

Change Log

ZKBio CVSecurity

Version: 5.0

Date: June 2026

Software Version: ZKBio CVSecurity_6.8.0_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 © 2026 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

1. USER-DEFINED PANEL	8
1.1. Supports free panel layout with open capabilities for dragging and resizing User-Defined Panel.....	8
1.2. Newly added Service Center Module components, including Event Record and Device Overview.	8
1.3. Supports role-based dashboard customization.....	9
2. ACCESS CONTROL	10
2.1. Advanced Functions / Global Linkage: Supports configuring different output actions for different persons under the same trigger condition and device.....	10
2.2. Advanced Functions / Crowd Control: Supports configuration to trigger alarms when the occupancy exactly reaches the maximum/minimum threshold, or exceeds/falls below the preset value.....	11
2.3. Advanced Functions / Authorization Limits: Add auto-reset function to usage count rules.....	12
2.4. Device Management / Event Type: Support custom event severity levels.....	13
2.5. Device Management / Real-Time Monitoring & Access Control Reports: Display operator user information for remote control operations including remote door opening and alarm cancellation.....	14
2.6. Device Management / Real-Time Monitoring & Map Center: Optimize the remote operation interface to display icons with corresponding text labels.....	14
2.7. Access Rule / Parameters: Allow users to customize notification template, includes subject and message body.....	15
3. TIME & ATTENDANCE	17
3.1. Attendance Management / Mobile Check-in Range: Remove the map key configuration function for attendance check-in range. Users are now required to manually input longitude, latitude and detailed address. A coordinate picker is newly added to help users obtain coordinates on their own.....	17
3.2. Attendance Management / Mobile Check-in Range: Support bulk import of check-in ranges via Excel. The import fields include: Area, Valid Range, Longitude, Latitude, Address. The import template is also available for download.....	18
3.3. Attendance Custom Report: Support splitting report fields to display only the fields selected by users.....	20
3.4. Attendance Setting / Holiday: Support annual cycle recurrence, with permission control for template download, import and export functions.....	21
4. PERSONNEL	23
4.1. Personnel / Person: Optimize the entry of biometric enrollment function for more prominent and intuitive access.....	23
4.2. Personnel / Parameters - Self-service Registration: New configuration parameter "Enable Employee ID + Name Verification Mode".....	23
4.3. Personnel / Parameters - Authorized Deletion Personnel: Add new configuration parameter "Administrator password is required when deleting personnel or departments".....	24
5. VISITOR MANAGEMENT	25
5.1. Basic Management / Parameters: The hybrid cloud link will become unavailable after disabling cloud visitor reservation.....	25
5.2. Visitor Registration / Visitor Check-in – Optimized display box for visited personnel to show full names.....	25
5.3. Basic Management / Parameters: Configurable mandatory fields for visitor registration page (Applicable to PC and H5).....	26

5.4. Basic Management / Custom Attributes: Add configuration option to set whether custom fields are mandatory. If a field is marked mandatory, visitors must fill in this field completely on both visitor registration and visitor reservation pages to save records successfully	27
5.5. Advanced / Notification Template – Supports uploading file attachments.	29
5.6. Visitor Registration / Visitor Check-in – Supports selecting a connected USB camera from a drop-down list during image capture.....	30
5.7. Visitor Registration / Visitor Check-in – Supports print preview on the registration interface.....	30
5.8. Visitor Registration, Visitor Reservation, Visitor Report, Daily/Weekly/Monthly Visitor Access Reports – Adds license plate filter condition.	32
5.9. Visitor Report - Daily/Weekly/Monthly Visitor Reports – Adds certification number filter condition.	33
5.10. Devices – Supports visitor terminals with BEST Protocol.....	34
6. SPACE MANAGEMENT	36
6.1. Device Management / Space Access Permission - Supports batch-assigning administrators by zone for multi-administrator space management. Administrators can verify their identity and enter their designated meeting rooms directly without a reservation.	36
6.2. Space Management / Space - Supports deleting uploaded space images.....	38
6.3. Modification of Meeting Email Subject Names	39
6.4. System – Support pushing space and facility information to terminal devices for display.....	39
6.5. Device Management - Device – Support pushing wallpapers to devices.....	40
6.6. Statistics Report / Access Events - A new access record report is added. Under the multi-administrator management mode, all personnel access records of spaces are retained to facilitate subsequent behavior tracing and inquiry.....	42
6.7. Reservation Management / Space Reservation - When administrators reserve meeting rooms on the PC client, the reservation applicant is automatically added to the attendee list by default without manual addition.	42
7. ENTRANCE CONTROL (NEW PASSAGE MODULE RELEASED WITH MULTIMODAL ALL-IN-ONE MACHINE-ZOPHON-S1000)	44
7.1. Passage Device	44
7.2. Passage Access	51
7.3. Passage Settings	54
7.4. Entrance Control Reports	57
7.5. Real-Time Monitoring	57
8. ELEVATOR CONTROL	59
8.1. Elevator Device / Reader: Add new card number bit reversal function. After enabling this function, the system will automatically reverse the card number data.	59
8.2. Elevator Device / Real-Time Monitoring – Interface Optimization : Adds a device list displaying key parameters including device address, serial number, online/offline status, and the number of expansion boards.	59
8.3. Elevator Device / Device-Selecting a device opens its edit page, with newly added time zone configuration parameters to support customized time zone settings for devices.....	60
8.4. DCS - Online/Offline Status Event Reporting: Support alarm subscription for Online/Offline status in event center.....	60
8.5. DCS - Supports elevator number feedback after call request.....	62
8.6. Elevator Integration / Service Config: Add communication status display for Kone & Mitsubishi elevator controllers.....	66

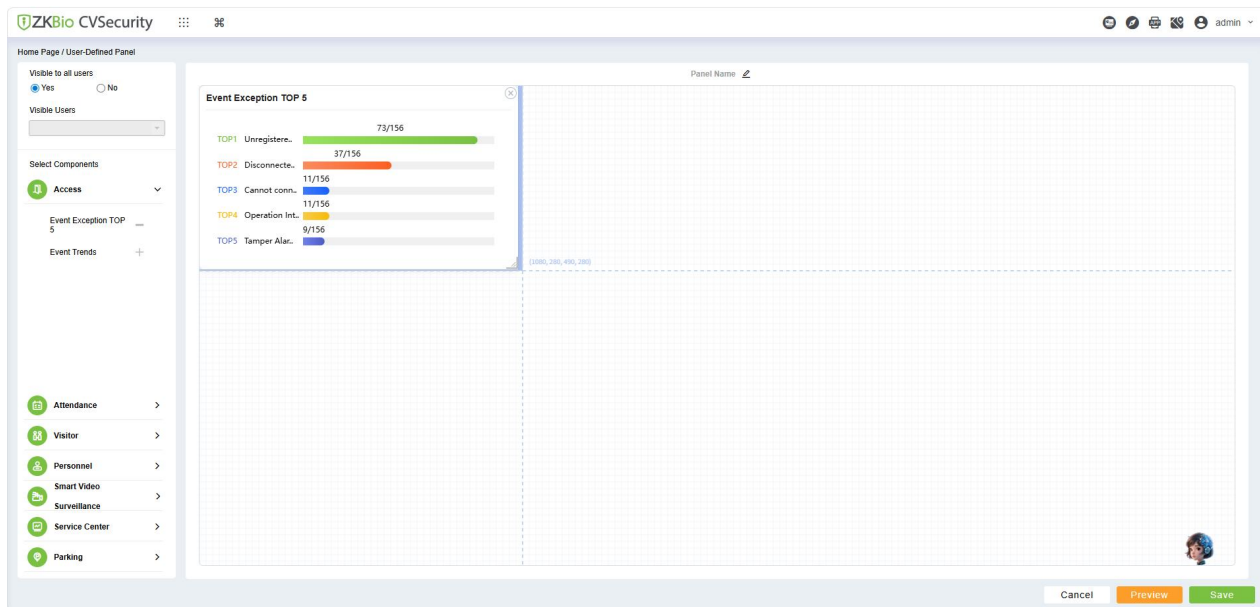
8.7. Elevator Device / Device: Add algorithm version selection during device creation.....	67
8.8. Elevator Device / Device: Modify the relay mode and check the direct access mode to reach the target floor directly without pressing any buttons.	68
9. SMART VIDEO SURVEILLANCE	71
9.1. Intelligence - Behavior Analysis: Support binding of ZKIVA Edge X1 face recognition and behavior analysis..	71
9.2. Intelligence - Global Linkage: Support linkage configuration for thermal alarm types of backend NVR (Smoking Detection, Temperature Alarm, Fire Spot Detection, Smoke & Fire Detection).....	76
10. PARKING	77
10.1. Basic Parking Management / Parking Lot Settings – Ticket Dispenser Setting: Support logo upload for receipt printing.....	77
10.2. Vehicle Management / Vehicle Authorization: Permission control added for batch authorization button.....	78
10.3. Vehicle Management / Vehicle Authorization: Start & End time supports Hour & Minute precision.....	78
10.4. Basic Parking Management / Dual Verification Settings: Multiple users can bind to one license plate for dual verification.....	78
11. CONSUMPTION	81
11.1. Consumption Basic Management / Commodity Information: Add import function to support batch import of commodity information via import template.....	81
11.2. Consumption Basic Management / Meal Information: Configure prepayment pricing after meal reservation to prevent no-show after reservation.....	81
11.3. Consumption Ordering / Order management: Add import function to support batch meal reservation via import template.....	82
11.4. Bug Fix: Optimize to support reissuing only deactivated consumption accounts to devices separately instead of full-volume distribution, improving distribution efficiency and avoiding illegal card swiping by resigned employees.....	83
11.5. Consumption Account Management / Subsidy Management: Add subsidy withdrawal function for unredeemed subsidies by canceling review process.....	83
12. VIDEO INTERCOM	85
12.1. Service Center / Linkage Center / Linkage Configuration: Support IVR linkage configuration.....	85
12.2. Extension Management / Extension Number: Max concurrent registration limit updated to 5 when creating new extensions.....	88
13. INTRUSION ALARM	90
13.1. Intrusion Device – Device Management: Support password update function.....	90
13.2. Relay Output Management.....	92
13.3. Intrusion Devices – Partition: Add perimeter fence sub-menu.....	93
13.4. Real-time Monitoring – Interface supports display of linked alarm events.....	93
13.5. Intrusion Device – Global Linkage: Add Pop-up video and display duration settings in video linkage module.....	94
13.6. Intrusion Device / Parameters: New alarm sound configuration function.....	95
14. SERVICE CENTER	96
14.1. Scene Center - Target Recognition: New structured fields – Hair & Hat (Supported Device: ZKIVA Edge X1).	96
14.2. Scene Center - Real-Time Attendance: Support one-click report export.....	96
14.3. Scene Center - Personnel Count.....	97

14.4. Scene Center - Target Recognition: Add box matching parameters (Parameters for shielding box service of intelligent video module).....	98
14.5. Map Center - Real-time Monitoring: Display assembly point devices on map after emergency assembly linkage trigger for quick positioning.....	99
14.6. Scene Center - Transparent Kitchen: Add time dimension for statistical data, support Daily/Weekly/Monthly statistics viewing.....	100
14.7. Scene Center - Transparent Kitchen: Add one-click statistical report export function.....	101
14.8. Scenario Center - Target Recognition: Search criteria not limited to allowlist and denylist personnel.....	102
14.9. Linkage Center - Linkage Configuration: Support assigning personnel to configured linkages for differentiated linkage rules by staff.....	102
15. SYSTEM	104
15.1. Compliance Requirements – Optimization of custom privacy agreement function.....	104
15.2. Authority Management / Role: Add permission control for each scene panel in scene center.....	105
15.3. Login Password Input Optimization: Eye icon added to all password input boxes (Toggle Show/Hide Password).....	106
15.4. Authority Management / Security Parameters: New session timeout configuration menu with custom time limit.....	106
15.5. Authority Management / API Authorization: Edit client ID without modifying client secret.....	107
15.6. Supports reading old Indonesian KTP, new Indonesian e-KTP, Indonesian driving license.....	109
16. API CHANGE NOTICE	113
16.1. Personnel Module: New batch Enable & Disable interfaces.....	113
16.2. Attendance Module: New return fields for /api/v2/transaction/listAttTransaction.....	113
16.3. Attendance Module: New attendance point query interface.....	114
16.4. Global API Authentication Response Optimization	115
16.5. Access Control: New door control API interfaces.....	115
16.6. Consumption Module: New consumption record query interface (Ticket HOC-524).....	118
16.7. Add APIs for creating, updating and deleting areas, as well as an API to retrieve the area list.....	119
16.8. Parking Module: Time field upgrade for /api/v2/parkPlate/addAllowDisabled.....	119
16.9. Parking Module: Valid white list plate query API.....	119
16.10. Visitor Module: Batch Check-in & Check-out interfaces.....	120
16.11. Video Intercom: Add new APIs for personnel-associated extension number query and extension list retrieval.....	121
16.12. The API interface log list and query function support displaying and filtering the client secret key and requester IP address fields.....	122
17. ZKBIO ZEXUS MOBILE APPLICATION CHANGE NOTICE	123
17.1. Admin - Personnel Registration: Support uploading personnel avatars via mobile terminals.....	123
17.2. Admin - Personnel Registration: Support license plate entry. Personnel - Me - Personal Information: Support license plate display.....	123
17.3. Admin - Personnel Registration: Remove mandatory input restriction for the email field.....	124
17.4. Admin - Video Monitoring: Add door opening button on the video preview page.....	124
17.5. Admin - Dashboard: Supports selecting to view device status of different modules via drop-down options.....	125
18. PROJECT MANAGEMENT	126
18.1. Add Project Management Platform	126

1. User-Defined Panel

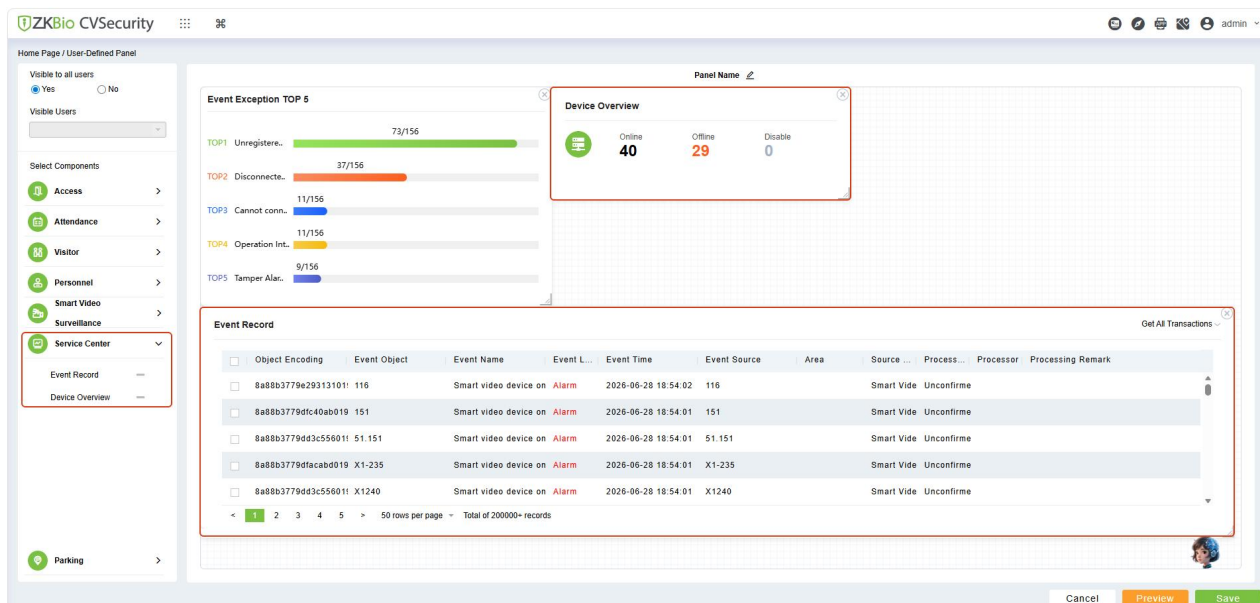
1.1. Supports free panel layout with open capabilities for dragging and resizing User-Defined Panel.

Users can drag components from the left sidebar onto the canvas and place them anywhere freely. They can quickly resize components by dragging the control point at the bottom-right corner of each component.



1.2. Newly added Service Center Module components, including Event Record and Device Overview.

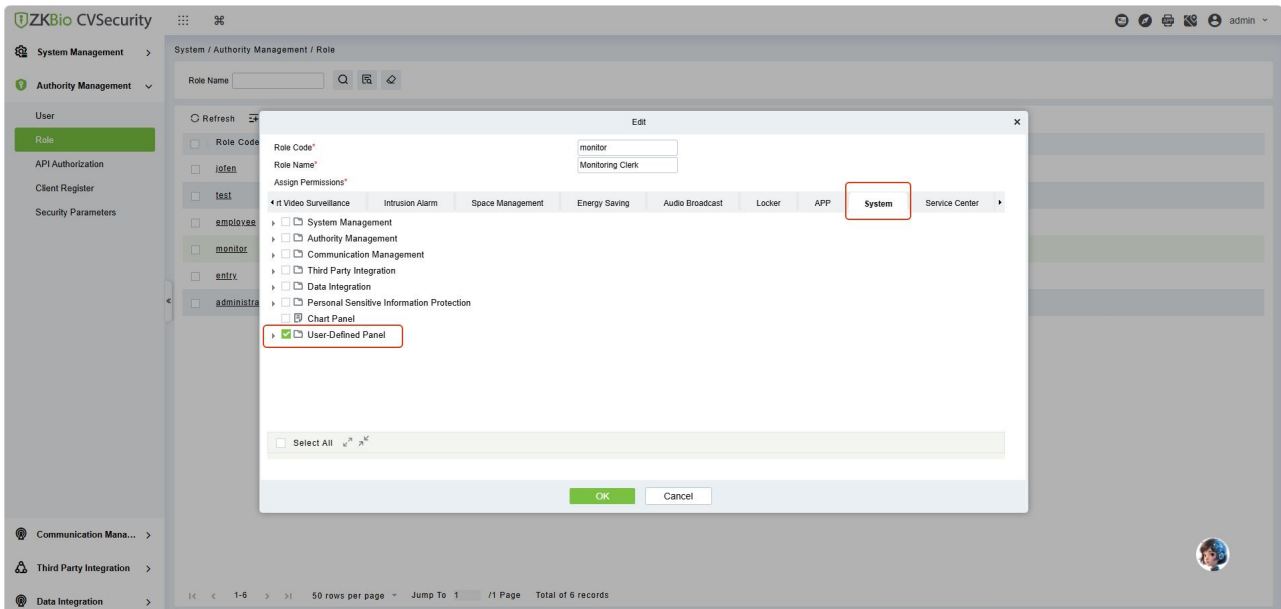
- Event Record component: synchronizes records from the Event Center and supports filtered queries by module
- Device Overview component: displays device status including online, offline and disabled



1.3. Supports role-based dashboard customization.

User-defined panel only display content of modules authorized to the current user.

- Prerequisite: The User-Defined Panel permission under the System Management module must be granted on the role authorization page.

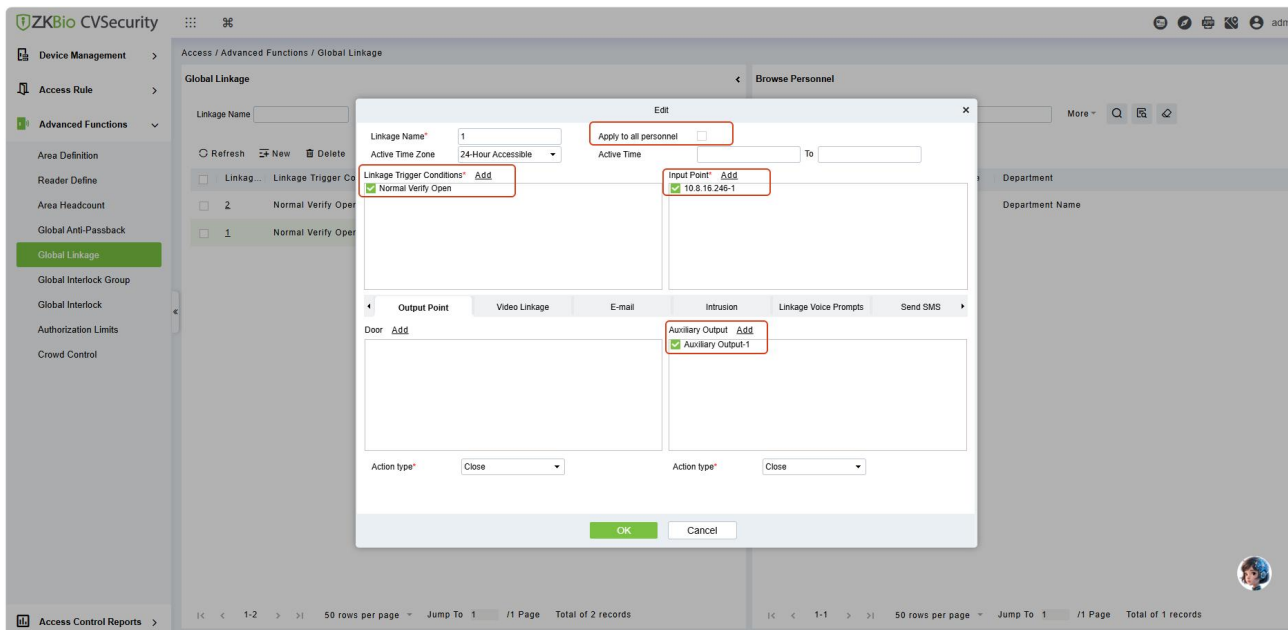


2. Access Control

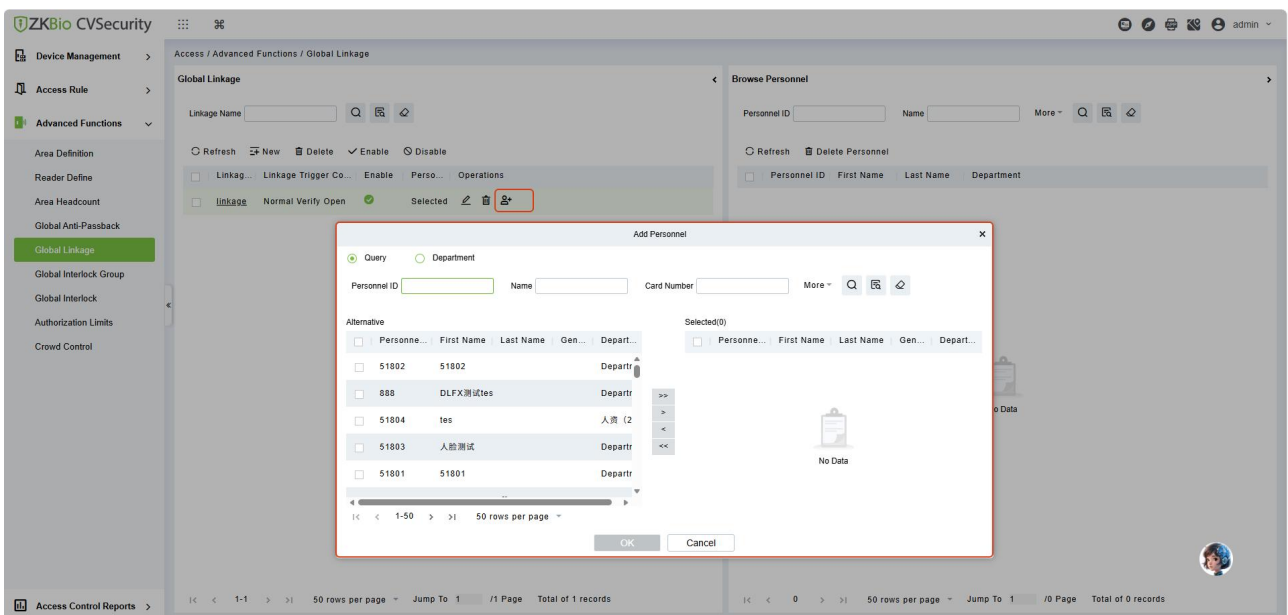
2.1. Advanced Functions / Global Linkage: Supports configuring different output actions for different persons under the same trigger condition and device.

Step 1: Navigate to "Access Control / Advanced Functions / Global Linkage", click New, then select linkage trigger conditions, input points and output points.

- **Note:** If different output points of the same device under the same linkage trigger condition need to take effect for different personnel, you must uncheck "Apply to all personnel" first.

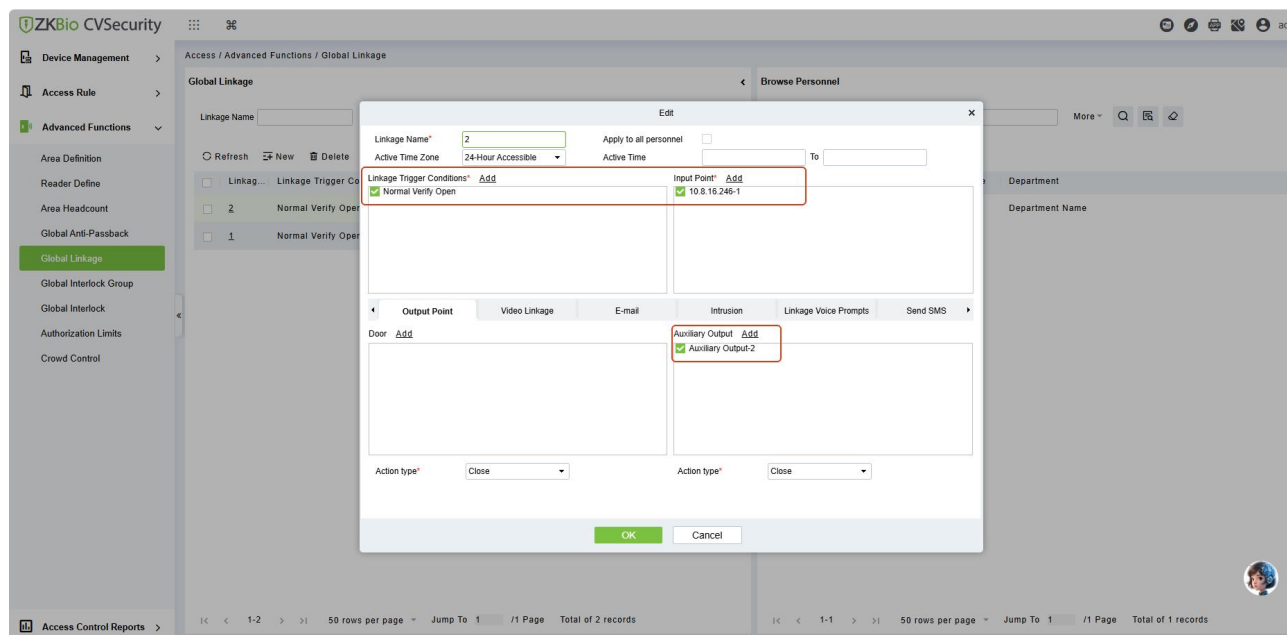


Step 2: After creating the linkage, click the Add Personnel button and select the personnel applicable to this linkage.



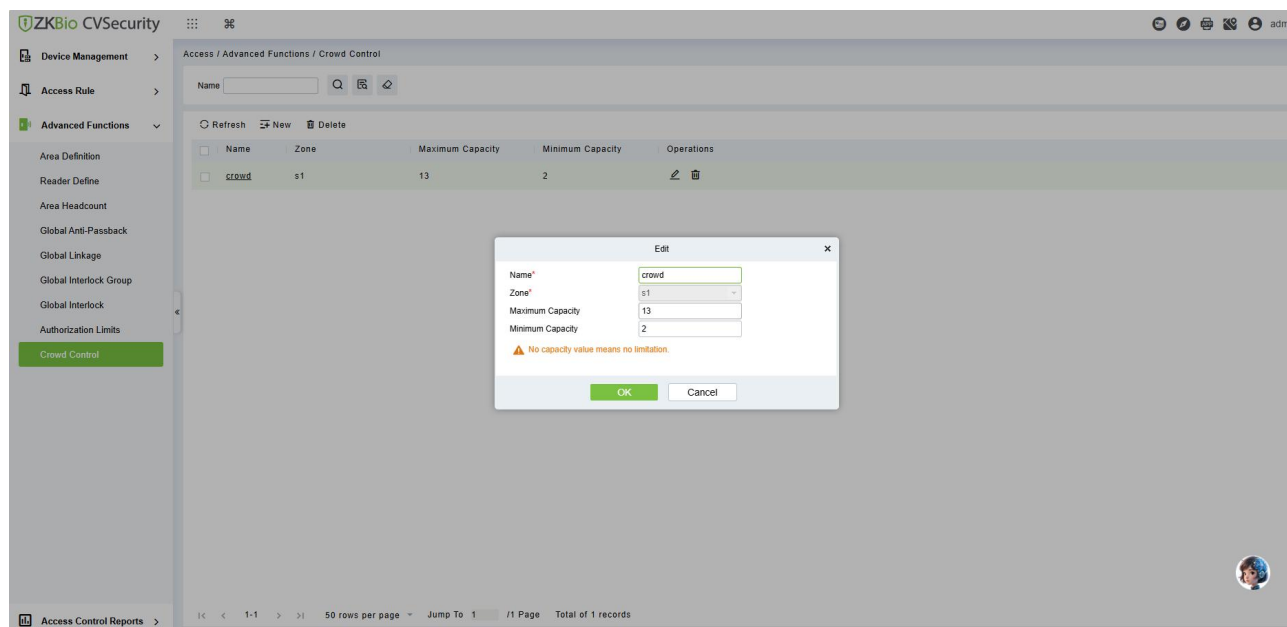
Step 3: Create a new linkage with the same trigger condition and input point, only modify the output point. Once the linkage is created, add corresponding applicable personnel. This fulfills the

requirement that different output points of the same device under the same linkage trigger condition take effect for different personnel.



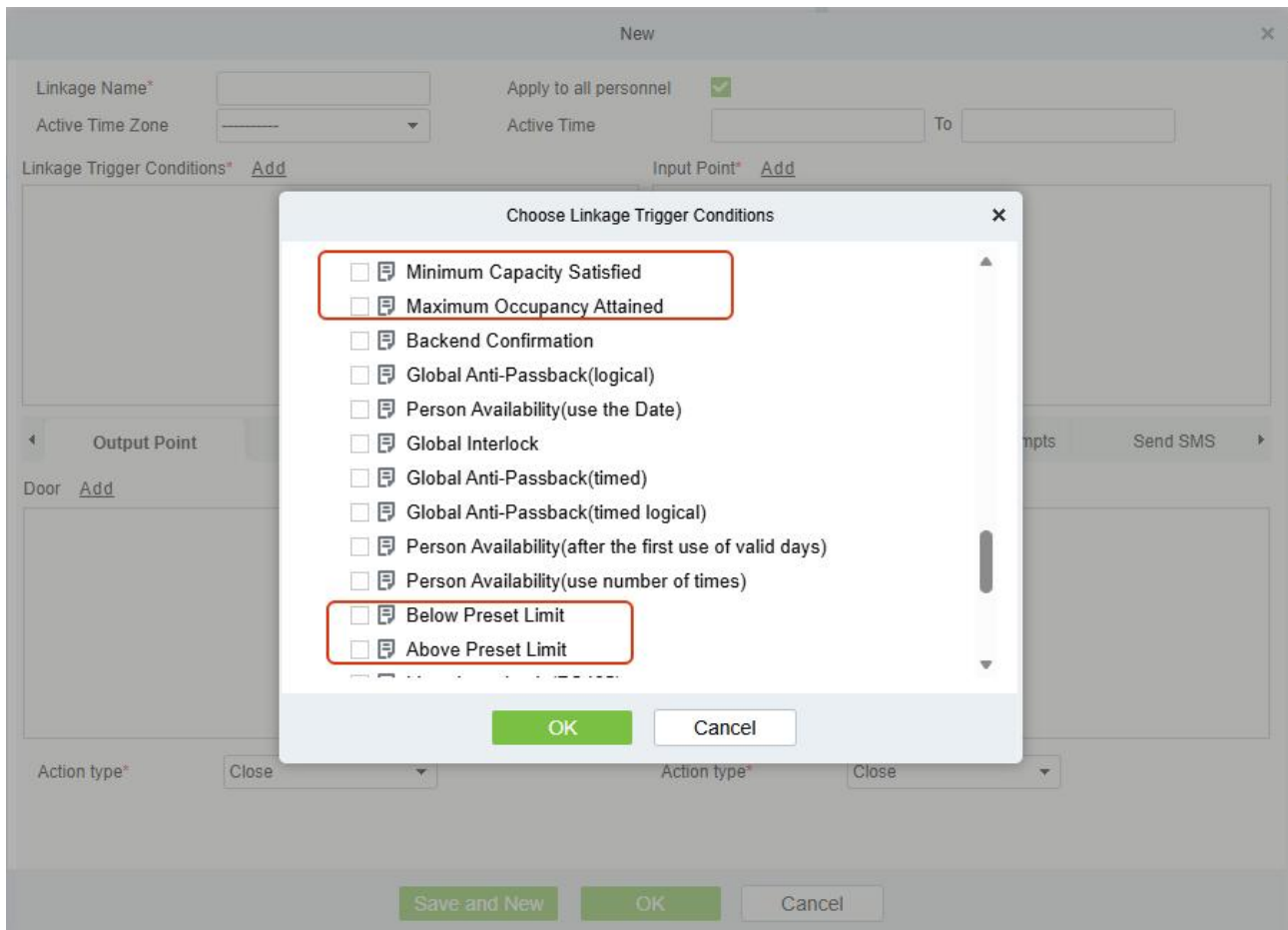
2.2. Advanced Functions / Crowd Control: Supports configuration to trigger alarms when the occupancy exactly reaches the maximum/minimum threshold, or exceeds/falls below the preset value.

Step 1: Navigate to "Access Control / Advanced Functions / Crowd Control" and set the maximum and minimum occupancy limits for the designated area.



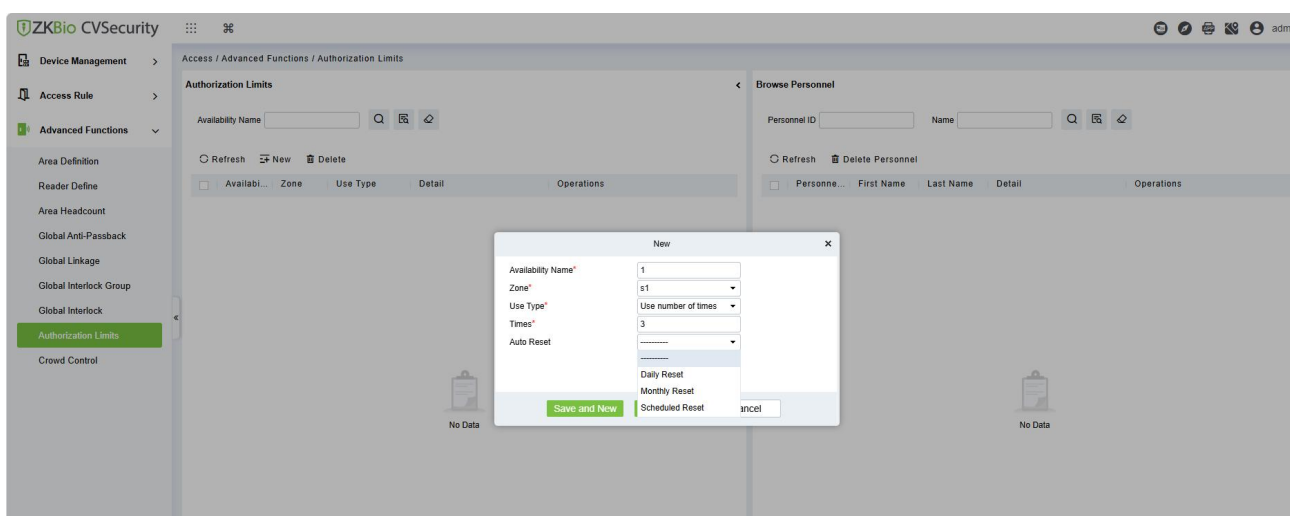
Step 2: Navigate to "Access Control / Advanced Functions / Global Linkage". Four new linkage trigger conditions are available: Reached Minimum Capacity, Reached Maximum Capacity, Below Preset Capacity, Exceeded Preset Capacity. Users may configure alarms to be triggered when the occupancy hits the exact maximum/minimum threshold, or goes above/below the preset value as

required.



2.3. Advanced Functions / Authorization Limits: Add auto-reset function to usage count rules.

Navigate to "Access Control / Advanced Functions / Authorization Limits". When selecting "Usage Count" as the usage mode, users can configure auto-reset rules according to actual business needs.



Three optional reset rules are provided, and only one rule can be selected at a time:

- Daily fixed-time reset: Users may specify a fixed time for daily automatic reset.

New

Availability Name* 1

Zone* s1

Use Type* Use number of times

Times* 3

Auto Reset Daily Reset

Reset Time ? 00 : 00

Save and New OK Cancel

- Monthly fixed-time reset: Users may set a specific time on a designated date each month for automatic reset.

New

Availability Name* 1

Zone* s1

Use Type* Use number of times

Times* 3

Auto Reset Monthly Reset

Reset Time ? 1 00 : 00

Save and New OK Cancel

- One-time future scheduled reset: Automatically reset at a specific date and time after the current moment.

New

Availability Name* 1

Zone* s1

Use Type* Use number of times

Times* 3

Auto Reset Scheduled Reset

Reset Time ? 05-25 00 : 00

Save and New OK Cancel

2.4. Device Management / Event Type: Support custom event severity levels.

Navigate to "Access Control / Device Management / Event Type". Select a target event in the event list and click Edit to modify its event severity level.

ZKBio CVSecurity

Access / Device Management / Event Type

Event Description Event Number Event Level Device Name Serial Number Operations

Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Normal Verify Open	0	Normal	fanyat0.8.16.109	CJR2201260029	
Verify during Passage Mode T	1	Normal			
First Personnel Open	2	Normal			
Multi-Personnel Open	3	Normal			
Emergency Password Open	4	Normal			
Open during Passage Mode T	5	Normal			
Linkage Event Triggered	6	Normal			
Cancel Alarm	7	Normal			
Remote Opening	8	Normal			
Remote Closing	9	Normal			
Disable Intruder Passage Mode	10	Normal			

Edit

Device Name fanyat0.8.16.109

Event Name Normal Verify Open

Event Number 0

Event Level Normal

Event Sound Normal

Copy to all devices

OK Cancel

2.5. Device Management / Real-Time Monitoring & Access Control Reports: Display operator user information for remote control operations including remote door opening and alarm cancellation.

- Access Control / Device Management / Real-Time Monitoring

Two records are displayed here: one is the device-reported data record, and the other is the software-reported data record.

Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2026-05-13 16:48:29	Area Name	10.8.16.130(CO3X23346000)	10.8.16.130-1	Remote Opening			Other	Other
2026-05-13 16:48:29	Area Name	10.8.16.130(CO3X23346000)	10.8.16.130-1	Remote Opening		admin	Other	Other

- Access Control / Access Control Reports / All Transactions

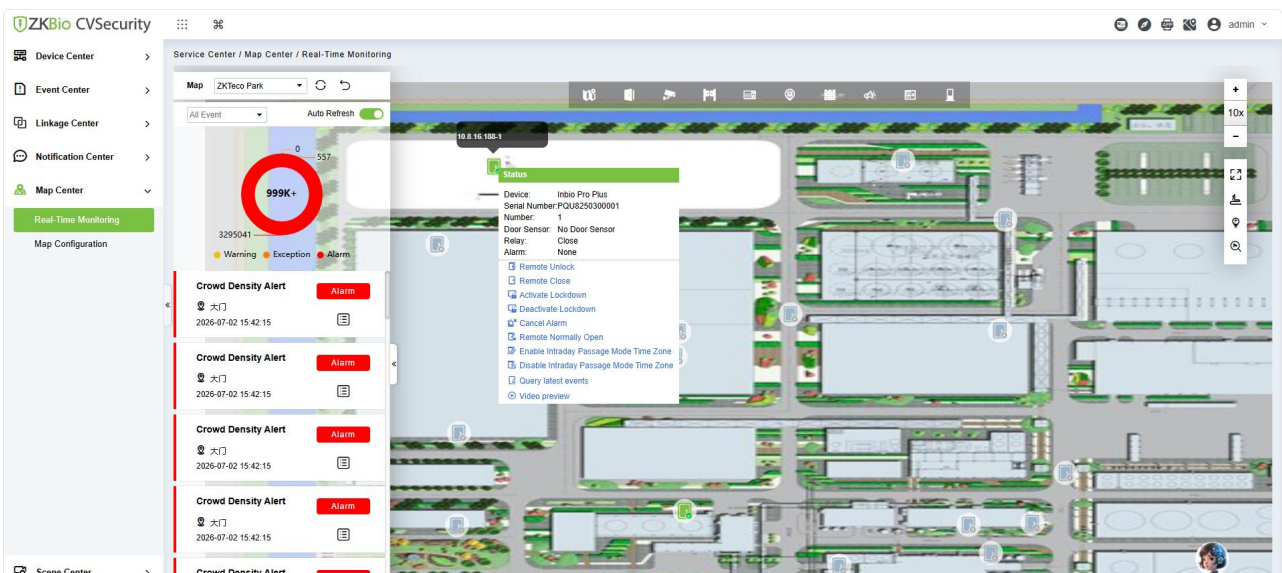
Time	Area Name	Device Name	Event Point	Event Description	Event Level	Media File	Personnel ID	Name	Card Number	Department	Reader Name	Verification Mode
2026-06-05 14:55:46	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Reader Offline	Alarm(Weak)						10.8.55.125-1-In	Other
2026-06-05 14:55:22	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Unregistered Per	Exception				117223539843		10.8.55.125-1-In	Only Card
2026-06-05 14:54:30	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Unregistered Per	Exception				2153219154		10.8.55.125-1-In	Only Card
2026-06-05 14:54:30	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal						Other	Other
2026-06-05 14:54:30	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal		hjc2				Other	Other
2026-06-05 14:54:29	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal						Other	Other
2026-06-05 14:54:29	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal		hjc1				Other	Other
2026-06-05 14:36:21	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Unregistered Per	Exception						10.8.55.125-1-In	Only Password
2026-06-05 14:35:16	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Unregistered Per	Exception						10.8.55.125-1-In	Only Password
2026-06-05 14:35:07	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Normal Verification	Normal		11112222			Department No	10.8.55.125-1-In	Card+Password
2026-06-05 14:34:34	Area Name	10.8.55.125(NSC)	10.8.55.125-1	Reader Online	Normal						10.8.55.125-1-In	Other
2026-06-05 14:30:19	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal						Other	Other
2026-06-05 14:30:19	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal		hjc2				Other	Other
2026-06-05 14:30:14	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal						Other	Other
2026-06-05 14:30:14	Area Name	10.8.55.124(NSC)	10.8.55.124-1	Remote Unlock	Normal		hjc1				Other	Other
2026-06-05 13:55:28	Area Name	10.8.16.244(NSC)		Server Connectio	Normal						Other	Other

2.6. Device Management / Real-Time Monitoring & Map Center: Optimize the remote operation interface to display icons with corresponding text labels.

- Access Control / Device Management / Real-Time Monitoring

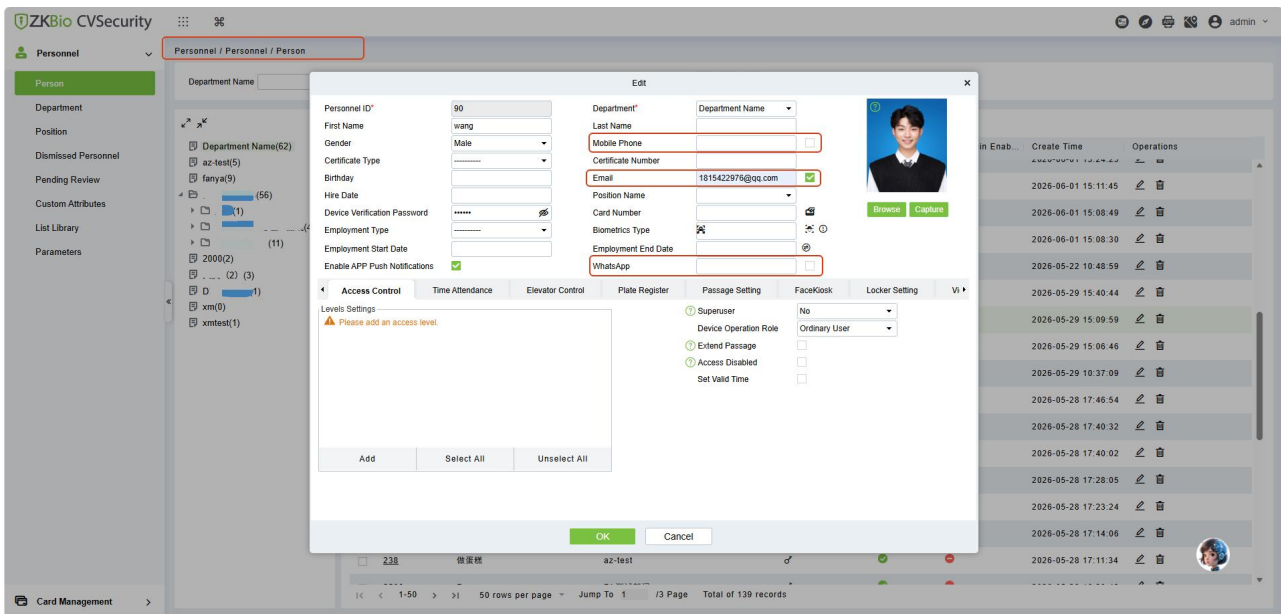


● Service Center / Map Center / Real-Time Monitoring



2.7. Access Rule / Parameters: Allow users to customize notification template, includes subject and message body.

Message Receiving Address Configuration: Navigate to Personnel / Personnel / Person. Click New or select an existing employee ID to enter the editing page. Three message push channels are available: Mobile Phone, Email, and WhatsApp. Tick your preferred push methods and enter valid receiving addresses accordingly.



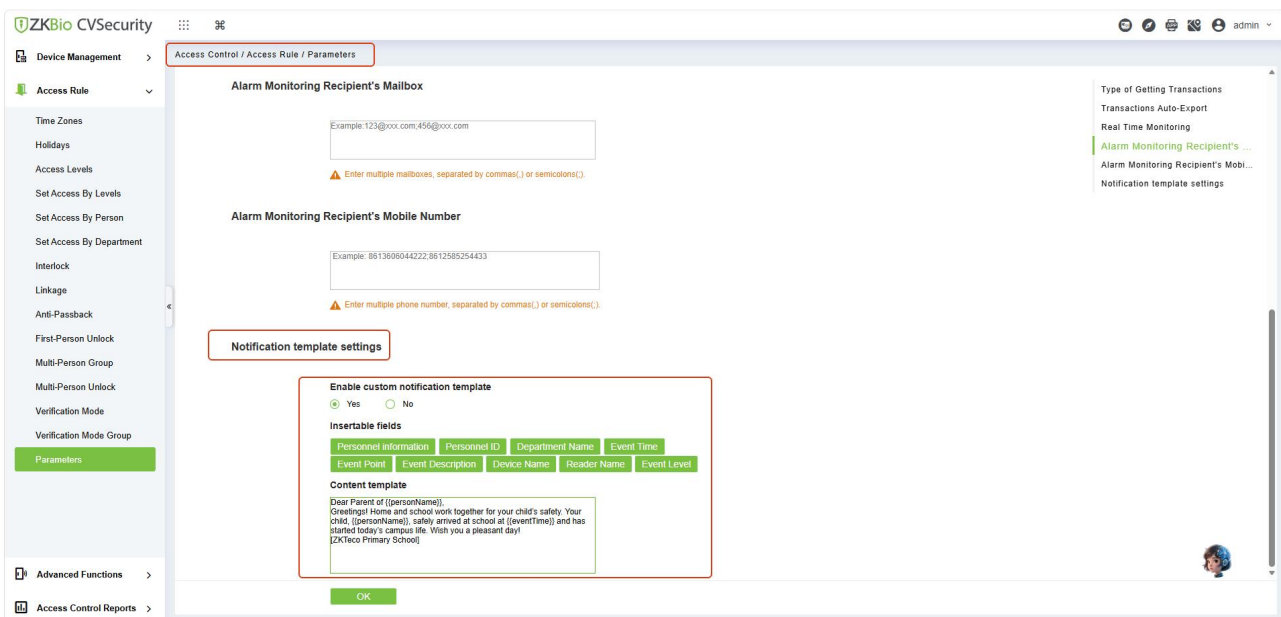
Navigate to Access Control / Access Rule / Parameters - Notification Template Settings, enable the custom notification template, and you may enter custom text in the body template area, where field information can be inserted freely.

● Example:

Dear Parent of {{personName}},

Greetings! Home and school work together for your child's safety. Your child, {{personName}}, safely arrived at school at {{eventTime}} and has started today's campus life. Wish you a pleasant day!

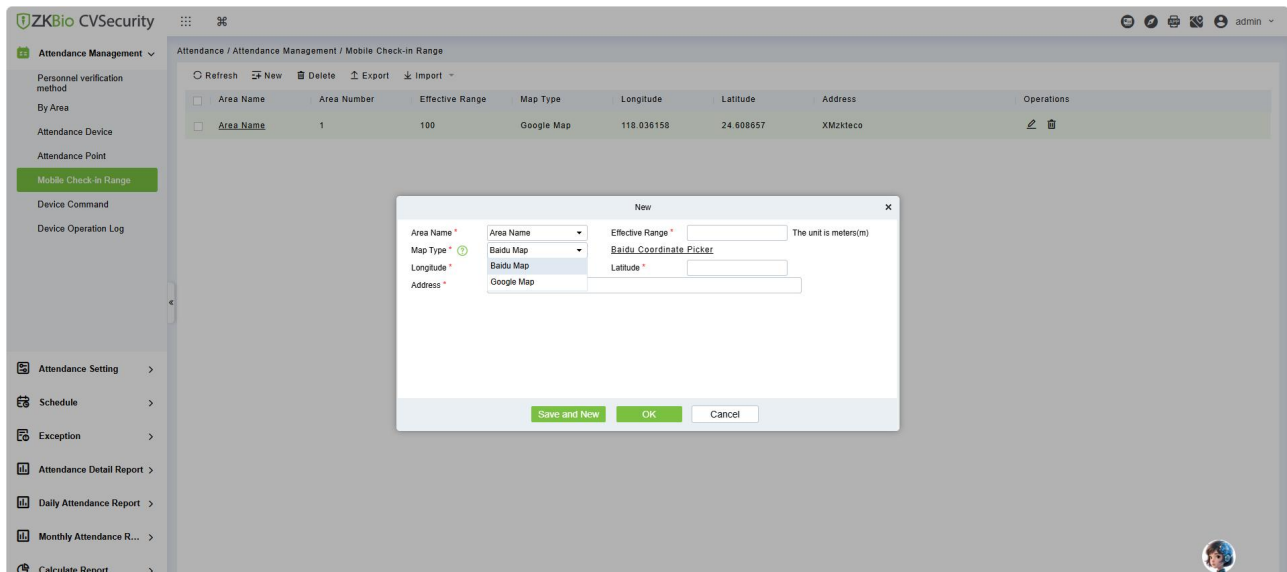
[ZKTeco Primary School]



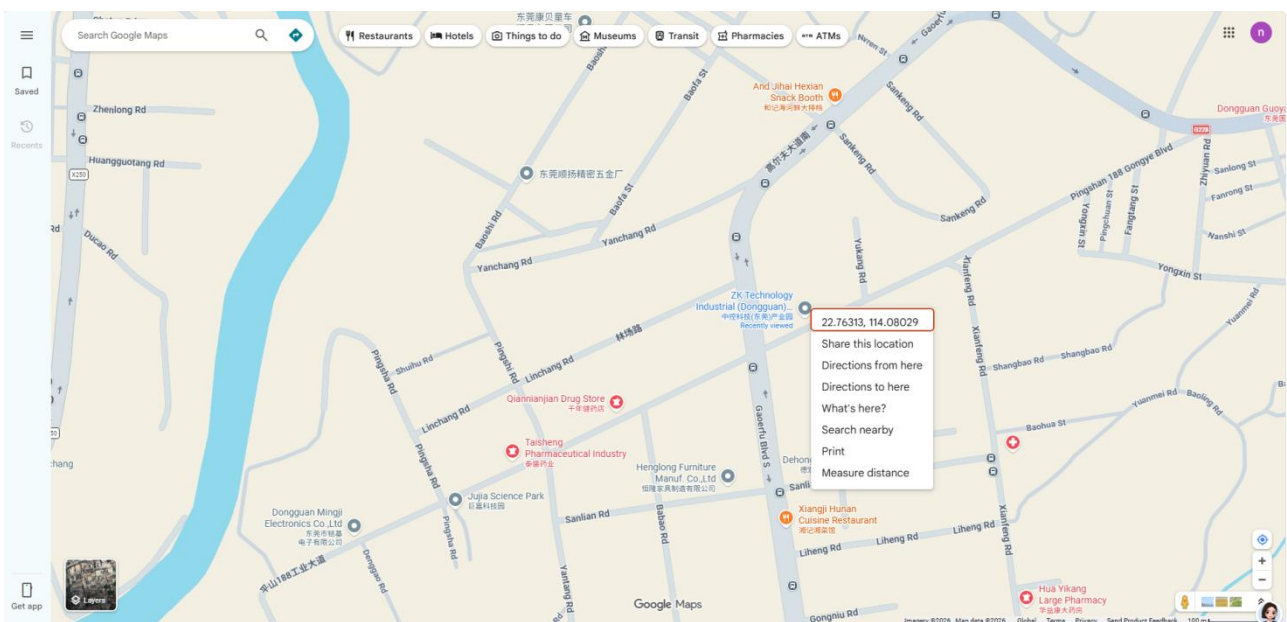
3. Time & Attendance

3.1. Attendance Management / Mobile Check-in Range: Remove the map key configuration function for attendance check-in range. Users are now required to manually input longitude, latitude and detailed address. A coordinate picker is newly added to help users obtain coordinates on their own.

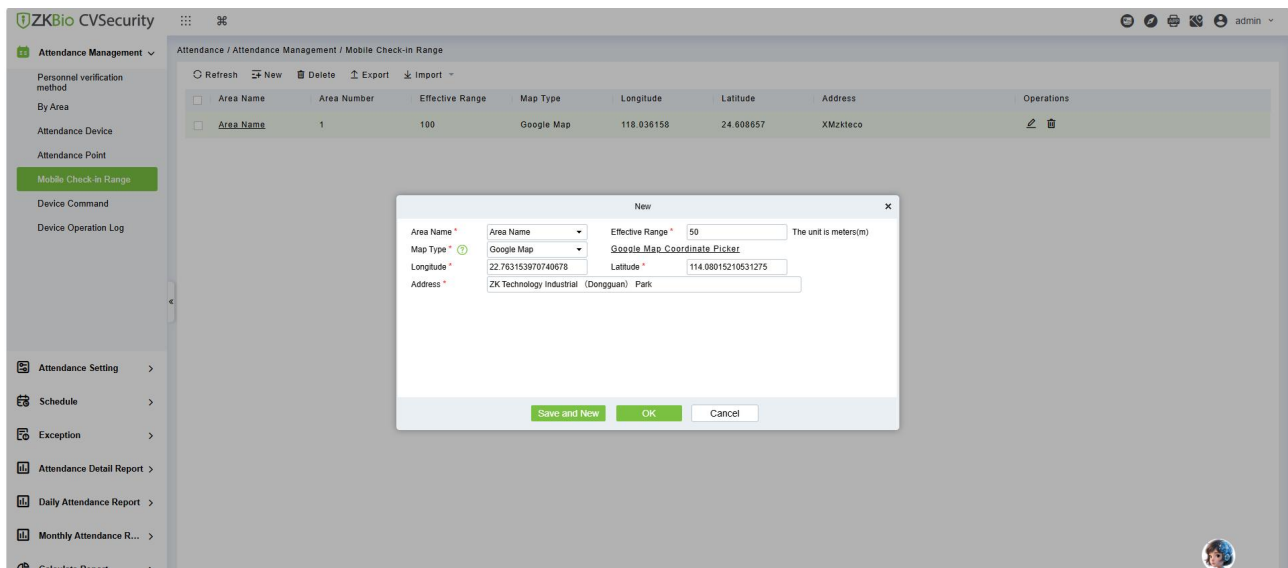
Step 1: Navigate to "Attendance / Attendance Management / Mobile Check-in Range", click New to enter the address configuration page. Baidu Map and Google Map are two available map types.



Step 2: Select the map type first, then launch the corresponding coordinate picker to get longitude and latitude from the coordinate picking website. The screenshot below shows the coordinate acquisition interface of Google Map. After locating the target position, right-click the point to view and copy the latitude and longitude data.



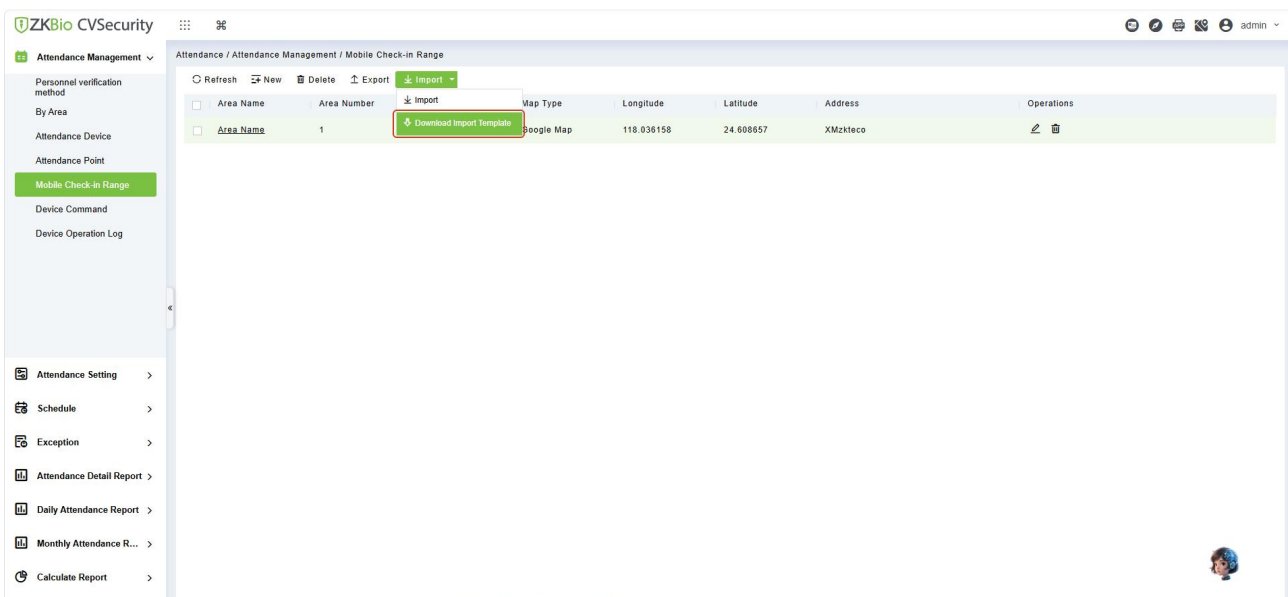
Step 3: Return to the system page, paste the copied longitude and latitude into the corresponding input boxes and fill in the detailed address. The attendance check-in range will be added successfully.



3.2. Attendance Management / Mobile Check-in Range: Support bulk import of check-in ranges via Excel. The import fields include: Area, Valid Range, Longitude, Latitude, Address. The import template is also available for download.

● Bulk Import of Check-in Ranges

Step 1: Navigate to "Attendance / Attendance Management / Mobile Check-in Range", click "Import" → "Download Import Template".



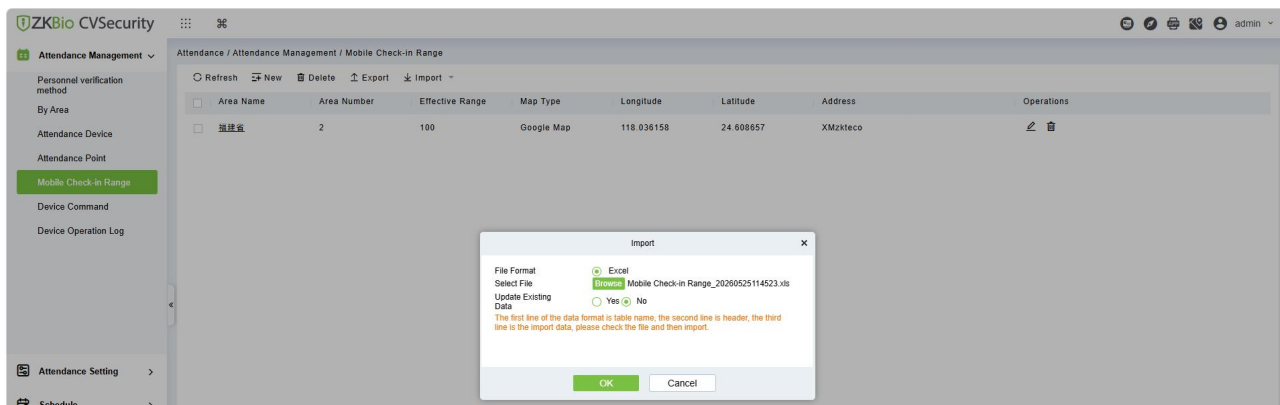
Step 2: The fields of the import template include: Area Name, Area No., Valid Range, Map Type, Longitude, Latitude, Address.

