

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.

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

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

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	8
ACCESS CONTROL	12
● Background Verification-Requires manual approval from management personnel after device authentication, adding a second layer of verification before granting access.....	12
● Open Door Duration-Set different door opening durations based on personnel.....	13
● Navigate Access > Access Rule: Personnel export from permission groups now includes name field in exported data.....	13
● Navigate Access > Access Rule: Batch import now supports setting validity periods for multiple personnel simultaneously.....	14
● The holiday settings for access control now support batch import and export.....	16
VISITOR MANAGEMENT	18
● Navigate Visitor - Visitor Report - Visiting Record: Added department field to visiting record display.....	18
● Visitor Check-in Parameter Optimization.....	18
● Filter visitor reports according to user permissions. For example, User 1 can only view visitor records related to Department 1.....	19
● After a successful reservation, visitors need to authorize the corresponding parking lot area, rather than being able to enter all parking lots.....	20
● When sending a visitor invitation via the APP and selecting "Direct Access," optimize the content of the visitor email to display detailed visit information.....	21
TIME & ATTENDANCE	22
● Add a "PUSH Version" field display in the Attendance Device Menu.....	22
● Automatic Report supports department selection, sending attendance records only for the selected department to recipients.....	23
● The holiday settings for attendance module now support batch import and export.....	23
PERSONNEL	25
● 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.....	25
SPACE MANAGEMENT	26
● Space reservations allow visitors to be selected as attendees.....	26
● Zoom Integration-Supports binding one Zoom ID to each meeting room, automatically generating meeting links for app-based reservations.....	27
● Microsoft 365 integration synchronizes Teams / Outlook meeting reservations with conference room devices.....	33
VIDEO INTERCOM	44
● Supports bulk import of devices via excel.....	44
● The shortcut menu has been moved under the Device Management menu.....	46
● In apartment visual intercom scenarios, remote door unlocking via the entrance terminal is supported, along with the allocation of elevator access permissions for visitors.....	49
● The SIP service mode has been moved to the Video Intercom → Parameters page.....	52

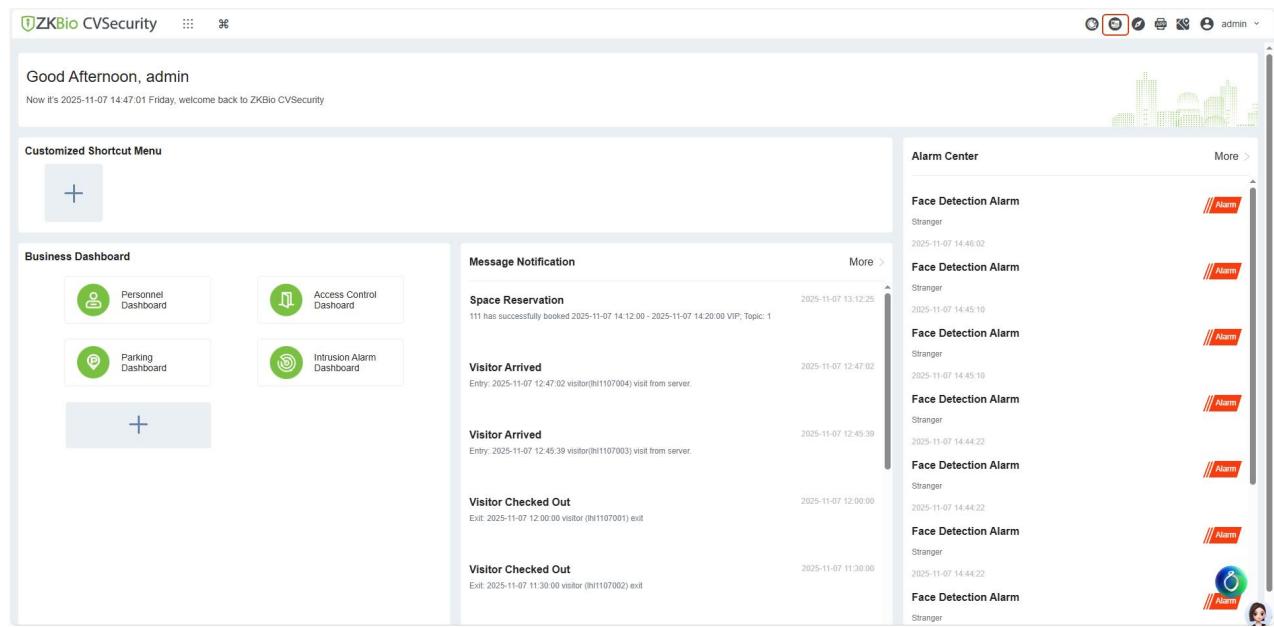
SERVICE CENTER	54
● Map Center-Supports voice intercom operations when previewing camera points.....	54
● Map Center-Added visual intercom points.....	54
● Map Center-Intrusion alarm zones support secondary editing and display of zone numbers.....	55
● Linkage Center-Added "Remind Message" as a new output action option, supporting Email, SMS, and WhatsApp.....	56
● Linkage Center-When a doorbell is pressed, it can activate linked cameras to start recording.....	57
● Linkage Center-The linkage trigger condition has added an Intrusion Alarm.....	58
● Linkage Center-The output action has added an Emergency Evacuation.....	58
● Event Center-Added event subscription notifications.....	59
● Event Center-Supports batch selection and processing of events.....	60
● Push Center-Added vehicle entry and exit records.....	61
● Scene Center-Added work safety scenarios.....	61
● Scene Center-Emergency Evacuation Scene: Added support for parking module devices at the main entrance and exit.....	66
● Scene Center-Added Personnel Entry & Exit Panel.....	66
● Scene Center-Added Intelligent Visitor Panel.....	69
INTRUSION ALARM	72
● 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.....	72
ELEVATOR CONTROL	73
● DCS function optimized.....	73
● 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.....	77
● The holiday settings for Elevator Control now support batch import and export.....	80
SMART VIDEO SURVEILLANCE	82
● Integrated with TP-Link NVR to enable preview, playback, intelligent alert display, and alarm linkage.....	82
● Supports batch synchronization of list databases to multiple devices.....	86
● Support linkage with IPC (access control or video linkage with IPC).....	88
SYSTEM	89
● Supports reading Malaysian ID cards via the RS100 passport scanner.....	89
● Card Printing Template Optimized.....	91
● 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.....	92
PARKING	93
● Function Optimized-BEST and HTTP protocol devices now fully compatible for simultaneous operation.....	93
● Ticket machines now record license plates (captured by LPRC300) for lost ticket recovery and payment.....	93
CONSUMPTION	95
● Personnel must complete attendance check-in on the same day before they can make consumption.....	95

● Added a filter for "Approval Status" in the offline consumption details table.....	95
● Added an "Type Name" field to the consumption details table.....	96
● Added a "Restaurant" field and filter option to the personal consumption statistics table.....	96
API	97
● Added license plate, remarks, and photo fields to visitor reservation API (POST / api/ visReservation / add)...	97
● Added attendance checkpoint data (personnel, time, location) to /api/v2/transaction/listAttTransaction.....	98
● A new intrusion alarm API interface has been added.....	99
● Added visitor check-in and check-out API endpoints for third-party systems to retrieve visit timestamps....	100
APP	101
● Video preview, playback, and PTZ control.....	101
● Background message notifications can redirect to the details page.....	105
● Supports one-click arming/disarming and viewing event records.....	106
● Visitor Approval Feature.....	108
● Visitor invitation now include a license plate number field.....	110
● When sending a visitor invitation via the APP and selecting "Direct Access," optimize the content of the visitor email to display detailed visit information.....	111
● Added a "Card Number" field to the personnel registration interface.....	112
● Space reservations allow visitors to be selected as attendees.....	113

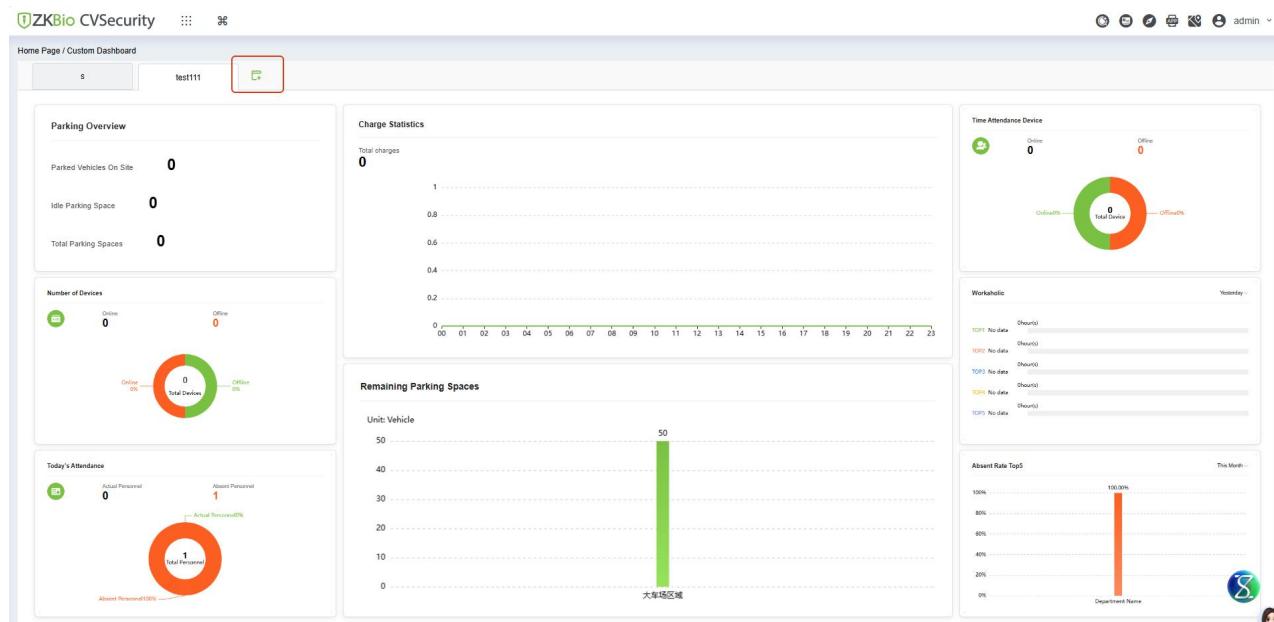
Custom Panel

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

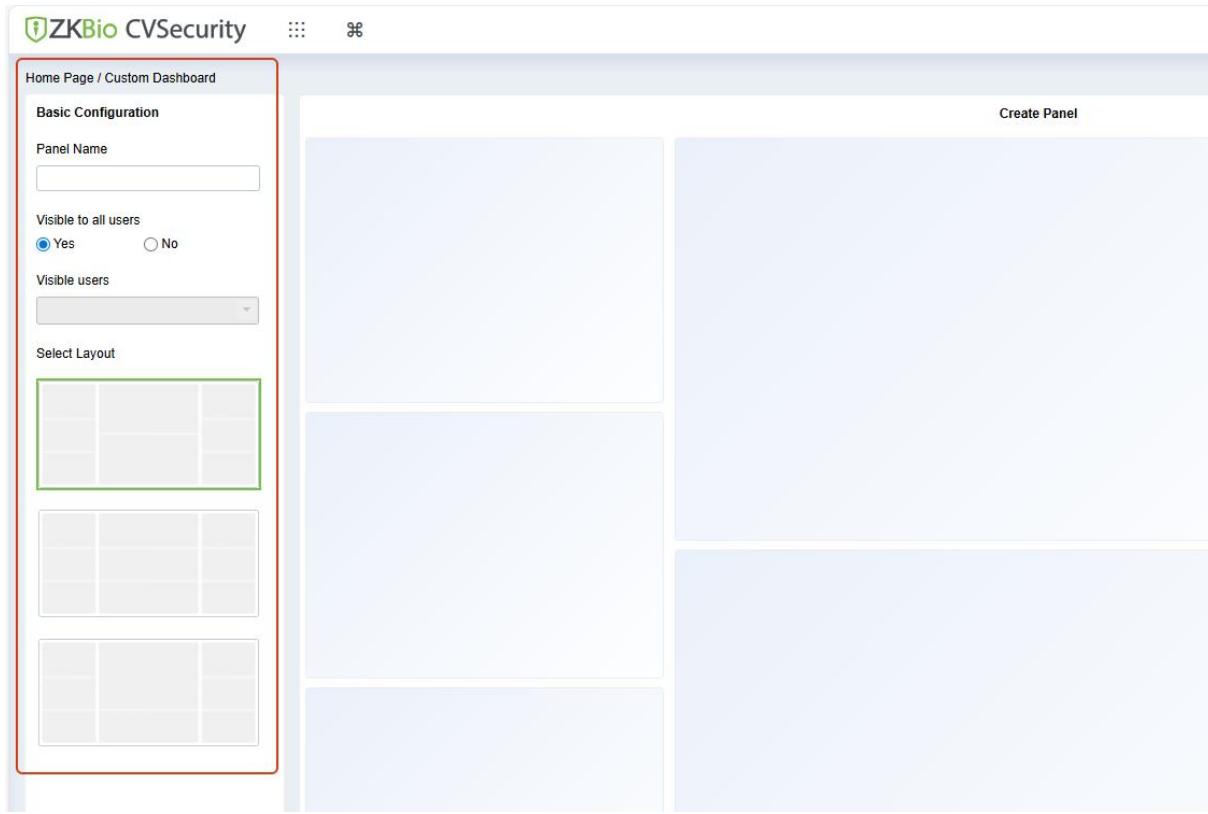
Step1: Click the small icon  of Custom Panel in the upper right corner to access the viewing and configuration interface.



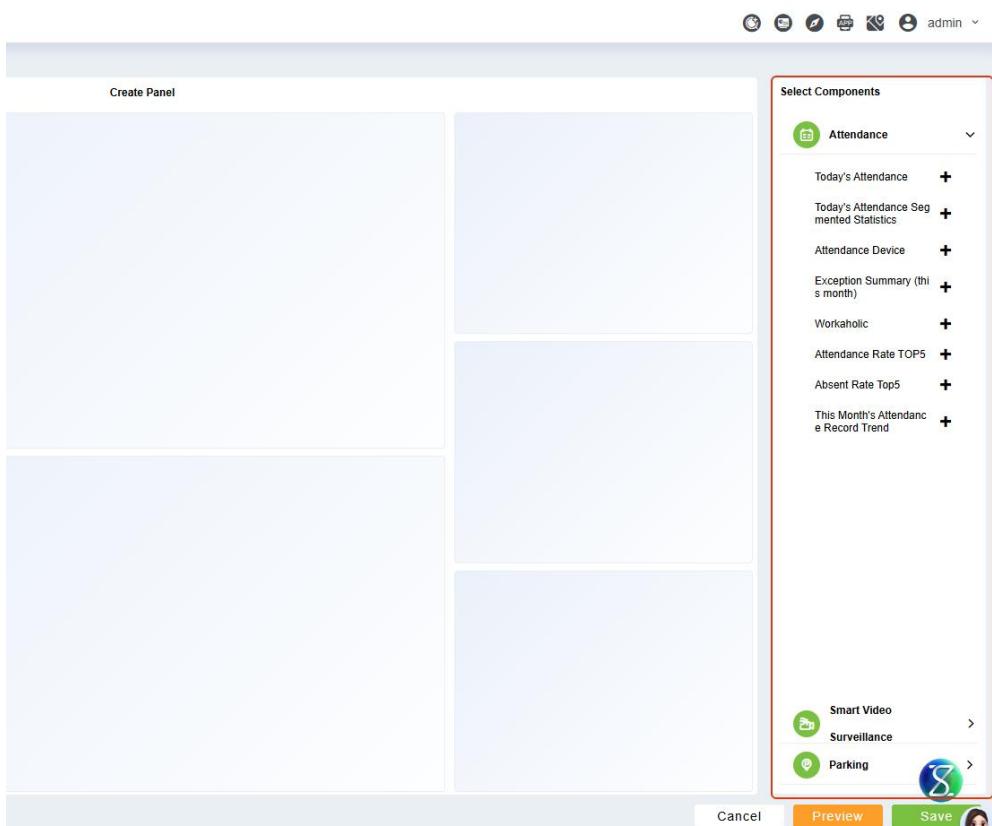
Step2: On this page, you can view the configured Custom Panels. Click the Add button  to access the configuration interface.



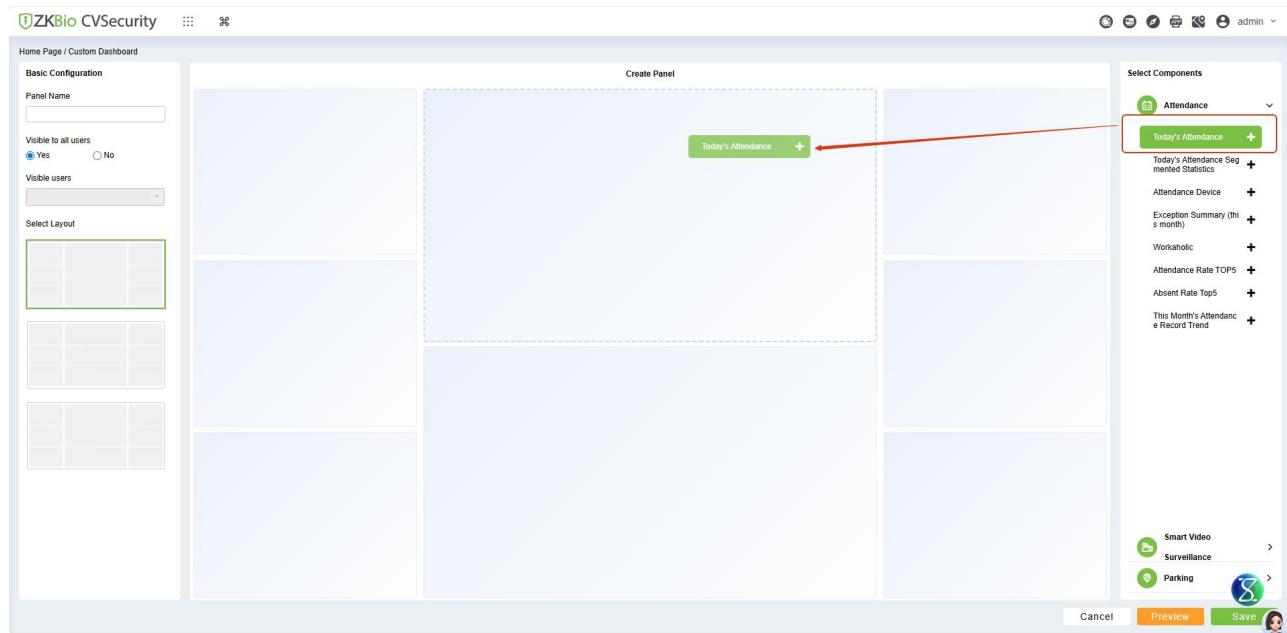
Step3: On the left side of the configuration interface, you can set the panel name and check whether it is visible to all users. If you select "No", you can further select which users are allowed to view it. Then choose a suitable panel layout to start the configuration.



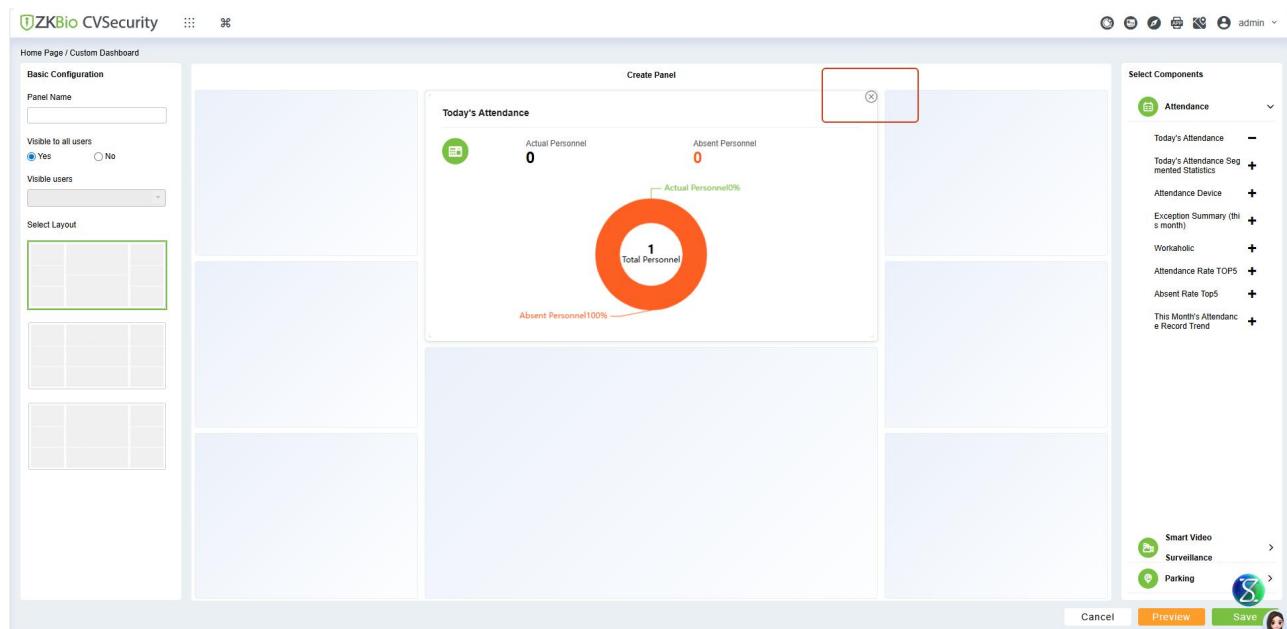
Step4: On the right side of the configuration interface, components for multiple modules are provided. Users can freely combine them to form a visualized data panel that suits their needs.



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.

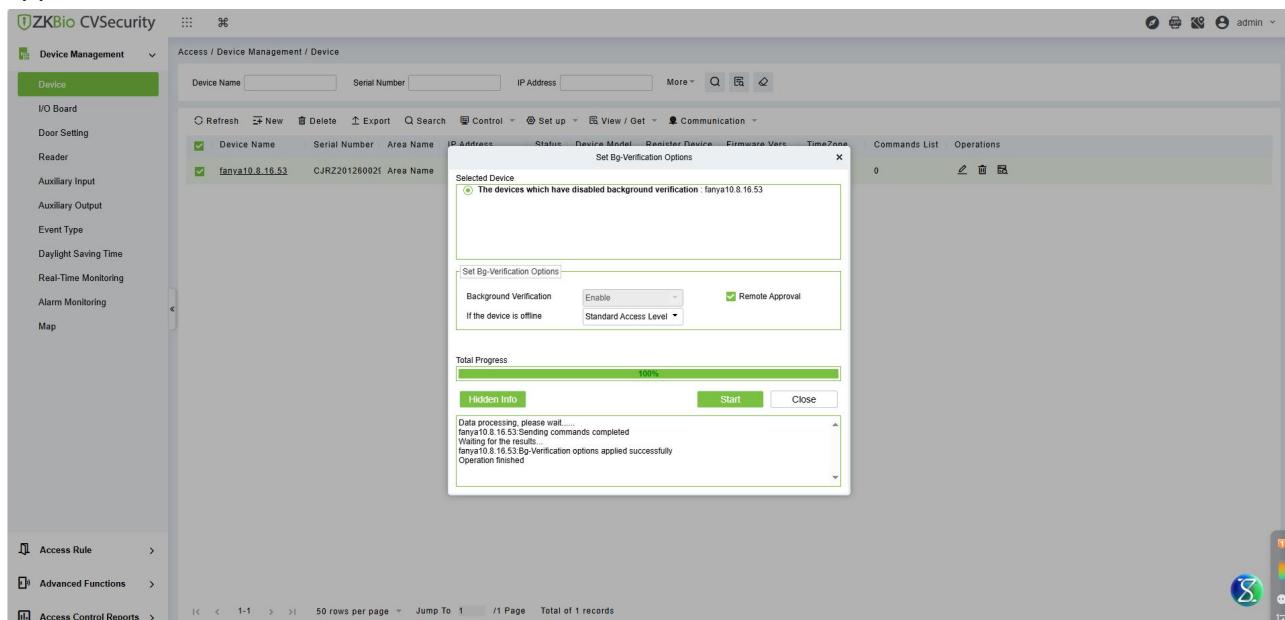
Users with permission can click the Delete button to remove the panel; once deleted, it will no longer be visible to all users.

Access Control

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

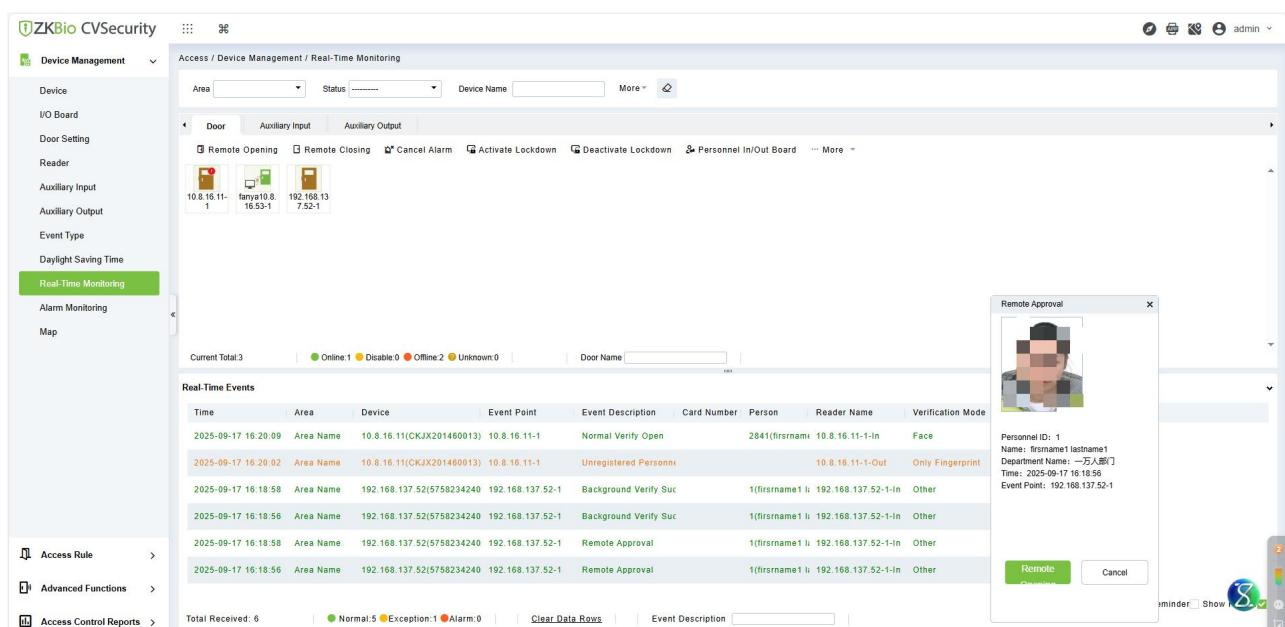
Applicable Scenarios: High-security areas such as bank vaults and data centers.

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.



The screenshot shows the ZKBio CVSecurity Device Management interface. On the left, a sidebar lists various device-related options like I/O Board, Door Setting, Reader, and Auxiliary Input. The main panel shows a table of devices with columns for Device Name, Serial Number, Area Name, IP Address, Status, Device Model, Reader Model, Firmware Ver., and Time Zone. A specific device, 'fanya10.8.16.53', is selected. A modal dialog box titled 'Set Bg-Verification Options' is open, containing a section for 'Background Verification' with a dropdown set to 'Enable' and a checked checkbox for 'Remote Approval'. Below this, a sub-section for 'If the device is offline' has a dropdown set to 'Standard Access Level'. A progress bar at the bottom of the dialog shows 100% completion. The status bar at the bottom of the main window indicates 'Data processing, please wait...' and 'Waiting for the results: fanya10.8.16.53 Bg-Verification options applied successfully'.

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:



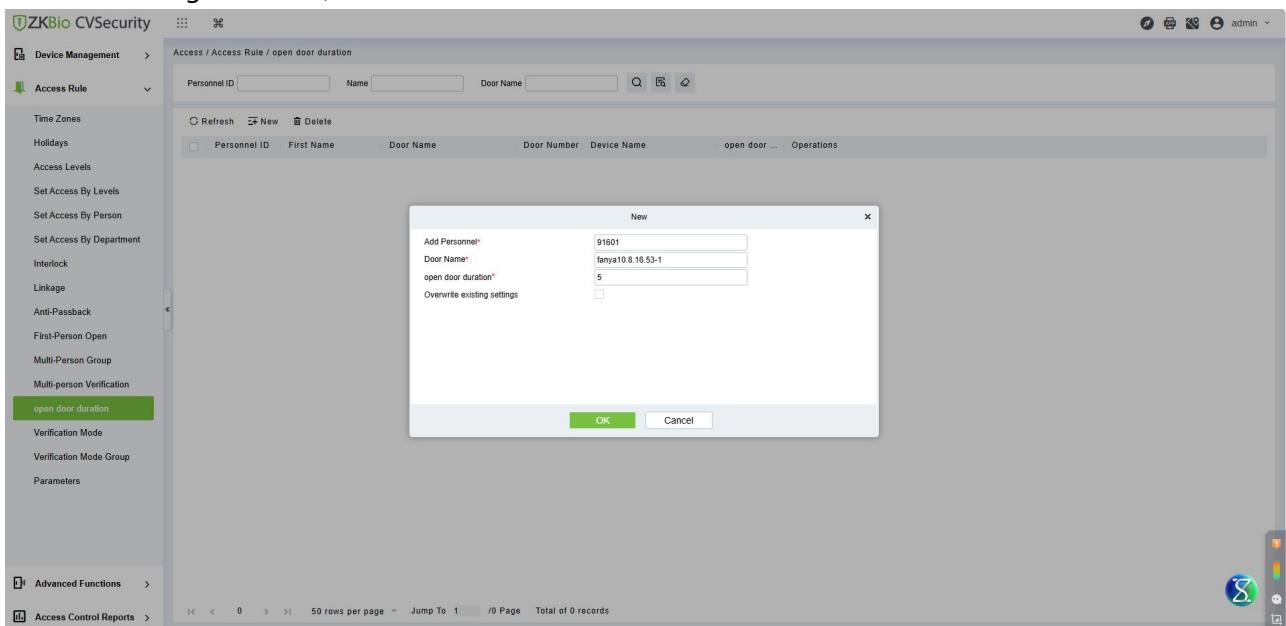
The screenshot shows the ZKBio CVSecurity Real-Time Monitoring interface. The left sidebar includes 'Real-Time Monitoring' under the 'Device Management' section. The main area displays a list of 'Real-Time Events' with columns for Time, Area, Device, Event Point, Event Description, Card Number, Person, Reader Name, and Verification Mode. The events listed are: 1. 2025-09-17 16:20:09, Area: 10.8.16.11(CKJX201460013), Device: 10.8.16.11-1, Event: Normal Verify Open, Person: 2841(firstname1), Reader: 10.8.16.11-1-in, Mode: Face. 2. 2025-09-17 16:20:02, Area: 10.8.16.11(CKJX201460013), Device: 10.8.16.11-1, Event: Unregistered Person, Person: 10.8.16.11-1-out, Reader: 10.8.16.11-1-out, Mode: Only Fingerprint. 3. 2025-09-17 16:18:58, Area: 192.168.137.52(5758234240), Device: 192.168.137.52-1, Event: Background Verify Suc, Person: 1(firstname1), Reader: 192.168.137.52-1-in, Mode: Other. 4. 2025-09-17 16:18:56, Area: 192.168.137.52(5758234240), Device: 192.168.137.52-1, Event: Background Verify Suc, Person: 1(firstname1), Reader: 192.168.137.52-1-in, Mode: Other. 5. 2025-09-17 16:18:58, Area: 192.168.137.52(5758234240), Device: 192.168.137.52-1, Event: Remote Approval, Person: 1(firstname1), Reader: 192.168.137.52-1-in, Mode: Other. 6. 2025-09-17 16:18:56, Area: 192.168.137.52(5758234240), Device: 192.168.137.52-1, Event: Remote Approval, Person: 1(firstname1), Reader: 192.168.137.52-1-in, Mode: Other. A 'Remote Approval' dialog box is overlaid on the interface, showing a blurred image of a person's face and the text: 'Personnel ID: 1', 'Name: firstname1 lastname1', 'Department Name: 一万人部门', 'Time: 2025-09-17 16:18:56', 'Event Point: 192.168.137.52-1', and two buttons: 'Remote Approval' and 'Cancel'.

- **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	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 screenshot shows the ZKBio CVSecurity software interface. On the left, a sidebar lists various access-related functions. The main area displays two tables: 'Edit Personnel For Levels' and 'Browse Personnel 28258 From Levels'. The 'Import' button is highlighted in the personnel list table, indicating the next step in the process.

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.

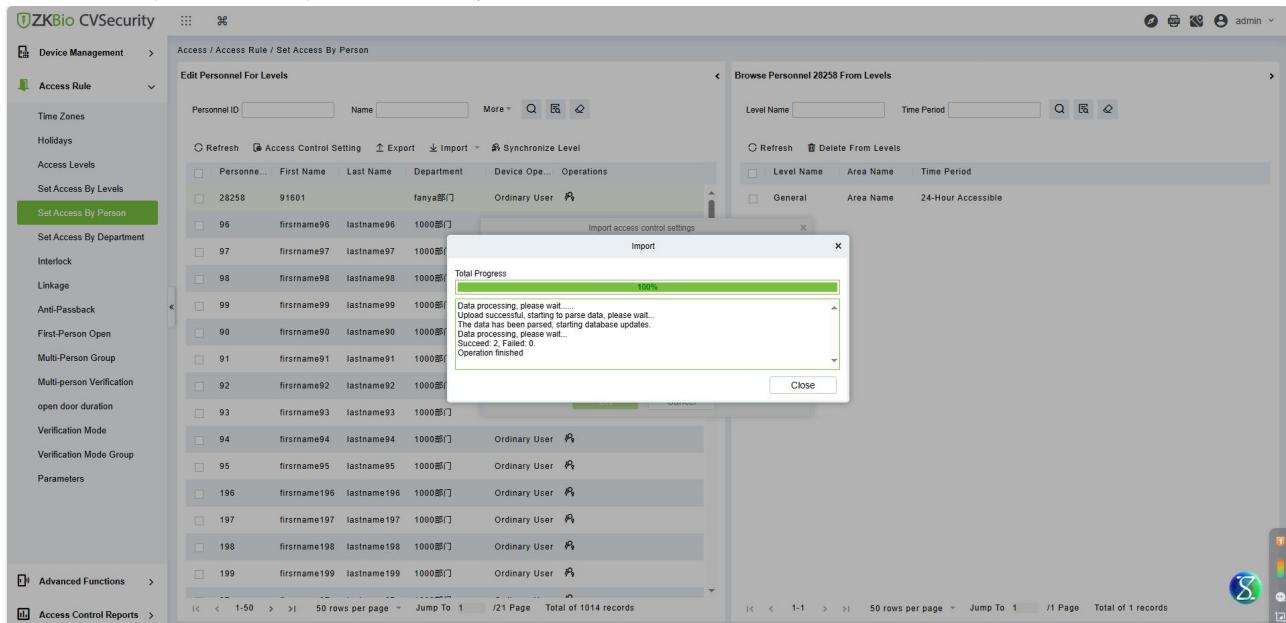
Cells with red triangles contain important annotations—click them to view data entry guidelines.

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."

The screenshot shows the ZKBio CVSecurity software interface. The 'Import access control settings' dialog box is open, showing the file format as 'Excel' and a file path selected. The background shows the 'Edit Personnel For Levels' and 'Browse Personnel 28258 From Levels' tables.

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.

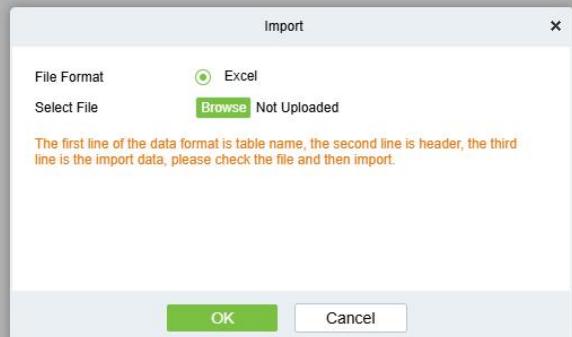


Step 2: Open the exported template file "Holiday Template.xls" for adding holiday information.

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.



Import

File Format: Excel

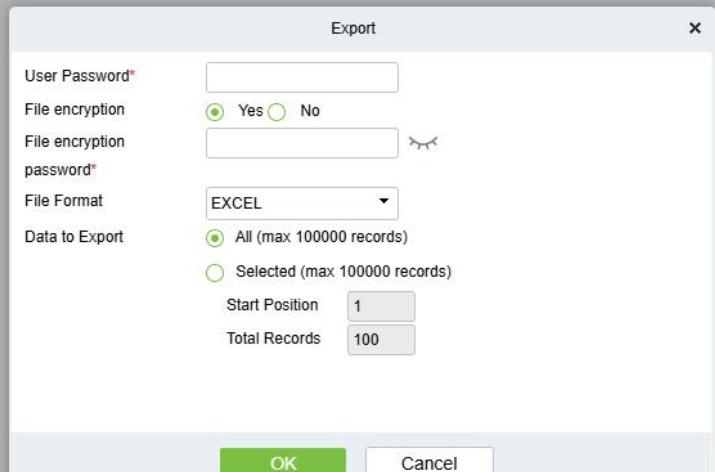
Select File: Not Uploaded

The first line of the data format is table name, the second line is header, the third line is the import data, please check the file and then import.

OK Cancel

■ Export:

Click the "Export" and set the relevant parameters.



Export

User Password*:

File encryption: Yes No

File encryption password*:

File Format: EXCEL

Data to Export: All (max 100000 records) Selected (max 100000 records)

Start Position: 1

Total Records: 100

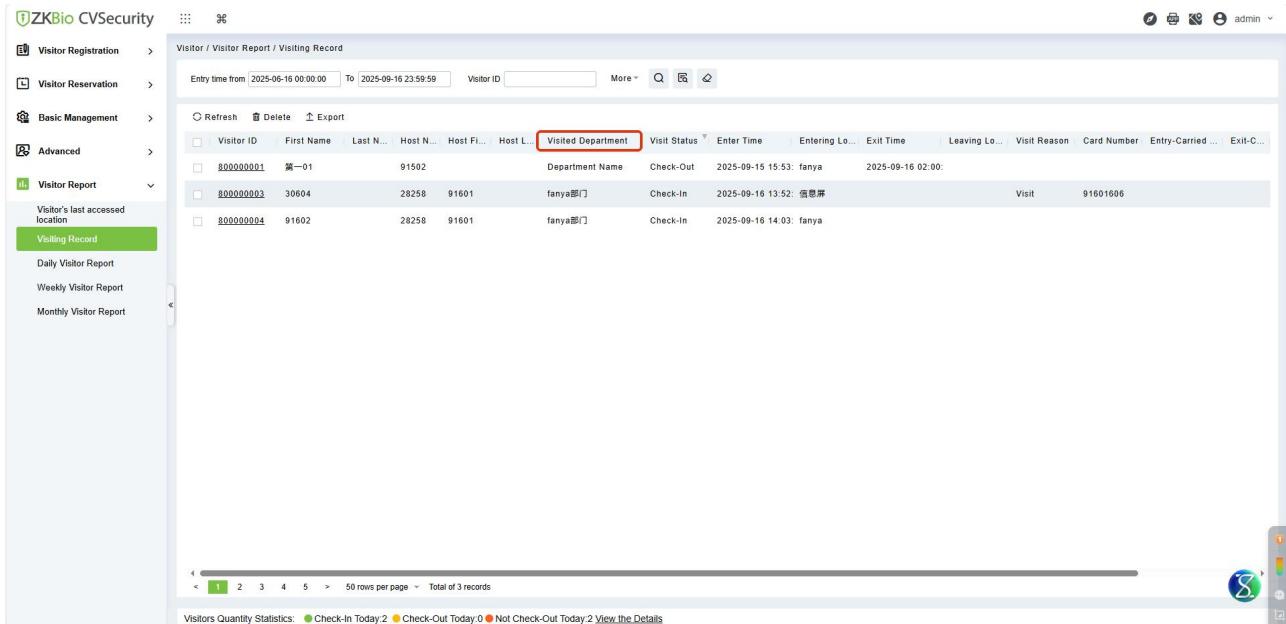
OK Cancel

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

Visitor Management

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

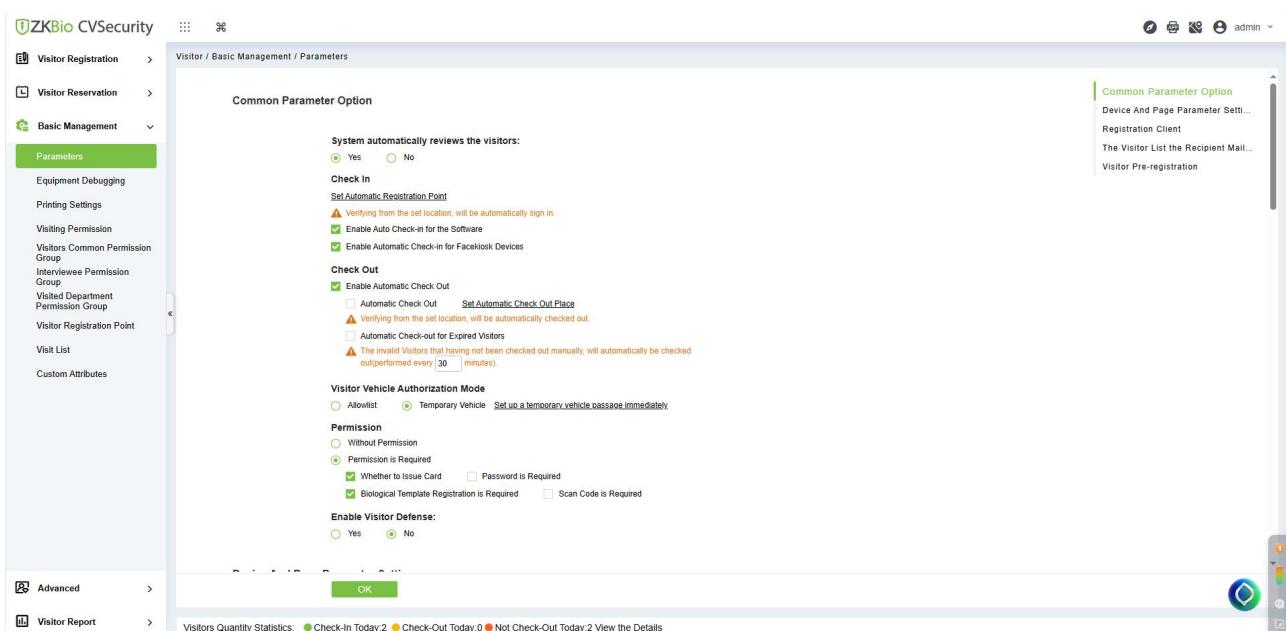
Step: Enter Visitor → Visitor Report → Visiting Record, can view the visiting Record, which includes the field of Visited Department.



The screenshot shows the 'Visiting Record' section of the ZKBio CVSecurity system. The 'Visited Department' column is highlighted in red. The data table includes columns for Visitor ID, First Name, Last Name, Host ID, Host Location, Visited Department, Visit Status, Enter Time, Entering Location, Exit Time, Leaving Location, Visit Reason, Card Number, and Entry-Carried. The 'Visited Department' column shows values like 'fanya部门' for visitors with IDs 80000003 and 80000004.

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

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



The screenshot shows the 'Parameters' section of the ZKBio CVSecurity system under 'Basic Management'. The 'Check In' section is highlighted. It includes options like 'Enable Auto Check-in for the Software' and 'Enable Automatic Check-in for FaceKiosk Devices'. The 'Check Out' section also contains options like 'Enable Automatic Check Out' and 'Set Automatic Check Out Place'.

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.

Visitor / Basic Management / Parameters

System automatically reviews the visitors:

Check In

Check Out

Visitor Vehicle Authorization Mode

Temporary Vehicle *Set up a temporary vehicle passage immediately*

Permission

Enable Visitor Defense:

Device And Page Parameter Settings

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.

