Smart IoT Platform

User Manual

V2.06

Contents

1 Overview....1

2 B/S Login and Initial Configuration....1

2.1 (For First Login) Set admin Password....2

2.2 (Optional) Reset admin Password....4

3 C/S Client....6

3.1 Auxiliary Screen....7

4 Homepage....8

4.1 Function Navigation....9

4.2 Custom Function Navigation....10

4.3 Configuration Wizard....11

5 Data Dashboard....12

5.1 Data Dashboard....12

5.2 Custom Data Dashboard....17

6 User Management....18

6.1 Organization Management....19

6.2 Role Management....20

6.3 User Management....23

6.4 AD Domain User....28

7 Device Management....31

7.1 Frontend Device....31

7.1.1 Device Discovery....32

7.1.2 Add One by One....32

7.1.3 Batch Add....40

7.1.4 Configure Frontend Device....41

7.1.5 Edit Device Info....42

7.1.6 Edit Access Control Device Type....42

7.1.7 Edit Channel Info....43

7.1.8 Move Device....44

7.1.9 Allocate Device....44

7.1.10 Others....45

7.2 Cloud Device....46

7.2.1 Manage Cloud Device....46

7.2.2 Long Time Preview....47

7.3 Edge Device....50

7.3.1 VSS NVR....50

7.3.2 Third-party Host....52

7.4 Terminal Device....56

7.4.1 Decoder & Video Wall Controller....56

7.4.2 Network Keyboard....57

7.5 Server Management..... 58
8 Video Storage Configuration..... 59
8.1 Add Storage Resource..... 60
8.2 Recording Storage..... 60
8.3 Recording Backup..... 63
8.4 Backup Status..... 66
8.5 Cross-Domain Storage Diagnosis..... 67
8.6 Video Compression..... 68
8.6.1 Batch Configuration..... 68
8.6.2 Single Configuration..... 70
8.6.3 Compression Statistics..... 70
9 Video Application..... 71
9.1 Live View..... 71
9.1.1 Camera Live View..... 72
9.1.2 Camera Sequence..... 73
9.1.3 Group Display..... 75
9.1.4 Group Sequence..... 76
9.1.5 Live View Operations..... 79
9.1.6 PTZ Control..... 82
9.1.7 Live View Resource Management..... 85
9.1.8 Fisheye Dewarping..... 86
9.1.9 Picture-in-Picture..... 87
9.1.10 Live Video Compression..... 89
9.1.11 Favorites..... 89
9.2 Playback..... 90
9.2.1 Search Recordings..... 90
9.2.2 Playback Operations..... 94
9.2.3 Search Backup Recordings..... 98
9.2.4 Recording Download..... 98
9.3 Video Wall..... 100
9.3.1 DX Video Wall..... 100
9.3.2 Multi-DC Video Wall..... 115
9.4 Smart Live View..... 120
9.4.1 Smart Live View..... 120
9.4.2 Face Recognition..... 121
9.4.3 Vehicle Application..... 123
9.4.4 Multi-Target Detection..... 125
9.5 Media Configuration..... 126
9.5.1 Video..... 127
9.5.2 Snapshot..... 128
9.5.3 Recording..... 129
9.5.4 Video Wall..... 129

9.5.5 PTZ....130
10 AR Live Map....130
10.1 Configuration....131
10.1.1 Configure High-Position Camera....131
10.1.2 Personalization....133
10.1.3 Other Configuration....134
10.2 High-Position Camera Switching....134
10.3 High-Position Camera Patrol....135
10.4 High-Low Position Camera Linkage....137
10.5 Add Label....137
10.5.1 Add Label....137
10.5.2 Label Operations....143
10.6 Label Management....145
10.7 Key Label....146
10.8 Filter Labels....147
10.9 Map Display....148
10.10 PTZ Control....150
11 Room Management....151
11.1 Community Room Management....152
11.1.1 Add Room....152
11.1.2 Manage Room....152
11.2 Resident Management....153
11.2.1 Add Manually....154
11.2.2 Add from Personnel....158
11.2.3 Add in Batches....158
11.2.4 Manage Resident....159
12 Personnel Management....160
12.1 Department Management....160
12.2 Add Person....162
12.2.1 Add in Batches....162
12.2.2 Add One by One....163
12.2.3 Get Personnel from Device Side....169
12.3 Personnel Management....170
12.4 Custom Attribute....171
13 Visitor Management....172
13.1 Registration....172
13.1.1 Register Visitor....172
13.1.2 Visitor Management....176
13.1.3 Custom Attribute....178
13.2 Visitor History....179
13.3 Visitor Settings....180
13.4 Blocklisted Person....180

14 Area Monitoring.....181
14.1 Vistor Monitoring Task.....181
14.2 Stranger Monitoring Task.....183
14.3 Task Management Operations.....184
14.4 Permission Search.....184
15 Access Control Management.....185
15.1 Access Control Permission.....185
15.1.1 Schedule Template.....185
15.1.2 Access Permission Config.....188
15.1.3 Permission Search.....193
15.2 Remote Control.....193
15.2.1 By Default Organization.....194
15.2.2 By Custom Group.....194
15.2.3 Custom Group Configuration.....195
15.3 Access Control Configuration (Access Controller & Speed Gate & Turnstile).....197
15.3.1 Device Parameter Configuration.....197
15.3.2 Door Parameter Configuration.....197
15.3.3 Verification Template Configuration.....199
15.3.4 Door Verification Configuration.....199
15.3.5 External Device Configuration.....200
15.3.6 Event Input Configuration.....202
15.3.7 Alarm Report Configuration.....203
15.3.8 Alarm Linkage Configuration.....204
15.4 Advanced Configuration.....206
15.4.1 Door Channel Configuration(General Access Control).....206
15.4.2 Multi-Factor Authentication (Access Controller & Speed Gate & Turnstile).....207
15.4.3 Anti-Passback (Access Controller & Speed Gate & Turnstile).....210
15.4.4 Multi-Door Interlocking (Access Controller & Speed Gate & Turnstile).....215
15.4.5 Keep-Open/Closed Schedule.....216
15.4.6 Door Opening Mode Configuration(Face Recognition Access Control).....219
15.5 Face Recognition Access Control Configuration.....221
15.5.1 Face Library Configuration.....221
15.5.2 Face Detection Configuration.....223
15.5.3 Recognition Display Configuration.....224
15.5.4 Port & Peripheral Configuration.....225
15.5.5 Advanced Configuration.....226
15.5.6 Personalized Configuration.....229
15.6 Access Control Live.....231
15.7 Pass-Thru Records.....232
16 Elevator Control Management.....233
16.1 Elevator Control Configuration.....234
16.1.1 Floor Configuration.....234

16.1.2 Custom Units..... 236
16.1.3 Link Devices..... 238
16.1.4 Device Parameter Configuration..... 241
16.1.5 Verification Template Configuration..... 242
16.1.6 Verification Configuration..... 243
16.1.7 External Device Configuration..... 244
16.2 Elevator Control Permission..... 246
16.3 Elevator Live Video..... 246
16.4 Elevator Controller Verification Records..... 247
17 Video Intercom..... 248
17.1 Call Recipient Management..... 248
17.1.1 Add Call Receipt..... 249
17.1.2 User Management..... 249
17.2 Device Location Config..... 250
17.2.1 Add Device Location..... 250
17.2.2 Sync Location..... 251
17.2.3 View Details..... 251
17.3 Incoming Call..... 252
17.4 Outgoing Call..... 252
17.5 Call Records..... 253
18 Attendance Management..... 253
18.1 Attendance Regulations..... 254
18.2 Staff Schedule..... 254
18.2.1 Set Time Period..... 254
18.2.2 Shifts Management..... 256
18.2.3 Schedule Management..... 257
18.2.4 Holiday Adjustment..... 258
18.3 Attendance Management..... 260
18.3.1 Leave Management..... 260
18.3.2 Re-Sign In&Out Management..... 261
18.3.3 Re-Sign In&Out Records..... 261
18.4 Attendance Statistic..... 261
18.4.1 Original Data..... 262
18.4.2 Attendance Details..... 262
18.4.3 Attendance Summary..... 263
19 Face Monitoring..... 264
19.1 Face Library Management..... 264
19.1.1 Manage Face Library..... 265
19.1.2 Add Face Data..... 265
19.1.3 Manage Face Data..... 267
19.1.4 Sync Face Data..... 268
19.2 Monitoring Task..... 269

19.2.1 Create Monitoring Task 269
19.2.2 Manage Task 271
20 Comprehensive Search 272
20.1 SeekFree 273
20.1.1 Search by Text 273
20.1.2 Search by Image 274
20.1.3 Search Results 275
20.2 Face Search 277
20.2.1 Search by Attribute/Alarm 277
20.2.2 Search by Image 278
20.2.3 Search by Frequency 280
20.2.4 Face Trajectory 282
20.3 Pedestrian Search 282
20.3.1 Search by Attribute 282
20.3.2 Search by Image 283
20.3.3 Pedestrian Trajectory 284
20.4 Motor Vehicle Search 285
20.4.1 Search by Attribute/Alarm/Violation 285
20.4.2 Search by Image 286
20.4.3 Motor Vehicle Trajectory 287
20.5 Non-Motor Vehicle Search 288
20.5.1 Search by Attribute 288
20.5.2 Search by Image 289
20.5.3 Non-Motor Vehicle Trajectory 289
21 AcuTrack 290
22 People Flow Counting 292
22.1 Real-Time People Counting 292
22.1.1 People Flow Counting 292
22.1.2 Crowd Density Monitoring 293
22.2 Data Statistics 295
23 Area Appearance Frequency Counting 296
23.1 Area Management 296
23.2 Appearance Frequency Counting 296
24 Radar Control 297
24.1 People Counting Monitoring 298
24.2 People Presence Monitoring 299
24.3 Fall Monitoring 301
24.4 Vital Sign Monitoring 302
25 Parking Management 303
25.1 Parking Lot Management 304
25.1.1 Add Parking Lot 304

25.1.2 Configure Alarm Rules....307
25.1.3 LED Config....309
25.2 Vehicle Management....310
25.2.1 Authorized Vehicle....310
25.2.2 Forbidden Vehicle....312
25.2.3 Vehicle Data Sync....313
25.3 Vehicle Volume....313
26 Electronic Patrol....314
26.1 Patrol Configuration....315
26.1.1 Patrol Point....315
26.1.2 Patrol Route....316
26.1.3 Patrol Team....319
26.1.4 Patrol Schedule....320
26.2 Patrol Search....322
26.2.1 Schedule Search....322
26.2.2 Records Search....323
26.2.3 Patrol Statistics....324
27 Map Configuration....325
27.1 Map Engine Management....327
27.1.1 Map Management....327
27.1.2 Scene Management....331
27.2 Edit Map....335
27.2.1 Bind Map....335
27.2.2 Device Point Management....337
27.2.3 View Map....339
27.2.4 Heat Zone....339
27.2.5 Map Display Management....340
27.2.6 Evacuation Route....342
27.2.7 Roam Config....344
27.2.8 Panoramic Config....347
27.3 Map Display Configuration....348
27.4 Map Application....349
28 Alarm Center....350
28.1 Alarm Configuration....351
28.1.1 User Subscription....351
28.1.2 Alarm Aggregation....353
28.1.3 Alarm Sound....353
28.1.4 Alarm Linkage....354
28.2 Real-time Alarm....363
28.3 Alarm Notification....368
28.4 Disk Full Alarm....369
28.5 Historical Alarm....369

28.5.1 Alarm Records....370
28.5.2 Pushed from Others....372
28.5.3 Alarm Statistics....375
29 System Configuration....376
29.1 Third-Party Application....376
29.2 Platform Cascading....377
29.2.1 Private Cascading....377
29.2.2 Platform Configuration....378
29.3 Protocol&Interconnection....379
29.3.1 Cloud Service....379
29.3.2 OpenAPI....380
29.4 Service Configuration....381
29.4.1 Time Configuration....381
29.4.2 Holiday Management....381
29.4.3 Email....382
29.4.4 Temperature....384
29.4.5 Data Sync Configuration....385
29.4.6 Video Intercom....386
29.4.7 Face Sync....387
29.4.8 Auto Time Sync....387
29.4.9 Alarm Input/Output Config....387
29.4.10 Card Attribute....390
29.5 Network Management....391
29.5.1 Network Configuration....391
29.5.2 Security Configuration....394
29.5.3 Network Security....398
29.6 Cluster Management....400
29.6.1 Primary/Replica Management....400
29.6.2 Dual-Server Hot Standby....402
29.7 Disk Configuration....406
29.7.1 Local Disk....406
29.7.2 IPSAN Management....412
29.8 Advanced Configuration....417
29.8.1 Function Switch....417
29.8.2 Alarm Customization....417
29.8.3 Style Personalization....418
29.8.4 Restore Defaults....419
29.9 License Management....419
29.9.1 License One-Click Activation....419
29.9.2 License Manual Activation....420
29.9.3 View License....420
29.9.4 License Deactivation....421
29.10 Basic Configuration....421

30 Operations&Maintenance 422
30.1 Operation Logs 422
30.2 Database Backup 422
30.3 Restart&Upgrade 424
30.4 System Diagnosis 426
30.4.1 Device Diagnostic Info 426
30.4.2 Server Diagnostic Info 428
30.4.3 Server Packet Capture 429
30.4.4 Network Test 431
30.5 Information Statistics 432
30.5.1 Server Performance 433
30.5.2 Device Status 433
30.5.3 Storage Capacity 434
30.5.4 Recording Status 434
30.6 Video Diagnosis 434
30.6.1 Diagnosis Configuration 435
30.6.2 Diagnosis Result 438
30.6.3 Diagnosis Statistics 441

1 Overview

The platform offers a comprehensive security solution tailored for general small to medium-sized campus environments. It leverages advanced modular technology, enabling seamless integration of edge IoT devices for unified access, data processing, forwarding and storage. Additionally, it facilitates rapid integration of various campus management subsystems, encompassing video management, pedestrian and vehicular traffic monitoring, and overall security operations. The platform supports the integration and management of various devices such as IPCs, NVRs, SmartBoxes, decoders, face recognition terminals, general access control devices, video intercom devices, and third-party devices (alarms, access control). Beyond basic video services, it extends to pedestrian management, vehicle management, and alarm management for fundamental campus applications. Additionally, it offers comprehensive security functions including attendance management, guard patrol, advanced operations and maintenance, and map. Its simple deployment, flexible scalability, and reliable stability make it suitable for a wide range of applications, from local-area network (like campuses, buildings, schools, hotels, venues) to wide-area network (such as networked retail).

- Efficient deployment: The platform integrates complete functions and does not require complex networking setup. Simply power it on and connect to network.
- Simple operations: The platform provide visual business management through an intuitive client interface. Based on different user roles and computer configuration, operations can be performed on B/S client, C/S client and APP respectively to meet the use needs of different users.

2 B/S Login and Initial Configuration

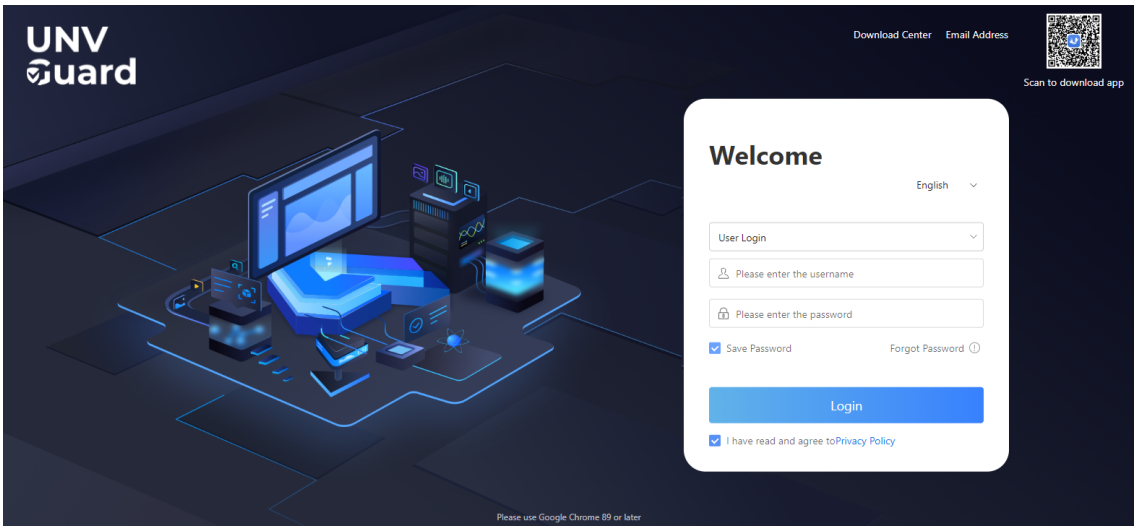
Log in to the B/S client using a browser, and change the default password after the first login to ensure system security.

Note:
Please use Google Chrome 89 or later.

1. Open a browser and enter the ***server IP address*** in the address bar.

   Note:

   - The default IP addresses are as follows. Modify according to the actual networking:
     - Network interface1：192.168.1.60
     - Network interface2：192.168.2.60
     - Network interface3：192.168.3.60
     - Network interface4：192.168.4.60
   - After login, you can change the IP address at **System > Network >**TCP/IP.
   - If you want to log in via HTTPS, please enable HTTPS in **System Config > Network Management > Security Config**.



2. Enter the username and password.
   - Log in as system user: Select **User Login**.

Default administrator	The system initially defaults to 2 administrator accounts: admin / loadmin; the default password: admin_123. **Note:** • The administrator accounts have full privileges over the system. • Upon first login with the default password, "admin" must follow the security guide to change the password. For the loadmin, you can Change Password in the upper-right corner after login.
Other users	See user information in User Management.

   - Log in as AD Domain user: Select **AD Domain Login**, and enter the domain user ID and password.

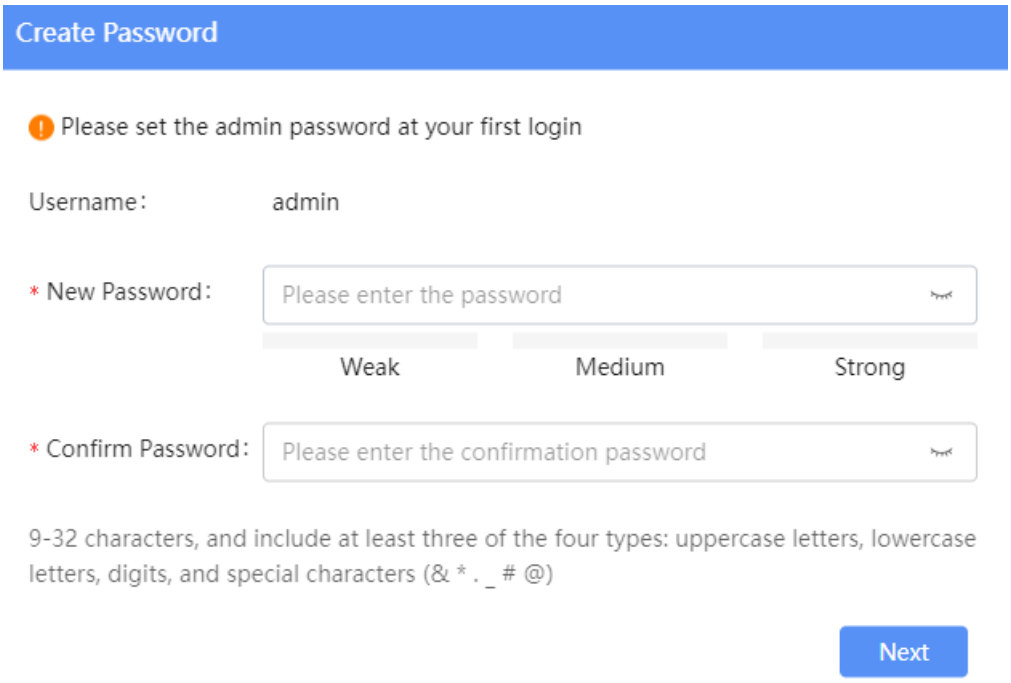
     Note:
     Please first complete the configuration of AD Domain User and import the AD domain user accounts.

3. Select **I have read and agree to Privacy Policy**. Click **Login**.

2.1 (For First Login) Set admin Password

When log in to the B/S client for the first time, please follow the instructions below to set a strong password for the admin user to ensure security.

1. When open the login page for the first time, a page as shown below appears.

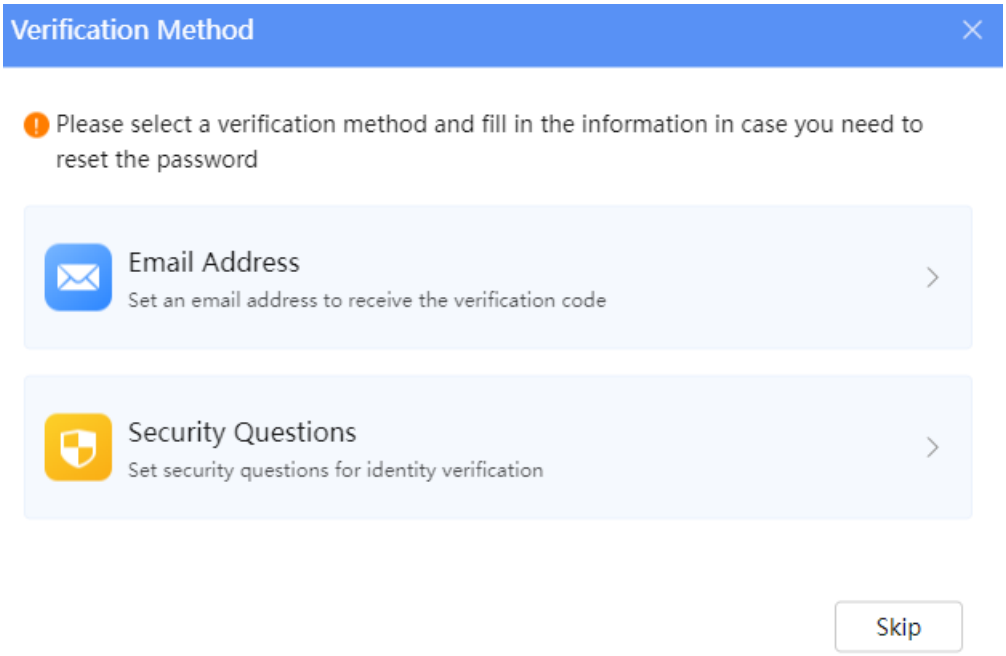


2. Set a password and confirm it.

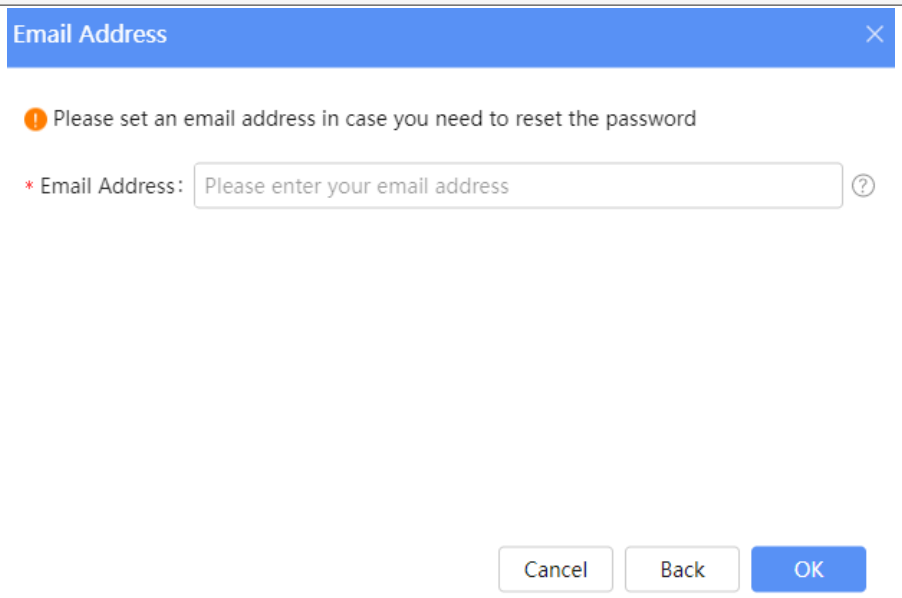
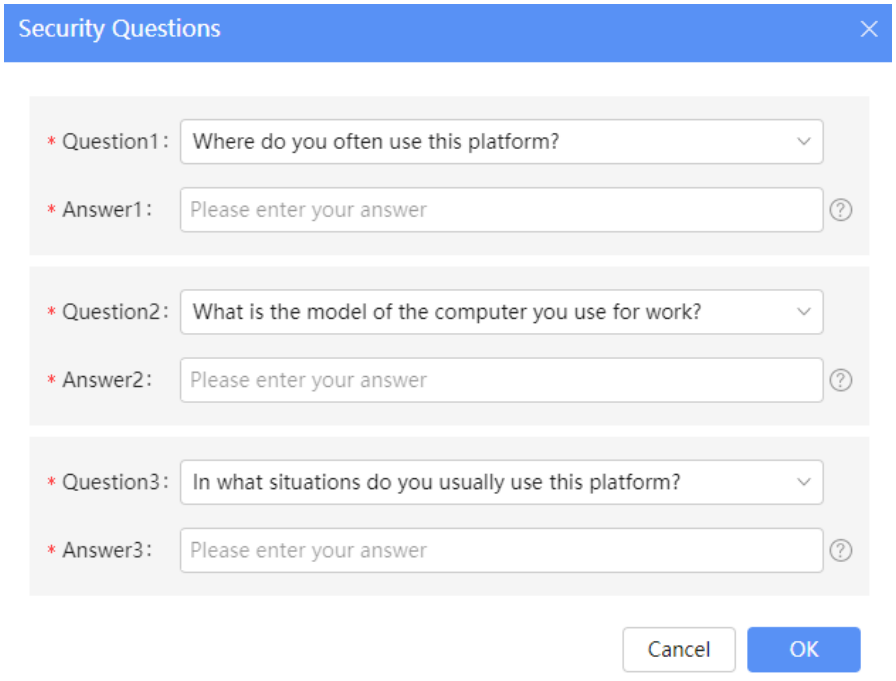
   Note:
   For security concerns, you must set a strong password with 9-32 characters, including uppercase and lowercase letters, digits, and special characters.

3. Click **Next**.

4. Set a verification method for security verification when resetting the password.
   If not required, click **Skip** to complete the configuration. If skipped, the system will prompt admin to set up an authentication method at each login, until one is configured.



Verification Method	Operation Steps
Email	Click **Email**. A dialog box as shown below appears.

Verification Method	Operation Steps
	 (1) Enter your email address and click **Send Code**. (2) Enter the verification code you received in your email inbox. (3) Click **OK**, and you will see a message confirming the successful setup.
Security Questions	Click **Security Questions**. A dialog box as shown below appears. Set questions and answers, click **OK**. 

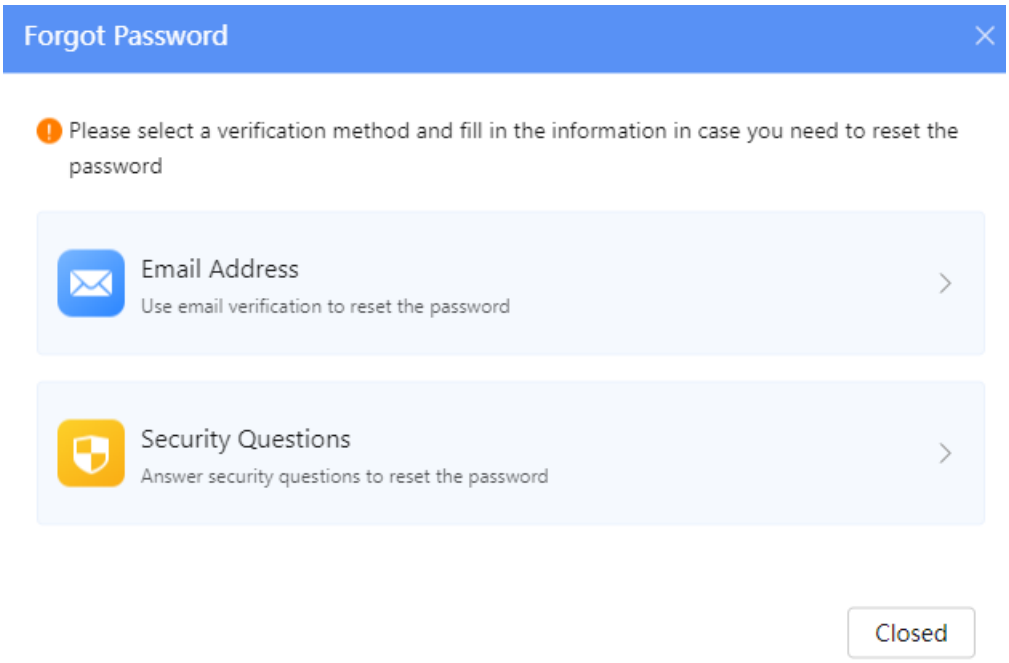
2.2 (Optional) Reset admin Password

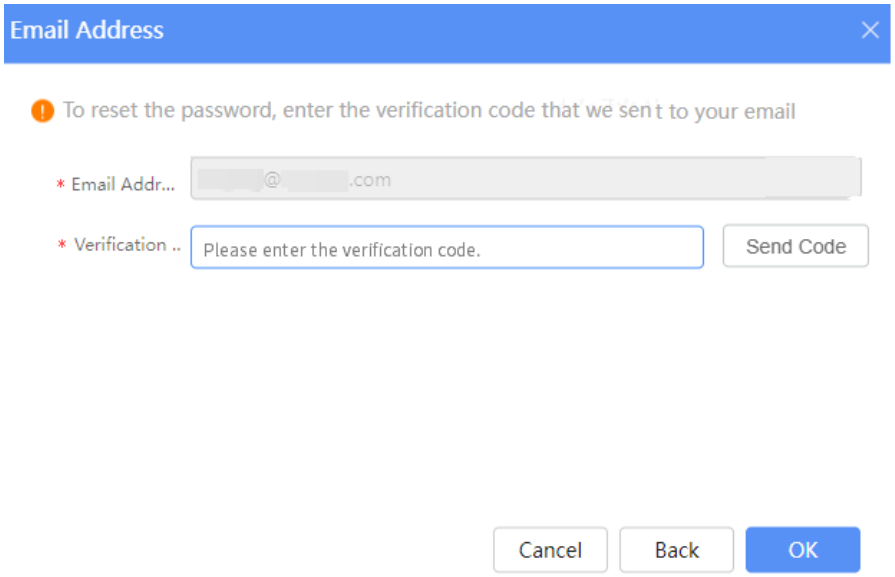
You can reset admin password via a security verification if you forgot the password.

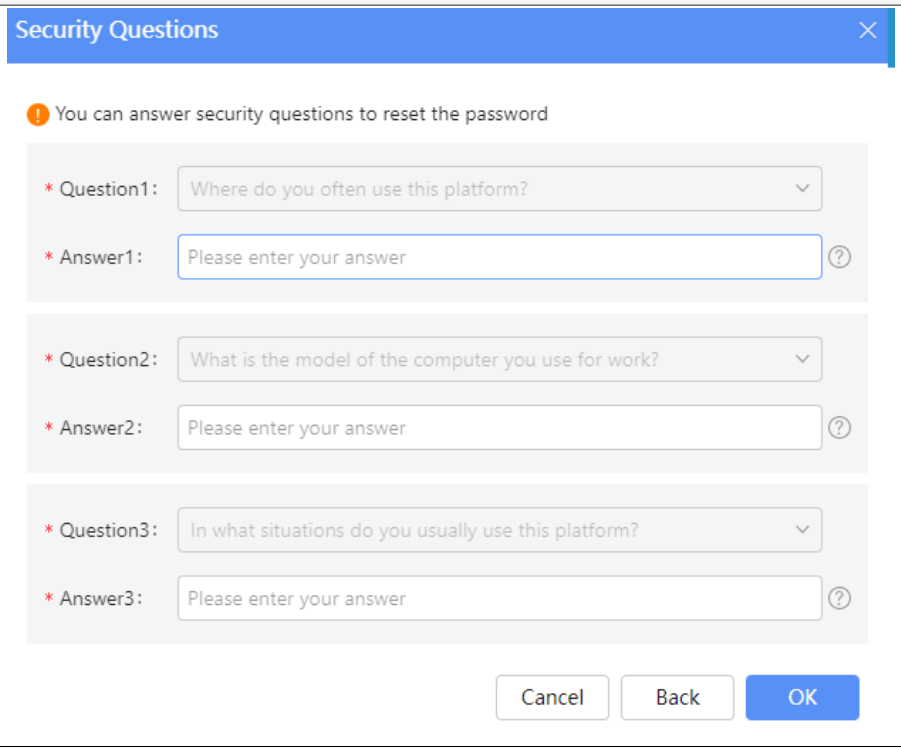
Note:

- If you have not provided an email address or security problems for admin, you will not be able to reset admin password here.
- If a non-admin user forgets password, they can contact admin user to modify in User Management.
- All users can click Change Password in the upper-right corner to change the password after login.

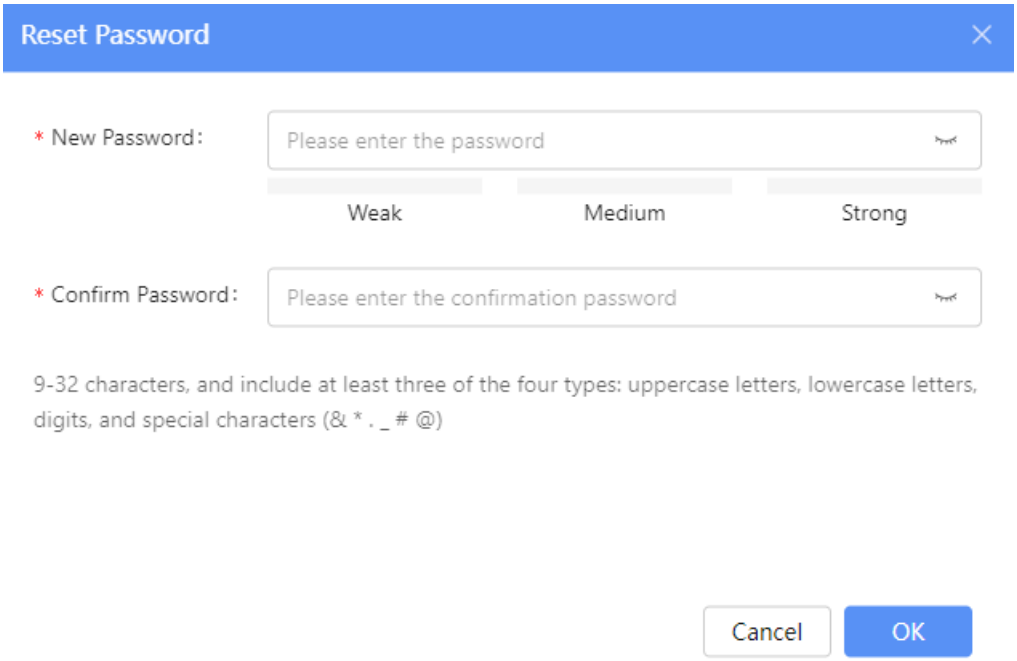
1. Click **Forgot Password** in the lower-right corner of the login page.
2. Select the verification method: **Email** or security problems.



Verification Method	Operation Steps
Email	Click **Send Code** to send a verification code to the reserved email address. Enter the verification code you received in your email inbox. 
Security Questions	Input questions and answers, click **OK**.

Verification Method	Operation Steps
	

3. Reset the password.



3 C/S Client

You can install the C/S client on your PC.

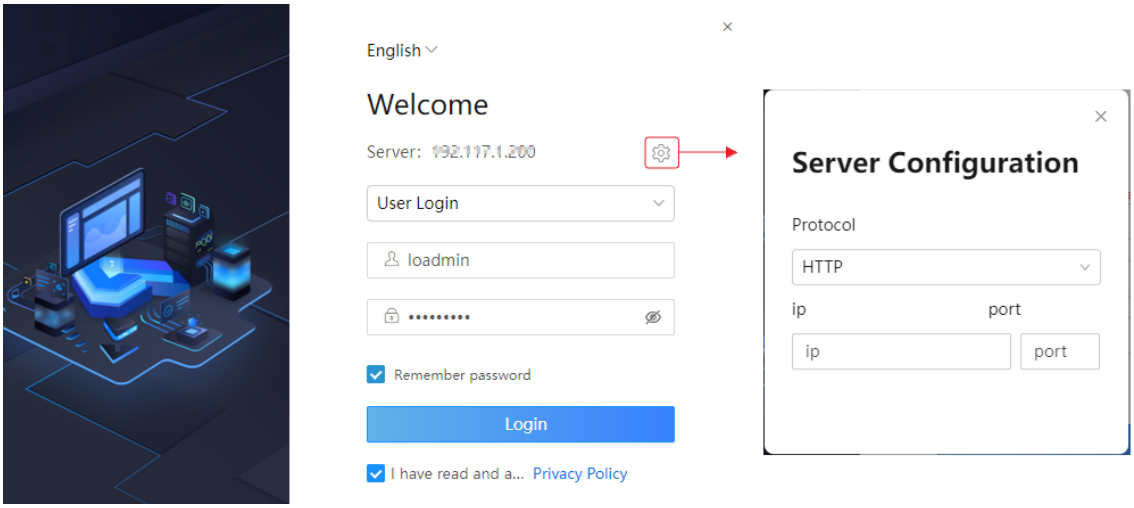
Computer System Requirements

The C/S client can be installed on the following computers:

Item	Requirements
Operating System	• Windows 11 64-bit • Windows 10 64-bit
Memory	16GB or more, with at least 10 GB free memory.

Install C/S Client

1. Click **Download Center** in the upper-right corner of the login page of the Web interface.
2. After downloading the C/S client, double-click the .exe file to install.
3. Once installed, a shortcut will appear on your desktop. Double-click the shortcut to open the login window.



4. Click ⚙. Select the login protocol (HTTP/HTTPS), enter the IP address and port (default: 80) of the server.

   Note:

   - If you want to log in via HTTPS, please enable HTTPS on the B/S client.
   - The server IP address is the IP address of the computer on which the B/S client is installed.

5. Enter the username and password.

   Note:

   - **User Login**: The username/password is same to the B/S client.
   - **AD Domain Login**: enter the domain user ID and password. Please first complete the configuration of AD Domain User and import the AD domain user accounts on the B/S client.

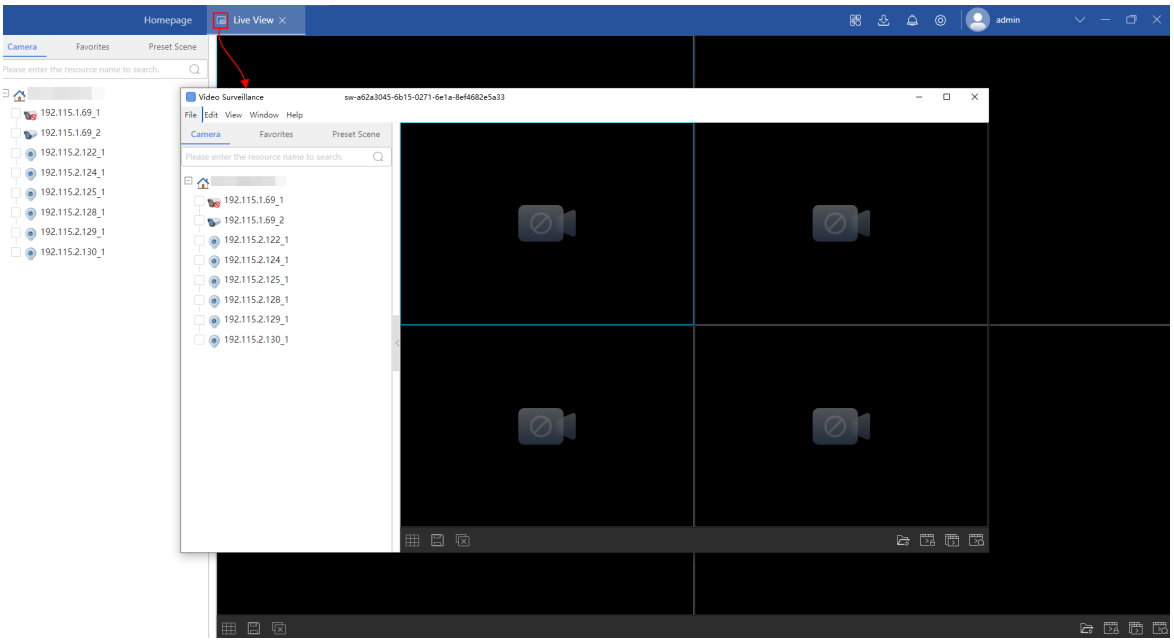
6. Select **I have read and agree to Privacy Policy**. Click **Login**.

3.1 Auxiliary Screen

Only the C/S client supports auxiliary screens.

On the C/S client, you can create auxiliary screens on **any level-2 submenu** page as independent video windows. If your PC is connected to multiple monitors, you can drag the auxiliary screen to any of the connected monitors to operate functions.

Click before **the level-2 submenu** to create an auxiliary screen.
The following uses the auxiliary screen of the **Live View** menu as an example:

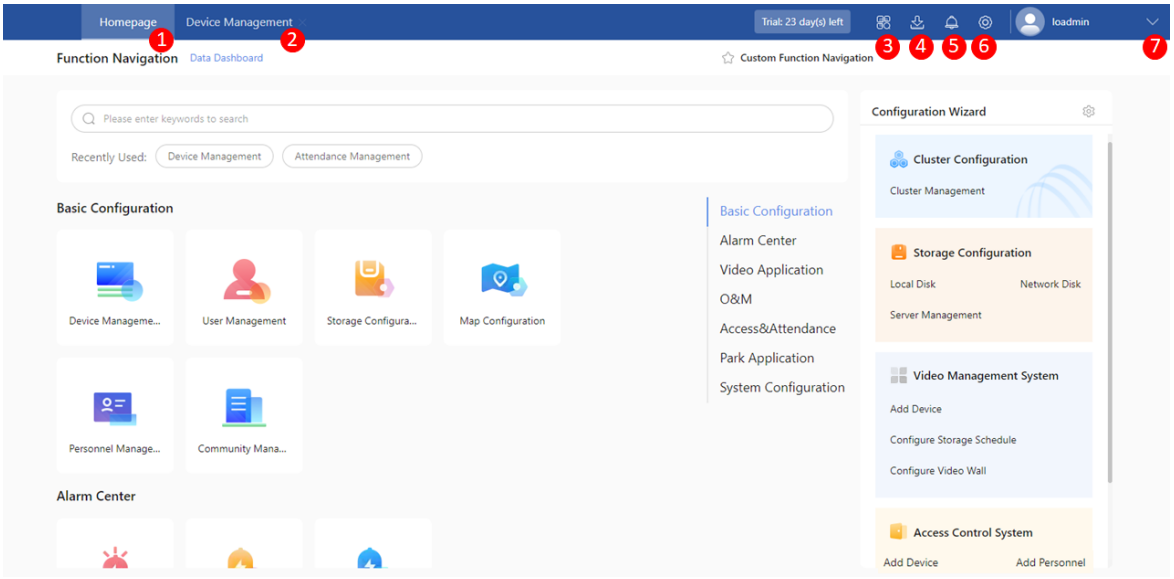


- The **Live View** menu supports creating up to 3 auxiliary screens, while other menus support a maximum of 1 auxiliary screen. Services on each screen operate independently.
- You can drag, maximize, restore, or close the auxiliary screen.
- Operations on the auxiliary screen are the same as those on the main screen.
- After exiting and restarting the client, previously opened auxiliary screens will be closed.

4 Homepage

The homepage appears when you are logged in successfully, which consists of some function menus and global buttons.

Note:
The interface may vary based on the purchased license, software version, user permissions, and custom settings (such as Custom Function Navigation, Style Personalization). The following takes the default interface as an example.

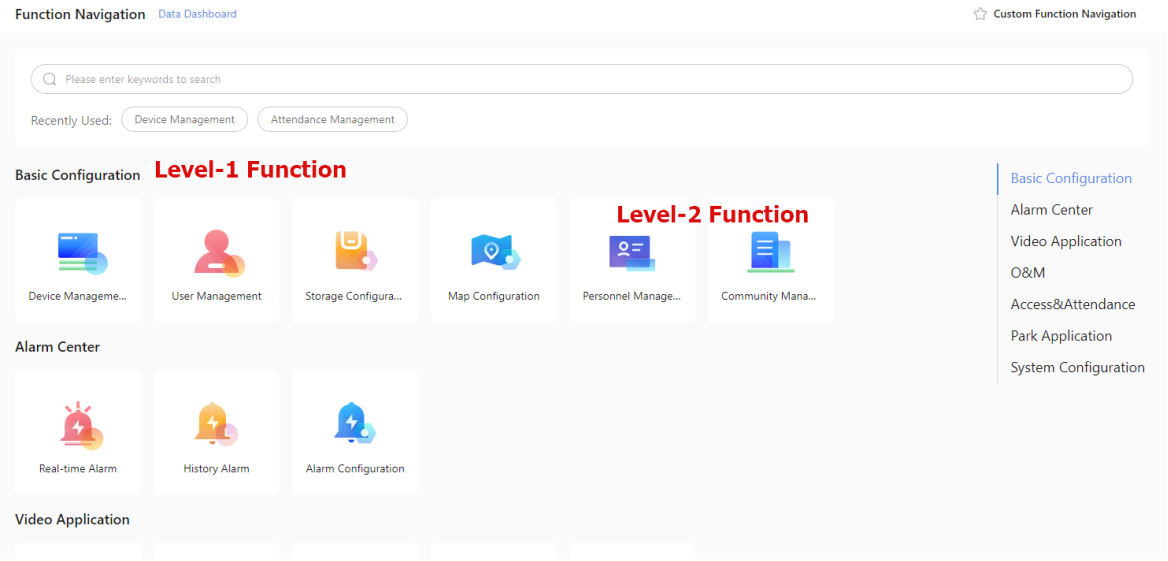


No.	Description
①	Provides an overview of functions, including Function Navigation, Data Dashboard.

No.	Description	
②	Opened function menu. Click X to close it.	
③	All functions: On any page, you can display the full list of level 1/2/3/4 menus through a drop-down box and search by keywords. Clicking a menu item will quickly take you to the corresponding page.	
④	Recording download task list: View the status of recording download tasks. You can also access the download directory, start, stop, and delete tasks.	
⑤	Alarm message: Displays the number of new alarms. Click the icon to enter the Real-time Alarm page.	
⑥	License Management	Please refer to License Management.
	Client Configuration	Set real-time alarm notification methods, including pop-up alarm window and alarm sound.
	Language Switching	Change the system language.
	Configuration Wizard	Show/hide Configuration Wizard.
	Customer Service Center	View the customer service phone number.
	Help	View privacy policy, system version, user manual, etc.
⑦	Username	The current logged-in user's username.
	Light/Dark Mode	Change the interface's background color: Choose Light (default) or Dark as needed. **Note:** All users can change the background color. The effective rules for the B/S client and C/S client are different: • B/S Client: Modification is applied only to the current browser page. Refreshing or re-logging in will revert the background color to the default setting. • C/S Client: Modification is permanently valid to the current client. Changing login user or server address will not affect the set background color.
	Change Password	Modify the password for the currently logged-in user.
	Email Address	Set the email address for identity verification if you want to reset the password.
	Security Questions	(**For admin**) Set security questions for identity verification if you want to reset the password.
	Logout	Log out the system and return to the login page.

4.1 Function Navigation

This page displays the function menus within the system. You can click on a function menu to enter the corresponding function page.



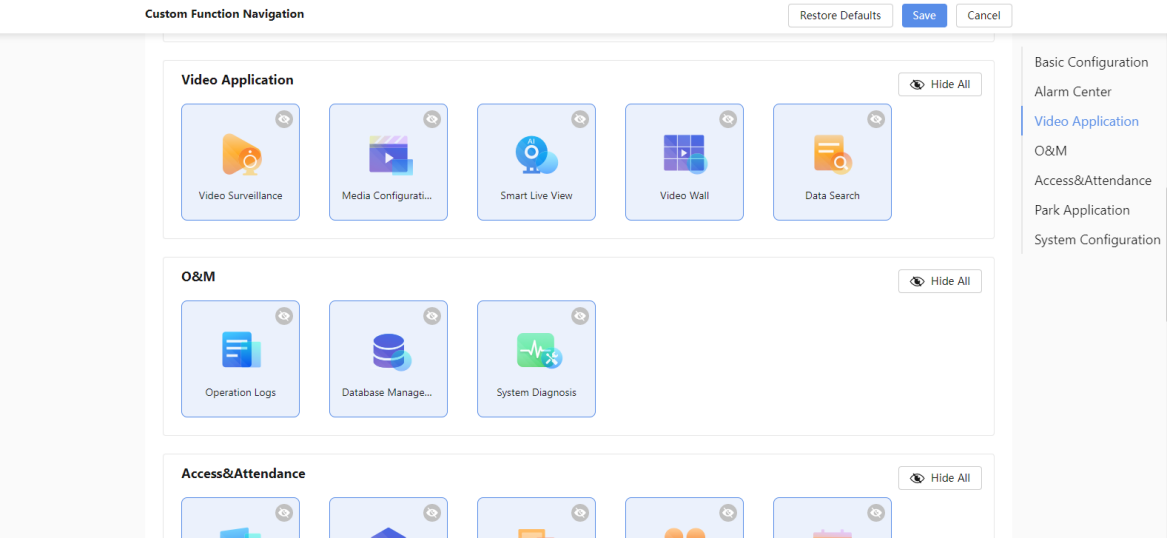
- Function menu: Displays the functions supported by the system. Click on the level-2 function menu to enter the corresponding page.

  Note:
  The function menus are displayed according to the License specification and user permission and can be customized to show/hide.

- Search: Click the search box to expand all the level-1/2/3/4 menus. Enter key words of the menu names to filter and find the corresponding functions.
- Recently used: Displays the last six functions recently visited (up to level-4 menus), with the latest used function listed first.

4.2 Custom Function Navigation

You can customize the function navigation by specifying which functions to show/hide. For example, hiding less frequently used functions can simplify the navigation.

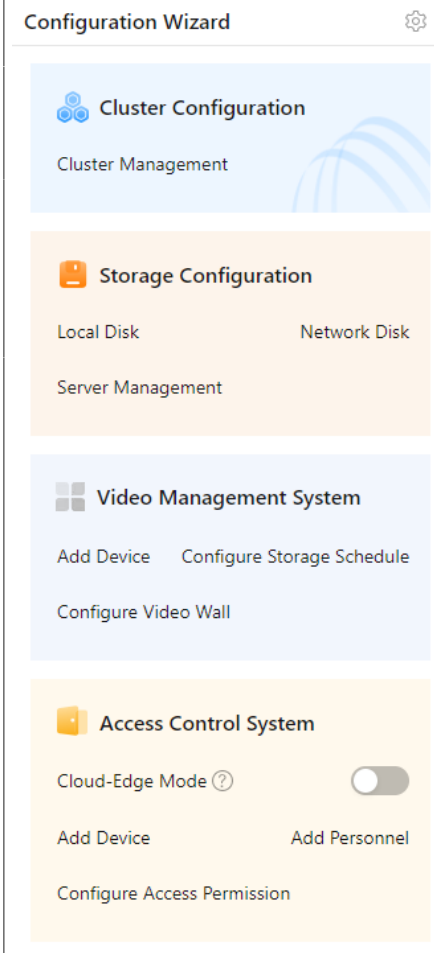


1. Click **Custom Function Navigation** in the upper-right corner.
   - Show: Click in the upper-right corner of the card to show the menu; click **Show All** to show all menus under the category.
   - Hide: Click in the upper-right corner of the card to hide the menu; click **Hide All** to hide all menus under the category.
   - Adjust order: To reorder cards within a category, click and drag the card to the desired position. To swap category positions, click and drag the category to the target location.
2. Click **Save**.

Note:
To restore the system's default interface, click **Restore Defaults**, then save.

4.3 Configuration Wizard

On the right side of the homepage, a configuration wizard is provided, displaying the setup steps for commonly used features. You can click on a setup step to navigate to the configuration page and configure the services.

Figure	Service Module	Configuration Steps
	Cluster Configuration	Cluster Management
	Storage Configuration	Local Disk Network Disk Server Management
	Video Management System	Add devices (Local Encoding Device, Cloud Encoding Device, Local Decoding Device) Configure storage schedule (Recording Storage, Recording Backup) Configure video wall (Video Wall)
	Access Control System	• Cloud-edge mode: Cloud-Edge Configuration, Add Device • Non-Cloud-Edge mode: Add Device, Add Personnel, Configure Access Permission (Access Permission Config, Schedule Template)

Note:
The business modules displayed in the configuration wizard depend on license specifications, user permissions, and Custom Function Navigation.

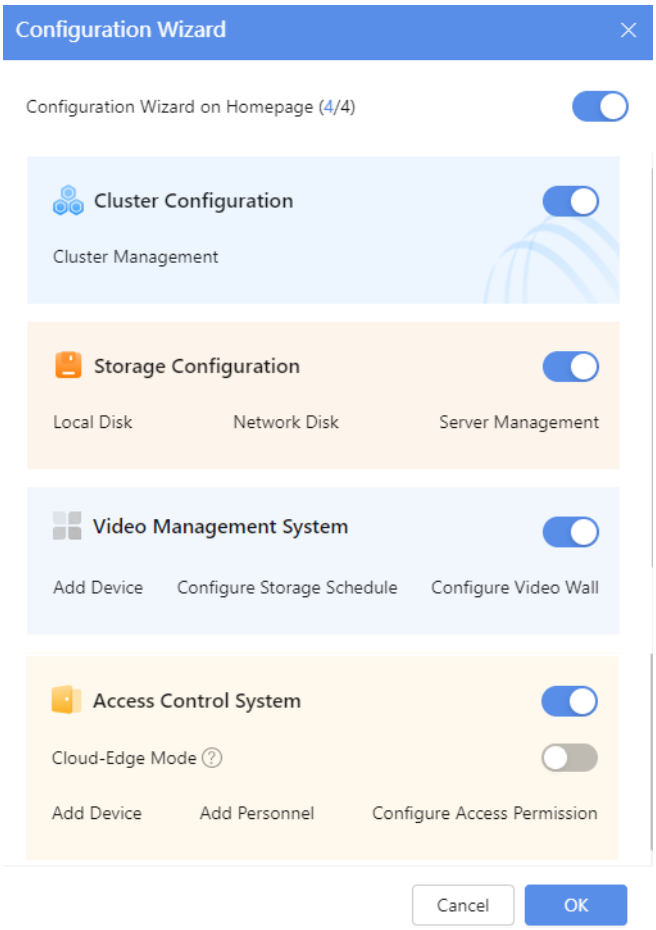
Show/Hide Configuration Wizard

You can show or hide the service modules displayed in the configuration wizard.

1. Click in the top right corner of the configuration wizard.

   Note:
   If the configuration wizard is not displayed on the homepage, click in the top right corner and then click **Configuration Wizard**.

2. Click the toggle to show or hide the service modules: (show,) or (hide).



Note:
For access control systems, please show or hide the cloud-edge mode based on whether it is integrated with EZCloud.

3. Click **OK**.

5 Data Dashboard

Data dashboard integrates various types of service data in the system and displays data statistics in visual diagrams. This facilitates users to view the status of service operations and enables users to take timely management measures based on the data.

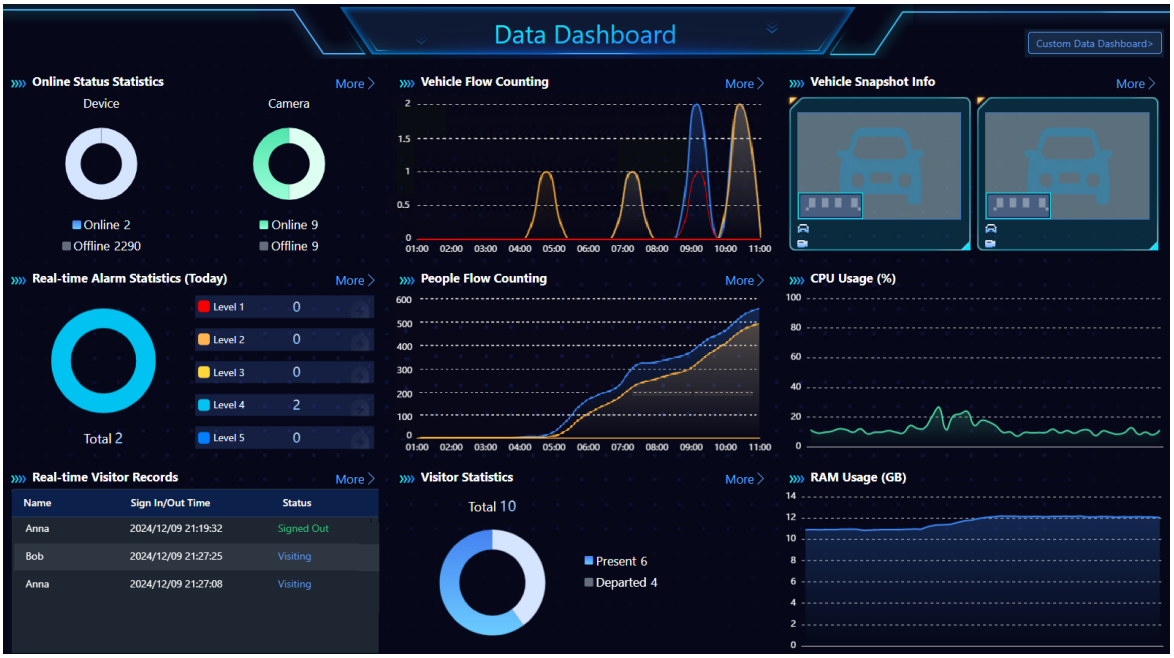
You can customize the data type and layout of the data dashboard to meet your needs.

5.1 Data Dashboard

After logging, click **Data Dashboard Mode** tab to switch to the dashboard view. To enlarge the dashboard to full screen, click in the upper-right corner.

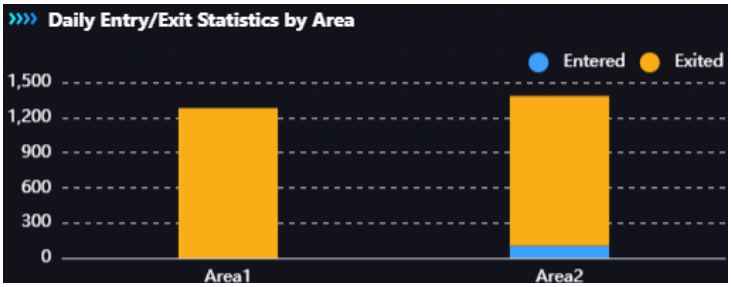
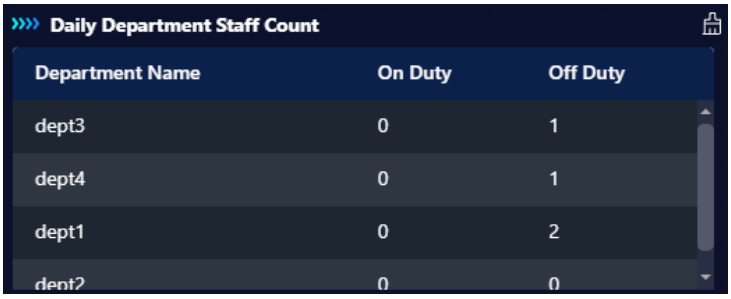
Figure 5-1: Example 1

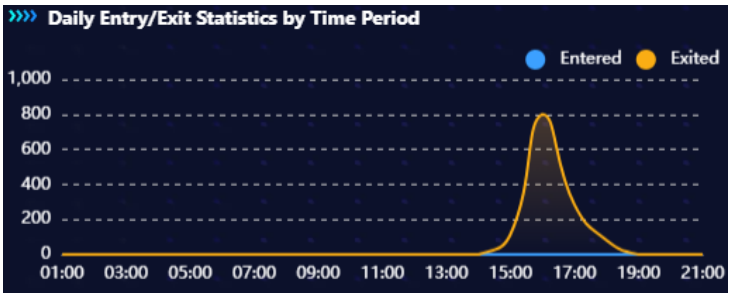
Figure 5-2: Example 2



Data Charts Description

Category	Statistical Item	Data Description
Access Management	Real-time Visitor Records	Displays real-time visitor access records, including visitor name, sign in/out time, and visit status (visiting/signed out).
	Visitor Statistics	Displays the total number of visitors today/staying/departed. Data source: Visitor Management. • Visitors Staying refers to the number of visitors who haven't signed out. • Visitor Departed refers to the number of visitors who have signed out.
	People Flow Counting	Displays the number of people entered/exited per hour today. For example, the value at 12:00 represents the number of people entered/exited from 11:00 to 12:00.

Category	Statistical Item	Data Description
		Data source: Smart Live View > People Counting, reported from smart IPCs/NVRs.
	Visitors Staying	Displays the current number of visitors, i.e. the number of visitors who have signed in today but have not yet signed out.
	Daily Entry/Exit Statistics by Area	Based on the entry and exit records of access control devices in each area for the day, counts the number of people entering and leaving each area.  • Entered: The sum of entry records from access control devices within the area. • Exited: The sum of exit records from access control devices within the area. **Note:** • Configure the entry/exit direction of access control passages in device management; passages without a direction are not counted. • Configure the access control devices under the area in Custom Data Dashboard > Chart. • Records that failed verification are not counted. • Data refreshes approximately every 30 seconds.
	Daily Department Staff Count	Counts the number of on-duty and off-duty employees in each department for the day.  • On duty: The last record is an entry. • Off duty: The last record is an exit. • Click in the upper right corner of the chart to reset the counting task, which sets all personnel to off-duty.

Category	Statistical Item	Data Description
		Note: • Configure the entry/exit direction of access control passages in device management; passages without a direction are not counted. • Configure the access control devices under the department and area in Custom Data Dashboard > Chart. • Records that failed verification are not counted. • Department data includes its sub-departments. • Data refreshes approximately every 30 seconds.
	Daily Entry/Exit Statistics by Time Period	Counts the number of people entering and leaving per hour for the day. For example: The entering count for 10:00 is the sum of entry records from 09:00:00 to 09:59:59.  **Note:** • Configure the entry/exit direction of access control passages in device management; passages without a direction are not counted. • Configure the access control devices under the area in Custom Data Dashboard > Chart. • Records that failed verification are not counted. • Data refreshes approximately every 30 seconds.
People Management	People Snapshot Info	Displays the latest people snapshot, snapshot device, snapshot time, and identity information. If there is a match between the captured person and a person in the library, the dashboard will display the matching record, the person name, and his/her department. Data source: Smart Live View > Door Access Control and Smart Live View > Face Recognition.
	People Staying	Displays the current number of people across all areas. Calculated as: People Staying = People Entered Today - People Exited Today. If the result is negative, the value will display as 0. Data source: Data Search > People Counting.
	Employees Present	Displays the number of people whose last capture record is "Entry" within the configured statistical areas, from 00:00 today until now. Data source is Data Search > Area Appearance Frequency Counting . **Note:** Configure statistical areas in Custom Data Dashboard > Chart.
Vehicle Management	Vehicle Snapshot Info	Displays the latest 2 snapshots of the vehicle, plate close-up, snapshot device, plate number, and snapshot time. Data source: Smart Live View > Vehicle Application.
	Vehicle Flow Statistics	Displays the number of vehicles entered/exited/violated per hour today. For example, the value at 12:00 represents the number of vehicles from 11:00 to 12:00.

Category	Statistical Item	Data Description
		• Data source of vehicles entered/exited: Parking Management > Vehicle Volume. • Data source of vehicles violated: Comprehensive Search > Motor Vehicle Search-By Violation.
	Vehicles In&Out	Displays the current number of motor vehicles. Calculated as: Vehicles In&Out = Vehicles Entered Today - Vehicles Exited Today. If the result is negative, the value will display as 0.
Alarm Management	Real-Time Alarm Statistics	Displays the total number of alarms today and alarms at different levels. Data source: Historical Alarm.
	Alarm Trend Statistics	Displays the number of alarms generated per hour today. For example, the value at 12:00 represents the number of alarms generated from 11:00 to 12:00.
	Real-Time Alarms	Displays the total number of alarms triggered today.
Device Management	Device Status Statistics	Displays the current number of online/offline devices(regardless of the device type) and cameras, and the percentage of devices/cameras online.

	Central Recording Storage Status	Statistics on the storage status of central recording schedules, with data sourced from Recording Storage.
		
		• Today's Rating = 8.0 + [Recording / (Recording + Not Recording)] x 2; base score 8 points, full score 10 points.
		  • ≤9 is Fair
		  • < 9.6 is Good
		  • ≥9.6 is Excellent
		• The proportion of schedules that are Recording and Not Recording.
		Note:
		Even if a recording schedule is in an enabled state, if it is not actually storing due to device offline/stream disconnection, etc., it is counted as Not Recording.

Server Performance	RAM Usage (GB)	Displays the real-time RAM usage trend. (Statistics start from entering the dashboard)
	CPU Usage (%)	Displays the real-time CPU usage trend. (Statistics start from entering the dashboard)

Note:

- You can hover the mouse over the diagram to view the detailed numerical values.
- You can click **More** in the upper-right corner of the diagram to redirect to the corresponding data record page.

Quick Access

If using the default system template (refer to Example Image 1), you can click on the function bubble to quickly access the corresponding module for detailed data.

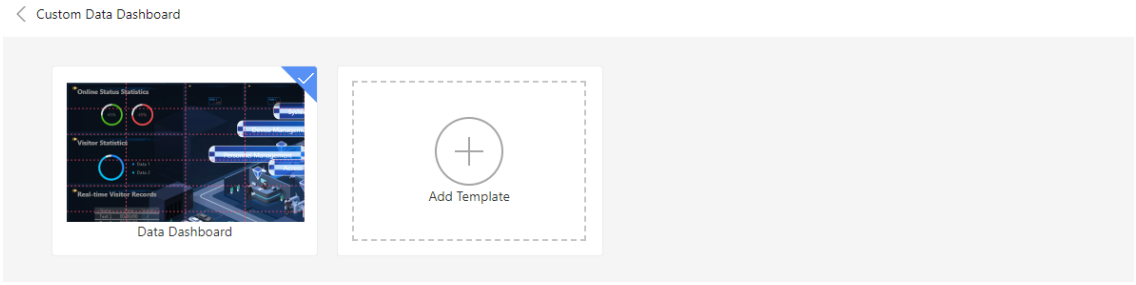
Note:
Supported functions: Personnel Management, Access Control, Attendance Management, Device Management, and System Diagnosis.
Users will only see the function bubbles they have permission for. For permission configuration, please refer to User Management.

5.2 Custom Data Dashboard

You can configure the data types and layout styles (including the number of charts, layout, title, background image, and chart borders) displayed on the dashboard.

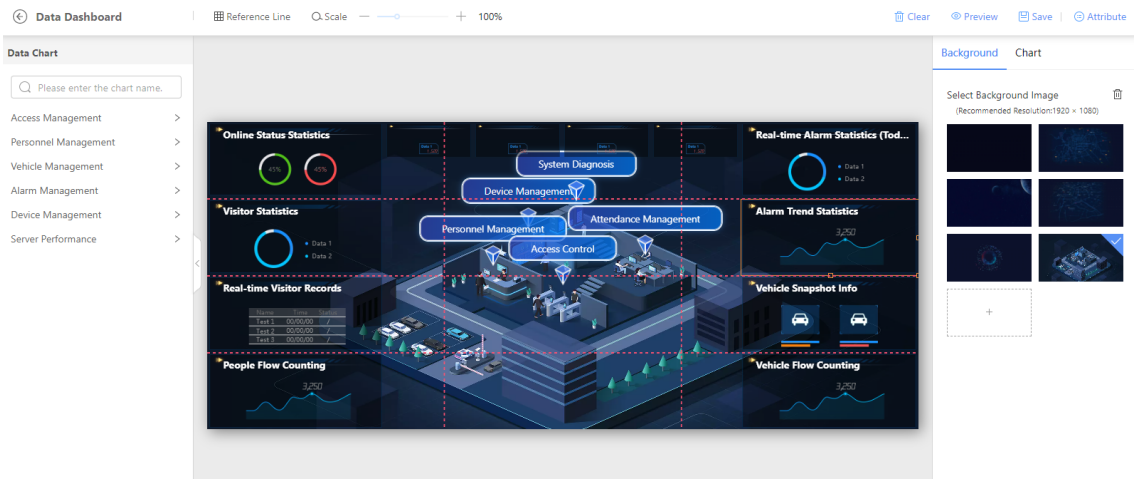
Note:
Only the super admin can configure the data dashboard.

1. On the **Data Dashboard** page, click **Custom Data Dashboard** in the upper-right corner.



2. Add new templates or modify existing templates as needed.
   - Add template: Click **Add Template**, enter the template name (the title of the dashboard), and then click **OK**.
   - Modify existing template: Hover the mouse over the template you want to modify and click **Edit**.

Note:
- For existing templates: Hover the mouse over the template. You can click **Preview** to preview its effect, click to edit its name, and click to delete it.
- Up to 20 templates are allowed.

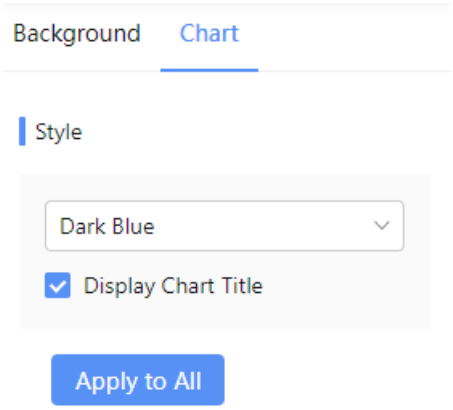


3. Click **Reference Line**. Choose a suitable reference line template (you can customize the Row x Column or select a preset option: 3*3, 3*4, 4*4, 5*5, 6*8, 8*8) to set the layout for charts.

Note:
In the central editing area, you can drag a reference line to adjust its position.

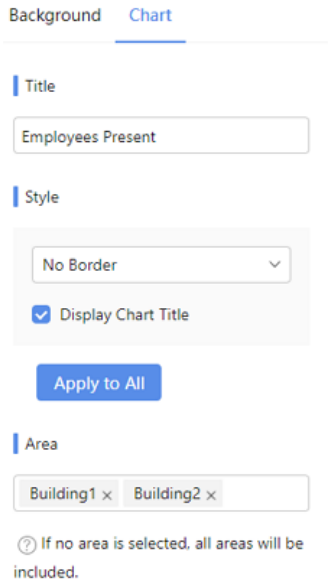
4. On the left side of the page, you can select the chart you want to display and drag it to the central editing area. The system can automatically adjust the chart size according to the layout.

5. On the right side of the page, you can set the background and chart properties.
   - In the **Background** tab, you can choose an existing background image or add a custom image (recommended resolution: 1920px*1080px; max. size: 20MB).
   - In the **Chart** tab, you can select the chart border style and set whether to display the chart title.



> **Note:**
> By default, chart property settings only apply to the currently selected chart. You can click **Apply to All** to apply the set style to all charts in the current editing area.

   - The Daily Department Staff Count, Daily Entry/Exit Statistics by Time Period, Daily Entry/Exit Statistics by Area charts require configuration of the statistical scope and table headers. For details, please refer to Data Charts Description.
   - For the **Employees Present** card, it is necessary to select statistical areas (multiple areas allowed). If no area is selected, the statistics will include all areas.



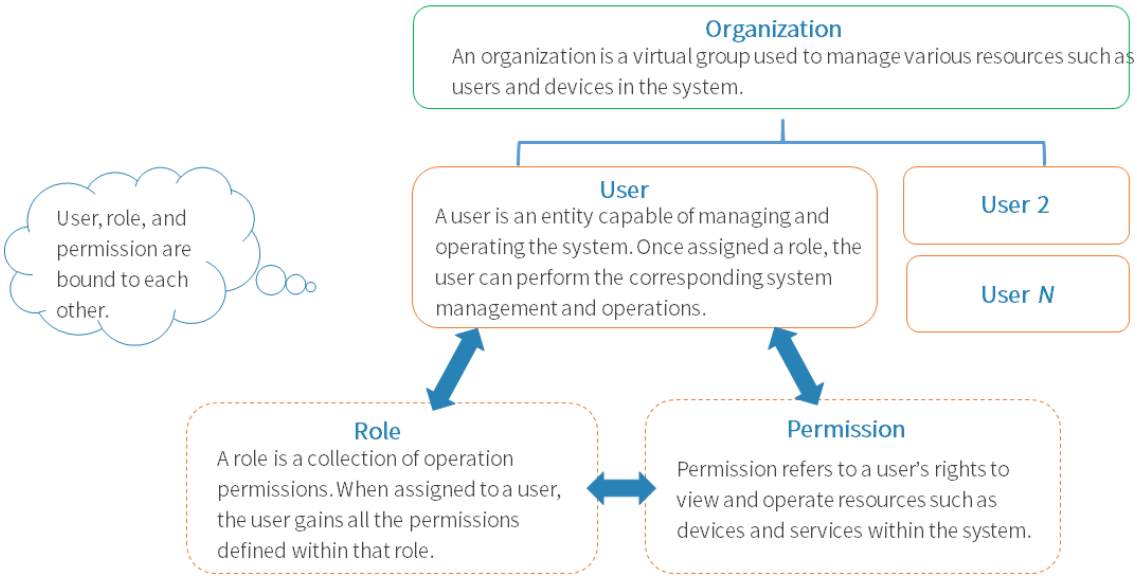
6. Click **Save**.
7. Click ⟵ in the upper-left corner to exit. Click the tick (√) in the upper-right corner of the template to set it as the active template. Now, you can call it in **Data Dashboard**.

6 User Management

Go to **Basic Configuration** > **User Management**.

Manage the users who log in and use the system, and assign the service permissions to individuals to achieve refined permission management.

The concepts involved are explained below:



6.1 Organization Management

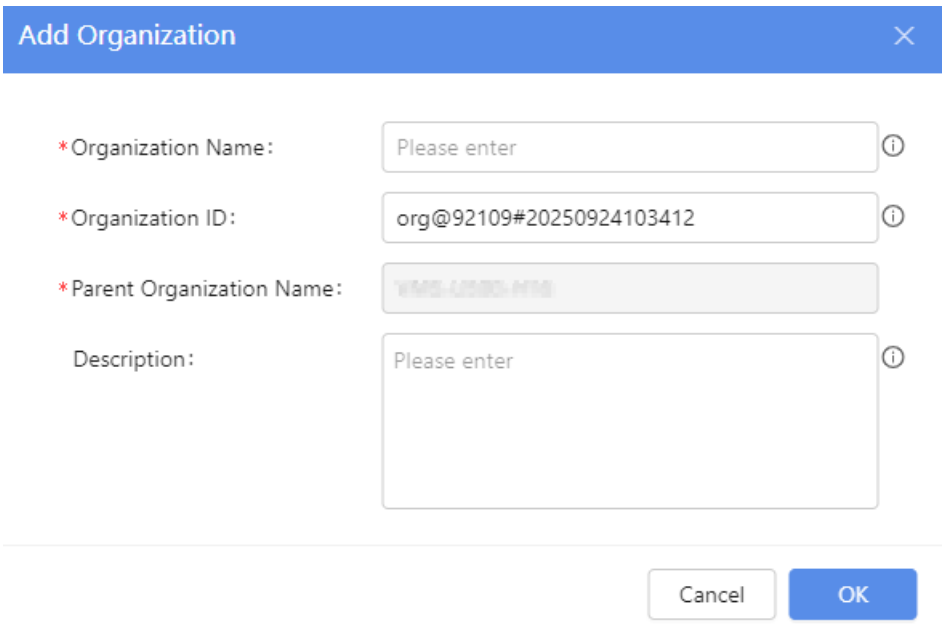
Organization is a virtual concept used to group and manage various system resources, such as users and devices. With organizations, you can precisely manage users' operational permissions for different resources. It is recommended that organizations plan according to the actual permission divisions.

Add Organization

Note: Up to 26 levels of organizations under the local domain are allowed (including the local domain).

1. Select a parent organization and then click + next to **Organization List**.

Figure 6-1: Add Organization



2. Enter the organization name, ID, and description.

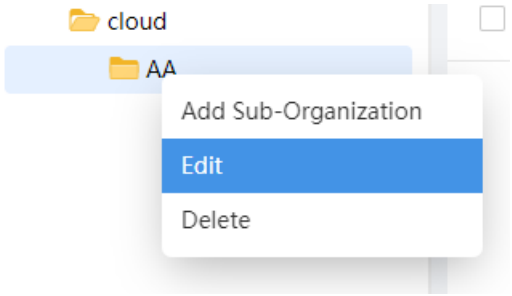
   Note: The organization ID must be unique.

3. Click **OK**.

Edit Organization

Right-click on an organization in the local domain and click **Edit** to edit the organization name and description.

Figure 6-2: Edit Organization



Delete Organization

Right-click on an organization in the local domain and click **Delete** to delete the organization.

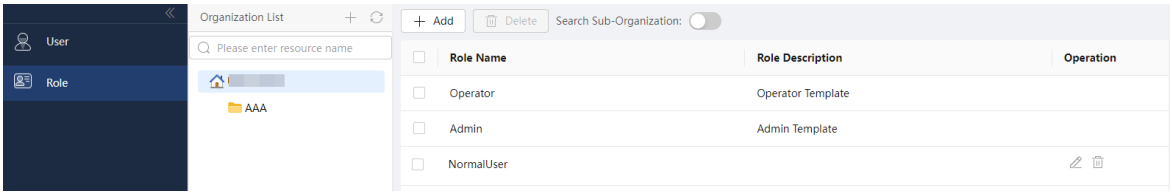
Note: If there are any users, roles, or sub-organizations under the organization, it cannot be deleted.

6.2 Role Management

Manage roles and role permissions.

Role is a collection of operation permissions. After a role is assigned to a user, the user has all permissions defined in the role. Role management facilitates the management and assignment of user permissions.

Figure 6-3: Role Management



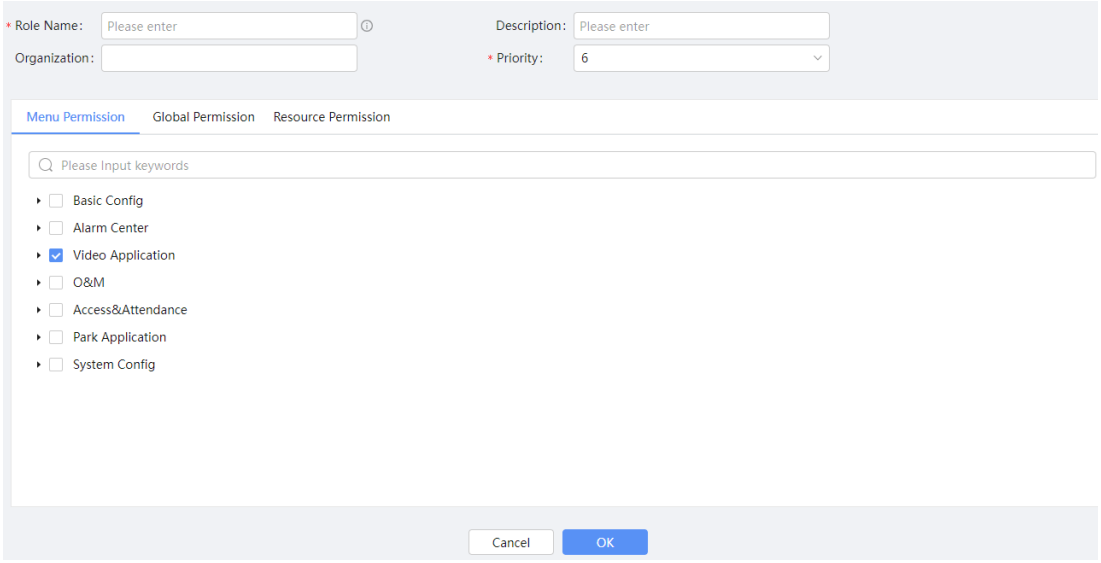
Permissions for role follow these principles:

Principle	Description
Depth First	If different permissions are configured for both the child and parent organizations simultaneously, the permissions granted to the child organization take precedence when authenticating the child organization.
Inheritance	If a parent organization has permissions configured and its child organization does not, the child organization inherits the permissions of the parent organization.
Union	If a user is granted multiple role permissions, the user's permissions are the union of all assigned roles, with the highest priority role determining the precedence.

