Change Log

ZKBio CVSecurity

Version: 3.0

Date: October 2025

Software Version: ZKBio CVSecurity_6.7.0_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

First of all, thank you for choosing our company's products. To better utilize all the functions in the software, please read the manual of this product carefully before use.Without the written consent of our company, no unit or individual may excerpt, copy any part or all of the content of this manual, nor may it be disseminated in any form.

The products described in this manual may include software copyrighted by the Company and its potential licensors. Without the permission of the relevant rights holder, no one may, in any form, copy, distribute, modify, excerpt, decompile, disassemble, decrypt, reverse engineer, lease, transfer, sublicense or engage in any other act that infringes upon the copyright of the aforementioned software, except where such restrictions are prohibited by applicable law.

Due to the continuous updates of our products, our company does not guarantee that the actual products will be consistent with this data. We also do not assume any disputes arising from the inconsistency between the actual technical parameters and this data. Any changes will not be notified in advance.

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 template-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.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface template 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.

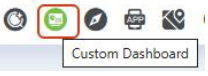
Symbols

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.

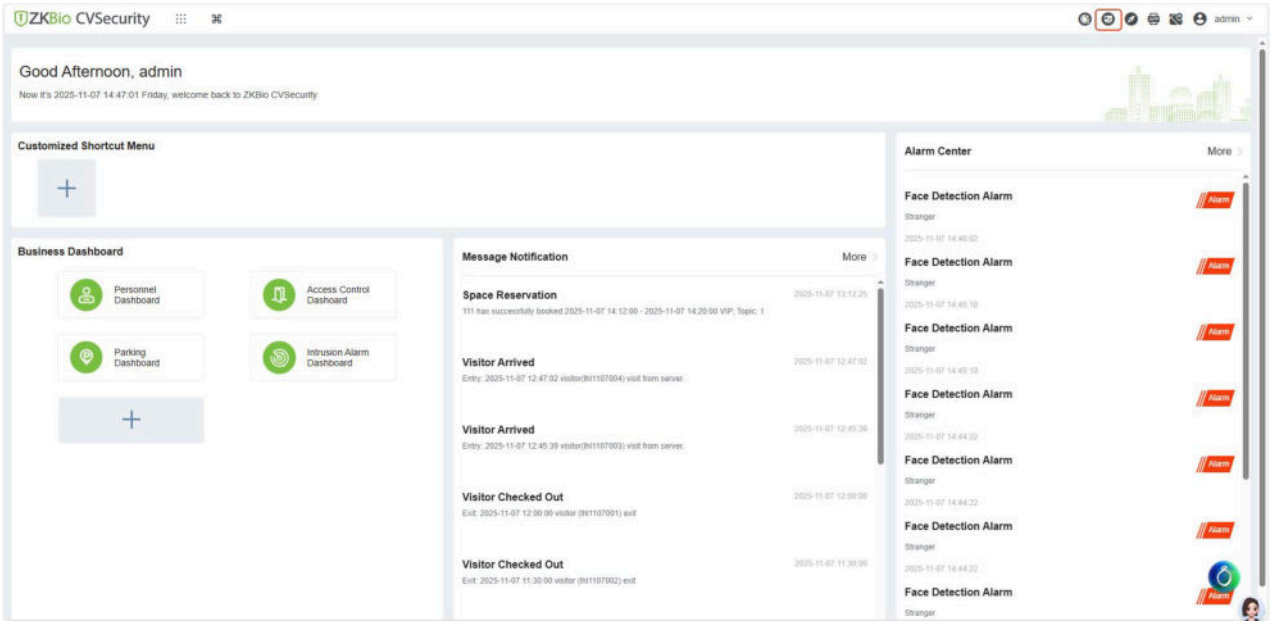
TABLE OF CONTENTS

Custom Panel

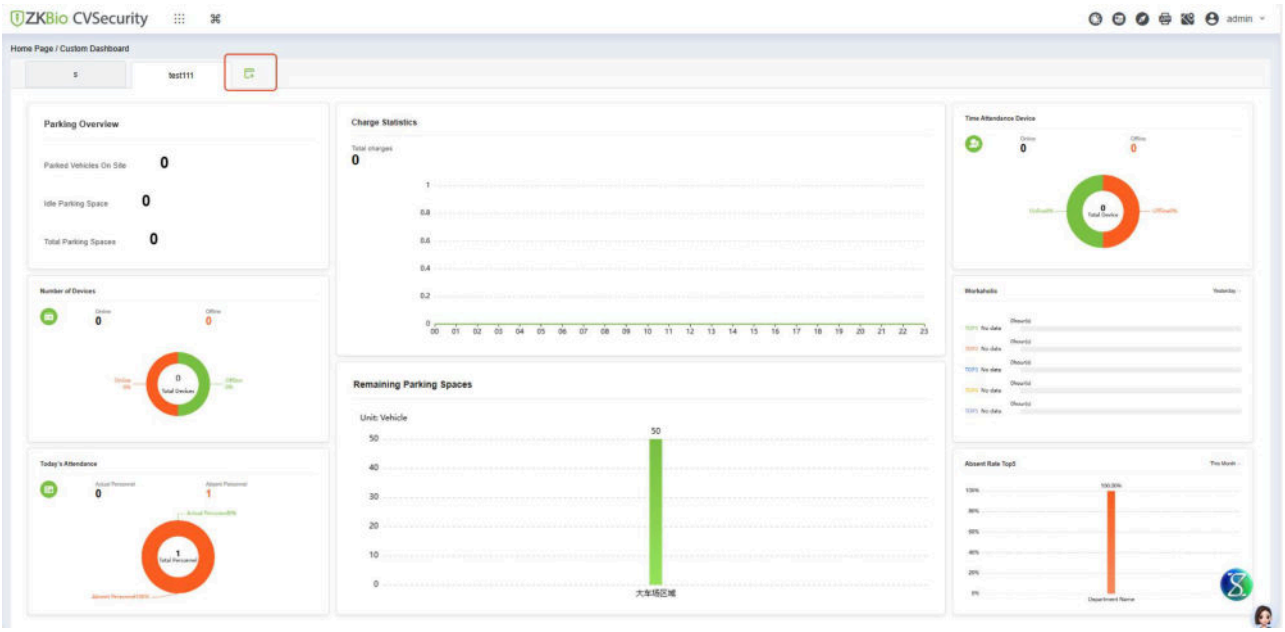
New customizable dashboard feature that allows users to create personalized data panels, configure widgets, and arrange key metrics for their specific monitoring requirements.

Step1: Click the small icon 

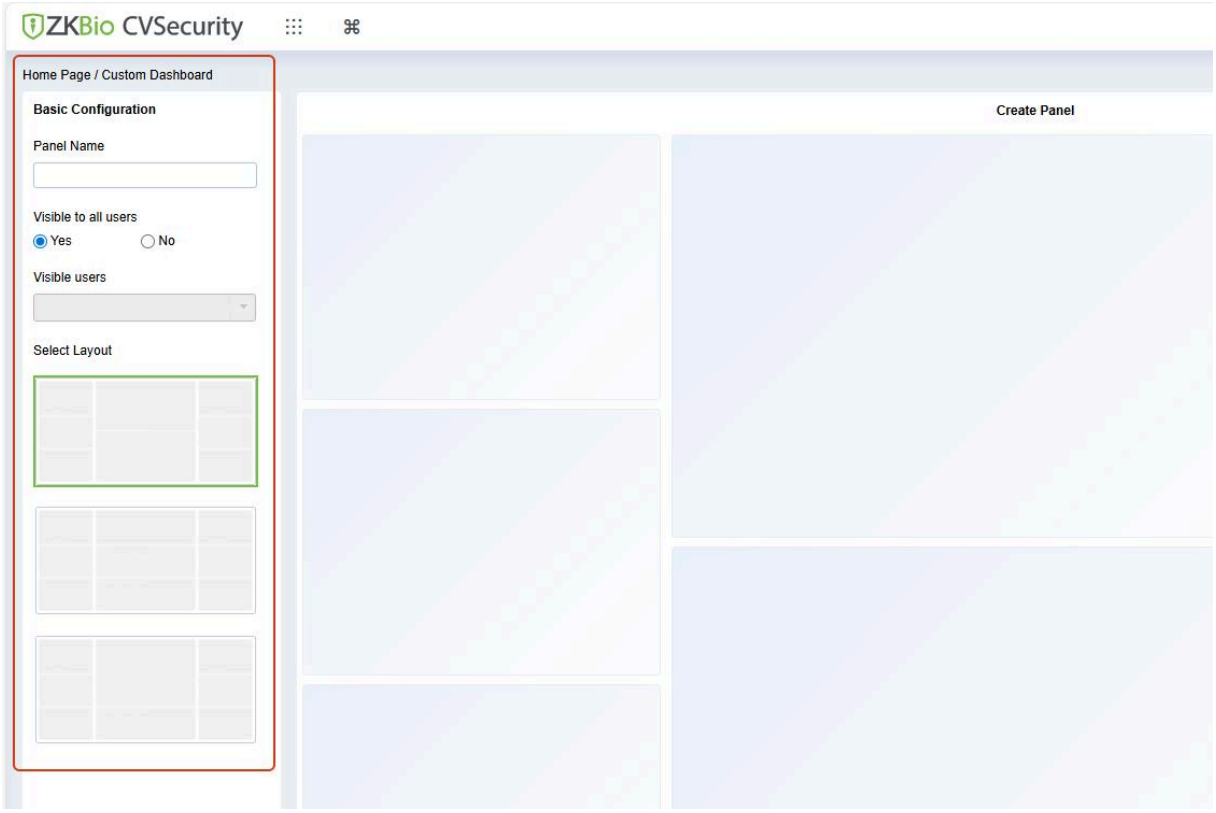
of Custom Panel in the upper right corner to access the viewing and configuration interface.



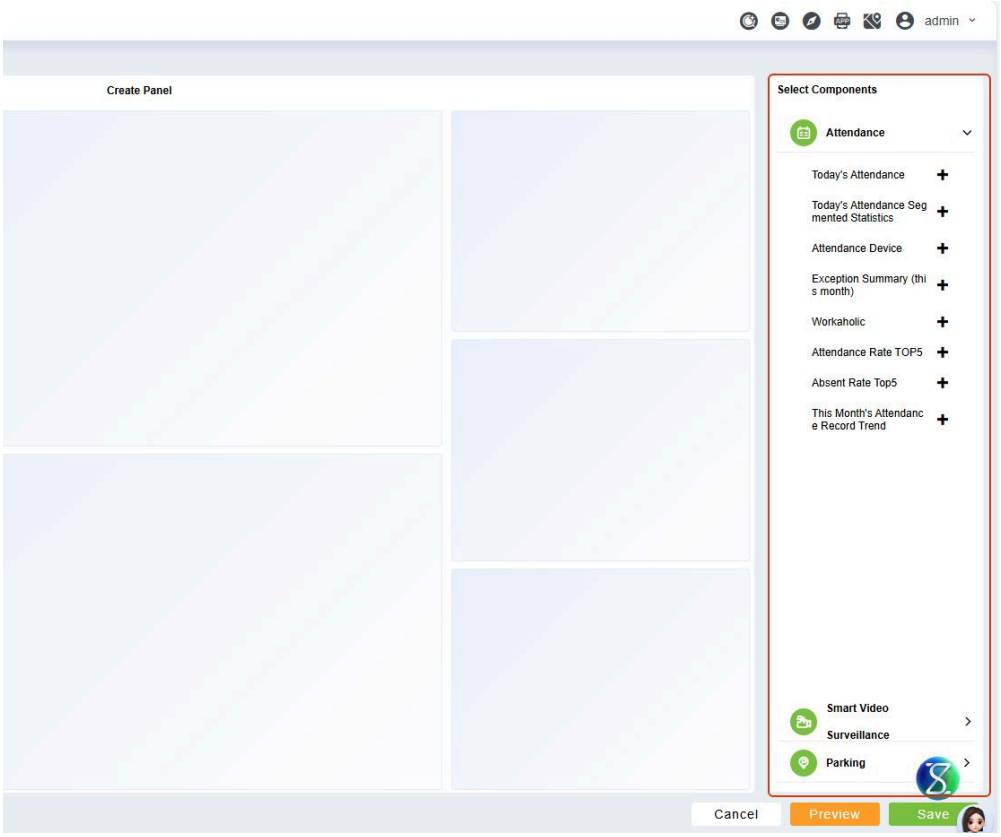
Step2: On this page, you can view the configured Custom Panels. Click the Add button  to access the configuration interface.



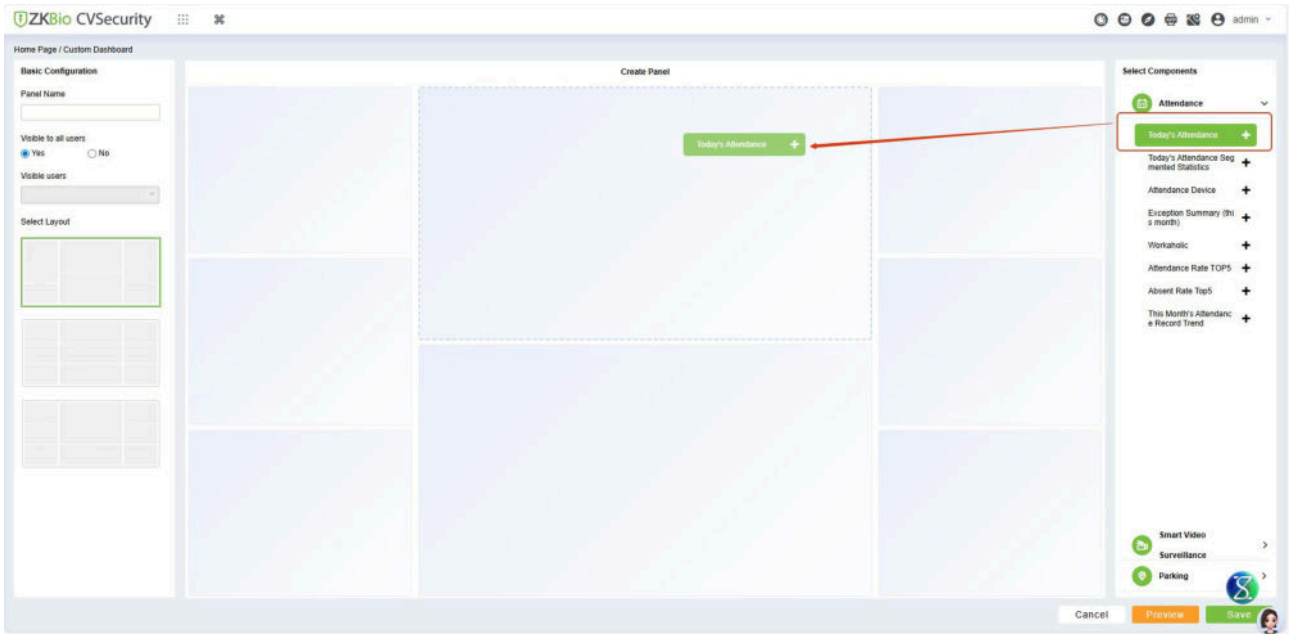
Step3: On the left side of the configuration interface, you can set the panel name and check whether it is visible to all users. If you select "No", you can further select which users are allowed to view it. Then choose a suitable panel layout to start the configuration.



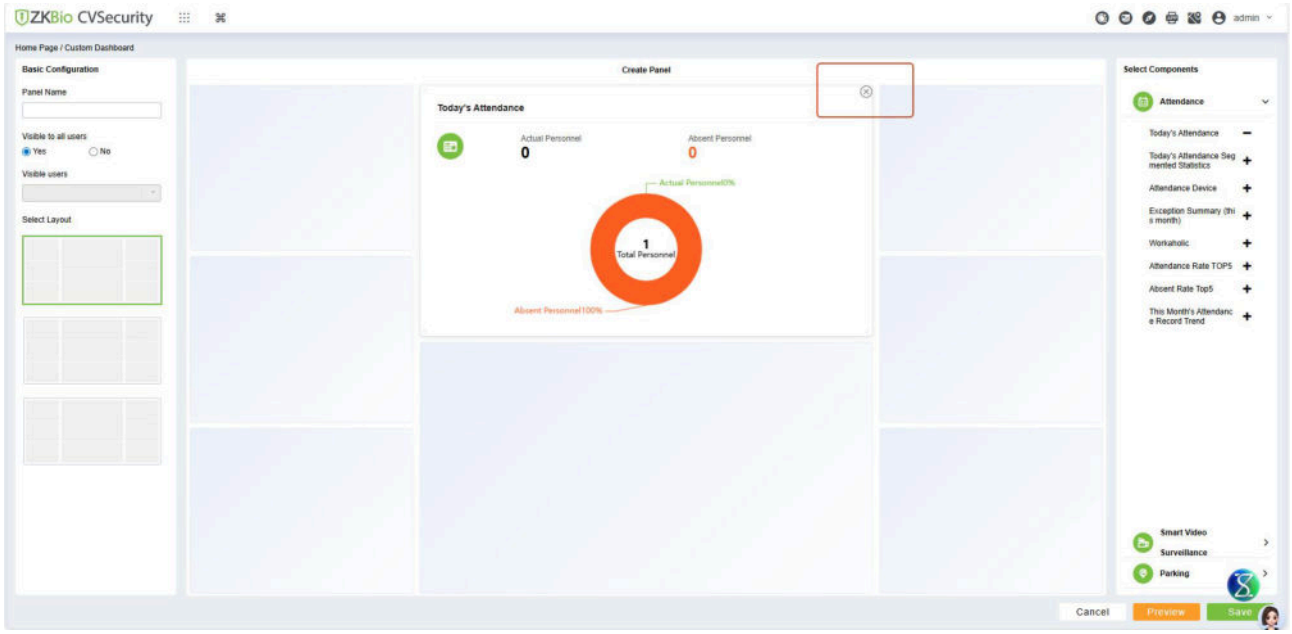
Step4: On the right side of the configuration interface, components for multiple modules are provided. Users can freely combine them to form a visualized data panel that suits their needs.



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.



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.

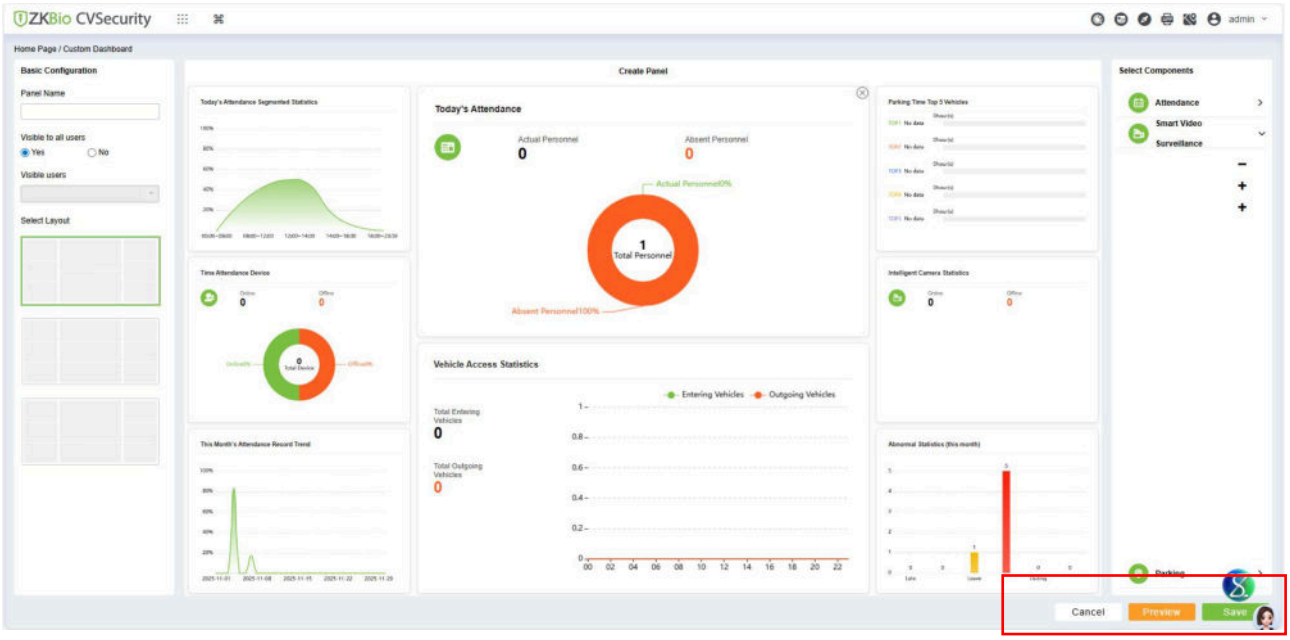


Step5: After completing the configuration:

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

Click "Cancel" to exit the configuration interface.

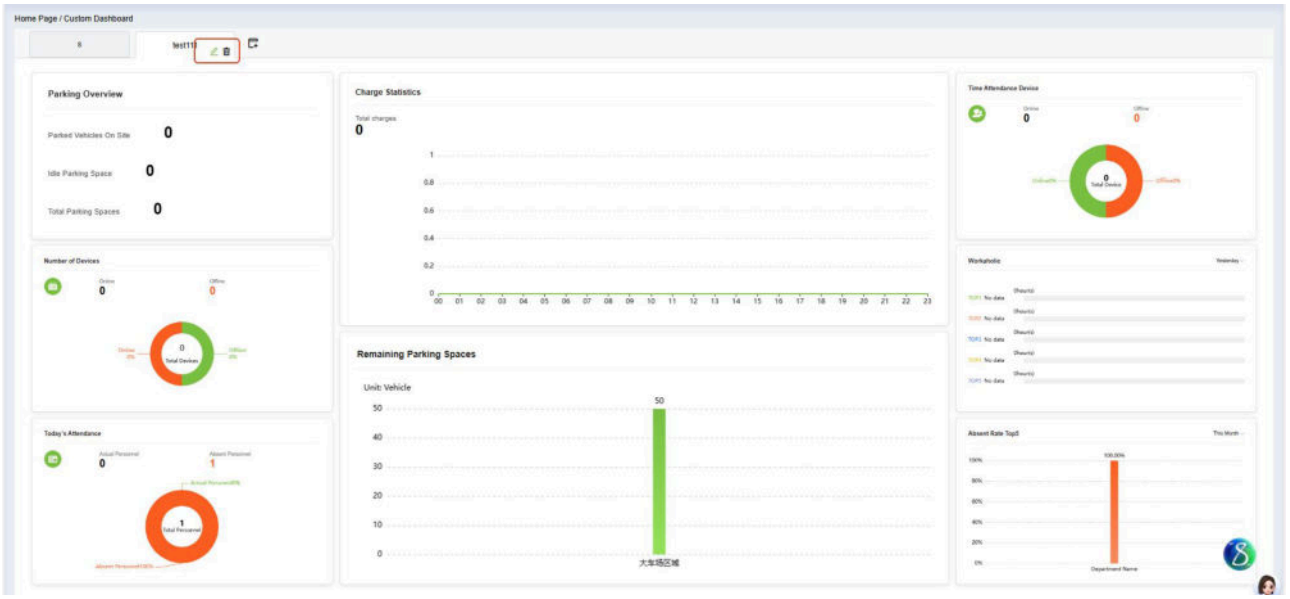
Click "Save" to save the current Custom Panel.



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.

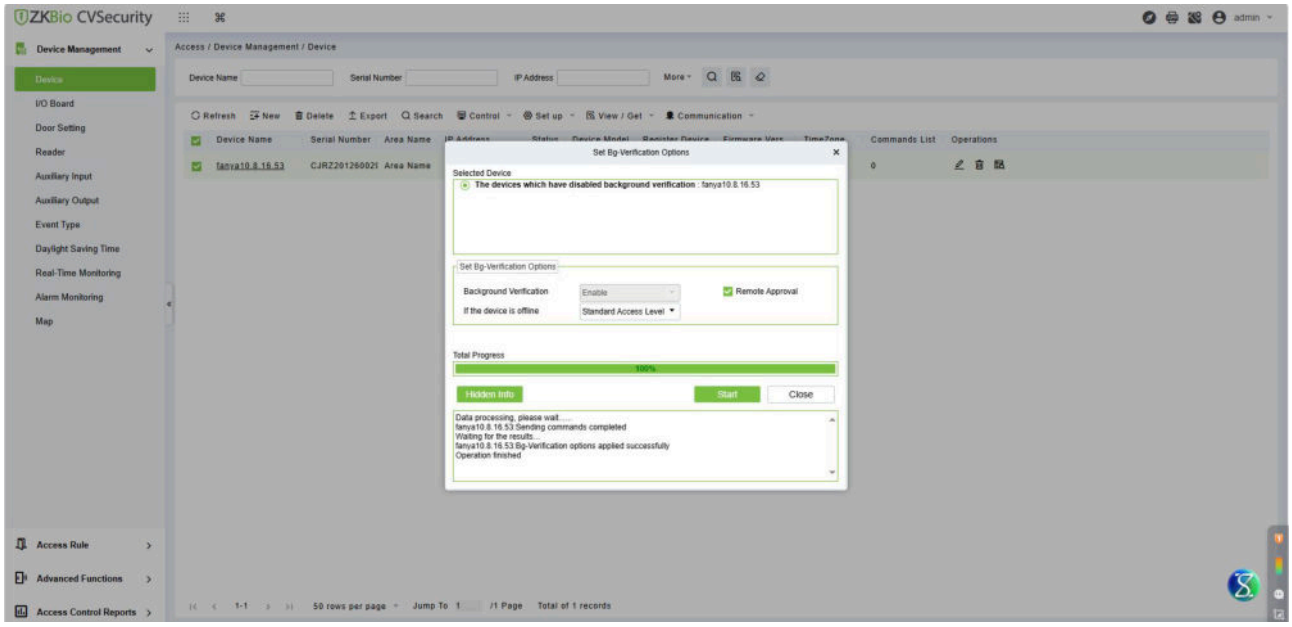


Access Control

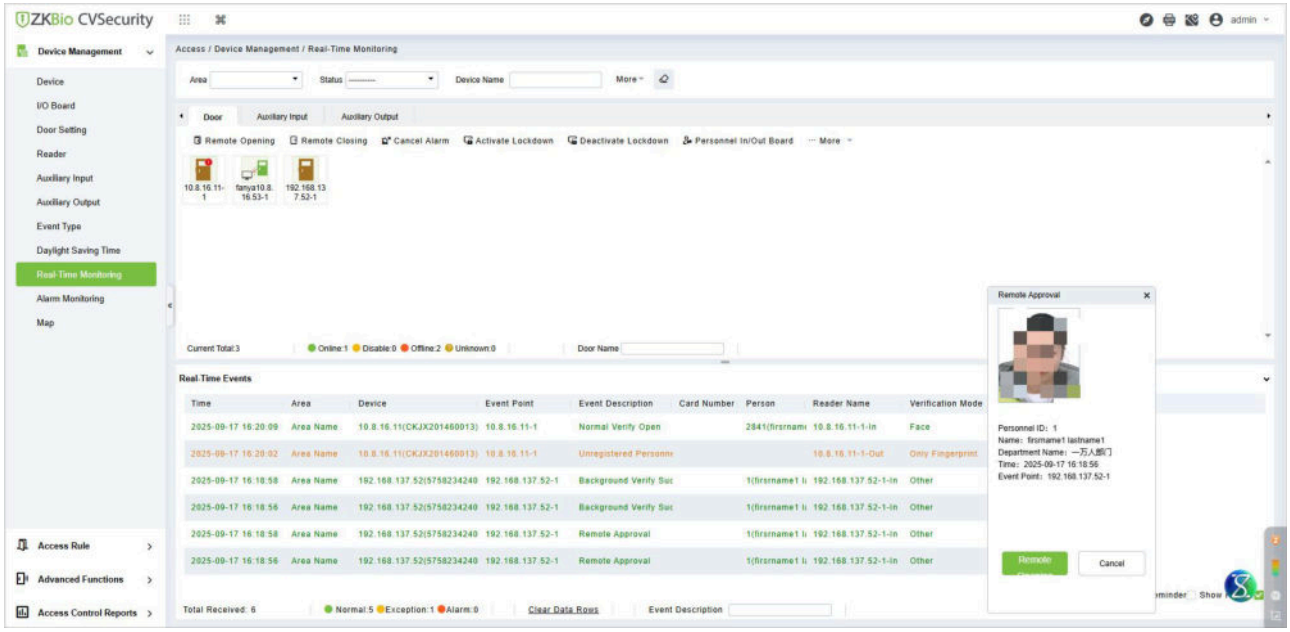
- **Background Verification-Requires manual approval from management personnel after device authentication, adding a second layer of verification before granting access.**

Applicable Scenarios: High-security areas such as bank vaults and data centers.

Step: Enter Access → Device Management → Device, select the device and click "Set up" → "Set Bg-Verification Options". Enable the background verification function and check the option for remote approval.



On the real-time monitoring interface, when a user attempts verification at this device, a secondary verification interface will pop up, as shown in the figure below:

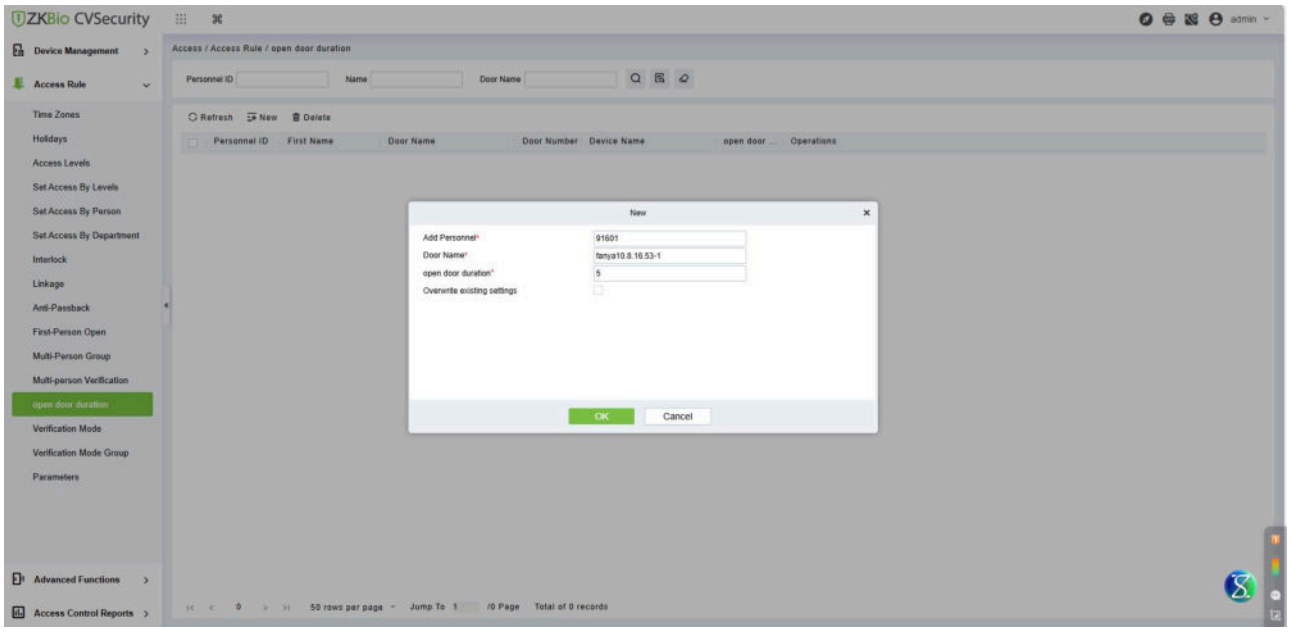


- **Open Door Duration-Set different door opening durations based on personnel.**

Applicable Scenarios: Warehouses, logistics centers, and industrial facilities with high-frequency access.

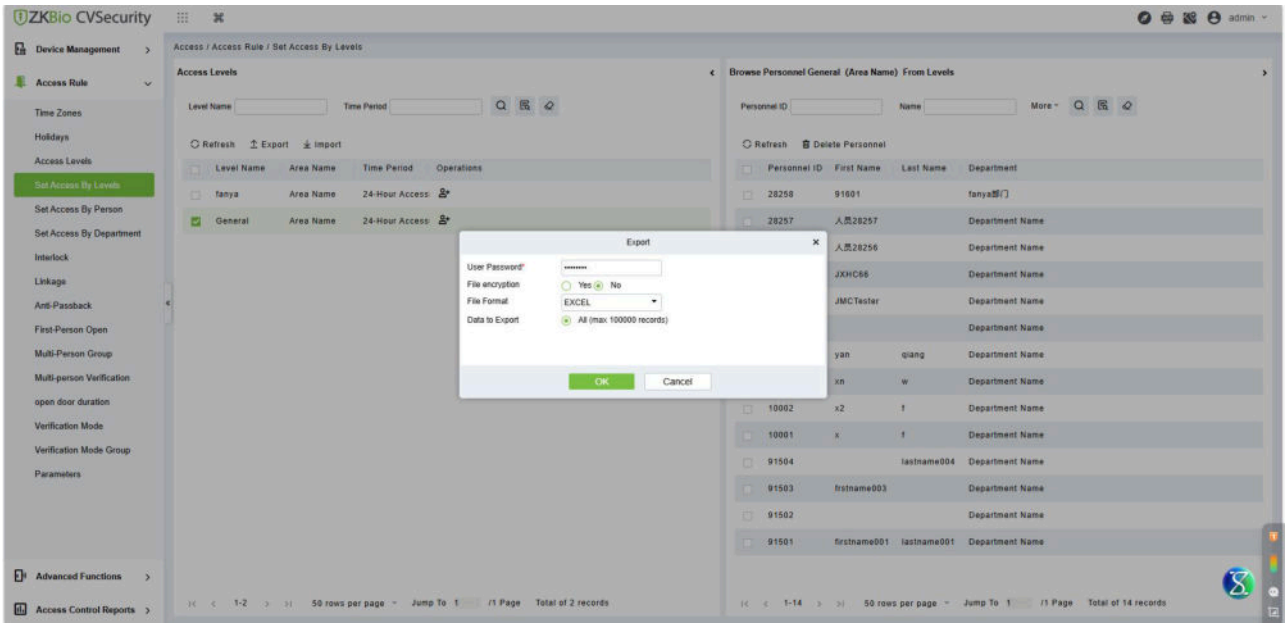
Supports flexible door timing based on operational needs — standard duration for shift changes or extended timing (e.g., 60 seconds) for cargo handling and equipment passage.

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.



- **Navigate Access > Access Rule: Personnel export from permission groups now includes name field in exported data.**

Step: Enter Access → Access Rule → Set Access By Levels, select the desired permission group(s) on the left, then click the "Export" button. As shown in the figure below, enter the page password to initiate the export of the permission group.



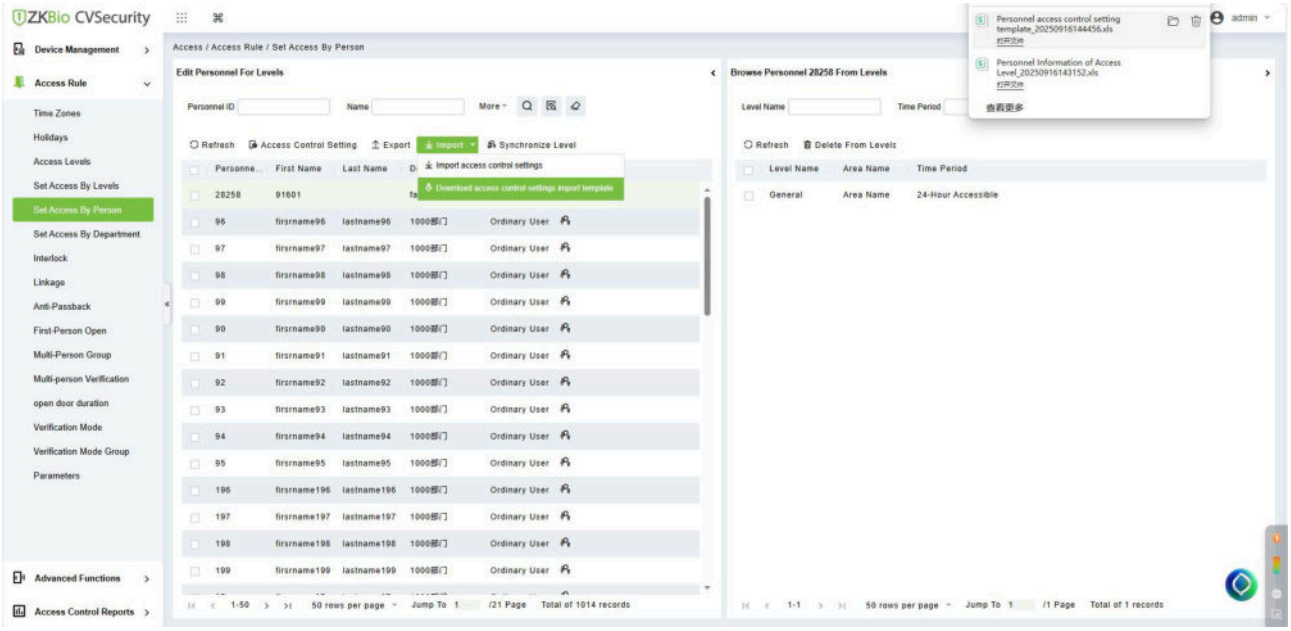
The exported permission group is shown in the following figure, including: Level Name, Personnel ID, First Name and Last Name.

Personnel Information of Access Level

Level Name	Personnel ID	First Name	Last Name
General	28258	91601	
General	28257	[redacted]28257	
General	28256	28256	
General	661128	JXHC66	
General	970312	JMCTester	
General	20252		
General	20251	yan	qiang
General	10003	xn	w
General	10002	x2	f
General	10001	x	f
General	91504		lastname004
General	91503	frstname003	
General	91502		
General	91501	firstname001	lastname001

- **Navigate Access > Access Rule: Batch import now supports setting validity periods for multiple personnel simultaneously.**

Step: Enter Access → Access Rule → Set Access By Person,click "Import" → "Download Access Control Settings Import Template".

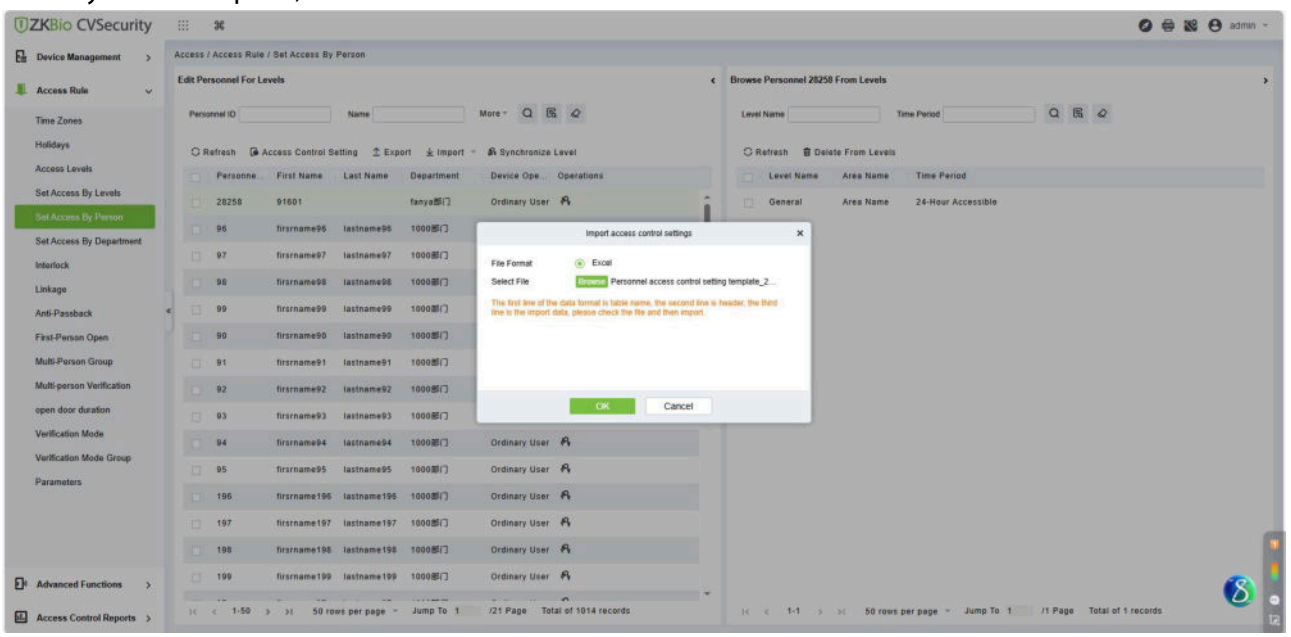


The template is shown in the figure below. Fill in the columns according to the headers: Personnel ID, Start Time and End Time. Save the template after completion.

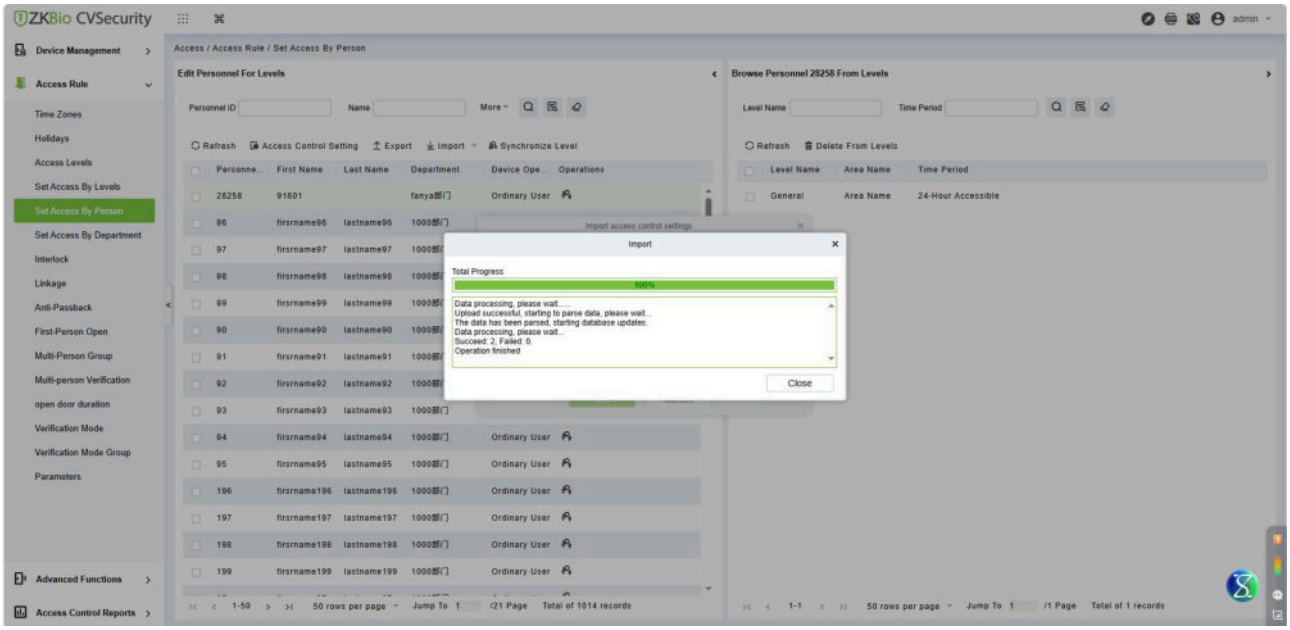
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.

Personnel access control setting template		
Personnel ID	Start Time	End Time
10010	2025/9/15	2026/10/15
10012	2025/9/17	2026/10/17

Return to the Set Access By Person page. Click "Import" → "Import Access Control Settings", select the recently saved template, and then click "OK."



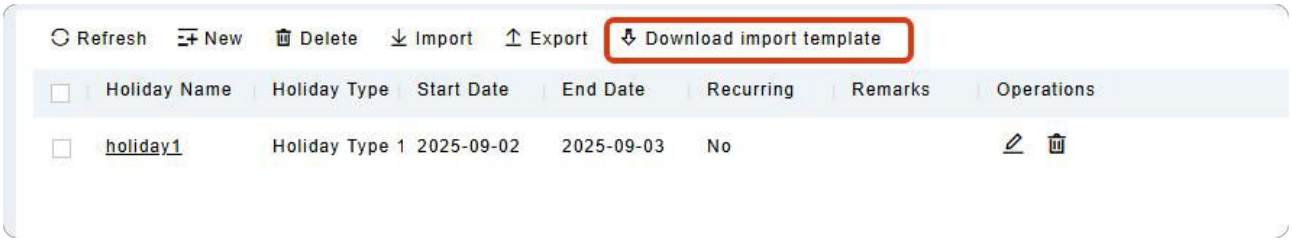
Data will begin importing automatically until the operation completion prompt appears.



- **The holiday settings for access control now support batch import and export.**

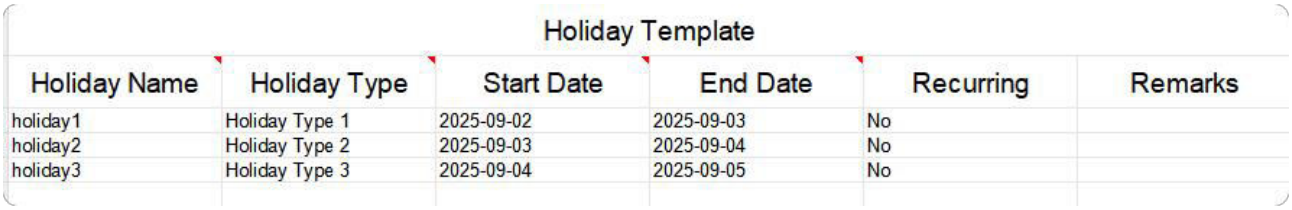
■ **Import:**

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



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

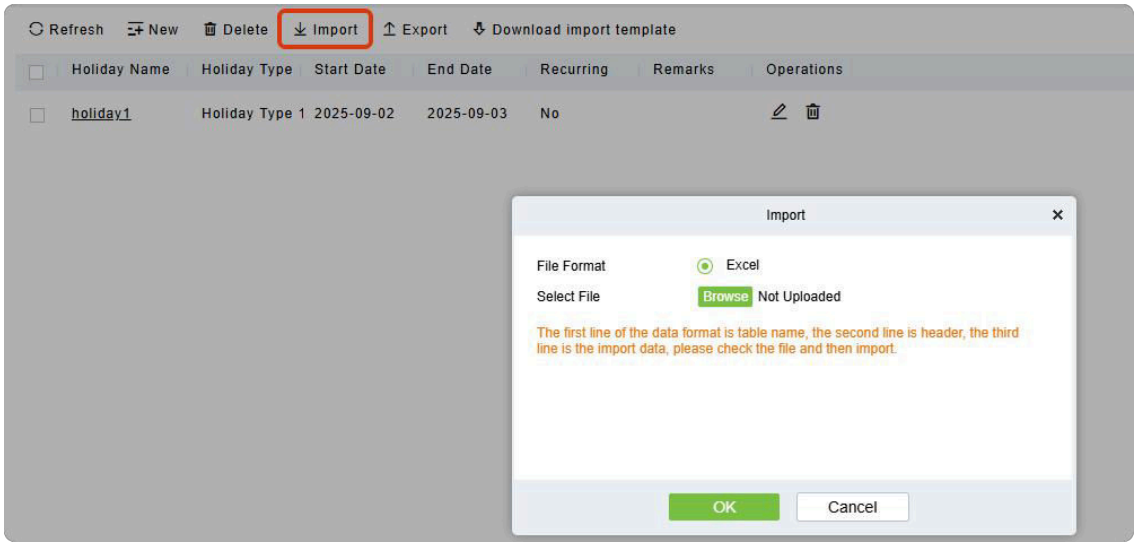
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.



Holiday Template

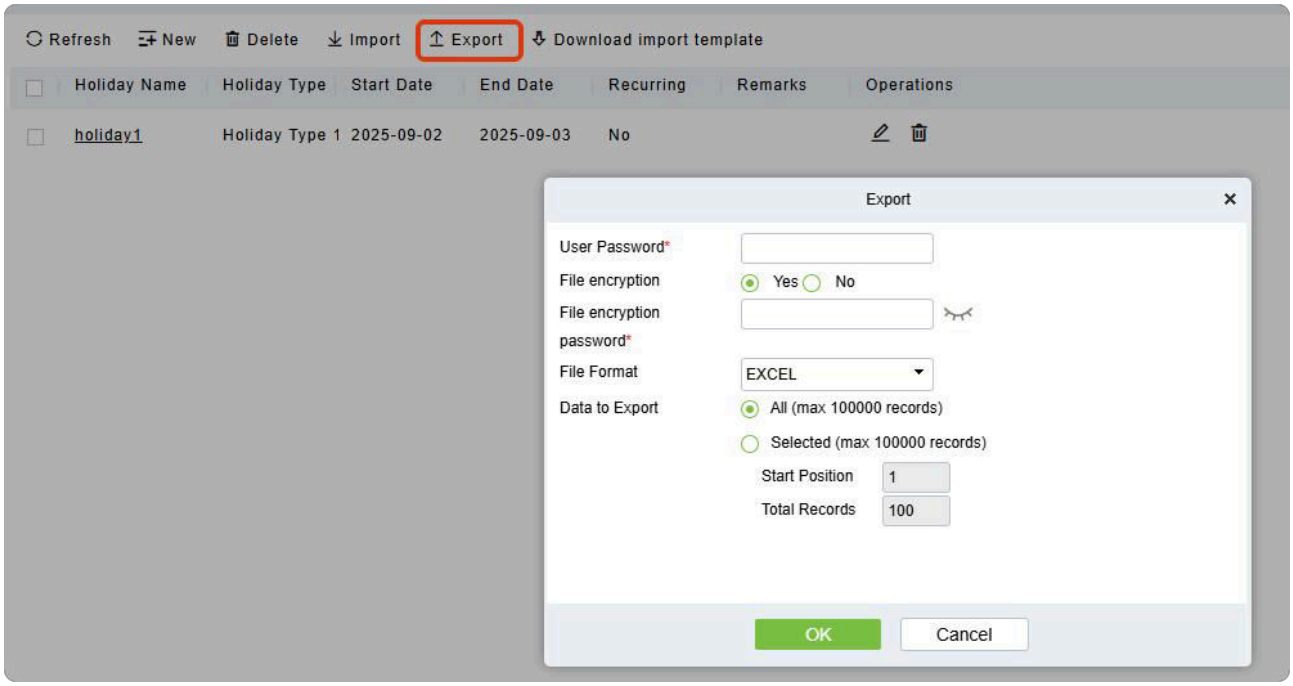
Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
holiday2	Holiday Type 2	2025-09-03	2025-09-04	No	
holiday3	Holiday Type 3	2025-09-04	2025-09-05	No	

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.



■ Export:

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

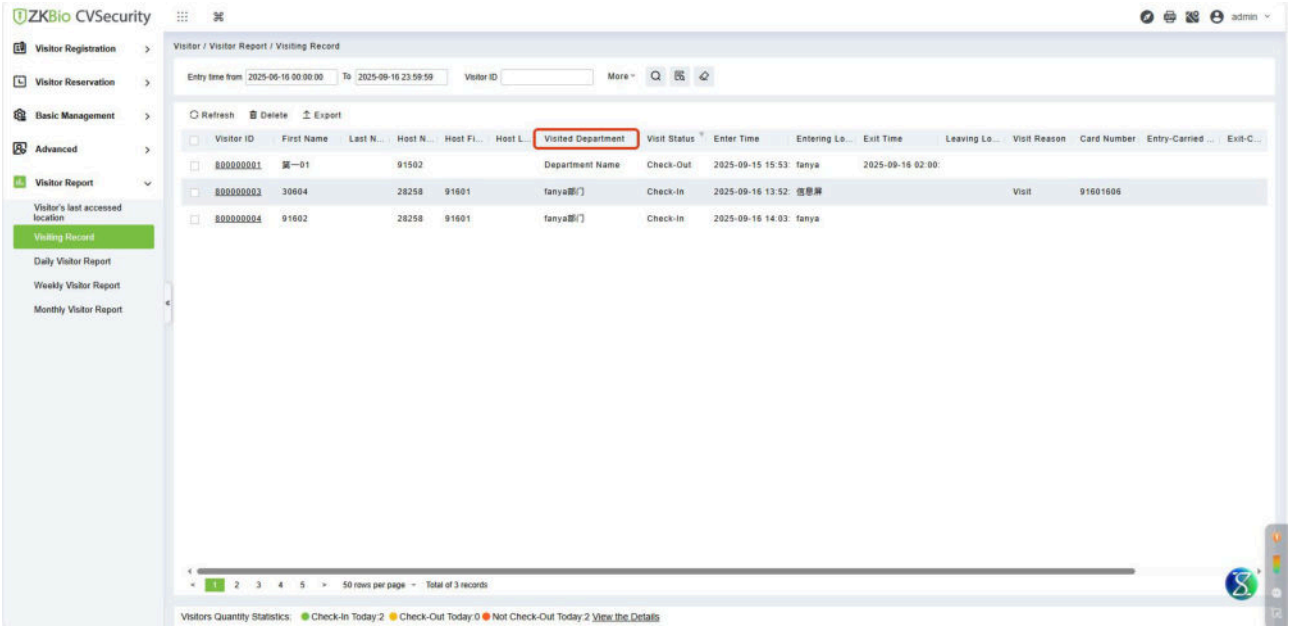


1	Holidays					
2	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
3	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
4						

Visitor Management

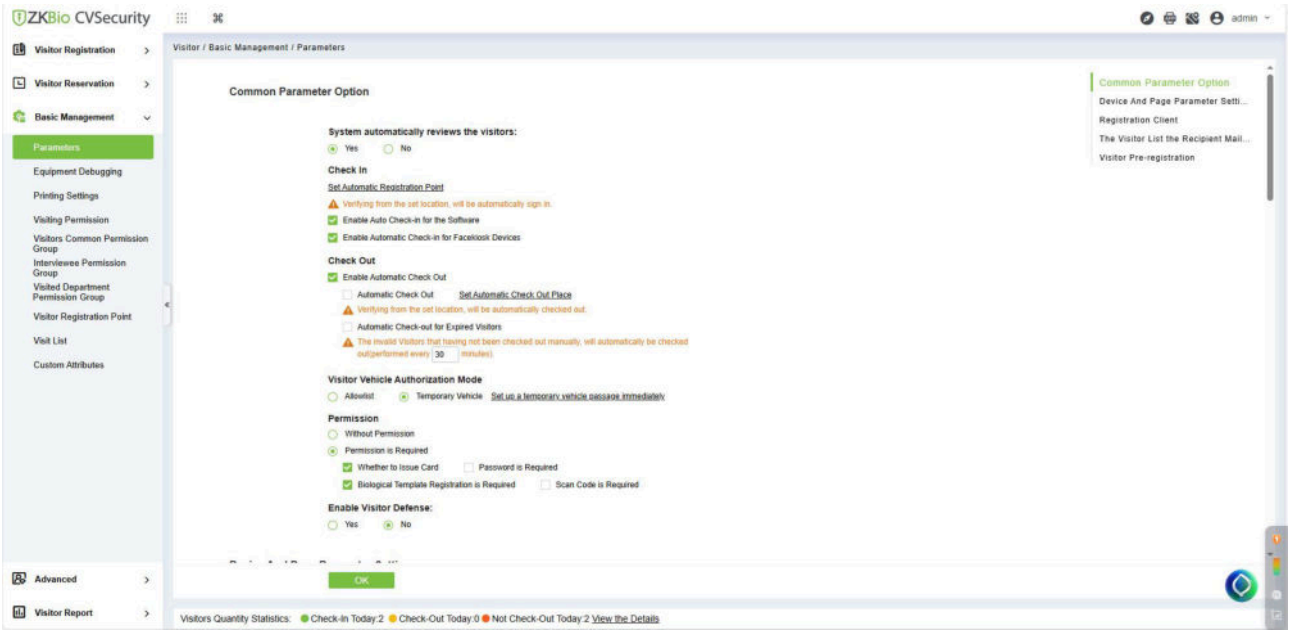
- **Navigate Visitor - Visitor Report - Visiting Record: Added department field to visiting record display.**

Step: Enter Visitor →Visitor Report → Visiting Record,can view the visiting Record, which includes the field of Visited Department.



- **Visitor Check-in Parameter Optimization.**

Step: Enter Visitor →Basic Management → Parameters.Rearrange the parameters under "Check-in" as follows:



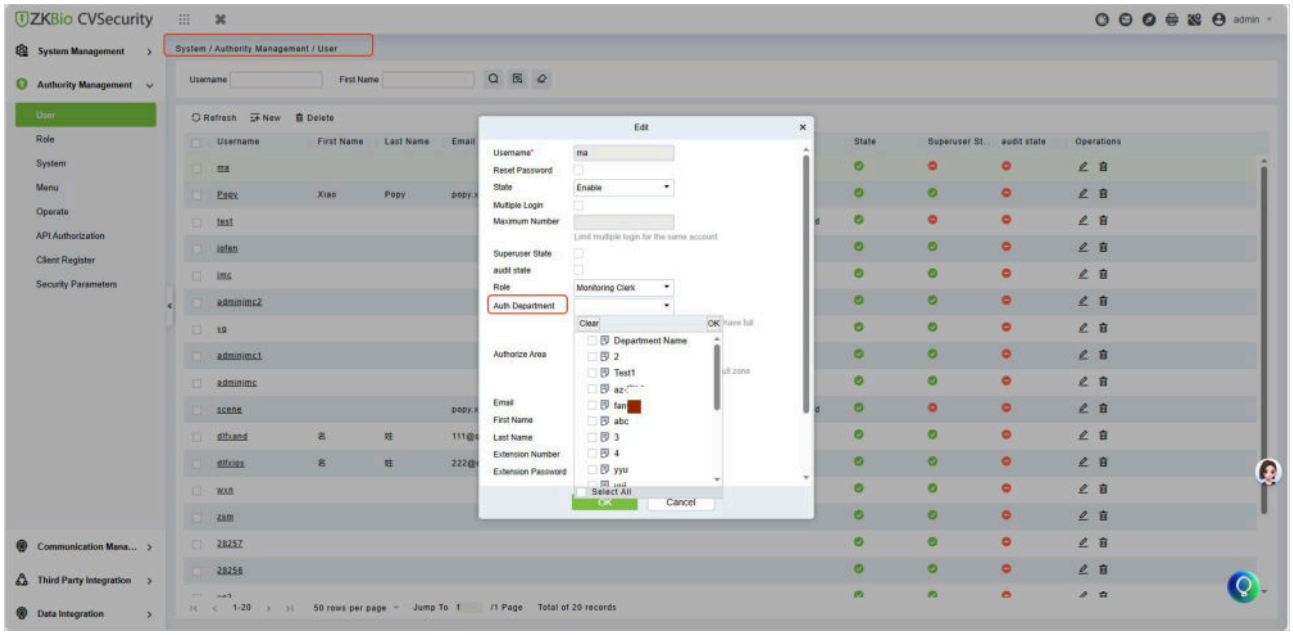
Set Automatic Registration Point: After clicking, you can select access control devices, entrance control devices, or parking equipment as automatic Registration point. When a visitor arrives, they can complete Registration and gain access at the selected automatic Registration point.

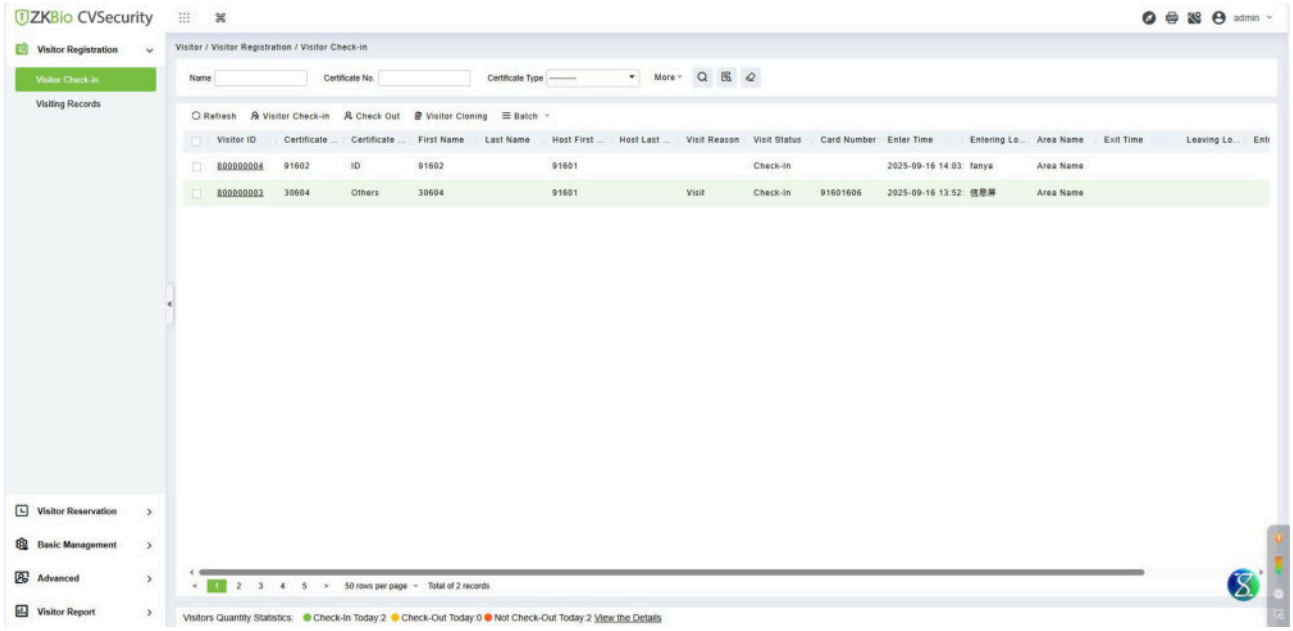
Enable Auto Check-in for the Software: When activated, the software will automatically check in the visitor 5 minutes before their scheduled visit begins.

Enable Automatic Check-in for Facekiosk Devices: When activated, visitors will be automatically checked in after registering at the visitor terminal.

- **Filter visitor reports according to user permissions. For example, User 1 can only view visitor records related to Department 1.**

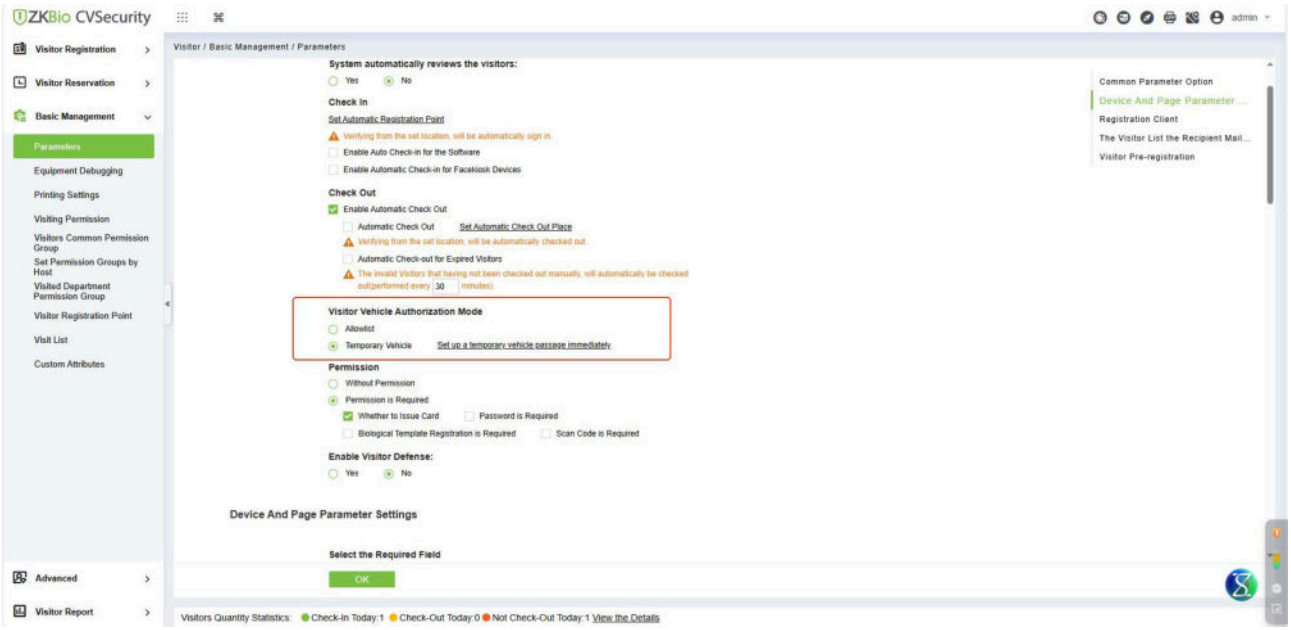
When a system user is configured with permissions limited to Department 1, both visitor registration and visitor reports will only display records related to visitors of Department 1.