Mobile Check-in Range						
Area Name	Area Number	Effective Range	Map Type	Longitude	Latitude	Address

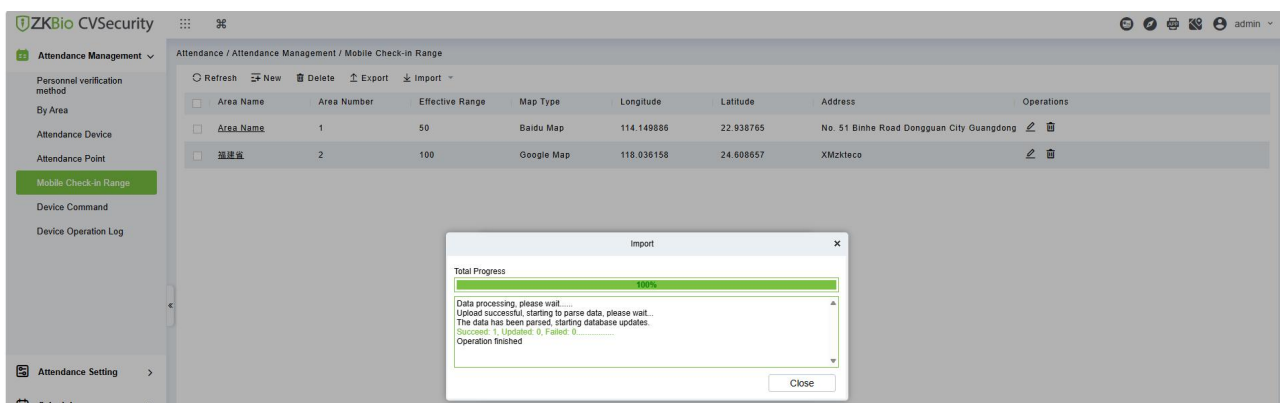
Fill in the table information in strict accordance with the standard format and requirements.

Mobile Check-in Range						
Area Name	Area Number	Effective Range	Map Type	Longitude	Latitude	Address
Area Name	2	50 Baidu Map		114.149886	22.938765	No. 51 Binhe Road, Dongguan City, Guangdong Province

Step 3: Click "Import" and select the completed table with filled information.

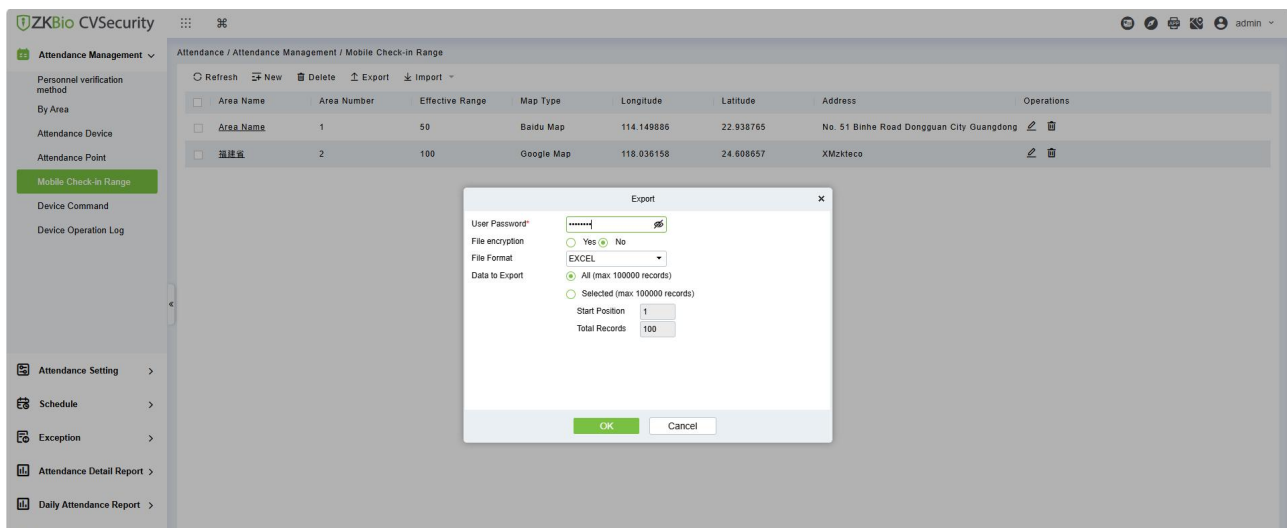


A successful import will display the following interface:



● Bulk Export of Check-in Ranges

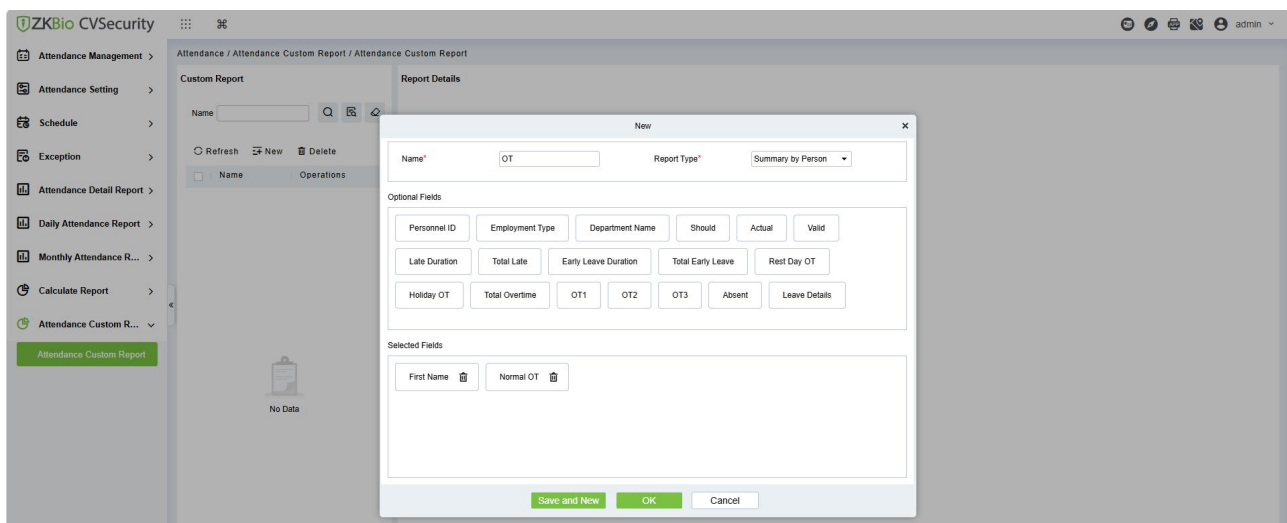
Click "Export" and enter the user password to complete the export.



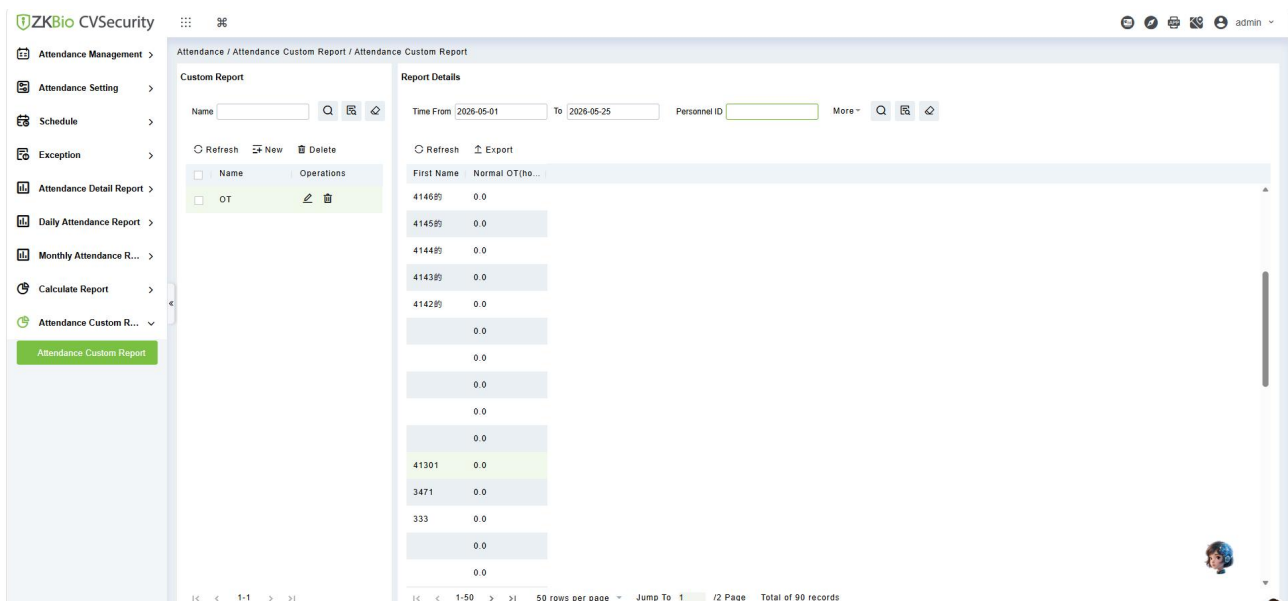
A	B	C	D	E	F	G
			Mobile Check-in Range			
Area Name	Area Number	Effective Range	Map Type	Longitude	Latitude	Address
Area Name	1	50	Baidu Map	114.149886	22.938765	No. 51 Binhe Road Dongguan City Guangdong Prov
福建省	2	100	Google Map	118.036158	24.608657	XMsktcco

3.3. Attendance Custom Report: Support splitting report fields to display only the fields selected by users.

Navigate to "Attendance / Attendance Custom Report / Attendance Custom Report", click New, enter the report name, select the report type, and tick the fields to be displayed.



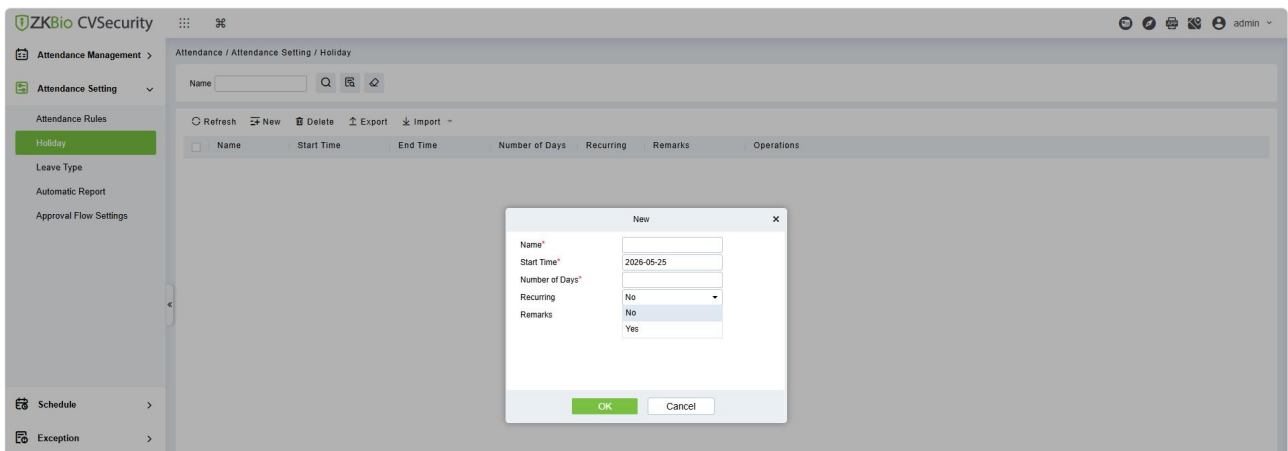
After creation, the custom report will only present the selected fields.



3.4. Attendance Setting / Holiday: Support annual cycle recurrence, with permission control for template download, import and export functions.

- Annual cycle recurrence supported in both list and import template

Navigate to "Attendance / Attendance Setting / Holiday". A new parameter "Recurring" is added. Users may configure this option as needed when creating new holidays. The holiday list will display a new column "Recurring" after creation.



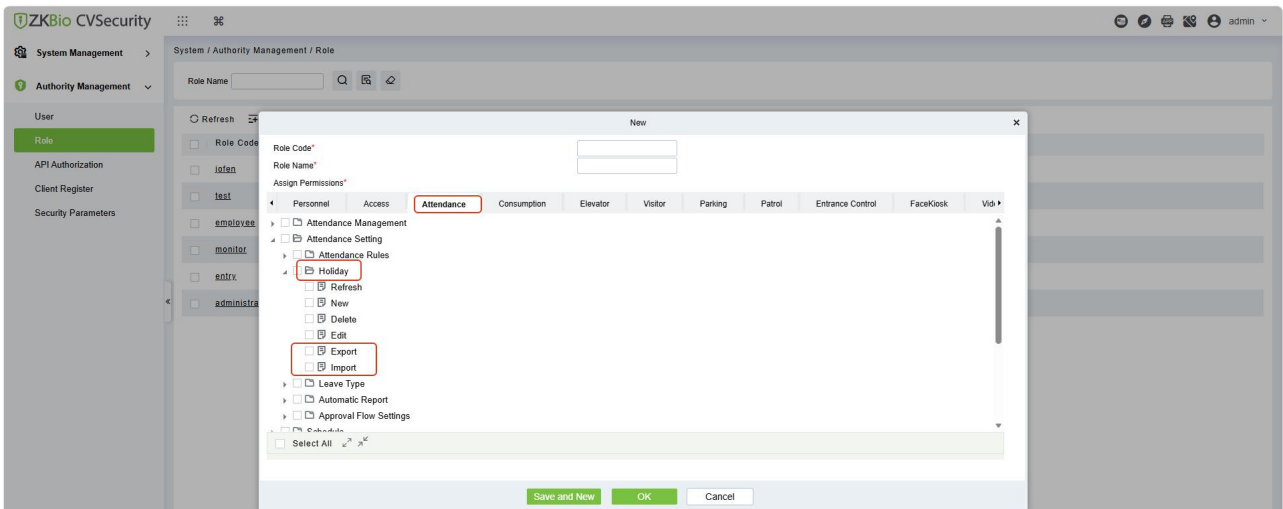
The import template is also updated with the "Recurring" field.

Holiday				
Name	Start Time	Number of Days	Recurring	Remarks

- Permission control for template download, import and export, consistent with the access control module

Go to "System / Authority Management / Role". When assigning permissions to roles, administrators can tick corresponding permissions to restrict template download, import and export of holiday data under the attendance module.

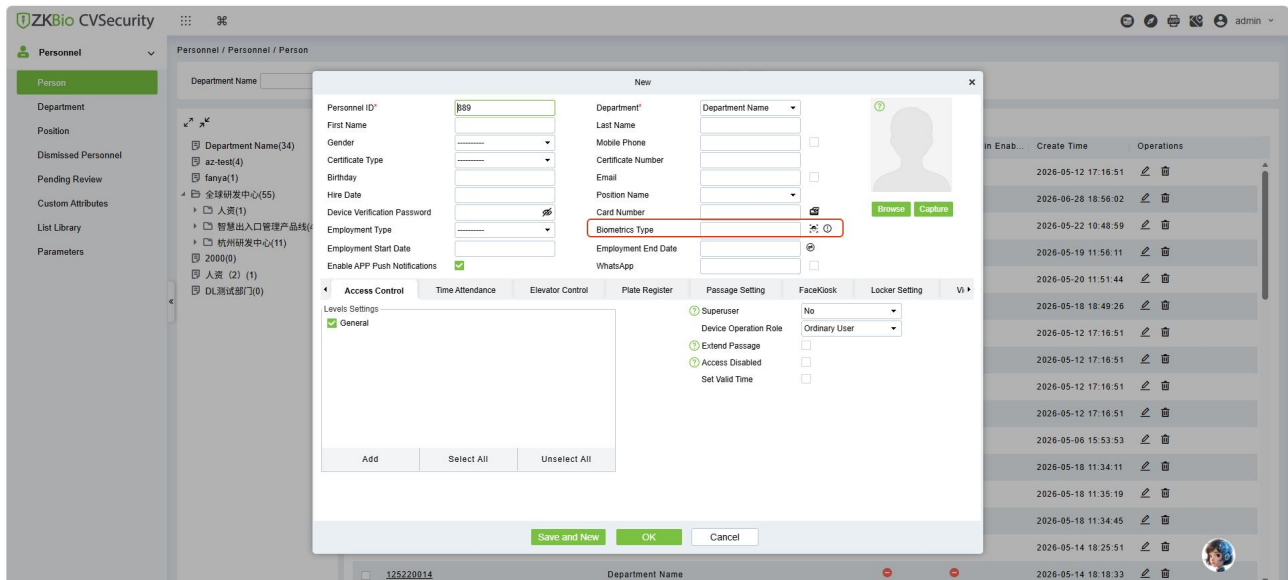
Note: Template download and data import are governed together by the "Import" permission checkbox.



4. Personnel

4.1. Personnel / Person: Optimize the entry of biometric enrollment function for more prominent and intuitive access.

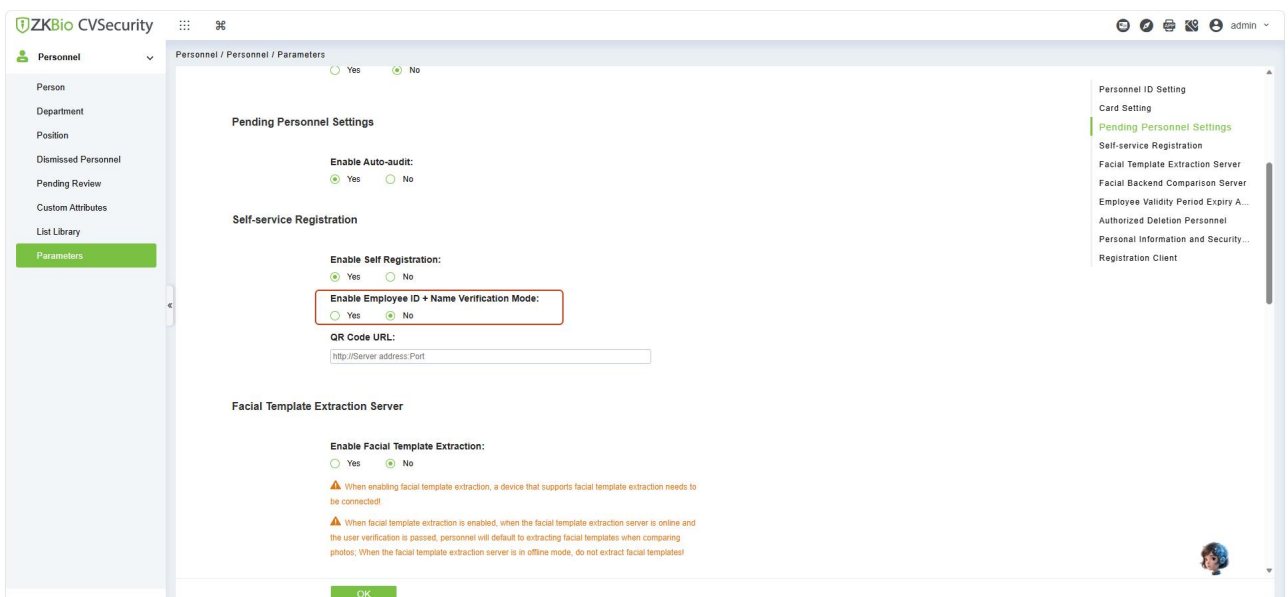
Navigate to "Personnel / Personnel / Person", click New to register staff information. The icon for biometric enrollment entry has been revised to make the function entry more intuitive.



4.2. Personnel / Parameters - Self-service Registration: New configuration parameter "Enable Employee ID + Name Verification Mode".

- **Remark:** Applicable to scenarios where customers have high security requirements for employee information registration.

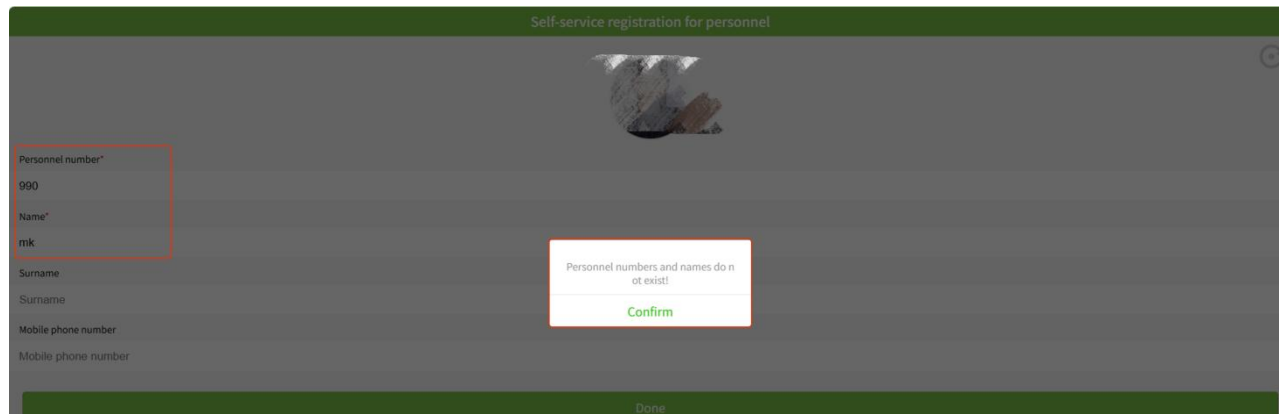
Navigate to "Personnel / Personnel / Parameters", where the new parameter "Enable Employee ID + Name Verification Mode" is available for configuration.



- When enabled: Users must enter both employee ID and full name on the H5 page and click Verify. Face template and mobile phone number registration is only allowed after successful verification (the ID exists and matches the corresponding name).

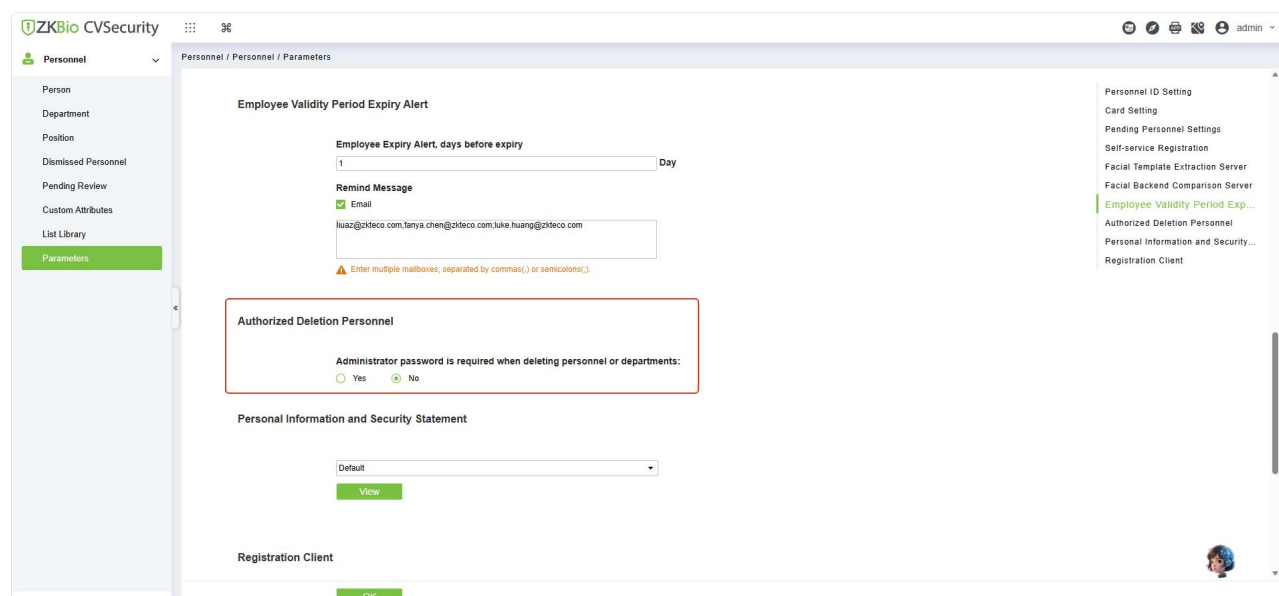
- When disabled: Users can complete registration directly without verification.

Self-service registration will be blocked if the employee ID and name do not match.



4.3. Personnel / Parameters - Authorized Deletion Personnel: Add new configuration parameter "Administrator password is required when deleting personnel or departments".

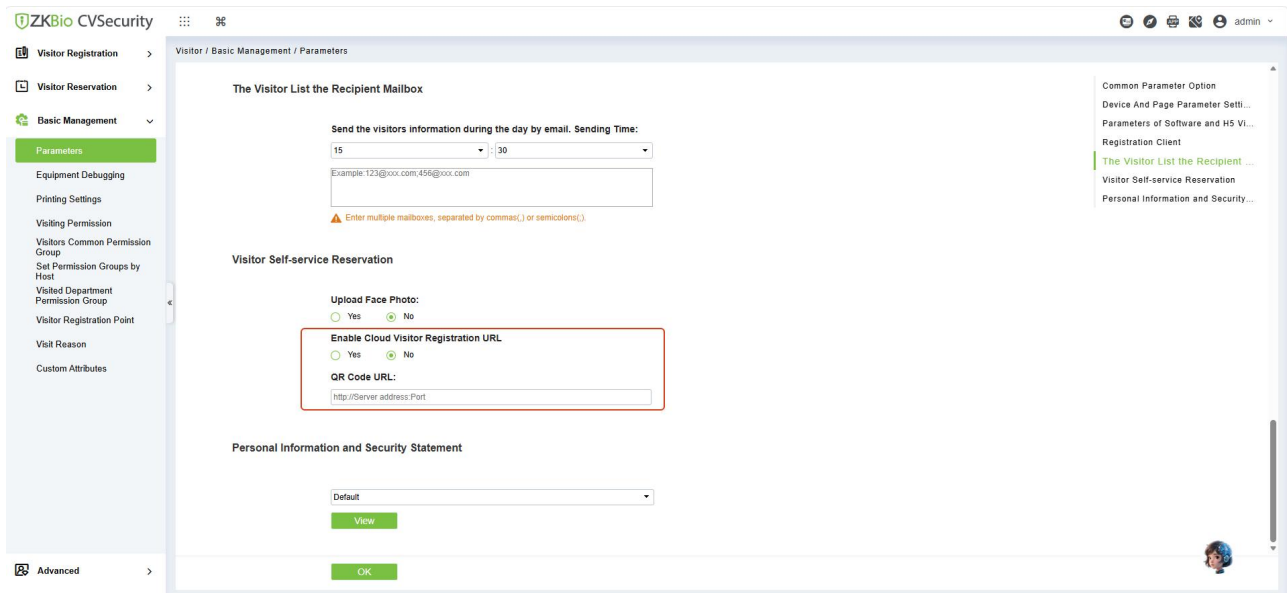
Navigate to "Personnel / Personnel / Parameters" to configure the newly added parameter "Administrator password is required when deleting personnel or departments". This parameter is disabled by default. Once enabled, administrator password verification is mandatory before completing any deletion operations in the personnel module, including single personnel deletion, single department deletion and batch deletion.



5. Visitor Management

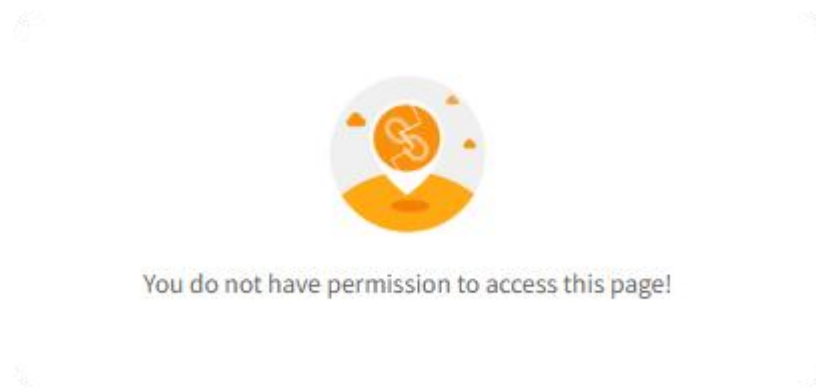
5.1. Basic Management / Parameters: The hybrid cloud link will become unavailable after disabling cloud visitor reservation.

Navigate to "Visitor / Basic Management / Parameters" - Visitor Self-service Reservation. Select "No" under the "Enable Cloud Visitor Registration URL" option, then click "OK".



The screenshot shows the ZKBio CVSecurity web interface. The left sidebar contains a menu with 'Visitor Registration', 'Visitor Reservation', and 'Basic Management'. Under 'Basic Management', 'Parameters' is selected. The main content area is titled 'Visitor / Basic Management / Parameters' and contains several sections: 'The Visitor List the Recipient Mailbox', 'Visitor Self-service Reservation', and 'Personal Information and Security Statement'. In the 'Visitor Self-service Reservation' section, the 'Enable Cloud Visitor Registration URL' option is set to 'No' and is highlighted with a red box. The 'QR Code URL' field is also visible. The 'Personal Information and Security Statement' section has a 'Default' dropdown and a 'View' button. The bottom of the interface has an 'OK' button.

Enter the original QR code URL into the web browser, and the page shown in the figure below will pop up; the link can no longer be accessed.



5.2. Visitor Registration / Visitor Check-in – Optimized display box for visited personnel to show full names.

Navigate to "Visitor / Visitor Registration / Visitor Check-in" and click "Visitor Check-in". After entering the information of the visited staff, the optimized display box can fully display long names without truncation.

5.3. Basic Management / Parameters: Configurable mandatory fields for visitor registration page (Applicable to PC and H5).

Navigate to "Visitor / Basic Management / Parameters" – Parameters of Software and H5 Visitor Registration Page, and check corresponding configuration options.

- On the page "Visitor / Visitor Registration / Visitor Check-in", the checked items will be set as mandatory input fields.

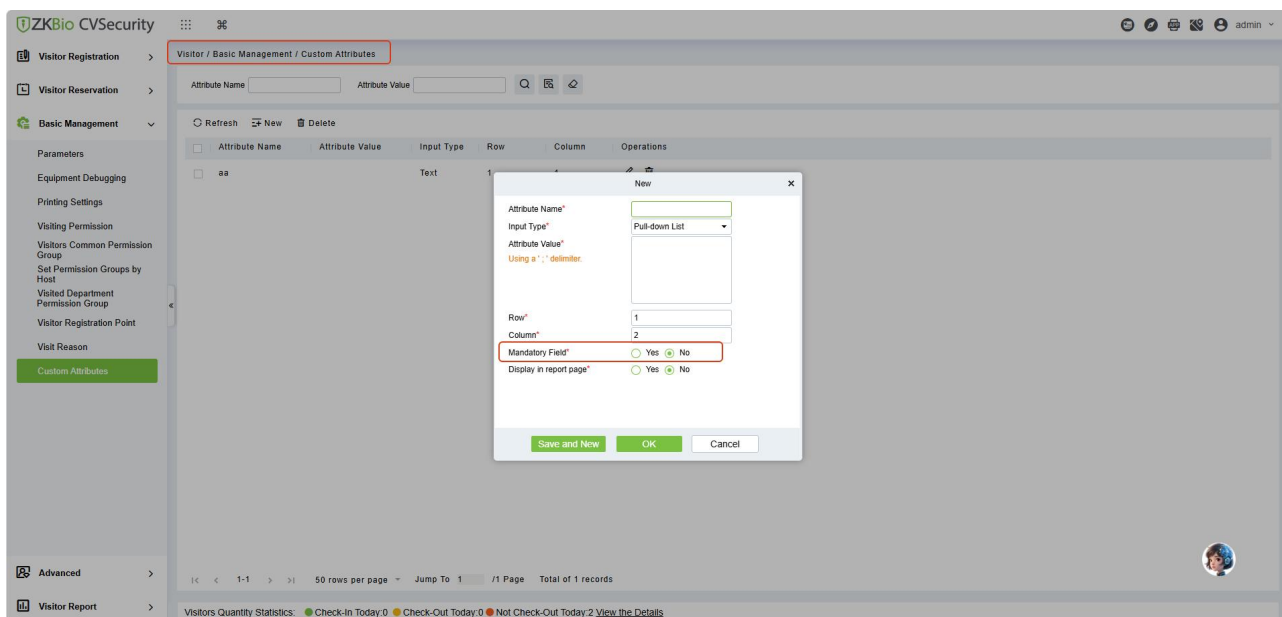
The screenshot shows the 'New' visitor registration form in the ZKBio CVSecurity system. The form is divided into several sections: 'Visitor Contact' (with fields for First Name, Last Name, Mobile Phone, Email, and Gender), 'Certificate' (with fields for Certificate Type, Certificate No., and License Plate), 'Permission' (with fields for Visitor Access Level, Default Floor, Start Time, End Time, Card Number, and Biometrics Type), and 'Capture' (with options for Captured Photo and Certificate Photo). Red boxes highlight the 'Email' field, 'Mobile Phone' field, and 'Gender' field, indicating they are mandatory. The form also includes a 'Select capture camera' dropdown and buttons for 'Print Preview', 'Save and New', 'OK', and 'Cancel'.

- On the H5 terminal page, the corresponding checked fields are also marked as required.

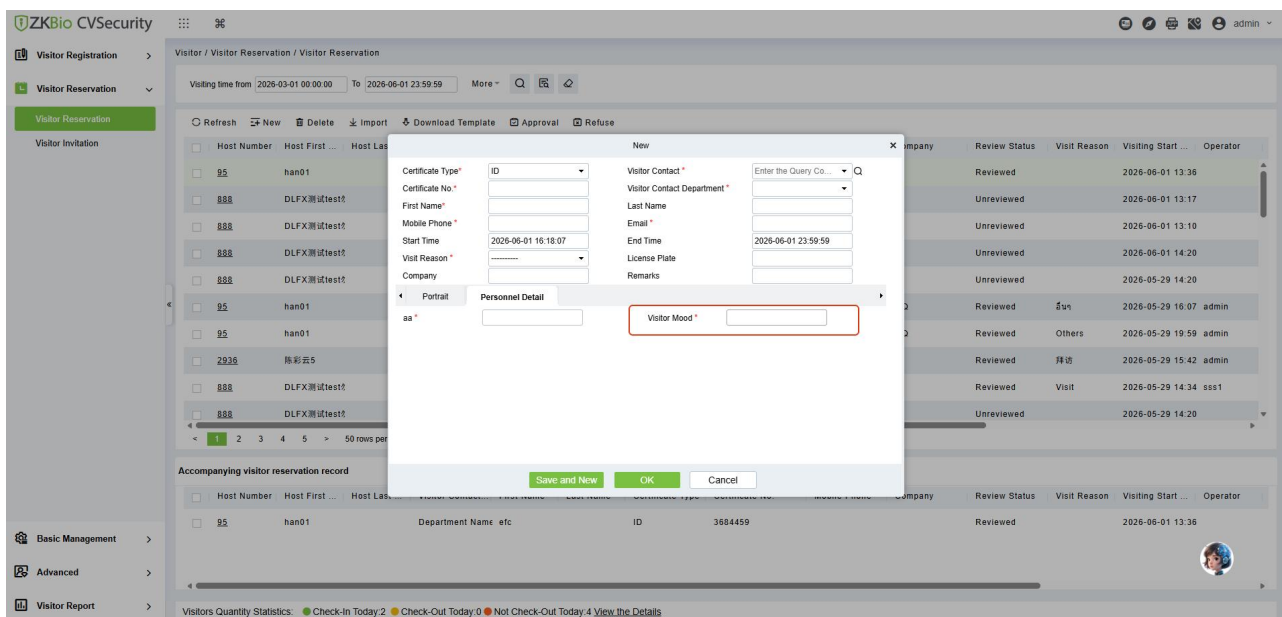
The screenshot shows the H5 terminal page of the visitor registration form. The form is divided into several sections: 'Visitor Contact' (with fields for First Name, Last Name, Mobile Phone, Email, and Gender), 'Certificate' (with fields for Certificate Type, Certificate No., and License Plate), 'Permission' (with fields for Visitor Access Level, Default Floor, Start Time, End Time, Card Number, and Biometrics Type), and 'Capture' (with options for Captured Photo and Certificate Photo). Red asterisks (*) next to the 'Email' field, 'Mobile Phone' field, and 'Gender' field indicate they are mandatory.

5.4. Basic Management / Custom Attributes: Add configuration option to set whether custom fields are mandatory. If a field is marked mandatory, visitors must fill in this field completely on both visitor registration and visitor reservation pages to save records successfully.

Navigate to "Visitor / Basic Management / Custom Attributes" and click New. Check or uncheck the "Mandatory Field" parameter to control whether the custom attribute is required.



Navigate to "Visitor / Visitor Reservation / Visitor Reservation", click New - Personnel Details. Custom attributes marked as mandatory will be displayed.



Navigate to "Visitor / Visitor Registration / Visitor Check-in", click New - Personnel Details. Custom attributes marked as mandatory will also be shown.

The screenshot shows the 'New' form for Visitor Registration / Visitor Check-In. The form is divided into several sections: Visitor Contact, Certificate, Permission, and Personnel Detail. The 'Visitor Mood' field in the Personnel Detail section is highlighted with a red box. The form also includes a 'Print Preview' button and a 'Save and New' button.

5.5. Advanced / Notification Template – Supports uploading file attachments.

Navigate to Visitor / Advanced / Notification Template, then click New. Select Email as the template type and Registration or Reservation as the event type. Check the sending rules and fill in the email subject. Under the Visitor Information section, tick the display fields; the system supports uploading relevant attachments in image and PDF formats.

The screenshot shows the 'Edit' form for the Advanced / Notification Template. The form is divided into several sections: Template Name, Template Type, Event Type, Send Rule, Subject, Body, Visitor Info, and Bottom. The 'Attachments' field in the Visitor Info section is highlighted with a red box. The form also includes a 'Browse' button and a 'Cancel' button.

Once the template configuration takes effect, the system will send email notifications automatically with the corresponding attachments and images attached when visitors complete registration or reservation.



5.6. Visitor Registration / Visitor Check-in – Supports selecting a connected USB camera from a drop-down list during image capture.

Navigate to Visitor / Visitor Registration / Visitor Check-in, click Visitor Check-In. After connecting your camera hardware, you may select any connected USB camera device via the dropdown menu.

New

Visitor Contact * Visitor Contact Department *

Certificate Type * Certificate No. *

First Name * Last Name

Company Mobile Phone *

Country/Region Visitor Quantity *

Email * Remarks

Visit Reason *

Entering Location *

Gender *

License Plate

Items Carried

Permission

Visitor Access Level Start Time * End Time *

Default Floor Card Number Biometrics Type

Capture

Captured Photo

No camera connected.

Certificate Photo

No camera connected.

Select capture camera

Print Preview Save and New OK Cancel

5.7. Visitor Registration / Visitor Check-in – Supports print preview on the registration interface.

Navigate to Visitor / Visitor Registration / Visitor Check-in, click Visitor Check-In. The Print Preview option box is displayed at the bottom of the page.

- Prerequisite: Install the printing control correctly under Local Settings in Visitors / Basic Visitor Management / Print Settings.

After filling in visitor information, click Print Preview to view the printing effect preview.

Visitor Badge
Visit Time: 2026-06-01 18:14:24



Visitor Name _____
 Gender _____
 Visit Reason _____
 Certificate Type ID _____
 Document No. _____
 Company _____
 Visitor's Contact _____
 Carrying Goods _____



5.8. Visitor Registration, Visitor Reservation, Visitor Report, Daily/Weekly/Monthly Visitor Access Reports – Adds license plate filter condition.

- Navigate to Visitor / Visitor Registration / Visitor Check-in, click More. The page supports entering License Plate as a filter condition.

Visitor Registration / Visitor Check-in

Name _____ Certificate No. _____ Certificate Type _____ Retract Q 🔍 🔗

Visit Status _____ Visit Reason _____ Visitor ID _____
 Host Name _____ License Plate

☐	800000218	193773788888	Others	28262	Check-In	2026-05-29 13:58	server	Area Name
☐	800000218	2107966	ID		Check-In	2026-05-29 09:58	server	Area Name
☐	800000217	199766646666	Others		Check-In	2026-05-29 09:56	server	Area Name
☐	800000216	18846666999	Others	28262	Check-In	2026-05-29 09:55	server	Area Name
☐	800000215	9466133	Others	28259	Late Check-Out	2026-05-29 09:46	server	Area Name

- Navigate to Visitor / Visitor Reservation / Visitor Reservation, click More. The page supports entering License Plate as a filter condition.

ZKBio CVSecurity

Visitor / Visitor Reservation / Visitor Reservation

Visiting time from 2026-03-01 00:00:00 To 2026-05-29 23:59:59 Retract Q 🔍 🔗

Visit Reason _____ Visit Status _____ Certificate Type _____
 Name _____ Certificate No. _____ Host Name _____
 Company _____ Review Status _____ License Plate

☐	95	han01	Department Name	ID	151928	18255556666	QQ	Reviewed	Others	2026-05-
--------------------------	----	-------	-----------------	----	--------	-------------	----	----------	--------	----------

- Navigate to Visitor / Visitor Report / Visiting Record, click More. The page supports entering License Plate as a filter condition.

Visitor / Visitor Report / Visiting Record

Entry time from 2026-03-01 00:00:00 To 2026-05-29 23:59:59 Visitor ID _____ Retract Q 🔍 🔗

Name _____ Visit Reason _____ Company _____
 Host Name _____ Visit Status _____ Certificate No. _____
License Plate

☐	800000218	2107966	2985		Check-In	2026-05-29 09:56	server
☐	800000217	199766646666	528004	fanya	Check-In	2026-05-29 09:56	server
☐	800000216	18846666999	28262	Department Ni	Check-In	2026-05-29 09:55	server
☐	800000215	9466133	28259	Department Ni	Late Check-Out	2026-05-29 09:46	server
☐	800000214	737363728826	2831		Check-Out	2026-05-28 17:13	server

- Navigate to Visitor / Visitor Report / Daily Visitor Report, click More. The page supports entering License Plate as a filter condition.

Visitor / Visitor Report / Daily Visitor Report

Visitor ID: Name: Host Name: Retract Q 🔍 🔗

Visit Reason: Company: Visit Status:

Certificate No.: License Plate

☐	800000219	访客6	19377378888	28262	员工28262	Department N:	Check-In	2026-05-29 13:58	server
☐	800000218	访客4	2107966	2985	曾扬明	技术服务部	Check-In	2026-05-29 09:58	server
☐	800000217	访客2	19976664666	528004	不	fanya	Check-In	2026-05-29 09:56	server
☐	800000216	访客2	18846666999	28262	员工28262	Department N:	Check-In	2026-05-29 09:55	server
☐	800000215	访客	9466133	28259	员工28259	Department N:	Late Check-Out	2026-05-29 09:46	server

- Navigate to Visitor / Visitor Report / Weekly Visitor Report, click More. The page supports entering License Plate as a filter condition.

Visitor / Visitor Report / Weekly Visitor Report

Visitor ID: Name: Host Name: Retract Q 🔍 🔗

Visit Reason: Company: Visit Status:

Certificate No.: License Plate

☐	800000219	访客6	19377378888	28262	员工28262	Department N:	Check-In	2026-05-29 13:58	server
☐	800000218	访客4	2107966	2985	曾扬明	技术服务部	Check-In	2026-05-29 09:58	server
☐	800000217	访客2	19976664666	528004	不	fanya	Check-In	2026-05-29 09:56	server
☐	800000216	访客2	18846666999	28262	员工28262	Department N:	Check-In	2026-05-29 09:55	server
☐	800000215	访客	9466133	28259	员工28259	Department N:	Late Check-Out	2026-05-29 09:46	server
☐	800000214	员工1	737363728828	2831	叶娇凤2	系统测试部	Check-Out	2026-05-28 17:13	server
								2026-05-29 02:00	

- Navigate to Visitor / Visitor Report / Monthly Visitor Report, click More. The page supports entering License Plate as a filter condition.

Visitor / Visitor Report / Monthly Visitor Report

Visitor ID: Name: Host Name: Retract Q 🔍 🔗

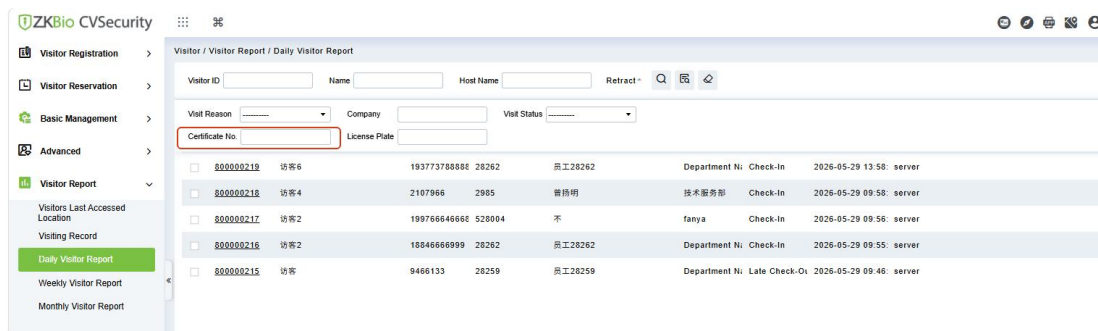
Visit Reason: Company: Visit Status:

Certificate No.: License Plate

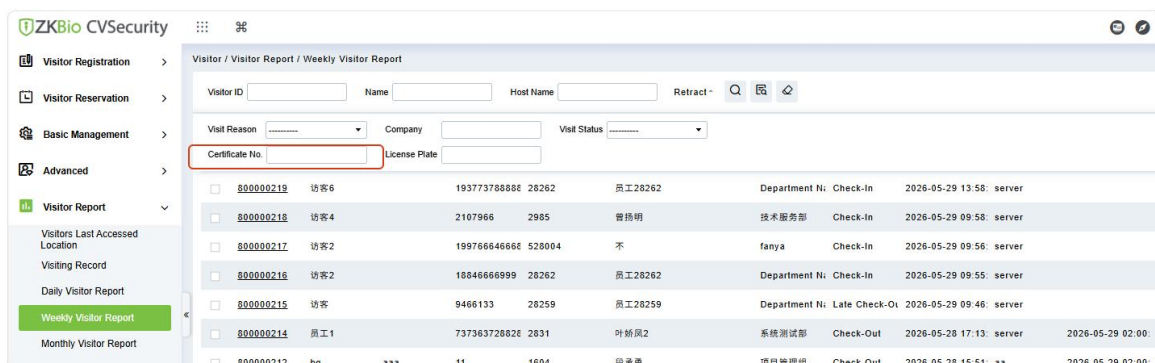
☐	800000219	访客6	19377378888	28262	员工28262	Department N:	Check-In	2026-05-29 13:58	server
☐	800000218	访客4	2107966	2985	曾扬明	技术服务部	Check-In	2026-05-29 09:58	server
☐	800000217	访客2	19976664666	528004	不	fanya	Check-In	2026-05-29 09:56	server
☐	800000216	访客2	18846666999	28262	员工28262	Department N:	Check-In	2026-05-29 09:55	server
☐	800000215	访客	9466133	28259	员工28259	Department N:	Late Check-Out	2026-05-29 09:46	server
☐	800000214	员工1	737363728828	2831	叶娇凤2	系统测试部	Check-Out	2026-05-28 17:13	server
								2026-05-28 17:13	server

5.9. Visitor Report - Daily/Weekly/Monthly Visitor Reports – Adds certification number filter condition.

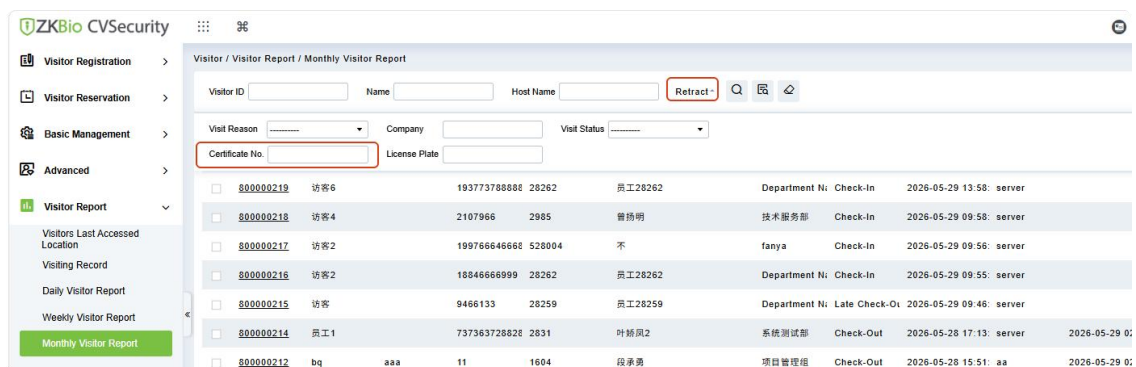
- Navigate to Visitor / Visitor Report / Daily Visitor Report, click More. The page supports entering Certificate No. as a filter condition.



- Navigate to Visitor / Visitor Report / Weekly Visitor Report, click More. The page supports entering Certificate No. as a filter condition.



- Navigate to Visitor / Visitor Report / Monthly Visitor Report, click More. The page supports entering Certificate No. as a filter condition.



5.10. Devices – Supports visitor terminals with BEST Protocol.

Navigate to Visitor / Basic Management / Visitor Registration Point, click New. Select Visitor Equipment - BEST in the Visitor Machine Type dropdown.

ZKBio CVSecurity 86

Visitor / Basic Management / Visitor Registration Point

Registration Point Name

Refresh New Delete Automatic Check-Out Location

Registration Point Name	IP Address	Area Name	Visitor Machine...	Photo Collection	Document Coll...	IP Camera Na...	Operations
96	10.8.24.30	Area Name	Ordinary Comput	USB Camera	USB Camera		
96	10.8.16.96	Area Name	Ordinary Comput	USB Camera	USB Camera		
test1	10.8.14.3	Area Name	Ordinary Comput	USB Camera	USB Camera		
9/3	192.168.137.2	Area Name	Ordinary Comput	USB Camera	USB Camera		
V13-test	10.8.42.23	12楼abcodeghi	Visitor Equipment	USB Camera	USB Camera		
V13	10.8.42.23	12楼abcodeghi	Visitor Equipment	USB Camera	USB Camera		
1111	10.8.16.86	福建省	Ordinary Comput	USB Camera	USB Camera		
123	10.8.51.243	Area Name	Ordinary Comput	USB Camera	USB Camera		
1000A	10.8.16.170	Area Name	Ordinary Comput	USB Camera	USB Camera		
server	127.0.0.1	Area Name	Ordinary Comput	USB Camera	USB Camera		

New

Registration Point Name*

IP Address*

Physical information*

Visitor Machine Type

Photo Collection

Document Collection

Default permissions

Area Name*

Test Connection

Save and New OK Cancel

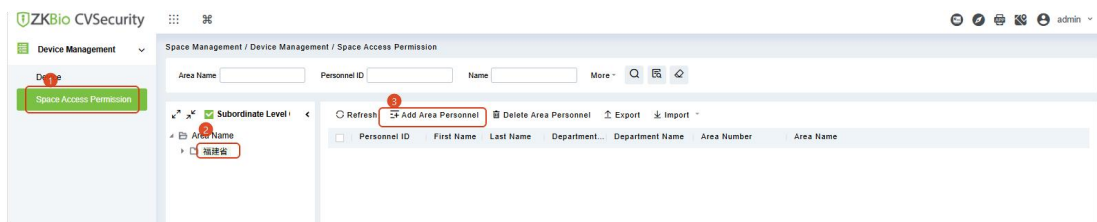
6. Space Management

6.1. Device Management / Space Access Permission - Supports batch-assigning administrators by zone for multi-administrator space management. Administrators can verify their identity and enter their designated meeting rooms directly without a reservation.

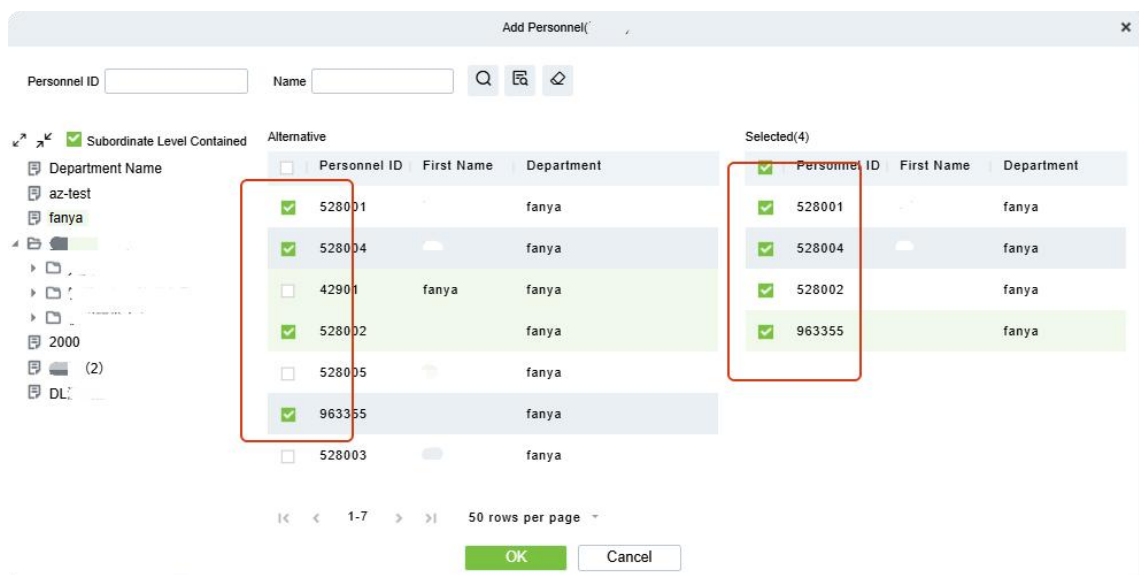
- **Hardware devices supporting this function:** DG03-A9W10, DG03-A9W15(ZKBioMeet Version 1.2.0)

Two configuration methods:

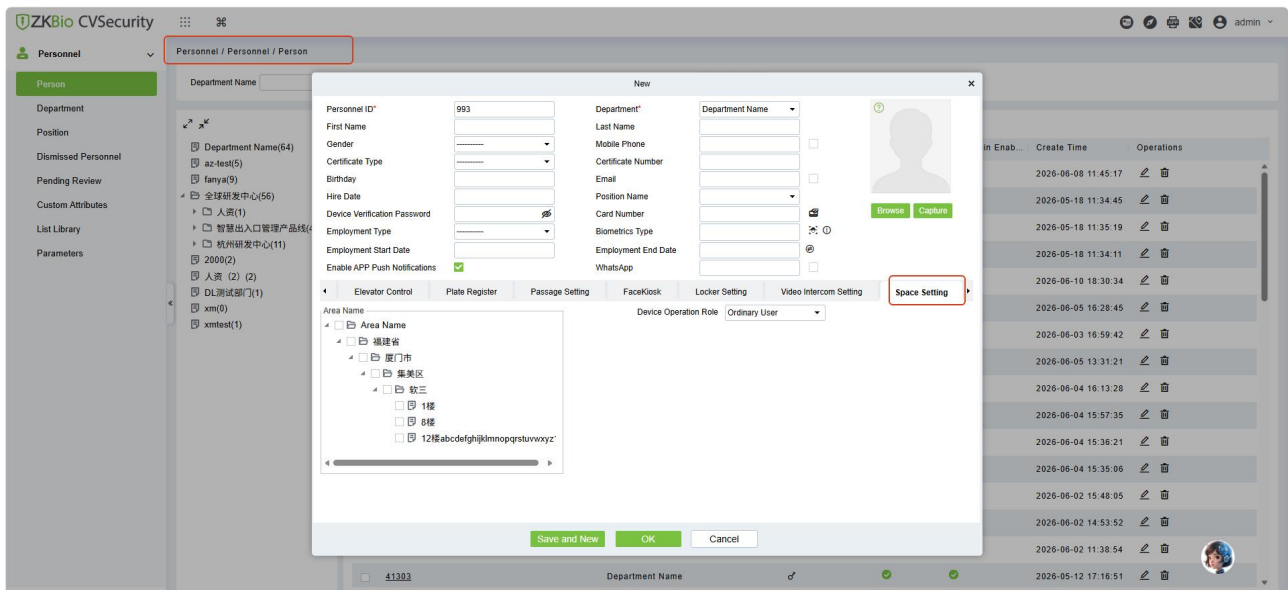
① Navigate to Space Management / Device Management / Space Access Permission. Since devices are bound to areas, select an area first and click "Add Area Personnel".



Then you adding administrators in batches. Click OK to complete the addition. Administrators can verify their identity and directly access meeting rooms within their jurisdiction without prior reservations.



② Navigate to Personnel / Personnel / Person, click New or select personnel to enter the editing page. Select Space Setting in the lower part of the editing page; the device operation role can be set to Ordinary User or Super Administrator.



- Notes: The area must be selected for the device operation permission to take effect.

Edit

Personnel ID* 990

First Name jh

Gender

Certificate Type

Birthday

Hire Date

Device Verification Password

Employment Type

Employment Start Date

Enable APP Push Notifications ☒

Department* Department Name

Last Name

Mobile Phone

Certificate Number

Email

Position Name

Card Number

Biometrics Type

Employment End Date

WhatsApp

Area Name

Area Name

Device Operation Role Super Administrator

Ordinary User

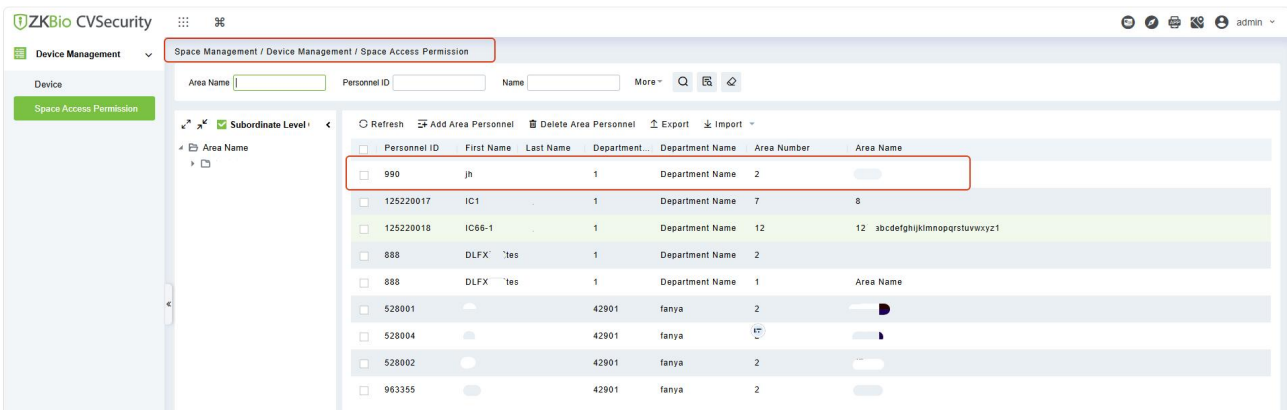
Super Administrator

OK Cancel

- Ordinary User space permission: Allows access verification without reservations or meeting credentials.

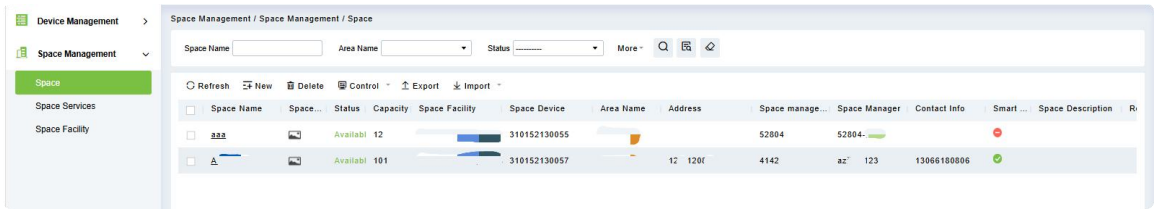
- Super Administrator space permission: Allows access verification without reservations or meeting credentials, device menu access, and meeting termination.

Personnel with configured device operation permissions here will be automatically synced to the list under Space Management / Device Management / Space Access Permission.