Add Role

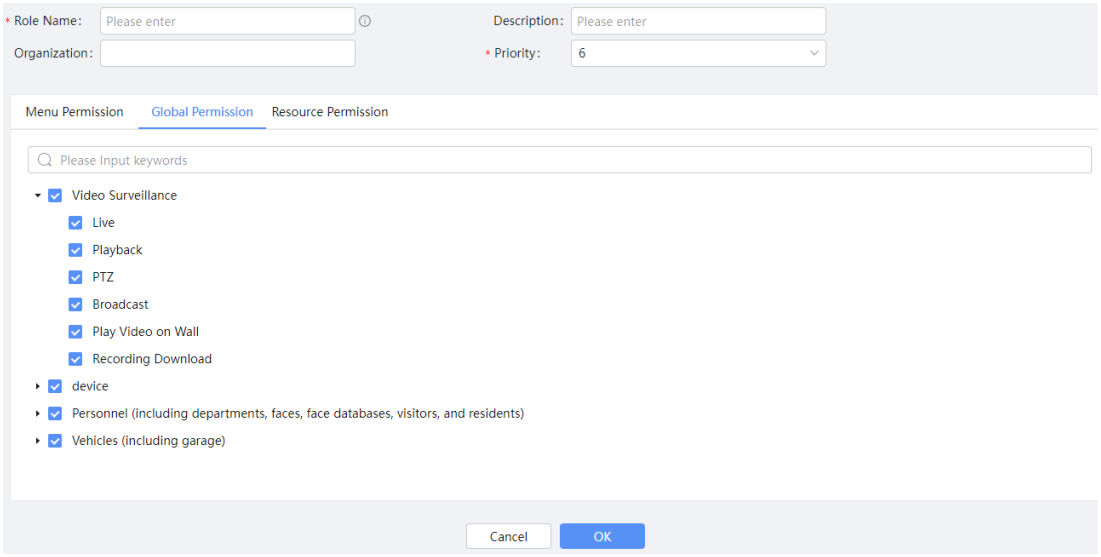
1. In the organization list, select an organization, and then select the **Role** tab. (Roles only apply to users and resources within the organization.)
2. Click **Add**.
3. Enter the role name and select permission(s).
   - Menu permission: Permission to view and operate the system application management menu. Menu permissions should be preferentially configured. If not pre-configured, the configured function permissions are still invalid.

Figure 6-4: Add Role-Menu Permission



- Global permission: Permission to operation functions and devices in the system, which includes the global permission and resource permission.

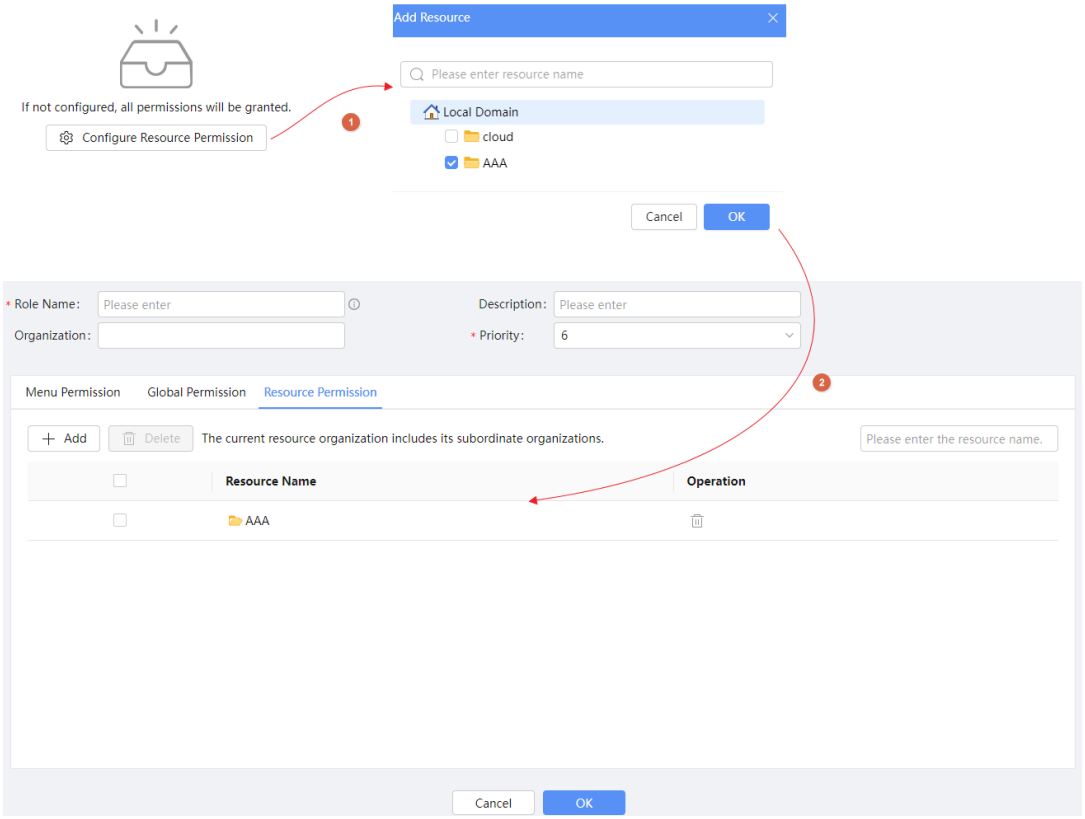
Figure 6-5: Add Role-Function Permission



- Resource Permission: Assign resource permissions to users by organization. If no organization is specified, the user will have full access to all resources within the role's organization and its sub-organizations. If an organization is specified, the user will only have access to resources within the specified organization and its sub-organizations.
  On the **Resource Permission** tab, click **Configure Resource Permission**, and then select organization(s).

Note:
Only organizations within the role's organization and its sub-organizations can be selected.

Figure 6-6: Add Role-Resource Permission

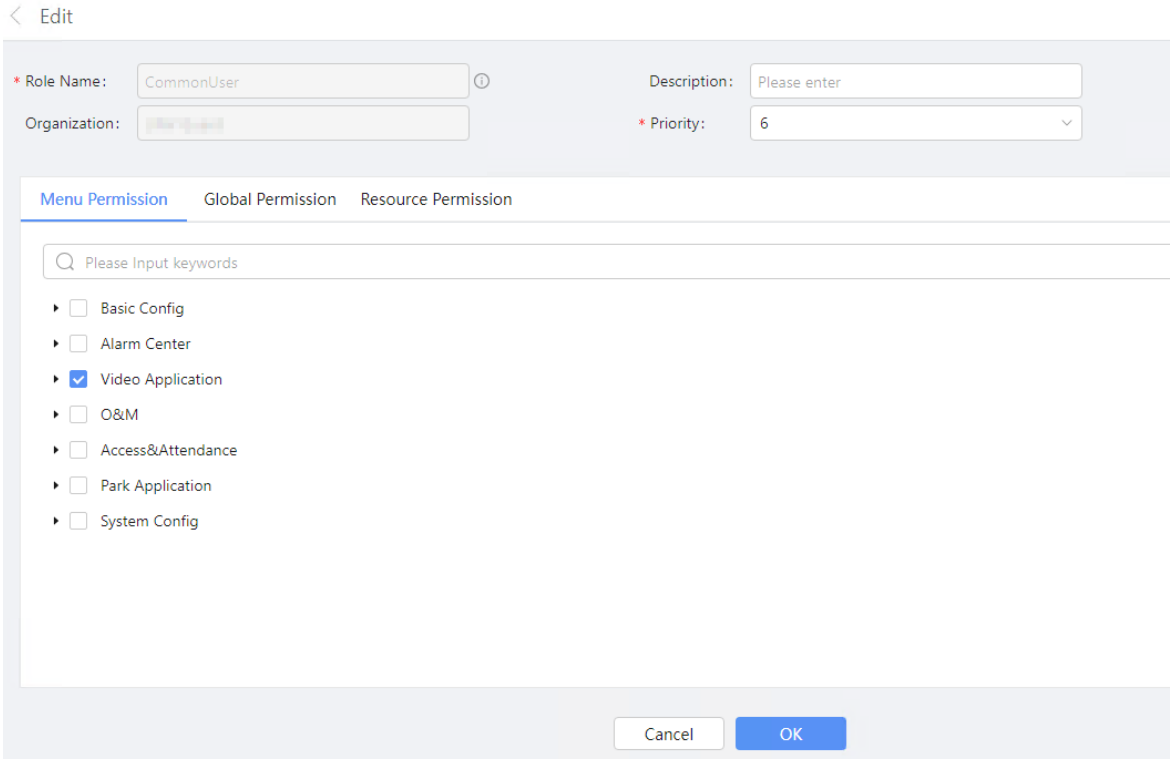


- Role priority: 1-63 levels, the lower the number the higher the priority. In resource preemption scenarios, roles with higher priority have superior preemption permission.

4. Click **OK**.

Edit Role

Click in the **Operation** column to edit the role description and permissions.



Delete Role

- Delete one by one: Click in the **Operation** column and confirm the deletion.
- Delete in batches: Select roles to delete, click **Delete**, and then confirm the deletion.

Note:

- The deleted role cannot be restored.
- Cannot delete roles that have been bound to any user.

6.3 User Management

Manage user information.

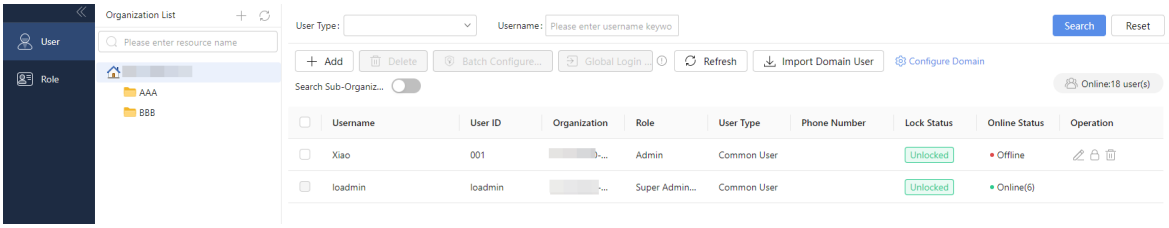
Users are entities that manage and operate the system. After being assigned role(s), user can log in to the system and perform the allowed operations.

The system allows simultaneous login to the same account from multiple clients. This simplifies user configuration and management, and allows normal operations with a small number of user accounts.

Note: The system has two default users: admin and loadmin.

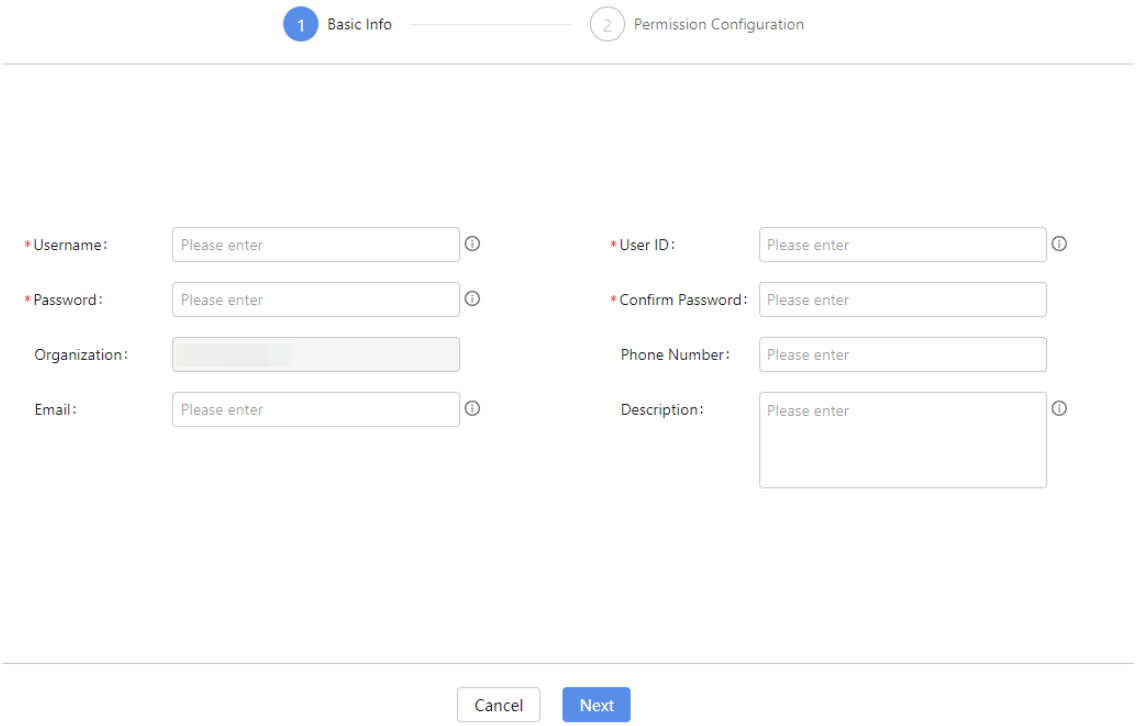
- Both have the role of the super administrator and the highest privilege in the system.
- Admin can grant/revoke the super administrator privilege to/from other users.
- Neither admin nor loadmin can be deleted.

Figure 6-7: User Management



Add User

1. In the organization list, select an organization, and then select the **User** tab.
2. Click **Add**.

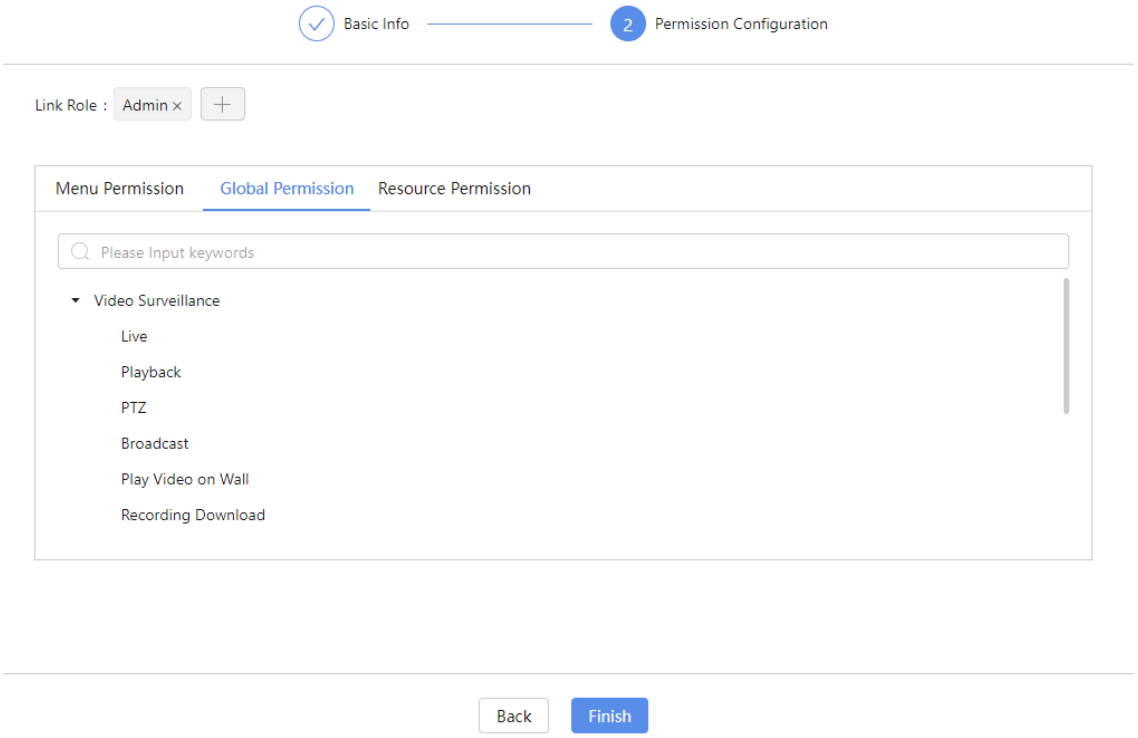


3. Enter the basic user information (fields with * are required), including username, user ID, password, and confirm password.

Note:

- The username and user ID must be unique.
- The password must be a strong password.

4. Click **Next** to go to the **Permission Configuration** page.

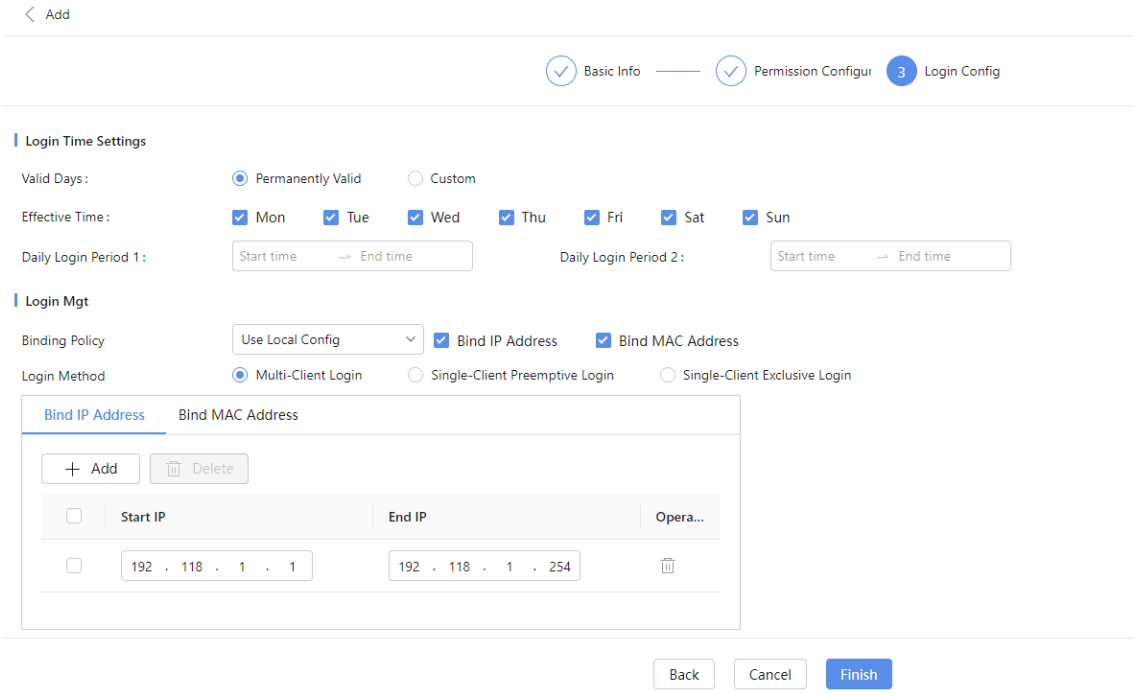


(1) Click ⊞ next to **Link Role** to expand the role list. Select role(s). To create a new role, click **New Role** (see operations in Role Management).

Note:
Only roles within the same organization (including sub-organizations) as the user can be bound.

(2) Click **OK** to assign role(s).

5. (**Only admin users can configure**) Click **Next** to configure the allowed login time and login PCs for users.



Valid Days	• Permanently Valid: The user can always log in to the system. • Custom: Enter a number. After saving the configuration, the user will automatically become invalid after the specified number of days, and invalid users will not be able to log in to the system.
Effective Time	Select the dates when the user is allowed to log in. **Note:** At least one date must be selected, otherwise, the user will not be able to log in even if the user is within the validity period.
Daily Login Period	Set the time periods during which the user can log in each day (supports two time periods). If no time period is set, the user is allowed to log in throughout the day.
Login Mgt	• Use Global Config: The settings will follow the Global Login Management global configuration. • Use Local Config: Configure the binding policy and login method for the user here.
Binding Policy	Only allows the user to log in from specific IP addresses and MAC addresses. • Bind IP Address: Add the allowed IP address range for login. • Bind MAC Address: Add the allowed MAC addresses for login. **Note:** If a MAC address has been bound to this user account, the user must first download and install the MAC address collection plugin as prompted when logging in to the client. Login will only be allowed after the MAC address is successfully matched.
Login Method	• Multi-Client Login: The same username can log in on multiple PCs simultaneously. • Single-Client Preemptive Login: The same username can only log in on one PC at a time. When the user logs in on one PC, the login session on the other PC will be forcibly logged out. • Single-Client Exclusive Login: The same username can only be logged in on one client at a time and cannot be preempted by another client.

6. Click **Finish**.

Edit User

Click in the **Operation** column to edit the user information.

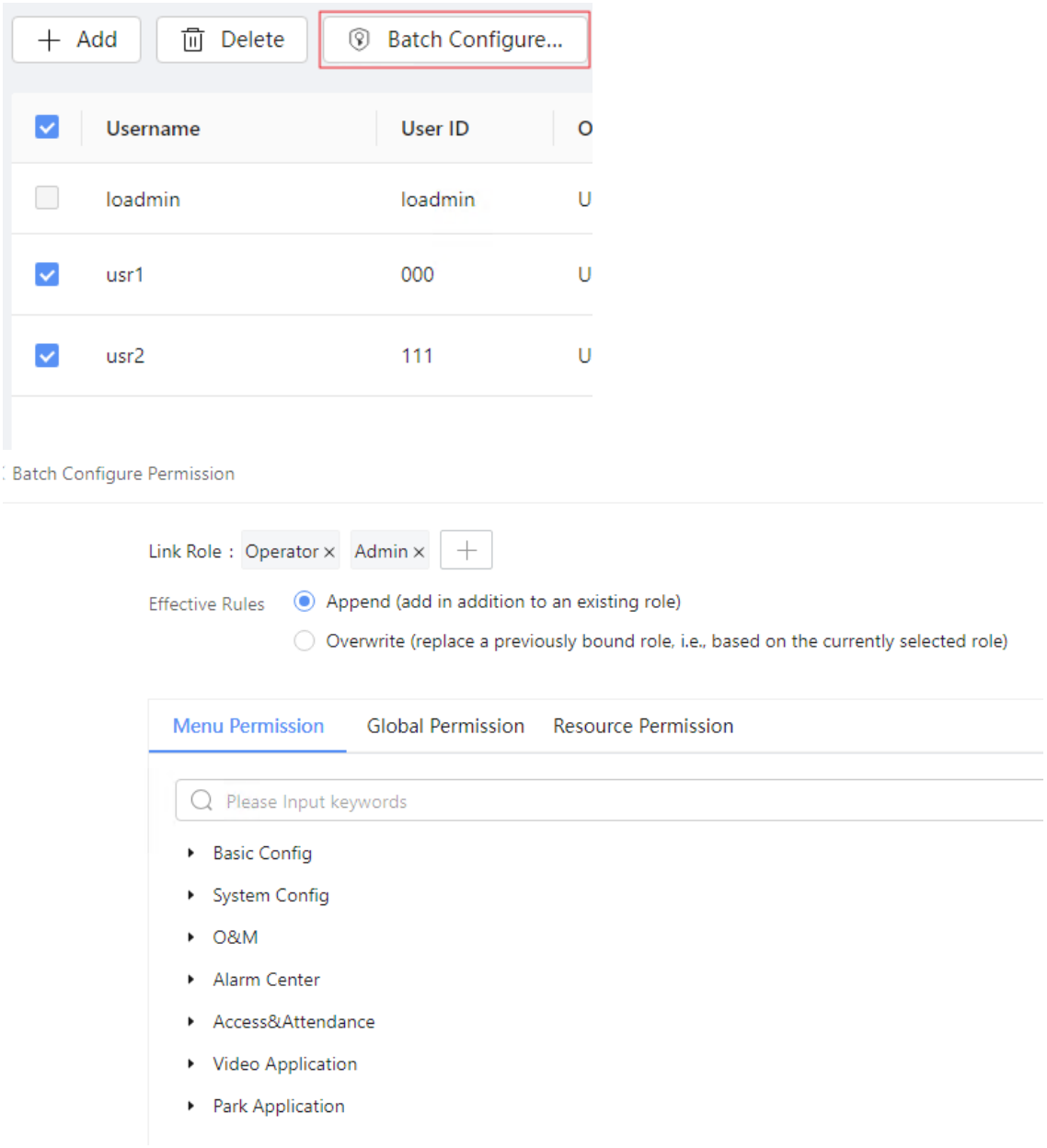
Note:

- The user ID and organization cannot be edited.
- Only admin can edit the user information of other super administrators.
- Editing AD domain users' username/password information is not supported in this system.

Batch Configure Permission

Assign role(s) to multiple users in batches.

1. Select users (≥2) and click **Batch Configure Permission**.



2. Click ⊞ next to **Link Role** to expand the role list. Select role(s) as needed. To create a new role, click **New Role** (see operations in Role Management).
3. Select an effect rule.
   - Append: Retain the existing linked role(s) and add new role(s).
   - Overwrite: Replace the linked role(s). i.e. The currently selected role(s) will take precedence.
4. Click **OK**.

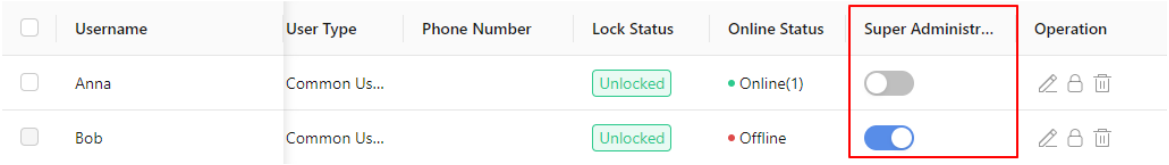
Lock/Unlock User

In the user list, click 🔒 in the **Operation** column to lock the user. Once locked, the user cannot log in to the system. Click again to unlock.

Set as Super Administrator

After logging in as an admin, click ⬭ for the user to set the user as a super administrator. Click again to revoke.

Note:
Only admin can designate other users as super administrators.

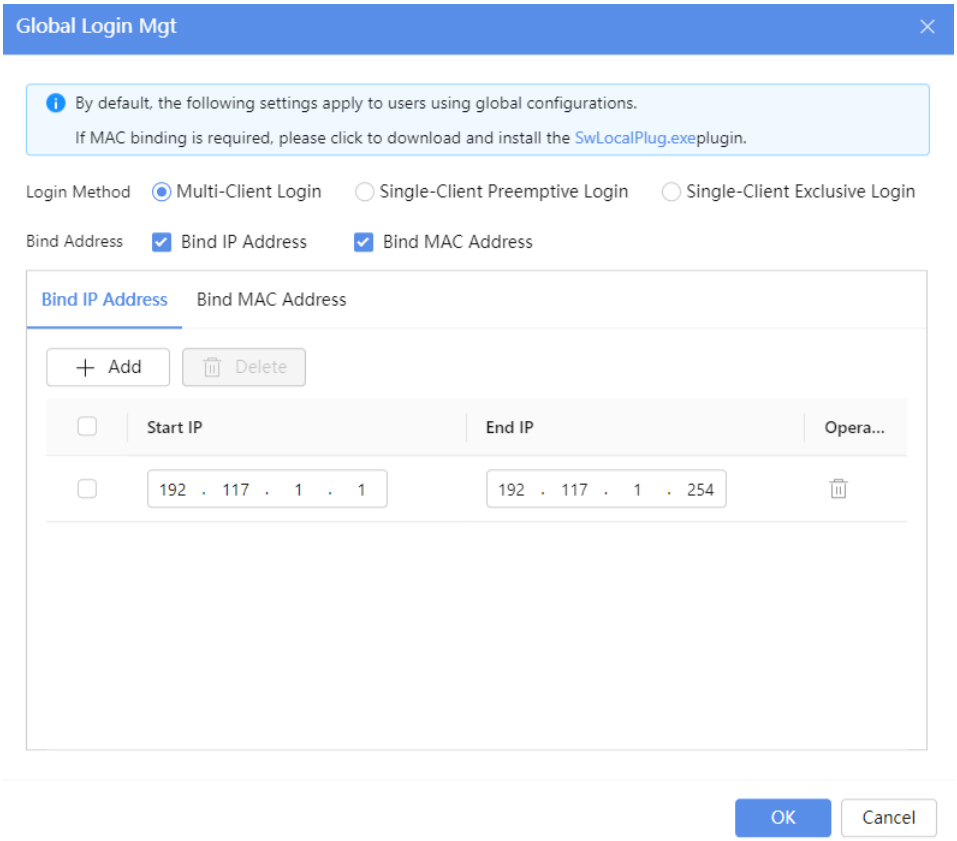


Global Login Management

The system supports globally restricting user login methods and login PCs. When the user login policy is set to **Use Global Config**, the settings here will take effect.

Note:
Only admin can configure the global login rules.

1. Log in as admin, and click **Global Login Management**.
2. Configure the login rules, and then click **OK**.



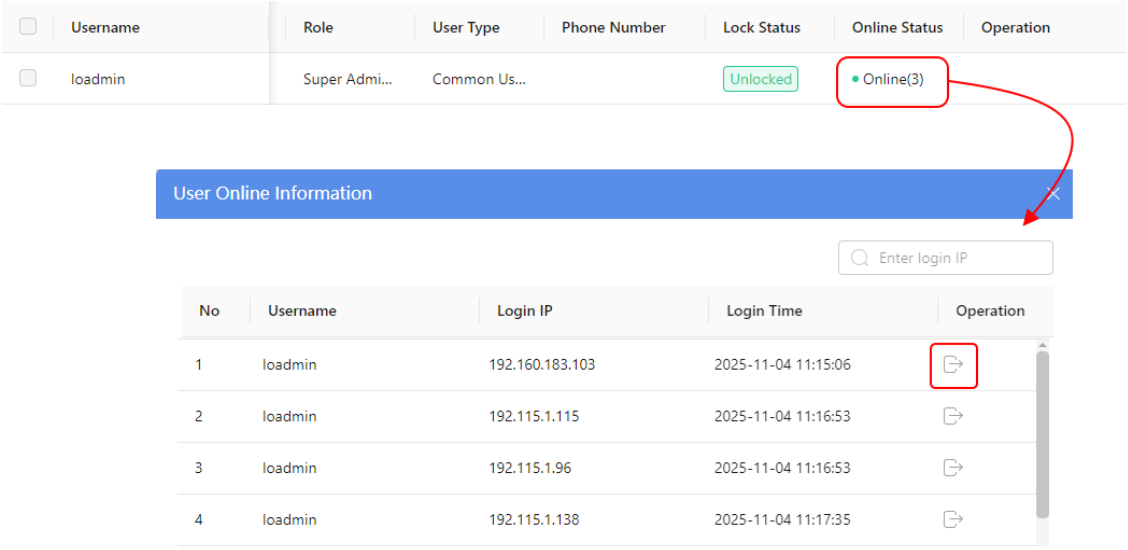
Login Method	• Multi-Client Login: The same username can log in on multiple PCs simultaneously. • Single-Client Preemptive Login: The same username can only log in on one PC at a time. When the user logs in on one PC, the login session on the other PC will be forcibly logged out. • Single-Client Exclusive Login: The same username can only be logged in on one client at a time and cannot be preempted by another client.
Bind Address	Only allows the user to log in from specific IP addresses and MAC addresses. • Bind IP Address: Add the allowed IP address range for login. • Bind MAC Address: Add the allowed MAC addresses for login. **Note:** If a MAC address has been bound to this user account, the user must first download and install the MAC address collection plugin as prompted when logging in to the client. Login will only be allowed after the MAC address is successfully matched.

3. For non-admin users, after logging in, hovering over the **Global Login Management** button will show the login method.

Manage Online Users

The system supports viewing the number of online users and forcing users offline.

1. Click the **Online Status** column corresponding to an online user to view the user's login IP and login time.



2. Click the corresponding to force a login session offline.

Note:

- If a user has logged in on multiple pages on the same PC, only the page corresponding to the login time will be logged out. The login time is based on the server's time.
- After a user is forced offline, any further actions on the page will trigger an error message and immediately log the user out. If no actions are taken, the user will be automatically logged out when the page's keep-alive mechanism fails.

Delete User

- Delete one by one: Click in the **Operation** column and confirm the deletion.
- Delete in batches: Select user(s) to delete, click **Delete**, and then confirm the deletion.

Note:

- The deleted user cannot be restored.
- Only admin can delete other super administrators (excluding loadmin).
- Neither admin nor loadmin can be deleted.

6.4 AD Domain User

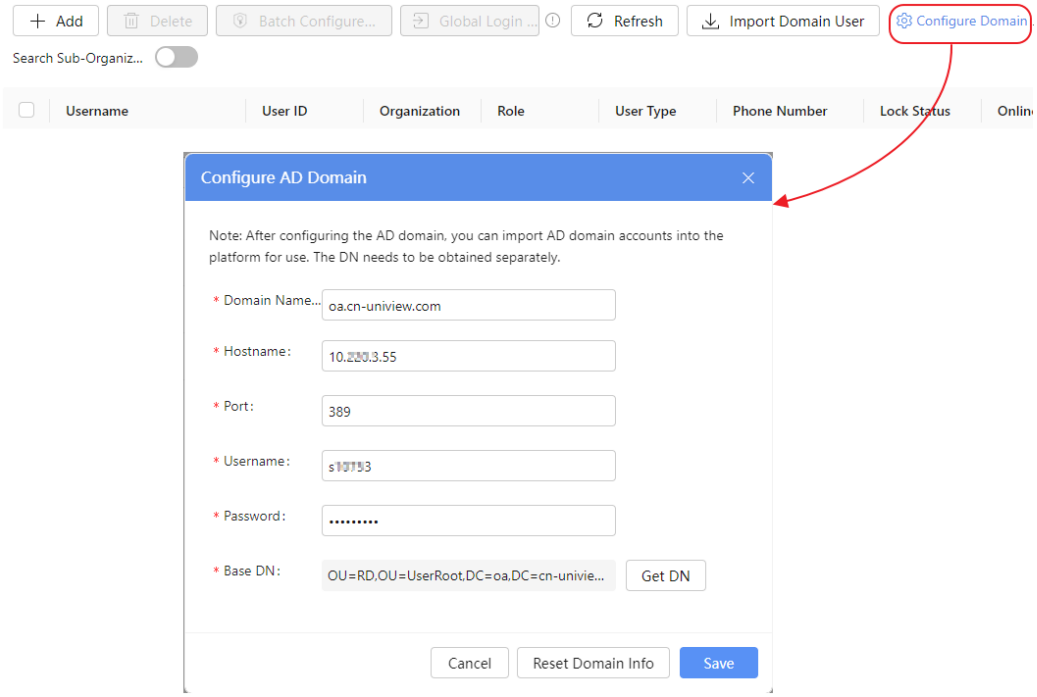
The system supports integration with AD Domain and importing AD Domain users, allowing login to the system using AD domain user accounts.

AD Domain (Active Directory Domain) refers to the directory service used by Windows servers, which stores company computer information, user accounts/passwords, groups, and other data. It acts as an organizational unit. Companies can define security boundaries using AD Domain, and employees can authenticate and log in to the company's domain system via domain accounts. While operating within the domain, employees must adhere to the company's defined security policies. The domain manager allows remote management and configuration across multiple regions, enabling centralized management.

Once the company’s internal AD domain is integrated into this system, administrators can configure employee permissions, allowing employees to log in to the system via domain accounts/passwords. This eliminates the need for users to remember multiple usernames and passwords, facilitating secure and efficient login management

Configure AD Domain

1. Go to **User Management > User**, click **Configure Domain**.



2. Fill in the AD Domain information by referring to the table below.

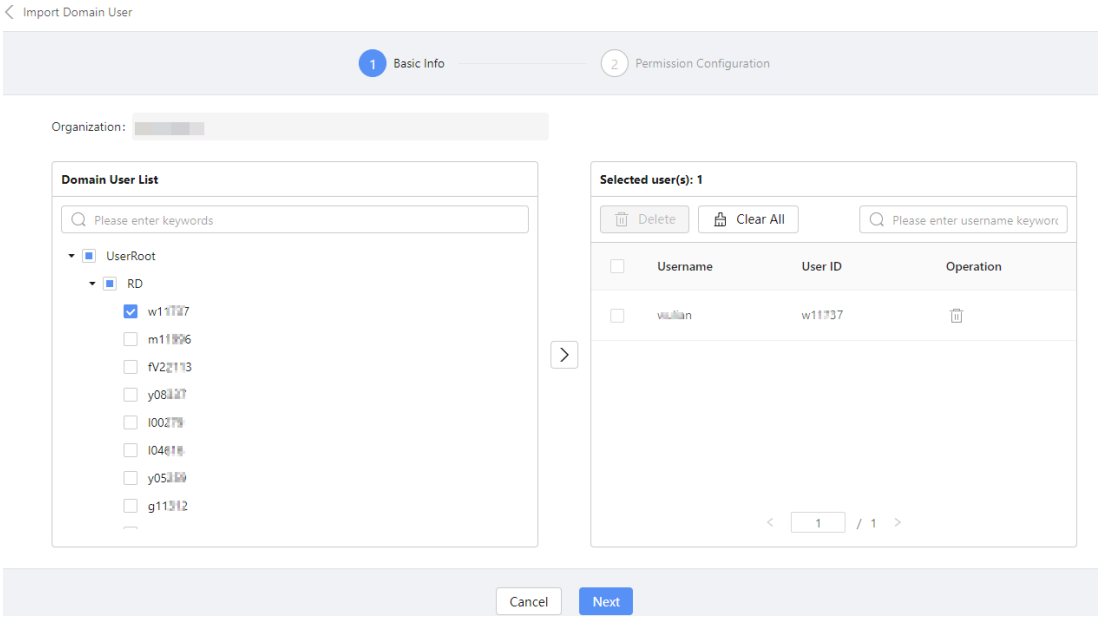
Parameter	Description
Domain Name	AD Domain name, obtained from the AD domain side.
Hostname	IP address or hostname of the AD domain server.
Port	Port number of the AD domain server.
Username/Password	Username and password of the AD domain administrator. **Note:** This user serves as the credential for interaction with the domain. Once saved, do not modify the user's password in the AD domain, as this may cause password errors when importing domain users.
Base DN	Click **Get DN** to obtain the root directory name of the AD domain in order to query the AD domain user list. Once the base DN is correctly obtained, click **Save** to save the configuration to VMS.

3. After configuration, click **Save** to integrate with the AD domain.

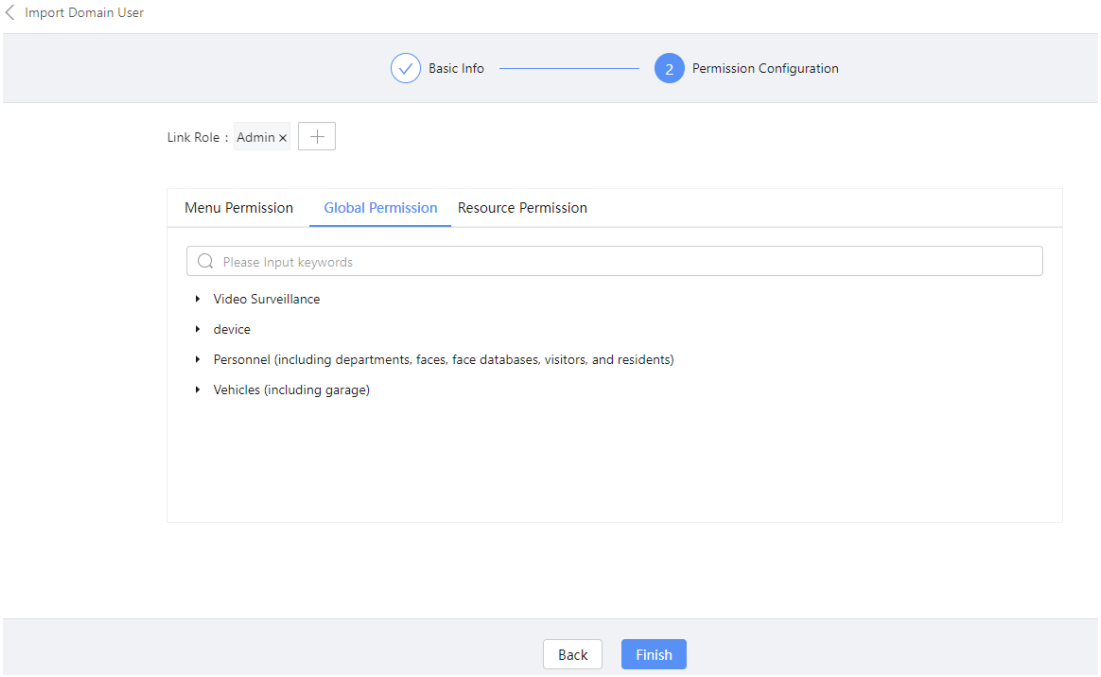
Import Domain Users

1. Go to the **User Management > User**.
2. Click **Import Domain Users** above the user list.
3. Follow the steps to add domain users, configure permissions, and set login rules.

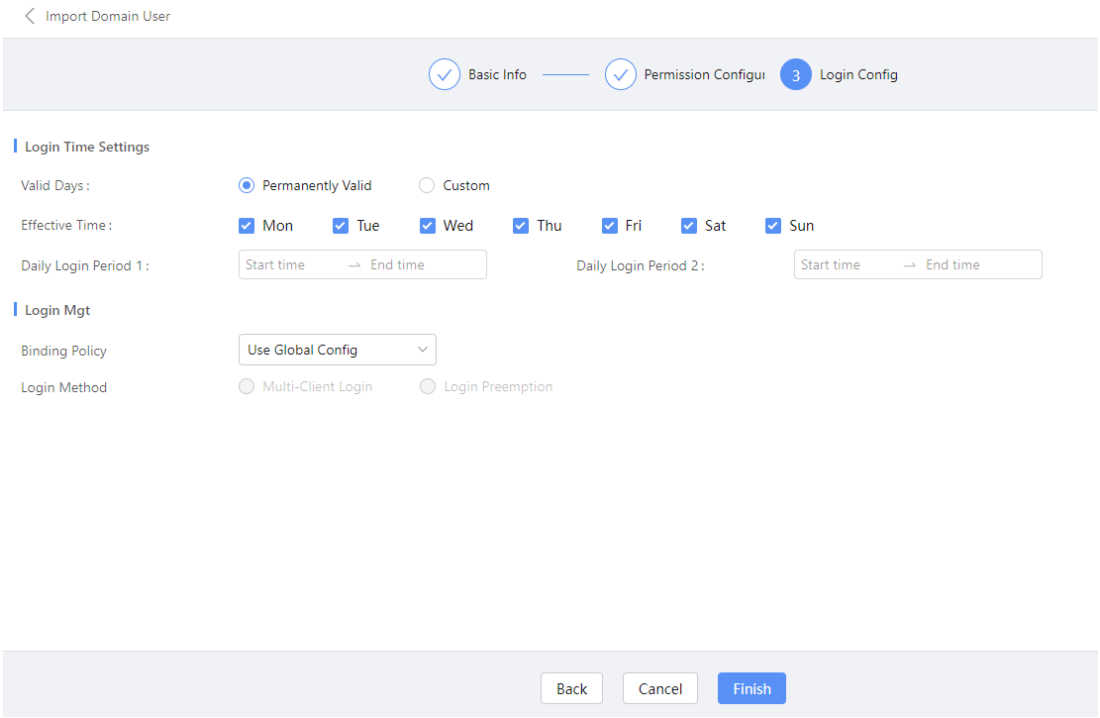
   (1) Add domain users: Select the domain users that need to be added to this system.



(2) Configure permissions: Bind roles to the domain users, granting them the permissions associated with those roles.



(3) (**Only admin users can configure**) Configure the allowed login time and login PCs for users.



Domain User Login

On the login page, select **AD Domain Login** as the account type. Enter the imported AD domain user credentials (user ID/password), and after successful verification, you can log in.

7 Device Management

Go to **Basic Config** > **Device Mgt**.

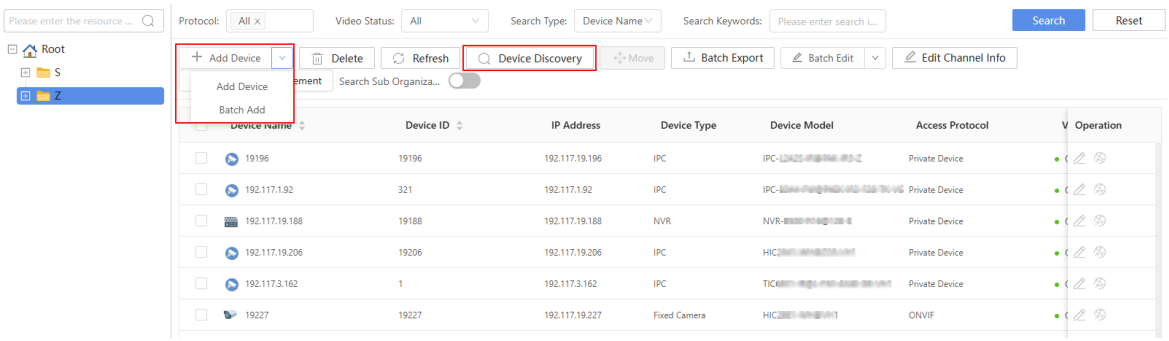
You can add various park devices to platform and configure them. For supported device types, see Supported Devices.

7.1 Frontend Device

Frontend devices include cameras, access control devices, network video recorders, etc., which are used to access the image and video data collected in the field, as well as the target attributes and alarm data generated by intelligent analysis.

Choose a way to add your device:

- Device Discovery: Discover devices on the same LAN automatically and select them one by one or in batches from the search results for adding.
- Add One by One: Enter information such as the device's IP address or device ID to add devices one by one.
- Batch Add: Import devices in batches using a template.

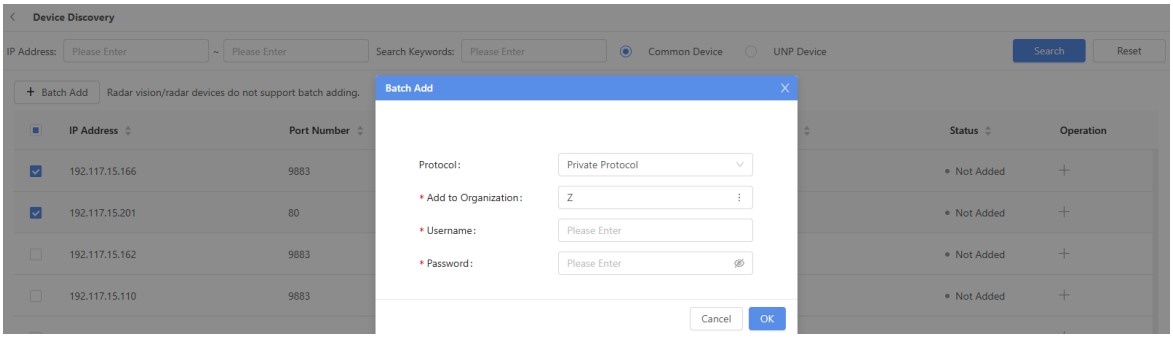


Note:
In the device list, the **Video Status** column displays the online status of the video channel, while the **Image Status** column displays the online status of the image channel. For offline channels, hover over **?** to view the causes of the offline status.

7.1.1 Device Discovery

Discover and add devices (camera, LPC, LPR, NVR, face recognition terminal, general access control device, access controllers, indoor station, outdoor station (door station/zone station), radar, radar vision) in specified network segments on the same LAN as the platform.

1. Click **Device Discovery**.
2. Specify the network segment to search by setting the start and end IP address. Up to 8 network segments are allowed, i.e., 192.168.1.1-192.168.9.255.
3. Click **Search**.
4. Click ＋ in the **Operation** column to add devices one by one or select multiple devices and click **Batch Add** to add devices in batches.
   - Protocol Type: ONVIF/Private.
   - Username/Password: Username and password of device login.



7.1.2 Add One by One

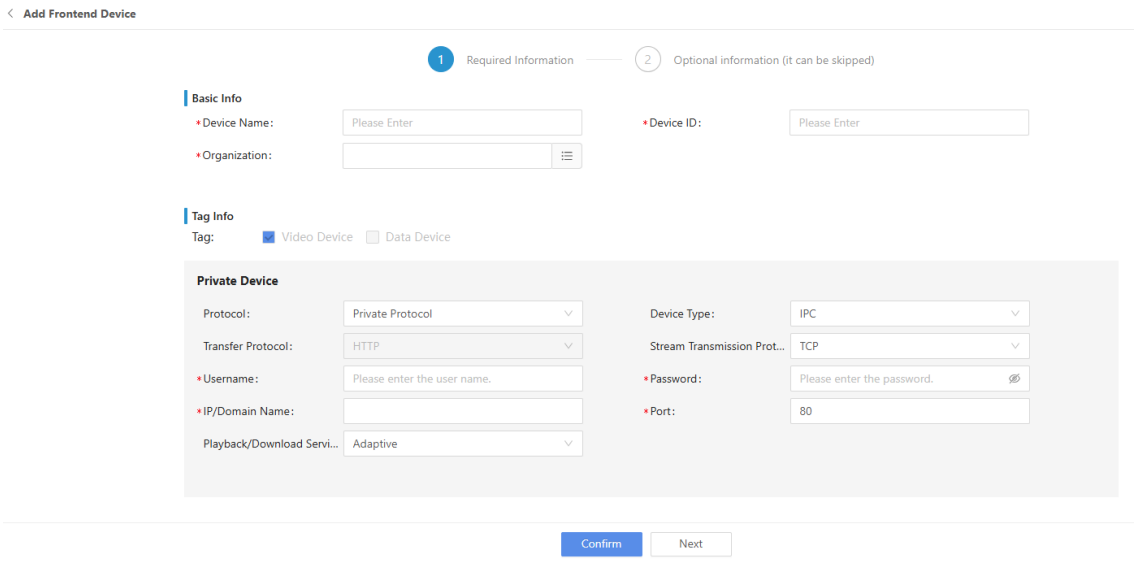
Add frontend devices one by one.

Go to **Device Mgt** > **Frontend Device**. Select an organization for the device in the left-side organization tree and click **Add Device** > **Add Device**.

7.1.2.1 Private Device

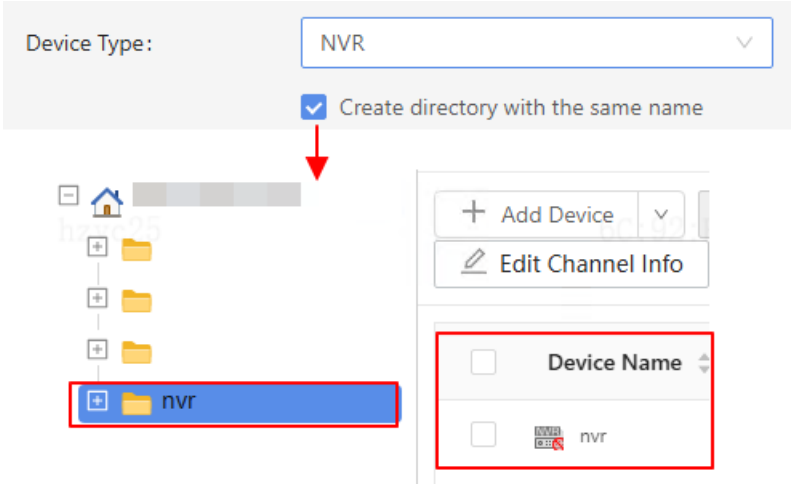
Add devices such as camera, LPC (license plate capture camera), LPR (license plate recognition camera), NVR (network video recorder), Smart Box (intelligent edge computing server), EIA (intelligent edge analysis server), Radar, indoor station, outdoor station (door station/zone station), face recognition terminal, general access control device, access controller, elevator controller, speed gate & turnstile, etc., via Uniview's private protocol (LAPI).

1. On the **Add Frontend Device** page, select **Video Device**.
2. Set **Protocol Type** to **Private Protocol**.

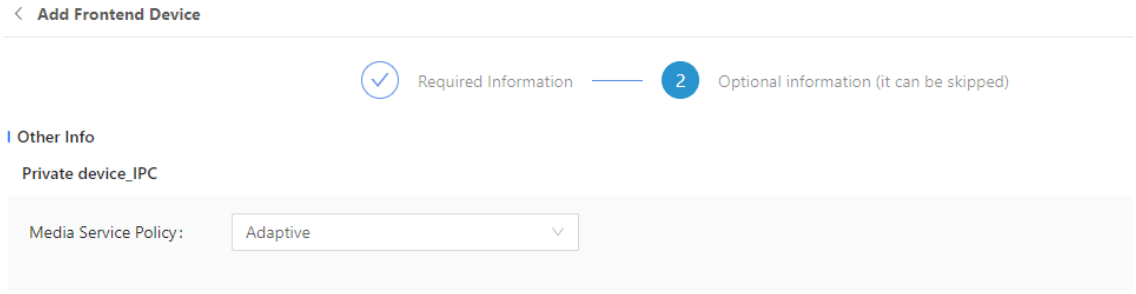


3. Configure the required parameters. The parameters available may vary with device model. Please refer to the actual interface.

Parameter	Description
Device Name	Device name.
Device ID	Unique device ID in the local domain. No format requirements. **Note:** The device ID must match the one on Device's Web interface. Otherwise, the device cannot go online.
Organization	Organization that the camera belongs to.
Device Type	IPC, LPC, LPR, NVR, Smart Box, EIA, Radar, Radar-Video fusion camera,indoor station, outdoor station (door station/zone station), face recognition terminal, general access control device, access controller, elevator controller, speed gate & turnstile. **Note:** • General access control device: Refers to the OER-SR12/22/42 series access controllers. • Access controller: Refers to the OER-601/602/604/501/502/504 serials access controllers. • Speed gate & turnstile: Refers to the OFP-B3-8501 serials speed gates. Models are subject to change. Please contact the technical support for details.
Create directory with the same name	Configurable when the device type is NVR. • Selected: A sub-organization, named after the device, will be created under the parent organization. The NVR will then be added to this identically named organization. This facilitates locating the NVR in the organization tree by searching the organization name.

Parameter	Description
	 • Unselected: The NVR will be added directly under the parent organization.
Transfer Protocol	After selecting the device type, the system will show the transfer protocols supported by the device. • Regular radar/Radar-Video fusion camera: Select WebSocket. • Visual intelligent alarm detector (ADRDV351, a radar device): Select HTTP. • IPC/NVR/Access Control and other devices: Select HTTP. **Note:** HTTP refers to ordinary network signaling interactions; while WebSocket (also known as HTTP over WebSocket), is suitable for scenarios involving NAT traversal.
Stream Transmission Protocol	TCP or UDP. Please select it according to the actual network situations.
Username/Password	Username and password of device login (required).
IP Address/Domain Name	IP address or domain name of the device.
Port No.	The registered port number of the device (default: 80).

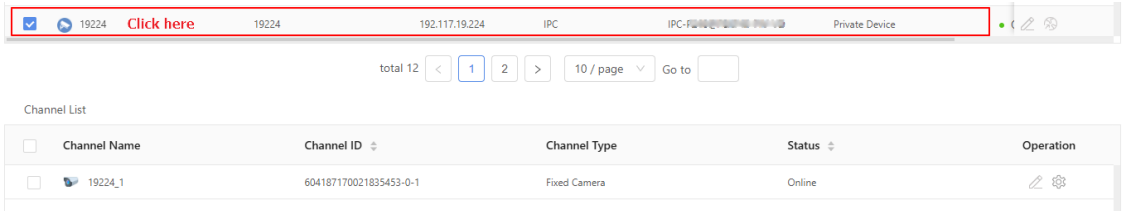
4. Click **Confirm**.
5. (Optional) Click **Next** and fill in the optional information.



Parameter	Description
Media Service Policy	• The default is **Adaption**. All MSs share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When an MS is available but has insufficient forwarding capacity, the Direct Connection First policy will be adopted.

Parameter	Description
	• You can choose whether to bypass the specified MS as needed. If you want to forward multiple media streams, specify the MS.

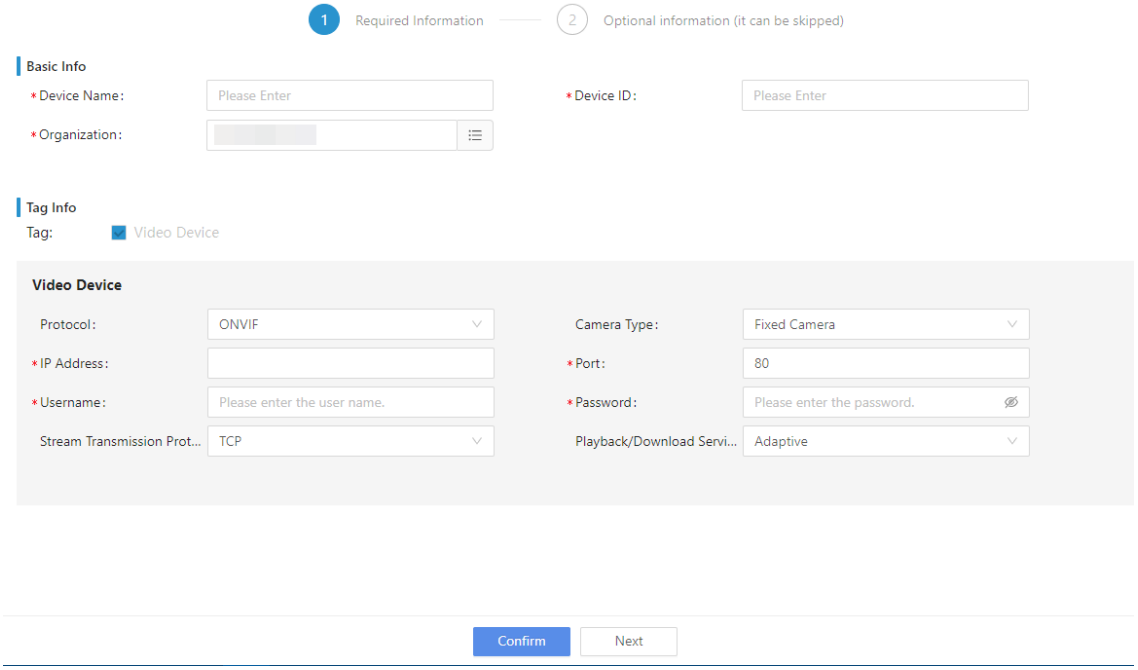
6. Click **OK**.
7. In the **Frontend Device** list, select the device, and its channels are displayed below.



7.1.2.2 ONVIF Camera

Add cameras via the ONVIF protocol.

1. On the **Add Frontend Device** page, select **Video Device**.
2. Set **Protocol Type** to **ONVIF**.

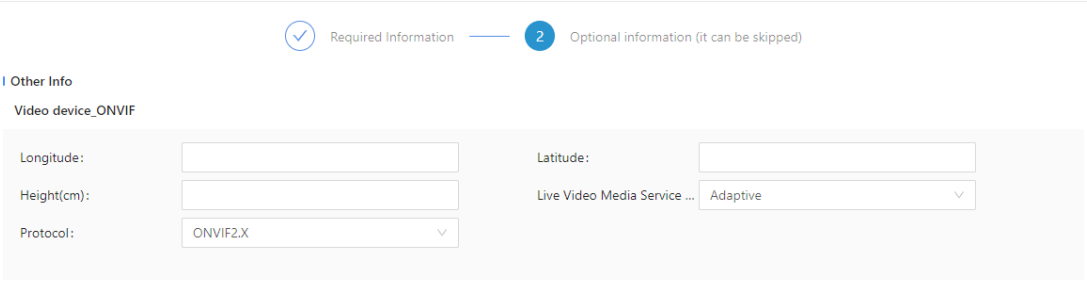


3. Configure the required parameters.

Parameter	Description
Device Name	Device name.
Device ID	Custom a unique device ID in the local domain. No format requirements.
Organization	Organization that the camera belongs to.
Camera Type	14 types available (Fixed Camera, PTZ Camera, Fixed HD Camera, HD PTZ Camera, In-Vehicle Camera, Uncontrollable SD Dome Camera, Uncontrollable HD Dome Camera, Isolate Video Access, Motorized Lens Camera, Ultra Clear Face Capture Camera, Multi-eye Splicing Camera, Access Control Device, Fixed Dome Camera, Vari-Focal Fixed Dome Camera).
IP Address	IP address of the camera.
Port No.	Port number on which the camera receives messages.
Username	Camera's username (required when authentication is enabled).
Password	Camera password (required when authentication is enabled).

Parameter	Description
Stream Transmission Protocol	TCP or UDP. Please select it according to the actual network situations.
Playback/Download Service Policy	• Auto-Adaptation (default): The MS server automatically load balances the stream sent by the IPC to the client (unless the client player and decoder in the local domain is configured as Direct Connection First). If the forwarding capacity of the MS server is insufficient, the IPC will send the stream directly to the client. • You can choose whether the stream is forwarded via the MS server as needed. It is recommended to use the MS server for forwarding if there are multiple media streams.

4. Click **Confirm**.
5. (Optional) Click **Next** and fill in the optional information.



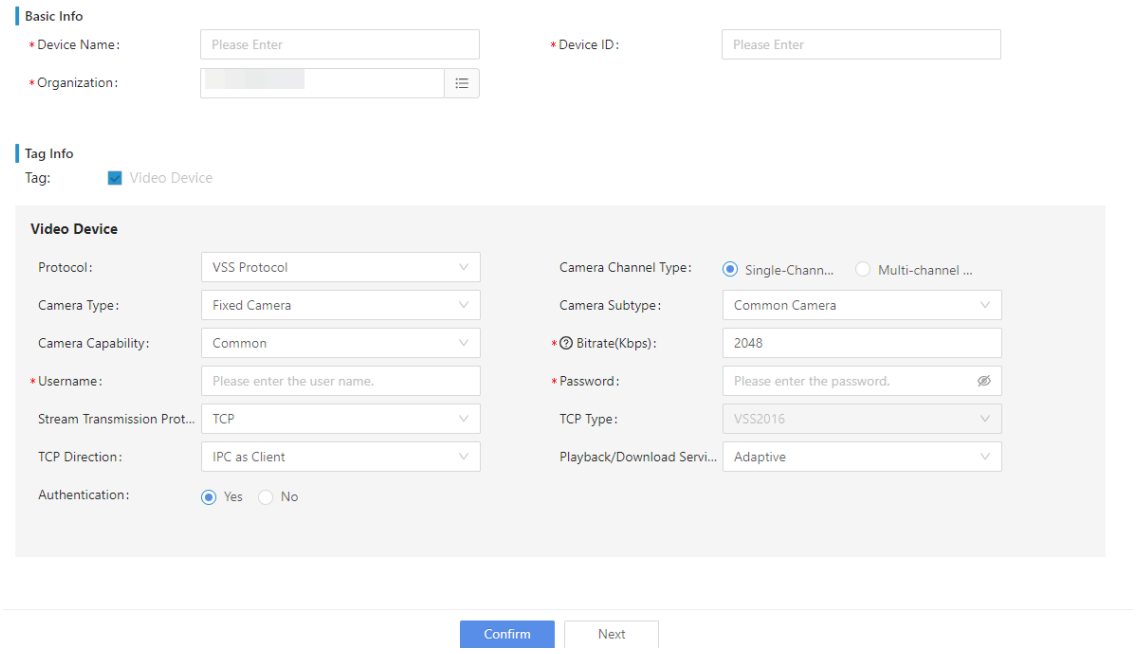
Parameter	Description
Longitude	Longitude of the camera's location.
Latitude	Latitude of the camera's location.
Height	Height of the camera's location.
Live View Service Policy	• Auto-Adaptation (default): The MS server automatically load balances the stream sent by the IPC to the client (unless the client player and decoder in the local domain is configured as Direct Connection First). If the forwarding capacity of the MS server is insufficient, the IPC will send the stream directly to the client. • You can choose whether the stream is forwarded via the MS server as needed. It is recommended to use the MS server for forwarding if there are multiple media streams.

6. Click **OK**.

7.1.2.3 VSS Single-Channel Camera

Add single-channel cameras via the VSS protocol.

1. On the **Add Frontend Device** page, select **Video Device**.
2. Choose **VSS Protocol** and **Single-Channel Camera**, as shown in the figure below.

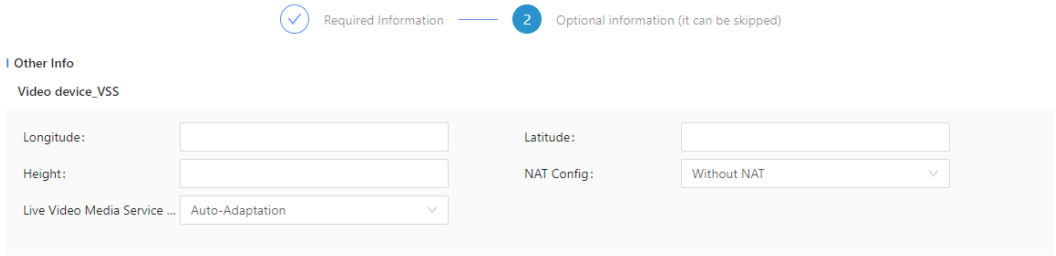


3. Configure the required parameters.

Parameter	Description
Device Name	Device name.
Device ID	Unique device ID in the local domain. **Note:** • The device ID must match the one on the camera's Web interface. Otherwise, the device cannot go online. • Follow the VSS code rules: 20 digits, digits 11-13 must be 119-129, 131, or 132.
Organization	Organization that the camera belongs to.
Camera Type	14 types available (Fixed Camera, PTZ Camera, Fixed HD Camera, HD PTZ Camera, In-Vehicle Camera, Uncontrollable SD Dome Camera, Uncontrollable HD Dome Camera, Isolate Video Access, Motorized Lens Camera, Ultra Clear Face Capture Camera, Multi-eye Splicing Camera, Access Control Device, Fixed Dome Camera, Vari-Focal Fixed Dome Camera).
Camera Subtype	Choose common camera, deep learning camera (to recognize pedestrians, non-motor vehicles, motor vehicles, and extract structured attributes), private camera (camera connected via private protocol to capture image data; the corresponding image asset information is required).
Camera Capability	Choose the camera capability: Common/Support Area People Counting/Support Tripwire People Counting/Support Area and Tripwire People Counting.
Bitrate	Encoding rate. Calculate storage space based on the bitrate.
Username	Camera's username (required when authentication is enabled).
Password	Camera password (required when authentication is enabled).
Stream Transmission Protocol	The default is **TCP**. If you choose **TCP**, you need to choose the TCP type (VSS2014/ VSS2016) and TCP direction (IPC as Client or as Server). Please select it according to the actual network situations.
Playback/Download Service Policy	• The default is **Auto-Adaption**. All MSs share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When an MS is available but has insufficient forwarding capacity, the Direct Connection First policy will be adopted.

Parameter	Description
	• You can choose whether to bypass the specified MS (group) as needed. If you want to forward multiple media streams, specify the MS (group). • This configuration takes effect only for playback and download.
Authentication	The default is **Yes**. • **Yes** (authentication enabled): The IPC verifies the username and password stored on the server when connecting to the server; the IPC can go online only when the authentication is successful. • **No** (authentication disabled): The IPC can go online without username and password required.

4. (Optional) Click **Next** and fill in the optional information.



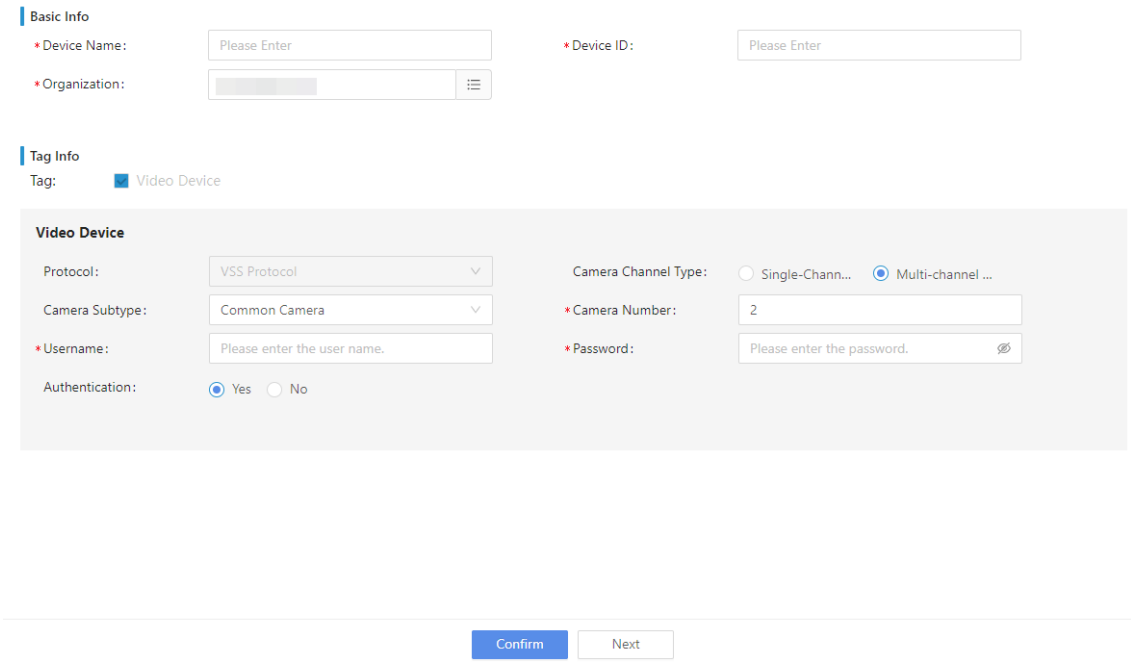
Parameter	Description
Longitude	Longitude of the camera's location.
Latitude	Latitude of the camera's location.
Height	Height of the camera's location.
NAT Config	• If the IPC is behind the NAT and the local domain is in front of the NAT, choose **IPC Behind the NAT**. • If the local domain is behind the NAT and the IPC is in front of the NAT, choose **IPC in front of the NAT**. • If IPC and the external domain are behind different NATs, choose **IPC and Local Domain Behind Different NATs**. • If data streams of the IPC do not need to traverse the NAT, choose **Without NAT**.
Live Video Media Service Policy	• The default is **Auto-Adaption**. All MSs share the load (except when the client player or decoder in the local domain adopts the Direct Connection First policy). When an MS is available but has insufficient forwarding capacity, the Direct Connection First policy will be adopted. • You can choose whether to bypass the specified MS as needed. If you want to forward multiple media streams, specify the MS. • This configuration takes effect only for live videos.

5. Click **Confirm**.

7.1.2.4 VSS Multi-Channel Camera

Add multi-channel cameras via the VSS protocol. Multi-channel cameras have multiple video channels (multiple lens).

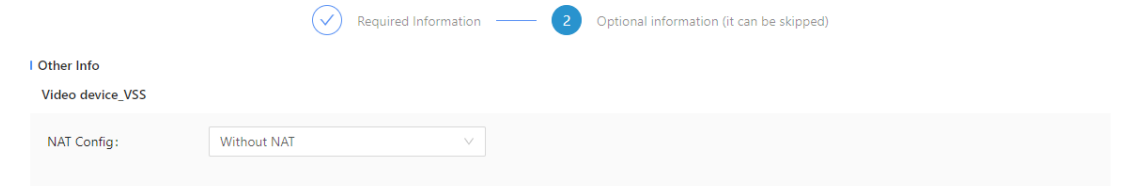
1. On the **Add Frontend Device** page, select **Video Device**.
2. Choose **VSS Protocol** and **Multi-Channel Camera**, as shown in the figure below.



3. Configure the required parameters.

Parameter	Description
Device Name	Device name.
Device ID	Unique device ID in the local domain. **Note:** The device ID must match the one on the camera's Web interface. Otherwise, the device cannot go online.
Organization	Organization that the camera belongs to.
Camera Subtype	Choose common camera, deep learning camera (to recognize pedestrians, non-motor vehicles, motor vehicles, and extract structured attributes), private camera (camera connected via private protocol to capture image data; the corresponding image asset information is required).
Username	Camera's username (required when authentication is enabled).
Password	Camera password (required when authentication is enabled).
Authentication	The default is **Yes**. • **Yes** (authentication enabled): The IPC verifies the username and password stored on the server when connecting to the server; the IPC can go online only when the authentication is successful. • **No** (authentication disabled): The IPC can go online without username and password required.

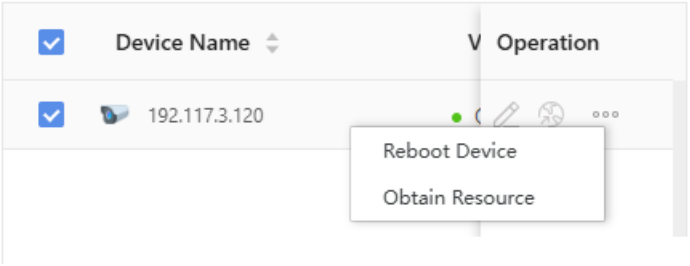
4. (Optional) Click **Next** and fill in the optional information.



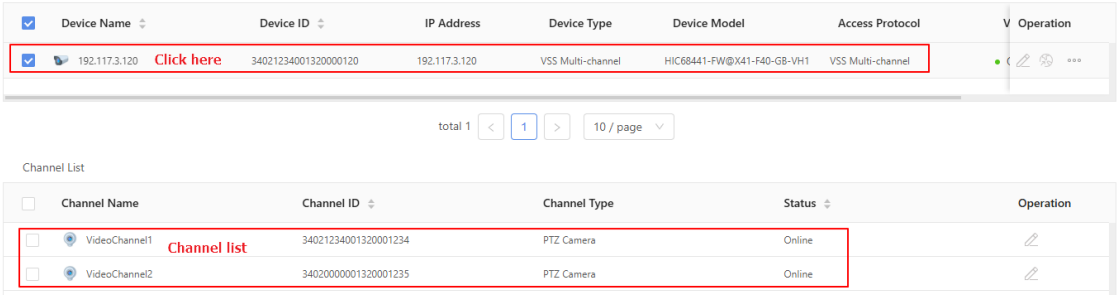
Parameter	Description
NAT Config	• If the IPC is behind the NAT and the local domain is in front of the NAT, choose **IPC Behind the NAT**.

Parameter	Description
	• If the local domain is behind the NAT and the IPC is in front of the NAT, choose **IPC in front of the NAT**. • If IPC and the external domain are behind different NATs, choose **IPC and Local Domain Behind Different NATs**. • If data streams of the IPC do not need to traverse the NAT, choose **Without NAT**.

5. Click **Confirm**.
6. When the VSS multi-channel camera goes online successfully, click **Obtain Resource** to obtain the channels under it.



7. In the **Frontend Device** list, select the VSS multi-channel camera, and its channels are displayed below.



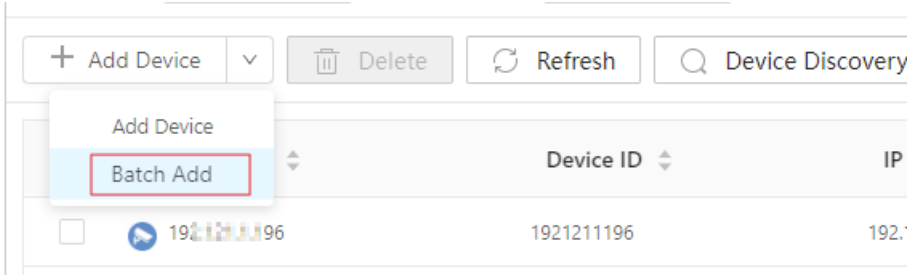
Note:

- VSS single-channel camera has only one channel, so the channel configuration and device configuration are integrated.
- VSS multi-channel camera has multiple channels, so the channel configuration and device configuration are separate.

7.1.3 Batch Add

Import devices in batches using a template.

1. Go to **Device Mgt** > **Frontend Device**. Select an organization for the device in the left-side organization tree and click **Add Device** > **Batch Add**.

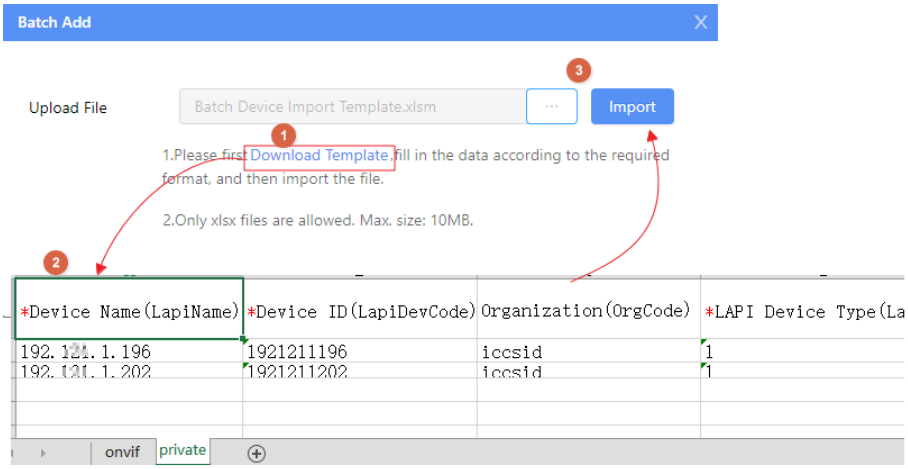


2. Click **Download Template**. Fill in the device information as instructed in the template.

Note:

- The template contains 2 sheets: onvif and private. Please enter the device information in the appropriate sheet based on the protocol.
- Only xlsx files are allowed. Max. size: 10MB.

3. Click ... to upload the modified template from local, and click **Import**.



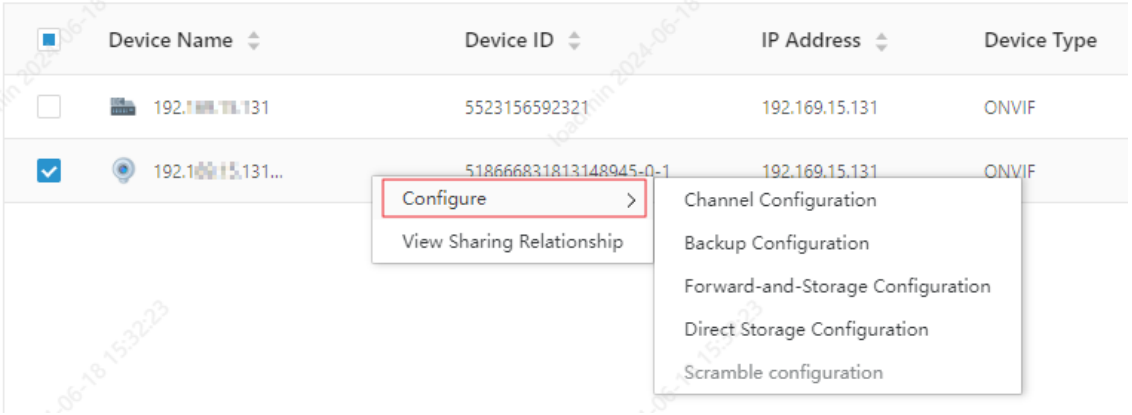
4. The successfully imported devices are displayed in the device list. For devices that failed to import, you can view the failure cause.

7.1.4 Configure Frontend Device

You can configure camera channels, storage resources, etc.

Note:
This operation is supported only by VSS cameras.

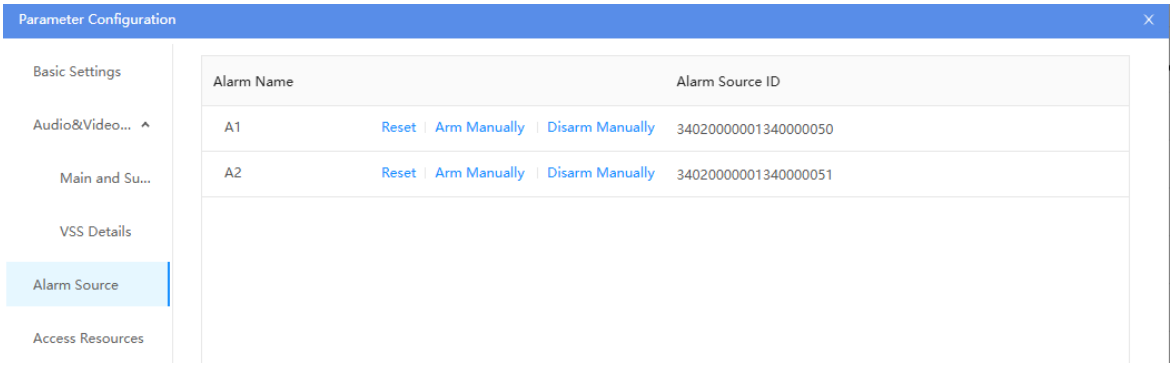
1. In the **Frontend Device** list, click ••• for the online camera.
2. Select **Configure**.



Configure storage resources (forward-and-storage configuration and backup configuration) for the camera. See configuration descriptions in Video Storage Configuration.

VSS Device Alarm Input

After a VSS device is connected, go to **Configure> Channel Configuration > Alarm Source**, the following operations are supported:



- **Alarm Reset**: After the platform receives an alarm input reported by the device, click **Reset** to send a reset command to the device. After reset, the device clears the current alarm status, and will only report again when the alarm input is triggered again.

  Note:
  If the alarm reset operation is not performed, the platform will not be able to receive the same alarm input again.

- **Arm Manually**: Click **Arm Manually** to enable the alarm input function of the device. When armed, if the alarm input status changes, the device will trigger an alarm and report it to the platform.
- **Disarm Manually**: Click **Disarm Manually** to disable the alarm input function of the device. When disarmed, if the alarm input status changes, the device will not report alarms to the platform.

7.1.5 Edit Device Info

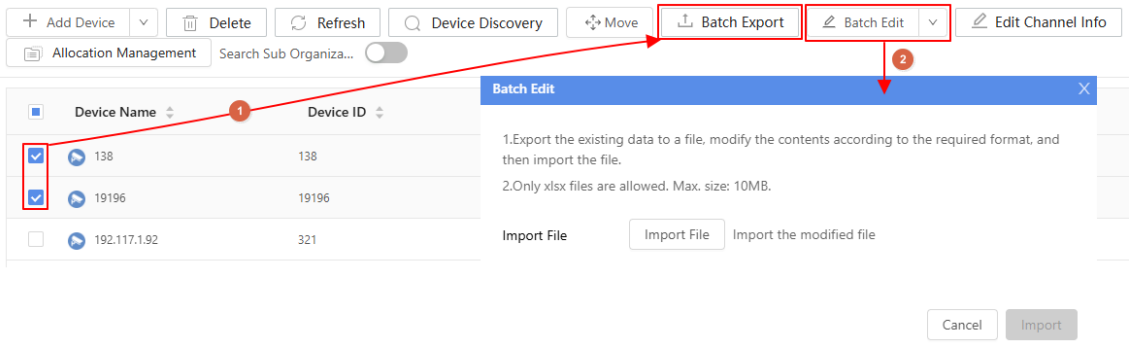
Edit device information one by one or in batches.

