figure 8- 87 To Delete WatchList

Step 3: Click **OK** to perform the delete operation.

8.6.2.3Enable WatchList

In **Visito**r module Click **WatchList** > **Advance**, select a blocked visitor, and click **Enable**.

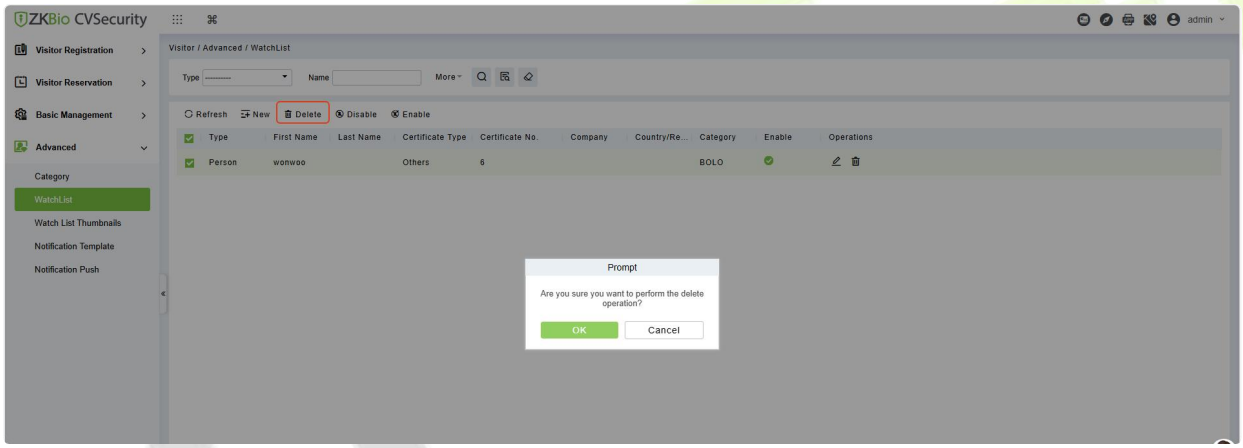


Figure 8- 88 Enabling WatchList

Click **OK** to enable the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor's Watch list is enabled.

8.6.2.4Disable WatchList

In **Visito**r module Click **WatchList** > **Advance**, select a visitor, and click **Disable**.

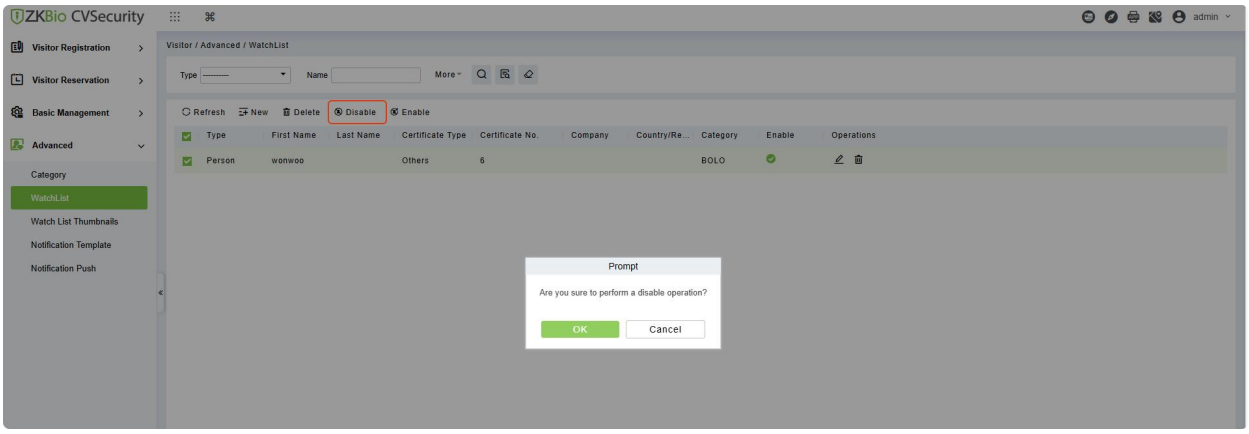


Figure 8- 89 Disabling WatchList

Click **OK** to block the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor's Watch list is blocked.

8.6.3Watch List Thumbnails

Displays the thumbnail of watchlist person's image.

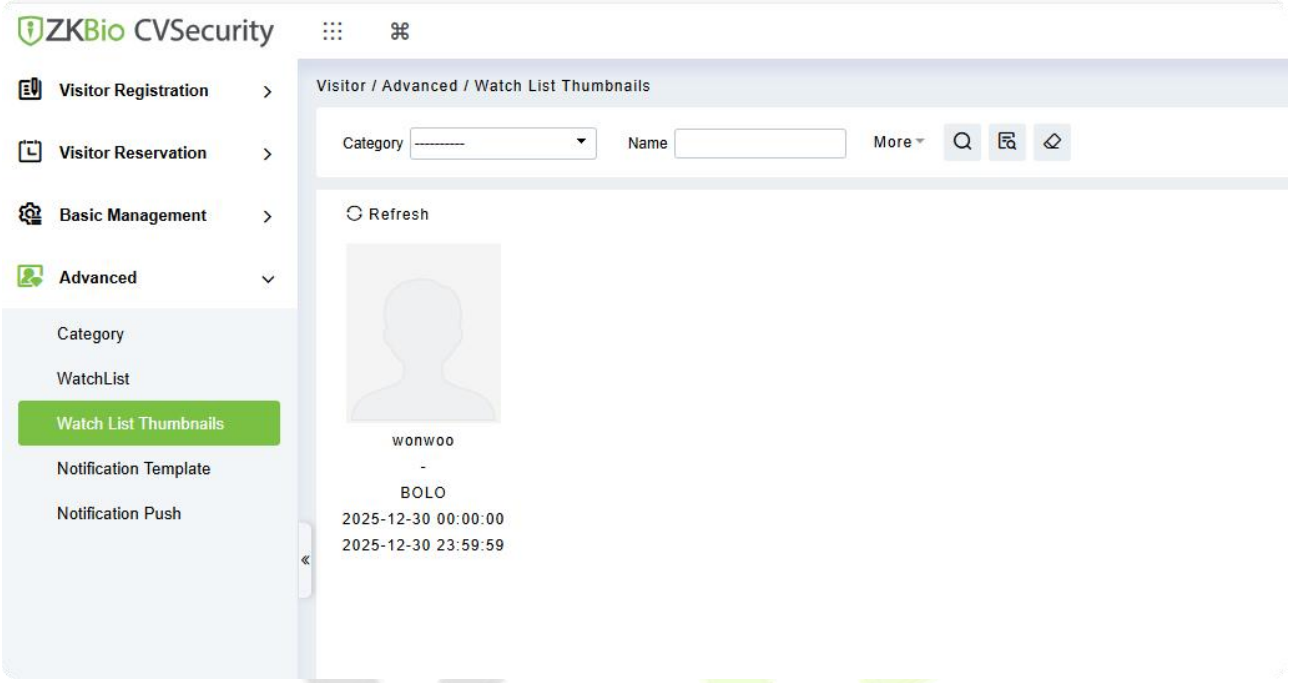


Figure 8- 90 WatchList Thumbnails Interface

8.6.4Notification Template

This feature can add, edit the message templates. Different events have different template types. When a visitor reserved, checked in, checked out, reserved timeout, and visited timeout, the system will alert the visitor and the host via email or SMS.

8.6.4.1To Add Alert Template (New)

● Operation Steps:

Step 1: In the **Visitor** module, click **Advanced > Alert Template** and click **New** to add Alert Template.

Step 2: Enter the Details such as Template Name, Template Type, Event Type and Visitor Information.

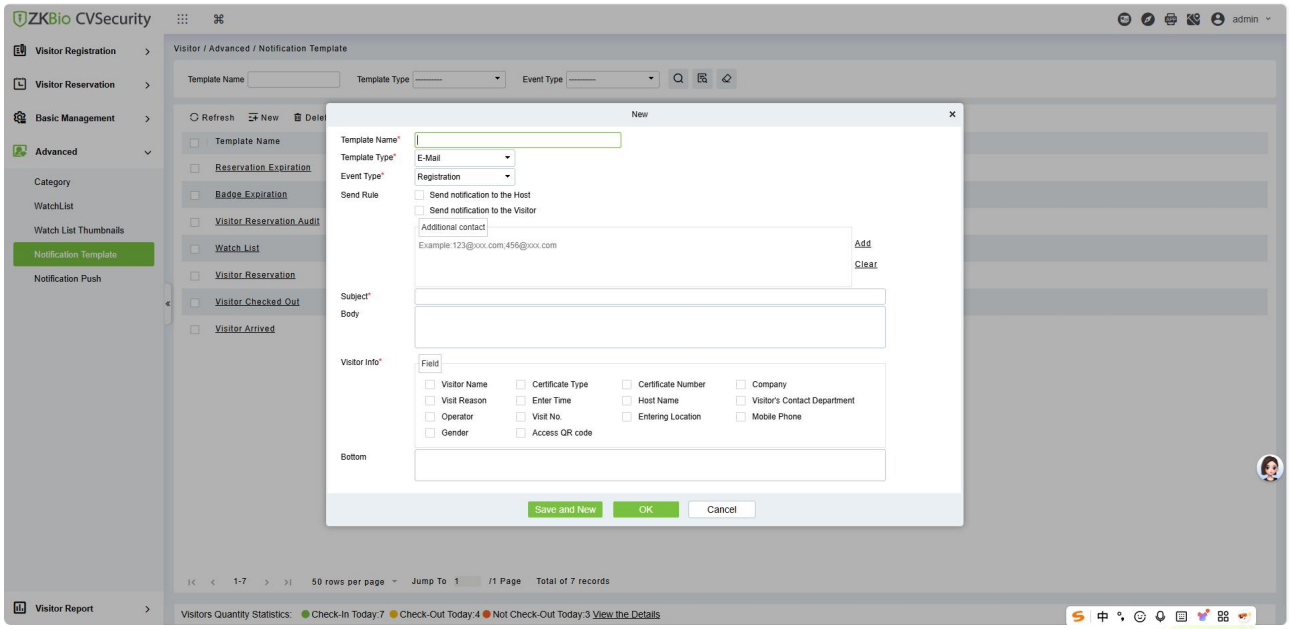


Figure 8- 91 Alert Template Interface

Step 3: Click **Save** and New to save the alert template.

Parameter	Description
Template Name	Enter the Template Name
Template Type	Select template type such as E-mail or SMS.
Event Type	Select the event type from the drop-down list such as Registration, Reservation, Check-out, Watch List etc.
Send Rule	You can set the send rule by clicking on check boxes. By using this option admin can send notification to the Host as well as visitor about the events (like Registration, Check Out Timing, etc.). Admin can add additional Email in Additional Contact column.
Subject And Body	Enter the template's subject and message to send to the host or visitor.
Visitor Info	Admin can add visitor information like Visitor Name, Visit Reason, Certificate Type etc. by clicking on the check boxes.

Table 8- 19 Description of Alert Template Parameters

8.6.4.2Delete Alert Template

● Operation Steps:

Step 1: In the **Visitor Module,** click **Advanced > Alert Template** and select the template to be deleted.

Step 2: Click **Delete** to delete the selected template.

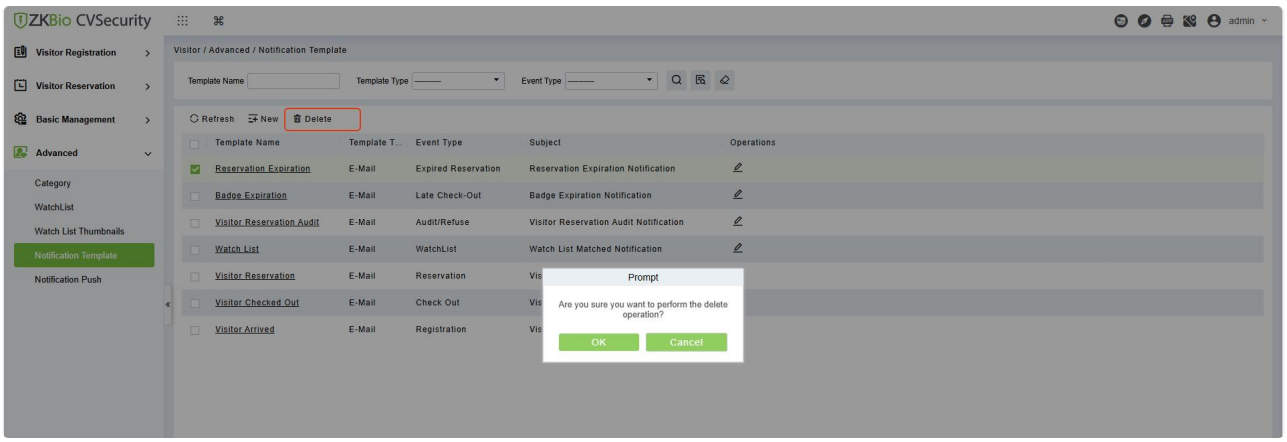


Figure 8- 92 To Delete Alert Template

Step 3: Click **OK** to perform the delete operation.

8.6.5Notification Push

This feature allows you to create a linkage function for each event. You can select the event, entrance and the Email template.

8.6.5.1New

●Operation Steps:

Step 1: In the **Visitor** module, click **Advanced > Notification Push** and click **New** to add linkage.

Step 2: Enter Linkage name and select Entrance, SMS Template and E-mail Template.

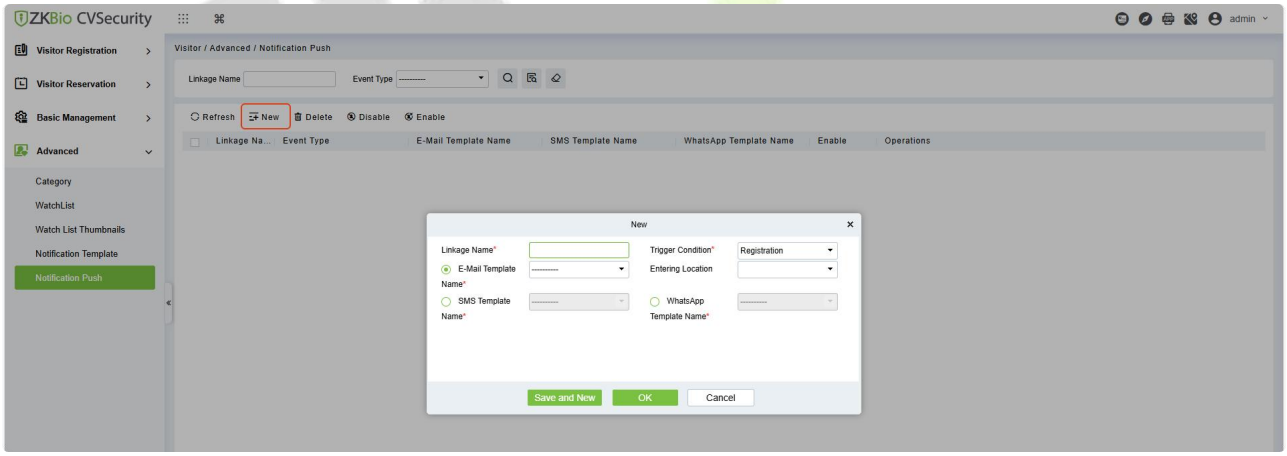


Figure 8- 93 Linkage Interface

Step 3: Click **Save and New** to save the details.

Parameter	Description
Linkage Name	Enter the Linkage Name.
Trigger Condition	Select trigger condition such as registration, reservation, check out etc.
Email Template	Select E-mail template from drop-down list.

Parameter	Description
SMS Template	Select SMS template from drop-down list.
Entrance	Select the Entry place.

Table 8- 20 Description of Linkage Parameters

8.6.5.2Delete

● Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Notification Push** and select the linkage to be deleted.

Step 2: Click **Delete** to delete the selected linkage.

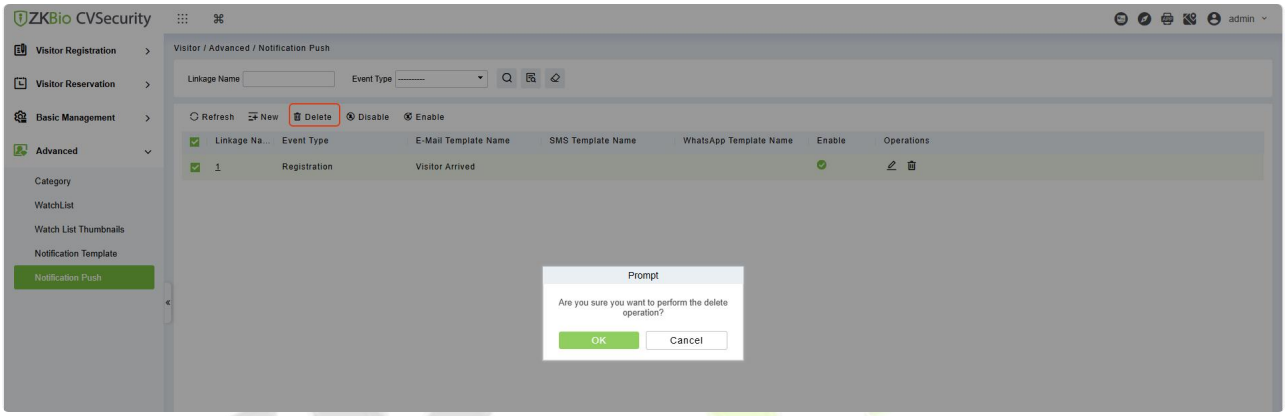


Figure 8- 94 To Delete Linkage

Step 3: Click **OK** to perform the delete operation.

8.6.5.3Enable

In the **Visitor** module, click **Advanced** > **Notification Push**, select a blocked Linkage to enable that, and click **Enable**.

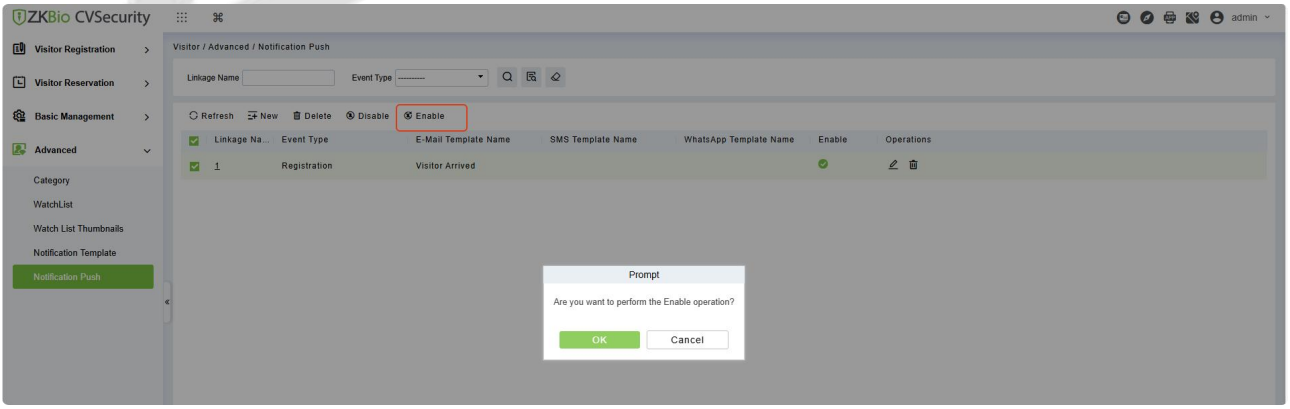


Figure 8- 95 Enabling Linkage

Click **OK** to enable the linkage. The enable entry for the corresponding selected linkage will show indicates the linkage is enabled.

8.6.5.4Disable

In the **Visitor** module, click **Advanced** > **Notification Push**, select linkage to be disable, and click **Disable**.

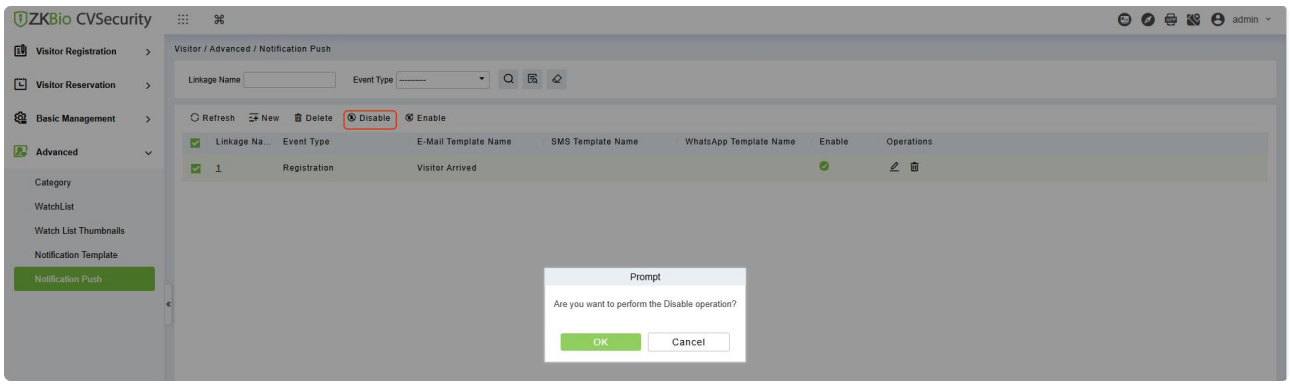


Figure 8- 96 Disabling Linkage

Click **OK** to block the linkage. The enable entry for the corresponding selected linkage will show indicates the linkage is blocked.

8.7 Visitor Report

8.7.1 Visitor's Last Accessed Location

In the **Visitor** module, click **Reports** > **Last Visited Location** to view the reports. The reports can be filtered by different conditions.

You can export the data into an Excel, PDF, CSV or TXT. See the following figure by clicking **Export** option.

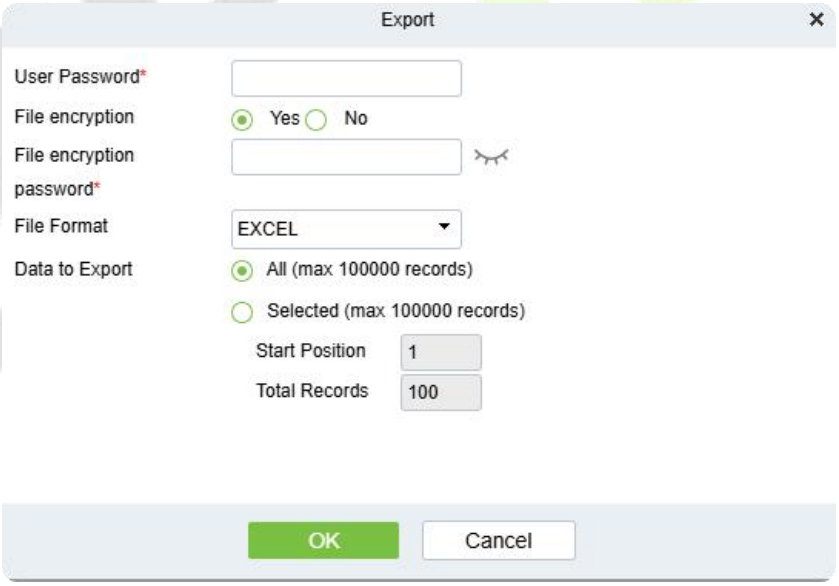


Figure 8- 97 Export Option

Select file format and data to be export, then click **OK**.

Last Visited Location

Visitor Code	First Name	Last Name	Event Date	Enter Time	Event Point	Event Description	Reader Name	Verification Mode	Area	Stay Time
800000020	usuop	sss	2022-07-27 09:42:13	2022-07-27 09:41:24	10.10.20.73-1	Normal Verify Open	10.10.20.73-1-In	Only Pin	Area Name	00:00:48

Figure 8- 98 Last Visited Location Record

8.7.2 Visiting Record

In the **Visitor Module,** click **Reports** > **Visitor History Record** to view the reports. The reports can be filtered by different conditions.

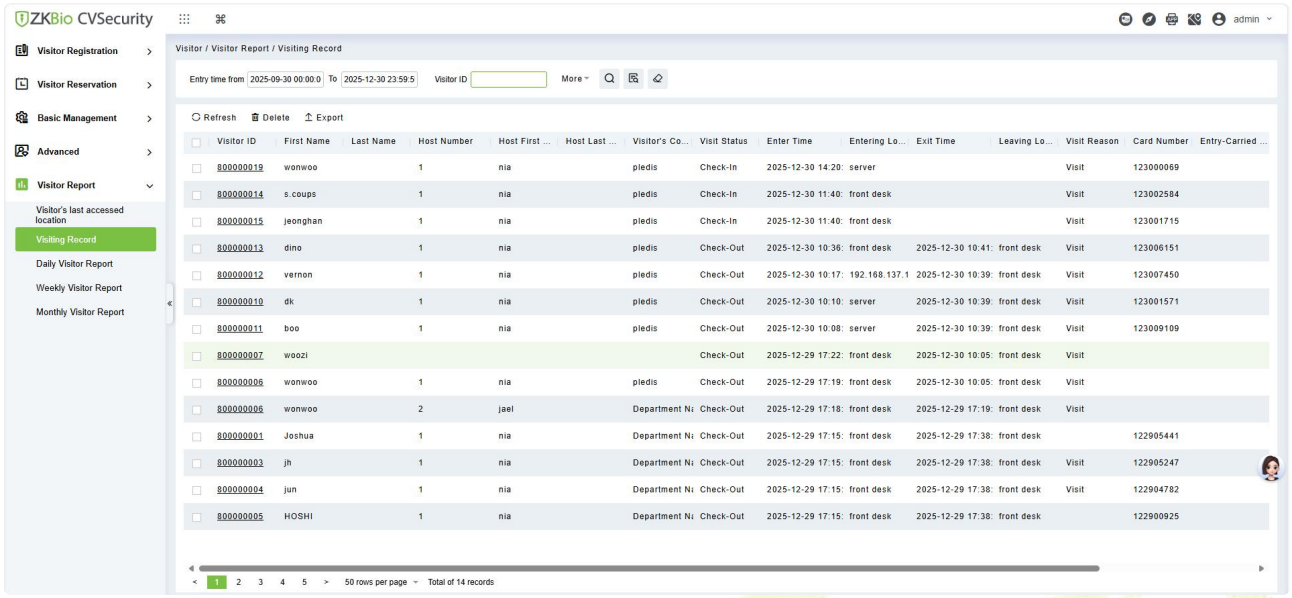


Figure 8- 99 Visitor History Record Interface

8.7.2.1 Export

You can export the records into an Excel, PDF, or CSV file. See the following figure by clicking **Export**.

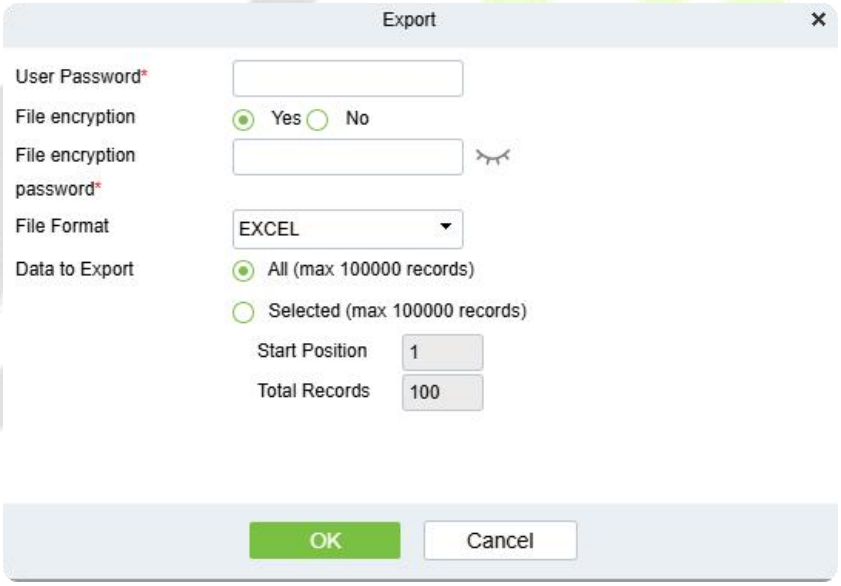
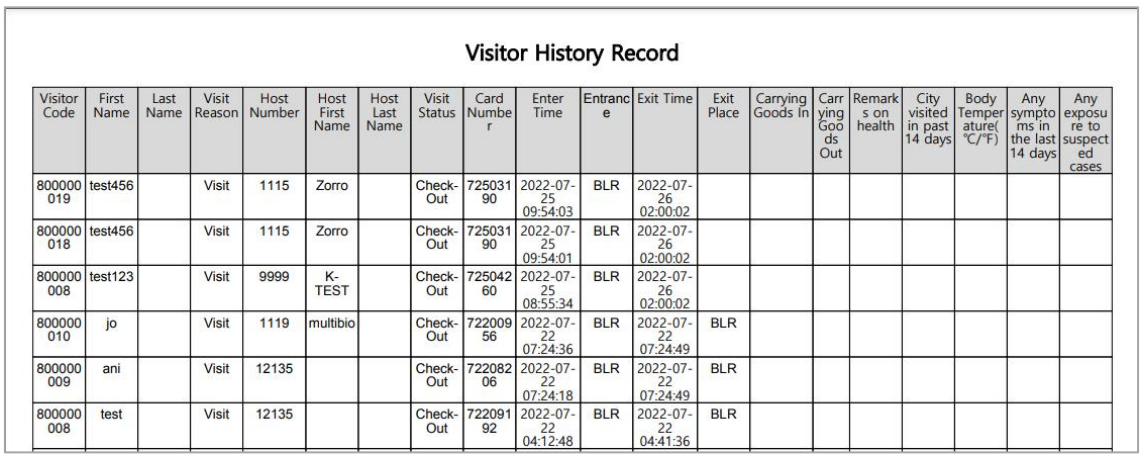


Figure 8- 100 Export Option

Select file format and data to be export, then click **OK**.



Visitor History Record

Visitor Code	First Name	Last Name	Visit Reason	Host Number	Host First Name	Host Last Name	Visit Status	Card Number	Enter Time	Entrance	Exit Time	Exit Place	Carrying Goods In	Carrying Goods Out	Remarks on health	City visited in past 14 days	Body Temperature(℃/℉)	Any symptoms in the last 14 days	Any exposure to suspected cases
800000019	test456		Visit	1115	Zorro		Check-Out	72503190	2022-07-25 09:54:03	BLR	2022-07-26 02:00:02								
800000018	test456		Visit	1115	Zorro		Check-Out	72503190	2022-07-25 09:54:01	BLR	2022-07-26 02:00:02								
800000008	test123		Visit	9999	K-TEST		Check-Out	72504260	2022-07-25 08:55:34	BLR	2022-07-26 02:00:02								
800000010	jo		Visit	1119	multibio		Check-Out	72200956	2022-07-22 07:24:36	BLR	2022-07-22 07:24:49	BLR							
800000009	ani		Visit	12135			Check-Out	72208206	2022-07-22 07:24:18	BLR	2022-07-22 07:24:49	BLR							
800000008	test		Visit	12135			Check-Out	72209192	2022-07-22 04:12:48	BLR	2022-07-22 04:41:36	BLR							

Figure 8- 101 Visitor History Record

8.7.2.2Delete Visitor History

● Operation Steps:

Step 1: In the **Visitor** module, click **Reports > Visitor History Record** and select the visitor's history to be deleted.

Step 2: Click **Delete** to delete the visitor history.

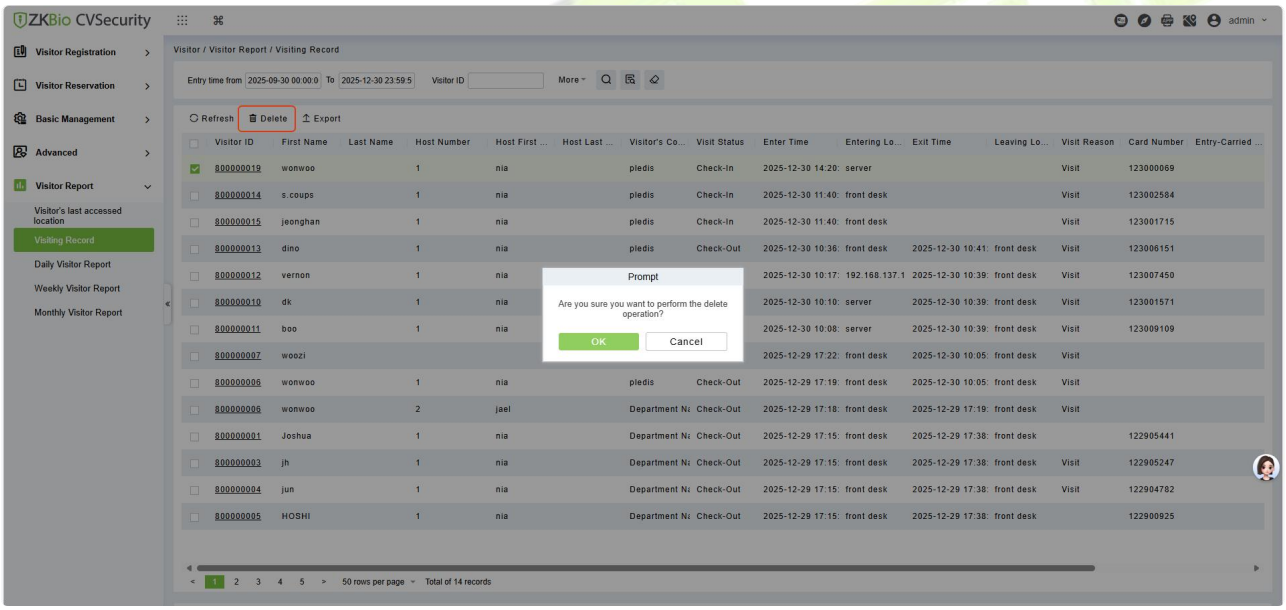


Figure 8- 102 To Delete Alert Template

Step 3: Click **OK** to perform the delete operation.

8.7.3Daily Visitor Report

View and export today's visitor visit history.

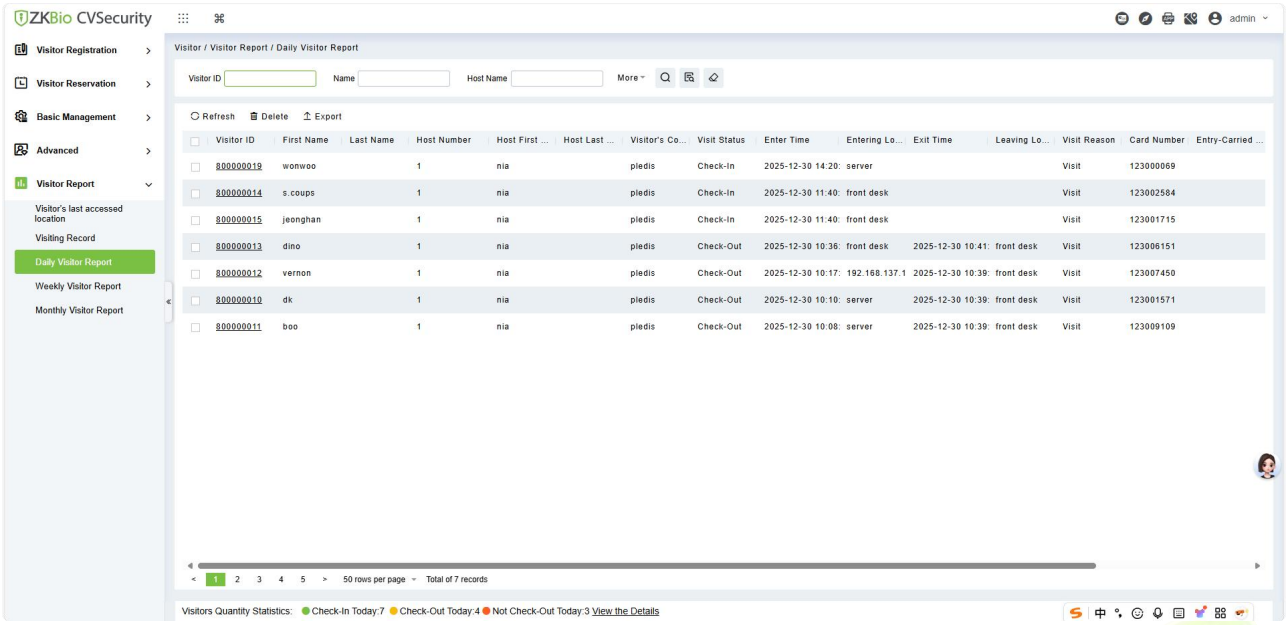


Figure 8- 103 Daily Visitor Report

8.7.4Weekly Visitor Report

View and export this week's visitor visit history.

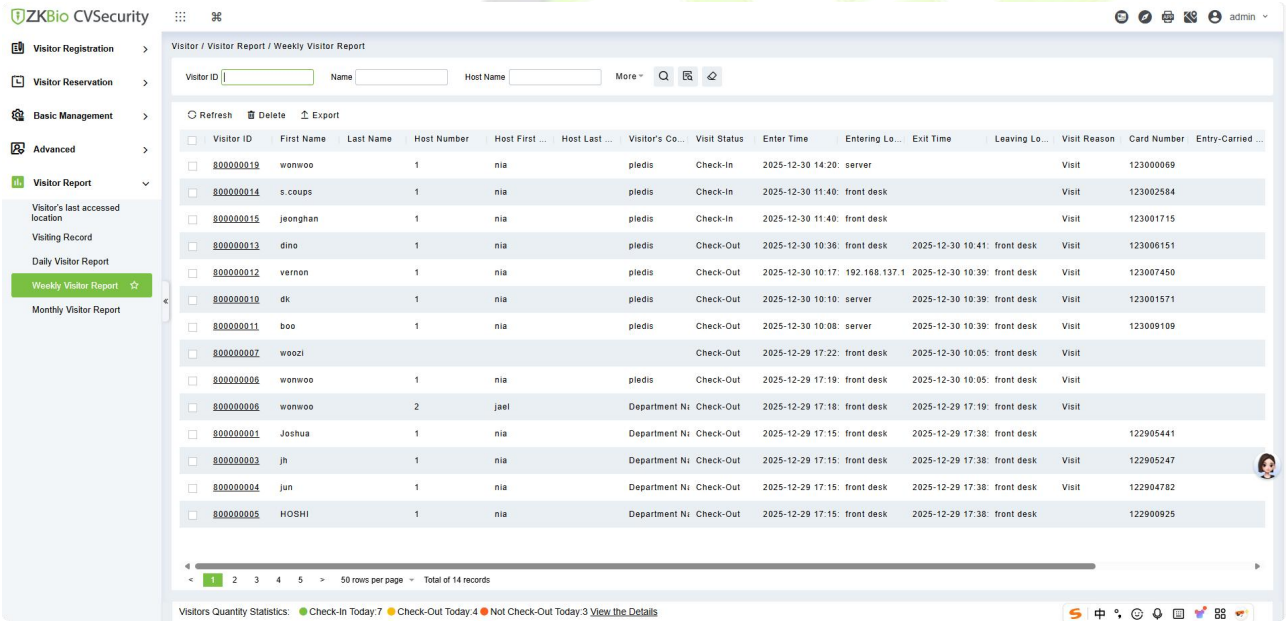


Figure 8- 104 Weekly Visitor Report

8.7.5Monthly Visitor Report

View and export this monthly's visitor visit history.

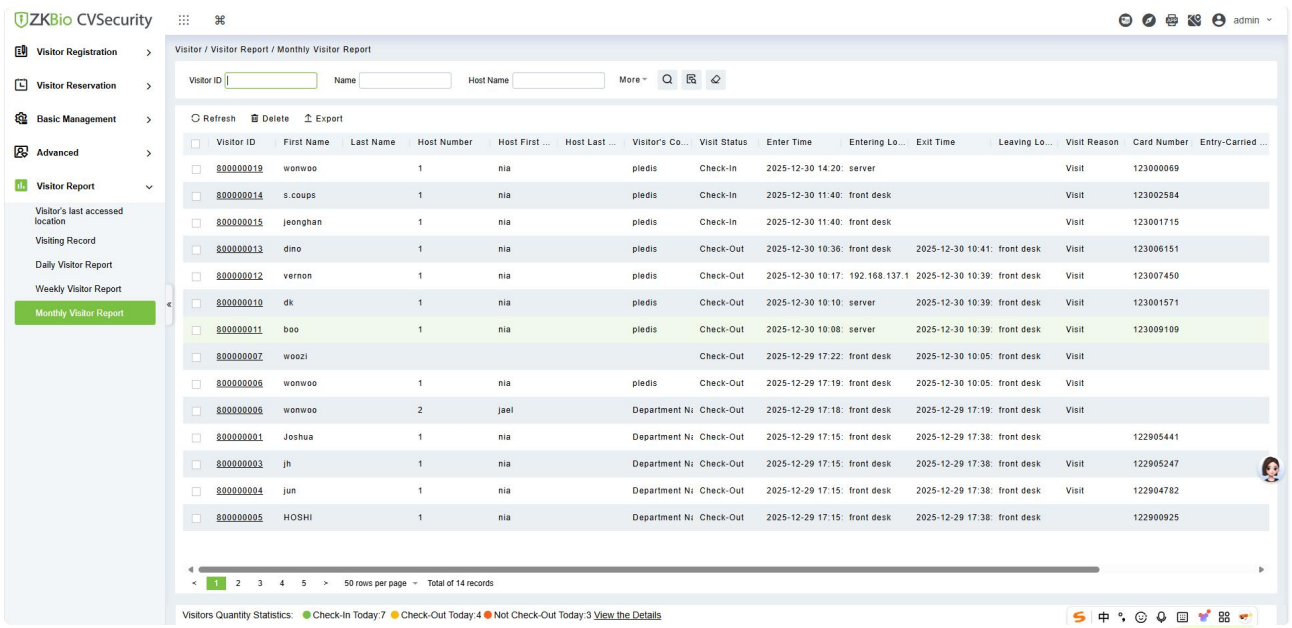


Figure 8- 105 Monthly Visitor Report

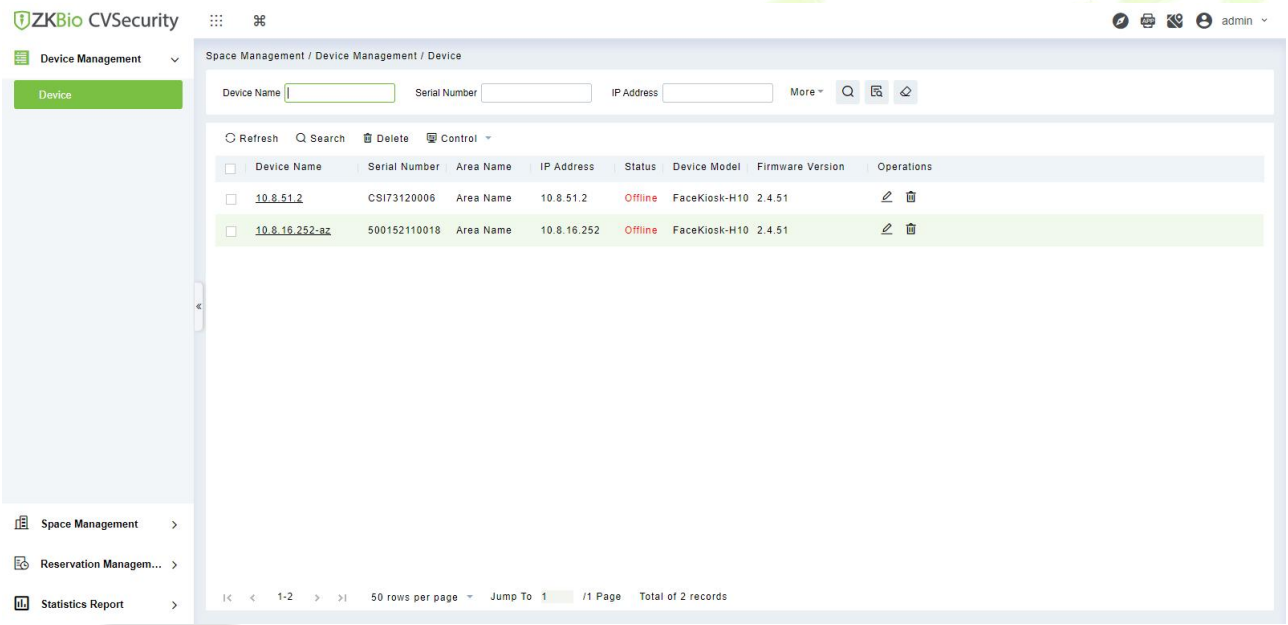
9 Space Management

The ZKBio CVSecurity Space Management Module is a comprehensive space management platform designed to help users efficiently manage space resources, including meeting rooms, Rest rooms, rehearsal rooms, etc.Through this module, users can manage devices, manage spaces, manage reservations, and view statistical reports, as well as make space reservations and manage them through the APP.

The ZKBio CVSecurity Space Management Module is a comprehensive platform for efficiently managing space resources, such as meeting rooms, restrooms, and rehearsal spaces. It allows users to manage devices, spaces, reservations, and view reports, as well as make and manage reservations via the app.

9.1 Device Management

The Device Management module allows user can manage devices effectively.



9.1.1 Search and Add Device

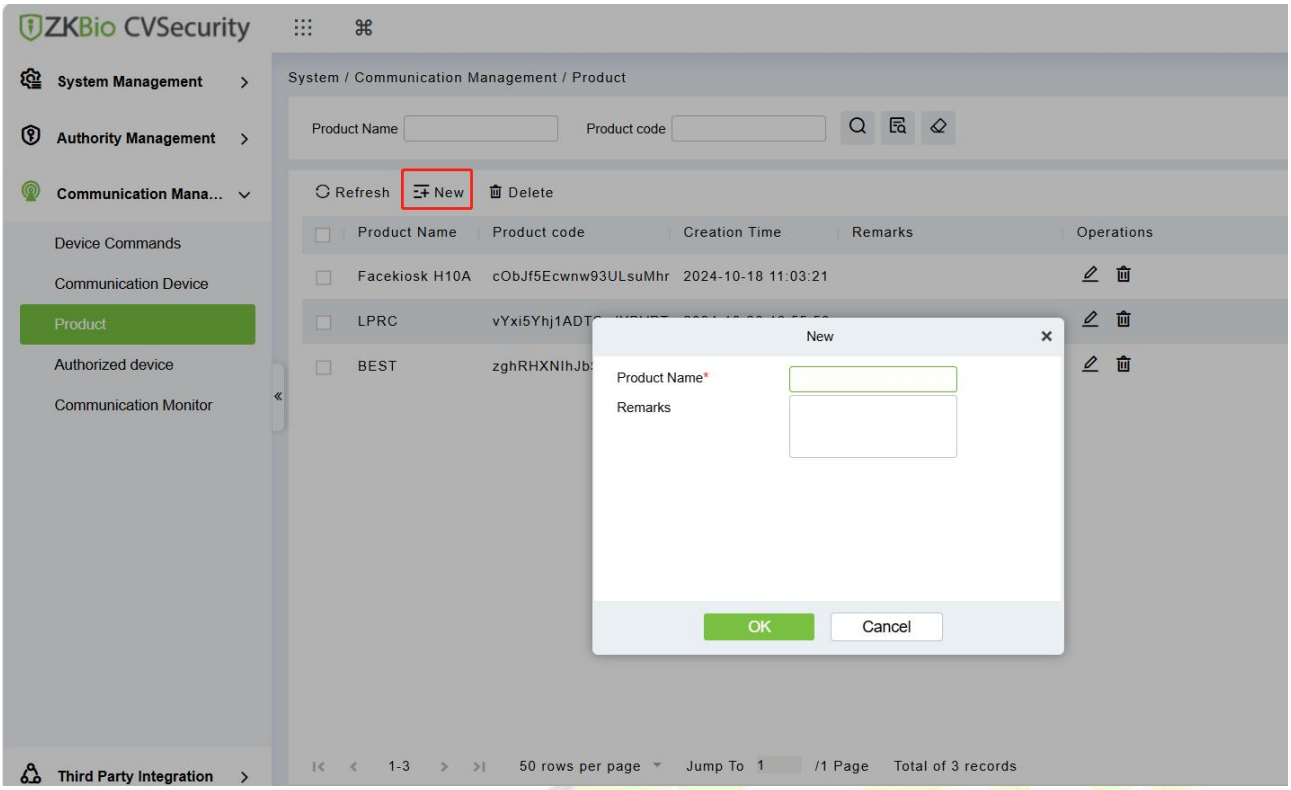
The module enables the search and registration of Facekiosk-H10A devices.

Prerequisites:

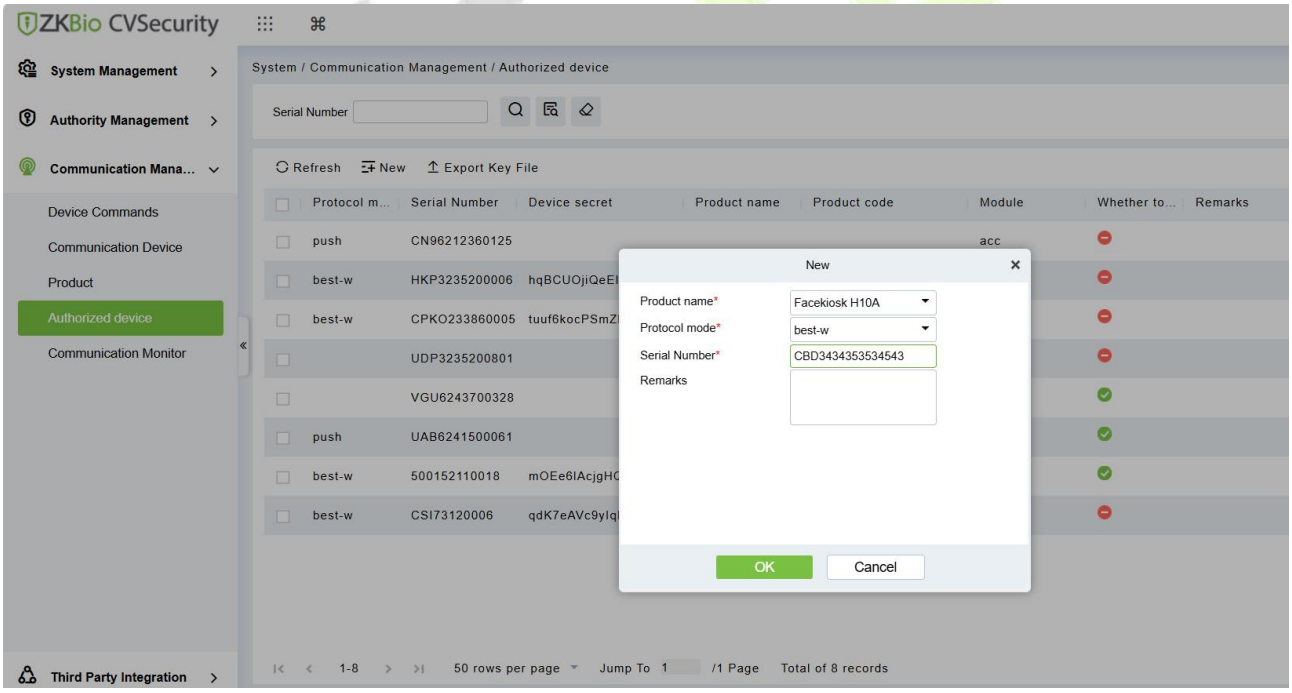
1) Facekiosk-H10A devices. (Device version requirement: ZKBio Meet Version 2.4.51 or higher)

2) **Device Authorization**: Before use, user must authorize the Facekiosk-H10A device. Follow these steps to complete the authorization process:

Step 1: Click on **System -> Communication Management -> Product menu** and click **New** to add a new product type, you can customize the product name.



Step2: Click on System -> Communication Management -> Authorized Device ,and click New to authorized device.



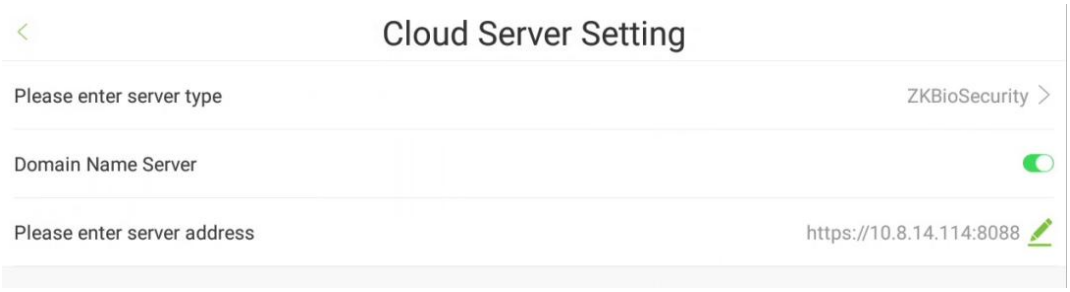
Enter the required information and then click **OK** to finish authorizing the device.

Product Name: Select the product type you have defined.

Product Mode: Choose BEST-W.

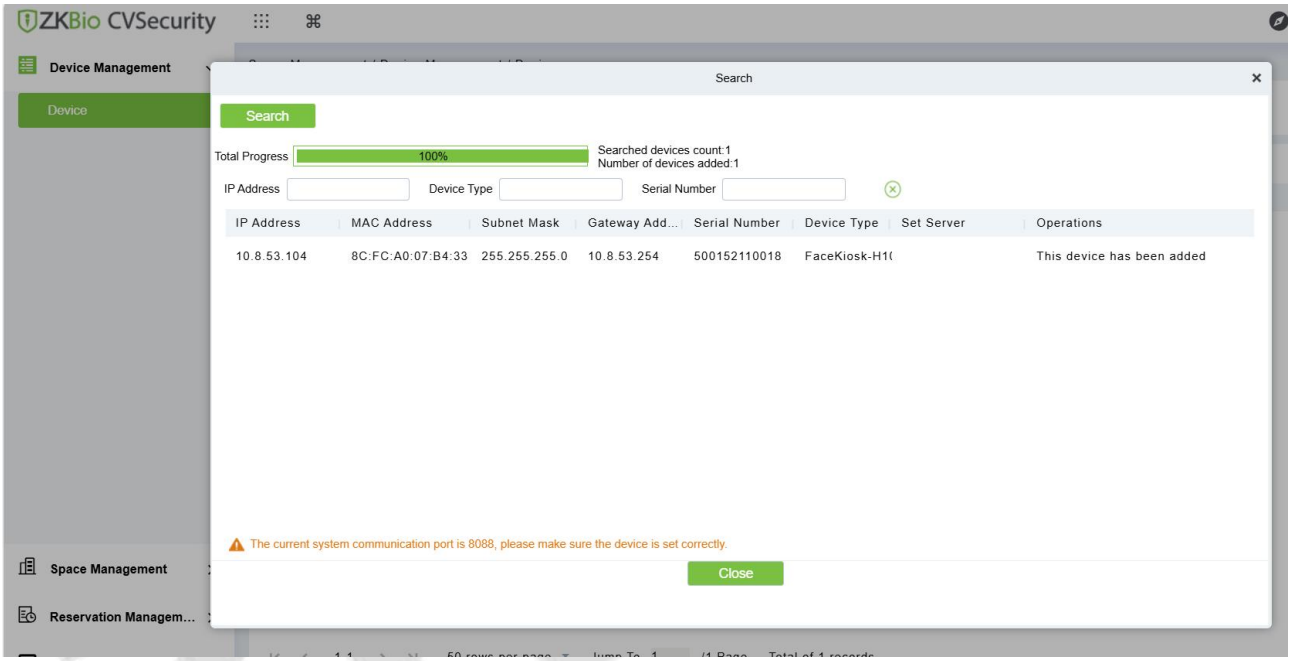
Serial Number: Enter the serial number of the device.

Step 3: For Facekiosk H10A, go to **Communication Setting -> Cloud Server Setting** to configure the ZKBio CVSecurity server address. Please ensure that the **Domain Name** is enabled, and then enter the correct ZKBio CVSecurity server address in the format shown in the figure below.



Once the Once the prerequisites are met, you can proceed to search for and add devices.

Go to **Space Management -> Device Management -> Device**, click Search, and after the search, click Add Device to add the device to your system.



9.1.2Delete

Click to delete the device.

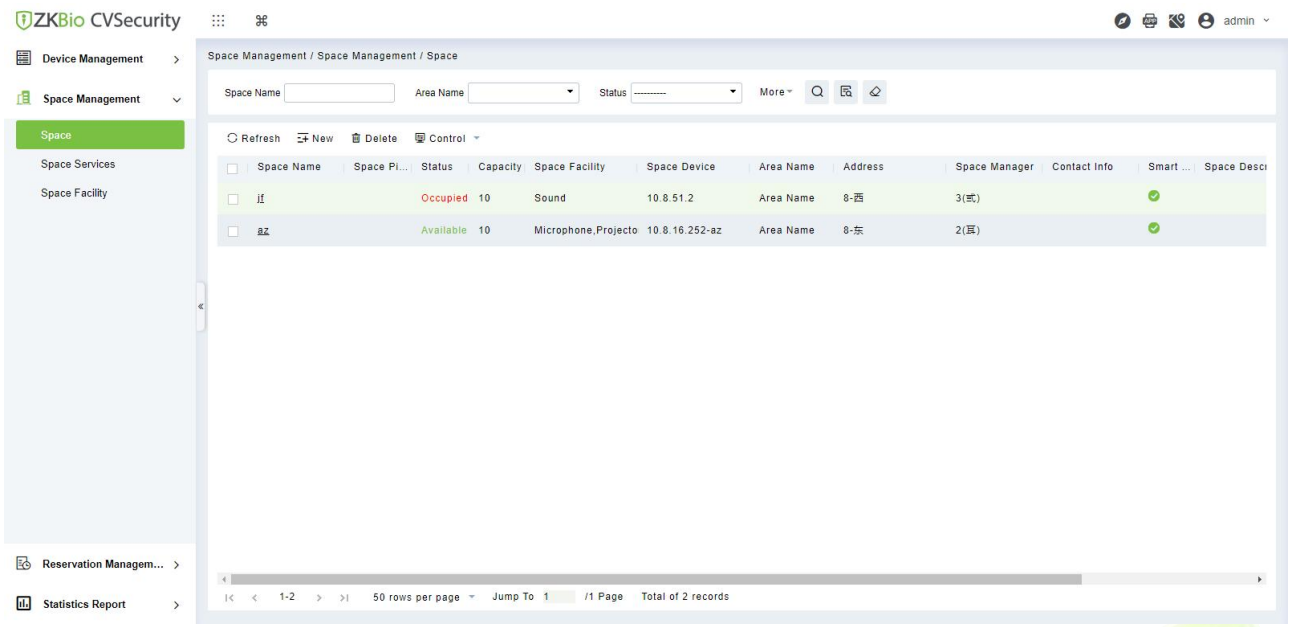
9.1.3Control

Includes operations such as Synchronize Time, Reboot Device, and Clear Information.

9.2 Space Management

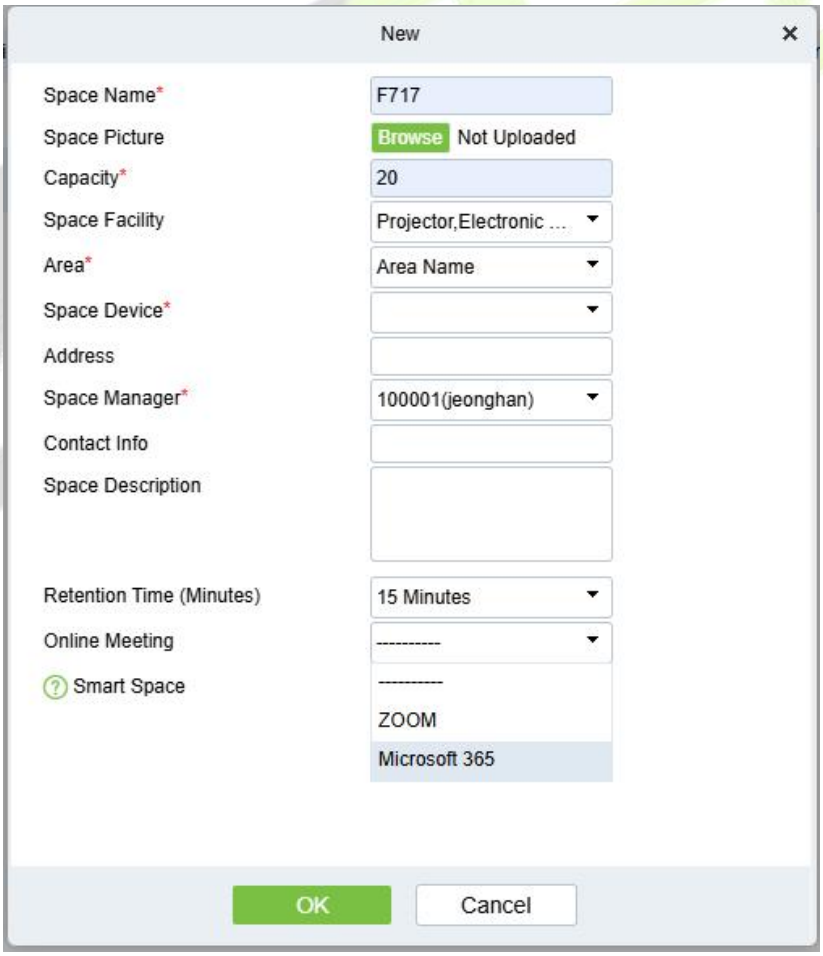
9.2.1Space

Click on the **Space Management > Space** , you can start creating spaces and space usage rules.



9.2.1.1 Add Space

Click **[Space Management]** > **[Space]** > **[+New]** to add new devices to the Space Management Module.

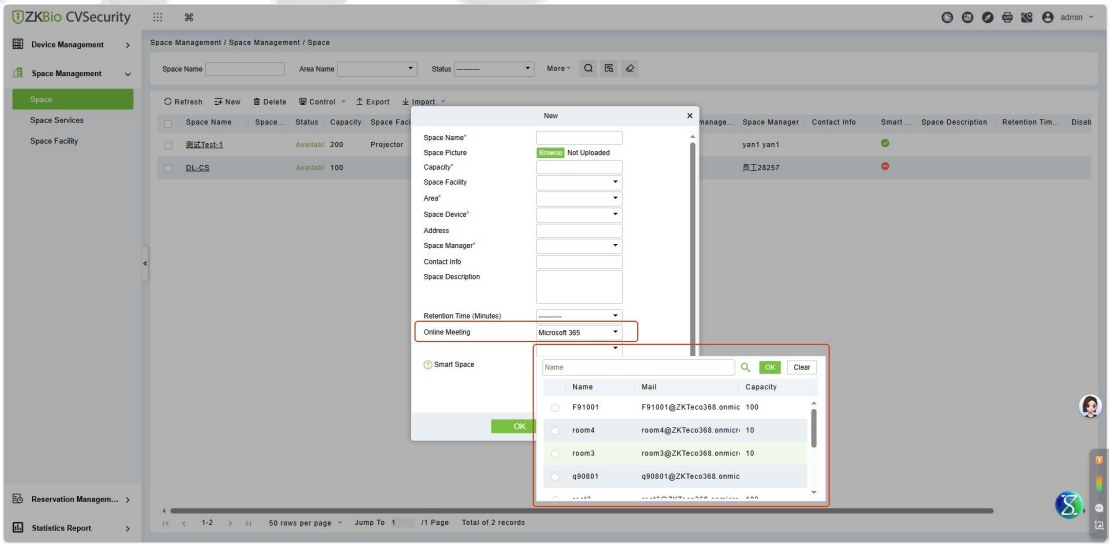


Fields are as follows:

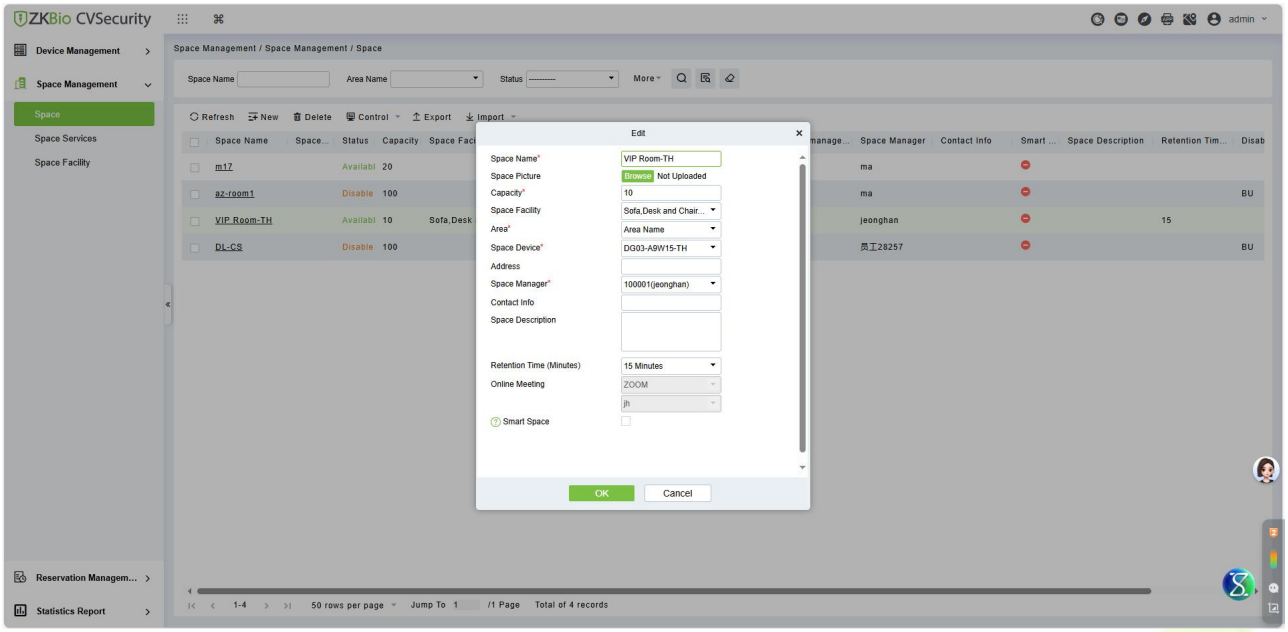
Parameter	Description
Space Name	Enter the name of the Space

Parameter	Description
Space Picture	Upload the Image of the Space
Capacity	Define the capacity of the space to indicate the number of people it can accommodate, facilitating filtering during the reservation process.
Space Facility	List the amenities available in the space to provide information that can aid in the reservation process.
Area	Choose the area, as the area is linked to the space.
Space Device	Select the device to be associated with the space within the space management module.
Address	Address of the Space
Space Manager	Person in Charge of the Space
Contact Info	Fill in the contact information of the space manager.
Space Description	Description of the Space
Retention Time (Minutes)	Reservation Retention Time; for example, if a meeting is scheduled from 9:00-12:00 and the retention period is set to 30 minutes, the system will automatically end the meeting if no one checks in after 9:30.
Online Meeting	You can select Zoom or Microsoft 365 as the online meeting resource.
Smart Space	You can choose whether to enable Smart Spaces, which can be used for quick filtering during the reservation process.

- If you choose Microsoft 365 for the online meeting, bind the virtual meeting room resource to the physical meeting room space based on the synchronized content. When you select one of the virtual meeting room resources, the system will automatically synchronize and fill in basic information such as the space name, meeting room email, and capacity.For detailed configuration, please refer to System / Third Party Integration / Microsoft 365.

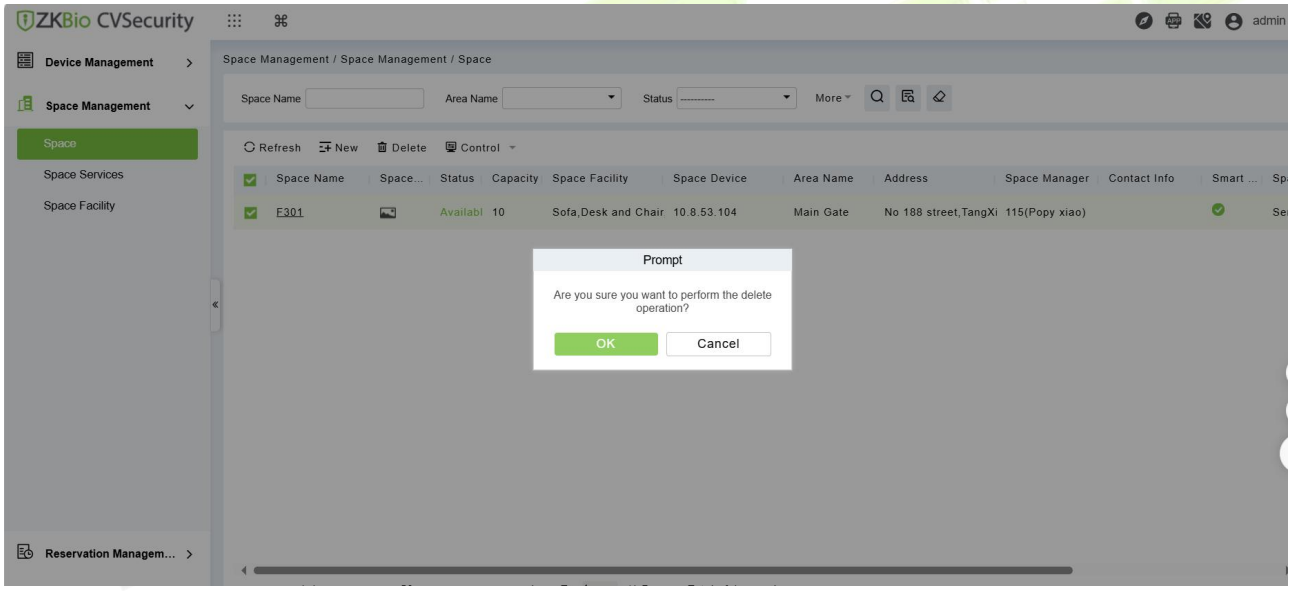


- If you choose Zoom for the online meeting, bind the virtual meeting room resource to the physical meeting room space based on the synchronized content. For detailed configuration, please refer to System / Third Party Integration / Zoom.



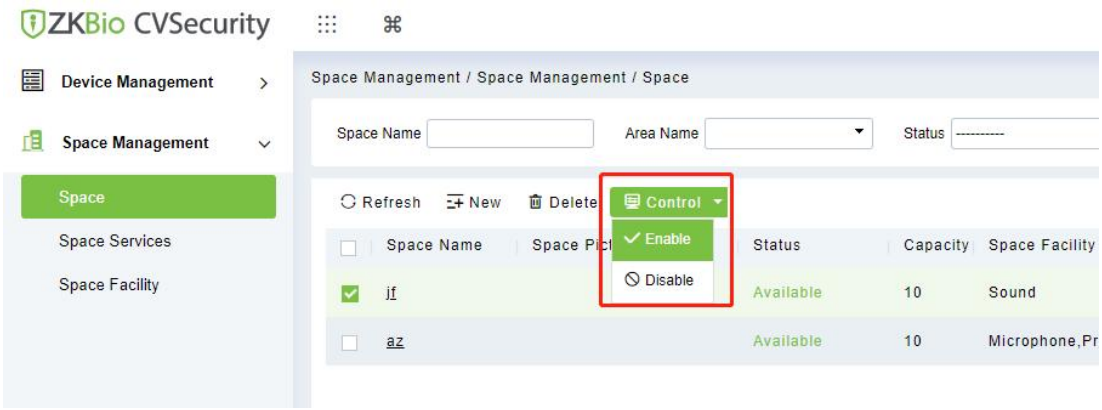
9.2.1.2Delete

To delete a selected space, click **[Space Management]** > **[Space]** > **[Delete]**.



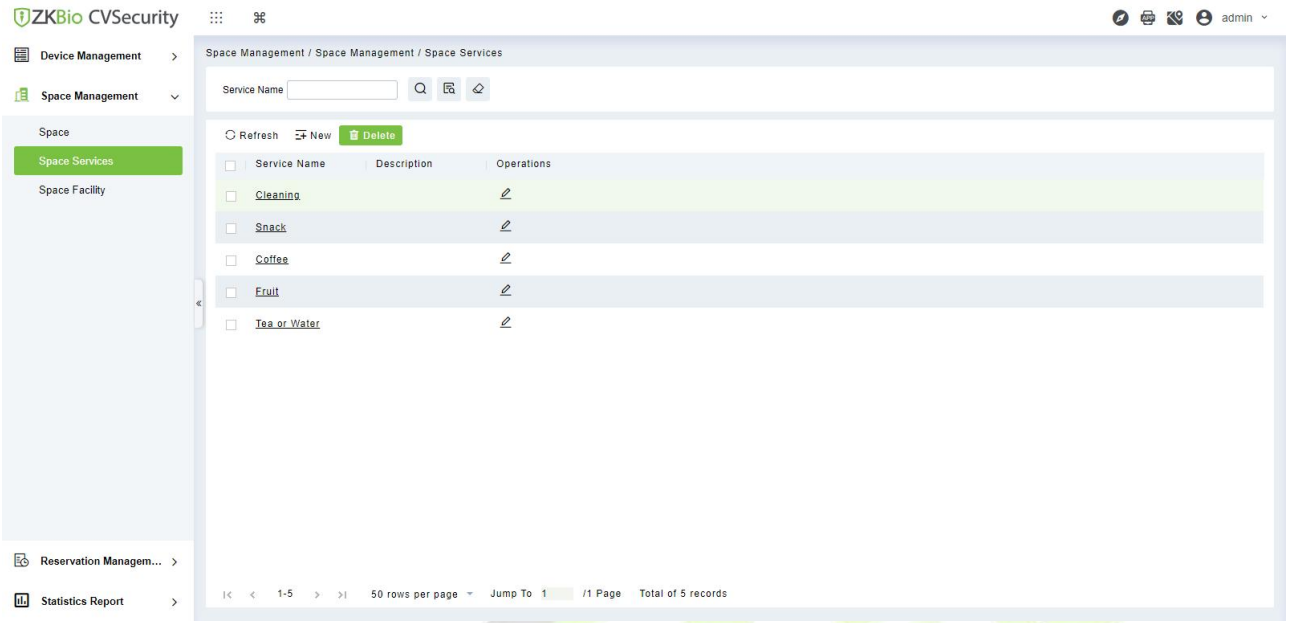
9.2.1.3Control

First, select the space, then, choose to either enable it, setting the status to **[Available]**, or disable it, which will update the status to **[Disabled]**.

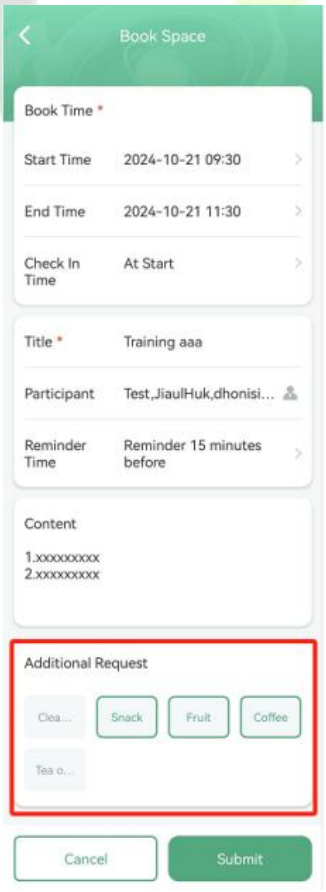


9.2.2Space Services

Space Services allow for defining the scope of services within a space, covering a variety of standard services such as cleaning, tea, coffee, and more. Additionally, customized services can be added to meet the specific needs of the space.

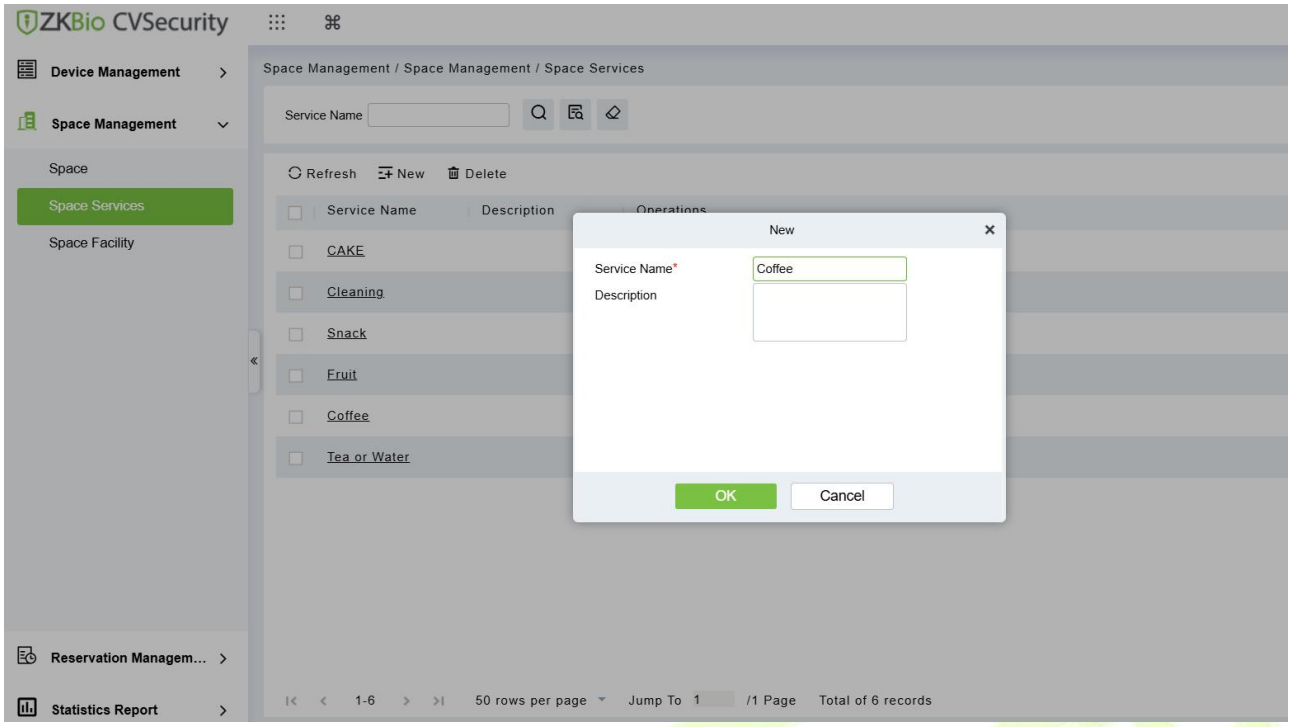


After services are defined, personnel can select needed services when booking a space through the app, as shown in the figure below.



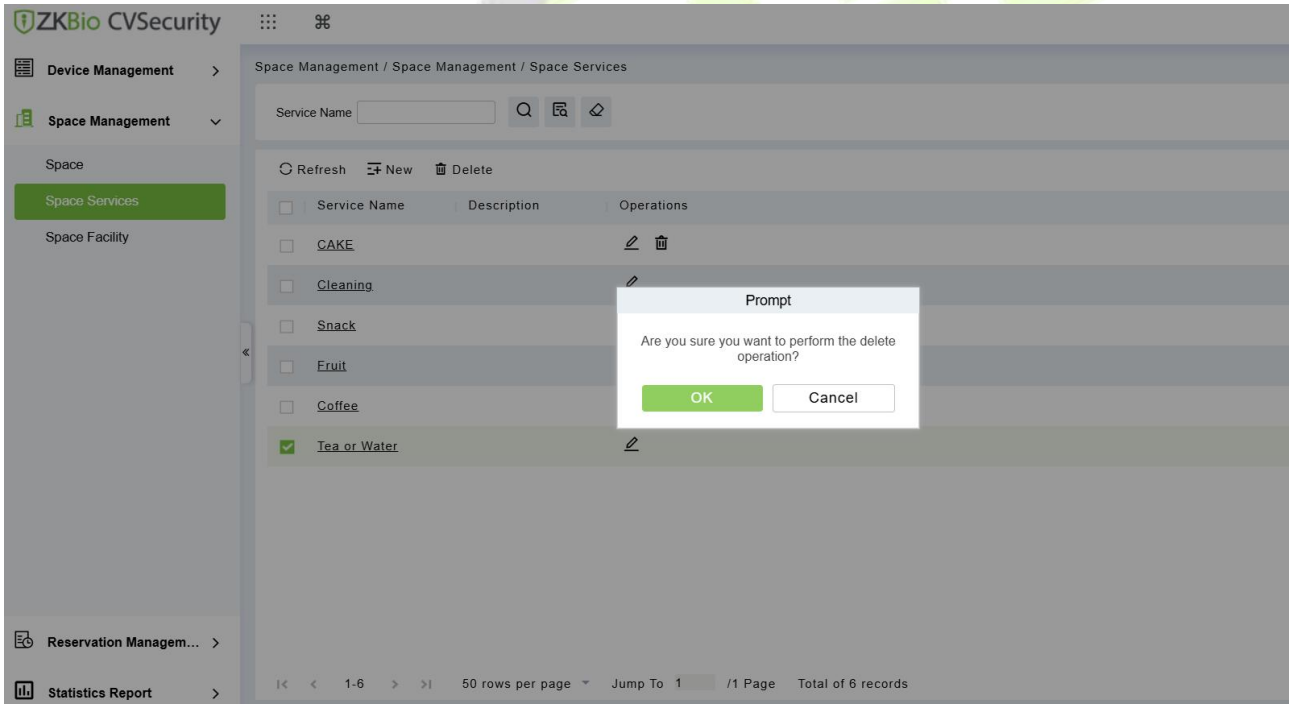
● New

Click **[Space Management]** > **[Space Service]** > **[+New]** to add a new customized service.



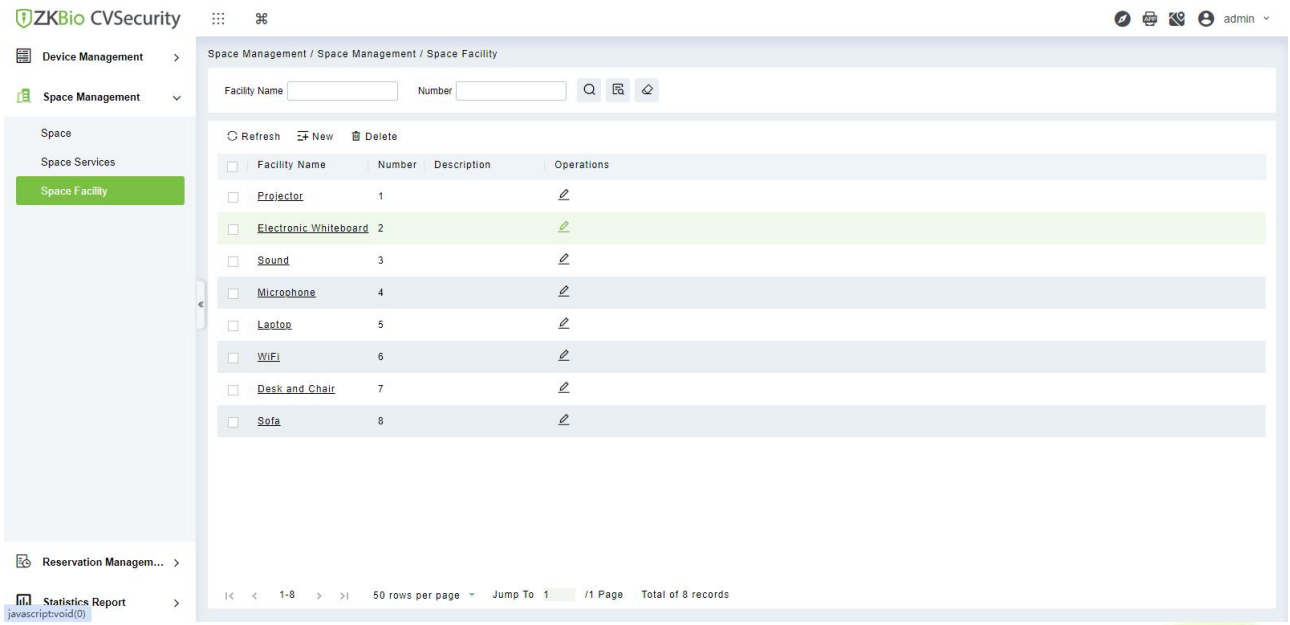
● Delete

Click **[Space Management] > [Space Service] > [Delete]** to delete added service.



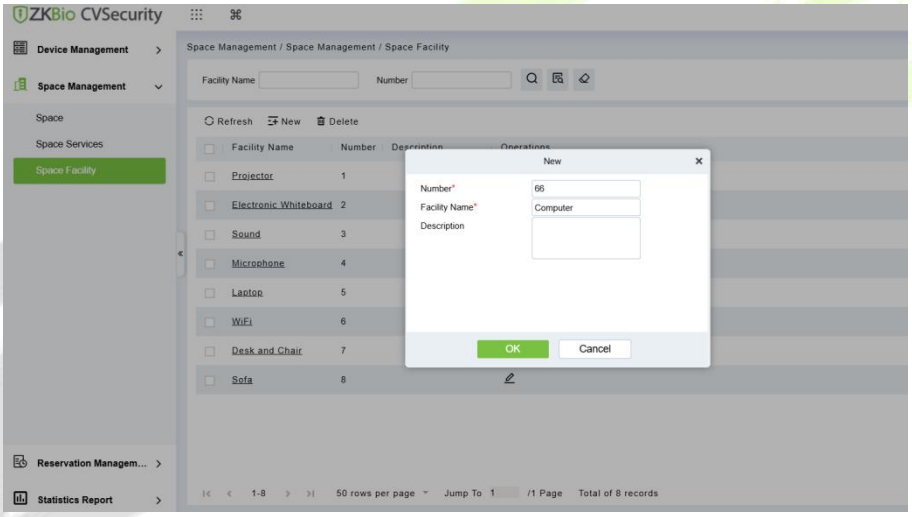
9.2.3 Space Facility

Manage the service facilities within the space, with the flexibility to customize and add additional facilities as needed. This capability enables a tailored approach to space management, ensuring that the space is equipped with the precise services and amenities required to accommodate a diverse range of events and occupant needs.



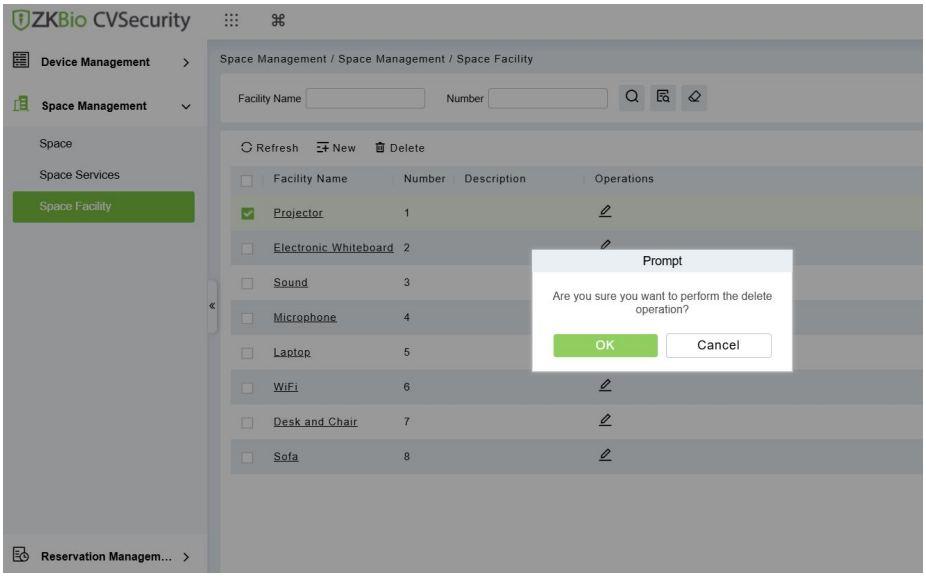
● Add New

Click **[Space Management]** > **[Space Facility]** > **[+New]** to add a new space facility.



● Delete

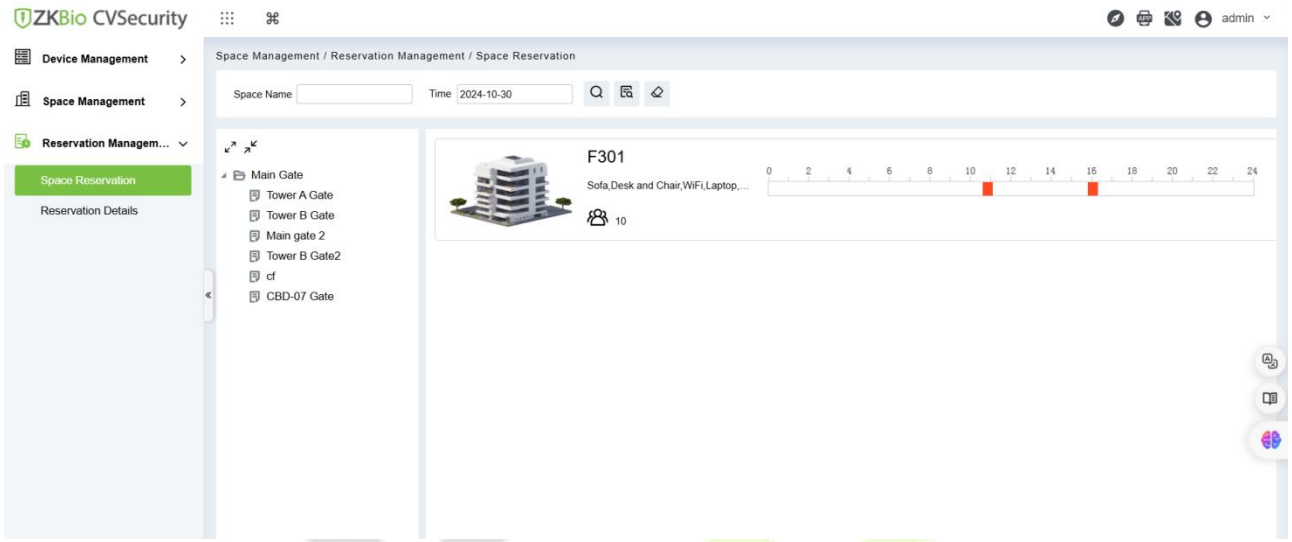
Click **[Space Management]** > **[Space Facility]** > **[Delete]** to delete added space facility.



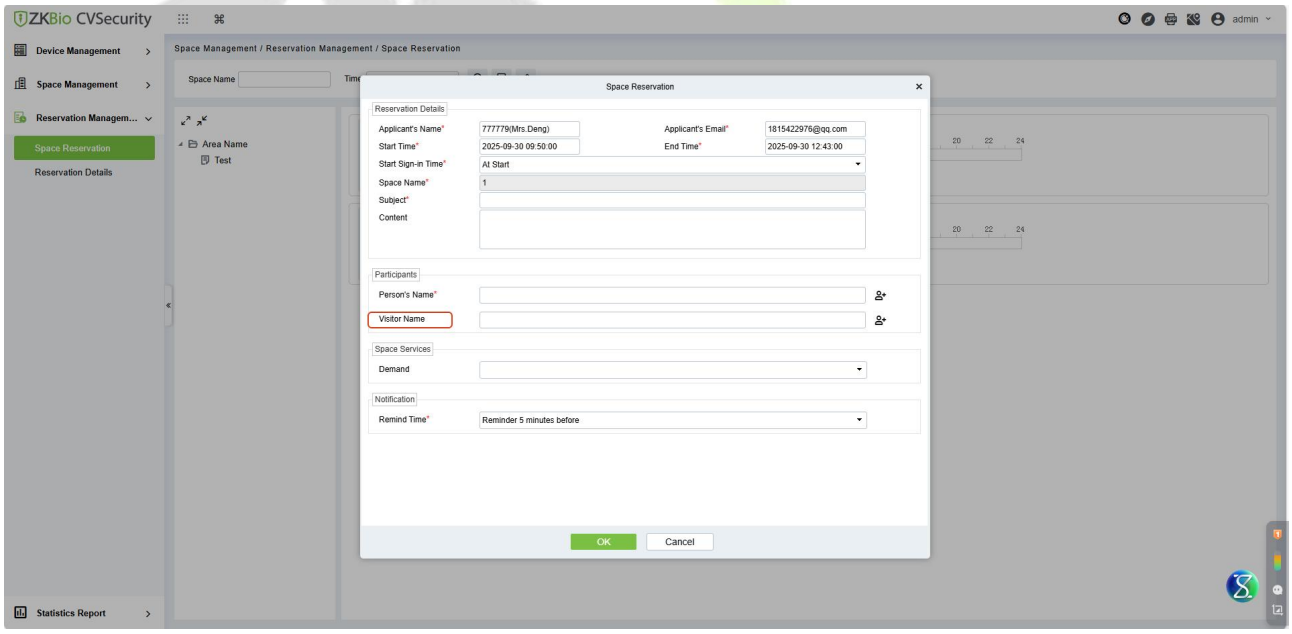
9.3 Reservation Management

9.3.1 Space Reservation

The Space Reservation module provides an intuitive interface displaying the occupancy status of all spaces for the current day, allowing users to filter by area or search for specific spaces by name. This module enables seamless reservation operations, including selecting the desired date and time, adding the applicant and participants, choosing from a range of space services, and setting up notifications to stay informed about upcoming reservations.



Administrators can click on the space card to enter the space reservation interface.



Fields are as follows:

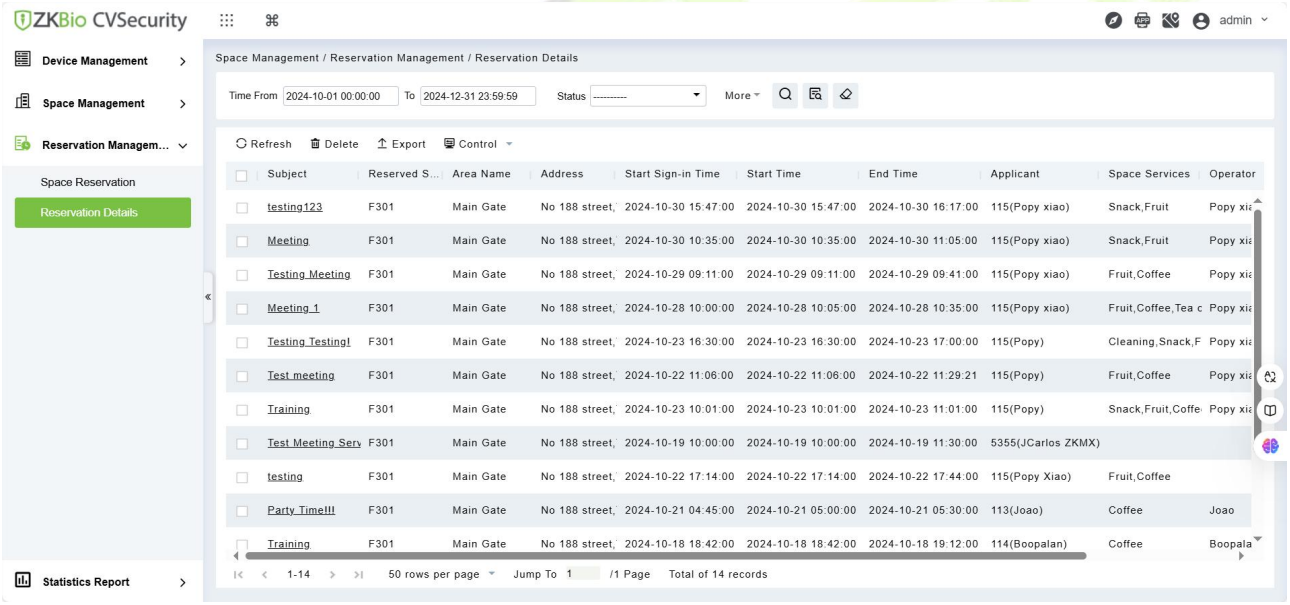
Parameter	Description
Applicant's Name	Name of the applicants
Applicant's Email	Email of the applicants
Start Time/End Time	Set the start time and end time for the reservation space.
Start Sign-in Time	Allowed to start check-in time on the device: At Start, 5 minutes before the start,

Parameter	Description
	15 minutes before the start, 30 minutes before the start.
Space Name	Name of the Space.
Subject	Subject of the space.
Content	Content of the Space
Person's Name	Select participants for the meeting space.
Visitor Name	Select "visitor" as the participant.
Demand	Select the services required for the space.
Remind Time	Select the reminder time for the space reservation.Notifications will be sent to the participants via email or APP.

Note: The types of visitors who can be selected as attendees are those who have made an reservation or check-in.

9.3.2Reservation Details

Click **[Space Management]** > **[Reservation Management]** > **[Reservation Detail]** to enter the reservation details, where we can view the specific appointment situation.

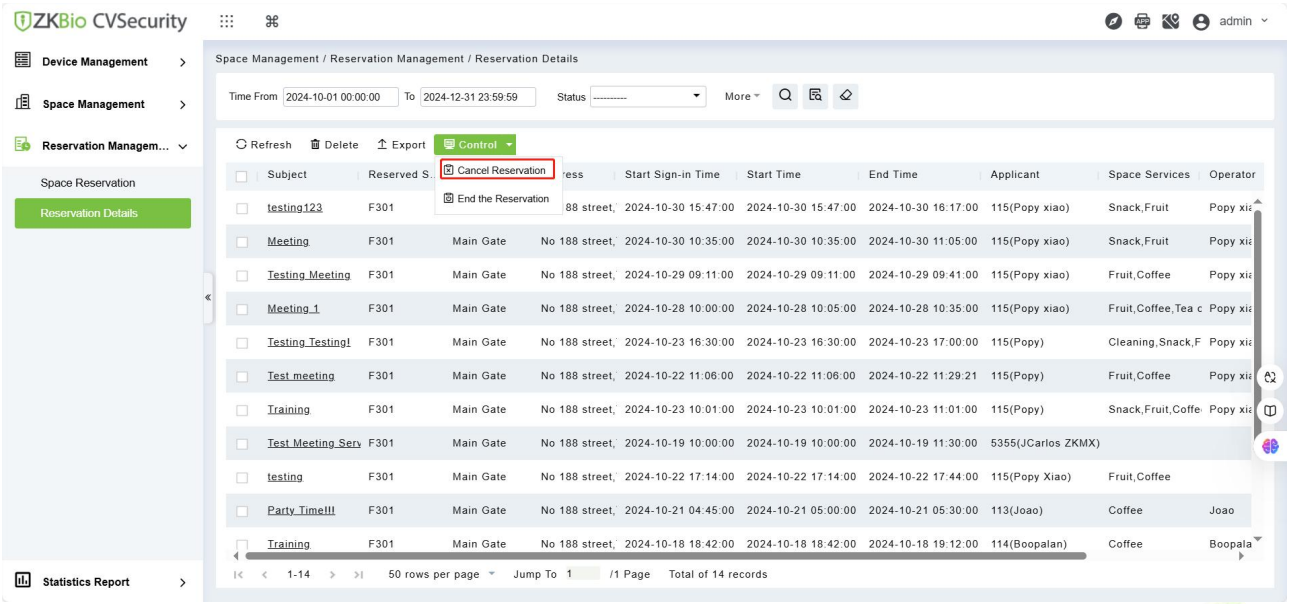


● Cancel Reservation

Click **[Space Management] > [Reservation Management] > [Reservation Detail] >[Control]>**

[Cancel Reservation], we can cancel a previously booked space.

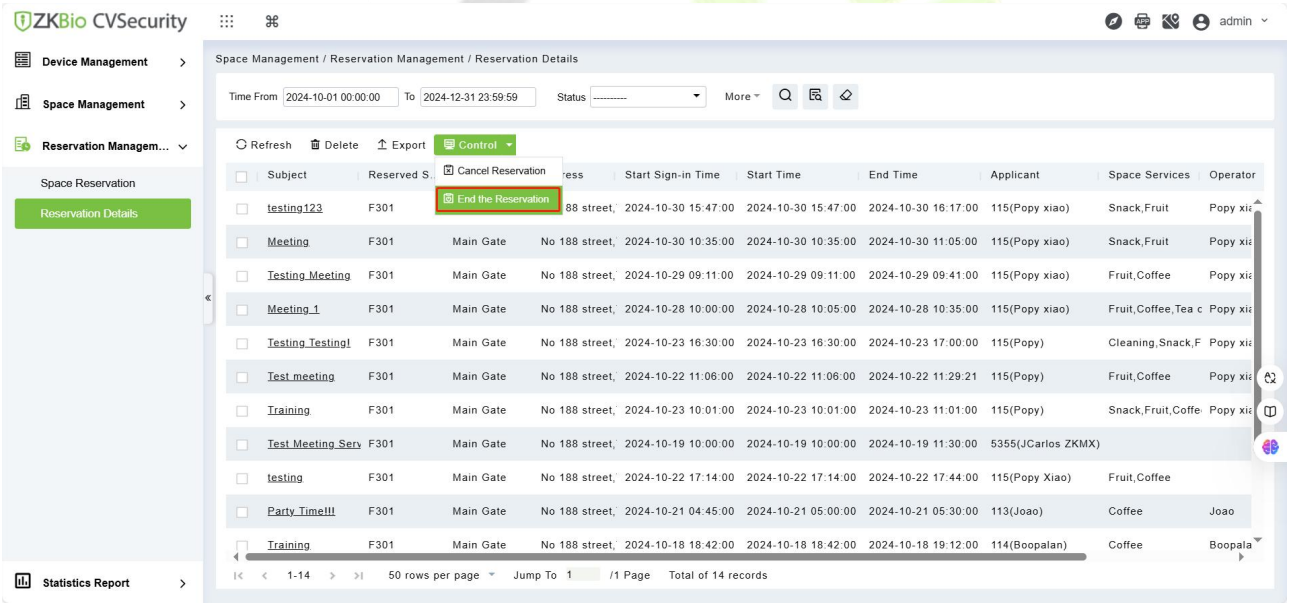
Note: Only events with the status **[Pending Start]** can be canceled. Clicking **[Cancel]** will release the entire reserved time slot back to an available state.



● End the Reservation

Click **[Space Management] > [Reservation Management] > [Reservation Detail] > [Control] > [End the Reservation]**, we can conclude the event for the space that is currently in use.

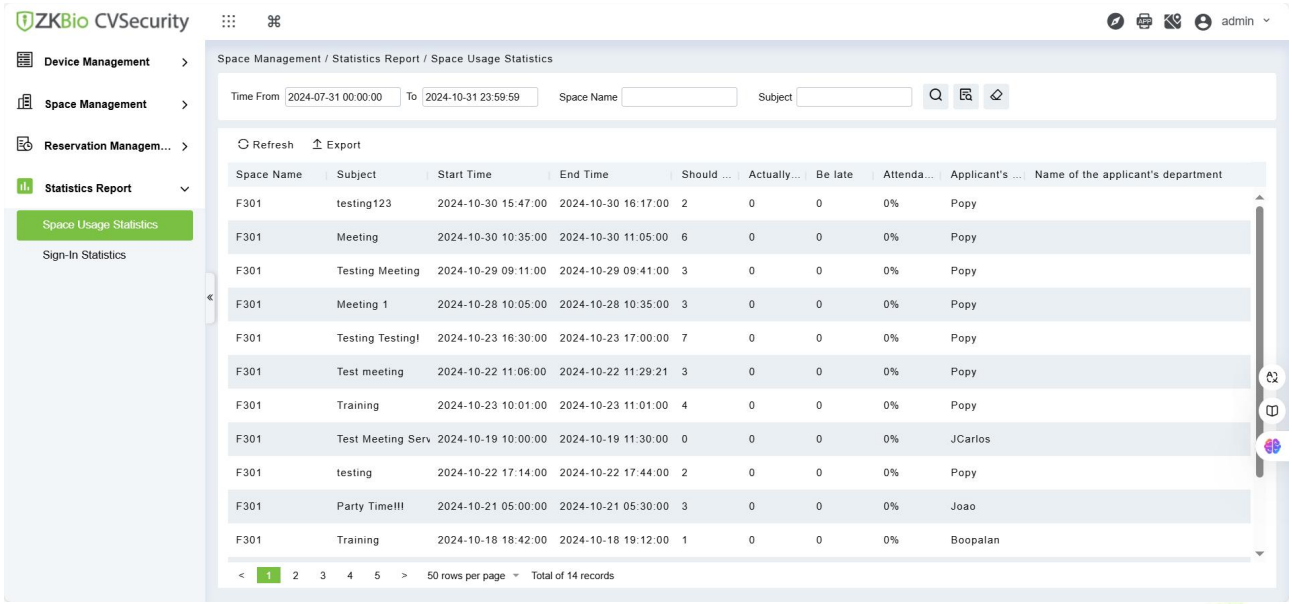
Note: Only meetings that are currently in progress can be ended. For meetings that have not yet started, it is not possible to perform an **[End the Reservation]** operation, but we can cancel the reservation for that space.



9.4 Statistics Report

9.4.1 Space Usage Statistics

The Space Usage Report provides an overview of space utilization.



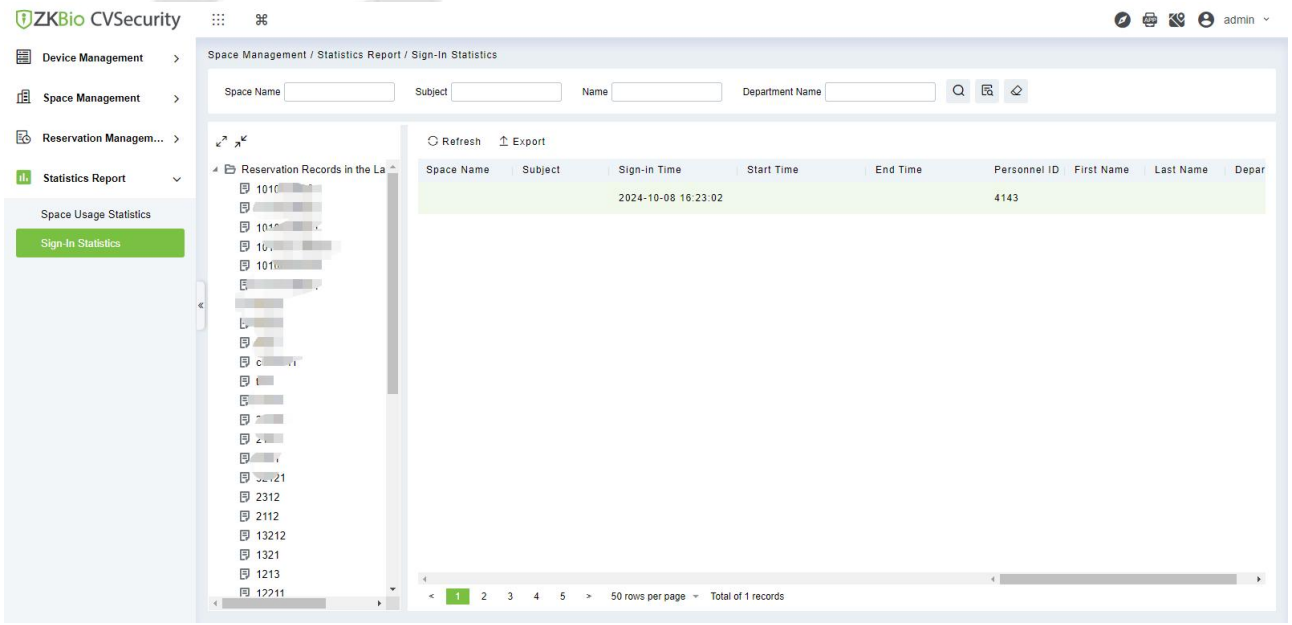
Click **Export**, then you can export the report.

Space Usage Statistics

Space Name	Subject	Start Time	End Time	Should arrive	Actually arrive	Be late	Attendance rate	Applicant's Name	Name of the applicant's department
F301	testing123	2024-10-30 15:47:00	2024-10-30 16:17:00	2	0	0	0%	Popy	
F301	Meeting	2024-10-30 10:35:00	2024-10-30 11:05:00	6	0	0	0%	Popy	
F301	Testing Meeting	2024-10-29 09:11:00	2024-10-29 09:41:00	3	0	0	0%	Popy	
F301	Meeting 1	2024-10-28 10:05:00	2024-10-28 10:35:00	3	0	0	0%	Popy	
F301	Testing Testing!	2024-10-23 16:30:00	2024-10-23 17:00:00	7	0	0	0%	Popy	
F301	Test meeting	2024-10-22 11:06:00	2024-10-22 11:29:21	3	0	0	0%	Popy	
F301	Training	2024-10-23 10:01:00	2024-10-23 11:01:00	4	0	0	0%	Popy	
F301	Test Meeting Service Solution	2024-10-19 10:00:00	2024-10-19 11:30:00	0	0	0	0%	JCarlos	
F301	testing	2024-10-22 17:14:00	2024-10-22 17:44:00	2	0	0	0%	Popy	
F301	Party Time!!!	2024-10-21 05:00:00	2024-10-21 05:30:00	3	0	0	0%	Joao	
F301	Training	2024-10-18 18:42:00	2024-10-18 19:12:00	1	0	0	0%	Boopalan	
F301	Meeting	2024-10-19 14:39:00	2024-10-19 15:09:00	1	0	0	0%	Boopalan	
F301	jess	2024-10-18 15:39:00	2024-10-18 16:09:00	3	0	0	0%	Jessica	
F301	ZKBio CVACCESS Training	2024-10-18 13:35:00	2024-10-18 14:05:00	0	0	0	0%	Popy	

9.4.2 Sign-In Statistics

The Check-in Report allows us to view the check-in status of individuals within the space.



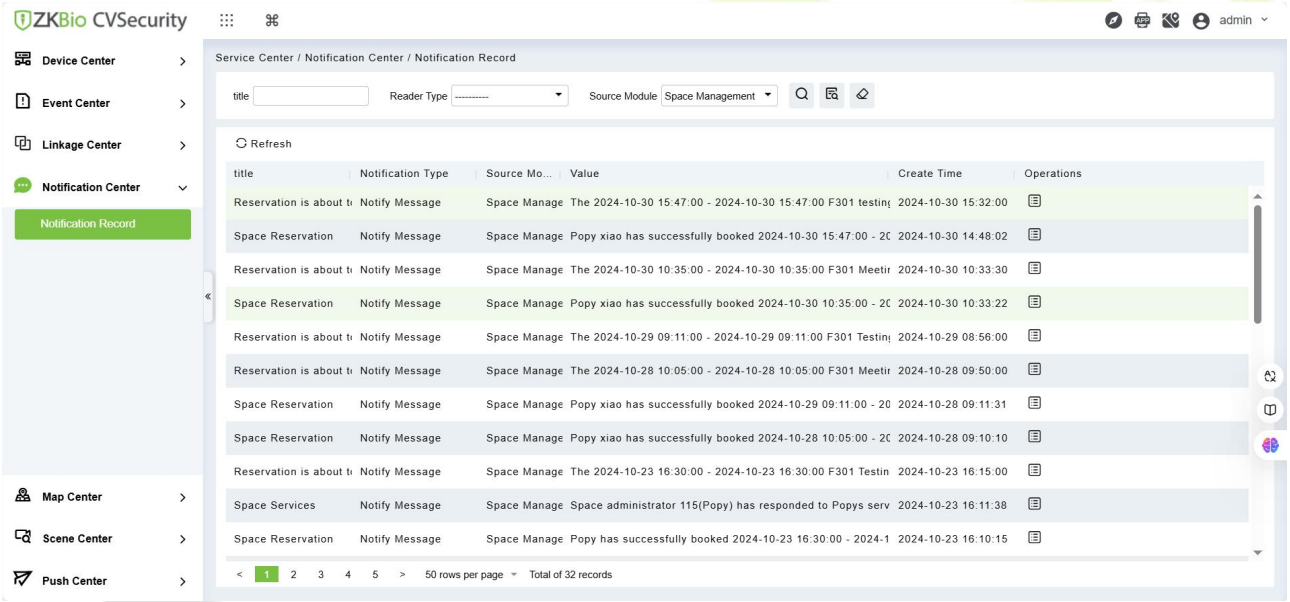
Click **Export**, then you can export the report.

Sign-In Statistics

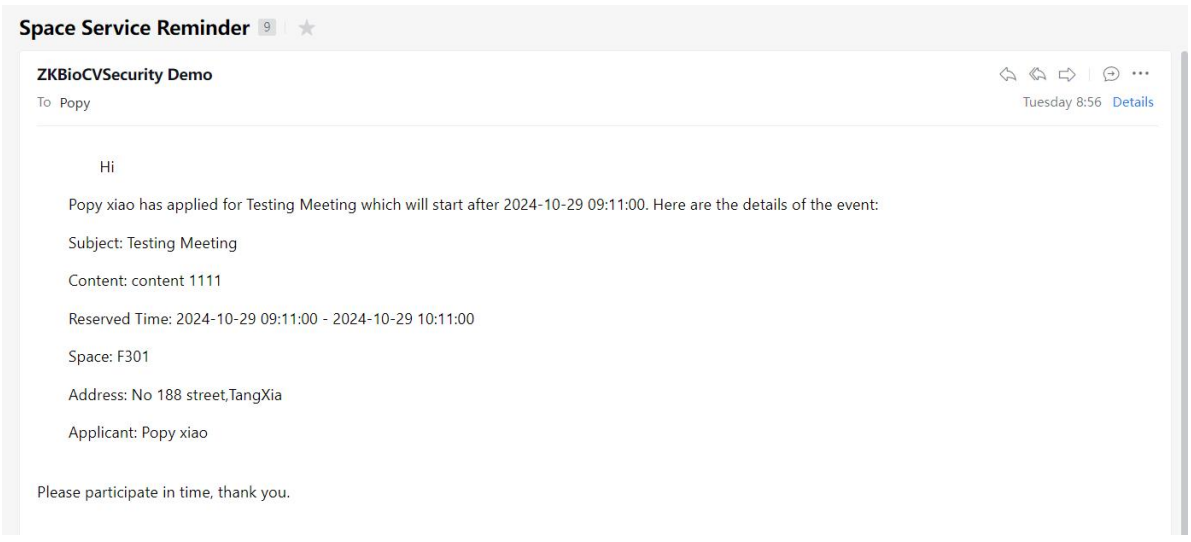
Space Name	Subject	Sign-in Time	Start Time	End Time	Personnel ID	First Name	Department Name
F301	Testing Meeting1	2024-10-09 15:25:32	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy1	Testing
F302	Testing Meeting2	2024-10-09 15:19:39	2024-10-09 13:47:01	2024-10-09 14:43:01	4142	Popy2	Testing
F303	Testing Meeting3	2024-10-09 15:15:07	2024-10-09 13:47:02	2024-10-09 14:43:02	4142	Popy3	Testing
F304	Testing Meeting4	2024-10-09 14:28:07	2024-10-09 13:47:03	2024-10-09 14:43:03	4142	Popy4	Testing
F305	Testing Meeting5	2024-10-09 14:19:48	2024-10-09 13:47:04	2024-10-09 14:43:04	4142	Popy5	Testing
F306	Testing Meeting6	2024-10-09 14:00:47	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy6	Testing
F307	Testing Meeting7	2024-10-09 13:48:31	2024-10-09 13:47:00	2024-10-09 14:43:00	4145	Popy7	Testing
F308	Testing Meeting8	2024-10-09 13:48:21	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy8	Testing
F309	Testing Meeting9	2024-10-09 13:48:19	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy9	Testing
F310	Testing Meeting10	2024-10-09 13:48:06	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy10	Testing
F311	Testing Meeting11	2024-10-09 13:48:04	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy11	Testing
F312	Testing Meeting12	2024-10-09 13:47:54	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy12	Testing
F313	Testing Meeting13	2024-10-09 13:47:52	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy13	Testing
F314	Testing Meeting14	2024-10-09 13:47:50	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy14	Testing
F315	Testing Meeting15	2024-10-09 13:47:15	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy15	Testing
F316	Testing Meeting16	2024-10-09 13:47:14	2024-10-09 13:47:00	2024-10-09 14:43:00	4142	Popy16	Testing
F317	Testing Meeting17	2024-10-09 13:45:14			4142	Popy17	Testing
F318	Testing Meeting18	2024-10-09 13:45:12			4142	Popy18	Testing
F319	Testing Meeting19	2024-10-09 13:44:53			4142	Popy19	Testing
F320	Testing Meeting20	2024-10-09 12:27:52			4142	Popy20	Testing
F321	Testing Meeting21	2024-10-09 12:26:21			4142	Popy21	Testing
F322	Testing Meeting22	2024-10-09 11:57:51			4142	Popy22	Testing
F323	Testing Meeting23	2024-10-09 11:57:49			4142	Popy23	Testing
F324	Testing Meeting24	2024-10-09 11:57:47			4142	Popy24	Testing

9.5 Notification

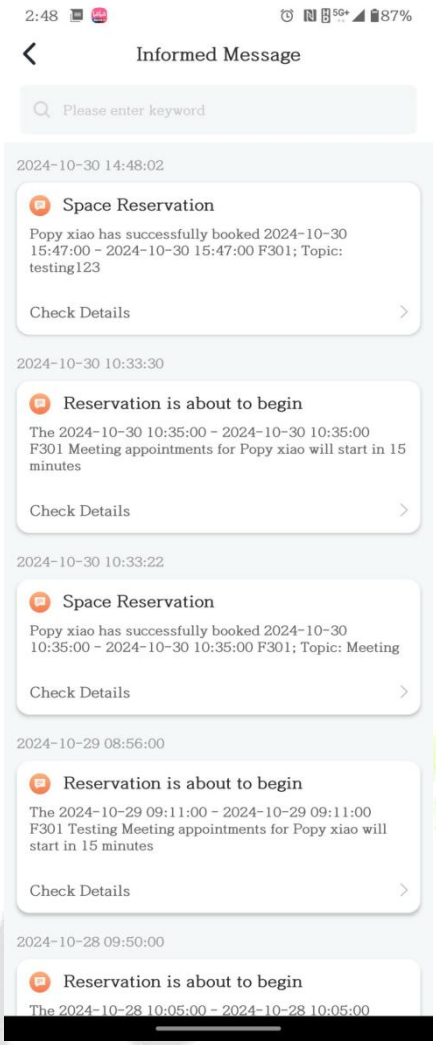
Administrators can go to **Service Center -> Notification Center -> Notification Records** to view historical notification records.



After the applicant books a meeting, the applicant, attendees, and space manager will all receive corresponding emails or app push notifications. The content of the email notification is as follows:



The APP notification content is as follows:



10 Elevator Control

The following is the manual of online elevator control. The Elevator Control System is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's rights to floors and elevator control time, and supervise elevator control events. You can set registered users' rights to floors. Only authorized users can reach certain floors within a period of time after being authenticated.

10.1 Operation Scenario

Elevator control management, also known as elevator access control management, realizes the unified management of personnel entering and leaving the elevator through the configuration of floors and personnel authority groups.

Elevator control solves the elevator floor arrival authority of registered personnel, that is, in a certain period, on certain floors, authorized personnel can be verified and passed.

10.2 Operation Flow

Introduce the configuration process of Elevator control management business.

The business configuration process of Elevator control management business is shown in figure below:

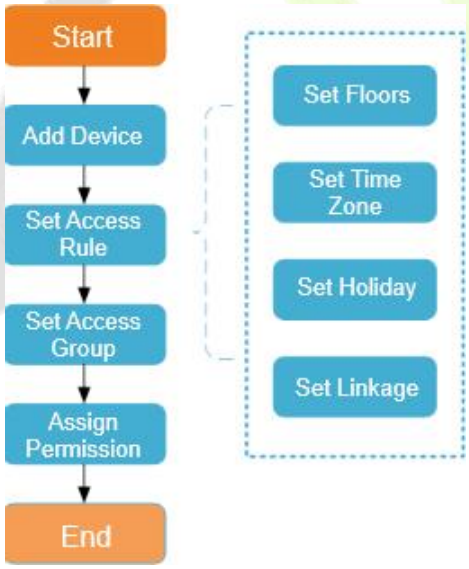


Figure 10- 1 Elevator Control Configuration Flow

10.3 Elevator Device

10.3.1 Add EC10- Elevator Control Device

Configuration steps of adding Elevator Control device in platform.

10.3.1.1 Add device (New)

● Operating Steps:

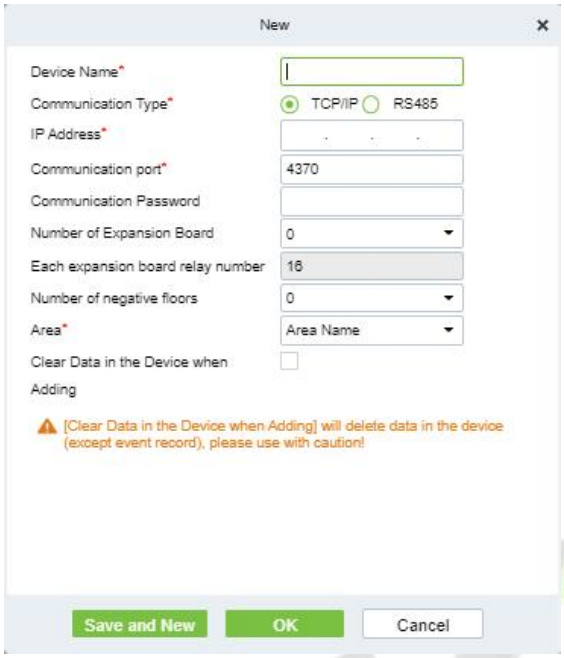
Step 1: In the Elevator Control module, select **Elevator Control Device > Device**.

Step 2: In the device management interface, click the **New** button to pop up the New box.

Step 3: Fill in the corresponding parameter information in the new box. The new box of device is shown in the figures below. Please refer to below table for parameter setting instructions.

Step 4: Click **OK** to complete the operation of adding Elevator control device.

TCP/ IP communication mode



RS485 communication mode

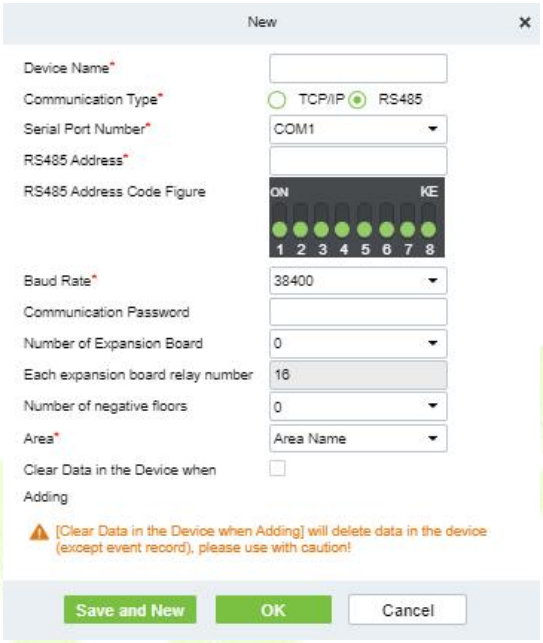


Figure 10- 2 Add Elevator Control Configuration Flow

Parameter	How to set
Device Name	Customize the name of this device
Communication Mode	Choose the communication mode of TCP/IP
IP Address	Fill in the IP address of Elevator control device
Communication Port	The default device communication port is 4370
Communication Cipher	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Plates	The Elevator control device can control the expansion of the number of floors
Number of Relays Per Expansion Board	Each expansion board has 16 relays

Parameter	How to set
Region	The device is divided into regions, and the device can be filtered according to the regions during real-time monitoring
Delete Data in Device When Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.

Table 10- 1 Description of Settings for Adding Devices

10.3.1.2Delete

Step 1: On the **Device** interface, select the required Device from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

10.3.1.3Export

You can export all transactions in Excel, PDF, CSV format.

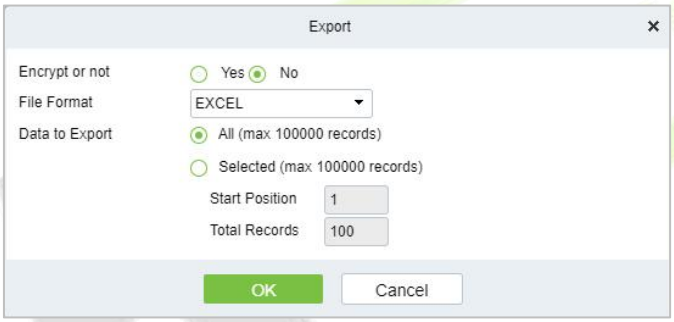


Figure 10- 3 Export Elevator Control Configuration Flow

10.3.1.4Search And Add Elevator Control Device (Search)

The configuration steps of adding Elevator control device in by searching.

Through the way of searching, the Elevator control device in the local area network is searched, and the Elevator control device that has been searched out is directly added, which is convenient to operate.

●Operating Steps:

Step 1: In the Elevator Control module, select "**Elevator Control Device > Device**".

Step 2: In the device management interface, click the **Search** button to pop up the search box.

Step 3: Click "**Start Search**" in the search box to display the Elevator control devices that can be added, as shown in figure below:

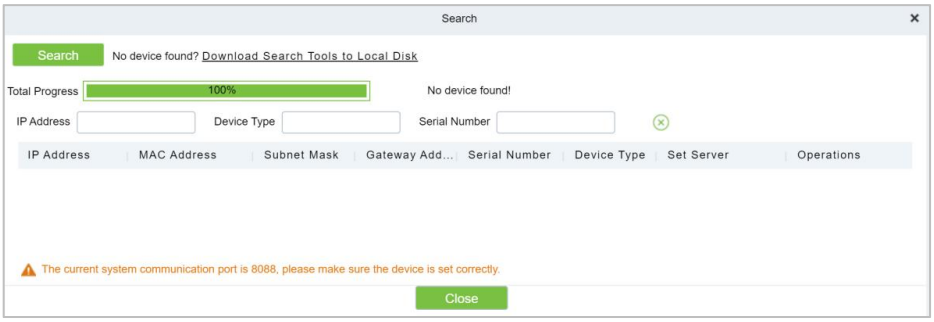


Figure 10- 4 Device Search Add Interface

Step 4: Optional: Modify the IP address of Elevator control device and click "**Modify IP Address**". Modifying IP address will restart the device, and the IP address modification will be completed after restarting.

Step 5: For the Elevator control device searched, click the **Add** button in the operation bar to add the device; The device addition settings are shown in figure below, and the parameter settings are shown in table below.

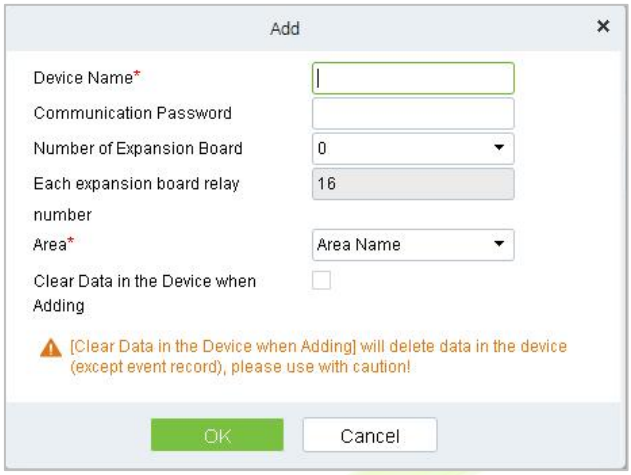


Figure 10- 5 Add Interface

Parameter	How to set
Device Name	Customize the name of the device.
Communication Cipher	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Plates	Elevator control device can control the expansion of the number of floors.
Number of Relays Per Expansion Board	Each expansion board has 16 relays.
Region	The device is divided into regions, and the device can be filtered according to the regions during real-time monitoring.
Delete Data in Device When Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.

Table 10- 2 Device Search Added Settings Description

Step 6: Click **OK** to complete the operation of adding Elevator control device.

Step 7: Click **Close** to close the Device Search Add interface.

10.3.1.5Control

Upgrade Firmware

Tick the device that needs to be upgraded, click **Upgrade firmware** to enter edit interface, then click **Browse** 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. Unauthorized upgrade may affect normal operations.

Reboot Device

It will reboot the selected device.

Synchronize Time

It will synchronize device time with server's current time.

Disable/Enable

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

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.

10.3.1.6Set Up

Modify IP Address

Select a device and click **Modify IP address** to open the modification interface. It will obtain a real-time network gateway and subnet mask from the device. (Failed to do so, you cannot modify the IP address). Then enter a new IP address, gateway, and subnet mask. Click **OK** to save and quit. This function is the similar as Modify IP Address Function in Device.

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:** Communication password shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password setting can improve the device's security. It is recommended to set communication password for each device.

Modify RS485 Address

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

Modify the Fingerprint Identification Threshold

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.

Set extended Parameters

We can set the extended parameters of device like temperature detection and mask detection

10.3.1.7View/Get

Get Device Option

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

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.

Get Transactions

Get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.

10.3.2Add EC16-Elevator Control Device

This sub module introduces the configuration steps of adding Access Control device in platform. The elevator control device is added in a new way by TCP/IP and RS485 communication.

10.3.2.1Add Device (New)

Operating Steps:

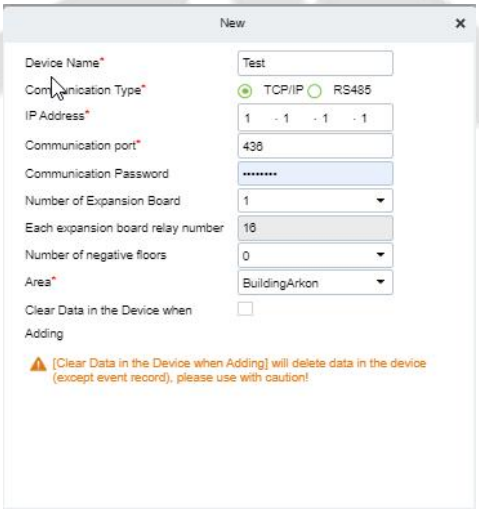
Step 1: In the Elevator module, select "**Elevator Device > Device**".

Step 2: In the device management interface, click on **New** to pop up the New box.

Step 3: Fill in the corresponding parameter information in the new box. The new box of device is shown in the figures below. Please refer to below table for parameter setting instructions.

Step 4: Click **OK** to complete the operation of adding Elevator control device.

TCP/IP Communication



RS485 Communication

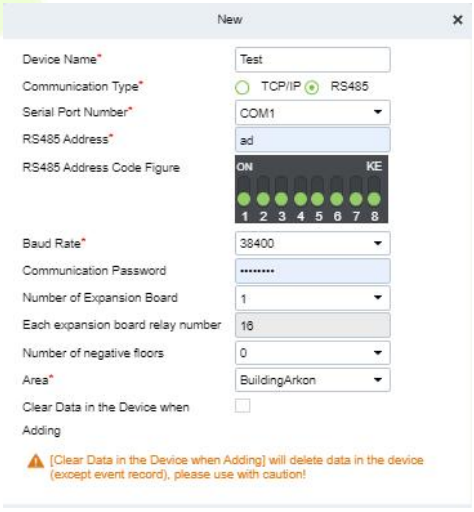


Figure 10- 6 Add Elevator Control Configuration Flow

Fields to be filled for TCP/IP

Parameter	How to set
Device Name	Customize the name of this device.
Communication Type	Choose the communication mode of TCP/IP.
IP Address	Enter the IP address.
Communication Port	The default device communication port is 4370.
Communication	Fill in the communication password of the device. If there is no password, it

Parameter	How to set
Password	does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Board	The Elevator control device can control the expansion of the number of floors.
Each expansion board relay number	Each expansion board has 16 relays.
Number of negative floors	Select the number of negative floor from the default list of 5.
Area	The device is divided into areas, and the device can be filtered according to the area during real-time monitoring.
Clear Data in the Device when Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.
Fields to be filled for RS485	
Device Name	Customize the name of this device.
Communication Type	Choose the communication mode of TCP/IP.
Serial Port Number	Select the serial port number from the list up to COM255.
RS485 Address	Enter the Address in integer only and it must be 1-63. Once after enter figure, RS485 will update automatically.
RS485 Address Code Figure	Set the address code figure by clicking or toggling on the required number. It must be from 1-63 only. Once it is done the RS485 Address will update automatically.
Baud Rate	Select one of the baud rate from the list 19200, 38400, 57600, and 115200.
Communication Password	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory devices and initialized devices, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Board	The Elevator control device can control the expansion of the number of floors.
Each expansion board relay number	Each expansion board has 16 relays
Number of negative floors	Select the number of negative floor from the default list of 5.
Area	The device is divided into areas, and the device can be filtered according to the area during real-time monitoring.
Clear Data in the Device when Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.

Table 10- 3 Description of Settings for Adding Devices

10.3.2.2 Delete

Step 1: On the **Device** interface, select the required Device from the list.

Step 2: Click **Delete** or click on the icon to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

10.3.2.3Search and Add Elevator Control Device (Search)

The configuration steps for adding an elevator control device through a search method. By searching within the local area network, the elevator control device is identified and directly added, providing a convenient operation process.

Operating Steps:

Step 1: Click **Elevator** > **Elevator Device** >**Device** > **Search**, to open the Search interface in the software.

Step 2: Click **Search** to search the elevator controller.

Step 3: After searching, the list and total number of elevator controllers will be displayed.

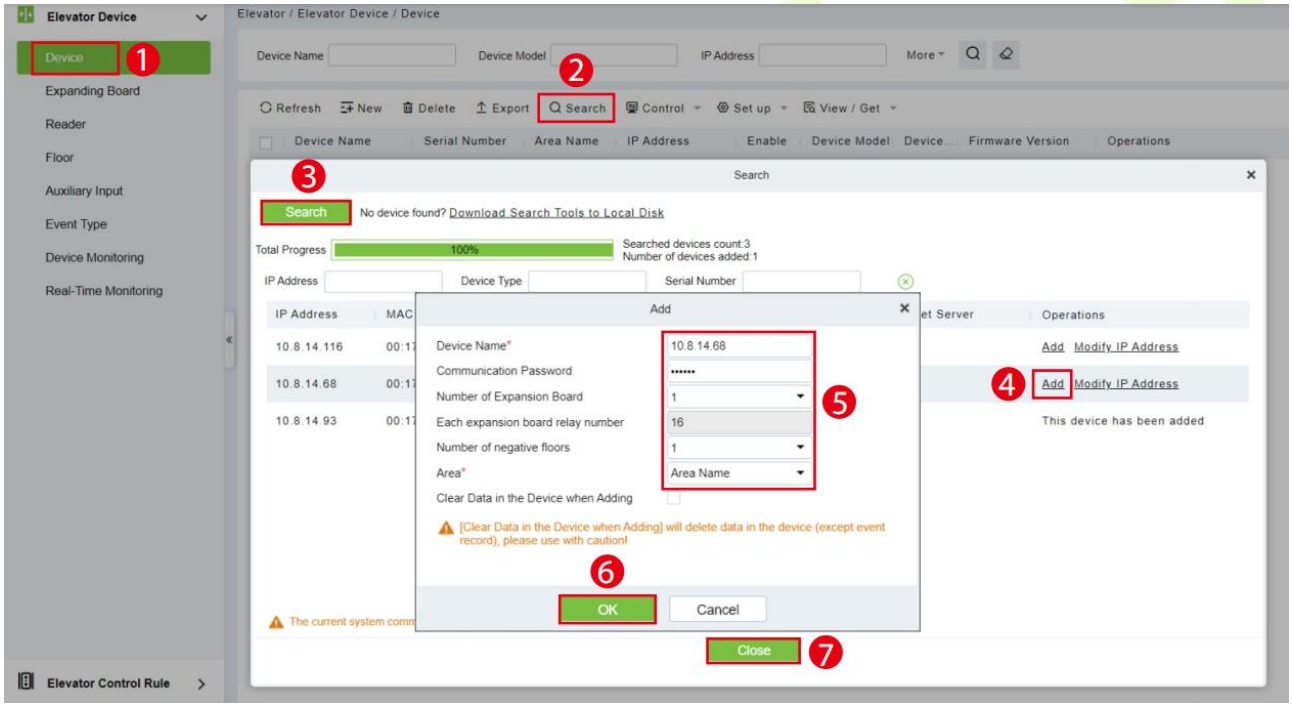


Figure 10- 7 Device Search Add

Step 4: For the Elevator control device searched, click **Add** in the operation bar to add the device.

Step 5: Click **OK** to complete the operation of adding elevator control device.

Step 6: Click **Close** to close the Device Search Add interface.

Parameter	How to set
Device Name	Customize the name of this device.
Communication Password	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web

Parameter	How to set
	page and enter the background to customize the verification password.
Number of Expansion Plates	The Elevator control device can control the expansion of the number of floors.
Number of Relays Per Expansion Board	Each expansion board has 16 relays.
Region	The device is divided into regions, and the device can be filtered according to the regions during real-time monitoring.
Delete Data in Device When Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.

Table 10- 4 Device Search Added Settings Description

10.3.3Expanding Board (EC10+EX16)

This introduces the configuration Steps of adding **Expanding Board** device in the platform.

10.3.3.1Add Device (New)

● Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control device > Expanding Board".

Step 2: In the expanding board interface, click the **New** button to pop up the New box.

Step 3: Fill in the corresponding parameter information in the new box. The new box of device is shown in figure below. Please refer to table below for parameter setting instructions.

Step 4: Click **OK** to complete the operation of adding Expanding board interface.

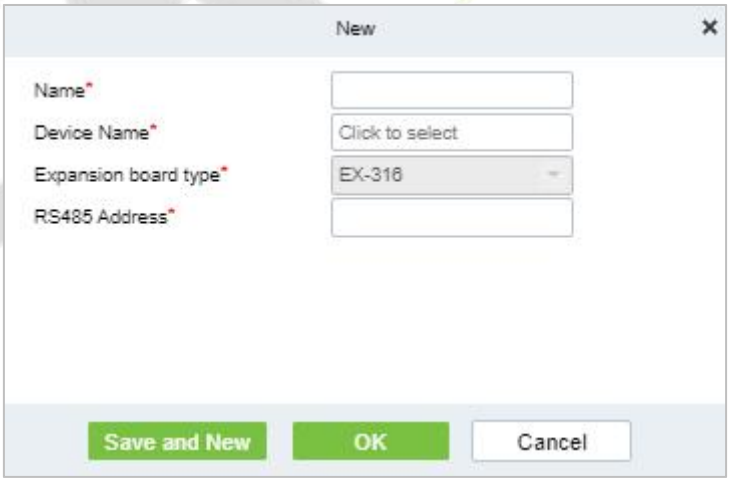


Figure 10- 8 Add Expanding Board

10.3.3.2Delete

Step 1: On the **Expanding Board** interface, select the required Device from the list.

Step 2: Click **Delete** or click on the icon to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

10.3.4Expanding Board (EC16+DEX16)

10.3.5Add Expanding Board

Step 1: Connect the expansion board correctly and set the RS485 address of the expansion board with the dip switch, then restart the device within 6 minutes.

Step 2: In the Elevator Control module, select "**Elevator Control device > Expanding Board**".

Step 3: In the expanding board interface, click the **New** button to pop up the New box.

Step 4: Fill in the corresponding parameter information in the new box.

Step 5: Click **OK** to complete the operation of adding Expanding board interface.

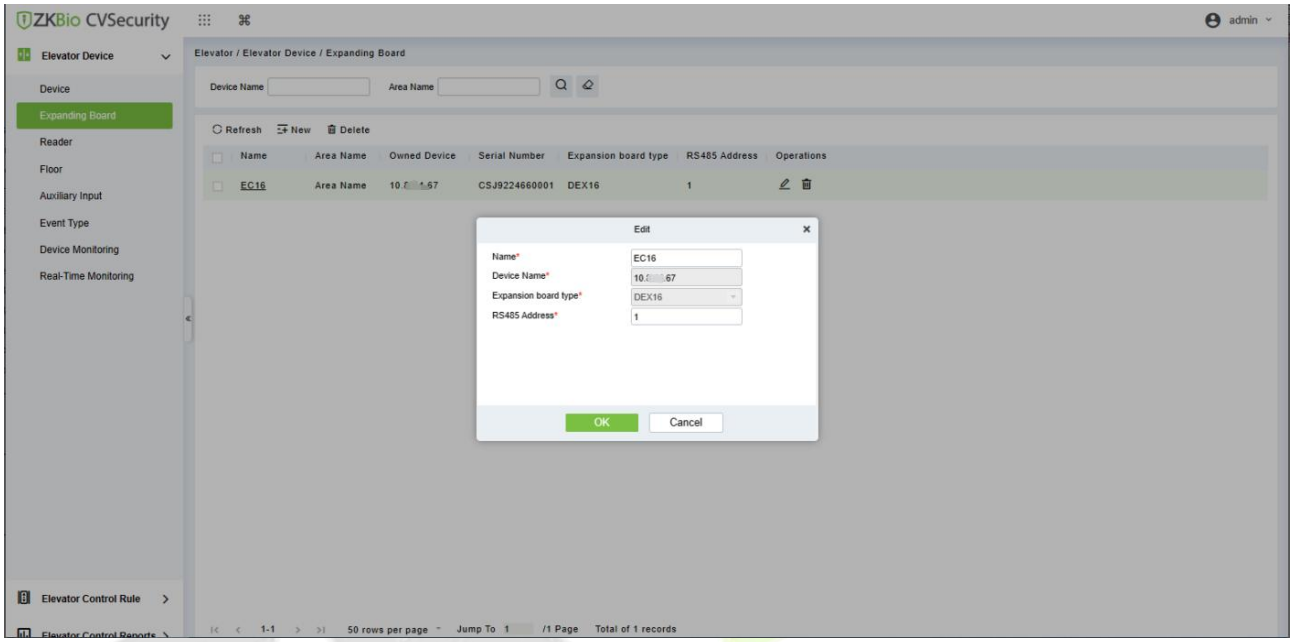


Figure 10- 9 Add Expanding Board

Parameter	Description
Name	The name of Expanding Board.
Device Name	Select the corresponding elevator control device.
Expansion Board Type	The type of expanding board. And the expansion board type cannot be modified.
Rs485 Address	Communication protocol between expansion board and reader. The communication protocol should be consistent.

Table 10- 5 Description of Expanding Board

10.3.5.1Delete

Step 1: On the Expanding Board interface, select the required Device from the list.

Step 2: Click Delete or click on the icon to delete the selected Device.

Step 3: Click Delete, to ensure and delete the selected Device from the list.

10.3.6Reader

Each elevator device has a reader, the reader information can be set.

● Operating Steps:

Click **Elevator Device** > **Reader**, select a reader name in the reader list:

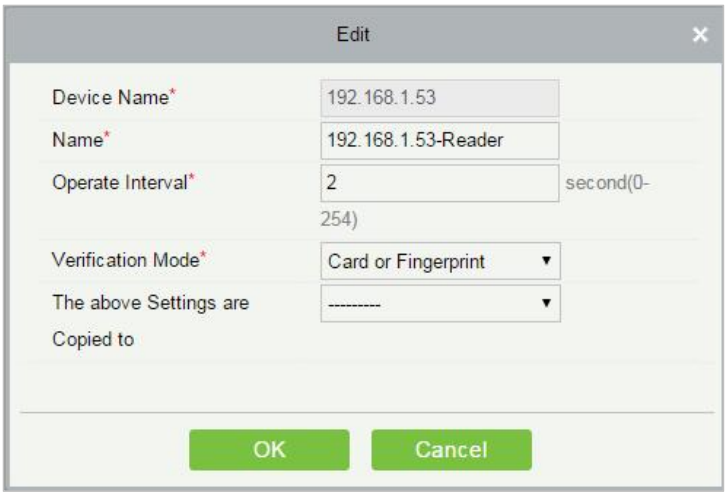


Figure 10- 10 Edit Reader interface

Parameter	How to set
Device Name	It is not editable.
Name	The default format is "Device Name - Reader", editable in 30 characters.
Operate Interval	The interval between two verifications. The default value is 2 seconds, the range is 0 to 254 seconds.
Verification Mode	The default setting is "Card or Fingerprint". The Wiegand reader supports" Only Card", "Only Password", "Card or Password", "Card and Password", "Card or Fingerprint". The RS485 reader supports "Card or Fingerprint". Make sure the reader has a keyboard when the verification mode is "Card and Password".
The above settings are copied to	Apply the above settings to all readers within the current user's level. Click **OK** to save and exit.

Table 10- 6 Reader Setting

10.3.7 Floor

The setting of floor parameters affects the logical judgment of Elevator control verification.

10.3.7.1 Edit

● Operating Steps:

Step 1: In the Elevator Control module, select **Elevator Control device > Floor**.

Step 2: In the floor management interface, click the **Edit** button in the floor selection operation bar to pop up the floor parameter setting box.

Step 3: In the floor parameter setting interface, fill in the corresponding parameters according to the addition requirements, as shown in figure below. Please refer to table below for parameter filling

instructions.

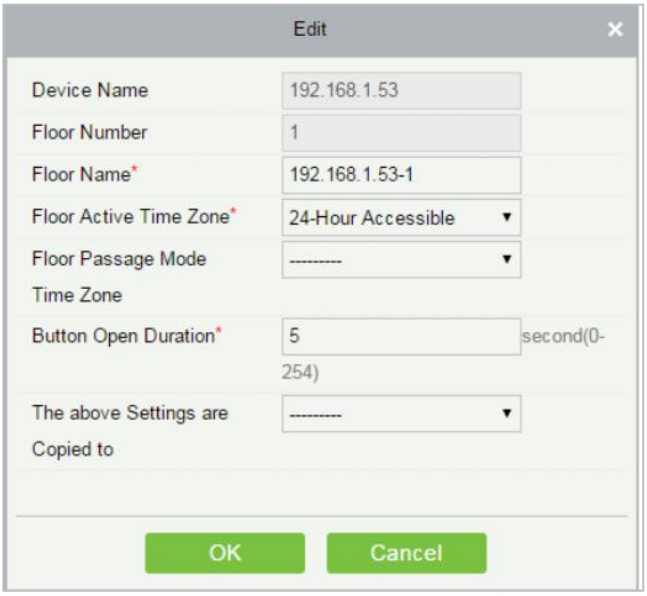


Figure 10- 11 Floor Parameter Setting

Parameter	How to set
Owned Device	Displays the basic information of this floor, and reset is not supported.
Floor Number	The system automatically numbers the device according to the number of relays.
Floor Name	It defaults to "device Name-Floor Number", which can be repaired as needed, and can be filled in with a maximum of 30 arbitrary characters.
Effective Time Period of Floor	When editing a floor, the effective time period of the floor is required. Only after the effective time period of the floor is set can the close floor button be continuously released.
Time Period for Continuously Releasing Keys	It must be valid within the effective period of the floor. It is recommended to set the continuous release period of the floor. The setting is included in the effective period of the floor.
Key Holding Time	Used to control swiping cards or pressing fingerprints, within the range of time, you can press the floor buttons of elevators. The default is 5 seconds, and the range is 0-254.
Copy The Above Settings To	Set which floors the above floor parameters also apply to. The options are: all floors of current device and floors of all device.

Table 10- 7 Instructions for Setting Floor Parameters

Step 4: Click **OK** to complete the operation of adding Elevator-controlled floors.

10.3.7.2Remotely Release the Button

It determines whether the corresponding key to the selected floor can be pressed. You can customize

the key release duration (15s by default) or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

10.3.7.3 Remotely Lock the Button

This normal event is triggered if a user remotely locks a button successfully.

10.3.7.4 Remote Normal Opening

The person having open door permission punch effective card at the opened door to trigger this normal event.

10.3.7.5 Enable Intraday Passage Mode Timezone

If the intraday passage mode time zone is disabled, punch effective card for five times (must be the same user) or select Enable Intraday Passage Mode Time Zone in remote opening operation, and this normal event is triggered.

10.3.7.6 Disable Intraday Passage Mode Timezone

In door normal open state, punch effective card for five times (must be the same user) or select **Disable Intraday Passage Mode Time Zone** in remote closing operation, and this normal event is triggered.

10.3.8 Auxiliary Input

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

10.3.8.1 Edit

● Operating Steps:

Step 1: Click **Elevator Device** > **Auxiliary Input** on the Action Menu, enter into the following page.

Step 2: Click **Edit** to modify the parameters

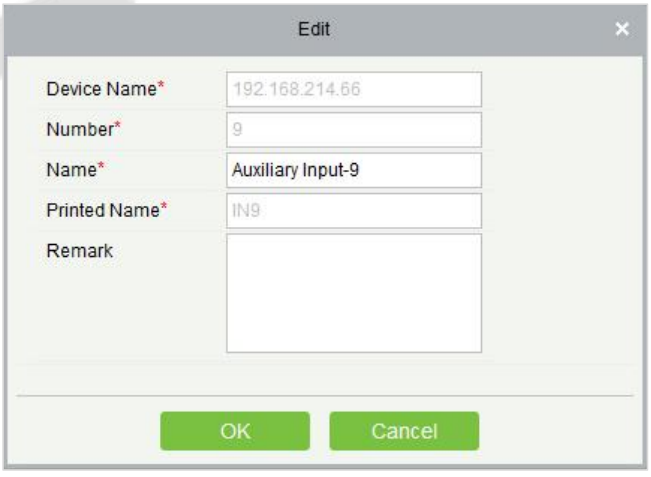


Figure 10- 12 Auxiliary Input Add Interface

Parameter	How to set
Device Name	You can customize the name according to your preference.

Parameter	How to set
Number	Displays the Number.
Name	It displays the default name of "Auxiliary Input"
Printed Name	The printing name in the hardware, for example IN9.
Remark	Displays the Comment.

Table 10- 8

10.3.9Event Type

Display the event types of the elevator devices.

● Operating Steps

Step 1: Click **Elevator Device** > **Event Type**, the following page is displayed:

Refresh

Event Name	Event No.	Event Level	Device Name	Serial No.
Normal Punch Open	0	Normal	192.168.90.235	0013130700074
Punch during Passage Mode Time Zone	1	Normal	192.168.90.235	0013130700074
Open during Passage Mode Time Zone	5	Normal	192.168.90.235	0013130700074
Remote Release	8	Normal	192.168.90.235	0013130700074
Remote Locking	9	Normal	192.168.90.235	0013130700074
Disable Intraday Passage Mode Time Zone	10	Normal	192.168.90.235	0013130700074
Enable Intraday Passage Mode Time Zone	11	Normal	192.168.90.235	0013130700074
Normal Fingerprint Open	14	Normal	192.168.90.235	0013130700074
Press Fingerprint during Passage Mode Time Zc	16	Normal	192.168.90.235	0013130700074
Operate Interval too Short	20	Exception	192.168.90.235	0013130700074
Button Inactive Time Zone(Punch Card)	21	Exception	192.168.90.235	0013130700074
Illegal Time Zone	22	Exception	192.168.90.235	0013130700074
Access Denied	23	Exception	192.168.90.235	0013130700074

Figure 10- 13 Event Type Interface

10.3.10Real Time Monitoring

10.3.10.1Operating Steps

Click **Elevator Device** > **Real-Time Monitoring**, real-time monitor the status and real-time events of elevator controllers in the system, including normal events and abnormal events (including alarm events).

Area Device Name Remotely Release the Button Remotely Lock the Button

Time	Area Name	Device Name	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2017-02-10 16:11:12	Area Name	192.168.214.66(00131	192.168.214.66-2	Remote Release				Other
2017-02-10 16:11:12	Area Name	192.168.214.66(00131	192.168.214.66-1	Remote Release				Other
2017-02-10 16:11:01	Area Name	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint
2017-02-10 16:10:47	Area Name	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint
2017-02-10 16:10:44	Area Name	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint

Figure 10- 14 Real Monitoring

10.3.10.2Remotely Release the Button

1. Click Remotely Release Button:

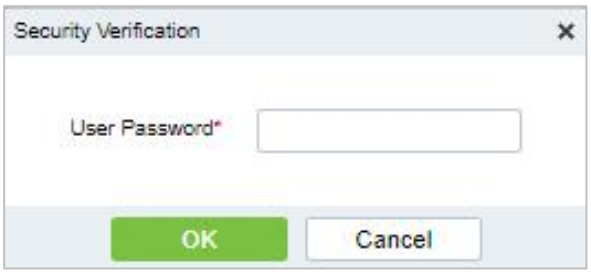


Figure 10- 15 Security Verification

2. Input the user password (the system logging password), click Next Step:

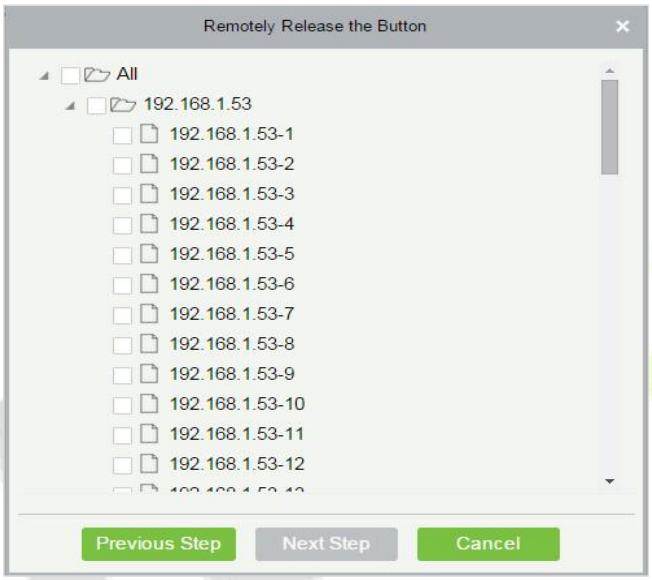


Figure 10- 16 Remotely Release Button

3. Select the floor, and click Next Step:

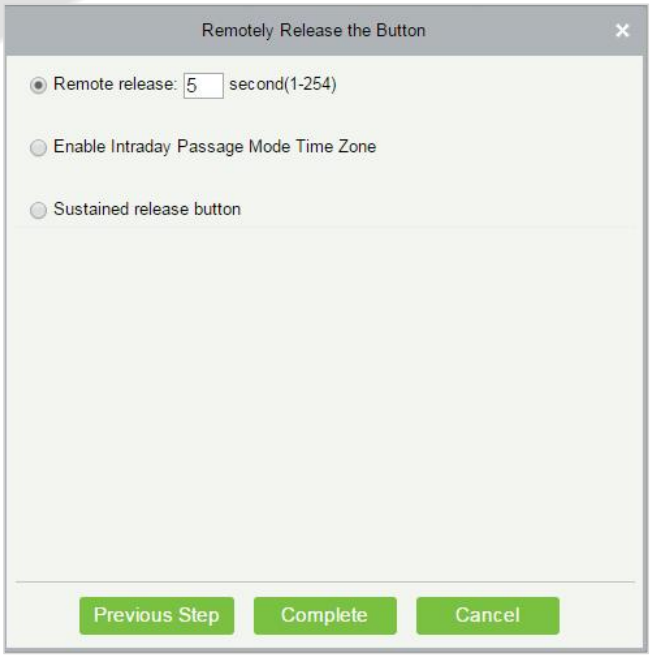


Figure 10- 17 Remotely Release Button

10.3.10.3Remotely Lock the Button

Same as “Remotely Release the button”.

● Remote Release:

It determines whether the corresponding key to the selected floor can be pressed. You can customize the key release duration (15s by default) or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

● Enable Intraday Passage Mode Time Zone:

To close a floor, you must first set Disable Intraday Passage Mode Time Zone to prevent the case that the floor is opened because other continuous open periods take effect. Then, you need to set to close the Remote Lock Button.

● Sustained Release Button:

The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

✍**Note:** If a failure message is always returned for the remote release key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

Select the options, click **Complete** to finish enabling the button.

10.4 Elevator Control Rule

10.4.1Time Zones

In Elevator control, time period is a very important basic concept, which is used to set the use time of floors and specify that Elevator control can be used in effective time period.

The configuration steps to add time period manually.

10.4.1.1New

● Operating Steps:

Step 1: In the Elevator Control module, select "**Elevator Control Rules > Time Period**".

Step 2: Click **Add** to pop up the interface of adding time period.

Step 3: Add the interface in the time period and set the corresponding content according to the new requirements, as shown in figure below Please refer to Table 9-8 for parameter setting instructions.

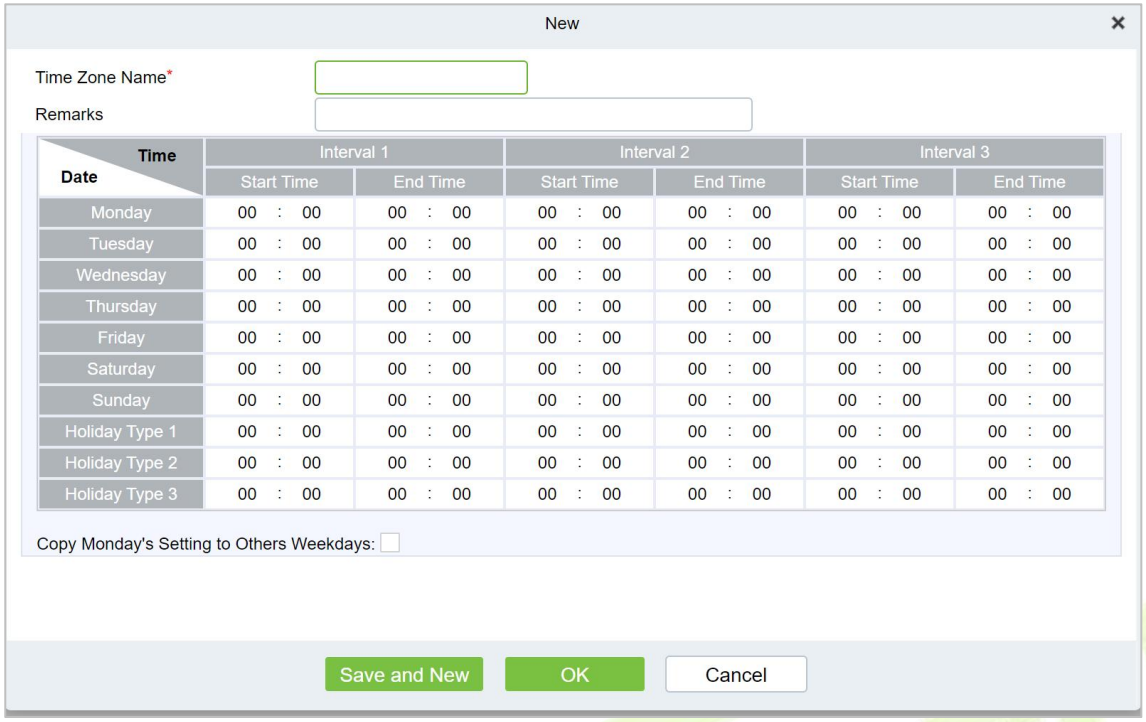


Figure 10- 18 New Time Period

Parameter	How to set
Time Period Name	Custom setting time period name for easy memory.
Remarks	Custom Setting Notes Description.
Time Interval	Set the start and end time in each time interval. Time period includes one week and three holiday type time intervals.
Copy Monday time to other working days	You can quickly copy Monday settings to other workdays.

Table 10- 9 Description of New Parameter Settings in Time Interval

Step 4: Click **OK** to complete the addition of this time period.

10.4.1.2Delete

Step 1: On the **Time Zone** interface, select the required time zone from the list.

Step 2: Click **Delete** or click on the icon to delete the selected time zone.

Step 3: Click **Delete**, to ensure and delete the selected time zone from the list.

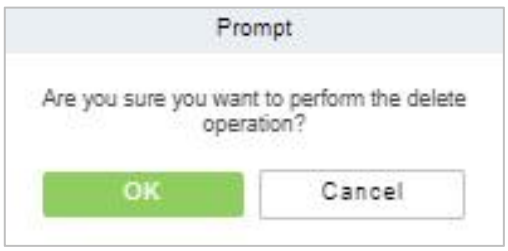


Figure 10- 19 Delete Time Period

10.4.2Holidays

The Elevator control time on holidays may be different from the usual Elevator control time. For simple operation, the system supports setting the Elevator control time separately on holidays.

It introduces the configuration steps of manually adding holidays in.

10.4.2.1New

● Operating Steps:

Step 1: In the **Elevator Control** module, select "Elevator Control Rules > Holidays".

Step 2: Click **New** to pop up the holiday adding interface.

Step 3: In the holiday new interface, set the corresponding content according to the new requirements, as shown in figure below; Please refer to Table 9-9 for parameter setting instructions.

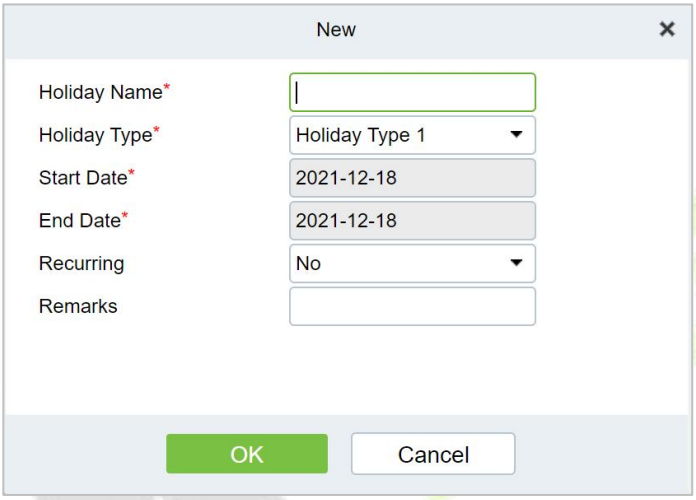


Figure 10- 20 New Holidays

Parameter	How to set
Holiday Name	Customize the holiday name for easy memory.
Holiday Type	Customize the holiday type: Holiday Type 1, Holiday Type 2, Holiday Type 3. The holiday type is set and selected in the "Time Period" addition.
Start Time/End Time	Set the time range for this holiday.
Annualized Cycle	Set whether this holiday cycle year by year: Yes, no. For example, if New Year's Day is January 1 of each year, it can be set to "Yes"; Mother's Day is the second Sunday in May every year. If the date is uncertain, it will be set to "No".
Remarks	Custom settings description.

Table 10- 10 Parameter Setting Description for Holidays

Step 4: Click **OK** to complete the operation of Elevator-controlled holidays.

10.4.2.2Delete

Step 1: On the **Holidays** interface, select the required holidays from the list.

Step 2: Click **Delete** or click on the icon to delete the selected holidays.

Step 3: Click **Delete**, to ensure and delete the selected holidays from the list.

10.4.2.3Import

Step 1: Select and click the "**Download Import Template**" button,download the template "Holiday Template.xls" locally.

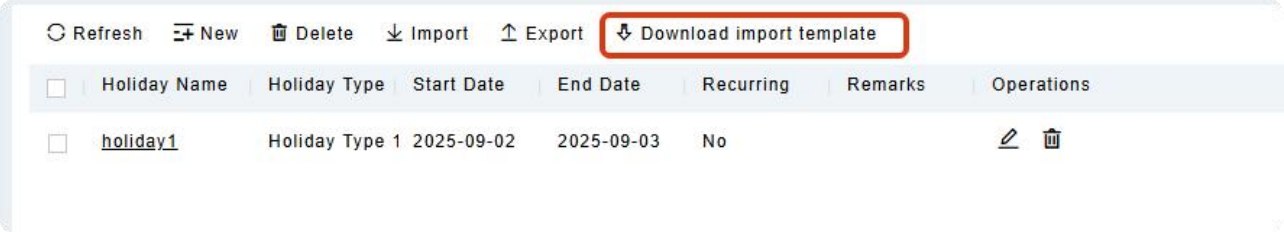
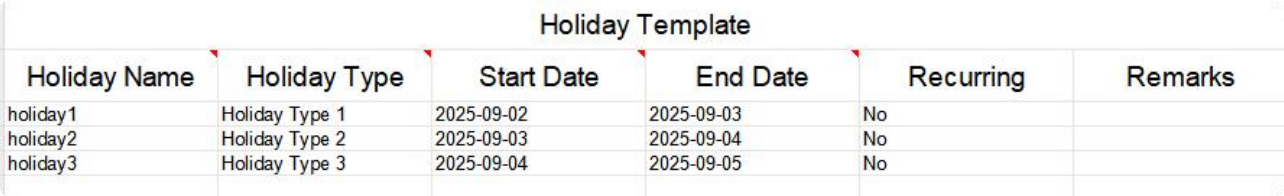


Figure 10- 21 Download Import Template

Step 2: Open the exported template file "Holiday Template.xls" for adding holiday information.



Holiday Template

Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
holiday2	Holiday Type 2	2025-09-03	2025-09-04	No	
holiday3	Holiday Type 3	2025-09-04	2025-09-05	No	

Figure 10- 22 Import Template

Step 4: Select and click the "**Import**" button; click the "**Browse**" button to import the batch import template into the system and click OK, as shown in figure below.

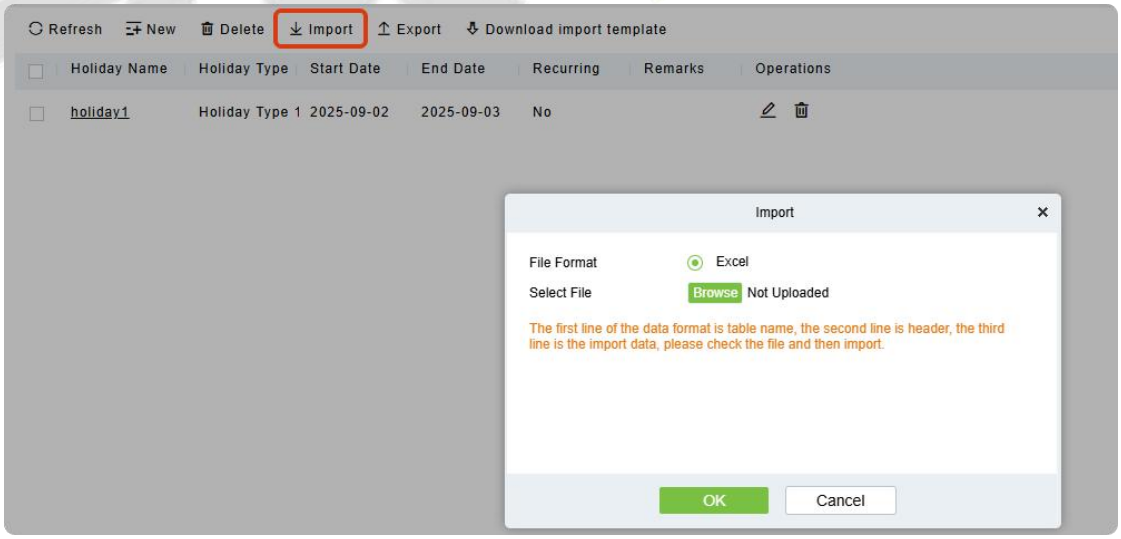


Figure 10- 23 Import

10.4.2.4Export

Click the "**Export**" and set the relevant parameters.

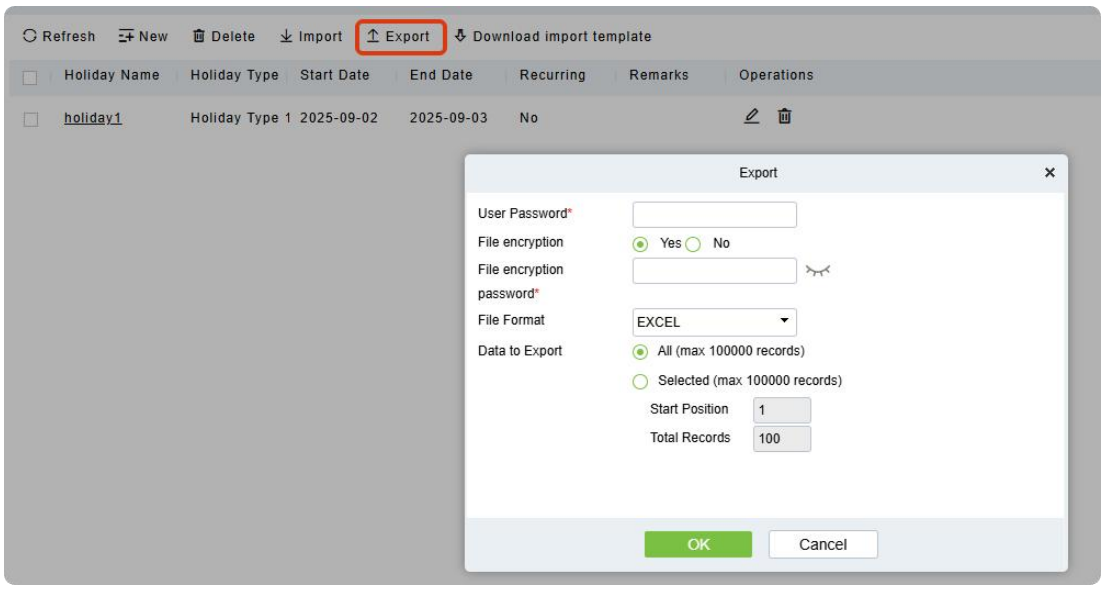


Figure 10- 24 Export

	Holidays					
2	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
3	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
4						

Figure 10- 25 Export

10.4.3Elevator Levels

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

10.4.3.1New

●Operating Steps:

Step 1: Click **Elevator >Elevator Control Rule > Elevator Levels >New** to enter the Add Levels editing interface.

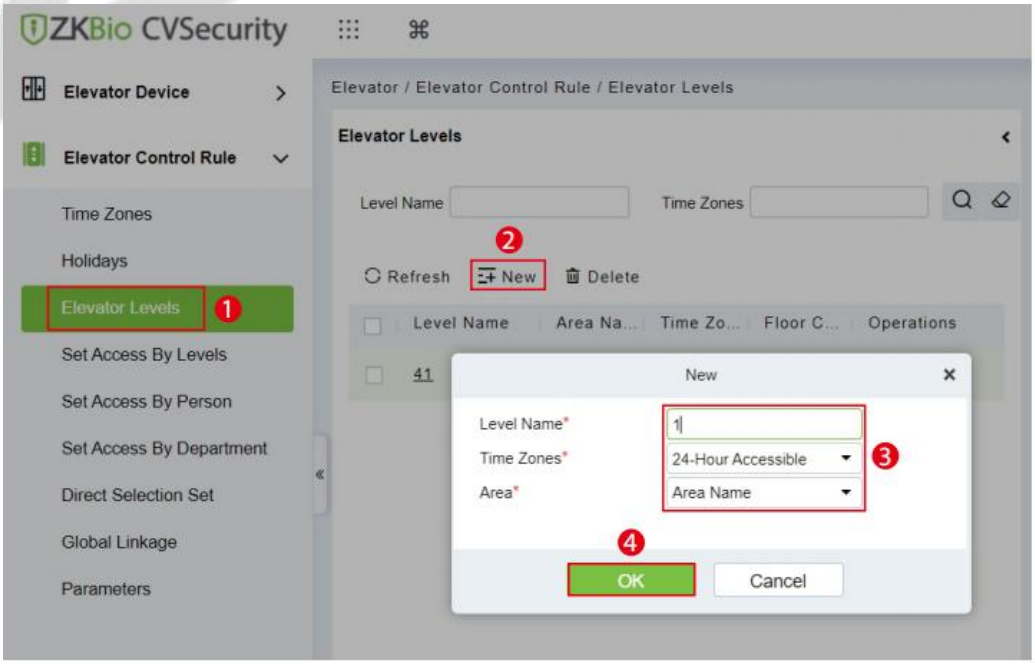


Figure 10- 26 Elevator Level Add Interface

Step 2: Set each parameter: Level Name (unrepeatable), Time Zone and Area.

Step 3: Click **OK**, the system prompts" Add floors to the current elevator control level immediately", click **OK** to add floors, click **Cancel** to return the elevator levels list. The added level is displayed in the list.

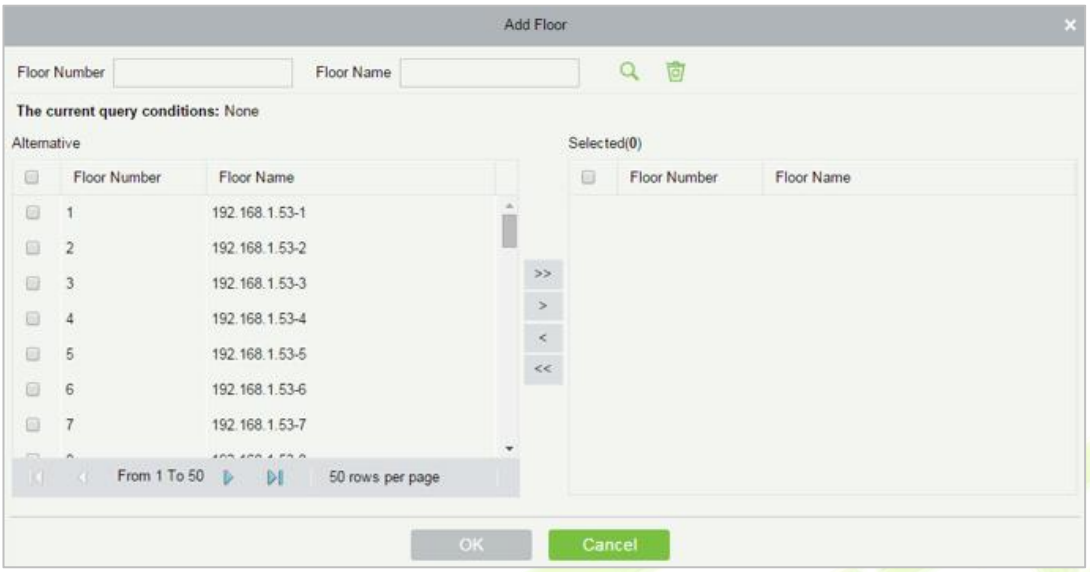


Figure 10- 27 Elevator Level Add Interface

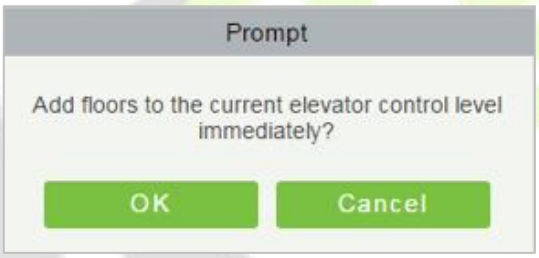


Figure 10- 28 Elevator Level Cancel Interface

✍**Note:** Different floors of different elevator controllers can be selected and added to an elevator level.

10.4.3.2Delete

Step 1: On the **Elevator Level** interface, select the required level from the list.

Step 2: Click **Delete** or click on the icon to delete the selected level floors.

Step 3: Click **Delete**, to ensure and delete the selected level from the list.

10.4.3.3Set Access by Levels

● Operating Steps:

Step 1: Click Elevator > **Set by Levels** to enter the edit interface, Click an Elevator level in left list, personnel having right of opening door in this access level will display on right list.

Step 2: In the left list, click **Add Personnel** under Operations to pop-up the Add Personnel box; select personnel (multiple) and click > to move it to the right selected list, then click **OK** to save and complete.

Step 3: Click the level to view the personnel in the right list. Select personnel and click **Delete Personnel** above the right list, then Click **OK** to delete.

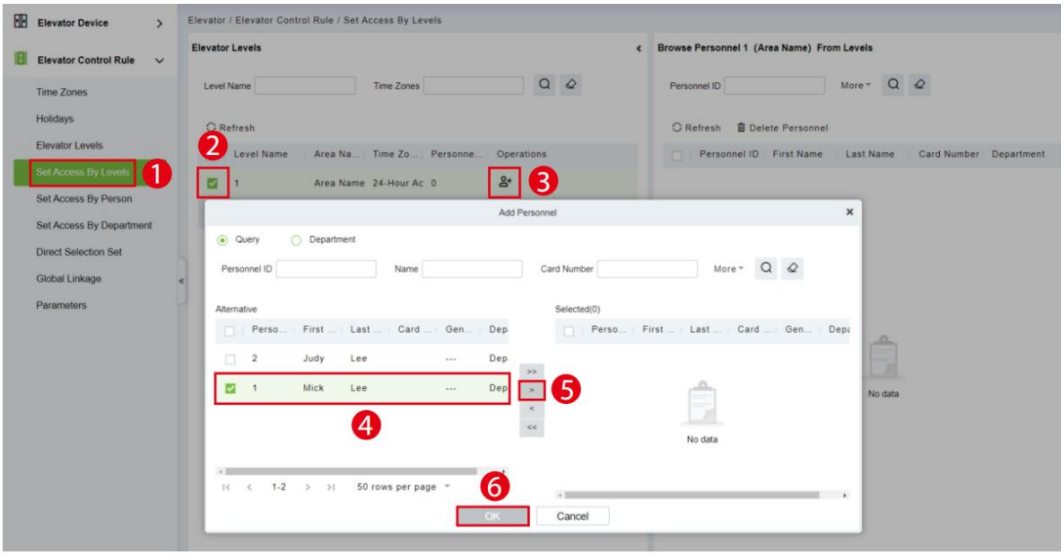


Figure 10- 29 Set Access by Levels

10.4.3.3.1 Delete Personnel

Step 1: On the **Access Level** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon to delete the selected Personnel ID.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

10.4.3.4Set Access by Person

Add selected personnel to selected elevator levels or delete selected personnel from the elevator levels.

● Operating Steps:

Step 1: Click **Elevator** > **Elevator Levels** > **Set by Person**, click employee to view the levels in the right list.

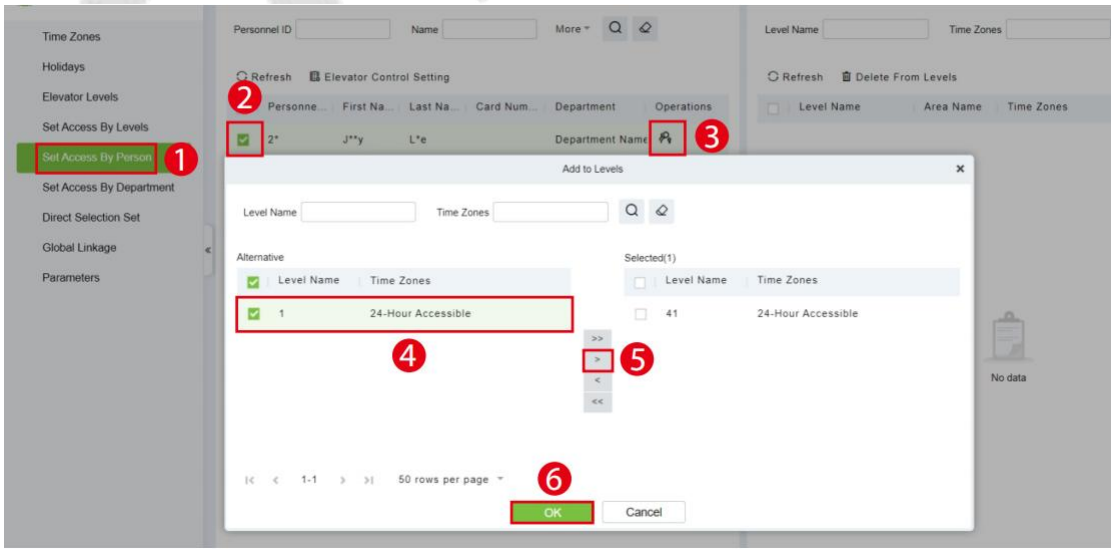


Figure 10- 30 Set Access by Person Interface

10.4.3.4.1 Delete from Levels

Step 1: Select Level (multiple) in the right list and click **Delete from levels** above the list, then click **OK** to delete the selected levels.

10.4.3.4.2 Elevator Control Setting

● Setting Levels for Selected Personnel:

Step 1: Select a person in the list on the left and click **Elevator Control Setting**. The following page is displayed:

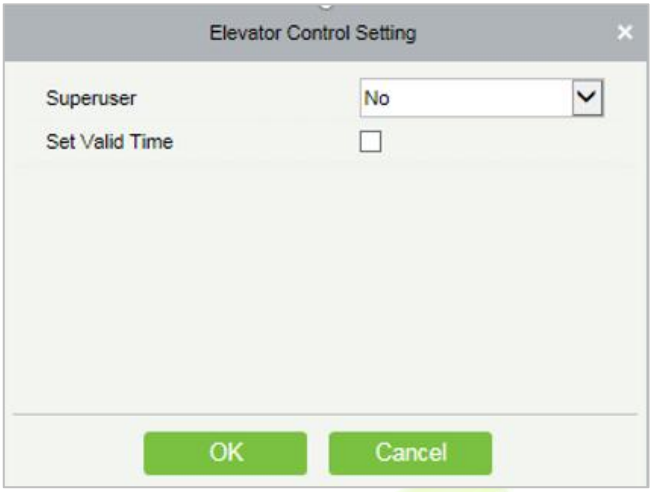


Figure 10- 31 Elevator Control Setting

Step 2: In the left list, click **Add Personnel** under Operations to pop-up the Add Personnel box; select personnel (multiple) and click > to move it to the right selected list, then click **OK** to save and complete.

10.4.3.5 Set Access by Department

● Operating Steps:

Step 1: Add selected department to selected elevator levels or delete selected department from the elevator levels. The access of the staff in the department will be changed.