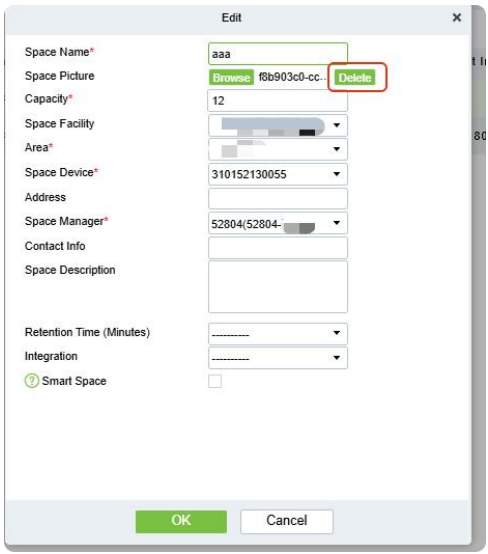
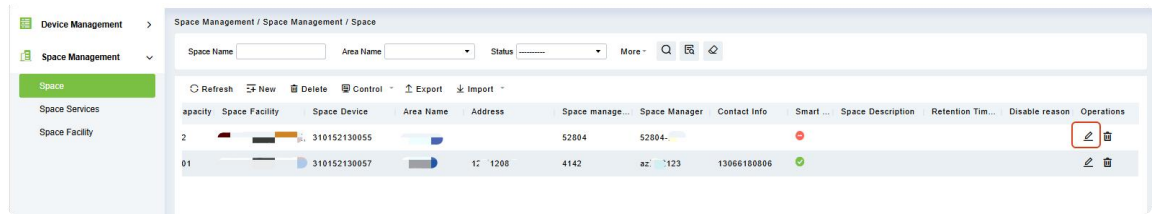


6.2. Space Management / Space - Supports deleting uploaded space images.

Navigate to Space Management / Space Management / Space, select a created space with uploaded images.



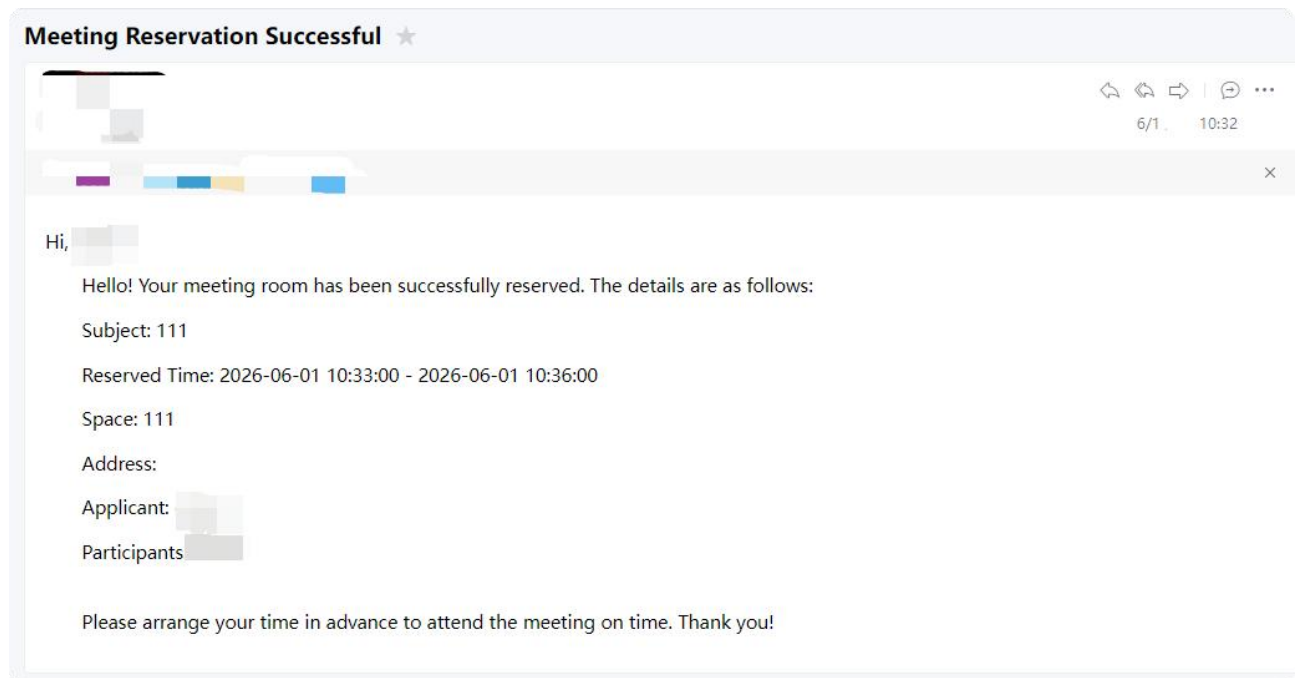
Click the edit icon, click Delete, then click OK. Return to the space page; the image will be removed.



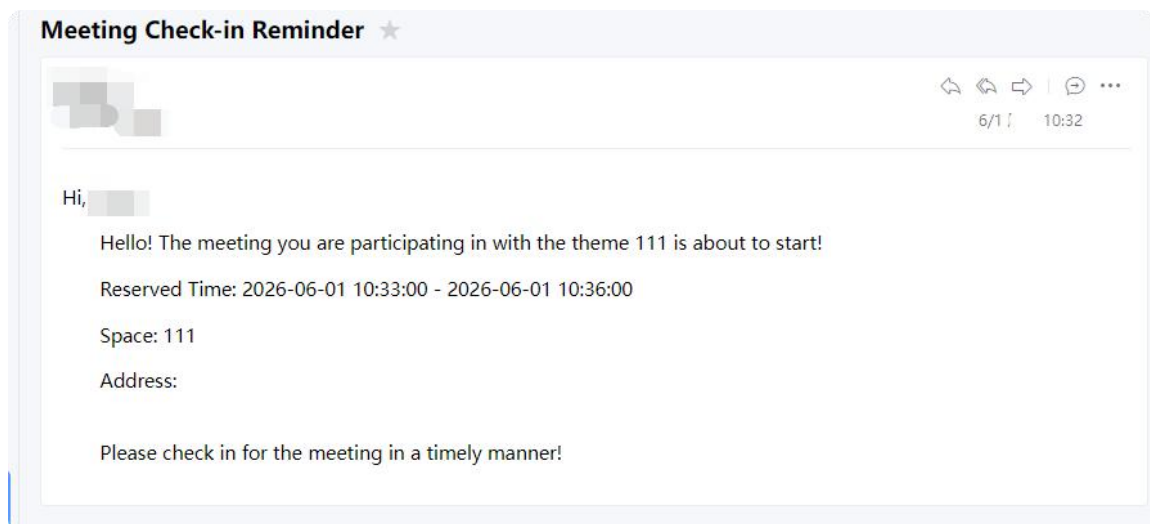
☐	Space Name	Space...	Status	Capacity	Space Facility	Space Device	Area Name	Address	Space manage...	Space Manager	Contact Info	Smart ...	Space Description	R
☐	aaa		Available	12		310152130055			52804	52804-				
☐	Δ		Available	101		310152130057		1205	4142	azt	23		13066180806	

6.3. Modification of Meeting Email Subject Names

- Change the current subject "Meeting Reservation Confirmation" to "Meeting Reservation Successful".

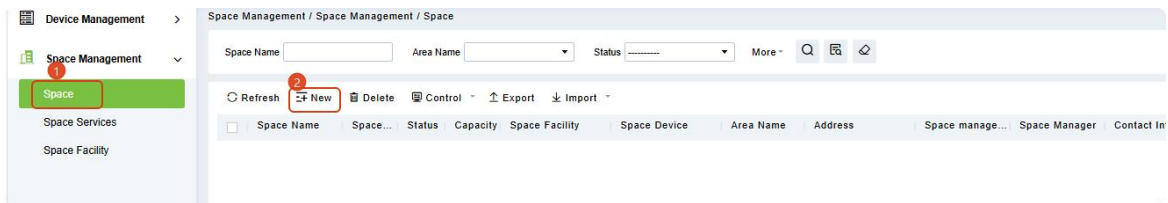


- Change the current subject "Meeting Service Preparation" to "Meeting Check-in Reminder".



6.4. System – Support pushing space and facility information to terminal devices for display.

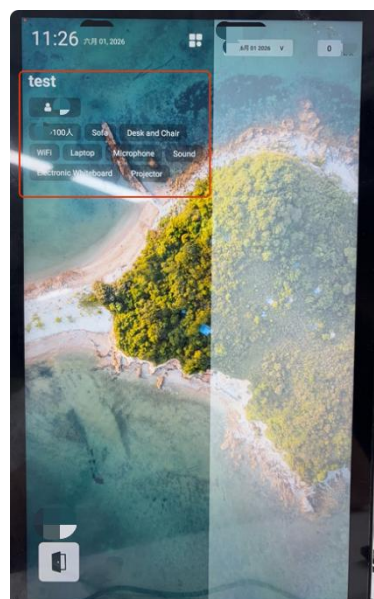
Navigate to Space Management / Space Management / Space and click New.



Enter Space Name and Capacity, select available Space Facilities within the space, and choose Area, Space Devices and Space Administrator, then click OK.

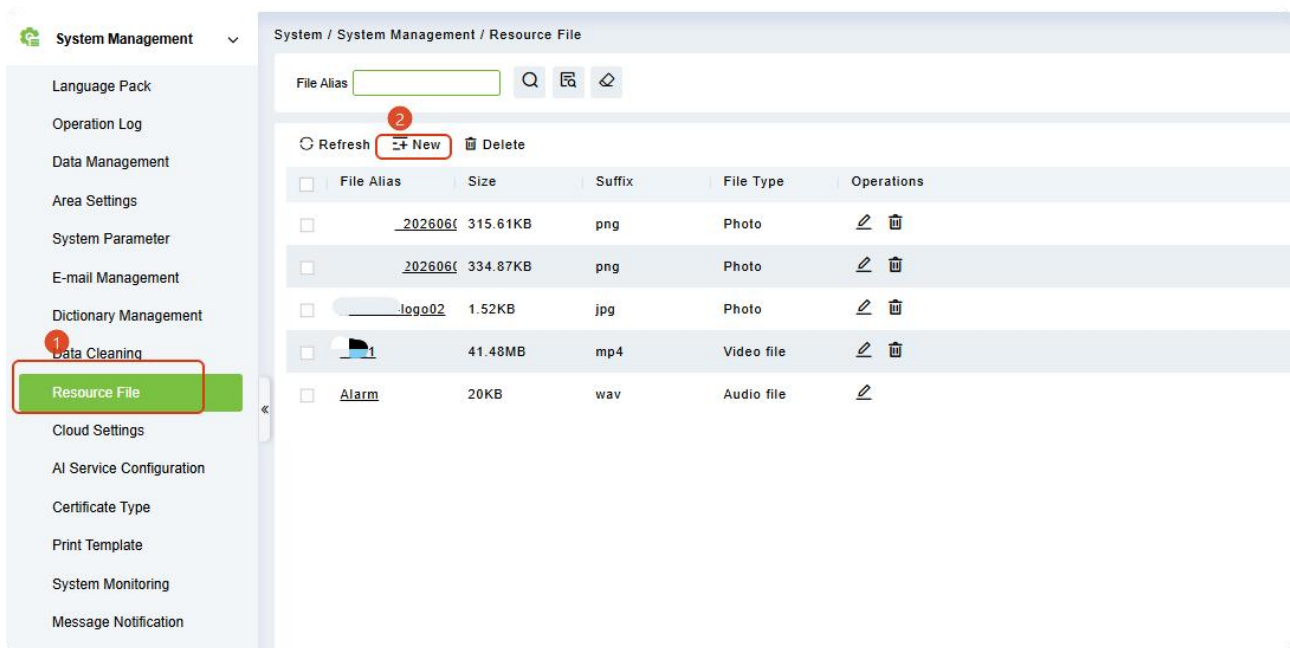
Space Name	Space...	Status	Capacity	Space Facility	Space Device	Area Name	Address	Space manage...	Space Manager	Contact Info	Smart ...	Space Description
test		Available	100	Laptop, Microphone, S	test	Area Name	1	cbq				

After the space is successfully bound to devices, space and facility information will be pushed to terminal devices for display.

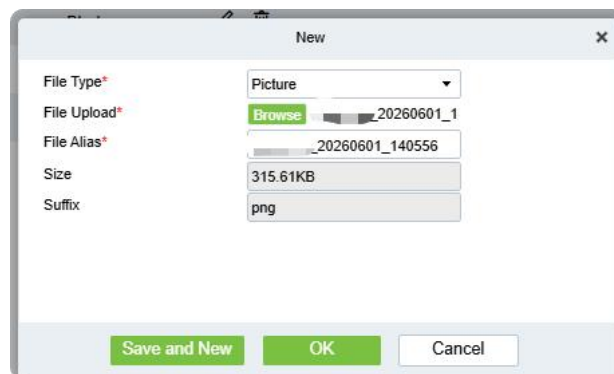


6.5. Device Management - Device – Support pushing wallpapers to devices.

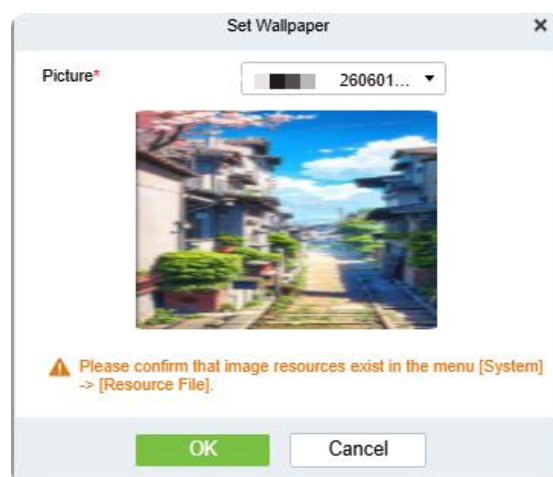
Step 1: Navigate to System / System Management / Resource File and click New.



Upload the wallpaper to be pushed, then click Save.



Step 2: Navigate to Space Management / Device Management / Device, check target devices and click Set Wallpaper.



The wallpaper on the device terminal will be updated.



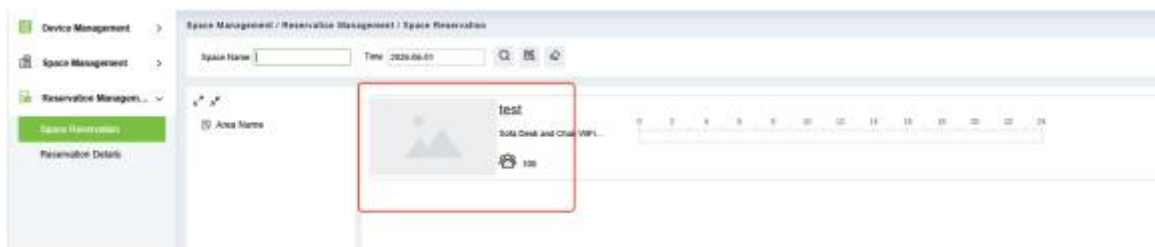
6.6. Statistics Report / Access Events - A new access record report is added. Under the multi-administrator management mode, all personnel access records of spaces are retained to facilitate subsequent behavior tracing and inquiry.

Navigate to Space Management / Statistics Report / Access Events to view detailed access records of personnel entering and exiting spaces.

Space Name	Event Time	Personnel ID	First Name	Last Name	Department Name
text	2026-06-01 14:38:47	1	cbq		Department Name
text	2026-06-01 14:38:45	1	cbq		Department Name
text	2026-06-01 14:38:44	1	cbq		Department Name

6.7. Reservation Management / Space Reservation - When administrators reserve meeting rooms on the PC client, the reservation applicant is automatically added to the attendee list by default without manual addition.

Navigate to Space Management / Reservation Management / Space Reservation and click Space.



Select the applicant; the reservation applicant will be automatically added to the attendee list with no manual operation required.

Space Reservation

Reservation Details

Applicant's Name*

1(cbq)

Applicant's Email

Start Time*

End Time*

Start Check-in Time*

At Start

Space Name*

text

Subject*

Content

Participants

Person's Name*

1(cbq)

Visitor Name

D+

D+

Space Services

Demand

Notification

Remind Time*

Reminder 5 minutes before

OK

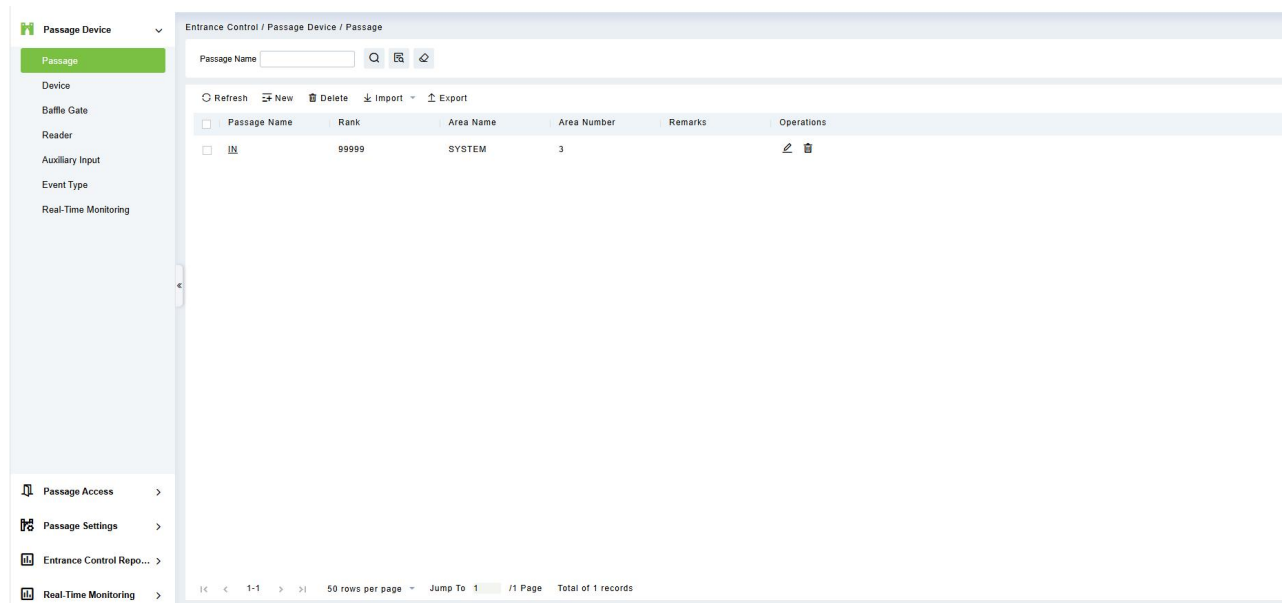
Cancel

7. Entrance Control (New passage module released with multimodal all-in-one machine-Zophon-S1000)

- Passage Device Firmware Version: Zophon-S1000 : 4.3.218-DH-34

7.1. Passage Device

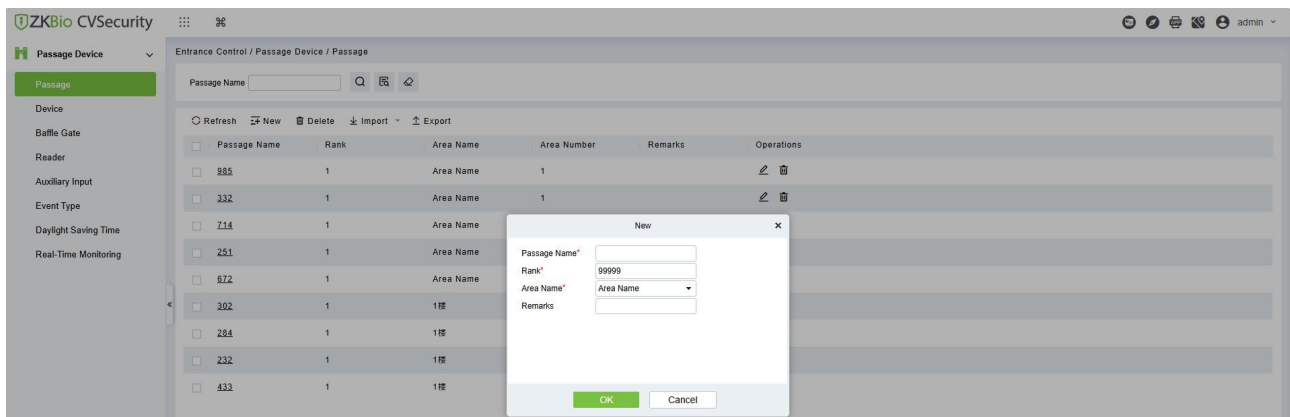
Subpages: Passage, Device, Baffle Gate, Reader, Auxiliary Input, Event Type, Daylight Saving Time, Real-Time Monitoring



Area Settings: Reuse the area settings under System Management for allocation and definition of passage areas. (Note: To enable cross-device operations, authorization management is supported for passage areas. For instance, under an administrator account, gate opening and closing permissions can be authorized for a specific passage area at the turnstile terminal.)

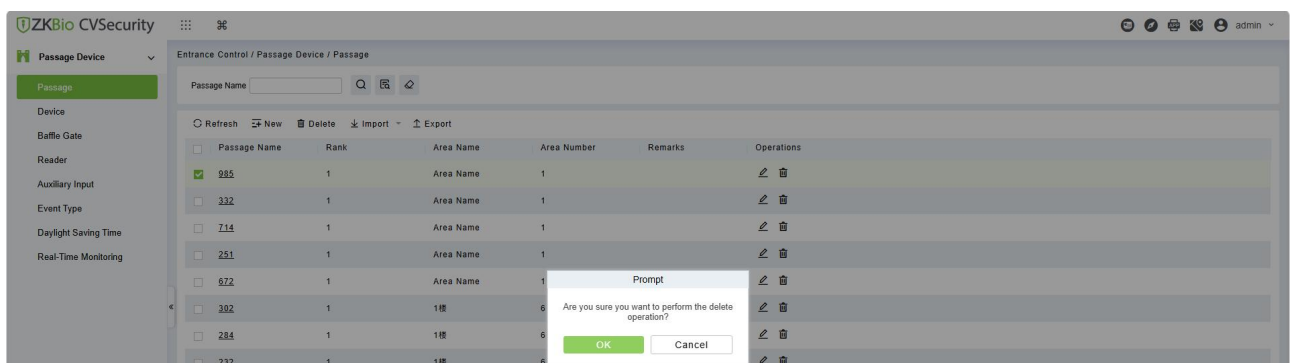
1.1. Passage: Define the area that the passage belongs to, facilitating users to manage passage devices within a specific region. After configuring passage, devices under passage can be filtered by region during real-time monitoring. The passage page supports Add, Edit, Delete, Import and Export functions.

- New: Navigate to Entrance Control / Passage Device / Device. Click the New button, and a pop-up window will display Passage Name, Rank, Area Name and Remarks.
- Passage Name: Any combination of characters with a maximum length of 20 characters, duplicates are not allowed.
- Rank: Only numeric values are supported, up to six digits, duplicates permitted. Entries with smaller sort order values appear earlier in Real-time Monitoring.
- Area Name: Select the affiliated region.
- Remarks: Any characters with a maximum length of 100 characters.

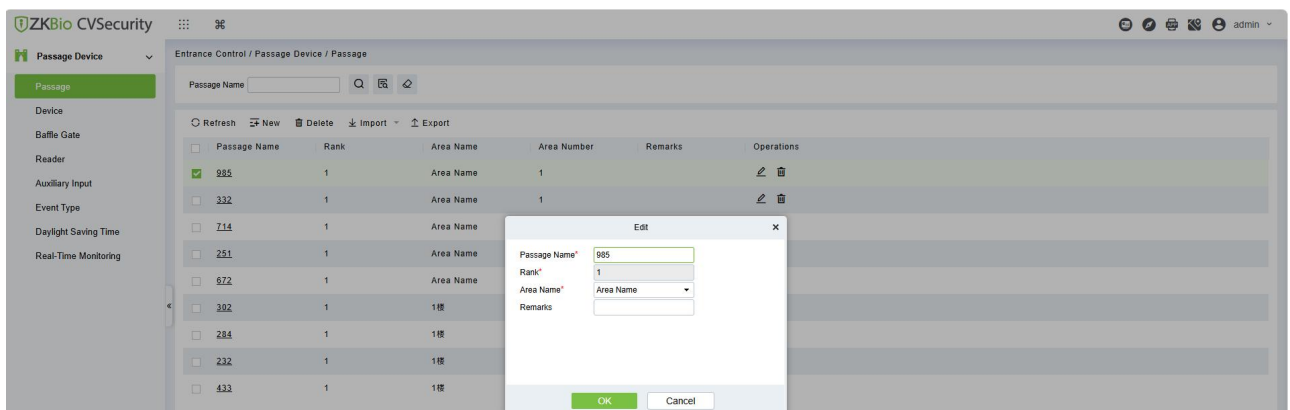


- Delete: Remove passage information after selecting the target passage.

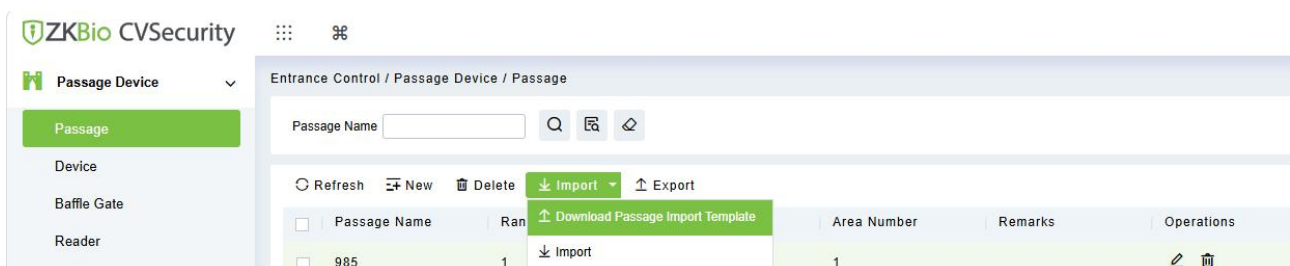
(Caution: Passage bound with devices cannot be deleted. Reassign the associated devices to other passage or delete the devices first before deleting the passage.)



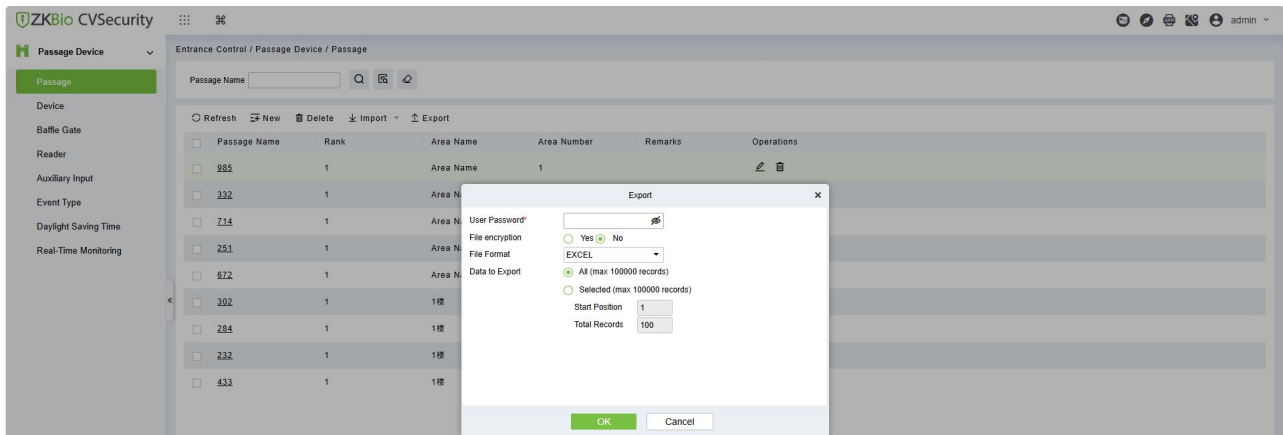
- Edit: Click [Edit] under the operation column of Passage Devices to modify passage information; all fields are consistent with those on the New page.



- Import: Click [Import] under the operation column of passage Devices. Supports importing passage data and downloading import templates.



- Export: Click [Export] under the operation column of passage Devices. Supports exporting passage information with configurable options including file encryption status, export formats (EXCEL/PDF/CSV), and export scope (Export All / Export Selected Data).



1.2. Device: Add channel devices and configure communication parameters for connected devices, including configurations in the system and channel device modules. After successful communication, users can view information of connected devices and perform operations such as control, configuration, viewing and data retrieval on the devices.

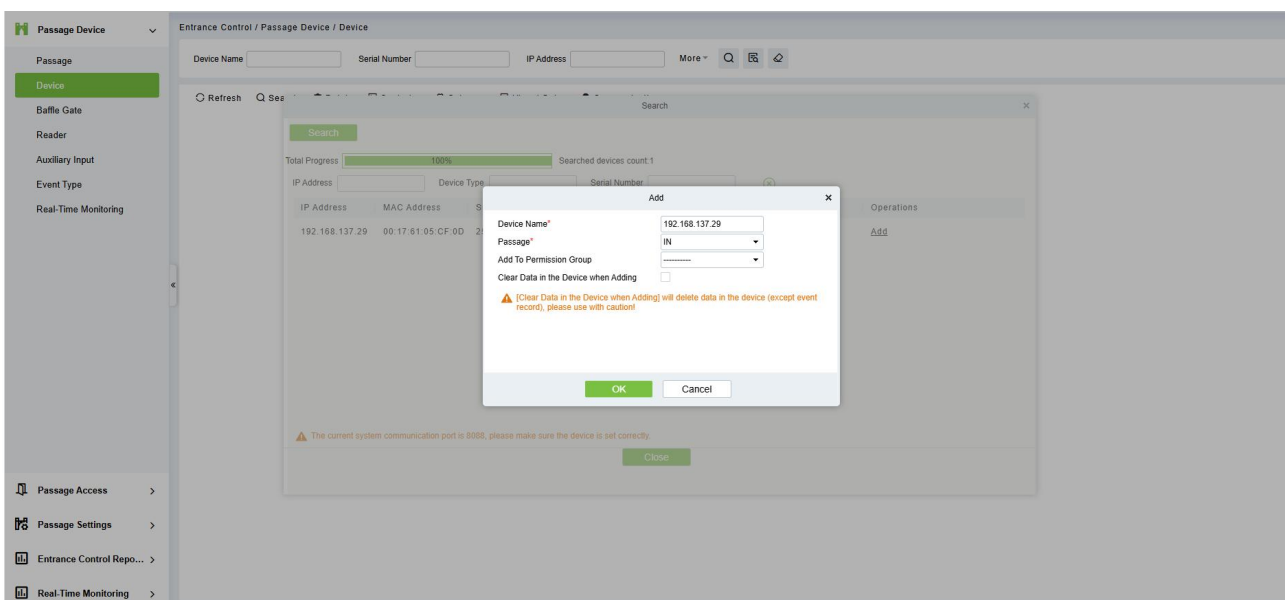
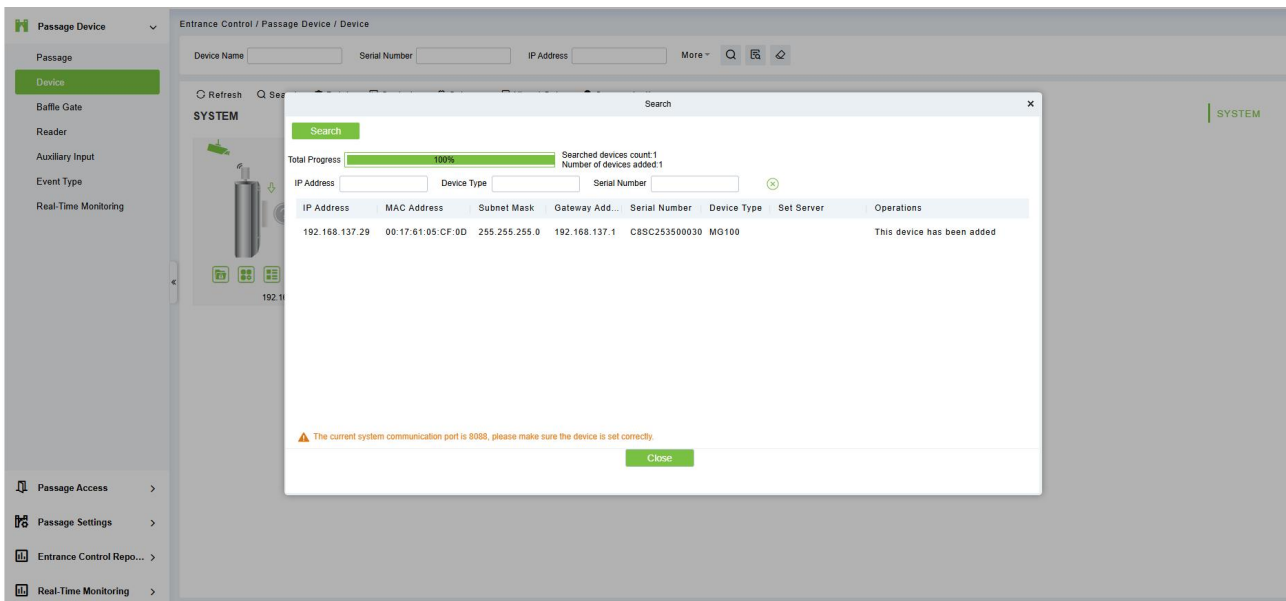
- Add Devices by Searching Access Controllers Search for access controllers in the Ethernet with the following procedures:

(1) Navigate to Entrance Control / Passage Device / Device.

(2) Click [Search], and the prompt "Searching..." will appear.

(3) Upon completion of the search, the channel list and total number of discovered devices will be displayed.

(4) Click [Add] next to the target device: An edit dialog box will pop up when a device is detected. Enter customized information including device name, channel name, access group assignment and channel binding (bind according to serial numbers corresponding to channel quantities). Click [OK] to finish adding the device to the device list.

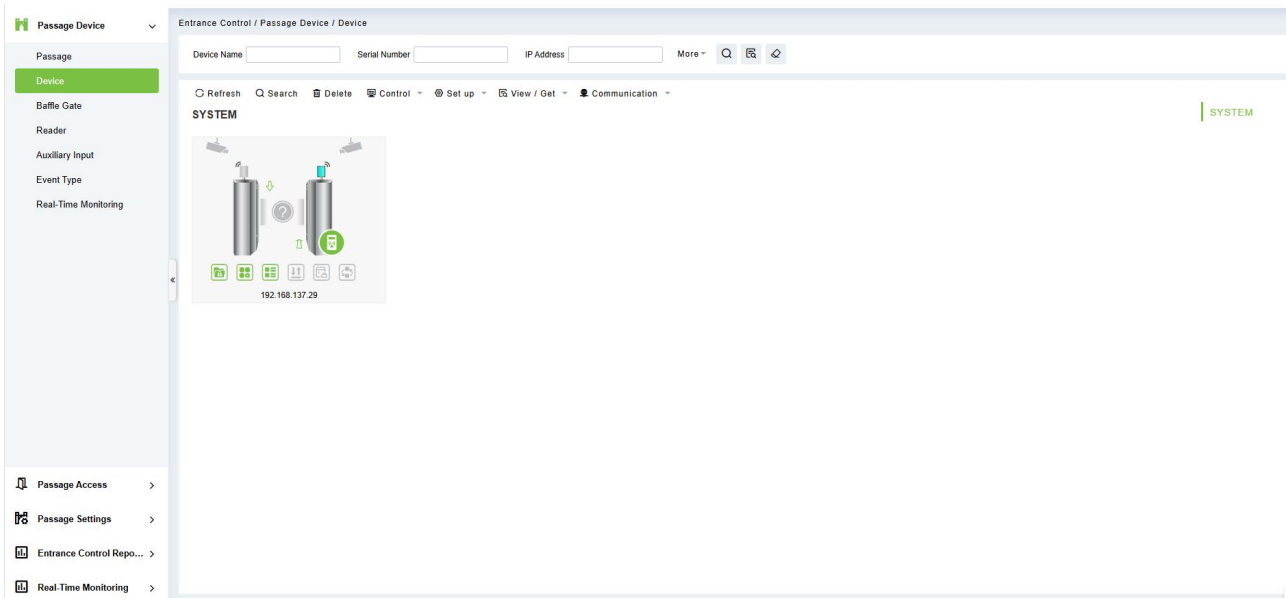


- **Device Operations:** Corresponding operations on devices are required to realize communication between the system and devices, data acquisition, and synchronization of configuration information.

Device operations cover the following categories:

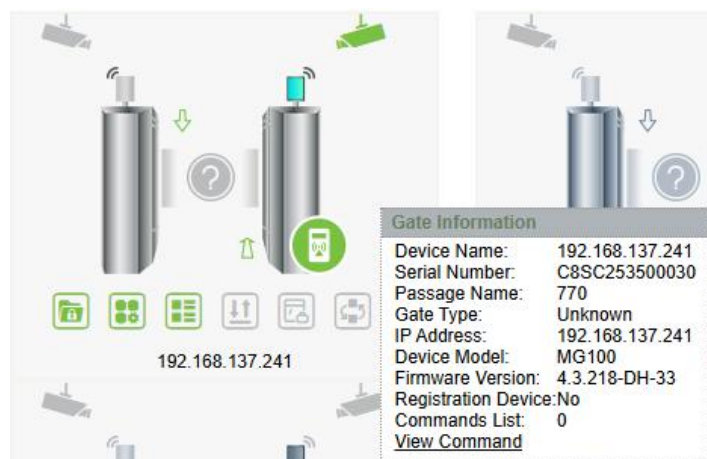
Device Control: Firmware upgrade (supports newly added multimodal all-in-one machines and turnstile control boards), device reboot, time synchronization, enable, disable, synchronize all data.

Settings: Enrollment machine configuration, daylight saving time setup, fingerprint matching threshold modification. **Information Viewing & Retrieval:** Retrieve device parameters, retrieve personnel data, retrieve event records, query device storage capacity. **Communication Configuration:** Modify IP address, modify communication password.



- Information Viewing & Convenient Configuration:

Gate information available for viewing includes device name, serial number, passage name, gate type, IP address, device model, firmware version, registration device, and number of pending commands. Clicking "View Command" will automatically redirect to the target page.



- Visual Interactive Configuration:

Binding/unbinding the camera, Add to Levels, Controller, Gate Parameters, Control Panel, Anti-Passback and Linkage settings. (Icons within the red box are all clickable for operations)



1.3. Baffle Gate: Retain Existing Functions

The screenshot shows the 'Baffle Gate' configuration page. The left sidebar has a menu with 'Baffle Gate' selected. The main area has a header with 'Entrance Control / Passage Device / Baffle Gate' and search filters for 'Baffle Gate Name', 'Owned Device', and 'Area Name'. Below the header is a toolbar with buttons for 'Refresh', 'Remote Opening (In)', 'Remote Opening (Out)', 'Cancel Alarm', 'Remote Normally Open', and 'More'. A table lists the Baffle Gate configuration:

Baffle Gate Name	Area Name	Owned Device	Serial Number	Baffle Gate Number	Verification Mode	Operations
192.168.137.29-1	SYSTEM	192.168.137.29	CSCC253500030	1	Automatic Identification	Edit

At the bottom, there is a pagination bar showing '50 rows per page', 'Jump To 1', '/1 Page', and 'Total of 1 records'.

1.4. Reader: Retain Existing Functions

The screenshot shows the 'Reader' configuration page. The left sidebar has a menu with 'Reader' selected. The main area has a header with 'Entrance Control / Passage Device / Reader' and search filters for 'Reader Name' and 'Baffle Gate Name'. Below the header is a toolbar with a 'Refresh' button. A table lists the Reader configuration:

Reader Name	Baffle Gate Name	Number	In/Out	Bound Camera	Operations
192.168.137.29-1-A	192.168.137.29-1	1	In		Edit Bind/Unbind
192.168.137.29-1-B	192.168.137.29-1	2	Out		Edit Bind/Unbind

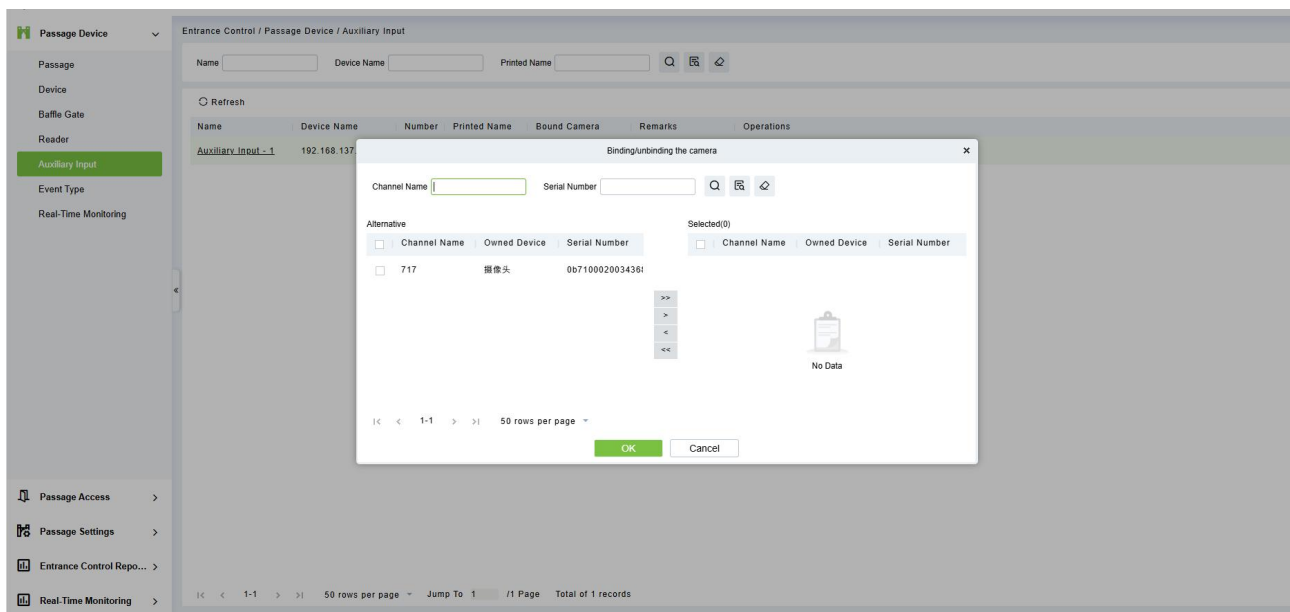
At the bottom, there is a pagination bar showing '50 rows per page', 'Jump To 1', '/1 Page', and 'Total of 2 records'.

1.5. Auxiliary Input: Display auxiliary input information connected to the current device and bind cameras. If relevant linkage configurations are set, video linkage will be triggered once corresponding events occur on this auxiliary input (including video, fire alarm, infrared detection, alarm, etc.).

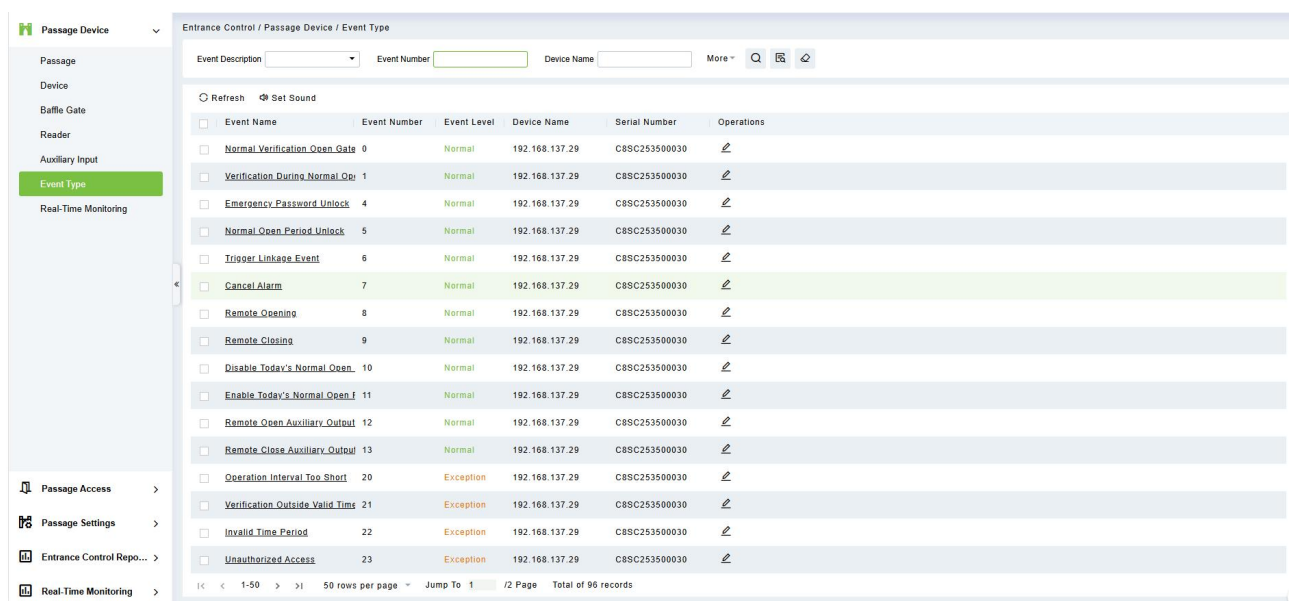
Click [Binding/Unbinding the camera] under the operation column of Auxiliary Input.

Bind/Unbind Camera: Bind or unbind cameras for multimodal all-in-one machines. If video linkage rules are configured, video linkage actions will be triggered when events occur on the multimodal all-in-one machine (pop-up live video, video recording, snapshot capture).

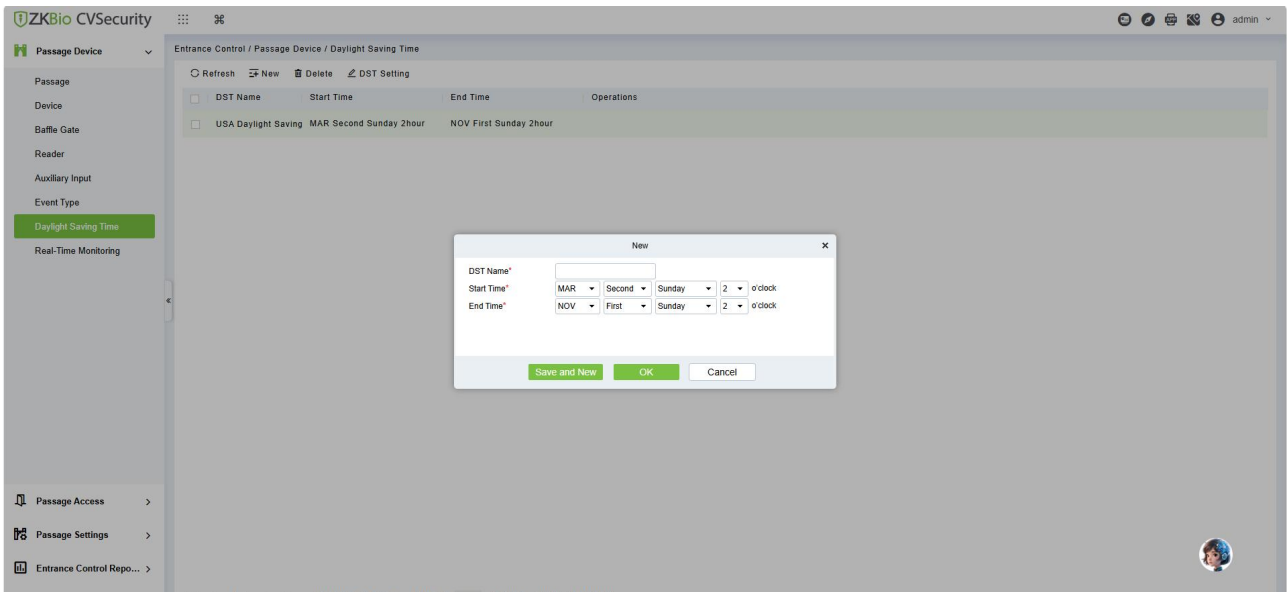
- Notes: One multimodal all-in-one machine can be bound to one or multiple cameras; multiple multimodal all-in-one machines can also share the same camera.



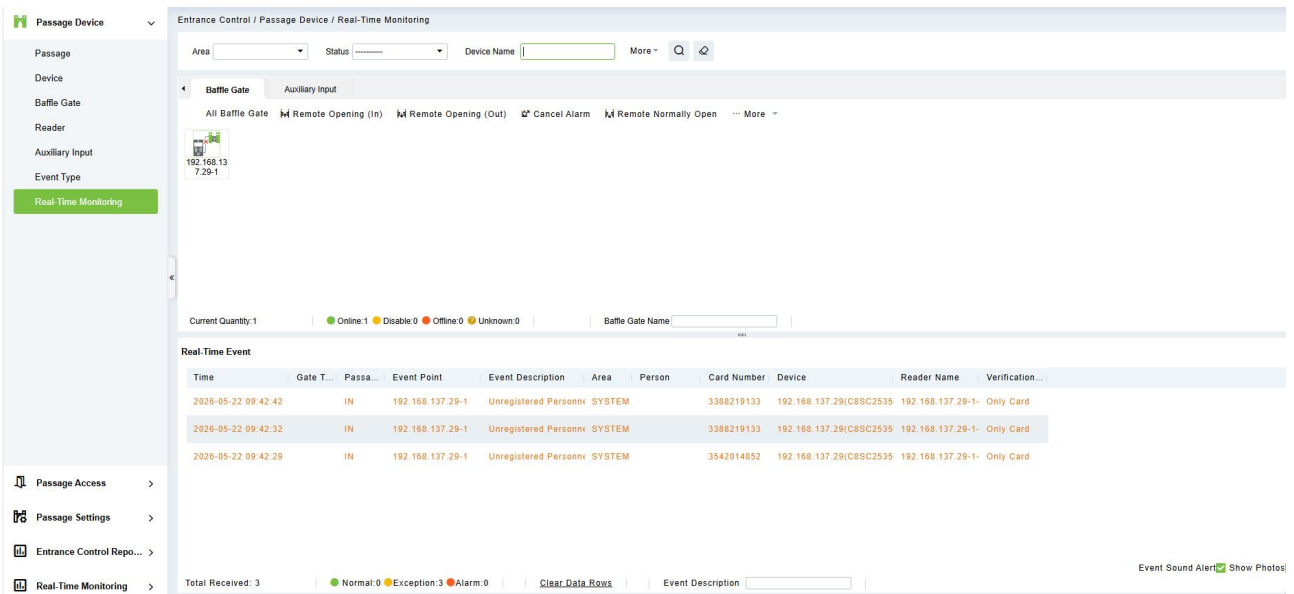
1.6. Event Type: The system comes with built-in default event types, and no new event types can be added. Users may customize and adjust the priority level of event types via Event Type in the Service Center.



1.7. Daylight Saving Time

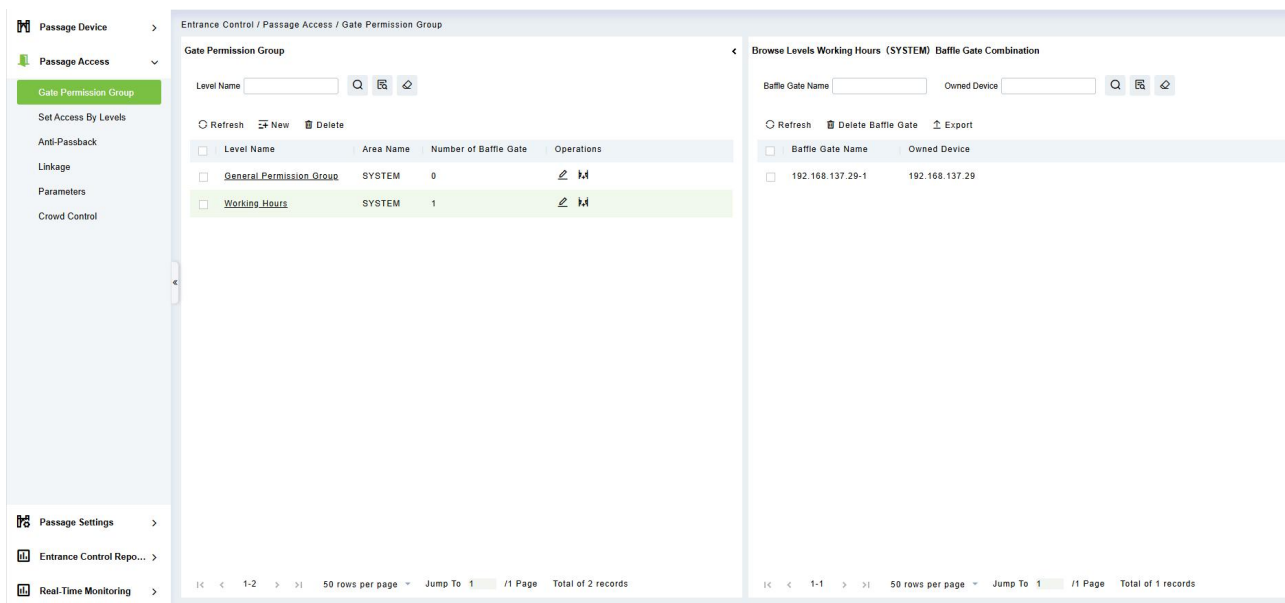


1.8. Real-Time Monitoring

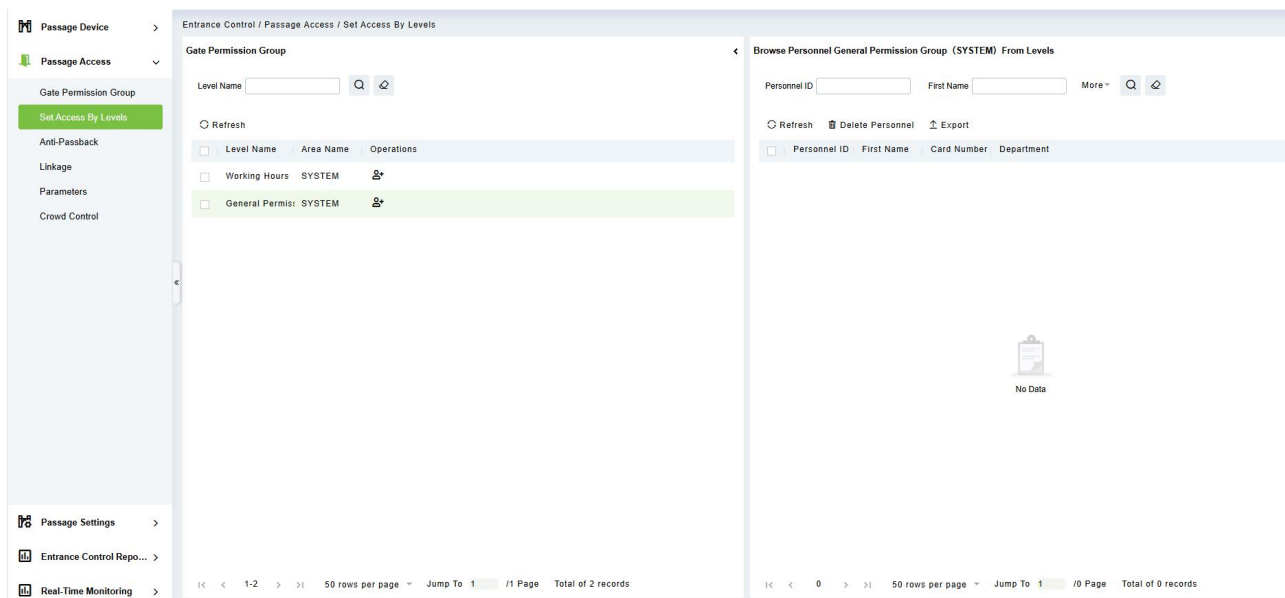


7.2. Passage Access

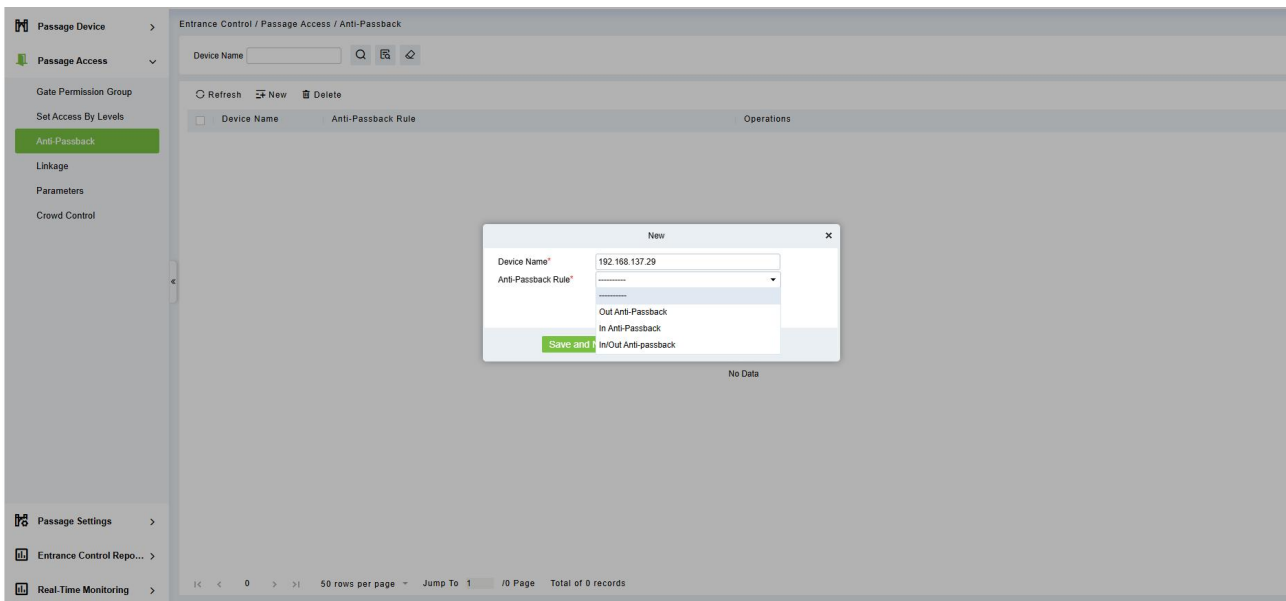
2.1. Gate Permission Group: Retain Existing Functions



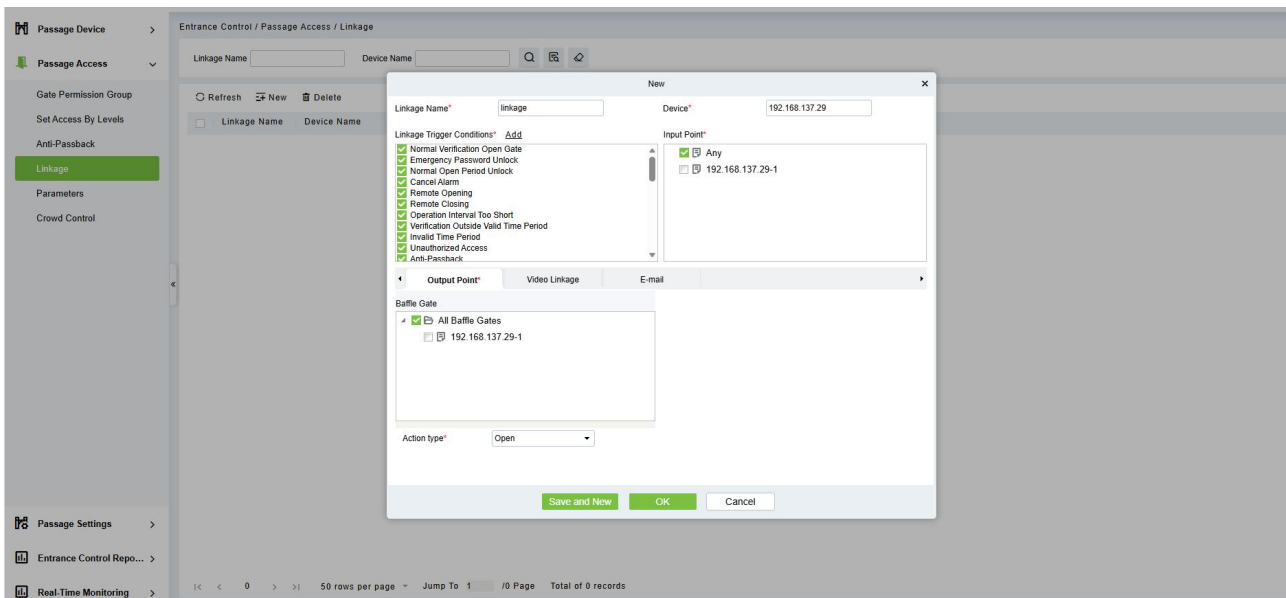
2.2. Set Access By Levels: Retain Existing Functions



2.3. Anti-Passback: Retain Existing Functions



2.4. Linkage: Retain Existing Functions



2.5. Parameters: Retain Existing Functions

2.6. Crowd Control(New)

Add a new subpage "Crowd Control", which supports configuring the maximum and minimum occupancy limits for regions created under Entrance Control / Passage Access / Crowd Control.

● New

Navigate to Entrance Control / Passage Access / Crowd Control. Configure occupancy parameters for the access region: Name, Channel Region, Maximum Occupancy, Minimum Occupancy.