Edit One by One

1. In the device list, click for the camera.
2. Edit the parameters as needed.

Batch Edit

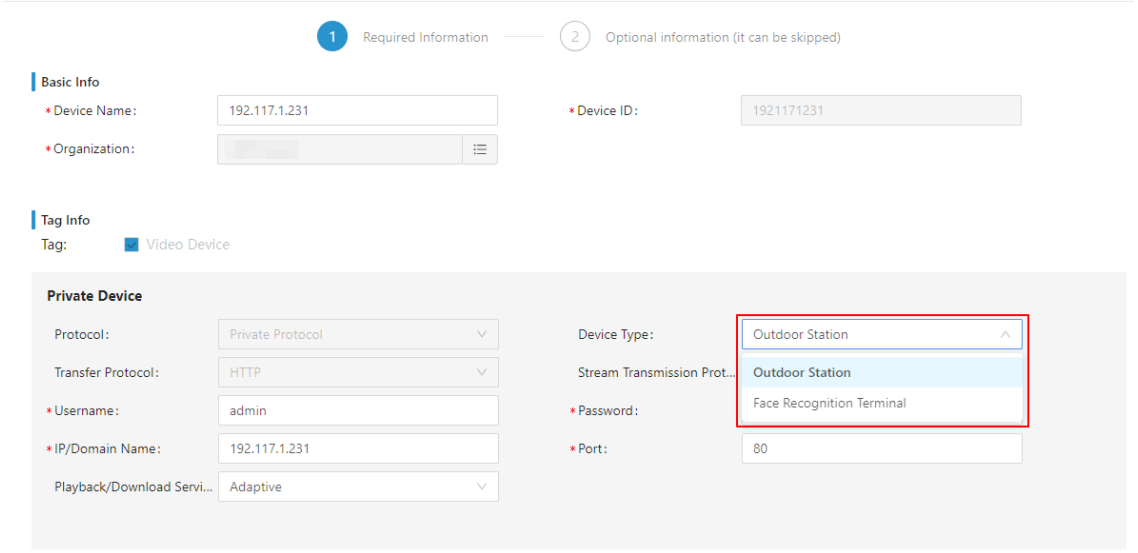
1. Select devices in the device list, and click **Batch Export** to export the selected device information into a xlsx file.
2. Modify the device information in the file.
3. Click **Batch Edit**. In the pop-up window, click ... to upload the modified file from local, and then click **Import**.



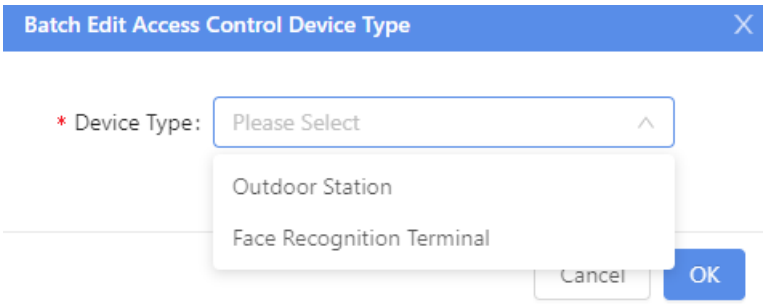
7.1.6 Edit Access Control Device Type

An access control device can be set to face recognition terminal mode or outdoor station mode (door station/ zone station). The device type can be modified on the platform for access control or video intercom purposes.

- Edit one by one: Click the corresponding for the access control device to change its type to **Outdoor Station** or **Face Recognition Terminal**.



- Edit in batches: Select multiple access control devices and click **Batch Edit Access Control Device Type** to set their type to **Outdoor Station** or **Face Recognition Terminal**.

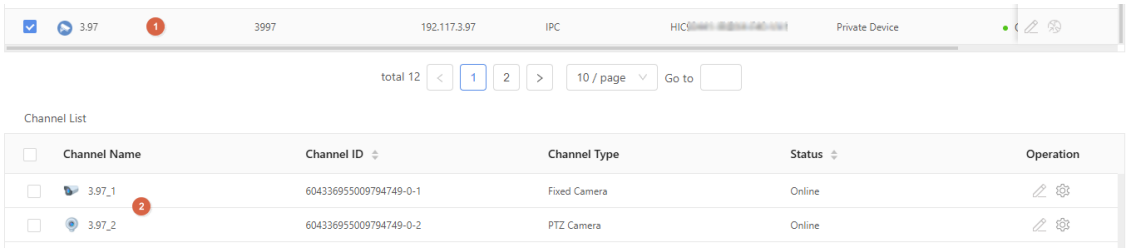


7.1.7 Edit Channel Info

Edit information for channels under device one by one or in batches.

Edit One by One

1. In the device list, select a device to display the channels under it.



2. Click for the channel to edit its information.

Note:

- For video channels, you can edit its basic configuration and main/sub stream parameters.
- For access control channels, you can edit the channel name and entry/exit direction.

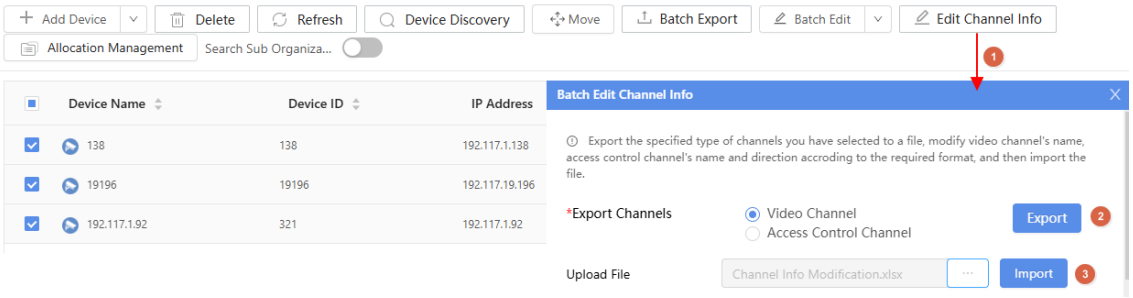
Batch Edit

1. Click **Edit Channel Info**.
2. Select the channel type (Video Channel/Access Control Channel) you want to edit, and then click **Export** to export the corresponding channel information table into a file.
3. Modify channel information in the file and save it.

Note:

- Video Channel: Only the channel name can be modified.
- Access control channel: Only the channel name and entry/exit direction can be modified.
- Do not modify the parameters displayed in gray in the table.

4. Click **Import** to upload the modified file.



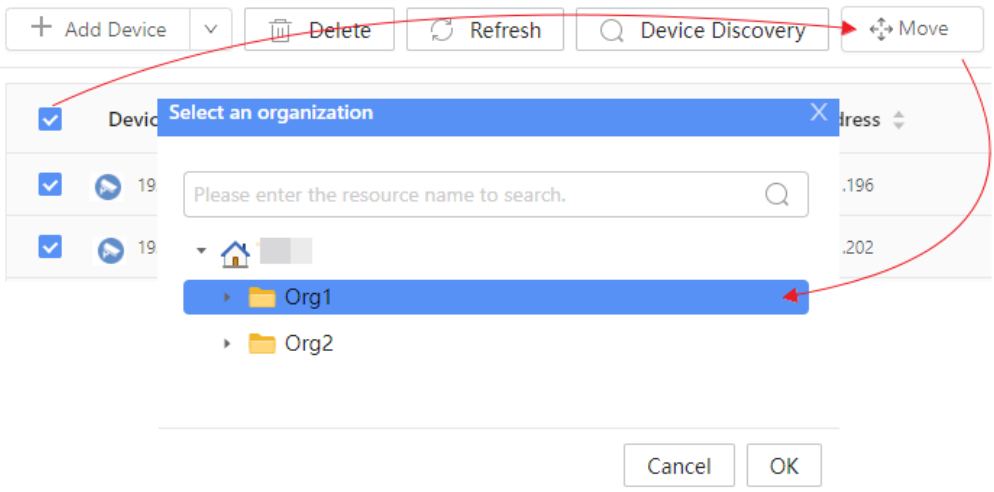
7.1.8 Move Device

Move devices to another organization.

Note:

- You can only move devices to another organization within the same domain (excluding the cloud organization and organizations under alarm controllers).
- Cannot move shared devices.

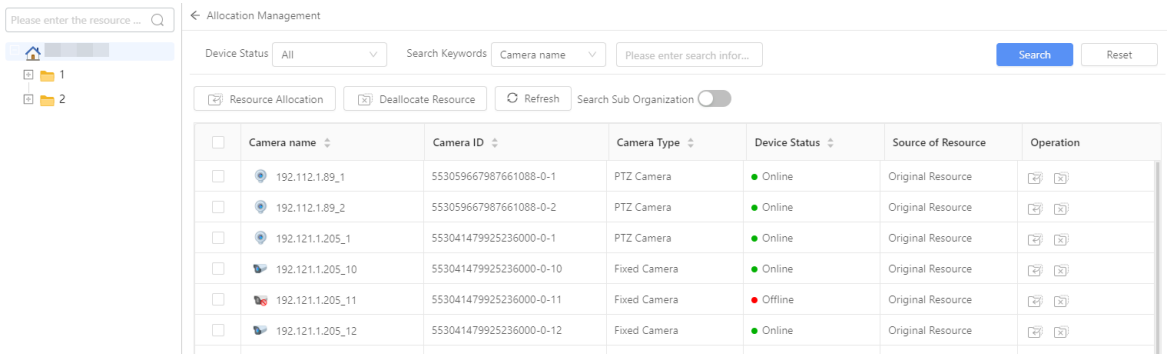
1. Select device(s) in the device list, and click **Move**.
2. Select the destination organization, and click **OK**.



7.1.9 Allocate Device

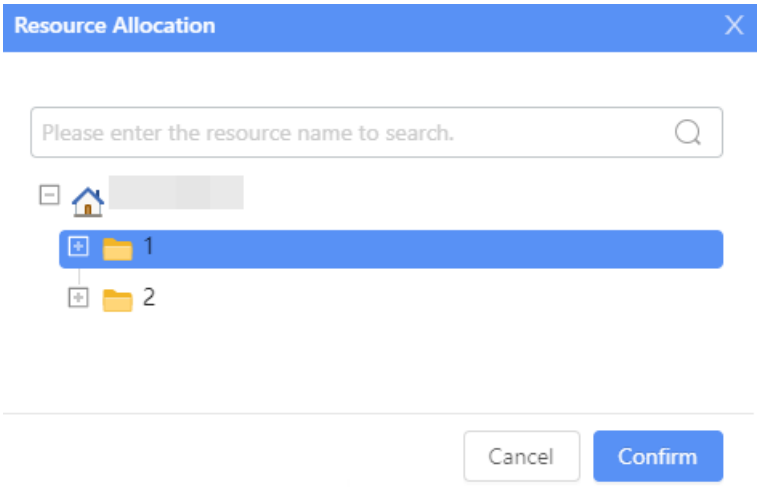
Allocate devices from one organization to another. After allocation, the device will exist in both the new organization and the source organization.

Click **Allocation Management** above the device list.



Allocate Resource

1. Select device(s) and then click **Resource Allocation** above the list; or click for the device.
2. Select a destination organization.



3. Click **Confirm**.

Cancel Allocation

For devices allocated from other organizations, you can also cancel the allocation.

1. In a destination organization (where the device has been allocated to), select device(s), and then click **Deallocate Resource**; or click for the device.
2. Confirm the operation to remove device from the organization.

7.1.10 Others

Search, edit, delete, export, and move frontend devices.

Search

- Search frontend devices by device type, device name, device ID, device model, and IP address.
- Select **Search Sub Organization** to search devices under sub organizations.

Delete

Select device(s) in the device list, and then click **Delete**.

Batch Export

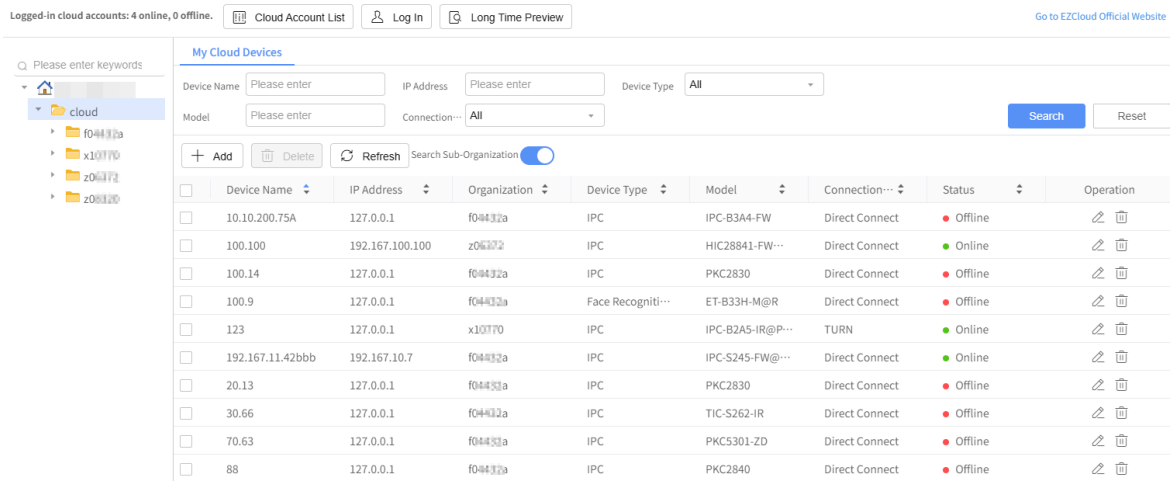
Select device(s) in the device list, and then click **Batch Export**.

Go to Device Web

In the device list, click corresponding to the device to access its web interface.

7.2 Cloud Device

Cloud devices refer to devices added on EZCloud Service, used in WAN networking scenario. After adding devices such as IPC, NVR, and face recognition terminal to EZCloud, you can log in to the cloud account on the platform and manage the devices under that cloud account (must be online).

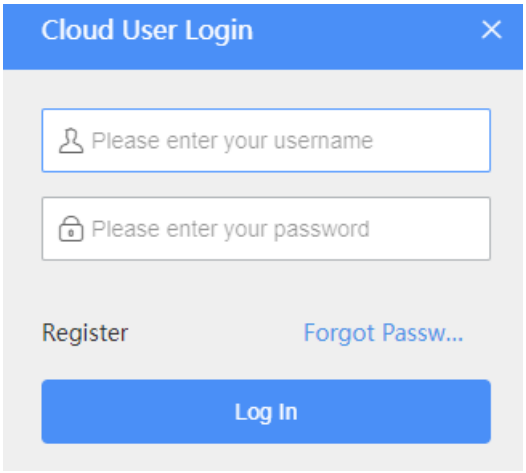


7.2.1 Manage Cloud Device

Log in to a cloud account to get devices from cloud.

Log In to Cloud Account

1. Click **Log In** in the center of the page. Enter the cloud account information and click **Log In**.



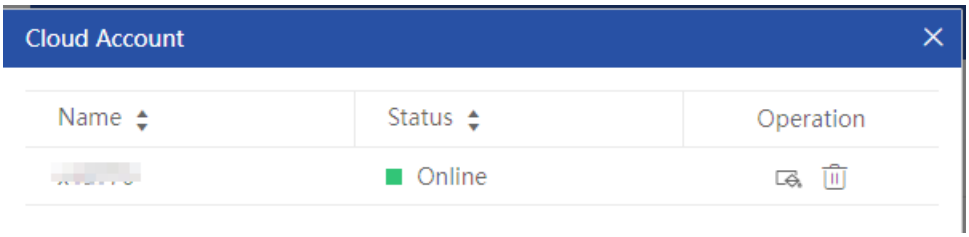
2. After successful login, the devices under the cloud account will be displayed in the list. Click **Refresh** to refresh the device status.

Note:
You can also log in to multiple cloud accounts (no upper limit) to manage devices under them. When logged in, you can click on the cloud account on the left organization tree to view the devices under it.

Manage Cloud Account

Click **Cloud Account List** to view the logged-in cloud accounts.

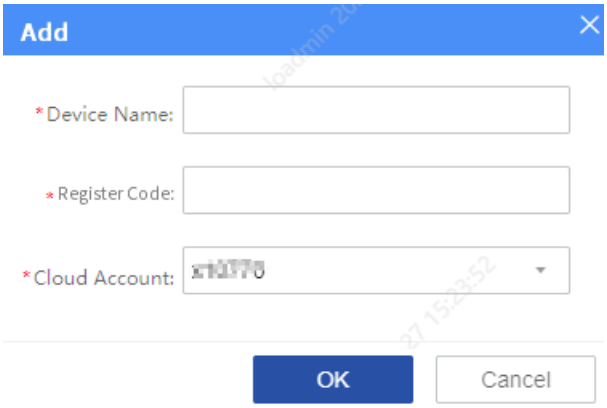
- Click to refresh the organization and device information under the cloud account (you need to log in to the cloud account again).
- Click to log out from the cloud account.



Add Cloud Device

You can add devices to online cloud accounts.

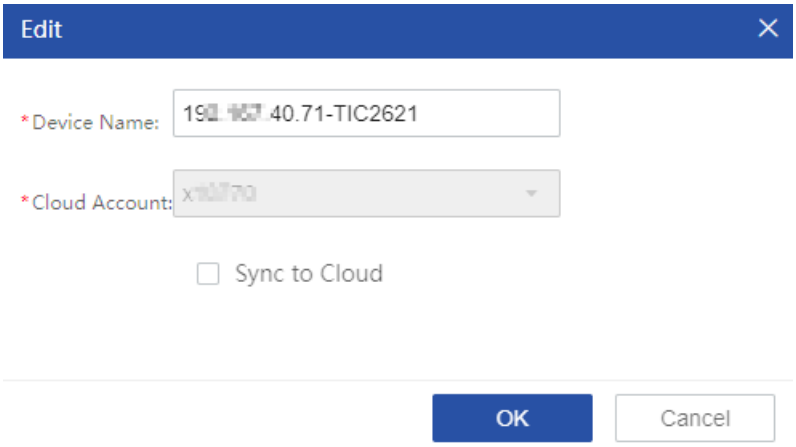
1. Click **Add** at the upper-left of the device list.



2. Enter the device name and register code (can be find on device body or device's Web interface).
3. Click **OK**. The successfully added devices are displayed in **My Cloud Devices** list.

Edit Cloud Device

1. Click for the device.



2. Edit the device name.
   If **Sync to Cloud** is selected, the modified device name will be synced to cloud; otherwise, only the device name on the platform will be modified.
3. Click **OK**.

Delete Cloud Device

Click for the cloud device to delete it from the current cloud account.

7.2.2 Long Time Preview

To view full-length videos from cloud devices, please recharge a long time preview plan as needed.

Each channel of the cloud device offers 20 minutes of free video playing daily. This duration accumulates based on the total video playing time on the channel, with simultaneous playing across multiple windows or clients counting as a single session. Video stops after 20 minutes.

A long time preview plan specifies the validity period and the number of available long time preview channels. When activated, you can view videos from cloud devices within the plan specifications (validity period and number of available long time preview channels).

Note:

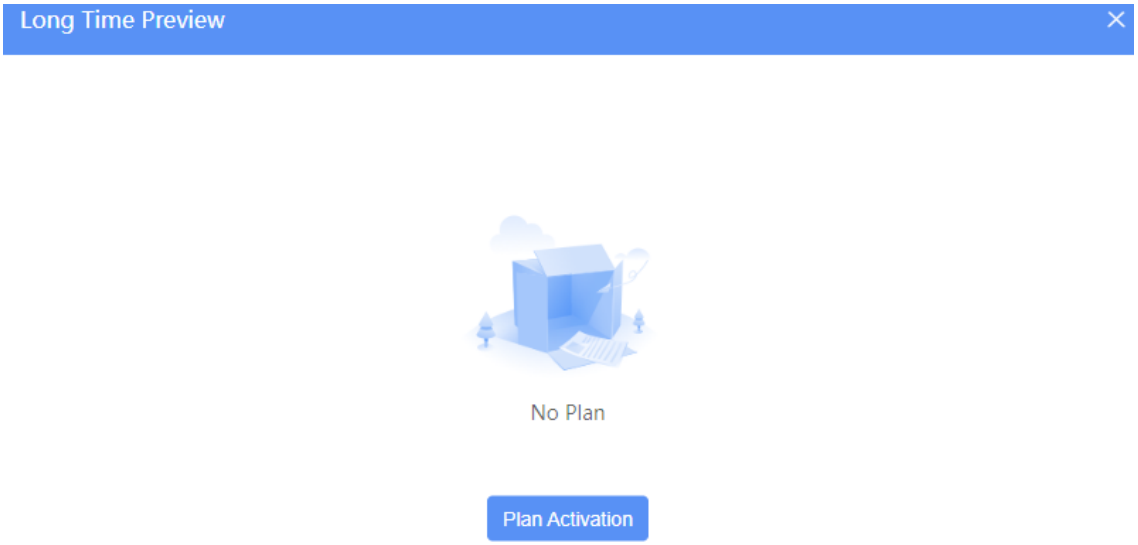
- The same channel can occupy up to 2 long time preview channels (one for live view, one for playback). Playing live videos from the same channel in multiple windows (camera sequence, group sequence, etc.) counts as one long time preview channel. The playback counts as one long time preview channel (single channel supports only one-channel front-end playback only).
- Application Scenarios: Terminals (client/video wall/app), video formats (live view, camera sequence, group sequence, playback, etc.)

Workflow:

① Contact our sales personnel to purchase the desired plan and obtain a recharge code; ② Enter the recharge code on this page to activate the plan. Plan upgrades (increase long time preview channels available) and renewals (extend plan duration) on activated plans are also allowed.

First Activation

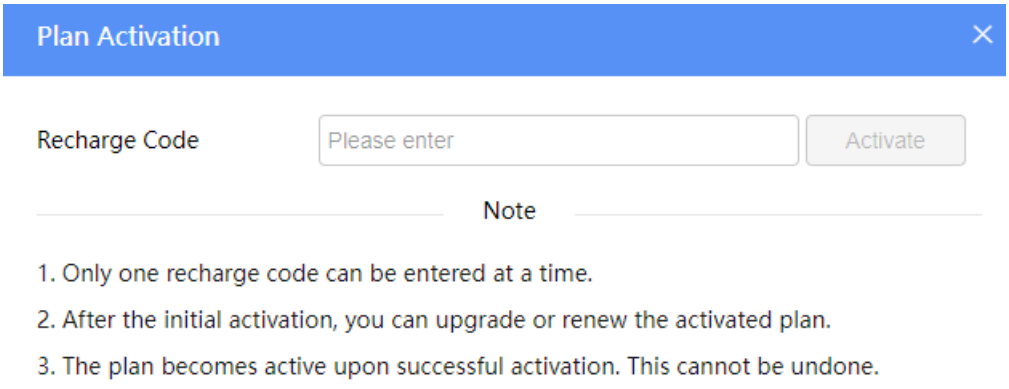
1. Click **Long Time Preview**.



2. Click **Plan Activation**.
3. Enter the recharge code and click **Activate**.

Note:

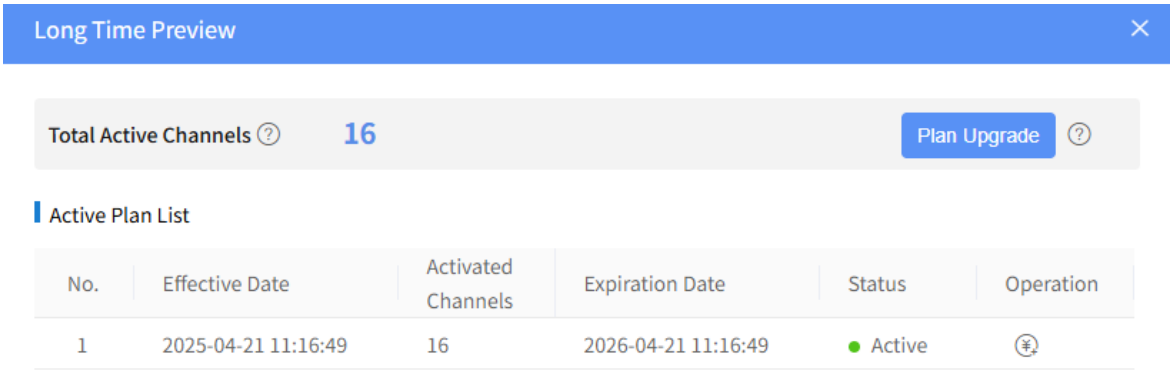
- Activation is irreversible.
- The plan becomes effective after restarting the service; or it will automatically take effect at 3:00 AM the following day.



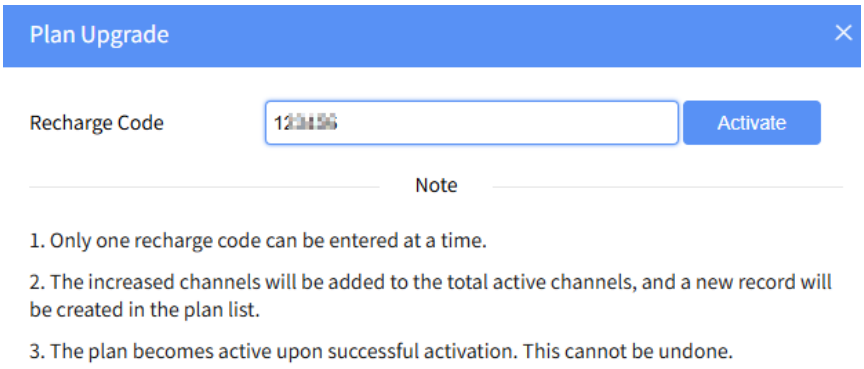
View/Upgrade/Renew Plan

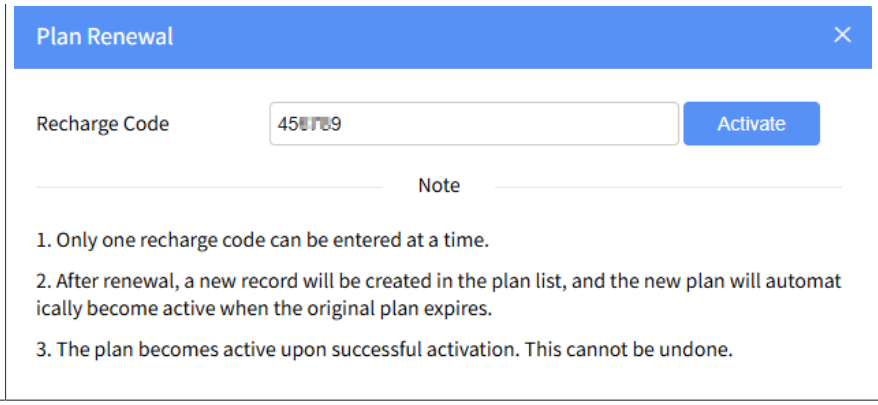
If you have already activated plan, you can click **Long Time Preview** to view the list of active plans.

If there are plans with overlapping validity periods, the number of available long time preview channels during the overlapping periods is the sum of these plans.



For plan upgrades and renewals:

Upgrade Plan (increase long time preview channels available)	Click **Plan Upgrade**, enter the recharge code, and then click **Activate**. • Activation is irreversible. • The plan becomes effective after restarting the service; or it will automatically take effect at 3:00 AM the following day. • Newly added available long time preview channels will be added to the current total number of available long time preview channels. The expiration date of the upgrade plan = Start date of the upgrade plan + Duration of the upgrade plan (unaffected by the original plan's expiration date). 
Renew Plan (Extend Plan Duration)	Click for a plan, enter the recharge code, and then click **Activate**. • Activation is irreversible. • The new plan will automatically take effect after the original plan expires. The expiration date of the renewal plan = Start date of the renewal plan + Duration of the renewal plan.



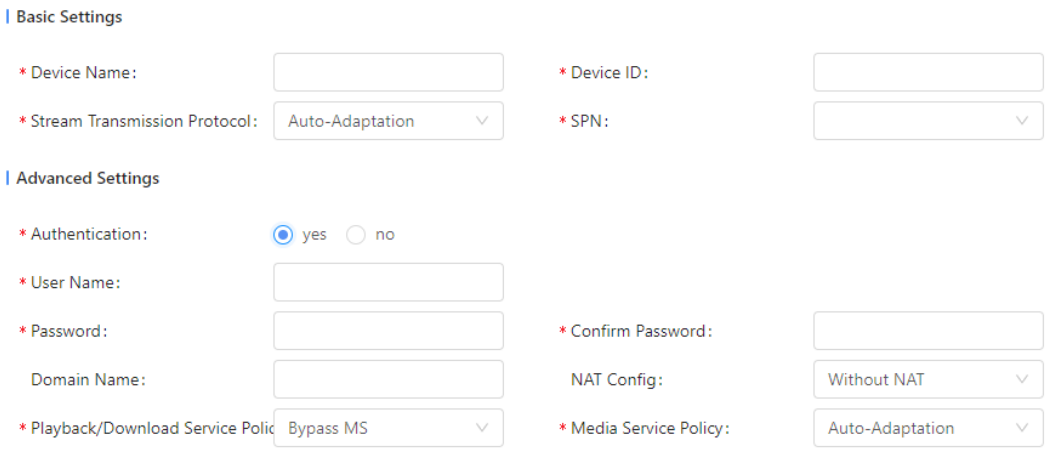
7.3 Edge Device

7.3.1 VSS NVR

You can add NVRs (Network Video Recorders) via the VSS protocol and view the camera resources under the NVR on the management platform.

Add NVR

1. Click **Add** and configure device parameters.

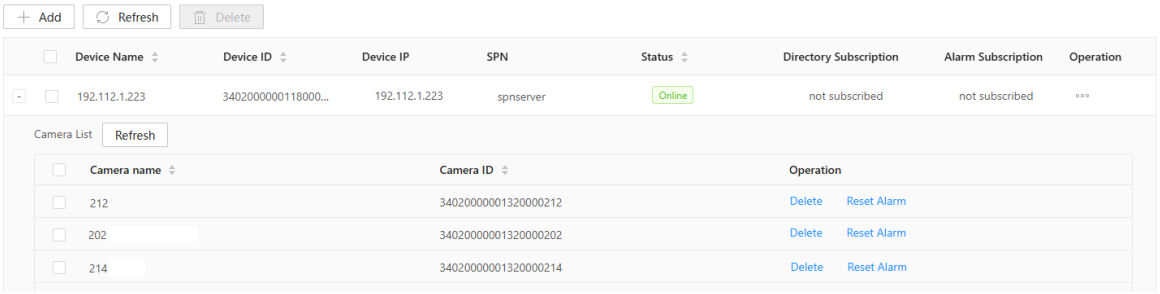


Parameter	Description
Device Name	Customize the device name of the NVR for easy differentiation.
Device ID	Consistent with the device code of the NVR.
Stream Transmission Protocol	• Auto-Adaption (default): This platform can receive TCP or UDP video streams sent by the NVRs, which is determined by system negotiation. • TCP: This platform can only receive TCP video streams sent by the NVR.
SPN	Select an SPN for NVR to push resources.
Authentication	If enabled, the username/password of the NVR will be authenticated.
Domain Name	Optional. For VSS protocol authentication. If configured, it should be the same as the domain name configured on the NVR.
NAT Config	Select the corresponding scenario depending on whether the NVR and the cameras under it are in the same network with this platform.

Parameter	Description
Playback/Download Service Policy	Configure the service policy for playing back or downloading resources of the NVR on this platform: • Auto-Adaption (default): If there is no MS available, the policy of Bypass MS will be followed. If there is MS available, the policy of Not Bypass MS First will be followed. • Bypass MS: The playback/download will bypass the MS. **Note:** Whether the media streams bypass the MS is determined based on multiple configurations and MS deployment. See details in **Local Config** > **Video Parameters** > **Advanced Config** > **Playback/Download Service Selection Policy**.
Media Service Policy	• Auto-Adaption (default): Whether the video streams bypass the MS is determined by the system according to the media service selection policy of the NVR and the MS deployment. • Specified MS: The video streams will not bypass the specified MS. • Specified MS Group: The video streams will not bypass the MS in the specified MS group. • Bypass MS: The video streams bypass the MS. **Note:** If an MS is deployed but has insufficient forwarding capacity, then the Bypass MS policy will be adopted.

View/Delete Device Resources

Click + on the left-side of the NVR to expand the list of cameras under it.



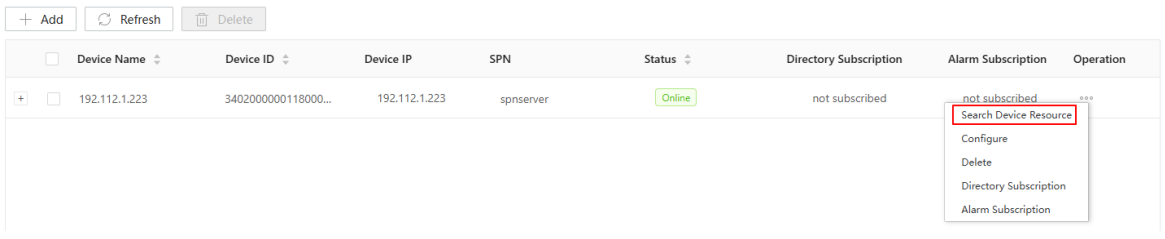
- **Delete**: In the camera list, click **Delete** in the **Operation** column to delete the camera from the list and synchronously delete the camera from the NVR.
- **Reset Alarm**: After the platform receives an alarm input reported by the device, click **Reset Alarm** to send a reset command to the device. After reset, the device clears the current alarm status, and will only report again when the alarm input is triggered again.

  Note:
  If the alarm reset operation is not performed, the platform will not be able to receive the same alarm input again.

Search Device Resource

You can manually obtain camera resources under the NVR.

Click ... in the **Operation** column and select **Search Device Resource** to obtain the latest device resources under it.

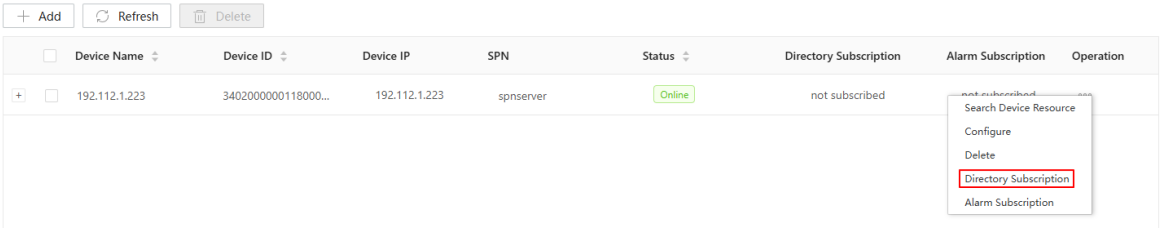


Subscribe to Directories

You can subscribe to directories to synchronize the status and name of the camera resources under the NVR.

Subscription Description

Click ••• in the **Operation** column and select **Directory Subscription**.



Cancel Subscription

To cancel the subscription to directories, click ••• in the **Operation** column and select **Cancel Subscription to Directories**.

Subscribe to Alarms

You can subscribe to the alarms generated by the NVR and the cameras under it.

Subscription Description

Click ••• in the **Operation** column and select **Subscribe to Alarms**.

Cancel Subscription

To cancel the subscription to directories, click ••• in the **Operation** column and select **Cancel Subscription to Alarms**.

Edit NVR

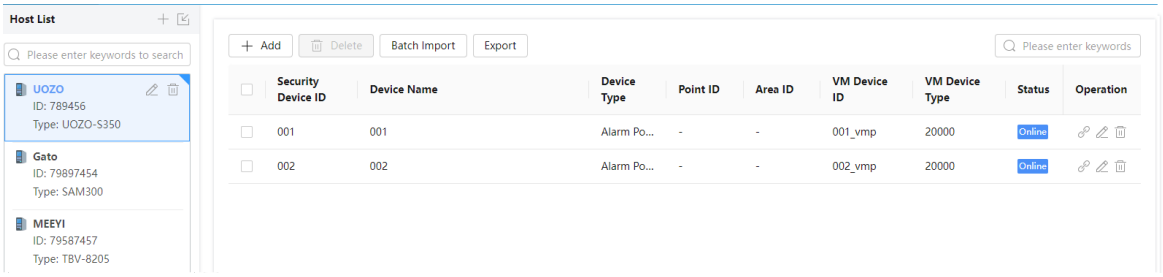
Click ••• in the **Operation** column and select **Configure**; or double-click on the device name to edit the basic parameters.

Delete NVR

Click ••• in the **Operation** column and select **Delete**; or select multiple NVRs and click **Delete** at the top of the list.

7.3.2 Third-party Host

The platform supports connection with third-party alarm controllers to receive alarms from alarm devices and allow user to control these alarm devices, including arming/disarming and opening/closing doors.



7.3.2.1 Host Management

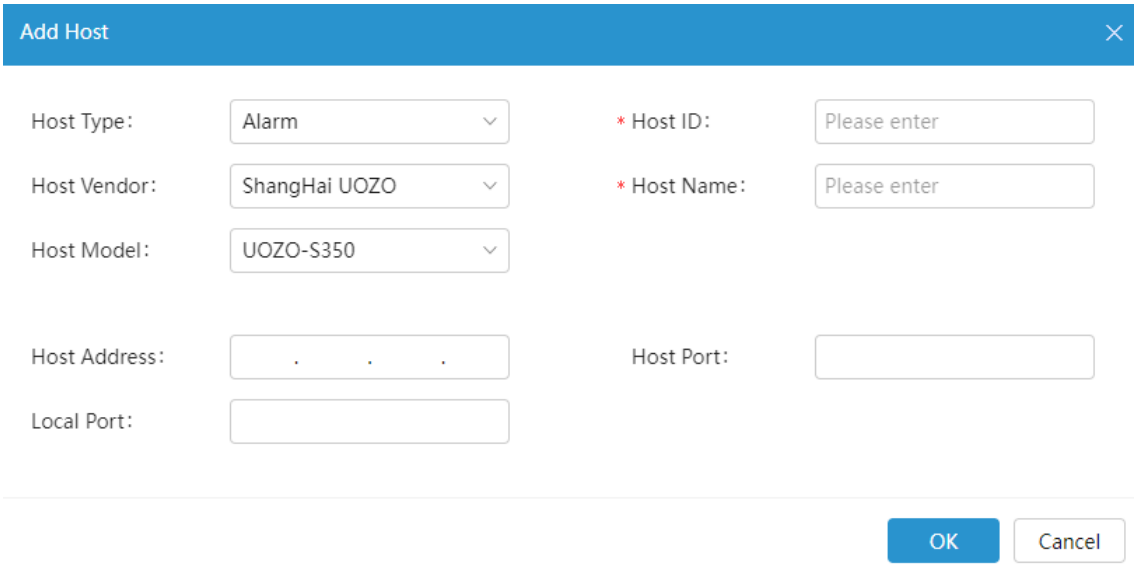
Add, edit, and delete hosts.

Add Host

Add one by one or in batches.

Add one by one

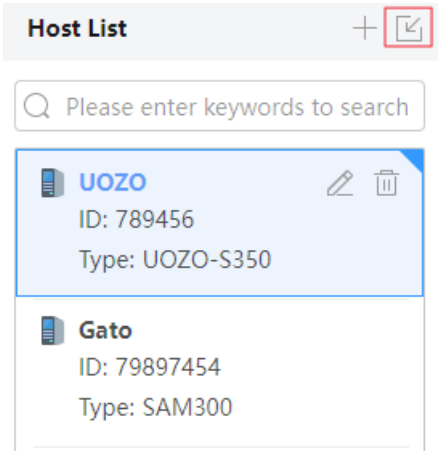
1. Click + in the upper-right corner of the host list.



The parameters are described below.

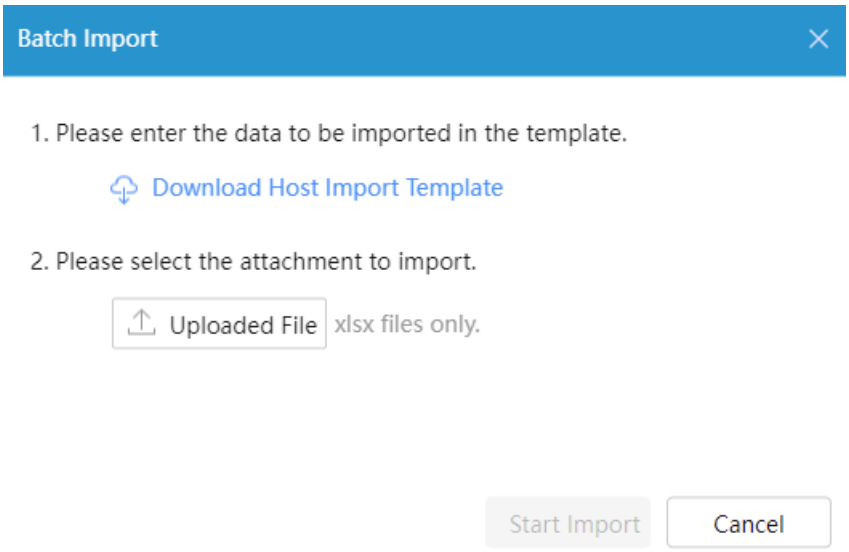
Parameter		Description
Basic configuration	Host Type	Includes alarm controllers, access controllers, intercom devices, and environmental sensors.
	Host ID (required)	Enter a unique host ID.
	Vendor	Choose the vendor.
	Host Name (required)	Enter the host name.
	Host Model	Choose a model from the list.
Connection parameters		The parameters may vary depending on the type, manufacturer, and model. Set according to the actual requirements.

2. Click **OK**. The added host appears.



Batch import

1. Click in the upper-right corner of the host list.



2. Download the template.
3. Complete the required information according to the template.
4. Click **Upload File** and then select the file you just completed.
5. Click to import the file.

Other Operations

- Edit host: Click to modify the host information.
- Delete host: Click to delete a host. If there are devices under the host, then the host cannot be deleted.

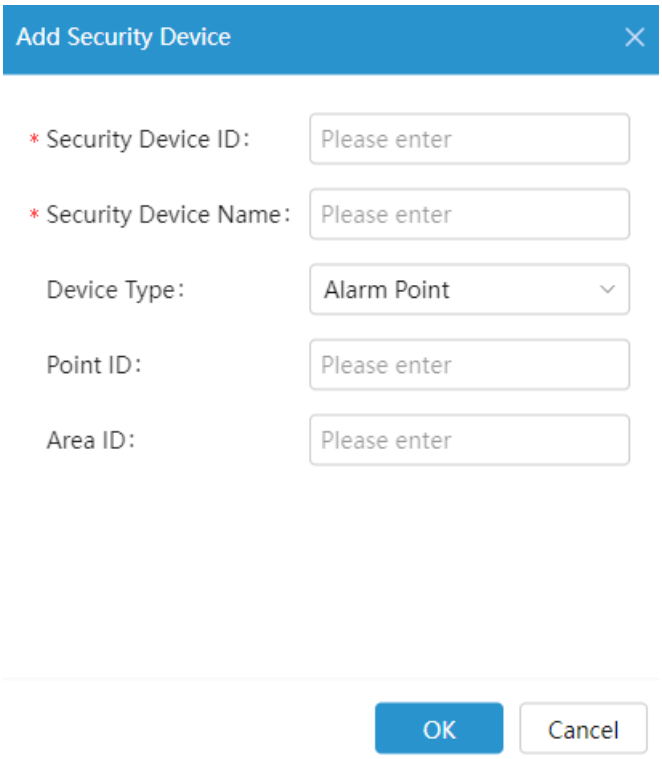
7.3.2.2 Device Management

Add third-party security devices, for example, environmental sensors, access control devices, security scanners, etc; and modify or delete devices.

Add Device

Add one by one

1. Choose the host for which you want to add the device.
2. Click **Add**.



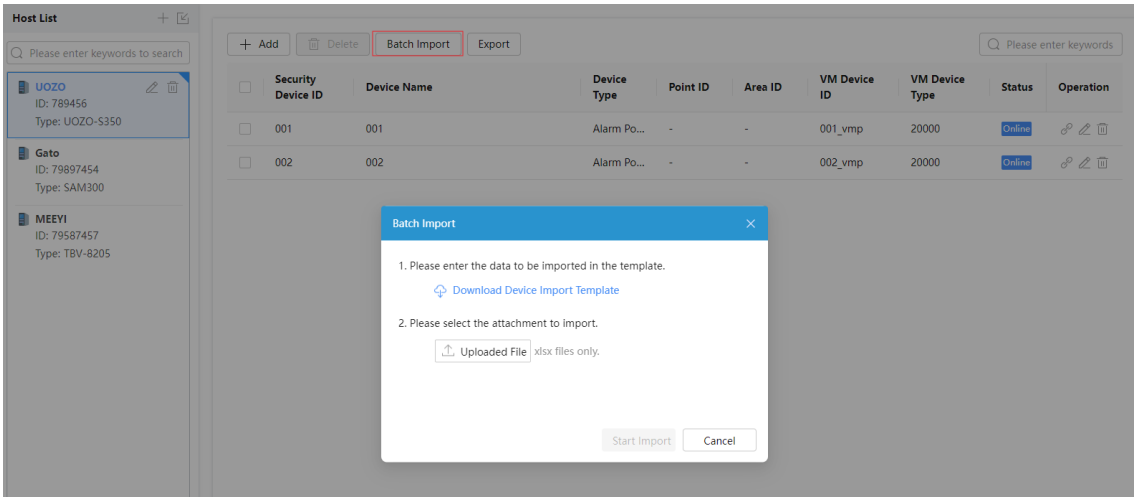
The parameters are described below.

Parameter	Description
Security Device ID (required)	Enter a unique ID for the device.
Security Device Name (required)	Enter a name for the device.
Device Type	Choose the device type from the list.
Point ID	Device's area ID (zone ID), must be consistent with the area ID configured in the host. Leave it empty if there's no zone ID.
Area ID	Host ID, must be consistent with the host ID configured in the host.

3. Click **OK**.

Batch import

1. Choose the host for which you want to add the device.
2. Click **Batch Import**.



3. Download the device import template.
4. Complete the required information according to the template.

5. Click **Upload File** and then select the file you just completed.
6. Click to import the file.

Other Operations

- Edit device: Click to modify the device information.
- Delete device: Click to delete a device; or select devices and then click **Delete**.

7.4 Terminal Device

Terminal devices include decoders, video wall controllers, and network keyboards, which are used for playing videos on video wall.

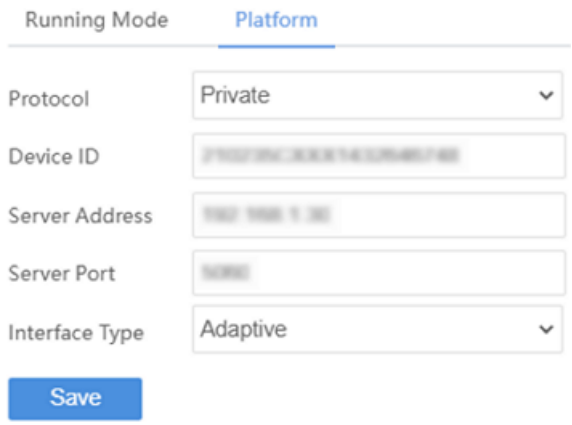
7.4.1 Decoder & Video Wall Controller

Decoders (ADU88 series, ADU87 series, DC series, A9 series) can convert digital signals from cameras or local channels into analog signals and output them to the video wall for display.

Decoder Device Configuration

1. Access **http://decoder_IP_address** through a browser and log in to the Web interface of the decoder device.
2. On the **Operation Mode > Platform Configuration** page, configure the platform information.

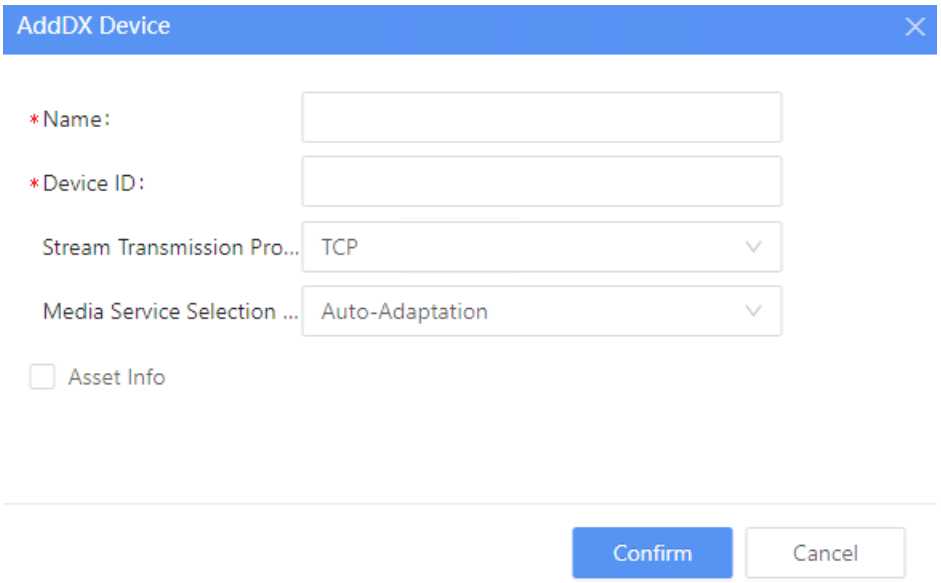
Note:
Configuration paths vary by decoder models. Please refer to the actual device.



Parameter	Description
Protocol	Select Private protocol.
Device ID	Defaults to the device serial number. Customization is supported.
Server Address	IP address of the connected platform.
Server Port	5060.
Interface Type	Adaptive.

Add Device

1. Select an organization for the device in the local domain.
2. Click **Add**.



3. Configure the parameters by referring to the table below.

Parameter	Description
Name	Device name.
Device ID	Enter the device ID of the decoder device. For details, refer to Decoder Device Configuration.
Stream Transmission Protocol	• TCP (default): The DX device only receives media streams carried by TCP. • Auto-Adaptation: The DX device can receive media streams carried by UDP or TCP, and the protocol is determined by the system through automatic negotiation.
Media Service Selection Policy	Choose whether IPC's media streams are forwarded to DX device via MS server. • Adaptation (default): The system decides whether to forward IPC streams via MS based on factors such as the forwarding capacity of MS server. • Direct Connection First: IPC streams are directly sent to the DX device, bypassing MS server.

7.4.2 Network Keyboard

Network keyboards are used with video wall and allow remote video control (such as play and pause) on the video wall by associating keyboard keys with cameras.

Supported keyboard model: KB2100.

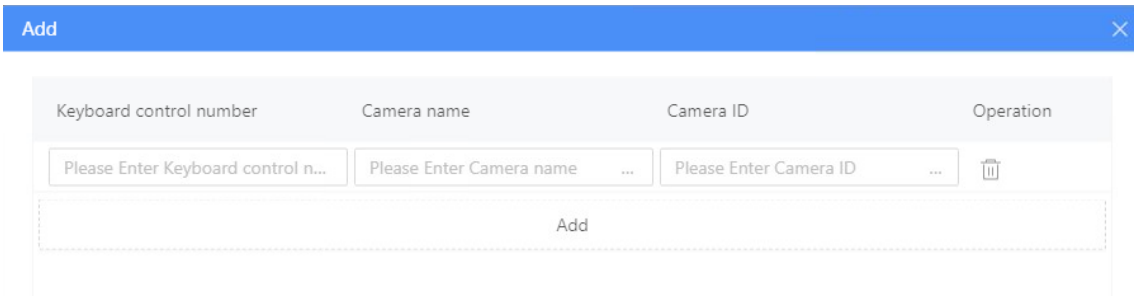
Note:
Enter the IP address of the platform on KB2100 to log in. When succeeded, the keyboard can obtain devices and video wall resources from the platform directly, without adding the keyboard on the platform.

Keyboard Control Configuration

Camera Control Relationship

Set the correspondence between keyboard control numbers and camera IDs so users can control a camera with a keyboard. One keyboard control number corresponds to one camera. For example, if set the number key 1 to correspond to camera 1, then when you press the number key 1, the keyboard will control camera 1. You can also press other function keys on the keyboard to perform operations such as playing live video on wall.

1. Go to the **Camera Control Relationship** tab.
2. Click **Add**.



3. Enter the keyboard control number. Select a camera, and the camera ID will be filled in automatically. To add more items, click **Add**.

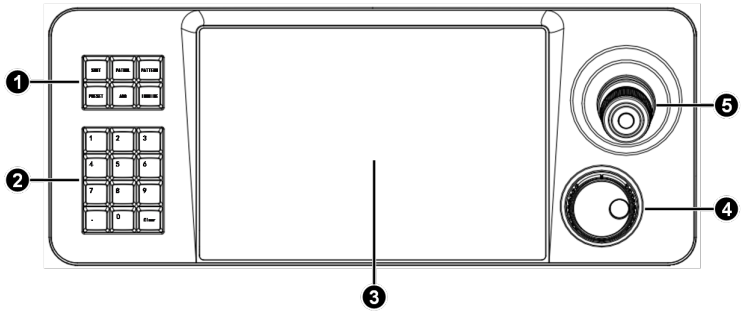
Note:

- The keyboard control number must be a number; the camera ID is the ID of the camera you want to control using the keyboard.
- One keyboard control number corresponds to one camera ID.

4. Click **Confirm**.

Keyboard Key Description

The diagram below is for illustrative purpose only. The device functions may vary with version or model. Please refer to the latest device document.



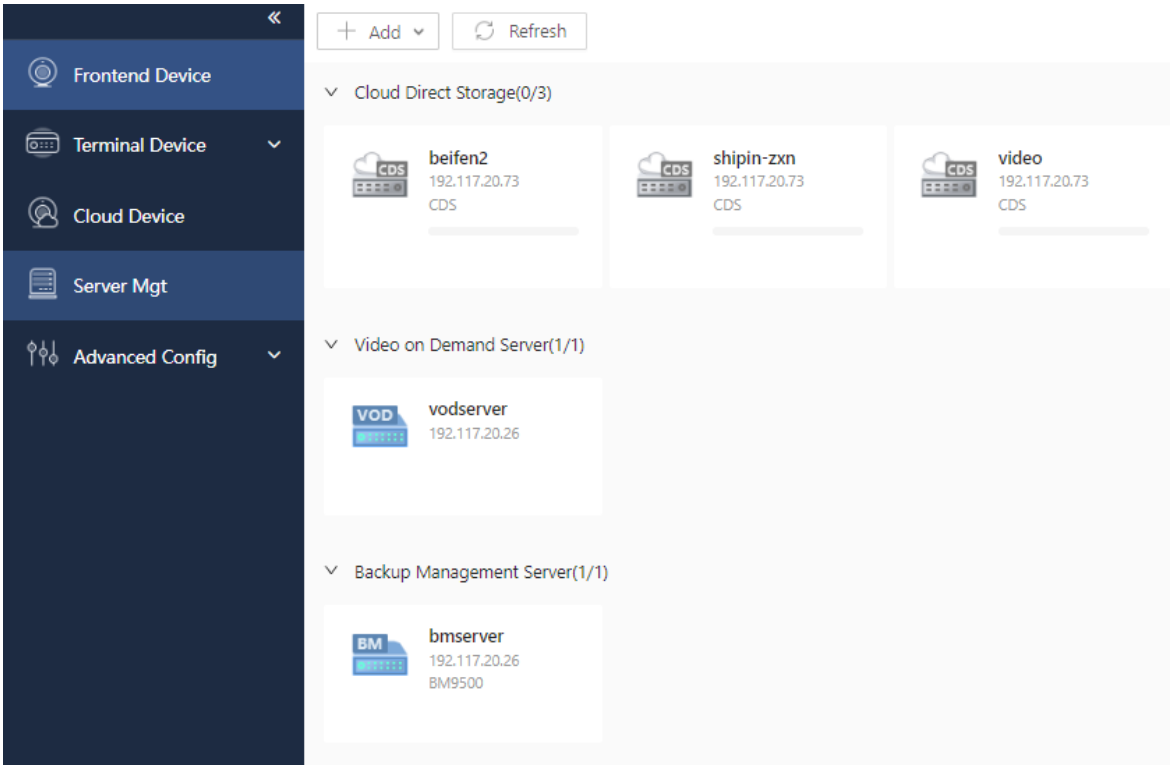
No.	Name	Description
1	Function key	• PRESET: Set presets. • ADD: Play video on wall. • Other keys are reserved. Please refer to the device's document.
2	Number key	• Digit (0-9) and decimal point. • Clear: Clear input.
3	Touch screen	View video on the touch screen or mirror video to an HDMI-connected display device.
4	Dial	Rotate the outer wheel to adjust the focus. Rotate the inner wheel to adjust the iris.
5	4D joystick	Move the joystick up/down/left/right/upper-left/lower-left/upper-right/lower-right to control the PTZ camera to rotate in all directions and quickly locate objects.

7.5 Server Management

The platform has built-in media servers and storage devices.

External intelligent compression server is supported: Click **Add**, select the server type, fill in parameters such as the device ID, and then add it.

Note:
The device ID must be consistent with that on the device side, which can be obtained via the device's web interface.



Media Server

Responsible for replicating the live video streams from IPCs into multiple streams and then forwarding them to UMS clients and storage devices.

Storage Device

Storage devices include three service modules: cloud direct storage, backup management server, and video on demand server.

- Cloud direct storage: Stores video recordings from IPCs and images reported by front-end devices. For the adding procedure, refer to Video Storage Configuration.
- Backup management server: Performs secondary storage of video recordings.
- Video on demand server: When a client searches for a recording, the video on demand server locates the recording in the storage resources and streams it to the client for playback.

Intelligent Compression Server

Supports compressing videos to reduce storage space. For function details, refer to Video Compression.

8 Video Storage Configuration

Go to **Basic Configuration > Storage Configuration**.

Configure video storage for cameras. Videos will be stored in the local disks or external storage devices connected to the platform. During playback, the stored videos can be retrieved for viewing.

Scheduled storage, alarm-triggered storage, manual storage, and scheduled recording backup are supported.

Note:

- This chapter describes how to configure central recording storage (stored in the local disks or the external storage devices).
- You can also configure storage on IPC or NVR if you don't want to use the central recording storage.

8.1 Add Storage Resource

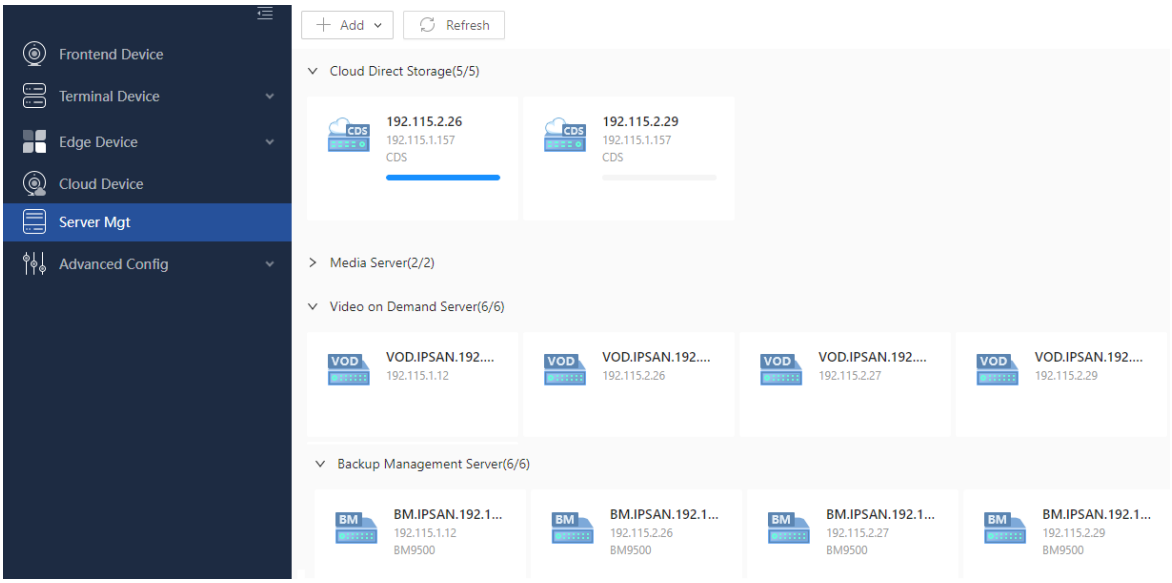
The platform can use the local disks or external storage devices to provide recording storage for IPCs.

Configuration Steps

Please first configure local disks/RAID or add external IPSAN in **System Configuration** >Disk Configuration .

After configuration, the system will automatically create a storage resource for the usage.

At the **Device Management** > **Server Management** page, the following servers will be automatically added to the system: Cloud Direct Storage (for storage management), Video on Demand Server (for video playback), and Backup Management Server (for recording backup).



8.2 Recording Storage

You can allocate the size of the storage resource space to cameras and configure different storage methods for cameras.

The following storage modes are available: manual storage, alarm-triggered storage, and scheduled storage.

- Manual storage: User starts/stops central recording manually.
- Alarm-triggered storage: Storage is triggered by alarms. You need to configure post-alarm recording time.
- Scheduled storage: Configure a storage schedule for the camera.

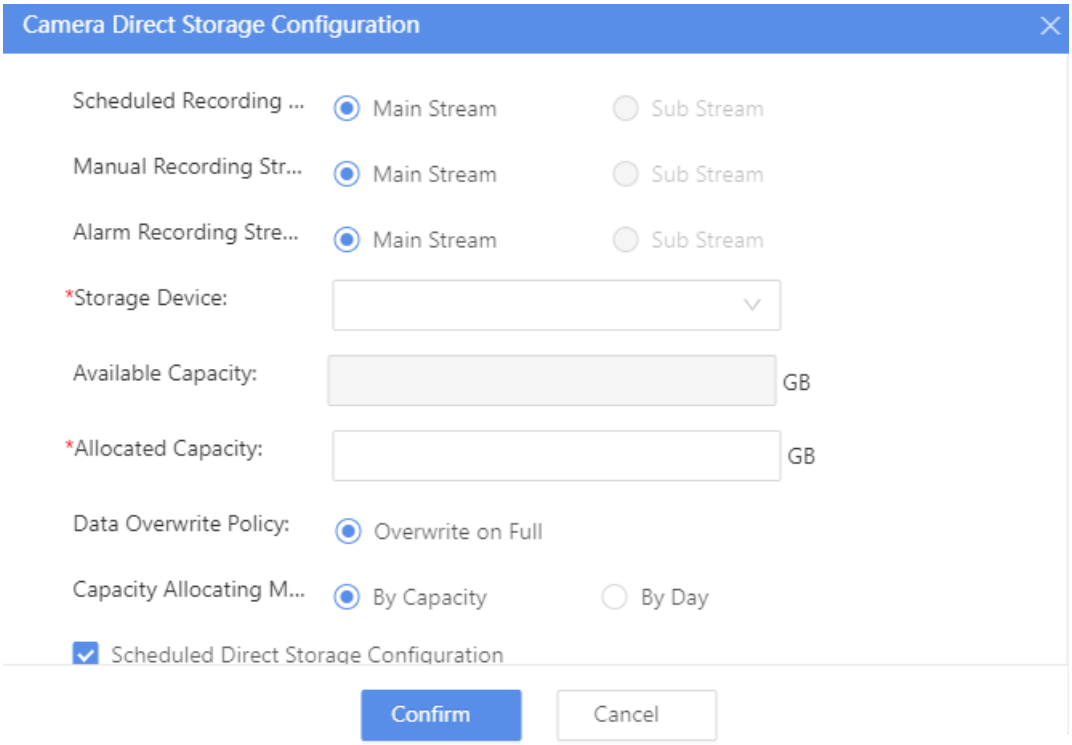
Configure Storage Resource

1. On the left-side organization tree, choose an organization, choose the target camera, click , or select multiple cameras of the same type (IPC or EC) and then click **Batch Add**.

   Note:

   - If you need to configure storage for cloud devices, please enable **Cloud Device Storage Configuration** on the Function Switch page beforehand.
   - Cloud device storage of video recordings is limited by the **Long Time Preview** plan. Please purchase and activate Long Time Preview.

A page as shown below appears. (The parameters displayed may vary with camera. The figure below is an example.)

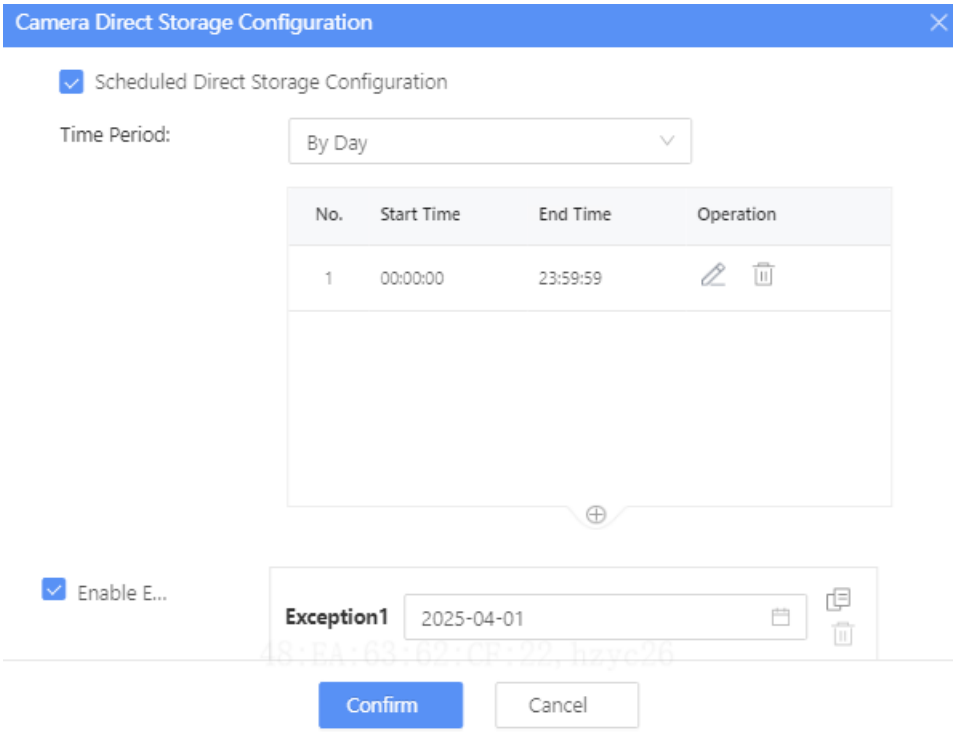


2. Configure the parameters by referring to the table below.

Parameter	Description
Scheduled Recording Stream	Choose main stream or sub stream. The selected stream type will be used for scheduled storage.
Manual Recording Stream	Choose main stream or sub stream. The selected stream type will be used for manual storage.
Alarm Recording Stream	Choose the stream type for alarm-triggered recording. **Note:** Choose main stream or sub stream according to the encoding parameters of the IPC or the encoder connected to the camera.
Direct Storage Device	Select recording storage resource (created in Disk Configuration).
Available Capacity	Available capacity on the storage device. The system reads the capacity automatically after you select a direct storage device.
Allocated Capacity	Storage space assigned to the camera.
When HDD Full	Overwrite: When the storage space assigned to the camera is used up, new data will overwrite the old data from the beginning repeatedly.
Capacity Allocating Mode	• By Capacity: Allocate storage resource to the camera according to the allocated space. • By Day: Calculate the space to be allocated based on stream type, storage days, and scheduled storage settings, and then allocate storage resource to the camera. **Note:** This parameter is displayed only when you are configuring a single camera.
Storage Days	This parameter is required if you are configuring for a single camera and the capacity allocating mode is **By Day**. Set the storage days and then click **Calculate**. The system automatically calculates the needed forward-and-storage space and displays it in “allocate capacity” or “expansion capacity”.

Parameter	Description
	Note: The video storage space needed by a camera is calculated using this formula: Needed space = N (hours) * 3600 (seconds) * encoder stream / IPC (bps) * (1.08) / 8, where 1.08 is the needed space plus 8% margin. For example, assume each video channel is 2M, so the space needed every hour is 2048*3600*1.08/(8*1024*1024)=0.95GB, so 22.8GB is needed for 24-hour recording. If each camera records 30 days, then one VX1600 with 16 1TB HDDs can satisfy space requirements of 16000/(22.8*30)≈24 cameras at most.

3. Enable/disable scheduled recording (when enabled, the camera records video according to the schedule).



4. (Optional) If scheduled direct storage is enabled, configure scheduled direct storage by referring to the table below.

Parameter	Description
Time Period	You can set the storage schedule by day or by week. **Note:** After completing the storage schedule for a day, you can click **Copy** to copy and apply the schedule to other days.
Enable Exception	If necessary, enable exception to set special time periods and perform special storage during these periods. On special days, the system performs storage during the set periods only; on other days, the system performs storage according to the schedule. **Note:** • Click **Add Exception** to add an exception. Up to 16 exceptions are allowed. • Click to delete an exception. • After completing the storage schedule for a day, you can click to copy and apply the schedule to other days.

5. Click **Confirm**.

Capacity Expansion/Reduction

1. Choose the target camera, click in the **Operation** column.

2. In expansion capacity, enter the capacity you want to expand or reduce. A positive number means expansion. A negative number means reduction.

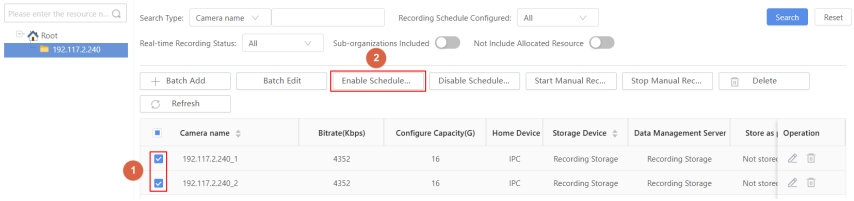
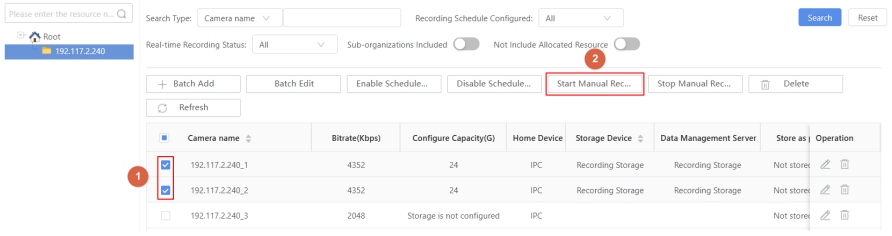
   Note:

   - For capacity expansion, make sure the expansion is less than or equal to the capacity available.
   - To reduce cloud storage capacity, make sure the modified capacity is greater than or equal to 16GB.

3. Click **Confirm**.

Start/Stop Storage

You can start or stop storage after completing storage resource configuration for a camera.

Storage Type	Operation
Scheduled Storage	1. Click the organization on the left-side organization list, and then select the target camera in the organization. 2. Click **Start Scheduled Storage/Stop Scheduled Storage**.  **Note:** The system automatically starts the recording schedule when scheduled recording is configured.
Manual Storage	You can perform manual storage after configuring storage resources for the camera. 

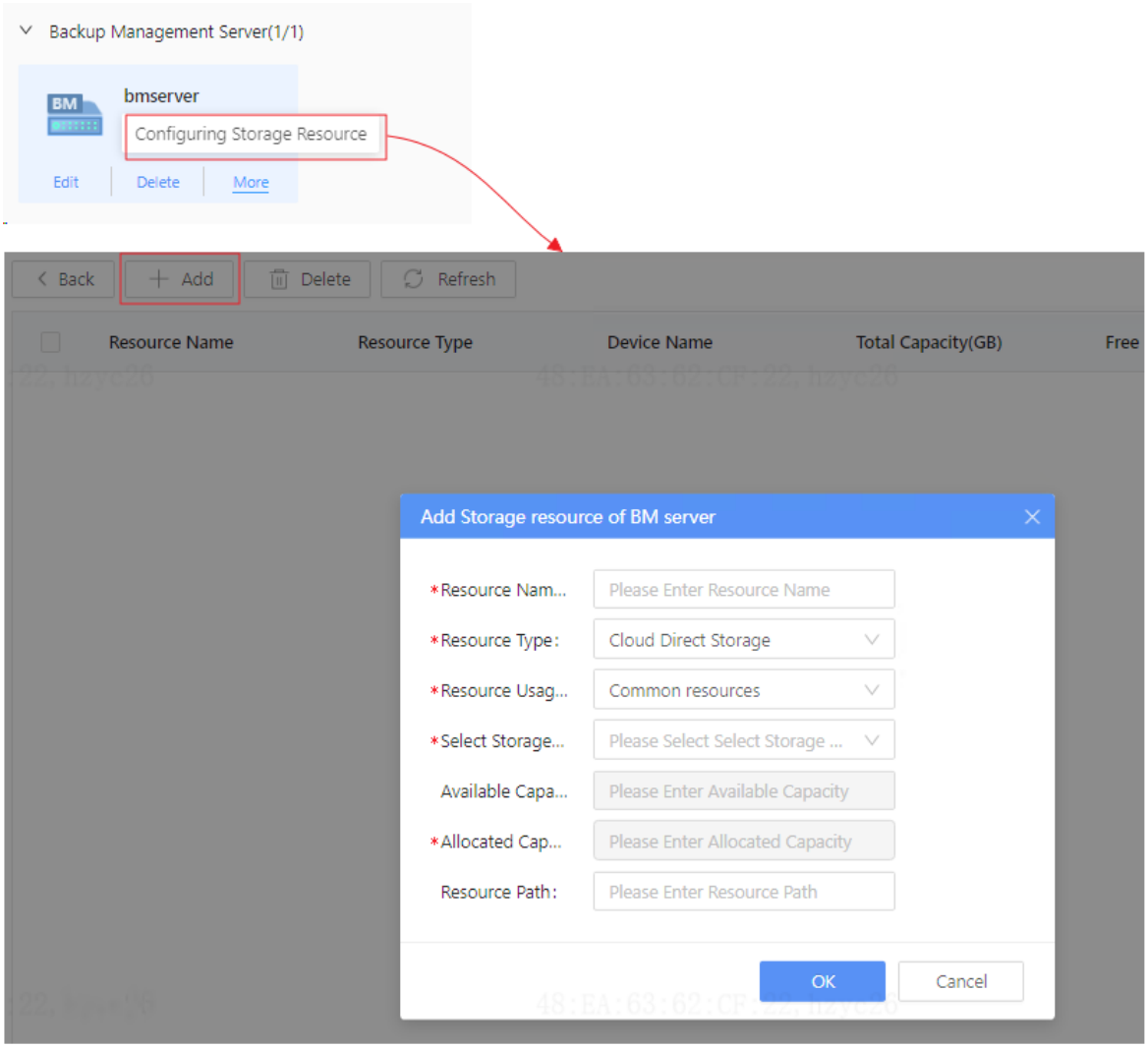
8.3 Recording Backup

Backup refers to storing the existing stored recordings again, the purpose is to prevent the original recordings from being written or deleted, or the video data is very important and needs to be stored twice.

Prerequisites

Please bind the backup server with recording backup resource first.

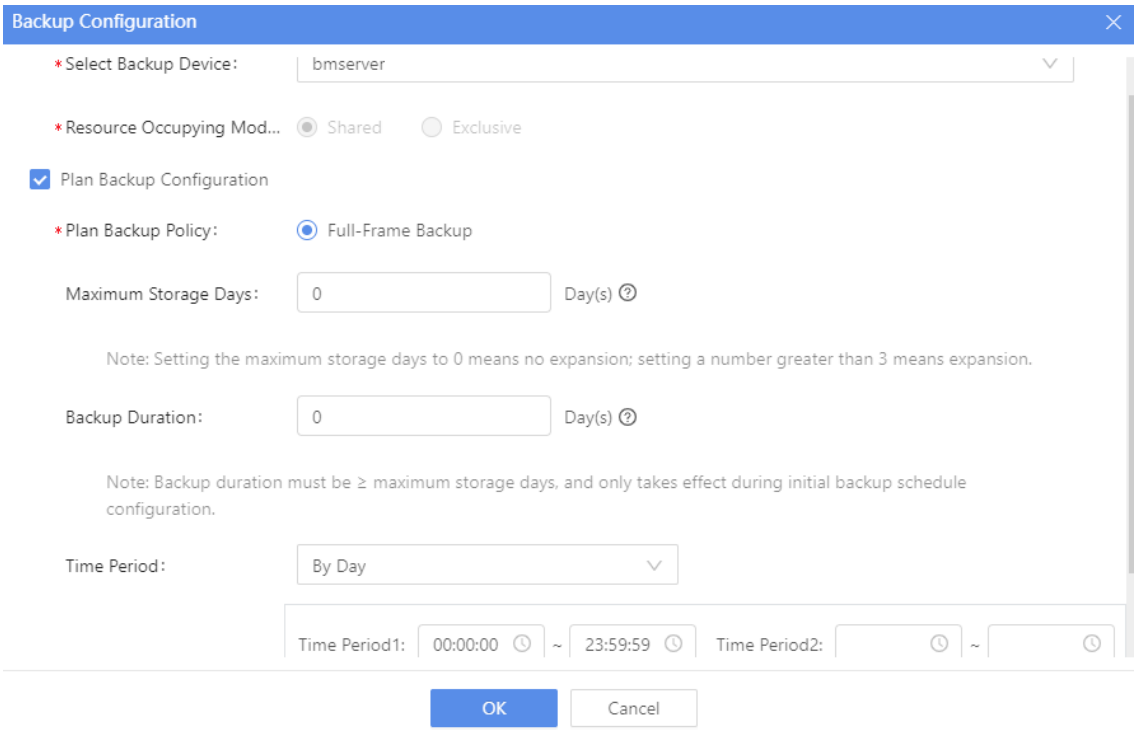
1. Go to **Device Management** > **Server Management**.
2. Click **More** > **Configuring Storage Resource** for a backup server.
3. Click **Add**.



Item	Description
Resource Name	Enter a custom resource name.
Resource Type	Choose Cloud Direct Storage.
Select Storage Device	Select recording backup resource (created in Disk Configuration).
Available Capacity	Automatically read by the system after selecting the storage device.
Allocated Capacity	The capacity allocated to the backup resource.

Backup Configuration

1. Go to **Storage Configuration** > **Recording Backup**.
2. Click the target organization on the left-side organization list.
3. Select multiple cameras (at least 2) in the organization, click **Batch Add**; or click for the camera. A page as shown below appears.



Parameter	Description
Select Backup Device	Select a backup server to assign recording backup resources to the camera.
Resource Occupying Mode	How the camera uses BM backup resources. • Shared (only supported): All the cameras that are specified to use the BM device share the backup resource.

4. Select whether to enable scheduled backup (Scheduled backup creates a backup schedule for recordings, periodically backing up recordings from specified time periods).
If scheduled backup is enabled, configure the parameters by referring to the table below.

Parameter	Description
Plan Backup Policy	Full-Frame Backup: Back up continuous frames.
Backup Duration	Used with **Maximum Storage Days** to determine the backup start time. If it is set to Y, it means that after the schedule is created, BM will start backup from the video recorded Y days ago. **Note:** • Valid range: 0-45. Must be greater than or equal to the maximum storage days. The same value is used by default. • The backup time span takes effect only when the backup schedule is configured for the first time. Once saved, the setting cannot be changed.
Maximum Storage Days	Used with **Backup Duration**, it defines the backup end time. If set to X, it means the BM will stop backup after X days from the start time. **Note:** Valid range: 0; 3-45. Setting it to 0 indicates continuous backup. Setting it to a value that is greater than or equal to 3 indicates backup for the specified number of days.
Time Period	You can configure the backup schedule by day or by week. The system will periodically back up recordings from the specified time periods according to this schedule.

5. Click **OK** to save the settings.

Note: The system starts the backup schedule by default after the configuration is completed.

Start/Stop Backup Schedule

- To start or stop the backup schedule for a camera, click Stop / Enable for the camera.
- To start or stop backup schedules for multiple cameras at a time, select the cameras and then click **Start** or **Stop**.

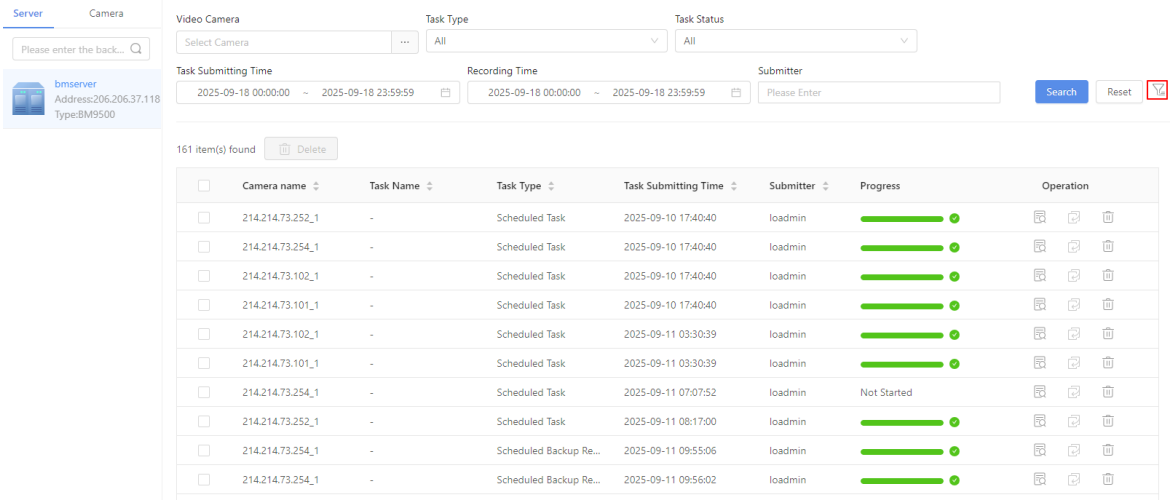
8.4 Backup Status

Check the status of backup tasks.