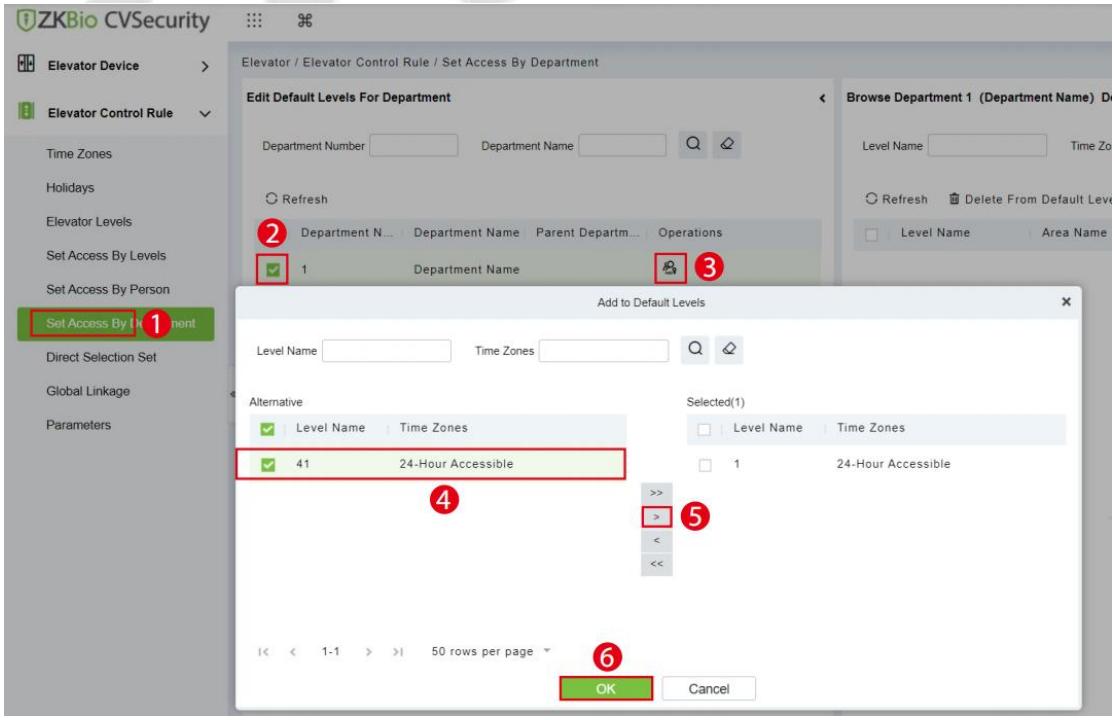


Figure 10- 32 Set Access by Department

10.4.3.5.1 Delete from Default Levels

Select Level (multiple) in the right list and click **Delete from levels** above the list, then click **OK** to delete the selected levels.

10.4.3.6Direct Selection Set (EC16)

Assign the user the right to go directly to the floor, then the user can reach the target floor after verification.

Operating Steps:

Step 1: Click **Elevator Control Rule** > **Direct Selection Set**.

Step 2: Selected target personnel.

Step 3: Click to add direct selection layer.

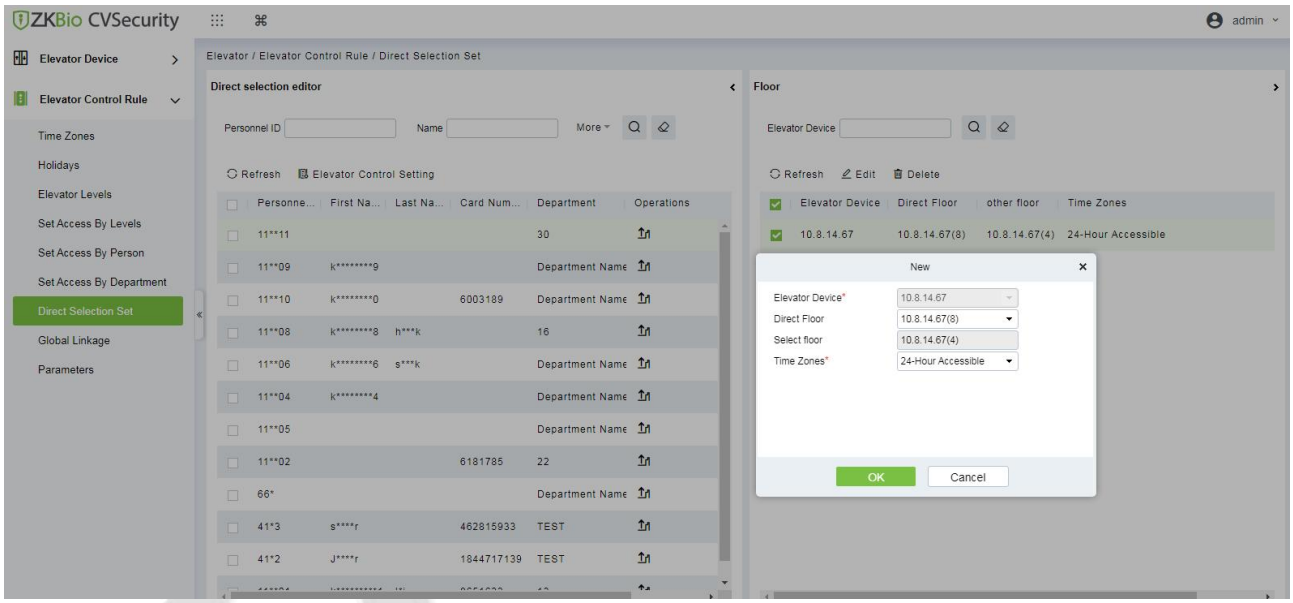


Figure 10- 33 Direct Selection Set

Parameter	Instructions
Elevator Device	Select the elevator device of the controller.
Direct Floor	After the verification is completed, you can reach the designated floor.
Select Floor	Floors that users can reach in addition to direct floors. After the first verification, the elevator can reach the direct floor. At this time, it needs to be verified again before the user can press the elevator button to reach the selected floor.
Time Zones	The period of time that the user is allowed to use the elevator.

Table 10- 11 Description of Direct Selection Set

10.4.3.7Global Linkage

The use method and scene of linkage are very flexible. After a specific event is triggered at an input point in the Elevator control system, a linkage action will be generated at the designated output point to control the events such as door opening, alarm and abnormality in the system.

10.4.3.7.1 New

●Operating Steps:

Step 1: In the **Elevator Control** module, select "Elevator Control Rules > Global Linkage".

Step 2: In the linkage setting interface, select and click the **Add** button, as shown in figure below, and refer to Table 9-11 for linkage parameter setting.

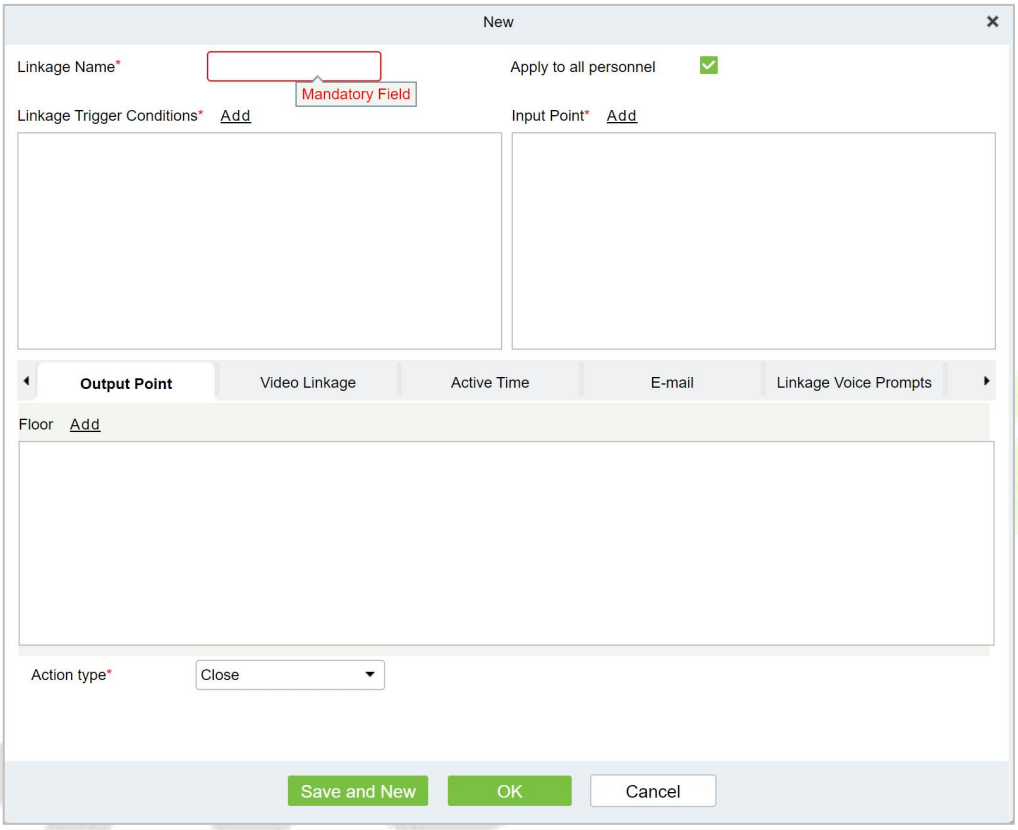


Figure 10- 34 New Linkage Configuration Interface

Parameter	How to set
Linkage Name	Custom setting linkage name for easy reference
Linkage Trigger Condition	Select the condition that the linkage operation triggers, that is, the type of event generated by the selected device
Input Point	Select the input point to set the device input
Output Point	Select the output point to set the output of the device
Linkage Action Setting	Select and set linkage action, including device operation at output point, video linkage and mail

Table 10- 12 New Linkage Parameter Setting Description

Step 5: Click **OK** to complete the linkage configuration.

10.4.3.7.2 Delete

Step 1: On the **Elevator** interface, select the required linkage from the list.

Step 2: Click **Delete** or click on the icon to delete the selected linkage.

Step 3: Click **Delete**, to ensure and delete the selected linkage from the list.

10.4.3.7.3 Enable/Disable

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

10.4.3.7.4 Delete Personnel

Step 1: On the **Elevator** interface, select the required Personnel ID of the Global Linkage from the list.

Step 2: Click **Delete** or click on the icon to delete the selected Personnel ID.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

10.4.4Parameters

● Operating Steps:

Step 1: Click **Elevator** > **Elevator** > **Parameters**:

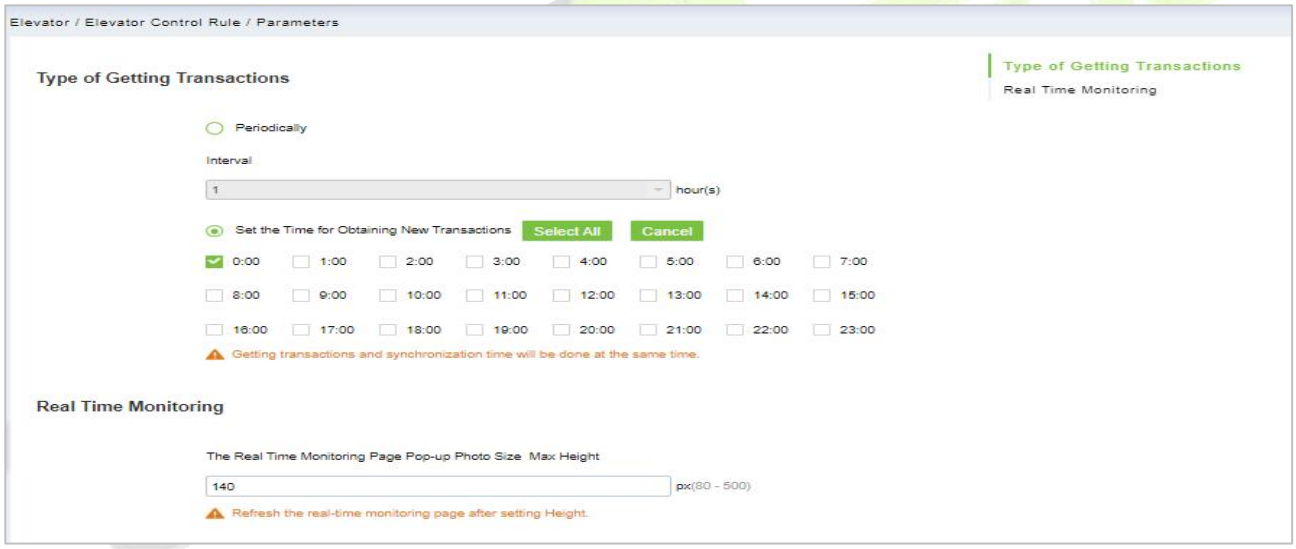


Figure 10- 35 Parameters Interface

Parameter	How to set
Type of Getting Transaction	Start from the setting and efficient time, the system attempts to download new transactions every time interval.
Real Time Monitoring	When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

Table 10- 13 Parameter Setting Description

10.5 Elevator Control Reports

10.5.1 All Transaction

The system displays the latest three months transactions by default. As the data size of elevator access control event records is large, you can view elevator access control events as specified condition when querying.

10.5.1.1 Clear All Data

● Operating Steps:

Step 1: Click **Elevator Control Reports** > **All Transactions** to view all transactions:

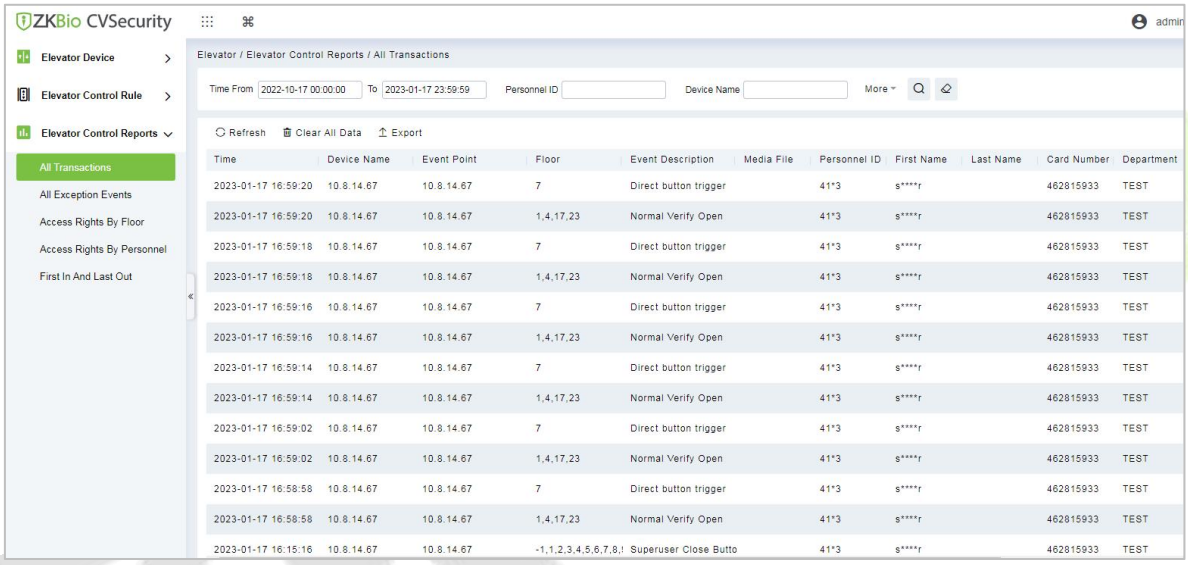


Figure 10- 36 All Transaction Interface

Step 2: Click **Clear All Data** to pop up prompt and click **OK** to clear all transactions.

10.5.1.2 Export

You can export all transactions in Excel, PDF, CSV format.

All Transactions

Time	Device Name	Event Point	Floor	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area
2023-01-17 16:59:20	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:20	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:18	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:18	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:16	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:16	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:14	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:14	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:02	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:59:02	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:58:58	10.8.14.67	10.8.14.67	7	Direct button trigger	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:58:58	10.8.14.67	10.8.14.67	1,4,17,23	Normal Verify Open	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name
2023-01-17 16:15:16	10.8.14.67	10.8.14.67	-1,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31	Superuser Close Buttons	4143	summer		462815933	TEST	10.8.14.67-Reader1	Card	Area Name

Figure 10- 37 All Transaction Export Interface

10.5.2All Exception Events

10.5.2.1Clear All Data

● Operating Steps:

Step 1: Click **Reports** > **All Exception Events** to view exception events in specified condition. The options are same as those of **All Transactions**.

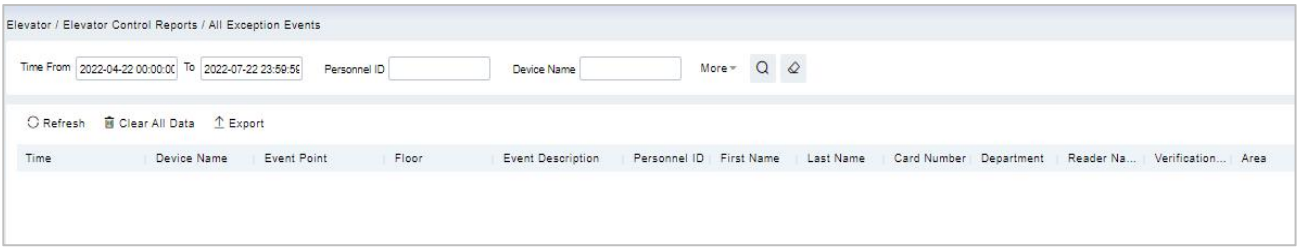


Figure 10- 38 All Exception Events Interface

Step 2: Click **Clear All Data** to pop up prompt, click **OK** to clear all exception events.

10.5.2.2Export

Step 1: You can export all exception events in Excel, PDF, CSV format.

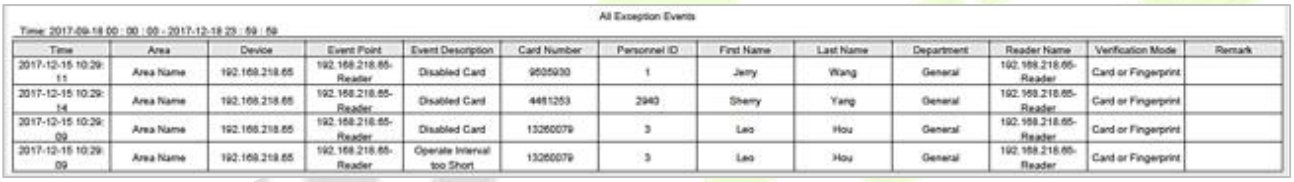


Figure 10- 39 All Exception Events Export Interface

10.5.3Access Rights By Floor

● Operating Steps:

Step 1: Click **Reports** > **Access Rights by Floor**, the data list in the left side shows all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.

Figure 10- 40 Access Right by Floor Interface

10.5.3.1Export

Step 1: You can export all the personnel having access levels to the floor data in Excel, PDF, CSV format

192.168.218.65-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department

Figure 10- 41 Access Right by Floor Export Interface

10.5.4Access Rights By Personnel

●Operating Steps:

Step 1: Click **Reports** > **Access Rights by Personnel**, the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

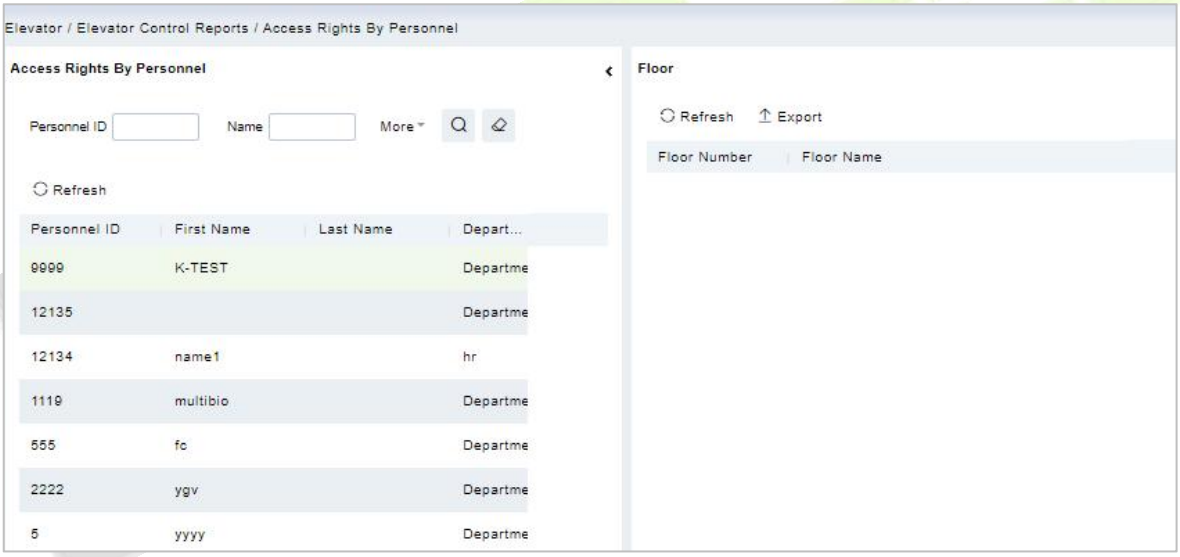


Figure 10- 42 Access Right by Personnel Interface

10.5.4.1Export

Step 1: You can e export all the floor information in Excel, PDF, CSV format.

2940(Sherry) Having Level to Access

Floor Number	Floor Name
1	192.168.218.65-1
2	192.168.218.65-2
3	192.168.218.65-3
4	192.168.218.65-4
5	192.168.218.65-5
6	192.168.218.65-6
7	192.168.218.65-7
8	192.168.218.65-8
9	192.168.218.65-9
10	192.168.218.65-10

Figure 10- 43 Access Right by Personnel Export Interface

10.5.5First In and Last Out

Click **Elevator Controls Reports** > **First In And Last Out** to view the First and the Last time interval.

10.5.5.1Clear All Data

Click **Clear All Data** to pop up prompt and click **OK** to clear all transactions.

10.5.5.2Export

You can export all transactions in Excel, PDF, CSV format.

10.6 Elevator Integration

10.6.1Service Config

Login to the ZKBio CVSecurity Software, and click **Elevator Module**, click **Elevator Integration** > **Service Config** > **New**, and fill in the information.

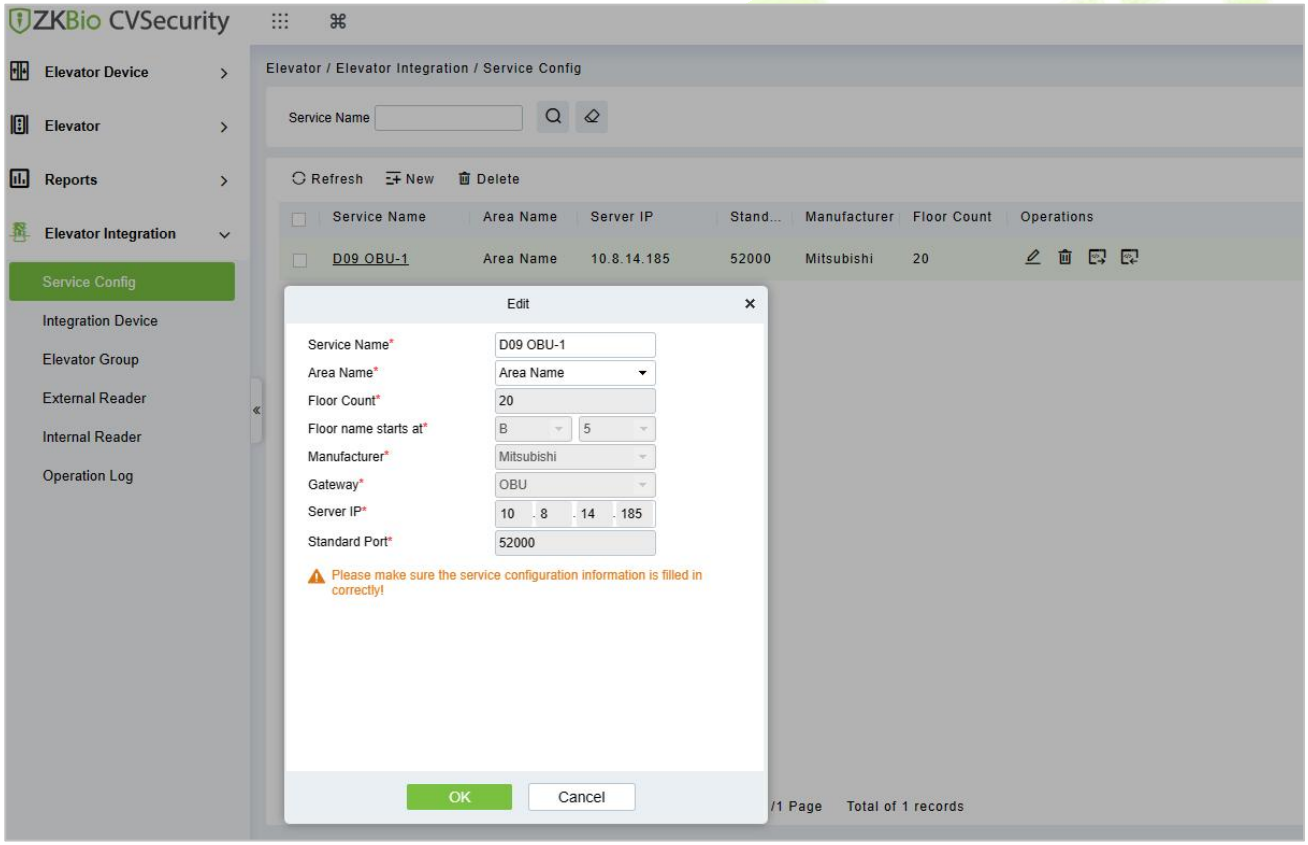


Figure 10- 44 New Service Config Interface

Parameter	How to set
Service Name	User-defined.
Area Name	Based on the actual situation.
Floor Count	Based on the actual situation.

Floor name starts at	Based on the actual situation.
Manufacturer	Mitsubishi.
Gateway	ELSGW/OBU.
Server IP	The computer IP where the ELSGW Emulator is installed.
Standard Port	52000(default).

Table 10- 14 Parameter Setting Description

Click **Set external global mask**, and select the arrive situation according to the actual situation.

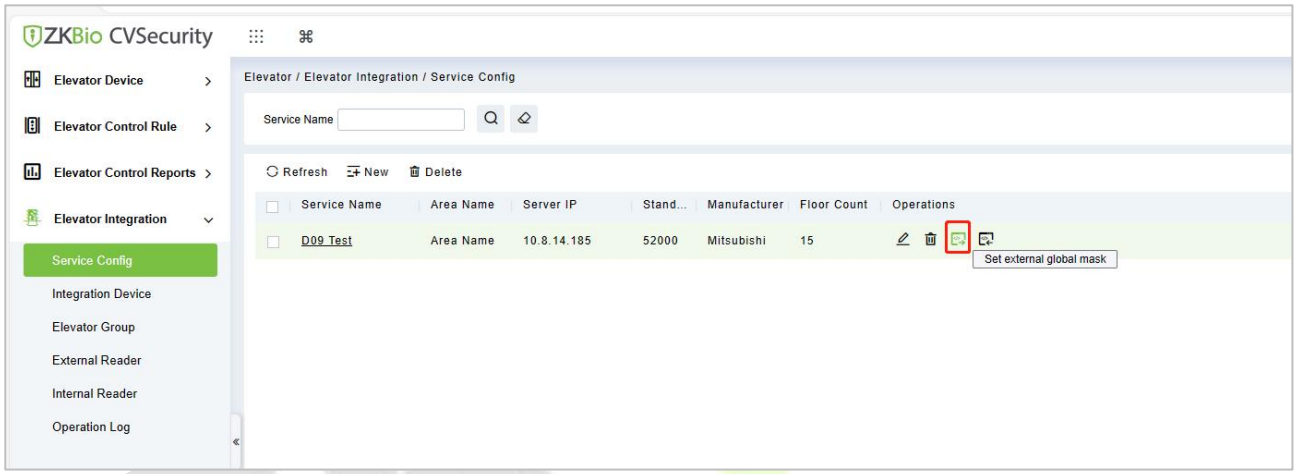


Figure 10- 45 Set External Global Mask Interface

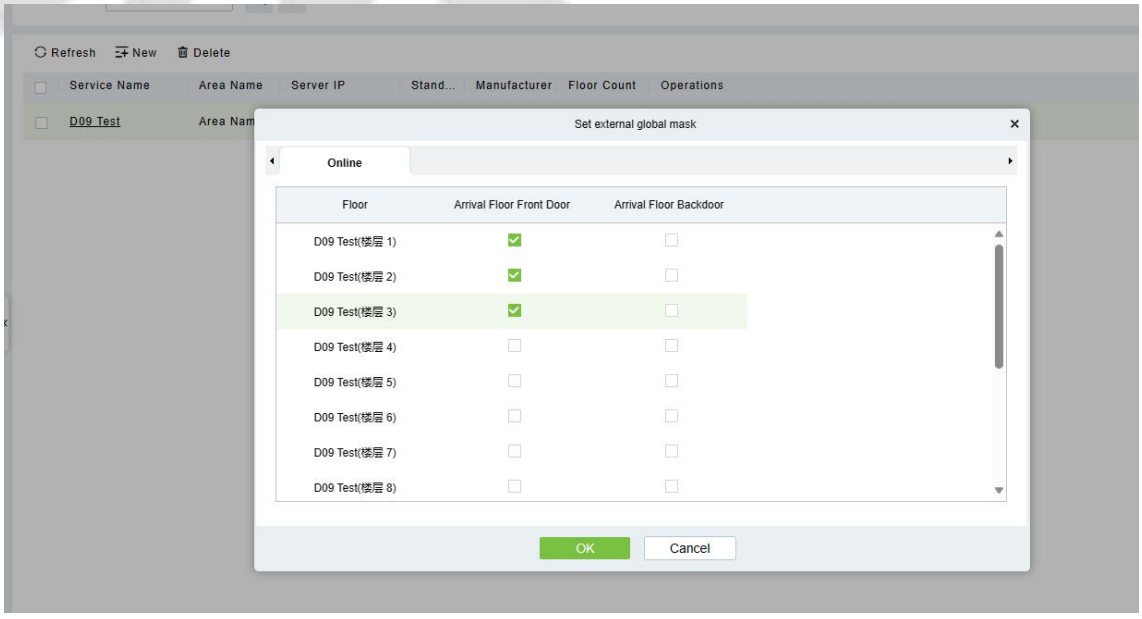


Figure 10- 46 Set External Global Mask setting Interface

Click **Set internal global mask**, and select the internal situation according to the actual situation.

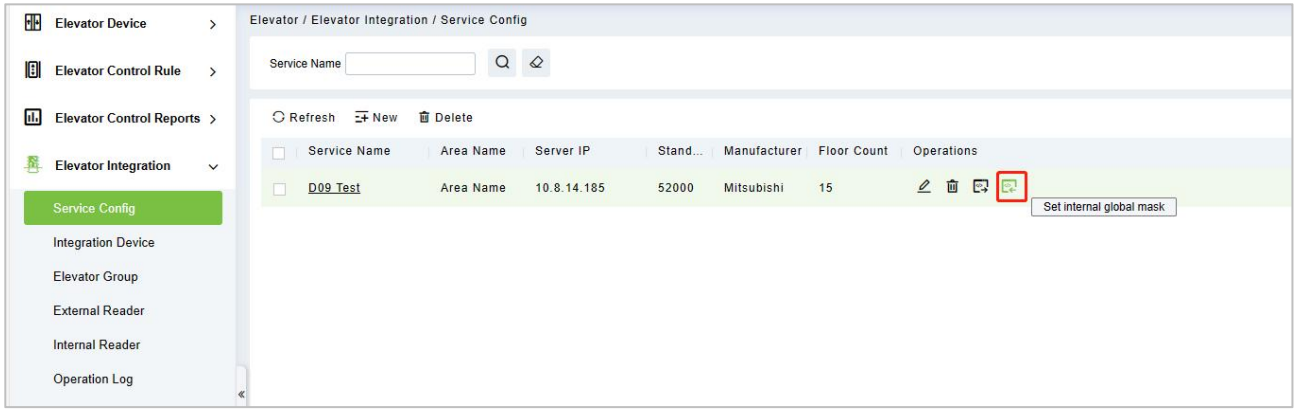


Figure 10- 47 Set Internal Global Mask Interface

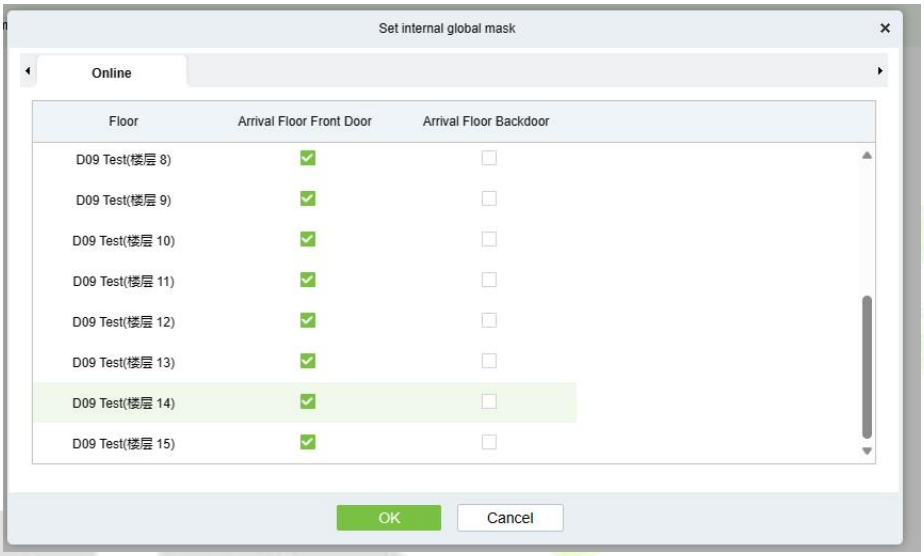


Figure 10- 48 Set Internal Global Mask Setting Interface

10.6.2Integration Device

In the Elevator > Elevator Integration > Integration Device> New, add the related access control devices.

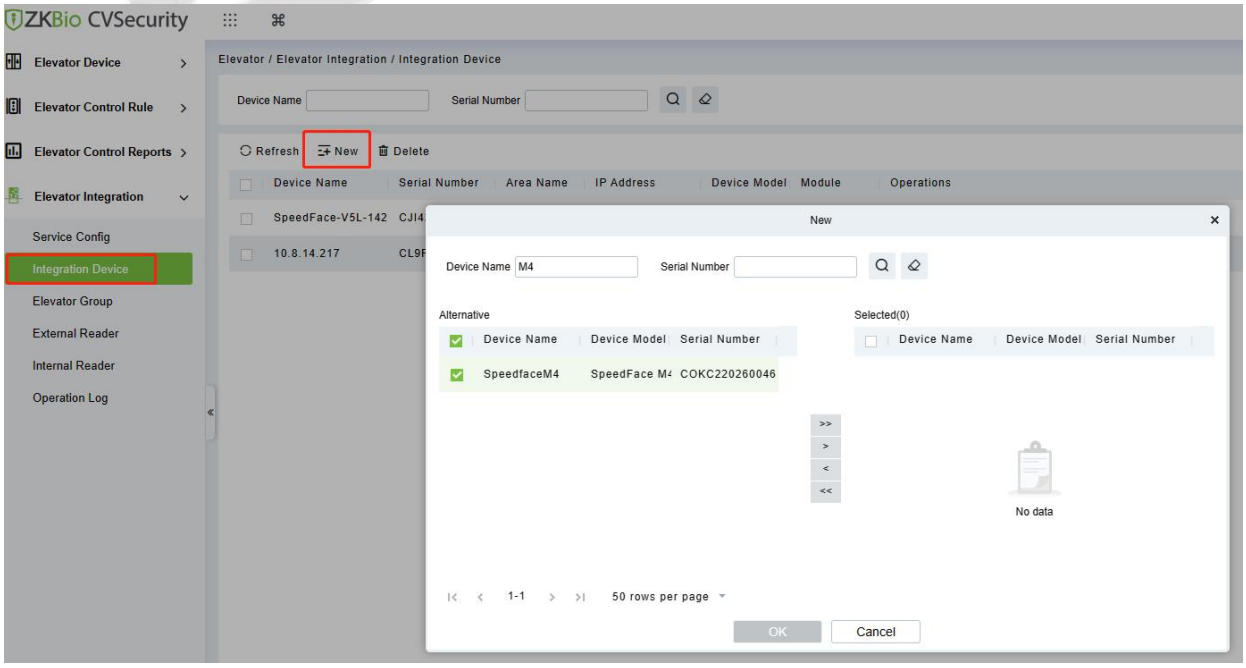


Figure 10- 49 New Integration Device Interface

10.6.3Elevator Group

In the **Elevator > Elevator Integration > Elevator Group> New**, fill in the group name and group number, and select the service that we just added.

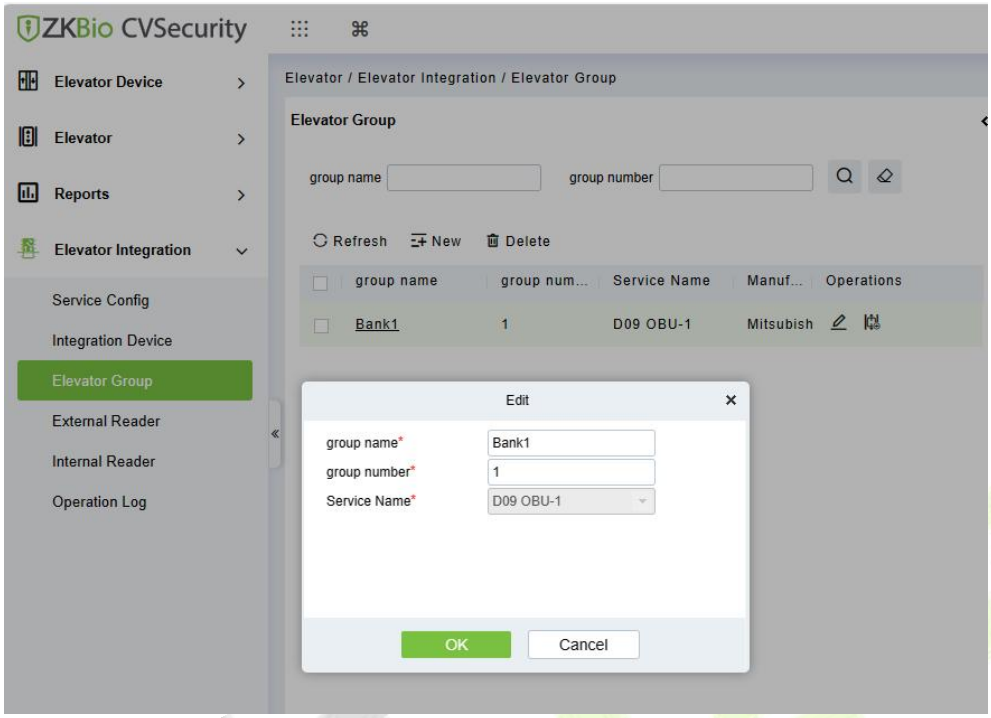


Figure 10- 50 New Elevator Group Interface

Then add the Elevator for the elevator group.

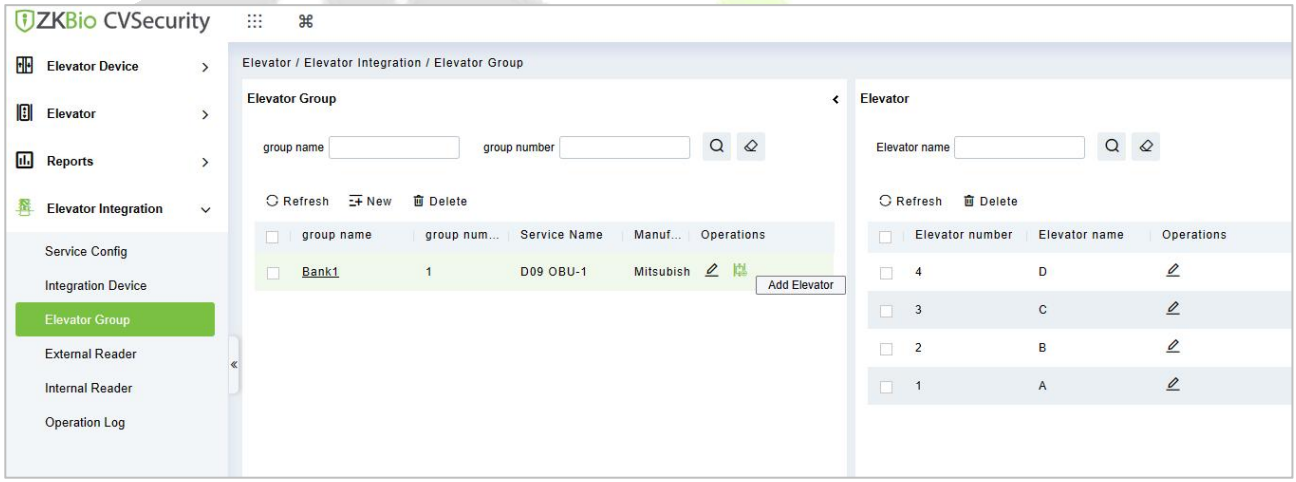


Figure 10- 51 Elevator Group Interface

10.6.4External Reader

Eternal Reader refers to the reader installed outside the elevator, generally used for DOP/HOP.

In the Elevator > Elevator Integration > External Reader> New, and fill in the information.

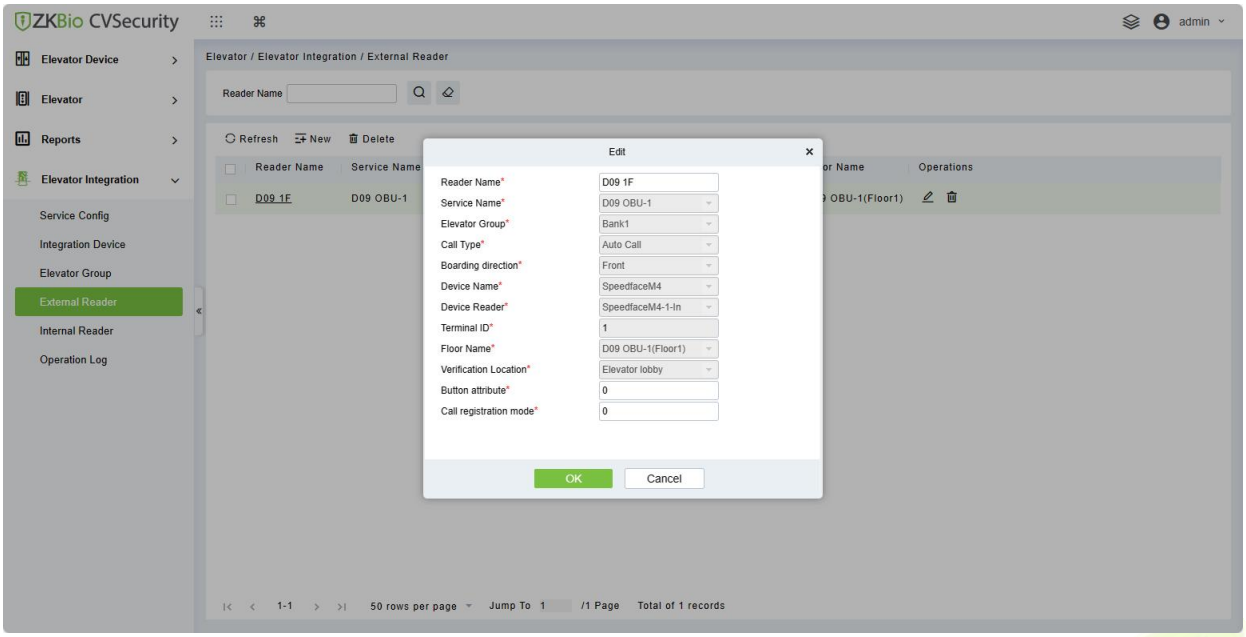


Figure 10- 52 New External reader Interface

Parameter	How to set
Reader Name	User-defined.
Service Name	Select corresponding service that added in Service Config.
Elevator Group	Select corresponding elevator group that added in Elevator Group.
Call Type	**Option 1. Manual Call:** which means manually calling the destination floor. **Option 2: Auto Call**, which means the system automatically calls the user's default floor.
Boarding direction	Based on the actual situation: **Front / Rear.**
Device Name	User-defined.
Device Reader	Select the integration device based on the actual situation.
Terminal ID	User-defined.
Floor Name	Select the floor according to the actual situation.
Verification Location	Based on the actual situation: Elevator lobby / Entrance / Room / Security gate.
Button attribute	User-defined.
Call registration mode	User-defined.

Table 10- 15 Parameter Setting Description

10.6.5Internal Reader

Internal Reader refers to the reader installed outside the elevator, generally used for COP.

Click **Elevator > Elevator Integration> Internal Reader> New**, and fill in the relevant information.

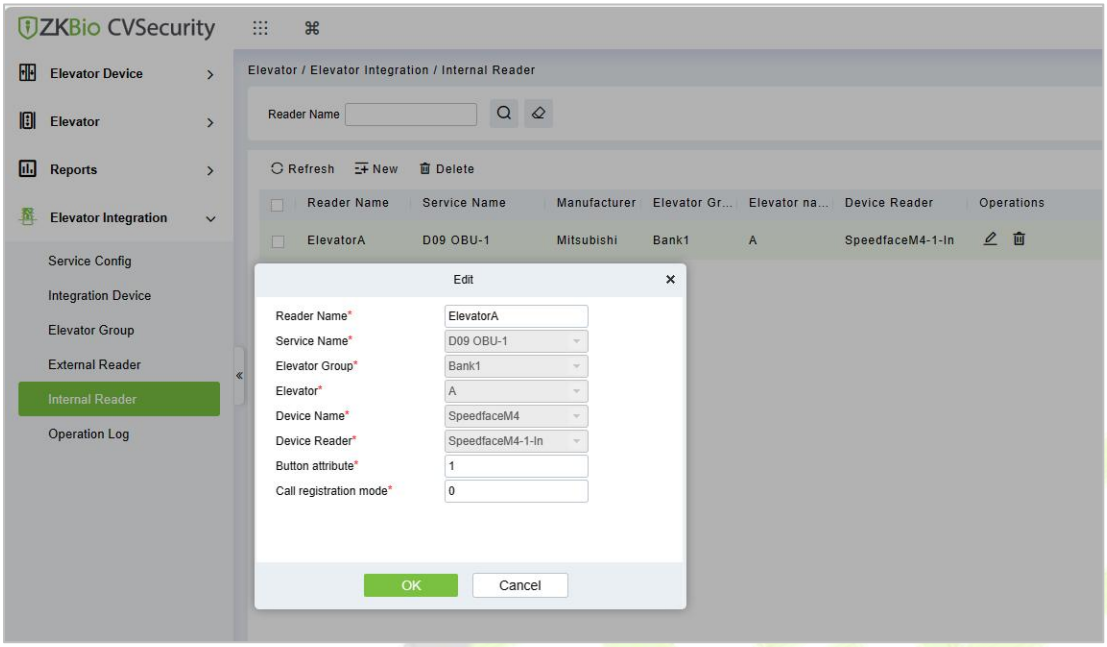


Figure 10- 53 New Internal Reader Interface

Parameter	How to set
Reader Name	User-defined.
Service Name	Select corresponding service that added in Service Config.
Elevator Group	Select corresponding elevator group that added in Elevator Group.
Elevator	Select the elevator based on the actual situation.
Device Name	User-defined.
Device Reader	Select the integration device based on the actual situation.
Button attribute	User-defined.
Call registration mode	User-defined.

Table 10- 16 Parameter Setting Description

ZKBio CVSecurity-Mitsub

For more information, please refer to the following materials .

11 Consumption (Offline)

The devices for which the offline consumption module is applicable are Promerc 10, Peomerc 20.

11.1 Consumption System

This module allows the user to set up a consumption system with the device and realize their functions. The device can be set as either a “Consumer Machine”, a “Cashier Machine” or a “Subsidy Machine”. The “Consumer machine” type combines various consumption modes to meet the diversified consumption requirements such as fixed value mode or amount mode. The “Cashier Machine” type realizes the device recharge and refund function. The “Subsidy machine” type is used to receive allowances/subsidies. This module will collect the data from the device and summarize it on the various consumption reports. It can also perform various operations like issue card, card return, card suspend and resume, and other operations through the card reader connected to the software.

11.1.1 Consumption Basic Management

11.1.1.1 Piecewise Fixed Value

Piecewise Fixed value is the value and validity of a card which is supposed to be used on the consumer device.

Click **Consumption Basic Management** > **Piecewise Fixed Value** as shown in the following figure:

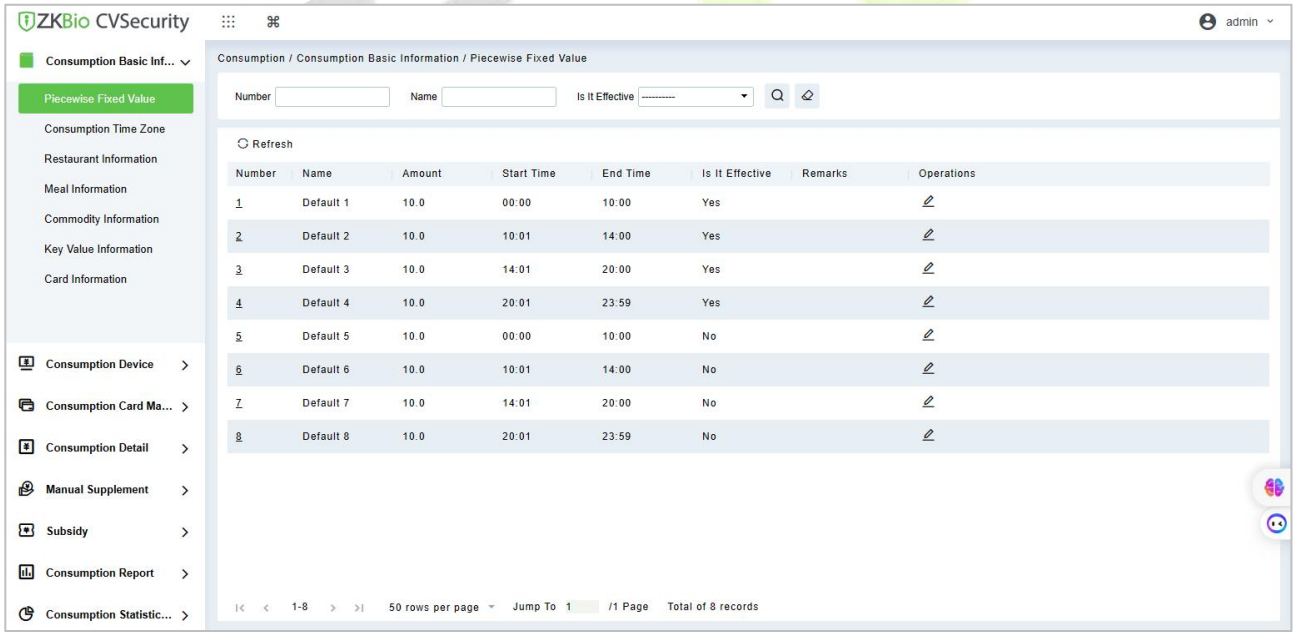


Figure 11- 1

● Edit:

By default, there are eight values, click **Edit** on the operation column to open the modification dialog box.

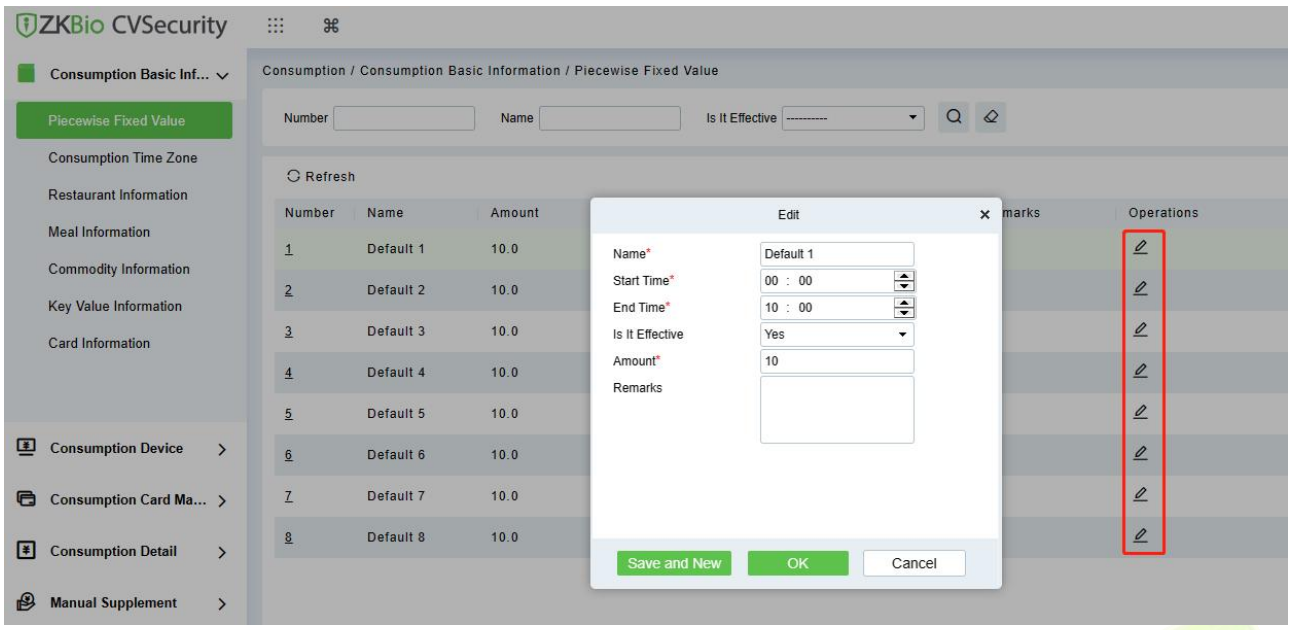


Figure 11- 2

You can provide the desired information in the dialog box which include: **Name**, **Start time**, **End time**, **Whether Effective** (status of the card), **Amount**, and **Remarks**.

11.1.1.2Consumption Time Zone

Click **Consumption Basic Management** > **Consumption Time Zone** as shown in the following figure:

By default, the system has some Consumption Time zones, you can select and edit according to your preferences.

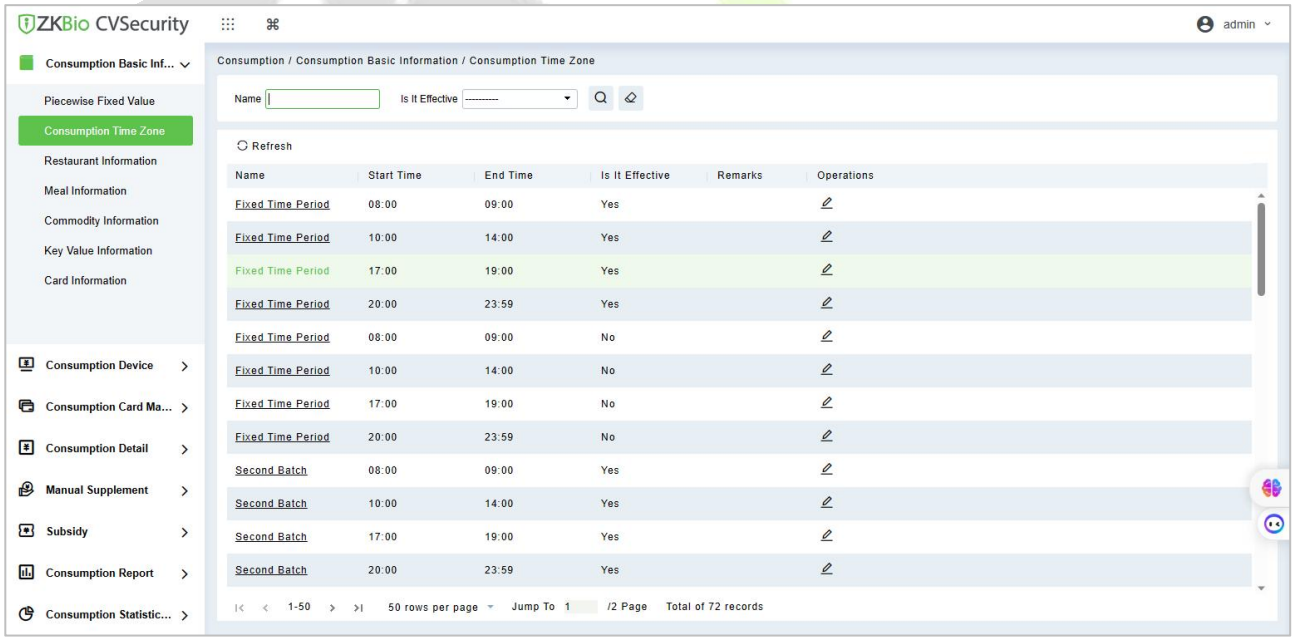


Figure 11- 3

● Edit:

Click **Edit** column on the operation column to open the modification dialog box.

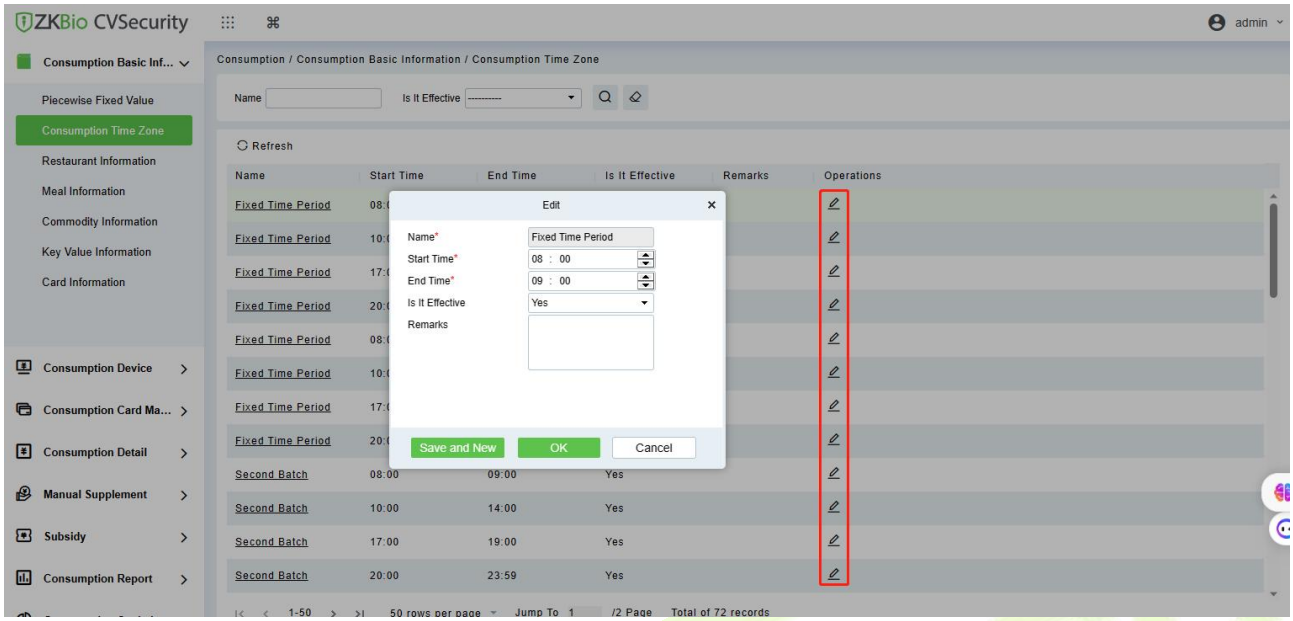


Figure 11- 4

On the dialog box, you can select the required **Start time**, **End time**, **Whether Effective**, and **Remarks** (optional), as shown in the above figure. After providing the information, click **OK**.

11.1.1.3 Restaurant Information

By default, a Restaurant name is already added, you can edit it and also add new ones.

Click **Consumption Basic Management** > **Restaurant Information**, shown as following figure:

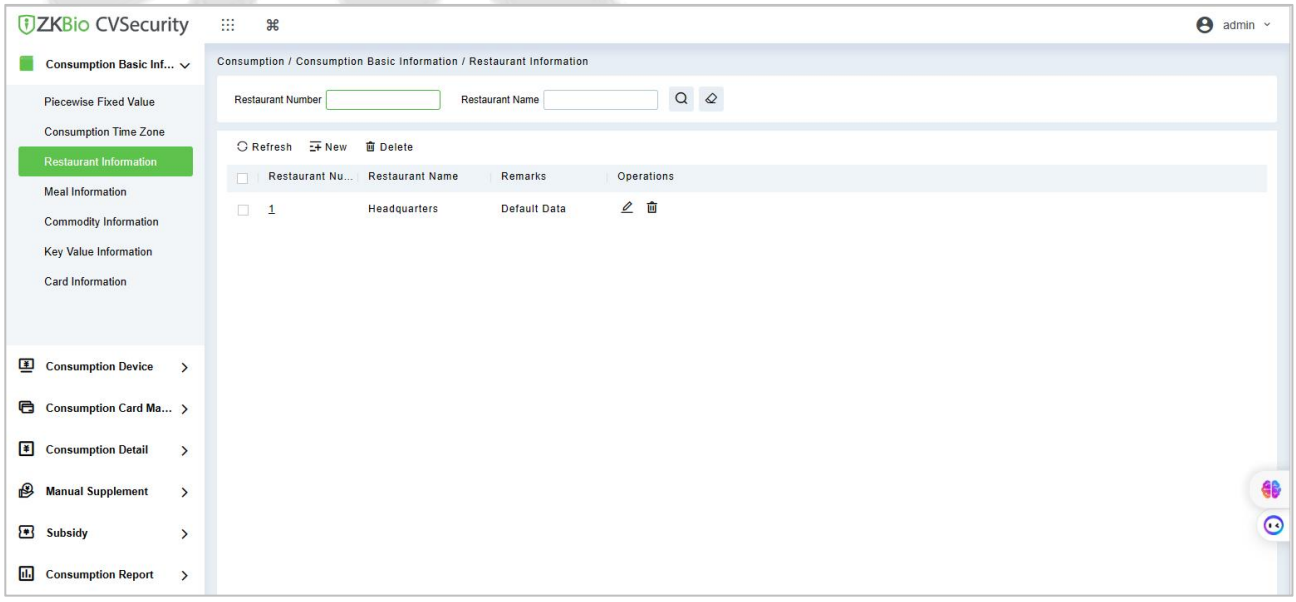


Figure 11- 5

● New:

Click **New**, to add a restaurant.

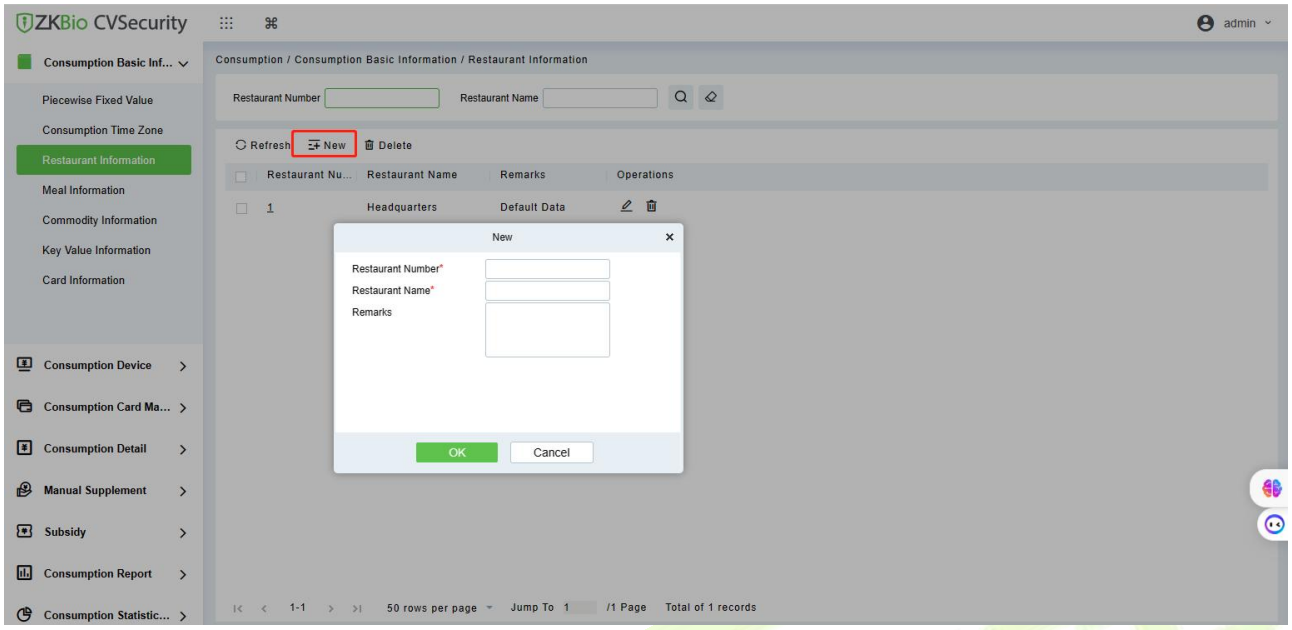


Figure 11- 6

Type the preferred Restaurant number, Restaurant name, and Remarks (optional) information, and then click **OK** to save and close or click **Save and New** for continue adding.

● Delete:

You can directly click **Delete** on the required hotel to remove it from the system.

Figure 11- 7

For deleting in batch, select the required hotel(s) as shown below and click **Delete**. The default restaurant number 1 cannot be deleted.

Figure 11- 8

● Edit:

Click **Edit** in the operation column to open the modification dialog box.

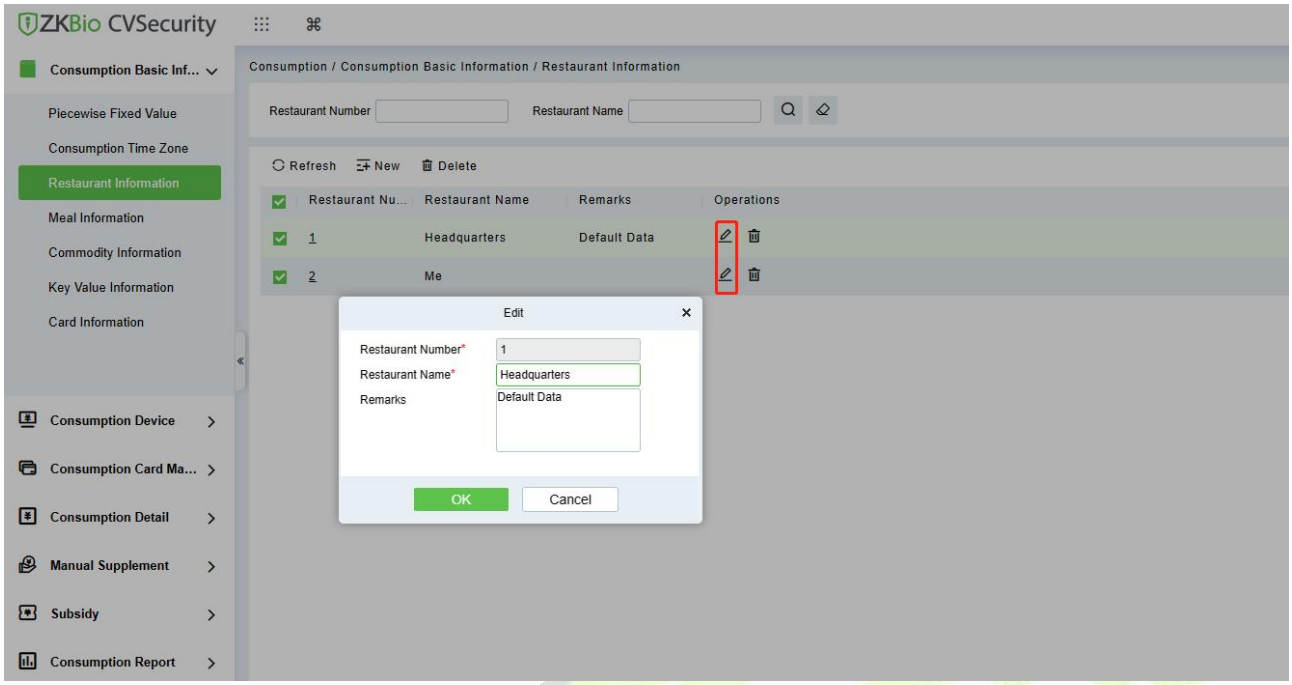


Figure 11- 9

11.1.1.4Meal Information

Click **Consumption Basic Management** > **Meal Information**, shown as following figure:

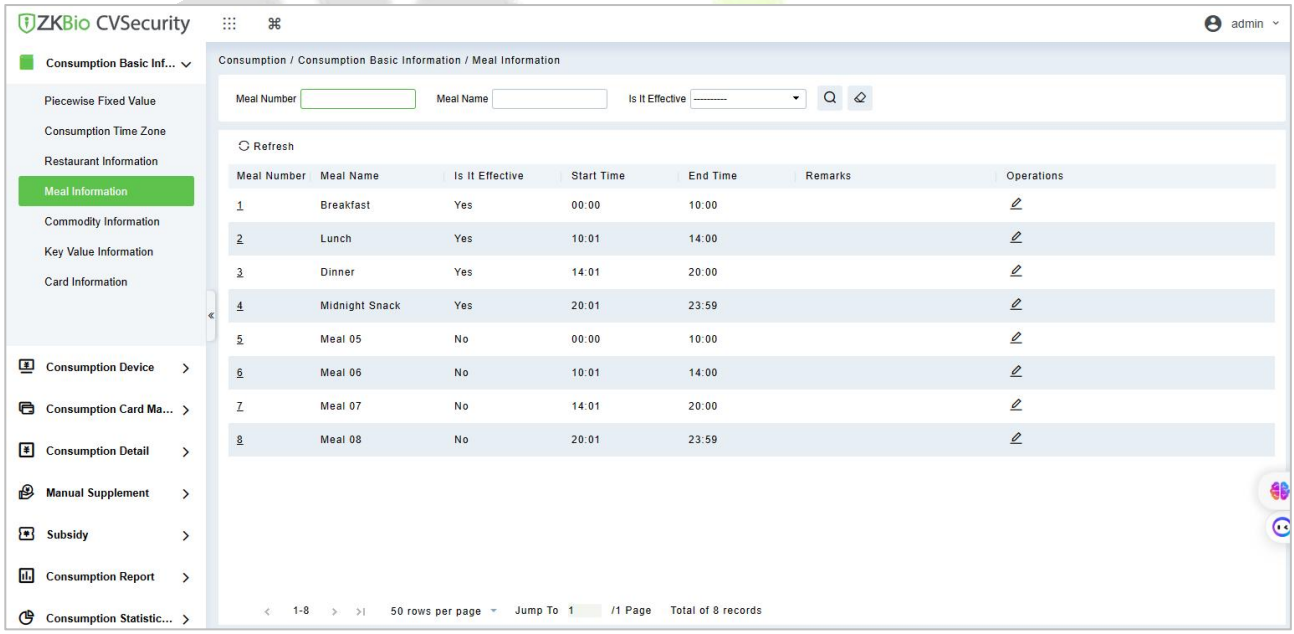


Figure 11- 10

● Edit:

Click on the meal number of list and the edit column of the operation to pop up the modification dialog box.

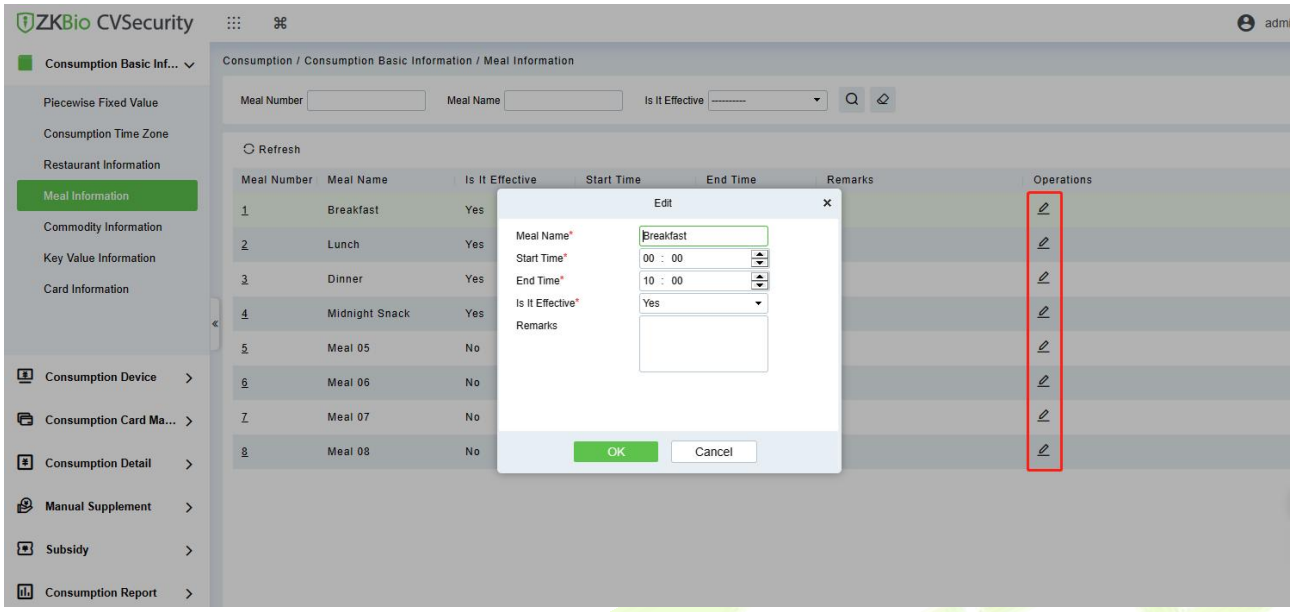


Figure 11- 11

Enter the information in the dialog box which include: **Meal Name**, **Start Time**, **End time**, **Whether Effective** (status), **Remarks** (optional) and then click **OK** to save.

11.1.1.5Commodity Information

Click **Consumption Basic Management** > **Commodity Information** as shown in the following figure:

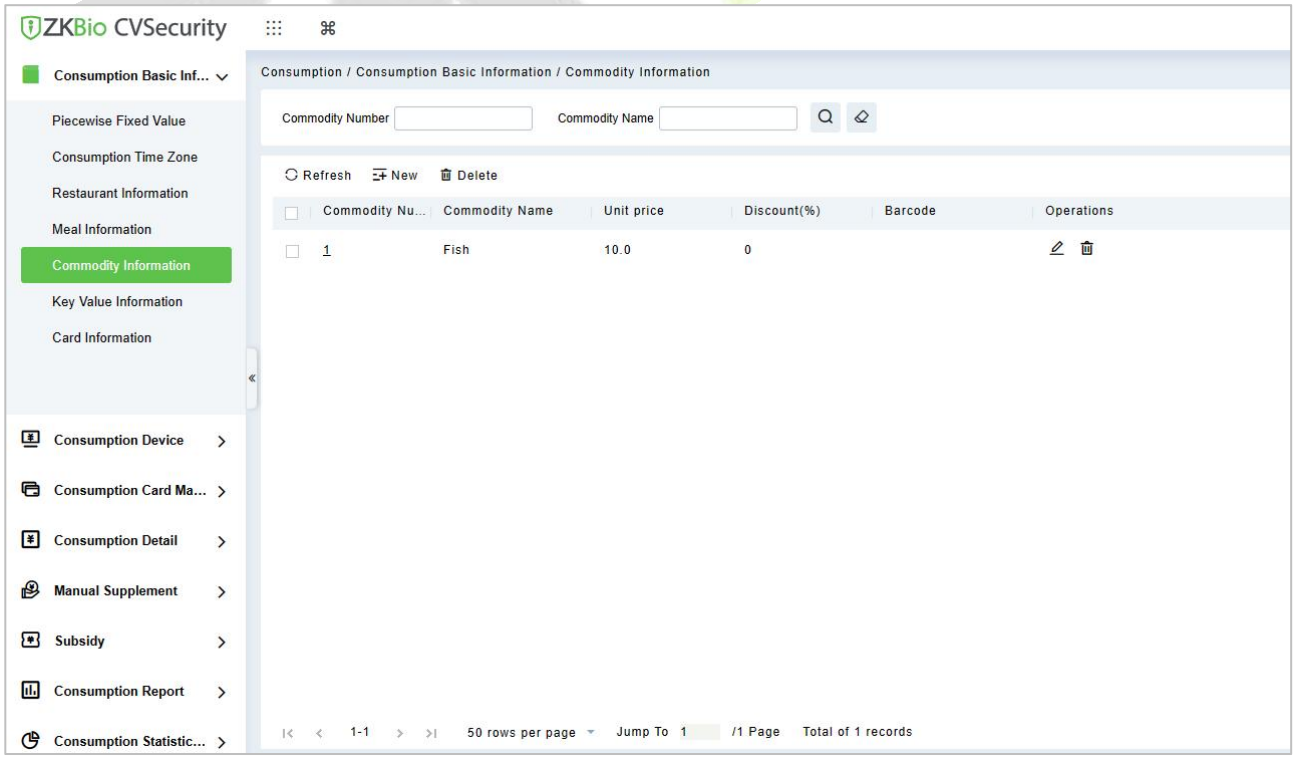


Figure 11- 12

● New:

Click **New** to add, enter required **Commodity number**, **Commodity Name**, **Barcode**, **Unit price**, **Discount** in the dialog box, and then click **OK** to save and close or click **Save and New** for continue adding.

✍**Note:** If you put 0 in **Discount**, then the product is not discounted.

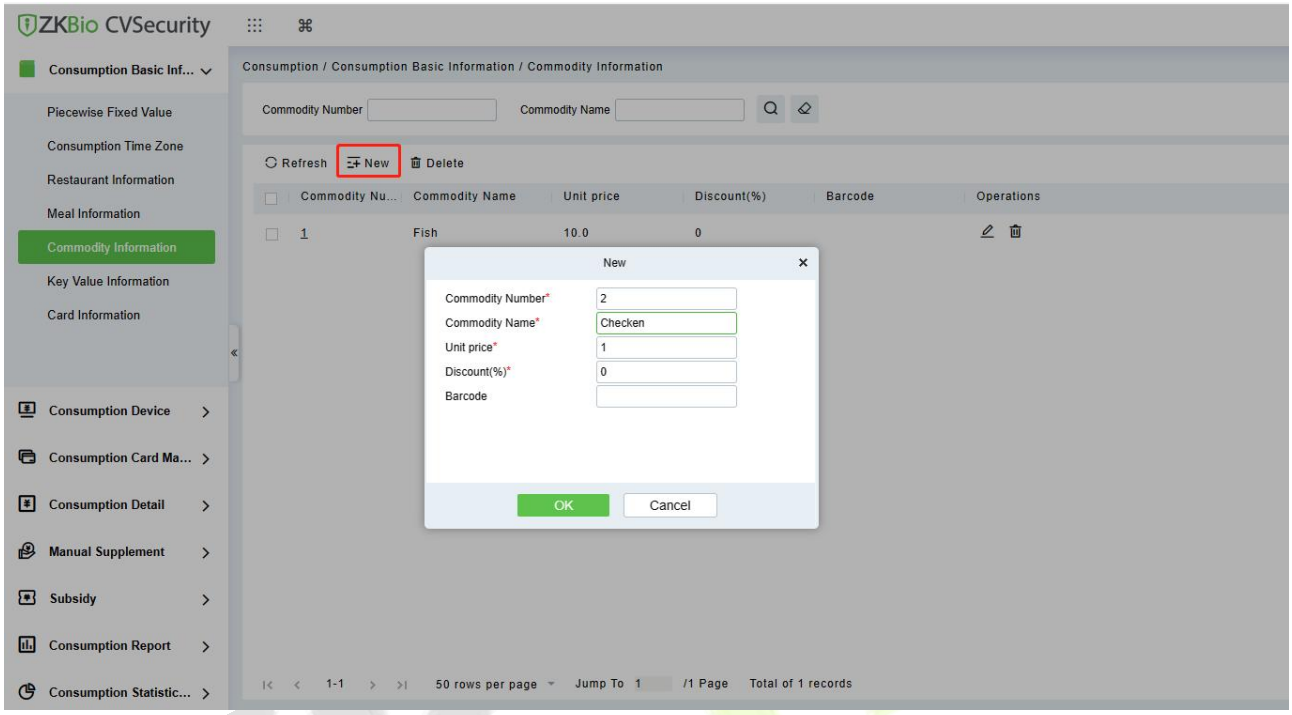


Figure 11- 13

● Delete:

You can directly click **Delete** on the required Commodity to remove it from the system.

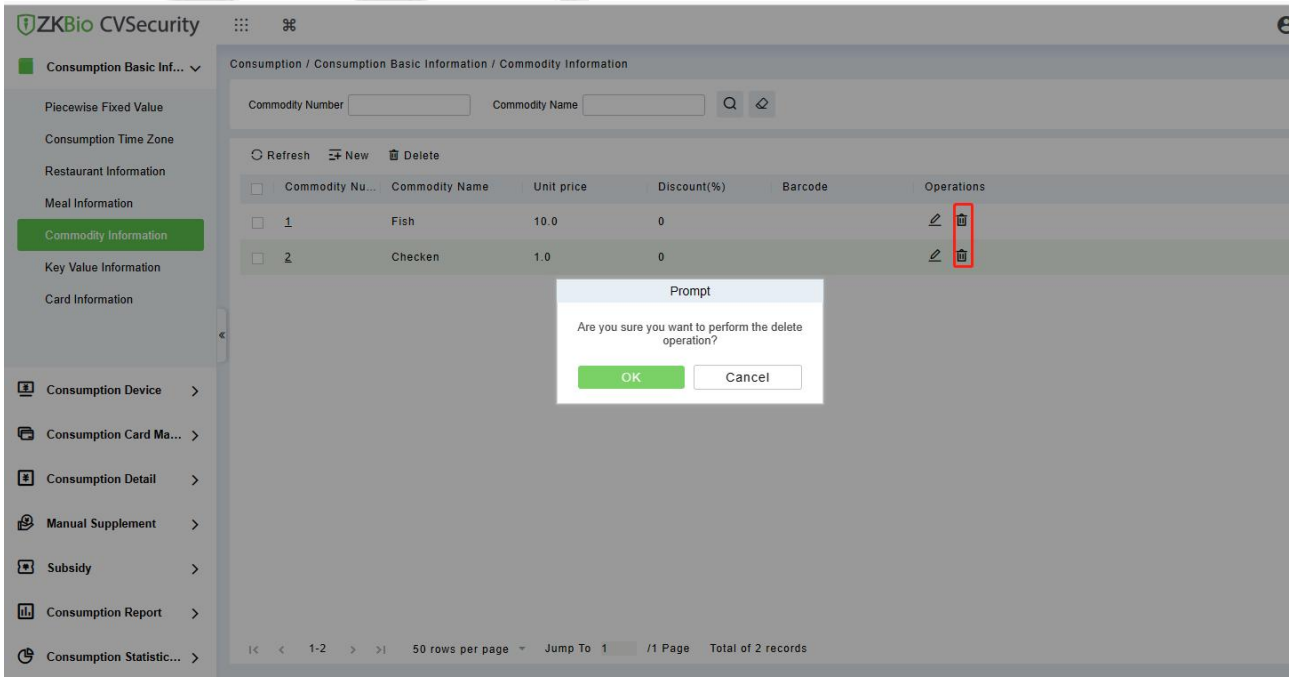


Figure 11- 14

For deleting in batch, select the required Commodity(s) as shown below and click **Delete**.

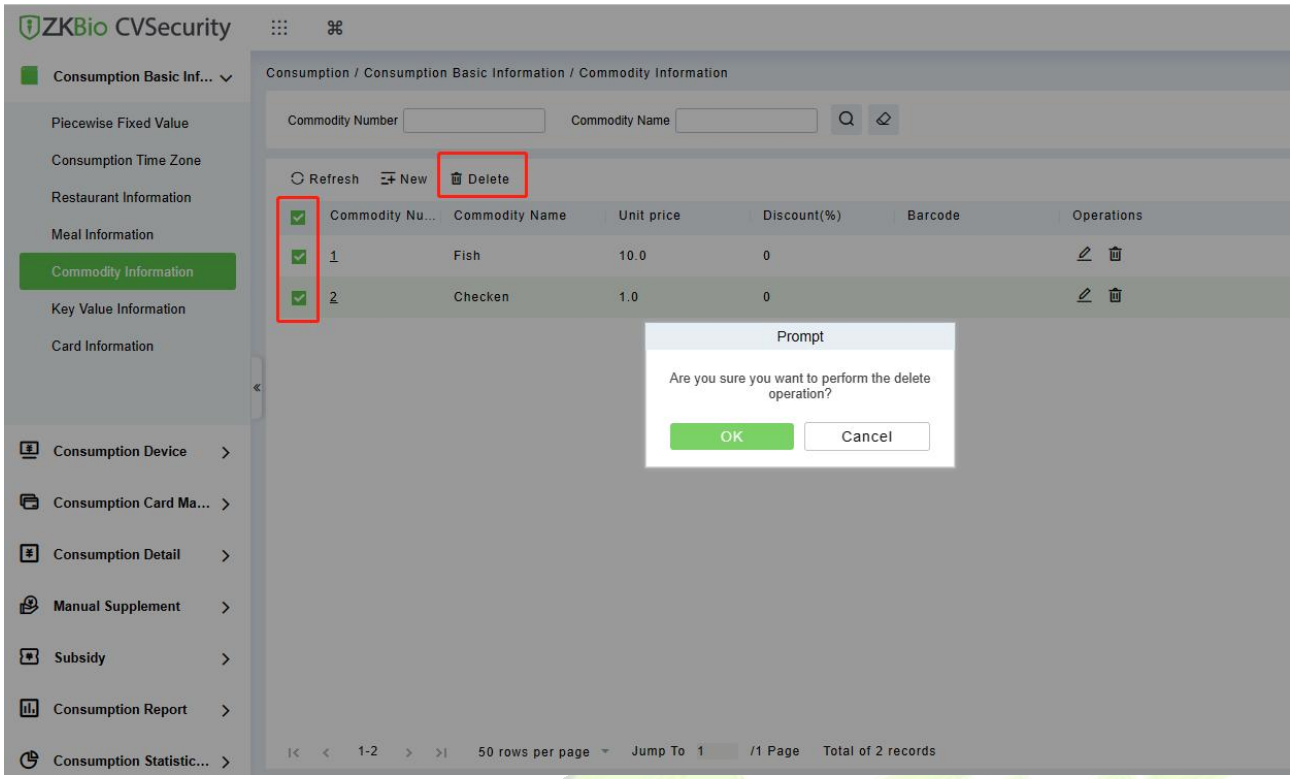


Figure 11- 15

11.1.1.6Card Information

Click Consumption Basic Management > Card Information, as shown below:

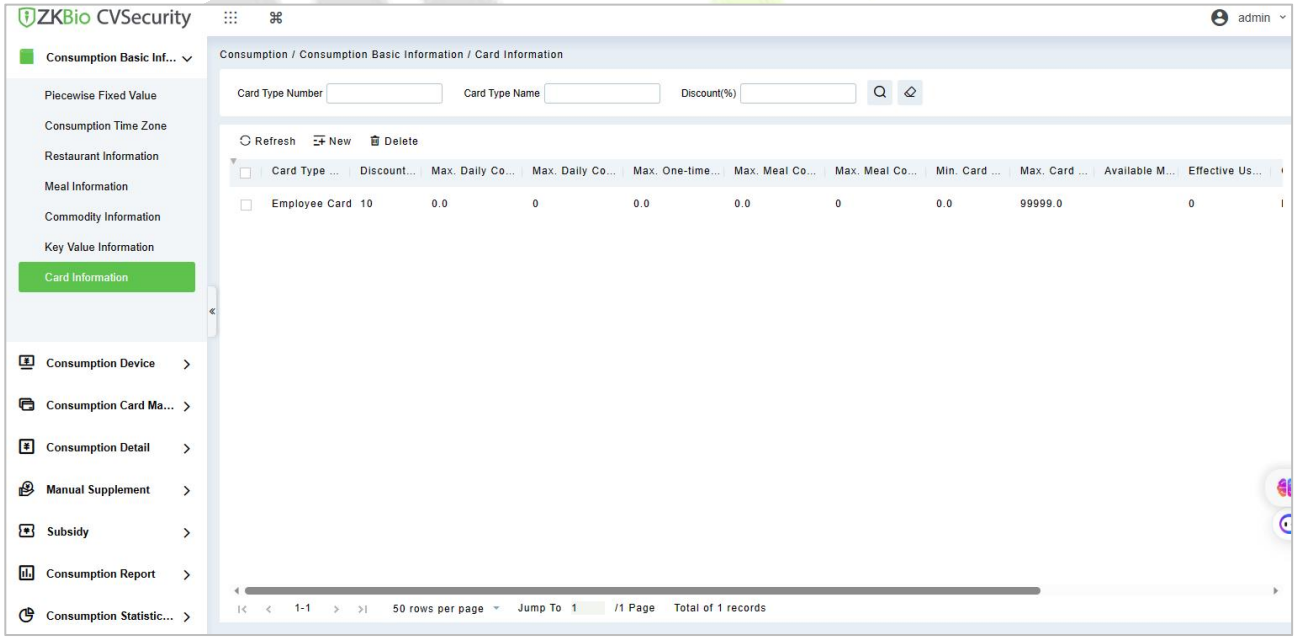


Figure 11- 16

● New:

Click **New**, in the dialog box, you can fill in the Card Type Number, Card Type Name, Discount, Consumption Time Zone, Maximum Daily Consumption Amount, Maximum Daily Consumption Times, Maximum One-Time Consumption Amount, Maximum Meal Consumption Amount, Maximum Meal Consumption Times, Minimum Card Balance, Maximum Card Balance, Effective Use of Days, Available Meal, Available Device, Remarks, as shown below:

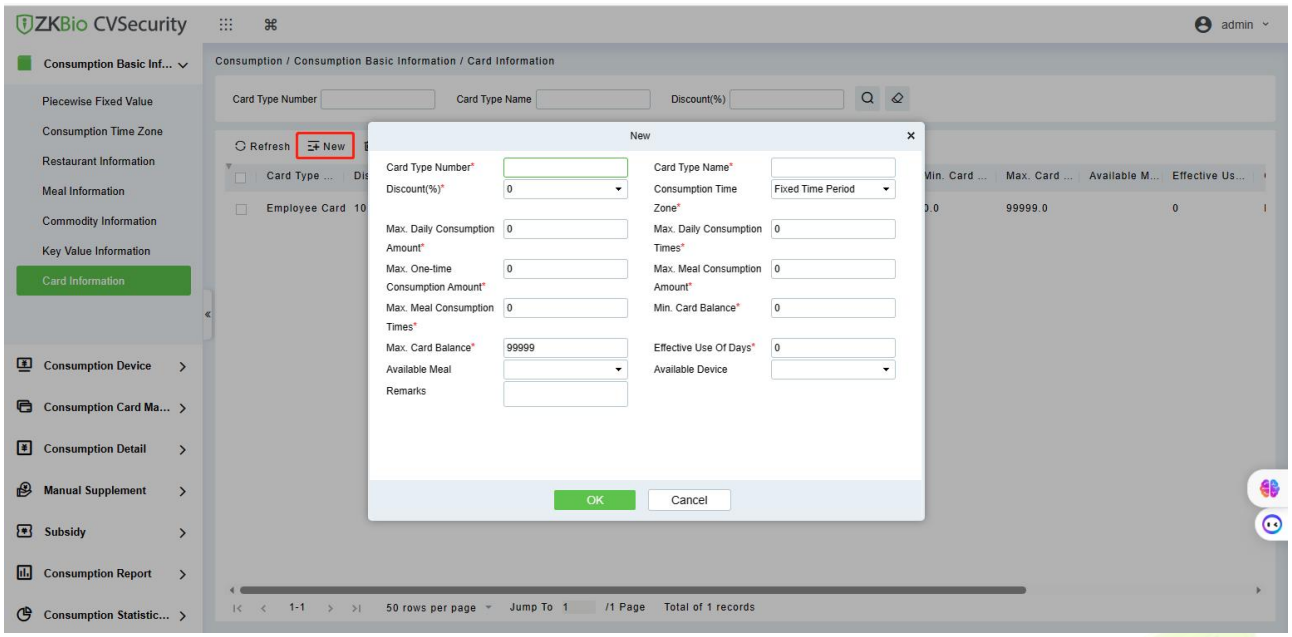


Figure 11- 17

● Edit:

Click the card type number of the list and the edit column of the operation to pop up the modification dialog box.

● Delete:

You can directly click **Delete** on the required Card to remove it from the system.

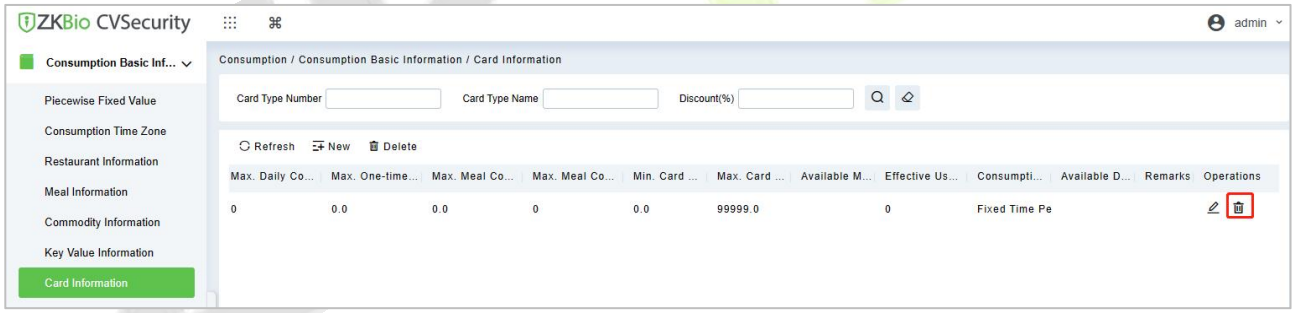


Figure 11- 18

For deleting in batch, select the required Card (s) as shown below and click **Delete**. The default employee card cannot be deleted.

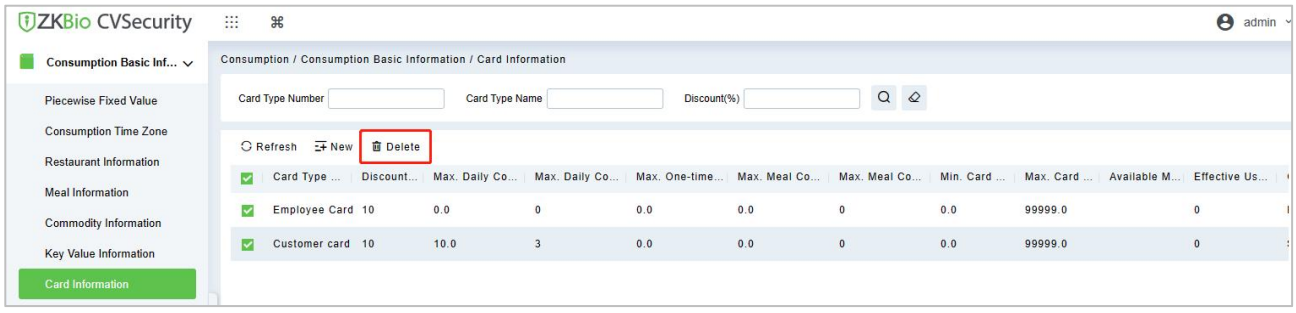


Figure 11- 19

11.1.2Key Value Information

Click **Consumption Basic Management** > **Key Value Information** to enter the unit value in the

consumer device as shown below:

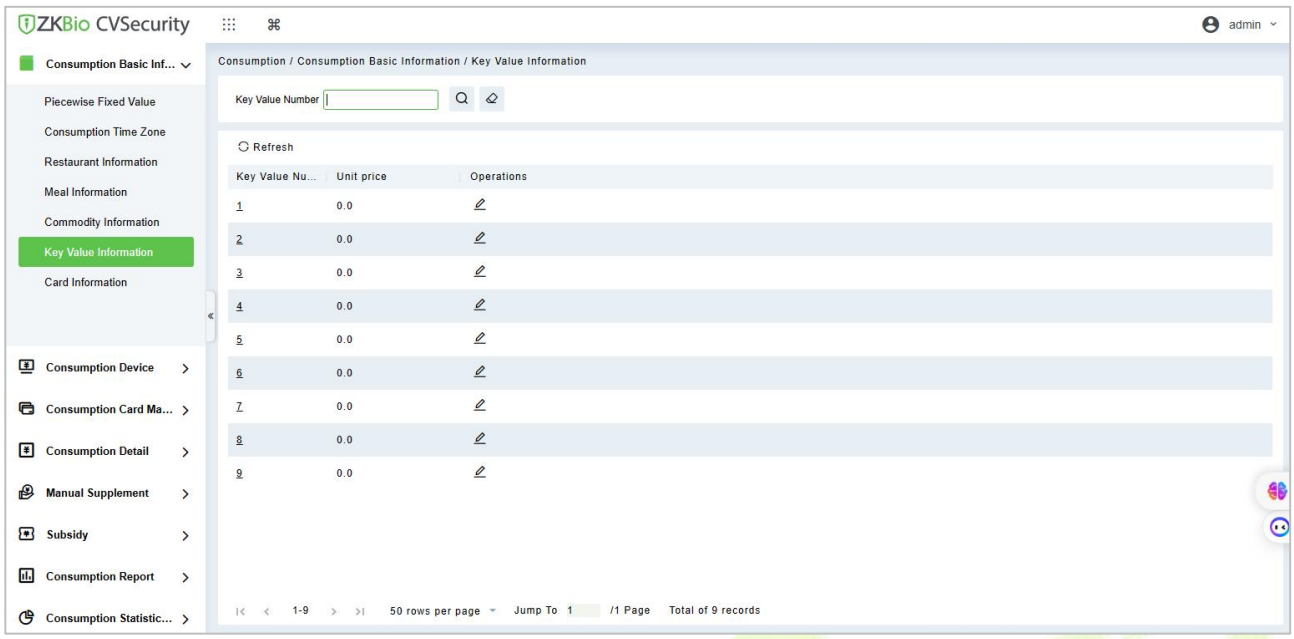


Figure 11- 20

● Edit:

Click the key value number of the list and the edit column of the operation to pop up the modification dialog box. Only the unit price can be modified. The specific display of the dialog box is as follows:

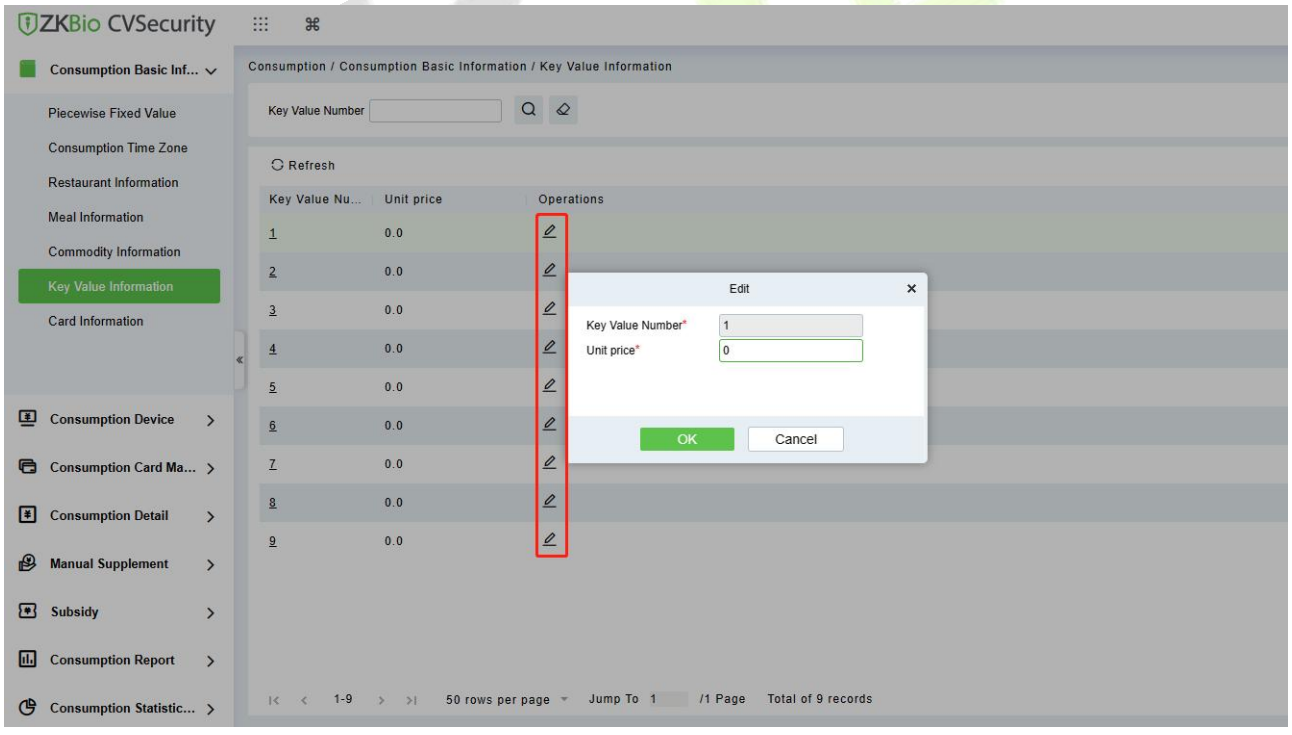


Figure 11- 21

11.2 Consumption Device Management

This module is used to manage consumer devices and set basic parameters of the consumer system.

11.2.1 Consumption Device

Click Consumption Device > Consumption Device, as shown below:

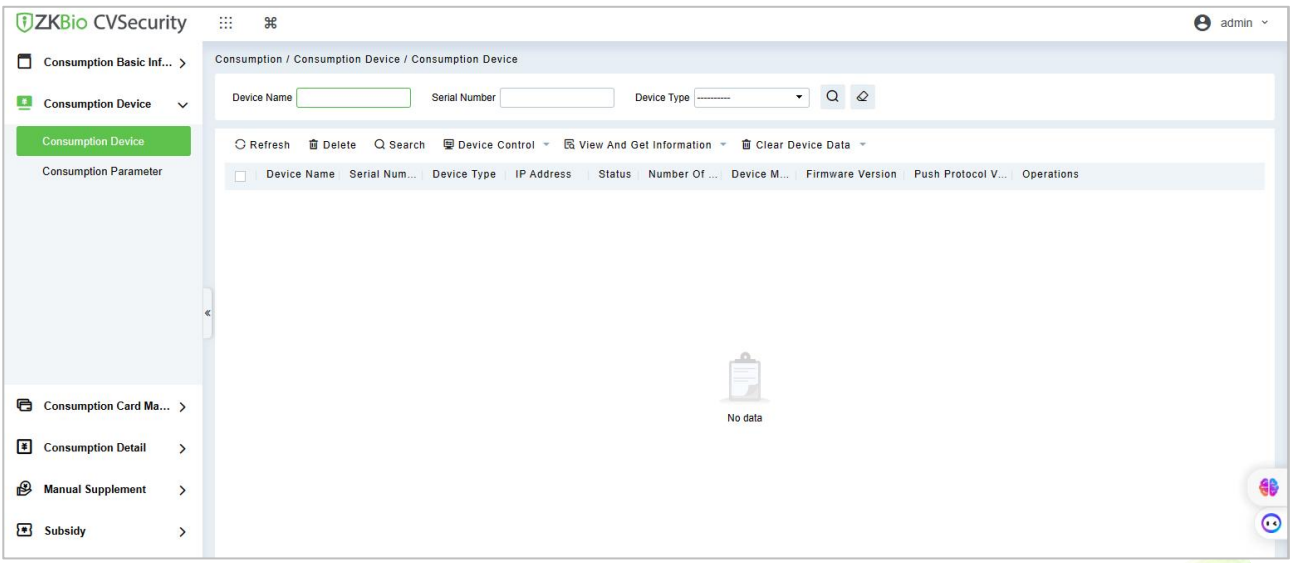


Figure 11- 22

● New:

Click **Search**, the system will automatically searching to add the device . The specific display of the dialog box is as follows:

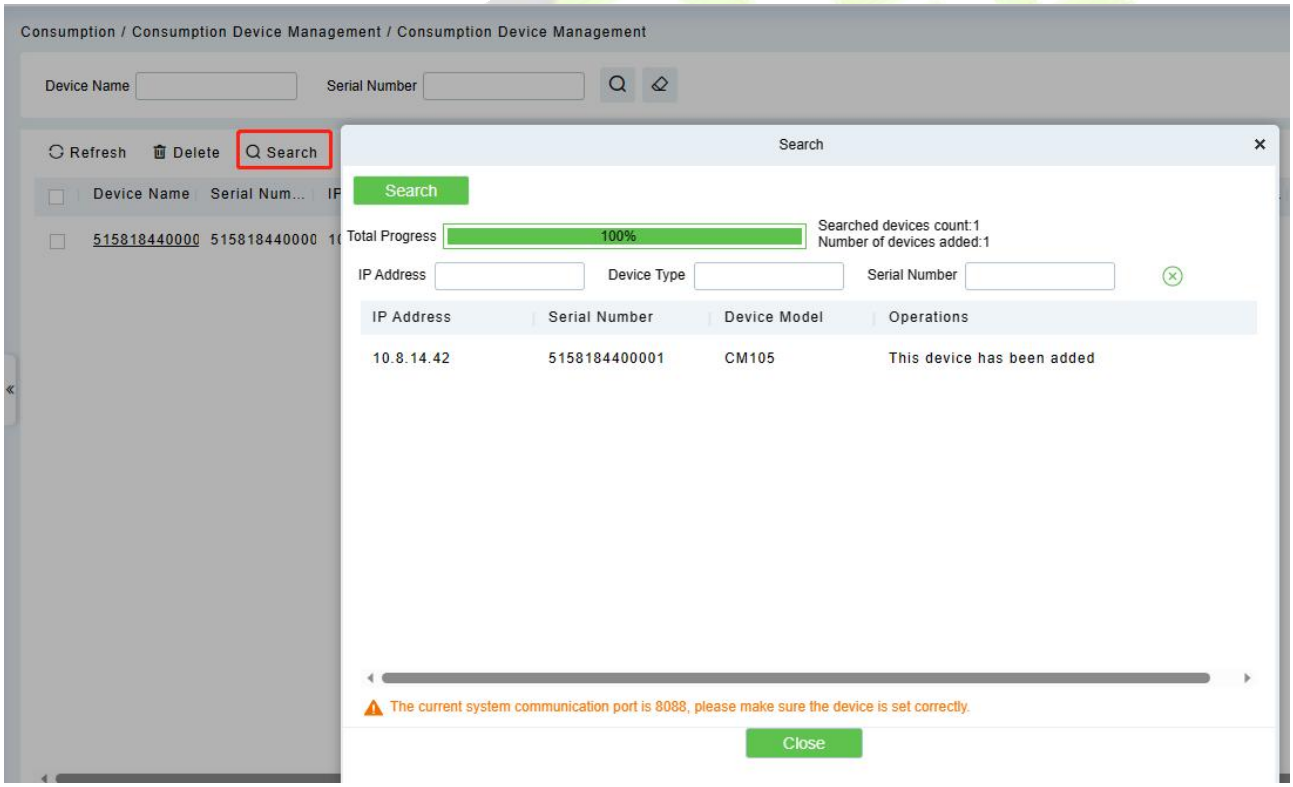


Figure 11- 23

● Some parameters are explained as follows:

Equipment use: This will define the usage type of the consumer device.

Whether accounting: It appears when the device type is selected as Consumer machine. If the **Whether Accounting** check box is selected, the billing record is generated when the card is swiped and the amount is not deducted from the card.

Operator check: If the **Operator Card Check** checkbox is selected, the device will be initially in locked

state after being added to the system. To unlock the device, the operation card needs to be swiped. Please note that, the operation card must have been issued before using this parameter.

Consumption mode: The options are fixed value mode, Amount Mode, Key-value mode, Counting mode, Commodity mode, Recording Time Mode. Selected for different needs.

Cumulative Subsidy: It appears when the device type is selected as Subsidy machine. If the accumulative subsidy is not checked, only the last subsidy application can be received when there are multiple unsubsidized records; when the accumulative subsidy is checked, all the subsidized amounts will be collected.

Clear subsidy: Displayed only when the device is a subsidized machine. If the zero subsidy is not checked, the subsidy application will be directly received; if the zero subsidy is checked, the original subsidy in card will be cleared first and then collect the latest subsidy.

● Edit:

Click the device name of the list or the edit column of the operation to pop up the modification dialog box. The items that can be modified in the modification dialog box includes device name, area, device usage, whether accounting, operator card check, consumption mode, and restaurant. And you can also view the segmentation value, card type, and key value data corresponding to the device, as shown in the following figure.

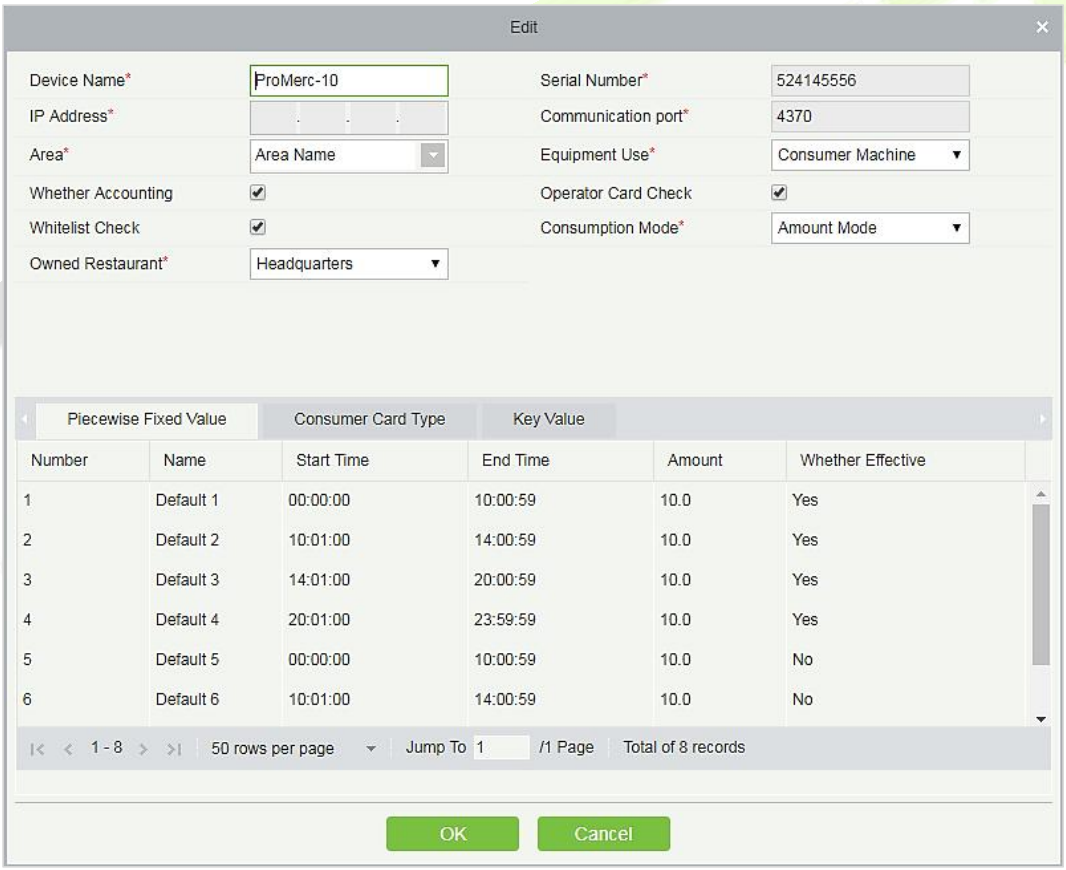


Figure 11- 24

● Delete:

Check the consumer device record, click **Delete** at the top of the list or **Delete** under the operation bar, **OK** to delete the selected consumer device data, and **Cancel** to cancel the operation.

● Clear Swipe Card Data:

Click the **Clear Swipe Card Data** button at the top of the list, a dialog box will pop up as shown below.

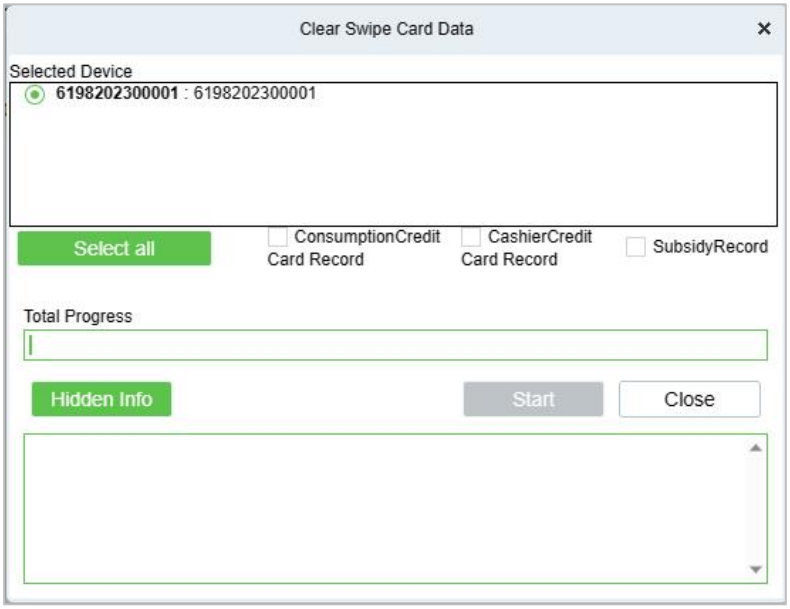


Figure 11- 25

The operation here is to select the device first, then you can check the type of the card record, you can select all, click **Start** will clear the data of the selected card record, click **Close** will close the current dialog box, no operation.

● Clear consumer device settings:

Click the **Clear Consumer Device Settings** button at the top of the list, a dialog box will pop up as shown below.

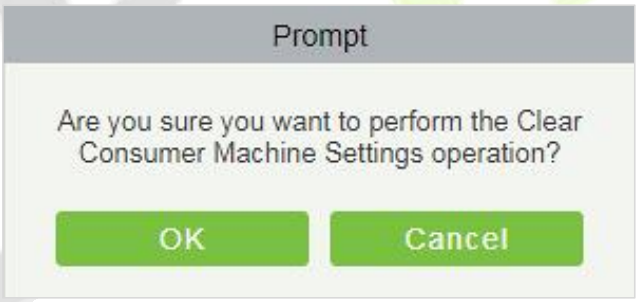


Figure 11- 26

Clicking **OK** will clear the setting information of the consumer device, and clicking **Cancel** will close the current dialog box and do nothing.

● Delete device command:

Select a device in the device list below, click and select the device check box on the left side, click the Delete Device command, and the following dialog box will pop up. Click **OK**. The command to be parsed by the device will be deleted and cleared.

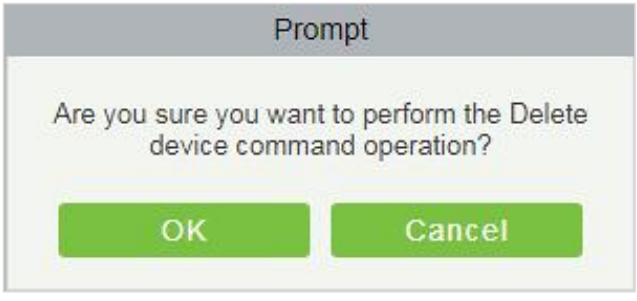


Figure 11- 27

● Collect all data:

Select a device in the device list below, click and select the device from the list, click to collect all data, and the following dialog box will pop up. According to the operator's needs, check the data that needs to be synchronized. Click Start and wait for the data to sync until the synchronization is complete.

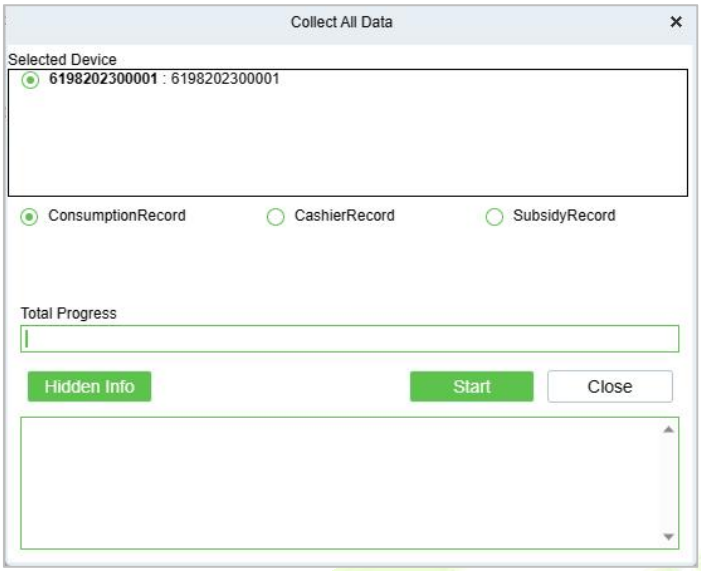


Figure 11- 28

● More:

There are two hidden function buttons under the button, which are to restart the device and synchronize the software data to the device:

Restart the device: Check one device, click this button, the device will automatically restart.

Synchronize software data to device: Select a device, click this button, it will send data such as setting parameters of the software to the device to achieve the function of synchronization information so that the device can set the properties synchronously.

11.2.2Consumption Parameter

Click **Device** > **Consumption Parameters**, as shown below:

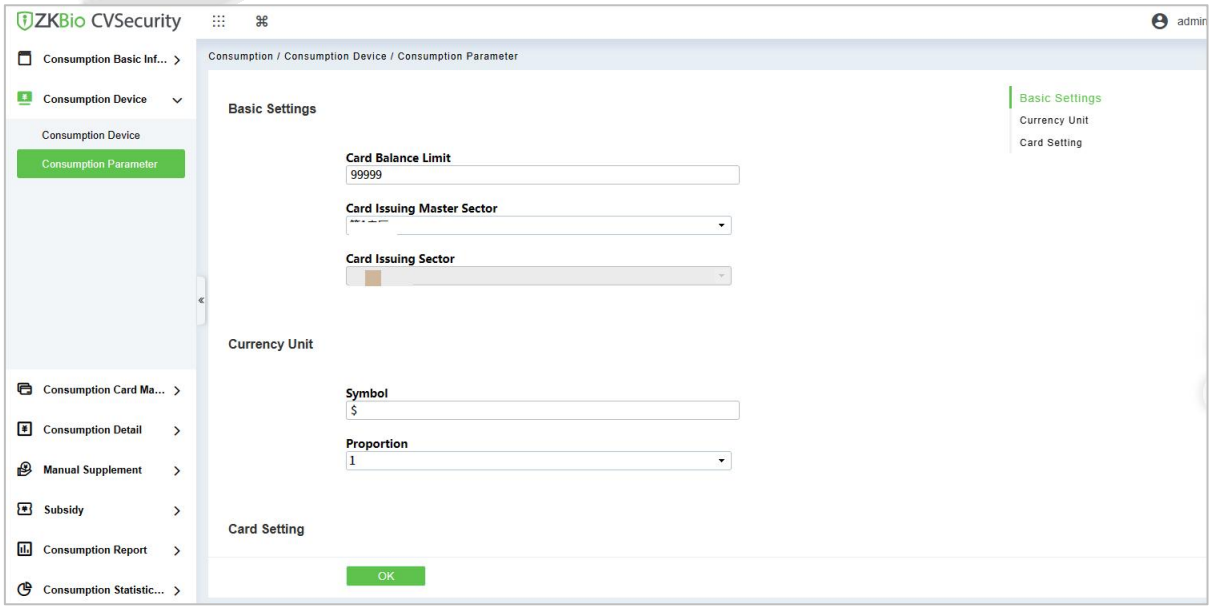


Figure 11- 29

● Basic Setting:

1) Set the upper limit of the card balance. You can set an integer value between 1~9999, default value is 9999.
2) Set the master and slave sectors of card issuing: The master sector of card issuing can be selected from sector 1 to sector 14, and the default is sector 1 and it cannot be edited.
3) Consumption rate is the value set to obtain the consumption amount with respect to the entered amount on the device.
4) Set the system password: The default is 123456 and you need to change it before using the password for 1st time. This password will be written on the card while issuing.
5) The default mode is **Single wallet mode.**
6) Click **OK** to save the modified consumption parameter information.

✍ **Note:** The system password and mode are not allowed to be changed again after the device has been added.

11.3 Card Management

11.3.1 Card Service

Using this option, you can issue different types of card and set their usage limits. You can also manage the already existing cards.

The initial interface of this module is shown below:

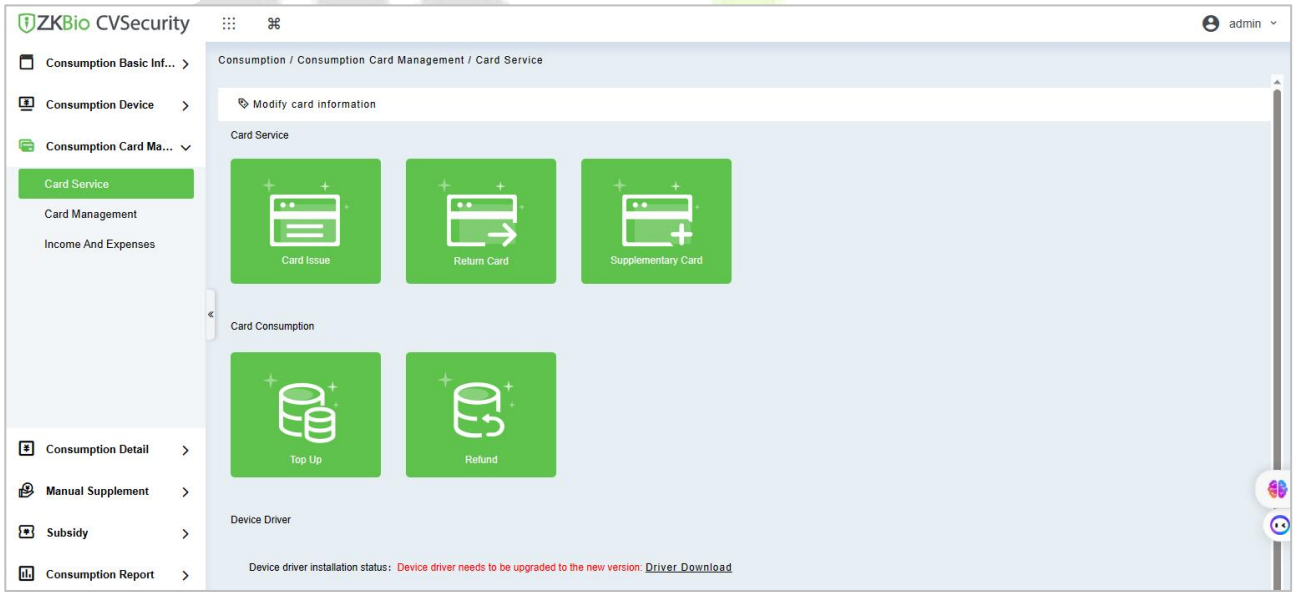


Figure 11- 30

11.3.1.1 Device Driver

First of all, you need to check the status of the Device driver at the bottom of this interface.

If it is not installed, you need to click **Driver Download** and install it before using this function.

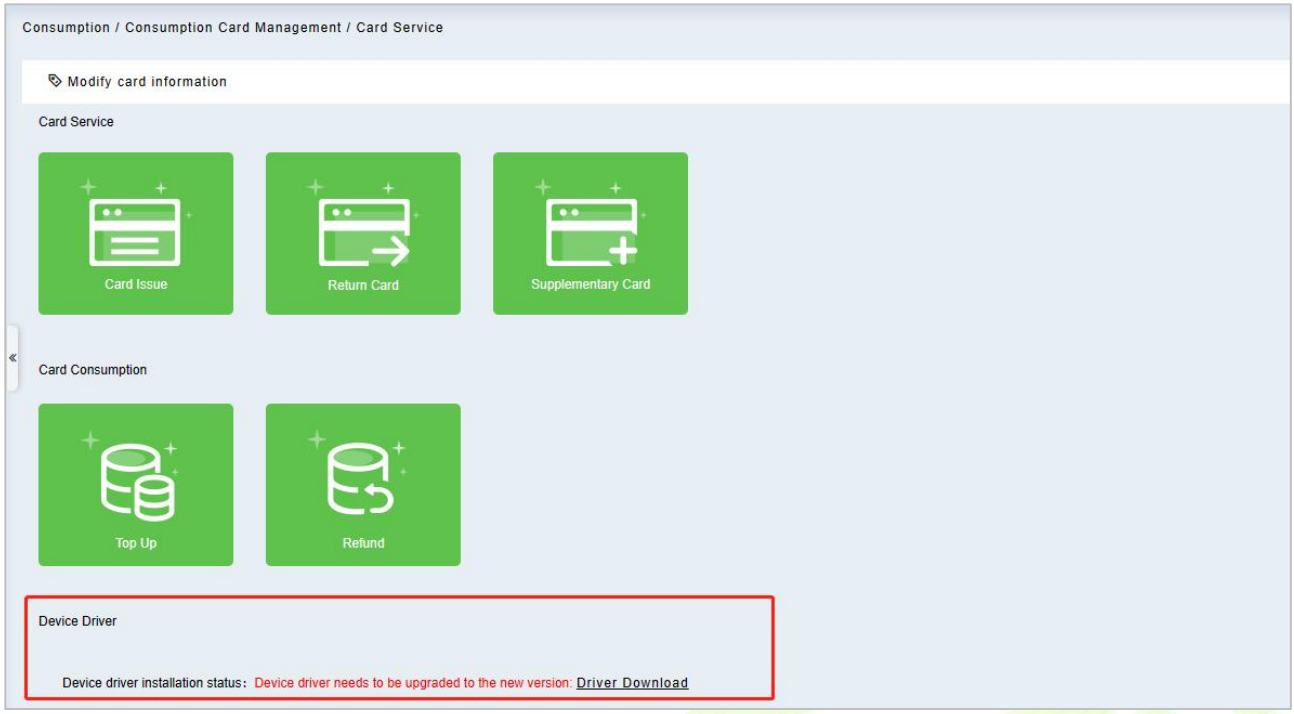


Figure 11- 31

Click **Driver Download** to start downloading. Once it is downloaded, install it as per the on-screen prompts. After the installation is complete, you can see the updated status as shown below:

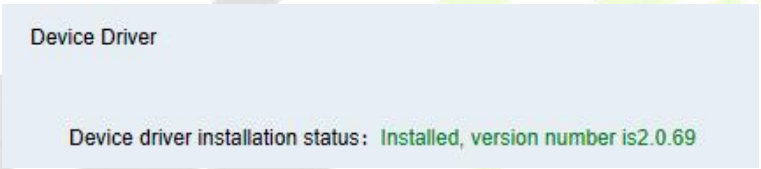


Figure 11- 32

11.3.1.2Modify Card Information

Place the card on the card reader, click **Modify card information** as shown below. A dialog box will appear with all the details of the card.

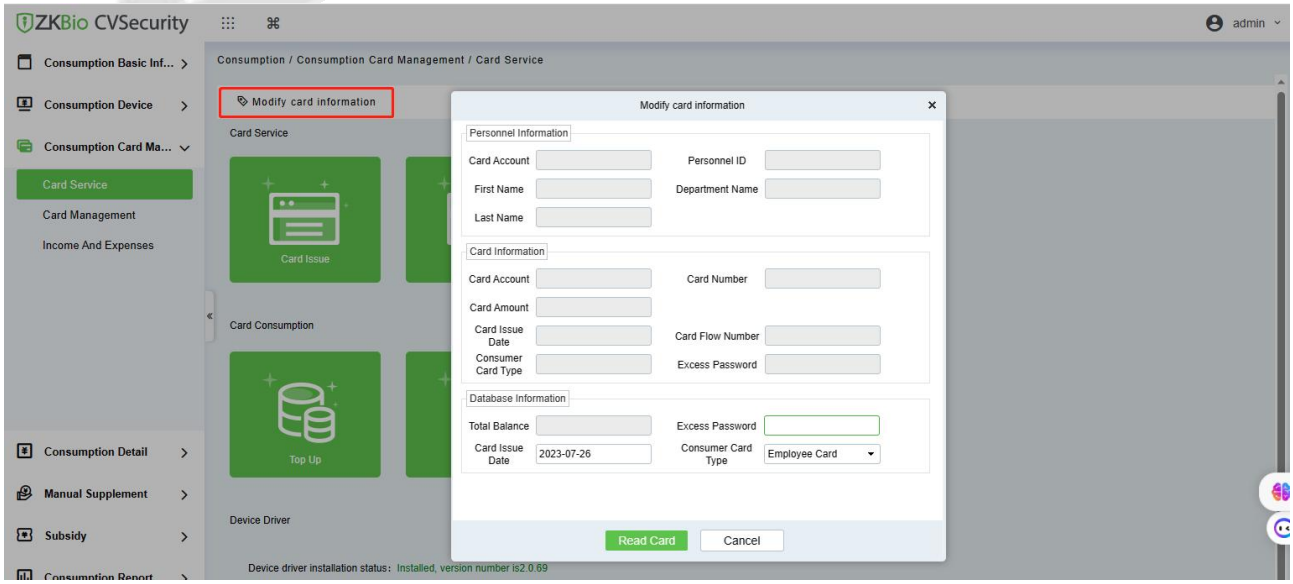


Figure 11- 33

11.3.1.3Card Issue

You must initialize a card through this system before using it on the consumer device.

Click on the card issue icon, the card issuing interface is as follows.

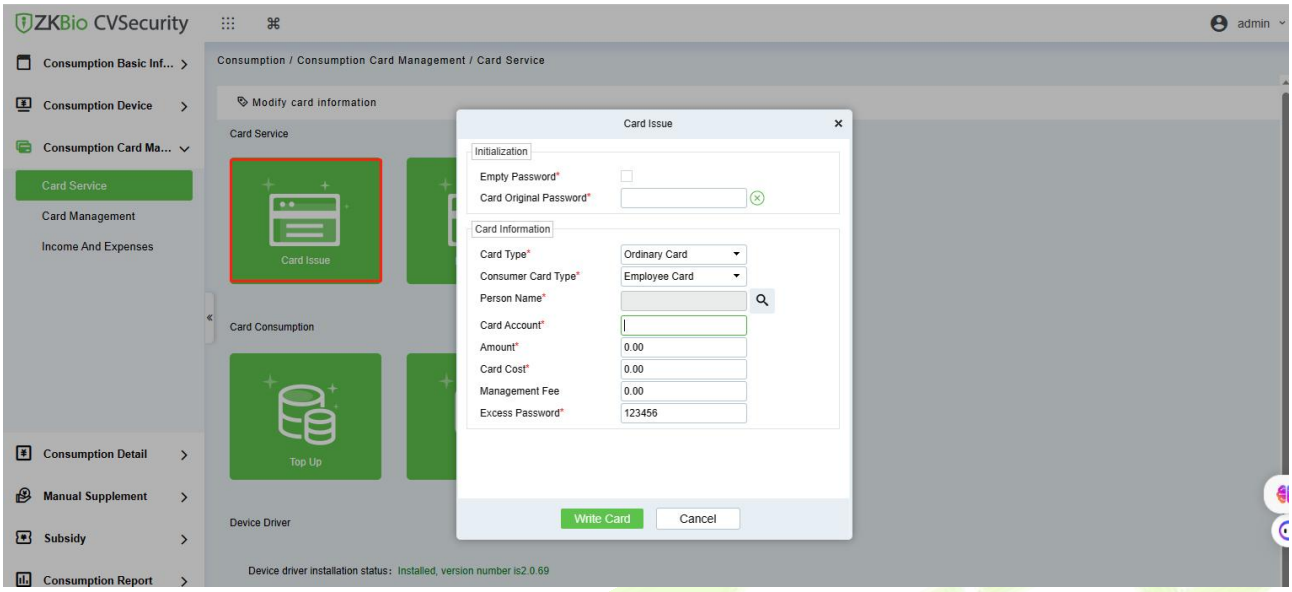


Figure 11- 34

If the card is previously used before initialization, you can set blank password or keep the original password of the card. After setting the card type and consumer card ty in this window, click the icon beside the Person's name field and select the required personnel (you need to add the required personnel in the personnel module before issuing card). Then set the Card Account, Amount, Card Cost, Management Fee, Excess Password, click Issue card to complete.

● Prerequisites:

1. Make sure the required person is already added in the personnel module before issuing card.
2. The card needs to be initialized before issuing the card.

11.3.1.4Return Card

Return Card operation is performed to stop the card being used further in the consumption software system.

After clicking **Return card**, a pop-up window will give additional information for the operation. Put the card on the card reader, click on the card to read, the card information will be displayed, check the information and click OK to block or revoke the card.

● Prerequisites:

To withdraw a card approval, you must have an issued card.

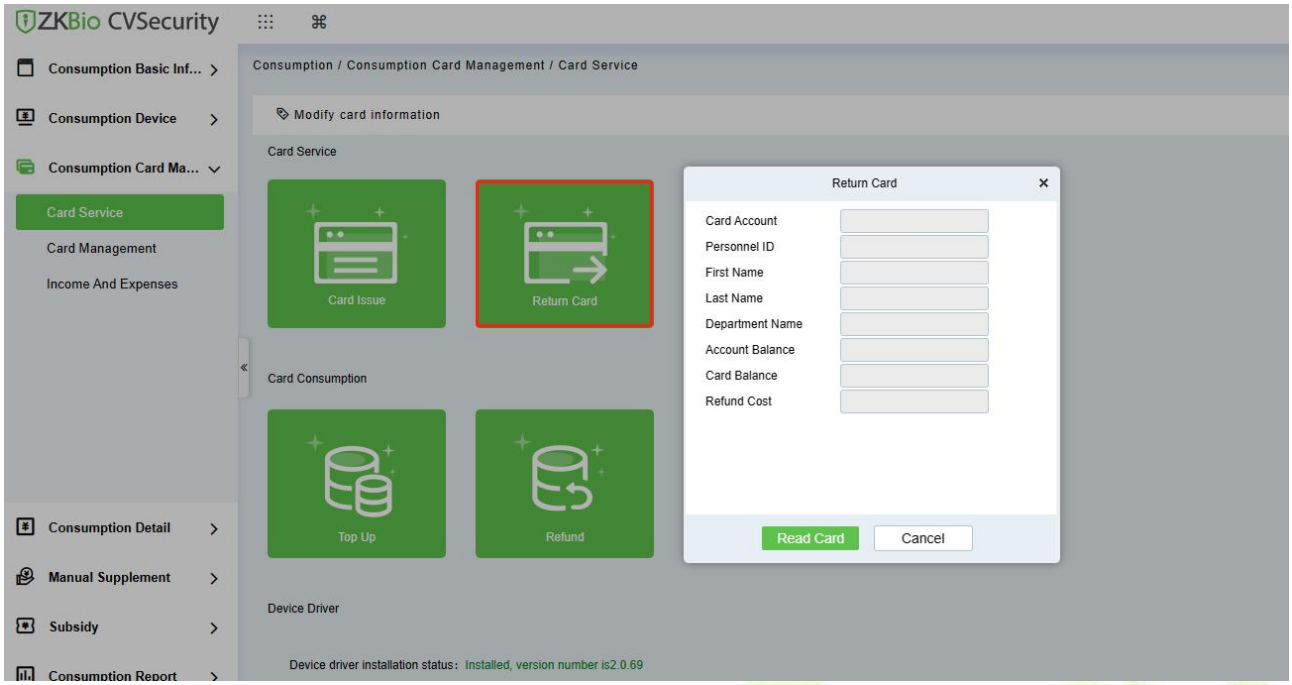


Figure 11- 35

11.3.1.5Supplementary Card

● Prerequisite:

This function is used when a card is reported lost.

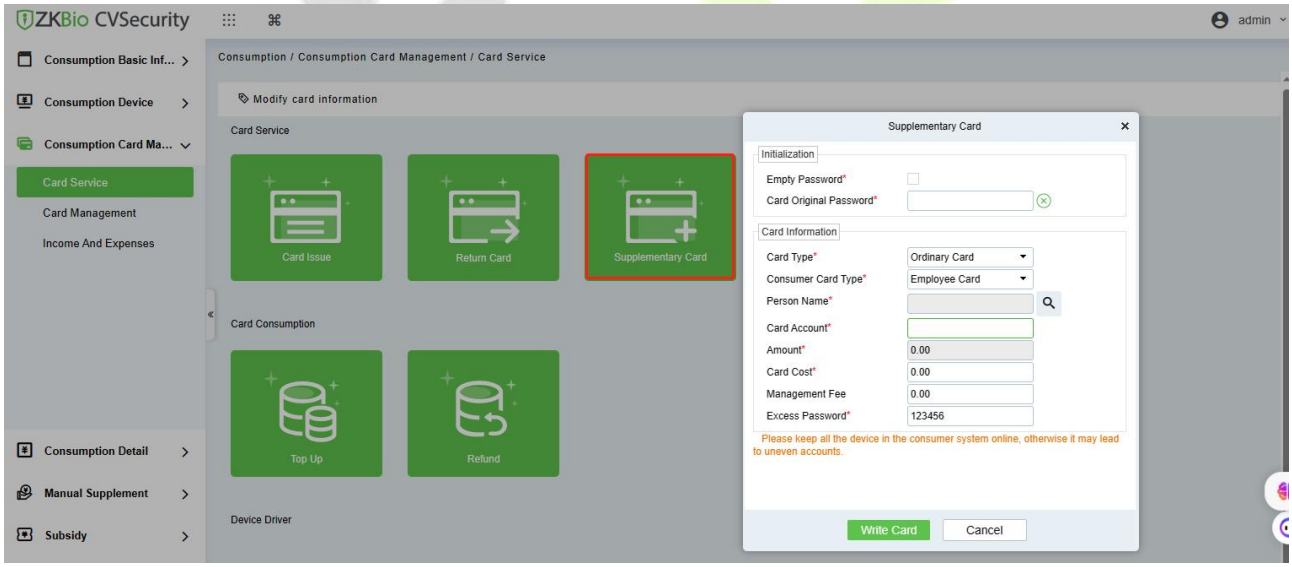


Figure 11- 36

Click the search icon beside the Person Name field and select the person who has lost the card. Click to write the card with the same information as the lost card. After the card is issued, the balance and other information in the original card will be written into the new card. (The used card needs to be initialized, and the card can be set to a blank password or a card original password at the initialization interface.)

✍**Note:** Please ensure that all devices in the consumption system are online. Otherwise, the processing result after the above operation cannot be synchronized to other devices. And the original card can still be used for consumption, resulting in the card balance being inconsistent with the actual amount and the account being uneven. Please be careful with this!

11.3.2Top Up

This function is used to add an extra amount to the card balance. Click the top up button to open the Top-up interface. Put the card on the card reader, click on the card to confirm the card information. Enter the amount you need to recharge and then click OK to execute the operation.

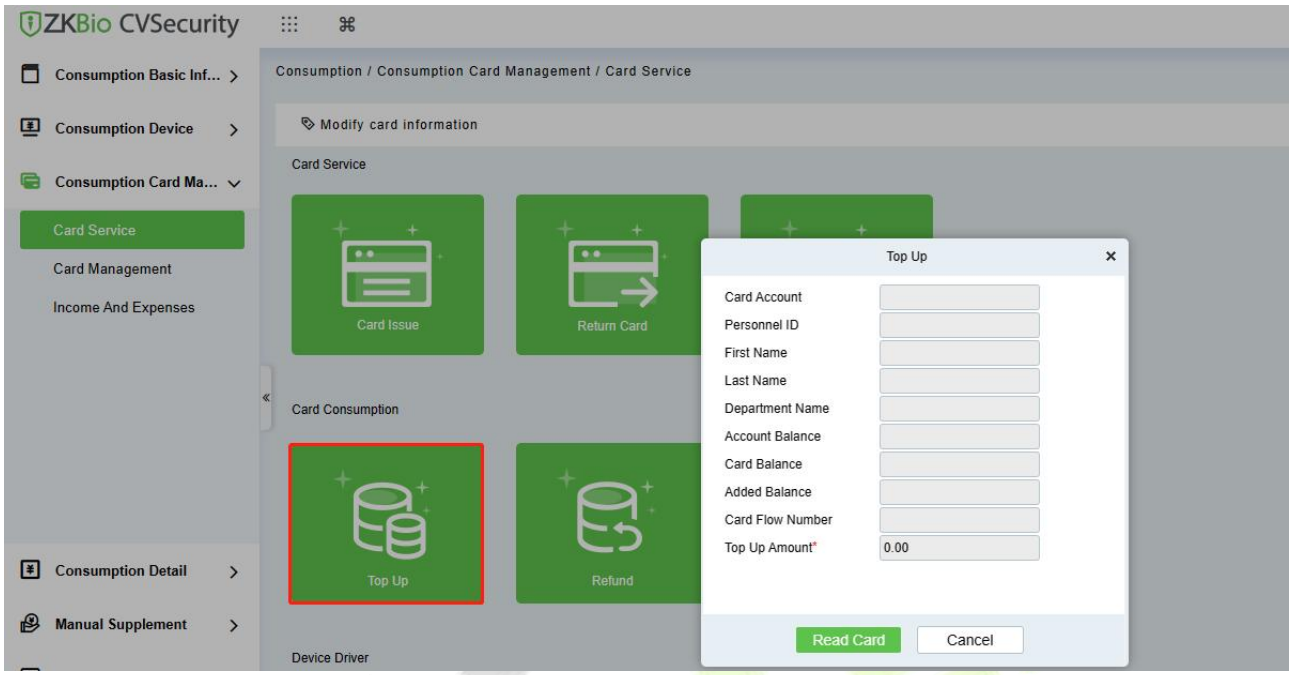


Figure 11- 37

11.3.2.1Refund

Refund operation is used to return a specified amount to the card. Click the refund button to open the refund interface, put the card on the card reader, click on the Read card to confirm the card information. Enter the amount you need to refund, and click OK to execute the operation.

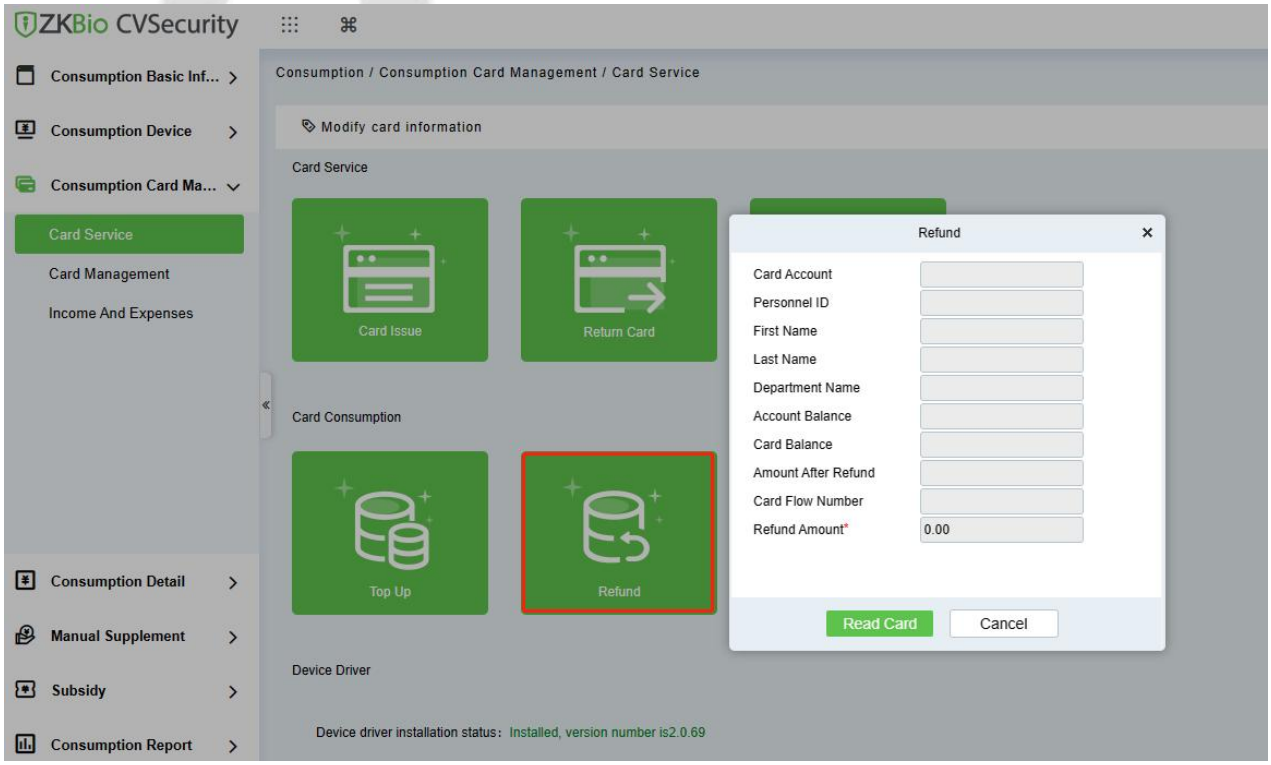


Figure 11- 38

11.3.3Card Management

This function is used to perform two operations; **Logout Management Card and Non-Card Return Card**. And on this interface, you can also view the card information that has been issued till date.

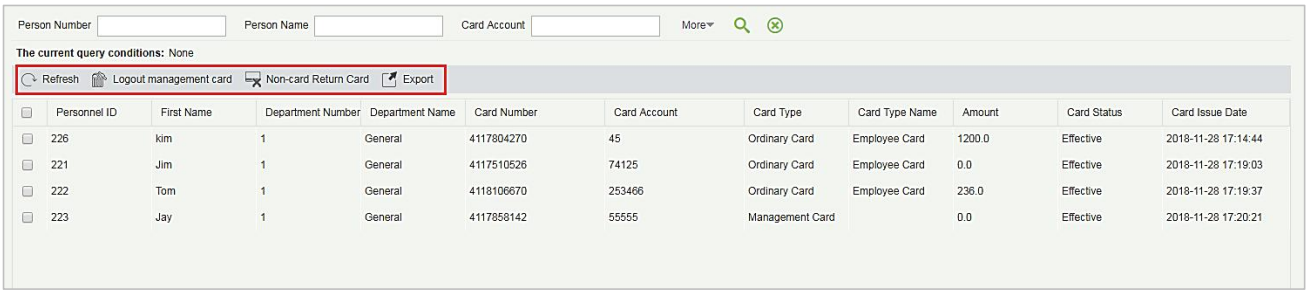


Figure 11- 39

The top of the interface provides several search criteria:

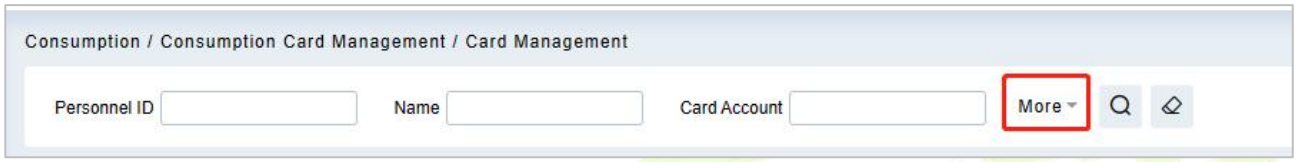


Figure 11- 40

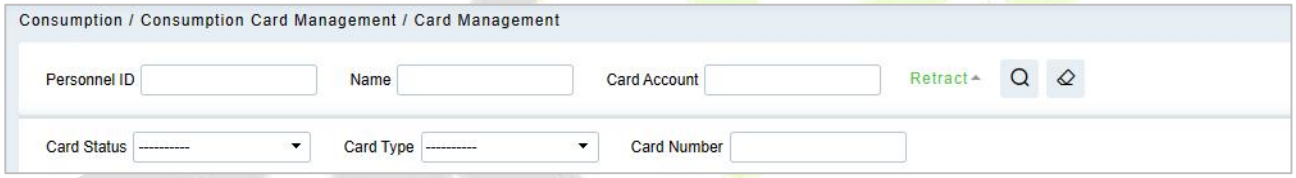


Figure 11- 41

Enter the known information in the respective field to search for the corresponding card information. For example, if you need to search all the ordinary cards, click the card type drop-down menu, select Ordinary card, and click the icon on the right to get the search results. The search results are displayed on the report interface at the bottom of the page. As shown below.

Figure 11- 42

11.3.3.1Logout Management Card

This function is used to log out the management and the operation card. After the logout operation, the management card or operation card will be invalid.

11.3.3.2Non-Card Return Card

Click **Non-card return card**, select the desired refund option and click **OK**. If the card is eligible for the refund, the amount will be refunded to the card and a refund record will be generated in the system.

The card will not be used in this consumer system after the card is not returned.

✍**Note: Non-card return card** Please ensure that all devices in the consumption system are online before operation. Otherwise, the processing result after operation may not be synchronized to other

devices in time. The card can still be consumed, resulting in the card balance being inconsistent with the actual amount and unbalanced situation. Please be careful with this!

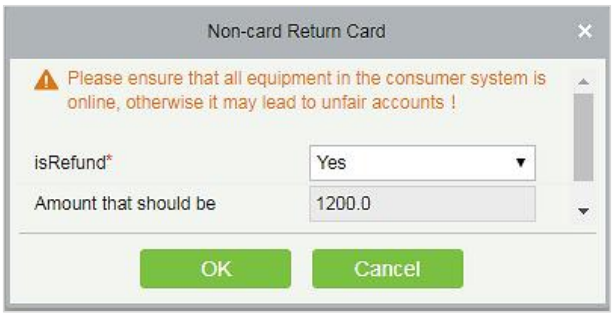


Figure 11- 43

11.3.3.3Refresh

It is used to update the card interface with new data.

11.3.3.4Export

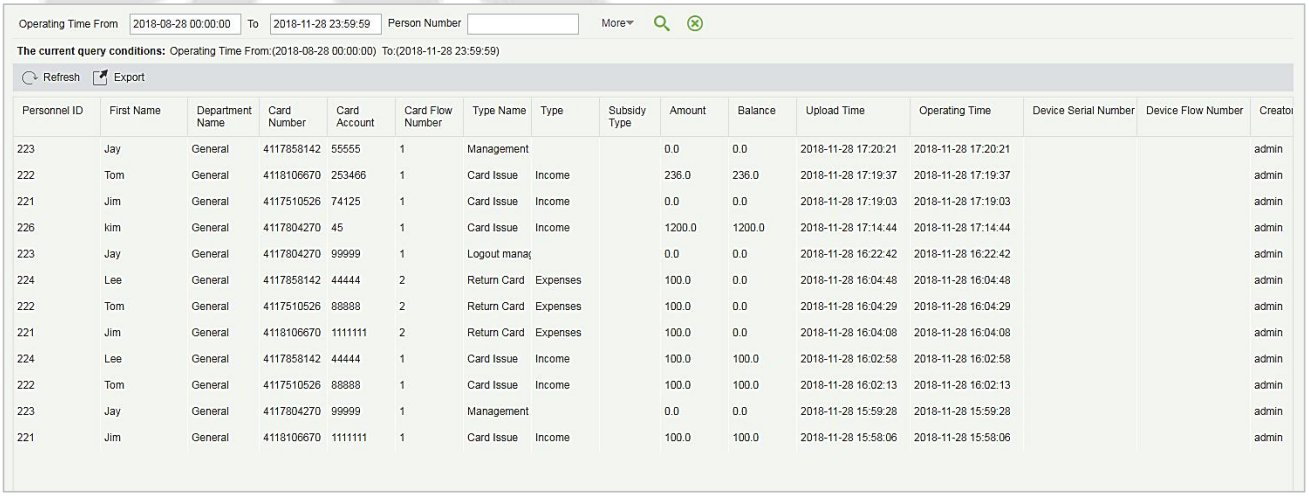
It exports the current report data.

✍**Note:** The report loss/resume card operation is performed in the card management in the **Personnel Module**.

11.3.4Income and Expenses

This function will show all the payments and due amount data of all the cards in the consumption system.

Click **Card Management** > **Income and Expenses**, as shown below:



Personnel ID	First Name	Department Name	Card Number	Card Account	Card Flow Number	Type Name	Type	Subsidy Type	Amount	Balance	Upload Time	Operating Time	Device Serial Number	Device Flow Number	Creator
223	Jay	General	4117858142	55555	1	Management			0.0	0.0	2018-11-28 17:20:21	2018-11-28 17:20:21			admin
222	Tom	General	4118106670	253466	1	Card Issue	Income		236.0	236.0	2018-11-28 17:19:37	2018-11-28 17:19:37			admin
221	Jim	General	4117510526	74125	1	Card Issue	Income		0.0	0.0	2018-11-28 17:19:03	2018-11-28 17:19:03			admin
226	kim	General	4117804270	45	1	Card Issue	Income		1200.0	1200.0	2018-11-28 17:14:44	2018-11-28 17:14:44			admin
223	Jay	General	4117804270	99999	1	Logout mana(			0.0	0.0	2018-11-28 16:22:42	2018-11-28 16:22:42			admin
224	Lee	General	4117858142	44444	2	Return Card	Expenses		100.0	0.0	2018-11-28 16:04:48	2018-11-28 16:04:48			admin
222	Tom	General	4117510526	88888	2	Return Card	Expenses		100.0	0.0	2018-11-28 16:04:29	2018-11-28 16:04:29			admin
221	Jim	General	4118106670	1111111	2	Return Card	Expenses		100.0	0.0	2018-11-28 16:04:08	2018-11-28 16:04:08			admin
224	Lee	General	4117858142	44444	1	Card Issue	Income		100.0	100.0	2018-11-28 16:02:58	2018-11-28 16:02:58			admin
222	Tom	General	4117510526	88888	1	Card Issue	Income		100.0	100.0	2018-11-28 16:02:13	2018-11-28 16:02:13			admin
223	Jay	General	4117804270	99999	1	Management			0.0	0.0	2018-11-28 15:59:28	2018-11-28 15:59:28			admin
221	Jim	General	4118106670	1111111	1	Card Issue	Income		100.0	100.0	2018-11-28 15:58:06	2018-11-28 15:58:06			admin

Figure 11- 44

11.3.4.1Refresh

Click **Refresh** to load the latest card cash receipts and payments data.

11.4 Consumption Detail Report

Click **Consumption Details** > **Consumption Details Report**, as shown below:

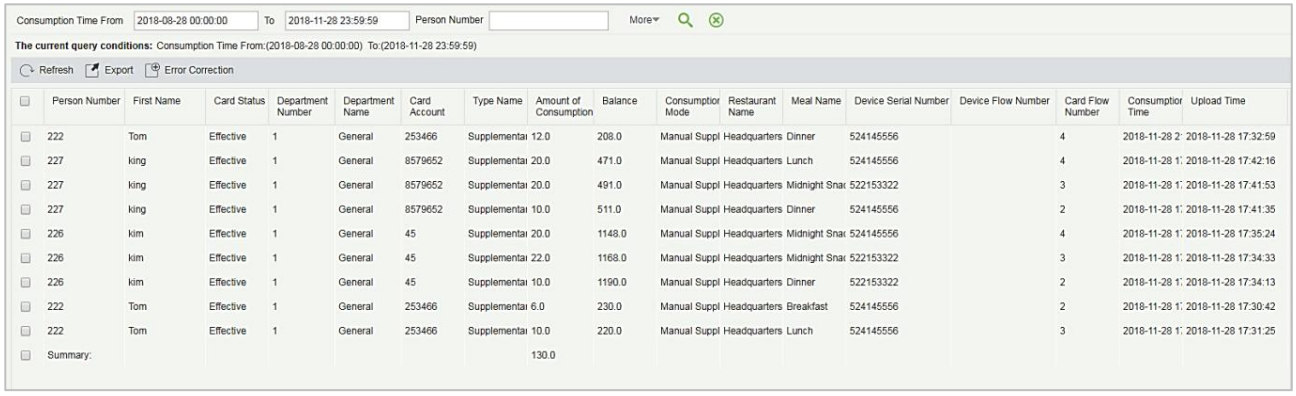


Figure 11- 45

11.4.1.1 Refresh

Click **Refresh** to load the latest consumption details.

11.4.1.2 Export

This feature allows you to export consumption details in EXCEL, PDF, CSV format files.

11.4.1.3 Error Correction

Click **Error Correction**. You can carry out the error correction process on the software. This operation is only valid for the records where the consumption type is the amount mode. Select a consumption record, read out the current balance of the card, enter the correct amount of consumption, and modify the balance of the card.

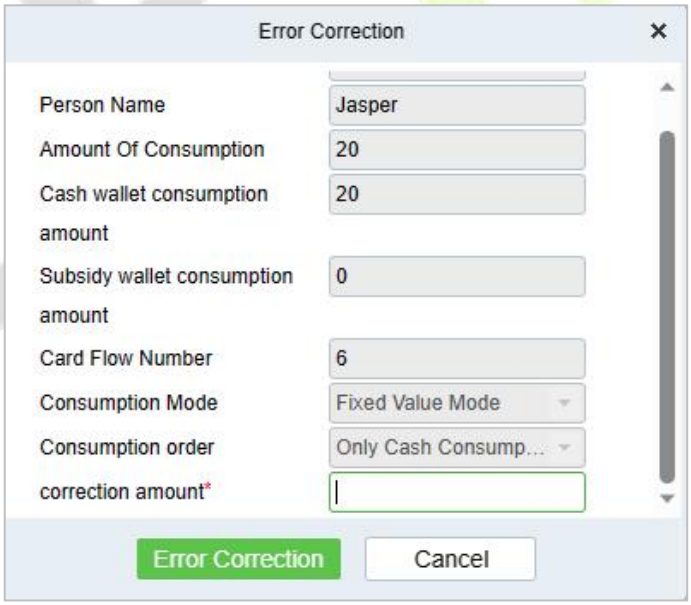


Figure 11- 46

✍Notes:

1) The same consumption record cannot be corrected repeatedly.
2) Software error correction automatically produces two new records: One is the record for the system error correction of the return of the original error consumption amount, the other is the correct consumption record of the manual supplement.

11.4.1.4 Import U Disk Record

If the equipment consumption record is found inconsistent with the software, you can export the consumption records of the machine (Select **U disk management** > **Download consumption records**) to the U disk, and then import the consumption records into the software (Select **Consumption** > **Consumption detail** > **Consumption detail report** > **Import U disk Records**).

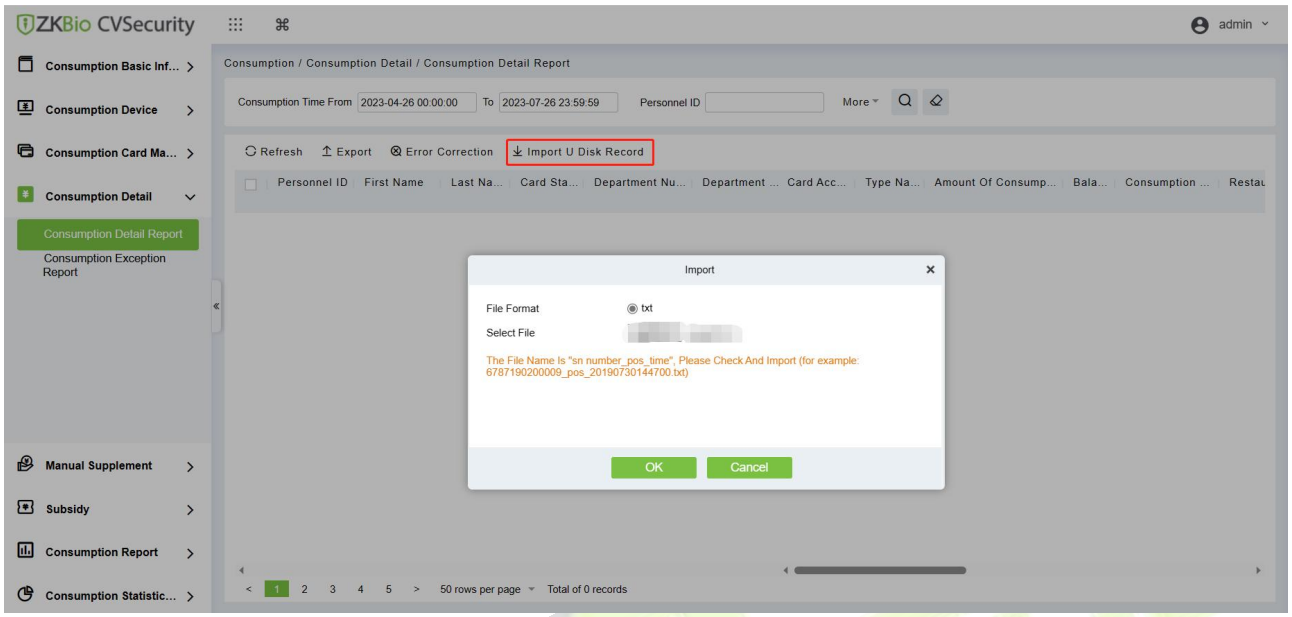


Figure 11- 47

11.5 Manual Supplement

It is used to enter some consumptions record details manually in the system.

✍**Note:** Before performing this operation, you need to have the relevant operation card.

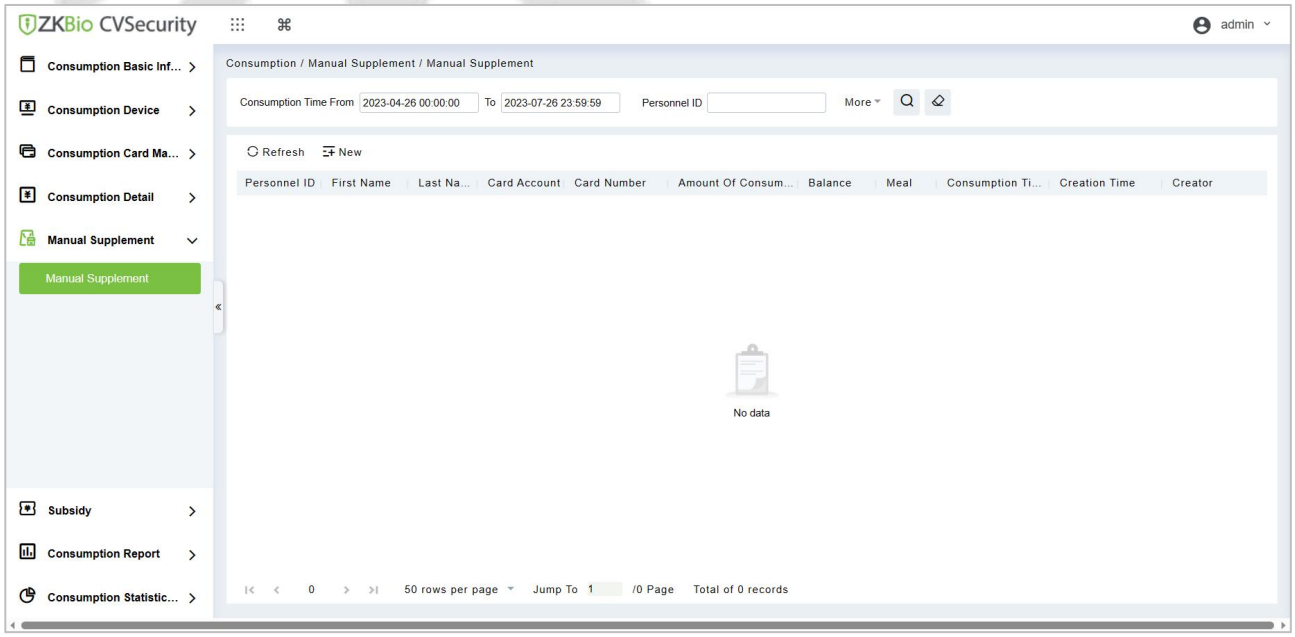


Figure 11- 48

11.5.1 New

You can manually enter some consumptions entries. Click **New** to open the addition interface.

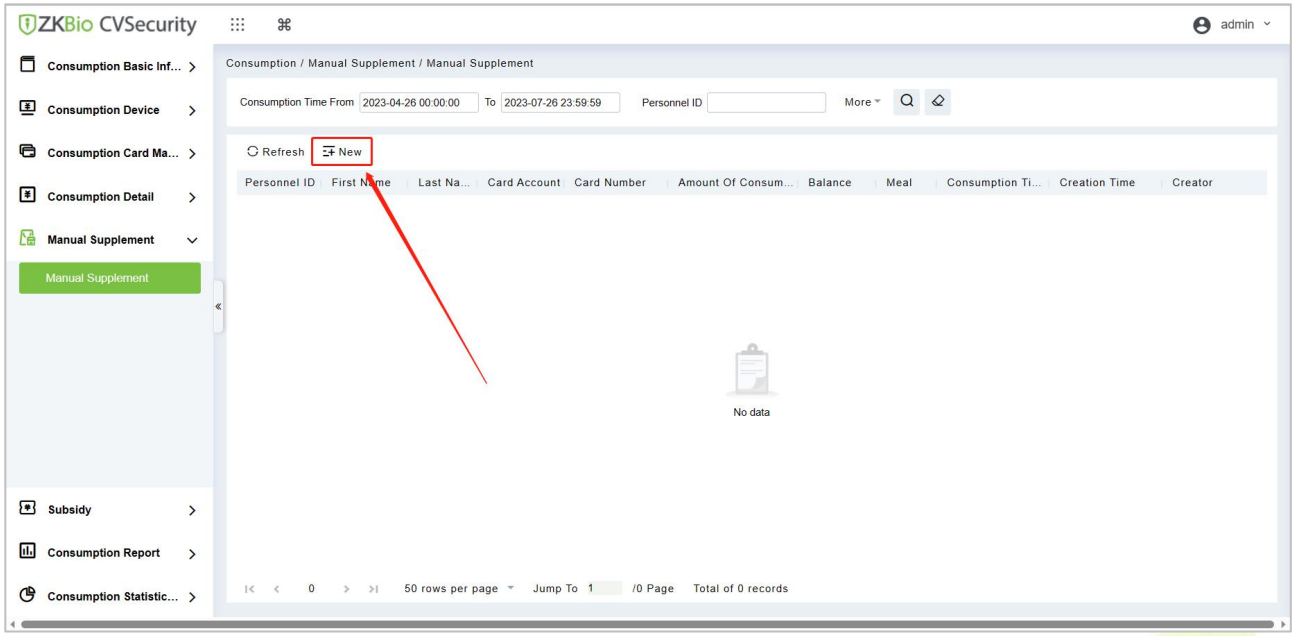


Figure 11- 49

You need to cross-check the relevant information of the card. When the user puts the relevant card into the card reader, click on read card to read the detailed data such as the Card Account, Card Number, Name, Person Number, Balance, Card Flow Number. Meals, Available Device, Consumption time and Consumption Amount.

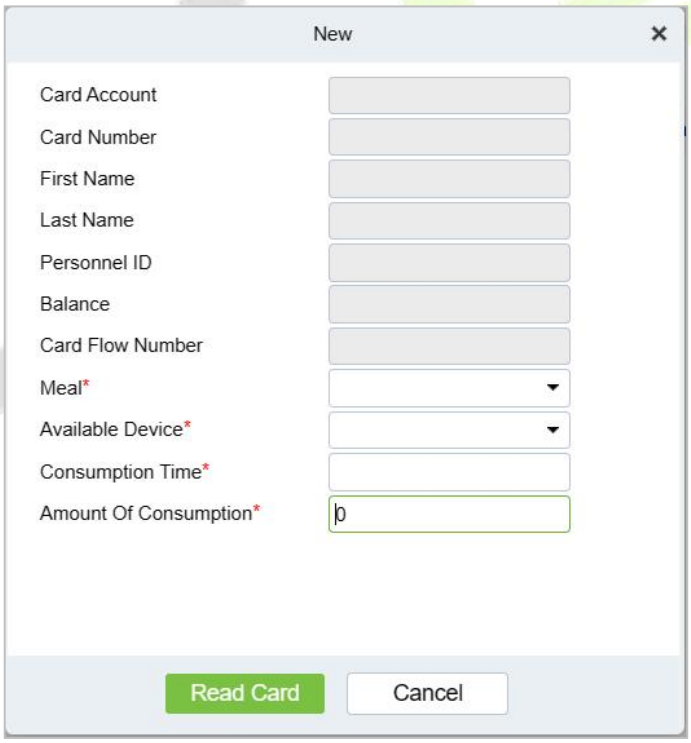


Figure 11- 50

11.5.2Refresh

This feature is mainly used to update the interface content with new data.

11.6 Subsidy

11.6.1 Subsidy Management

Click **Subsidy** > **Subsidy Management** to enter the subsidy page, you can perform different function related to subsidy:

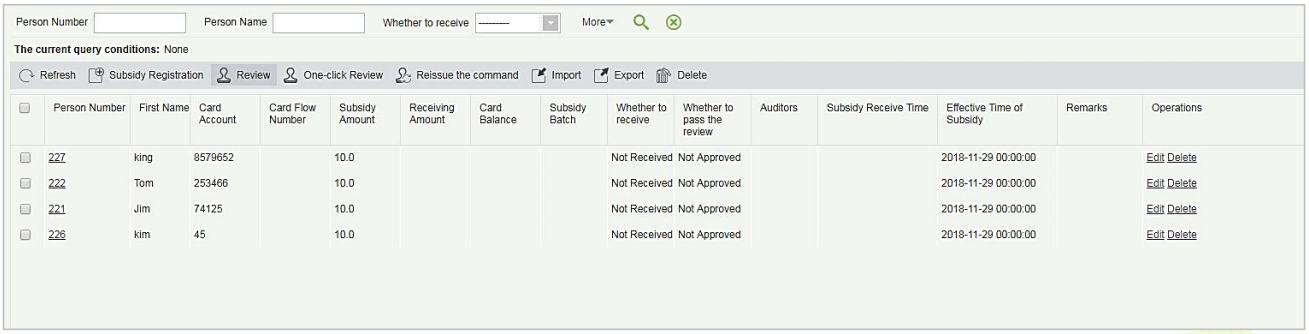


Figure 11- 51

✍**Note:** Before the subsidy operation, you need to add personnel in the **Personnel** module.

11.6.1.1 Add

1. Click Subsidy > Subsidy Management > Subsidy Registration to enter the subsidy registration interface.

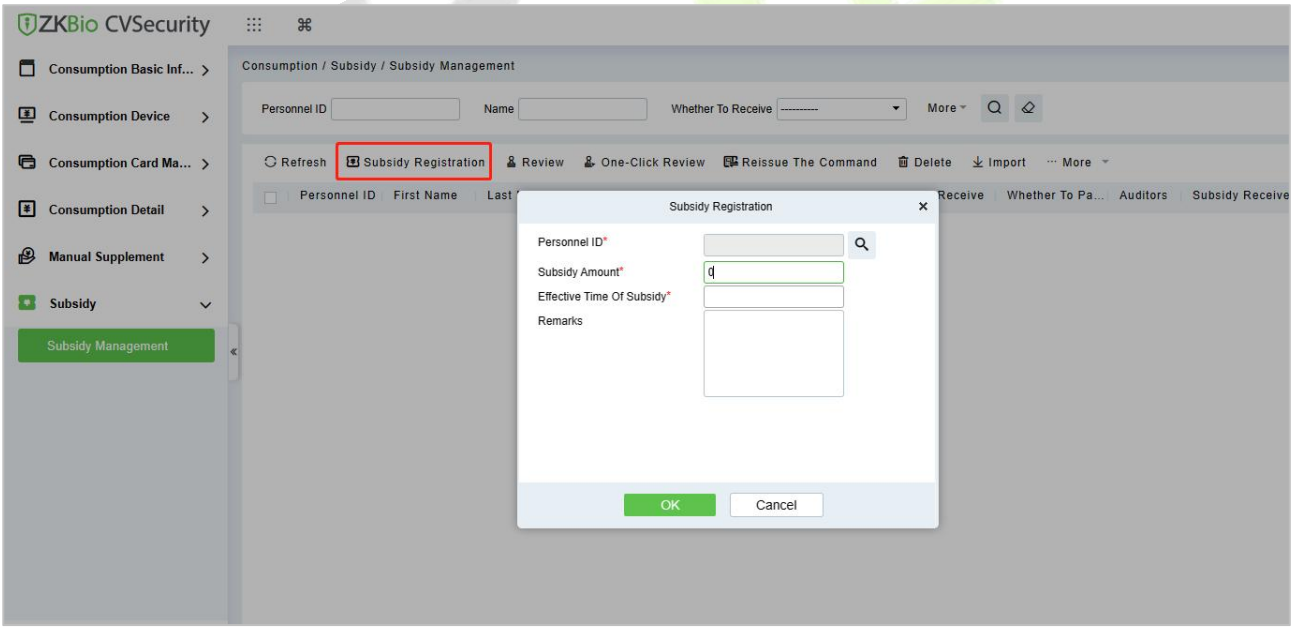


Figure 11- 52

2. Fill in the information and click OK to confirm.

11.6.1.2 Review

This function is mainly to review the audit. Before performing audit, you need to select the subsidy (select in the multi-select box). After clicking the review, an audit dialog box will pop up. The dialog box will display the person number and name as selected by the user.

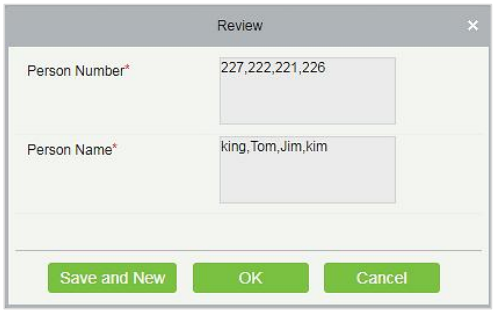


Figure 11- 53

11.6.1.3One-Click Review

This function is mainly to review the unapproved subsidies in the system, and will not deal with the subsidy records that have been approved. During the review process, if the unapproved subsidy cannot be approved for some reason (such as the user has already returned the card), the subsidy will not be processed.

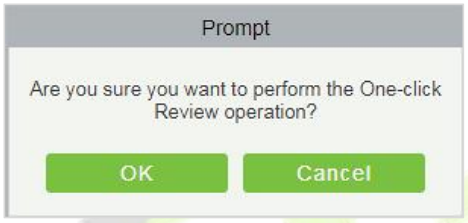


Figure 11- 54

11.6.1.4Reissue the Command

This function is primarily used to re-issue the subsidy to the subsidy machine. Select the required subsidy(s), then click Reissue the command. The dialog box will display the person number and name selected by the user, click OK to reissue the subsidy order to the subsidy machine.

Figure 11- 55

11.6.1.5Import

This function is used to import subsidies in batches.

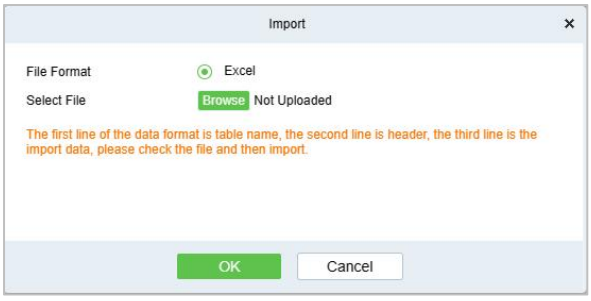


Figure 11- 56

If you want to download the sample template excel file for importing, click the **xlsx template** hyperlink.

Once the sample excel is downloaded, you can fill your data into it and save. Then click **Choose File** and select the saved excel file.

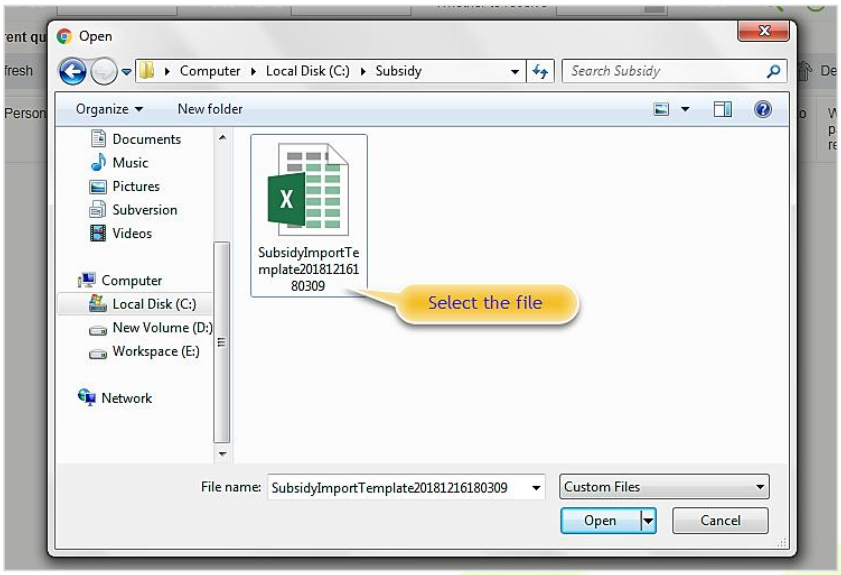


Figure 11- 57

Click **Open**.

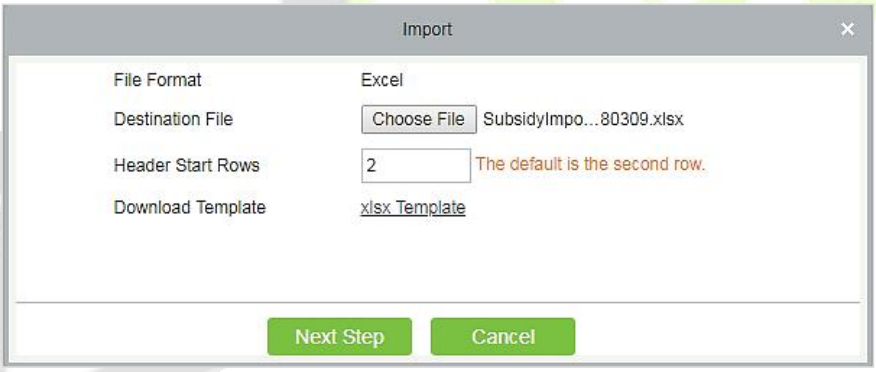


Figure 11- 58

Click **Next Step** button to proceed.

Figure 11- 59

Select the corresponding relationship between the subsidy record field and the imported field in Excel. Then click **Next Step** button to import the subsidy into the system. After the subsidy is imported, it will go directly to the approved or unapproved status based on your installation in which the initialization parameters of this software are determined.

11.6.1.6Export

This function is used to export the queried subsidies. Click on Export to open the exporting interface.

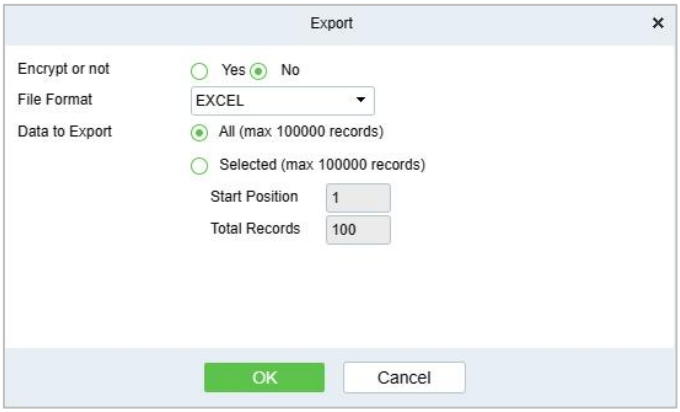


Figure 11- 60

Select the file type and export mode. If you select **All data**, then all query data limited to 40,000 will be exported. If you want to export only few results from the query, then select the second mode and enter the desired start and end points of the required data to be exported.

Click **OK** to finish.

11.6.1.7Delete

Select the required subsidy record(s) and click Delete under the operation bar to delete the subsidy record. It only supports the removal of unapproved subsidy(s).

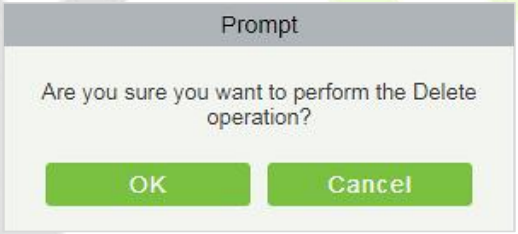


Figure 11- 61

11.6.1.8Edit

Click **Edit** under the operation bar to modify the unapproved subsidies.

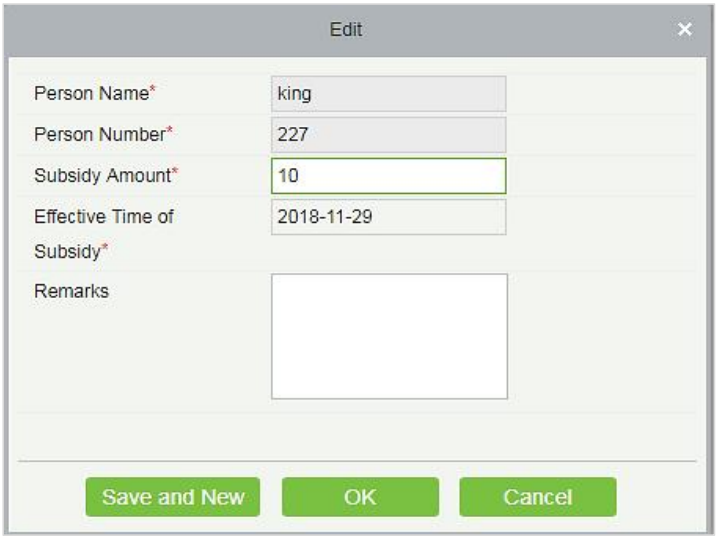


Figure 11- 62

Modify the required information and click the **OK** to save successfully.