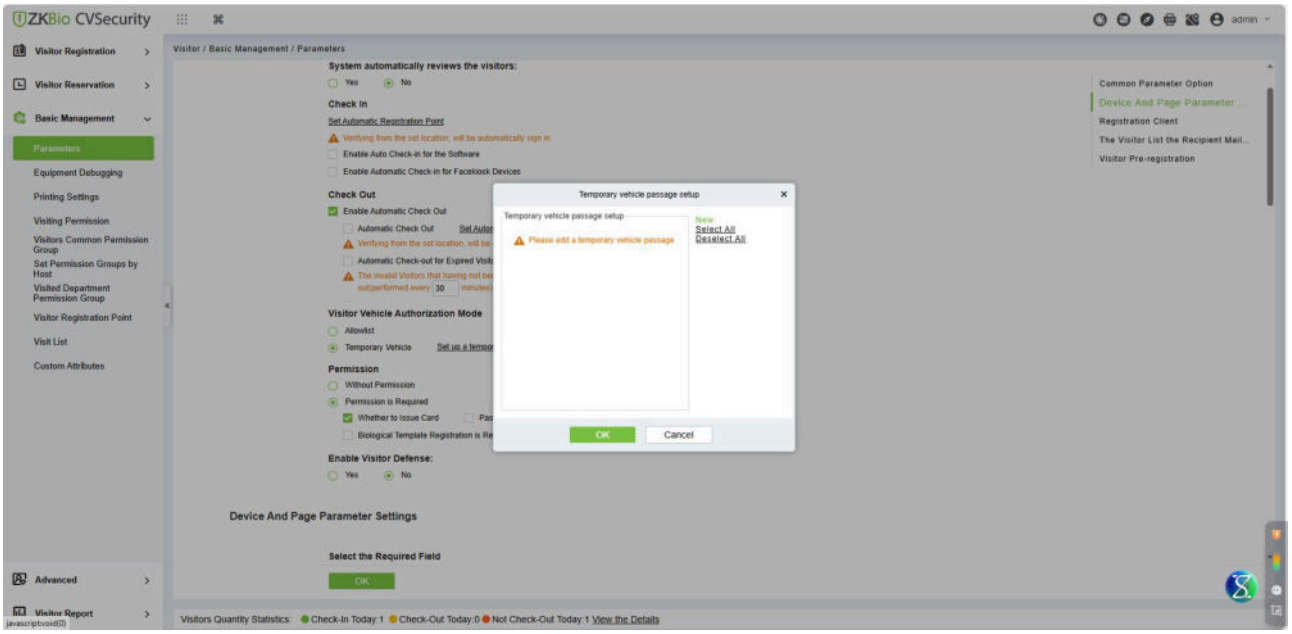


- **After a successful reservation, visitors need to authorize the corresponding parking lot area, rather than being able to enter all parking lots.**

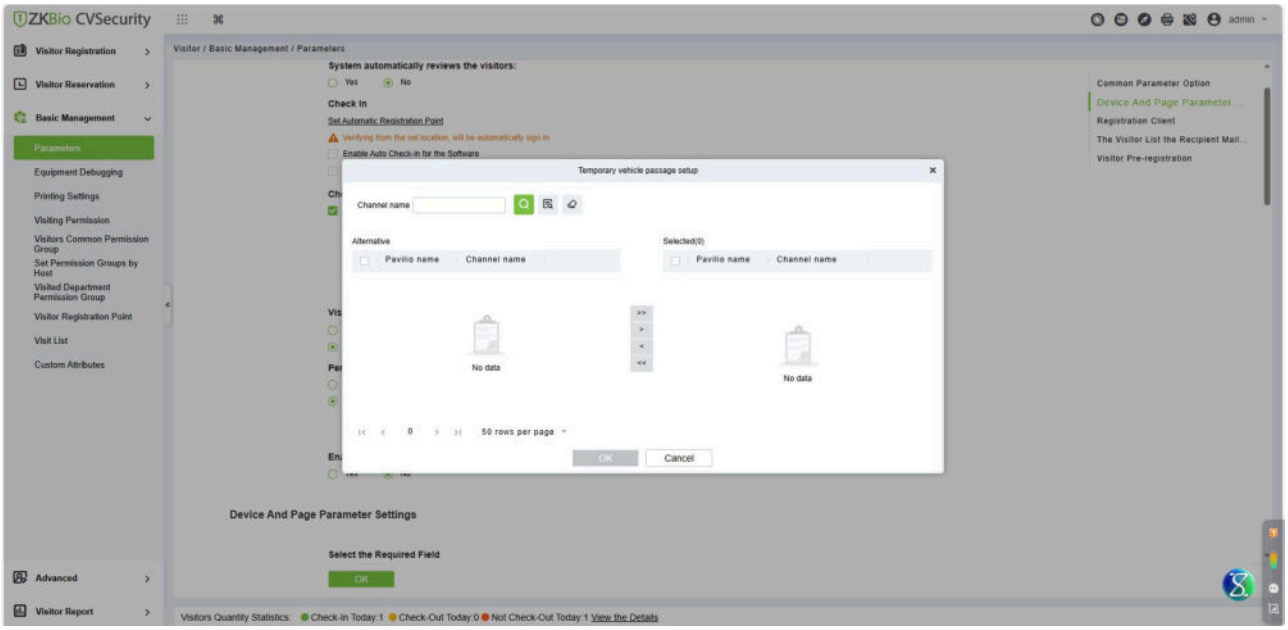
Step1: Enter Visitor → Basic Management → Parameters → Visitor Vehicle Authorization Mode.



Step2: Check the temporary vehicle option, click " Set up a temporary vehicle passage immediately".Click "New" to enter the channel selection page. Click "Select All" to check all the added temporary vehicle channels. Click "Deselect All" to uncheck all the added temporary vehicle channels. After the selection is completed, click "OK" to finish the operation.

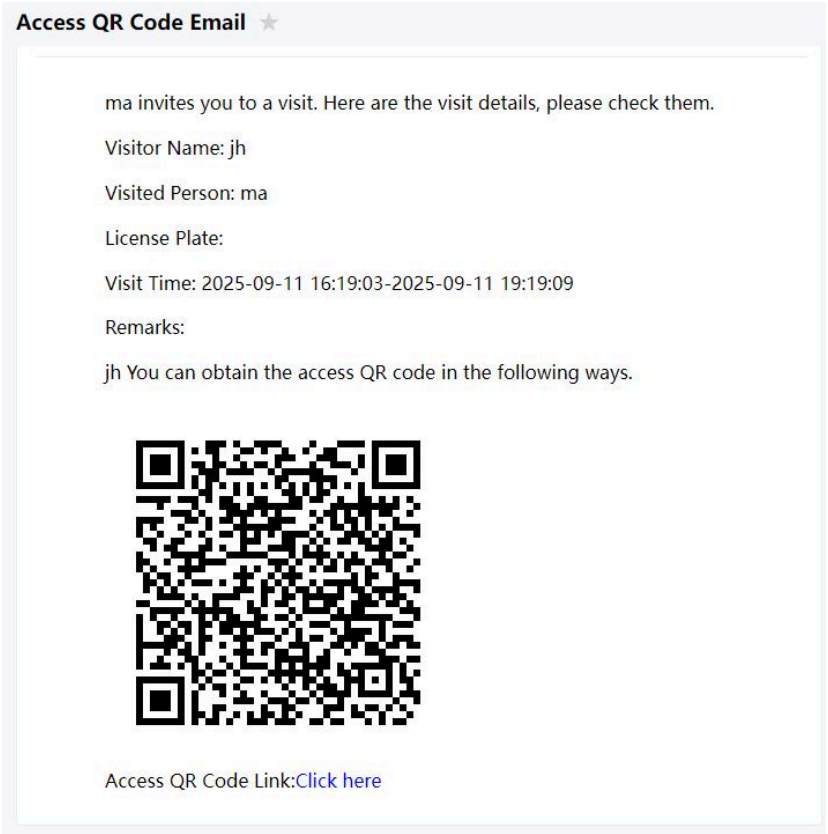


Click "New" to enter the channel selection page. Check the required channels and move them to the right. Click "OK" to complete the operation.



- **When sending a visitor invitation via the APP and selecting "Direct Access," optimize the content of the visitor email to display detailed visit information.**

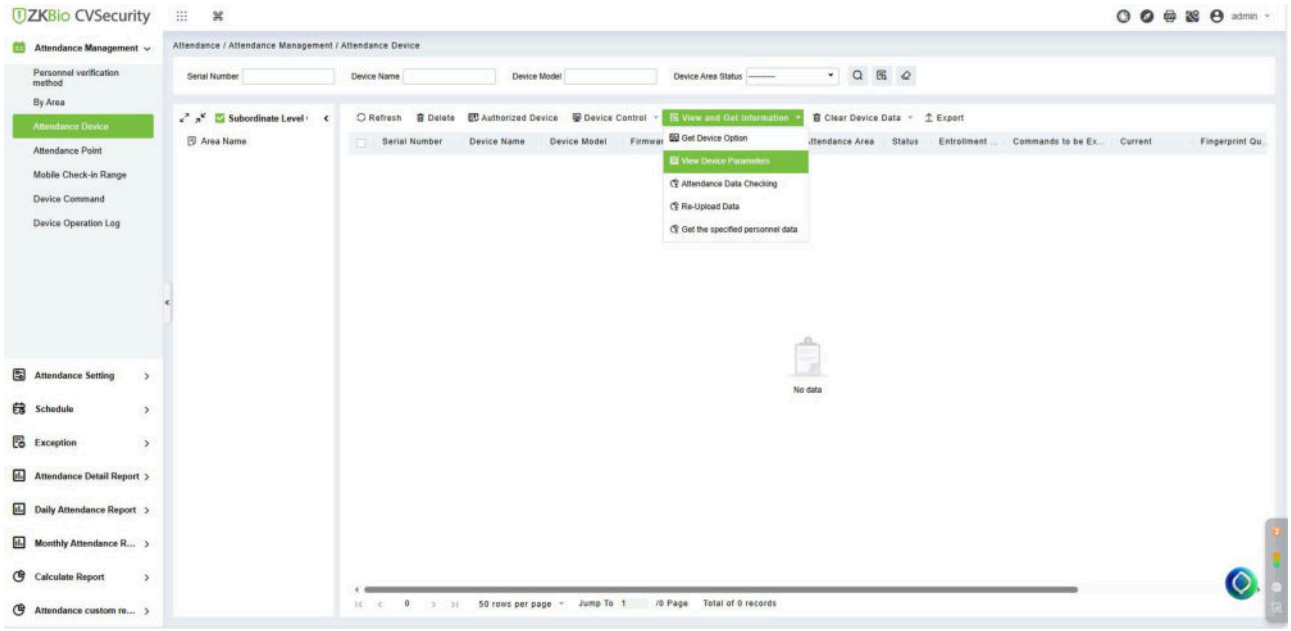
When a user logs into the APP to invite a visitor and selects "Direct Access" as the visitor type, the email content received by the visitor after a successful invitation is shown in the figure below:



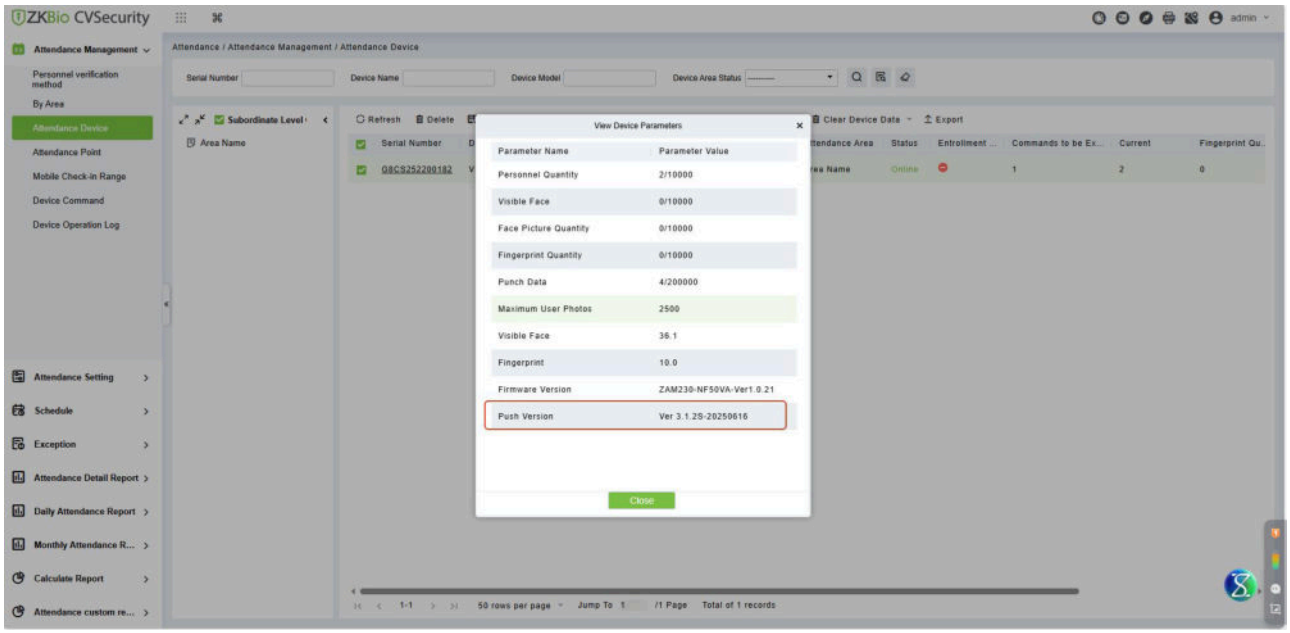
Time & Attendance

- **Add a "PUSH Version" field display in the Attendance Device Menu.**

Step: Enter Attendance → Attendance Management → Attendance Device,after checking the device, click "View and Get Information" - View Device Parameters.

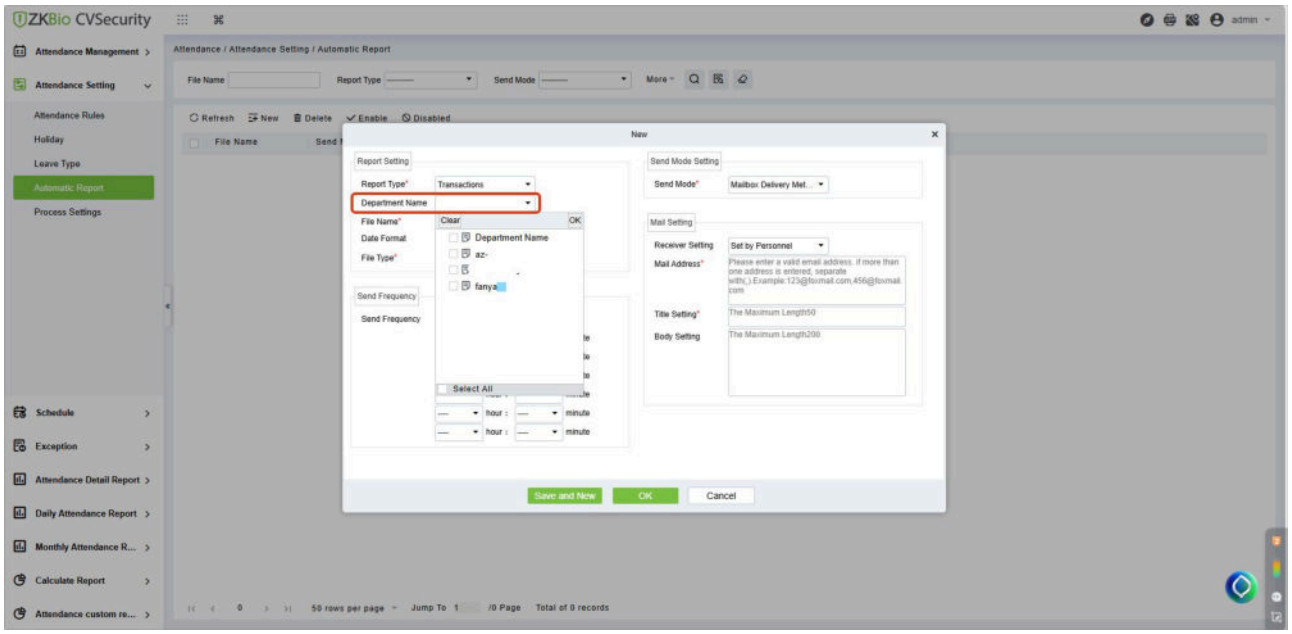


Here you can view detailed device parameters, including the Push version.



- **Automatic Report supports department selection, sending attendance records only for the selected department to recipients.**

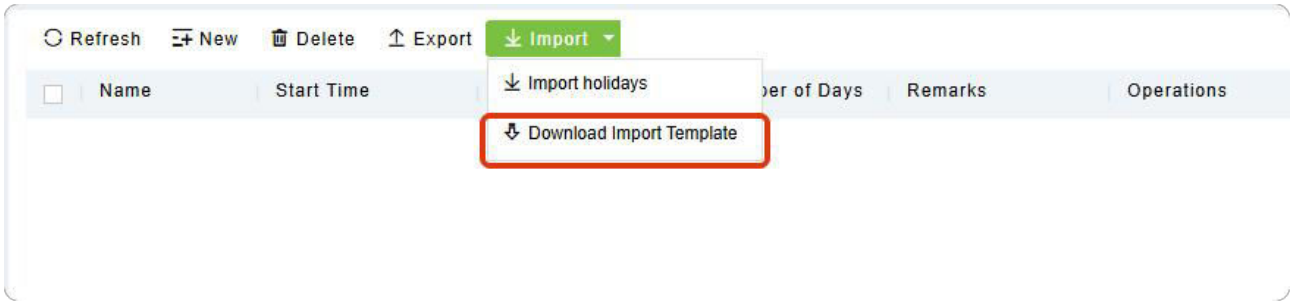
Step: Enter Attendance → Attendance Setting → Automatic Report, click "New", and in the Report Settings column, you can select the department name. After selection, only the attendance records of the selected department will be pushed to the recipients.



- **The holiday settings for attendance module now support batch import and export.**

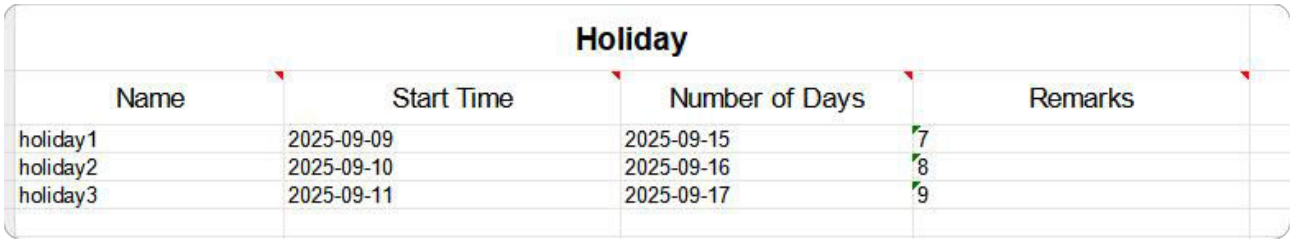
- **Import:**

Step 1: Enter Attendance → Attendance Setting → Holiday.Select and click the "**Import->Download Import Template**" button,download the template "Holiday Template.xls" locally.



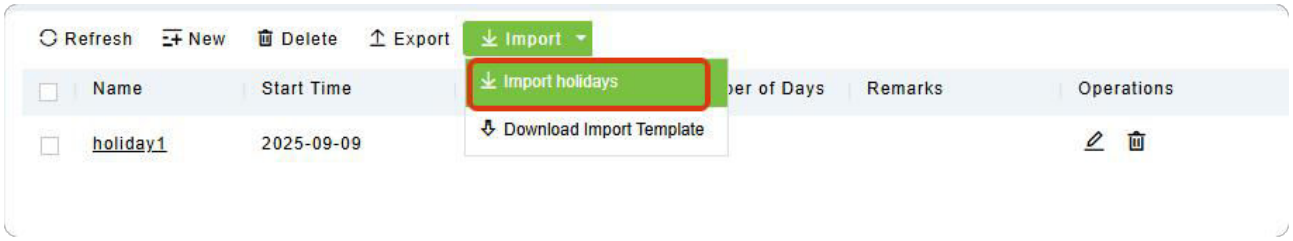
Step 2: Open the exported template file "Holiday.xls" for adding holiday information.

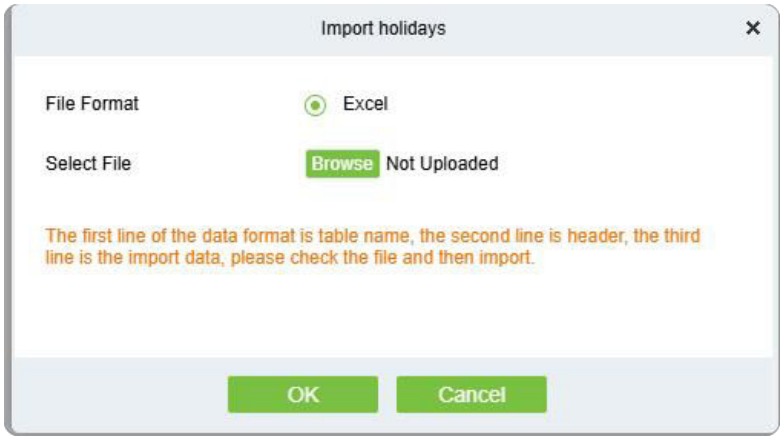
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.



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

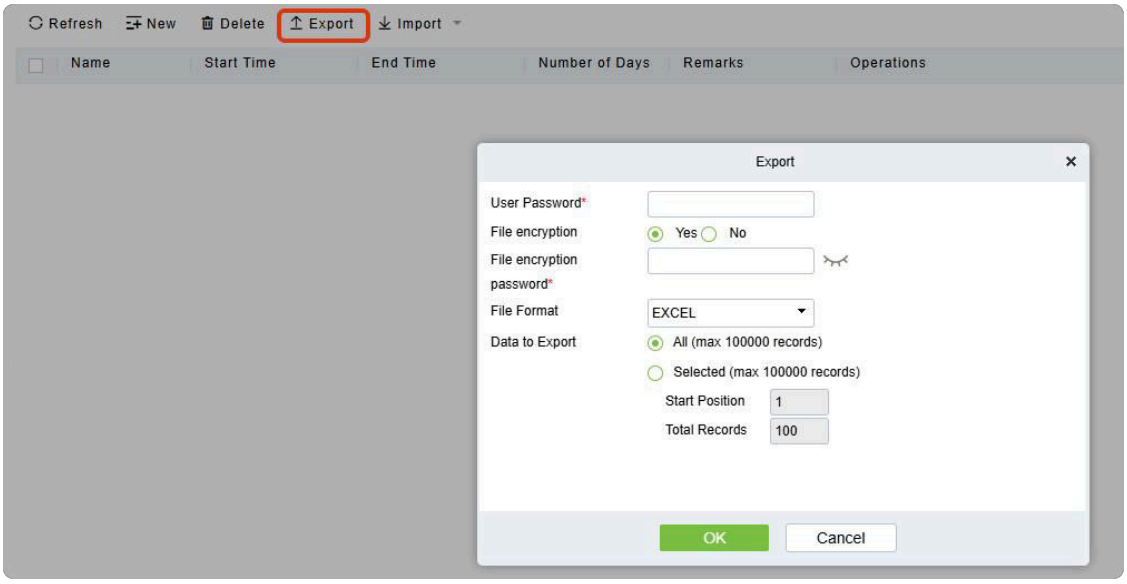
Step 4: Select and click the "**Import**" button; click the "**Browse**" button to import the batch import template into the system and click OK, as shown in figure below.





■ Export:

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

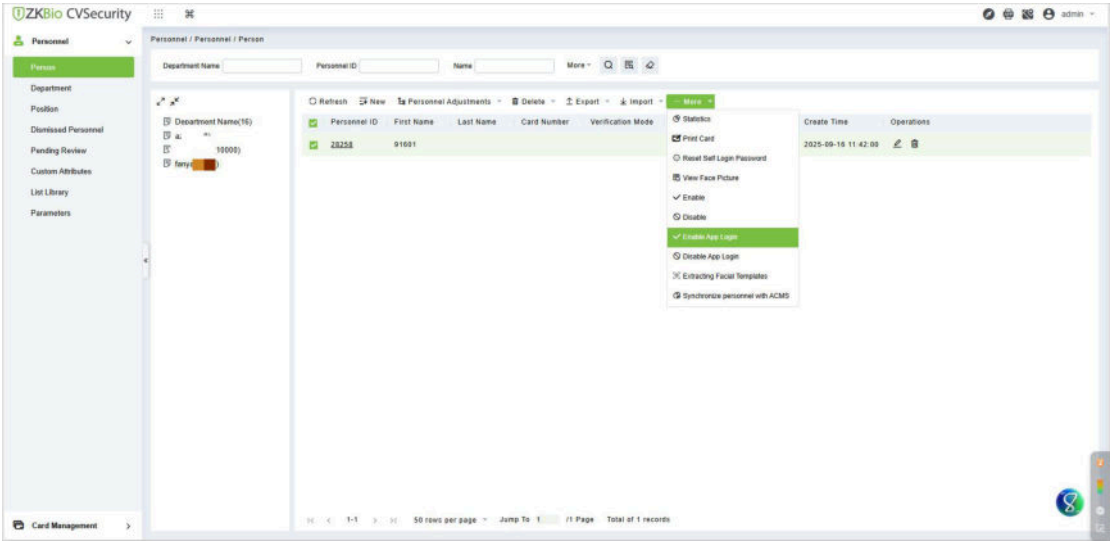


Holiday				
Name	Start Time	End Time	Number of Days	Remarks
holiday1	2025-09-09	2025-09-15	7	

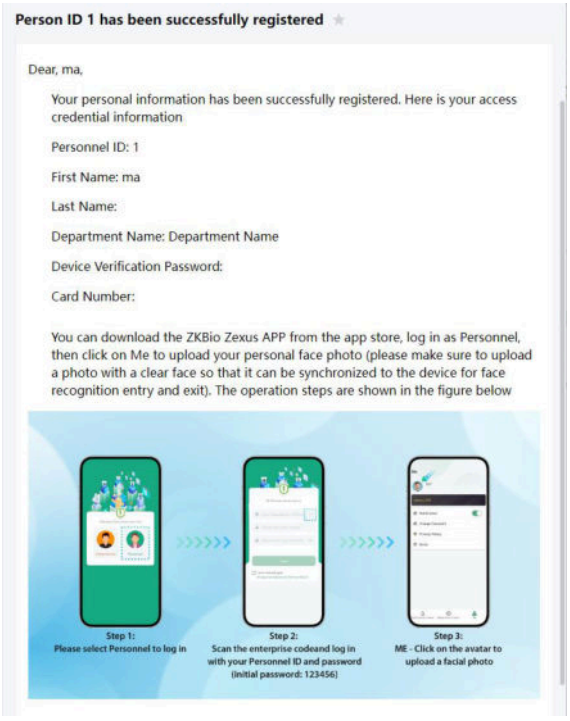
Personnel

- **After selecting personnel, enabling the "APP Log In" feature will automatically send an email to the individual with instructions on how to use the app.**

Step: Enter Personnel → Employee List, after selecting the corresponding employee and clicking "More" → "Enable APP Login", the system will automatically send an email notification to the selected individual.



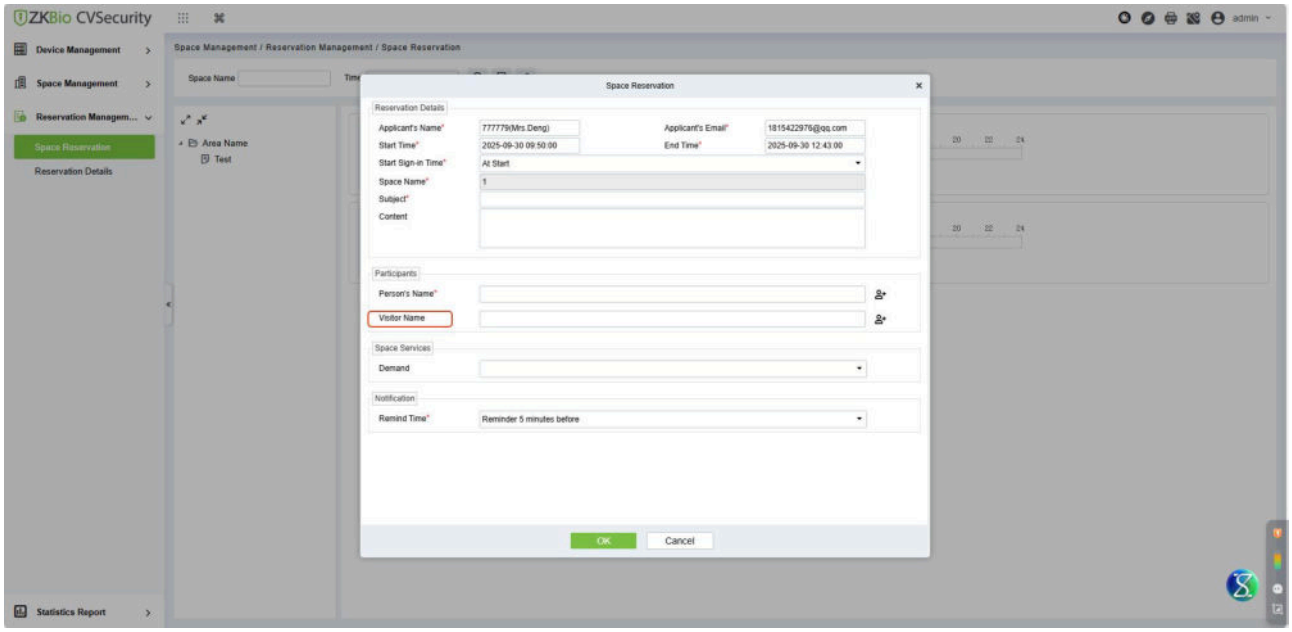
The content of the email notification is as shown in the figure below: The employee can directly follow the guidance in the email to begin using the app login.



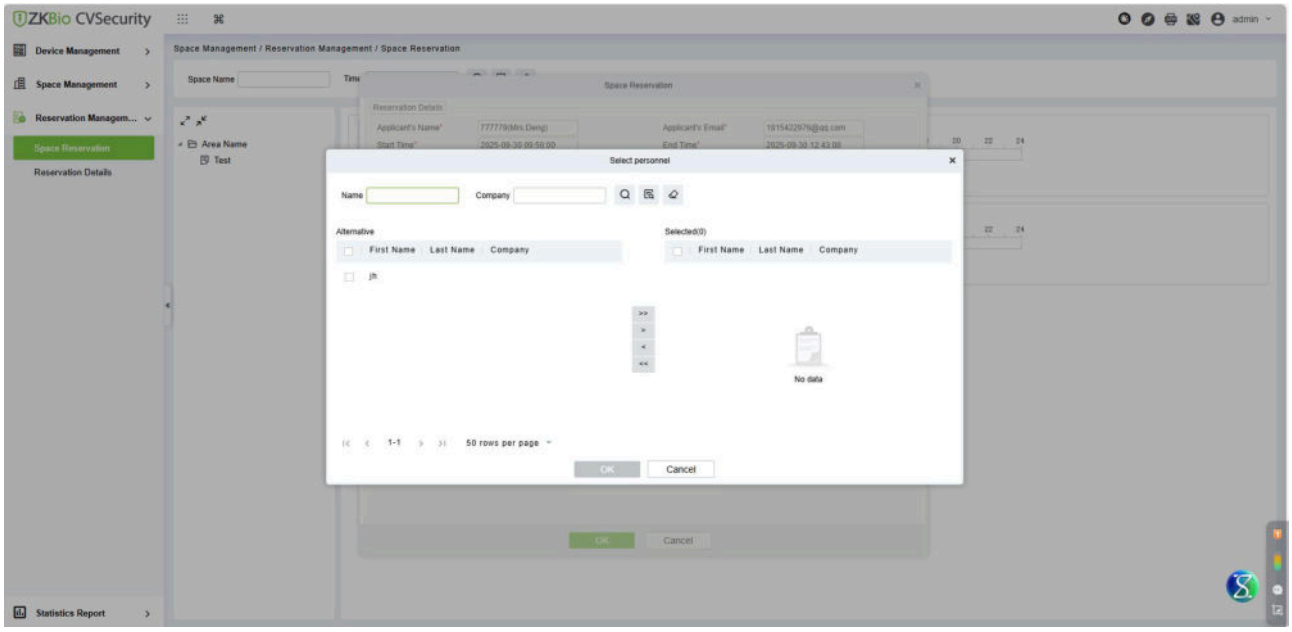
Space Management

- **Space reservations allow visitors to be selected as attendees.**

Step1: Enter Space Management → Reservation Management→ Space Reservation. When clicking on Space to make a reservation, you can click the icon on the right in the visitor name field of the Participants column to add a visitor.



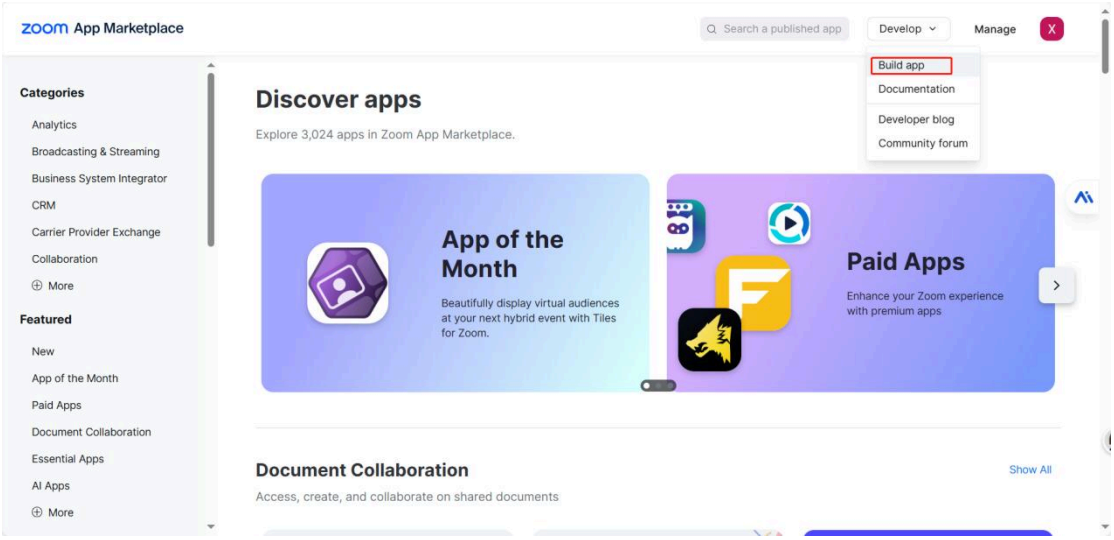
Step2: After selecting the visitor, move it to the right and click "OK" to complete the operation.



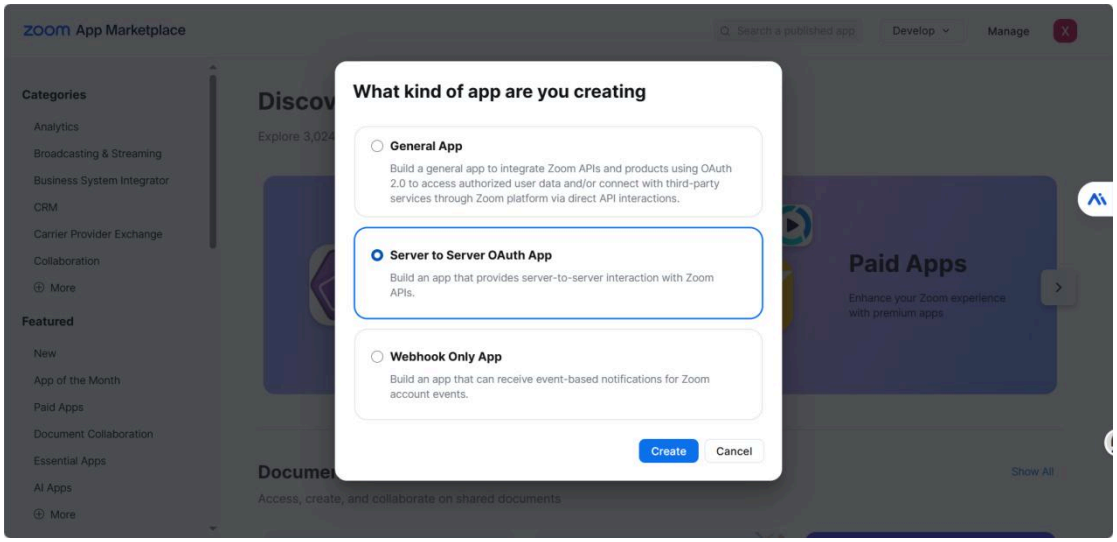
Note: The types of visitors who can be selected as attendees are those who have made an reservation or check-in.

- **Zoom Integration-Supports binding one Zoom ID to each meeting room, automatically generating meeting links for app-based reservations.**

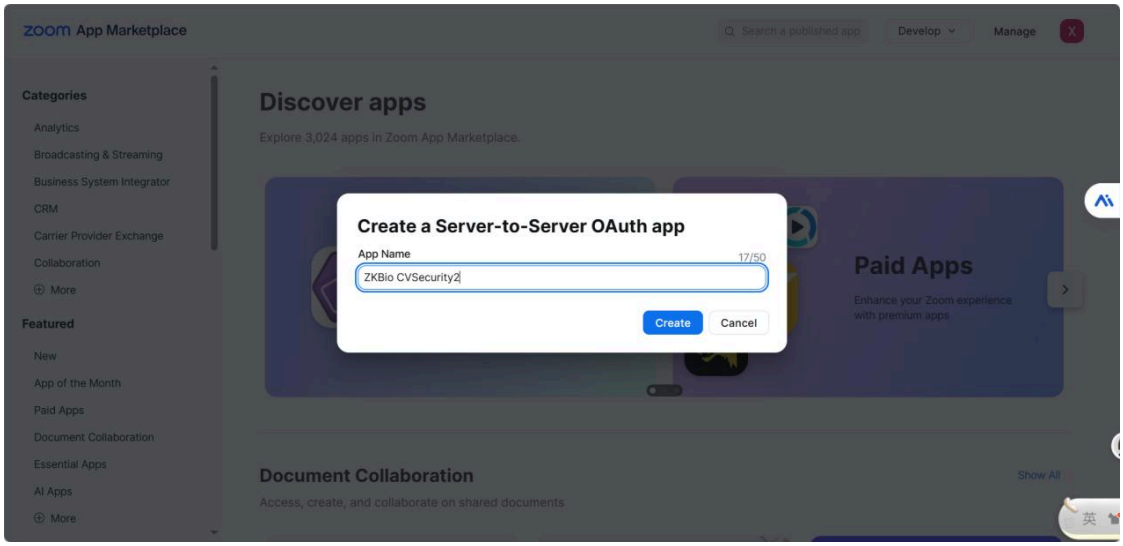
Step1: Open the App Marketplace and log in; after logging in, click **Build app.**



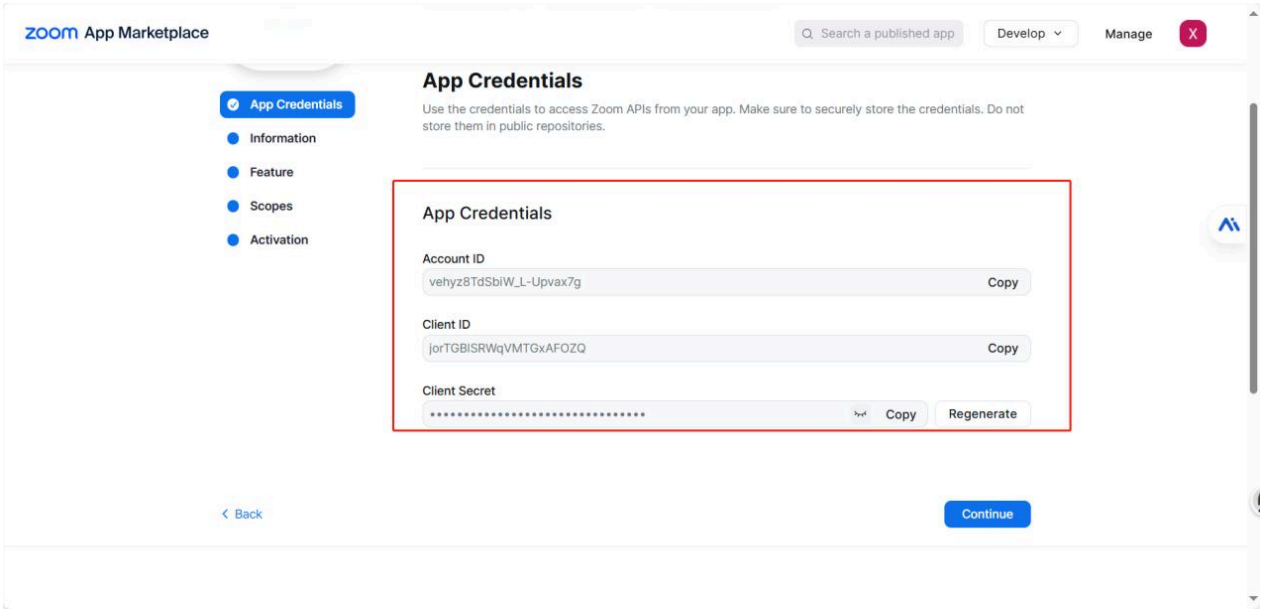
Step2: Select **Server to Server OAuth App** and create App Name.



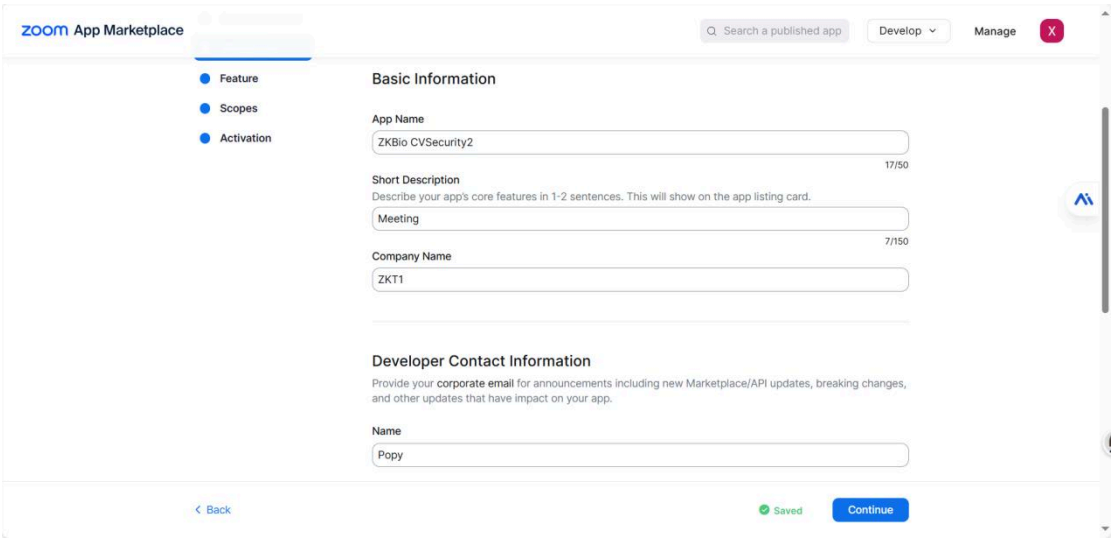
Enter the app name.



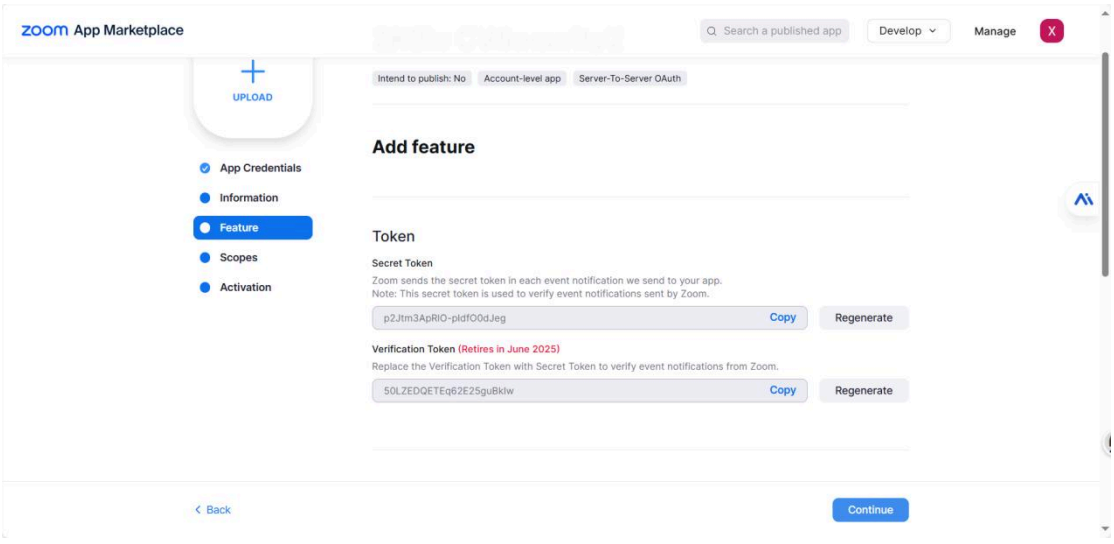
Step3: After creation, APP Credentials will appear.Click "Continue" to proceed to the next step.



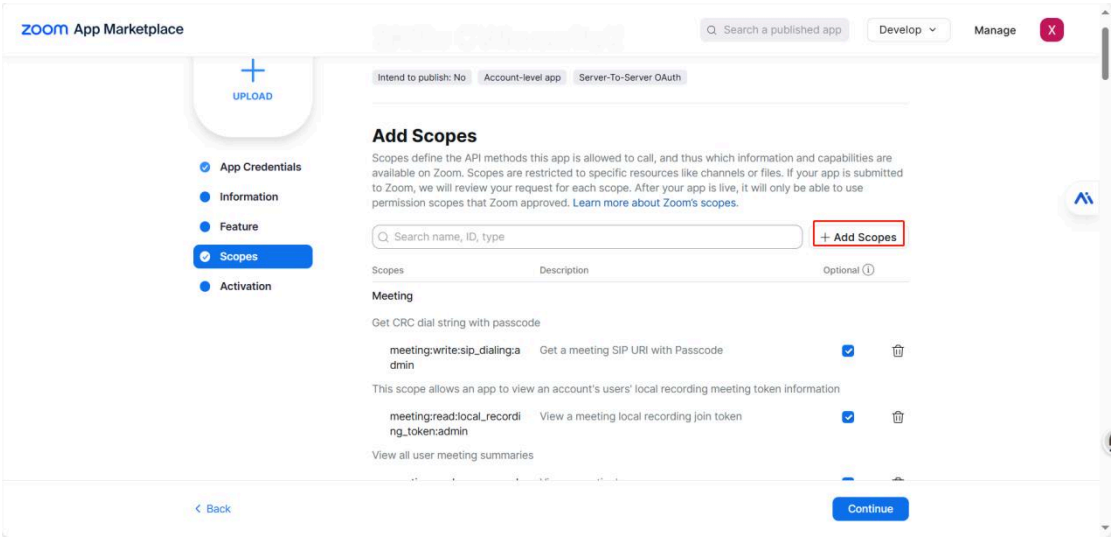
Step4: Fill in all the blanks in Basic Information and click "Continue".



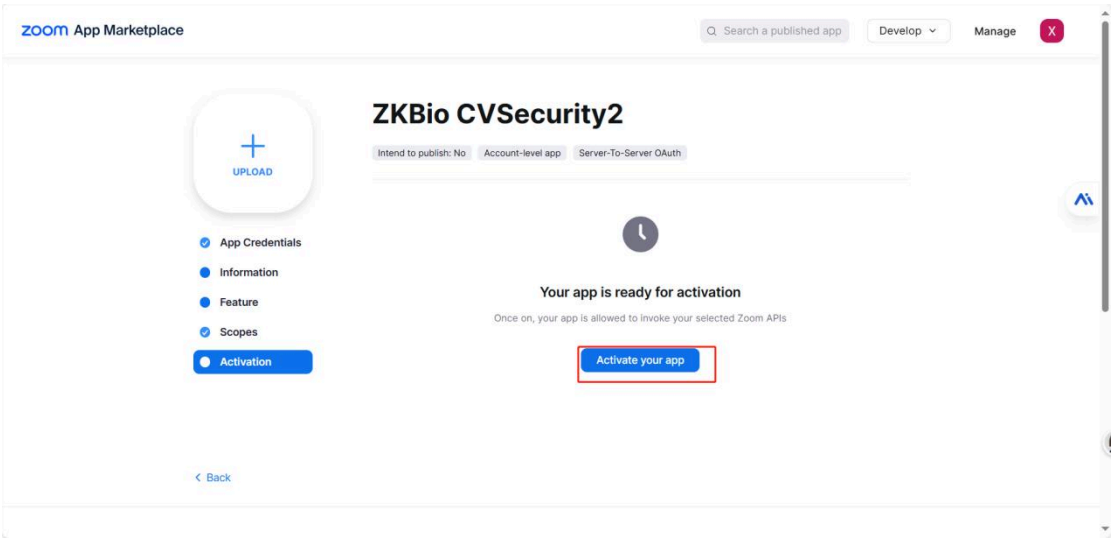
Step5: Add Features :This page does not need to be operated. Click "Continue".



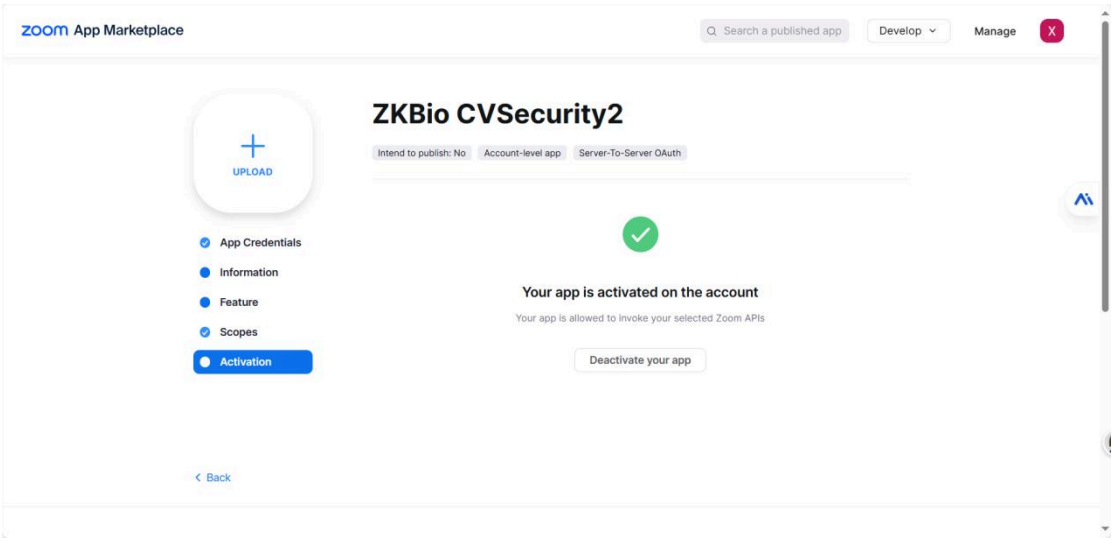
Step6: Click "Add Scopes", select Meeting, and check the required Scopes as needed. Click "Continue".



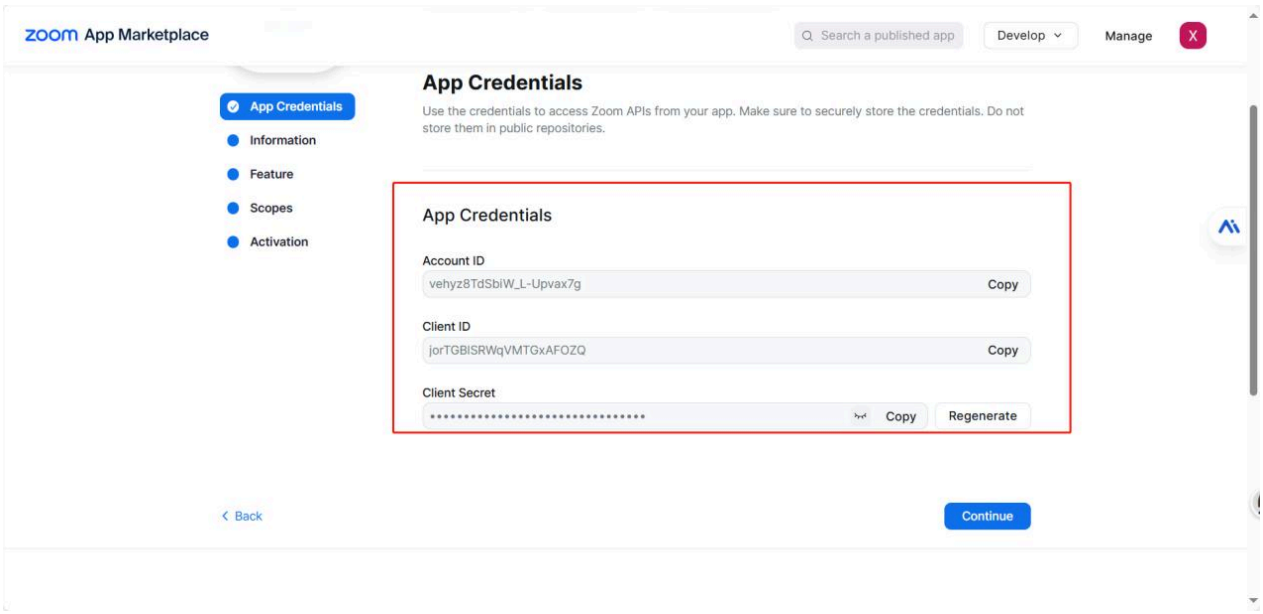
Step7: Then click "Activate your app".



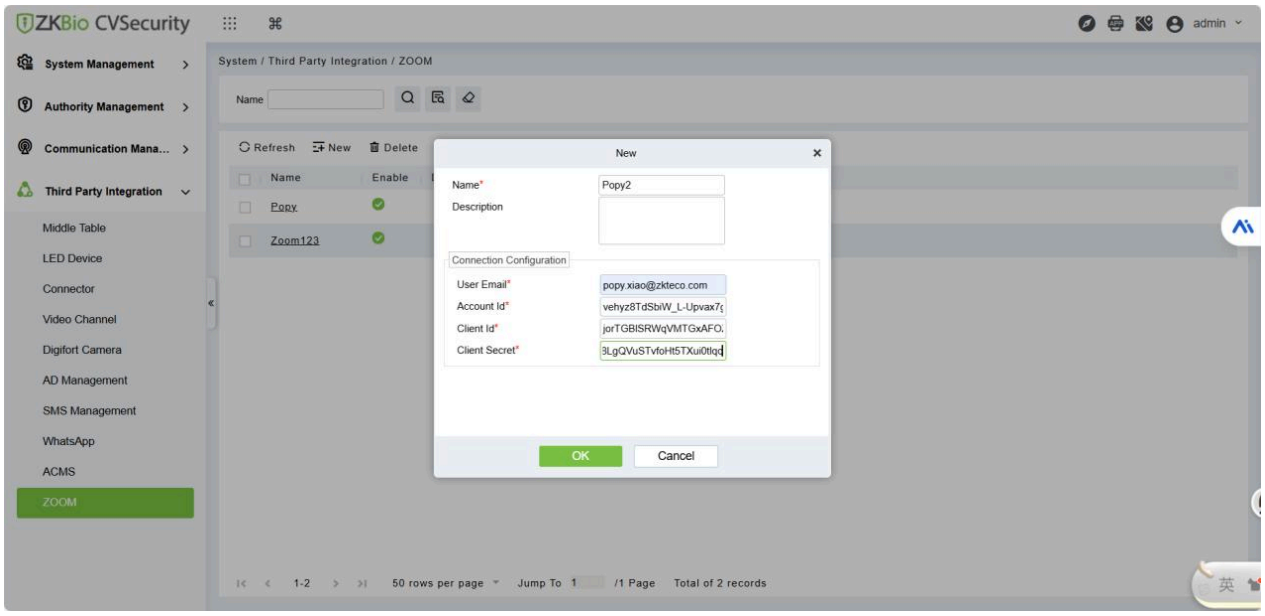
Until the display activation is successful.



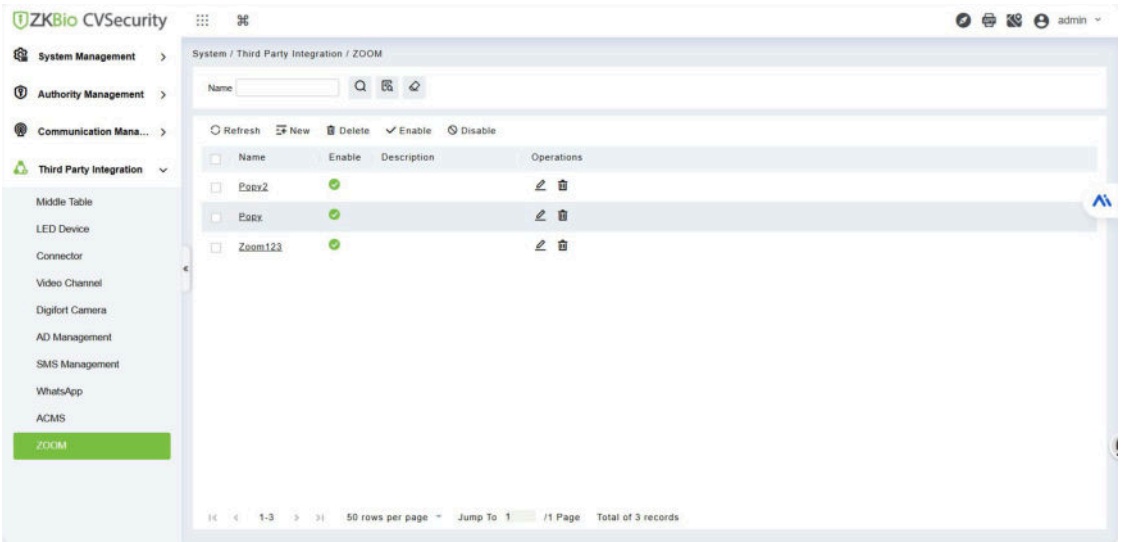
Step8: Then go back to the **APP Credentials** and copy the values in this field to **ZKBio CVSecurity-System-Third Party Integration-ZOOM** configuration page.



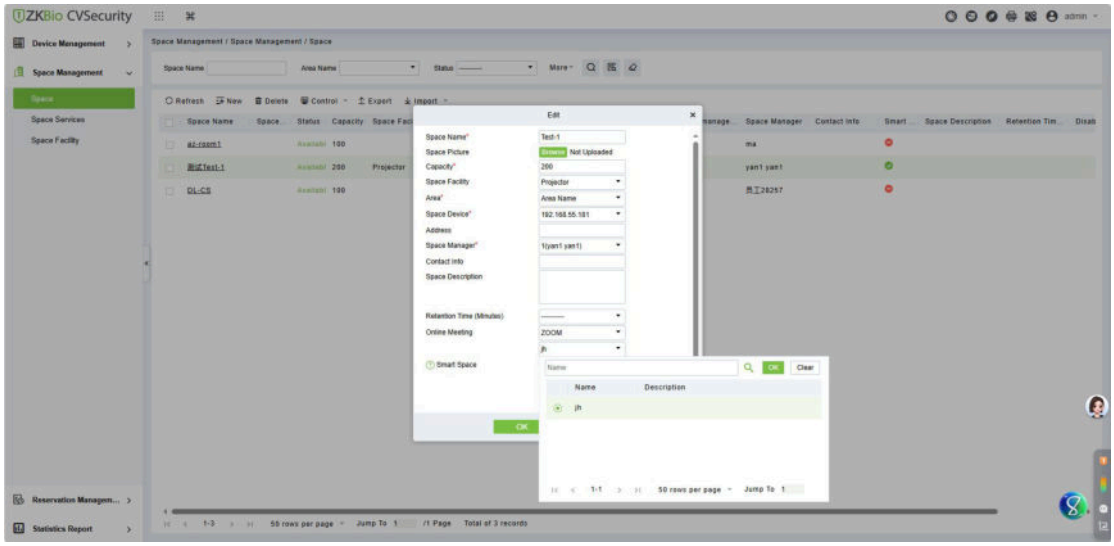
Click "New", copy the corresponding ID, paste it in, and then click "OK".



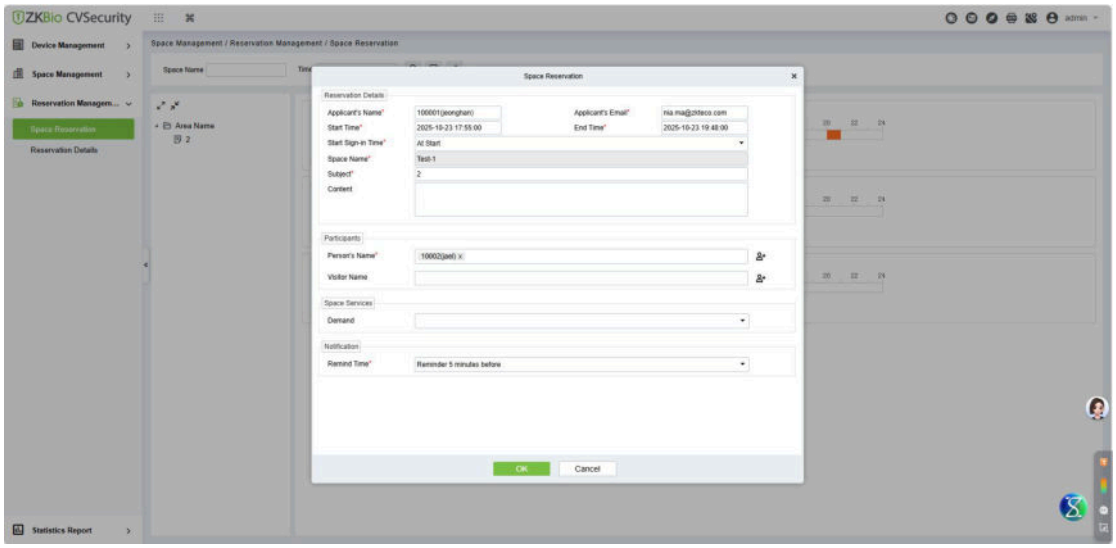
Click "OK" to return Operation Succeed.