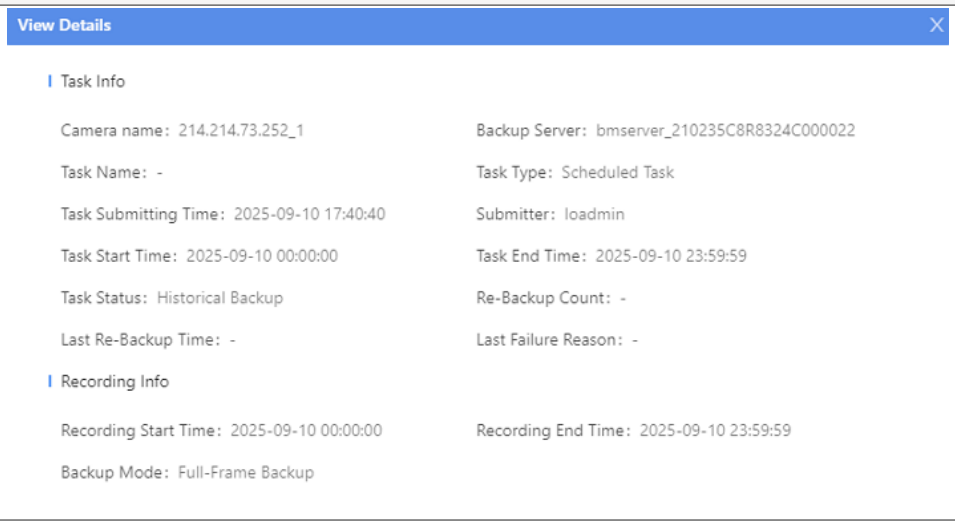
View Status by Server

Select the backup management server to view all backup tasks under that server.

You can search by camera, task type, task status, task submission time, recording time, and submitter. Click to expand or collapse the search criteria.

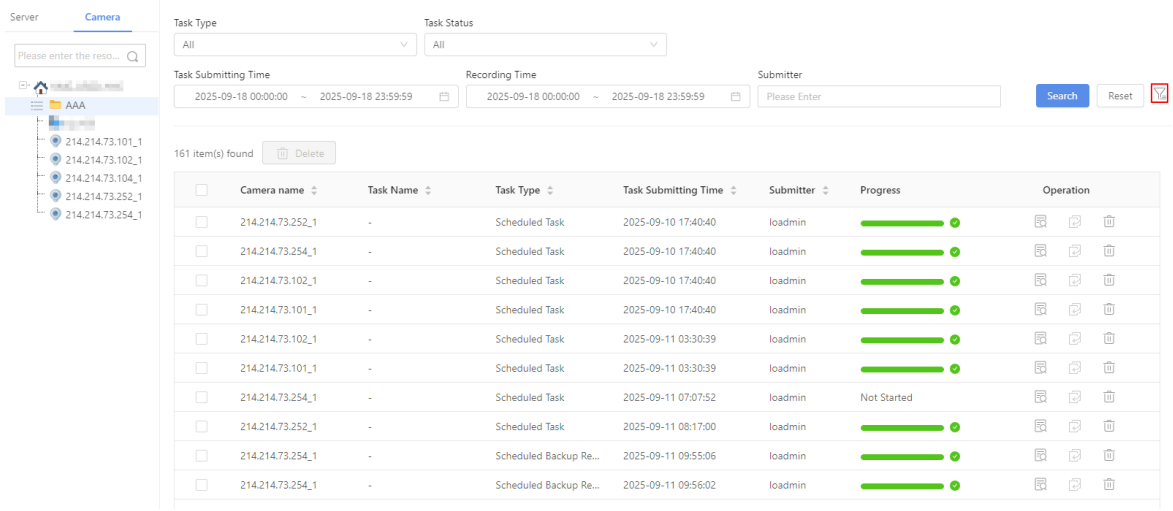


Parameter	Description
Camera	Search the backup tasks for the camera.
Task Type	• Scheduled Task: Backup according to a schedule. • Manual/Linkage Task: Manual backup, alarm-triggered backup. • Scheduled Backup Retry Task: After a scheduled backup fails, the system retries the backup.
Task Status	• Not started: The system will start backup after the recording has been stored for a while. • Backing up • Historical backup: Progress is at 100%. • Suspended • Paused: The schedule is stopped manually.
Task Submitting Time	Search for backup tasks created within that time period. **Note:** After the scheduled backup starts, a task will be automatically created for each recording period.
Recording Time	Search for tasks that have backed up recordings within that time period.
Submitter	The user who created the backup task.
Operation column	View details: Click to view the detailed information about a backup task.

Parameter	Description
	
	Re-backup: For a failed backup task, click to retry the recording backup.
	Delete: Click and then confirm to delete the backup task. **Note:** • Deleting a task will not delete the recordings that have already been backed up. • For scheduled tasks, if today's task is deleted, the backup will continue tomorrow.

View Status by Camera

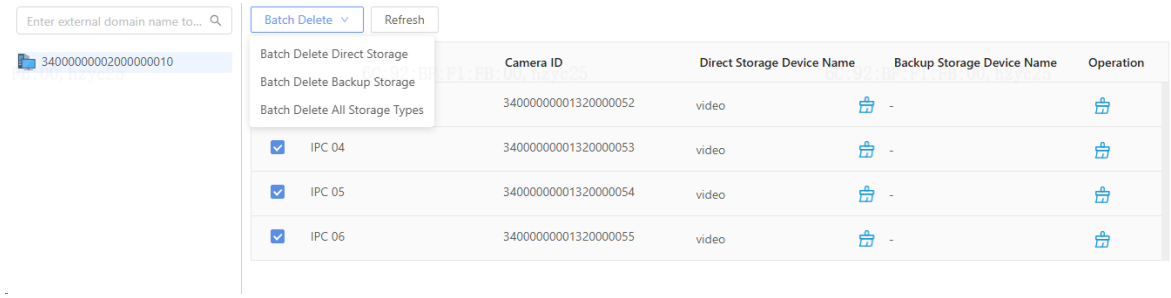
Select a camera to view its backup tasks. For parameter descriptions, see View Status by Server.



8.5 Cross-Domain Storage Diagnosis

After deleting an external domain or VSS NVR, the storage configured for its channels is not automatically deleted. Please manually remove the residual storage.

Go to **Storage Configuration > Cross-Domain Storage Diagnosis**. Select an external domain on the left to view devices with residual storage under that domain.



- Delete one by one: Click next to Direct Storage/Backup Storage to remove the corresponding storage; click in the **Operation** column to remove all storage types.
- Delete in batch: Select cameras, then click **Batch Delete**. You can choose to delete Direct Storage, delete Backup Storage, or delete all storage types.

8.6 Video Compression

This feature supports decoding an already-encoded video and then compressing it to generate a new re-encoded file, thereby further improving the compression ratio and reducing storage space. After compression, the bit rate is reduced, which saves transmission bandwidth. The video frame rate, video encoding format, and video resolution remain unchanged, with almost no loss of feature values, and no impact on video viewing or intelligent analysis services.

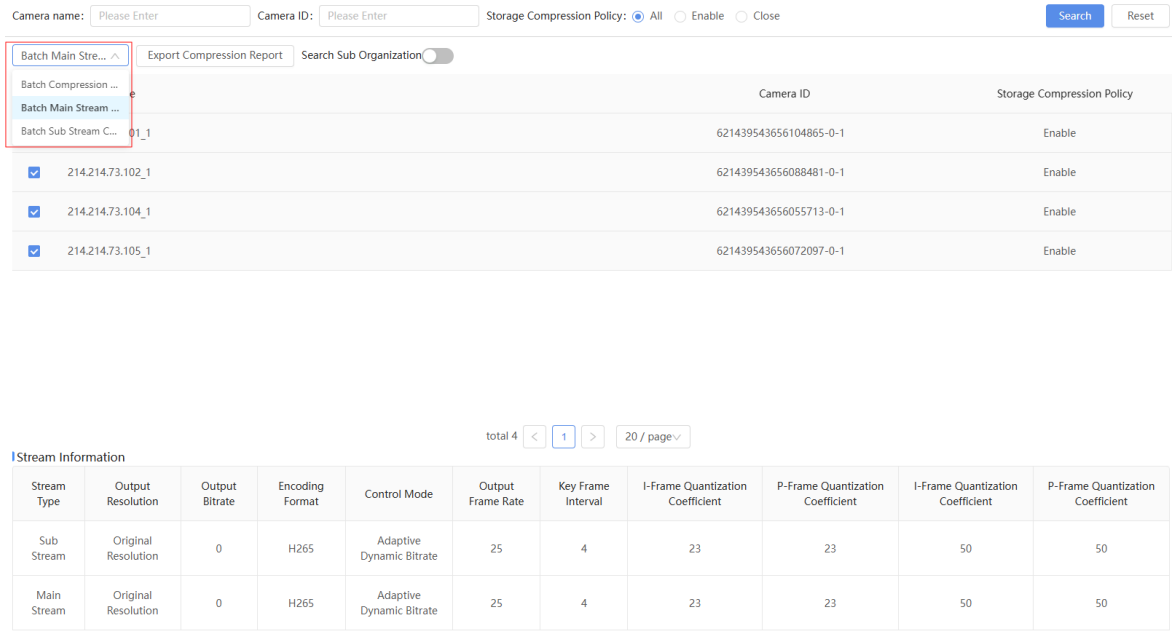
Compression Target	• Supports live video stream compression: saves bandwidth consumption • Supports storage stream compression: saves storage space
Applicable Networking	• Supports cameras accessed via local domain private/VSS/ONVIF protocols

Note:
This feature requires the configuration of an IVC9500- video compression server. Go to **Device Management** > **Server Management** to add a video compression server.

On the **Video Compression** page, you can configure video compression parameters, including storage compression policy, main stream compression, and sub stream compression.

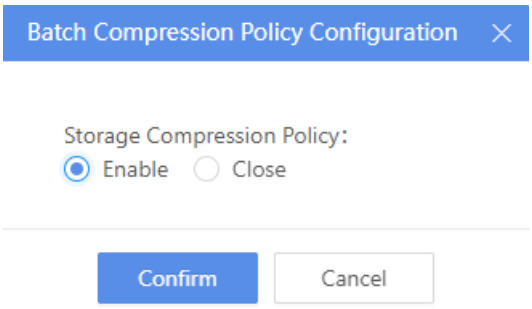
8.6.1 Batch Configuration

Select the cameras, and select the configuration item from the drop-down list.



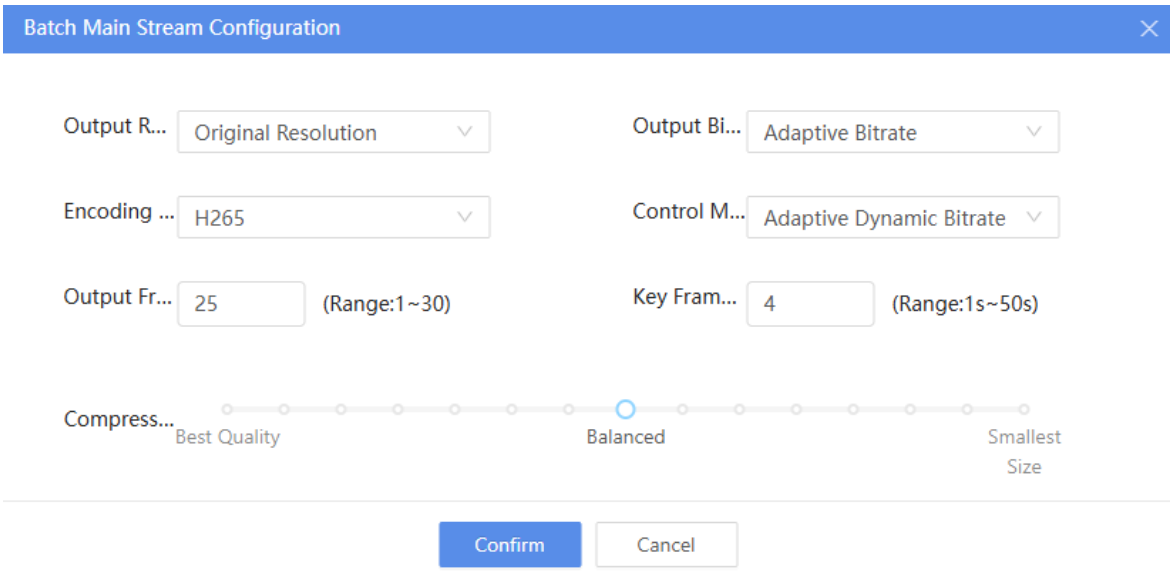
Batch Compression Policy Configuration

Configure whether to enable stream compression. When enabled, the stream is compressed before being written to the storage device.



Batch Main/Sub Stream Configuration

Configure the compression parameters for the main stream and sub stream respectively. The settings will apply to main/sub stream live video compression and main/sub stream storage compression.



Parameter	Description
Output Resolution	By default, the original resolution is retained. A smaller resolution results in a smaller compressed video size but lower image clarity.
Output Bit Rate	By default, the original bit rate is retained. A lower bit rate results in a smaller video size but lower image clarity.
Encoding Format	Set the video encoding format after compression: H264 or H265. Video size is reduced by changing the video encoding. H265 produces a smaller video size with a higher compression ratio.
Control Mode	Fixed bit rate, dynamic bit rate, adaptive dynamic bit rate (adjusting the bit rate based on inter-frame changes), or fixed quantization parameter. Adaptive dynamic bit rate provides the highest compression ratio.
Output Frame Rate	1–30. The default value of 25 is recommended. A lower frame rate reduces the space occupied by the video and increases the compression ratio (not recommended to reduce, as it may cause stuttering).
Key Frame Interval	1s–50s. The default value is 4s. A larger key frame interval reduces the space occupied by the video and increases the compression ratio.
Compression Quality	The smaller the compressed size, the worse the image quality.

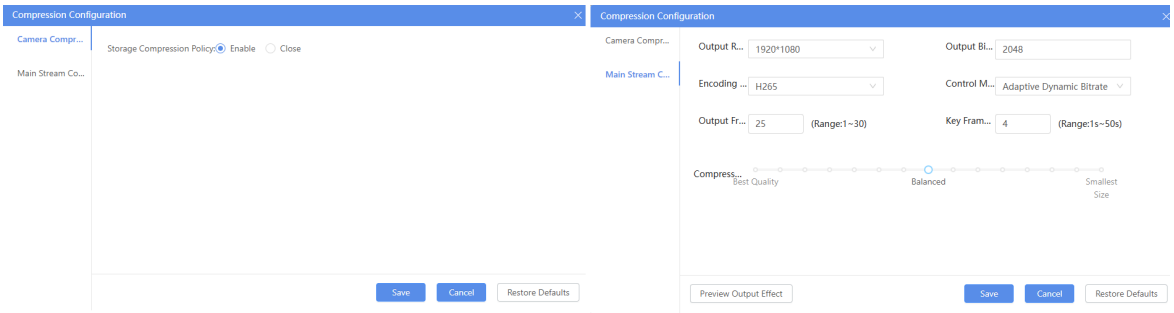
Parameter	Description
	• If the image details are simple, it is recommended to select smaller size to achieve a higher compression ratio. • If the image details are complex, it is recommended to select better quality to ensure good video quality.

View Stream Information

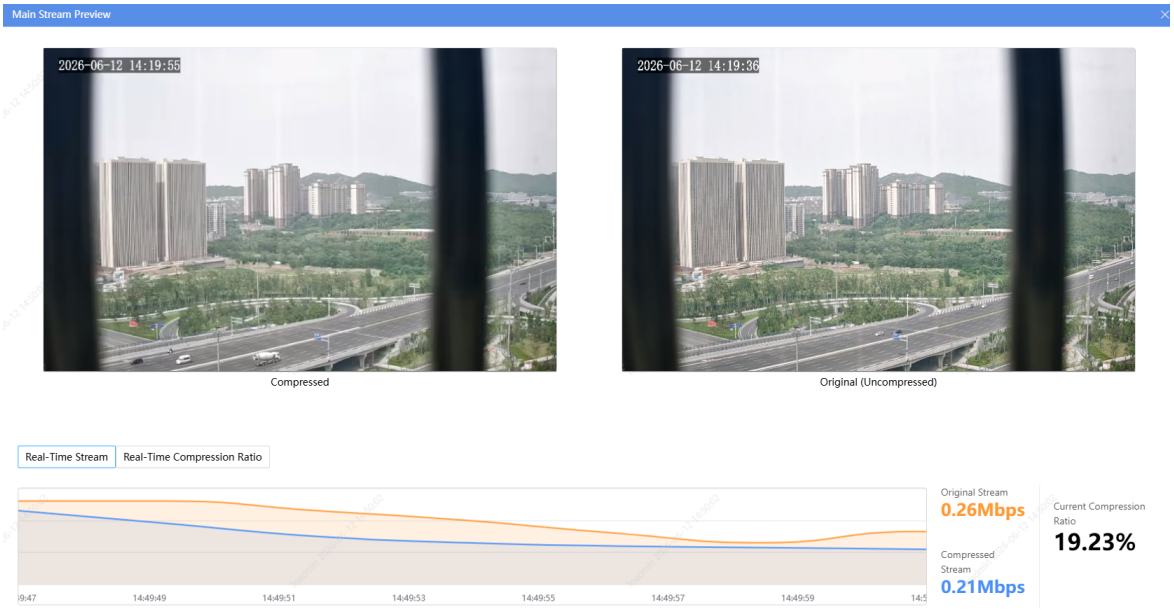
After configuration, select a camera in the list to view its main stream and sub stream compression parameters.

8.6.2 Single Configuration

Hover over the camera name, and click to configure the compression policy and compression parameters for the camera. For parameter descriptions, see Batch Configuration .



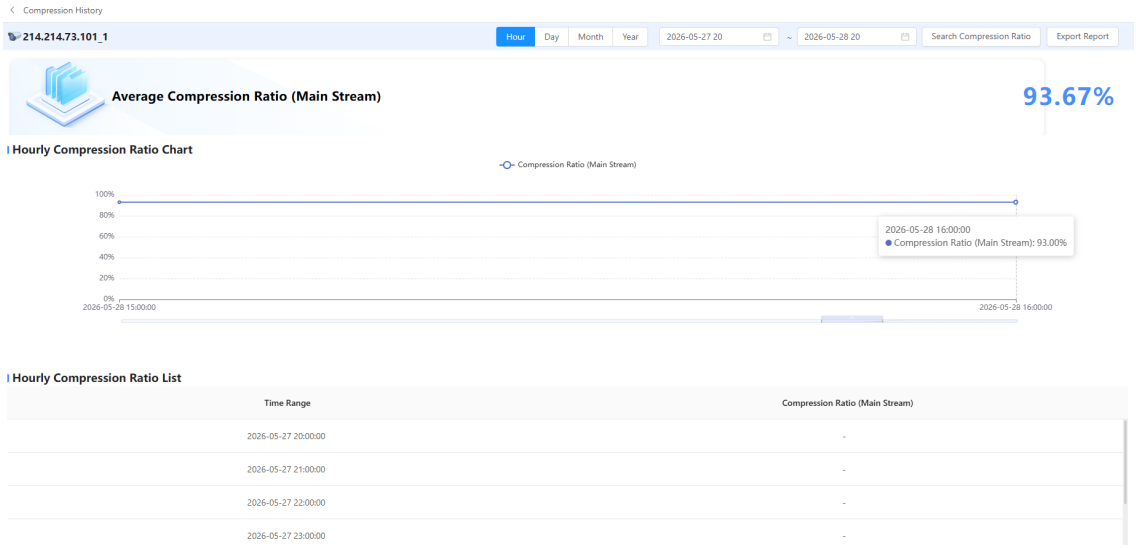
When configuring a single camera, click **Preview Output Effect** to view the comparison of the image/stream before and after compression. Depending on the compression parameter settings, the compressed image may have reduced quality.



8.6.3 Compression Statistics

You can view the historical compression status of cameras, including average compression ratio, compression ratio trend chart, and compression ratio detailed data.

1. Hover over the camera name, and click .
2. In the upper-right corner, select the time unit and time range, and click **Search Compression Ratio** to display the search results.



3. Click **Export Report** to export the compression ratio list.

9 Video Application

Based on the live videos collected from front-end devices, this function provides various options for live and playback viewing and scenario-based applications. This allows users to view real-time situations and review past events, replacing on-site security patrols and improving the efficiency of security management.

Functions

Menu	Description
Live View	Allows users to view real-time audio and video information collected by cameras in video windows for on-site status and timely detection of any anomalies. You can view the live video from a single camera or call the preset scene using camera sequence, group display, and group sequence. During live view, operations such as PTZ control, patrol, and video intercom are supported.
Playback	Allows users to search and download recordings stored on the storage resources of the platform, camera's SD cards, and NVR disks, as well as backtrack historical events with anomalies.
Video Wall	Allows users to create video wall layout on the client and bind video output channels of decoders to play video images on a physical video wall.
Smart Live View	Allows users to view live videos of video channels under smart IPCs and NVRs, as well as access control devices. The real-time snapshot data and alarms (face match records, vehicle match records, and person/motor vehicle/non-motor vehicle data from multi-target detection) are displayed when playing smart live view.

Note:
The Live View and Playback functions are integrated in the **Live View** page. For the same camera, the unified right-click operation allows you to start live view or search recordings. Additionally, live videos and recordings can be displayed on one screen simultaneously. The client display screen supports up to 64 split screens and allows for customized screen layouts, allowing you view more videos from different channels at various times.

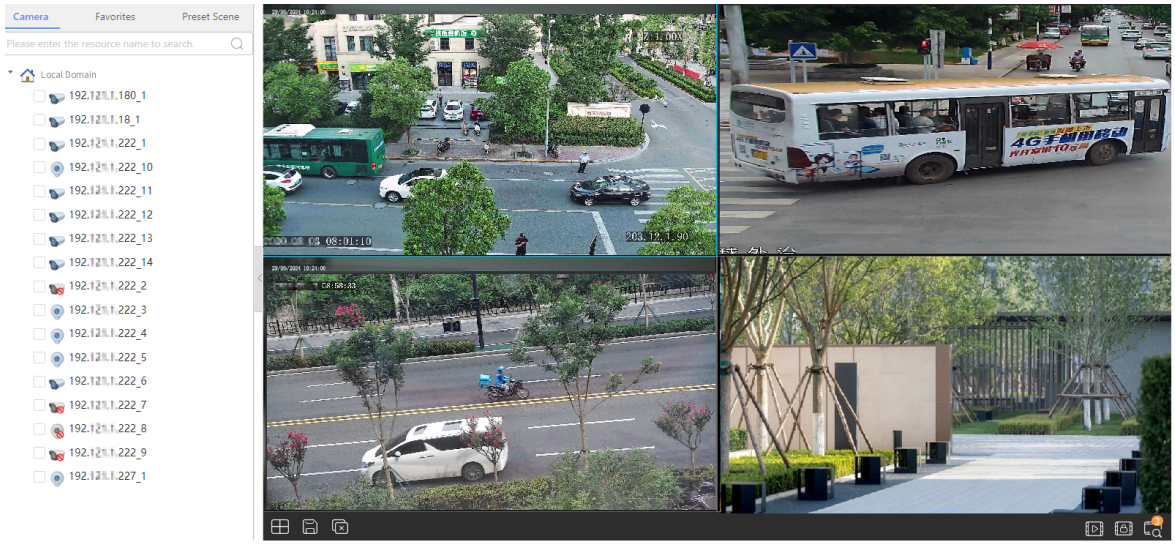
9.1 Live View

Go to **Video Application > Live View**.

View real-time audio and video information collected by cameras in video windows for on-site status and timely detection of any anomalies.

Workflow

1. Add cameras. See Device Management > Private Device or ONVIF Camera.
2. Start live view. See Camera Live View.



9.1.1 Camera Live View

View real-time live videos collected from cameras.

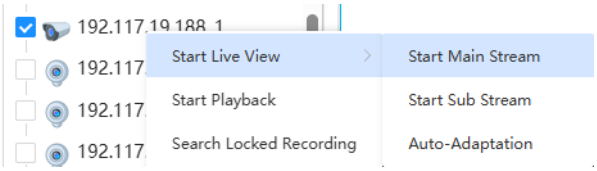
Start Live View of Single Channel

- Select a window and double-click on an online camera.
- Drag the online camera to a window.

Figure 9-1: Start Live View

- Select a window, right-click on an online camera, click **Start Live View**, and then select **Start Live View** or **Auto-Adaptation**.

Figure 9-2: Right-Click Menu

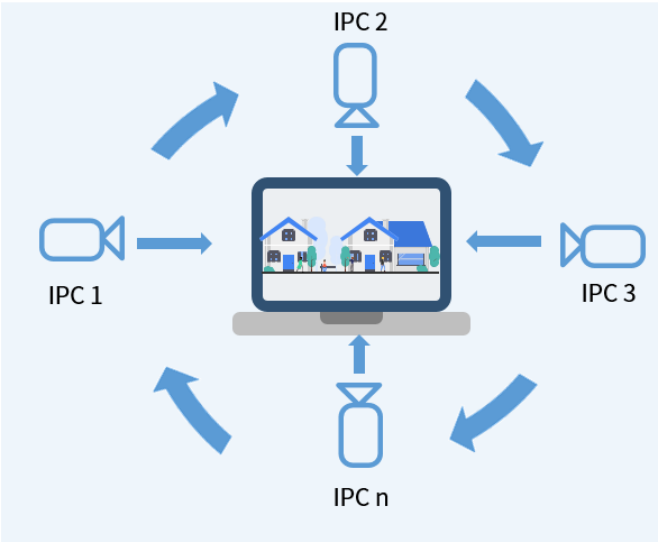


Batch Start Live View

- Select cameras, right-click on cameras, select **Batch Start Live View**, and then live videos of the selected cameras will be played in an adaptive layout.
- Right-click on organization, and select **Batch Start Live View**, and then live videos of all cameras within the selected organization will be played in an adaptive layout.

9.1.2 Camera Sequence

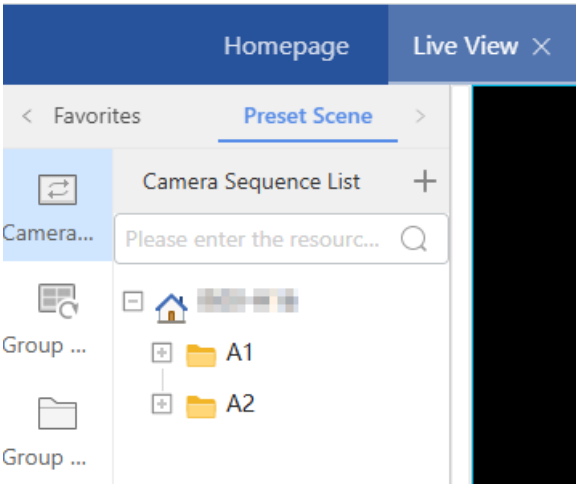
Play live videos of cameras in one window in sequence.



9.1.2.1 Camera Sequence Resource

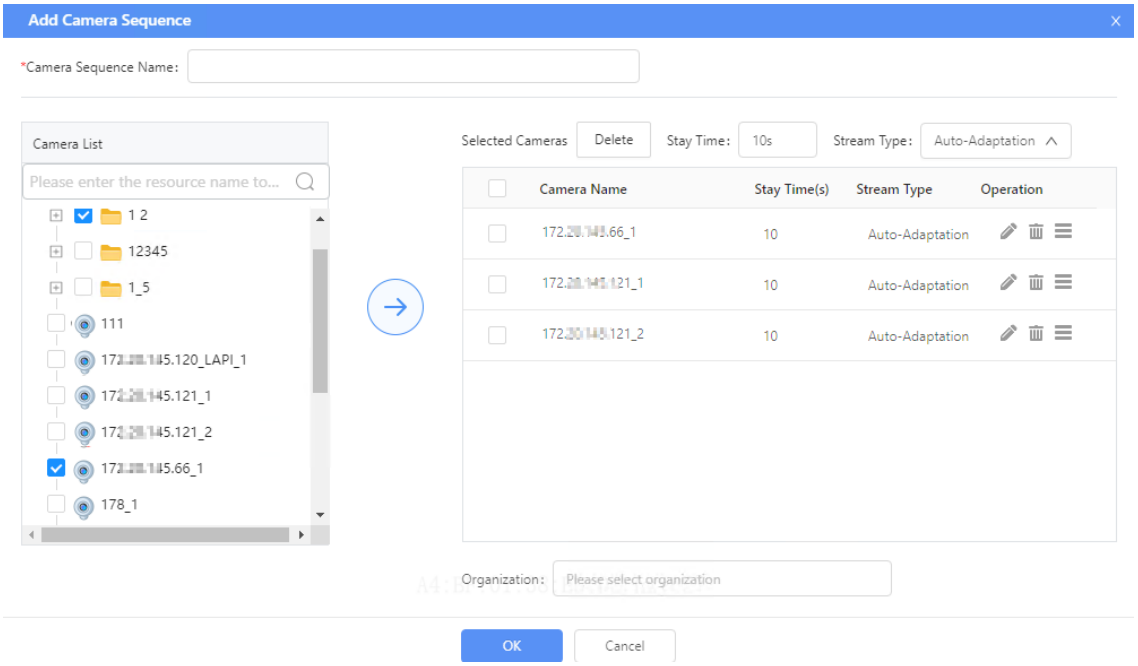
Add Camera Sequence Resource

1. Go to **Live View - Preset Scene - Camera Sequence**.



2. Click + in the upper-right corner of the camera sequence resource list.

Figure 9-3: Add Camera Sequence



3. Set the camera sequence name (max 20 characters and must not contain & < > |)
4. Select cameras from the left-side list (you can also select organization for batch selection) and then click → to add them to the camera sequence group.

Note:

- You can also set the stay time and stream type display interval and stream type for them. When added, you can click ✎ in the **Selected Camera List** to modify.
- You can click 🗑 to delete the camera or select cameras and click **Delete** to delete them in batches.
- You can drag ☰ to adjust its display order.

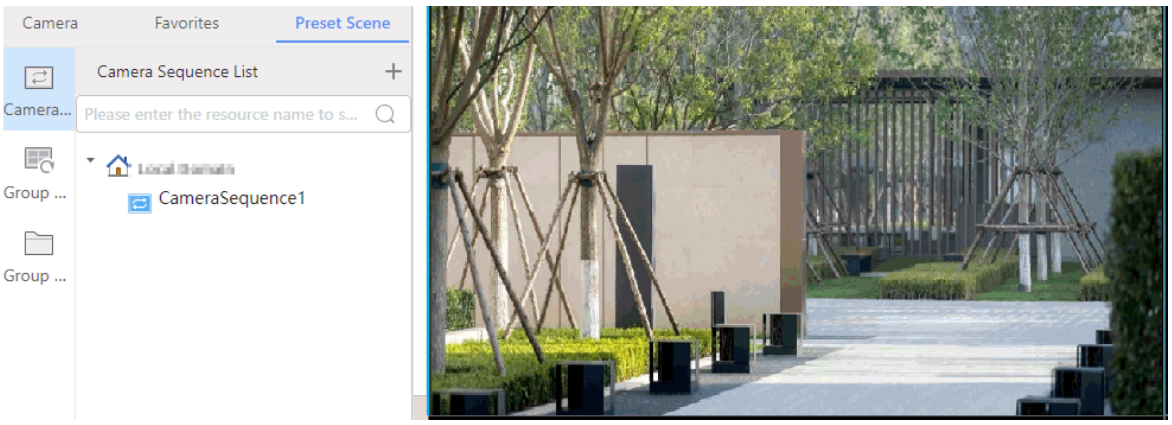
5. Choose an organization for the camera sequence resource.
6. Click **OK**.

Start Camera Sequence

Choose a way to start camera sequence:

- Select a window, and then double-click on the camera sequence resource.
- Drag the camera sequence resource to a window.
- Select a window, right-click on the camera sequence resource, and then select **Start**.

Figure 9-4: Camera Sequence



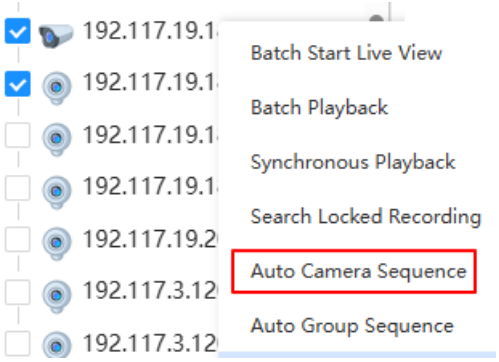
After double-clicking to enlarge a window in the camera sequence, you can click < > in the toolbar to switch to the previous/next camera.

Manage Camera Sequence

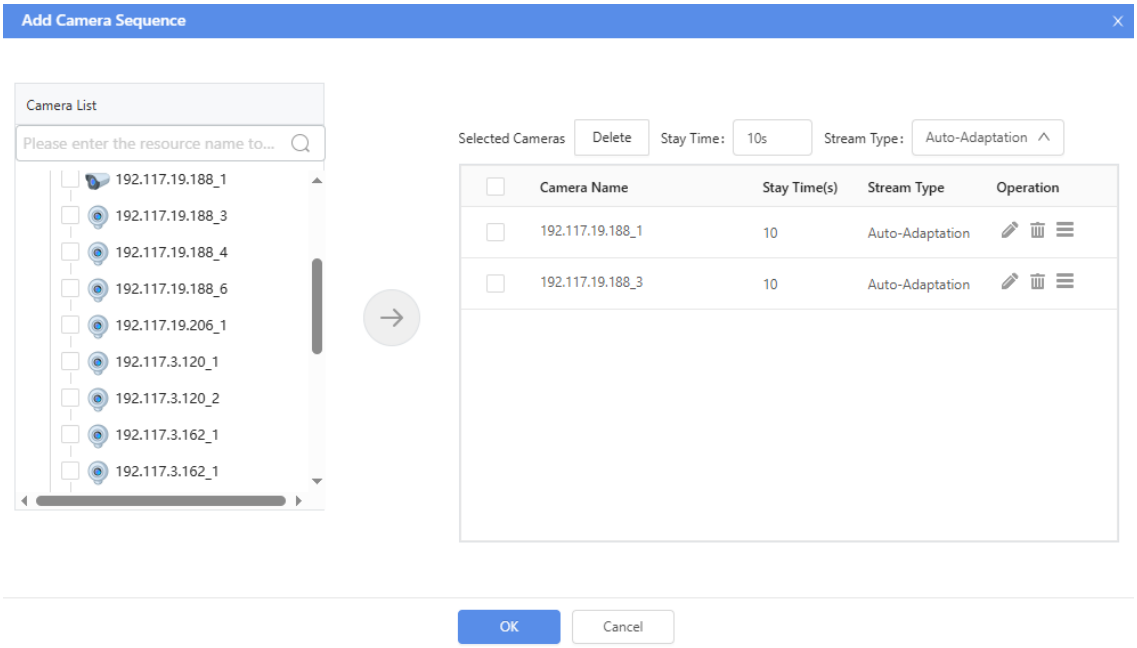
Right-click on a camera sequence resource to edit, delete, or add to favorites.

9.1.2.2 Auto Camera Sequence

1. In the camera list, select two or more cameras or choose an sub-organization.
2. Right-click and select **Auto Camera Sequence**.



3. Set the camera sequence parameters, then click **OK**, the live videos of the selected cameras will be played in single window in sequence.



9.1.3 Group Display

Group display is a kind of view in which multiple cameras are playing live videos in specific windows. By saving commonly used video views as group displays, you can easily call them with one-click, allowing for quick and convenient access to your preferred camera combinations.

Add Group Display

When live videos are playing, you can click on the toolbar to save the ongoing live view services as a group display.

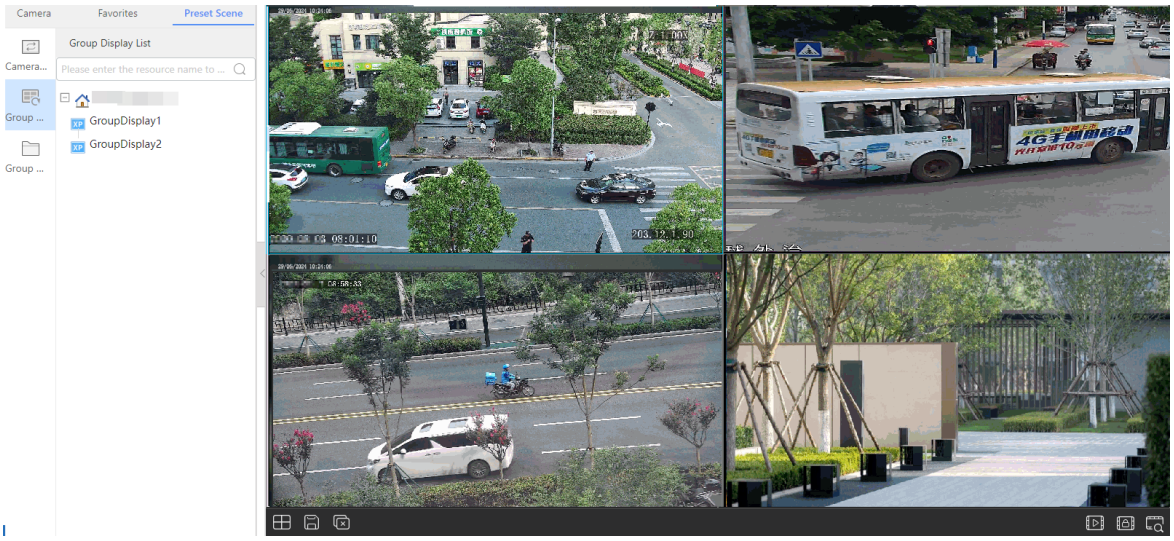
Note:
If a camera sequence/group sequence is playing in the window, only the currently active live view services in the window will be saved.

Start Group Display

Choose a way to start group display:

- Double-click on a group display resource.
- Right-click on a group display resource and choose **Start**.

Figure 9-5: Group Display



After double-clicking to enlarge a window in the group display, you can click < > in the toolbar to switch to the previous/next camera.

Manage Group Display

Right-click on a group display resource to delete or add to favorites.

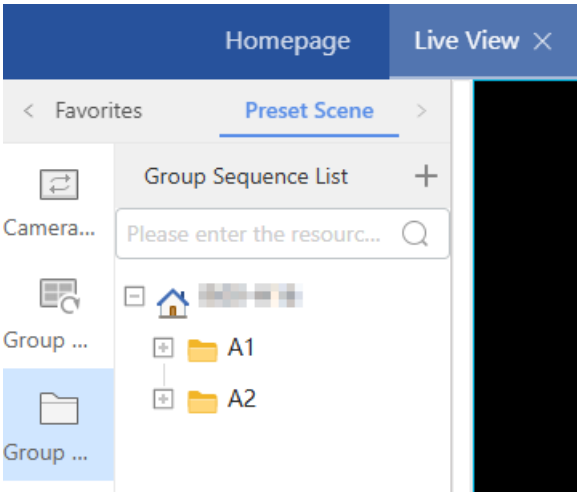
9.1.4 Group Sequence

Cycle through live videos of multiple group displays at set intervals in multiple windows.

9.1.4.1 Sequence Resource

Add Sequence Resource

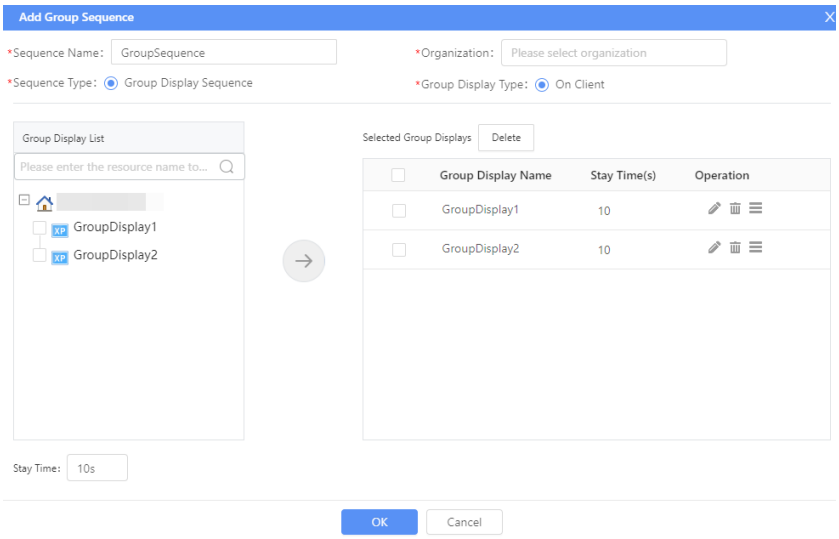
1. Go to **Live View - Preset Scene - Group Sequence**.



2. Click + in the upper-right corner of the sequence resource list.
3. Set sequence parameters such as sequence name, and also create sequence groups.

Note:
The sequence name allows up to 20 characters and must not contain % < > |

Table 9-1: Sequence Configuration Description

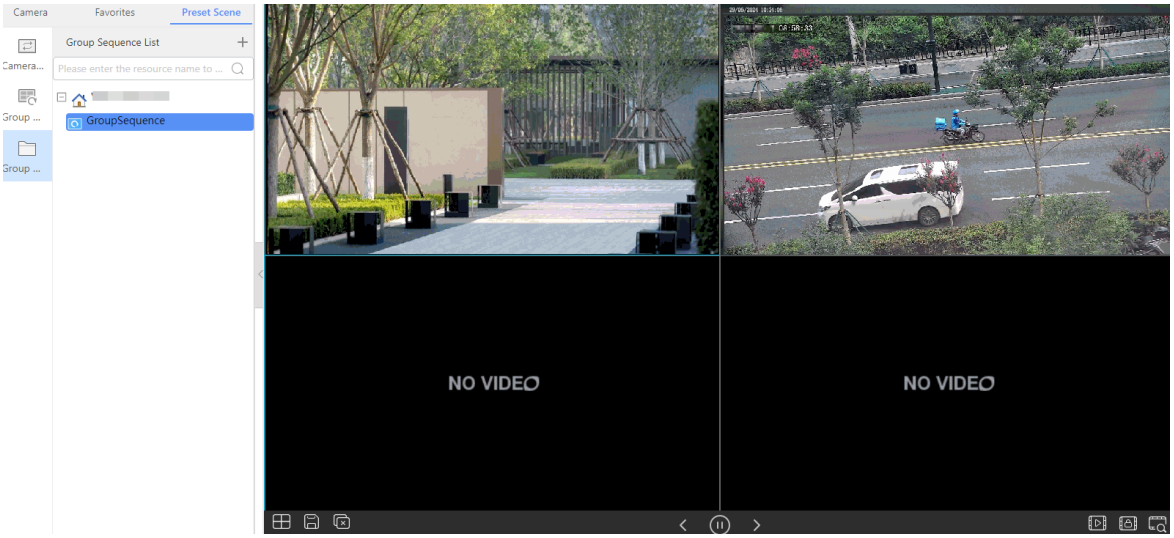
Sequence Type	Description
Group Display Sequence	Play multiple camera groups in sequence. **Note:** Prerequisite: You have Group Display resources configured.  (1) Select group display resources from the left-side list, set the duration of the live video per group, and then click → to add them to the sequence group. (2) In the right-side list, you can: click ✎ to edit the group display stay time; click 🗑 to delete the group display from the group sequence group; drag ☰ to adjust the group display order.

4. Click **OK**.

Start Group Sequence

In the group sequence list, double-click on a group sequence resource to start.

Figure 9-6: Group Sequence

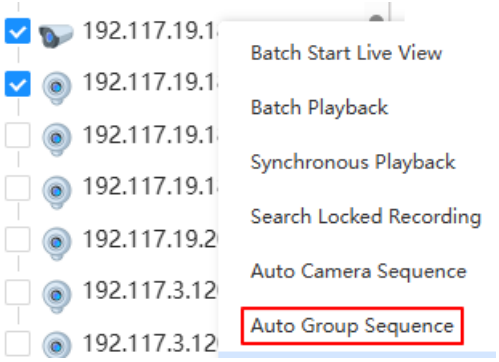


Manage Group Sequence

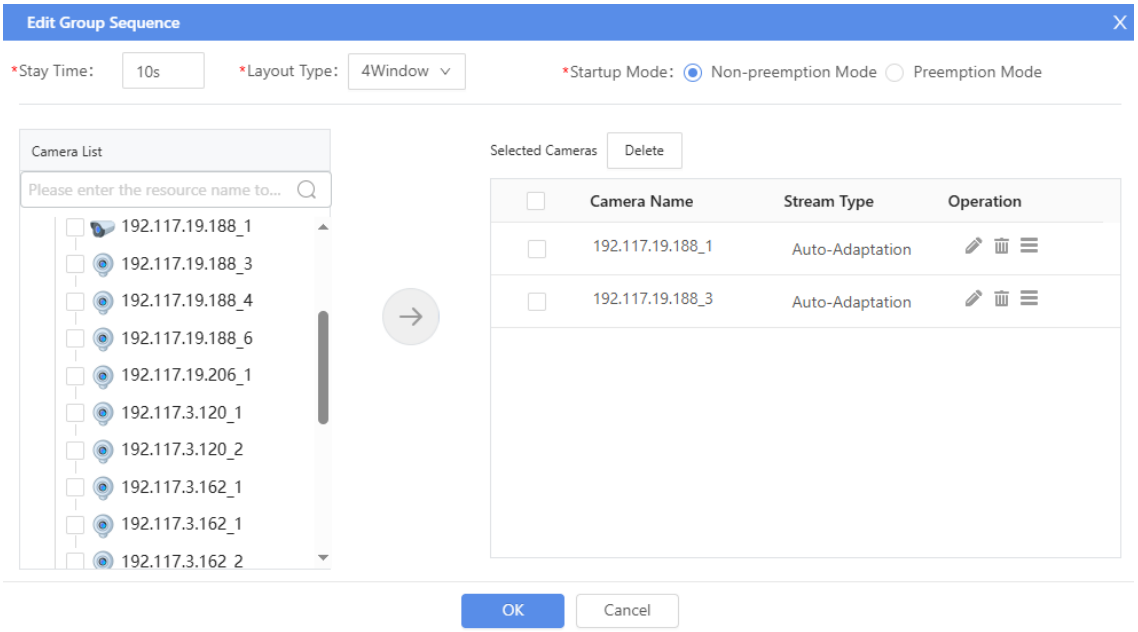
Right-click on a group sequence resource to edit, delete, or add to favorites.

9.1.4.2 Auto Group Sequence

1. In the camera list, select two or more cameras.
2. Right-click and choose **Auto Group Sequence**.

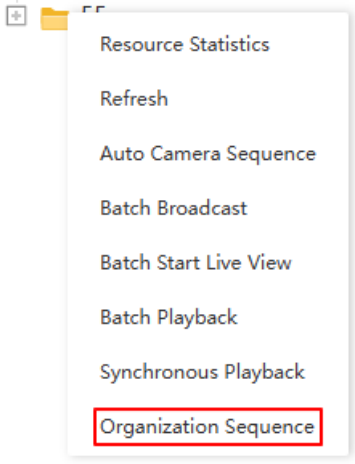


3. Set the group sequence parameters, then click **OK**, the live videos of the selected cameras will be played in all windows in sequence.



9.1.4.3 Organization Sequence

1. In the camera list, select an organization.
2. Right-click and choose **Organization Sequence**.



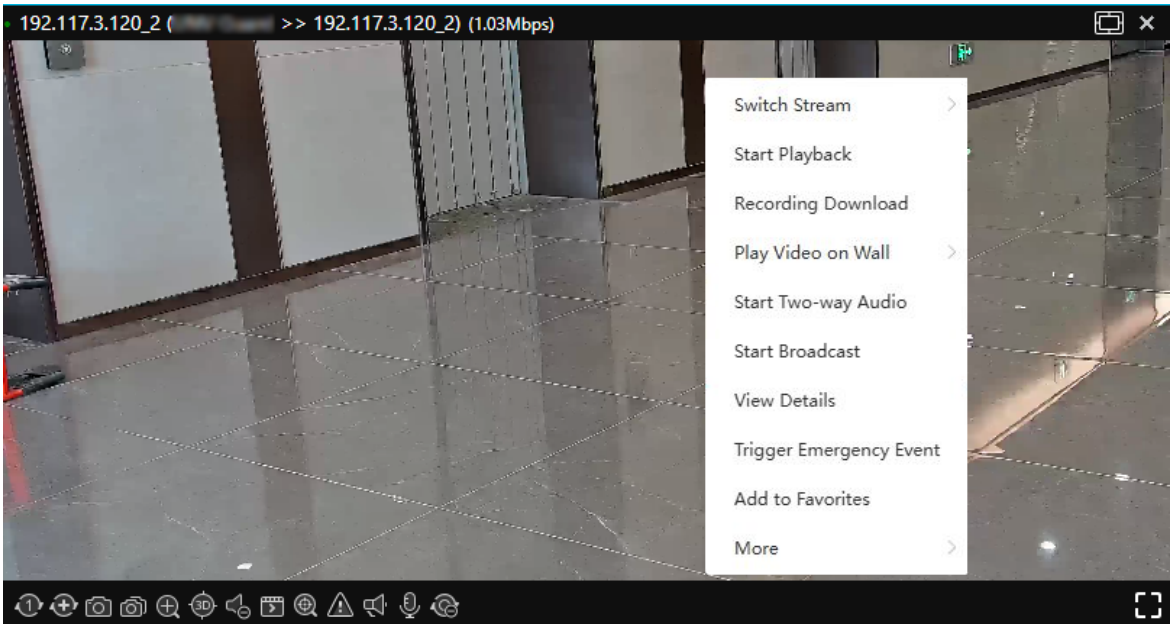
3. Set the sequence interval, then click **OK** to play the live videos from the cameras under the selected organization in all windows in sequence.

9.1.5 Live View Operations

Use the right-click menu, live view toolbar to set live video parameters, take snapshots, etc.

Live View Right-Click Menu Operations

You can right-click on a live view window and then use the pop-up menu to switch stream, start playback, recording download, play video on wall, start two-way audio, start broadcast, view details, trigger emergency event, add to favorites, or more options.



Live View Toolbar Operations

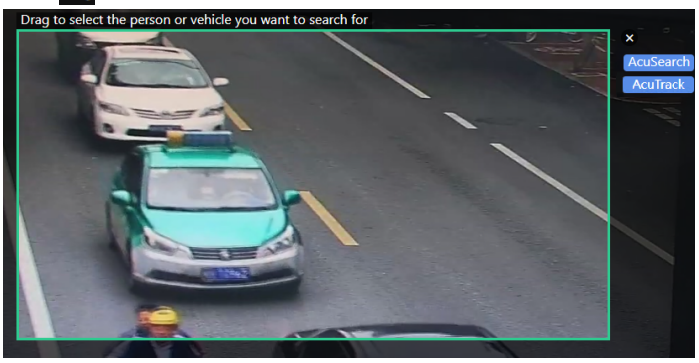
The toolbar appears when you hover the mouse over a window.

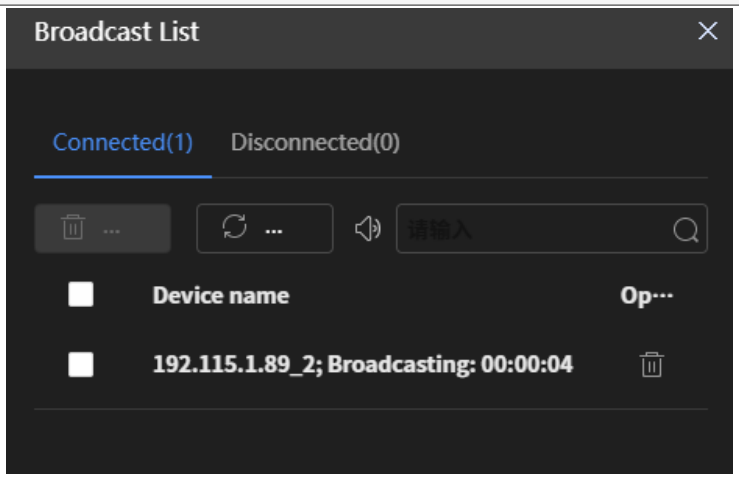
Figure 9-7: Window Toolbar

For toolbar buttons, please refer to the actual page.

Table 9-2: Toolbar Operations

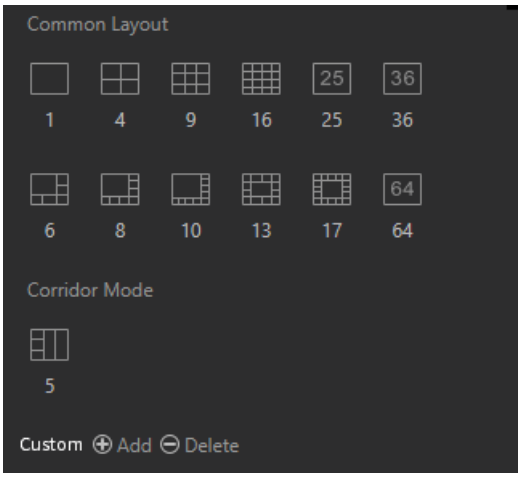
Icon	Function	Description
	Snapshot	Capture the current image(s) in the window and save to local.
	Continuous Snapshots	
	Digital Zoom	Zoom in on the area of interest on the image. **Note:** Use the scroll wheel to zoom in or out.
	Preset	Buttons for No.1 and other presets. Click to call the corresponding preset and view images of the desired scene instantly.

Icon	Function	Description
	3D Positioning	Perform 3D positioning, including click-to-position and drag-to-zoom. • Click to position: Click anywhere on the image, and the camera automatically centers on the point that you clicked to display the image. • Drag to zoom: Drag on the image from top left to bottom right to zoom in, and drag in the opposite direction to zoom out.
	Volume control	Click to use the slider to adjust the volume of the video.
	Start/Stop Local Recording	Record the live record a live window the live view image, and save it to.
	AcuSearch/AcuTrack	When a target of interest is identified in the live video you can select the motor vehicle/non-motor vehicle/pedestrian target in the current image to search the full video and image data for scenes where the target appeared. 1. Click to freeze the current frame.  2. Select the target to search for: • Hold down the mouse and drag the area within the green box to move its position. • Hover the mouse over the edges or corners of the green box, when the cursor changes to an arrow, hold and drag to resize the green box. • To exit the search, click X. 3. Choose a search mode. Two modes are available: • Click the **AcuSearch** button at the top right corner of the green box to go to the SeekFree page, where the system will automatically search for all capture records of the target within the green box (see Search by Image). • Click the **AcuTrack** button at the top right corner of the green box to go to the AcuTrack page, where you can search for recordings containing the target in the green box.
	Trigger Emergency Event	Clicking the icon will trigger an emergency event. This function allows users to manually trigger an alarm when they notice an abnormality during live view.
	Start/Stop Broadcast	Click the icon to start one-to-one audio broadcast to the camera. The broadcast is one-way.

Icon	Function	Description
		
	Two-way audio	Click the icon to start one-to-one audio intercom with the camera. The intercom is two-way. • Audio: Sound from the camera to the client. • Microphone: Sound from the client to the camera. • Click **Hang Up** to end the two-way audio.
	Enable/Disable PTZ Shortcuts	• Enabled: Preset buttons appear in the live view toolbar. Clicking on the video image allows you to control PTZ movement, enabling quick operations. • Disabled: Preset buttons are hidden from the live view toolbar. Clicking on the video will not trigger PTZ movement, preventing accidental operations.

You may also use the toolbar at the bottom:

- : Change the window layout. You can customize the number of windows, or choose 1/4/6/8/9/10/13/16/17/25/36/64 windows or corridor mode (intended for narrow scenes such as a corridor) as needed.



- : Save the current widow services as a group display.
- : Close all videos.
- : Play local videos in the window.

9.1.6 PTZ Control

For PTZ cameras, clicking on the live video will expand the PTZ control panel.

Figure 9-8: PTZ Control Panel

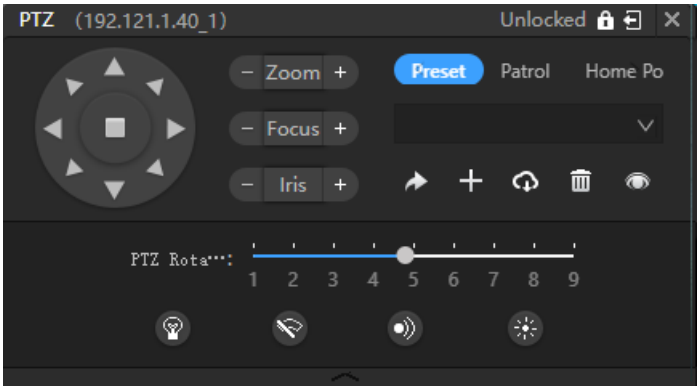
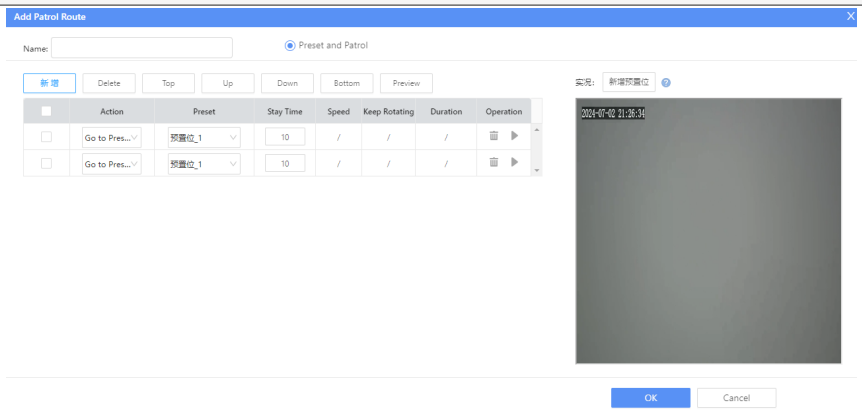
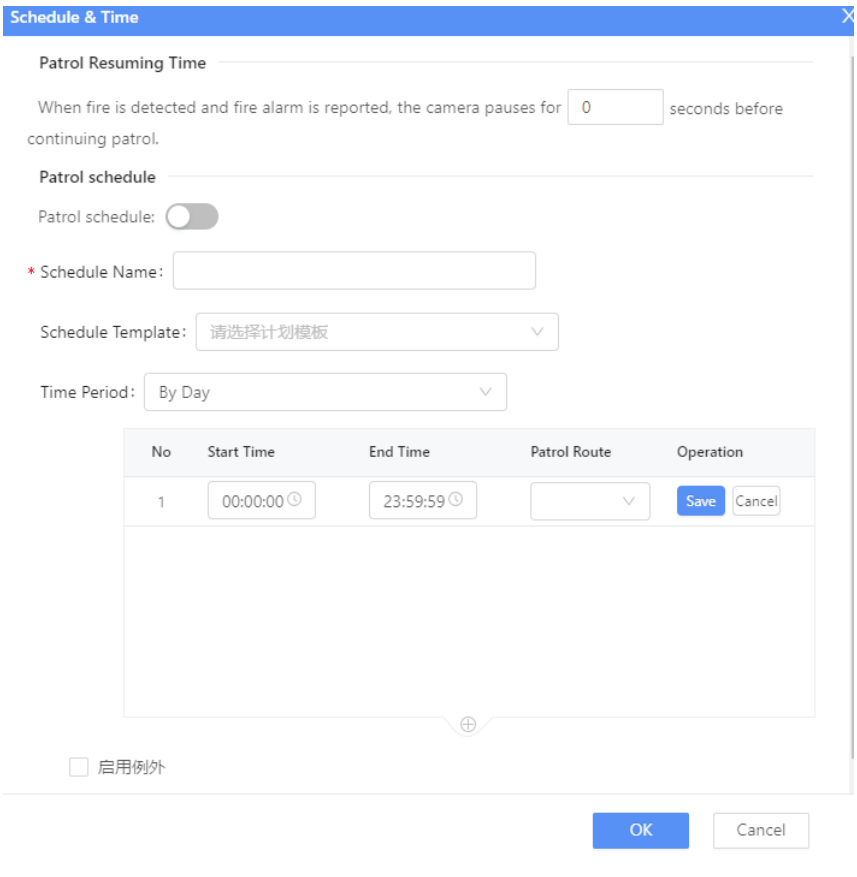
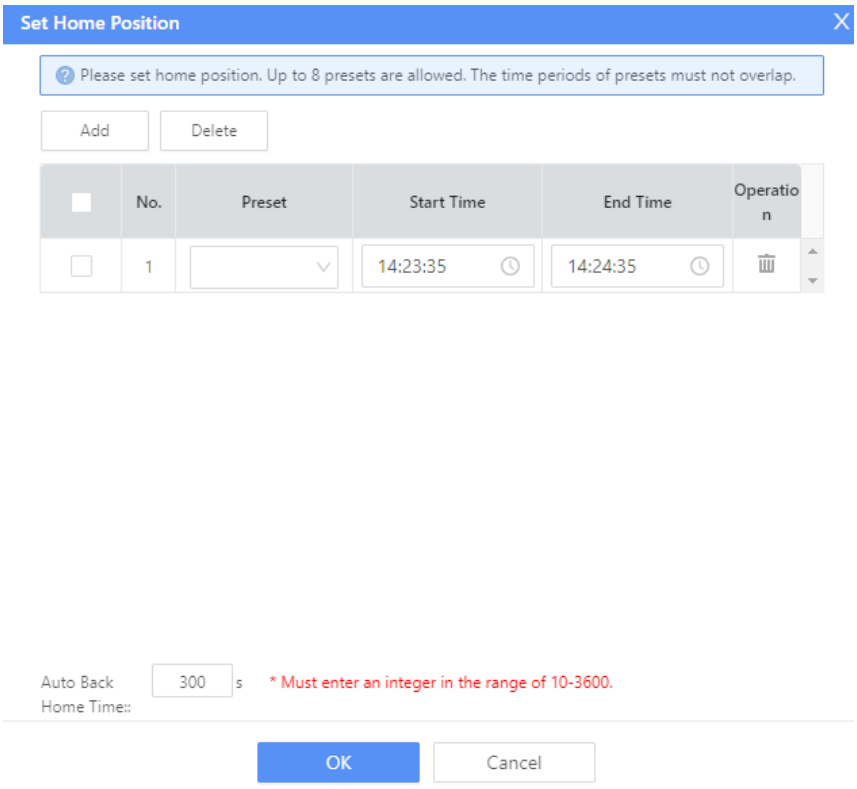
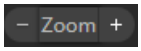
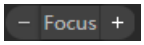
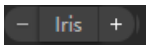
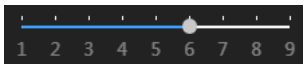


Table 9-3: PTZ Control Panel Operations

Icon	Description
/	Lock or unlock the PTZ. • When the PTZ is locked, only the super admin can control the PTZ. Other users must wait till the PTZ is unlocked or till the auto release time expired. • When the PTZ is unlocked, a high-level user can preempt control from a low-level user. • For parent and child domains that are connected via GB/T28181, the parent domain can lock the PTZ in the child domain. **Note:** • Any user can control an idle PTZ. Default policy of PTZ control: a high-priority user can preempt control from a low-priority user; a user in the parent domain can preempt control from a user of the same priority level in the child domain; in other cases, the first user operating the PTZ gains the control. The priority level of a local-domain user is the priority level of the user's role; the priority level of the external-domain user is priority level of the user's role in the external domain. • The policy of PTZ control and PTZ auto release time are configured in the PTZ.
	Release PTZ.

Icon	Description	
	• The PTZ is idle after being released and can be controlled by any user. • The locked PTZ is automatically unlocked after being released.	
Preset	Preset: You can set desired shooting angles or positions as presets to focus on areas of interest. After being idle (without user action) for a certain length of time, the PTZ automatically goes to a specified preset to view the key area.	
		Go to a preset. Rotate the camera to a specified preset.
		Add a preset. Add a preset for cameras in the local or external domain, that is, adding the current pan/tilt status to the preset list. **Attention:** Make sure the preset ID is not in use; otherwise, the current preset status of the preset ID will be replaced by the new preset status.
		Sync with front-end presets. For cameras within the platform, the preset positions configured on the camera side will be synchronized to the platform. For cameras in lower-level platform, the preset positions configured for the camera in the lower-level platform will be synchronized to the higher-level platform. **Note:** This function is available to cameras connected via private protocol, not to cameras connected via ONVIF.
		Delete a preset.
		Set the home position: Choose a preset position that the camera automatically returns to after PTZ control is released. • Set an idle time before the camera returns to the home position. By default, the newly added preset is the home position; you may also choose an existing preset as the home position. • The camera automatically returns to the home position after PTZ control is released and the idle time expired (no user operation during the specified period). • The home position mode can be single-home mode or multi-home mode. For multi-home mode, you need to set a schedule (up to 8 periods) and assign a period for each home position. • If a home position already exists, it will be replaced by the new home position.
Patrol	Patrol route: The camera pans and tilts according to a sequence of preset actions.	
		Start patrol.
		Stop patrol.
		Add a patrol route. Click the icon, and then add a patrol route in the pop-up window.

Icon	Description
	 • To rotate the camera to a preset, you need to set the preset ID/description, and the length of time that the camera stays at the preset. • To rotate up/down/left/right, you need to set the rotation speed, whether to keep rotating, and the rotation duration. **Note:** • A patrol route includes at least two actions, including going to a preset and rotating up/down/left/right. It may include one action only when the action is rotating up/down/left/right all the time. • If the action is set to rotating up/down/left/right all the time, then actions following it will not be performed.
	Delete a patrol route.
	Edit a patrol route.
	Configure a patrol schedule. Click the icon, and then add a patrol schedule in the pop-up window. 

Icon	Description
Home Position	Set whether to enable home position. To enable home position, click **Set** and then set the home position. 
	Control rotation directions (by clicking triangle buttons) and stop patrol (by clicking the square button in the center).
	Zoom in/out.
	Focus far/near.
	Increase/decrease iris.
	PTZ rotation speed. **Note:** The rotation speed supports 9 levels from 1 to 9. 1 is the slowest and 9 is the fastest.
	Turn on/off the light.
	Turn on /off the wiper.
	Turn on/off the IR.
	Turn on/off the heater.

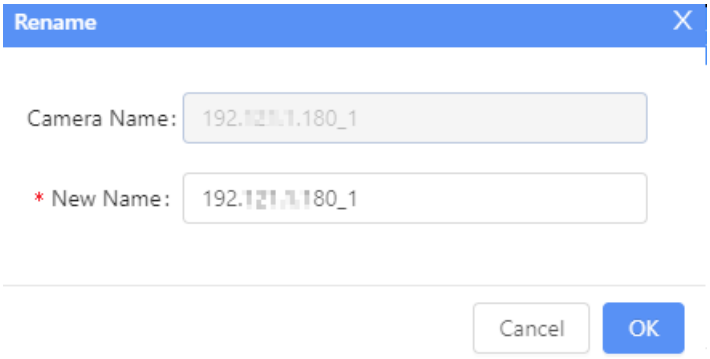
9.1.7 Live View Resource Management

View camera information, rename cameras, and view resource statistics.

Rename Camera

Right-click on the camera on the resource list and then choose **Edit Name** to rename the camera.

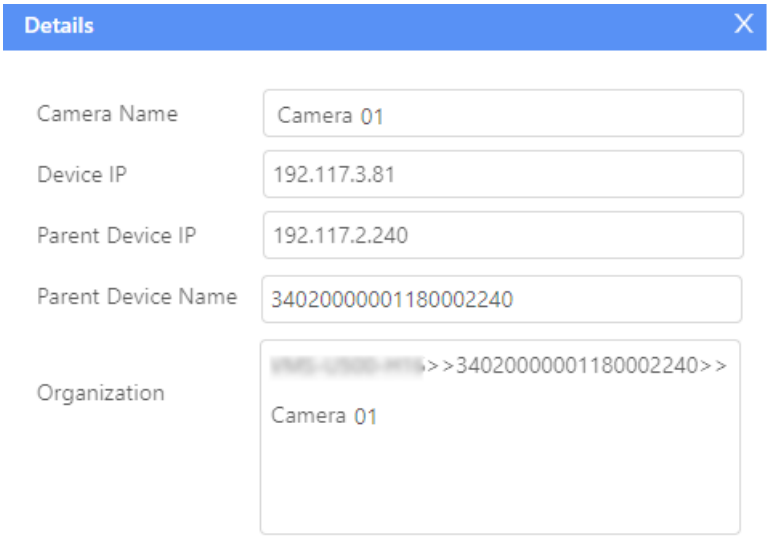
Figure 9-9: Change Name



View Camera Information

Right-click a camera on the resource list , and then choose **View Details** to view the camera name, device IP, parent device IP, parent device name,organization.

Figure 9-10: Detailed Camera Attributes

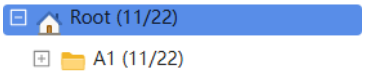


Resource Statistics

View the statistical information of camera/camera sequence/group display/group sequence resources.

Right-click on an organization, and then choose **Resource Statistics** to view camera statistics of the organization, including the number of online cameras, the total number of cameras in the organization. After resources have been changed, you need to perform this operation again to update the statistics.

Figure 9-11: Resource Statistics



9.1.8 Fisheye Dewarping

Supports correcting fisheye images based on the fisheye camera's mount mode and display mode.

A fisheye camera is an ultra-wide-angle lens with a viewing angle close to or equal to 180°. To achieve the maximum photographic angle of view, the front lens element has a very short diameter and protrudes forward, resembling a fish's eye, hence the name "fisheye camera". The images captured by a fisheye camera are distorted and can be restored to a normal view through dewarping.

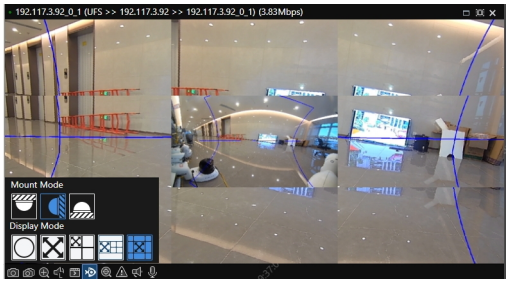
Note:
Fisheye cameras must be connected to the platform via the private protocol or the ONVIF protocol.

Enable Fisheye Dewarping

1. On the live view page, start the live video from the fisheye camera.
2. Click the window toolbar icon , then select the mount mode and display mode.

Mount Mode	Display Mode
Ceiling mount, desktop mount	Original Image, 2*180°Panoramic, 180°Panoramic+1PTZ, 180°Panoramic+6PTZ, Fisheye+3PTZ, Fisheye+4PTZ, Fisheye+8PTZ.
Wall mount	Original Image, Panoramic, Panoramic+3PTZ, Panoramic+4PTZ, Panoramic+8PTZ.

3. The dewarping effect is as follows (example: Wall Mount, Panoramic+8PTZ).

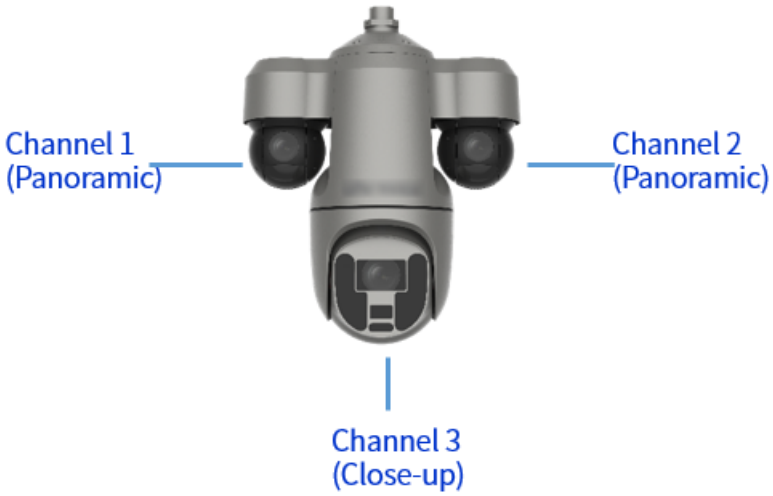


9.1.9 Picture-in-Picture

Starting Picture-in-Picture for a multi-channel camera allows the overlay display of the live video from the associated channel.

For example, camera model HIC98442: MultiView Network PTZ Dome Camera (Channel 1 and channel 2 are panoramic channels responsible for target detection; Channel 3 is a close-up channel responsible for target tracking).

Note:
Picture-in-Picture is only supported for multi-channel cameras connected via the private protocol in the local domain, and picture-in-picture linkage operations are supported only with the private protocol.

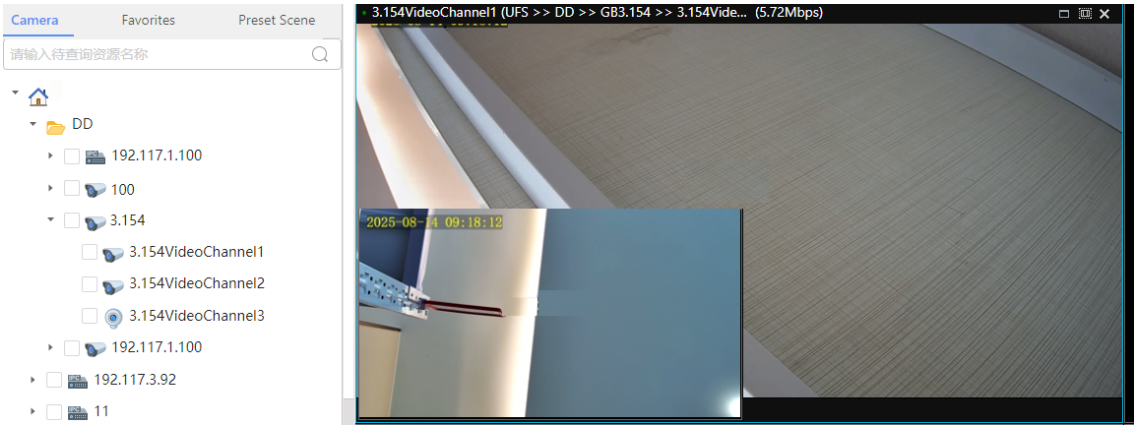


Start Picture-in-Picture

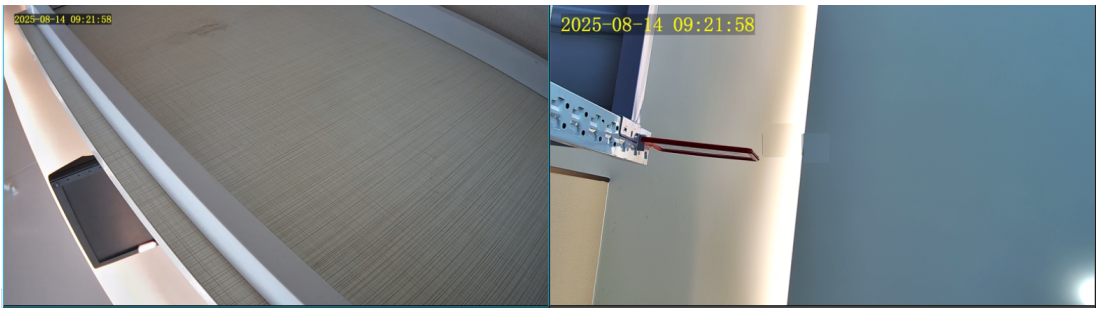
1. In the resource tree, select a channel of the multi-channel camera, right-click and choose **Start Picture-in-Picture**.

   Note:
   Picture-in-Picture can only be started for one camera channel at a time.

2. A small window will appear on the current channel's live video, displaying the associated channel's video.



- You can drag the small window to change its position on the large window; drag its four corners to change the window size.
- Right-click the live video and select **Small/Large Window Switch** to switch the live video between the large and small windows.
- Right-click the live video and select **Move Small Window to Next Window** to move the small window to the right window for independent live video display. (This action cannot be reverted to Picture-in-Picture).



Linkage Operations

Note:

- Linkage and calibration must first be performed on the camera's web interface.
- If Picture-in-Picture is not started, linkage operations are not supported when starting live view directly.
- Only box cameras support enabling click-to-link, drag-to-link, and manual tracking.

On the Picture-in-Picture enabled live video, you can right-click and then choose the following linkage actions:

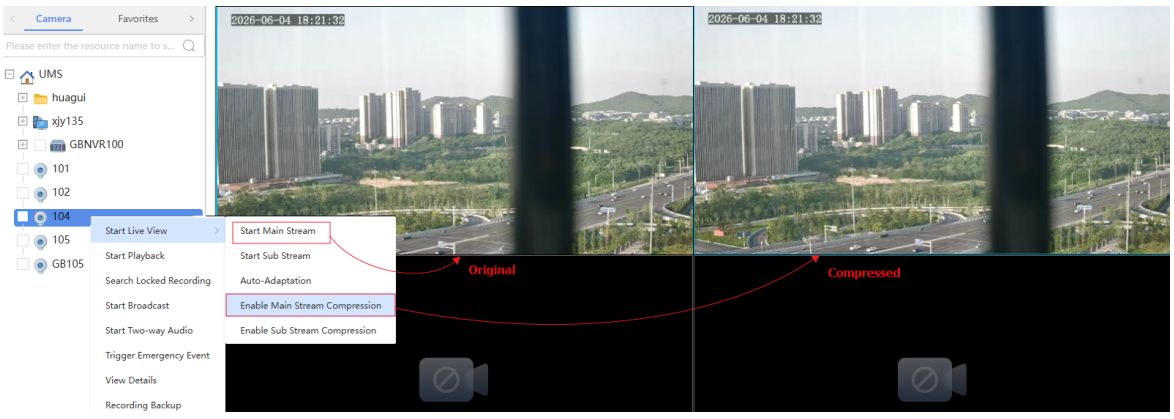
- Click-to-link: Click anywhere on the panoramic image, and the close-up image will rotate to the corresponding position on the panoramic image.
- Drag-to-link: Drag from the top-left to the bottom-right on the panoramic image, and the close-up image will zoom in on the selected area; drag from the bottom-right to the top-left on the panoramic image, and the close-up image will zoom out on the selected area.
- Manual Tracking: Manually select a target on the panoramic image, and the close-up image will track the target until the tracking time expires or the target moves beyond the detection range.

9.1.10 Live Video Compression

This feature supports playing live video on the client using the compressed stream.

Note:
Please add a video compression server and configure it first. Video Compression

In the camera list, right-click a camera, and select **Enable Main Stream Compression** or **Enable Sub Stream Compression**.



Depending on the compression parameter settings, the image quality may be slightly reduced after compression, but bandwidth usage is reduced and video smoothness is improved.

9.1.11 Favorites

Add resources such as cameras, camera sequences, group displays, sequences to favorites to find them easily.

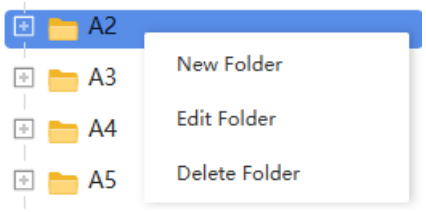
Create New Favorites Folder

Up to 3 levels of favorites folders (including the parent favorites folder) are allowed.

1. Right-click on the parent folder, select **New Folder**, enter the folder name, and then click **OK**.

2. When created, right-click on the parent folder, and then select **Refresh** to refresh the resource tree manually.

Figure 9-12: Create New Favorites Folder



Add Resources to Favorites

Right-click on the resource in the corresponding resource tree and select **Add to Favorites**.

Favorites Folder Operations

For resources added to favorites, you can perform the operations below. The following takes camera as an example.

Table 9-4: Favorites Folder Operations

Item	Description
Edit Name	Right-click on the folder, and then select **Edit Folder** to rename the folder.
Delete Folder	Right-click on the folder, and then select **Delete Folder** to delete the folder from the list.
Refresh Folder	Click to refresh the favorites folder.
Remove from Favorites	Right-click on the camera, and then select **Remove Favorites** to remove the camera from the favorites folder.
Batch Start Live View	Select cameras, right-click on any camera, and then select **Batch Start Live View** to play the live videos of the selected cameras simultaneously.
Synchronous Playback	Select cameras, right-click on any camera, and then select **Synchronous Playback** to play the recordings of the selected cameras simultaneously.
Auto Camera Sequence	Select cameras, right-click on any camera, select **Auto Camera Sequence**, and then configure parameters such as camera sequence interval and order, the live videos of the selected cameras will be played in single window in sequence.
Auto Group Sequence	Select cameras, right-click on any camera, select **Auto Group Sequence**, and then configure parameters such as group sequence interval and order, the live videos of the selected cameras will be played in all windows in sequence.

9.2 Playback

Go to **Video Application > Live View** or **Video Application > Playback**.

You can search recordings stored on the storage resources of the platform, camera's SD cards, and NVR disks, as well as backtrack historical events with anomalies.

Workflow

1. Add cameras. See Device Management > Private Device and ONVIF Camera.
2. Configure storage resources for cameras. See Video Storage Configuration. You can also configure storage on cameras or NVRs.
3. Search recordings for playback. See Search Recordings.

9.2.1 Search Recordings

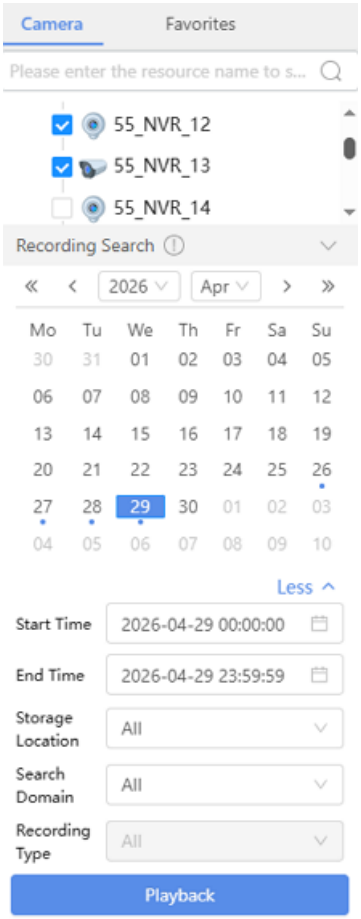
You can search recordings stored on storage resources for playback.