11.6.2Consumption Report

The statistical report consists of 9 modules: Issue Card Table, Top Up Table, Refund Table, Subsidy Table, Table of Return Card, Card Cost Table, Card Balance Table, Non-Card Return Card Table, And Table of Resume The Card.

11.6.2.1Issue Card Table

Click Consumption Report > Issue Card Table, as shown below:

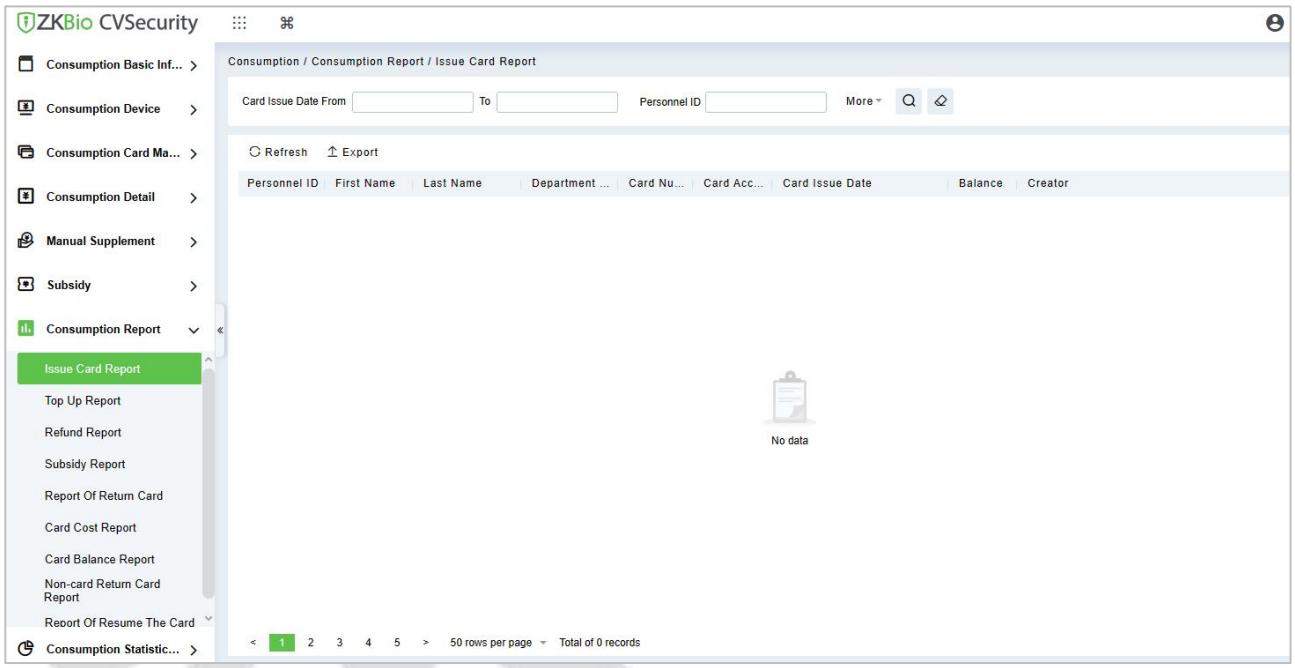


Figure 11- 63

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

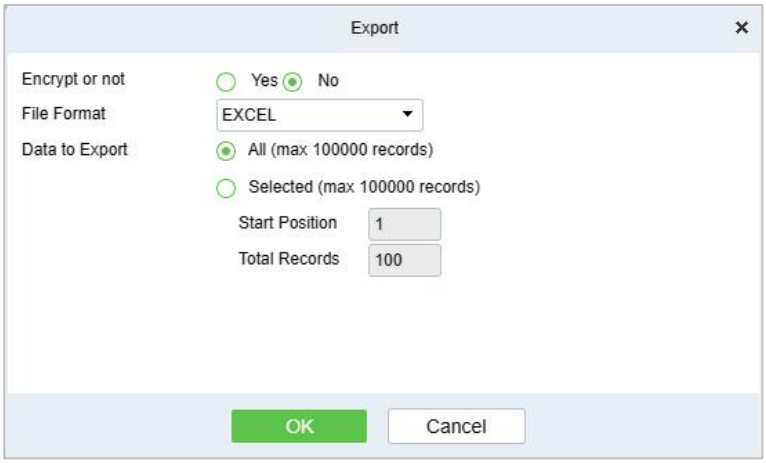


Figure 11- 64

11.6.2.2Top Up Table

Click Consumption Report > Top Up Table, as shown below:

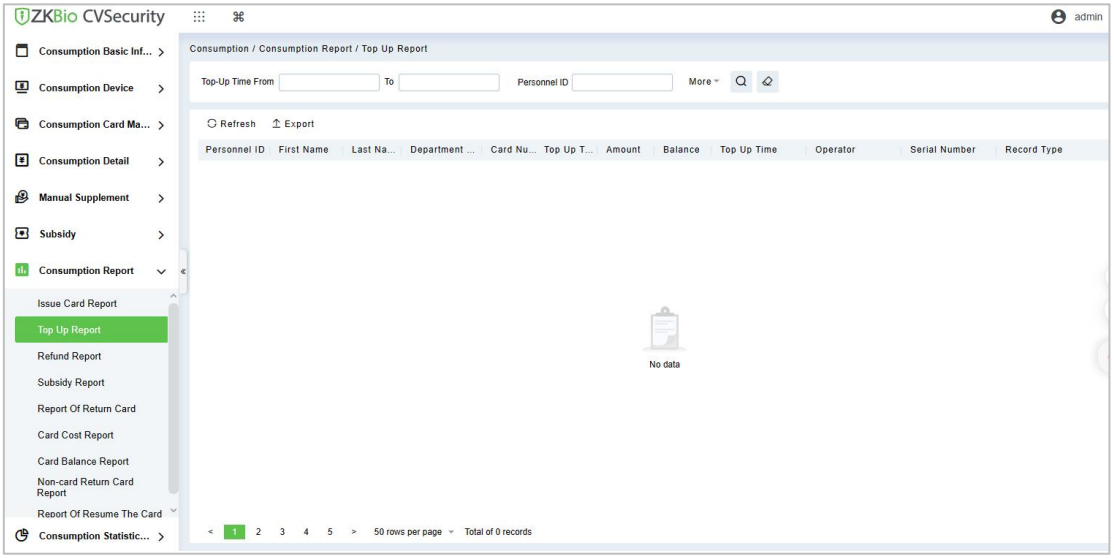


Figure 11- 65

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

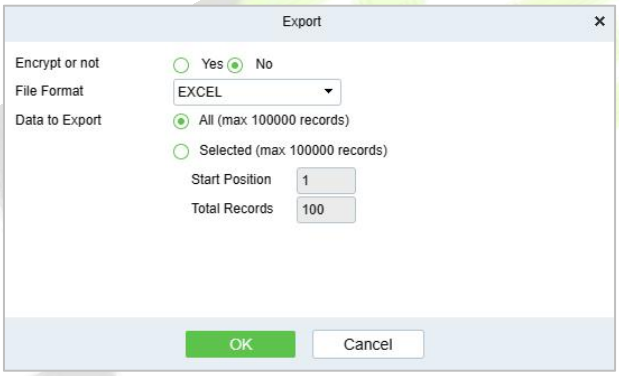


Figure 11- 66

11.6.2.3 Refund Table

Click Consumption Report > Refund Table, as shown below:

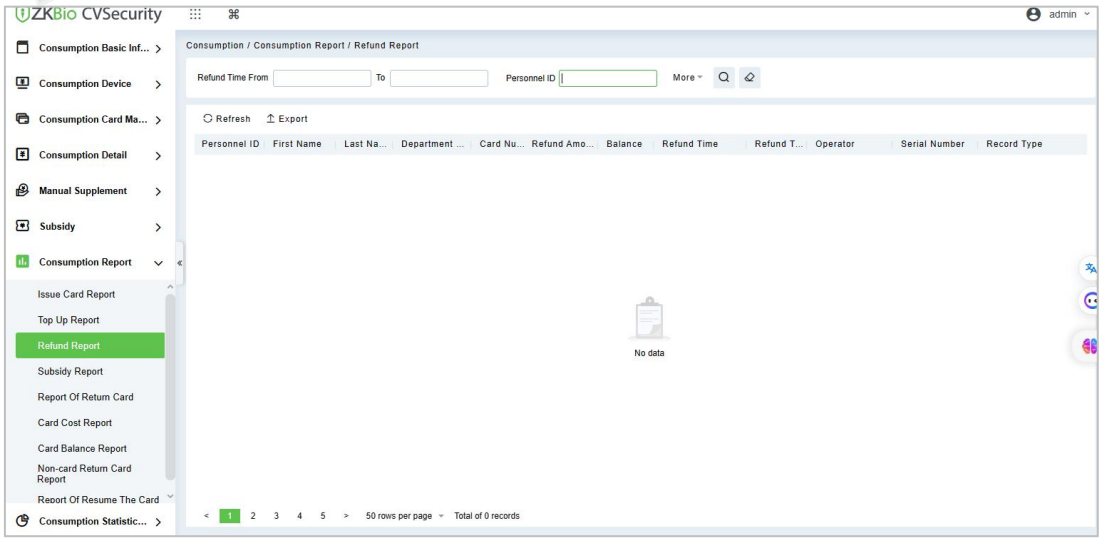


Figure 11- 67

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

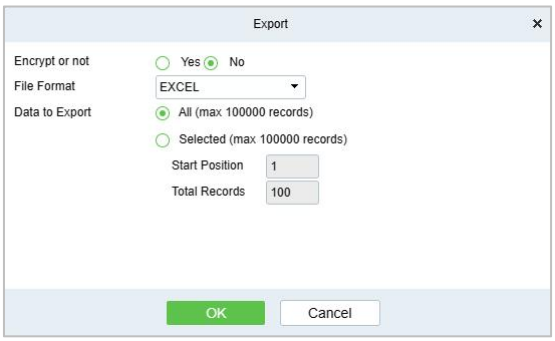


Figure 11- 68

11.6.2.4Subsidy Table

Click Consumption Report > Subsidy Table, as shown below:

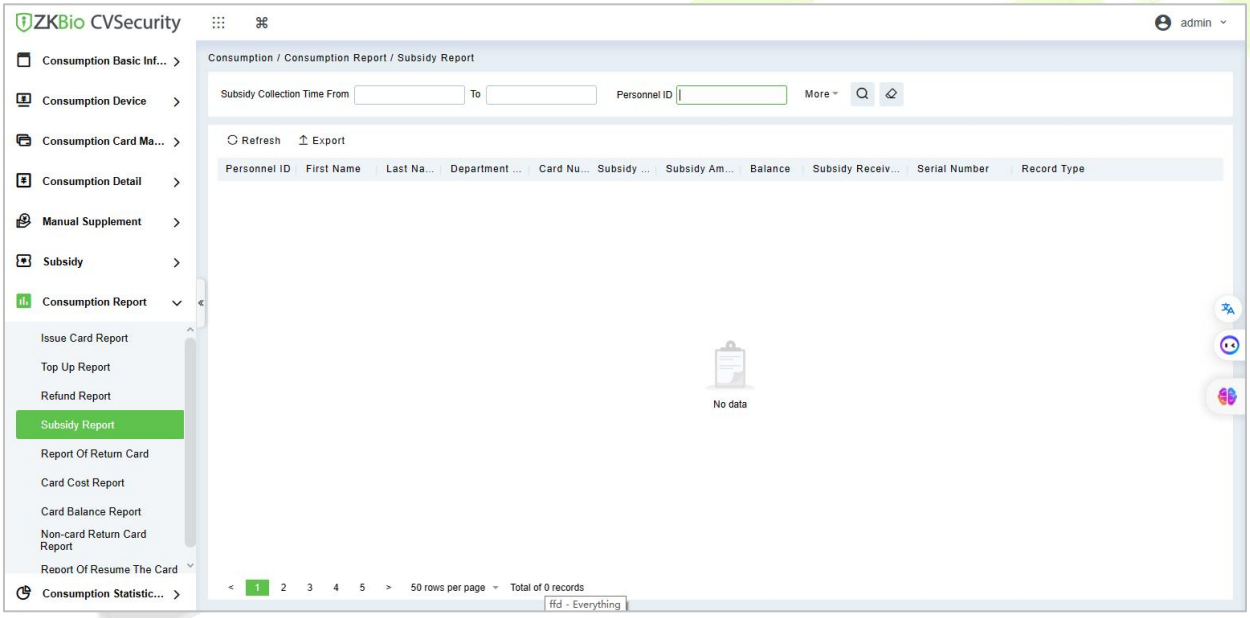


Figure 11- 69

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

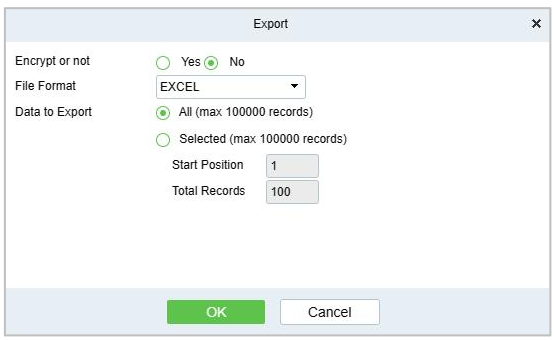


Figure 11- 70

11.6.2.5Report of Return Card

Click **Consumption Report** > **Table of Return Card**, as shown below:

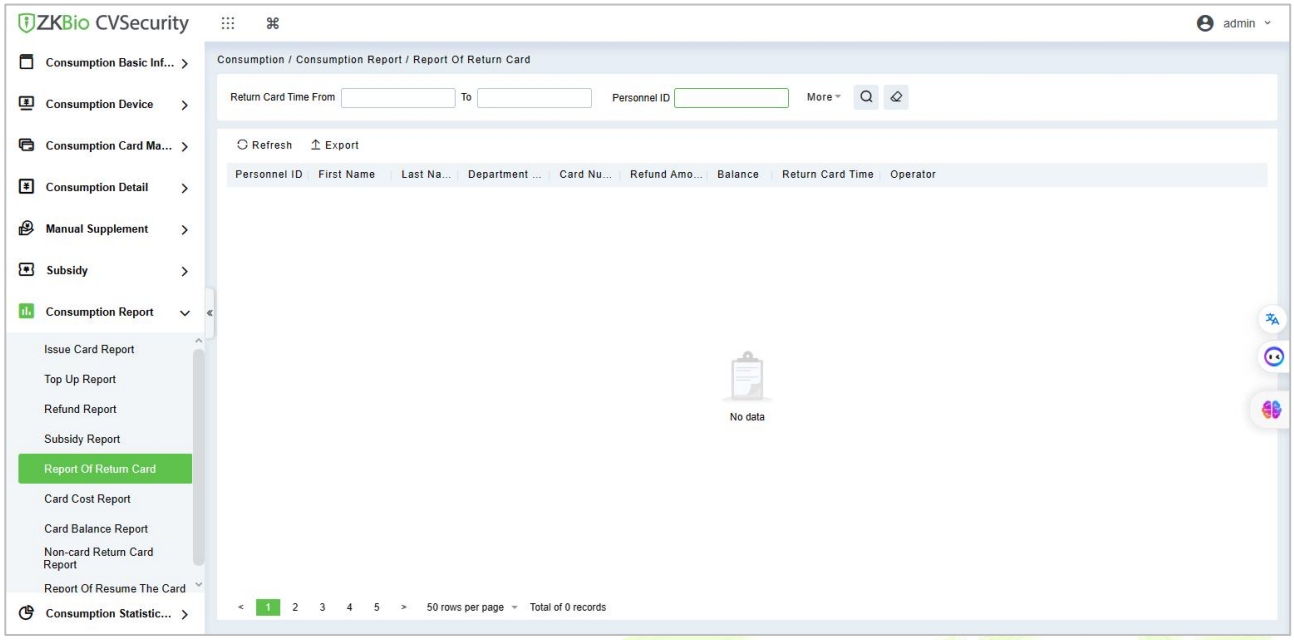


Figure 11- 71

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

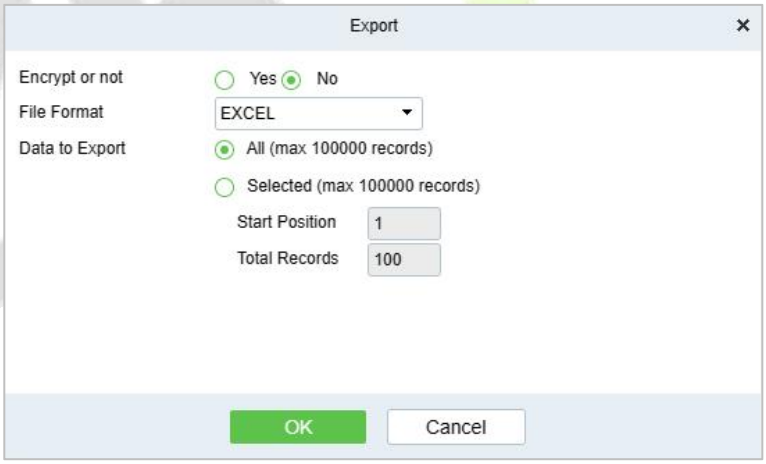


Figure 11- 72

11.6.2.6Card Cost Table

Click **Consumption Report** > **Card Cost Table**, as shown below:

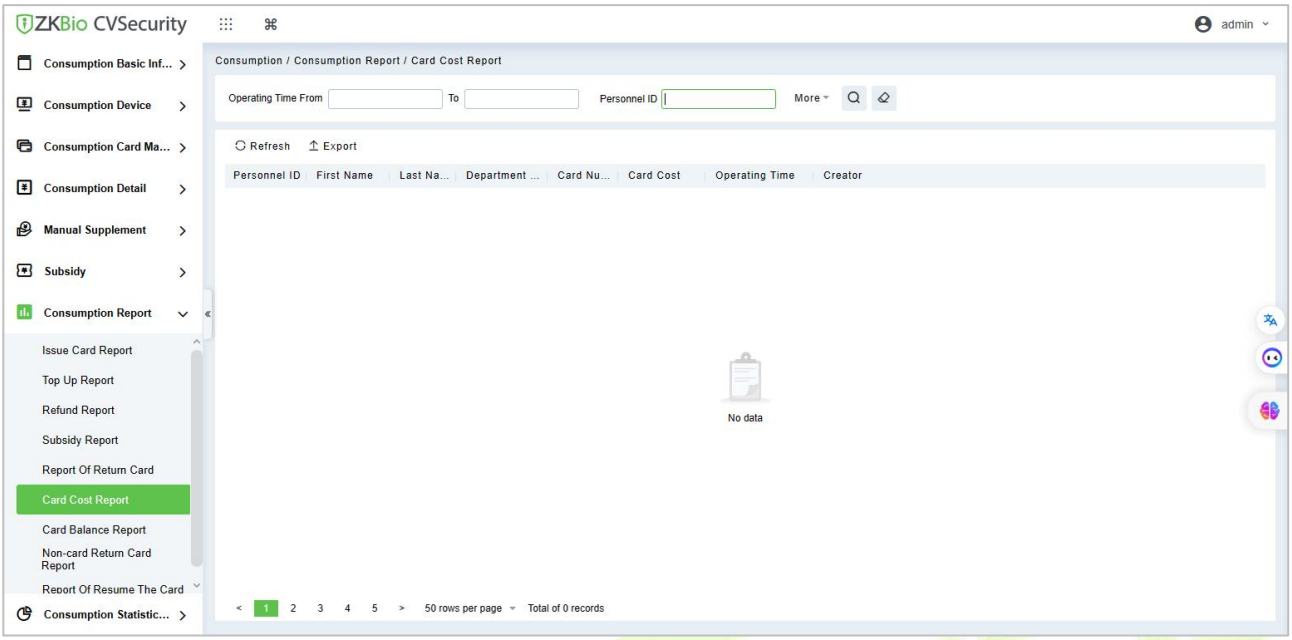


Figure 11- 73

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

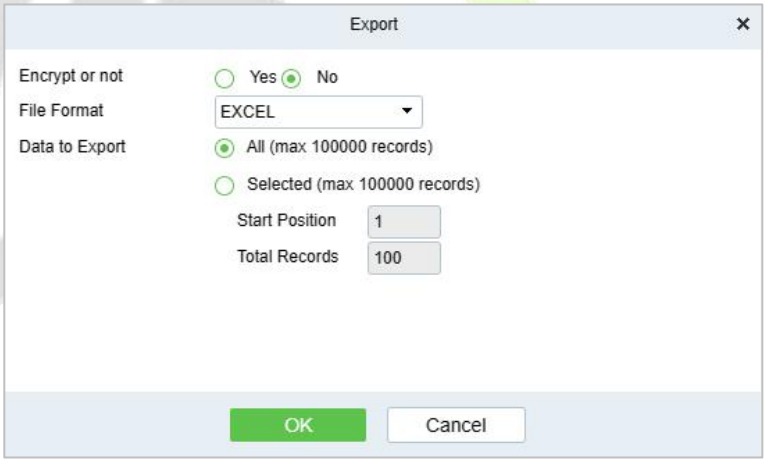


Figure 11- 74

11.6.2.7Card Balance Table

Click **Consumption Report** > **Card Balance Table**, as shown below:

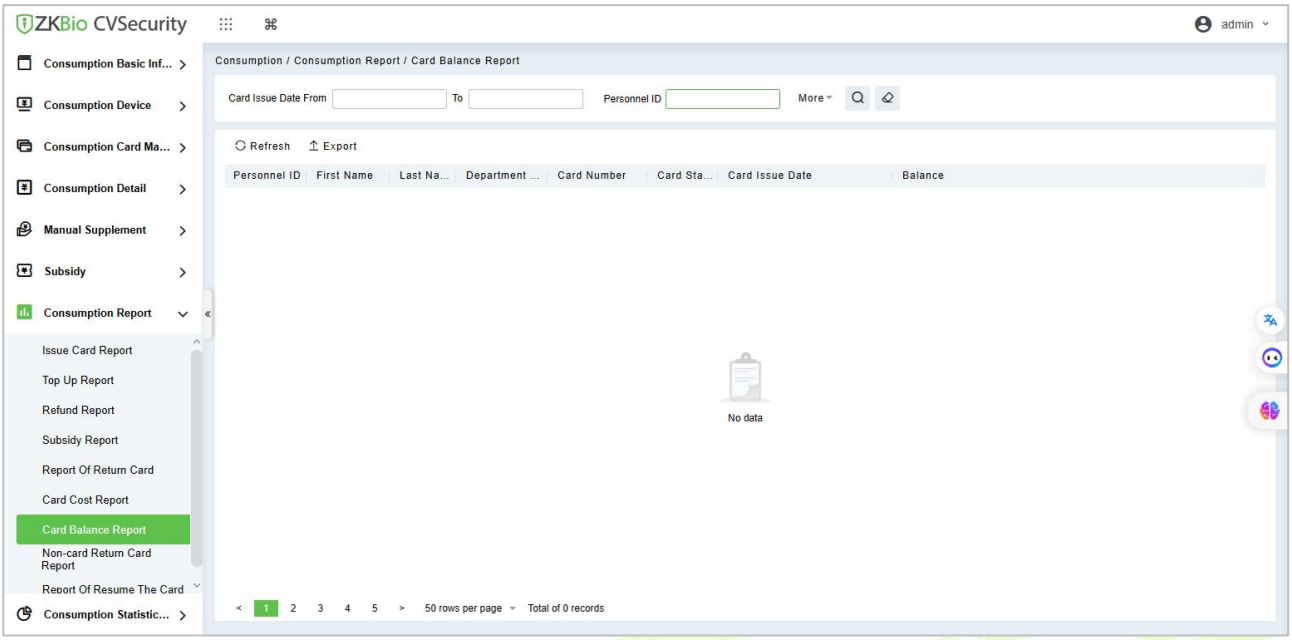


Figure 11- 75

Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

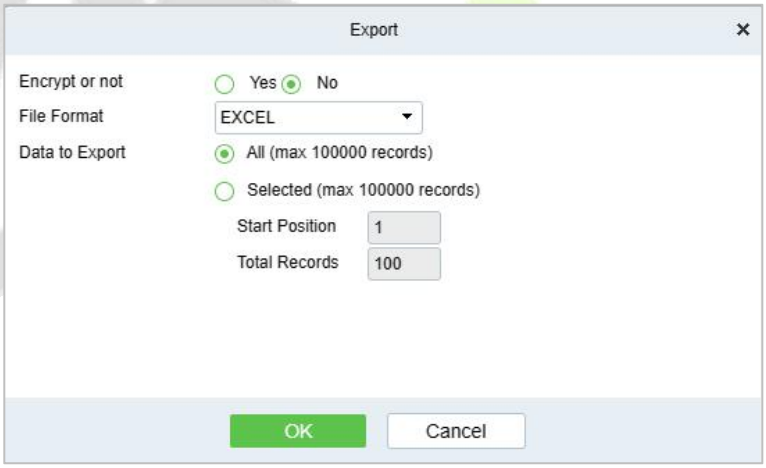


Figure 11- 76

11.6.2.8Non-card Return Card Table

Click **Consumption Report** > **Non-card Return Card**, as shown below:

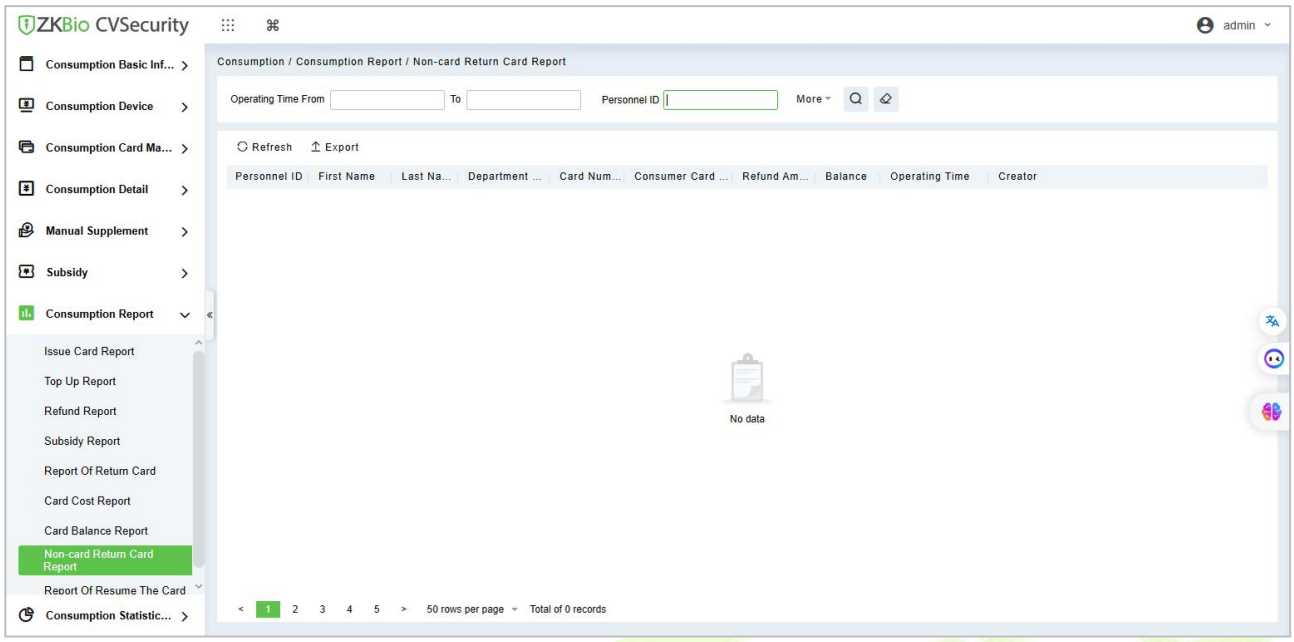


Figure 11- 77

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

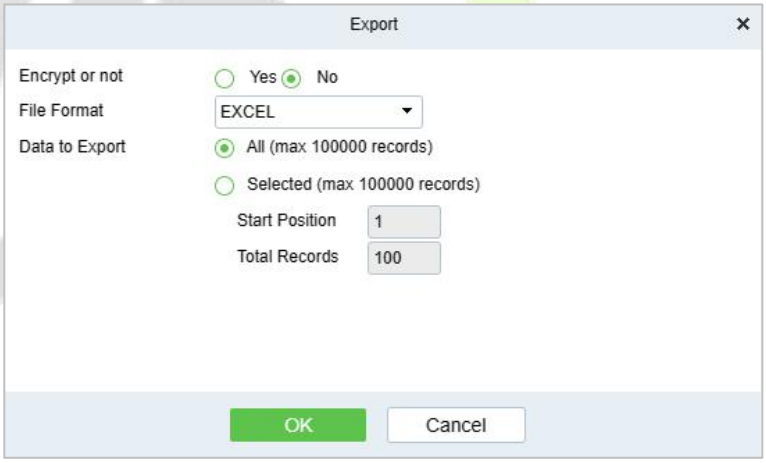


Figure 11- 78

11.6.2.9Table of Resume the Card

Click **Consumption Report** > **Table of Resume the Card**, as shown below:

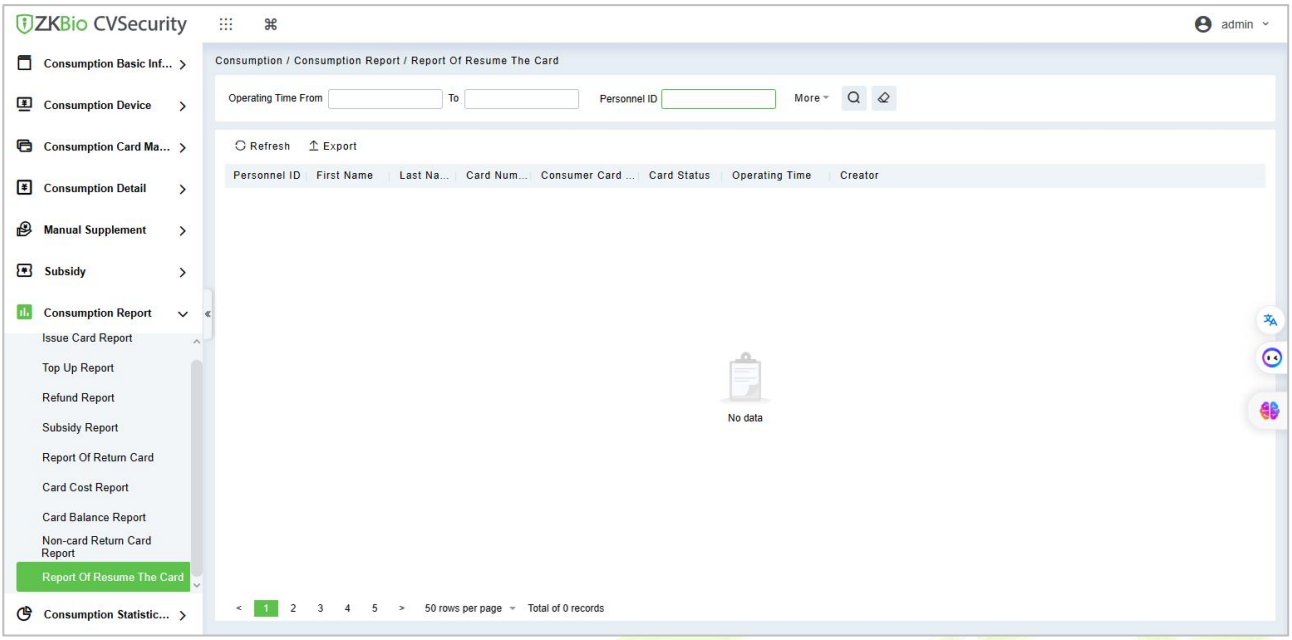


Figure 11- 79

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

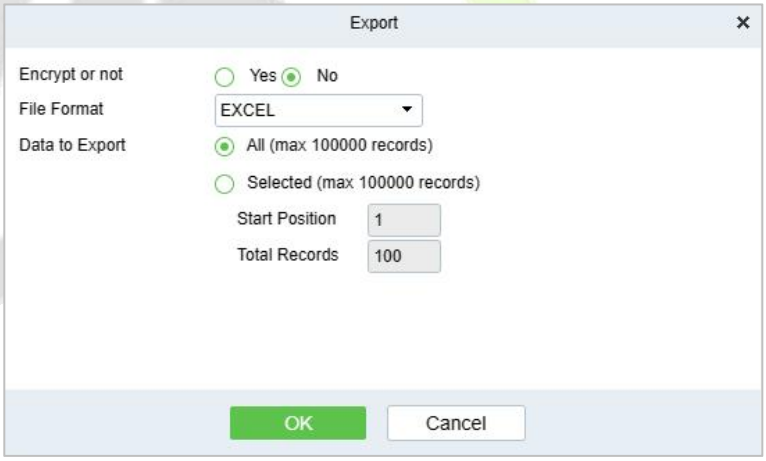


Figure 11- 80

11.6.3 Statistical Report

The statistical report contains the statistical information of consumption system module.

11.6.3.1 Personal Consumption Table

Click **Statistical Report** > **Personal Consumption Table**, as shown below:

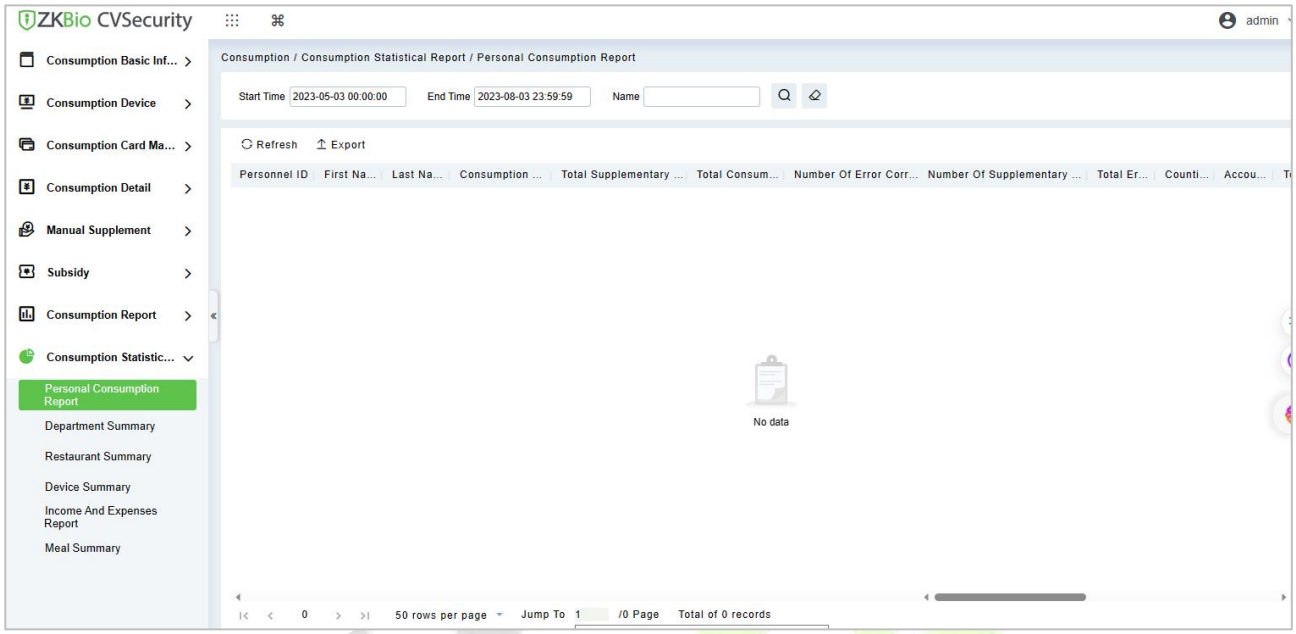


Figure 11- 81

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

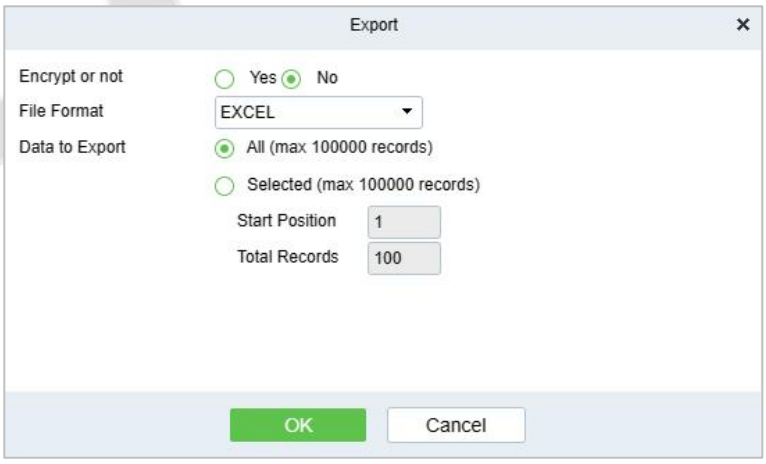


Figure 11- 82

● Refresh:

Click **Refresh** to load the latest personal consumption statistics table data.

✍ **Note:** If the page personal consumption statistics table data is more, you can also enter the person name, department name, consumption time in the search field, click to search and query.

The data statistics column includes below information:

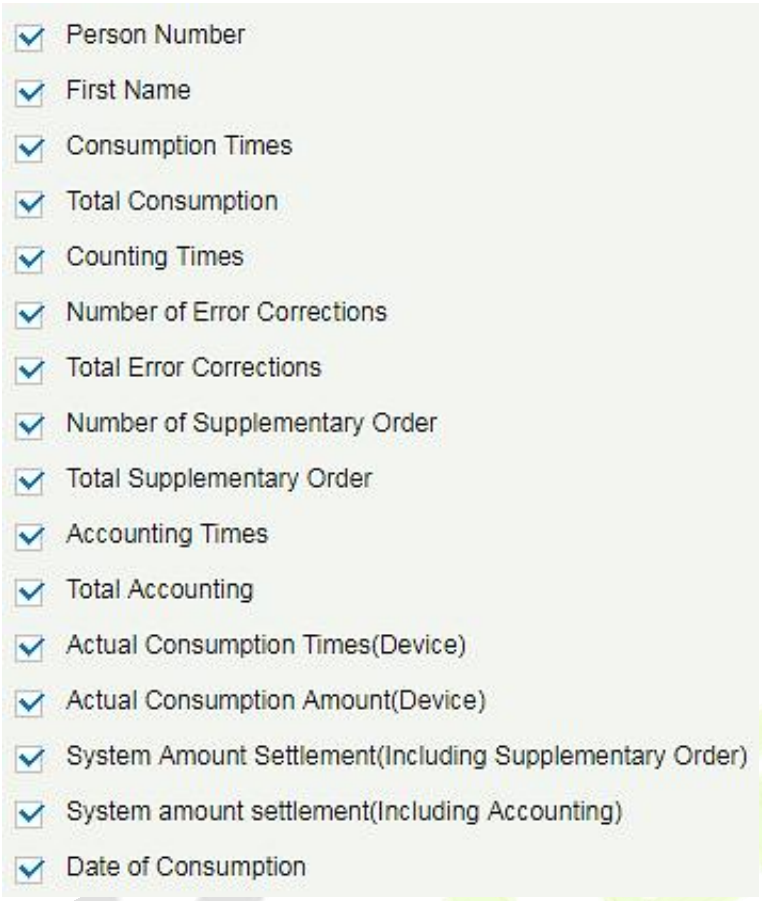


Figure 11- 83

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number Of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times Of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (Device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (Device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (Including Supplementary Order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (Including Billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

11.6.3.2Department Summary Table

Click **Statistical Report** > **Department Summary Table** as shown below:

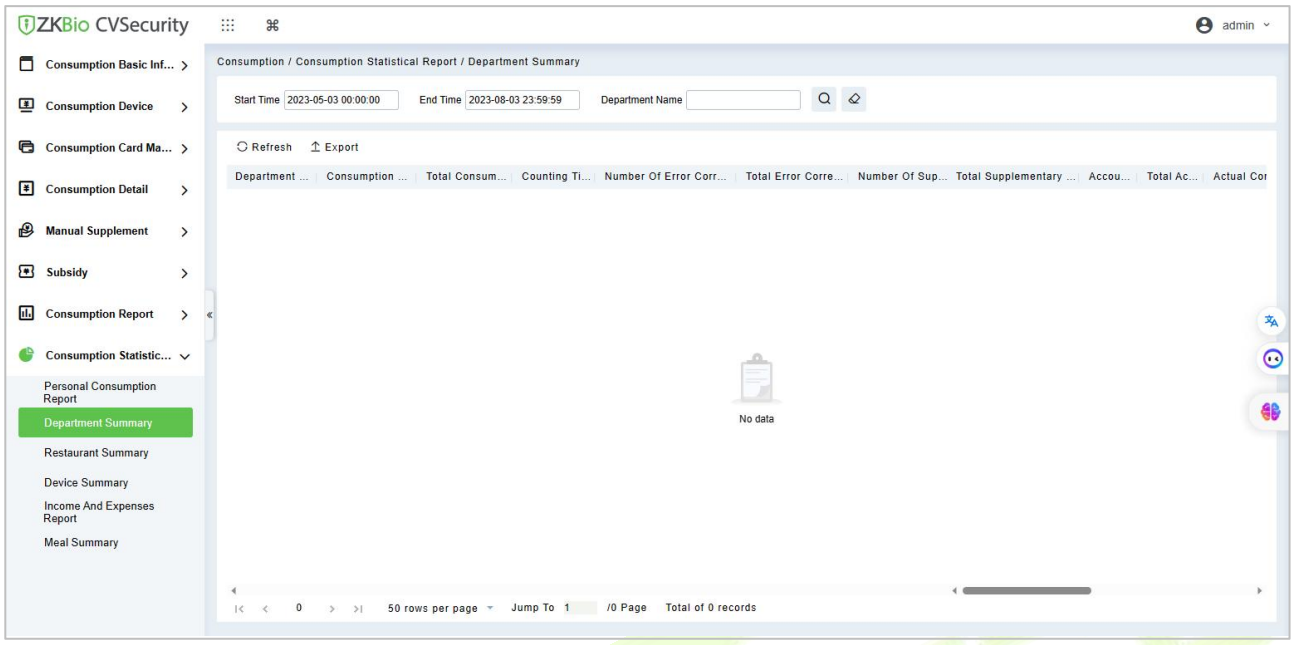


Figure 11- 84

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

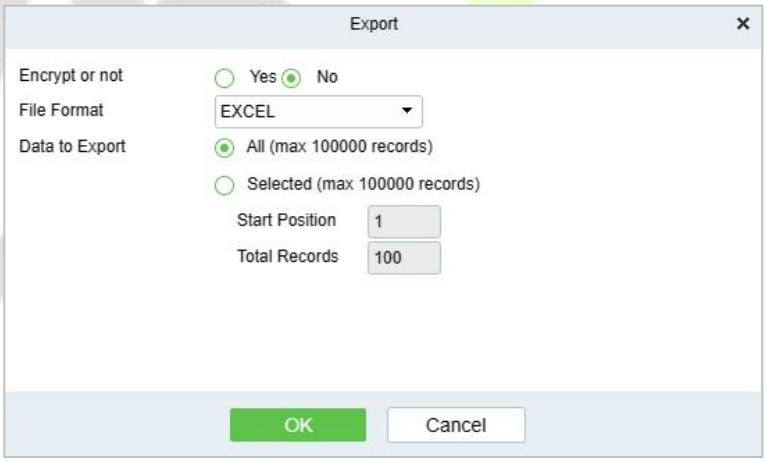


Figure 11- 85

Refresh

Click **Refresh** to load the latest department summary table data.

✍**Note:** If the page department summary table data is more, you can also enter the department name and consumption time in the search field, and click to search for the query.

The data statistics column includes:

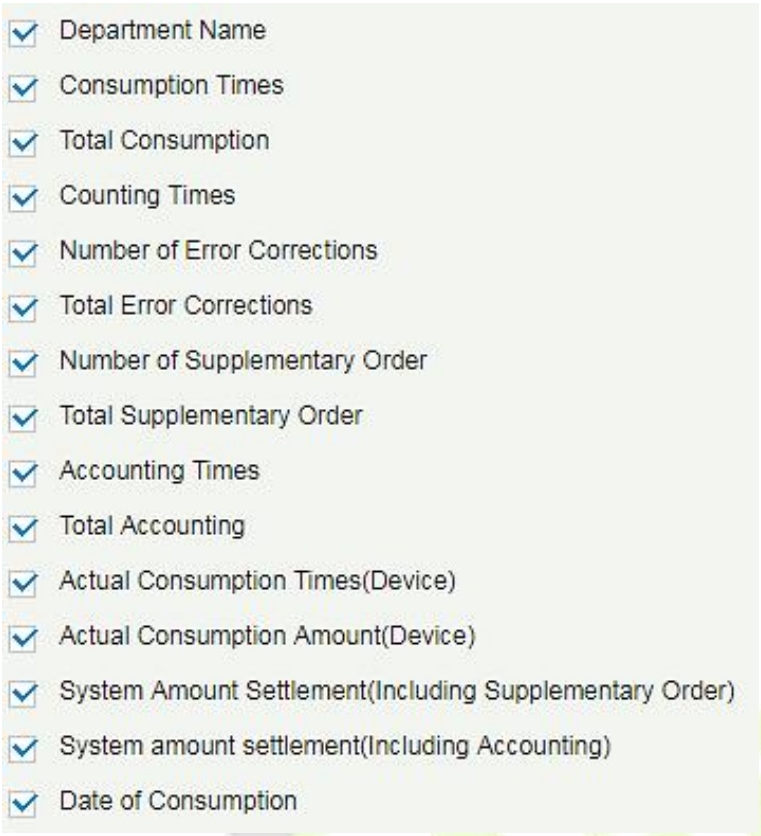


Figure 11- 86

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type.
- **Total Error Correction** = Total amount of error correction for the particular type.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

11.6.3.3 Restaurant Summary

Click **Statistical Report** > **Restaurant Summary**, as shown below:

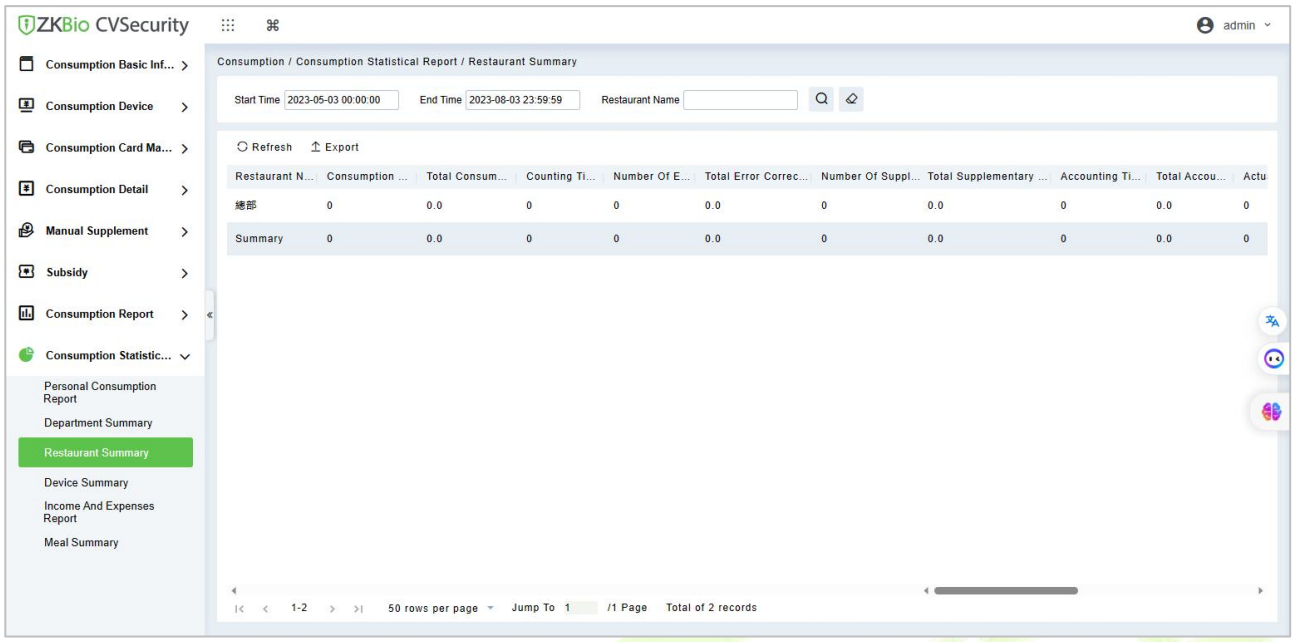


Figure 11- 87

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

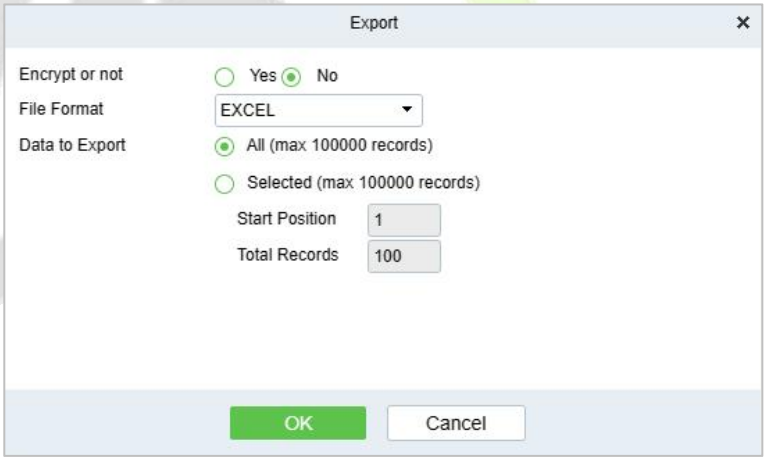


Figure 11- 88

● Refresh:

Click **Refresh** to load the latest restaurant summary table data.

✍ **Note:** If the page restaurant summary table data is more, you can also enter the restaurant name, consumption time in the search bar, click to search and query.

The data statistics column includes:

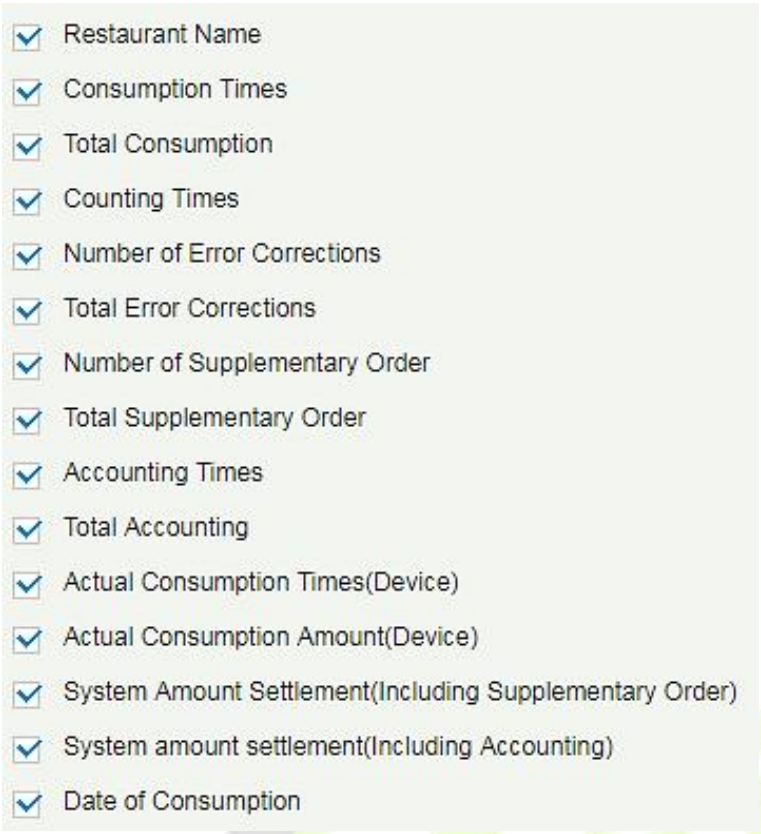


Figure 11- 89

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

11.6.3.4Device Summary Table

Click **Statistical Report** > **Device Summary Table**, as shown below:

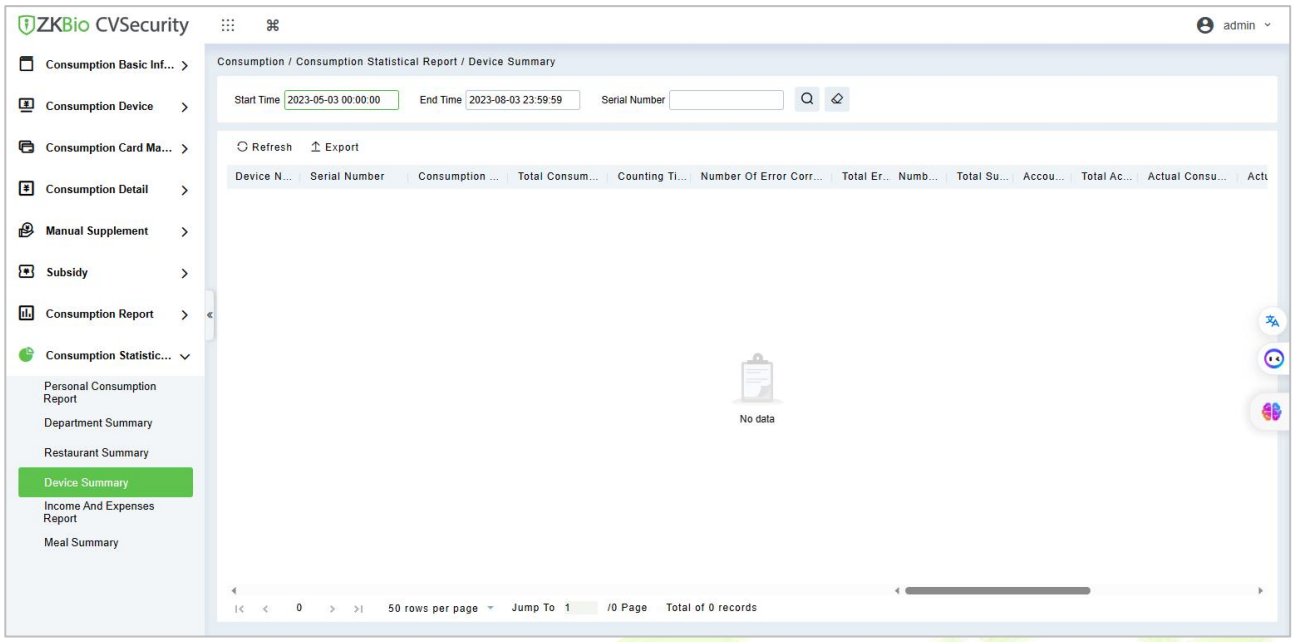


Figure 11- 90

Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

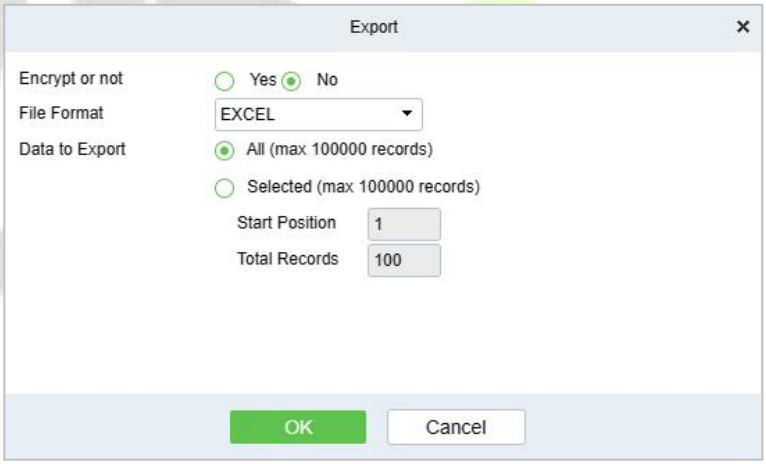


Figure 11- 91

● Refresh:

Click **Refresh** to load the latest equipment summary table data.

✍**Note:** If there is more data on the page device summary table, you can also enter the device name and consumption time in the search field, and click to search for it.

The data statistics column includes:

Figure 11- 92

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

11.6.3.5Income and Expenses Table

Click **Statistical Report** > **Income and Expenses Table**, as shown below:

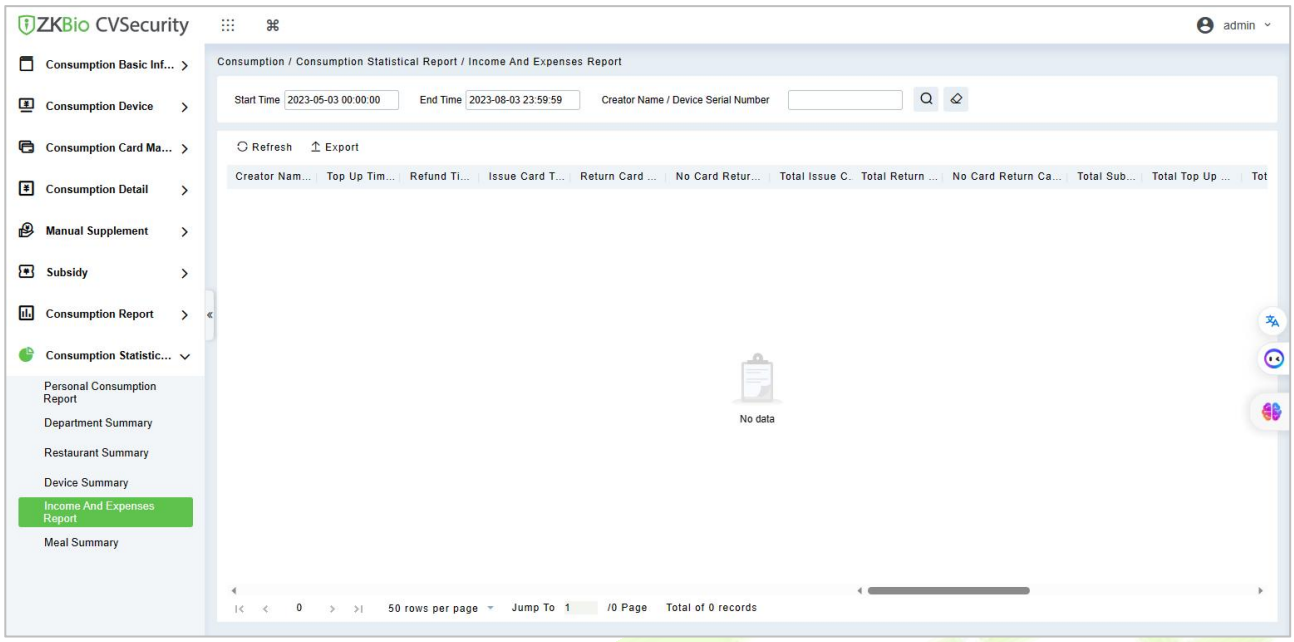


Figure 11- 93

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

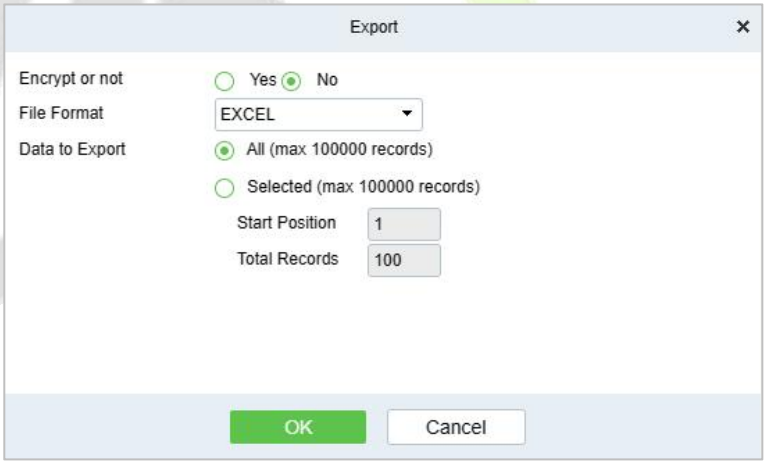


Figure 11- 94

● Refresh:

Click **Refresh** to load the latest revenue and expenditure summary table data.

✍**Note:** If there is more data on the page income and expenditure summary table, you can also enter the creator name/device serial number and summary time in the search field, and click to search for it.

The data statistics column includes

Figure 11- 95

- **Top up Times** = The total number of counts a card was added extra amount.
- **Refund Times** = The total number of counts a card were refunded.
- **Issue Card Times** = The total number of counts a card were issued.
- **Return Card Times** = The total number of counts the cards were returned.
- **Non-card Return card Times** = The total count of Non-card Return card.
- **Total Issue Card** = The total number of issued card.
- **Total Return card** = The total number of cards returned.
- **No Card Return Card Total** = The total number of blocked card which are not returned.
- **Total Subsidy** = The total amount of subsidy for the card type.
- **Total Top-up Offer** = The total amount of top-up discount for the card type.
- **Total Top-up** = The total amount of top-up for the card type.
- **Total Refund** = The total amount of refund for the card type.
- **Card Cost Support** = The total amount of card cost for the card type.
- **Management Fee** = The total amount of management fee for the card type.
- **Card Cost Expense** = The total amount of card cost for the card type.
- **Total Revenue and Expenditure** = (Total Top up + Card Cost Expense + Total Issue Card + Management fee) - (Total Refund - Total Return Card).

11.6.3.6Meal Summary Table

Click **Statistical Report** > **Meal Summary Table**, as shown below:

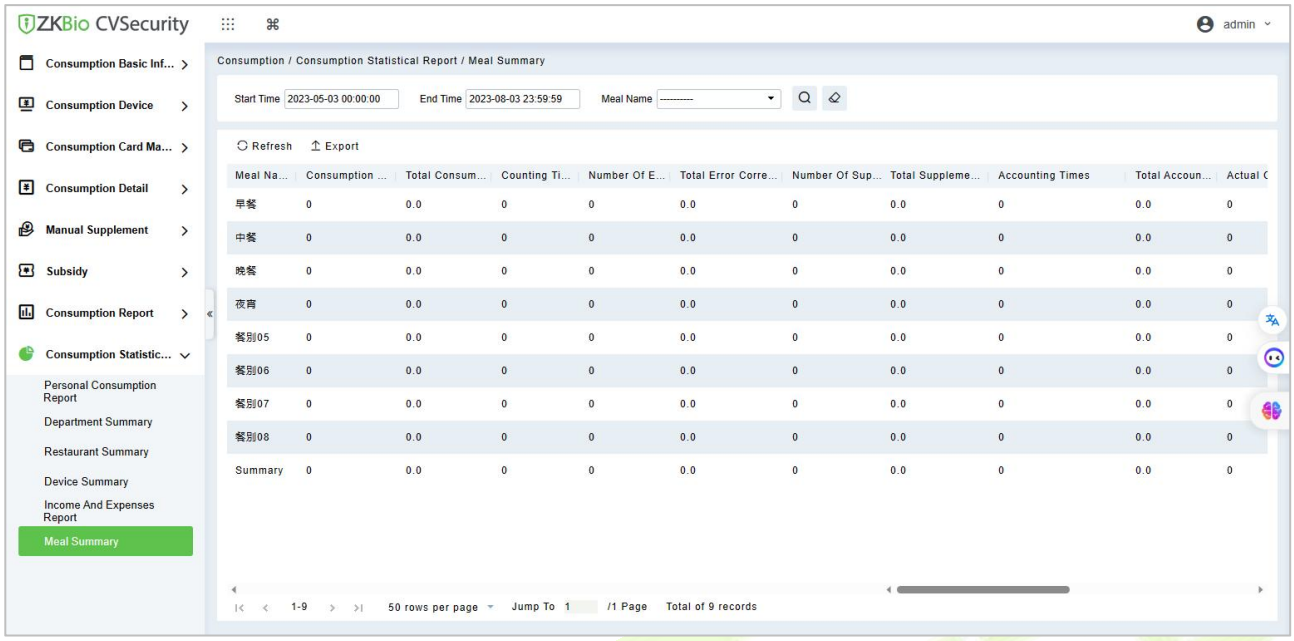


Figure 11- 96

● Export:

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

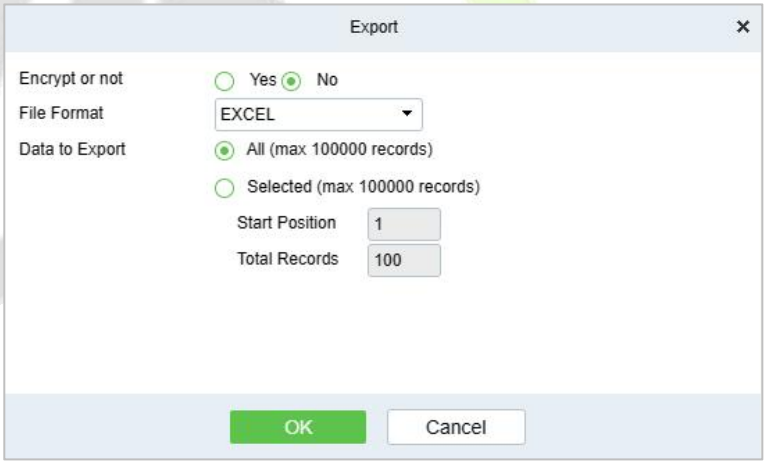


Figure 11- 97

● Refresh:

Click **Refresh** to load the latest meal summary table data.

✍ **Note:** If there is more data in the page meal summary table, you can also enter the device name, name, and consumption time in the search field, and click to search for it.

The data statistics column includes:

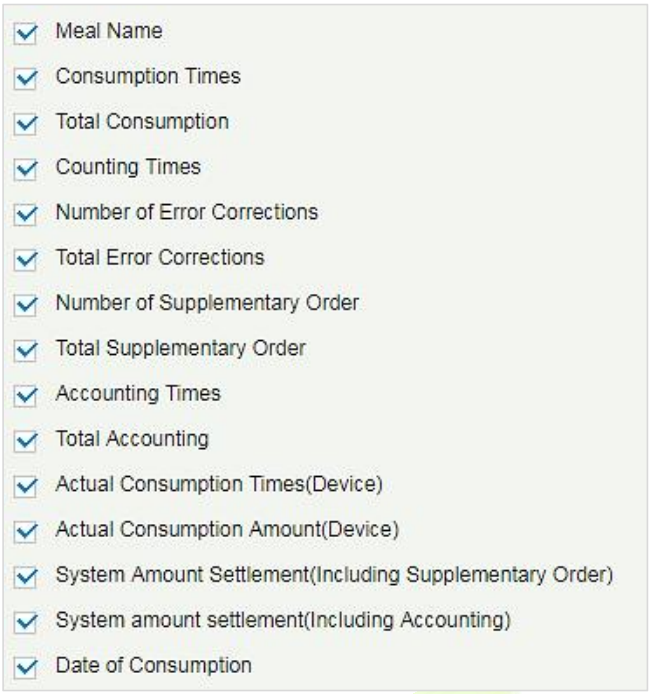


Figure 11- 98

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12 Consumption (Online) System

Based on controlled devices by software, it realizes the online consumption mode combining the functions of the Promerc-300 face consumer machine. The software mainly configures background data, including consumption time zone, commodity information, restaurant information and other data. Centralize various data on the device, generate consumption reports, and operate online account creating, refund, recharge, subsidy, etc. on the software.

12.1 Consumption Basic Management

12.1.1 Piecewise Fixed Value

Piecewise Fixed value is the value and validity of a card which is supposed to be used on the consumer device. Click **Consumption Basic Management** > **Piecewise Fixed Value** as shown in the following figure.

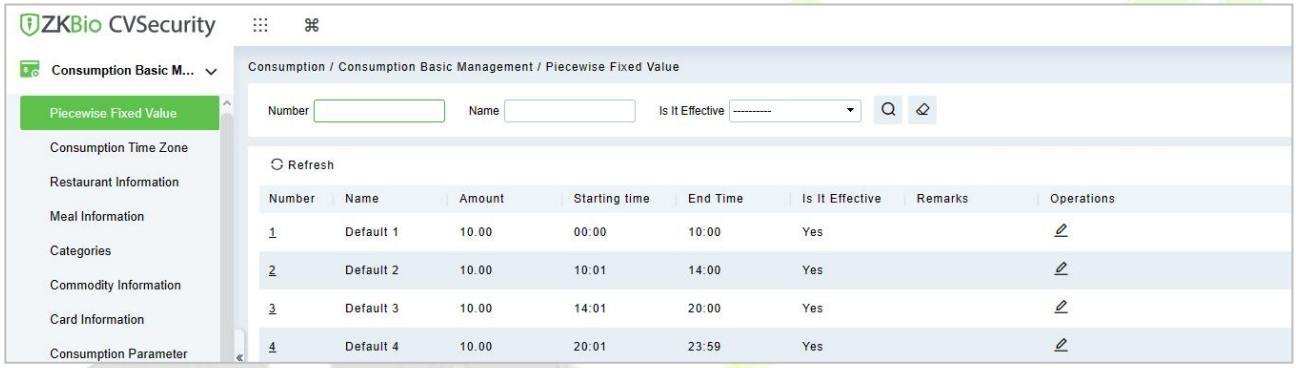


Figure 12- 1

12.1.1.1 Edit

By default, there are eight values, Click **Edit** on the operation column to open the modification dialog box.

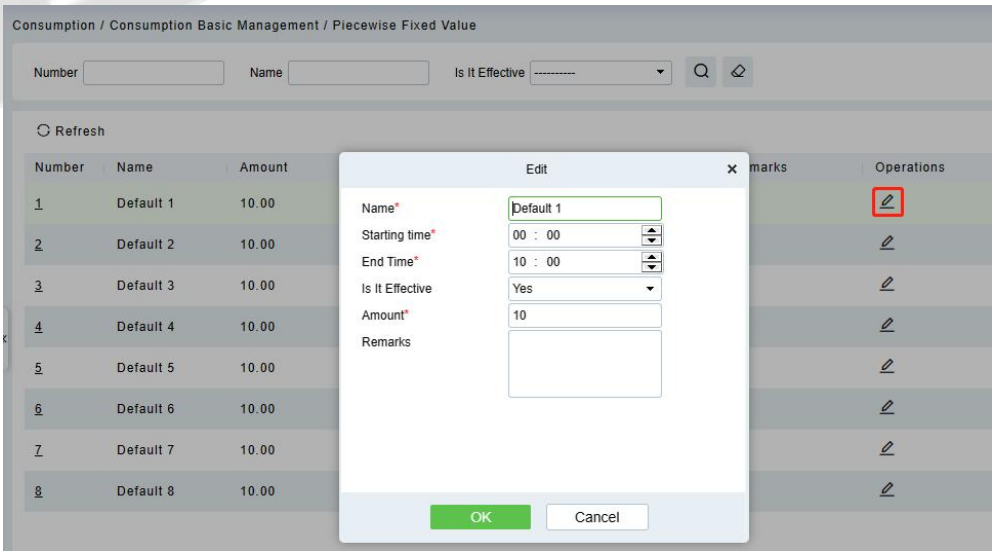


Figure 12- 2

You can provide the desired information in the dialog box which include: **Name**, **Start time**, **End time**, **Whether Effective**, **Amount**, and **Remarks**.

12.1.2Consumption Time Zone

Click **Consumption Basic Management** > **Consumption Time Zone** as shown in the following figure:

By default, the system has some Consumption Time zones, you can select and edit according to your preferences.

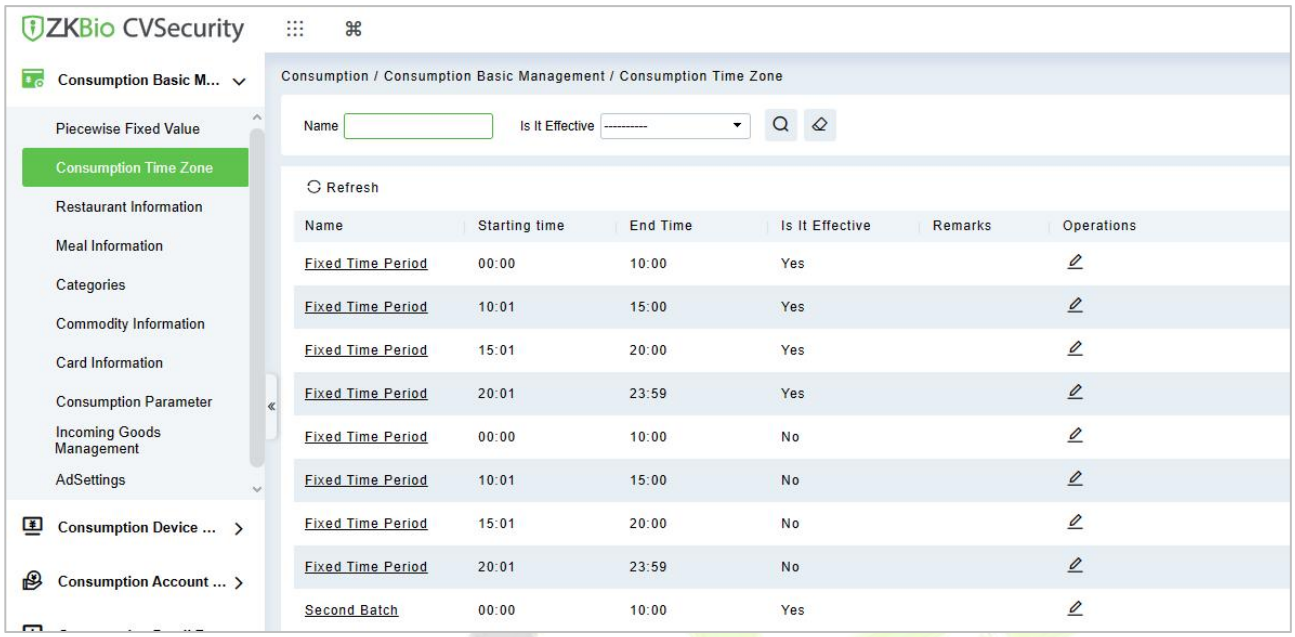


Figure 12- 3

12.1.2.1Edit

Click **Edit** column on the operation column to open the modification dialog box.

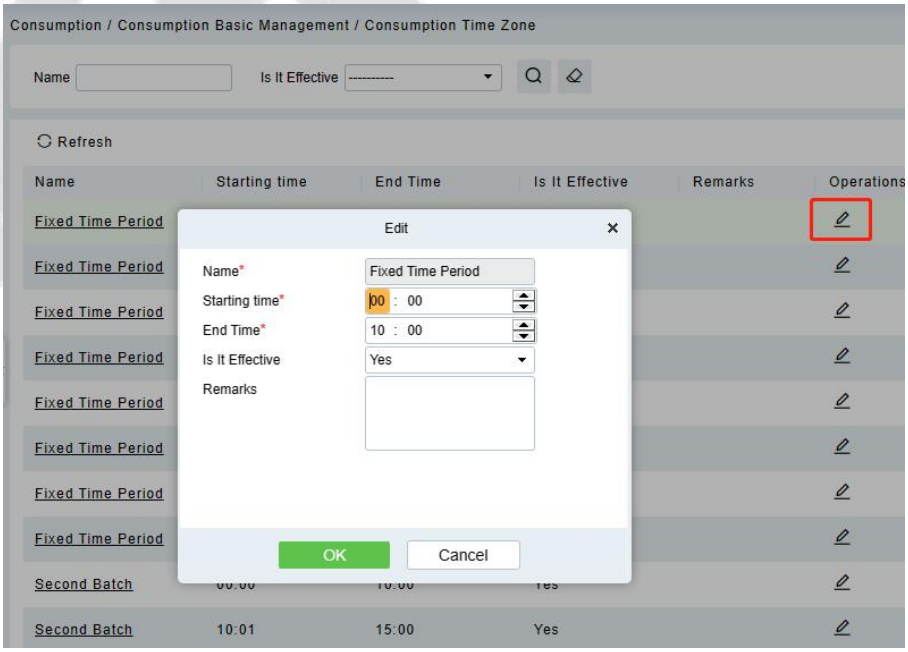


Figure 12- 4

On the dialog box, you can select the required **Start time**, **End time**, **Whether Effective**, and **Remarks** (optional), as shown in the above figure. After providing the information, click **OK**.

12.1.3Restaurant Information

By default, a Restaurant name is already added, you can edit it and also add new ones.

Click **Consumption Basic Management** > **Restaurant Information**, shown as following figure:

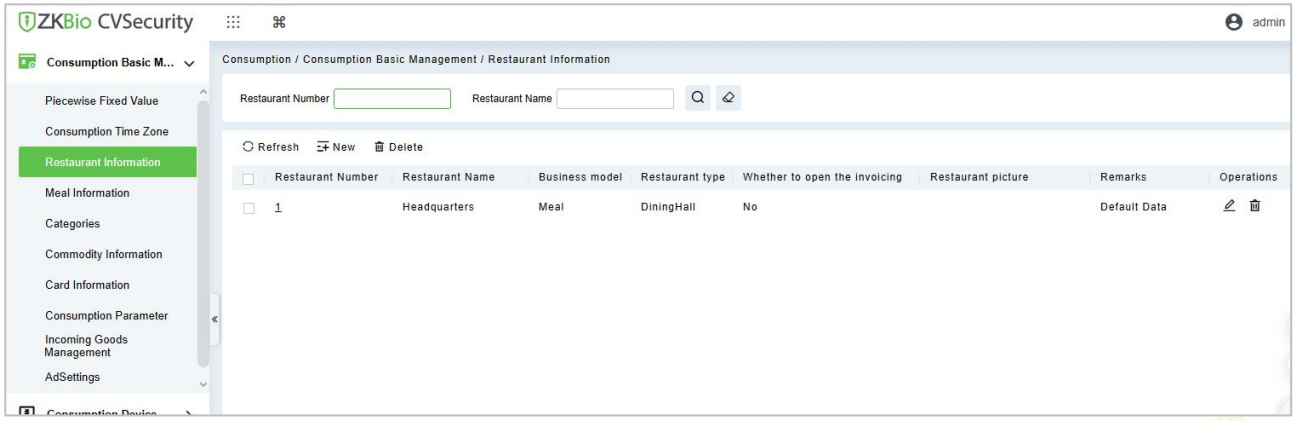


Figure 12- 5

12.1.3.1New

Click **New**, to add a restaurant.

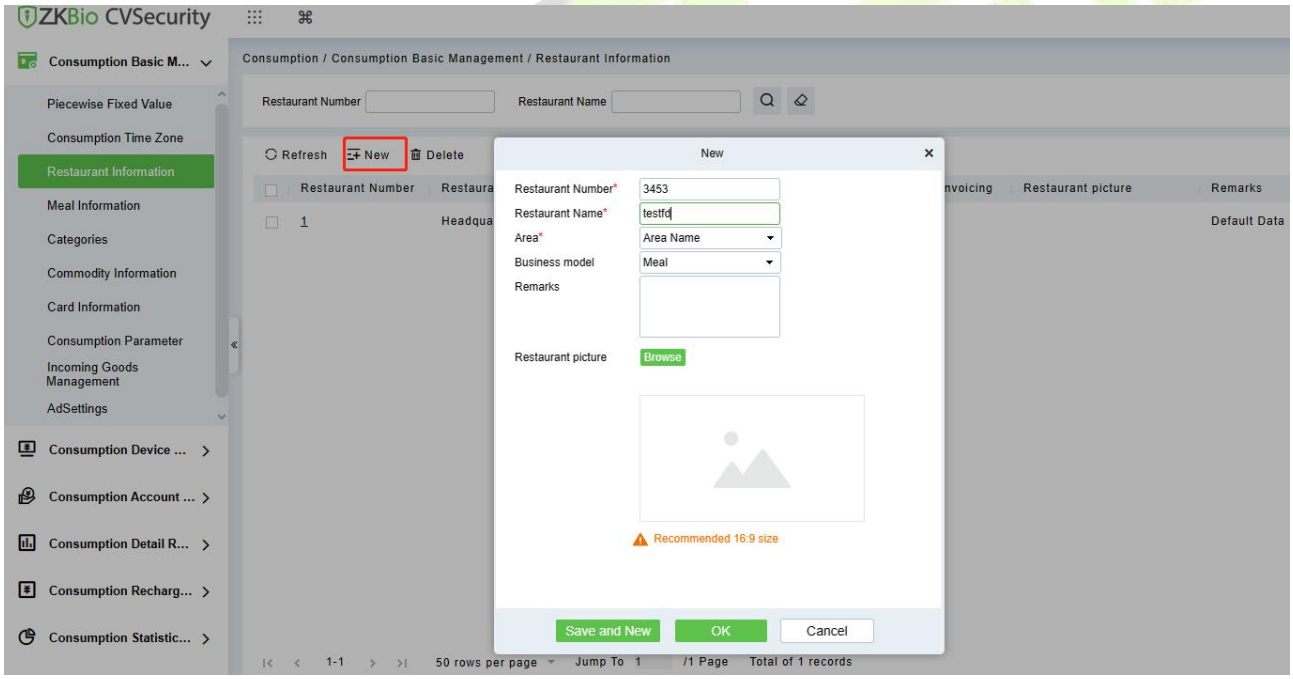


Figure 12- 6

Type the preferred Restaurant number, Restaurant name, and Remarks (optional) information, choose whether to open the invoicing, and allows user to upload restaurant picture, then click **OK** to save and close or click **Save and New** for continue adding.

12.1.3.2Edit

Click **Edit** in the operation column to open the modification dialog box.

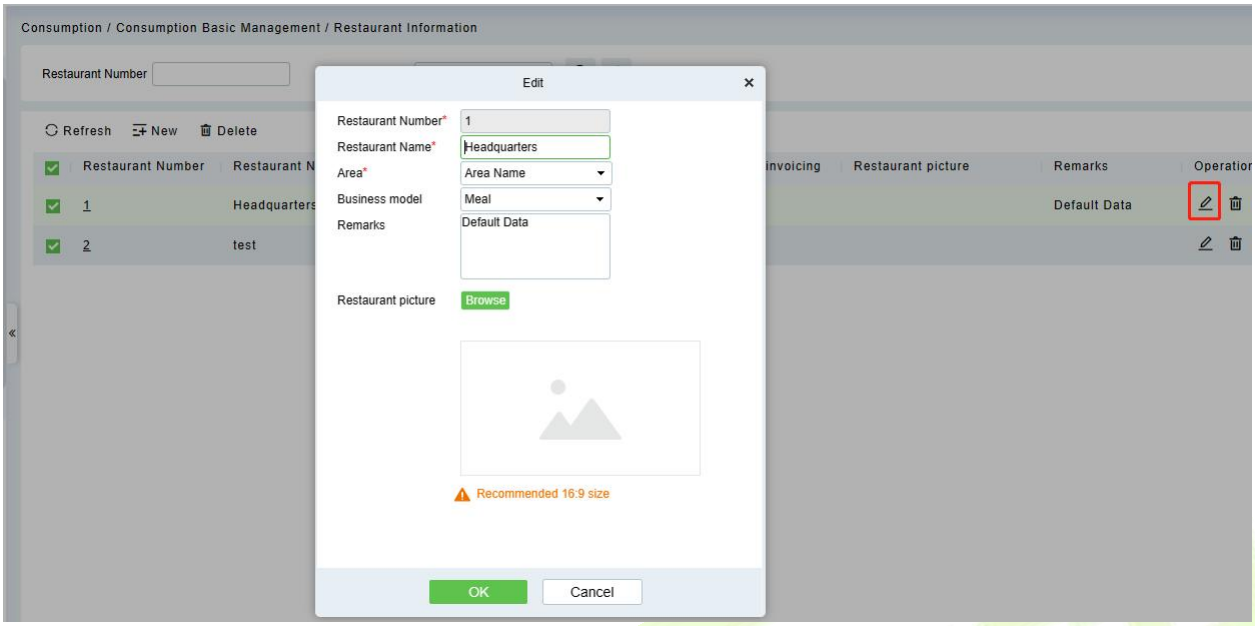


Figure 12- 7

12.1.3.3Delete

You can directly click **Delete** on the required hotel to remove it from the system.

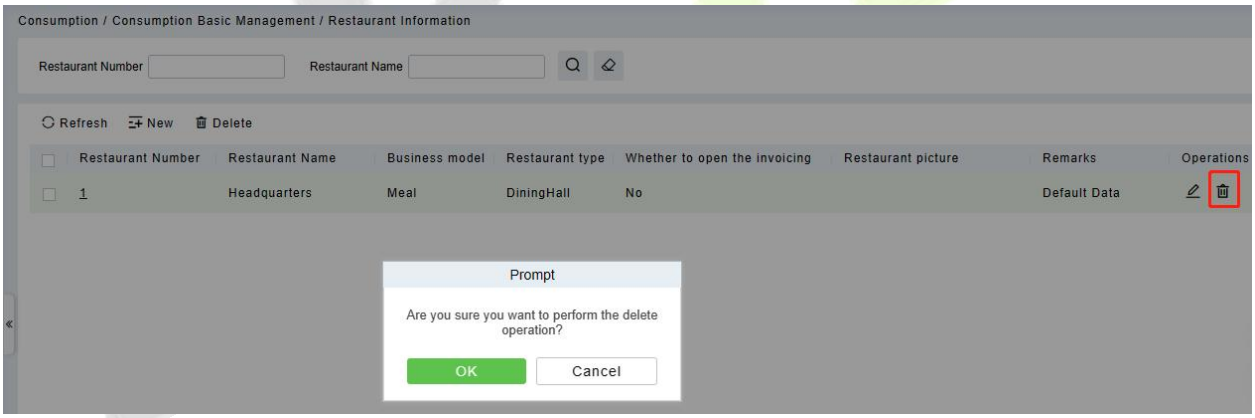


Figure 12- 8

For deleting in batch, select the required hotel(s) as shown below and click **Delete**. The default restaurant number 1 cannot be deleted.

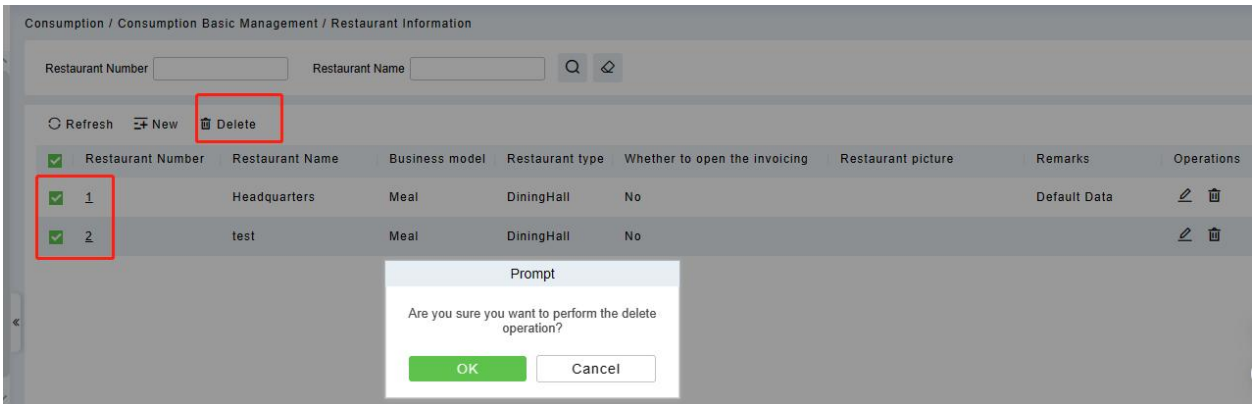


Figure 12- 9

12.1.4Meal Information

Click **Consumption Basic Management** > **Meal Information**, shown as following figure:

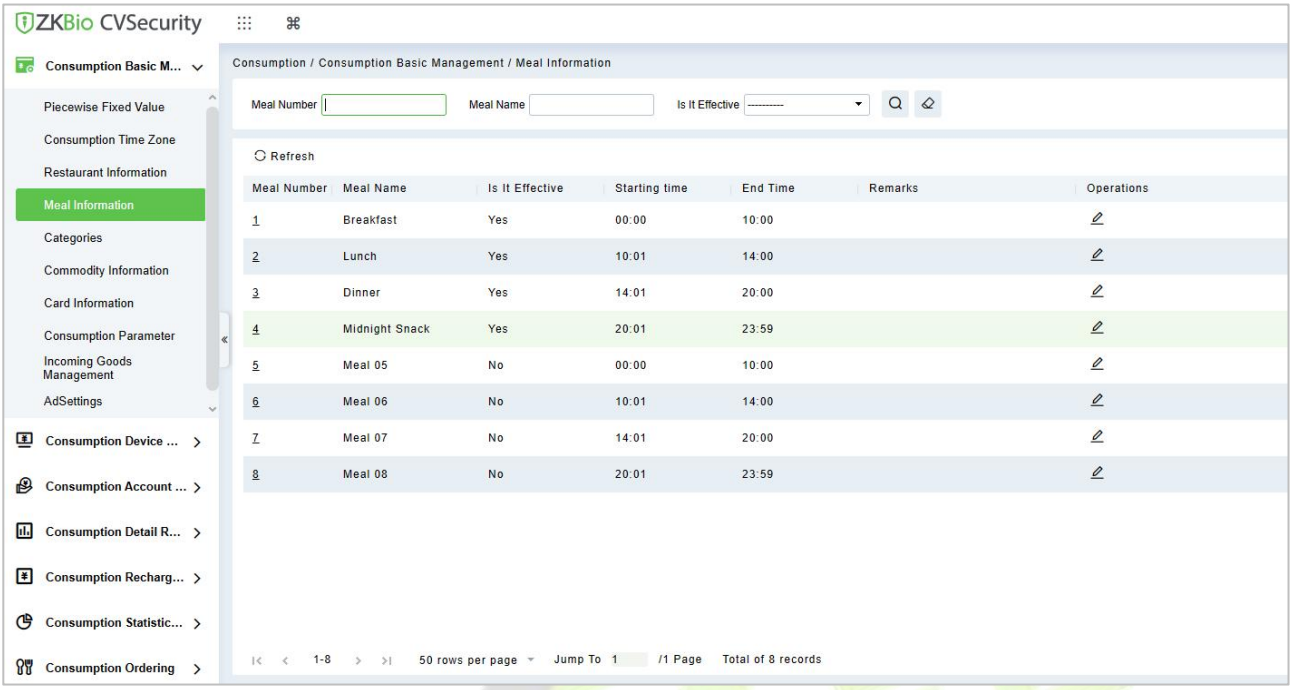


Figure 12- 10

12.1.4.1Edit

Click on the meal number of list and the edit column of the operation to pop up the modification dialog box.

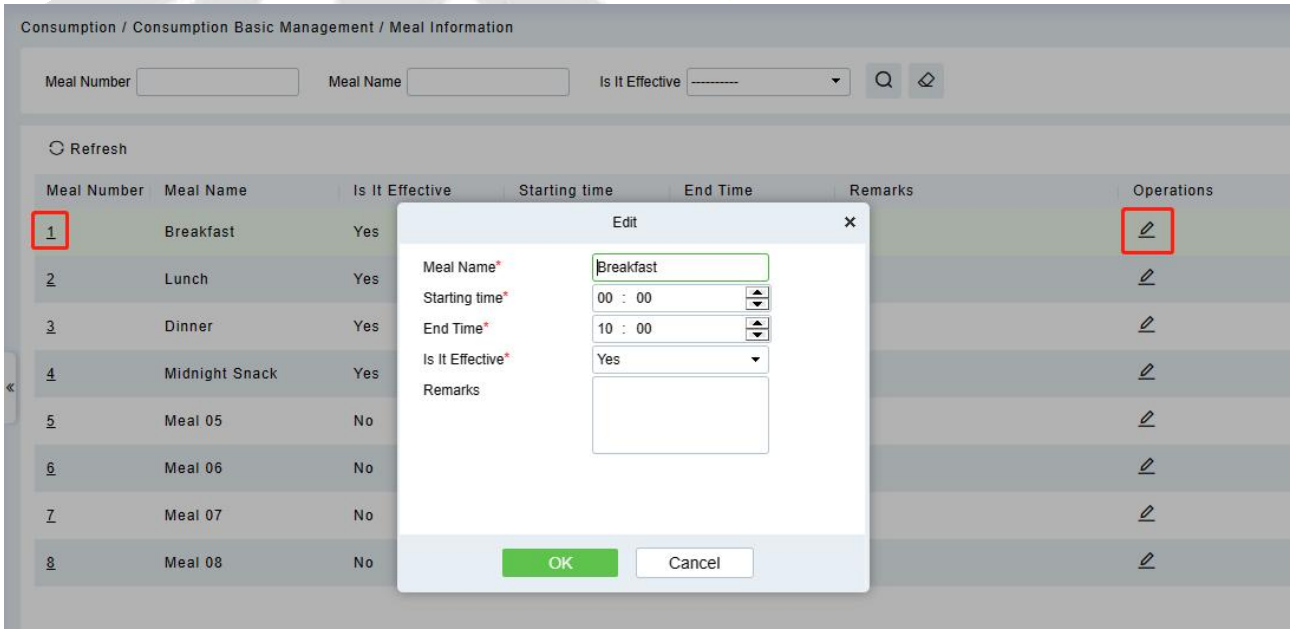


Figure 12- 11

Enter the information in the dialog box which include: **Meal Name**, **Start Time**, **End time**, **Whether Effective** (status), **Remarks** (optional) and then click **OK** to save.

12.1.5Categories

Click **Consumption Basic Management** > **Categories** as shown in the following figure:

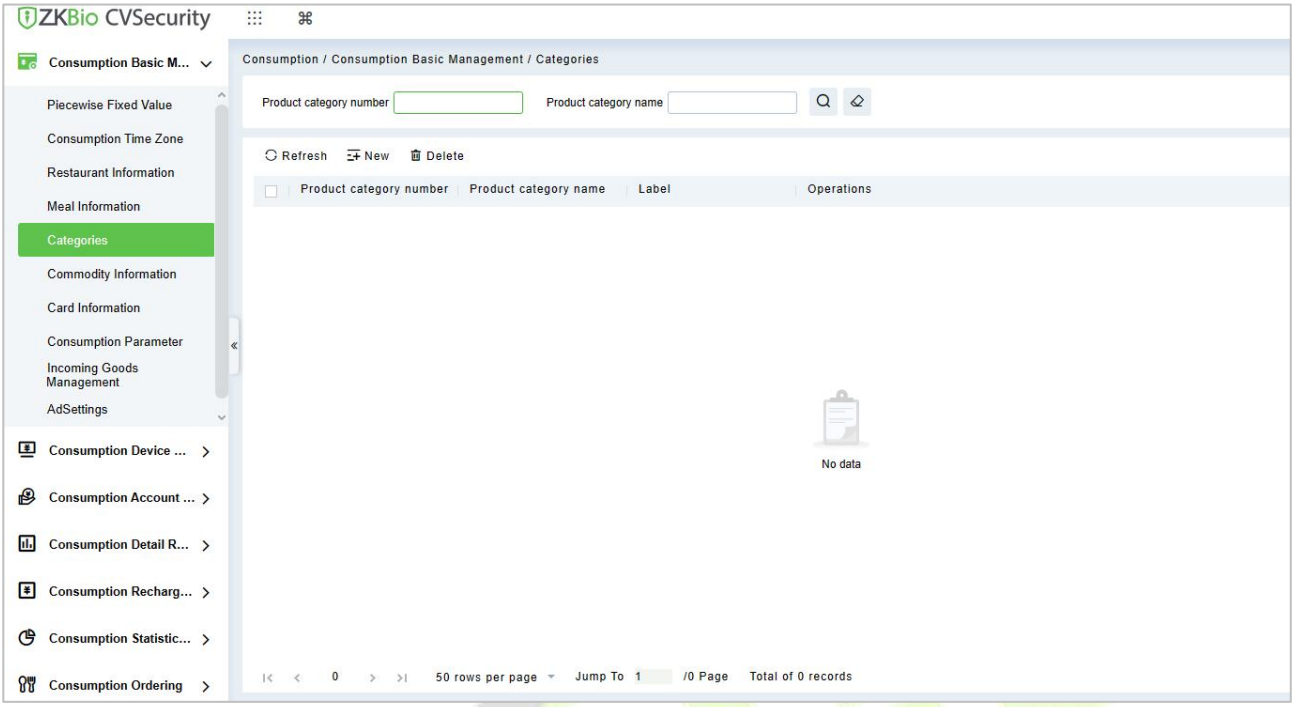


Figure 12- 12

12.1.5.1New

Click **New** to add, enter required **Product category number**, **Product category name**, in the dialog box, and then click **OK** to save.

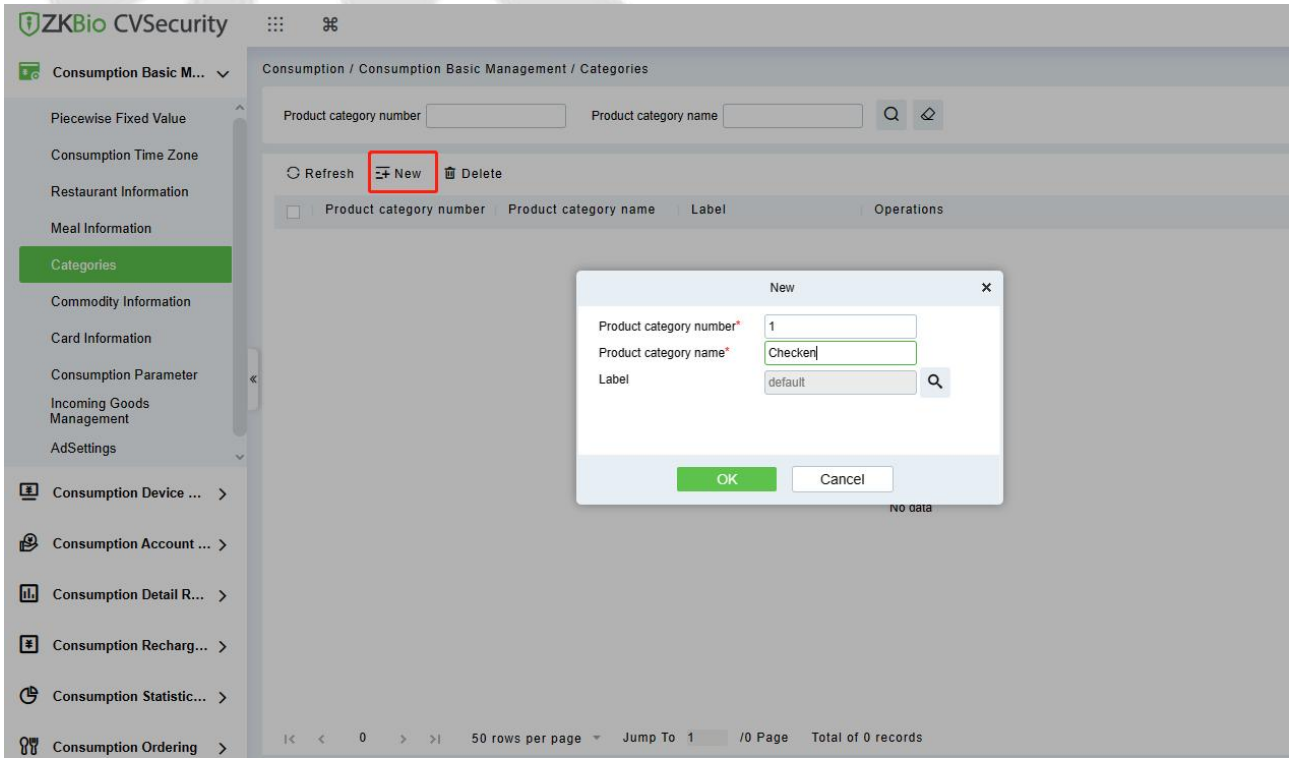


Figure 12- 13

12.1.6Commodity Information

Click **Consumption Basic Management** > **Commodity Information** as shown in the following figure:

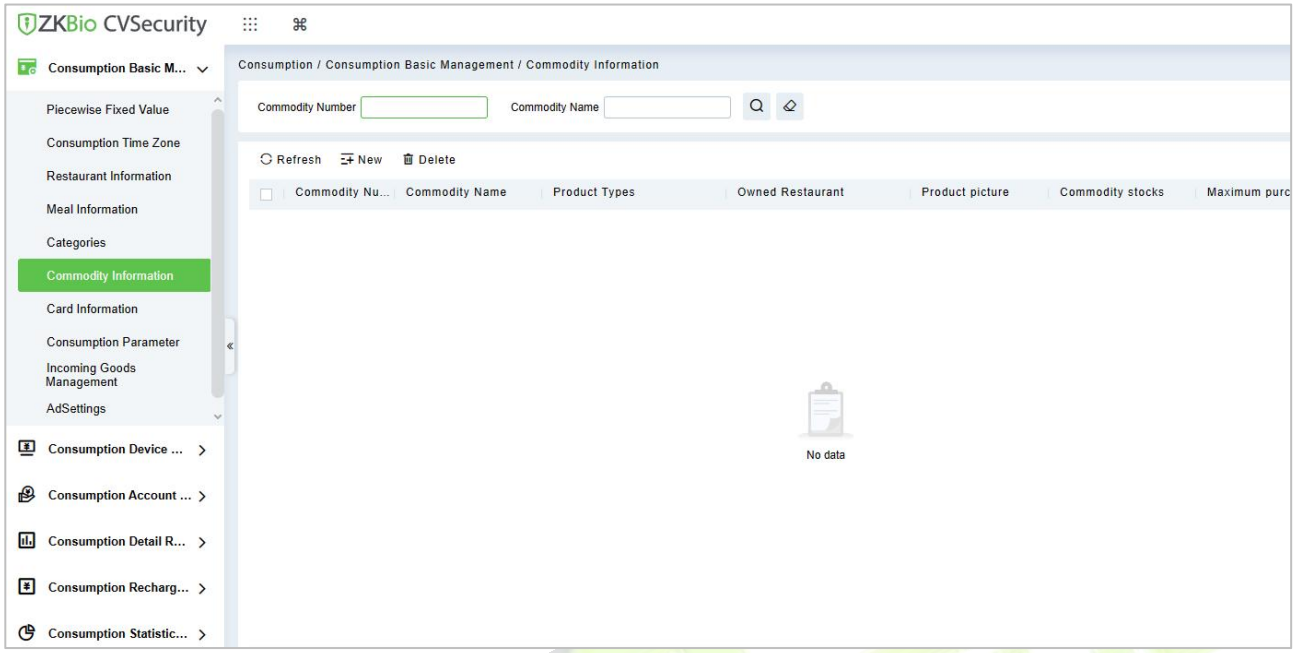


Figure 12- 14

12.1.6.1New

Click **New** to add, enter required **Commodity number**, **Commodity Name**, Commodity stocks, Maximum purchase quantity, **Unit price, Member price, Barcode, and remarks** in the dialog box, choose the Commodity categories and Owned Restaurant in the pull-down list, and then click **OK** to save and close or click **Save and New** for continue adding.

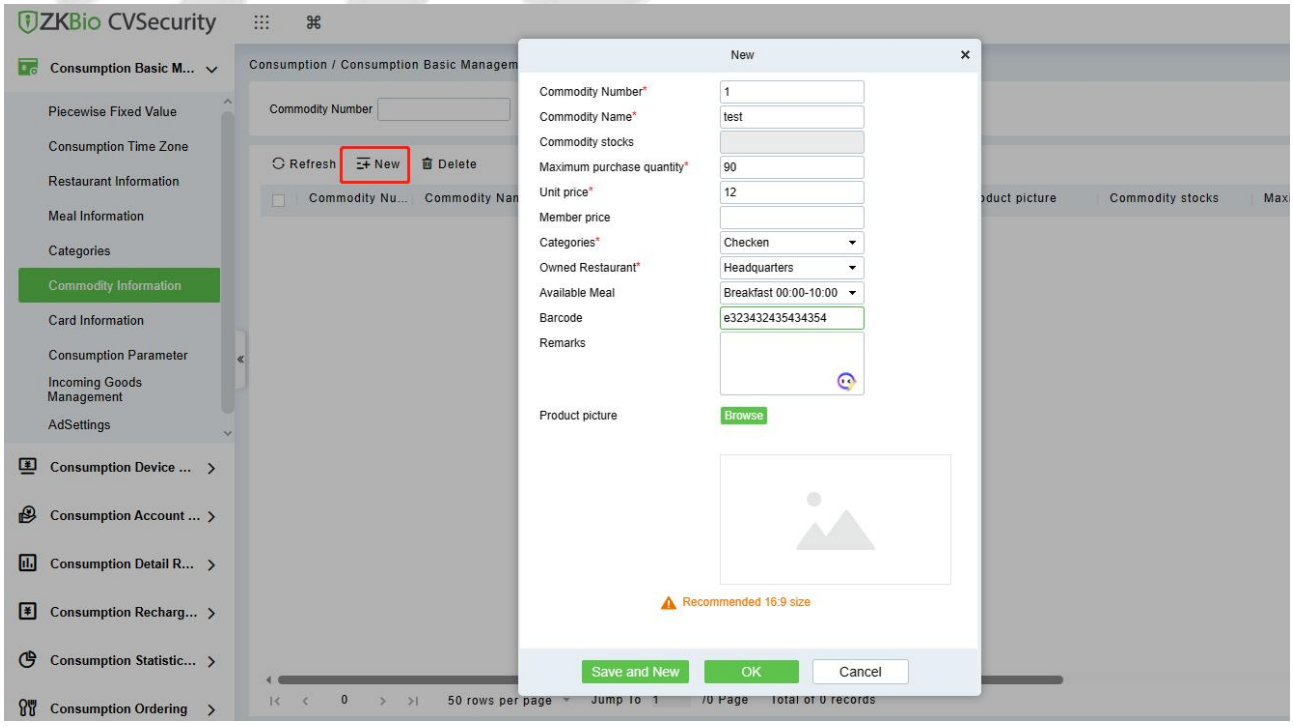


Figure 12- 15

12.1.6.2Delete

You can directly click **Delete** on the required Commodity to remove it from the system.

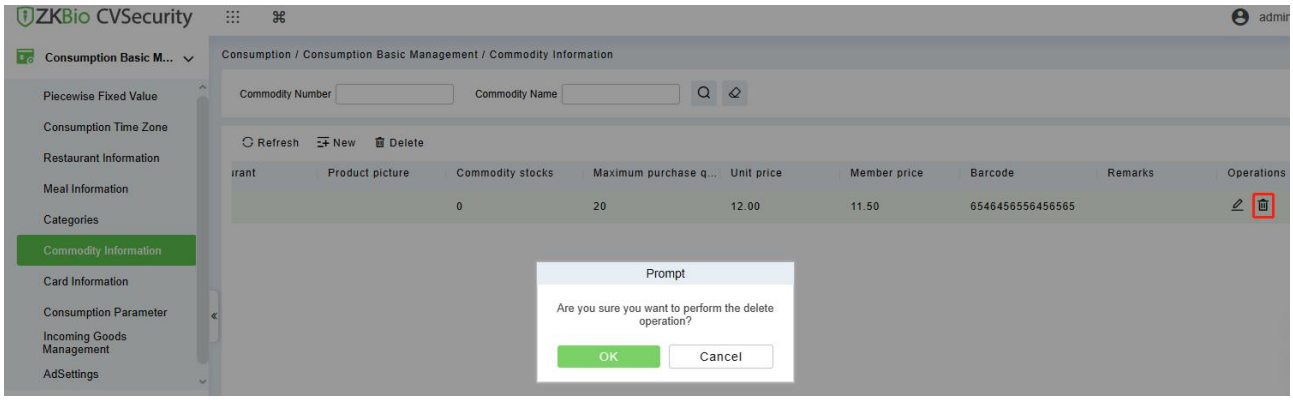


Figure 12- 16

For deleting in batch, select the required Commodity(s) as shown below and click **Delete**.

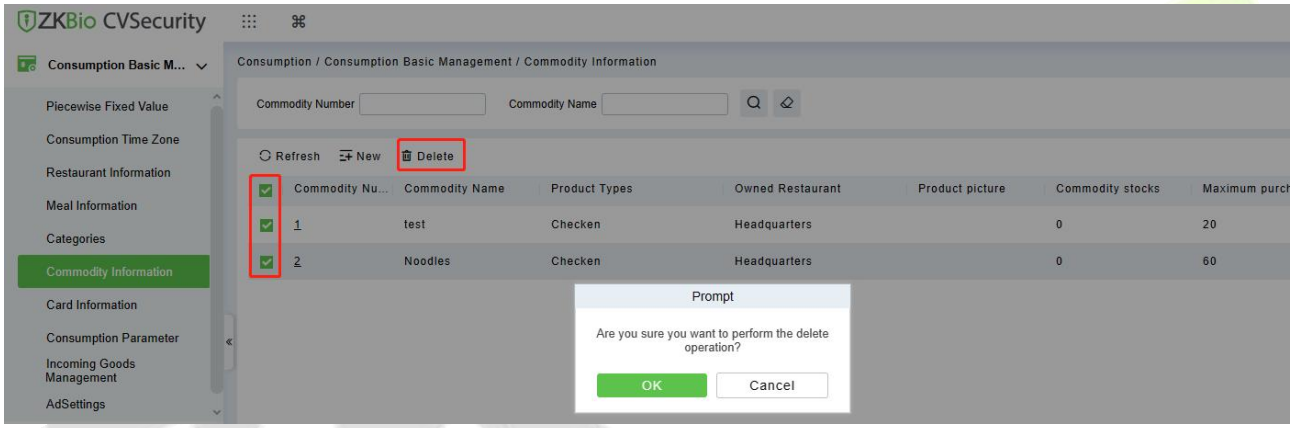


Figure 12- 17

12.1.7Card Information

Click Consumption Basic Management > Card Information, as shown below:

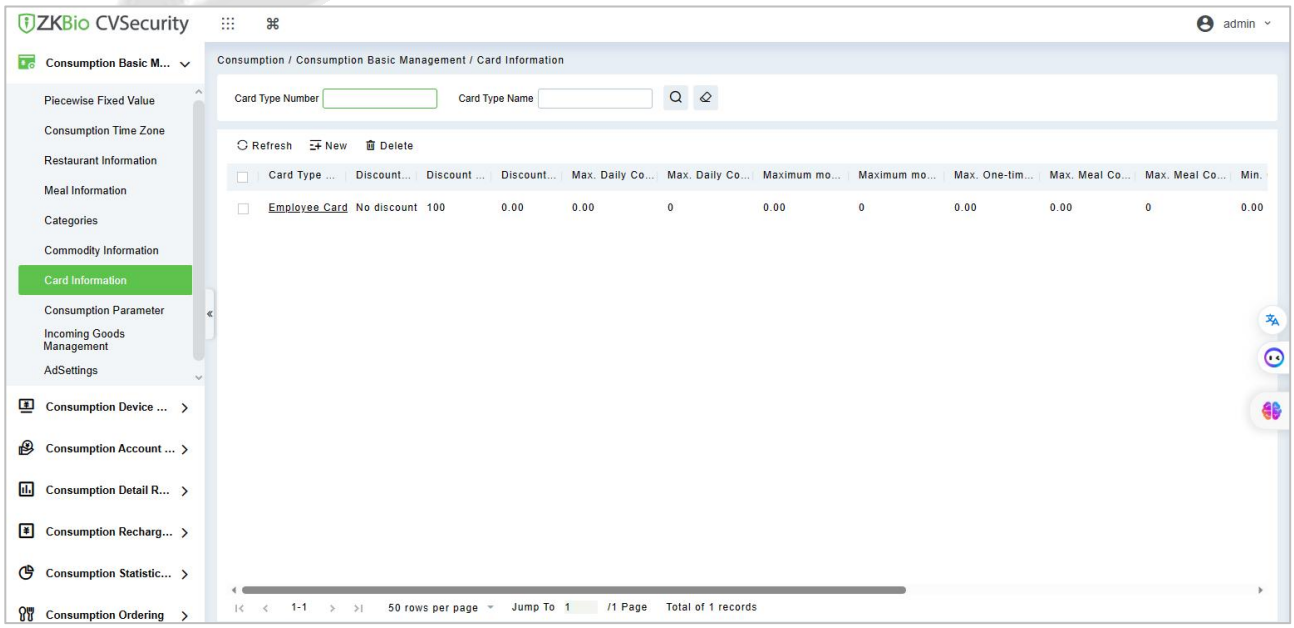


Figure 12- 18

12.1.7.1New

Click **New**, in the dialog box, you can fill in the card type number, card type name, discount, consumption time zone, maximum daily consumption amount, maximum daily consumption times, maximum one-time consumption amount, maximum meal consumption amount, maximum meal consumption times, minimum card balance, maximum card balance, effective use of days, available meal, available device, remarks, as shown below:

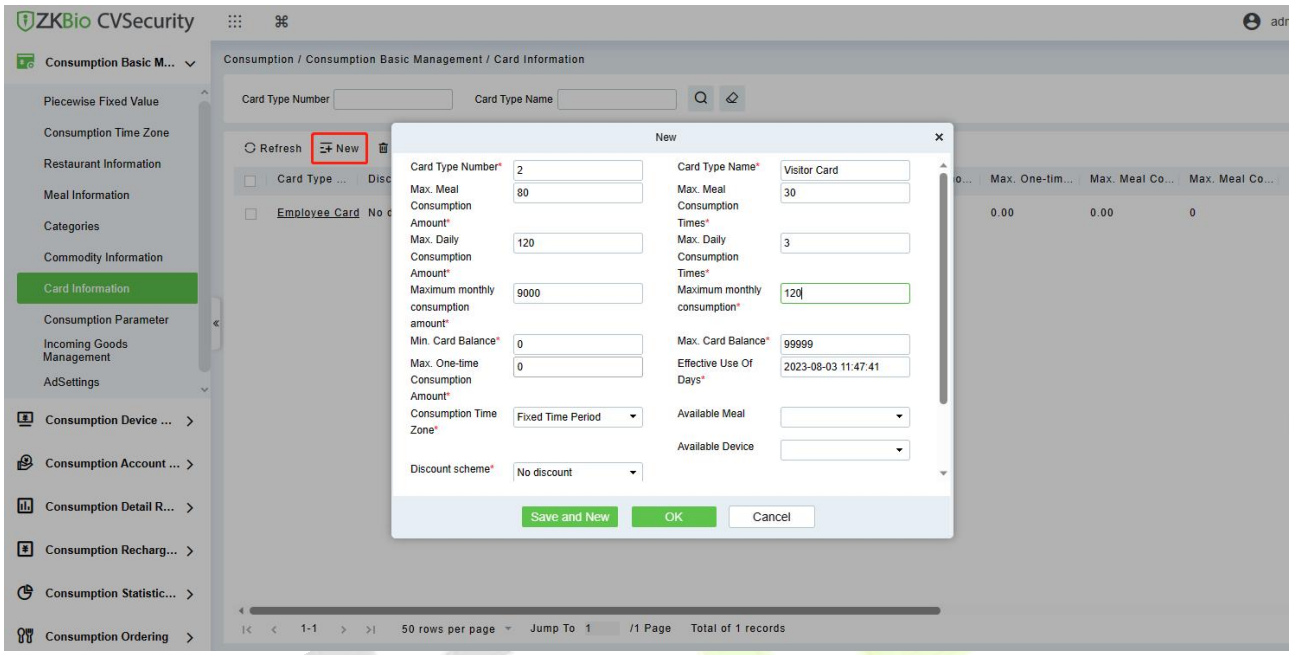


Figure 12- 19

12.1.7.2Edit

Click the card type number of the list and the edit column of the operation to pop up the modification dialog box.

12.1.7.3Delete

You can directly click **Delete** on the required Card to remove it from the system.

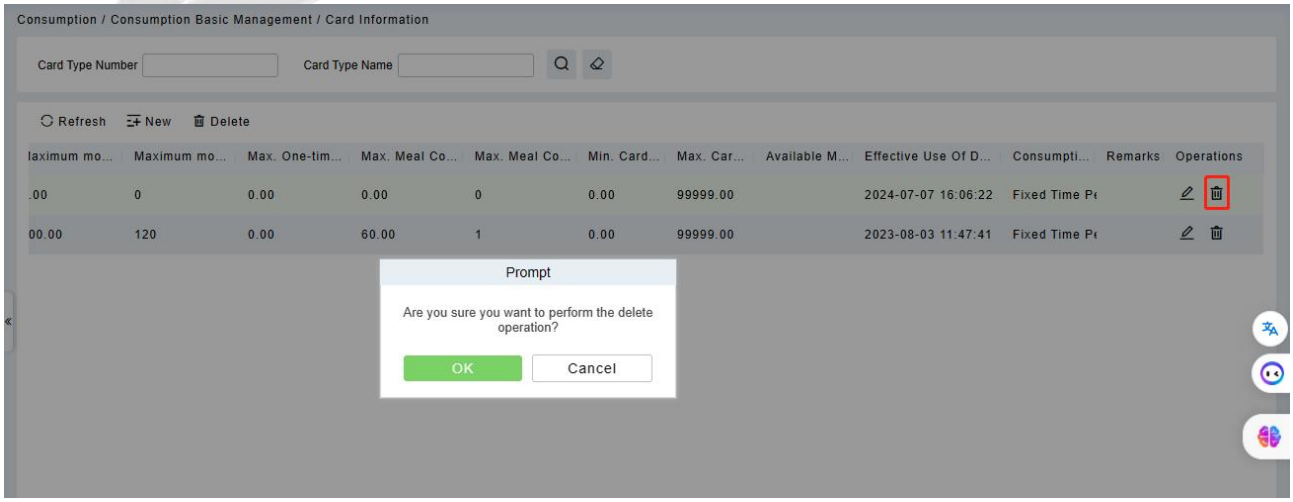


Figure 12- 20

For deleting in batch, select the required Card (s) as shown below and click **Delete**. The default employee card cannot be deleted.

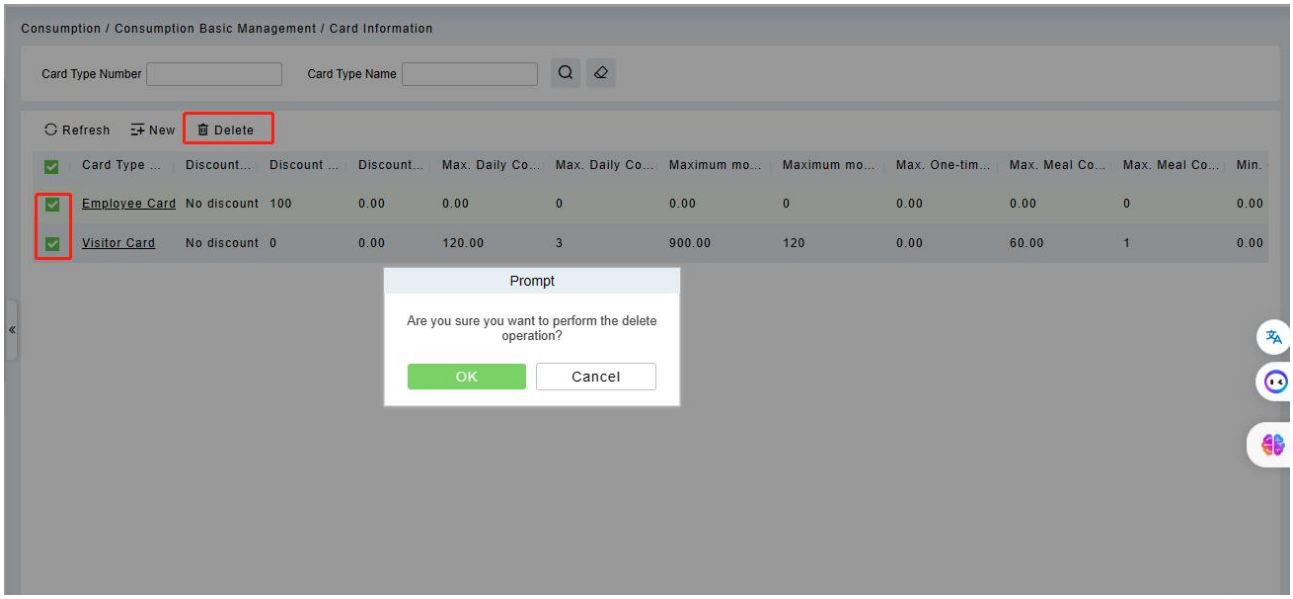


Figure 12- 21

12.1.8Consumption Parameter

Click **Consumption Basic Management** > **Consumption Parameter** to enter the consumption module setting, shown below:

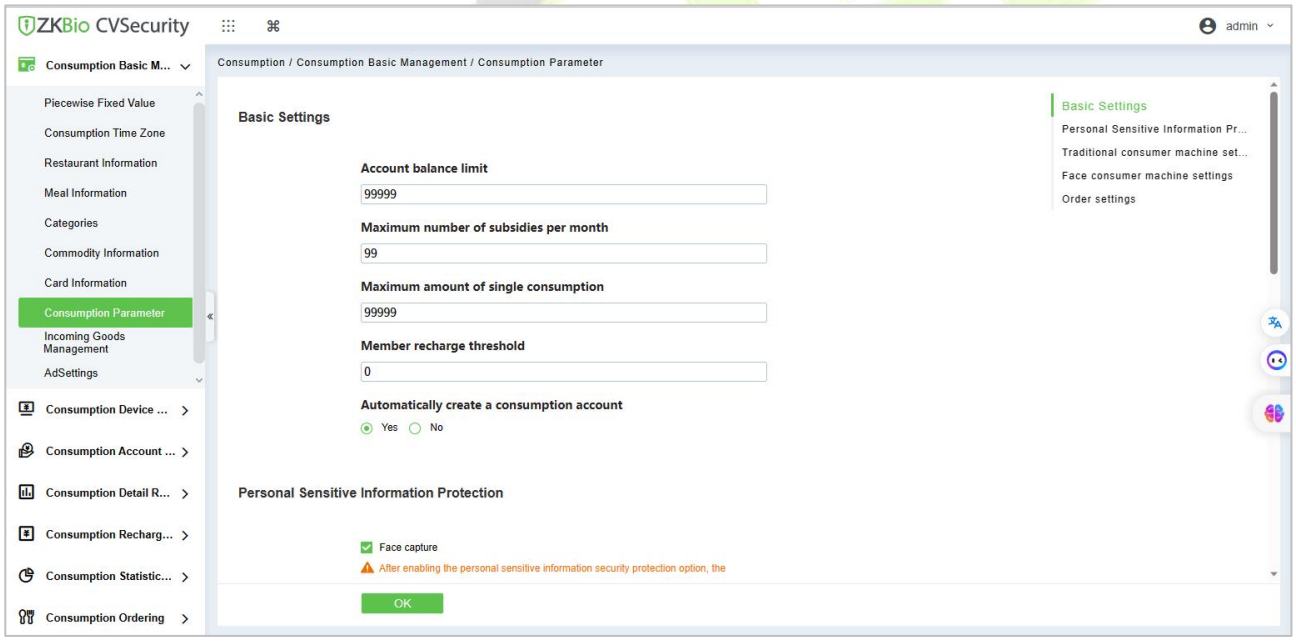


Figure 12- 22

● Basic Settings:

1. Set the upper limit of the account balance. You can set an integer value between 1~99999, default value is 9999.
2. Set the upper limit number of the subsidies. You can set an integer value between 1~99, default value is 99.
3. Set the upper limit amount of single consumption. You can set an integer value between 1~9999, default value is 9999.
4. Member recharge threshold. Default value is 0, maximum number is 9999.

● Traditional consumer machine settings:

1. Set the prompt timing mode starts billing. Allows user define the prompt slogan.

2. Set the Timekeeping mode whether subject to start or end rules.

● Face consumer machine settings:

1. Set the Insufficient balance reminder threshold. Default is 0.

2. Set the prompt words when the amount below the threshold .

3. Set whether to open the second consumption function.

● Order settings:

1. Set whether ordering is required to consume: Default is no;

2. Set the number of days in advance for ordering: Default is 1-7 days;

3. Set the amount of time (in minutes) required to cancel an order in advance: Default is 60 minutes;

4. Double Wallet Wallet Consumption Order: Dual wallet spending pattern configuration: cash-only spending, subsidized spending only, or cash spending first, subsidized spending later.

Note:

1) The parameters for reminder threshold for insufficient balance and prompt message for amount below the threshold are not supported by traditional consumption machines, but are supported by facial recognition consumption machines.

2) The parameters for enabling double confirmation of consumption are not supported by traditional consumption machines, but are supported by facial recognition consumption machines.

12.1.9 Incoming Goods Management

Click **Consumption Basic Management** > **Incoming Goods Management** to enter the commodity purchase management page, through the bar-code corresponding to the commodity, shown below:

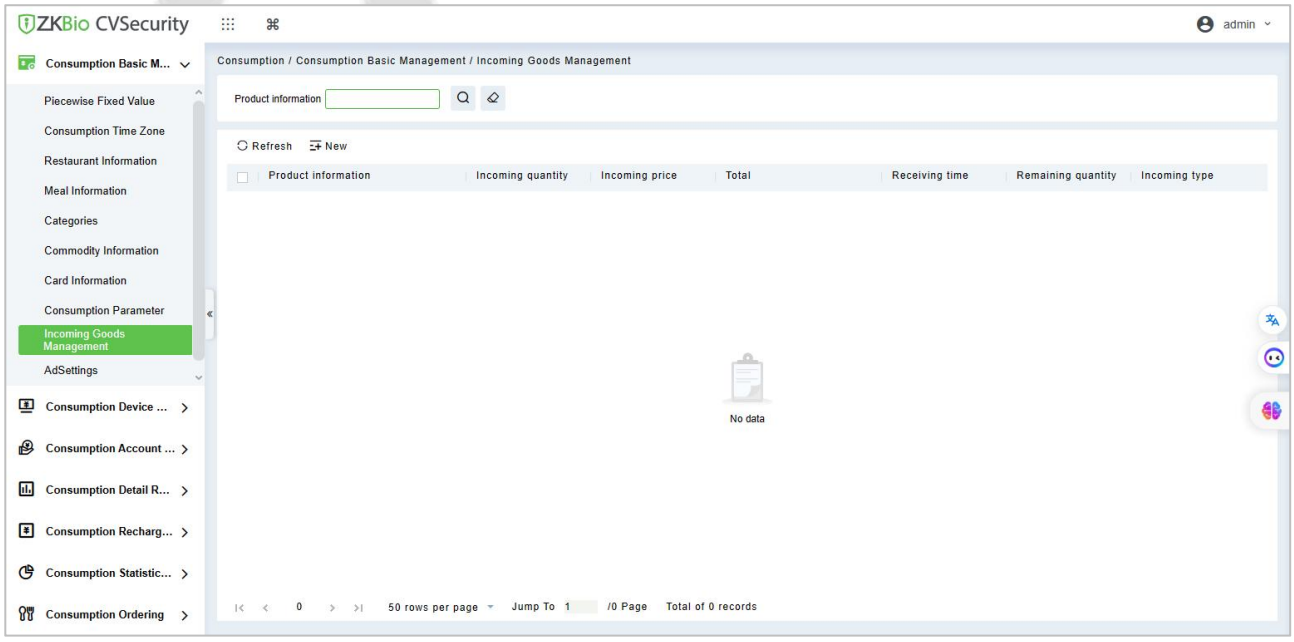


Figure 12- 23

12.1.9.1New

Click the New button, to enter the goods edit page. Input the Commodity bar-code, incoming quantity, incoming price, total amount and receiving time.

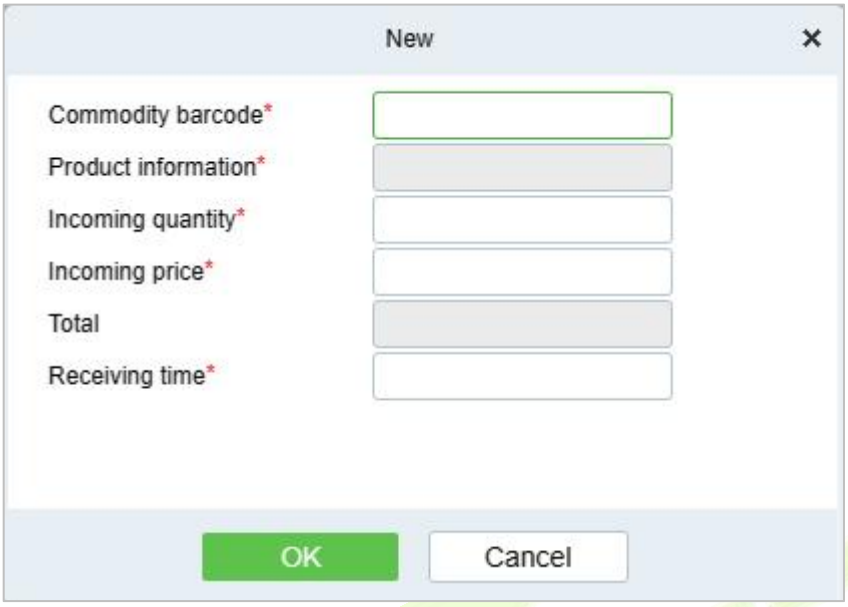


Figure 12- 24

12.1.10AD Setting

Click **Consumption Basic Management** > **Incoming Goods Management,** as shown below:

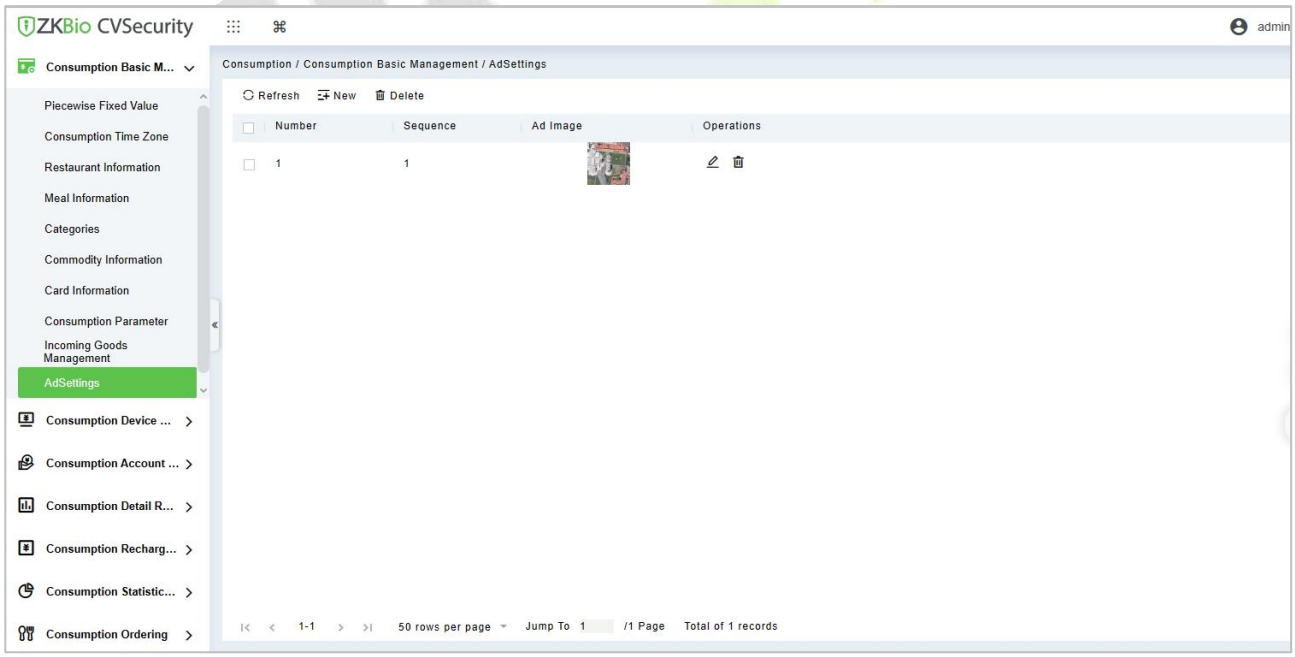


Figure 12- 25

12.1.10.1 New

Click **New**, in the dialog box, fill in **Number,Sequence,Upload Image**.then click **OK**.

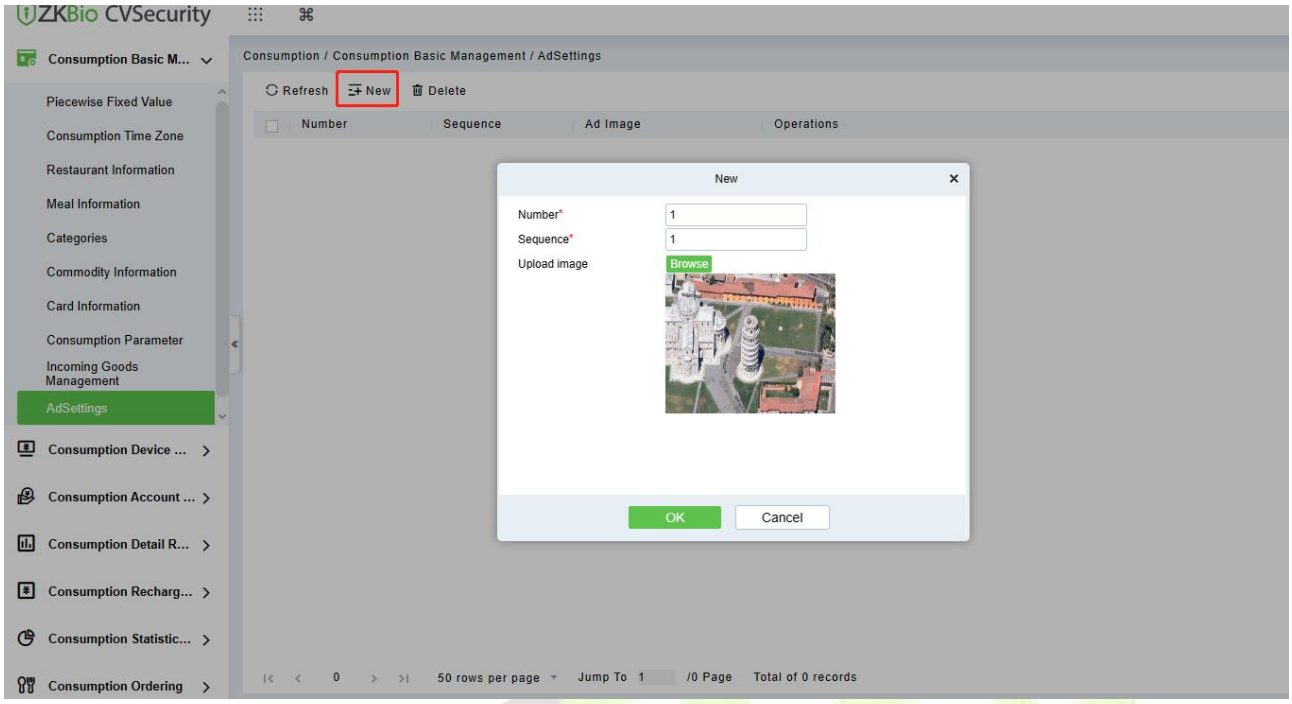


Figure 12- 26

12.2 Device Management

This module is used to manage online face consumer devices.

12.2.1 Consumption Device Management

This menu is available for **Promerc-30, Peomerc-40.**

Click Consumption Device Management > Consumption Device Management, as shown below:

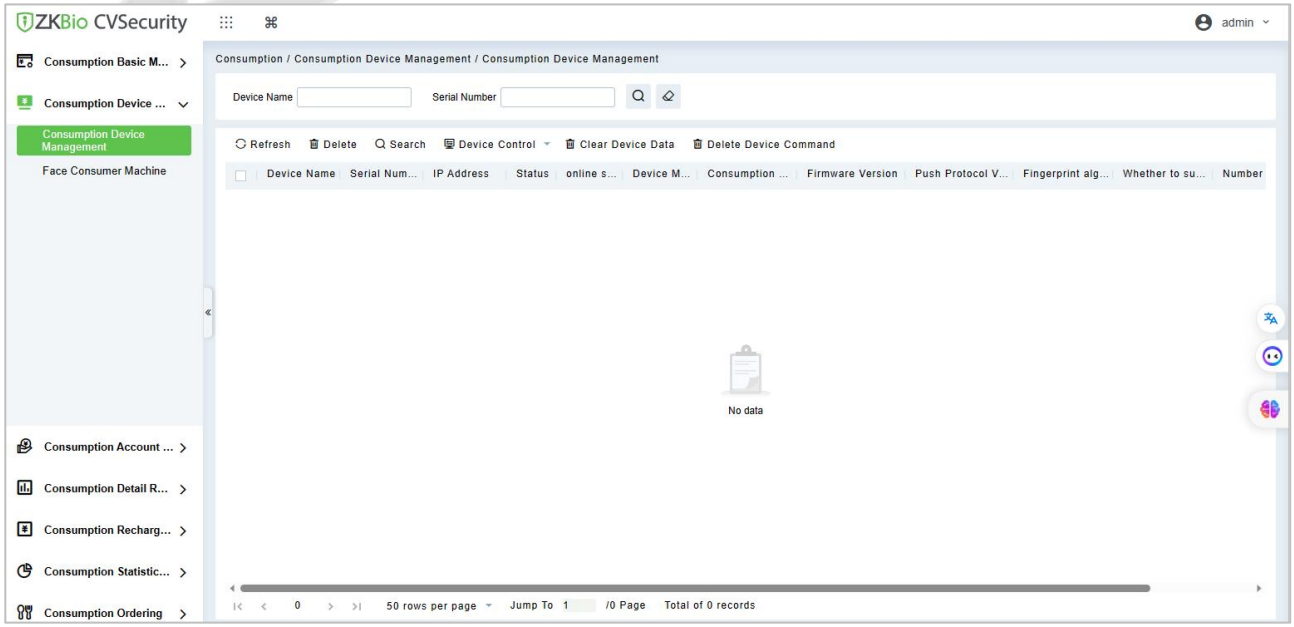


Figure 12- 27

12.2.2Face Consumption Machine

This menu is available for **Promerc-300.**

Click Consumption Device Management > Face Consumption Machine, as shown below:

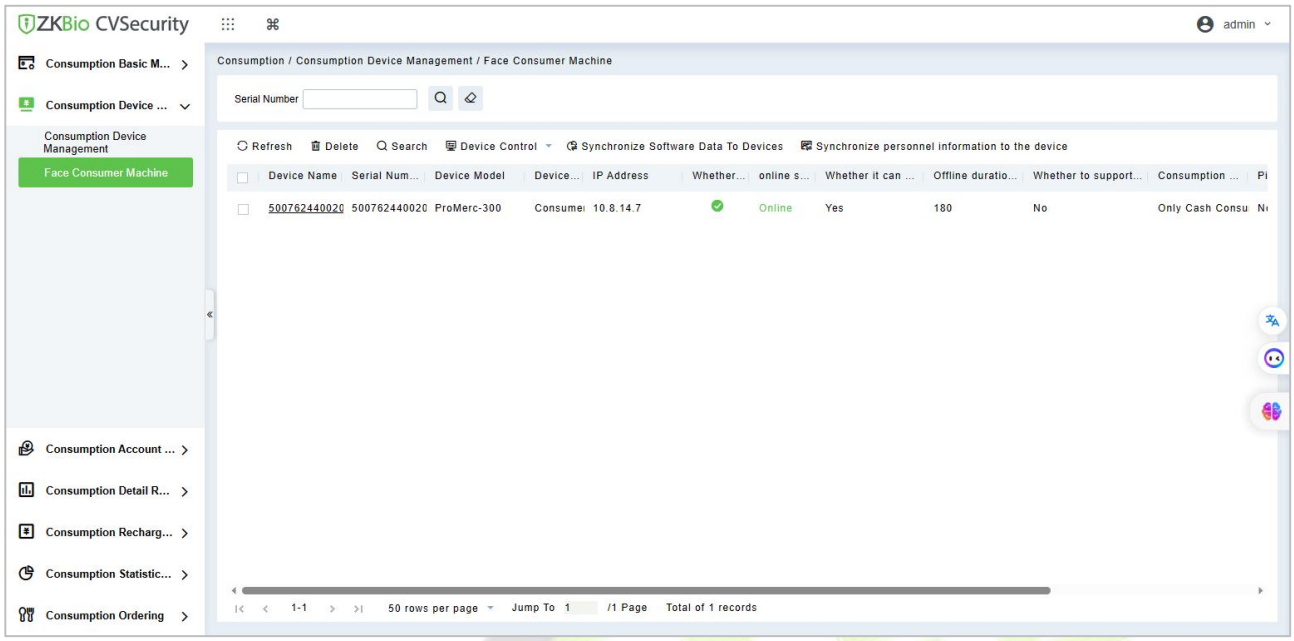


Figure 12- 28

12.2.2.1Search

Click **Search**, and the page is show as follows:

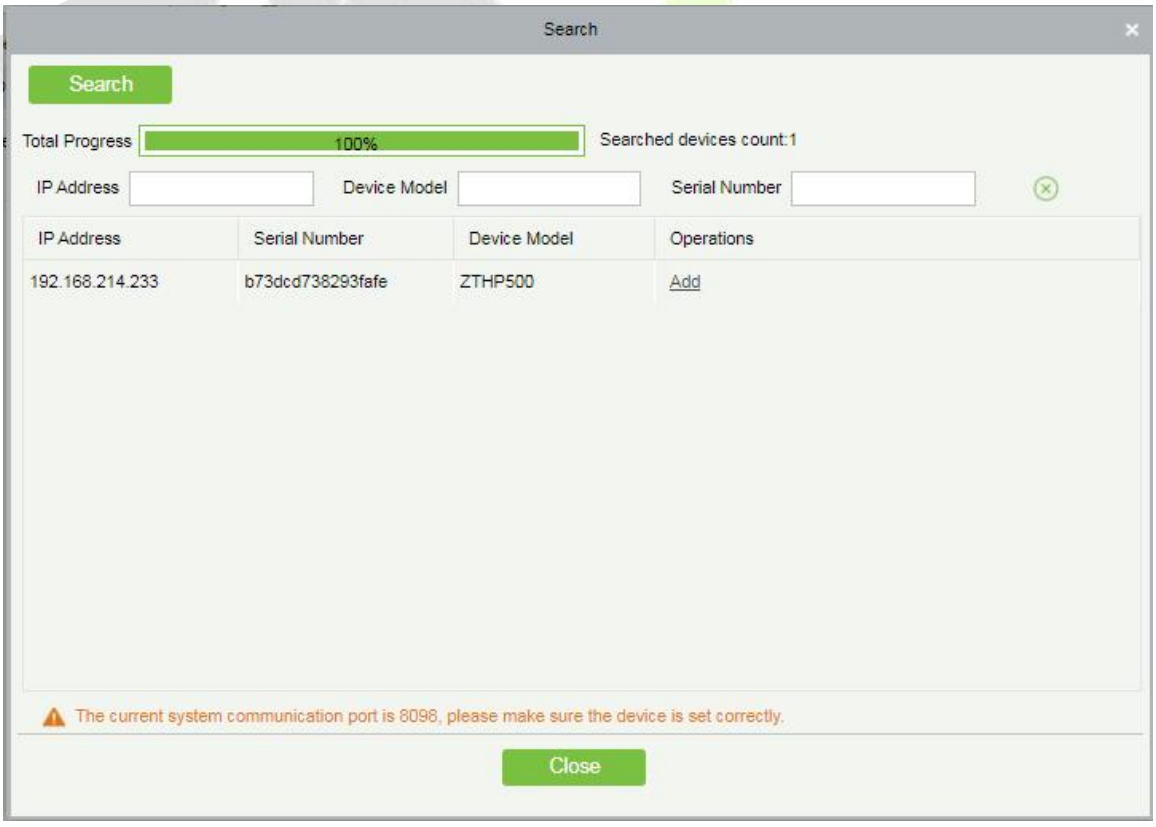


Figure 12- 29

Click **Add** to enter the device edit page.

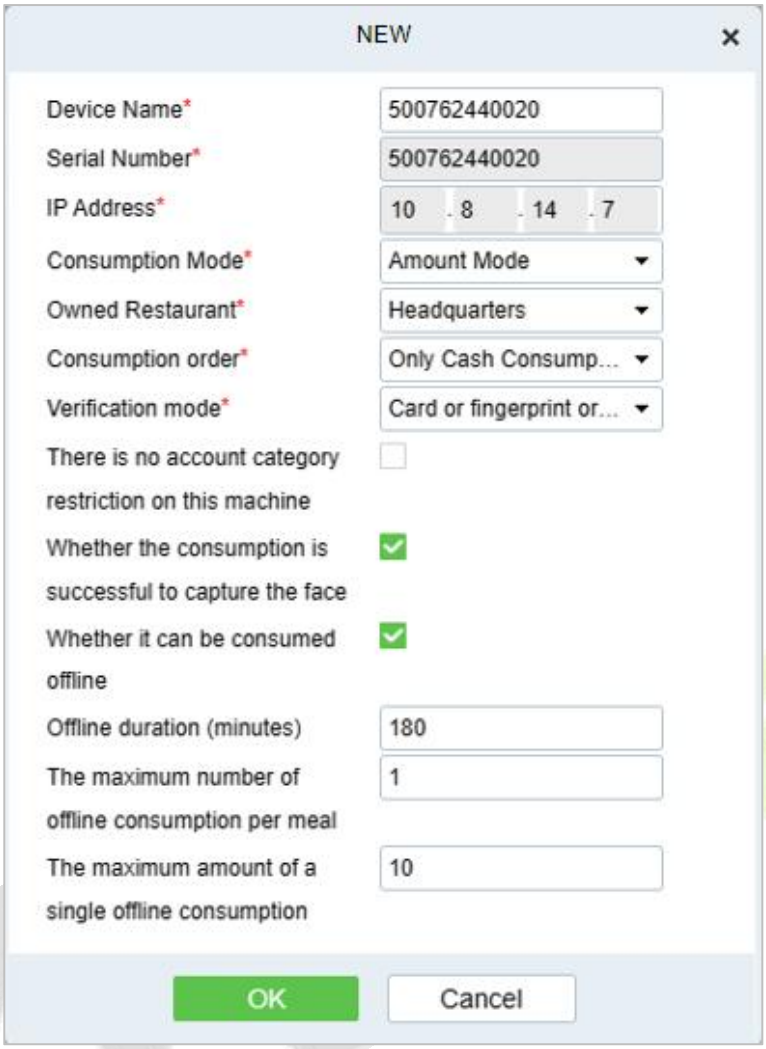


Figure 12- 30

● Some parameters are explained as follows:

Device Name: Device name, non-special characters, consisting of up to 20 characters.

Serial Number: It get from device, not editable.

IP Address: Device IP address, get from device.

Consumption Mode: Sets the consumption mode used by the device.

Can choose fixed value mode, amount mode, counting mode, commodity mode, timing mode, ordering mode.

The fixed value mode can choose fixed value (input fixed amount) and segmented fixed value (obtained from the basic data > segmented fixed value).

Timing mode to define the time price and time to take the whole number of minutes.

Owned Restaurant: Choose device owned restaurant.

Consumption Oder: Set the device to specify wallet consumption order: cash consumption only, subsidy consumption only, subsidy consumption first, then cash consumption, cash consumption first, then subsidy consumption;

1) Cash consumption only: only consumption of cash, not consumption subsidies, when the balance is insufficient, can continue to consume through the way of recharge;

2) Subsidies consumption only: only consumption subsidies, do not consume cash, when the balance is insufficient, you can continue to consume by issuing subsidies;

3) Consumption cash first, subsidies second: Consume cash first, and then consume subsidies, through the way of top up or send subsidies to continue the consumption;

4) first consume subsidies, then consume cash: can be topped up or issued subsidies to account to continue consumption;

Verification Mode: Set the verification method used by the device. You can select card or fingerprint or face (1: N), card & face, card & fingerprint, fingerprint & face.

Whether it can be consumption offline: To enable the device offline consumption function.

Offline Duration: Define the duration of offline consumption, default is 180 minutes.

The maximum number of offline consumptions per meal: 1-999.

The maximum amount of a single offline consumption: Maximum amount of offline consumption per transaction (1-99999).

12.2.2.2Edit

Click the device name of the list or the edit column of the operation to pop up the modification dialog box. The items that can be modified in the modification dialog box includes device name, area, consumption mode, owned restaurant, consumption order, whether can be offline work mode, offline duration, consumption mode, whether support scanning box and so on, as shown in the following figure.

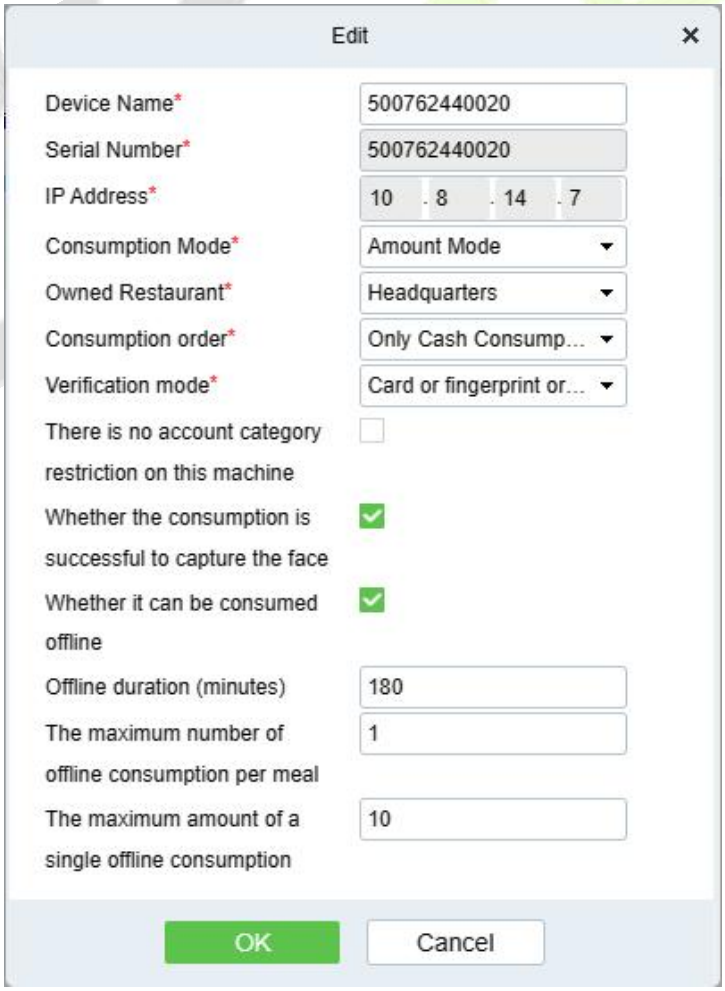


Figure 12- 31

12.2.2.3 Disable/Enable

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

12.2.2.4 Synchronize Software Data to Device

Select a device, click this button, it will send data such as setting parameters of the software to the device to achieve the function of synchronization information so that the device can set the properties synchronously.

12.2.2.5 Synchronize Personnel Information to Device

Select a device, click this button, it will send personnel data of the software to the device, as shown below:

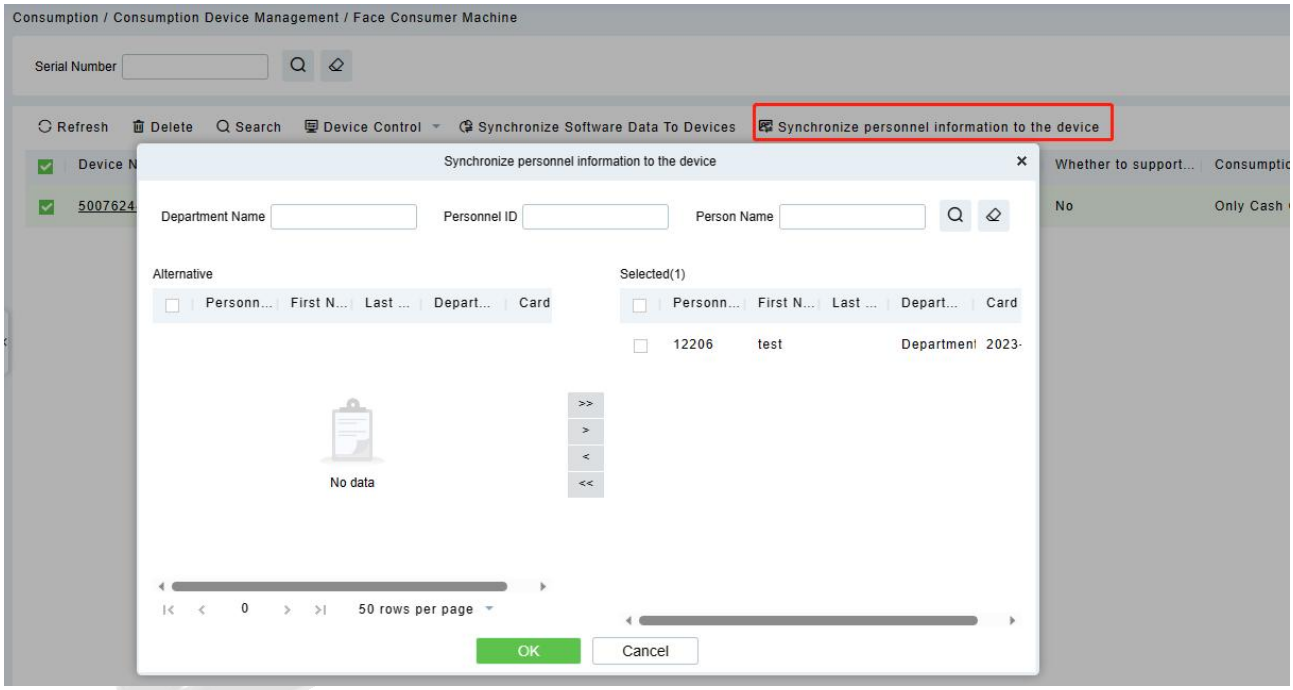


Figure 12- 32

12.3 Consumption Account

12.3.1 Account Service

Using this option to manage staff account, allows to mange top up, refund, account opening, modify card information.

The initial interface of this module is shown below:

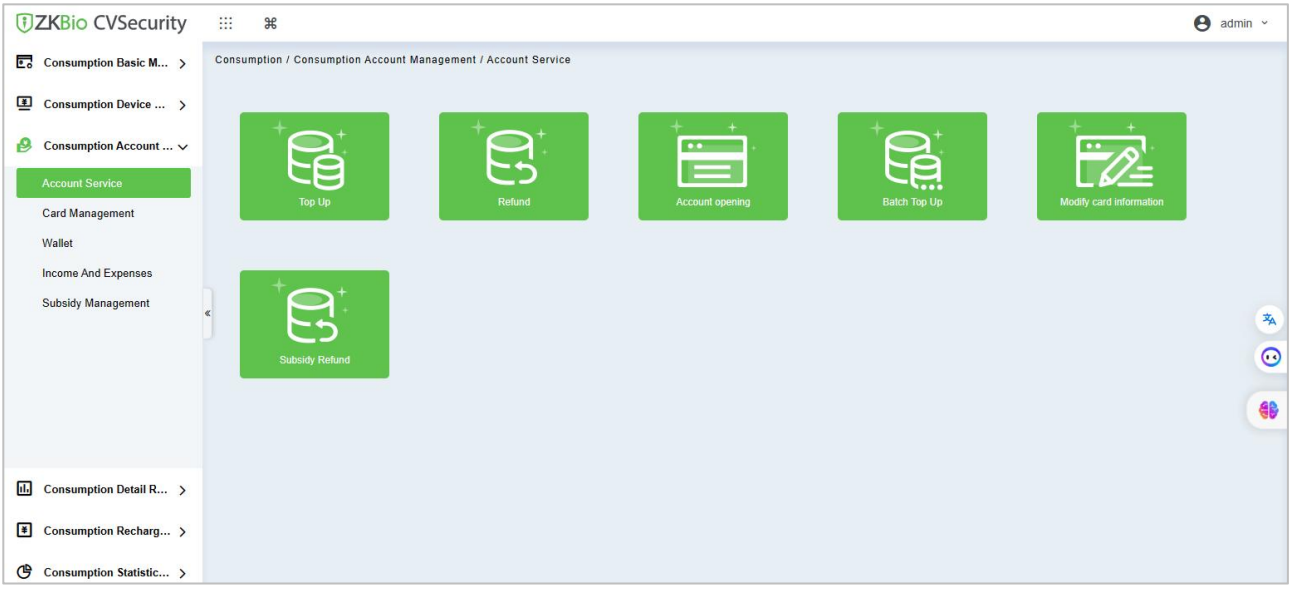


Figure 12- 33

12.3.1.1Top Up

Top up for staff account, click **Top Up**, choose the account, confirmed the account information in the pop up dialog window, input the to up amount, click **Top Up** to finish the top up recharge .

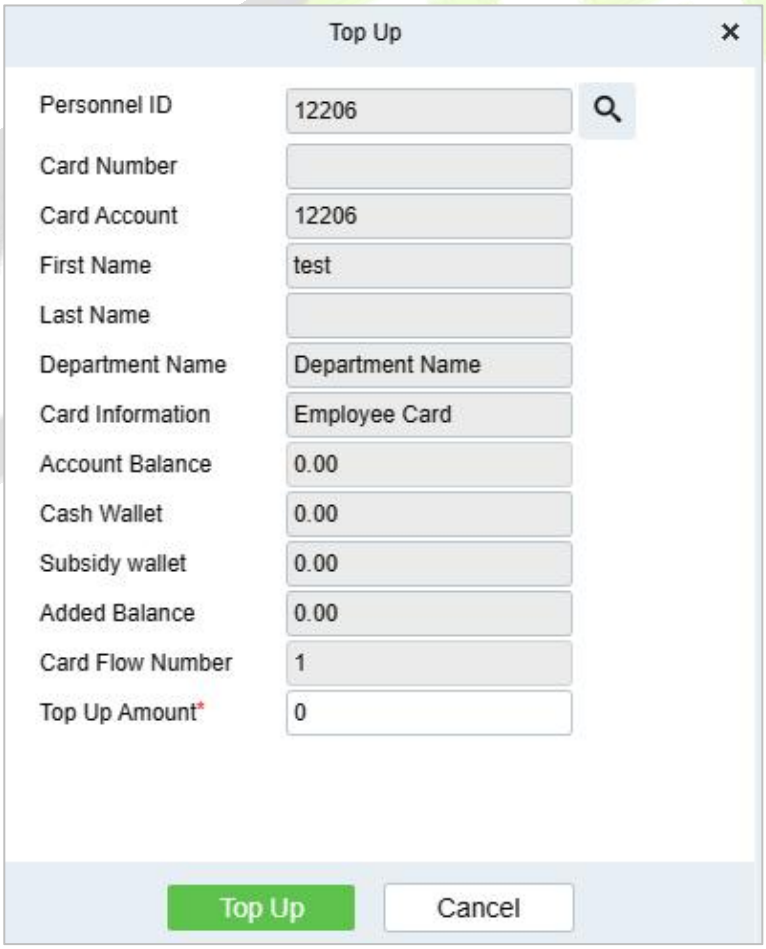


Figure 12- 34

12.3.1.2Refund

Refund for staff account, click **Refund** to enter refund operation dialog box, choose the staff account, input the refund money, click Refund to finish the refund.

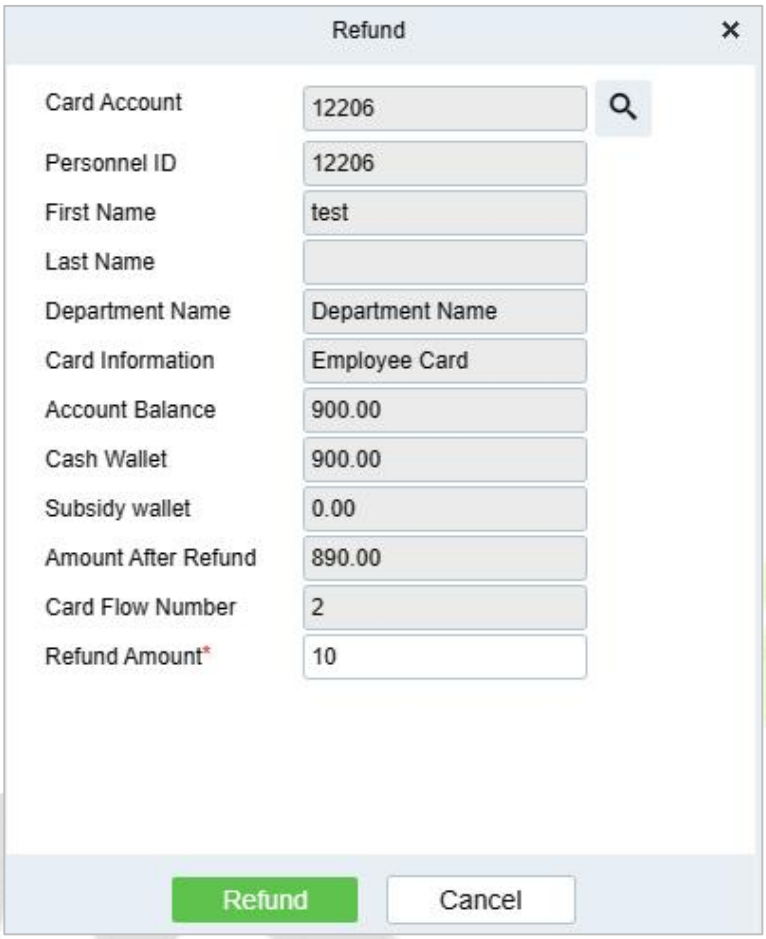


Figure 12- 35

12.3.1.3Account Opening

Open consumption account for personnel in the system, newly staff will open the account automatically, batch import staff need manually to open his account.

Click **Account Opening** to open the account opening dialog box, select the personnel information and click **Account Opening** to finish the process.

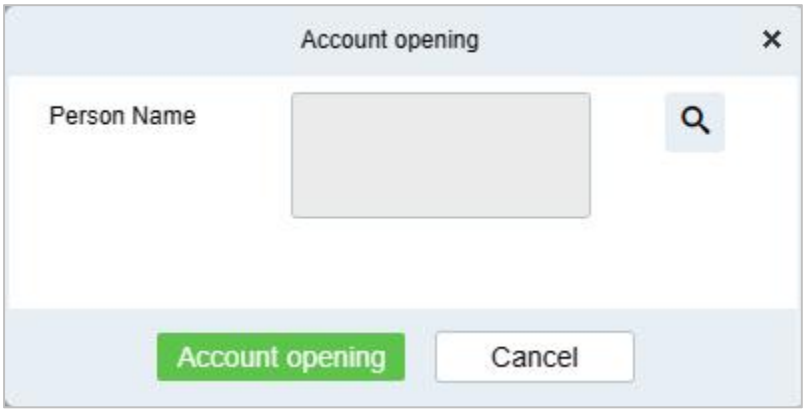


Figure 12- 36

12.3.1.4Batch Top Up

- Batch recharge employee accounts; click **Batch Top Up**, select multiple personnel, click confirm and enter the recharge amount, click **Top Up**.

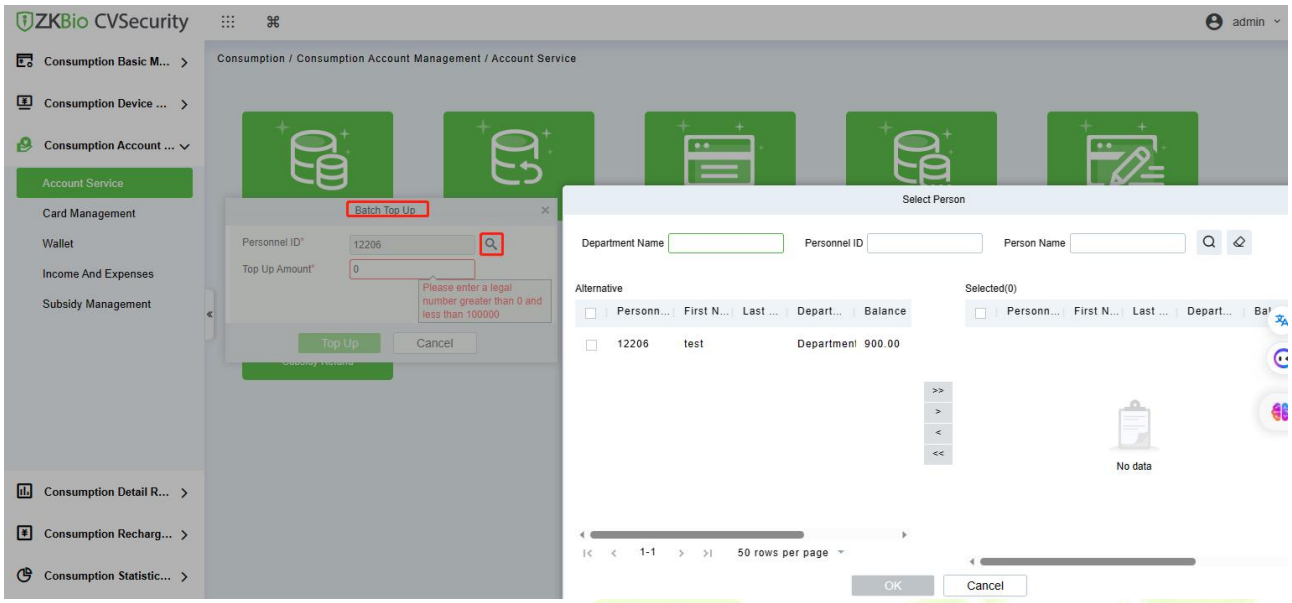


Figure 12- 37

12.3.1.5Modify Card Information

Select the account, modify the account information.

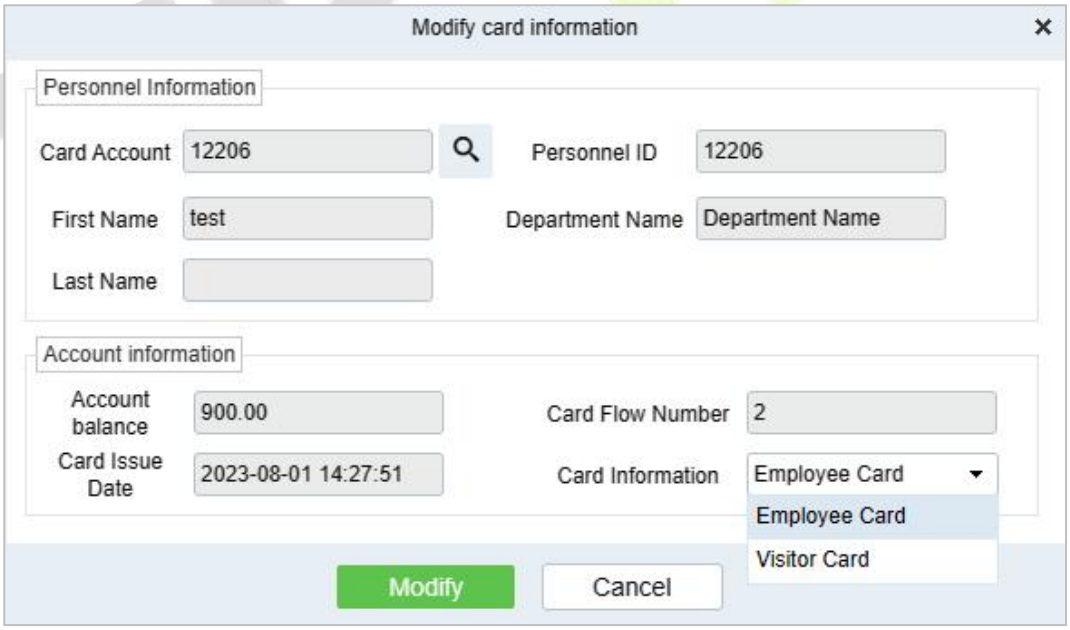


Figure 12- 38

All fields are not editable except for the **Card Information** (account category) which can be modified.

12.3.1.6Subsidy Refund

Subsidized refunds to designated accounts.

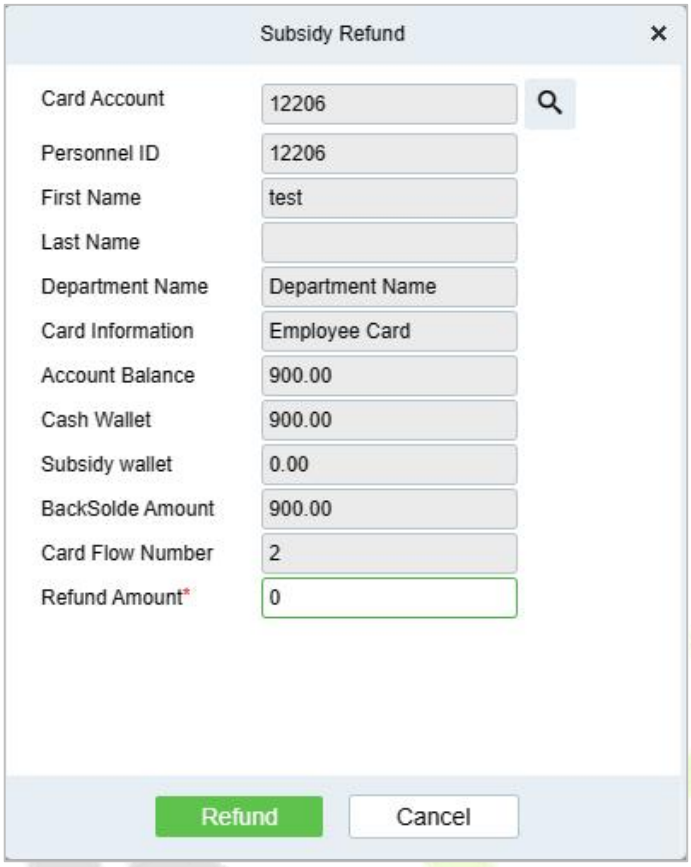


Figure 12- 39

12.3.2Card Management

This function is used to manage account, such as enable, disable, set operator, modify account category .

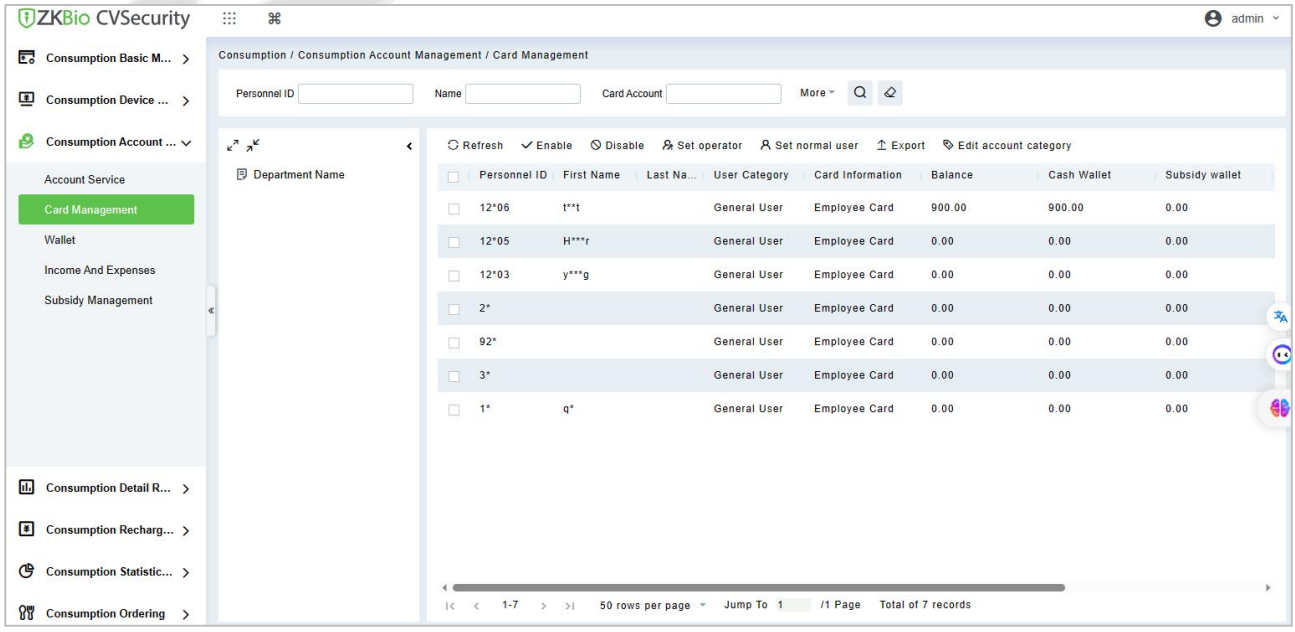


Figure 12- 40

12.3.2.1 Enable/Disable

These functions are used to enable or disable staff account .

12.3.2.2 Set Operator

Check the account and click this button to set this account as the device operator. The balance of the consumption account of the operator must be 0, and it cannot be consume normally, and it is the operation manager of consumption device.

12.3.2.3 Set Normal User

Check the account and click this button to set this account as the normal user. The normal user is normal consumption user.

12.3.2.4 Export

It exports the current report data.

12.3.2.5 Edit Account Category

It allows user to modify the account category, batch editable.

12.3.3 Wallet

This page will show all the accounts information in the system, include status, balance.

Click **Consumption Account Management** > **Wallet**, as shown below:

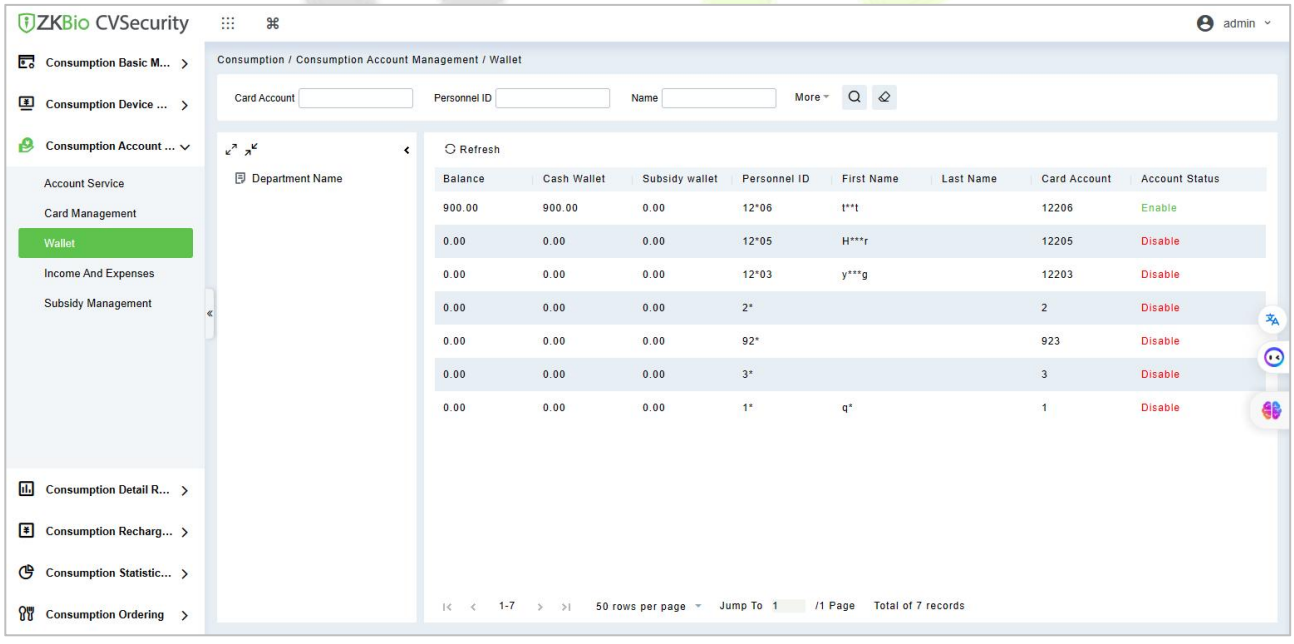


Figure 12- 41

12.3.4 Income and Expenses

This function will show all the payments and due amount data of all the accounts in the consumption system.

Click **Card Management** > **Income and Expenses**, as shown below:

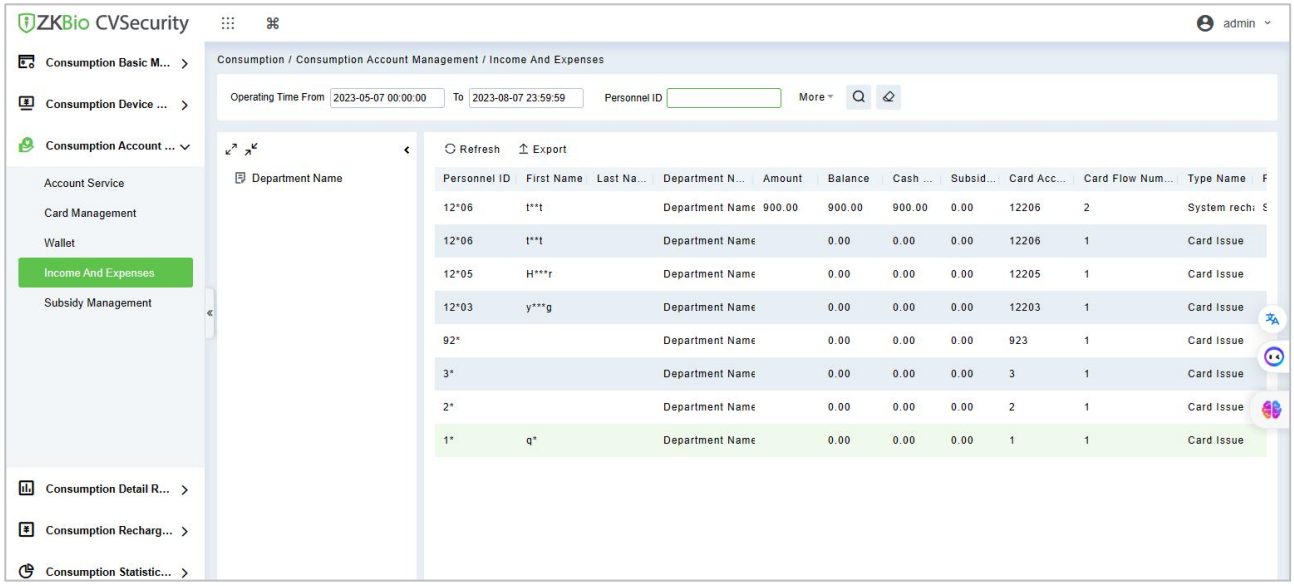


Figure 12- 42

12.3.4.1 Refresh

Click **Refresh** to load the latest account cash receipts and payments data.

12.3.5 Subsidy Management

Click **Subsidy** > **Subsidy Management** to enter the subsidy page, you can perform different function related to subsidy:

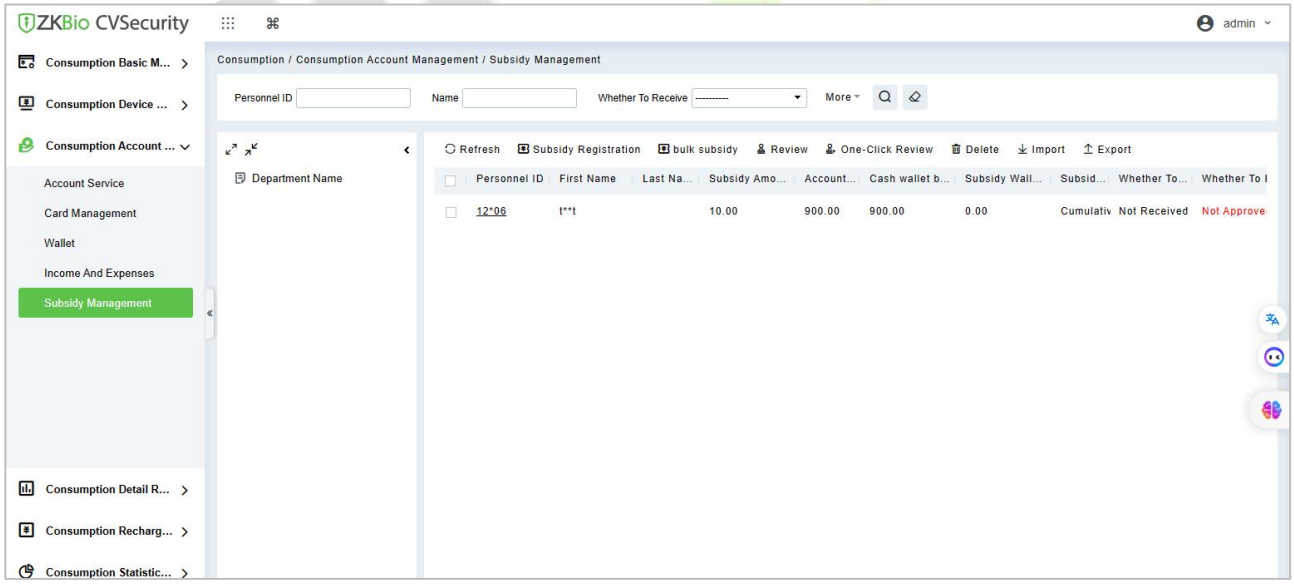


Figure 12- 43

12.3.5.1 Add

Click **Subsidy Management** > **Subsidy Registration** to enter the subsidy registration interface:

Select the account you want to performed, input the subsidy money and type, and select the arrival time, then click OK to finish the subsidy registration.

Accumulated subsidy: the current subsidy amount and the historical subsidy amount are accumulated.