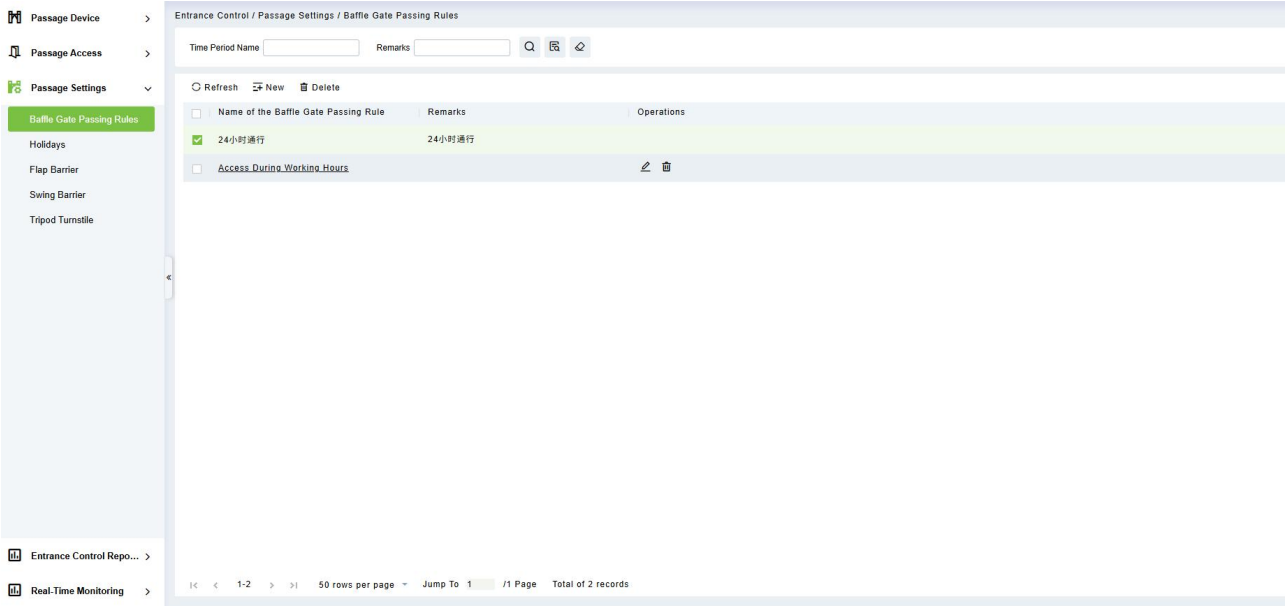
Click [OK] to save settings and close the page; the newly created channel region occupancy entry will be displayed in the list.

● Delete

Remove selected records to clear occupancy limit configurations of the corresponding access regions.

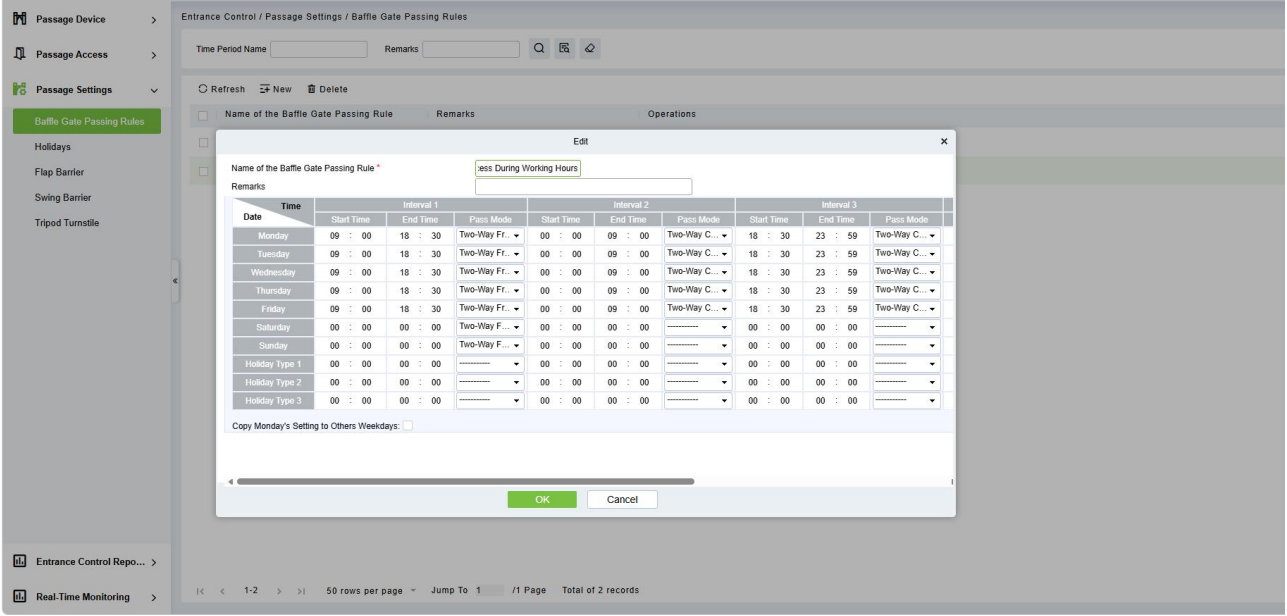
7.3. Passage Settings

It supports configuration of device access rules. Based on existing functions, new turnstile types such as tripod turnstiles are added.



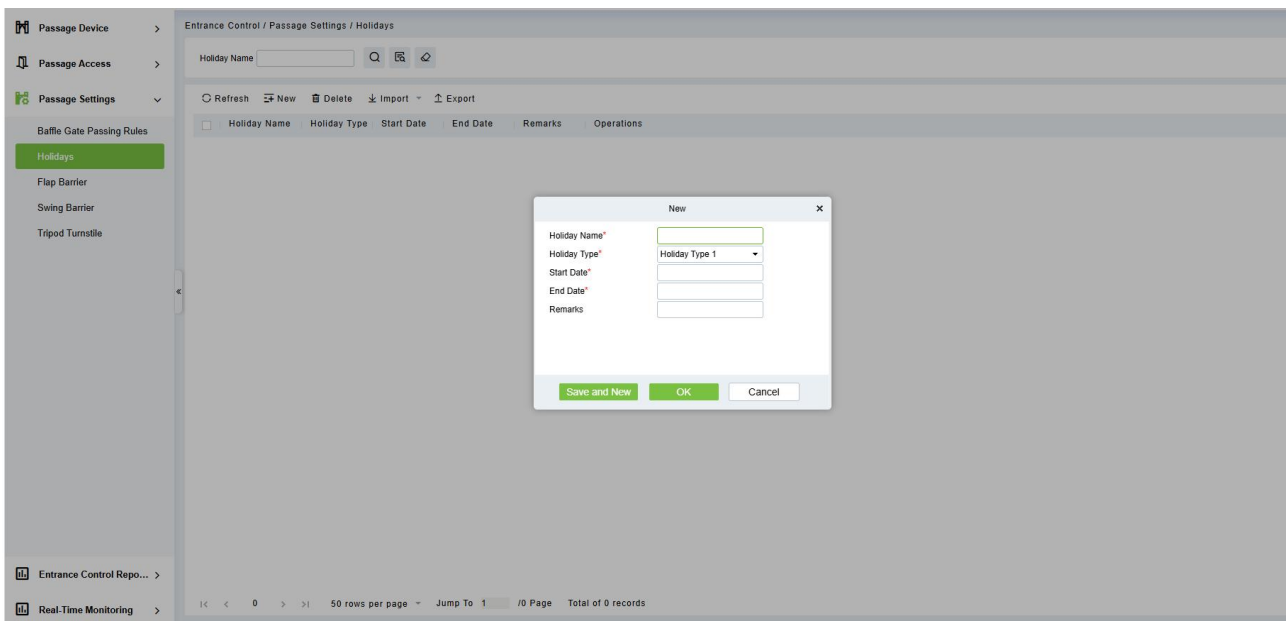
3.1. Baffle Gate Passing Rules

Configure access time and corresponding access modes. Requirements: Time periods can be customized by users as needed (a maximum of 5 time intervals supported), and three new holiday types are added.



3.2. Holidays

Add a Holiday page. Access schedules for holidays may differ from regular days. To simplify operations, the system supports separate channel time configurations for holidays. Channel holiday management functions include Add, Edit and Delete channel holidays.



● New

Navigate to Entrance Control / Passage Settings / Holidays. Field descriptions are as follows:

- Holiday Name: Any combination of characters with a maximum length of 30 characters.
- Holiday Type: Holiday Type 1, Type 2, Type 3. Each type can contain up to 32 holiday entries. All newly added holidays must be assigned to one of the three types.
- Start Date & End Date: Date format: YYYY-MM-DD (e.g. 2025-01-01). The start date cannot be later than the end date; the year of the start date cannot be earlier than the current year; holiday periods cannot span two calendar years.
- Annual Recurrence: Defines whether the holiday configuration needs annual adjustment. Default value: No. Set to Yes for fixed annual dates (e.g. New Year's Day on January 1 every year). Set to No for floating dates with unfixed specific dates each year (e.g. Mother's Day, the 2nd Sunday of May).

Example: Set New Year's Day as January 1, 2025 under Holiday Type 1. On January 1, access control schedules will follow the rules of Holiday Type 1 instead of the regular Friday schedule. After configuration, click [OK] to save, and the new holiday entry will appear in the holiday list.

● Edit

Click the holiday name or [Edit] under the Operation column to enter the edit page. Click [OK] to save modified configurations.

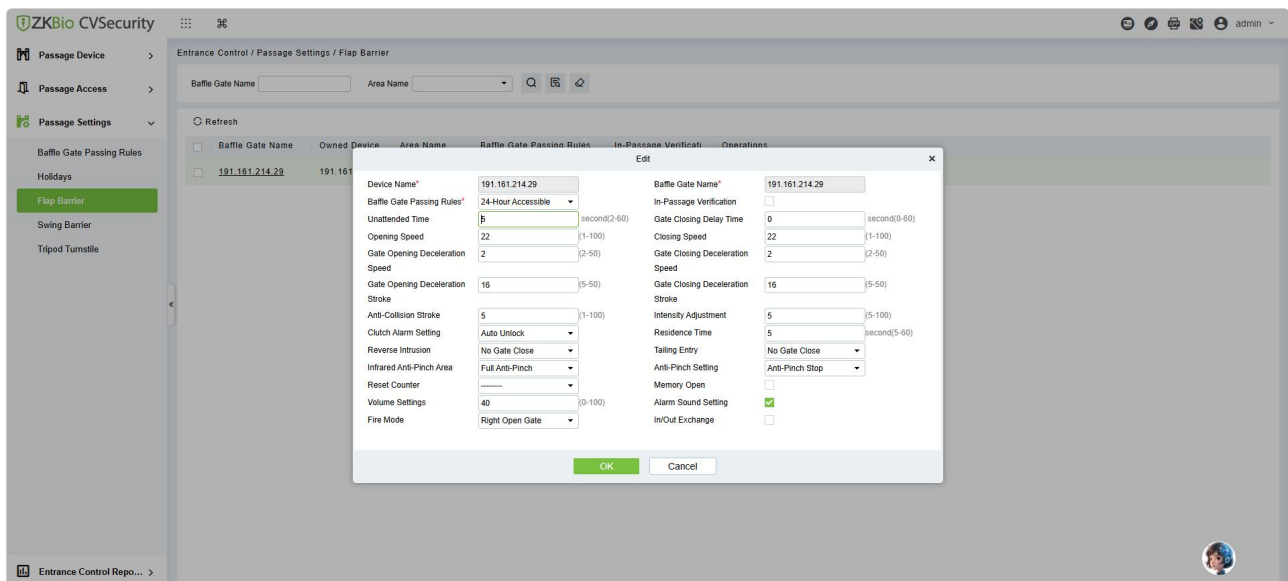
● Delete

Click the [Delete] button under the Operation column for a single holiday, or tick one or multiple holiday entries and click the bulk [Delete] button at the top of the list. Click [OK] to remove selected holidays, or [Cancel] to abort the operation. Holidays that are currently in use in access rules cannot be deleted.

3.3. Flap Barrier: Retain the functions of the original page to display all supported product models.

3.4. Swing Barrier: Retain the functions of the original page to display all supported product models.

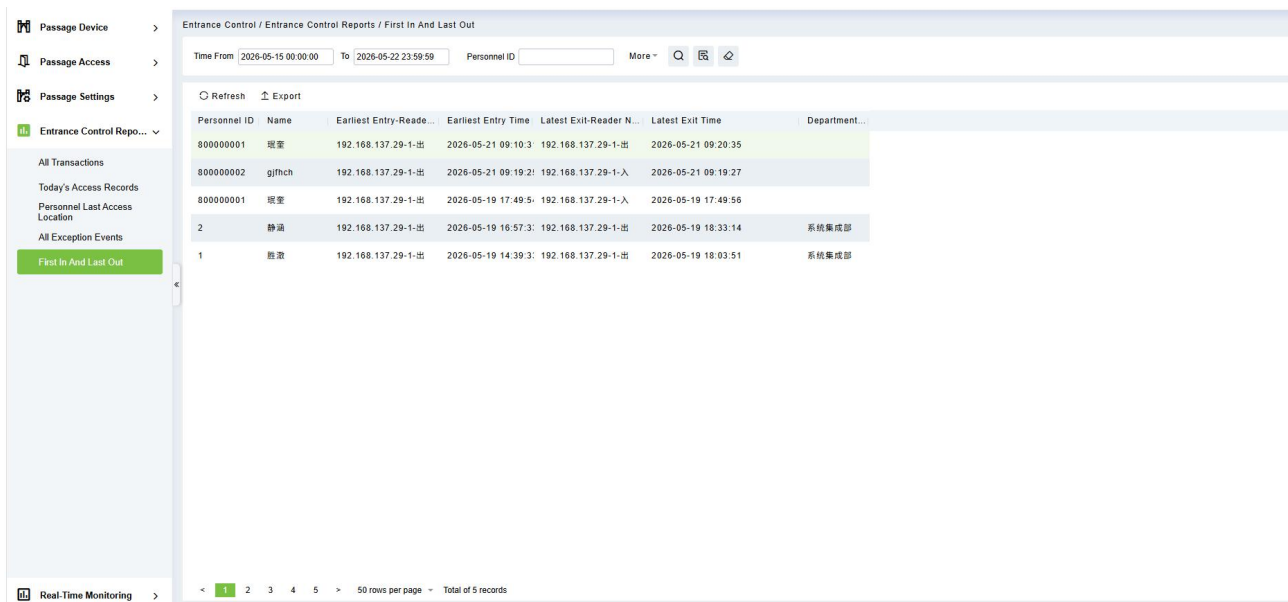
3.5. Tripod Turnstile: Display all supported product models.



7.4. Entrance Control Reports

Retain Existing Functions. Users can view all records within a specified time range, today's access records, the latest access location of personnel, and all abnormal records.

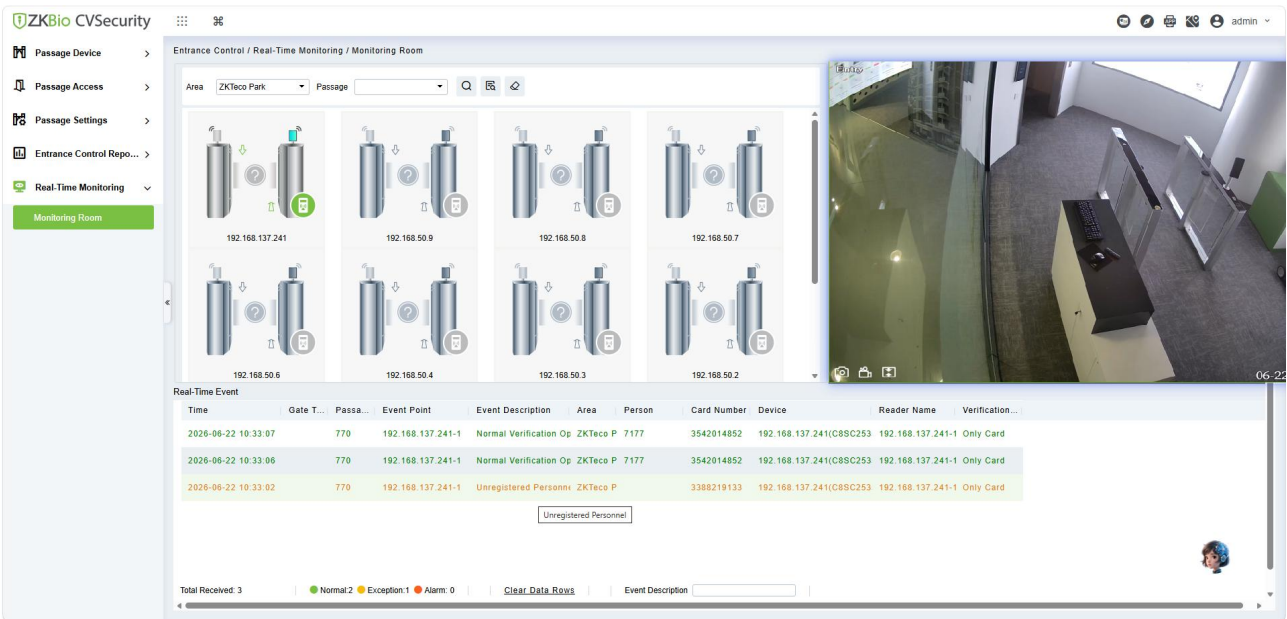
- New First In And Last Out Records:



7.5. Real-Time Monitoring

Real-time monitoring of gate status and real-time events of all turnstiles in the system, including normal events and abnormal events (including alarm events). Remote control operations for turnstiles are supported: remote lock/unlock, remote open entry gate, remote open exit gate, clear alarm, permanent open mode, enable daily permanent open period, disable daily permanent open period,

turn cleaning mode on/off, turn emergency mode on/off. The dynamic real-time monitoring interface for real-time events is as follows:

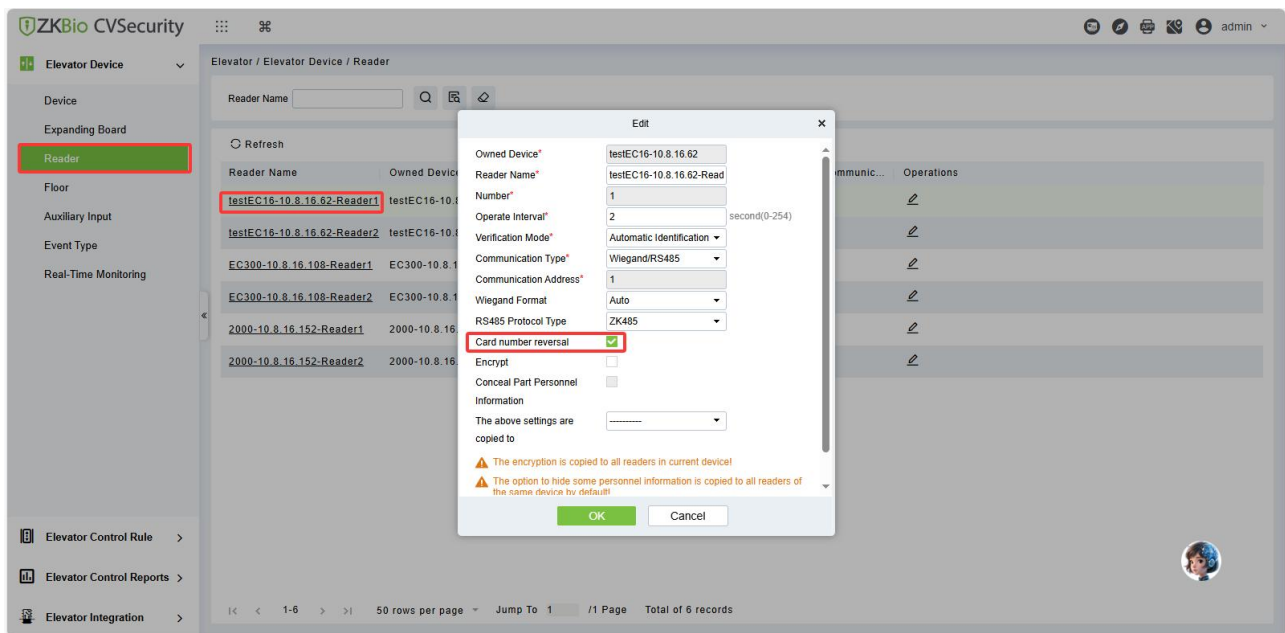


Add new video preview pop-up function: When a turnstile is selected, the preview stream of its bound camera will be displayed on the real-time monitoring screen.

8. Elevator Control

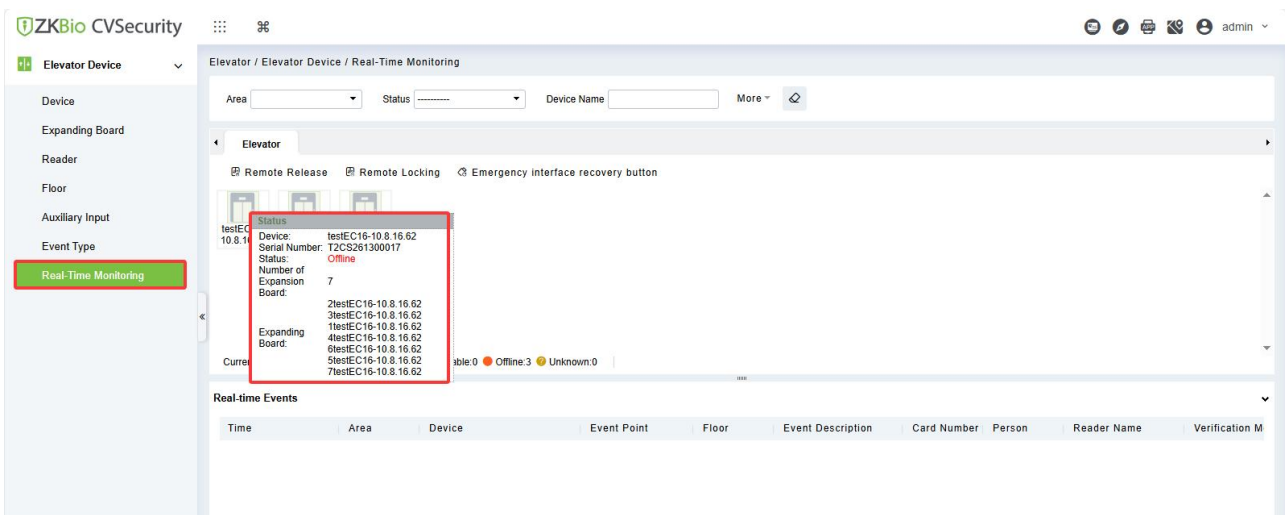
8.1. Elevator Device / Reader: Add new card number bit reversal function. After enabling this function, the system will automatically reverse the card number data.

Navigate to "Elevator / Elevator Device / Reader", click the target card reader to open the edit page, then check the Card Number Bit Reversal option to enable the function. Once enabled, the system will automatically reverse the data of the read card number.



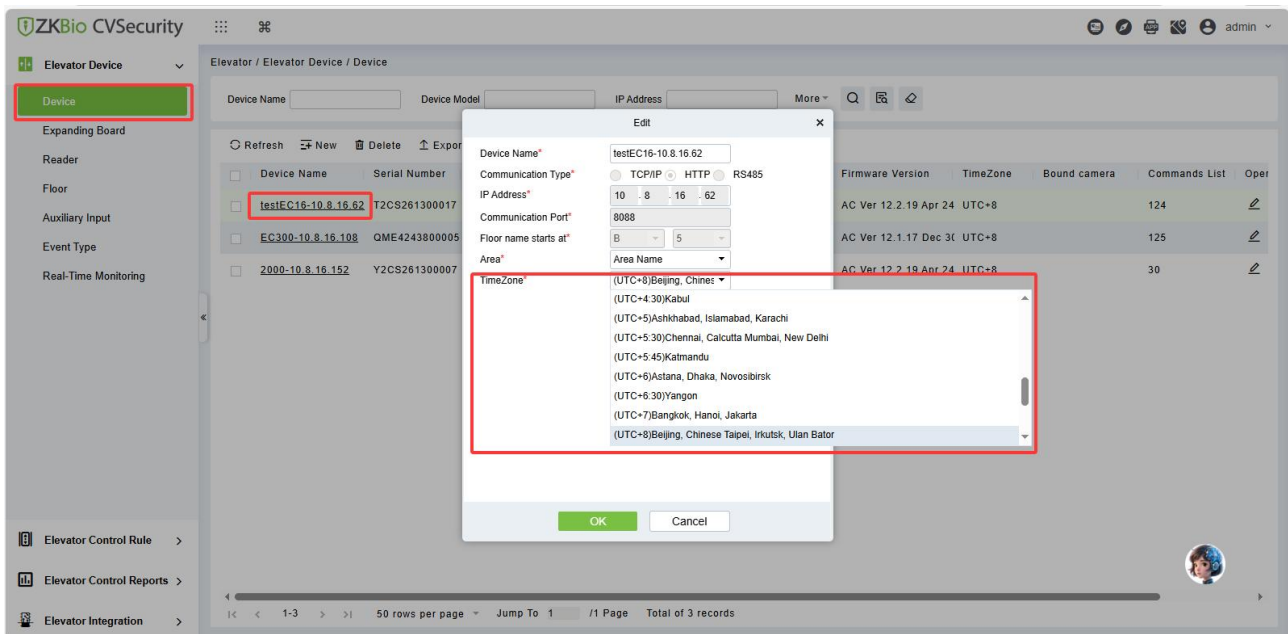
8.2. Elevator Device / Real-Time Monitoring – Interface Optimization: Adds a device list displaying key parameters including device address, serial number, online/offline status, and the number of expansion boards.

Navigate to "Elevator / Elevator Device / Real-Time Monitoring". Refer to the real-time monitoring interface of the access control module and add a structured device list that shows device address, serial number, online/offline status, and quantity of expansion boards.



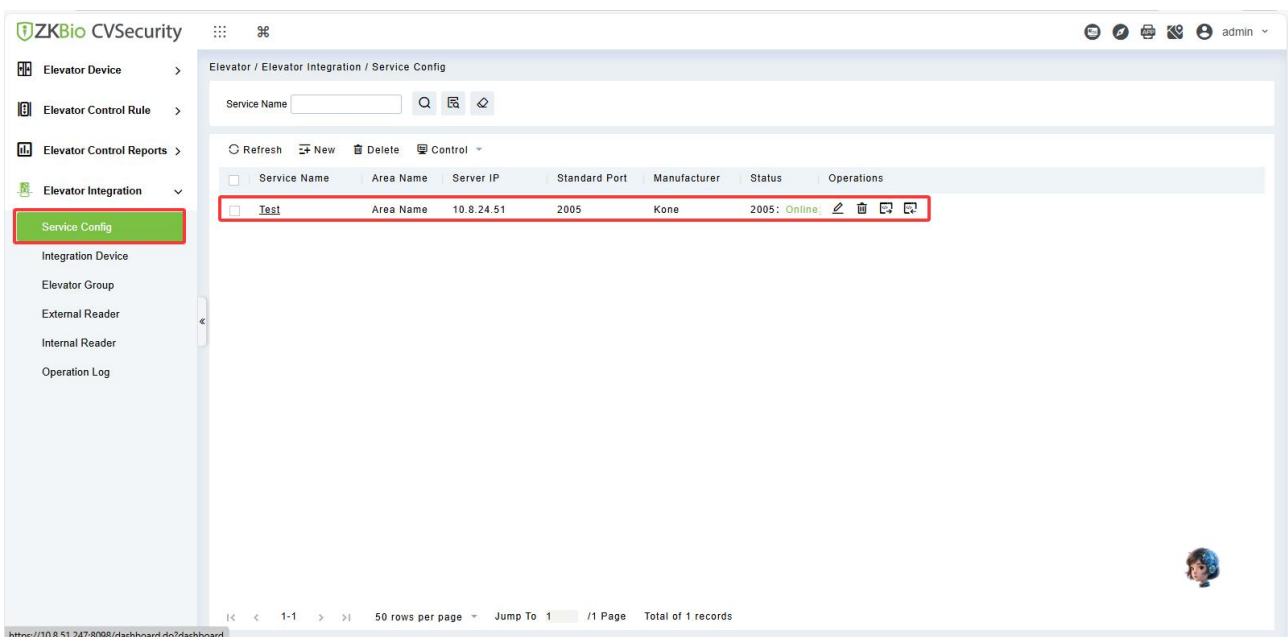
8.3. Elevator Device / Device-Selecting a device opens its edit page, with newly added time zone configuration parameters to support customized time zone settings for devices.

Navigate to "Elevator / Elevator Device / Device". Click a target device to open the edit interface, then select the local applicable time zone from the time zone dropdown selector.

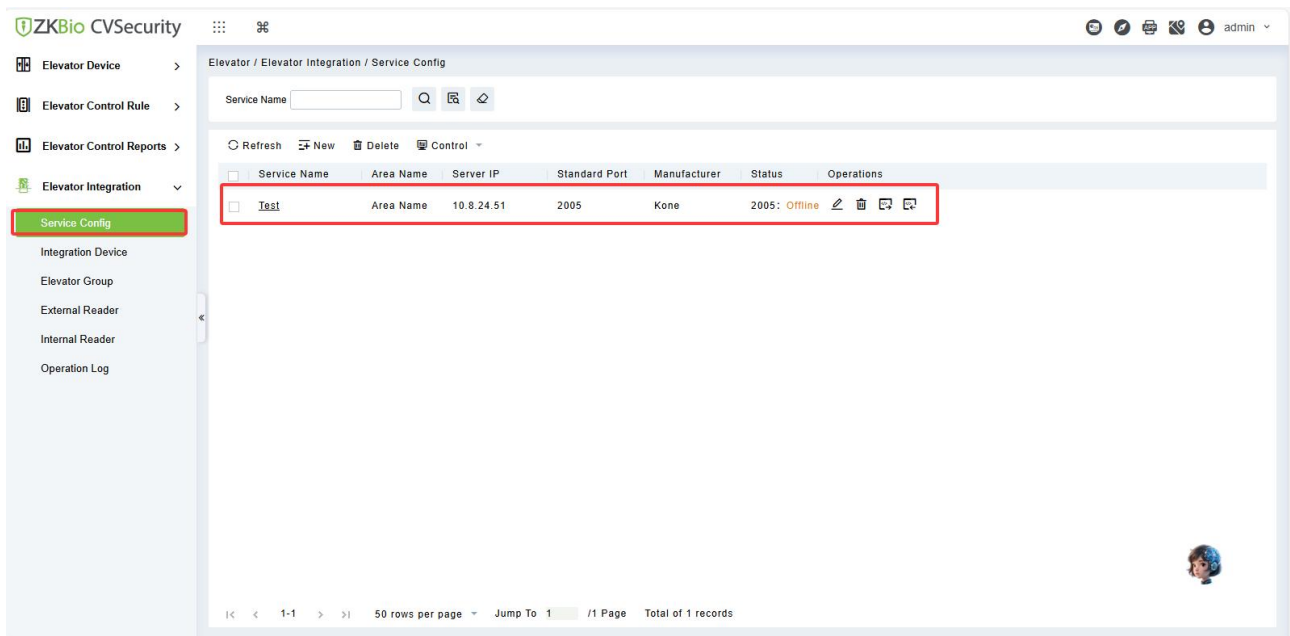


8.4. DCS - Online/Offline Status Event Reporting: Support alarm subscription for Online/Offline status in event center.

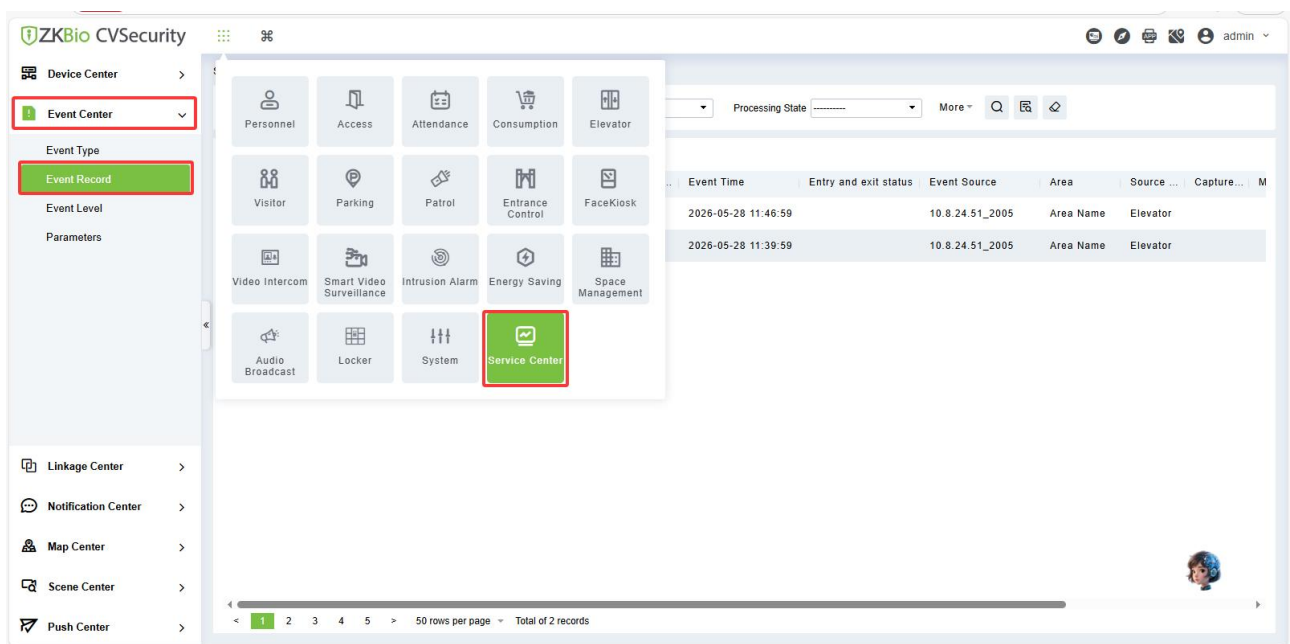
Navigate to "Elevator / Elevator Integration / Service Config", add the DCS service to bring it online, and the service status will display as Online.



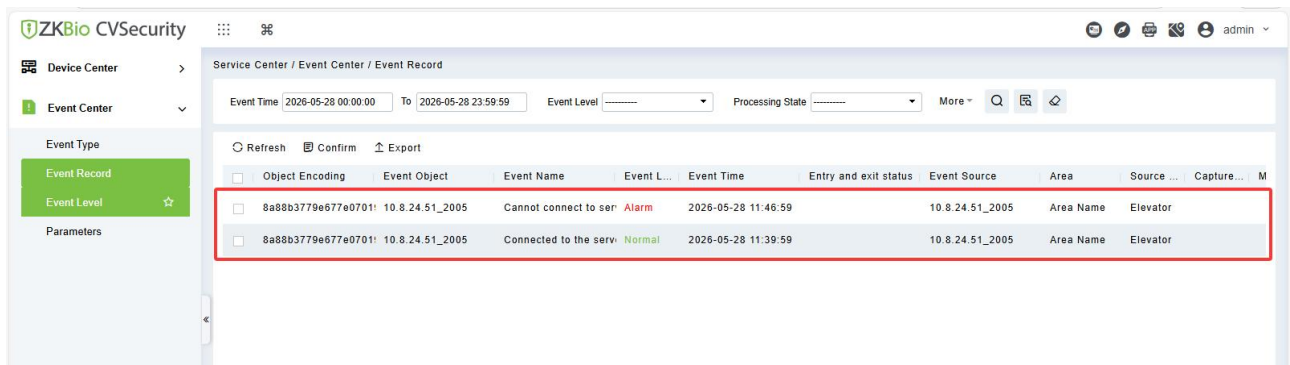
Disconnect the DCS service to make it offline, and the service status will switch to Offline accordingly.



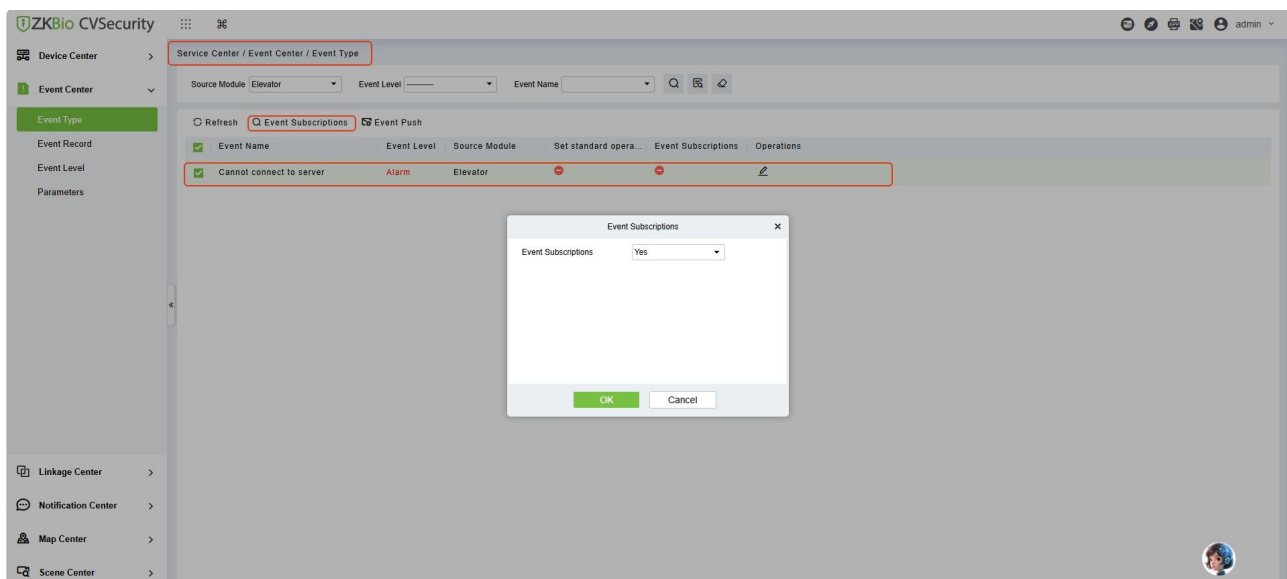
Go to "Service Center / Event Center / Event Record" to view all alarm logs.



Filter alarm messages with the source module as Elevator Control module, then alarms related to DCS service online/offline status can be viewed.



Check the events "Connected to the server" or "Cannot connect to server", then click Event Subscription to complete alarm subscription for DCS online and offline status changes.

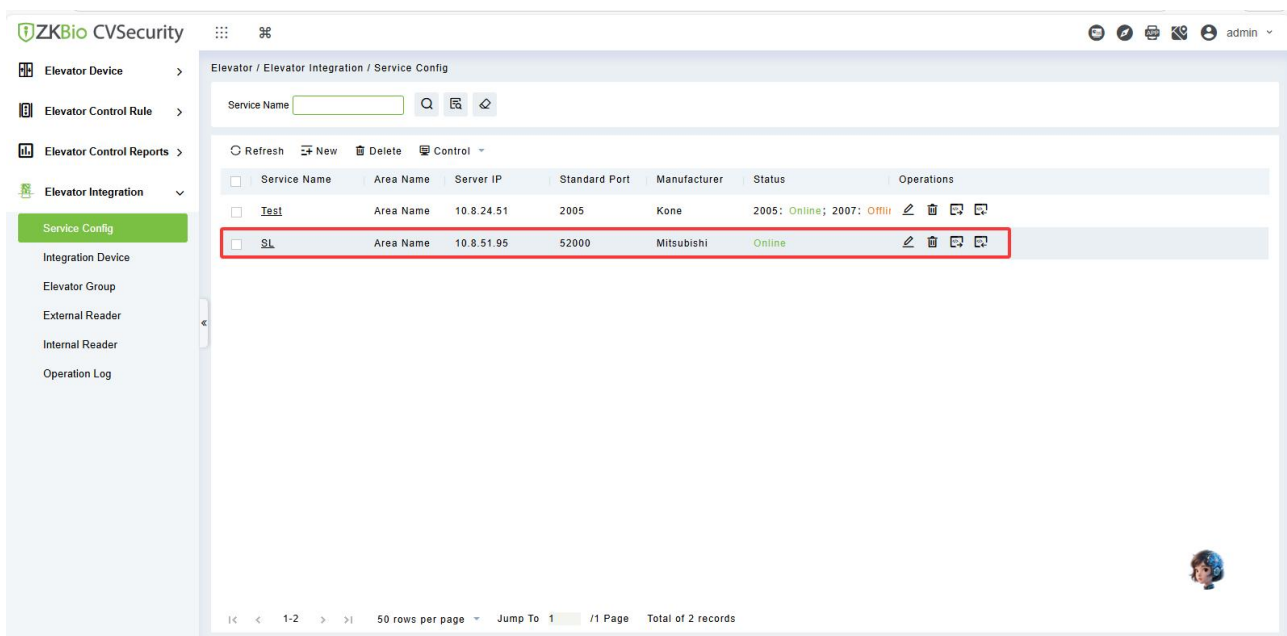


8.5. DCS - Supports elevator number feedback after call request.

After an elevator call is initiated via the OBU gateway, Mitsubishi OBU feeds back the called elevator number. The system transmits this cabin number to the Zophon-S1000 firmware via API for on-device display.

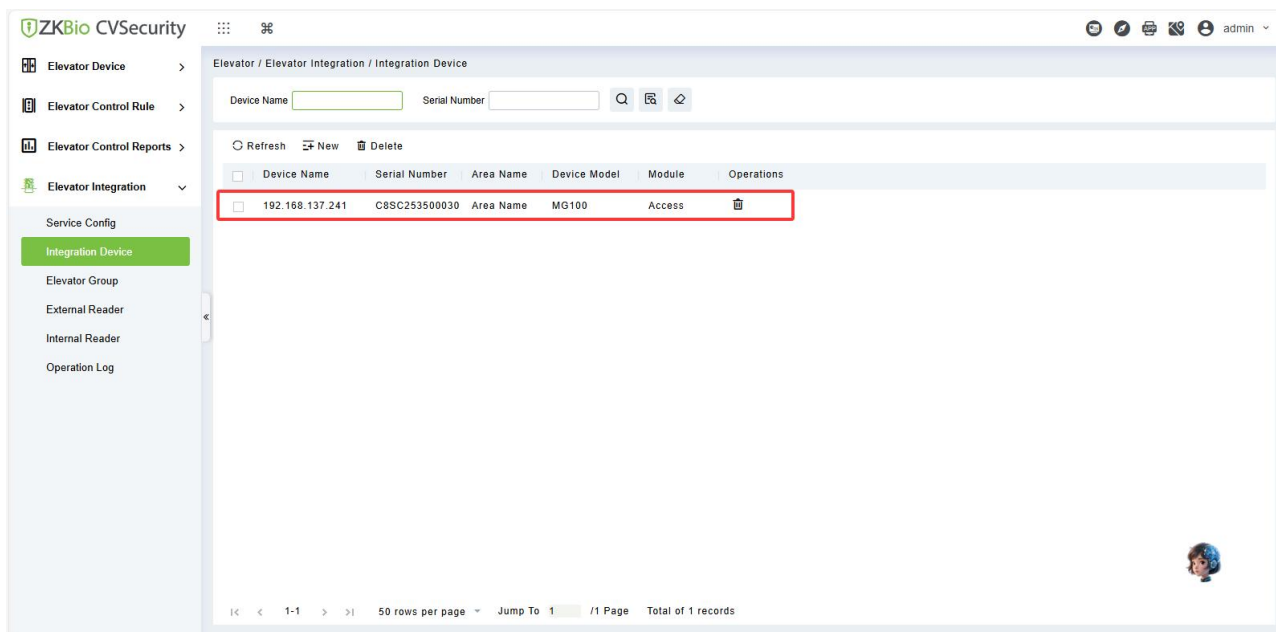
● Operation Steps

Step 1: Navigate to "Elevator / Elevator Integration / Service Config" and add the DCS service.

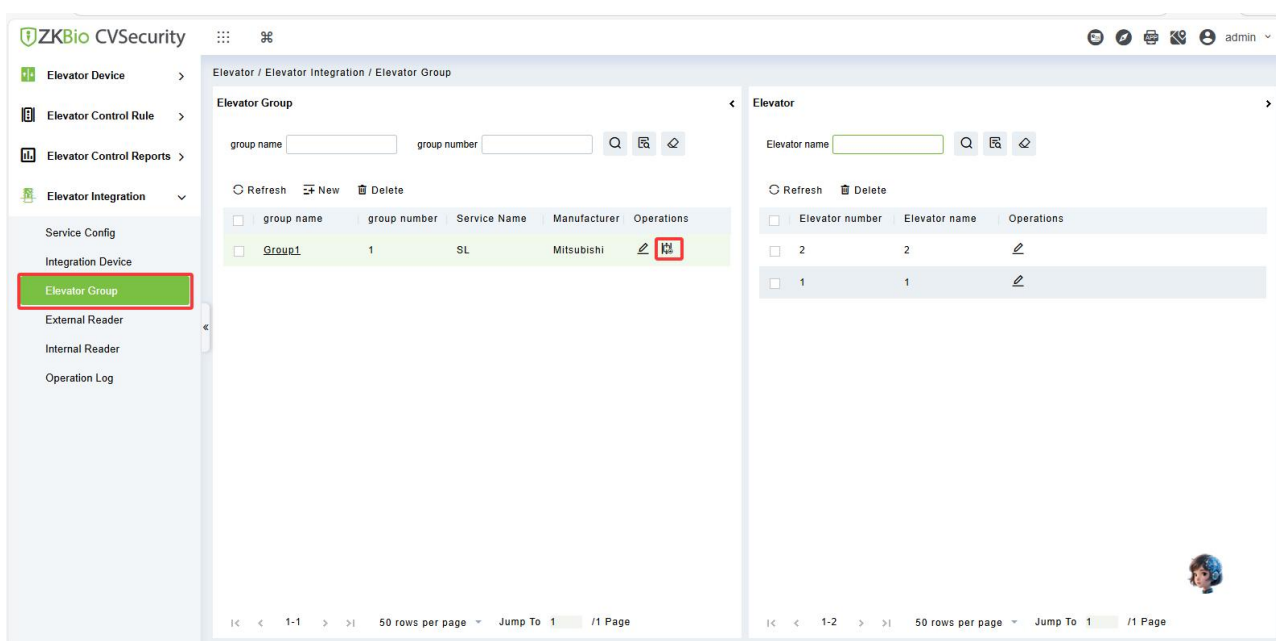


Step 2: Go to "Elevator / Elevator Integration / Integration Device" and add Zophon-S1000 to the integrated device list.

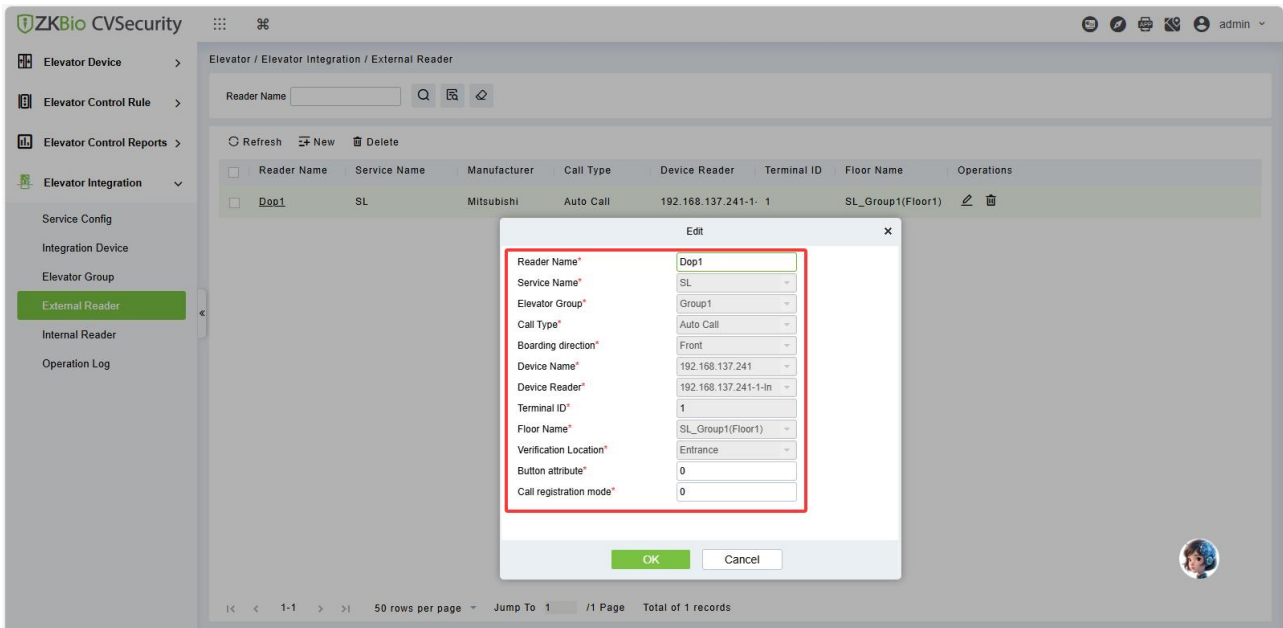
Note: Only Zophon-S1000 devices running access control firmware can be added here; units with channel firmware are not supported.



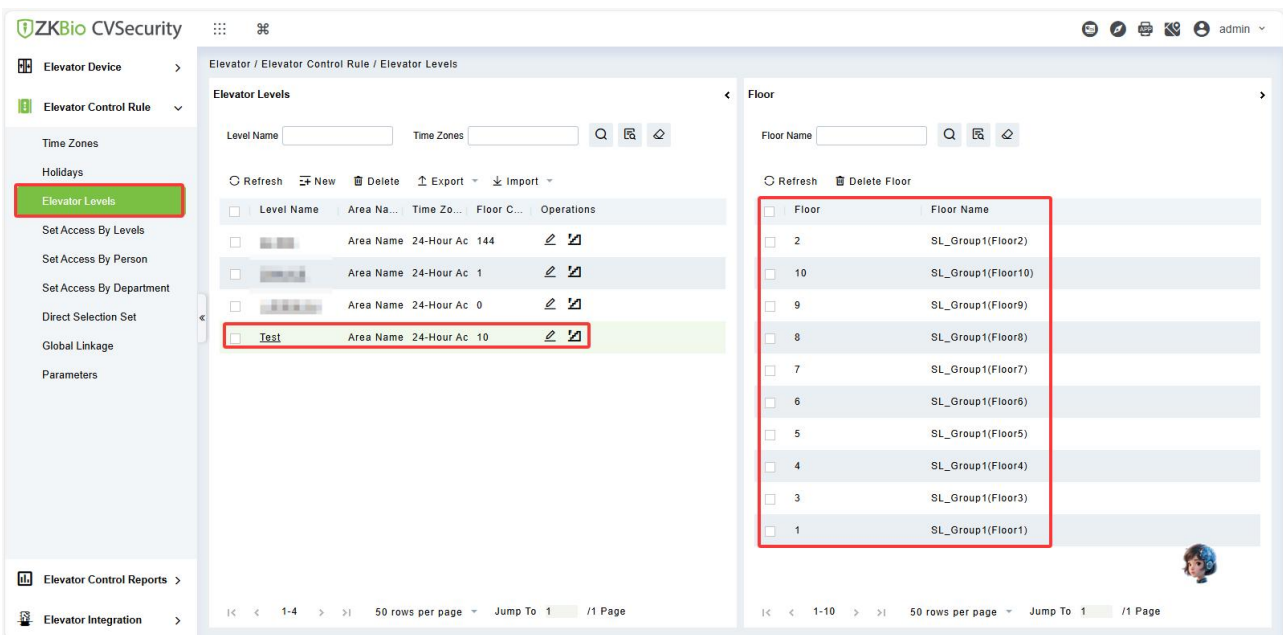
Step 3: Access "Elevator / Elevator Integration / Elevator Group". Create an elevator group and add elevators as needed. For this case, 2 elevators are added, with auto-assigned cabin numbers 1 and 2.



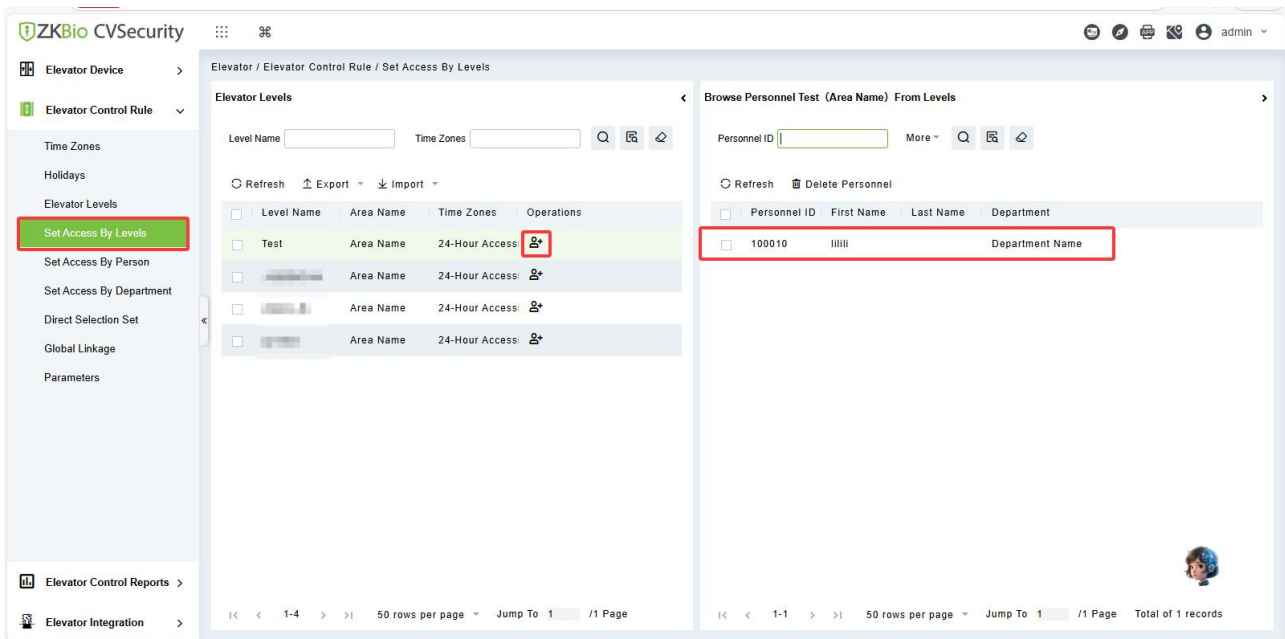
Step 4: Enter "Elevator / Elevator Integration / External Reader" to configure external reader parameters.



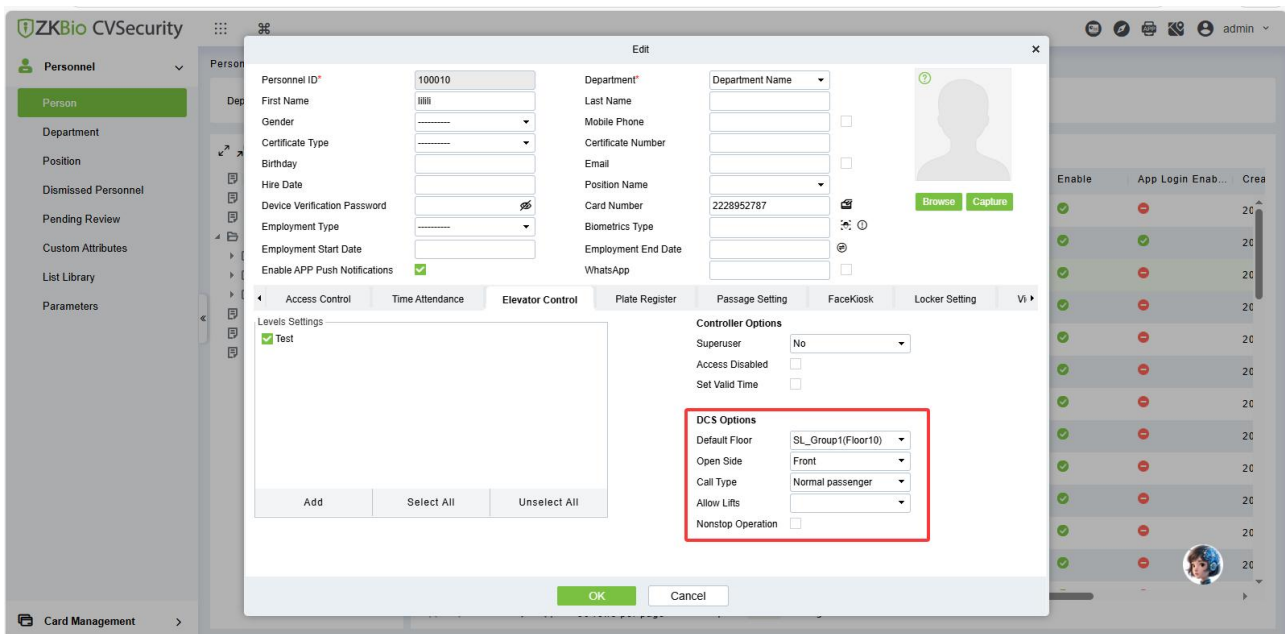
Step 5: Navigate to "Elevator / Elevator Control Rule / Elevator Levels" and assign authorized floors for each group.



Step 6: Open "Elevator / Elevator Control Rule / Set Access By Levels" and assign personnel to corresponding access groups.



Step 7: Go to "Personnel / Personnel / Person". Select a staff member to edit elevator access settings and complete DCS parameter configuration.



● Final Effect

When an elevator call succeeds through the OBU gateway, Mitsubishi OBU returns the target elevator number. This cabin number is pushed to Zophon-S1000 firmware through the interface for real-time display.

- Operation Log After Successful Execution

ZKBio CVSecurity

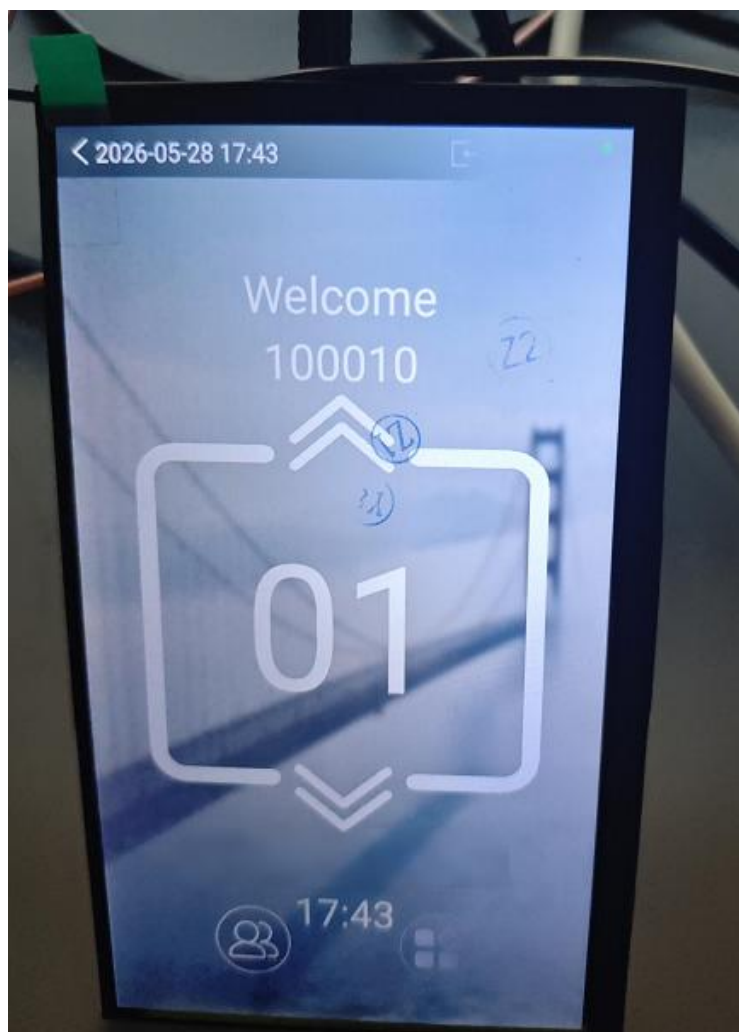
Elevator / Elevator Integration / Operation Log

Server IP:

Time	Server IP	Port	Personnel ID	First Name	Last Name	Event Point	Floor	Call Type	Nonstop Operation	Event Description	Returned Value
2026-05-28 17:43:45	10.8.51.95	52000	100010	liili		Dop1	10	Normal pas	No	Auto Call	0
2026-05-28 16:17:44	10.8.24.51	2005								Connected to the s	0
2026-05-28 16:17:34	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:17:23	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:17:12	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:17:01	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:16:50	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:16:39	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:16:28	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:16:26	10.8.51.95	52000								Connected to the s	0
2026-05-28 16:16:17	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:16:06	10.8.24.51	2005								Cannot connect to	0
2026-05-28 16:15:55	10.8.24.51	2005								Cannot connect to	0

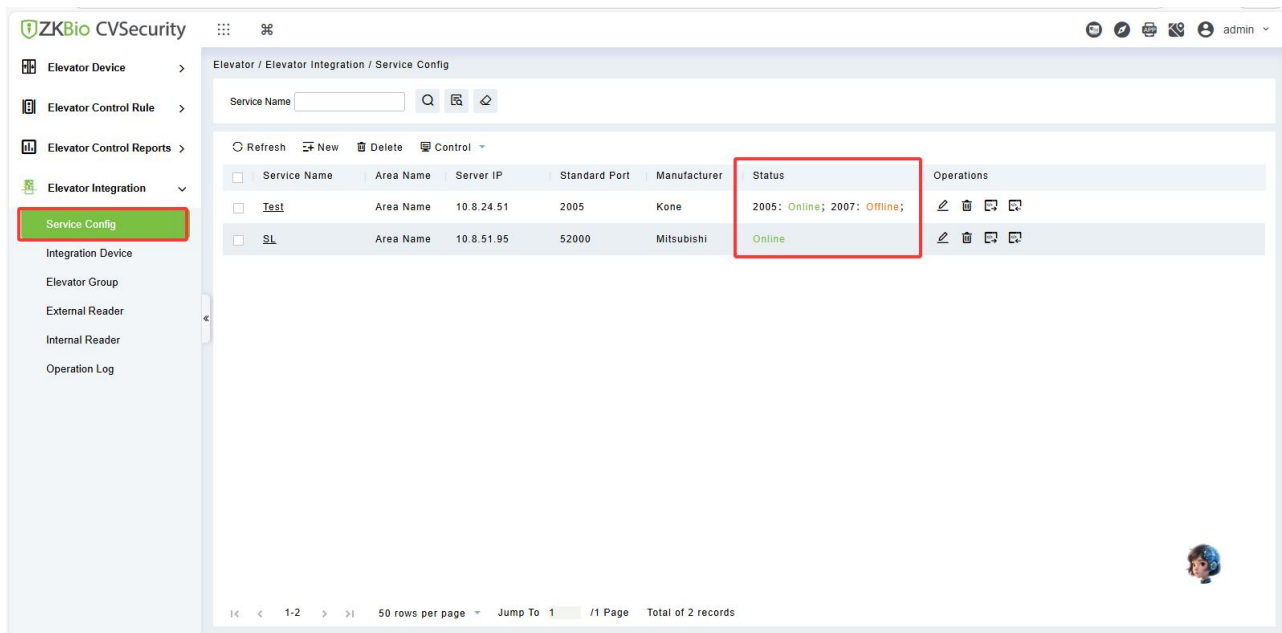
50 rows per page Total of 1512 records

- Scenario: Cabin No.1 auto-assigned, Zophon-S1000 firmware display content as follows:



8.6. Elevator Integration / Service Config: Add communication status display for Kone & Mitsubishi elevator controllers.

Navigate to "Elevator / Elevator Integration / Service Config". The page now displays dedicated communication status indicators for Kone and Mitsubishi elevator control devices.