Note:
Prerequisite: You need to configure storage resources for cameras. See Recording Storage.

Multiple methods are available for searching camera recordings.

- On the **Playback** page: Select the desired video channels in the resource tree, set the search conditions, and then click **Playback**.

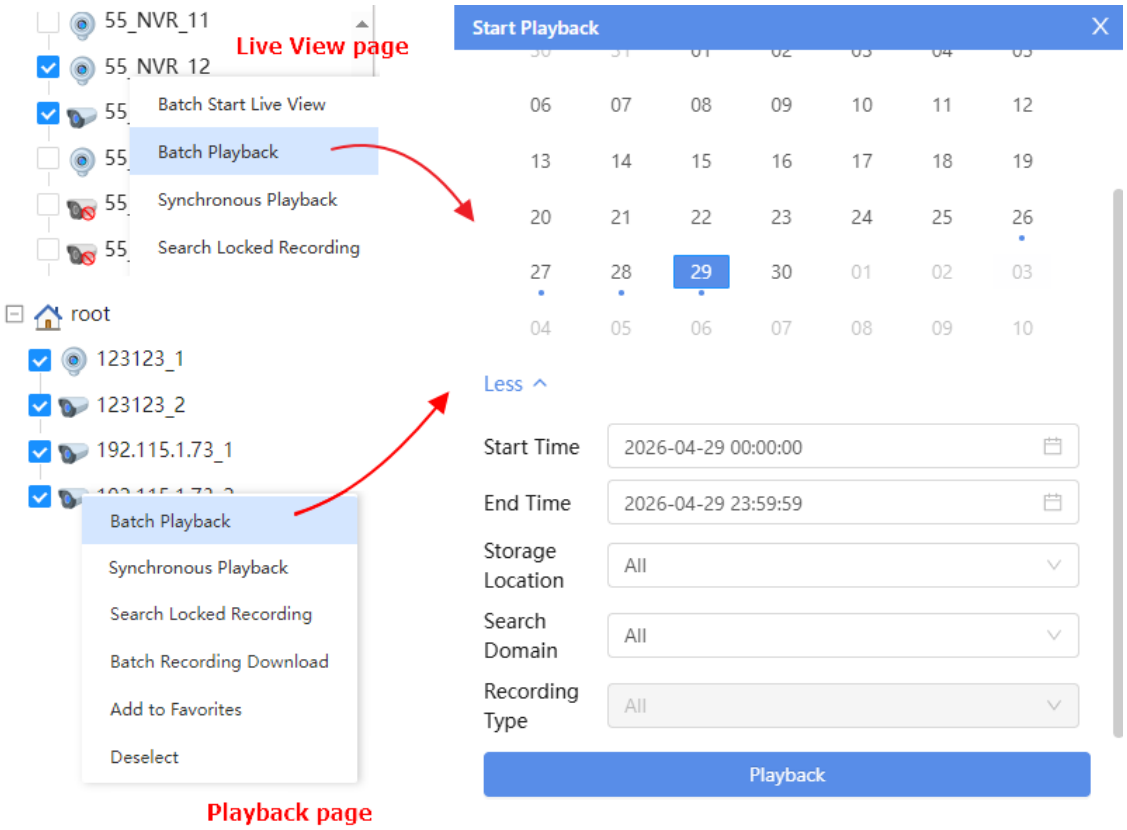
  Note:
  A maximum of 16 video channels can be selected for batch playback.



- On the **Playback** or **Live View** page:

  1. Right-click to open the search condition configuration window.
     - Single playback: Right-click a video channel and select **Start Playback**.
     - Batch playback: Select multiple video channels, right-click and select **Batch Playback**; or right-click an organization and select **Batch Playback**. Also supports right-clicking to select **Synchronous Playback**.

       Note:
       - If the organization contains more than 16 channels, only the first 16 channels will be played back.
       - After enabling **Synchronous Playback**, the selected channels will start playback from the same time point. The palyback across all channels remain synchronized when dragging the progress bar or adjusting the playback speed.
  2. Set the search conditions and click **Playback**.



Recording search condition description:

Item		Description
Recording Calendar		Select a date for searching recordings in the calendar panel, recordings for the entire day will be queried. **Note:** • Dates with recordings are marked with a blue dot at the bottom. • When searching multiple cameras simultaneously, if any camera has a recording on a given day, that day will be indicated as having recordings. • By default, the platform only displays the calendar for recordings from central recordings, backup recordings, and recordings from private front-end devices in the local domain. To view the recording calendar for Onvif/ VSS connected devices, please purchase and configure recording diagnosis. • The recording calendar is for reference only, as it is influenced by the statistical scope and time. Manually deleted recordings will not automatically update the calendar.
Start Time/End Time		Select the start and end time for the recording, with a maximum range of 31 days.
Storage Location	Device Recording	Recordings saved on storage resources of IPC/NVR.
	Central Recording	Recordings saved on central storage resources of the platform, for example, IPSAN, CDS.
	All	Search all recordings, including edge recording and central recording.

Item		Description
Search Domain	Device Registration Domain	Search recordings saved on the storage resources of the platform where the camera is registered.
	Local Domain	Search recordings saved on the storage resources in the local domain.
	Child Domain	Search for recordings in storage resources of the lower platform.
	All	Search recordings across all storage resources.
Recording Type **Note:** Only when searching recordings from the **local domain's central storage** can you configure the recording type.	Alarm Recording	Alarm-triggered recordings.
	Manual Recording	Recordings that are saved manually.
	All	Search all types of recordings.

The recording playback page is as shown below:

Figure 9-13: Start Playback on the Live View Page

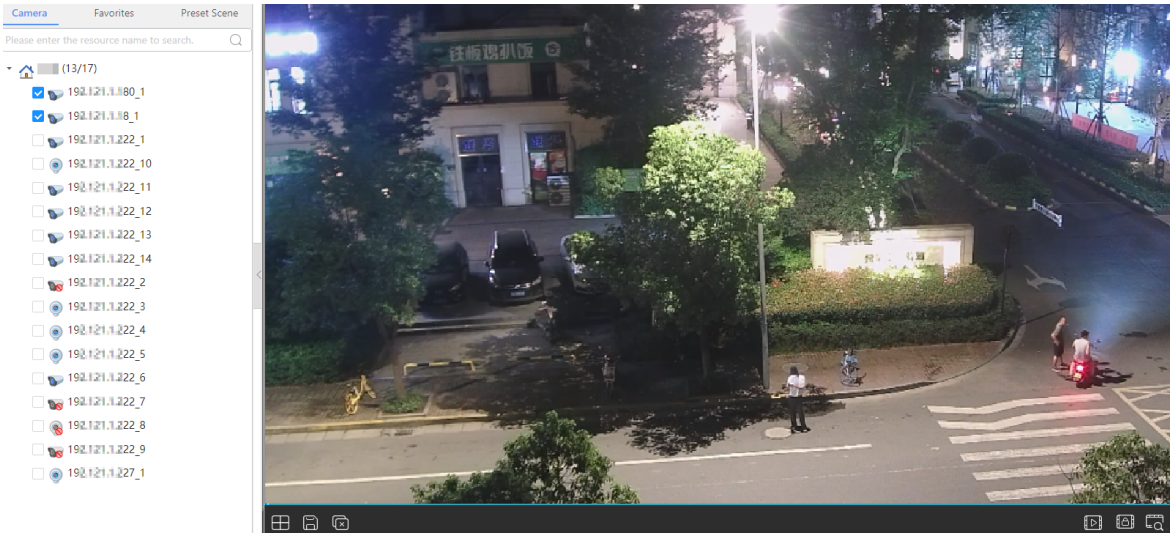
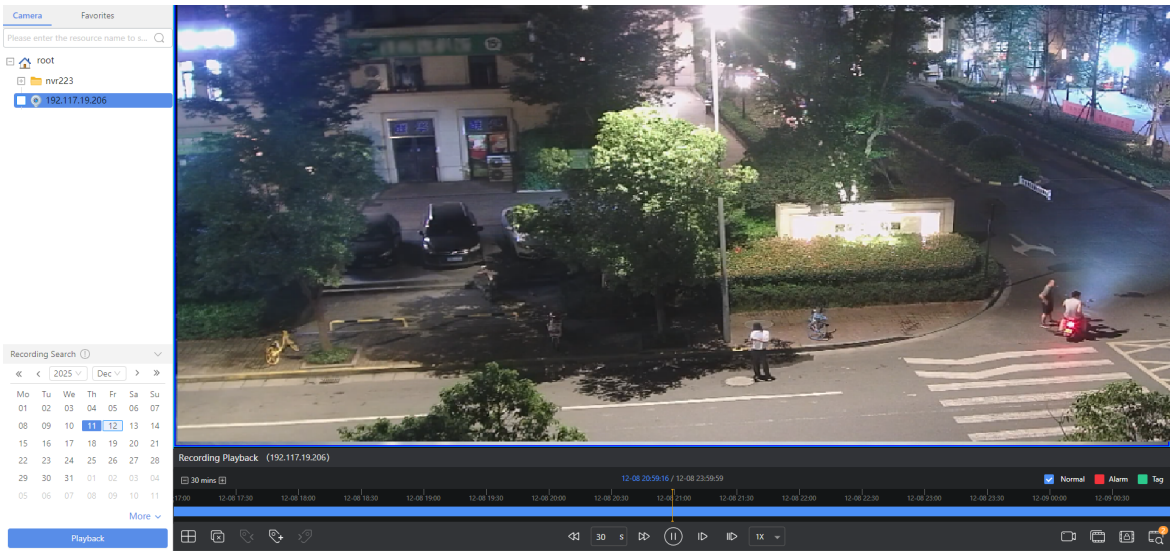


Figure 9-14: Start Playback on the Playback Page



9.2.2 Playback Operations

During video playback, you can perform related operations using the window toolbar, playback toolbar, and playback progress bar.

Figure 9-15: Playback Window on the Playback Page

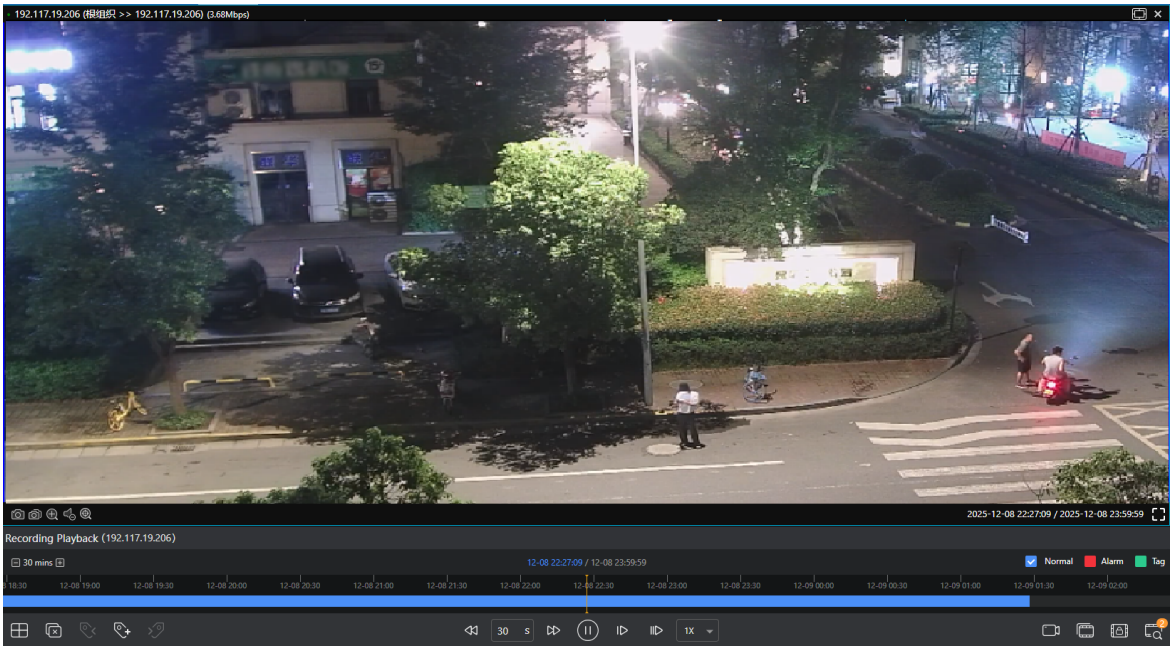
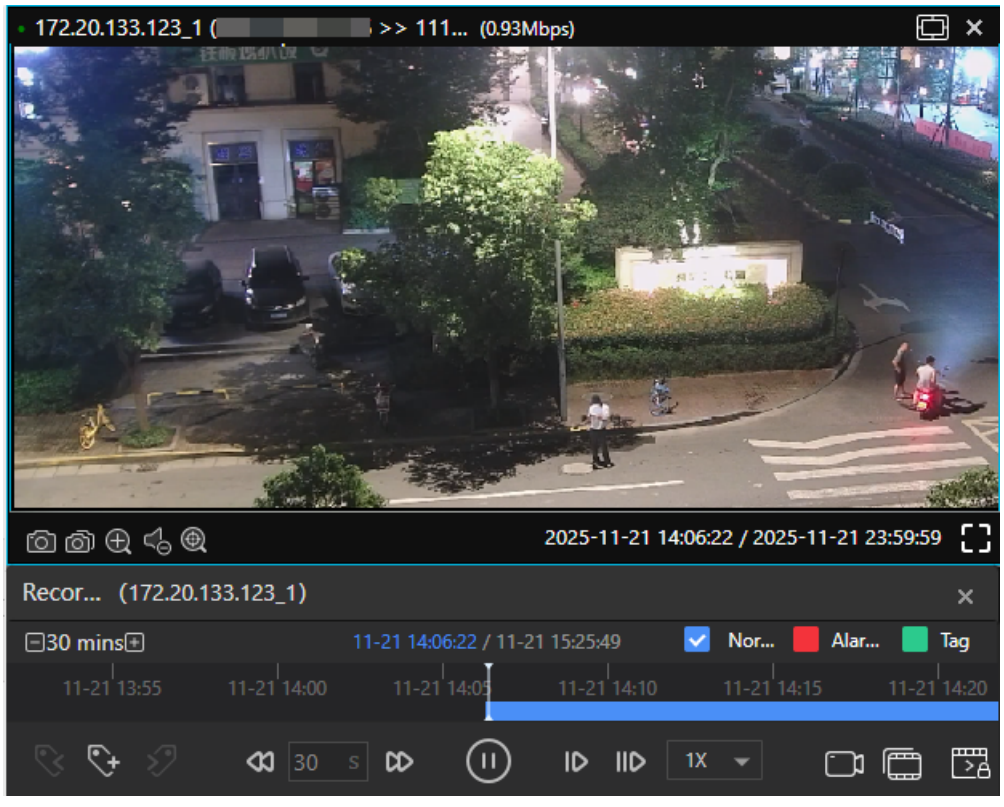
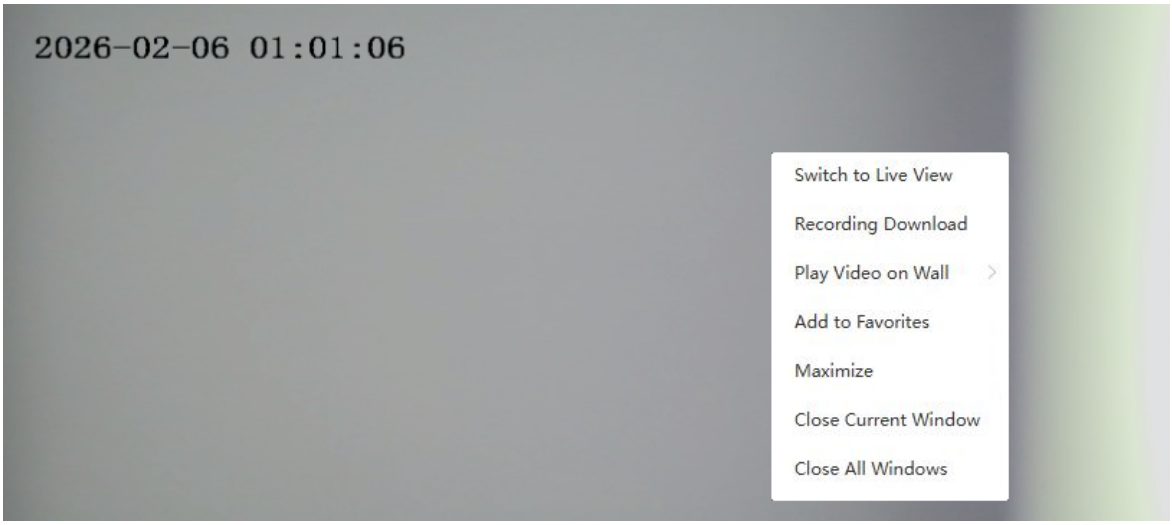


Figure 9-16: Playback Window on the Live View Page



Playback Right-Click Menu Operations

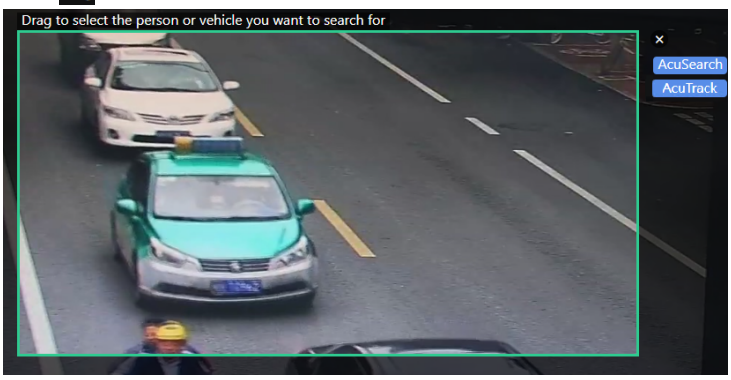
You can right-click on a live view window and then use the pop-up menu to switch to live view, recording download, play video on wall, add to favorites, maximize, close current window, or close all windows.



Window Toolbar

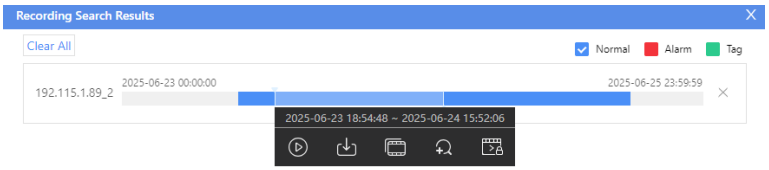
The toolbar appears when you hover the mouse over a windows.

Table 9-5: Window Toolbar Operations

Icon	Function	Description
	Snapshot	Capture the current image(s) in the window and save to local.
	Continuous Snapshots	
	Digital Zoom	Zoom in on an area of interest on the image in the window. Use the scroll wheel to zoom in or out, and click again to stop digital zoom.
	Volume control	Click to use the slider to adjust the volume of the video.
	AcuSearch/ AcuTrack	When a target of interest is identified in the recording, you can select the motor vehicle/non-motor vehicle/pedestrian target in the current image to search the full video and image data for scenes where the target appeared. 1. Click to freeze the current frame.  2. Select the target to search for: • Hold down the mouse and drag the area within the green box to move its position. • Hover the mouse over the edges or corners of the green box, when the cursor changes to an arrow, hold and drag to resize the green box. • To exit the search, click X. 3. Choose a search mode. Two modes are available: • Click the **AcuSearch** button at the top right corner of the green box to go to the SeekFree page, where the system will automatically

Icon	Function	Description
		search for all capture records of the target within the green box (see Search by Image). • Click the **AcuTrack** button at the top right corner of the green box to go to the AcuTrack page, where you can search for recordings containing the target in the green box.

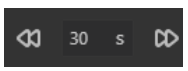
Bottom Toolbar

Icon	Function	Description
	Switch Window Layout	Change the window layout. You can customize the number of windows, or choose 1/4/6/8/9/10/13/16/17/25/36/64 windows or corridor mode (intended for narrow scenes such as a corridor) as needed.
	Close all videos	Close the video in all current windows.
	Play local recording	Select a video file from the computer to play. **Note:** This feature is available only on the **Live View** page.
	Search locked recordings	Search for locked recordings, and unlock them if necessary. **Note:** For descriptions about how to lock recordings, see Table 9-6: Playback Toolbar Operations.
	Recording search results	View the successful recording search results during the current login session.  You can select a video clip and then perform the following operations: play, download, backup, zoom in on the timeline, lock(only for admin).

Playback Toolbar

Click the window to display the playback toolbar.

Table 9-6: Playback Toolbar Operations

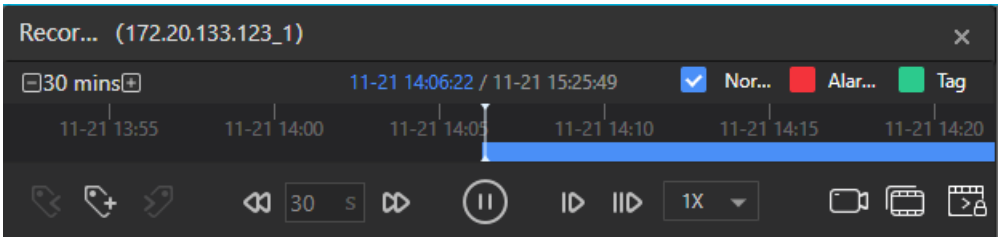
Icon	Function	Description
	Play/Pause	Play/pause the video.
	Forward/Rewind	Play the previous/next segment at the set interval (1-999s, default is 30s)
	Next Frame	Play next frame.
	Forward Frame by Frame	Play one frame of image per second. Local recording does not support this function.
	Adjust Speed	Choose a desired playback speed: ½x, 1x, 2x, 4x, 8x, 16x.
	Start screen recording	Click to record the currently playing recordings. Click again to finish. The recorded file will be saved to the browser's designated download directory.
	Back up Recording	Create a recording backup task to back up recordings within a specified time period.

Icon	Function	Description
	Lock Recording	When locked, other users cannot perform any operations to recordings. **Note:** Only recordings from the local domain's central storage support this feature.
	Add Tag	See Tag.

Playback Progress Bar

The playback progress bar shows the playback progress of recordings in the selected window.

Figure 9-17: Progress Bar



- Drag to adjust the playback progress, or double-click to skip to the time point, or click the current time (blue text) to select a specific time point and skit to it.
- Use 30 mins to adjust the time scale on the progress bar.

Alarm Recording

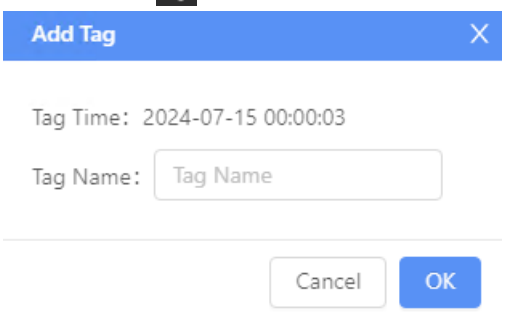
If you have configured recording storage function in Alarm Linkage, you can view recordings of alarm moments here.

Select **Alarm**. The alarm linkages will be marked in red on the progress bar. Double-click on a red marker to locate the recording.

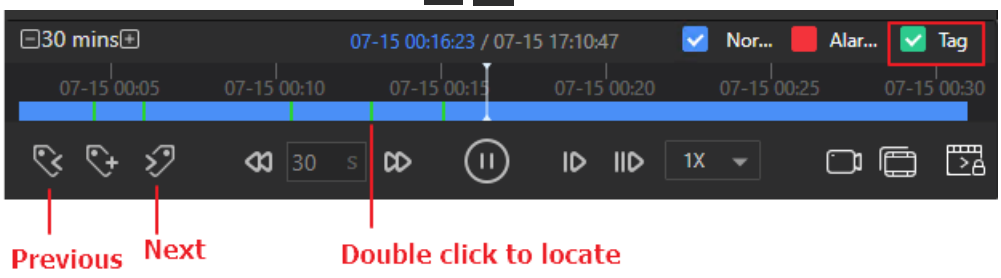
Tag

You can tag recordings of significant moments, allowing for quick retrieval of recordings using these tags later on.

- Add tag: Click . Enter a tag name for this recording time period.



- View tag: Select **Tag**. The added tags will be marked in green on the progress bar. Double-click a green tag to locate the recording. You can also click / to switch to the previous/next tag.

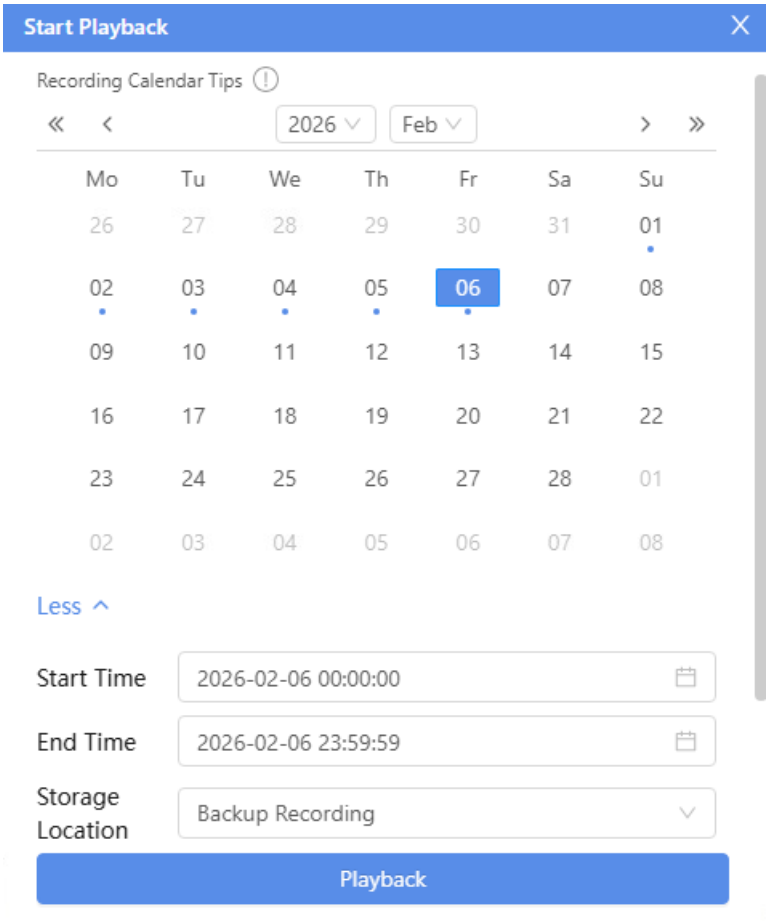


9.2.3 Search Backup Recordings

Search for recordings stored in backup resources.

Note:
Prerequisite: You need to configure backup tasks for cameras. See Recording Backup.

1. Right-click on the camera in the camera list and then choose **Start Playback**.
2. Select the search time range and the storage location as **Backup Recording**.



3. Click **Playback** to search the backup recording for the specified time period and play it in the designated window.

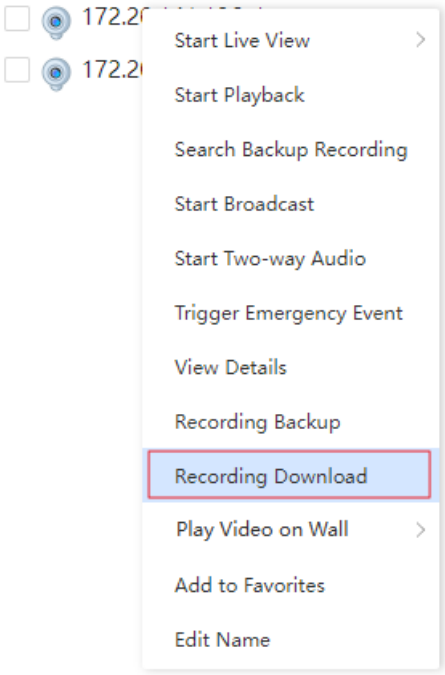
9.2.4 Recording Download

Download recordings to local.

Note:
Supported recording download formats: ts, mp4. To set the format, go to **Media Config** > Recording.

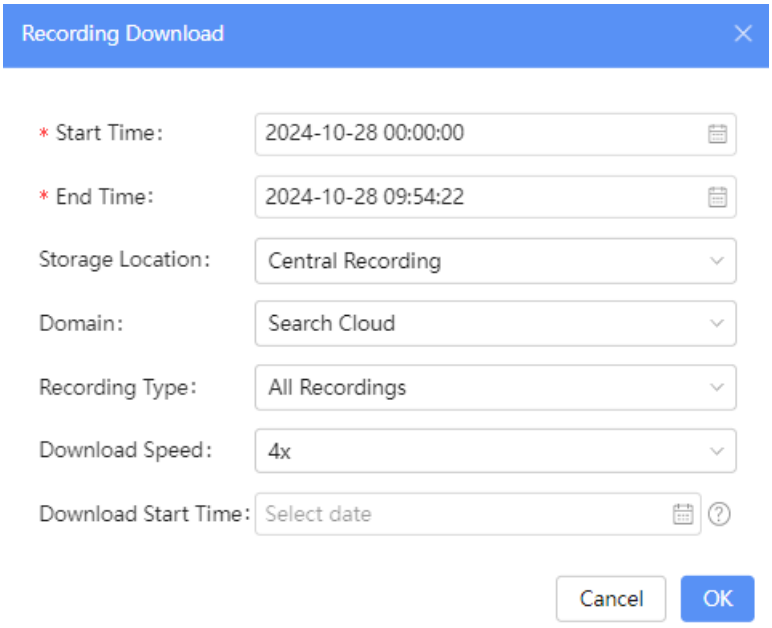
Recording Download

1. Right-click the camera on the camera list and then select **Recording Download**.



2. Specify a recording time period for downloading in the pop-up window, and set other parameters as needed.

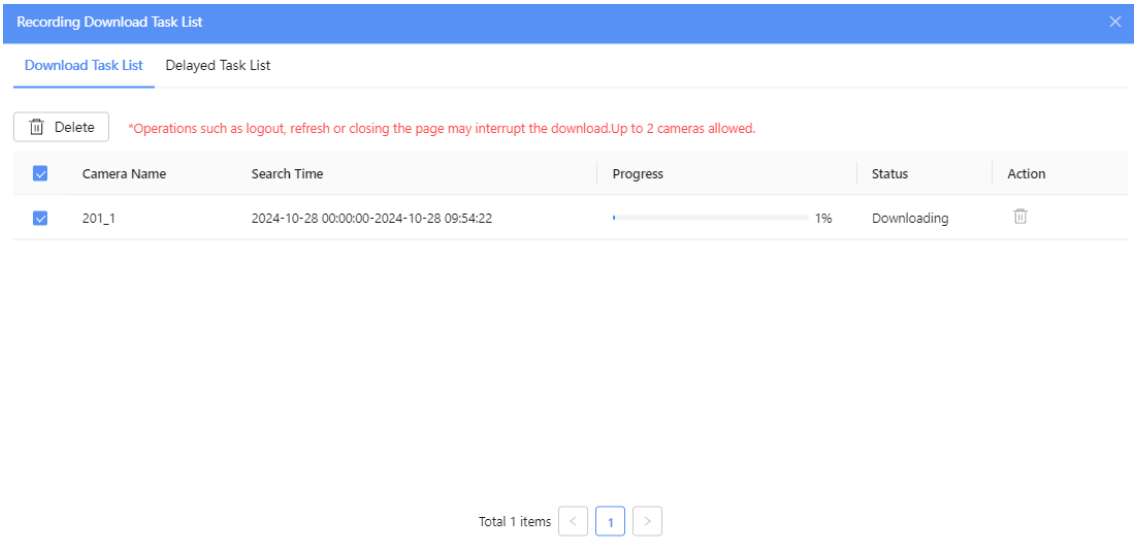
Figure 9-18: Recording Download



Note:
To schedule downloads during idle periods, you can set a start time for the download. The system will begin downloading at the specified time. Ensure the client is logged in at the set start time.

3. Click **OK**. For non-delayed tasks, the task starts immediately.
4. Click in the upper-right corner to enter the **Recording Download Task List** page.
   - Download task list: You can view details of ongoing recording download tasks such as the progress and status. Up to 2 tasks are allowed simultaneously. You can also click to delete the task.
   - Delayed task list: You can view details of the delayed recording download tasks such as the download start time. You can also click to delete the task.

Figure 9-19: Recording Download Task List



9.3 Video Wall

Go to **Video Application** > **Video Wall**.

You can create video wall layout on the client and bind video output channels of decoders to play video images on a physical video wall.

- DC video wall: The video wall can only be bound to output channels of one decoder or video wall controller. Playing live videos/recordings, local input, camera sequence, scene resources, and overlaying virtual LED are supported.
- Multi-DC video wall: The video wall can be bound to output channels of more than one decoder or video wall controller. Playing live videos/recordings and camera sequence are supported.

Workflow

1. Add decoders and video wall controllers. See Device Management > Decoder & Video Wall Controller.
2. Add videos and play videos on wall. See DX Video Wall and Multi-DC Video Wall.

9.3.1 DX Video Wall

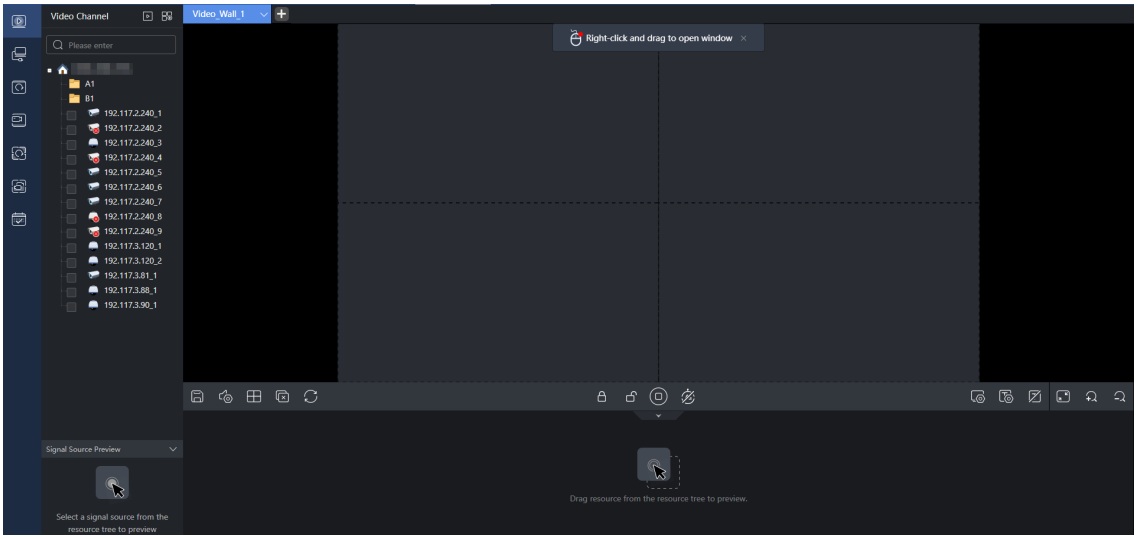
Add a DX video wall and configure and manage videos played on it. A DX video wall can only be bound to the output channels of the same video wall controller.

Note:
You need to first add video wall controllers in **Device Management > Terminal Device > Device Decode**.

9.3.1.1 Add Video Wall

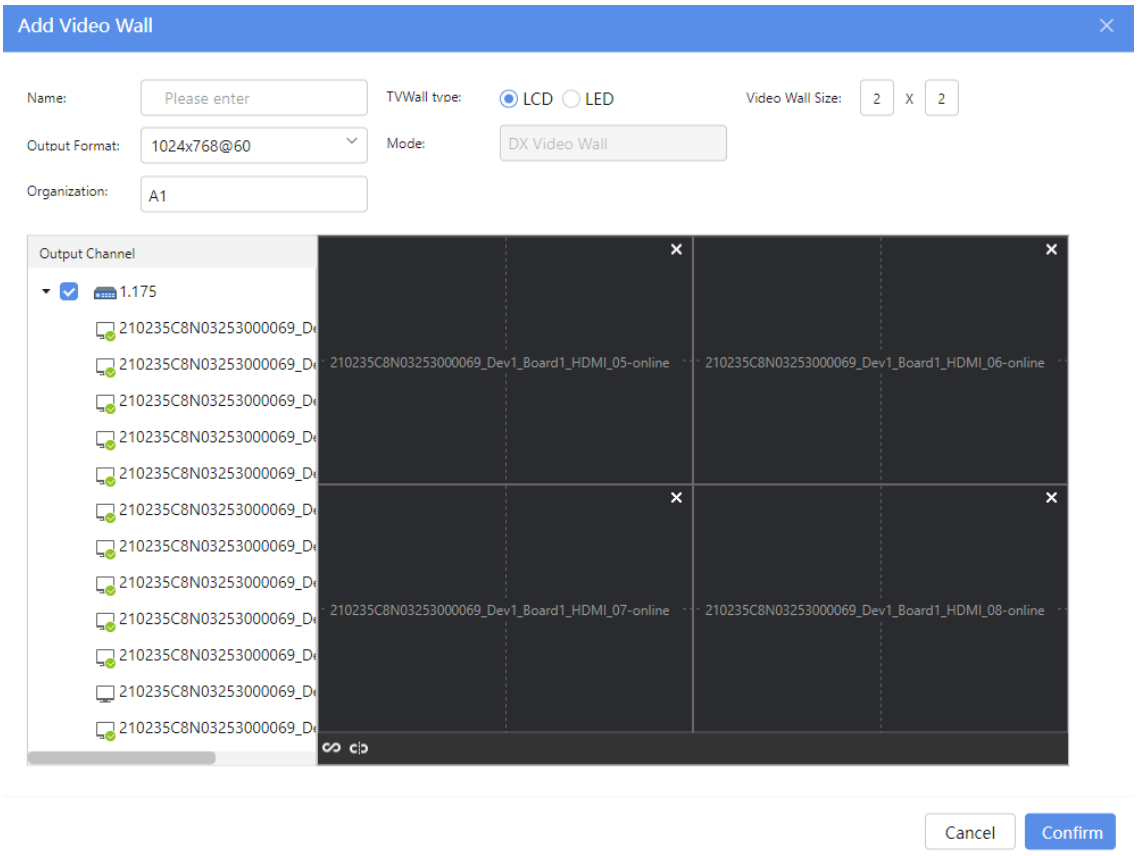
1. If no video wall has been created in the system, click Add Video Wall in the center of the initial page to add one.
   If a video wall has already been created, you can add a new one by clicking + on the top of the right-side pane.
   Select the DX Video Wall type.

Figure 9-20: Video Wall Page

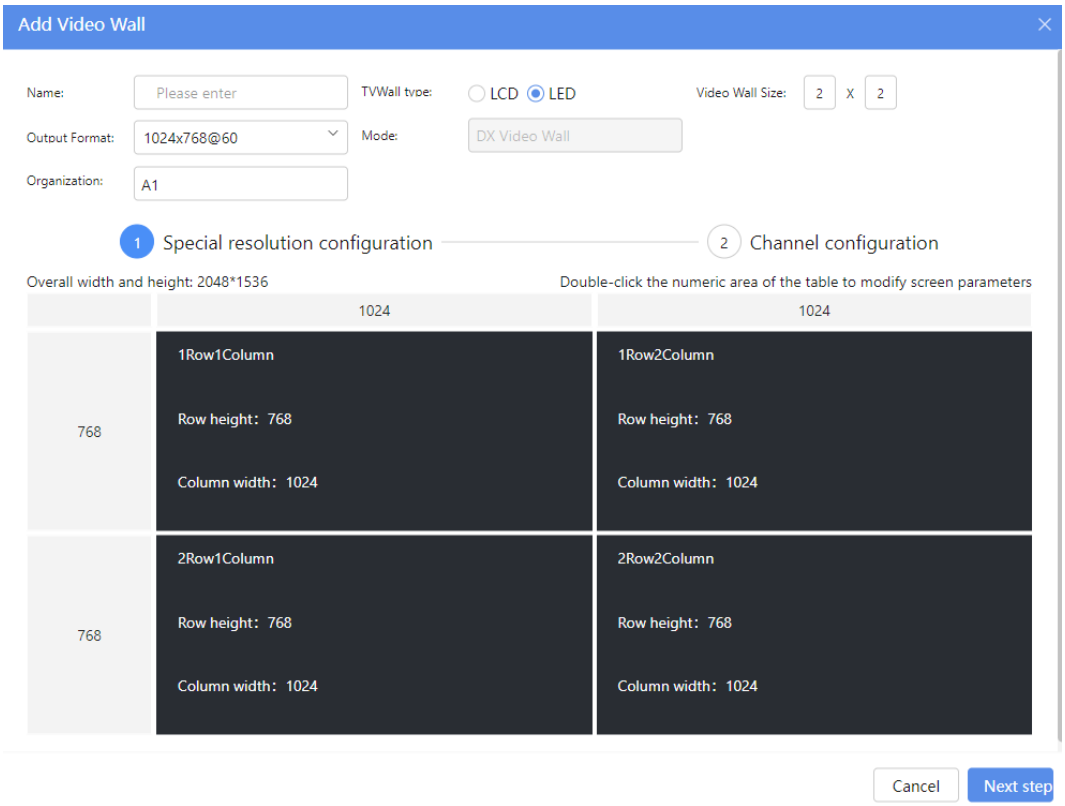


2. Set the video wall information in the pop-up **Add Video Wall** window.

Figure 9-21: Add Video Wall



- Name: Enter a custom name for the video wall.
- TVWall type: Video wall type. Choose LCD or LED.
  - LCD video wall: Suitable for LCD-type splicing display units. Only requires output channel configuration.
  - LED video wall: Suitable for LED-type display units. If the screen sizes differ, you can set the screen's row height and column width under **Special resolution configuration**, then configure the output channel.



Note:

- If special configuration of the LED screen's width and height is required, the number of LED rows and columns must be configured according to the actual splicing method when setting **Video Wall Size**.
- The unit of measurement for video wall width and height is pixels
- Double-click the numeric area to modify screen parameters.

- Video Wall Size: Number of windows on the video wall. After setting the video wall size, the panel below will display the layout.
- Organization: Select an organization for the video wall. The organization cannot be modified after the video wall is saved.
- Output Format: First select a video wall controller from the output channel list, and then select the output format (the maximum resolution supported by the video wall).

3. Drag the idle channels from the left-side list to the video wall windows one by one.

Note:
Bind/unbind all channels with one-click: Select the video wall controller on the output channel list, and then click in the lower-left corner of the video wall. The idle channels of the video wall controller will be bound automatically to the video wall windows (if some windows on the video wall are already bound, the current bindings will be cleared first). Click to delete all bindings.

4. Click **OK**. The video wall is created.

Note:
After adding a video wall, you can click the arrow right to the video wall name to edit, close, or delete the video wall.

9.3.1.2 Canvas Operations

Canvas refers to the background displaying the video wall windows.

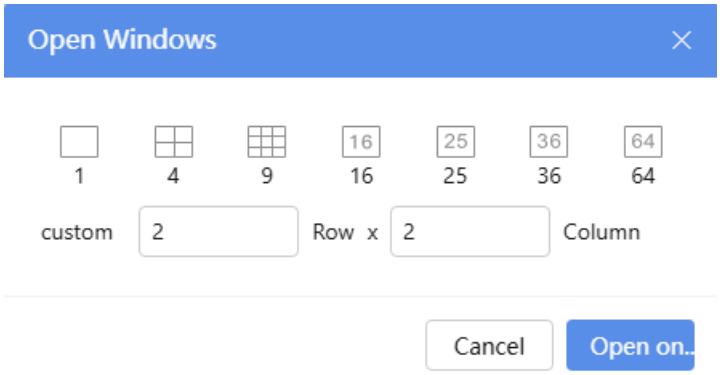
- Drag the outer area of the video wall to move the canvas.
- Scroll the mouse wheel to zoom in/out on the canvas.
- Click in the bottom toolbar to restore the view.

9.3.1.3 Window Operations

- **Open window**: Drag a camera or sequence resource from the left-side tree to the video wall to open a window; or drag with the right button pressed on the video wall to open a window; or click on the toolbar and then set a number to open multiple windows.
- **Close window**: Click in a window's top-right corner to close the window; or click on the toolbar to close all windows.
- You can drag a window to move it, and drag the window border to resize the window.

  Note:
  Window dragging is only available to certain video wall controllers.
- **Auto-snap**: When creating or moving a window, if the distance between its edge and the nearest grid line is less than 1/20 of the grid width (or height), the window will automatically snap to that grid line.

Video Wall Toolbar Operations

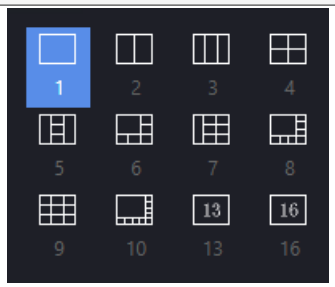
Icon	Description
	Save the current video wall layout and video services as a scene. • Save Scene: In the **Scene** resource list, select a scene and click **Save Scene** to save the current video wall services to that scene, overwriting the original scene. • Save As: Click **Save As**, enter a new scene name, and click **OK** to save the current video wall services as a new scene.
	Audio control, select audio output, and set audio volume to play audio on that channel.
	Set the number of rows and columns to open windows with one click.  • Open on Wall: Open windows on the entire video wall. • Open in Window: Open windows on a selected window (this button appears after you select a window). **Note:** The number of windows that can be opened is limited by the video wall controller's capability, usually with a maximum of 36 windows per output channel.
	Close all windows.
	Refresh the page and restore the default view.
	Lock/unlock all windows. The position and shape of the locked windows cannot be changed.
	Stops decoding in all windows.

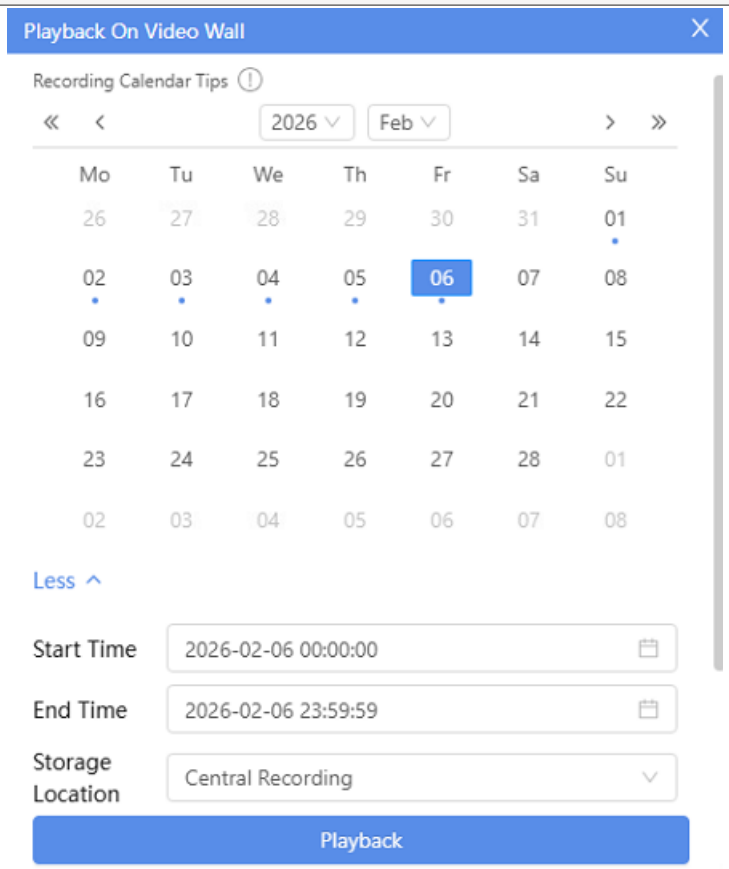
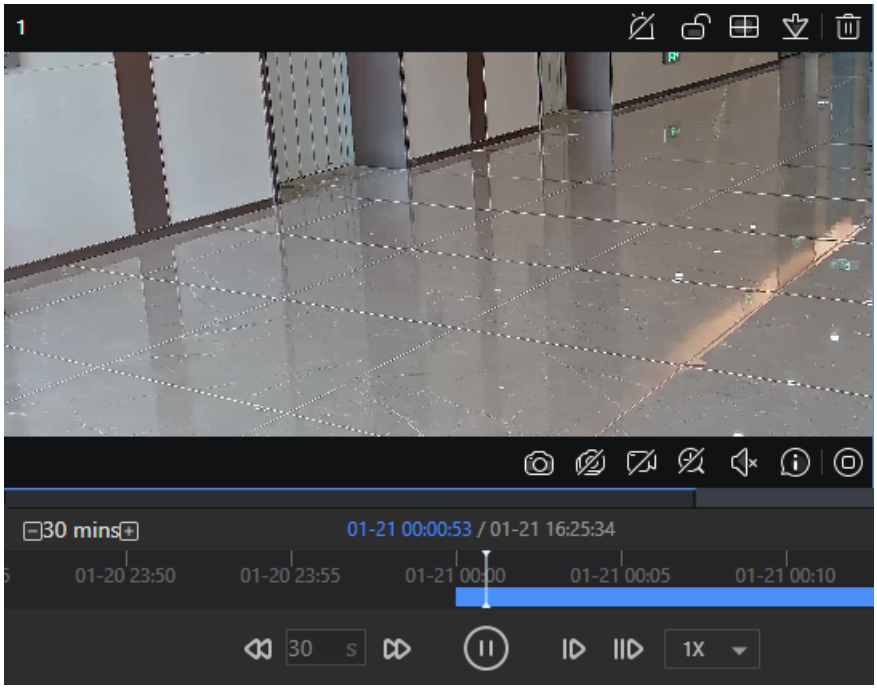
Icon	Description
	Note: When decoding stops, the video channels that are playing videos will display the last frame of image. You can set it to display a black screen by configuring on the video wall controller's web interface (Play Configuration > Advanced Configuration).
	Enable or disable intelligent mark. When enabled, intelligent analysis tripwires/area, object detection boxes, and object attributes will be displayed on the video images on the physical large screen. **Note:** The camera side needs to enable intelligent functions,such as perimeter defense, mixed traffic detection, face recognition, and vehicle recognition.
	Screen control. See Screen Control.
	Virtual LED configuration. See Configure Virtual LED .
	Show/hide virtual LED.
	Restore view: Reset the video wall view to its initial position.
	Zoom in/out on the view. You can also use the mouse wheel to zoom in/out.

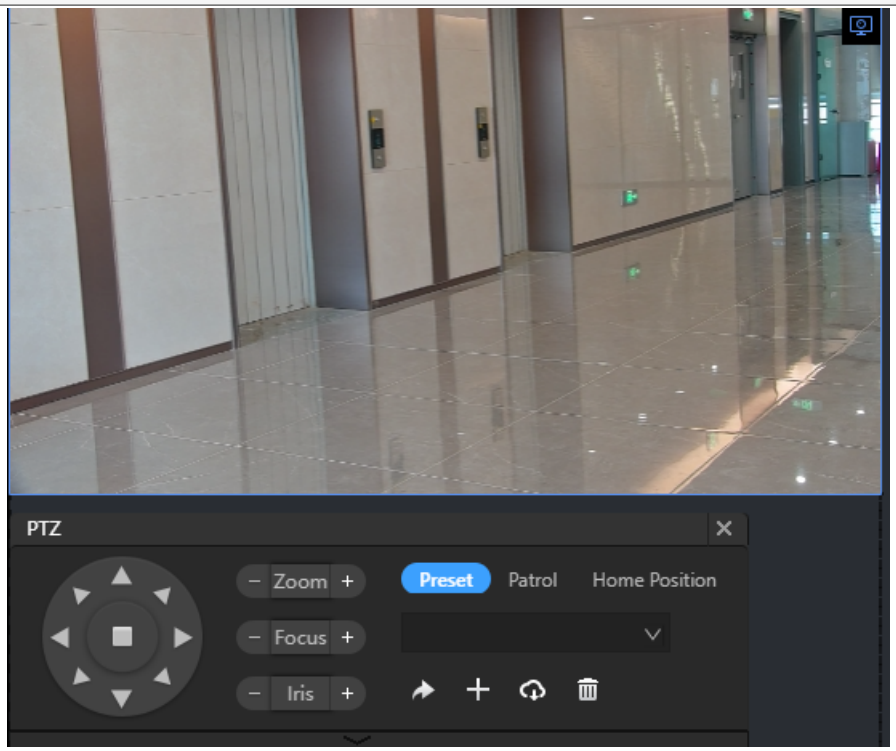
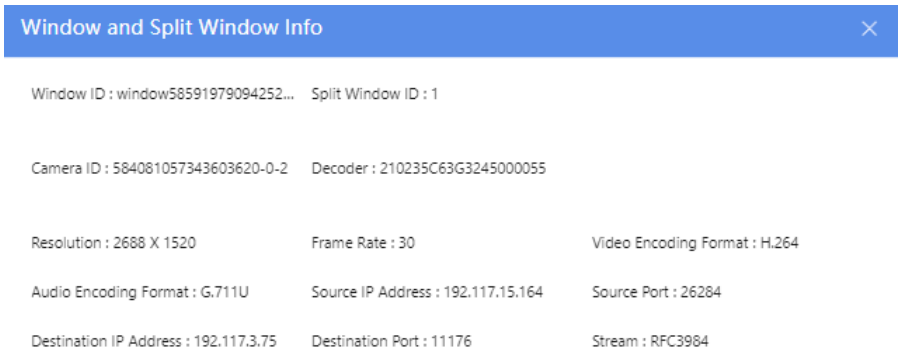
Window Toolbar Operations

The window toolbar appears when the mouse moves into the window.

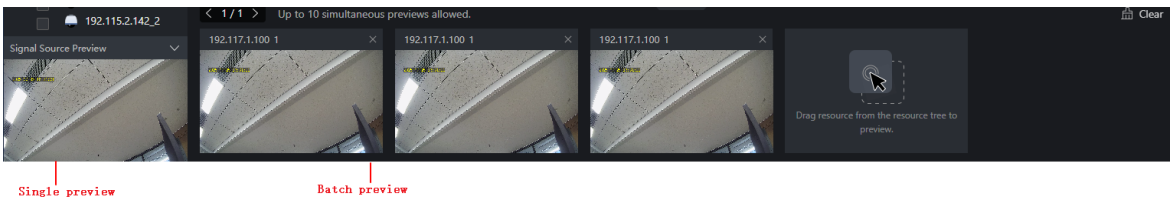
Icon	Description
1	Window ID (located at the top-left corner of the window). After adding or deleting a window, or after changing the position of a window, all windows will be automatically renumbered based on their latest positions, following a top-to-bottom, left-to-right order.
	Enable/disable alarm linkage. When enabled, the window will play the live video from the linked camera when an alarm is triggered. **Note:** You must go to Alarm Linkage Configuration and configure alarm-triggered live video to the video wall first.
	Lock/unlock the window. The position and shape of the locked windows cannot be changed.
	Split the window.

Icon	Description
	
	Display the window at the bottom of multiple overlapping windows.
	Delete the window.
	Preview the live video in the window. Click again to stop the preview. The following operations are allowed during preview: snapshot, continuous snapshots, local recording, and digital zoom. **Note:** Only one window can be previewed at a time.
/	Enable/disable PTZ shortcut operations: • Enabled: Clicking on the live view window allows you to control PTZ movement, enabling quick operations. • Disabled: Clicking on the live view window will not trigger PTZ movement, preventing accidental operations.
	Turn on/off audio in the window.
	Switch to playback on video wall, set search criteria, and preview the retrieved recordings in the window.

Icon	Description
	 Click the playback preview window, expand the toolbar, and then you can stop playback, adjust playback speed, etc. 
	Expand the PTZ control panel to control the rotation of the PTZ camera.

Icon	Description
	
	View window and channel resource information in the window. 
	Stop decoding in the window.

9.3.1.4 Resource Preview

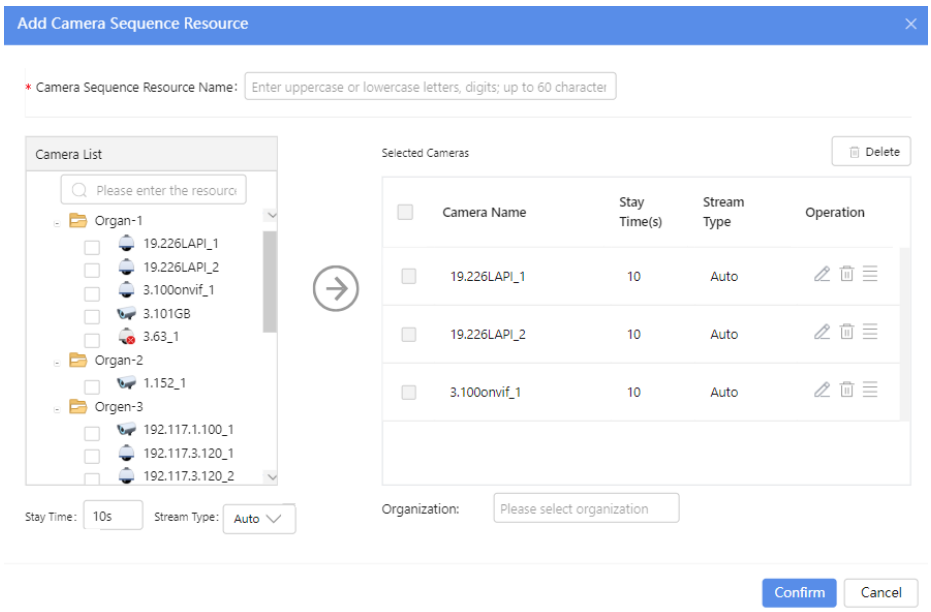


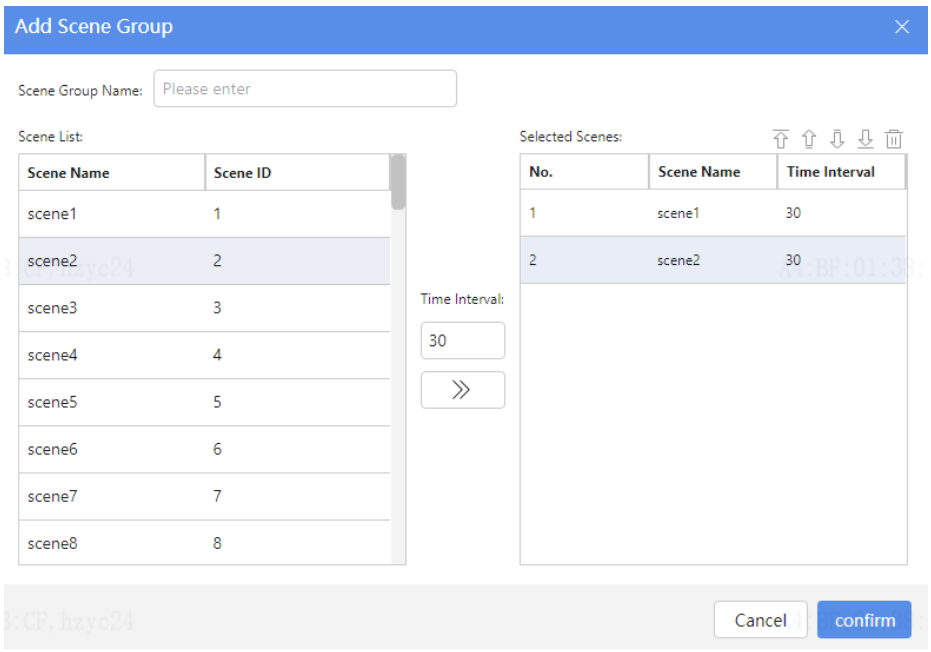
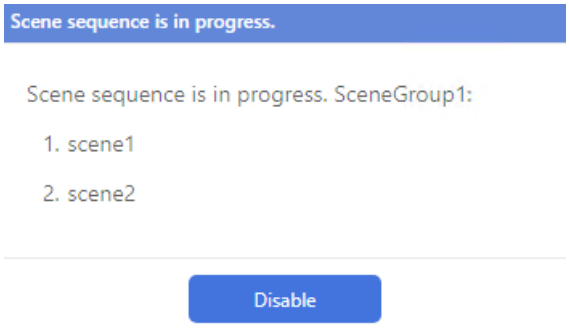
- **Single preview**: Click a video channel in the left resource tree to preview it.
- **Batch preview**: Drag video channels/local input channels from the left resource tree to the bottom of the page for preview (supports up to 10 resources for simultaneous preview).
  - Double-click the title bar to maximize the window.
  - Drag the title bar to play the live video on the video wall.
  - When multiple previews exist, click < 1/2 > to page through.
  - Click Clear to clear all preview resources.

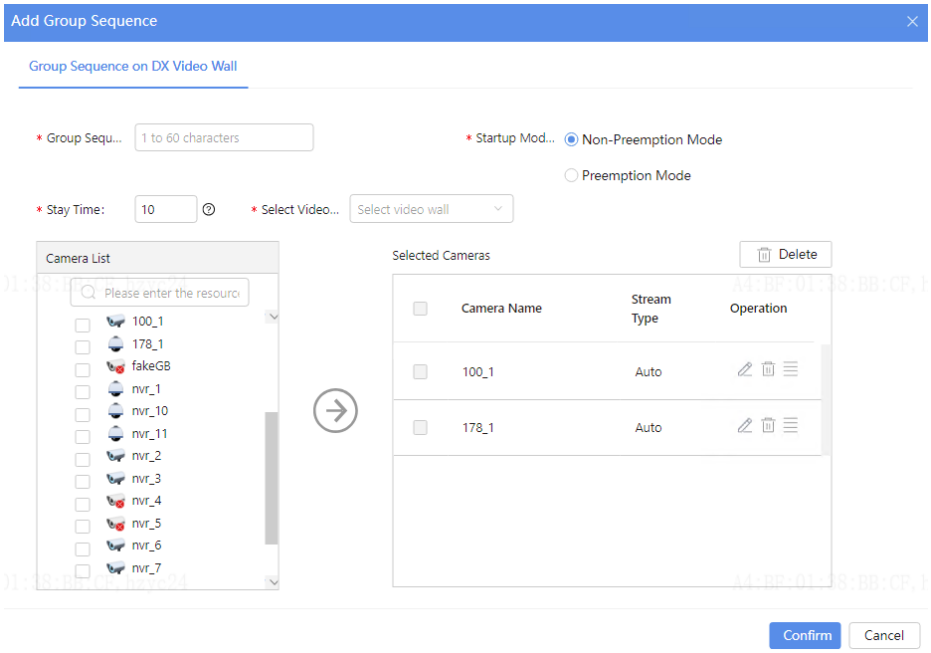
9.3.1.5 Play Video Resources on Video Wall

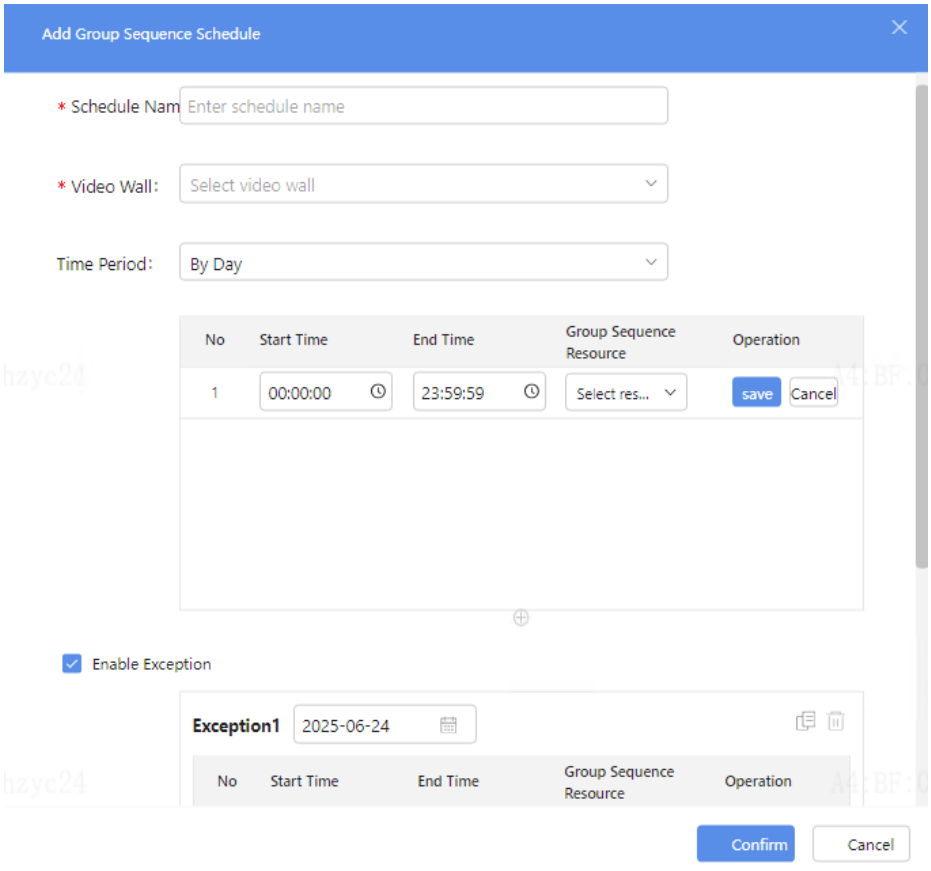
Click the icon on the left-side menu bar to view the corresponding resources.

Table 9-7: Play Different Video Resources on Video Wall

Resource	Operation
Video channel	• Play live video on video wall: Drag a camera to a video wall window; or click a window, right-click the camera, choose **Live View on Video Wall** > **Main Stream/Sub Stream/Auto** to start live video in the window. • Playback on video wall: To play recordings of a camera in a video wall window, click the window, right-click the camera and then choose **Playback on Video Wall**. In the pop-up window, set search parameters including playback time and search domain, and then click **OK**. • To play video in a window: Click the window, select a camera, click , and then choose a stream type to play video in the selected window. • Batch play on video wall: Click a window, select multiple cameras, click , and then choose a stream type to play video in the selected window and its subsequent windows.
Local Input	Drag a local input channel to a window; or click a window, right-click the local input channel, and then choose **Start** to play the local input resource on the video wall.
Camera Sequence	Play the live video of multiple cameras in one window in sequence. • Add a camera sequence: Click + above the camera sequence list and add multiple cameras to the camera sequence group. **Note:** • Stay Time: Set the duration of the live video for each camera. • Stream Type: Choose from Adaptive (determined by **Auto-Switch to Sub Stream** setting in Media Configuration), Main Stream, Sub Stream, and Third Stream. • Display Order: Drag for a camera to adjust its order in the sequence group.  • Start camera sequence: Drag a camera sequence resource to a window to start camera sequence in the window. • Pause/resume camera sequence: Click the window, and then click on the toolbar to pause the camera sequence (but will continue to play the current live video); click to resume the camera sequence and switch to the next camera at the set interval.

Resource	Operation
	• Play previous/next: Click the window, and then click on the toolbar to switch to the previous/next camera. • Edit/delete camera sequence: Right-click a camera sequence resource and select Edit/Delete to edit or delete it.
Scene	• Save a scene: Right-click and then choose **Save Scene** to save the current video wall layout and video service (such as live video, sequence) as a scene. • Start a scene: Right-click a scene and select **Start Scene** to start it on the video wall. **Note:** If there is an active group sequence (schedule) on the video wall, you need to stop the group sequence (schedule) before starting a scene. Starting a scene will replace all the existing videos on the video wall. • Rename a scene: Right-click a scene and select **Change Name**.
Scene Sequence	Play multiple scenes on the video wall sequentially. • Add a scene sequence: Click + above the scene sequence list to add multiple scenes to a scene group. **Note:** • Time Interval: Set the time interval to switch to the next scene. • Display Order: Select a scene and use the arrows above the list to adjust its display order.  • Start a scene sequence: Right-click a scene sequence resource and select **Enable**. A message "Scene sequence is in progress." will display, indicating the successful operation. 

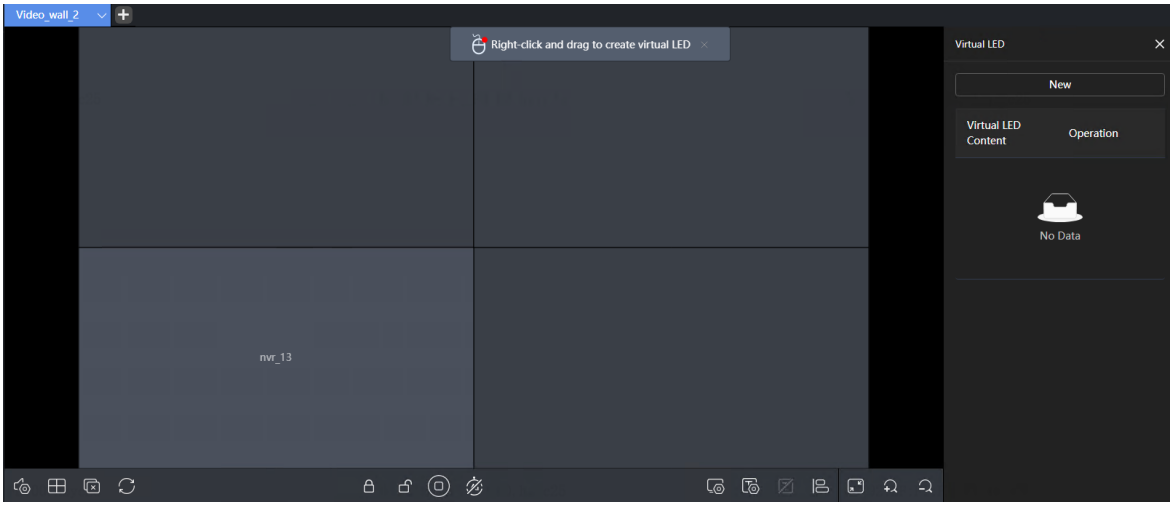
Resource	Operation
	Note: • If there is an active group sequence (schedule) on the video wall, you need to stop the group sequence (schedule) before starting a scene sequence. • Starting a scene sequence will replace all the existing videos on the video wall. • Stop scene sequence: Click **Disable** in the pop-up window to stop the scene sequence. The video wall will keep the current scene and stop switching. • Edit/delete scene sequence: Right-click a scene sequence resource and select **Edit**/**Delete** to edit or delete it.
Group Sequence	Play live video of multiple cameras in multiple video wall windows simultaneously. **Note:** • If the number of cameras is less than or equal to the number of windows, their positions remain fixed and are unaffected by the stay time. • If the number of cameras is greater than the number of windows, the cameras will cycle through the windows based on the stay time. For example, there are 4 windows in the scene and 5 cameras in the group sequence group, the cameras will cycle through the windows as follows: 1234, 5123, 4512, ... • Add group sequence: Click + above the group sequence list to add multiple cameras to a group sequence group. **Note:** • Startup Mode: Non-preemption mode-The group sequence will not replace the current video services at startup. Preemption mode-The group sequence will replace the current video services at startup. • Stay Time: Set the time interval to switch to the next screen. • Select Video Wall: Select a specific scene on the video wall (ensure that the scene is saved in advance, otherwise the scene resource cannot be found. The scene determines the window layout of the video wall, and hovering the mouse over the scene allows you to preview the scene layout).  • Start group sequence: Right-click the group sequence resource and then select **Enable**. **Note:** Only one group sequence can be enabled at a time. Once started successfully, the following operations are allowed:

Resource	Operation
	• Previous/Next Screen: If the number of cameras in the group sequence group is greater than the number of windows, the cameras will be divided into multiple groups as screens for playing. You can right-click on a resource and select **Previous Screen/Next Screen** to switch the camera group. • Pause/Resume: Right-click a group sequence resource and select **Pause** to retain the current camera group on the video wall; select **Resume** to resume cycling. • Stop: Right-click a group sequence resource and select **Stop** to stop the current group sequence and close the current video. • Edit/delete group sequence: Right-click a group sequence resource and then select **Edit/Delete** to edit or delete it.
Group Sequence Schedule	Set the play time for each group sequence resource on the video wall to cycle through them. • Add a group sequence schedule: Click + above the group sequence schedule. **Note:** • Video Wall: Select a video wall to add its group sequence resources to the schedule. • Period: By Day-Set time periods for each resource within a day; By Week-Set time periods for each resource on each day of the week. • Enable Exception: If needed, for special dates, specify custom time periods for resources.  • Enable a group sequence schedule: Right-click a schedule and then select **Enable**. The corresponding group sequence will automatically start at the set time. **Note:** Only one group sequence schedule can be enabled at a time. • Disable a group sequence schedule: Stop group sequence schedule: Right-click the group sequence schedule and then select **Disable**. The group sequence schedule will be disabled, and the group sequence will be stopped.

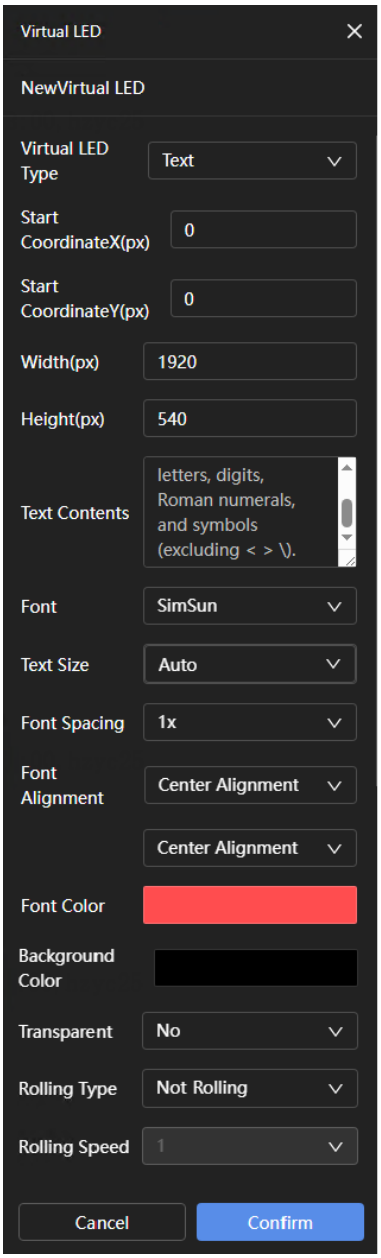
Resource	Operation
	• Edit/delete a group sequence schedule: Right-click the group sequence schedule and then select **Edit**/**Delete** to edit or delete it.

9.3.1.6 Configure Virtual LED

You can configure virtual LEDs to display custom text contents on the video wall.



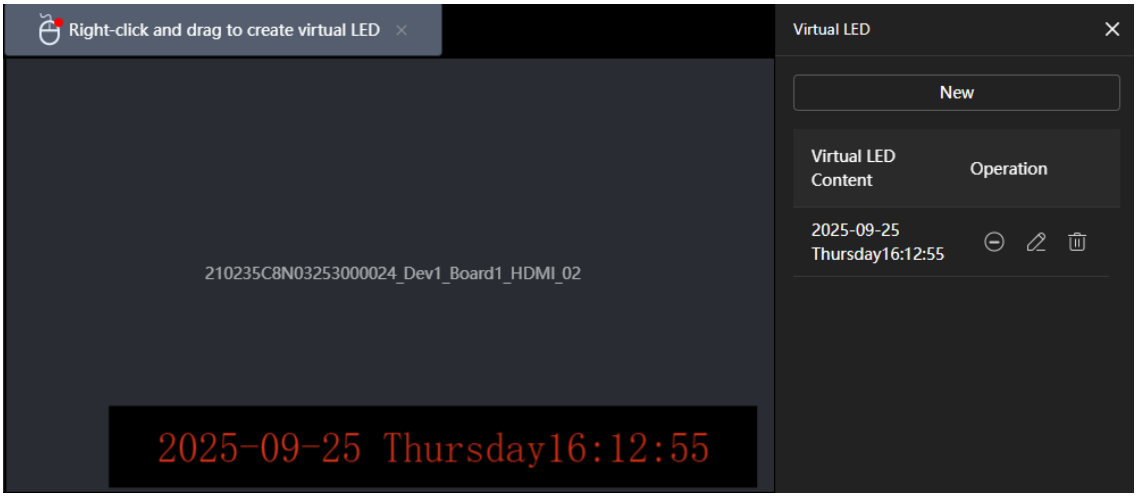
1. On the bottom toolbar, click to expand the virtual LED configuration panel.
2. On the video wall window, right-click and drag to draw a bounding box for the virtual LED; or, click **New** on the right panel.
3. On the expanded **Virtual LED** panel, set parameters such as the virtual LED type (text/time), position, width and height, style, and scrolling mode, and then click **OK**.



Note:

- A video wall supports one scrolling virtual LED and sixteen static virtual LEDs.
- The positions of virtual LEDs cannot overlap.

4. View the successfully added virtual LEDs on the video wall.



5. To edit the virtual LED, click to open the configuration page.

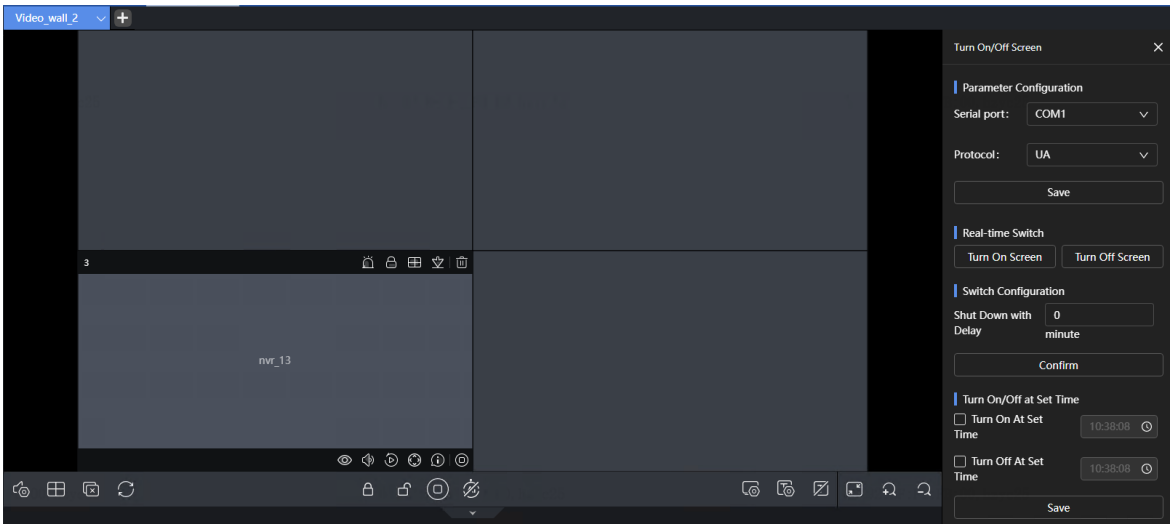
Table 9-8: Virtual LED Operations

Function	Description
Adjust the position/size of a virtual LED	Drag the virtual LED to move it, or drag its border to resize it.
Enable/disable a virtual LED	• Click in its top-right corner to enable/disable the virtual LED. • Select the virtual LED, and then click in the **Operation** column to enable/disable it.
Edit a virtual LED	Click in its upper-right corner; or select the virtual LED, and then click the corresponding in the **Operation** column to edit the virtual LED.
Delete a virtual LED	Click in its upper-right corner; or select the virtual LED, and then click the corresponding in the **Operation** column to delete the virtual LED.

9.3.1.7 Screen Control

Screen control is used to manage serial ports to turn on/off video wall screens.

Figure 9-22: Screen Control



1. Click on the bottom toolbar to expand the screen control panel.
2. Complete the settings by referring to the table below.

Table 9-9: Screen Control Parameter Descriptions

Category	Parameter	Description
Serial Port	Serial Port	Port type. Choose **COM1** or **COM2**.
	Protocol	Serial port protocol. Choose **UA**, or **MODBUS**.
Turn On/Off Screen	Turn On Screen	Turn on all the screens on the video wall.
	Turn Off Screen	Turn off all the screens on the video wall. **Note:** If you set to turn off screens with a delay, the screens will turn off automatically when the set time is over.
	Turn On At	When enabled, the screens will turn on automatically at the set time. **Note:** If the set time is earlier than the current time, the task will be performed at the set time on the following day.

Category	Parameter	Description
	Turn Off At	When enabled, the screens will turn off automatically at the set time. **Note:** If the set time is earlier than the current time, the task will be performed at the set time on the following day.
	Turn Off Screens with Delay	Select the checkbox, and then input the countdown (unit: minute). Click **Turn Off Screen**. The screens will turn off at the end of the set time. **Note:** Clicking **Turn On Screen** will cancel the configured delayed shutdown.

Note:

- Different display control devices support various types of serial ports and protocols. Please select the appropriate serial protocol based on the specific type of display control device.
- Screen control requires matching power distribution boxes, LED screens, LCD screens, specific cables, etc. For detailed configuration, please refer to the commissioning guide.