Subsidy After Zeroing: Empty the balance of historical subsidy and write the current subsidy amount.

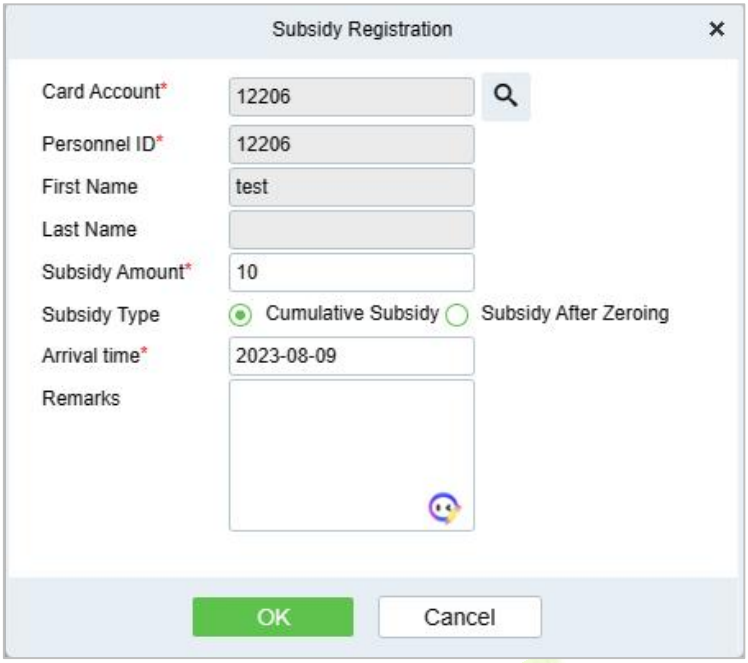


Figure 12- 44

12.3.5.2Review

This function is mainly to review the audit. Before performing audit, you need to select the subsidy (select in the multi-select box). After clicking the review, an audit dialog box will pop up. The dialog box will display the person number and name as selected by the user.

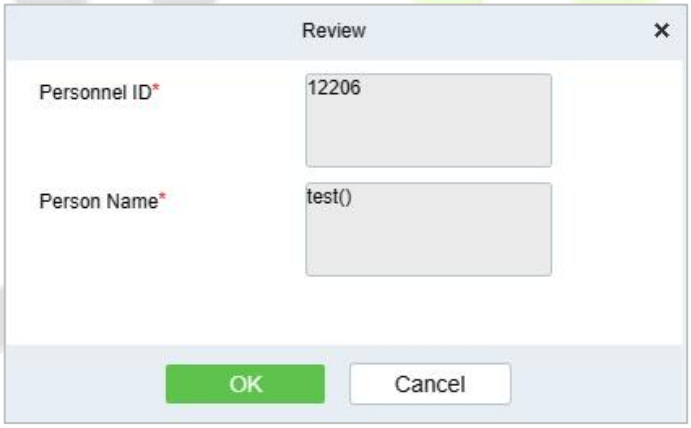


Figure 12- 45

12.3.5.3One-click Review

This function is mainly to review the unapproved subsidies in the system, and will not deal with the subsidy records that have been approved. During the review process, if the unapproved subsidy cannot be approved for some reason (such as the user has already returned the card), the subsidy will not be processed.

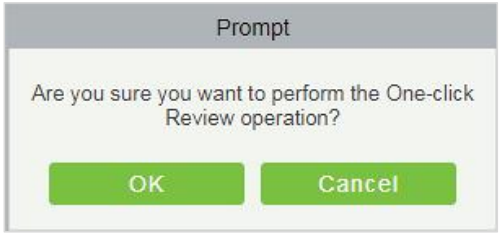


Figure 12- 46

12.3.5.4Delete

Select the required subsidy record(s) and click Delete under the operation bar to delete the subsidy record. It only supports the removal of unapproved subsidy(s).

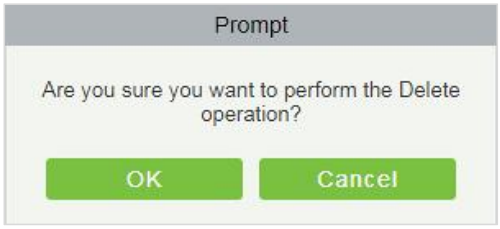


Figure 12- 47

12.3.5.5Import

This function is used to import subsidies in batches.

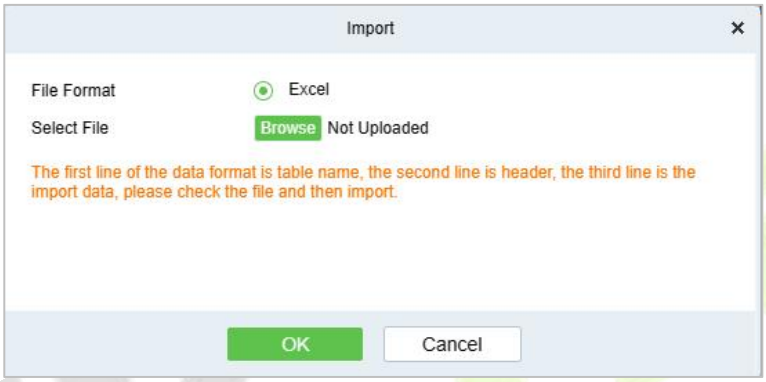


Figure 12- 48

12.3.5.6Export

This function is used to export the queried subsidies. Click on Export to open the exporting interface.

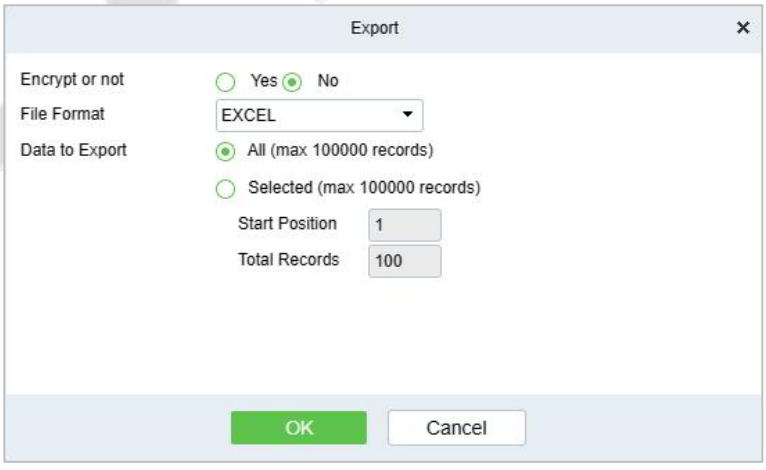


Figure 12- 49

Select the file type and export mode. If you select **All data**, then all query data limited to 40,000 will be exported. If you want to export only few results from the query, then select the second mode and enter the desired start and end points of the required data to be exported.

Click **OK** to finish.

12.4 Consumption Detail Report

12.4.1 Consumption Details Report

Click **Consumption Details** > **Consumption Details Report**, as shown below:

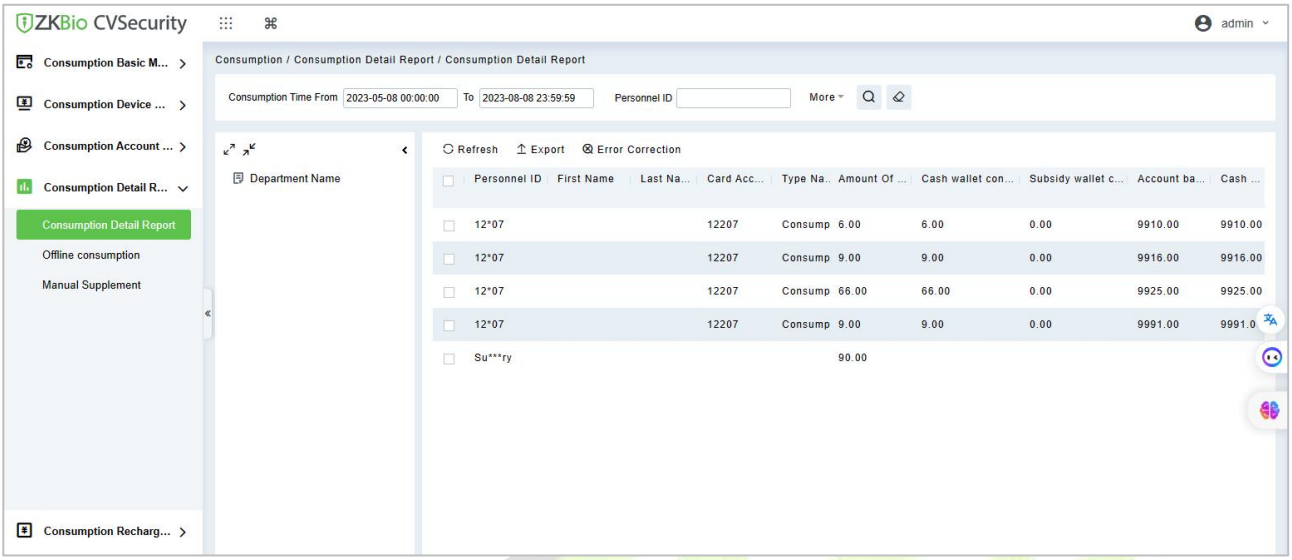


Figure 12- 50

12.4.1.1 Refresh

Click **Refresh** to load the latest consumption details.

12.4.1.2 Export

This feature allows you to export consumption details in EXCEL, PDF, CSV format files.

12.4.1.3 Error Correction

Click **Error Correction**. You can carry out the error correction process on the software. This operation is only valid for the records where the consumption type is the amount mode. Select a consumption record, read out the current balance of the card, enter the correct amount of consumption, and modify the balance of the card.

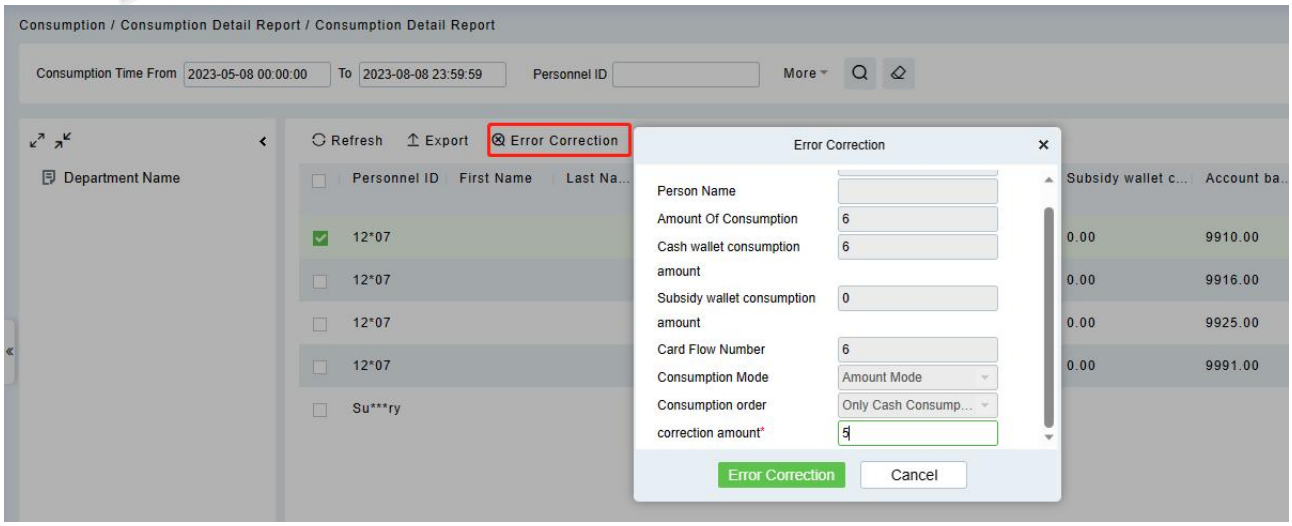


Figure 12- 51

✍Notes:

1) The same consumption record cannot be corrected repeatedly.
2) Software error correction automatically produces two new records: One is the record for the system error correction of the return of the original error consumption amount, the other is the correct consumption record of the manual supplement.

12.4.2Offline Consumption

If the device supports offline consumption, after offline consumption, it will upload the consumption record during the offline period when device connect to software, and allows user manually review it.:

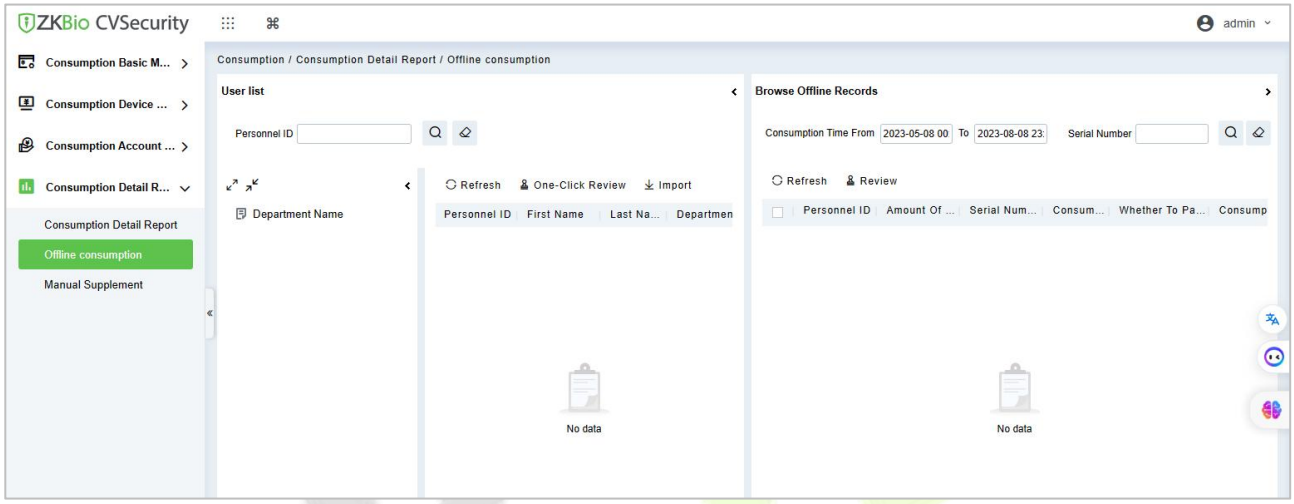


Figure 12- 52

The consumption records uploaded to the software during the offline period have not passed the audit and need to be manually reviewed before recorded.

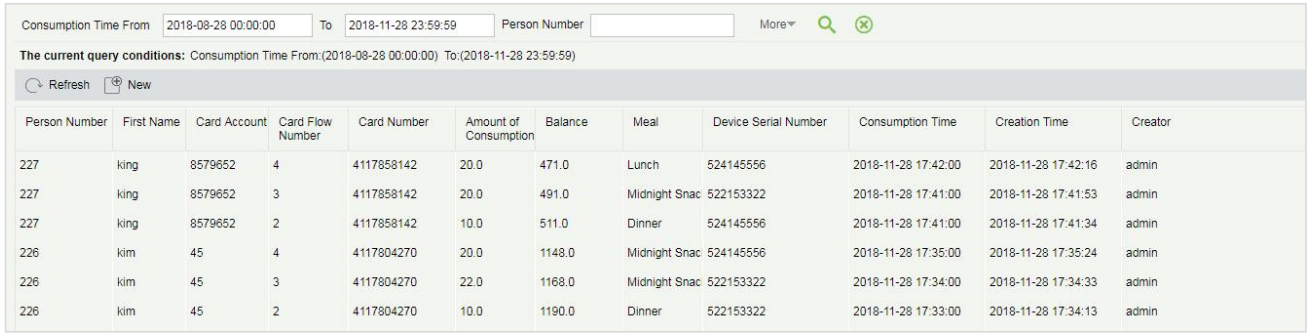
This function is mainly used to audit offline consumption records. Check the consumption records that have not passed the audit, click "Audit", and the audit dialog box will pop up. Click "OK" to complete the audit.

✍**Note:** After offline consumption audit, cash wallet may appear negative, subsidy wallet can not be negative, when the subsidy wallet balance is insufficient to automatically converted to cash wallet deduction.

12.4.3Manual Supplement

It is used to enter some consumption record details manually in the system.

✍**Note:** Before performing this operation, you need to have the relevant operation card.



Person Number	First Name	Card Account	Card Flow Number	Card Number	Amount of Consumption	Balance	Meal	Device Serial Number	Consumption Time	Creation Time	Creator
227	king	8579652	4	4117858142	20.0	471.0	Lunch	524145556	2018-11-28 17:42:00	2018-11-28 17:42:16	admin
227	king	8579652	3	4117858142	20.0	491.0	Midnight Snac	522153322	2018-11-28 17:41:00	2018-11-28 17:41:53	admin
227	king	8579652	2	4117858142	10.0	511.0	Dinner	524145556	2018-11-28 17:41:00	2018-11-28 17:41:34	admin
226	kim	45	4	4117804270	20.0	1148.0	Midnight Snac	524145556	2018-11-28 17:35:00	2018-11-28 17:35:24	admin
226	kim	45	3	4117804270	22.0	1168.0	Midnight Snac	522153322	2018-11-28 17:34:00	2018-11-28 17:34:33	admin
226	kim	45	2	4117804270	10.0	1190.0	Dinner	522153322	2018-11-28 17:33:00	2018-11-28 17:34:13	admin

Figure 12- 53

12.5 Consumption Recharge Detail Report

The consumption report consists of 4 type of reports: Top Up report, Refund report, Subsidy report, Card Balance report.

12.5.1 Top Up Table

Click Consumption Report > Top Up Table, as shown below:

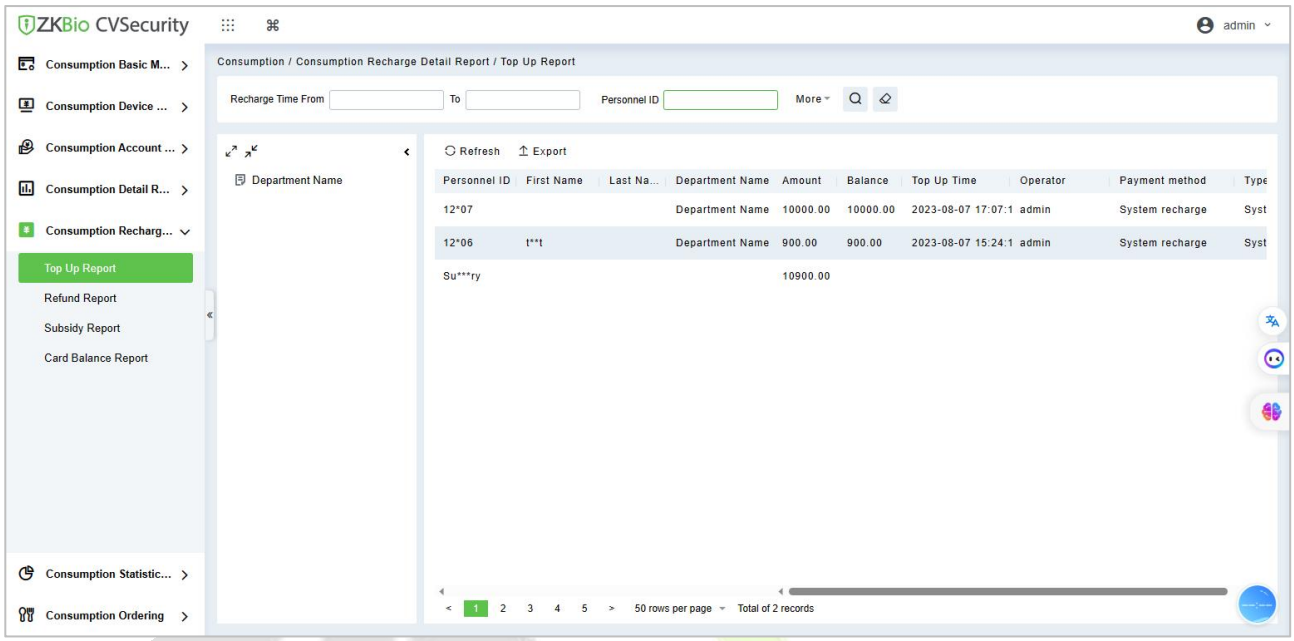


Figure 12- 54

12.5.1.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

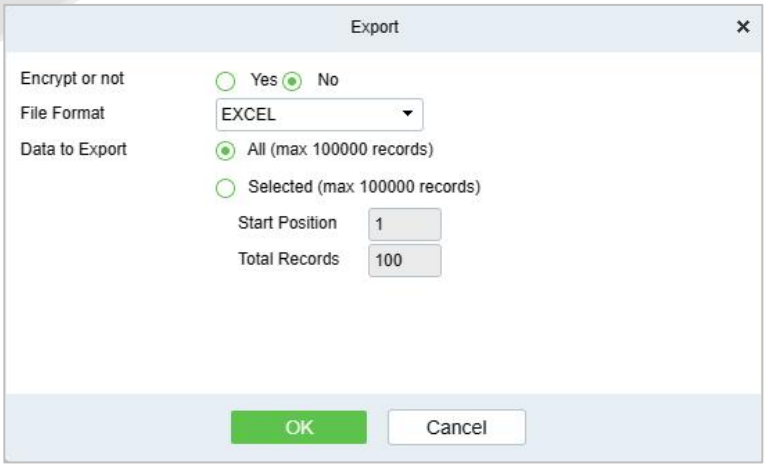


Figure 12- 55

12.5.2Refund Table

Click Consumption Report > Refund Table, as shown below:

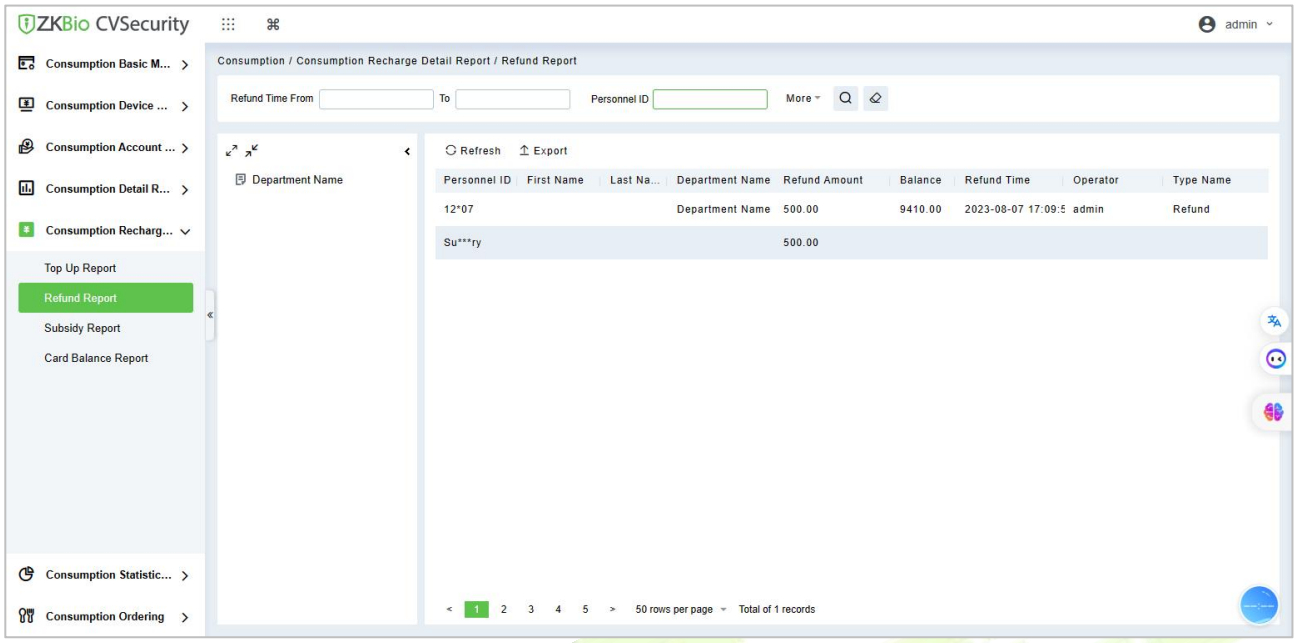


Figure 12- 56

12.5.2.1Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

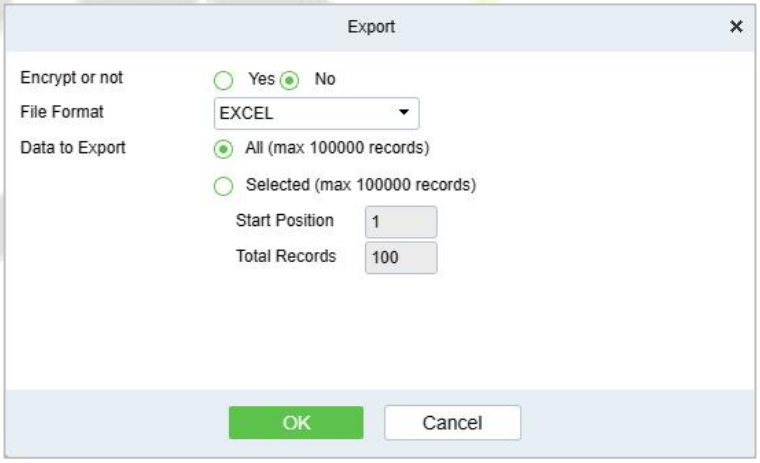


Figure 12- 57

12.5.3Subsidy Table

Click Consumption Report > Subsidy Table, as shown below:

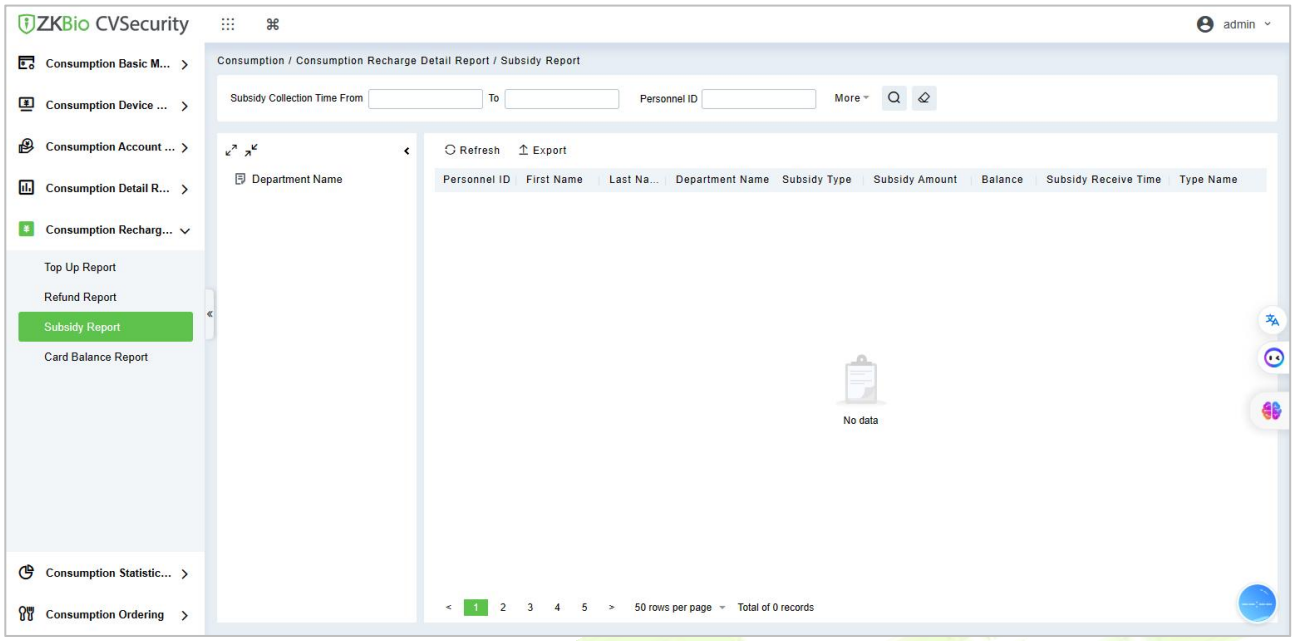


Figure 12- 58

12.5.3.1Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.5.4Card Balance Table

Click **Consumption Report** > **Card Balance Table**, as shown below:

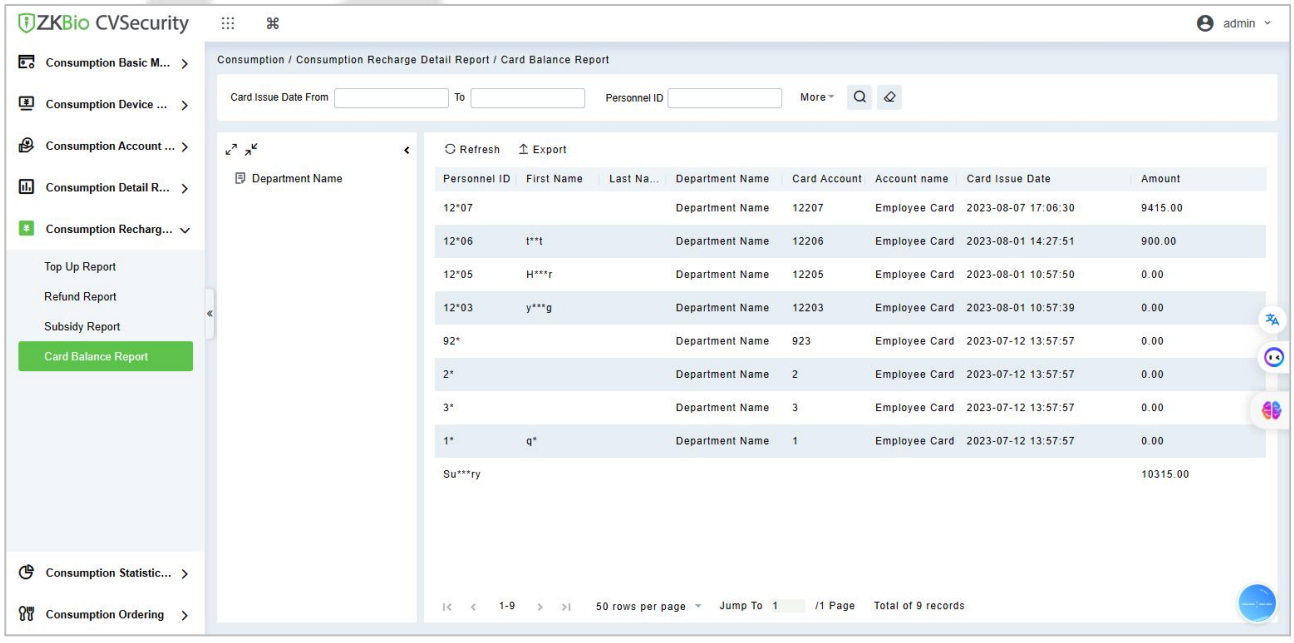


Figure 12- 59

12.5.4.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6 Consumption Statistical Report

The statistical report contains the statistical information of consumption system module.

12.6.1 Personal Consumption Statistics

Click **Statistical Report** > **Personal Consumption Statistics**, as shown below:

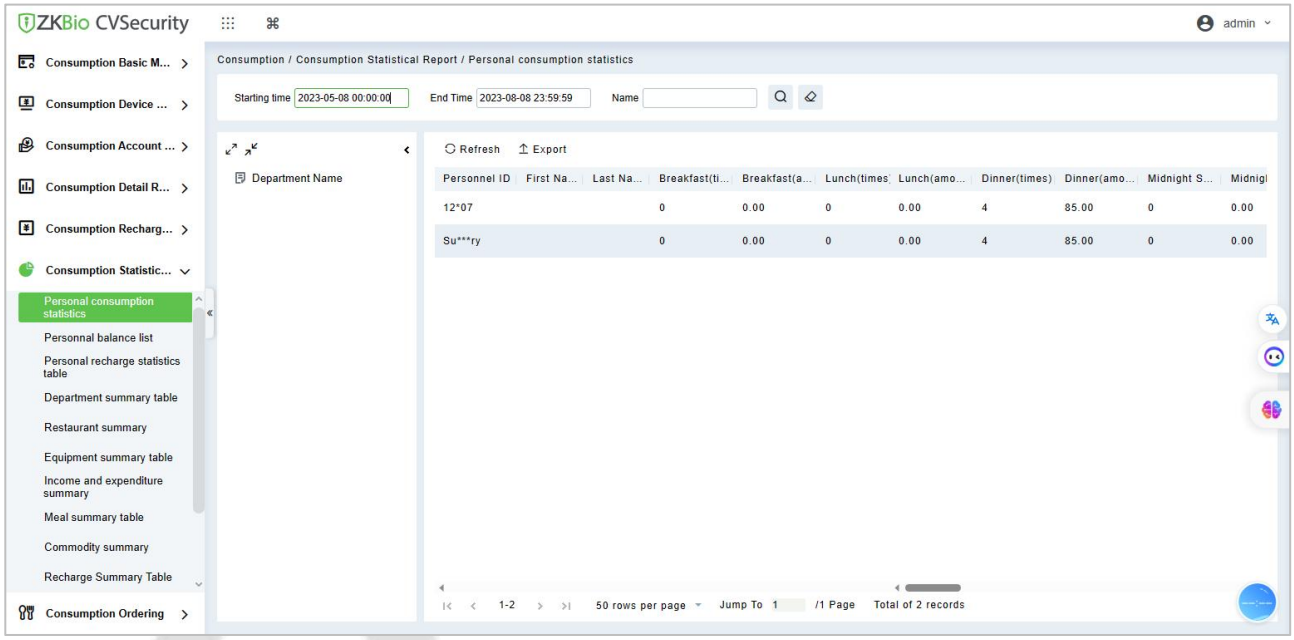


Figure 12- 60

12.6.1.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.1.2 Refresh

Click **Refresh** to load the latest personal consumption statistics table data.

✍ **Note:** If the page personal consumption statistics table data is more, you can also enter the person name, department name, consumption time in the search field, click to search and query.

The data statistics column includes below information:

Figure 12- 61

The following is the calculation formula of the specific column.

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12.6.2Personal Balance List

Click **Statistical Report** > **Personal Balance List**, as shown below:

This report list shows all account balance information.

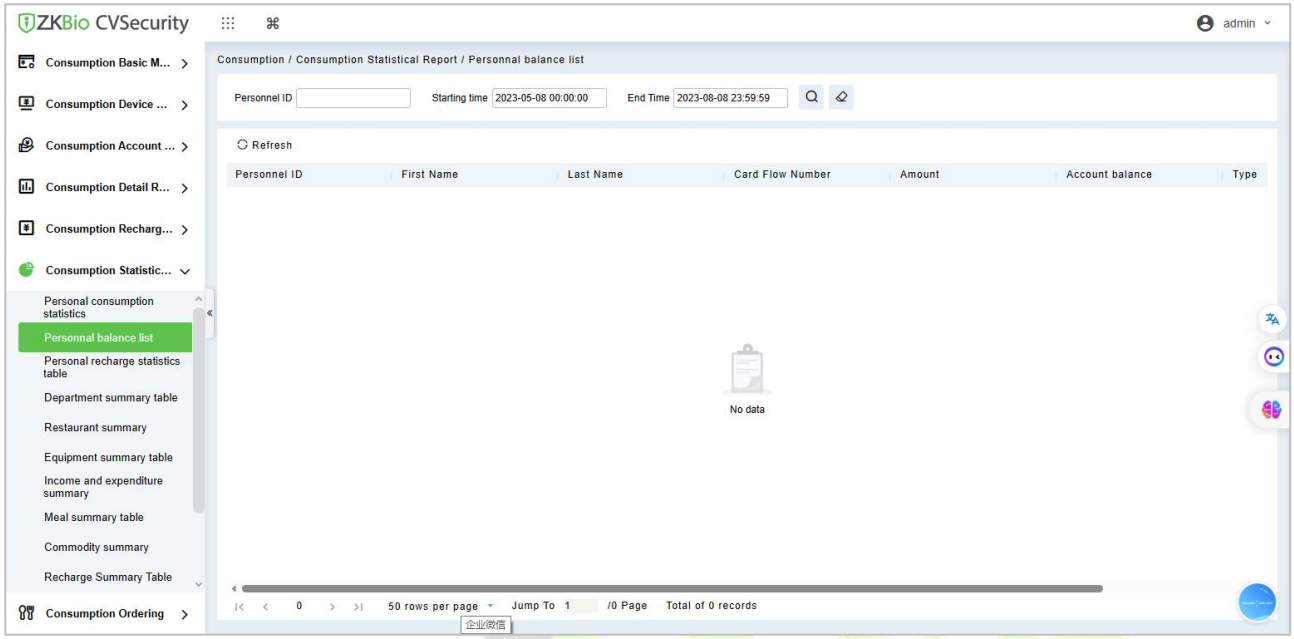


Figure 12- 62

12.6.3Personal Recharge Statistics Table

Click **Statistical Report** > **Personal Recharge List**, as shown below:

This report list shows all account recharge information.

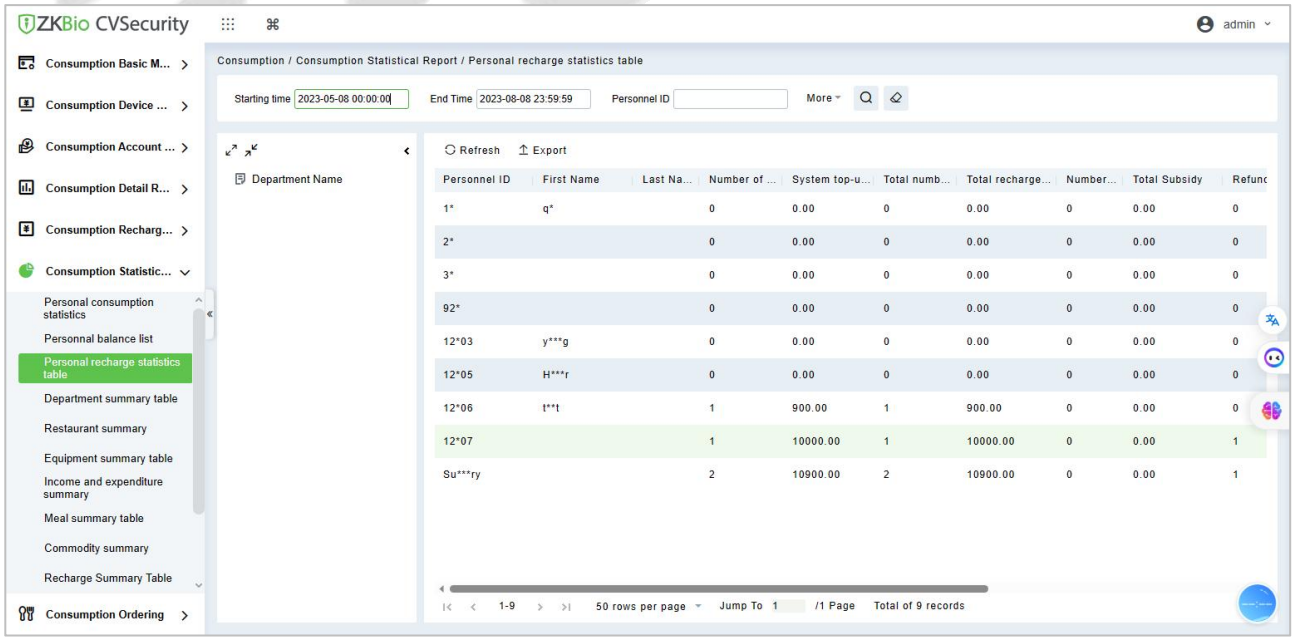


Figure 12- 63

12.6.4Department Summary Table

Click **Statistical Report** > **Department Summary Table** as shown below:

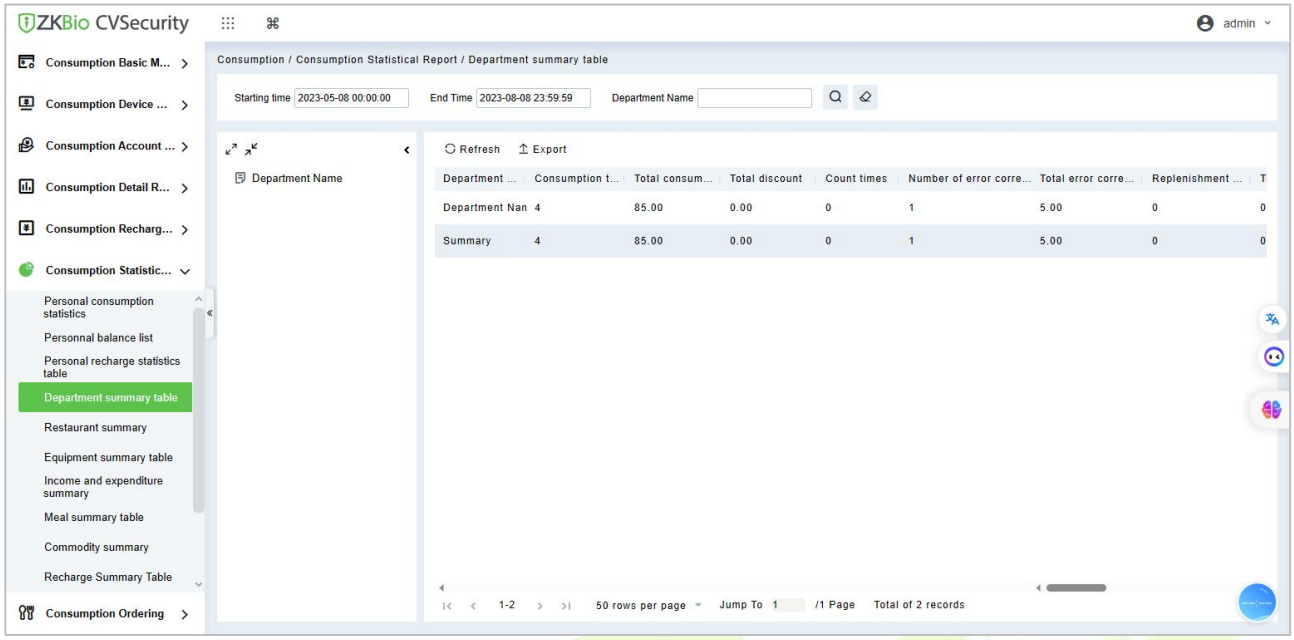


Figure 12- 64

12.6.4.1Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.4.2Refresh

Click **Refresh** to load the latest department summary table data.

✍**Note:** If the page department summary table data is more, you can also enter the department name and consumption time in the search field, and click to search for the query.

The data statistics column includes:

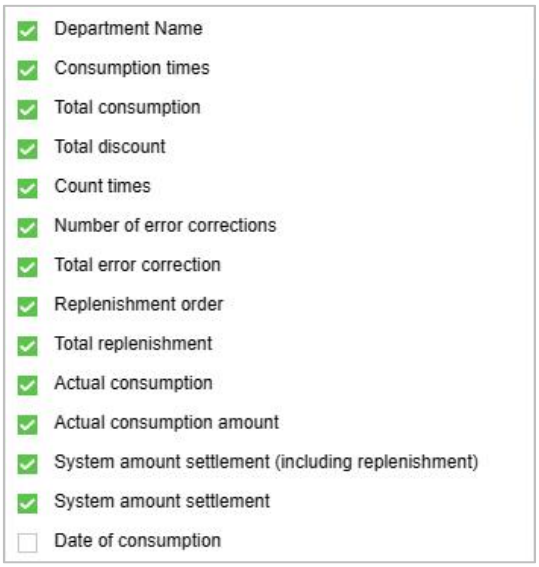


Figure 12- 65

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type.
- **Total Error Correction** = Total amount of error correction for the particular type.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12.6.5 Restaurant Summary

Click **Statistical Report** > **Restaurant Summary**, as shown below:

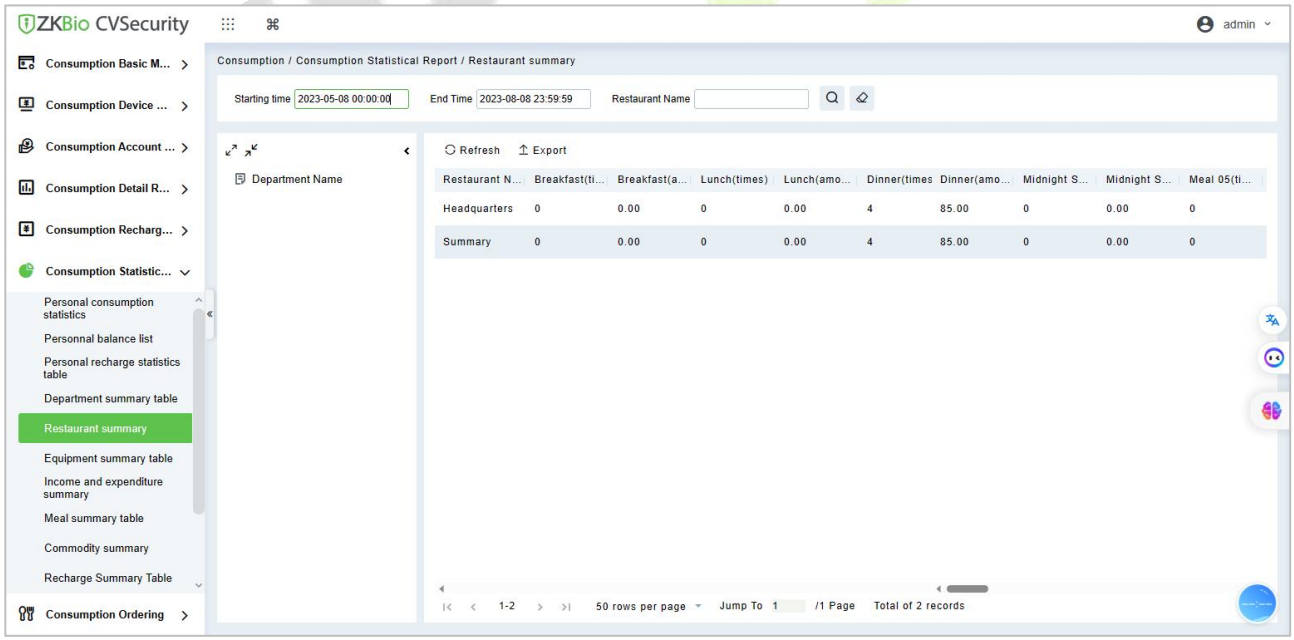


Figure 12- 66

12.6.5.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.5.2Refresh

Click **Refresh** to load the latest restaurant summary table data.

✍ **Note:** If the page restaurant summary table data is more, you can also enter the restaurant name, consumption time in the search bar, click to search and query.

The data statistics column includes:

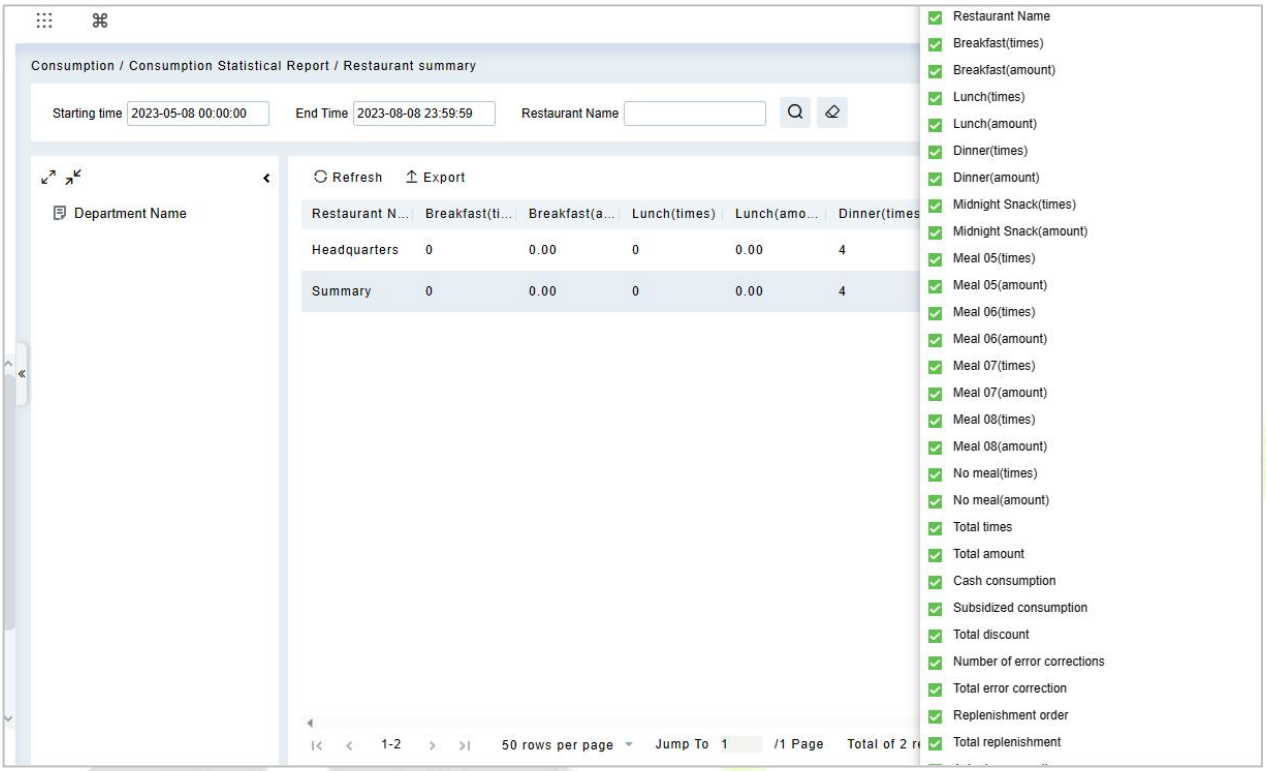


Figure 12- 67

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12.6.6Equipment Summary Table

Click **Statistical Report** > **Device Summary Table**, as shown below:

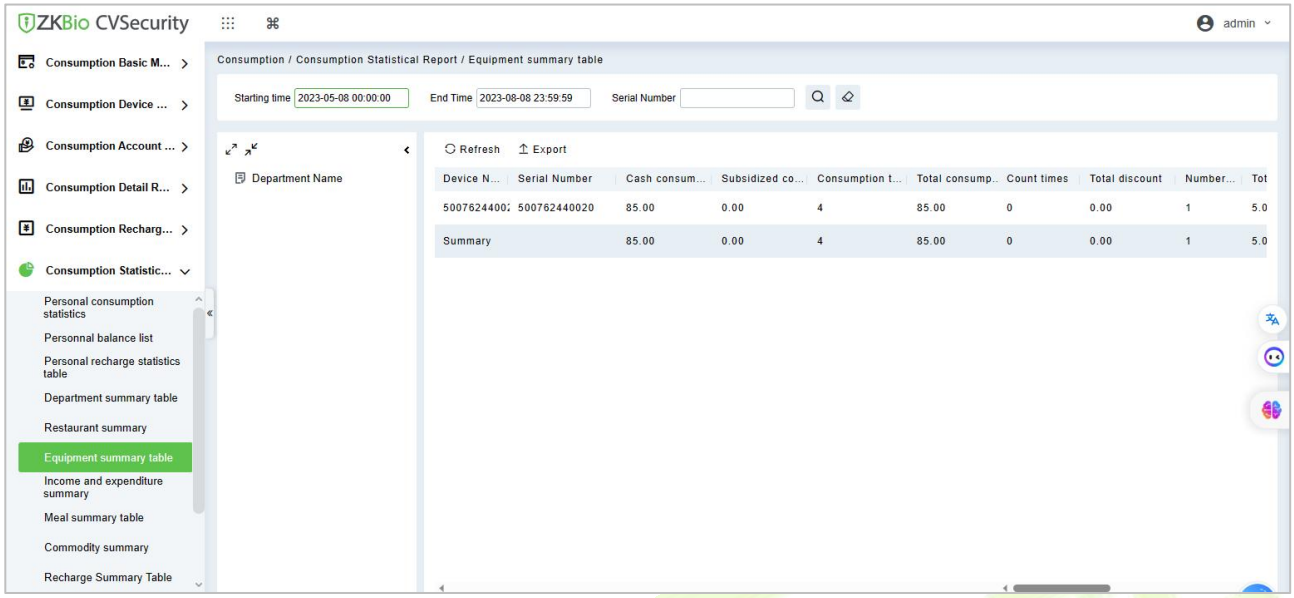


Figure 12- 68

12.6.6.1Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.6.2Refresh

Click **Refresh** to load the latest equipment summary table data.

✍**Note:** If there is more data on the page device summary table, you can also enter the device name and consumption time in the search field, and click to search for it.

The data statistics column includes:

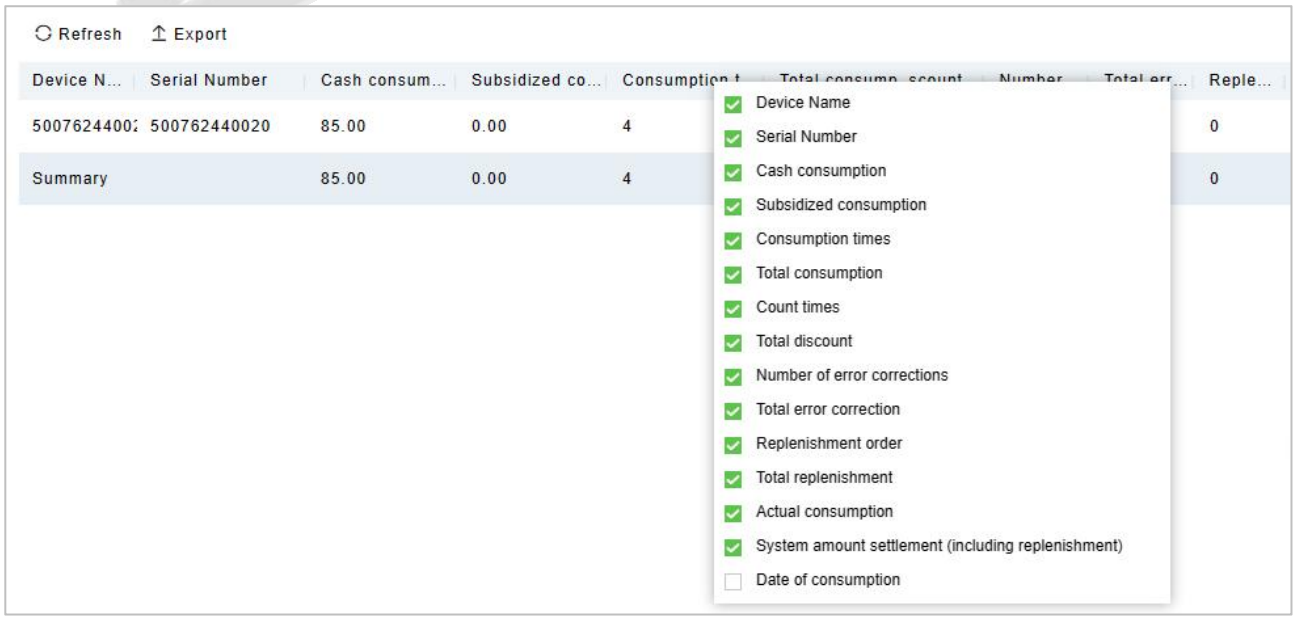


Figure 12- 69

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12.6.7 Income and Expenditures Summary

Click **Statistical Report** > **Income and Expenditures Summary**, as shown below:

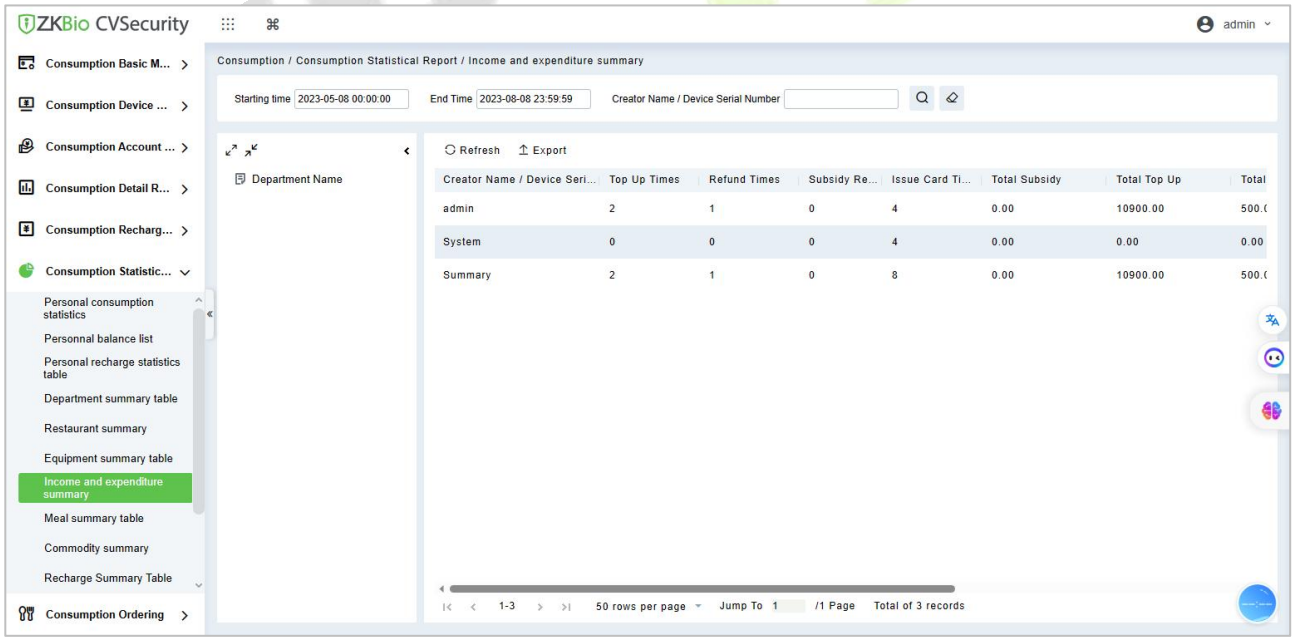


Figure 12- 70

12.6.7.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.7.2Refresh

Click **Refresh** to load the latest revenue and expenditure summary table data.

Note: If there is more data on the page income and expenditure summary table, you can also enter the creator name/device serial number and summary time in the search field, and click to search for it.

The data statistics column includes

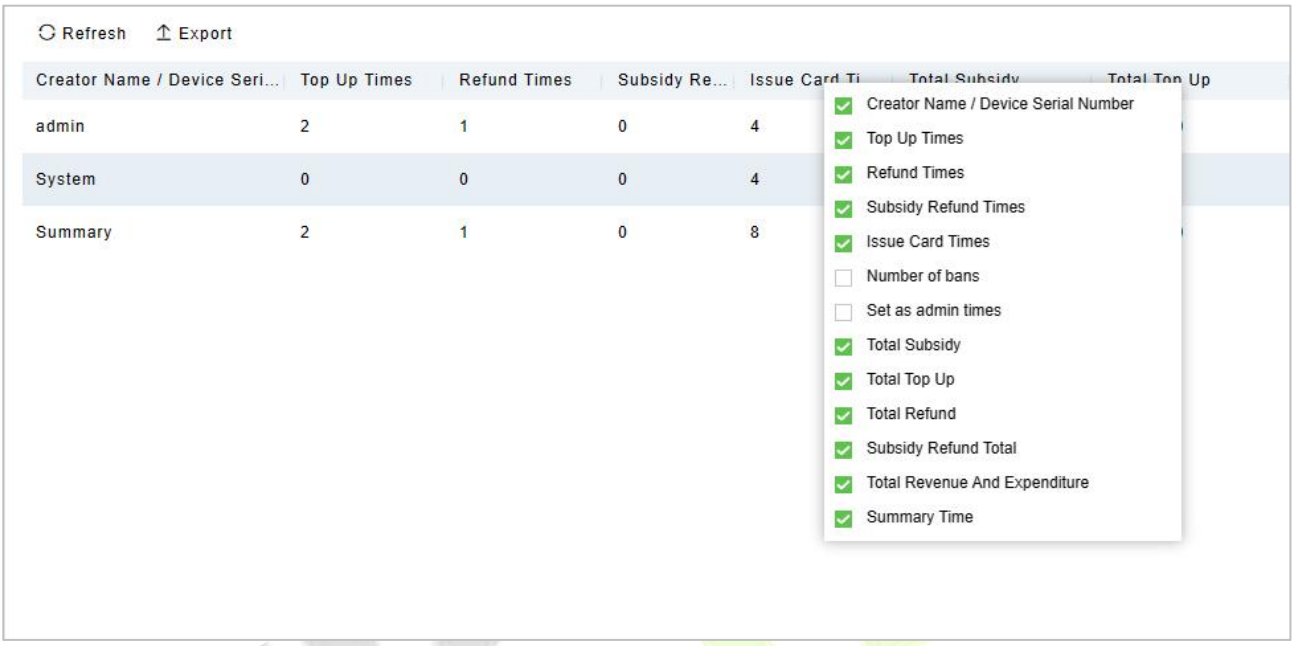


Figure 12- 71

- **Top up Times** = The total number of counts a card was added extra amount.
- **Refund Times** = The total number of counts a card were refunded.
- **Issue Card Times** = The total number of counts a card were issued.
- **Return Card Times** = The total number of counts the cards were returned.
- **Non-card Return card Times** = The total count of Non-card Return card.
- **Total Issue Card** = The total number of issued card.
- **Total Return Card** = The total number of cards returned.
- **No Card Return Card Total** = The total number of blocked card which are not returned.
- **Total Subsidy** = The total amount of subsidy for the card type.
- **Total Top-Up Offer** = The total amount of top-up discount for the card type.
- **Total Top-Up** = The total amount of top-up for the card type.
- **Total Refund** = The total amount of refund for the card type.
- **Card Cost Support** = The total amount of card cost for the card type.
- **Management Fee** = The total amount of management fee for the card type.
- **Card Cost Expense** = The total amount of card cost for the card type.
- **Total Revenue and Expenditure** = (Total Top up + Card Cost Expense + Total Issue Card + Management fee) - (Total Refund - Total Return Card).

12.6.8Meal Summary Table

Click **Statistical Report** > **Meal Summary Table**, as shown below:

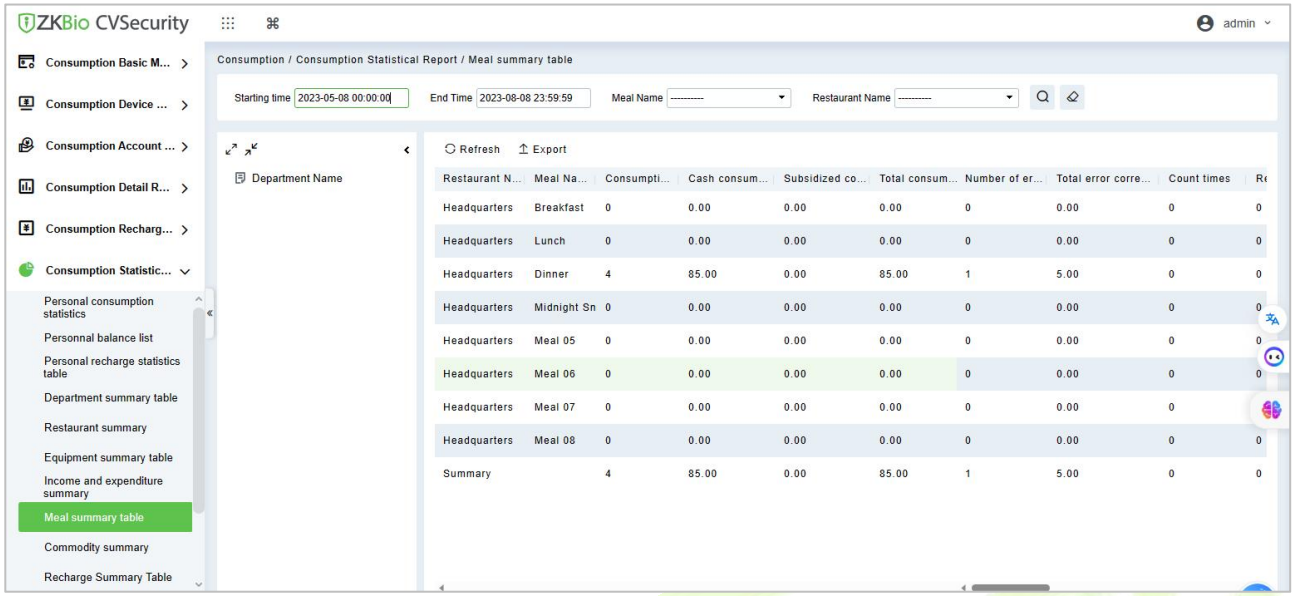


Figure 12- 72

12.6.8.1Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

12.6.8.2Refresh

Click **Refresh** to load the latest meal summary table data.

Note: If there is more data in the page meal summary table, you can also enter the device name, name, and consumption time in the search field, and click to search for it.

The data statistics column includes:

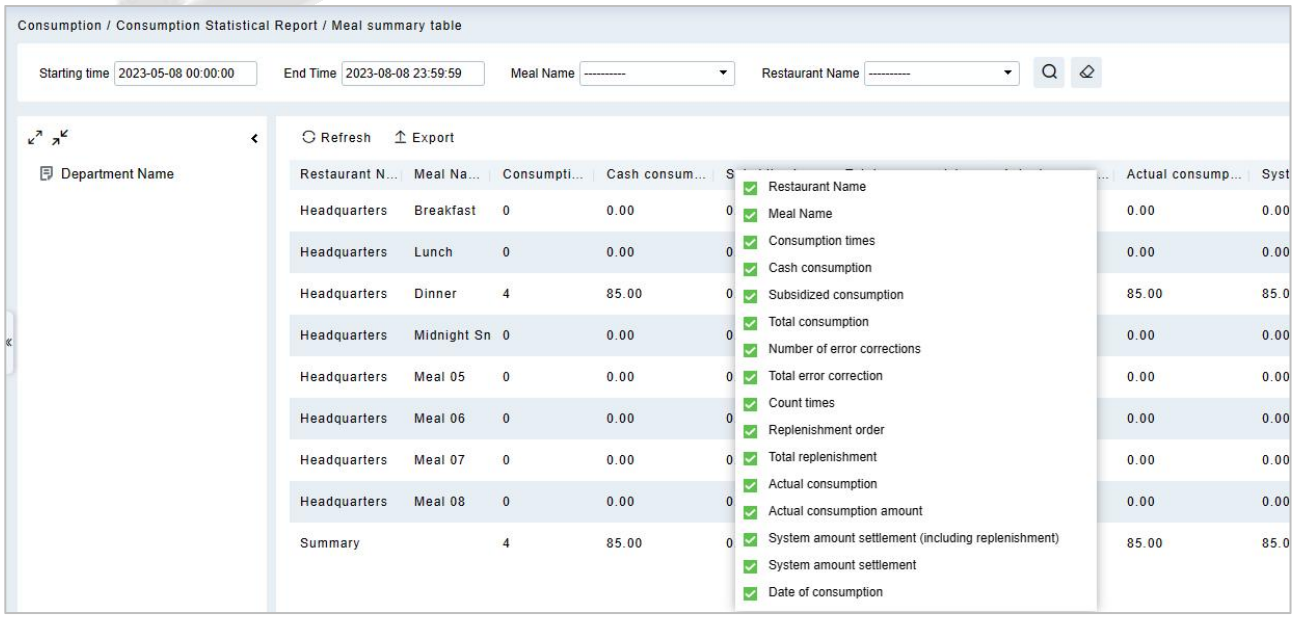


Figure 12- 73

The following is the calculation formula of the specific column.

- **Consumption Times** = Total number of count the particular type is consumed.
- **Total Consumption** = Total amount of money consumed for the particular type.
- **Counting Times** = Total number of times the type is counted.
- **Number of Error Corrections** = Total number of error correction for the particular type name.
- **Total Error Correction** = Total amount of error correction for the particular type name.
- **Times of Supplementary Order** = Total count of supplementary order for the particular type.
- **Total Supplementary Order** = Total amount of supplementary order for the particular type.
- **Accounting Times** = Total count of billing for the particular type.
- **Total Accounting** = Total amount of money billed for the particular type.
- **Actual Consumption Times (device)** = Consumption times - Number of error corrections.
- **Actual Consumption Amount (device)** = Total Consumption - Total Error Correction.
- **System Amount Settlement (including supplementary order)** = Total Consumption - (Total Error Correction + Total Supplementary Order).
- **System Amount Settlement (including billing)** = Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting).

12.6.9Commodity Summary

Click **Statistical Report** > **Meal Summary Table**, as shown below:

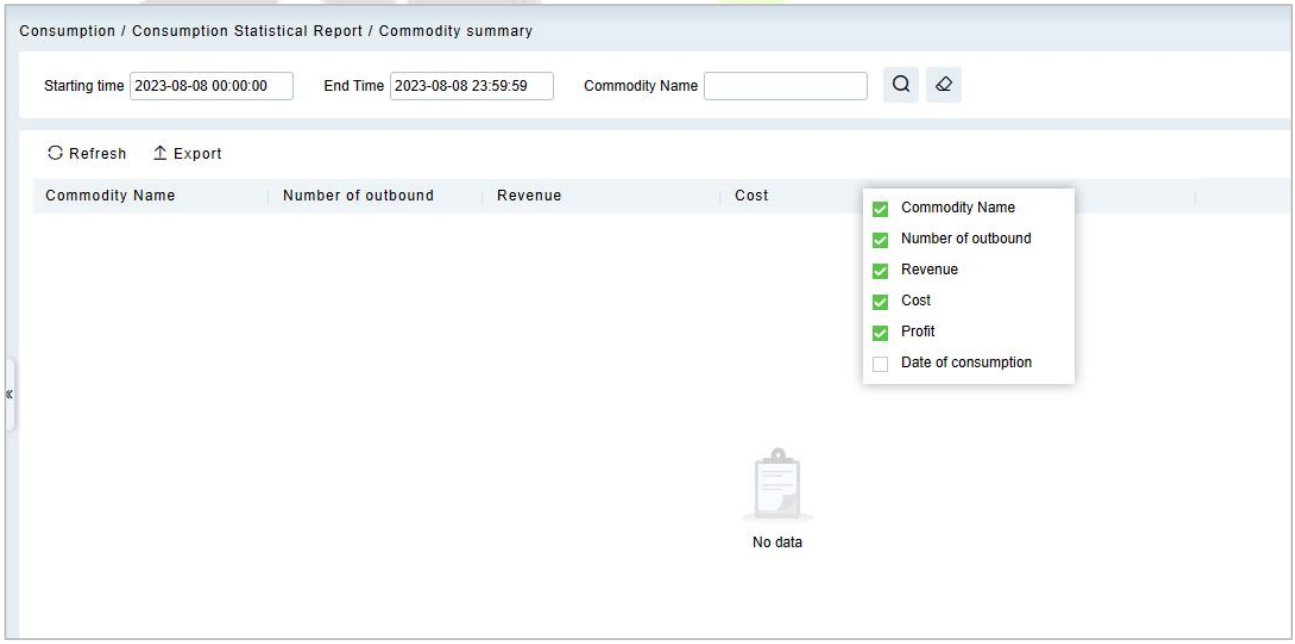


Figure 12- 74

The following is the calculation formula of the specific column.

- **Commodity Name** = Total name of count the name of consumption commodity.
- **Number of Outbound** = Total amount of consumption commodity.
- **Revenue** = Total number of revenue amount of the type is consumption commodity.

- **Cost** = Total number of cost amount of the type is consumption commodity.
- **Profit** = Total number of revenue amount of the type is consumption commodity - Total number of cost amount of the type is consumption commodity.
- **Date of Consumption** = Total name of consumption date of consume commodity.

12.6.10Recharge Summary Table

Click **Statistical Report** > **Recharge Summary Table**, as shown below:

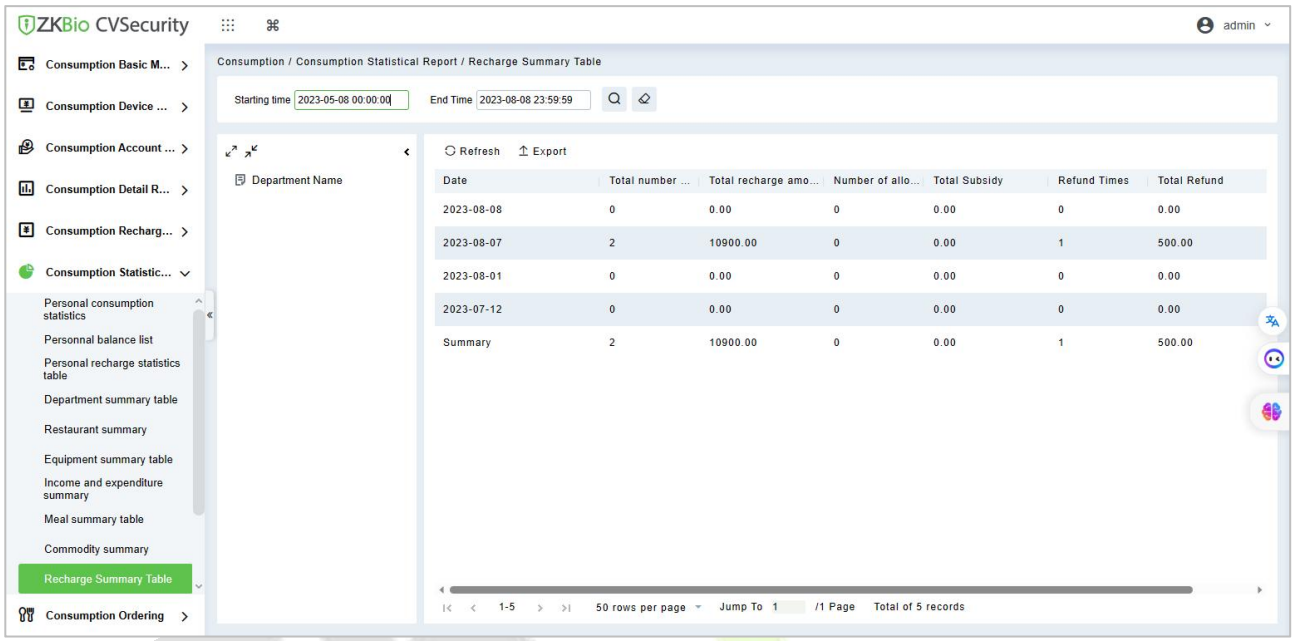


Figure 12- 75

12.6.11Personnel Meal Summary Table

Click **Statistical Report** > **Personnel Meal Summary Table**, as shown below:

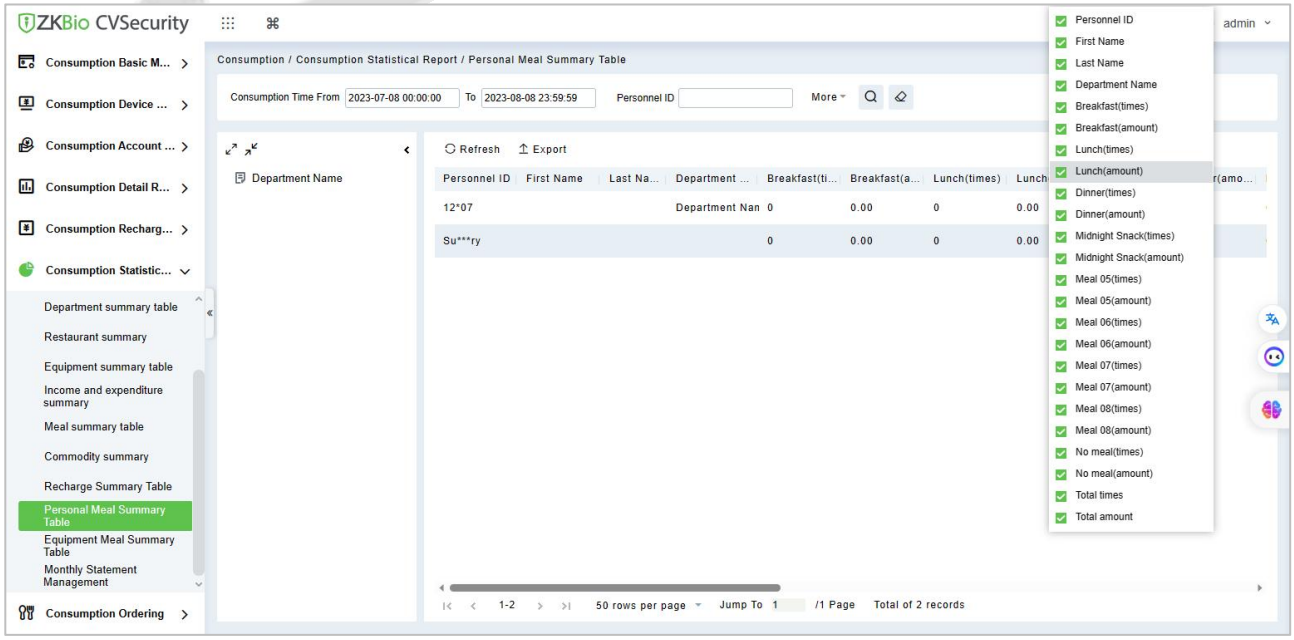


Figure 12- 76

12.6.12Device Meal Summary Table

Click **Statistical Report** > **Device Meal Summary Table**, as shown below:

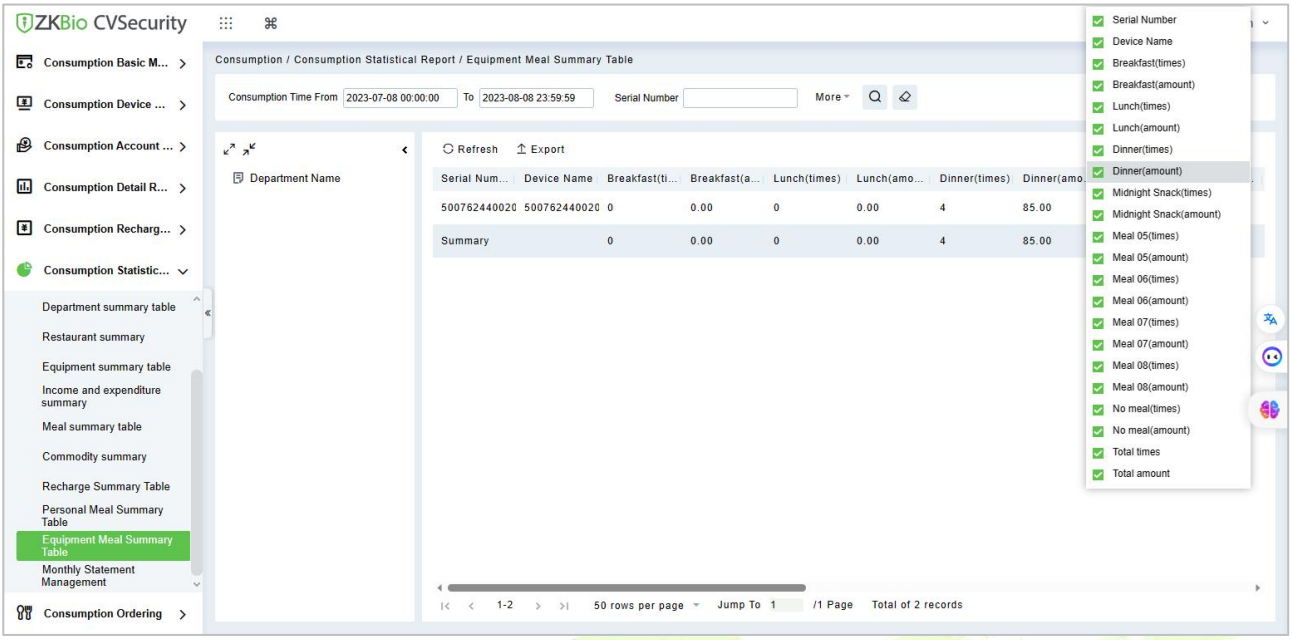


Figure 12- 77

12.6.13Monthly Statement Management

Click **Statistical Report** > **Monthly Statement Management**, as shown below:

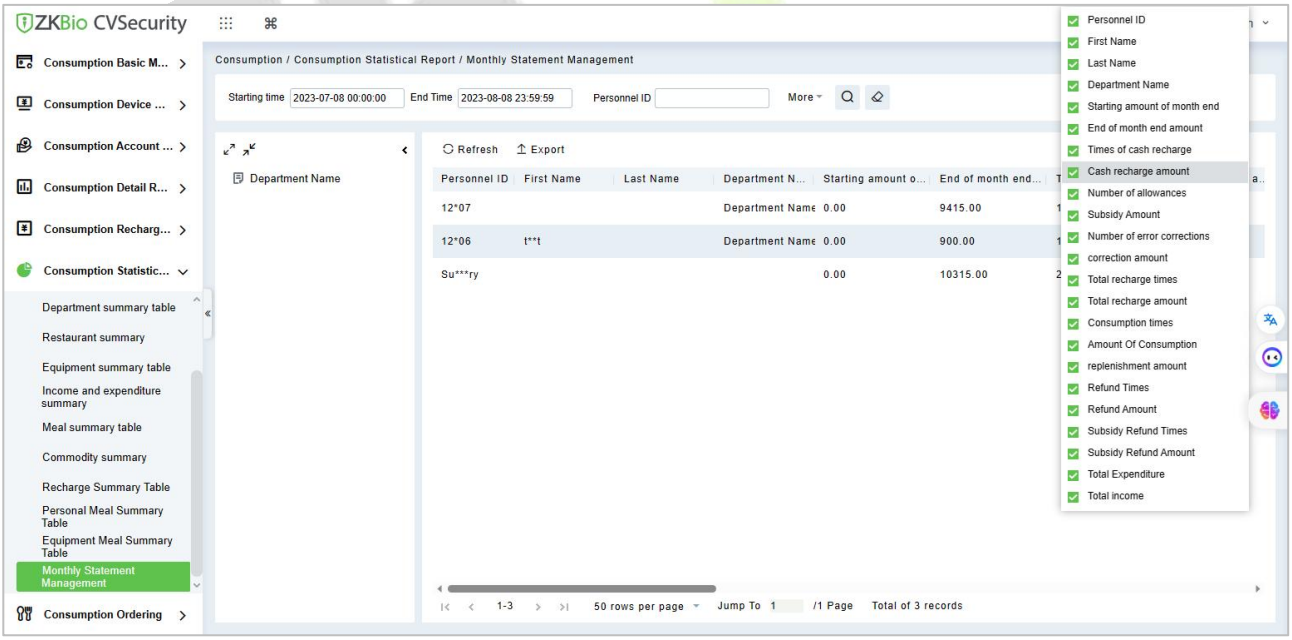


Figure 12- 78

12.7 Consumption Ordering

The platform provides food ordering management, employees can find the administrator to order food in advance.

12.7.1 Order Management

Click **Consumption Ordering** > **Order Management**, as shown below:

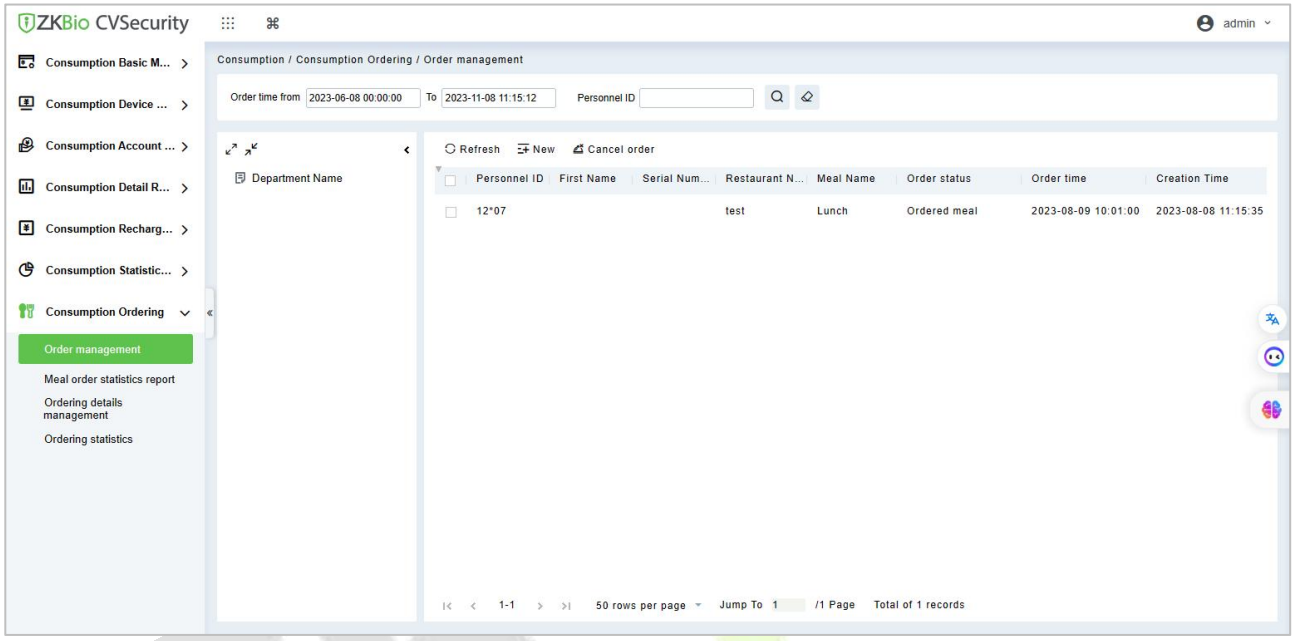


Figure 12- 79

12.7.1.1 New

Click **New** and select the personnel or department, fill in the meal ordering details.

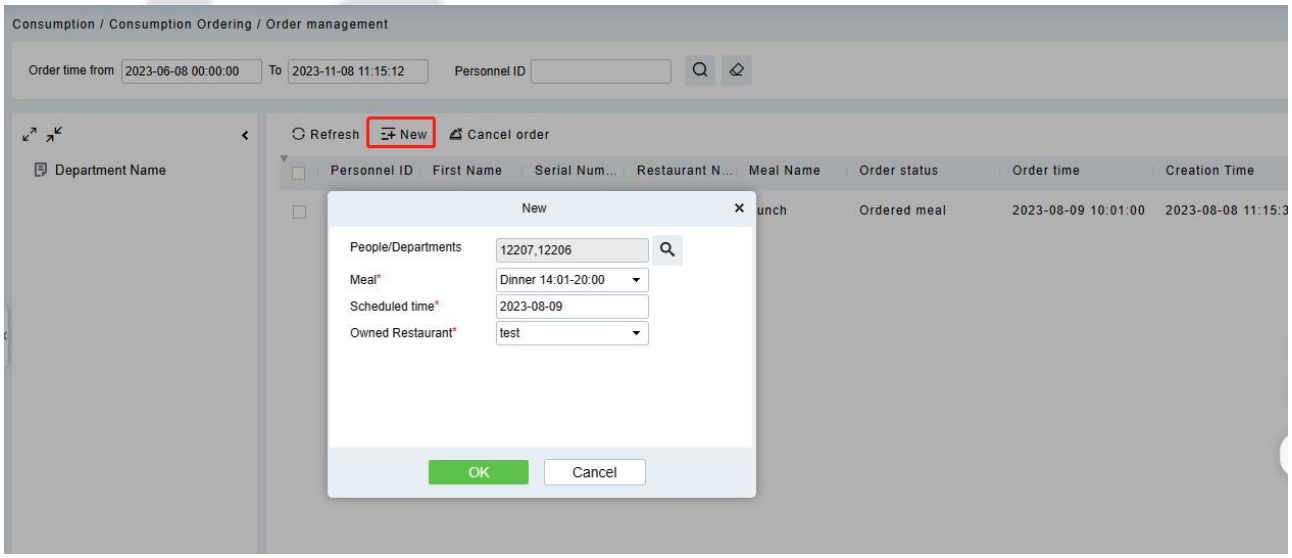


Figure 12- 80

12.7.1.2Cancel Order

Select the personnel, click **Cancel Order** to cancel the order.

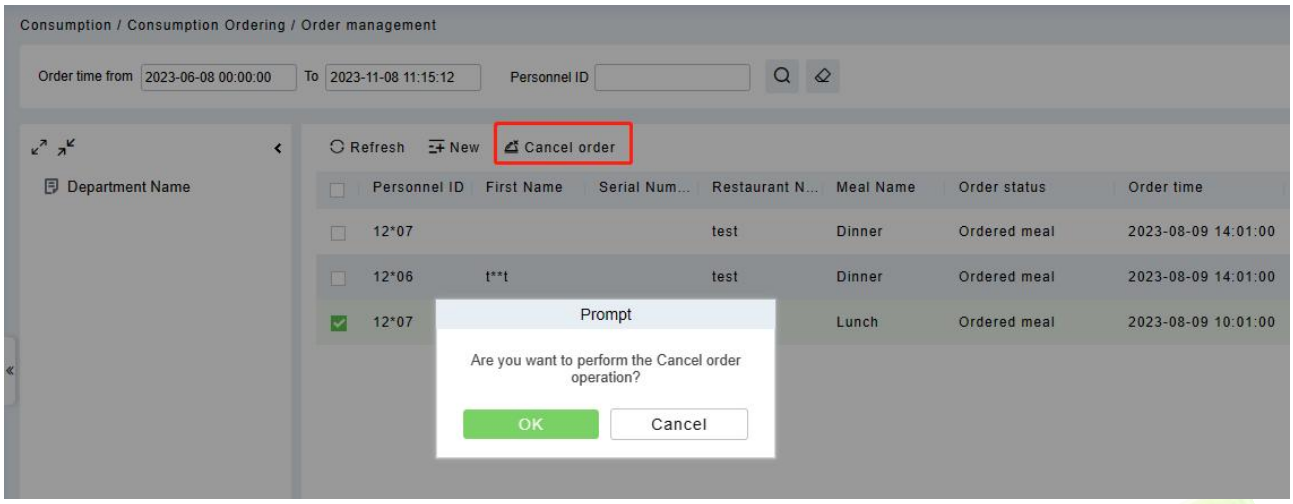


Figure 12- 81

12.7.2Meal Order Statistics Report

Click **Consumption Ordering** > **Meal Order Statistics Report**, as shown below:

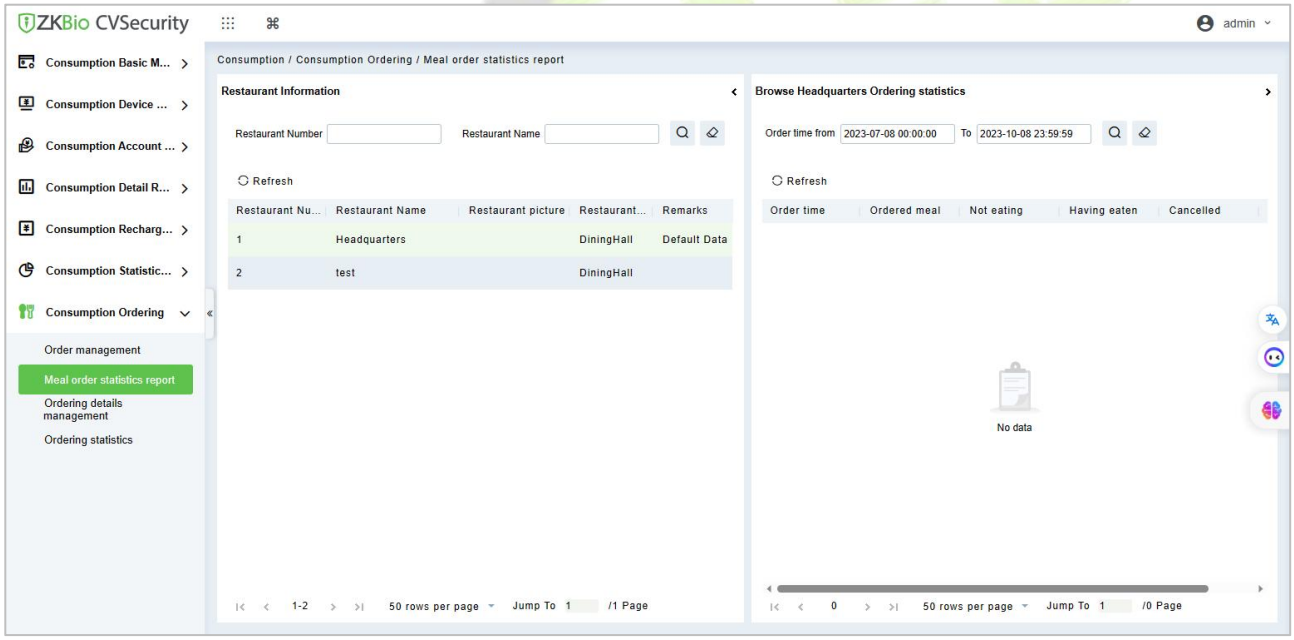


Figure 12- 82

12.7.3Ordering Details Management

Click **Consumption Ordering** > **Ordering Detail Management**, as shown below:

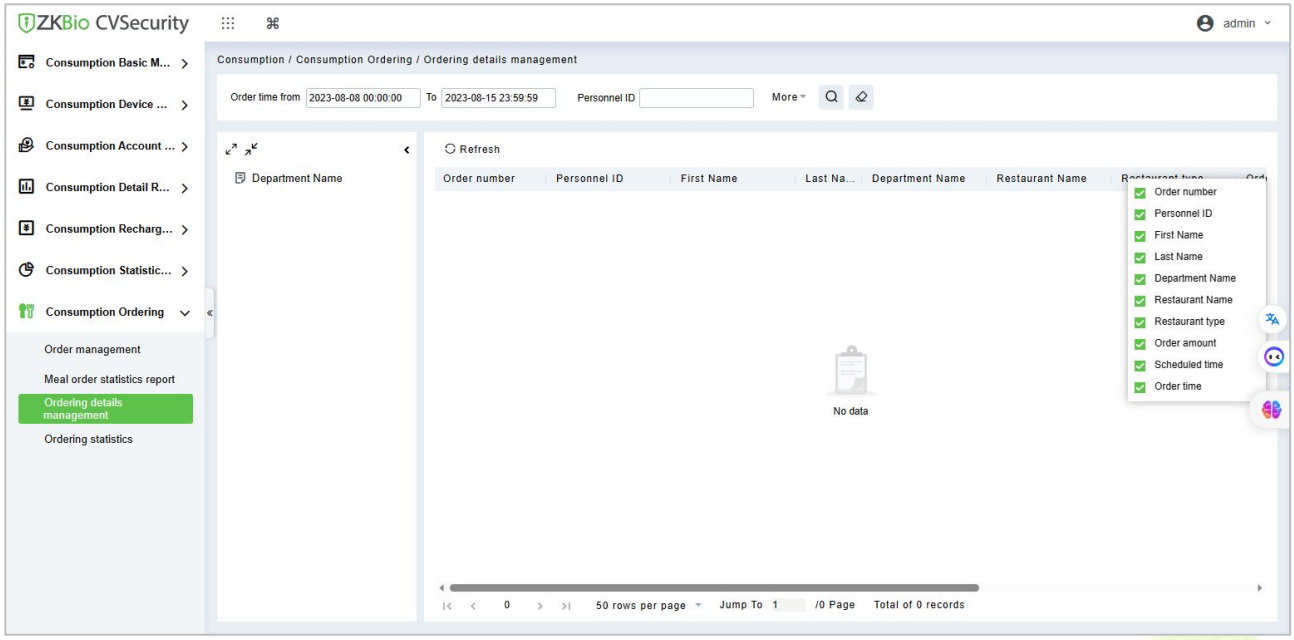


Figure 12- 83

12.7.4Ordering Statistics

Click **Consumption Ordering** > **Ordering Statistics**, as shown below:

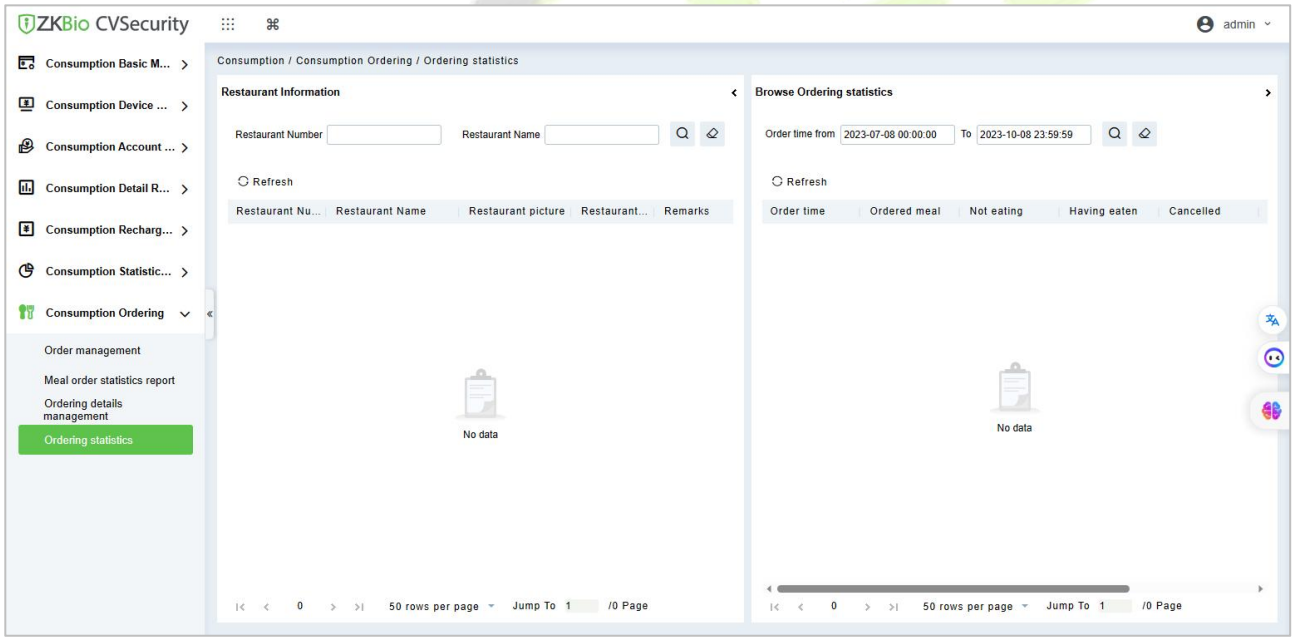


Figure 12- 84

13 Patrol

13.1 Operation Scenario

Patrol management business can realize the effective supervision and management of patrol personnel, patrol plan and patrol route by enterprise managers, and at the same time, it can also make regular statistics and analysis on patrol route and results.

13.2 Operation Flow

Introduce the configuration process of patrol management.

The patrol management configuration process is shown in figure below.

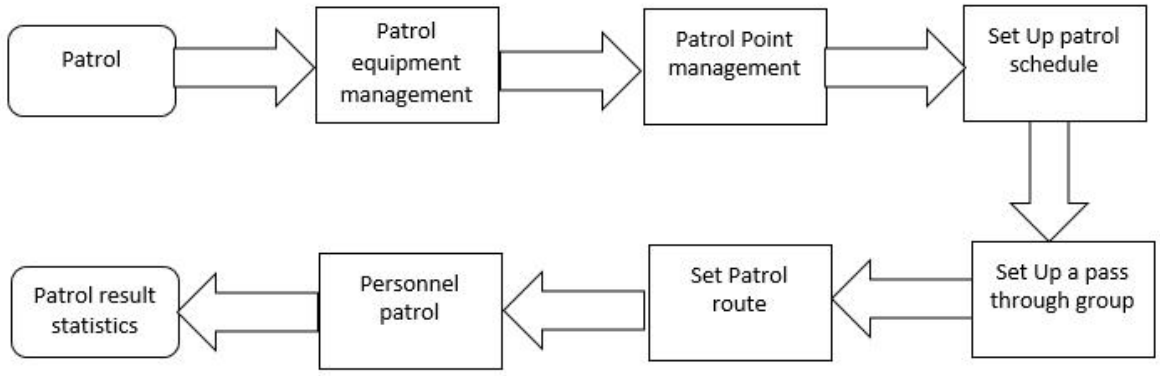


Figure 13- 1 Patrol Configuration Flow

13.3 Patrol Route Monitoring

13.3.1 Patrol Monitoring

Displays all the scheduled routes in the patrol plan on the same day. When the patrol personnel patrol normally as planned, the patrol points in the corresponding patrol routes will turn green; If you don't patrol according to the rules, the patrol point will turn red. This interface is shown in the patrol monitoring interface, as shown in figure below. Refer to Table 13-1 for status description.

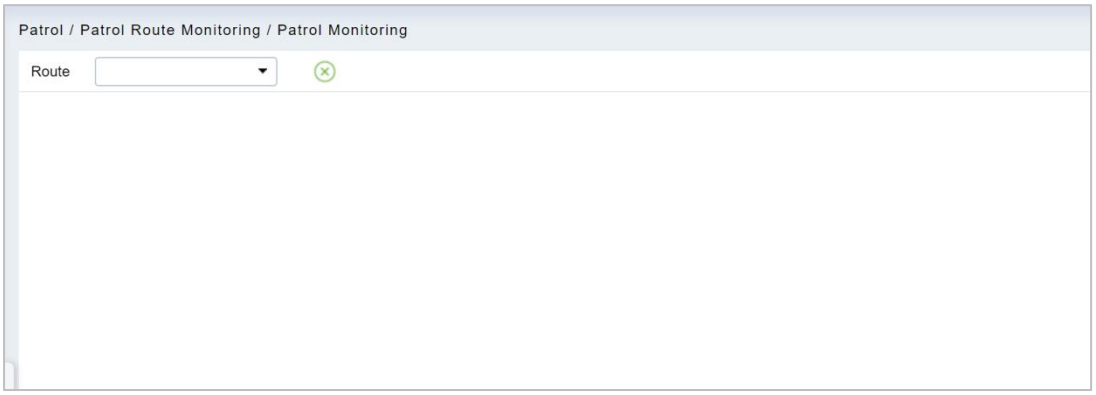


Figure 13- 2 Patrol Monitoring

Parameter	Description
Normal Patrol	Personnel complete patrol in a normal time period according to normal sequence rules.
Wrong Patrol	The personnel completed the patrol within the normal time period but did not follow the regular route.
Leakage Patrol	The personnel did not complete the patrol within the normal time period, that is, one or part of the patrol points did not patrol.
Absence	Personnel has not completed the patrol within the normal time period, that is, the whole patrol route has not completed one patrol.
	The patrol route is wrong/missed.
	Normal patrol.
	Not patrolling.

Table 13- 1 Patrol Status Description

13.4 Patrol Basic Management

13.4.1 Device

13.4.1.1 Add device (New)

Select a device to be used as the patrol device from the access control devices. Click **Basic Management** > **Device** > **New**. In the **Alternative** box, add available devices and click **OK** to save the setting. The page is displayed as follows:

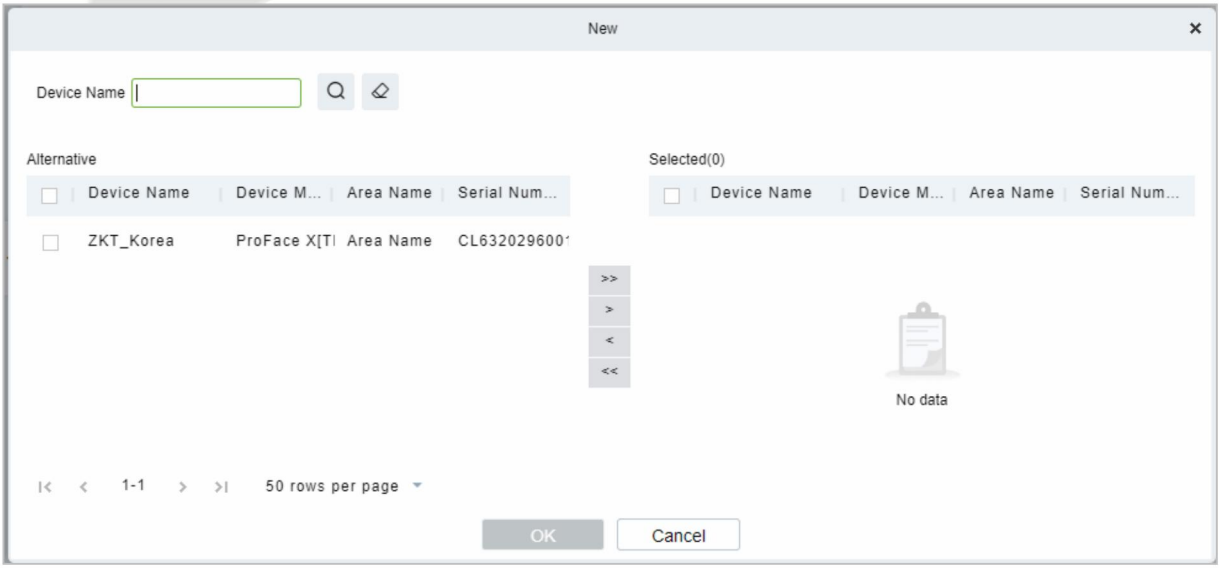


Figure 13- 3 Add Device (New)

●Precondition:

Before the patrol operation, it is necessary to add patrol device in the **Access Control** module and patrol personnel in the **Personnel** module.

Parameters	Instructions
Device Name	Customize the name of this device
Serial Number	Customize the device serial number.
Area Name	Divide the area for the device.
Device Model	Manufacturer of the device.

Table 13- 2 Access Control

13.4.1.2Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol group

13.4.1.3Edit

Click a device name or Edit in the operation column to go to the Edit page. Make modifications and click OK to save modifications.

13.4.2Checkpoint

13.4.2.1Add Checkpoint (New)

Step 1: Click **Basic Management** > **Checkpoint** > **New**. The page is displayed as follows:

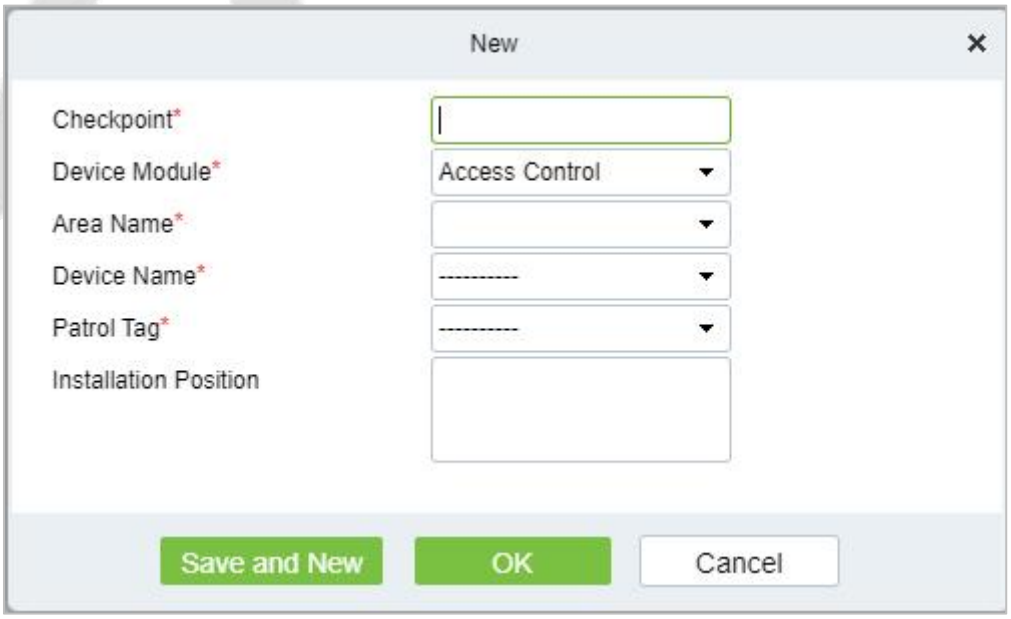


Figure 13- 4 New Checkpoint

Step 2: After the setting (parameters with * are mandatory), click **OK** to save the setting. You can also click **Save and New** to save the current setting and add another checkpoint. Click **Cancel** to cancel the setting and return to the upper-level menu.

Parameters	Description
Checkpoint	Unique name which can identify a route.
Device Module	Displays the device number.
Area Name	It can support typing anything alphabet but can't typing the common.
Device Name	Manufacturer of the device.
Patrol Tag	Currently, only access control readers are supported
Installation Position	Set a suitable name for the position. Any character, maximum combination of 100 characters. Position names should not be repeated.
Operations	The patrol operation, it is necessary to add patrol device in the Access Control module.

Table 13- 3 New Checkpoint

13.4.2.2Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the checkpoint

13.4.2.3Edit

Click a device name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

✍**Note:** Patrol tags that have been used by checkpoints cannot be used again when you add another checkpoint.

13.4.3Parameters

Step 1: Click **Patrol** > **Basic Management** > **Parameters**.

Step 2: Set the interval for patrol statistics collection.

Step3: Click **OK** to save the setting.

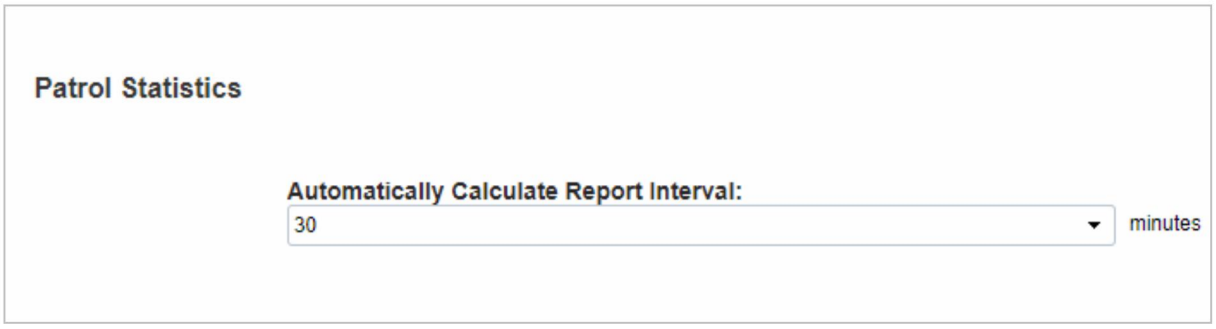


Figure 13- 5 Parameters

13.5 Patrol Management

13.5.1 Plan

13.5.1.1 Add Plan (New)

● Operating Steps:

Step 1: In the Patrol module, select "**Patrol Management > Patrol Plan**" and click New.

Step 2: In the **New** window that pops up, configure the patrol plan information, as shown in figure below, and describe the key parameters as shown in Table 13-4.

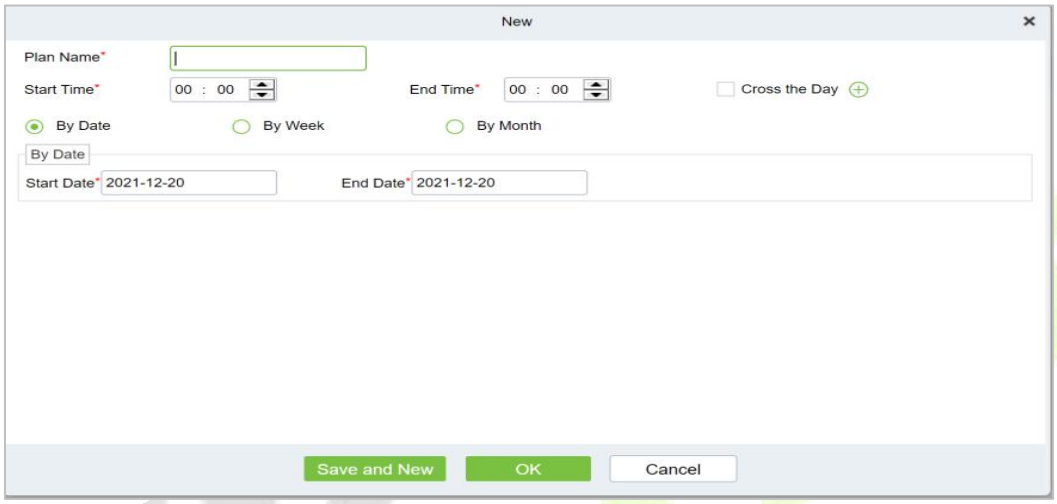


Figure 13- 6 Patrol Plan

Parameter	Instructions
Time Period	You can set the time to be set in a day, or you can set it across days.
By Date	The patrol plan is scheduled daily. Check by Date to set the start date and end date of the patrol plan.
By Week	The patrol plan is scheduled on a weekly basis.
By Month	The patrol plan is scheduled monthly. There are two ways to implement the monthly plan: daily implementation or regular implementation. Choose the patrol plan to perform the patrol task every day in the selected month; If you choose to perform regularly, you will perform the patrol task within the specified date in the month.

Table 13- 4 Parameter Setting Description

Step 3: Click **OK**.

Parameter	Instructions
Plan Name	Customize the Plan Name.

Cycle Type	Customize the Cycle Type.
Plan	A maximum of three patrol shifts can be added for a patrol plan.
Time Zone	This abnormal event is triggered if a user with the floor opening right punches his/her card beyond the effective periods
Operations	The patrol operation, it is necessary to add patrol device in the **Access Control** module.

Table 13- 5 Parameter Setting

13.5.2Patrol Group

13.5.2.1Add Patrol Group (New)

● Operating Steps:

Step 1: In the Patrol module, select "**Patrol Management > Patrol Group**" and click New.

Step 2: In the pop-up **New** window, configure the patrol personnel group information, as shown in figure below.

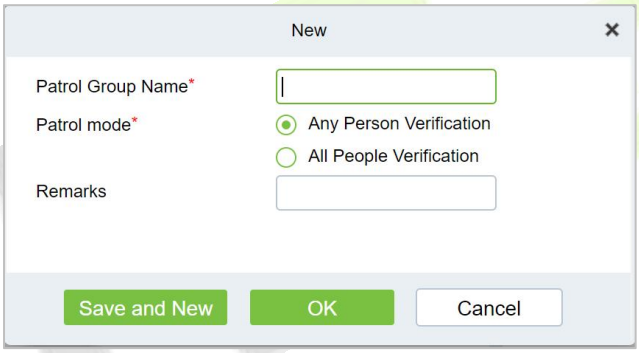


Figure 13- 7 Patrol Personnel Group

Step 3: Click **OK**.

Step 4: Under the operation of the patrol group interface, click "**Add Personnel**".

Step 5: In the **Add Person** window that pops up, configure the person information, as shown in figure below.

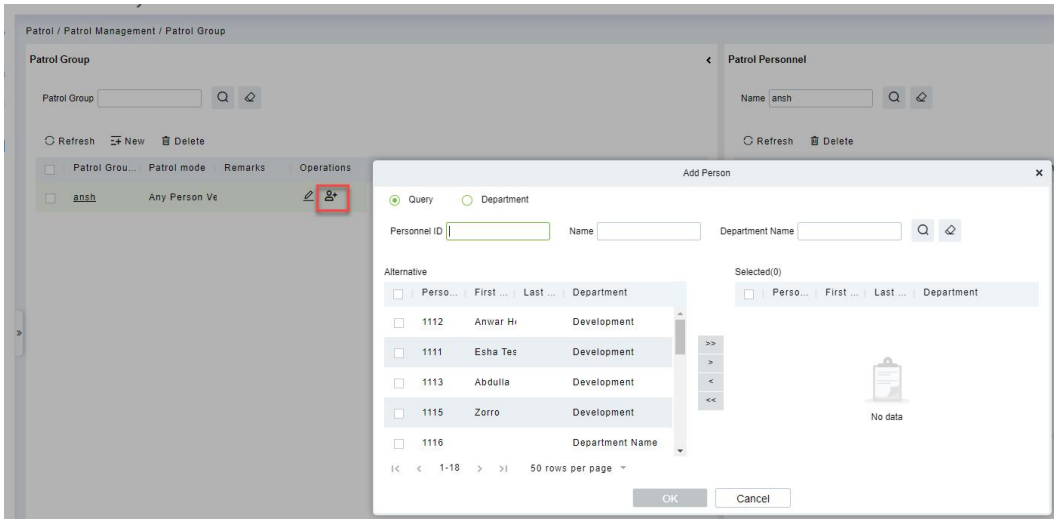


Figure 13- 8 Adding Patrol Team Personnel

Step 6: Click **OK**.

13.5.2.2Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol group.

Parameters	Instructions
Patrol Group	Click a patrol group from the list on the left. Personnel in the patrol group are displayed in the list on the right.
Patrol Mode	A patrol group cannot be edited or deleted when it is used by a patrol route.
Remarks	Custom Setting Notes Description.
Operations	The patrol operation, it is necessary to add patrol device in the **Access Control** module.
Personnel ID	Click **Add Personnel** under Operation in the list on the left. The page for adding personnel is displayed (or adding by department). Add personnel to the list on the right and click **OK** to finish the setting.
First Name/ Last Name	The maximum length cannot exceed 50, does not support comma; value sources Personnel field, cannot add, modify, delete.
Department Name	Select from the pull-down menu and click **OK**. If the department was not set previously, only one department named **Company Name** will appear.

Table 13- 6 Delete Personnel

13.5.3Route

13.5.3.1Add Route (New)

● Operating Steps:

Step 1: In the Patrol module, select "**Patrol Management > Patrol Route**" and click Add.

Step 2: In the pop-up **Add** window, configure the patrol route information as shown in Figure 12-9 and figure below, and describe the key parameters as shown in Table 13-7.

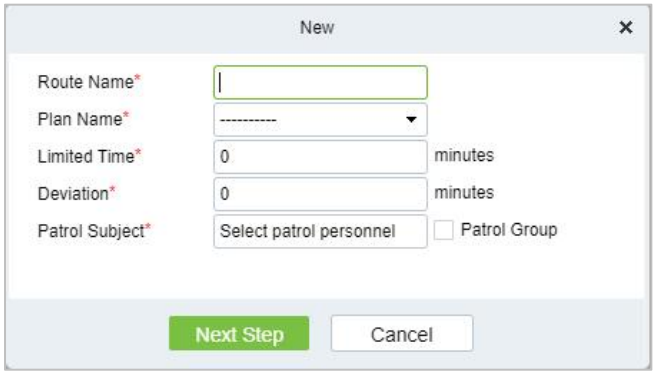


Figure 13- 9 The First Step of The Patrol Route

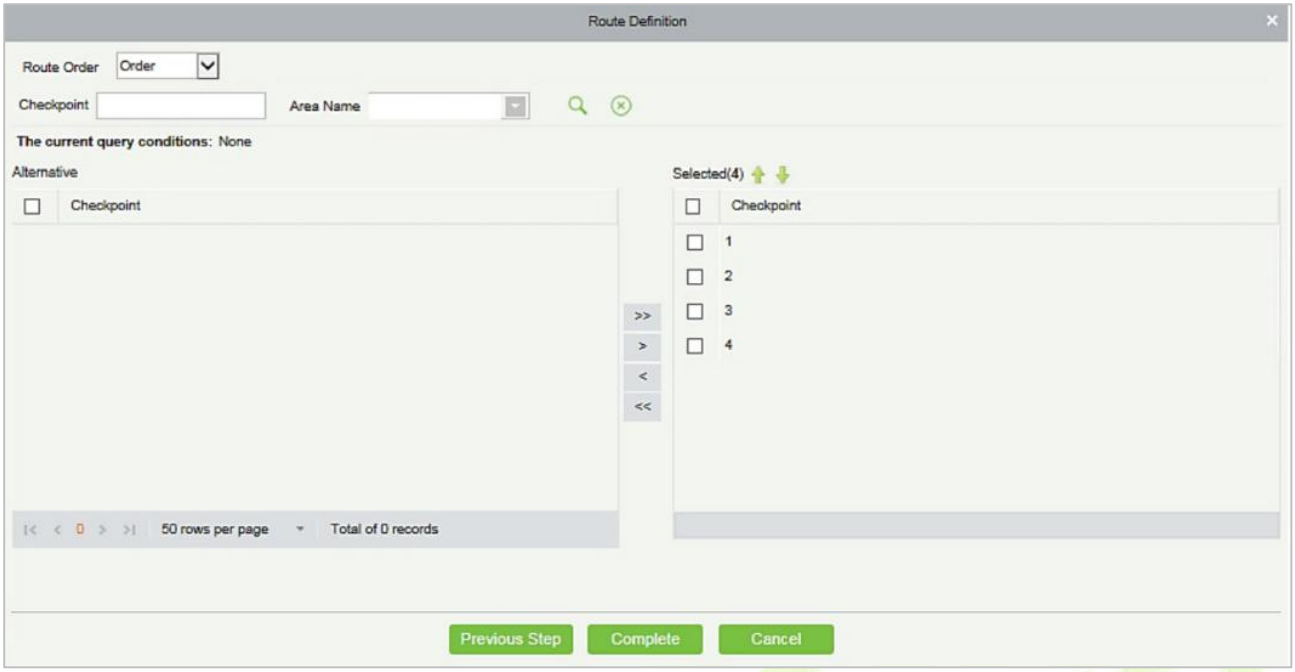


Figure 13- 10 The Second Step of The Patrol Route

Parameters	Instructions
Route Name	**Customize the Route Name.**
Plan Name	**Customize the plan Name.**
Patrol Subject	**Select the patrol personnel.**
Checkpoint Order	**In the patrol route, all checkpoints are 2 types of order and disorder routes.**
Limited Time	**Set up the desired Limited Time.**
Deviation	**Set up the required Deviation Time.**
Route Status	**Displays the route status.**
Sort Type	**Fill in the number of the superior department.**
Operations	**The patrol operation, it is necessary to add patrol route in the Access Control module.**

Table 13- 7 Second Step of Patrol Route

13.5.3.2Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol route.

13.5.3.3Enable/ Disable

Select device, click **Enable/Disable** to stop/start using the device. When communication between the

device and the system is interrupted or device fails, the device may automatically appear in disabled status. After adjusting local network or device, click **Enable** to reconnect the device and restore device communication.

Parameter	How to set
Error	Allowable error time setting for patrol. Assuming that the patrol plan is not 9:00-12:00, and the allowable error time is 5 minutes before and after, then the records in the period of 8:55-12:05 are valid records, and those beyond the above range are invalid records, which will not be counted. As long as the patrol is not within the above time range, it is invalid.
Orderly Route	When carrying out the patrol plan, there is no time limit between the patrol points, and the patrol personnel can complete the patrol work of each patrol point in sequence according to their own habits within the limited time of the route.
Unordered Route	• Complete disorder: There is no order in all patrol points of the patrol route, and the patrol personnel can complete the patrol work of each patrol point within the total time limit according to their own habits. • Disorder outside the first point: in the patrol route, other patrol points except the designated patrol starting point are disordered. • Disorder outside the tail point: in the patrol route, other patrol points except for the last patrol point of the designated patrol route are disordered. • Disorder outside the beginning and end points: In the patrol route, except for the first and last patrol points in the designated patrol route, other patrol points are out of order.

Table 13- 8 Parameter Setting Description

13.6 Patrol Reports

In the patrol report, you can query the "All Records", "Patrol Records Today's", "Patrol Route Statistics" and "Patrol Personnel Statistics" report. You can choose to export all or export records after querying.

This part introduces the configuration Steps of report query and export, taking the "all records" report operation as an example.

13.6.1 All Transactions

Click **Reports** > **All transactions** to view all transactions, that is, all event records generated by the patrol device.

You can export all transactions into an Excel, PDF, or CSV file. See the following figure.

● Operating Steps:

Step 1: In the Patrol module, select **Report > All Records**.

Step 2: In the All Records interface, fill in the corresponding query information and click the **Query** symbol to complete the query of all record tables, as shown in figure below.

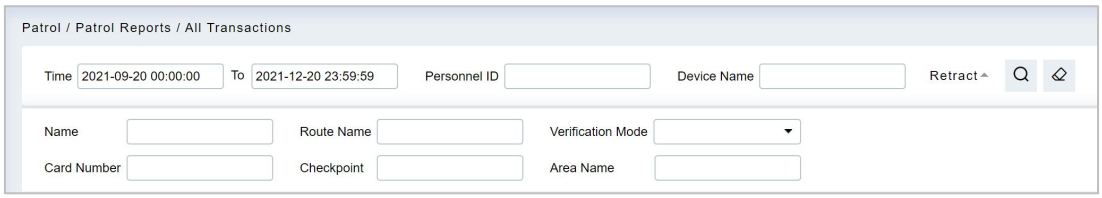


Figure 13- 11 All Records

Step 3: In the full record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in figure below.

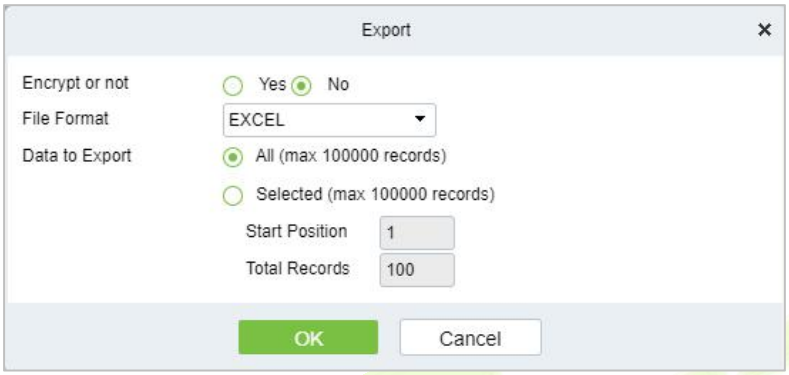
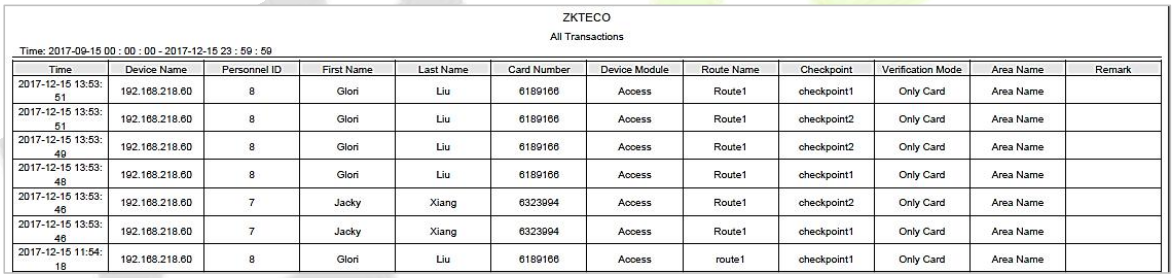


Figure 13- 12 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.



ZKTECO

All Transactions

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Time	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
2017-12-15 13:53:51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:49	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:48	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:18	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint1	Only Card	Area Name	

Figure 13- 13 Report Export File

Parameters	Instructions
Time	Set the start and end time in each time interval. Time period includes one week and three holiday-type time intervals.
Personnel ID	Displays the Personnel ID number.
Device Name	Manufacturer of the device.
Name	Select the desired name.
Route Name	Displays the Route name.
Verification Mode	You can set verification mode as following options: Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.

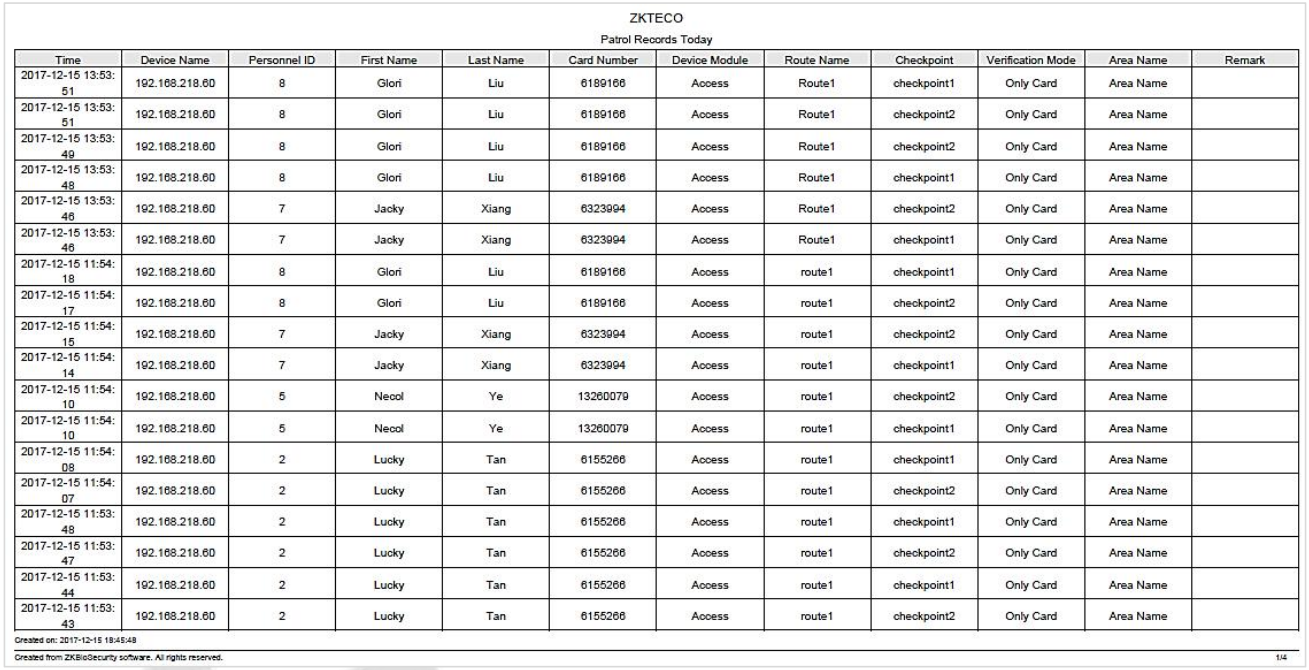
Card Number	The max length is 10, and it should not be repeated.
Checkpoint	Displays the Type of checkpoint.
Area Name	Customize the Area name.

Table 13- 9 Report Export File

13.6.2Patrol Records Today

Click **Reports** > **Patrol Records Today** to view event records generated by the patrol device today.

You can export patrol records today into an Excel, PDF, or CSV file. See the following figure.



ZKTECO

Patrol Records Today

Time	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
2017-12-15 13:53:51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:49	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:48	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:18	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:17	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:15	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:14	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:08	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:07	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:48	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:47	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:44	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:43	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	

Created on: 2017-12-15 18:45:48

Created from ZKBioSecurity software. All rights reserved. 1/4

Figure 13- 14 Patrol Records Today

Parameters	Description
Personnel ID	Displays the Personnel ID number.
Card Number	Displays the Card Number.
Name	Select the required Name.
Device	Manufacturer of the device.
Verification Mode	Displays the Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.
Route Name	Displays the Route name.
Checkpoint	Displays the Type of checkpoint.

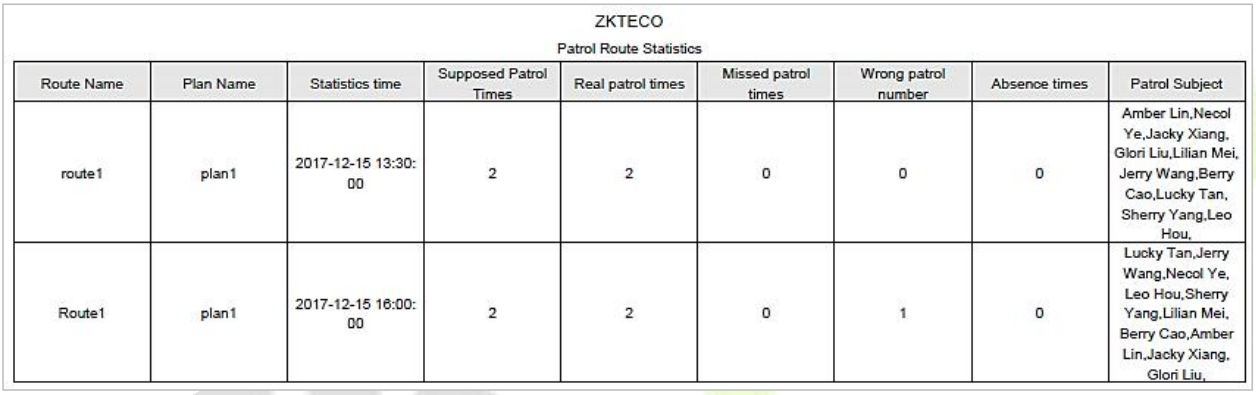
Area Name	Customize the Area name.
Time	Set the start and end time in each time interval. Time period includes one week and three holiday type time intervals.
Remarks	Custom Setting Notes Description.

Table 13- 10 Patrol Record Today

13.6.3Patrol Route Statistics

Click **Reports** > **Patrol Route Statistics** to view all normal and abnormal situations collected during the patrol process.

You can export patrol route statistics into an Excel, PDF, or CSV file. See the following figure.



ZKTECO

Patrol Route Statistics

Route Name	Plan Name	Statistics time	Supposed Patrol Times	Real patrol times	Missed patrol times	Wrong patrol number	Absence times	Patrol Subject
route1	plan1	2017-12-15 13:30:00	2	2	0	0	0	Amber Lin,Necol Ye,Jacky Xiang, Glori Liu,Lilian Mei, Jerry Wang,Berry Cao,Lucky Tan, Sherry Yang,Leo Hou,
Route1	plan1	2017-12-15 16:00:00	2	2	0	1	0	Lucky Tan,Jerry Wang,Necol Ye, Leo Hou,Sherry Yang,Lilian Mei, Berry Cao,Amber Lin,Jacky Xiang, Glori Liu,

Figure 13- 15 Patrol Route Statistics

Parameters	Description
Route Name	Displays the required route name.
Plan Name	Displays the type of plan name.
Statistics time	Displays the Time and date of patrol route statistics.
Supposed Patrol Times	Number of times that the patrol personnel should normally patrol.
Real Patrol Times	Number of times that the patrol personnel patrol
Wrong Patrol Times	Number of times that the patrol personnel do not patrol based on the patrol route.
Missed Patrol Times	Number of times that the patrol personnel miss one or more checkpoints in the patrol route within the patrol time.
Absence Times	Number of times that the patrol personnel do not patrol.

Table 13- 11 Patrol Route Statistics

13.6.4Patrol Personnel Statistics

Click **Reports** > **Patrol Personnel Statistics** to view patrol statistics of patrol personnel.

You can export patrol personnel statistics into an Excel file. See the following figure.

Patrol Personnel Statistics

Personnel ID	Person Name	Route Name	Plan Name	Statistics time	Supposed Patrol Times	Real patrol times	Missed patrol times	Wrong patrol number	Absence times
4	Berry Cao	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
3	Leo Hou	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
8	Glori Liu	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
2940	Sherry Yang	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
6	Amber Lin	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
5	Necol Ye	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
7	Jacky Xiang	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
6	Amber Lin	Route1	plan1	2017-12-15 16:00:00	2	2	0	0	0
4	Berry Cao	Route1	plan1	2017-12-15 16:00:00	2	2	0	0	0
1	Jerry Wang	Route1	plan1	2017-12-15 16:00:00	2	2	0	0	0
9	Lilian Mei	Route1	plan1	2017-12-15 16:00:00	2	2	0	0	0
7	Jacky Xiang	Route1	plan1	2017-12-15 16:00:00	2	2	0	1	0

Figure 13- 16 Patrol Personnel Statistics

Parameters	Description
Supposed Patrol Times	Number of times that the patrol personnel should normally patrol.
Real Patrol Times	Number of times that the patrol personnel patrol
Wrong Patrol Times	Number of times that the patrol personnel do not patrol based on the patrol route.
Missed Patrol Times	Number of times that the patrol personnel miss one or more checkpoints in the patrol route within the patrol time.
Absence Times	Number of times that the patrol personnel do not patrol.

Table 13- 12 Patrol Personnel Statistics

14 Entrance Control

14.1 Operation Scenario

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

14.2 Operation Flow

Introduce the configuration process of channel service.

The channel business configuration process is shown in figure below.

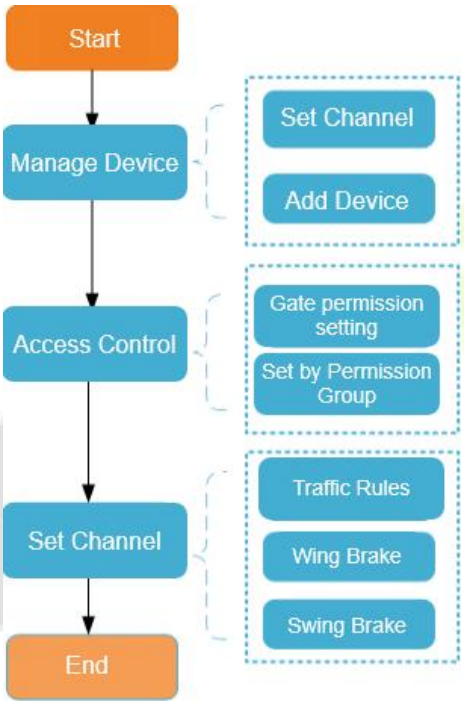


Figure 14- 1 Channel Configuration Flow

14.3 Baffle Gate

Add channel integrated machine Device, and the integrated machine communicates with the gate control board through RS485 to control the gate

14.3.1 Passage

Setting the area to which the channel belongs is convenient for users to manage the channel Device in a specific area. After setting the channel, the Device under the channel can be filtered according to the area during real-time monitoring.

This part introduces the Steps of creating and configuring channels in ZKBio CVSecurity.

14.3.1.1 To Add Passage (New)

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Device > Passage**.

Step 2: In the channel interface, click **New** and fill in the relevant parameters, as shown in figure below. Please refer to Table 14-1 for parameter description.

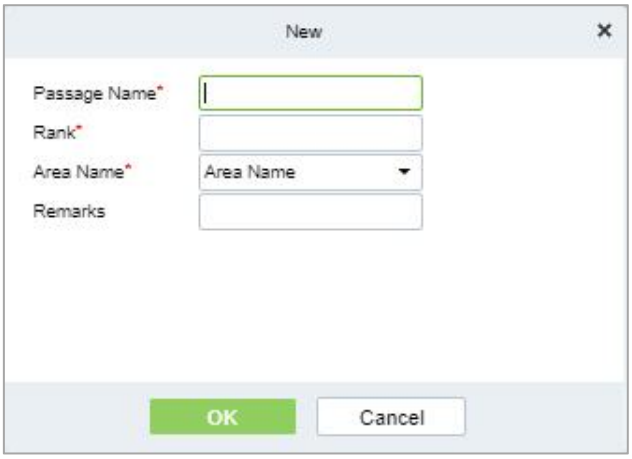


Figure 14- 2 New Channel Interface

Parameter	How to set
Passage Name	Any character, a combination of up to 20 characters, cannot be repeated.
Rank	Only numbers are supported, up to six digits, and repeatable. The smaller the ranking, in real-time monitoring, the display will move forward.
Area Name	Select the region to which the channel belongs.
Remarks	Any character with a maximum character length of 100.

Table 14- 1 Description of New Channel Parameters

Step 3: Click **OK** to complete the channel setting.

14.3.1.2Delete Passage

●Operation Steps:

Step 1: In the **Entrance Control module**, select **Channel Device > Passage** and select the template to be deleted.

Step 2: Click **Delete** to delete the selected template. Click **OK** to perform the delete operation

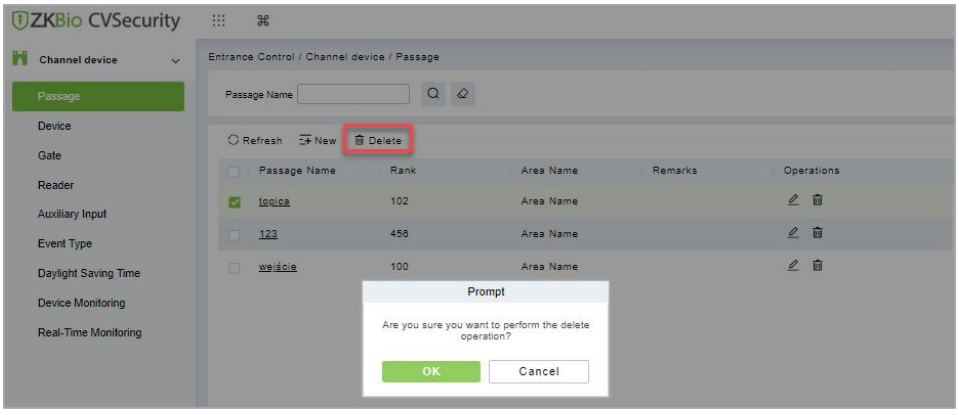


Figure 14- 3 To Delete Passage

14.3.2Device

14.3.2.1Searching for Additional Channel Devices (Search)

Introduces the configuration Steps of searching for additional channel devices in ZKBio CVSecurity.

● Precondition:

1. Set up IP allocation before adding channel devices.
2. Before searching and adding the device, it is necessary to set the address pointing to the server in advance and set the IP address and port of the current server, that is, the IP address and port installed by the current.

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Device > Devices**.

Step 2: In the device interface, click "**Search**" to pop up the search box.

Step 3: Click **Search** in the search box to display the channel devices that can be added, as shown in figure below.

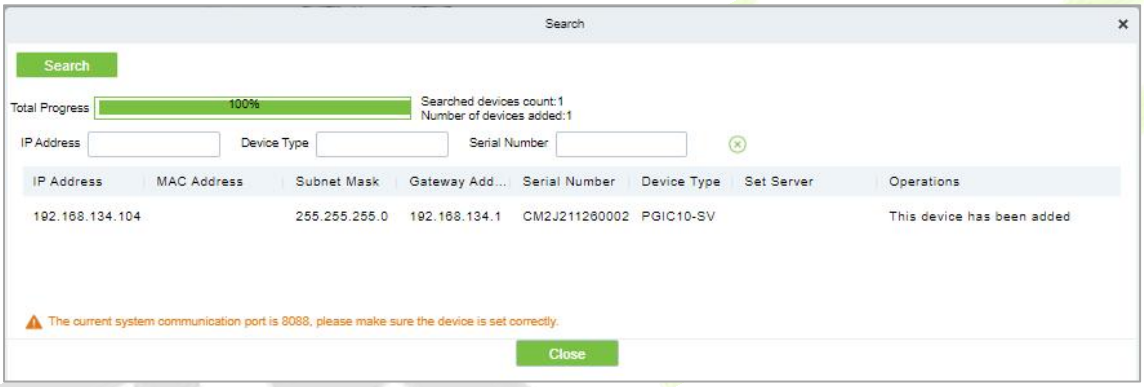


Figure 14- 4 Device Search Interface

Step 4: For the channel Device found, click the **Add** button in the operation bar to **Add** the device, and fill in the parameters of device addition, as shown in figure below. Please refer to Table 14-2 for parameter description.

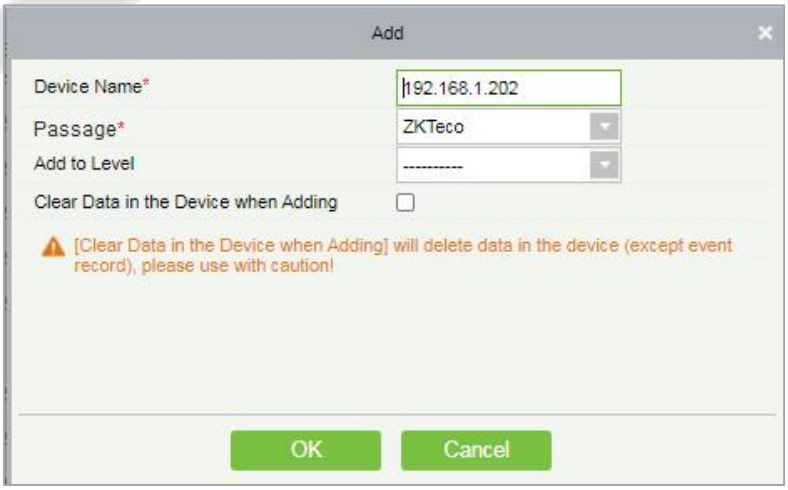


Figure 14- 5 Device Addition Interface

Parameter	Description
Device Name	Any character, a combination of up to 20 characters, cannot be repeated.

Channel	Select the channel to which the device belongs.
Add to Permission Group	Automatically adds the device to the selected permission group.
Delete Data in Device When Adding	When the device is added, the data in the device except the event record is deleted.

Table 14- 2 Description of Device Addition Parameters

Step 5: Click **OK** to complete the addition of channel device.

14.3.2.2Delete

●Operation Steps:

Step 1: In the Entrance Control, click **Channel Device > Device** and select device to be deleted.

Step 2: Click **Delete** to delete the device.

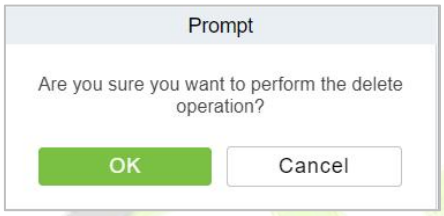


Figure 14- 6 Delete Device

Step 3: Click **OK** to perform the delete operation.

14.3.2.3Control

In this option admin can upgrade firmware and LCD screen firmware. Also, this option helps to reboot the device, enable and disable the devices, and synchronize time and all data.

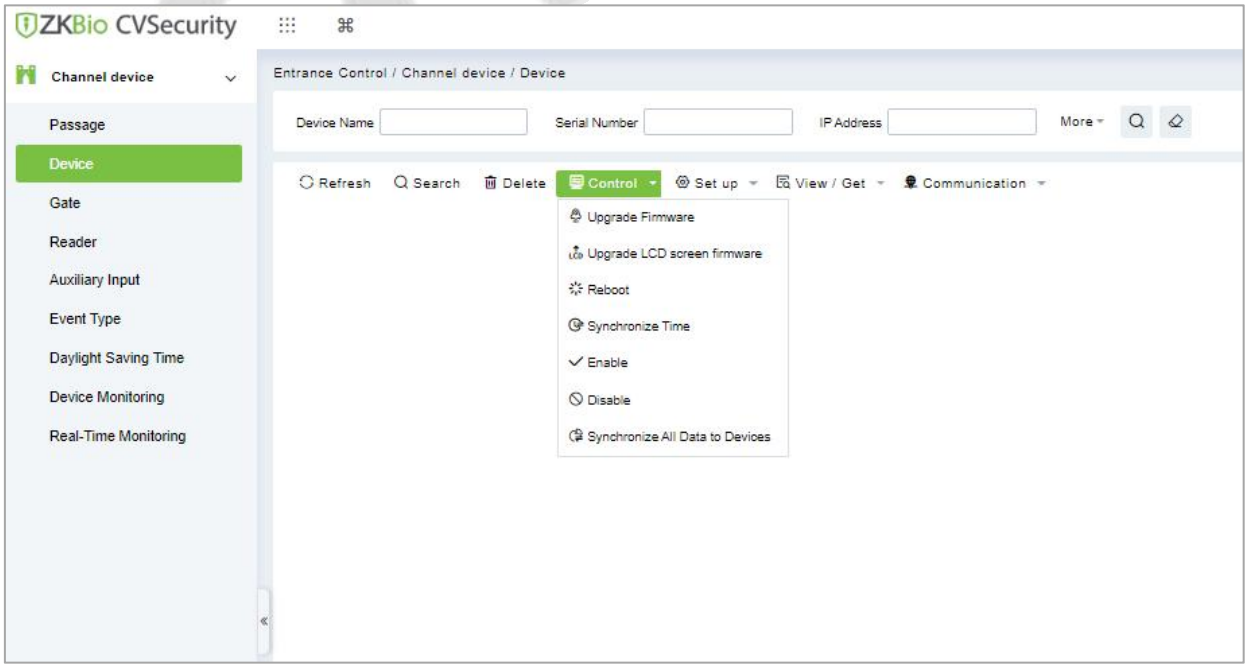


Figure 14- 7 Device Control Interface

Upgrade Firmware

Select the device to be upgraded and click **Upgrade Firmware** to open the setting page. Click **Browse**,

select the firmware upgrade file (file name is emfw.cfg). Click **Start** to start upgrading the firmware.

Notes:

Please be cautious while upgrading the firmware. If the firmware has not been updated properly, it may lead to device failure. If you have any queries, please contact the representative or pre-sales technical support team.

Upgrade LCD Screen Firmware

Admin can upgrade LCD screen firmware of device using this option. Select the device to be upgraded and click **Upgrade LCD Screen Firmware** to open the settings page. Click **Browse** and select the firmware upgrade file. Click **Start** to start upgrading the firmware.

Reboot the Device

Admin can send a restart command to the device to automatically restart. Select the device to be reboot and click **Reboot** to restart the device.

Synchronize Time

When the device's time is not accurate, select the device to be synchronized and then click **Synchronize Time** to synchronize the server time to the device.

Disable/Enable

Select the device and click **Disable/Enable** to stop/start using the device. When communication between the device and the system is interrupted or there is a problem with the device, the device may be automatically displayed as disabled. After adjusting the network or device, click **Enable**. The system reconnects to the device, and the communication status of the device is restored.

Synchronize All Data to Devices

This option synchronizes the data in the system to the device. Select the device, click **Synchronize All Data to Devices**, and click the **Synchronize** button to synchronize data:

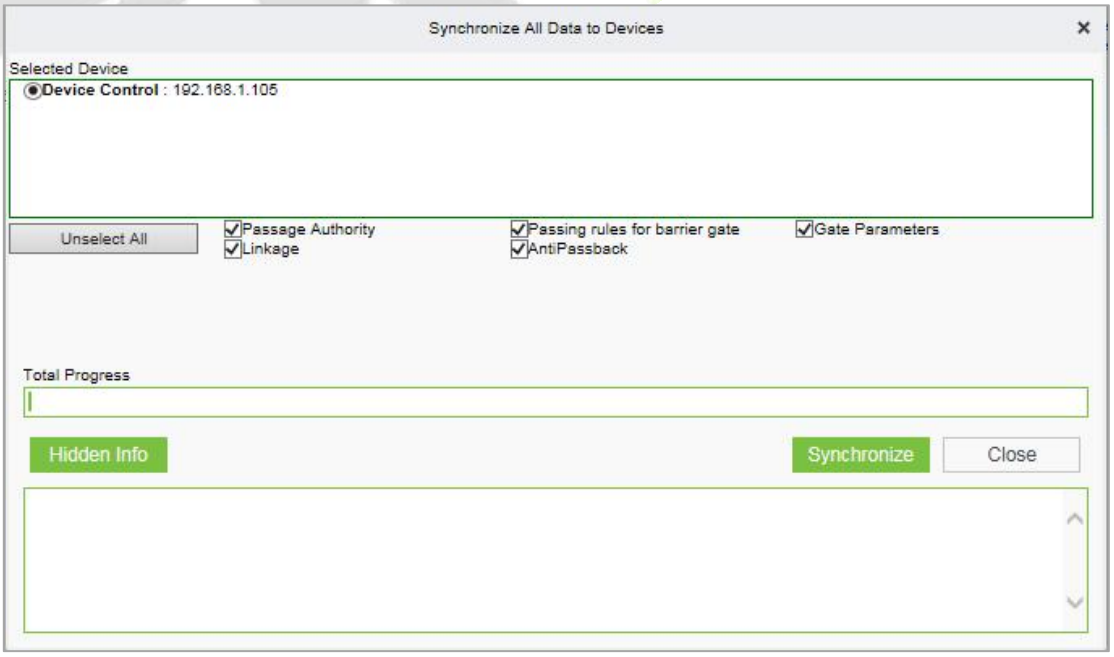


Figure 14- 8 Synchronize All Data to Devices Interface

Notes:

The operation of synchronizing all data will first delete the existing data in the device (excluding event records) and then download all the setting information again. When performing this operation, please try to ensure that the network is unblocked and avoid power failure. When the device is running

normally, please use this operation with caution. It is recommended to synchronize the data when the device is unused.

14.3.2.4Set up

In this interface help you to set the time zone, registration, daylight saving time, fingerprint identification information and LCD screen display of the selected device.

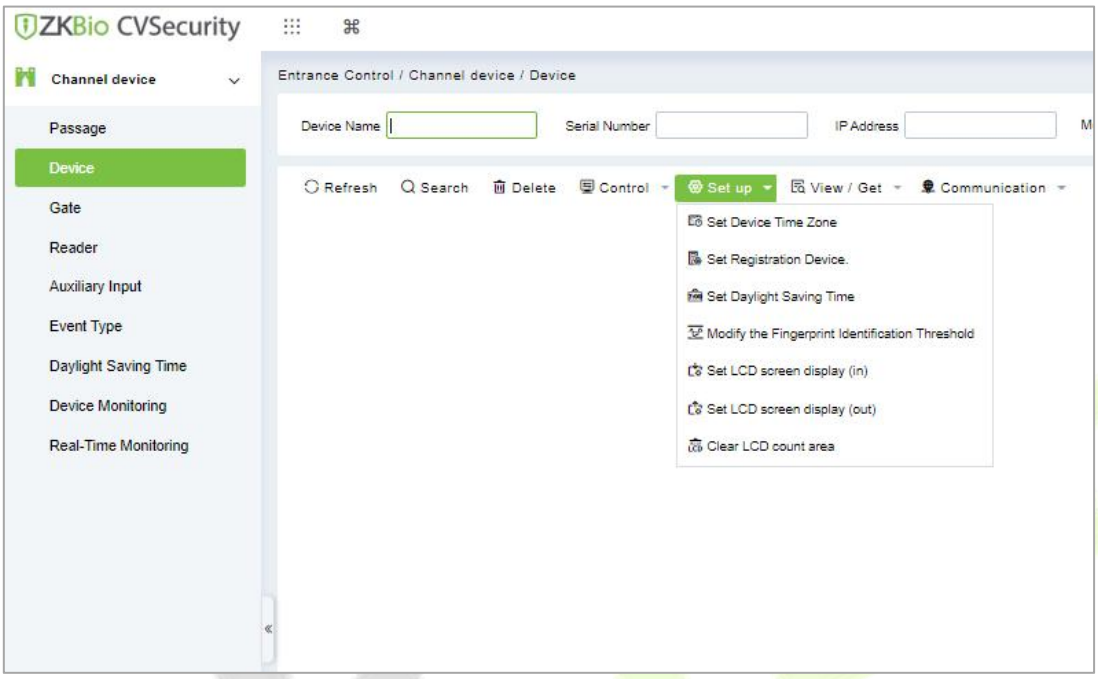


Figure 14- 9 Set up Options

Set Device Time Zone

Set Device Time Zone allows you to set the accurate time zone, if device shows wrong time zone. For that in **Entrance Control** interface, click **Channel Device > Device > Set-up**, select the device to be set up. Then click **Set Device Time Zone** to set up the selected device.

Set Registration Device

The passage standalone device can only automatically upload the personnel and other data entered by the device when the registration device is set. For that in **Entrance Control** interface, click **Channel Device > Device > Set-up,** select the device to be set up. Then click **Set Registration Device** to set up the selected device.

Set Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

In the **Entrance Control** interface, click **Channel Device > Device > Set-up** and select the device to be set Daylight Saving Time. Then click **Set Daylight Saving Time** to set up the selected device.

Modify the Fingerprint Identification Threshold

The user can modify the fingerprint comparison threshold in the device, ranging from 35 to 70, and the factory default value is 55. When a new device is added, the system will read the value from the device, and the user can view the current fingerprint comparison threshold size through the device list (Please make sure the device supports the fingerprint function).

In the **Entrance Control** interface, click **Channel Device > Device > Set-up** and select the device to be

modify the fingerprint identification. Then click **Modify the Fingerprint Identification Threshold** to set up the selected device.

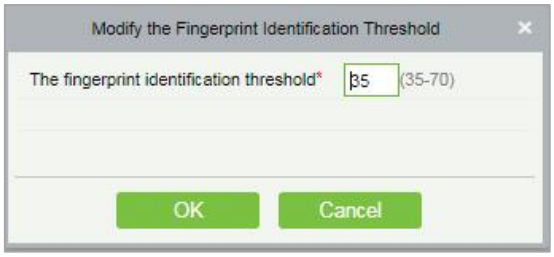


Figure 14- 10 Modify the finger Identification Option

Set LCD Screen Display (In)/(Out)

Select the device and set the LCD screen display (in/out). The upper part is the video area 30%, the middle part is the gate channel display area 30%, and the lower part is the picture cycle 40%. Each area can be corresponding to the video and background, The image browsing and clearing operations are confirmed and sent to the LCD screen of the controller for display.

In the **Entrance Control** interface, click **Channel Device > Device > Set-up** and select the device to be set LCD screen display. Then click **Set LCD Screen Display (In)/(Out)** to set up the selected device.

Clear the LCD Counting Area

Select the device, clear the middle counting area of the LCD screen, and restart counting.

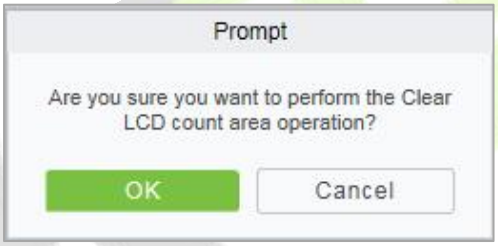


Figure 14- 11 Clear LCD Counting Area

In the Entrance Control interface, click **Channel Device > Device > Set-up** and select the device to clear the LCD counting area. Then click **Clear the LCD Counting Area** to clear counting area the selected device.

14.3.2.5View/ Get

In this interface admin can view device options, personal information and transaction details

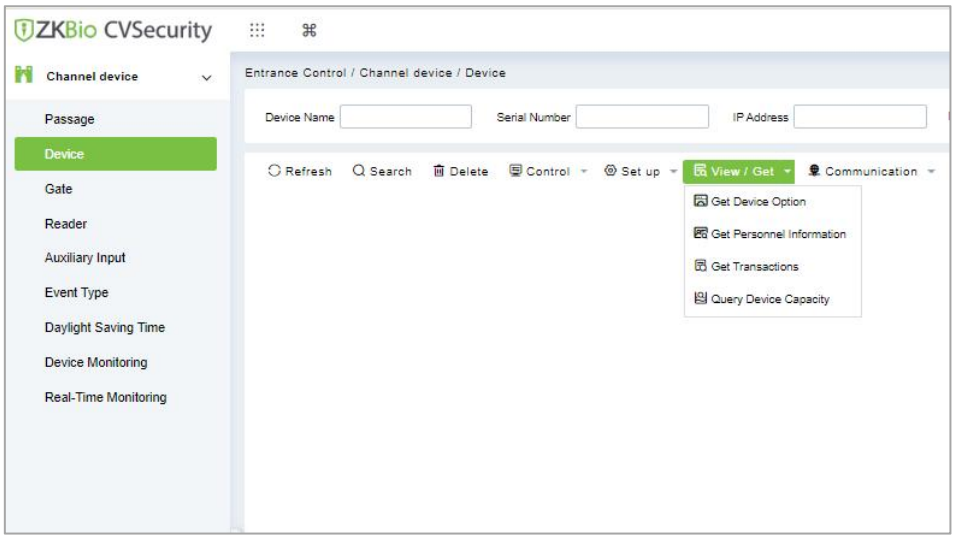


Figure 14- 12 View/Get Option

Get Device Option

This option allows you to view the common parameters of the device. For example, get the firmware version after the device is updated.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view device options. Then select **Get Device Option** to view device options.

Get Personnel Information

This function obtains the data of Persons, Fingerprints, and Palm prints in the device or obtains the corresponding number.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view personnel information. Then select **Get Personnel Information** to view personnel information.

Get Transaction

This function obtains the event records in the device to the system, and the user can choose to obtain new records or all the records.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to get transaction. Then select **Get Transaction** to view transaction information.

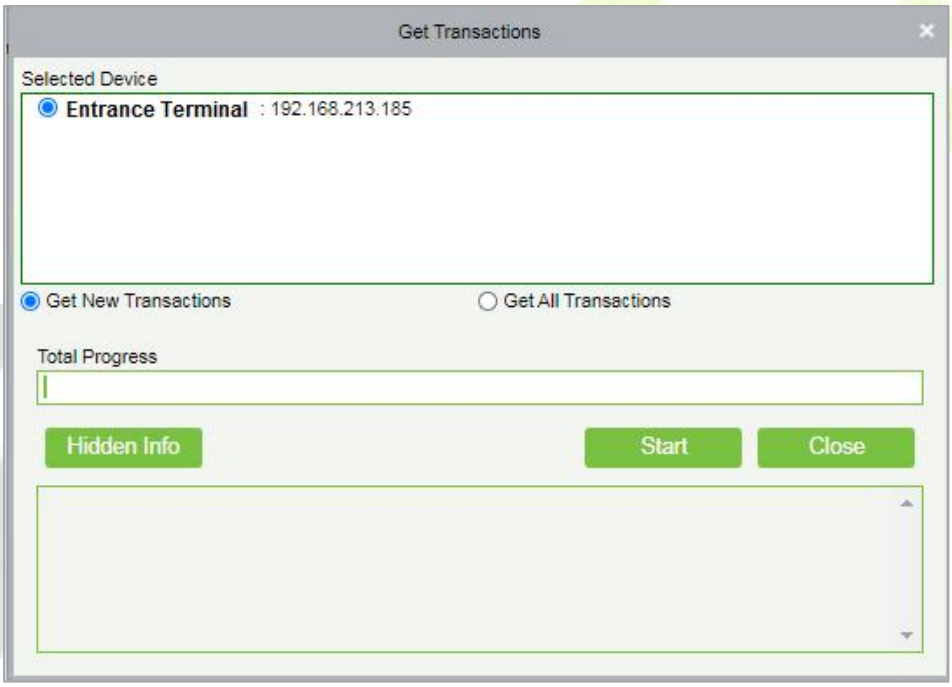


Figure 14- 13 Get Transactions

When the network is in good condition and the communication between the system and the device is normal, the system will obtain the event record in the device in real-time and saves it in the database. When the communication is interrupted, the event record in the device is not uploaded to the system in real-time. At this time, the user can perform this operation to manually obtain the event records in the device.

Query Device Capacity

Here, the user can view the capacity information of the device in the software and manually obtain the usage information (person, fingerprint, finger vein, face, imprint) in the device. When the user finds that the information obtained from the software and the device is inconsistent, the user can manually synchronize the data.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view the capacity information of the device. Then select **Query Device Capacity** to view the user can view the capacity information of the device in the software and manually obtain the usage information.

14.3.2.6Communication

In the **Entrance Control** interface, click **Channel Device > Device > Communication** to modify IP address and communication password.

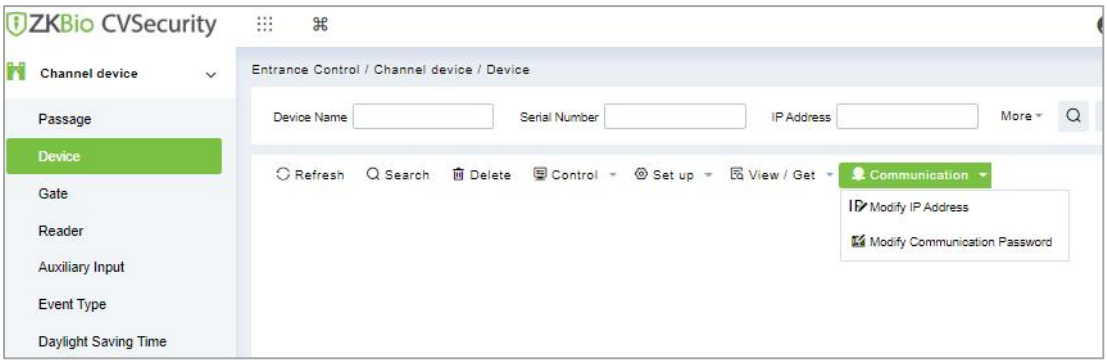


Figure 14- 14 Communication Option

Modify IP Address

Select a device and click **Modify IP address** to open the modification interface. It will obtain a real-time network gateway and subnet mask from the device. (Failed to do so, you cannot modify the IP address). Then enter a new IP address, gateway, and subnet mask. Click **OK** to save and quit. This function is the similar as Modify IP Address Function in Device.

Modify Communication Password

Select a device and click **Modify Communication Password** to open the modification interface The system will ask for the old communication password before modifying it. After verification, input the new password twice, and click **OK** to modify the communication password.

Note: Communication passwords shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password settings can improve the device's security. It is recommended to set communication passwords for each device.

14.3.3Baffle Gate

In the Entrance Control module, select Channel Device > Gate.

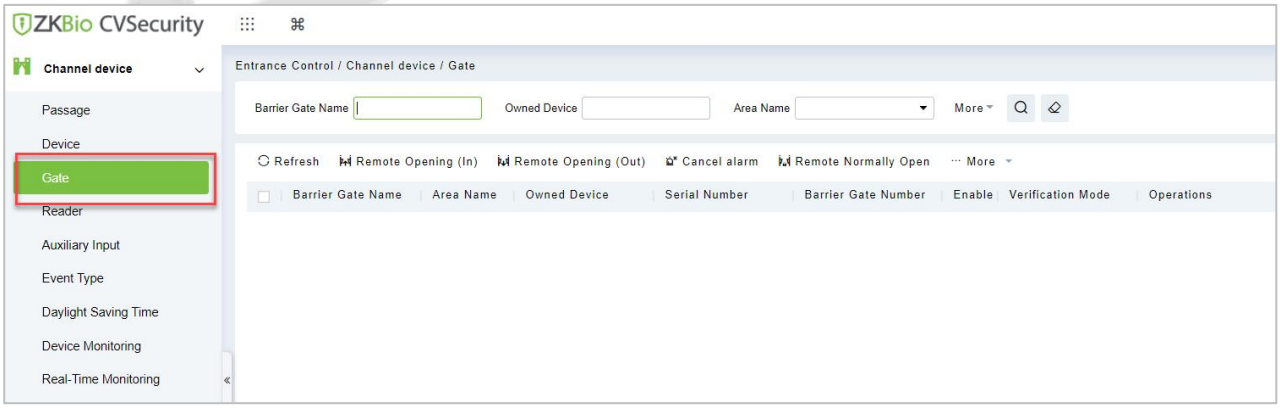


Figure 14- 15 Channel Device Gate

14.3.3.1Remote Gate Opening (in)/(out)

In the **Entrance Control** interface, click **Channel Device > Gate** interface allows the user to control one gate or all gates. To control a single gate right-click over it and click **Remote Opening (In/Out)** in the pop-up dialog box. To control all gates, directly click **Remote Opening (In/Out)** behind Current All.

14.3.3.2Cancel the Alarm

Once an alarm door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for a single gate or all gates.

In the **Entrance Control** interface, click **Channel Device > Gate** and select the alarm gate to be modified. Then click **Cancel the Alarm** to cancel the alarm**.**

Note: If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

14.3.3.3Remote Normally Open

It will set the gate as normal open by remote.

In the **Entrance Control** interface, click **Channel Device > Gate** and select the gate to be set as normal open. Then click **Remote Normal Open** to set the gate as normal open by remote**.**

14.3.3.4More Options

In the **Entrance Control** interface, click **Channel Device > Gate >More** to activate the door lockdown status (remote lock and unlock).

Remote Lock:

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

Remote Unlock:

It will unlock a locked door. This function is supported only by certain devices.

Enable / Disable Intraday Passage Mode Time Zone

In remote opening, user can define the door opening duration (The default is 15s). You can select **Enable Intraday Passage Mode Time Zone** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select **Disable Intraday Passage Mode Time Zone** first, to avoid enabling other normal open time zones to open the door, and then select **Remote Closing**.

14.3.4Reader

Each Entry device has a reader, user can view the reader information in this interface.

● Operating Steps

Click **Entrance Control** > **Channel Device > Reader** to view the reader information such as reader name, barrier gate name, bound camera and it in/out details.

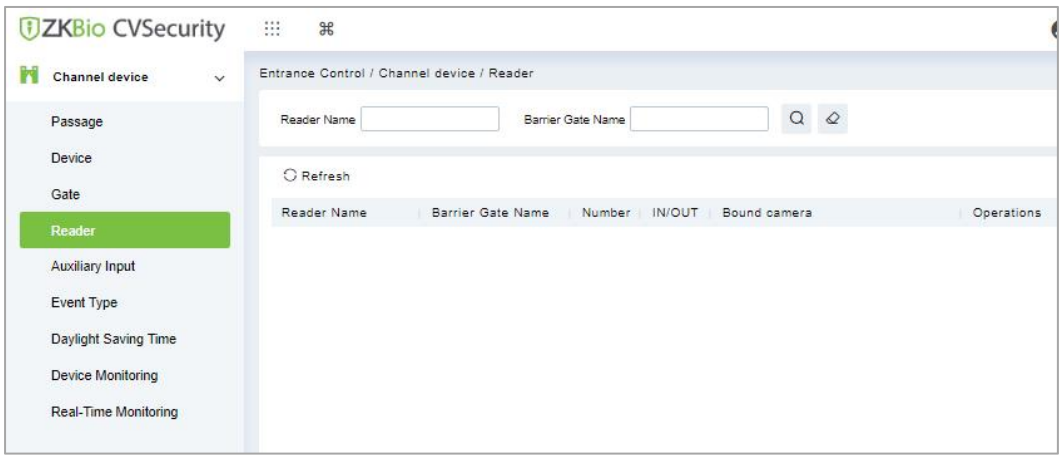


Figure 14- 16 Reader Interface

14.3.5Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

Click **Entrance Control** > **Channel Device >** Auxiliary Input, to access below shown interface.

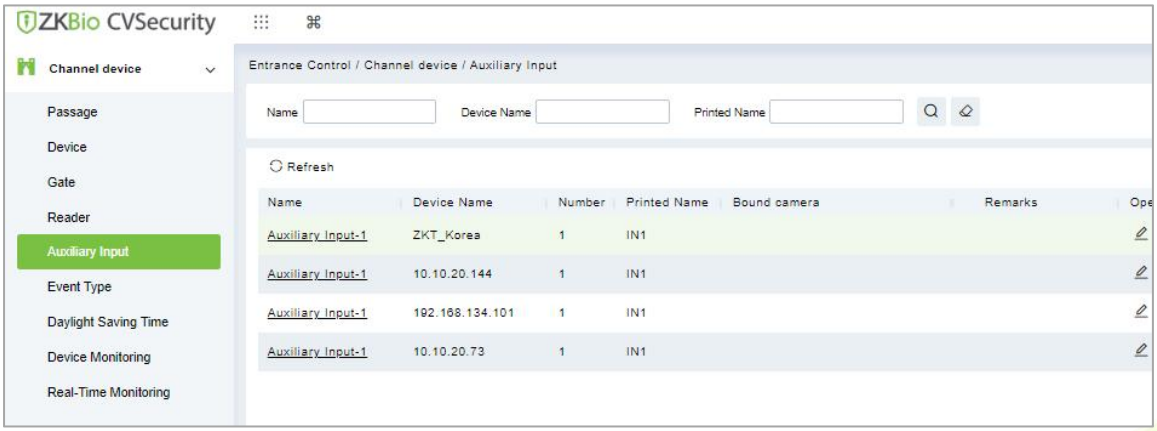


Figure 14- 17 Auxiliary input

Bind/Unbind Camera

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

Note: An auxiliary input point can bind more than one channel.

14.3.6Event Type

The Event Type is mainly used to display various event types included in the channel device. Click **Entrance Control** > **Channel Device > Event Type**, and the following interface appears

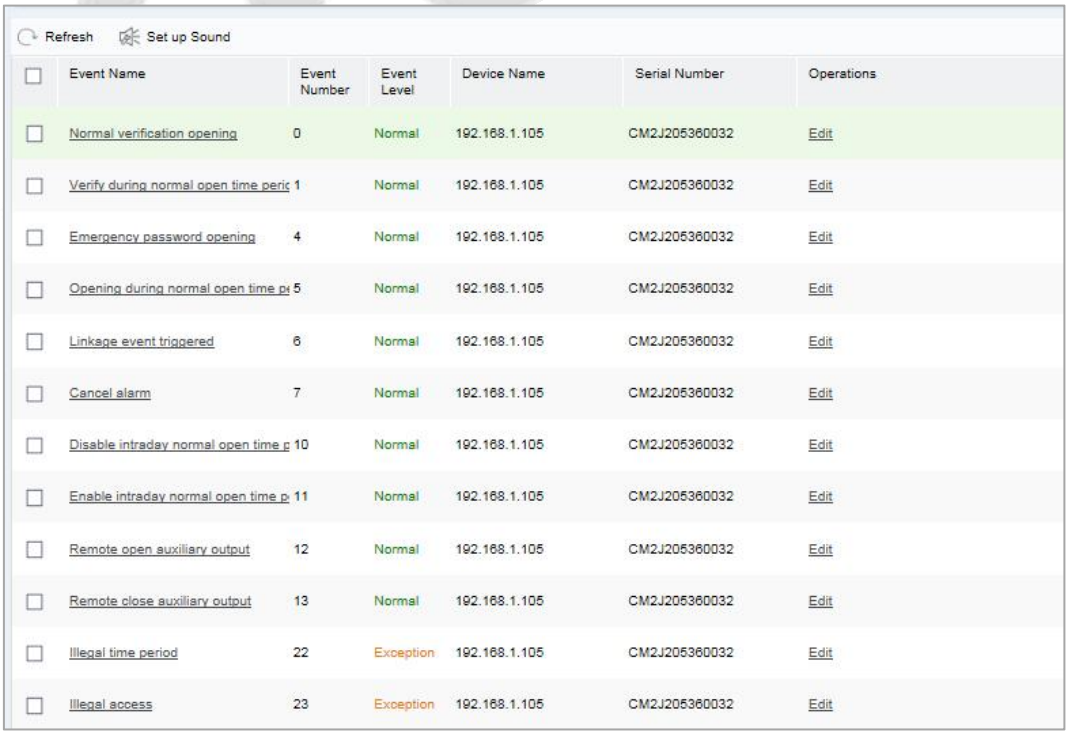


Figure 14- 18 Event Type

Set the sound

Here, the user can set the event sound. First, select the event to be set sound and then click **Set up Sound** on the page.

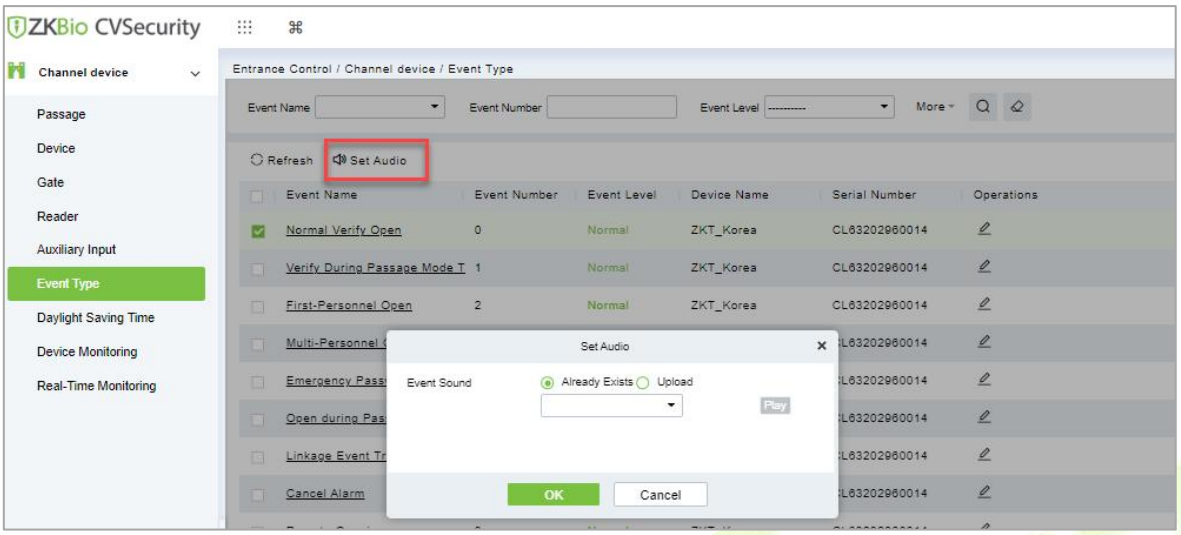


Figure 14- 19 Set Sound Option

The audio file can be uploaded locally. The file must be in wav or mp3 format, and the size cannot exceed 10MB.

14.3.7 Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. The regulations are different in different countries. At present, nearly 70 countries adopt DST.

To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

14.3.7.1 Add DST (New)

● Operation Steps:

Step 1: Click Entrance Control > Channel Device > Daylight saving Time > New.

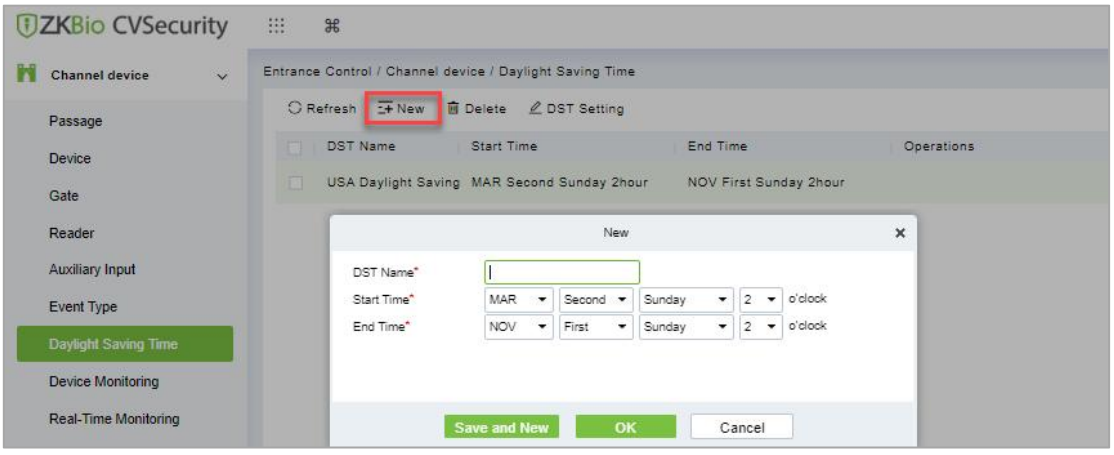


Figure 14- 20 Daylight Saving Mode

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as “second Monday in March, 02:00”. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Parameter	Description
DST Name	Any character, a combination of up to 20 characters, cannot be repeated.
Start and End Time	Enter the start and end time. Set as Month-Weeks-week hour: minute format.

Table 14- 3 Description of New DST Parameters

14.3.7.2Delete

● Operation Steps:

Step 1: Click **Entrance Control** > **Channel Device** > **Daylight saving Time** and select DST information to be delete.

Step 2: Click **Delete** and click **OK** to delete the DST.

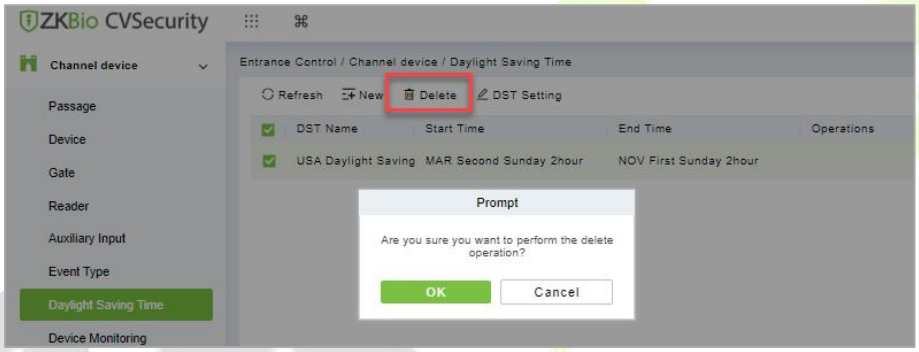


Figure 14- 21 Daylight Saving Mode Delete

14.3.7.3DST Setting

● Operation Steps:

Step 1: Click **Entrance Control** > **Channel Device** > **Daylight Saving Time** and select DST information to be modify.

Step 2: Click **DST Setting** and select device from the appeared window.

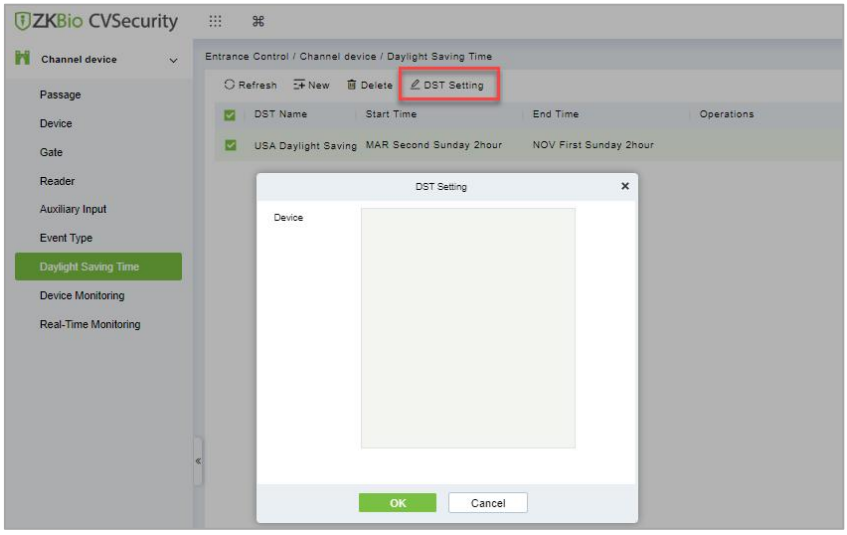


Figure 14- 22 DST Setting

Step 3: Click **OK** to save the settings.

14.3.8Real-Time monitoring

On the real-time management screen, the status of the added device is displayed, and the device can be opened or closed. At the same time, the dynamic of real-time events is monitored. If the gate opening can be verified and corresponding access control events can be generated, the access control management service configuration is complete.

14.3.8.1Remote Gate Opening (In)/(Out)

In the **Entrance Control** interface, click **Channel Device > Real Time Monitoring** interface allows the user to control one gate or all gates.