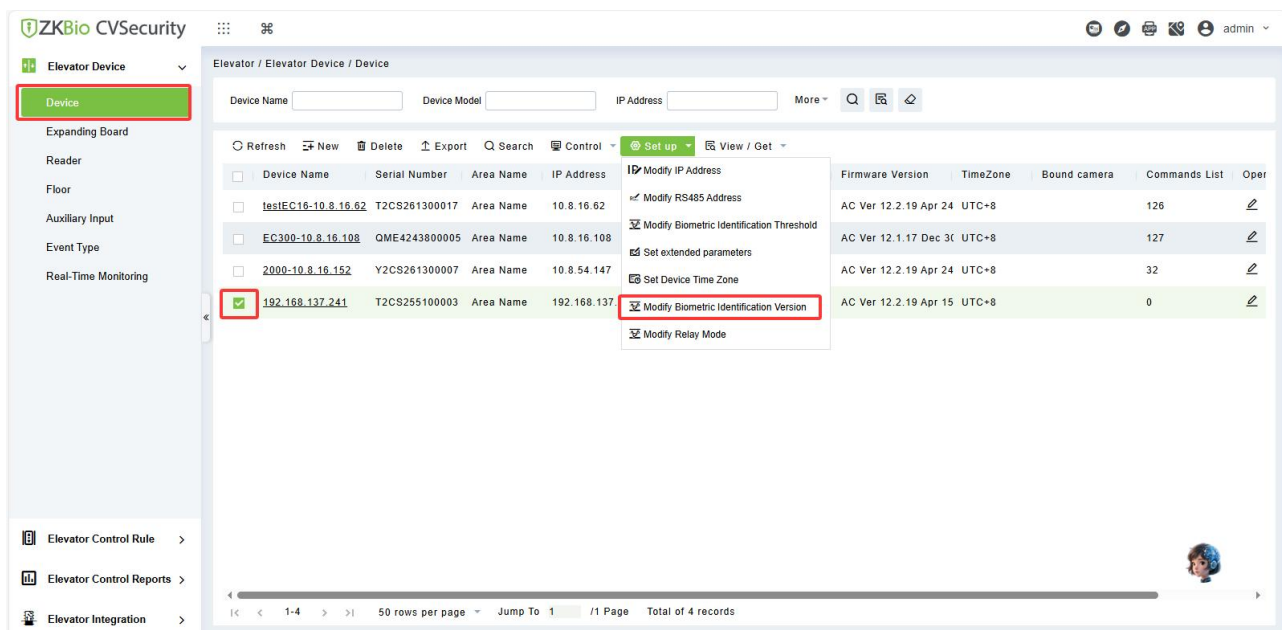
8.7. Elevator Device / Device: Add algorithm version selection during device creation.

When adding elevator control devices in the system, an algorithm version selection option is newly added.

- EC16 factory default biometric algorithm version: 13.0

● Operation Steps

Navigate to "Elevator / Elevator Device / Device", tick the target device, click Set up → Modify Biometric Identification Version to switch the algorithm version as required. EC16 devices come pre-configured with algorithm V13.0 by factory setting.



8.8. Elevator Device / Device: Modify the relay mode and check the direct access mode to reach the target floor directly without pressing any buttons.

- Supported Hardware Devices: EC16-AC Ver 12.2.19 Apr 15 2026 and above
- Relay Modes

- Direct Mode:

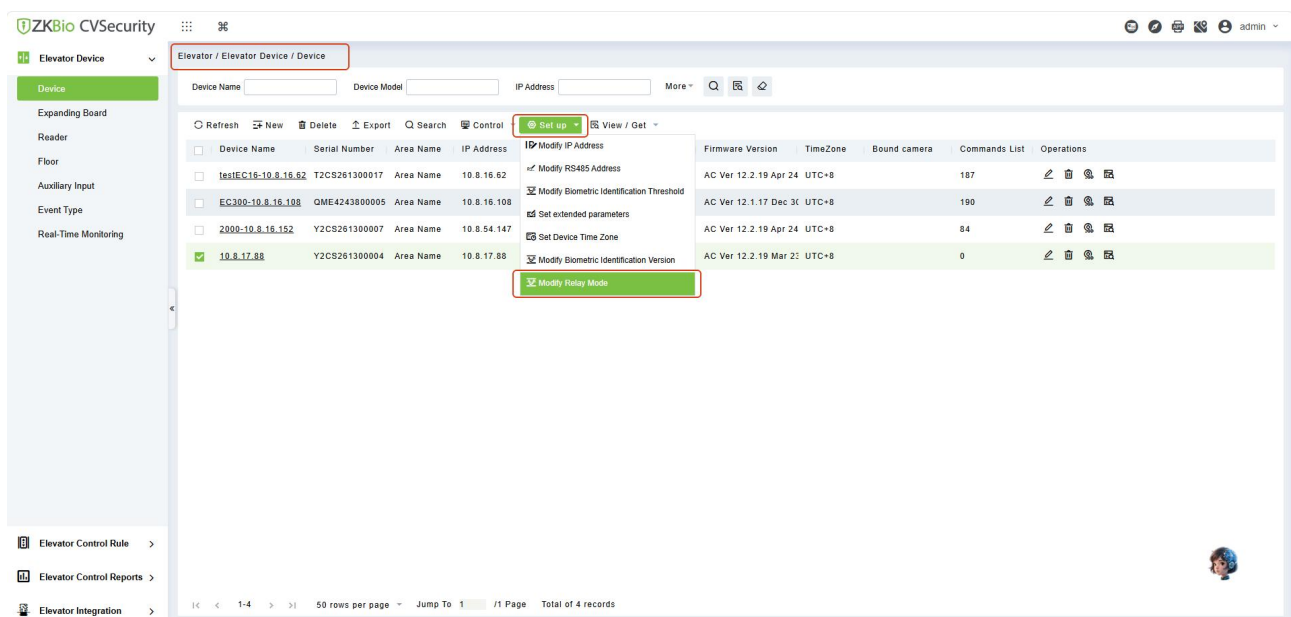
Default working mode. Dual relays work together to enable floor direct access without button operation. Connect NC/COM to the normally closed elevator control system. After user identity verification, the authorized target floor button on the elevator panel will light up automatically.

- Normal Mode:

Configurable switchable mode. Dual relays are configured to function as a single relay, allowing connection of NO/COM to the normally open elevator control system. After user identity verification, the user's authorized floor permissions are unlocked, but the corresponding elevator floor button needs to be pressed manually to activate.

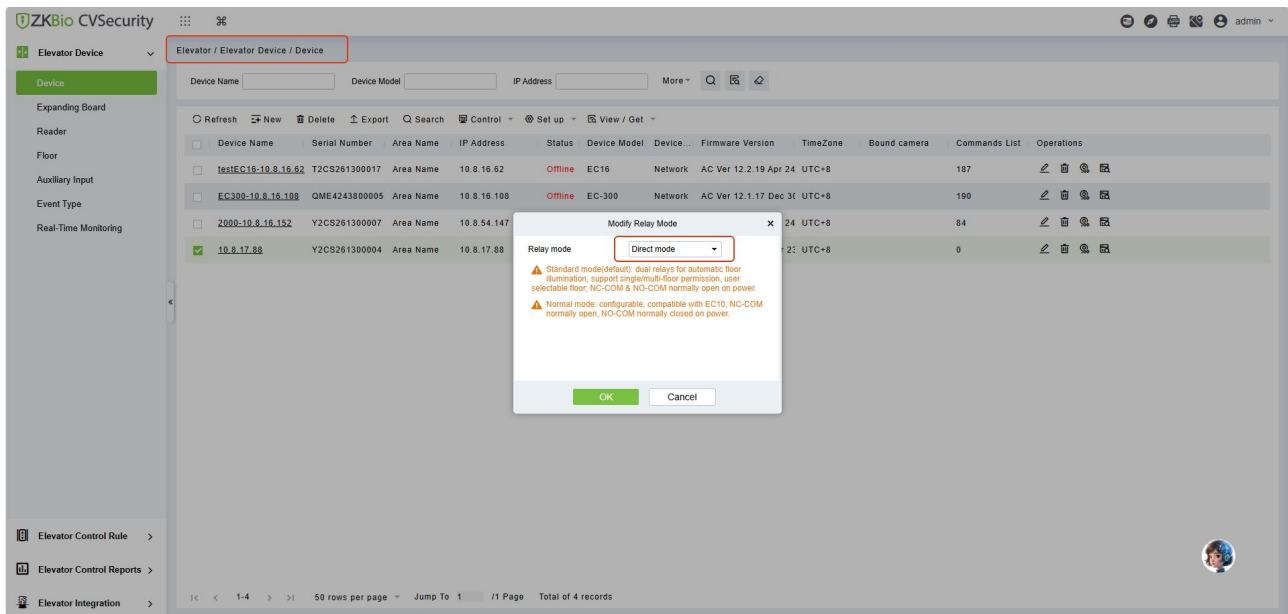
- Step-by-Step Configuration for Direct Mode

Step 1: Navigate to "Elevator / Elevator Device / Device", select a target elevator controller, click "Set up - Modify Relay Mode", then choose direct mode.

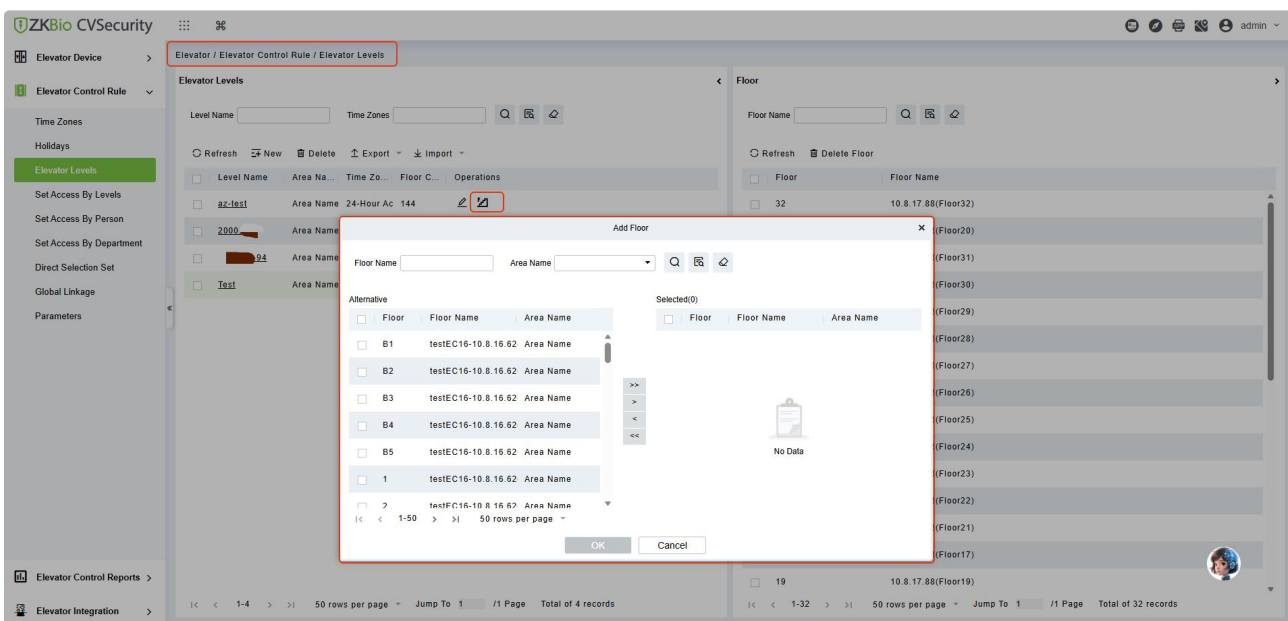


The screenshot displays the ZKBio CVSecurity web interface. The left sidebar shows the navigation menu with 'Elevator Device' selected. The main content area is titled 'Elevator / Elevator Device / Device'. A table lists four devices. The 'Set up' dropdown menu is open for the selected device, showing options like 'Modify IP Address', 'Modify RS485 Address', 'Modify Biometric Identification Threshold', 'Set extended parameters', 'Set Device Time Zone', 'Modify Biometric Identification Version', and 'Modify Relay Mode'. The 'Modify Relay Mode' option is highlighted. Below the table, there is a pagination bar showing '50 rows per page' and 'Total of 4 records'.

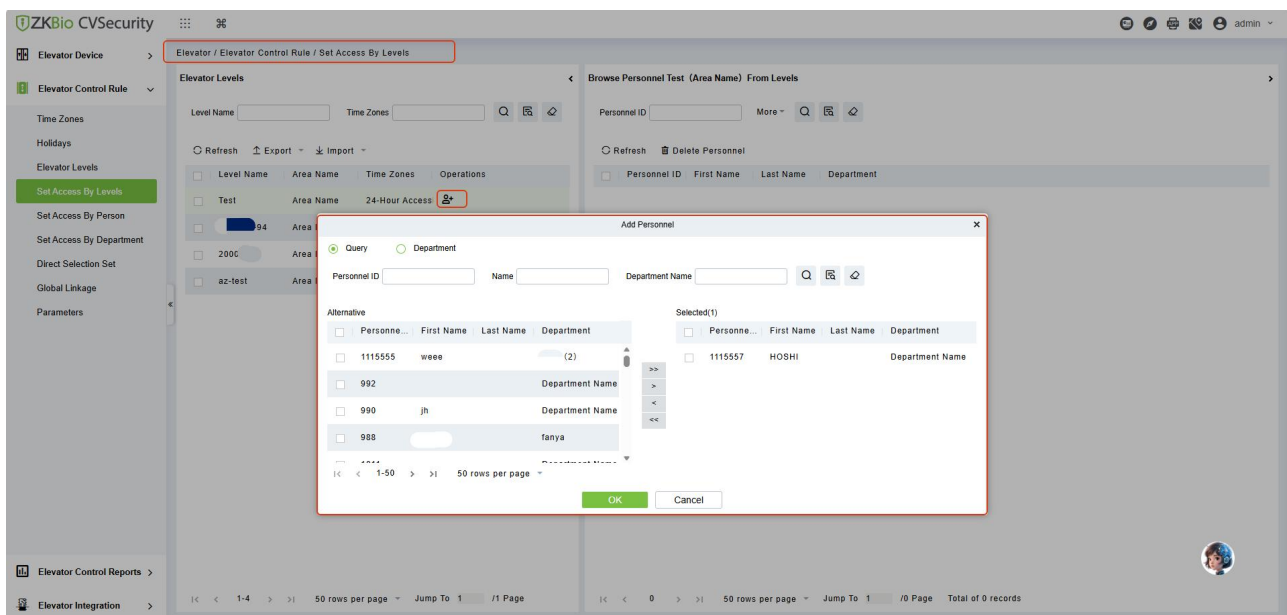
Device Name	Serial Number	Area Name	IP Address	Firmware Version	TimeZone	Bound camera	Commands List	Operations
testEC16-10.8.16.62	T2C9261300017	Area Name	10.8.16.62	AC Ver 12.2.19 Apr 24	UTC+8	187		
EC300-10.8.16.108	QME4243800005	Area Name	10.8.16.108	AC Ver 12.1.17 Dec 31	UTC+8	190		
2800-10.8.16.152	Y2C9261300007	Area Name	10.8.54.147	AC Ver 12.2.19 Apr 24	UTC+8	84		
10.8.17.88	Y2C9261300004	Area Name	10.8.17.88	AC Ver 12.2.19 Mar 22	UTC+8	0		



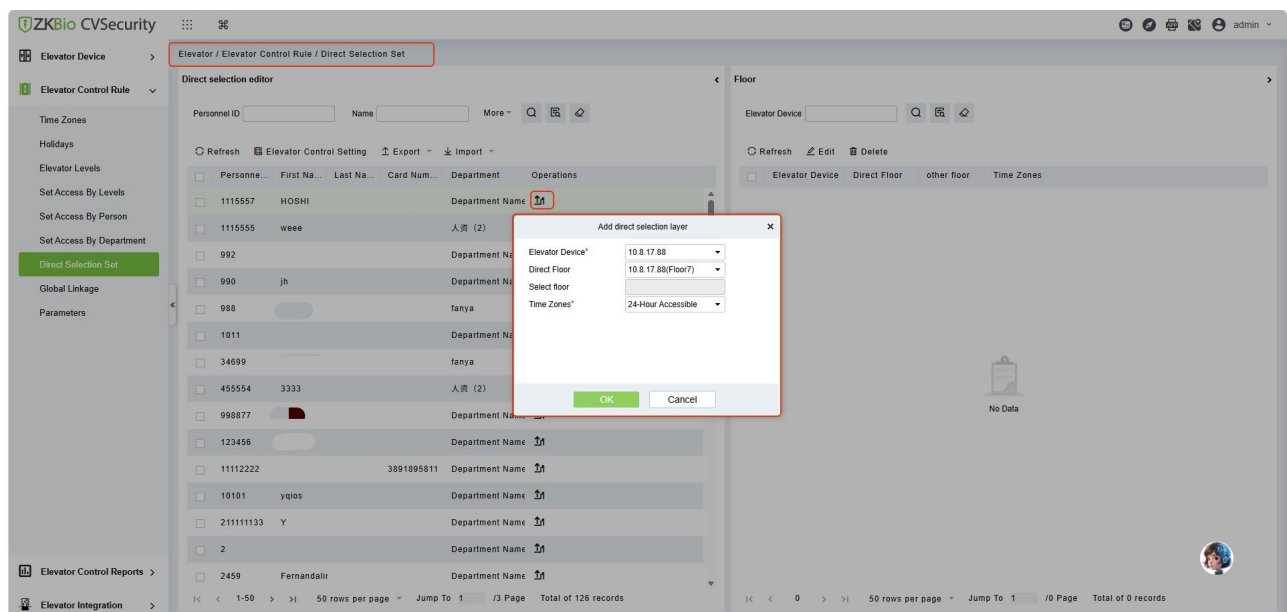
Step 2: Navigate to “Elevator / Elevator Control Rule / Elevator Levels”, create an elevator access permission group and bind the selected elevator controller to this group.



Step 3: Navigate to “Elevator / Elevator Control Rule / Set Access By Levels”, assign personnel to the permission group to ensure valid identity authentication on the elevator controller.



Step 4: Navigate to “Elevator / Elevator Control Rule / Direct Selection Set”, assign direct-access floors to authorized personnel. Configuration completes. Upon successful verification on the elevator controller, the preconfigured floor will illuminate automatically.



9. Smart Video Surveillance

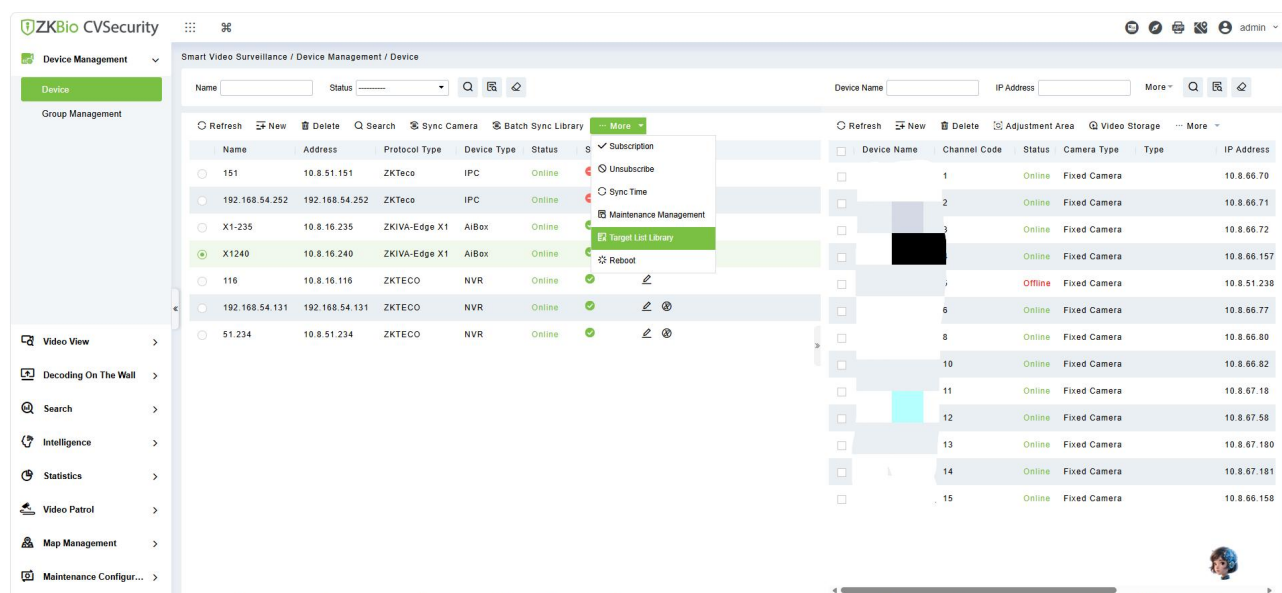
9.1. Intelligence - Behavior Analysis: Support binding of ZKIVA Edge X1 face recognition and behavior analysis.

When a behavior analysis alarm is triggered, the system automatically links facial authentication to verify personnel identity, and displays monitoring data in real time on Live Alarm, Event Center and Map Center.

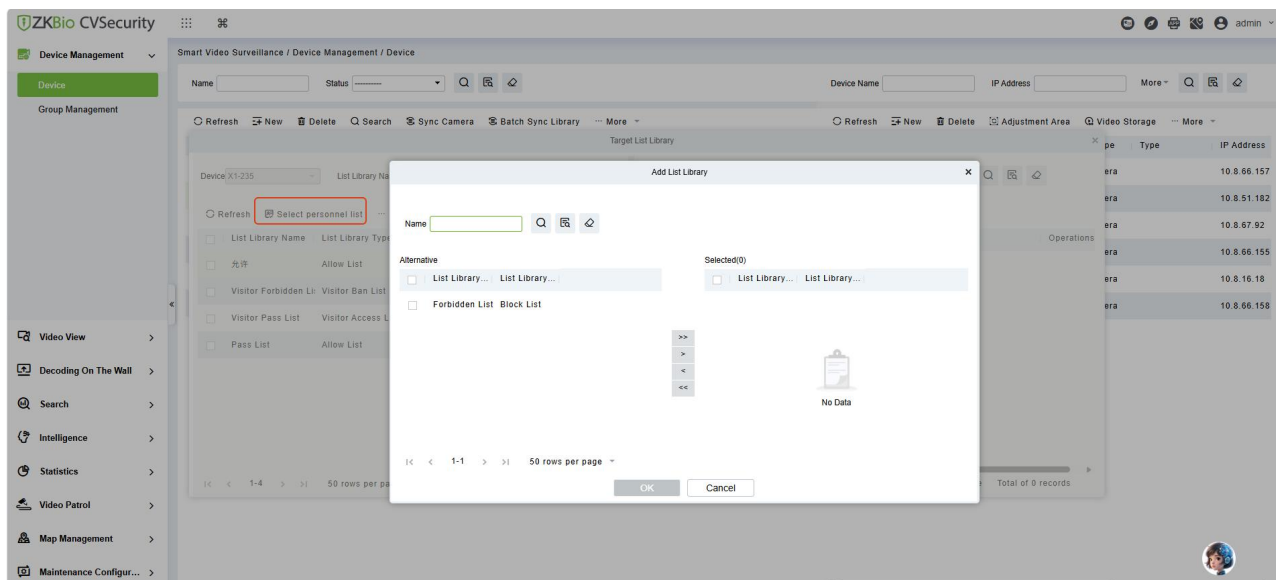
- Matching firmware requirement: ZKIVA Edge X1 firmware version 3.4.0-RL.ZK.1.NE or higher
- Prerequisite: Face data must be distributed to the device to activate this function

Operation Steps

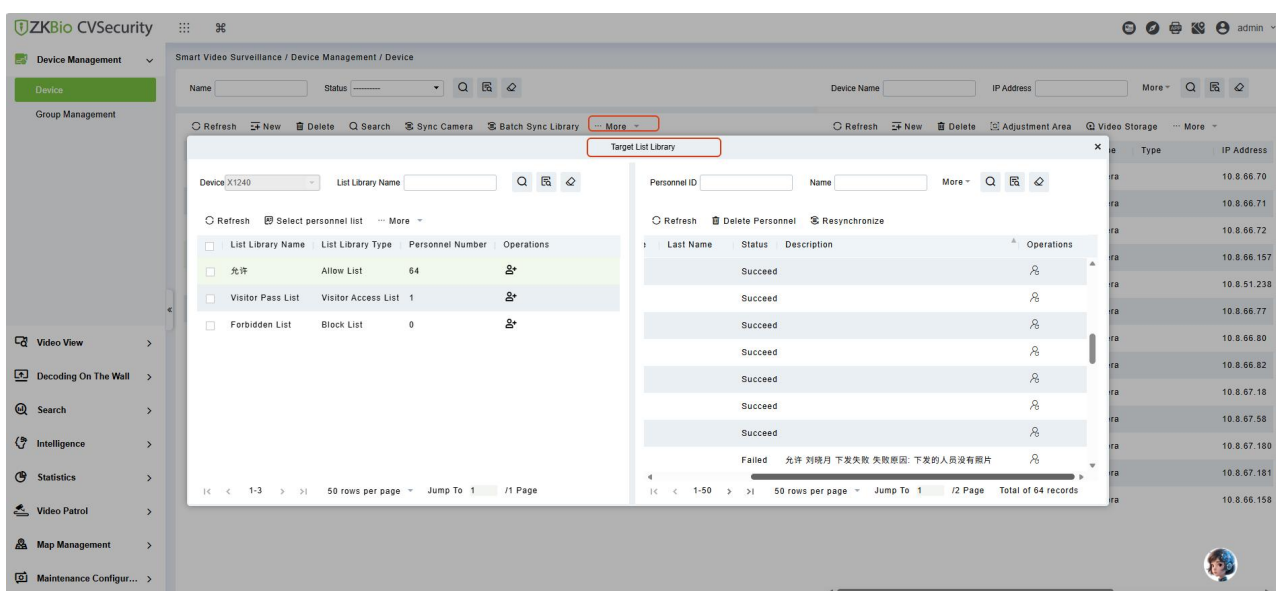
Step 1: Navigate to "Smart Video Surveillance / Device Management / Device", click More → Target List Library



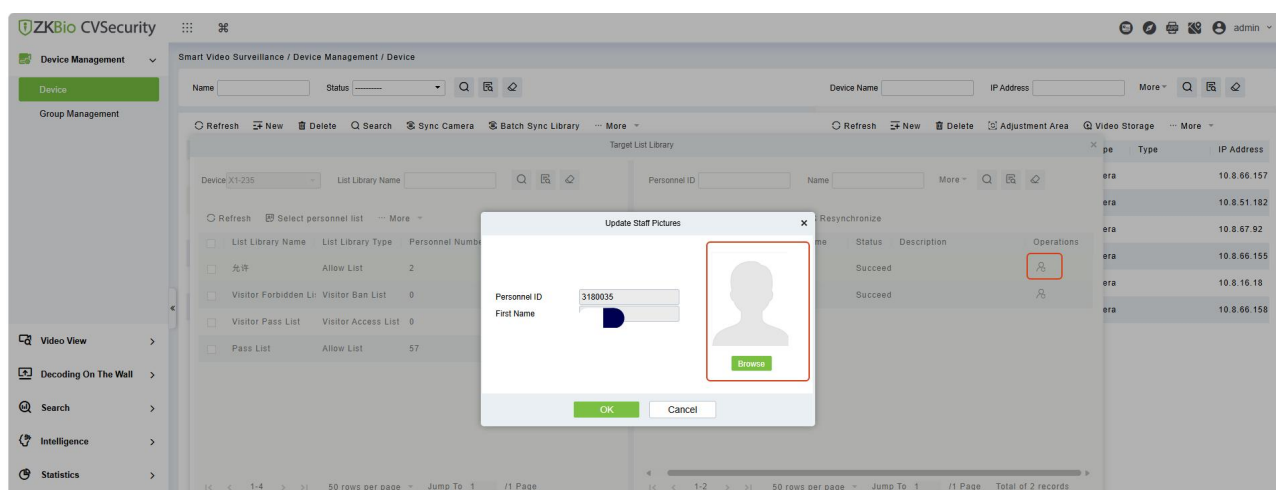
Click Select Watchlist Library to tick the target libraries for configuration.



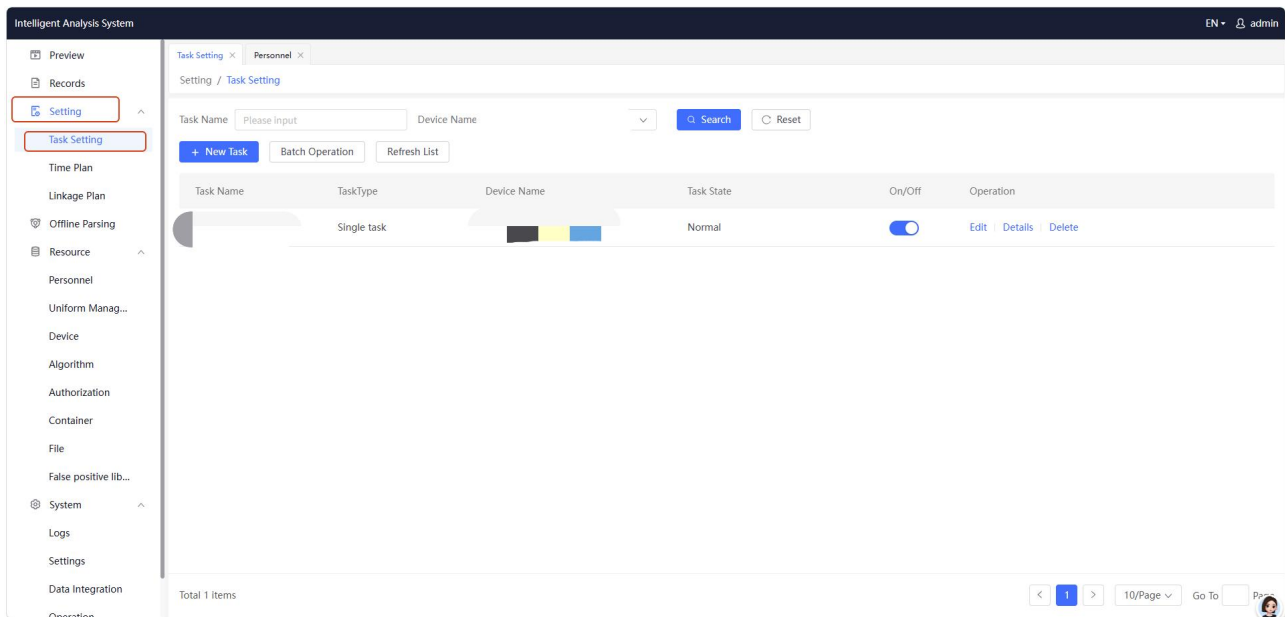
Personnel can be added to each watchlist library separately.



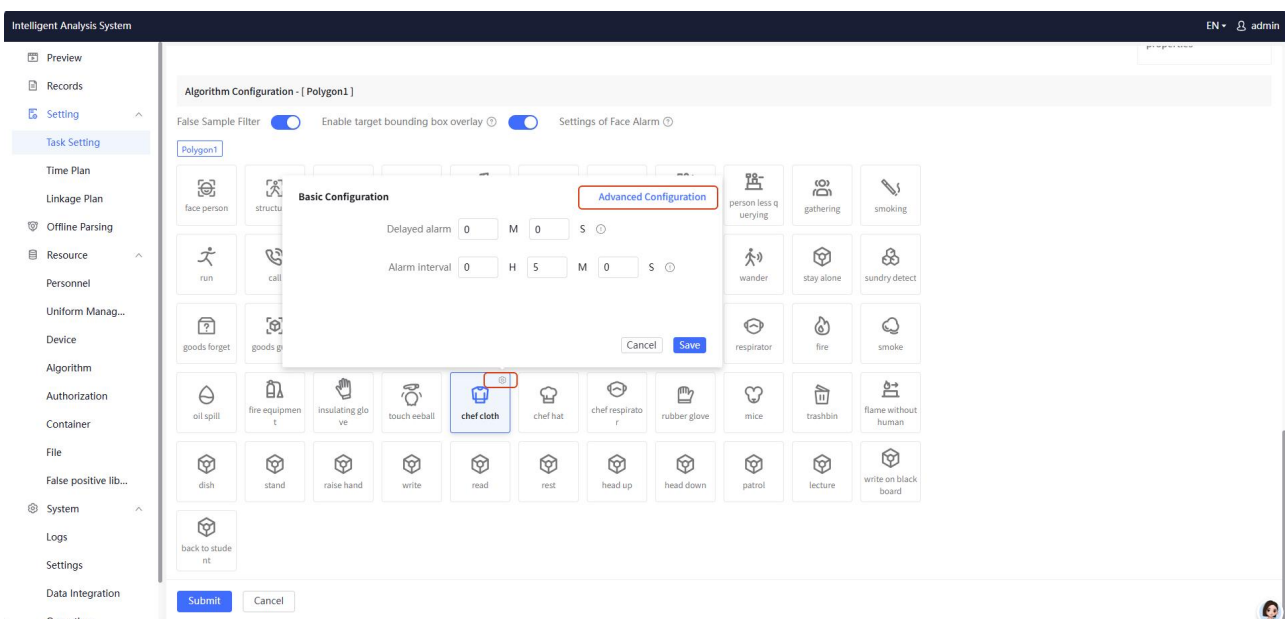
After adding personnel to the library, click the icon in the operation column of personnel info to upload face template photos.



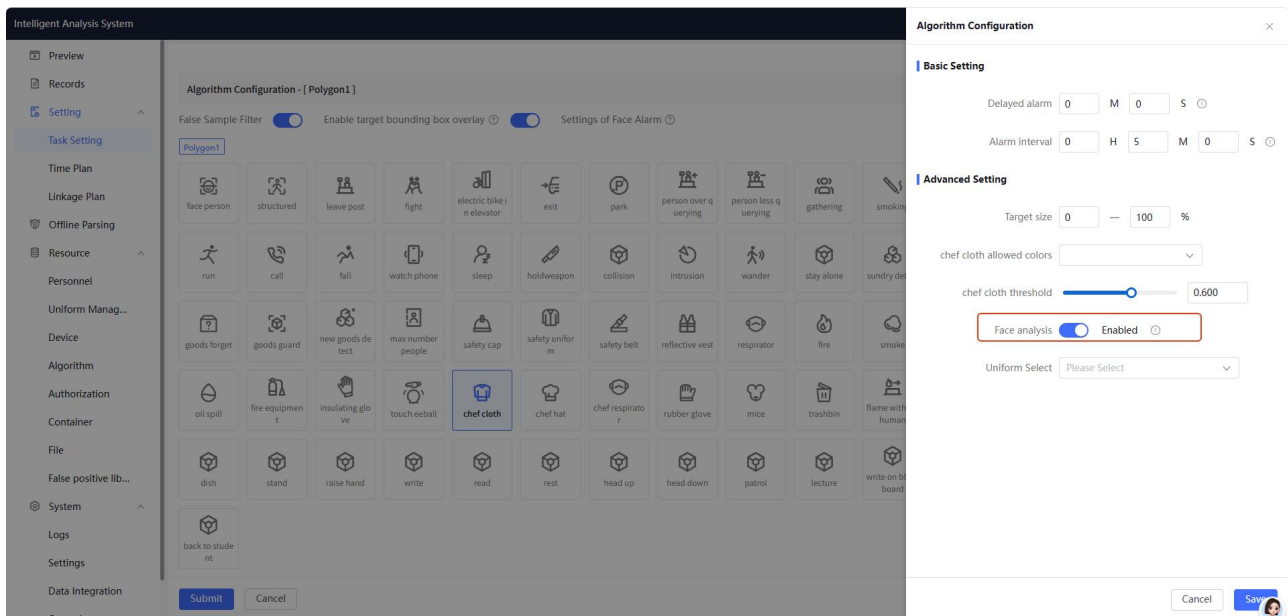
Step 2: Log in to the backend of the X1 device and enter "Setting / Task Setting"



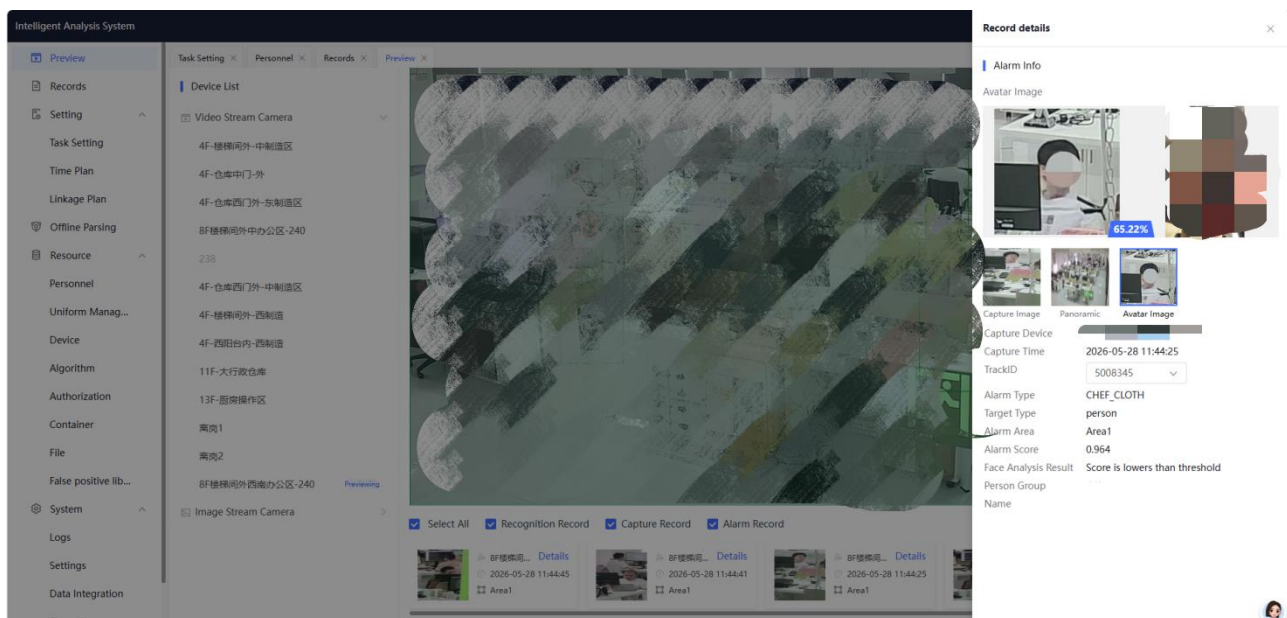
Click New Task and complete basic and rule configurations. During algorithm configuration, select the target algorithm, click the setting icon at the top right of the algorithm box, then enter Advanced Configuration.



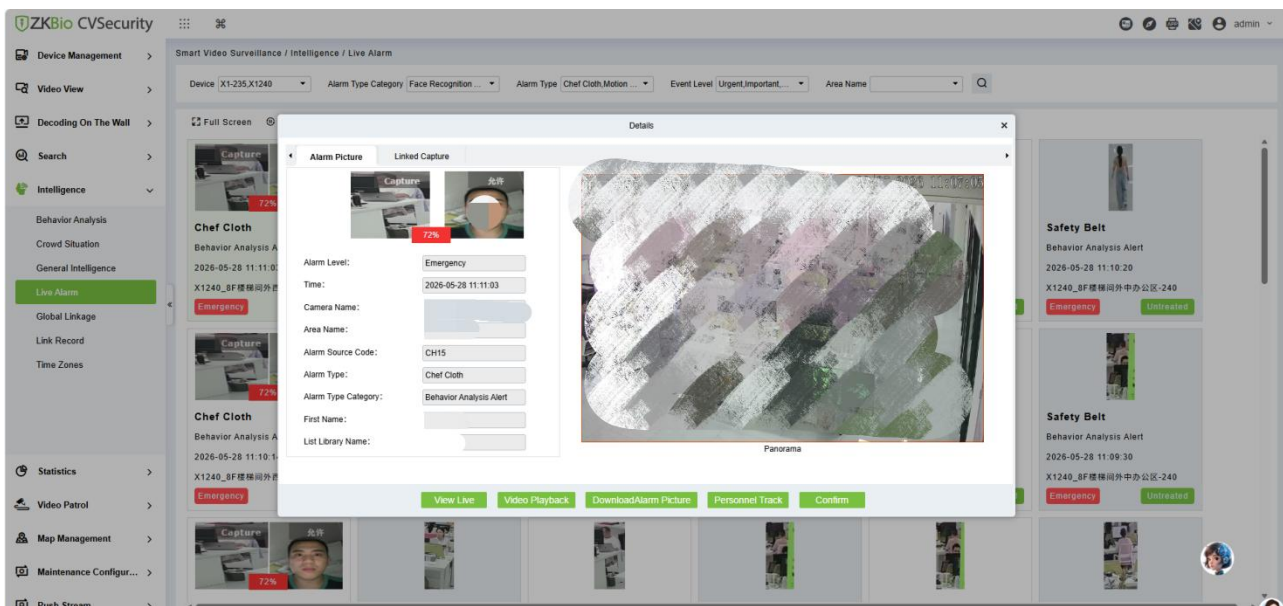
Enable Face Template Analysis the advanced configuration page; after activation, face template analysis will be bound with behavior analysis.



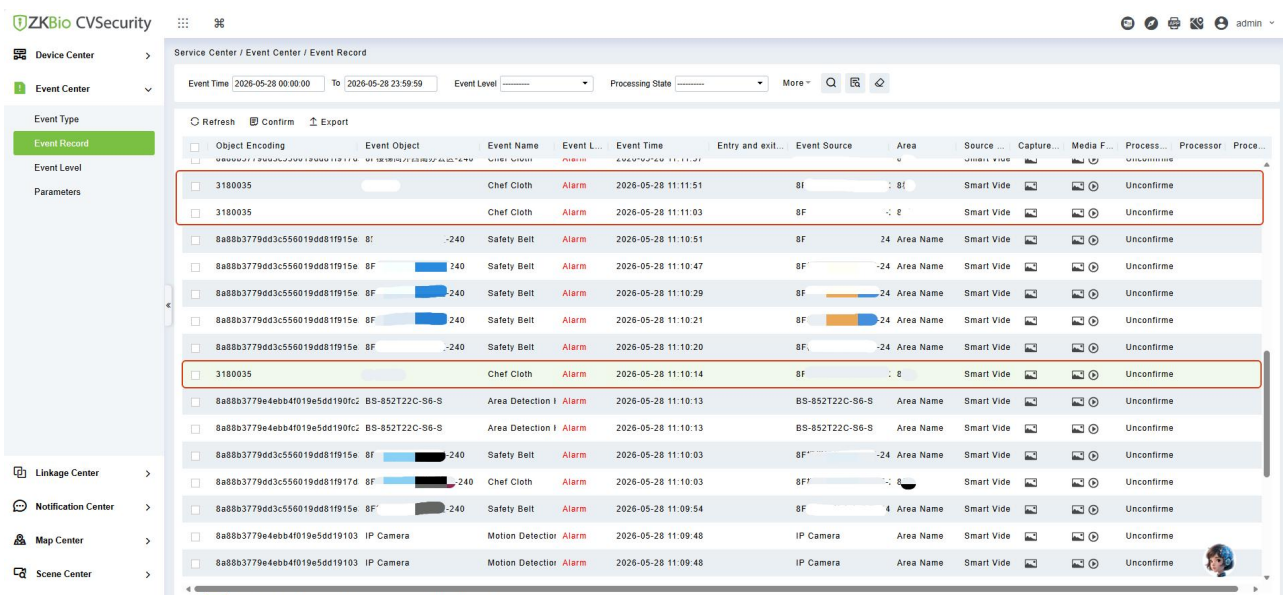
● ZKIVA Edge X1 Alarm Display Interfaces



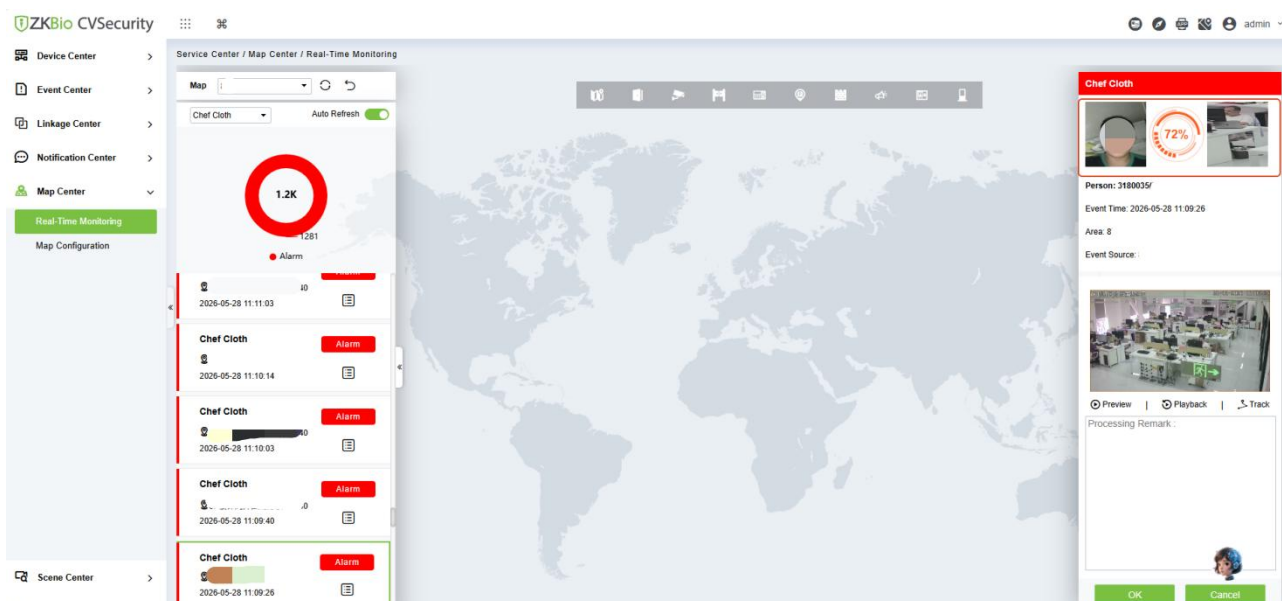
Navigate to "Smart Video Surveillance / Intelligence / Live Alarm". Click any behavior analysis alarm uploaded by ZKIVA Edge X1 to view alarm details, where face template comparison results will be displayed.



Navigate to "Service Center / Event Center / Event Record". The identified personnel name will be shown as the event subject of corresponding behavior analysis records in the list.

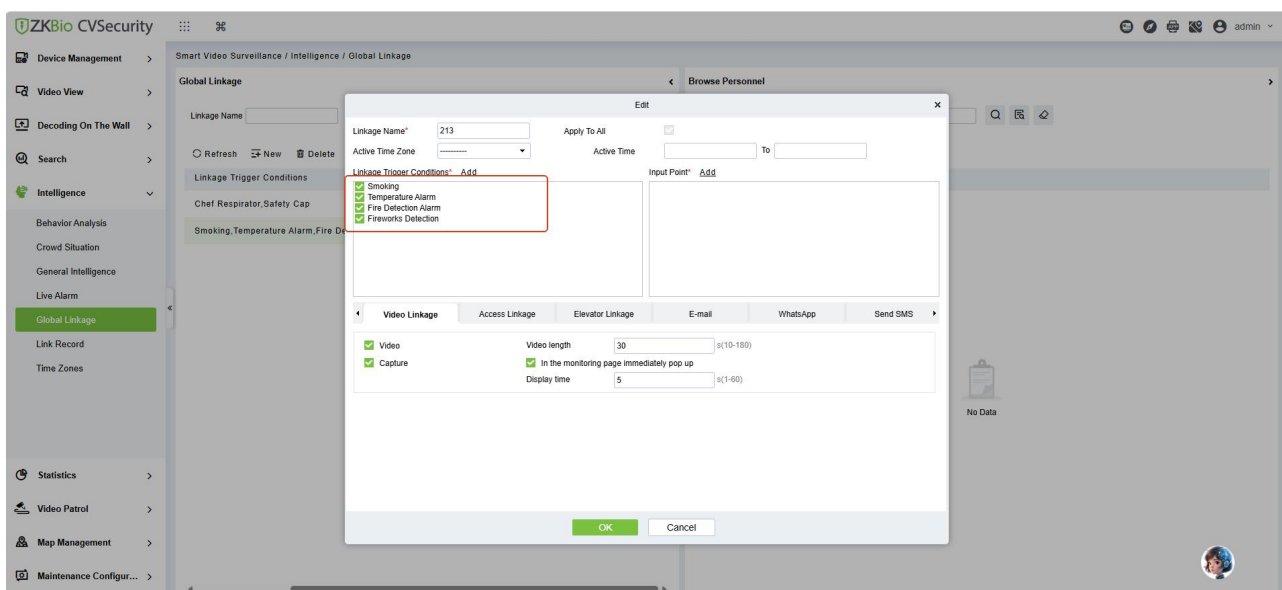


Navigate to "Service Center / Map Center / Real-Time Monitoring". Open the detail pop-up of any behavior analysis alarm; newly added facial authentication records will be displayed on the interface.



9.2. Intelligence - Global Linkage: Support linkage configuration for thermal alarm types of backend NVR (Smoking Detection, Temperature Alarm, Fire Spot Detection, Smoke & Fire Detection).

Navigate to "Smart Video Surveillance / Intelligence / Global Linkage" to add new linkage trigger conditions. Available options include Smoking Detection, Temperature Alarm, Fire Detection and Fireworks Detection.

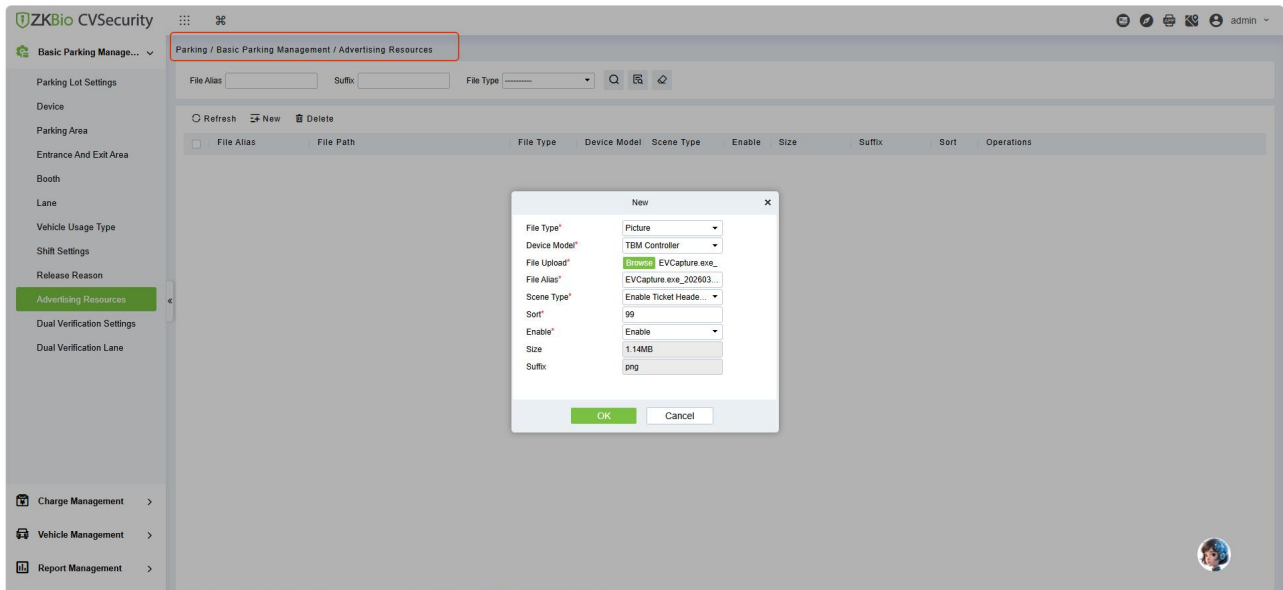


10. Parking

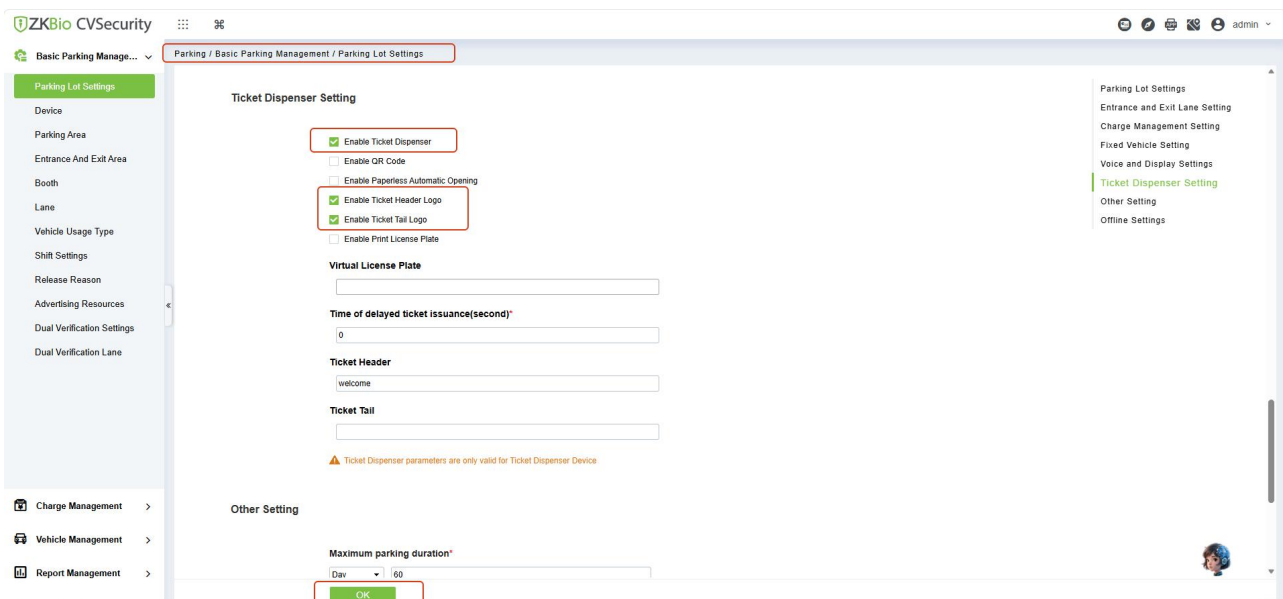
10.1. Basic Parking Management / Parking Lot Settings – Ticket Dispenser Setting: Support logo upload for receipt printing.

Navigate to "Parking / Basic Parking Management / Advertising Resources", click New, select picture as file type and TBM Controller as device model, upload the logo image file, choose either Enable Ticket Header Logo or Enable Ticket Tail Logo as scene type, then select Enabled to save configuration.

- Note: The picture is too large. Please upload a picture file smaller than 10KB.

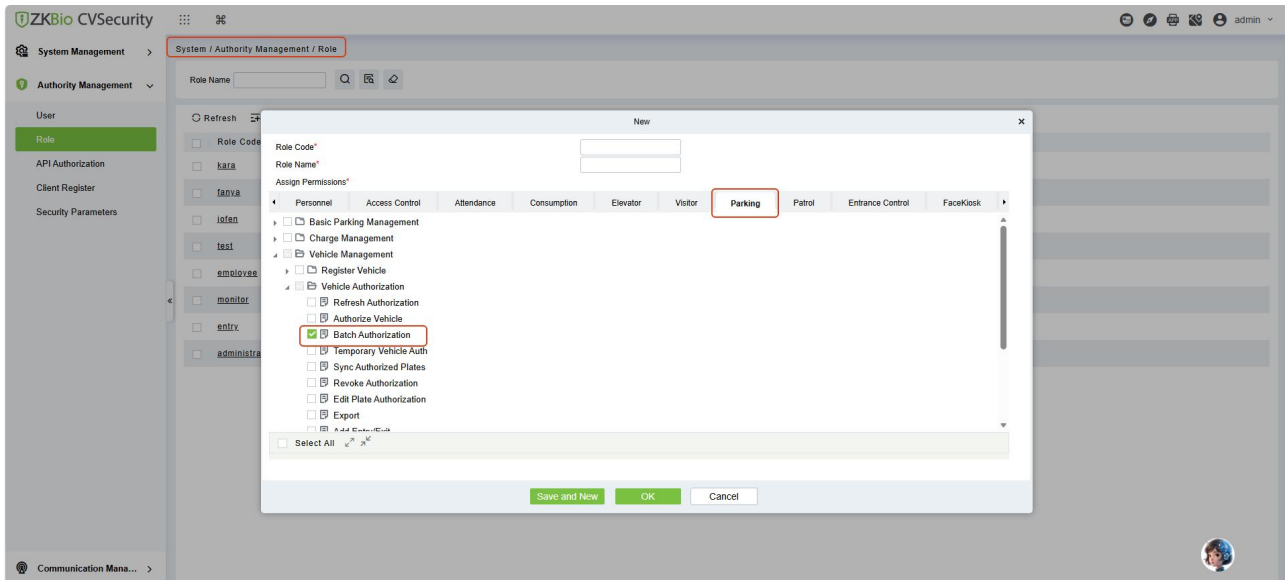


Go to "Parking / Basic Parking Management / Parking Lot Settings", open Ticket Dispenser Setting and tick Enable Ticket Dispenser– Enable Ticket Header Logo / Enable Ticket Tail Logo, then click OK. The uploaded logo will be printed on parking receipts.