9.3.2 Multi-DC Video Wall

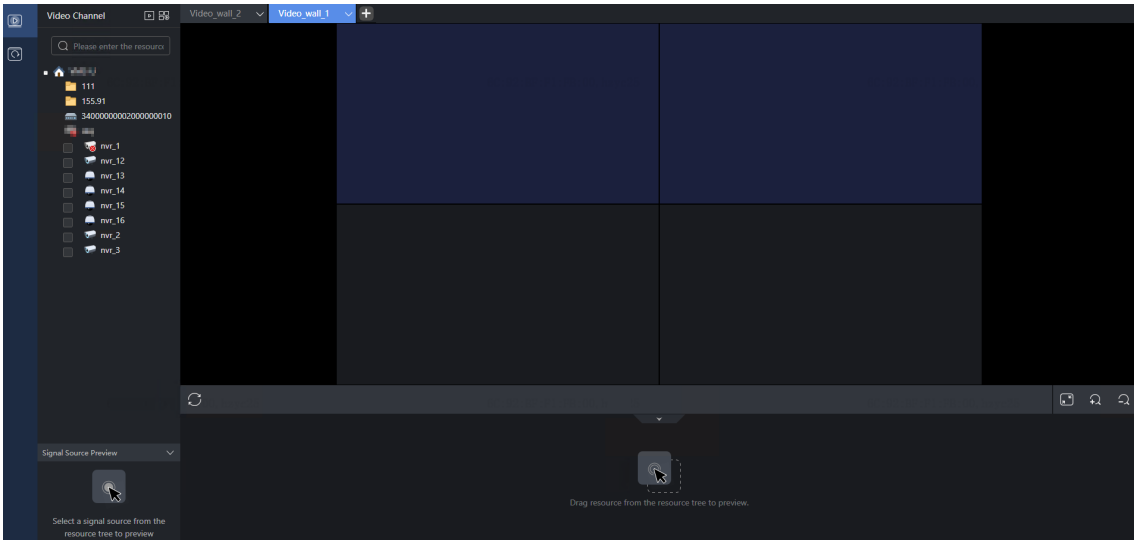
Add a video wall and configure video resources to be played on it. The video wall can be bound to output channels of more than one decoder or video wall controller.

Note:
You need to first add video wall controllers in **Device Management > Terminal Device > Device Decode**.

9.3.2.1 Add Video Wall

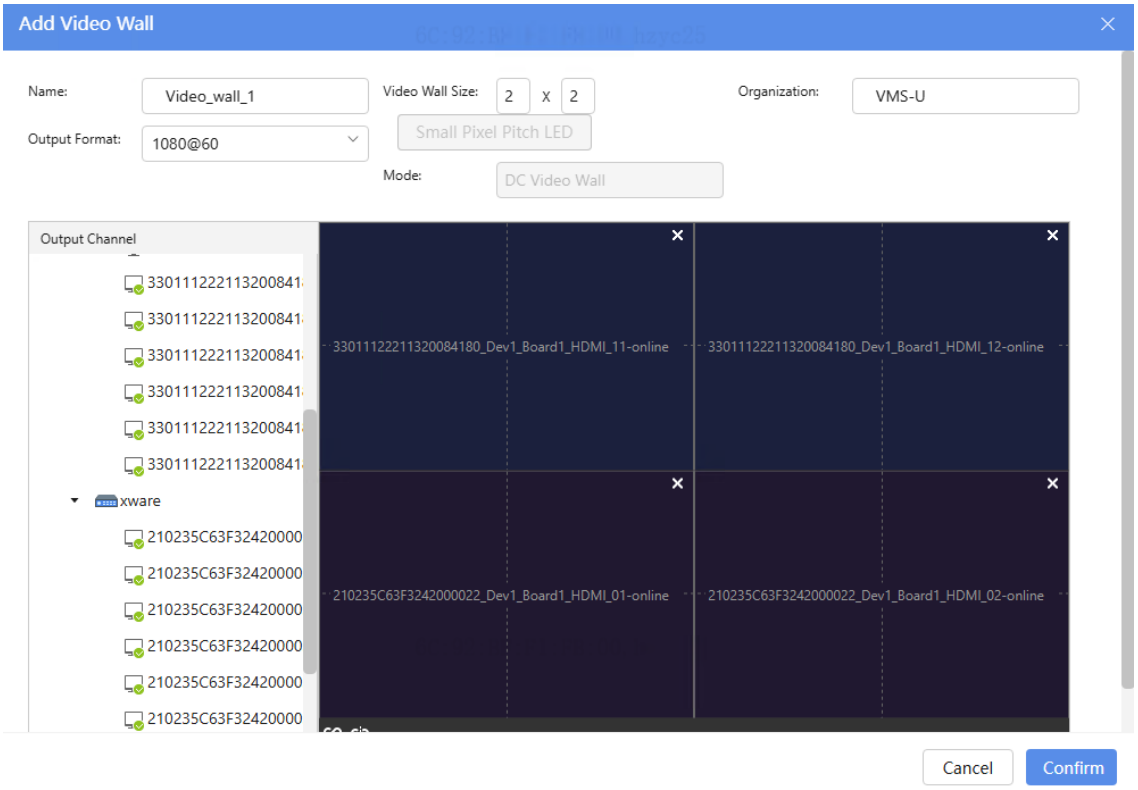
1. If no video wall has been created in the system, click Add Video Wall in the center of the initial page to add one.
   If a video wall has already been created, you can add a new one by clicking + on the top of the right-side pane.
   Select the Multi-DC Video Wall type.

   Figure 9-23: With Exiting Video Wall



2. In the pop-up **Add Video Wall** window, set the video wall name, size, organization, and output format. The configured video wall appears in the pane below.

Figure 9-24: Add Video Wall



3. Drag the idle channels from the left-side list to the video wall windows one by one. The video wall can be bound with channels of different video wall controllers.

   Note:
   Bind/unbind all channels with one-click: Select the video wall controller on the output channel list, and then click in the lower-left corner of the video wall. The idle channels of the video wall controller will be bound automatically to the video wall windows (if some windows on the video wall are already bound, the current bindings will be cleared first). Click to delete all bindings.

4. Click **OK**. The video wall is created.

Note:
After adding a video wall, you can click the arrow right to the video wall name to edit, close, or delete the video wall.

9.3.2.2 Canvas Operations

Canvas refers to the background displaying the video wall windows.

- Drag the outer area of the video wall to move the canvas.
- Scroll the mouse wheel to zoom in/out on the canvas.
- Click in the bottom toolbar to restore the view.

9.3.2.3 Window Operations

- **Open window**: Drag a camera or sequence resource from the left-side tree to the video wall to open a window; or drag with the right button pressed on the video wall to open a window.

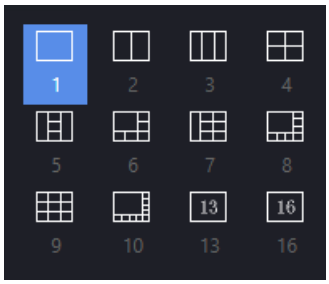
  Note:
  The multi-DC video wall only supports opening windows with full VO.

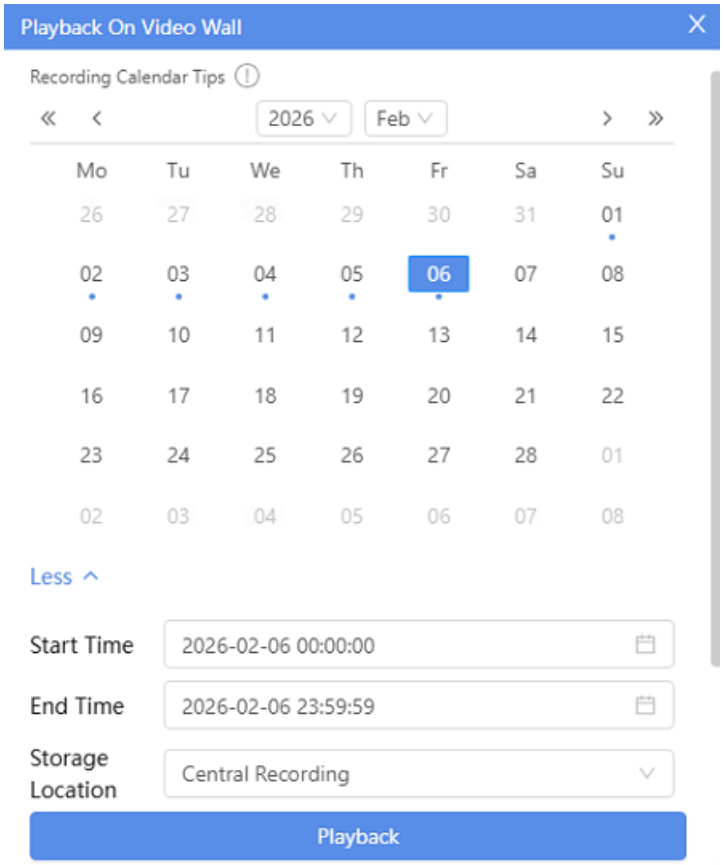
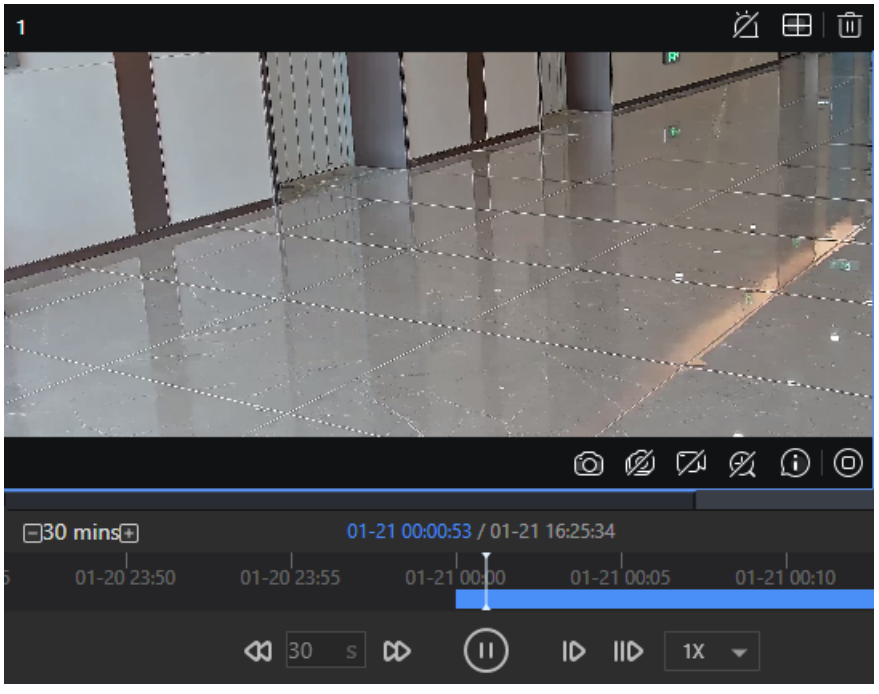
- **Close window**: Click in a window's top-right corner to close the window.

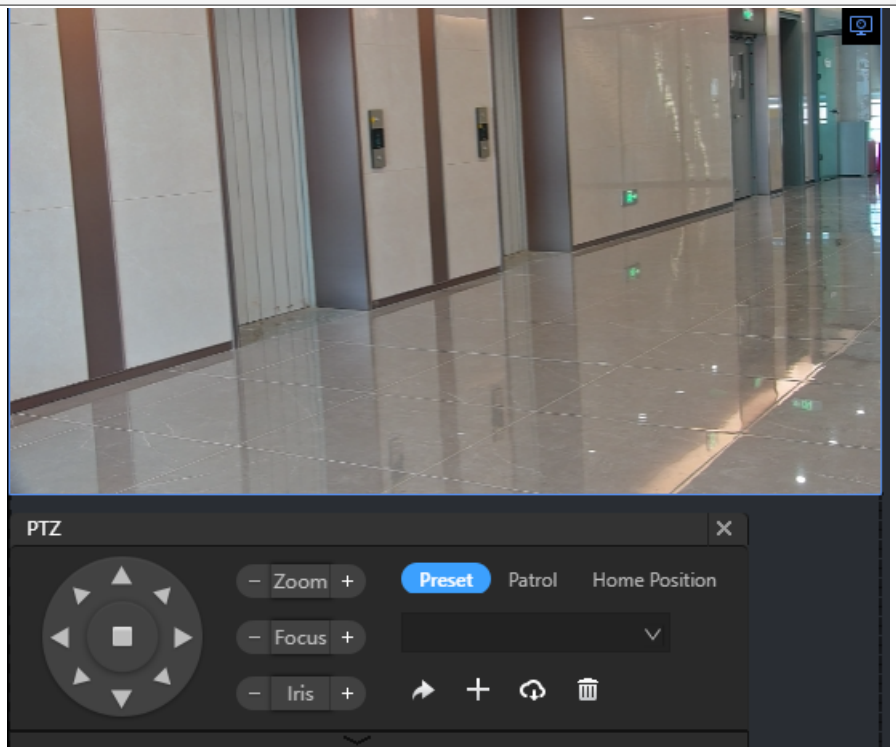
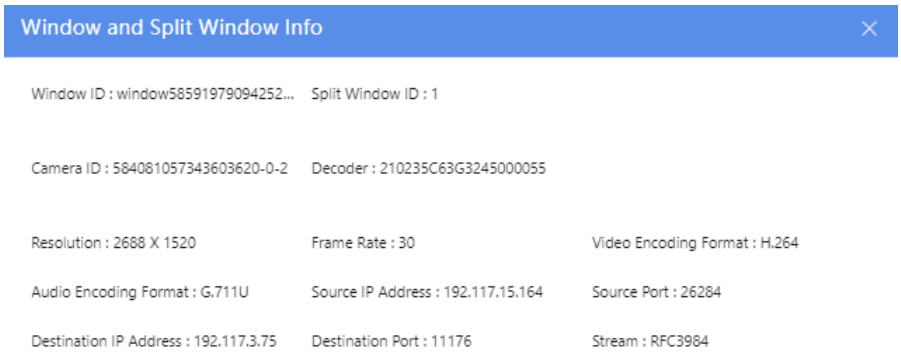
Video Wall Toolbar Operations

Icon	Description
	Refresh the page.
	Restore view: Reset the video wall view to its initial position.
/	Zoom in/out on the view. You can also use the mouse wheel to zoom in/out.

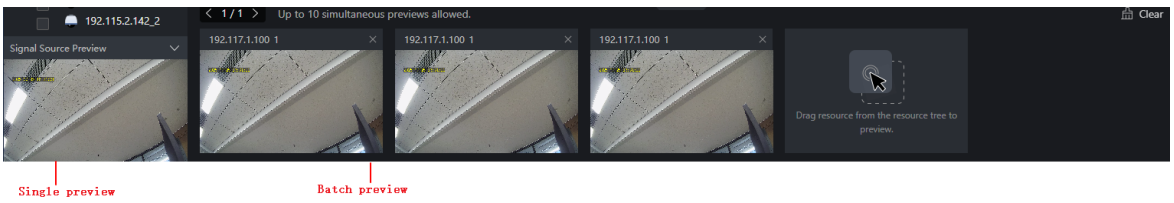
Window Toolbar Operations

Icon	Description
1	Window ID.
	Enable/disable alarm linkage. When enabled, the window will play the live video from the linked camera when an alarm is triggered. **Note:** You must go to Alarm Linkage Configuration and configure alarm-triggered live video to the video wall first.
	Split the window. 
	Delete the window.
	Preview the live video in the window. Click again to stop the preview. The following operations are allowed during preview: snapshot, continuous snapshots, local recording, and digital zoom. **Note:** Only one window can be previewed at a time.
/	Enable/disable PTZ shortcut operations: • Enabled: Clicking on the live view window allows you to control PTZ movement, enabling quick operations.

Icon	Description
	• Disabled: Clicking on the live view window will not trigger PTZ movement, preventing accidental operations.
	Switch to playback on video wall, set search criteria, and preview the retrieved recordings in the window.  Click the playback preview window, expand the toolbar, and then you can stop playback, adjust playback speed, etc. 
	Expand the PTZ control panel to control the rotation of the PTZ camera.

Icon	Description
	
	View window and channel resource information in the window. 
	Stop decoding in the window.

9.3.2.4 Resource Preview



- **Single preview**: Click a video channel in the left resource tree to preview it.
- **Batch preview**: Drag video channels/local input channels from the left resource tree to the bottom of the page for preview (supports up to 10 resources for simultaneous preview).
  - Double-click the title bar to maximize the window.
  - Drag the title bar to play the live video on the video wall.
  - When multiple previews exist, click < 1/2 > to page through.
  - Click Clear to clear all preview resources.

9.3.2.5 Play Video Resources on Video Wall

Click the icon on the left-side menu bar to view the corresponding resources.

Table 9-10: Play Different Video Resources on Video Wall

Resource	Operation
Video channel	• Play live video on video wall: Drag a camera to a video wall window; or click a window, right-click the camera, choose **Live View on Video Wall** > **Main Stream/ Sub Stream/Auto** to start live video in the window. • Playback on video wall: To play recordings of a camera in a video wall window, click the window, right-click the camera and then choose **Playback on Video Wall**. In the pop-up window, set search parameters including playback time and search domain, and then click **OK**
Camera sequence	Drag a camera sequence resource to a video wall window to start camera sequence in the window.

9.4 Smart Live View

View live videos and snapshots of Face Recognition, Vehicle Application, Multi-Target Detection, People Counting, Door Access Control.

9.4.1 Smart Live View

Go to **Video Application > Smart Live View > Smart Live View**.

Allows users to view live videos of video channels under smart IPCs and NVRs, as well as access control devices. The real-time snapshot data and alarms (face match records, vehicle match records, and person/motor vehicle/ non-motor vehicle data from multi-target detection) are displayed when playing smart live view.

Prerequisite

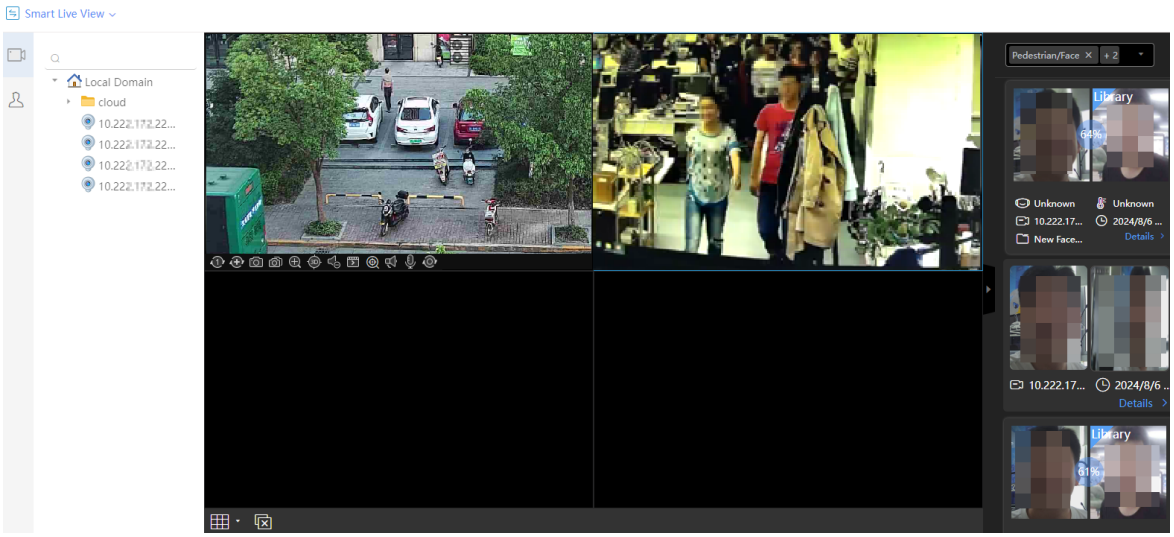
- Smart IPC/NVR have been added to the platform. See **Device Management** > **Frontend Device**.
- Face recognition/vehicle recognition/people counting/multi-target detection function have been enabled on the device.
- Face Monitoring and Vehicle Monitoring tasks have been configured.

Play Live View

Double-click on a camera in the channel list to view the live view of the camera in a window.

Note:

- Up to 4 cameras' live view can be displayed at the same time. You can click in the lower-left corner to switch to 1/3/4 windows.
- To perform operations on the live view, see **Live View Toolbar**.
- Face comparison records, vehicle comparison records, and the multi-target detection results can be reported after the Live View started.



Data Display

The face comparison records, vehicle comparison records, person/motor vehicle/non-motor vehicle information from multi-target detection are displayed on the right side. You can select the target type from the drop-down list to filter data.

Note:
You can customize the attributes displayed on the card as needed. See Card Attribute.

Click **Details** in the lower-right corner of the snapshot to view more details.

9.4.2 Face Recognition

Go to **Video Application > Smart Live View > Face Recognition**.

You can view live videos of video channels under smart IPCs and NVRs, face recognition data reported by devices, face match/not match alarms, important person alarms, real-time passing persons, and abnormal persons.

Prerequisites

- Smart IPC/NVR have been added to the platform. See Device Management > Frontend Device> Private Device.
- Face recognition function has been enabled on the device.
- Face Monitoring task has been configured.

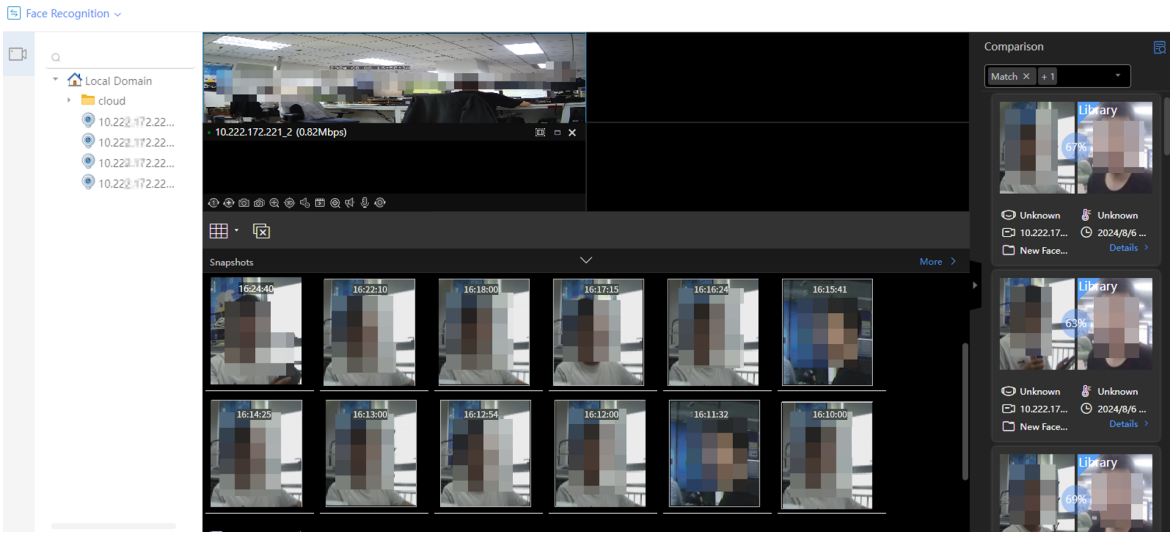
On the **Smart Live View** page, click and select **Face Recognition**.

Play Live View

Double-click on a camera in the channel list to view the live video of the camera in a window.

Note:

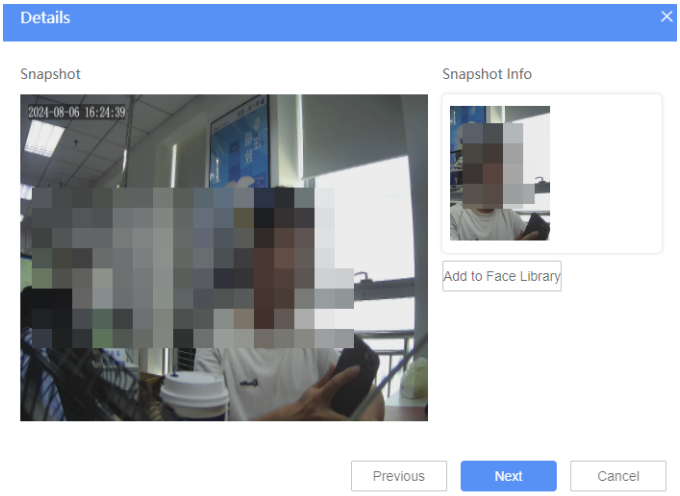
- Up to 4 cameras' live videos can be displayed at the same time. You can click in the lower-left corner to switch to 1/3/4-window.
- To perform operations on the live view, see Live View Toolbar.



Snapshots Records

The real-time face snapshots are displayed under the live view window.

- Click a snapshot to view more details.

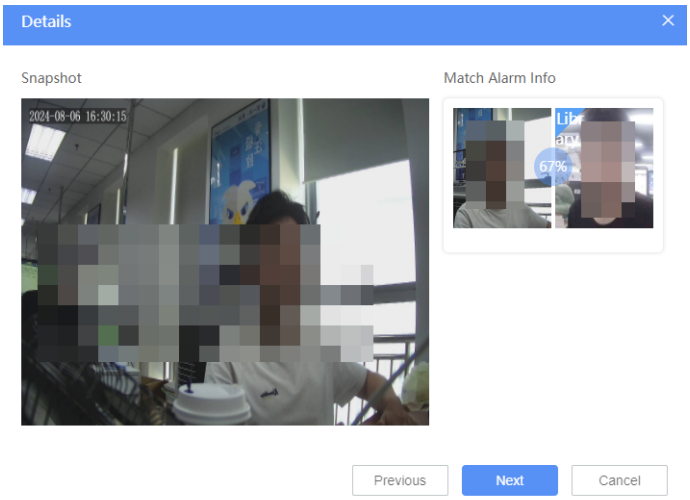


- For a stranger's snapshot, hover the mouse over the snapshot and click ＋ to add the stranger to Face Library.
- Click **More** to redirect to the page and search the snapshots by attributes.

Alarm Records

The real-time face comparison records are displayed on the right side. You can select criteria from the drop-down list to filter match/not match alarms.

- Click **Details** to view more details.



- For a stranger's snapshot, hover the mouse over the snapshot and click + to add the stranger to Face Library.
- Click in the upper-right corner to redirect to the Face Search page and search the snapshots by events.

Related Operation

You can customize the attributes displayed on the snapshot record and alarm record cards as needed. See Card Attribute.

9.4.3 Vehicle Application

Go to **Video Application > Smart Live View > Vehicle Application**.

You can view live videos of video channels under smart IPCs and NVRs, vehicle recognition data and speeding alarms reported by devices, match/not match alarms by monitoring task, real-time passing vehicles and abnormal vehicles, as well as open gate manually.

Prerequisite

- Smart IPC/NVR have been added to the platform. See Device Management **>** Private Device.
- Vehicle recognition function has been enabled on the device.
- The pre-registered vehicle list and forbidden vehicle list have been configured. See **Parking Mgt-**Vehicle Management.
- Speeding rules have been configured for speeding alarms. See details in Configure Alarm Rules.

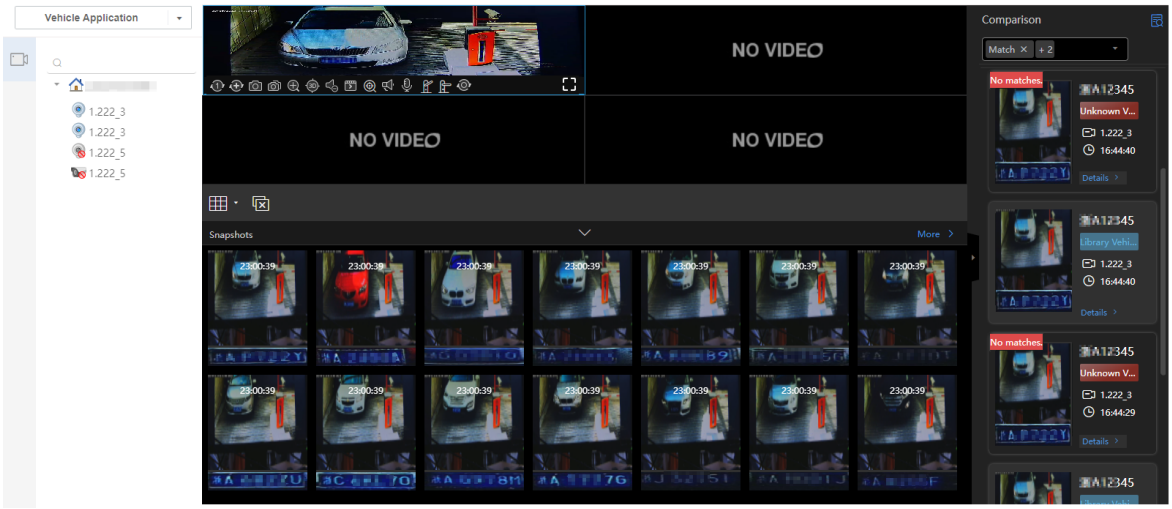
On the **Smart Live View** page, click and select **Vehicle Application**.

Play Live View

Double-click on a camera in the channel list to view the live video of the camera in a window.

Note:

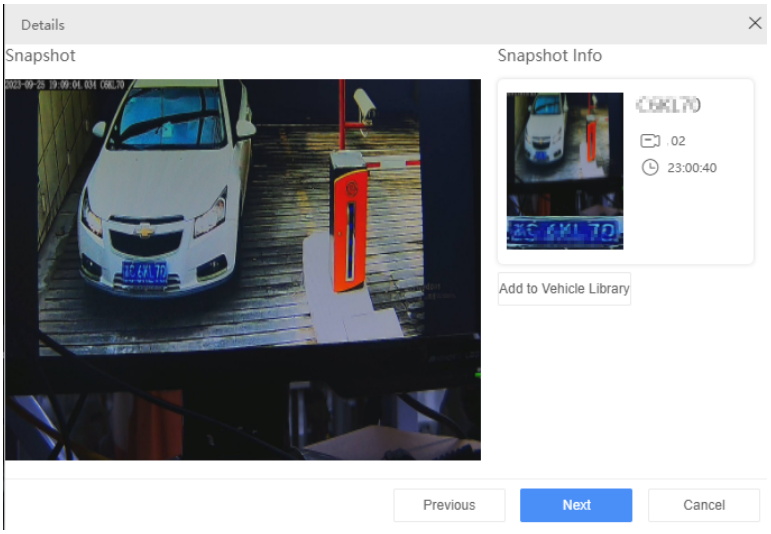
- Up to camera's live videos can be displayed simultaneously. You can click in the lower-left corner to switch to 1/3/4 windows.
- To perform operations on the live view, see Live View Toolbar.
- To manually open/close the gate, click / on the toolbar, or right-click the camera to select **Open Gate** / **Close Gate**.



Snapshots Records

The real-time vehicle snapshots and vehicle plate images are displayed under the live view window.

- Click a snapshot to view more details.

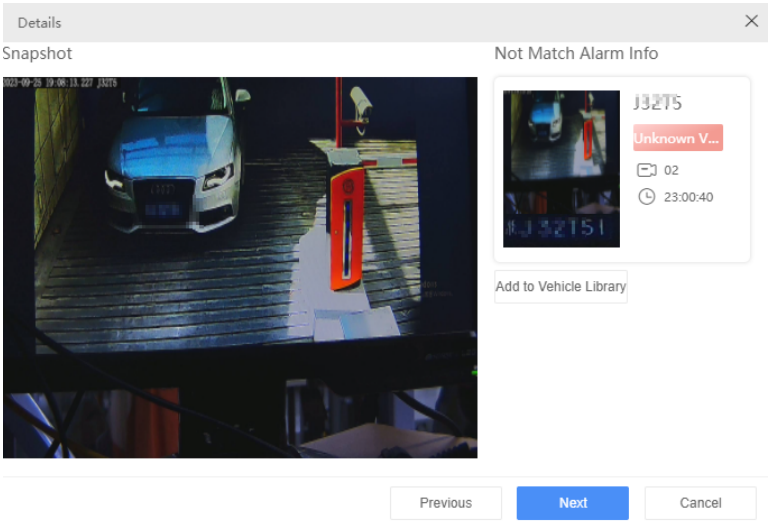


- For an unknown vehicle's snapshot, hover the mouse on the snapshot and click + to add the unknown vehicle to the Vehicle Library.
- Click in the upper-right corner to redirect to the Motor Vehicle Search page and search the snapshots by attributes.

Alarm Records

The real-time vehicle comparison records are displayed on the right side. You can select criteria from the drop-down list to filter match/not match alarms and speeding alarms.

- Click a comparison record to view more details.



- For an unknown vehicle's snapshot, hover the mouse on the snapshot and click + to add the unknown vehicle to the Vehicle Library.
- Click **More** to redirect to the Motor Vehicle Search page and search the snapshots by events or by violation.

Related Operation

You can customize the attributes displayed on the snapshot record and alarm record cards as needed. See Card Attribute.

9.4.4 Multi-Target Detection

Go to **Video Application > Smart Live View > Multi-Target Detection**.

View the live videos of the video channels under the smart IPC/NVR and the motor vehicle/non-motor vehicle/pedestrian/face recognition data reported by the device.

Prerequisite

- Smart IPC/NVR have been added to the platform. See **Device Management** > **Private Device**.
- Multi-target detection function has been enabled on the device.

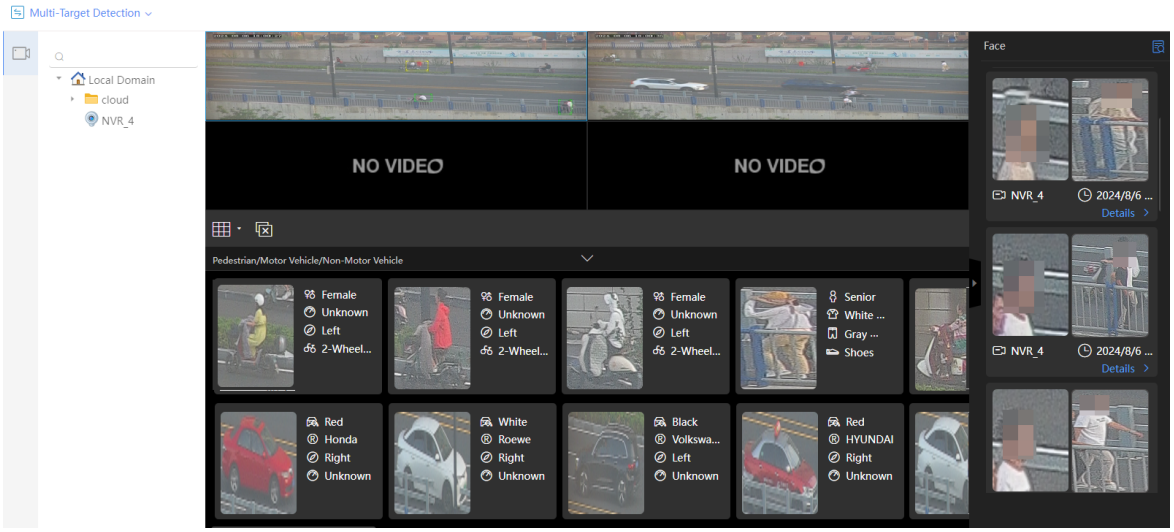
On the **Smart Live View** page, click ⌄ and select **Multi-Target Detection**.

Play Live Video

Double-click on a camera in the channel list to view the live video of the camera in a window.

Note:

- Up to 4 live video windows can be displayed at the same time, you can click ⊞ in the bottom left corner to switch to 1/3/4 windows.
- To perform operations on the live view, see Live View Toolbar.



Snapshots Records

The latest pedestrian/motor vehicle/non-motor vehicle snapshots are displayed below the live view window. The latest face snapshots are displayed on the right side.

Note:

You can customize the attributes displayed on the card as needed. See Card Attribute.

Click a snapshot, or click **Details** in the lower-right corner to view more details.

9.5 Media Configuration

Go to **Video Application > Media Config**.

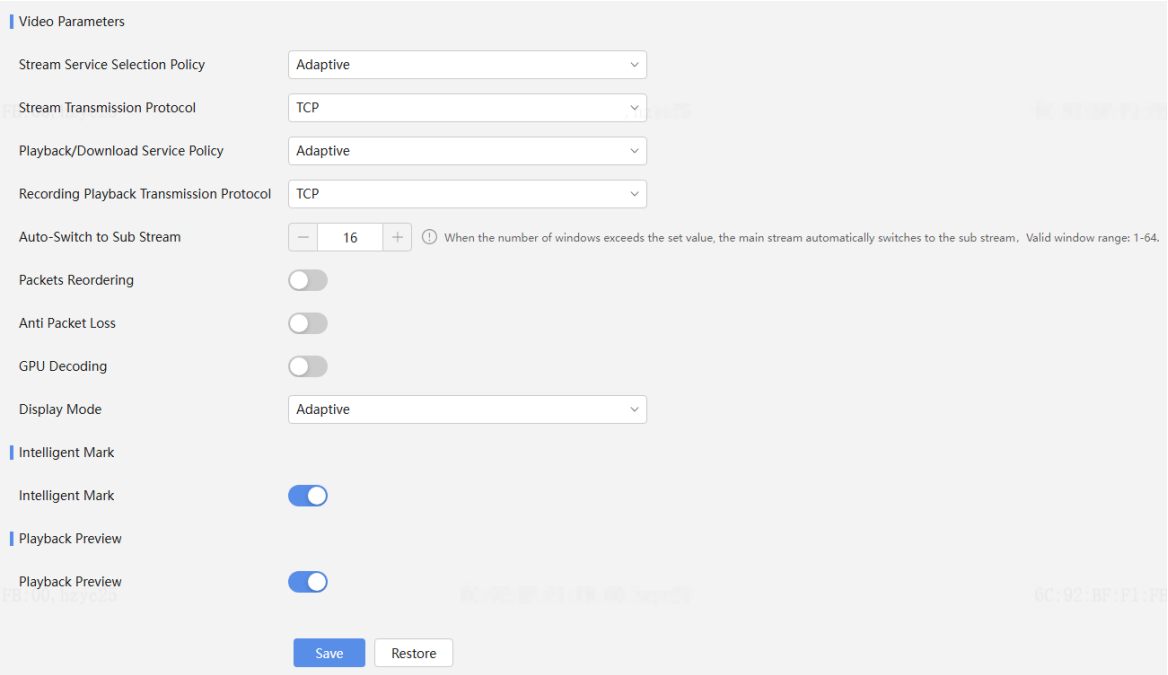
Configure live, playback stream, snapshot, recording and PTZ parameters.

Note:

- B/S media configuration is globally effective, while C/S media configuration is effective only on the current login PC.
- B/S and C/S media configurations do not affect each other; i.e., B/S configuration affects only B/S services, not C/S services.

9.5.1 Video

Video Application > Media Config > Video: Configure live and playback stream parameters.



Parameter	Description
Stream Service Selection Policy	For live view streams: • **Adaptive**: The system selects the appropriate stream selection policy based on the actual network conditions and server's forwarding capacity. • **Direct Connection Priority**: Streams from encoders are preferably sent directly to the client without passing through the server, reducing the server's forwarding load.

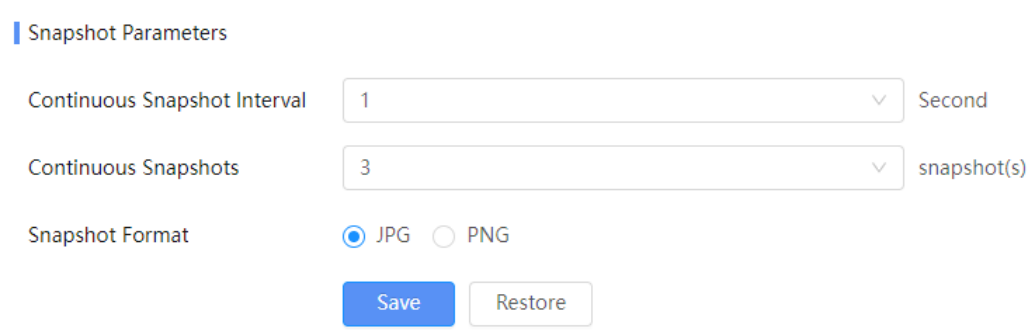
Stream Transmission Protocol	For live view streams:
	• When the **Stream Service Selection Policy** is set to **Adaptive**, then the **Stream Transmission Protocol** must also be set to **Adaptive**. The system will select the appropriate transmission protocol based on the network conditions and the encoder's configuration.
	• When the **Stream Service Selection Policy** is set to **Direction Connection Priority**, then the **Stream Transmission Protocol** can be set either **TCP** or **Follow Device**.
	  • **TCP**: (the encoder's transmission protocol must be set to TCP) Offers better video smoothness but may have some delay. It is recommended to choose it in poor network conditions to ensure the complete reception of streams.
	  • **Follow Device**: Uses the same transmission protocol as the encoder.

Playback/Download Service Policy	For playback/download streams: • **Adaptive**: The system selects the appropriate service policy based on the actual network conditions and server's forwarding capacity. • **Direct Connection Priority**: Streams are sent directly to the client without passing through the server, reducing the server's forwarding load.
Recording Playback Transmission Protocol	For playback streams: • **TCP**: Offers better video smoothness but may have some delay. It is recommended to choose it in poor network conditions to ensure the complete reception of streams. • **UDP**: Offers better real-time performance but may result in frame loss.

Parameter	Description
Auto-Switch to Sub Stream	When the number of windows exceeds the set value, the main stream automatically switches to the sub stream. Valid range: 1-64.
Packets Reordering	When enabled, the system will automatically detect and reorder any out-of-order streams. Generally, reordering improves the image quality and smoothness, though there might be a slight delay.
Anti Packet Loss	Packet loss can affect audio and video quality. If you encounter issues such as image stuttering in live videos, we recommend enabling this function, though there might be a slight delay.
GPU Decoding	When enabled, live videos and recordings are decoded using the GPU of the current login PC, which reduces CPU load and improves the number of decoding channels and video smoothness. **Note:** • The PC must be configured with an Intel or NVIDIA graphics card; AMD graphics card is currently not supported. • Enabling both GPU decoding and intelligent mark simultaneously may affect the overlay of intelligent marks on live video.
Display Mode	For CPU decoding only. • Adaptive (Default): When the image resolution is greater than 1080P, no processing is applied, and the original image is retained. When the image resolution is less than or equal to 1080P, bilinear interpolation is applied, which reduces the rendering load and increases the number of concurrent video streams, but may result in slight aliasing. • Anti-aliasing: Applies bicubic interpolation to the image, which eliminates aliasing and smoothens the image. However, this increases CPU usage and GPU rendering load. • Original quality: No processing is applied to the image, preserving the original image quality.
Intelligent Mark	When enabled, the target detection box(es) of intelligent detection will be overlaid on the live video. **Note:** The camera side needs to enable perimeter defense, mixed traffic detection, face recognition, and vehicle recognition functions.
Playback Preview	When enabled, you can preview the playback thumbnail on the recording playback timeline.

9.5.2 Snapshot

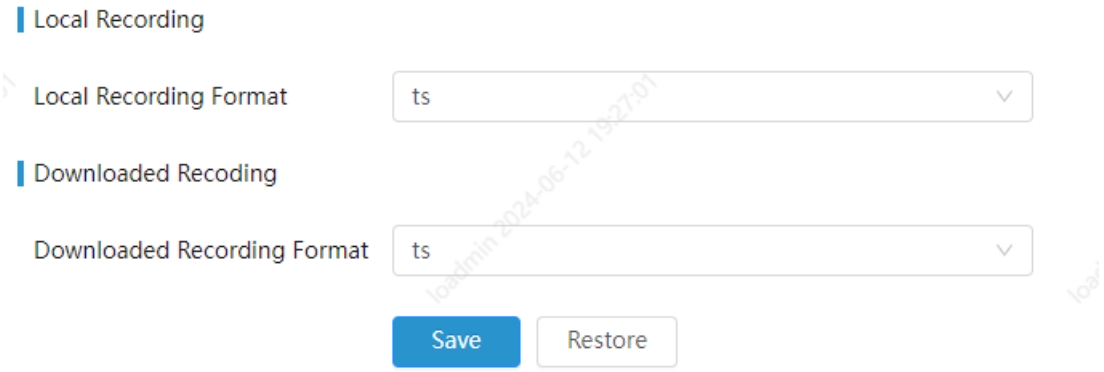
Video Application > Media Config > Snapshot : Configure the snapshot mode and parameters.



Parameter	Description
Continuous Snapshot Interval	Time interval between two snapshots.
Continuous Snapshots	Number of snapshots to take every time.
Snapshot Format	Set the format of snapshots, JPG or PNG

9.5.3 Recording

Video Application > Media Config > Recording : Configure recording format (ts or mp4).

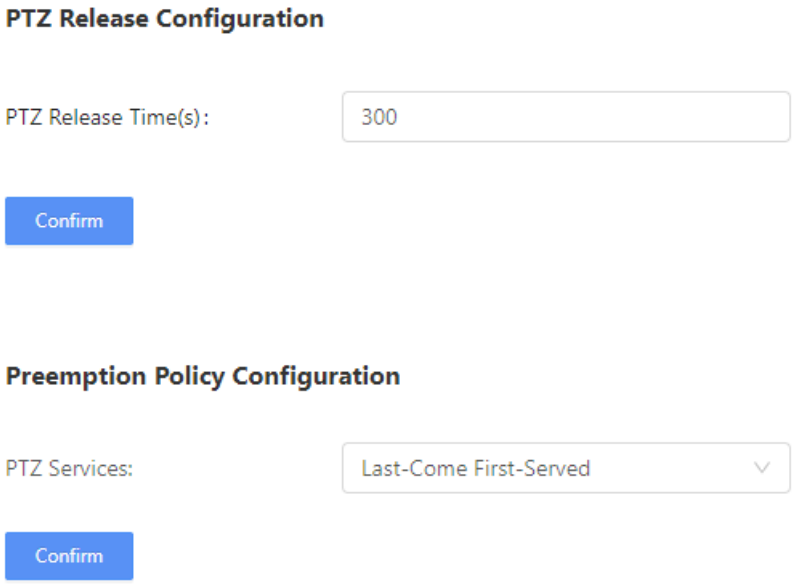


9.5.4 Video Wall

Video Wall Live View Parameters: When the split windows in a window exceed the specified value, live video in this window automatically switches to the sub stream. Split window count range: 1-16.

9.5.5 PTZ

System Config> Media Service Config > PTZ Mgt : Configure PTZ control parameters.



- PTZ release time: When the PTZ without being operated for a specified release time and enters the idle status, any user can control it without preemption, and the originally locked PTZ will be unlocked automatically.
- Preemption policy configuration: When multiple users attempt to operate the same PTZ simultaneously, the system determines the preemption strategy based on user priority and the order of operations.

10 AR Live Map

Go to **Video Application > AR Live Map**.

AR live map upgrades the traditional 2D map command system, which lacks a sense of presence, into a three-dimensional command system based on augmented reality.

Using the live video from an high-position camera as a real-world map, it supports the overlay of additional resource labels (such as surveillance points, buildings, roads, etc.), while integrating with a 2D map to construct a comprehensive, multi-angle video surveillance network, providing multi-dimensional information support for command and dispatch.

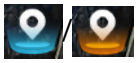
Note:
By default, one high-position camera is supported. For multiple AR cameras, additional licenses are required.

Go to the AR live map page:

- If no high-position camera is available, please first configure high-position cameras.

- If a high-position camera already exists, the live video from the first camera in the high-position camera list will automatically play.

Table 10-1: Icons

Icon	Function Description
	Expand or collapse the toolbar below.
	View AR live map in full screen.
	Show or hide all label names.
	Enable or disable 3D positioning. **Note:** VSS cross-domain cameras do not support 3D positioning.
	Show or hide the PTZ control panel.
	Show or hide the map.
	After displaying the map, switch between the map and the live view.
	After displaying the map, zoom in or out on the map.

10.1 Configuration

Click the **Configure** button in the toolbar at the bottom to go to the **Configuration** page.

Perform high-position camera configuration, personalization, high-position camera image rotation, and more.

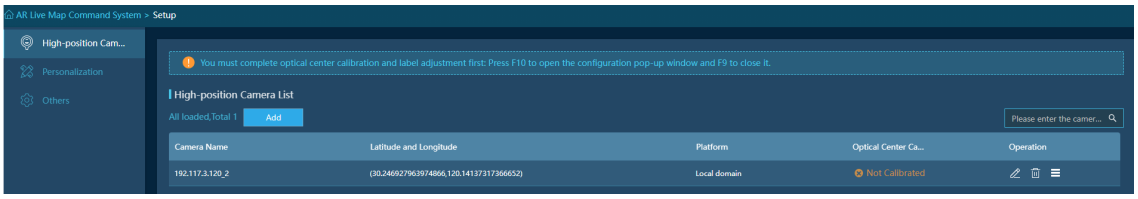
10.1.1 Configure High-Position Camera

AR live maps can only be accessed after a camera has been configured as a high-position camera.

Add High-Position Camera

1. Click **Configure** at the bottom of the **AR Live Map** page, go to **Configuration > High-Position Camera Setup**.

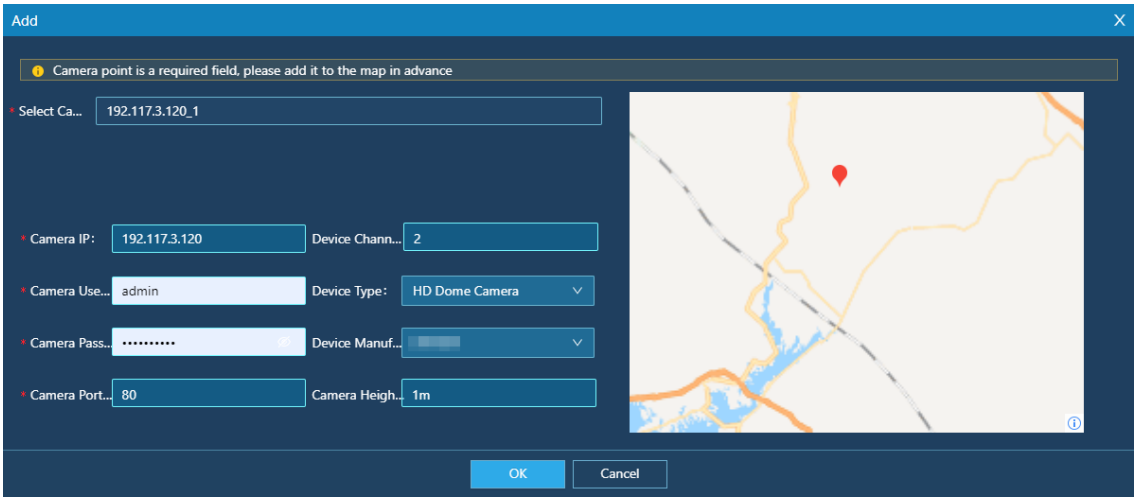
   Figure 10-1: High-Position Camera Setup

2. Click **Add**, go to the **Add** page and configure the high-position camera information.

   Note:
   Ensure that the high-position camera has been added to the map in advance in Edit Map.
   Currently, 2D maps and GIS maps are supported.

Figure 10-2: Add High-Position Camera



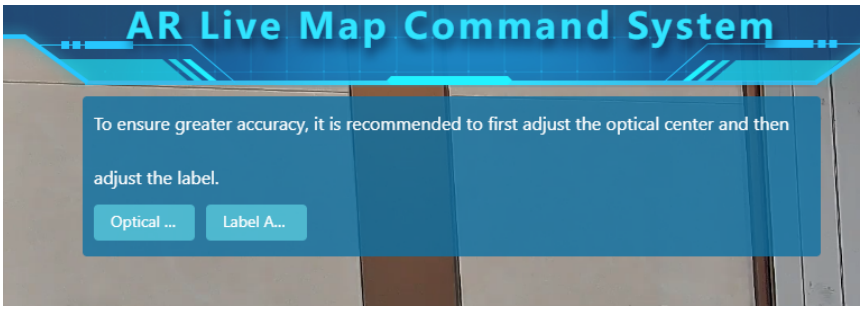
(1) Click the **Select Camera** input field and select a camera from the organizational tree.

(2) When the device type is selected as a PTZ camera, fill in the camera IP and other information for login authentication to enable full functionality such as PTZ control and 3D positioning.

3. Click **OK** to add the high-position camera.

Note:
The first high-position camera in the list will be displayed by default when entering the AR live map interface.
The order of high-position cameras can be adjusted by dragging them in the list.

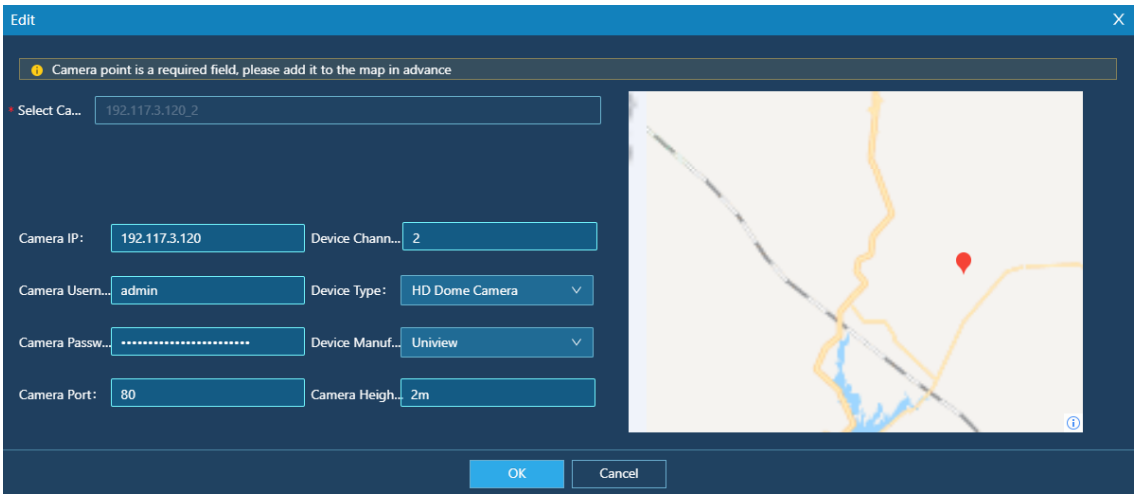
4. Calibrate the high-position camera: Return to the AR live map page, press F10 to enter calibration mode, adjust the screen to position the camera's optical center and label angles, and press F9 to exit calibration mode after completion.



Modify High-Position Camera Information

1. In the high-position camera list, click the corresponding for the camera to go to the page as shown below.

Figure 10-3: Modify Camera Point Marking

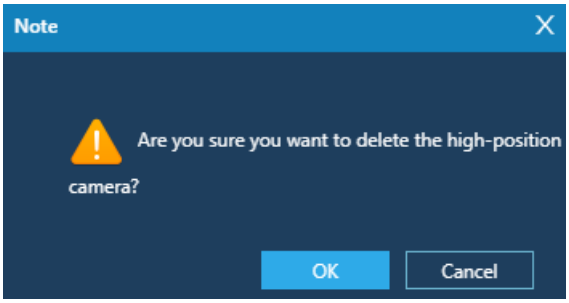


2. Adjust the camera parameter settings and click **OK** to save the changes.

Note:
Modifying the camera position is not supported.

Delete High-Position Camera

1. In the high-position camera list, click the corresponding for the camera.
2. Click **OK** to confirm the deletion.

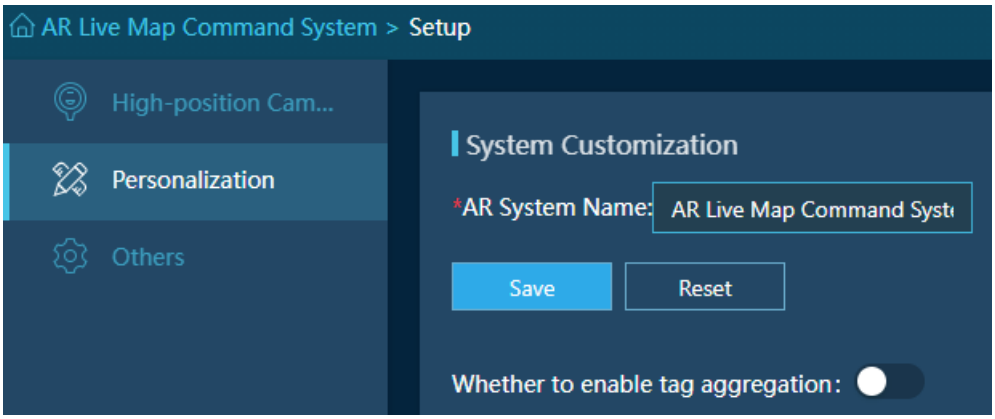


10.1.2 Personalization

Customize the AR live view title name and label aggregation.

Go to **Setup > Personalization**.

Figure 10-4: Personalization

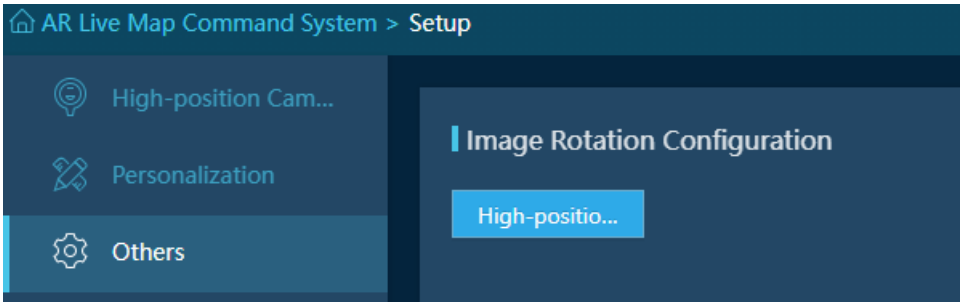


- AR system name: The title name displayed at the top of the AR page. The default name is "AR Live Map Command System," and it supports up to 12 characters.
- Enable label aggregation: When enabled, multiple nearby labels will be aggregated into a single point (the number indicates the label count). Click the aggregation point to expand the label list. It is recommended to enable this when there are many labels to prevent them from overlapping.

Figure 10-5: Display Effect

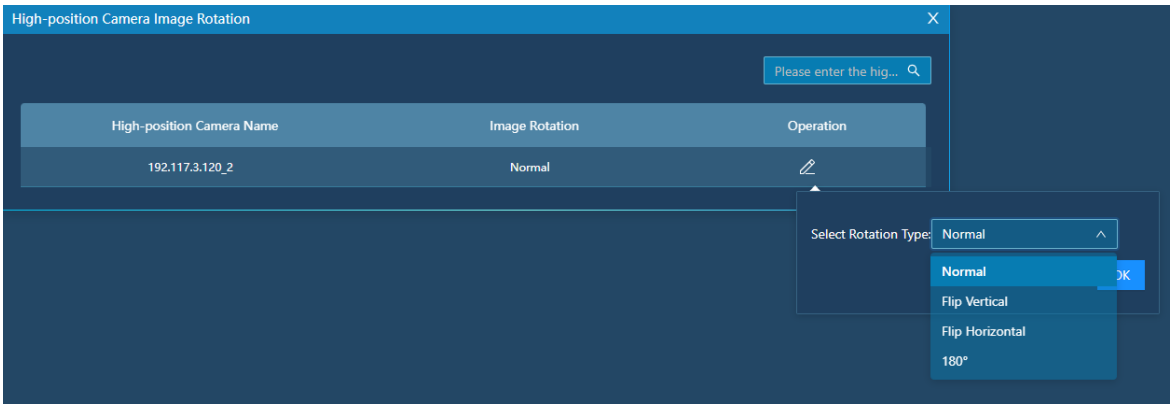
10.1.3 Other Configuration

Figure 10-6: Other Configuration



High-Position Camera Image Rotation

If the camera's image is reversed compared to the real-world scene perspective, the image can be flipped through rotation.



10.2 High-Position Camera Switching

Switch between high-position cameras to view their respective live video.

The system only supports displaying the AR live video from one high-position camera at a time. To view other high-position cameras, perform the following switching operation:

1. Click the to expand the list of high-position cameras.
2. In the camera list, select the desired camera to switch to its AR live view.

Figure 10-7: Swtich High-Position Camera

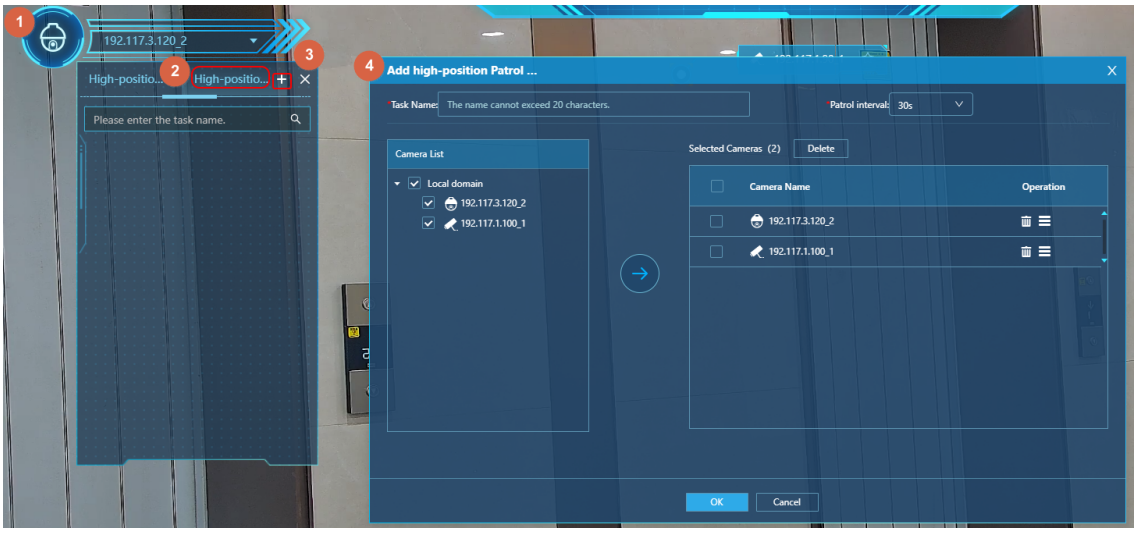
10.3 High-Position Camera Patrol

Add high-position patrol tasks to view live video from multiple high-position cameras in sequence.

Add a High-Position Patrol Task

1. Click , select **High-Position Patrol Task**.
2. Click to add a high-position patrol task.

Figure 10-8: Add High-Position Patrol Task



(1) Enter a task name and set the patrol interval (i.e., the time duration between switching high-position cameras).

(2) In the camera list, select a high-position camera and click → to add it to the patrol group. (Drag ☰ to adjust the order; click 🗑 to remove a camera.)

(3) Click **OK** to complete the task creation.

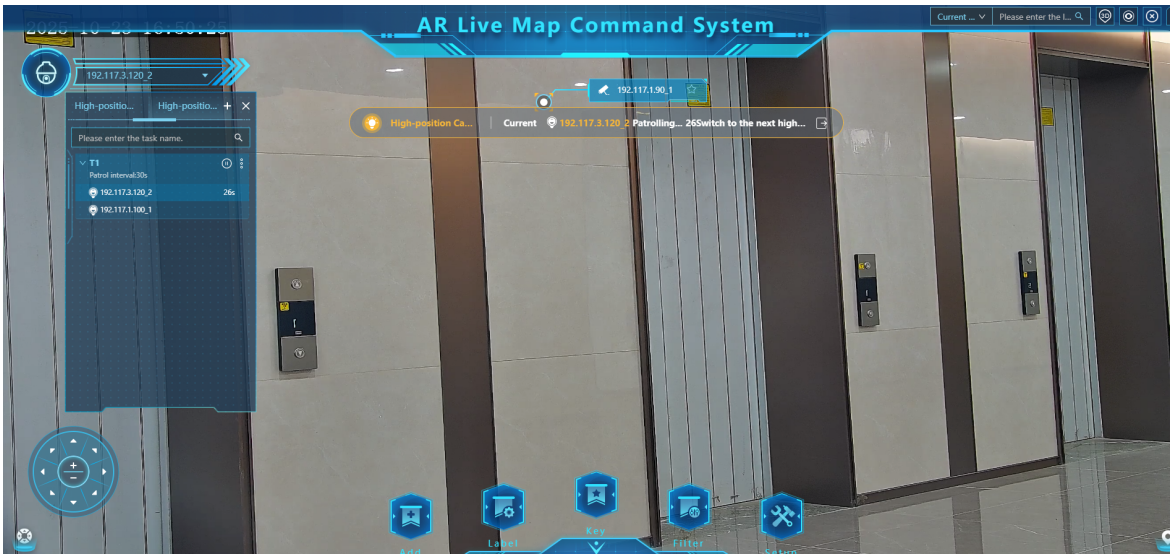
Start High-Position Patrol

In the high-position patrol task list, click ▶ corresponding to the task to initiate the patrol. The high-position cameras in the patrol group will switch and play live video sequentially according to the set time interval. The currently playing camera information is displayed above the live video.

Click ⏸ to pause the patrol task, remaining on the current camera's live video.

Click ⏏ to exit the patrol task.

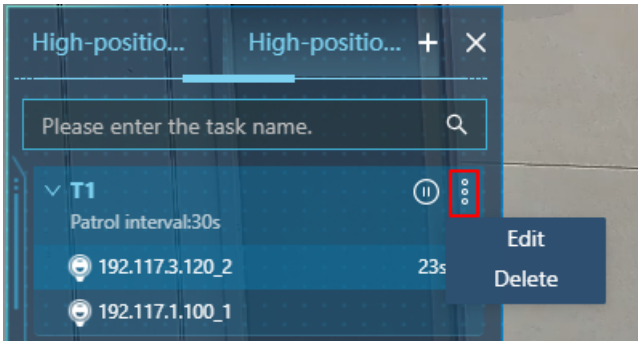
Figure 10-9: High-Position Patrol



Modify Patrol Task

In the high-position patrol task list, click the corresponding ⋮ for the task, select **Edit** to modify task parameters. Refer to Add High-Position Patrol Task for specific operations.

Figure 10-10: Task Operation



Delete Patrol Task

In the high-position patrol task list, click the corresponding ⋮ for the task, select **Delete**, and then confirm the deletion.

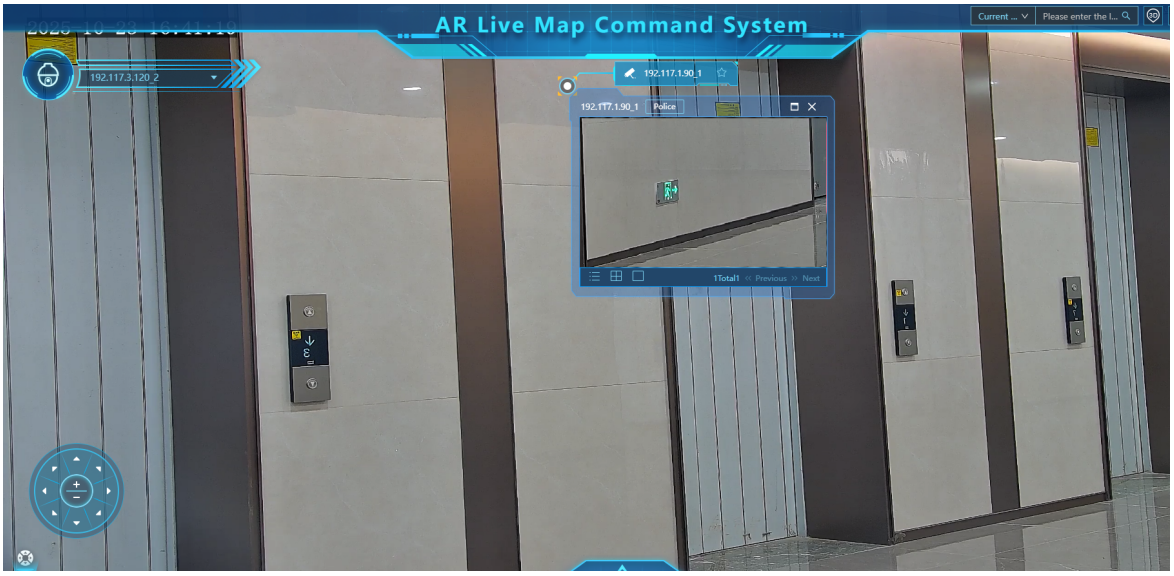
10.4 High-Low Position Camera Linkage

When abnormal situations are detected in the panoramic view of a high-position camera, you can click the low-position camera labels on the screen to view their live videos for detailed monitoring.

On the high-position camera's live view image, click a low-position camera label to open its live video.

Note:
A maximum of 5 labeled live videos can be displayed simultaneously on the high-position camera's live video image.

Figure 10-11: High-Low Position Camera Linkage



A low-position camera's live view window supports the following operations:

- Drag the window border to move its position.
- Top-right toolbar: Zoom in/restore the window, close the window.
- Bottom-left toolbar: View the list of cameras associated with this low-position label, switch to 4-split window, switch to single window.

10.5 Add Label

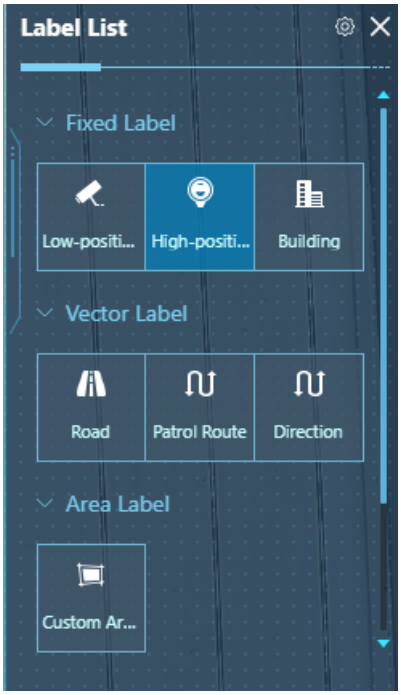
Supports overlaying various types of information - such as monitoring points, roads, and buildings—onto the high-position camera's live video in the form of labels on the AR live map screen, serving as monitoring aids.

10.5.1 Add Label

Add fixed labels, vector labels, area labels, and personalized labels to the AR live map.

Click the **Add Label** button at the bottom of the page to display the label list on the left.

Figure 10-12: Label List

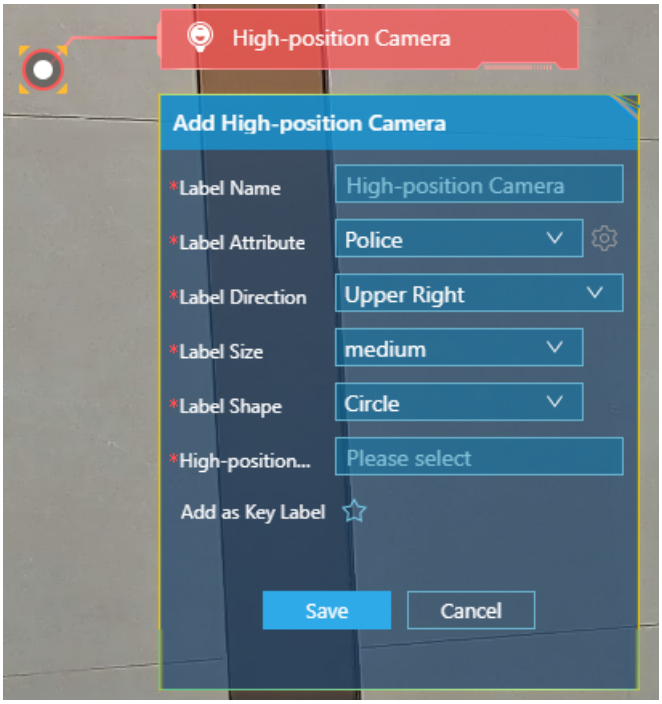


Fixed Label

Fixed labels include low-position cameras, high-position cameras, buildings, and custom labels. The addition method is similar for all. Here, adding a high-position camera label is used as an example:

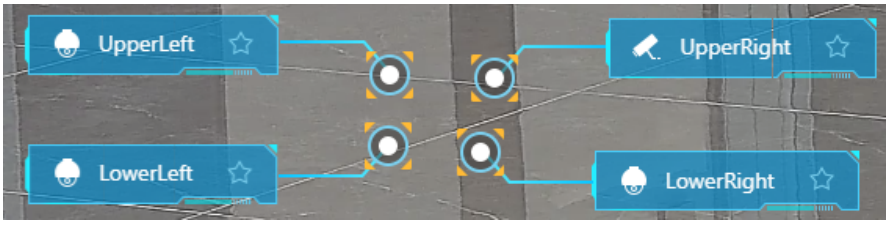
1. Select **High-Position Camera** from the label list.
2. Move the cursor to the map and click the location to be marked. The **Add High-position Camera** page pops up.

   Figure 10-13: Add High-Position Camera Label

3. Enter the label name and configure relevant parameters, then click **Save** to complete the addition.

Table 10-2: Fixed Label Parameters

Parameter	Description
Label Name	The name of the camera label. If left blank, it will be automatically populated with the camera's name.
High-Position Camera	Click to open the camera resource list. Select the camera and click **OK** to bind the corresponding camera to this label.
Label Attribute	• Click to expand the options and select a label attribute (e.g., Public Security Network / Police / Industry / Key Personnel / Surveillance Equipment / Public Area / Road Facility / Duty Post / Other). • Click to go to **Label Attribute Management** and add new label attributes.
Label Direction	The direction of the label, including: UpperRight / LowerRight / UpperLeft / LowerLeft. 
Label Size	The size of the label in the AR live map (Large, Medium, Small).
Label Shape	The shape of the label in the AR live map (Diamond, Circle, Hexagon, Rectangle).
Add as Key Label	Click to add this label to the key labels list.

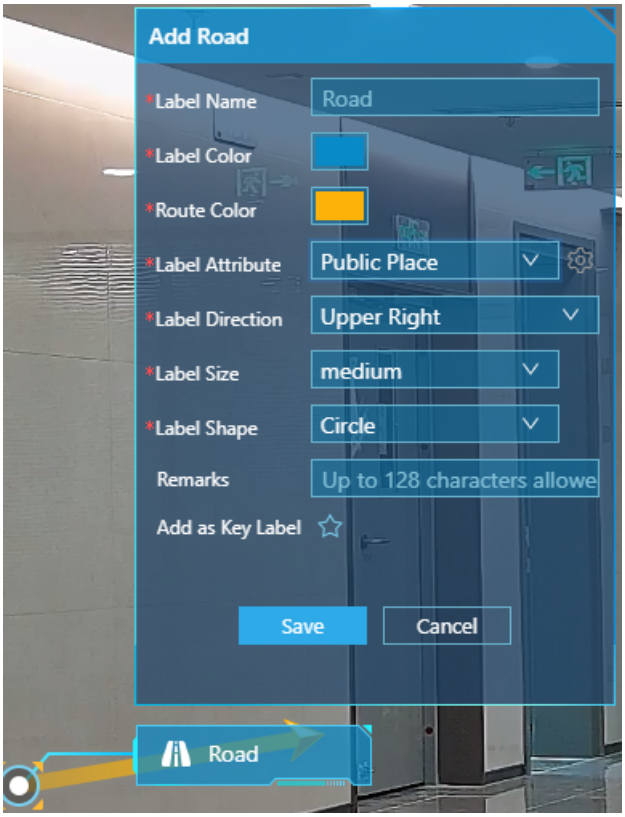
Vector Label

Vector labels include roads, security routes, directions, and custom labels. The addition methods are similar. Here, adding a road label is used as an example:

1. Select **Road** from the label list.
2. Move the cursor to the map. Click the location to be marked for the first time to set the starting point, then click again to set the endpoint. The **Add Road** page pops up.

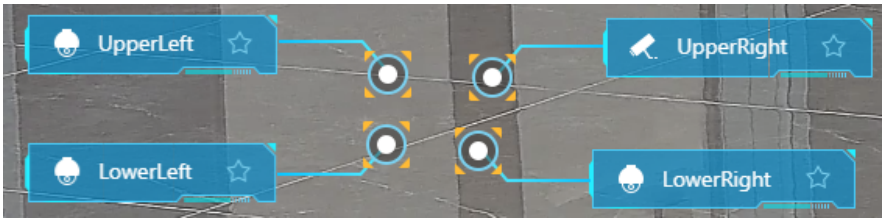
Note:
When adding a security route label, you can repeatedly click the left mouse button to plot the route, and click the right mouse button to end the plotting.

Figure 10-14: Add Road Label



3. Enter the label name and configure relevant parameters, then click **Save** to complete the addition.

Table 10-3: Vector Label Parameters

Parameter	Description
Label Name	Name of the label.
Label Color	Color of the label.
Route Color	Color of the label route.
Label Attribute	Attribute of the label. • Click to expand the options and select a label attribute (e.g., Public Security Network / Police / Industry / Key Personnel / Surveillance Equipment / Public Area / Road Facility / Duty Post / Other). • Click to go to **Label Attribute Management** and add new label attributes.
Label Direction	The direction of the label, including: UpperRight / LowerRight / UpperLeft / LowerLeft. 
Label Size	The size of the label in the AR live map (Large, Medium, Small).
Label Shape	The shape of the label in the AR live map (Diamond, Circle, Hexagon, Rectangle).
Remarks	Remarks related to the label.
Add as Key Label	Add the label to the key label management list.

Area Label

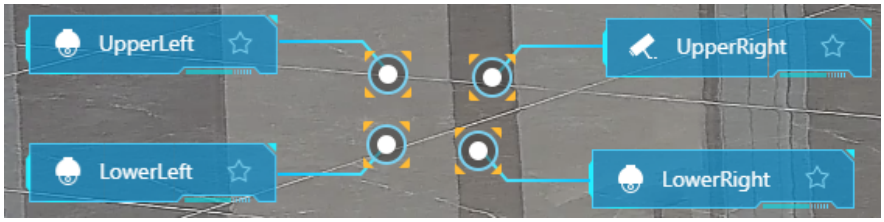
Area labels include custom areas and other custom labels. The addition methods are similar. Here, adding a custom area is used as an example:

1. Select **Custom Area** from the label list.
2. Move the cursor to the map. Left-click to select points for the area to define the shape, then right-click to finish drawing. The **Add Custom Area** page pops up.

Figure 10-15: Custom Area

3. Enter the label name and configure relevant parameters, then click **Save** to complete the addition.

Table 10-4: Custom Label Parameters

Parameter	Description
Label Name	Name of the label.
Label Color	Label colors include blue, red, pink, purple, green, orange, and gray.
Label Attribute	Attribute of the label. • Click to expand the options and select a label attribute (e.g., Public Security Network / Police / Industry / Key Personnel / Surveillance Equipment / Public Area / Road Facility / Duty Post / Other). • Click to go to **Label Attribute Management** and add new label attributes.
Label Direction	The direction of the label, including: UpperRight / LowerRight / UpperLeft / LowerLeft. 

Parameter	Description
Label Size	The size of the label in the AR live map (Large, Medium, Small).
Label Shape	The shape of the label in the AR live map (Diamond, Circle, Hexagon, Rectangle).
Fill	Fill color of the area.
Opacity	Transparency level of the area display.
Stroke	Line style of the area border, which can be set to solid or dashed, with configurable line thickness.
Remarks	Remarks related to the label.
Add as Key Label	Add the label to the key label management list.

Custom Label

Custom label types include third-party webpages and custom labels, which have similar addition methods. Here, using a third-party webpage as an example:

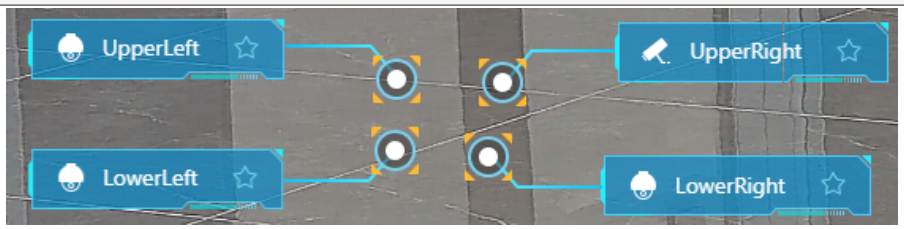
1. Select **Third-Party Webpage** from the label list.
2. Move the cursor to the map and click the location to be marked. The **Add Third-Party Webpage** page pops up.

Figure 10-16: Add Third-Party Webpage

3. Enter the label name and configure relevant parameters.

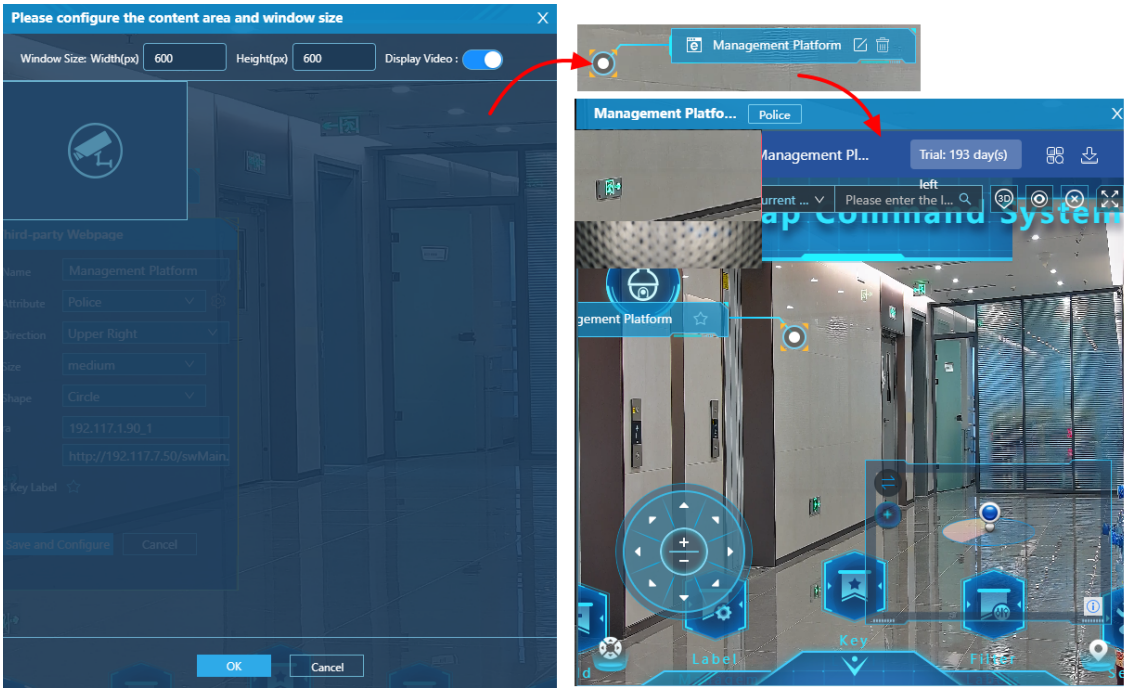
Table 10-5: Custom Label Parameters

Parameter	Description
Label Name	Name of the label.
Label Direction	The direction of the label, including: UpperRight / LowerRight / UpperLeft / LowerLeft.