●Operation Steps:

Step 1: Check whether the device is online. Check whether the icon status of the added device is online. Click **Barrier Gate** to check and modify the real-time status of the added devices

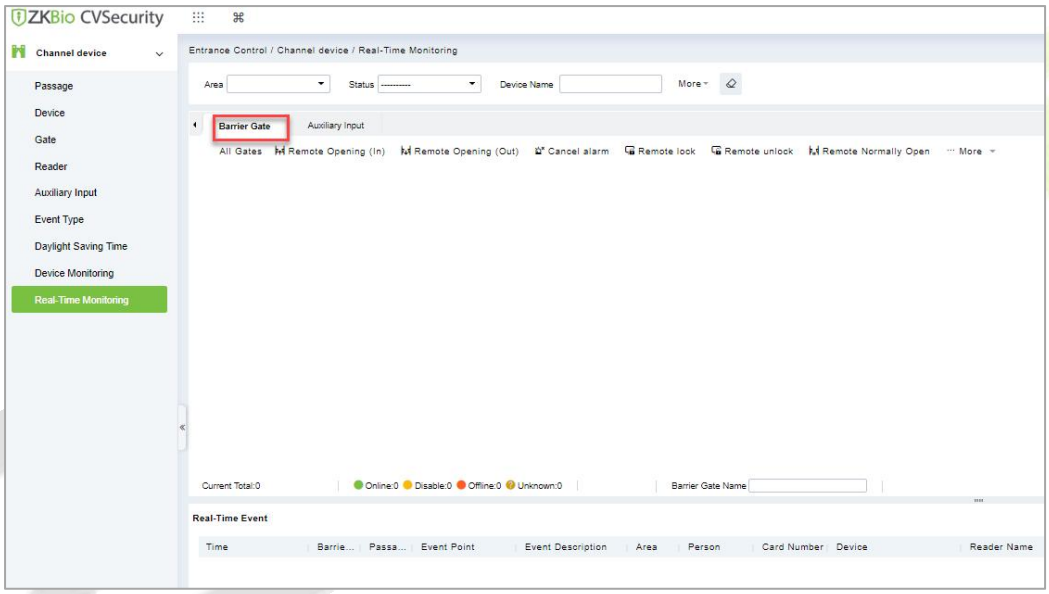


Figure 14- 26 Barrier Gate Option in Real-Time Monitoring Interface

Step 2: Remote opening in/out verification, taking remote opening in as an example. Select the online barrier gate device, click **Remote opening in**, enter the user password in the pop-up security verification, and click **OK**.

On the remote door opening screen, enter the time to open the door and tap **OK**. If Operation succeeded in is displayed, the remote door opening Operation is complete.

14.3.8.2Cancel the Alarm

In the **Entrance Control** interface, click **Channel Device > Real Time Monitoring** interface and select the alarm gate to be modified. Then click **Cancel the Alarm** to cancel the alarm**.**

Note: If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

14.3.8.3Remote Lock

In the **Entrance Control** interface, click Channel Device > Real-Time Monitoring and select the barrier to modify the lock status Then click Remote Lock to activate the door lockdown status (remote lock and unlock).

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

14.3.8.4Remote Unlock

In the **Entrance Control** interface, click **Channel Device > Real-Time Monitoring** and select the barrier to modify the lock status Then click **Remote Unlock** to activate the door lockdown status (remote lock and unlock).

It will unlock a locked door. This function is supported only by certain devices.

● Auxiliary Input:

In this interface, the user can identify real-time connected sensor devices such as infrared sensors or smog sensors.

To view the list of real-time connected devices, click **Entrance Control > Channel Device > Real-Time Monitoring** and select **Auxiliary Inputs**.、

14.4 Entrance Control

By setting the gate authority group and assigning it to the corresponding personnel, the gate authority of the personnel can be controlled. At the same time, it is also possible to set the response rules to the gate through Anti-Passback and linkage, to meet the requirements of different entry and exit scenarios.

14.4.1Baffle Gate Permission Group

Gates added to the system should be set in the form of permission groups. Set the corresponding permission group, add gates to the permission group, and define the area where the permission group belongs.

14.4.1.1To Add Gate Permission (New)

● Operating Steps:

Step 1: In the **Entrance Control** module, select **Entrance Control** > **Barrier Gate Permission Group**. In the barrier gate permission group interface, click **New** in the left column of the mouse to pop up the gate permission group adding interface.

Step 2: In the **New** interface of gate permission group, set the corresponding content according to the new requirements, as shown in figure below. Please refer to Table 14-4 for parameter filling instructions.

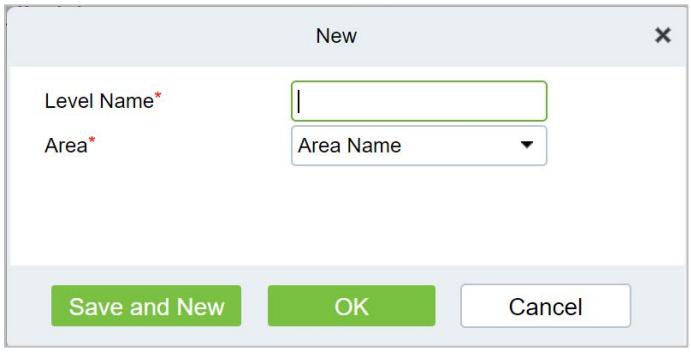


Figure 14- 27 Add Gate Permission Group Interface

Parameter	How to set
Level Name	Any character, consisting of up to 30 characters, cannot be repeated.
area	Permission groups belong to a zone to which users assigned permissions can manage permission groups under the zone.

Table 14- 4 Description of Added Gate Permission Parameters

Step 3: Click **OK** to complete the configuration of the access control authority group.

Step 4: In the gate permission group interface, click **Add Barrier Gate** icon on the right side of the created gate permission group, and the interface of selecting Add Gate will pop up, and the corresponding gate will be added according to the requirements, as shown in figure below.

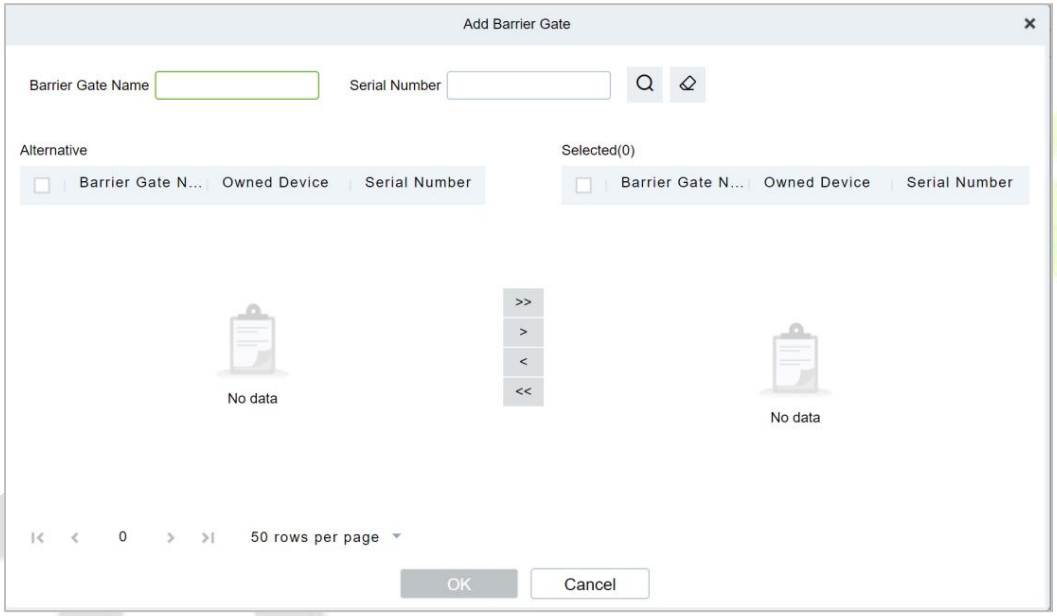


Figure 14- 28 Adding Gate Interface

Step 5: Click **OK** to complete the setting of gate permissions.

14.4.1.2Delete

● Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Barrier Gate Permission Group** and select gate permission group to be delete.

Step 2: Click **Delete** and click **OK** to delete gate permission group.

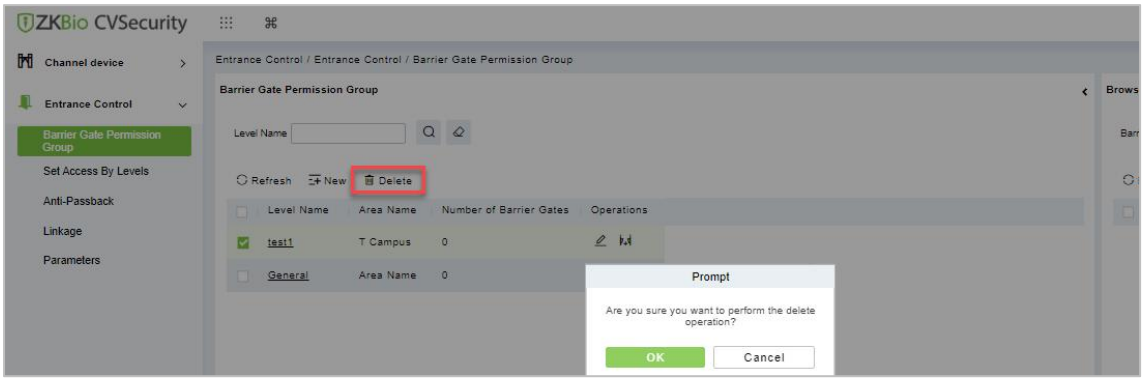


Figure 14- 29 Deleting Gate Interface

14.4.1.3Delete Barrier Gate

● Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Barrier Gate Permission Group** and select barrier gate name to be delete.

Step 2: Click **Delete** and click **OK** to delete barrier gate from the group.

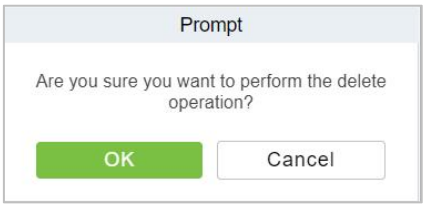


Figure 14- 30 Delete Barrier Gate

14.4.1.4Export

You can export barrier gate details into an Excel, PDF, or CSV file. See the following figure below.

● Operating Steps:

Step 1: In **Entrance Control** > **Entrance Control** > **Barrier Gate Permission Group** > **Export** to export the barrier gate records to Excel sheet or PDF or CSV. Enter the User password in the prompt.

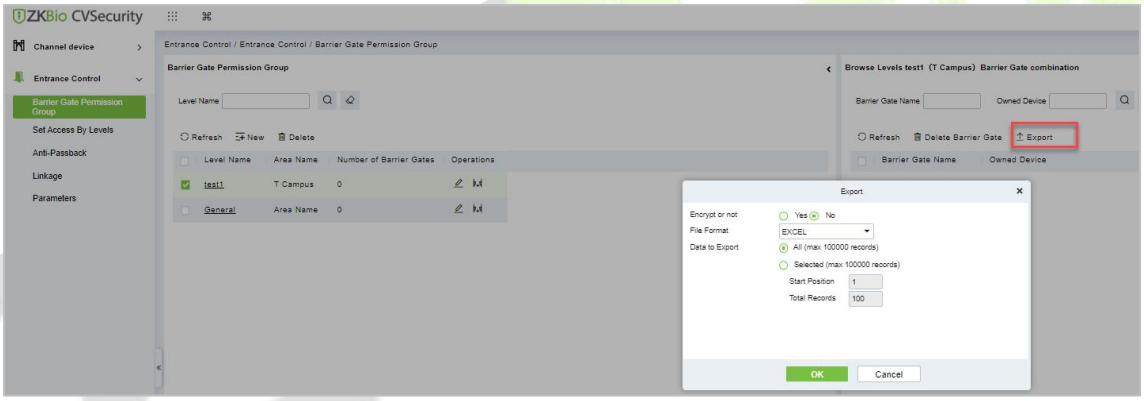


Figure 14- 31 Export Interface

Step 2: Select the file format and click **OK**.

14.4.2Set Access by Levels

Assign the added gate permission group to the person.

Introduces the operation Steps of allocating personnel authority according to authority group in ZKBio CVSecurity.

14.4.2.1Add Person

● Operating Steps:

Step 1: In the Entrance Control module, click **Entrance Control** > **Set Access By Levels**.

Step 2: Click **Add Person** icon in the operation bar of the corresponding permission group to open the interface of adding person. Select the corresponding person as needed, as shown in figure below.

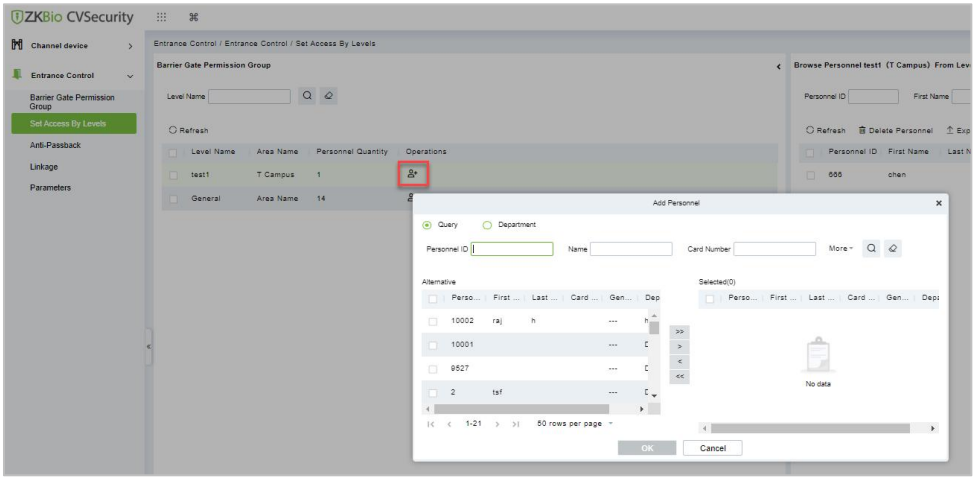


Figure 14- 32 Add Person Option

Step 3: Click **OK** to complete the assignment of personnel permissions.

14.4.2.2Delete Personnel

●Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Set Access By Levels** and select person to be delete.

Step 2: Click **Delete Personnel** and click **OK** to delete barrier gate from the group.

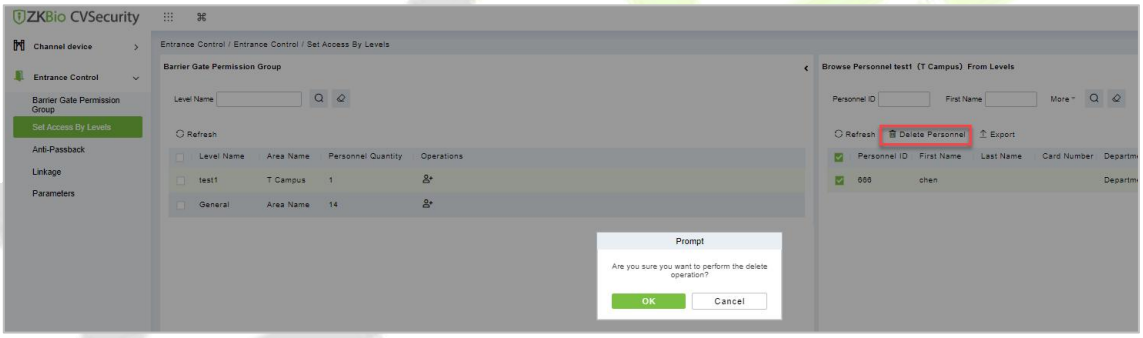


Figure 14- 33 Delete Person

14.4.2.3Export

You can export barrier gate details into an Excel, PDF, or CSV file. See the following figure below.

●Operating Steps:

Step 1: In **Entrance Control** > **Entrance Control** > **Set Access by Levels** > **Export** to export the persons records to Excel sheet or PDF or CSV. Enter the User password in the prompt.

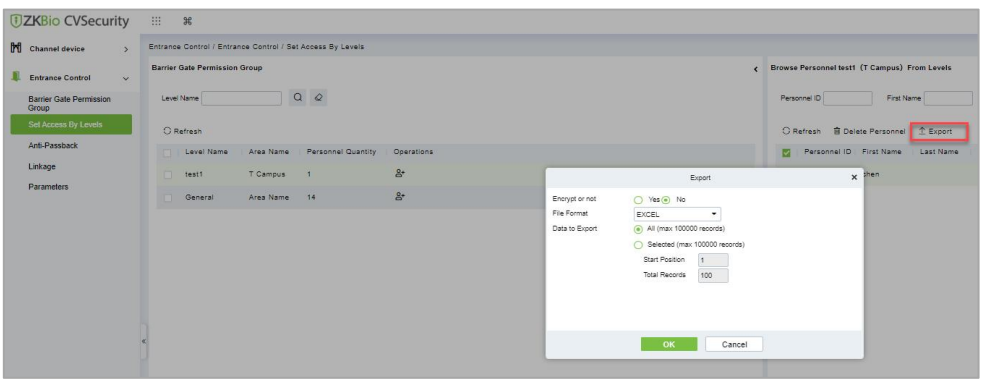


Figure 14- 34 Export Interface

Step 2: Select the file format and click **OK**.

14.4.3Anti-Passback

At present, it supports Anti-Passback in and out. On some occasions, people who require card swiping verification must swipe their cards from another channel when they come in from one channel, and the card swiping records must be strictly corresponding to one entry and one exit. Users can use this function when they enable it in settings, which is generally used in special units, scientific research, bank vaults and other occasions.

14.4.3.1To Add Anti-Passback

This part introduces the configuration Steps of adding Anti-Passback effect in.

●Operating Steps:

Step 1: In the Entrance Control module, select **Entrance Control** > **Anti-Passback** and Click New.

Step 2: Select the specified device.

Description:

When adding Anti-Passback, you can't see the device that has been set up in Anti-Passback in the device list. After deleting the set Anti-Passback information, the device returns to the device list.

Anti-Passback settings of all-in-one machine: Anti-Passback, Anti-Passback and Anti-Passback.

Step 3: Select the Anti-Passback rule and click **OK** to complete the setting, as shown figure below. The newly added Anti-Passback settings are displayed in the list of selected Anti-Passback rules.

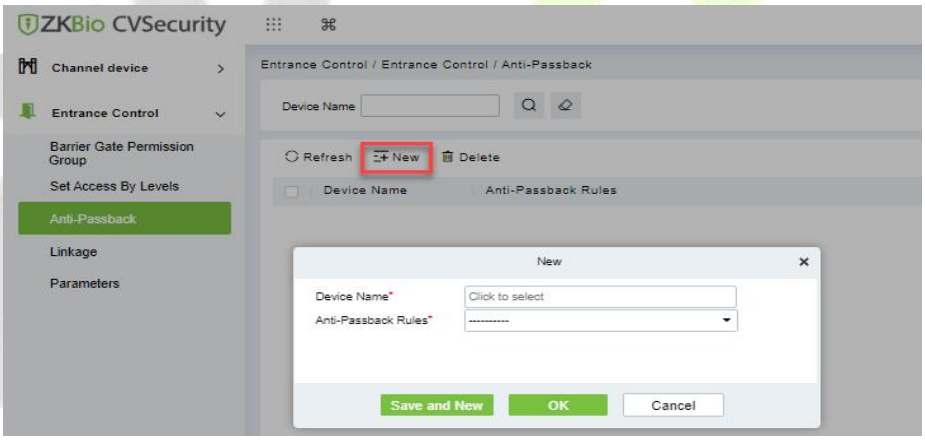


Figure 14- 35 Add Anti-Passback Interface

14.4.3.2Delete

●Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Anti-Passback** and select device name to be delete.

Step 2: Click **Delete** and click **OK** to delete Anti-passback from the group.

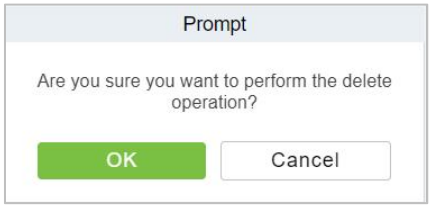


Figure 14- 36 Delete Anti-Passback

14.4.4Linkage

After a specific event is triggered at a certain input point in the channel system, a linkage action will be generated at the specified output point to control the events such as verification opening, alarm and anomaly in the system, which will be displayed in the corresponding event list monitored.

● Precondition:

Before linking new configurations, you need to do the following:

1. Gate device, input point, output point, reader binding camera add settings.

2. Mailbox parameter configuration.

14.4.4.1Add Linkage

● Operating Steps:

Step 1: In the Entrance Control module, select **Entrance Control > Linkage**.

Step 2: In the linkage setting interface, select and click the **New** button to fill in the corresponding parameters, as shown in figure below. Please refer to Table 14-5 for linkage parameters.

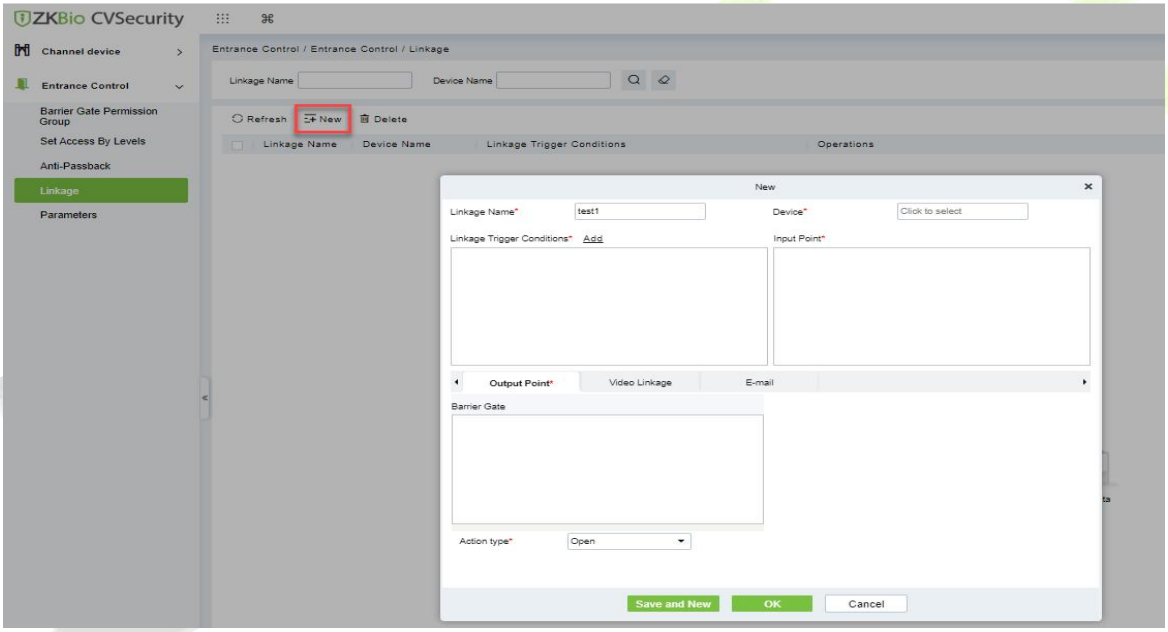


Figure 14- 37 New Linkage Interface

Parameter	Description
Linkage Name	Custom setting linkage name for easy reference.
Device	Customize and select the added access control device.
Linkage Trigger Conditions	Select the condition under which the linkage operation is triggered, that is, the type of event generated by the selected device.
Input Point	Select the input point to set the device input.
Output Point	Select the output point to set the output of the device.

Action Type	Choose to set up linkage action, including device operation of output point, video linkage and mail. Refer to Table 14-6 for configuration description of the three modes.

Table 14- 5 Description of New Linkage Parameters

Parameter	Description
Output Point	Set the action type of output point: closed, open and normally open. Sets the delay time if the output point action is on.
Video Linkage	Pop-up video, display duration: check the pop-up video in the real-time monitoring interface and set the pop-up duration. Video recording and video recording duration: Check to record and set the video recording duration. Capture: Set whether the linkage action takes pictures: If you take pictures, you also need to set whether it pops up in the real-time monitoring interface and the display time.
E-mail	Set the email address of the received linkage content when the linkage event occurs.

Table 14- 6 Explanation of Output Action Parameters

Step 3: Click **OK** to complete the linkage configuration.

14.4.4.2Delete

● Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Linkage** and select the linkage name to be delete.

Step 2: Click **Delete** and click **OK** to delete linkage.

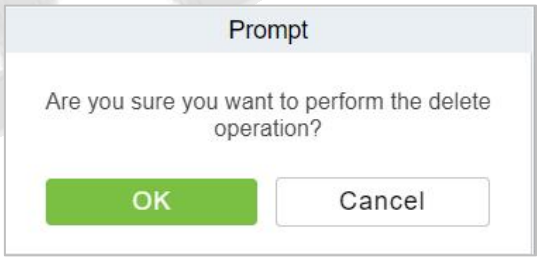


Figure 14- 38 Delete Linkage

14.4.5Parameters

Click **Entrance Control** > **Entrance Control**> **Parameter** to enter the parameter setting interface.

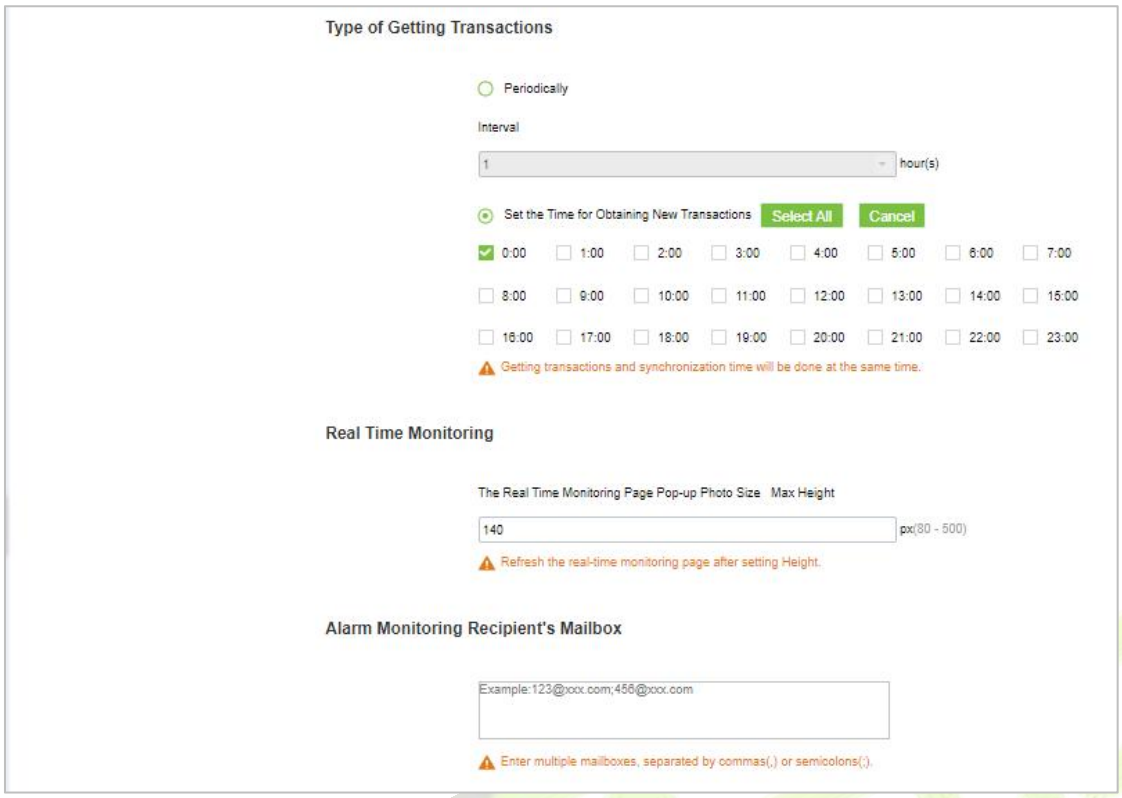


Figure 14- 39 Add Parameters

●Type of Getting Transactions:

Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Set the Time for Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

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

14.5 Passage Settings

By maintaining the gate traffic rules (control time period and traffic mode) and setting the gate parameters corresponding to the gate, the gate function can be directly controlled by software.

14.5.1 Baffle Gate Passing Rules

Set the passage time and passage mode of the gate, so that the gate can set different entry and exit passage modes in different time periods. It can be applied to flap Barrier and swing Barrier.

14.5.1.1 Add Barrier Gate Passing Rules

This part introduces the configuration Steps of gate traffic rules in ZKBio CVSecurity.

● Operating Steps:

Step 1: In the Entrance Control module, select **Passage Settings > Barrier Gate Passing Rules**.

Step 2: Click **New** with the mouse, and the interface for adding gate traffic rules will pop up.

Step 3: In the new interface, set the corresponding contents according to the new requirements, as shown in figure below. Please refer to Table 14-7 for parameter setting instructions.

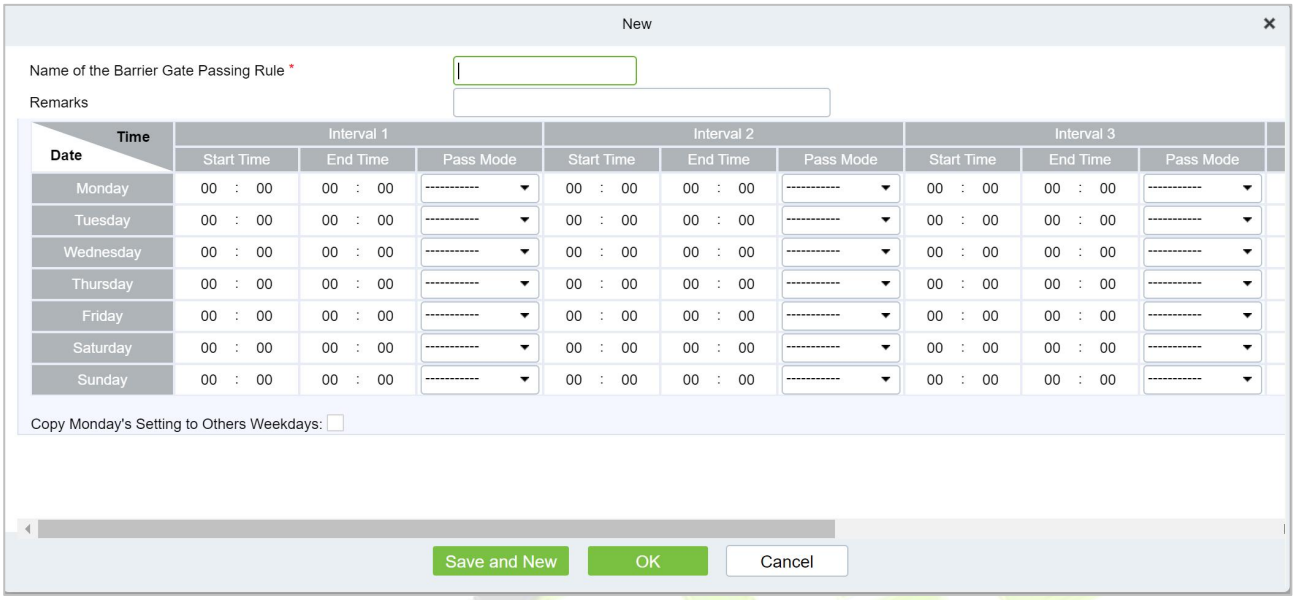


Figure 14- 40 Interface of Adding Gate Traffic Rules

Parameter	Description
Name of Gate Traffic Rules	Any character, up to 30 characters.
Remarks	The explanation of the current time period and the main application occasions shall consist of 5 0 characters at most.
Time Interval	A gate passage rule contains up to five-time intervals in a week.
Time Interval-Start/End Time	Set the start and end time in each time interval.
Pass Mode	Set the traffic mode in each time interval and select it from drop-down. There are 10 traffic modes by default: "Two-way controlled", "free entry and exit controlled", "controlled entry and exit free", "two-way freedom", "forbidden entry and exit controlled", "forbidden entry and exit free entry", "free entry and exit forbidden entry", "two-way prohibition", "remote normal opening".
Copy Monday Time to Other Working Days	You can quickly copy Monday settings to other workdays.

Table 14- 7 Parameter Description of Gate Traffic Rules

Step 4: Click **OK** to complete the addition of the gate traffic rules.

14.5.1.2Delete Passage

● Operation Steps:

Step 1: In the Entrance Control module, select **Passage Settings > Barrier Gate Passing Rules**. and select the rule to be deleted.

Step 2: Click **Delete** to delete the selected rule.

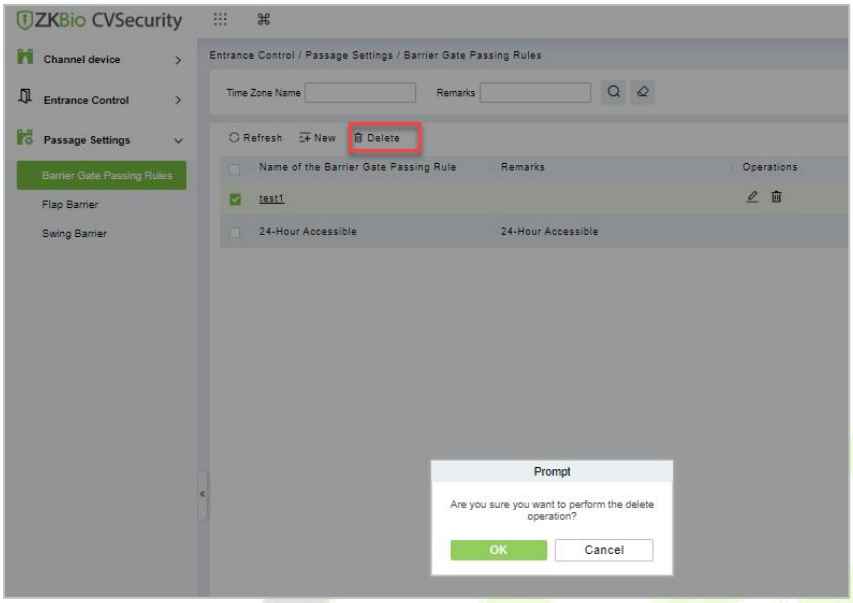


Figure 14- 41 To Delete Barrier Gate Passage Rule

Step 3: Click **OK** to perform the delete operation.

14.5.2Flap Barrier

Introduces the parameter configuration Steps of wing Barrier in ZKBio CVSecurity.

● Operating Steps:

Step 1: In the Entrance Control module, select **Passage Settings > Flap Barrier**.

Step 2: In the flap Barrier interface, click the **Edit** button under the name or operation of the flap Barrier to enter the flap Barrier parameter editing interface, as shown in figure below. Please refer to Table 14-8 for parameter description.

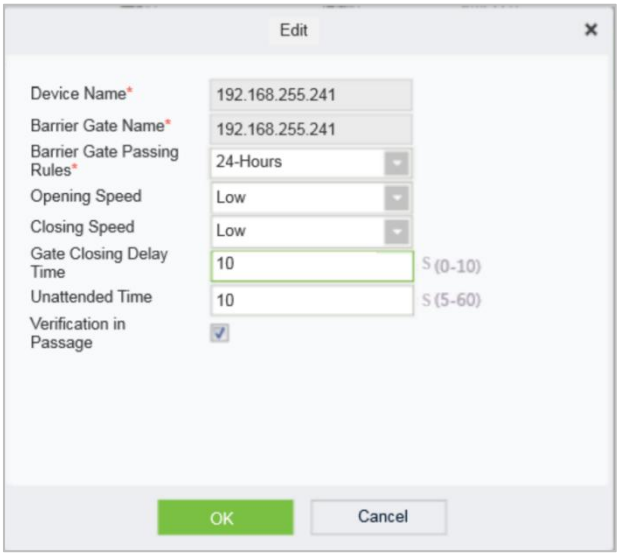


Figure 14- 42 Flap Barrier Parameter Configuration Interface

Parameter	How to set
Device Name	Name of flap Barrier device, non-editable.
Barrier Gate Name	Custom Setting Notes Description.
Barrier Gate Traffic Rules	Drop-down selection, the option is taken from the data of Passage Setting > Barrier Gate Passing Rules.
Opening Speed/ Closing Speed	Low speed, medium speed and high speed, set the speed of opening and closing the gate.
Gate Closing Delay Time	After passing through the last pair of infrared channels, set the delay closing time. You can set 0 to 10s, and the default is 0s.
Unattended Time	The maximum waiting time after verification is 5 to 60s, and the default value is 10s. If no pedestrians pass beyond the set time, the gate will be closed.
Verification in Passage	No authentication in the channel is allowed. • When checked the verification in the channel can open the gate; • If it is not checked, the gate cannot be opened for verification in the channel, and the gate can be verified only after exiting the gate.

Table 14- 8 Explanation of Flap Barrier Parameters

Step 3: Click **OK** to complete the configuration of flap Barrier parameters.

14.5.3Swing Barrier

This part introduces the parameter configuration Steps of swing Barrier in ZKBio CVSecurity.

●Operating Steps:

Step 1: In the Entrance Control module, select **Passage Settings > Swing Barrier**.

Step 2: In the swinging interface, click the **Edit** button under the swinging name or operation to enter the swinging parameter editing interface, as shown in figure below. Please refer to Table 14-9 for parameter description.

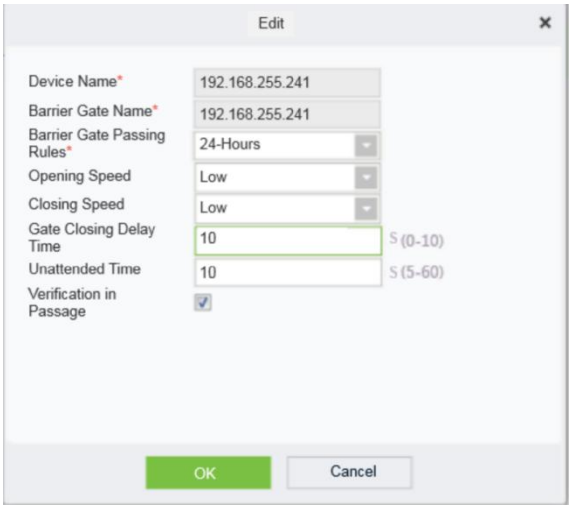


Figure 14- 43 Swing Barrier Parameter Configuration Interface

Parameter	How to set
Device Name	The name of the swing Barrier device cannot be edited.
Barrier Gate Name	The gate name corresponding to the swing gate device is generally one all-in-one device corresponding to one gate, which cannot be edited.
Barrier Gate Traffic Rules	Drop-down selection, the option is taken from the data of Passage Setting > Barrier Gate Passing Rules.
Opening Speed/ Closing Speed	Low speed, medium speed and high speed, set the speed of opening and closing the gate.
Gate Closing Delay Time	After passing through the last pair of infrared channels, set the delay closing time. You can set 0 to 10s, and the default is 0s.
Unattended Time	The maximum waiting time after verification is 5 to 60s, and the default value is 10s. If no pedestrians pass beyond the set time, the gate will be closed.
Verification in Passage	Whether authentication in the channel is allowed. • When checked the verification in the channel can open the gate; • If it is not checked, the gate cannot be opened for verification in the channel, and the gate can be verified only after exiting the gate.

Table 14- 9 Description of Swing Barrier Parameters

Step 3: Click **OK** to complete the configuration of wing Barrier parameters.

14.6 Reports

In the Channel report, you can query the All Transactions, Today's Access Records, Person's Last Access Location, and All Exception Events. You can choose to export all or export records after querying.

14.6.1 All Transactions

This part introduces the configuration Steps of report query and export in, taking All Transaction report operation.

14.6.1.1 Export

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports> All Transactions**.

Step 2: In the All Records interface, fill in the corresponding query information and click the **Query** symbol to complete the query of all record tables, as shown in figure below.

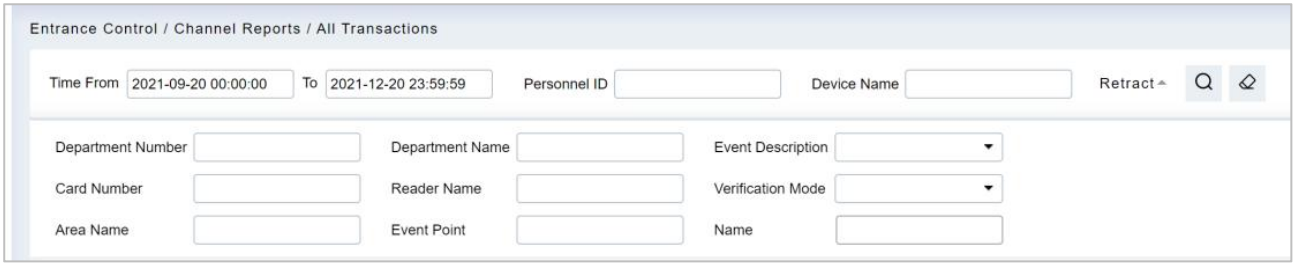


Figure 14- 44 All Transactions

Step 3: In the full record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in figure below.

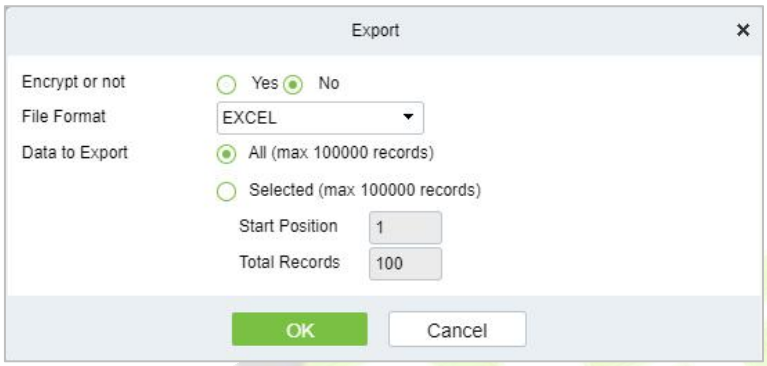


Figure 14- 45 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

14.6.1.2Clear All Data

This option allows user to clear all data available in all transaction interface.

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports> All Transactions**.

Step 2: Click the **Clear All Data** to clear all transactions.

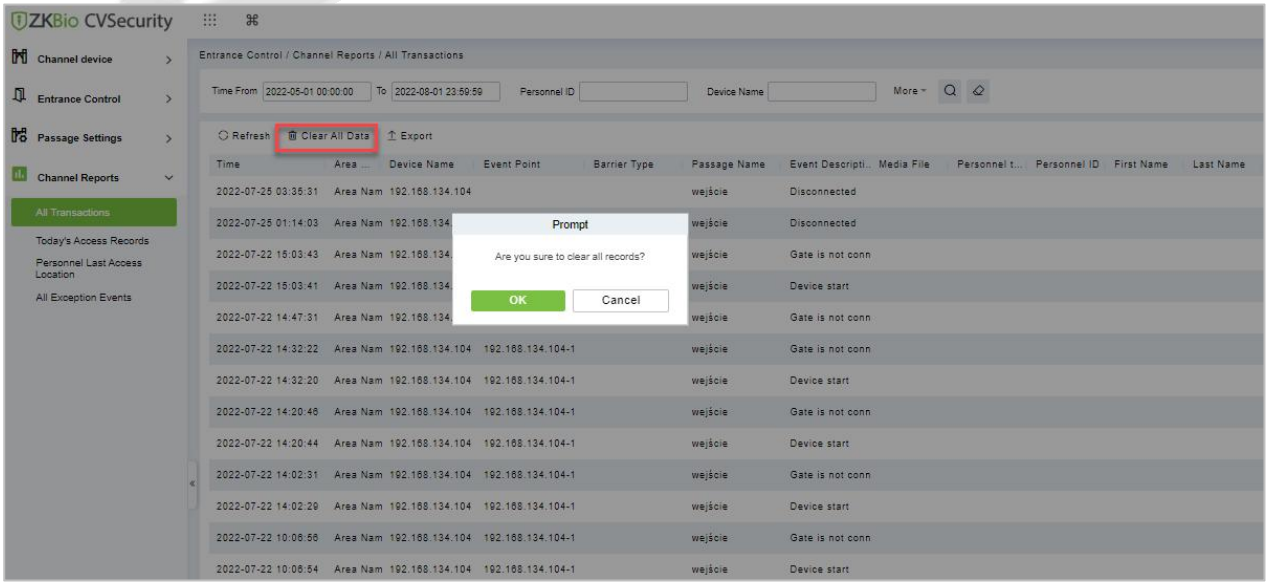


Figure 14- 46 Clear All Data Option

Step 3: Click **OK** to clear all records.

14.6.2Today's Access Records

The access records for today are displayed in this option.

14.6.2.1Export

●Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports > Today's Access Record**.

Step 2: In Today's Access Record interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in figure below.

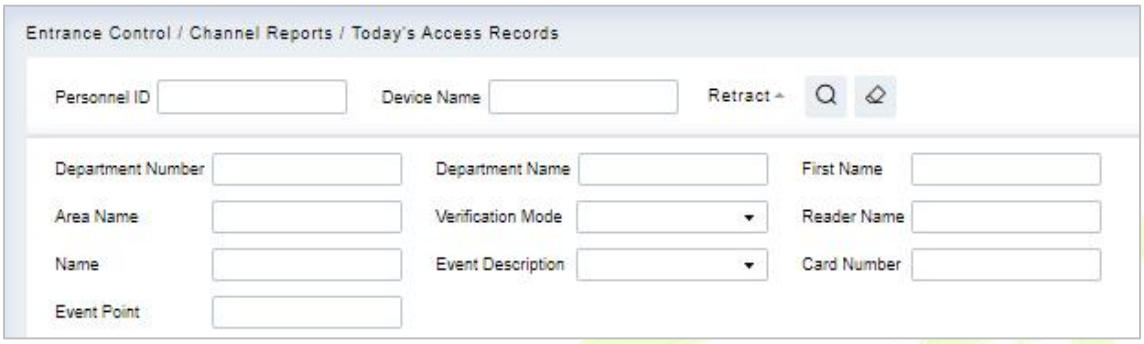


Figure 14- 47 Today's Access Record

Step 3: In the access record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in figure below.

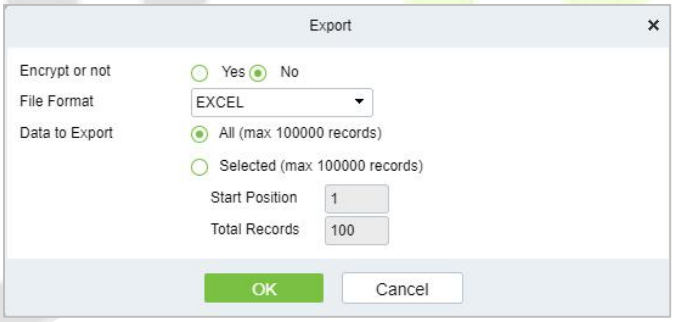


Figure 14- 48 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

14.6.2.2Clear All Data

This option allows users to clear all data available in today's access record interface.

●Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports> Today's Access Record**.

Step 2: Click the **Clear All Data** to clear access records.

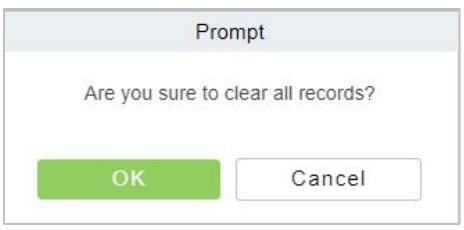


Figure 14- 49 Clear All Data Option

Step 3: Click **OK** to do the delete operation.

14.6.3Personnel Last Access Location

Displays the last location visited by persons with access rights. It is convenient for users to quickly locate the location of personnel.

14.6.3.1Export

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports > Personnel Last Access Location**.

Step 2: In Personnel Last Access Location interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in figure below.

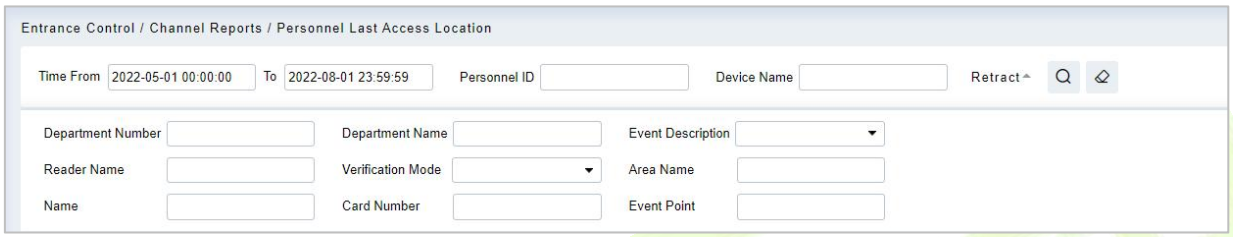


Figure 14- 50 Today's Access Record

Step 3: In the access location interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in figure below.

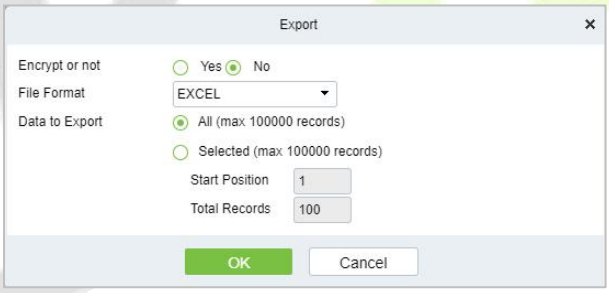


Figure 14- 51 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

14.6.3.2Clear All Data

This option allows users to clear all data available in Personnel Last Access Location interface.

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports > Personnel Last Access Location**.

Step 2: Click the **Clear All Data** to clear the access location records of the persons, as shown in figure below.

Step 3: Click **OK** to do the delete operation.

14.6.4All Exception Events

Click **Channel Report > All Exception Events** to view the abnormal events (including alarm events) such as unregistered persons, illegal entry, gate opening timeout, and failure to connect to the server under specified conditions (including alarm events).

14.6.4.1 Export

● Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports > All Exception Events.

Step 2: In All Exception Events interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in figure below.

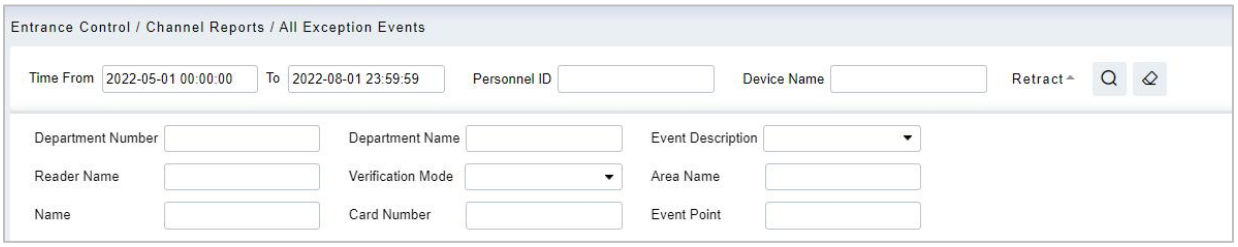


Figure 14- 52 All Exception Events

Step 3: In the All-Exception Events interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in figure below.

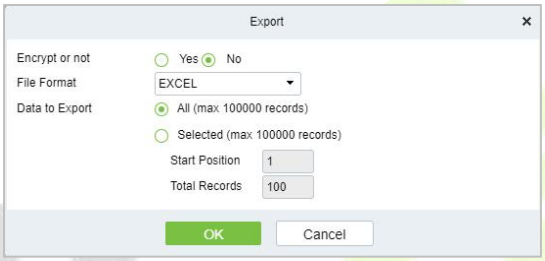


Figure 14- 53 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

14.6.4.2 Clear All Data

This option allows users to clear all data available in All Exception Events interface.

● Operating Steps:

Step 1: In the Entrance Control module, select **Channel Reports> All Exception Events**.

Step 2: Click the **Clear All Data** to clear exception events record.

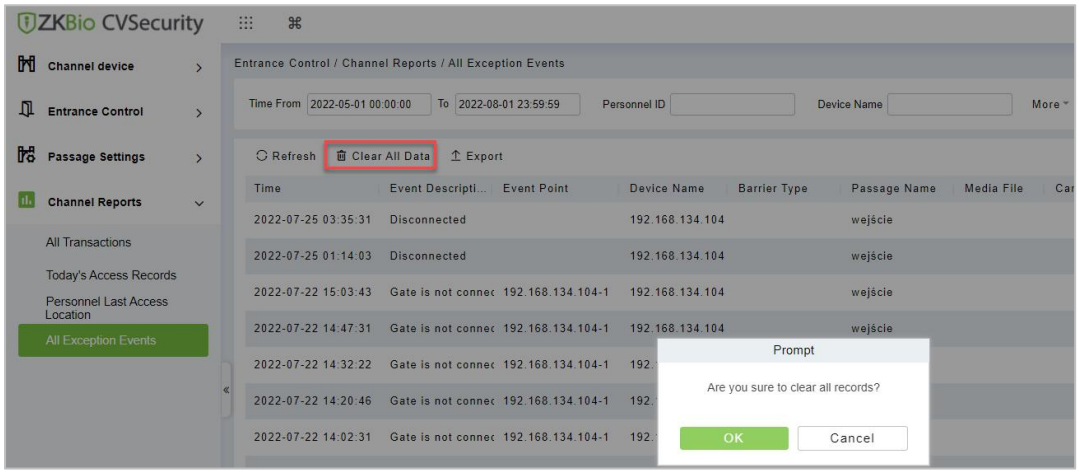


Figure 14- 54 Clear All Data Option

Step 3: Click **OK** to do the delete operation.

15 FaceKiosk

15.1 Facekiosk Device

15.1.1 Device

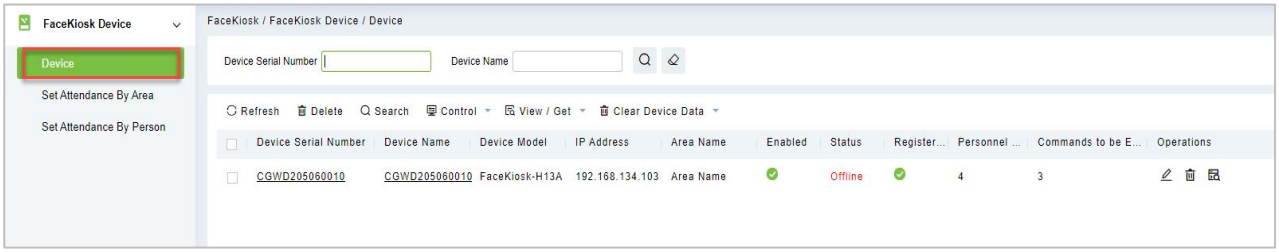


Figure 15- 1 Device

15.1.1.1 Delete

Select one or more devices and click **Delete** at the upper part of the list and click **OK** to delete the selected facekiosk device. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single device.

15.1.1.2 Search Device

In the tool bar, select the "**Search device**" menu. Add the device to the software server.

Note: User need to entry the hardware device and setting some parameters which is supported to setting the software server address.

15.1.1.3 Control

Click **FaceKiosk Device** > **Device**, then select Control to Enable/ Disable, Reboot, synchronize software Data, and Issued QRCode Address of the device.

Function	Description
Enable/ Disable	Select device, click Disable/ Enable to stop/ start using the device. When communication between the device and the system is interrupted or device fails, the device may automatically appear in disabled status. After adjusting local network or device, click Enable to reconnect the device and restore device communication.
Reboot Device	It will reboot the selected device
Synchronize software Data to the Device	Synchronize data of the system to the device. Select device, click Synchronize All Data to Devices and click OK to complete synchronization.
Issued QRCode Address	Select the Issued QRCode Address.

Table 15- 1 Device Control

15.1.1.4View / Get

Click **FaceKiosk Device > Device**, then select View/Get to Get Device Option, View Device Parameters, Re-upload Data, and to Gets the Specified Person Data.

Parameters	Description
Get Device Option	It gets the common parameters of the device. For example, get the firmware version after the device is updated.
View Device Parameters	Show the capacity detail.
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/personnel information/attendance photo, click the confirmation to get such information again from the device.
Gets the Specified Person Data	It gets the Specified person Data from the device.

Table 15- 2 Device View/Get

15.1.1.5Clear Device Data

Click **FaceKiosk Device > Device**, then select Clear Device Data to clear Device Command, Verification Photo and Validation Record.

Parameters	Instruction
Clear Device Command	Select the device to be cleared. It clears the operation command issued by the software in the setting.
Clear Verification Photo	Select the device. This function will clear all the verification photo records from the device.
Clear Validation Record	Select the device. This function will clear all the validation data records from the device.

Table 15- 3 Clear Device Data

15.1.1.6Edit

Click advertisement resources or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

15.1.2Set Attendance by Area

Click **FaceKiosk > FaceKiosk Device**, then Select Set Attendance by Area.

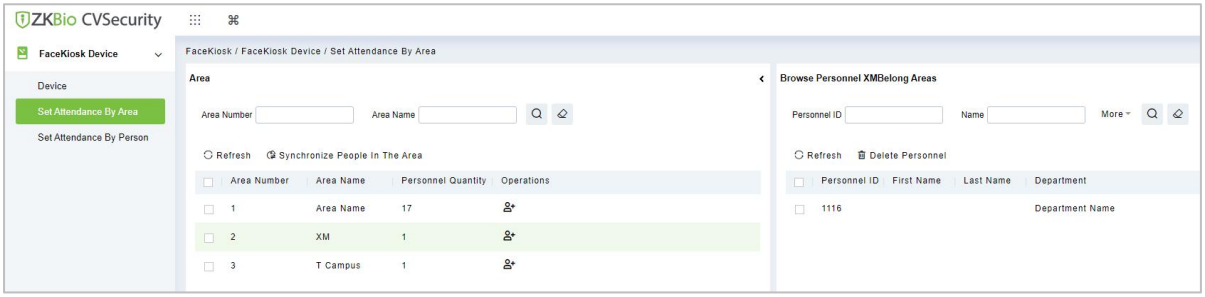


Figure 15- 2 Set Attendance by Area

15.1.2.1 Synchronize People in the Area

Click **FaceKiosk > FaceKiosk Device > Set Attendance by Area**, then select Synchronize People in The Area.

Click **OK** to save and exit.

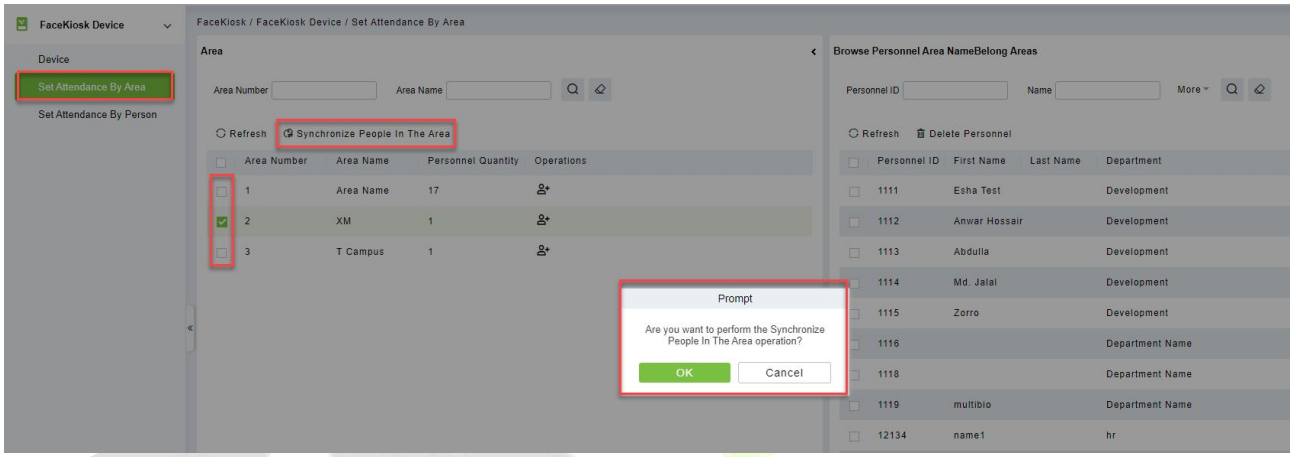


Figure 15- 3 Set Attendance by Area

15.1.3 Set Attendance by Person

Click **FaceKiosk > FaceKiosk Device**, then Select Set Attendance by Person.

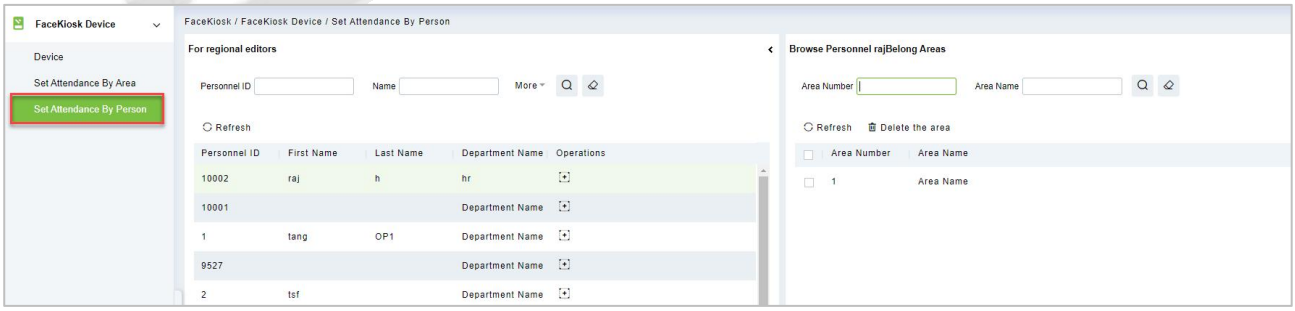


Figure 15- 4 Set Attendance by Person

15.2 Media Advertisement Resources

15.2.1 Advertisement Resources

Click **FaceKiosk > Media Advertisement Resources**, then Select Advertisement Resources.

In the Advertisement resources module, it can support to create/edit/delete advertisement resources.

15.2.1.1 Add (New)

Support to upload some new advertisement resources to software server.

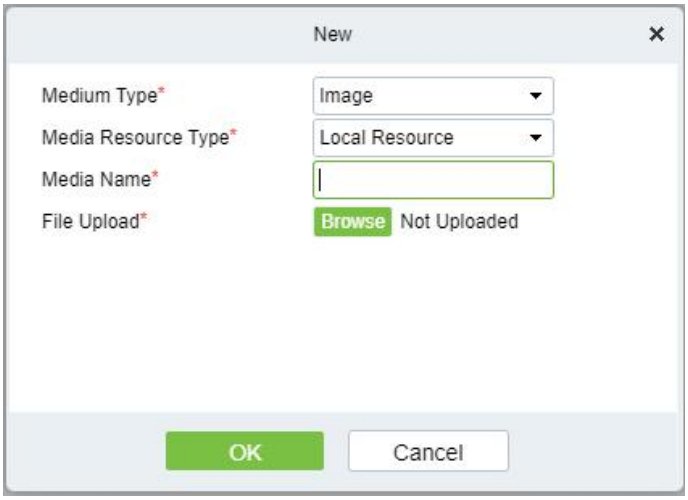


Figure 15- 5 Media advertisement Resources

15.2.1.2 Edit

Click device name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

15.2.1.3 Delete

Select one or more advertisement resources and click **Delete** at the upper part of the list and click **OK** to delete the selected advertisement resources. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single advertisement resource.

15.2.2 Advertisement Settings

Click **FaceKiosk > Media Advertisement Resources**, then Select Advertisement Settings.

This module support to create **Edit** and **Delete** the advertising.

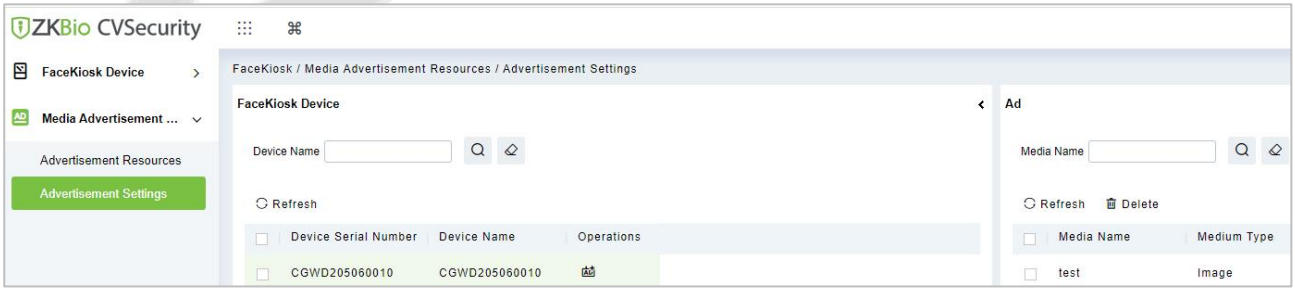


Figure 15- 6 Advertisement settings

15.3 FaceKiosk Reports

15.3.1 Verification Record

Click > **FaceKiosk** > **FaceKiosk Reports, then Verification Record** to view specified events in specified condition.

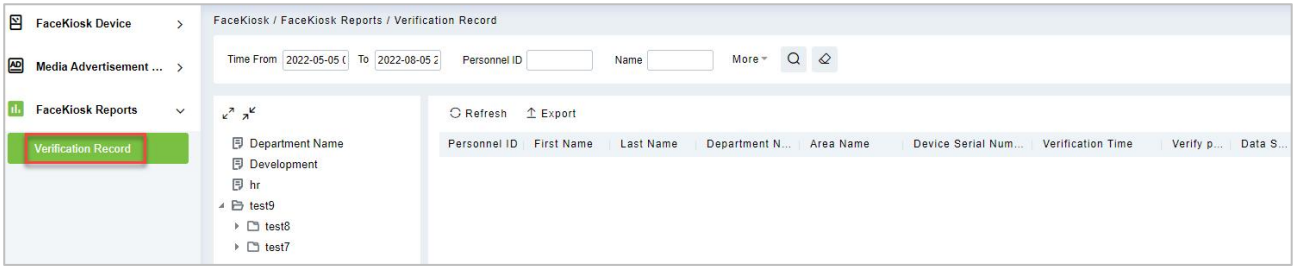


Figure 15- 7 Verification Record

15.3.1.1 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

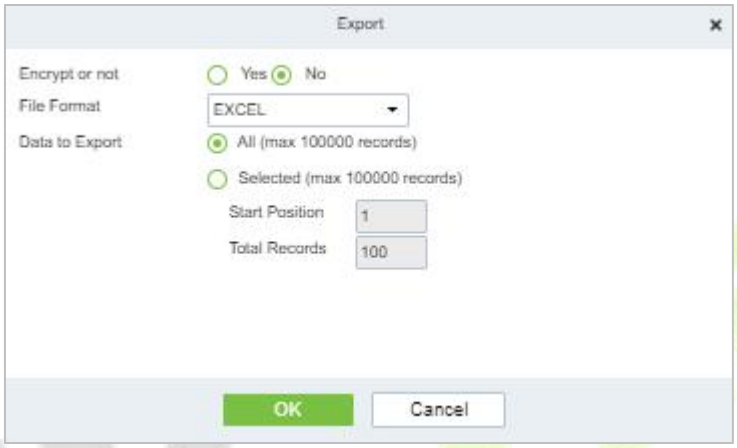


Figure 15- 8 Verification Record

16 Locker

16.1 Locker Device Management

16.1.1 Device

16.1.1.1 Add Devices (New)

Step 1: Go to **Locker> Locker Device Management > Device**.

Step 2: Click **New**, the interface for adding a device will pop up.

Step 3: In the interface for adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the figure below. Please refer to Table 16-1 for the description of parameter.

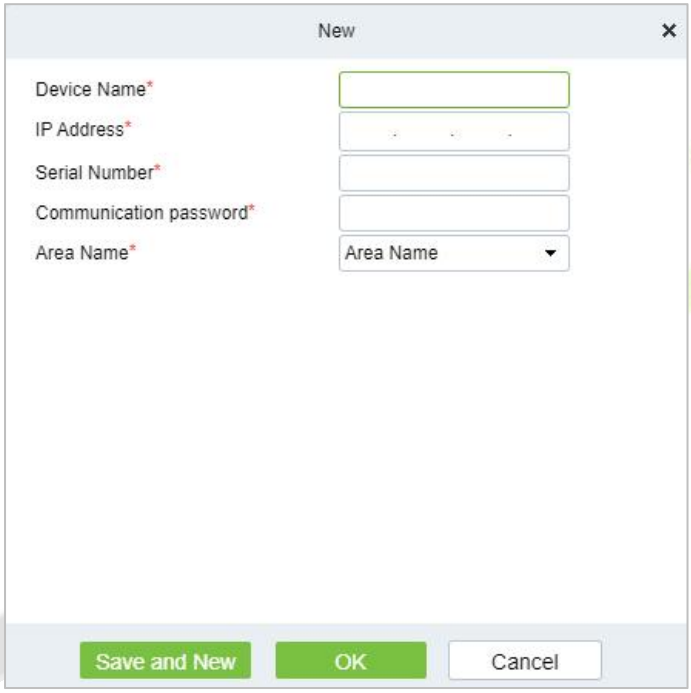


Figure 16- 1 Adding Device Interface

Parameter	Description
Device Name	Customize the name of the device.
IP Address	Fill in the IP address of the device.
Serial Number	Fill the device serial number.
Communication Password	Fill in the communication password of the device. You can add it only after the verification is successful.
Area Name	Divide the area for the device.

Table 16- 1 Adding Device Parameters

16.1.1.2 Delete

Step 1: Go to Locker> Locker Device Management > Device.

Step 2: Select device, click **Delete**, then click **OK** to delete device.

Figure 16- 2 Delete Device

16.1.1.3Control

● Set Administrator:

Administration has permission to set the administrator permission to device. Select the person, click **>**, and click **OK**.

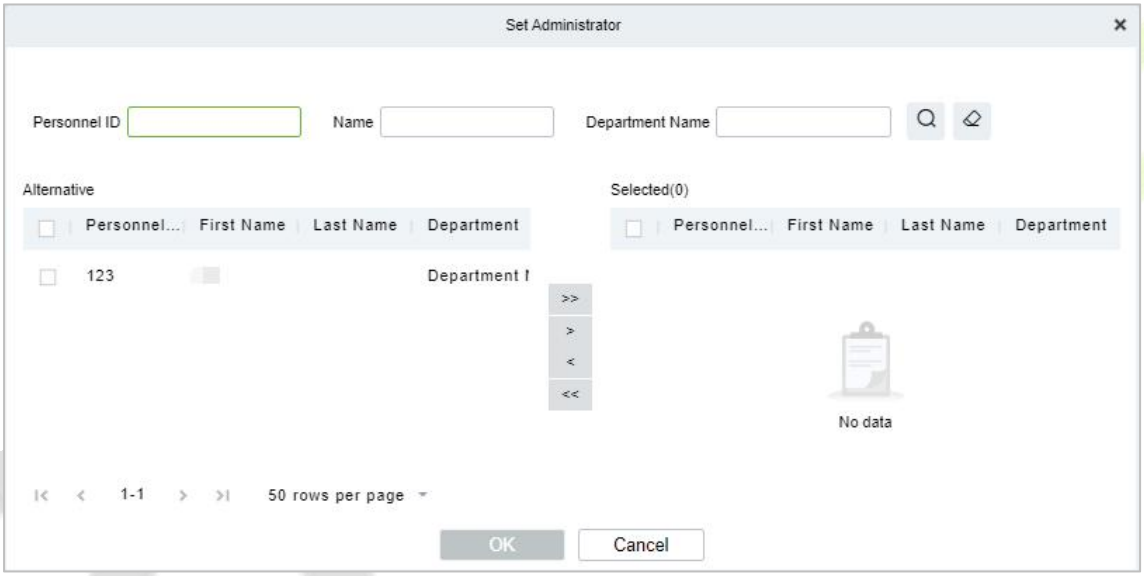


Figure 16- 3 Set Administrator Interface

● Clear Administrator:

Administration has permission to clear the administration permission from device.

● Reboot Device:

It will reboot the selected device.

● Synchronize Time:

It will synchronize device time with server's current time.

● Synchronize All Data to Devices:

Synchronize data of the system to the device. Select device, click **Synchronize All Data to Devices** and click **Synchronize** to complete synchronization.

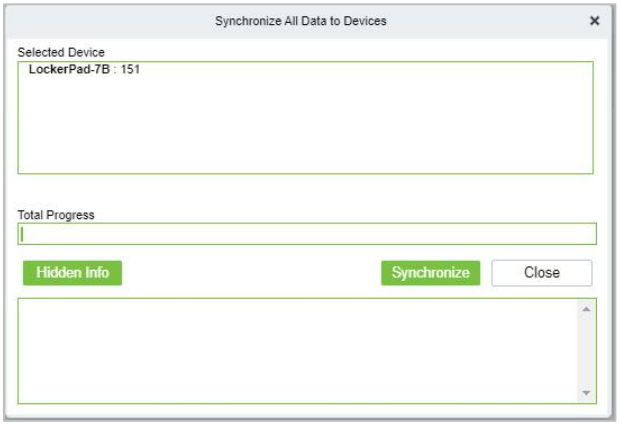


Figure 16- 4 Synchronize All Data to Devices Interface

● Distribute Advertising Resources:

Administrator selects the AD resource on the computer and delivers it to lockerpad-7b. Click **Distribute Advertising Resources**, click **Browser**, then select the picture or video and click **OK**.

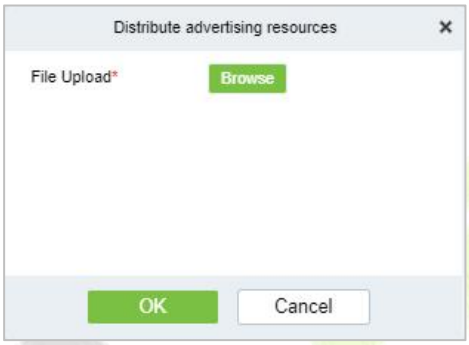


Figure 16- 5 Distribute Advertising Resources Interface

● Clear All Ads:

Clears all ads resources from the selected device.

16.1.1.4 Binding/Unbinding the Camera

● Steps:

Step 1: In Locker module, select **Locker Device Management > Device**.

Step 2: Choose device, click icon .

Step 2: Select **Channel**, click **>** and click **OK**.

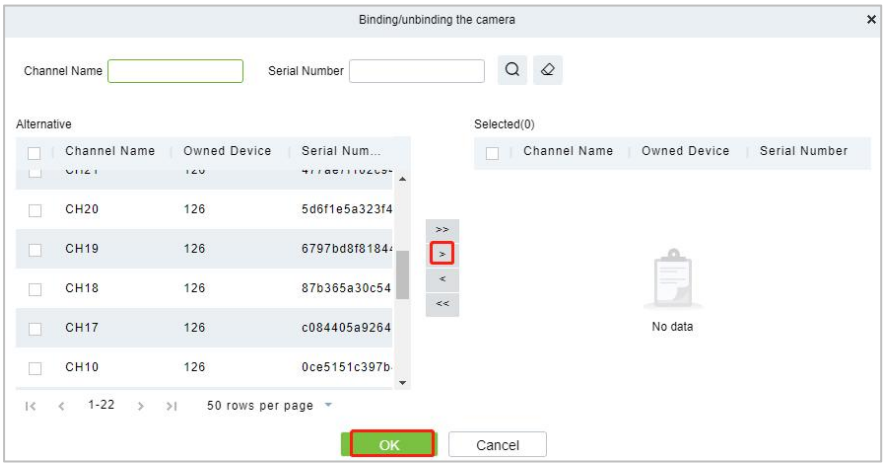


Figure 16- 6 Binding Camera

16.1.2Parameters

In **Locker** module, click Locker **Device Management** > **Parameter** to set the parameters.

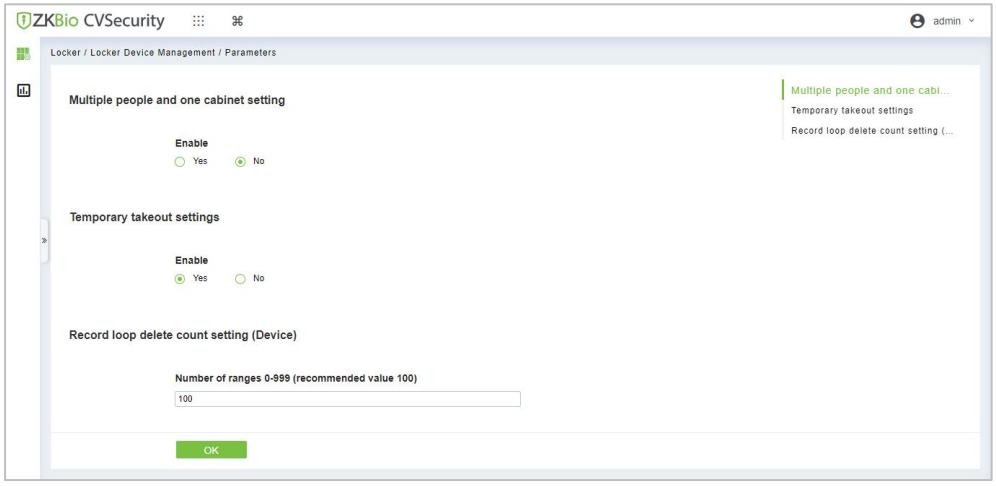


Figure 16- 7 Parameter

Item	Description
Multiple people and one cabinet setting	Multiple users can share a cabinet when it is enabled.
Temporary takeout settings	When enabled, users can remove objects without losing access to the cabinet
Record loop delete count setting (Device)	When a specified number of stored records is reached, a certain number of records will be deleted from the beginning, the number of records you fill in the space.

Table 16- 2 Parameter Description

16.1.3Visual Panel

In this function, admin can bind users in the software to the corresponding cabinet.

16.1.3.1Distribution Cabinet

● Steps:

Step 1: In the Locker module, select **Locker Device Management > Visual Panel**, as shown in figure below.

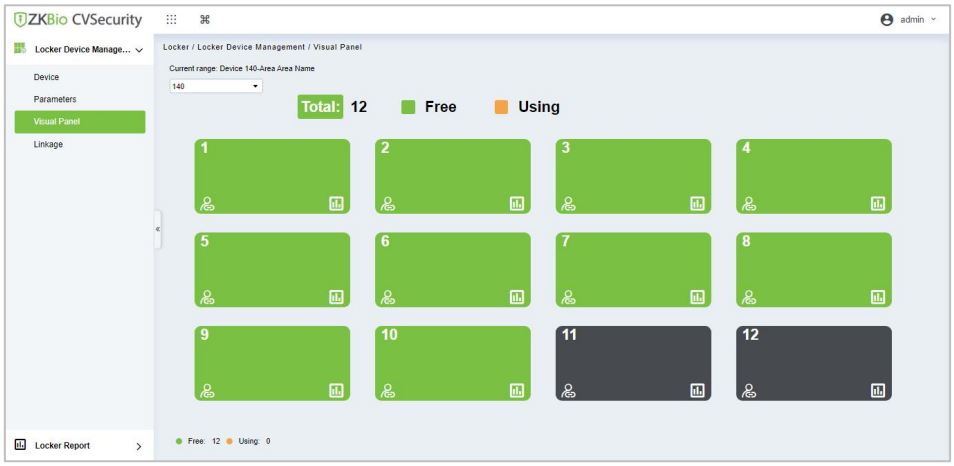


Figure 16- 8 Visual Panel

Step 2: Select a panel, click , and the interface of Select Person will pop up, as shown in figure below.

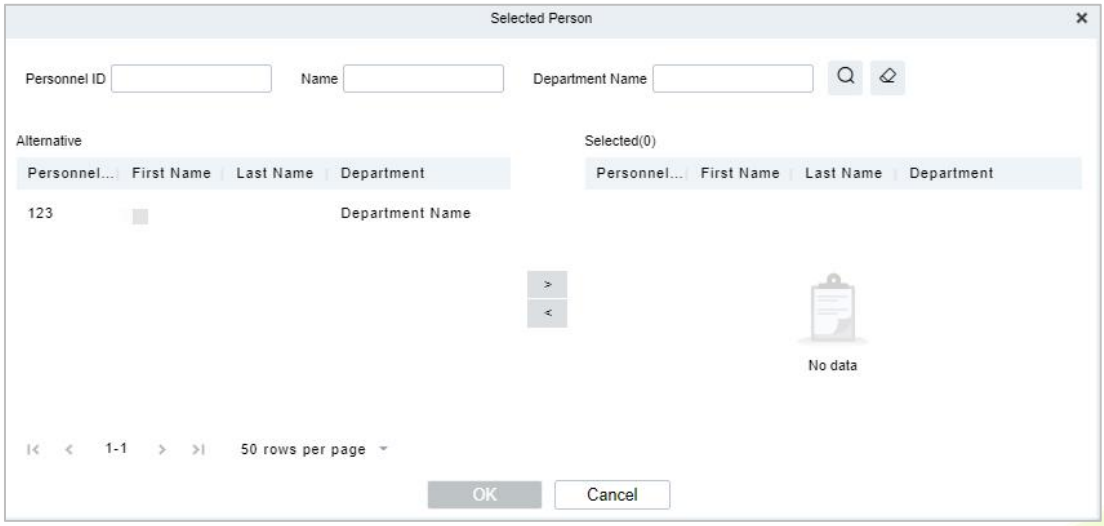


Figure 16- 9 Select Person Interface

Step3: Select the user that the admin wants to bind with the cabinet. Then click **>** and **OK**.

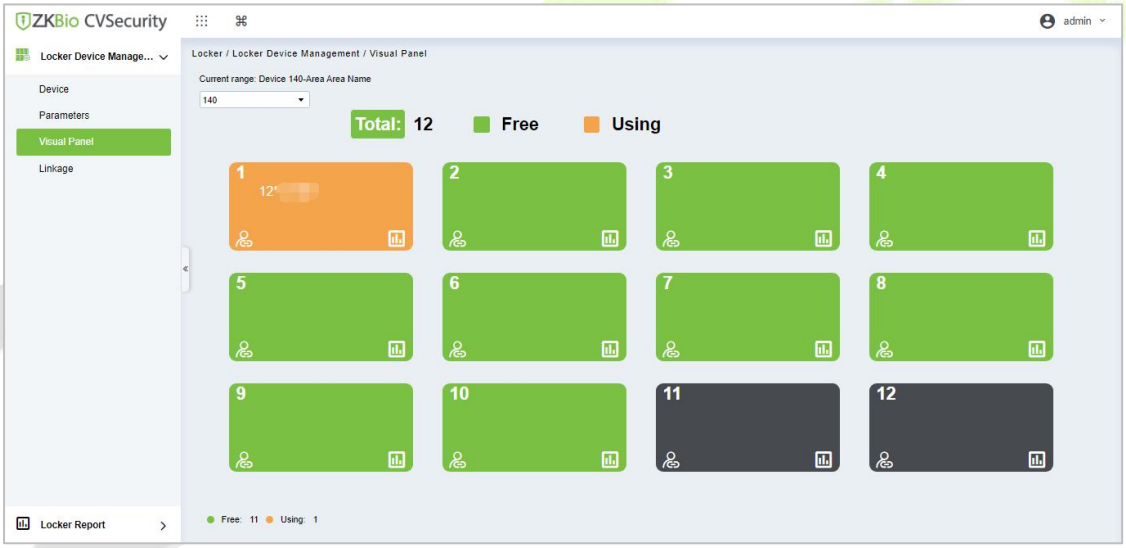


Figure 16- 10 Visual Panel Interface

16.1.3.2View the Last 5 Records

● Steps:

Step 1: In the Locker module, select **Locker Device Management** > **Visual Panel**.

Step 2: Select a panel, click , and the interface of View the last 5 records will pop up, as shown in figure below.

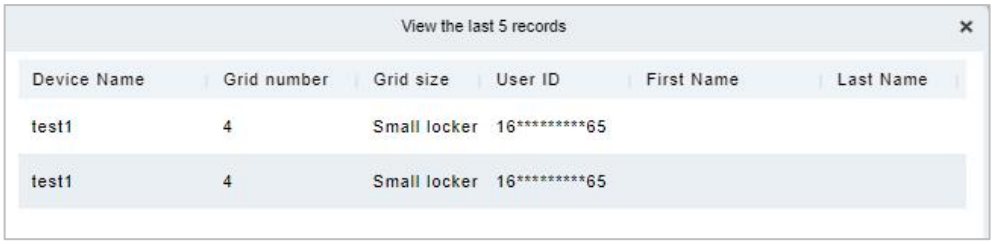


Figure 16- 11 Visual Panel Interface

✍Notes:

Color definition:

Figure 16- 12 Enable, no person has bound, available.

Figure 16- 13 Enable, personnel have been bound, unavailable.

Figure 16- 14 Enable, personnel have been bound, unavailable.

Figure 16- 15 Not enabled, can be manually enabled.

16.1.4Global Linkage

The use method and scenario of linkage are flexible. After a specific event is triggered by an input point in the locker system, a linkage action will be generated at the specified output point to control events such as video recording and send e-mail in the system.

This section describes how to add Step to the linkage effect in ZKBio CVSecurity.

16.1.4.1Add

● Preconditions:

Before adding a linkage configuration, the system needs to have an intrusion device.

● Steps:

Step 1: In the Locker module, choose **Locker Device Management > Linkage**.

Step 2: On the linkage setting screen, click **Add**, as shown in figure below. Table 16-3 and Table 16-4 refer to the linkage parameters.

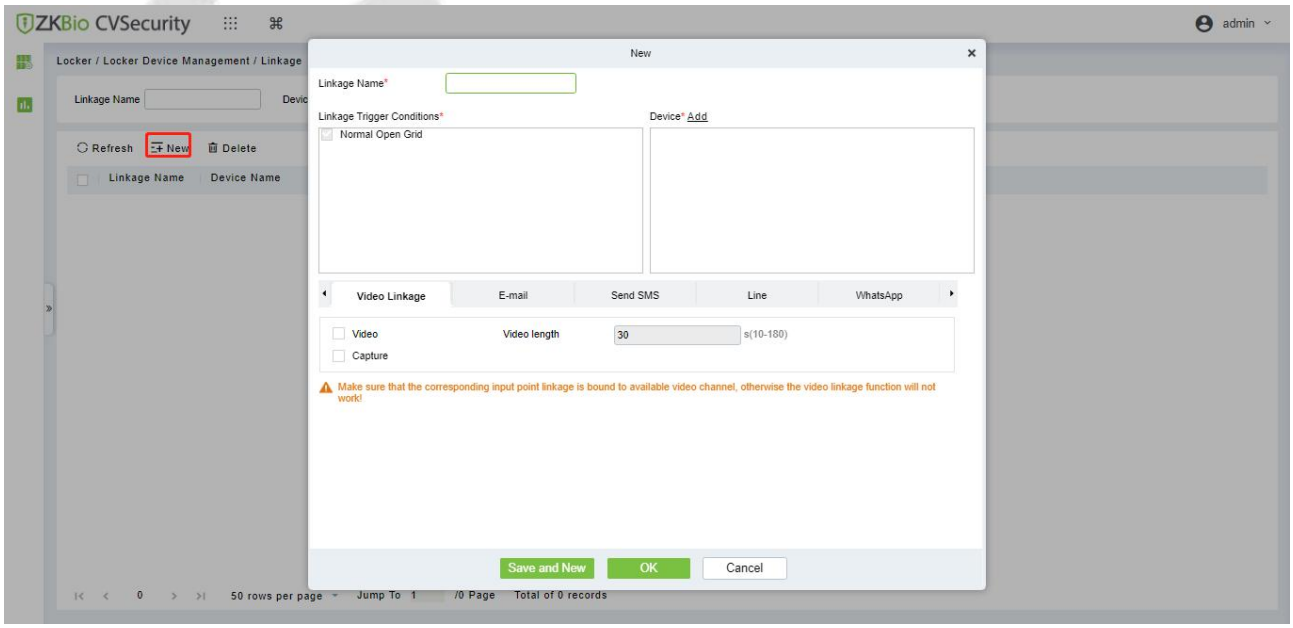


Figure 16- 16 Adding Linkage

Parameter	Description
Linkage Name	You can customize the linkage name for easy query.
Linkage Trigger Conditions	Select the condition triggered by the linkage Operation, that is, the event type generated by the selected device.
Device	Select the locker to be linked.

Table 16- 3 Linkage parameters

Parameter	Description
Video Linkage	Pop-up video and display duration: Select pop-up video on the real-time monitoring screen and set the pop-up duration. Video recording and Video Duration: Select Video recording to set the video duration. 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
Mail	Set the email address that receives the linkage content when a linkage event occurs.

Table 16- 4 Linkage parameters

16.1.4.2Delete

● Steps:

Step 1: Select **linkage**, click **Delete**, and click **OK** to delete the linkage.

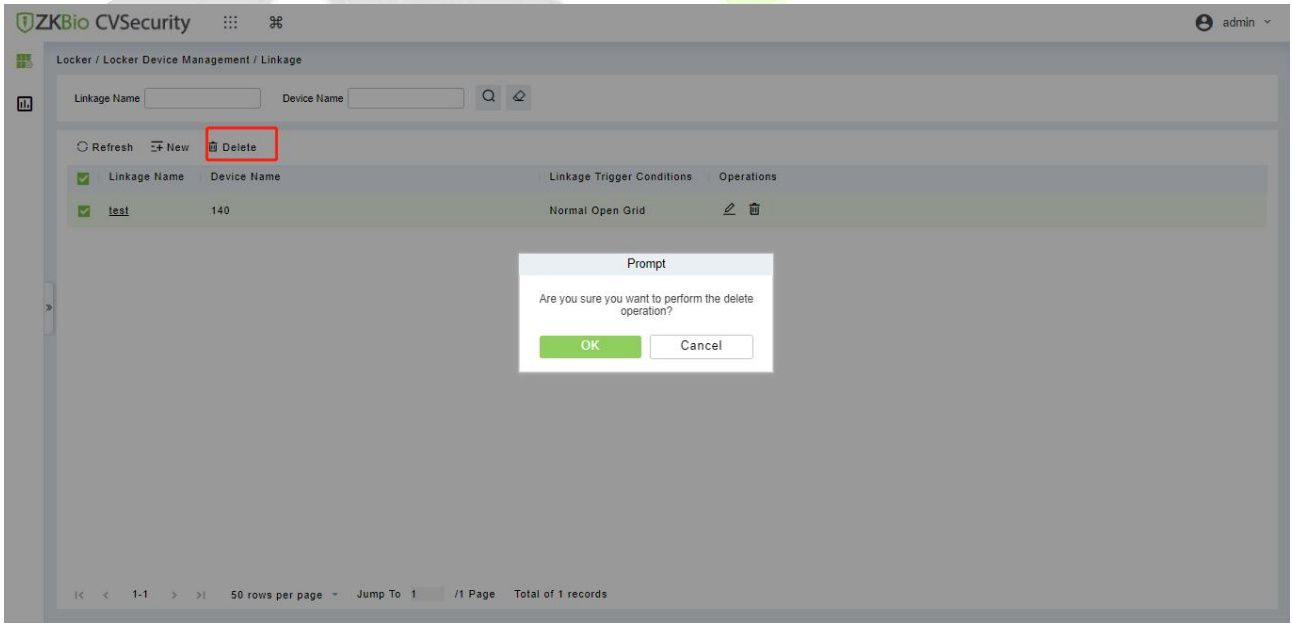


Figure 16- 17 Delete Linkage

16.2 Locker Report

16.2.1All Transactions

● Steps:

Step 1: Go to **Locker > Locker Report > All transaction**.

Step 2: On the **All Records** interface, fill in the corresponding query information and click **Search** symbol to complete the query of all records.

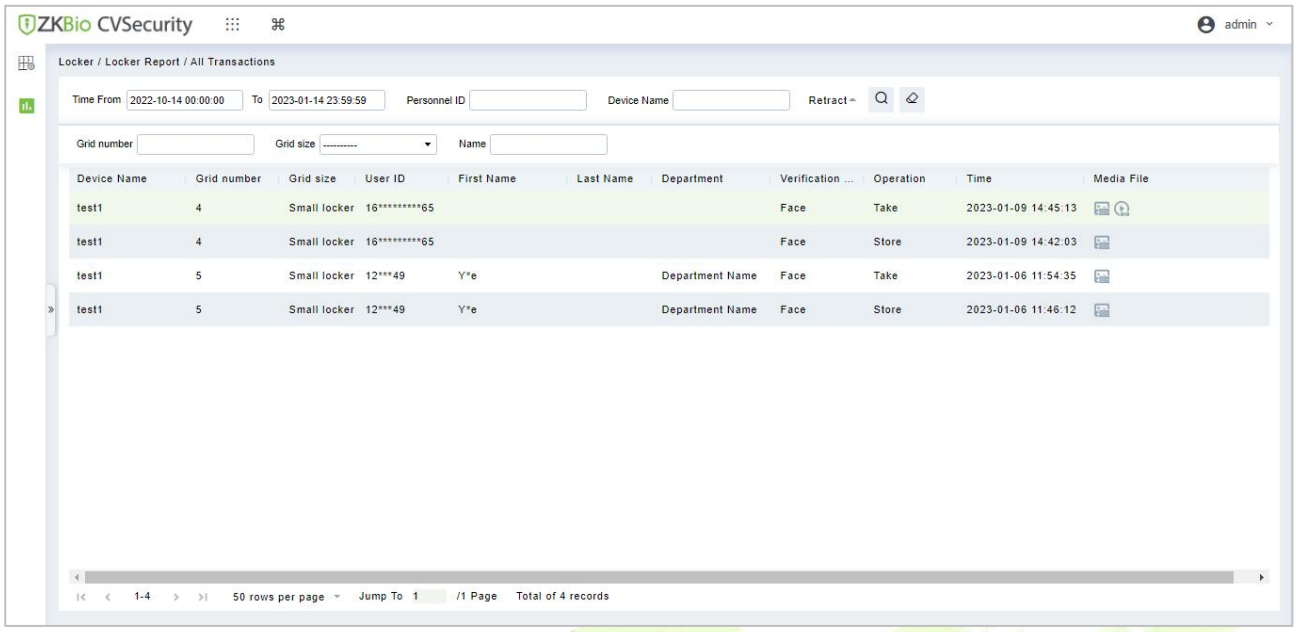


Figure 16- 18 Report Query Page

Notes:

: Click on this icon and it will show the image taken by LockerPad-7b when the cabinet was opened.

: Click on this image and it will show the video taken by the bound camera when the linkage is triggered.

16.2.1.1 Export

On the **All Records** interface, click **Export**, enter the admin 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**.

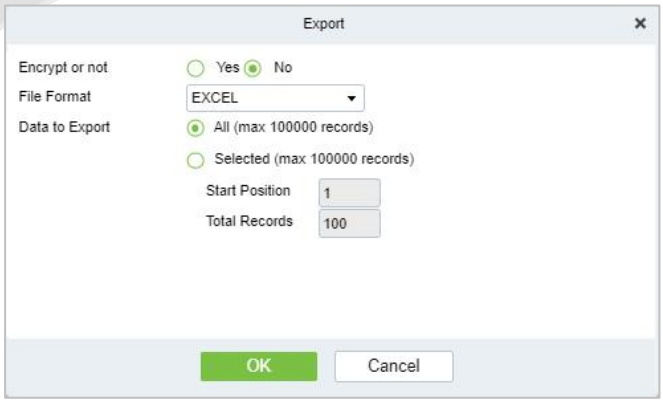


Figure 16- 19 Report Export Page

	A	B	C	D	E	F	G
1	All Transactions						
2	Device Name	Grid number	Grid size	User ID	First Name	Last Name	Department
3	196	1	Small locker	1			
4	196	1	Small locker	1			
5	196	1	Small locker	1665310457633			
6	196	1	Small locker	1665310457633			
7	151	8	Small locker	1665194322753			
8	151	8	Small locker	1665194322753			

Figure 16- 20 Event Export

16.2.1.2Clear All Data

Click **Clear All Data**, then click **OK** to clear all transactions on the **Prompt** interface.

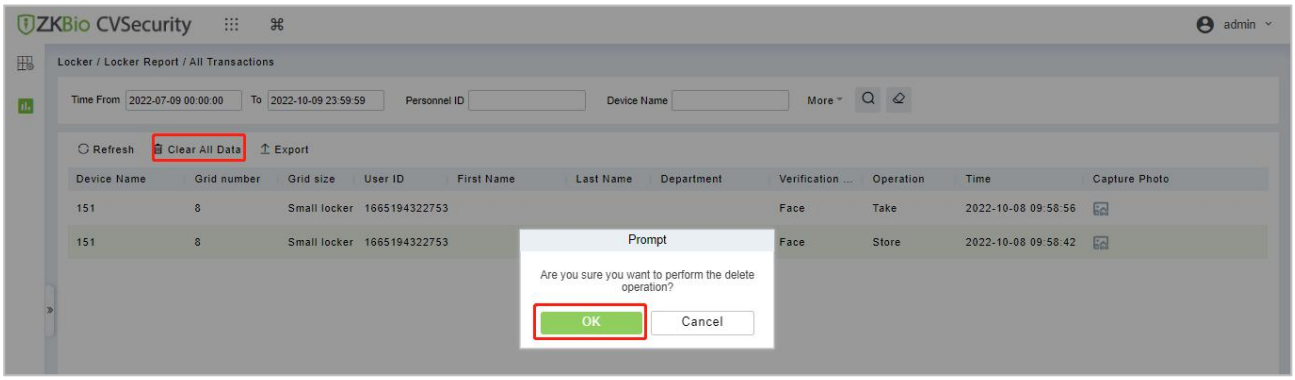


Figure 16- 21 Report Clear All Data

17 Intrusion Alarm

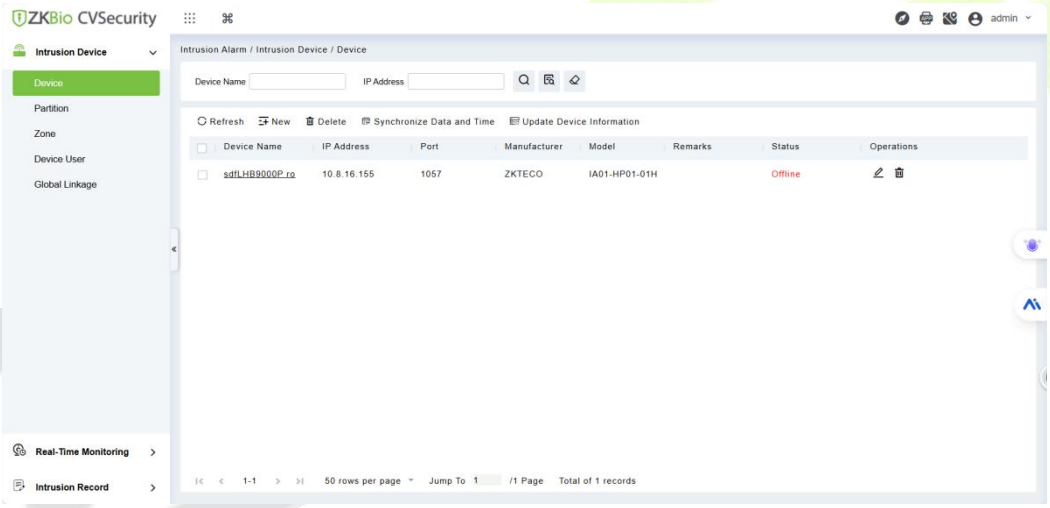
The intrusion alarm system is a robust security solution for monitoring and protecting restricted areas. It provides real-time detection of unauthorized access, identifies intrusions, and triggers configurable alarms. Integrated with the security management platform, it supports multiple detection zones, adjustable sensitivity, and flexible alarm escalation, ensuring centralized monitoring and rapid response for effective protection of critical areas.

17.1 Intrusion Device

Device includes Panel/ Partition/ Point/ Output and some of the alarm linkage of the intrusion alarm panels.

17.1.1 Device

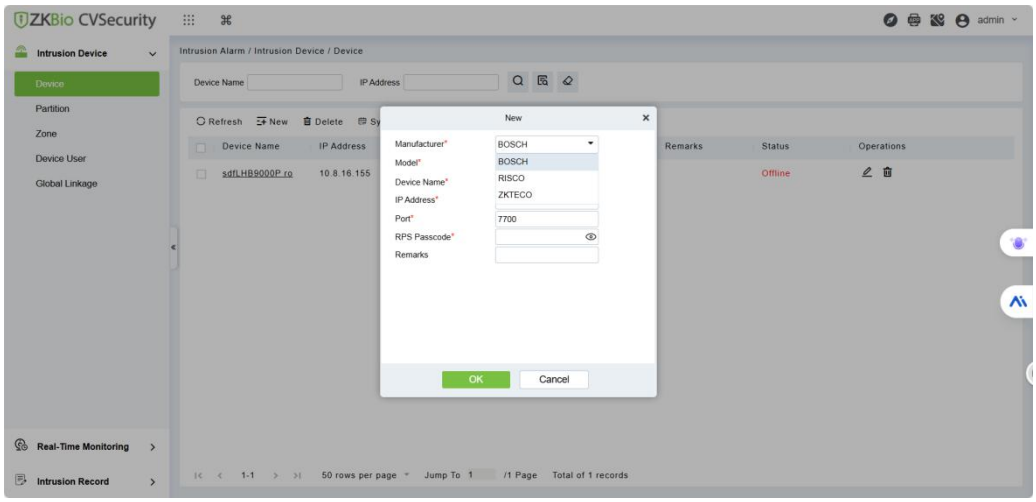
This menu is used to add and manage devices.



17.1.1.1 New

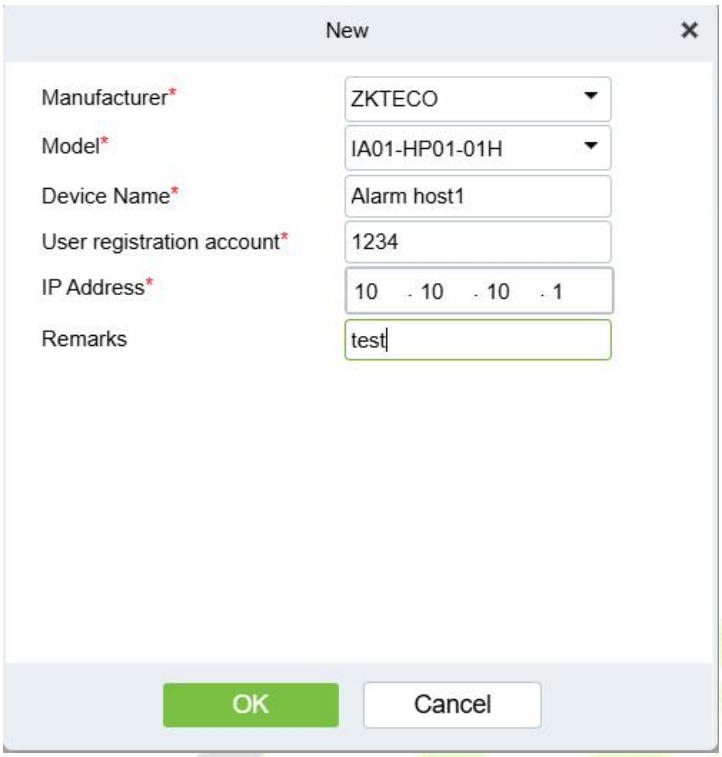
Click **[+New]** button to add a new device.

✍ **Note:** The Manufacturer current support BOSCH/RISCO/ZKTECO. After selecting the corresponding manufacturer, you can further select the device model.



Add ZKTeco Alarm Host

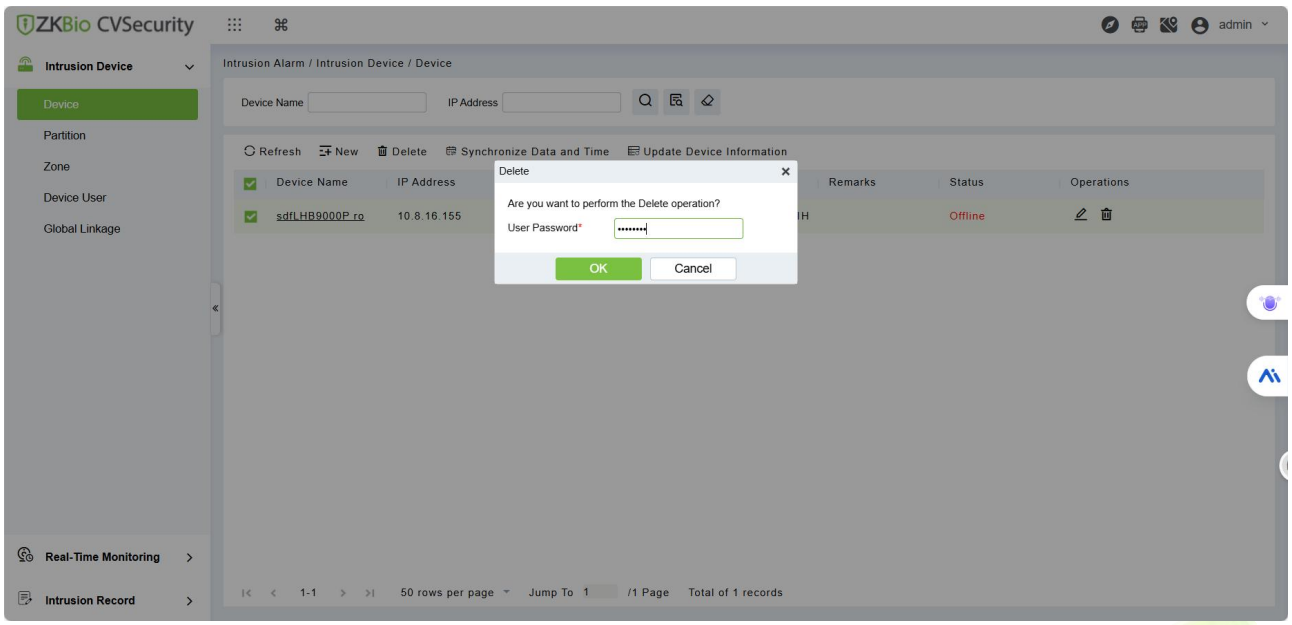
The following introduces the method of adding the alarm host of ZKTeco.Click **New.**



Parameter	Description
Manufacture	The Manufacturer current support BOSCH/RISCO/ZKTECO,Selected ZKTECO.
Model	Support IA01-HP01-01H and IA01-HP02-01H,Select according to your actual model.
Device Name	Customize the device name
User Registration Account	Registration Account for the alarm host
IP Address	IP Address of the alarm host
Remarks	You can make remarks about other information of the alarm host.

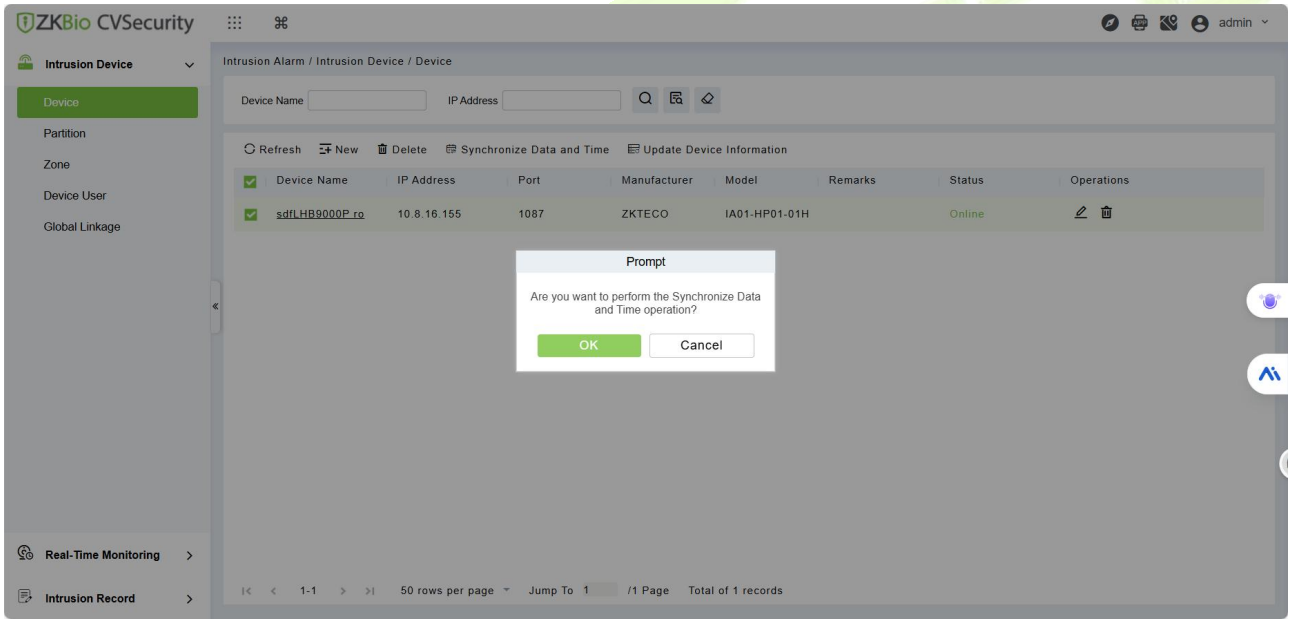
17.1.1.2Delete

You can select the device in the list and click "Delete".After entering the login password of the software, you can complete the deletion operation.



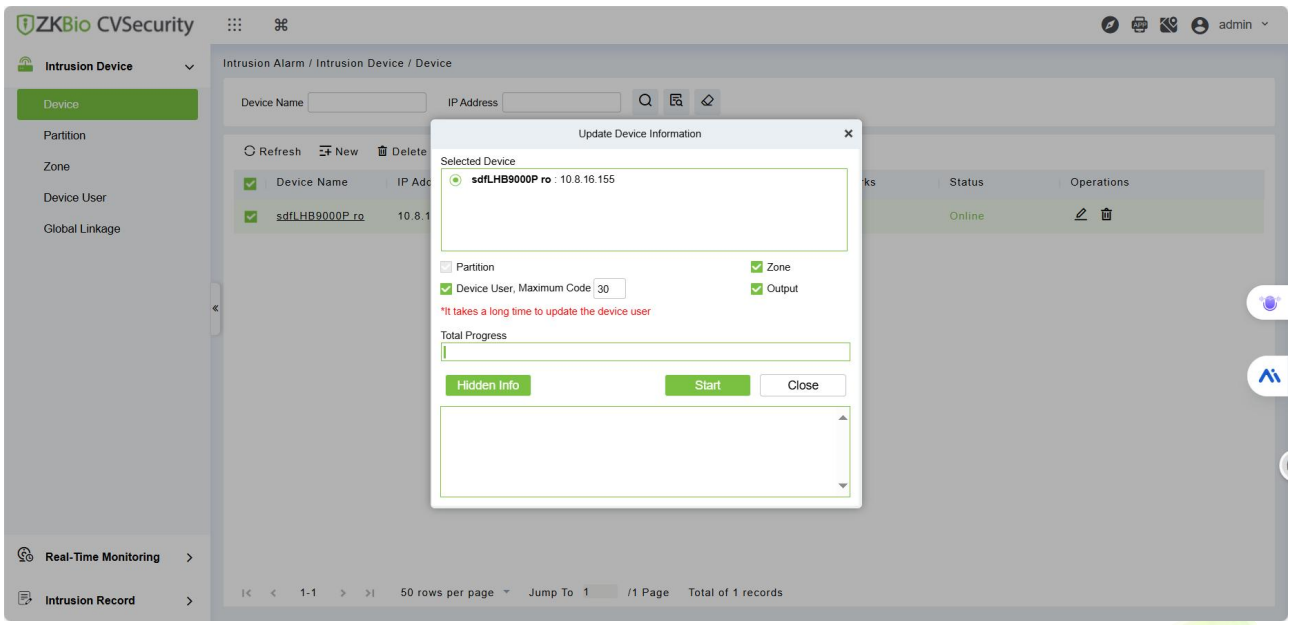
17.1.1.3 Synchronize Data and Time

Synchronize the server time to the alarm host. Currently, the devices of ZKTeco do not support this function.



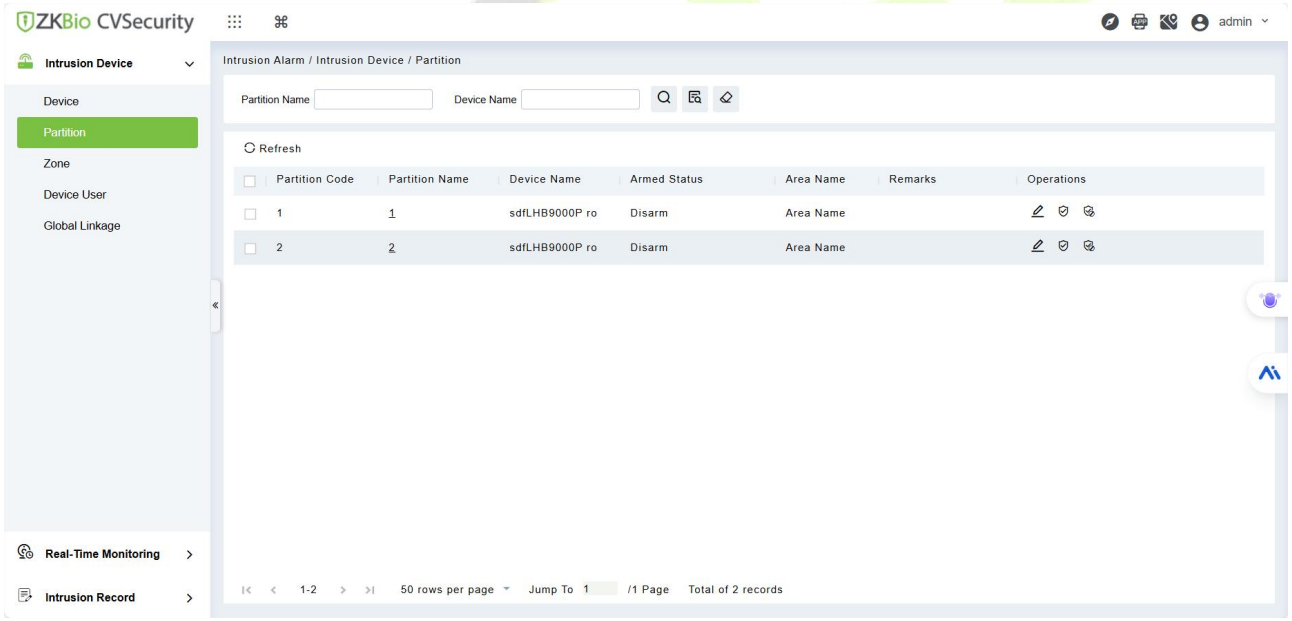
17.1.1.4 Update Device Information

Upload alarm host information, including partitions, zones, outputs, and user codes. This function is not supported by ZKTeco devices.



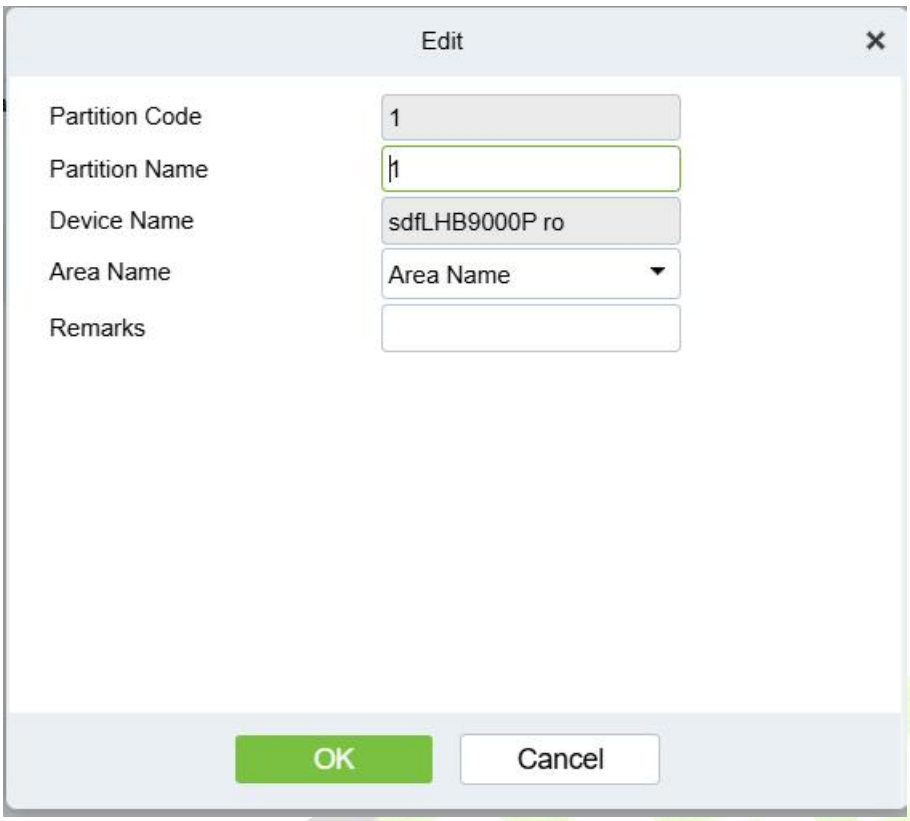
17.1.2Partition

Partition: A space, such as a front door, floor or hallway, is can assign multiple Points.After being connected to the alarm host, it will be automatically synchronized to the partition list.

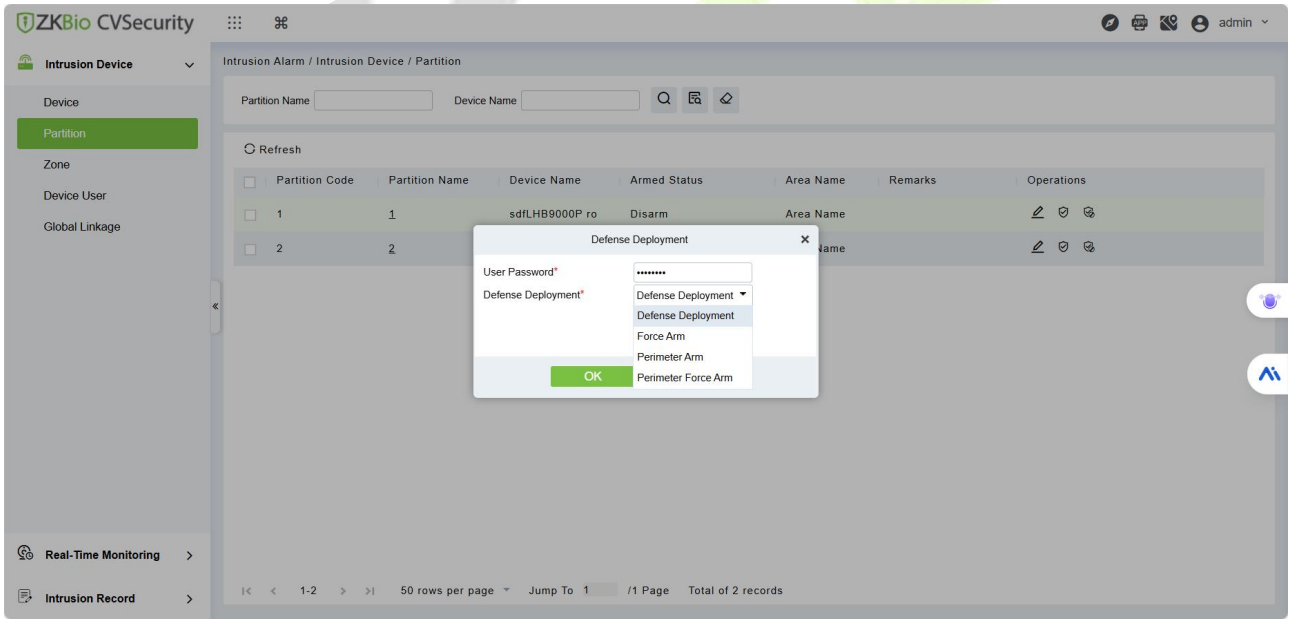


17.1.2.1Edit

After clicking "Edit", you can assign an area to this partition and add remarks for other information.



17.1.2.2Arming



User Password :ZKBio CVSecurity login Password.

Defense Deployment: It includes the following ways of setting up security.

- **Arming:** It means setting the alarm system to the working state, putting the detectors in the system (such as infrared detectors, door and window magnetic switches, etc.) in the normal monitoring state. When the detector detects an abnormal situation, it will send a signal to the alarm host. Once the host receives the signal, it will trigger an alarm. For example, before getting off work at night or going to bed, arm the alarm system of the office or home. In this

way, once an illegal intrusion or other abnormal situations occur, the system will give an alarm in a timely manner.

- **Forced arming:** It is a special way of arming. Usually, in some special situations, even if there are some situations where the system does not meet the normal arming conditions (such as a detector malfunctioning, not being ready, or someone not having left the armed area, etc.), it forces the alarm system to enter the armed state. Generally, specific operation permissions are required for forced arming to ensure that only authorized personnel can perform this operation and prevent misoperations or illegal operations. For example, in an emergency, it is necessary to quickly provide security protection for a certain area. Even if some devices have problems, the normal devices can be made to start working through forced arming to ensure safety.

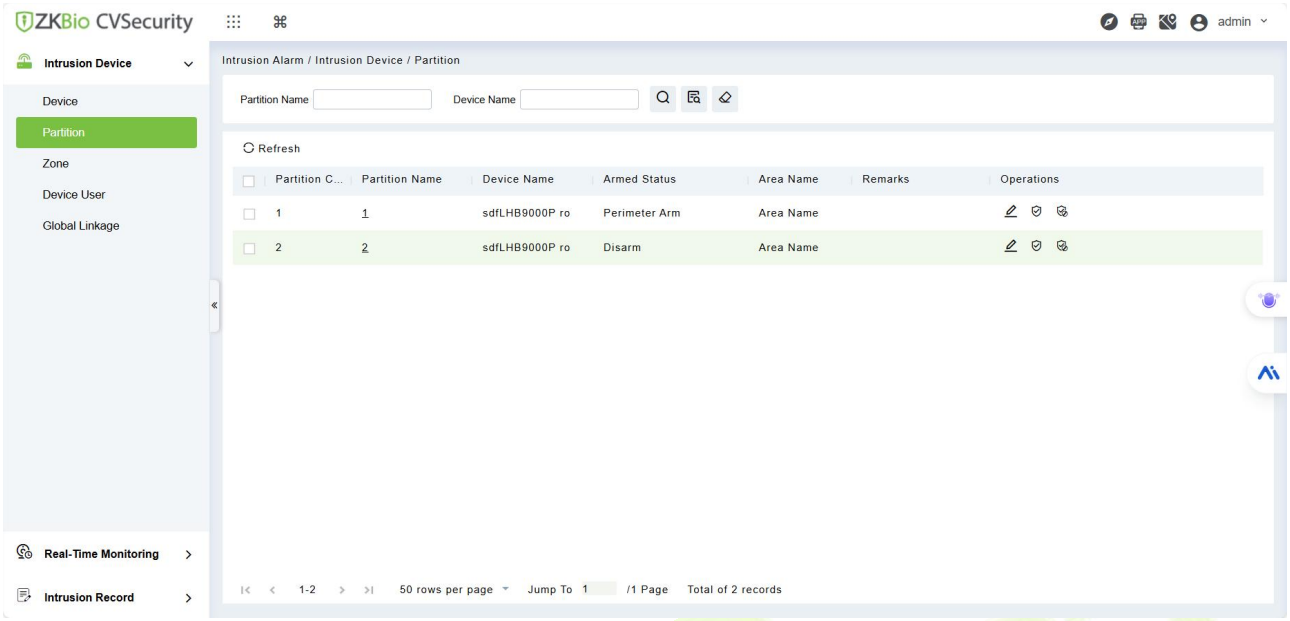
Note: Forced arming will automatically bypass the faulty protection zone. When the faulty protection zone is set as prohibited from being bypassed, forced arming will also fail.

- **Perimeter arming:** It means setting up alarm devices at the boundaries of a specific area, making the system enter the alert state to achieve comprehensive protection of the area and prevent unauthorized personnel from entering or leaving the specific area. When someone attempts to illegally cross the armed area, the corresponding detector will detect the abnormality and send a signal to the alarm host. Once the host receives the signal, it will trigger an alarm and notify the relevant personnel. For example, infrared beam detectors are installed around the enclosure of a residential community. When someone crosses the enclosure, the infrared light is blocked, and the detector will send out an alarm signal. Perimeter arming can be achieved through various methods, commonly including infrared beam detection, microwave detection, vibration sensing, video surveillance, etc.
- **Forced perimeter arming:** It is a special form of perimeter arming. Usually, when there are some situations where the system does not meet the normal arming conditions, such as a detector malfunctioning, not being ready, or someone not having left the perimeter armed area, etc., it still forces the perimeter alarm system to enter the armed state. Generally, specific operation permissions are required for forced perimeter arming to ensure that only authorized personnel can perform this operation and prevent misoperations or illegal operations. For example, in an emergency situation, such as when an important person is about to arrive at a certain place, it is necessary to quickly provide security protection for the perimeter of the place. Even if some detectors have problems, the normal devices can be made to start working through forced perimeter arming to ensure perimeter security.

Result verification:

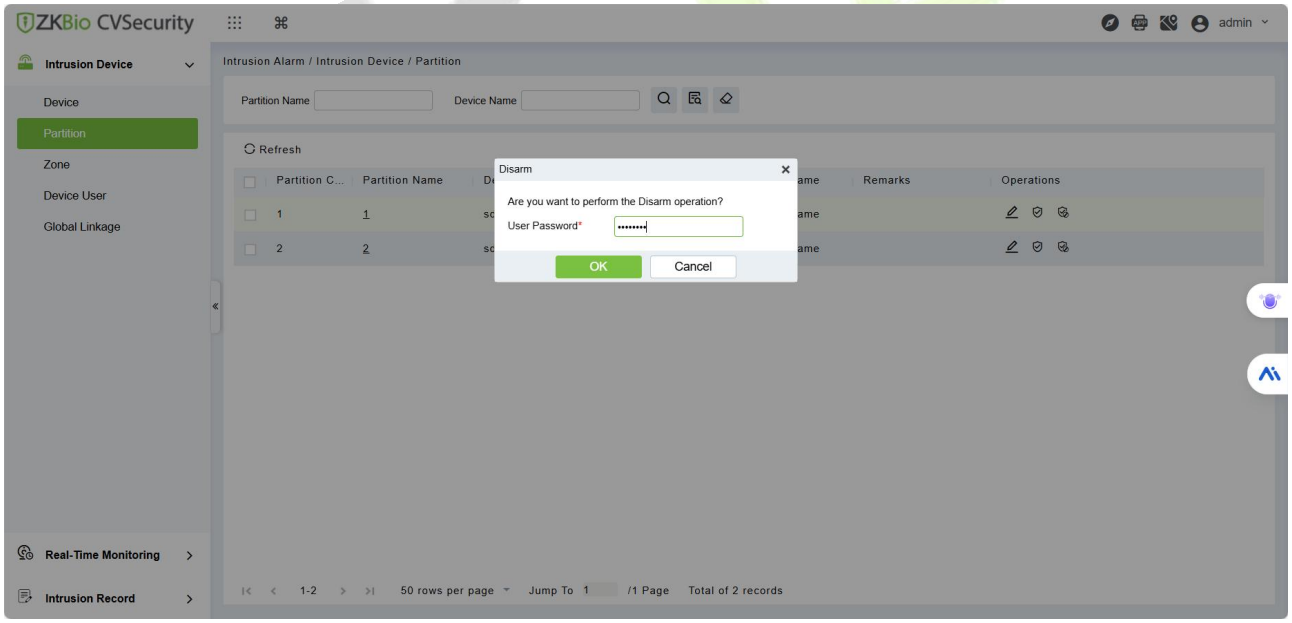
After successfully entering the ZKBio CVSecurity user password and the arming type, the status will

switch to the corresponding armed state.



17.1.2.3Disarming

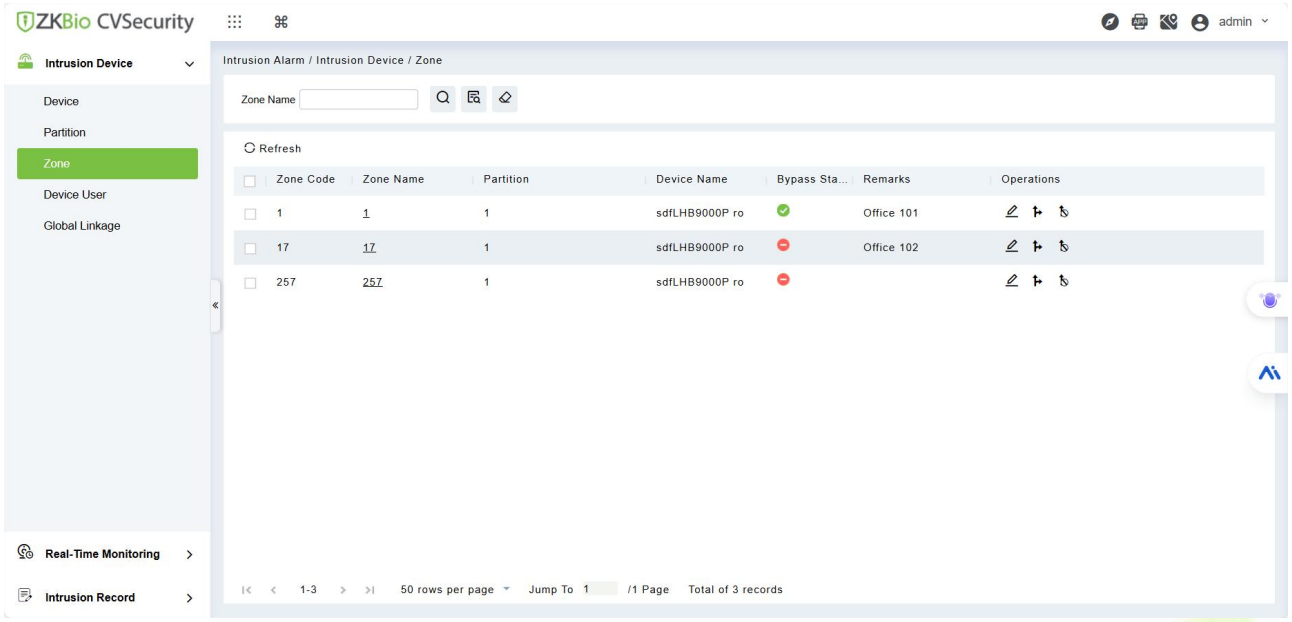
Disarming can be achieved by entering the ZKBio CVSecurity administrator password. After confirmation, the status in the list will change to "Disarm".



17.1.3Zone

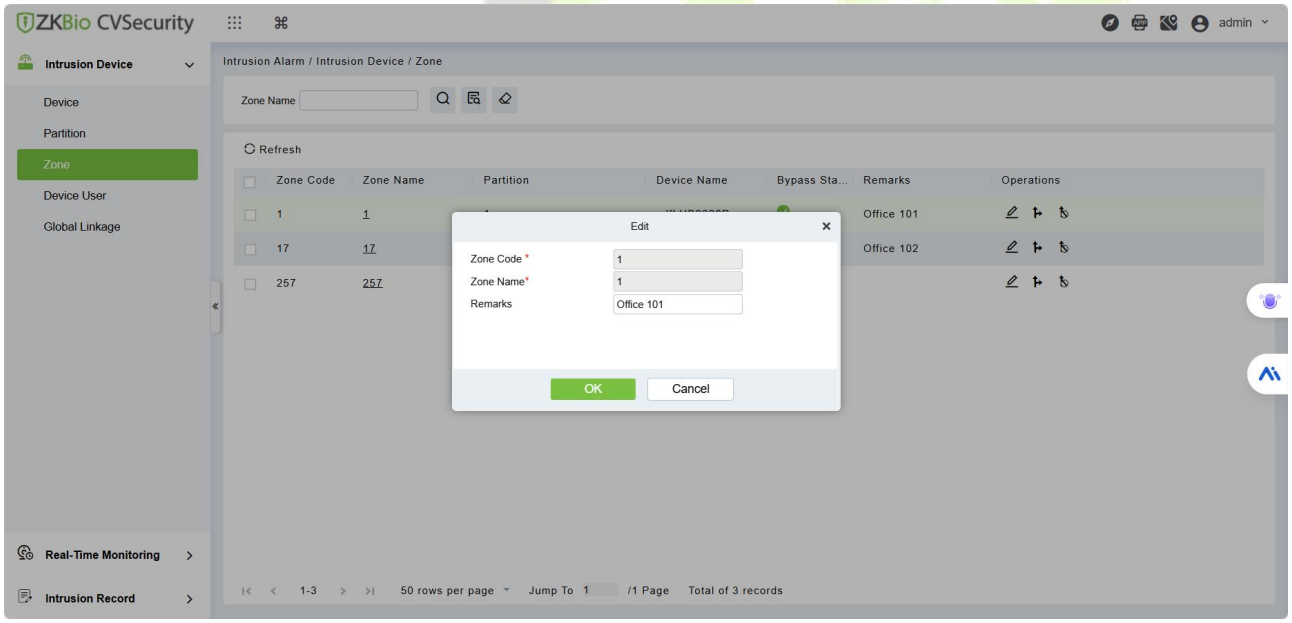
Zone: A protection zone refers to dividing the area that requires security precautions into several independent parts, and each part is a protection zone. The purpose of this division is to more accurately locate the alarm position, making it easier for management and maintenance.

Note: ZKBio CVSecurity can only perform editing and bypass management. If you need to adjust the partition to which the protection zone belongs, please configure it in the Device Web - Protection Zone Configuration menu.



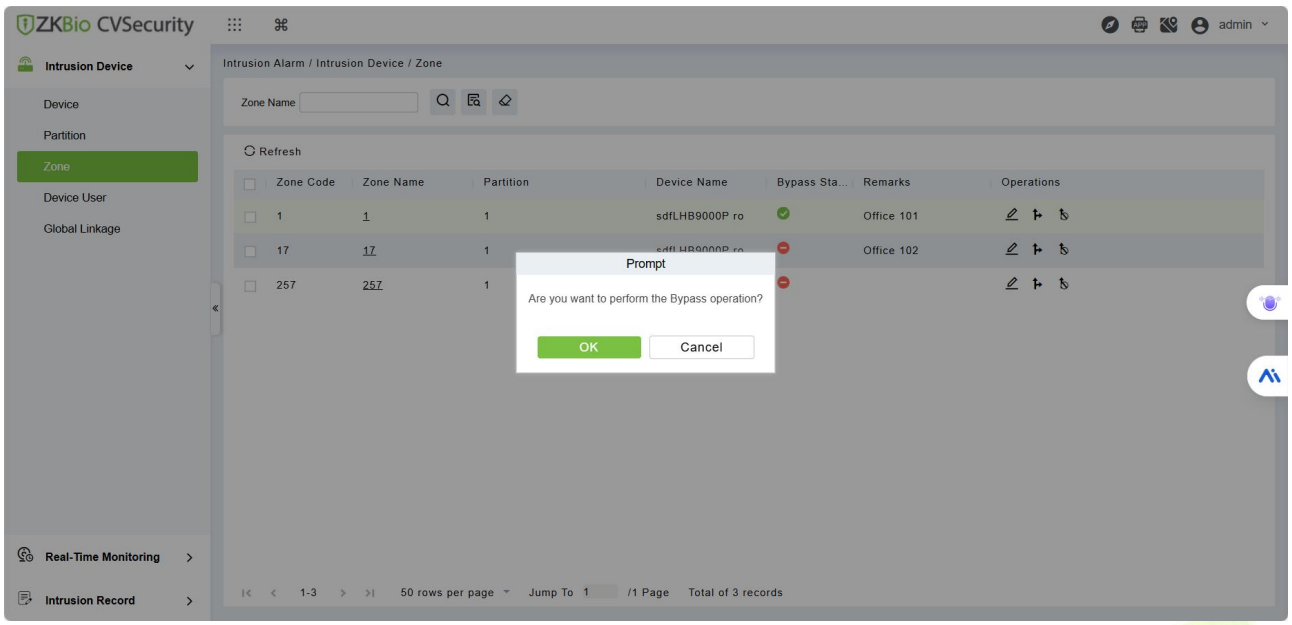
17.1.3.1 Edit

Click "Edit" to add remarks for the protection zone, such as noting the location of the protection zone or other explanations.



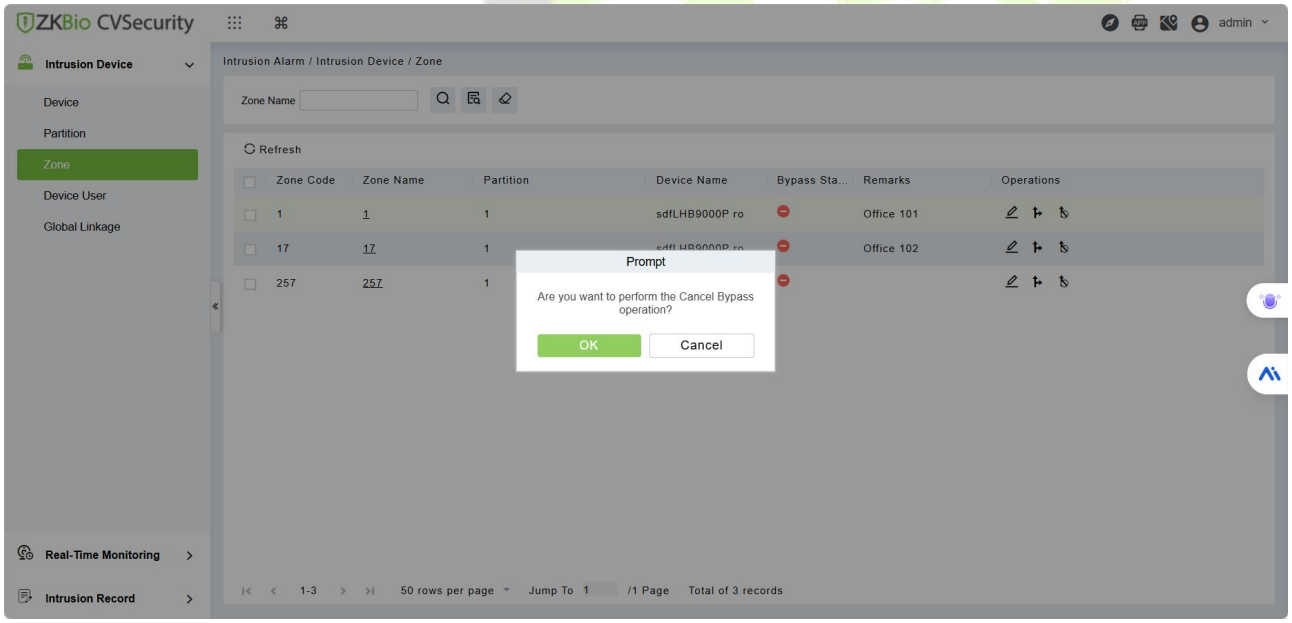
17.1.3.2 Bypass

Bypassing means isolating a certain detector or multiple detectors and protection zones from the alarm system temporarily, so that they do not participate in the normal alarm monitoring work when the system is armed. After clicking the "Bypass" button and confirming, the bypass status in the list will change to the enabled state.



17.1.3.3Cancel Bypass

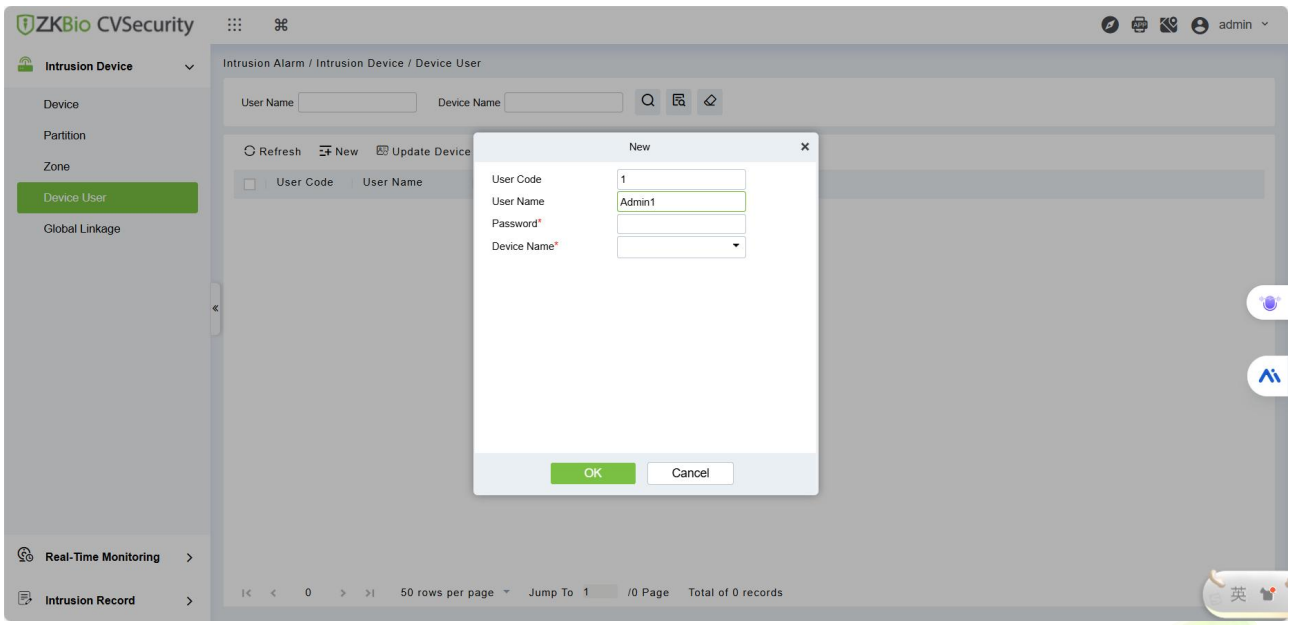
After clicking the "Cancel Bypass" button and confirming, the bypass status in the list will change to the disabled state.



17.1.4Device User

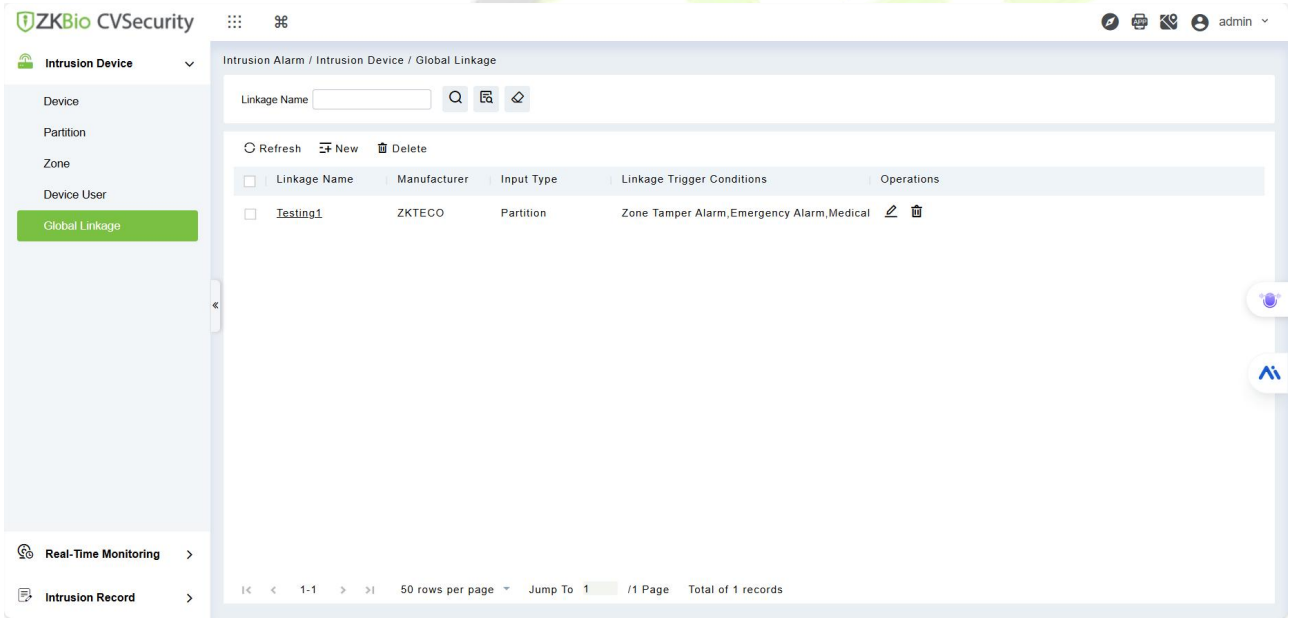
This menu is used to manage users and passwords for the alarm host device. After the configuration is completed, please click "Update Device User" to synchronize with the device.

Note: The current alarm host of ZKTeco does not support this function. You need to configure the user password on the web page of the device.



17.1.5Global Linkage

It is used to configure the system linkage. When the sensor detects an abnormality, it can trigger linkage with systems such as the alarm or video systems.



17.1.5.1New

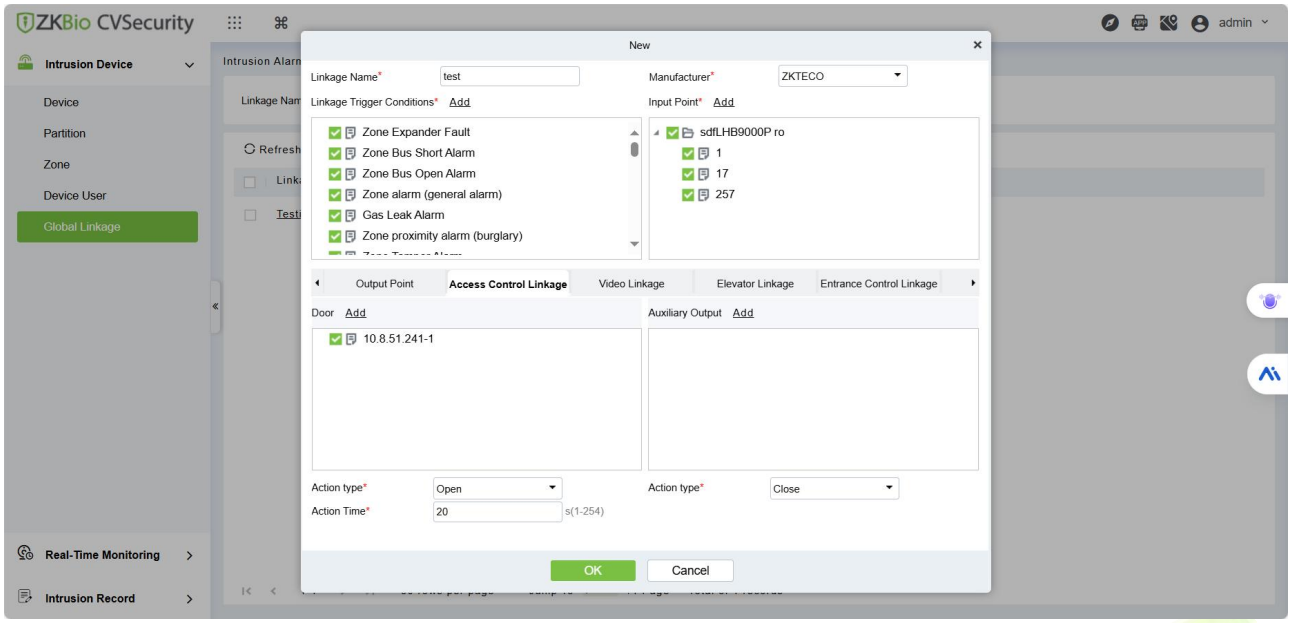
After clicking "New", you can configure the linkage task. As shown in the figure below:

Linkage Name: Customize the name of the linkage task.

Manufacturer: The brand of the alarm host. After selection, the Input Points of this brand will be automatically filtered.

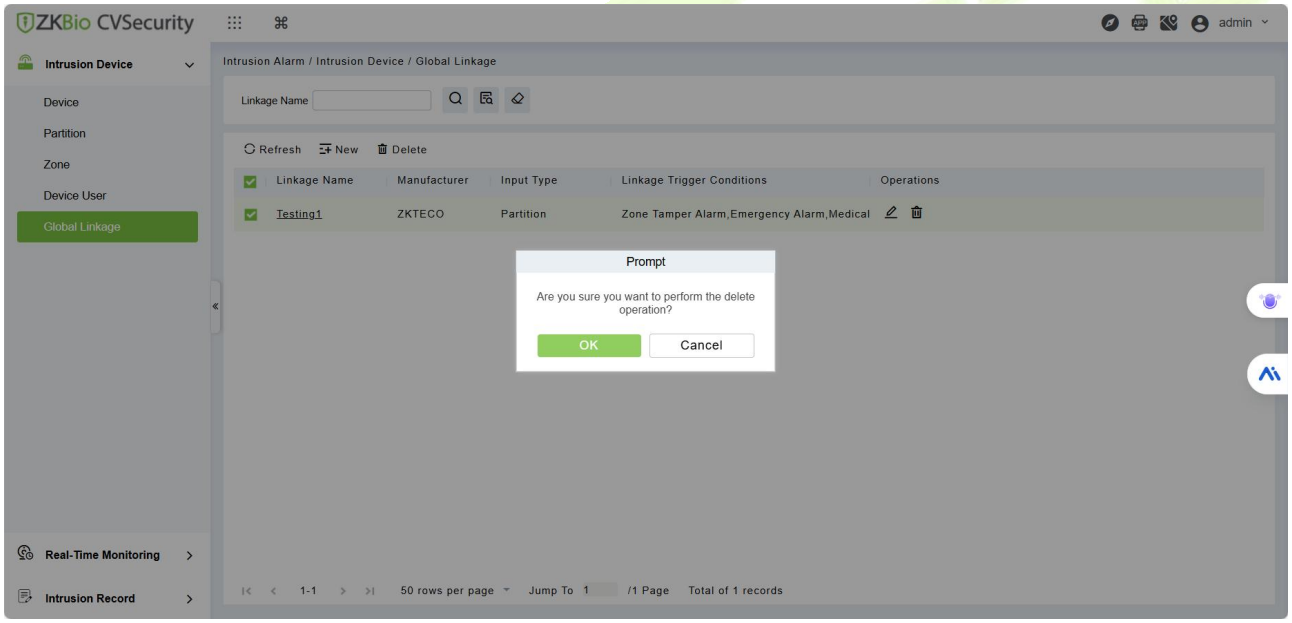
Linkage Trigger Conditions: Select partition or protection zone alarm events.

Input Point: Select the device or partition, which will be filtered according to the selected brand.



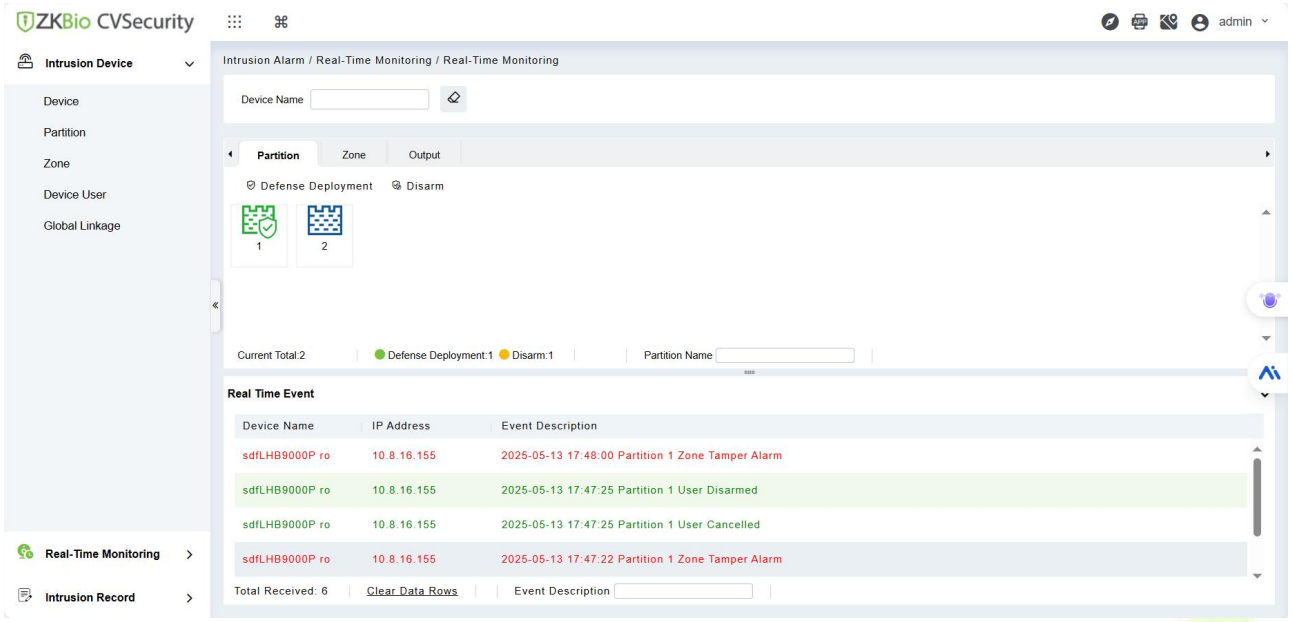
17.1.5.2Delete

You can select a linkage task from the list and click "Delete" to complete the deletion operation.



17.2 Real-time Monitoring

View the current device status or event content in real time.



17.2.1 Partition

Quick operations:

1) Click on a partition, then click the "Arm" or "Disarm" button on the quick action panel to perform the corresponding operation.

2) Select multiple partitions by clicking their icons, then use the "Arm" or "Disarm" buttons at the top to apply the action to all selected partitions.

The explanation of the status icons is as follows:

Parameter	Description
	It indicates that it is currently in the armed state.
	It indicates that it is currently in the disarmed state.

17.2.2Zone

Quick operations:

1) Click on a protection zone and then click "Bypass" or "Cancel Bypass" on the quick operation page to perform the quick operation.

2) Click on the icons of multiple protection zones to select them in batches, and then click the "Bypass" or "Cancel Bypass" button above to perform the quick operation.

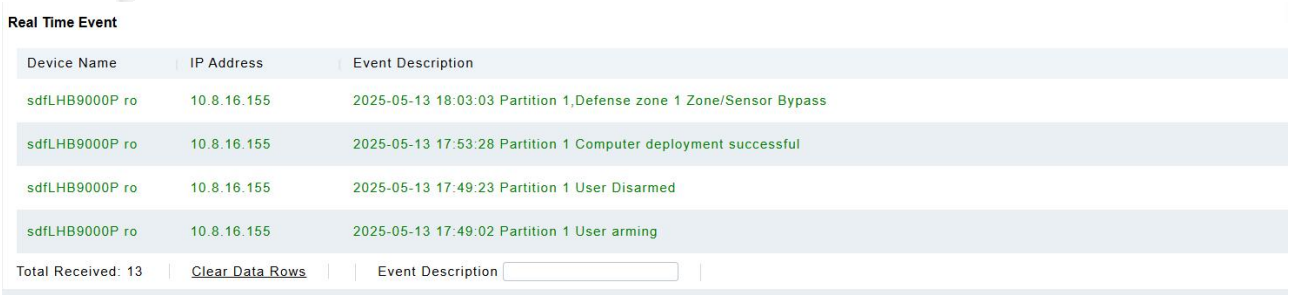
The explanation of the status icons is as follows:

Parameter	Description
	Not configured for bypass;
	Bypass has been configured.

17.2.3Real Time Event

View the current event in real time.

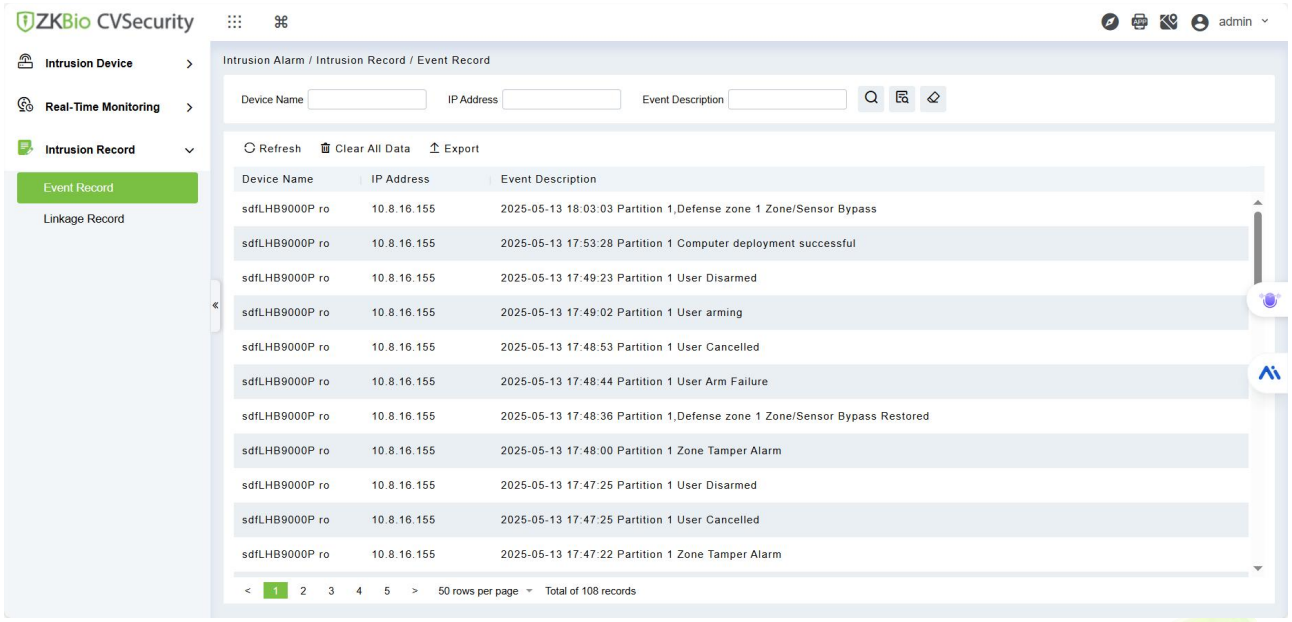
- **Clear Data Rows:** Clicking it will delete all events on the current page.



17.3 Intrusion Record

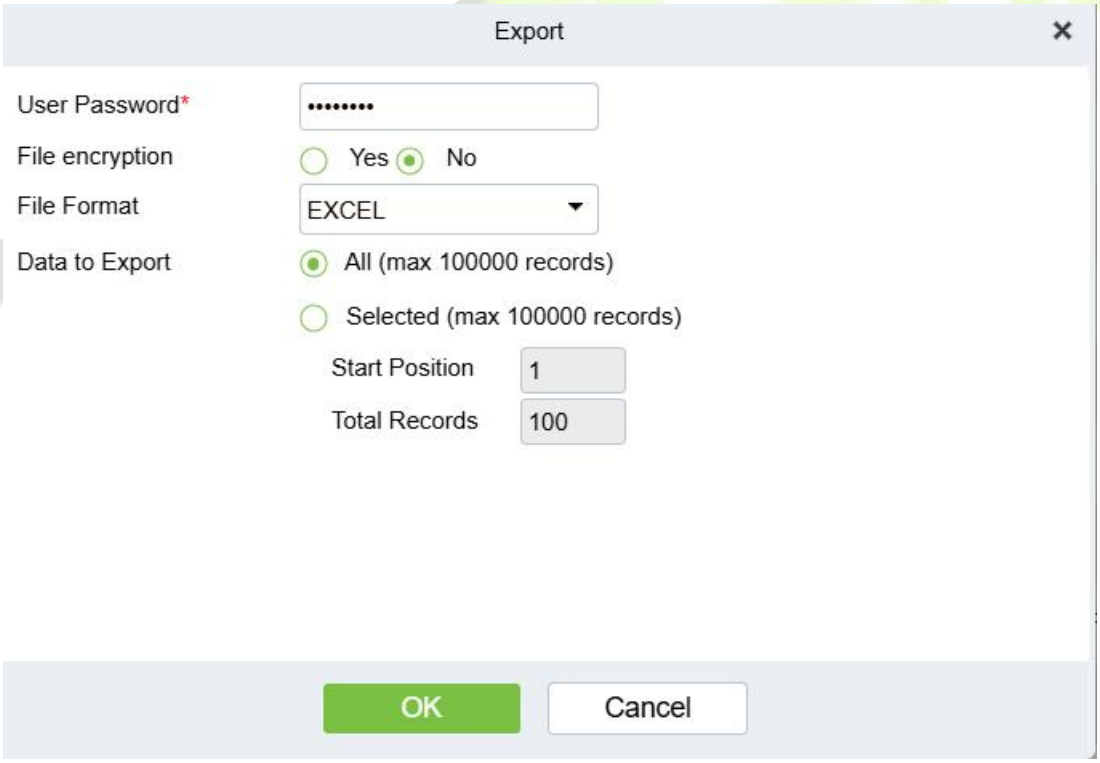
17.3.1Event Record

View the event logs of all alarm hosts.



17.3.1.1 Export

After clicking "Export", enter the user password and basic configuration, and then you can export the report.



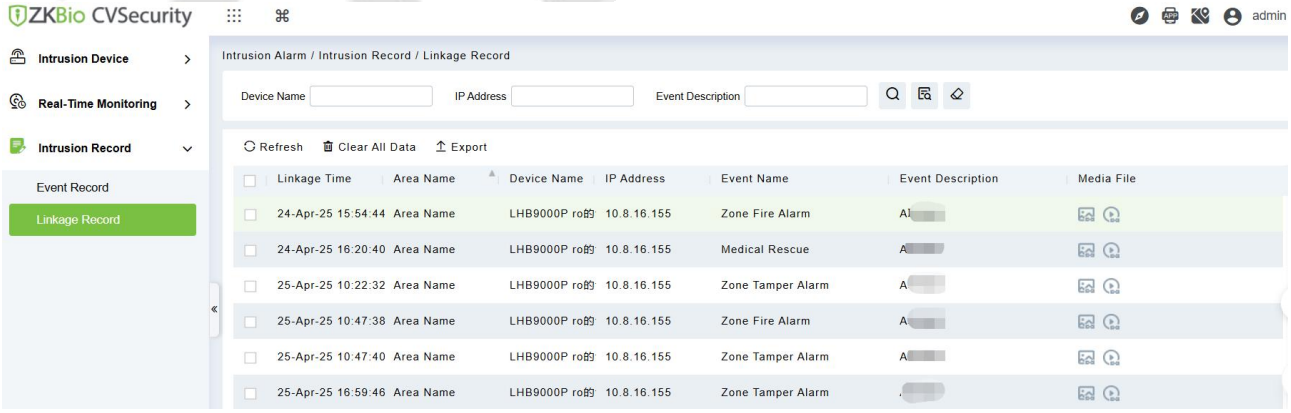
- **Result verification:**

The exported report is shown in the following figure:

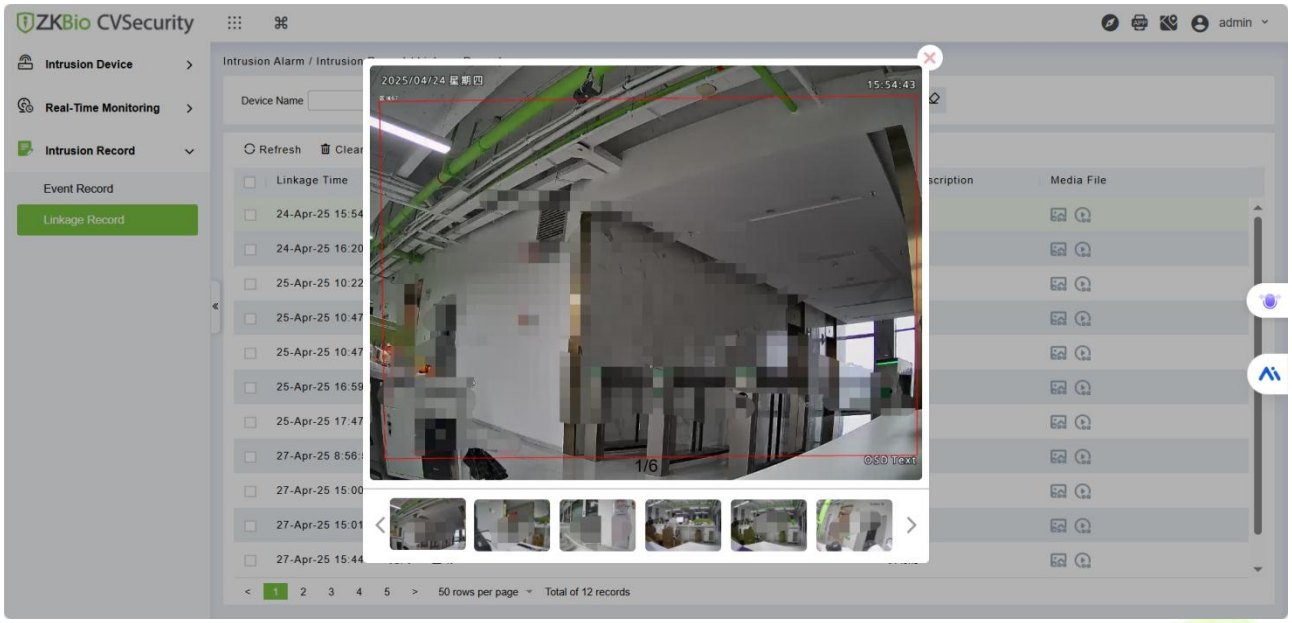
Event Record		
Device Name	IP Address	Event Description
sdfLHB9000P ro	10.8.16.155	2025-05-13 18:03:03 Partition 1,Defense zone 1 Zone/Sensor Bypass
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:53:28 Partition 1 Computer deployment successful
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:49:23 Partition 1 User Disarmed
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:49:02 Partition 1 User arming
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:48:53 Partition 1 User Cancelled
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:48:44 Partition 1 User Arm Failure
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:48:36 Partition 1,Defense zone 1 Zone/Sensor Bypass Restored
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:48:00 Partition 1 Zone Tamper Alarm
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:47:25 Partition 1 User Disarmed
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:47:25 Partition 1 User Cancelled
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:47:22 Partition 1 Zone Tamper Alarm
sdfLHB9000P ro	10.8.16.155	2025-05-13 17:45:39 Partition 1 Time/Date Reset
sdfLHB9000P ro	10.8.16.155	2049-09-14 01:37:17 Partition 2 User Disarmed
sdfLHB9000P ro	10.8.16.155	2049-09-14 01:11:29 Partition 2 User arming
sdfLHB9000P ro	10.8.16.155	2049-09-14 01:10:52 Partition 1,Defense zone 1 Zone/Sensor Bypass
sdfLHB9000P ro	10.8.16.155	2049-09-14 01:10:08 Partition 1,Defense zone 1 Zone/Sensor Bypass Restored
sdfLHB9000P ro	10.8.16.155	2049-09-14 00:58:32 Partition 1 Computer deployment successful
sdfLHB9000P ro	10.8.16.155	2049-09-14 00:57:59 Partition 1,Defense zone 1

17.3.2Linkage Record

View all linkage records.

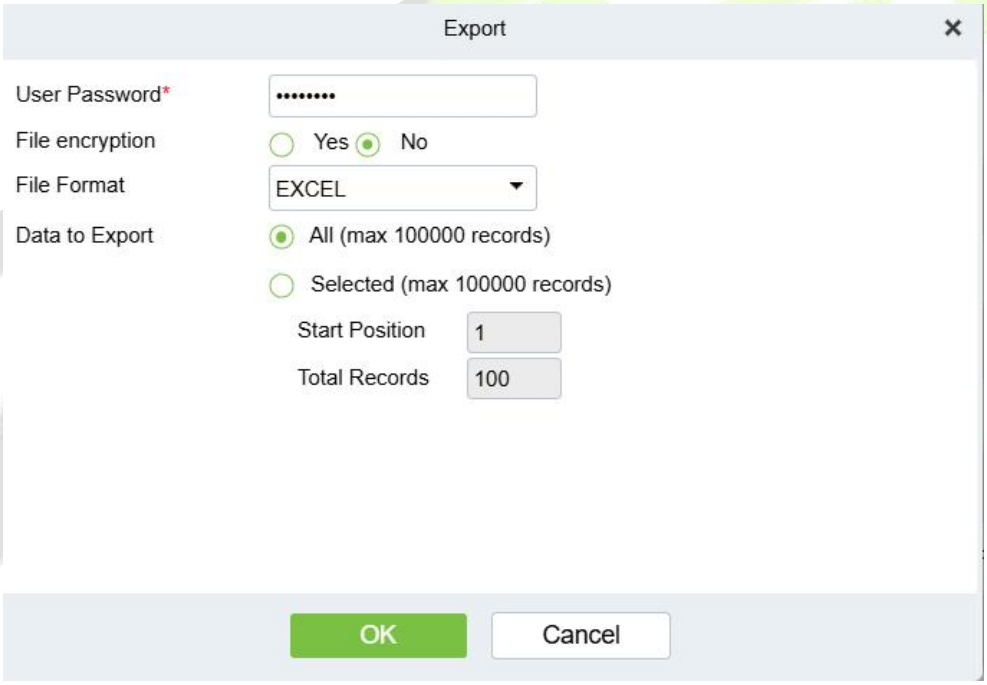


Media File: You can click the icon  in the list to view the pictures or videos captured by the video linkage.



17.3.2.1 Export

After clicking "Export", enter the user password and basic configuration, and then you can export the report.



● Result verification:

The exported report is shown in the following figure:

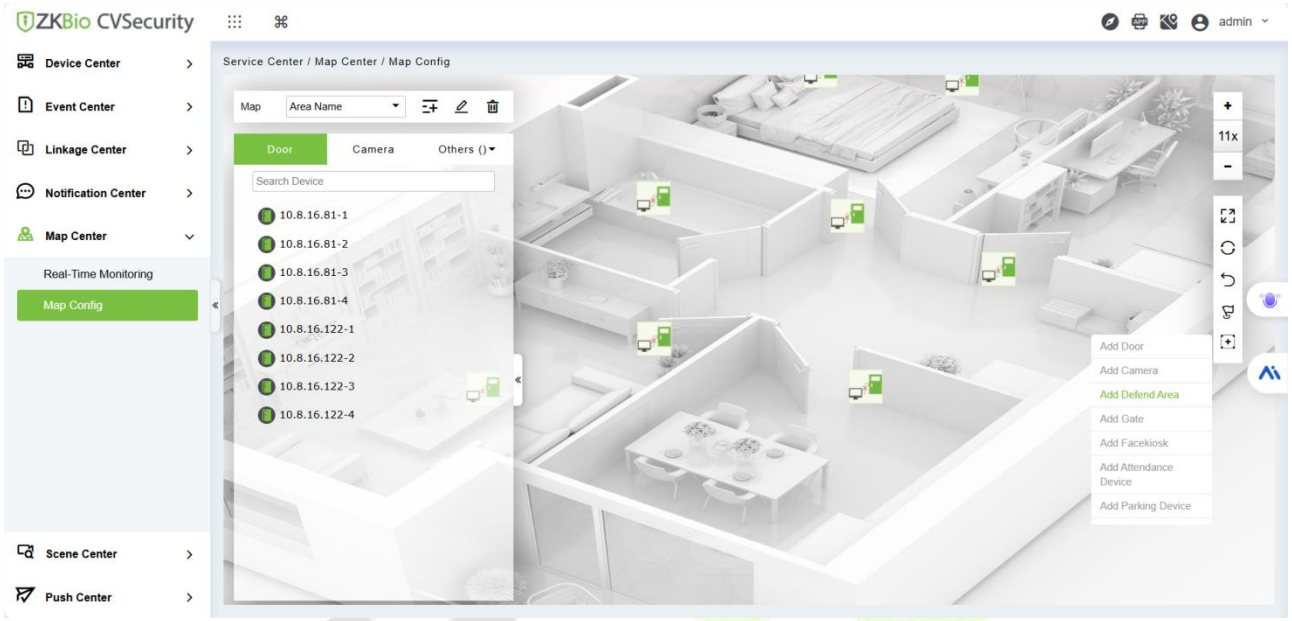
Linkage Record

Linkage Time	Area Name	Device Name	IP Address	Event Name	Event Description
2025-04-24 15:54:44	Area Name	LHB9000P ro	10.8.16.155	Zone Fire Alarm	A Linkage
2025-04-24 16:20:40	Area Name	LHB9001P ro	10.8.16.155	Medical Rescue	A Linkage
2025-04-25 10:22:32	Area Name	LHB9002P ro	10.8.16.155	Zone Tamper Alarm	A Linkage
2025-04-25 10:47:38	Area Name	LHB9003P ro	10.8.16.155	Zone Fire Alarm	A Linkage
2025-04-25 10:47:40	Area Name	LHB9004P ro	10.8.16.155	Zone Tamper Alarm	A Linkage
2025-04-25 16:59:46	Area Name	LHB9005P ro	10.8.16.155	Zone Tamper Alarm	A Linkage
2025-04-25 17:47:52	Area Name	LHB9006P ro	10.8.16.155	Medical Rescue	A Linkage
2025-04-27 08:56:54	Area Name	LHB9007P ro	10.8.16.155	Zone Tamper Alarm	A Linkage
2025-04-27 15:00:20	Area Name	LHB9008P ro	10.8.16.155	Medical Rescue	A Linkage
2025-04-27 15:01:34	Area Name	LHB9009P ro	10.8.16.155	Medical Rescue	A Linkage
2025-04-27 15:44:28	Area Name	LHB9010P ro	10.8.16.155	Medical Rescue	A Linkage
2025-04-27 15:45:08	Area Name	LHB9011P ro	10.8.16.155	Medical Rescue	A Linkage

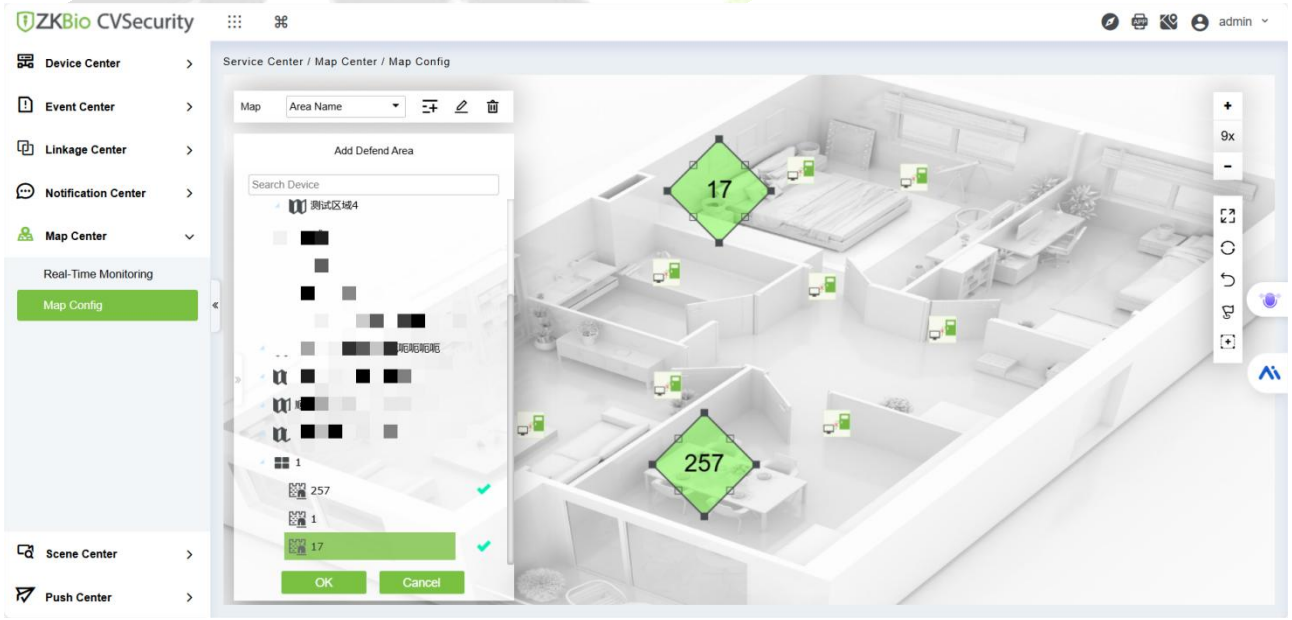
17.4 Real Time Monitoring on Map

17.4.1 Map Configure

Under the menu of **Service Center -> Map Center -> Map Configure,** in the right-side menu, first click the Add icon and select Add Defend Area.

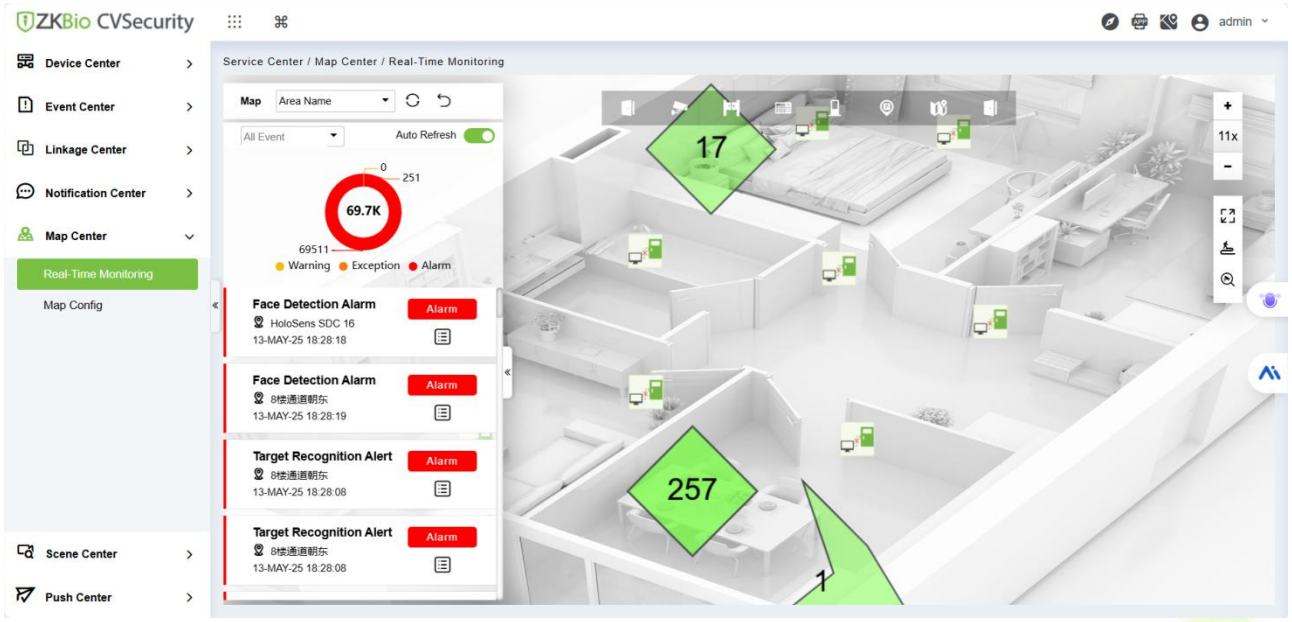


On the left side, select the corresponding protection area under "Add Defend Area", drag it onto the map, adjust the position and size of the protection area, and click "OK" to complete the configuration and save it.



17.4.2 Real Time Monitoring

Go to **Service Center -> Map Center -> Real Time Monitoring** to view the status of the protection zone in real time. When an abnormality occurs, the protection zone on the map will flash red continuously.

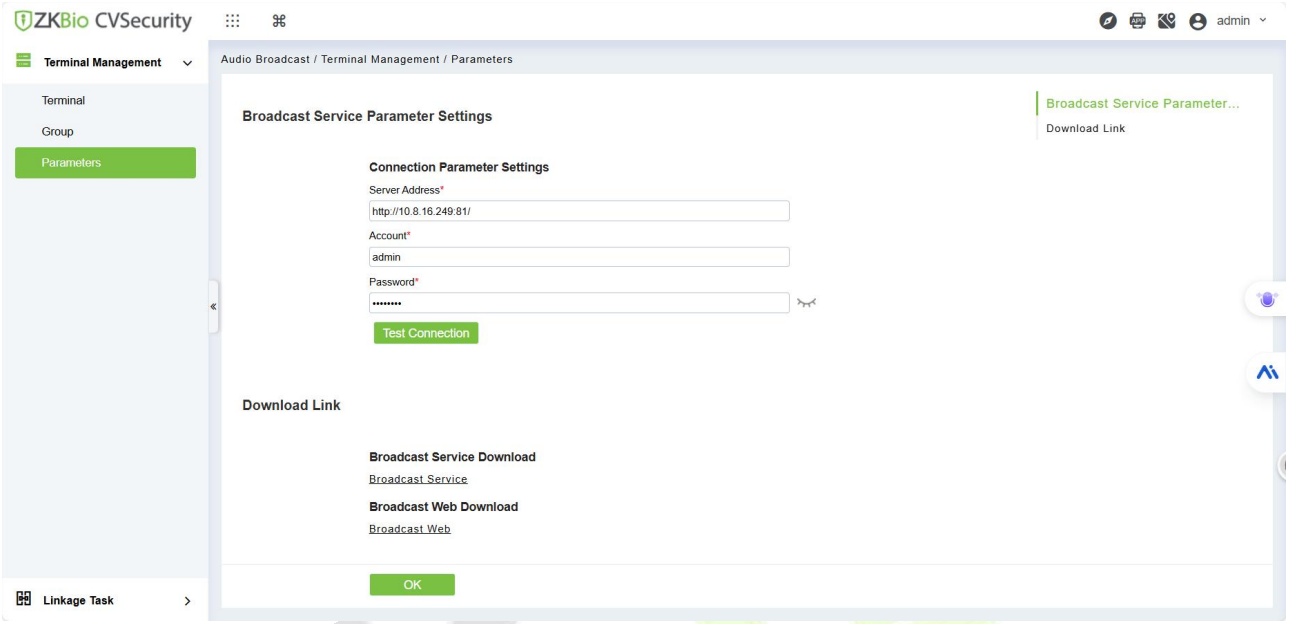


18 Audio Broadcast

This module is mainly used for synchronizing broadcast terminals and configuring linkage tasks.