Visitor / Basic Management / Parameters

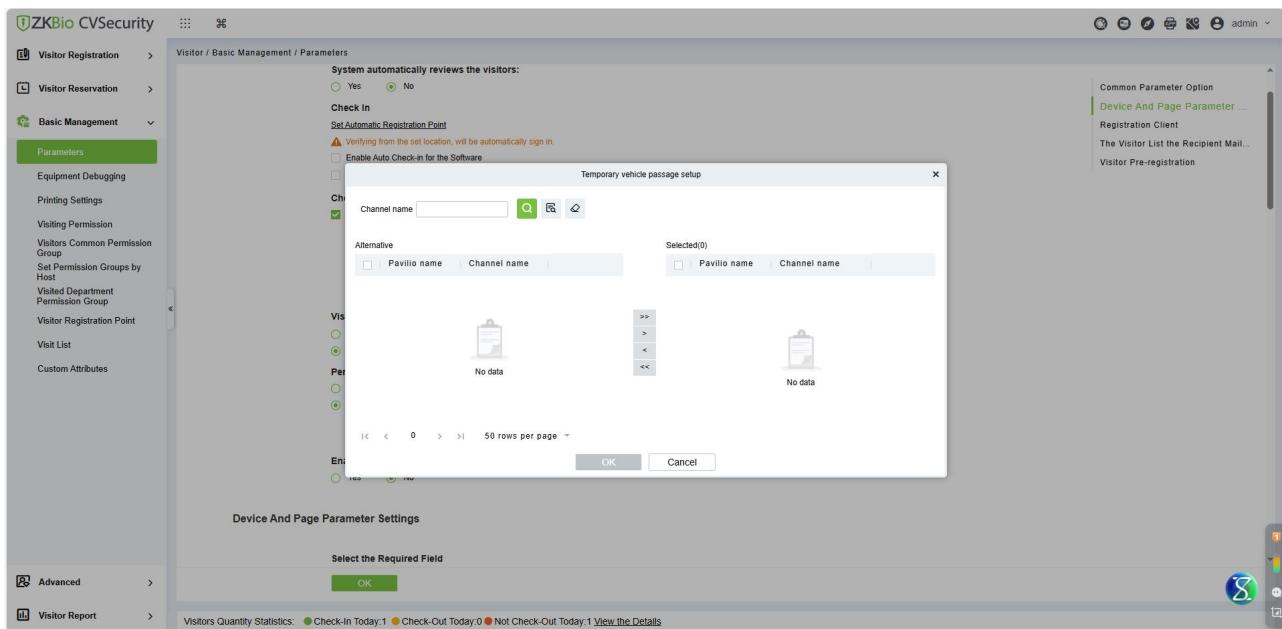
Temporary vehicle passage setup

Please add a temporary vehicle passage

New
Select All
Deselect All

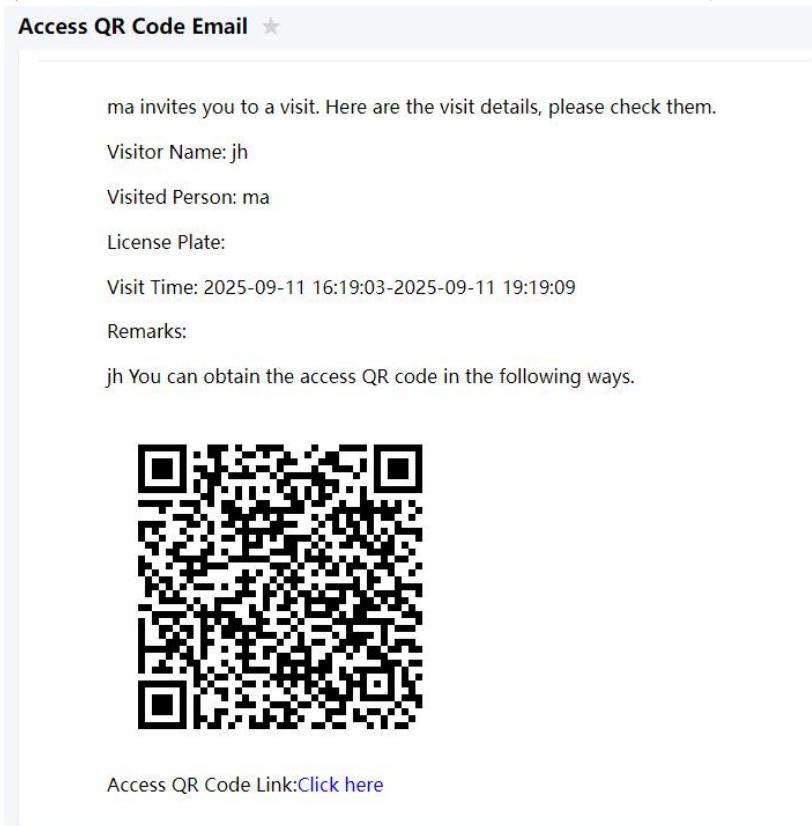
Temporary Vehicle *Set up a temporary vehicle passage immediately*

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.**

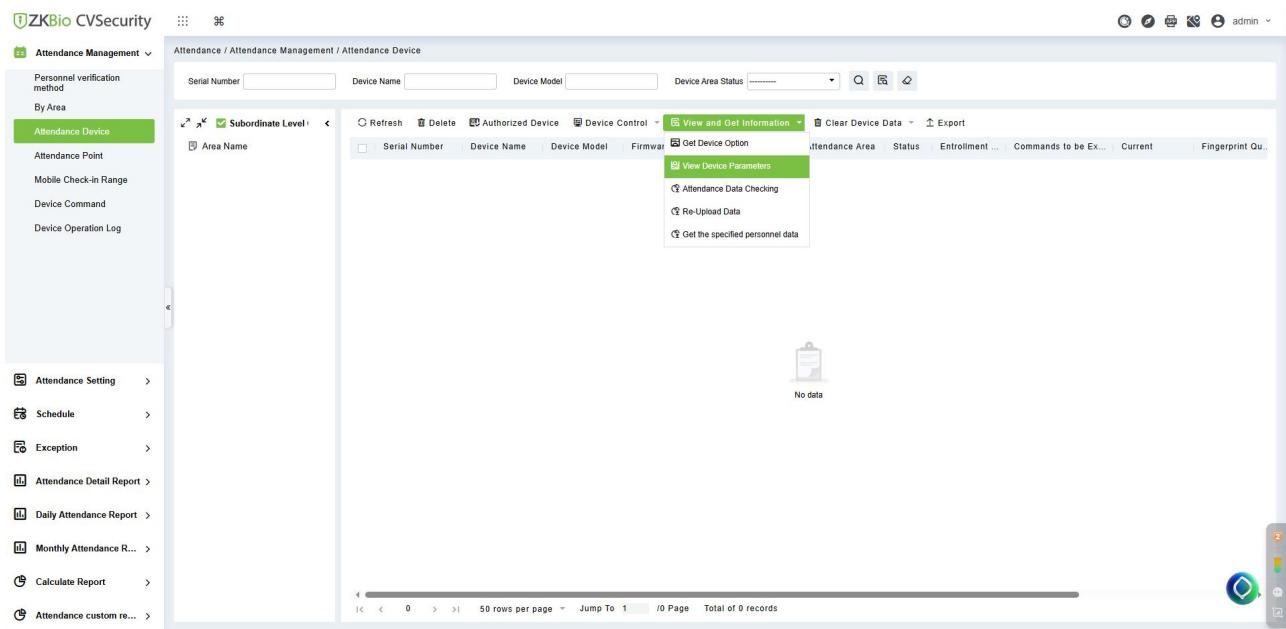
When a user logs into the APP to invite a visitor and selects "Direct Access" as the visitor type, the email content received by the visitor after a successful invitation is shown in the figure below:



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.



ZKBio CVSecurity

Attendance Management / Attendance Device

Attendance / Attendance Management / Attendance Device

Serial Number: [] Device Name: [] Device Model: [] Device Area Status: []

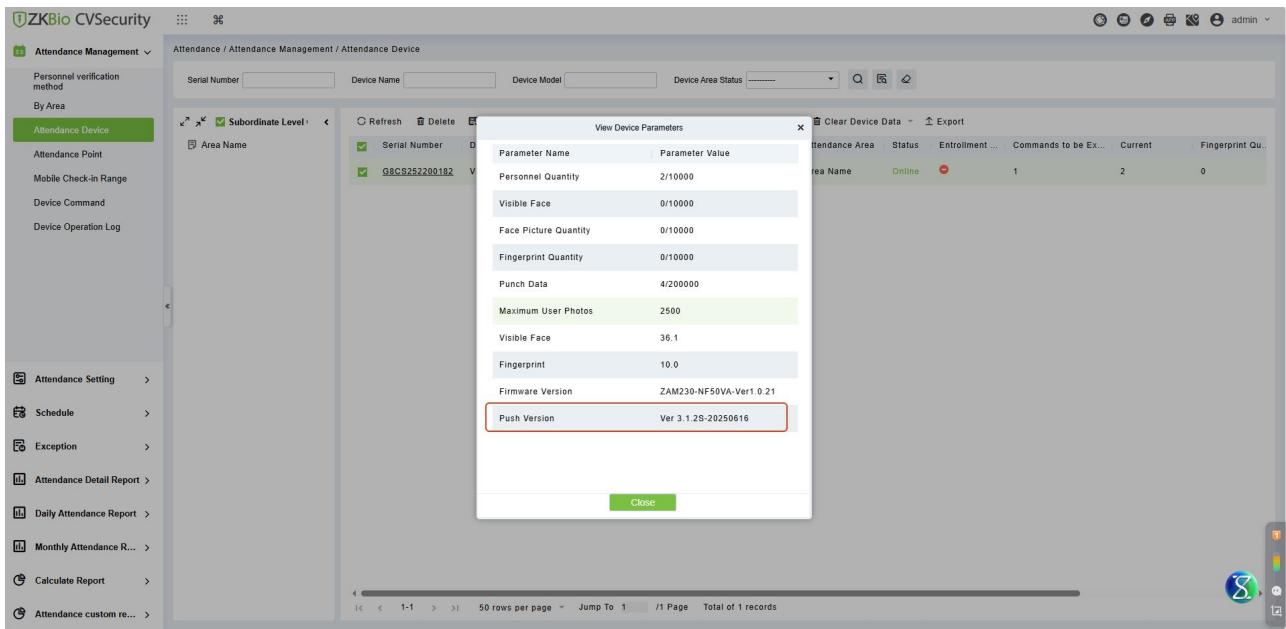
View and Get Information

- View Device Parameters
- Attendance Data Checking
- Re-Upload Data
- Get the specified personnel data

Serial Number	Device Name	Device Model	Firmware
GBCS252200182	GBCS252200182	ZAM230-NF58VA	ZAM230-NF58VA-Ver1.0.21

No data

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



ZKBio CVSecurity

Attendance Management / Attendance Device

Attendance / Attendance Management / Attendance Device

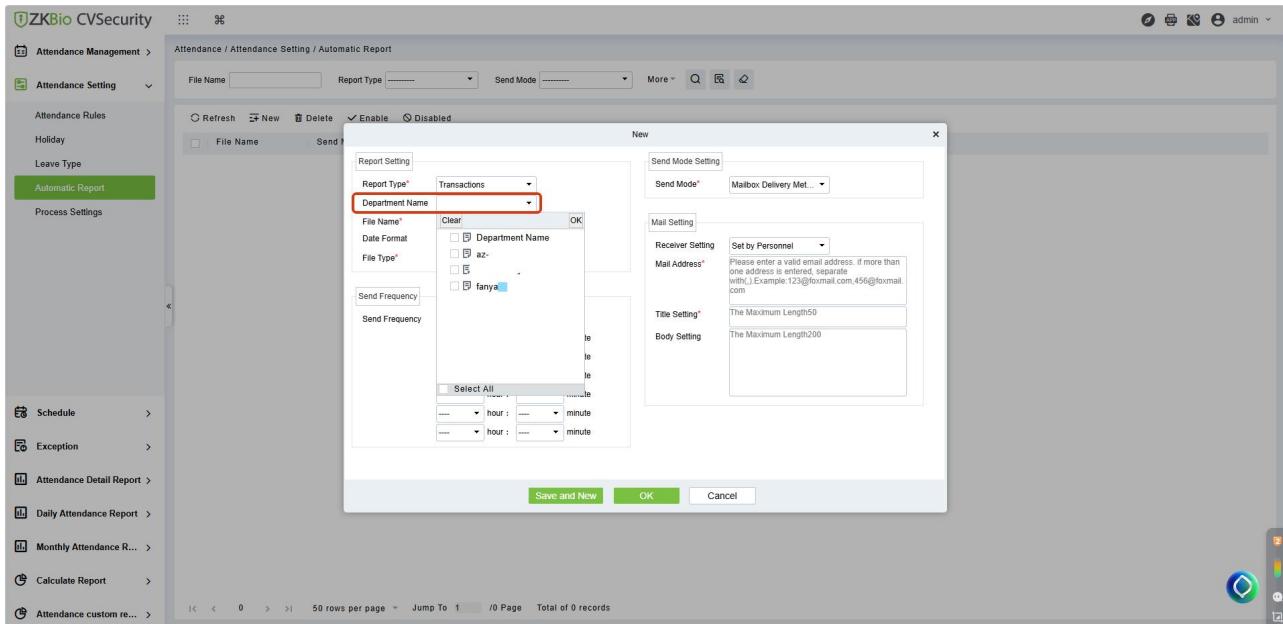
View Device Parameters

Parameter Name	Parameter Value
Personnel Quantity	2/10000
Visible Face	0/10000
Face Picture Quantity	0/10000
Fingerprint Quantity	0/10000
Punch Data	4/200000
Maximum User Photos	2500
Visible Face	36.1
Fingerprint	10.0
Firmware Version	ZAM230-NF58VA-Ver1.0.21
Push Version	Ver 3.1.2S-20250616

Close

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

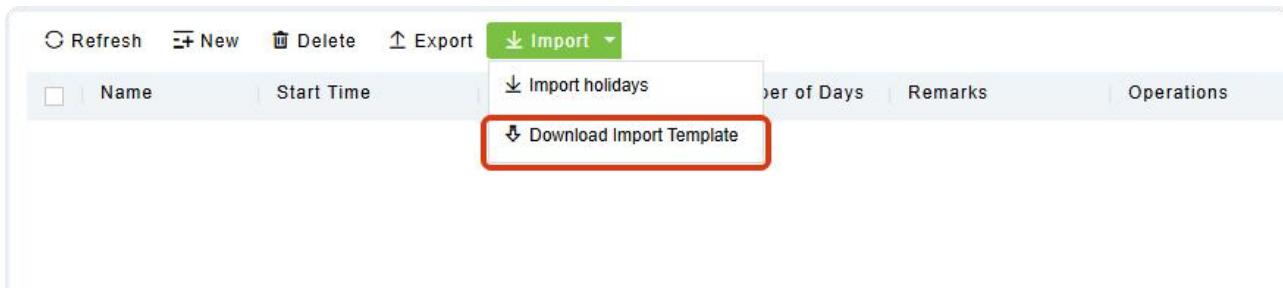
Step: Enter Attendance → Attendance Setting → Automatic Report, click "New", and in the Report Settings column, you can select the department name. After selection, only the attendance records of the selected department will be pushed to the recipients.



- **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.

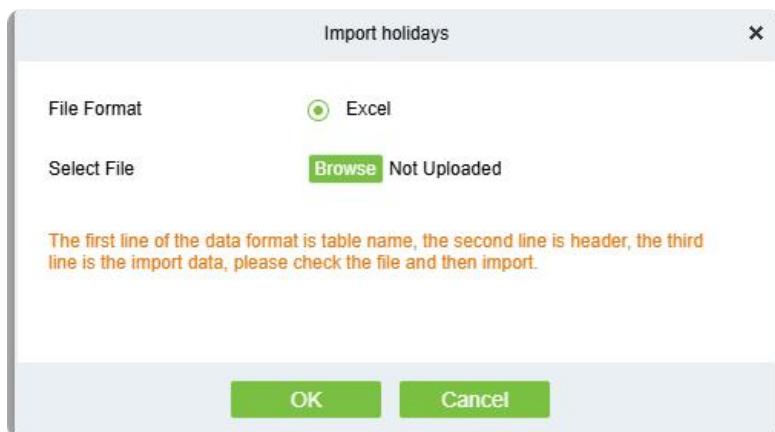
Cells with red triangles contain important annotations—click them to view data entry guidelines.

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.

Import

Import holidays



■ Export:

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

Export

User Password*

File encryption: Yes

File format: EXCEL

Data to Export: All (max 100000 records)

Start Position: 1

Total Records: 100

OK Cancel

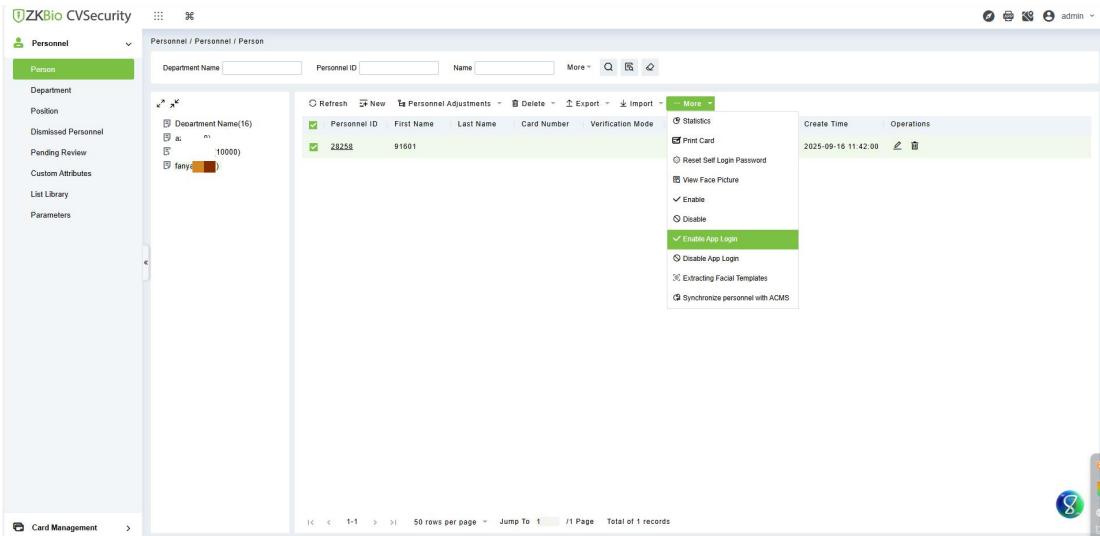
Holiday					
	Name	Start Time	End Time	Number of Days	Remarks
1	holiday1	2025-09-09	2025-09-15	7	

Personnel

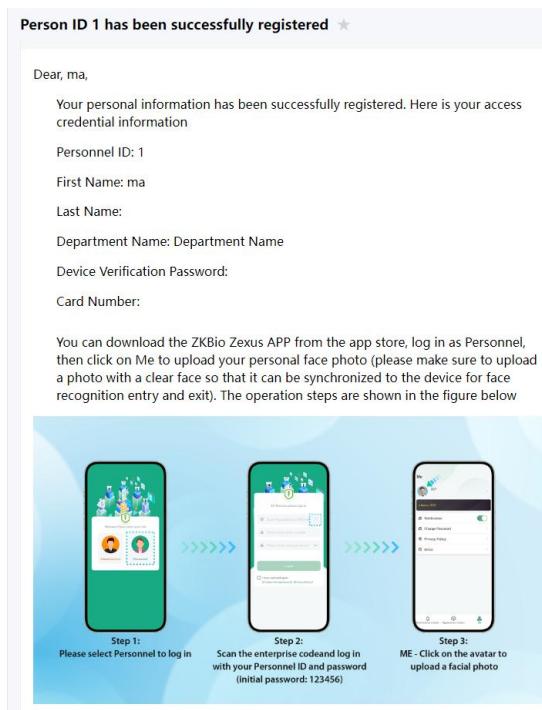
- After selecting personnel, enabling the "APP Log In" feature will automatically send an email to the individual with instructions on how to use the app.

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.



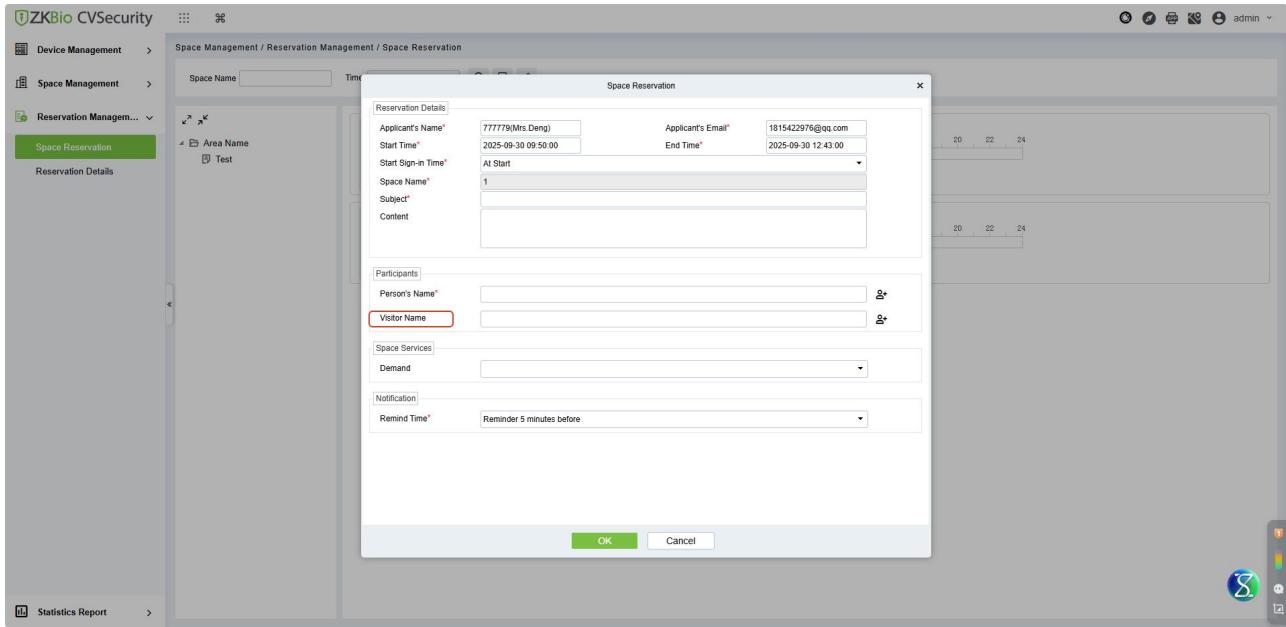
The content of the email notification is as shown in the figure below: The employee can directly follow the guidance in the email to begin using the app login.



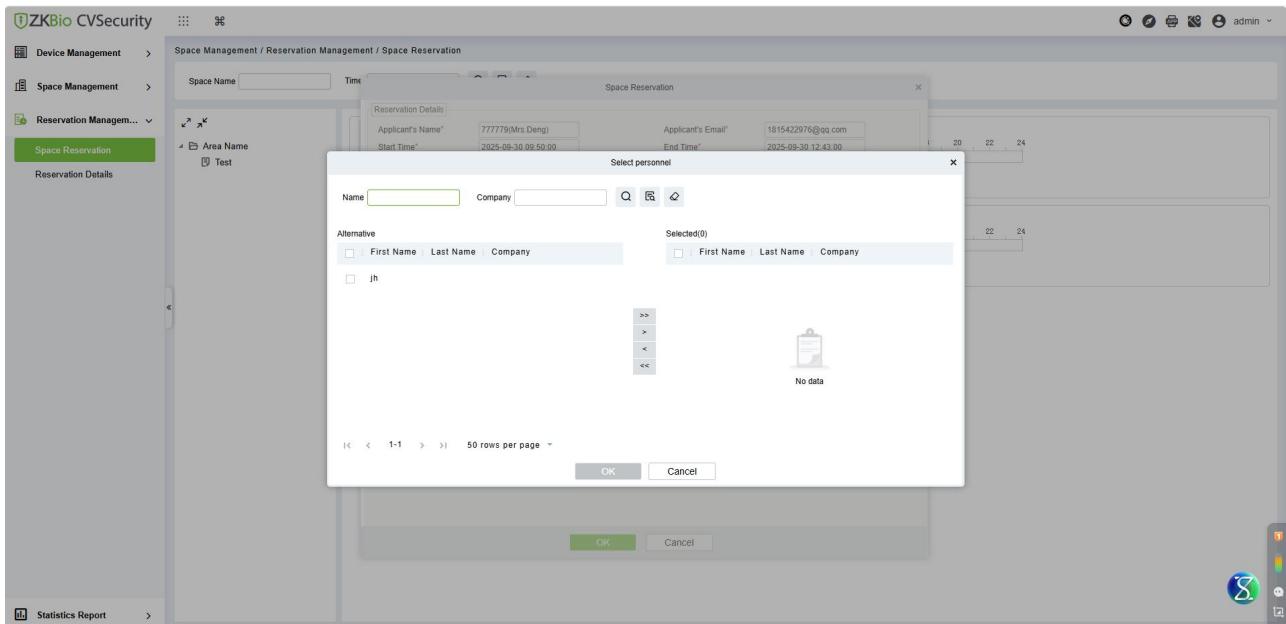
Space Management

- 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 a 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**.

The screenshot shows the Zoom App Marketplace interface. On the left, there's a sidebar with 'Categories' and 'Featured' sections. The 'Categories' section includes links like Analytics, Broadcasting & Streaming, Business System Integrator, CRM, Carrier Provider Exchange, Collaboration, and More. The 'Featured' section includes links like New, App of the Month, Paid Apps, Document Collaboration, Essential Apps, AI Apps, and More. The main area is titled 'Discover apps' and says 'Explore 3,024 apps in Zoom App Marketplace.' It features two main sections: 'App of the Month' (with a purple icon) and 'Paid Apps' (with a purple icon). A dropdown menu in the top right corner is open, showing options: 'Search a published app', 'Develop', 'Manage', 'Build app' (which is highlighted with a red box), 'Documentation', 'Developer blog', and 'Community forum'.

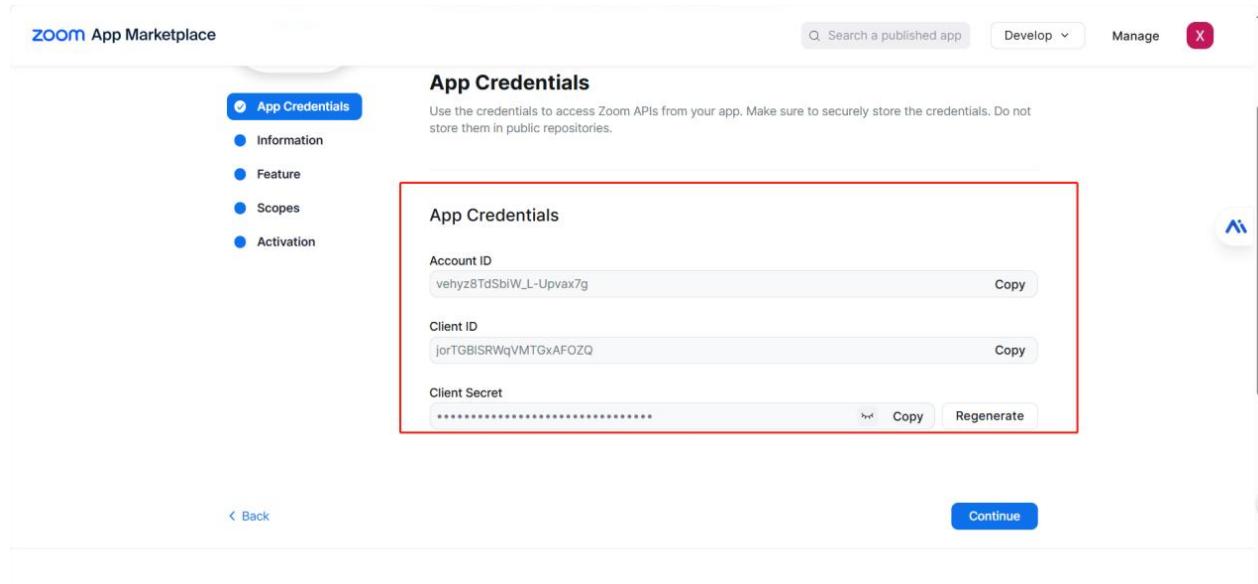
Step2: Select **Server to Server OAuth App** and create App Name.

The screenshot shows a modal dialog box titled 'What kind of app are you creating?'. It contains three options: 'General App', 'Server to Server OAuth App' (which is selected and highlighted with a blue border), and 'Webhook Only App'. Below the options, there is a 'Create' button and a 'Cancel' button. The background of the dialog is dark, matching the overall theme of the Zoom App Marketplace.

Enter the app name.

The screenshot shows a modal dialog box titled 'Create a Server-to-Server OAuth app'. It has a text input field labeled 'App Name' containing the value 'ZKBio CVSecurity2'. There is a character count indicator '17/50' next to the input field. Below the input field are 'Create' and 'Cancel' buttons. The background of the dialog is dark, matching the overall theme of the Zoom App Marketplace.

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



zoom App Marketplace

App Credentials

Use the credentials to access Zoom APIs from your app. Make sure to securely store the credentials. Do not store them in public repositories.

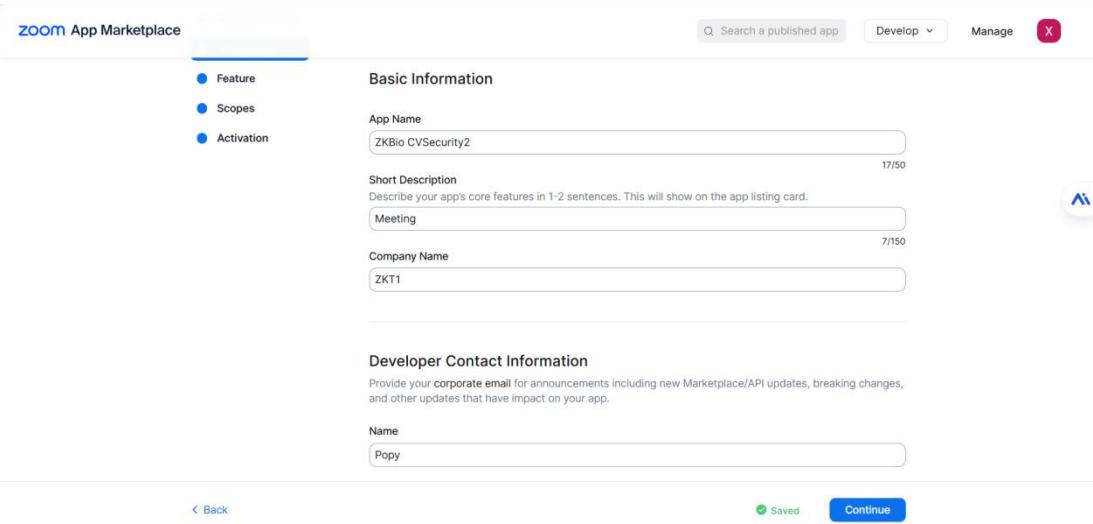
Account ID
velhyz8TdSbiW_L-Upxax7g Copy

Client ID
jorTGBISRwqVMTGxAFOZQ Copy

Client Secret
***** Copy Regenerate

Back Continue

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



zoom App Marketplace

Basic Information

App Name
ZKBio CVSecurity2

Short Description
Describe your app's core features in 1-2 sentences. This will show on the app listing card.
Meeting

Company Name
ZKT1

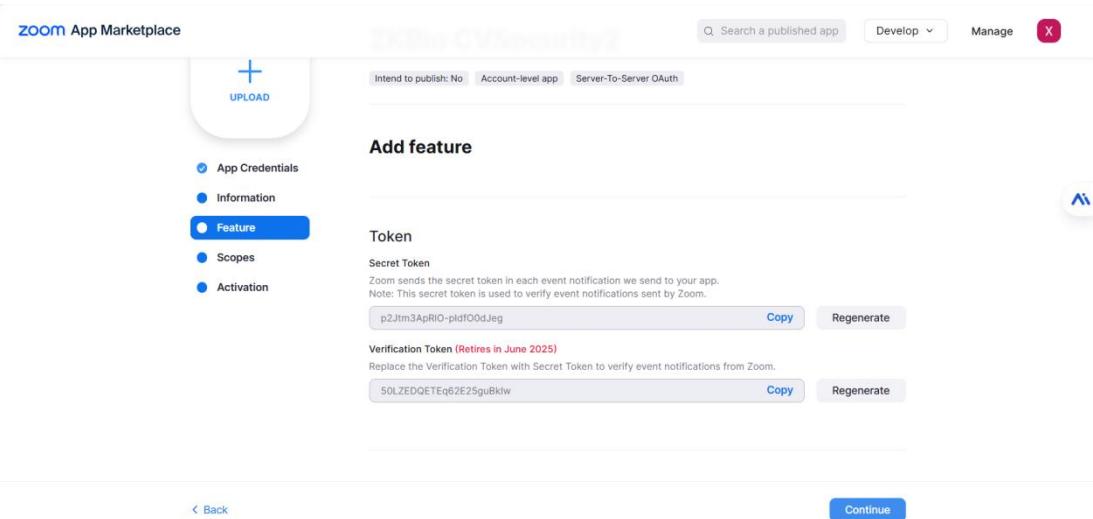
Developer Contact Information

Provide your [corporate email](#) for announcements including new Marketplace/API updates, breaking changes, and other updates that have impact on your app.

Name
Popy

Back Saved Continue

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



zoom App Marketplace

UPLOAD

Intend to publish: No Account-level app Server-To-Server OAuth

Add feature

Feature

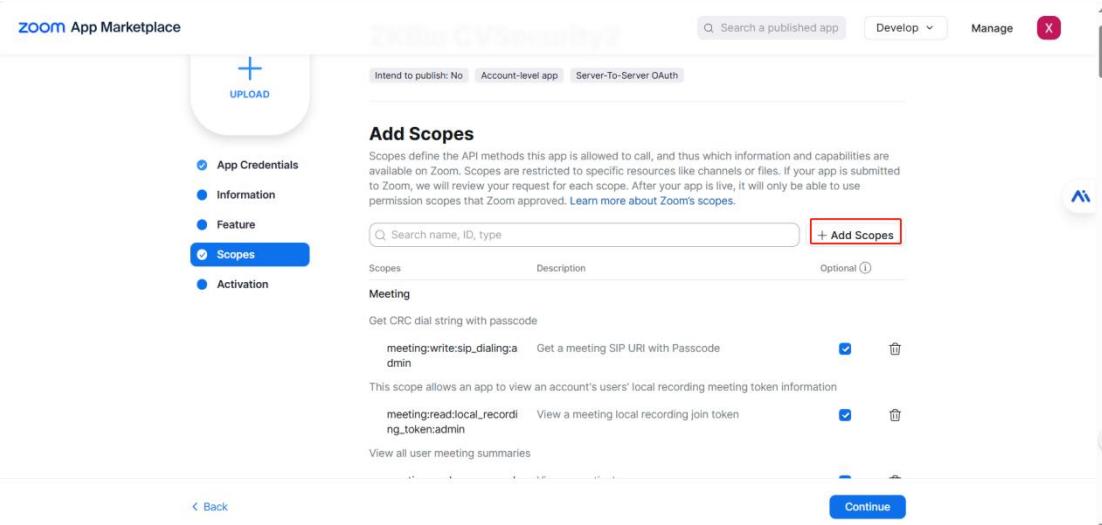
Token

Secret Token
Zoom sends the secret token in each event notification we send to your app.
Note: This secret token is used to verify event notifications sent by Zoom.
p2Jlm3ApRI0-pIdf00dJeg Copy Regenerate

Verification Token (Retires in June 2025)
Replace the Verification Token with Secret Token to verify event notifications from Zoom.
50LZEDQETEq62E25guBkiw Copy Regenerate

Back Continue

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



zoom App Marketplace

UPLOAD

Add Scopes

Intend to publish: No Account-level app Server-To-Server OAuth

Scopes Description Optional

Meeting

Get CRC dial string with passcode

meeting:write:sip_dialing:a Get a meeting SIP URI with Passcode

This scope allows an app to view an account's users' local recording meeting token information

meeting:read:local_record View a meeting local recording join token

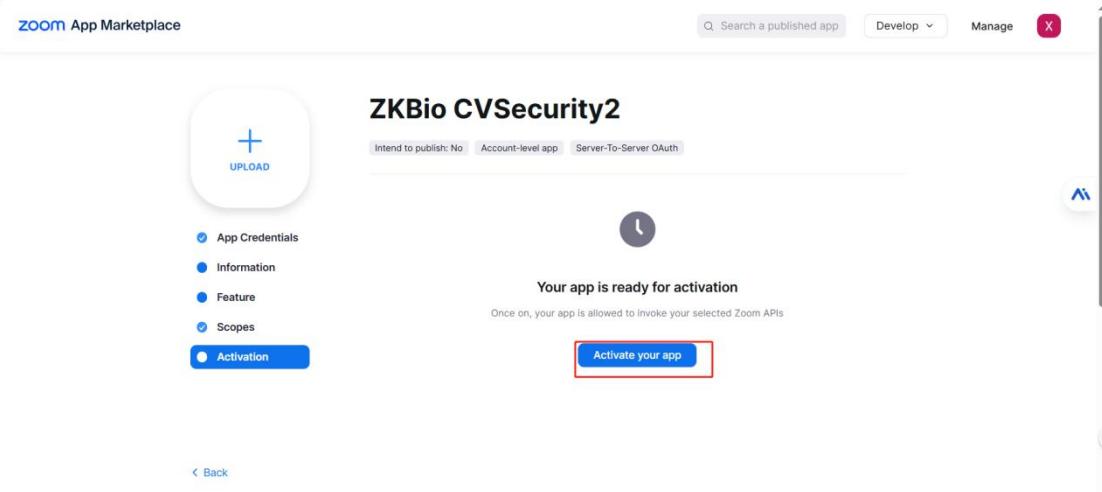
ng_token:admin

View all user meeting summaries

Search name, ID, type + Add Scopes

Continue

Step7: Then click "Activate your app".



zoom App Marketplace

UPLOAD

ZKBio CVSecurity2

Intend to publish: No Account-level app Server-To-Server OAuth

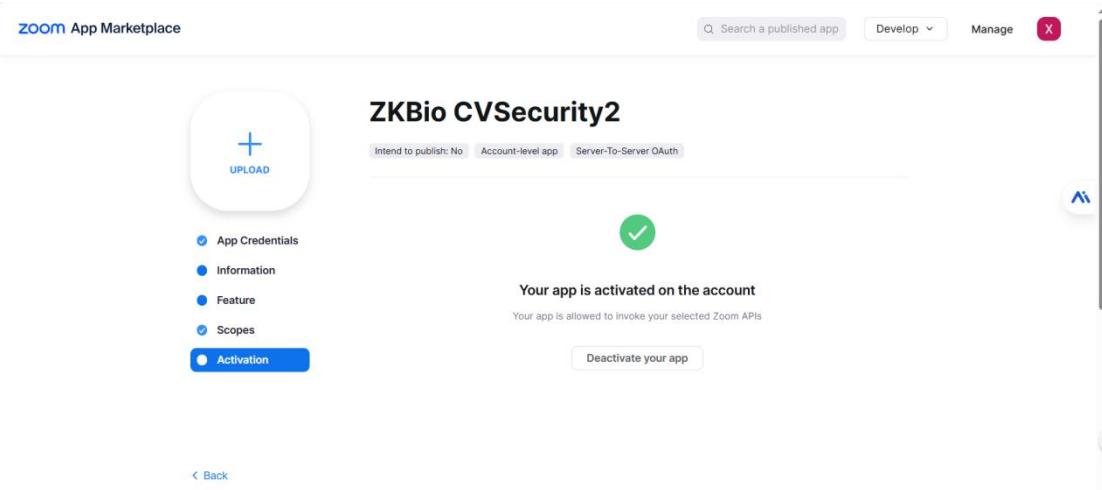
Your app is ready for activation

Once on, your app is allowed to invoke your selected Zoom APIs

Activate your app

Back

Until the display activation is successful.



zoom App Marketplace

UPLOAD

ZKBio CVSecurity2

Intend to publish: No Account-level app Server-To-Server OAuth

Your app is activated on the account

Your app is allowed to invoke your selected Zoom APIs

Deactivate your app

Back

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.

Zoom App Marketplace

App Credentials

Information

Feature

Scopes

Activation

Account ID: `vehyz8TdSbW_L-Upvax7g` [Copy](#)

Client ID: `jorTGBISRWqVMTGxAFOZQ` [Copy](#)

Client Secret: `3LgQVuSTvfoH5TXui0tq4` [Copy](#) [Regenerate](#)

Back [Continue](#)

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

System Management

Authority Management

Communication Management

Third Party Integration

Middle Table

LED Device

Connector

Video Channel

Digifort Camera

AD Management

SMS Management

WhatsApp

ACMS

ZOOM

Name: [Search](#) [Delete](#)

[Refresh](#) [New](#) [Delete](#)

New

Name*:

Description:

Connection Configuration

User Email*:

Account Id*:

Client Id*:

Client Secret*:

[OK](#) [Cancel](#)

50 rows per page [Jump To](#) 1 /1 Page Total of 2 records

Click "OK" to return Operation Succeed.

System Management

Authority Management

Communication Management

Third Party Integration

Middle Table

LED Device

Connector

Video Channel

Digifort Camera

AD Management

SMS Management

WhatsApp

ACMS

ZOOM

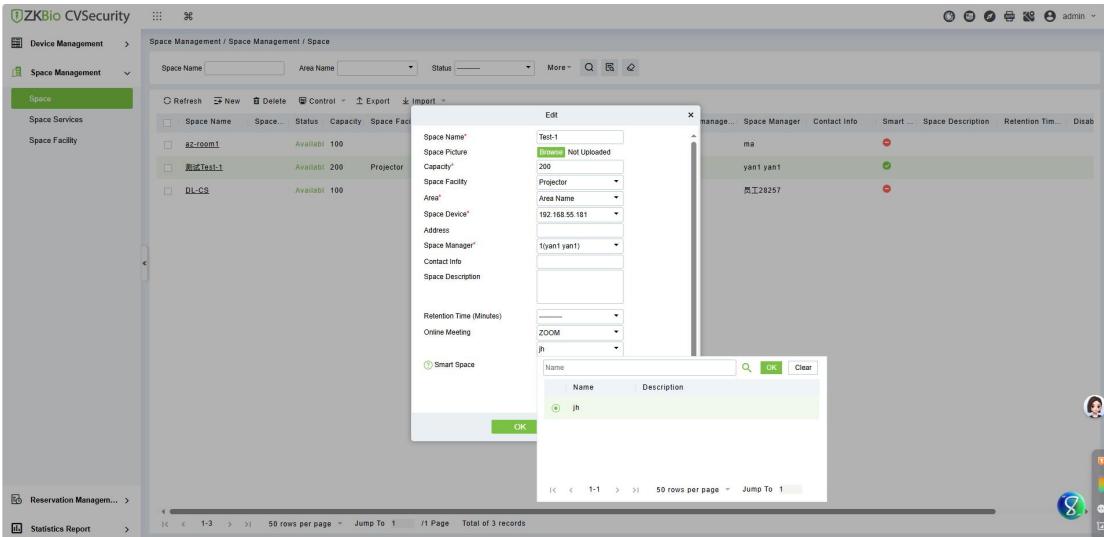
Name: [Search](#) [Delete](#)

[Refresh](#) [New](#) [Delete](#) Enable Disable

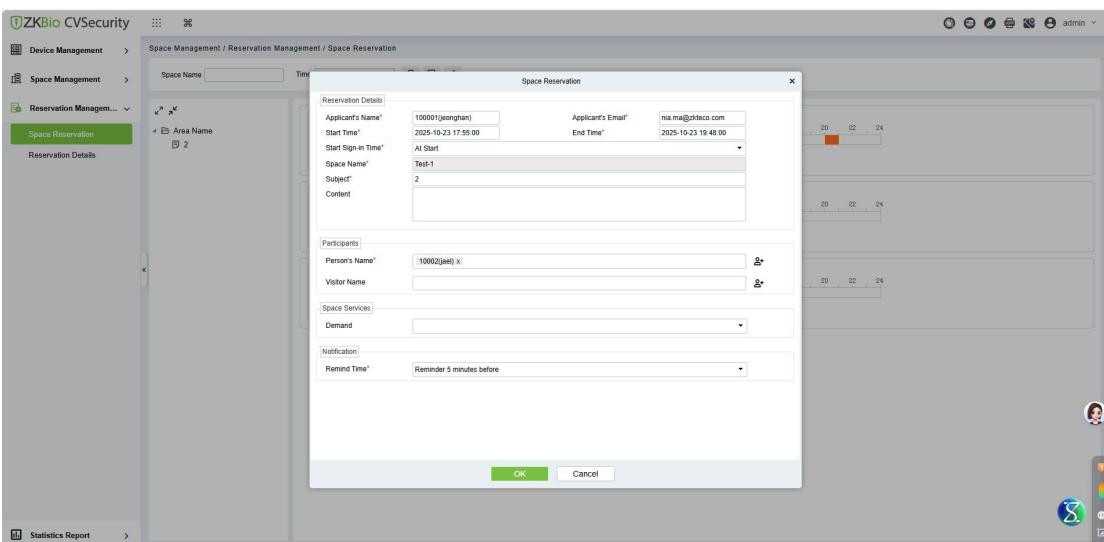
Name	Enable	Description	Operations
Popy2			
Popy			
Zoom123			

50 rows per page [Jump To](#) 1 /1 Page Total of 3 records

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.

Space Service Reminder 8 | ★

ZKBioCV Demo

收件人: Popy

刚刚 详情

Hi

Popy has applied for zoom1 and it is about to start. Here are the topic details:

Subject: zoom1

Content:

Reserved Time: 2025-06-18 15:34:00 - 2025-06-18 16:29:00

Space: Testing Space-66-123

Address:

Applicant: Popy

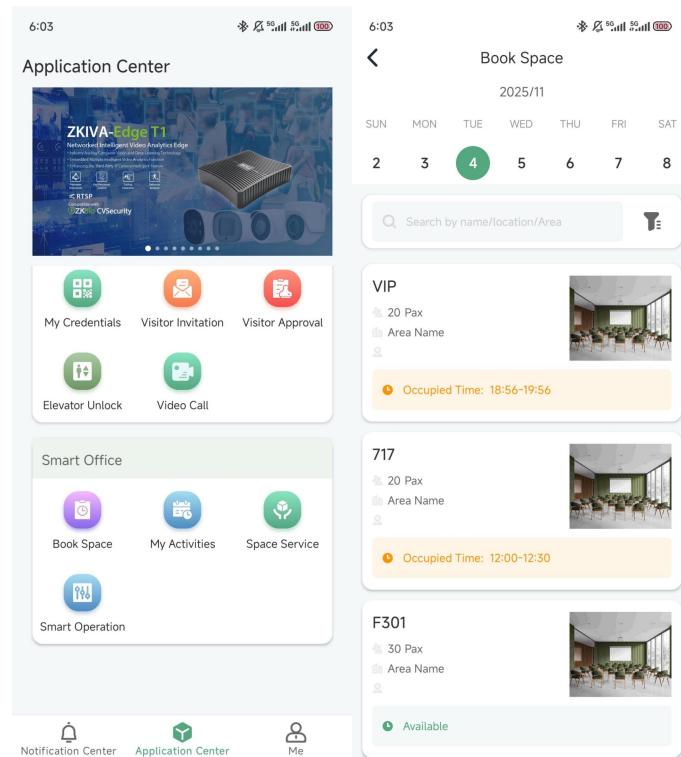
ZOOM Meeting Link: <https://us05web.zoom.us/j/86925284727?pwd=ked3bGKDPRvGZAufQE3YacENzaCt2f1>

Meeting ID: 86925284727

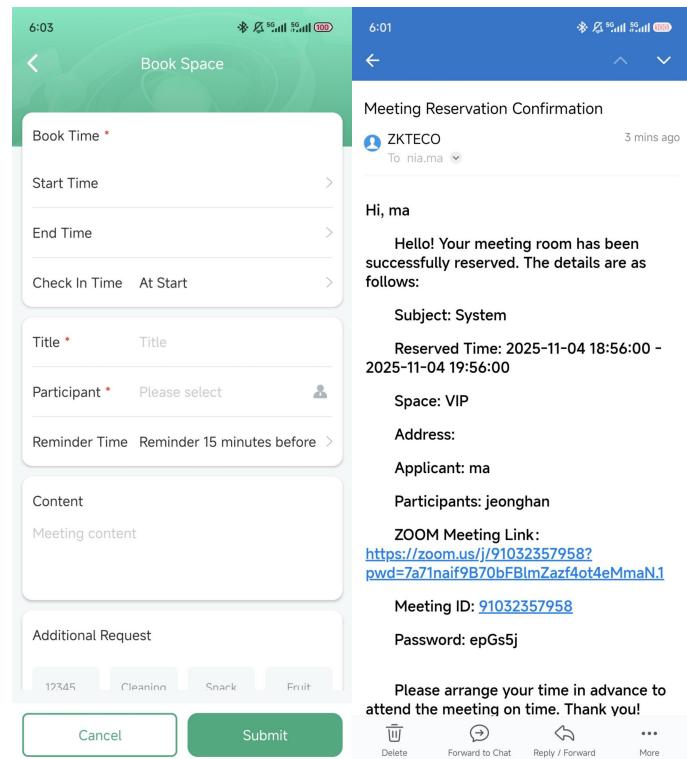
Password: w808aF

Please participate in time, thank you.