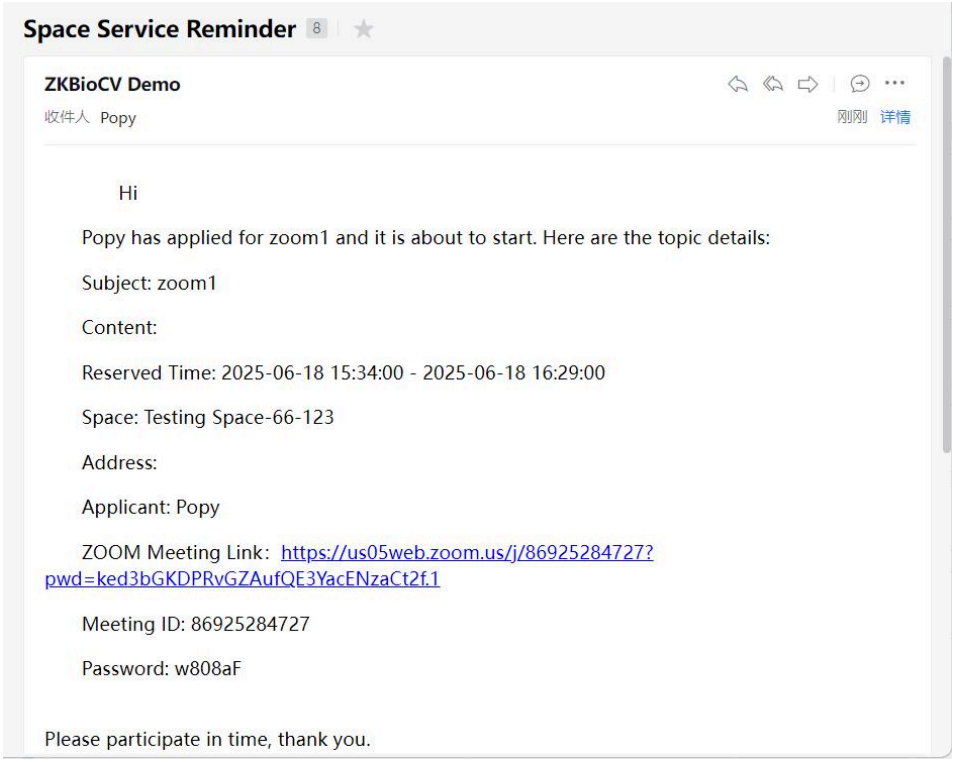
Step9: Now, you can go to the **Space Management module-Space**, click "New" to add a meeting room, you can select the corresponding meeting room resource from Zoom.Fill in the basic information , then select the Zoom App you have created in Create an online meeting, and finally click "OK".



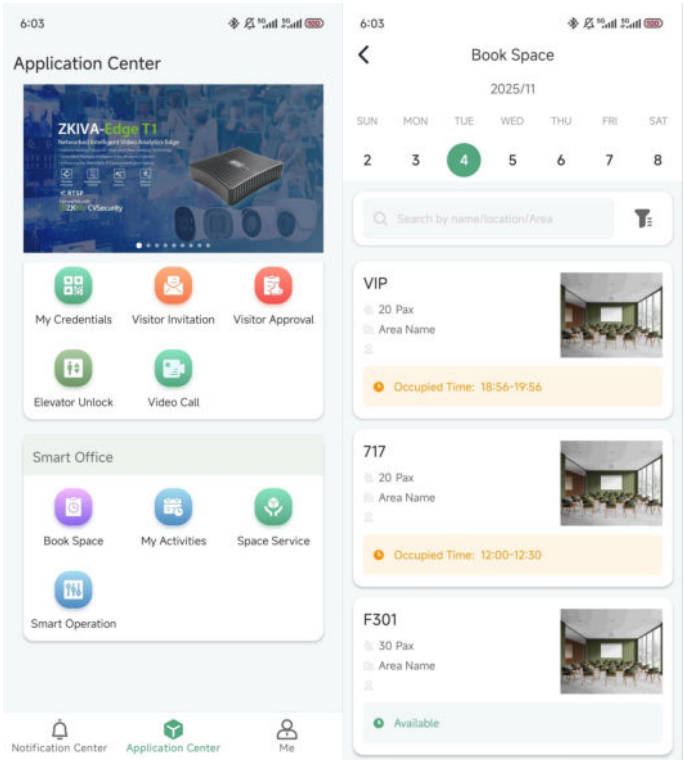
Step10: You can go to the **Reservation Management module-Space Reservation**, click the conference to start booking the meeting.



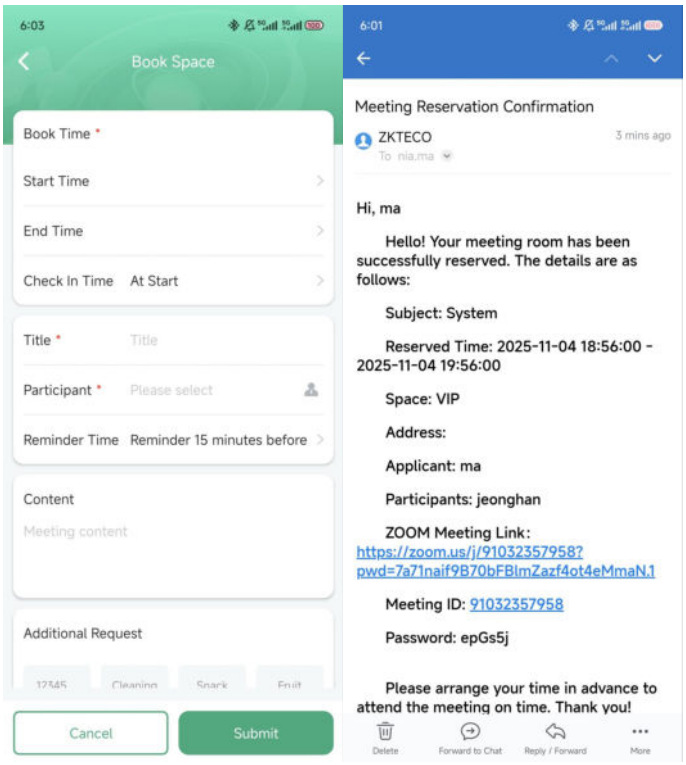
The corresponding participants will receive the online meeting link with Zoom in the corresponding meeting reservation information.



Step11: You can use the mobile APP to book a meeting.Select a meeting room integrated with Zoom and fill in the relevant information to complete the reservation.



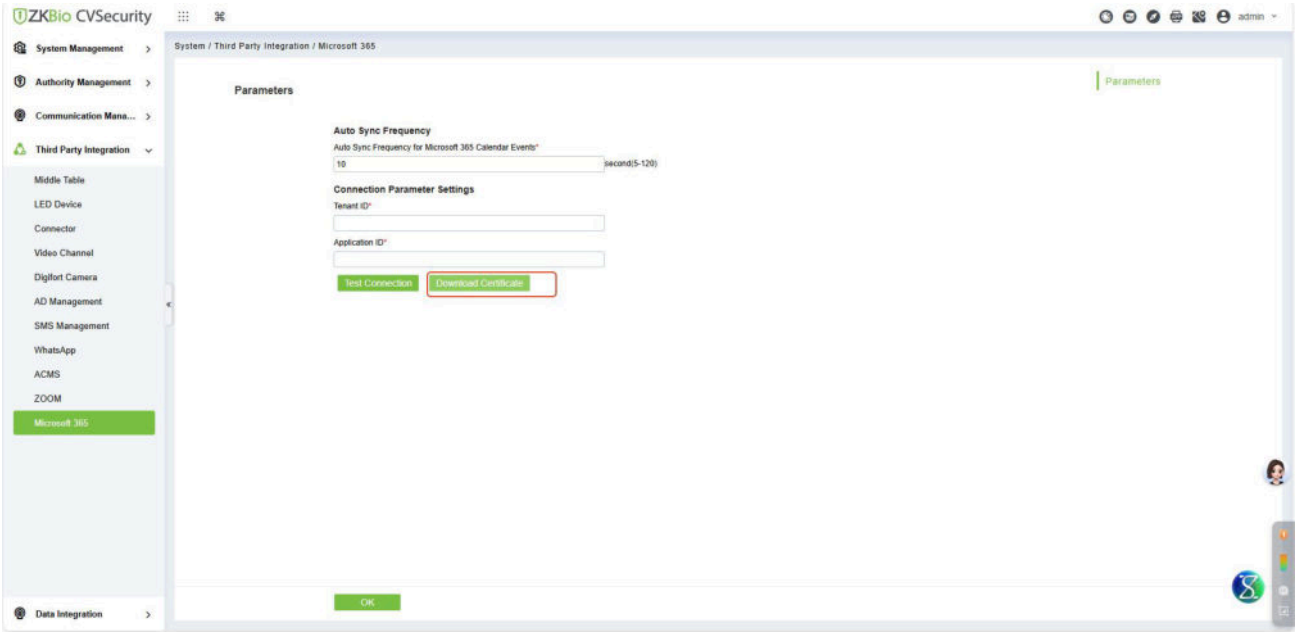
The corresponding participants will receive the online meeting link with Zoom in the corresponding meeting reservation information.



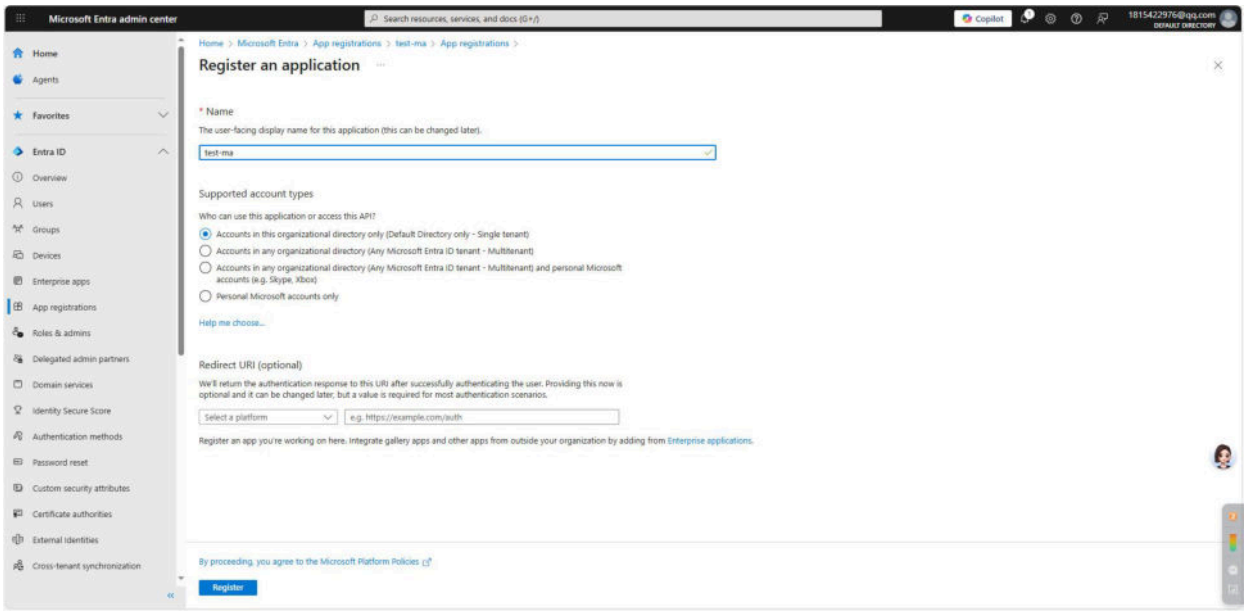
- **Microsoft 365 integration synchronizes Teams / Outlook meeting reservations with conference room devices.**

1. Register Application:

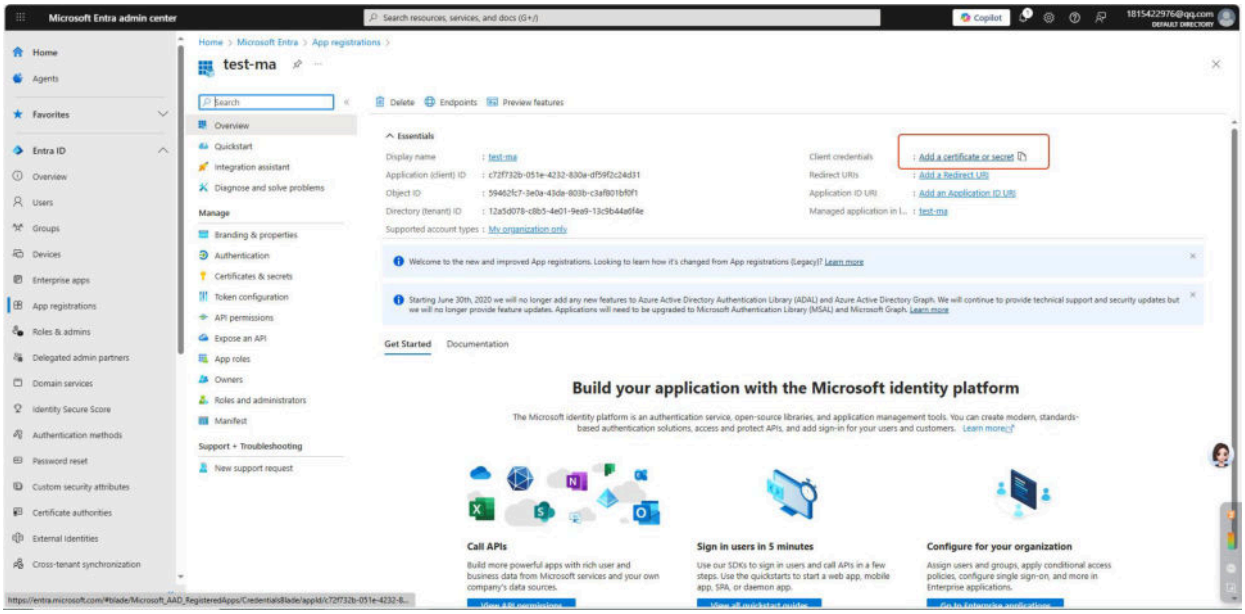
Step1: Enter System → Third Party Integration → Microsoft 365, click "Download Certificate" to download the certificate on the ZKBio CVSecurity platform.



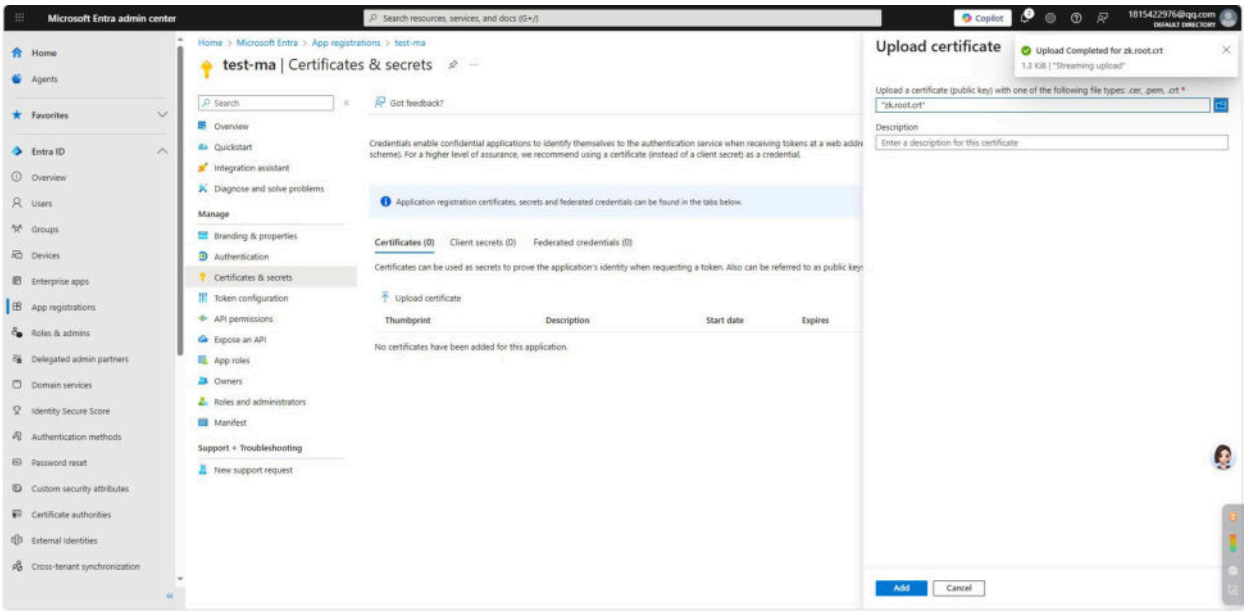
Step2: Enter the Microsoft Entra admin center, click "App registrations" → "New registration", and add a new application.Fill in the relevant information and click "Register".



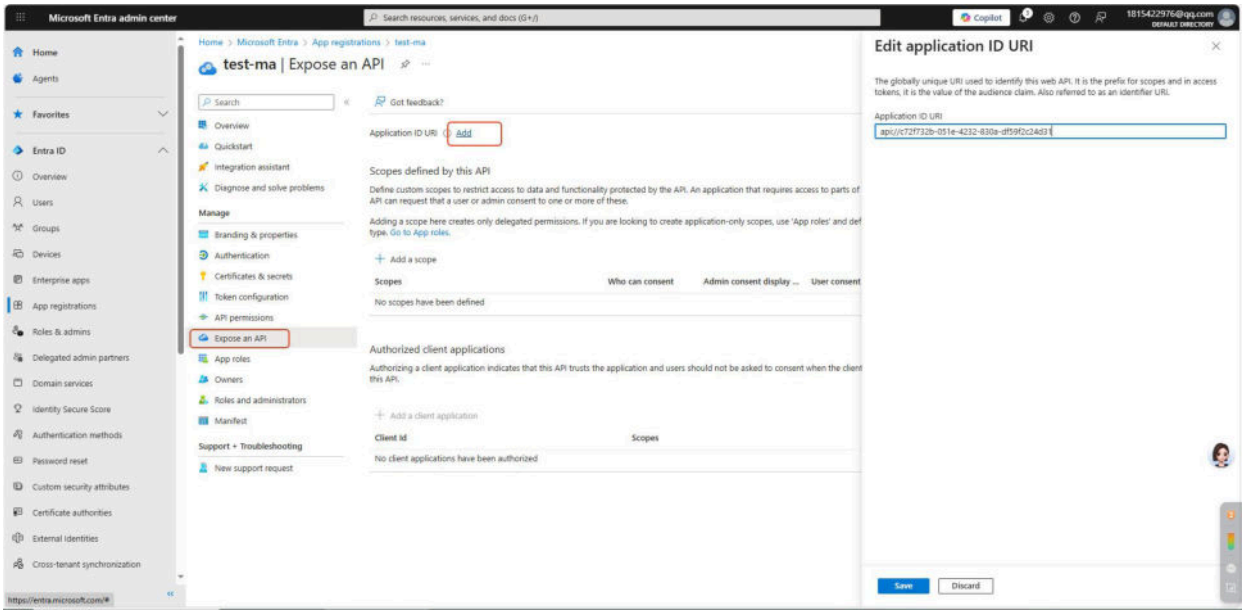
Step3: Enter Overview and click "Add a certificate or secret".



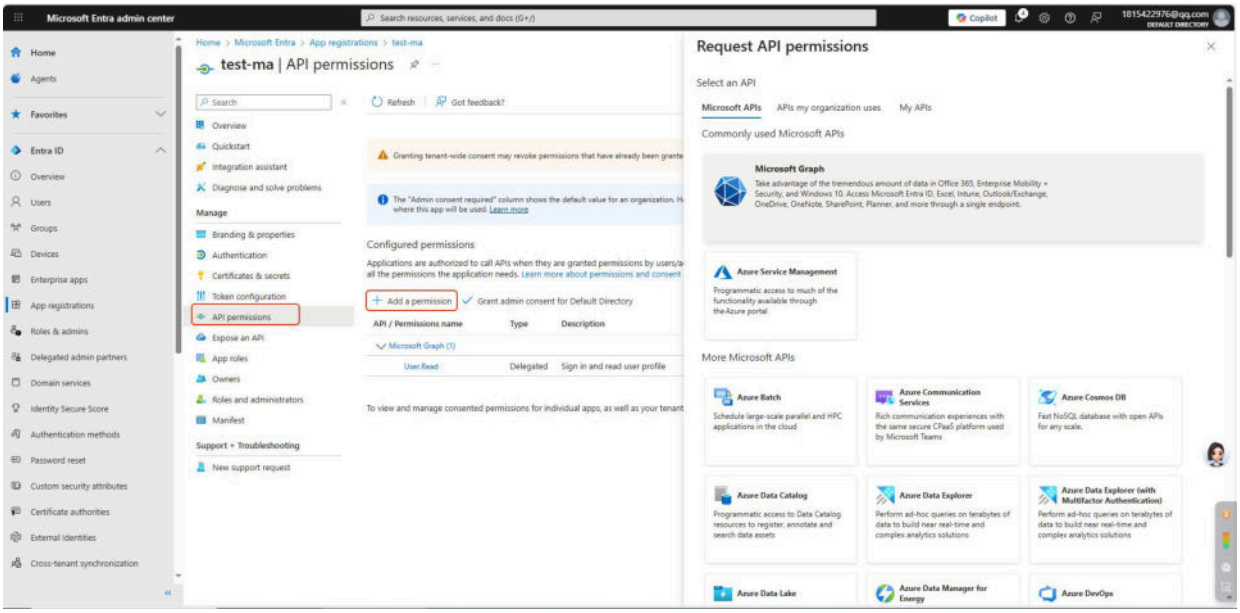
Click "Certificates" - "Upload certificate", and upload the certificate file that has been added in ZKBio CVSecurity.



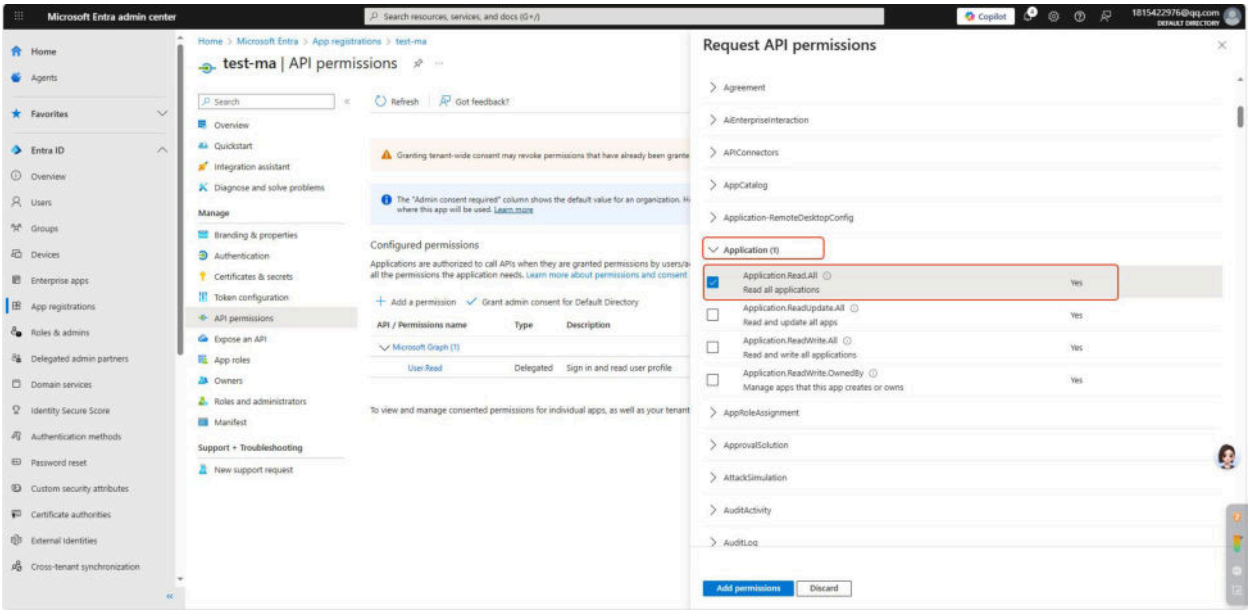
Step4: Enter Expose an API and click "Add" next to Application ID URI.



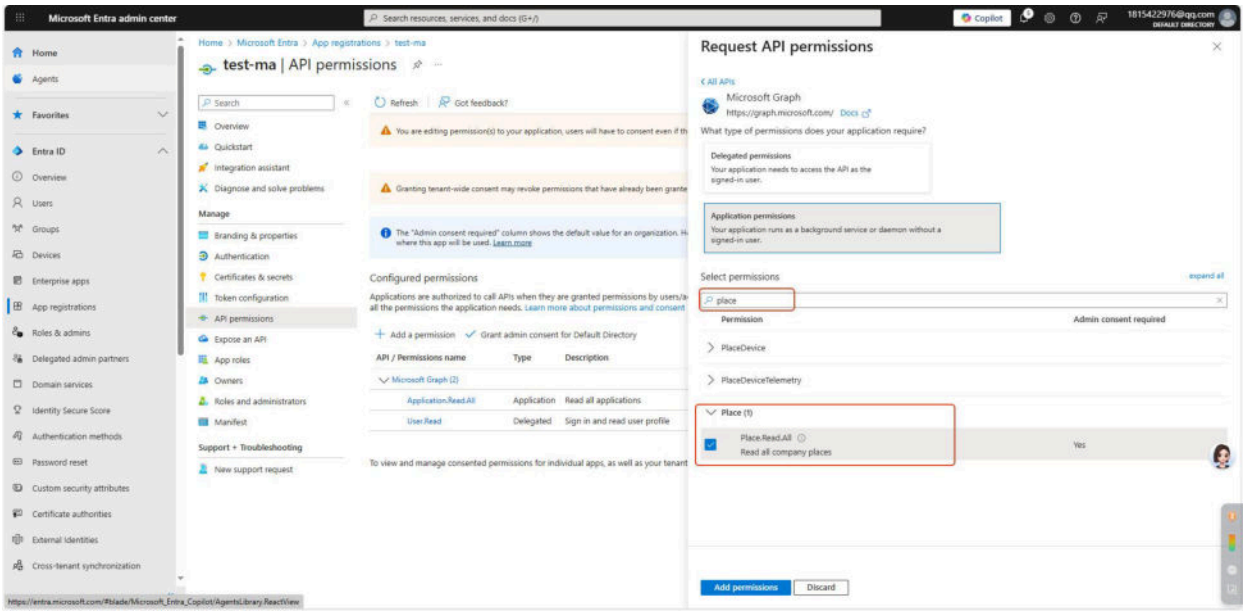
Step5: Enter API permissions and click "Add a permission"→"Microsoft API"→"Microsoft Graph".



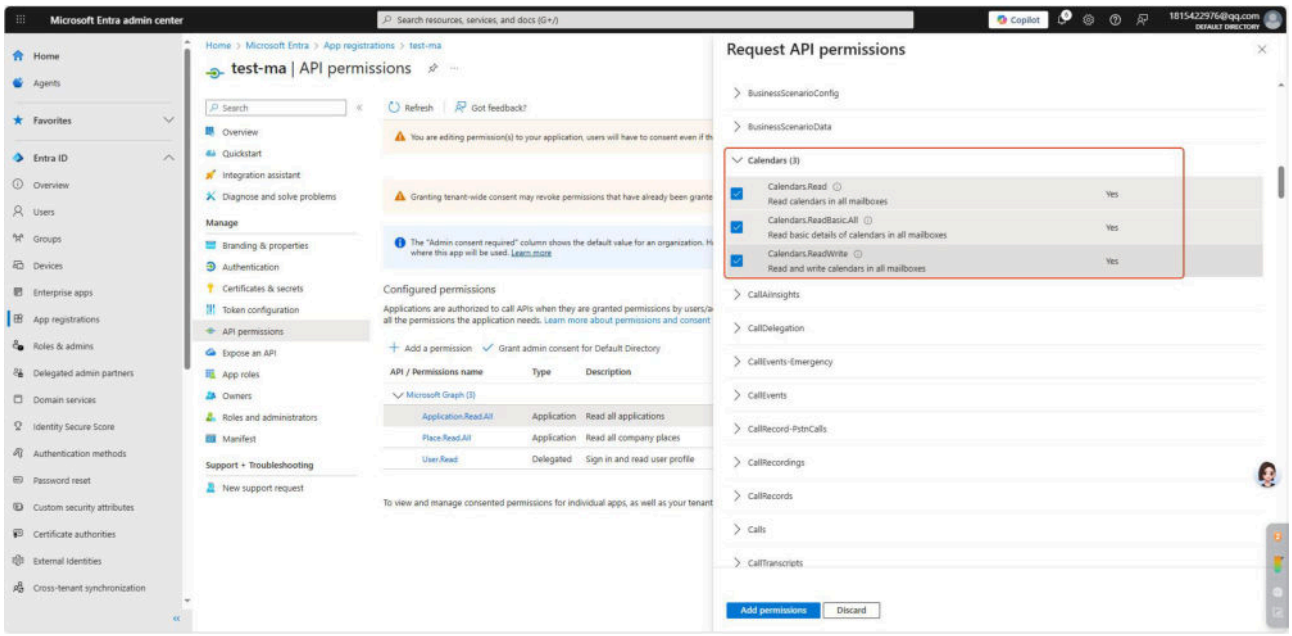
Check the "Application.Read.All" and click "Add a permission".



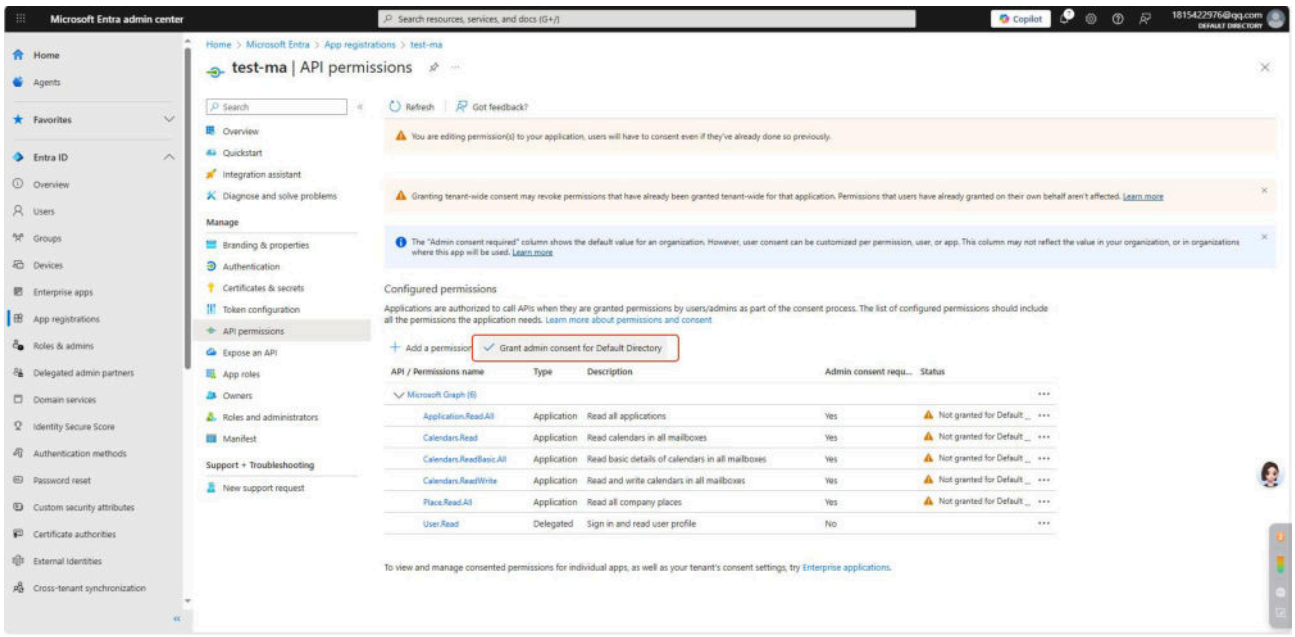
Check the "Place.Read.All" and click "Add a permission".



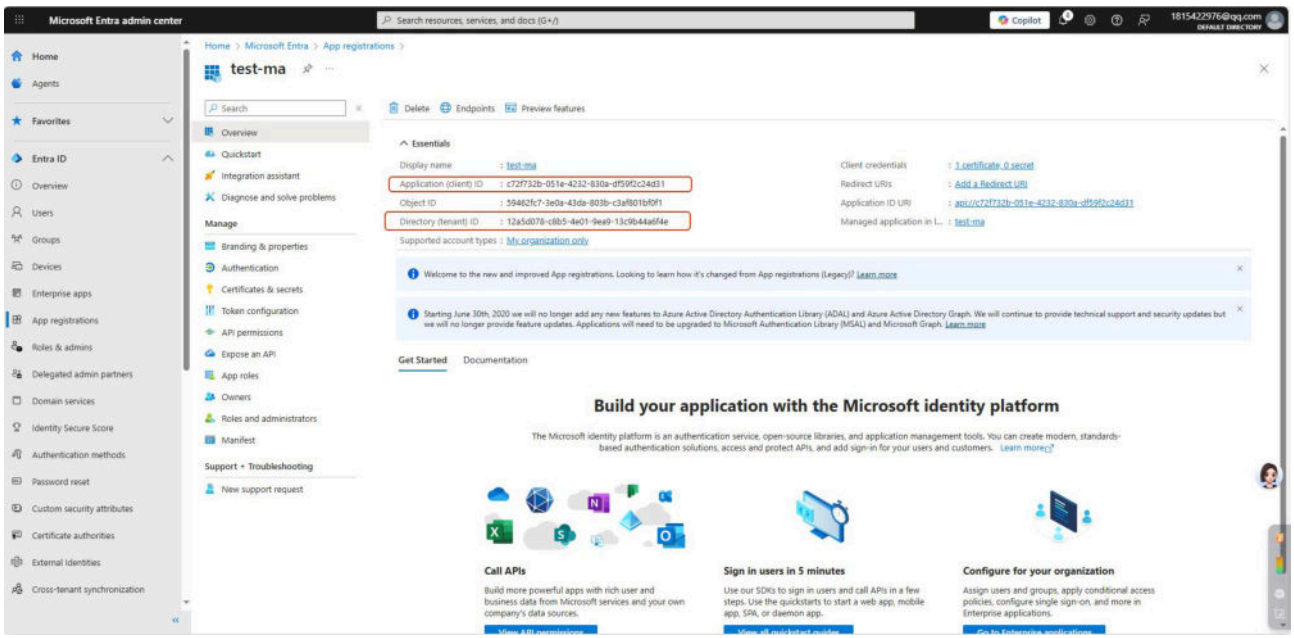
Check the "Calendars.Read.","Calendars.ReadBasic.All"and"Calendars.ReadWrite".Then click "Add a permission".



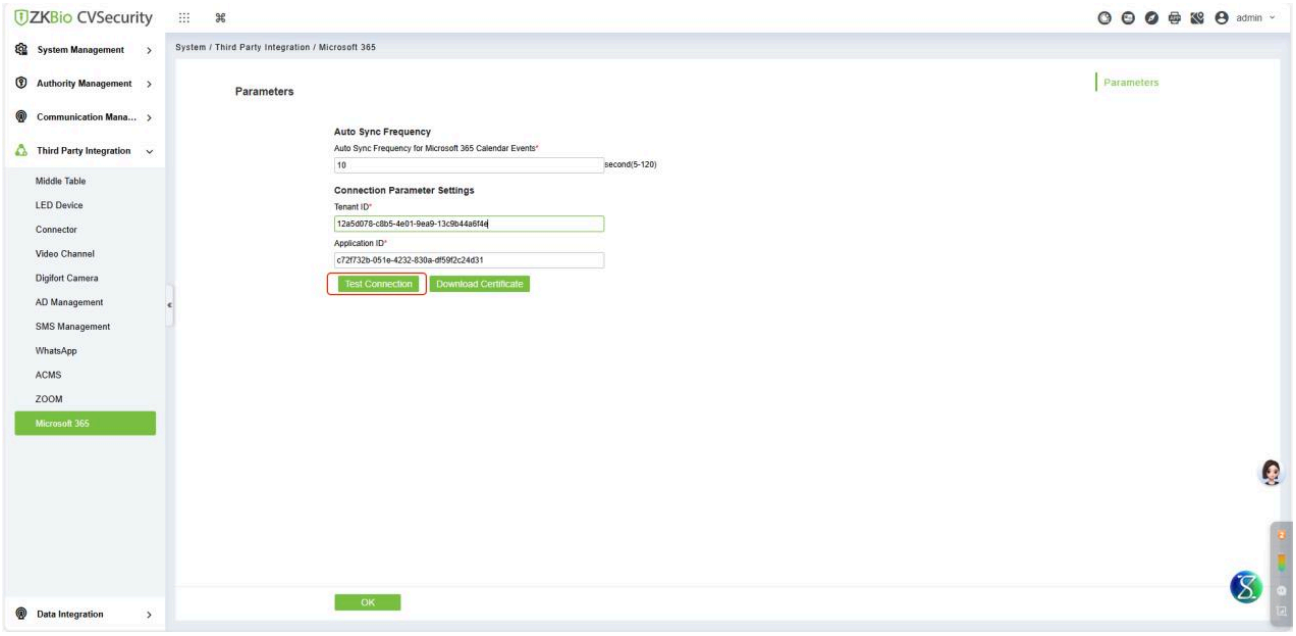
Step6: Click "Grant admin consent on behalf of the organization"to authorize the permissions.



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.

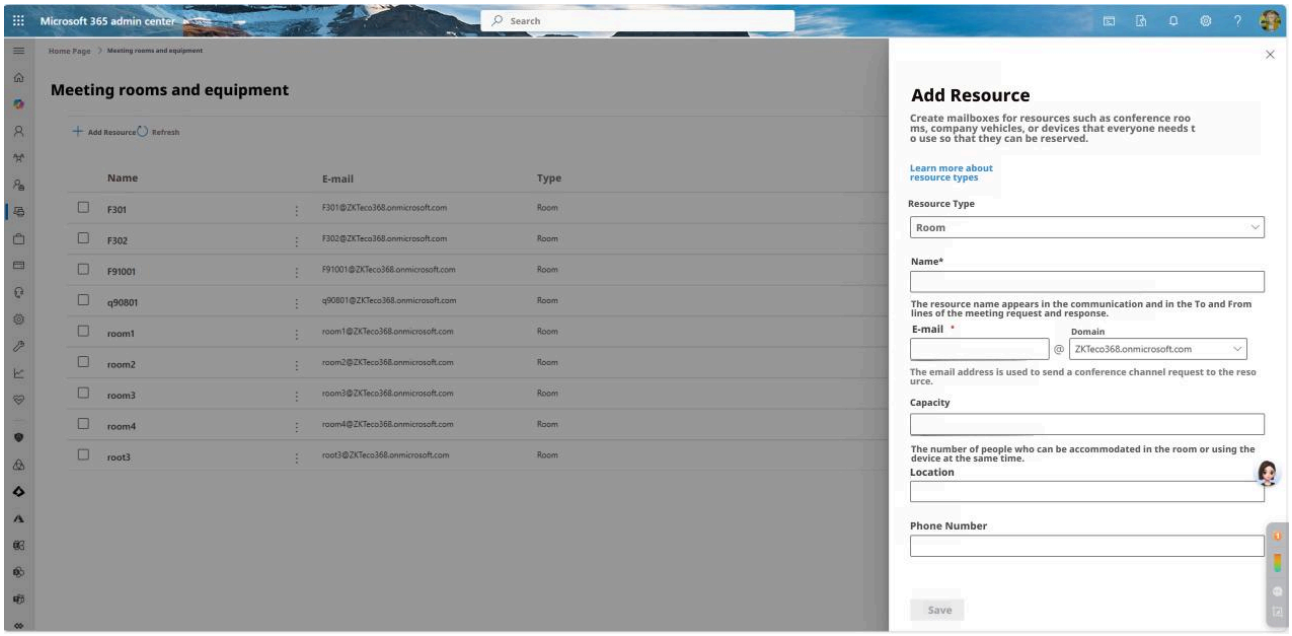


Step8: Click "Test Connection".

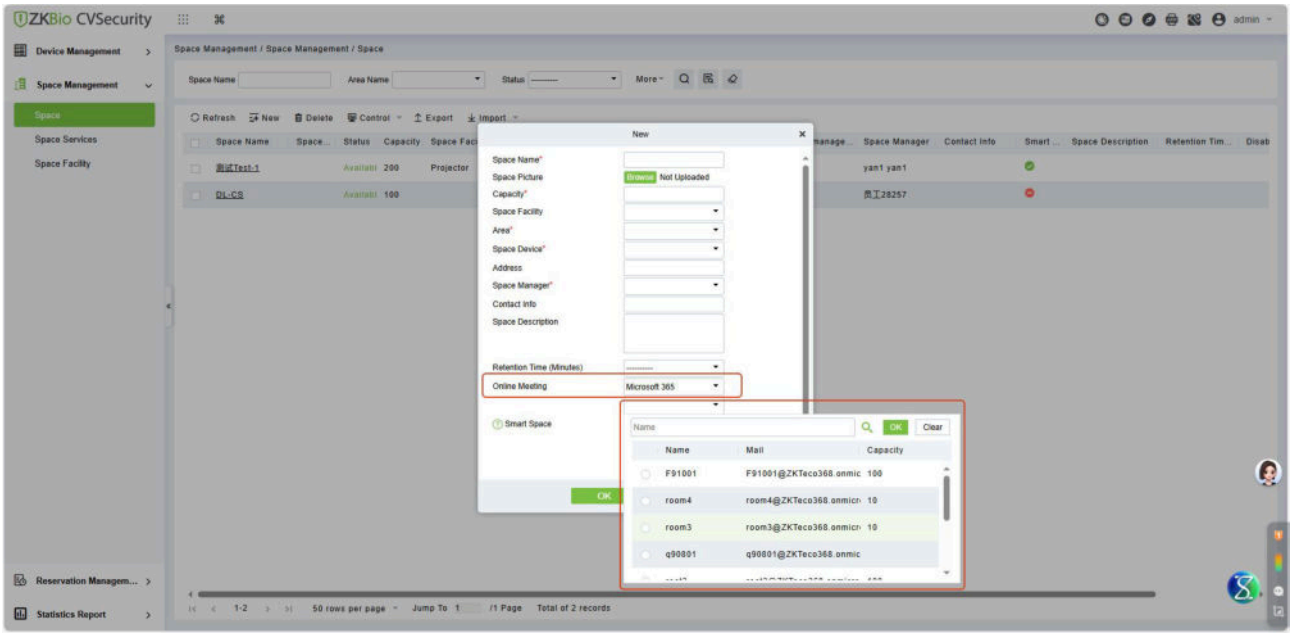


2. Add Meeting Room:

Step1: Enter the Microsoft 365 admin center platform, click Resources → Meeting Rooms & Equipment → Add Resource.

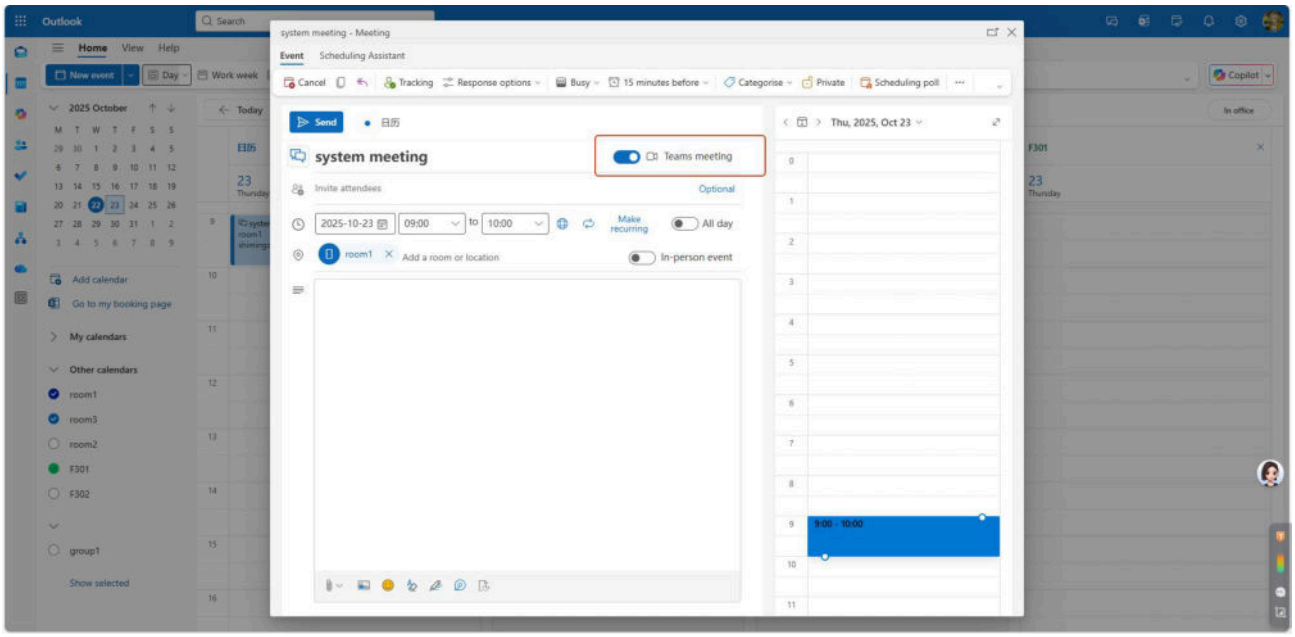


Step2: Enter the ZKBio CVSecurity →Space Management → Space Management → Space.Click "New" to add a meeting room, you can select the corresponding meeting room resource from Microsoft 365.

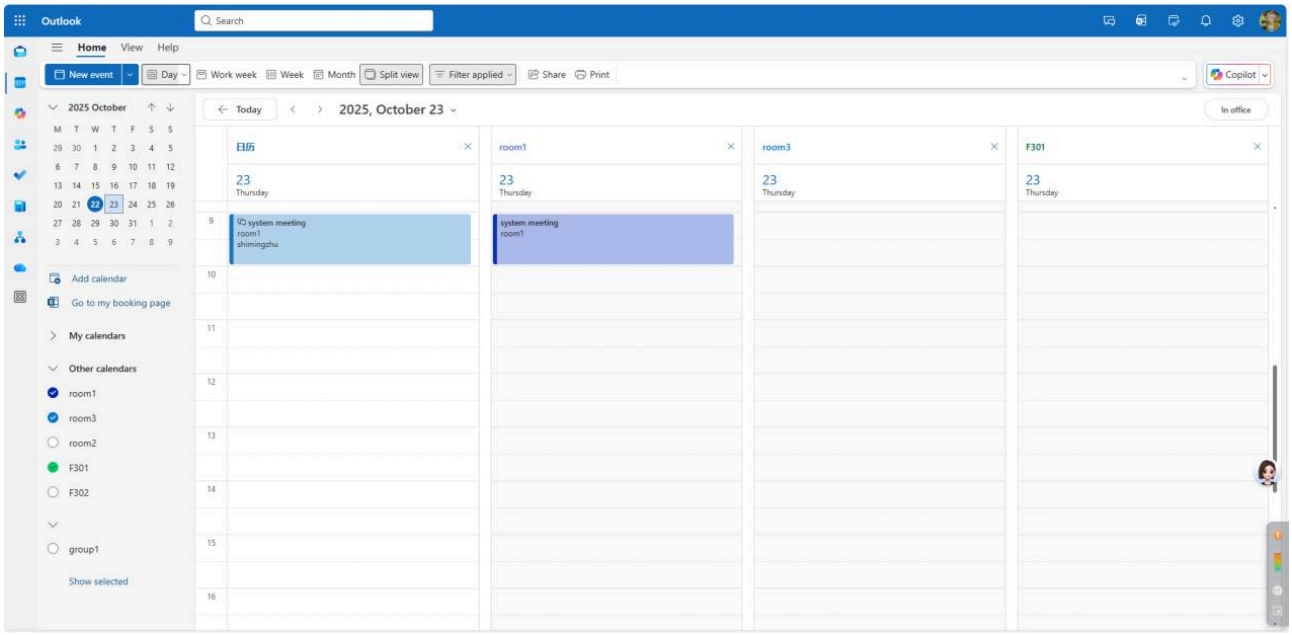


3. Sync Microsoft 365 events:

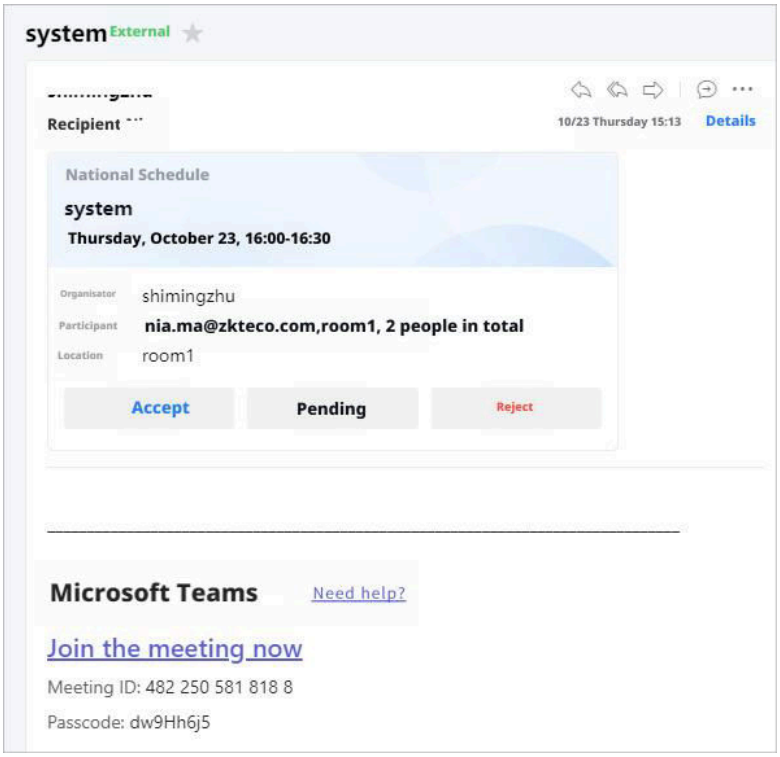
Step1: Create a new event on the Outlook platform.Access the [Calendar] configuration page, select the required meeting schedule time range, expand the advanced configuration options, complete the schedule creation, and send it.



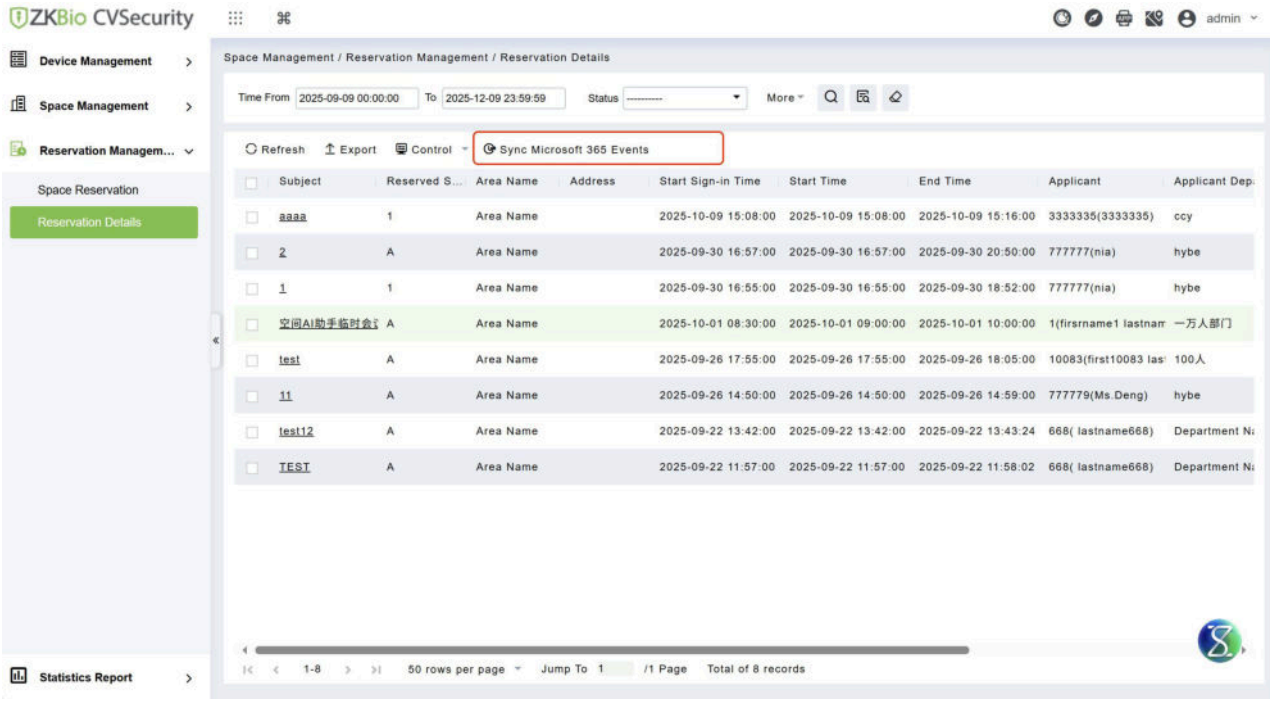
Meeting schedule status display.The calendar information on Teams is completely synchronized with that on Outlook. You only need to make a schedule reservation in either module, and the reservation information will be synchronized between the two.

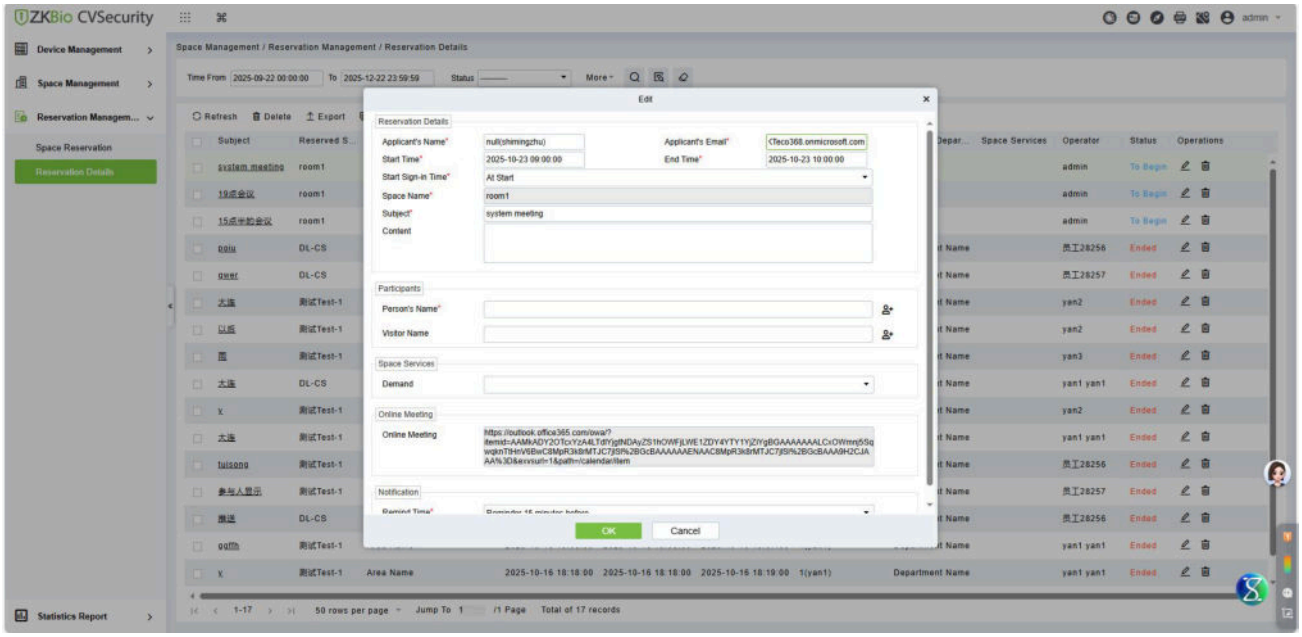


The meeting invitation email is as shown in the figure. When the meeting time arrives, participants working remotely can quickly join the meeting via the online link.

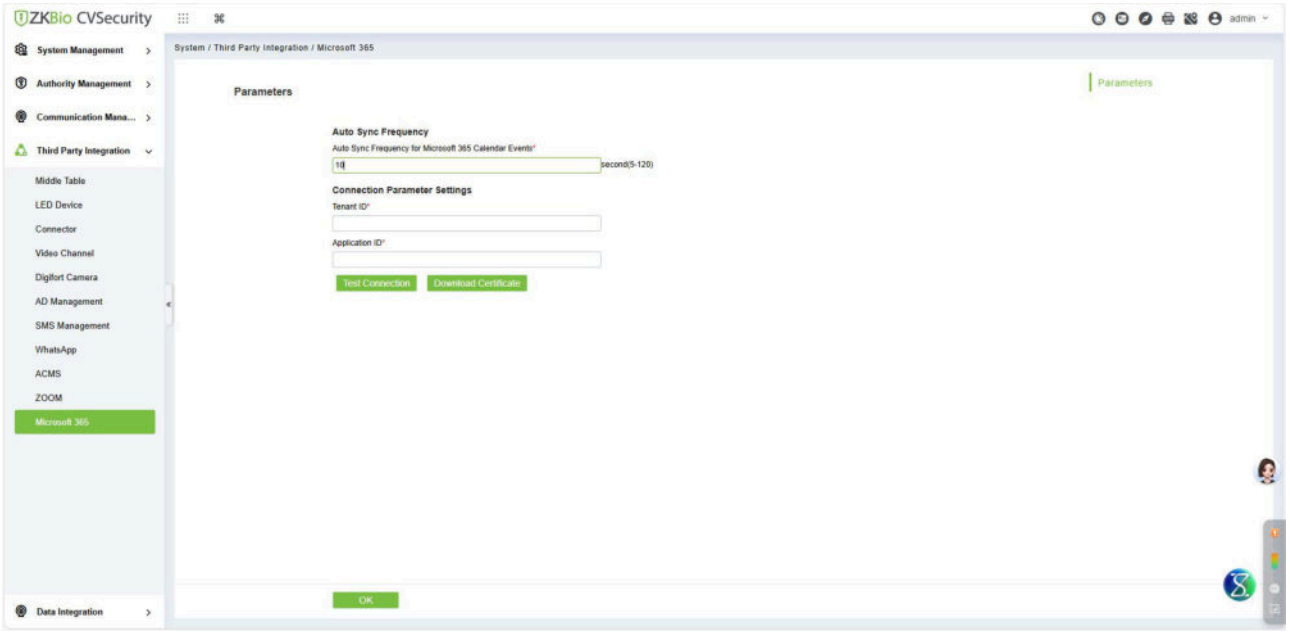


Step 2: Enter the ZKBio CVSecurity →Space Management → Reservation Management → Reservation Details.Click "Sync Microsoft 365 Events" → "OK" to complete the information synchronization.System / Third Party Integration / Microsoft 365





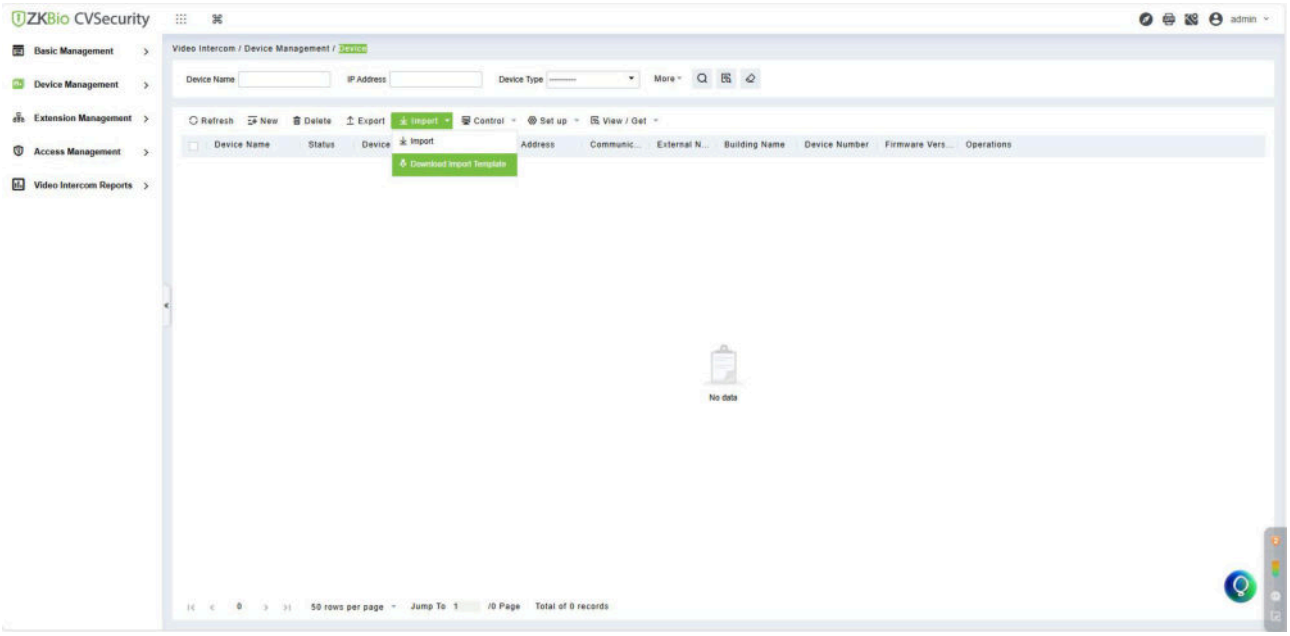
Step 3: Enter the System → Third Party Integration → Microsoft 365.The Auto Sync Frequency can be modified in the parameter settings.The system automatically synchronizes Microsoft 365 calendar events at a frequency of 120 seconds. Within the range of 5 to 120 seconds, the frequency can be customized and modified.