Operation Step :

Step 1 : Configure IP Broadcast Server Address

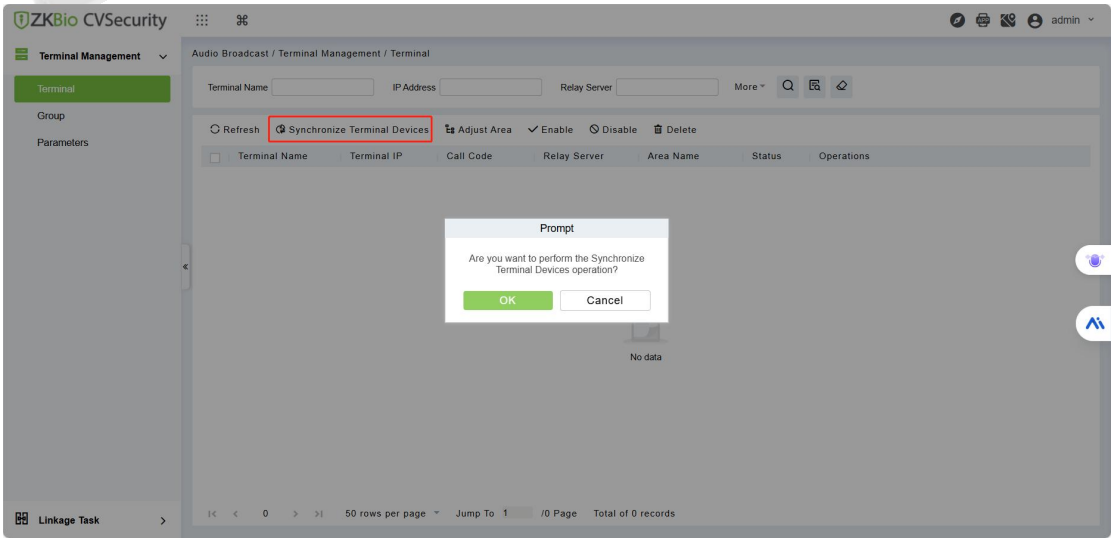


- **Server Address:** The server address of IP Broadcast. Please note that the format is http://broadcast ip: port.
- **Account:** IP Broadcast Web login account
- **Password**: IP Broadcast Web login password

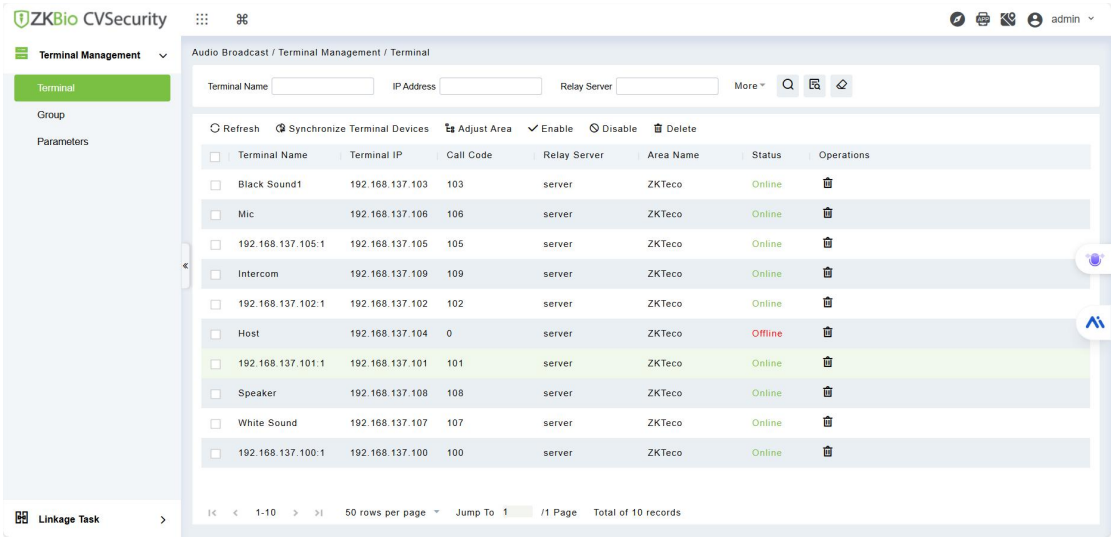
Note: You need to download, install and register the Broadcast Service and Broadcast Web System. For more details, you can refer to the IP Broadcast User Manual.

Step 2: Synchronize the broadcast terminal to ZKBio CVSecurity

Go to the Terminal Management->Terminal menu and click on Synchronize Terminal Device

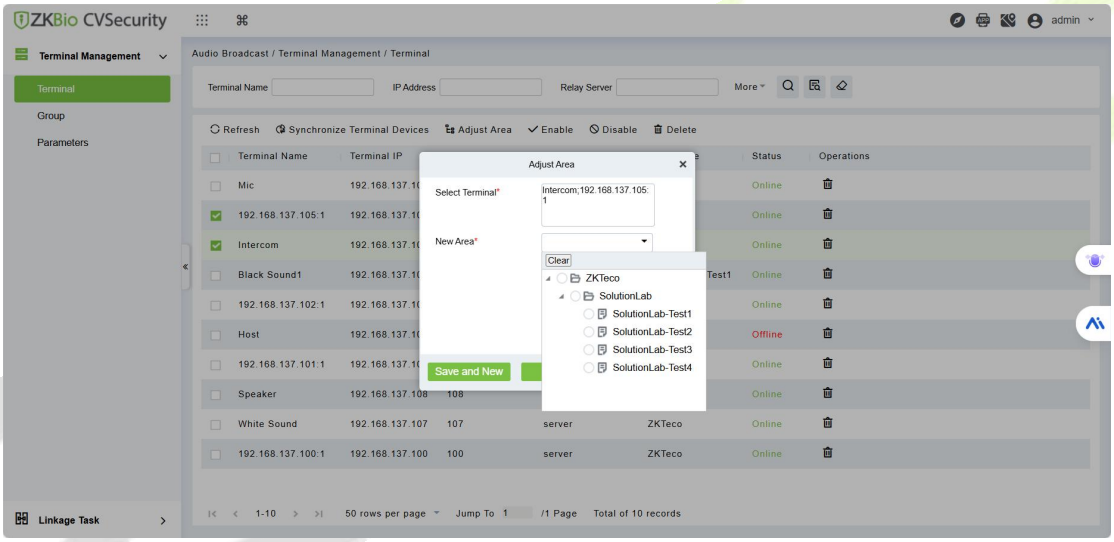


Click **OK** to automatically synchronize the terminal to ZKBio CVSecurity.



- **Control space**

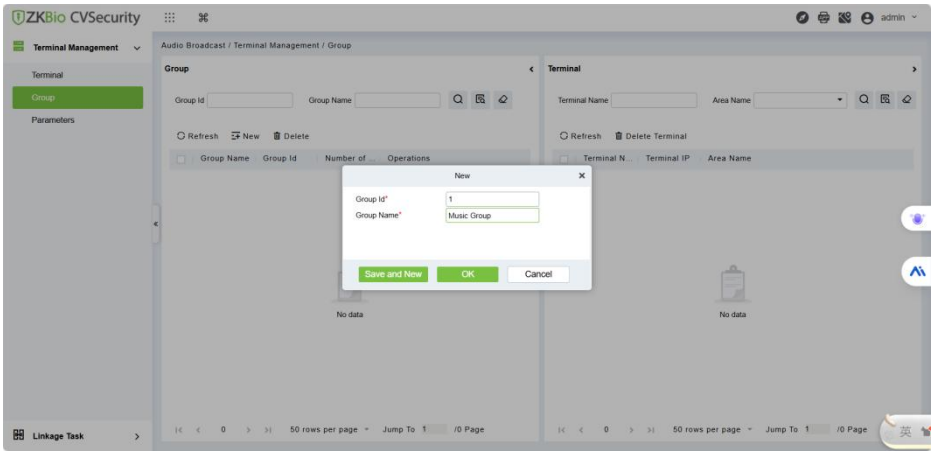
The adjustment area is easy to display in the center of the map



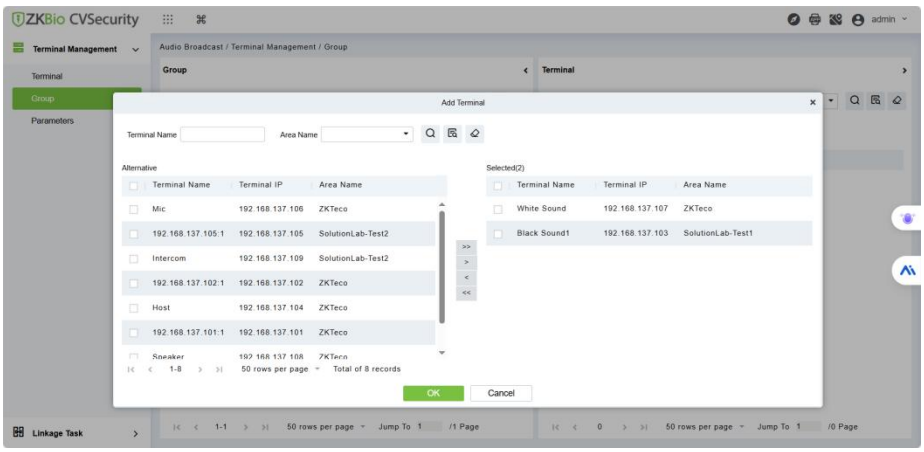
- **Add groups**

Grouping facilitates management and can be used for linked task selection and group playback;

Go to **Terminal Management-> Group** and click **New** to create a group.



Click on the group list  to add a terminal to the group. Click OK to display it in the right list.

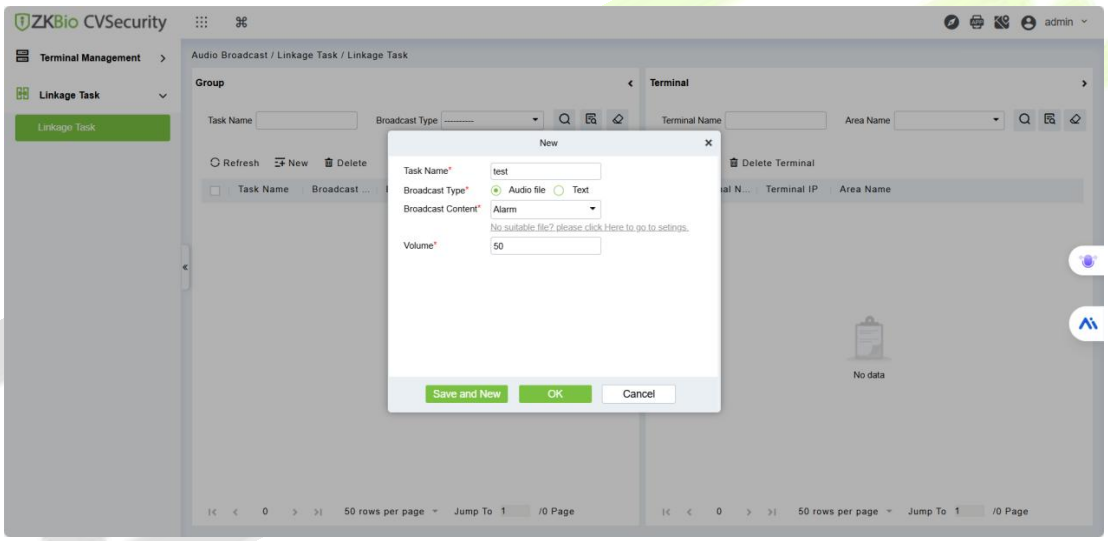


Step 3 :Configure the linked task

① **Voice tasks**

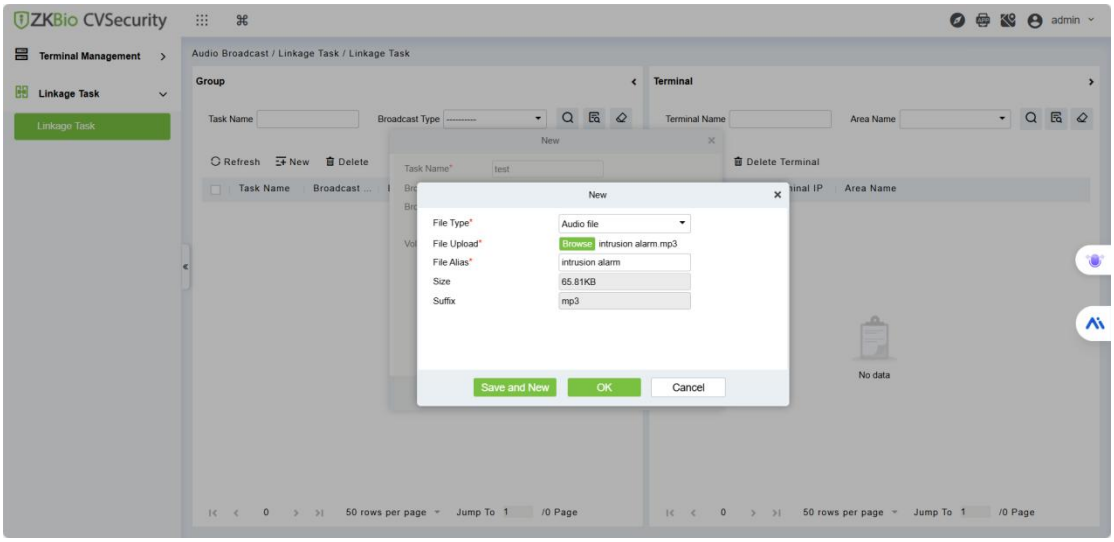
Create a voice task, upload the audio file, and when the linkage condition is triggered, the audio file will be played.

Linkage Task Click **New**, Broadcast Connect select the audio file.



If there are five audio files, you can click 

to **upload the audio file**.



② Text tasks

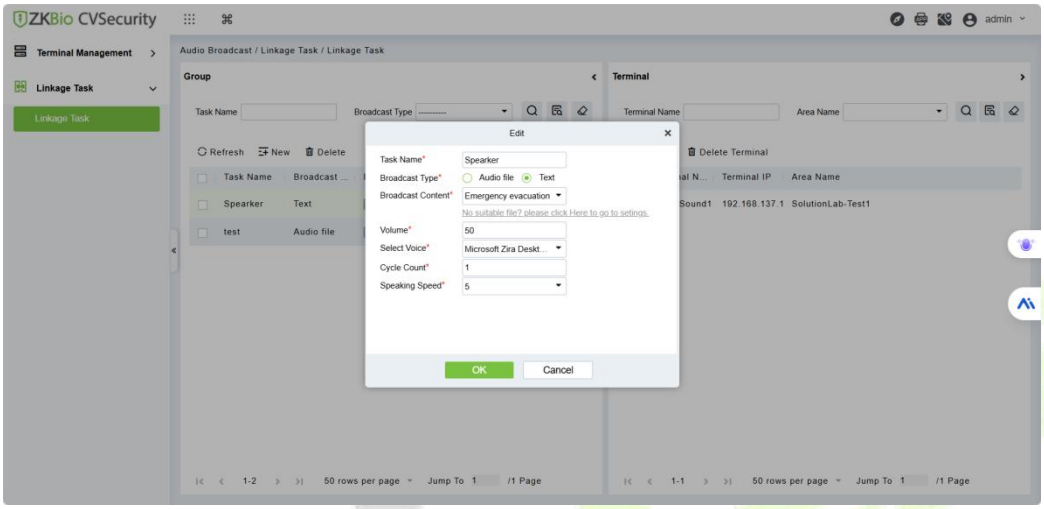
Click **New**, Broadcast Type select Text to start the text task.

Broadcast Content: Select the text file

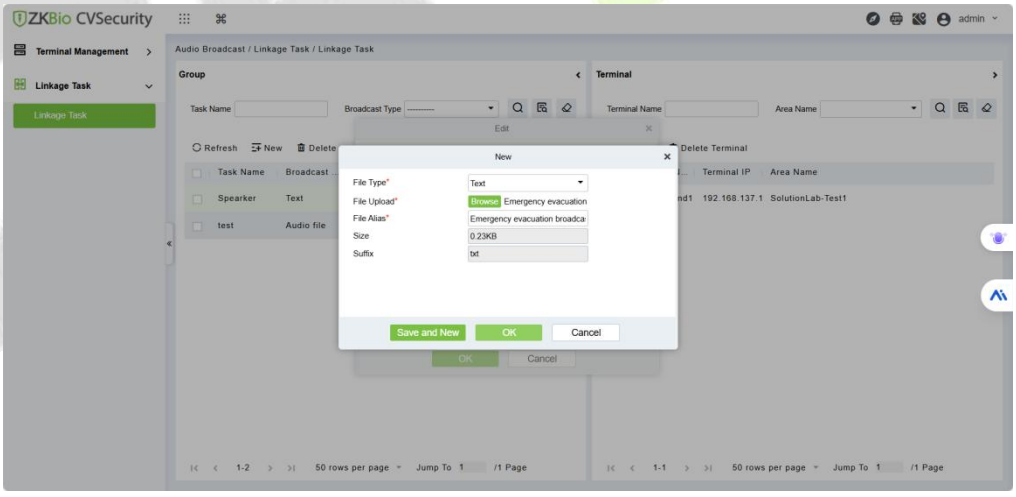
Select Voice: Select the sound to play the text content. Currently, only Chinese or English is supported.

Cycle Count: Number of times to play the loop

Speaking Speed: Select the speech rate, which is set to 5 by default. The larger the value, the faster the speech rate.

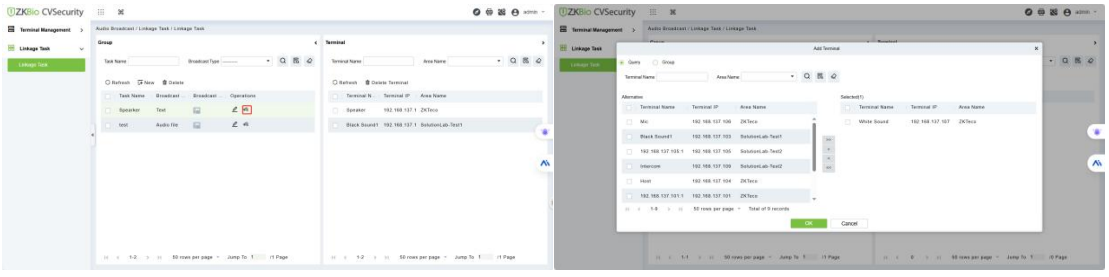


If there is no text file, you can click No suitable file? please click Here to go to setings. to add text content, such as fire emergency broadcast guidance, you can enter escape precautions and other content in the text, when the fire triggers, the text will automatically play the content (text to voice)



③ Assign the task to the terminal

Click the icon  in the list to assign a terminal to the task.

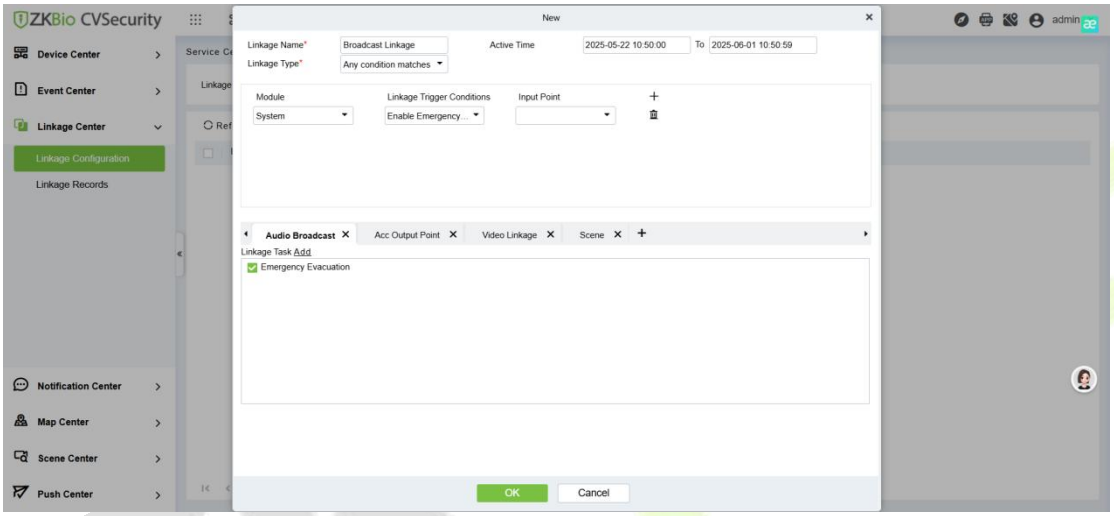


Step 4: Configure broadcast linkage

Go to **Service Center->Linkage Configuration**, click New, you can select the corresponding trigger conditions and output actions.

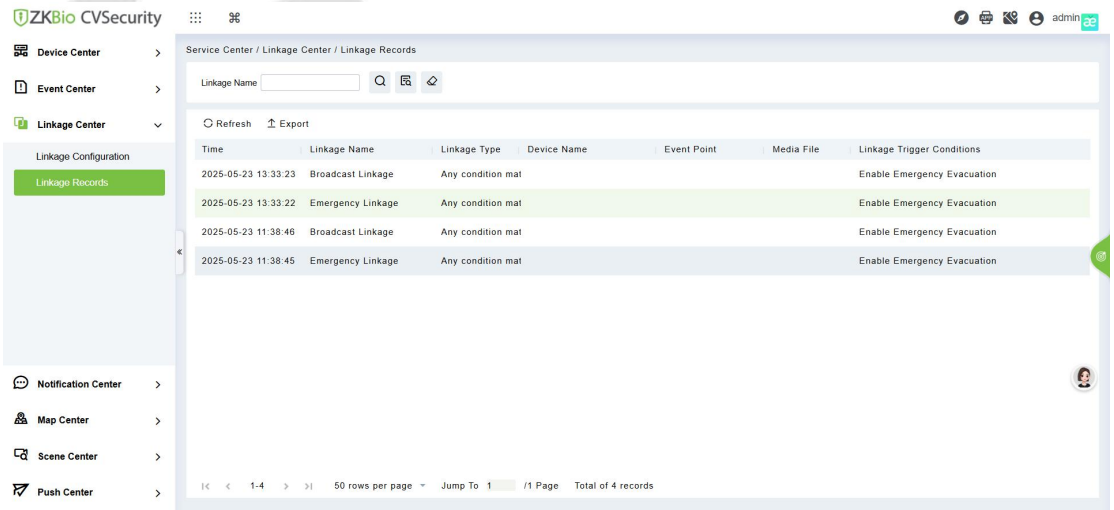
- **Active Time:** Time of linkage activation
- **Linkage Type:** You can choose any condition match or multiple conditions combination; Any condition match means that when any trigger condition matches, the linkage action output will start; Multiple conditions combination means that the linkage action output will only be output when all selected trigger conditions match.

As shown in the figure below: In the example, System module-Enable Emergency Evacuation is selected as the trigger condition; Audio Broadcast Module-Emergency Evacuation Text Task (text task configured in Step 6) is selected as the output action



- **Result verification:**

When the condition is triggered, the corresponding action will be output in conjunction with it. As shown in the figure below, after the emergency assembly is opened, the broadcast system will automatically start the emergency escape guidance and convert the text into voice.



19 Energy Saving

The module automatically controls lighting and air conditioning in meeting rooms and offices based on occupancy detected by smart sensors.
When rooms are unoccupied, systems automatically shut down to reduce energy consumption and costs, move towards a greener future.

Note: Compatible only with Lifesmart IoT devices.

19.1 Device Management

The user needs to first add a gateway, and then add terminal devices to it.

19.1.1 Gateway

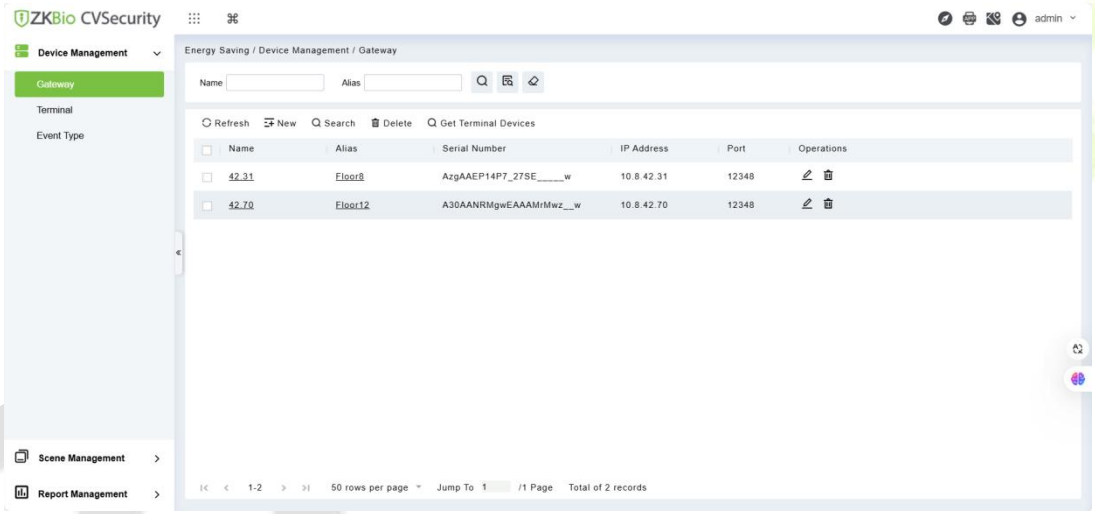


Figure 19- 1 Gateway

19.1.1.1 New

Click on **Device Management > Gateway > New** enter the required details and then click **OK** to add a new gateway.

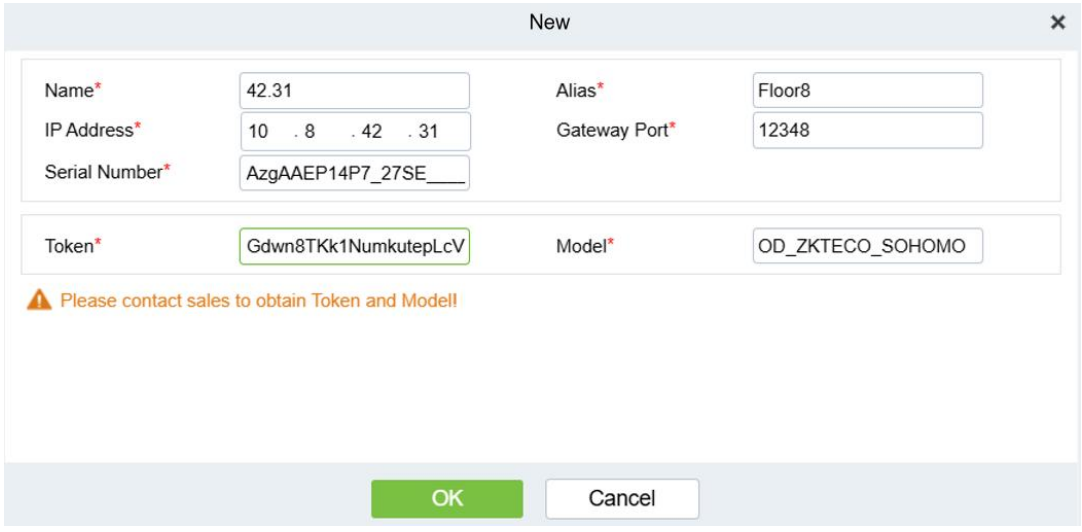


Figure 19- 2 New Gateway

Parameter	Description
Name	Enter name of the gateway
Alias	Enter the gateway's alias, which can be displayed in the ZKBio Zexus APP
IP Address	Enter IP address of the gateway
Gateway Port	Gateway port number, default is 12348
Serial Number	The serial number of the gateway .
Token	To obtain the Token value, please get in touch with our sales team.
Model	To obtain the Model value, please get in touch with our sales team.

Table 19- 1 Linkage parameters

19.1.1.2Search

Click **Search** allows you to add gateway through the search function.

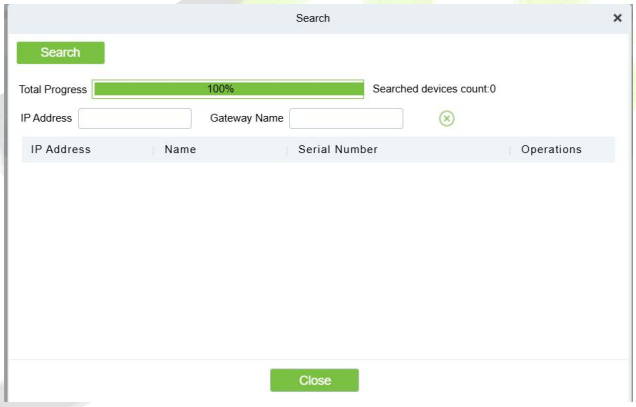


Figure 19- 3 New Gateway

Note: *ZKBio CVSecurity and the gateway must be in the same network segment to be searched out,For gateways in the different network segments,they can be added manually.*

19.1.1.3Delete

Click **Delete** removes the gateway.

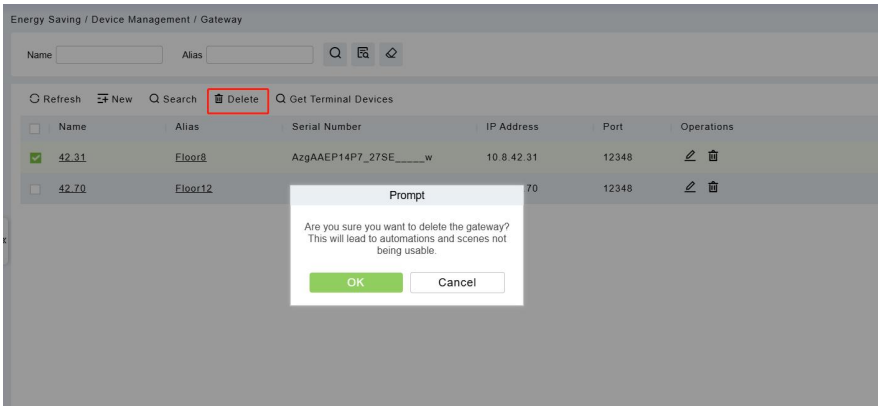


Figure 19- 4 Delete Gateway

19.1.1.4Get Terminal Device

If the user has already added terminals to this gateway through the Lifesmart app, they can click 'Get Terminal Devices' to display all terminals connected to the gateway in the **Energy Saving -> Device Management -> Terminal** list.

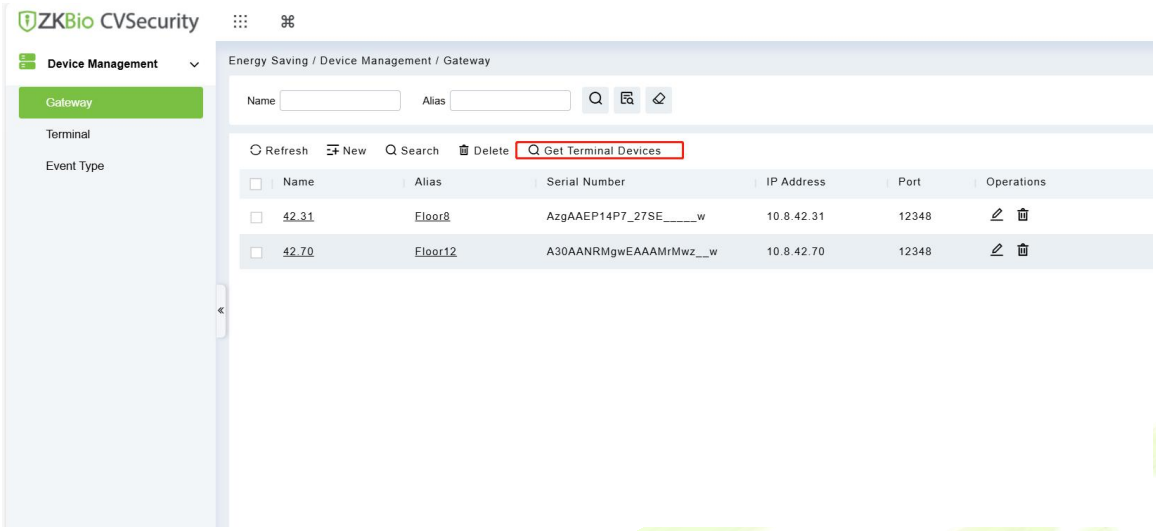


Figure 19- 5 Get Terminal Device

19.1.1.5Paring Terminals

Check the required gateway in the list, then click "**Pairing Terminals**", select the **Pairing Protocol**, click "**OK**", and the gateway will start pairing with nearby terminals.

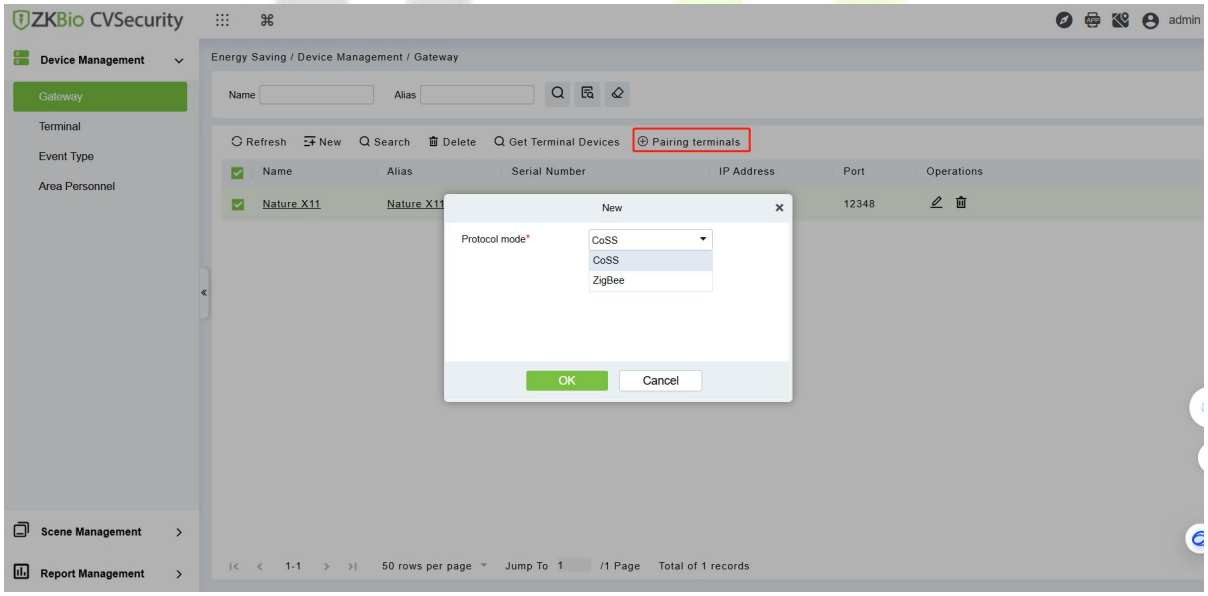


Figure 19- 6 Pairing Protocol

Precautions for pairing:

1)Before pairing the terminals, check the user manual of the terminal to confirm the protocol it uses.

2)Click "Pairing Terminals" and select the matching protocol. Its function is to send an instruction to the gateway to search for nearby devices.

3)Press and hold the pairing button of the terminal according to the pairing operation method of the terminal device.

4)Once it prompts that the pairing is successful, the pairing operation is completed. Only one terminal device can be paired in one pairing operation.

Note: *The administrator can also achieve terminal pairing through the Mobile APP. Log in to the "ZKBio Zexus APP" to perform the operation.*

19.1.2Terminal

Terminals must be added to the gateway through the app and cannot be added directly through the software.

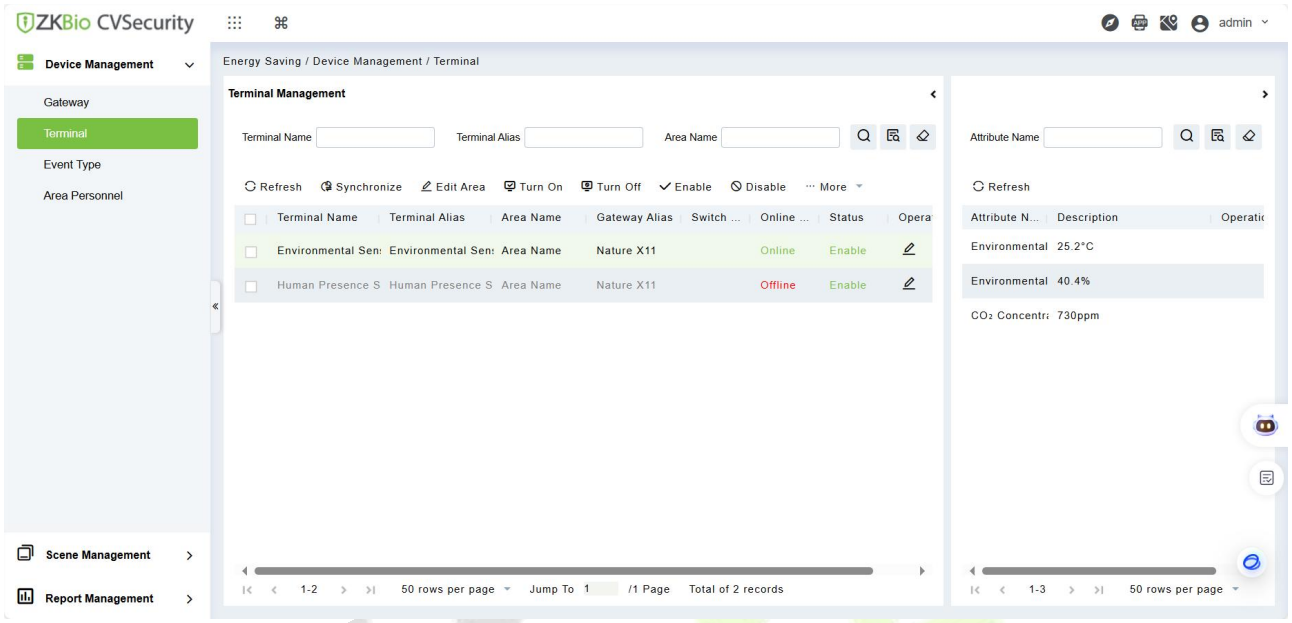


Figure 19- 7 Terminal

19.1.2.1Synchronize

Clicking the **Synchronize** button will displays the terminal devices added to the gateway in the list.

19.1.2.2Edit Area

Modify the location area of the terminal.

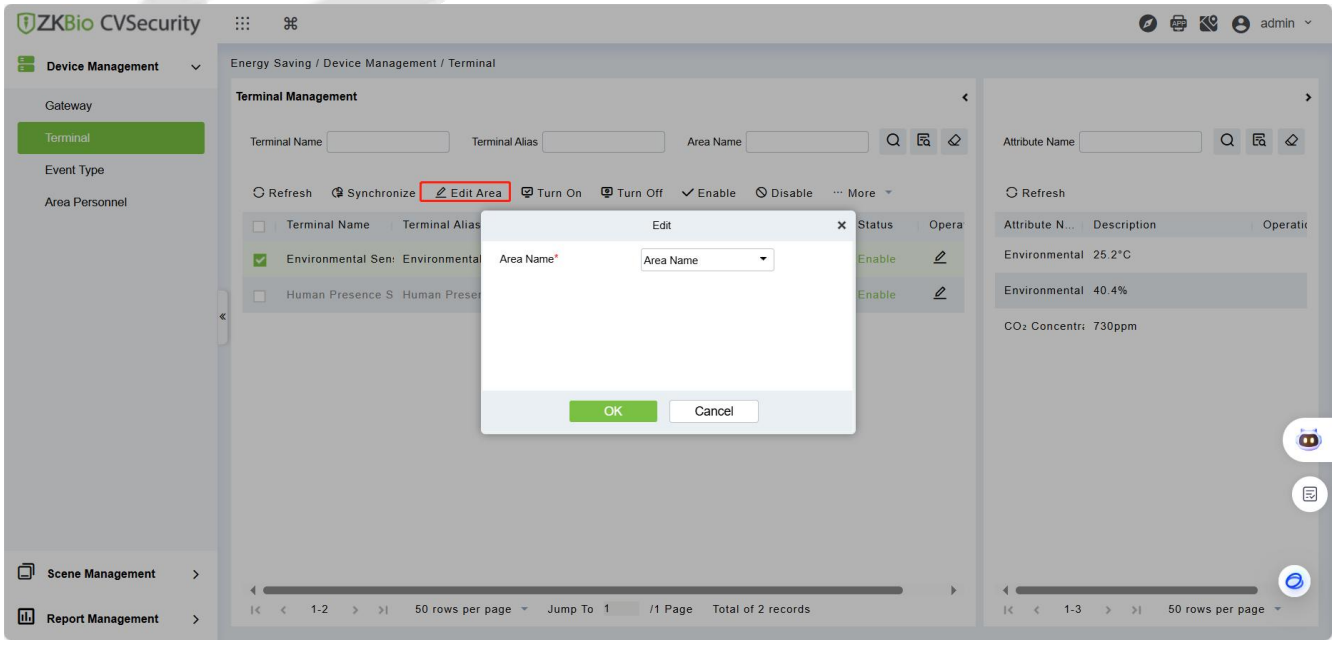


Figure 19- 8 Edit Area

19.1.2.3Turn On / Off

Remotely turn terminals on/off, such as air conditioners, lights, and other devices.

Note: *Terminal devices of the sensor type do not support remote Turn On/Off.*

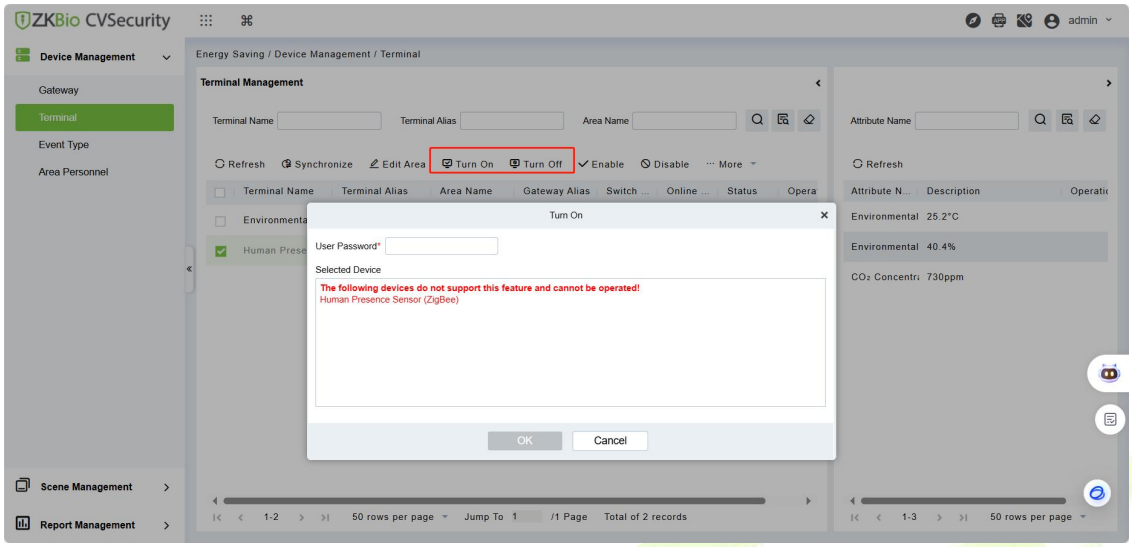


Figure 19- 9 Remote Open

19.1.2.4Enable / Disable

Remotely enable or disable terminals.

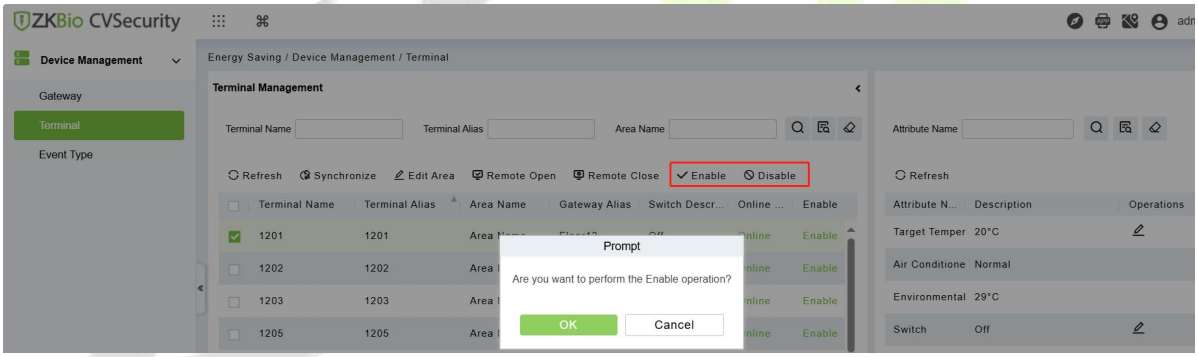


Figure 19- 10 Enable / Disable

19.1.2.5Terminal Control

Once a terminal is selected, its current status will be displayed in the window on the right.

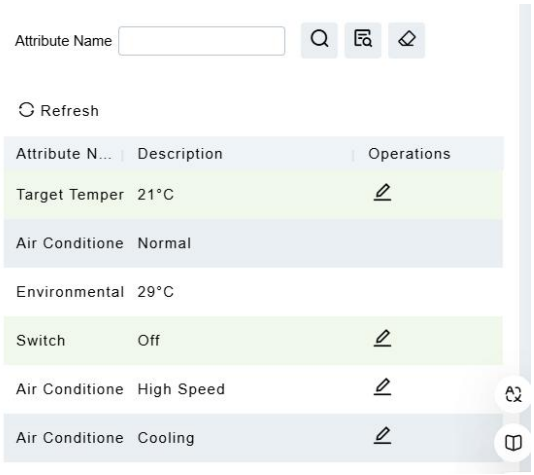


Figure 19- 11 Terminal Control

Click the edit button to adjust the terminal.

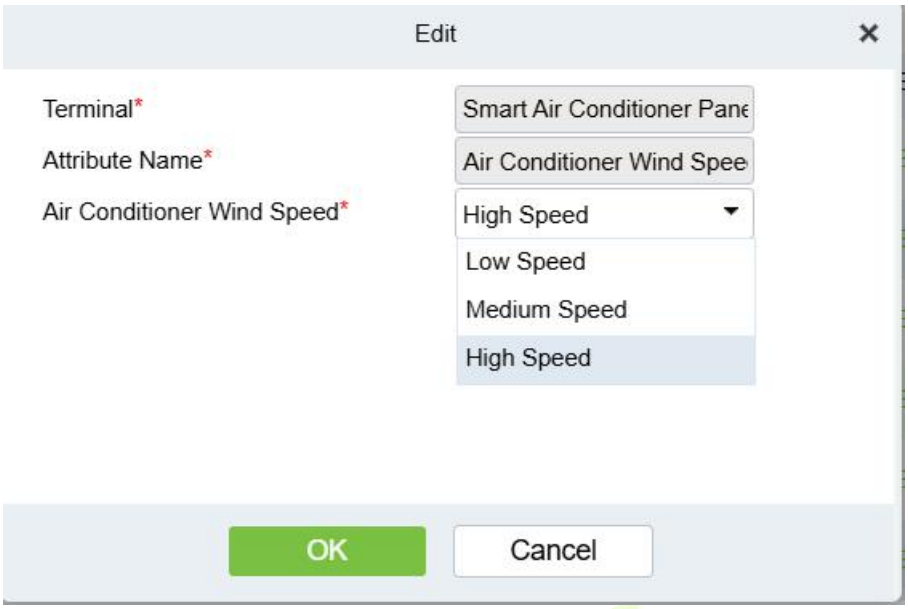


Figure 19- 12 Terminal Control

19.1.3Event Type

The event type display all event types of the module, allowing administrators to edit event values, such as setting triggers for alarms when CO2 levels exceed a specified threshold.

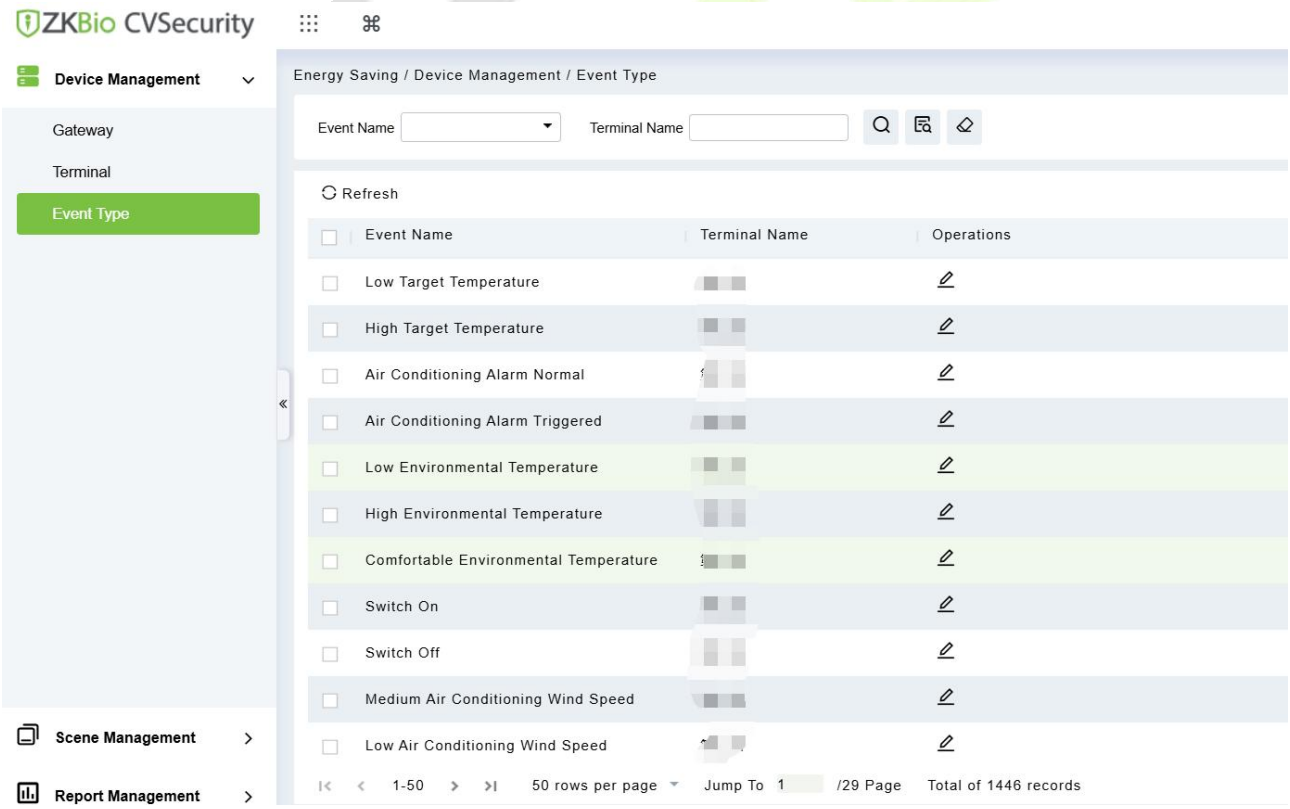


Figure 19- 13 Event Type

Click on the icon to edit the values of specific event types.

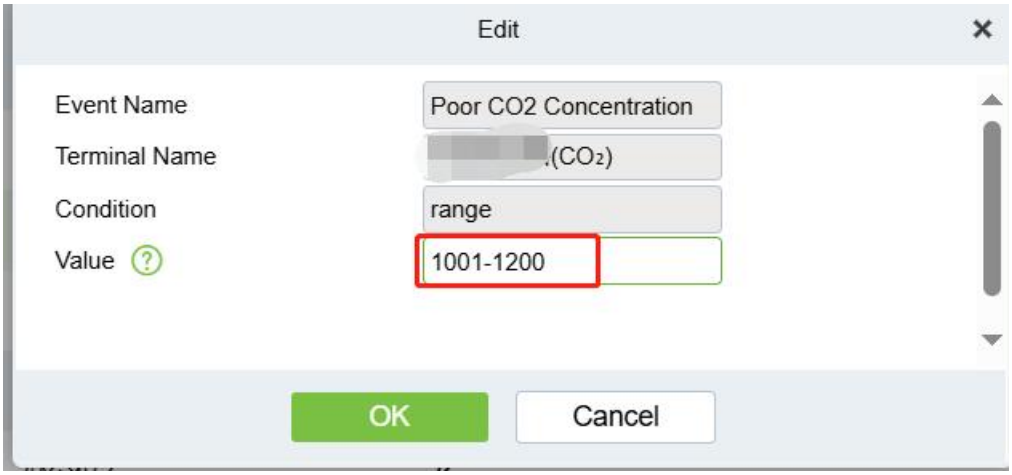


Figure 19- 14 Event Type

19.1.4Area Personnel

This function is used to manage the operation permissions of personnel for terminals in different areas. For example, a person with ID 123 can only view and operate the terminals in Area A. After configuring here, when this person logs into the ZKBio Zexus APP, they can only operate the terminals in Area A.

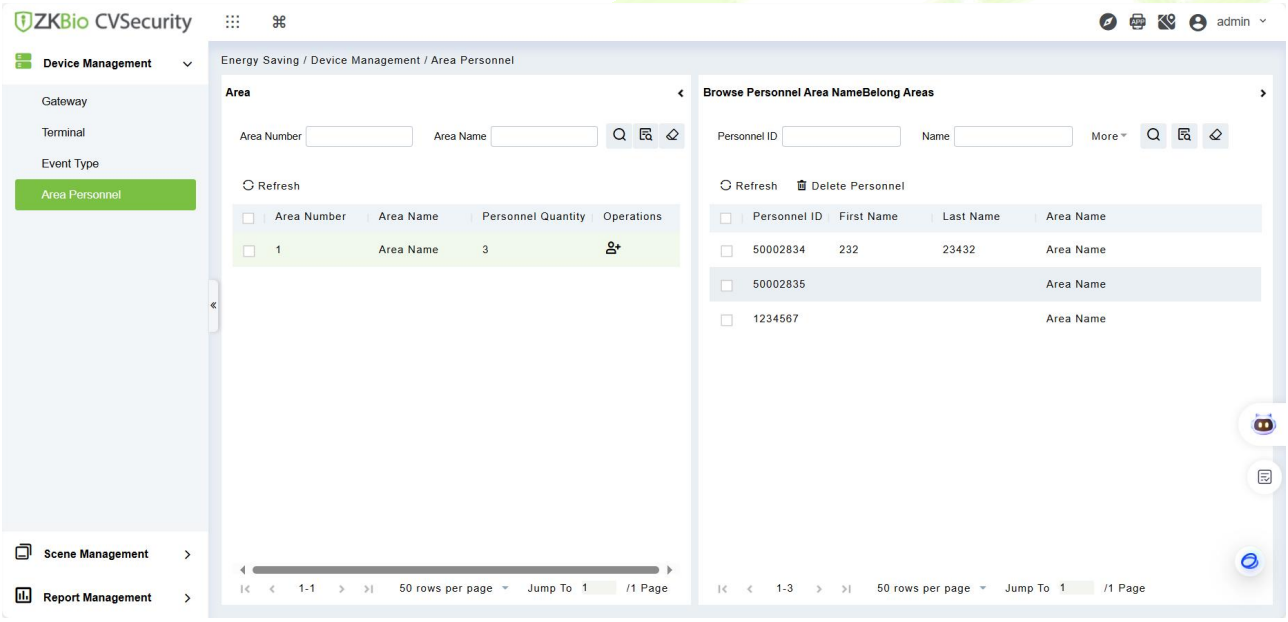


Figure 19- 15 Area Personnel

19.2 Scene Management

Linkage: By configuring the terminal's attribute values to meet specific conditions, certain scene functions can be triggered simultaneously. For example, when a human sensor detects that no one is present in a given area, the lights and air conditioning can be automatically turned off.

Scene Configuration: Configure the attribute values to trigger a scene mode through linkage. It can also be integrated with other modules, such as space management (e.g., meeting rooms), to activate a scene, such as triggering a specific scene after a meeting check-in.

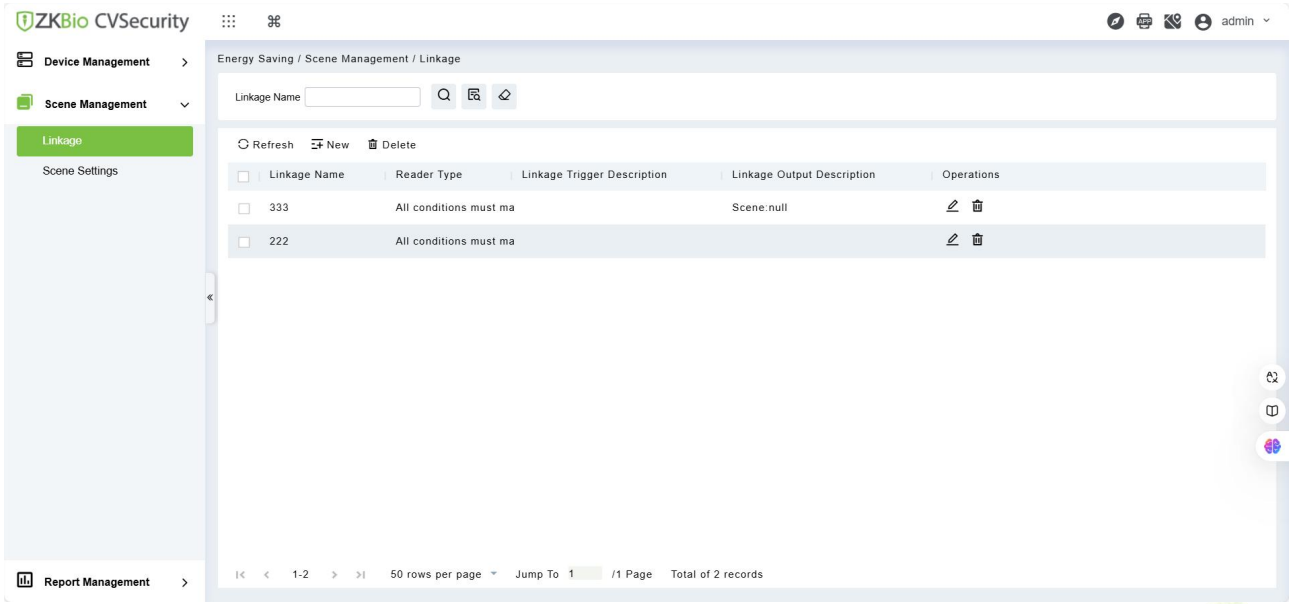


Figure 19- 16 Linkage

19.2.1 Linkage

19.2.1.1 Create a New Linkage

Click on the **Scene Management > Linkage > New** it will displays the new linkage interface here, enter the required details click **OK** to create a new linkage.

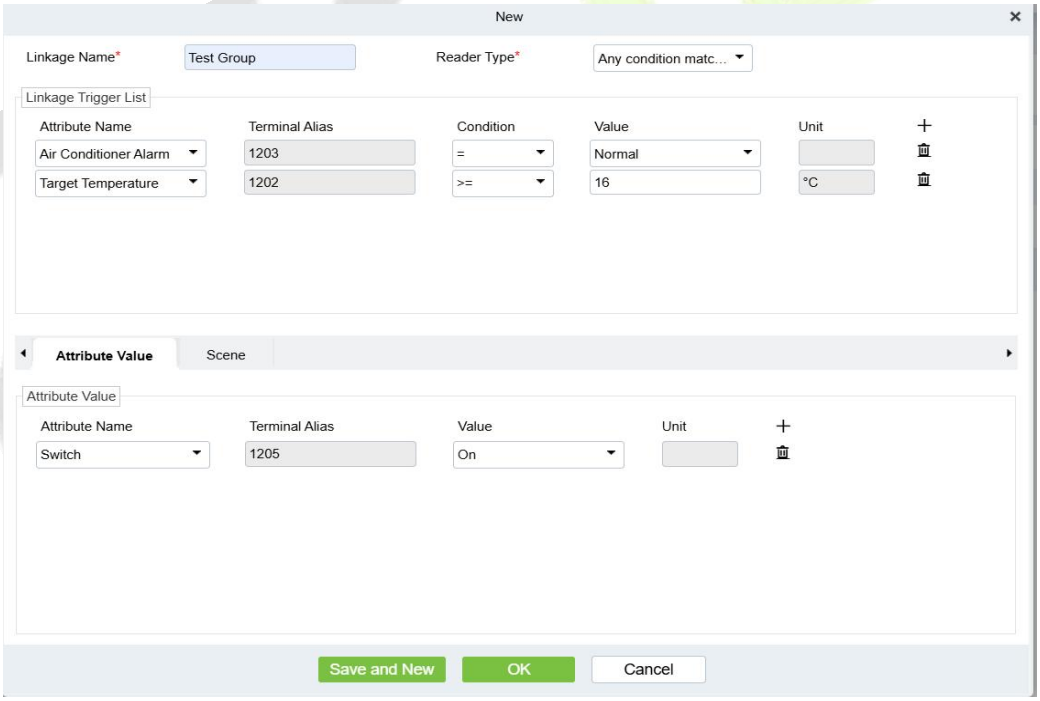


Figure 19- 17 Linkage

Linkage Trigger List: Configure the conditions that activate the linkage.

Attribute Value: Configure the corresponding output actions.

Scene: Select the scene mode to be triggered (please configure this in advance under Scene Settings).

19.2.1.2 Delete Linkage

After selecting the linkage name, click the **Delete** button to remove it.

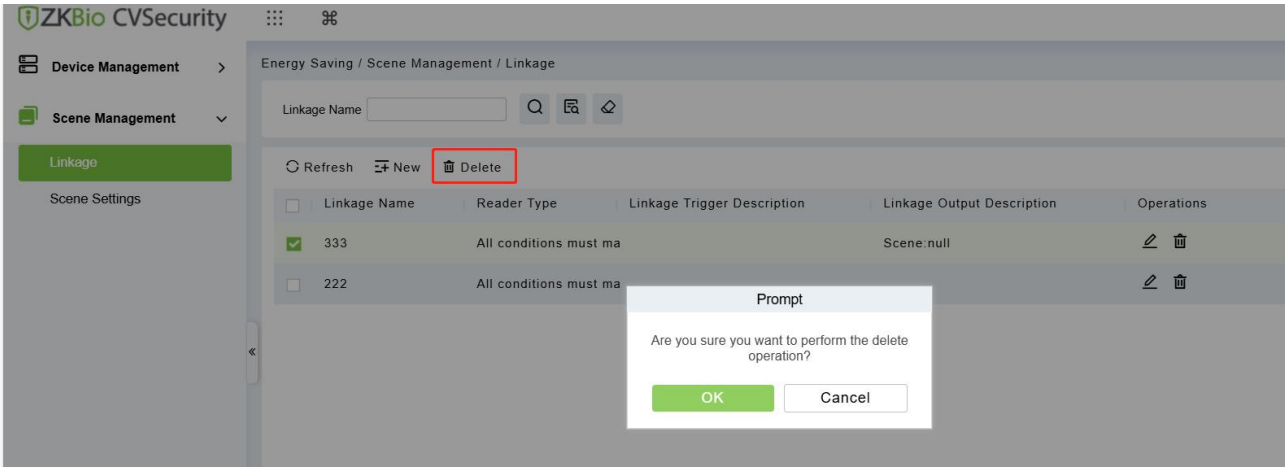


Figure 19- 18 Delete Linkage

19.2.2 Scene Settings

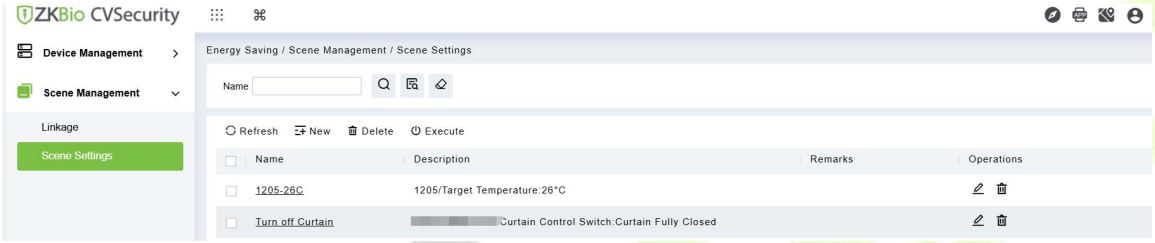


Figure 19- 19 Scene Setting

19.2.2.1 New Scene

Configure the scene name and attribute values for the scene mode, as shown in the figure below.

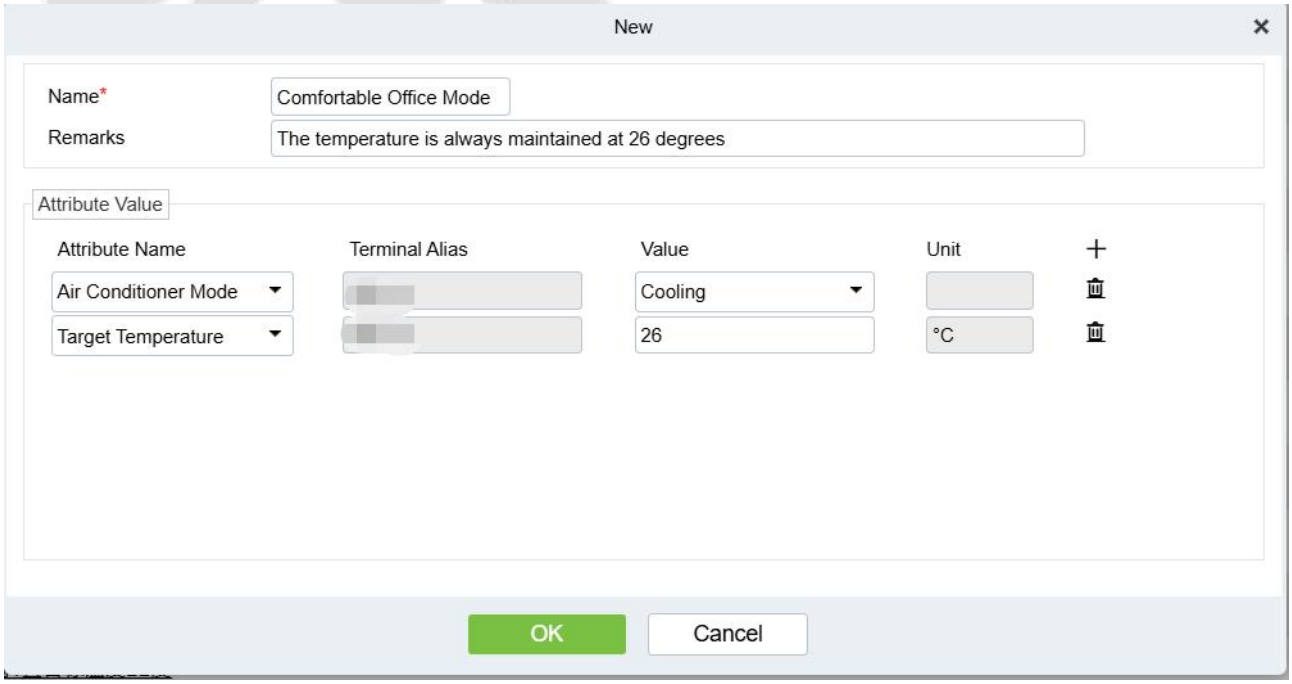


Figure 19- 20 New Scene

19.2.2.2 Delete Scene

Select the scene then click **Delete** button to delete the scene mode.

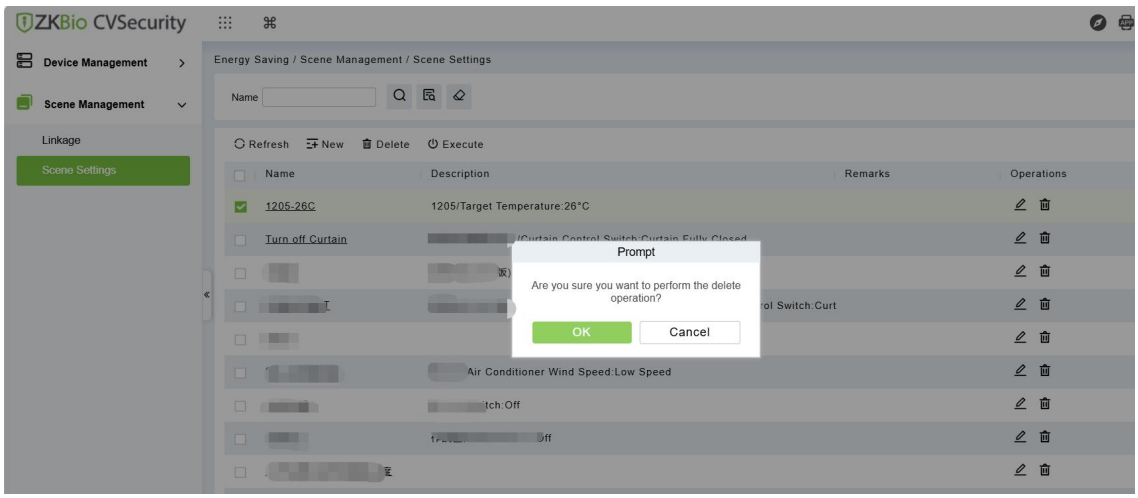


Figure 19- 21 Delete Scene

19.2.2.3Execute Scene

Click the **Execute** button, enter the password, and then immediately activate the scene mode without waiting for the linkage conditions to be triggered.

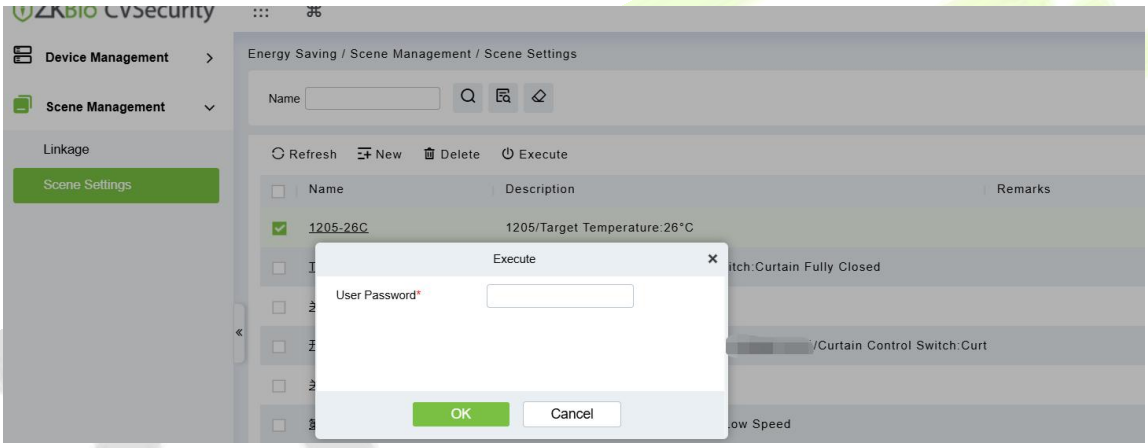


Figure 19- 22 Execute Scene

19.3 Report Management

19.3.1Linkage Report

Click on the **Report Management > Linkage Report** to view the linkage report.

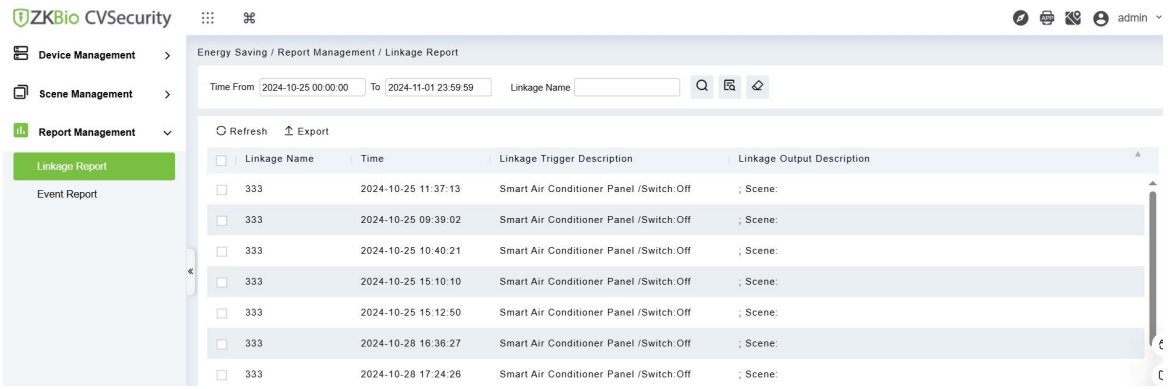


Figure 19- 23 Linkage Report

Export Linkage Report

Click on the **Report Management > Linkage Report > Export** to export the linkage reports.

Linkage Report

Linkage Name	Time	Linkage Trigger Description	Linkage Output Description
333	2024-10-25 11:37:13	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-25 09:39:02	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-25 10:40:21	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-25 15:10:10	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-25 15:12:50	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-28 16:36:27	Smart Air Conditioner Panel /Switch:Off	; Scene:
333	2024-10-28 17:24:26	Smart Air Conditioner Panel /Switch:Off	; Scene:

Figure 19- 24 Export Linkage Report

19.3.2Event Report

Click on the **Report Management > Event Report** to view the event report.

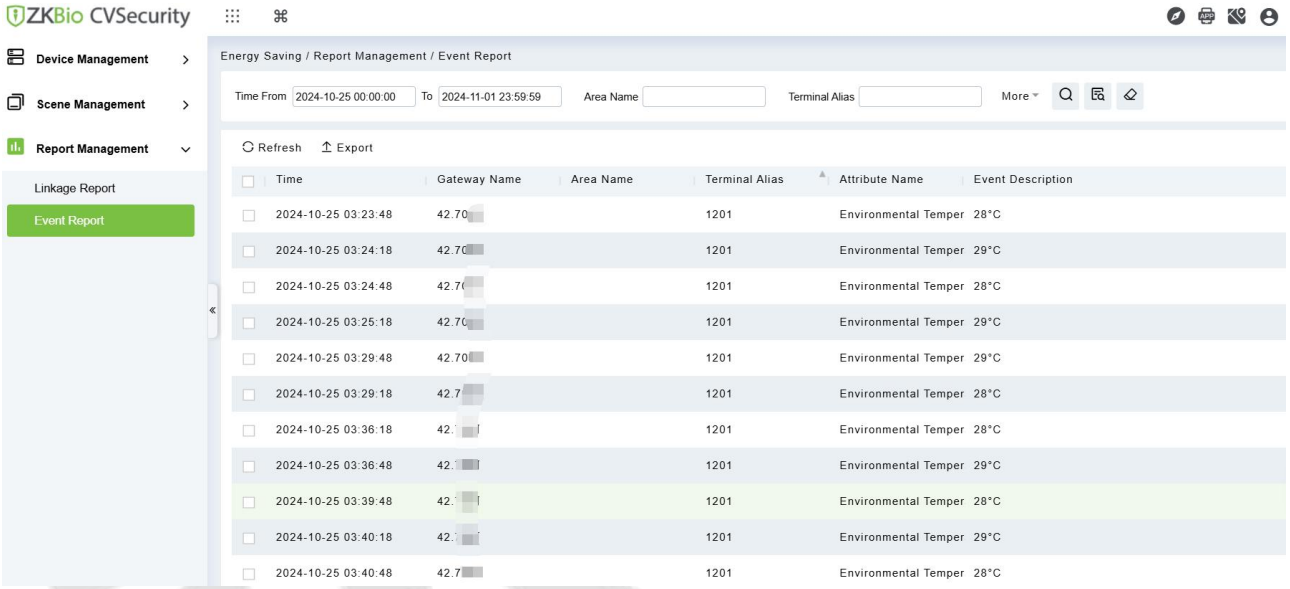


Figure 19- 25 Event Report

Export Event Report

Click on the **Report Management > Event Report > Export** to export the event reports.

Event Report

Time	Gateway Name	Area Name	Terminal Alias	Attribute Name	Event Description
2024-10-25 03:23:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:24:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:24:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:25:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:29:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:29:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:36:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:36:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:39:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:40:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:40:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:41:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:42:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:43:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:51:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:51:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:54:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:54:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:56:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:56:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:57:18	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:57:48	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:58:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 03:59:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 03:59:48	42.7		1201	Environmental Temperature	28° C
2024-10-25 04:00:18	42.7		1201	Environmental Temperature	29° C
2024-10-25 04:01:18	42.7		1201	Environmental Temperature	29° C

Figure 19- 26 Export Event Report

20 System

20.1 System Management

System settings primarily include assigning system users (such as company management user, registrar, access control administrator) and configuring the roles of corresponding modules, managing database, setting system parameters and view operation logs, etc.

20.1.1 Operation Log

● Operation Step

Step 1: Click **System > System Management > Operation Log**.

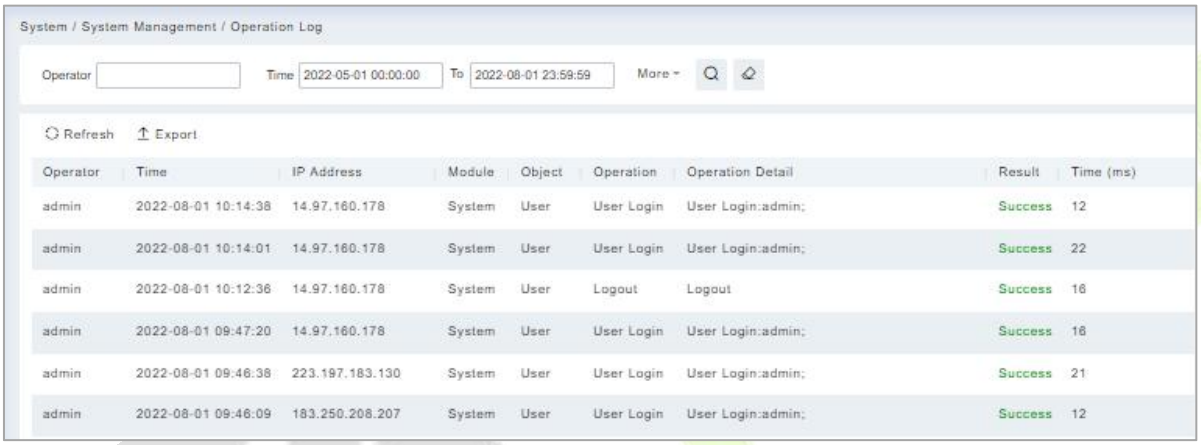


Figure 20- 1 Operation Log Interface

All operation logs are displayed in this page. You can query specific logs by conditions.

20.1.1.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the operation log.

20.1.1.2 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. See the following figure.

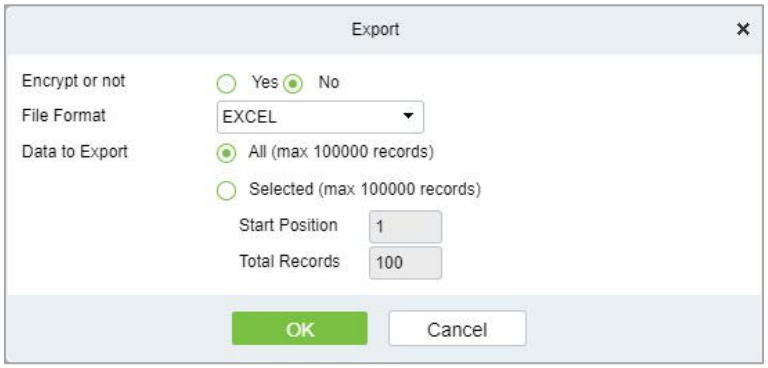


Figure 20- 2 Export Option

20.1.2Data Management

● Operation Step

Step 1: Click **System** > **System Management** > **Database Management**.

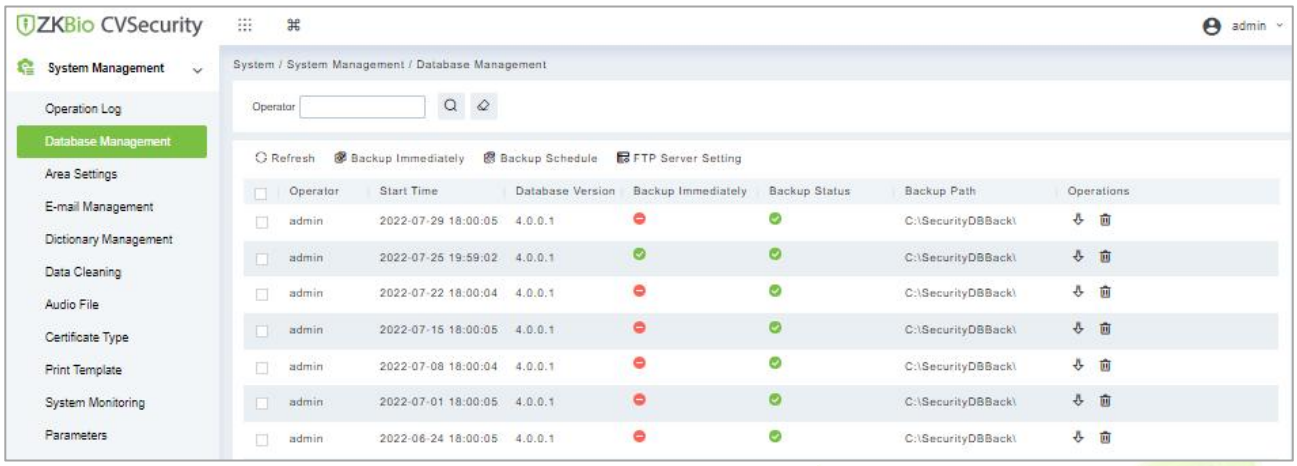


Figure 20- 3 Database Management Interface

All history operation logs about database backup are displayed in this page. You can refresh, backup and schedule backup database as required.

20.1.2.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the operation log.

20.1.2.2Backup Immediately

Step 1: Click **Backup Immediately**.

Backup database to the path set in installation right now.

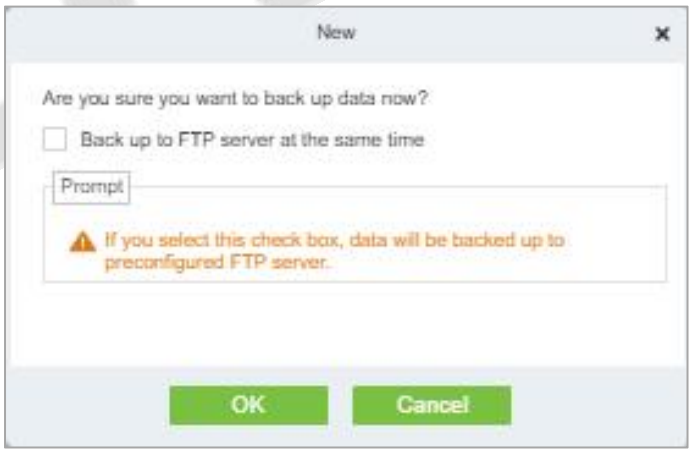


Figure 20- 4 Back up Immediately Option

✍ **Note:** The default backup path for the system is the path selected during the software installation. For details, refer to '*Software Installation Guide*'.

20.1.2.3Backup Schedule

Step 1: Click **Backup Schedule**:

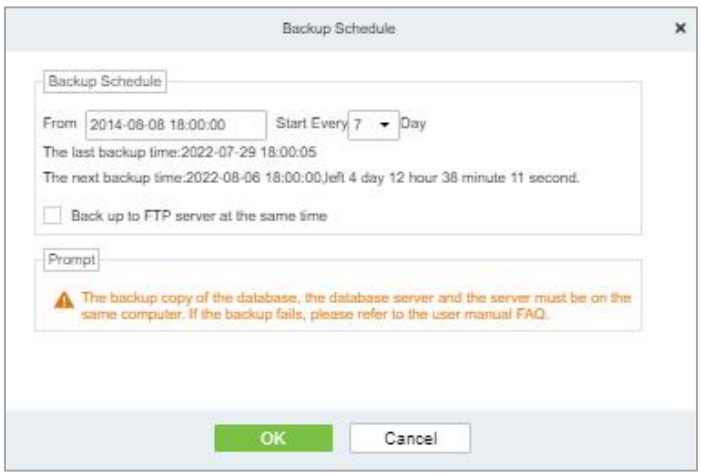


Figure 20- 5 Back up Schedule Option

Step 2: Set the start time, set interval between two automatic backups, click **OK**.

20.1.2.4FTP Server Setting

When send mode is FTP Send Method, FTP parameters should be set. The parameters are FTP Server Address, Server Port, Folder Location, Username, and Password.

Figure 20- 6 FTP Server Setting

Parameter	Description
FTP Server Address	Enter the address FTP Server Address E.g.: such as 192.168.1.10.
Port	Enter the port number.
Folder Location	Enter the Folder location.
Username	Enter the Username of the FTP server.
Password	Enter the password for the FTP server.
Test Connection	After configuring the FTP parameters, click **Test Connection** to test whether the FTP server is communicating normally.

Table 20- 1 Description of FTP Server Setting Parameters

After the setup is completed, click the **OK** button, save and return to the Database Management interface.

20.1.3Area 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.

The system, by default, has an area named **Headquarters** and numbered **1**.

20.1.3.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the area setting page.

20.1.3.2New

Step 1: Click **System** > **System Management** > **Area Setting** > **New**.

Step 2: Click **OK** to finish adding.

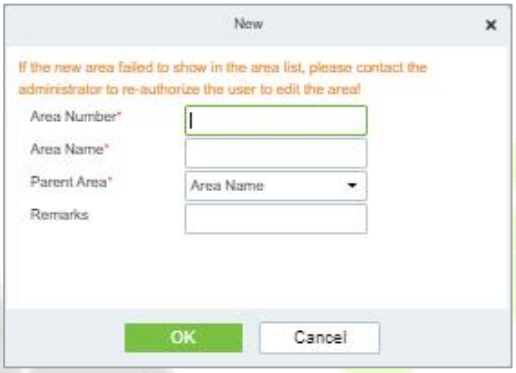


Figure 20- 7 Area Setting

Parameter	Description
Area Number	Enter the area number. It must be unique.
Area Name	Enter the area name. Any characters with a length less than 30.
Parent Area	Determine the area structure of system.

Table 20- 2 Description of area Setting Parameters

20.1.3.3Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

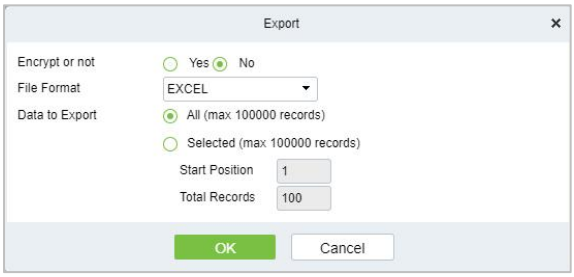


Figure 20- 8 Export Option

20.1.3.4Edit/Delete an Area

Click **Edit** or **Delete** as required under **Operation** to go to the edit or delete page. Then click **OK** to save the setting.

20.1.3.5Import

If there is a personnel file in your computer, you can Import it into the system.

Step 1: Click **Import**.

Figure 20- 9 Import Interface

Step 2: Select the file format to be imported (default is Excel) and choose the file to be imported.

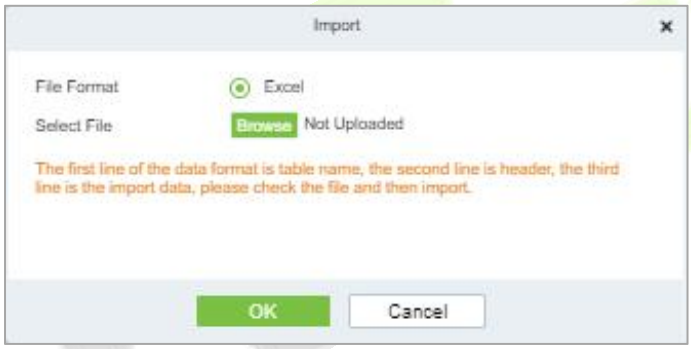


Figure 20- 10 Import Option

Step 3: If you want to download the sample template excel file for importing, click the **Download Area Import Template.**

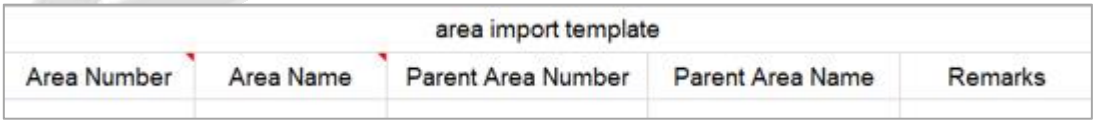


Figure 20- 11 Area Import Template

Step 4: Once the sample excel is downloaded, you can fill your data into it and save it. Then upload the saved file.

20.1.4E-mail Management

Set the email sending server information. The recipient e mail should be set in Linkage Settings.

Step 1: Click System > **System Management** > **Email Management**

20.1.4.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Email management page.

20.1.4.2Delete

Click **Delete** as required under operation to go to the edit or delete page. Then click **OK** to save the setting.

20.1.4.3Outgoing Mail Server Settings

Click System > **System Management** > **Email Management** > **Outgoing Mail Server Settings**.

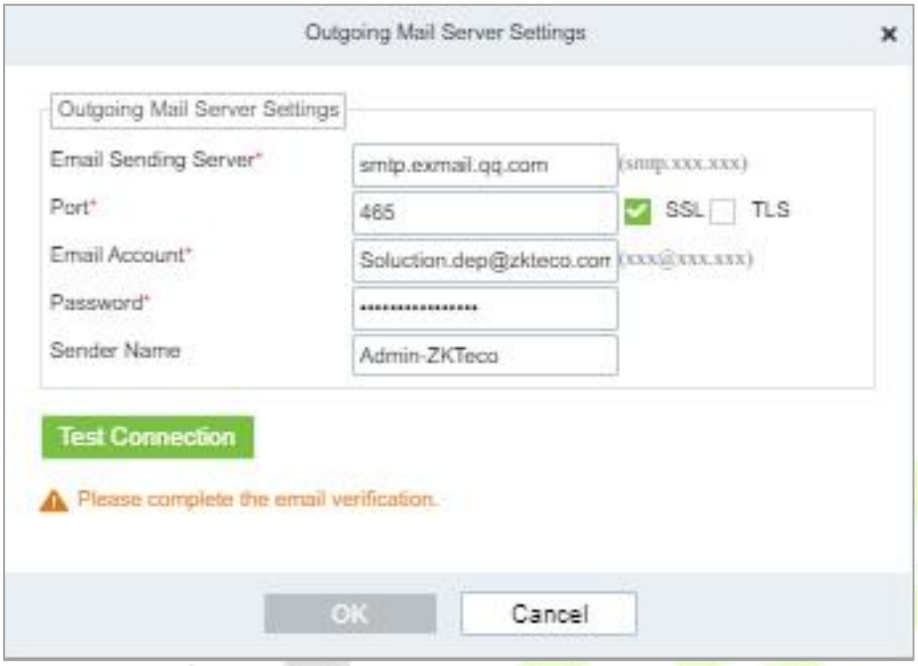


Figure 20- 12 Outgoing Mail Server Setting

Note: The domain name of E-mail address and E-mail sending server must be identical. For example, the Email address is test@gmail.com, and the E-mail sending server must be smtp.gmail.com.

20.1.4.4Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

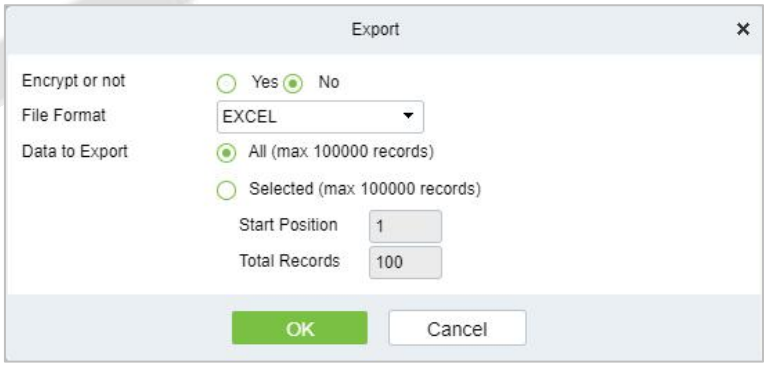


Figure 20- 13 Export Option

20.1.5Dictionary Management

Data dictionary management function, users can find the meaning of error code and self-check software errors.

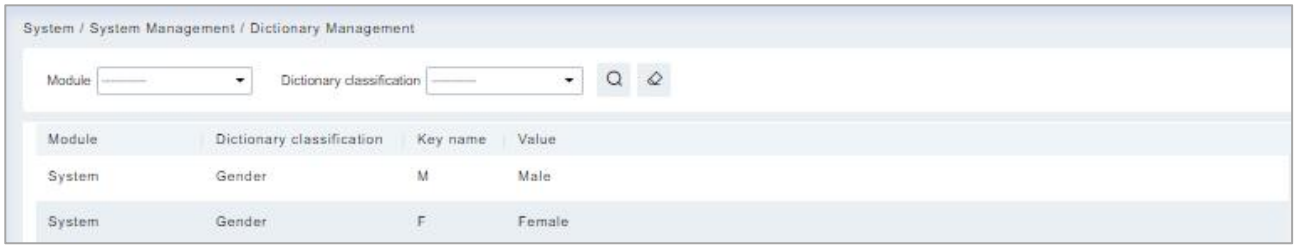


Figure 20- 14 Dictionary Management Interface

20.1.6Data Cleaning

To save disk storage space, the expired data generated by the system must be cleaned up regularly

Click **System** > **System Management** > **Data Cleaning**. The data cleaning frequency can be set to Day/Week/Month.

20.1.6.1Record

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.

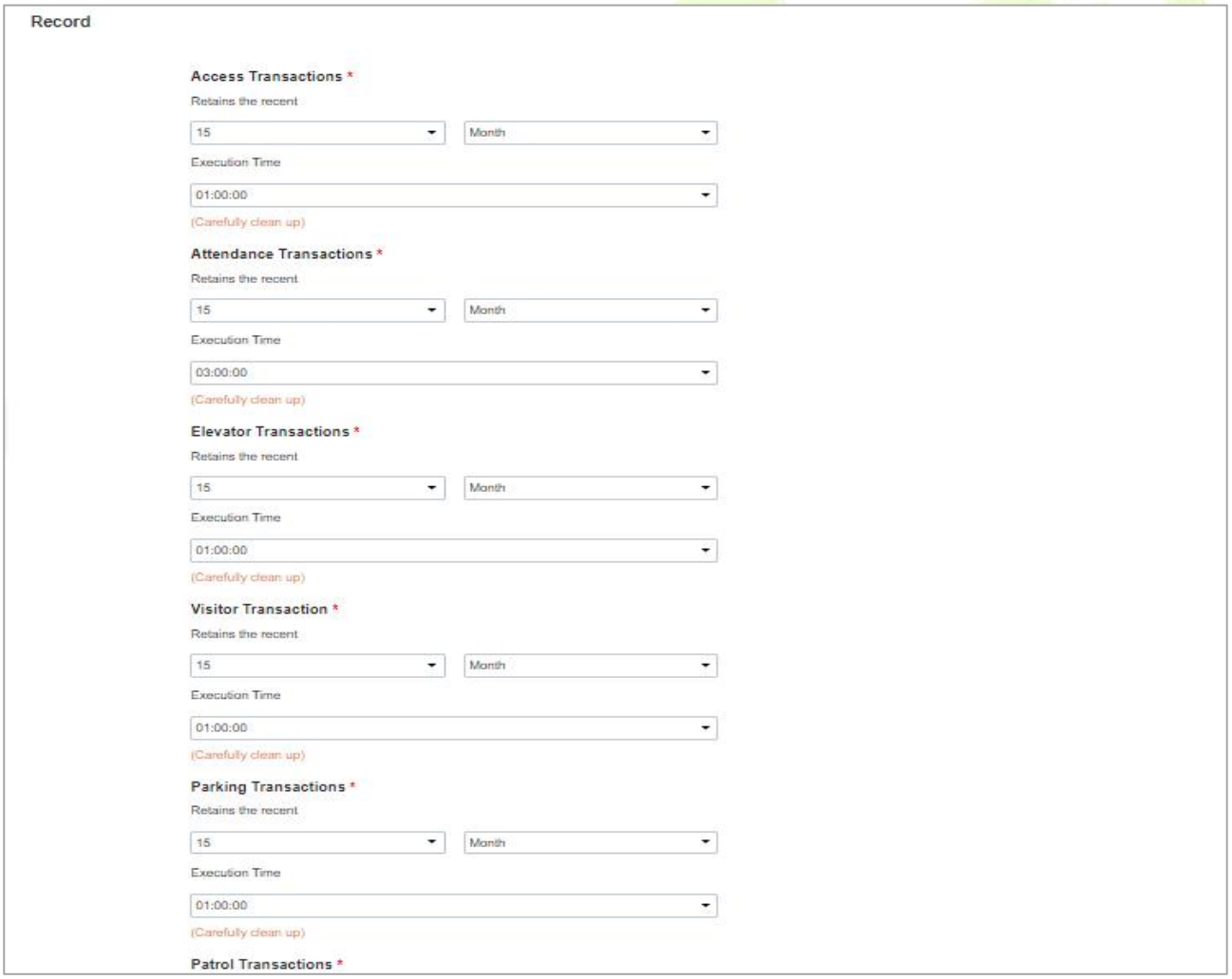


Figure 20- 15 Record Interface

20.1.6.2Disk Space Cleanup

In this option you can set the frequency of the retains the recent and also clean up the selected days data.

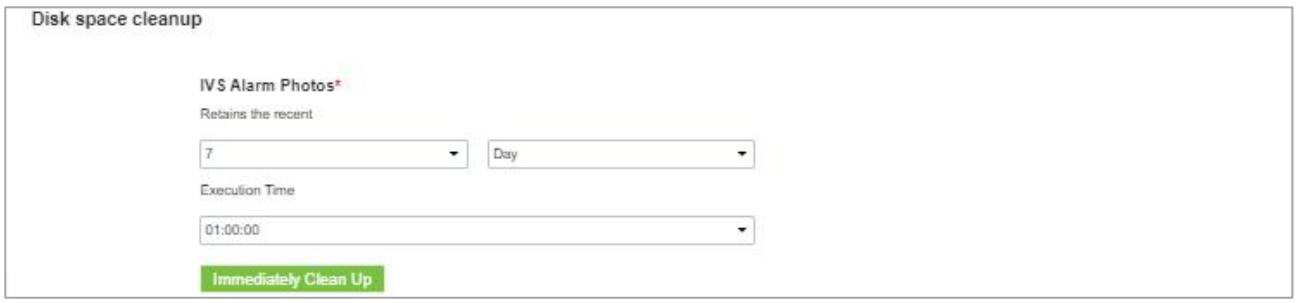


Figure 20- 16 Space Cleanup Interface

20.1.6.3System

This option helps you to clean up the system operation log, device commands and database backup file.

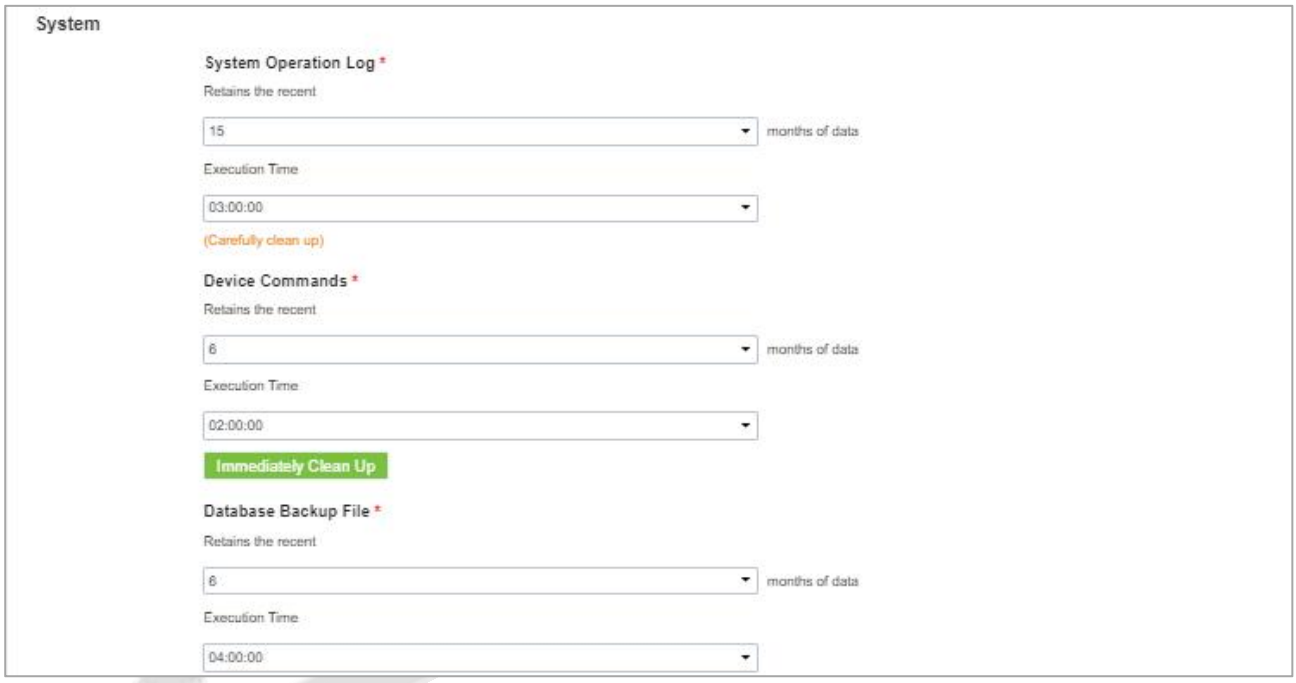


Figure 20- 17 System Interface

20.1.7Resource File

Click **System > Basic Management > Audio File** to open the following interface:

Figure 20- 18 Audio File Interface

20.1.7.1New

● Operation Steps

Step 1: Click **System** > **System Management** > **Audio File** > **New**, the following window appears:

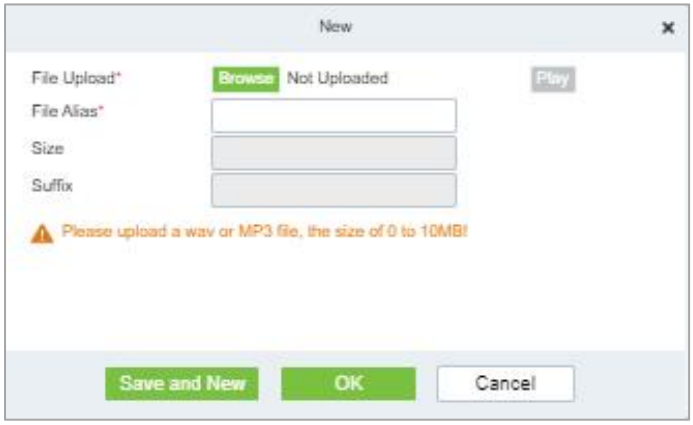


Figure 20- 19 New Option

Step 2: Browse to upload an audio file locally. The file format must be in WAV or mp3 format and must not exceed 10MB in size.

Parameter	Description
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.

Table 20- 3 Description New option parameter

20.1.7.2Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Audio file page.

20.1.7.3Edit

Click the file name or **Edit** to edit the audio file details which support replacing the audio files and editing the file name. The "size" and "suffix" automatically change depending on the size and type of audio file being uploaded. After editing, click **OK** and **Exit**.

20.1.7.4Delete

Select the specified audio file to delete and click Delete. Then click **OK** to save the setting.

20.1.8Cloud Settings

Enable hybrid cloud services and then use the Mobile APP.

Please refer to the attachment for the operation steps of the Mobile APP.ZK_ZKBio CVSecurity Mobile APP UM_EN v2.0_20240719.pdf

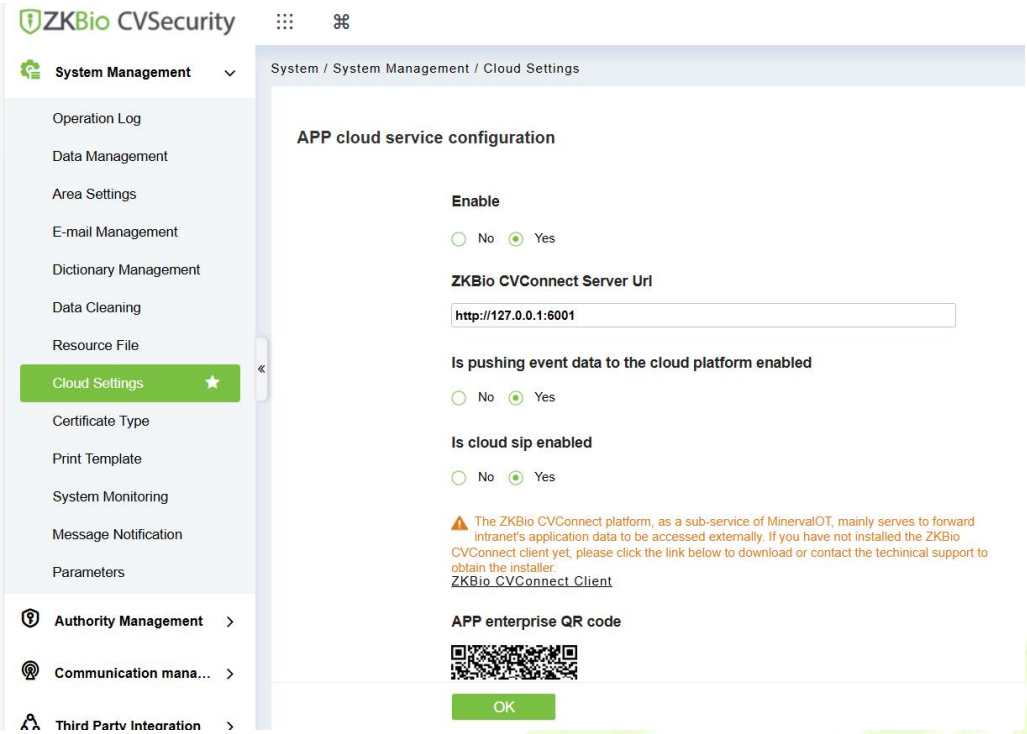


Figure 20- 20 Cloud Settings

Parameter Description

- Enable: Whether to enable hybrid cloud services, enabling them allows users to start using the Mobile APP.
- ZKBio CVConnect Server Url: The address of the ZKBio CVConnect Client that you need to bind.
- Is pushing event to the cloud platform enabled: Whether to store data on the cloud platform, the default is No, data will not be stored in the cloud, it will only be forwarded to the APP.
- Is Cloud Sip enabled :Whether to enable the cloud SIP feature, after enabling it, you can configure the extension number for use in the visual intercom module, refer to the Extension Management
- APP enterprise QR Code :The QR code for APP login generated after registering and activating in the ZKBio CVConnect.

20.1.9Certificate Type

The system initializes 9 certificate types. User can add the required certificate type for personnel and visitor registration.

Click **System> Basic Management > Certificate Type**.

Figure 20- 21 Certificate Type Interface

20.1.9.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the certificate type page.

20.1.9.2New

●Operation Step:

To add the certificates, click System > Basic Management > Certificate Type> New:

Certificate Name: Enter the certificate name.

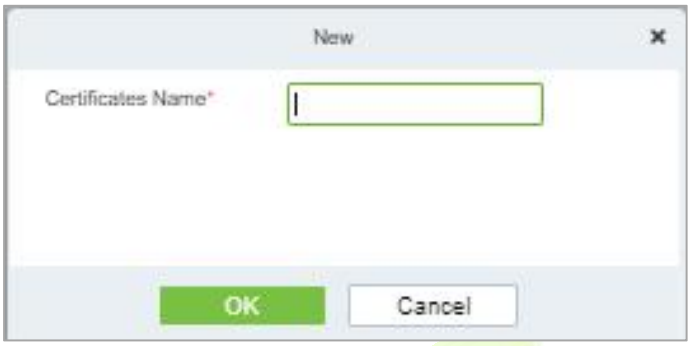


Figure 20- 22 New Option

20.1.9.3Delete

Select the specified certificate to delete and click **Delete.** Then click **OK** to save the setting.

20.1.10Print Template

You can manage templates for different cards here: personnel card templates and visitor pass templates. The system is pre-configured with 5 types of personnel and visitor printing templates.

Click **System> System Management> Print template**.

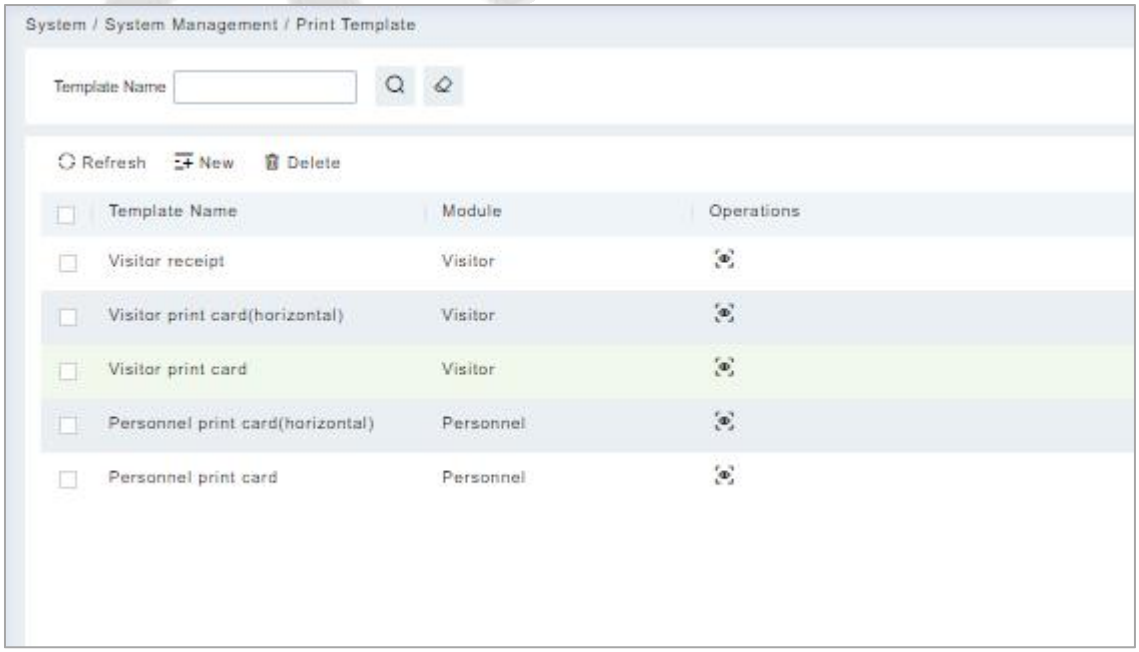


Figure 20- 23 Print Template

20.1.10.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Print Template page.

20.1.10.2Add

To add the certificates, click **System > System Management > Print Template> New**:

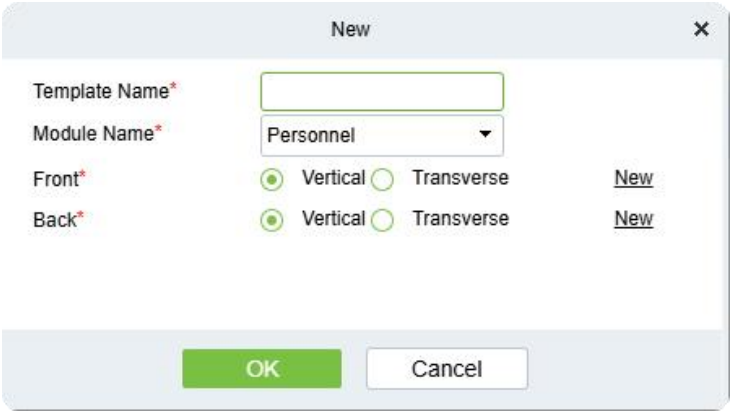


Figure 20- 24 New Option

On the above page, you can set the template name and module category, select the front or back side, choose between vertical or transverse page orientation, and finally click "**New**" to enter the detailed editing interface.

In the template detail settings interface, you can:

- Insert a background image and customize its size and background.
- Customize the size of user photos.
- Customize font style, position, size, color, and bold formatting.
- Insert images and customize their size and position.

✍Note:

The available font styles for printing templates include:

Arial, Arial Narrow, Cambria, Calibri, Tahoma, Verdana Pro, Times New Roman.

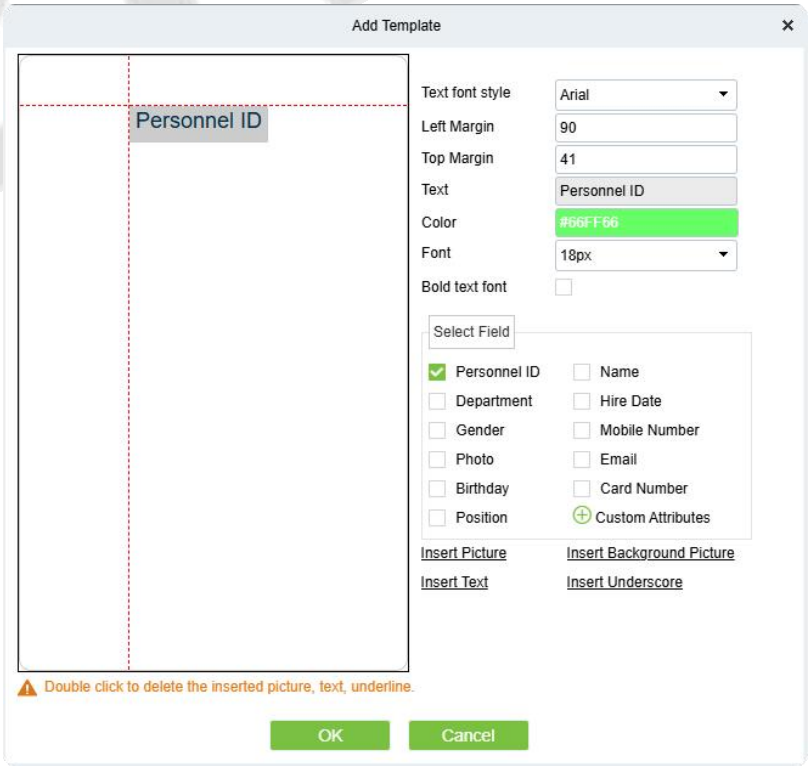


Figure 20- 25 Print Template

20.1.10.3Delete

Select the specified template to delete and click **Delete.**

20.1.11System Monitoring

The system monitoring function displays the server processor usage, host memory usage, processor information, memory information, java virtual machine memory usage and other information.

Click **System> System Management > System Monitoring**.

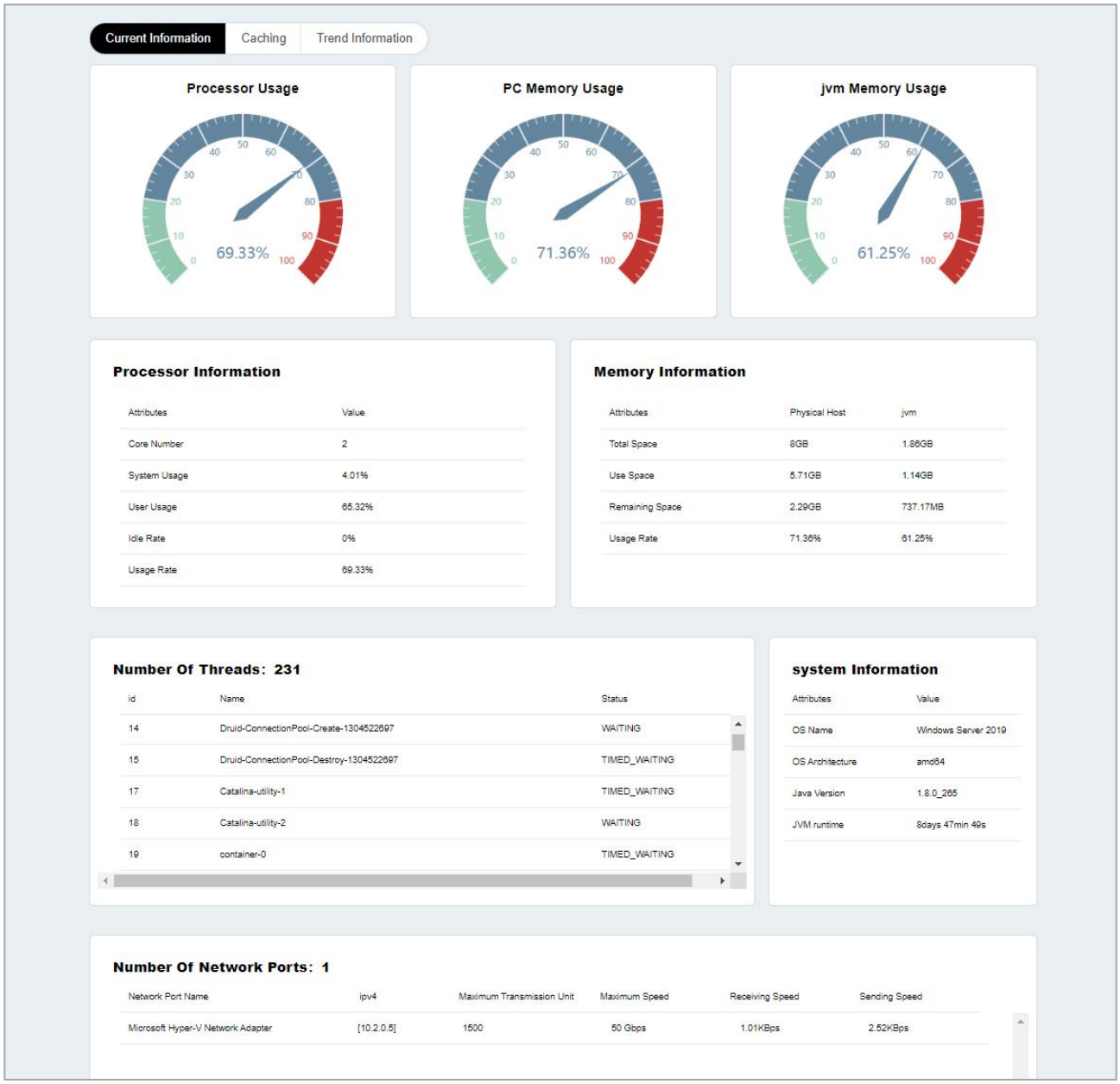


Figure 20- 26 System Monitoring Interface

20.1.11.1Caching

This option helps you to know about memory information, Redis information, client information and also current data base.

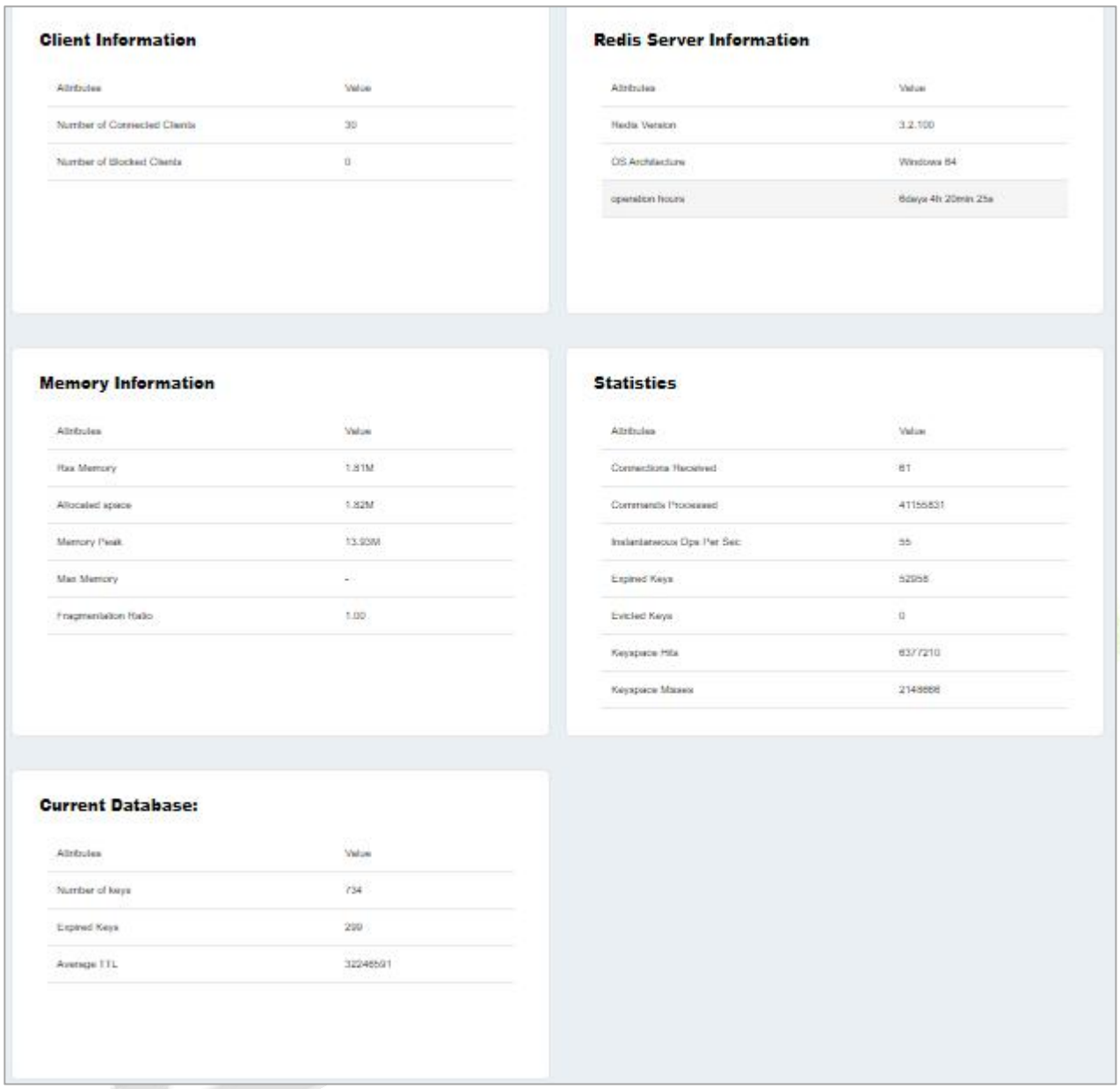


Figure 20- 27 Caching Interface

20.1.11.2Trend Information

This option shows the graphical representation of processor usage, PC memory usage and JV memory usage.

Figure 20- 28 Trend Information Interface

20.1.12Parameters

20.1.12.1QR Code Setting

Step 1: Click **System> System Management > Parameter > QR Code Setting**.

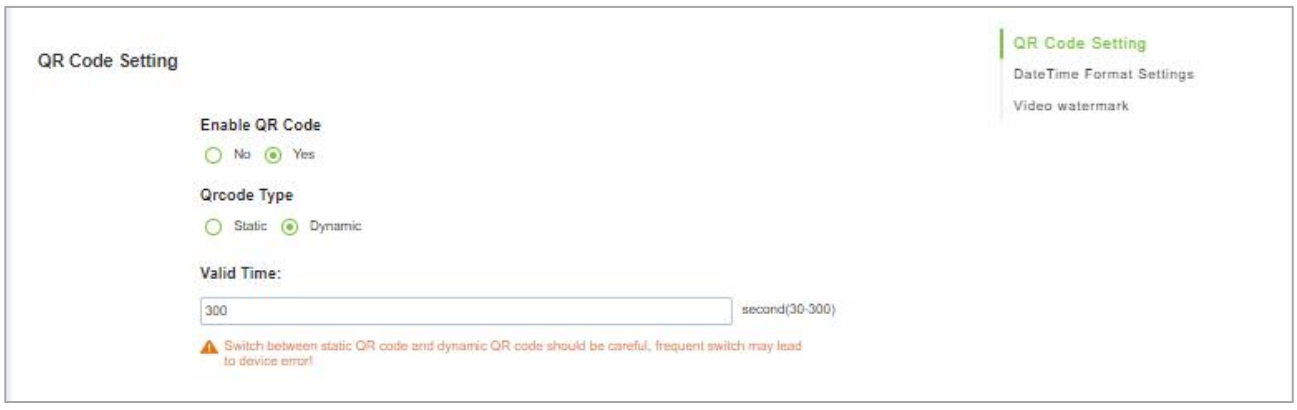


Figure 20- 29 QR Code Setting interface

Step 2: Enable QR code Click **System**> **System Management** > **Parameter** > **YES** or **NO** for Enable the

QR code.

Step 3: Enable QR code If YES click **YES** > **Static**. It will be fixed the QR information same manner for the rest of time.

Step 4: Enable QR code If YES click **YES**> **Dynamic** > **Valid Time**. It will generate new QR code every 30 seconds.

20.1.12.2Date Time Format Setting

Here you can set the date and time format.

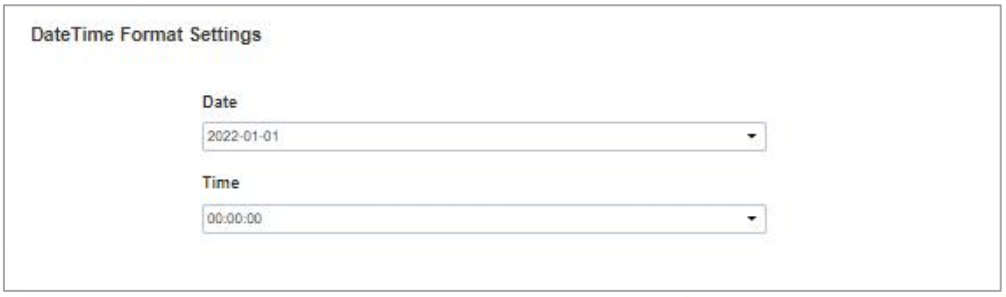


Figure 20- 30 Date and Time Format Setting Interface

20.1.12.3Video Watermark

This option helps you to add watermark and tile to your videos.

Figure 20- 31 Video Watermark Setting

20.2 Authority Management

20.2.1User

20.2.1.1New

This section describes how to configure Step to add an administrator user in ZKBio CVSecurity.

●Operation Step

Step 1: In the System module, choose **Authority Management** > **User**.

Step 2: Click **Add** to pop up the new user interface.

Step 3: On the Add role page, set role rights as required, as shown in the figure below and the below Table describes parameters to be set.

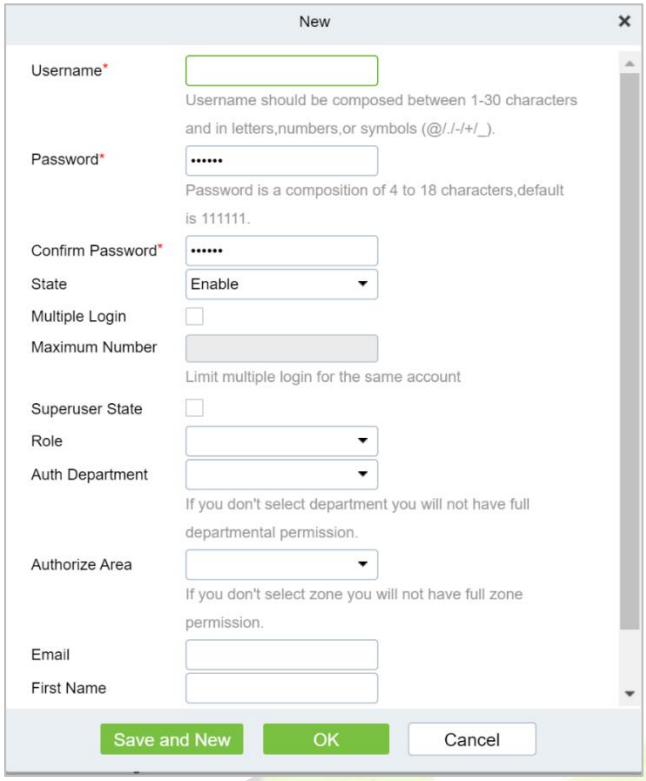


Figure 20- 32 Adding User Interface

Parameter	How to set up
User Name/Password	You can customize the user's name and password used for login.
State	Set whether the user can log in and operate the system.
Connection Limit/Maximum Logins	If this parameter is not selected, the number of simultaneous logins is not limited.
Superuser Status	This parameter specifies whether the user has all rights by default. If you click this parameter, the user is a super user, and no role is required.
Role	Set a role for the user. The user has all Operation permissions configured for the role.
Authorize Department	Authorization Sets the department permissions of the user.
Authorized Permission	Authorization Sets the area rights that the user has.
Email	Customizes this user's mailbox, which can be used to retrieve the password.
The Name	Custom sets the name of this user.
The Fingerprint Registration	Register this user's fingerprint.

Table 20- 4 Parameters for Adding a User

Step 4: Click **OK** to finish configuring the new user.

20.2.1.2Edit/Delete

Click **Edit** or **Delete** as required.

20.2.2Role

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.

20.2.2.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the user page.

20.2.2.2New

● Operation Steps:

Step 1: Click **System > Authority Management > Role > New**.

Step 2: Set the name and assign permissions for the role.

Step 3: Click **OK** to save.

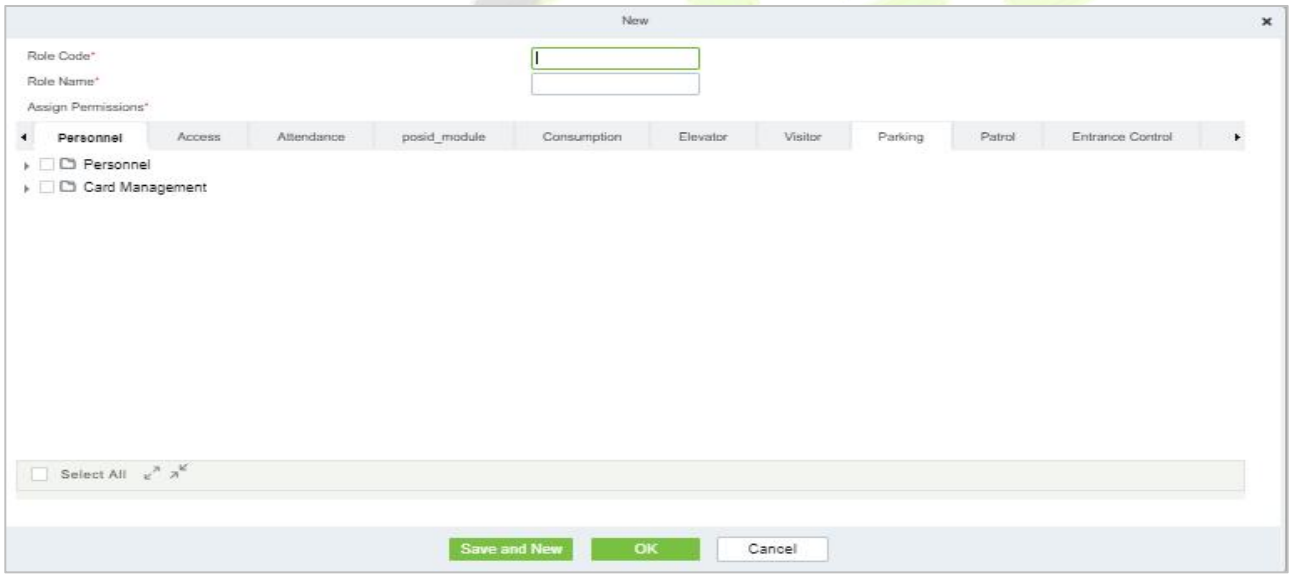


Figure 20- 33 Add Role Option

20.2.2.3Edit/Delete

Click **Edit** or **Delete** as required.

20.2.3API Authorization

20.2.3.1Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the API authorization page.

20.2.3.2New

Operation Steps:

Step 1: Log in to the system (as the super user, for exportation.min) to enter the software. Click **System** > **Authority Management** > **API Authorization** >**New**, which must be unique, and a client secret, which will be used when the API is invoked.

Step 2: Only when the client ID and secret are added can the next API operation page be displayed normally. Otherwise, the access is abnormal):

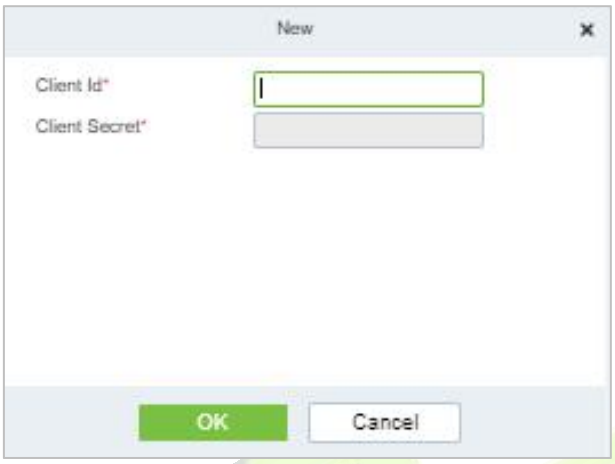


Figure 20- 34 API Authorization Option

20.2.3.3Browse the API

After the client ID and secret are added, click Browse API on the API Authorization page to skip to the API operation page (The page of the ZKBio CVSecurity system must be open for normal access of the API operation page). This page provides multiple API.

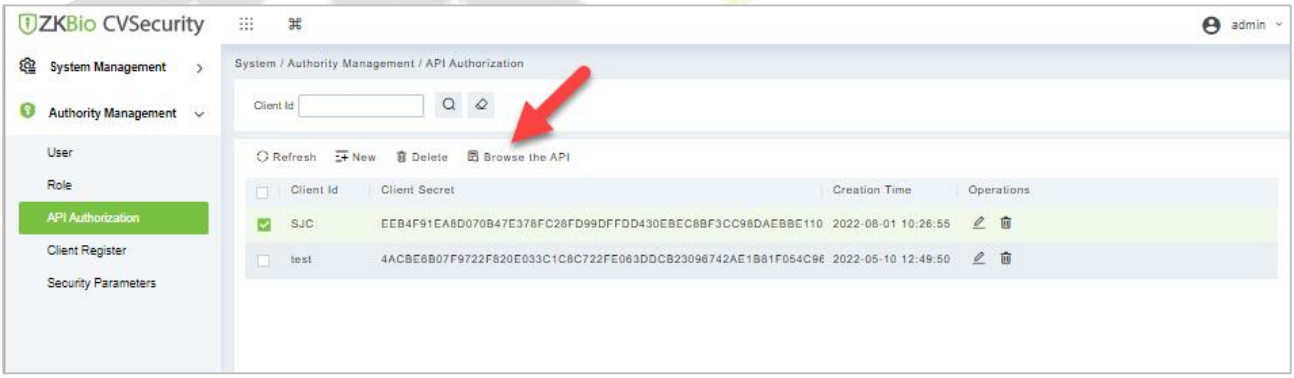


Figure 20- 35 Browse the API

Figure 20- 36 ZKBIO CV Security API Interface

When API are invoked, URLs of all request API must contain the access token parameter, whose value is determined by the client key configured on the background (if there are multiple keys, only one is selected), for example:

Figure 20- 37 Request URL

The access token parameter must be added when the API is invoked (one request URL can be invoked):

http://localhost:8091/system/swagger/index.html?clientId=1653914953805#!/Person/getByPinUsingGET.

20.2.3.4Edit

Click the **Edit** icon to edit the API Authorization details. Enter the required Details.After editing, click **OK** and exit.

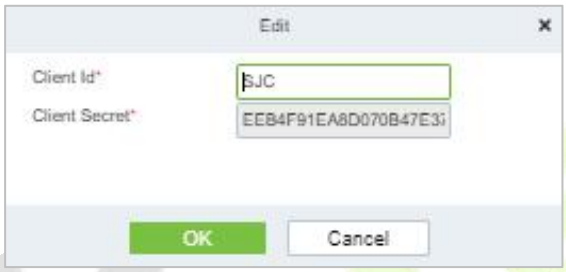


Figure 20- 38 Edit Option

20.2.3.5Delete

Select the specified Client id to delete and click **Delete.**Then Click **OK** to confirm the operation.

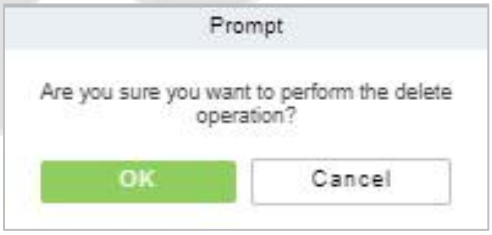


Figure 20- 39 Delete Option

20.2.4Client 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.

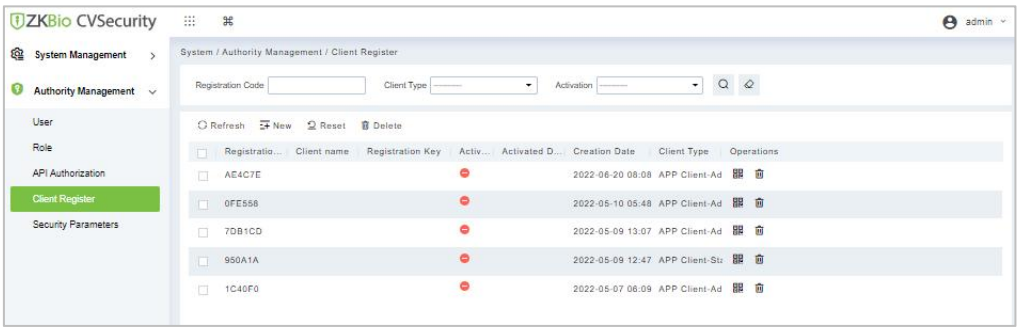


Figure 20- 40 Client Register Interface

20.2.4.1New

Click **System Management** > **Authority Management** > **Client Authorization** > **New** to go to the New page.

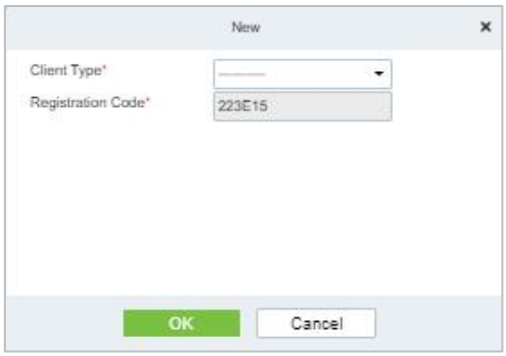


Figure 20- 41 Add Client Register

Parameter	Description
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.

Table 20- 5 Description Add Client Register parameter

20.2.4.2Reset

To reset a client, select the client and click **Reset**.

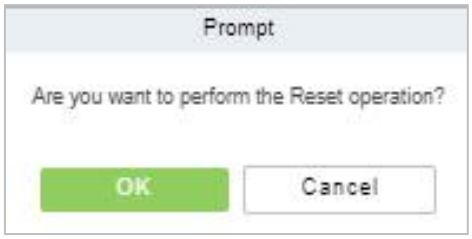


Figure 20- 42 Reset Option

20.2.4.3Delete

To delete a client, select the client and click **Delete**.

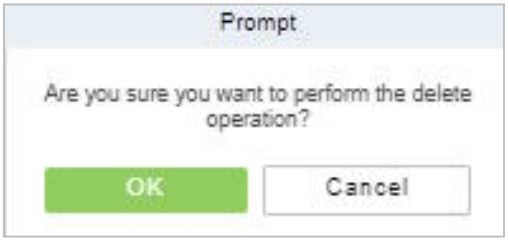


Figure 20- 43 Delete Option

Click **OK** to delete the client.

20.2.5Security Parameters

Click **System Management > Authority Management > Set Security Parameters**.

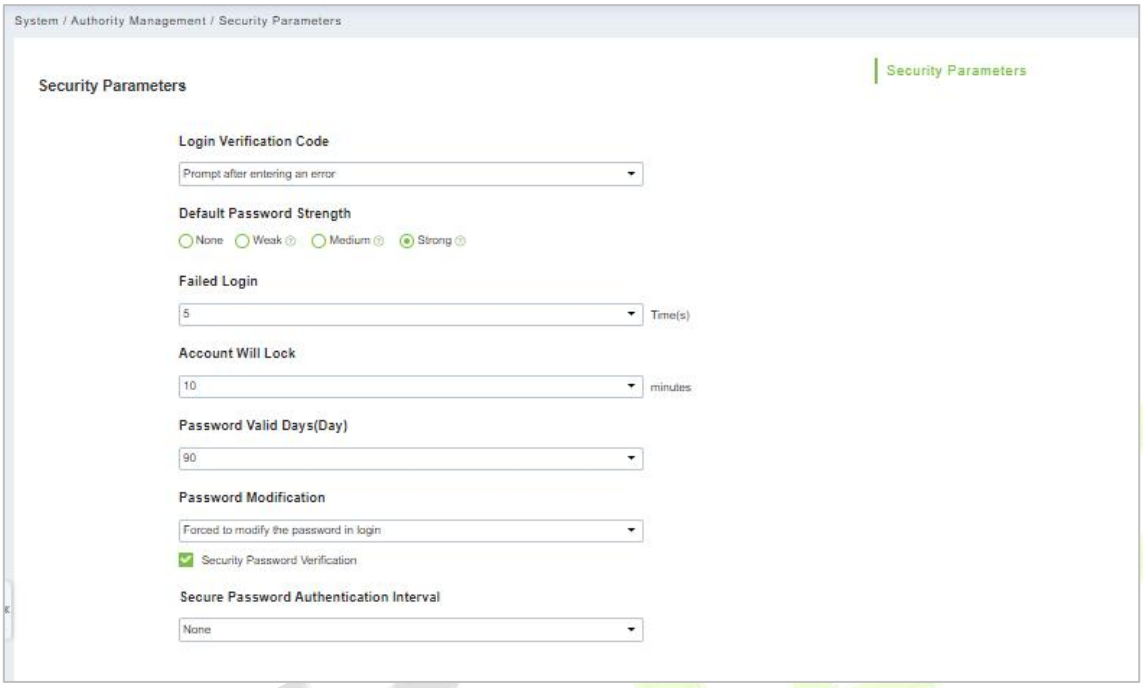


Figure 20- 44 Security Parameter Interface

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

The path is System -> Authority Management-> Set Security Parameter.

Figure 20- 45 Password Strength Option

Lock Account

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.

Figure 20- 46 Lock Account

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.

Figure 20- 47 Password Valid Days

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.

Figure 20- 48 Password Modification Option

Secure Password Authentication Interval

Figure 20- 49 Secure Password Authentication Interval

20.3 Communication Management

20.3.1 Device Commands

Click **System** > **Communication** Management > **Device Commands**, the commands lists will be displayed.

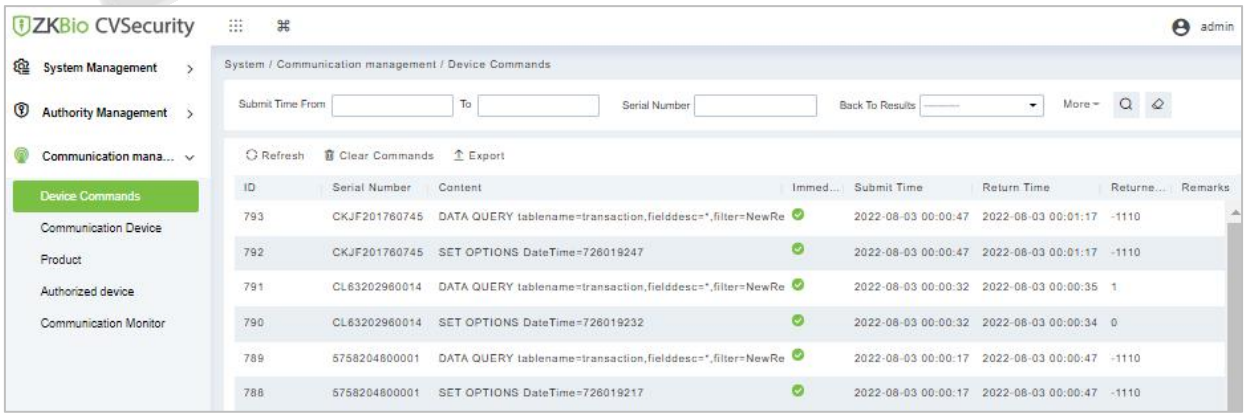


Figure 20- 50 Device Command interface

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 is failed to be issued.

20.3.1.1 Export

Export the command lists to the local host. You can export it 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=2AuthorizeTimezoneId=1AuthorizeDoorId=1 Pin=1AuthorizeTimezoneId=1AuthorizeDoorId=1 ...	false	2017-12-18 10:51:15	2017-12-18 10:51:21	0
1502	20100501999	DATA UPDATE mulcarduser Pin=2CardNo=5dec02LossCardFlag=0CardType=0 Pin=1CardNo=4412c5LossCardFlag=0CardType=0 ...	false	2017-12-18 10:51:14	2017-12-18 10:51:21	0

Figure 20- 51 Export File

20.3.1.2 Refresh

Click **Refresh** at the upper part of the list to load new temporary Device Commands.

20.3.1.3 Clear Commands

Click **Clear Commands** to clear the command lists.

20.3.2 Communication Device

Click **System > Communication Management > Communication,** 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.

Figure 20- 52 Communication Device Interface

20.3.2.1 View Authorized Device

View the authorized device information.

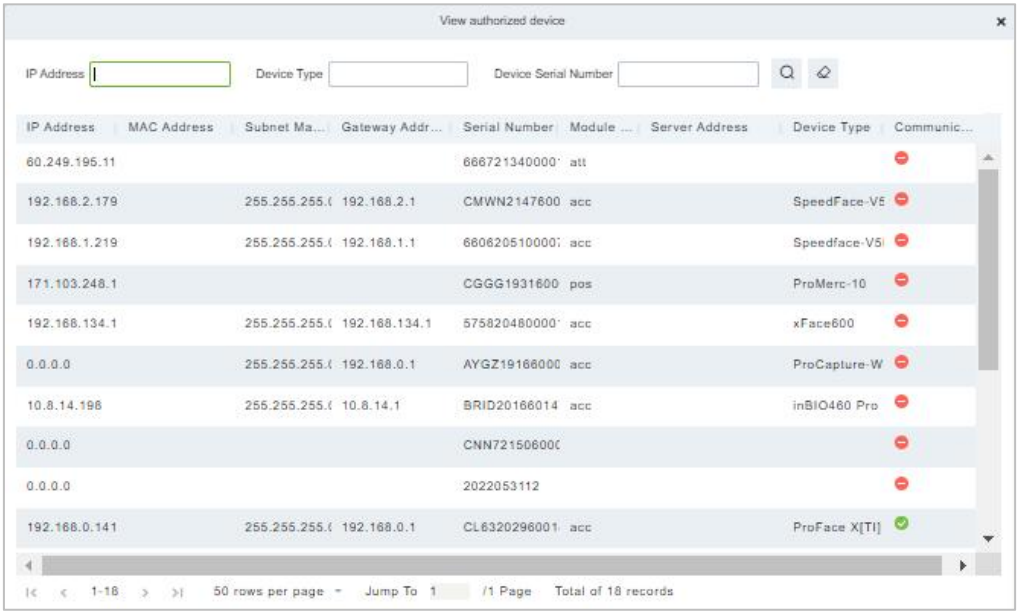


Figure 20- 53 View Authorized Device Interface

20.3.2.2Refresh

Click **Refresh** at the upper part of the list to load the new temporary Communication Device.

20.3.3Product

Click **System > Communication Management** > **Product,** and the product lists will be displayed.

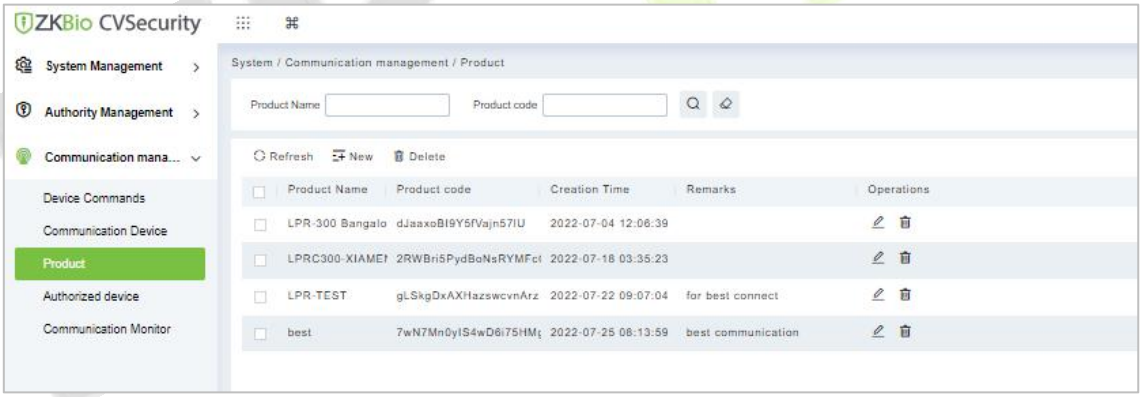


Figure 20- 54 Product Interface

20.3.3.1New

Click **System** > **Communication** Management > **Product** >**New**, to add the new product name.

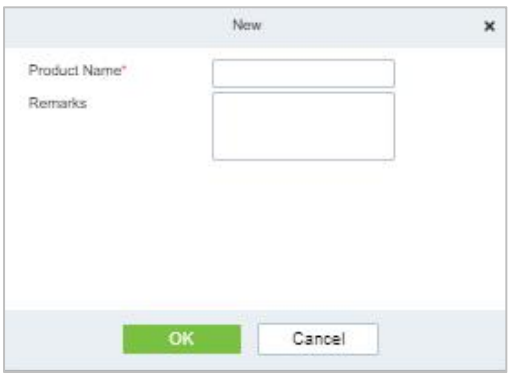


Figure 20- 55 Add Product Option

20.3.3.2Delete

Click **Delete** to delete the Product Operation.

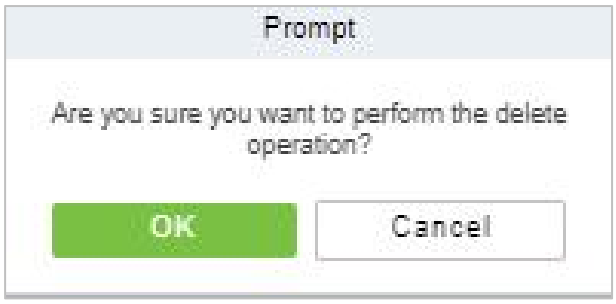


Figure 19- 54 Delete Product Option

20.3.3.3Edit

Click **Edit** to delete the Product information.

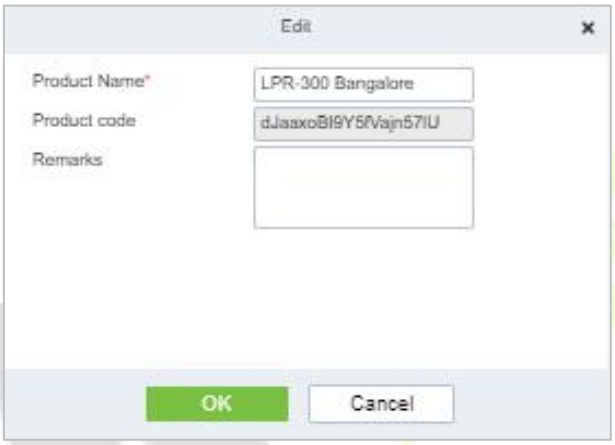


Figure 19- 55 Edit Product Information

20.3.4Authorized Device

Click **System** > **Communication Management** > **Authorized Device**, and the product lists will be displayed.

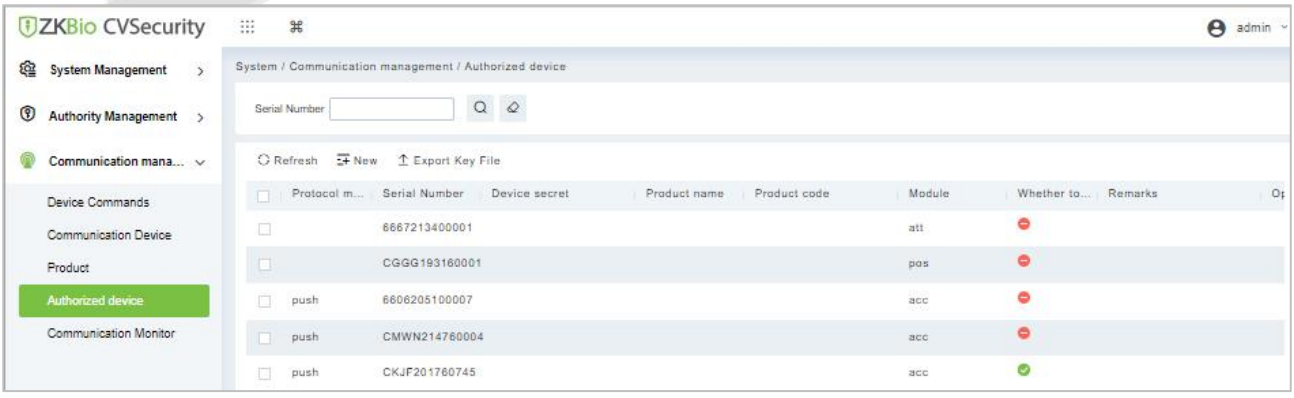


Figure 20- 58 Authorized Device Interface

20.3.4.1New

Click **System > Communication** > **Authorized Device** >**New,** to add the authorized product device.

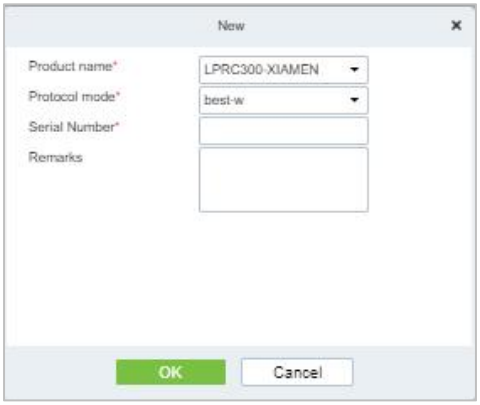


Figure 20- 59 Add Authorized Device

20.3.4.2Export Key File

Click **System** > **Communication** > **Authorized Device**, Select the protocols to export and click the **Export Key File,** to export the key file of the authorized product device.

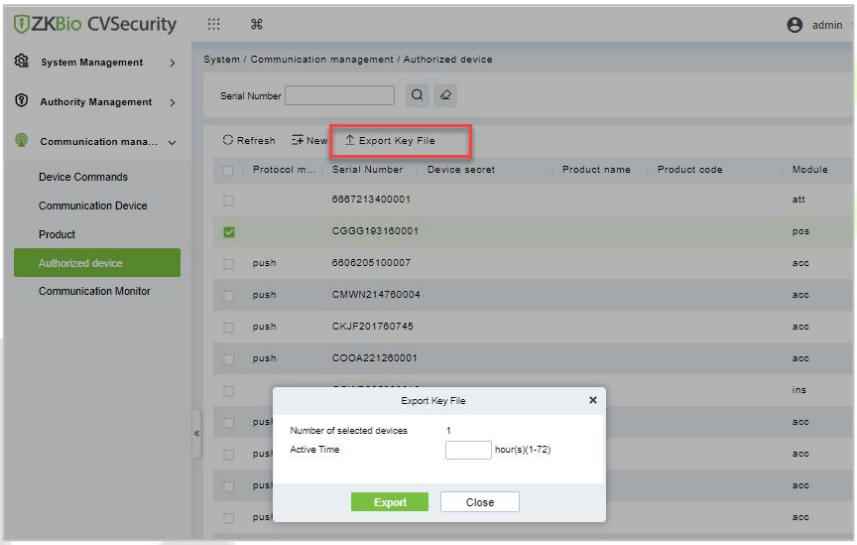


Figure 20- 60 Export Key Option

20.3.5Communication Monitor

Click **System** > **Communication** > **Communication Monitor**, and the communication mode will be displayed.

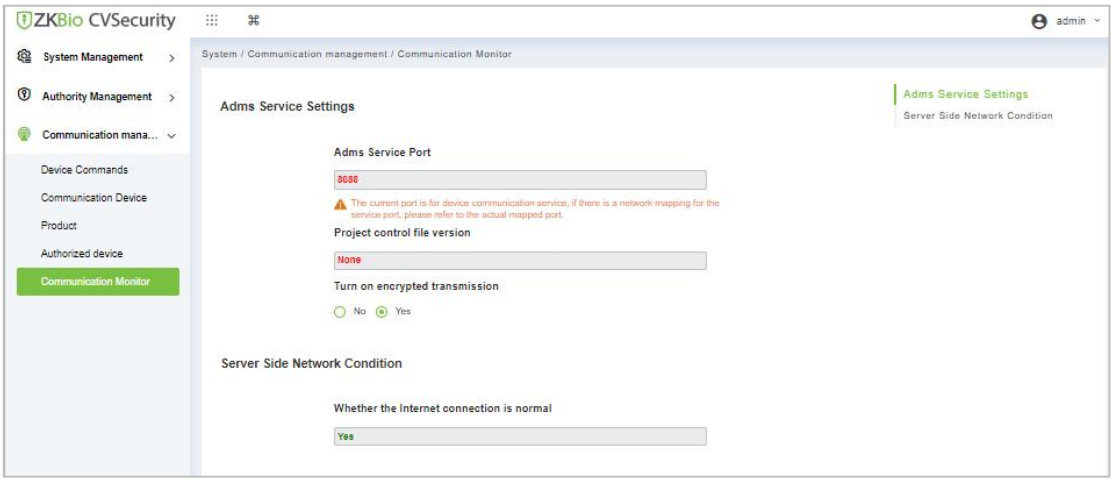


Figure 20- 61 Communication Monitor

20.4 Third Party Integration

20.4.1 LED Device

The system integrated outsourcing LED equipment (control card: lumens 3200/4200), provides a window to display data; it can provide customers personnel in the access area quantity statistics, real-time information about personnel going in and out and personnel information in the area, etc.

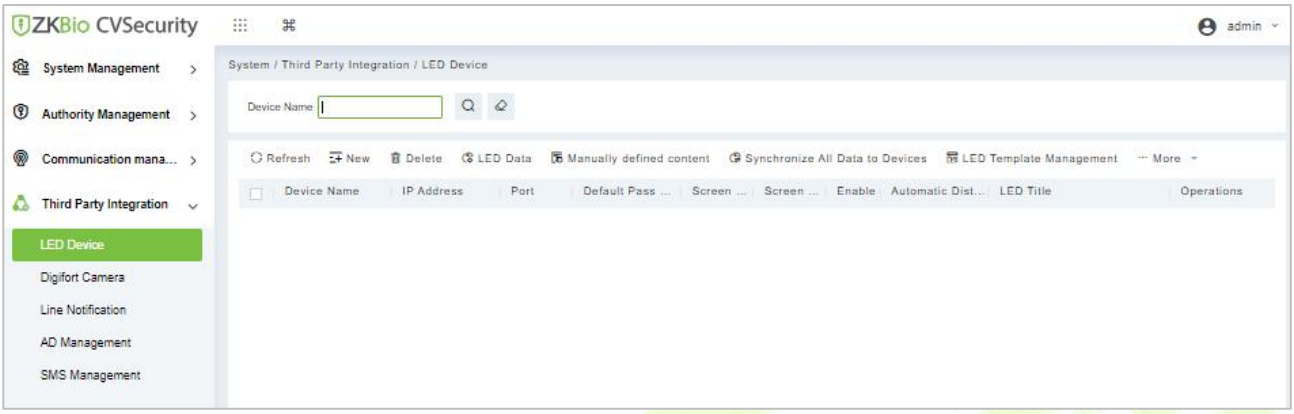


Figure 20- 62 LED Device

20.4.1.1 New

● Operation Step:

Click **System**> **Extended Management**> **LED Device**> **New**. The page is displayed as follows:

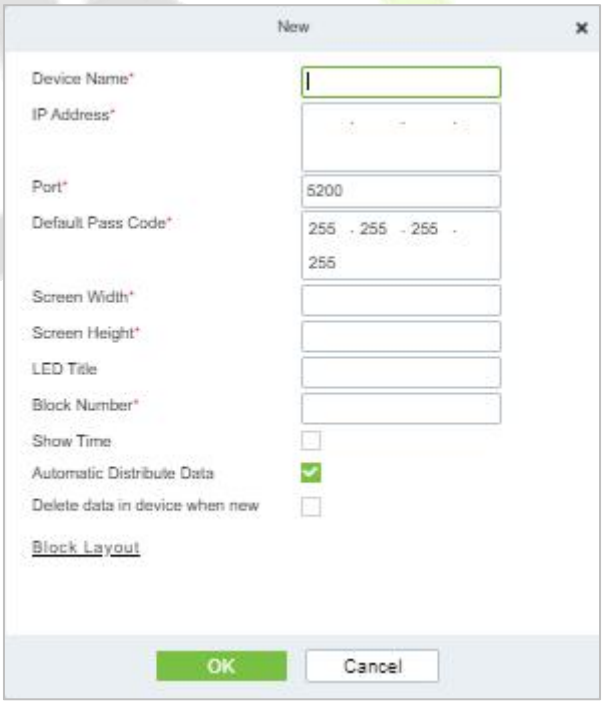


Figure 20- 63 Add LED Device

Parameter	Description
Device Name	Enter the name of the LED device.

IP Address	Enter the IP address of the LED device.
Port	Enter the port number. The default communication port is 5200.
Default Pass Code	Displays the pass code. The default value is 255.255.255.255.
Screen Width	Width of the dot matrix (resolution).
Screen Height	Height of the dot matrix (resolution).
LED Title	Select whether to display the title. If the parameter is left blank, the title is not displayed.
Block Number	Number of blocks that the LED is divided into (Note that the blocks do not contain the title and system time blocks).
Show Time	It will display time on the LED screen. Once you select it, you will find two options to choose from: Single Line and Multi-line Display. Choose according to your choice.
Automatic Distribute Data	By default, this parameter is selected. You send data to the LED in the access control module only when you select this parameter. Otherwise, the content to be sent needs to be manually defined.
Delete Data in the Device When New	Delete the original data in the device when adding an LED device.

Table 20- 6 Description Add LED Device Parameter

After you click **Block Layout**, the following box is displayed:

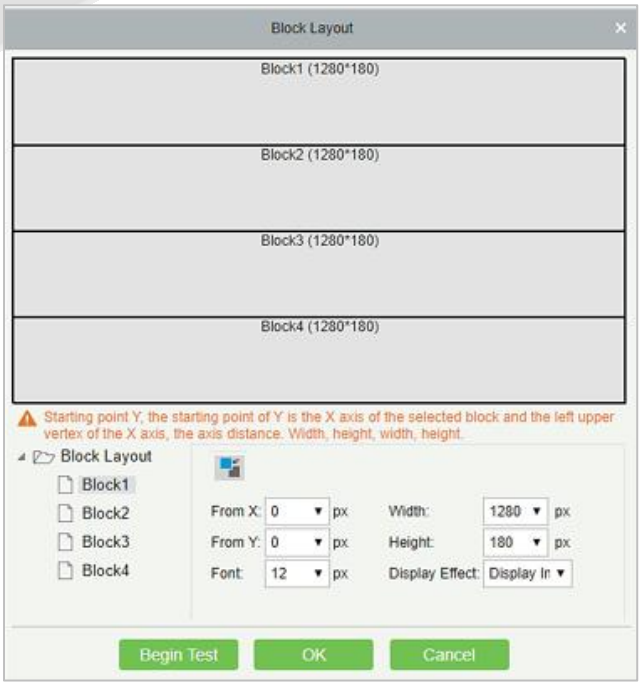


Figure 20- 64 Block Layout

✍Notes:

Parameters must be set for each block.

The height of each block must be equal to or larger than 12. Otherwise, the letters cannot be completely displayed.

The total height of all blocks cannot be larger than the screen height.

20.4.1.2Delete

Click a device name or **Delete** under Operation in the device list and click **OK** to delete the device or click **Cancel** to cancel the operation. Select one or more devices and click Delete above the list and click **OK** to delete the selected device(s) or click **Cancel** to cancel the operation.

20.4.1.3LED Data

LED data option let you view the details about outsourcing LED equipment such as zone device block details etc. user can add new LED data in this interface also.

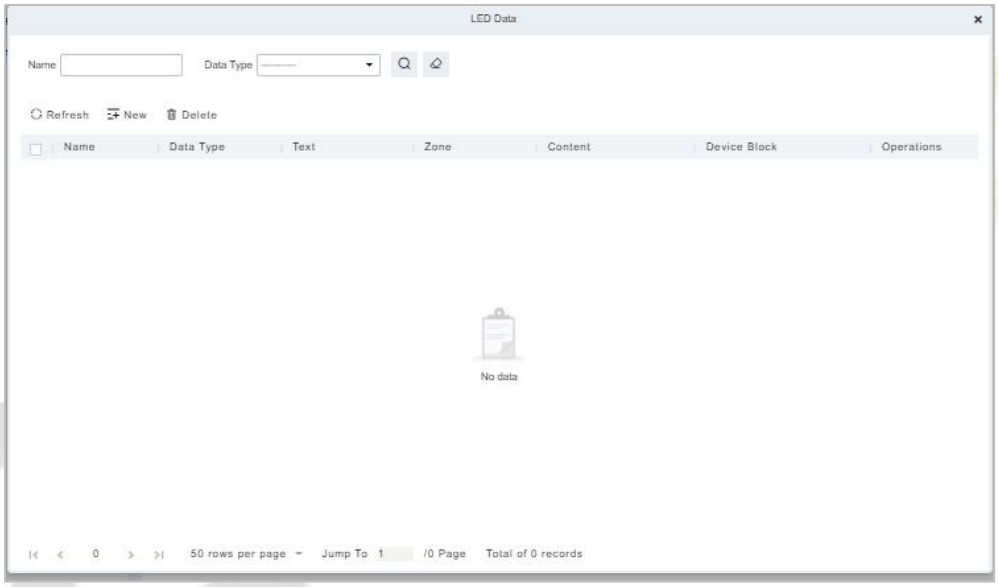


Figure 20- 65 LED Data

20.4.1.4Manually Defined Content

Select a device and click **Manually Defined Content**. The page is displayed as follows:

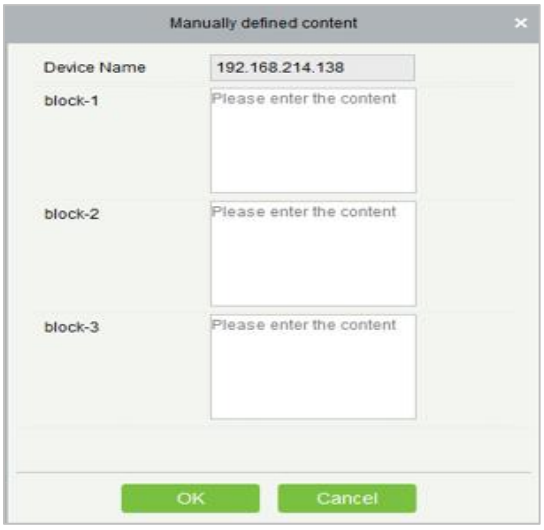


Figure 20- 66 Manually Defined Content Option

✍**Notes:**

At least one block must be selected for the distribution of manually defined content.

After the manually defined content is selected, the access control module cannot send data to the LED device.

Contact the technical support team for the intermediate table, line notification, active directory page, and other materials.

20.4.1.5LED Template Management

Through this function, you can create a template for the blocks. This template you can directly use at the time of adding an LED device. When you are adding an LED device, then after defining the dimensions of the block, you will be prompted to save the template as shown below:

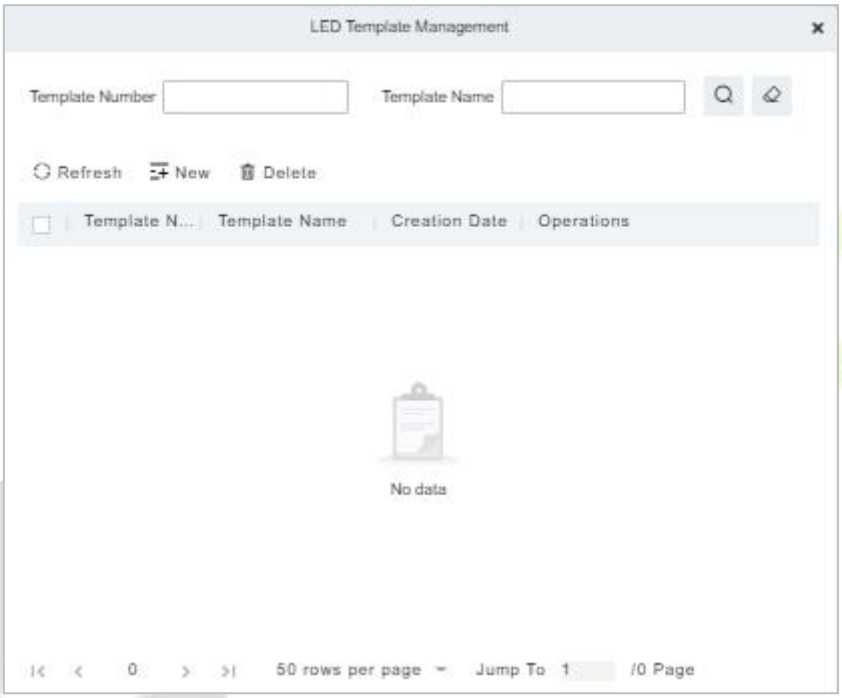


Figure 20- 67 LED Template Management

20.4.1.6Synchronize All Data to Devices

Synchronize the LED block layout and LED data set in the system to the device. Select a device, click **Synchronize All Data to Devices**, and then click **Synchronize** to synchronize the data.

20.4.1.7Edit

Click a device name or **Edit** under operation to go to the edit page. After editing the device, click **OK** to save the setting.

20.4.1.8Enable/Disable

Select a device and click **Enable/Disable** to start/stop using the device. If the device is enabled, data is transmitted to the device. Otherwise, no data is transmitted to the device.

20.4.1.9Restart

After you restart the device, the LED control card system will be restarted, data on the screen is cleared and data saved in the system is restored. After the device is successfully restarted, click **Synchronize All Data to Devices** to display all distributed content on the LED screen.

20.4.1.10 Modify IP Address

Modify the IP address of the device. The default IP address of the control card is 192.168.1.222.

20.4.2 Digifort Camera

It's integrated with third-party camera management system and the client uses “Digifort” to manage the cameras.

20.4.2.1 Sync with Server

It will help you to synchronize device with the server.

20.4.2.2 Delete

Click **Third Party Integration** > **Digifort Camera**, then select a Device Name, and click **Delete** > **OK** to delete.

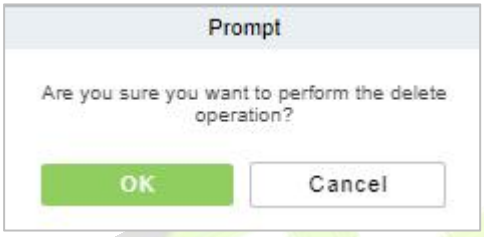


Figure 20- 68 Delete Option

20.4.2.3 Parameters

Click **Third Party Integration > Digifort Camera > Parameters** to update the server details.

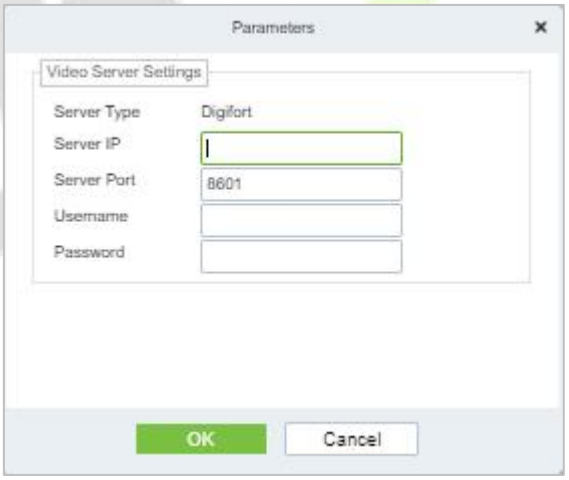


Figure 20- 69 Digifort Camera Device Parameters

Parameter	Description
Server Type	By default, the server settings “Digifort”.
Server IP	Enter the Arteco Server IP.
Server Port	Enter the Arteco Server Port.Default value is 8601

Username	Enter the Arteco User Username.
Password	Enter the User Password.

Table 20- 7 Description Digifort Camera Parameter

20.4.3Arteco Integration

Please refer to the attached operating instructions for ARTECO.

2-ZKBio CVSecurity Integra

20.4.4Line Notification

Click **System > Third Party integration > Line Notification** to enter the interface:

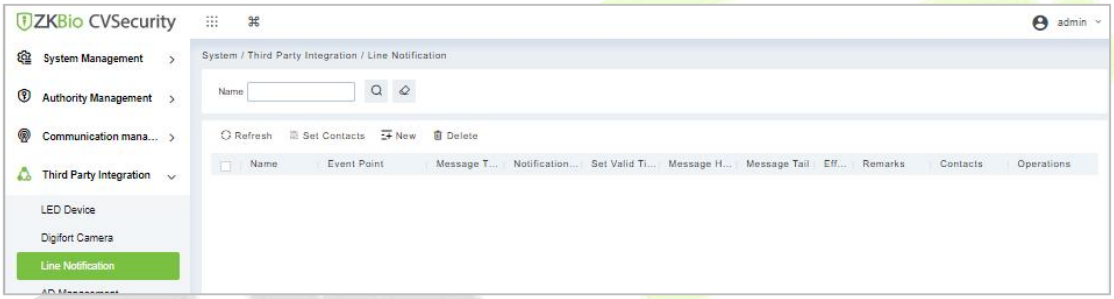


Figure 20- 70 Line Notification Interface

20.4.4.1Refresh

Click **Refresh** at the upper part of the list to load the new temporary line Notification.

20.4.4.2Set Contacts

Step 1: Add Line Integration. Log in ZKBio CVSecurity and go to **System > Third Part Integration > Line Integration**, then click **Set Contacts**.

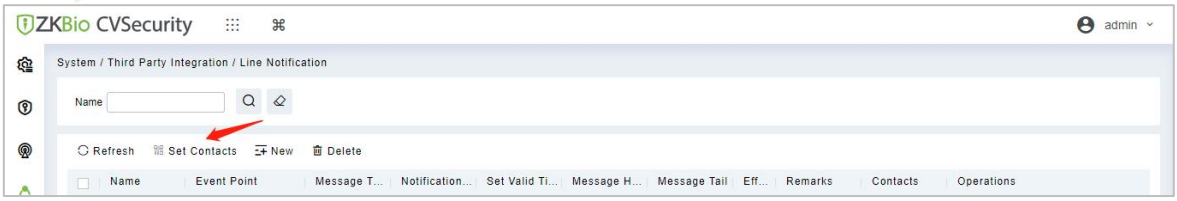


Figure 20- 71 Set Contacts Option

Step 2: After the windows is displayed, please click **New**.

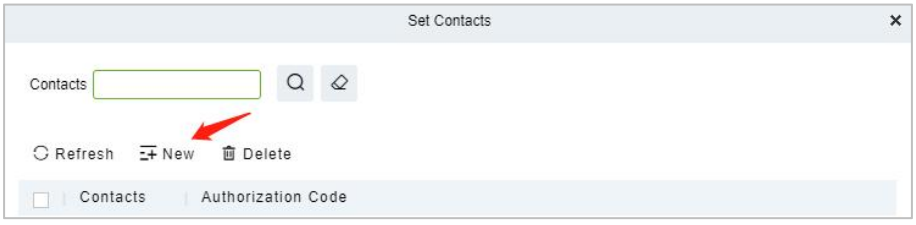


Figure 20- 72 Add Contacts Option

Step 3: After the windows is displayed, please click **Click to enter**.

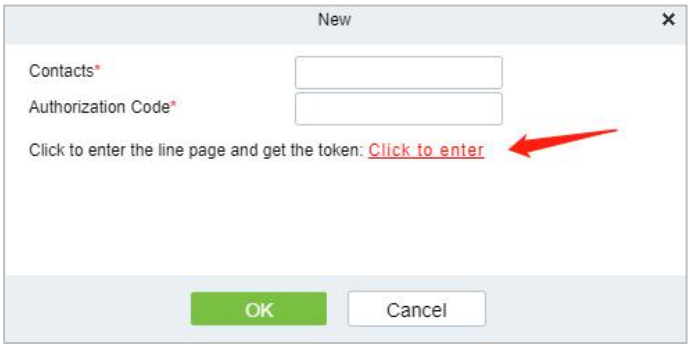


Figure 20- 73 New Option

Step 4: Line web page, please use the account and password of line to log in.

Figure 20- 74 Line Interface

Step 5: After login, slide down and click **Generate token**.

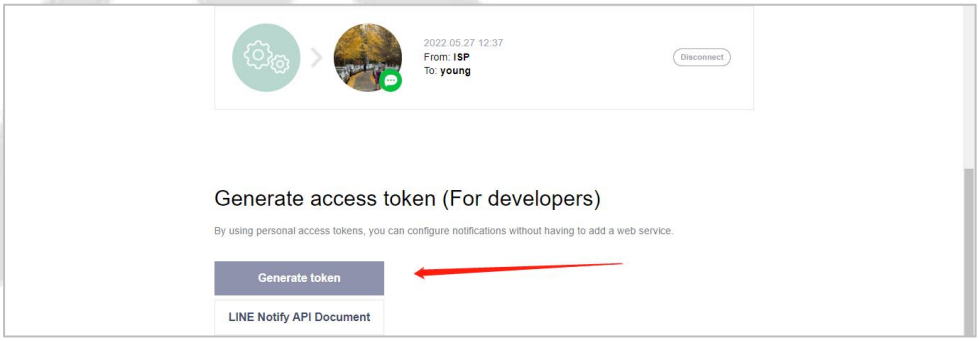


Figure 20- 75 Generate Token option

Step 6: Fill in the name of token and select the group you created earlier, then click Generate token

Note: The group you selected is used to receive Line-linked messages, please make sure that the group members do not disclose information security.

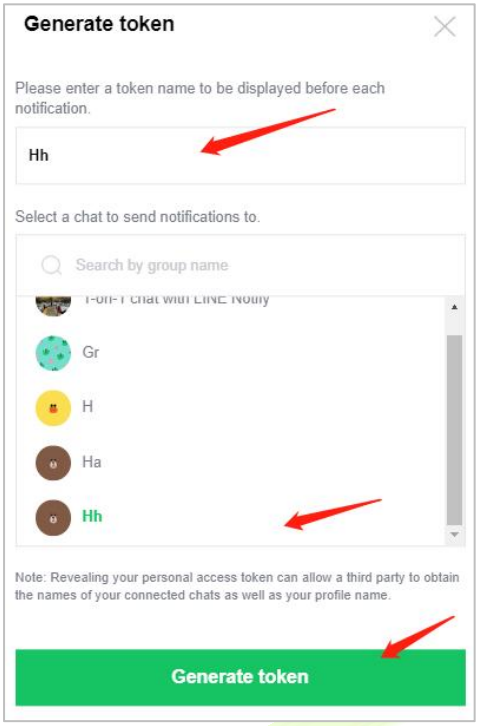


Figure 20- 76 Generate Token Option

Step 7: Please click **Copy**.

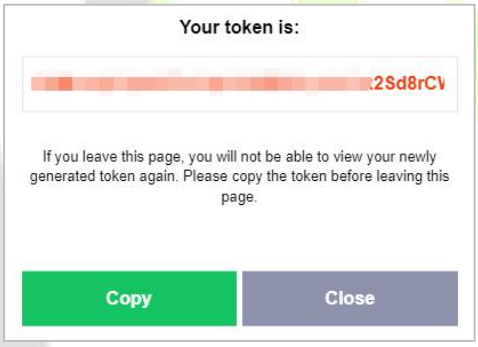


Figure 20- 77 Token Interface

Step 8: Back to **ZKBio CVSecurity > System Page**, paste the Authorization Code and fill in Contacts.