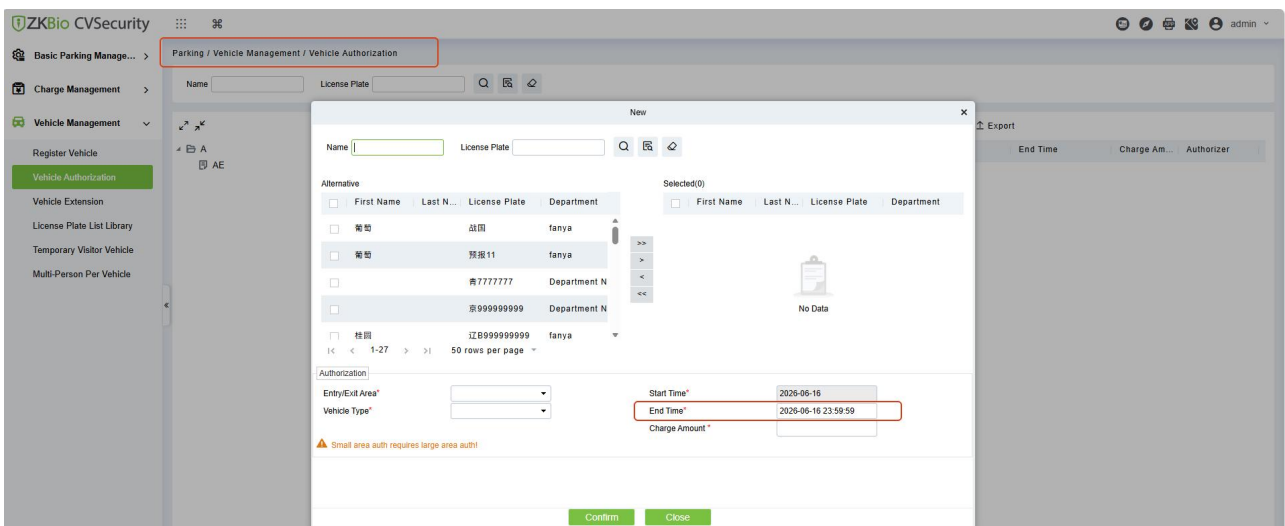
10.2. Vehicle Management / Vehicle Authorization: Permission control added for batch authorization button.

Navigate to "System / Authority Management / Role". When creating or editing a role, find Parking Module – Vehicle Management – Vehicle Authorization – Batch Authorization in the permission allocation list to configure access rights for this operation button.



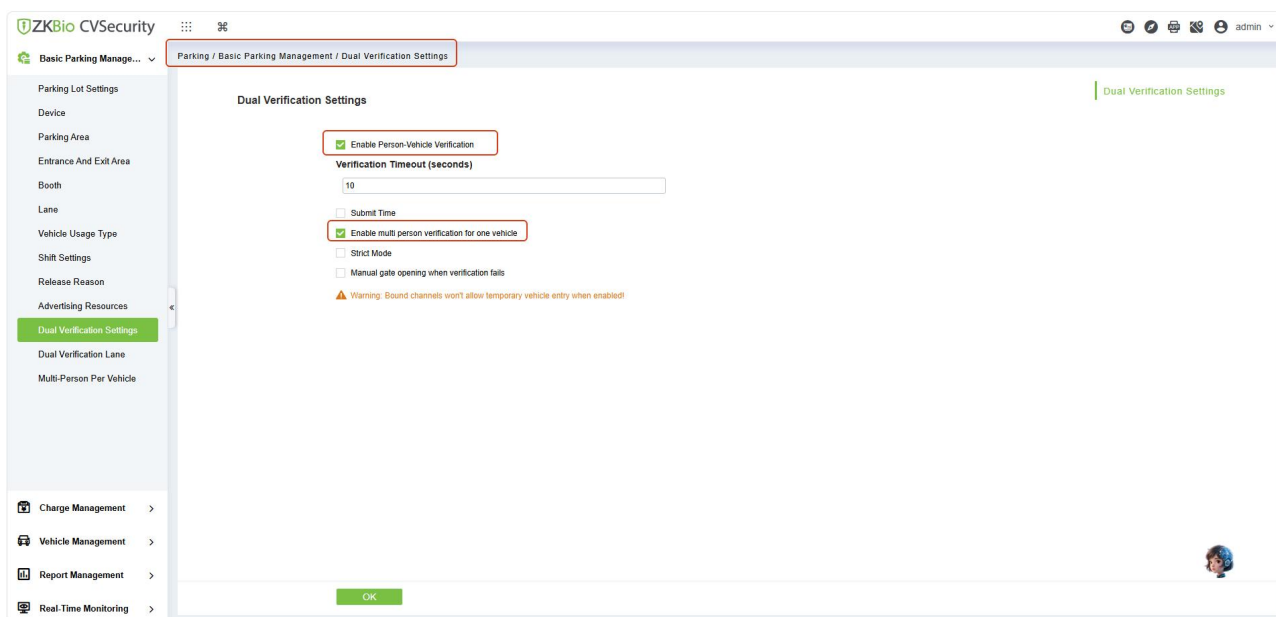
10.3. Vehicle Management / Vehicle Authorization: Start & End time supports Hour & Minute precision.

Navigate to "Parking / Vehicle Management / Vehicle Authorization" and open Batch Authorization. The end time can be set accurate to minutes and seconds.



10.4. Basic Parking Management / Dual Verification Settings: Multiple users can bind to one license plate for dual verification.

Step 1: Navigate to "Parking / Basic Parking Management / Dual Verification Settings", tick Enable Person-Vehicle Verification – Enable multi person verification for one vehicle and click OK.



● Parameter Description:

- Verification Timeout: Maximum time interval between license plate recognition and personnel recognition

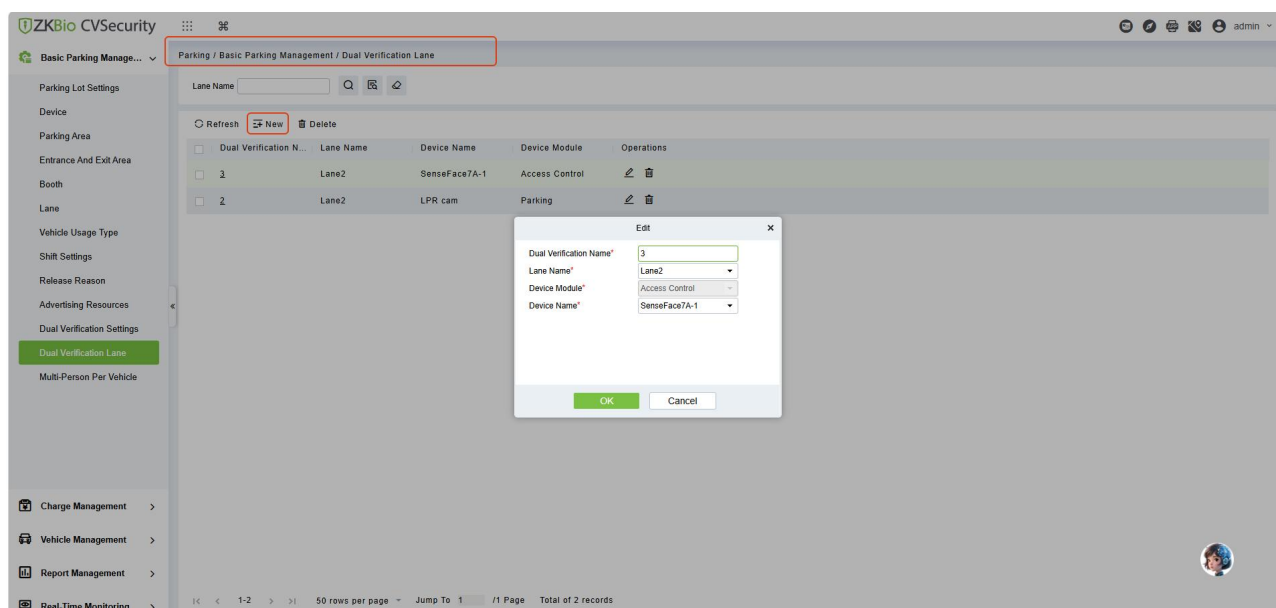
- Submit Time: Check this option to use the record upload time if there is a large time deviation between access control devices and platform server

- Strict Mode:

Enable: Once one round of vehicle-person verification is completed, re-recognition of both person and vehicle is required for next access

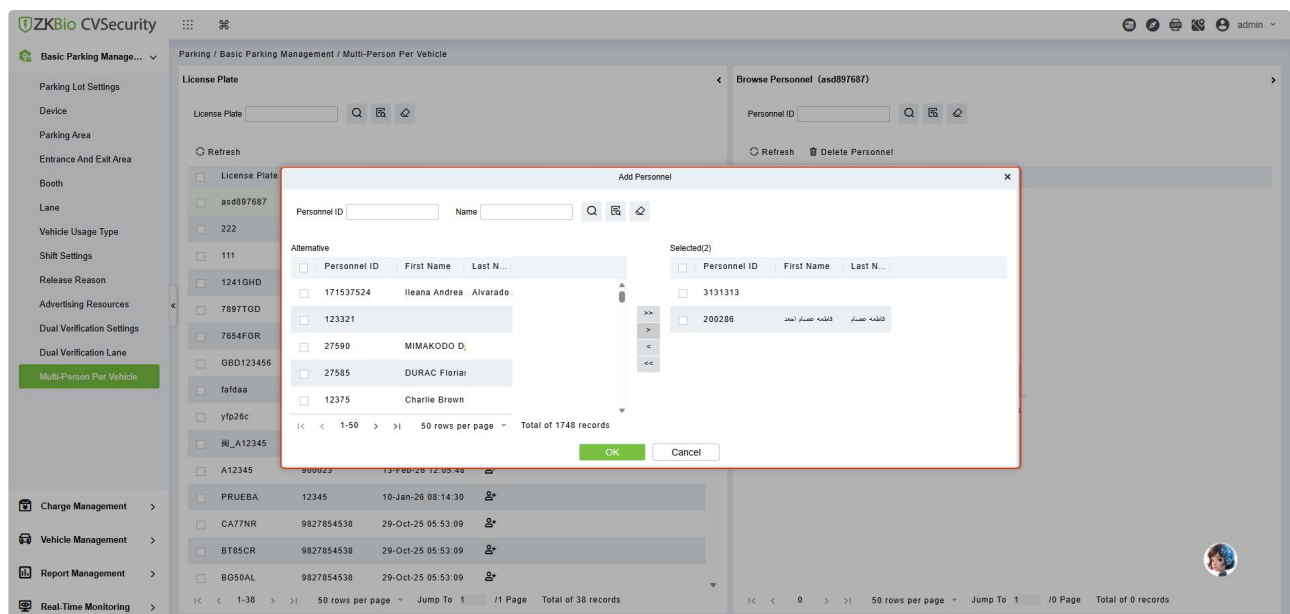
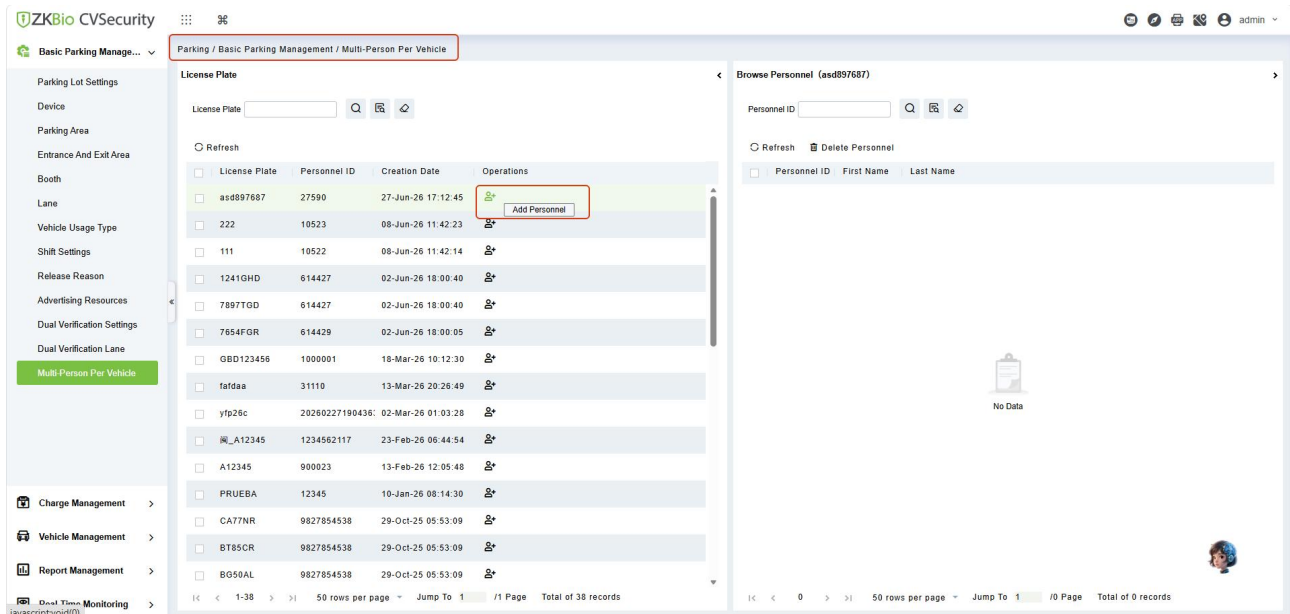
Disable: The same person can be recognized multiple times until matching succeeds within the timeout window

Step 2: Navigate to "Parking / Basic Parking Management / Dual Verification Lane", click New to bind corresponding access control devices and parking cameras respectively.



Step 3: Navigate to "Parking / Basic Parking Management / Multi-Person Per Vehicle", click Add Personnel beside the target license plate to bind multiple persons to one plate.

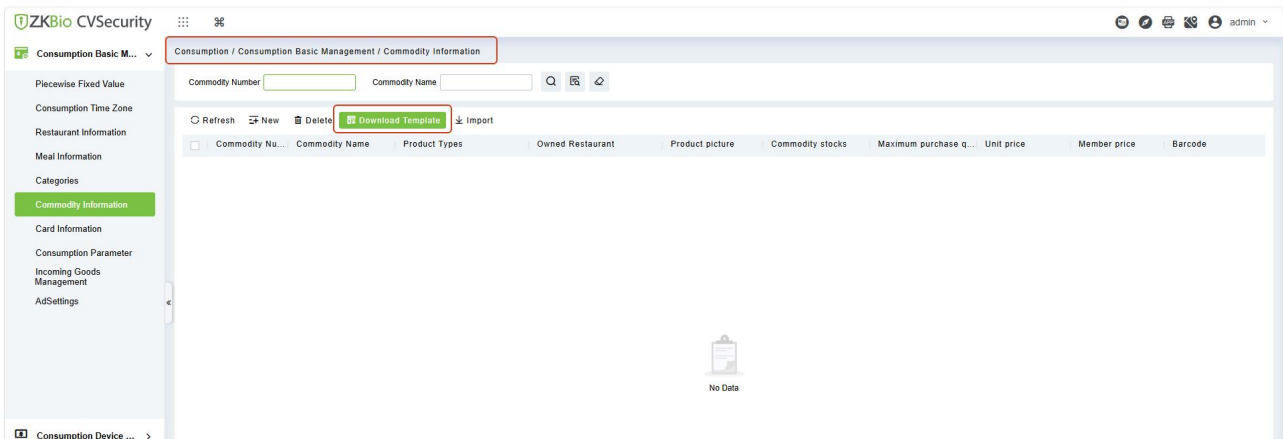
- This function fits family parking scenarios where one vehicle is shared by several family members.



11. Consumption

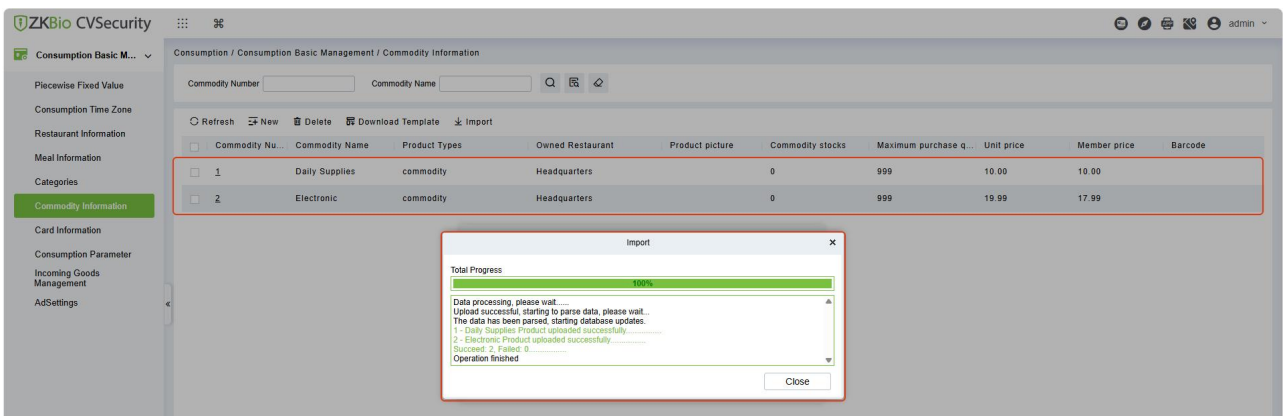
11.1. Consumption Basic Management / Commodity Information: Add import function to support batch import of commodity information via import template.

Navigate to "Consumption / Consumption Basic Management / Commodity Information". Click Download Template to get the commodity import template.



Fill in data according to header rules, then click Import and select the filled file to complete bulk commodity import.

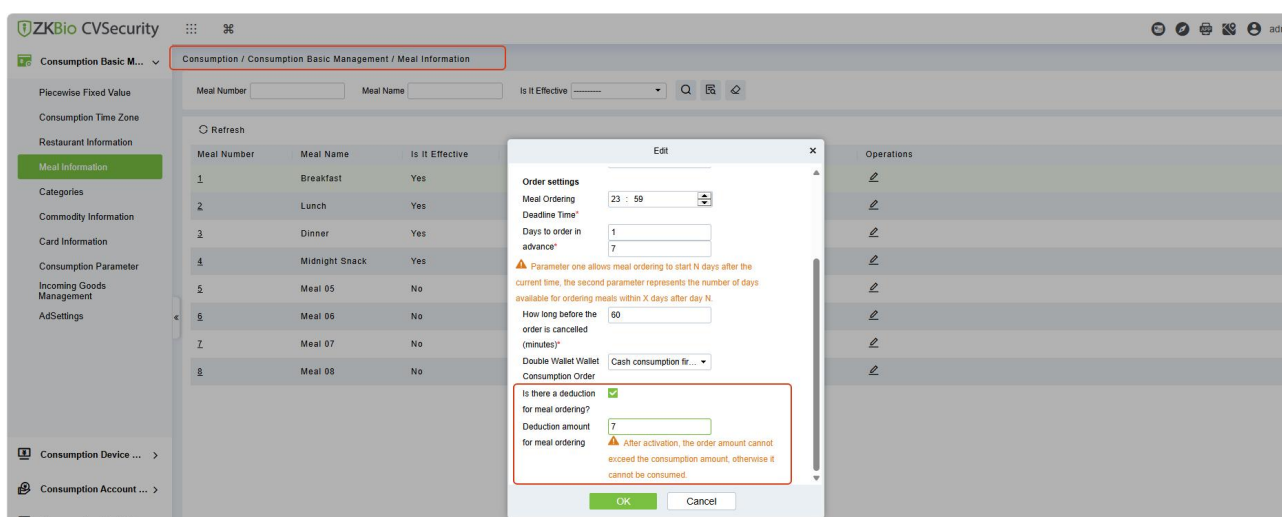
Product import template							
Product number (required*)	Product name (required*)	Maximum purchase quantity (* less than 10,000)	Unit price (* Price less than 1000)	Member price (less than 1000)	Product category number (required*)	Restaurant number (required*)	Meal type number (use ',' to separate multiple selections)
1	Daily Supplies	999	10	10	1	1	1,2,3
2	Electronic Accessories	999	19.99	17.99	1	1	1,2,3



11.2. Consumption Basic Management / Meal Information: Configure prepayment pricing after meal reservation to prevent no-show after reservation.

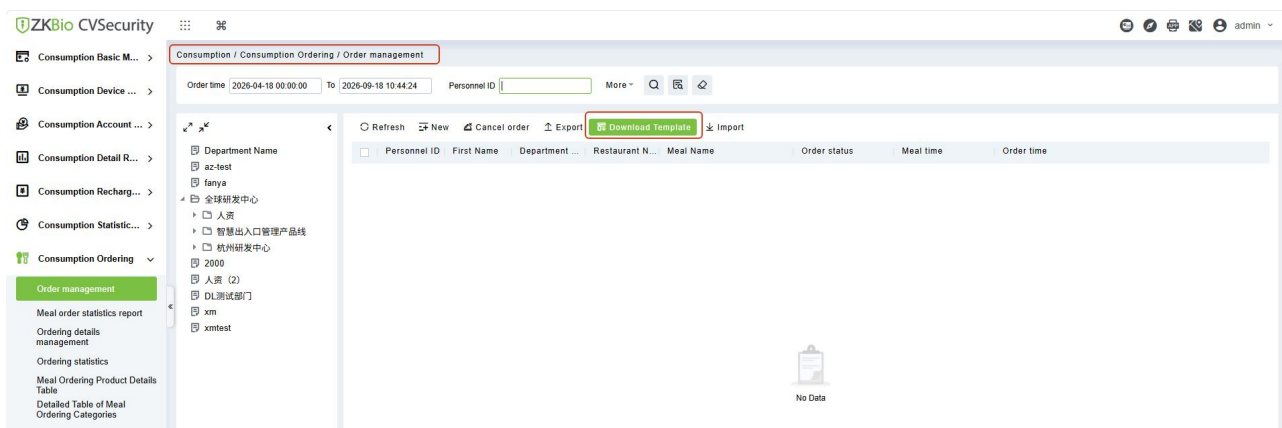
Navigate to "Consumption / Consumption Basic Management / Meal Information". Click the edit icon in the operation column of the target meal type. Enable the parameter "Is there a deduction for meal ordering?" and set the deduction amount to realize pre-payment of fixed fees after meal reservation.

- Note: After enabling this parameter, the configured reservation deduction amount cannot exceed the actual consumption amount; otherwise, consumption transactions will fail.

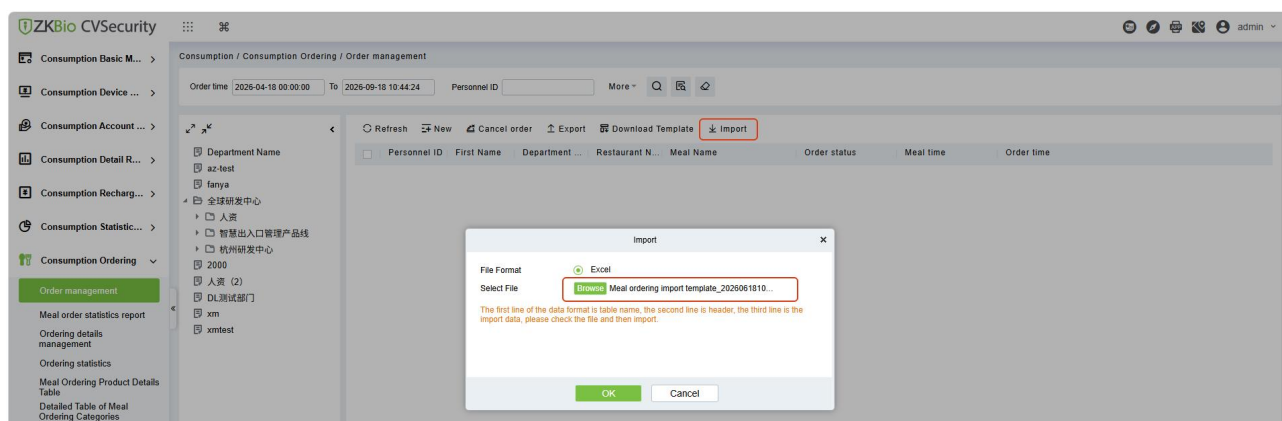


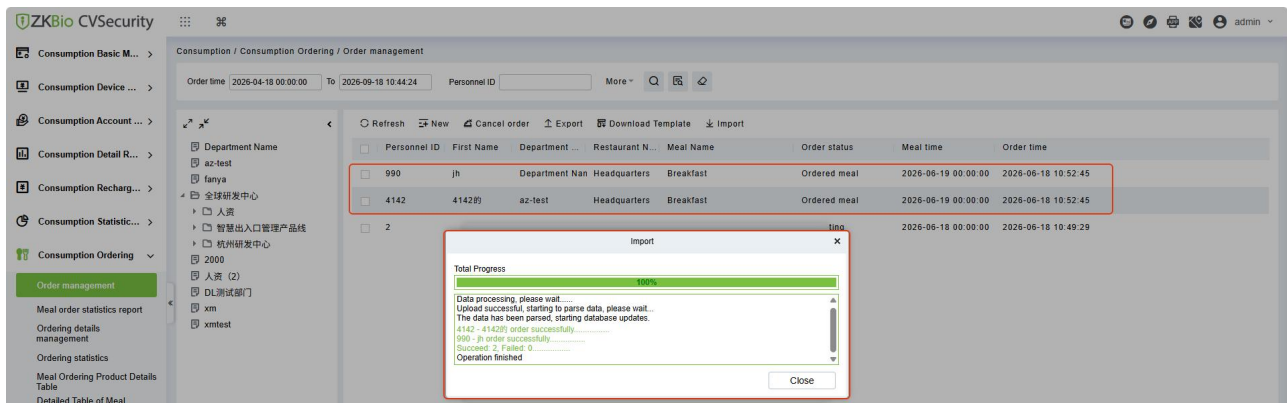
11.3. Consumption Ordering / Order management: Add import function to support batch meal reservation via import template.

Bulk Import Meal Reservation Records Enter "Consumption / Consumption Ordering / Order management". Click Download Template to obtain the meal reservation import template, complete filling following table headers, then click Import and upload the file to finish batch reservations.



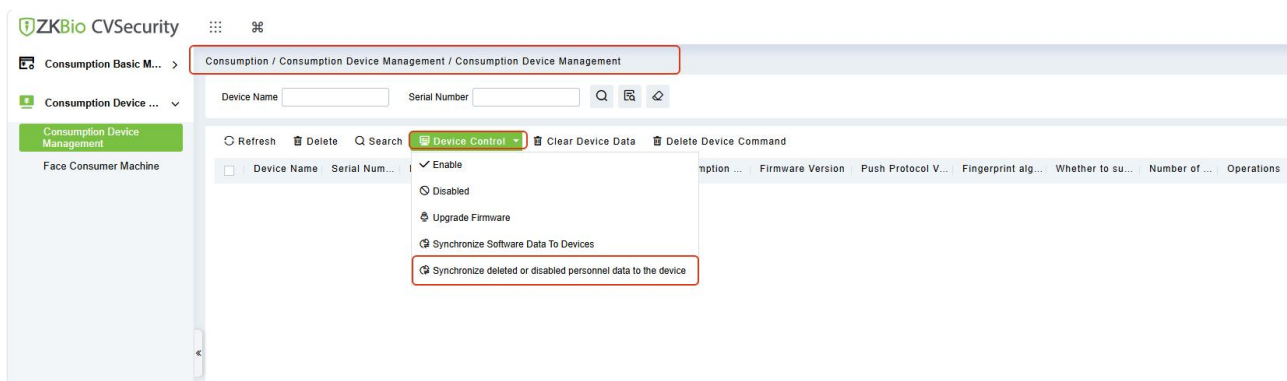
Meal ordering import template				
Personnel number/Department number (required*)	Meal type number (required*)	Reservation time (required*)	Restaurant number (required*)	Order by personnel or department (0 for personnel order, 1 for department order required*)
4142	1	2026-06-19	1	0
990	1	2026-06-19	1	0





11.4. Bug Fix: Optimize to support reissuing only deactivated consumption accounts to devices separately instead of full-volume distribution, improving distribution efficiency and avoiding illegal card swiping by resigned employees.

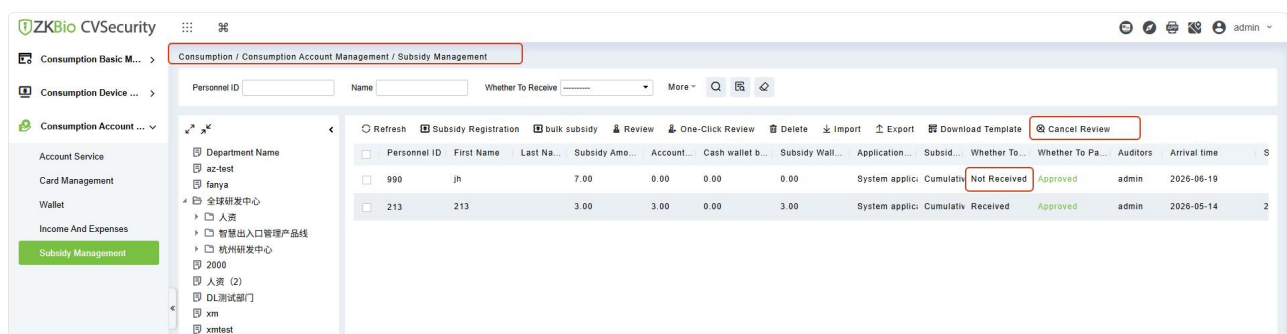
Navigate to "Consumption / Consumption Device Management / Consumption Device Management". Tick target devices, click Device Control – Synchronize deleted or disabled personnel data to the device. This function separately pushes disabled consumption account data to selected terminals.



11.5. Consumption Account Management / Subsidy Management: Add subsidy withdrawal function for unredeemed subsidies by canceling review process.

Navigate to "Consumption / Consumption Account Management / Subsidy Management". Tick subsidies with status "Not Received", then click "Cancel Review" to withdraw the corresponding subsidies.

Note: Only subsidies with the status "Not Received" can be revoked.



ZKBio CVSecurity

Consumption Basic M...>

Consumption Device ...>

Consumption Account ...>

Account Service

Card Management

Wallet

Income And Expenses

Subsidy Management

Consumption / Consumption Account Management / Subsidy Management

Personnel ID: Name: Whether To Receive: More

Refresh Subsidy Registration bulk subsidy Review One-Click Review Delete Import Export Download Template Cancel Review

Personnel ID	First Name	Last Na...	Subsidy Amo...	Account...	Cash wallet b...	Subsidy Wall...	Application...	Subsid...	Whether To...	Whether To Pa...	Auditors	Arrival time	S
999	jh		7.00	0.00	0.00	0.00	System applic: Cumulativ	Not Received	Not Approved			2026-06-19	8
213	213		3.00	3.00	0.00	3.00	System applic: Cumulativ	Received	Approved	admin		2026-05-14	2

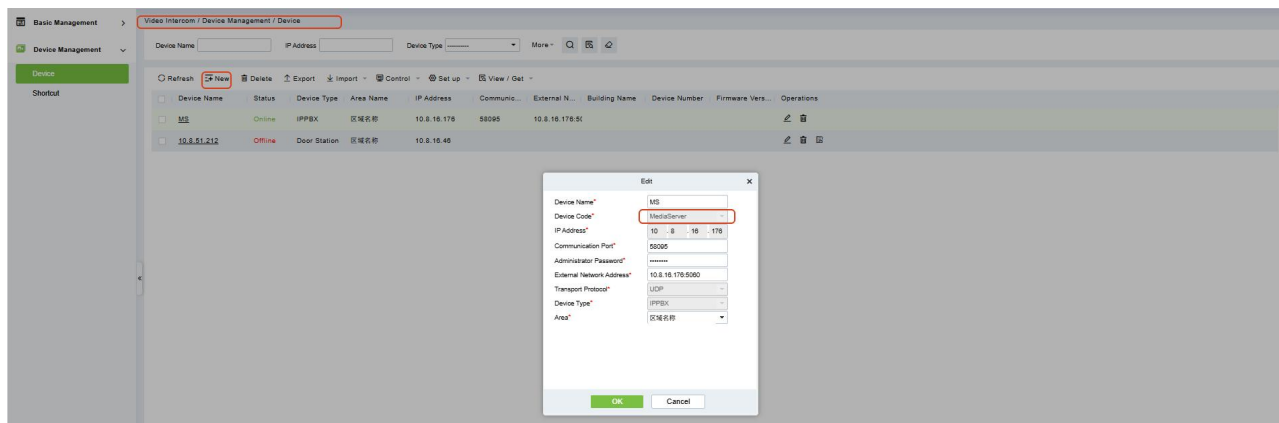
The operation succeeded!

12. Video Intercom

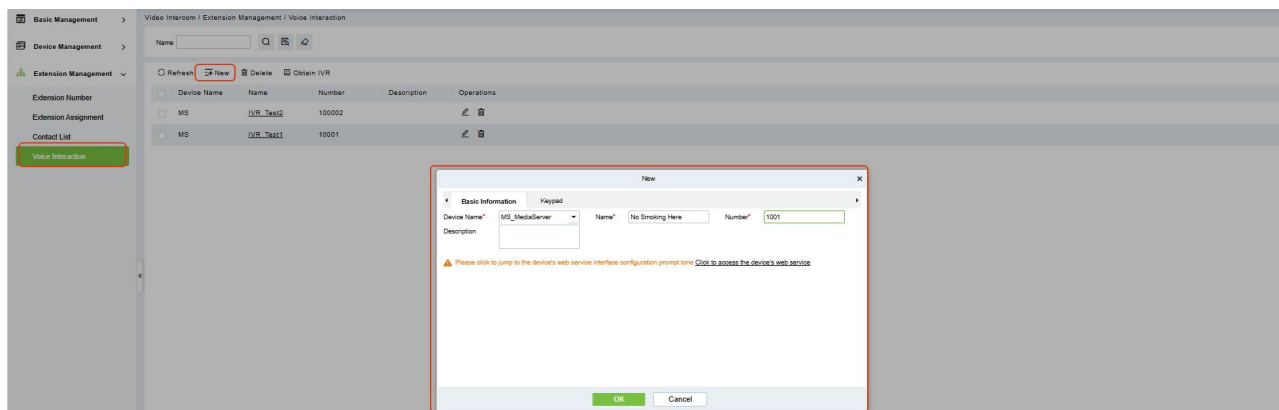
12.1. Service Center / Linkage Center / Linkage Configuration: Support IVR linkage configuration.

- Operation Steps

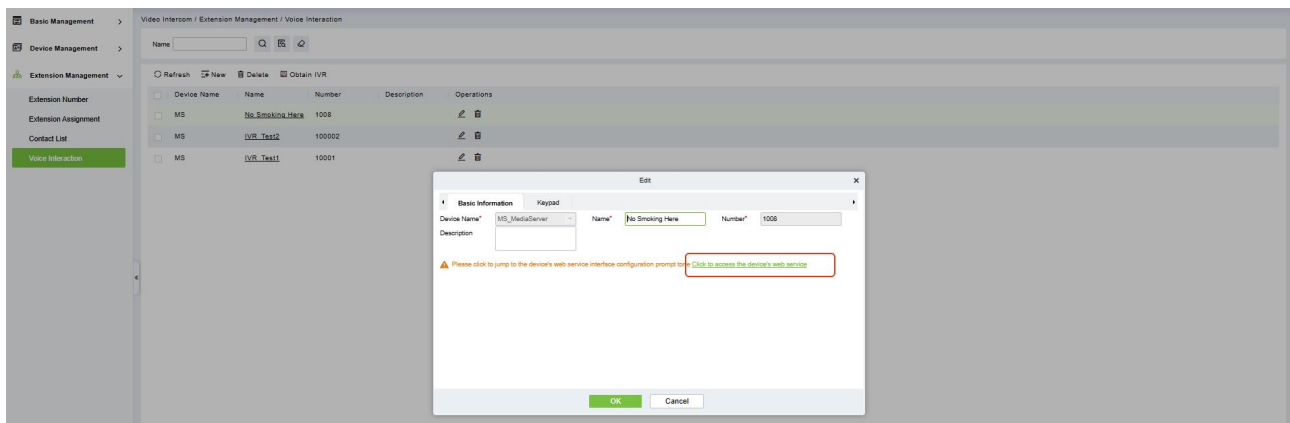
Step 1: Navigate to "Video Intercom / Device Management / Device. Check MediaServer as the manufacturer, fill in the server IP address and SIP address (port 5060), select the corresponding area, and leave other parameters unchanged.



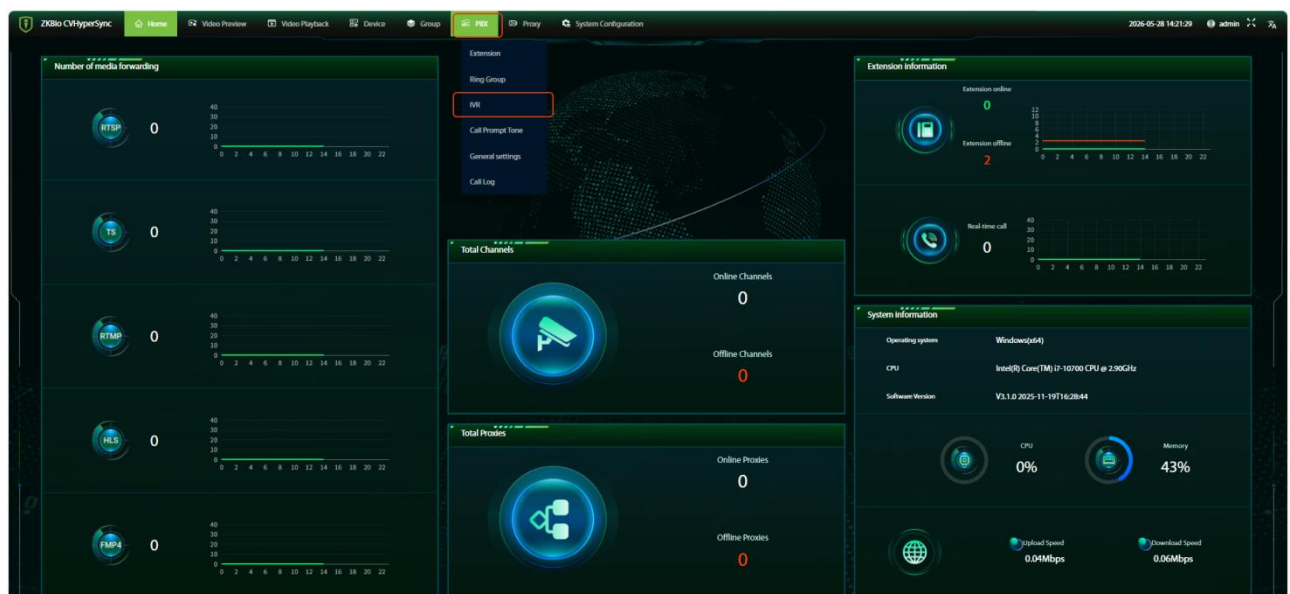
Step 2: Go to "Video Intercom / Extension Management / Voice Interaction", click Add to create an IVR entry. Tick MediaServer as the device, then customize the IVR name and number.



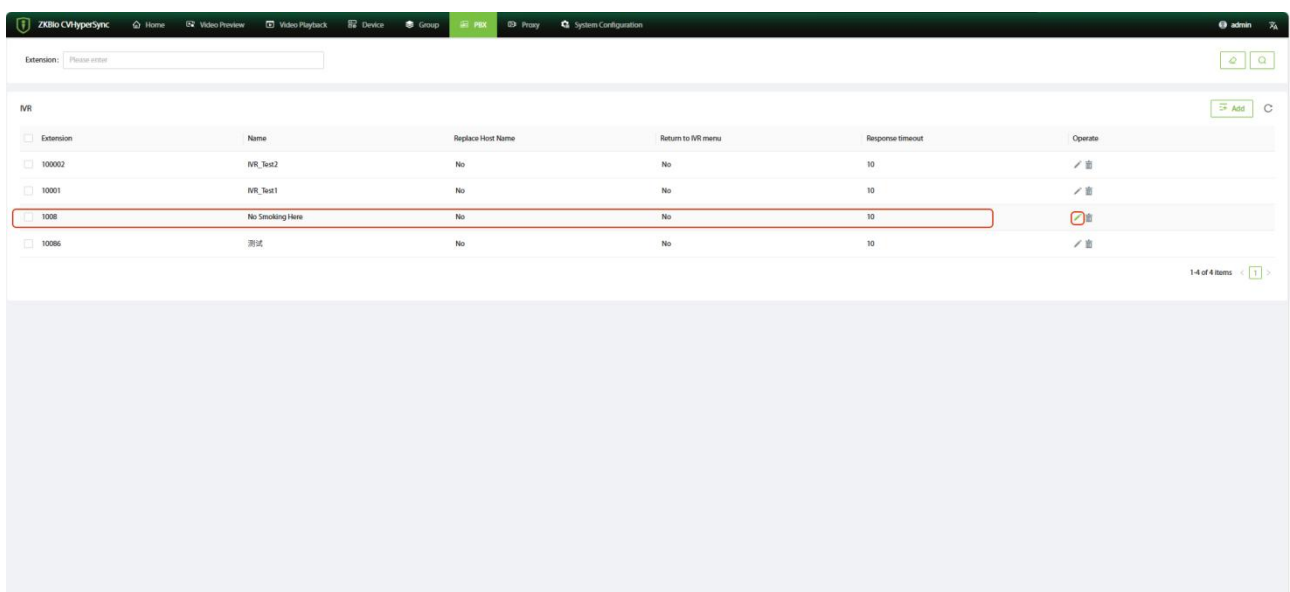
Step 3: Click Jump to access the device web management page.



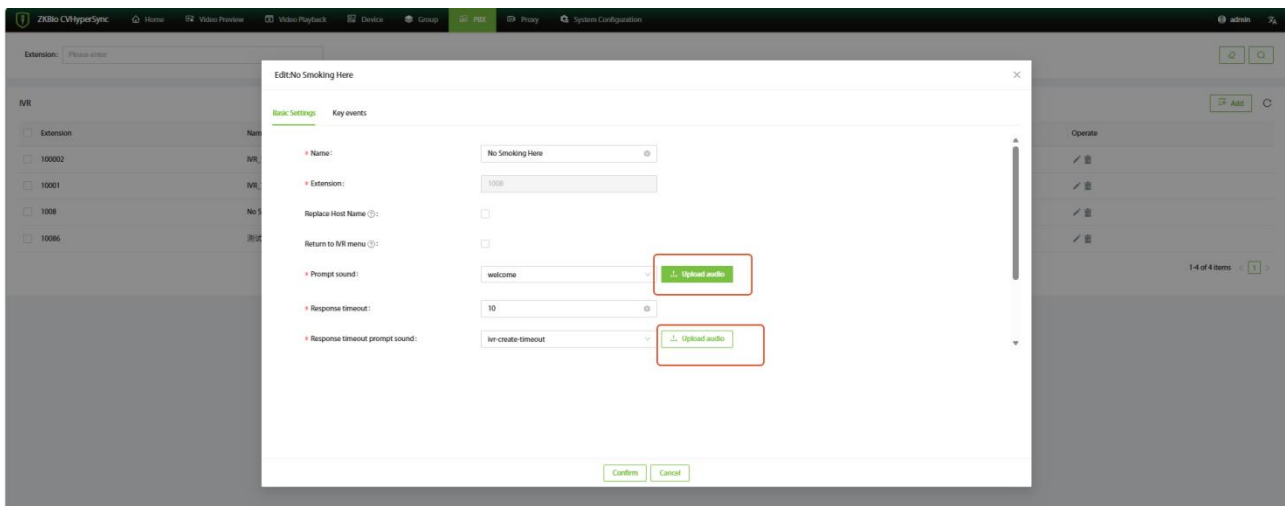
Step 4: On the web page, enter "PBX - IVR".



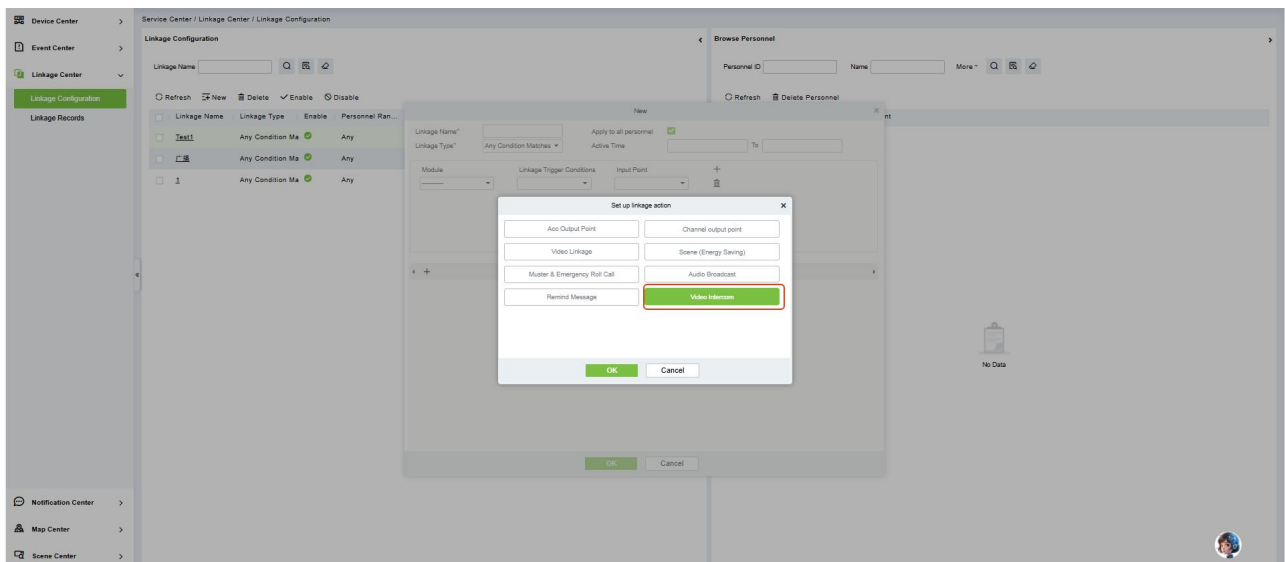
The IVR created in ZKBio CVSecurity will be displayed here.



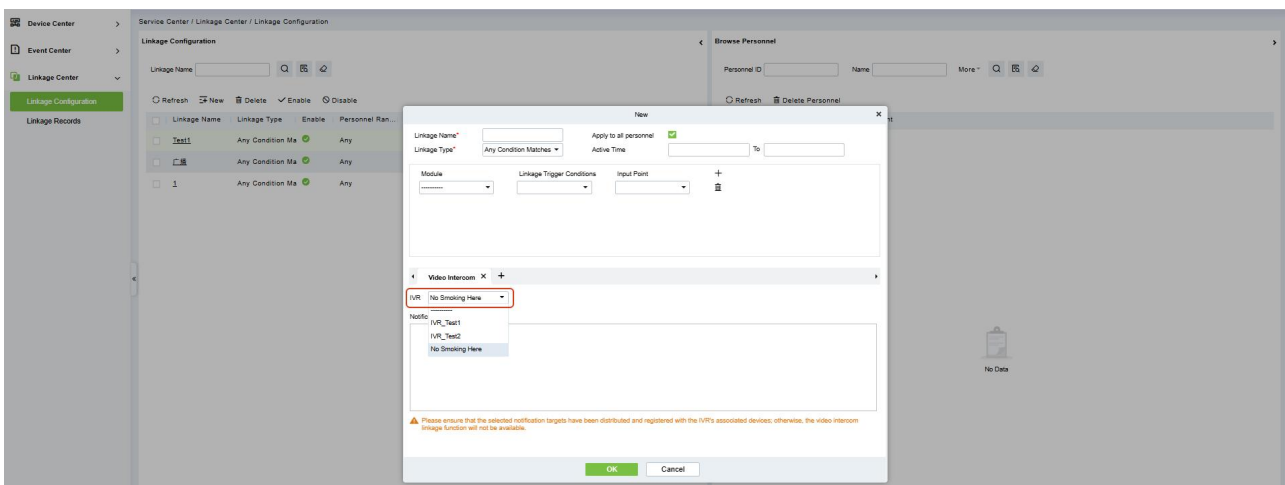
Click Edit to upload audio files and configure voice prompts.



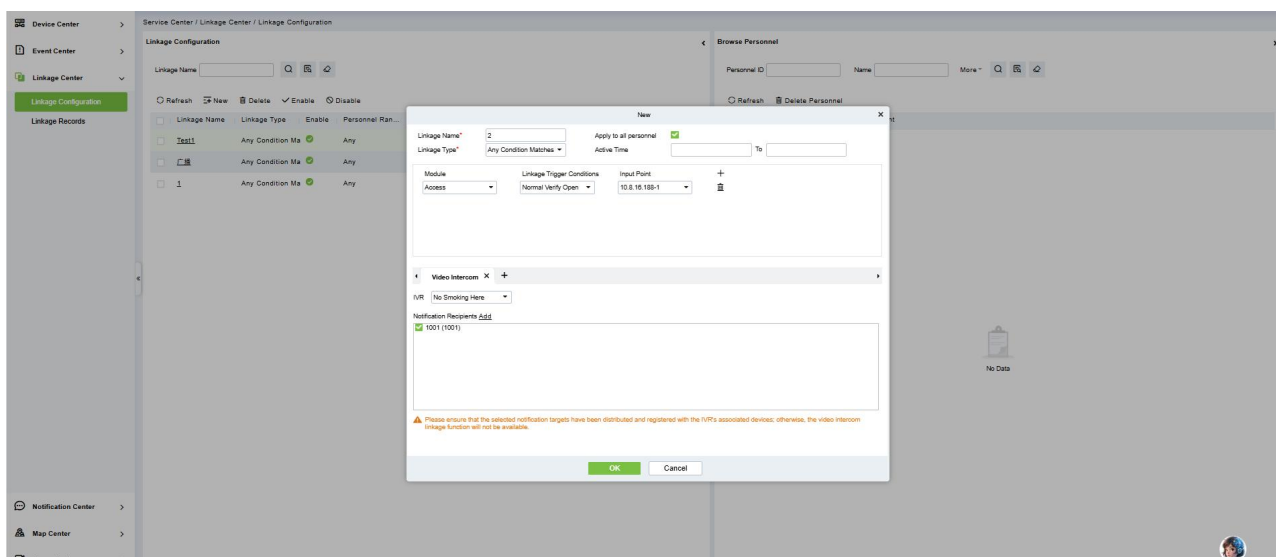
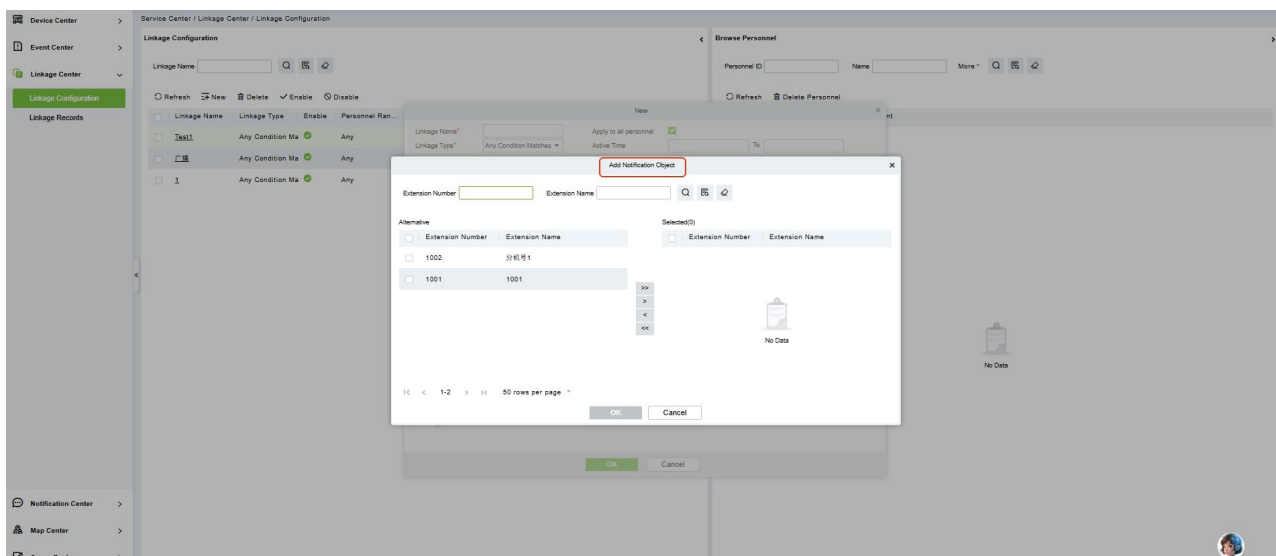
Step 5: Navigate to "Service Center / Linkage Center / Linkage Configuration", click Add to open the linkage configuration page. Select Video Intercom as the linkage action.



Choose the preconfigured IVR.



Then select notification targets to finish IVR linkage setup.



12.2.Extension Management / Extension Number: Max concurrent registration limit updated to 5 when creating new extensions.

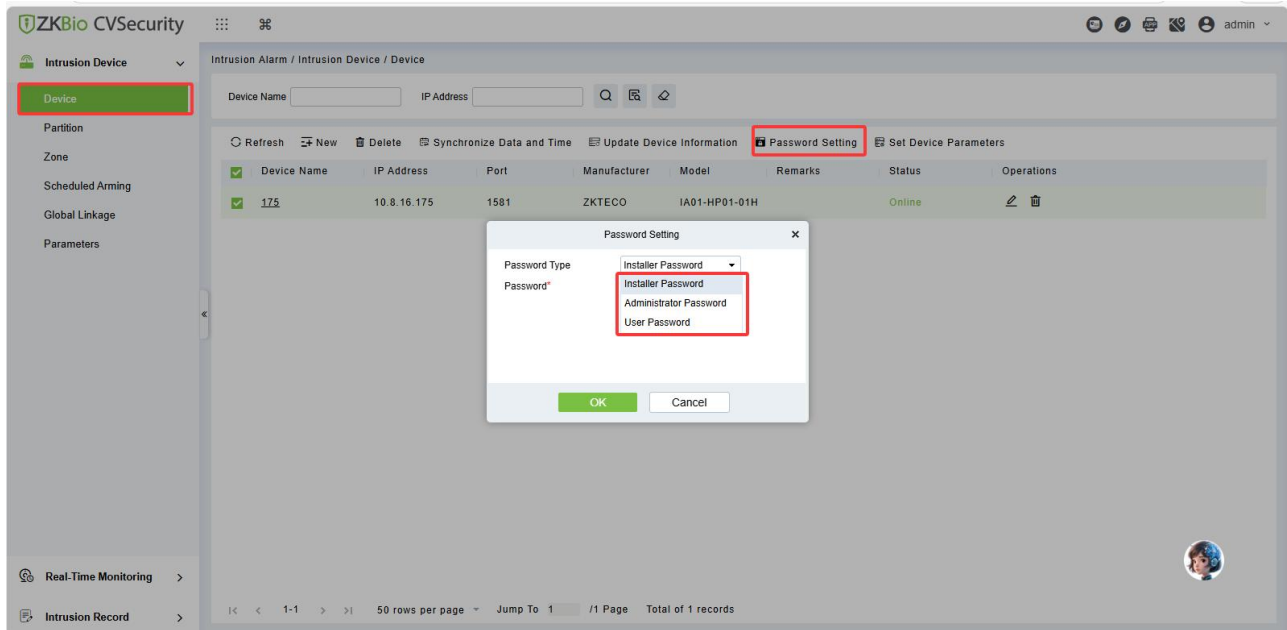
Navigate to "Video Intercom / Extension Management / Extension Number" and click Add. The concurrent registration quantity limit for extension numbers ranges from 1 to 5.

The screenshot displays the ZKBio CVSecurity Video Intercom Extension Management interface. The 'New' dialog box is open, showing fields for Name, Extension Number, Voice Mail, Registered Terminal Count, Incoming Call Number, Direct Dialing Address, Extension Type, Extension Password, Voice Mailbox Password, and SIP. A red box highlights the 'Registered Terminal Count' field with the value '6' and a tooltip message: 'Please enter a value between 1 and 5.' The left sidebar shows navigation options: Basic Management, Device Management, Extension Management (selected), Extension Assignment, Contact List, Voice Interaction, and Access Management. The top bar shows the user 'admin'.

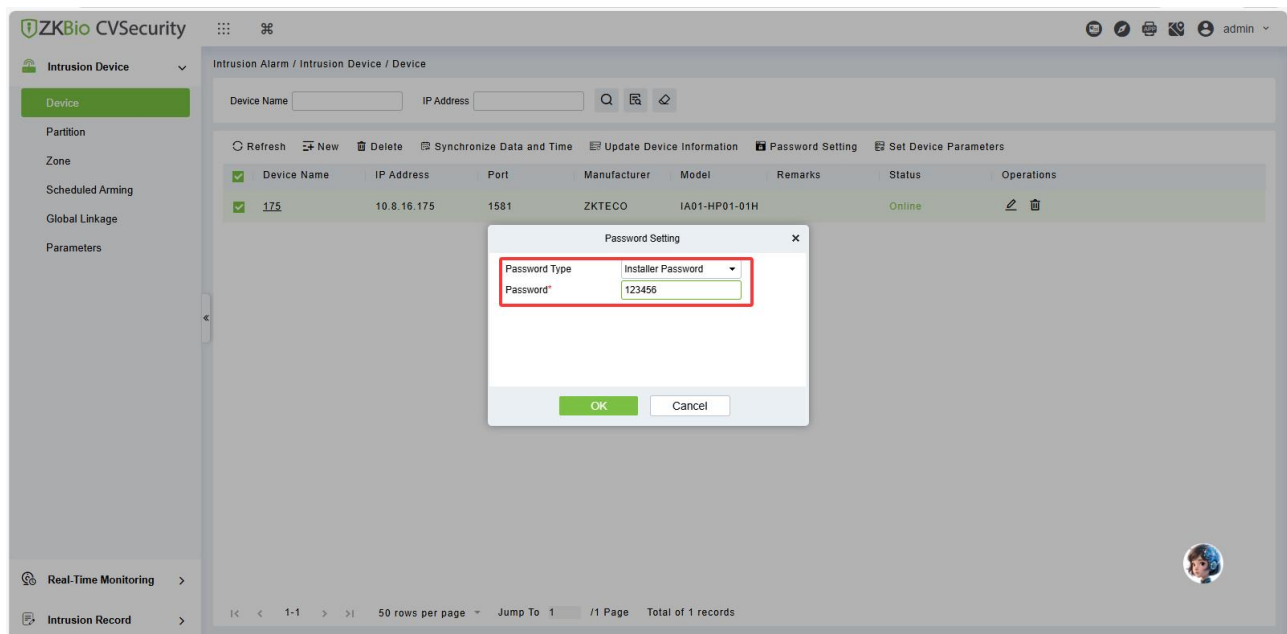
13. Intrusion Alarm

13.1. Intrusion Device – Device Management: Support password update function.

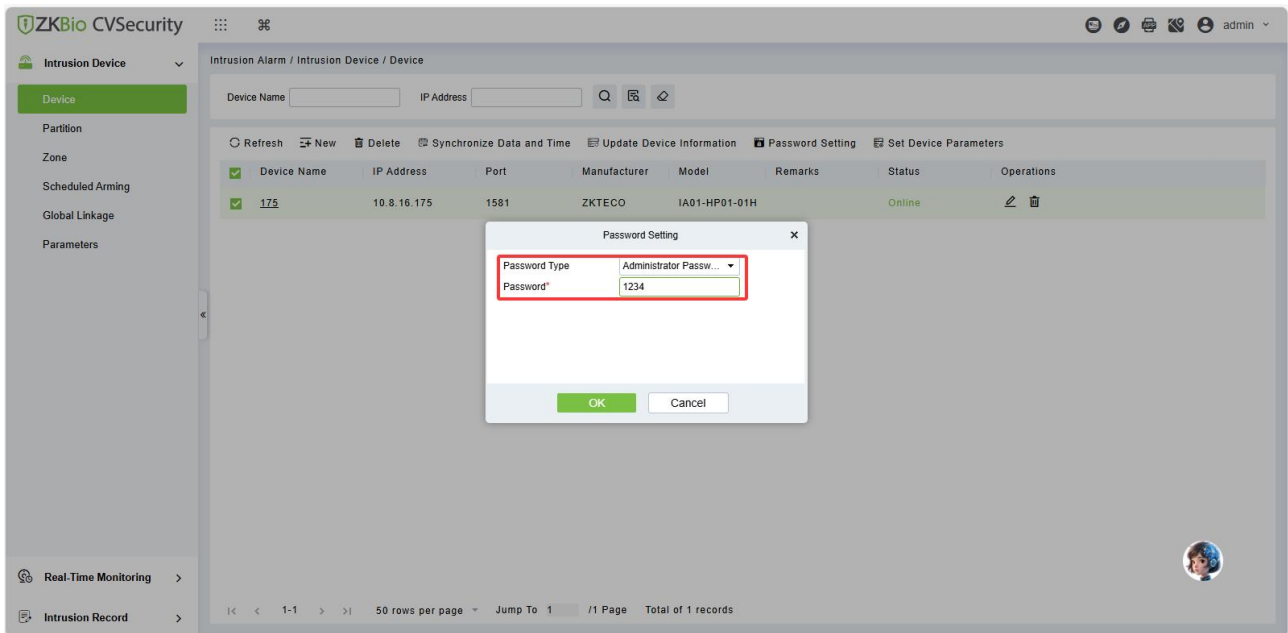
Navigate to "Intrusion Alarm / Intrusion Device / Device" and open Password Settings to update the password of the intrusion alarm host. Three types of passwords are available for modification; it is recommended not to reuse the same password across the three categories.