ZKBio CVSecurity
admin
System Management
Authority Management
Communication Mana...
Third Party Integration
Middle Table
LED Device
Connector
Video Channel
Digifort Camera
AD Management
SMS Management
WhatsApp
ACMS
ZOOM
Microsoft 365
Data Integration
System / Third Party Integration / Microsoft 365
Parameters
Parameters
Auto Sync Frequency
Auto Sync Frequency for Microsoft 365 Calendar Events*
10
second(5-120)
Connection Parameter Settings
Tenant ID*
Application ID*
Test Connection
Download Certificate
OK

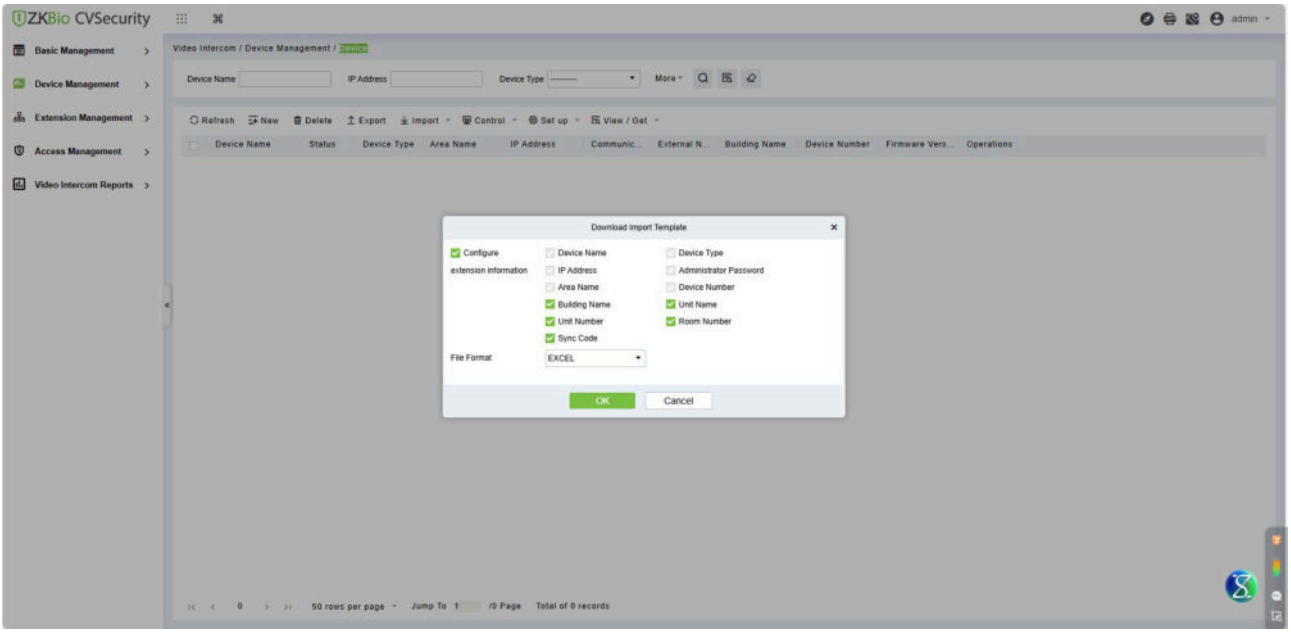
Video Intercom

- **Supports bulk import of devices via excel.**

Step1: Enter Video Intercom → Device Management → Device,click "Import" → "Download Import Template".

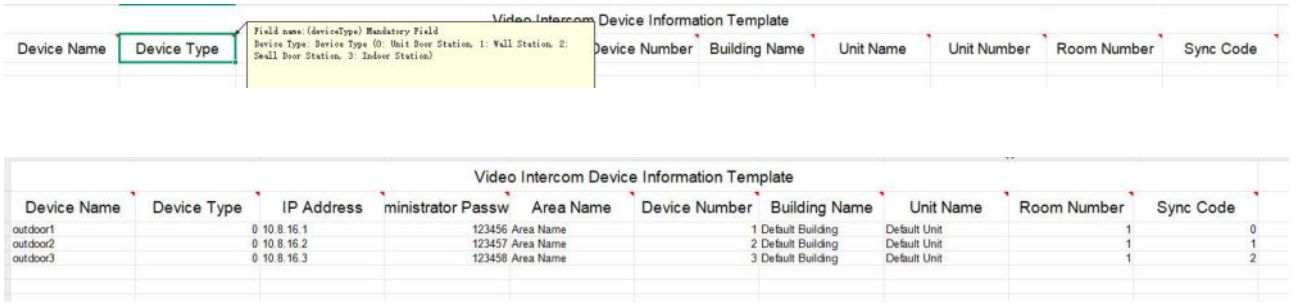


Step2: As shown in the figure below, you can select the desired import fields as needed.



Step3: Fill in the required content according to the instructions in the import template and save it.

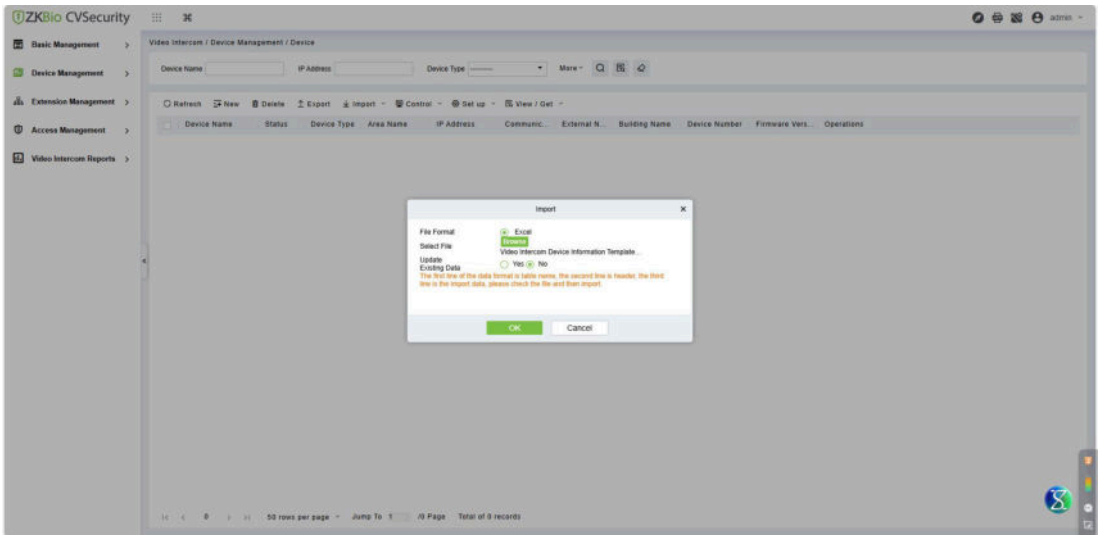
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.



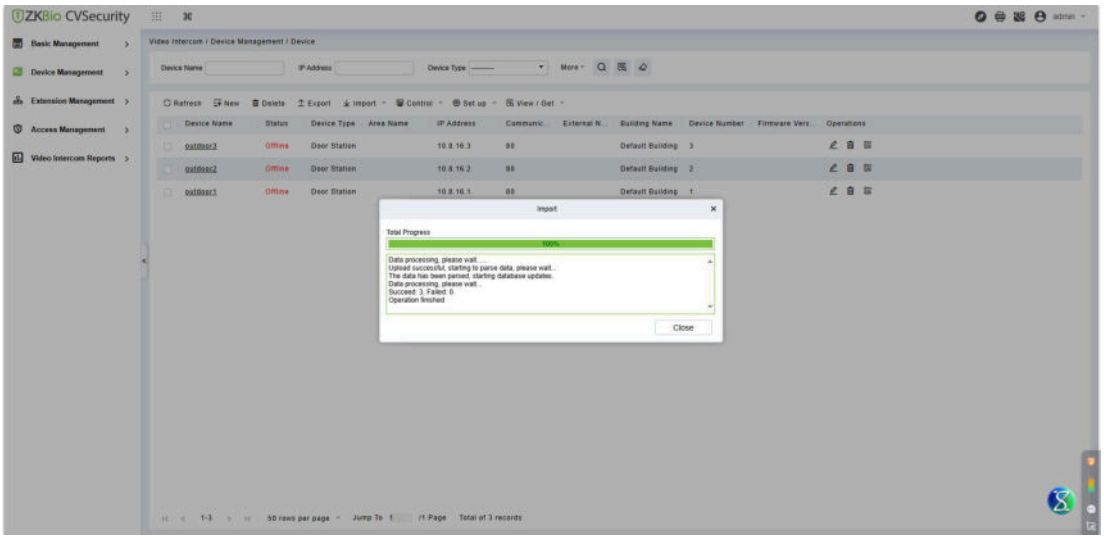
Video Intercom Device Information Template

Device Name	Device Type	IP Address	ministrator Passw	Area Name	Device Number	Building Name	Unit Name	Room Number	Sync Code
outdoor1	0	10.8.16.1	123456	Area Name	1	Default Building	Default Unit	1	0
outdoor2	0	10.8.16.2	123457	Area Name	2	Default Building	Default Unit	1	1
outdoor3	0	10.8.16.3	123458	Area Name	3	Default Building	Default Unit	1	2

Return to the software interface, click "Import", select the import template, and then click "Confirm" to begin importing devices

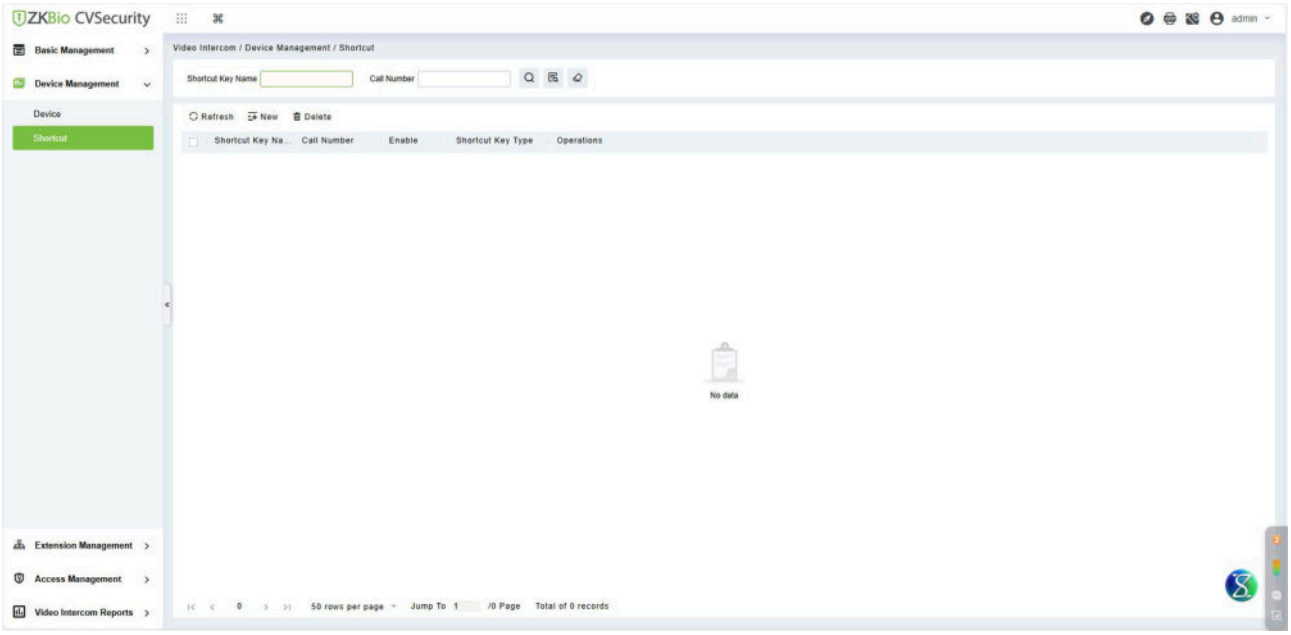


The import status is shown in the figure below. You can view the number of successful imports until the operation is complete, and the imported devices will be displayed in the list.



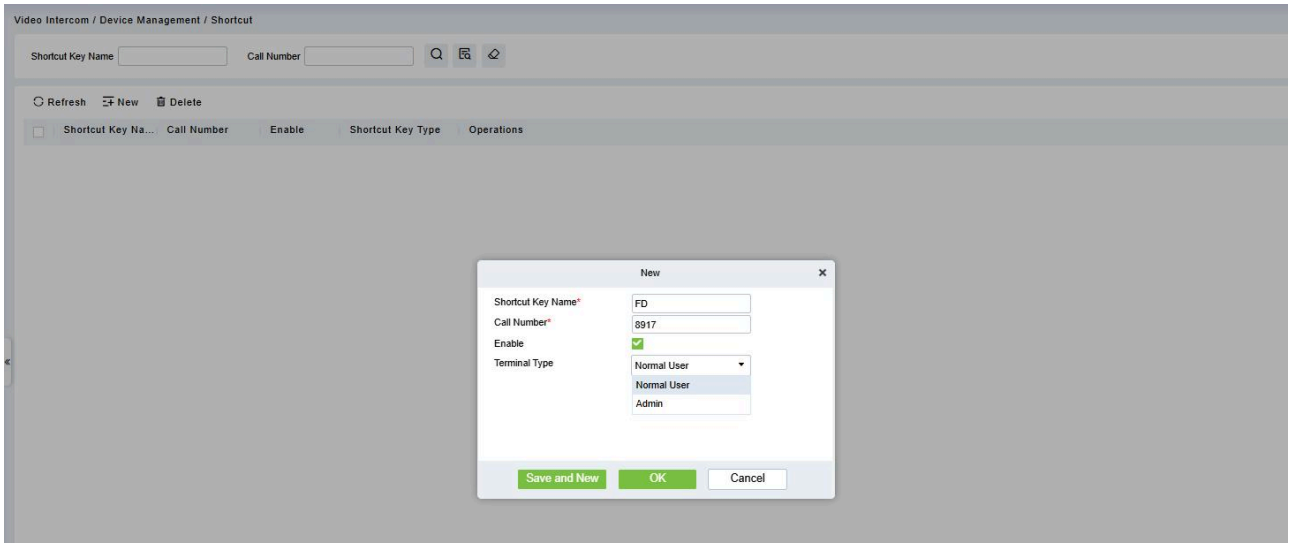
- **The shortcut menu has been moved under the Device Management menu.**

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

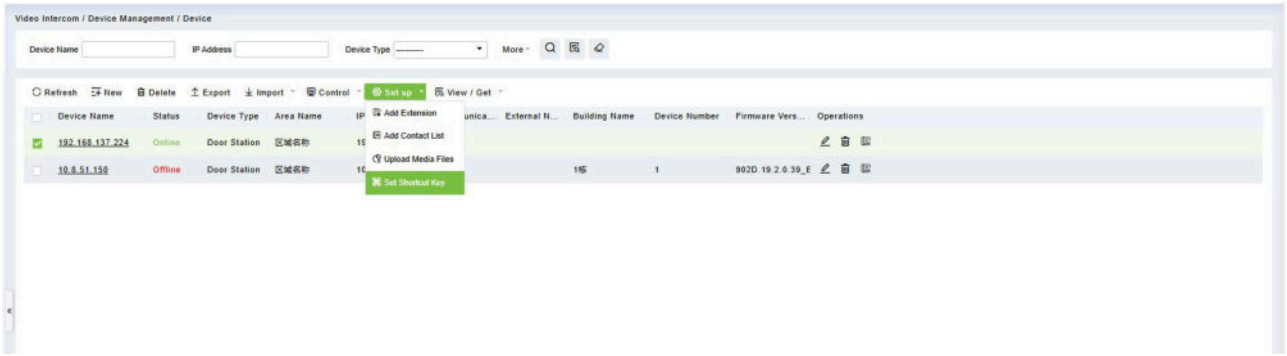


Note: Currently, this function only supports ZKTECO access control devices and does not support DNK devices.

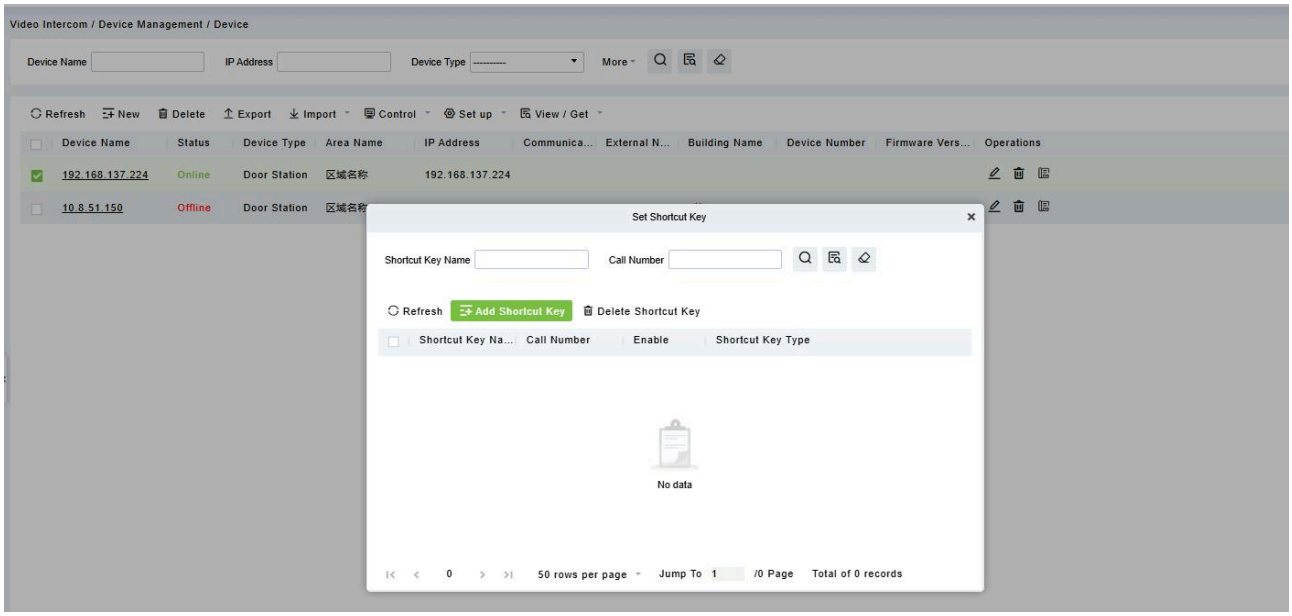
Step1: Click "New", fill in the Shortcut Key Name and the Call Number (if the SIP Service Mode is Cloud Sip, fill in the sip account; if the SIP Service Mode is Local IPPBX, fill in the extension number), check whether to enable it, and select the binding type as Normal user or Admin.



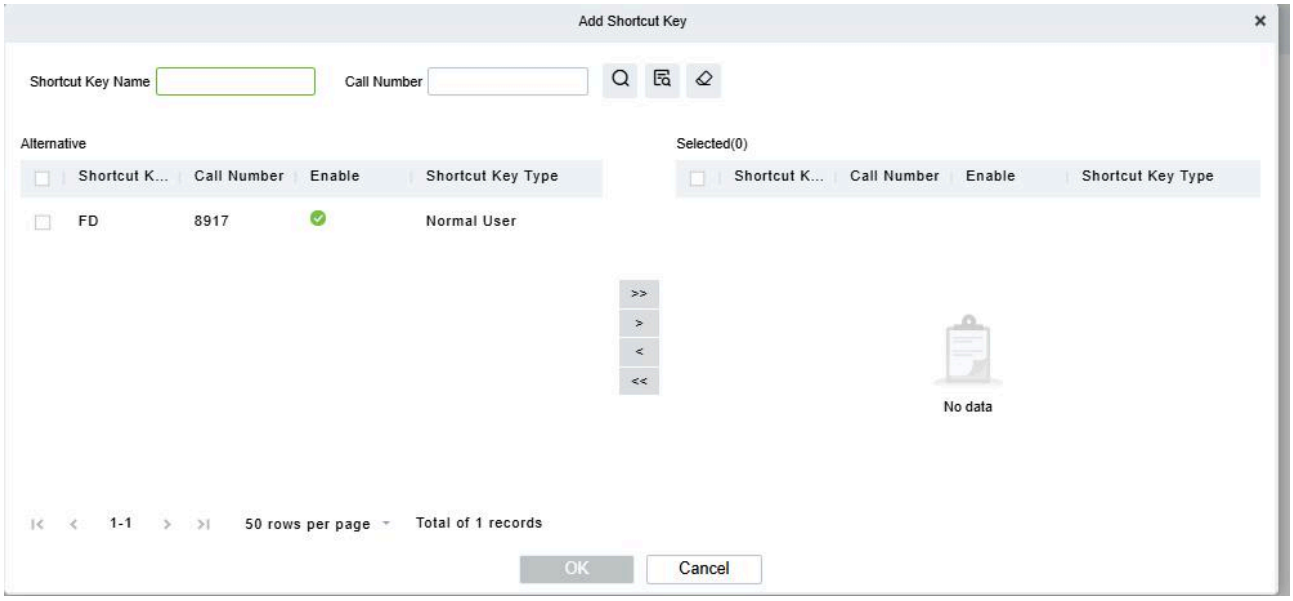
Step 2: After adding the shortcut keys, go to Video Intercom → Device Management → Device, select the device, and then click "Set up" → "Set Shortcut Key".



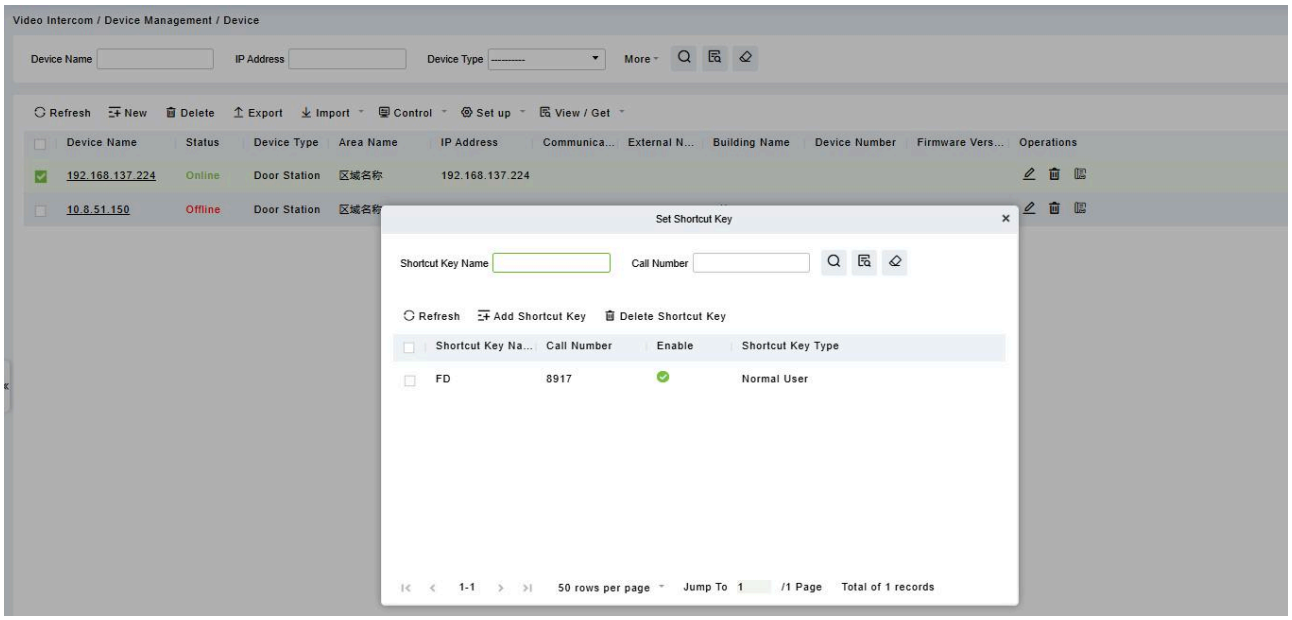
Step 3: Click "Add Shortcut Key".



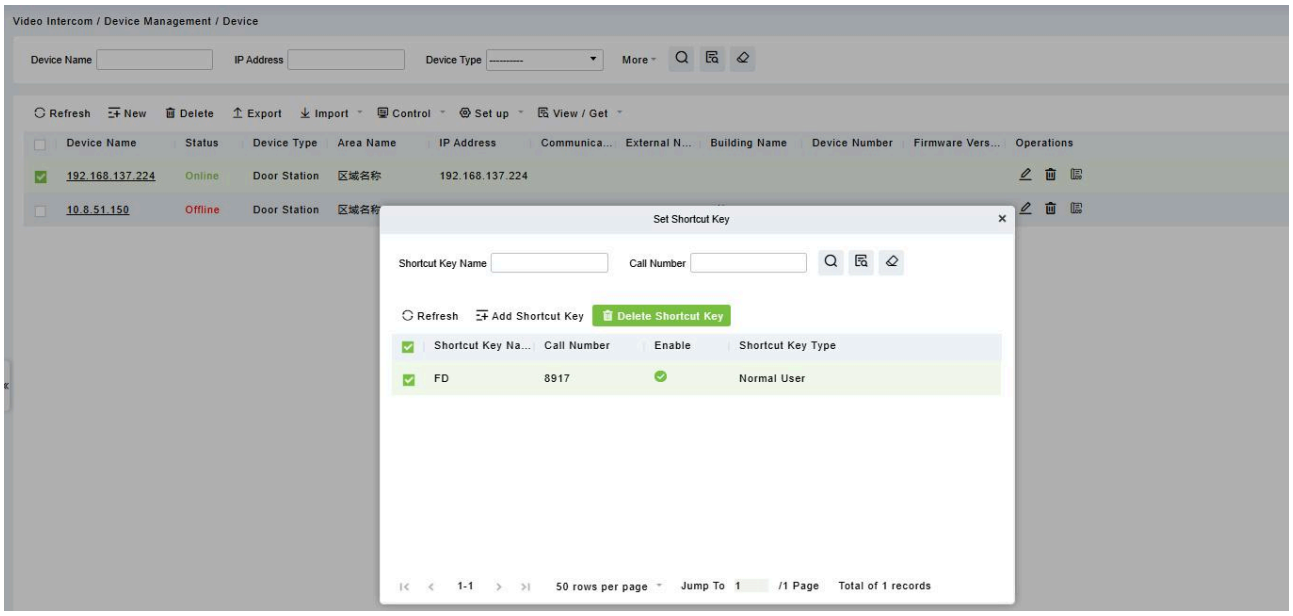
Step 4: Move the shortcut key you want to add to the right side and click "OK" to complete the operation.



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.



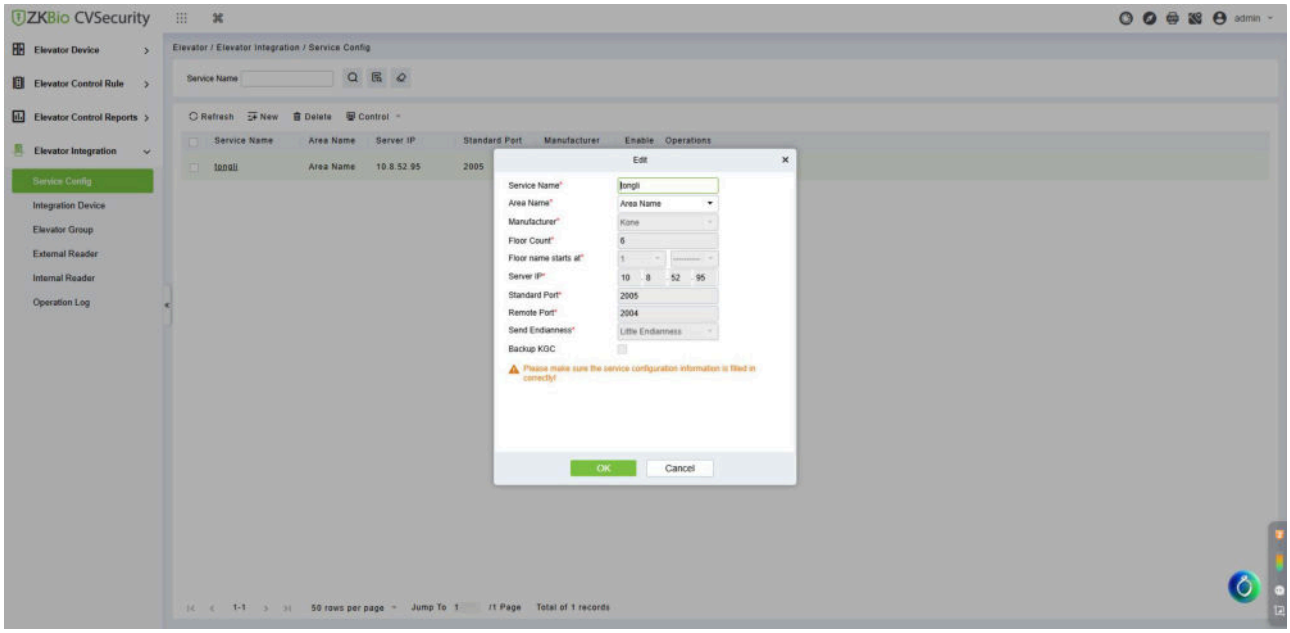
After checking the shortcut key, click "Delete Shortcut Key" to delete the shortcut key. The access control door will delete it simultaneously.



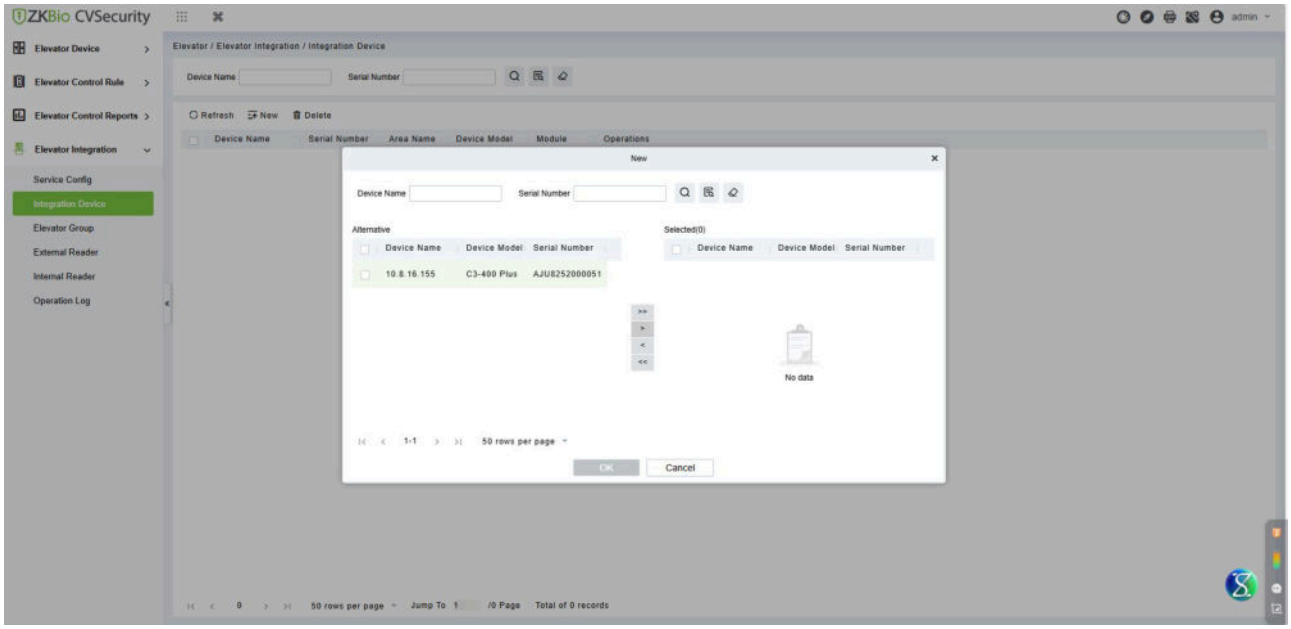
- **In apartment visual intercom scenarios, remote door unlocking via the entrance terminal is supported, along with the allocation of elevator access permissions for visitors.**

Applicable Scenarios: In an apartment visual intercom scenario, when a visitor uses the first-floor video intercom terminal to call the resident, the resident can remotely unlock the entrance door. The system will then automatically dispatch the elevator to the first floor and authorize it to access the resident's floor.

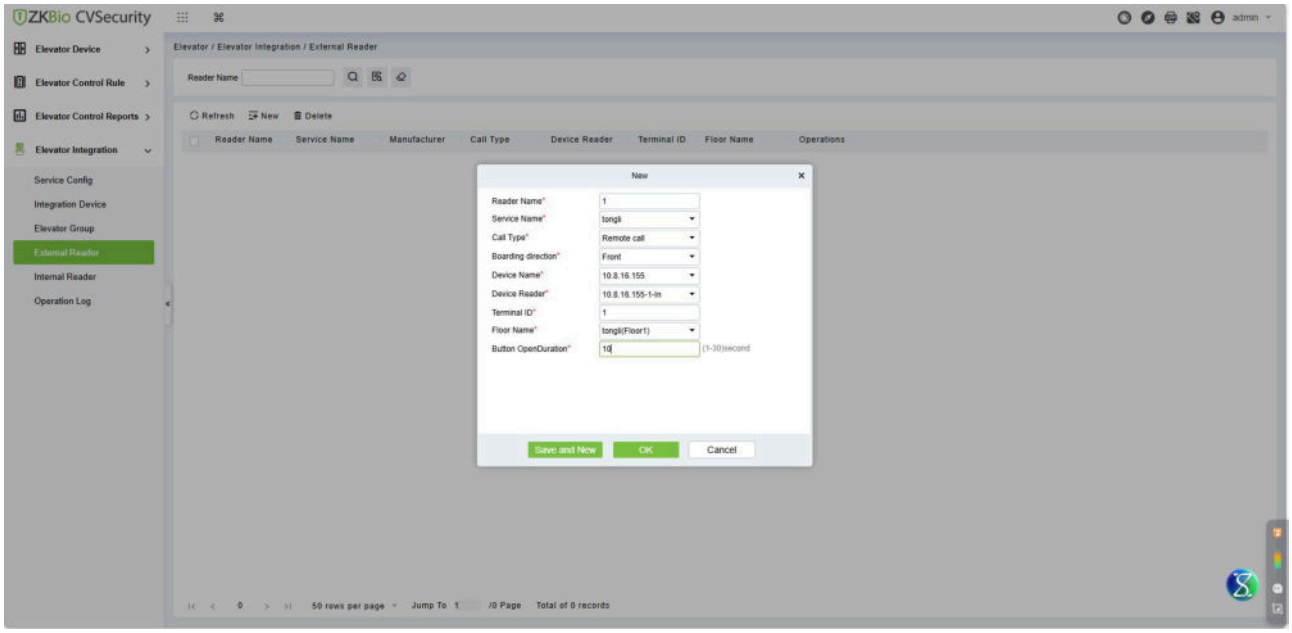
Step1: Enter Elevator → Elevator Integration → Service Config ,click "New" to set up the DCS service configuration.



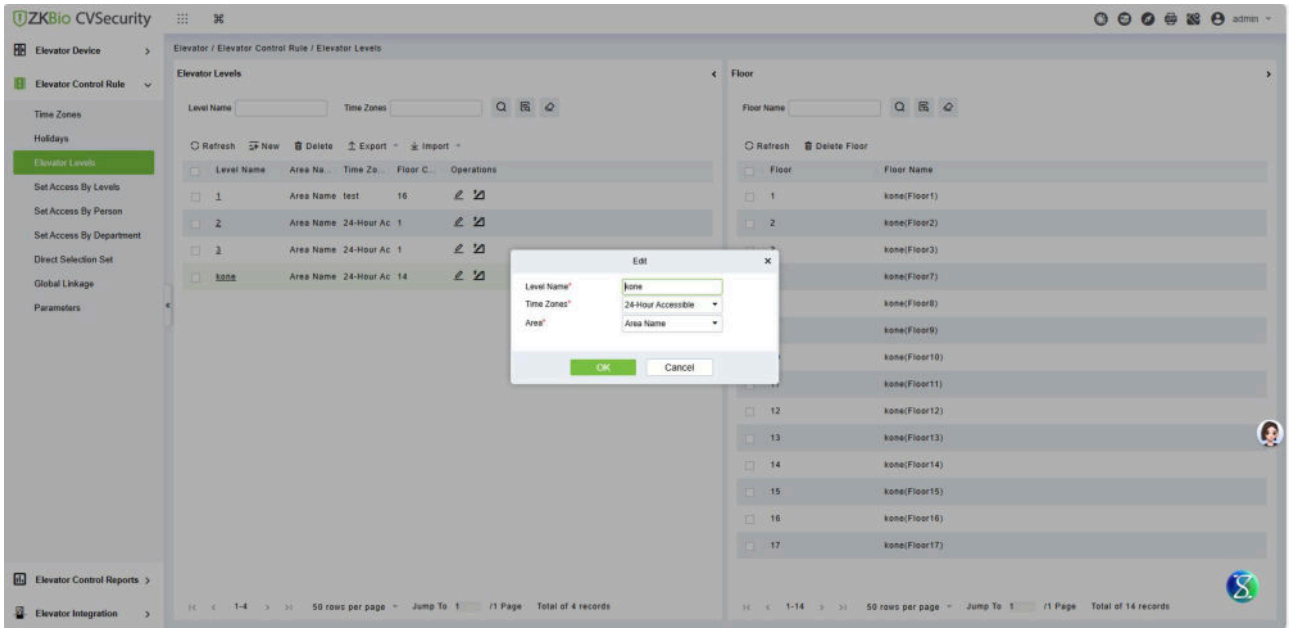
Step 2: Enter Elevator → Elevator Integration → Integration Device, click "New", select the access control devices with video intercom function and move them to the right, then click "OK" to complete the addition of integrated devices.



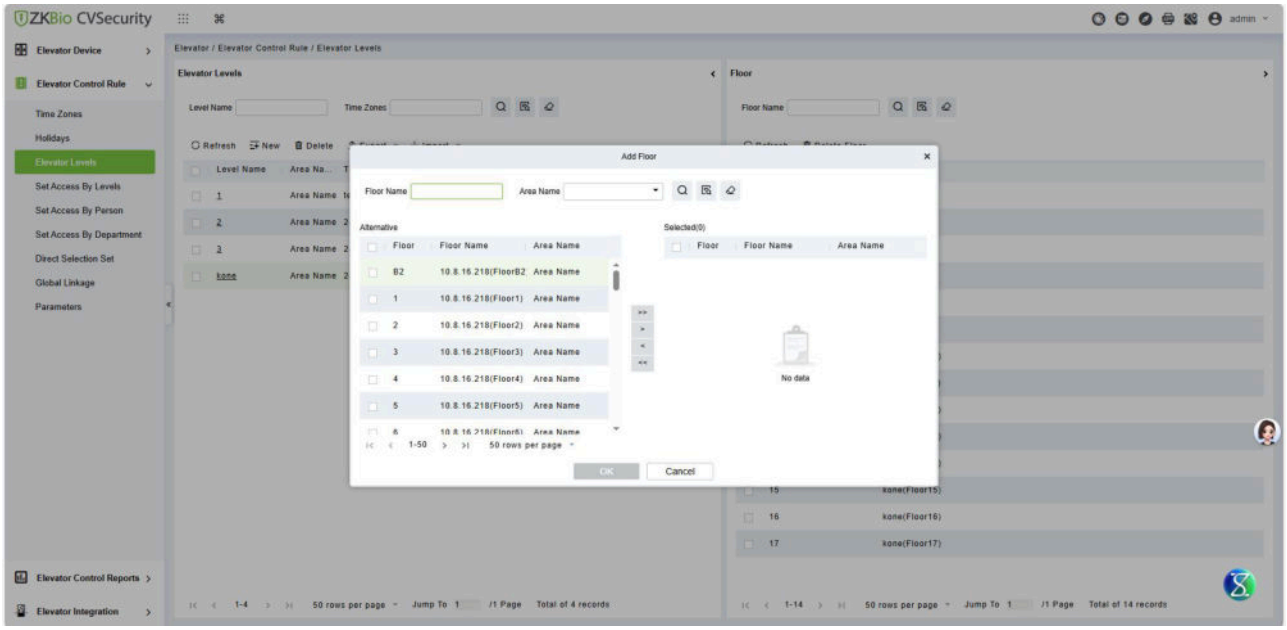
Step 3: Enter Elevator → Elevator Integration → External Reader, set the external reader (Mitsubishi for automatic call, KONE for remote call), and select the integrated video intercom equipment for the device. The floor selected here is the one that the elevator can automatically assign to, usually the first floor where the visitor is located.



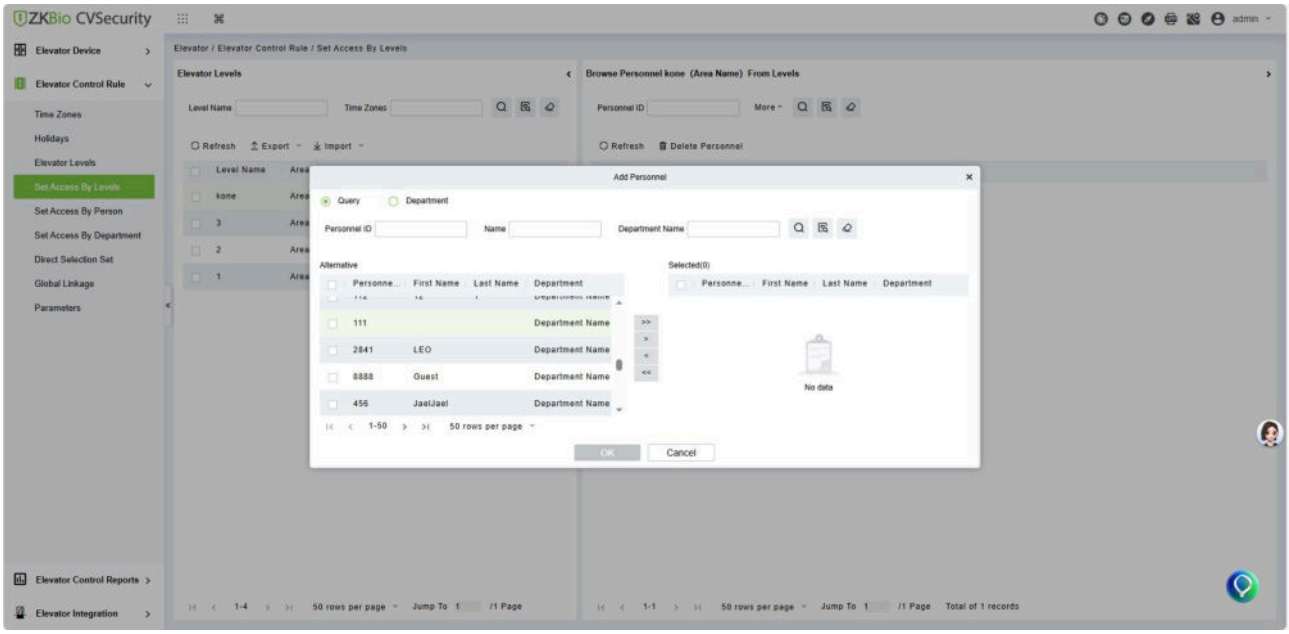
Step 4: Enter Elevator → Elevator Control Rule → Elevator Levels, click "New",add a new elevator levels, enter the relevant information and click OK to complete the operation.



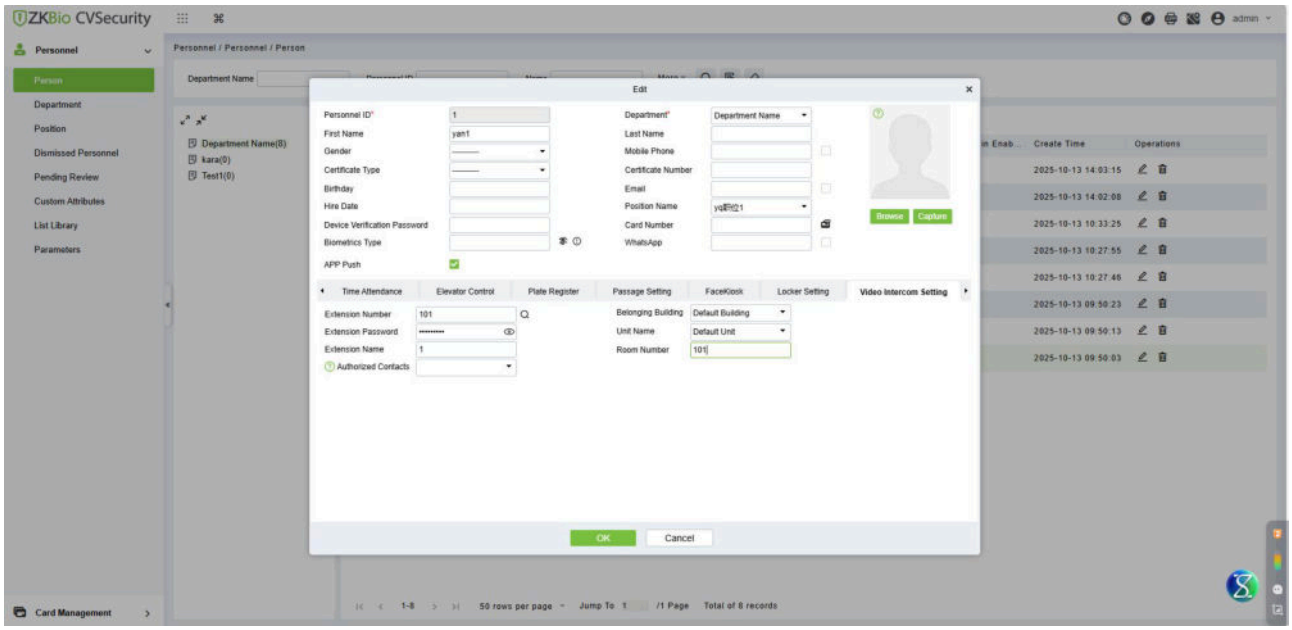
Click OK or Add Floor icon in the operation column, move the corresponding elevator floor from the left to the right, and click OK.



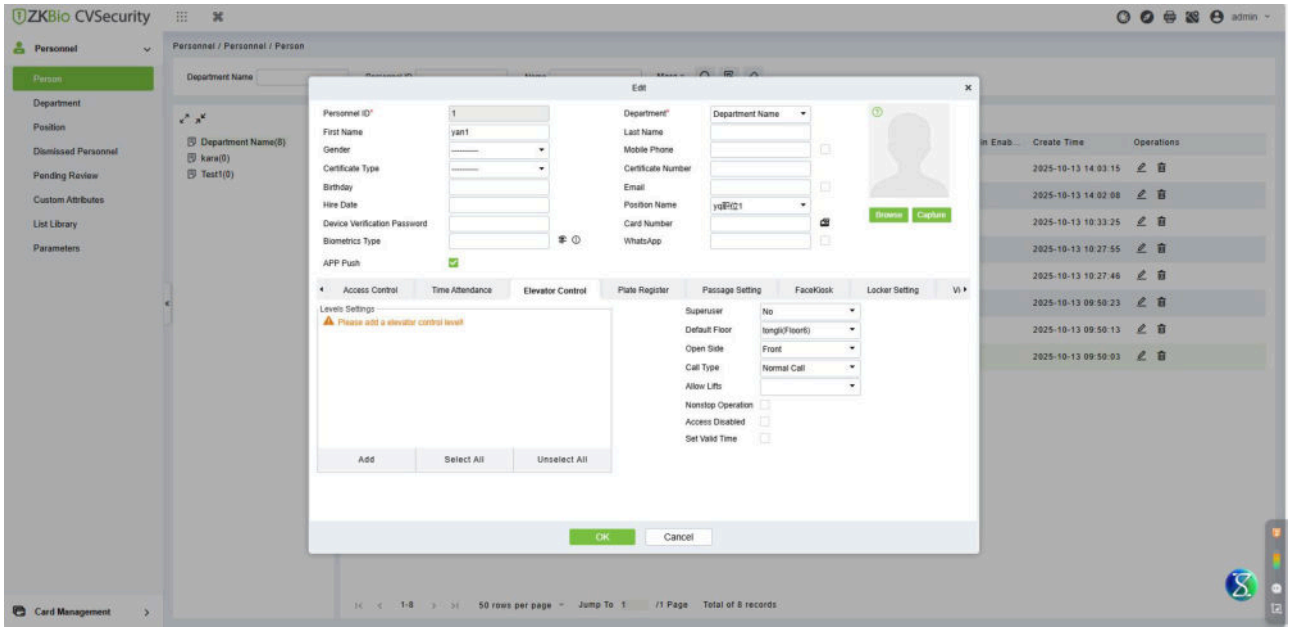
Step 5: Enter Elevator →Elevator Control Rule → Set Access By Levels,click the "Add Personnel" icon in the operation column of the new elevator levels that was just added, move the corresponding personnel from the left to the right, and click OK to complete the operation.



Step 6: Enter Personnel → Personnel → Person, click on the Personnel ID to enter the editing interface, and fill in the extension number information in the video intercom Settings column.

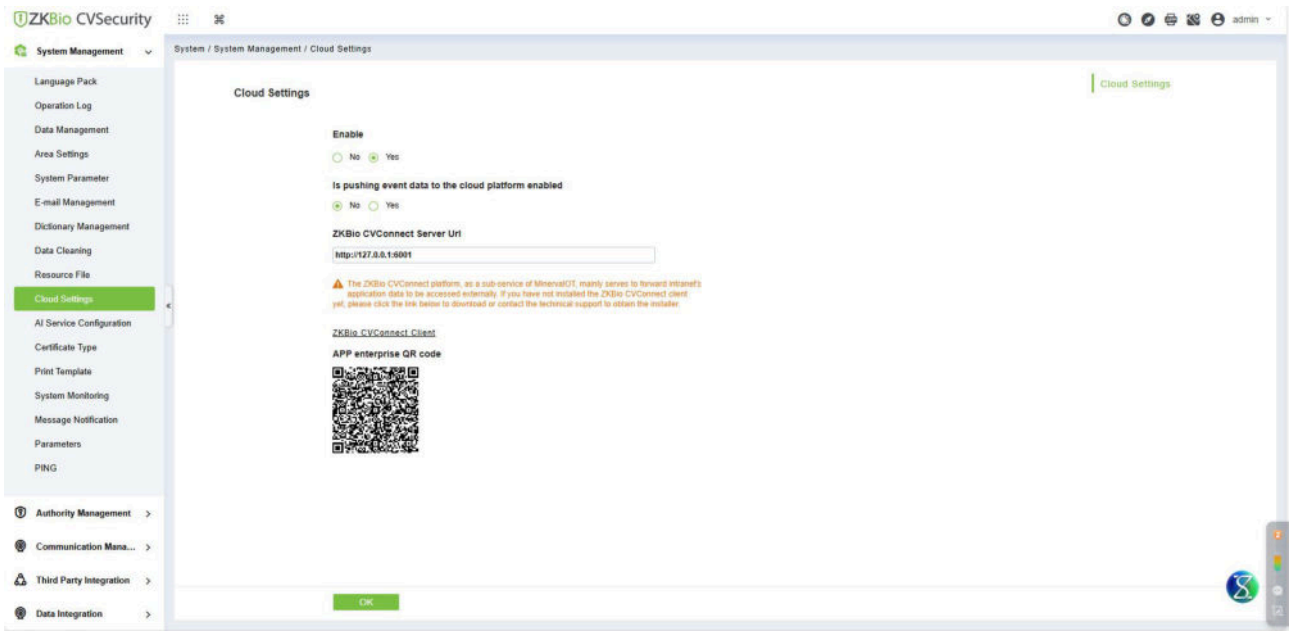


Step 7: In the personnel editing interface, click on the elevator control Settings bar to set the default floor (the floor where the user is located) and its related configurations.

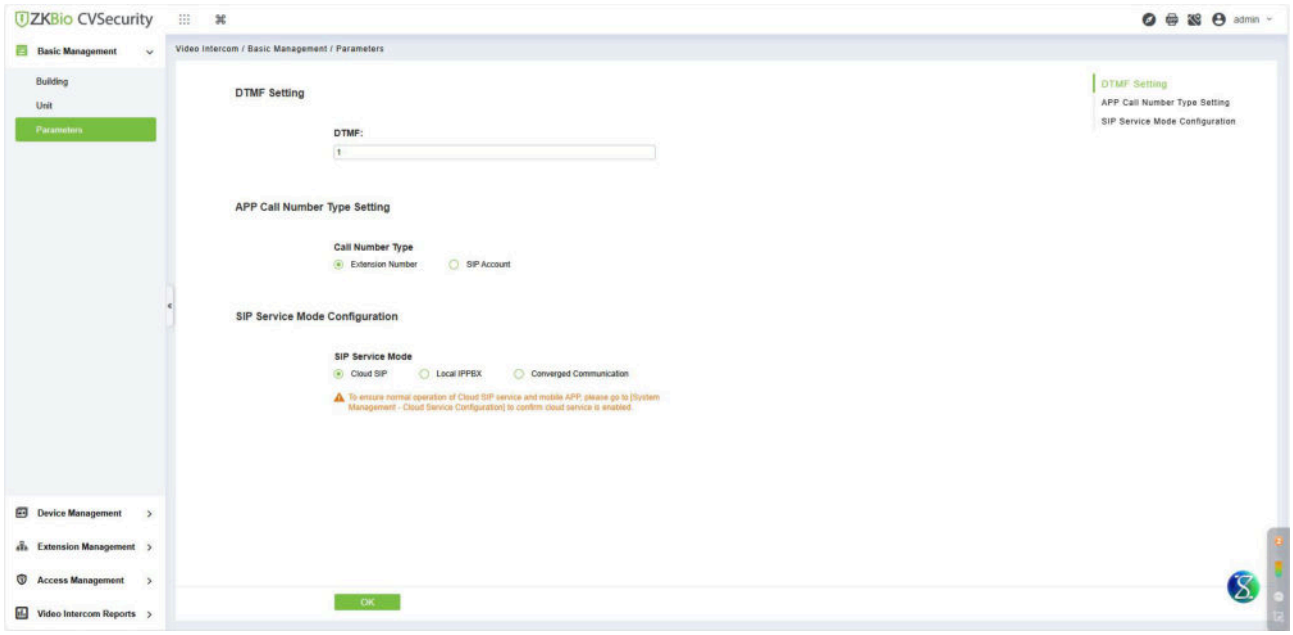


- **The SIP service mode has been moved to the Video Intercom → Parameters page.**

The "SIP Service Mode" option in System → Cloud Settings has been hidden.



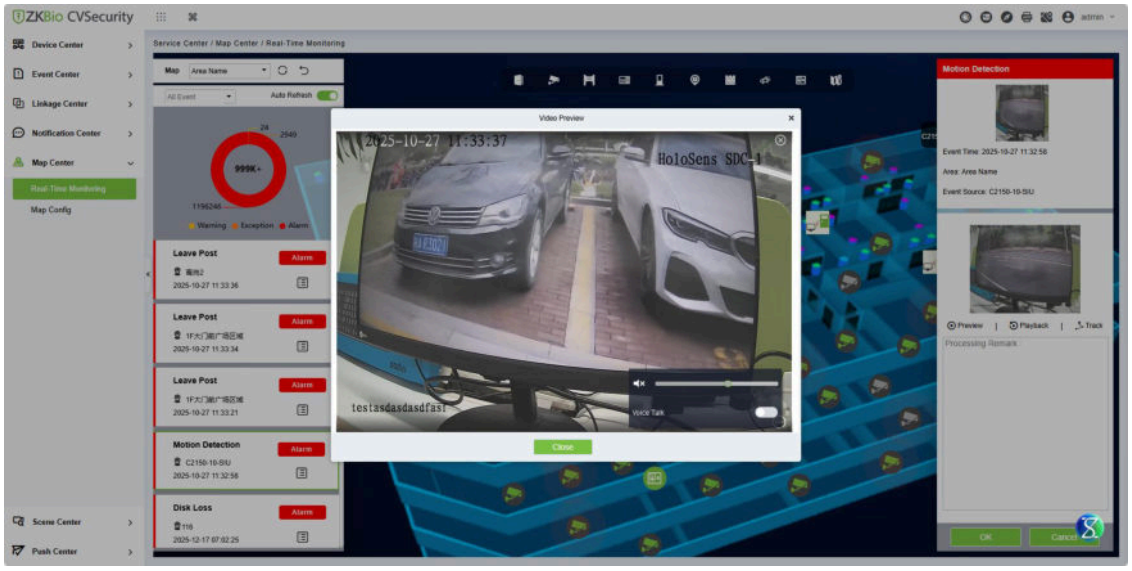
A new "SIP Service Mode" option has been added to Video Intercom → Parameters .



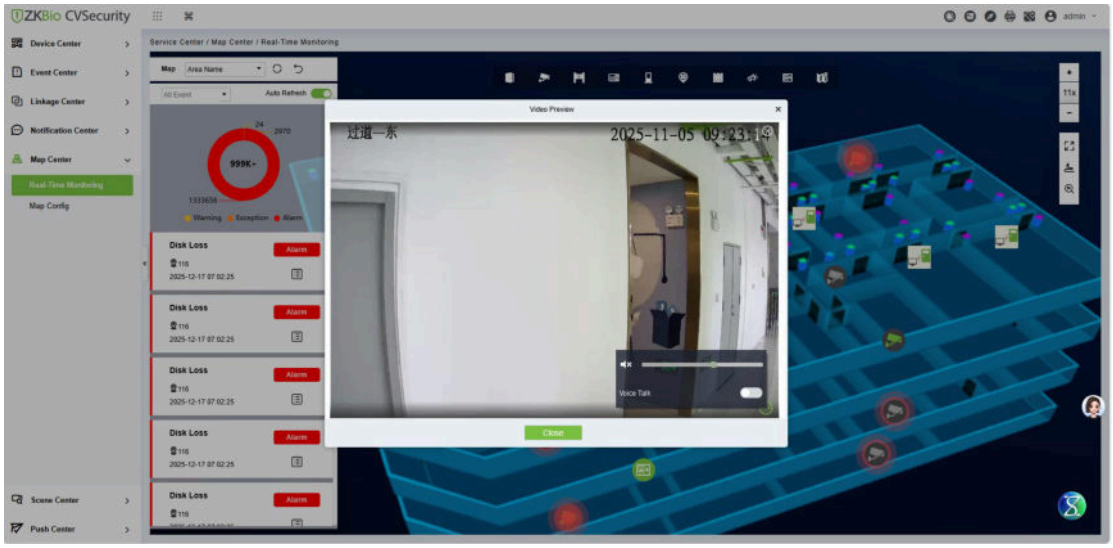
Service Center

- **Map Center-Supports voice intercom operations when previewing camera points.**

Step: Enter the Service Center → Map Center → Real-Time Monitoring, click "  ".Click to view the video preview. In the preview interface, cameras that support intercom allow you to turn on the microphone for voice intercom.

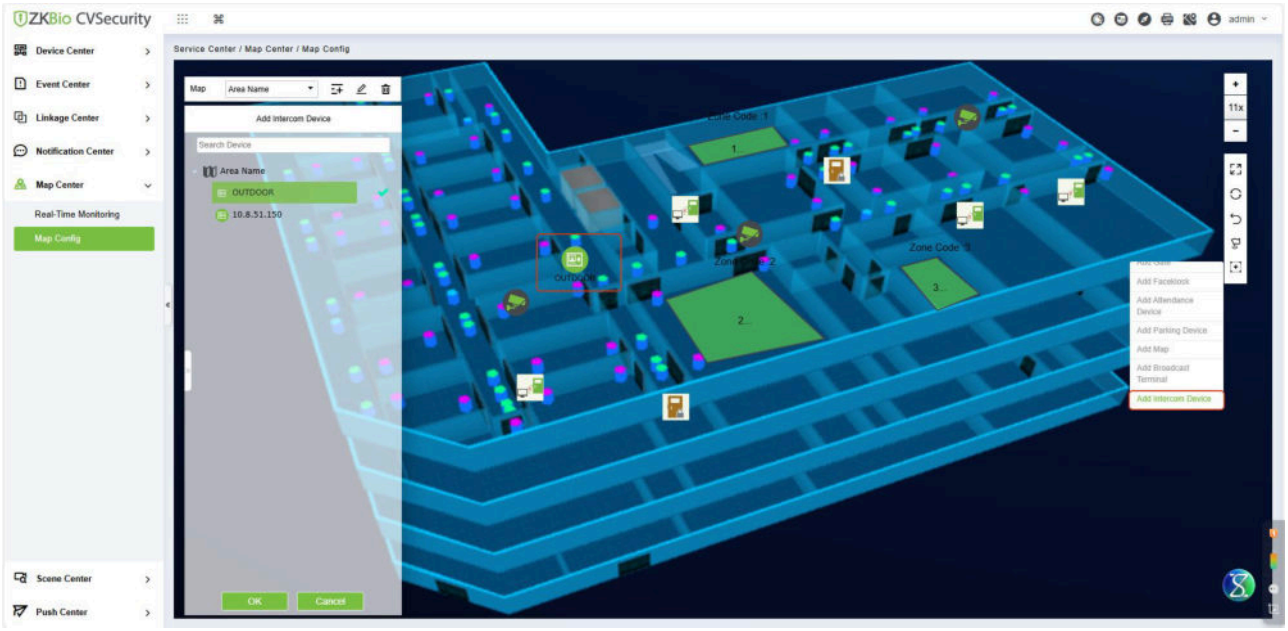


When you double-click the camera preview, cameras that support the intercom function will allow you to enable the voice intercom feature.



- **Map Center-Added visual intercom points.**

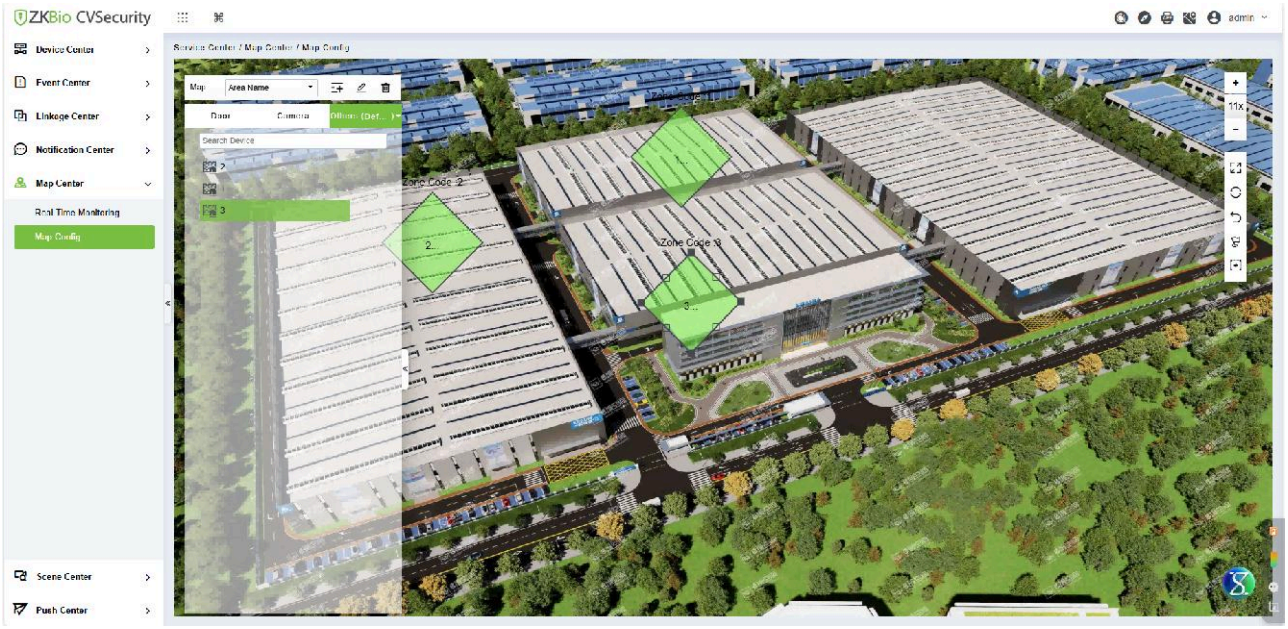
Step: Enter the Service Center → Map Center → Map Config, click "Others", and you can select Video Intercom.



Note: The optional equipment here is a DNK device.