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.

System Management > System / Third Party Integration / Microsoft 365

Third Party Integration > Microsoft 365

Parameters

Auto Sync Frequency
Auto Sync Frequency for Microsoft 365 Calendar Events*
10 second(5-120)

Connection Parameter Settings
Tenant ID*
Application ID*

Buttons: Test Connection, Download Certificate

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

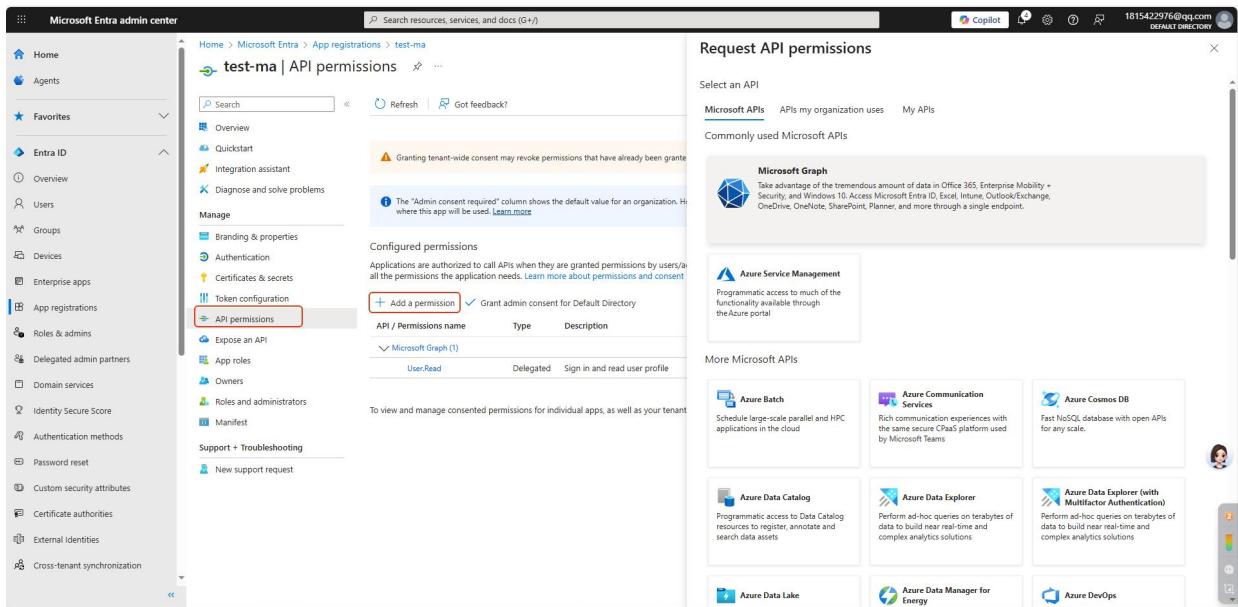
Step3: Enter Overview and click "Add a certificate or secret".

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

Thumbprint	Description	Start date	Expires
zkroot	Upload Completed for zk.root.crt	1.3 KB "Streaming upload"	Never

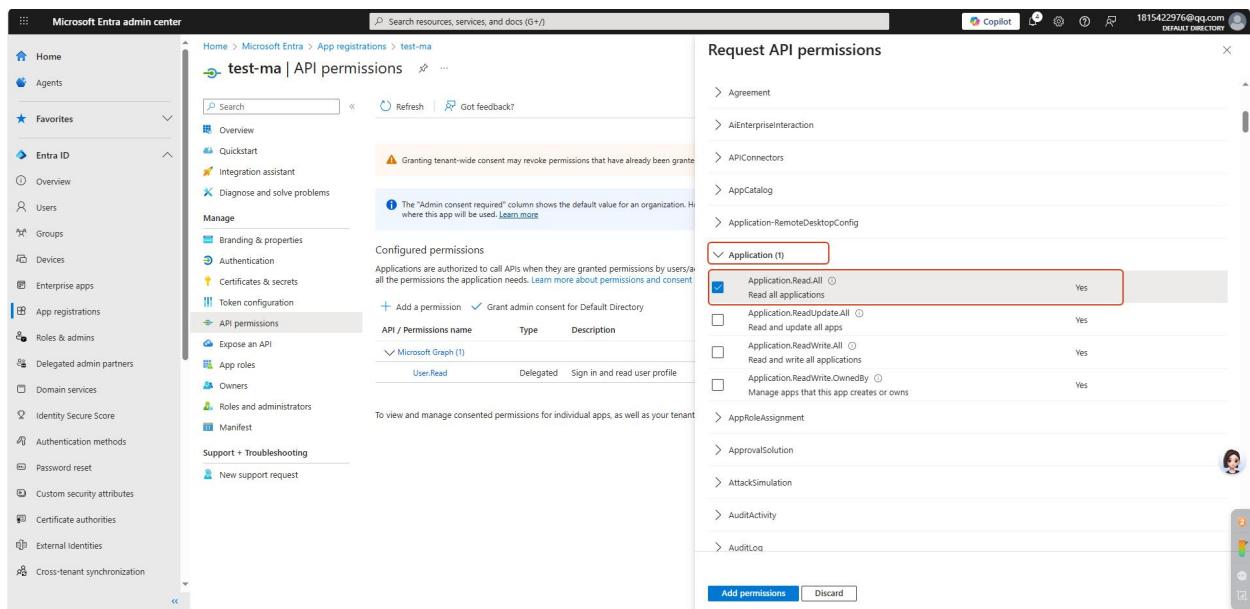
Step4: Enter Expose an API and click "Add" next to Application ID URI.

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



The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External identities, and Cross-tenant synchronization. The main content area is titled 'test-ma | API permissions'. It shows a search bar, a refresh button, and a 'Got feedback?' link. A warning message states: 'Granting tenant-wide consent may revoke permissions that have already been granted'. Below this, a note says: 'The "Admin consent required" column shows the default value for an organization. Here where this app will be used.' A 'Learn more' link is provided. The 'Configured permissions' section is visible, with a note: 'Applications are authorized to call APIs when they are granted permissions by users/admins or all the permissions the application needs. Learn more about permissions and consent'. A red box highlights the 'Add a permission' button. The 'Request API permissions' panel on the right lists 'Microsoft APIs', 'APIs my organization uses', and 'My APIs'. It features a section for 'Commonly used Microsoft APIs' with 'Microsoft Graph' (selected), 'Azure Service Management', and 'More Microsoft APIs' including 'Azure Batch', 'Azure Communication Services', 'Azure Cosmos DB', 'Azure Data Catalog', 'Azure Data Explorer', 'Azure Data Explorer (with Multifactor Authentication)', 'Azure Data Lake', 'Azure Data Manager for Energy', and 'Azure DevOps'.

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



The screenshot shows the 'Request API permissions' panel from the previous step. The 'Application (1)' section is expanded, showing the 'Application.Read.All' permission selected with a checked checkbox. A red box highlights this checkbox. Other options like 'Read all applications' and 'Read and update all apps' are also listed. The 'Add permissions' and 'Discard' buttons are at the bottom. The left side of the screen shows the same 'test-ma | API permissions' page as the previous screenshot.

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

Request API permissions

Microsoft Graph

Application permissions

Place

Place.Read.All

Add permissions

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

Request API permissions

Calendars

Calendars.Read

Calendars.ReadBasic.All

Calendars.ReadWrite

Add permissions

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

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is filled with various administrative options like Home, Agents, Favorites, and App registrations. The main content area is titled 'test-ma | API permissions'. It displays a table of configured permissions for the Microsoft Graph API. The 'Grant admin consent for Default Directory' button is highlighted with a red box. The table includes columns for API / Permissions name, Type, Description, Admin consent req..., and Status. Most permissions have 'Not granted for Default...' status.

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.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is filled with various administrative options like Home, Agents, Favorites, and App registrations. The main content area is titled 'test-ma'. The 'Essentials' section is expanded, showing the application's display name, client credentials, redirect URLs, and application ID URI. The 'Application (client) ID' is highlighted with a red box. The 'Object ID' and 'Directory (tenant) ID' are also highlighted with red boxes. Below the essentials, there are sections for 'Get Started', 'Documentation', and 'Build your application with the Microsoft identity platform'. The 'Call APIs', 'Sign in users in 5 minutes', and 'Configure for your organization' sections are also visible.

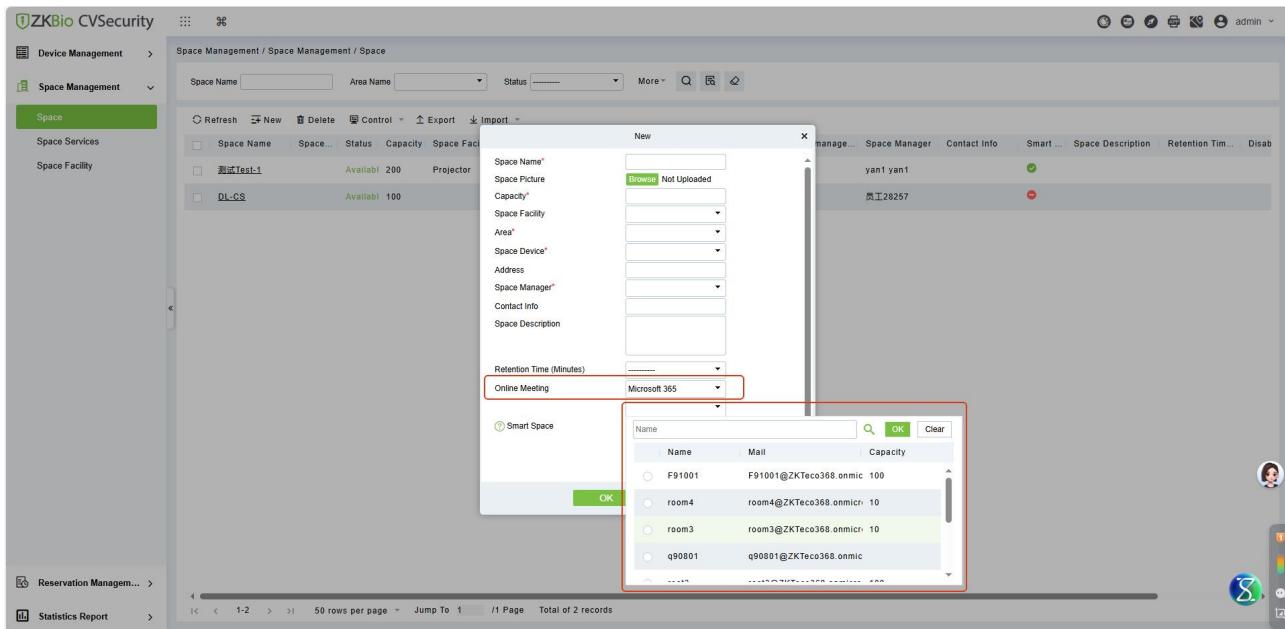
Step8: Click "Test Connection".

2. Add Meeting Room:

Step1: Enter the [Microsoft 365 admin center](#) platform, click Resources → Meeting Rooms & Equipment

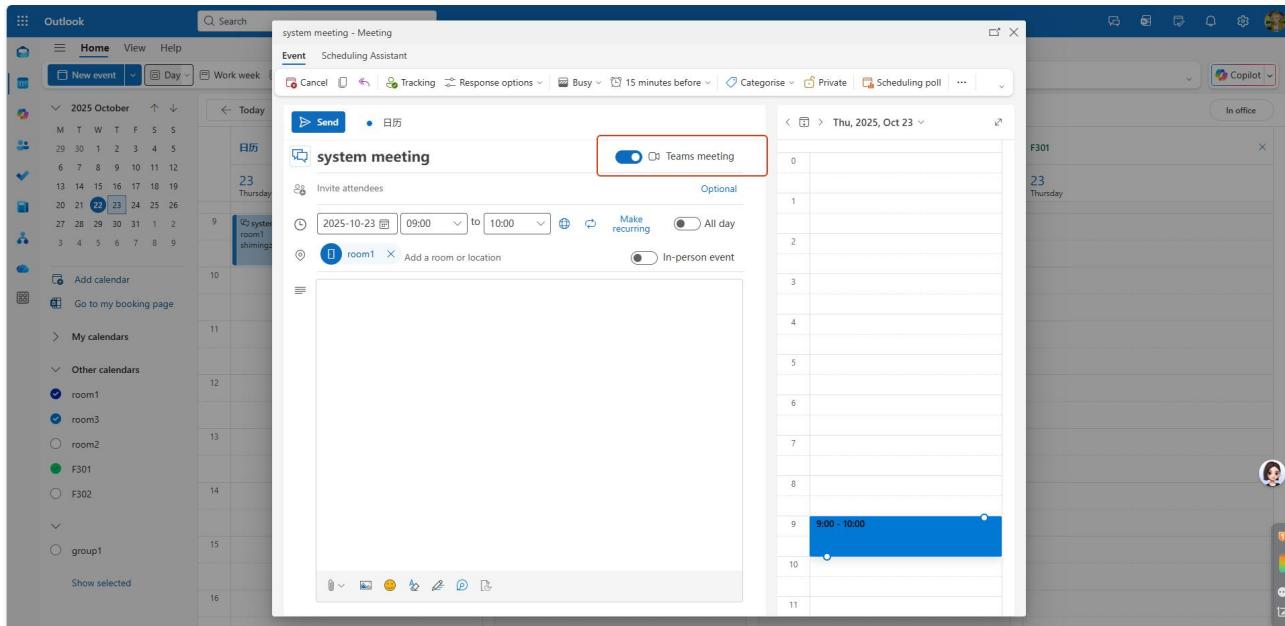
→ Add Resource.

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.

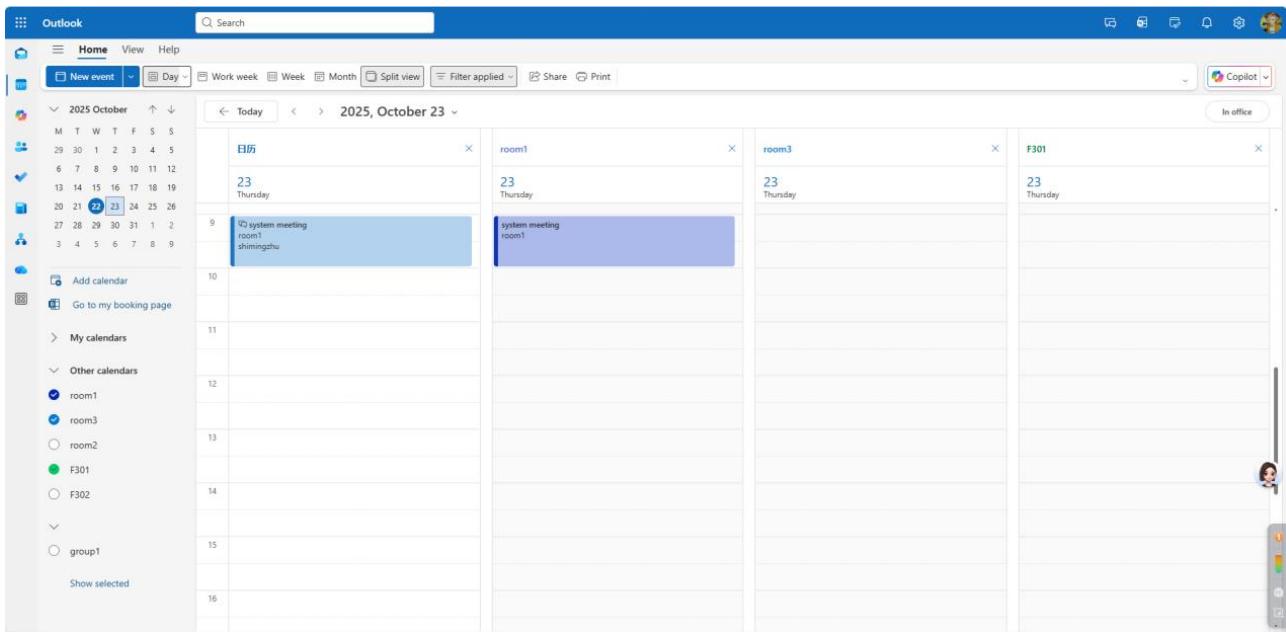


3. Sync Microsoft 365 events:

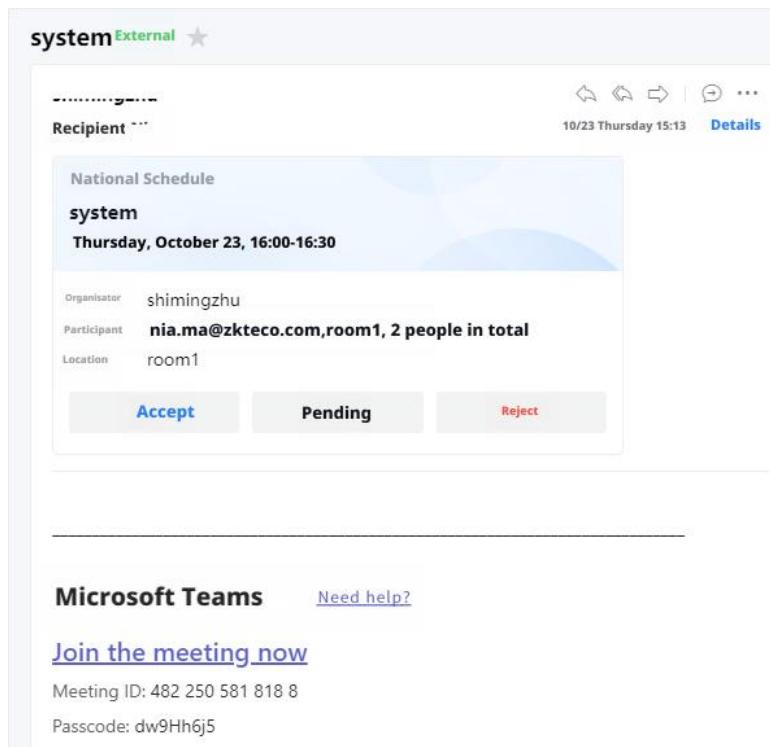
Step1: Create a new event on the [Outlook](#) platform. Access the [Calendar] configuration page, select the required meeting schedule time range, expand the advanced configuration options, complete the schedule creation, and send it.



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

ZKBio CVSecurity

Device Management >

Space Management >

Reservation Management >

Space Reservation

Reservation Details

Space Management / Reservation Management / Reservation Details

Time From: 2025-09-09 00:00:00 To: 2025-12-09 23:59:59 Status: ----- More > Search Filter

Sync Microsoft 365 Events

Subject	Reserved S...	Area Name	Address	Start Sign-in Time	Start Time	End Time	Applicant	Applicant Dep...
aaaa	1	Area Name		2025-10-09 15:08:00	2025-10-09 15:08:00	2025-10-09 15:16:00	33333335(33333335)	ccy
2	A	Area Name		2025-09-30 16:57:00	2025-09-30 16:57:00	2025-09-30 20:50:00	7777777(nia)	hybe
1	1	Area Name		2025-09-30 16:55:00	2025-09-30 16:55:00	2025-09-30 18:52:00	7777777(nia)	hybe
空间AI助手临时会	A	Area Name		2025-10-01 08:30:00	2025-10-01 09:00:00	2025-10-01 10:00:00	1(firstname1 lastname1)	一万人部门
test	A	Area Name		2025-09-26 17:55:00	2025-09-26 17:55:00	2025-09-26 18:05:00	10083(first10083 lastname10083)	100人
11	A	Area Name		2025-09-26 14:50:00	2025-09-26 14:50:00	2025-09-26 14:59:00	777779(Ms.Deng)	hybe
test12	A	Area Name		2025-09-22 13:42:00	2025-09-22 13:42:00	2025-09-22 13:43:24	668(lastname668)	Department Name
TEST	A	Area Name		2025-09-22 11:57:00	2025-09-22 11:57:00	2025-09-22 11:58:02	668(lastname668)	Department Name

50 rows per page Jump To 1 / Page Total of 8 records

ZKBio CVSecurity

Device Management >

Space Management >

Reservation Management >

Space Reservation

Reservation Details

Space Management / Reservation Management / Reservation Details

Time From: 2025-09-22 00:00:00 To: 2025-12-22 23:59:59 Status: ----- More > Search Filter

Sync Microsoft 365 Events

Reservation Details

Edit

Department	Space Services	Operator	Status	Operations
admin	To Begin			
admin	To Begin			
admin	To Begin			
it Name	员工28256	Ended		
it Name	员工28257	Ended		
it Name	yan2	Ended		
it Name	yan2	Ended		
it Name	yan3	Ended		
it Name	yan1 yan1	Ended		
it Name	yan2	Ended		
it Name	yan1 yan1	Ended		
it Name	员工28256	Ended		
it Name	员工28257	Ended		
it Name	员工28256	Ended		
it Name	yan1 yan1	Ended		

Participants

Space Services

Online Meeting

Notification

OK Cancel

50 rows per page Jump To 1 / Page Total of 17 records

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

System Management > System / Third Party Integration / Microsoft 365

Authority Management > Parameters

Communication Mana... >

Third Party Integration > Parameters

Middle Table

LED Device

Connector

Video Channel

Digital Camera

AD Management

SMS Management

WhatsApp

ACMS

ZOOM

Microsoft 365

Auto Sync Frequency

Auto Sync Frequency for Microsoft 365 Calendar Events*

10 second(s)(5-120)

Connection Parameter Settings

Tenant ID*

Application ID*

Test Connection Download Certificate

OK

Parameters

admin

Profile icon

Notification icon (1)

Search icon

Logout icon

Left sidebar: Microsoft 365

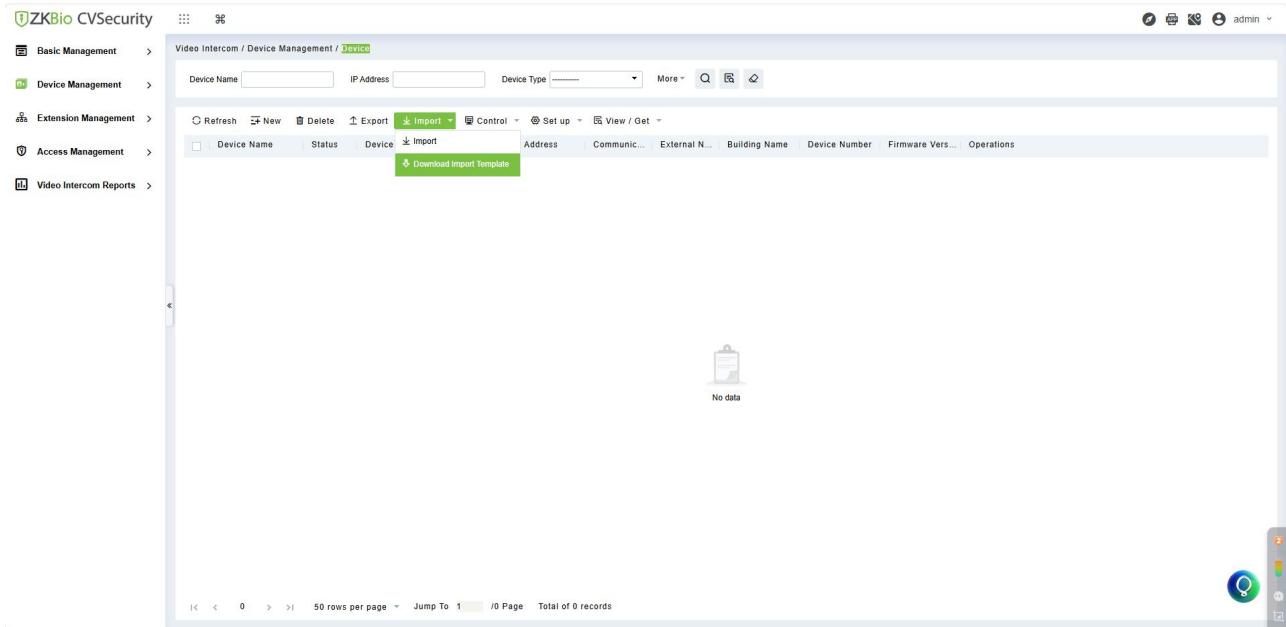
Bottom navigation: Data Integration

Right sidebar: Microsoft 365 parameters

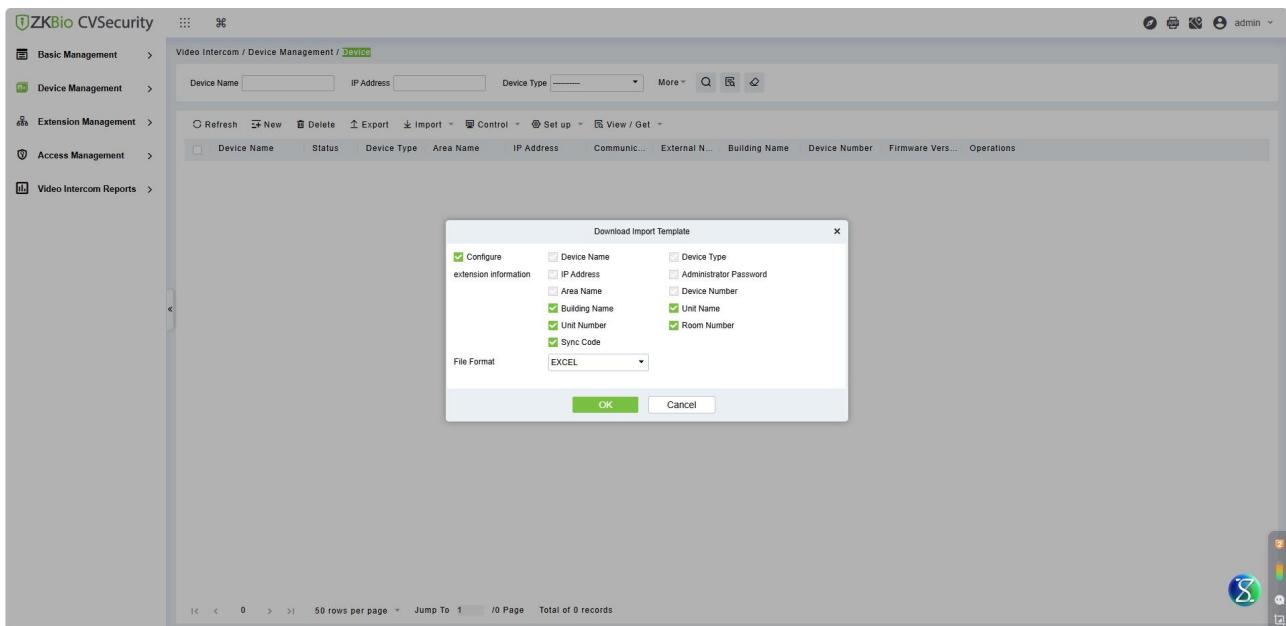
Video Intercom

- **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.

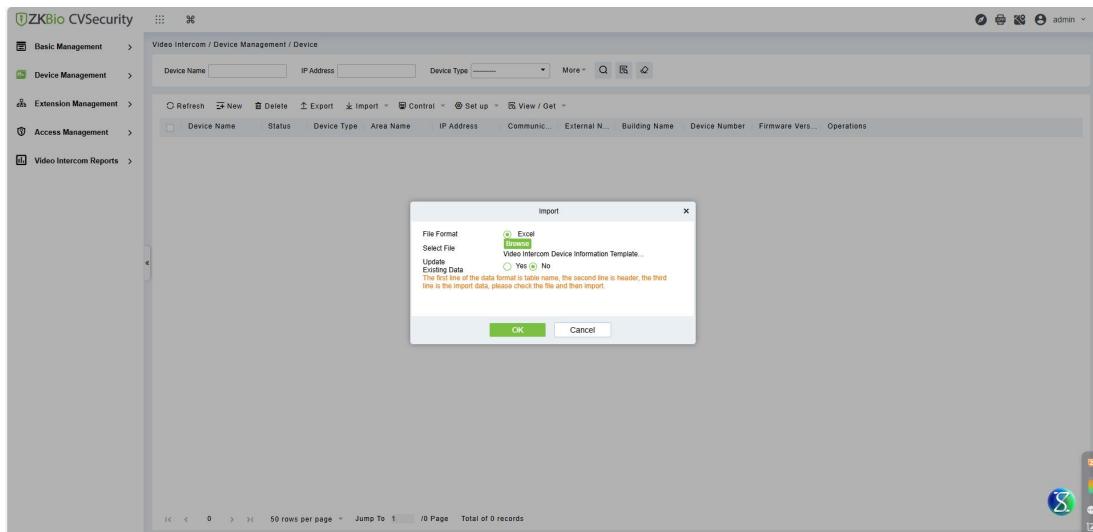


Step3: Fill in the required content according to the instructions in the import template and save it.

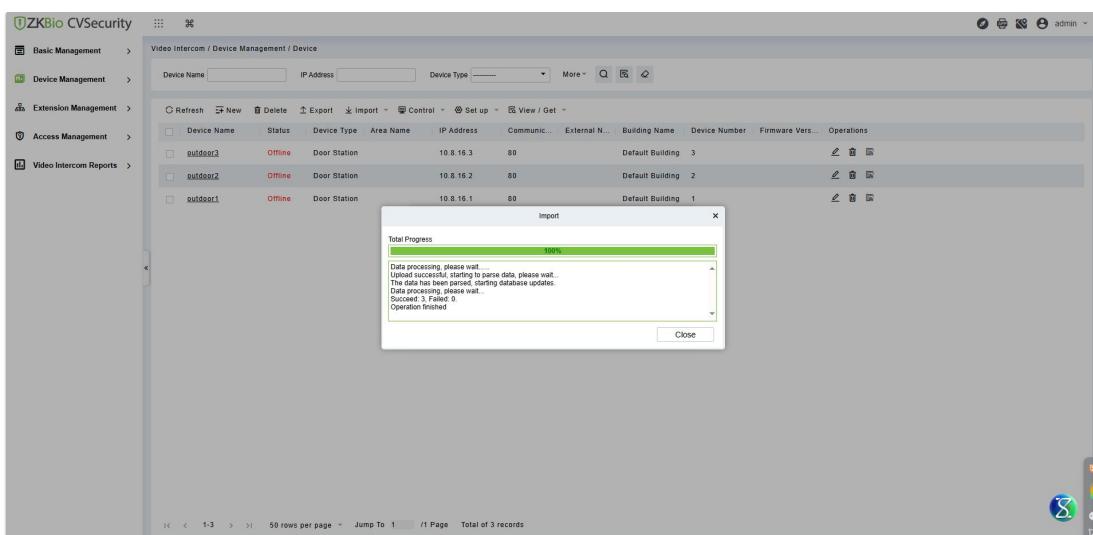
Note: Before entering data in the template, review the cell comments for formatting requirements. Cells with red triangles contain important annotations—click them to view data entry guidelines.

Video Intercom Device Information Template										
Device Name	Device Type	IP Address	Administrator Password	Area Name	Device Number	Building Name	Unit Name	Unit Number	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

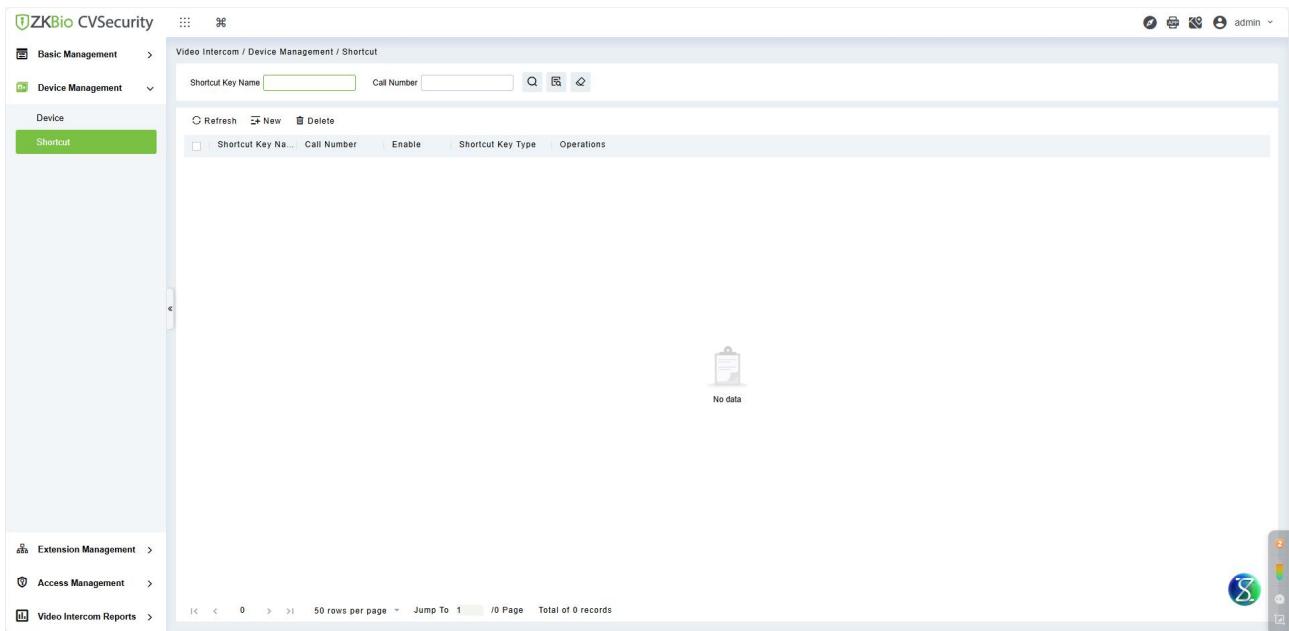


The import status is shown in the figure below. You can view the number of successful imports until the operation is complete, and the imported devices will be displayed in the list.



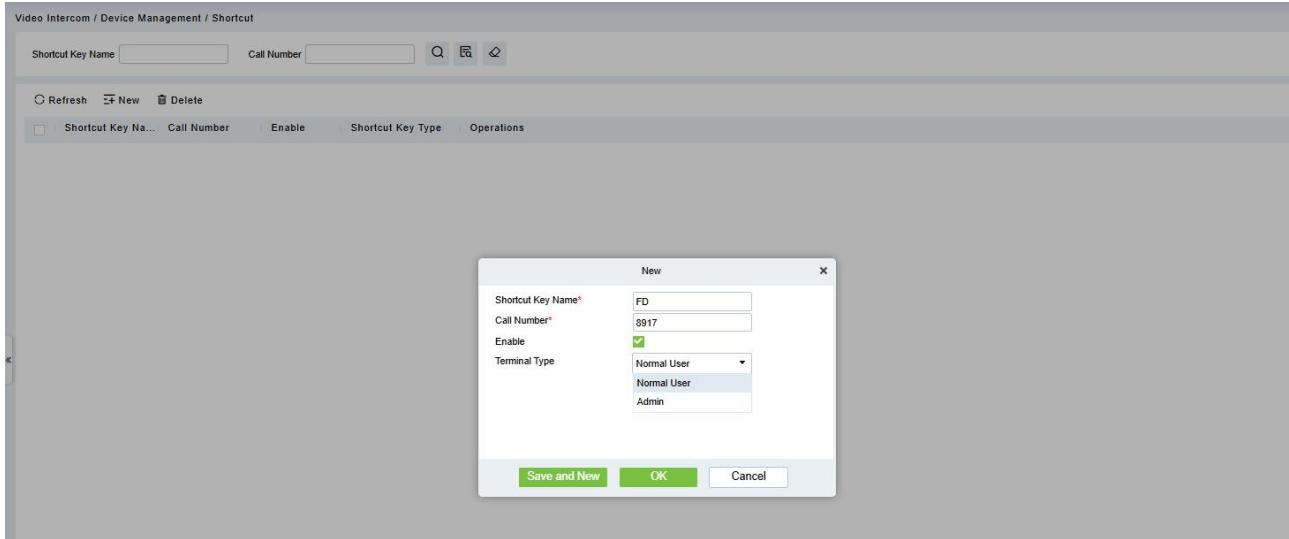
- The shortcut menu has been moved under the Device Management menu.

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

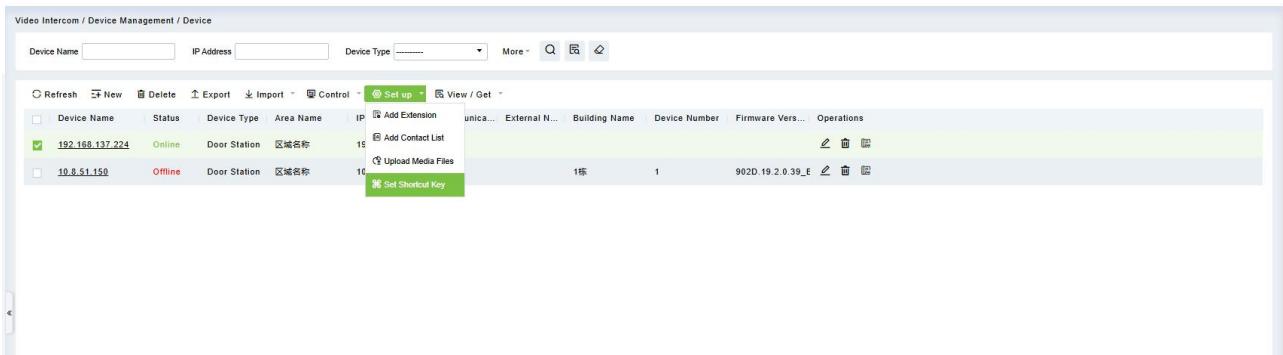


Note: Currently, this function only supports ZKTECO access control devices and does not support DNK devices.

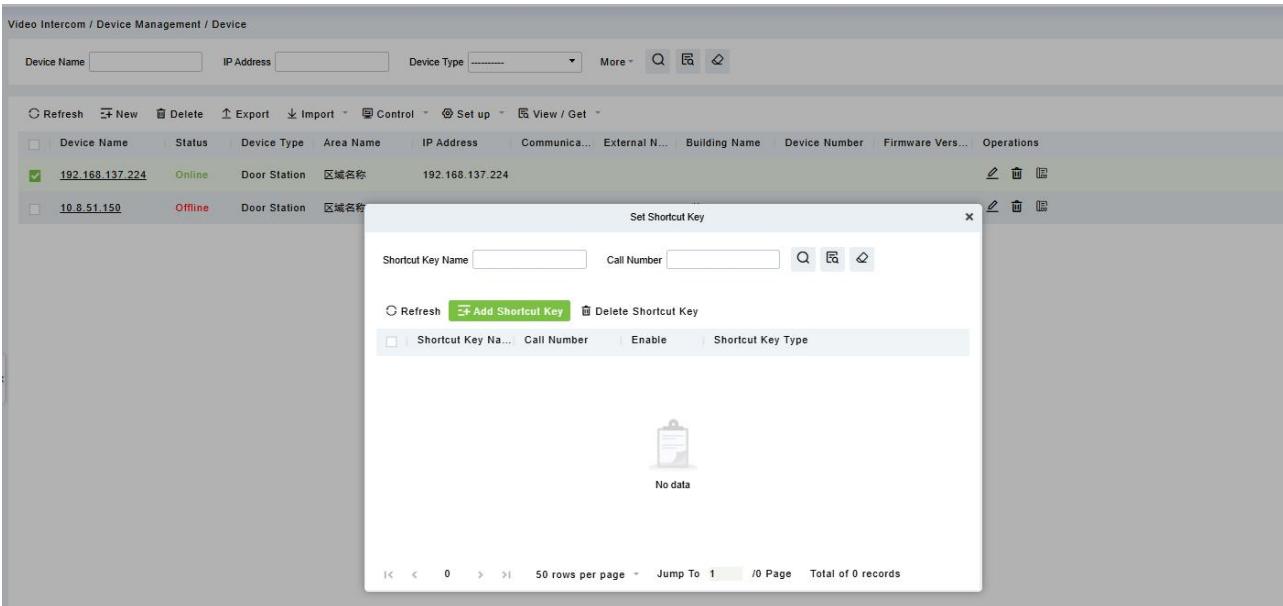
Step1: Click "New", fill in the Shortcut Key Name and the Call Number (if the SIP Service Mode is Cloud Sip, fill in the sip account; if the SIP Service Mode is Local IPPBX, fill in the extension number), check whether to enable it, and select the binding type as Normal user or Admin.



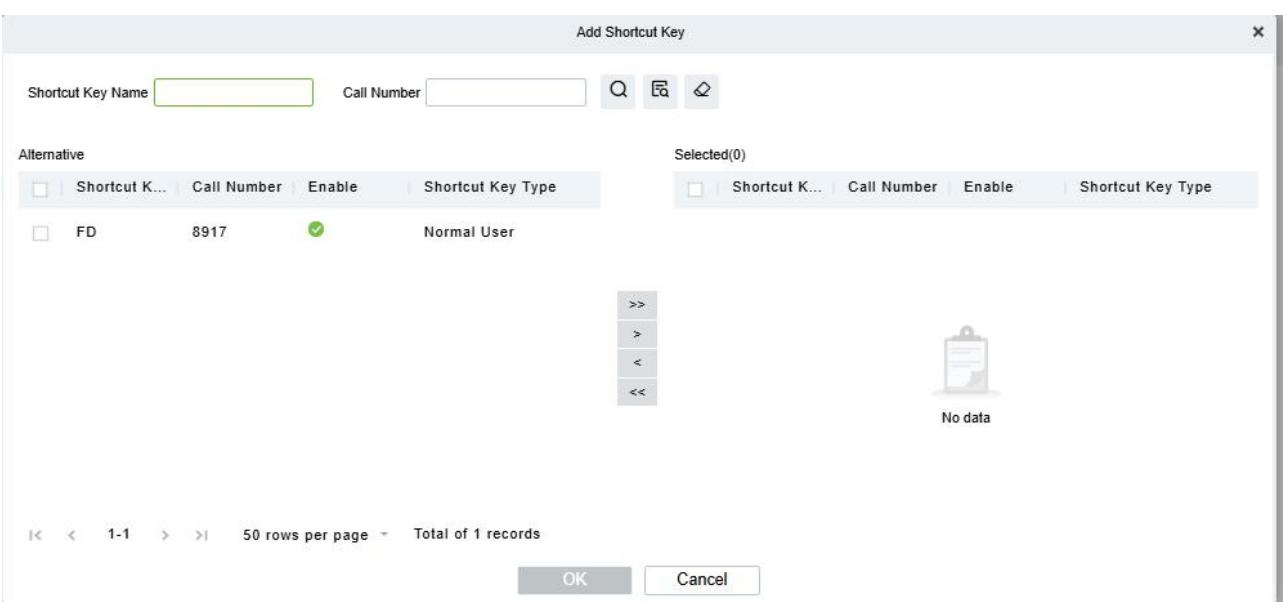
Step 2: After adding the shortcut keys, go to Video Intercom → Device Management → Device, select the device, and then click "Set up" → "Set Shortcut Key".



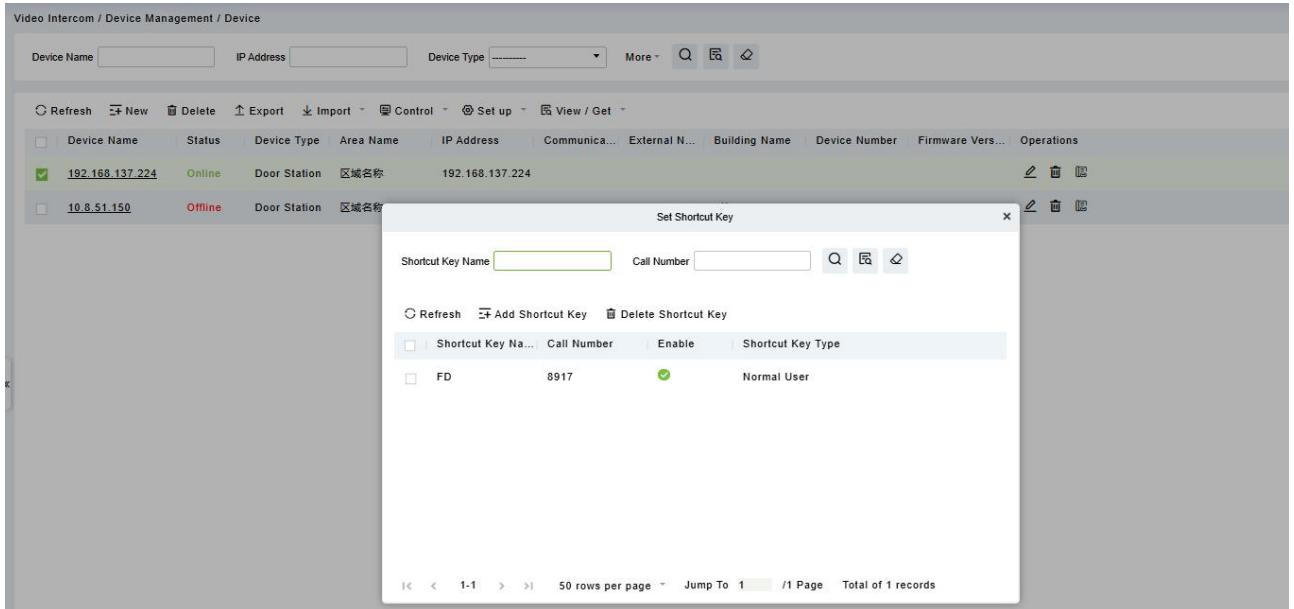
Step 3: Click "Add Shortcut Key".