Parameter	Description
	
Label Attribute	Attribute of the label. • Click to expand the options and select a label attribute (e.g., Public Security Network / Police / Industry / Key Personnel / Surveillance Equipment / Public Area / Road Facility / Duty Post / Other). • Click to go to **Label Attribute Management** and add new label attributes.
URL	Third-party webpage URL link.
Bind Camera	Click to open the camera resource list, select the camera, and click **OK** to bind the corresponding camera to this label.
Add as Key Label	Add the label to the key label management list.

4. Click **Save and Configure** to set the label size and choose whether to display video within the label area.
5. Click **OK** to save the settings.
   Clicking a web label in the AR live map will open the web address (the example shown in the diagram is the management platform) and overlay the camera's live video on the webpage.

Figure 10-17: Third-Party Webpage Configuration and Display Effect



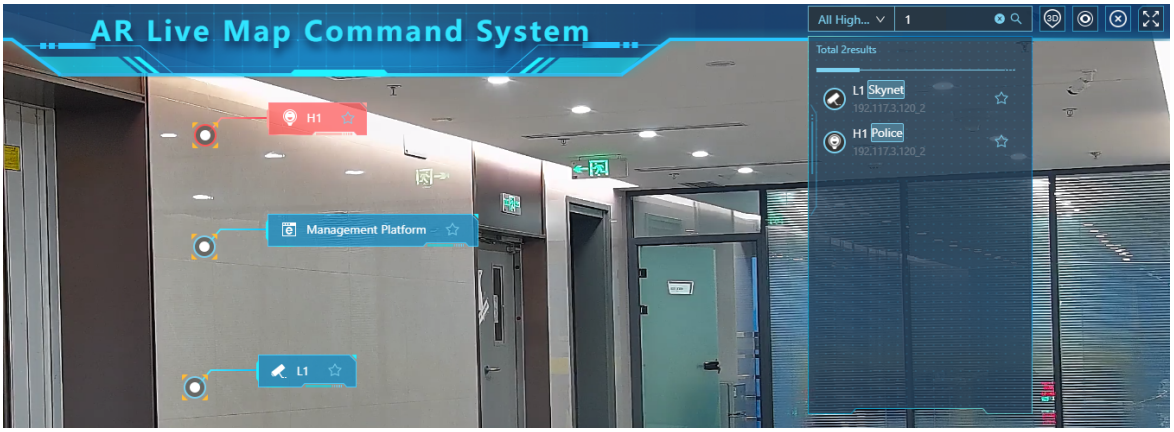
10.5.2 Label Operations

Supports modifying, deleting, hiding, and other operations on labels.

Search Labels

Enter keywords in the upper-right corner of the page to search for labels under the current high-position camera or all high-position cameras. Clicking a label will jump to the camera view where the label is located and highlight it on the image.

Figure 10-18: Keyword Search



Manage Labels

Click **Add Label** to enter label editing mode, where the following operations can be performed:

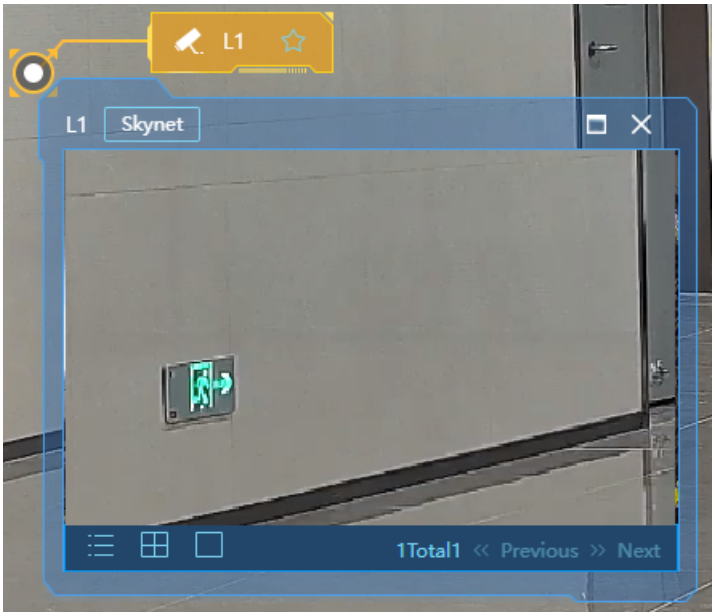
- Move label: Vector labels and area labels cannot be moved after being added. Other labels can be dragged to change their position.
- Modify label: Click corresponding to a label to modify its parameters.
- Delete label: Click corresponding to a label to delete it.

View Labels

Exit label editing mode. Click the label name to view label details or the camera's live video.

- For low-position camera labels, clicking the label name will open the live video of that camera.

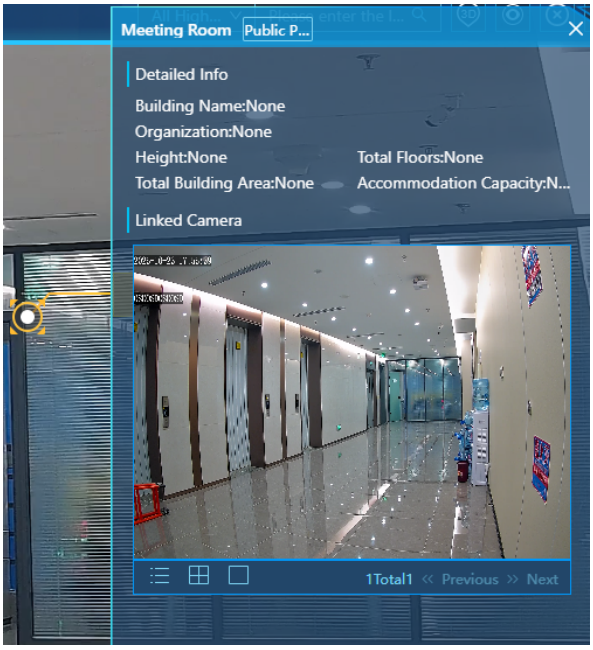
  Figure 10-19: Low-Position Camera Label Details

  Note:
  A maximum of 5 label live videos can be displayed simultaneously in the high-position camera view.

- For high-position camera labels, clicking the label name will switch to the AR live view of that high-position camera.
- For building labels, clicking the label name will display label details and open the live video of the associated camera.

Figure 10-20: Building Label Details



- For third-party webpage labels, clicking the label name will open the third-party webpage and play the live video of the associated camera.
- For other types of labels, clicking the label name will display label details, etc. Specific behaviors are subject to the screen display.

Hide Label Names

Exit label editing mode, supports showing or hiding label names for a clearer view of label information.

- Click of a label to hide its name. Click again to restore the display.
- Click in the upper-right corner to hide all label names. Click again to restore the display.

10.6 Label Management

Centrally manage labels, supporting operations such as editing and deleting.

Click **Label Management** at the bottom of the page. The **Label Management** list will appear on the left side, allowing you to view and manage all labels.

Figure 10-21: Label Management

- Click a label to go to the high-position camera view where the label is located.
- Search: Select either the current high-position camera or all high-position cameras, then enter keywords to search for labels.
- Edit: Click next to a label and select **Edit** to modify its content.
- Delete: Click next to a label and select **Delete** to delete the label.

10.7 Key Label

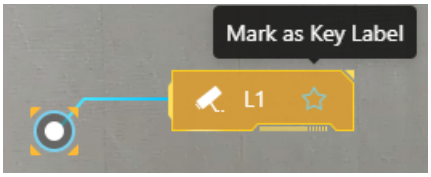
Manage key labels of focus. Clicking a label quickly navigates to its location.

Add Key Label

Three methods are supported for adding labels to key labels:

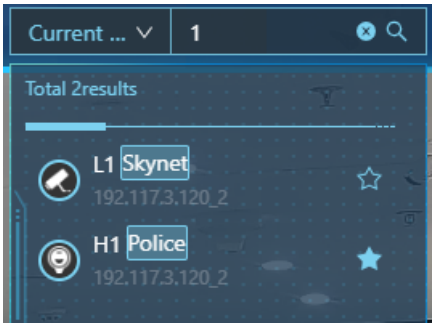
- In the AR live map, click the on a label to add it to the key label list under the corresponding label category.

  Figure 10-22: Mark as Key Label

- In the upper-right corner of the AR live map page, enter keywords to search for a label, then click the corresponding to add the label to the key label list under the corresponding label category.

Figure 10-23: Add to Key Label



- When adding a new label, set it as a key label. For details, see Add Label.

Key Label List

Click **Key Label** at the bottom of the page to display the **Key Label** list on the left side of the page, showing all key labels in the system.

Figure 10-24: Key Label List

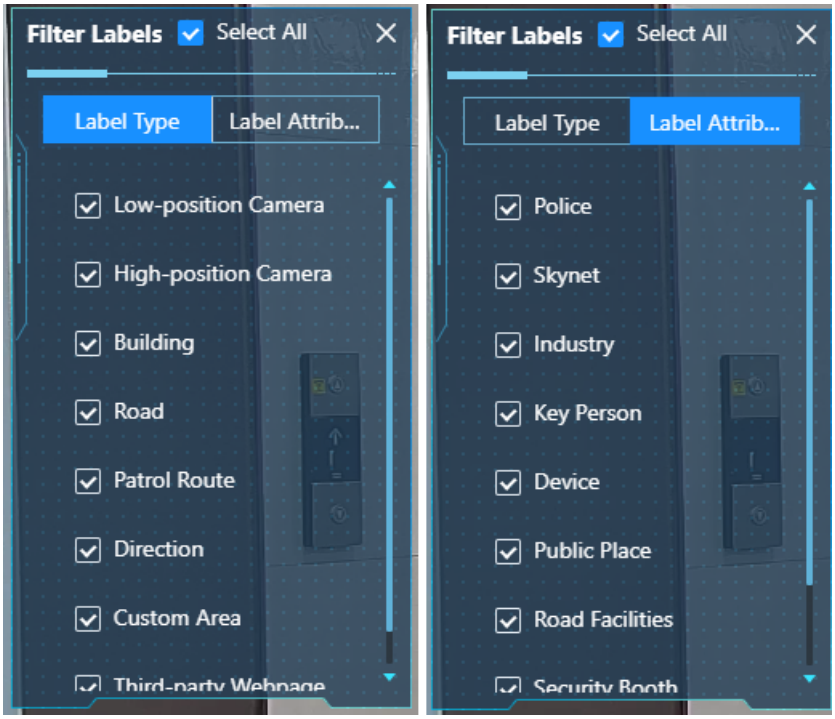
- Filter key labels: Supports filtering key labels of all high-position cameras or key labels in the current high-position camera; supports keyword search.
- In the key label list, select a label. If the label is not in the current field of view, the camera will automatically move to the label's position.
- Delete key label: Click after a label to remove it from the key label list.

10.8 Filter Labels

Filter labels by type or attribute for convenient viewing of desired labels.

1. Click **Filter Labels** at the bottom of the page to display the **Filter Labels** list on the left side.
2. Select the desired label types or attributes, and only the selected labels will be shown in the live view.

Figure 10-25: Filter Labels

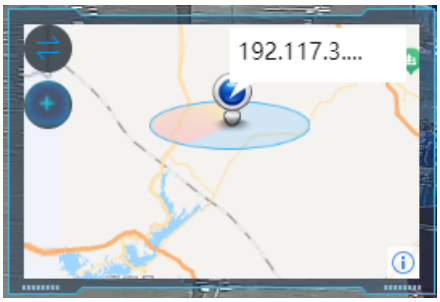


10.9 Map Display

View the current high-position camera's location on the map.

Click in the lower-right corner of the page to open the 2D map.

Figure 10-26: Map Display



- The point indicated by the blue icon represents the current high-position camera. Double-click other high-position cameras on the map to switch to the AR live view of the corresponding camera.
- Switch map / live view: Click to toggle between the map view and the live view.

Figure 10-27: Map View

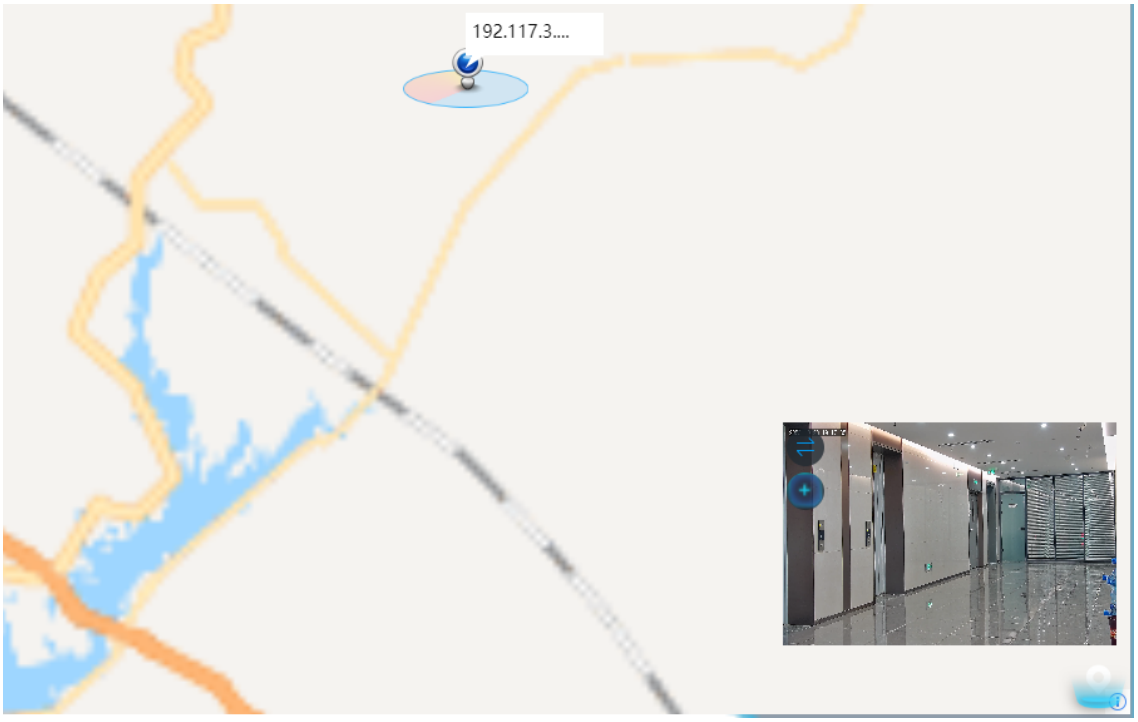


Figure 10-28: Live View

- Zoom in/out on the floating panel in the lower right: Click **+** to zoom in; click **-** to zoom out.

Figure 10-29: Zoom In on Live View Floating Panel

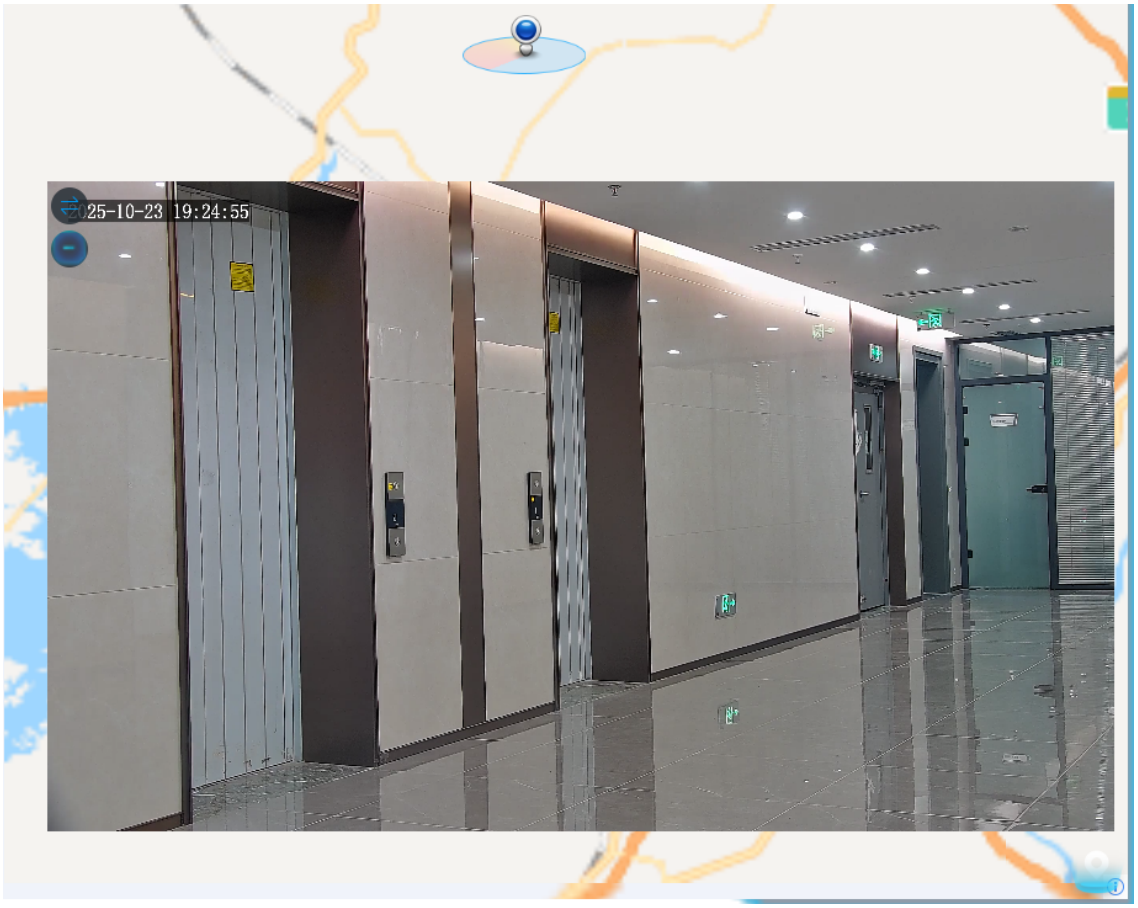


Figure 10-30: Zoom In on Map Floating Panel

- Place the mouse over the map, hold down the left mouse button to drag and view the map, and scroll the mouse wheel to zoom the map in or out.

10.10 PTZ Control

If the high-position camera is a PTZ camera, PTZ control is supported.

Note:
VSS cross-domain cameras do not support the PTZ control function.

- Click the in the lower right corner of the page to open the PTZ control panel (click again to hide it). Direction arrows such as and can be used to adjust the PTZ orientation, while and can adjust the camera's focal length to zoom the picture in or out.

  Figure 10-31: PTZ Control Panel

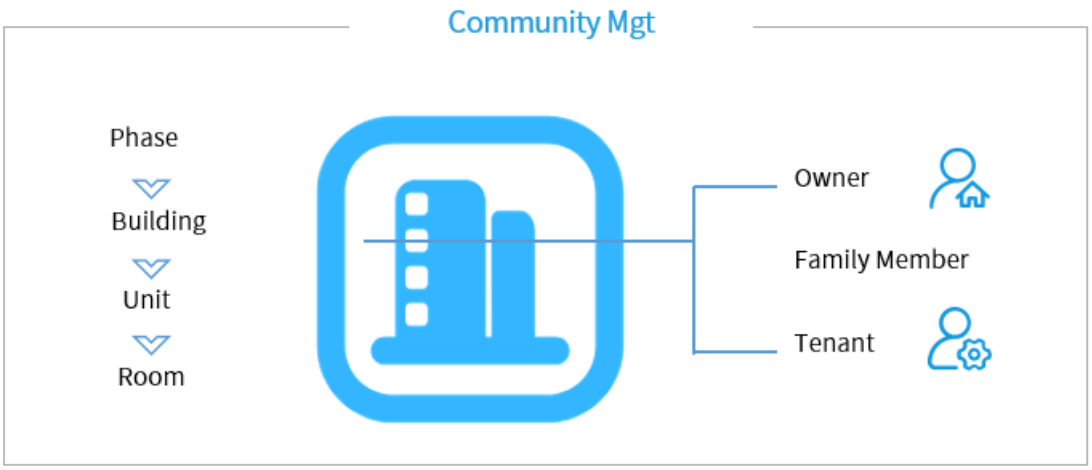
- Click the direction arrows , , , around the AR live view to adjust the PTZ orientation.
- In the live view, scroll the mouse wheel to zoom the picture in or out.
- Click the in the upper left corner of the page to enable the 3D positioning function (click again to disable it).
  - Click to locate: Click any point in the picture, and the PTZ camera will rotate to center on that location.
  - Drag to Zoom: Hold down the left mouse button and drag a box in the picture. Drag from top-left to bottom-right to zoom in; drag from bottom-right to top-left to zoom out.

  Note:
  If 3D positioning is not activated, you can also hold down Ctrl + left mouse button to drag a box for zooming.

11 Room Management

Go to **Basic Config > Community Mgt**.

Manage the information of rooms and residents in the community. By establishing a community information file, you can quickly learn about the rooms and residents in the community and improve the efficiency of community management.

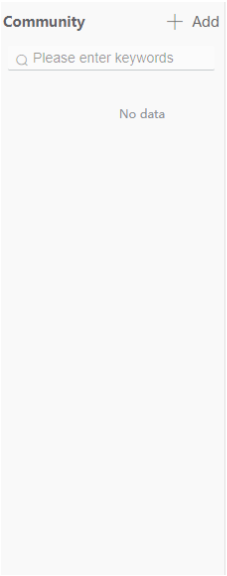


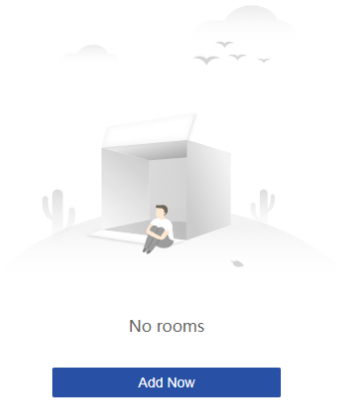
- Community Room Management: Add phases/buildings/units/rooms to the community according to the actual occupancy situation. You can also edit or delete community information here.
- Resident Management: Associate residents with rooms based on their occupancy status (owner/family member/tenant).

11.1 Community Room Management

Add phases/buildings/units/rooms to the community according to the actual occupancy situation. You can also edit or delete community information here.

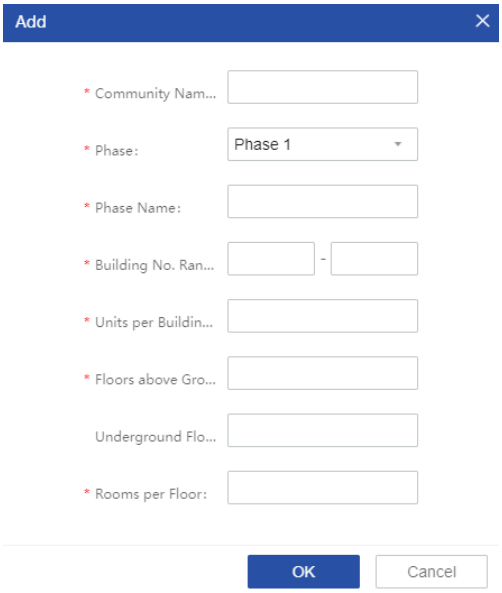
Go to **Basic Config > Room Mgt**.





11.1.1 Add Room

1. Click **Add Now**. A page as shown below appears.



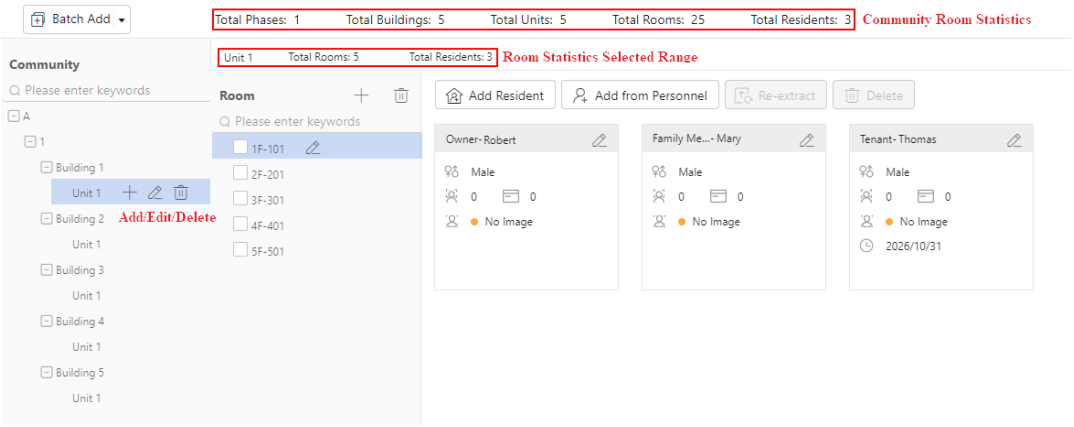
2. Enter the community name, phase(1-20), phase name, building number range (1-99), units per building (1-99), floors above ground (1-99), underground floors (0-99) and rooms per floor (1-99).

   Note: Up to 5000 rooms can be added in total.

3. Click **OK**.

11.1.2 Manage Room

View the added rooms in the room list.



- Community room statistics: View the total number of phases, buildings, units, rooms, and residents in the community.
- Room statistics in selected range: View the total number of rooms and residents within the selected phase/building/unit.
- Edit name: Hover the mouse over a community/phase/building/unit/room name, and click to edit the name.
- Add phase: Hover the mouse over a community and click to add a phase and its subordinate level within the community.
- Add building: Hover the mouse over a phase and click to add a building and its subordinate level within the phase.
- Add unit: Hover the mouse over a building and click to add a unit and its subordinate level within the building.
- Add room: Hover the mouse over a unit and click to add a floor and a room within the unit.
- Delete community/phase/building/unit: Hover the mouse over a community/phase/building/unit and click to delete it.
- Delete room: Select room(s), click , and then confirm to delete the selected room(s).

Note:
Deleting a room will remove the room information of personnel associated with it, but it will not delete the personnel themselves.

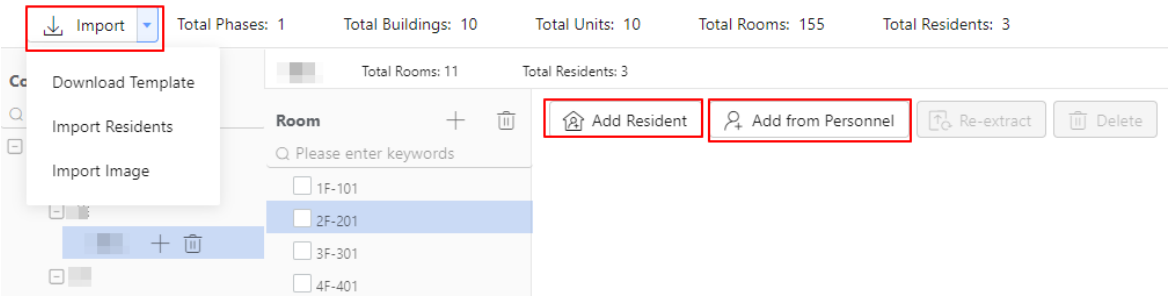
11.2 Resident Management

Associate residents with rooms based on their occupancy status (owner/family member/tenant).

Note:

- Each room can be associated with up to 10 residents, with only one resident can be specified as the owner.
- A person can be associated with multiple rooms (no upper limit) and can be an owner, a family member, or a tenant in different rooms simultaneously. However, a resident cannot be associated with a room using different identities.

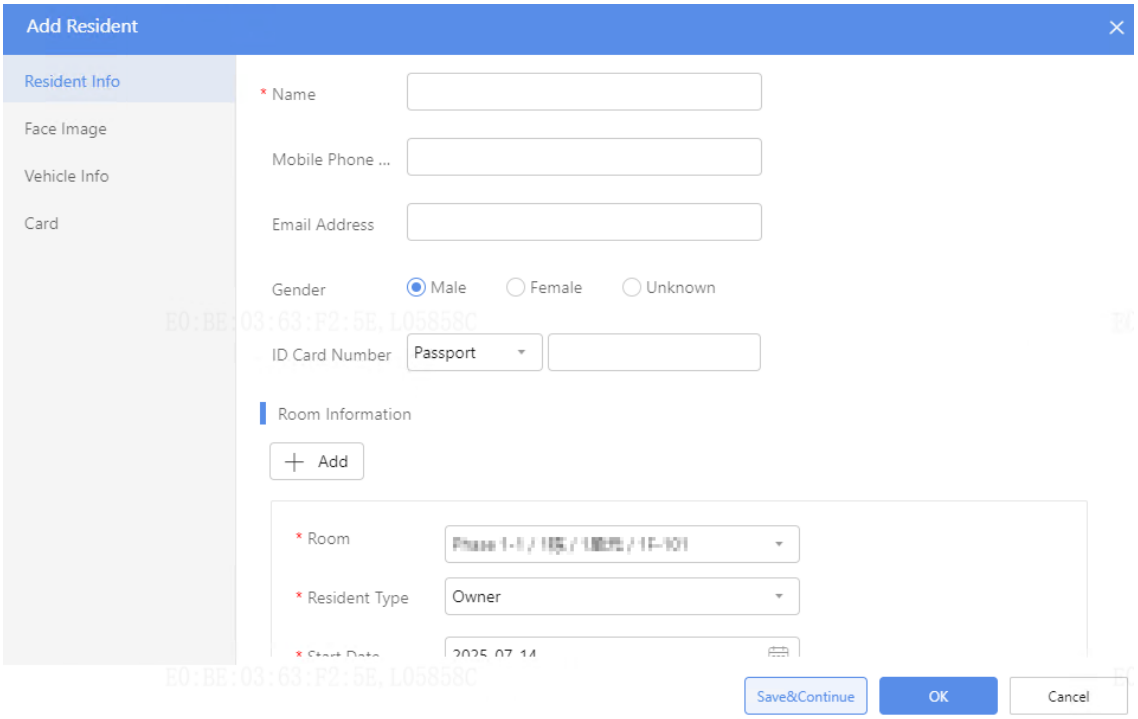
You can add residents using any of the following 3 methods.



11.2.1 Add Manually

You can enroll resident information, including identity information, room information, face image, vehicle information, and card.

1. Select a room and click **Add Resident**. A page as shown below appears.



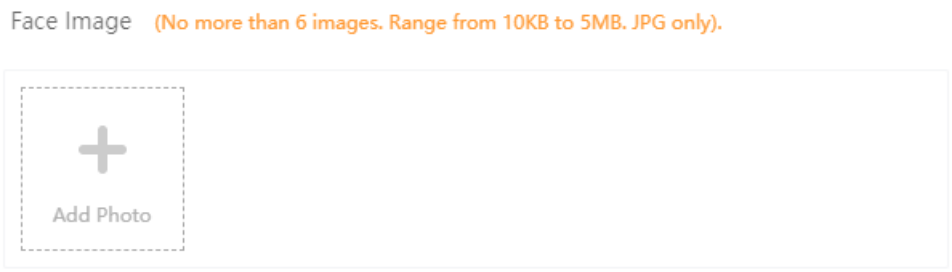
2. Complete the resident information.

Item	Description
Identity Info	Name (required), mobile phone number, email address, ID number (choose the ID type from the list, and then input the ID number), and gender.
Room Info	• Room: Select a specific room. • Resident type: Owner, family member, and tenant. • Start date: Cannot be earlier than the current time. • Expiration date: Cannot be earlier than the start date. Required for tenants; optional for owners and family members. No expiration date selected means permanently valid. If the resident has multiple rooms, you can click **Add** to add more room information.

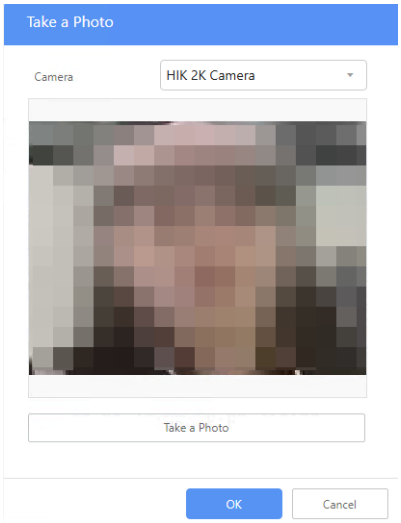
3. (Optional) Upload the resident's face images.

Note:
Image verification is enabled by default. To disable it, see Face Image Verification.

Click **Add Photo**. Choose a way to add photos:



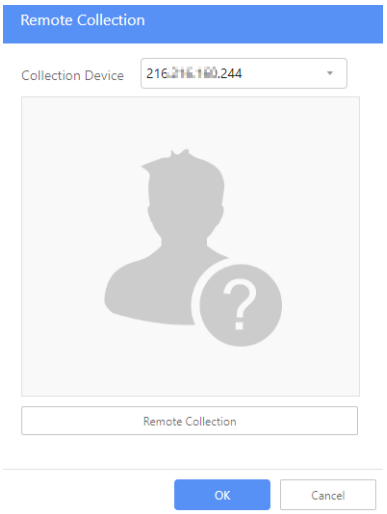
- Upload: Select a photo of the person from the PC and upload it.
- Take a photo: Select a camera to view its real-time screen on the PC. Click **Take a Photo** to capture the current frame. Click **OK** to save the photo, or click **Retry** to take another one.



Note:

- Please first enable HTTPS and log in via the HTTPS protocol before taking photos.
- The camera device supports USB cameras and the built-in camera of the computer. If you are using a USB camera, connect it to the PC in advance.

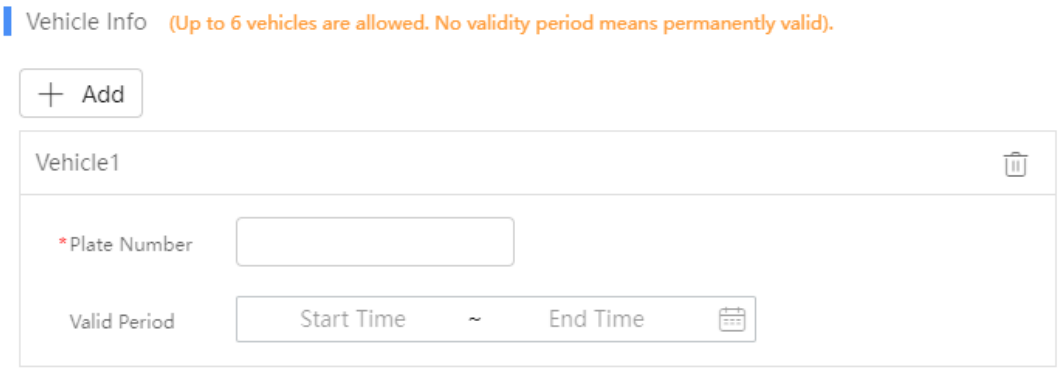
- Remote collection: Select a face recognition access control device and click **Remote Collection**. After the device completes face collection, you can check the collected photo on the client. Click **Re-Collect** if necessary, or click **OK** to complete the collection.



Note:
Only some access control devices support remote collection.

4. (Optional) Add the person's vehicle information. Up to 6 vehicles are allowed per person.

   (1) On the **Vehicle Info** tab, click **Add**.

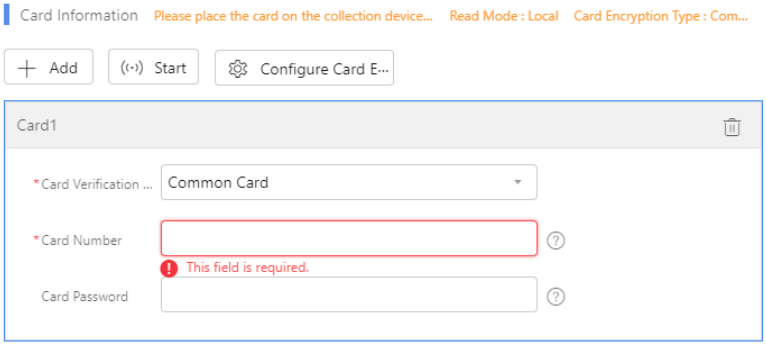


(2) Enter the license plate number and select a validity period.

Note:
Vehicles added/edited/deleted here will be automatically synced to **Parking Mgt** > Authorized Vehicle. To sync vehicles to devices, see operations in Vehicle Data Sync. Only vehicles within the validity period can access the gates at the entrance and exit.

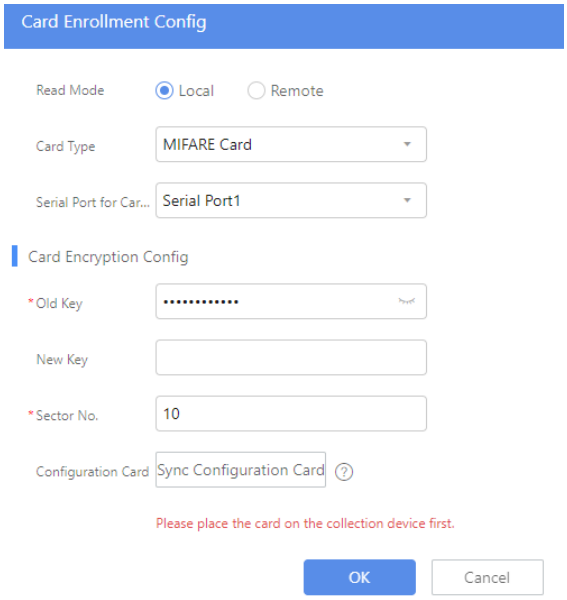
5. (Optional) Add card information.

(1) Go to the **Card** tab.



(2) Click **Configure Card Enrollment**, and configure parameters as needed. (It only needs to be configured once and card information can be then read for multiple people.)

Read Mode	Description	
Local	Connect the card enroller to the PC's port, and then place the card on the enroller to read/enroll it. **Note:** On the PC, right-click **Computer**, select **Manage> Device Manager > Ports (COM & LPT)**, and check for the **USB Serial Device (COMX)**, where **X** is the serial port number.	
	Common Card	Common card supports card reading only. 1. Connect the card enroller to the PC's port. 2. Select the card enroller model: (O)EC-W1D-EMC or (O)EC-W2D-M. 3. To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click **Sync Configuration Card**, and then swipe it on the general access control device/access controller. **Note:** The configuration card is used to send the common card information to the general access control device/access controller.

Read Mode	Description	
	MIFARE Card	MIFARE card supports card reading and enrollment. And you can also encrypt sectors to prevent from data leakage.  1. Connect the card enroller to the PC's port. **Note:** Only (O)EC-W2D-M supports reading the MIFARE card. So you don't need to select the card enroller model. 2. Card encryption configuration: Enter the card's old key and sector number to encrypt the specified sector. To change the key, please enter the new key. 3. To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click **Sync Configuration Card**, and then swipe it on the general access control device/access controller. **Note:** The configuration card is used to send the encryption card information to the general access control device/access controller.
Remote	Select an access control device as collection device, and then swipe a card on it to read the card. **Note:** This feature is only available to certain access control devices. Please refer to the actual interface.	

(3) Click **Add** to add cards.

Note:
Up to 8 cards can be added. The number of cards supported may vary with device; if the device's capacity is less than the number of cards an individual has, only a portion of the cards can be synced successfully.

Parameter	Description
Card Verification Type	• Common Card: Can open doors with access permissions normally without triggering an alarm. • Duress Card: Can open doors with access permissions normally while simultaneously triggering a duress alarm.
Card Number	Read or enroll the card.

Parameter	Description
	Note: Preparation: (Local)Place the card on the card enroller; (Remote)Swipe the card on the access control device. • Read card: Click **Start** to read the card. • Enroll card (only when the MIFARE card is read locally): Enter the card number manually and then click **Start**; or, click **Start** to read the physical card number.
Card Password	Only cards for general access control devices need to be configured with a card password. **Card Password** is hidden by default. You can enable it in Function Switch.

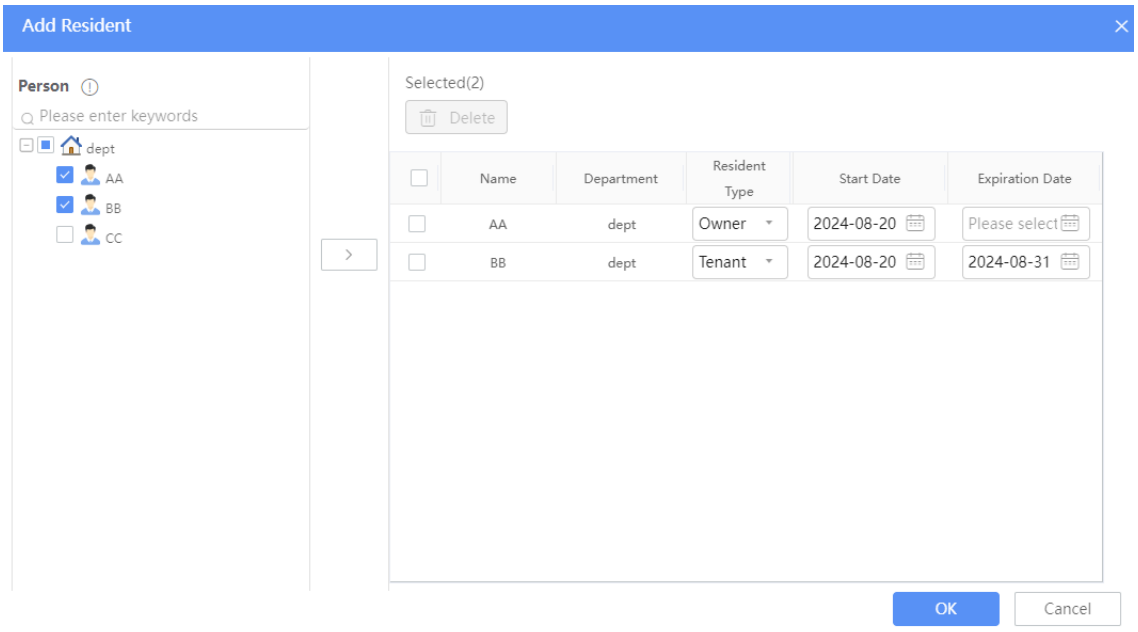
6. Click **OK** to finish or click **Save&Continue** to add more resident information.

11.2.2 Add from Personnel

Select persons from Person Library and add them as residents.

1. Select a room and click **Add from Personnel**. An **Add Resident** page appears.
2. Select residents from the left person list and click » to add them to the selected list.

Note:
Up to 200 people can be displayed for each department. People not displayed can be found by search, with up to 200 displayed.



3. Select the resident type, start date, and expiration date for each person.

Note:
- Start date: Cannot be earlier than the current time.
- Expiration date: Cannot be earlier than the start date. Required for tenants; optional for owners/family members. No expiration date selected means permanently valid.
- Modifying the start/expiration date will be automatically synced to the person's Validity Period, while modifying the person's validity period not affect start/expiration date.

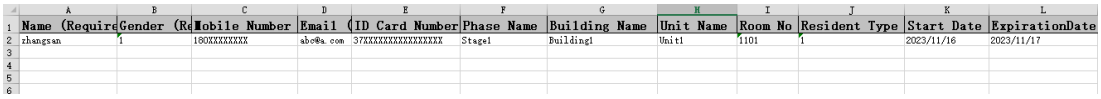
4. Click **OK**.

11.2.3 Add in Batches

Import residents in batches using a template.

1. Prepare a template.

   (1) Click the drop-down arrow next to **Import** and select **Download Template**.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Name (Require	Gender (Re	Mobile Number	Email (	ID Card Number	Phase Name	Building Name	Unit Name	Room No	Resident Type	Start Date	ExpirationDate
2	zhangsan	1	180XXXXXXXX	abc@a.com	37XXXXXXXXXXXXXXXX	Stage1	Building1	Unit1	1101	1	2023/11/16	2023/11/17
3												
4												
5												
6												

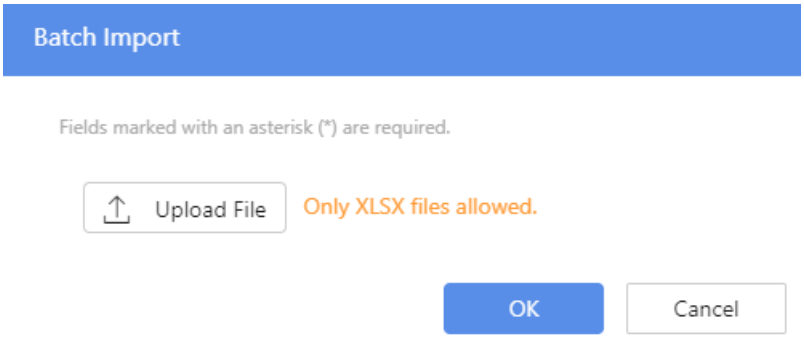
   (2) Complete the resident information in the template and save it.

   (3) Name the resident images based on this format: *Mobile Phone Number_No.*.jpg (e.g. 123456_3.jpg). Up to 6 images are allowed per resident. And then package all images into a .zip format file.

2. Import the template.

   (1) Click the drop-down arrow next to **Import** and select **Import Residents**.

   (2) Click **Upload File** and select the modified template file from local.



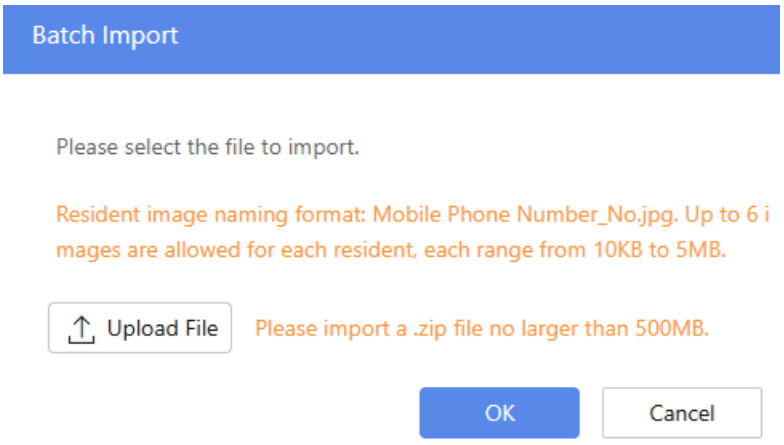
   (3) Click **OK**.

   Note: If the import failed, please modify the content according to the error message.

3. Import images.

   (1) Click the drop-down arrow next to **Import** and select **Import Image**.

   (2) Click **Upload File** and select the prepared compressed package (.zip) from local.

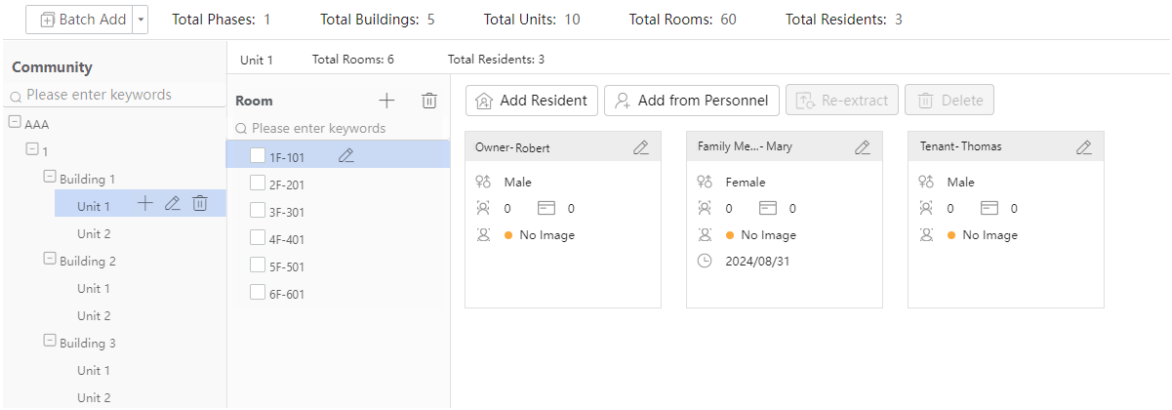


   (3) Click **OK**.

   Note: If the import failed, please modify the content according to the error message.

11.2.4 Manage Resident

Select a room to view the residents under it. The displayed resident information includes resident type, name, gender, mobile phone number, number of images, image feature extraction status, number of cards, and the expiration date.



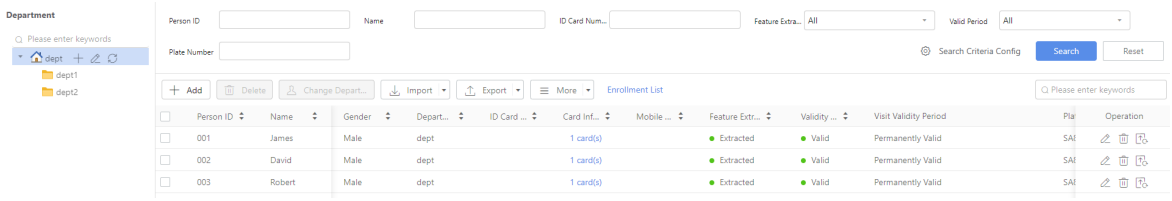
- Unlink: Select a resident and click **Delete** to remove the resident from the room.
- Edit: Click in the card's upper-right corner to modify the resident information.
- Re-extract: Select a resident and click **Re-extract** to re-extract the feature from the resident image.

12 Personnel Management

Go to **Basic Config > Personnel Mgt**.

You can manage long-term residents within the area, such as company employees, residential community inhabitants, school faculty and students, allowing functions like access control permissions management and attendance management.

- Department Management: Create departments according to the actual organization structure to manage personnel in different groups.
- Personnel Management: Add person information to departments one by one or in batches, including the basic information, room information, face image, vehicle information, card, fingerprint, Custom Attribute, etc.



12.1 Department Management

You can create departments according to the actual organization structure to manage personnel in different groups.

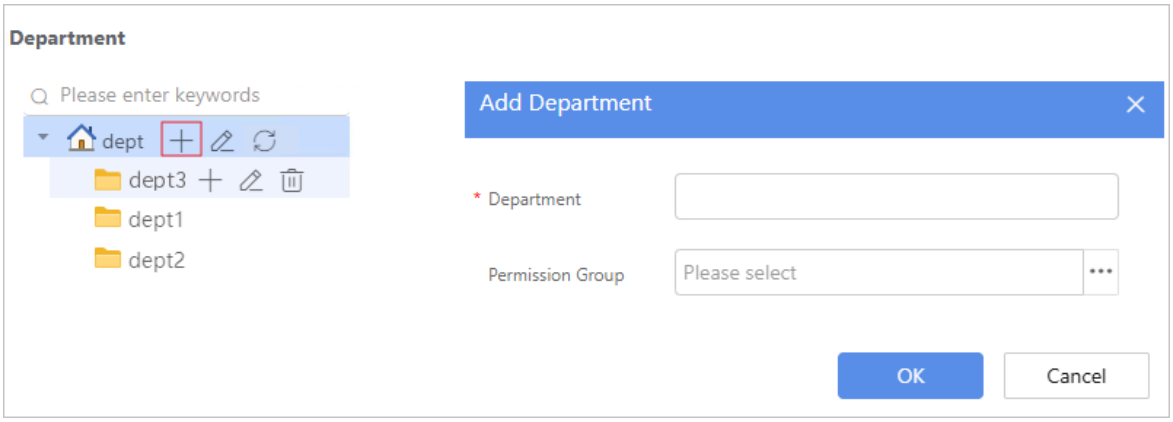
By default, there is a root department which cannot be deleted, but can be renamed. New departments are added under the root departments.

Note: Up to 10 levels of departments are allowed.

Add a Department

Click + for the department, input the department name, select permission groups and then click **OK**, a sub-department will be added.

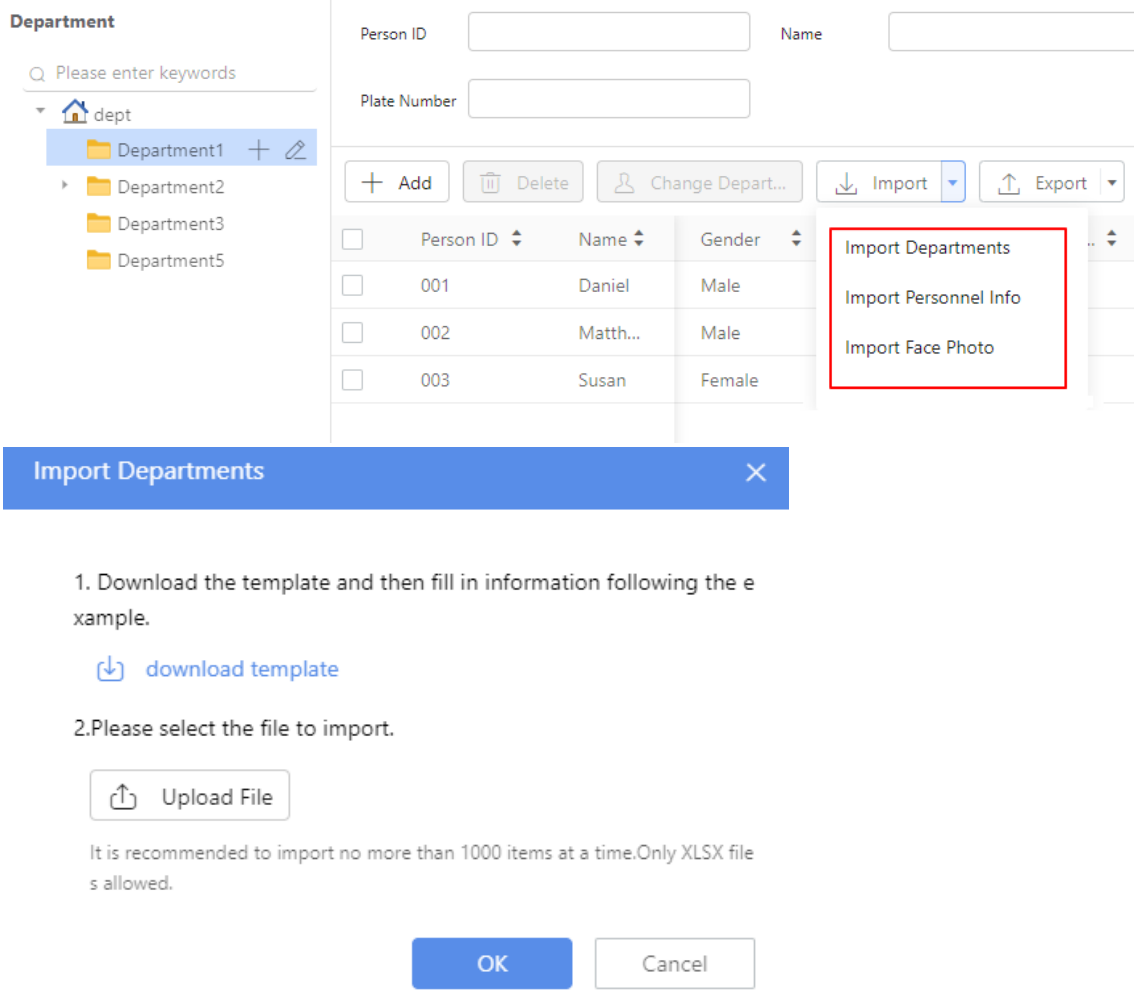
Note:
After binding a permission group to a department, personnel subsequently added to the department will automatically be granted the corresponding permissions.



Import Departments

Import departments in batches using template.

1. Click **Import**, select **Import Departments**, download the spreadsheet template.



2. Fill in the departments to be imported in the template. Fields marked with an asterisk (*) are mandatory.

   Note:
   It is recommended to import no more than 1000 entries at a time, otherwise the import may be very slow.

3. Click Upload File, upload the completed template.
4. Click **OK** to complete the import.

Rename Department

Click for the department to change its name. After editing, click **OK** to save it.

Delete Department

Click for the department to delete it.

Note: Cannot delete the root department and departments containing sub-departments or person.

Refresh Department

If a department was modified on another client, the department information displayed on this page may not update automatically. Please click next to the root department name to refresh manually.

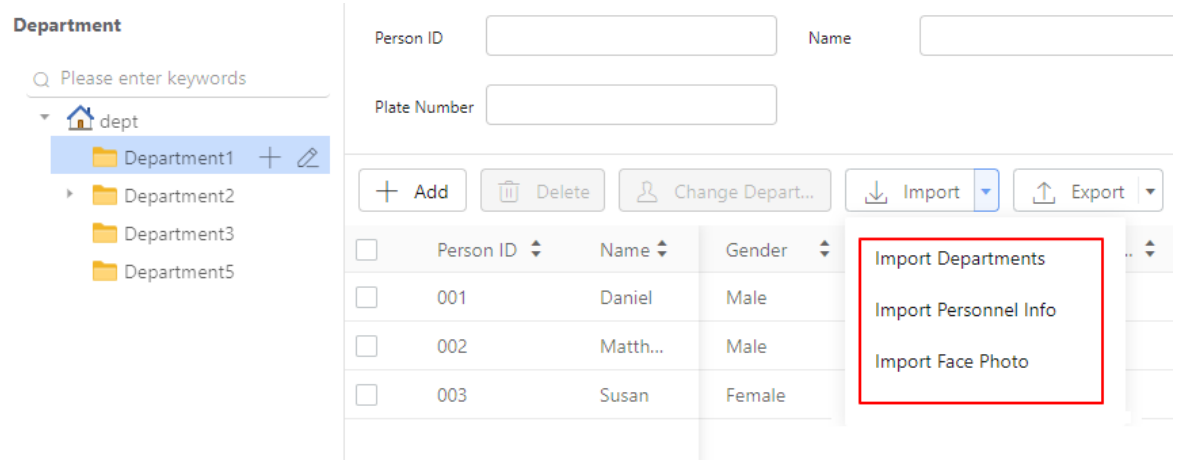
12.2 Add Person

Add person information to departments one by one or in batches, including the basic information, room information, face image, vehicle information, card, fingerprint, Custom Attribute, etc.

Note:
Residents added in Resident Management will be automatically synced to the root department.

12.2.1 Add in Batches

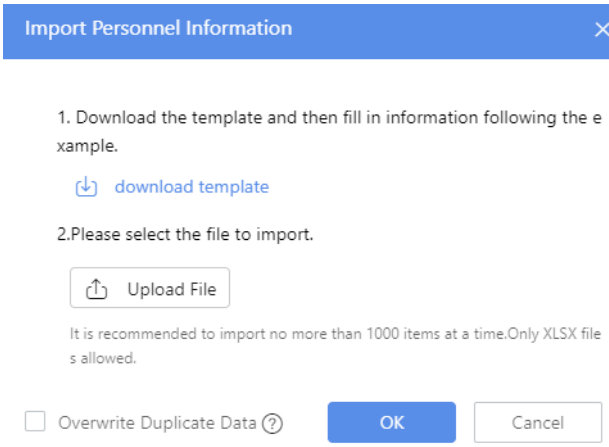
Import personnel information and face photos in batches.



Import Personnel Information

Import personnel information in batches through templates.

1. Click **Import**, select **Import Personnel Info**, download the spreadsheet template.



2. In the template, enter the person information that you want to import. Fields marked with an asterisk (*) are required.

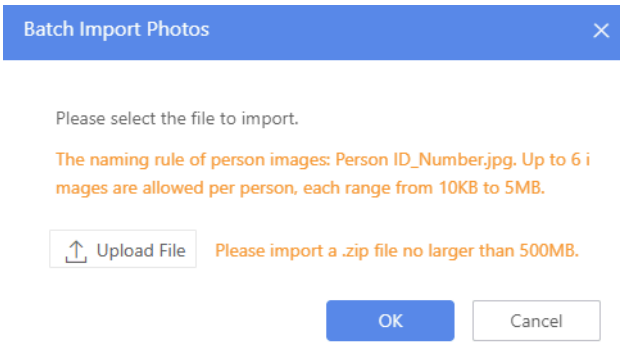
Note:
It is recommended to import no more than 1000 entries at a time, otherwise the import may be very slow.

3. In the **Batch Import** dialog box, click **Upload File** to select the file.
4. (Optional) Select **Overwrite Duplicate Data**. When an employee ID already exists, the corresponding employee's information will be overwritten and updated.
   If not selected, the import will fail if the imported employee ID duplicates an existing employee ID.
5. Click **OK**.

Import Face Photos

Batch import face photos using a .ZIP file.

1. Name the photos as *Person ID_No.*.jpg. Up to 6 photos are allowed per person. And then pack all photos into a .ZIP file.
2. Select a target department from the left-side department tree, and then click **Import** > **Import Face Photo**.
3. Click **Upload File** to upload the ZIP file.

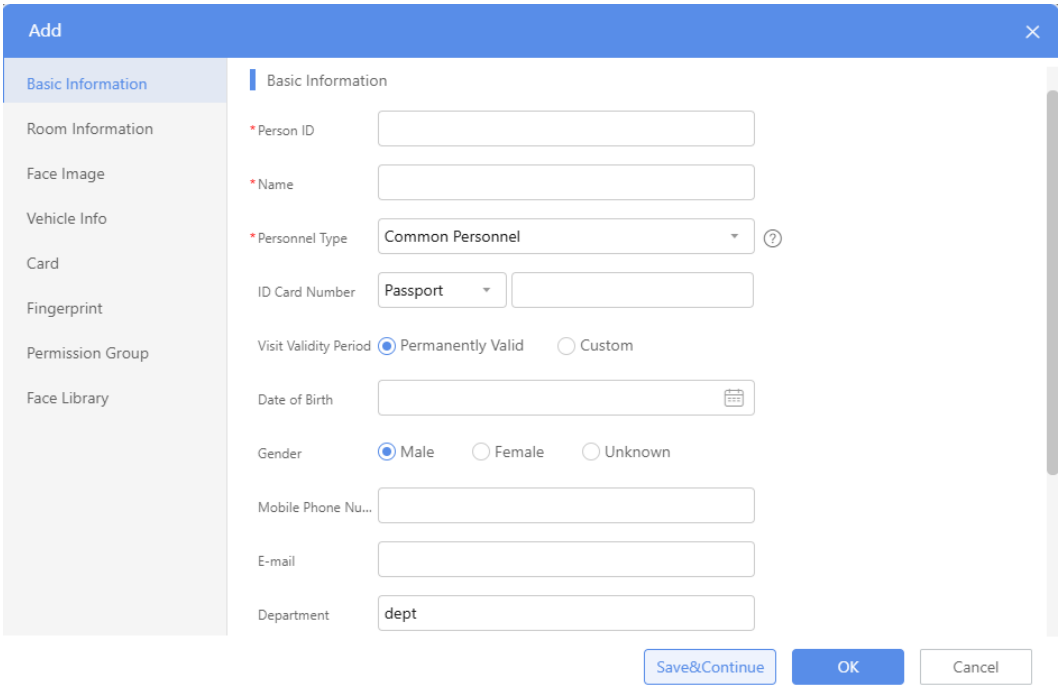


4. Click **OK**.

12.2.2 Add One by One

Select the target department from the left-side department tree, and click **Add**. Enroll the person's basic information, room information, face image, vehicle information, card, fingerprint, etc., set access permissions, add persons to the face library, and then click **OK** or click **Save&Continue** to add more people information.

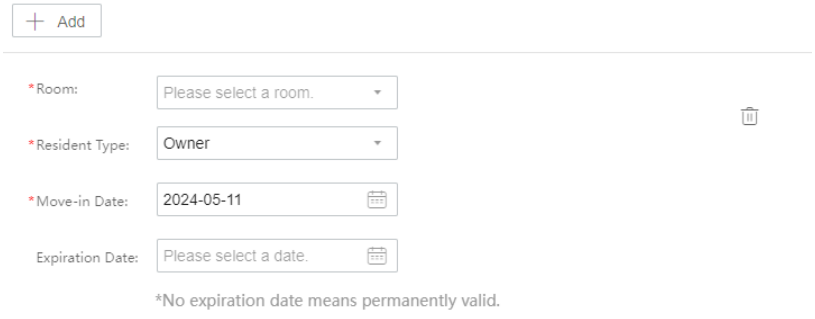
Basic Information



Parameters	Description
Identity Information	Enter the person ID (letters/digits/underscores/hyphens), name and other information as needed.
Personnel Type	• Common Personnel: Access permissions are determined by their permission groups and verification rules. • Super Personnel **(applies only to access controllers)**: Can access doors they have permission for, bypassing restrictions like keep closed, anti-passback, interlocking (excluding multi-factor authentication); verification will fail for doors that they have no permission. • Unauthorized Personnel **(applies only to access controllers)**: Cannot access any door. Verification attempts on a door they have permission for will not unlock the door but will trigger an unauthorized access alarm; verification will fail for doors that they have no permission.
ID Card Number	Select the ID type from the list, and then input the ID number.
Visit Validity Period	The visitor can access with card, face recognition, or password only within the set period. • Only within the validity period can the credentials (face, card, password, etc.) be successfully verified on authorized access control devices. • After the validity period expires, even if the visitor has access permission, verification will not succeed. If the access control device is also used for recording attendance, no attendance records will be generated (except pass-thru records). **Note:** You can choose Permanently Valid, 1 Day, 7 Days, 30 Days or Custom. When custom validity period, the earliest start time of the visit validity period is 00:00 on the current day, the latest end time must be later than the start time.
Extend Door Opening Time	**(Applies only to access controllers)** Upon successful verification on a door with access permission, the door opening time is three times the door opening time set on the access controller, facilitating the passage of people with mobility impairments.
Door Opening Password	Door opening passwords can be generated automatically or entered manually. After a door opening password is set, the person can use the password to access specified doors configured in Access Permission Config.
Others	Configure Custom Attribute as needed.

(Optional) Room Information

1. Click **Add** in Room Information.
2. Then complete the information. Rooms are created in Room Management.

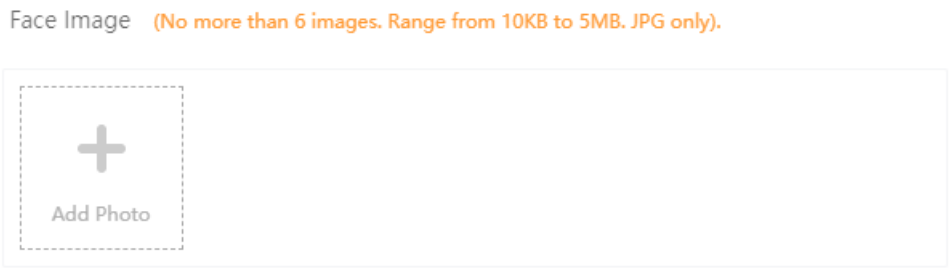


Note:
Modifying the move-in/expiration date will be automatically synced to the person's Validity Period, while modifying the person's validity period not affect move-in/expiration date.

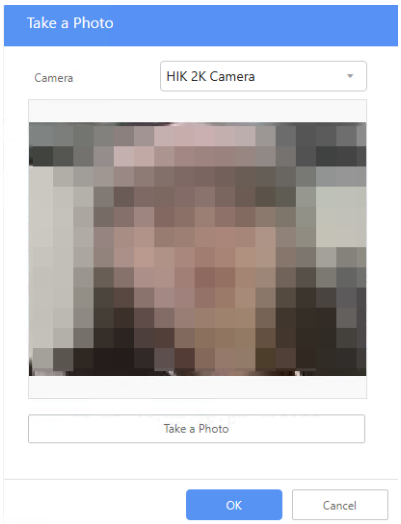
(Optional) Face Image

Note:
Image verification is enabled by default. To disable it, see Face Image Verification.

Click **Add Photo**. Choose a way to add photos:



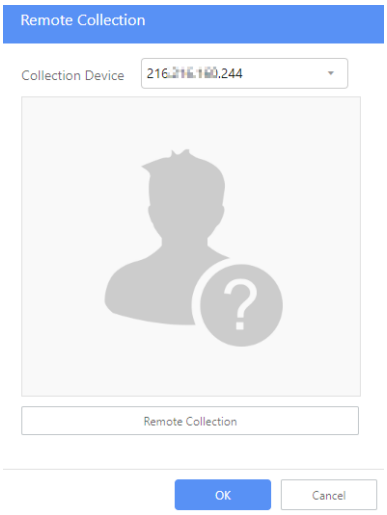
- Upload: Select a photo of the person from the PC and upload it.
- Take a photo: Select a camera to view its real-time screen on the PC. Click **Take a Photo** to capture the current frame. Click **OK** to save the photo, or click **Retry** to take another one.



Note:

- Please first enable HTTPS and log in via the HTTPS protocol before taking photos.
- The camera device supports USB cameras and the built-in camera of the computer. If you are using a USB camera, connect it to the PC in advance.

- Remote collection: Select a face recognition access control device and click **Remote Collection**. After the device completes face collection, you can check the collected photo on the client. Click **Re-Collect** if necessary, or click **OK** to complete the collection.



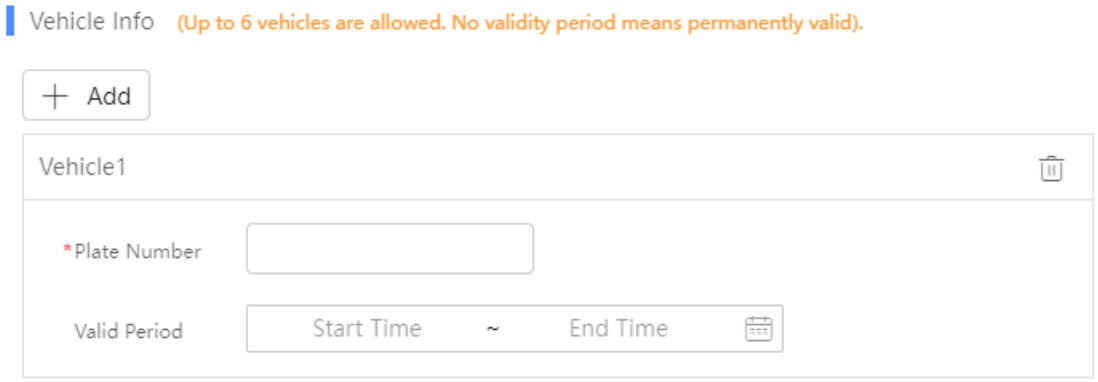
Note:
Only some access control devices support remote collection.

After the photo is uploaded, the feature extraction status is Not Extracted. Features will be extracted after saving the information.

(Optional) Vehicle Information

Add the person's vehicle information. Up to 6 vehicles are allowed per person.

1. On the **Vehicle Info** tab, click **Add**.



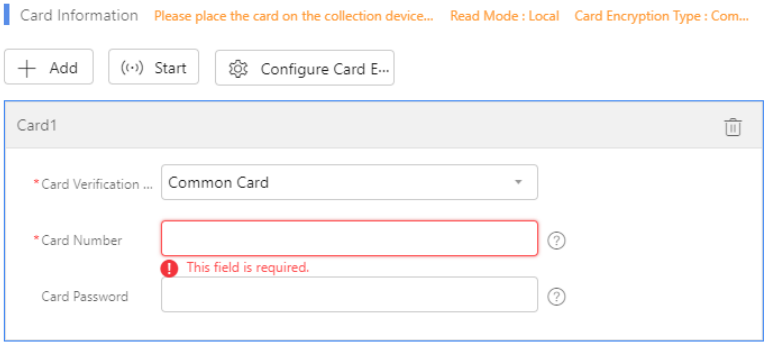
2. Enter the license plate number and select a validity period.

Note:
Vehicles added/edited/deleted here will be automatically synced to **Parking Mgt** > Authorized Vehicle. To sync vehicles to devices, see operations in Vehicle Data Sync. Only vehicles within the validity period can access the gates at the entrance and exit.

(Optional) Card Information

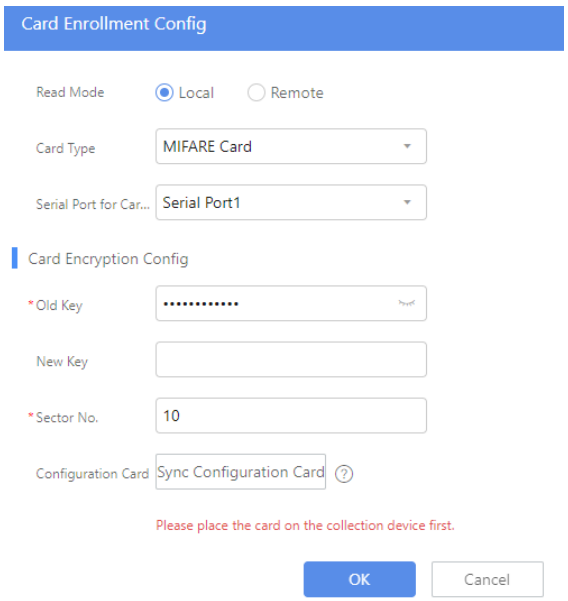
Supports reading and enrolling cards.

1. Go to the **Card** tab.



2. Click **Configure Card Enrollment**, and configure parameters as needed. (It only needs to be configured once and card information can be then read for multiple people.)

Read Mode	Description
Local	Connect the card enroller to the PC's port, and then place the card on the enroller to read/enroll it. **Note:** On the PC, right-click **Computer**, select **Manage> Device Manager > Ports (COM & LPT)**, and check for the **USB Serial Device (COMX)**, where **X** is the serial port number.

<table>
<tr><th>Read Mode</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2"></td><td>Common Card</td><td>Common card supports card reading only.
(1) Connect the card enroller to the PC's port.
(2) Select the card enroller model: (O)EC-W1D-EMC or (O)EC-W2D-M.
(3) To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click Sync Configuration Card, and then swipe it on the general access control device/access controller.
Note:
The configuration card is used to send the common card information to the general access control device/access controller.</td></tr>
<tr><td>MIFARE Card</td><td>MIFARE card supports card reading and enrollment. And you can also encrypt sectors to prevent from data leakage.
 

(1) Connect the card enroller to the PC’s port.
Note:
Only (O)EC-W2D-M supports reading the MIFARE card. So you don’t need to select the card enroller model.
(2) Card encryption configuration: Enter the card’s old key and sector number to encrypt the specified sector. To change the key, please enter the new key.
(3) To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click Sync Configuration Card, and then swipe it on the general access control device/access controller.
Note:
The configuration card is used to send the encryption card information to the general access control device/access controller.</td></tr>
<tr><td>Remote</td><td colspan="2">Select an access control device as collection device, and then swipe a card on it to read the card.
Note:
This feature is only available to certain access control devices. Please refer to the actual interface.</td></tr>
</table>

3. Click **Add** to add cards.

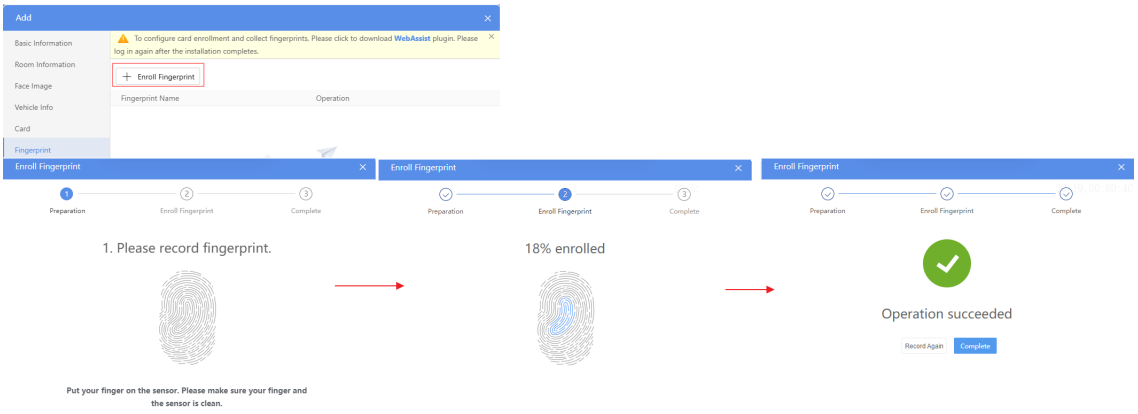
Note:
Up to 8 cards can be added. The number of cards supported may vary with device; if the device's capacity is less than the number of cards an individual has, only a portion of the cards can be synced successfully.

Parameter	Description
Card Verification Type	• Common Card: Can open doors with access permissions normally without triggering an alarm. • Duress Card: Can open doors with access permissions normally while simultaneously triggering a duress alarm.
Card Number	Read or enroll the card. **Note:** Preparation: (Local)Place the card on the card enroller; (Remote)Swipe the card on the access control device. • Read card: Click **Start** to read the card. • Enroll card (only when the MIFARE card is read locally): Enter the card number manually and then click **Start**; or, click **Start** to read the physical card number.
Card Password	Only cards for general access control devices need to be configured with a card password. **Card Password** is hidden by default. You can enable it in Function Switch.

(Optional) Fingerprint Information

Each person can enroll up to 10 fingerprints for fingerprint verification to open doors.

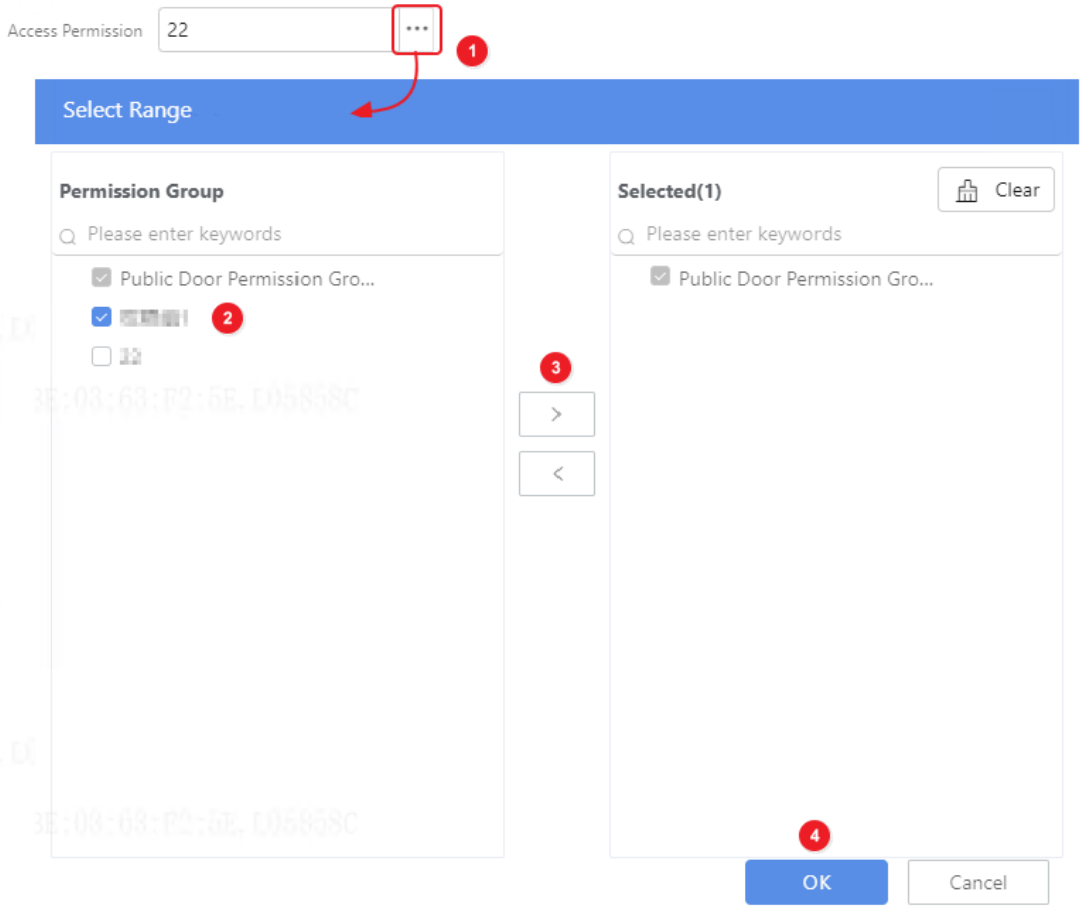
1. Connect the fingerprint collector to the USB port of the PC.
2. On the **Fingerprint** tab, click **Enroll Fingerprint**.
3. Place the finger on the fingerprint collector to start enrollment. Adjust multiple angles to enroll the fingerprint 5 consecutive times to complete the enrollment.



(Optional) Permission Group

Assign access permissions to personnel. Permission groups are created in Access Permission Config.

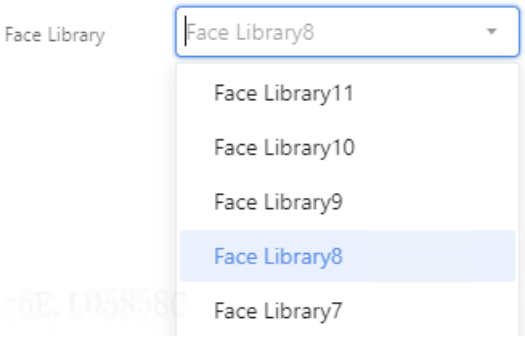
Click ... and then select the permission group.



(Optional) Face Library

Add face photos to a face library for monitoring. Face libraries are created in Face Library Management.

Select a face library from the drop-down list.