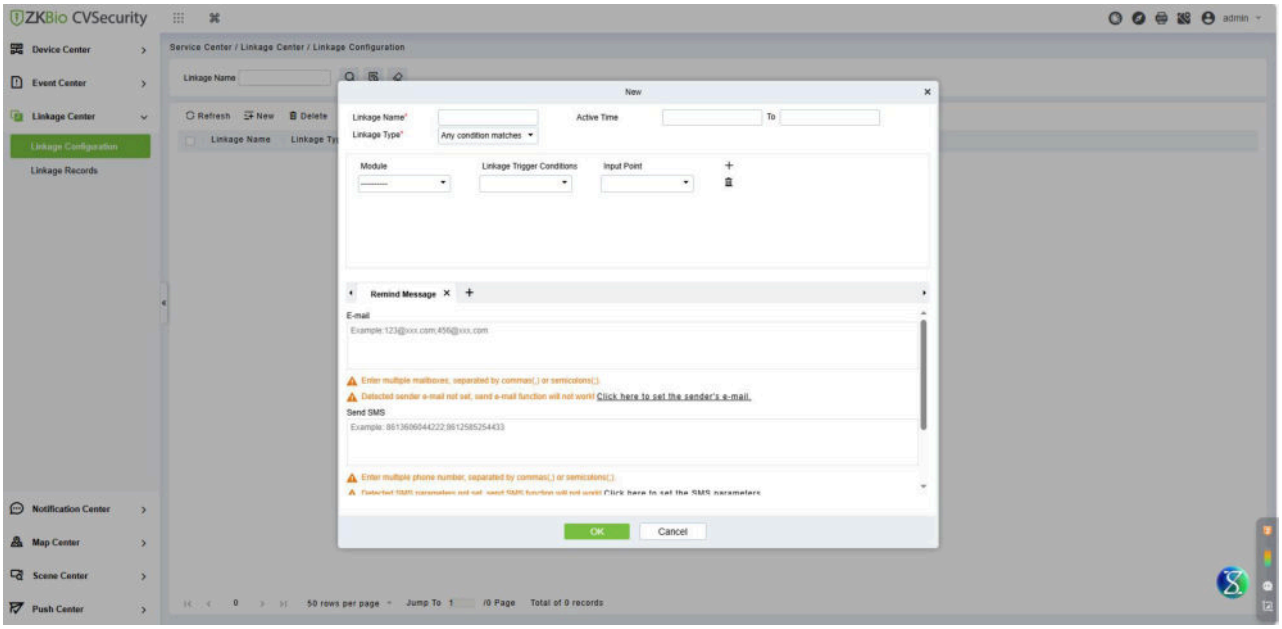
- **Map Center-Intrusion alarm zones support secondary editing and display of zone numbers.**

Step: Enter the Service Center → Map Center → Map Config. The map will display the area and area number of each defense zone. Right-click on the defense zone with the mouse to adjust the range of the defense zone.



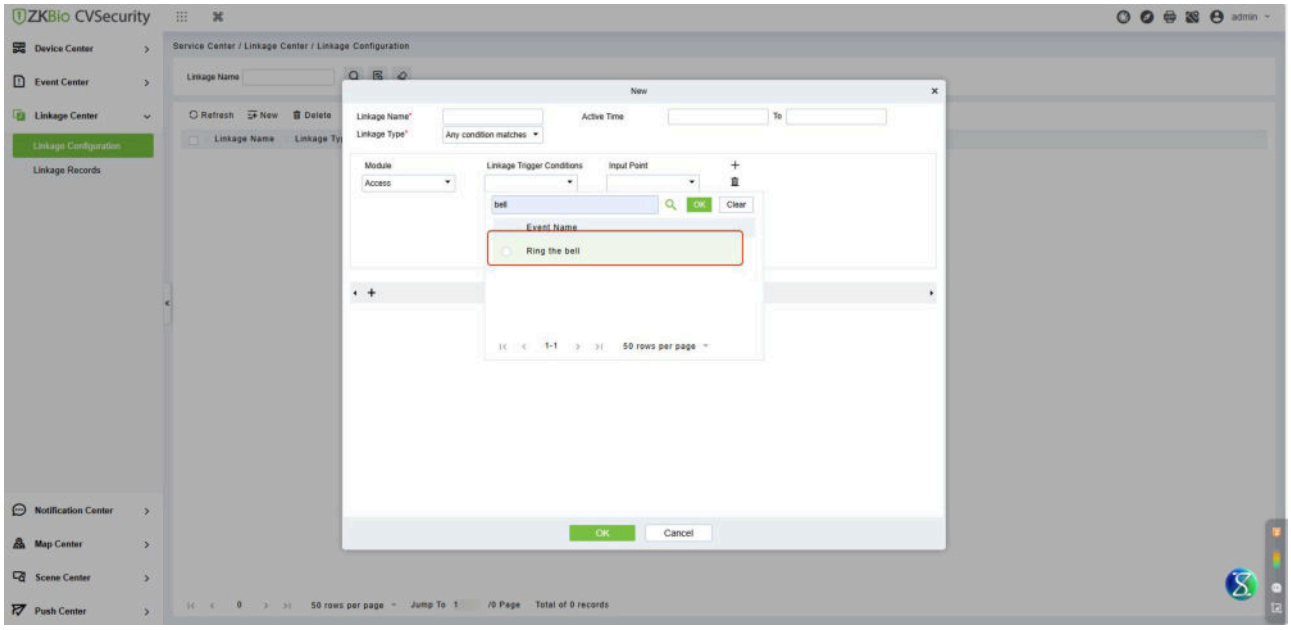
- **Linkage Center-Added "Remind Message" as a new output action option, supporting Email, SMS, and WhatsApp.**

Step: Enter the Service Center → Linkage Center → Linkage Configuration, click "New" to configure the linkage. In the output action bar at the bottom of the interface, you can set Remind Message and fill in your email ,SMS, and WhatsApp messages.

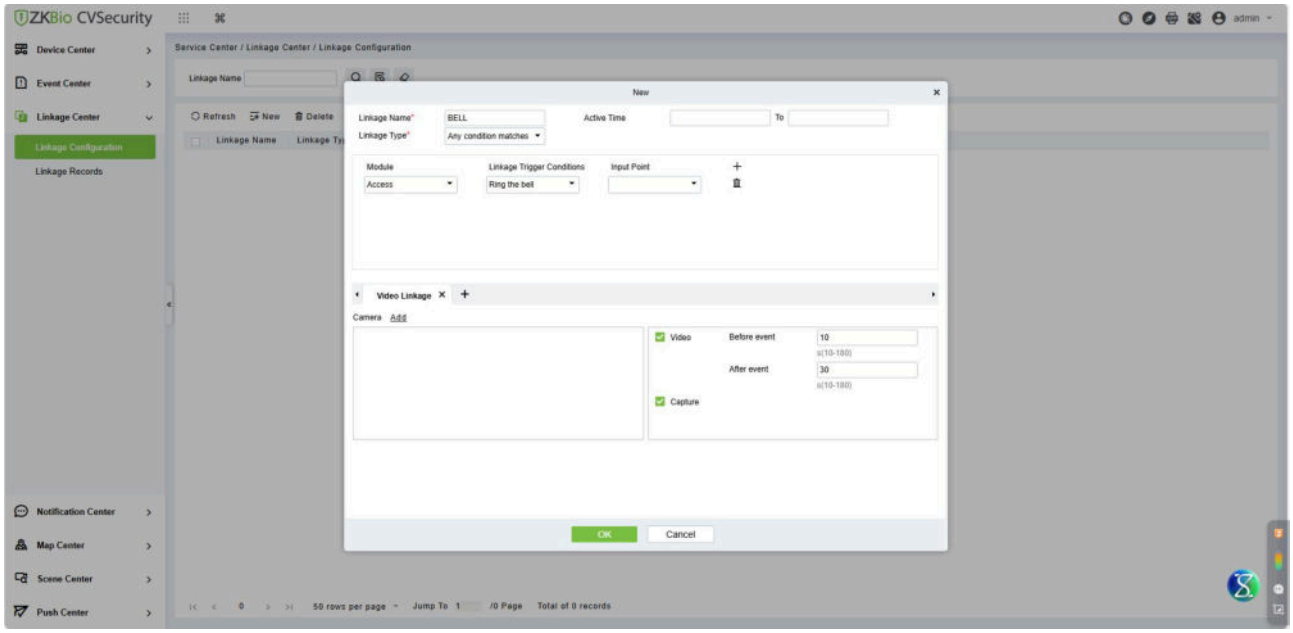


- **Linkage Center-When a doorbell is pressed, it can activate linked cameras to start recording.**

Step1: Enter Service Center → Linkage Center → Linkage Configuration, click "New" for editing, select the access control module as the module, choose "Ring the bell" as the linkage trigger condition, and select the corresponding access control reader as the input point.



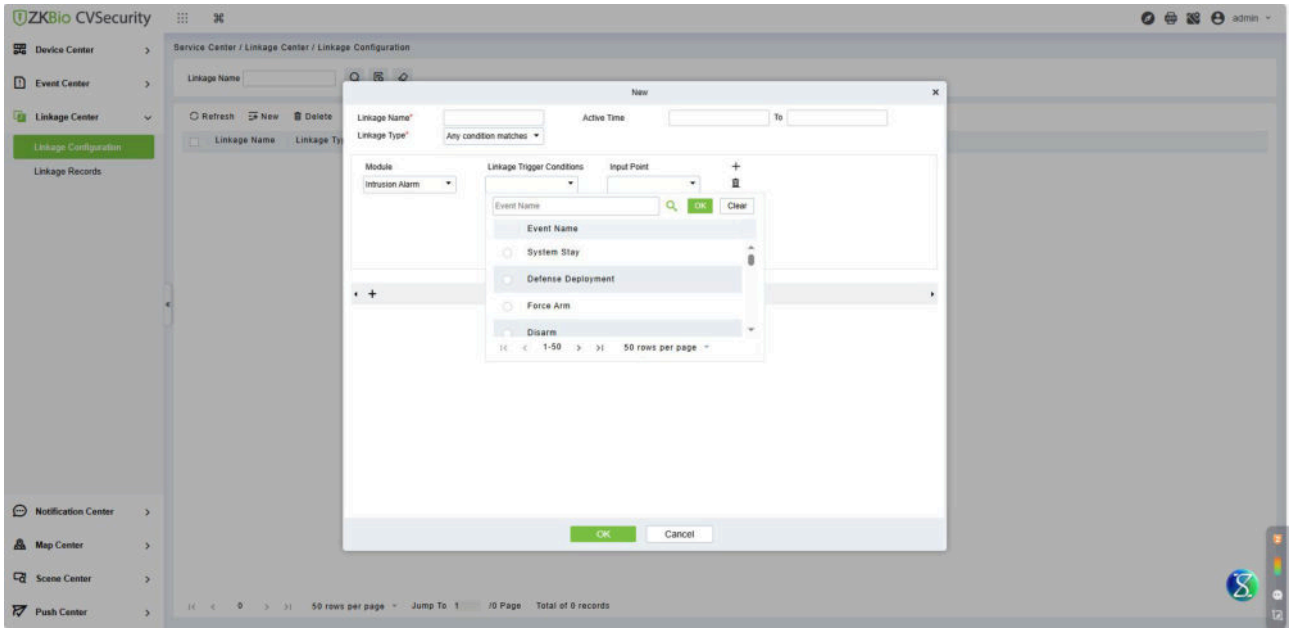
Step2: Select the video linkage for the output action, and check the box for video capture to complete the linkage configuration. Access control devices with doorbell function will activate the camera to start capturing and recording when a person rings the doorbell.



Note: Only ZKTECO video intercom devices support this function; DNK devices do not support it.

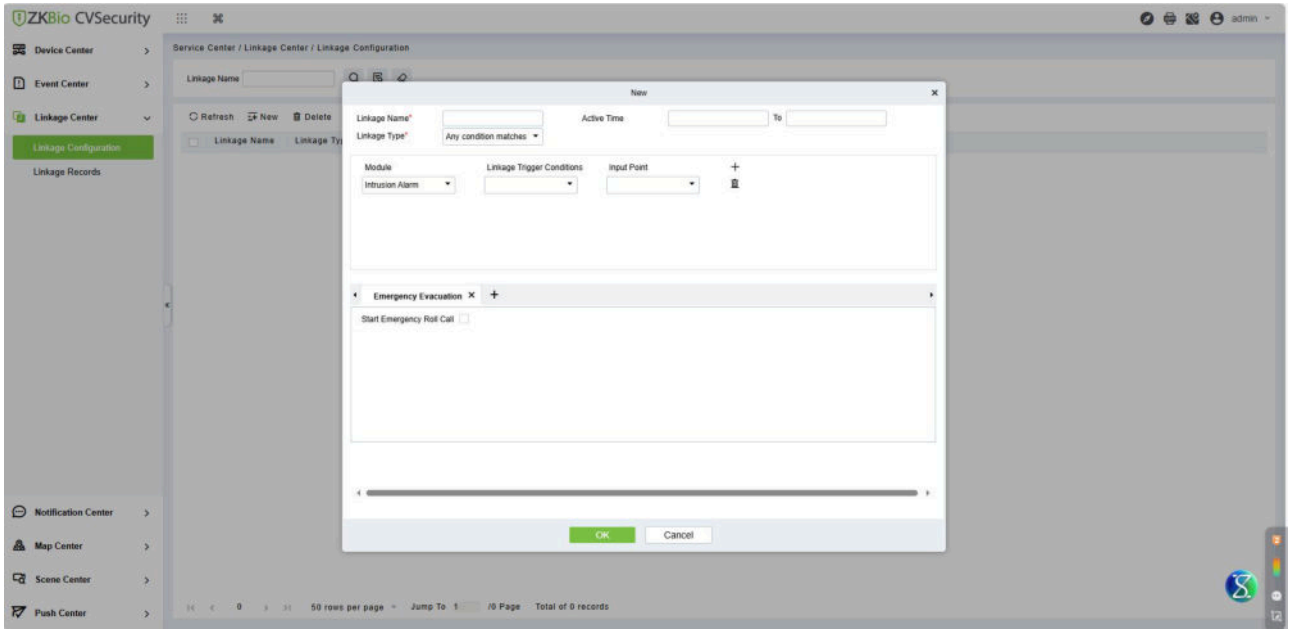
- **Linkage Center-The linkage trigger condition has added an Intrusion Alarm.**

Step: Enter Service Center → Linkage Center → Linkage Configuration, click "New" for editing, and in the module, you can select "Intrusion Alarm".

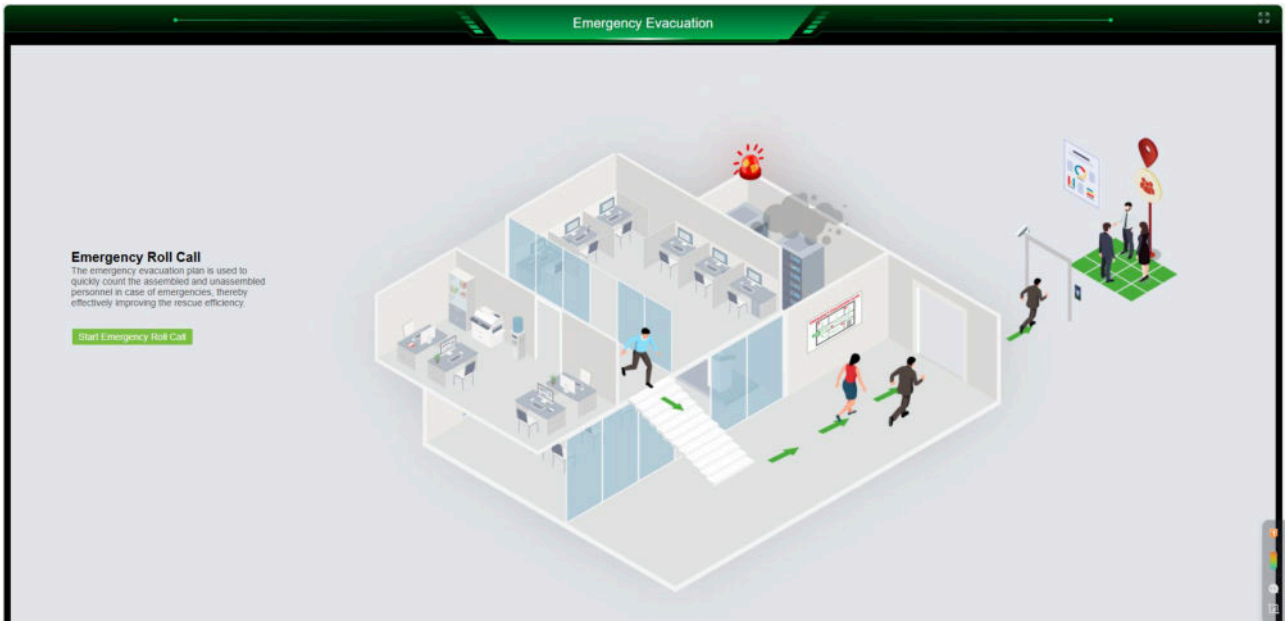


- **Linkage Center-The output action has added an Emergency Evacuation.**

Step: Enter Service Center → Linkage Center → Linkage Configuration, click "New" for editing. In the output action bar, you can select the emergency evacuation.

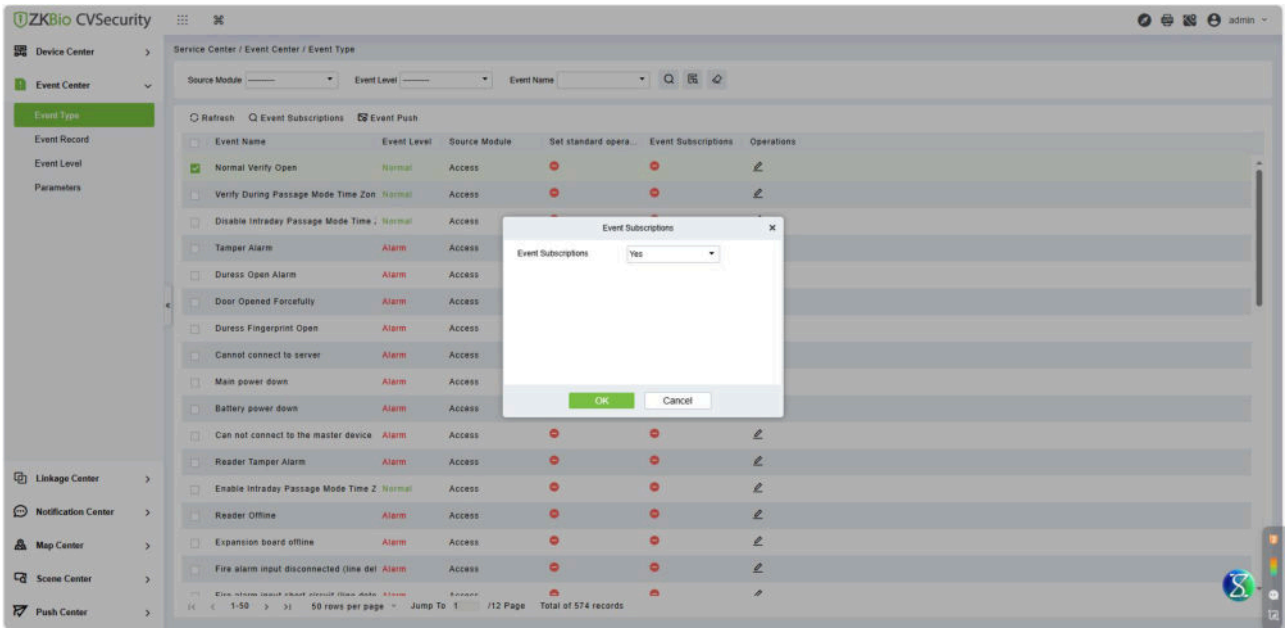


When the configured input action is triggered, the output action will be activated to start the emergency evacuation roll call.

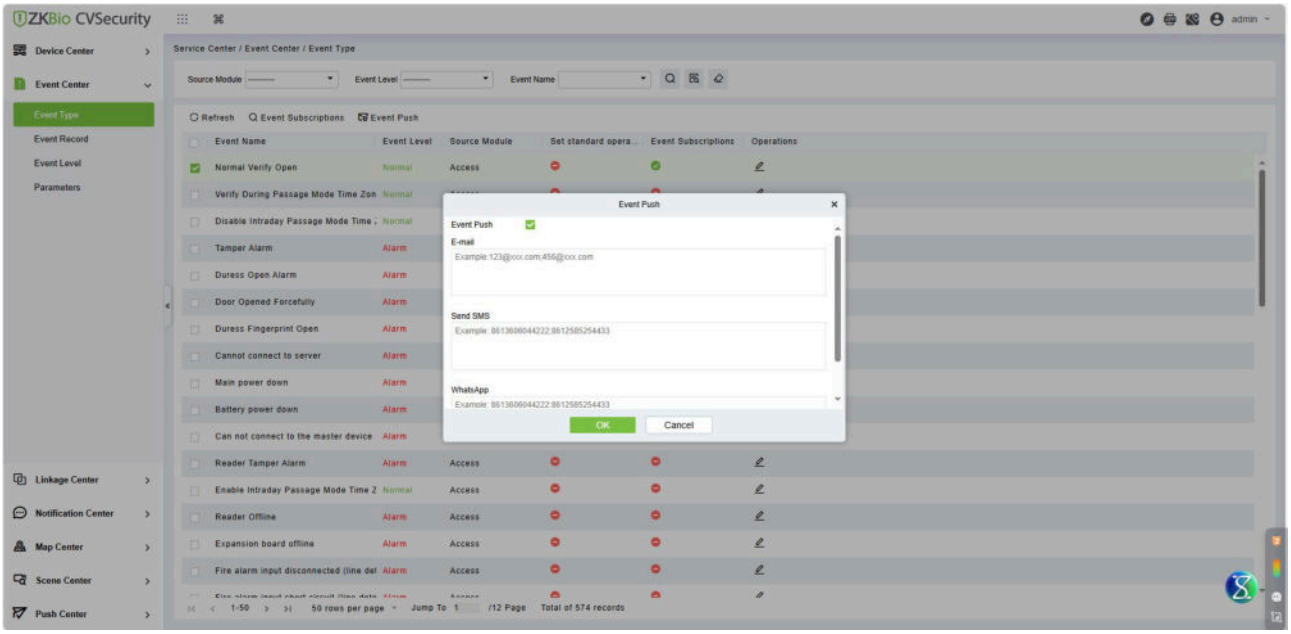


- **Event Center-Added event subscription notifications.**

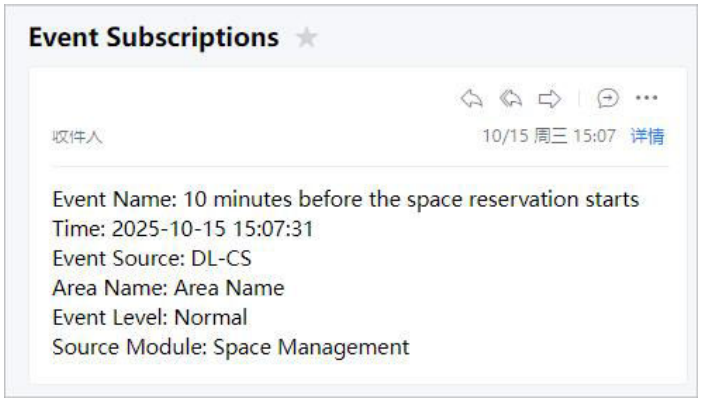
Step1: Service Center → Event Center → Event Type, select multiple event types and then click "Event Subscriptions". Choose "Yes" and click "OK". The subscription status can then be viewed in the list.



Step2: Then, click "Event Push", check the "Enable Event Push" option in the new window, and fill in the email address. When the event occurs, a notification will be pushed via email to the designated personnel.

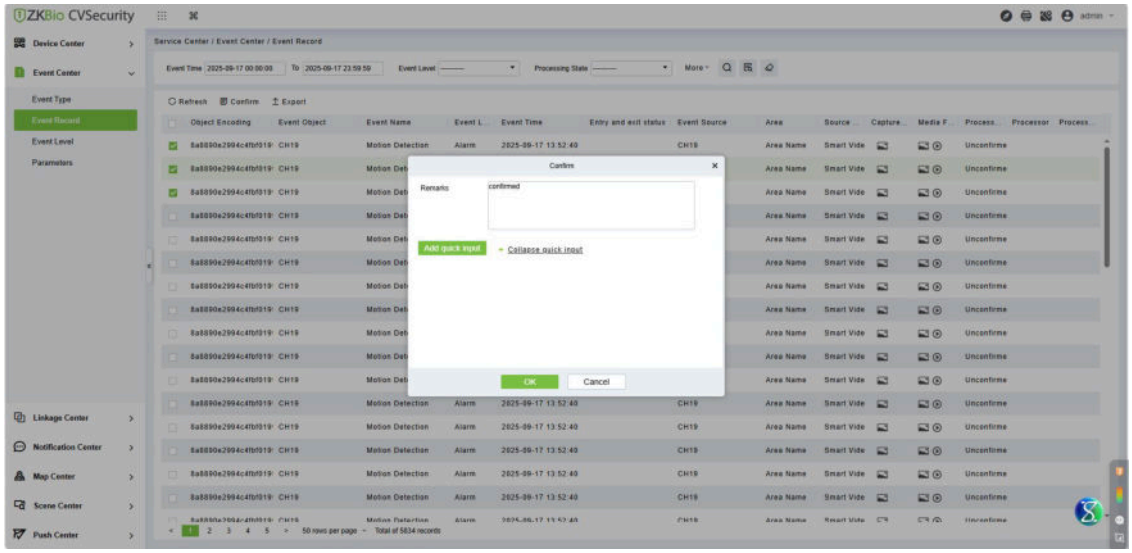


The content of the email is as shown in the following figure:



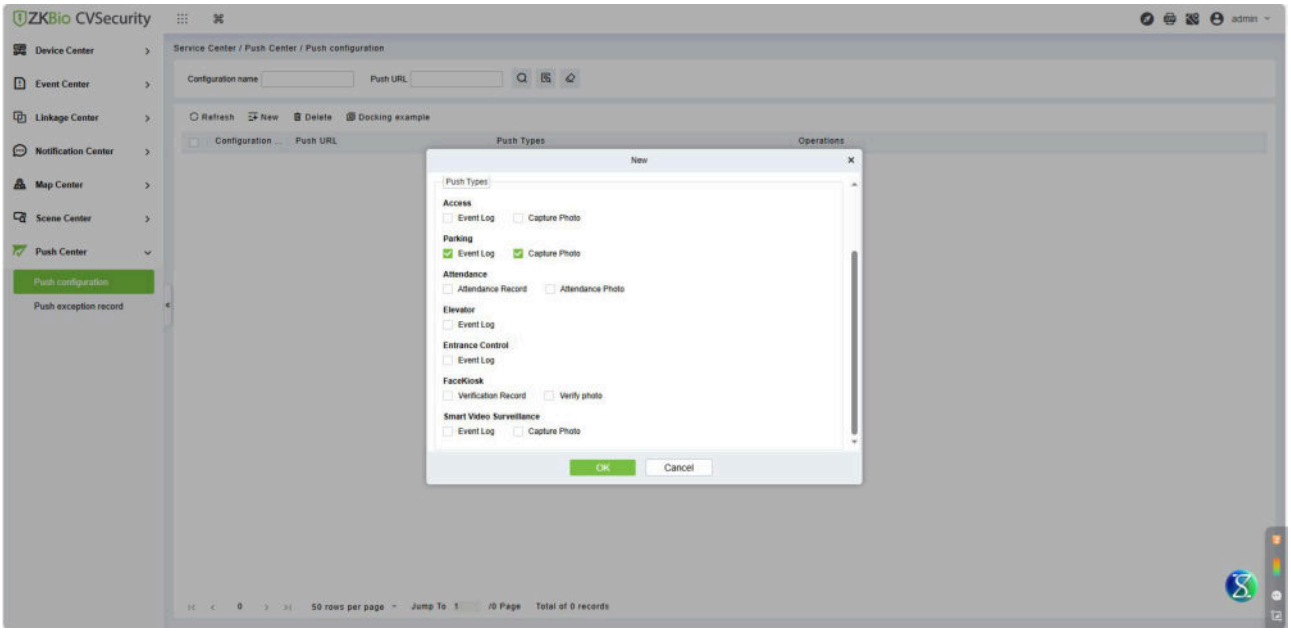
- **Event Center-Supports batch selection and processing of events.**

In the event record list, after selecting multiple events and clicking Confirm, enter the confirmation details and save. The processing status of the selected events will then change to "Confirmed".



- **Push Center-Added vehicle entry and exit records.**

Step: Enter the Service Center → Push Center → Push Configuration, click "New", and you can select the Event Log and Capture Photo of the parking module for push.



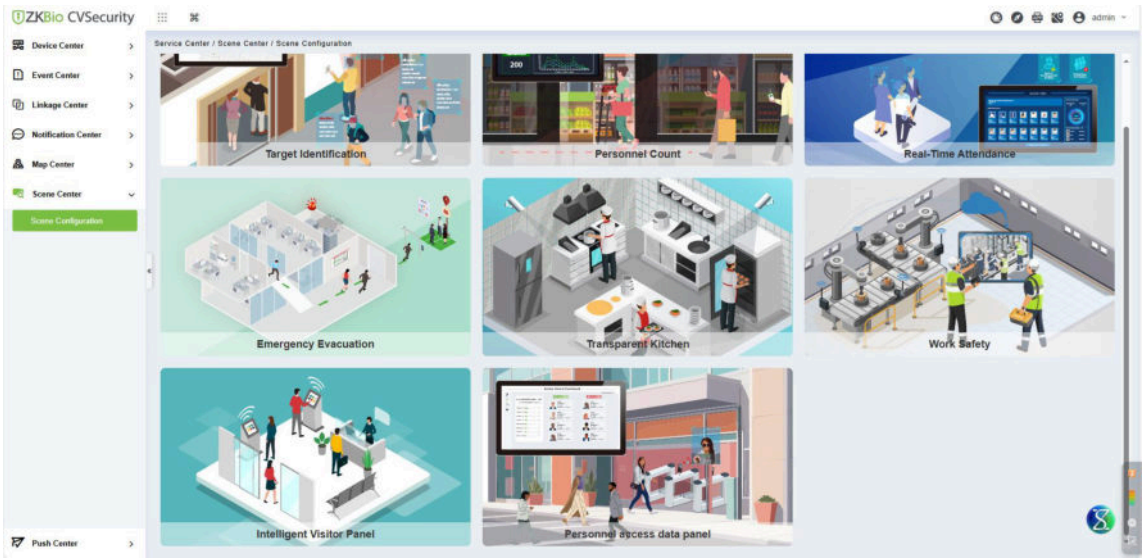
- **Scene Center-Added work safety scenarios.**

Applicable Scenarios: This scenario is applicable to settings such as construction sites or smart factories where safety operations and production requirements are critical.

Algorithms: The work safety algorithms include: safety cap、safety uniform、safety belt、reflective vest、respirator、fire、smoke、oil_spill、fire_equipment.

Operating Steps:

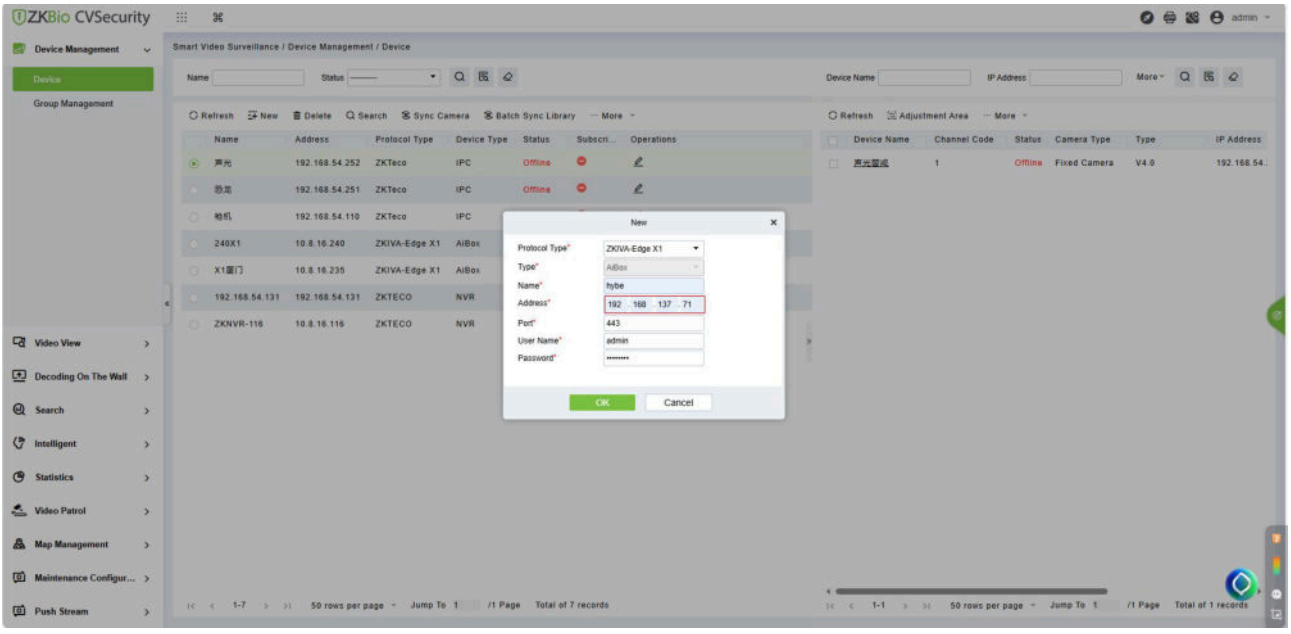
Enter Service Center → Scene Center → Scene Configuration, locate the Work Safety scene, and click "Configuring Scenarios".



Quickly complete the configuration by following the step-by-step guide on the right.

Step1: Add ZKIVA-Edge X1device

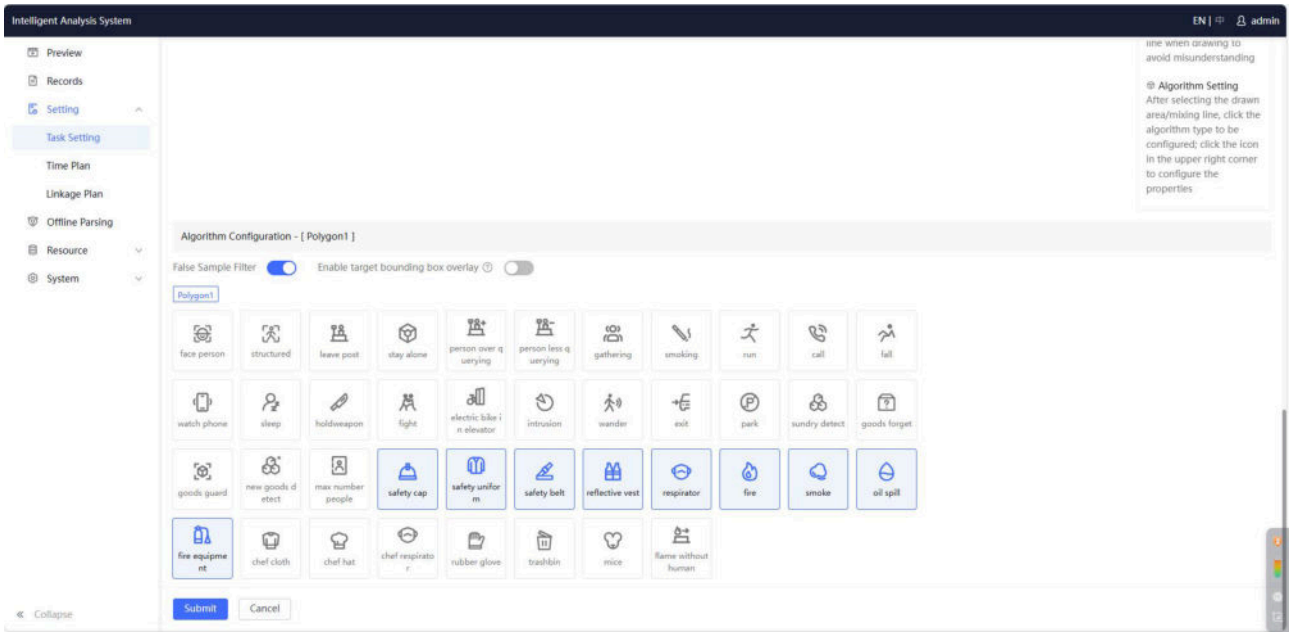
In the operation wizard, click "Add Device" to quickly jump to the device menu. Click "Add New" to include the ZKIVA-Edge X1 device, as shown in the figure below:



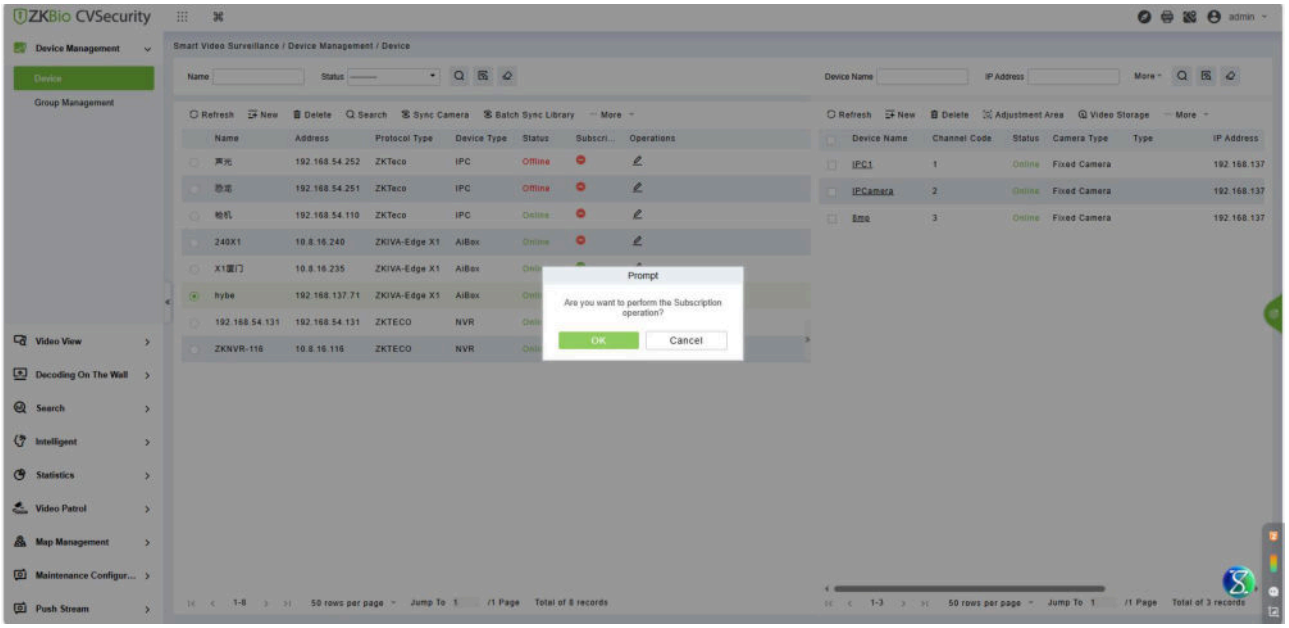
Step2: Configure Channel Intelligence

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 algorithm.

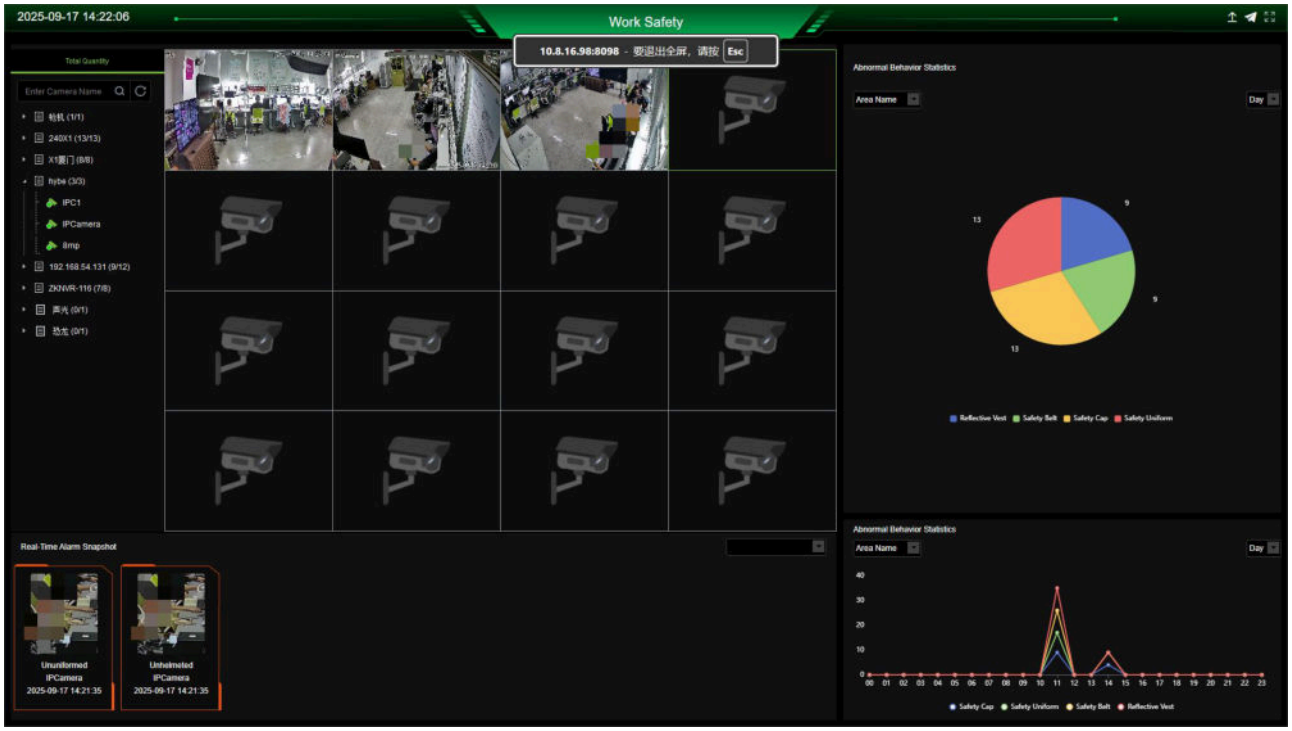
(Note: The IVS-X1 device must have the work safety algorithm package preconfigured before leaving the factory.)



After configuring the algorithms, return to the software interface, select the ZKIVA-Edge X1 device, click More > Subscription to begin receiving alerts.

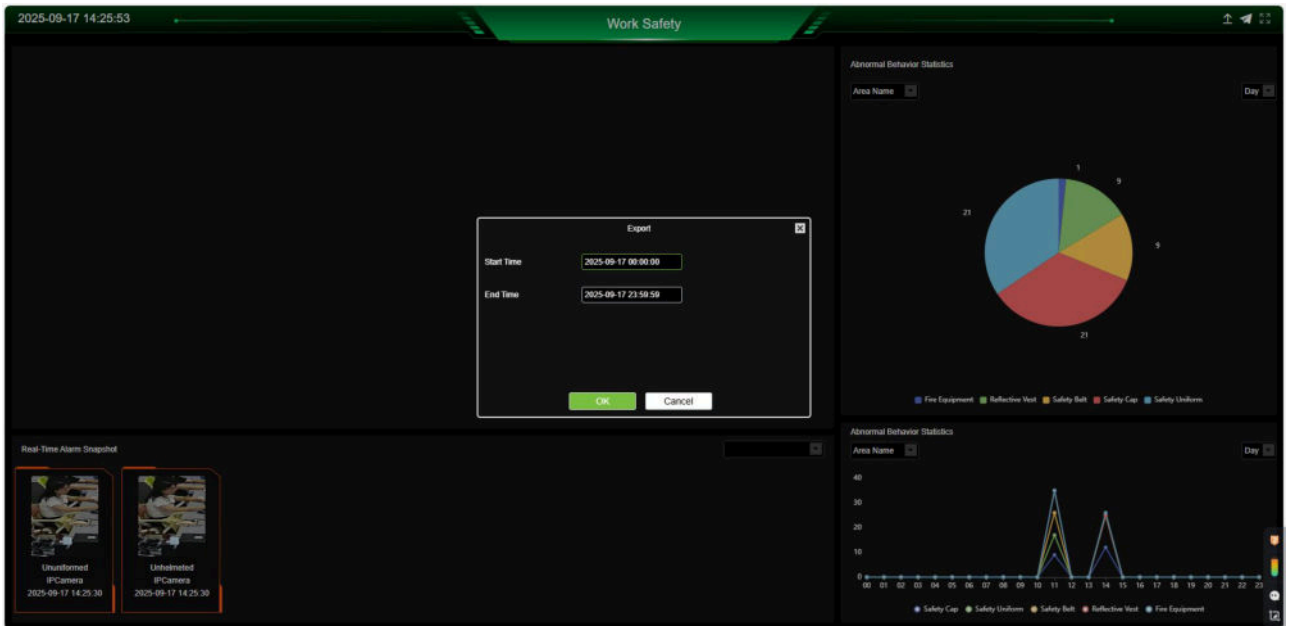


Step3: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:



■ 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:

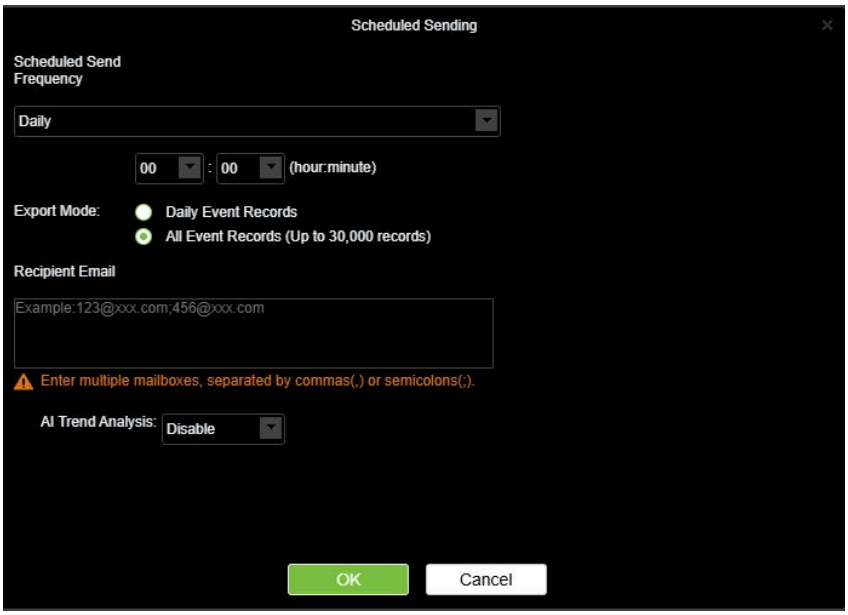


The exported report records are shown in the figure below:

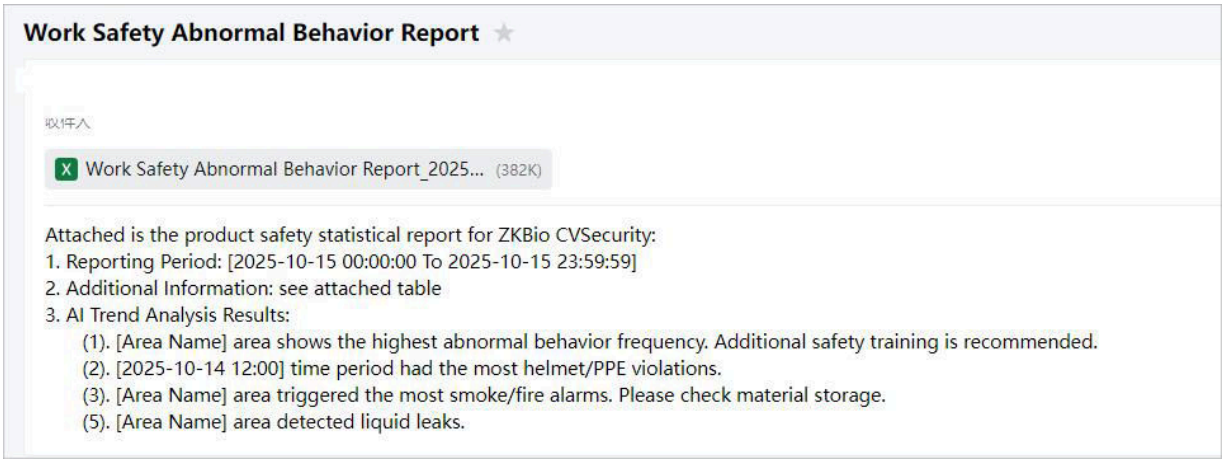
Work Safety Abnormal Behavior Report							
Event Name	Event Source	Area	Event Level	Event Time	Processing State	Processor	Processing Remark
Safety Cap	IPCamera	Area Name	Alarm	2025-09-17 14:26:19	Unconfirmed		
Safety Uniform	IPCamera	Area Name	Alarm	2025-09-17 14:26:19	Unconfirmed		
Safety Uniform	IPCamera	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		

■ 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:

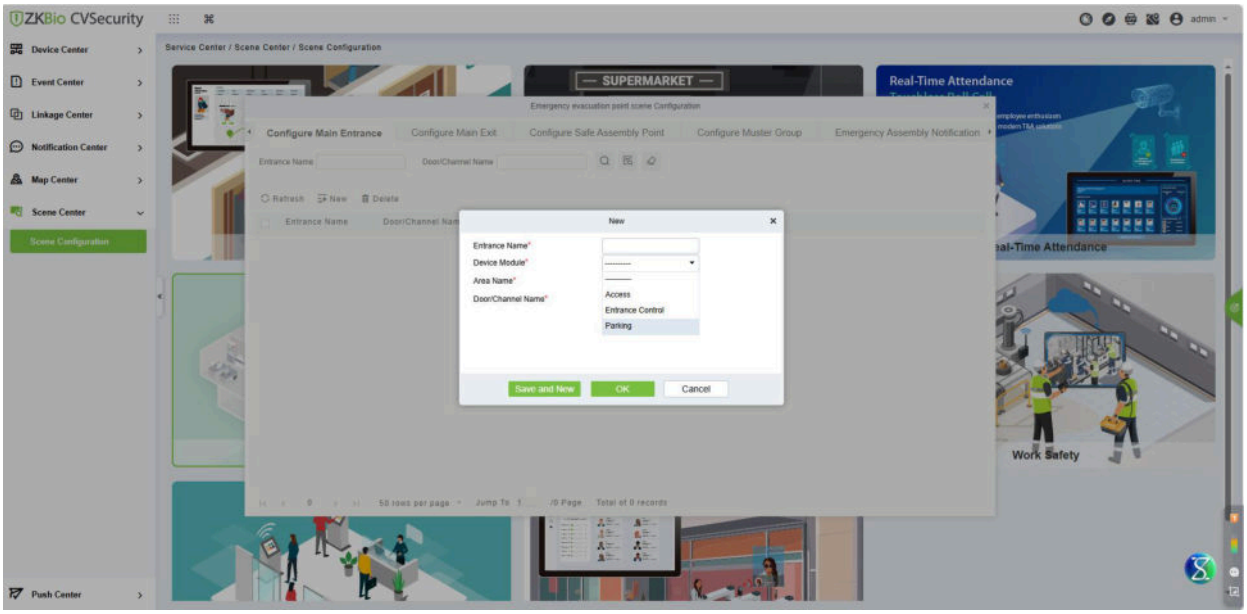


- Scheduled Send Frequency:
- Optional daily or weekly; If "Daily" is selected, you can further fill in the specific time. If "Monthly" is selected, you can further choose the exact date of each month for sending.
- Export Mode:You can choose daily event records or all event records.
- Recipient Email:Fill 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:



- **Scene Center-Emergency Evacuation Scene: Added support for parking module devices at the main entrance and exit.**

Step: Enter Service Center → Scene Center → Scene Configuration, select the Emergency Evacuation → Configuring Scenarios → Emergency Evacuation Basic Configuration. The equipment module can be optionally the parking module, as shown in the following figure::



Note: Select the LPR device in the door/passage name field.

- **Scene Center-Added Personnel Entry & Exit Panel.**

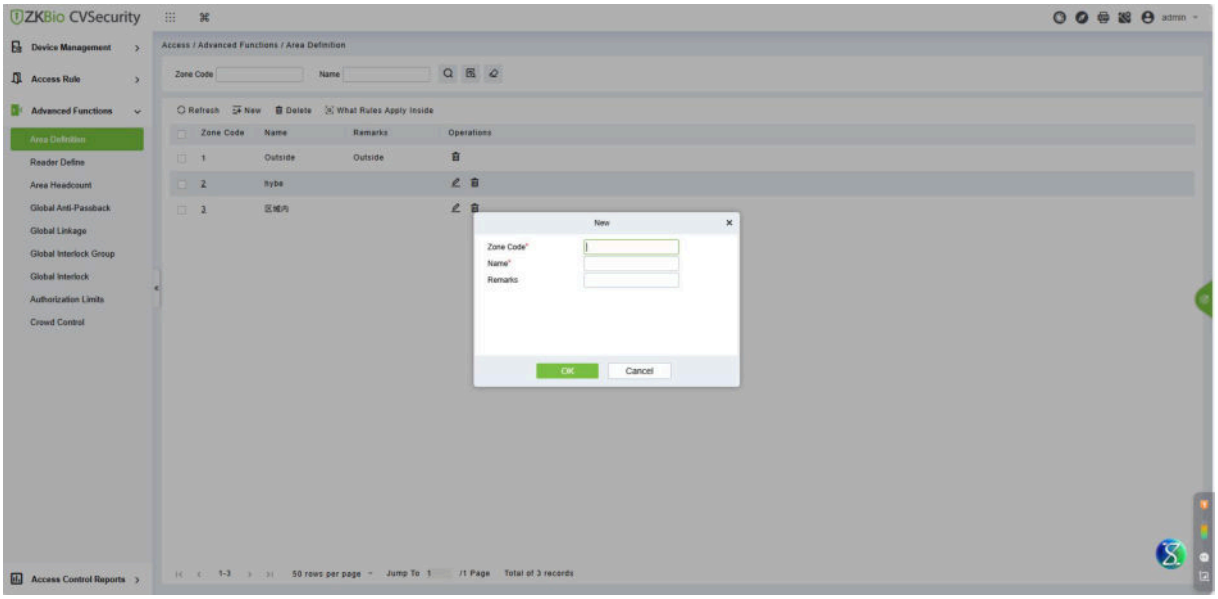
This panel, by providing accurate and real-time personnel dynamic data, it becomes a key infrastructure for improving factory/park safety, operational efficiency, management refinement level, and compliance capabilities.

Operating Steps:

Enter Service Center → Scene Center → Scene Configuration, locate the Personnel Access Data Panel scene, and click "Configuring Scenarios".

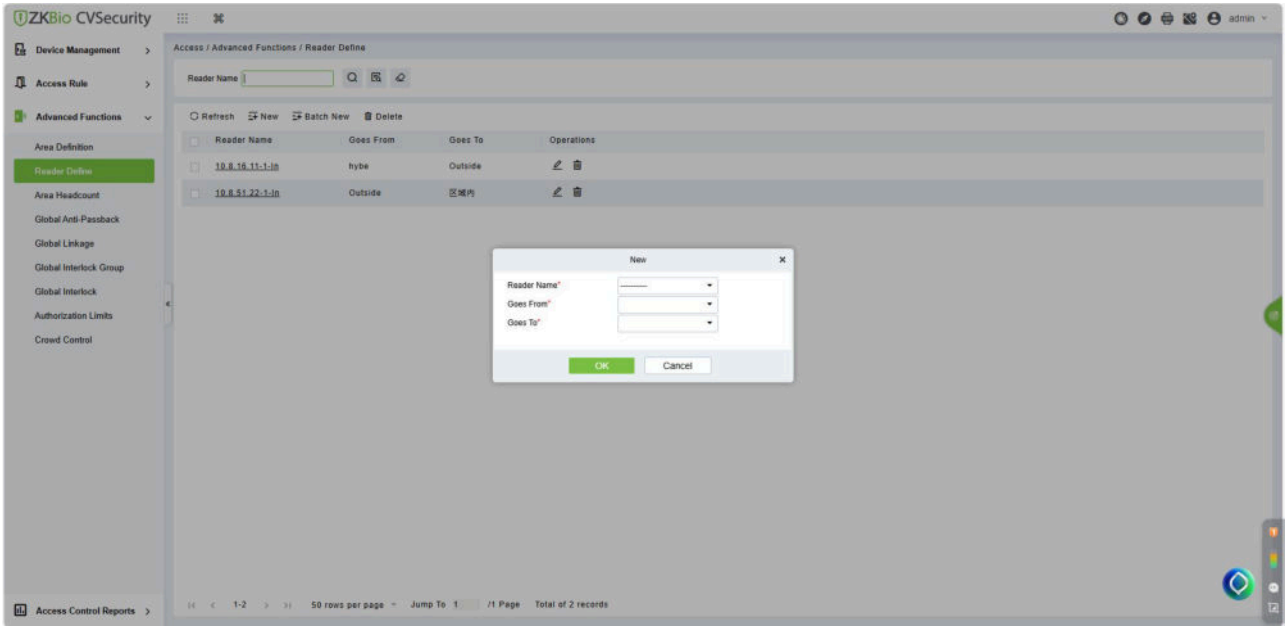
Step1: Access control area configuration

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:

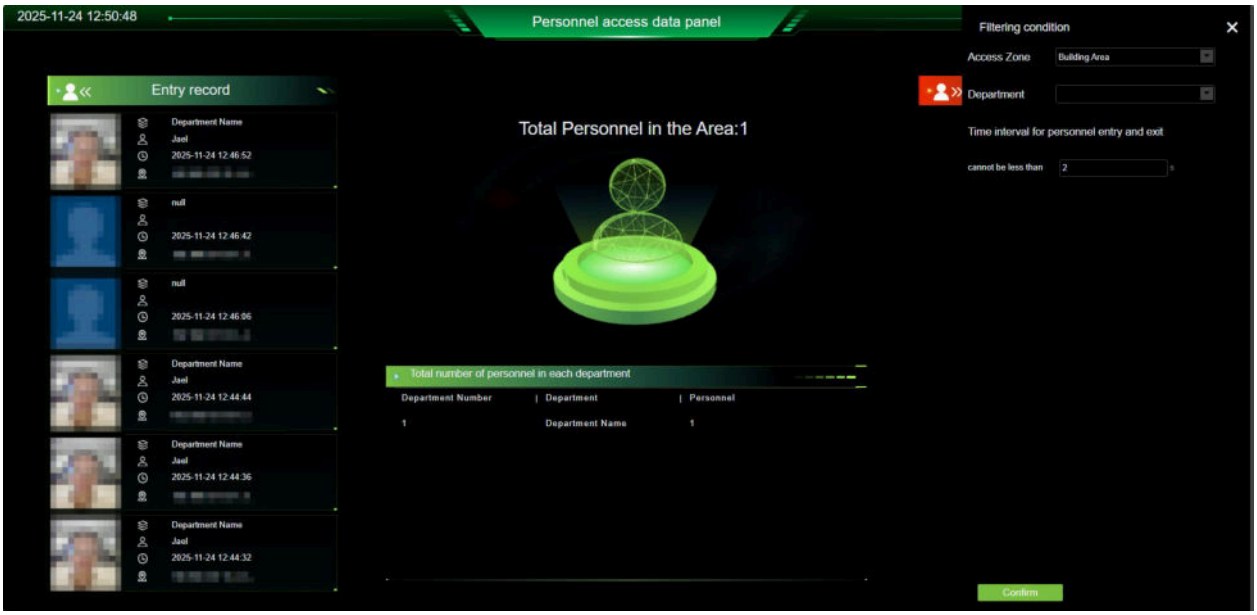


Step2: Reader definition configuration

Please configure the reader definition.Configure the input and output reader for the dynamic data area in the 'Reader Definition',as shown in the figure below:



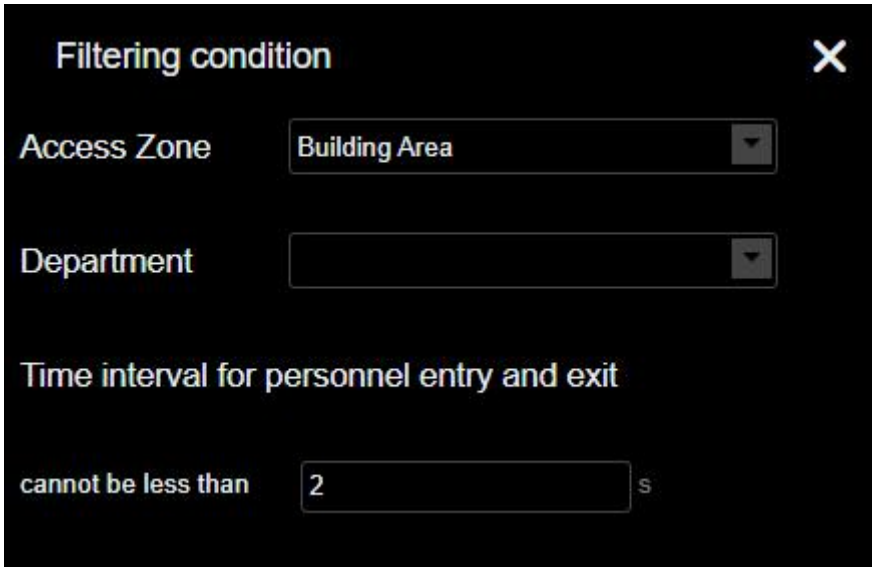
Step3: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:



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.

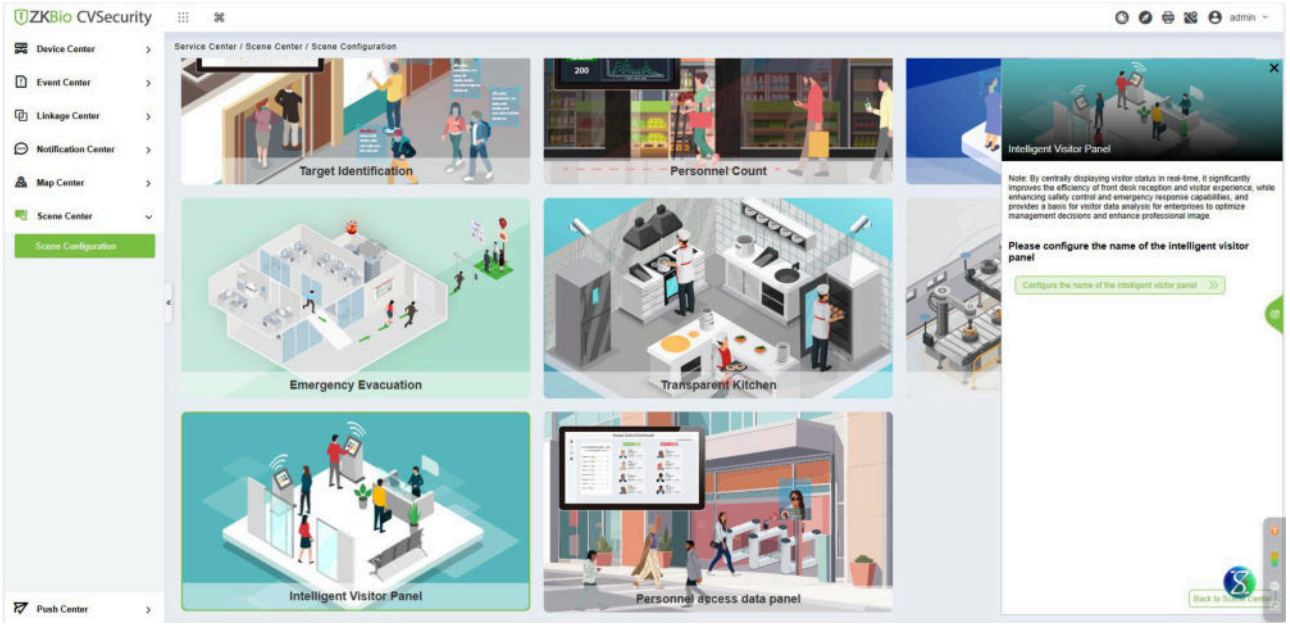


- **Scene Center-Added Intelligent Visitor Panel.**

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.