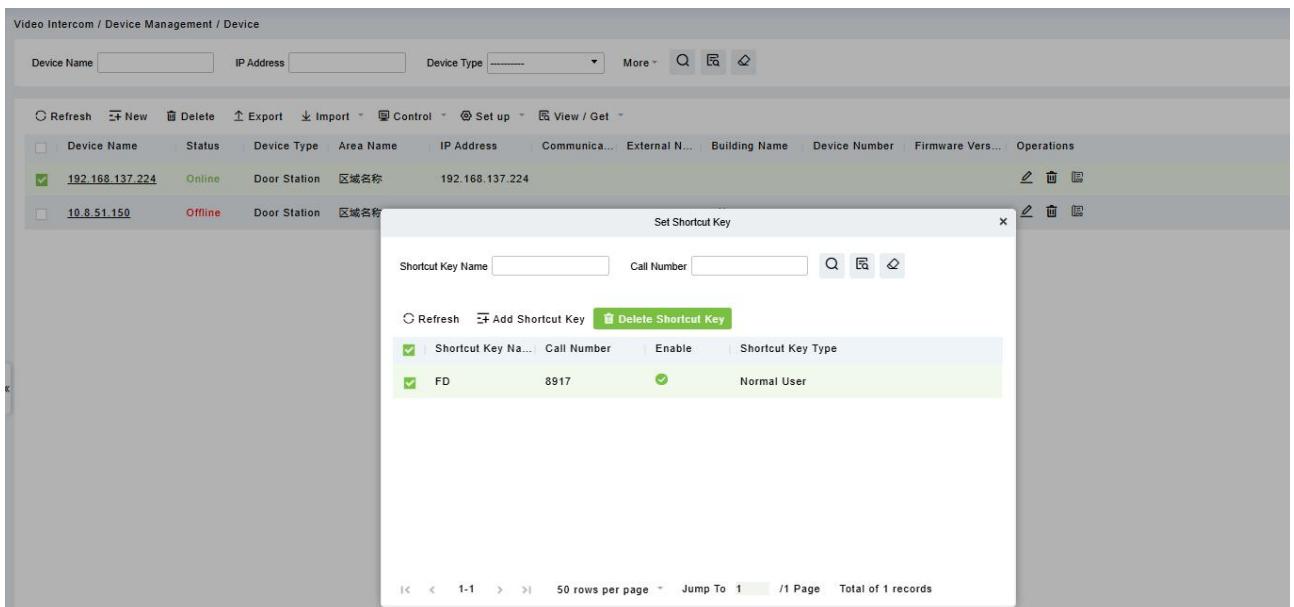
Step 4: Move the shortcut key you want to add to the right side and click "OK" to complete the operation.



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.



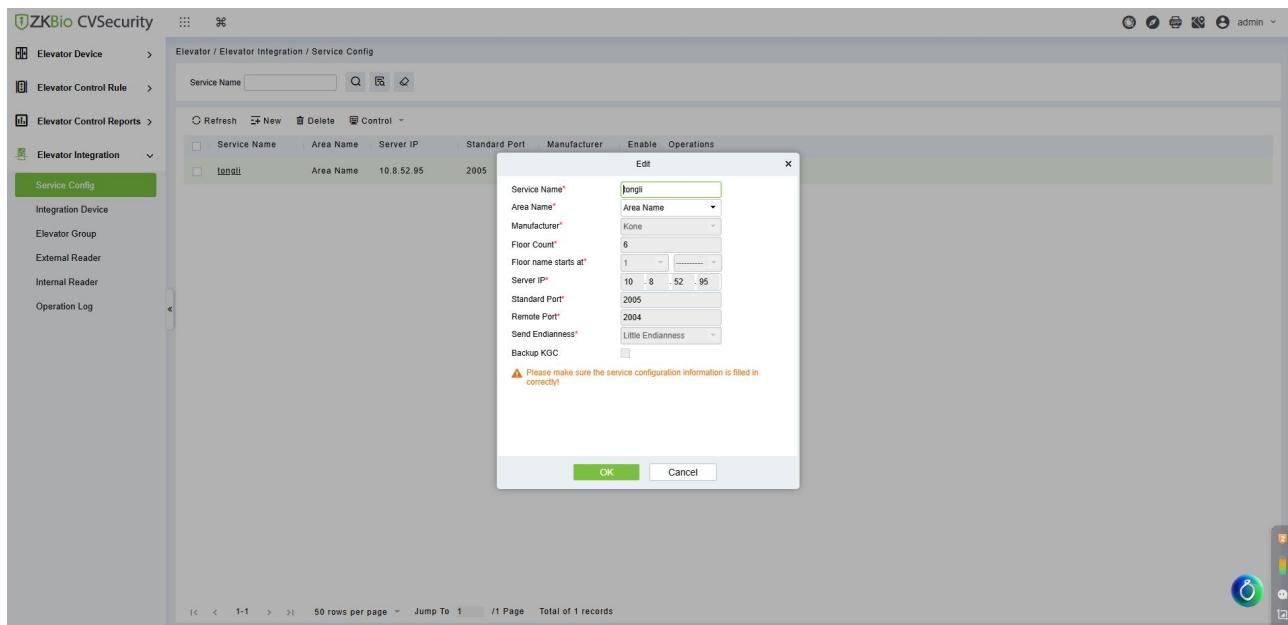
After checking the shortcut key, click "Delete Shortcut Key" to delete the shortcut key. The access control door will delete it simultaneously.



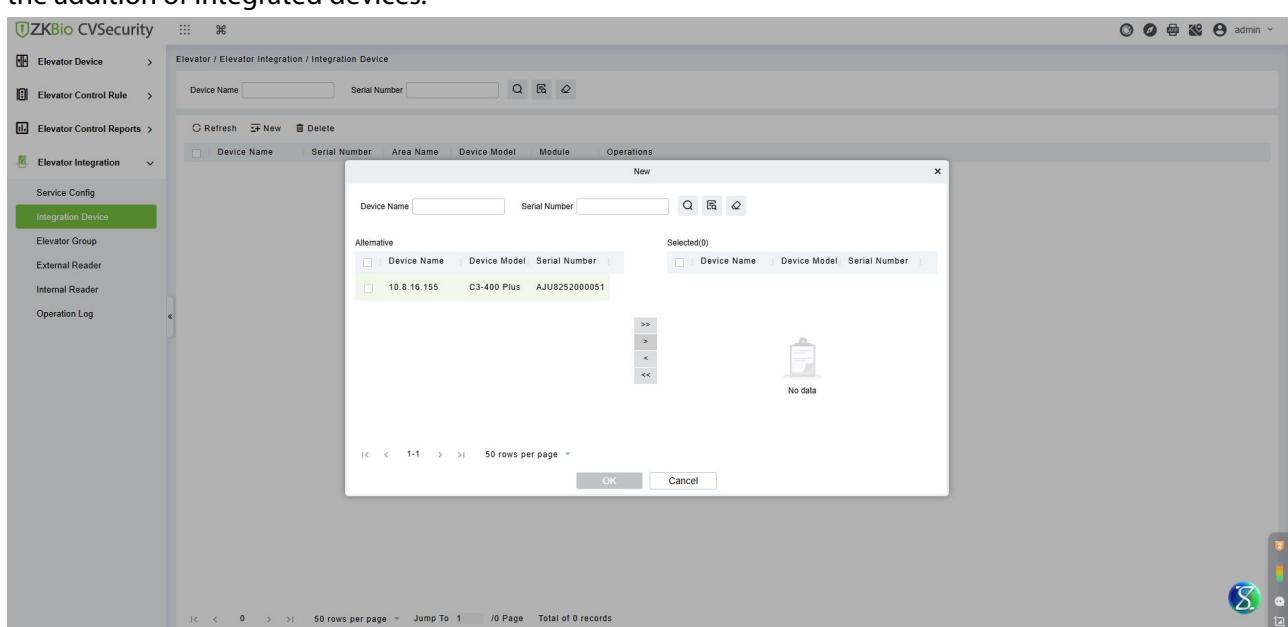
- In apartment visual intercom scenarios, remote door unlocking via the entrance terminal is supported, along with the allocation of elevator access permissions for visitors.

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.

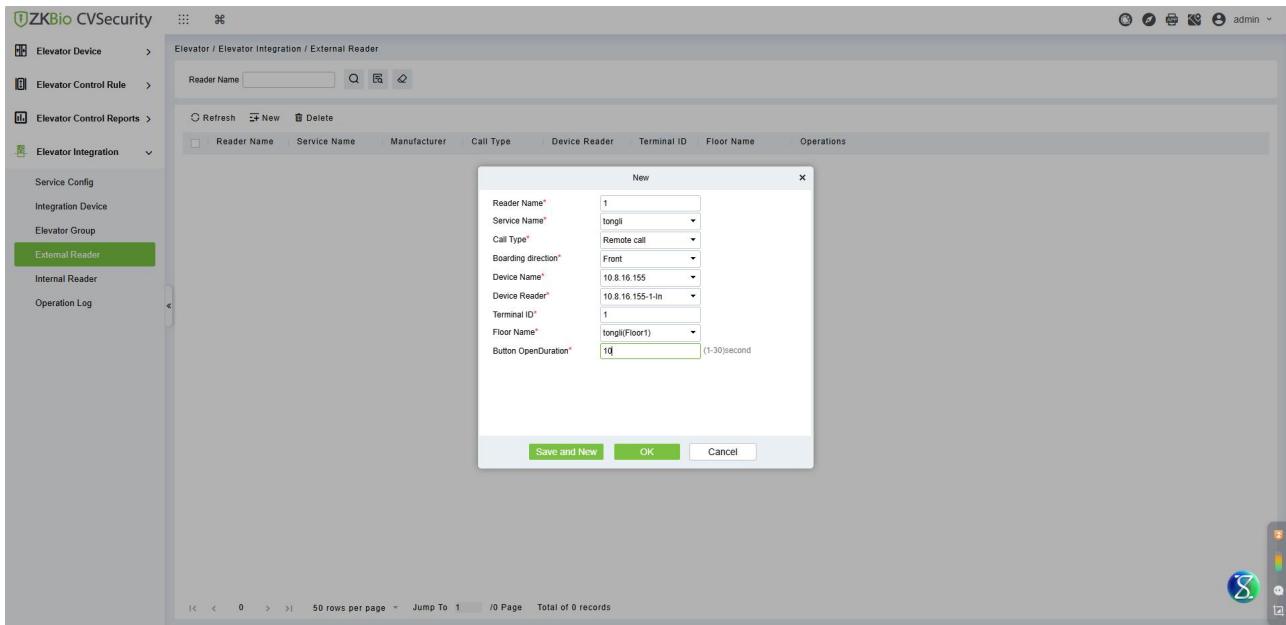
Step1: Enter Elevator → Elevator Integration → Service Config ,click "New" to set up the DCS service configuration.



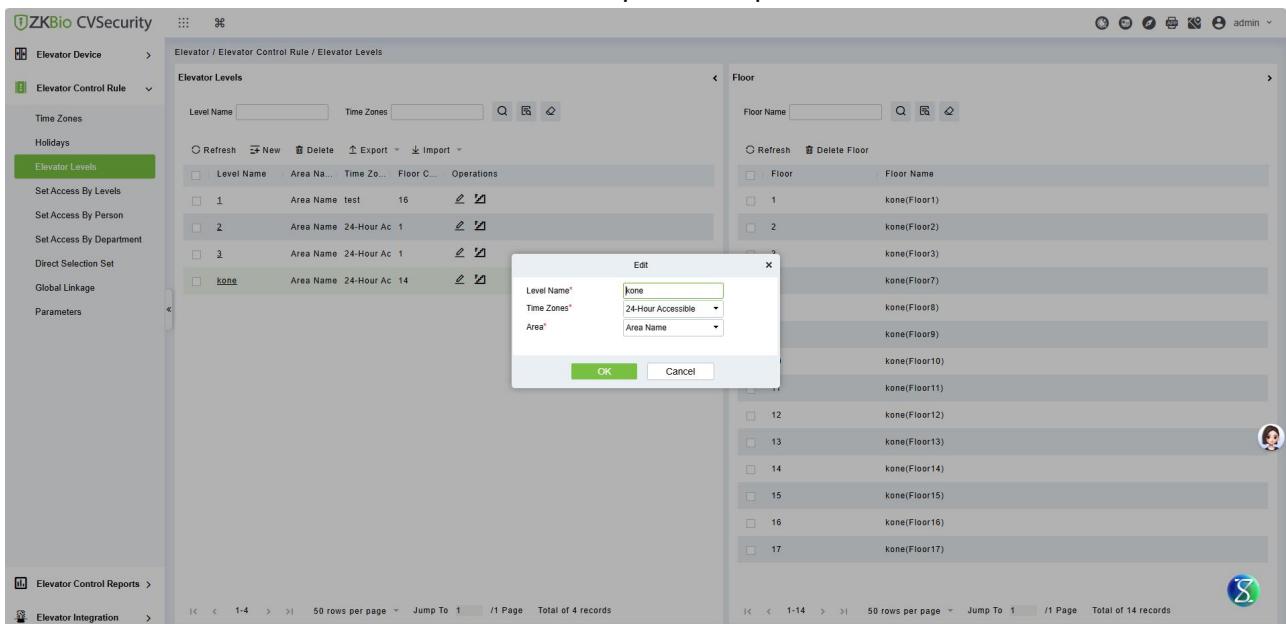
Step 2: Enter Elevator → Elevator Integration → Integration Device, click "New", select the access control devices with video intercom function and move them to the right, then click "OK" to complete the addition of integrated devices.



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.



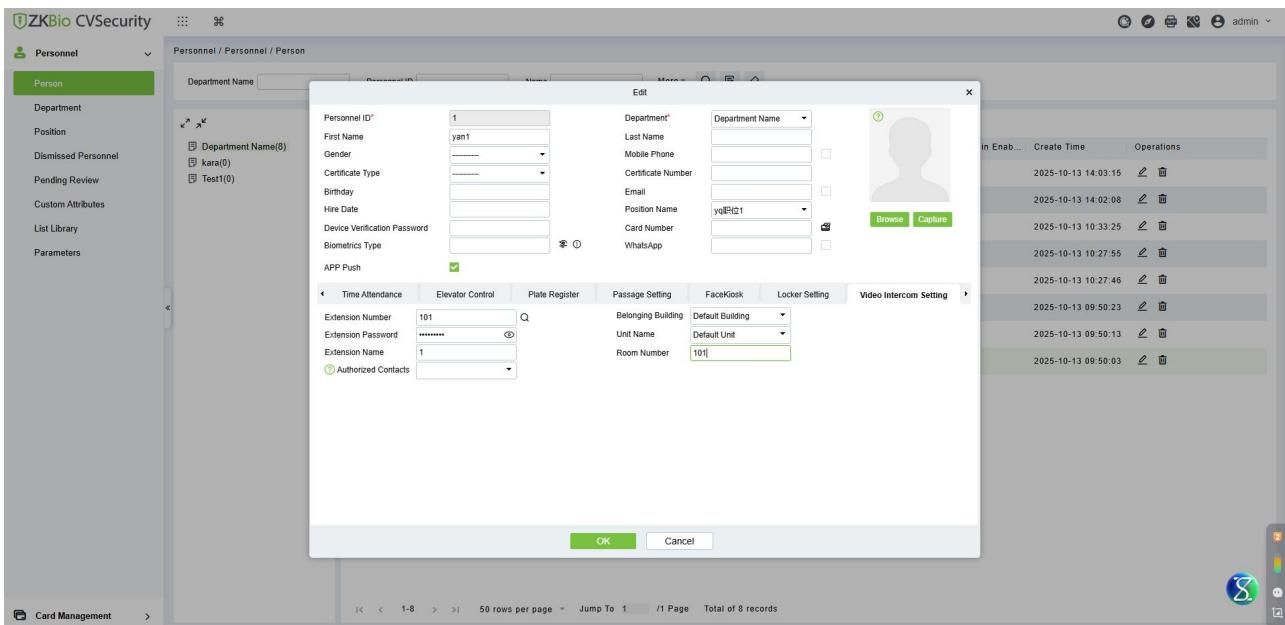
Click OK or Add Floor icon in the operation column, move the corresponding elevator floor from the left to the right, and click OK.

The screenshot shows the ZKBio CVSecurity software interface. The main window displays 'Elevator / Elevator Control Rule / Elevator Levels' with a list of elevator levels (1, 2, 3, kone) and their corresponding area names. A modal dialog box titled 'Add Floor' is open, showing a list of floors (B2, 1, 2, 3, 4, 5, 6) and their area names. The 'Selected(0)' section is empty. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The main interface at the bottom shows a list of 14 records.

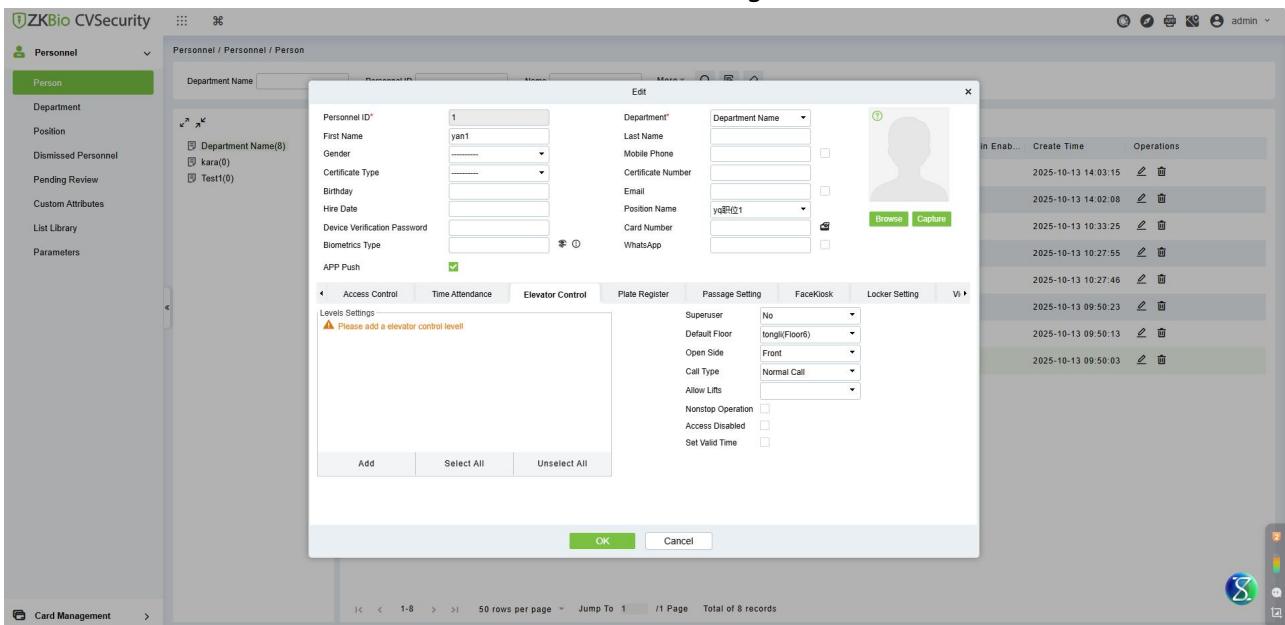
Step 5: Enter Elevator → Elevator Control Rule → Set Access By Levels, click the "Add Personnel" icon in the operation column of the new elevator levels that was just added, move the corresponding personnel from the left to the right, and click OK to complete the operation.

The screenshot shows the ZKBio CVSecurity software interface. The main window displays 'Elevator / Elevator Control Rule / Set Access By Levels' with a list of elevator levels (1, 2, 3, kone). A modal dialog box titled 'Add Personnel' is open, showing a list of personnel (111, 2841, 8888, 456) with their names and department names. The 'Selected(0)' section is empty. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The main interface at the bottom shows a list of 1 record.

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.

ZKBio CVSecurity

System Management / Cloud Settings

Cloud Settings

Enable

No Yes

Is pushing event data to the cloud platform enabled

No Yes

ZKBio CVConnect Server Url

http://127.0.0.1:6001

⚠ The ZKBio CVConnect platform, as a sub-service of MinervaOT, mainly serves to forward intranet's application data to be accessed externally. If you have not installed the ZKBio CVConnect client yet, please click the link below to download or contact the technical support to obtain the installer.

ZKBio CVConnect Client

APP enterprise QR code



OK

Cloud Settings

Language Pack
Operation Log
Data Management
Area Settings
System Parameter
E-mail Management
Dictionary Management
Data Cleaning
Resource File
Cloud Settings
AI Service Configuration
Certificate Type
Print Template
System Monitoring
Message Notification
Parameters
PING

Authority Management
Communication Mana...
Third Party Integration
Data Integration

admin

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

ZKBio CVSecurity

Video Intercom / Basic Management / Parameters

DTMF Setting

DTMF:

1

APP Call Number Type Setting

Call Number Type

Extension Number SIP Account

SIP Service Mode Configuration

SIP Service Mode

Cloud SIP Local IPPBX Converged Communication

⚠ To ensure normal operation of Cloud SIP service and mobile APP, please go to [System Management - Cloud Service Configuration] to confirm cloud service is enabled.

OK

DTMF Setting
APP Call Number Type Setting
SIP Service Mode Configuration

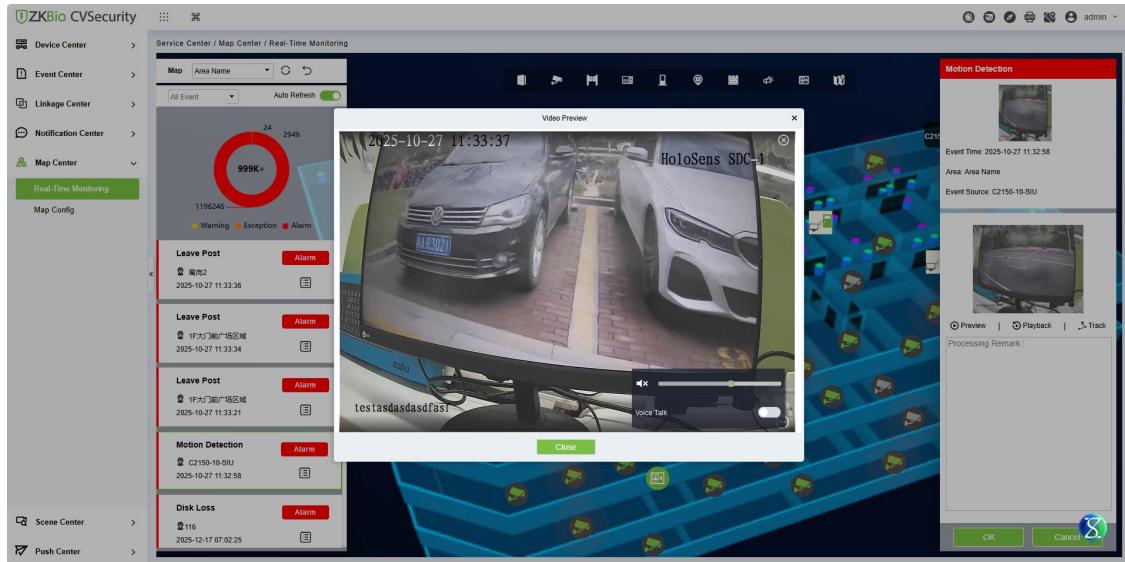
Device Management
Extension Management
Access Management
Video Intercom Reports

admin

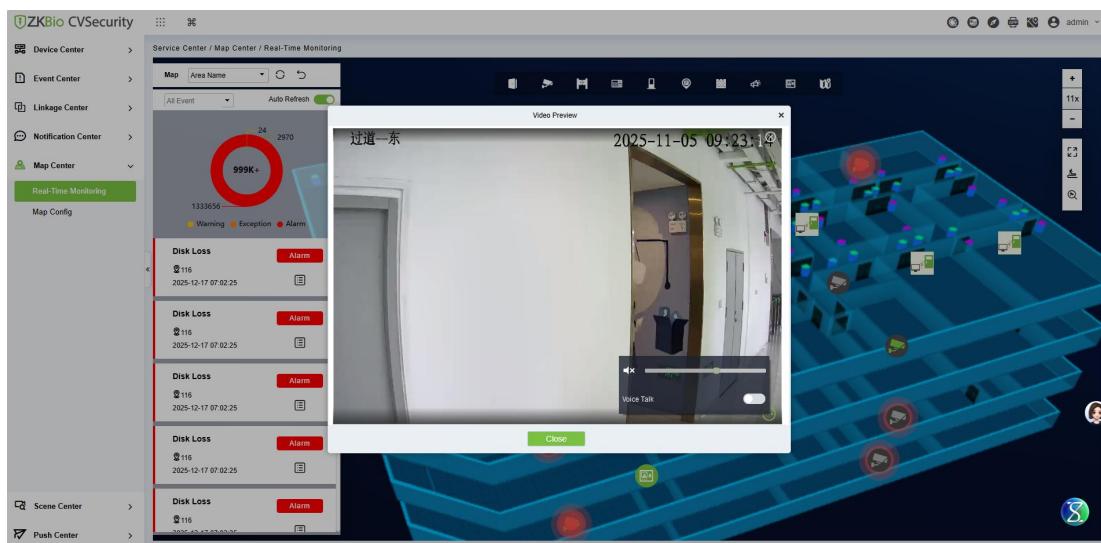
Service Center

● 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.

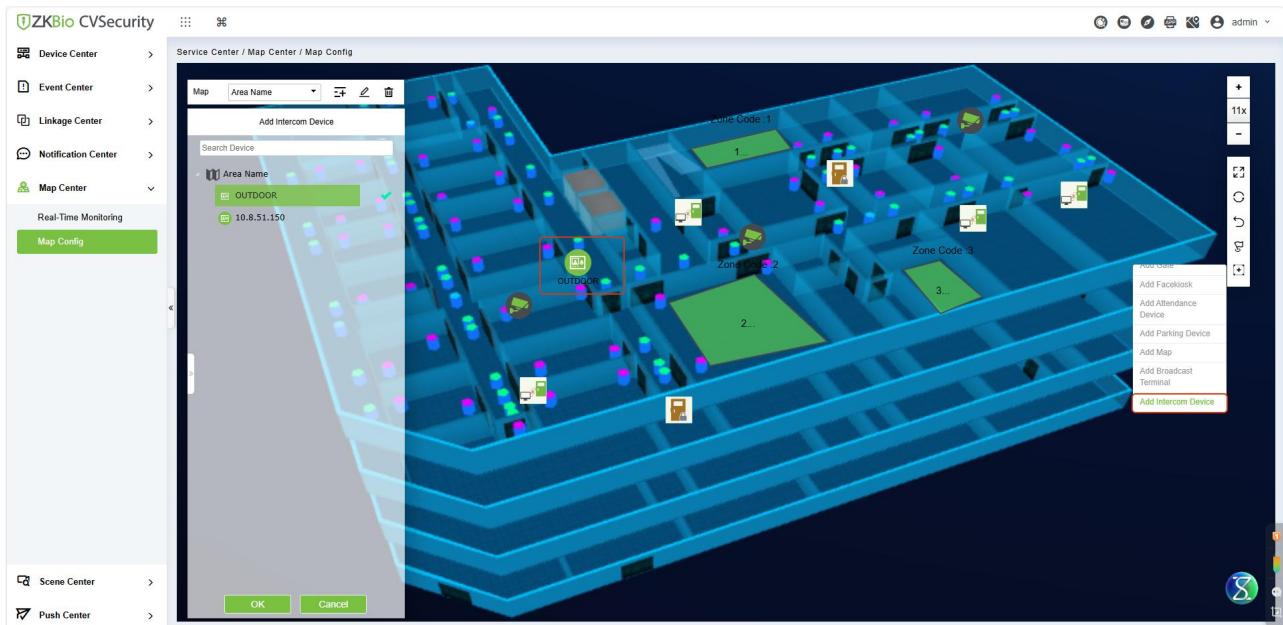


When you double-click the camera preview, cameras that support the intercom function will allow you to enable the voice intercom feature.



● Map Center-Added visual intercom points.

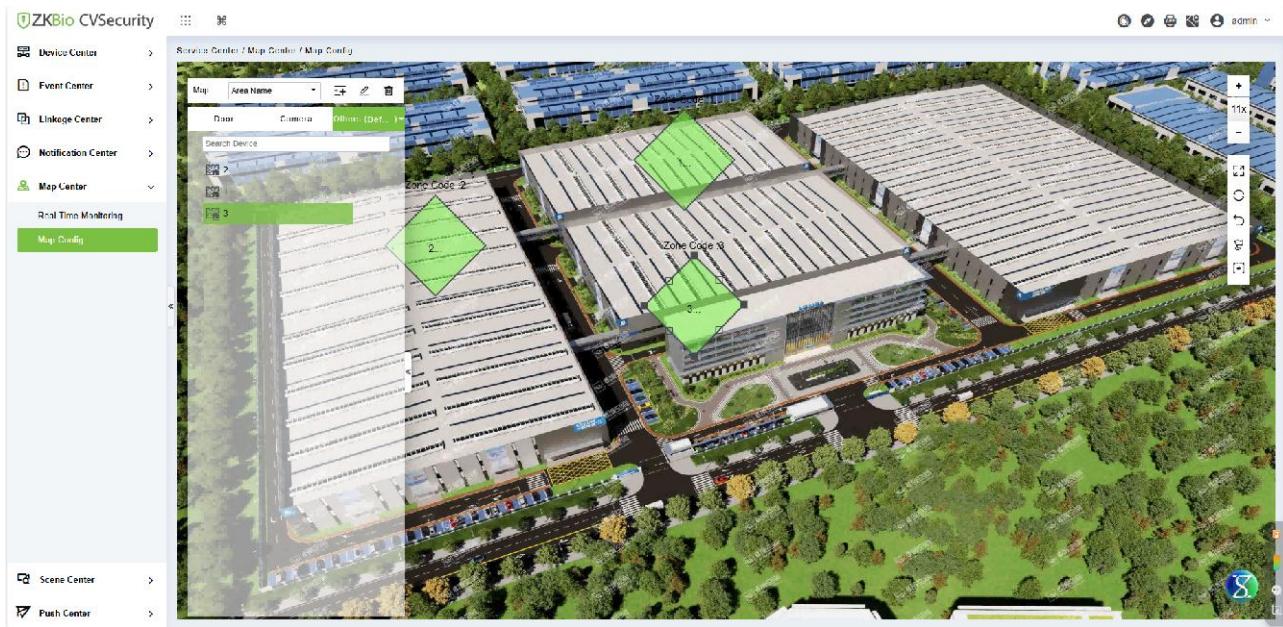
Step: Enter the Service Center → Map Center → Map Config, click "Others", and you can select Video Intercom.



Note: The optional equipment here is a DNK device.

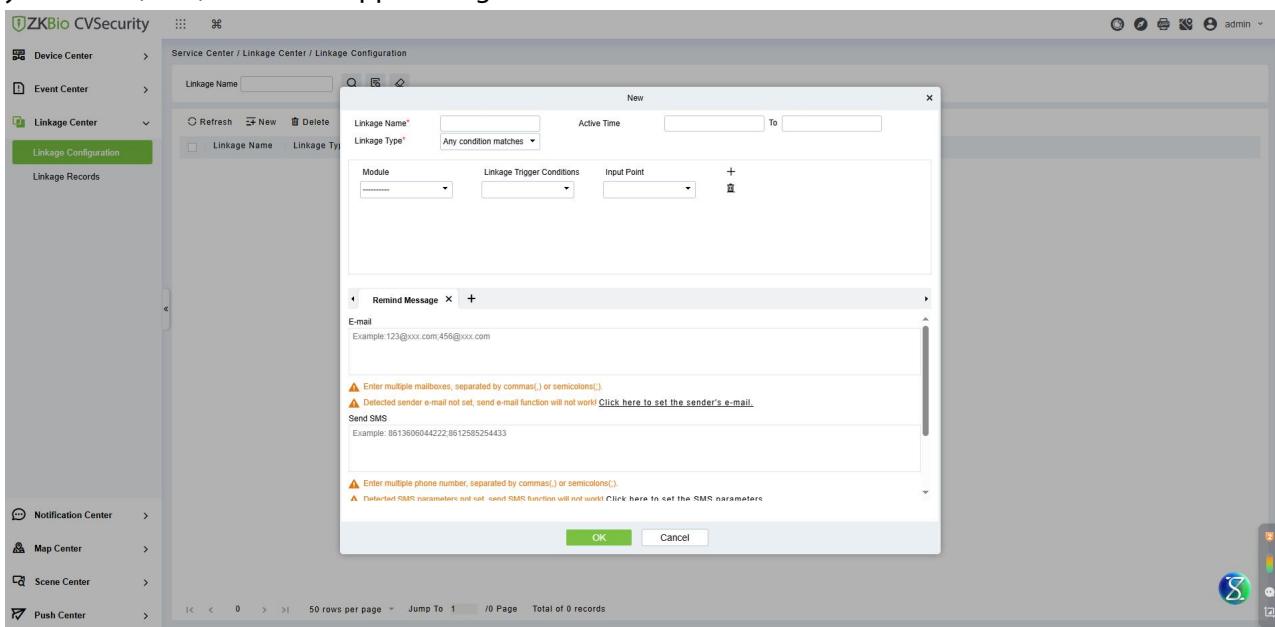
- **Map Center-Intrusion alarm zones support secondary editing and display of zone numbers.**

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.



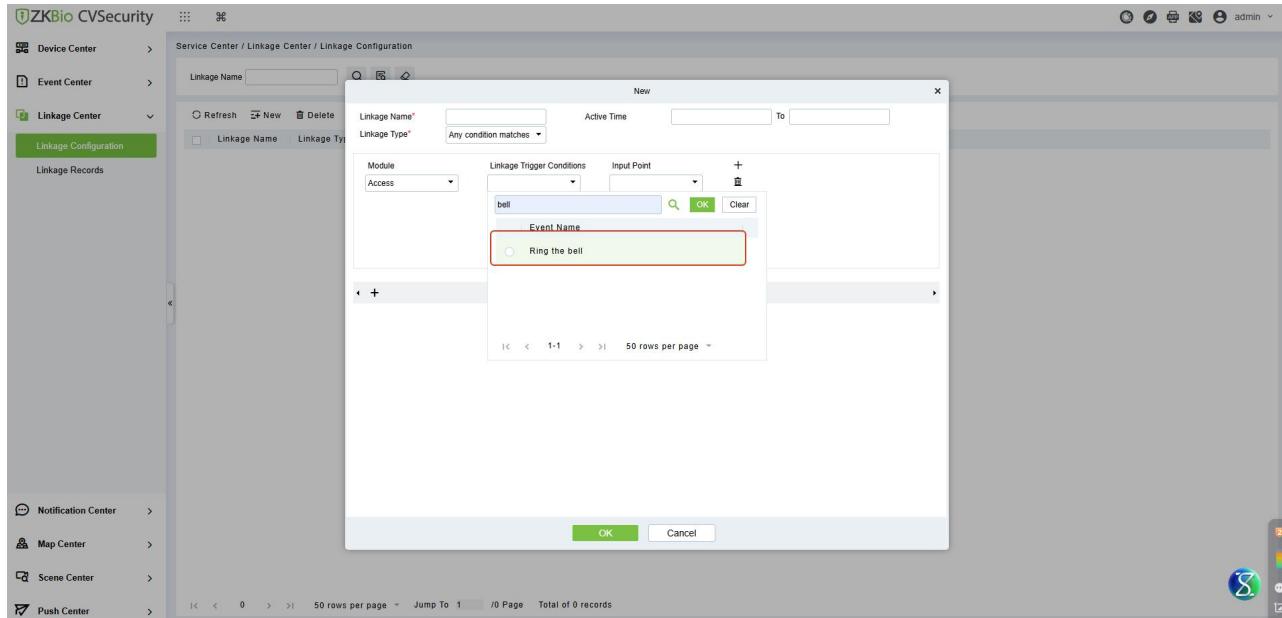
- **Linkage Center-Added "Remind Message" as a new output action option, supporting Email, SMS, and WhatsApp.**

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.

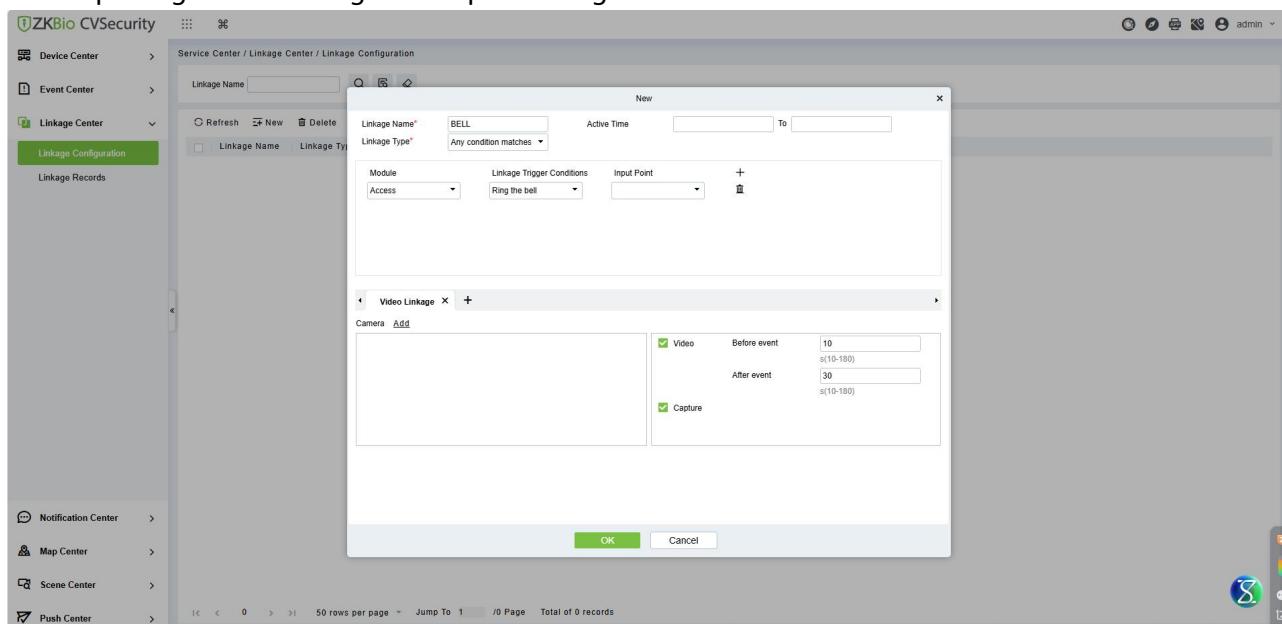


- **Linkage Center-When a doorbell is pressed, it can activate linked cameras to start recording.**

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.



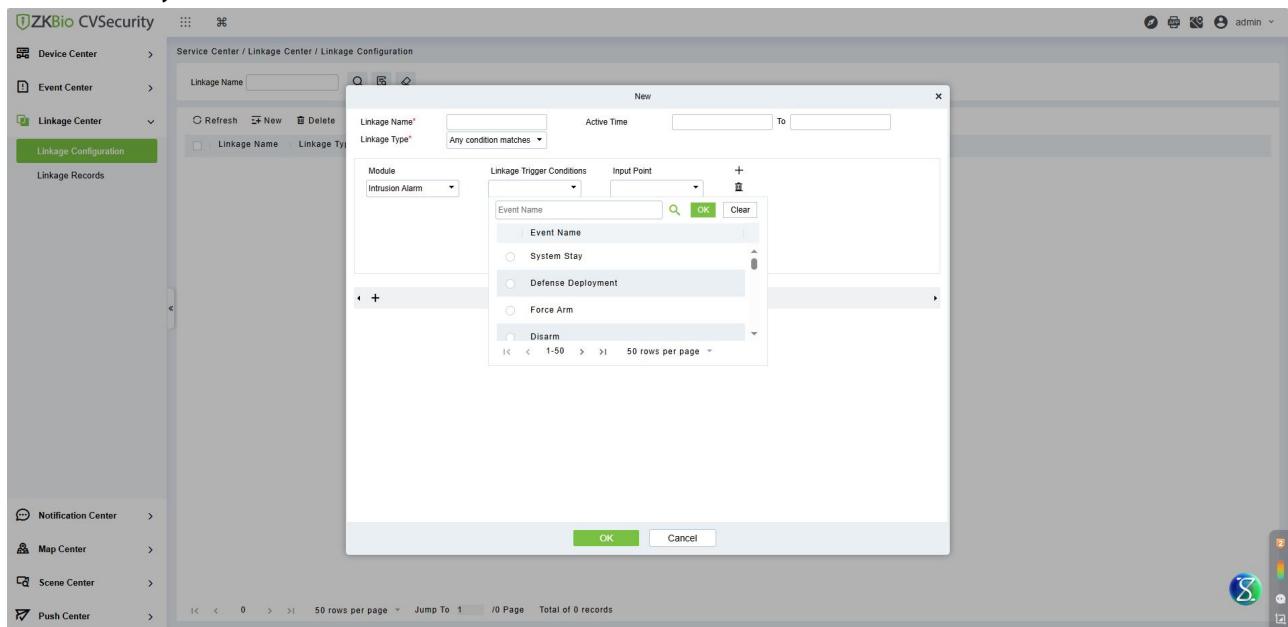
Step2: Select the video linkage for the output action, and check the box for video capture to complete the linkage configuration. Access control devices with doorbell function will activate the camera to start capturing and recording when a person rings the doorbell.



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

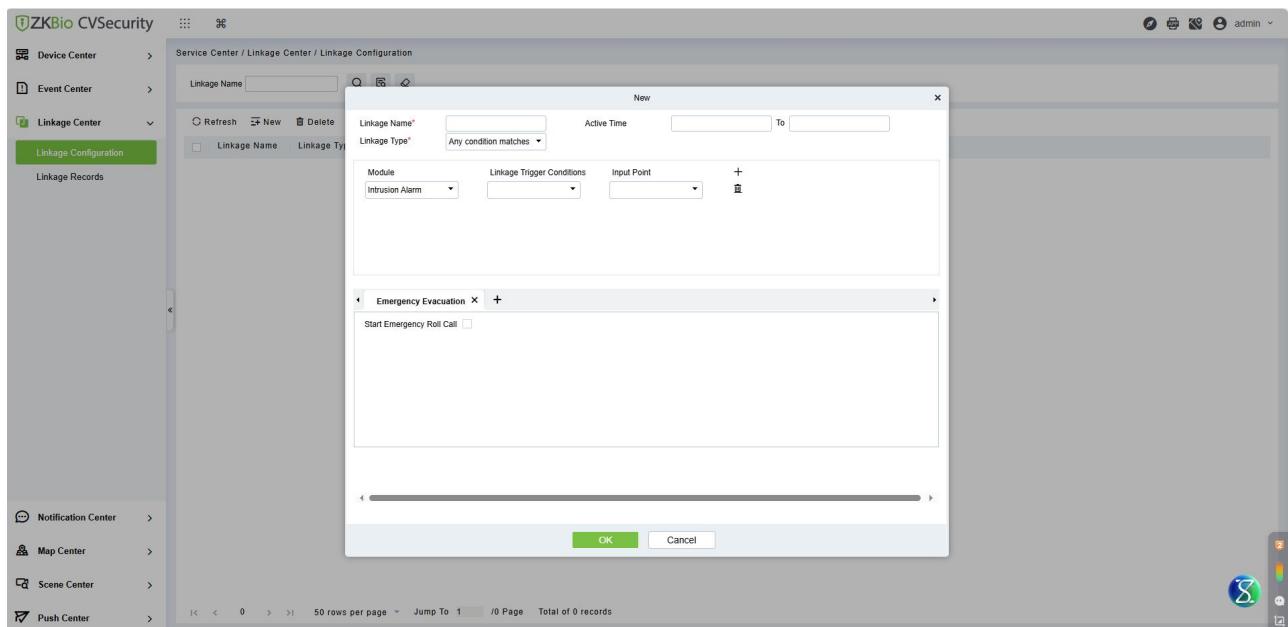
● Linkage Center-The linkage trigger condition has added an Intrusion Alarm.

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

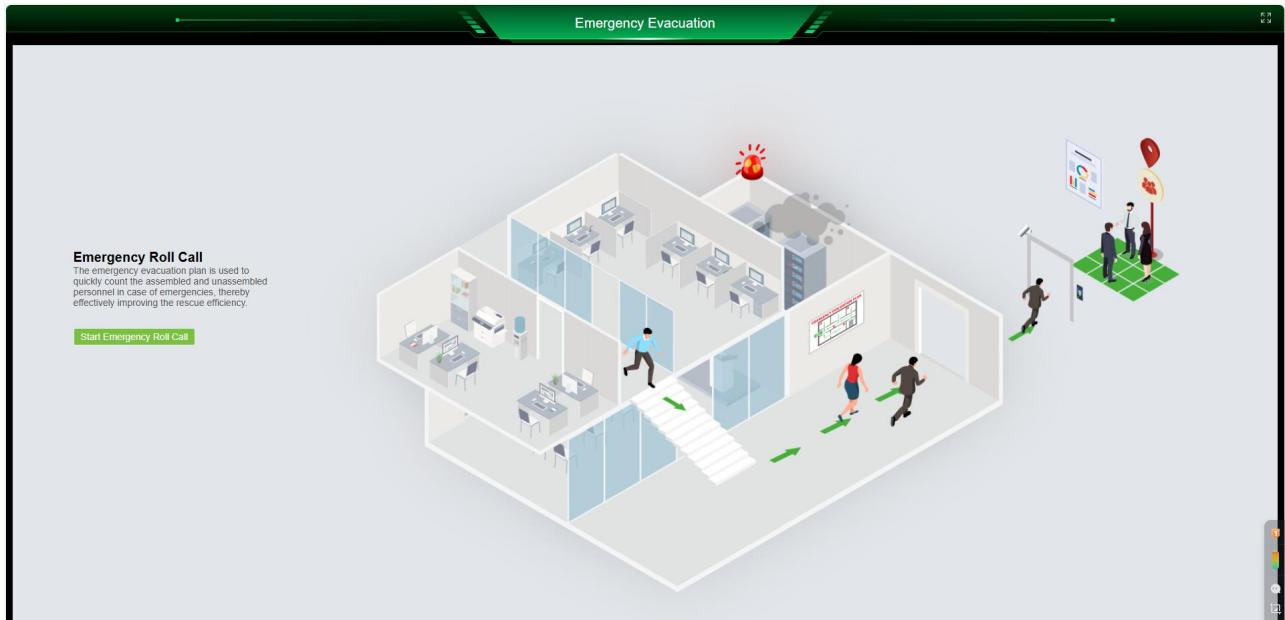


● Linkage Center-The output action has added an Emergency Evacuation.