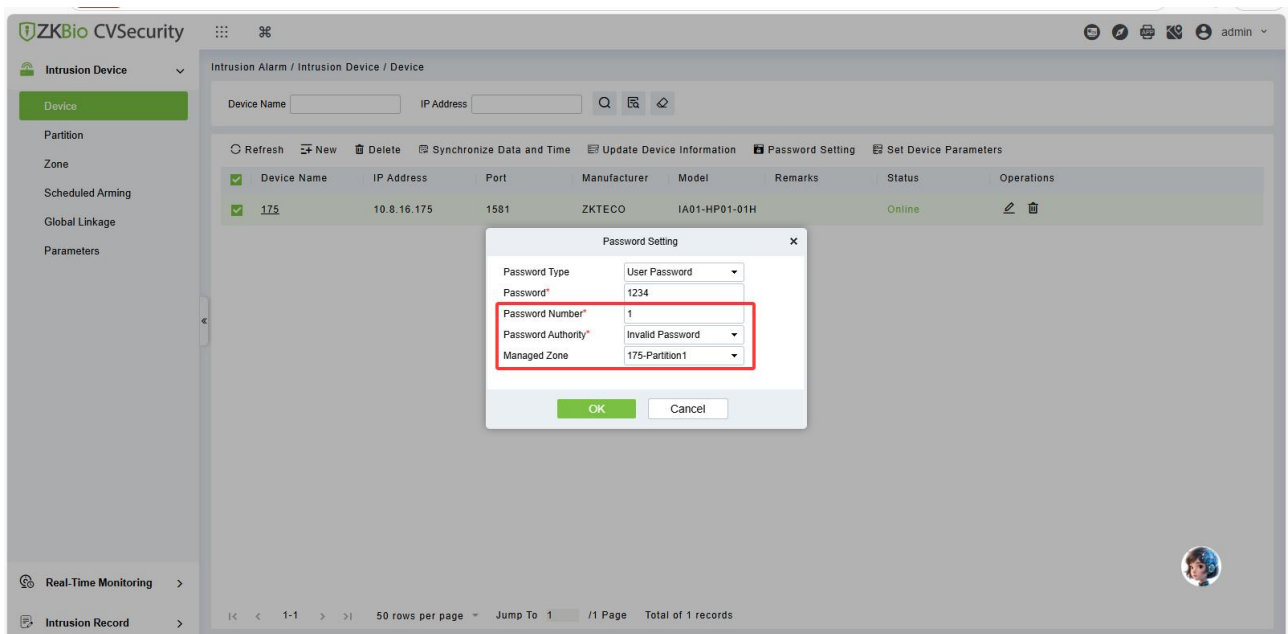
- Installer Password Limited to 6 digits only. Enter the password in the input box and click OK to save changes.



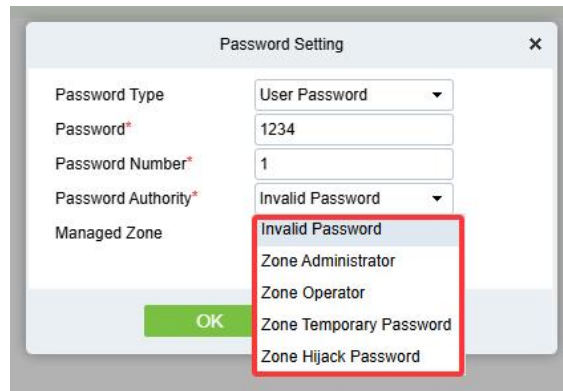
- Administrator Password Length range: 4–6 digits. Input the password and click OK to apply modifications.



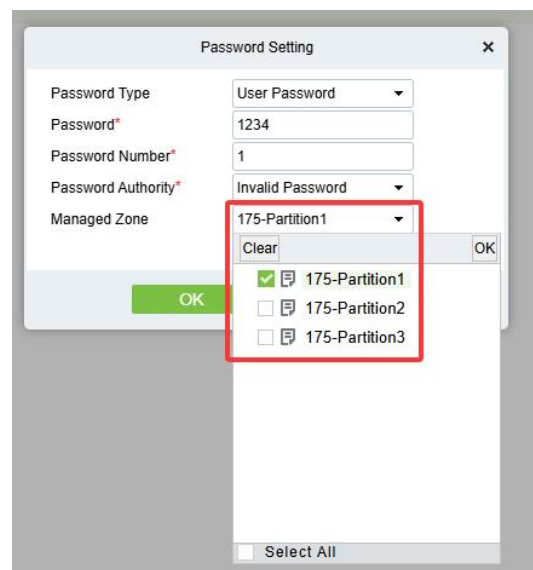
- User Password Length range: 4–6 digits. Fill in the new password, password serial number, user permission level, and zones managed by the corresponding user serial number, then click Confirm to complete the update.



Five permission levels are available for user passwords.

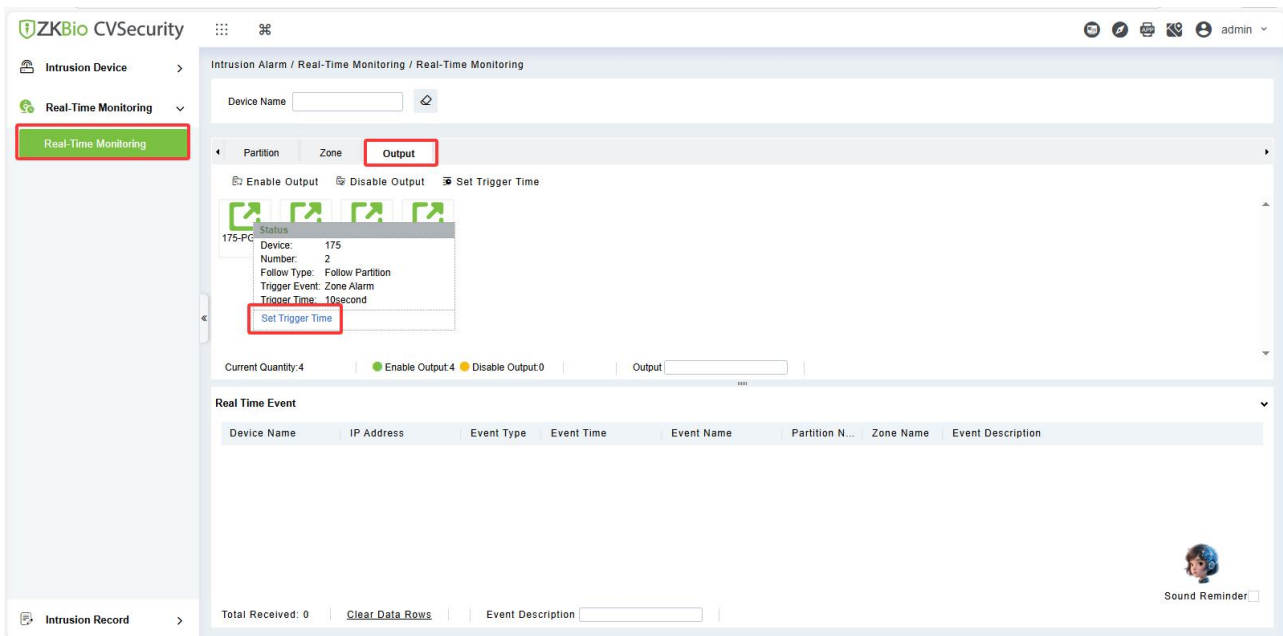


Managed zones for user passwords support single selection or multiple selections based on actual requirements.



13.2. Relay Output Management

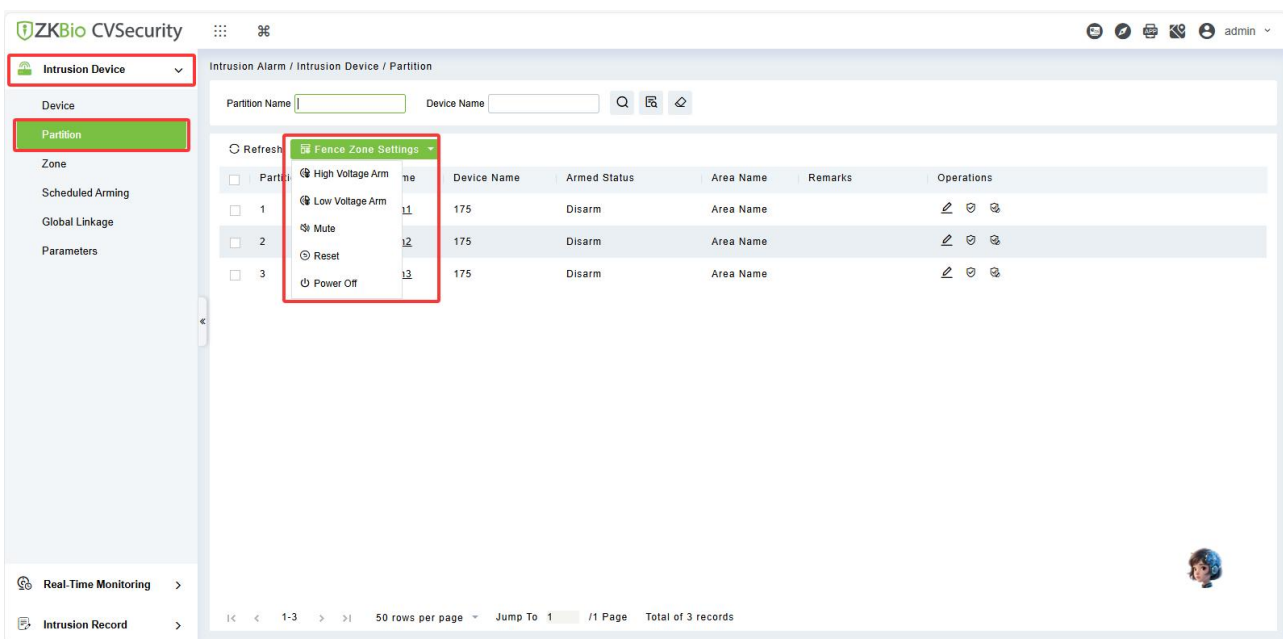
Navigate to "Intrusion Alarm / Real-time Monitoring / Real-time Monitoring" and switch to the Output tab. Select the target relay output port to configure its trigger duration, and perform operations to activate or deactivate the output.



13.3. Intrusion Devices – Partition: Add perimeter fence sub-menu.

- Zone, detector zone and bypass functions follow mainstream industry standards.

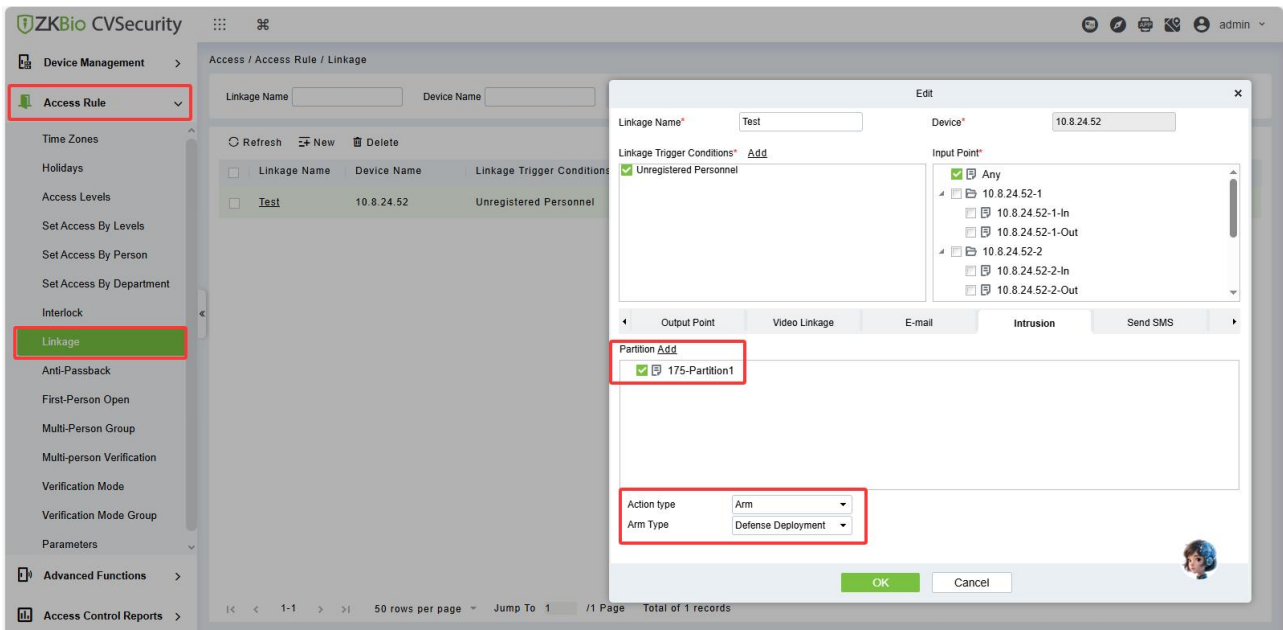
Navigate to "Intrusion Alarm / Intrusion Device / Partition" and open the Perimeter Fence submenu. Operate high-voltage arming, low-voltage arming, mute, reset and power-off for fence zones on this page.



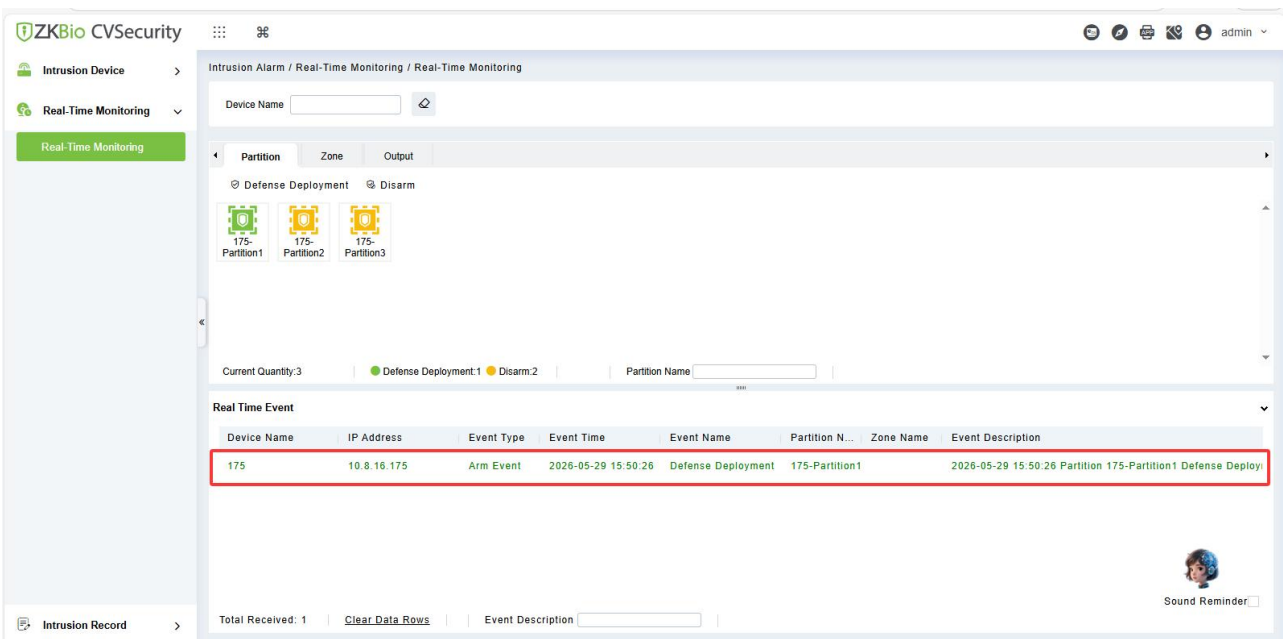
13.4. Real-time Monitoring – Interface supports display of linked alarm events.

- Example scenario: Access control validates abnormal swiping and triggers automatic arming of intrusion alarm zones.

Navigate to "Access Control / Access Rule / Linkage", create a new linkage task to automatically arm the zone when an unregistered person swipes a card.

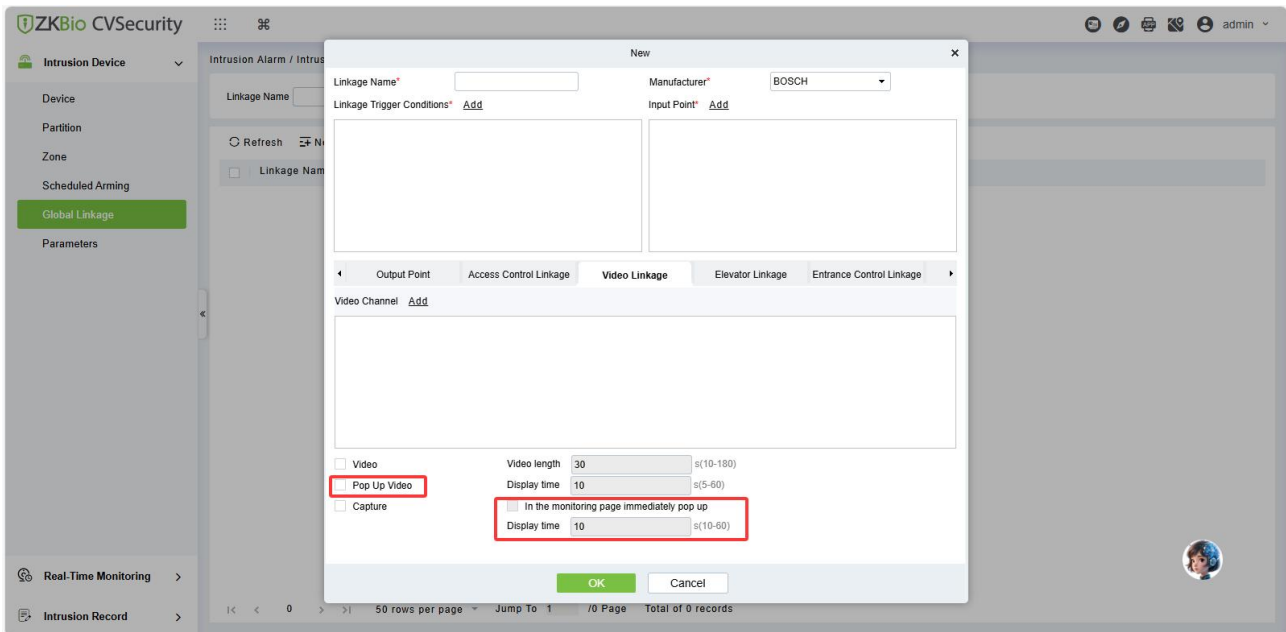


Go to "Intrusion Alarm / Real-Time Monitoring / Real-Time Monitoring", all triggered linked alarm events will be displayed on the interface.



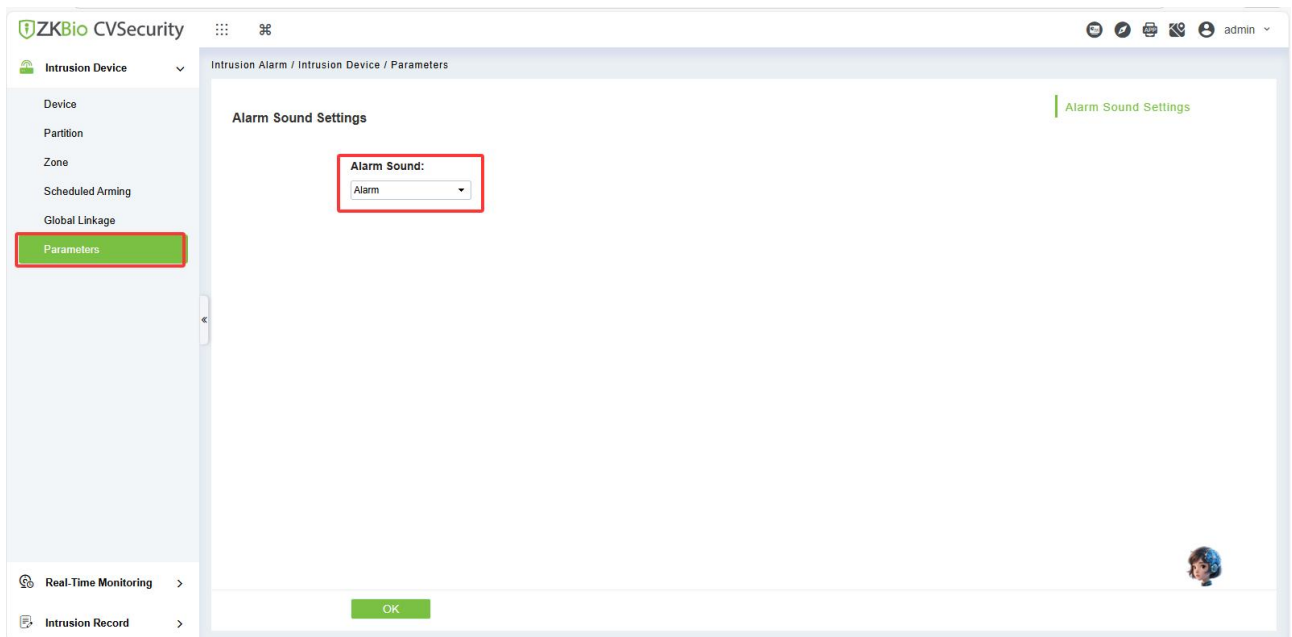
13.5. Intrusion Device – Global Linkage: Add Pop-up video and display duration settings in video linkage module.

Navigate to "Intrusion Alarm / Intrusion Device / Global Linkage" to configure pop-up video display and the video playback duration.



13.6. Intrusion Device / Parameters: New alarm sound configuration function.

Navigate to "Intrusion Alarm / Intrusion Device / Parameters" and enter the Alarm Sound subpage to customize alarm audio.



14. Service Center

14.1. Scene Center - Target Recognition: New structured fields – Hair & Hat (Supported Device: ZKIVA Edge X1).

Navigate to "Service Center / Scene Center / Scene Configuration", select Target Recognition to enter the corresponding scenario page. Two new filter fields Hair and Hat are added to the search bar, selectable via drop-down menus.

- Hair options:

Unlimited, Unknown, Crew Cut, Middle Part, Side Part, Front Baldness, Nape Baldness, Complete Baldness, Curly Hair, Wavy Hair, Braid, Updo, Shoulder-length Hair, Short Hair, Long Hair

- Hat options:

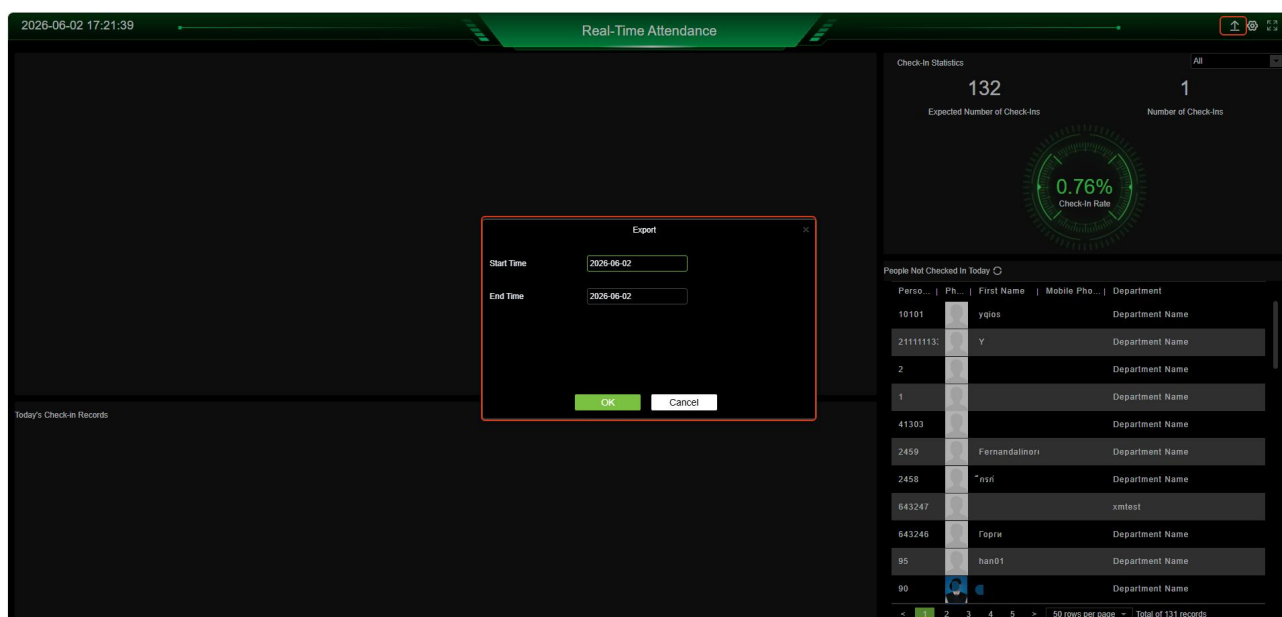
Unlimited, Wearing Hat, No Hat, Unknown

The screenshot displays the 'Target Recognition' interface. On the left, there's a 'Total Quantity' section with a list of camera names and their counts. The main area shows four camera feeds. On the right, there's a 'Target Search' panel with fields for Personnel ID, Name, Gender, Glasses, Mask, Start Time, End Time, and Channel. It also includes a 'Picture' upload button and a 'Threshold' slider. Below the search panel is a 'Movement Report' table with columns for Person ID, First Name, Event Time, Area, Event, Snapshot, and Event Name. The table lists several events, including 'Target Allowlist Alert' and 'Target Recognition Alert'. At the bottom, there's a 'Select Target Recognition Device' dropdown and three buttons labeled 'Allowed List', 'Strangers', and 'Forbidden List'.

Person...	First Na...	Event Time	Area	Event ...	Snapshot	Event Name
3180035		2026-06-02 16:07:37	8	8F		Target Allowlist Alert
	Stranger	2026-06-02 15:44:55	8	8F		Target Recognition Alert
	Stranger	2026-06-02 14:22:47	8	8F		Target Recognition Alert
3180035		2026-06-02 14:12:44	8	8F		Target Allowlist Alert
3180035		2026-06-02 12:25:22	8	8F		Target Allowlist Alert
3180035		2026-06-02 12:19:08	8	8F		Target Allowlist Alert
	Stranger	2026-06-02 11:57:04	8	8F		Target Recognition Alert
3180035		2026-06-02 10:51:13	8	8F		Target Allowlist Alert
	Stranger	2026-06-02 10:49:12	8	8F		Target Recognition Alert

14.2. Scene Center - Real-Time Attendance: Support one-click report export.

Navigate to "Service Center / Scene Center / Scene Configuration", select Real-Time Attendance to enter the scenario page. A new one-click report export function is added; users only need to select the start and end time to export the report.



Report details are as follows:

Personnel ID	First Name	Last Name	Department Name	Record Date	Record Counts	Earliest Time	Latest Time
12	gyfghuddg		Department Name	2026-05-29	4	09:52:20	10:08:50
2831			Department Name	2026-05-29	1	06:52:00	06:52:00
888	DLFX	est hanks	Department Name	2026-05-29	1	16:01:00	16:01:00
12	gyfghuddg		Department Name	2026-05-28	1	10:39:44	10:39:44
467	ug		Department Name	2026-05-28	1	16:31:00	16:31:00
28262	28262		Department Name	2026-05-28	1	04:17:00	04:17:00
556	Tg		Department Name	2026-05-28	4	00:00:00	23:59:00
28261	28261		Department Name	2026-05-28	1	16:00:00	16:00:00
28260	38260		Department Name	2026-05-28	1	17:00:00	17:00:00
28259	28259		Department Name	2026-05-28	1	19:00:00	19:00:00
2651			Department Name	2026-05-27	1	00:00:00	00:00:00
12	gyfghuddg		Department Name	2026-05-26	5	11:23:40	11:35:26
2831			Department Name	2026-05-26	1	21:53:00	21:53:00
12	gyfghuddg		Department Name	2026-05-25	3	09:26:00	10:16:21
2831			Department Name	2026-05-25	2	06:56:00	09:00:00
12	gyfghuddg		Department Name	2026-05-22	4	15:51:13	17:15:50
12	gyfghuddg		Department Name	2026-05-20	1	10:48:02	10:48:02
12	gyfghuddg		Department Name	2026-05-19	6	09:50:42	18:13:18
12	gyfghuddg		Department Name	2026-05-18	2	17:49:58	18:27:37
12	gyfghuddg		Department Name	2026-05-18	1	17:28:16	17:28:16

14.3. Scene Center - Personnel Count

- New statistics display panel to show real-time inbound and outbound personnel counts



- Support query and export of daily, weekly and monthly reports

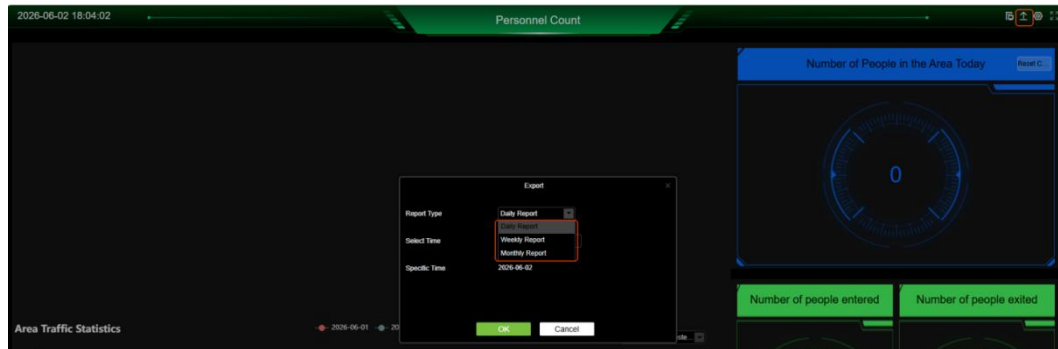
- Query Function

Available time range options: Compare with Yesterday, Last 3 Days, Last 7 Days



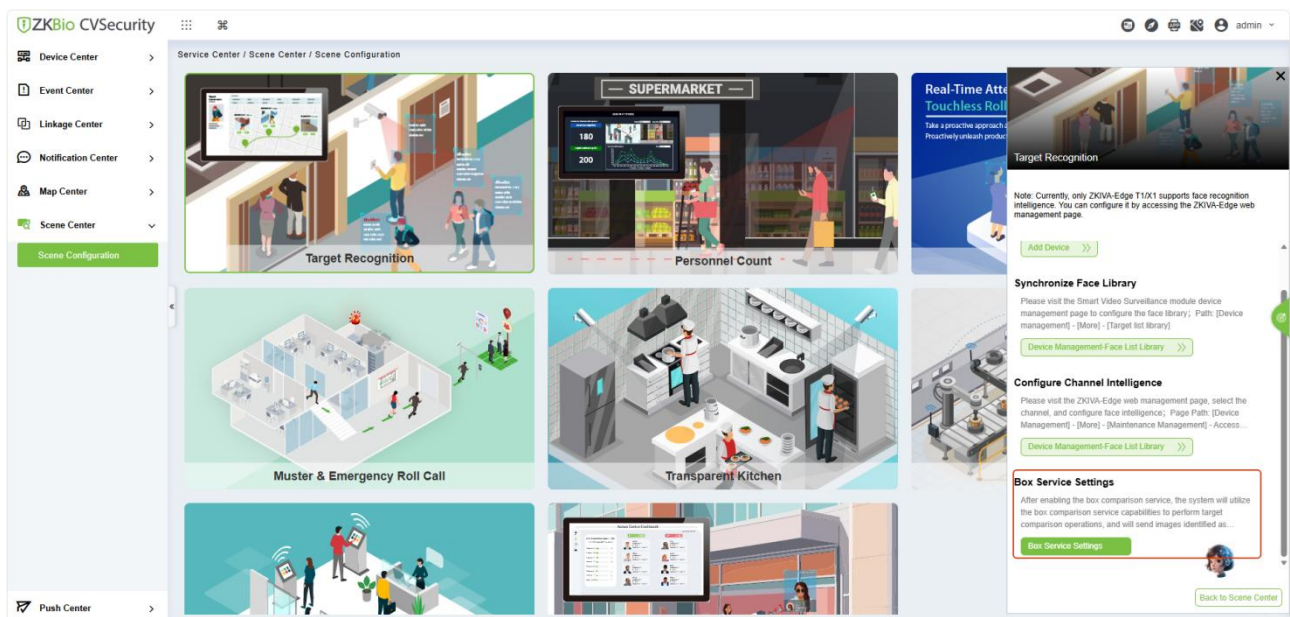
- Export Function

Supports exporting daily, weekly and monthly statistical reports



14.4. Scene Center - Target Recognition: Add box matching parameters (Parameters for shielding box service of intelligent video module).

Navigate to "Service Center / Scene Center / Scene Configuration" → Target Recognition, then click "Configure Scenarios - Box Service Settings".



Users can enable the recognition service. After turning on the box matching service, the system relies on the computing capability of the box service to complete target matching calculations. Images judged as strangers will be sent to designated recognition devices for subsequent business processing.

Box Service Settings

Box service

Whether to enable recognition service

Yes

⚠ After activation, the system will compare the capabilities of the box comparison service and send pictures of strangers to recognition devices for processing.

Box Recognition Device

X1-235

⚠ The selected device serves as the sending terminal for receiving images from strangers, while also serving as the role of performing box service capability comparison.

OK

Cancel

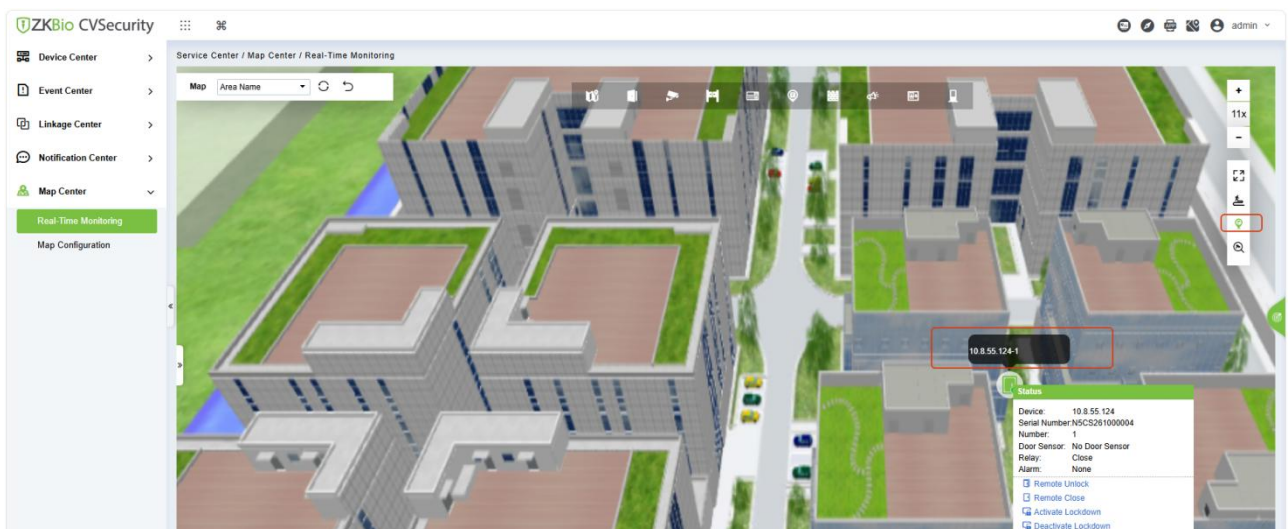
14.5. Map Center - Real-time Monitoring: Display assembly point devices on map after emergency assembly linkage trigger for quick positioning.

Navigate to "Service Center / Scene Center / Scene Configuration" - Muster & Emergency Roll Call - Emergency Roll Call Basic Configuration, assign corresponding devices as safe assembly point.

Go to "Service Center / Map Center / Real-Time Monitoring", click the Emergency Assembly Points button on the right sidebar. The map will filter and only display devices set as emergency assembly points to facilitate fast location lookup.

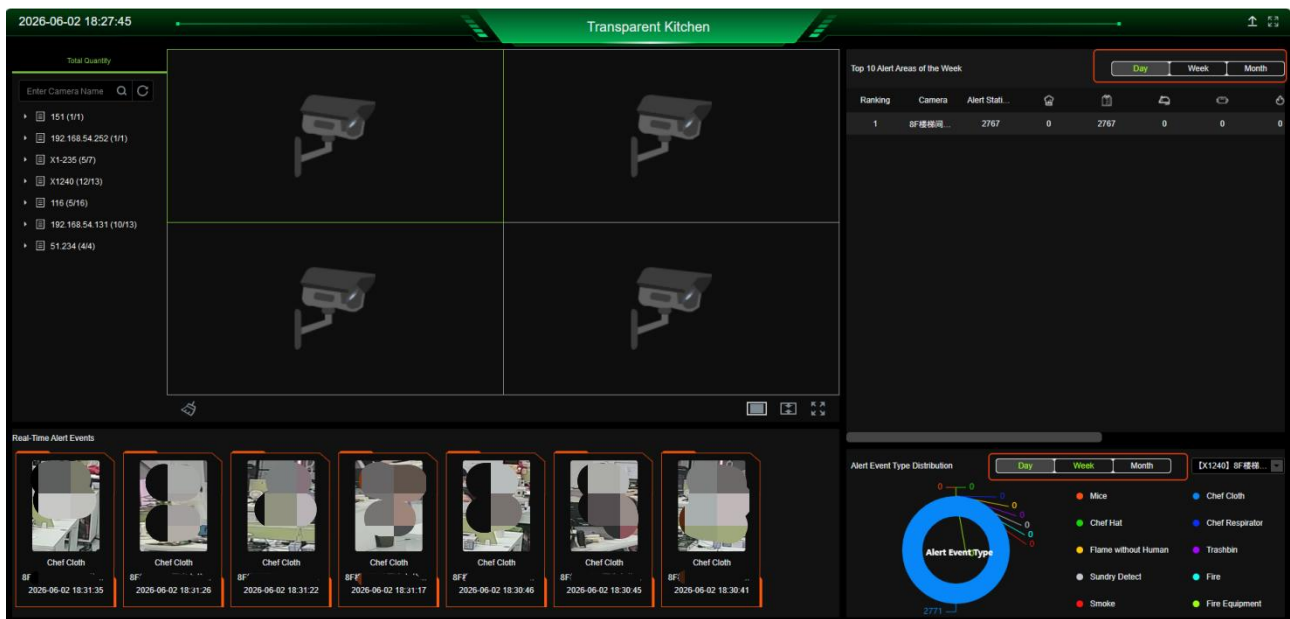


- Display mode: Show emergency assembly point devices only.



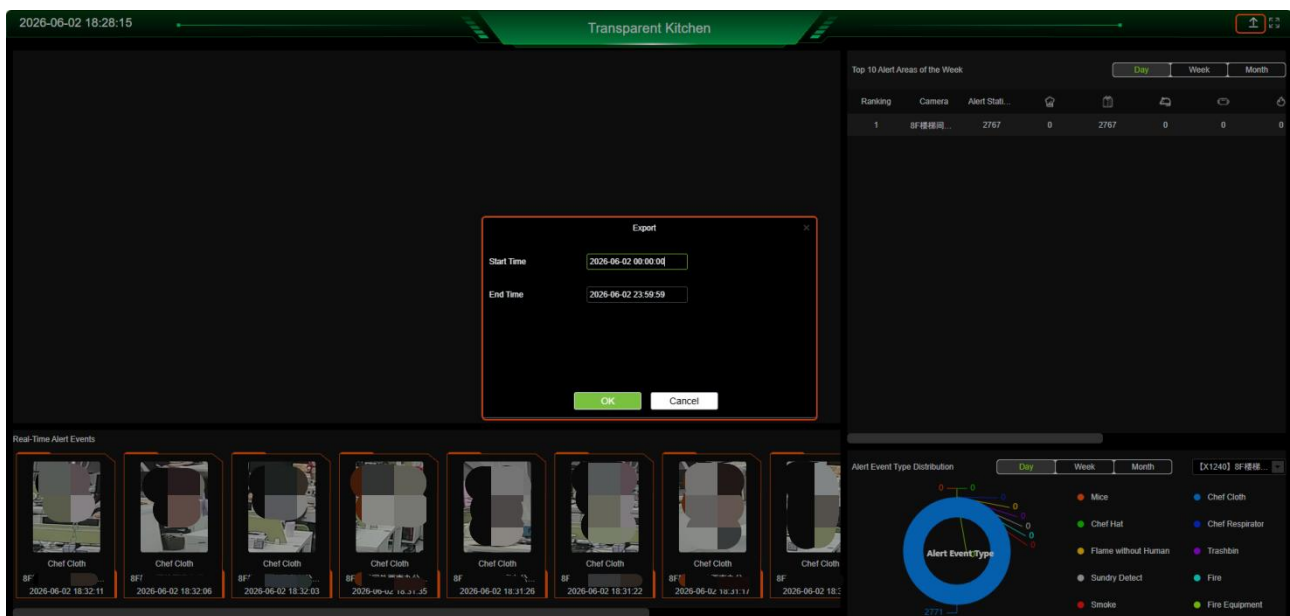
14.6. Scene Center - Transparent Kitchen: Add time dimension for statistical data, support Daily/Weekly/Monthly statistics viewing.

In the Transparent Kitchen scenario, the right-side modules "Top 10 Alert Areas of the Week" and "Alert Event Type Distribution" both support filtering statistics by day, week or month.



14.7. Scene Center - Transparent Kitchen: Add one-click statistical report export function.

A report export button is newly added in the upper right corner of the Transparent Kitchen scenario page. Users can select a time range and export statistical reports with one click.

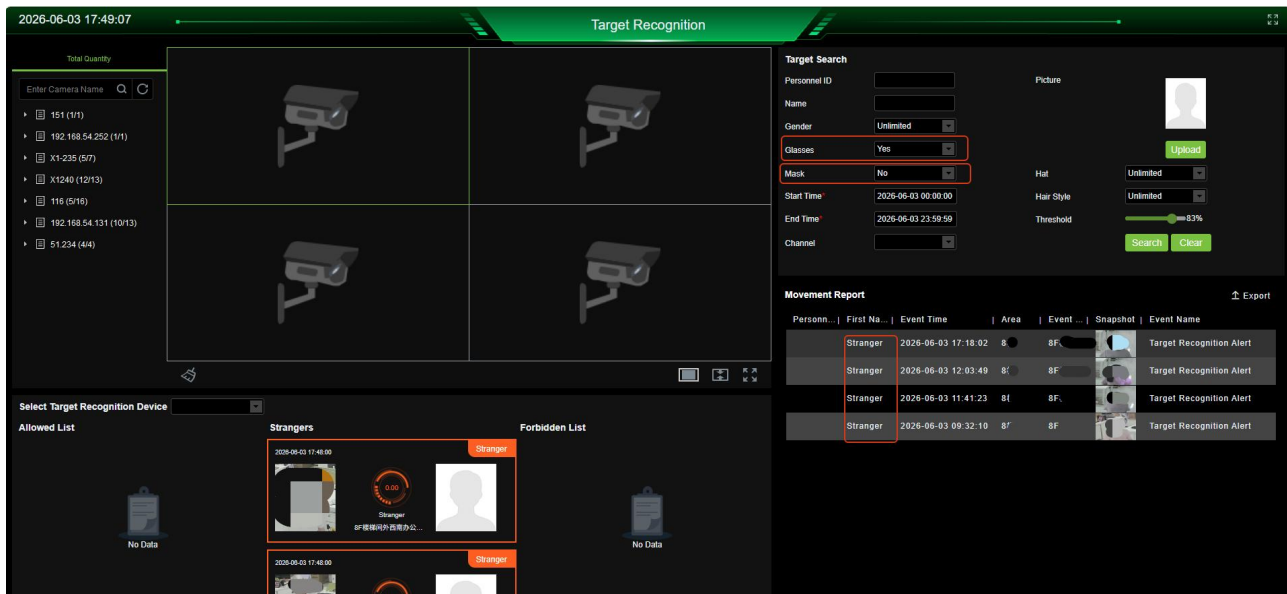


The contents of the exported statistical report are as follows:

Report on Abnormal Behaviors in Transparent Kitchens							
Event Name	Event Source	Area	Event Level	Event Time	Processing State	Processor	Processing Remark
Chef Cloth	8F	-240	8	2026-06-02 18:32:24	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:32:18	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:32:17	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:32:11	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:32:06	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:32:03	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:31:35	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:31:26	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:31:22	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:31:17	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:46	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:45	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:41	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:28	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:13	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:10	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:30:08	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:29:53	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:29:40	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:29:34	Unconfirmed		
Chef Cloth	8F	-240	8	2026-06-02 18:29:19	Unconfirmed		

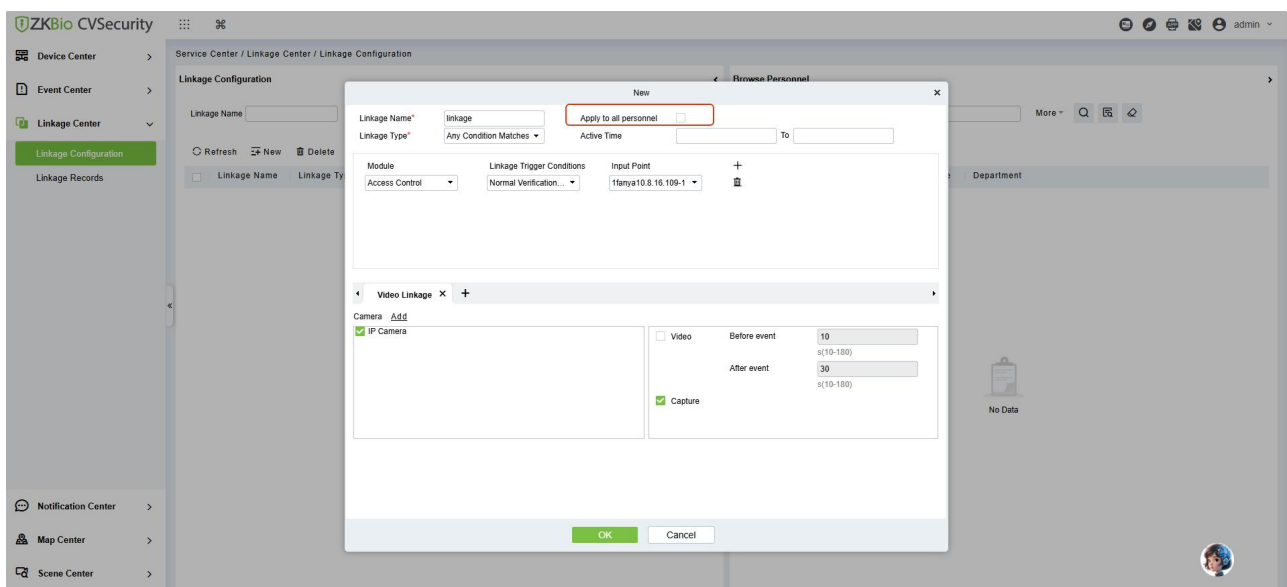
14.8. Scenario Center - Target Recognition: Search criteria not limited to allowlist and denylist personnel.

In the target recognition scenario, when searching for personnel trajectories with configured filter criteria, the search results will include strangers that match the search conditions, instead of being restricted only to personnel in the allowlist and denylist.

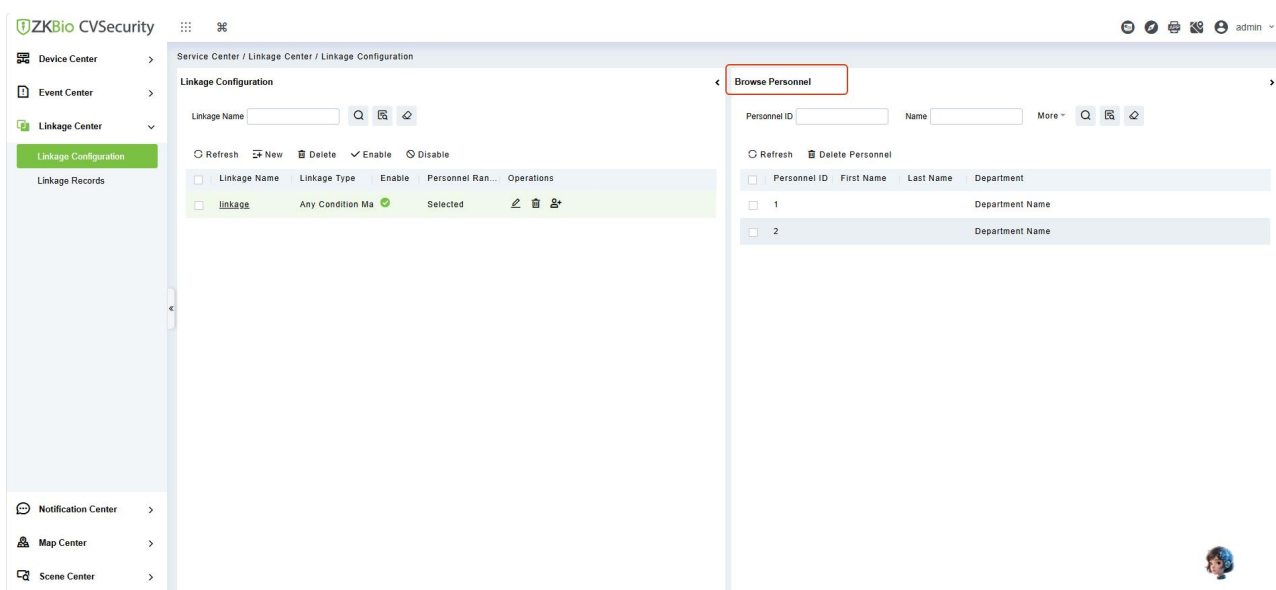
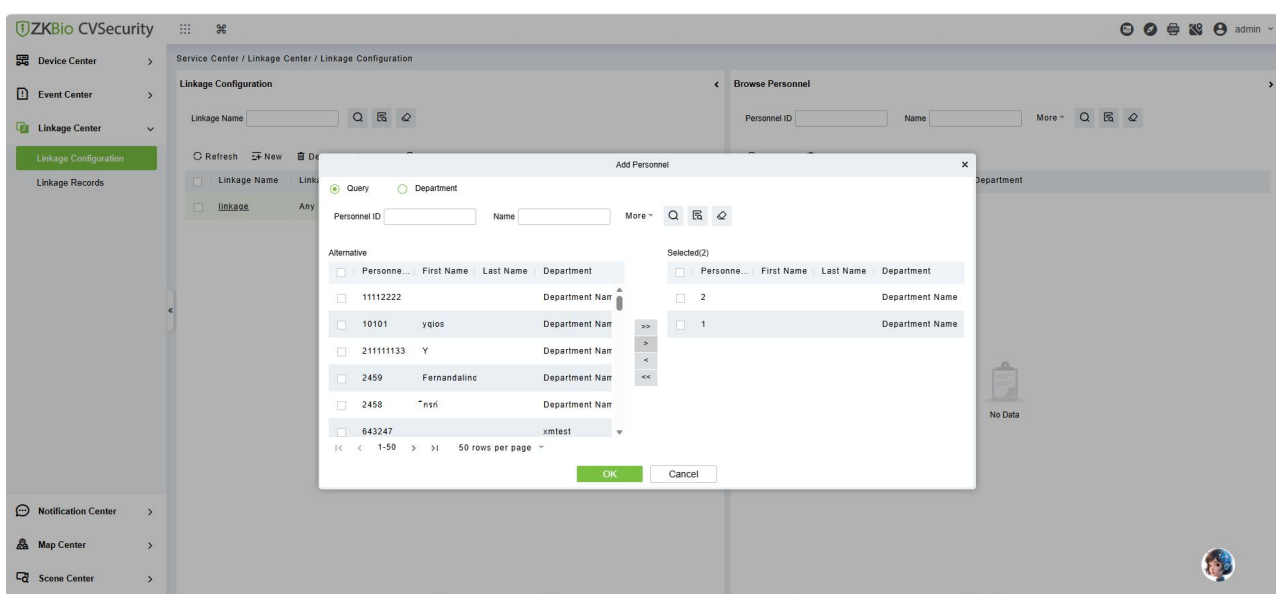
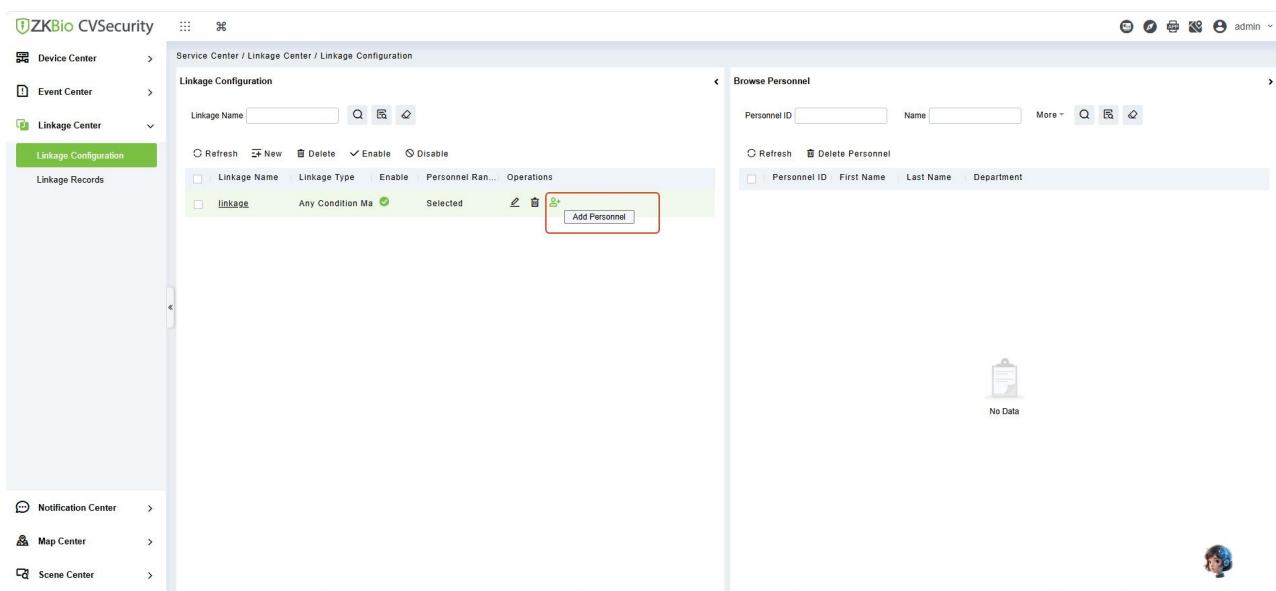


14.9. Linkage Center - Linkage Configuration: Support assigning personnel to configured linkages for differentiated linkage rules by staff.

Navigate to "Service Center / Linkage Center / Linkage Configuration". When creating or editing a linkage rule, uncheck the option "Apply to all personnel".



After finishing linkage parameter setup, click "Add Personnel" in the operation column to assign specific staff members, enabling differentiated linkage applications for different personnel.



15. System

15.1. Compliance Requirements – Optimization of custom privacy agreement function.

- Personnel Module: New privacy policy configuration entry under Personnel Management Parameters

Navigate to "Personnel / Personnel / Parameters" → Personal Information and Security Statement.

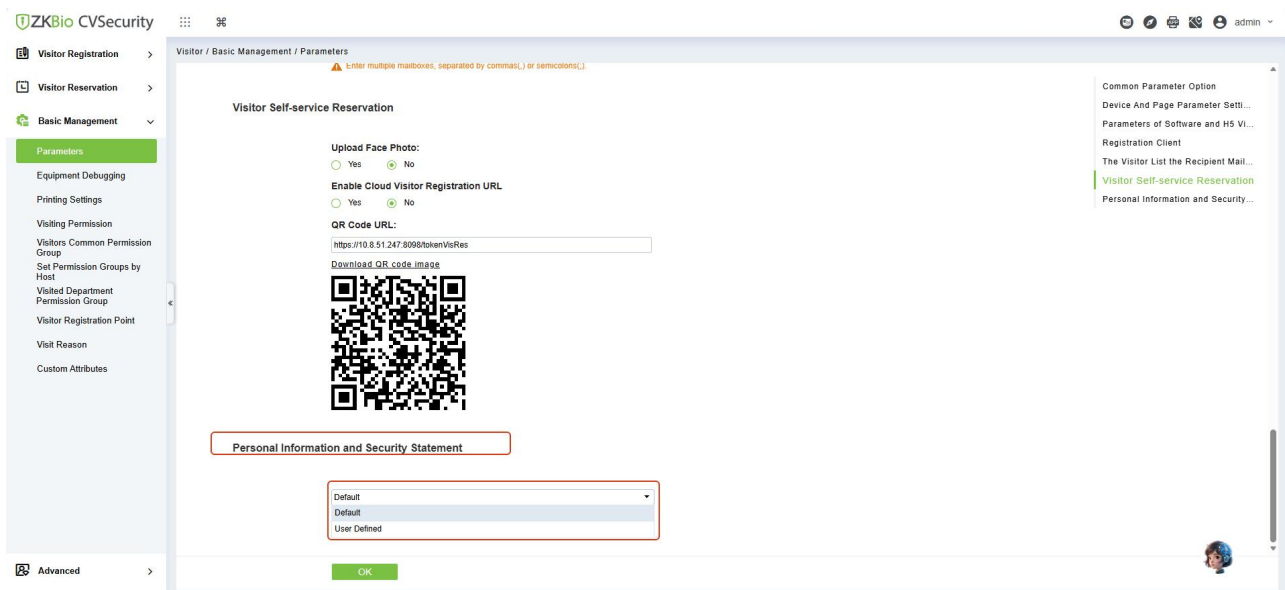
The screenshot shows the ZKBio CVSecurity web interface. The left sidebar has a 'Personnel' dropdown menu with options: Person, Department, Position, Dismissed Personnel, Pending Review, Custom Attributes, List Library, and Parameters (highlighted). The main content area is titled 'Personnel / Personnel / Parameters'. It features a 'Personal Information and Security Statement' section with a dropdown menu set to 'User Defined'. Below this is a 'Registration Client' section with 'Device Driver' and 'Certificate Recognition' status indicators. A right-hand sidebar lists various system settings, with 'Authorized Deletion Personnel' highlighted.

Select the Custom mode to import a TXT file containing self-defined privacy agreement content.

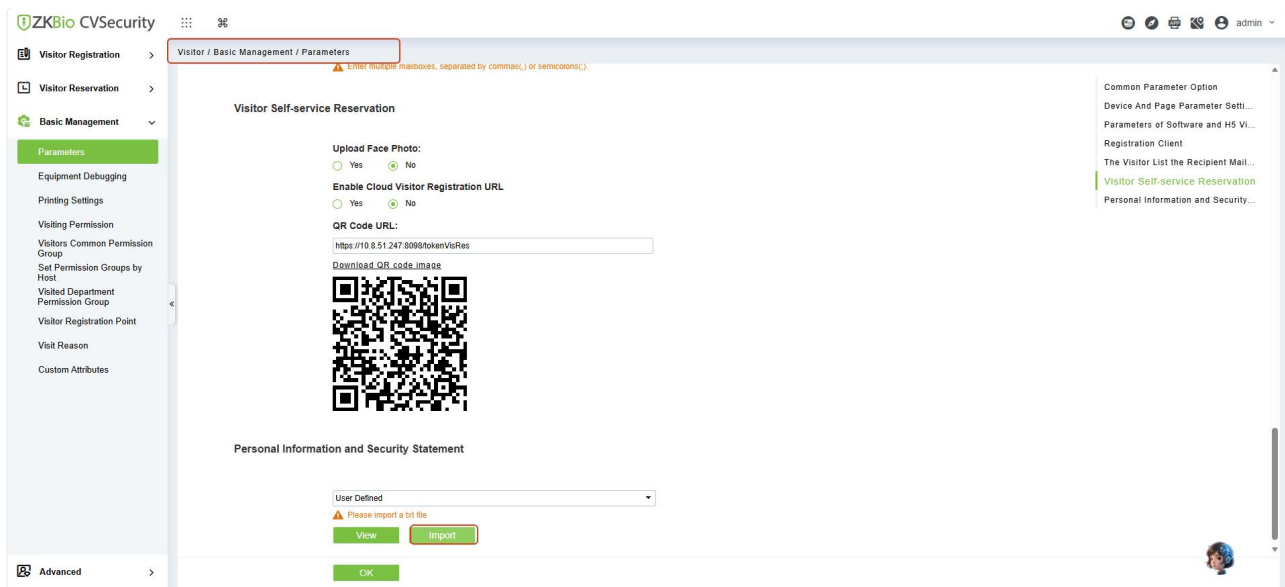
The screenshot shows the ZKBio CVSecurity web interface. The left sidebar has a 'Personnel' dropdown menu with options: Person, Department, Position, Dismissed Personnel, Pending Review, Custom Attributes, List Library, and Parameters (highlighted). The main content area is titled 'Personnel / Personnel / Parameters'. It features a 'Personal Information and Security Statement' section with a dropdown menu set to 'User Defined'. Below this is a 'Registration Client' section with 'Device Driver' and 'Certificate Recognition' status indicators. A right-hand sidebar lists various system settings, with 'Authorized Deletion Personnel' highlighted.