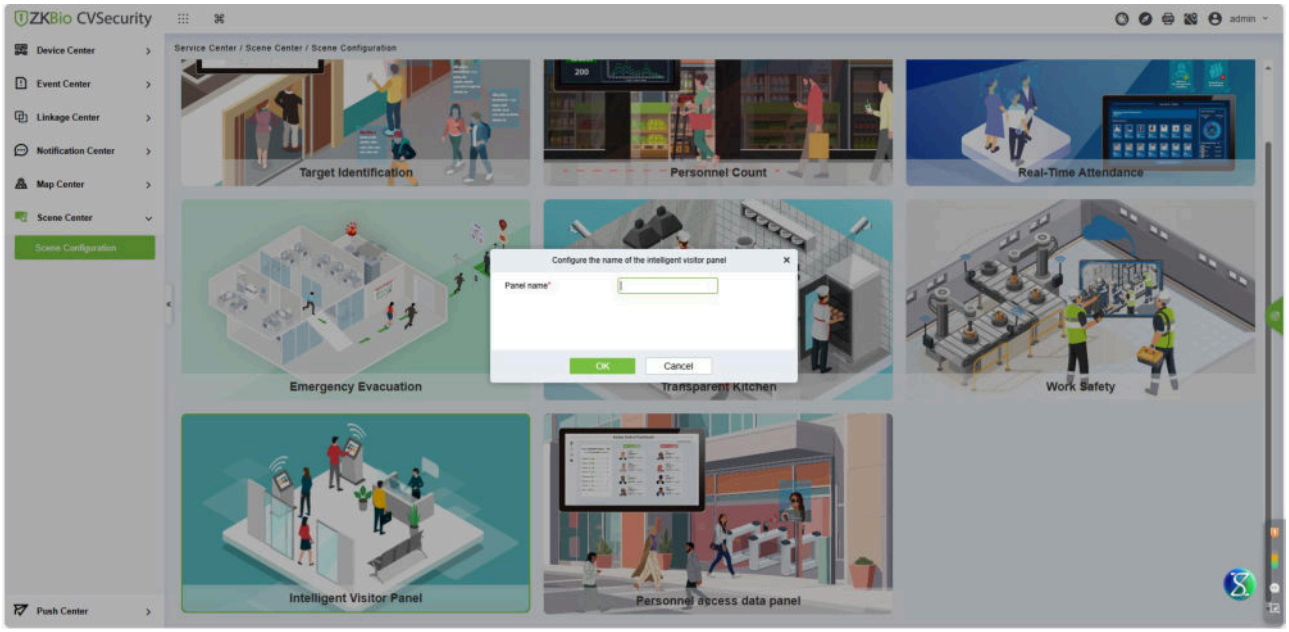
Operating Steps:

Enter Service Center → Scene Center → Scene Configuration, locate the Intelligent Visitor Panel scene, and click "Configuring Scenarios".

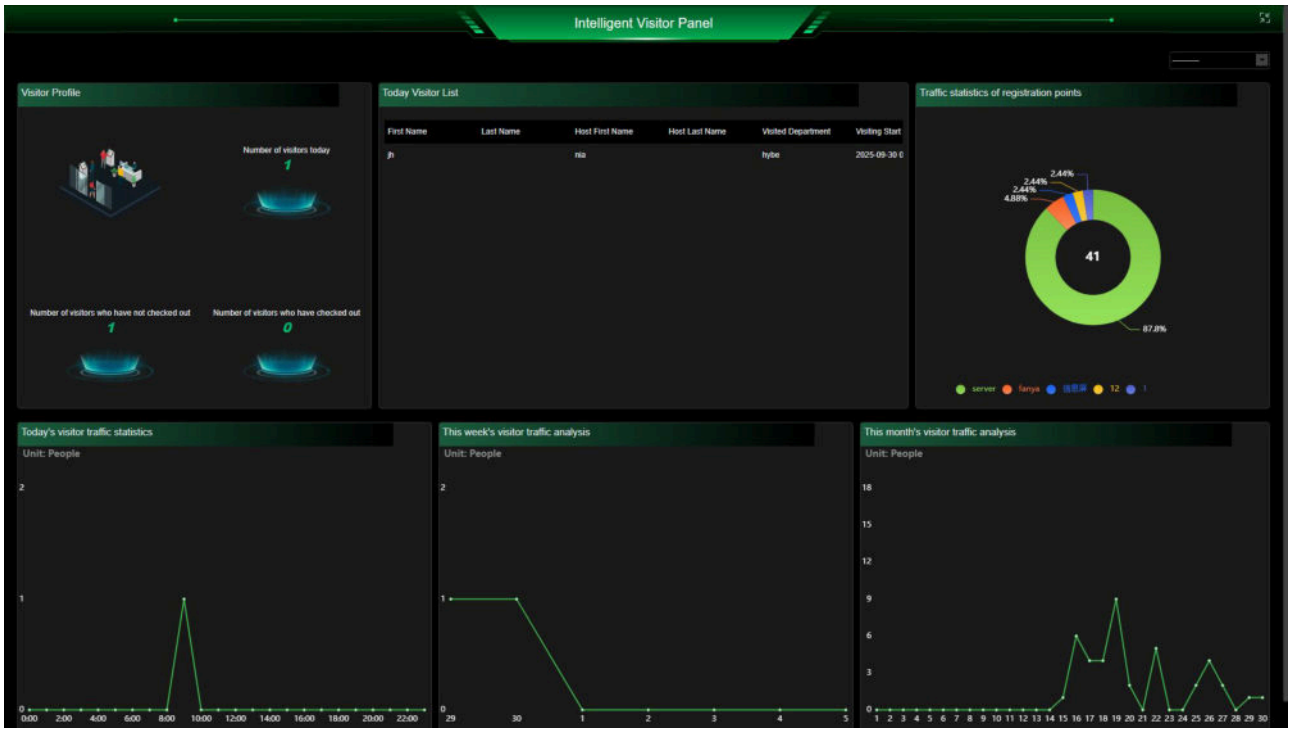


Step1: Configure the name of the intelligent visitor panel

Please configure the name of the intelligent visitor panel,as shown in the figure below:

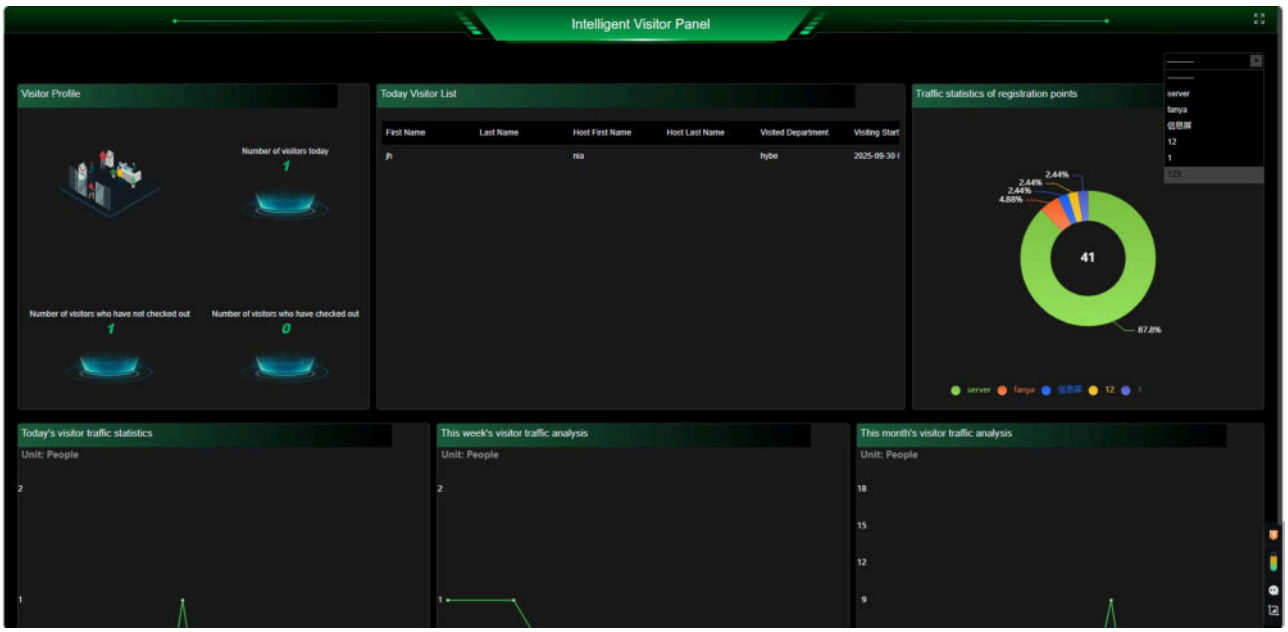


Step2: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:



■ Filtering condition

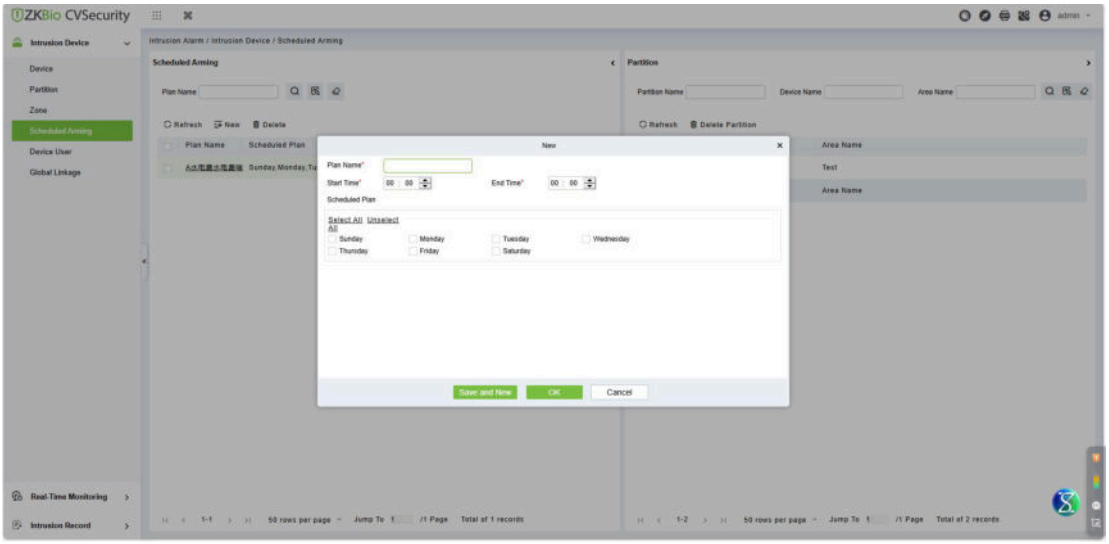
Click the the drop-down box in the upper right corner to select the Visitor Registration Point, as shown in the following figure:


Intelligent Visitor Panel
Visitor Profile
Number of visitors today
1
Number of visitors who have not checked out
1
Number of visitors who have checked out
0
Today Visitor List
First Name
Last Name
Host First Name
Host Last Name
Visited Department
Visiting Start
jh
nia
hybe
2025-09-30 (
Traffic statistics of registration points
server
fanya
12
1
2.44%
2.44%
2.44%
4.88%
41
87.8%
server
fanya
12
Today's visitor traffic statistics
Unit: People
2
1
This week's visitor traffic analysis
Unit: People
2
1
This month's visitor traffic analysis
Unit: People
18
15
12
9

Intrusion Alarm

- **Supports setting scheduled times for arming and disarming operations. For example, schedule automatic arming or disarming for after-hours and holidays in a chemical warehouse.**

Step: Enter Intrusion Alarm → Intrusion Device → Scheduled Arming, and click "New" to perform arming and disarming operations at scheduled times.

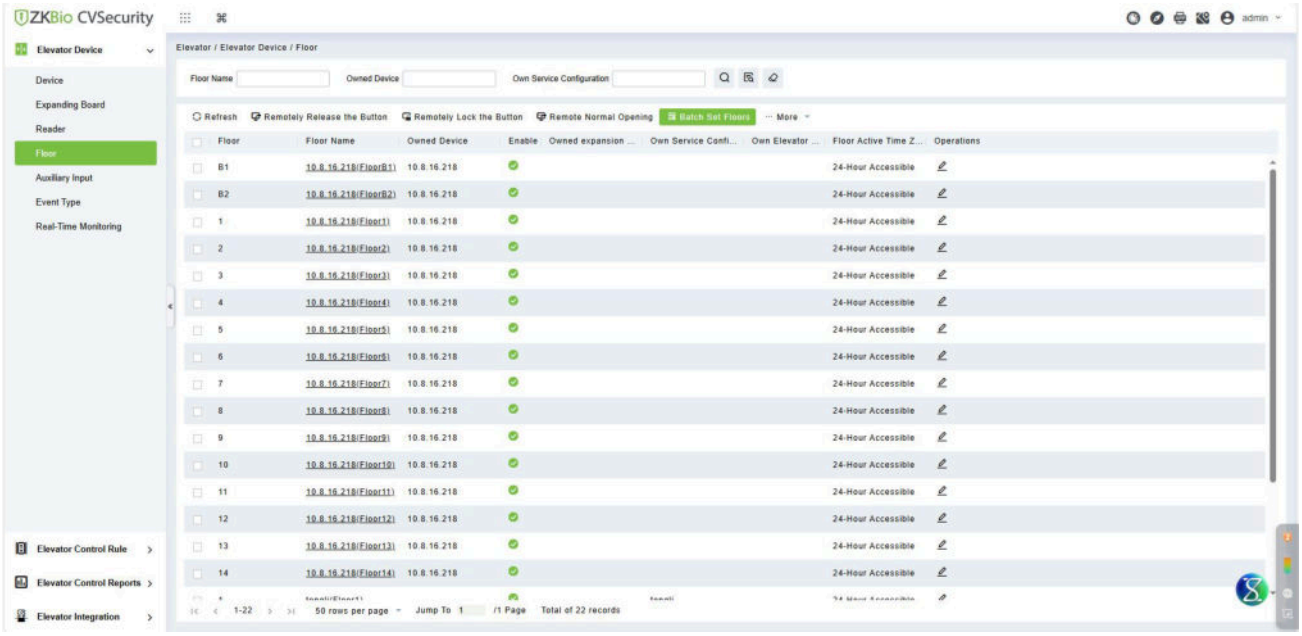


Elevator Control

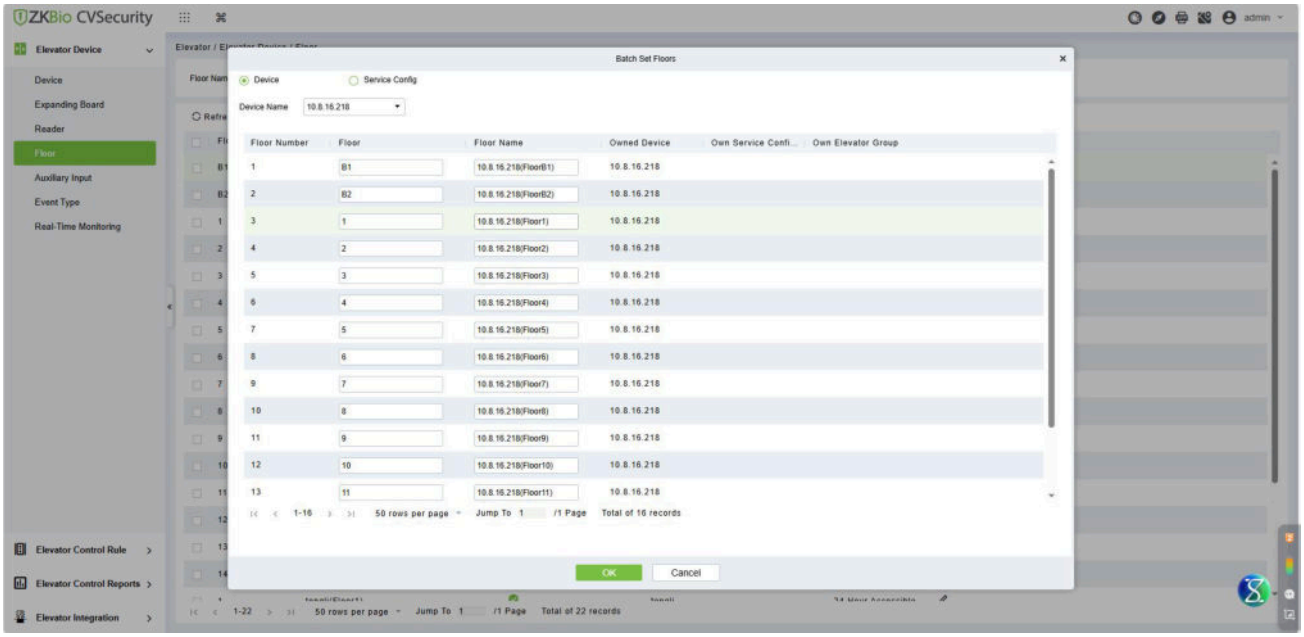
- **DCS function optimized**

1. Floor has added the function of Batch Set Floors. Solve the problems corresponding to the DCS floor.

Step1: Enter Elevator → Elevator Device → Floor, and click "Batch Set Floors".

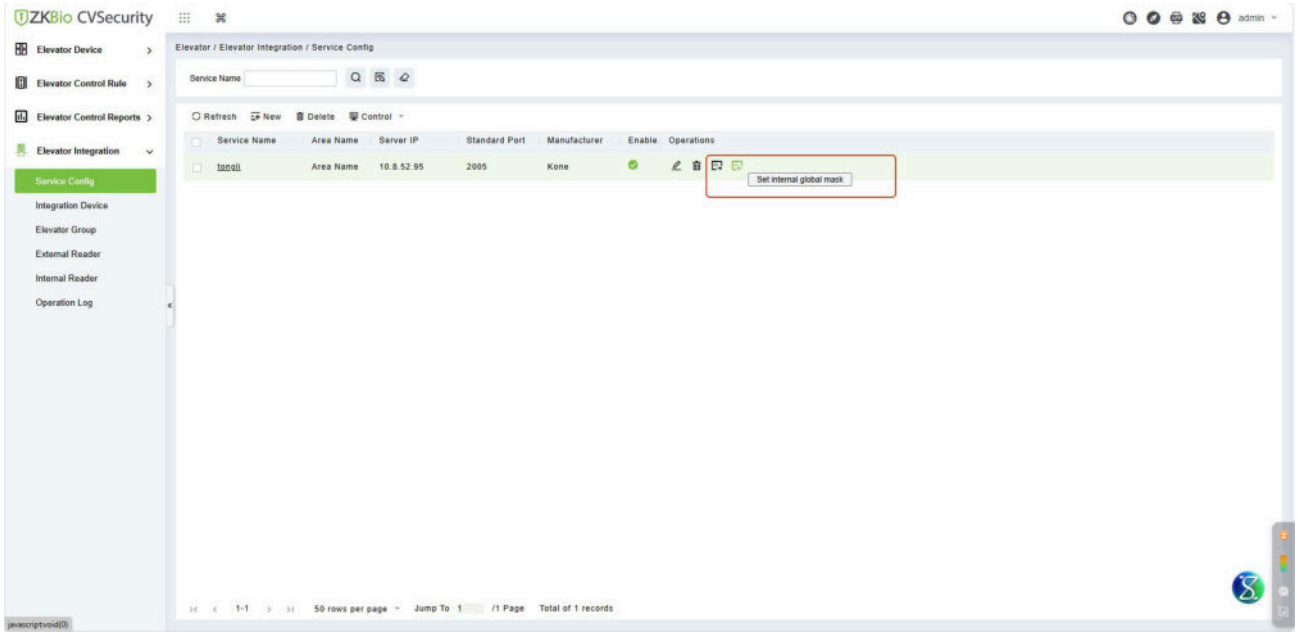


Step2: You can choose to set floors in batches by device or service config, and edit floor and floor name.

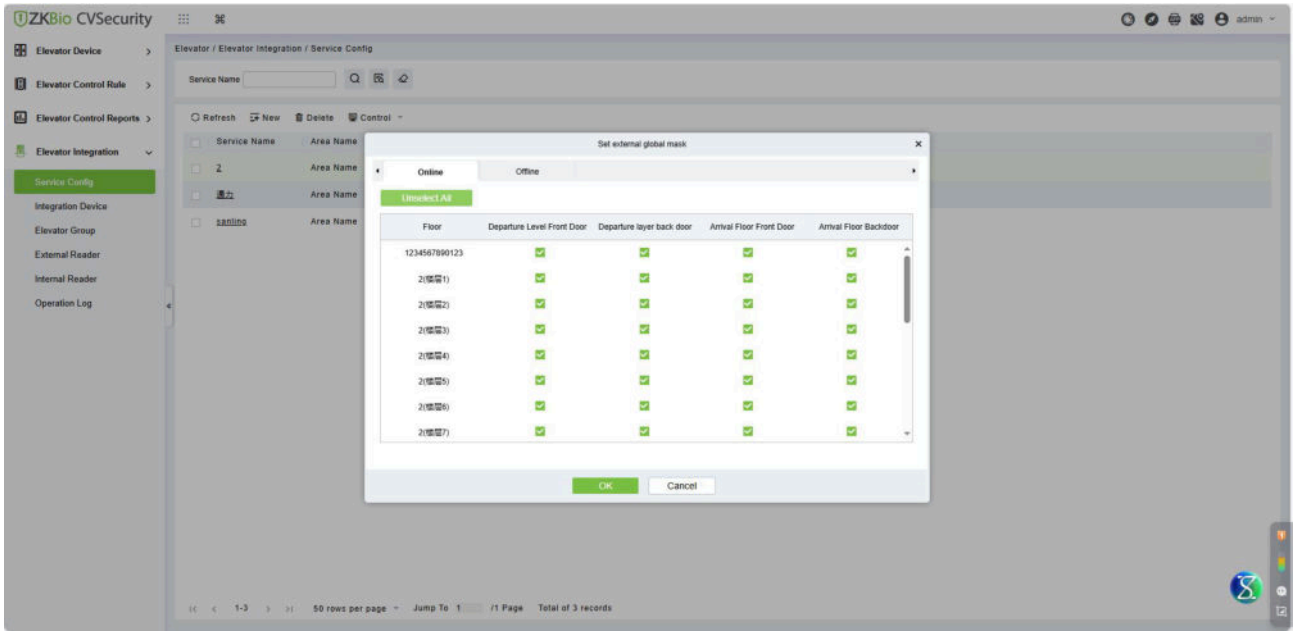


2. The DCS global mask and specified mask configuration interface support full selection.

Step1: Enter Elevator → Elevator Integration → Service Config, and click the mask setting icon in the operation column.

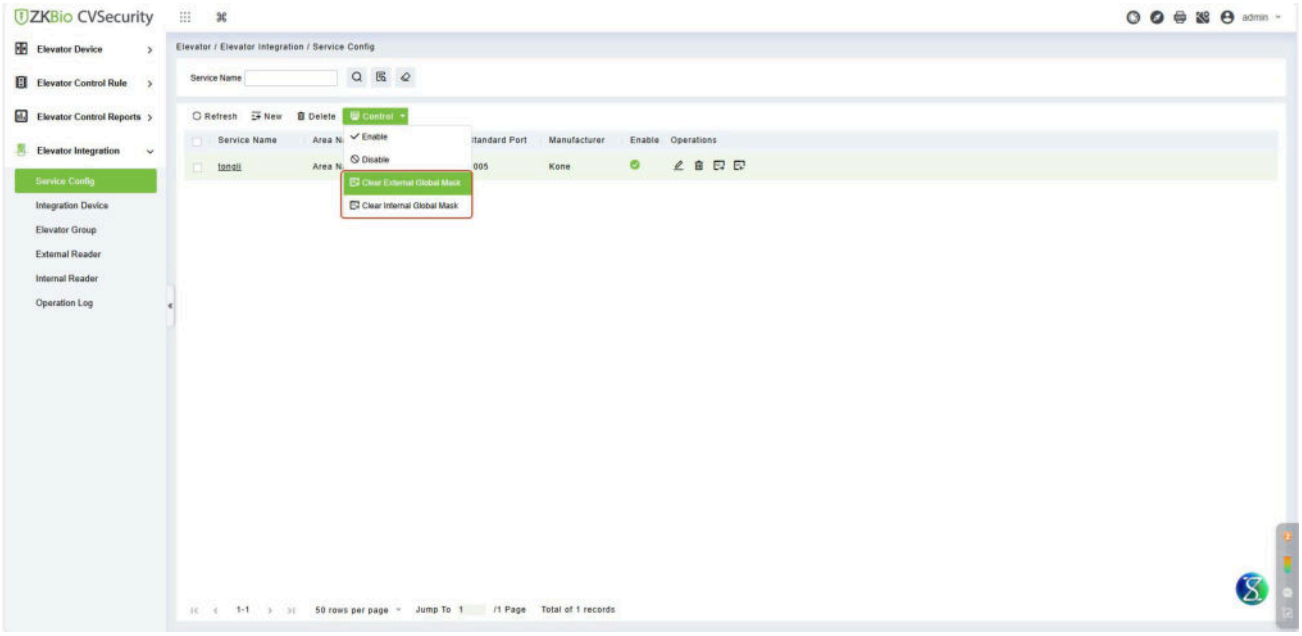


Step2: Click "Select All" to perform batch operations.



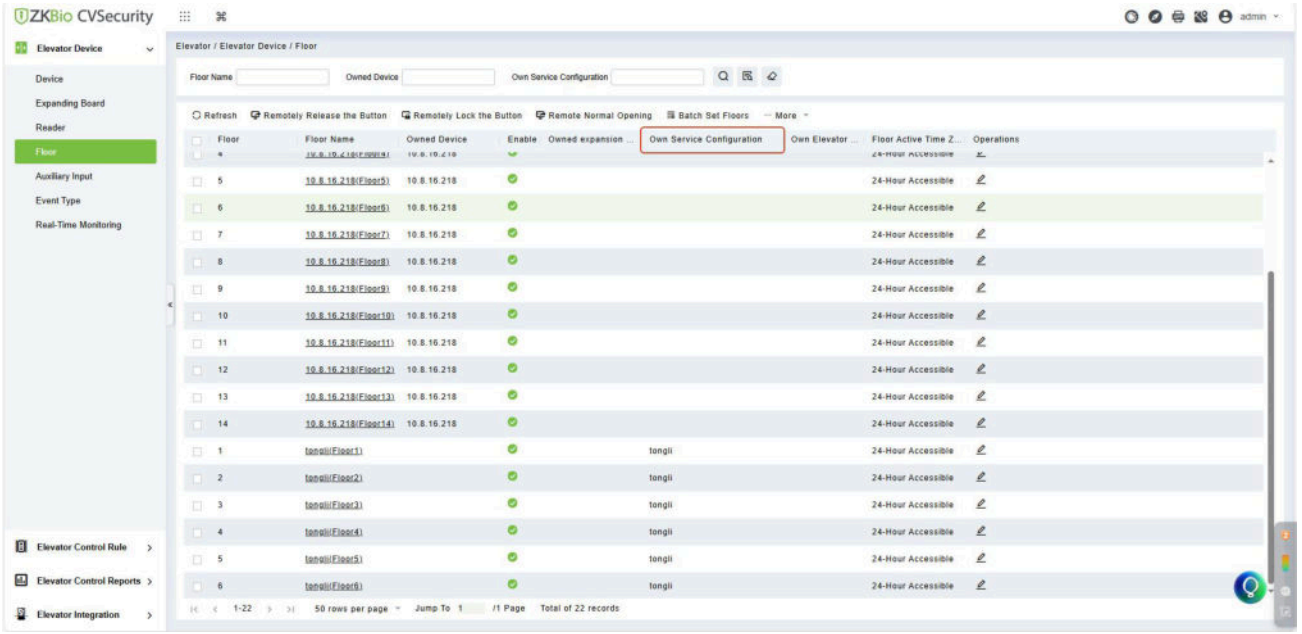
3. The service configuration has added a new operation to clear the mask.

Step: Enter Elevator → Elevator Integration → Service Config, select the service, then click "Control" → "Clear External Global Mask" or "Clear Internal Global Mask" to complete the mask clearing operation.



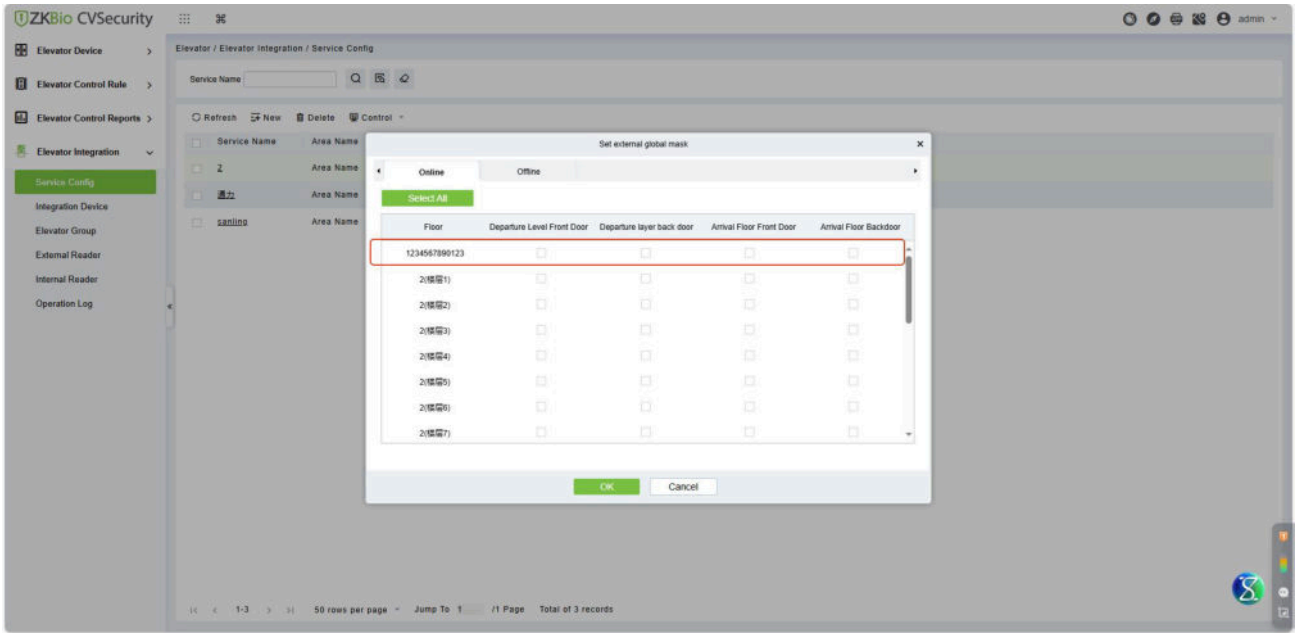
4. Add the search condition of "Owned Services" to the Floor menu.

Step: Enter Elevator → Elevator Device → Floor. In the search bar, you can search for floors through the Own Service Configuration.

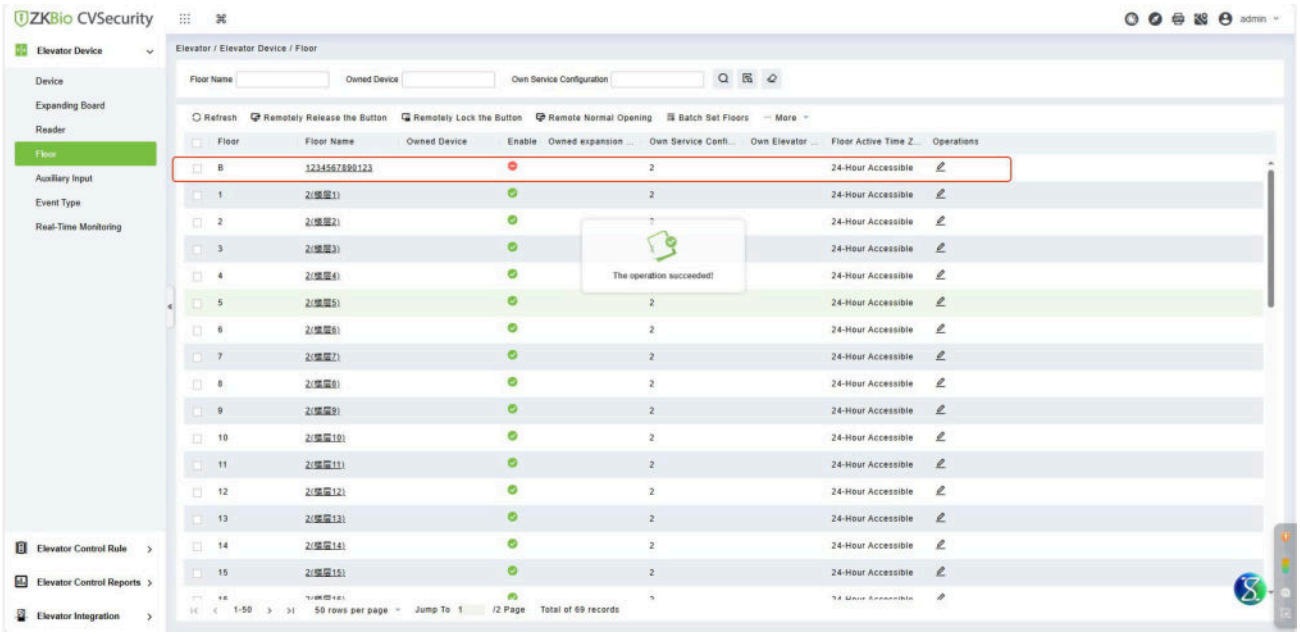


5. Floors that have been disabled may not appear under the mask configuration menu.

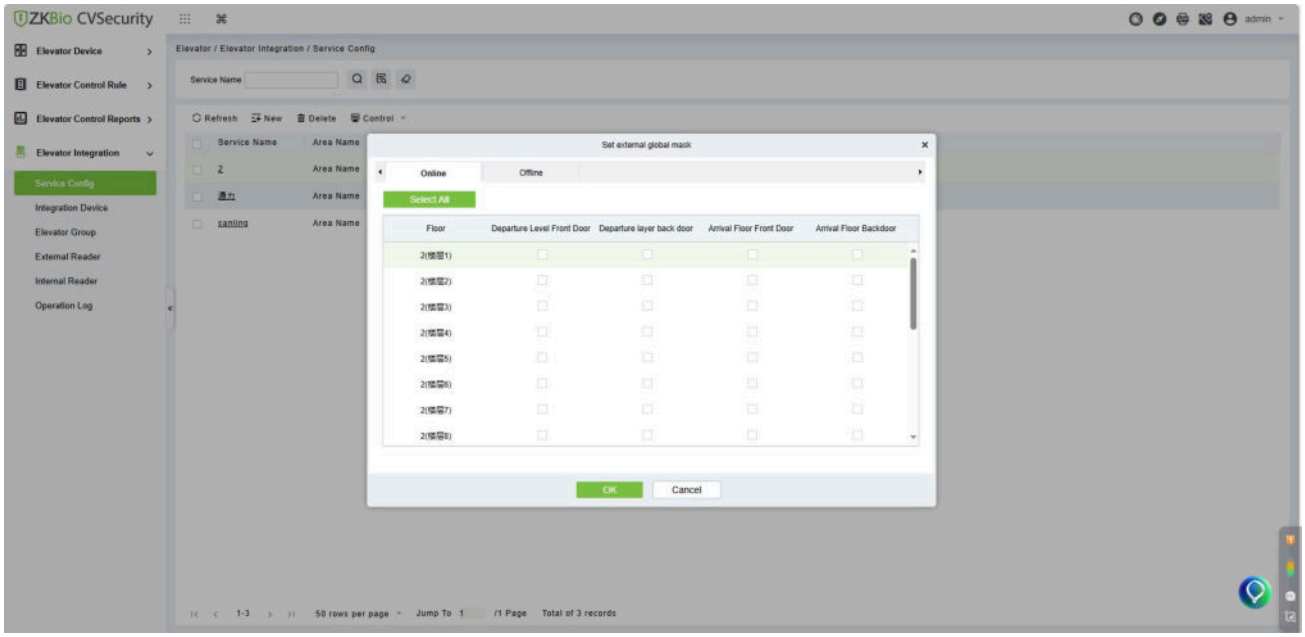
Step1: Enter Elevator → Elevator Integration → Service Config, click the mask setting icon in the operation column, and you can view and edit all enabled floors.



Step2: Enter Elevator → Elevator Device → Floor, select the floor and then click "More" → "Disable".

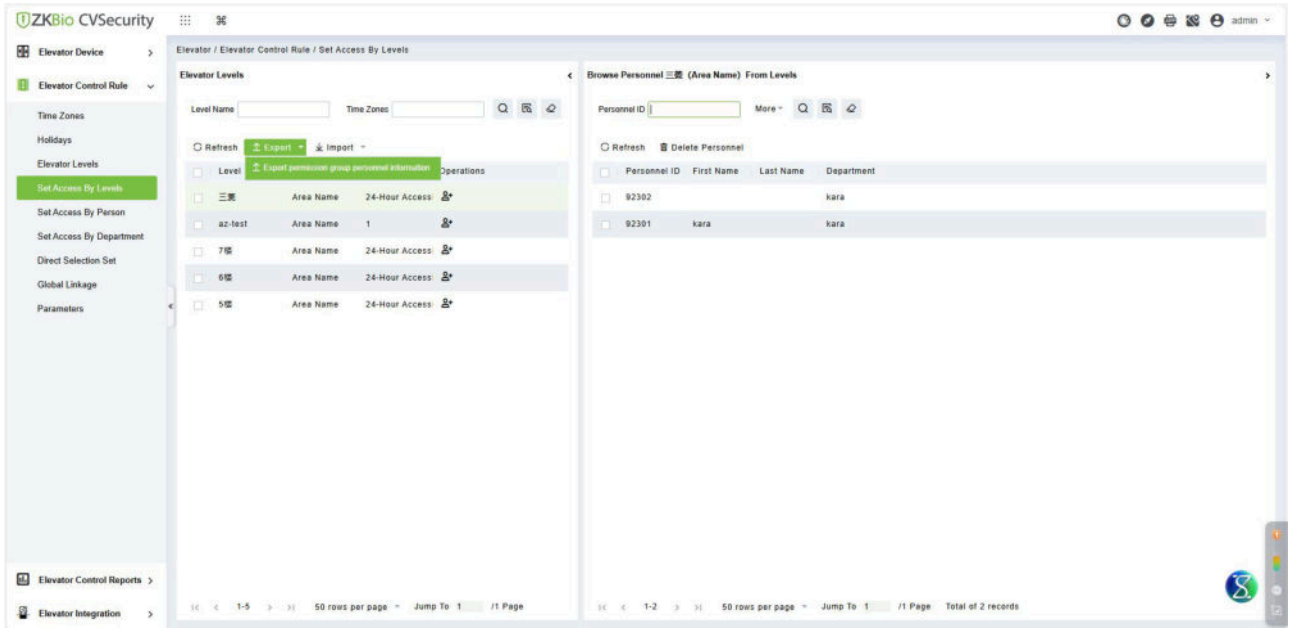


Step3: Return to Elevator → Elevator Integration → Service Config, click the mask setting icon in the operation column. Floors that have been disabled will not appear in the mask configuration menu.

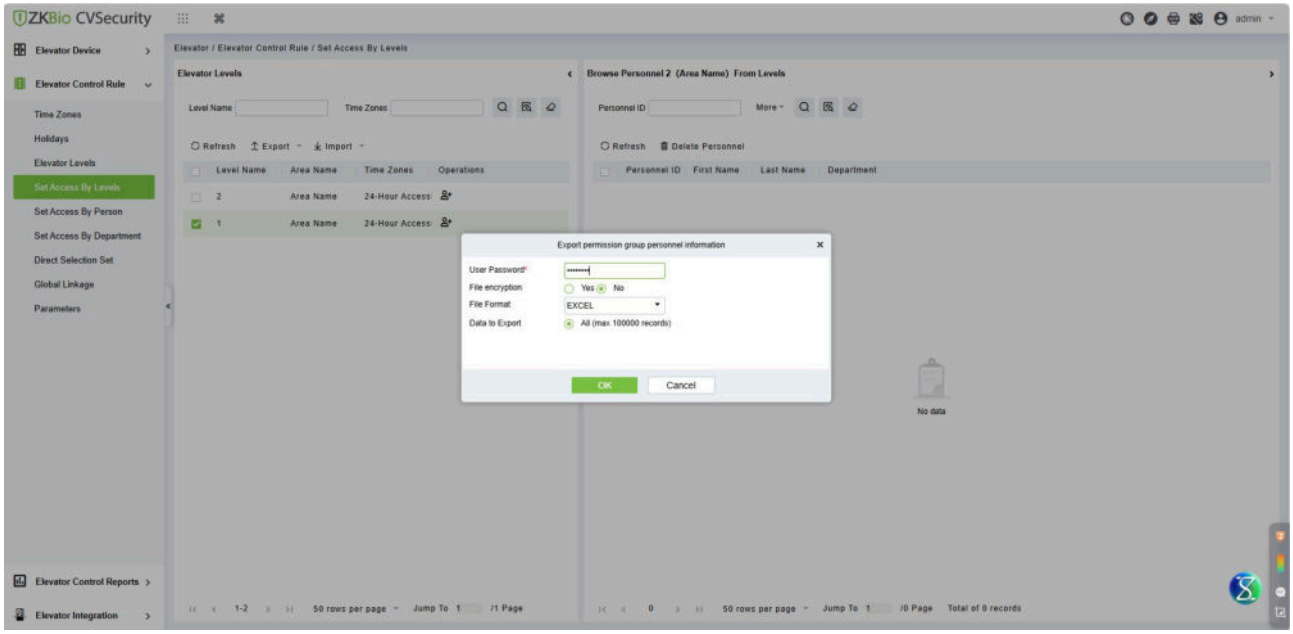


- **In the software elevator control module, under Elevator Control Rule → Set Access By Levels, the import and export functionality for permission group personnel information has been added. The fields include:Level Name, Personnel ID, First name and Last Name.**

Step1: Enter the Elevator → Elevator Control Rule → Set Access By Levels, check the left permission group, and click the "Export → Export Permission Group Personnel Information" button, as shown in the following figure.



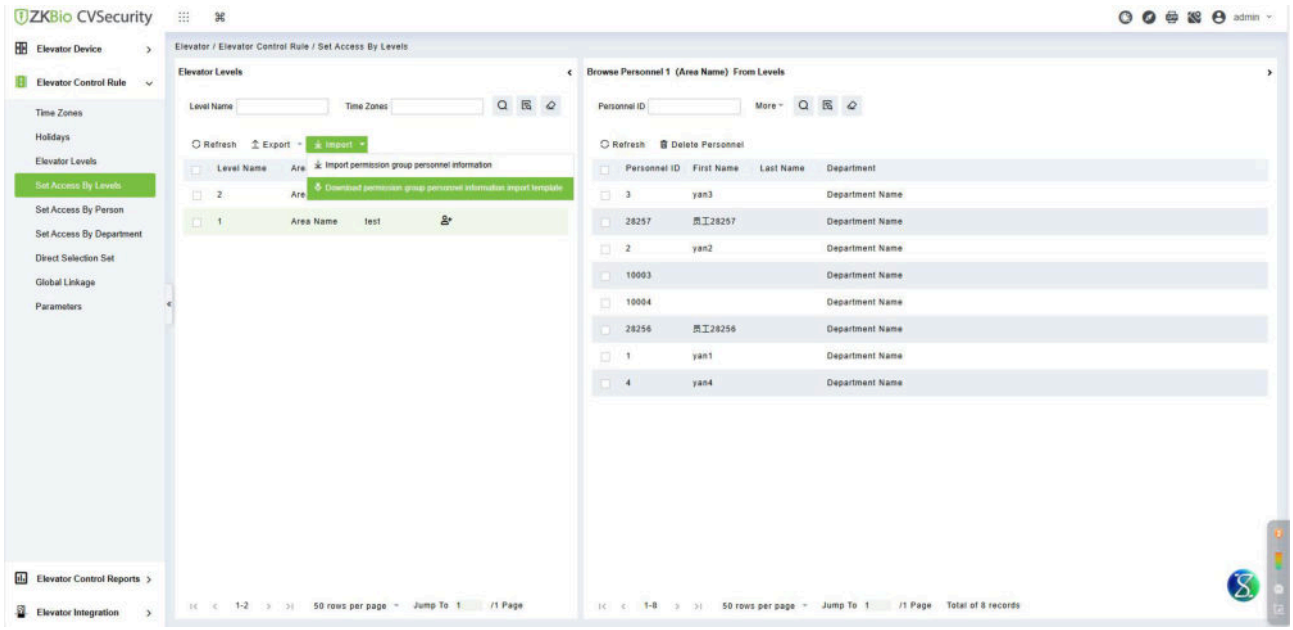
Step2: Enter the user password to start exporting the permission group.



The exported permission group is shown in the following figure, including: Level Name, Personnel ID, First name and Last Name.

Personnel information of the elevator control permission group			
Level Name	Personnel ID	First Name	Last Name
1	10003		
1	10004		
1	28256	员工28256	
1	1	yan1	
1	4	yan4	
1	3	yan3	
1	28257	员工28257	
1	2	yan2	

Step3: Enter the Elevator → Elevator Control Rule → Set Access By Levels, click "Import" → "Download permission group personnel information import template".

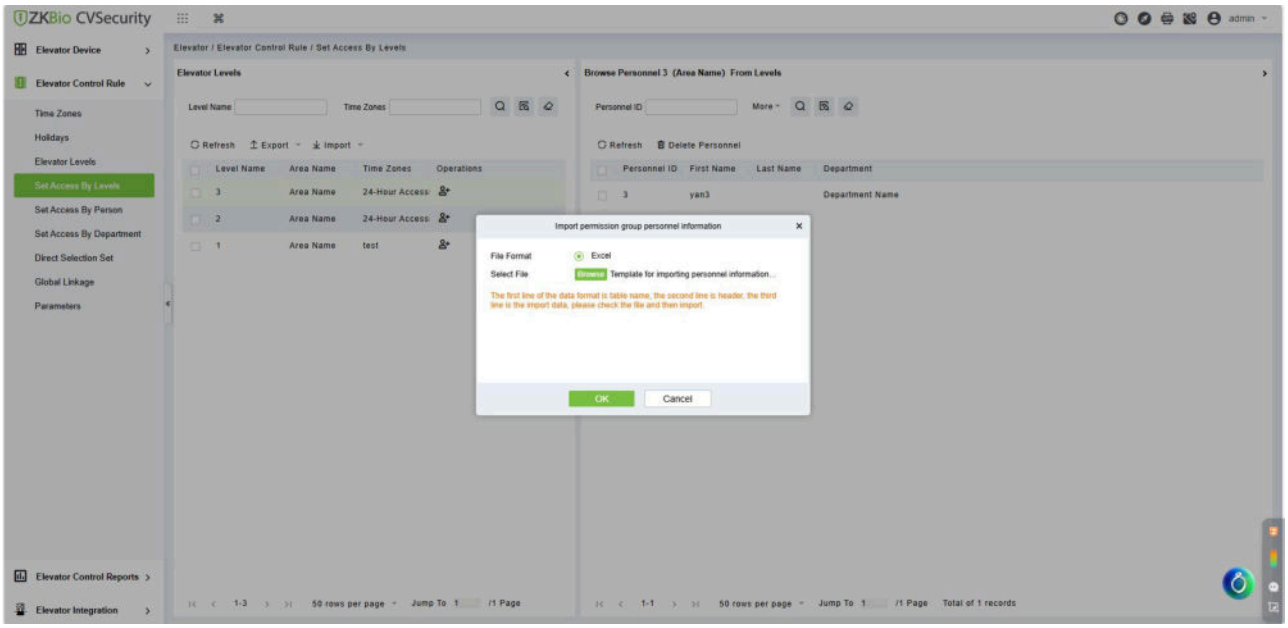


The template is shown in the following figure. Fill in the title content with: Level Name, Personnel ID, First name and Last Name.. After completion, save the template.

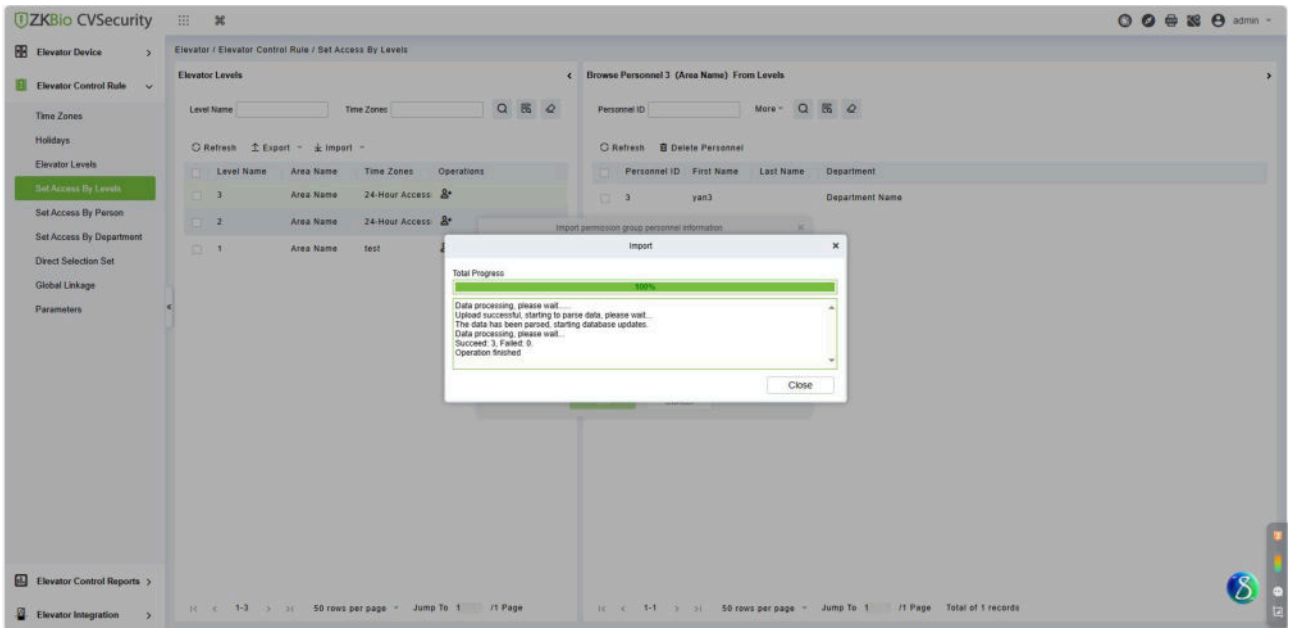
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.

Template for importing personnel information of elevator control permission group			
Level Name	Personnel ID	First Name	Last Name
1	1	yan1	
2	2	yan2	
3	3	yan3	

Step4: Return to the Elevator → Elevator Control Rule → Set Access By Levels, click "Import"→"Import permission group personnel information", select the template you just saved, and then click "OK".



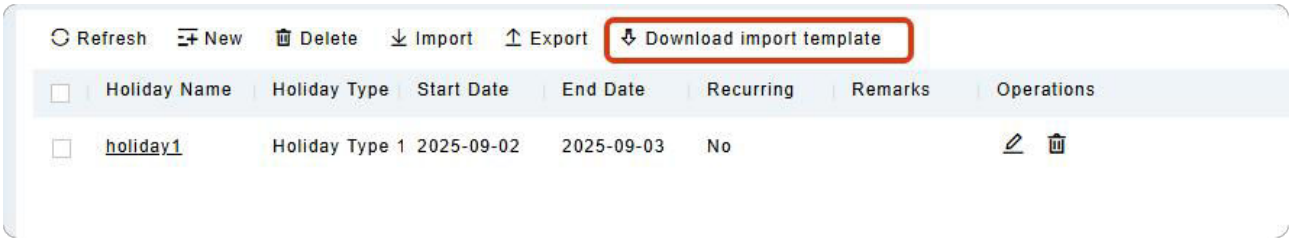
Data will start to be imported automatically until the operation completion prompt is given.



- **The holiday settings for Elevator Control now support batch import and export.**

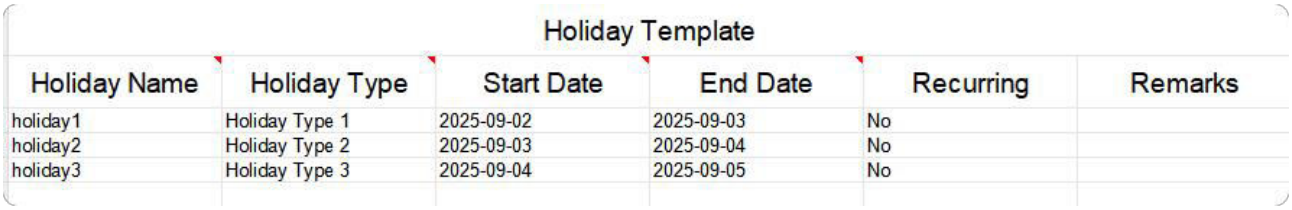
■ Import:

Step 1: Enter Elevator → Elevator Control Rule → Holidays.Select and click the "**Download Import Template**" button,download the template "Holiday Template.xls" locally.



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

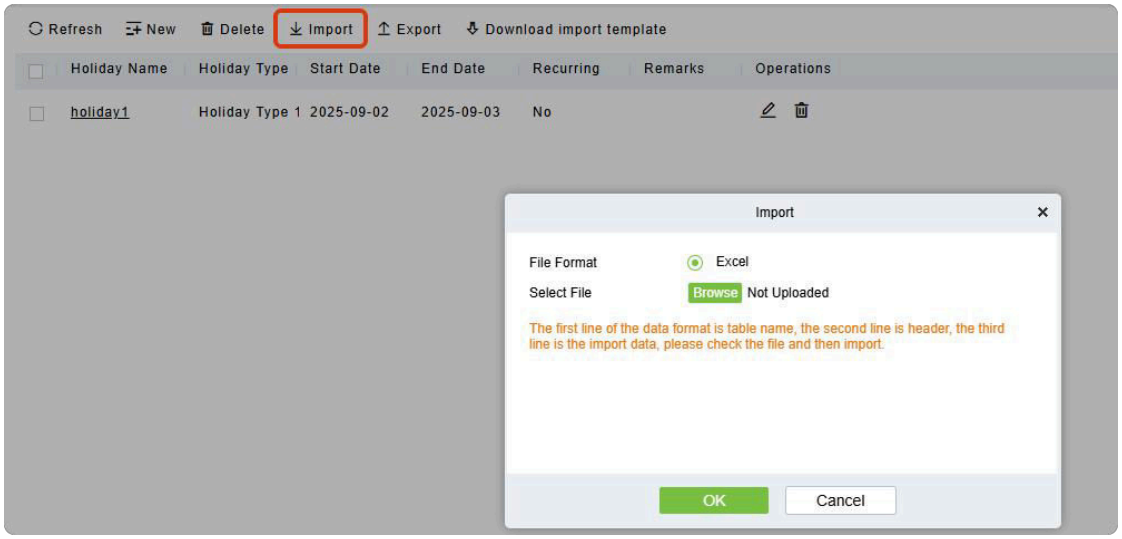
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.



Holiday Template

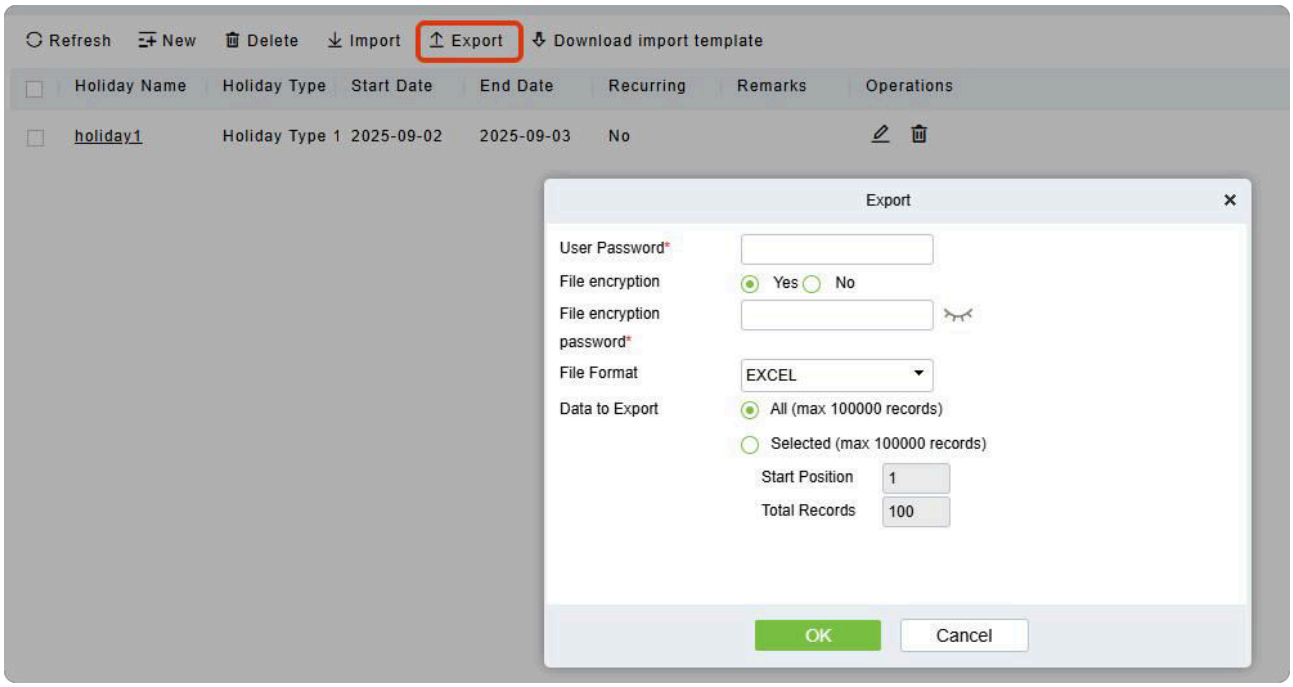
Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
holiday2	Holiday Type 2	2025-09-03	2025-09-04	No	
holiday3	Holiday Type 3	2025-09-04	2025-09-05	No	

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.



■ Export:

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



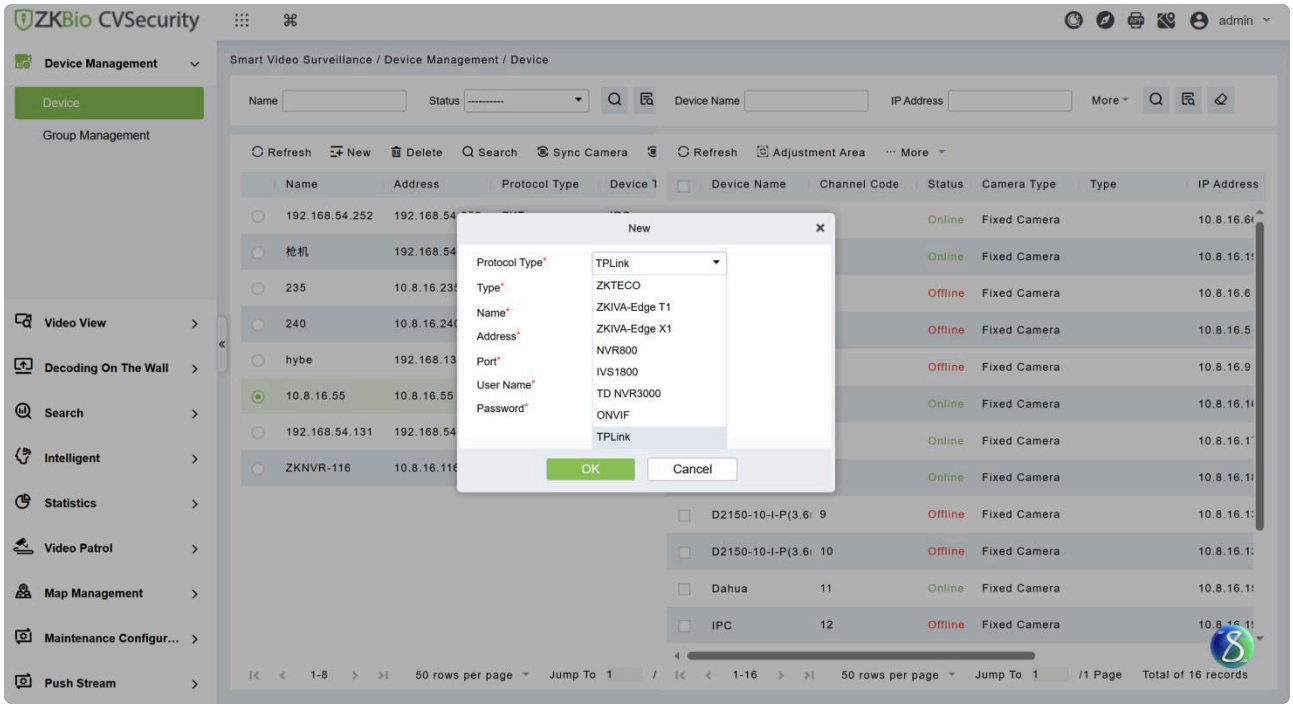
1	Holidays					
2	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
3	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
4						

Smart Video Surveillance

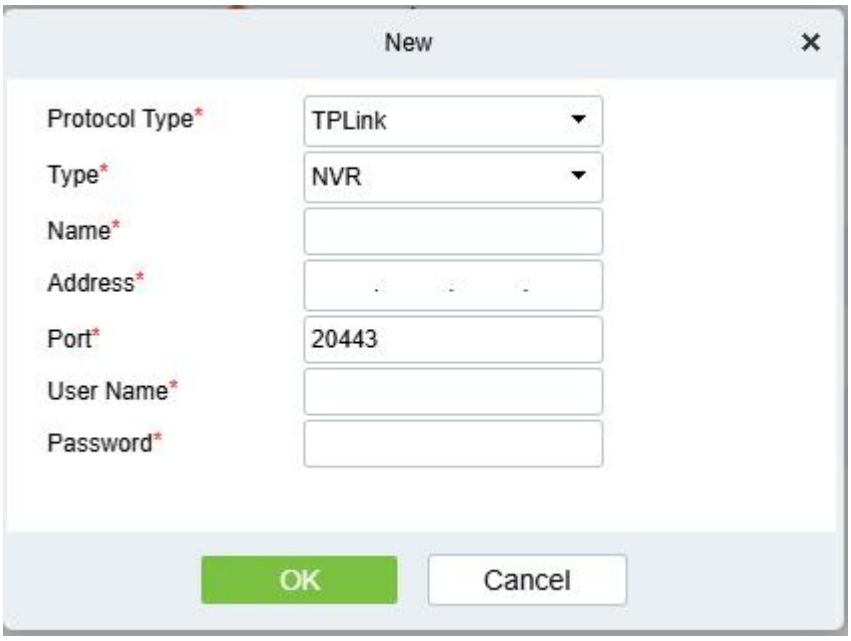
- **Integrated with TP-Link NVR to enable preview, playback, intelligent alert display, and alarm linkage.**

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.