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.

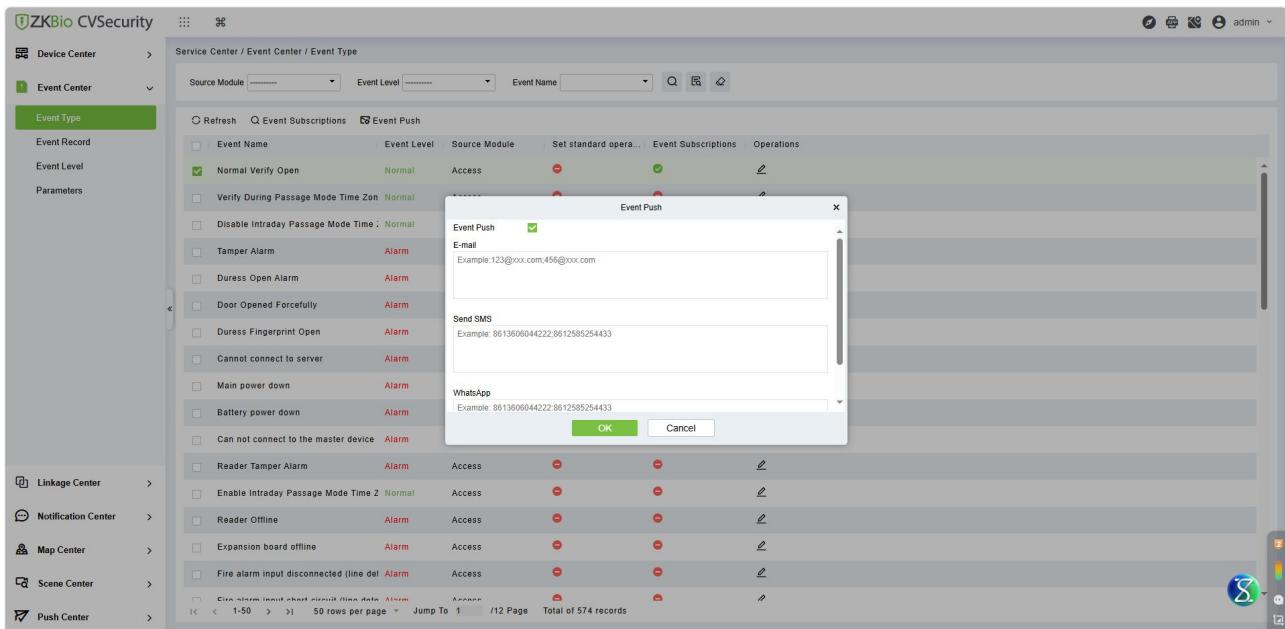


● Event Center-Added event subscription notifications.

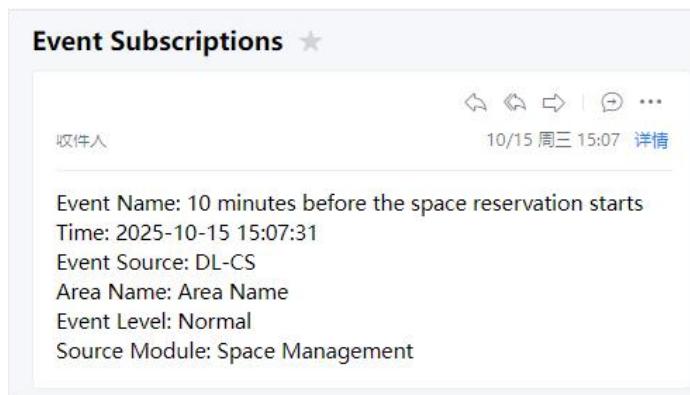
Step1: Service Center → Event Center → Event Type, select multiple event types and then click "Event Subscriptions". Choose "Yes" and click "OK". The subscription status can then be viewed in the list.

Event Name	Event Level	Source Module	Set standard opera...	Event Subscriptions	Operations
Normal Verify Open	Normal	Access
Verify During Passage Mode Time Zon	Normal	Access
Disable Intraday Passage Mode Time	Normal	Access
Tamper Alarm	Alarm	Access
Duress Open Alarm	Alarm	Access
Door Opened Forcefully	Alarm	Access
Duress Fingerprint Open	Alarm	Access
Cannot connect to server	Alarm	Access
Main power down	Alarm	Access
Battery power down	Alarm	Access
Can not connect to the master device	Alarm	Access
Reader Tamper Alarm	Alarm	Access
Enable Intraday Passage Mode Time 2	Normal	Access
Reader Offline	Alarm	Access
Expansion board offline	Alarm	Access
Fire alarm input disconnected (line del	Alarm	Access
Fire alarm input short circuit fire data	Alarm	Access

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.

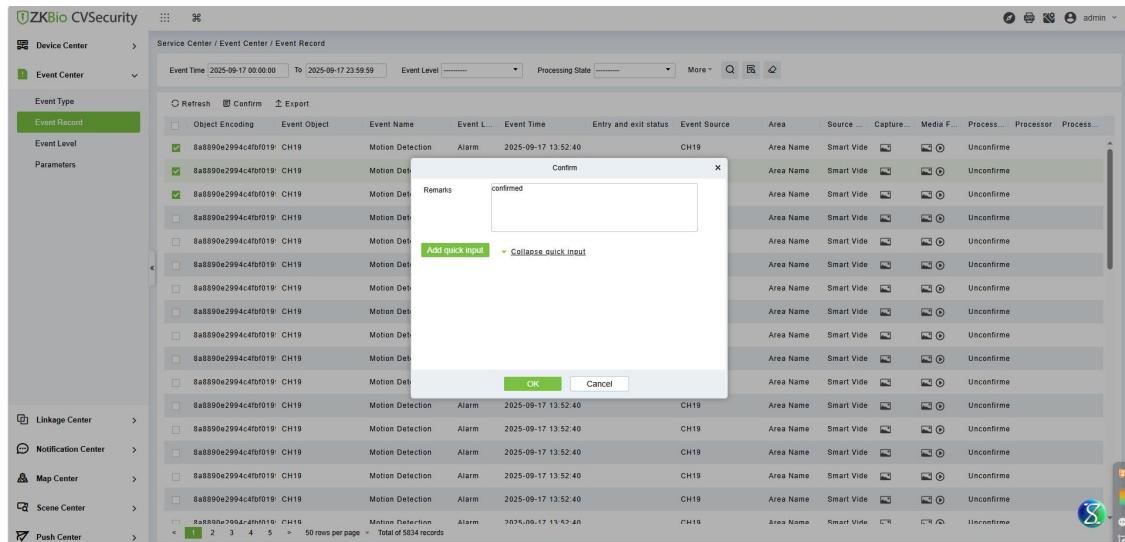


The content of the email is as shown in the following figure:



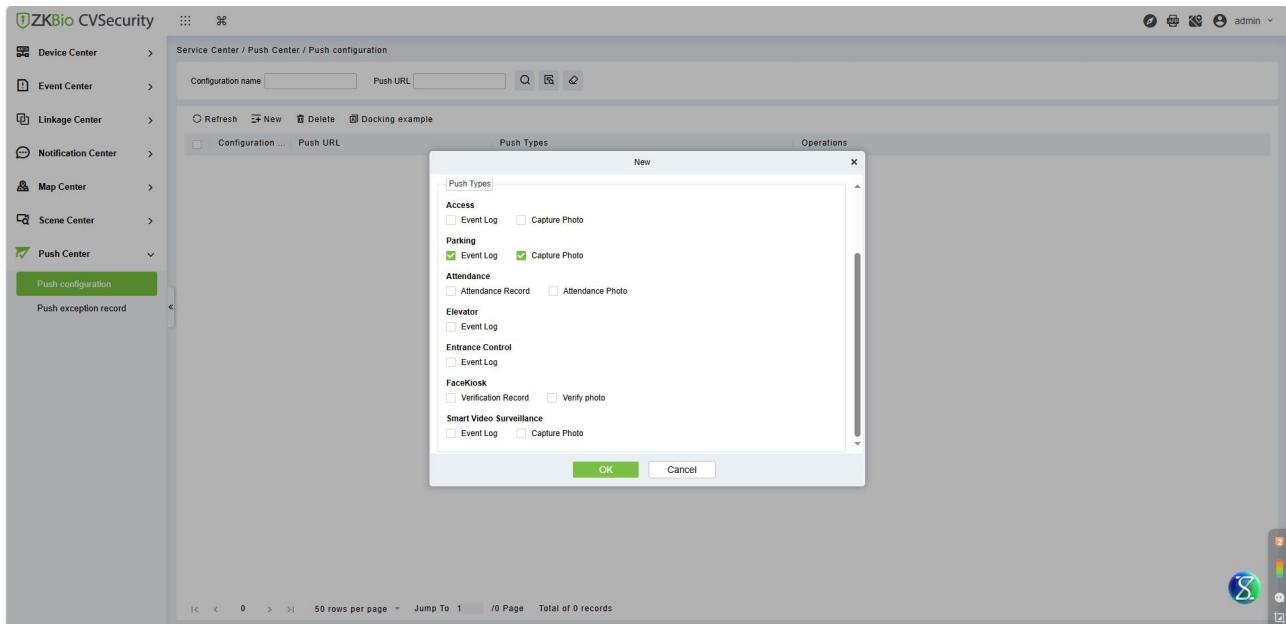
● Event Center-Supports batch selection and processing of events.

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.



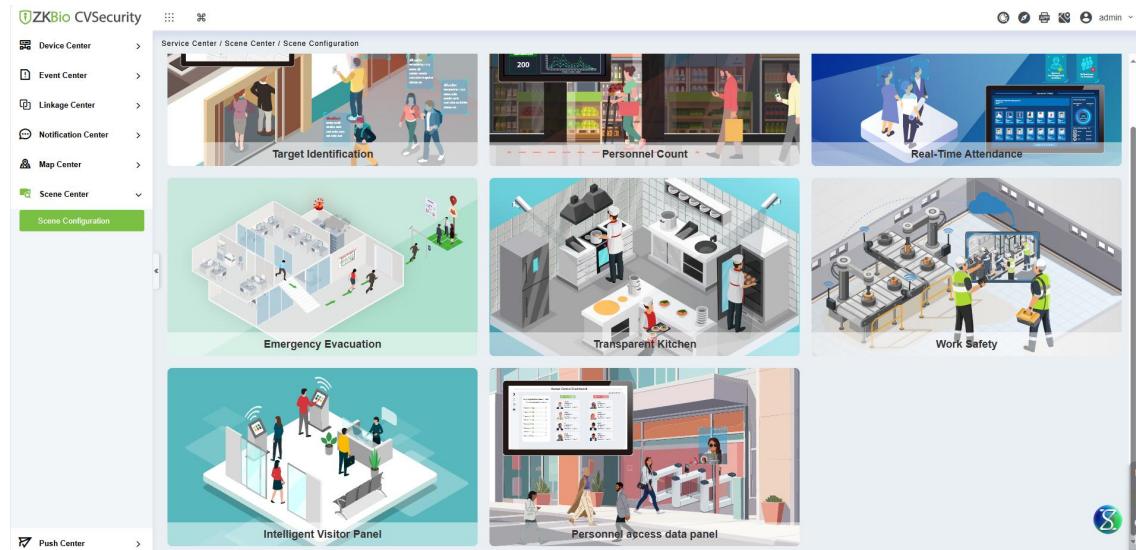
● Scene Center-Added work safety scenarios.

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

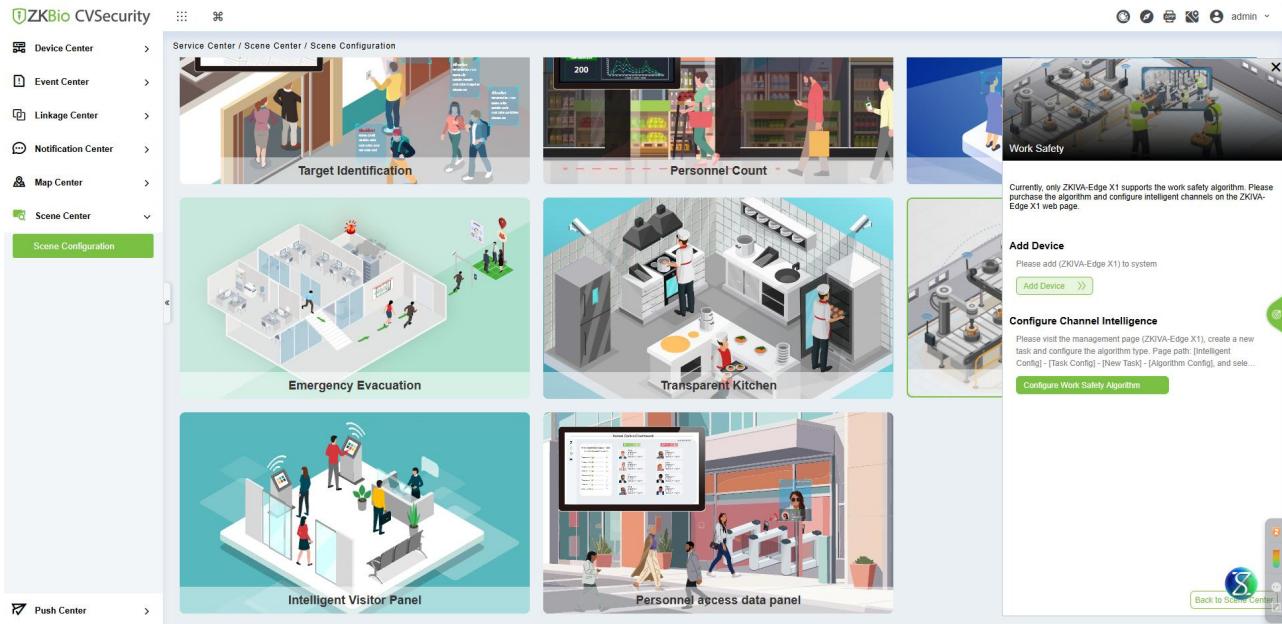
Algorithms: The work safety algorithms include: safety cap、safety uniform、safety belt、reflective vest、respirator、fire、smoke、oil_spill、fire_equipment.

Operating Steps:

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

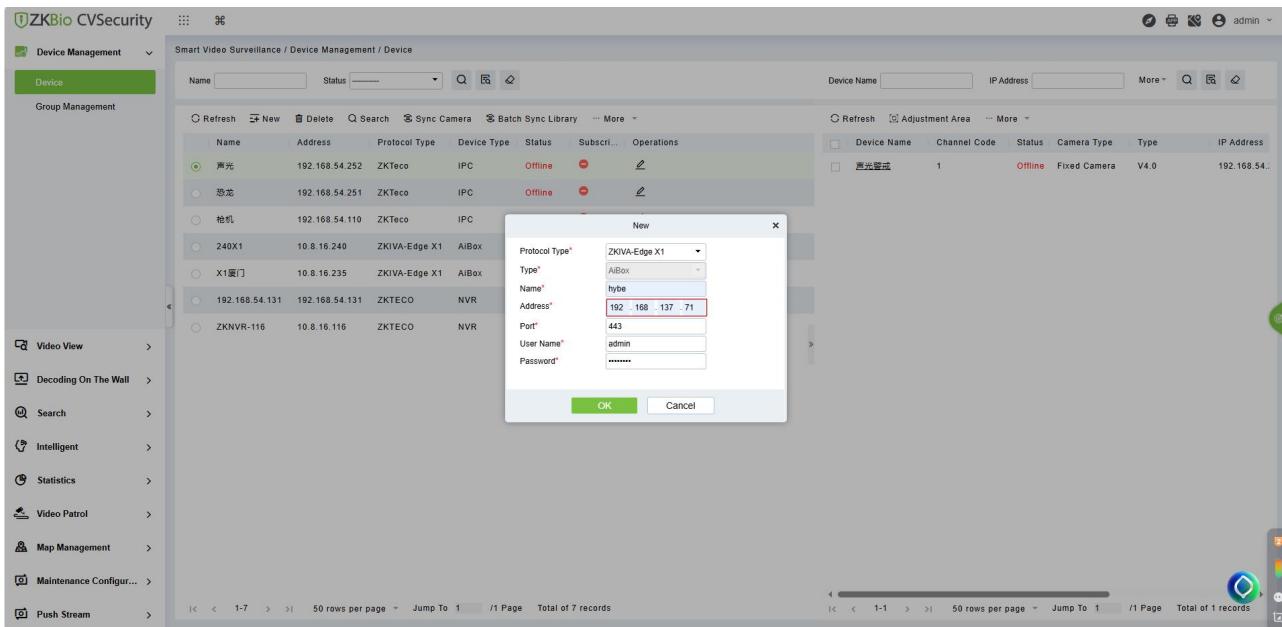


Quickly complete the configuration by following the step-by-step guide on the right.



Step1: Add ZKIVA-Edge X1 device

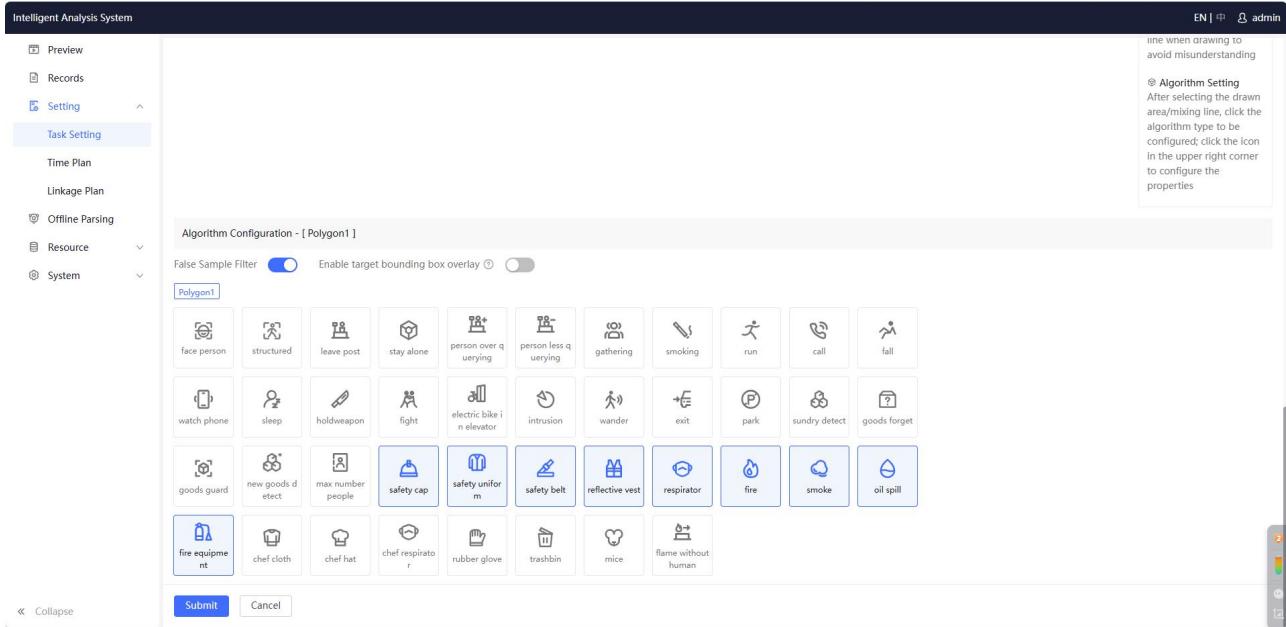
In the operation wizard, click "Add Device" to quickly jump to the device menu. Click "Add New" to include the ZKIVA-Edge X1 device, as shown in the figure below:



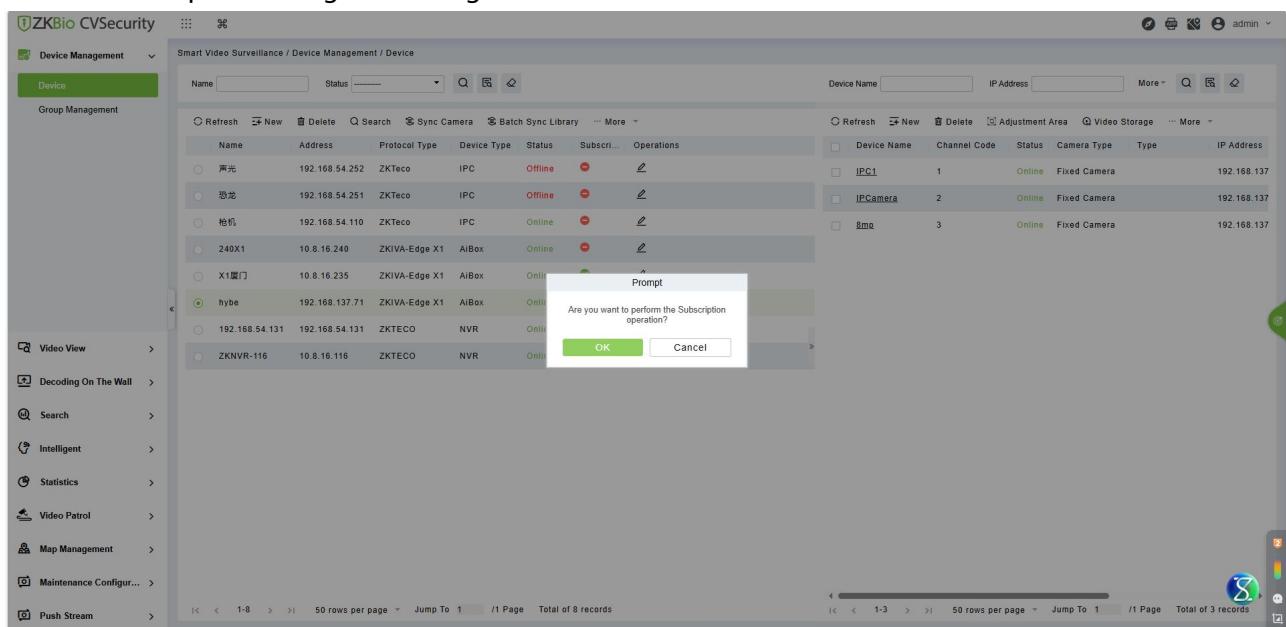
Step2: Configure Channel Intelligence

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.

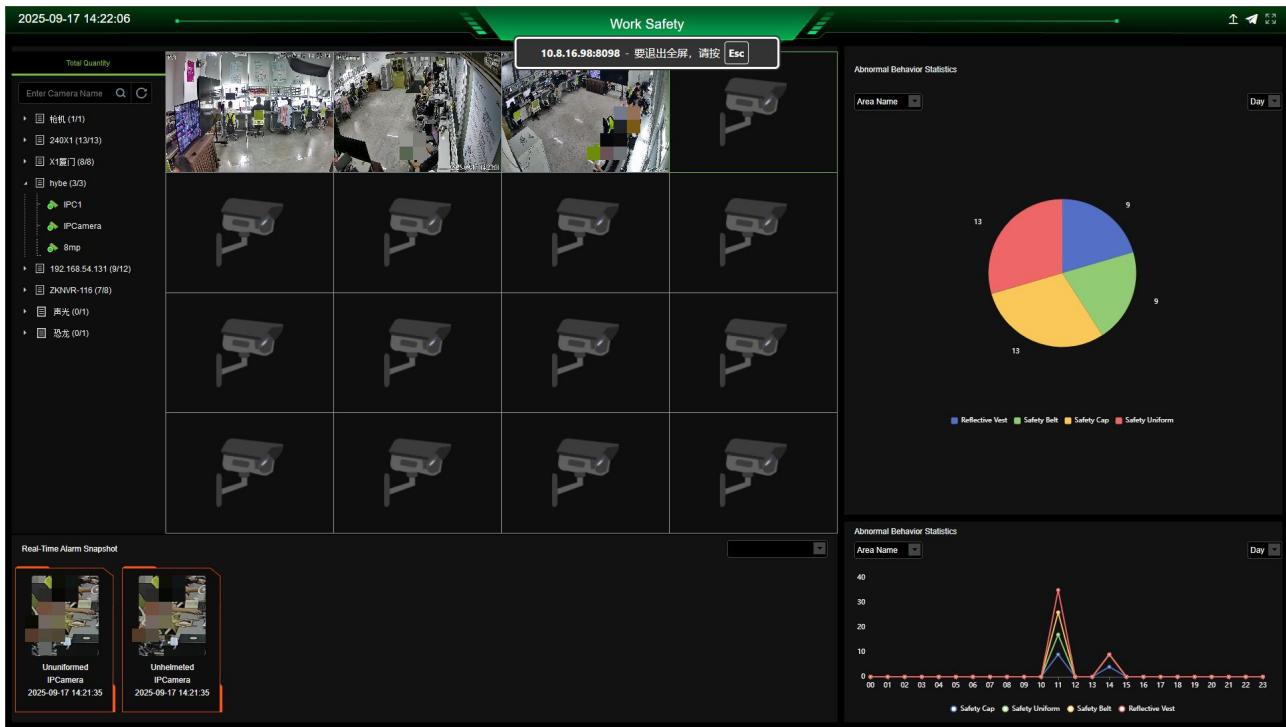
(Note: The IVS-X1 device must have the work safety algorithm package preconfigured before leaving the factory.)



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

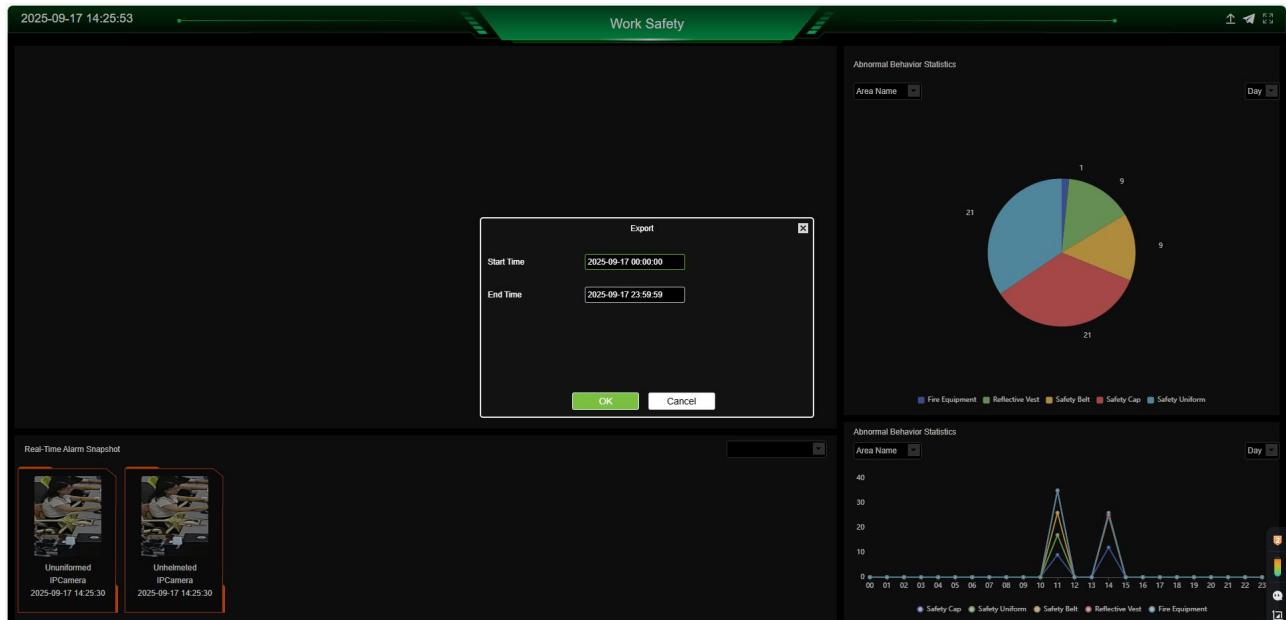


Step3: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:



■ 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:

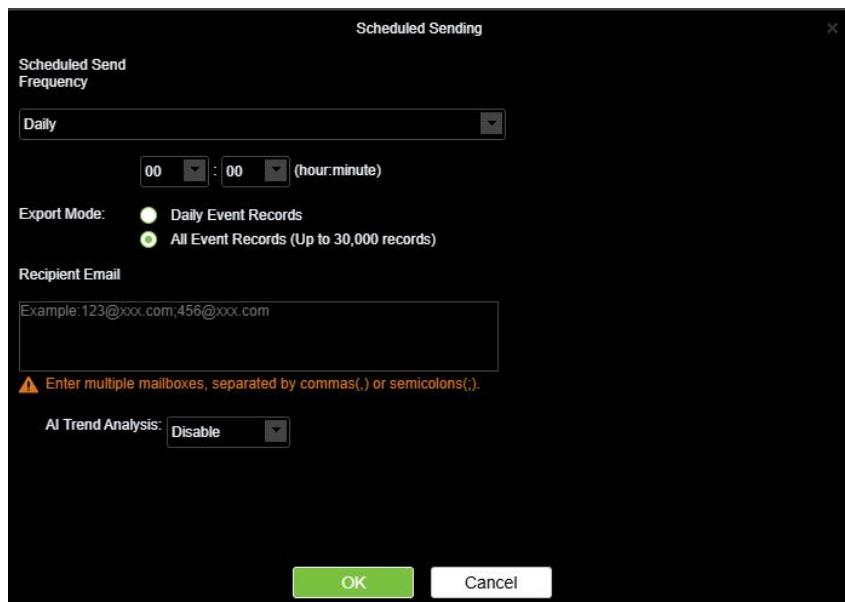


The exported report records are shown in the figure below:

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 14:26:09	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:

Work Safety Abnormal Behavior Report ★

附件一

X Work Safety Abnormal Behavior Report_2025... (382K)

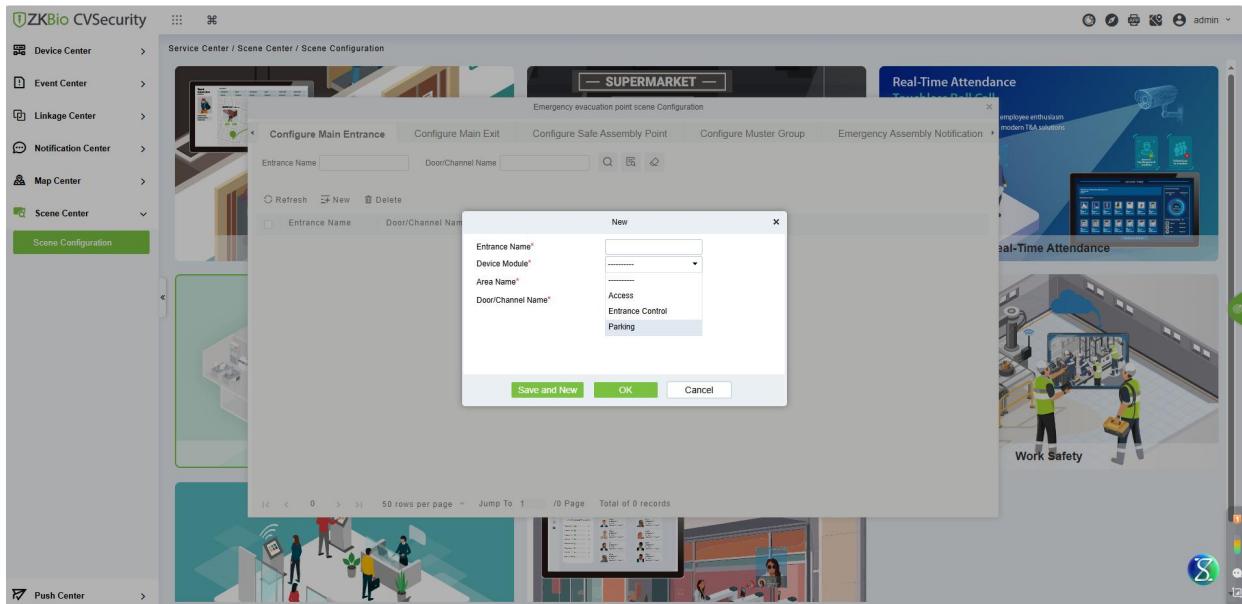
Attached is the product safety statistical report for ZKBio CVSecurity:

1. Reporting Period: [2025-10-15 00:00:00 To 2025-10-15 23:59:59]
2. Additional Information: see attached table
3. AI Trend Analysis Results:
 - (1). [Area Name] area shows the highest abnormal behavior frequency. Additional safety training is recommended.
 - (2). [2025-10-14 12:00] time period had the most helmet/PPE violations.
 - (3). [Area Name] area triggered the most smoke/fire alarms. Please check material storage.
 - (5). [Area Name] area detected liquid leaks.

● 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:



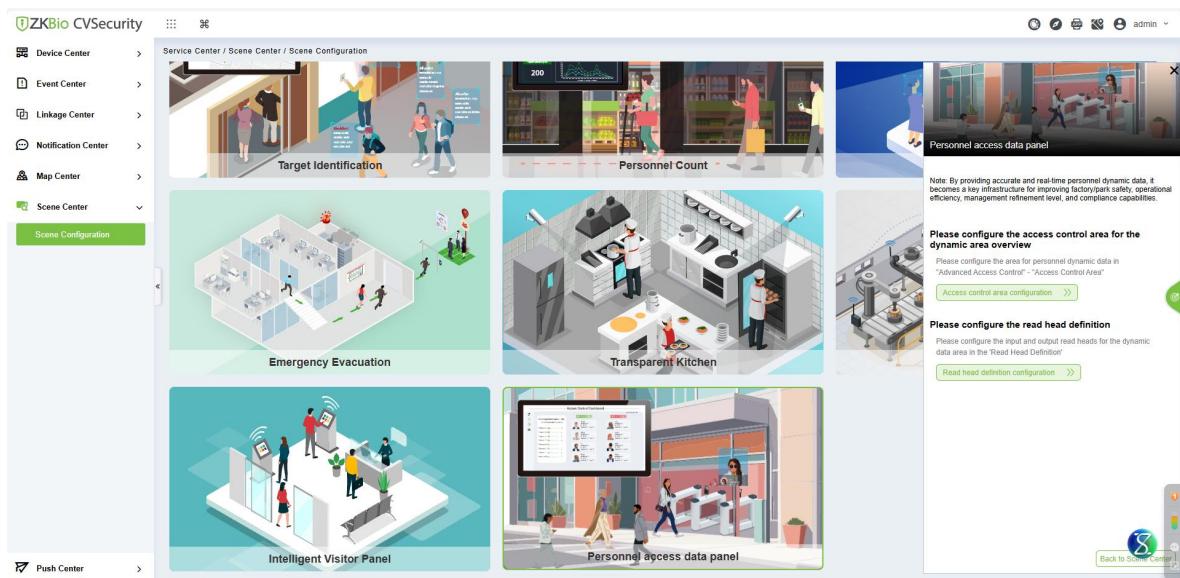
Note: Select the LPR device in the door/passage name field.

● 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.

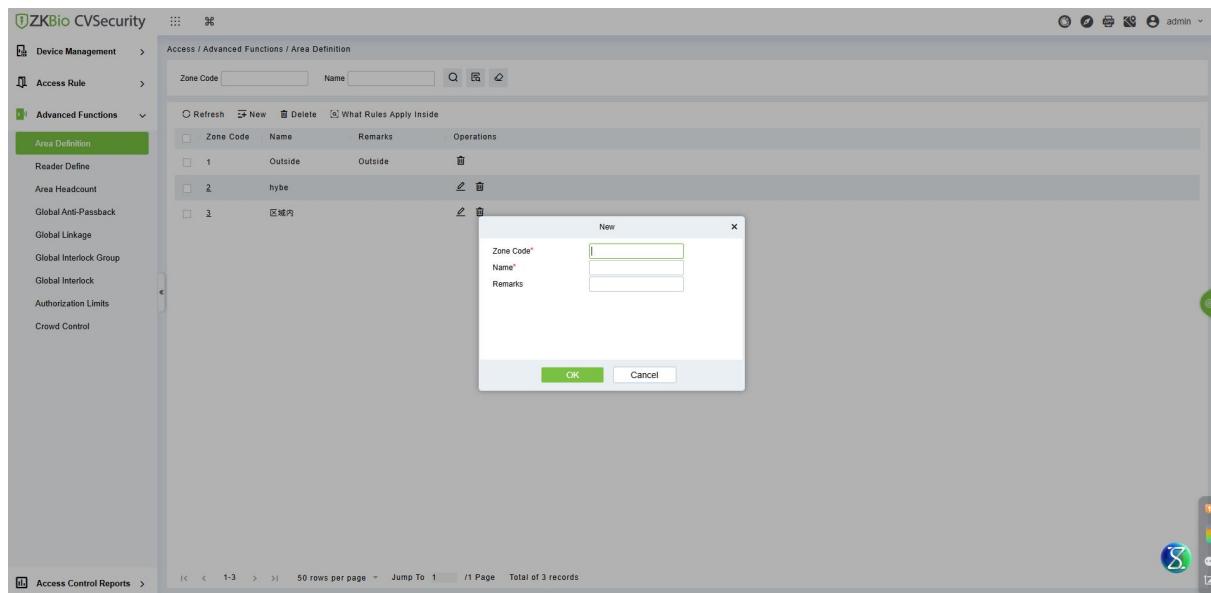
Operating Steps:

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:

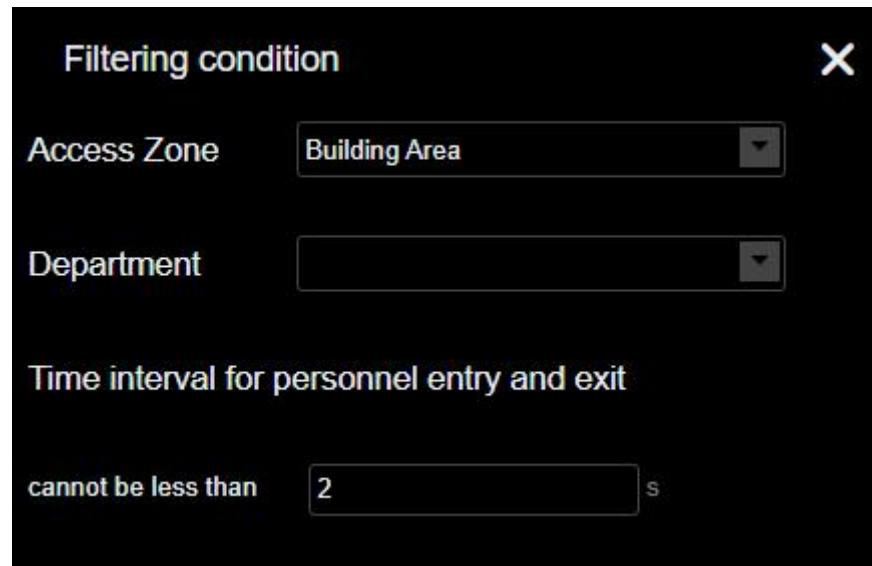
Step3: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:

Department Number	Department	Personnel
1	Department Name Jail	1

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.

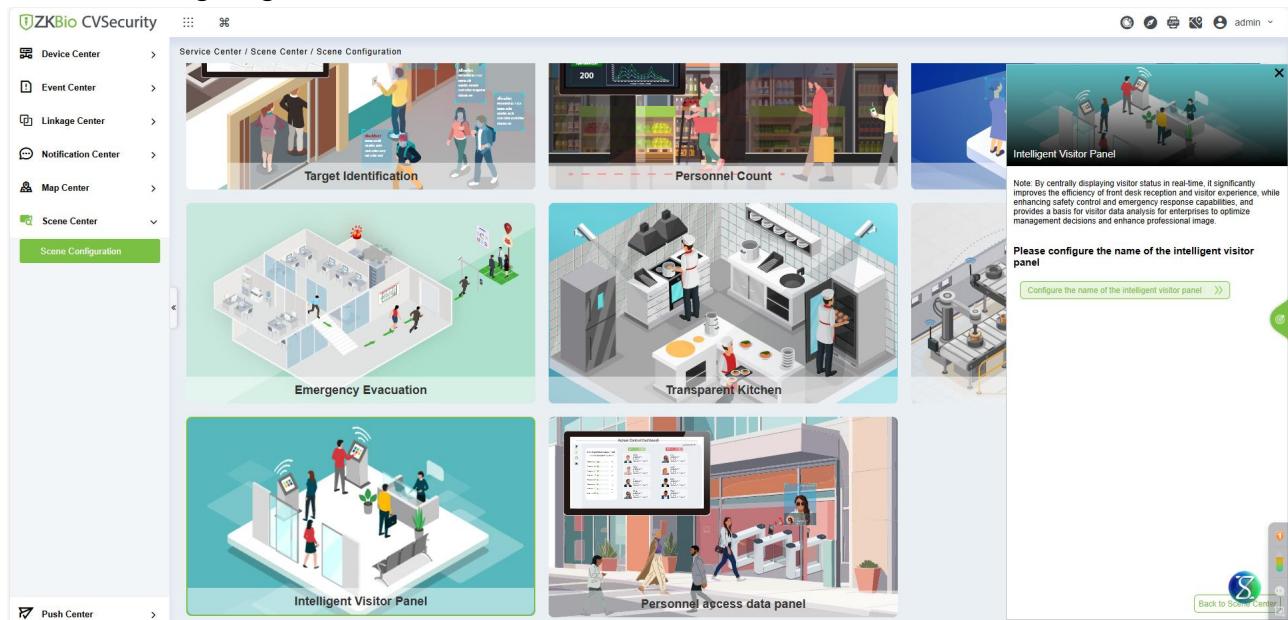


● Scene Center-Added Intelligent Visitor Panel.

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.