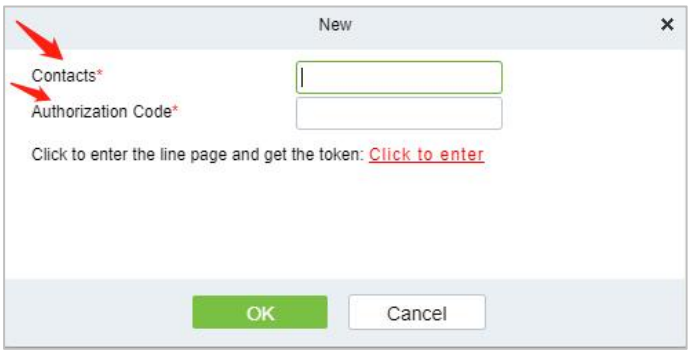


Figure 20- 78 Add Contact Option

20.4.4.3New

Step 1: Click **Third Party > Line Notification > New** to enter the Add Levels editing interface:

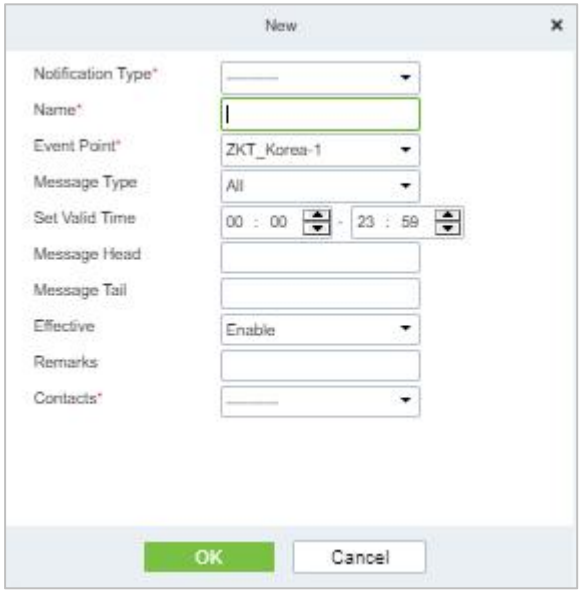


Figure 20- 79 Add Line Notification

Step 2: Fill in all the required details and save. Once saved, you will get the template at the Line Notification device adding interface.

20.4.4.4Delete

Click **Third Party** > **Line management**, then select a receiver, and click **Delete** > **OK** to delete.

20.4.5AD Management

20.4.5.1Server Configuration

●Operation Step:

Step 1: In the System module, select **Third Party Integration > AD Management**.

Step 2: In the **AD Management** interface, fill in the **Server Configuration** as required in the details below.

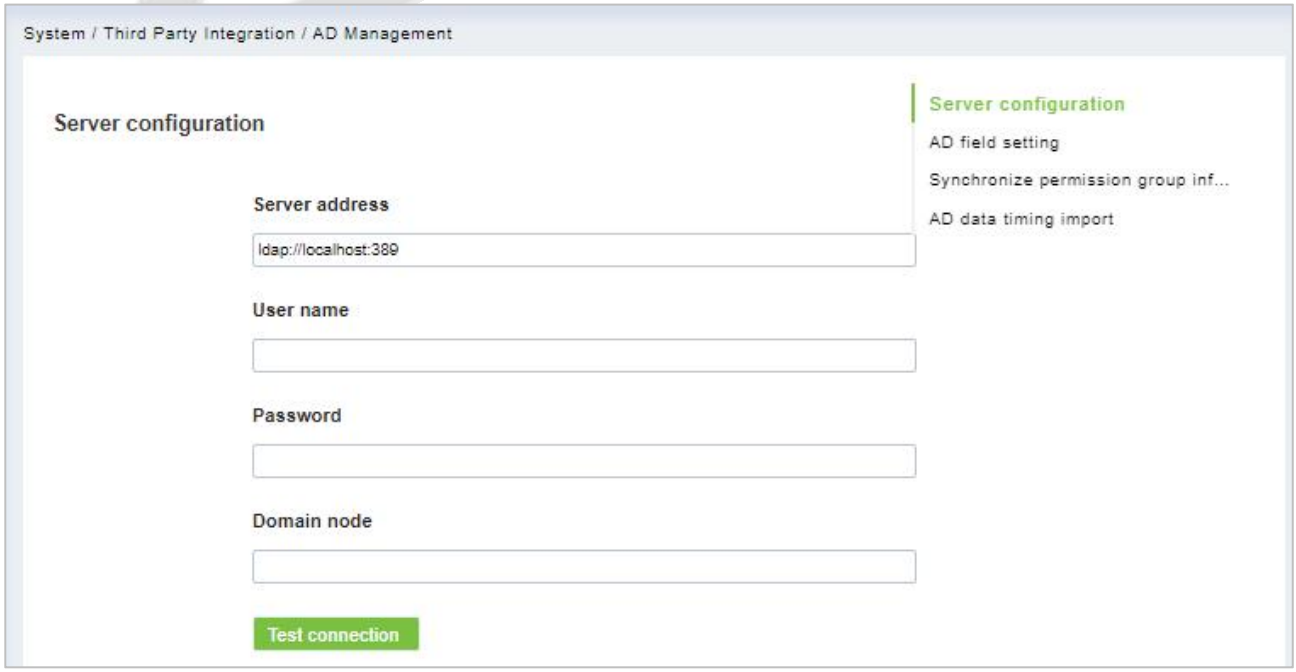


Figure 20- 80 Ad Management Interface

20.4.5.2AD Field Setting

● Operation Step:

Step 1: In the System module, select **Third Party Integration > AD Management**.

Step 2: In the **AD Management** interface, fill in the **AD field setting** as required in the details below.

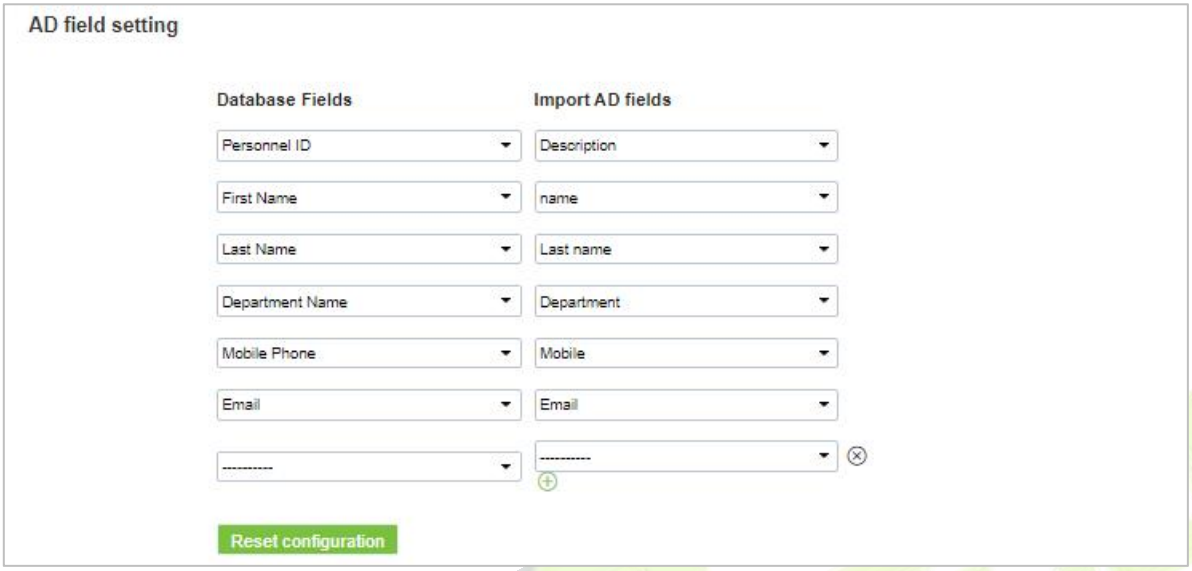


Figure 20- 81 AD Field Setting

20.4.5.3Synchronize Permission Group Information

● Operation Step:

Step 1: In the System module, select **Third Party Integration > AD Management**.

Step 2: In the **AD Management** interface, fill in the **Synchronize permission group information** as required in the details below.

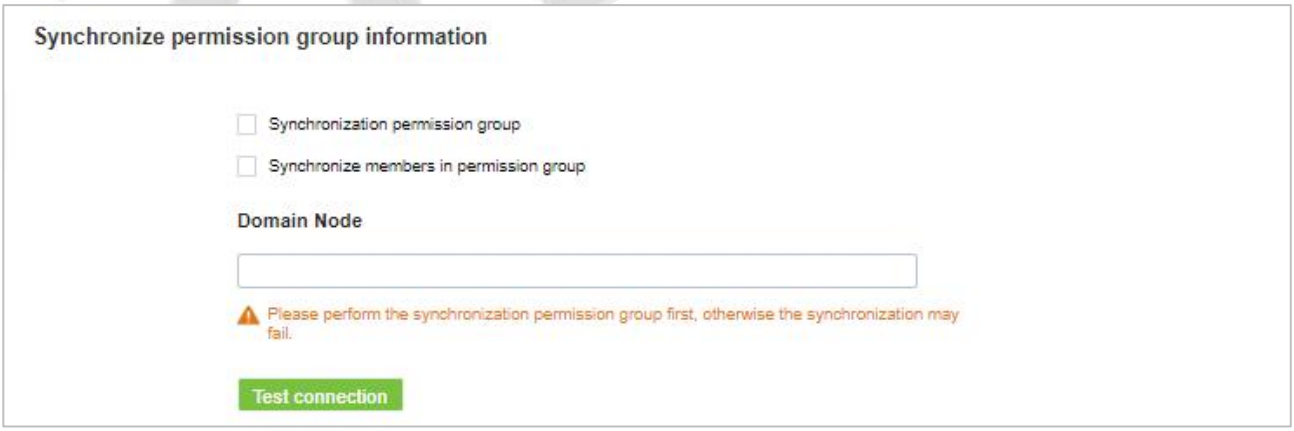


Figure 20- 82 Synchronize Permission Group Information

20.4.5.4AD Data Timing Import

● Operation Step

Step 1: In the System module, select **Third Party Integration > AD Management**.

Step 2: In the **AD Management** interface, fill in the **AD data timing import** as required in the details below.

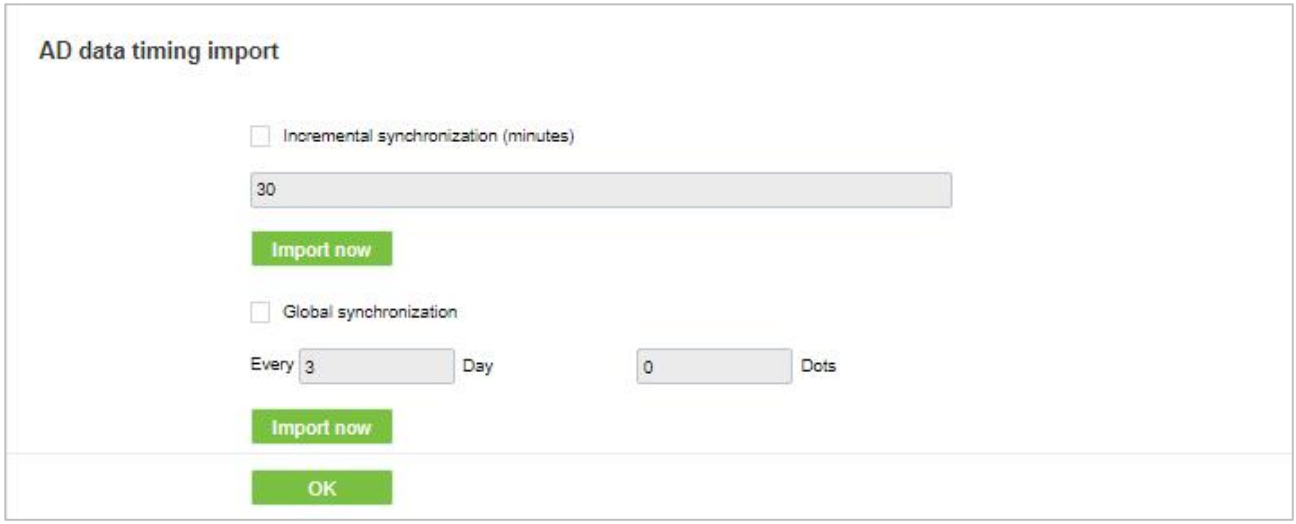


Figure 20- 83 AD Data Timing Import

Note: Please refer to the documentation for more details*3-ZKBio CVSecurity AD (Active Directory) Function Introduction.pdf*

20.4.6SMS Management

The SMS Management feature helps in sending text messages to the personnel in case of any access or elevator event. If the checkbox is selected, the message will be sent to the corresponding person.

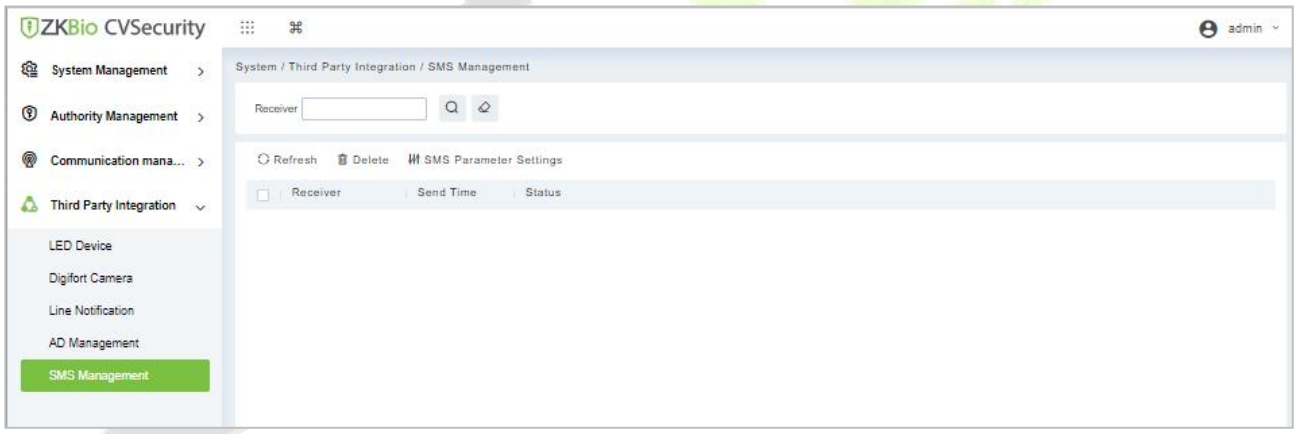


Figure 20- 84 SMS Management Interface

20.4.6.1Refresh

Click **Refresh** at the upper part of the list to load a new temporary SMS Management.

20.4.6.2Delete

Click **Third Party** > **SMS Management**, then select a receiver, and click **Delete** > **OK** to delete.

20.4.6.3SMS Parameter Settings

Supports sending text message to Personnel once any access or elevator event occurs.

After selecting the checkbox next to the Mobile Number, the system will send an email to the relevant person once access or an elevator event occurs.

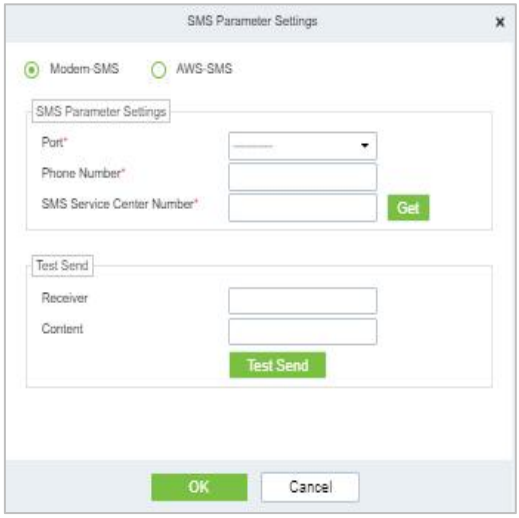


Figure 20- 85 Modern SMS Parameter Setting

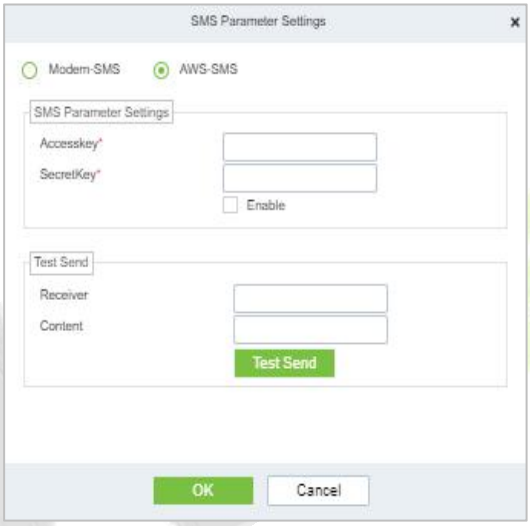


Figure 20- 86 AWS-SMS Parameter Settings

20.4.7Zoom

- **Supports binding one Zoom ID to each meeting room, enabling the generation of an online meeting link after app-based reservation.**

Step1: Open the App Marketplace and log in; after logging in, click **Build app.**

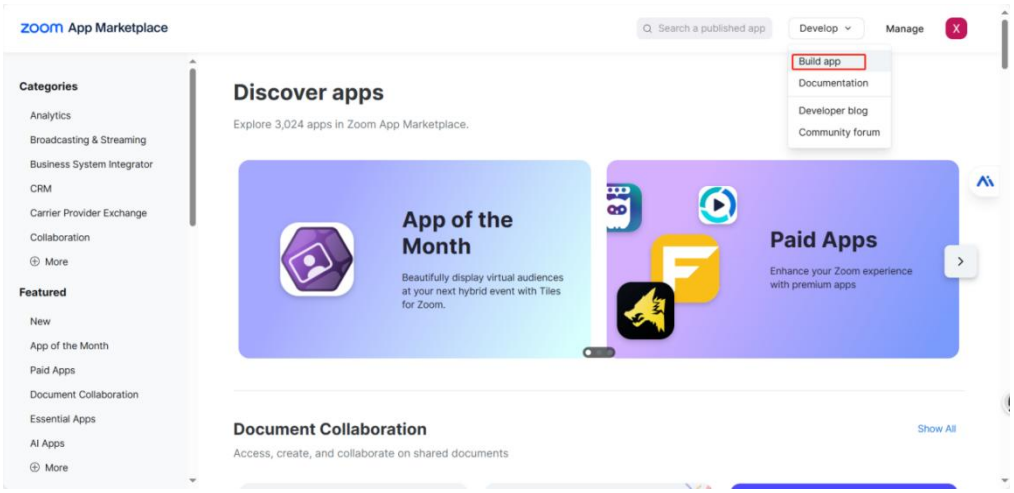


Figure 20- 87 Build app

Step2: Select **Server to Server OAuth App** and create App Name.

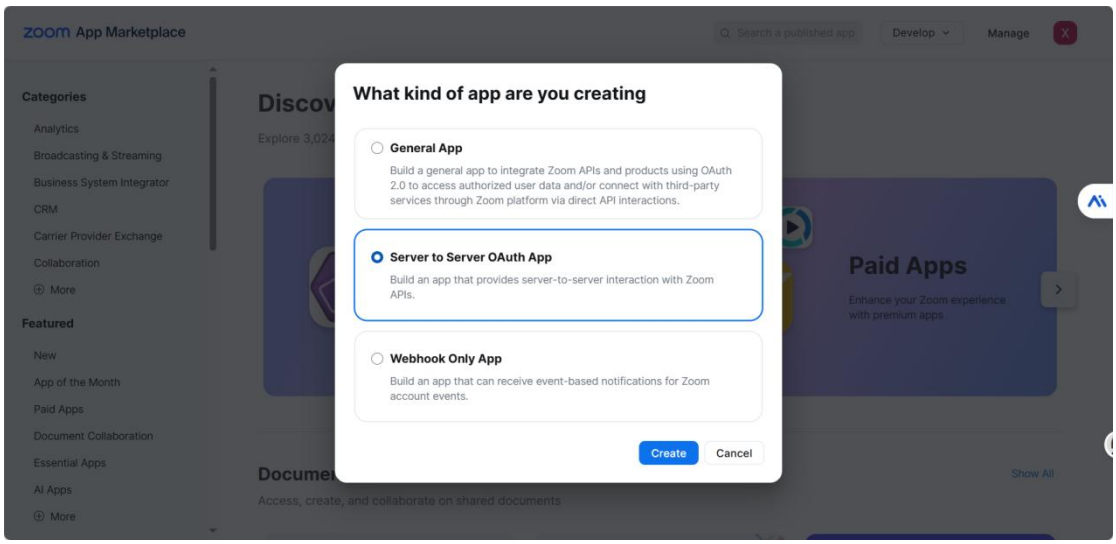


Figure 20- 88 Build app

Enter the app name.

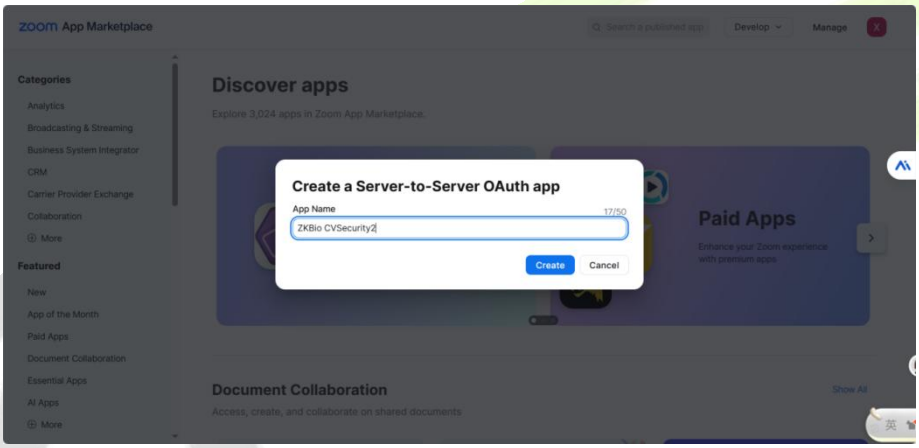


Figure 20- 89 Build app

Step3: After creation, APP Credentials will appear.Click "Continue" to proceed to the next step.

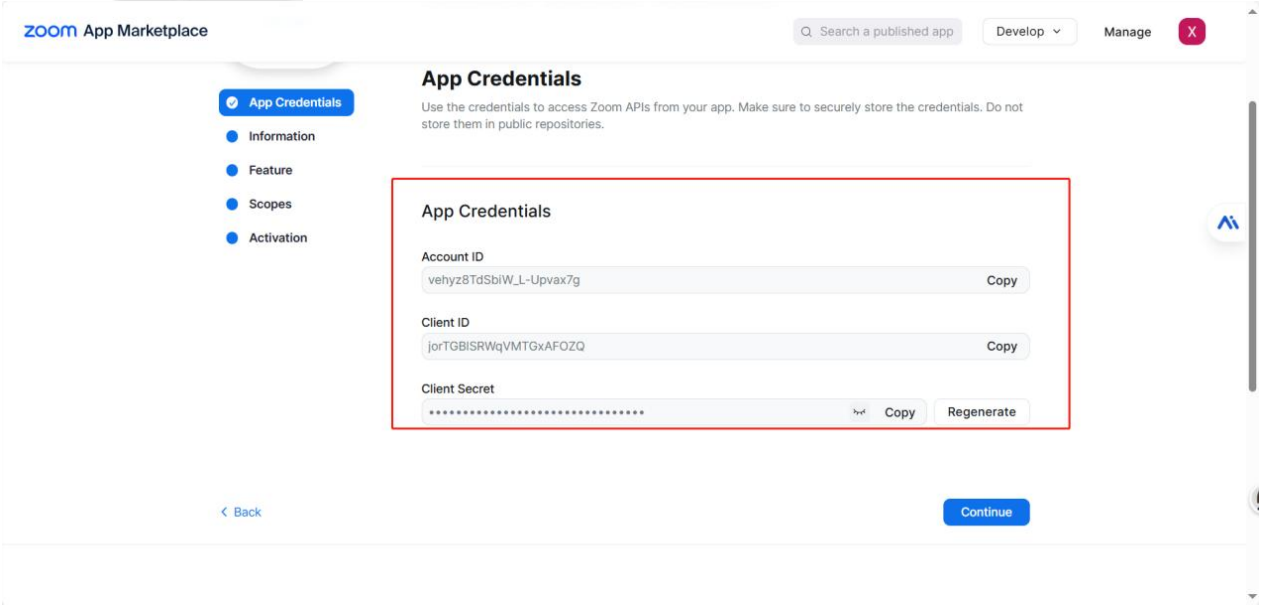


Figure 20- 90 APP Credentials

Step4: Fill in all the blanks in Basic Information and click "Continue".

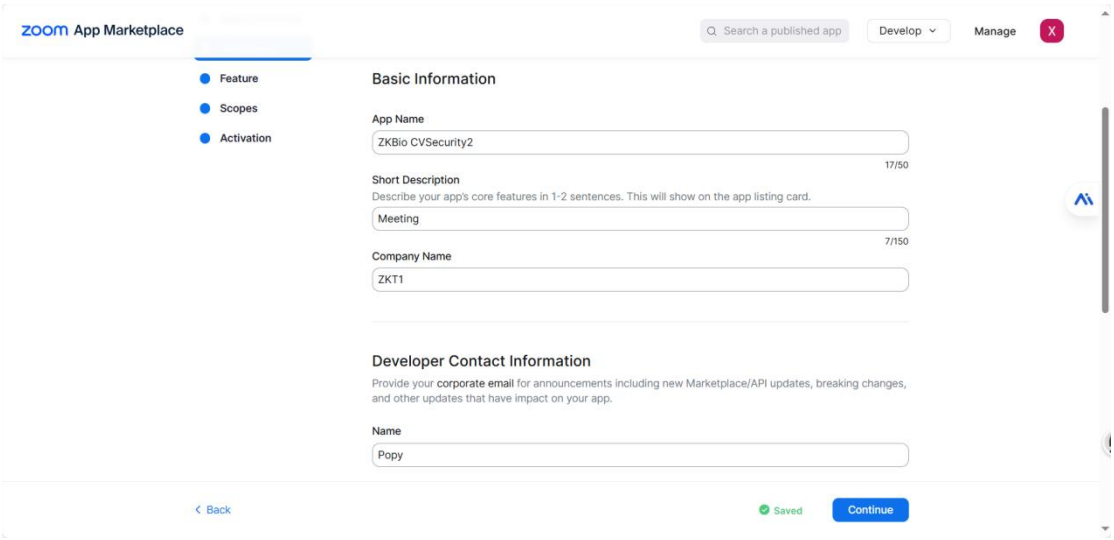


Figure 20- 91

Step5: Add Features :This page does not need to be operated. Click "Continue".

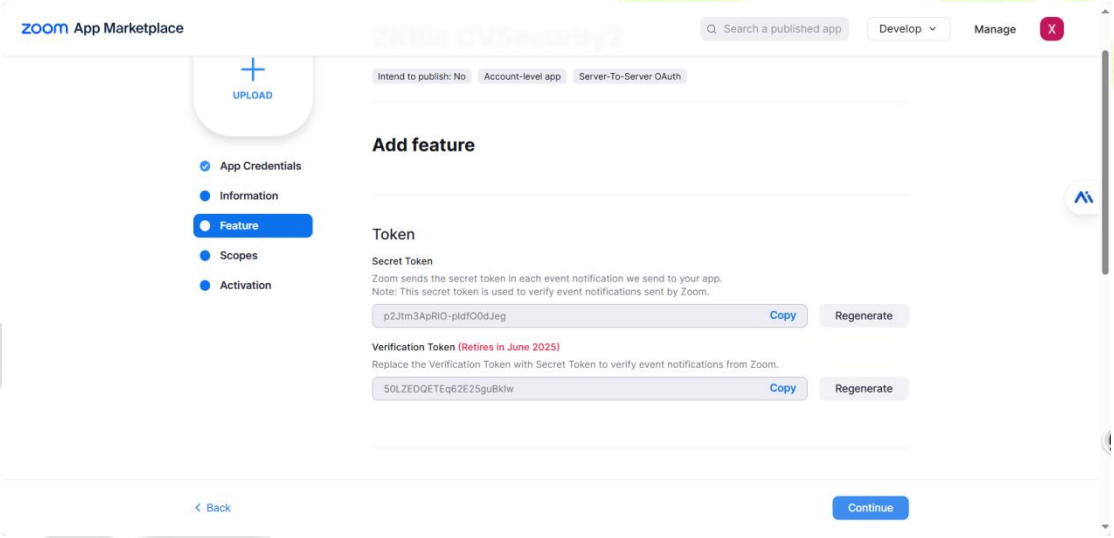


Figure 20- 92

Step6: Click "Add Scopes", select Meeting, and check the required Scopes as needed. Click "Continue".

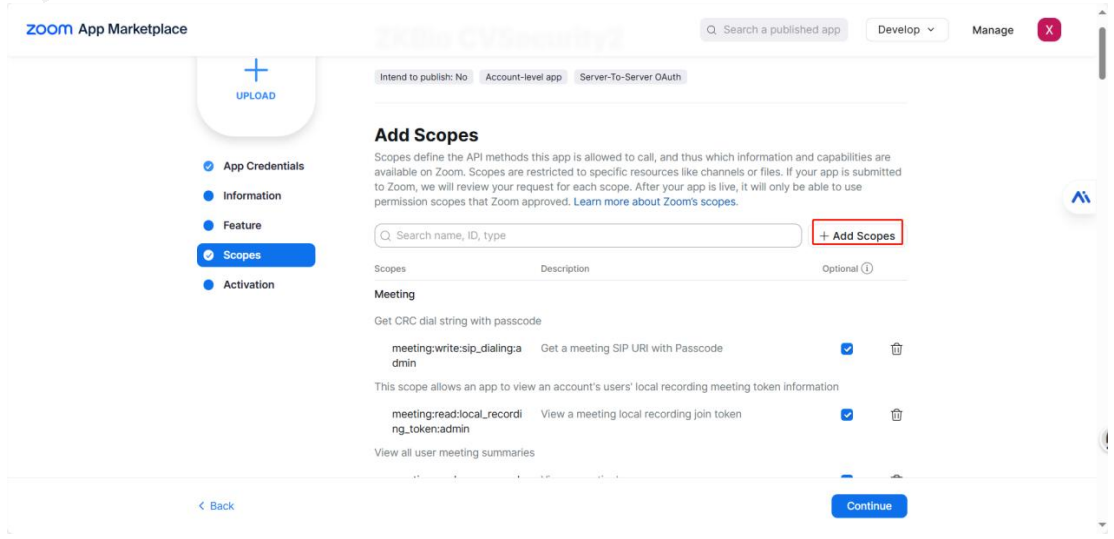


Figure 20- 93

Step7: Then click "Activate your app".

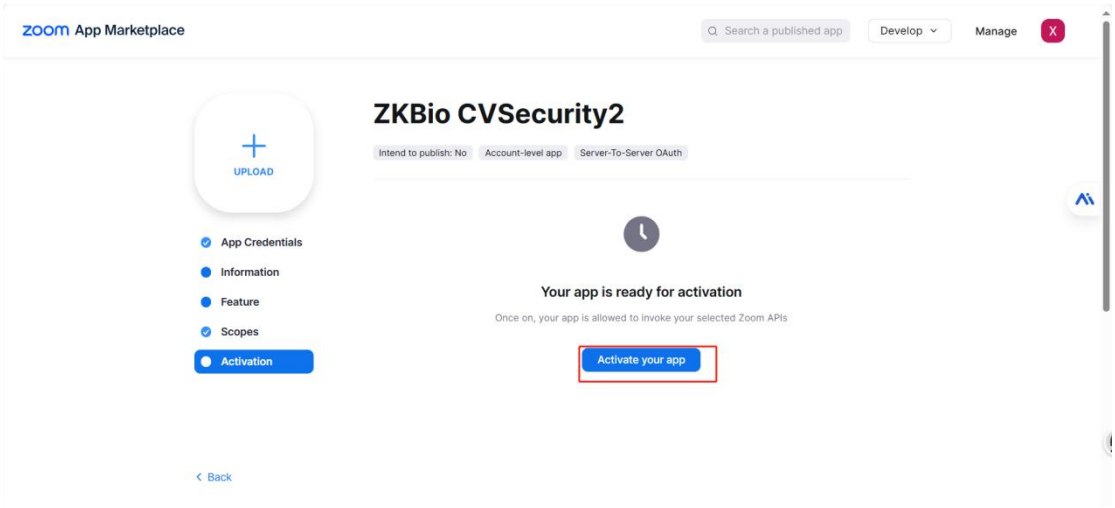


Figure 20- 94

Until the display activation is successful.

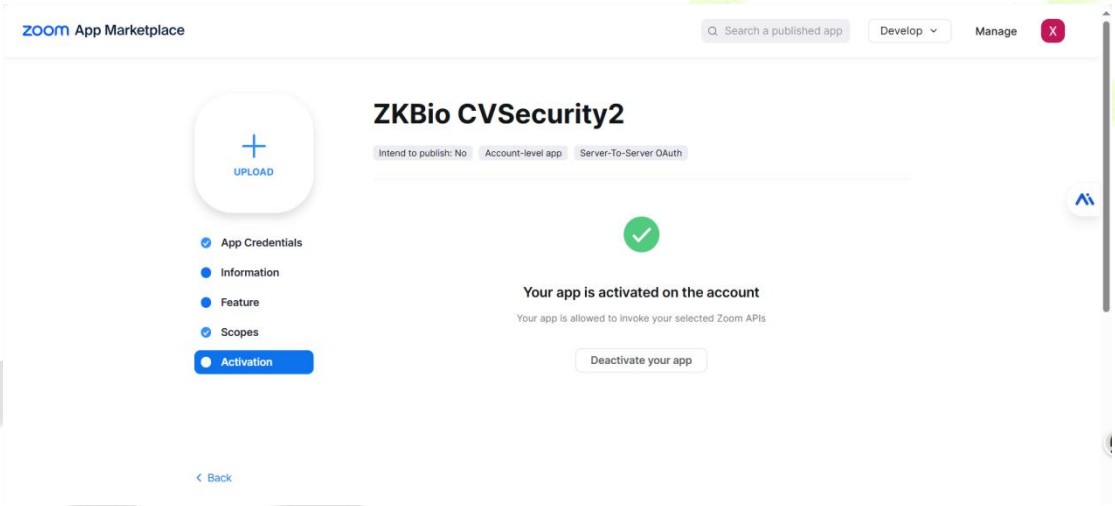


Figure 20- 95

Step8: Then go back to the **APP Credentials** and copy the values in this field to **ZKBio CVSecurity-System-Third Party Integration-ZOOM** configuration page.

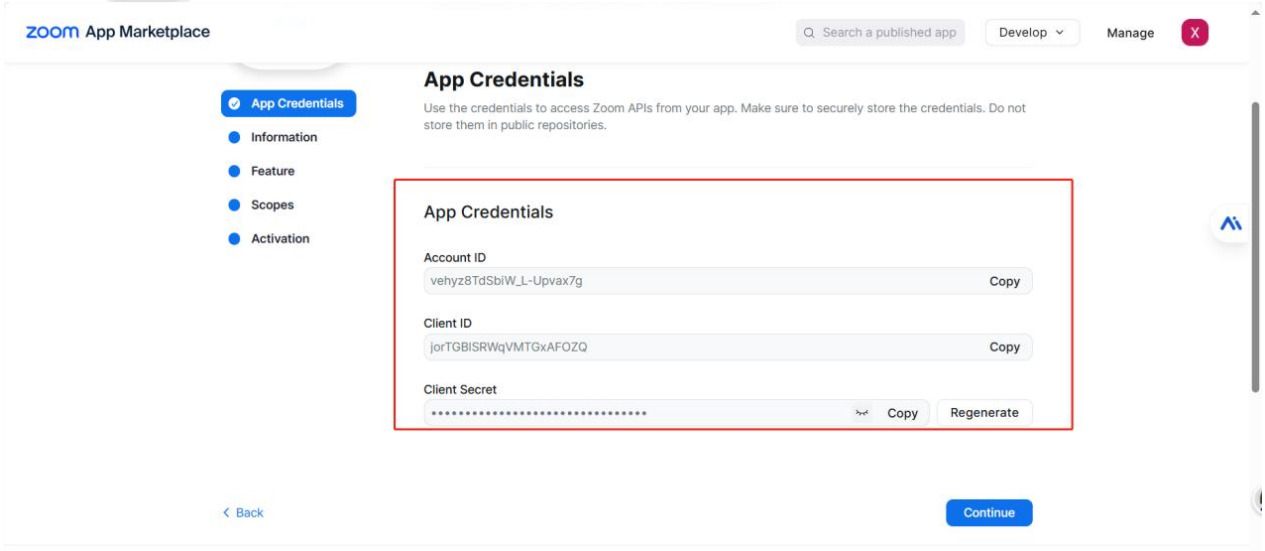


Figure 20- 96

Click "New", copy the corresponding ID, paste it in, and then click "OK".

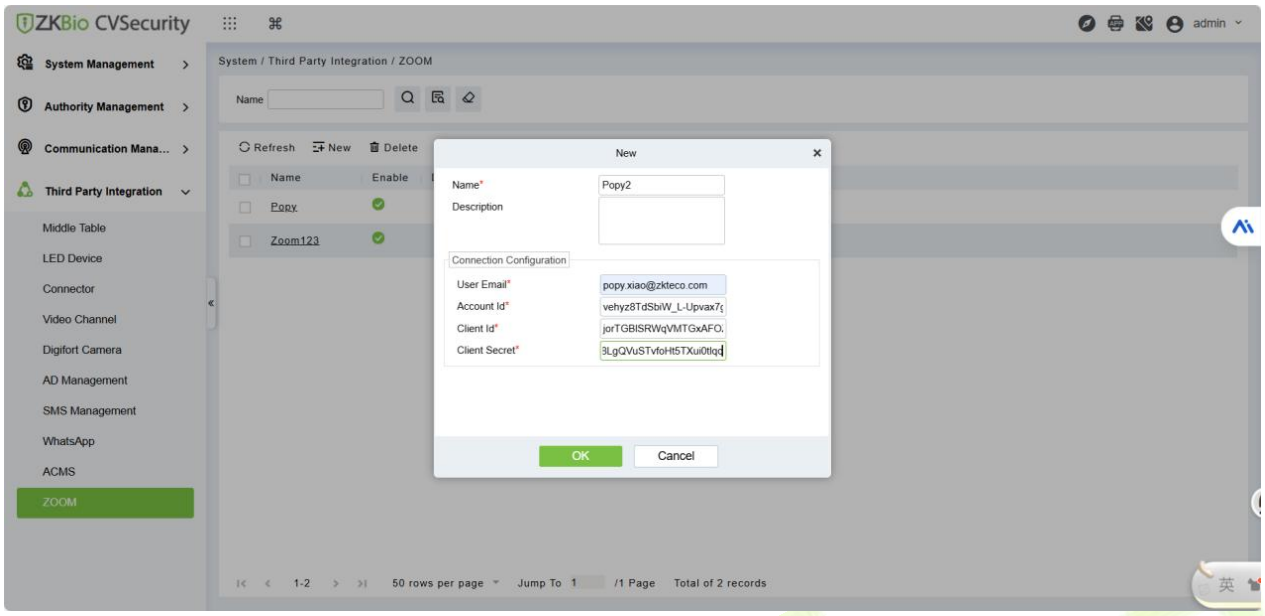


Figure 20- 97

Click "OK" to return Operation Succeed.

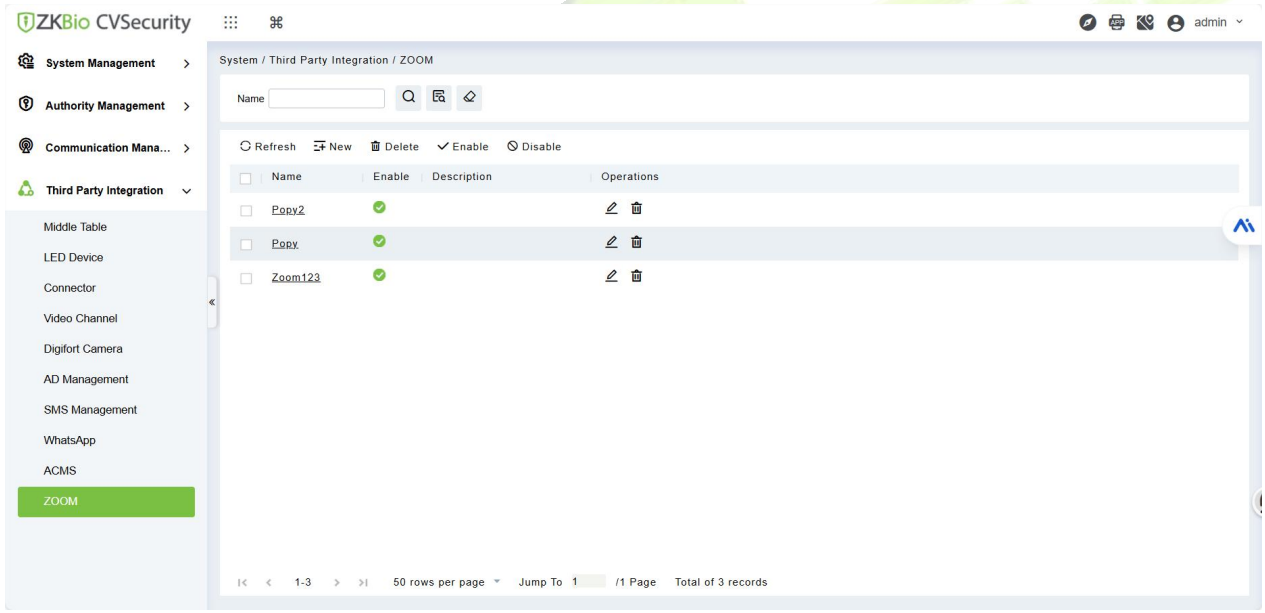


Figure 20- 98

Step9: Now, you can go to the **Space Management module-Space**, click "New" to add a meeting room, you can select the corresponding meeting room resource from Zoom.Fill in the basic information , then select the Zoom App you have created in Create an online meeting, and finally click "OK".

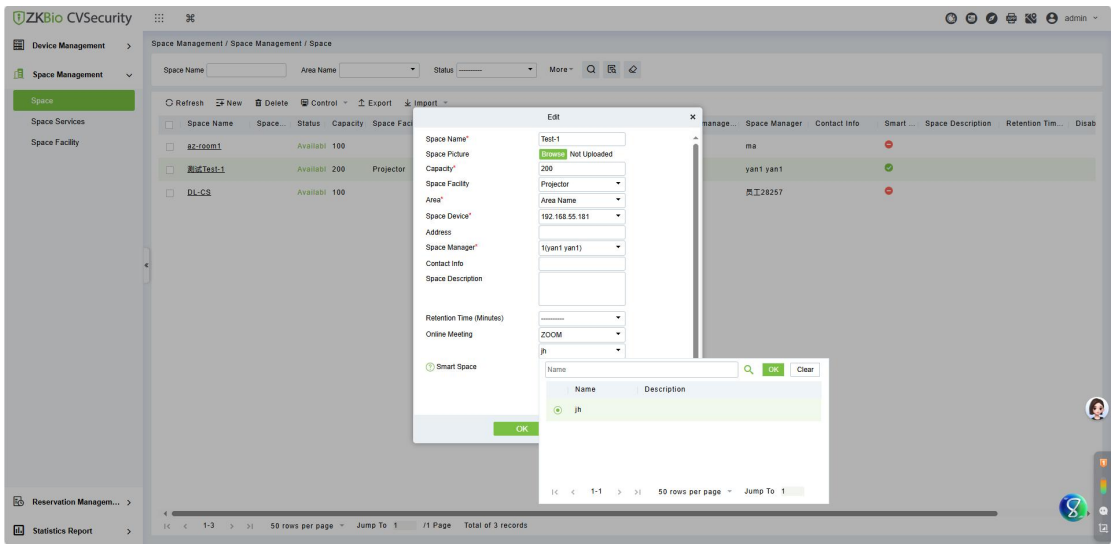


Figure 20- 99

Step10: You can go to the **Reservation Management module-Space Reservation**, click the conference to start booking the meeting.

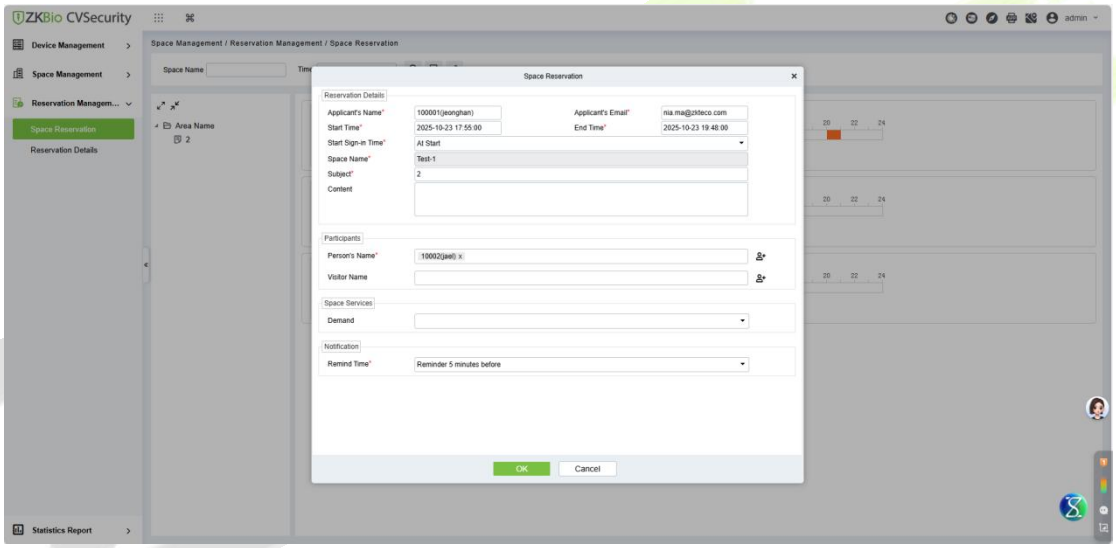
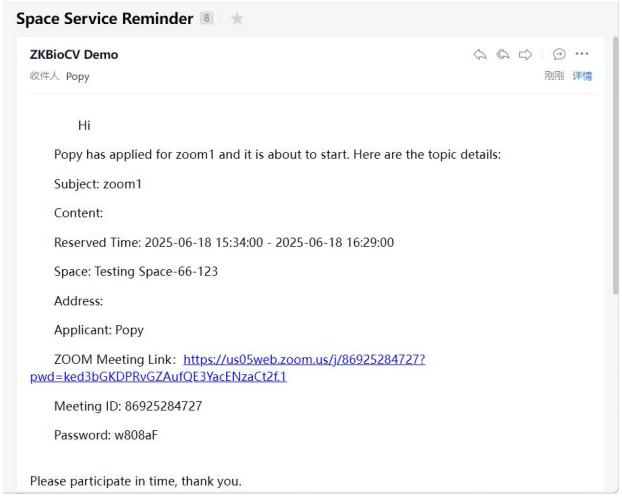


Figure 20- 100 Booking the meeting

The corresponding participants will receive the online meeting link with Zoom in the corresponding meeting reservation information.



Space Service Reminder

ZKBioCV Demo

收件人 Popy

刚刚 详情

Hi

Popy has applied for zoom1 and it is about to start. Here are the topic details:

Subject: zoom1

Content:

Reserved Time: 2025-06-18 15:34:00 - 2025-06-18 16:29:00

Space: Testing Space-66-123

Address:

Applicant: Popy

ZOOM Meeting Link: https://us05web.zoom.us/j/86925284727?pwd=ked3bGKDPRvGZAufQE3YacENzaCt2f.1

Meeting ID: 86925284727

Password: w808aF

Please participate in time, thank you.

Figure 20- 101 Email

20.4.8Microsoft 365

●Integrated with Microsoft 365 to synchronize Teams/Outlook meeting reservations with conference room devices.

20.4.8.1Register Application:

Step1: Enter System → Third Party Integration → Microsoft 365, click "Download Certificate" to download the certificate on the ZKBio CVSecurity platform.

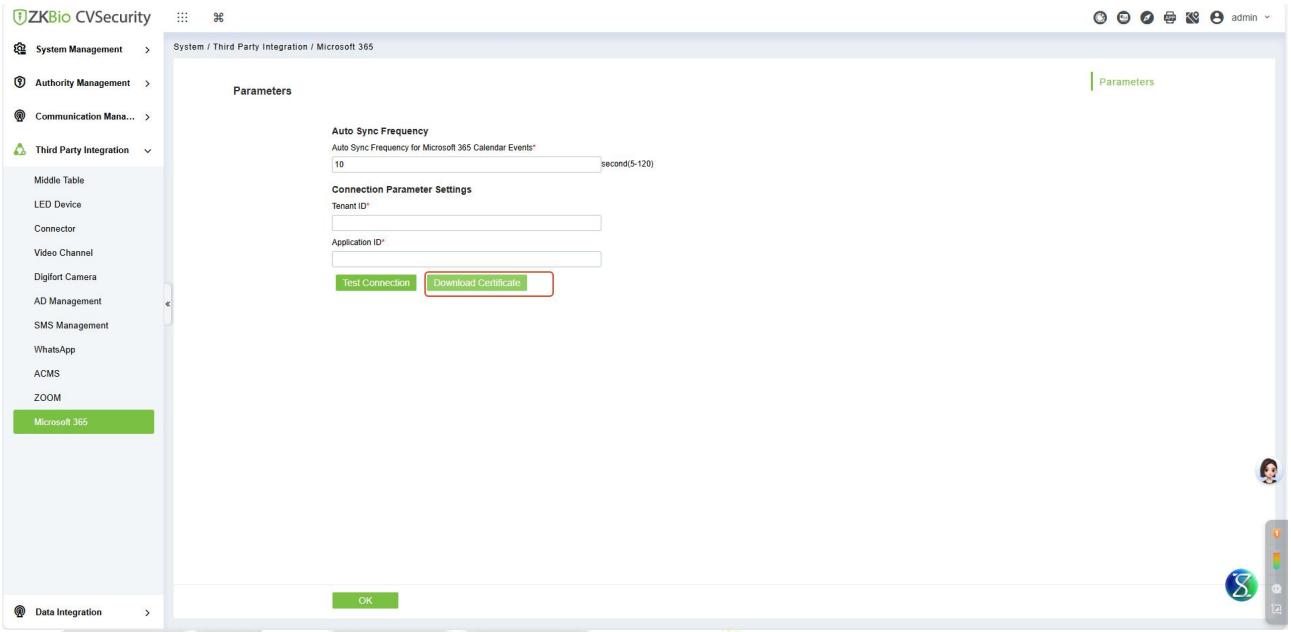


Figure 20- 101 Download Certificate

Step2: Enter the Microsoft Entra admin center, click "App registrations" → "New registration", and add a new application.Fill in the relevant information and click "Register".

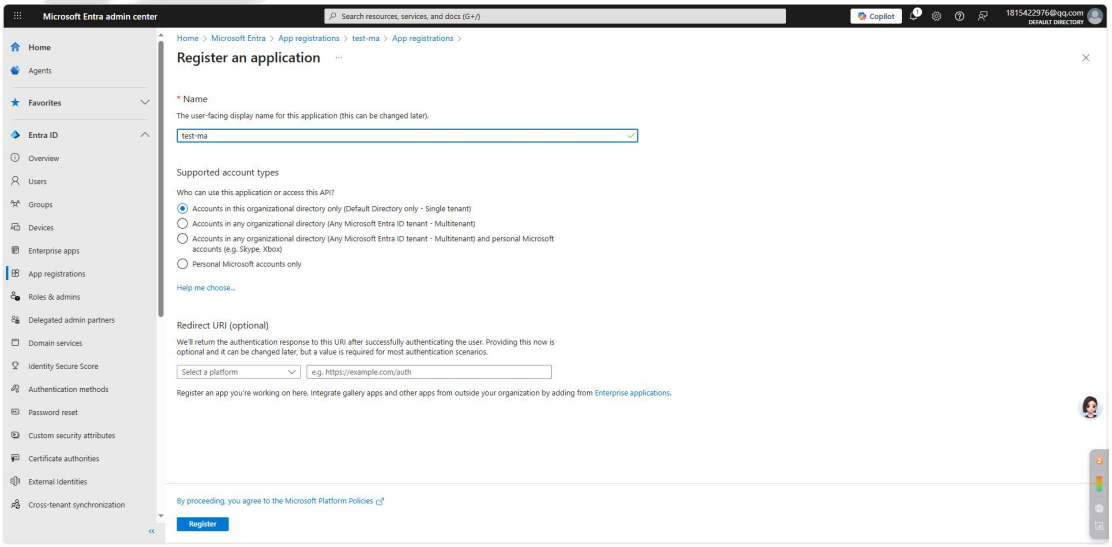


Figure 20- 102 App registrations

Step3: Enter Overview and click "Add a certificate or secret".

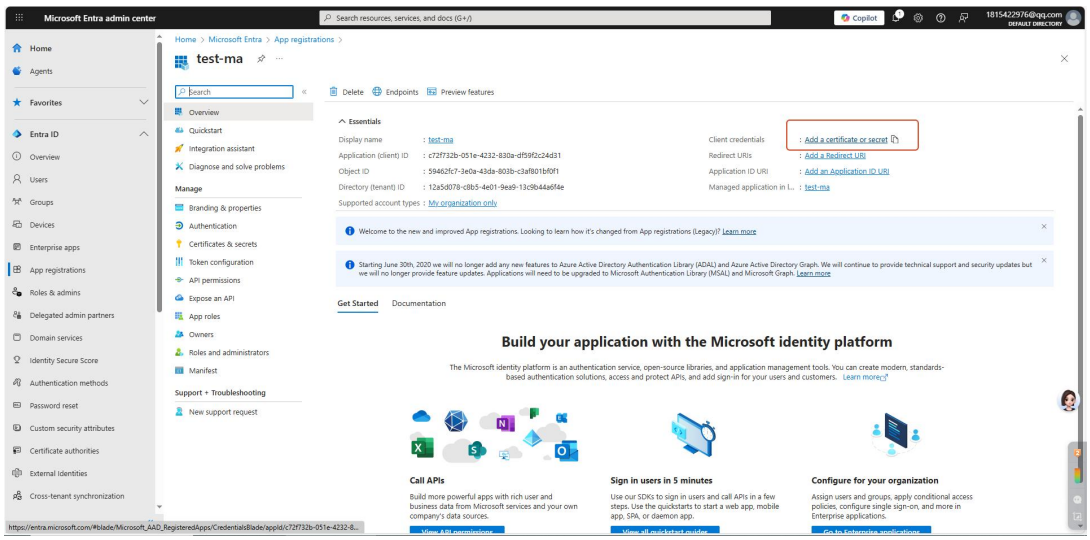


Figure 20- 103 Add a certificate or secret

Click "Certificates" - "Upload certificate", and upload the certificate file that has been added in ZKBio CVSecurity.

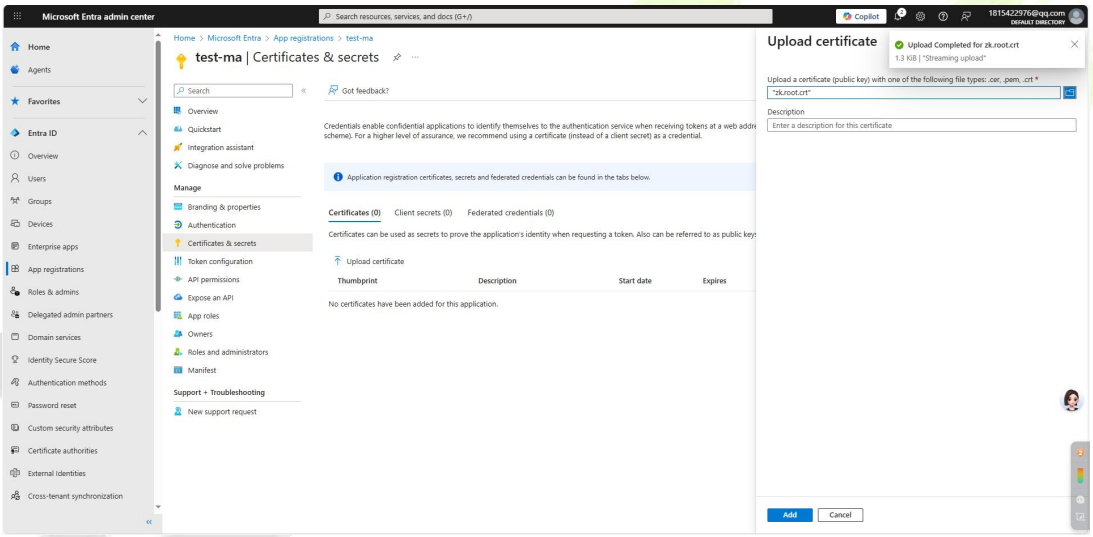


Figure 20- 104 Upload certificate

Step4: Enter Expose an API and click "Add" next to Application ID URI.

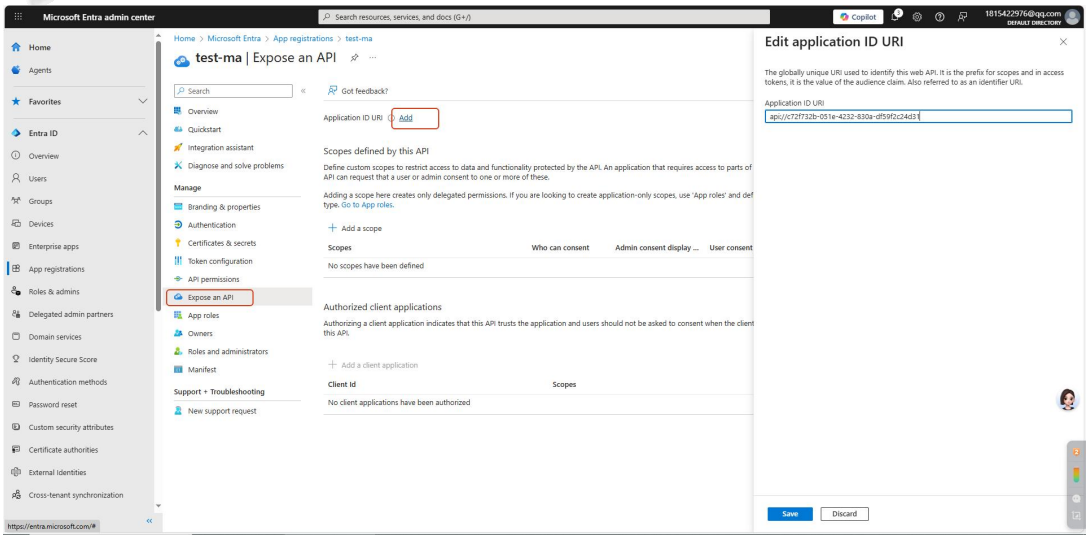


Figure 20- 105 Expose an API

Step5: Enter API permissions and click "Add a permission"→"Microsoft API"→"Microsoft Graph".

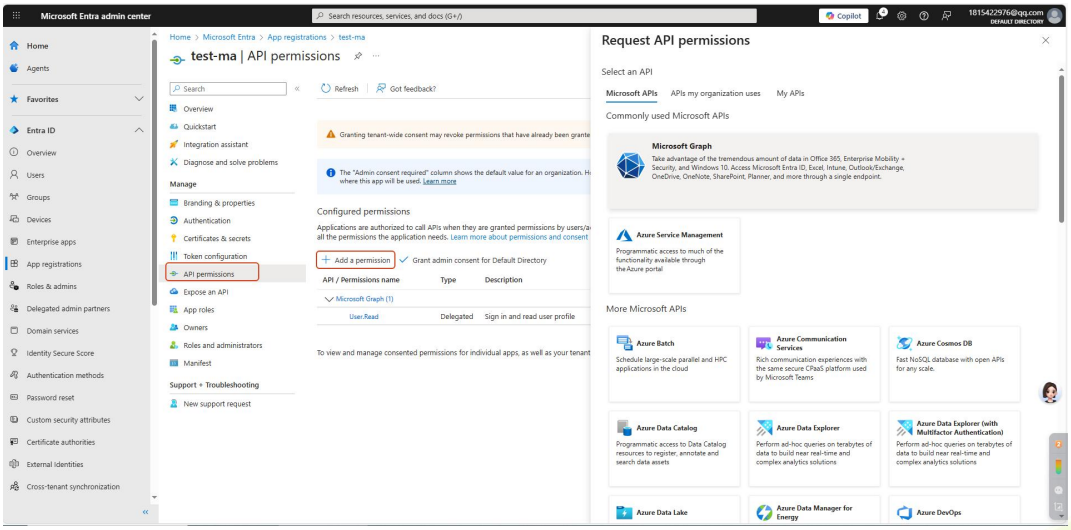


Figure 20- 106 Add a permission

Check the "Application.Read.All" and click "Add a permission".

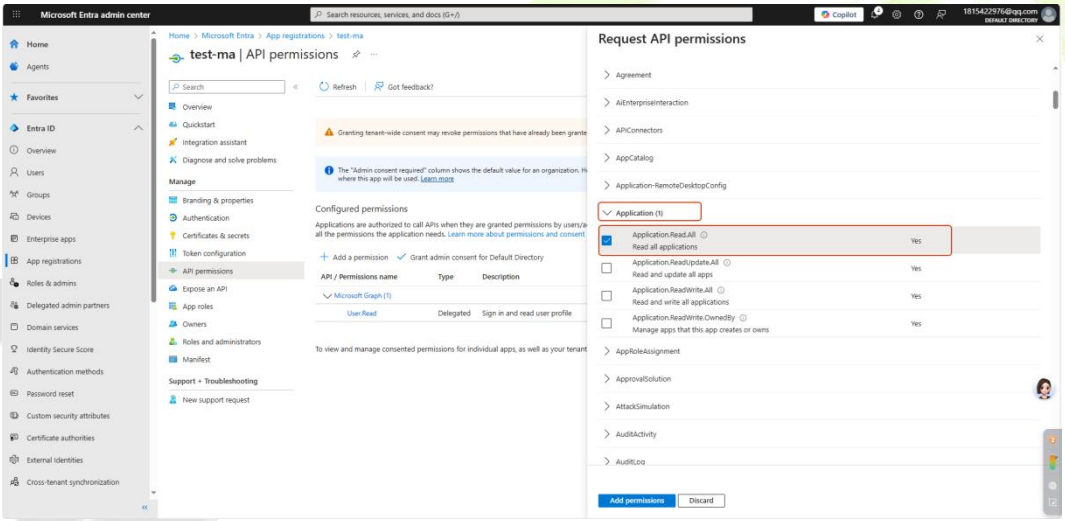


Figure 20- 107 Add a permission

Check the "Place.Read.All" and click "Add a permission".

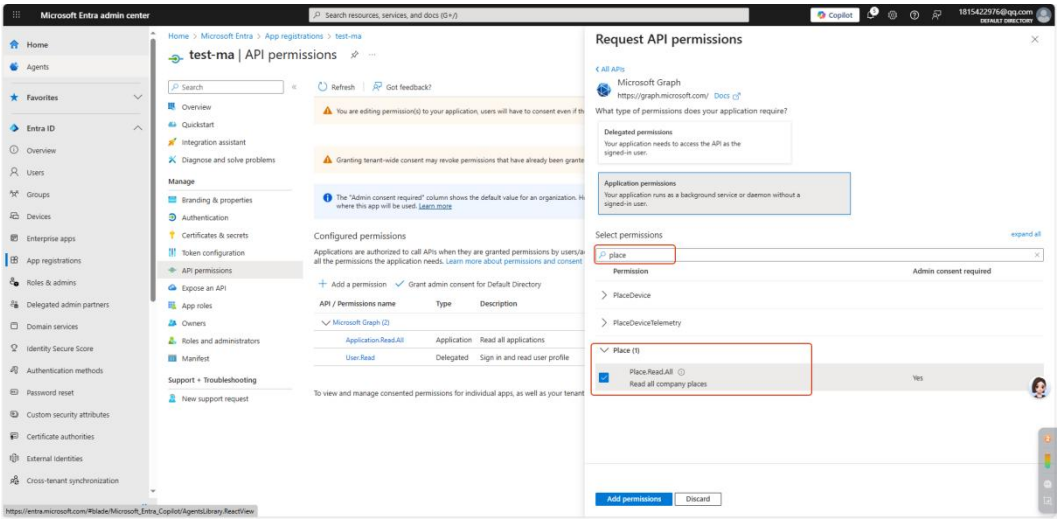


Figure 20- 108 Add a permission

Check the "Calendars.Read.","Calendars.ReadBasic.All"and"Calendars.ReadWrite".Then click "Add a permission".

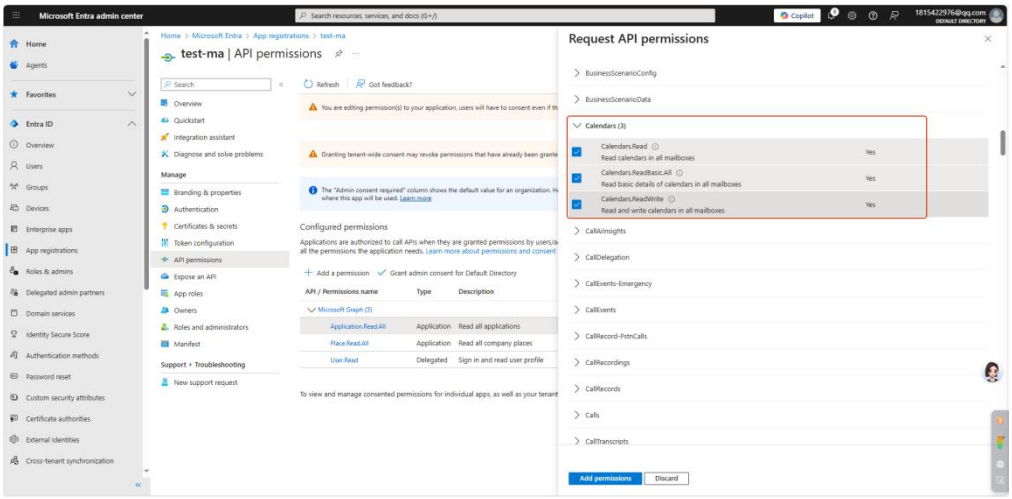
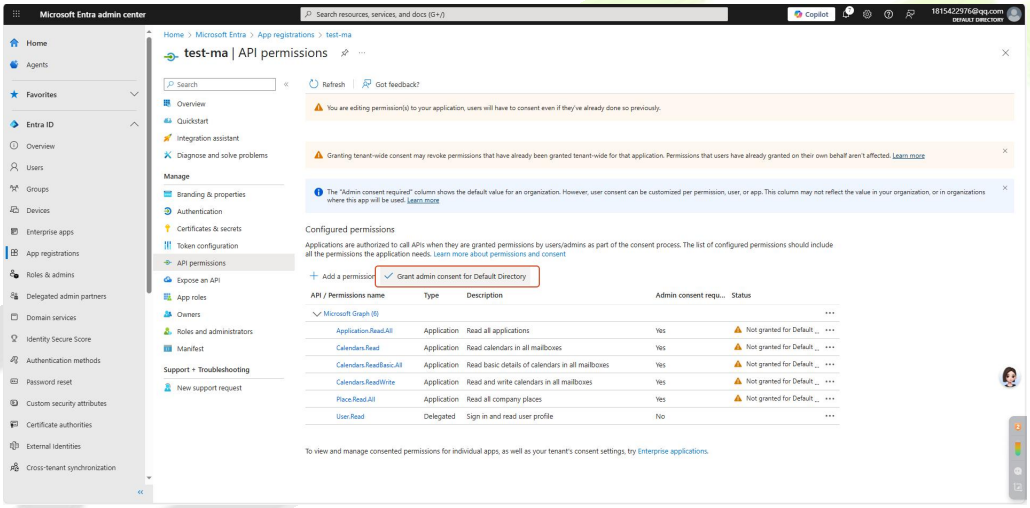


Figure 20- 109 Add a permission

Step6: Click "Grant admin consent on behalf of the organization"to authorize the permissions.



Step7: Copy the Application ID and Tenant ID, then navigate to System → Third Party Integration → Microsoft 365 → Connection Parameter Settings in ZKBio CVSecurity to fill them in.

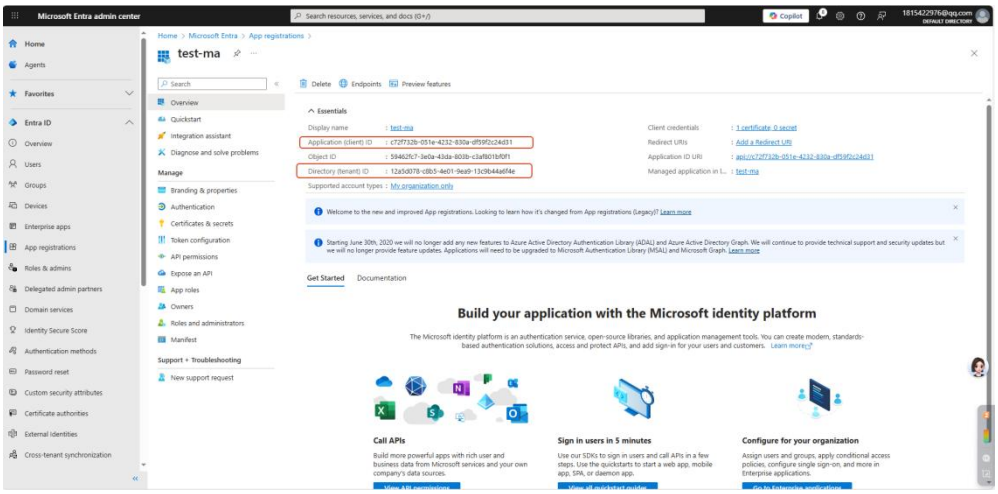


Figure 20- 110 Copy the Application ID and Tenant ID

Step8: Click "Test Connection".

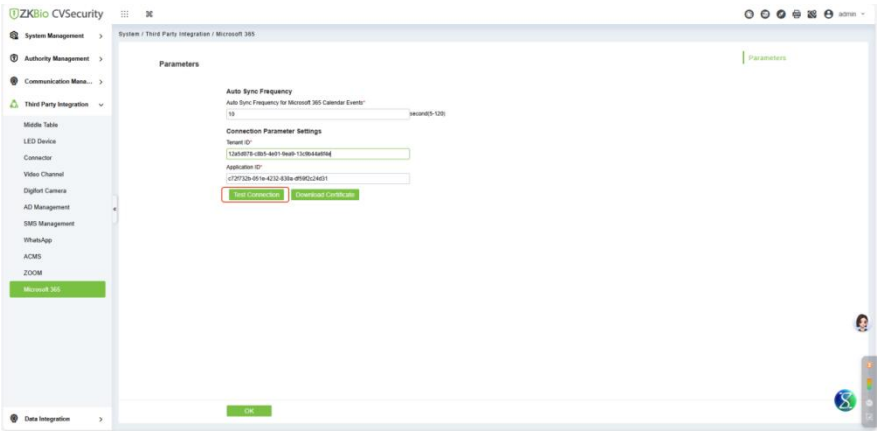


Figure 20- 111 Test Connection

20.4.8.2Add Meeting Room:

Step1: Enter the Microsoft 365 admin center platform, click Resources → Meeting Rooms & Equipment → Add Resource.

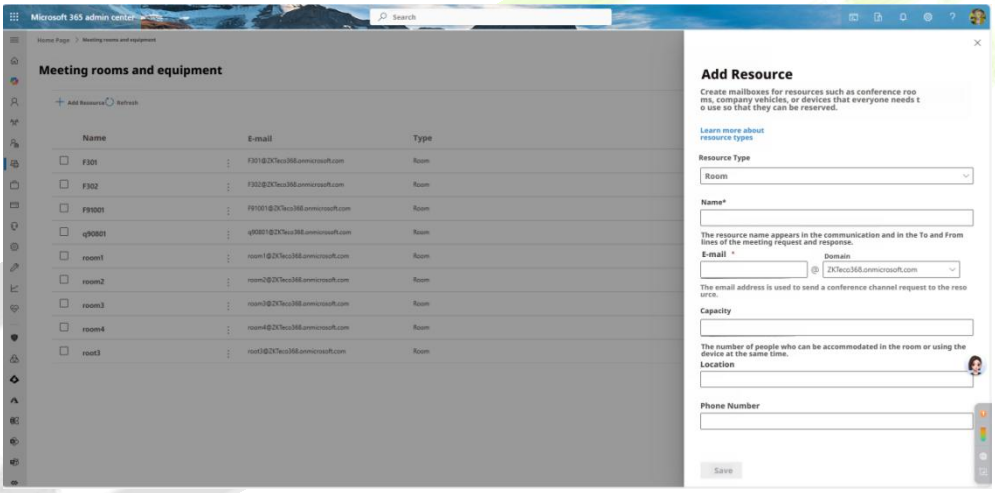


Figure 20- 112 Add Resource

Step2: Enter the ZKBio CVSecurity →Space Management → Space Management → Space.Click "New" to add a meeting room, you can select the corresponding meeting room resource from Microsoft 365.

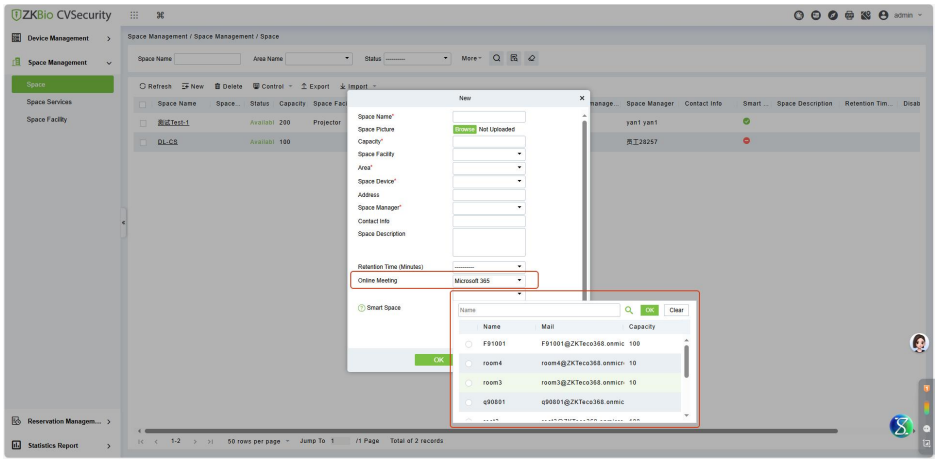


Figure 20- 113 Add Meeting Room

20.4.8.3Sync Microsoft 365 events:

Step1: Create a new event on the Outlook platform.Access the [Calendar] configuration page, select the required meeting schedule time range, expand the advanced configuration options, complete the schedule creation, and send it.

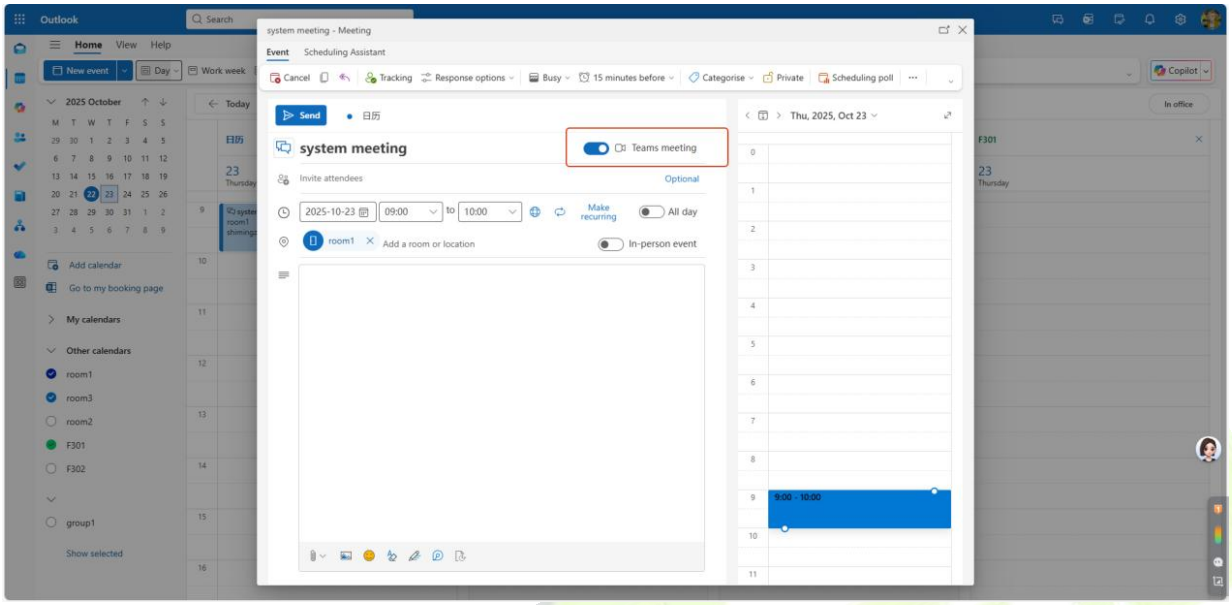


Figure 20- 114 Calendar

Meeting schedule status display.The calendar information on Teams is completely synchronized with that on Outlook. You only need to make a schedule reservation in either module, and the reservation information will be synchronized between the two.

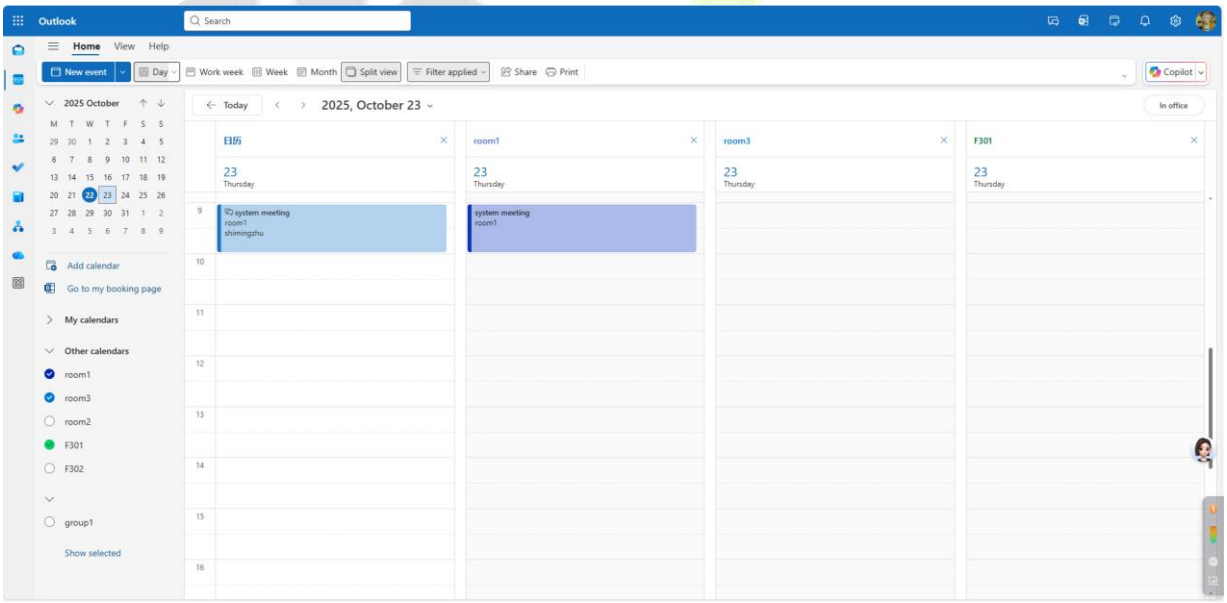


Figure 20- 115 Calendar

The meeting invitation email is as shown in the figure. When the meeting time arrives, participants working remotely can quickly join the meeting via the online link.

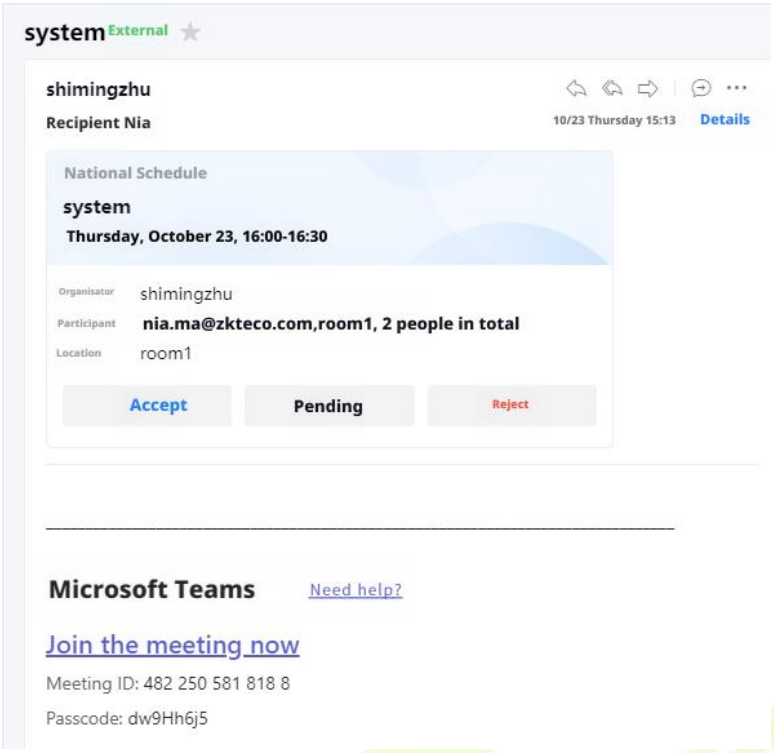


Figure 20- 116 Meeting Invitation Email

Step 2: Enter the ZKBio CVSecurity →Space Management → Reservation Management → Reservation Details.Click "Sync Microsoft 365 Events" → "OK" to complete the information synchronization.System / Third Party Integration / Microsoft 365

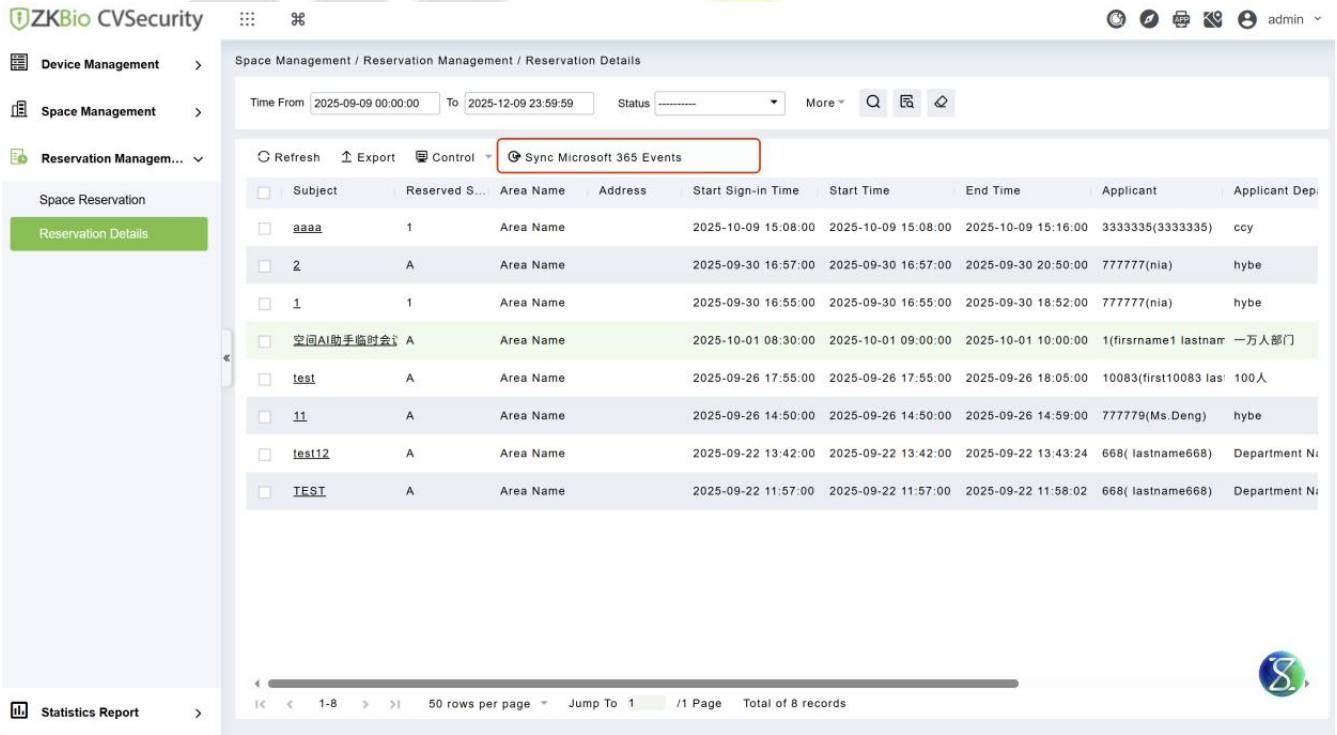


Figure 20- 117 Sync Microsoft 365 Events

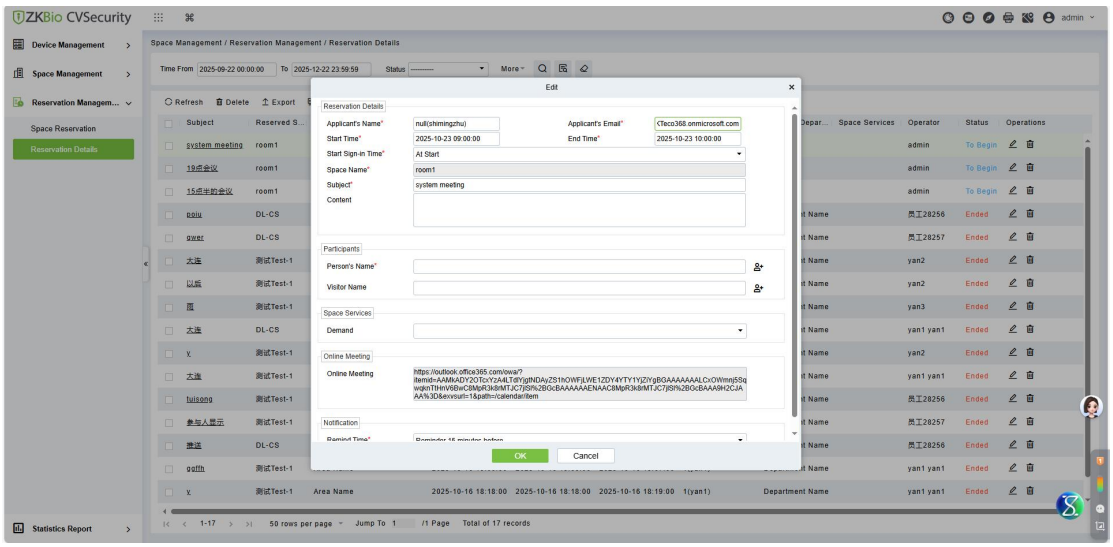


Figure 20- 118

Step 3: Enter the System → Third Party Integration → Microsoft 365.The Auto Sync Frequency can be modified in the parameter settings.The system automatically synchronizes Microsoft 365 calendar events at a frequency of 120 seconds. Within the range of 5 to 120 seconds, the frequency can be customized and modified.

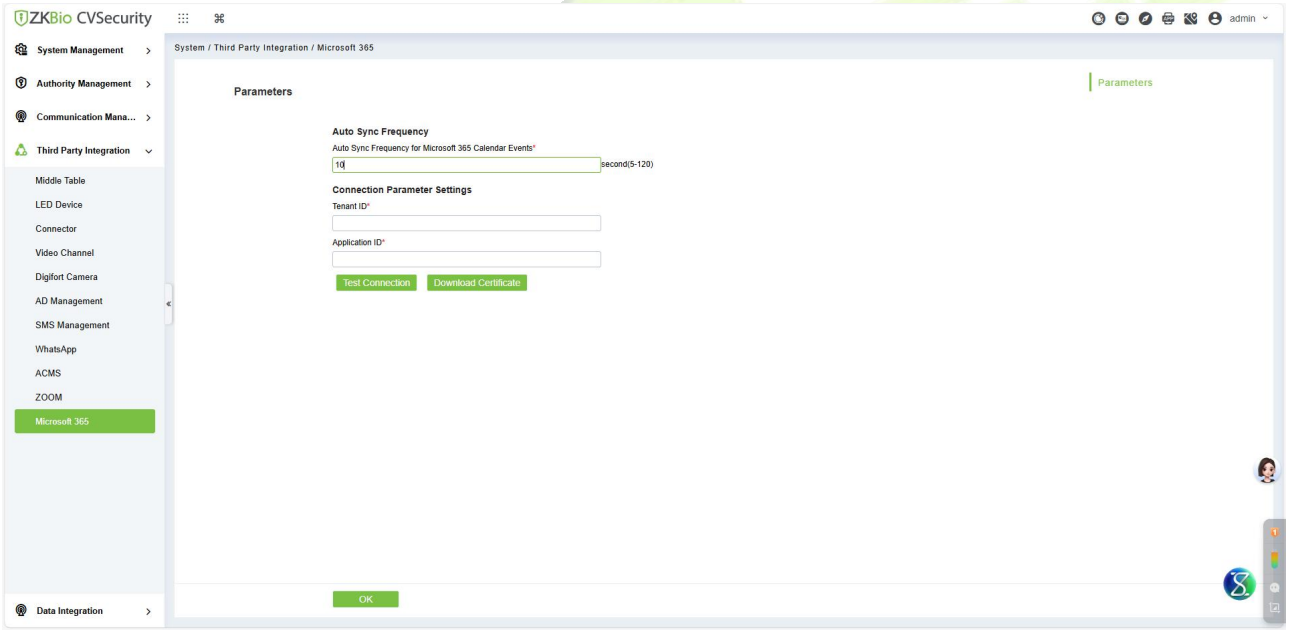


Figure 20- 119 Auto Sync Frequency

20.5 Data Integration

The "Data Integration" module enables the use of ZKBio CVSecurity as a data source to push data to third parties. It is also possible to use third-party data as the data source, and ZKBio CVSecurity can pull data from third parties. Among them, both push and pull have two integration methods: API integration and database integration. It is convenient to connect with the data of third parties.

20.5.1 Service Object （Step 1）

The service object is a named identifier for a service. A separate page is added for settings to facilitate setup operations on the service configuration page.

Click "New" to create a new service object.

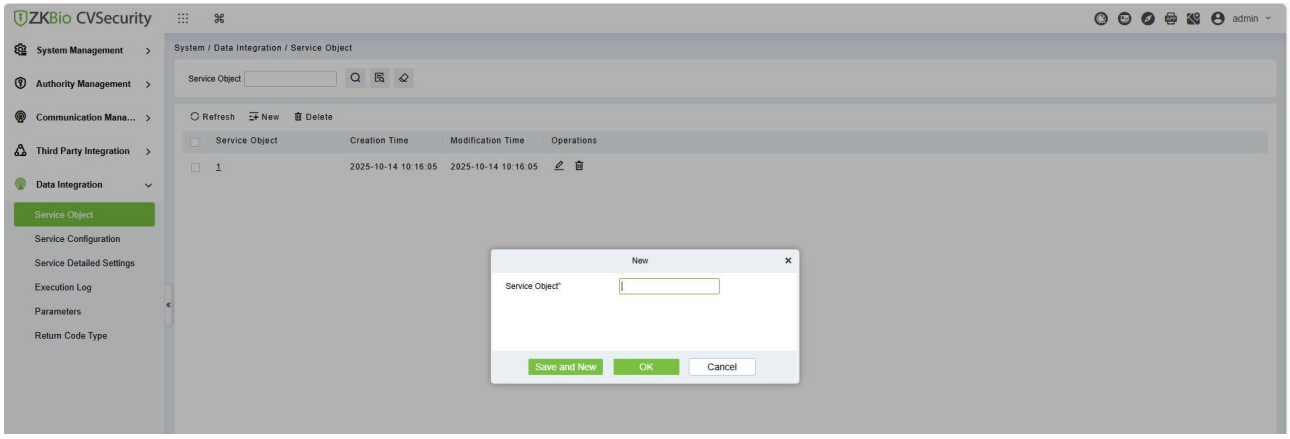


Figure 20- 120 Service Object

20.5.2Service Configuration（Step 2）

Different service types (including push and pull) can both be configured in the following two ways. When enabled, the operation of the corresponding service will be activated. Specific operations require detailed service settings in the next step. Among them, "push" means ZKBio CVSecurity acts as the data source to push data to a third party; "pull" means a third party acts as the data source, and data is pulled from the third party to ZKBio CVSecurity.

● Basic Configuration for API Integration Method

Configure the corresponding API address and authentication - related information.

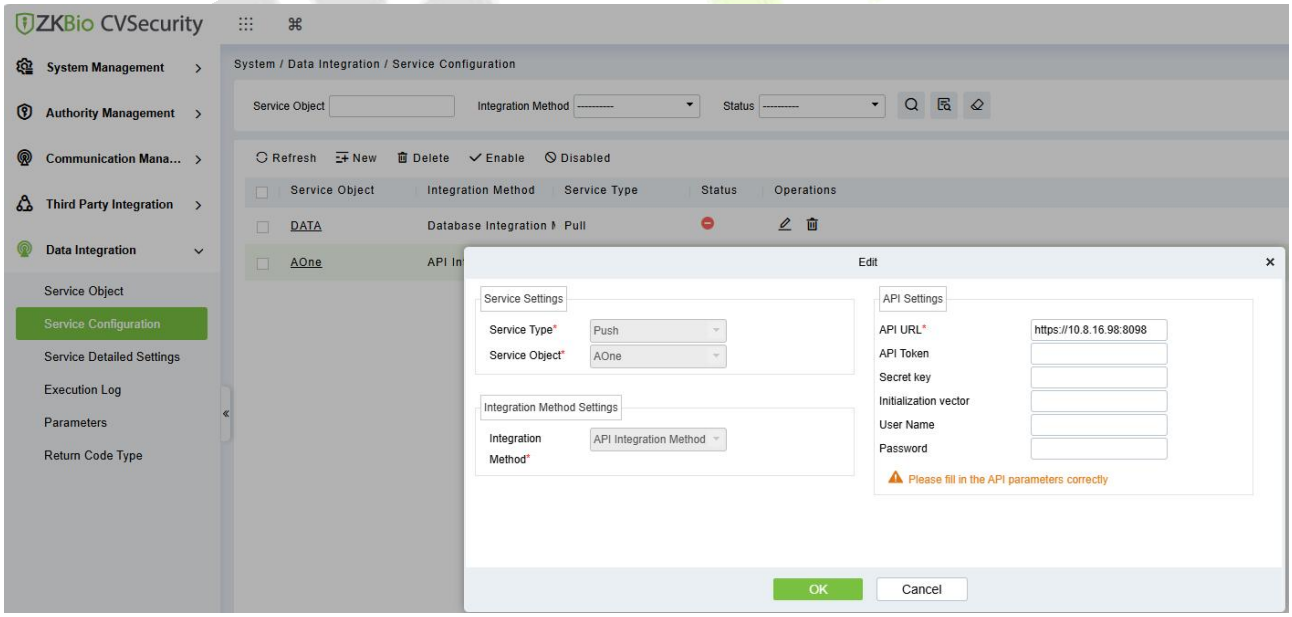


Figure 20- 121 Basic Configuration for API Integration Method

● Basic Configuration for Database Integration Method

Configure the database that needs to be connected. After configuration, please click Test Connection to check if the connection is successful.

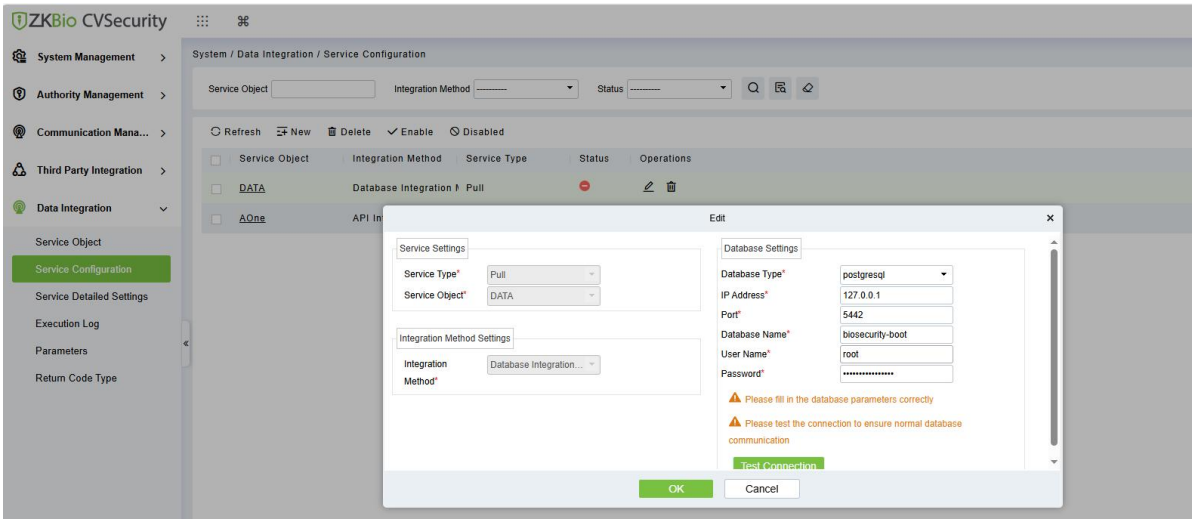


Figure 20- 122 Basic Configuration for Database Integration Method

20.5.3Service Detailed Settings（Step 3）

Configure the business objects for the configured integration method.

● Detailed Configuration for API Integration Method

Note: For the API integration method with the service type "Push", interface operations such as adding, editing, deleting, and retrieving are generally available. For the API integration method with the service type "Pull", generally only the retrieving interface operation is used.

Example: Taking ZKBio CVSecurity pushing "Department" data to AOne as an example, the figure below shows the Add Department API of AOne.

2.1.1 Add /Edit Department [department/add]

Post Request URL	https://serverIP:serverPort/api/department/add?access_token={apitoken}

Address: 1600 Union Hill Road Alpharetta Georgia 30005
Company website: armatura.us; Email: info@armatura.us

MATURA

Request Mode	POST

Request Content	{
	"code": "222",
	"name": "Department Name",
	"parentCode": "1"
	}

Request Parameter Description	code: Department Code, required; name: Department Name, required; parentCode: ParentDepartment Number;
Response Result	Refer to public response result, other can refer to Appendix-Error code
Response Result Description	public response parameter description

Figure 20- 123 Add Department API of AOne

Fill in the detailed service configuration information of ZKBio CVSecurity according to the relevant information of AOne's Add Department API.

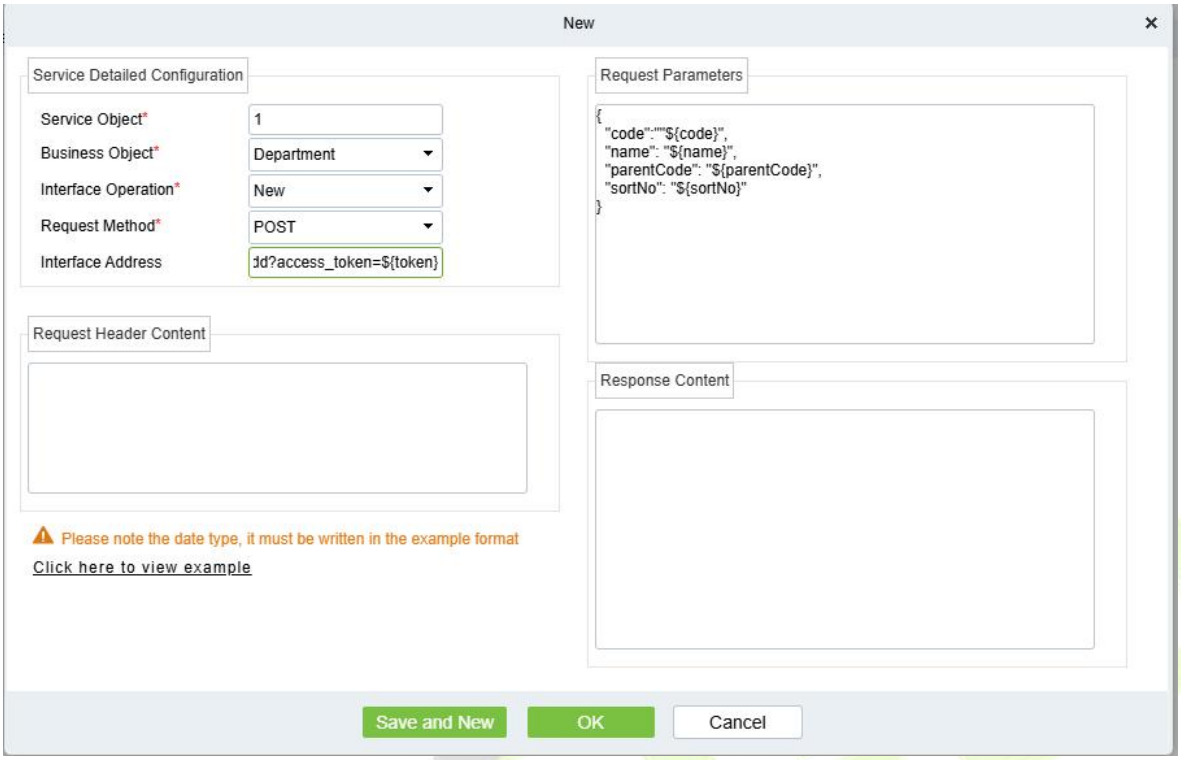


Figure 20- 124 Add Department API of AOne

Parameter	Description
Service Object*	Select the Service Object
Business Object*	It is obtained from the interface information of the integrated software. 
Interface Operation*	It is obtained from the interface information of the integrated software. 
Request Method*	It is obtained from the interface information of the integrated software. 
Interface Address	It is obtained from the interface information of the integrated software. **Note:** Replace {apitoken}in the URL with ${token}. 
Request Parameters	Write the Json data required for the API request content. Regarding the format of parameter values, take string and numeric types as examples: strings are expressed as "${field name}", while numeric values are expressed as ${field

Parameter	Description

	name} without double quotes.
	Request Content
	{
	"code": "222",
	"name": "Department Name",
	"parentCode": "1"
	}

Table 20- 8 Parameter

Note: For the specific parameter types in the request parameters, including the writing method of date formats, please refer to the examples.Or refer to Appendix Table 1 and the variable usage method.

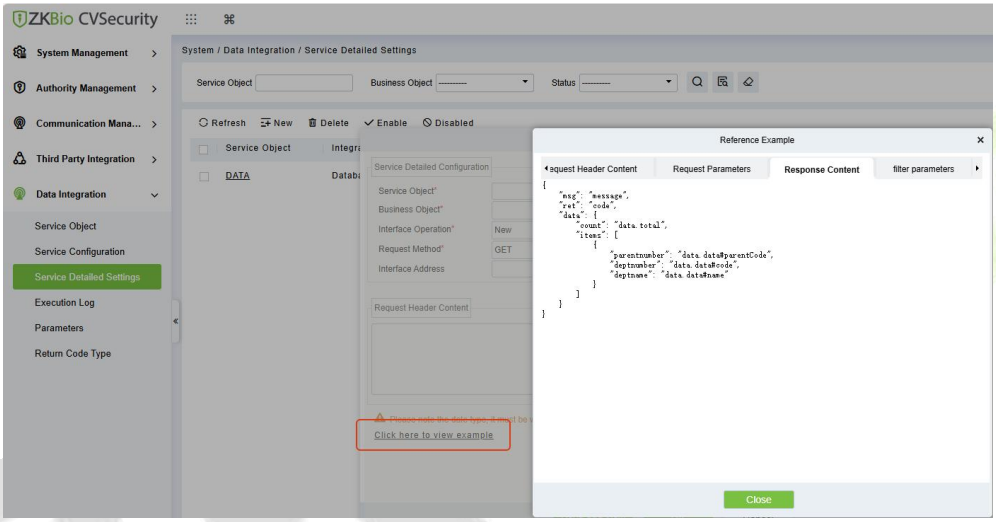


Figure 20- 125

● Detailed Configuration for Database Integration Method

Example: Departments are obtained from third parties through the database integration method.

The SQL statement for retrieving third-party department data.

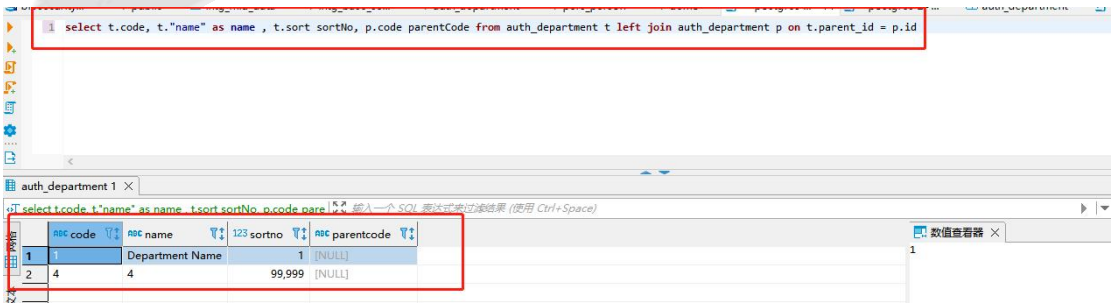


Figure 20- 126

Write the SQL statements with corresponding functions in the database tool, then replace them according to the global variables built in the appendix under the sections for update, delete, insert, and select. Note that you cannot save the statements if you directly use the above keywords. For fields of other related business objects, refer to Table 1 in the appendix for replacement.

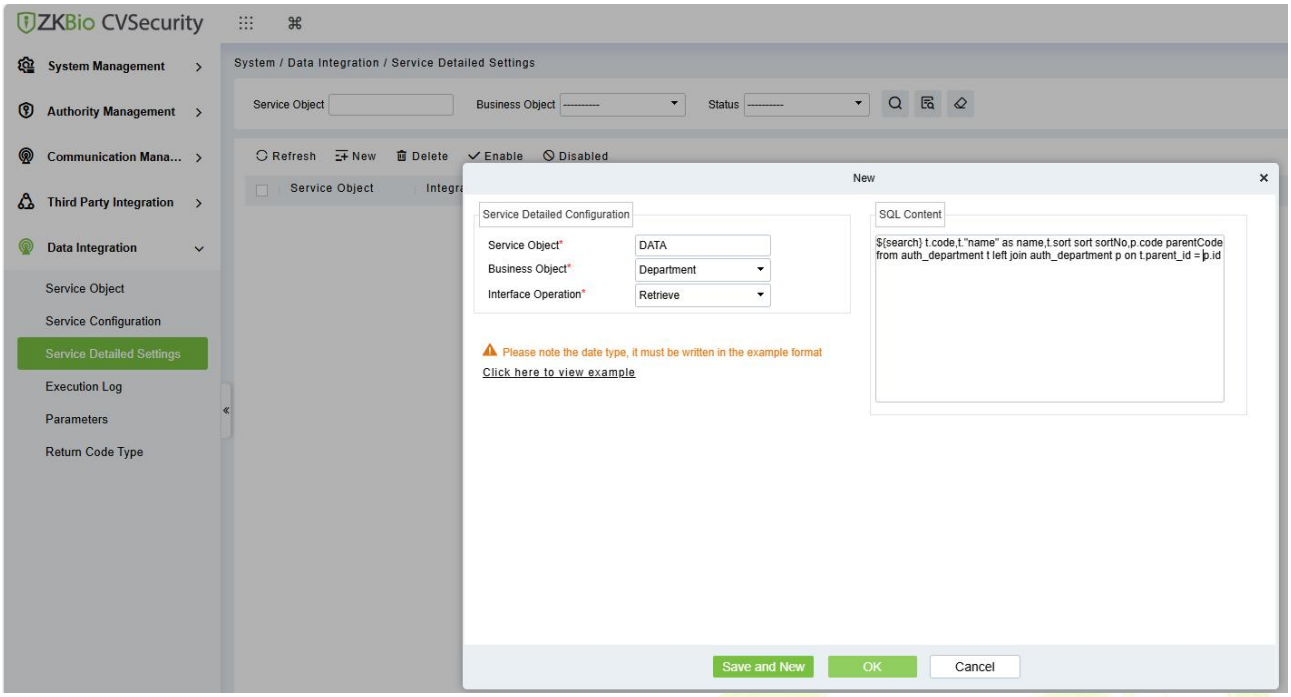


Figure 20- 127

●The data filtering function in access control data push and attendance record push.

When the business object is selected as Transaction or Attendance Record, a "Filter Parameters" input box will appear. The function of this input box is: only the data that meets the conditions in the input box will be pushed.

The rules for filling in filter parameters are as follows (you can check the example):

1. Filter parameters can only consist of parameter names, parameters, In, NotIn, (,), AND, and OR.

2. Parameters are separated by commas, and no spaces are allowed between parameters.

Example: (pinNotIn(1,2,3) AND devSnIn(aa,bb)) OR devSnIn(cc,dd).This parameter means that only data with device SN numbers "cc" or "dd", or data with SN numbers "aa" or "bb" but pin numbers not equal to "1", "2", or "3" will be pushed.

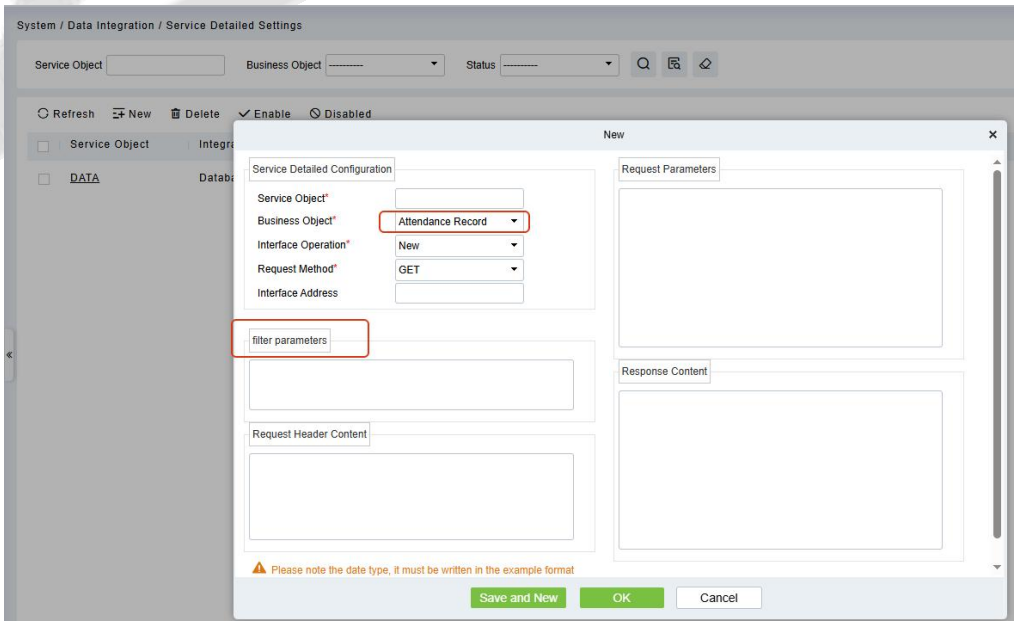


Figure 20- 128

20.5.4Return Code Type （Step 4）

Currently, only cases with the level "Abnormal" are processed: When the return code level returned by an interface call is "Abnormal", the data of this interface call will be continuously processed until one of the following two situations occurs—it will stop either when the return code level of the interface call data is no longer "Abnormal", or when the abnormal-level return code associated with this data is modified to another level to skip processing.

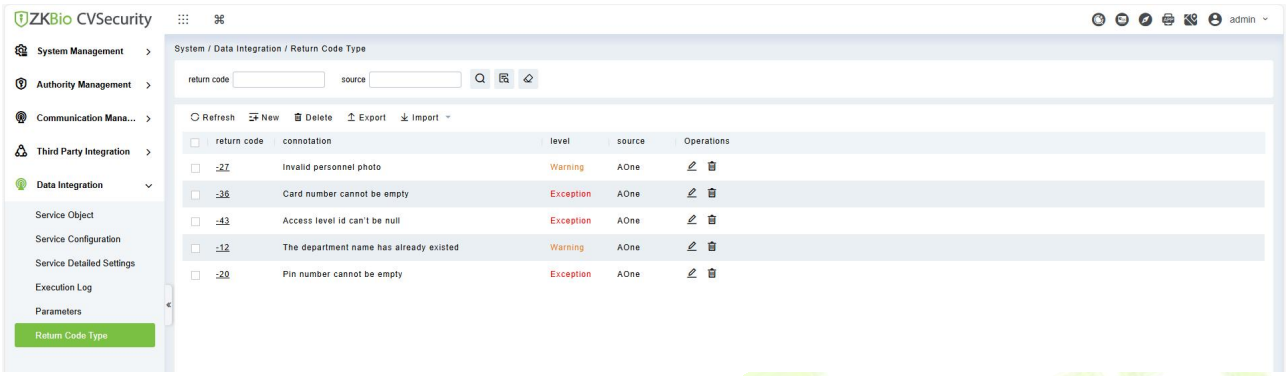


Figure 20- 129 Return Code Type

Click "New" to add a return code. A return code is a description of the call status returned by an API interface call.The source must correspond to the set service object name.

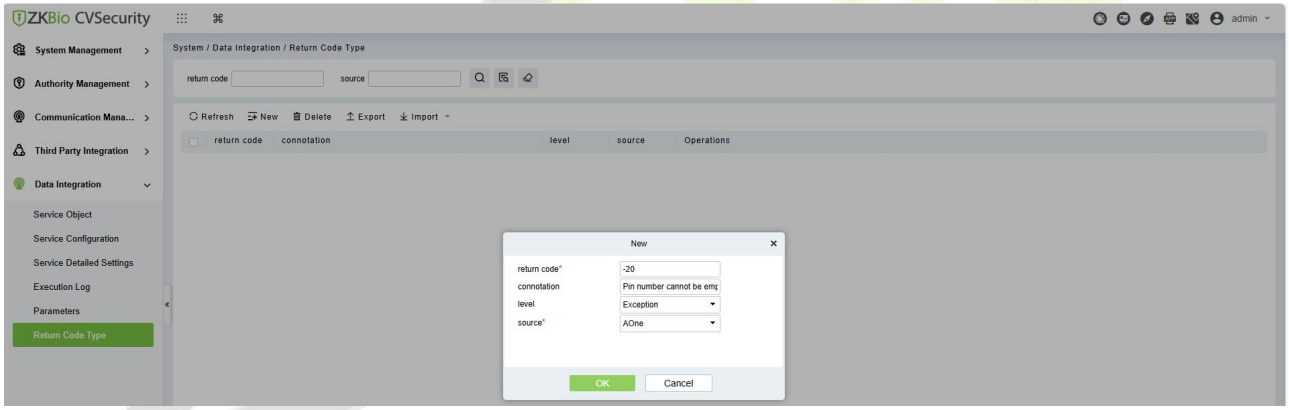


Figure 20- 130

20.5.5Perform data pushing and pulling

●To perform data pushing

you must first complete at least one operation (addition, editing, or deletion) on a business object. Then, enable the service configuration and service detailed settings. After that, any operations performed on the relevant business objects in the configured software will be pushed to the third party.

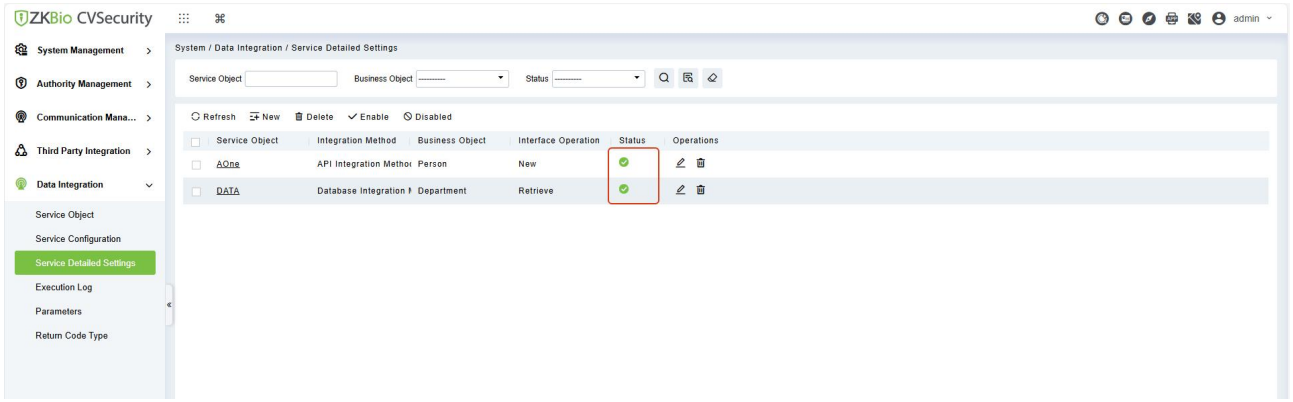


Figure 20- 131

The following example demonstrates data pushing through the API integration method. (If using the database integration method, it is also required to complete the corresponding interface operations for one business object.)

Example: When a department is added in ZKBio CVSecurity, it is pushed to AOne. The push is successful, and the receiver can see the data displayed on the page.

The pushing party:

Figure 20- 132

The receiving party:

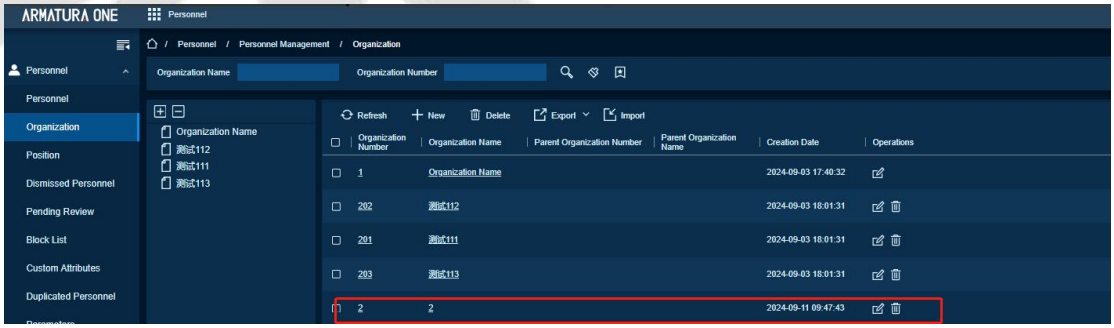


Figure 20- 133

●To perform data pulling

You need to first complete the retrieval of a business object, then enable the configurations in both the detailed service settings and service configuration. In the configured software, it will continuously poll and fully pull the relevant business objects for processing.

Example: When a department is added in ZKBio CVSecurity, it is pulled to another instance of ZKBio CVSecurity. The pull is successful, and the pulled party can see the data displayed on the page.

The pulled party:

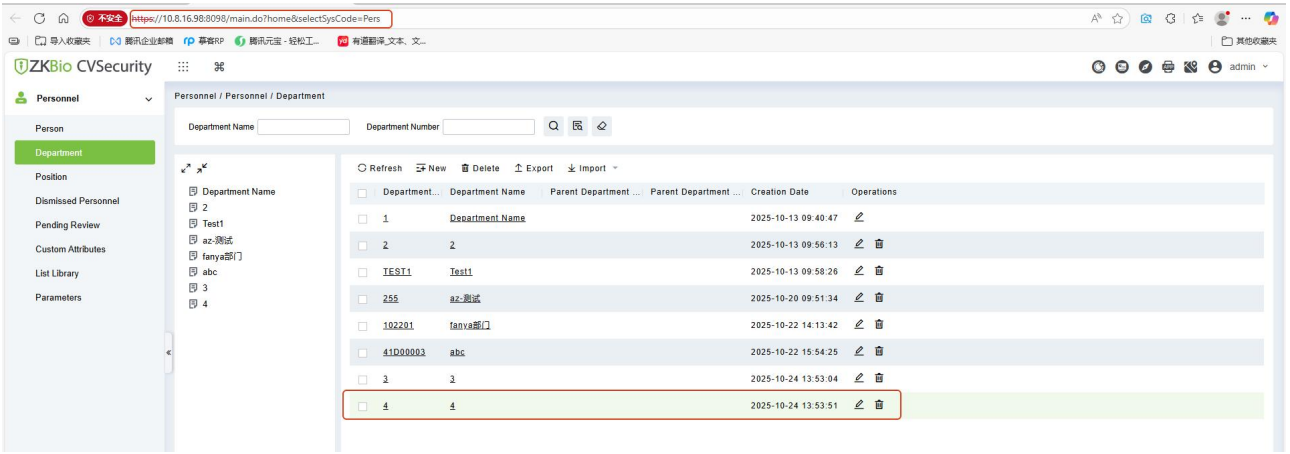


Figure 20- 134

The pulling party:

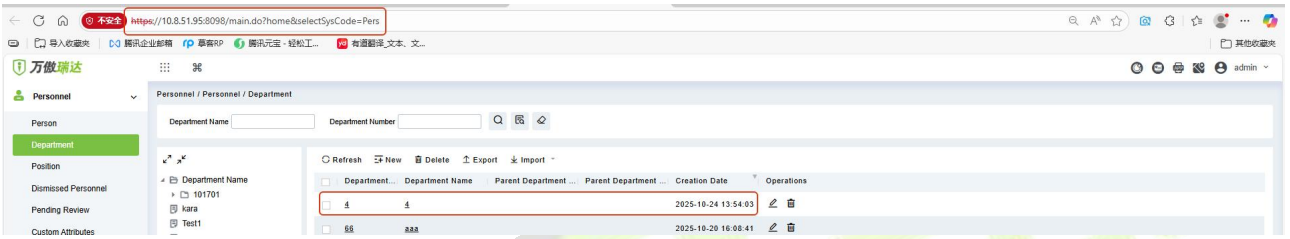


Figure 20- 135

20.5.6Execution Log

You can view the specific execution details by accessing the Execution Log page, as shown in the figure below.

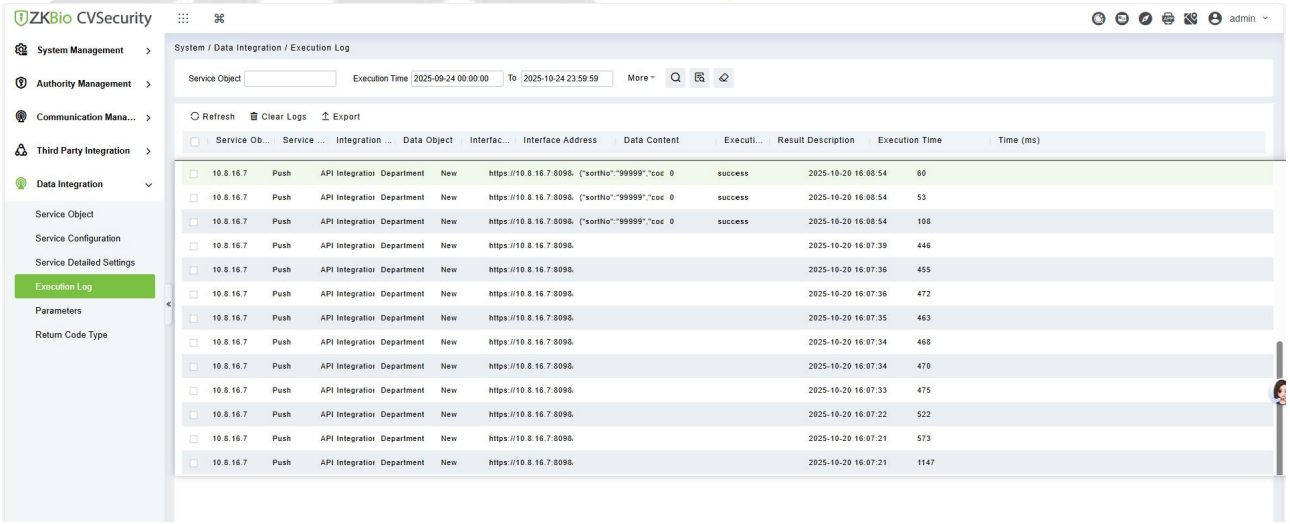


Figure 20- 136

20.5.7Parameters

Relevant content for data cleaning can be configured in the parameter settings, including the data retention period for intermediate tables, the retention period for service execution logs, and the execution time. Additionally, the time intervals for data pushing and data pulling can be configured.

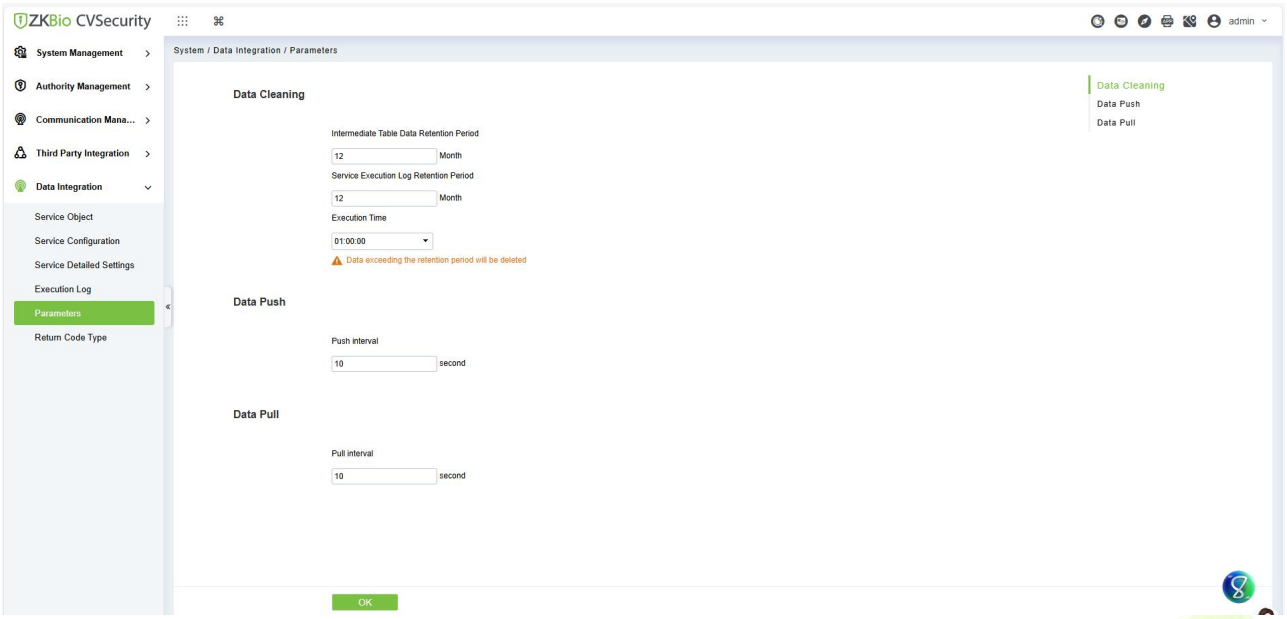


Figure 20- 137 Parameter

20.5.8 Appendix

Basic Usage of Freemarker Syntax in the Integration Module:

20.5.8.1 variable usage

```
// Usage of date type
"date":"${date!""}",
//Usage of string type
"accLevelIds": "${accLevelIds!""}",
// Usage of boolean type
"isSendMail": ${isSendMail},
// Usage of numeric type
"no": ${no}
```

Note: When writing SQL for database operations, use single quotes to denote string types.

20.5.8.2 Different business objects can obtain the fields within the corresponding business objects.

Business Object	Interface Operation	Field
Department	New,Edit	code
		name
		parentCode

		sortNo
	Delete	code
Person	New,Edit	pin
		name
		lastName
		gender
		deptCode
		cardNo
		positionCode
		birthday
		carPlate
		photoPath
		personPhoto
		certNumber
		certType
		email
		hireDate
		isDisabled
		isSendMail
		mobilePhone
		phoneCountryCode
		personPwd
		ssn

		supplyCards
		accLevelIds
		accStartTime
		accEndTime
	Delete	pin
Position	New,Edit	code
		name
		parentCode
	Delete	code
Area	New,Edit	code
		name
		parentAreaCode
		parentAreaName
	Delete	code
Access Level	New,Edit	accLevelId
		accLevelName
		authAreaCode
	Delete	accLevelId
Card	New,Edit	cardNo
		personPin
		cardType
		cardState
	Delete	cardNo

		personPin
Face Picture	New,Edit	pin
		photoPath
		personPhoto
	Delete	pin
		bioType
Biometric Template(Currently, only fingerprint is supported)	New,Edit	personPin
		version
		template
		templateNo
		templateNoIndex
		duress
	Delete	personPin
		version
		templateNo
		templateNoIndex
Transaction	New	eventTime
		areaName
		devAlias
		devId
		devSn
		eventPointName
		eventName

		deptName
		levelAndEventPriority
		pin
		name
		lastName
		cardNo
		deptCode
		readerName
		verifyMode
Attendance Record	New	personPin
		personName
		personLastName
		detpId
		deptCode
		deptName
		areaName
		deviceId
		deviceSn
		attDateTime
		attState
		attPointName

Table 1

Explanation: Under the business object "Department", using "${code}" allows you to obtain the value of "code" in ZKBio CVSecurity.

20.5.8.3 Built-in Global Variable

${add} represents insert

${modify} represents update

${del} represents delete

${search} represents select

20.5.8.4 Built-in Global Method

md5 Perform MD5 encryption

Example: ${md5(timestamp)} where the value of timestamp is "123456"

base64 convert to base64 format

formatDate convert the date-formatted string to a specified format

Example: "${formatDate(hireDate,"yyyy-MM-dd","dd-MM-yyyy")}"

where the value of hireDate is "2024-9-14"

20.5.8.5 Built-in Local Variable

The timestamp at that time, in string type (for API push)

timestamp

A random integer less than 1,000,000 (for API push)

nonce

The time at that moment, of Date type (for API push and database push)

curDate

Page number, default value is 1 (for database pull)

pageNo

Page size, with a default value of 800 (for database pull)

pageSize

21 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.

21.1 Device Center

21.1.1 Device

Devices added to the access control and video module, as well as subscribed devices added to modules such as intrusion alarm and video intercom, will be displayed on the screen. Basic device information, including online/offline status, will be shown, as illustrated in the figure below.

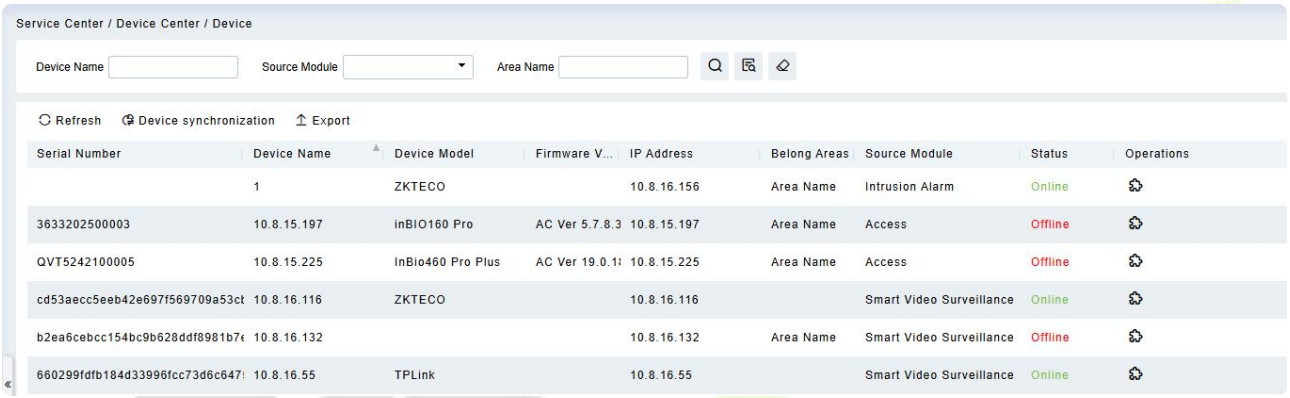


Figure 21- 1 Device Display Page

● 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.

21.2 Event Center

Through the definition of the event level and type, it makes the level prompt for the record generated under real-time monitoring.

21.2.1 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

● Operation Step:

Step 1: In 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.

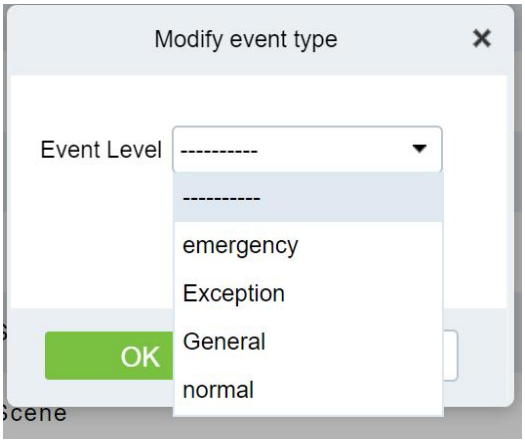


Figure 21- 2 Modify Event Level Page

Step 3: After selecting the desired level, Click **OK** to complete changing the event type level.

21.2.2Event Record

This screen records all events generated on the platform, as shown in figure below

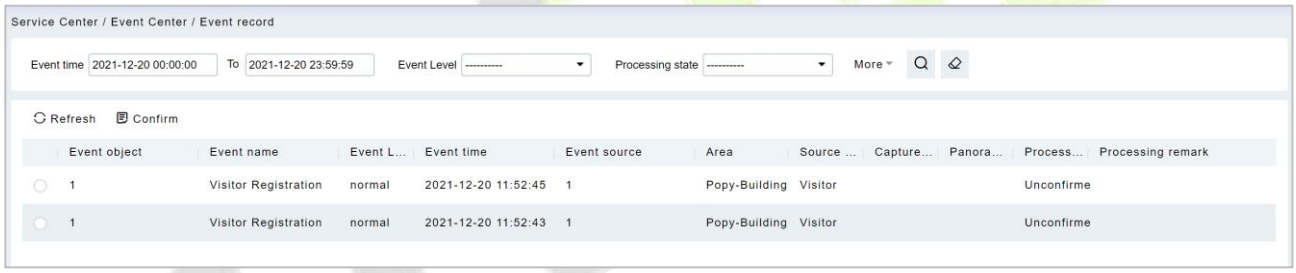


Figure 21- 3 Event Recording Page

21.2.3Event Level

This screen displays event levels and allows you to edit the color for each level.

Figure 21- 4 Event Level Page

21.2.4Parameters

This screen allows for parameter configuration, enabling you to choose whether events require confirmation.

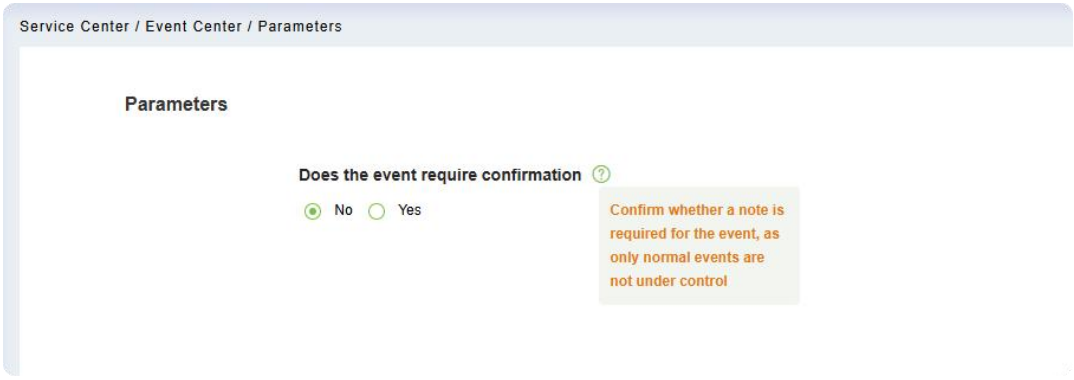


Figure 21- 5 Parameters Page

21.3 Linkage Center

You can configure the linkage settings for each module here and view detailed linkage records.

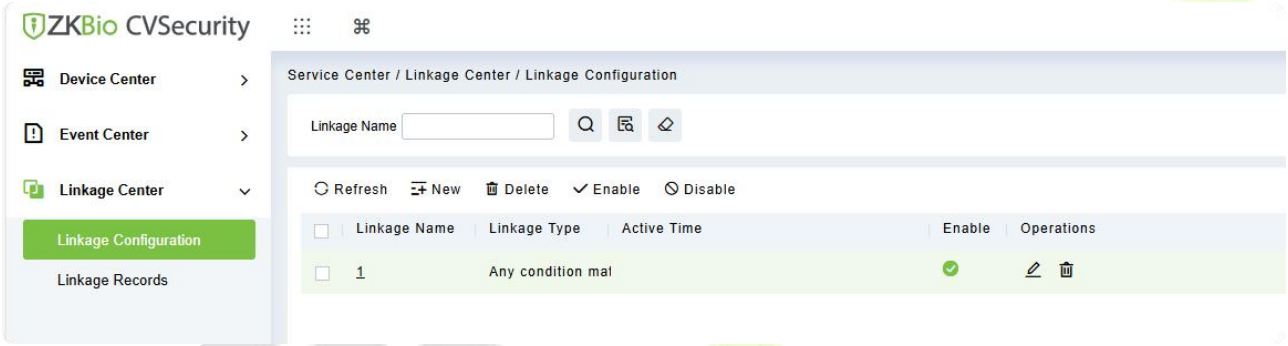


Figure 21- 6 Linkage Center Page

21.3.1 Linkage Configuration

21.3.1.1 Refresh

Click **Refresh** at the upper part of the list to load new linkage.

21.3.1.2 New

● Operation Step

Step 1: Click **New** to enter the configuration interface.

Step 2: Set the **linkage name**, **active time**, and **linkage type**. After selecting a module, you can proceed to choose linkage trigger conditions and input points.

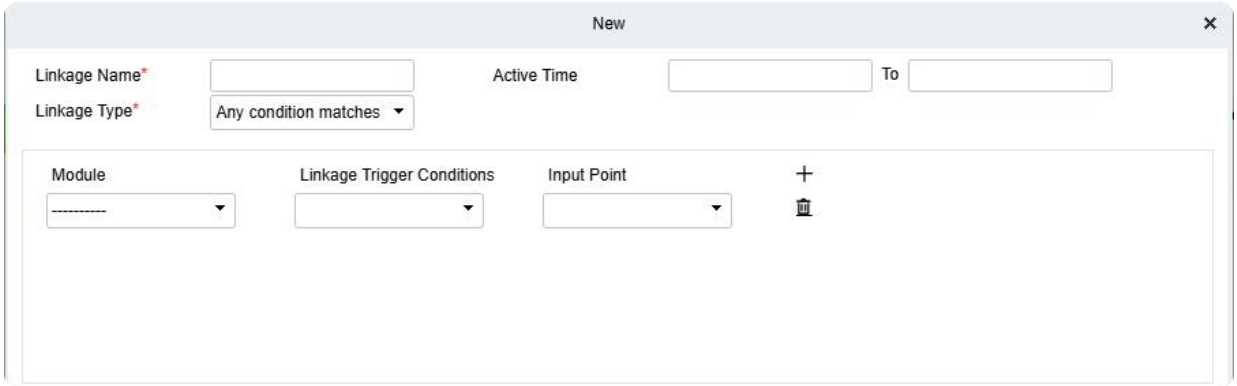


Figure 21- 7 New Page

Note:

● There are two types of linkage:

Any condition matches:The configured multiple linkage trigger conditions only require one of them to be met to activate the linkage.

All conditions match:The configured multiple linkage trigger conditions require all of them to be met to activate the linkage.

● There are 7 major modules in total:

Including **Access**,**Entrance Control**,**Smart Video Surveillance**,**Space Management**,**Energy Saving System** and **Intrusion Alarm**. For each module, you can select the corresponding linkage trigger conditions and choose specific added devices as input points. You can add multiple modules and input points by clicking the icon , and delete them using the icon .

Step 3: Finally select multiple linkage outputs.After adding them, you can configure specific settings for each label. Click "**OK**" to complete the linkage configuration once finished.

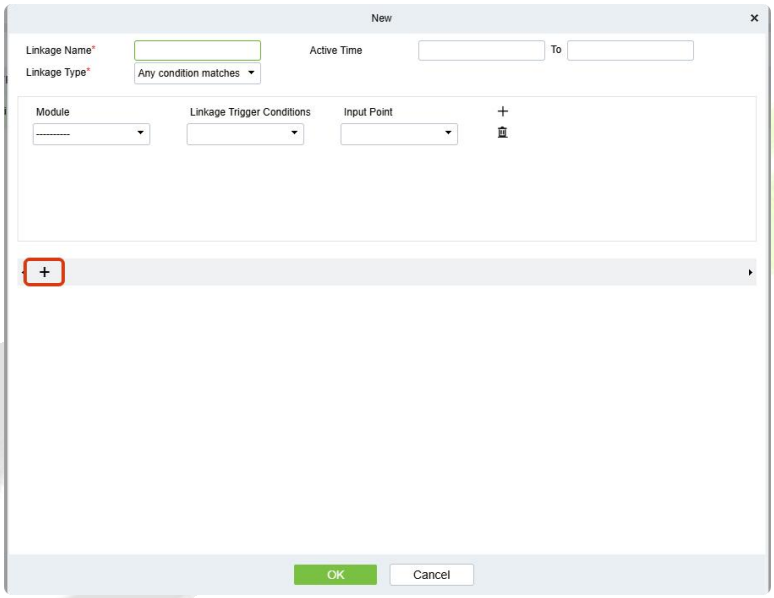


Figure 21- 8 New Page

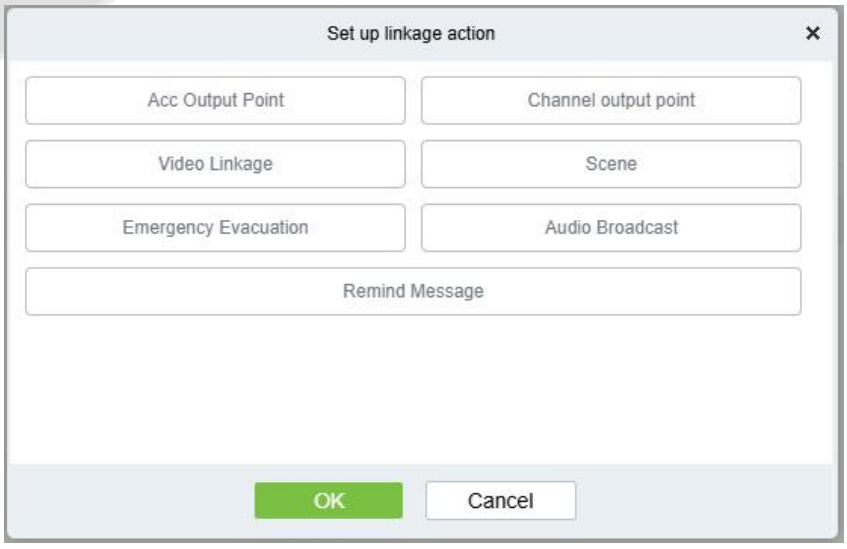


Figure 21- 9 Add Tabs Page

Note:

● There are 7 major modules in total:

Including **Acc Output Point**, **Channel Output Point**, **Video Linkage**, **Scene**,**Emergency Evacuation**, **Audio Broadcast** and **Remind Message**. For message notifications in output actions, you can choose from **Email, SMS, or WhatsApp**.

21.3.1.3Delete

After selecting the items you wish to delete,Click **Delete** > **OK** to delete.

21.3.1.4Enable

After selecting the items you wish to enable,Click **Enable** > **OK** to enable.

21.3.1.5Disable

After selecting the items you wish to disable,Click **Disable** > **OK** to disable.

21.3.2Linkage Records

This interface allows you to view detailed linkage records, including the time, linkage name, linkage type, device name, event point, captured photos or video playback, and linkage trigger conditions.

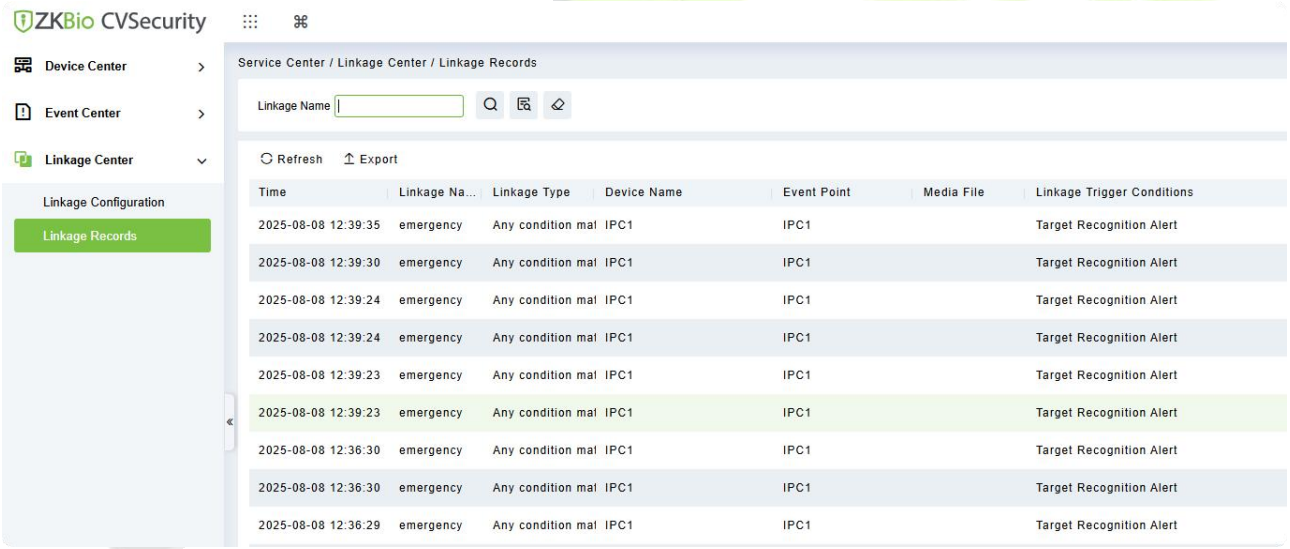


Figure 21- 10 Linkage Records Page

21.3.2.1Refresh

Click **Refresh** at the upper part of the list to update the linkage records.

21.3.2.2Export

Click **Export** at the upper part of the list and configure the relevant parameters to update the linkage records.

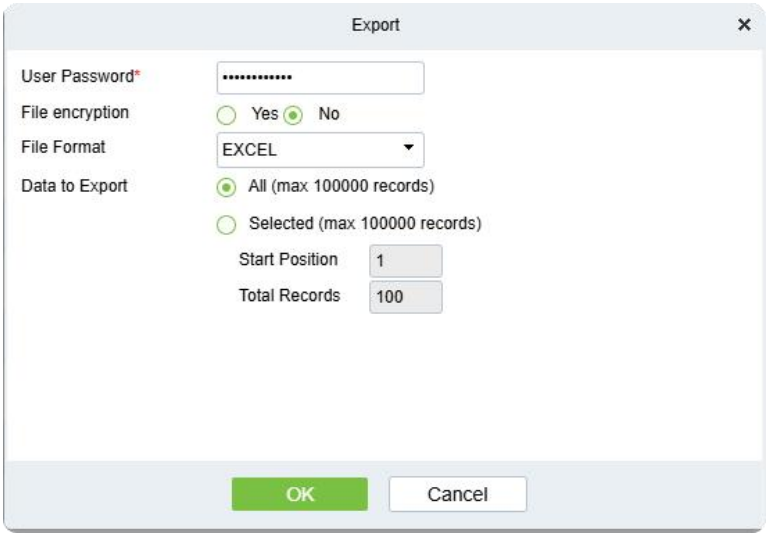


Figure 21- 11 Event Recording Page

Linkage Records

Time	Linkage Name	Linkage Type	Device Name	Event Point	Linkage Trigger Conditions
2025-08-08 12:39:35	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert
2025-08-08 12:39:30	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert
2025-08-08 12:39:24	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert
2025-08-08 12:39:24	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert
2025-08-08 12:39:23	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert
2025-08-08 12:39:23	emergency	Any condition matches	IPC1	IPC1	Target Recognition Alert

Figure 21- 12 Event Recording Page

21.4 Notification Center

● Notification Record

This interface records the notification reminding events generated by the attendance and visitor module.

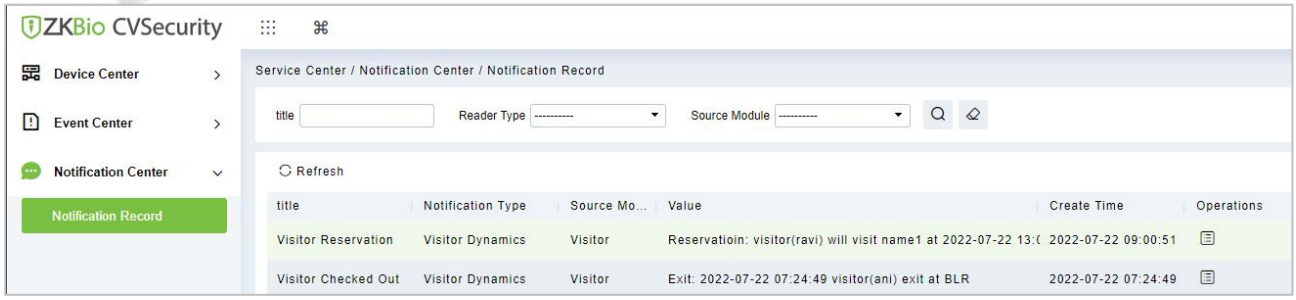


Figure 21- 13 Notification Record Page

21.5 Map Center

You can import a map to set monitoring points. When an alarm occurs, you can immediately view the location of the alarm source and surrounding conditions, select an appropriate monitoring point, and view live videos, playback, and personnel movements.

21.5.1 Real-Time Monitoring

Alarms generated in the access control and video modules are displayed on the real-time monitoring interface. You can query access control and video events by category. When an alarm is generated, you can view the location of the alarm source and surrounding conditions, select a suitable monitoring point, and view the live video, playback, and personnel movement. Operation that can handle doors in batches.

21.5.1.1 Personnel Movement

This part introduces the configuration Step for real-time monitoring of personnel movement in the service center module.

● Operation Step

Step 1: In the Service Center module, choose "Map Center > Real-time Monitoring".

Step 2: On the real-time monitoring screen, click the icon on the right in the personnel Trend window that is displayed, set related parameters.

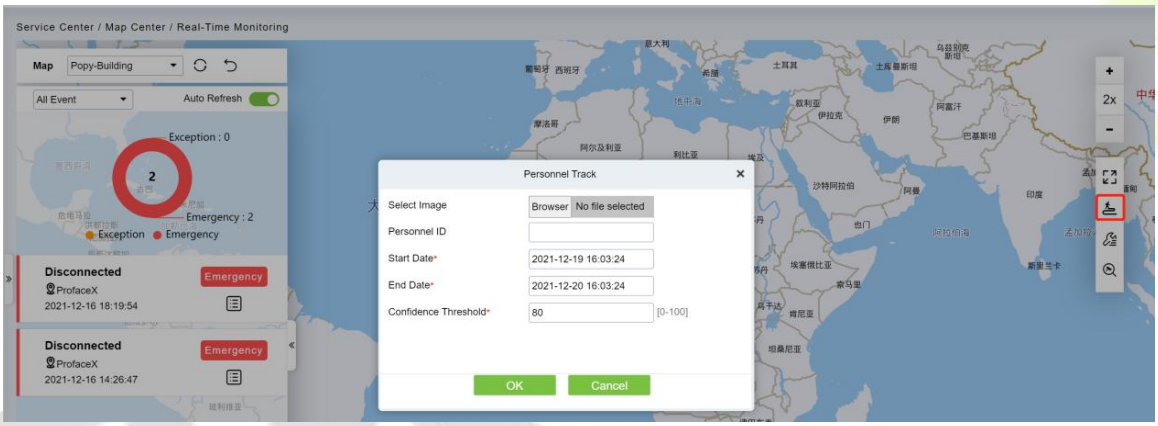


Figure 21- 14 Page for Querying Personnel Trends

Step 3: Click **OK** to display the movement chart on the map.

21.5.1.2 Batch Operation

This part introduces the configuration Step for real-time monitoring of batch operation in the service center module.

● Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Real-time Monitoring**".

Step 2: On the real-time monitoring screen, click the icon on the right in the personnel Trend window that is displayed, set related parameters,

● Remote Opening / Remote 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 remote opening, user can define the door opening duration (The default is 15s). You can select **Enable Intraday Passage Mode Time Zone** to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select **Disable Intraday Passage Mode Time Zone** first, to avoid enabling other normal open time zones to open the door, and then select **Remote Closing**.

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

● Activate Lockdown:

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

● Deactivate Lockdown:

It will unlock a locked door. This function is supported only by certain devices.

● Cancel Alarm:

Once an alarming door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click **Remote Opening/Closing** in 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

21.5.1.3Search Device

This part introduces the configuration Step for real-time monitoring of search device in the service center module.

Add a Door

This part introduces the configuration Step of map configuration and door addition in the service center module.

● Operation Step:

Step 1: In the service Center module, choose "**Map Center > Map Configuration**".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen  to add the gate.

Step 3: In the Add Door list on the left of the page, drag the required **Access Control** device to place it on the map,

Step 4: Click **Submit** under the left door bar to complete the operation of adding a door on the map.

Adding a Camera

This section describes how to add camera Step for map configuration in the Service Center module.

● Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Map Configuration**".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen to add a camera.

Step 3: In the Add Camera list on the left of the screen drag the required camera device to place it on the map,

Others

This section describes how to add others Step for map configuration in the Service Center module.

● Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Real Time Monitoring**".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen to add Others.

Step 3: In the Add Other list on the left of the screen drag the required other device to place it on the map,

Map

Click the Map: It will show the area of the map.

Defense Area

It will show the defence area in the map.

21.5.1.4Handle Video Alarm Details

This section describes the Step configuration for handling video alarm event details in the Service Center module.

● Operation Step

Step 1: In the Service Center module, choose "**Map Center > Real-time Monitoring**".

Step 2: On the real-time monitoring screen, select a video alarm in the left pane and click to display detailed information. As shown in Figure 20-15.

Instructions:

Function description of the detailed information interface:

1. Preview: Displays the live view of the current video device.Click to view the video preview. In the preview interface, cameras that support intercom allow you to turn on the microphone for voice intercom.
2. Playback: Plays back the records generated by alarm events.
3. Trend: record the corresponding trend record of personnel.
4. Report: You can note the event status.

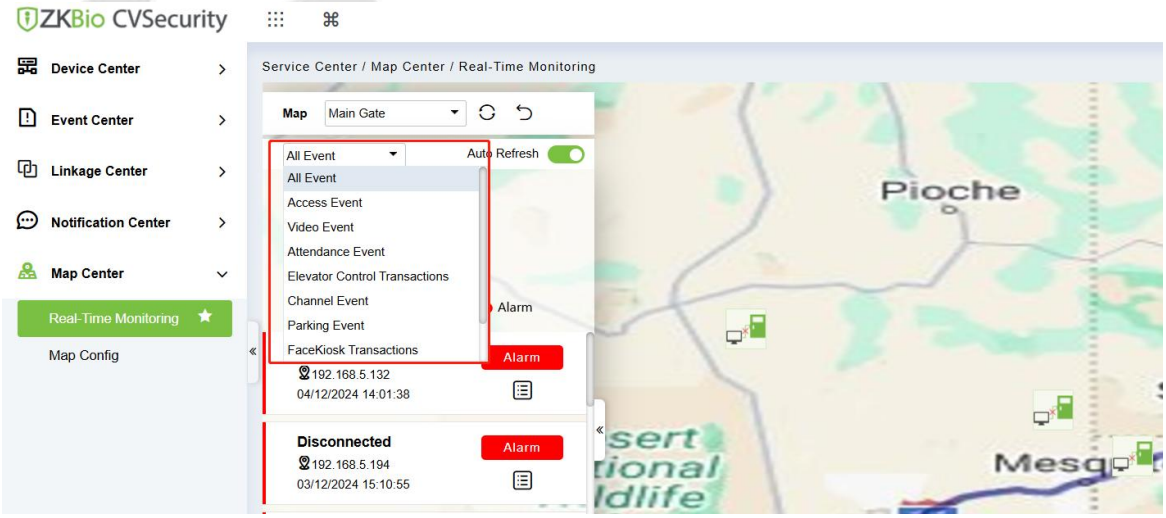


Figure 21- 15 Video Alarm Details Screen

Step 3: After viewing the detailed information and remarks, click **Submit**.

21.5.1.5Handle Door Alarms in Details

This section describes the Step configuration for handling gate alarm event details in the Service Center module.

● Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Real-time Monitoring**".

Step 2: On the real-time monitoring page, select the event for which the access control alarm is generated in the left pane and click The detailed information is displayed.

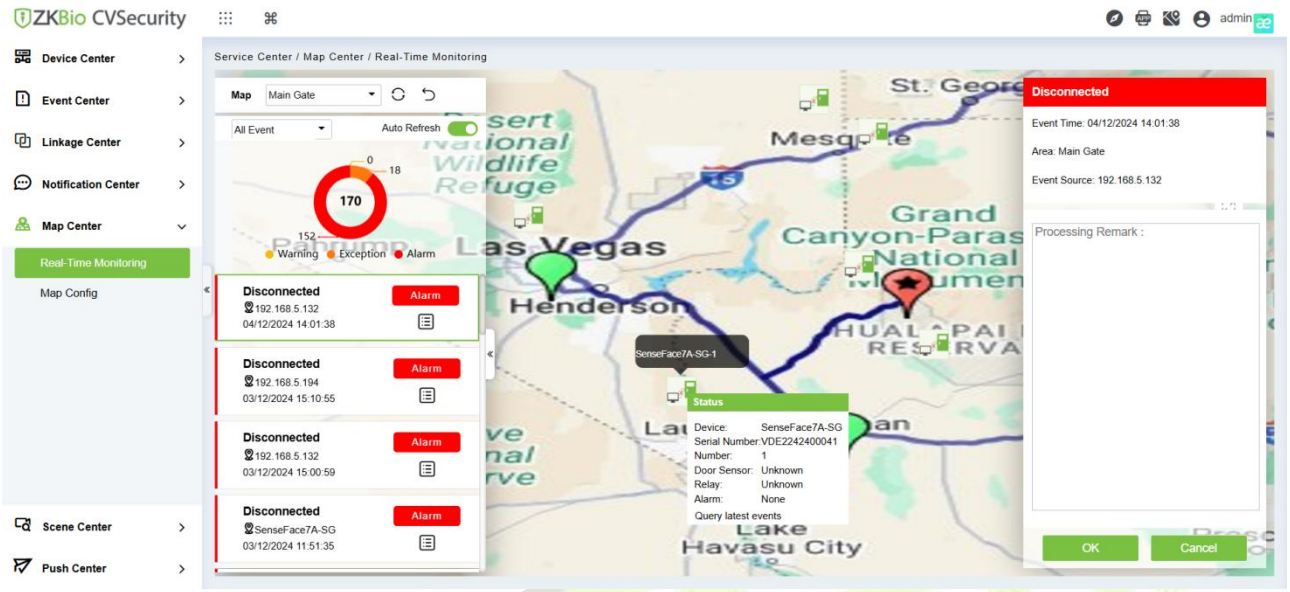


Figure 21- 16 Access Alarm Details Page

Step 3: After filling in the report remarks, click **Submit**.

21.5.2Map Config

By importing the map and configuring the corresponding monitoring points, the distribution of the current monitoring points can be intuitively displayed.

● Instructions:

Table 21-1 describes the ICONS on the map configuration page.

Icon	Instructions
	Full screen.
	The refresh.
	Return to the previous level.
	Drag ICONS of **Access Control** and camera and move coordinates; After Operation is finished, click , can be saved.
	Add the icon of the **Access Control** device.
	Add a camera icon.

Icon	Instructions
	Add sub maps.
+ 11x -	Operation to zoom in and out of the map.
	Move the mouse over the "door or Video" device on the map and right click it out.
	Add a map.
	The editor.

Table 21- 1 Map Configuration Icons

● The Premise Conditions:

1. The access control device is added to the Access Control module.

2. Add the camera device under the video module.

21.5.2.1 Add Map

This section describes how to add Step of map configuration in the Service Center module.

● Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Map Configuration**".

Step 2: In the map configuration screen, click on the left bar . The page for adding a map is displayed, as shown in Figure 21-17. For details about the parameters, see Table 21-2.

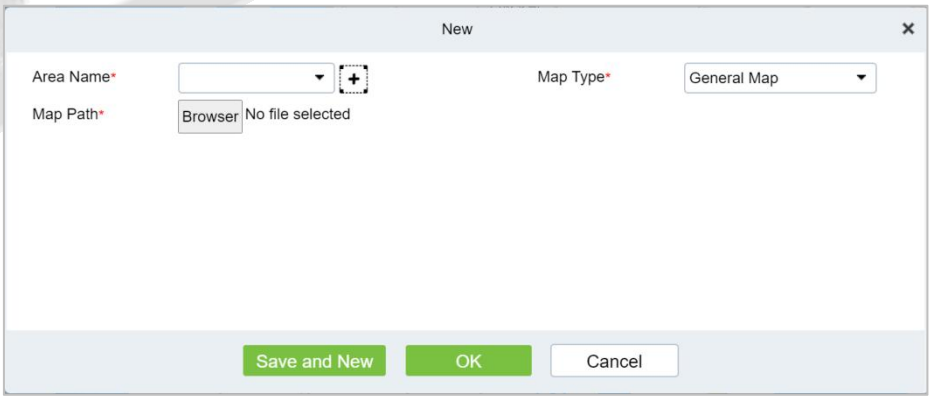


Figure 21- 17 Add Map Page

The Map Type	Parameter	Instructions
Normal	Name	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.

The Map Type	Parameter	Instructions
Mapping (Using the map drawn by the user, as the background loading,)	Map Path	Select the map you want to add, that is, the map image file that exists on the local server in advance. **Instructions** • Map is supported formats. Jpe \. JPG \. JPEG \. GIF \. PNG \. BMP \. Ico \. SVG \. SVGZ \. Tif \. Tiff \. Ai \. DRW \. PCT \. PSP \. XCF \. PSD \. Raw \. Webp image file. • Map image file size should not exceed 1120 × 380px.
Hyper graph	Name	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
	Map Path	To set up a GIS server, set parameters on the server, and then set these parameters.
	Route Analysis Path	
	Projection	
	The Center X/Y Coordinate	Fill in the latitude and longitude.
	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	Maximum Zoom Level/Minimum Zoom Level	Custom map zoom size.
Google Maps	Area	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
	The Map Key	Log on to the platform for https://cloud.google.com/maps-platform for registration for the key. **Instructions:** You need to turn on the Directions API on Google's platform to map people's movements.
	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	The Center X/Y Coordinate	Fill in the latitude and longitude.
Baidu Map	Area	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
	The Map Key	Log in to http://lbsyun.baidu.com/ to register and obtain the key.

The Map Type	Parameter	Instructions
	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	The Center X/Y Coordinate	Fill in the latitude and longitude.

Table 21- 2 Parameters for Adding a Map

Step 3: Set parameters based on the type of the map to be added and Click **OK** to finish adding the map.

21.5.2.2Add Sub-map (Optional)

This section describes how to add sub-map configuration Step on the map in the **Service Center** module.

●Operation Step:

Step 1: In the Service Center module, choose "**Map Center > Map Configuration**".

Step 2: Select a region map and click on the "Add Map"to add sub-maps.

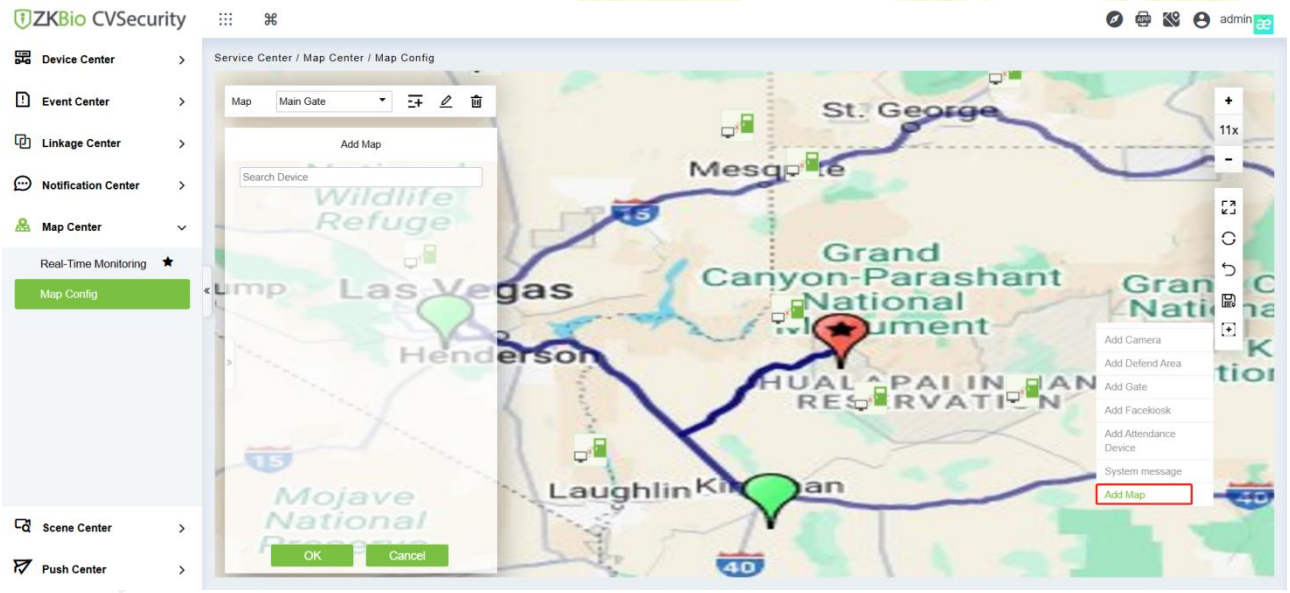


Figure 21- 18 Add Sub-map Page

Step 3: Click **OK** under add map on the left to complete the configuration of the sub-map.

21.5.2.3Add Door

This part introduces the configuration Step of map configuration and door addition in the service center module.

●Operation Step

Step 1: In the service Center module, choose "**Map Center > Map Configuration**".

Step 2: On the map configuration screen, select the map of the desired area and click **"Add Door"**on the right of the screen to add the gate.

Step 3: In the Add Door list on the left of the page, drag the required **Access Control** device to place it on the map.

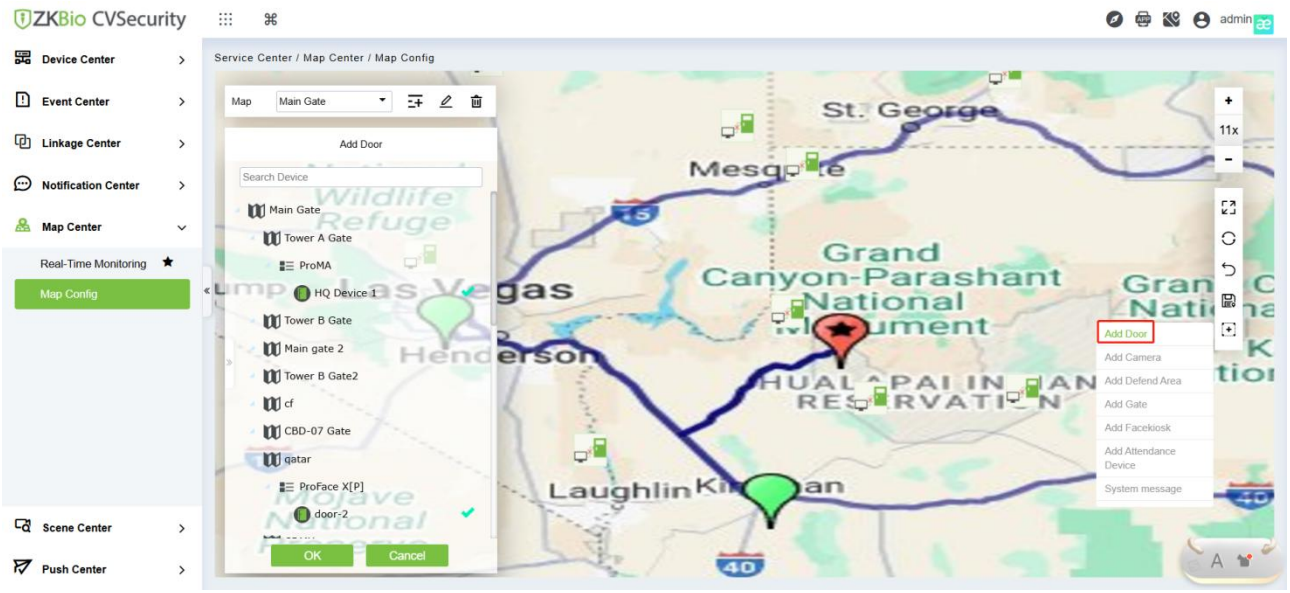


Figure 21- 19 Add Door Page

Step 4: Click **Submit** under the left door bar to complete the operation of adding a door on the map.

21.5.2.4Add Camera

This section describes how to add camera Step for map configuration in the Service Center module.

● Operation Step

Step 1: In the Service Center module, choose "**Map Center > Map Configuration**".

Step 2: On the map configuration screen, select the map of the desired area and click **"Add Cameras"** on the right of the screen to add a camera.

Step 3: In the Add Camera list on the left of the screen, drag the required camera device to place it on the map.

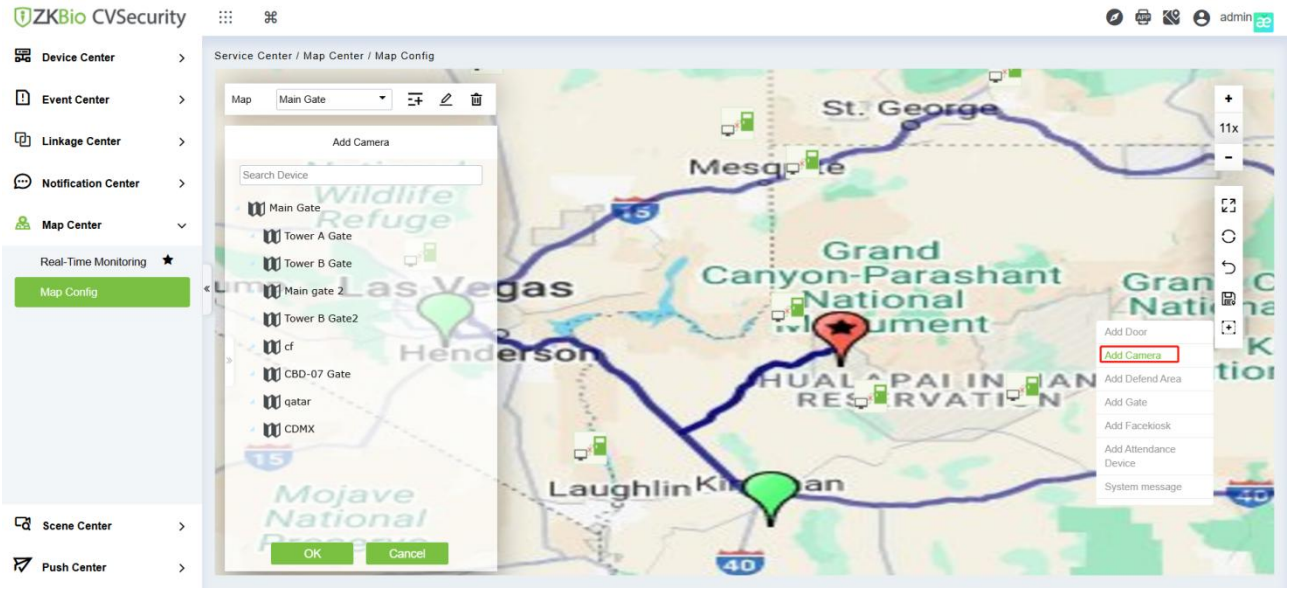


Figure 21- 20 Add Camera Screen

Step 4: Click **Submit** in the left column of Adding a camera to complete the configuration of adding a camera to the map.

21.5.2.5Add Defence Area

We can view the Intrusion Alarm states in real time through the map center.

Step 1: Go to **Service Center** > **Map Center** > **Map Config**. Click the **add icon** on the right side of the interface and select "**Add Defend Area**".

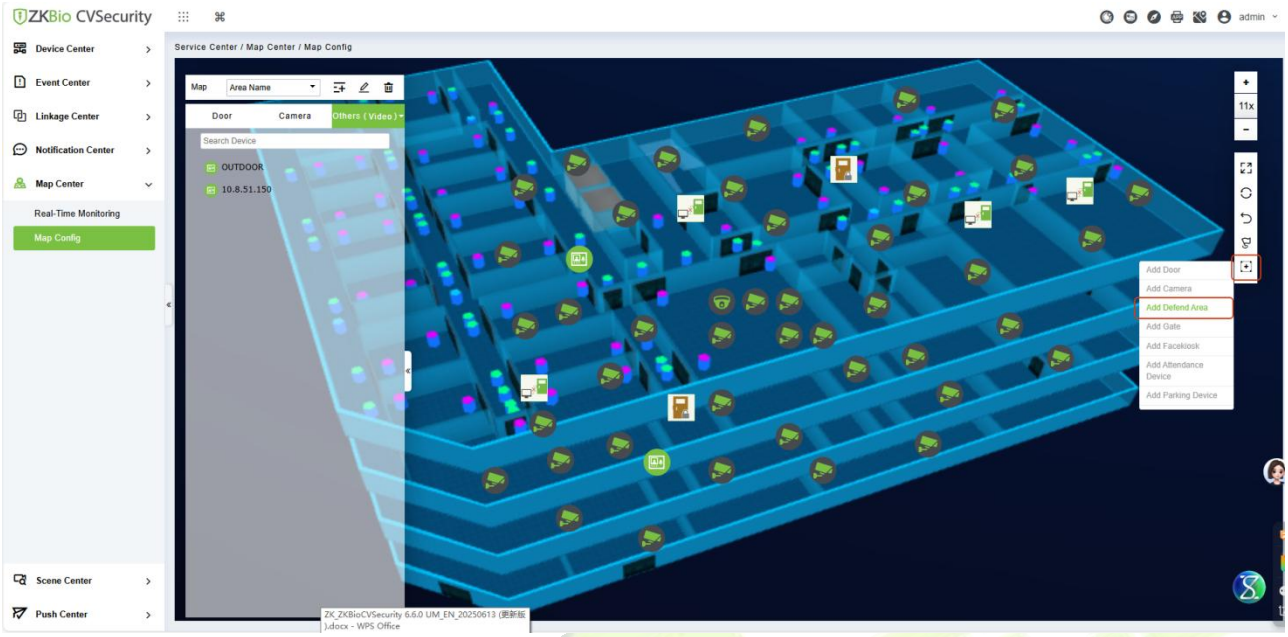


Figure 21- 21 Adding Defense Interface

Step 2: Click the **Adding Defence Area** on the left of the screen, drag the required partition or zone to place it on the map.

Step 3: Click **OK** the left column of **Adding Defence Area** to complete the configuration of adding a partition.

21.5.2.6Add Intercom Device

We can check the online/offline status of DNK devices on the Real-Time Monitoring interface.

Step 1: Go to **Service Center** > **Map Center** > **Map Config**. Click the **add icon** on the right side of the interface and select "**Add Intercom Device**".

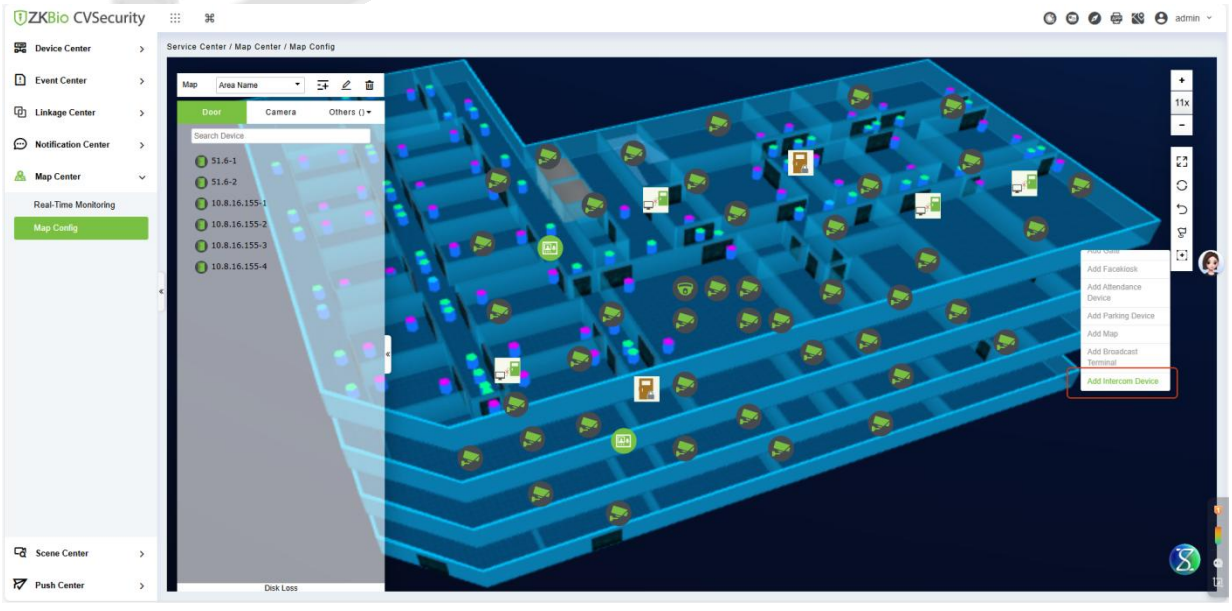


Figure 21- 22 Adding Intercom Device Interface

Step 2: Click the **Add Intercom Device** on the left of the screen, drag the required device to place it on

the map.

Step 3: Click **OK** the left column of **Add Intercom Device** to complete the configuration of adding a partition.

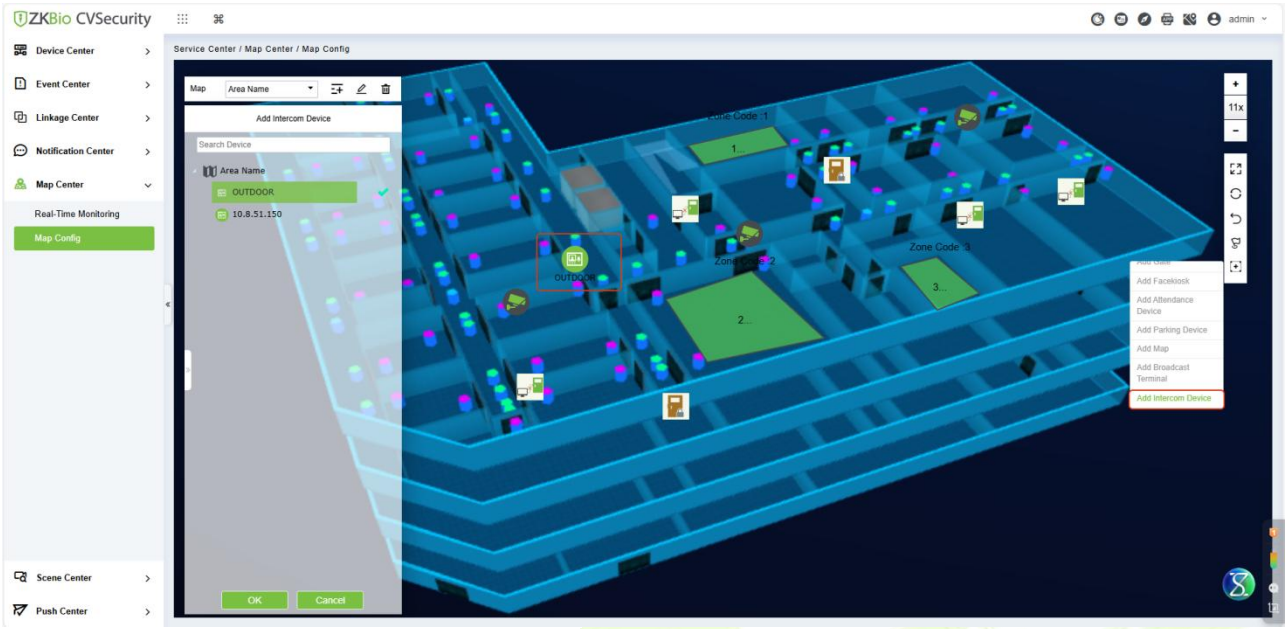


Figure 21- 23 Adding Intercom Device Interface

21.5.2.7Map

Click the Map: It will show the area of the map.