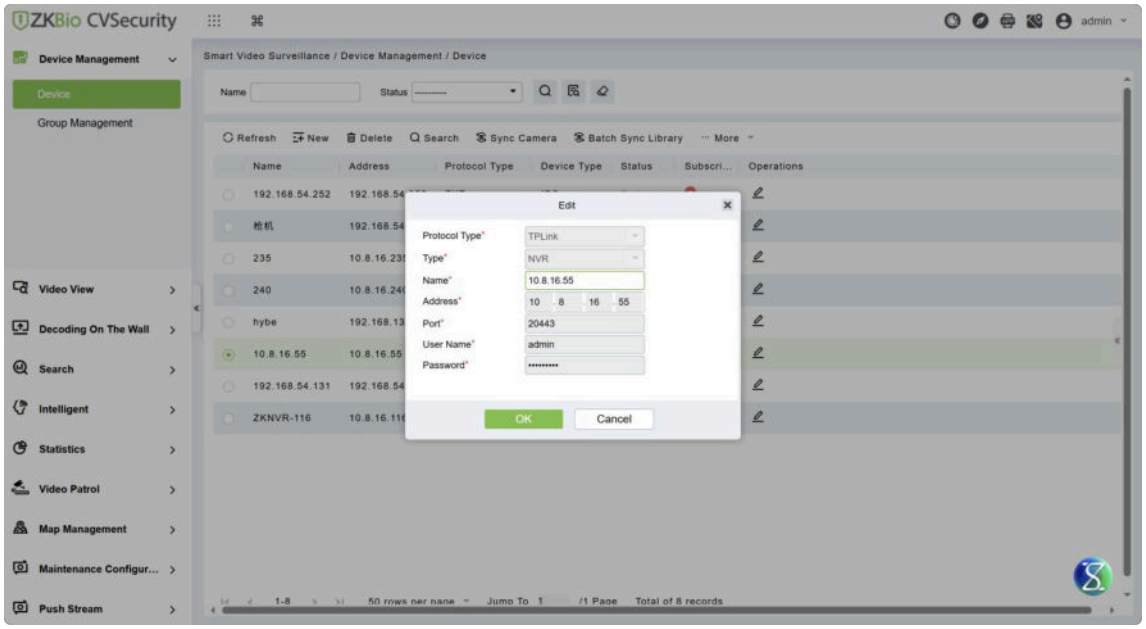
Step2: You can choose NVR devices based on the TP-Link protocol.



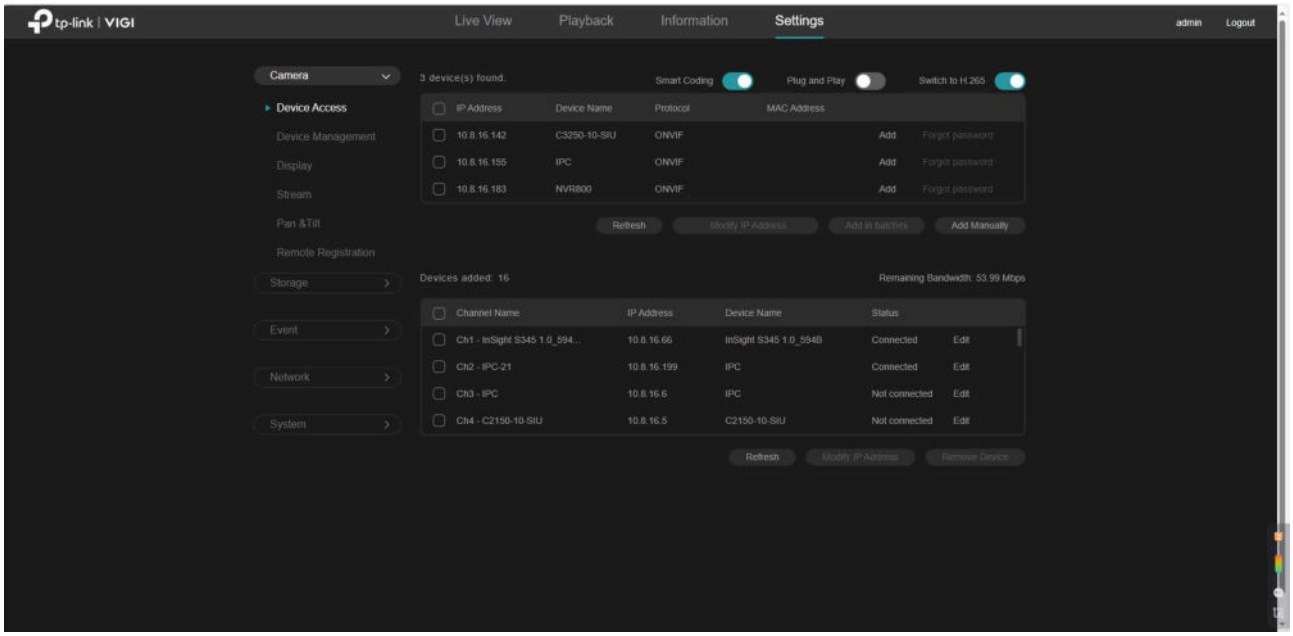
The description of each parameter is shown in Table.

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. Note: For TPLink NVR, the default account is (admin,Admin@135)

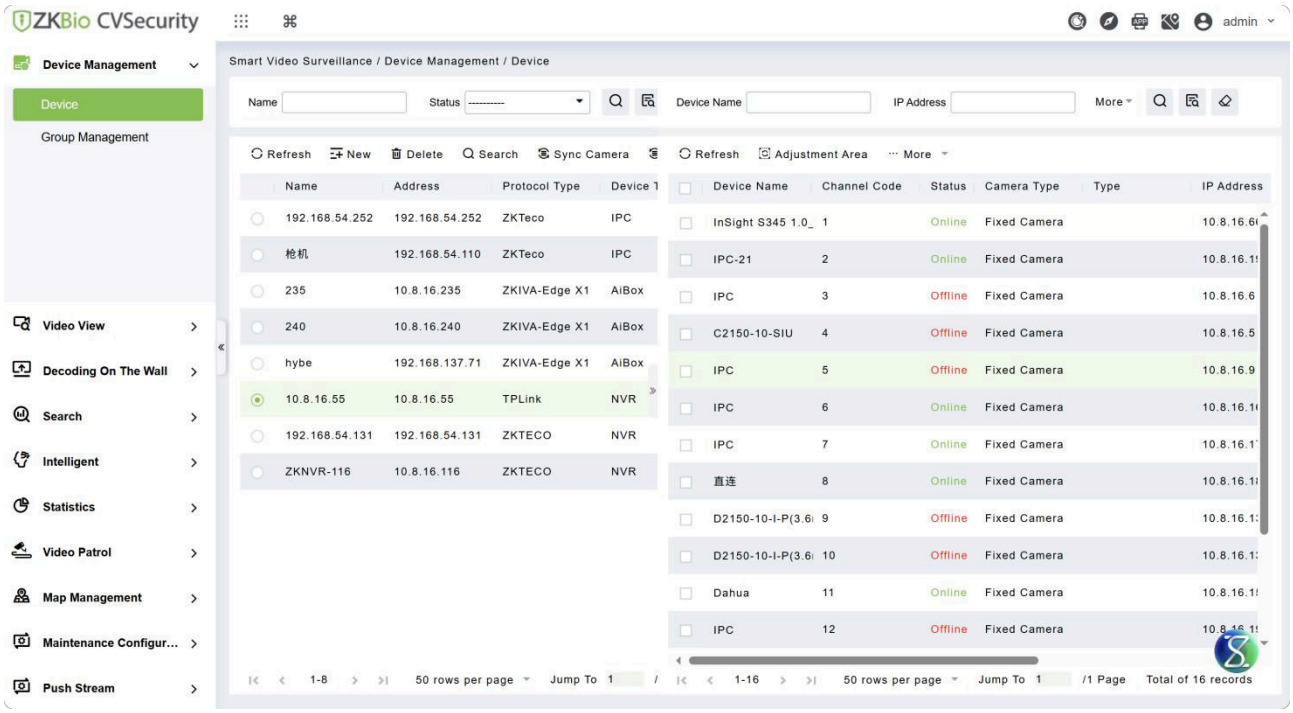
Step 3: Click **OK**.



Step 4: Add IPCs on the NVR client.

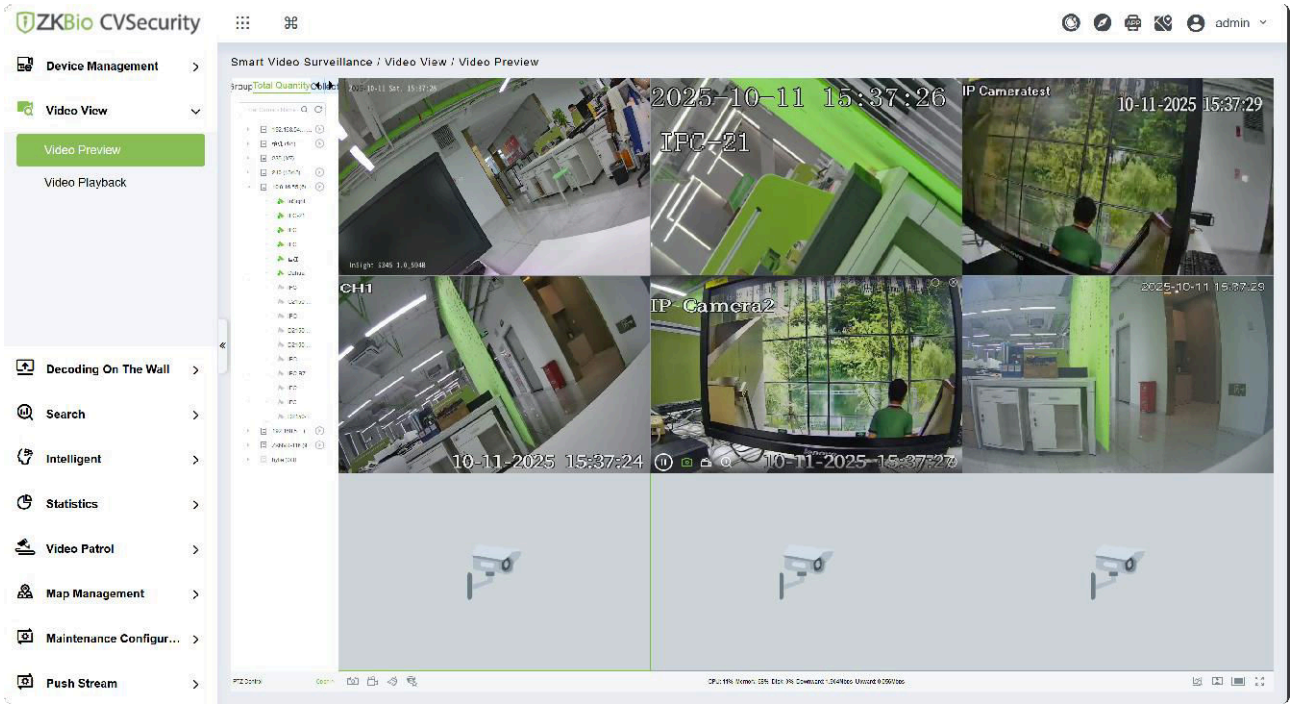


The software interface will automatically synchronize the added camera devices.



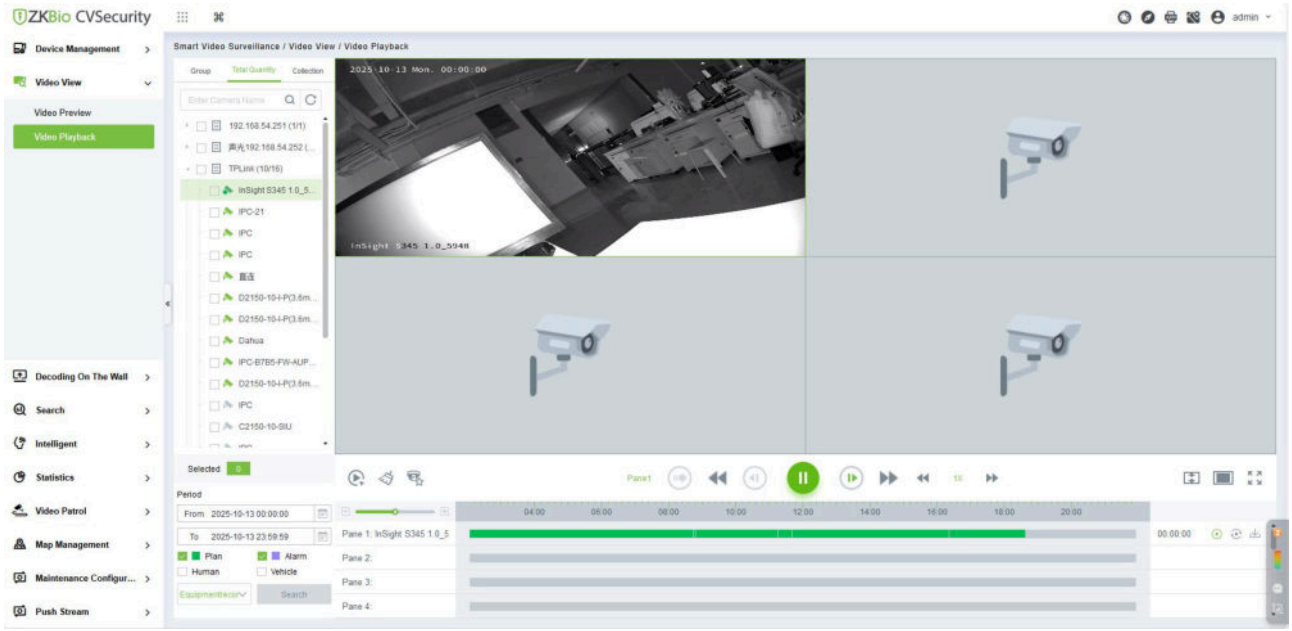
Enter Smart Video Surveillance > Video View > Video Preview.

You can view the video preview here.



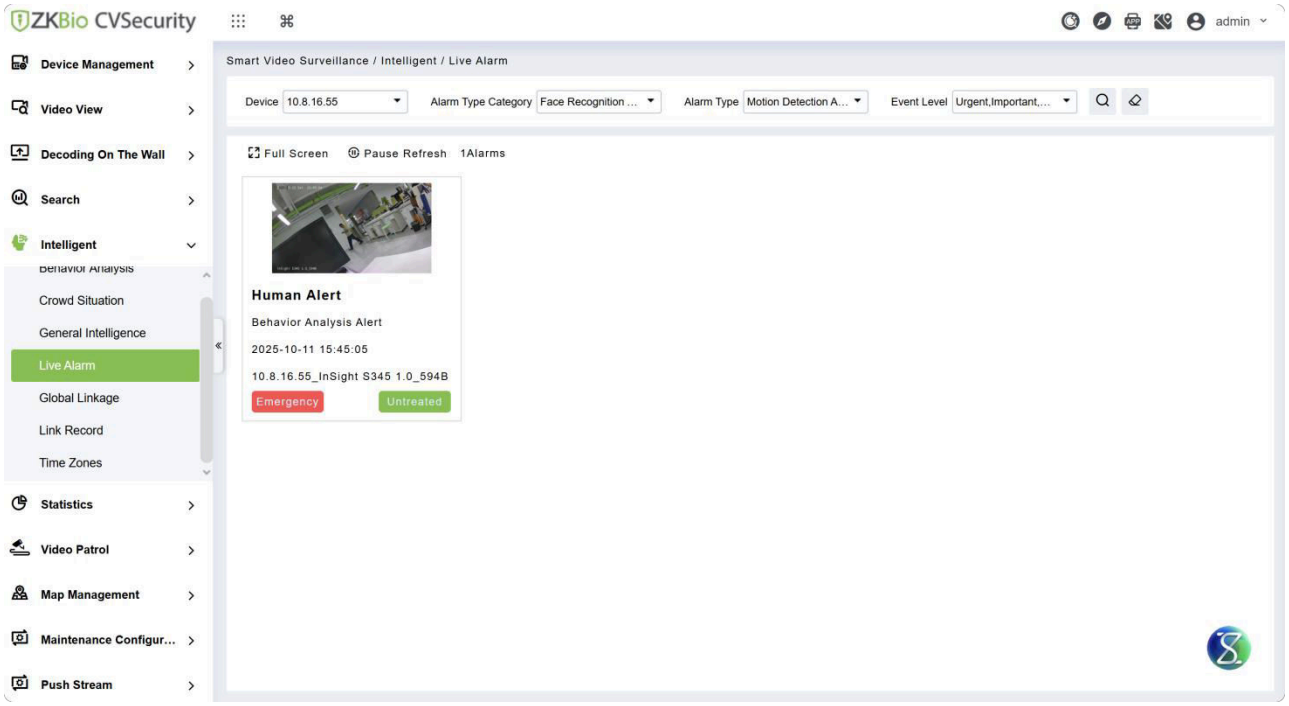
Enter Smart Video Surveillance > Video View > Video Playback.

You can view the video replay here.

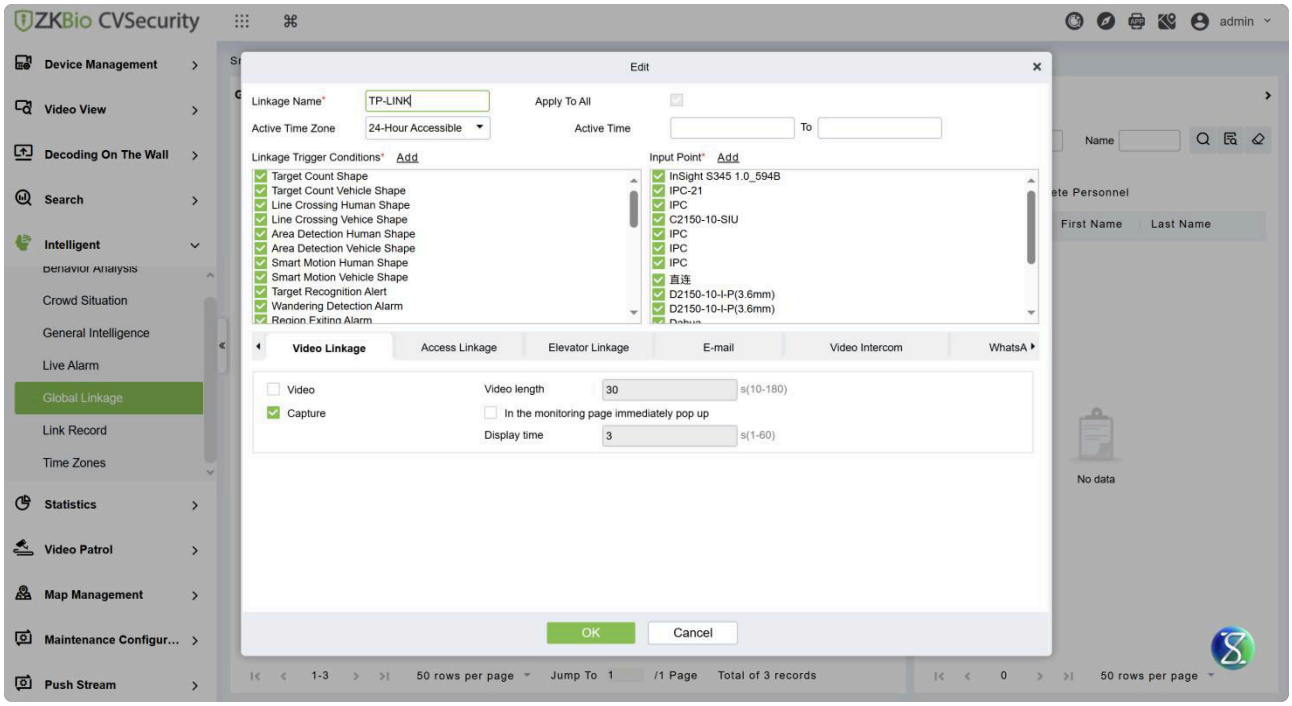


Enter Smart Video Surveillance > Intelligent > Live Alarm.

You can view real-time video alarm monitoring here.

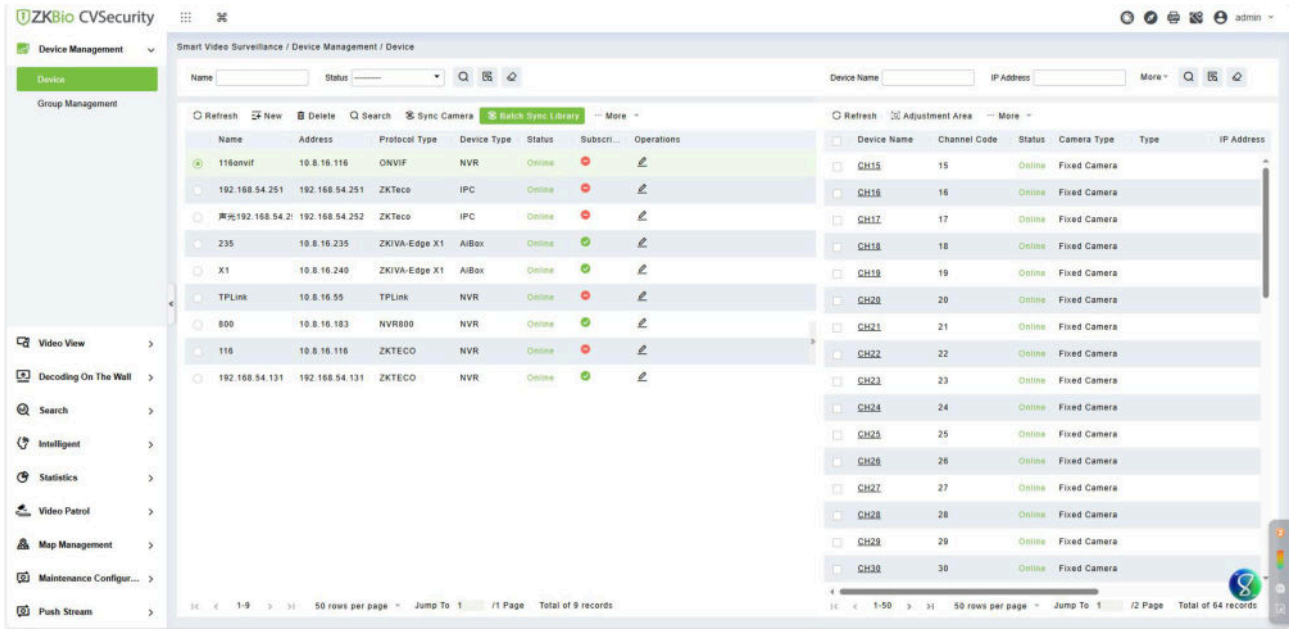


Enter Smart Video Surveillance > Intelligent > Global Linkage, click New to set the video linkage.

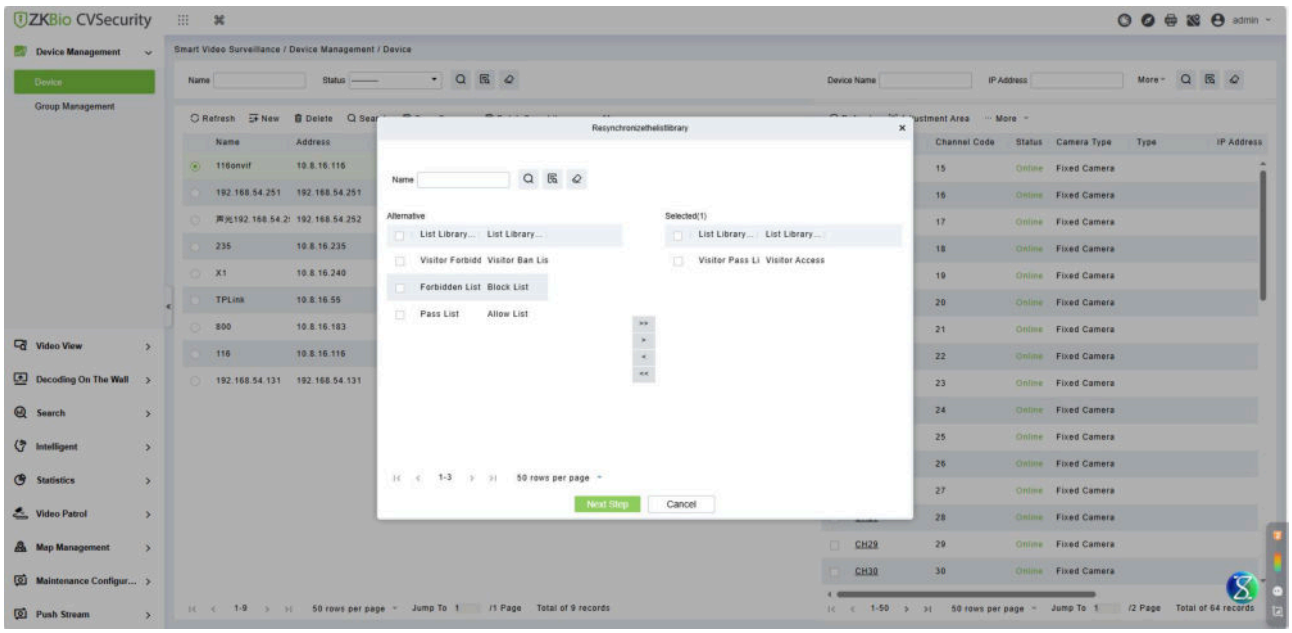


- **Supports batch synchronization of list databases to multiple devices.**

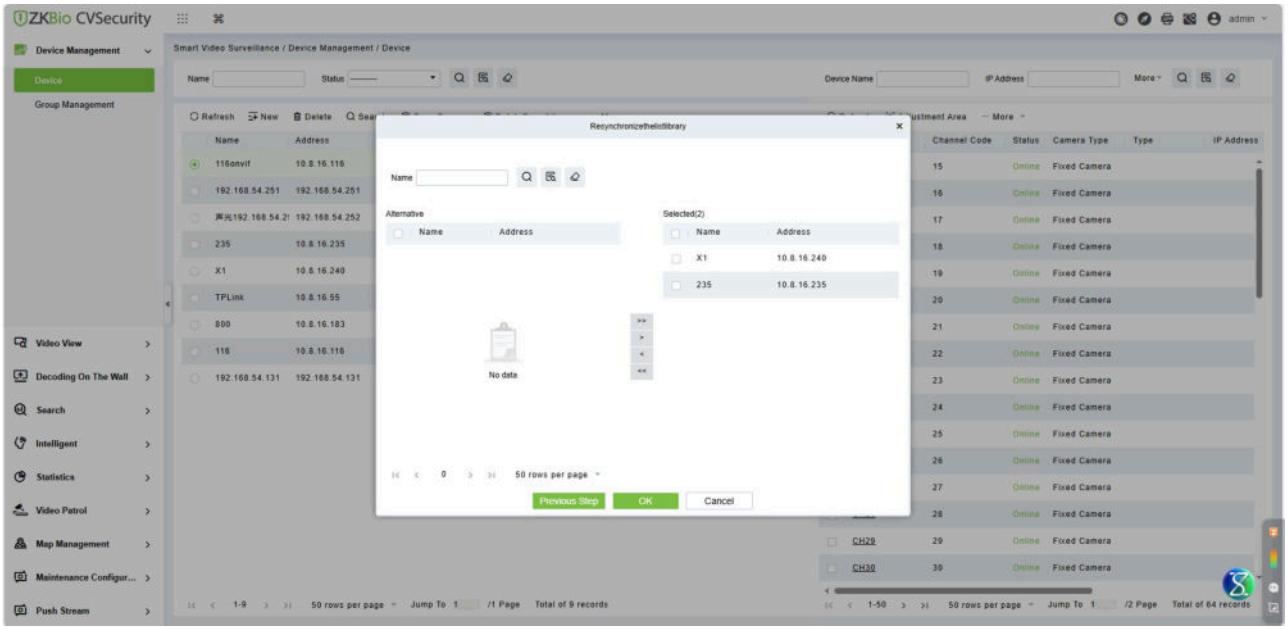
Step1: Enter Smart Video Surveillance → Device Management → Device, and click "Batch Sync Library".



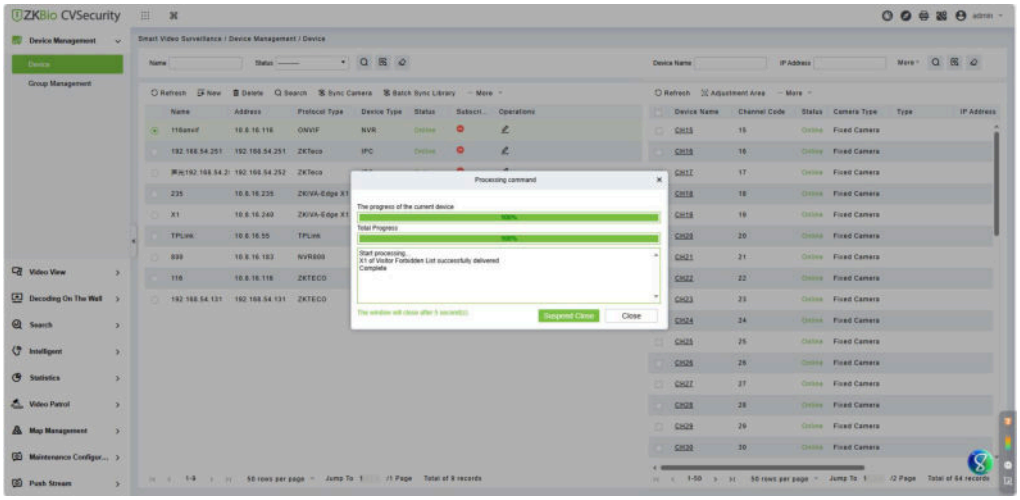
Step2: Select the list you want to synchronize and move it to the right,and click "Next Step".



Step3: Select the devices for which you want to synchronize the list (multiple can be checked at once), move them to the right, and click "OK" to complete the list library synchronization.

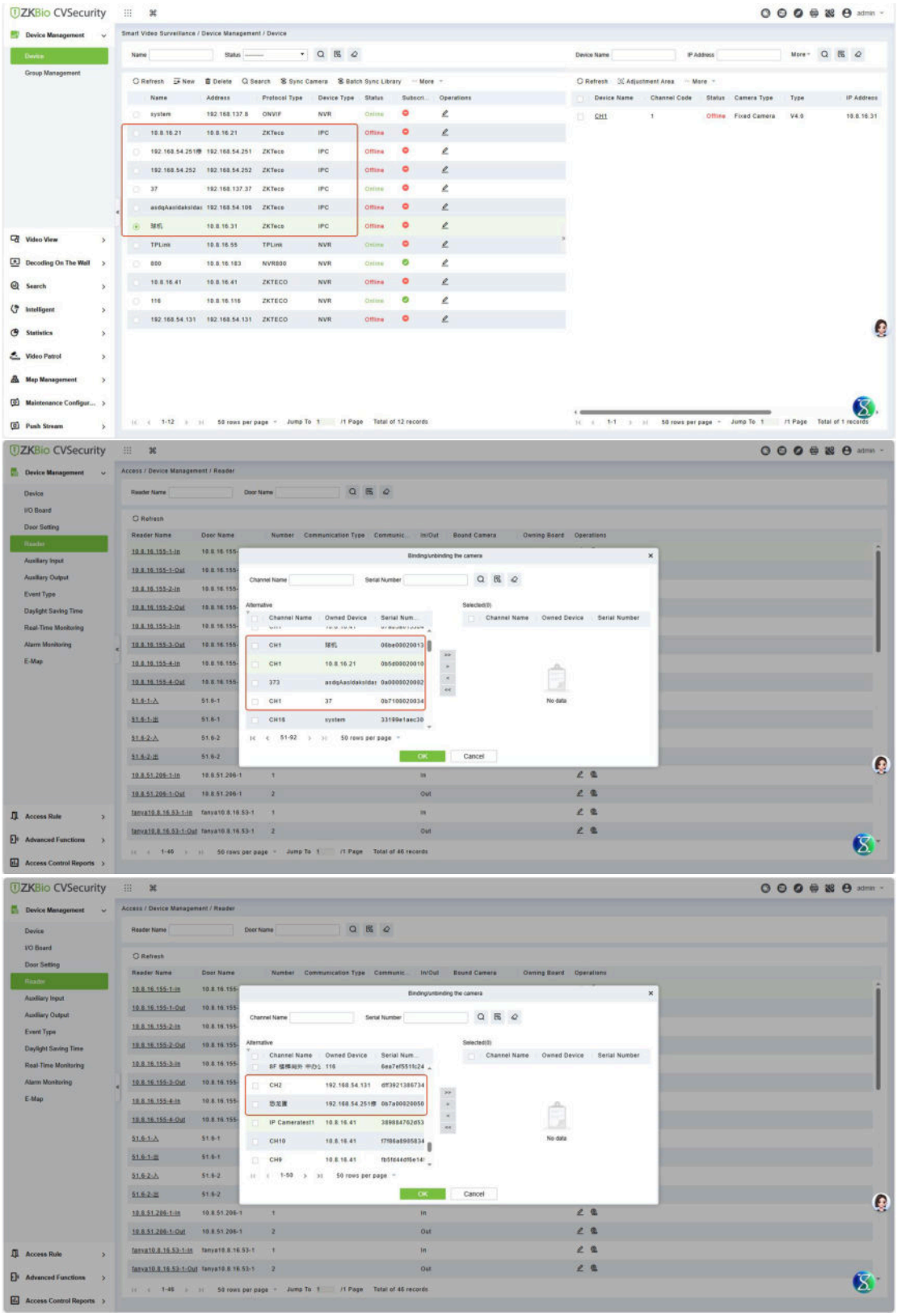


Data will start to be imported automatically until the operation completion prompt is given.



- **Support linkage with IPC (access control or video linkage with IPC).**

Can directly bind IPC devices (not limited to IPC devices in NVR devices)

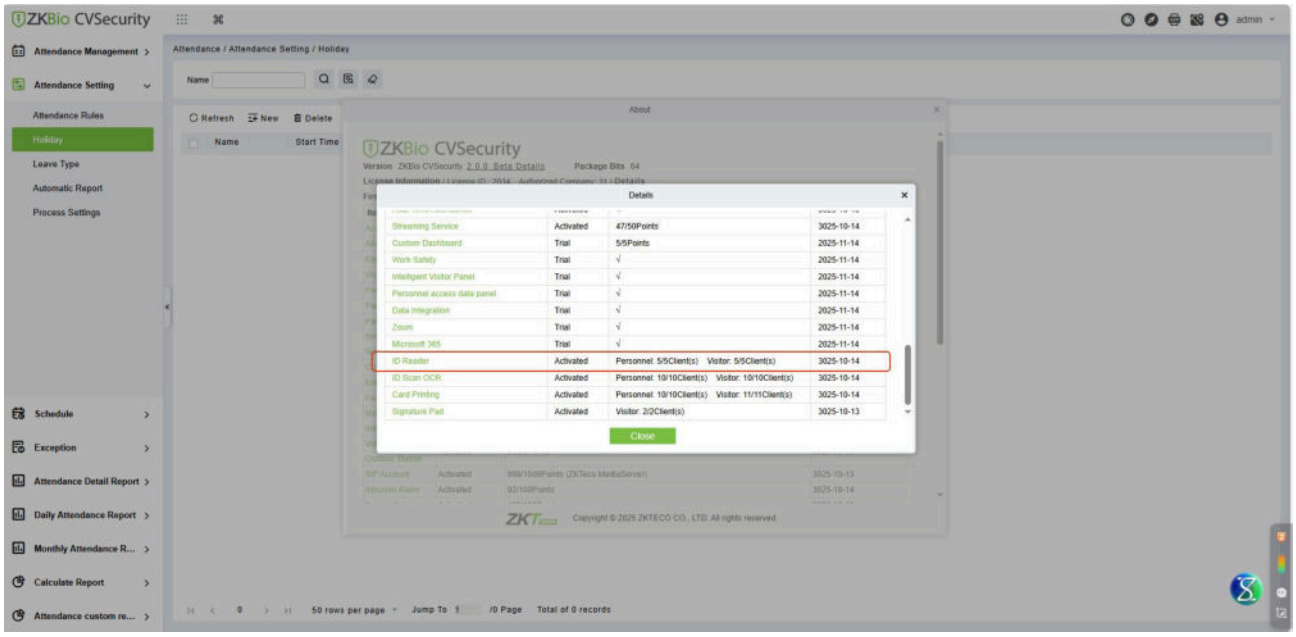


Note: Due to the inconsistent SDK interface standards among different brands of cameras, some devices do not support snapshot interfaces, making it impossible to implement linked snapshot functionality. For the specific models of devices that are supported, you may contact the technical support team to obtain the device compatibility list for verification.

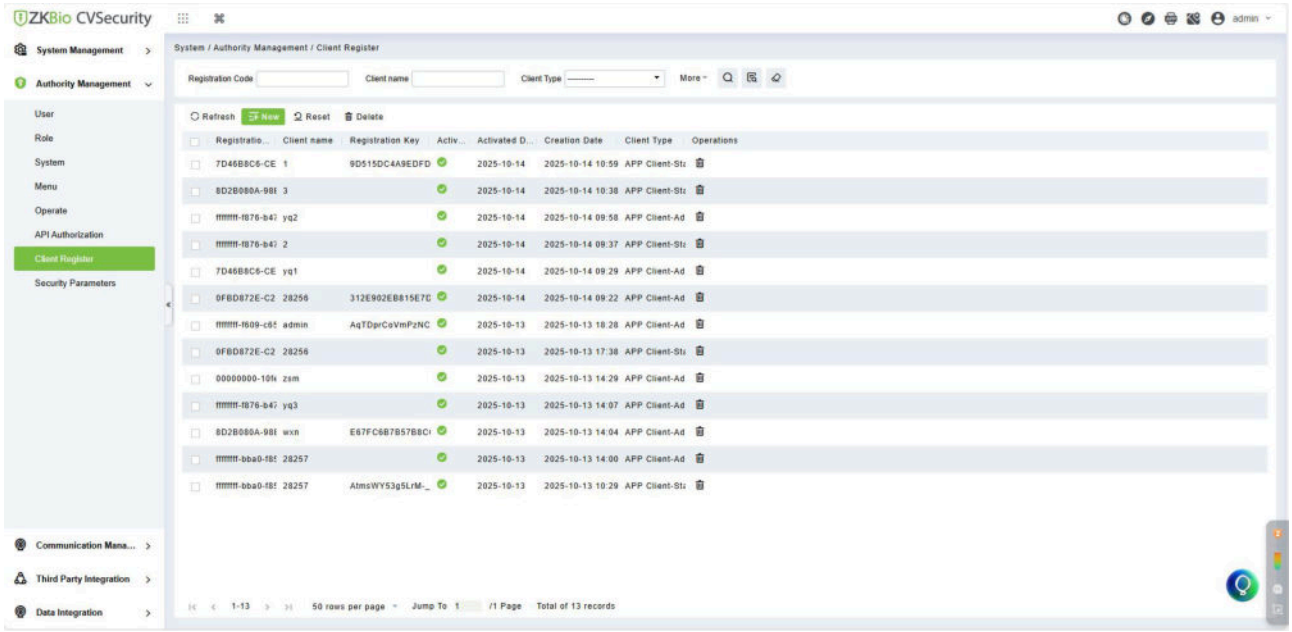
System

- **Supports reading Malaysian ID cards via the RS100 passport scanner.**

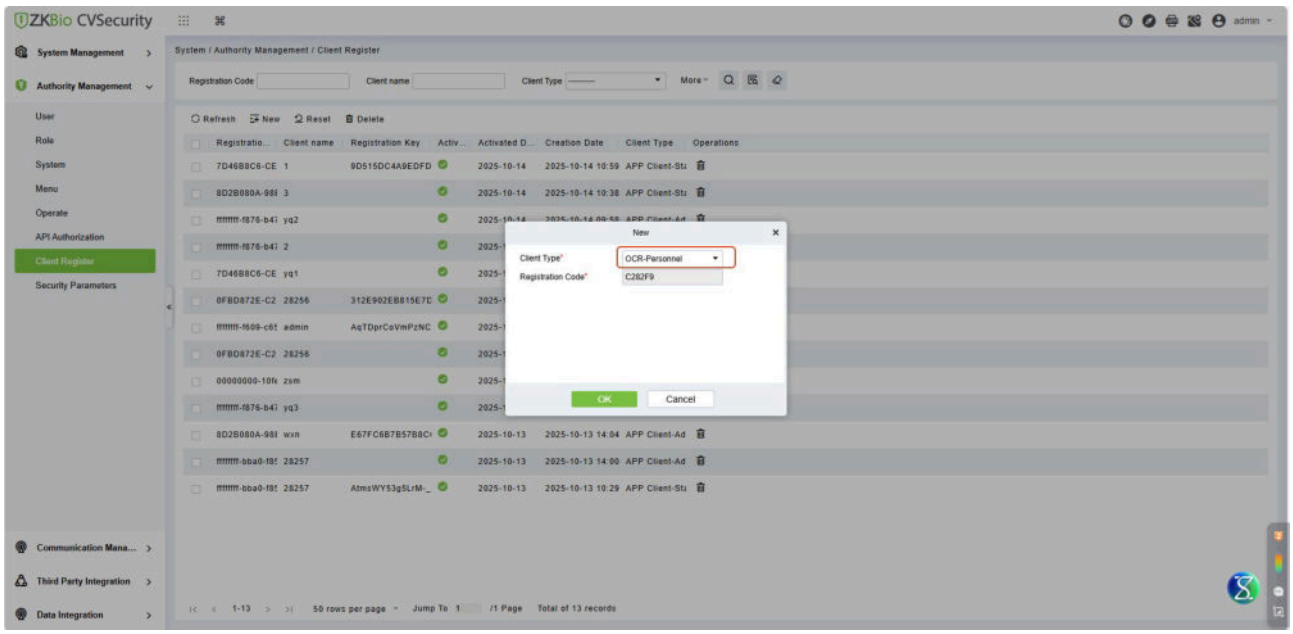
First, it is necessary to confirm that the ID card reader license has been activated.



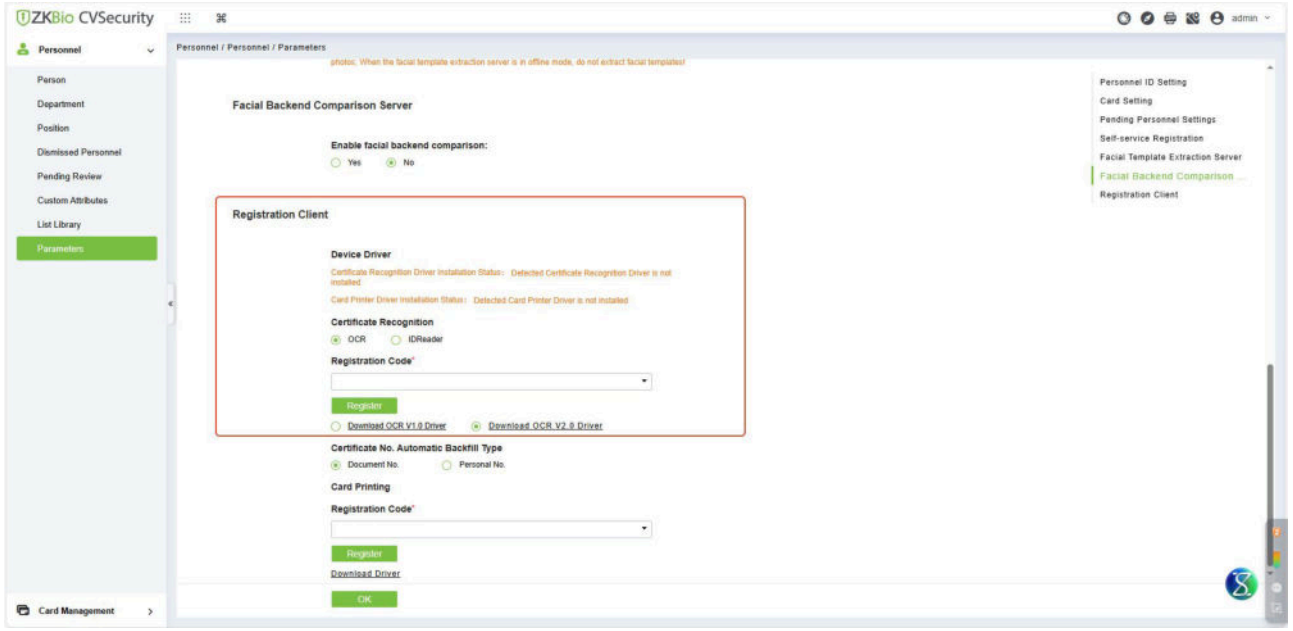
Step1: Enter System → Authority Management → Client Register, and click "New".

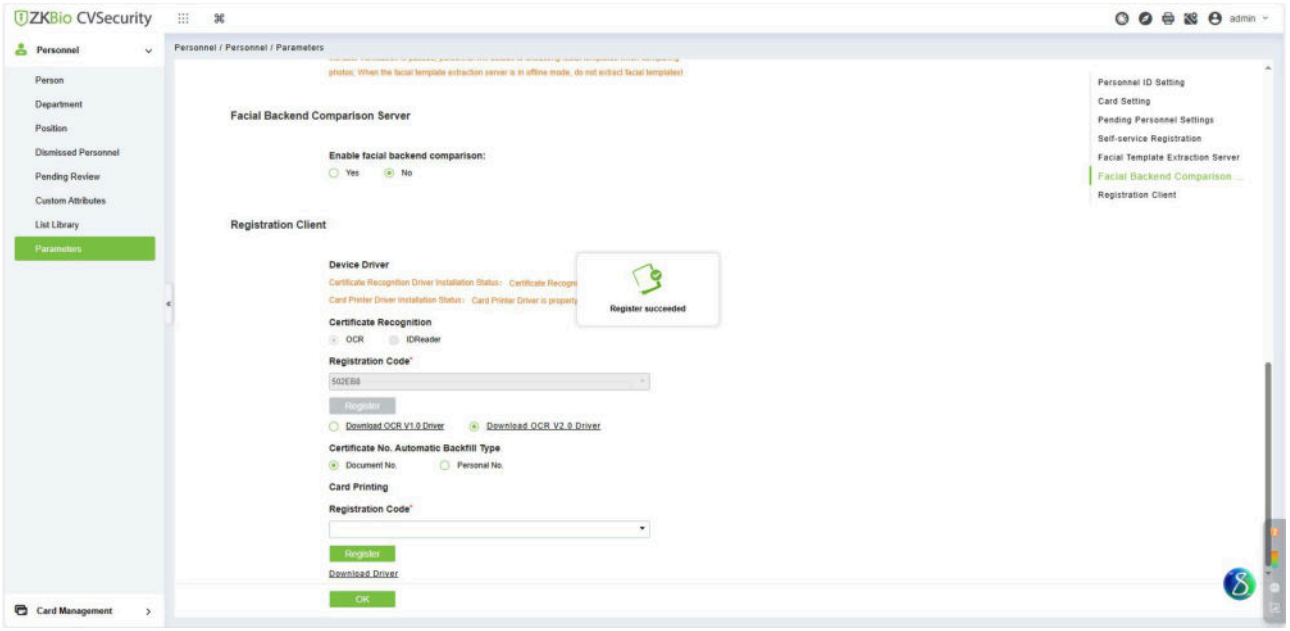


Step2: Select "**OCR- Personnel**" as the client type, and the registration code will be generated automatically.

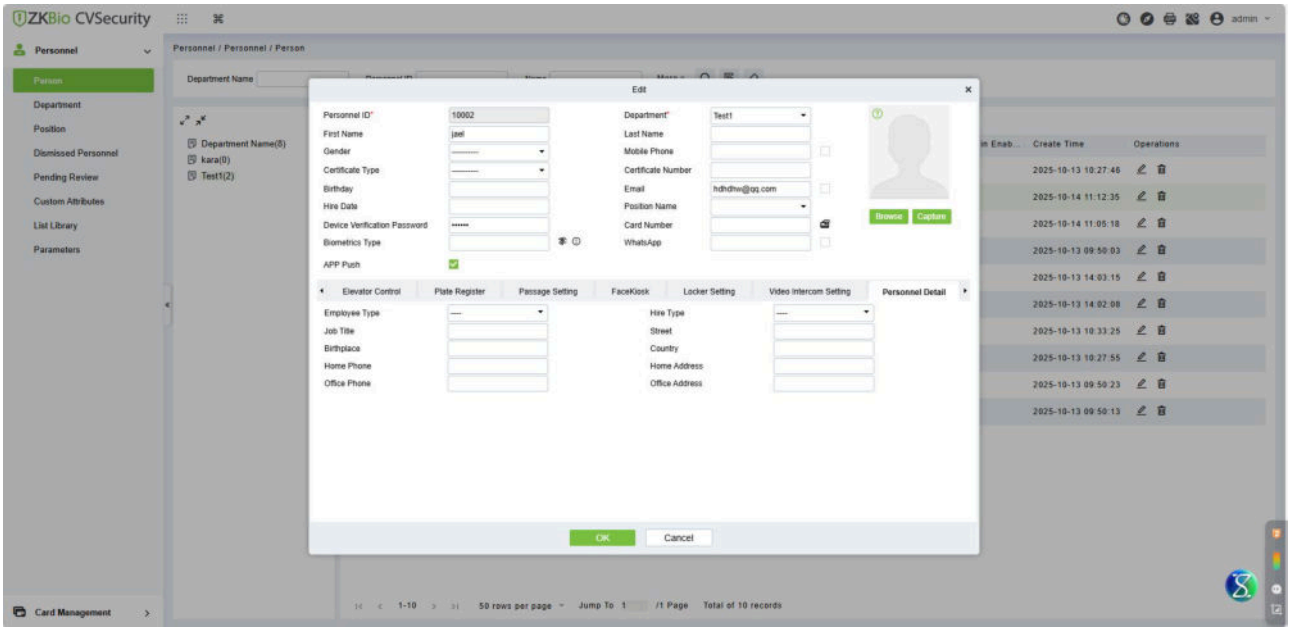


Step3: Enter Personnel → Personnel → Parameters, and activate in the Registration Client bar (driver download is required). For Certificate Recognition, select **OCR**. For the registration code, choose the new item added in the system management in the previous step. Click "**Register**" to complete the activation.





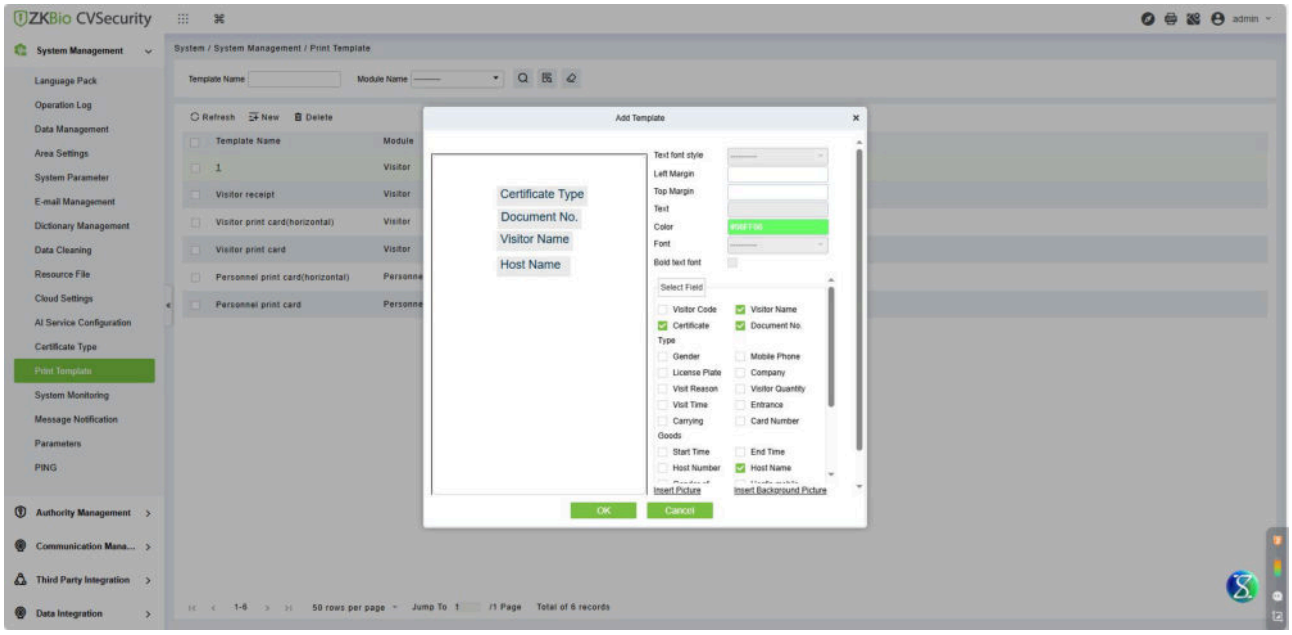
Step4: Scanning with the RS100 passport scanner can automatically extract and fill in the person's headshot, name, date of birth, certificate number and home address.



- **Card Printing Template Optimized.**

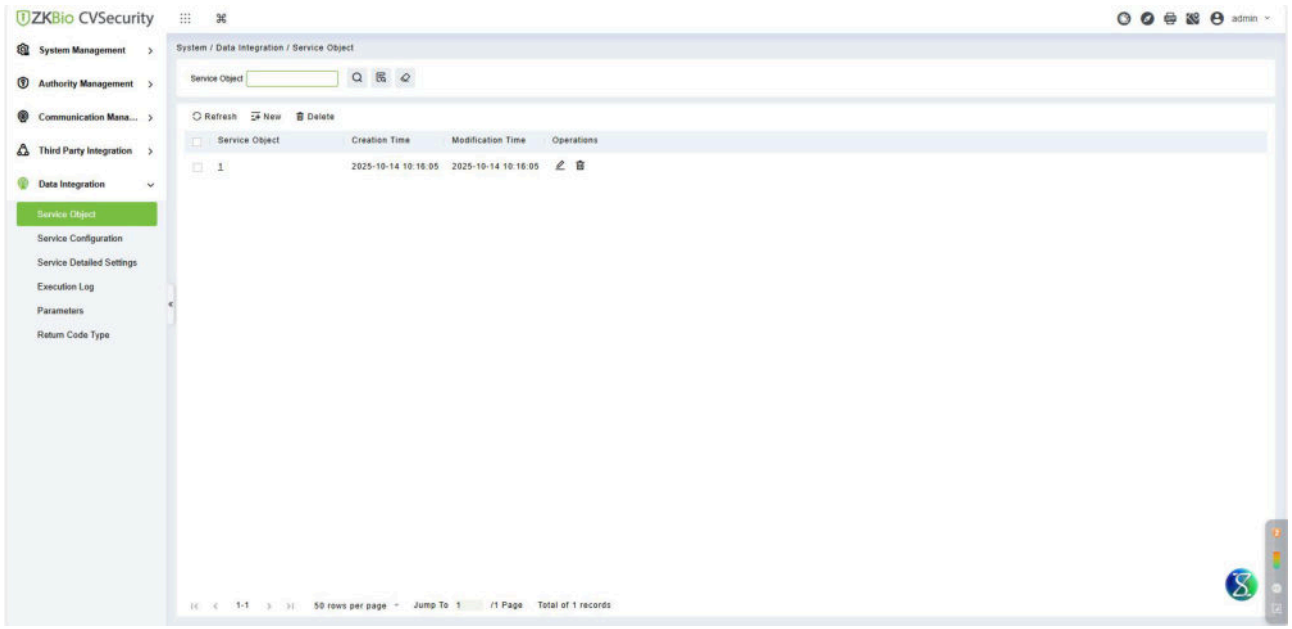
Step: Enter System→ System Management → Print Template , and the interface for adding a new template is shown in the figure below:

1. Support customizing image size and position.
2. Support customizing user photo size.
3. Support customizing font style, position, size, color and whether to bold.



- **Added a data integration module: Supports integrating third-party platforms to synchronize data from external sources into the system or export system data to third-party platforms.**

Enter System→ 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.

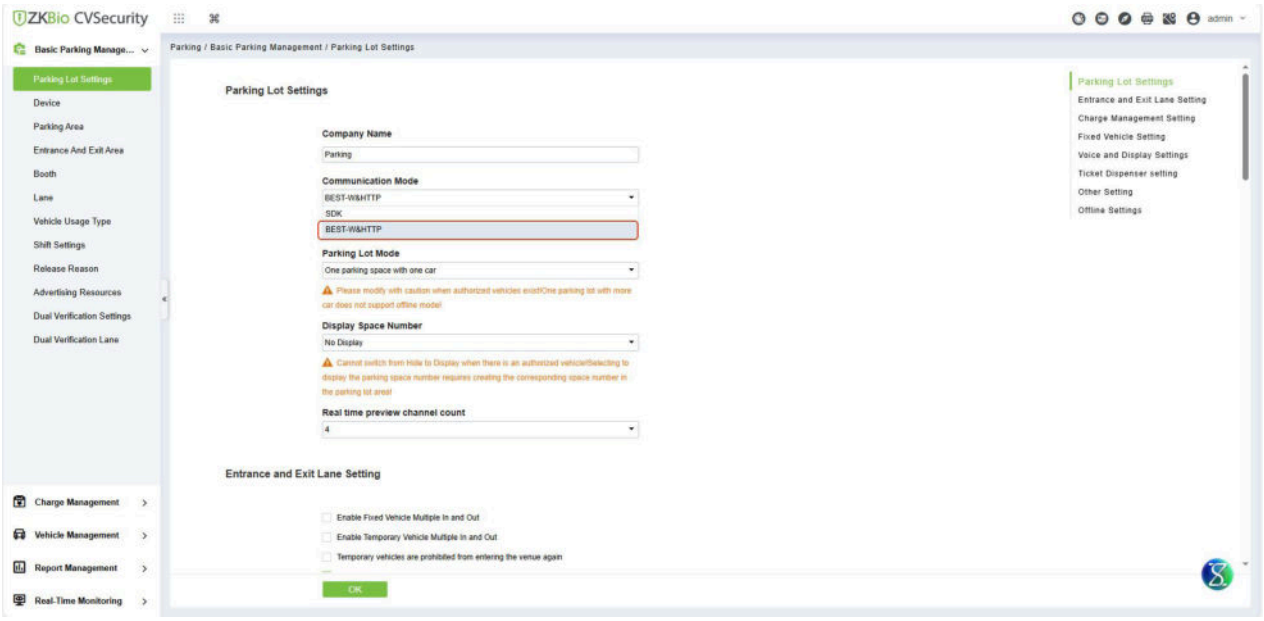


Note: For detailed configuration steps, please refer to the ZKBio CVSecurity 6.7.0 UM_EN.

Parking

- **Function Optimized-BEST and HTTP protocol devices now fully compatible for simultaneous operation.**

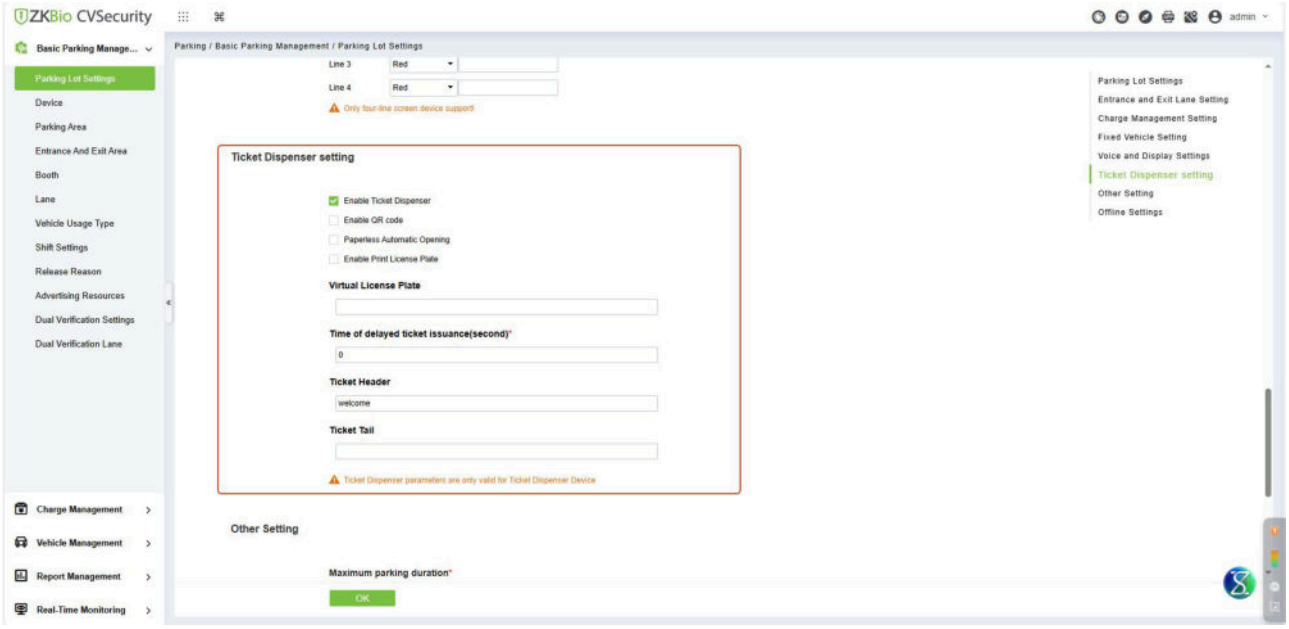
When this mode is selected, LPR devices using the BEST-W protocol or HTTP protocol can be used simultaneously.



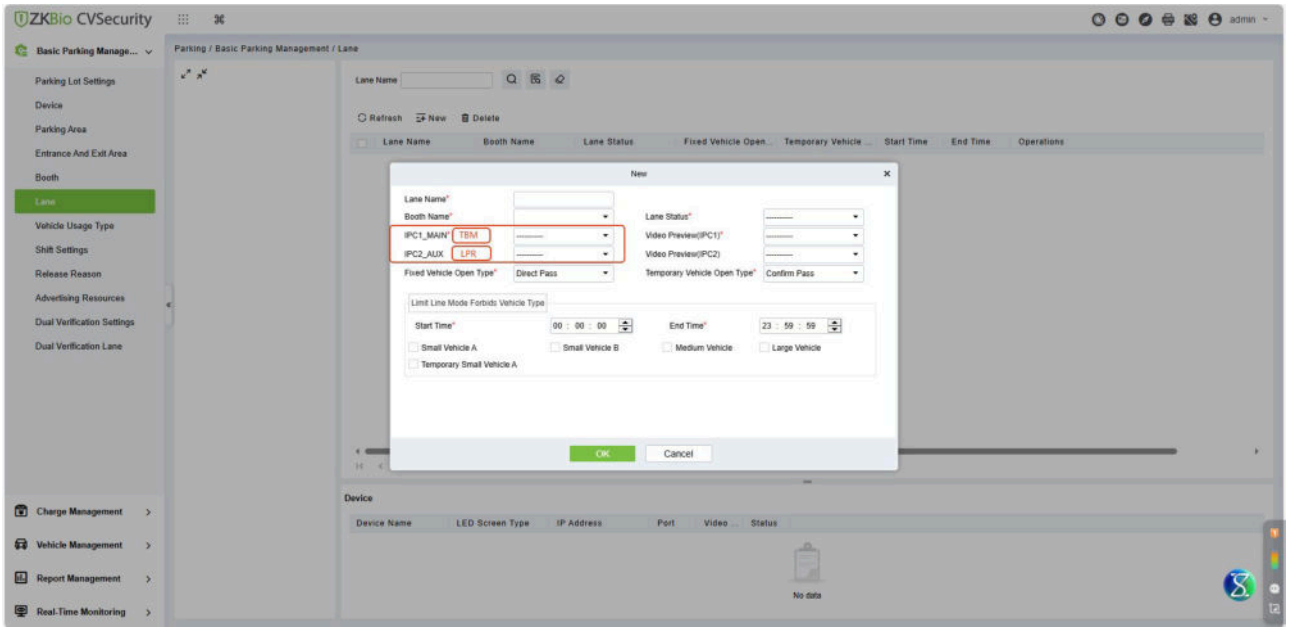
- **Ticket machines now record license plates (captured by LPRC300) for lost ticket recovery and payment.**

In the case of lost receipts, payment can be made by checking the license plate number. Auxiliary license plates are not used for any other business processing.