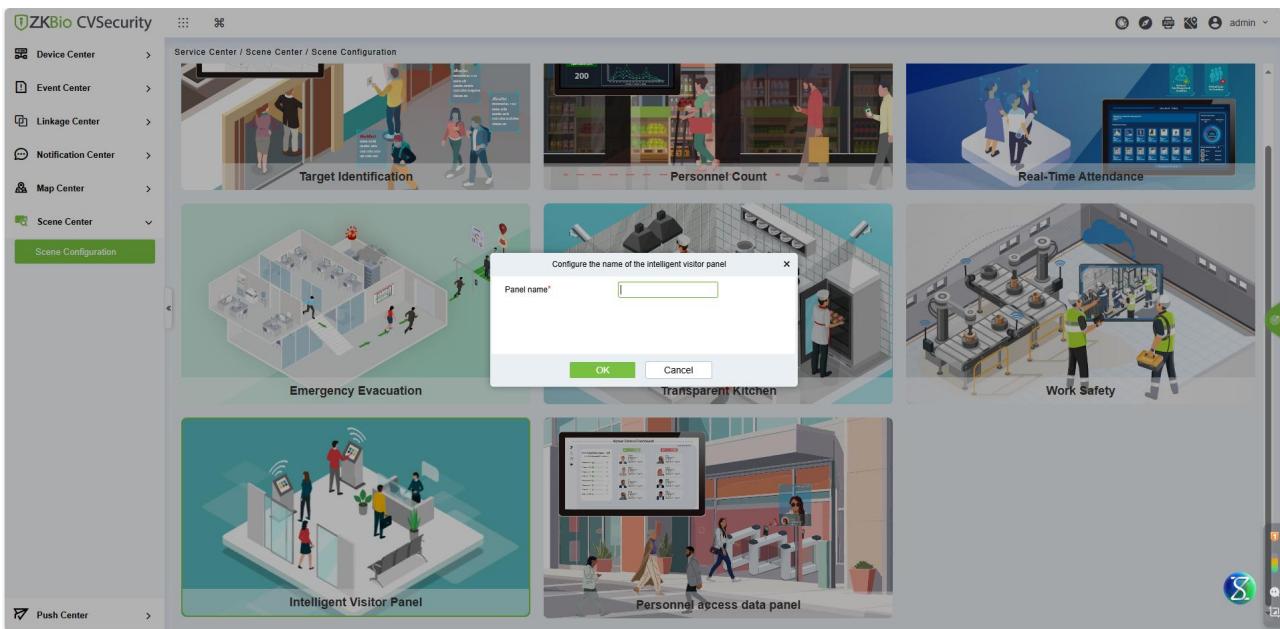
Operating Steps:

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

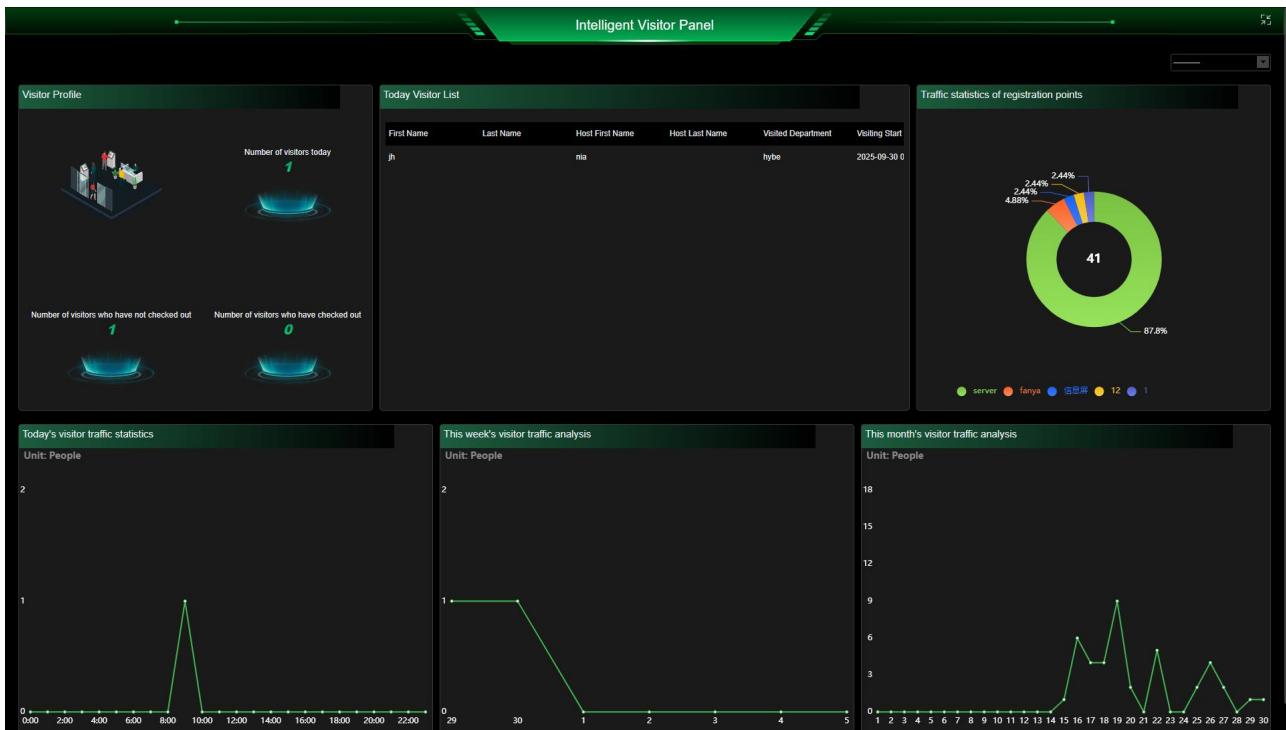


Step1: Configure the name of the intelligent visitor panel

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

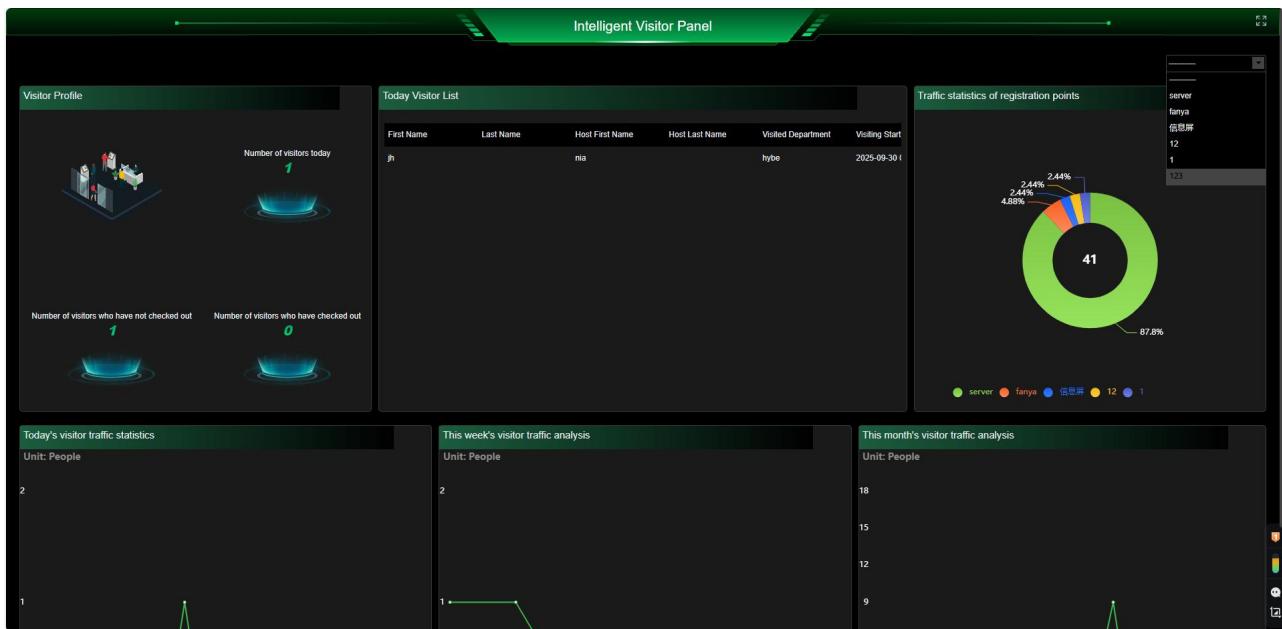


Step2: Return to the Scene Center interface, click to enter the scene, and begin viewing real-time records for this scene, as shown in the figure below:



■ Filtering condition

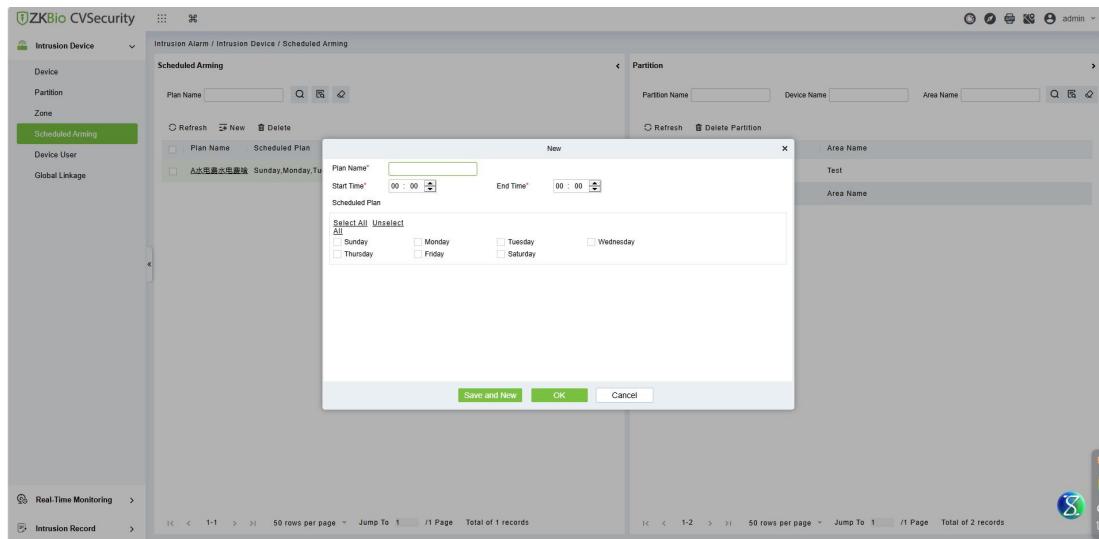
Click the the drop-down box in the upper right corner to select the Visitor Registration Point, as shown in the following figure:



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.

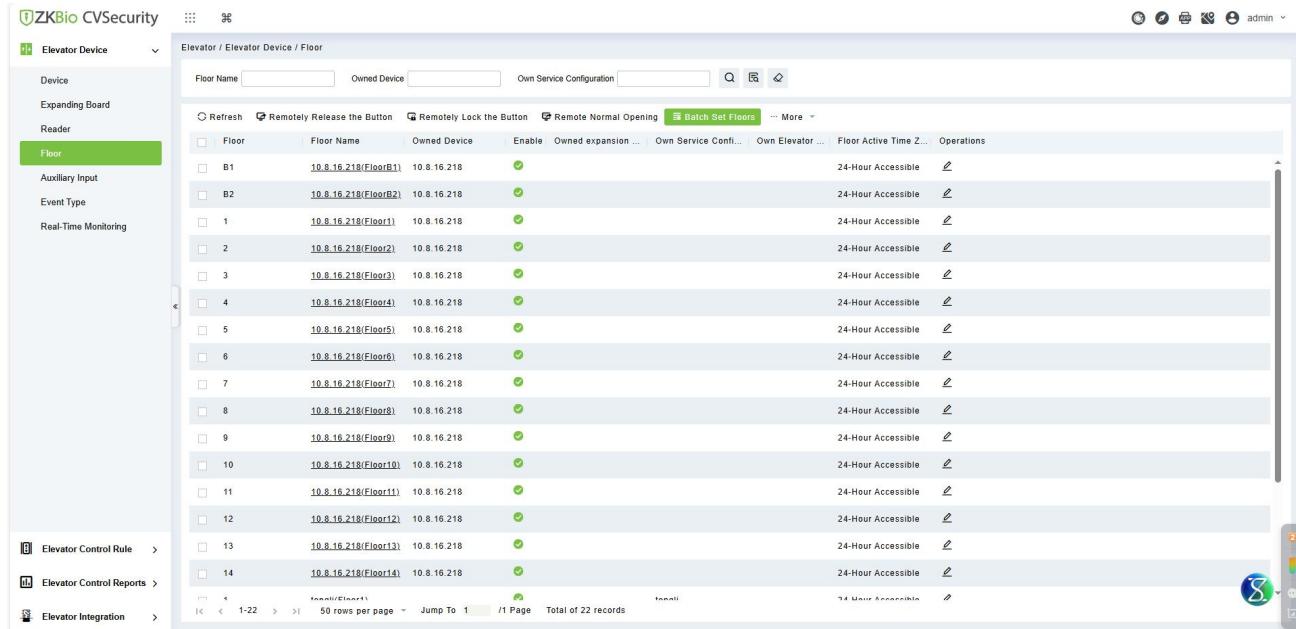


Elevator Control

● DCS function optimized

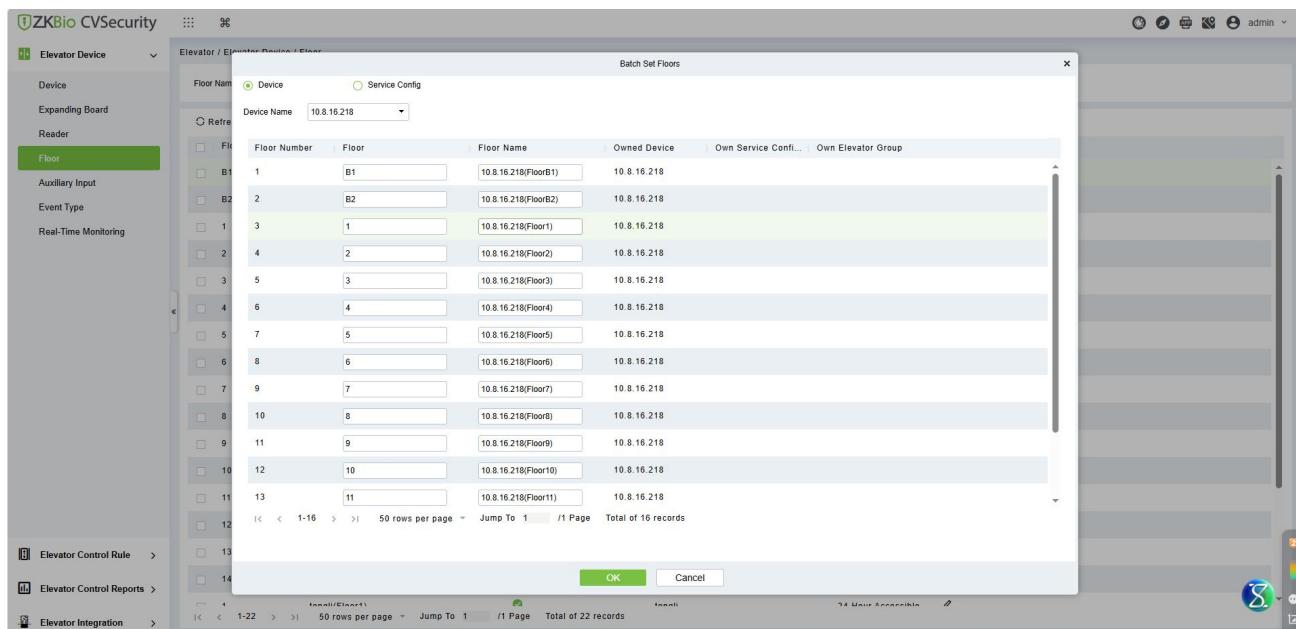
1. Floor has added the function of Batch Set Floors. Solve the problems corresponding to the DCS floor.

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



The screenshot shows the ZKBio CVSecurity software interface. The left sidebar has a 'Floor' category selected. The main panel displays a table of floors for device 10.8.16.218. A green button labeled 'Batch Set Floors' is highlighted in the top right of the table header. The table columns include Floor Number, Floor Name, Owned Device, Enable, Own Service Configuration, Own Elevator Group, Floor Active Time Zone, and Operations. The floor names range from B1 to B14. The 'Operations' column contains icons for edit and delete.

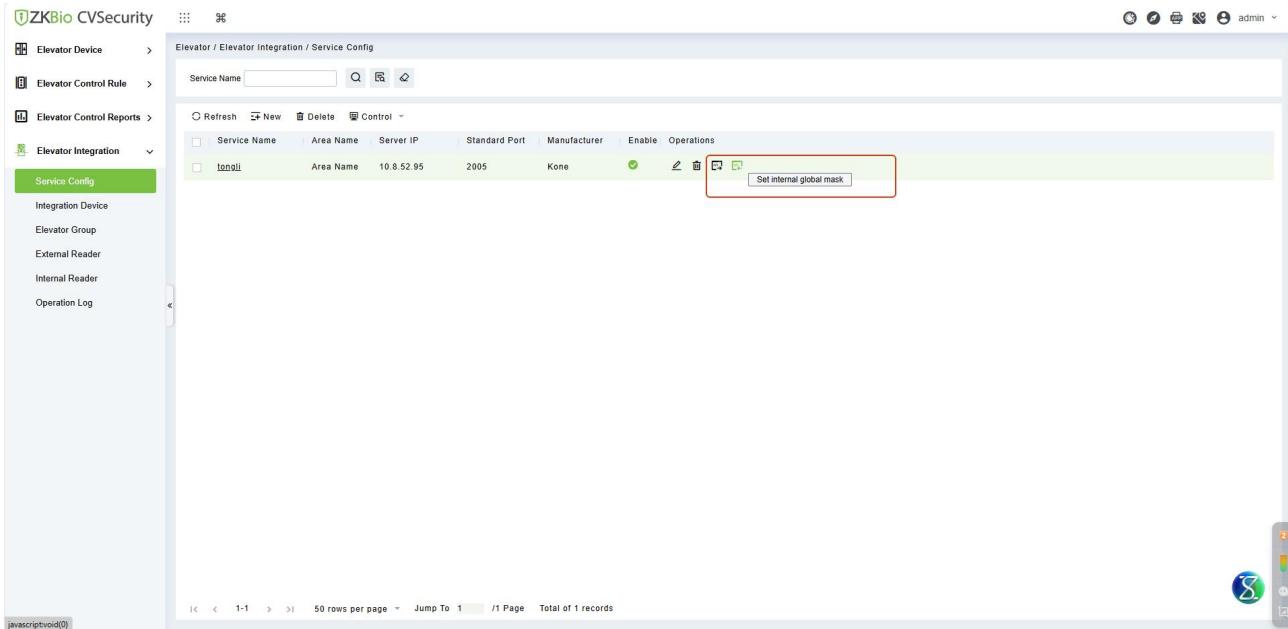
Step2: You can choose to set floors in batches by device or service config, and edit floor and floor name.



The screenshot shows the ZKBio CVSecurity software interface with a 'Batch Set Floors' dialog box overlaid. The dialog box has a 'Device Name' dropdown set to '10.8.16.218'. The main table lists floors 1 through 13, each with a 'Floor Number' and 'Floor Name' (e.g., B1, B2, 1, 2, etc.). The 'Operations' column contains icons for edit and delete. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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.



ZKBio CVSecurity

Elevator / Elevator Integration / Service Config

Service Name: tonli

Set internal global mask

Service Config

Integration Device

Elevator Group

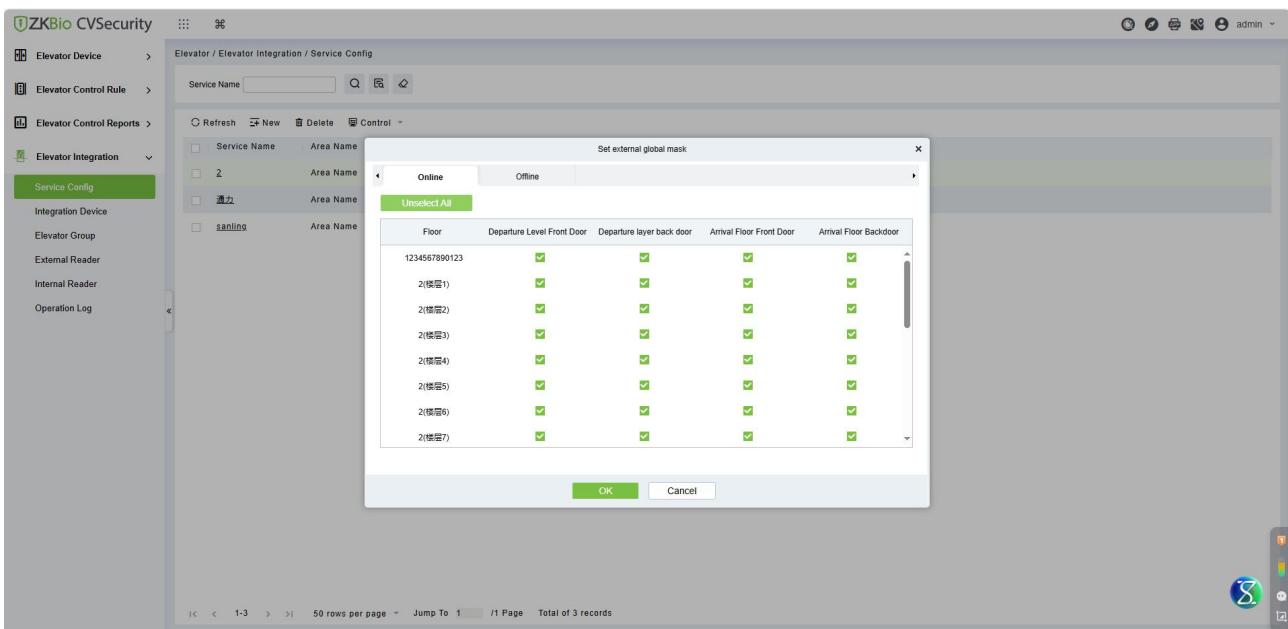
External Reader

Internal Reader

Operation Log

1 < < 1-1 > > 50 rows per page Jump To 1 /1 Page Total of 1 records

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



ZKBio CVSecurity

Elevator / Elevator Integration / Service Config

Service Name: tonli

Set external global mask

Online Offline

Unselect All

Floor	Departure Level Front Door	Departure layer back door	Arrival Floor Front Door	Arrival Floor Backdoor
1234567890123	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层1)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层3)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层4)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层5)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层6)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2(楼层7)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Cancel

1 < < 1-3 > > 50 rows per page Jump To 1 /1 Page Total of 3 records

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

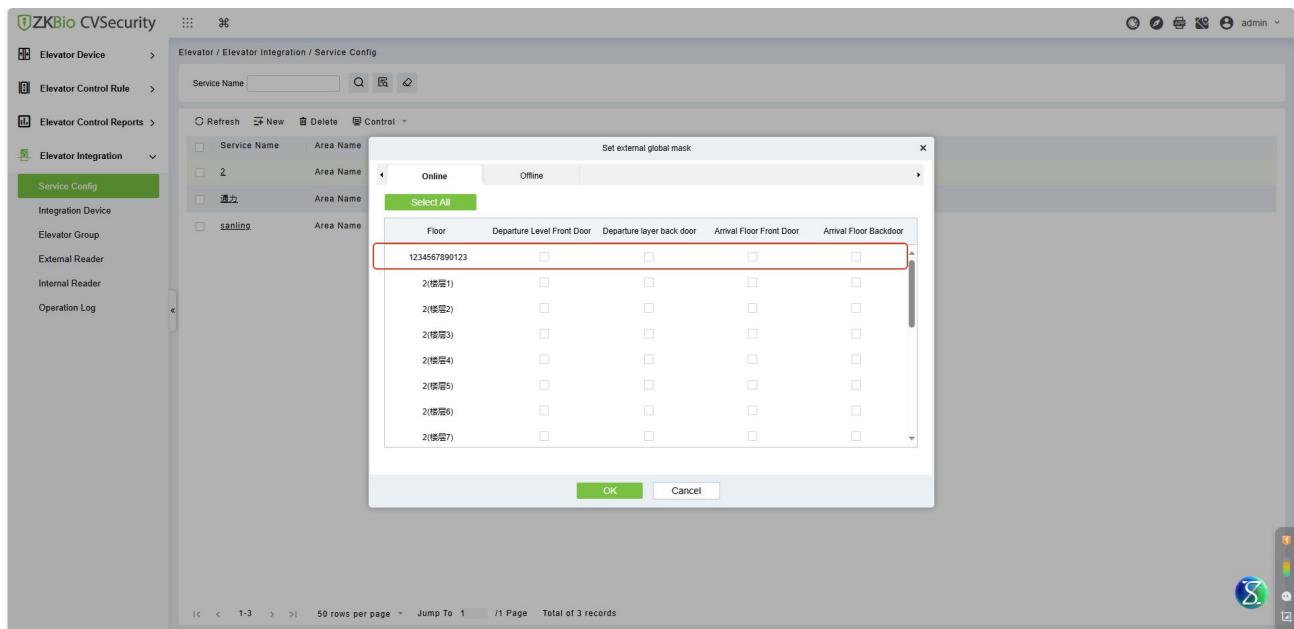
Step: Enter Elevator → Elevator Integration → Service Config, select the service, then click "Control" → "Clear External Global Mask" or "Clear Internal Global Mask" to complete the mask clearing operation.

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

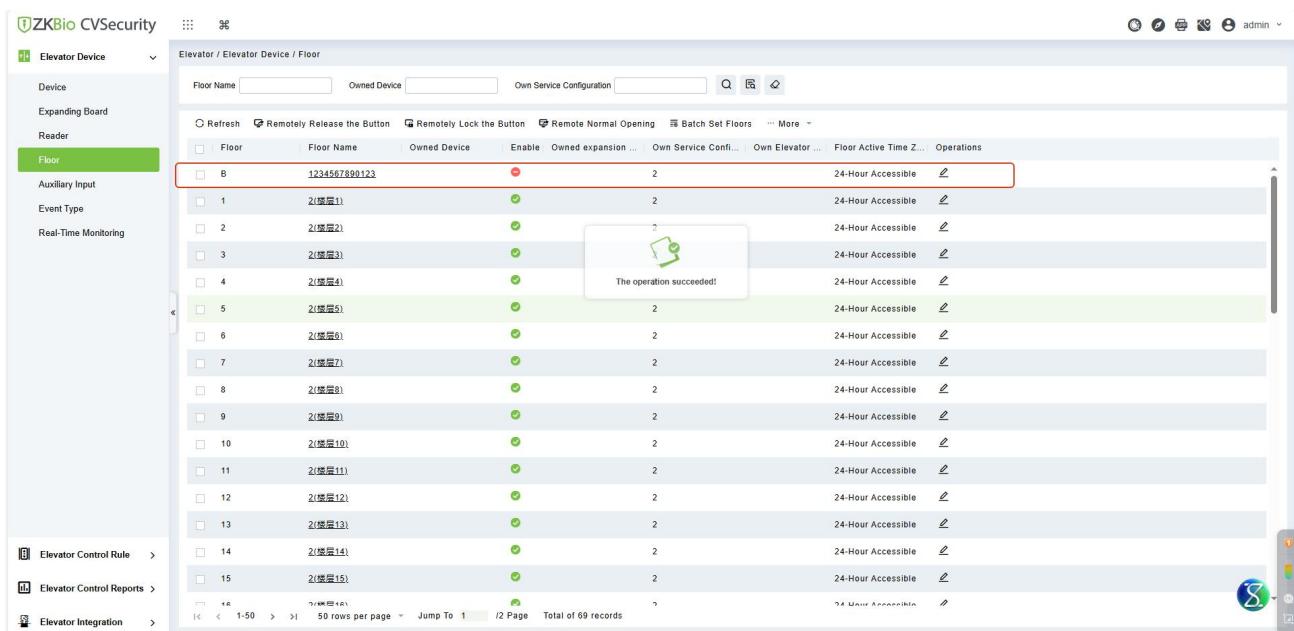
Step: Enter Elevator → Elevator Device → Floor. In the search bar, you can search for floors through the Own Service Configuration.

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

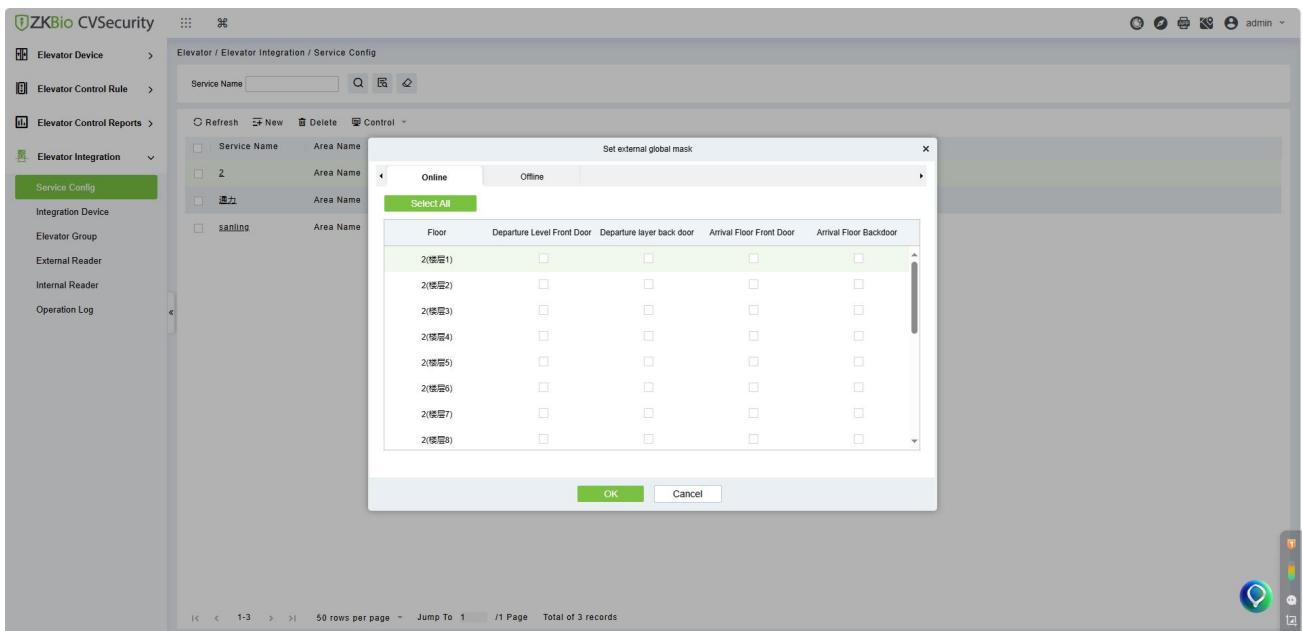
Step1: Enter Elevator → Elevator Integration → Service Config, click the mask setting icon in the operation column, and you can view and edit all enabled floors.



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



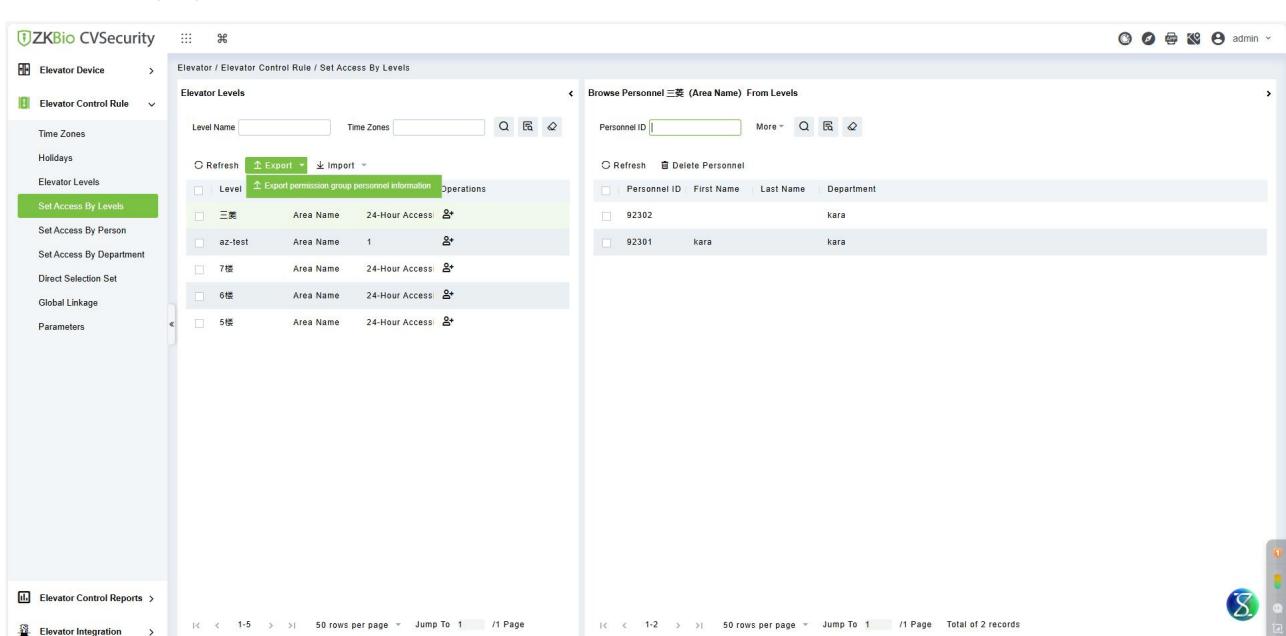
Step3: Return to Elevator → Elevator Integration → Service Config, click the mask setting icon in the operation column. Floors that have been disabled will not appear in the mask configuration menu.



- 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.

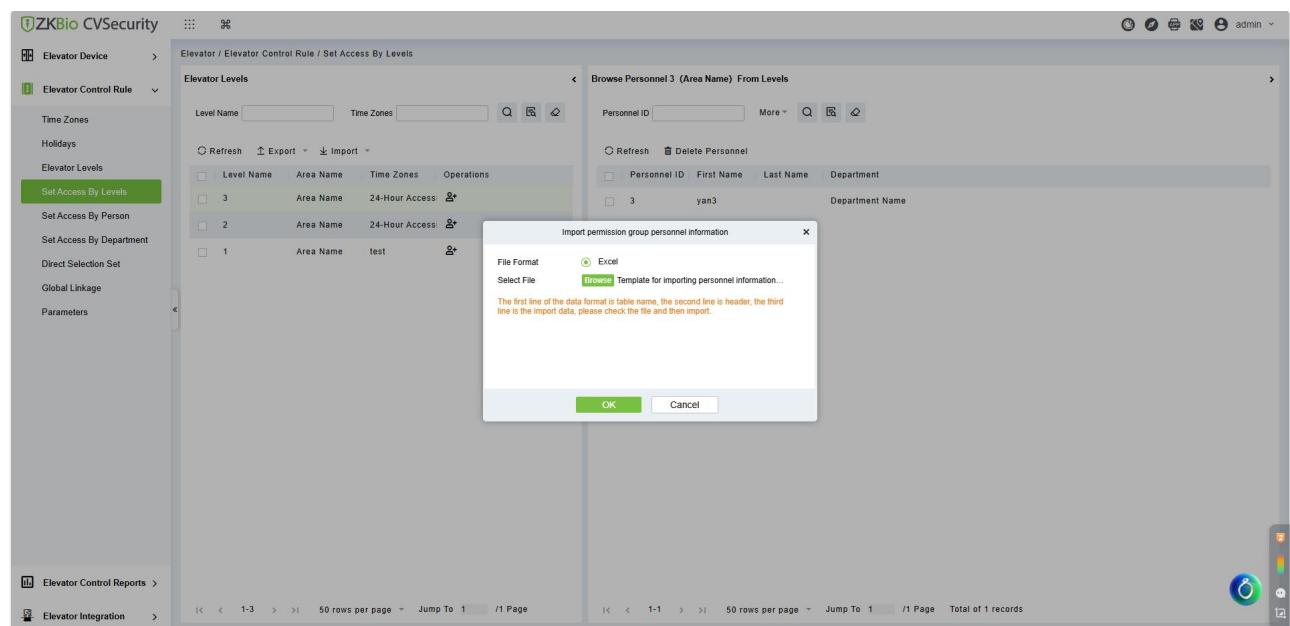
Note: Before entering data in the template, review the cell comments for formatting requirements.

Cells with red triangles contain important annotations—click them to view data entry guidelines.

Template for importing personnel information of elevator control permission group

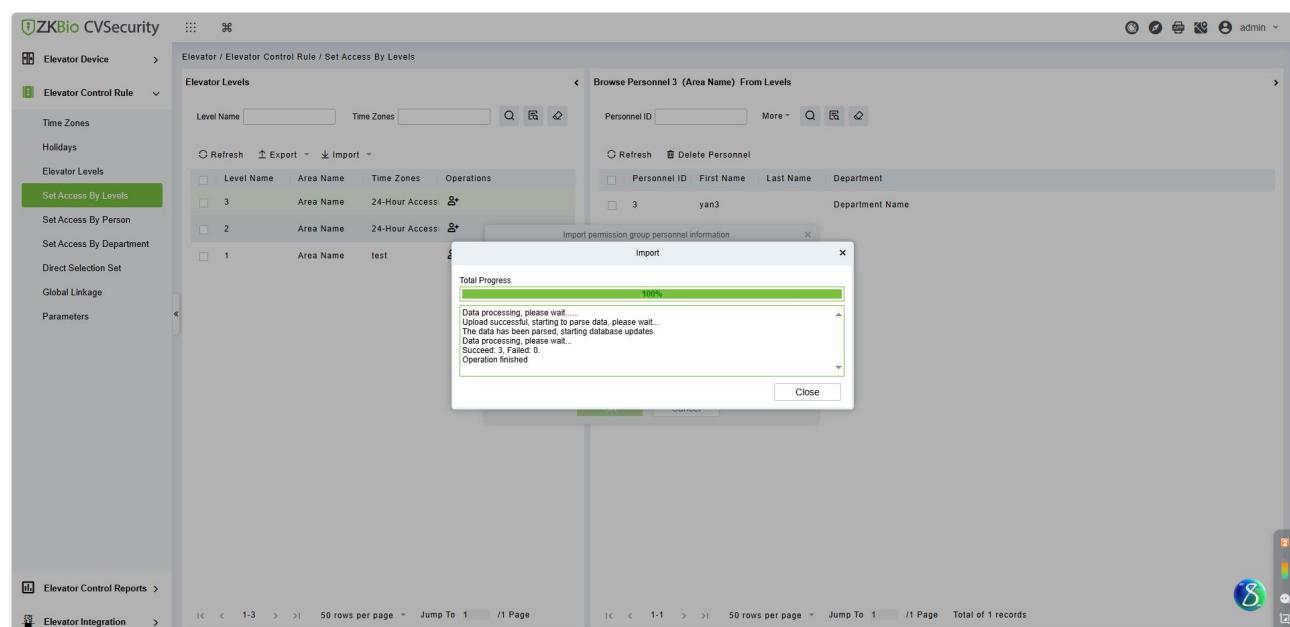
Level Name	Personnel ID	First Name	Last Name
1		1 yan1	
2		2 yan2	
3		3 yan3	

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".



The screenshot shows the ZKBio CVSecurity software interface. On the left, there is a navigation sidebar with various options like 'Elevator Device', 'Elevator Control Rule', 'Elevator Levels', 'Set Access By Levels' (which is currently selected and highlighted in green), and 'Elevator Control Reports'. The main content area is titled 'Elevator / Elevator Control Rule / Set Access By Levels'. It displays two tables: 'Elevator Levels' and 'Browse Personnel 3 (Area Name) From Levels'. A modal dialog box is open in the center, titled 'Import permission group personnel information'. It contains a radio button for 'File Format' (set to 'Excel') and a 'Select File' button with the path 'Template for importing personnel information...'. Below the file path, there is a note: 'The first line of the data format is table name, the second line is header, the third line is the import data, please check the file and then import.' At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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



The screenshot shows the ZKBio CVSecurity software interface again. The 'Set Access By Levels' screen is visible in the background. A modal dialog box is open in the foreground, titled 'Import'. It shows a progress bar at 100%. Below the progress bar, there is a message: 'Data processing, please wait... Upload successful, starting to parse data, please wait... The data has been parsed, starting database updates... Data processing, please wait... Succeeded: 3, Failed: 0. Operation finished.' At the bottom of the dialog is a 'Close' button.

- 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.



The screenshot shows a software interface for managing holidays. At the top, there are buttons for Refresh, New, Delete, Import, Export, and Download import template. The 'Download import template' button is highlighted with a red box. Below the buttons is a table header with columns: Holiday Name, Holiday Type, Start Date, End Date, Recurring, Remarks, and Operations. Under the Holiday Name column, there is a row for 'holiday1' with a checkmark. The table shows the following data:

Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks	Operations
holiday1	Holiday Type 1	2025-09-02	2025-09-03	No		 

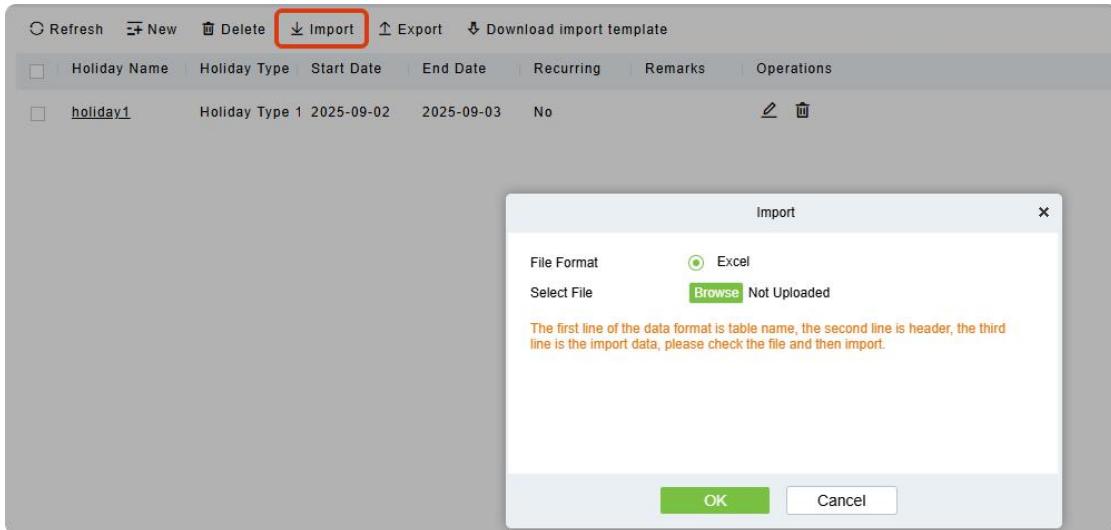
Step 2: Open the exported template file "Holiday Template.xls" for adding holiday information.

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.



The screenshot shows the 'Import' dialog box overlaid on the Holiday Management interface. The dialog box has the following fields:

- File Format: Excel (radio button selected)
- Select File: Browse (button) Not Uploaded (text)
- Note: The first line of the data format is table name, the second line is header, the third line is the import data, please check the file and then import.

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

■ Export:

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

Refresh

<input type="checkbox"/>	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks	Operations
<input type="checkbox"/>	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No		

Export

User Password*

File encryption Yes No

File encryption password*

File Format

Data to Export All (max 100000 records) Selected (max 100000 records)

Start Position

Total Records

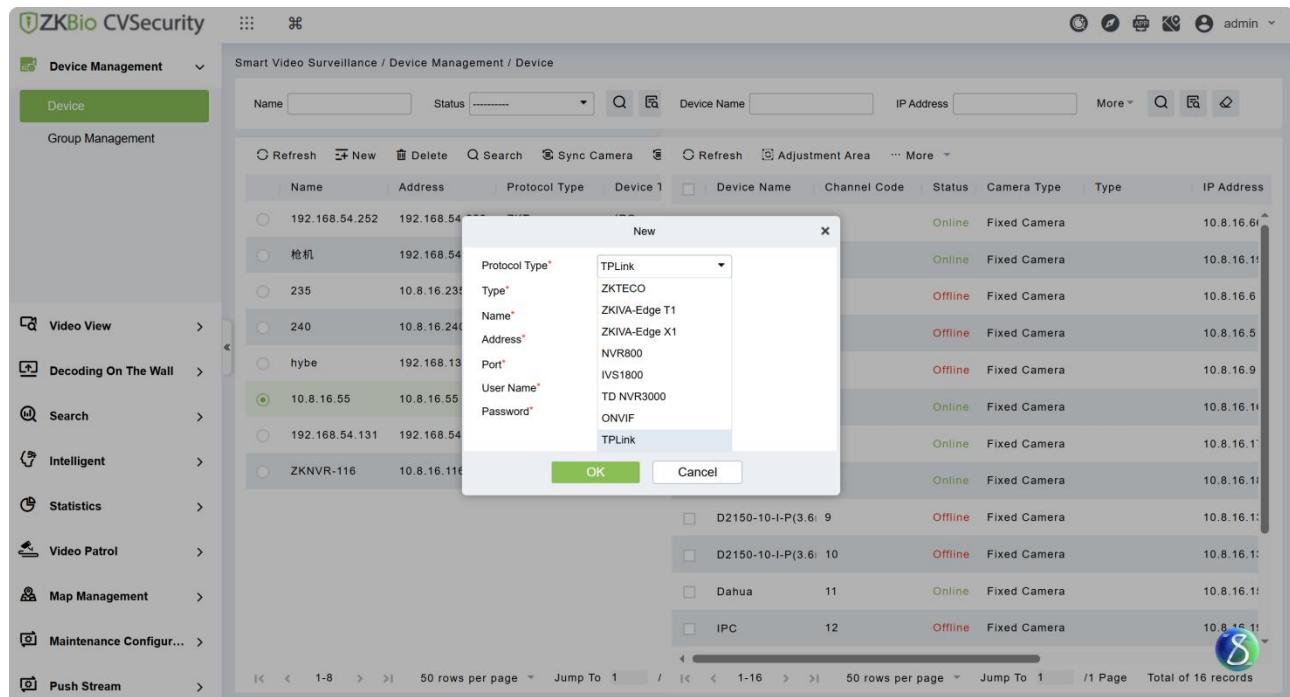
1	Holidays					
2	Holiday Name	Holiday Type	Start Date	End Date	Recurring	Remarks
3	holiday1	Holiday Type 1	2025-09-02	2025-09-03	No	
4						

Smart Video Surveillance

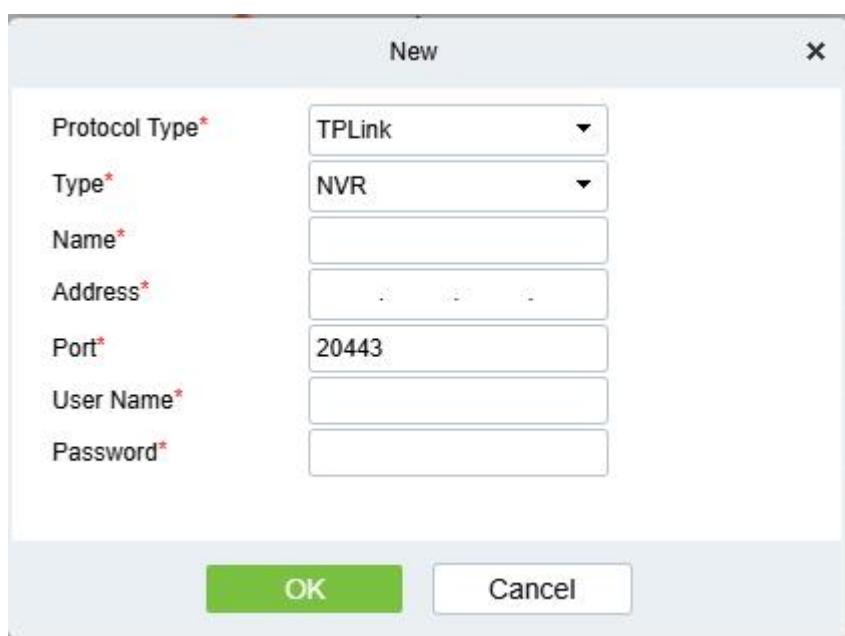
- Integrated with TP-Link NVR to enable preview, playback, intelligent alert display, and alarm linkage.

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.



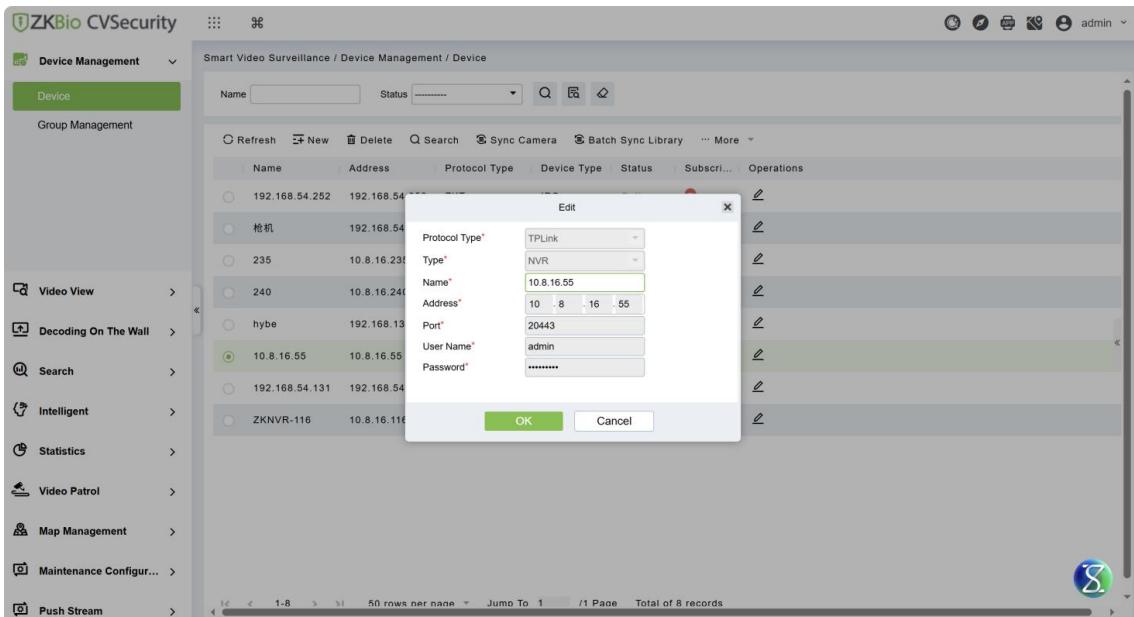
Step2: You can choose NVR devices based on the TP-Link protocol.