21.6 Scene Center

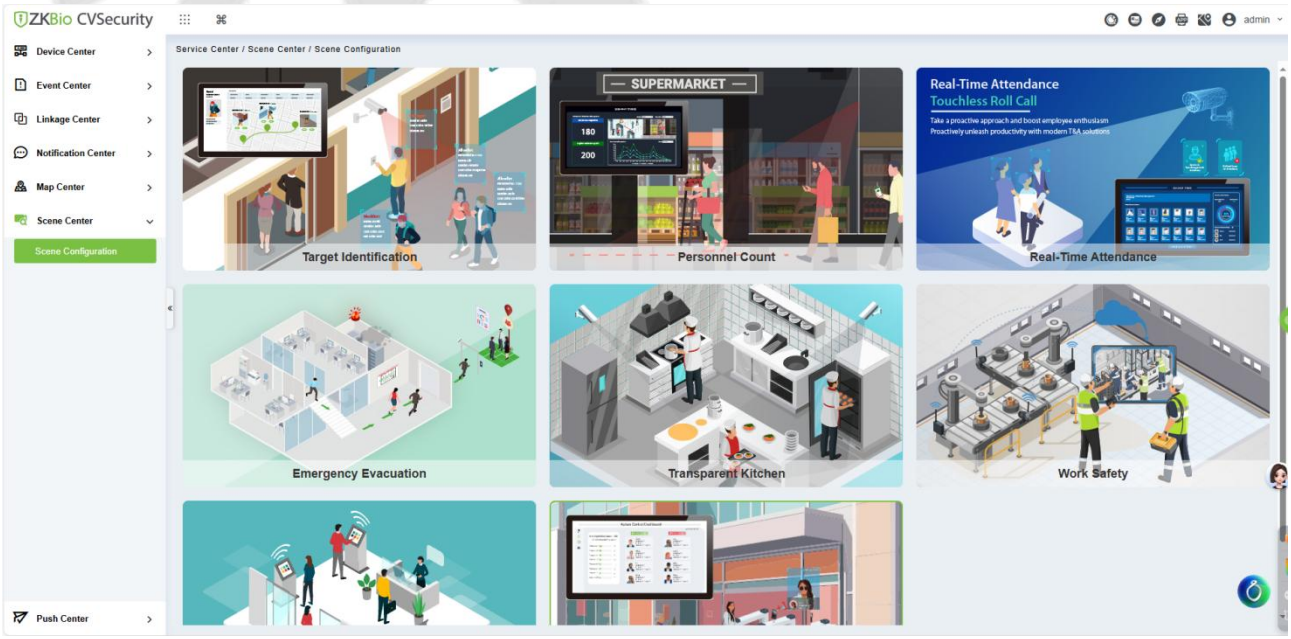


Figure 21- 24 Scene Center Interface

Note: The corresponding business modules must be installed to use the functions of the scenario center. The supporting modules are as follows：

- **Target Identification:** Smart Video Surveillance Module must be installed.
- **Personnel Count:**Smart Video Surveillance Module must be installed.
- **Real-time Attendance** :Time&Attendance and Smart Video Surveillance Module must be installed.
- **Emergency Evacuation** :Access Control and Smart Video Surveillance Module must be installed.
- **Transparent Kitchen:**Smart Video Surveillance Module must be installed.
- **Work Safety:**Smart Video Surveillance Module must be installed.
- **Intelligent Visitor Panel:**Visitor Module must be installed.
- **Space Occupancy Count:**Access Module must be installed.

21.6.1Target Identification

Hardware Supported : ZKIVA-Edge X1 /T1

Click this icon into Target Identification Guide:

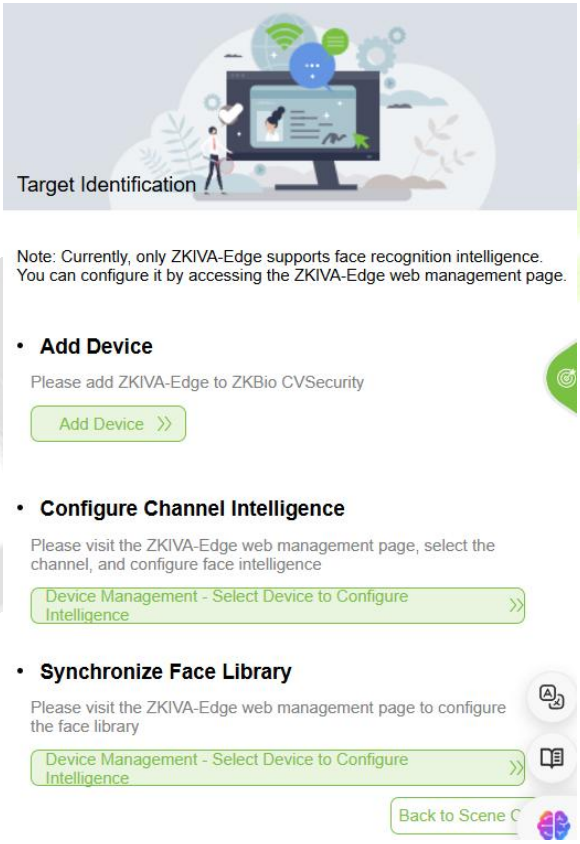


Figure 21- 25

✍ **Note:** Currently, only ZKIVA-Edge supports face recognition intelligence. You can configure it by accessing the ZKIVA-Edge web management page.

- **Operation Step**

Step1: Add Device

Click **Add Device**, the system will automatically jump to **[Smart Video Surveillance]** > **[Device Management]** > **[Device]**, you can add ZKIVA-Edge devices here, and you can refer 4.1 Device Management for specific operation.

Step2: Synchronize Face Library

1. Click Synchronize Face Library to jump to [Smart Video Surveillance] > [Device Management] >

[Device], in this page we can configure the face library.

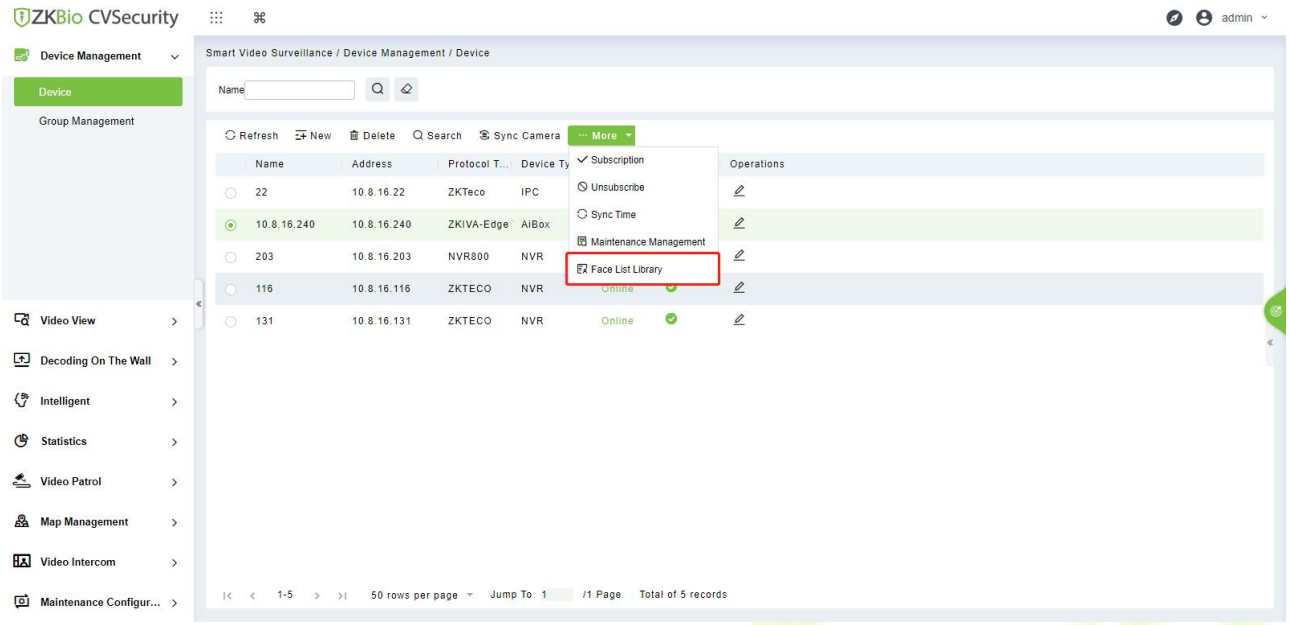


Figure 21- 26

2. Select the face library to be added

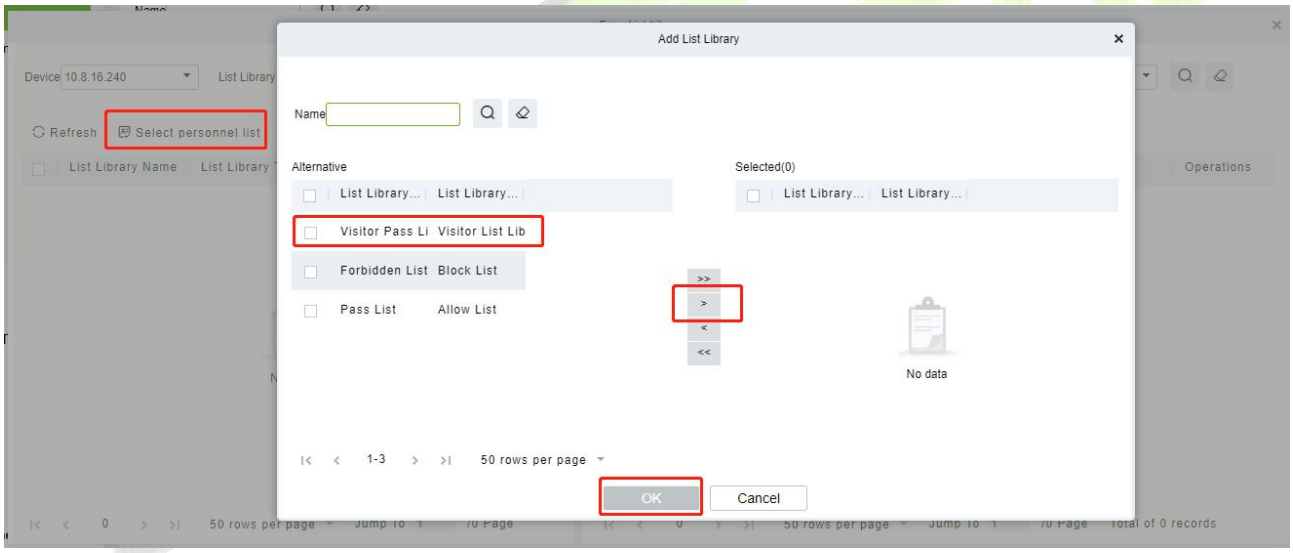


Figure 21- 27

Step 3: Configure Channel Intelligent

The Face Intelligence configuration feature is now moved to the web side of the device, Please visit the ZKIVA-Edge web management page, select the channel, and configure face intelligence.

1. Click Configure Channel Intelligent to jump to [Smart Video Surveillance]>[Device Management] > [Device].
2. Click [Smart Video Surveillance]>[Device Management]>[Device]>[Maintenance Management] to jump to device web management page.

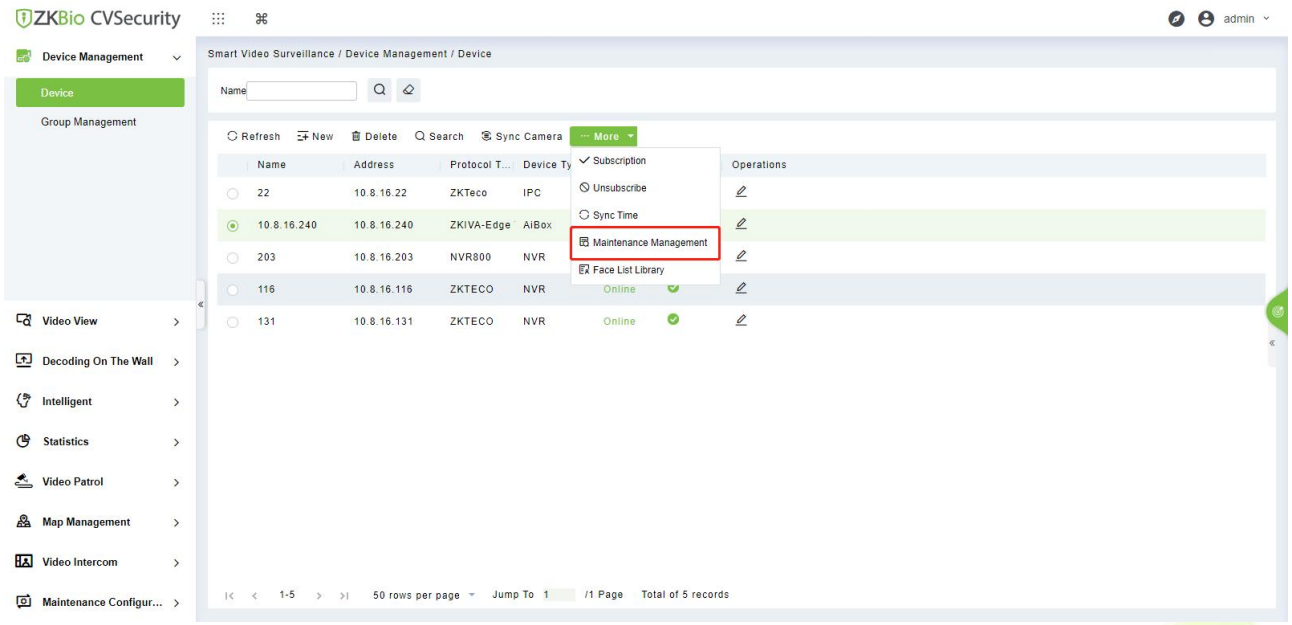


Figure 21- 28

Note: Take the web management page of ZKIVA-Edge T1 for example:

1. Click [Data connect]>[Active reporting] >[Server address] to fill in the server address and active report your server IP to device.

Server address Format: http://main (ip):port/

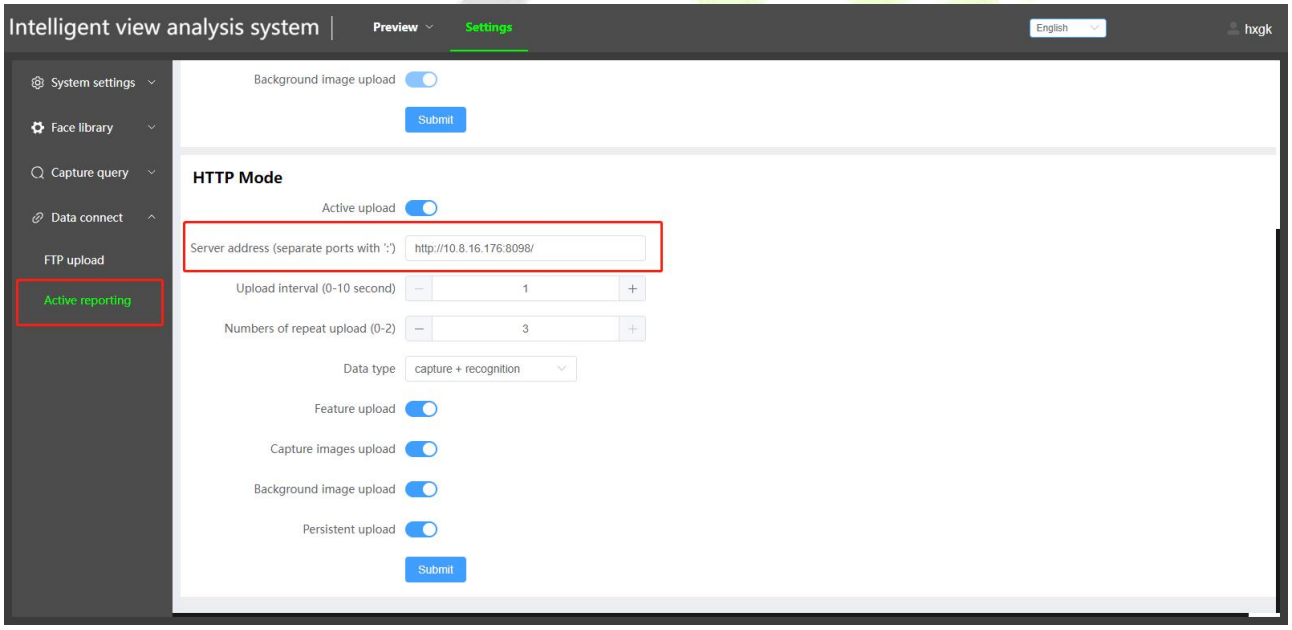


Figure 21- 29

2. Click [Channel management]>[View/Edit] to visit the channel management interface.

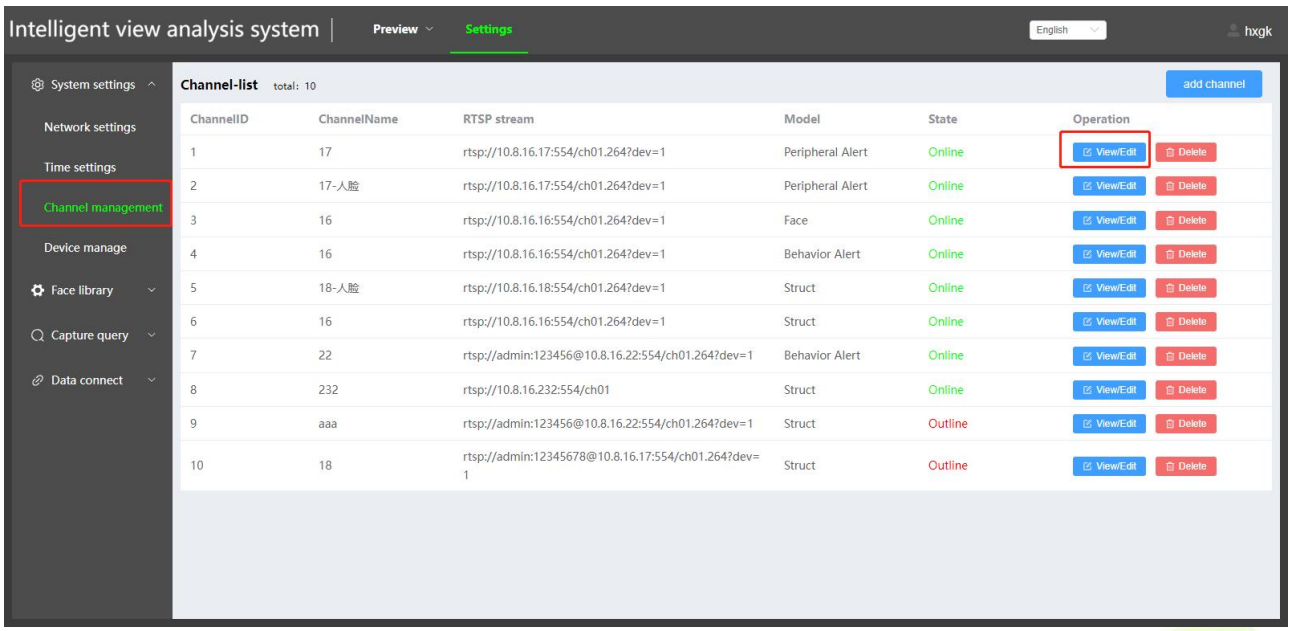


Figure 21- 30

3. Select the type of channel as Face to perform face recognition rule configuration and then submit the configuration to enable the Target identification.

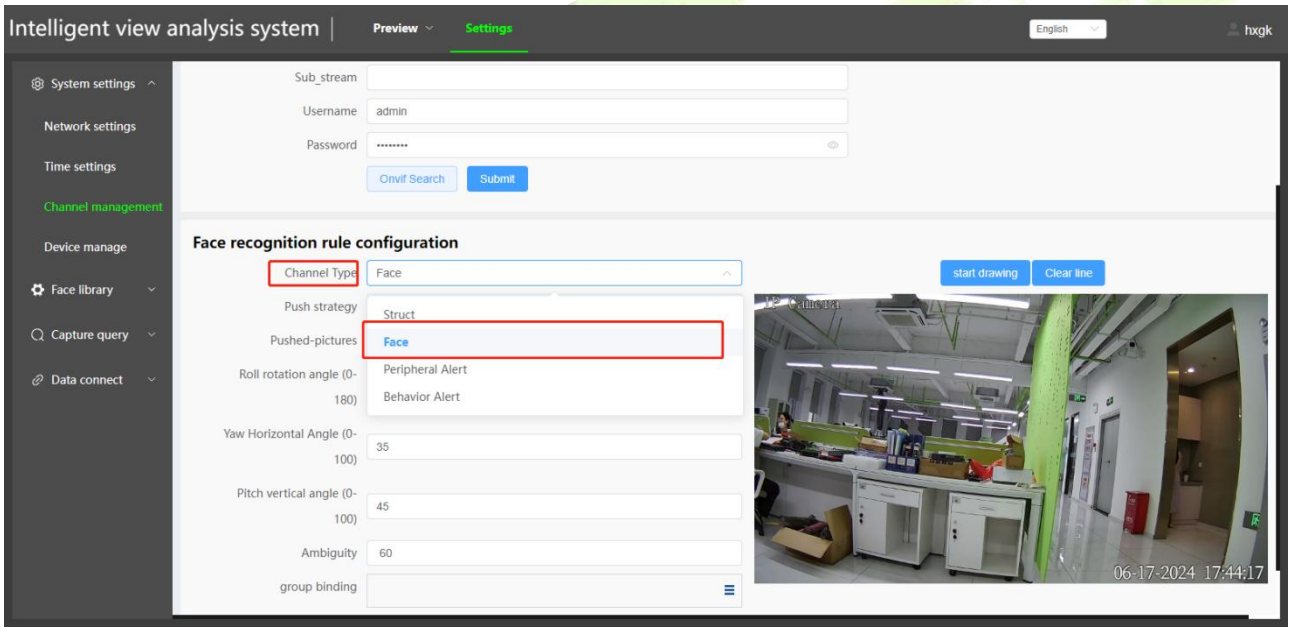


Figure 21- 31

● Target Identification Scene Page

Click **Enter Scene** to enter the target identification function.

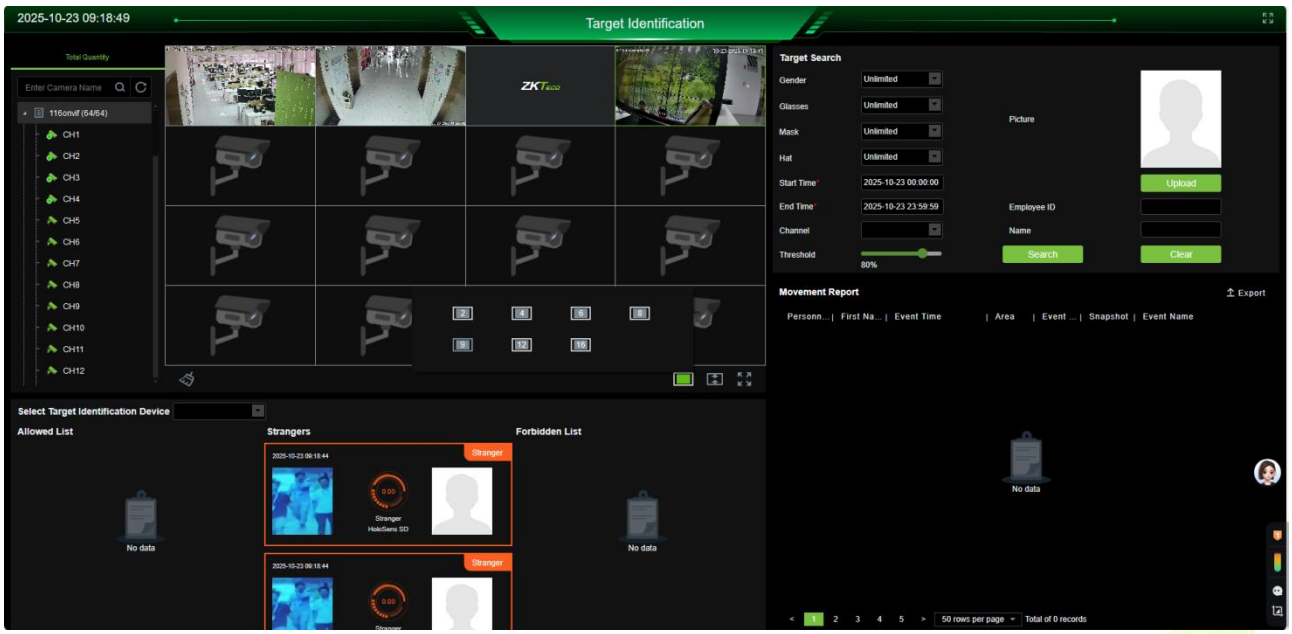


Figure 21- 32

Click the toolbar below to close all screens.

Click the toolbar below to switch the number of video - preview windows.The preview window in the scenario center supports up to 16 channels for simultaneous on-screen preview.

- **Quick Search**

Right-click on the list of triggered events to quickly retrieve people.

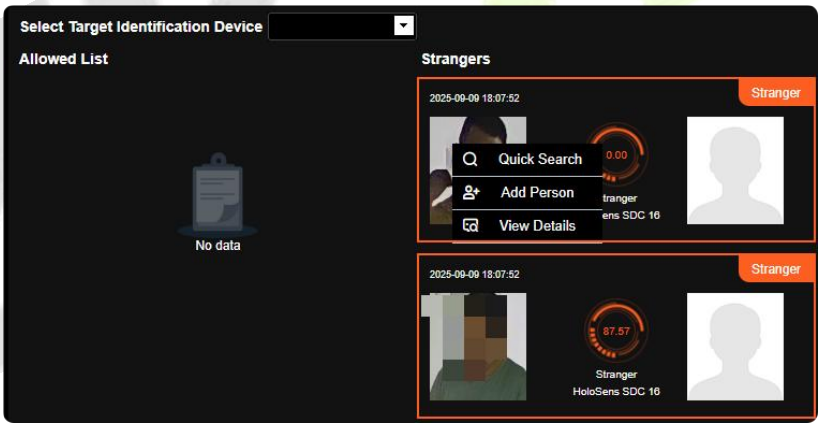


Figure 21- 33

- **Target Search**

It is possible to track personnel's passage by searching for their name, employee ID, photo, gender, whether they are wearing glasses, a mask, or a hat.

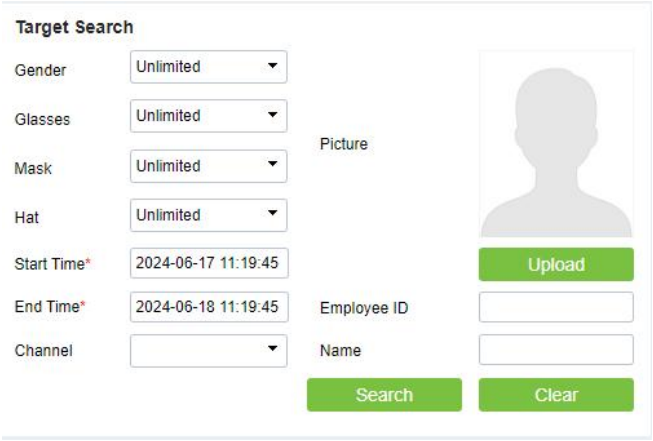


Figure 21-34

- **Movement Report**

In the movement report, you can see the movement track of specific personnel, and click **[export]** to export the movement track report of personnel.

Figure 21-35

21.6.2 Personnel Count

Hardware Supported : ZKIVA-Edge X1

Click this icon into Personnel Count Guide:

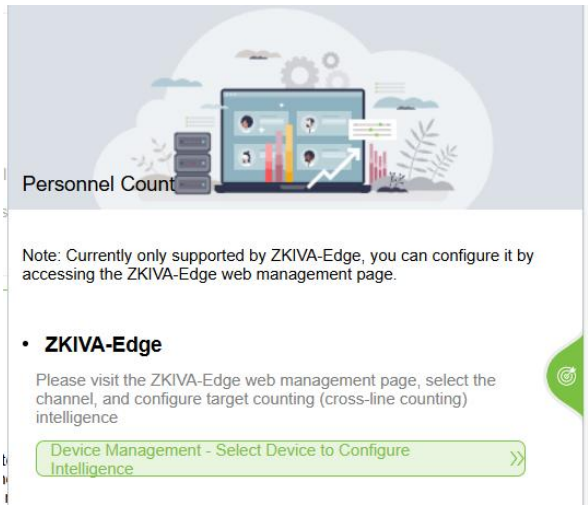


Figure 21-36

Note: Currently, only ZKIVA-Edge X1 supports Cross-line statistics intelligence. You can configure it by accessing the ZKIVA-Edge X1 web management page.

● Operation Step

Step1: Add Device

Add ZKIVA Edge device, please refer to Target Identification for details.

Step2: ZKIVA-Edge

Visit the ZKIVA-Edge web management page, select the channel, and configure target counting (cross-line counting) intelligence.

Take the web management page of ZKIVA-Edge X1 for example:

1. Click [Setting]>[Task Setting] to add a new task.FG

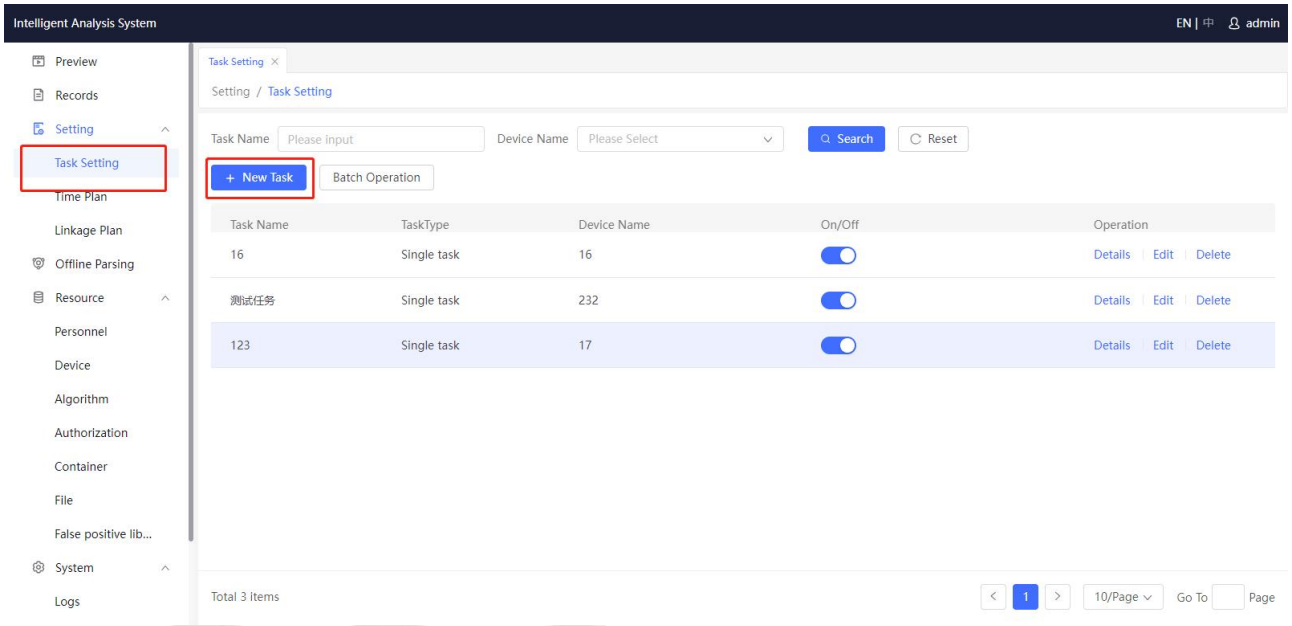


Figure 21- 37

2. Perform basic configuration, and then click Submit.

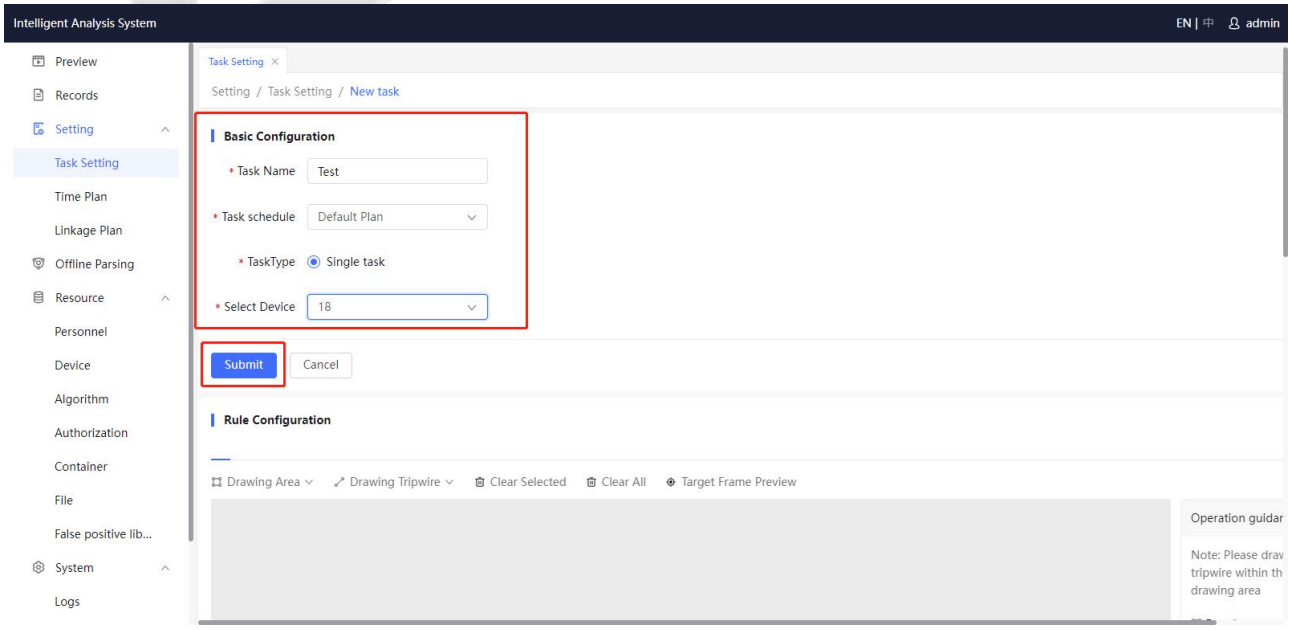


Figure 21- 38

3. After submit the basic setting, click [Drawing Tripwire]>[Entry/Exit Tripwire] to draw entry and exit tripwire, select the configured algorithm and submit it.

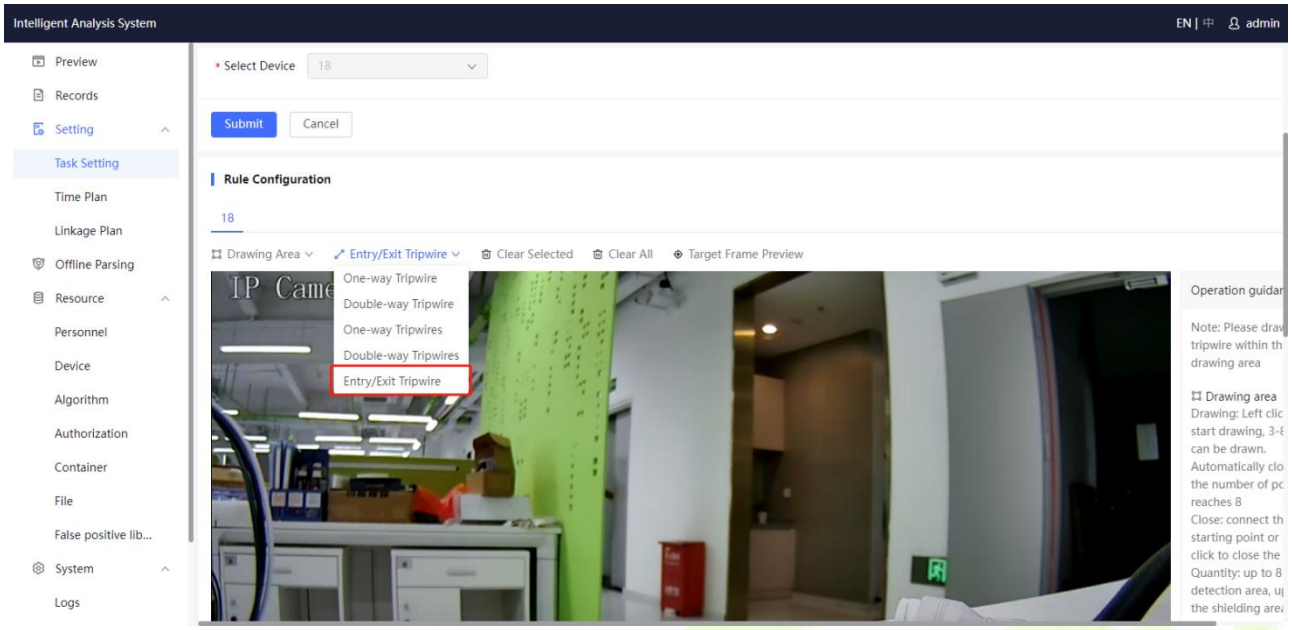


Figure 21- 39

● Personnel Count Scene Page

Click **Enter Scene** to enter the personnel count function.

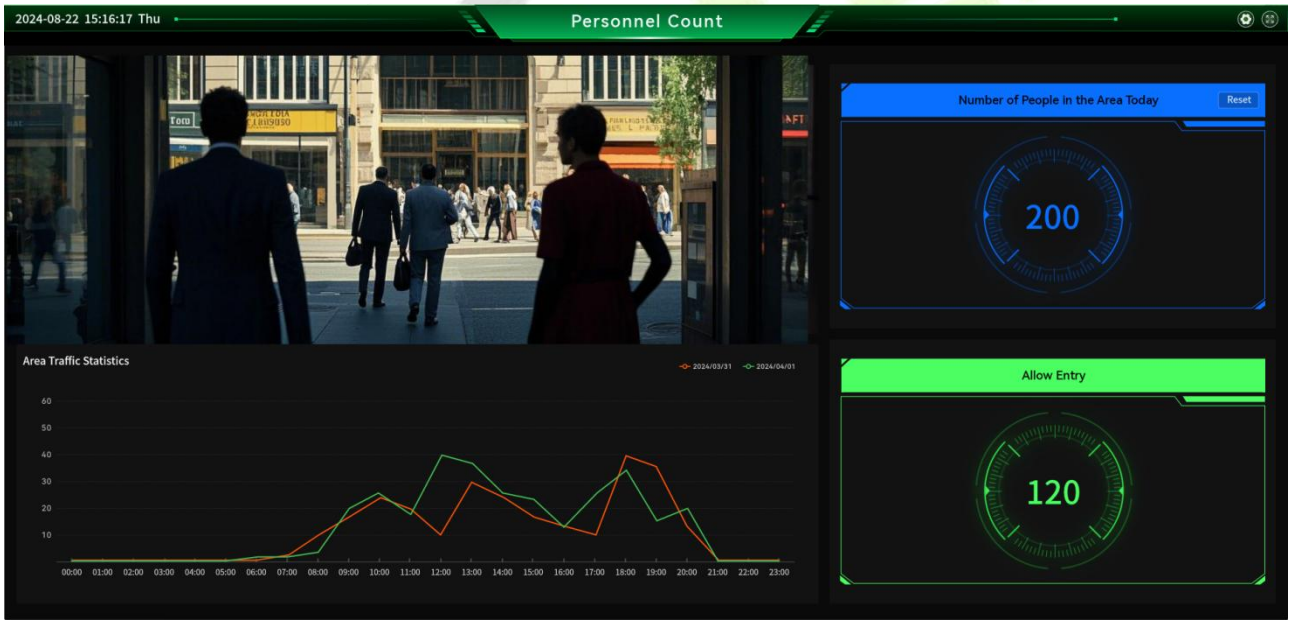


Figure 21- 40

21.6.3Real Time Attendance

Hardware Supported : ZKIVA-Edge X1 /X1

● **Operation Step**

Click Configuring Scenarios, to view the operation wizard.

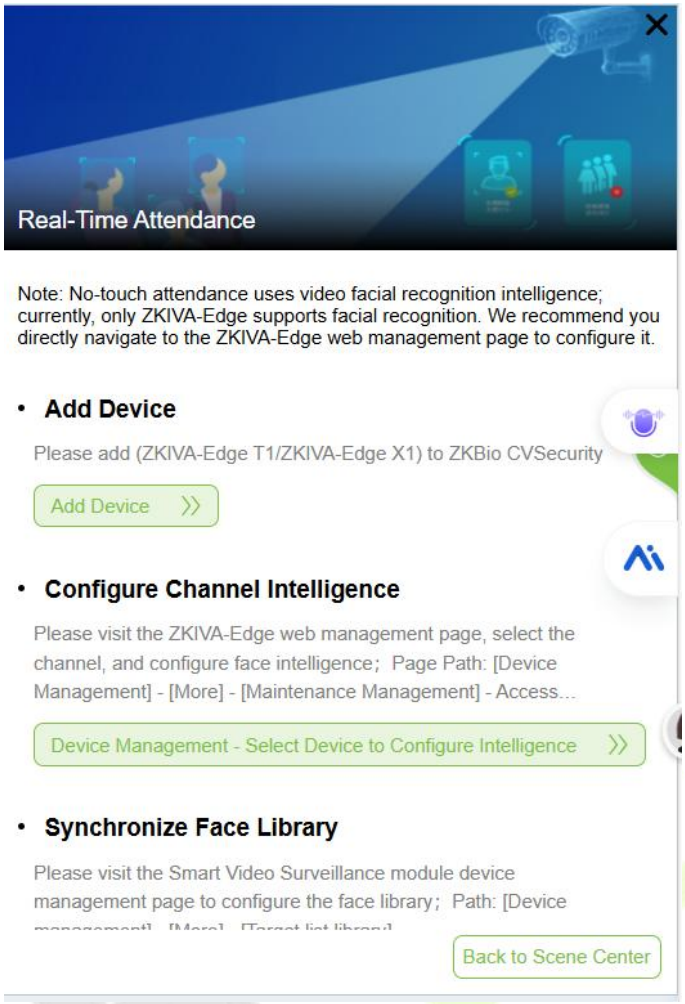


Figure 21- 41

Step 1: Refer to Target Identification to add the ZKIVA-Edge device, and configure the face recognition intelligence.

Step 2: Refer to Target Identification to synchronize the Face Library.

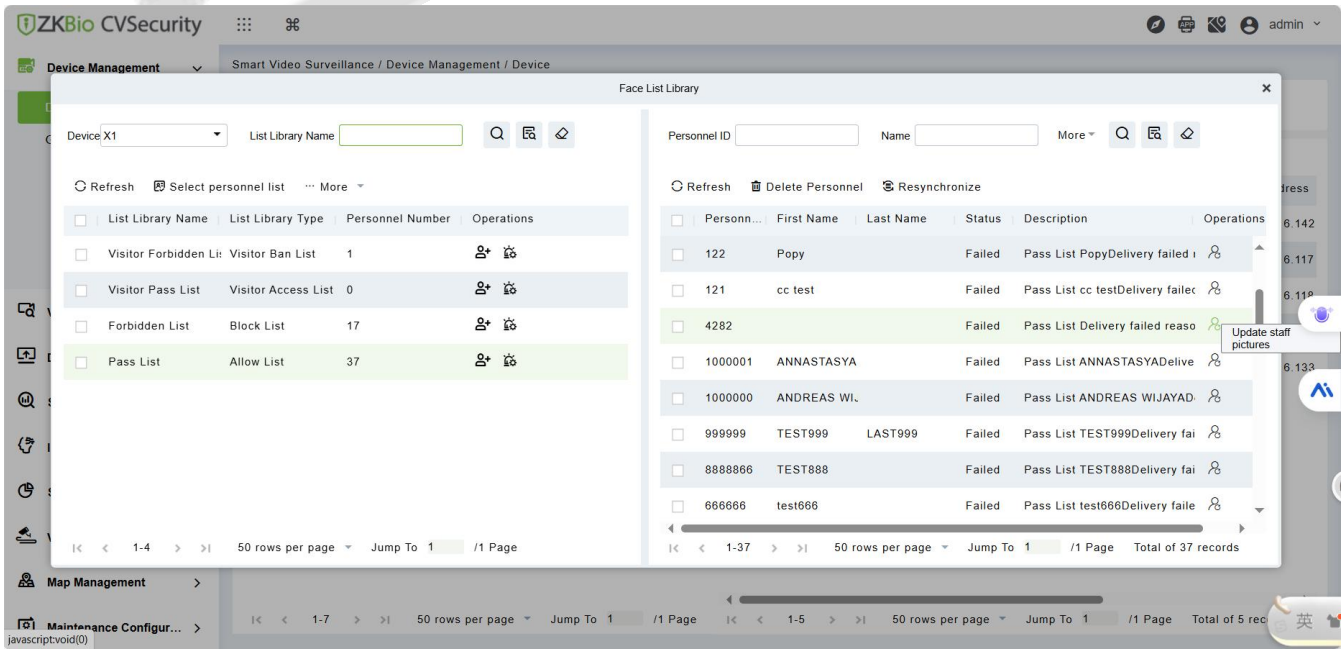


Figure 21- 42

Step 3: Configure the attendance point:

Please go to **Attendance -> Attendance Management -> Attendance Point**, and click **New** to configure the ZKIVA-Edge device as the attendance point:

Device Module: Please select Smart Video Surveillance.

Device List: Please select the channel with face recognition algorithm in the ZKIVA-Edge device that you configured previously.

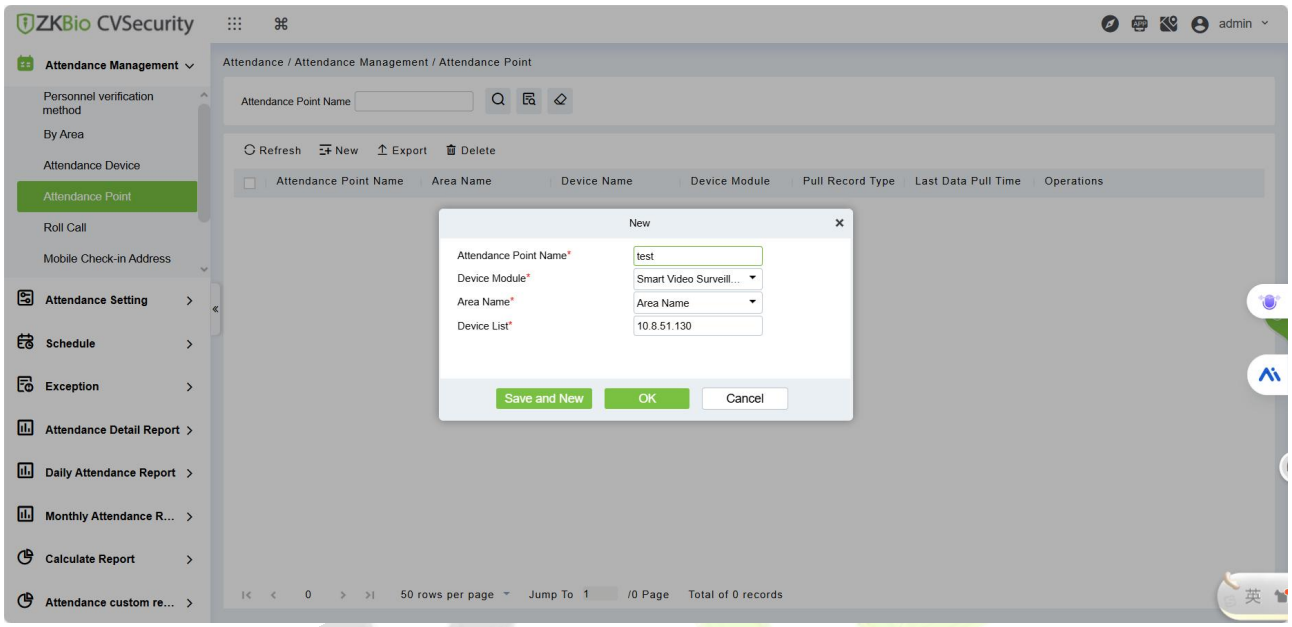


Figure 21- 43

Note: After configuring the attendance point, be sure to assign attendance shifts to the personnel.

● **Result verification:**

Click "**Back to Scene Center**" in the Operation Wizard. Click "**Enter Scene**" on the Real Time Attendance card.

Figure 21- 44

Then you can enter the Real-time Attendance page to view the roll call data in real time.The preview window in the scenario center supports up to 16 channels for simultaneous on-screen preview.

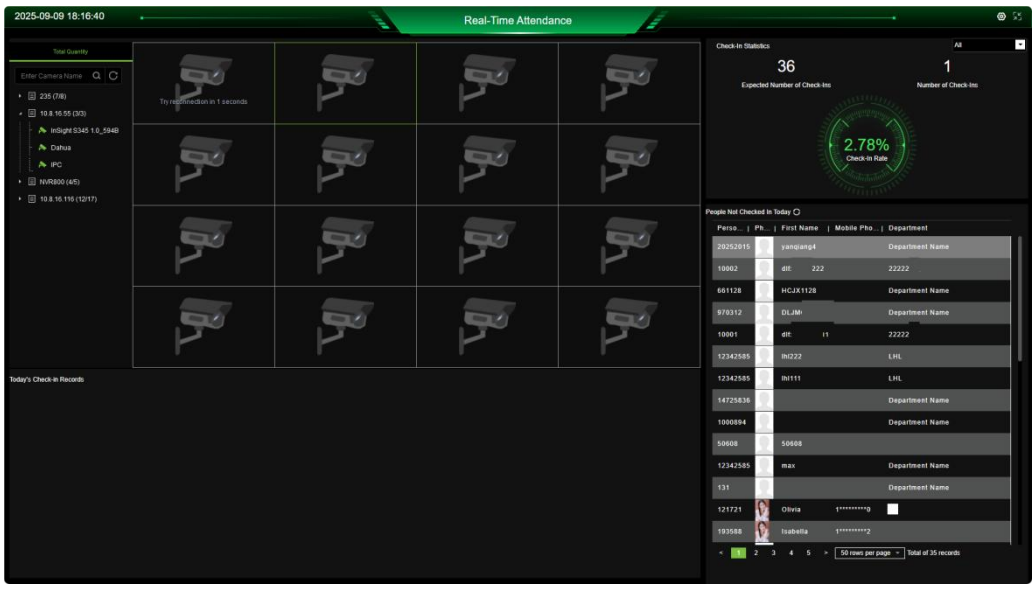


Figure 21- 45

21.6.4Emergency Evacuation

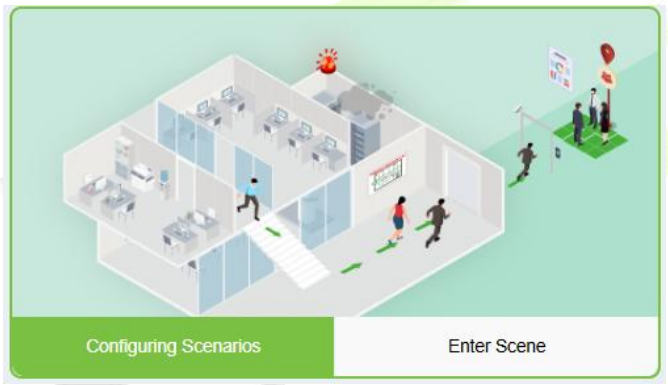


Figure 21- 46

Click **Configuring Scenarios** to enter the scene configuration of Emergency Evacuation;

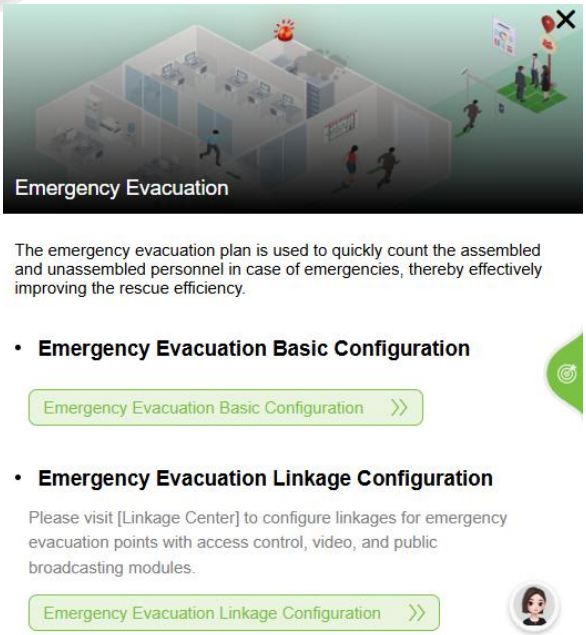


Figure 21- 47

Click **Emergency Evacuation Basic Configuration** and follow the Tab page above to complete the operation.

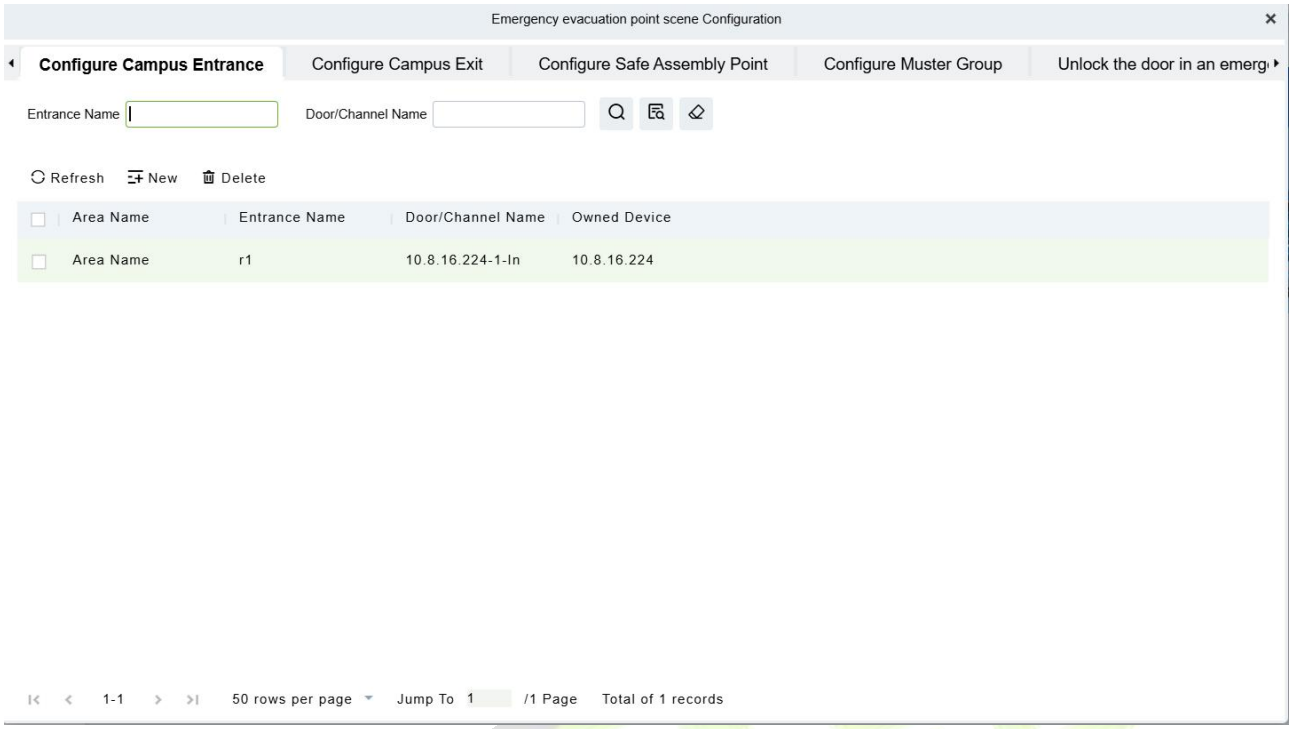


Figure 21- 48

Operation Step :

Step 1: Configure Main Entrance

This menu is used to configure the main entrance, which is used to count the people entering. To avoid missing statistics, please be sure to configure all the main entrances within the set range.

Click **New** and select the main entry device. As shown in the following figure:

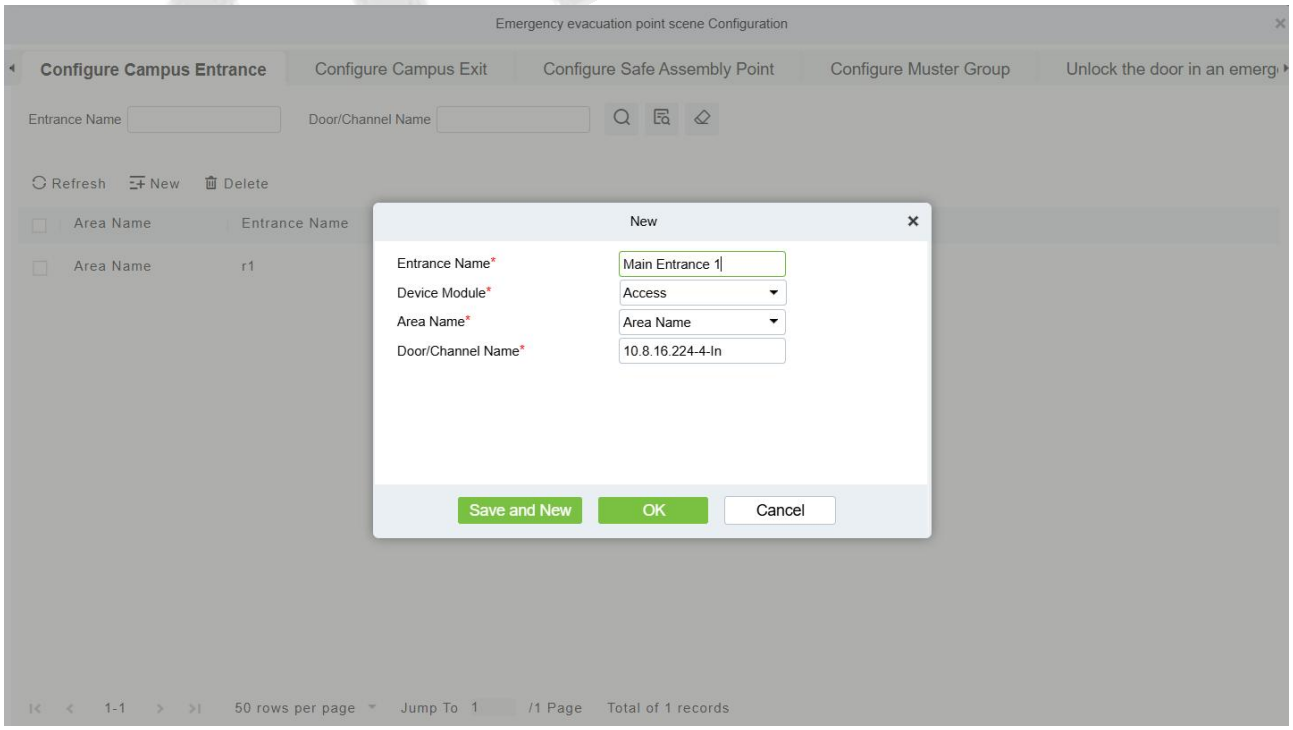


Figure 21- 49

The supported device modules include: Access , Entrance Control, and Parking.

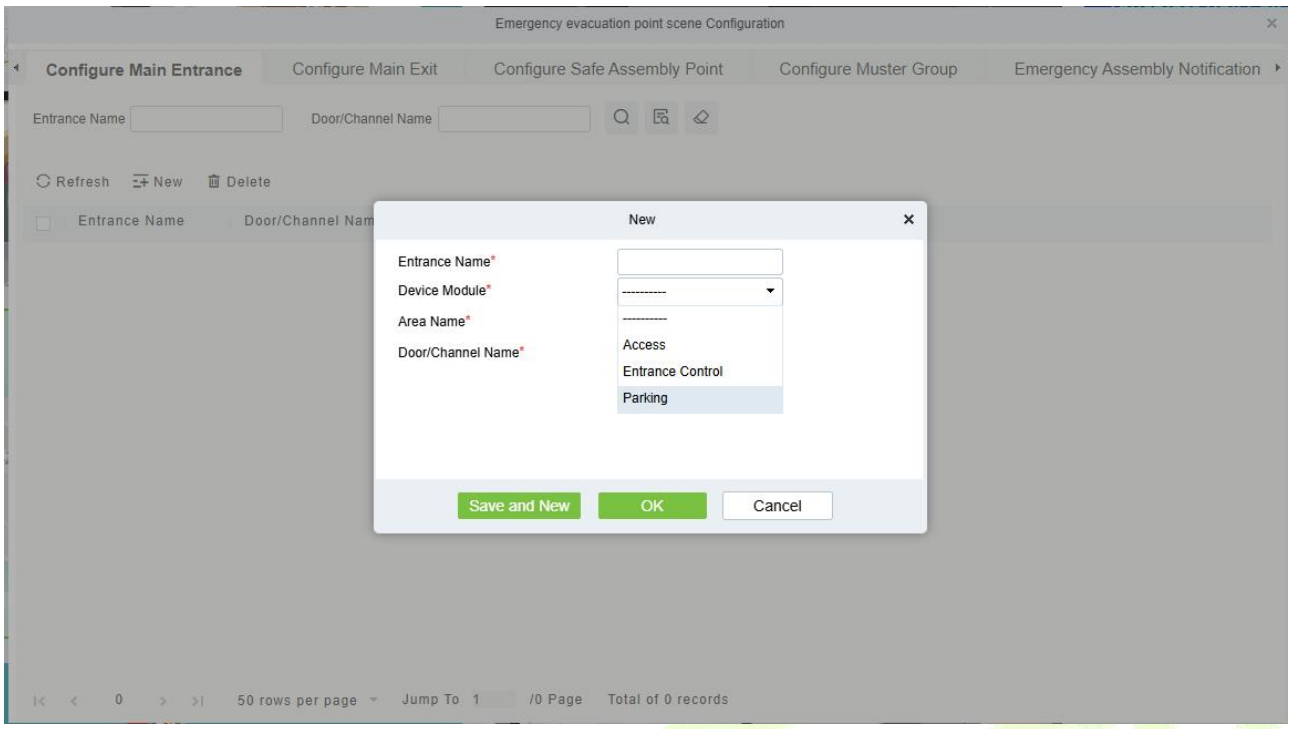


Figure 21- 50

Step 2: Configure Main Exit

This menu is used by users to configure the main exit, which is used to count the people who go out; when an emergency is triggered, the statistical resources will mainly count the people inside the building; the people who have gone out will not be included in the statistical resources. To avoid missing statistics, please make sure to configure all exits within the collection range.

Click **New** and select the main export device. As shown in the following figure:

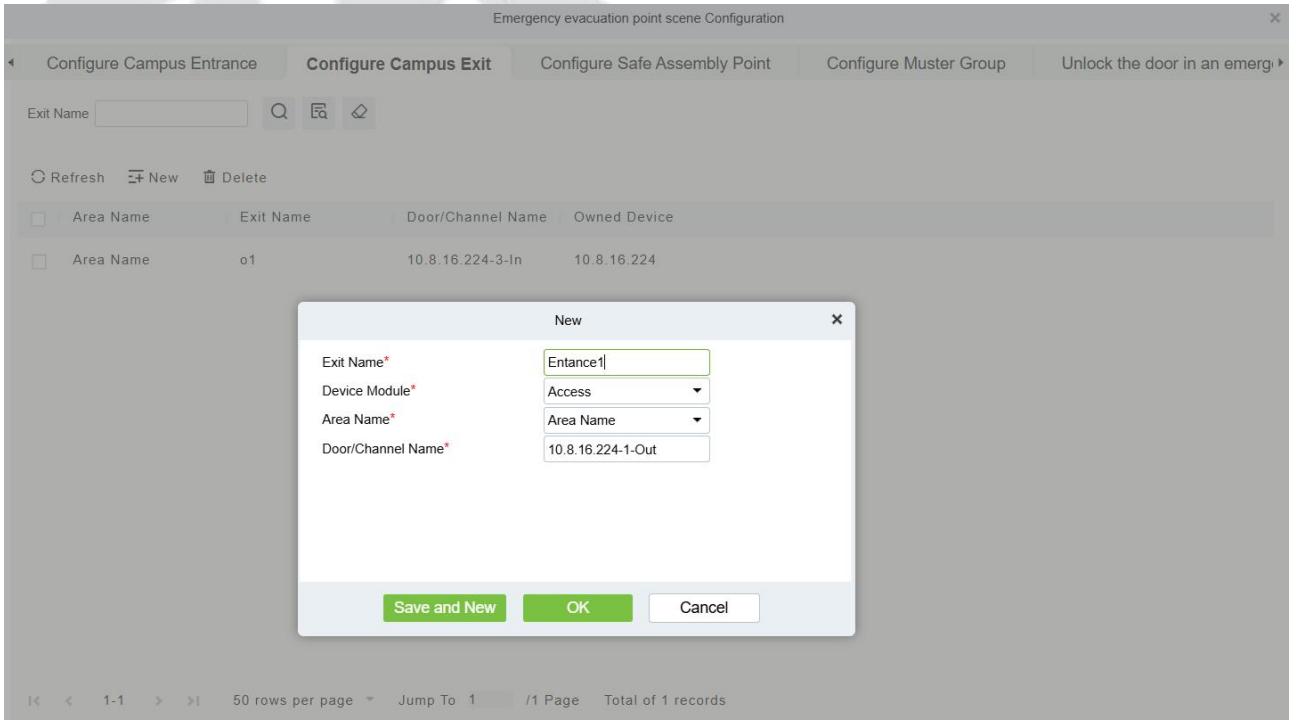


Figure 21- 51

The supported device modules include: Access , Entrance Control, and Parking.

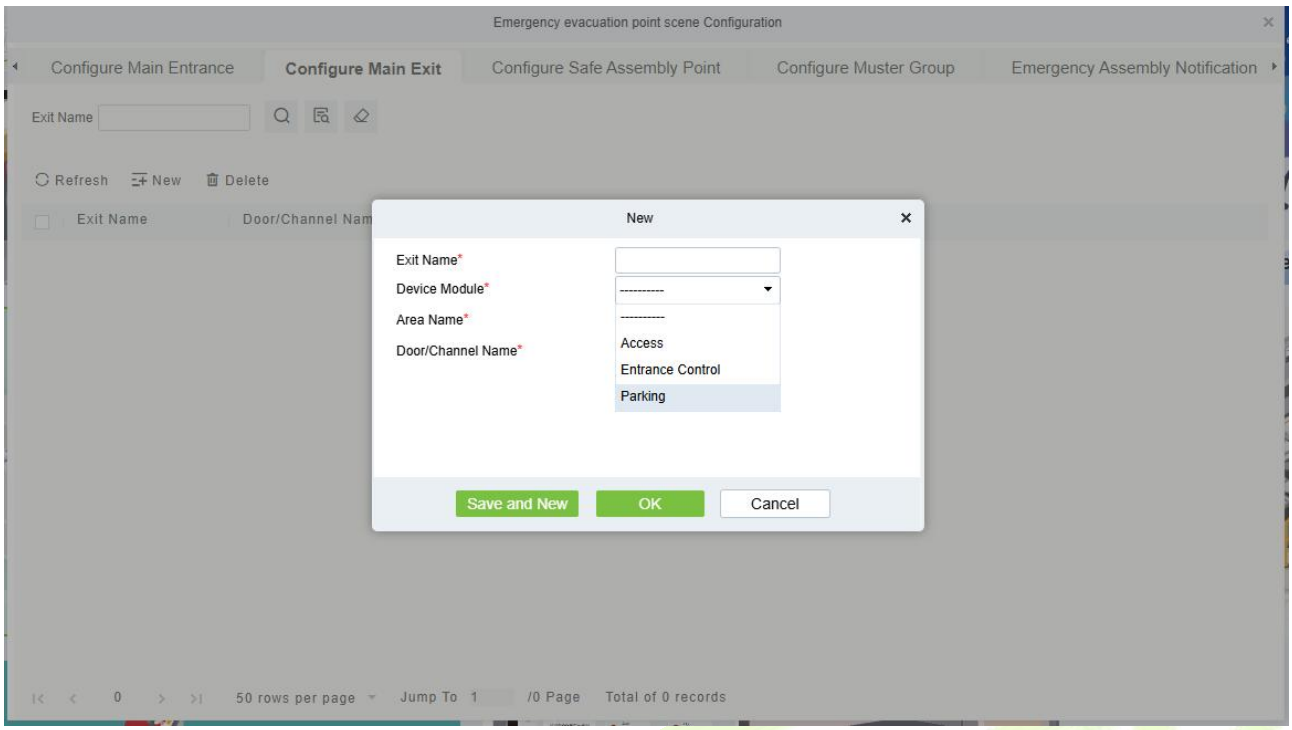


Figure 21- 52

Step 3: Configure Safe Assembly Point

This menu is used to configure the security point, and the equipment of the security point can take attendance of the assembled personnel in real time;

Security point support: access control equipment and face camera

Click **New** to select the device of the access control, channel or video module; when the personnel arrive at the security point, they need to verify the device of the corresponding security point for reporting the collection record. The verified personnel will be marked as "Assembled", otherwise, they will be marked as "Disassembled"

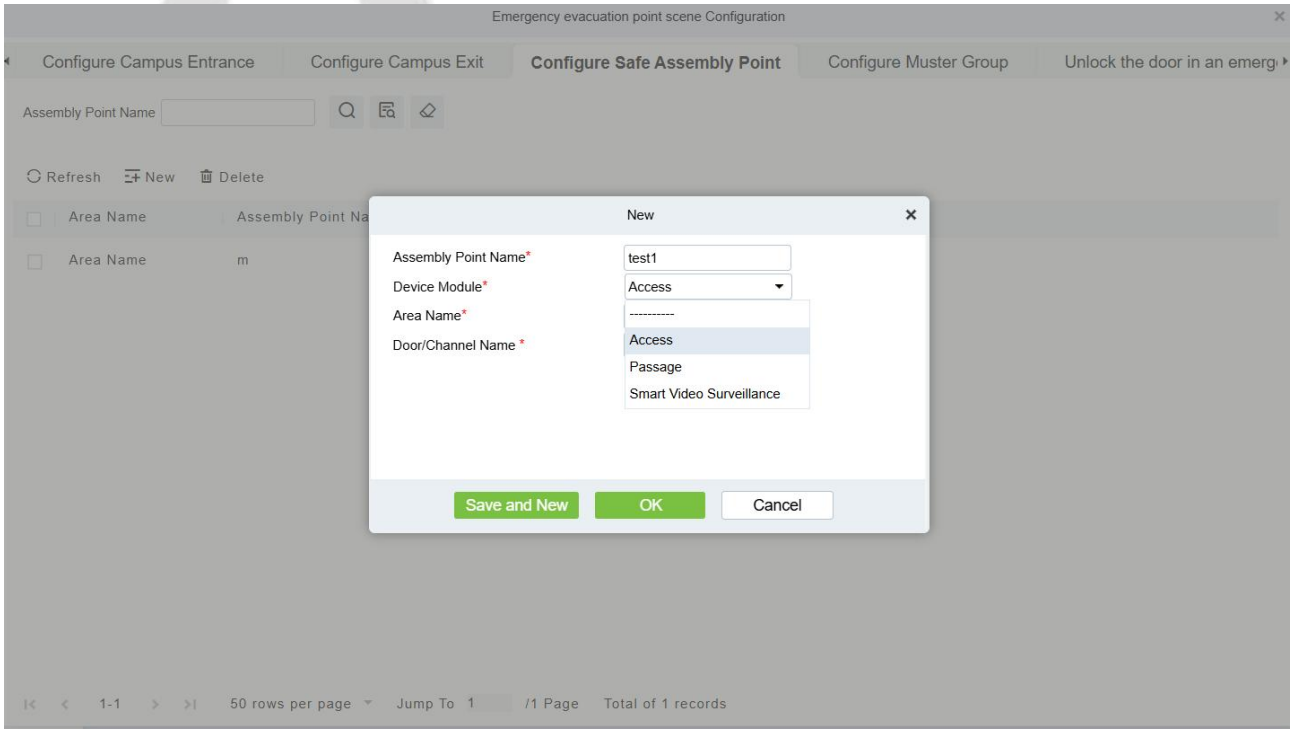


Figure 21- 53

Step 4: Configure Muster Group

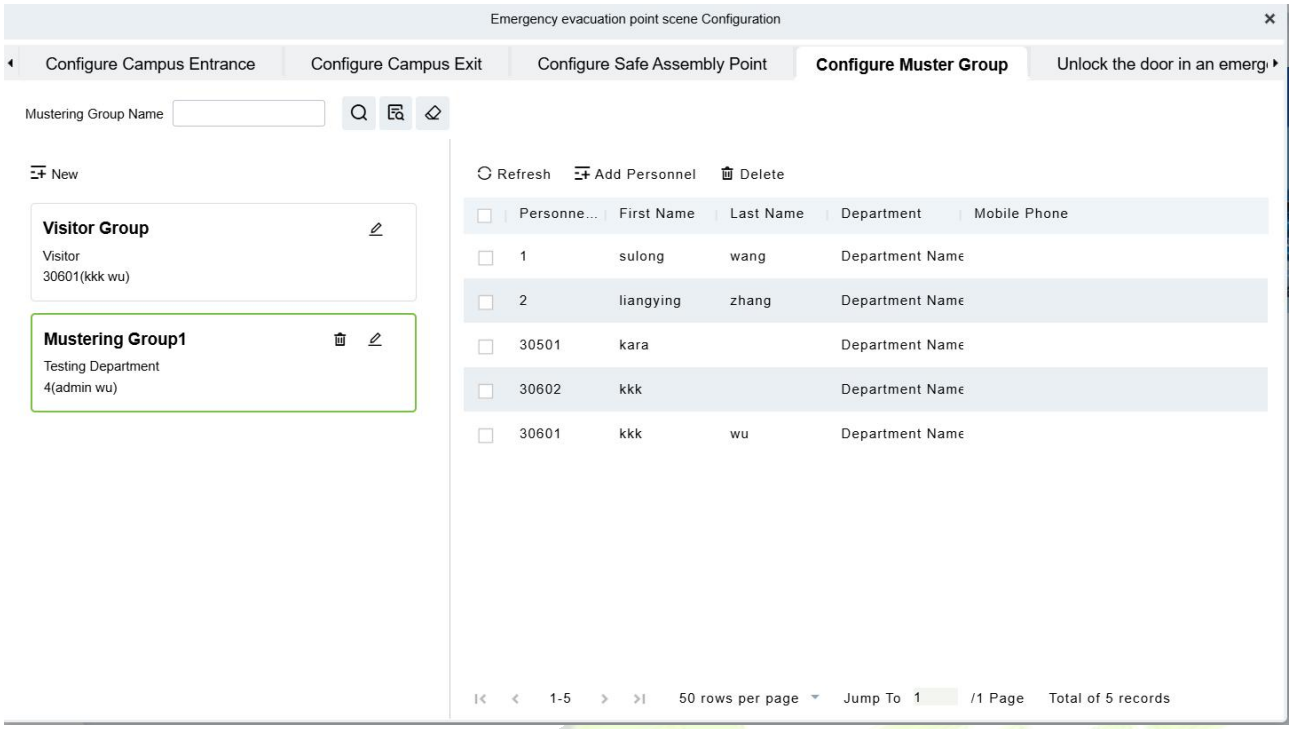


Figure 21- 54

Click **New** on the left to add a collection group

Mustering Group Name: Customize the group name

Remarks: Description of the set group

Group Administrator: Group administrator, used for offline secondary verification of the group list

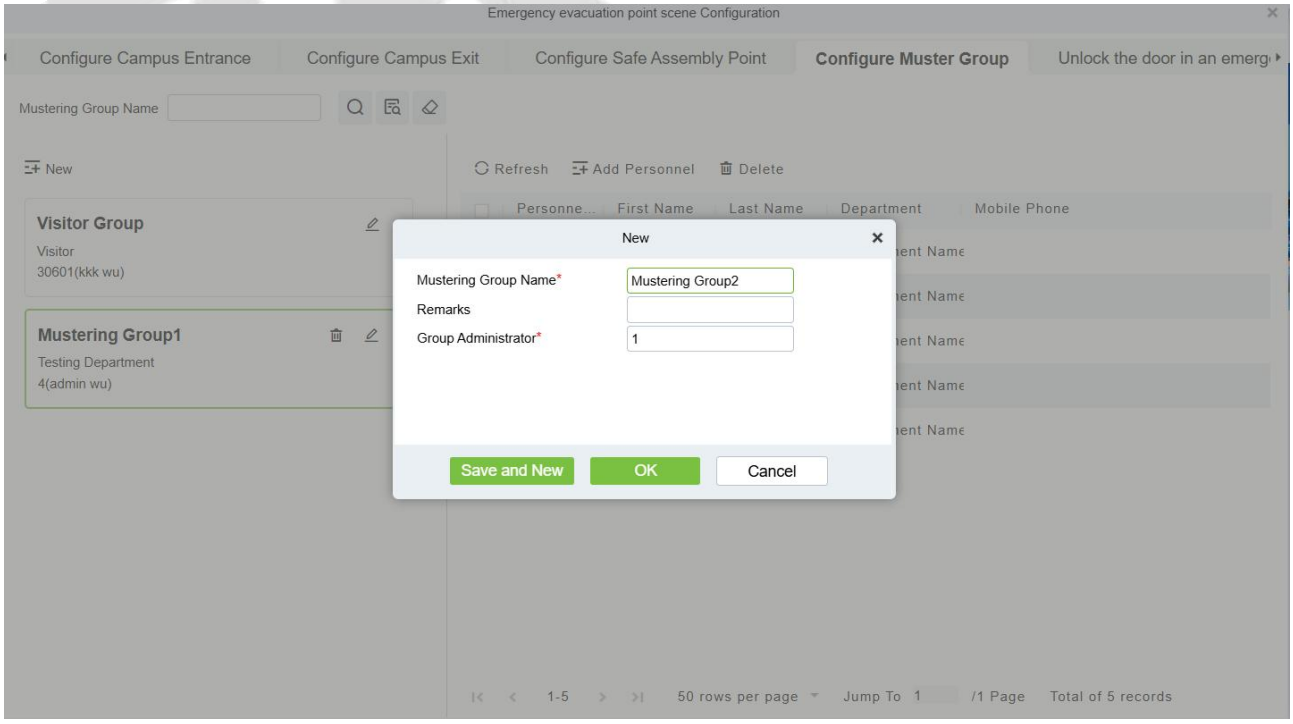


Figure 21- 55

Click **Add Personnel** on the right to add people to the group.

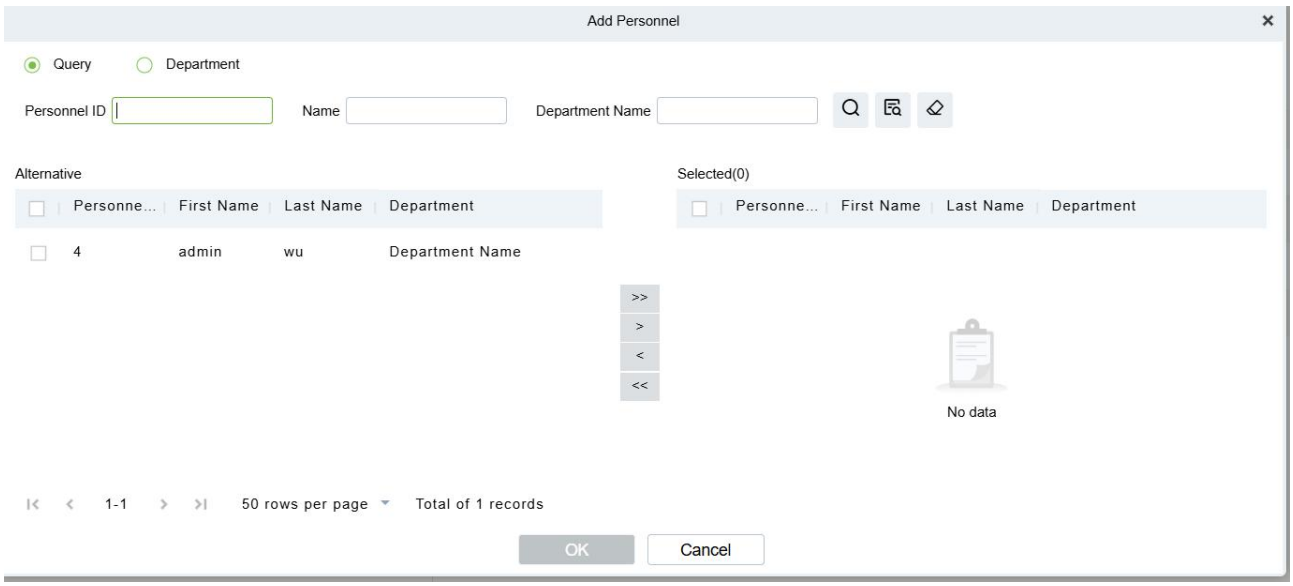


Figure 21- 56

Note: The visitor group will be used to count the visitors who have signed in but have not gone out in an emergency. You can add administrators to the visitor group; however, you cannot delete or add people to the visitor group.

Step 5: Emergency Assembly Notification

This menu is used to configure the message set.

Statistical Period: Used to configure the scope of statistical resources. For example, if 7 days are selected, the personnel and visitors who entered the building in the past 7 days but did not leave when an emergency was triggered will be counted.

Emergency Assembly Message Notification: Whether to enable the message notification function. If enabled, when the emergency assembly is activated, the assembly notification will be automatically sent to the people and visitors in the assembly group.

Notification Method: Message notification mode, can be Email, SMS, WhatsApp, APP.

Send Statistical Report: Whether the configuration sends statistical reports regularly

- **Send Periodically:** Whether to send regularly. After enabling, you can further configure the sending frequency.
- **Sending Frequency:** Optional sending frequency; if the configuration is 30min, then when the emergency assembly is activated, the system will send statistical reports to the corresponding personnel every 30 minutes
- **Send to Group Administrator:** After enabling, the statistical report will be automatically sent to each group administrator
- **Other Recipients:** You can configure the email address of other recipients.

Step 6:Emergency Evacuation Linkage

Click **Emergency Evacuation Linkage Configuration** in the operation wizard to jump to the linkage configuration page.

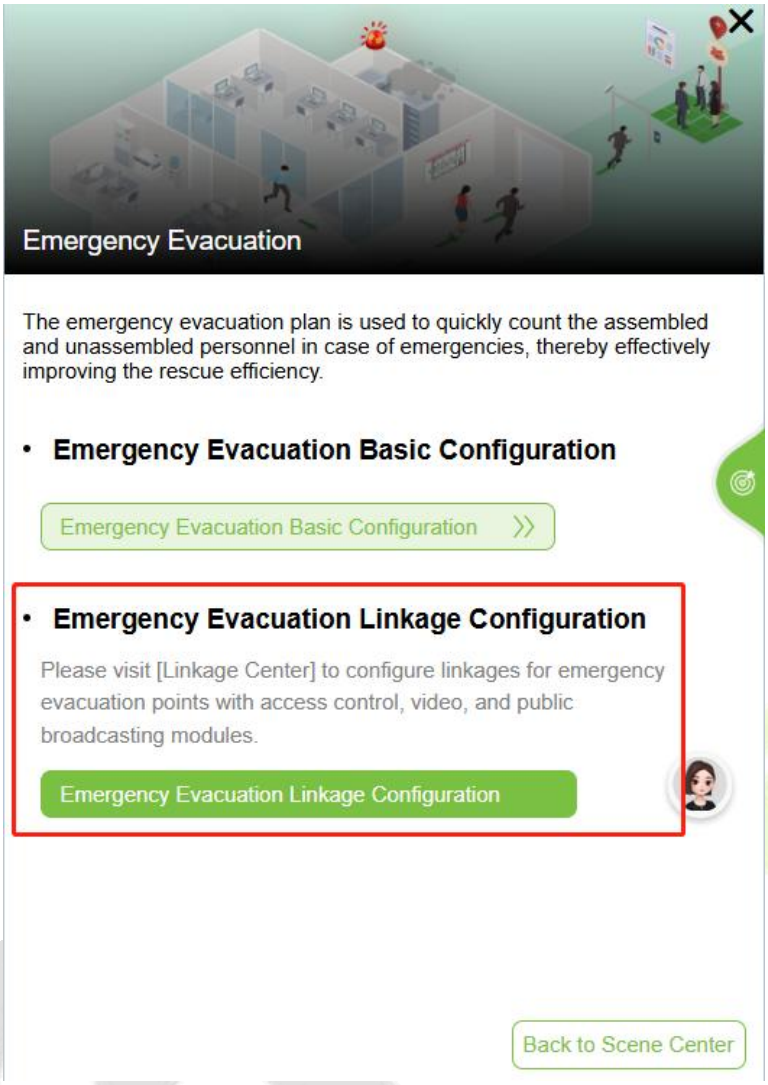


Figure 21- 57

Linkage Configuration->New, carry out linkage configuration as shown in the figure below. You can configure automatic linkage of fire door to open when smoke is detected; you can also configure linkage of broadcast to play escape guidance after Emergency Evacuation activation, as shown in the figure below:

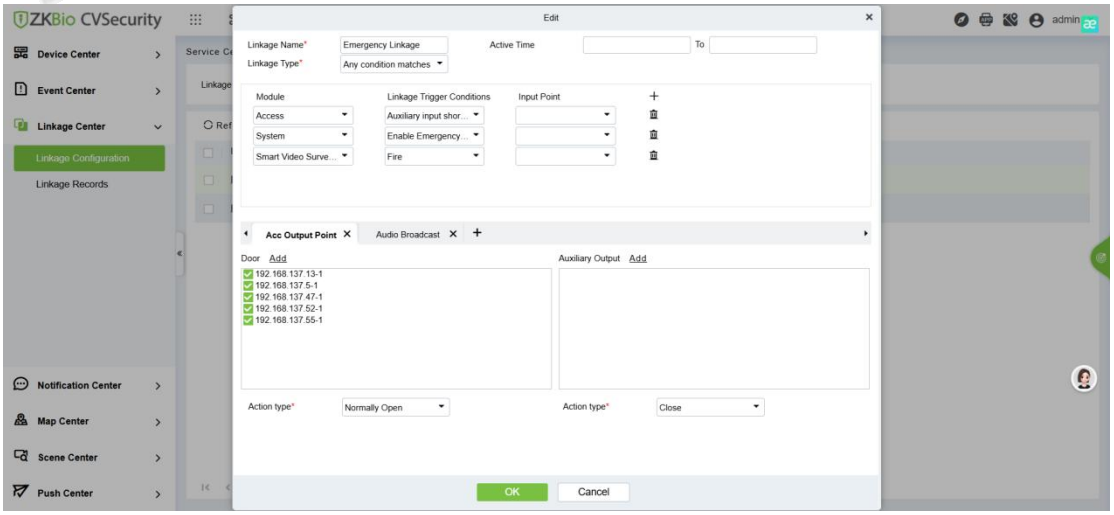


Figure 21- 58

Result verification:

When a fire drill or emergency such as a fire occurs, the system administrator can manually click Enter Scene,

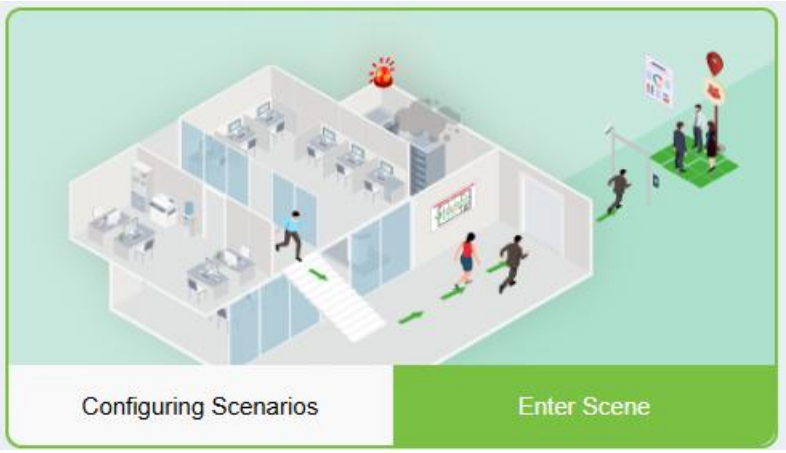


Figure 21- 59

➢Start Emergency Roll Call

To enter the following page, click Start Emergency Roll Call,

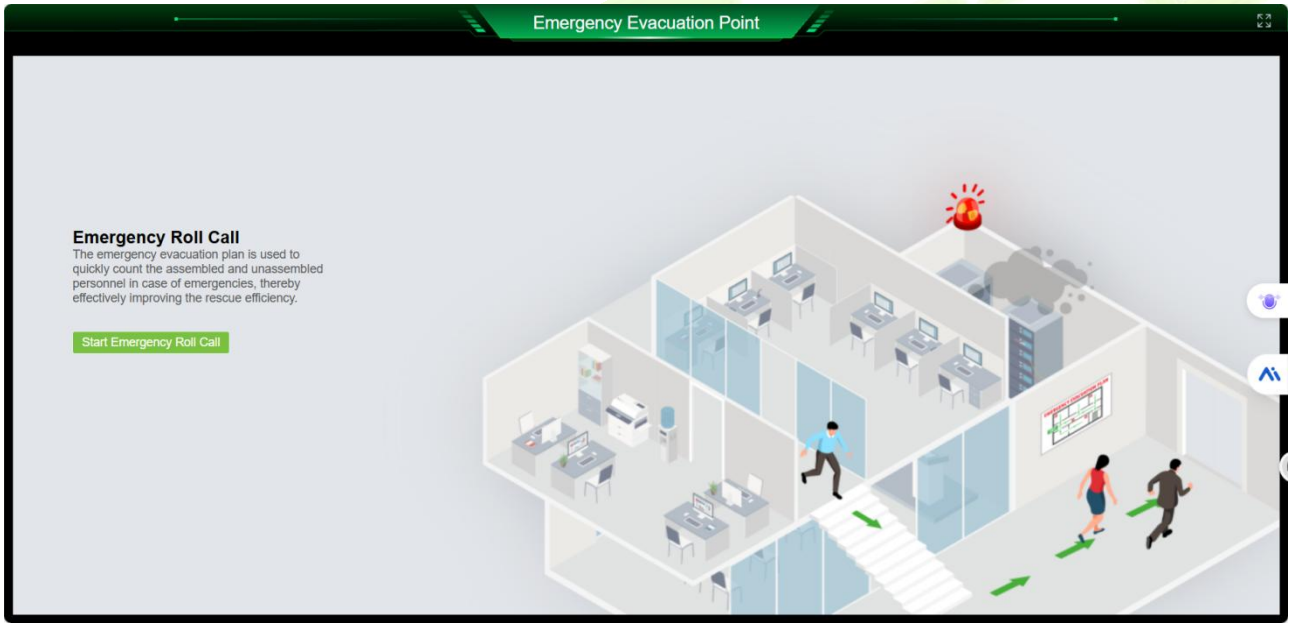


Figure 21- 60

Enter the real-time statistics interface to view, as shown in the following figure:

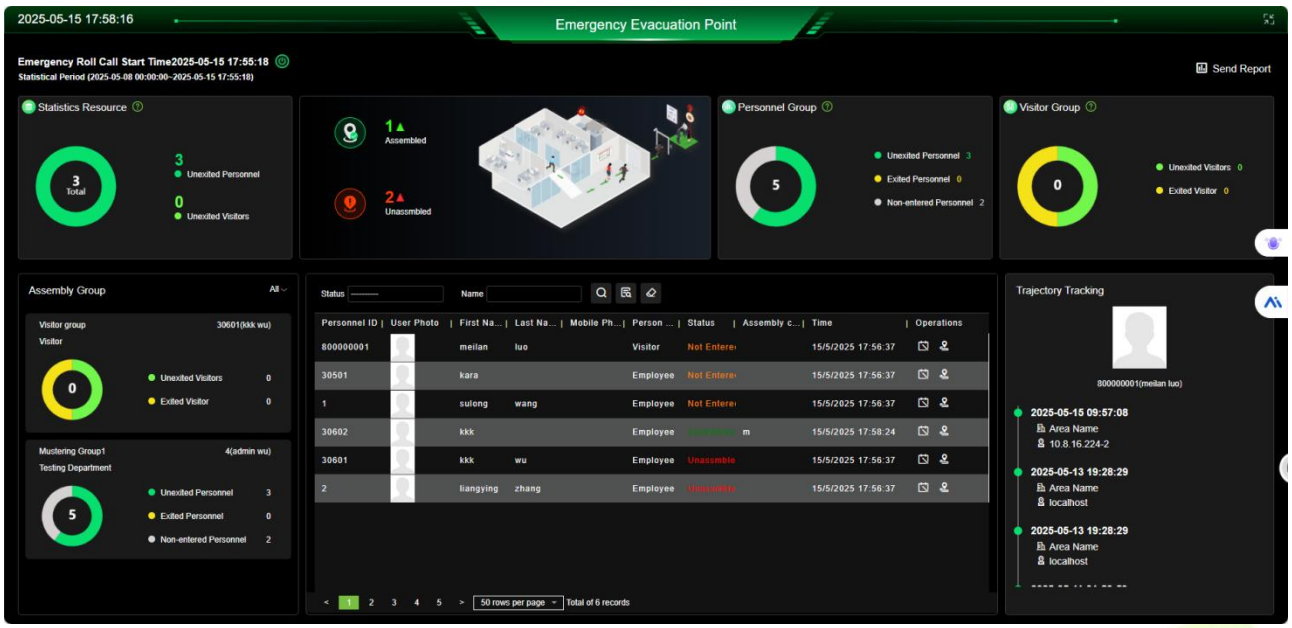
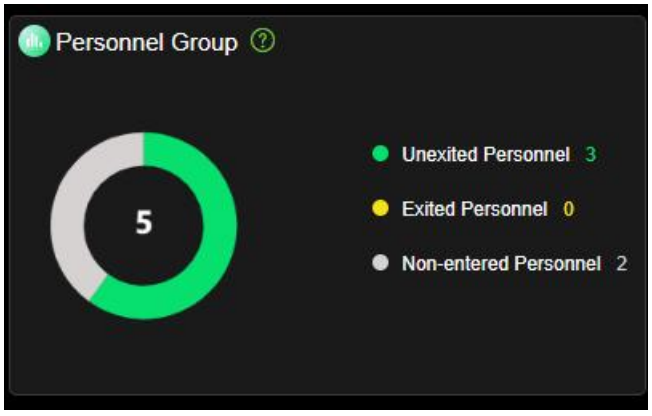


Figure 21- 61

Parameter	Description
	● Show the start time of the roll call ● The statistical period refers to the statistical scope of the configuration. For example, if the configuration is 7 days, the statistics start to urgently collect data from the past 7 days
	Statistical resources: refers to all the people and visitors who enter the country during the statistical period
	Display all collected and uncollected data; The sum of statistical resources = collected + not collected
	Display the data of all personnel groups during the statistical period. Personnel group = incoming personnel + outgoing personnel + not entered personnel

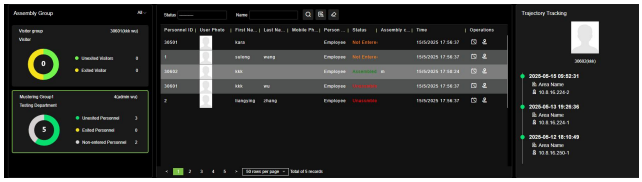
Parameter	Description
	Display visitor data for the statistical period Visitor group = visitors who have entered but not gone out + visitors who have gone out
	Display detailed data for each set

Table 21- 3 Parameters

Clicking on a set group on the left will automatically filter and display the details of the personnel set group; the status in the list includes: already set, not set, not out, already out, not in state.

- **Trajectory tracking:** The administrator can quickly screen the uncollected personnel, click the icon to view the trajectory of the person, and quickly learn the last location of the person to improve the rescue efficiency

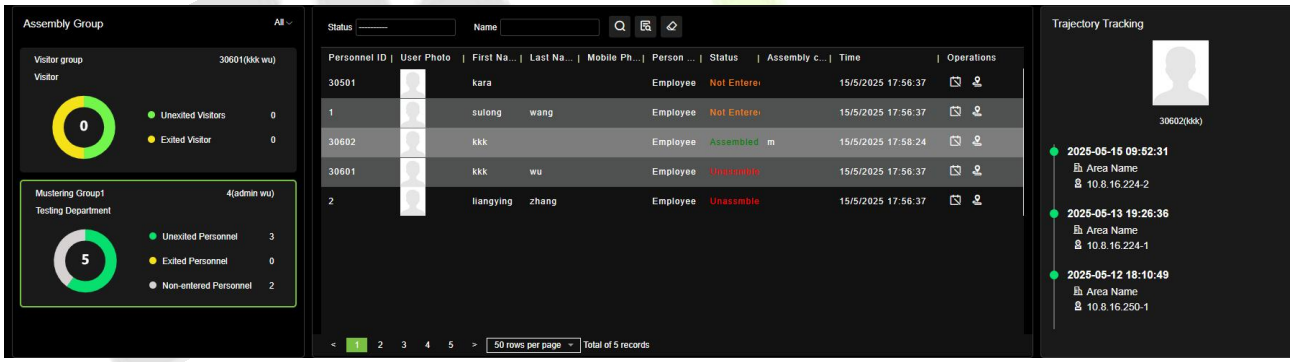


Figure 21- 62

- **Manual check-in:** If someone has been in the safe point but not in the device verification, the administrator can manually click the button to check in the person. If the person enters the dangerous area after gathering, the administrator can also change the gathering status of this person again

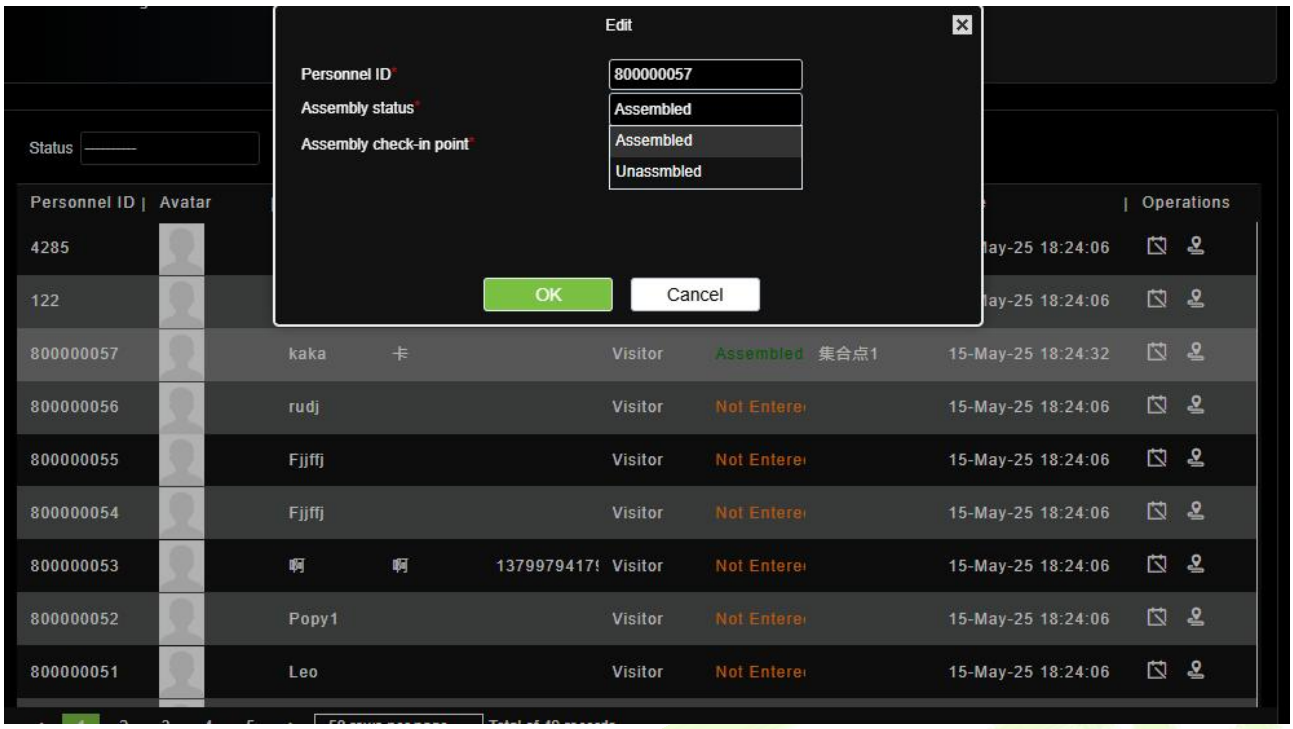


Figure 21- 63

➢Message notification

After Start Emergency Roll Call, the system will automatically send a collection message to the group members and visitors, as shown in the following figure:

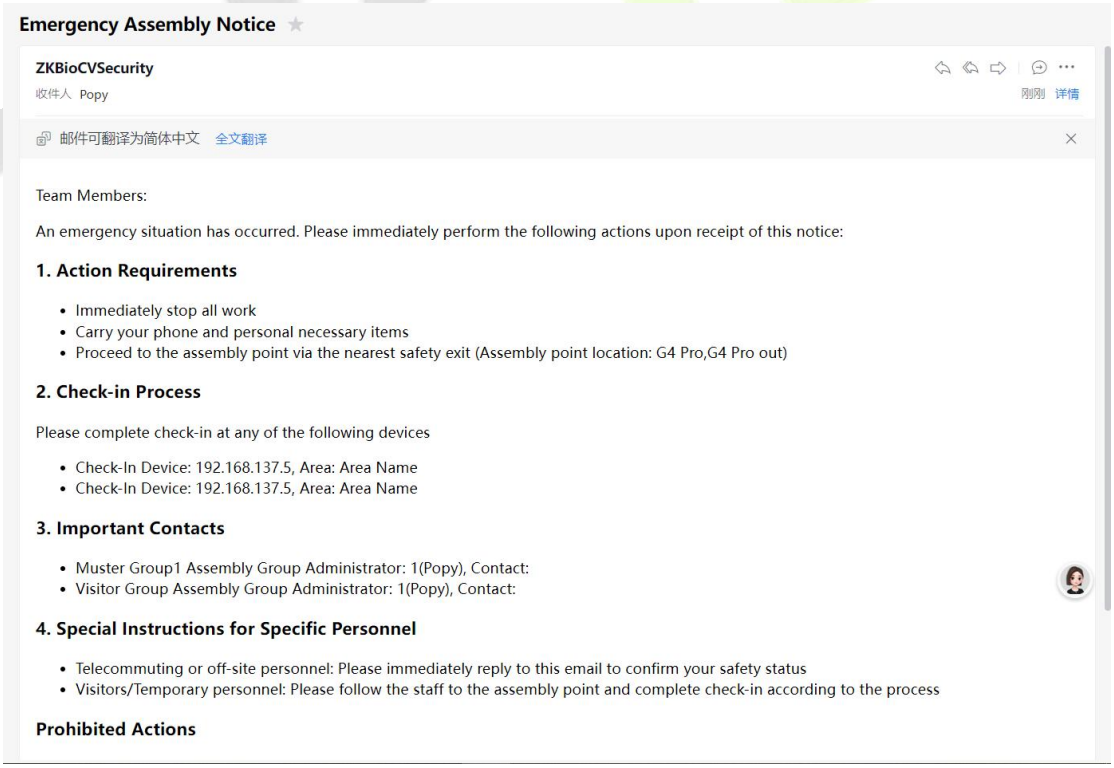


Figure 21- 64

➢Trigger linkage

If the emergency assembly joint has been configured in advance, the corresponding actions will be output. For example, the broadcast will convert the text of escape guidance into voice playback, and the voice guide personnel will escape; or the escape channel can be linked to open, so as to facilitate escape.

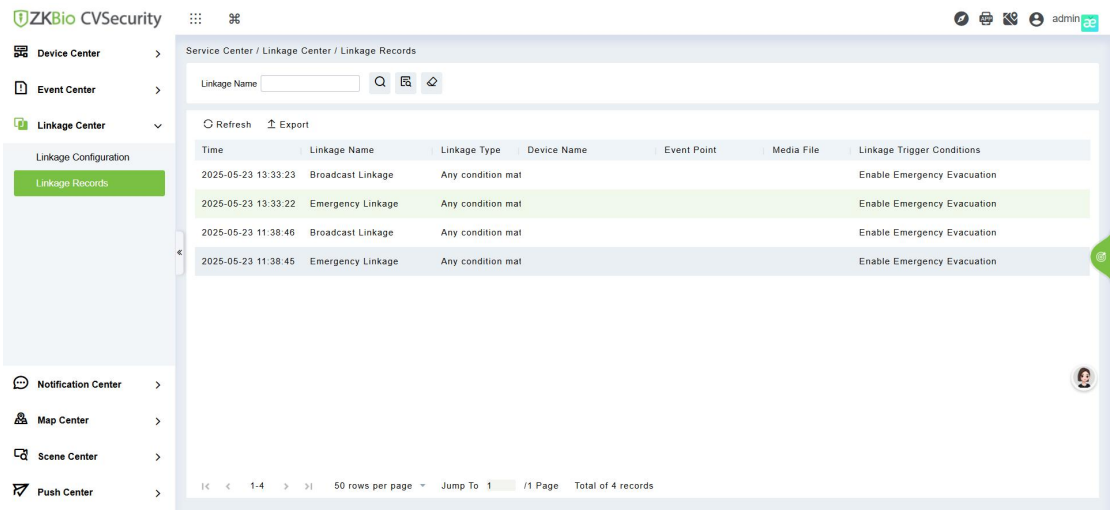


Figure 21- 65

➢End Emergency Roll Call

If the danger is removed, the administrator can end the emergency assembly state.

Click the one in  the upper left corner to pop up the following dialog box.

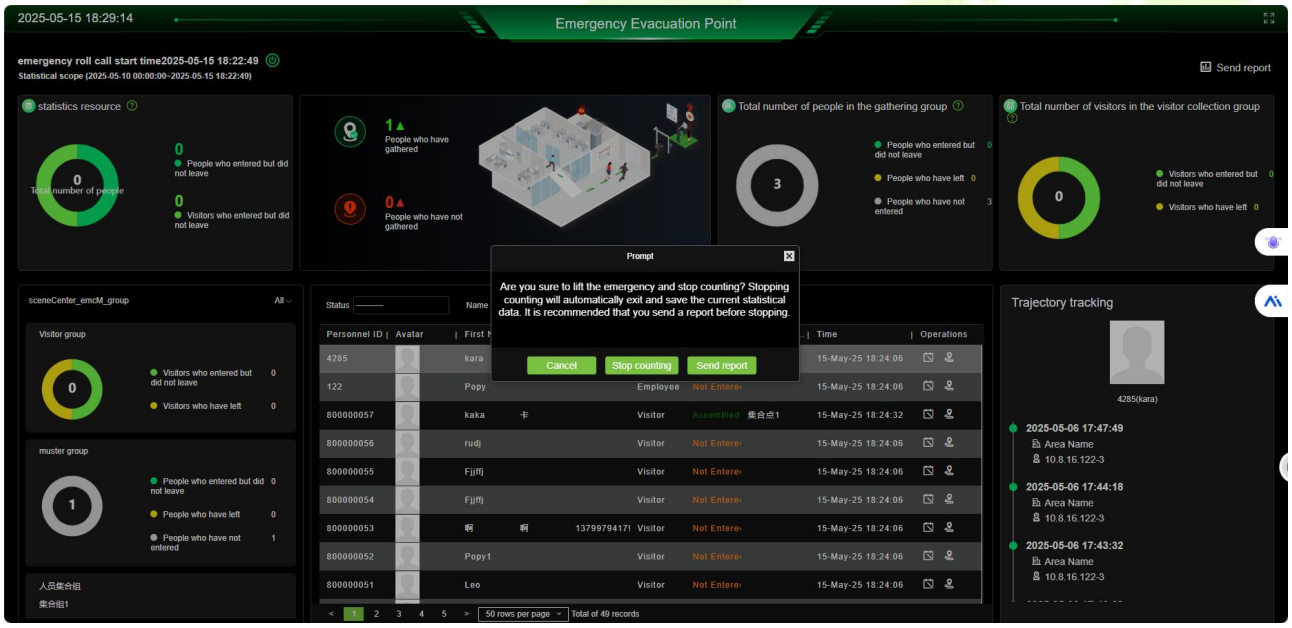


Figure 21- 66

- **Cancel**

Cancel this operation, click to continue to stay on the emergency roll call page

- **Stop Counting**

To end the emergency assembly state, click this button to clear the statistics of this session and return to the previous page

- **Send Report**

After clicking, the final statistical report will be sent to the person in charge and the recipient.

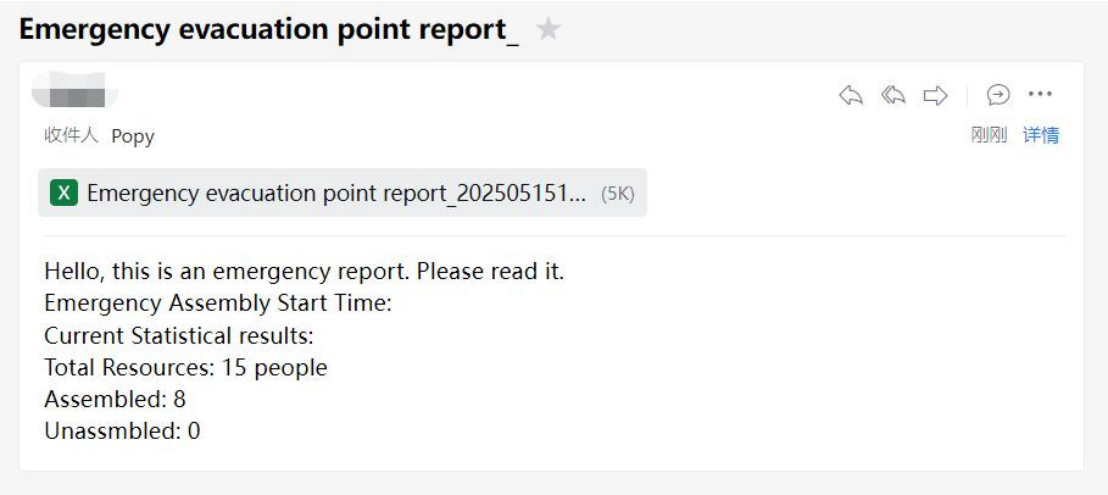
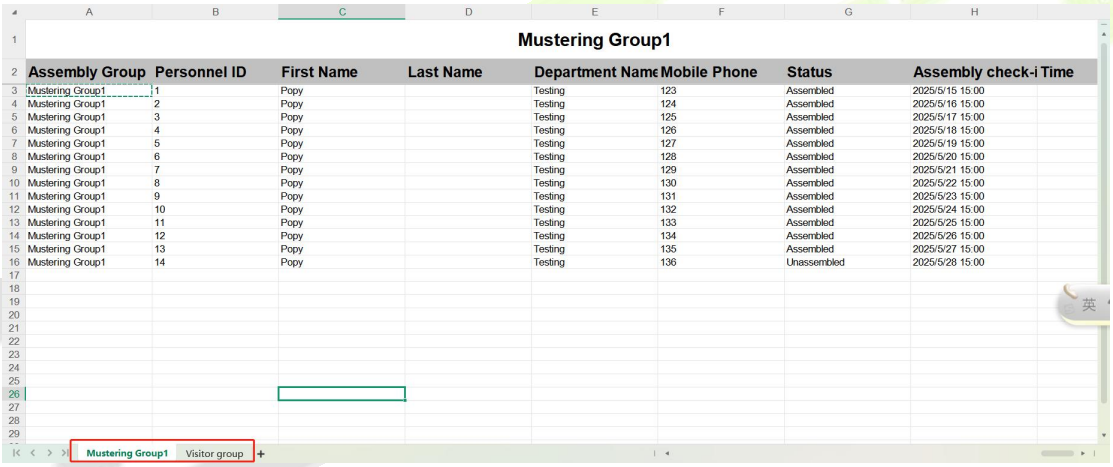


Figure 21- 67

The group administrator can open the attachment report to facilitate the offline secondary verification of the gathering situation of personnel. For the personnel who are already at the security point but whose status is "not gathered", they can sign in manually or let them verify on the equipment at the gathering point; they can also quickly contact the uncollected personnel through the mobile phone number on the report.



Mustering Group1

Assembly Group	Personnel ID	First Name	Last Name	Department Name	Mobile Phone	Status	Assembly check-i Time
Mustering Group1	1	Popy		Testing	123	Assembled	2025/5/15 15:00
Mustering Group1	2	Popy		Testing	124	Assembled	2025/5/16 15:00
Mustering Group1	3	Popy		Testing	125	Assembled	2025/5/17 15:00
Mustering Group1	4	Popy		Testing	126	Assembled	2025/5/18 15:00
Mustering Group1	5	Popy		Testing	127	Assembled	2025/5/19 15:00
Mustering Group1	6	Popy		Testing	128	Assembled	2025/5/20 15:00
Mustering Group1	7	Popy		Testing	129	Assembled	2025/5/21 15:00
Mustering Group1	8	Popy		Testing	130	Assembled	2025/5/22 15:00
Mustering Group1	9	Popy		Testing	131	Assembled	2025/5/23 15:00
Mustering Group1	10	Popy		Testing	132	Assembled	2025/5/24 15:00
Mustering Group1	11	Popy		Testing	133	Assembled	2025/5/25 15:00
Mustering Group1	12	Popy		Testing	134	Assembled	2025/5/26 15:00
Mustering Group1	13	Popy		Testing	135	Assembled	2025/5/27 15:00
Mustering Group1	14	Popy		Testing	136	Unassembled	2025/5/28 15:00

Figure 21- 68

21.6.5Transparent Kitchen

Hardware Supported : ZKIVA-Edge X1

Click **Configuring Scenarios** into Transparent Kitchen Guide:

Figure 21- 69

✍ **Note:** Currently, only ZKIVA-Edge X1 supports the work safety algorithm. Please purchase the algorithm and configure intelligent channels on the ZKIVA-Edge X1 web page.

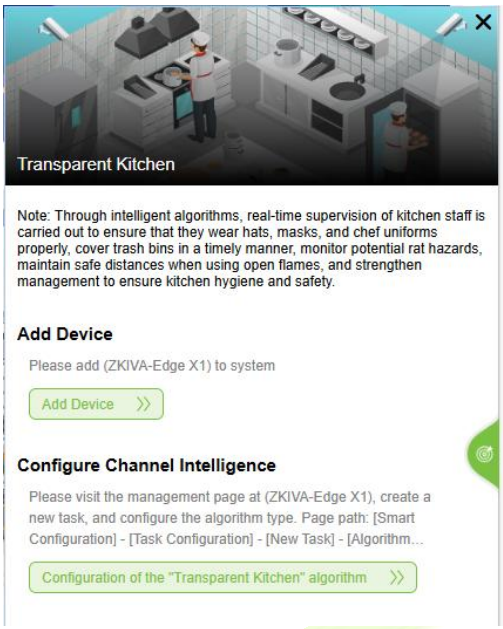


Figure 21- 70

● **Operation Step**

Step1: Add Device

Click **Add Device**, the system will automatically jump to **[Smart Video Surveillance]** > **[Device Management]** > **[Device]**, you can add ZKIVA-Edge X1 devices here, and you can refer 5.1 Device Management for specific operation.

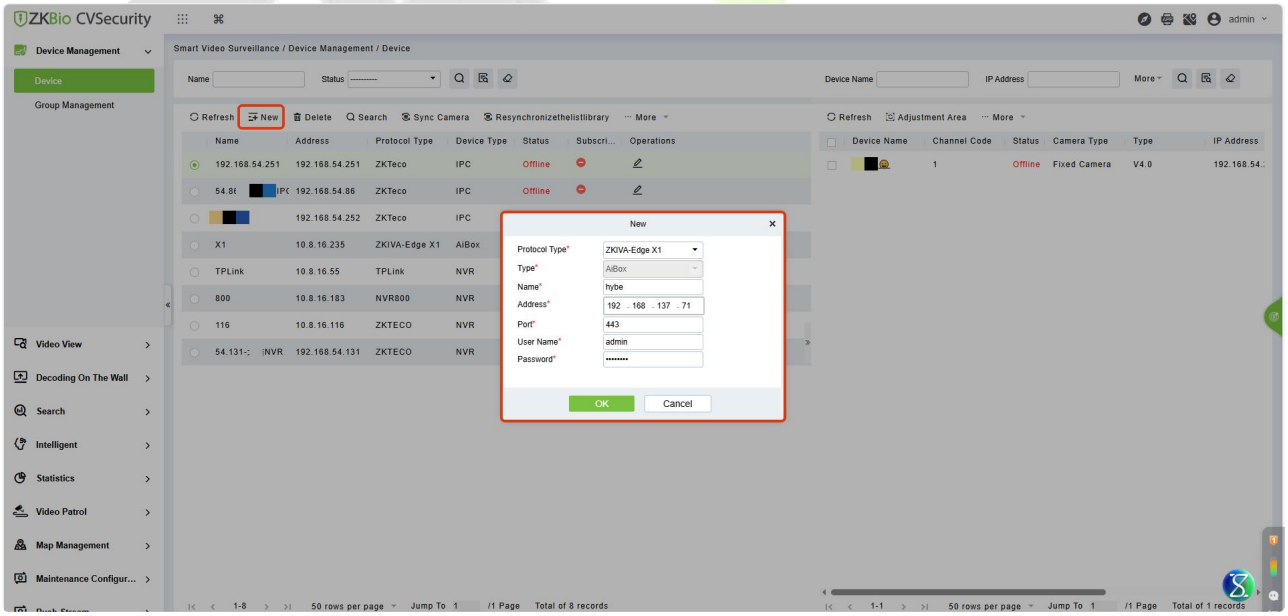


Figure 21- 71

Step 2: Configure Channel Intelligent

The algorithm configuration feature is now moved to the web side of the device, Please visit the ZKIVA-Edge X1 web management page, select the channel, and configure face intelligence.

1. Click Configure Channel Intelligent to jump to [Smart Video Surveillance]>[Device Management] > [Device].
2. Click [Smart Video Surveillance]>[Device Management]>[Device]>[Maintenance Management] to

jump to device web management page.

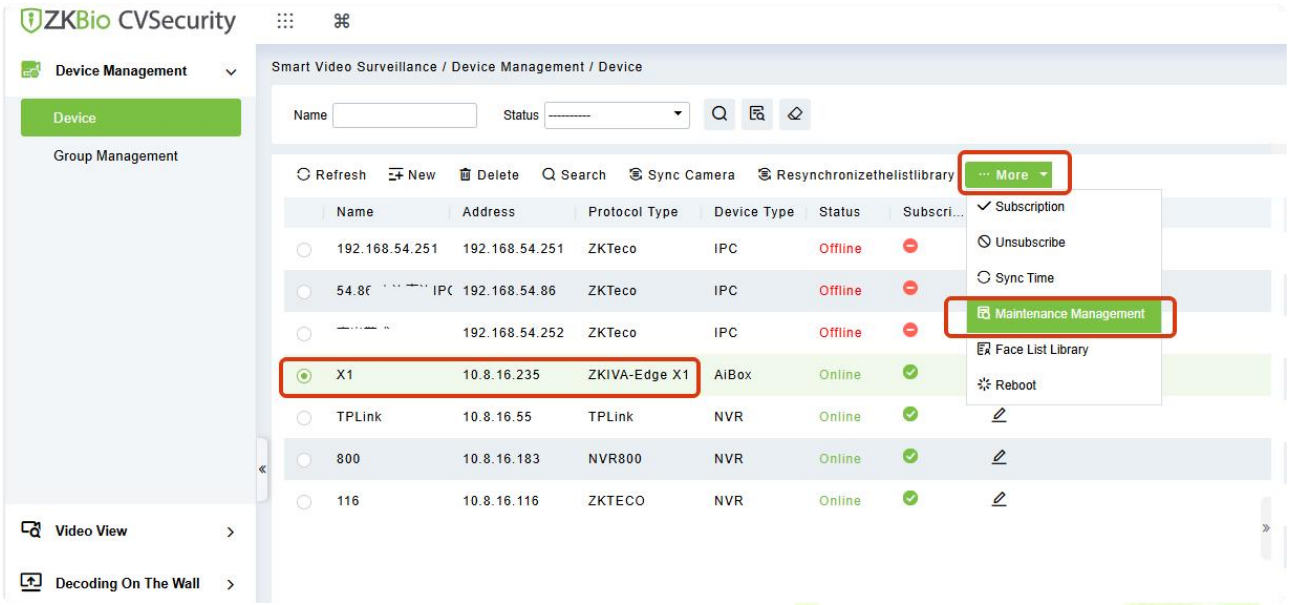


Figure 21- 72

Please visit the management page (ZKIVA-Edge X1), create a new task and configure the algorithm type. Page path: [Intelligent Config] - [Task Config] - [New Task] - [Algorithm Config], and select transparent kitchen related algorithms.

1. Click [Setting]>[Task Setting] to add a new task.

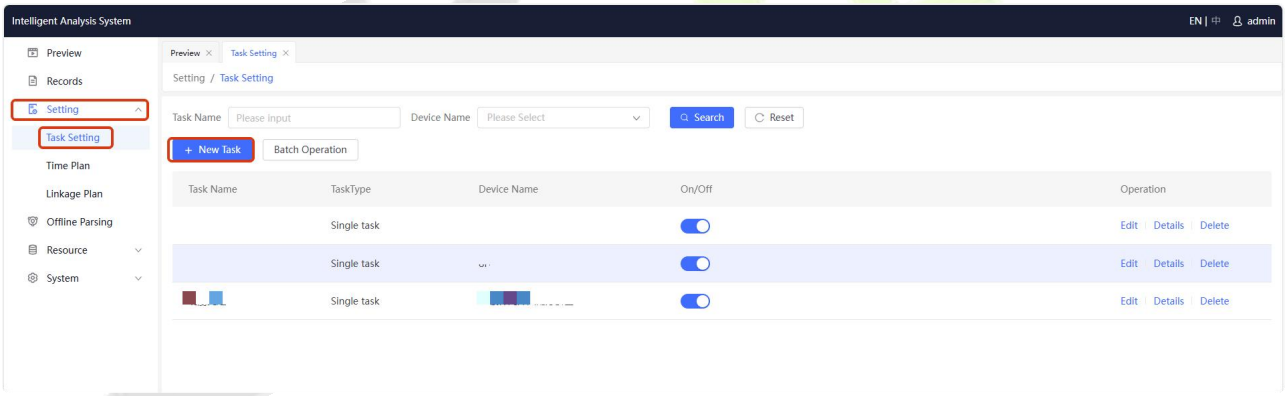


Figure 21- 73

2. Perform basic configuration, and then click Submit.

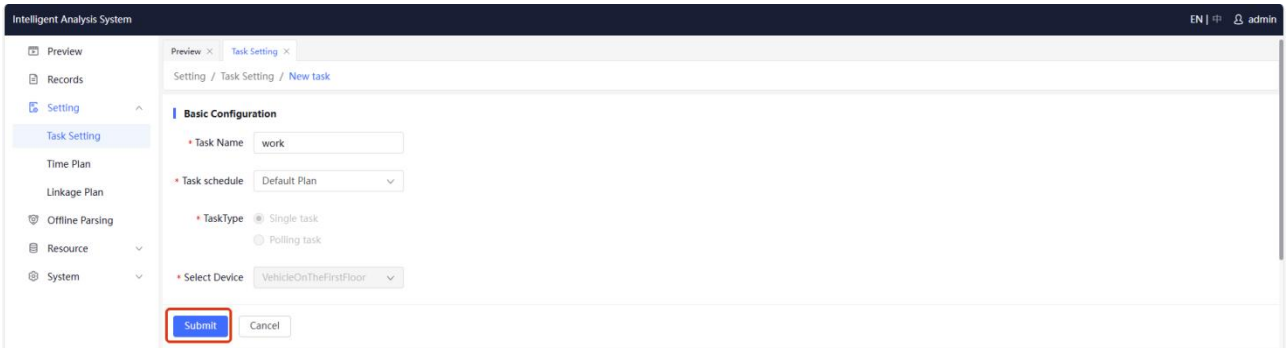


Figure 21- 74

3. After submit the basic setting, click [Drawing Area] to draw the monitoring area.

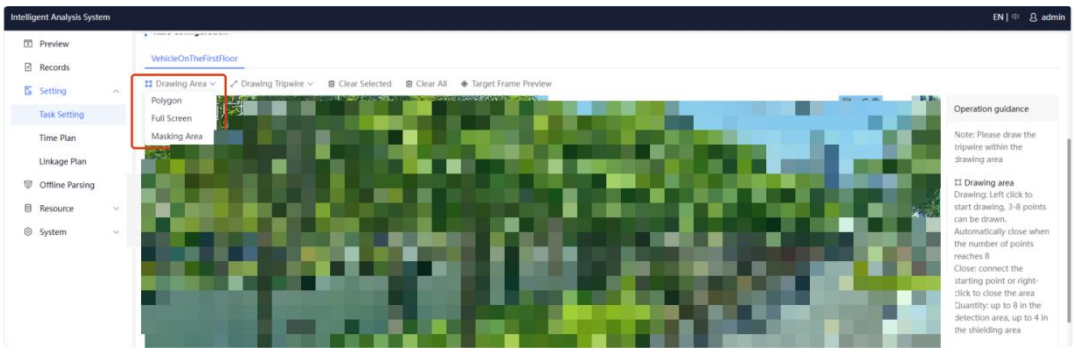


Figure 21- 75

4. Select the configured algorithm and submit it.

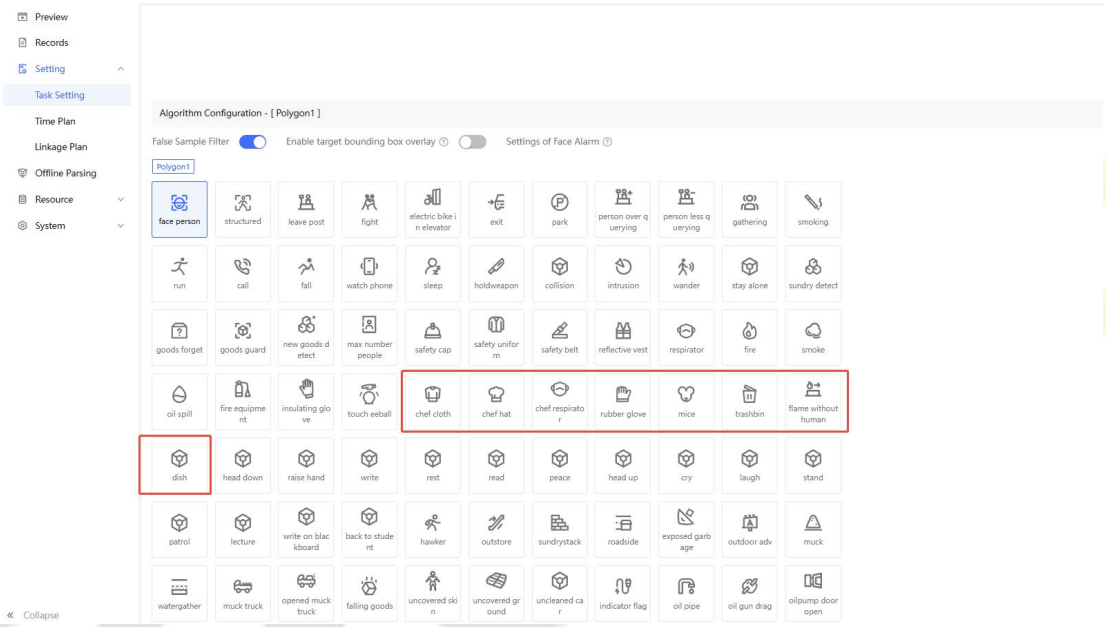


Figure 21- 76

● Scene Page

Click **Enter Scene** to enter the transparent kitchen function.

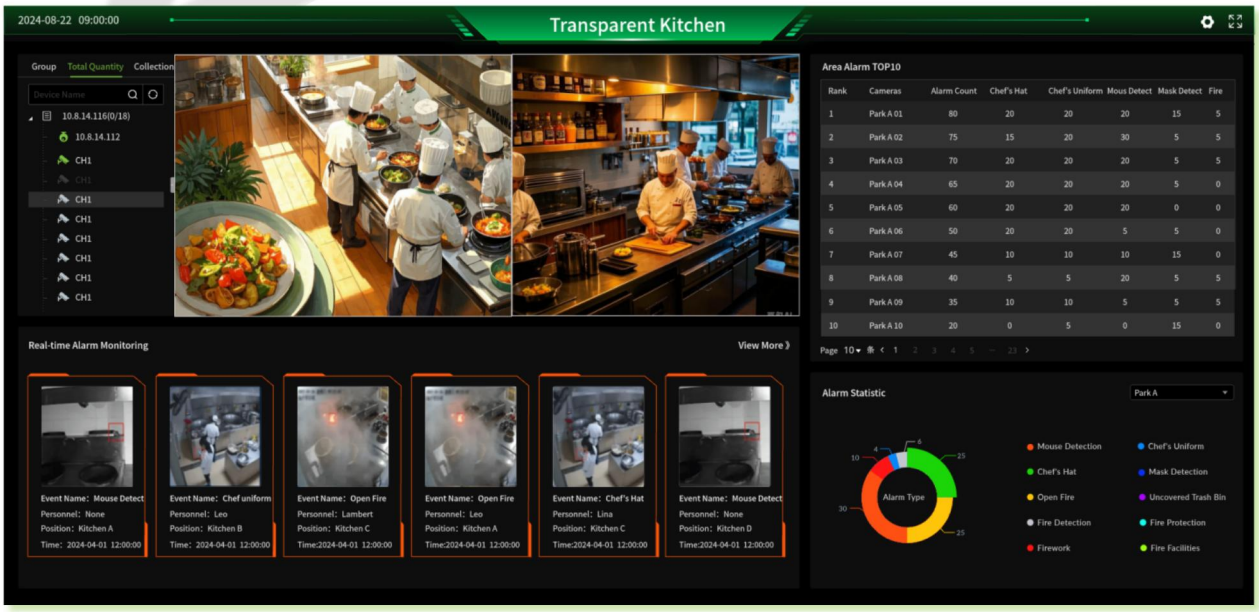


Figure 21- 77

21.6.6Work Safety

Hardware Supported : ZKIVA-Edge X1

Click **Configuring Scenarios** into Work Safety Guide:

Figure 21- 78

✍ **Note:** Currently, only ZKIVA-Edge X1 supports the work safety algorithm. Please purchase the algorithm and configure intelligent channels on the ZKIVA-Edge X1 web page.

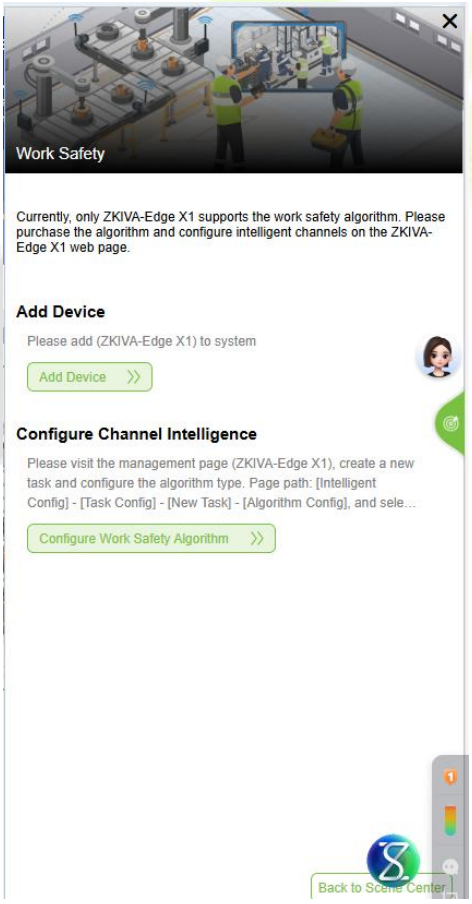


Figure 21- 79

● **Operation Step**

Step1: Add Device

Click **Add Device**, the system will automatically jump to **[Smart Video Surveillance]** > **[Device Management]** > **[Device]**, you can add ZKIVA-Edge X1 devices here, and you can refer 5.1 Device Management for specific operation.

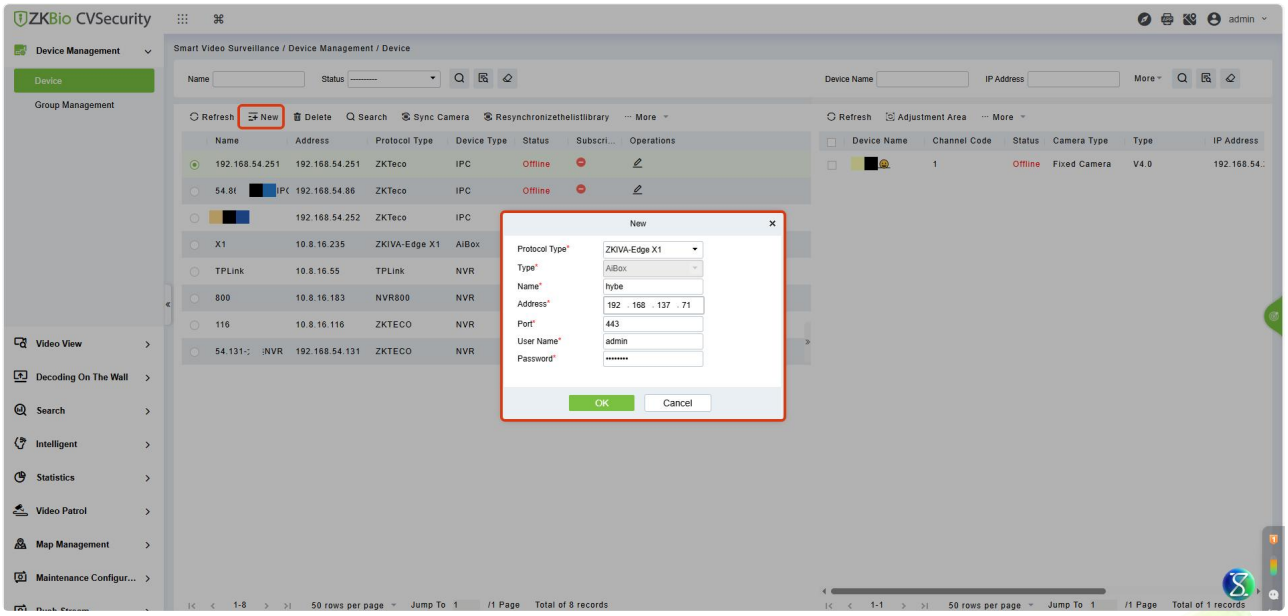


Figure 21- 80

Step 2: Configure Channel Intelligent

The algorithm configuration feature is now moved to the web side of the device, Please visit the ZKIVA-Edge X1 web management page, select the channel, and configure face intelligence.

1. Click Configure Channel Intelligent to jump to [Smart Video Surveillance]>[Device Management] > [Device].
2. Click [Smart Video Surveillance]>[Device Management]>[Device]>[Maintenance Management] to jump to device web management page.

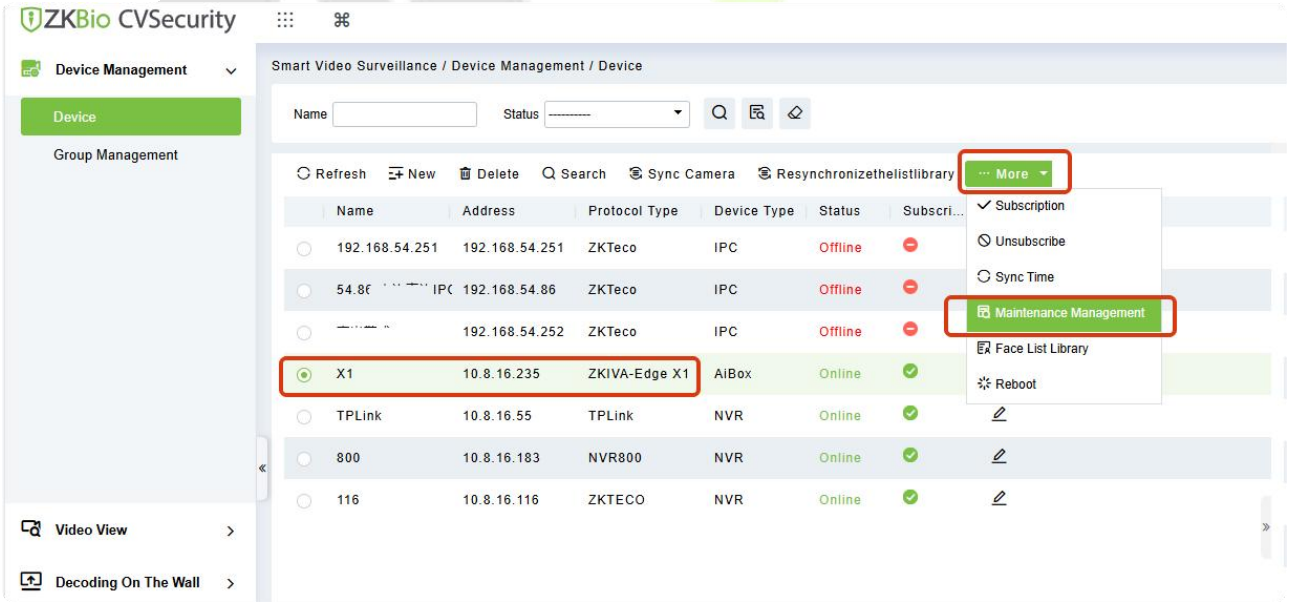


Figure 21- 81

Please visit the management page (ZKIVA-Edge X1), create a new task and configure the algorithm type. Page path: [Intelligent Config] - [Task Config] - [New Task] - [Algorithm Config], and select work safety related algorithms.

1. Click [Setting]>[Task Setting] to add a new task.

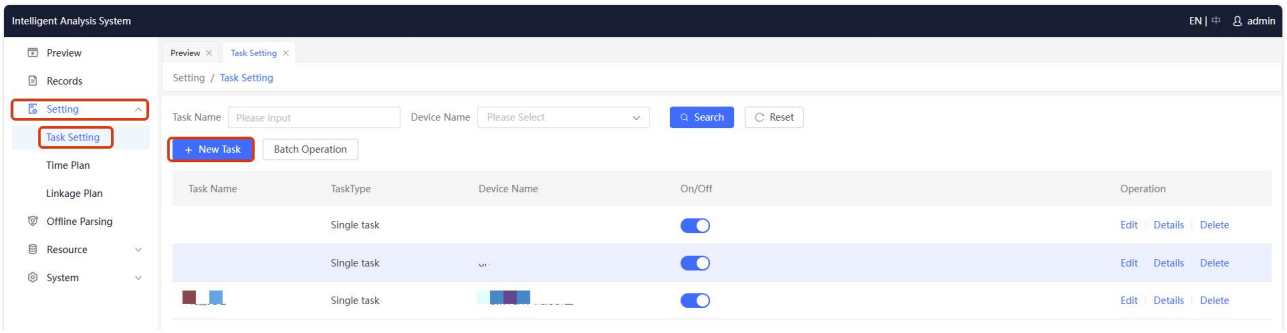


Figure 21- 82

2. Perform basic configuration, and then click Submit.

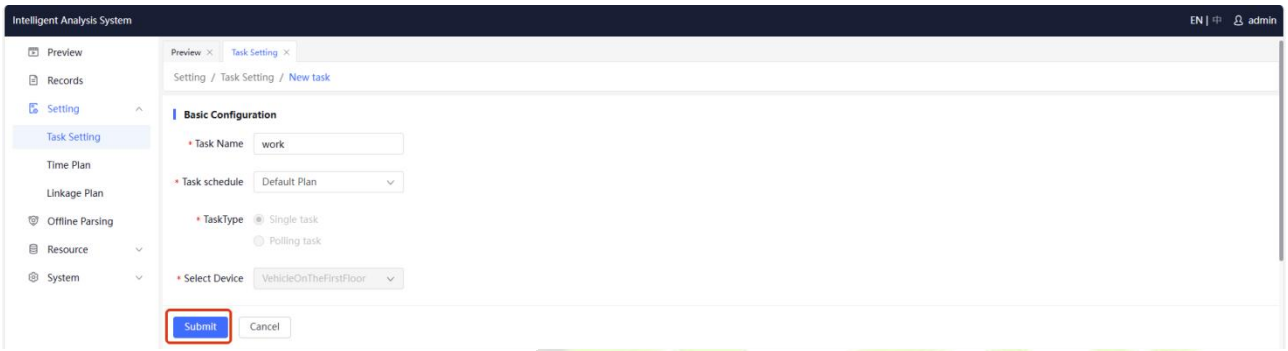


Figure 21- 83

3. After submit the basic setting, click [Drawing Area] to draw the monitoring area.

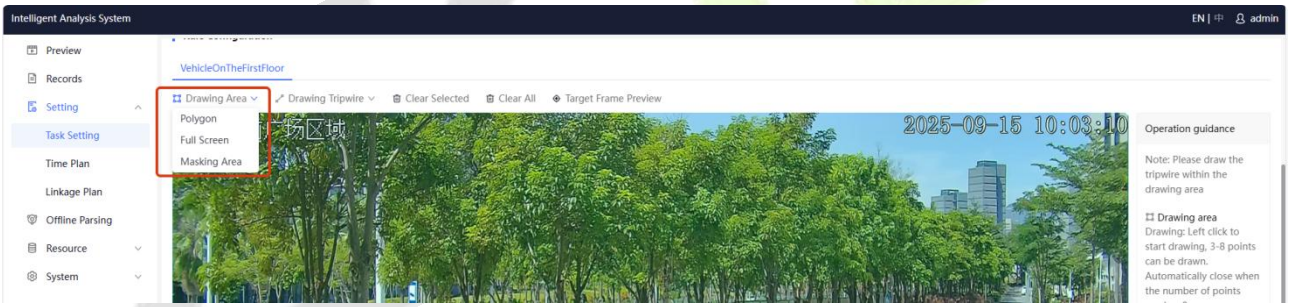


Figure 21- 84

4. Select the configured algorithm and submit it.

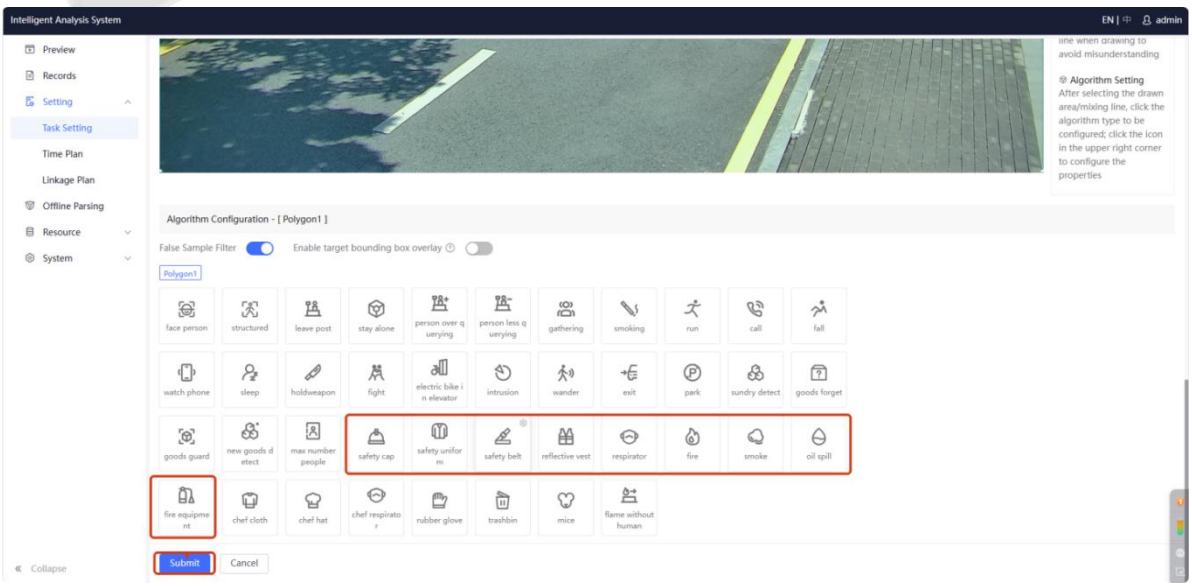


Figure 21- 85

●Scene Page

Click **Enter Scene** to enter the work safety function.

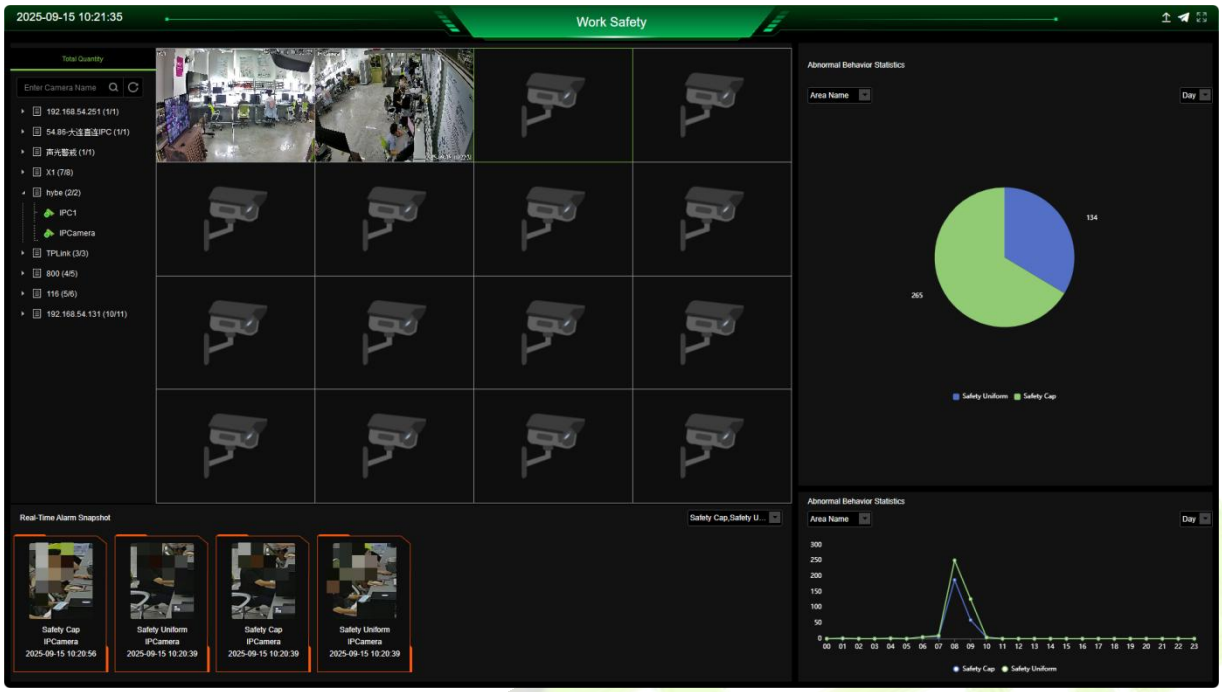


Figure 21- 86

●Export report

Click the export icon in the upper right corner, then select the desired time range for the report, as shown in the figure below:

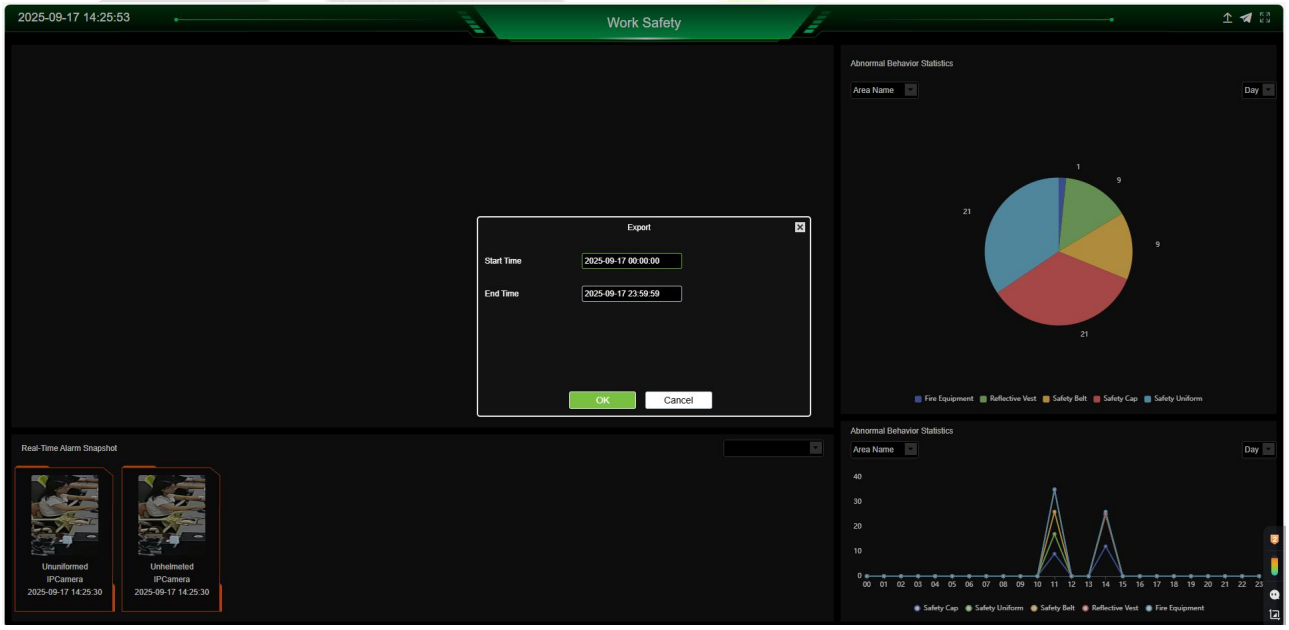


Figure 21- 87

The exported report records are shown in the figure below:

Work Safety Abnormal Behavior Report

Event Name	Event Source	Area	Event Level	Event Time	Processing State	Processor	Processing Remark
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:26:19	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:26:19	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:26:02	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:26:02	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:25:48	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:25:48	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:25:30	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:25:30	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:24:26	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:24:26	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:24:14	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:24:14	Unconfirmed		
Fire Equipment	IPCamera	Area Name	Alarm	2025-09-17 14:23:22	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:23:22	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:23:22	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:23:01	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:23:01	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:22:52	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:22:52	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:22:39	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:22:39	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:22:07	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:22:07	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:21:35	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:21:35	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:21:02	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:21:02	Unconfirmed		
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:20:42	Unconfirmed		

Figure 21- 88

●Scheduled Sending

Click the Scheduled Sending button to configure the sending frequency, which can be set to daily or monthly, as shown in the figure below:

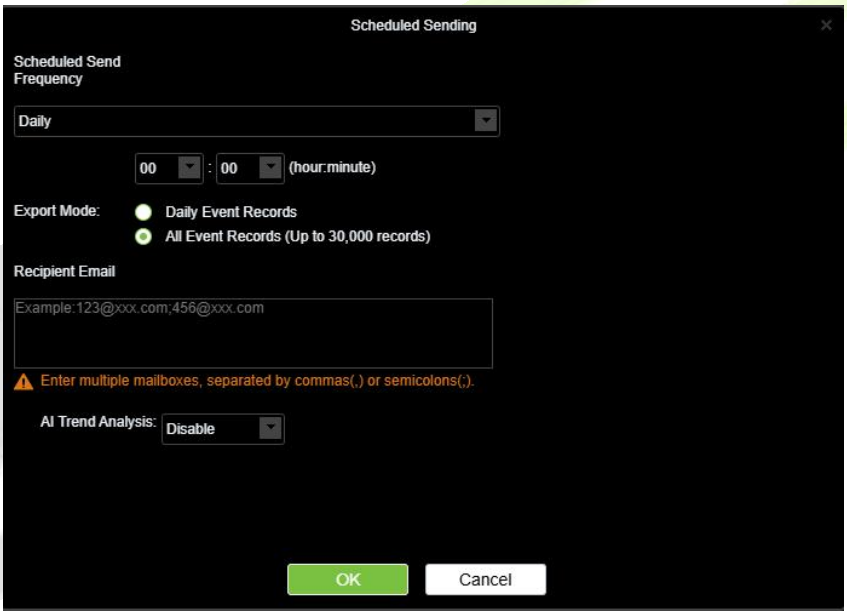


Figure 21- 89

- Scheduled Send Frequency:

Optional daily or weekly; If "Daily" is selected, you can further fill in the specific time. If "Monthly" is selected, you can further choose the exact date of each month for sending.

- Export Mode:You can choose daily event records or all event records.
- Recipient Email:Fill in the email address where you need to receive the report.
- AI Trend Analysis:It is disabled by default. Once enabled, AI trend analysis will be sent via email.The content of the email is as shown in the following figure:

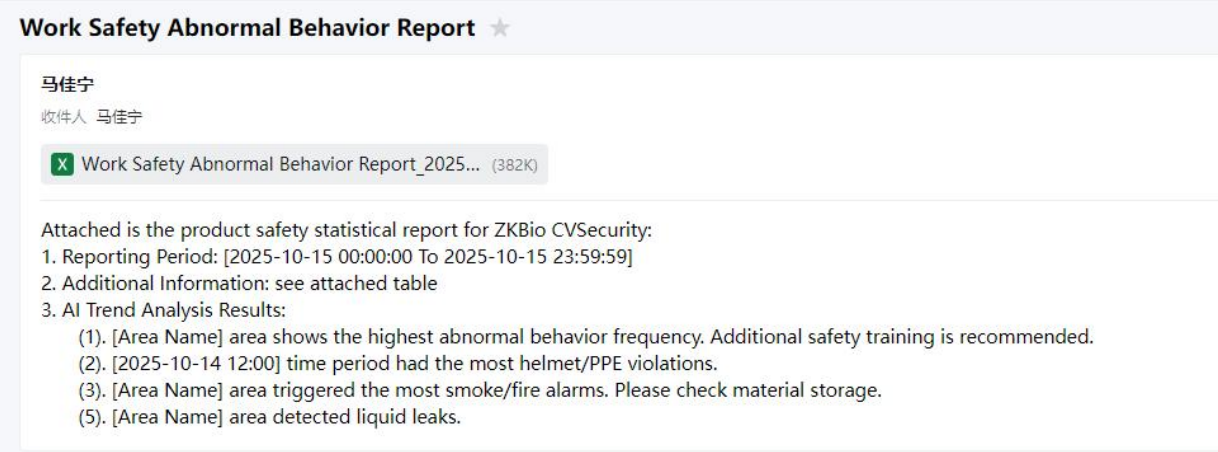


Figure 21- 90

21.6.7Intelligent Visitor Panel

This panel, by centrally displaying visitor status in real-time, it significantly improves the efficiency of front desk reception and visitor experience, while enhancing safety control and emergency response capabilities, and provides a basis for visitor data analysis for enterprises to optimize management decisions and enhance professional image.

●Operating Steps:

Enter Service Center → Scene Center → Scene Configuration, locate the Intelligent Visitor Panel scene, and click "Configuring Scenarios".

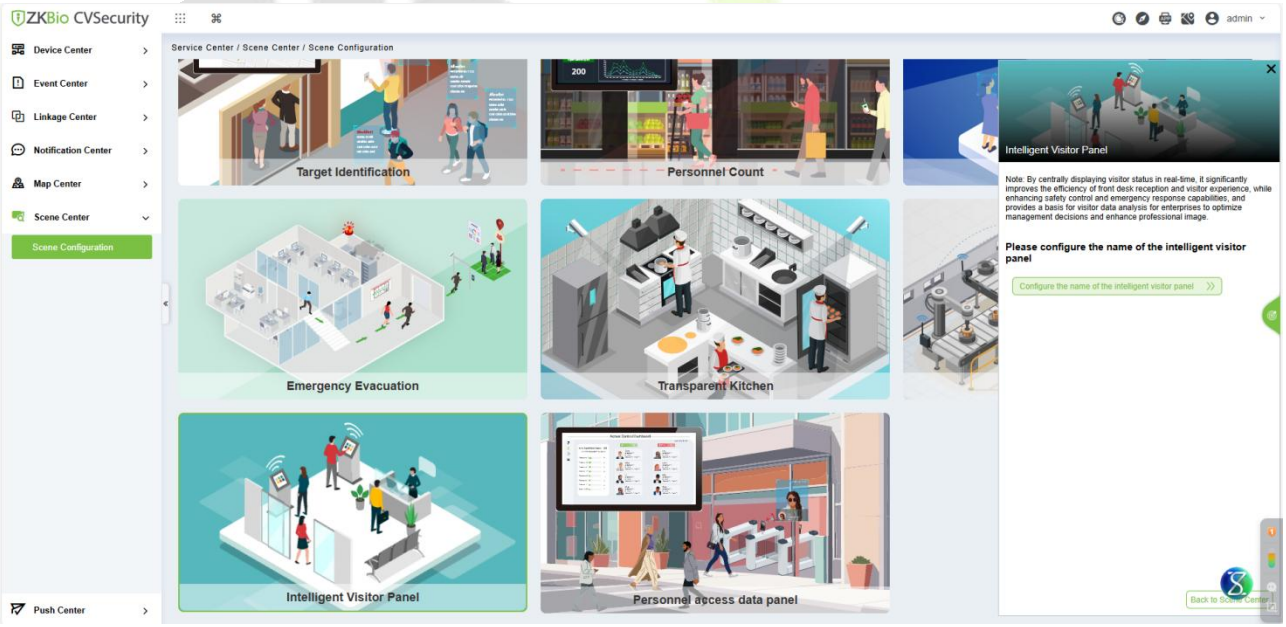


Figure 21- 91

Step1: Configure the name of the intelligent visitor panel

Please configure the name of the intelligent visitor panel,as shown in the figure below:

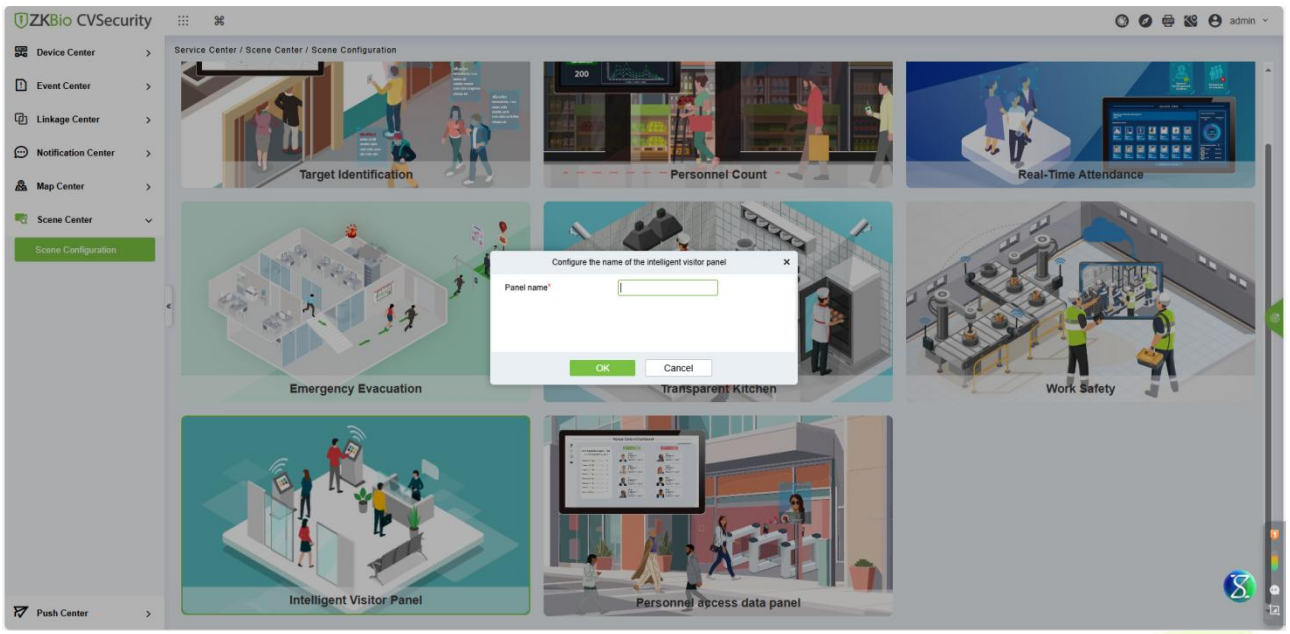


Figure 21- 92

Step2: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:

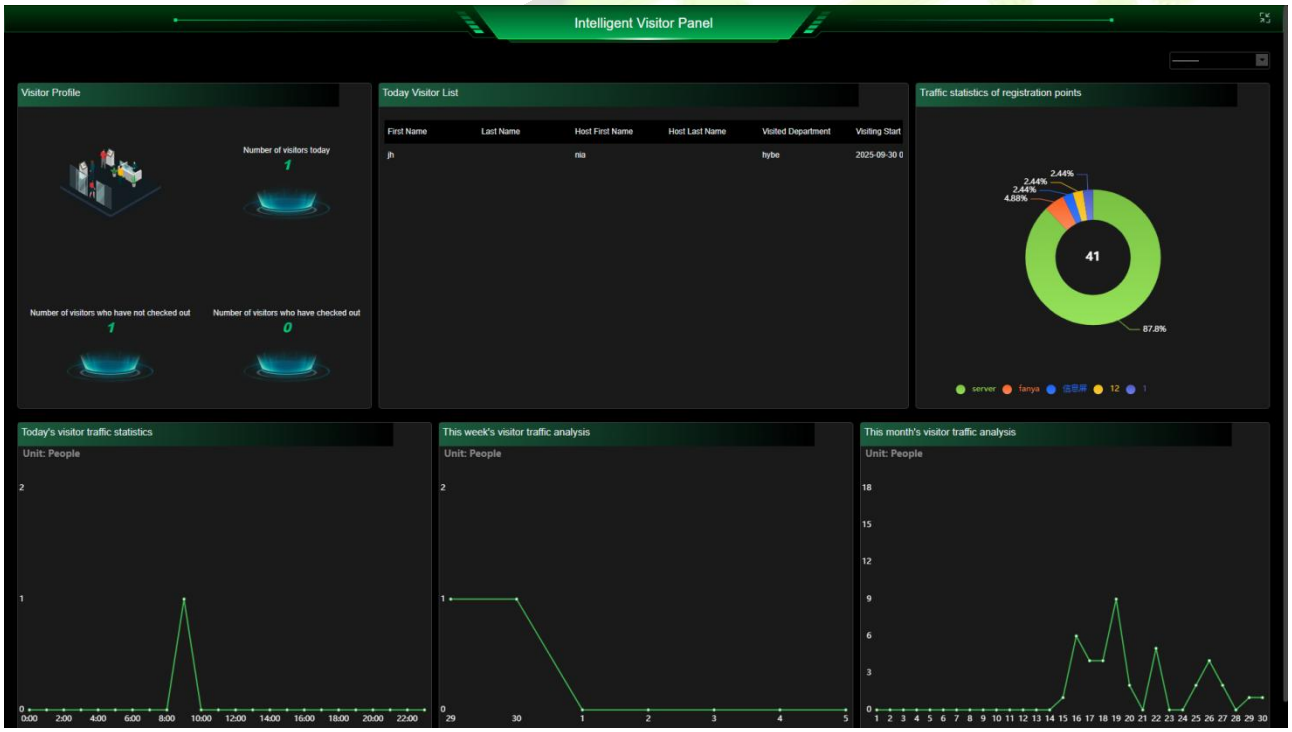


Figure 21- 93

●Filtering condition

Click the the drop-down box in the upper right corner to select the Visitor Registration Point, as shown in the following figure:

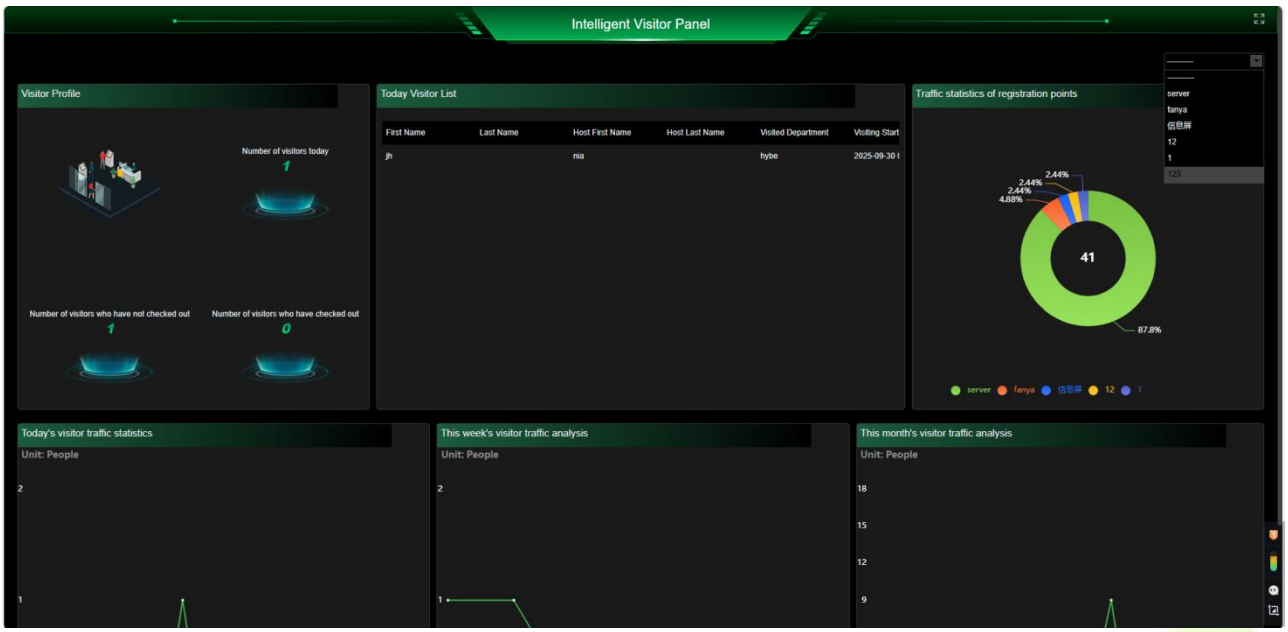


Figure 21- 94

21.6.8Personnel Entry & Exit Panel

The Space Management panel delivers accurate, real-time personnel tracking data, serving as a critical tool for enhancing factory and facility safety, operational efficiency, management precision, and regulatory compliance.

●Operating Steps:

Enter Service Center → Scene Center → Scene Configuration, locate the Personnel Access Data Panel scene, and click "Configuring Scenarios".

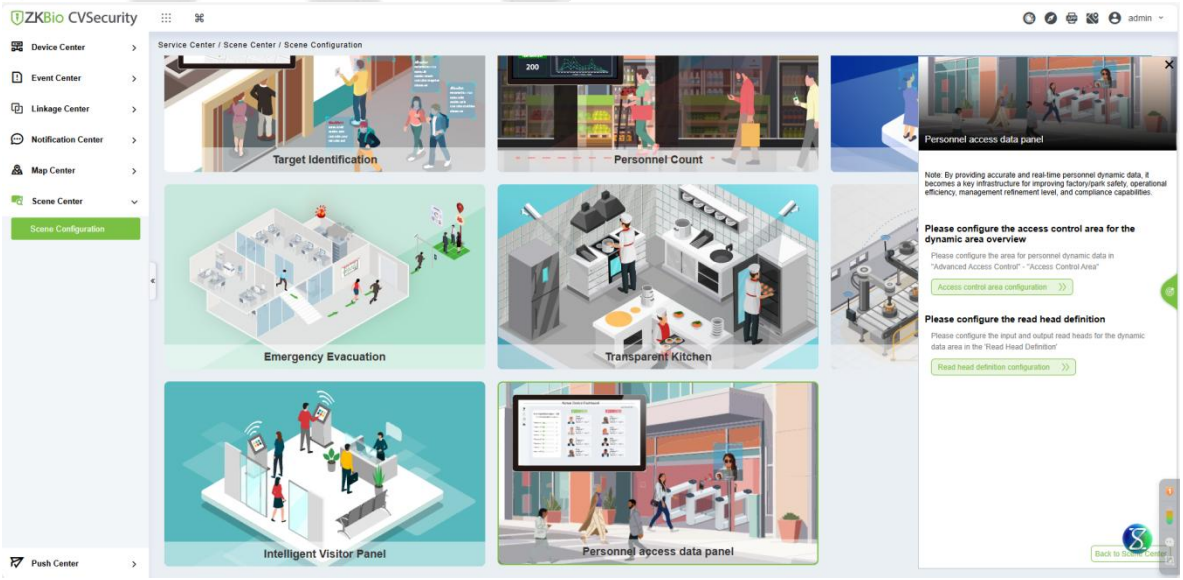


Figure 21- 95

Step1: Access control area configuration

Please configure the access control area for the dynamic area overview.Configure the area for personnel dynamic data in "Advanced Access Control" - "Access Control Area",as shown in the figure below:

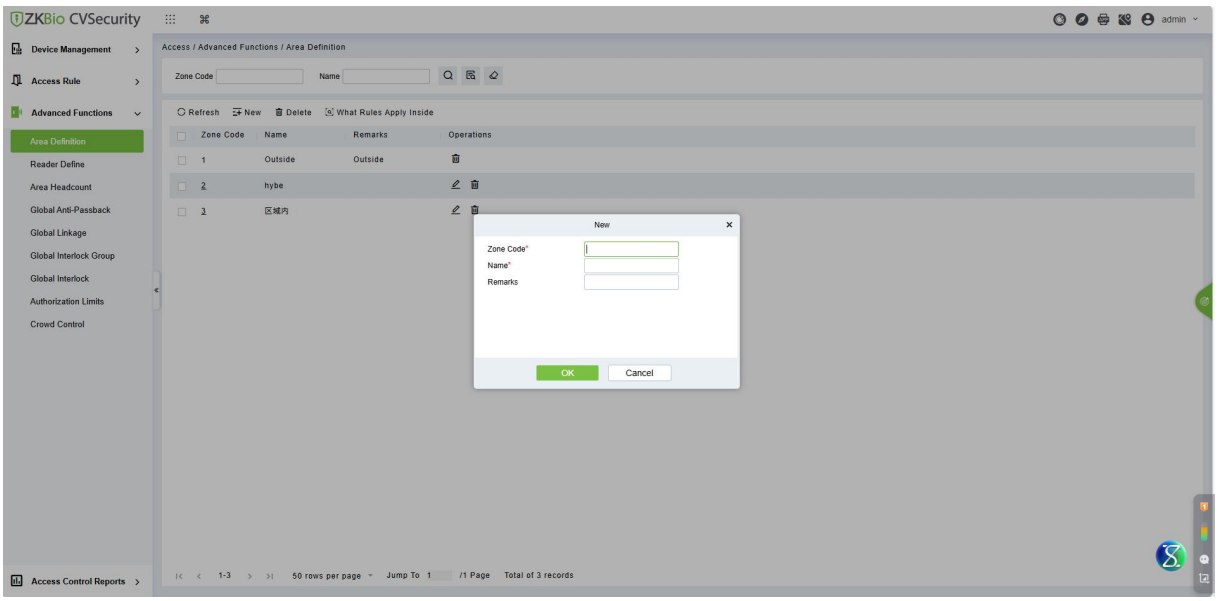


Figure 21- 96

Step2: Reader definition configuration

Please configure the reader definition.Configure the input and output readers for the dynamic data area in the 'Reader Definition',as shown in the figure below:

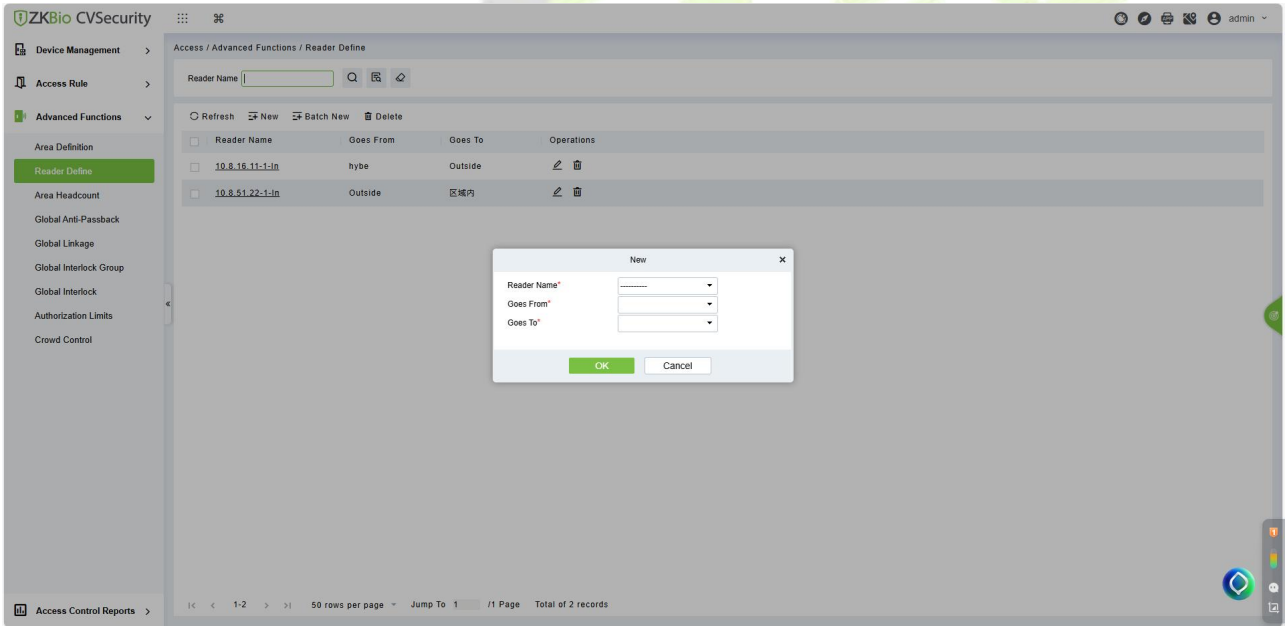


Figure 21- 97

Step3: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:

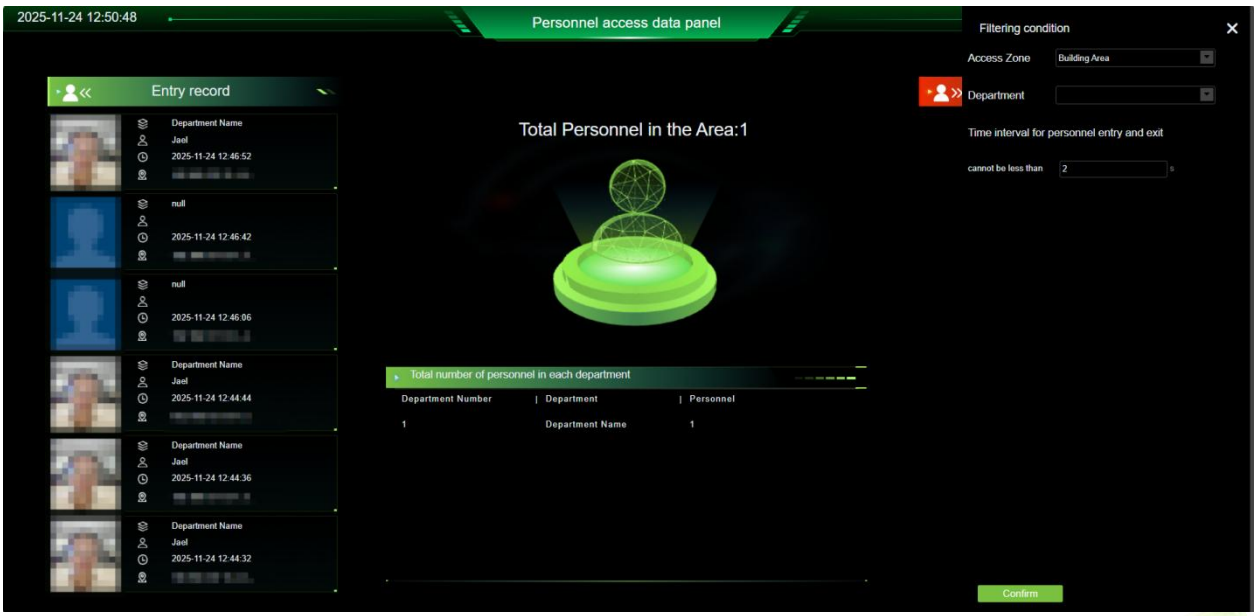


Figure 21- 98

Note: The entry records on the left and exit records on the right are the statistics of personnel entry and exit for the day; the total number of people in the region displayed in the middle is counted according to the actual number of people in the access control area. When a person enters the designated area through verification, the displayed number increases by 1, and when a person leaves the designated area through verification, the displayed number decreases by 1.

●Filtering condition

Click the Settings icon in the upper right corner to select the access control Zone and department. Users can customize the minimum number of seconds for the time interval between personnel entry and exit, so as to avoid the problem of repeated verification and repeated records in a short period of time.

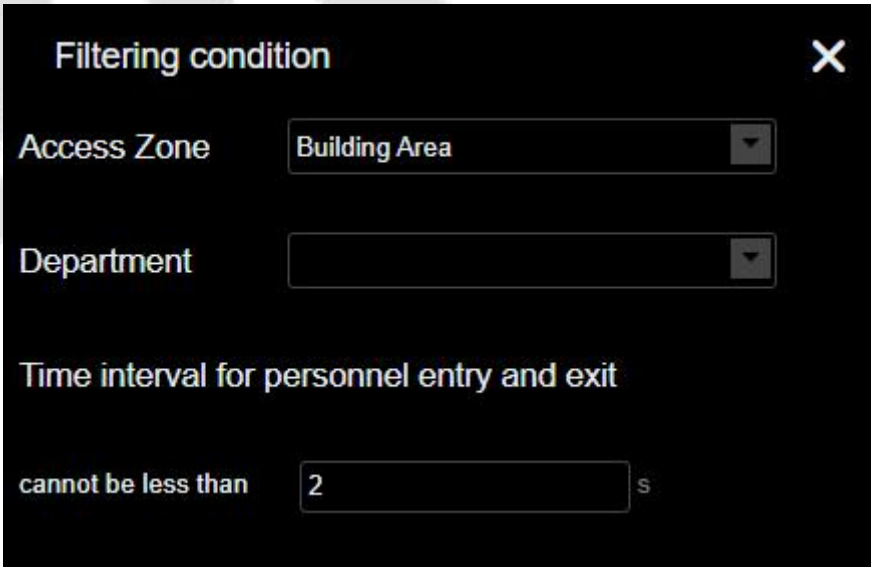


Figure 21- 99

21.7 Push Center

21.7.1Push Configuration

Add New

● Operation Step:

Step 1: In the Service Center module, choose "**Push Center > Push Configuration**".

Step 2: In the **Push Configuration** interface, click **Add New** and fill in the relevant parameters, as shown in Figure 21-78. Please refer to Table21-4 for parameter description.

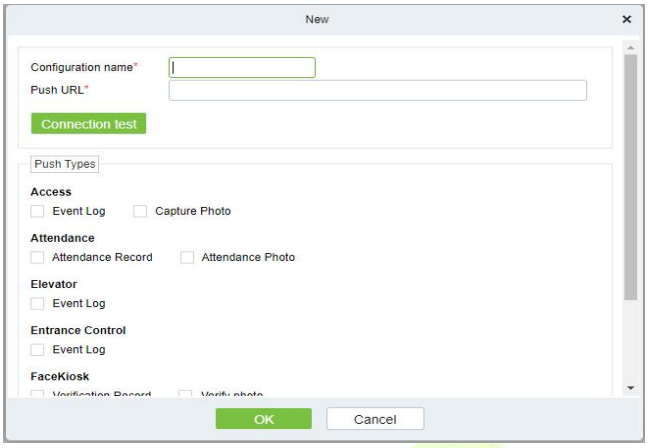


Figure 21- 100 Add Push Configuration

Parameter	Description
Configuration Name	Enter the configuration name
Push URL	Enter the push URL

Table 21- 4 Parameters for New

Delete

Select one or more push configuration and click **Delete** at the upper part of the list and click **OK** to delete the selected push configuration Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single push configuration.

Docking Example

It will show the example of data format as a code.

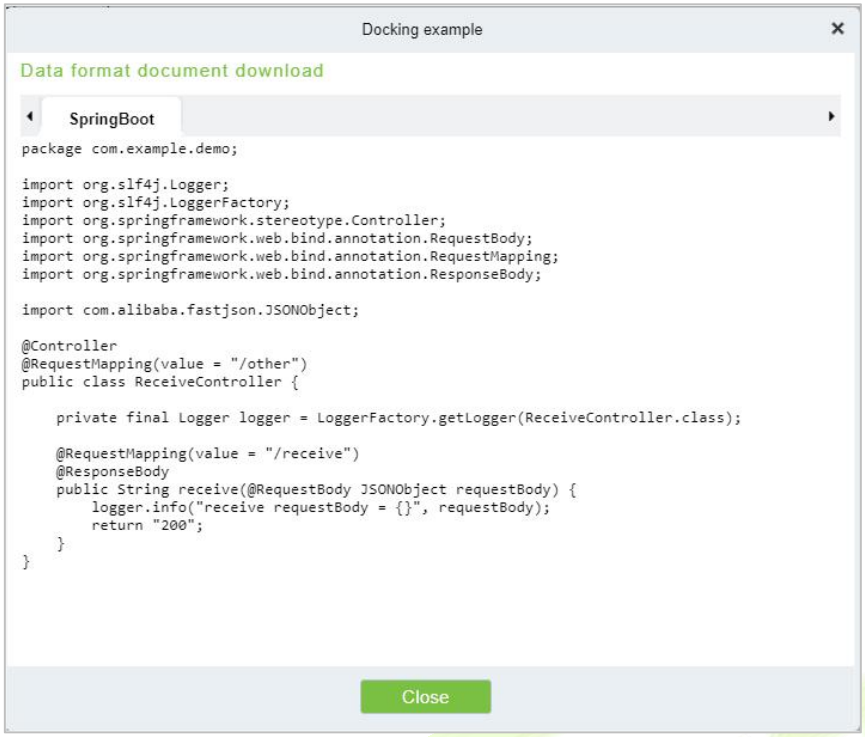


Figure 21- 101 Docking Example

21.7.2Push Exception Record

Delete

Select one or more push exception record and click **Delete** at the upper part of the list and click **OK** to delete the selected. push exception record Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single push exception record.

Re-push

If the data sync failed one time it will re-sync the data automatically to the software and device.

Manual Push

Manual push is we need to sync the data from device to the software.

ZKTeco Industrial Park, No.32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone : +86 769 - 82109991
Fax : +86 755 - 89602394
www.zkteco.com