- Visitor Module: Independent custom privacy agreement configuration

Navigate to "Visitor / Basic Management / Parameters" → Personal Information and Security Statement.

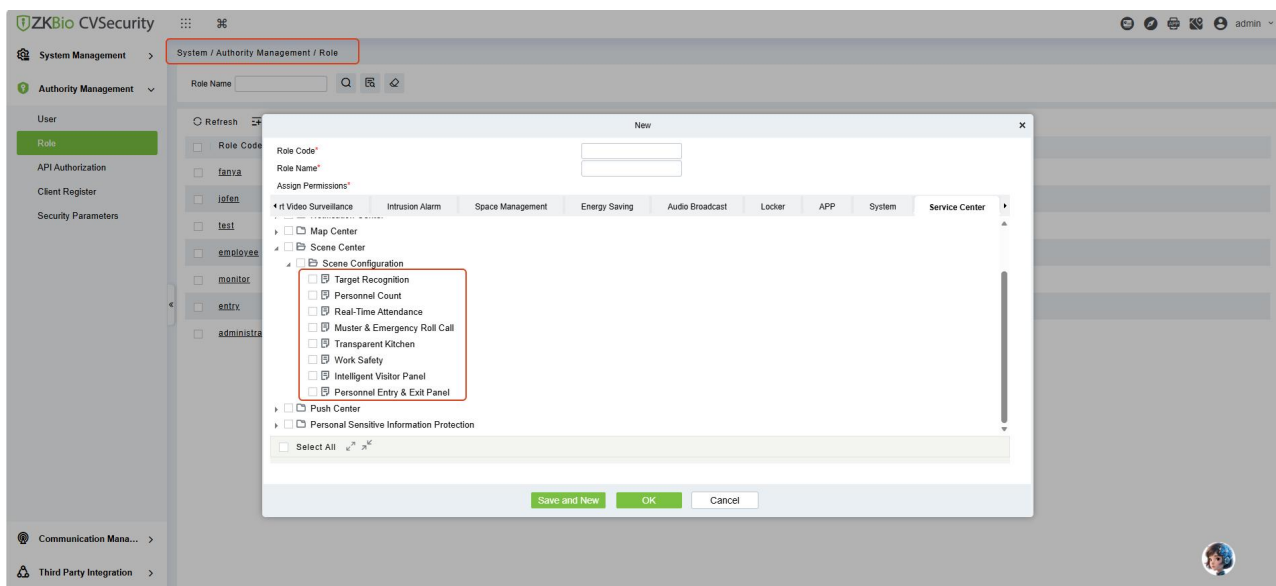


Switch to Custom mode and upload a TXT file for customized privacy terms.



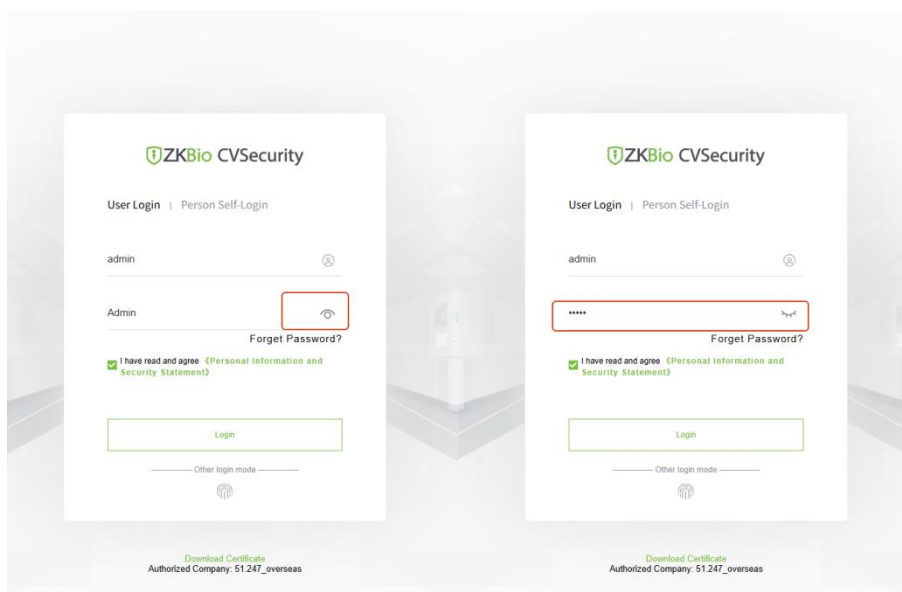
15.2. Authority Management / Role: Add permission control for each scene panel in scene center.

Navigate to "System / Authority Management / Role". Under the "Service Center - Scene Center" category, independent permission control is available for every individual scenario panel.



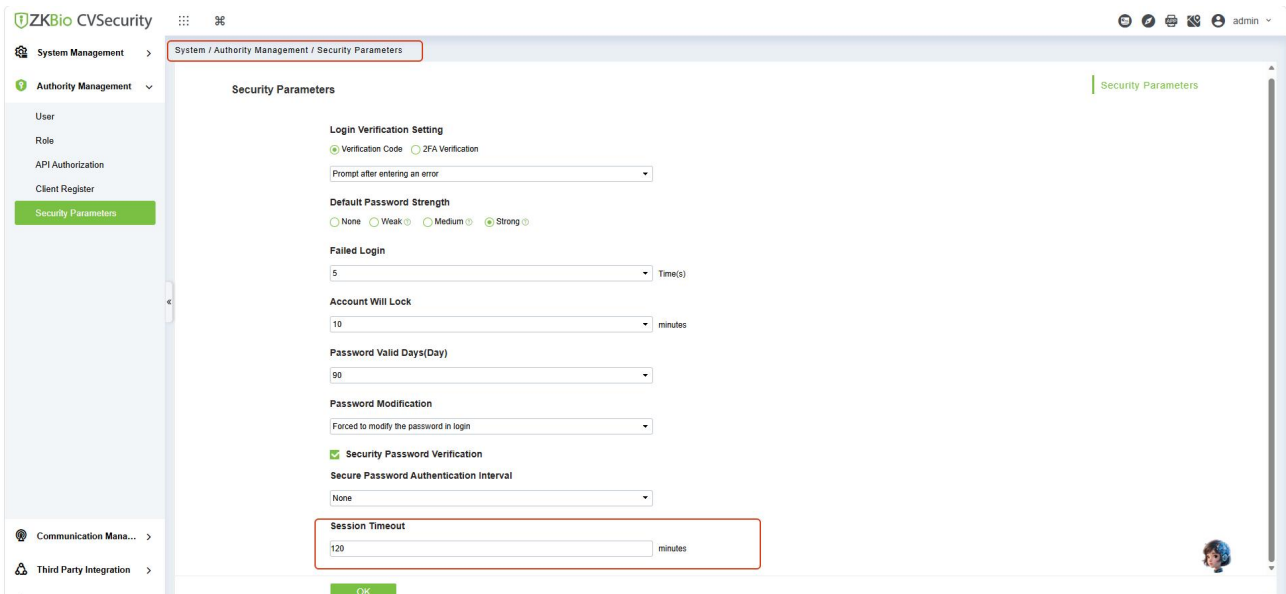
15.3. Login Password Input Optimization: Eye icon added to all password input boxes (Toggle Show/Hide Password).

An eye-shaped toggle icon is added to all password input fields across the whole platform, enabling users to display or hide entered passwords.



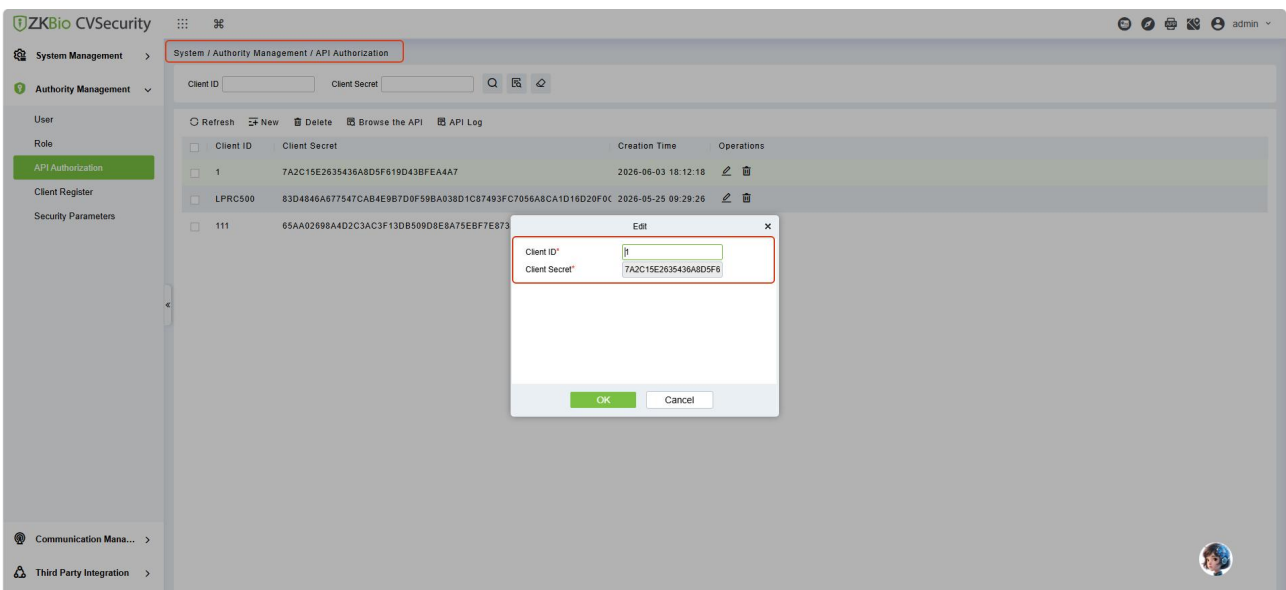
15.4. Authority Management / Security Parameters: New session timeout configuration menu with custom time limit.

Navigate to "System / Authority Management / Security Parameters". A new session timeout parameter is provided for users to customize the idle timeout duration. Once the set time expires, the browser will automatically log out the current account.

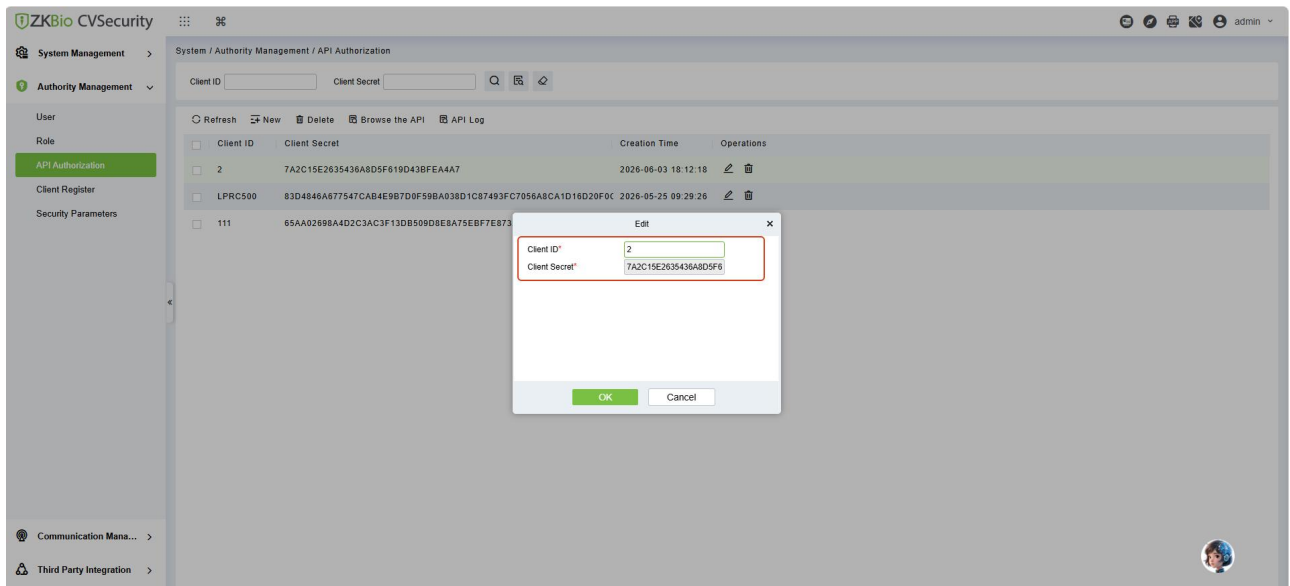


15.5. Authority Management / API Authorization: Edit client ID without modifying client secret.

Navigate to "System / Authority Management / API Authorization". Select an existing client and click Edit to modify the Client ID.

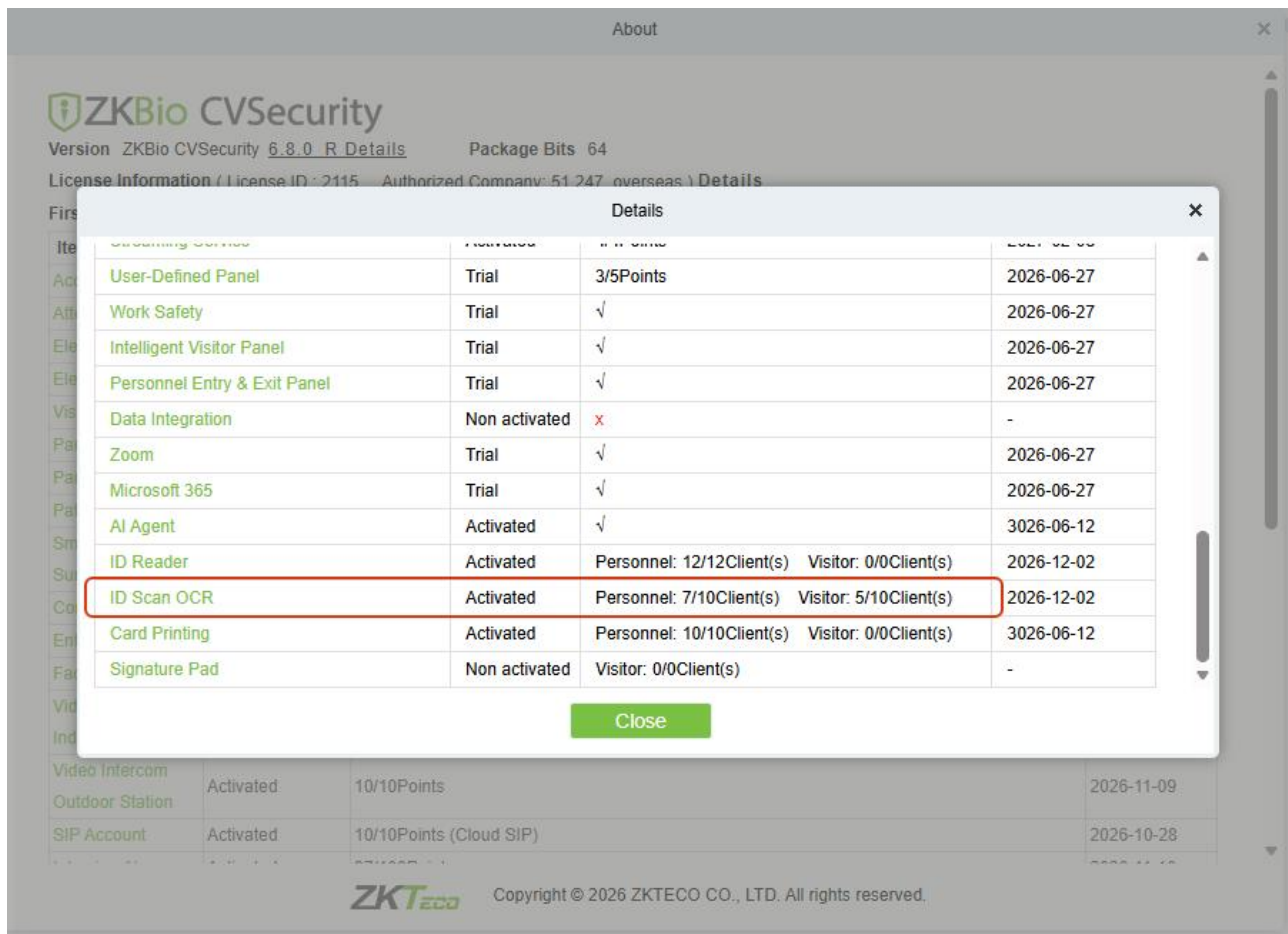


The Client Secret will remain unchanged after the Client ID update.

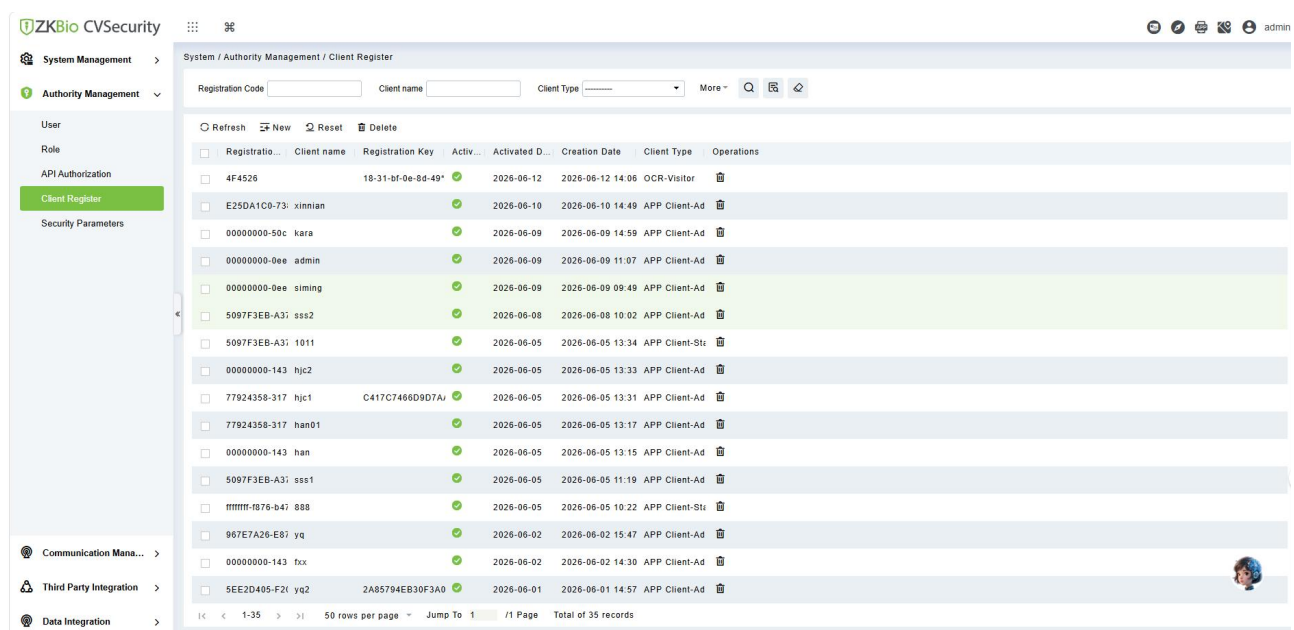


15.6. Supports reading old Indonesian KTP, new Indonesian e-KTP, Indonesian driving license.

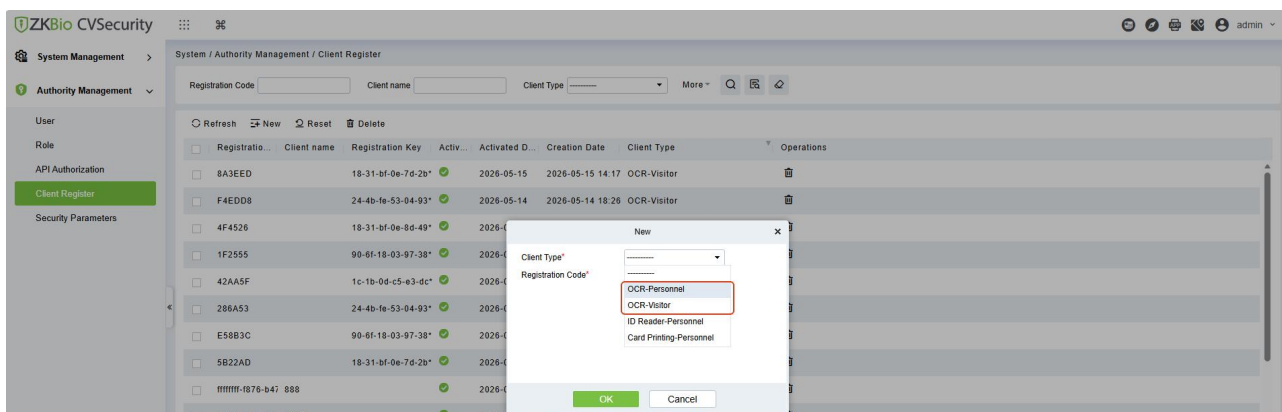
First, it is necessary to confirm that the ID Scan OCR license has been activated.



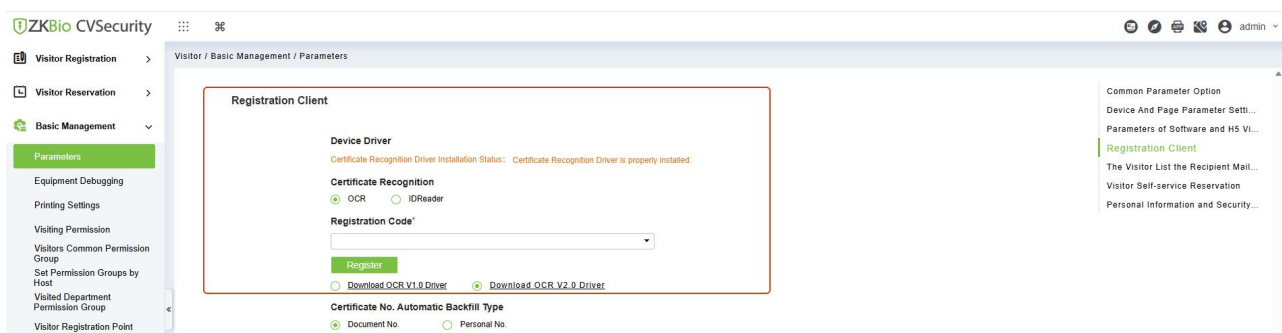
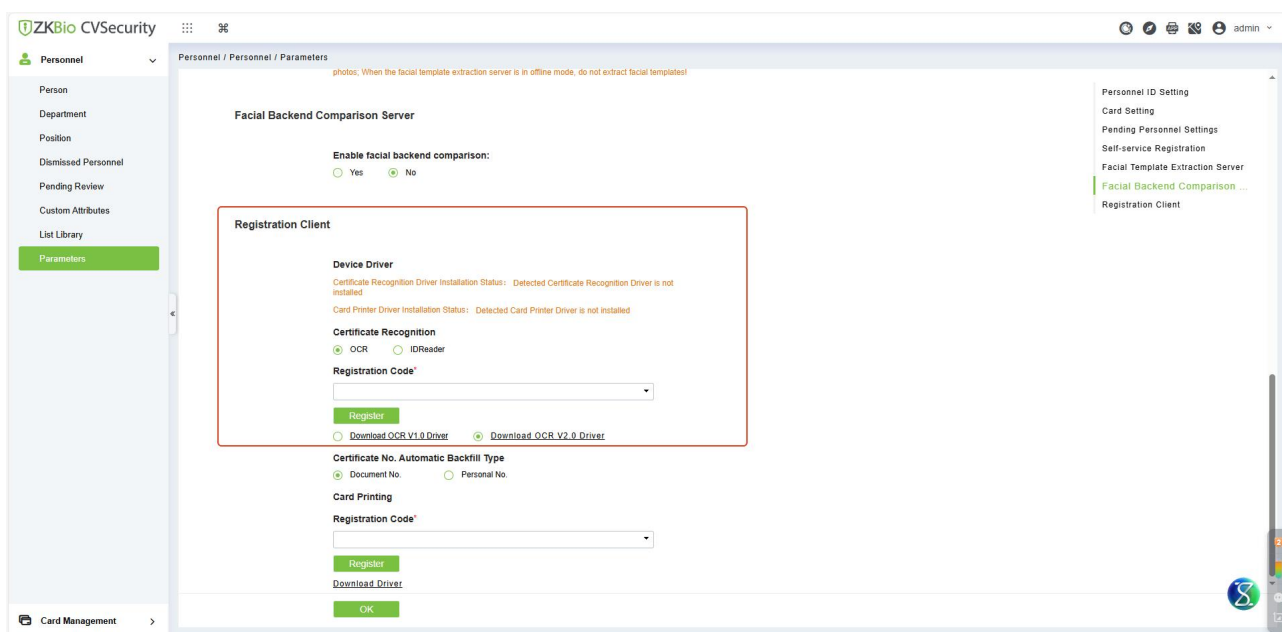
Step1: Enter System → Authority Management → Client Register, and click "New".

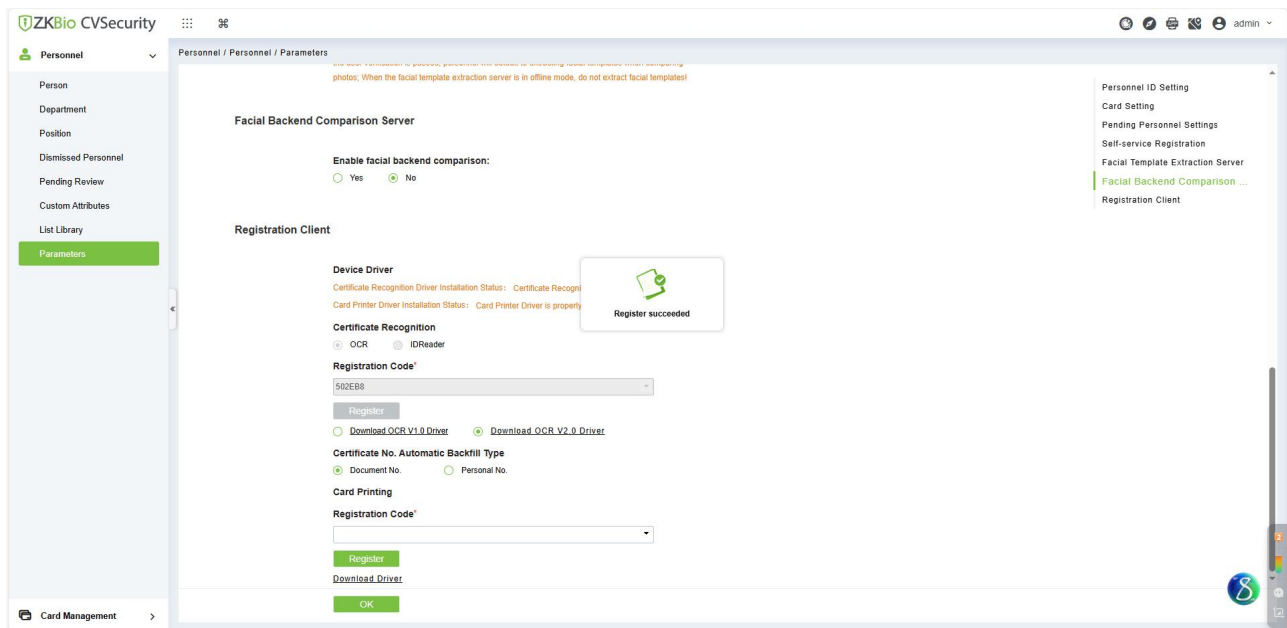


Step2: Select "OCR- Personnel" or "OCR-Visitor" as the client type, and the registration code will be generated automatically.



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





Step4: Scanning with passport scanner can automatically extract and fill in the Captured Photo, Name, Birthday and Certificate Number.

New

Visitor Contact

Enter the Query Co...

Q

Visitor Contact Department

Visit Reason

Certificate Type*

ID

FA

Certificate No.*

3674021707740003

Entering Location*

fanya

First Name*

HERYANTO HAND...

Last Name

Gender

Male

Company

Mobile Phone

License Plate

Country/Region

Visitor Quantity*

1

Items Carried

Email

Remarks

Permission

Visitor Access Level

Start Time*

2026-06-12 17:24:20

End Time*

2026-06-12 23:59:59

Default Floor

Card Number

61201813

Biometrics Type

Capture

Personnel Detail

Captured Photo

No camera connected.

Capture

Certificate Photo

No camera connected.

Capture

Select capture camera

Print Preview

Save and New

OK

Cancel

16. API Change Notice

- **Note:**

The following section serves as a summary of newly added API endpoints in ZKBio CVSecurity V6.8.0. It is a release notification to inform users of available new interfaces, and should not use as a complete API reference.

For detailed integration specification, please download the “ZKBio CVSecurity _3rd Party API_User Manual” from our official website.

All API screenshots in this section are for endpoint quick reference only.

16.1. Personnel Module: New batch Enable & Disable interfaces.

- Batch enable personnel interface

POST /api/v2/person/enabledByPins Batch Enabled Person

Implementation Notes
Enabled Person By Pins

Response Class (Status 200)
OK

Model | **Example Value**

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

- Batch disable personnel interface

POST /api/v2/person/disableByPins Batch Disable Person

Implementation Notes
Disable Person By Pins

Response Class (Status 200)
OK

Model | **Example Value**

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

16.2. Attendance Module: New return fields for /api/v2/transaction/listAttTransaction.

- If attendance record source = ACC access control device: add return field eventPointName
- If attendance record source = ATT attendance terminal: add return field attState

AttTransaction : att transaction

Show/Hide | List Operations | Expand Operations

GET /api/transaction/listAttTransaction

Get Att Transactions List

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"
}
```

Curl

```
curl -X GET --header 'Accept: application/json' 'https://10.8.51.247:8098/api/v2/transaction/listAttTransaction?pageNo=1&pageSize=1'
```

Request URL

```
https://10.8.51.247:8098/api/v2/transaction/listAttTransaction?pageNo=1&pageSize=1
```

Response Body

```
{
  "data": [
    {
      "id": "8a88b3779e6d18a1019e72c777d67726",
      "eventTime": "2026-05-29 16:08:50",
      "pin": "12",
      "name": "gyyfgghuddg",
      "lastName": null,
      "employmentType": null,
      "deptName": "Department Name",
      "areaName": "Area Name",
      "accZone": "1",
      "devSn": "YMK3241600014",
      "verifyModeName": "25",
      "eventPointName": null,
      "attPlace": null,
      "mark": "att",
      "devName": "YMK3241600014",
      "attState": "Check In"
    }
  ],
}
```

16.3. Attendance Module: New attendance point query interface.

GET /api/device/getAtt Get Att Device Info By Sn

Implementation Notes
Return Att Device Object

Response Class (Status 200)
OK

Model | Example Value

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

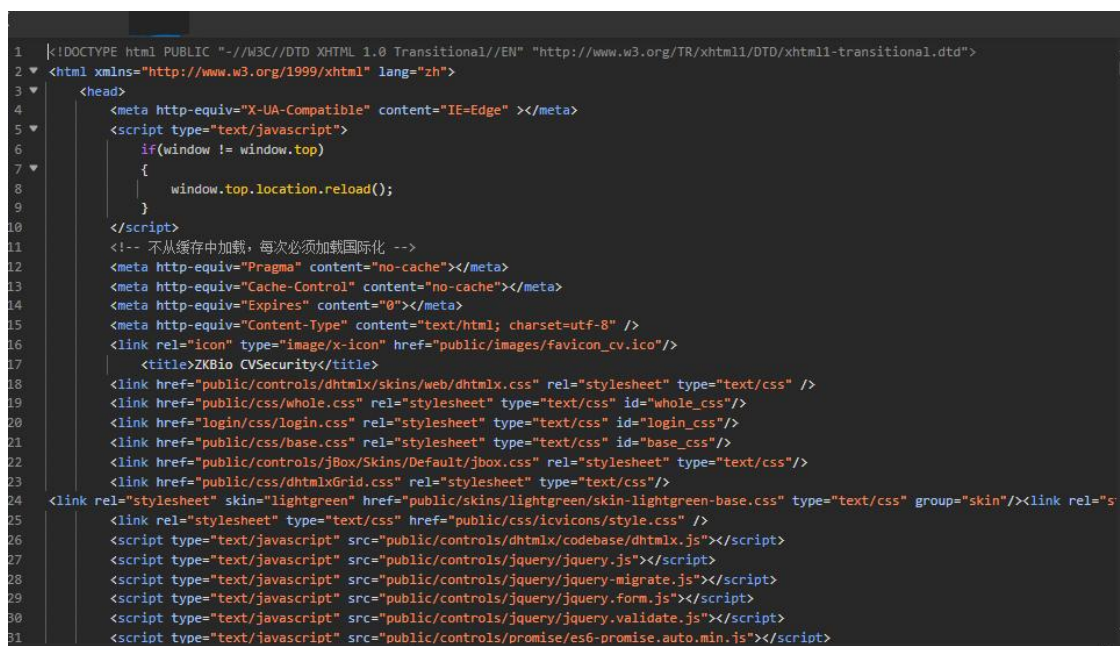
16.4. Global API Authentication Response Optimization

When authentication fails, the API returns standard JSON response instead of HTML page.

- Old



- New



16.5. Access Control: New door control API interfaces.

- Add the "Activate Lockdown" and "Deactivate Lockdown" APIs under the AccDoor API endpoint. These APIs support remote lockdown activation and deactivation via interface commands, with ByID and ByName available as filter criteria objects.

AccDoor : acc door

Show/Hide

List Operations

Expand Operations

GET	/api/door/allDoorState	Get Doors State
GET	/api/door/doorStateById	Get Door State By Id
GET	/api/door/doorStateBySn	Get Door State By Sn
GET	/api/door/get	Get Door By Id
GET	/api/door/list	Get Door List
POST	/api/door/remoteCloseById	Remote Close By Id
POST	/api/door/remoteCloseByName	Remote Close By Name
POST	/api/door/remoteLockById	Remote Lock By Id
POST	<u>/api/door/remoteLockByName</u>	Remote Lock By Name
POST	/api/door/remoteOpenById	Remote Open By Id
POST	/api/door/remoteOpenByName	Remote Open By Name
POST	/api/door/remoteUnlockById	Remote Unlock By Id
POST	<u>/api/door/remoteUnlockByName</u>	Remote Unlock By Name
GET	/api/v2/door/list	Get Door List

- Add new getter APIs named "Auxiliary Input" and "Auxiliary Output", which allow retrieving the list of auxiliary inputs and auxiliary outputs via API requests.

- Get Auxiliary Input

AccAuxIn : acc auxIn

Show/Hide

List Operations

Expand Operations

GET

/api/accAuxIn/list

Get Acc AuxIn

Implementation Notes

Return Acc AuxIn List

Response Class (Status 200)

OK

Model

Example Value

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

- Get Auxiliary Output

GET /api/accAuxOut/list Get Acc AuxOut

Implementation Notes
Return Acc AuxOut List

Response Class (Status 200)
OK

Model | Example Value

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

- Add related APIs for retrieving alarms and events. Support querying alarms and events by time period via the interfaces.

POST /api/transaction/getDoorTransactions Get Door Transactions List

Implementation Notes
Return Transactions

Response Class (Status 200)
OK

Model | Example Value

```
{
  "data": {},
  "i18nArgs": [
    {}
  ],
  "msg": "string",
  "ret": "string",
  "success": true
}
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
zkMessage	(required) Parameter content type: application/json	zkMessage	body	Model Example Value <pre>{ "activeType": "string", "appId": "string", "appKey": "string", "async": true, "content": {}, "contentId": "string", "defaultContent": "string", "listContent": [{}], }</pre>

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		

POST

/api/v2/transaction/getDoorTransactions

Get Door Transactions List

Implementation Notes

Return Transactions

Response Class (Status 200)

OK

Model

Example Value

```
{
  "data": {},
  "il8nArgs": [
    {}
  ],
  "msg": "string",
  "ret": "string",
  "success": true
}
```

Response Content Type

application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
zkMessage	(required) Parameter content type: application/json	zkMessage	body	Model Example Value

```
{
  "activeType": "string",
  "appId": "string",
  "appKey": "string",
  "async": true,
  "content": {},
  "contentId": "string",
  "defaultContent": "string",
  "listContent": [
    {}
  ],
}
```

16.6. Consumption Module: New consumption record query interface (Ticket HOC-524).

PosidTransaction : posid transaction

Show/Hide | List Operations | Expand Operations

GET

/api/transaction/listPosidTransaction

Get Posid Transactions List

Implementation Notes

Return Posid 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
endDate		endDate	query	string
pageNo	1	pageNo	query	integer
pageSize	1	pageSize	query	integer
personPin		personPin	query	string
startDate		startDate	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		

16.7. Add APIs for creating, updating and deleting areas, as well as an API to retrieve the area list.

AuthArea : auth area			Show/Hide	List Operations	Expand Operations
POST	/api/area/add	Add Area			
POST	/api/area/delete	Delete Area			
GET	/api/area/get	Get Area			
POST	/api/area/getAreaList	Get Area List			

16.8. Parking Module: Time field upgrade for /api/v2/parkPlate/addAllowDisabled.

Fields fromTime and toTime support hour + minute precisio.

POST

/api/v2/parkPlate/addAllowDisabled

Add Or Update Allow Disabled Plate

Implementation Notes

Add Or Update Allow Disabled Plate

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
carNumber	G234D	Car Number	query	string
fromTime	2026-06-02 11:38:55	yyyy-MM-dd HH:mm:ss	query	string
oldCarNumber		Original Car Number	query	string
parkCode		Parking Code	query	string
toTime	2026-06-03 11:38:55	yyyy-MM-dd HH:mm:ss	query	string
type	0	0: Allow 、 1: Disabled	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		

16.9. Parking Module: Valid white list plate query API.

Request method: GET

Path: /api/v2/parkPlate/getAllowDisabled

Request param: license plate number

Return data: plate number, valid start date, valid end date

GET

/api/v2/parkPlate/getAllowDisabled

Query Allow Disabled Plate

Implementation Notes

Query Allow Disabled Plate By CarNumber

Response Class (Status 200)

OK

Model

Example Value

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

16.10. Visitor Module: Batch Check-in & Check-out interfaces.

- Batch visitor check-in API

POST

/api/visRegistration/addVisitors

Batch Add Visitor

Implementation Notes

Batch Create Or Update Visitor

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
apiVisRegisterItemList	{required}	apiVisRegisterItemList	body	Model

Parameter content type:

application/json

Model

Example Value

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

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		

- Batch visitor check-out API

POST /api/visRegistration/exitVisitors Exit Visitors

Implementation Notes
Exit Visitors

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
visApiCertItemList	(required)	visApiCertItemList	body	Model Example Value

Parameter content type: application/json

```
[
  {
    "certNum": "1234567",
    "certType": "8"
  }
]
```

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		
401	Unauthorized		

16.11. Video Intercom: Add new APIs for personnel-associated extension number query and extension list retrieval.

- Query bound SIP account & SIP server info by login account and type (SIP domain, transport protocol etc.)

GET /api/extension/getSipAccount Get SipAccount

Implementation Notes
Get SipAccount By login name

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
loginName	(required)	loginName	query	string
loginType	(required)	loginType	query	string

Response Messages

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

[Try it out!](#)

- Fuzzy search extension list by extension number / name, returns bound device, personnel and user data.

GET /api/extension/getExtensionList Get Extension List By names And extensionNumbers

Implementation Notes
Return Extension 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
extensionNumbers		extensionNumbers	query	string
names		names	query	string
pageNo	(required)	pageNo	query	integer
pageSize	(required)	pageSize	query	integer

Response Messages

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

[Try it out!](#)

16.12. The API interface log list and query function support displaying and filtering the client secret key and requester IP address fields.

API log list page adds two filterable & displayable fields: Client secret key; Client request IP address

ZKBio CVSecurity

System Management > System / Authority Management / API Authorization

Client ID Client Secret

API Log

Time From 2026-05-08 00:00:00 To 2026-06-08 23:59:59 Request Interface Request Parameters Refract

Client Secret Request IP

Client Secret	Request IP	Request Interface	Request Parameters	Request Result	Start Date
192.168.137.2	/api/transaction/listPosidTransaction	["pageNo":"1","pageSize":"1"]	["code":"0","message":"success"]	2026-06-08 09:48:41	
192.168.137.2	/api/account/getAccount	["personPin":"1"]	["code":"0","message":"success"]	2026-06-08 09:47:01	
192.168.137.2	/api/v2/parkPlate/getAllowDisabled	["carNumber":"G234D"]	["code":"0","message":"success"]	2026-06-08 09:40:31	
192.168.137.2	/api/v2/parkPlate/getAllowDisabled	["carNumber":"G234D"]	["code":"0","message":"success"]	2026-06-08 09:39:51	
192.168.137.2	/api/v2/parkPlate/getAllowDisabled	["carNumber":"G234D","type":"0","fr"]	["code":"0","message":"success"]	2026-06-08 09:36:31	
192.168.137.2	/api/v2/transaction/listAttTransaction	["pageNo":"1","pageSize":"1"]	["code":"0","message":"success"]	2026-06-08 09:09:41	
192.168.137.2	/api/accAdvanced/getWholsinsideByZt	["code":"1"]	["code":"0","message":"success"]	2026-06-04 13:32:11	
192.168.137.2	/api/transaction/getDoorTransactions	["activeType":"string","appId":"string"]	["ret":"fail","msg":"pageNo and pageSi"]	2026-06-04 11:51:31	

4 1-31 50 rows per page Jump To 1 / 1 Page Total of 31 records

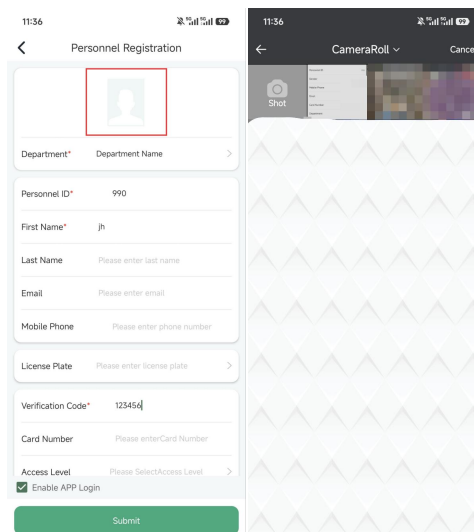
17. ZKBio Zexus Mobile Application Change Notice

- **Note:**

The following content and screenshot serve as the highlights of the new functions introduced to ZKBio Zexus mobile application. It gives you a quick overview of what's new and available for use.

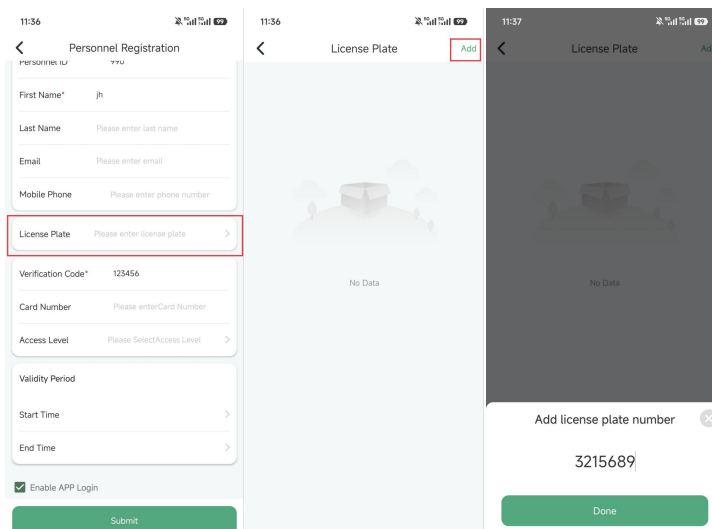
For step-by-step instructions on how to use these features, please consult the “ZKBio Zexus Mobile App_User Manual”.

17.1. Admin - Personnel Registration: Support uploading personnel avatars via mobile terminals.



17.2. Admin - Personnel Registration: Support license plate entry. Personnel - Me - Personal Information: Support license plate display.

- Admin:

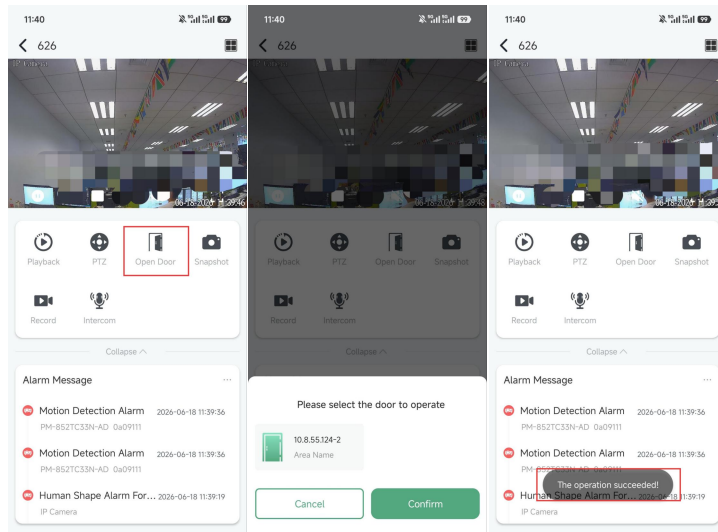


- Personnel:

17.3. Admin - Personnel Registration: Remove mandatory input restriction for the email field.

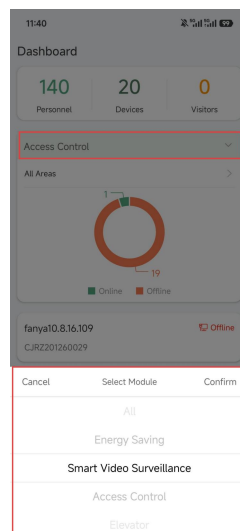
17.4. Admin - Video Monitoring: Add door opening button on the video preview page.

- Note: Before using this function, you need to go to the web portal > Access Control / Device Management / Reader to bind the camera to the corresponding door first.



17.5. Admin - Dashboard: Supports selecting to view device status of different modules via drop-down options.

- Optional options: All, Energy Saving, Smart Video Surveillance, Access Control, Elevator, Attendance, Intrusion Alarm, Parking, Entrance Control, Space Management.



18. Project Management

18.1. Add Project Management Platform

- Project Management Platform

The platform provides project protection for System Integrators (SIs), preventing one agent from snatching a project with lower prices after another agent has secured the customer project.

- Working Mechanism

Import relevant device information into the project management system to generate a dedicated project authorization file. Import this file into ZKBio CVSecurity platform to activate device restriction control for the target project.

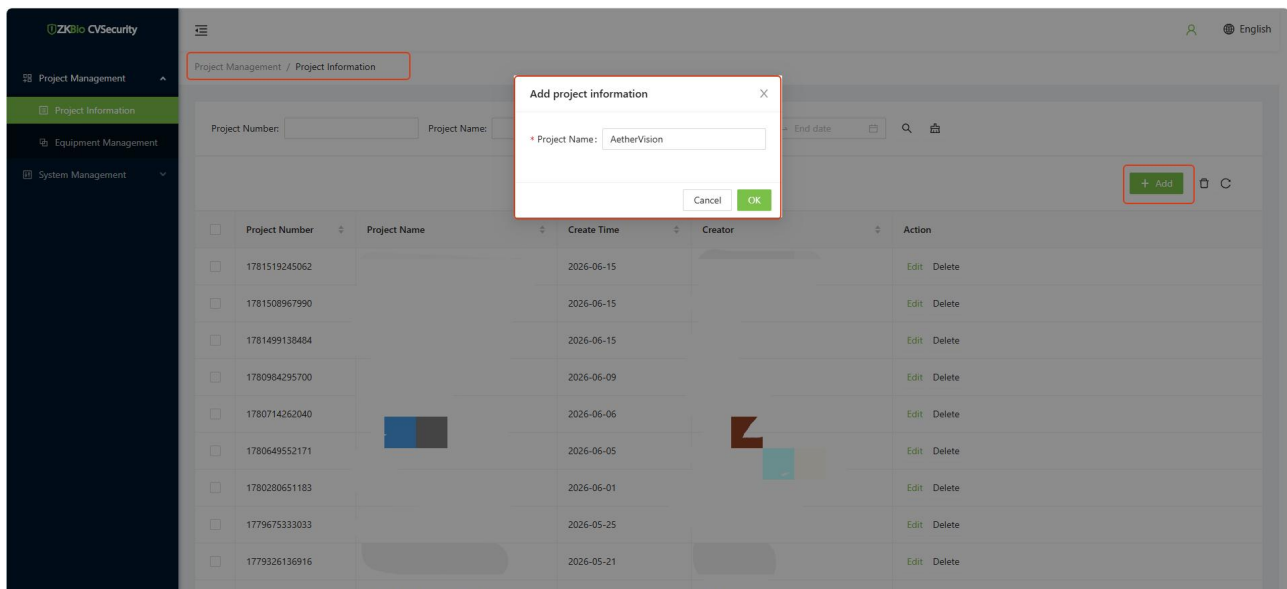
- Effect Achieved

The customer can only add devices that are listed within the imported authorization file. No other unapproved devices can be bound to this project.

- Operation Steps

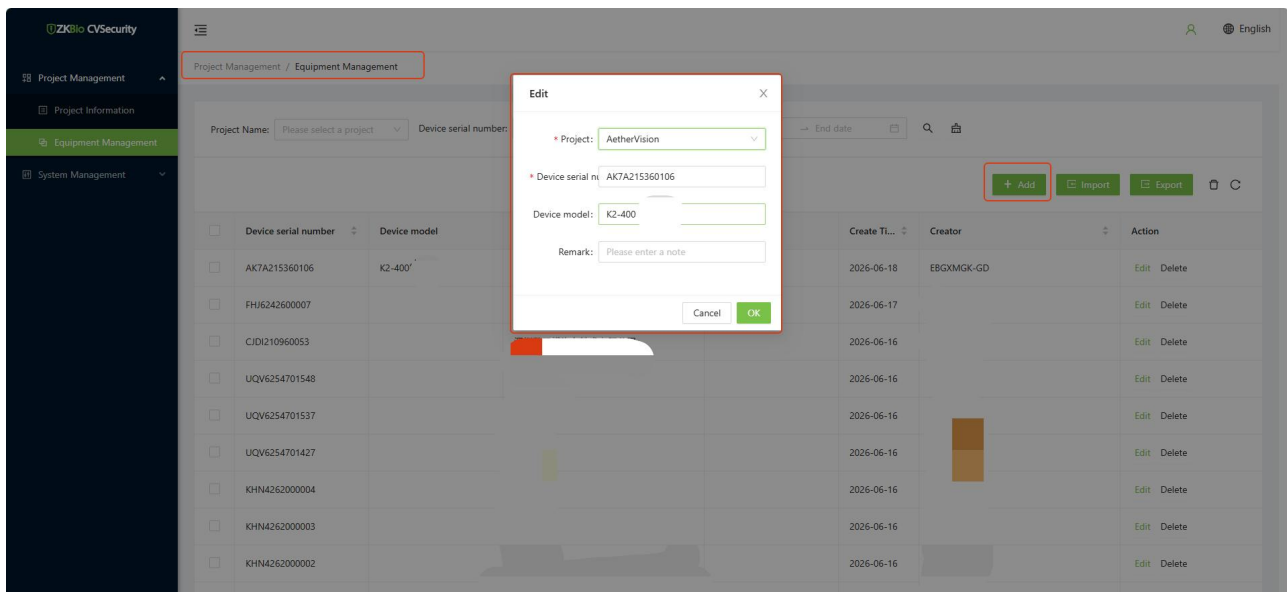
Step1:

Log in to the project control platform and navigate to "Project Management/Project Information". Click Add, enter the project name, and the system will automatically generate a project number after confirmation.

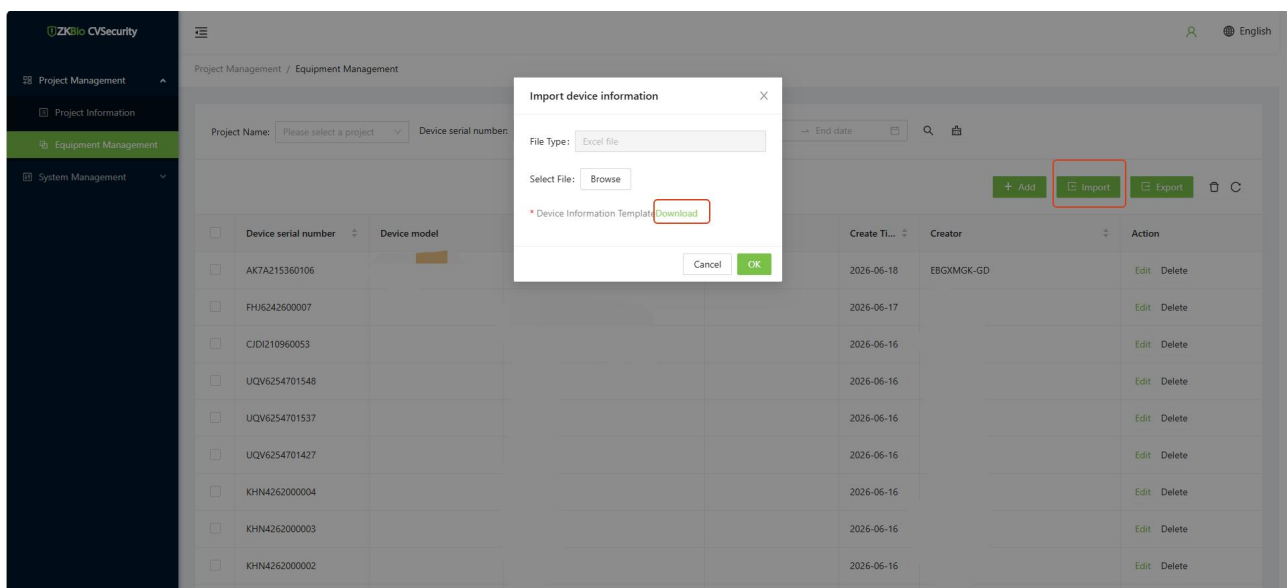


Step2:

Navigate to "Project Management/Equipment Management", click Add, select the corresponding project, then fill in the equipment serial number, model and remarks.



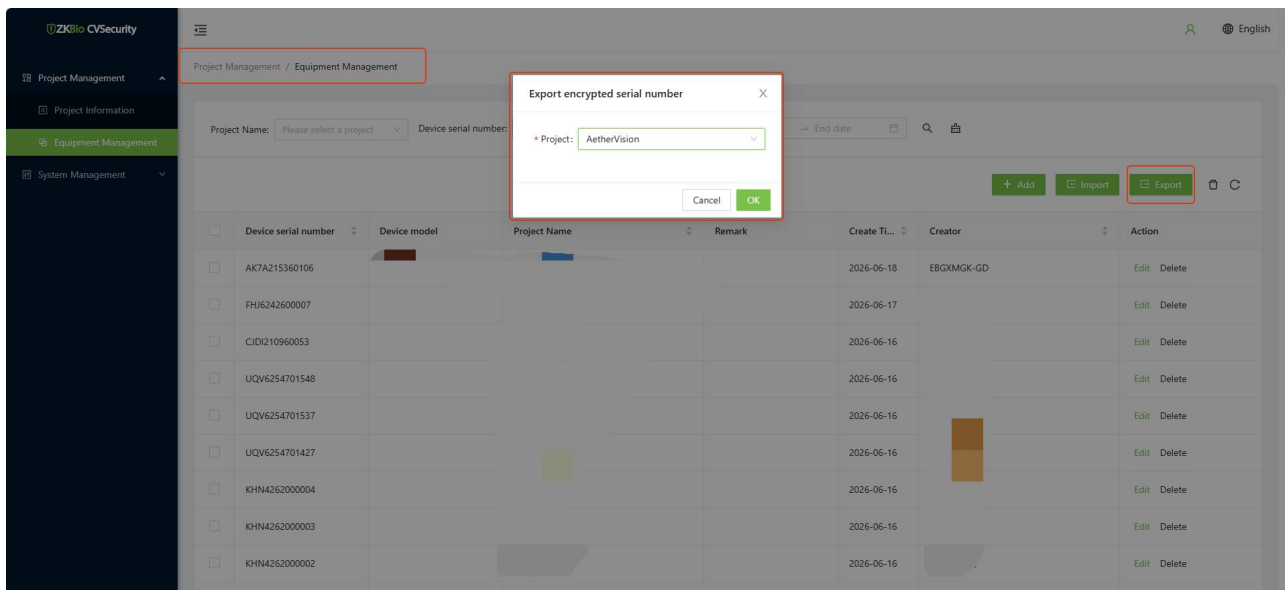
If you need to add multiple devices in batches, click Import to download the device information template. Fill in the data according to the table headers and save the file. Click Import again, select the table file, and complete the batch import of devices.



Equipment Management				
Project Number	Project Name	Device Serial Number	Device Model	Remarks
1781764299346	AetherVision	AK7A215360106	K2-400	

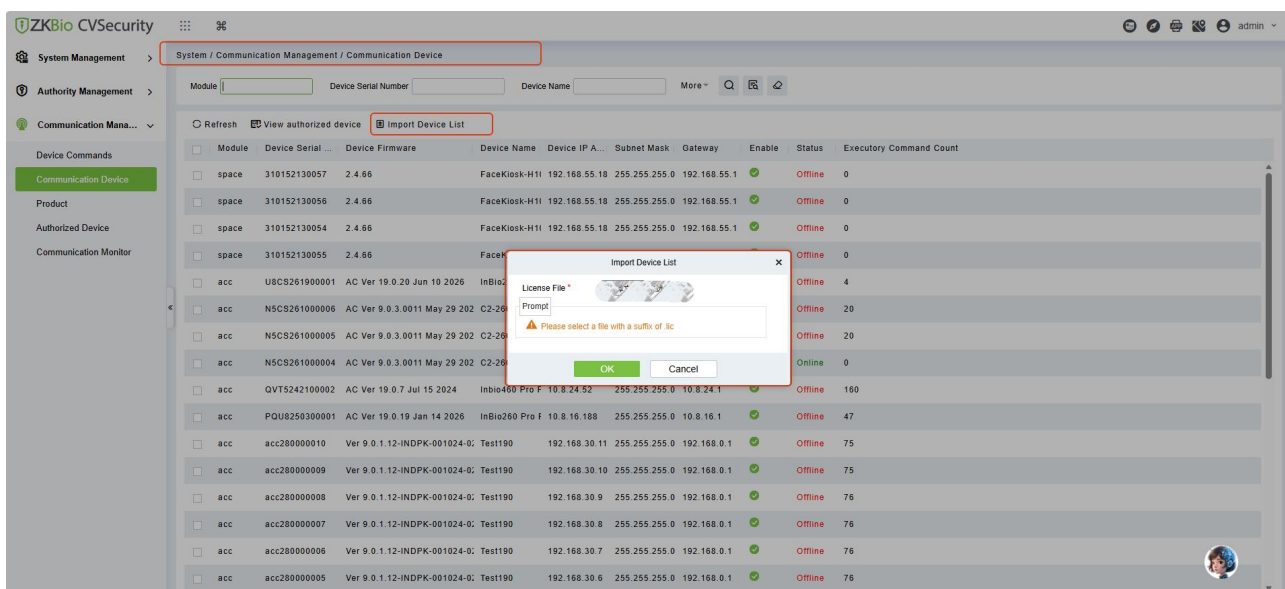
Step3:

Navigate to "Project Management/Equipment Management", click Export, select the project, then click OK Export to generate a file with the .lic suffix.



Step4:

Access ZKBio CVSecurity platform and navigate to "System / Communication Management / Communication Device". Click "Import Device List", select the .lic file exported from the project control platform, then click OK to finish the import.



Account Management of Project Control Platform:

Navigate to "System Management/Account Management" and click Add to create system login accounts for agents to manage project devices.

ZKteco CVSecurity

Project Management

System Management

Account Management

System Management / Account Management

Customer Name: Phone: Email: More

Add

Import

	Customer Name	Contact	Phone	Email	Roles	Create Ti...	Creator	Action
☐			15601666769			2026-06-01	administrator	Edit Delete
☐						2026-05-29	administrator	Edit Delete
☐						2026-01-23	administrator	Edit Delete
☐						2026-01-09	administrator	Edit Delete
☐			19017098960			2025-12-26	administrator	Edit Delete
☐			18094042866			2025-12-18	administrator	Edit Delete
☐			15218892637			2025-11-28	administrator	Edit Delete
☐			15017326827	popy.xiao@zktec...		2025-10-15	administrator	Edit Delete
☐			13899915401			2025-06-24	administrator	Edit Delete

ZKteco CVSecurity

Project Management

System Management

Account Management

System Management / Account Management / Add

Create an account for the agent to log in to the system, used to control project equipment.

* Customer Name: Please inputCustomer Name

Contact: Please inputContact

Phone: Please inputPhone

Email: Please inputEmail

* Roles: Please selectRoles

Agent Qualification: Please upload agent qualification image

Browse

* Password: *****
* The password is 4-18 characters. The default is 111111.

Cancel

Confirm

ZKTeco Industrial Park, No.32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone : +86 769 - 82109991
Fax : +86 755 - 89602394
www.zkteco.com



Copyright © 2026 ZKTECO CO., LTD. All Rights Reserved.