The description of each parameter is shown in Table.

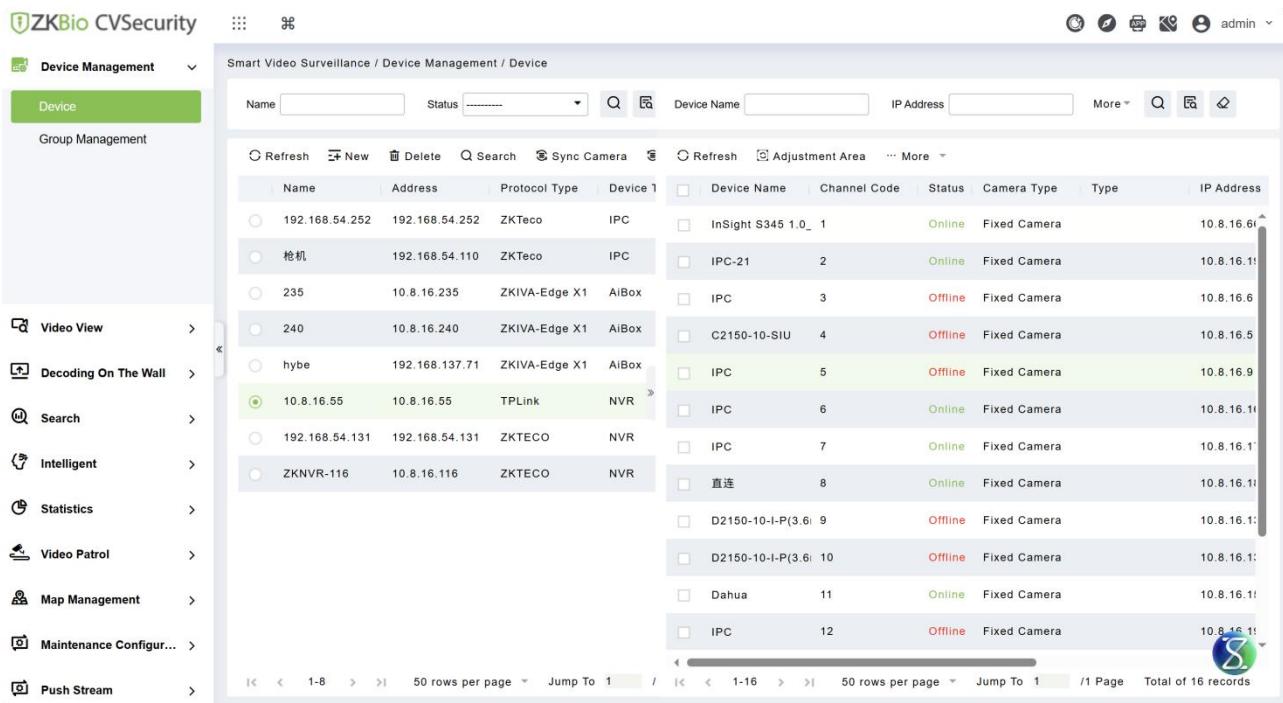
Parameters/Buttons	Description
Type	Select the device type.
Protocol Type	Select the type of protocol.
Name	Customize the device name.
Port	Configure the device port.TPLink NVR default is 20443.
Address	Configure the device address. The format is: xxx.xxx.xxx.xxx, for example: 192.168. 6.5
Username & Password	The NVR'S user name and password. Note: For TPLink NVR, the default account is (admin,Admin@135)

Step 3: Click OK.



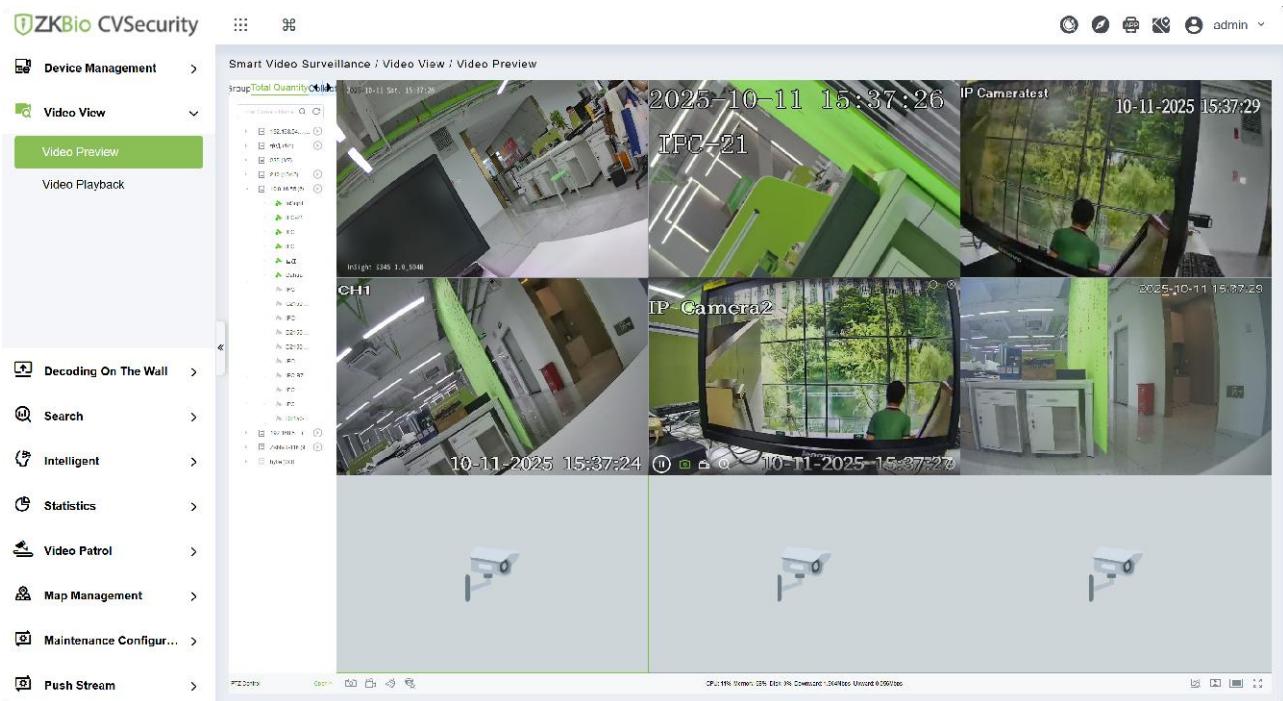
Step 4: Add IPCs on the NVR client.

The software interface will automatically synchronize the added camera devices.



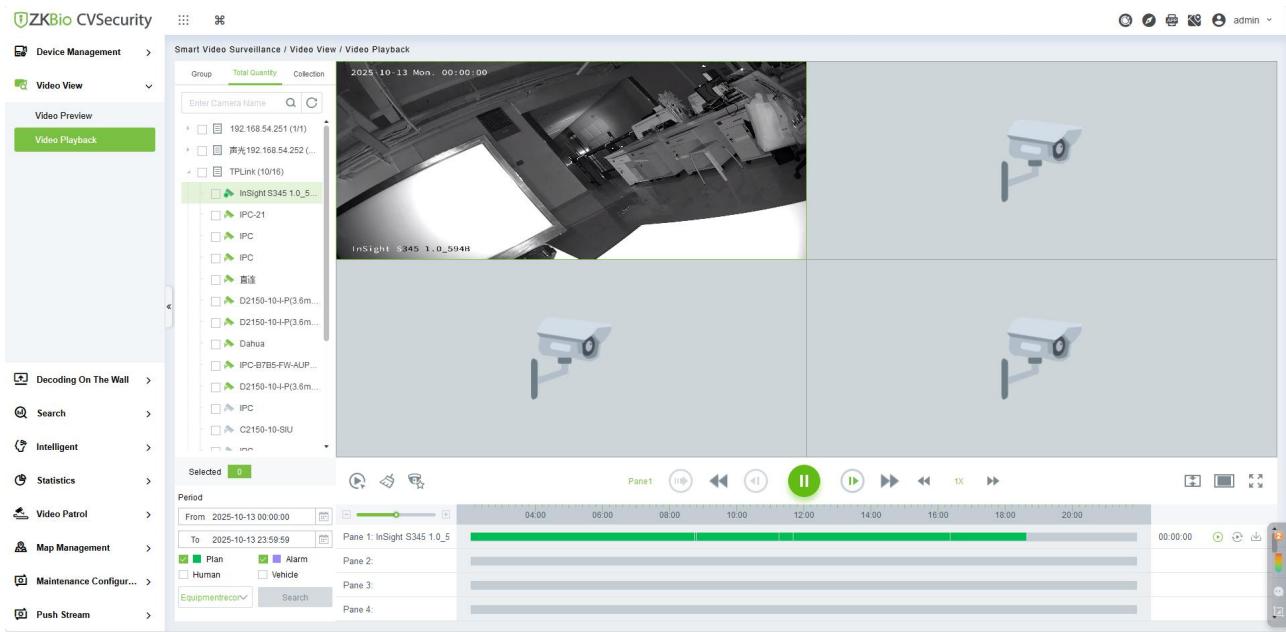
Enter Smart Video Surveillance > Video View > Video Preview.

You can view the video preview here.



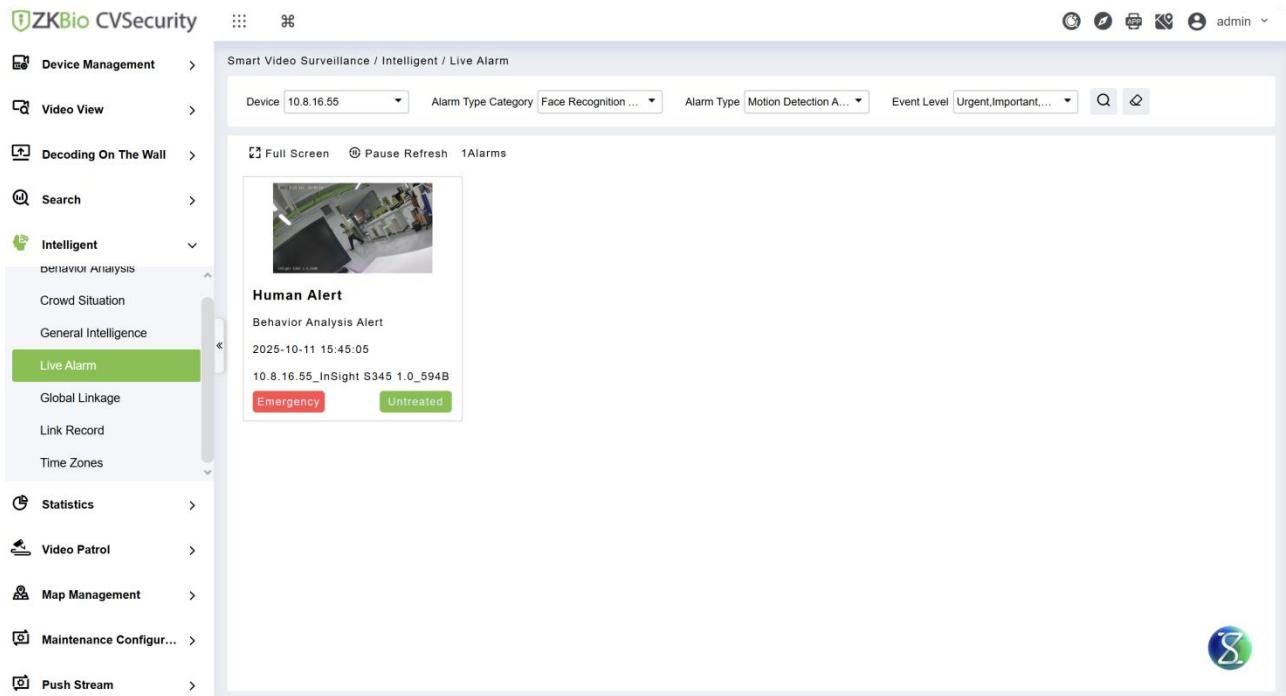
Enter Smart Video Surveillance > Video View > Video Playback.

You can view the video replay here.

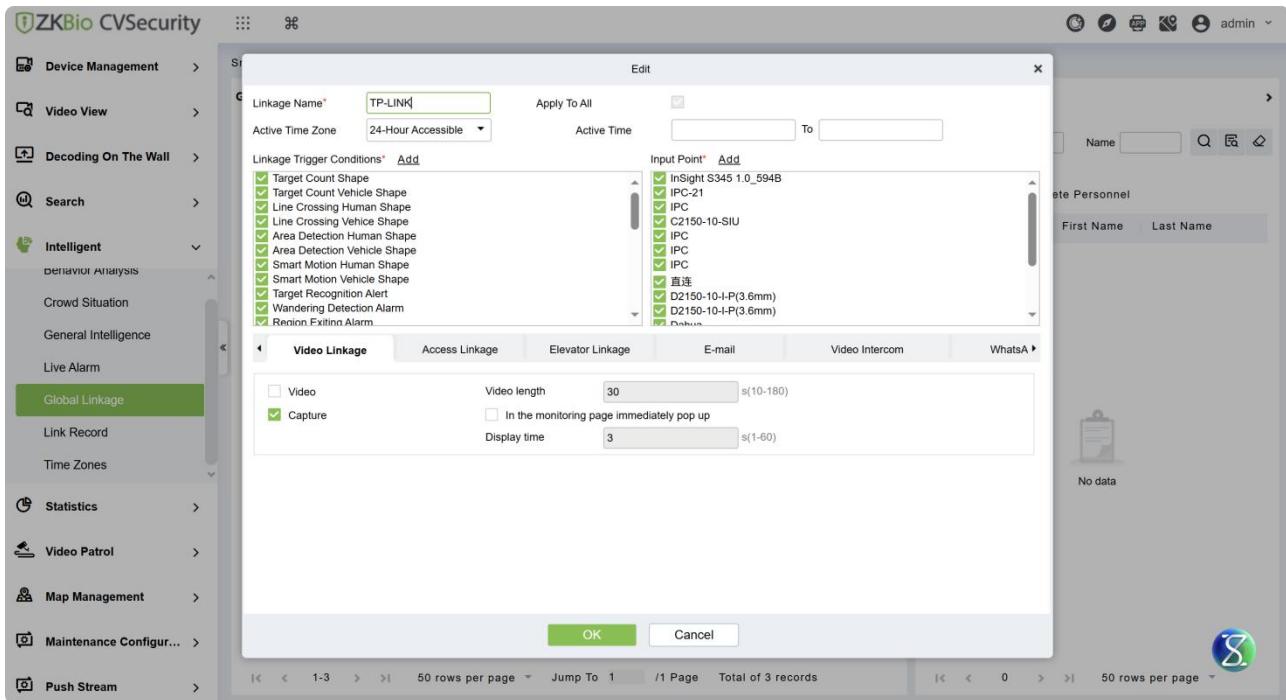


Enter Smart Video Surveillance > Intelligent > Live Alarm.

You can view real-time video alarm monitoring here.

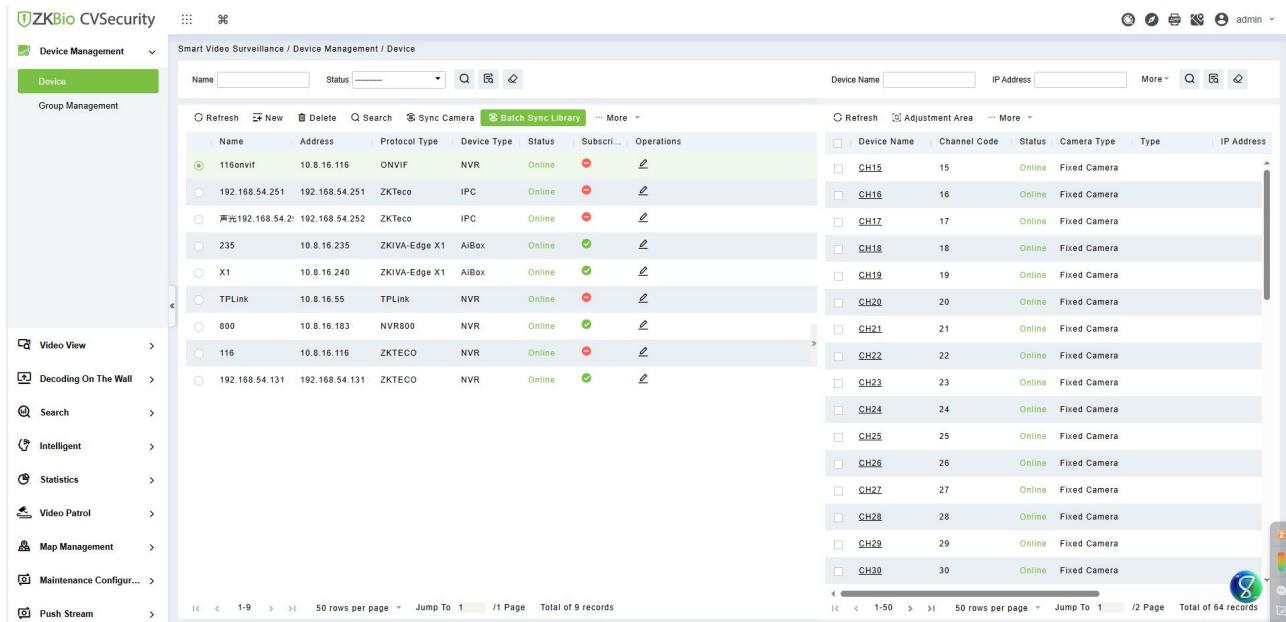


Enter Smart Video Surveillance > Intelligent > Global Linkage, click New to set the video linkage.



- **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".

The screenshot shows the ZKBio CVSecurity Device Management interface. On the left, there's a sidebar with various management options like Video View, Decoding On The Wall, and Statistics. The main area is titled 'Smart Video Surveillance / Device Management / Device'. A central dialog box is open, titled 'Resynchronize list library'. It lists devices to be synchronized: 116onvif, 192.168.54.251, 235, X1, TPLink, 800, 116, and 192.168.54.131. Below this is an 'Alternative' section with options like 'List Library...', 'Visitor Forbid...', 'Forbidden List...', 'Pass List...', and 'Allow List...'. On the right, a list of 64 cameras is shown with columns for Channel Code, Status, Camera Type, Type, and IP Address. The status for most cameras is 'Online' and 'Fixed Camera'. At the bottom of the dialog, there are 'Next Step' and 'Cancel' buttons.

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.

This screenshot is similar to the previous one but shows two devices selected for synchronization: 116onvif and 235. The 'Selected' section in the dialog shows these two devices. The 'OK' button is highlighted in green at the bottom of the dialog. The rest of the interface and the camera list on the right are identical to the first screenshot.

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

This screenshot shows the processing of a command. A dialog box is centered, titled 'Processing command'. It displays a progress bar with the text 'The progress of the current device' and 'Total Progress' both at 100%. Below the progress bar, it says 'Start processing X1 of Visitor Forbidden List successfully' and 'Complete'. At the bottom of the dialog, there are 'Suspend Close' and 'Close' buttons. The background shows the same device management interface with a list of cameras and their details.

● Support linkage with IPC (access control or video linkage with IPC).

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

The image consists of three vertically stacked screenshots of the ZKBio CVSecurity software interface, specifically the 'Device Management / Device' and 'Access / Device Management / Reader' sections.

Screenshot 1: Device Management / Device

This screenshot shows a list of devices. A specific entry for an 'IPC' device, '10.8.16.21' (ZKTeco), is highlighted with a red box. The interface includes search, filter, and operation buttons for each device entry.

Screenshot 2: Access / Device Management / Reader

This screenshot shows a list of readers. A specific entry for a reader, '10.8.16.155-3-In', is highlighted with a red box. A modal dialog box titled 'Binding/unbinding the camera' is open, showing a list of cameras. One camera entry, 'CH1 10.8.16.21 056be00020010', is highlighted with a red box. The 'Selected(0)' section of the dialog is empty.

Screenshot 3: Access / Device Management / Reader

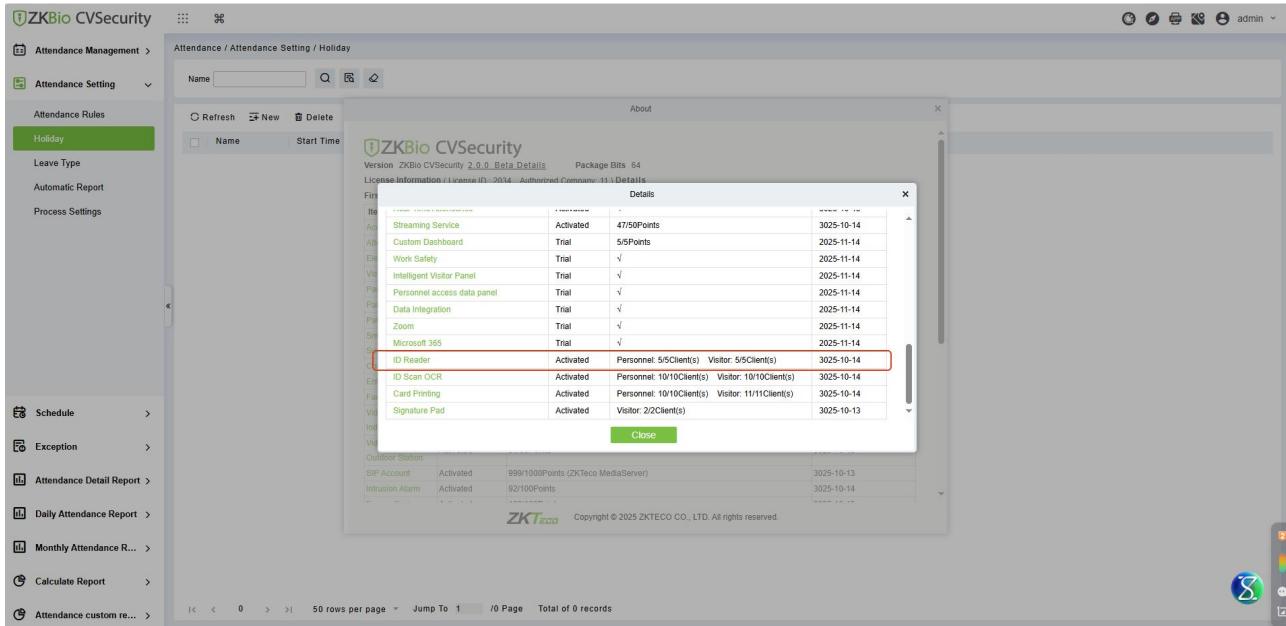
This screenshot is similar to the second one, showing the same list of readers and the same modal dialog box. A different camera entry, 'CH2 192.168.54.131 dtf3921386734', is highlighted with a red box in the list. The 'Selected(0)' section of the dialog is empty.

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

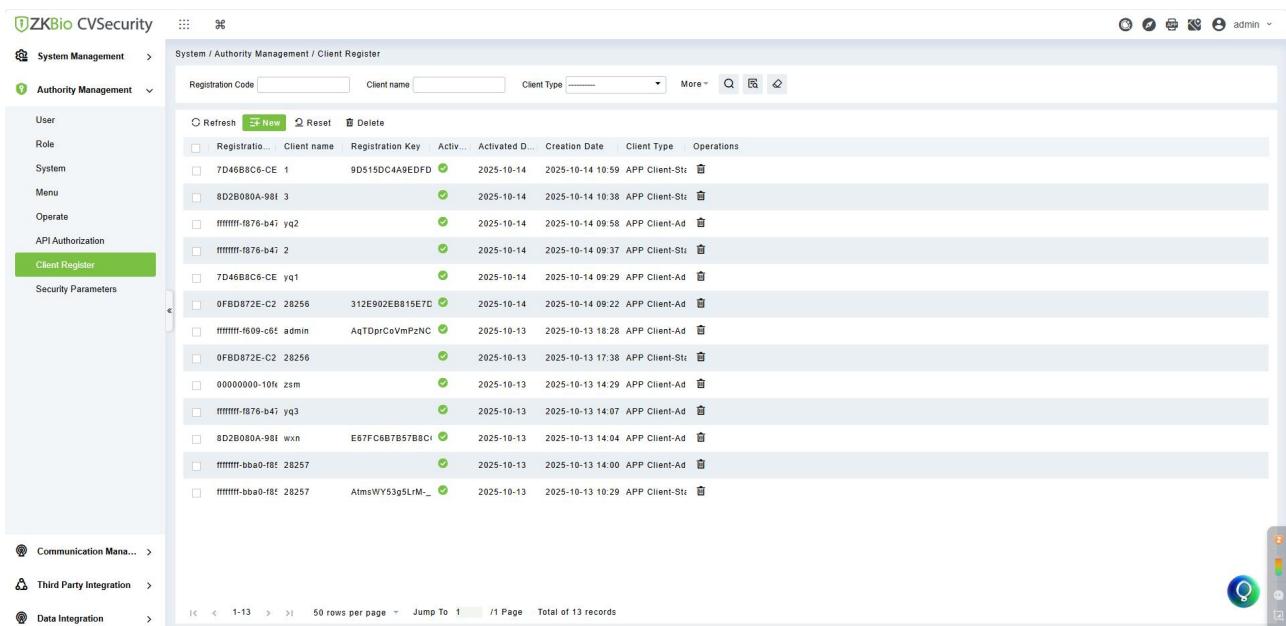
● Supports reading Malaysian ID cards via the RS100 passport scanner.

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



Item	Status	Activated	Details
Streaming Service	Activated	47/50Points	3025-10-14
Custom Dashboard	Trial	5/5Points	2025-11-14
Work Safety	Trial	✓	2025-11-14
Intelligent Visitor Panel	Trial	✓	2025-11-14
Personnel access data panel	Trial	✓	2025-11-14
Data Integration	Trial	✓	2025-11-14
Zoom	Trial	✓	2025-11-14
Microsoft 365	Trial	✓	2025-11-14
ID Reader	Activated	Personnel: 5/5Client(s) Visitor: 5/5Client(s)	3025-10-14
ID Scan OCR	Activated	Personnel: 10/10Client(s) Visitor: 10/10Client(s)	3025-10-14
Card Printing	Activated	Personnel: 10/10Client(s) Visitor: 11/11Client(s)	3025-10-14
Signature Pad	Activated	Visitor: 2/2Client(s)	3025-10-13

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



Registration Code	Client name	Registration Key	Activ...	Activated D...	Creation Date	Client Type	Operations
7D468BC6-CE_1	9D515D04A9EDFD	✓	2025-10-14	2025-10-14 10:59	APP Client-Std		
8D2B080A-981 3		✓	2025-10-14	2025-10-14 10:38	APP Client-Std		
fffff-f876-b47_yq2		✓	2025-10-14	2025-10-14 09:58	APP Client-Ad		
fffff-f876-b47_2		✓	2025-10-14	2025-10-14 09:37	APP Client-Std		
7D468BC6-CE_yq1		✓	2025-10-14	2025-10-14 09:29	APP Client-Ad		
0FBD872E-C2_28256	312E902EB815ED	✓	2025-10-14	2025-10-14 09:22	APP Client-Ad		
fffff-f609-c65 admin	AqTDprCoVmPzNC	✓	2025-10-13	2025-10-13 18:28	APP Client-Ad		
0FBD872E-C2_28256		✓	2025-10-13	2025-10-13 17:38	APP Client-Std		
00000000-10k_zsm		✓	2025-10-13	2025-10-13 14:29	APP Client-Ad		
fffff-f876-b47_yq3		✓	2025-10-13	2025-10-13 14:07	APP Client-Ad		
8D2B080A-981 wxn	E67FC6B7B57BBC	✓	2025-10-13	2025-10-13 14:04	APP Client-Ad		
fffff-bba0-f8c_28257		✓	2025-10-13	2025-10-13 14:00	APP Client-Ad		
fffff-bba0-f8c_28257	AtmsWY53g5LrM_-	✓	2025-10-13	2025-10-13 10:29	APP Client-Std		

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

System Management > Authority Management > Client Register

Client Type: OCR-Personnel

Registration Code: C282F9

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.

Personnel / Personnel / Parameters

Facial Backend Comparison Server

Enable facial backend comparison:
Yes (radio button selected)

Registration Client

Device Driver

Certificate Recognition Driver Installation Status: Detected Certificate Recognition Driver is not installed

Card Printer Driver Installation Status: Detected Card Printer Driver is not installed

Certificate Recognition

OCR (radio button selected)

Registration Code*

Register

Download OCR V1.0 Driver

Download OCR V2.0 Driver

Certificate No. Automatic Backfill Type

Document No. (radio button selected)

Personal No.

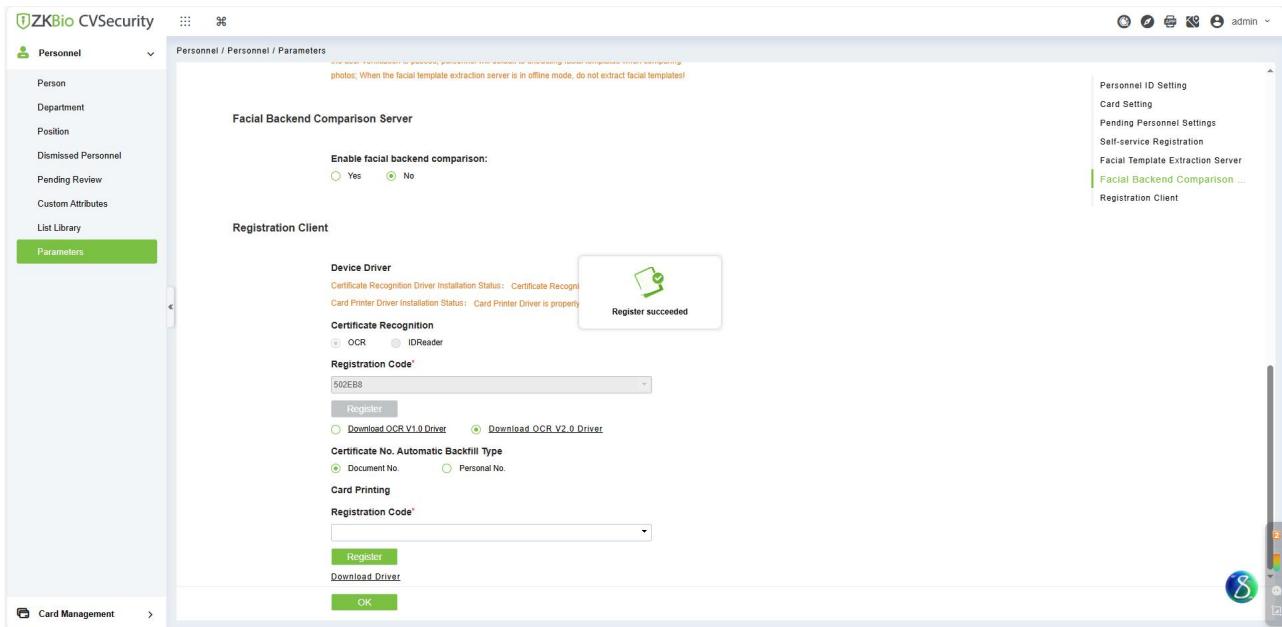
Card Printing

Registration Code*

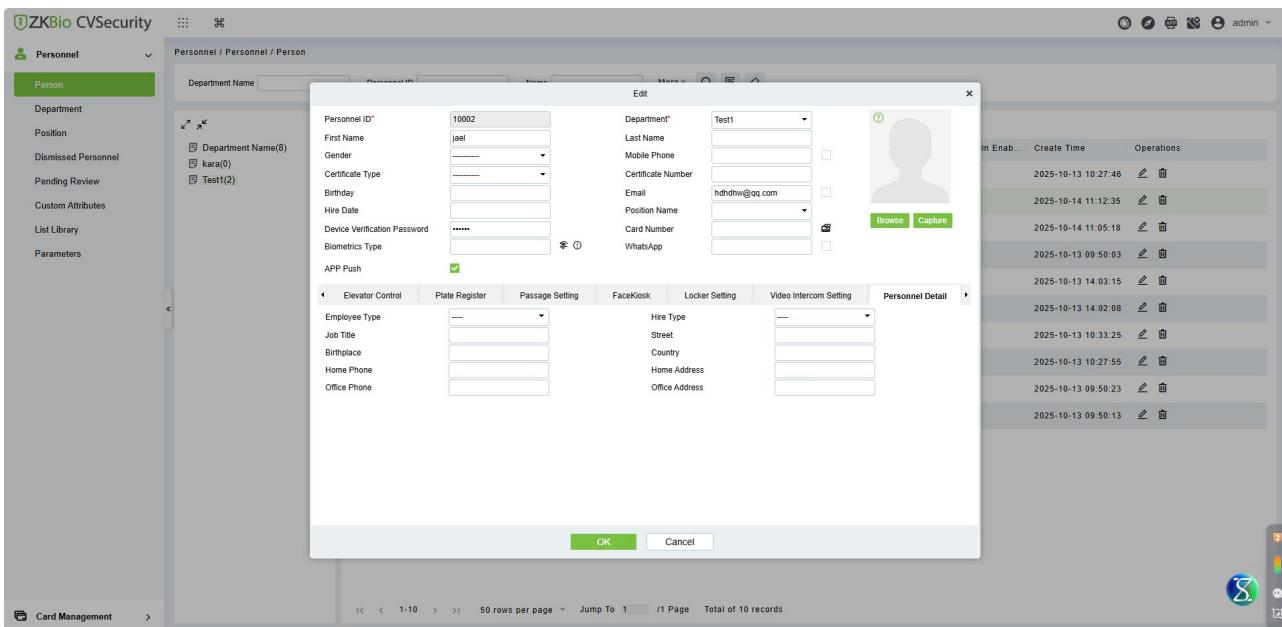
Register

Download Driver

OK



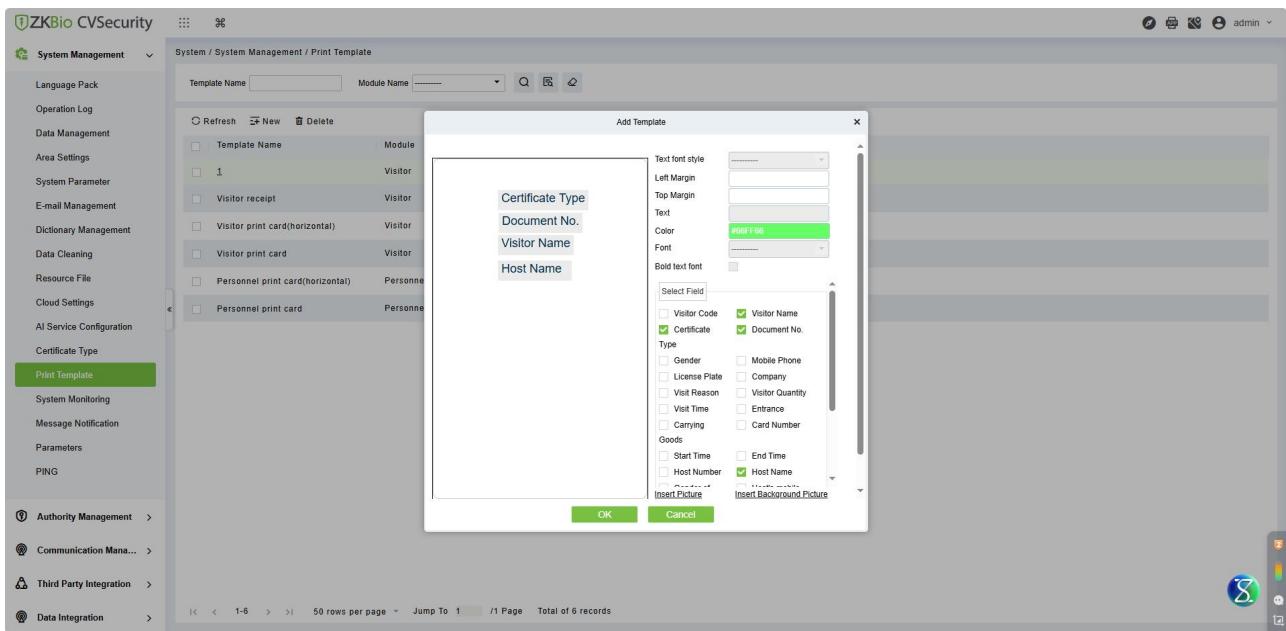
Step4: Scanning with the RS100 passport scanner can automatically extract and fill in the person's headshot, name, date of birth, certificate number and home address.



● Card Printing Template Optimized.

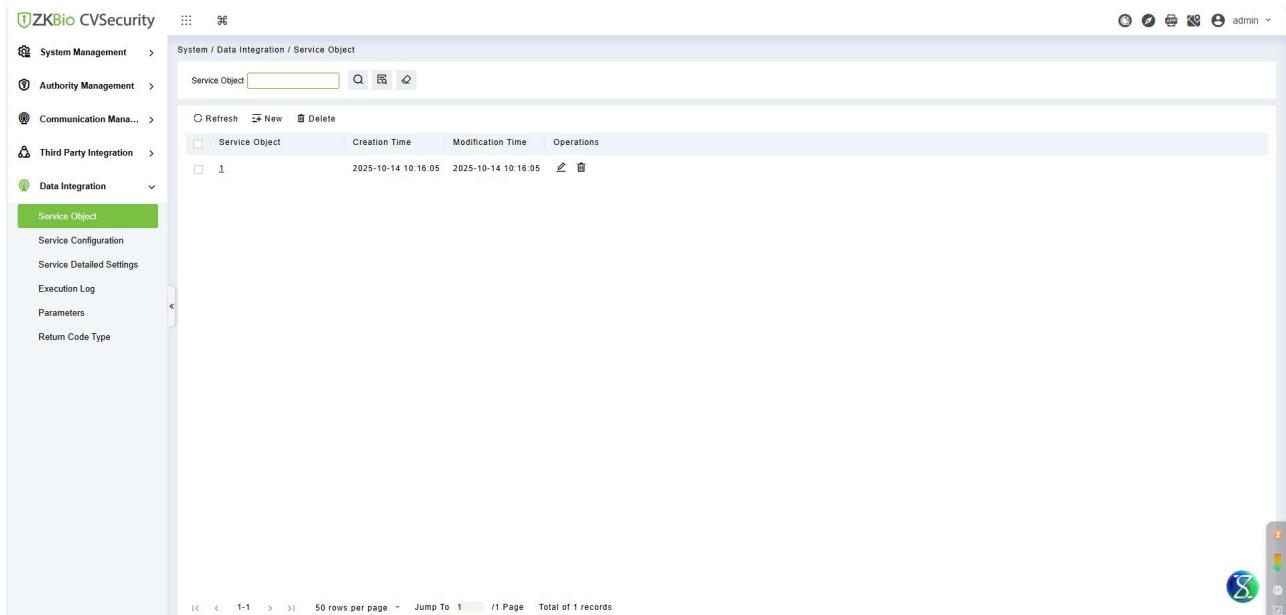
Step: Enter System→ System Management → Print Template , and the interface for adding a new template is shown in the figure below:

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.

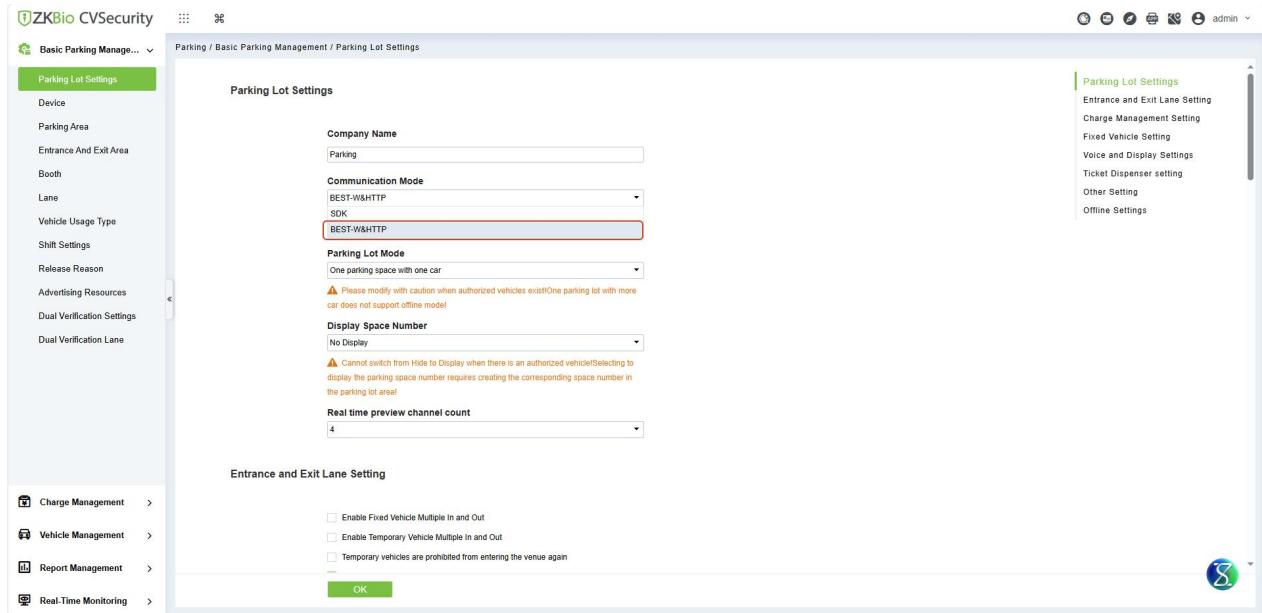


Note: For detailed configuration steps, please refer to the ZKBio CVSecurity 6.7.0 UM_EN.

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.

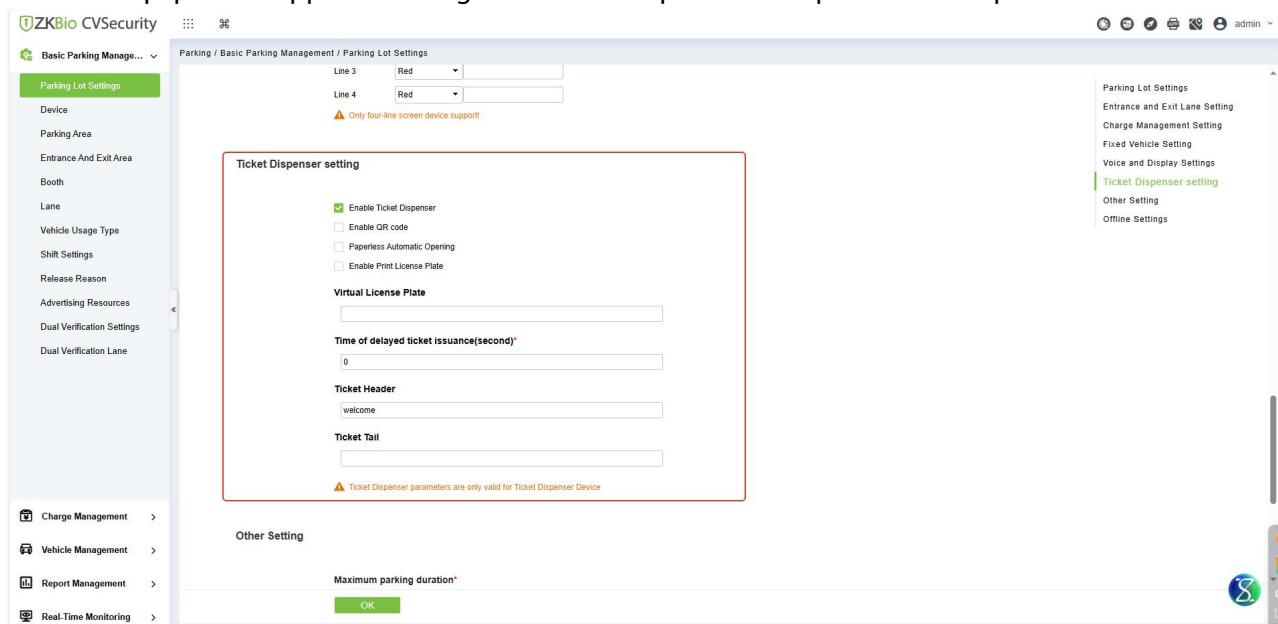


The screenshot shows the ZKBio CVSecurity software interface. The main window is titled 'Parking / Basic Parking Management / Parking Lot Settings'. On the left, there is a sidebar with various management options: Basic Parking Management, Parking Lot Settings (selected), Device, Parking Area, Entrance And Exit Area, Booth, Lane, Vehicle Usage Type, Shift Settings, Release Reason, Advertising Resources, Dual Verification Settings, and Dual Verification Lane. The 'Parking Lot Settings' section contains fields for 'Company Name' (set to 'Parking'), 'Communication Mode' (set to 'BEST-W&HTTP'), 'Parking Lot Mode' (set to 'One parking space with one car'), 'Display Space Number' (set to 'No Display'), and 'Real time preview channel count' (set to '4'). A note in the 'Display Space Number' field says: 'Please modify with caution when authorized vehicles exist! One parking lot with more car does not support offline mode!'. Another note in the 'Display Space Number' field says: 'Cannot switch from Hide to Display when there is an authorized vehicle! Selecting to display the parking space number requires creating the corresponding space number in the parking lot area!'. The right side of the interface shows a vertical sidebar with 'Parking Lot Settings' and other settings like 'Entrance and Exit Lane Setting', 'Charge Management Setting', 'Fixed Vehicle Setting', 'Voice and Display Settings', 'Ticket Dispenser setting', 'Other Setting', and 'Offline Settings'. At the bottom right, there is a status bar with a battery icon and a 'OK' button.