The TBM equipment supports binding LPR devices to print license plates on receipts:



The association between TBM and LPR:



■ 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

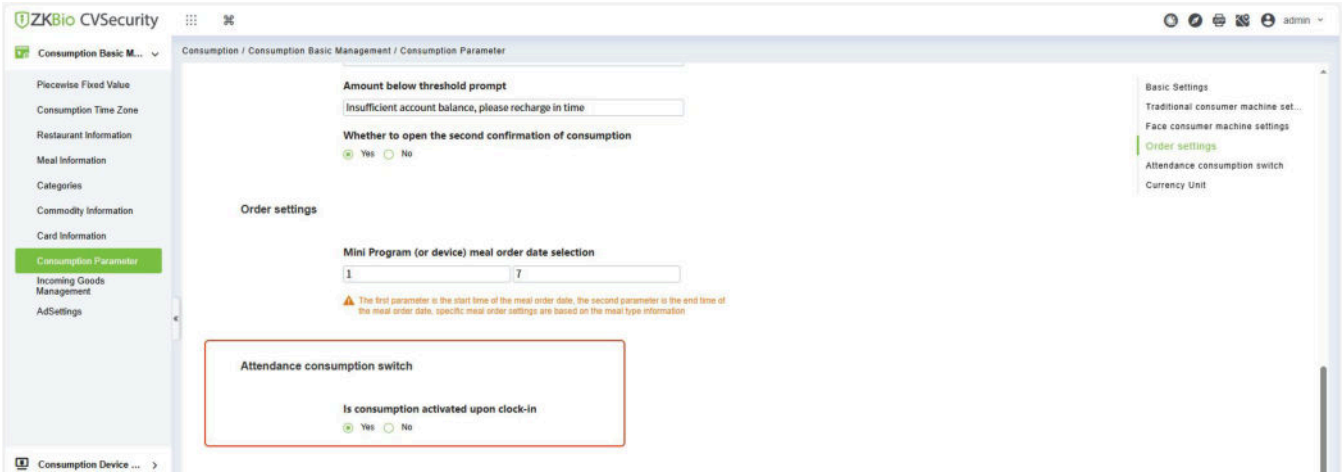
Temporary vehicle: Exit → LPR recognition → Ticket scanning (Auxiliary license plate recognition includes license plate recognition and photo recognition)

Fixed vehicle: Exit → LPR recognition → Swipe card (Auxiliary license plate recognition includes license plate recognition and photo recognition)

Consumption

- **Personnel must complete attendance check-in on the same day before they can make consumption.**

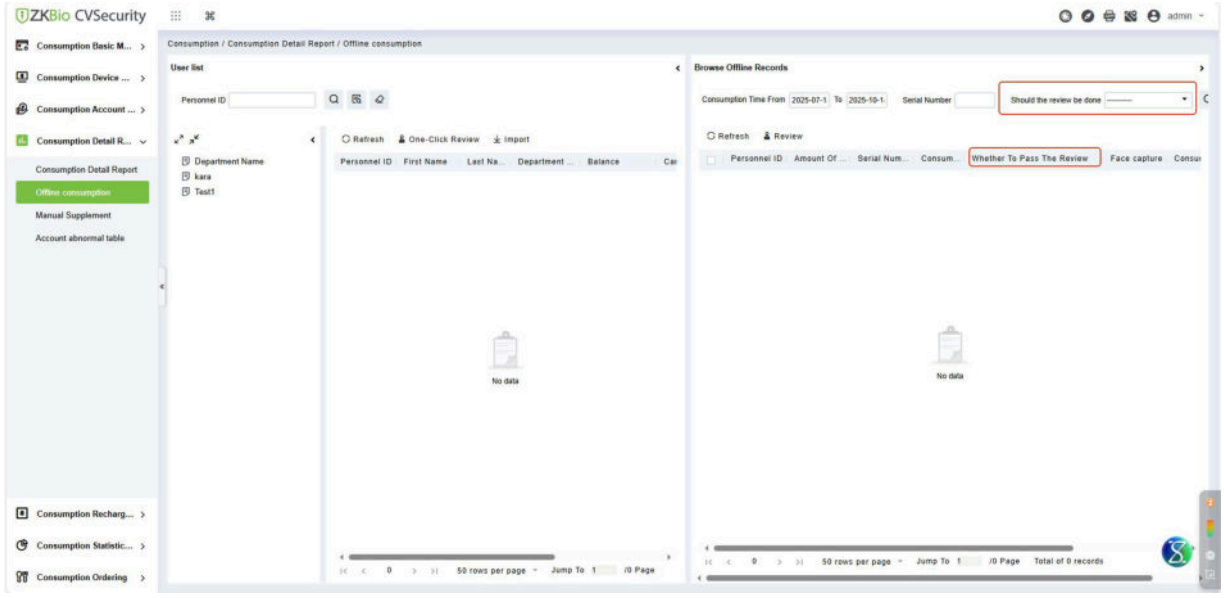
Step: Enter Consumption → Consumption Basic Management → Consumption Parameter, and check "**Yes**" in the "**Is consumption activated upon clock-in**" section of the **Attendance consumption switch** bar.



Result verification:
If the person fails to sign in on the same day, when verifying on the consumption machine, a prompt will appear saying "You haven't clocked in, so you can't make a purchase."

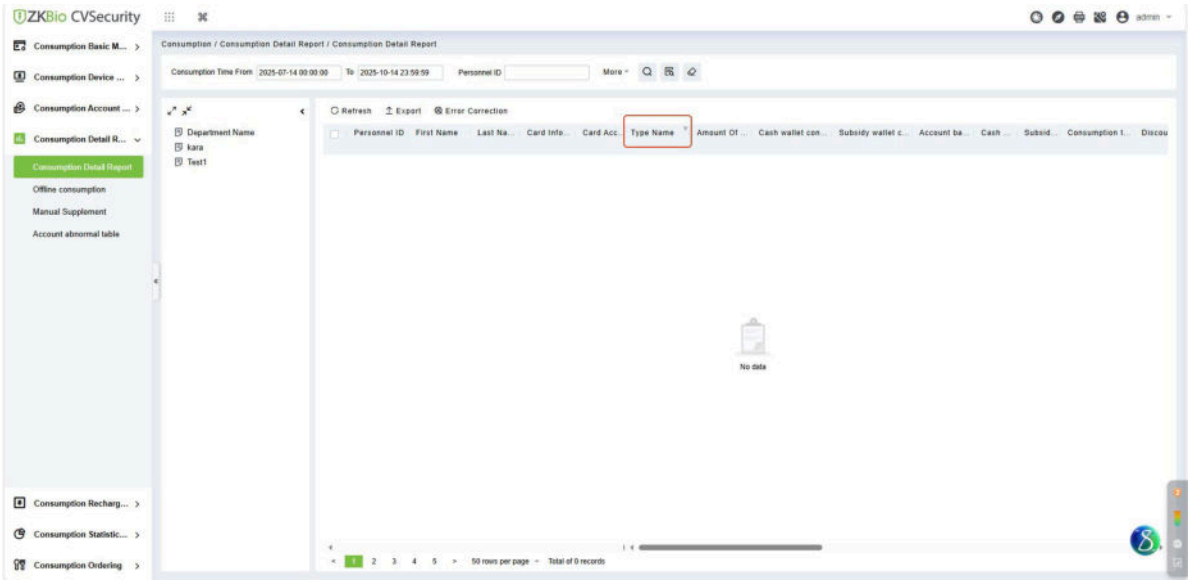
- **Added a filter for "Approval Status" in the offline consumption details table.**

Step: Enter Consumption → Consumption Detail Report → Offline consumption. In the search bar, you can filter the consumption records by whether the review are pass or not.



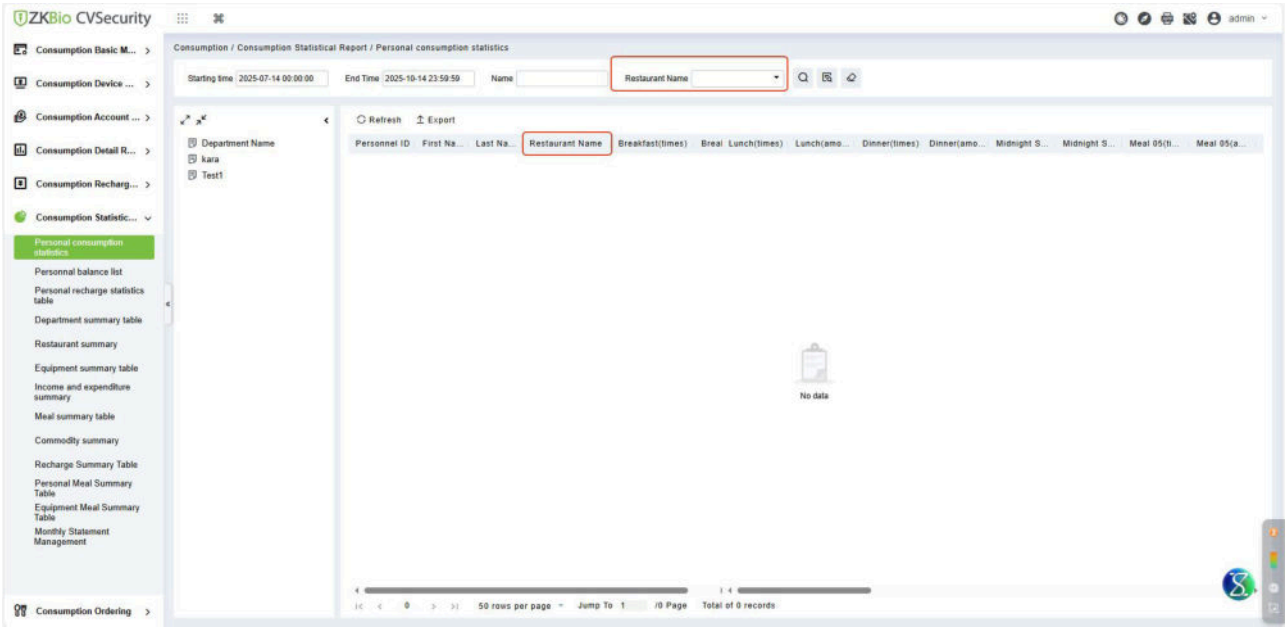
- **Added an "Type Name" field to the consumption details table.**

Step: Enter Consumption → Consumption Detail Report → Consumption Detail Report. The display fields of the report include "Type Name".



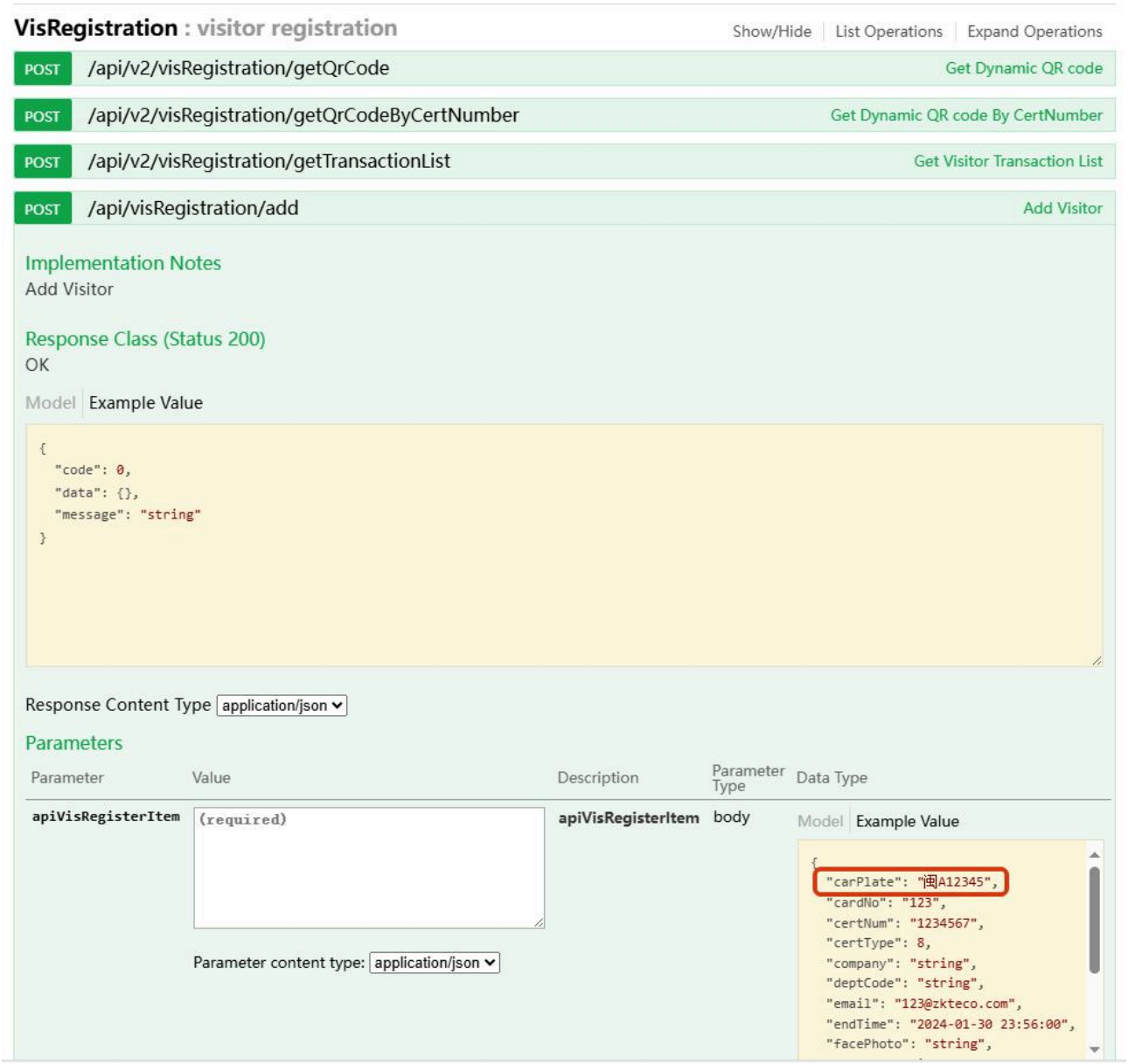
- **Added a "Restaurant" field and filter option to the personal consumption statistics table.**

Step: Enter Consumption → Consumption Statistical Report → Personal consumption statistics. The display fields of the report include "Restaurant Name", which can be filtered through the restaurant name condition in the search bar.

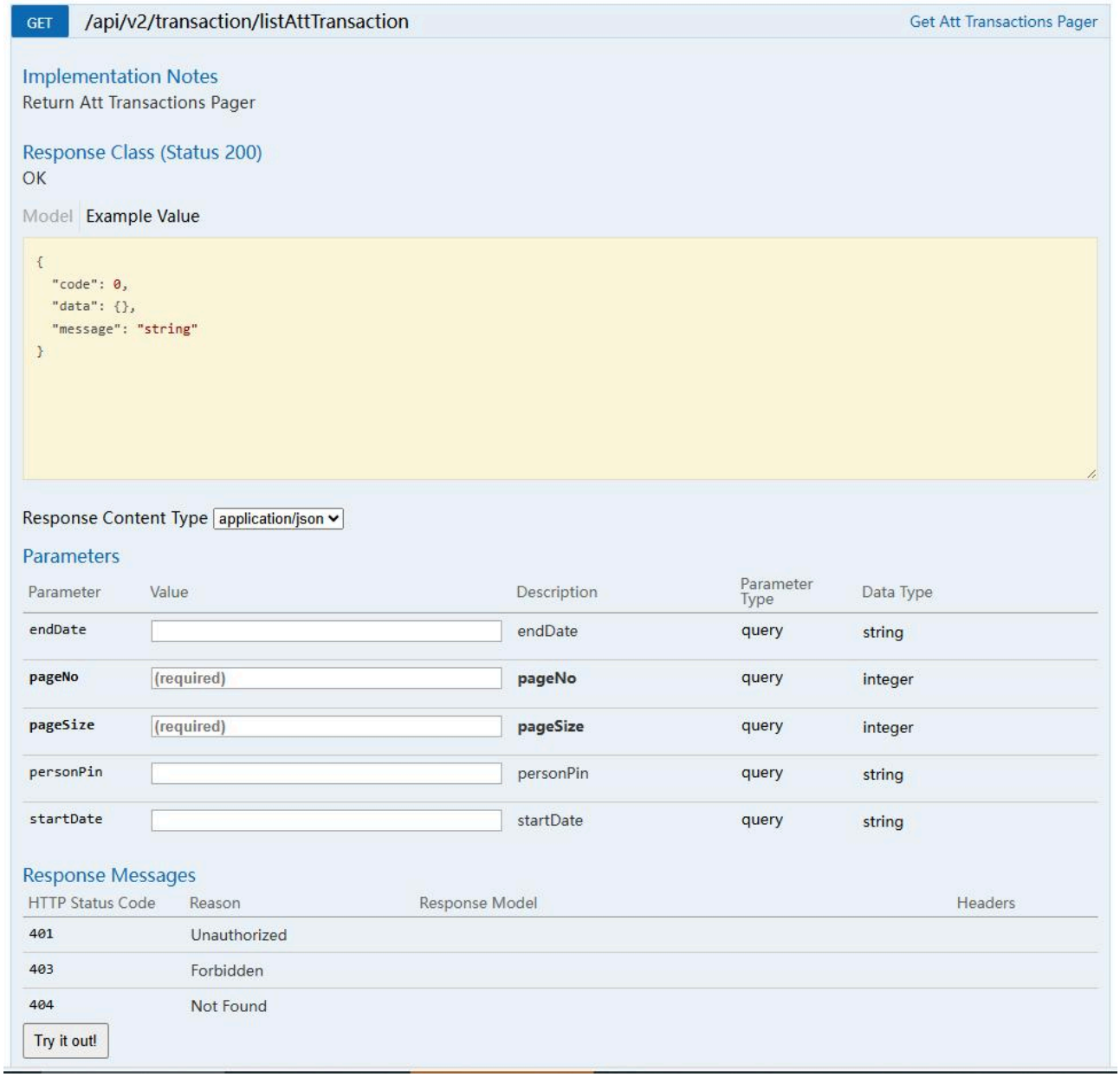


API

- **Added license plate, remarks, and photo fields to visitor reservation API (POST / api/ visReservation / add).**



- **Added attendance checkpoint data (personnel, time, location) to /api/v2/transaction/listAttTransaction.**



GET /api/v2/transaction/listAttTransaction — Get Att Transactions Pager

Implementation Notes

Return Att Transactions Pager

Response Class (Status 200)

OK

Model | Example Value

```
{
  "code": 0,
  "data": {},
  "message": "string"
}
```

Response Content Type application/json

Parameters

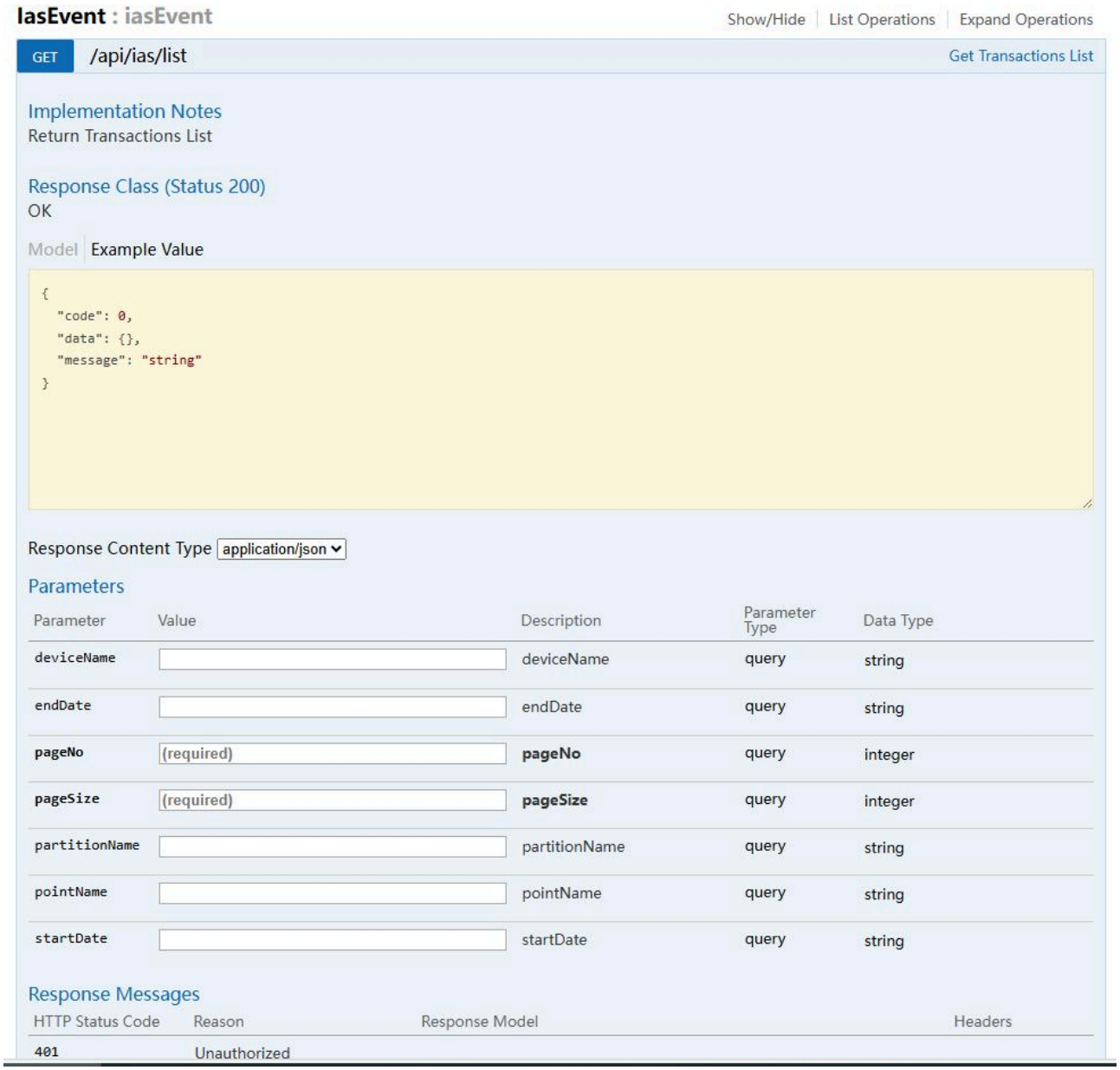
Parameter	Value	Description	Parameter Type	Data Type
endDate		endDate	query	string
pageNo	(required)	pageNo	query	integer
pageSize	(required)	pageSize	query	integer
personPin		personPin	query	string
startDate		startDate	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		
403	Forbidden		
404	Not Found		

Try it out!

- **A new intrusion alarm API interface has been added.**



IasEvent : iasEvent

Show/Hide | List Operations | Expand Operations

GET /api/ias/list — Get Transactions List

Implementation Notes

Return Transactions List

Response Class (Status 200)

OK

Model | Example Value

```
{
  "code": 0,
  "data": {},
  "message": "string"
}
```

Response Content Type application/json

Parameters

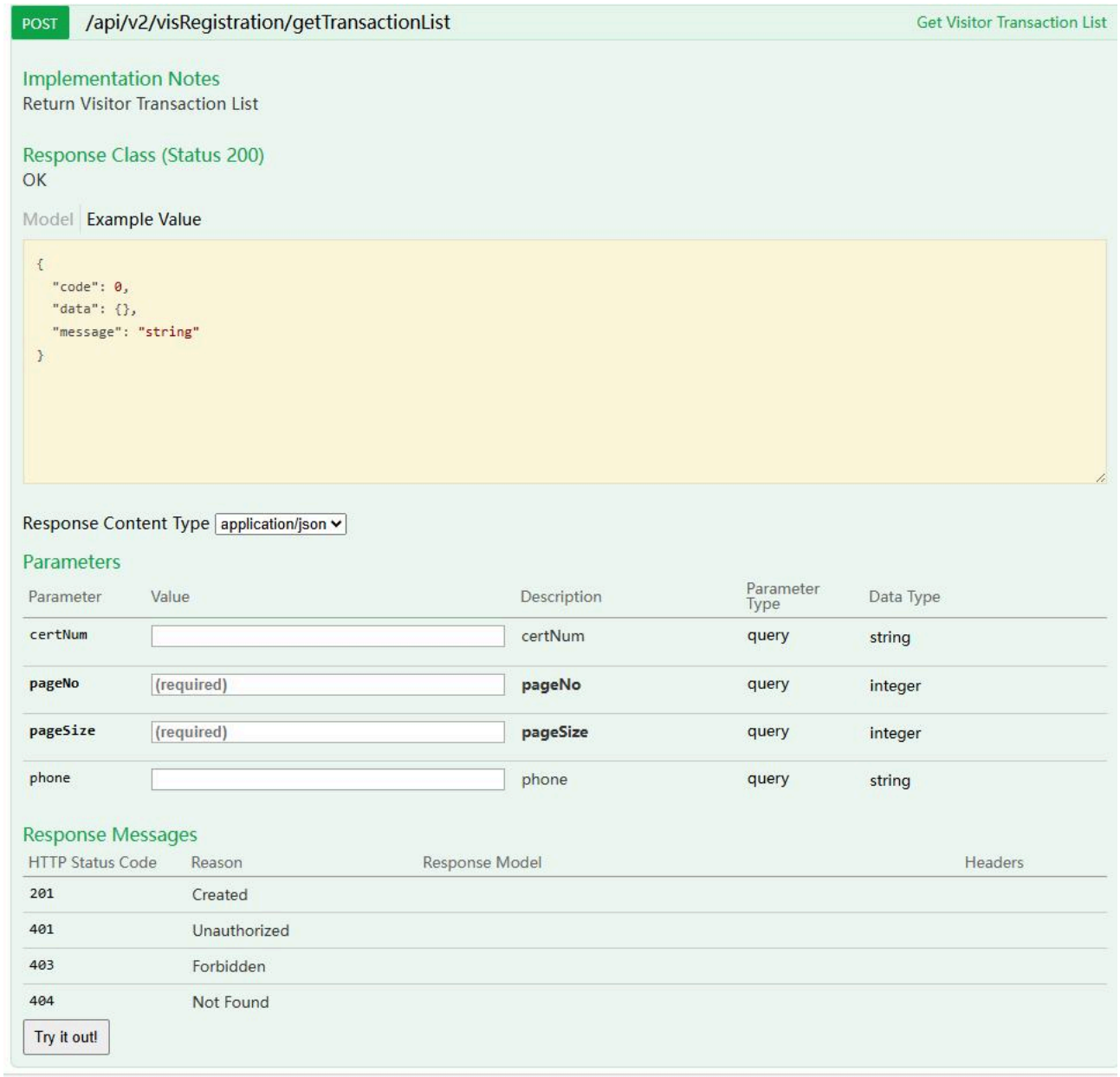
Parameter	Value	Description	Parameter Type	Data Type
deviceName		deviceName	query	string
endDate		endDate	query	string
pageNo	(required)	**pageNo**	query	integer
pageSize	(required)	**pageSize**	query	integer
partitionName		partitionName	query	string
pointName		pointName	query	string
startDate		startDate	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		

- **Added visitor check-in and check-out API endpoints for third-party systems to retrieve visit timestamps.**

The query needs to be made through the mobile phone number and ID number.



POST /api/v2/visRegistration/getTransactionList — Get Visitor Transaction List

Implementation Notes

Return Visitor Transaction List

Response Class (Status 200)

OK

Model | Example Value

```
{
  "code": 0,
  "data": {},
  "message": "string"
}
```

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
certNum		certNum	query	string
pageNo	(required)	pageNo	query	integer
pageSize	(required)	pageSize	query	integer
phone		phone	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		
401	Unauthorized		
403	Forbidden		
404	Not Found		

Try it out!

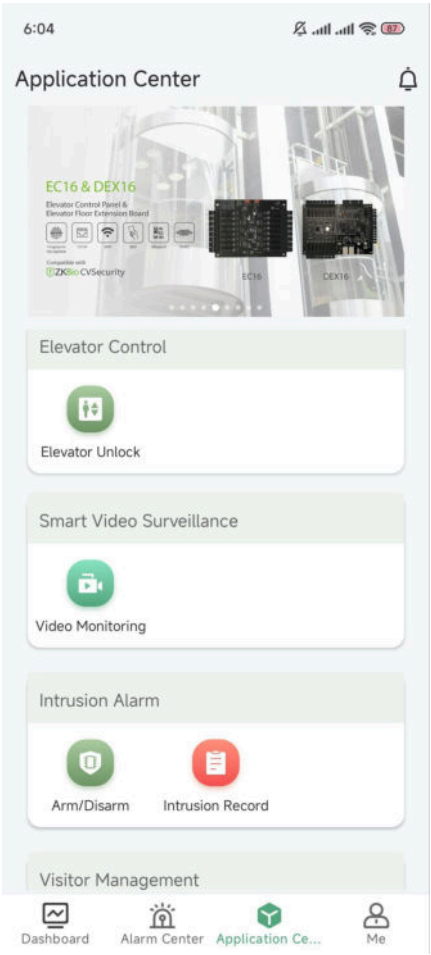
APP

- **Video preview, playback, and PTZ control.**

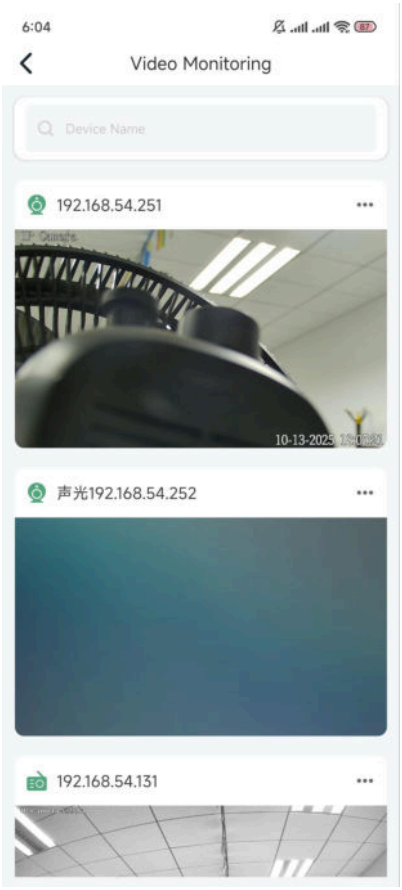
The APP has added a Smart Video Surveillance module. The main updates include support for video preview, video playback, PTZ control, video snapshot, manual recording, and intercom functions.

Note: The video stream of the ZKBio Zexus APP uses the T-cloud protocol. Only devices that support this protocol can view it in the APP.Currently, only devices with the latest ZKTECO firmware are supported. Third-party devices are not supported for management in the APP.

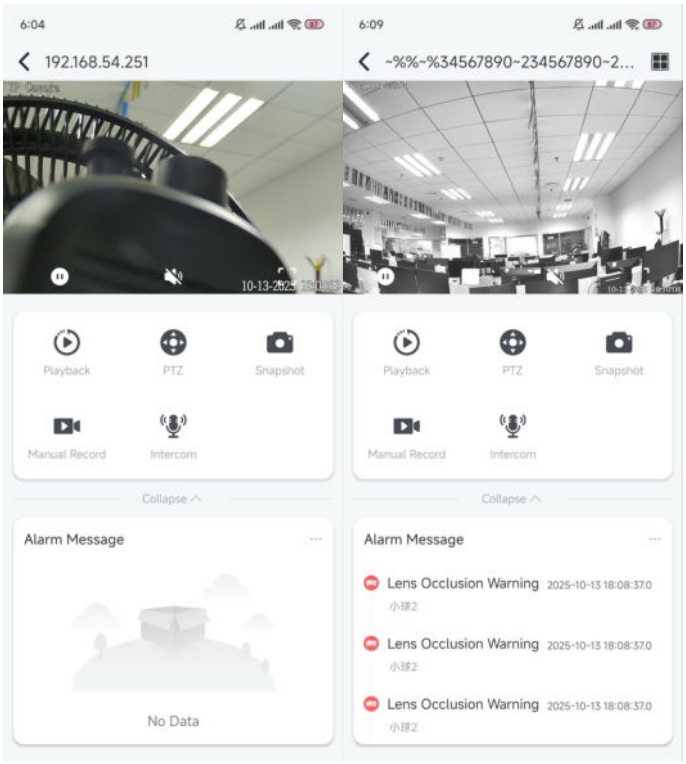
Operation (Administrator): Click on the Application Center -> Video Monitoring to enter the video view function. On the home page of this function.



You can view the device list and the current screen.

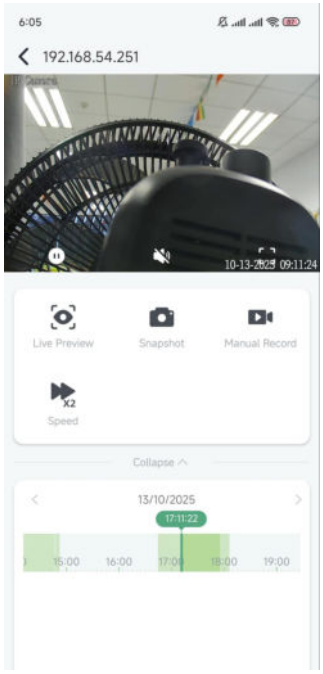


By clicking on the device, you can perform playback, PTZ control, snapshot, manual recording, and intercom operations.



■ **Playback:**

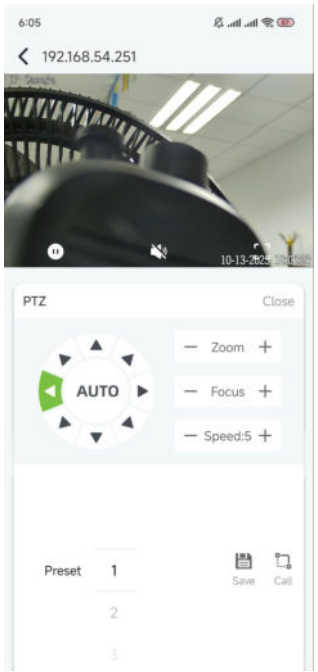
The playback of the picture can be achieved by dragging the timeline below. The playback page allows you to continue taking snapshots, manually record videos, or adjust the speed through "Speed". There are three speed Settings available:x 0.5, x1, and x2.



■ **PTZ:**

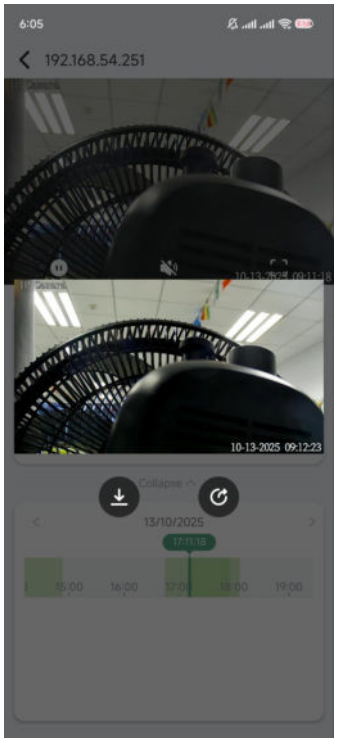
The camera can be remotely controlled in terms of direction, with a minimum adjustment Angle of 45 degrees. It also allows for zooming in and out of the picture, focus control, and adjustment of the camera's movement speed, ranging from 1 to 10.

You can save the preset position. Click "Save" at the current position to save the current position, and click "Call" to quickly restore to the saved position. It supports saving up to 255 preset bits at most.



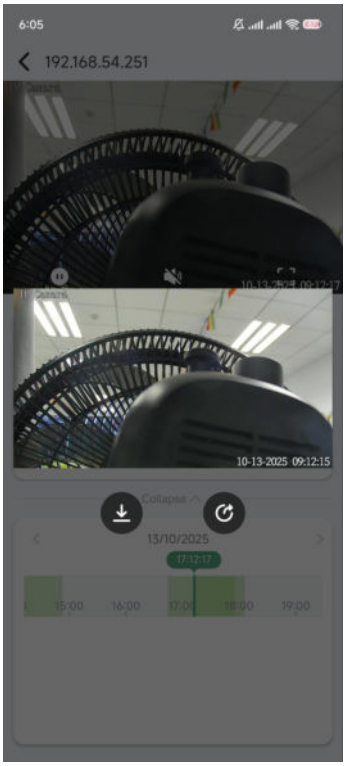
■ **Snapshot:**

Click "Snapshot" to capture the scene. You can save and forward the captured pictures.After clicking the download button, the captured image will be saved to the phone's album.



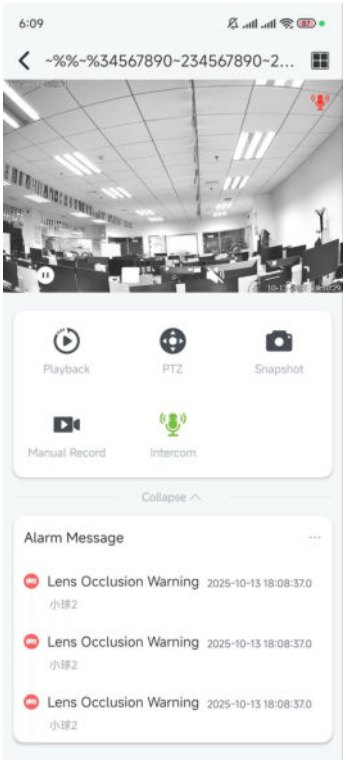
■ **Manual Record:**

Click "Manual Record" to achieve the video recording from the moment of clicking to the moment of clicking again.The video can be downloaded and forwarded.Click the download button and the video can be downloaded to your phone's album.



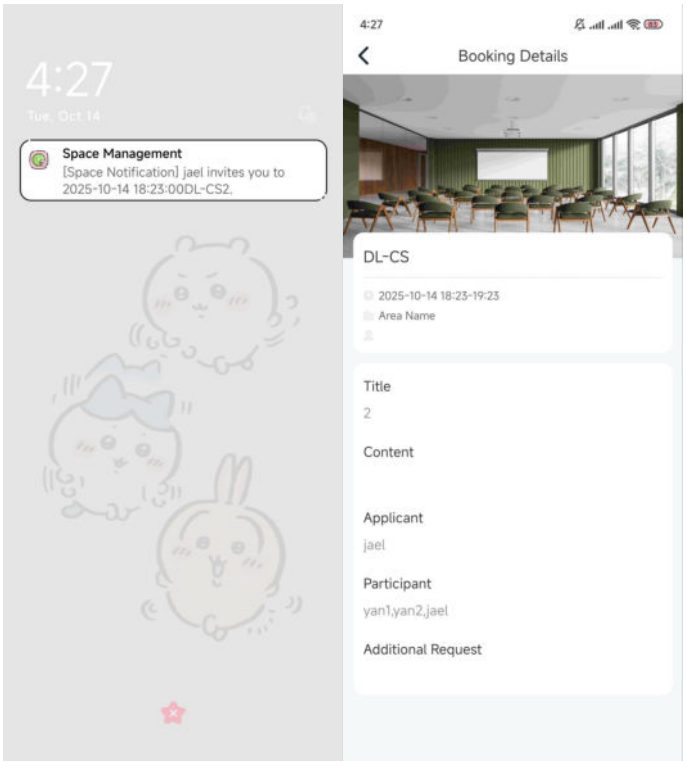
■ **Intercom:**

Click "Intercom" to activate real-time communication with the video scene through video intercom.



● **Background message notifications can redirect to the details page.**

A new function for viewing message details has been added. When there are message push notifications in the background, clicking on the message will redirect you to the message details page.



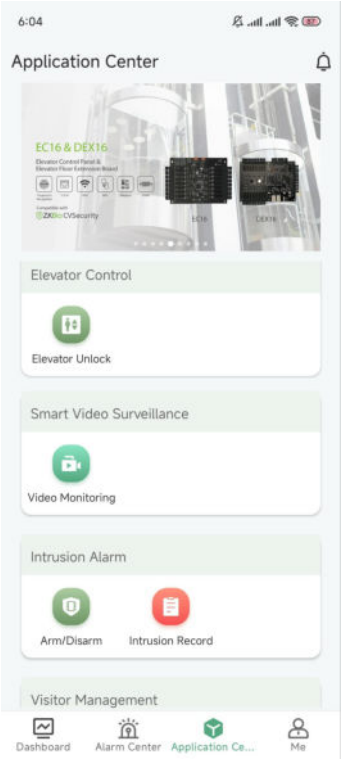
- **Supports one-click arming/disarming and viewing event records.**

The APP has added a Intrusion Alarm module.It is convenient for customers to perform operations such as adding one-click arming and disarming and viewing record functions on the mobile APP.

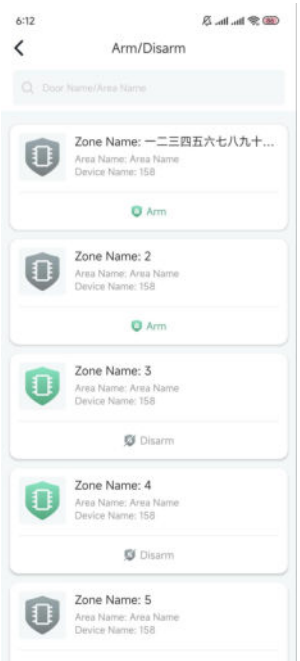
Operation (Administrator):

1. Arm/Disarm

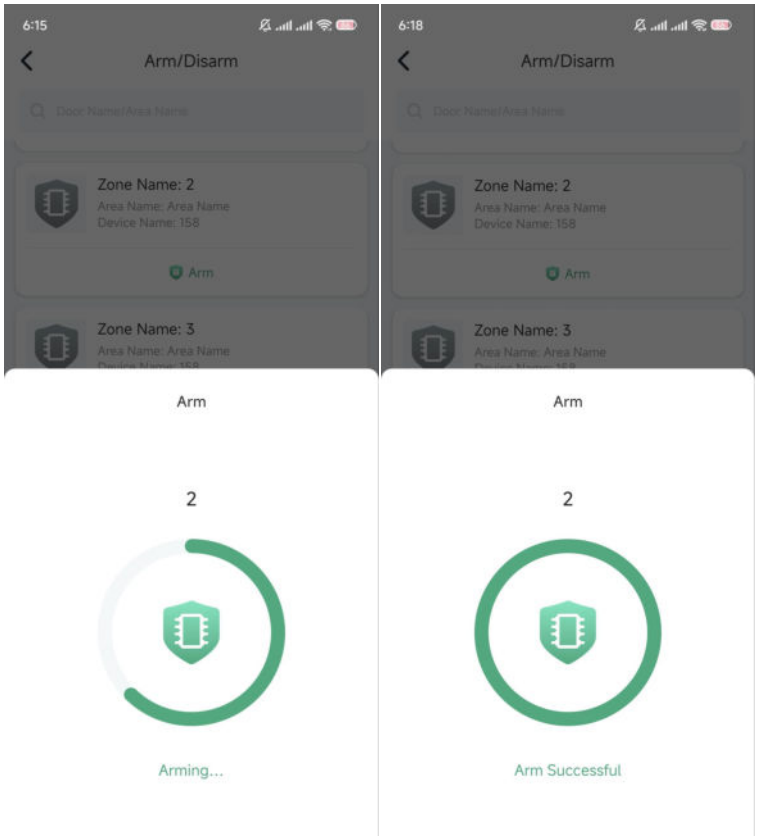
Enter the Application Center -> Intrusion Alarm -> Arm/Disarm.



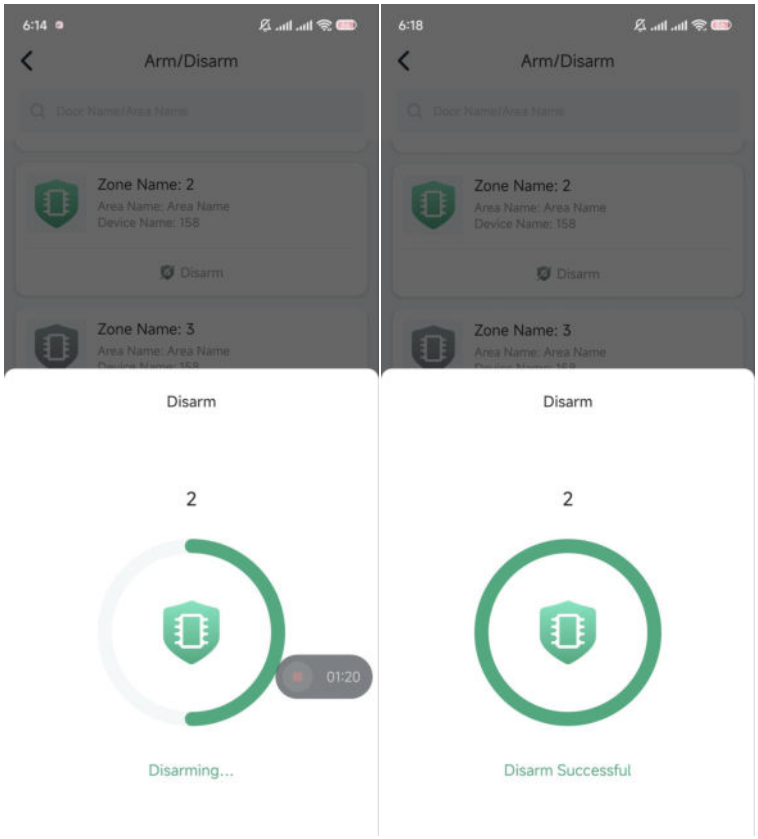
Click on "Arm/Disarm" under the corresponding partition to conveniently perform arming and disarming operations on different partitions on the APP.



Click the "Arm" button under the area to quickly arm that area.After the operation is successful, it will display that "Arm Successful".



Click the "Disarm" button under the area to quickly disarm that area.After the operation is successful, it will display that "Disarm Successful".



There are three types of defense zone states, and the ICONS are shown in the following figure:

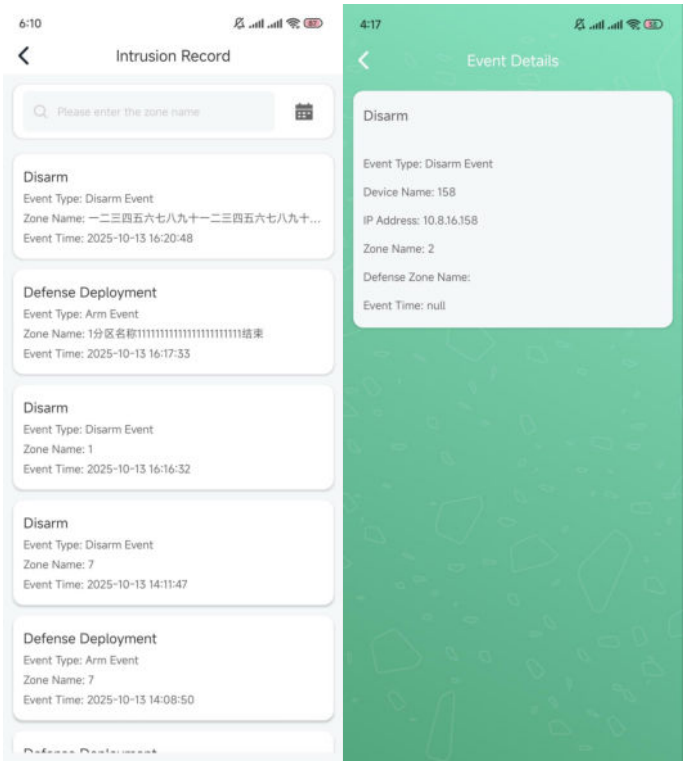
The green icon indicates that the current defense zone is armed, and the "Disarm" button is displayed below.

The gray icon indicates that the current defense zone is not armed, and the "Arm" button is displayed below.

The orange icon indicates that the current defense zone is armed and an alarm event has occurred. Below it, the "Disarm" and "Cancel Alarm" buttons are displayed.

2. Intrusion Record

Enter the Application Center -> Intrusion Alarm -> Intrusion Record, and view the intrusion records. It contains information such as the event type,zone name and event time.



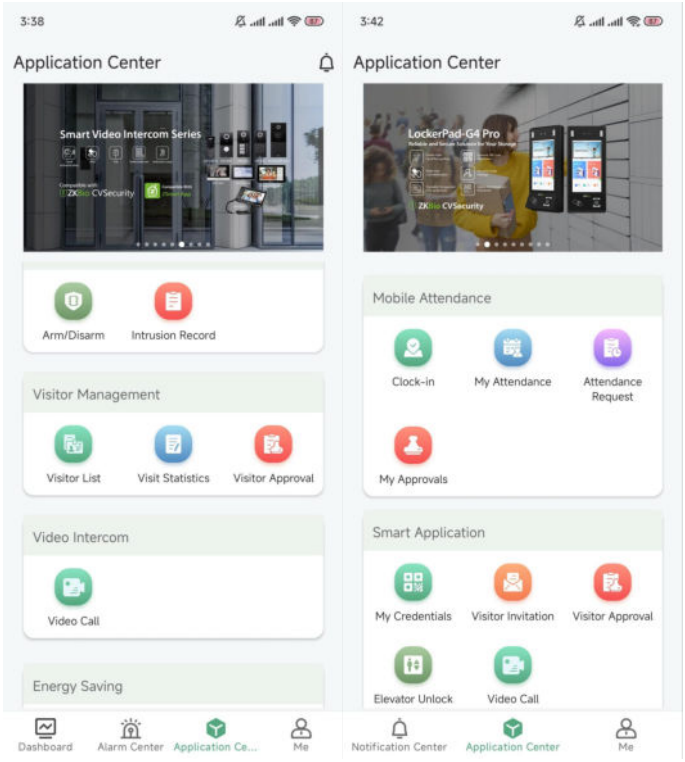
- **Visitor Approval Feature.**

A new visitor approval function has been added to the visitor management module. Users can quickly review visitors through the APP.

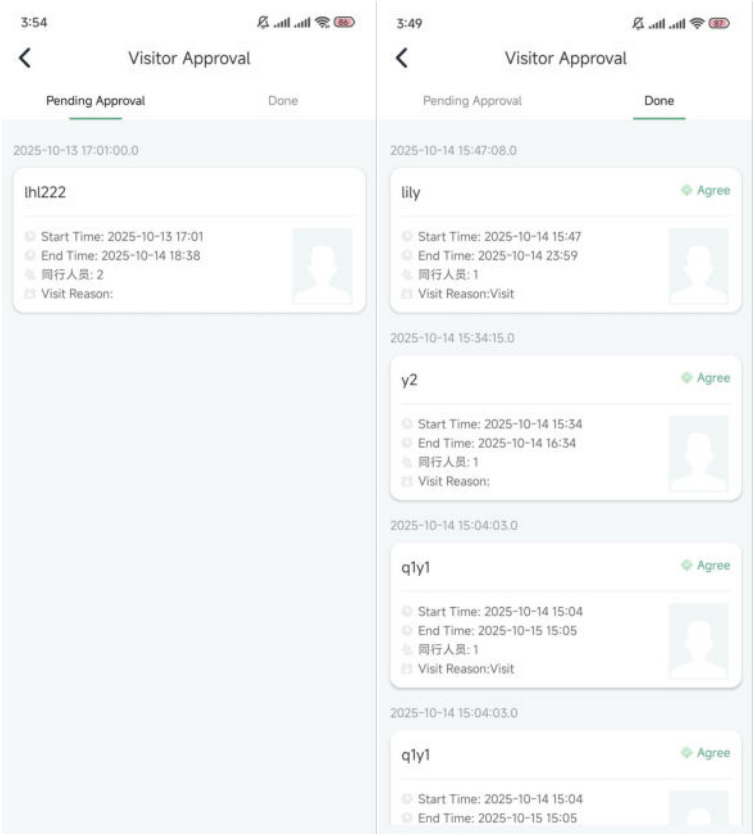
Operation (Administrator & Personnel):

Administrators can enter the Application Center -> Visitor Management -> Visitor Approval.

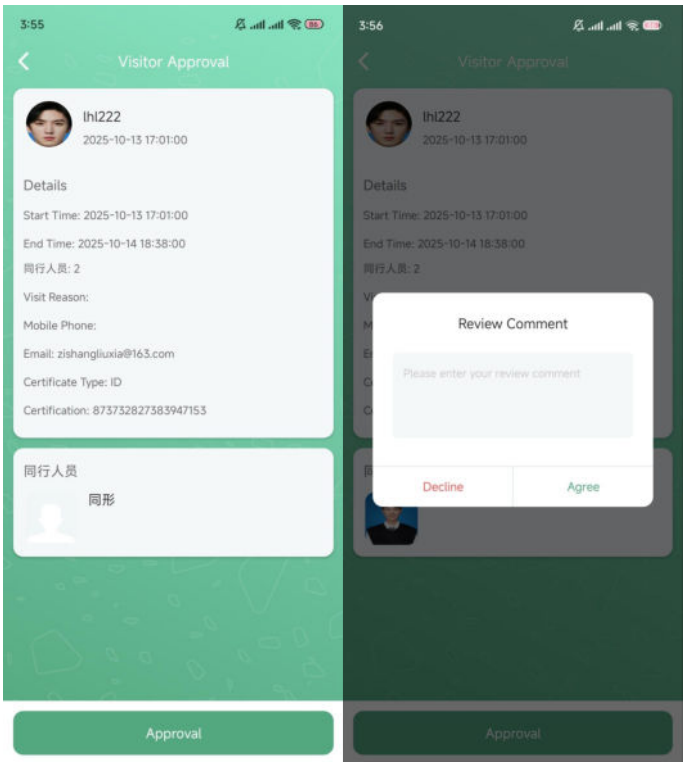
Personnel can enter the Application Center -> Smart Application -> Visitor Approval.



After entering, you can see the personnel pending approval and those that have been completed.



Clicking on this person allows you to approve it and fill in the review opinion of "Agree" or "Decline".

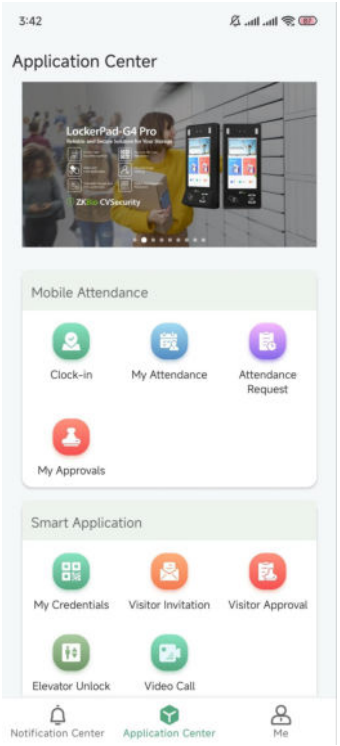


Note: Currently, only administrators and interviewees are supported to perform visitor review operations.Multi-level visitor review is not supported for the time being.

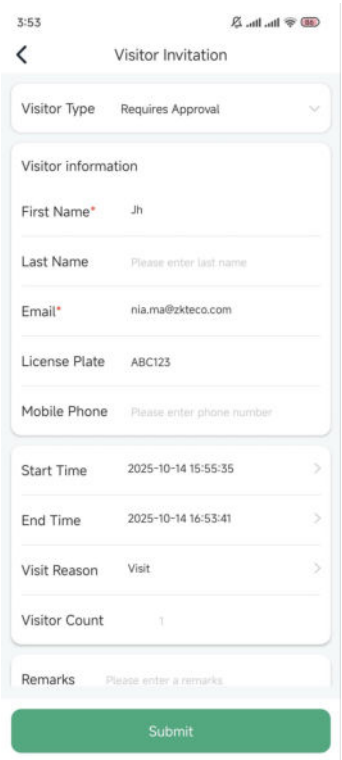
- **Visitor invitation now include a license plate number field.**

Operation (Personnel):

Enter the Application Center -> Smart Application -> Visitor Invitation.

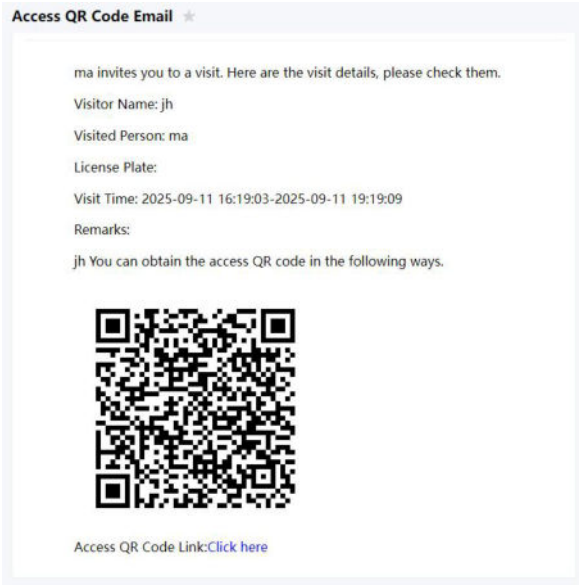


You can fill in the relevant information of the inviter. A new license plate number field has been added to the information, and users can select and fill it in as needed. After submission, a QR code page for information filling will be generated, and an email will be sent to the inviter at the same time.



- **When sending a visitor invitation via the APP and selecting "Direct Access," optimize the content of the visitor email to display detailed visit information.**

When a user logs into the APP to invite a visitor and selects "Direct Access" as the visitor type, the email content received by the visitor after a successful invitation is shown in the figure below:

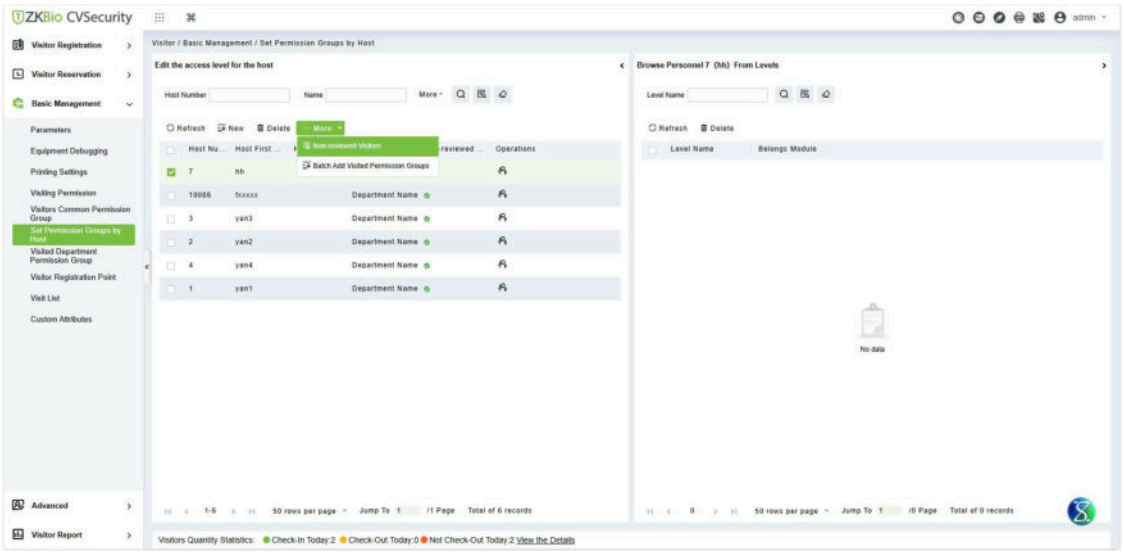


Note: This feature requires administrators to configure the **" Invitation Exemption from Review"** func tion in advance:

a. Navigate to **ZKBio CVSecurity → Visitor → Basic Management → Set Permission Groups by Host**.

b. Add the visitor(s) and assign their permissions.

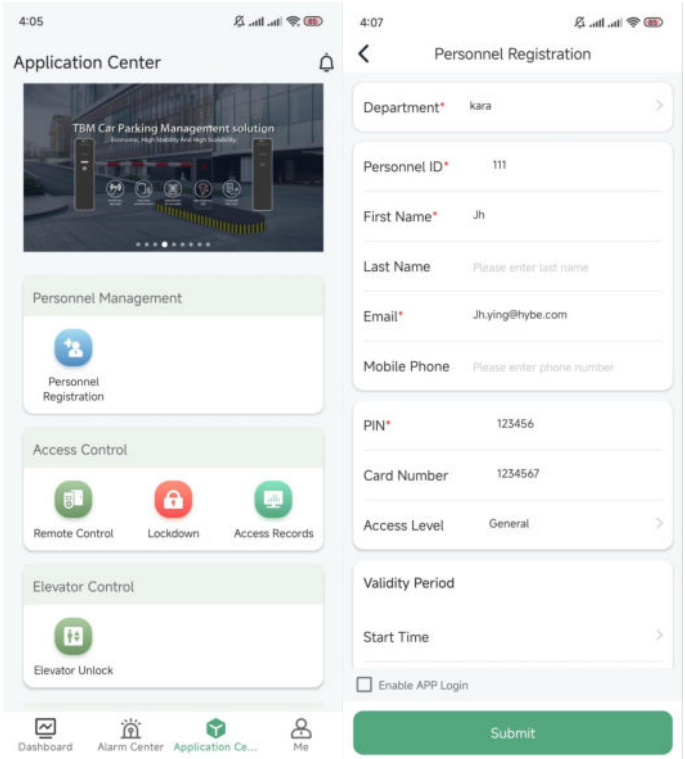
c. Click **More → Non-reviewed Visitors**.



- **Added a "Card Number" field to the personnel registration interface.**

Operation (Administrator End) :

Enter the Application Center -> Personnel Management -> Personnel Registration to register personnel information.

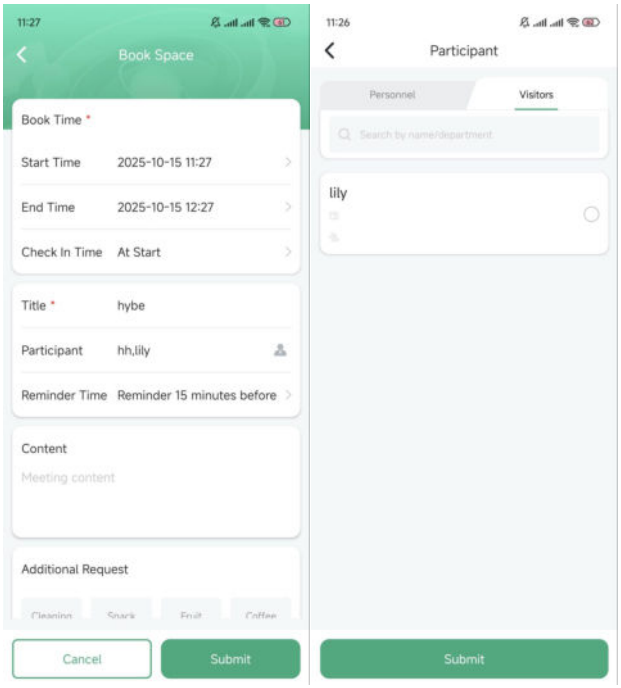


Note: Only one card number can be registered. Multiple card registrations are not supported.

- **Space reservations allow visitors to be selected as attendees.**

Operation (Personnel):

Enter the Application Center -> Smart Application -> Book Space. When clicking on the space to make a reservation, you can click the icon on the right in the "Participant" column to add a visitor. After checking the visitor box, click "Submit" to add successfully.



Note: The types of visitors who can be selected as attendees are those who have made an reservation or check-in.