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

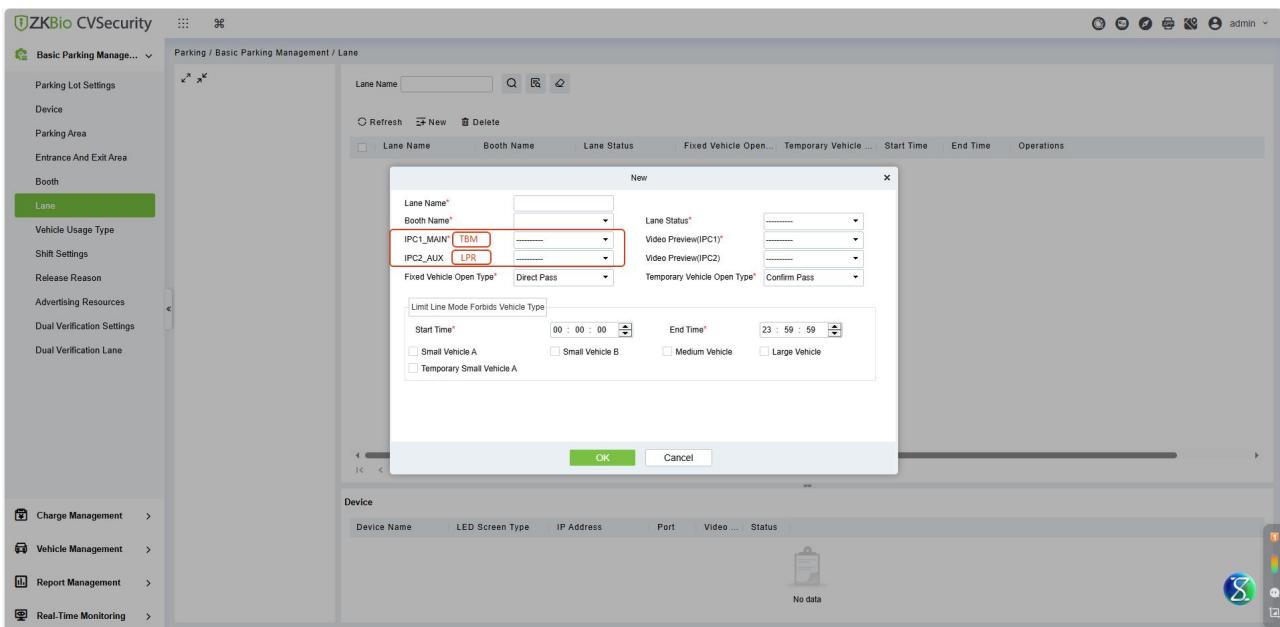
In the case of lost receipts, payment can be made by checking the license plate number. Auxiliary license plates are not used for any other business processing.

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



The screenshot shows the ZKBio CVSecurity software interface. The main window is titled 'Parking / Basic Parking Management / Parking Lot Settings'. On the left, there is a sidebar with various management options: Basic Parking Management, Parking Lot Settings (selected), Device, Parking Area, Entrance And Exit Area, Booth, Lane, Vehicle Usage Type, Shift Settings, Release Reason, Advertising Resources, Dual Verification Settings, and Dual Verification Lane. The 'Parking Lot Settings' section contains fields for 'Line 3' (set to 'Red') and 'Line 4' (set to 'Red'). A note in the 'Line 3' field says: 'Only four-line screen device support!'. The right side of the interface shows a vertical sidebar with 'Parking Lot Settings' and other settings like 'Entrance and Exit Lane Setting', 'Charge Management Setting', 'Fixed Vehicle Setting', 'Voice and Display Settings', 'Ticket Dispenser setting' (selected), 'Other Setting', and 'Offline Settings'. The 'Ticket Dispenser setting' section contains checkboxes for 'Enable Ticket Dispenser', 'Enable QR code', 'Paperless Automatic Opening', and 'Enable Print License Plate'. It also includes sections for 'Virtual License Plate' (with input fields for 'Ticket Header' and 'Ticket Tail'), 'Time of delayed ticket issuance(second)*' (set to '0'), and 'Ticket Header' (set to 'welcome'). A note in the 'Virtual License Plate' section says: 'Ticket Dispenser parameters are only valid for Ticket Dispenser Device'. At the bottom right, there is a status bar with a battery icon and a 'OK' button.

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)

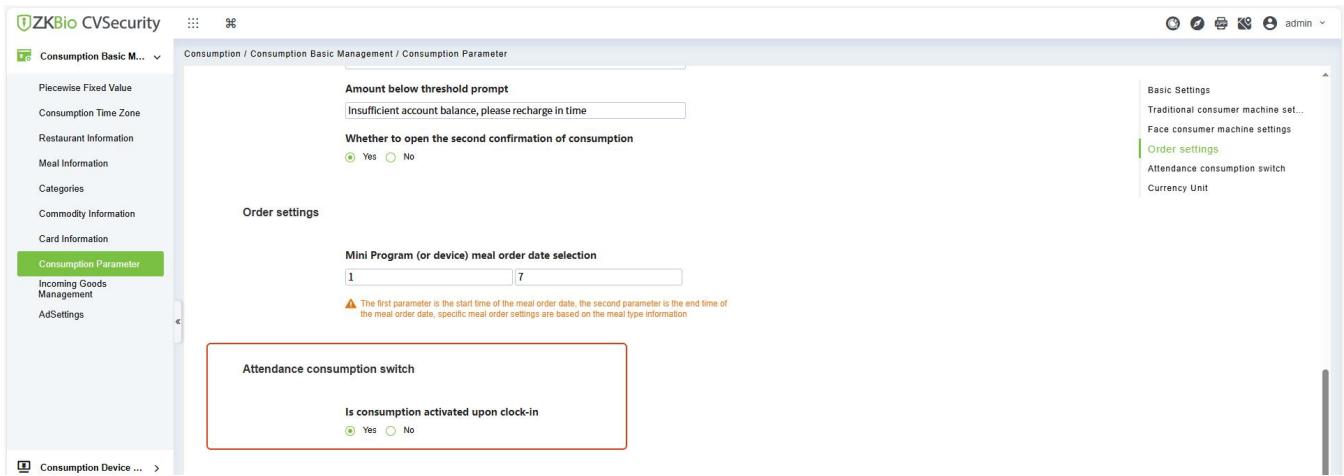
Fixed vehicle: Exit → LPR recognition → Swipe card (Auxiliary license plate recognition includes license plate recognition and photo recognition)

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.

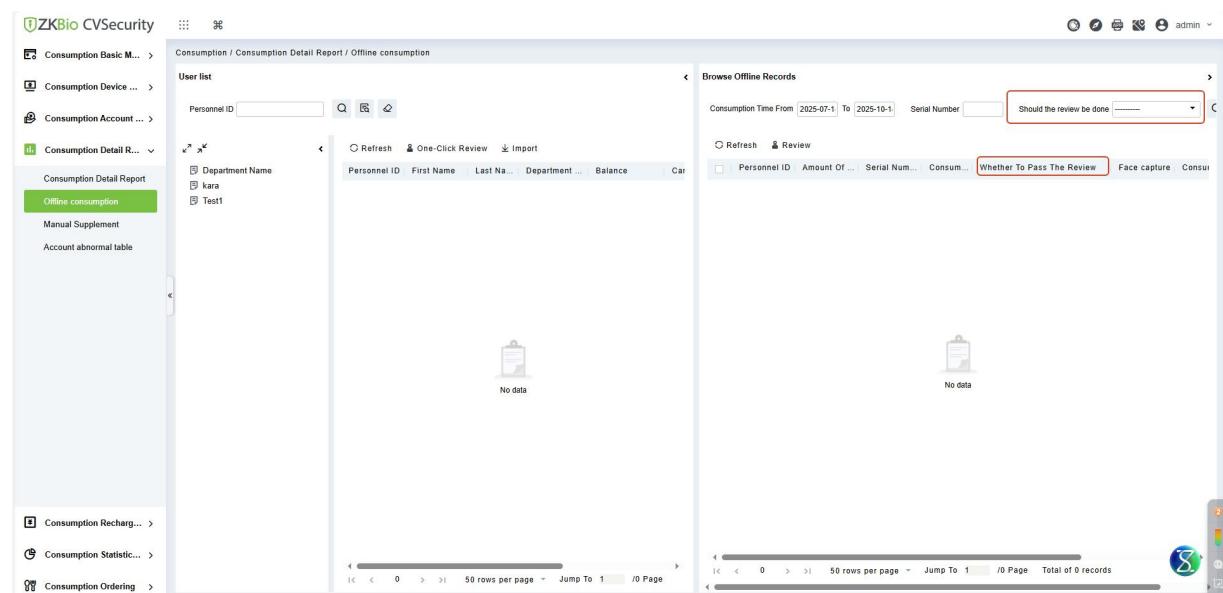


Result verification:

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."

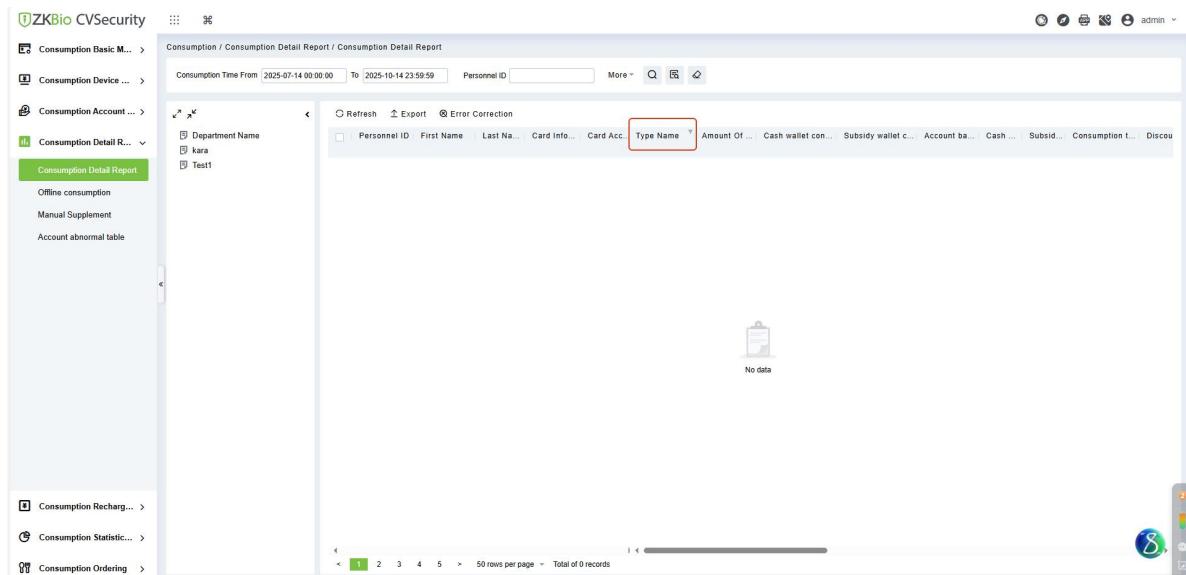
- **Added a filter for "Approval Status" in the offline consumption details table.**

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.**

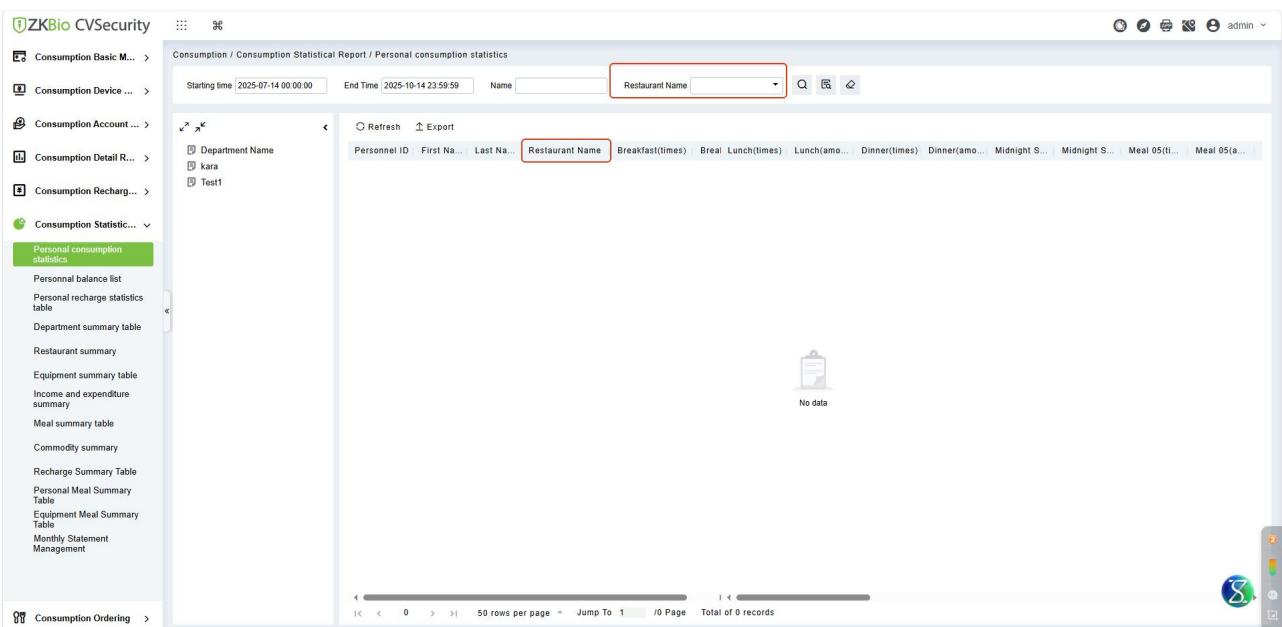
Step: Enter Consumption → Consumption Detail Report → Consumption Detail Report. The display fields of the report include "Type Name".



The screenshot shows a web-based application interface for consumption management. On the left, a sidebar menu lists various consumption-related modules. The main content area is titled 'Consumption / Consumption Detail Report / Consumption Detail Report'. It features a search bar with 'Consumption Time From' (2025-07-14 00:00:00) and 'To' (2025-10-14 23:59:59), a 'Personnel ID' input field, and a 'More' dropdown. Below the search bar is a toolbar with 'Refresh', 'Export', and 'Error Correction' buttons. The main table header includes columns for 'Personnel ID', 'First Name', 'Last Name', 'Card Info...', 'Card Acc.', 'Type Name' (which is highlighted with a red box), 'Amount Of...', 'Cash wallet con...', 'Subsidy wallet c...', 'Account ba...', 'Cash...', 'Subsid...', 'Consumption t...', and 'Discou...'. The table body shows a single row with 'Department Name' set to 'kara' and 'Personnel ID' set to 'Test1'. A message 'No data' is displayed below the table. At the bottom, there are navigation buttons for page numbers (1-5), a '50 rows per page' dropdown, and a 'Total of 0 records' message. The bottom right corner shows a status bar with a battery icon and a 'S' icon.

- **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.



The screenshot shows a web-based application interface for consumption management. On the left, a sidebar menu lists various consumption-related modules. The main content area is titled 'Consumption / Consumption Statistical Report / Personal consumption statistics'. It features a search bar with 'Starting time' (2025-07-14 00:00:00), 'End time' (2025-10-14 23:59:59), a 'Name' input field, and a 'Restaurant Name' dropdown (which is highlighted with a red box). Below the search bar is a toolbar with 'Refresh', 'Export', and 'Error Correction' buttons. The main table header includes columns for 'Personnel ID', 'First Name...', 'Last Name...', 'Restaurant Name' (highlighted with a red box), 'Breakfast(times)', 'Breakfast(amo...)', 'Lunch(times)', 'Lunch(amo...)', 'Dinner(times)', 'Dinner(amo...)', 'Midnight S...', 'Midnight S...', 'Meal 05(ti...', and 'Meal 05(amo...'. The table body shows a single row with 'Department Name' set to 'kara' and 'Personnel ID' set to 'Test1'. A message 'No data' is displayed below the table. At the bottom, there are navigation buttons for page numbers (1-5), a '50 rows per page' dropdown, and a 'Total of 0 records' message. The bottom right corner shows a status bar with a battery icon and a 'S' icon.

API

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

VisRegistration : visitor registration

Show/Hide | List Operations | Expand Operations

POST	/api/v2/visRegistration/getQrCode	Get Dynamic QR code
POST	/api/v2/visRegistration/getQrCodeByCertNumber	Get Dynamic QR code By CertNumber
POST	/api/v2/visRegistration/getTransactionList	Get Visitor Transaction List
POST	/api/visRegistration/add	Add Visitor

Implementation Notes

Add Visitor

Response Class (Status 200)

OK

Model | Example Value

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

Response Content Type

Parameters

Parameter	Value	Description	Parameter Type	Data Type
apiVisRegisterItem	(required)	apiVisRegisterItem	body	Model Example Value

Parameter content type:

```
{  
  "carPlate": "闽A12345",  
  "cardNo": "123",  
  "certNum": "1234567",  
  "certType": 8,  
  "company": "string",  
  "deptCode": "string",  
  "email": "123@zkteco.com",  
  "endTime": "2024-01-30 23:56:00",  
  "facePhoto": "string",  
}
```

- **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

Parameters

Parameter	Value	Description	Parameter Type	Data Type
endDate	<input type="text"/>	endDate	query	string
pageNo	<input type="text"/> (required)	pageNo	query	integer
pageSize	<input type="text"/> (required)	pageSize	query	integer
personPin	<input type="text"/>	personPin	query	string
startDate	<input type="text"/>	startDate	query	string

Response Messages

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

- 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	<input type="text"/>	deviceName	query	string
endDate	<input type="text"/>	endDate	query	string
pageNo	<input type="text"/> (required)	pageNo	query	integer
pageSize	<input type="text"/> (required)	pageSize	query	integer
partitionName	<input type="text"/>	partitionName	query	string
pointName	<input type="text"/>	pointName	query	string
startDate	<input type="text"/>	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

Parameters

Parameter	Value	Description	Parameter Type	Data Type
certNum	<input type="text"/>	certNum	query	string
pageNo	<input type="text"/> (required)	pageNo	query	integer
pageSize	<input type="text"/> (required)	pageSize	query	integer
phone	<input type="text"/>	phone	query	string

Response Messages

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

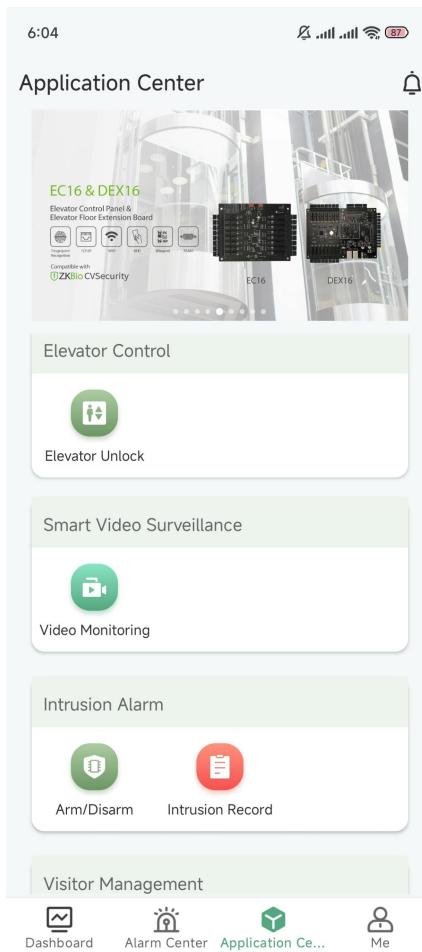
APP

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

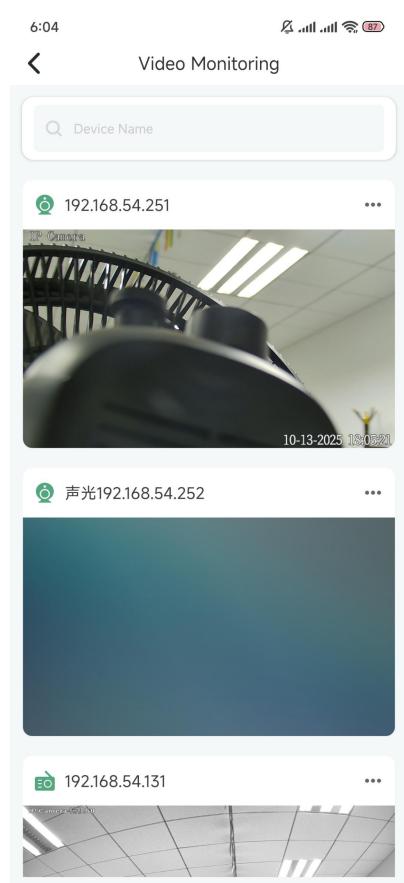
The APP has added a Smart Video Surveillance module. The main updates include support for video preview, video playback, PTZ control, video snapshot, manual recording, and intercom functions.

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.

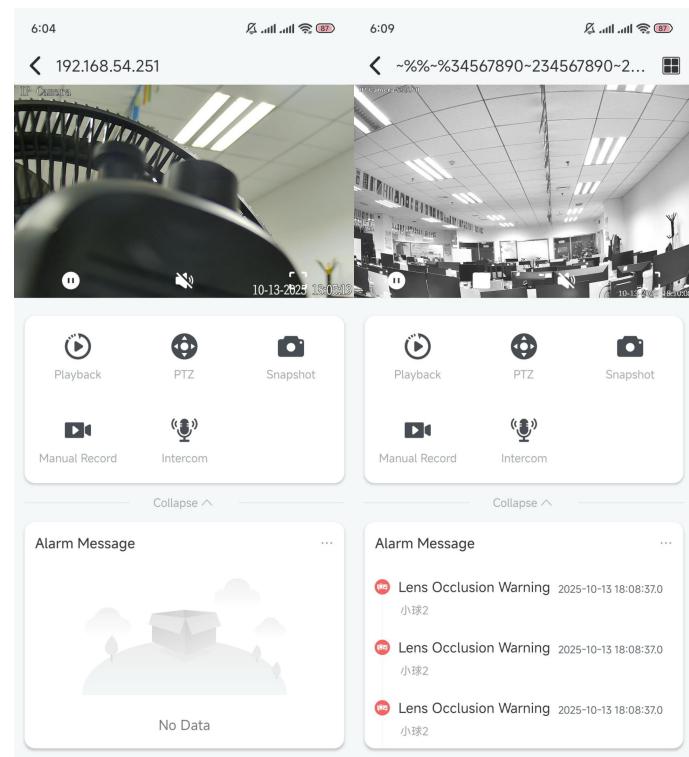
Operation (Administrator): Click on the Application Center -> Video Monitoring to enter the video view function. On the home page of this function.



You can view the device list and the current screen.

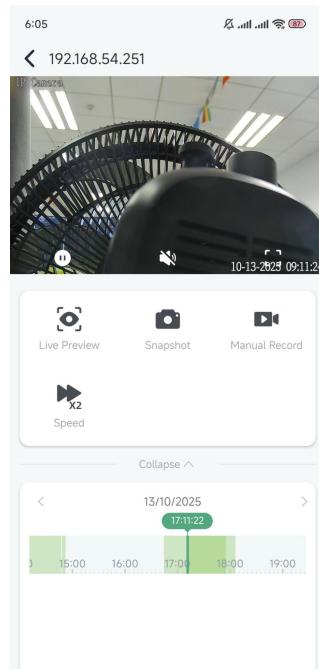


By clicking on the device, you can perform playback, PTZ control, snapshot, manual recording, and intercom operations.



■ **Playback:**

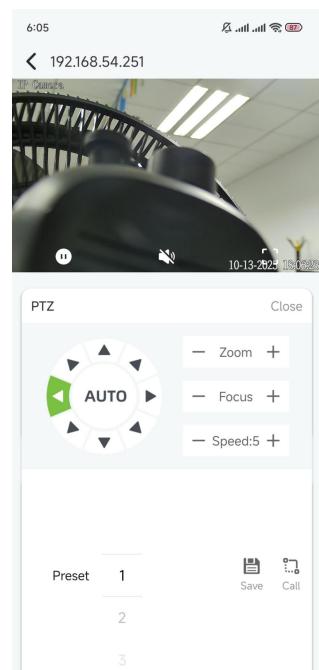
The playback of the picture can be achieved by dragging the timeline below. The playback page allows you to continue taking snapshots, manually record videos, or adjust the speed through "Speed". There are three speed Settings available: x 0.5, x1, and x2.



■ **PTZ:**

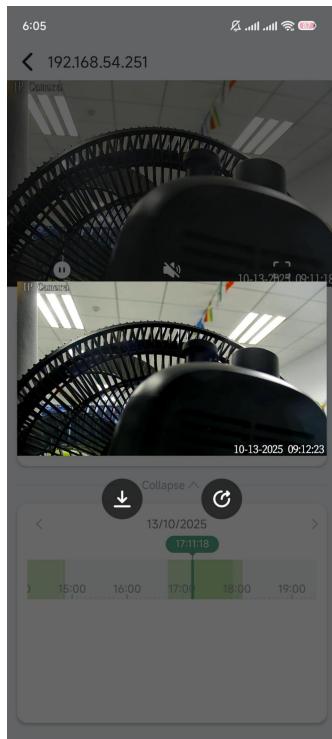
The camera can be remotely controlled in terms of direction, with a minimum adjustment Angle of 45 degrees. It also allows for zooming in and out of the picture, focus control, and adjustment of the camera's movement speed, ranging from 1 to 10.

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.



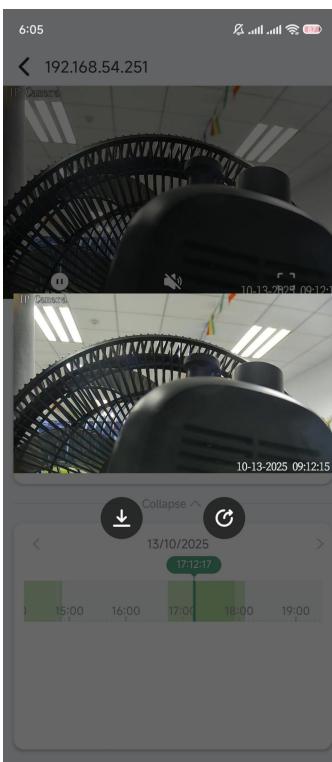
■ Snapshot:

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.



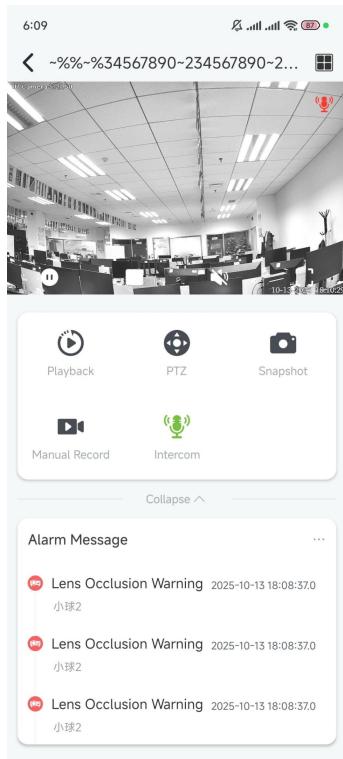
■ Manual Record:

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.



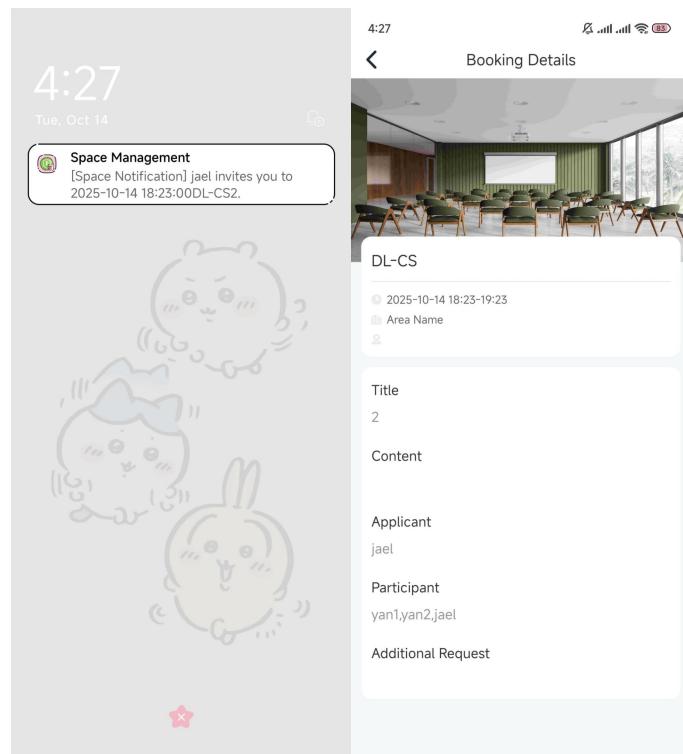
■ **Intercom:**

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.



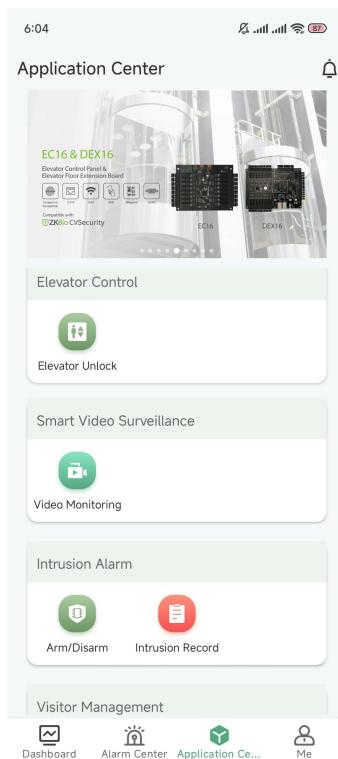
- **Supports one-click arming/disarming and viewing event records.**

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.

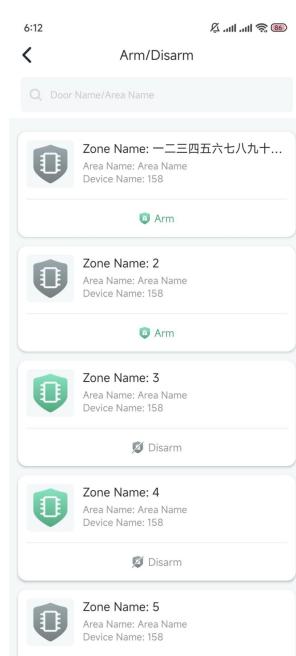
Operation (Administrator):

1. Arm/Disarm

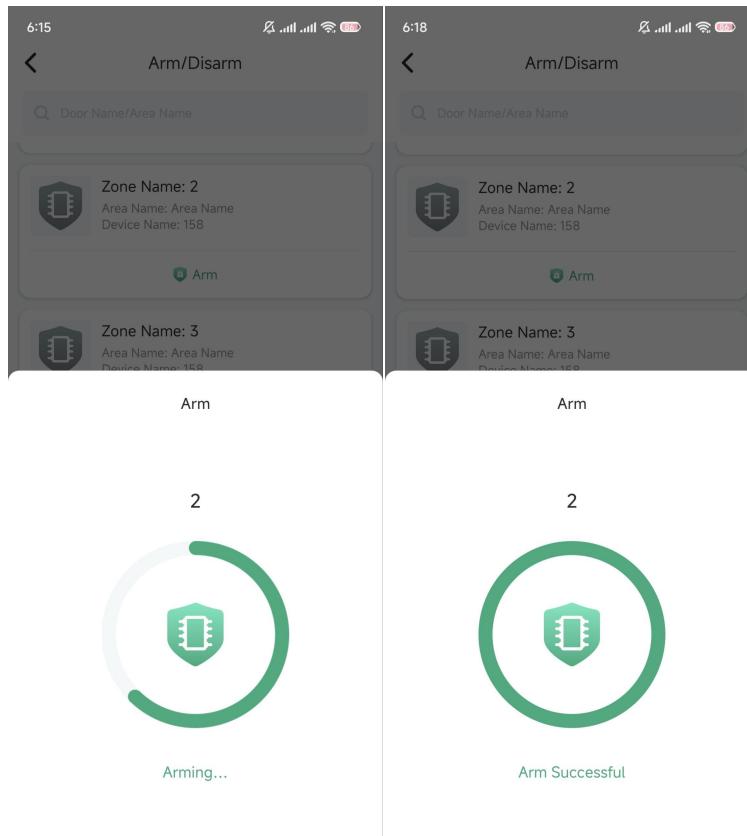
Enter the Application Center -> Intrusion Alarm -> Arm/Disarm.



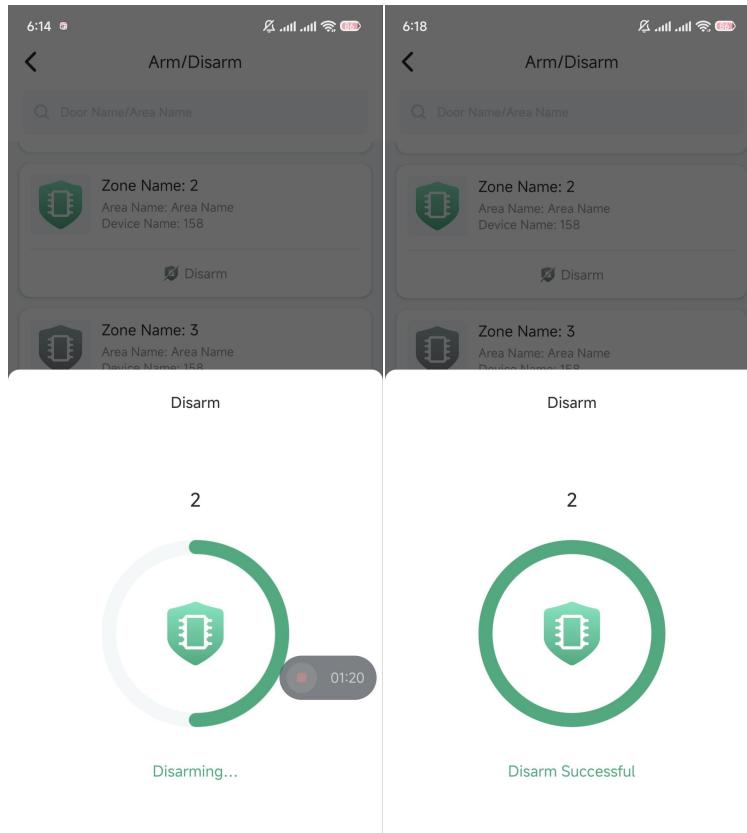
Click on "Arm/Disarm" under the corresponding partition to conveniently perform arming and disarming operations on different partitions on the APP.



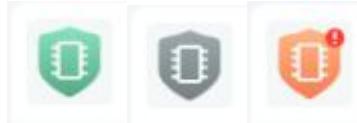
Click the "Arm" button under the area to quickly arm that area. After the operation is successful, it will display that "Arm Successful".



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:



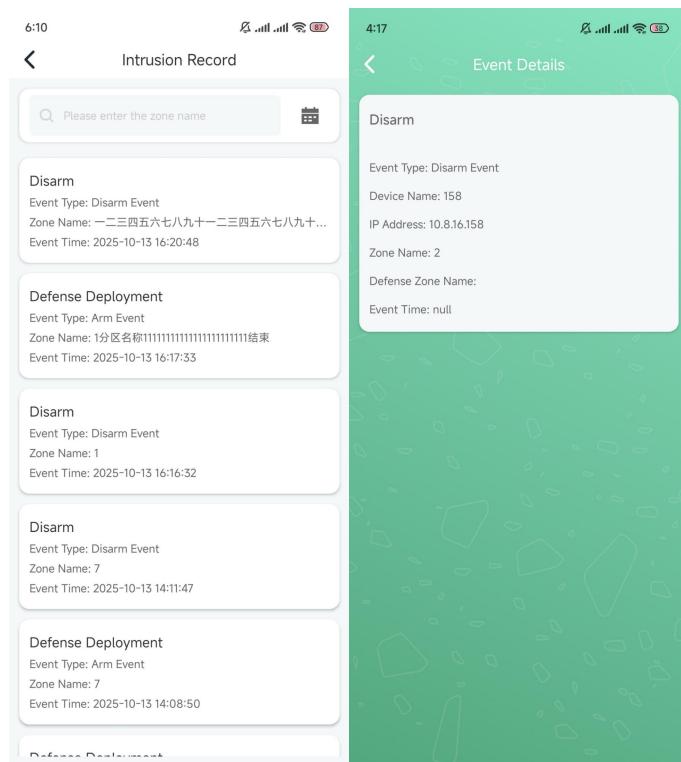
The green icon indicates that the current defense zone is armed, and the "Disarm" button is displayed below.

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.



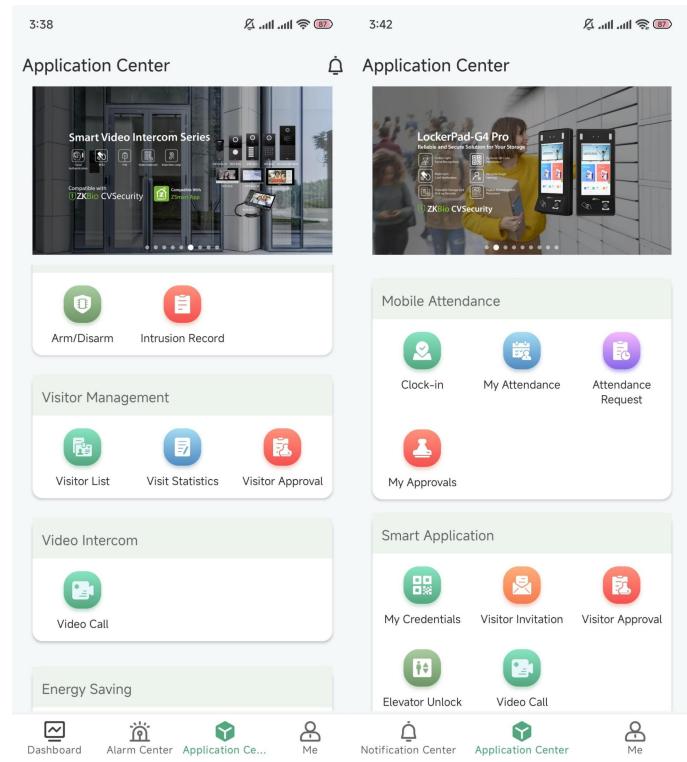
● Visitor Approval Feature.

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

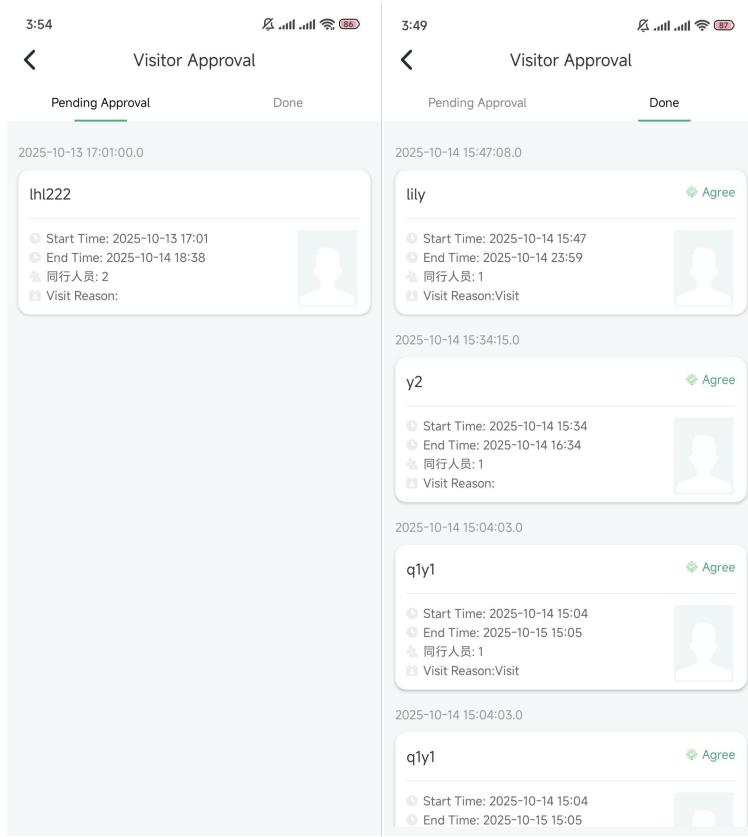
Operation (Administrator & Personnel):

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

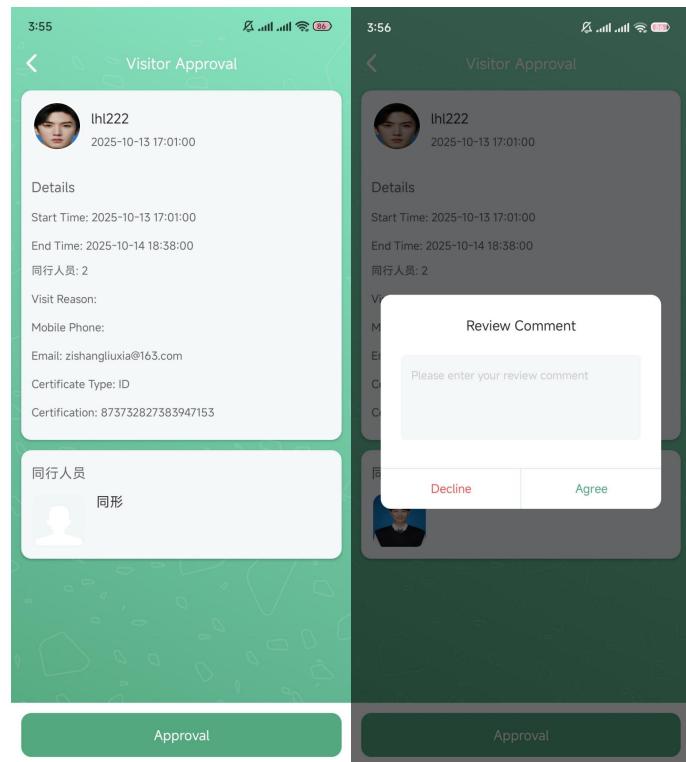
Personnel can enter the Application Center -> Smart Application -> Visitor Approval.



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".

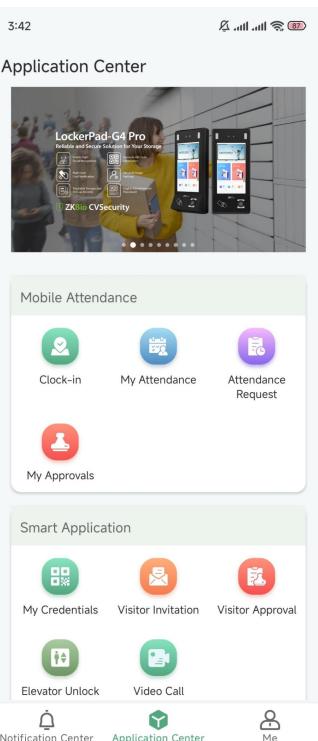


Note: Currently, only administrators and interviewees are supported to perform visitor review operations. Multi-level visitor review is not supported for the time being.

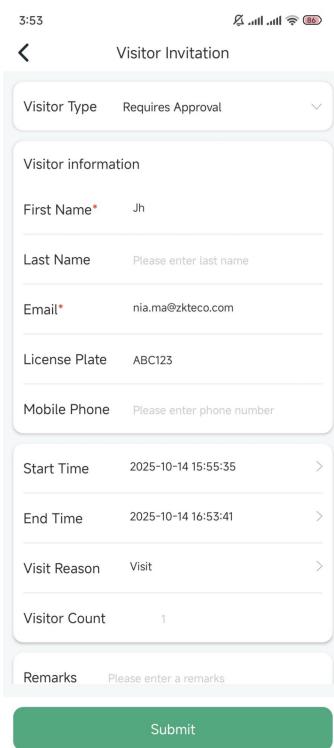
● Visitor invitation now include a license plate number field.

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.



Visitor Type: Requires Approval

Visitor information

First Name*: Jh

Last Name: Please enter last name

Email*: nia.ma@zkteco.com

License Plate: ABC123

Mobile Phone: Please enter phone number

Start Time: 2025-10-14 15:55:35

End Time: 2025-10-14 16:53:41

Visit Reason: Visit

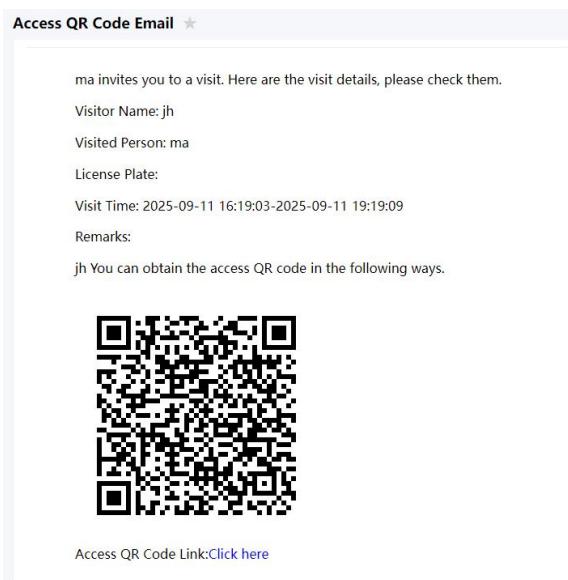
Visitor Count: 1

Remarks: Please enter a remarks

Submit

- **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" function in advance:

- Navigate to **ZKBio CVSecurity** → **Visitor** → **Basic Management** → **Set Permission Groups by Host**.
- Add the visitor(s) and assign their permissions.
- Click **More** → **Non-reviewed Visitors**.

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

Operation (Administrator End) :

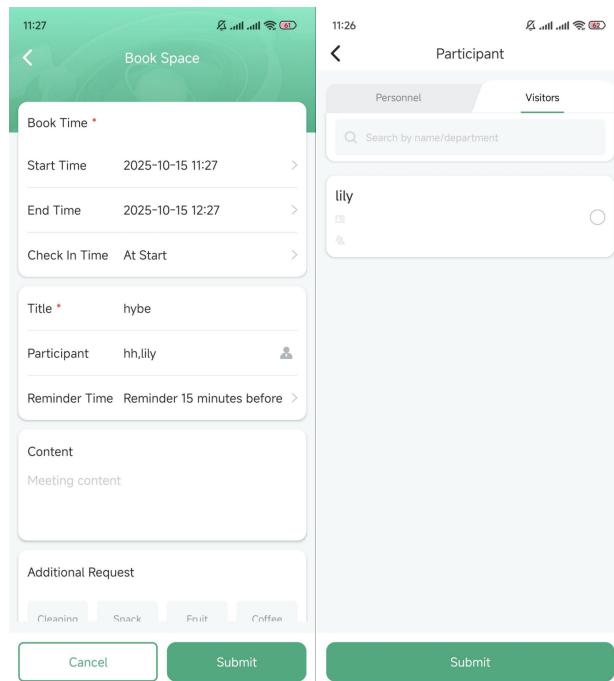
Enter the Application Center -> Personnel Management -> Personnel Registration to register personnel information.

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.