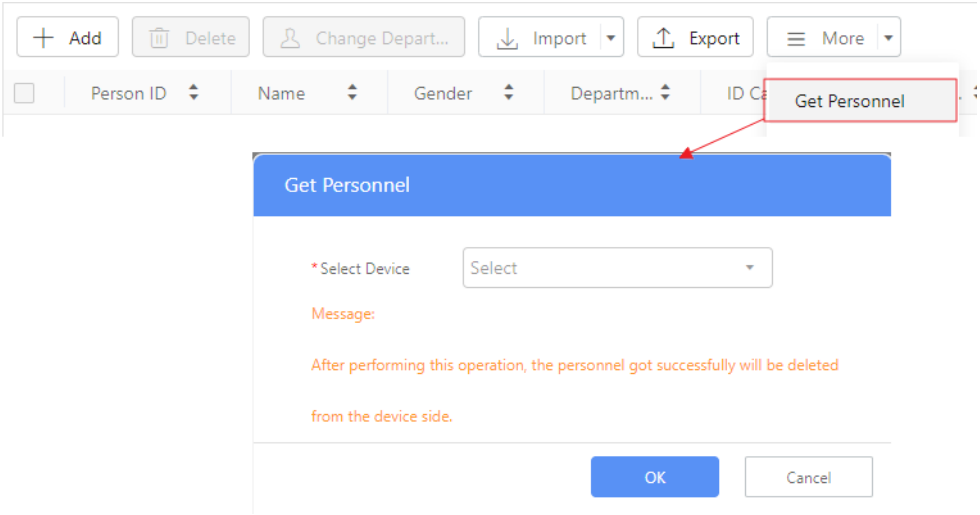
12.2.3 Get Personnel from Device Side

You can retrieve person information from access control devices to the platform.

Note:

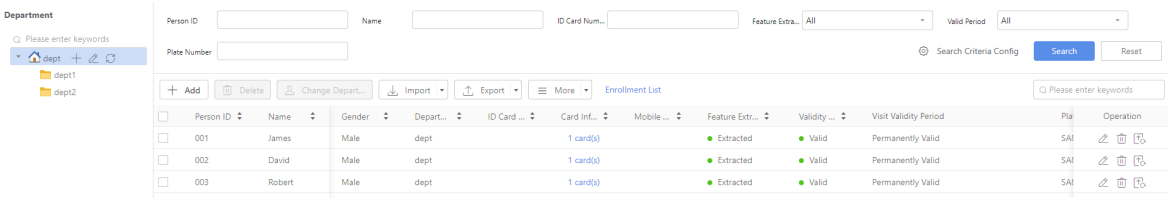
- This function is available on certain devices only. Please refer to the actual interface.
- Successfully retrieved person information will be deleted from the device.
- During the import process, the platform compares personnel names. If the device contains information about a person not listed on the platform, the platform will automatically create a new personnel entry. If both the device and the platform have information about the same person, the person information from the device will overwrite the existing information on the platform.

1. Click **Get Personnel**.
2. In the pop-up window, select the access control device(s) for sync and click **OK**. The person information will be synchronized from the device side to the platform.



12.3 Personnel Management

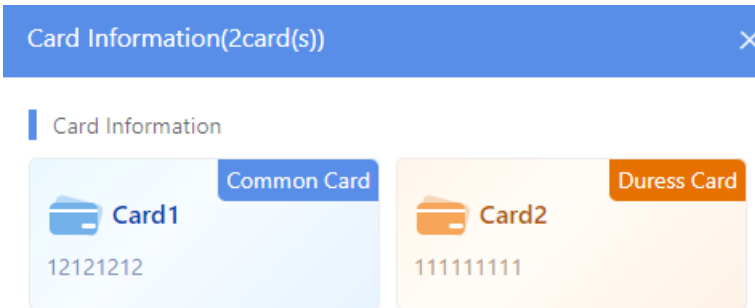
You can search, edit, delete, assign persons, and export person information.



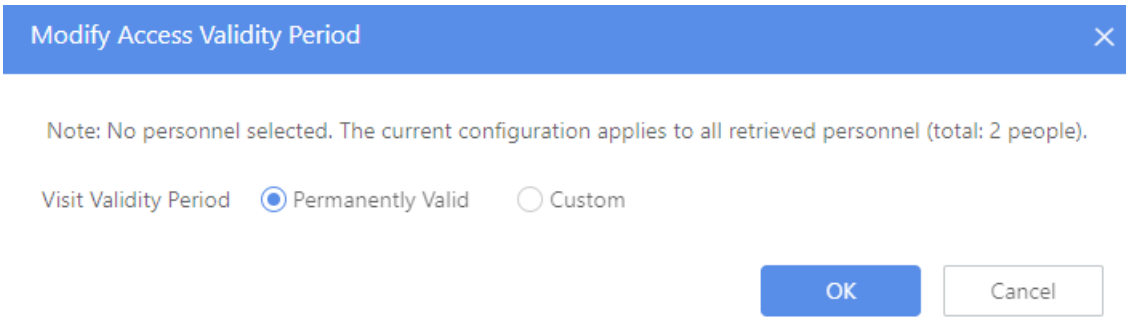
- Search: Set person ID, name, ID card number, feature extraction status as needed, and then click **Search**.

  Note:
  You can also set Custom Attribute as search criteria. Click **Search Criteria Config**, select up to 10 attributes, and then click **OK** to add them as search criteria.

- Edit person: Click in the **Operation** column to edit the person information.
- Delete person: Select person(s) to be deleted and click **Delete**, or click in the **Operation** column.
- Change department: Select the department on the left-side department tree, select the person(s) on the right, and then click **Change Department** to move the person(s) to another department.
- Export: Select the department on the left-side department tree, click **Export** and select **Export Personnel Info** or **Export Personnel Info and Images**.
- Re-extract: If the extraction fails, select person(s) and click **More >Re-extract**.
- View card information: Click the number in the card information column to view the card type and card number.



- Batch modify person access validity period: Click **More >Access Validity Period** to modify the access validity period for multiple persons in batches.



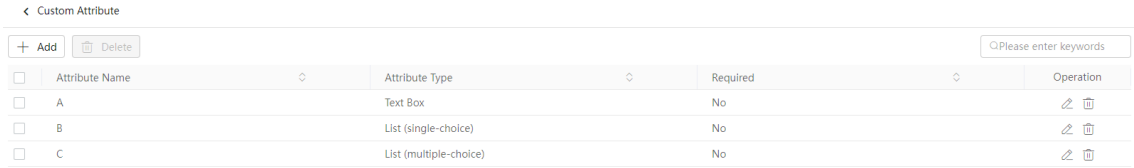
- If no persons are selected, the validity period of all found persons will be modified by default.
- If specific persons are selected, only the validity period of the selected persons will be modified.

12.4 Custom Attribute

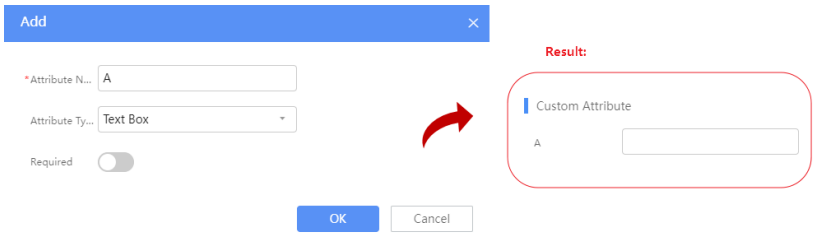
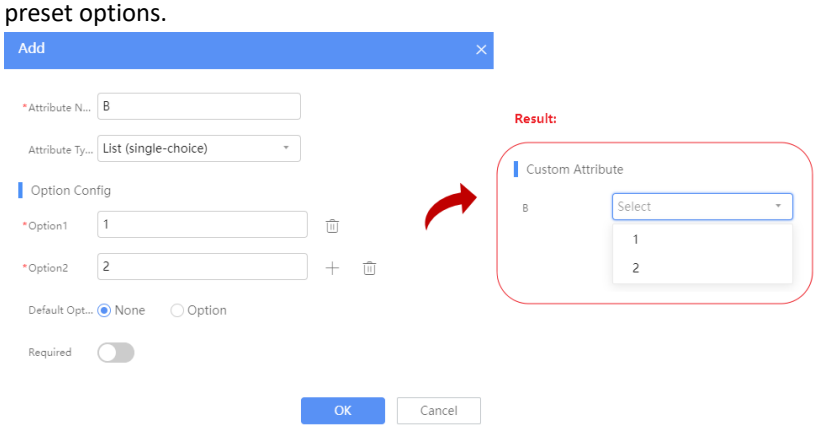
You can add custom attributes as supplements to person information. These custom attributes are displayed when adding, viewing, and modifying person information.

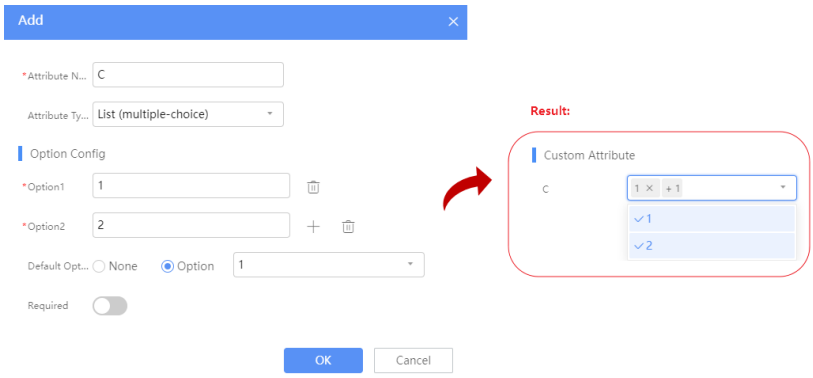
Add Attribute

1. Click **More > Custom Attribute** above the personnel list.



2. Click **Add**. Set the parameters by referring to the table, then click **Save**.

Item	Description
Attribute Name	Enter the custom attribute name.
Attribute Type	Choose one of the following type: • **Text Box**: When adding person, you need to manually enter the attribute information.  • **List (single-choice)**: You can add multiple options and set a default option for the attribute. When adding person, you can choose only one option from the preset options. 

Item	Description
	• **List (multiple-choice)**: You can add multiple options and set a default option for the attribute. When adding person, you can choose multiple options from the preset options. 
Required	If enabled, the attribute must be completed to submit the person information.

Other Operations

- Edit attribute: Click for the attribute to modify it. (Note: The attribute type cannot be changed.)
- Delete attribute: Select attribute(s) to be deleted and click **Delete**, or click in the **Operation** column.

13 Visitor Management

Go to **Access&Attendance> Visitor Management**.

Visitors are those who temporarily need access to a restricted area. The platform provides a comprehensive service for visitors, from pre-registration to sign-out.

- Pre-register the visitor information and assign temporary access permissions to them. Visitors can then enter the specified area within the validity period using face recognition or card swiping. After passing through an access control device, a visitor record is automatically generated.
- When visitors leave, they can be signed out manually by an admin or automatically by the system after their access end time, generating a sign-out record. Upon sign-out, the visitor's access permissions are cleared, ensuring prompt data updates.
- Search visit and sign-out records of visitors to manage visit information.
- Monitors whether visitors enter authorized areas during authorized time. If not, an unauthorized area access alarm or an unauthorized time access alarm will be reported.

13.1 Registration

Register visitor information and assign access permissions.

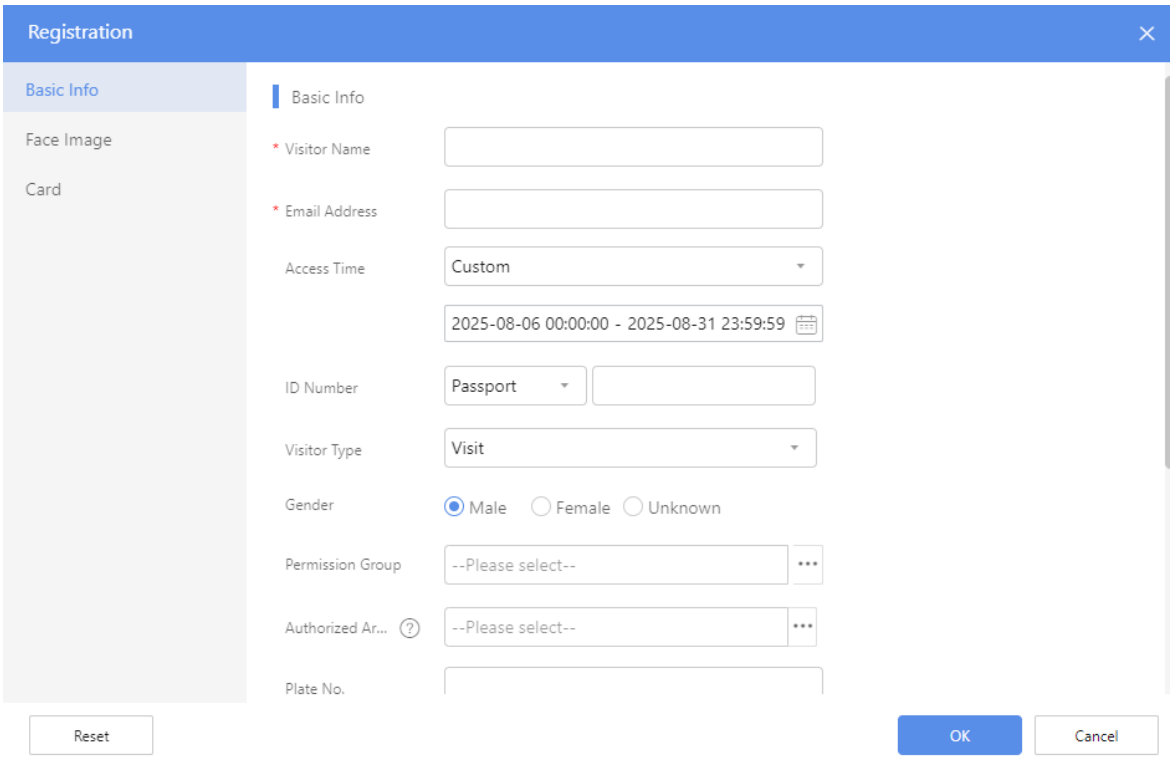
Go to **Visitor Management** > **Registration**.

Note:
You can also enroll the visitor information on the UNV Guard app. Please refer to the user manual of the app.

13.1.1 Register Visitor

Click **Add** to register the visitor information (identity information, card information, image, license plate number, Custom Attribute, etc.) and associate access permission groups and access time, and then click **OK**.

Basic Information



1. Complete the required information (fields marked with an asterisk *) for the visitor.
2. Select the access time (1 Day, 7 Days, 30 Days or Custom) and the permission groups. The permission groups set which doors the visitor can access and need to be created in advance (see Access Permission Config).
3. (Optional) Select the ID type from the list, and then input the ID number.
4. (Optional) Add the visitor's vehicle information. One visitor can only be associated with one vehicle.

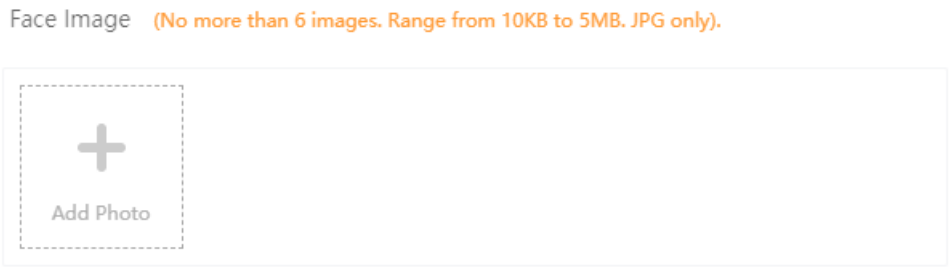
   Note:
   Vehicles added/edited/deleted here will be automatically synced to **Parking Mgt** > Authorized Vehicle. To sync vehicles to devices, see operations in Vehicle Data Sync. Only vehicles within the validity period can access the gates at the entrance and exit.
5. (Optional) Authorize area(s) for the visitor. An alarm will be triggered if the visitor enters an unauthorized area.

   Note:
   - For authorized areas, you can only select devices with existing Area Monitoring tasks (IPCs under smart NVRs and smart IPCs).
   - If an authorized area is configured, you must add a visitor photo. This photo will be used by smart devices to compare with the captured image to determine the visitor's permissions.
6. (Optional) Configure Custom Attribute as needed.

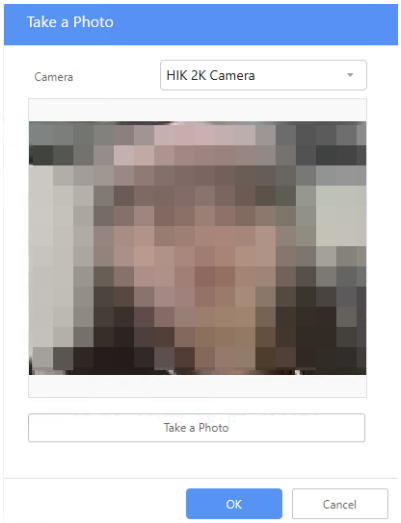
(Optional) Face Image

Note:
Image verification is enabled by default. To disable it, see Face Image Verification.

Click **Add Photo**. Choose a way to add photos:



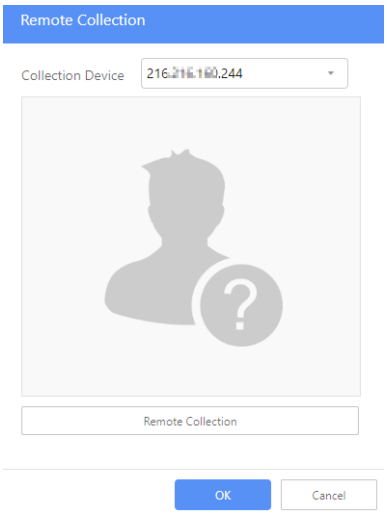
- Upload: Select a photo of the person from the PC and upload it.
- Take a photo: Select a camera to view its real-time screen on the PC. Click **Take a Photo** to capture the current frame. Click **OK** to save the photo, or click **Retry** to take another one.



Note:

- Please first enable HTTPS and log in via the HTTPS protocol before taking photos.
- The camera device supports USB cameras and the built-in camera of the computer. If you are using a USB camera, connect it to the PC in advance.

- Remote collection: Select a face recognition access control device and click **Remote Collection**. After the device completes face collection, you can check the collected photo on the client. Click **Re-Collect** if necessary, or click **OK** to complete the collection.



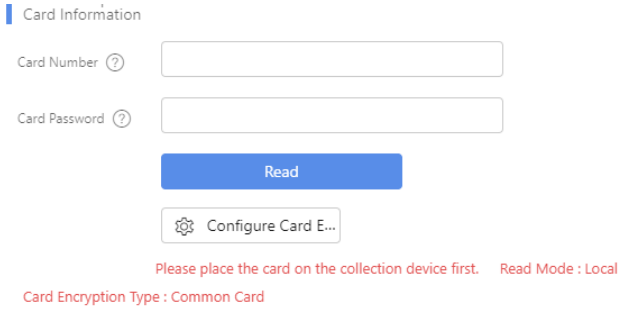
Note:
Only some access control devices support remote collection.

After the photo is uploaded, the feature extraction status is Not Extracted. Features will be extracted after saving the information.

(Optional) Card Information

Supports reading and enrolling cards.

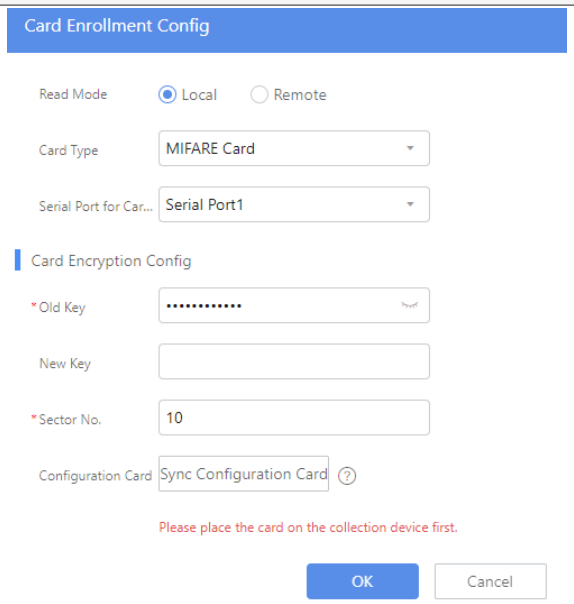
1. Go to the **Card** tab.



Note:
Only cards for general access control devices need to be configured with a card password. <Card Password> is hidden by default. You can enable it in Function Switch.

2. Click **Configure Card Enrollment**, and configure parameters as needed. (It only needs to be configured once and card information can be then read for multiple people.)

Read Mode	Description	
Local	Connect the card enroller to the PC's port, and then place the card on the enroller to read/enroll it. **Note:** On the PC, right-click **Computer**, select **Manage> Device Manager > Ports (COM & LPT)**, and check for the **USB Serial Device (COMX)**, where **X** is the serial port number.	
	Common Card	Common card supports card reading only. (1) Connect the card enroller to the PC's port. (2) Select the card enroller model: (O)EC-W1D-EMC or (O)EC-W2D-M. (3) To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click **Sync Configuration Card**, and then swipe it on the general access control device/access controller. **Note:** The configuration card is used to send the common card information to the general access control device/access controller.
	MIFARE Card	MIFARE card supports card reading and enrollment. And you can also encrypt sectors to prevent from data leakage.

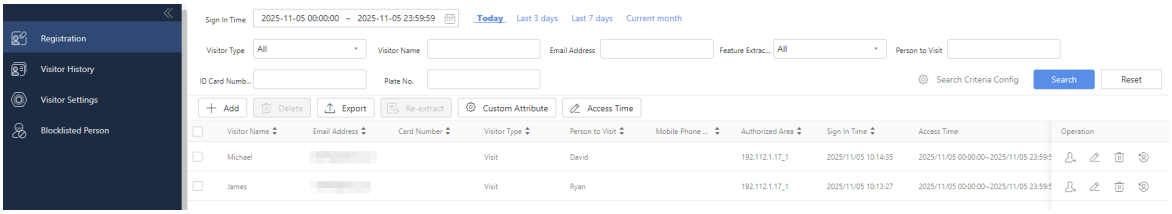
Read Mode	Description
	 (1) Connect the card enroller to the PC's port. **Note:** Only (O)EC-W2D-M supports reading the MIFARE card. So you don't need to select the card enroller model. (2) Card encryption configuration: Enter the card's old key and sector number to encrypt the specified sector. To change the key, please enter the new key. (3) To swipe a card on the general access control device/access controller, place the configuration card on the card enroller, click **Sync Configuration Card**, and then swipe it on the general access control device/access controller. **Note:** The configuration card is used to send the encryption card information to the general access control device/access controller.
Remote	Select an access control device as collection device, and then swipe a card on it to read the card. **Note:** This feature is only available to certain access control devices. Please refer to the actual interface.

3. Read or enroll the card.

Read Mode	Description
Local	Preparation: Place the card on the card enroller. • Read card: Click **Start** to read the card. • Enroll card (only for the MIFARE): Enter the card number manually and then click **Start**; or, click **Start** to read the physical card number.
Remote	Preparation: Swipe the card on the access control device. Read card: Click **Read** to read the card.

13.1.2 Visitor Management

You can view visitor status, edit, delete, export, search, and sign out visitors.



Vistor Status

- Unauthorized: The visitor has no permission group assigned.
- Registered: The visitor has been assigned a permission group, but has not arrived yet.
- Arrived: The visitor has been verified at the access control devices.
- Overstay: The visitor has not signed out upon expiration of the access period.

Sign out

Click in the **Operation** column to sign out the visitor. When signed out, the visitor will be removed from the visitor list and the related access permission will also be cleared.

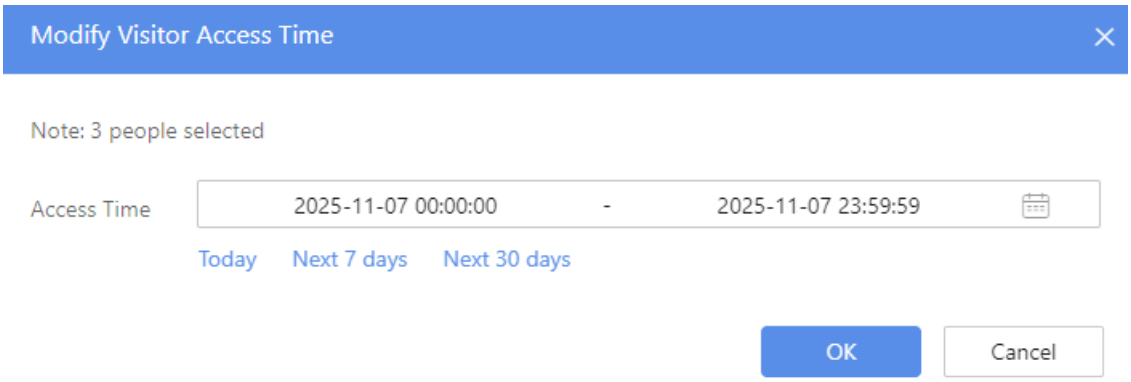
Note:
Visitors who haven't been signed out by the access permission end time will be automatically signed out at the set auto sign-out time (set in Visitor Settings).

More Operations

- Edit: To edit the visitor information and access permissions, click in the **Operation** column.
- Delete: To delete registered visitors, select the visitors to be deleted and click **Delete**, or click in the **Operation** column. The visitor's access permissions will be revoked after deletion.
- Export: Select visitors, click **Export**.
- Search: Set criteria such as sign in time and visitor name as needed, and then click **Search**.

  Note:
  You can also set Custom Attribute as search criteria. Click **Search Criteria Config**, select up to 10 attributes, and then click **OK** to add them as search criteria.
- Re-extract: If the extraction fails, select visitor(s) and click **Re-extract**.
- Convert Visitor to Personnel: Click in the **Operation** column to directly change a visitor into personnel.

  Note:
  After conversion, the visitor will be automatically signed out.
- Batch modify visitor access time: Click **Access Time** to modify the access time for multiple visitors in batches.



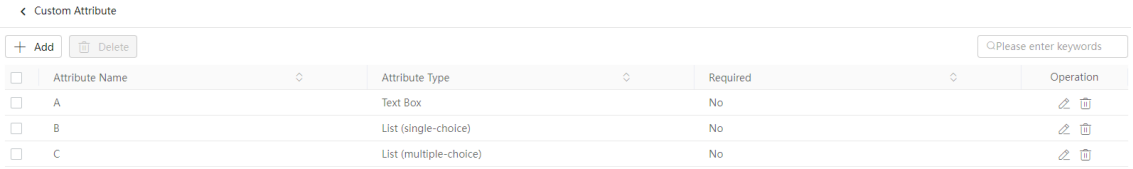
  - If no visitors are selected, the validity period of all found visitors will be modified by default.
  - If specific visitors are selected, only the validity period of the selected visitors will be modified.

13.1.3 Custom Attribute

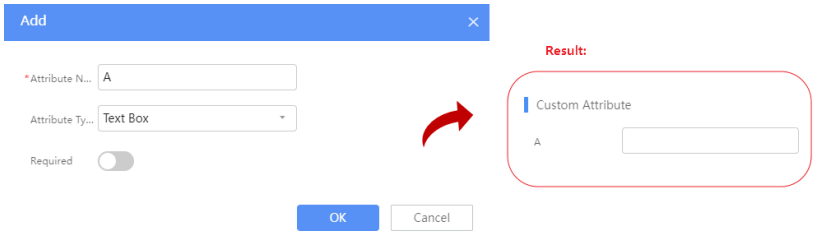
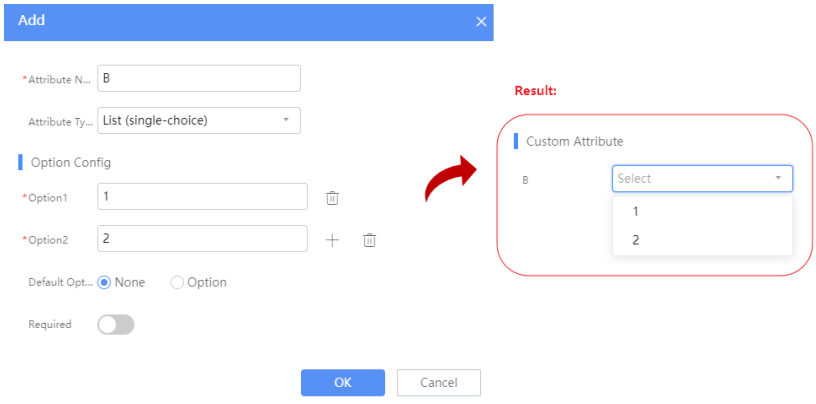
You can add custom attributes as supplements to visitor information. These custom attributes are displayed when adding, viewing, and modifying visitor information.

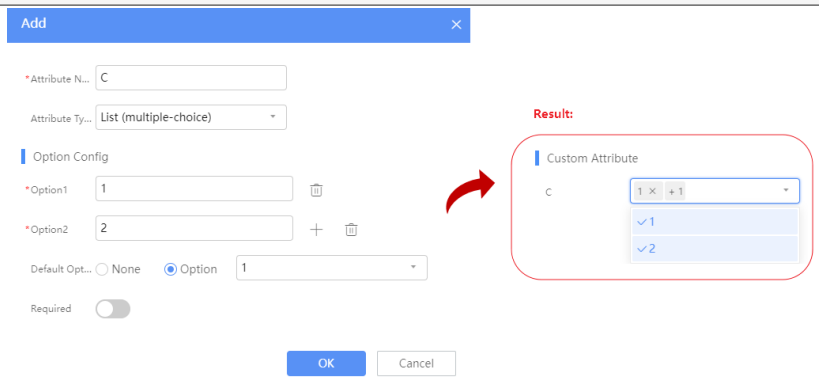
Add Attribute

1. Click **Custom Attribute** above the above list.



2. Click **Add**. Set the parameters by referring to the table, then click **Save**.

Item	Description
Attribute Name	Enter the custom attribute name.
Attribute Type	Choose one of the following type: • **Text Box**: When adding visitor, you need to manually enter the attribute information.  • **List (single-choice)**: You can add multiple options and set a default option for the attribute. When adding visitor, you can choose only one option from the preset options.  • **List (multiple-choice)**: You can add multiple options and set a default option for the attribute. When adding visitor, you can choose multiple options from the preset options.

Item	Description
	
Required	If enabled, the attribute must be completed to submit the visitor information.

Other Operations

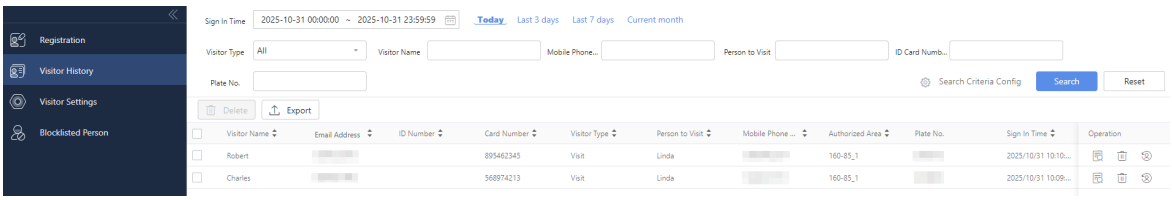
- Edit attribute: Click for the attribute to modify it. (Note: The attribute type cannot be changed.)
- Delete attribute: Select attribute(s) to be deleted and click **Delete**, or click in the **Operation** column.

13.2 Visitor History

The **Visitor History** page displays visitor records of those who have signed out.

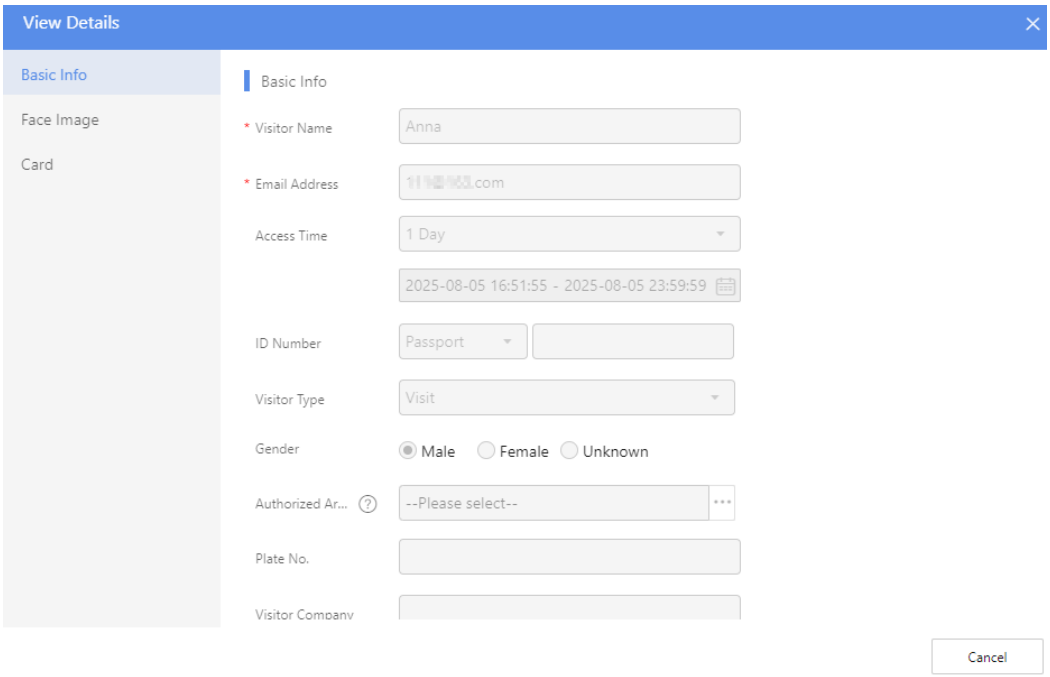
Search

1. Set search criteria such as sign in time and visitor name as needed. (You can also click **Search Criteria Config** to add custom attributes as search criteria.)
2. Click **Search** to view the visitor information within the specified time period.



More Operations

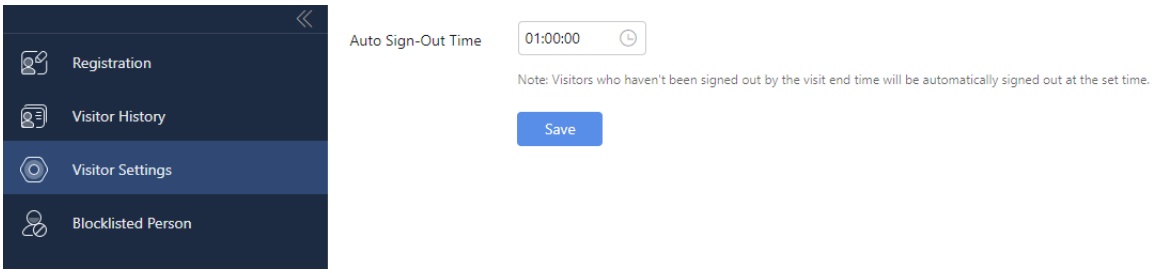
- View details: Click in the **Operation** column to view details about the visitor such as basic information and sign in/out time.



- Delete records: Select record(s) to be deleted and click **Delete**, or click in the **Operation** column.
- Export records: Select record(s) to be exported, click **Export**, and then select the storage path to save the records.

13.3 Visitor Settings

Set the automatic sign-out time for visitors. Visitors who **haven't been signed out by the access permission end time** will be automatically signed out at the set time each day.



On the day when a visitor's access permission ends:

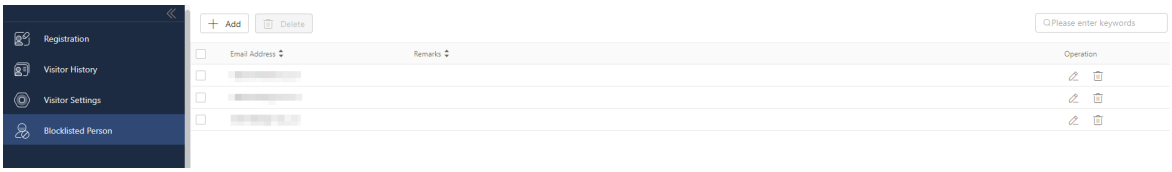
- If the auto sign-out time is later than the permission end time, the visitor will be automatically signed out at the set time on the same day.
- If the auto sign-out time is earlier than the permission end time, the visitor will be automatically signed out at the set time on the following day.

For example, if visitor A's access time is 8:00-11:00, visitor B's access time is 8:00-13:00, and the auto sign-out time is 12:00, then visitor A will be automatically signed out at 12:00 on the same day, while visior B will be automatically signed out at 12:00 on the following day.

13.4 Blocklisted Person

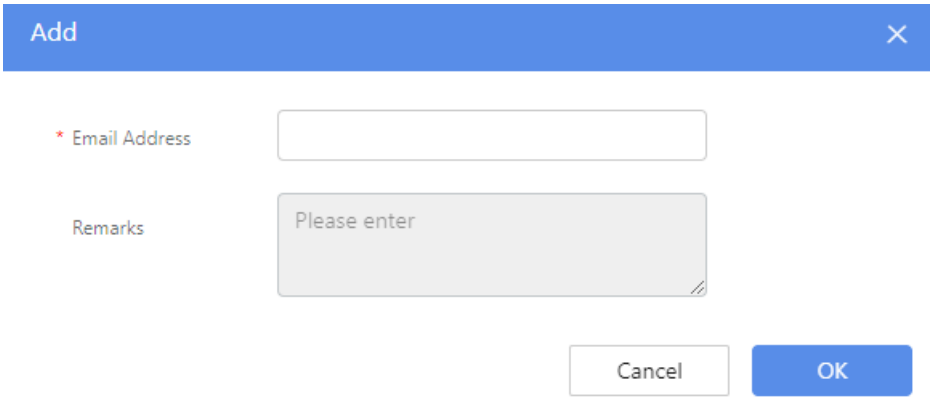
The system supports adding blocklisted persons. Once added, these individuals cannot be registered as visitors.

Note:
The blocklisted person feature is not supported in cloud-edge mode.



Add Blocklisted Person

Click **Add**, enter the blocklisted person's email address, and optionally provide remarks to explain the reason for restriction.



During addition, the system will check whether the blocklisted person already exists in the visitor list based on their email address.

- Not registered as a visitor: After successfully adding the blocklisted person, any subsequent attempt to register this individual as a visitor will fail.
- Already registered as a visitor: The visitor will be automatically signed out, and the blocklisted person will be successfully added.

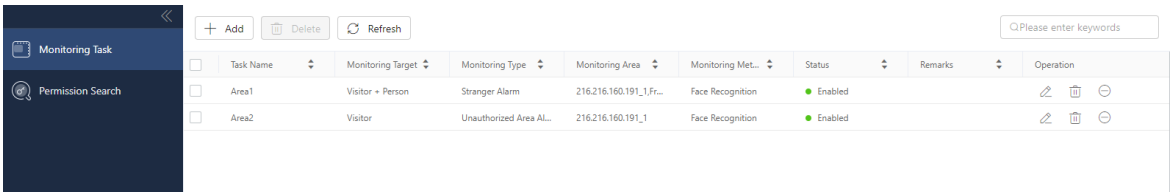
More Operations

- Search: Enter keywords in the upper-right corner to quickly find blocklisted persons.
- Edit: Click the corresponding for a blocklisted person to modify his/her information.
- Delete: Select the blocklisted person(s) and click **Delete**, or click in the **Operation** column.

14 Area Monitoring

Go to **Park Application** > **Area Monitoring**.

Monitor visitors within specified areas (including visitors visiting unauthorized areas or visiting during unauthorized times) and strangers.



Note:
You can create up to 10 monitoring tasks.

14.1 Vistor Monitoring Task

Go to **Park Application** > **Area Monitoring** > **Monitoring Task**.

Monitors whether visitors enter authorized areas during authorized time. If a visitor enters an unauthorized area or appears during unauthorized hours, an unauthorized area access alarm or an unauthorized time access alarm will be reported.

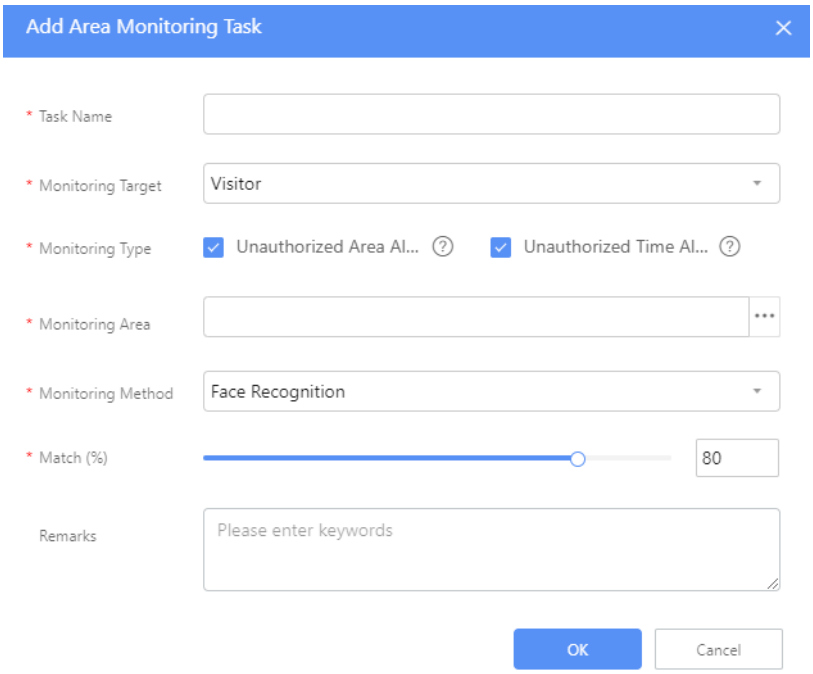
- The monitoring devices must support face recognition, including IPCs under smart NVRs and smart IPCs.
- After adding a monitoring task, visitor photos are automatically synced to smart devices in the monitoring areas, and Face Match monitoring tasks are created on the smart devices.
- When a smart device recognizes a visitor, it will verify whether the visitor is in an authorized area and appears during authorized hours.
  - If the device is not within the visitor's authorized area, an unauthorized area access alarm will be reported.
  - If the time is not within the visitor's access time, an unauthorized time access alarm will be reported.

Note:

- Please configure authorized area and access time for visitor in Registration.
- If the platform is connected to EZCloud, then visitor information cannot be edited on the platform. You need to configure the authorized area on the visitor review page on the UNV Guard app.

Add Task

1. Click **Add**.



Item	Description
Task Name	Enter a custom task name.
Monitoring Target	Select Visitor.
Monitoring Type	Select the monitoring type(s). • Unauthorized Area Alarm: Triggers an alarm when the monitored target enters an unauthorized area. • Unauthorized Time Alarm: Triggers an alarm when the monitored target appears during unauthorized hours.
Monitoring Area	Select IPCs under smart NVRs or smart IPCs.
Monitoring Method	Default is Face Recognition.
Match	If the match degree between the captured image and visitor photos meets or exceeds the set threshold, the system identifies it as the same person. The system then evaluates whether the access is unauthorized based on the visitor permissions.

2. Click **OK**. The system will automatically sync information of visitors who haven't been signed out to smart devices in the monitoring areas.

Subsequent Operations

- **Search for visitor match events**: When a smart device matches a visitor, it reports a visitor match event. View visitor match events in **Comprehensive Search > Face Search** .
- **Search for unauthorized access alarms**: If a visitor enters an unauthorized area or appears during unauthorized hours, an unauthorized area/time access alarm will be reported (in this case, no match alarm will be reported). If the visitor is within the authorized area and time, no alarm will be reported. View unauthorized area/time access alarms in Historical Alarm.

14.2 Stranger Monitoring Task

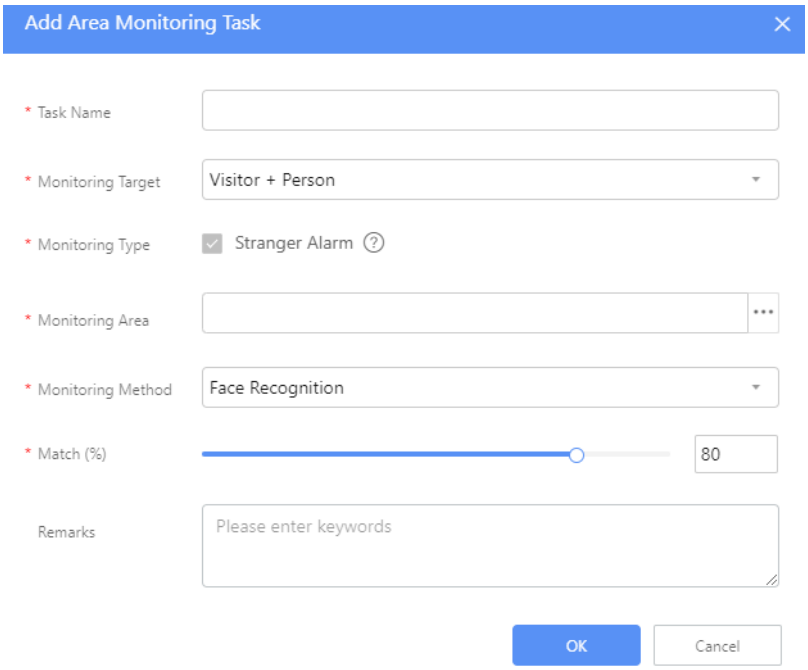
Go to **Park Application** > **Area Monitoring** > **Monitoring Task**.

Detect strangers within the monitoring areas.

- The monitoring devices must support face monitoring, including IPCs under smart NVRs and smart IPCs.
- After adding a stranger monitoring task, photos of personnel/visitors are automatically synced to smart devices in the monitoring area, and Face Not Match monitoring tasks are created on the smart devices.
- When a smart devices detects a person who is not in the personnel library or visitor library, it triggers a stranger alarm.

Add Task

1. Click **Add**. The **Add Area Monitoring Task** page appears.



Parameter	Description
Task Name	Enter a custom name.
Monitoring Target	Select **Visitor + Person**.
Monitoring Type	The default is **Stranger Alarm**.
Monitoring Area	Select IPCs under smart NVRs or smart IPCs.
Monitoring Method	The default is **Face Recognition**.
Match (%)	When the similarity between the person in a snapshot and persons or visitors in the library photos is below the threshold, the person is considered a stranger.

2. After the configuration is completed, click **OK** to create the task, and the system will automatically sync all personnel/un-signed-out visitor information to the devices in the monitoring area.

Follow-up Actions

- Search stranger alarms: When a stranger is detected, a stranger alarm is reported (Not Match alarm will not be reported) and can be retrieved at Historical Alarm. No alarms are triggered when a visitor or personnel are detected.
- Search stranger events: When a stranger is detected, a Not Match event is reported and can be retrieved at **Comprehensive Search > Face Search**

14.3 Task Management Operations

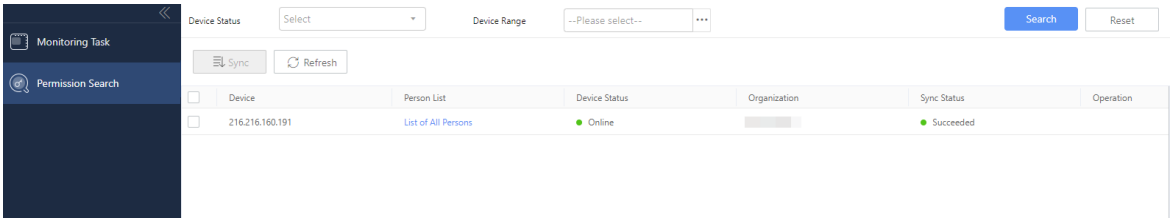
Go to **Park Application** > **Area Monitoring** > **Monitoring Task**.

- Edit: Click for the task to edit task parameters.
- Delete: Select task(s) to be deleted and click **Delete**, or click for the task.
- Enable/Disable: Click / for the task to enable or disable it.

14.4 Permission Search

Go to **Park Application** > **Area Monitoring** > **Permission Search**.

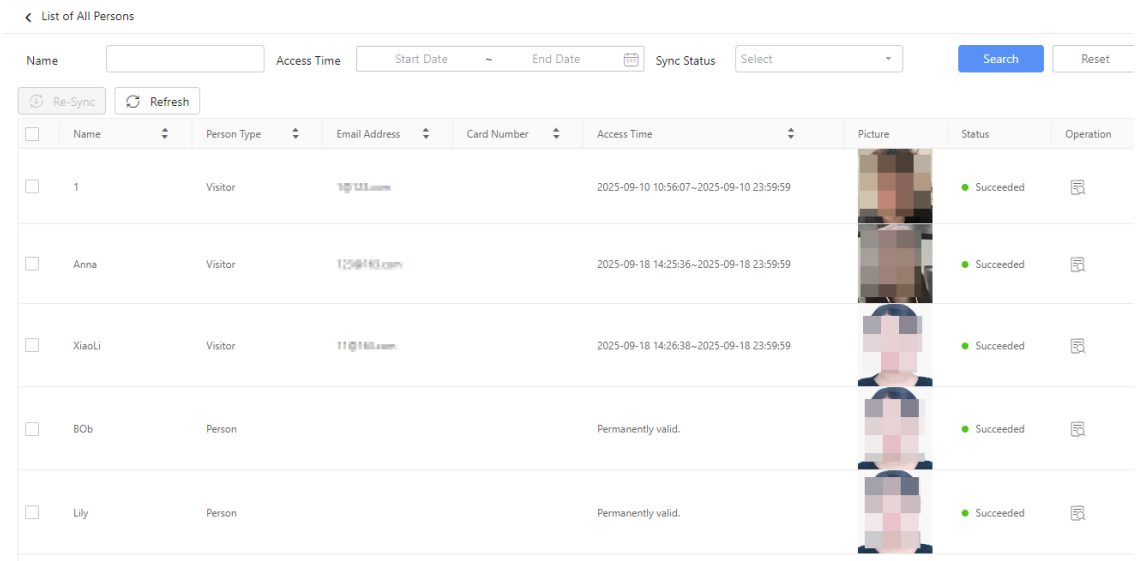
View synced personnel and visitors by device.



- Sync: The system automatically syncs personnel and visitors to devices in authorized areas. If the sync fails, you can select the device and click **Sync** to re-sync the personnel and visitor information.

  Note:
  Sync Status: Displays **Succeeded** only when all monitoring targets are successfully synced to the device; displays **Failed** if any monitoring target fails to be synced.

- View the person sync list:
  For visitor monitoring tasks: Click **Visitor List** (in blue) to view authorized visitors on the device (only visitors who haven't been signed out are displayed).
  For stranger monitoring tasks: Click **List of All Persons**(in blue) to view visitors (only visitors who are not signed out) and personnel on the device.



  - If the sync fails for any personnel or visitor, select the people and click **Re-Sync**.

- Click for the personnel or visitor to view details.

15 Access Control Management

Access control management offers permission management services for entrances and exits in locations like campuses, communities, buildings, and schools. With face recognition terminals, general access control devices, access controllers, etc., personnel can open doors using face recognition or card swiping once permissions are set. Administrators can view live videos from access control devices, remotely open or close doors, and review all historical access records. This function automates access verifications, prevents unauthorized entries, ensures safety, and improves the efficiency of gate management.

Functions

Menu	Description
Access Control Permission	Allows users to configure access permissions for personnel as needed, specifying accessible access control devices and their access times. You can view, search, and edit personnel access permissions after configuring. Personnel information, such as images, cards, is automatically synced to the linked access control devices, which can extract image features. When personnel pass through the access control devices, their information is verified with the stored data, allowing entry only if the verification succeeds.
Remote Control	Manage access control devices by system's default organization or custom organization, and batch open/close doors remotely.
Face Recognition Access Control Configuration	Configure the parameters of the face recognition access control device and sync the configuration.
Access Control Live	Allows users to view live videos from access control devices and captured access records. Capturing snapshots, enlarging live view images, remotely opening/closing doors are supported.
Pass-Thru Records	Allows users to filter personnel access records by date, access control device, etc.

Workflow

1. Add face recognition terminals, general access control devices, access controllers, etc.. See Device Management > Private Device.
2. Add persons. See Personnel Management .
3. Configure the effective time of access permission. See Access Control > Schedule Template.
4. Specify access control devices for persons. See Access Control > Access Permission Config.
5. View live videos of access control devices and people access records. See Smart Live View > Access Control Live and Data Search > Pass-Thru Records.

15.1 Access Control Permission

Go to **Access&Attendance** > **Access Control**.

By configuring schedule templates and access permission groups, you can restrict the access control channels and access periods for individuals, preventing unauthorized entry and ensuring campus security.

15.1.1 Schedule Template

Go to **Access Control** > **Schedule Template**.

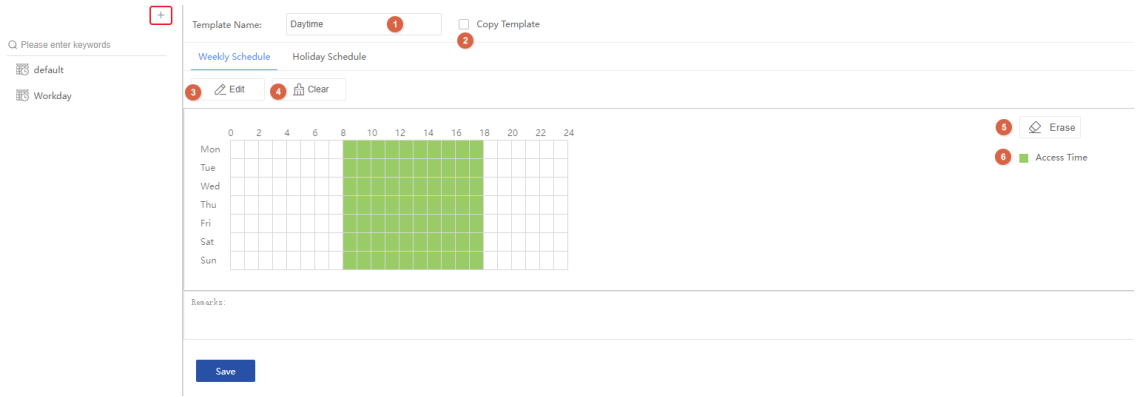
The schedule template is used to configure the effective time of access permission in each day. People can only access the specified doors/elevators within the set time period in the schedule template. By configuring schedule templates in advance, you can quickly apply the time settings from the template when configuring permission groups to set access permissions for personnel in batches effectively.

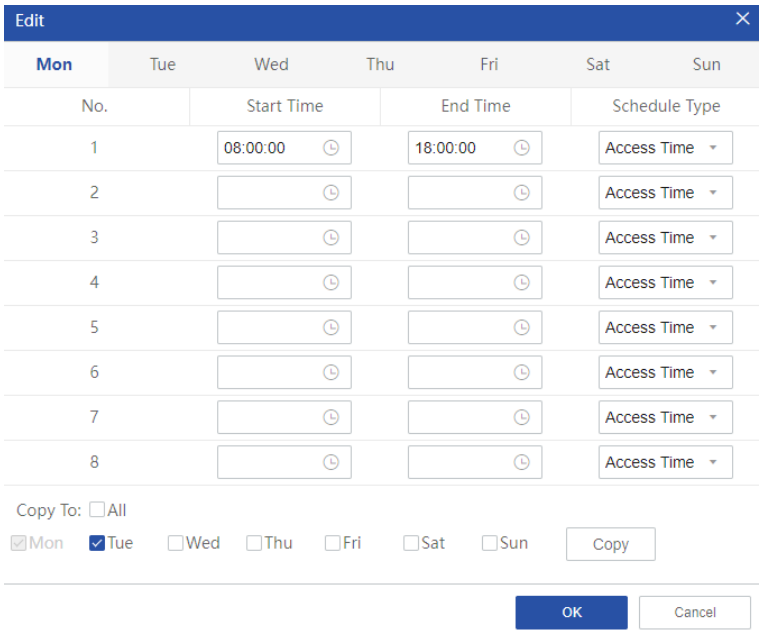
Note:

- There is a default template in the system for all-day access, which cannot be edited or deleted.
- You can customize new schedule templates, which can be edited and deleted.
- There are 2 kinds of schedule template: Weekly Schedule and Holiday Schedule. During regular periods, access permissions are executed based on the weekly schedule; while during holidays, the holiday schedule takes precedence and access permissions are executed based on the holiday schedule. For example, if access permissions are not granted during holiday periods, access will still be restricted even if those periods are within the access periods of the weekly schedule.

Add Schedule Template

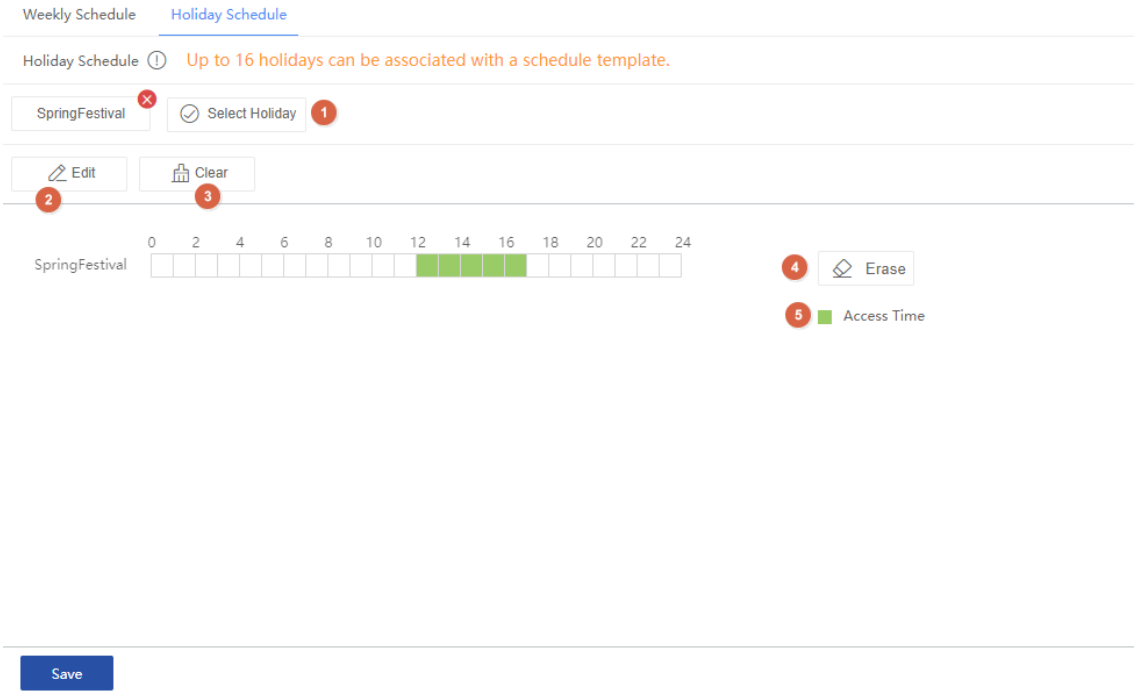
1. Click + to add a schedule template.
2. Configure the weekly schedule.



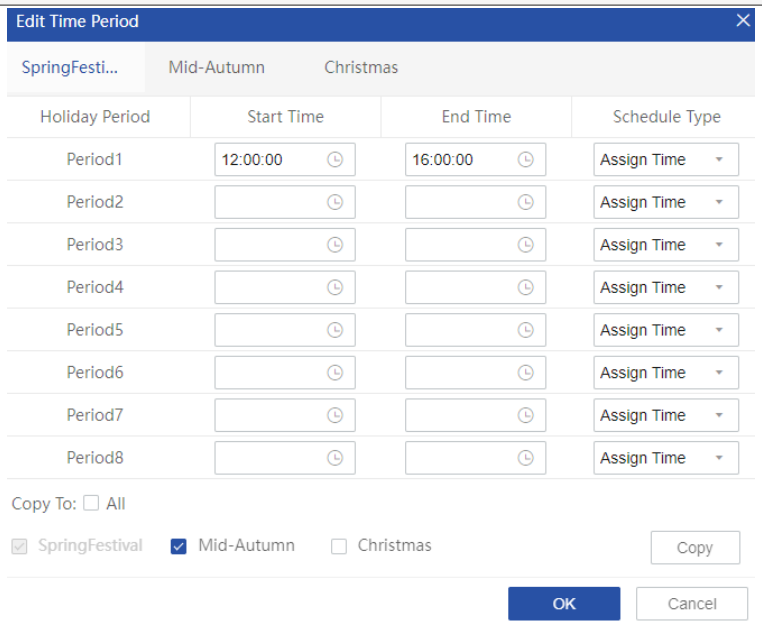
No.	Description
1	Set the template name.
2	Select **Copy Template** to choose an existing template and apply its time settings to the current template. You can then edit the copied time settings based on your needs.
3	Click **Edit** to set precise access periods for each day of a week. Up to 8 time periods are allowed per day.  After completing settings for a day, you can select other day(s) and click **Copy** to copy settings to them.

No.	Description
	Note: The access periods of general access control devices can be precise to the minute (for example, if the access time is set to 18:00:xx, then it will be valid until 18:00:59). The access periods of other access control devices can be precise to the second;.
4	Click **Clear** to clear all settings of this template.
5	Click **Erase** to erase the assigned time periods by clicking or dragging the left mouse button in the time chart.
6	Click **Access Time** to assign time periods by clicking or dragging the left mouse button in the time chart.

3. (Optional) Configure the holiday schedule.



No.	Description
1	Select holiday(s). (Holidays created in **System Config > Sercive Config > Holiday Management**) • Up to 16 holidays can be associated with a schedule template. • Click X in the upper-right corner of the holiday to delete it.
2	Click **Edit** to set precise access periods for each day of a holiday. Up to 8 time periods are allowed per day.

No.	Description
	 **Attention:** The access period for general access control devices can only be set as 00:00-11:59 or 12:00-23:59. After completing settings for a holiday, you can select other holiday(s) and click **Copy** to copy settings to them.
3	Click **Clear** to clear all settings of this template.
4	Click **Erase** to erase the assigned time periods by clicking or dragging the left mouse button in the time chart.
5	Click **Access Time** to assign time periods by clicking or dragging the left mouse button in the time chart.

4. Click **Save** to save the settings.

15.1.2 Access Permission Config

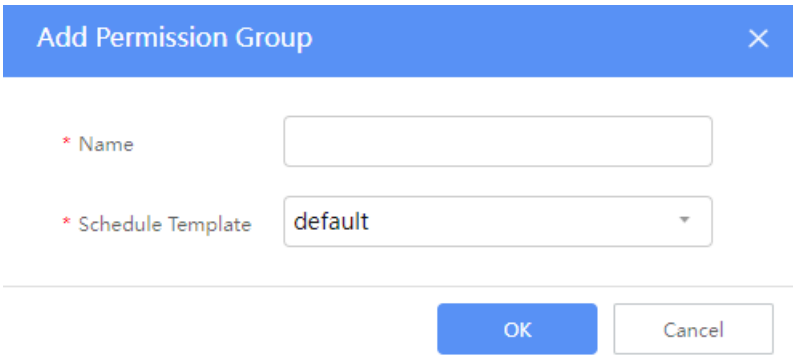
Configure permission groups to associate persons and effective period for access control devices (face recognition terminals, door stations, zone stations, general access control devices, access controllers, speed gate turnstile) and elevator controllers. You can assign access permissions to individuals to restrict their access to specific access control devices and elevators, allowing categorized permission management and ensuring security.

Note:

- By default, there is a public door permission group in the system that applies to all people at all times. You need to add access control devices and elevator controllers under this group. See Manage Permission Group.
- You can add multiple permission groups to meet your needs.
- Do not configure conflicting permission groups for personnel. For example, cannot assign different schedule templates to the same individual on the same device.

Add Permission Group

1. Click **Add**.



(1) Enter the permission group name.

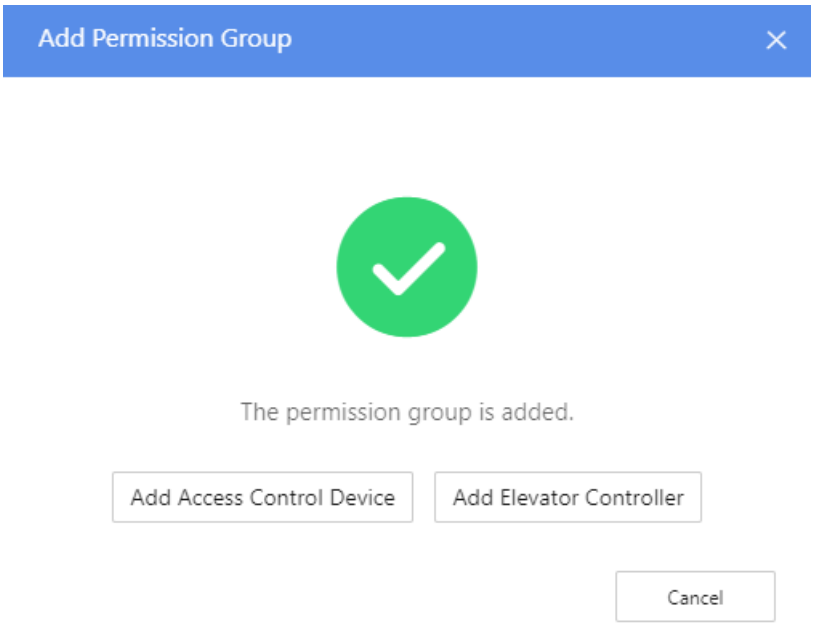
(2) Select a Schedule Template so that people can only access the specified access control devices within the set time period in the schedule template.

Note:

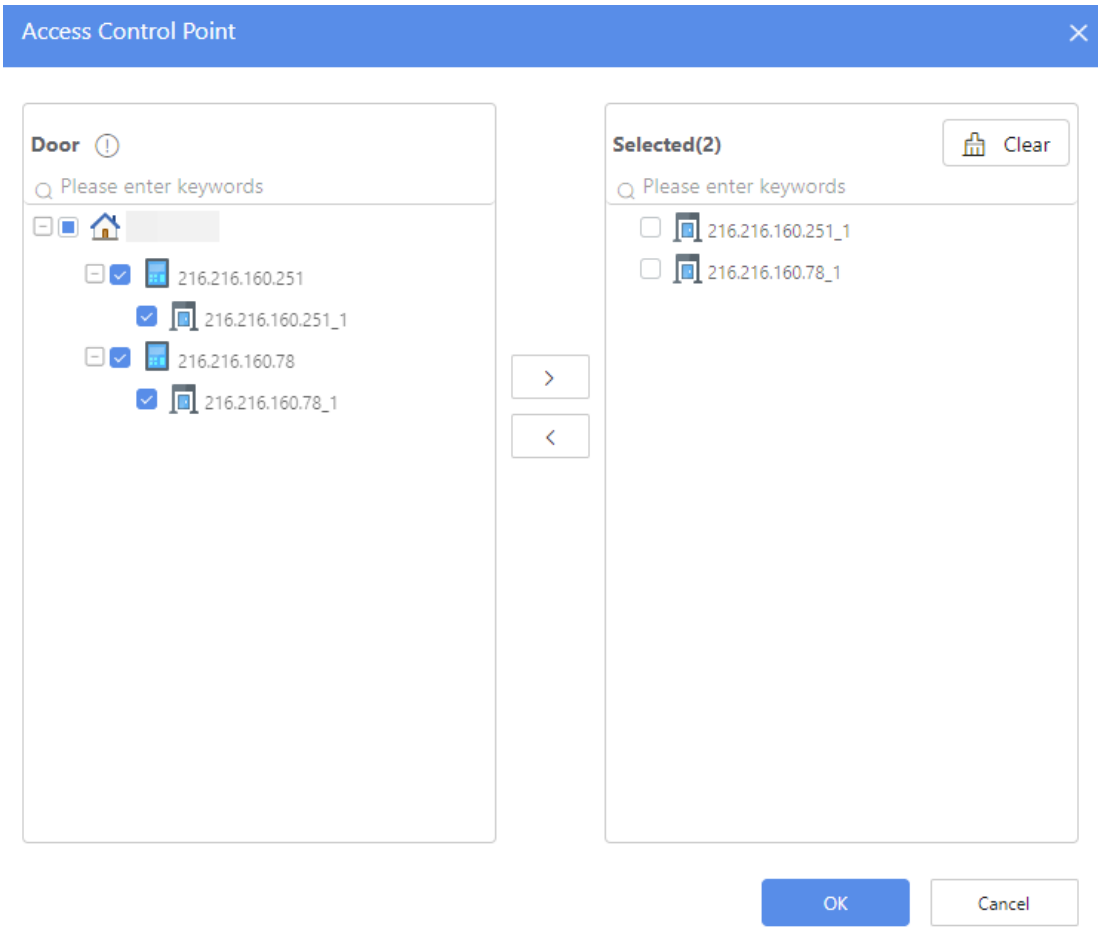
- The access period in the holiday schedule for general access control device can only be set as 00:00-11:59 or 12:00-23:59. Please make sure the selected schedule template is configured properly.
- Some models of face recognition terminals do not support holiday schedules.
- For certain models of face recognition access control terminals, after permissions are synced, if the verification template on the device side is empty, you can go to Face Library Configuration to configure and sync the verification template.

(3) Click **OK**.

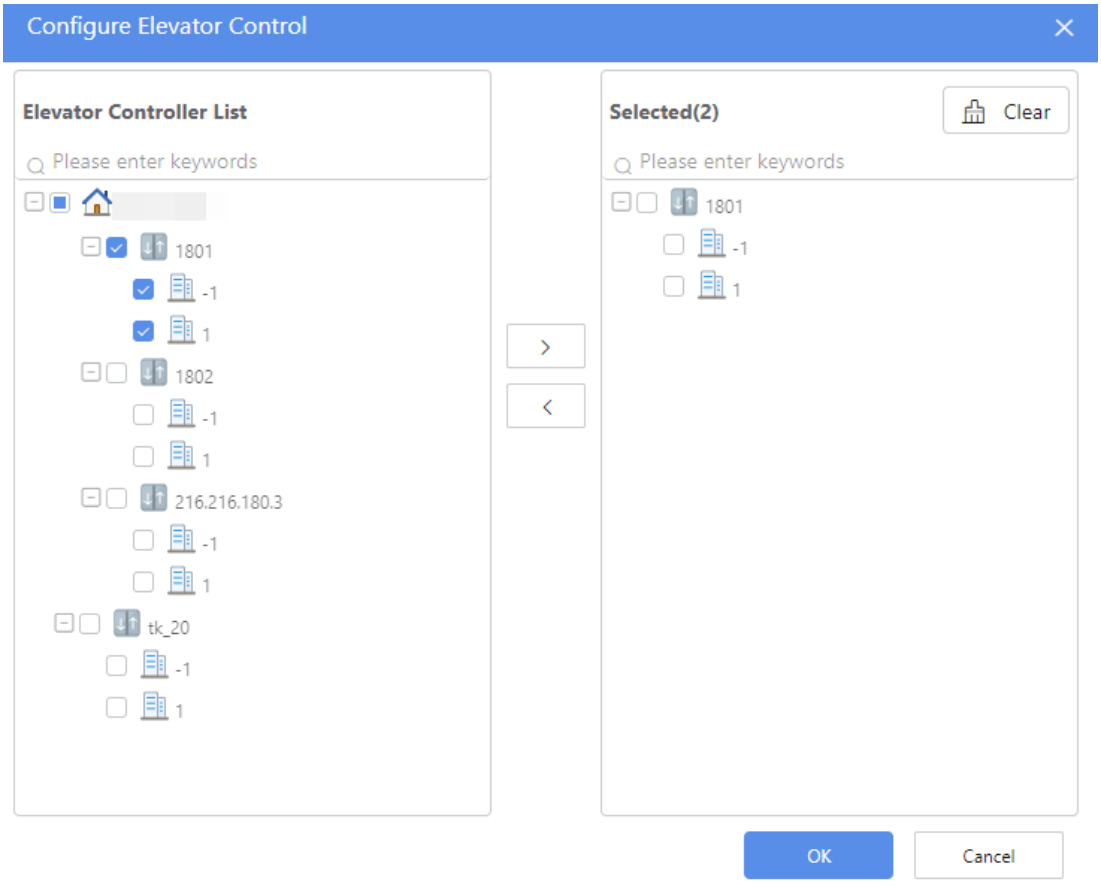
2. Add access control device(s) or elevator controller(s).



- **Add Access Control Device**: Click **Add Access Control Device**, select access control devices, and then click > to add them to the right-side list. Click **OK**.

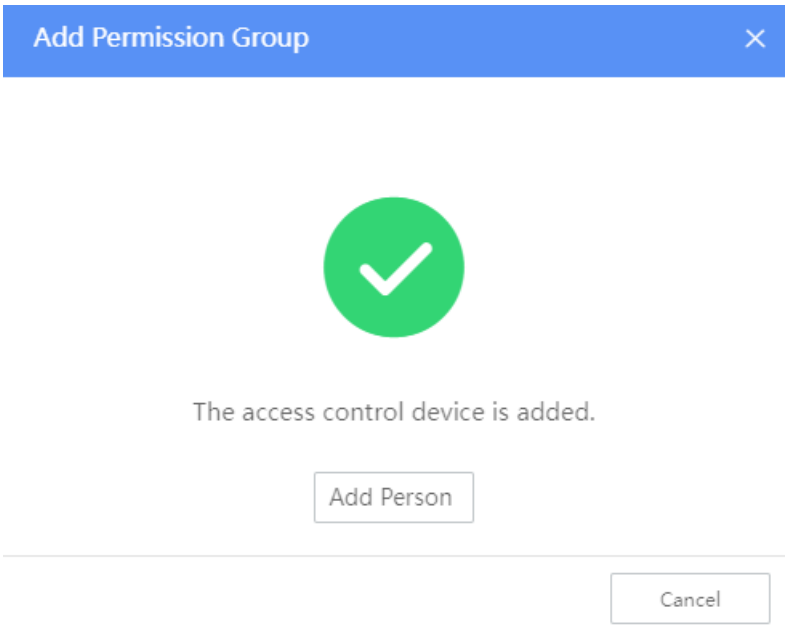


- **Add Elevator Controller**: Click **Add Elevator Controller**, select the floors bound to the elevator controller, and then click > to add them to the right-side list. Click **OK**.



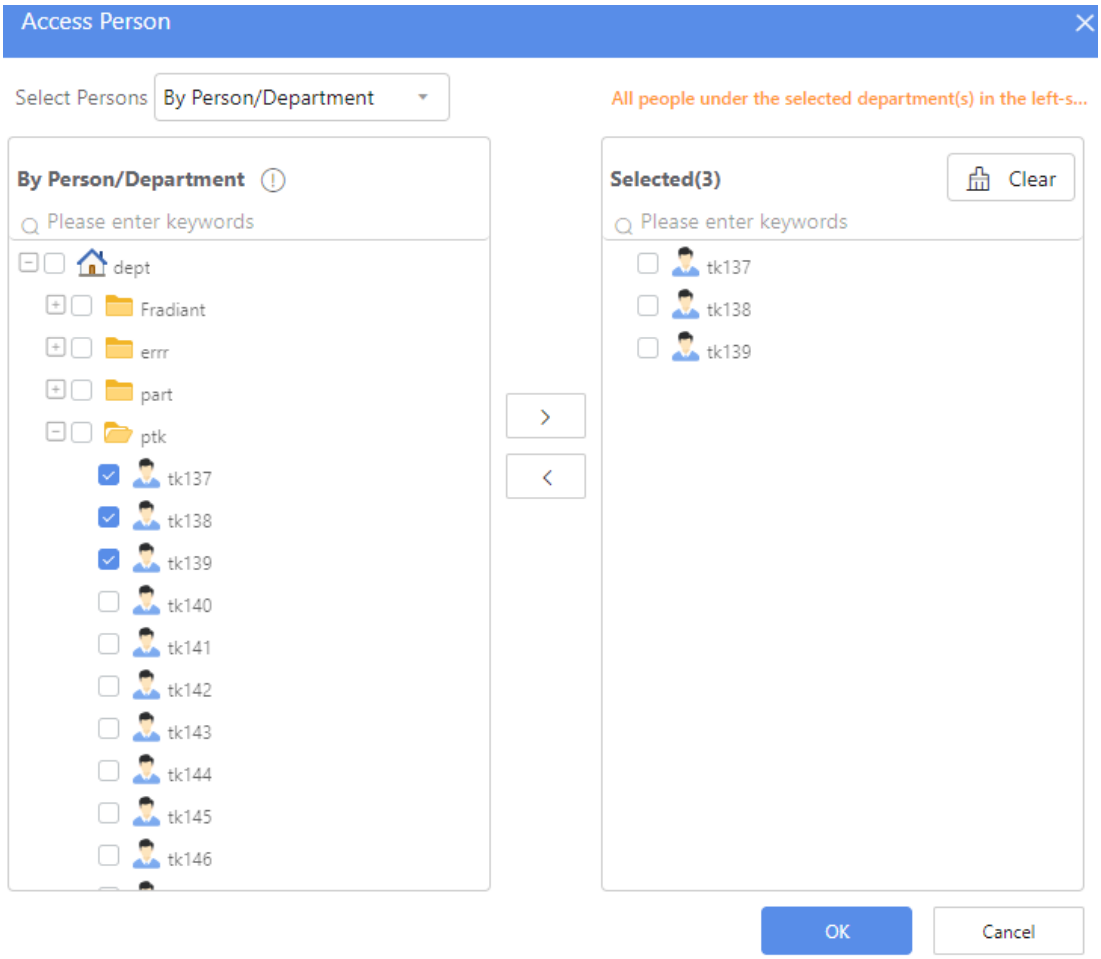
3. Add persons.

(1) Click **Add Person**.



(2) You can select persons **By Person/Department** or **By Building**. Select the persons you want to assign access permission to, and then click > to add them to the right-side list.

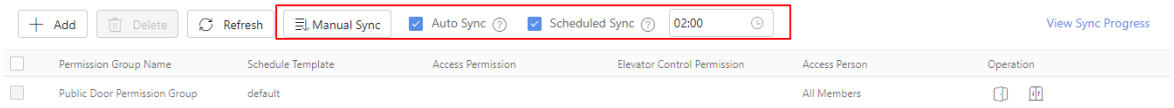
Note:
When **By Person/Department**, up to 200 people can be displayed for each department. People not displayed can be found by search, with up to 200 displayed.

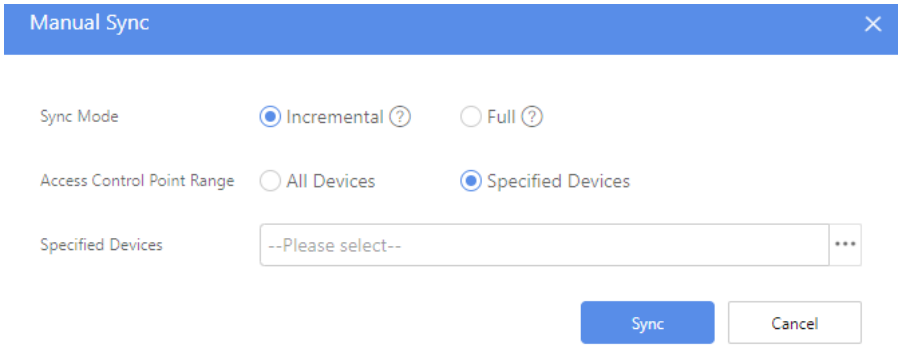


(3) Click **OK**.

Sync Permission Groups

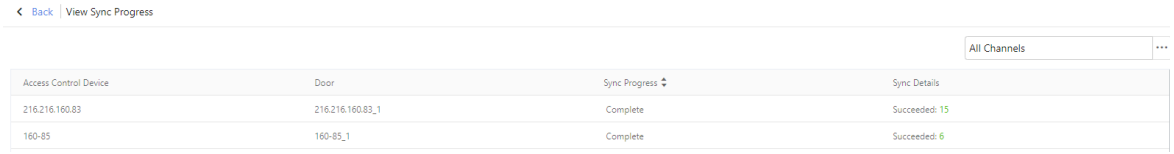
After adding a permission group, it is necessary to push personnel information to access control devices or elevator controllers. Personnel who have been synced will have access rights to the selected access control devices or elevator controllers.



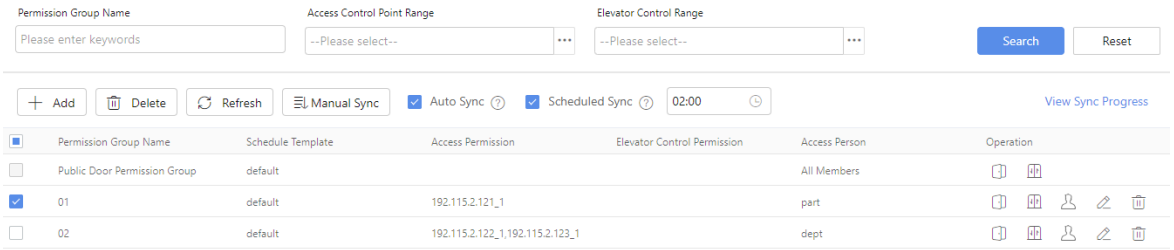
Auto Sync	Enabled by default. After selecting **Auto Sync**, the system will automatically sync incremental data for new or updated permission groups.
Scheduled Sync	Select **Scheduled Sync** and set a time. The system will sync the incremental data that have not been synced or have failed to be synced at the specified time.
Manual Sync	Click **Manual Sync**, select the sync mode and the access control point range, and click **Sync**.  • Incremental sync: Resync data that have not been synced or have failed to be synced. • Full sync: Resync all data, which will clear data synced by other platforms on the device, while retaining data added on the device.

If there are any failed syncs, the system will automatically retry at regular intervals until the sync succeeds.

View sync progress: Click **View Sync Progress** to view the sync progress and details by door.



Manage Permission Group



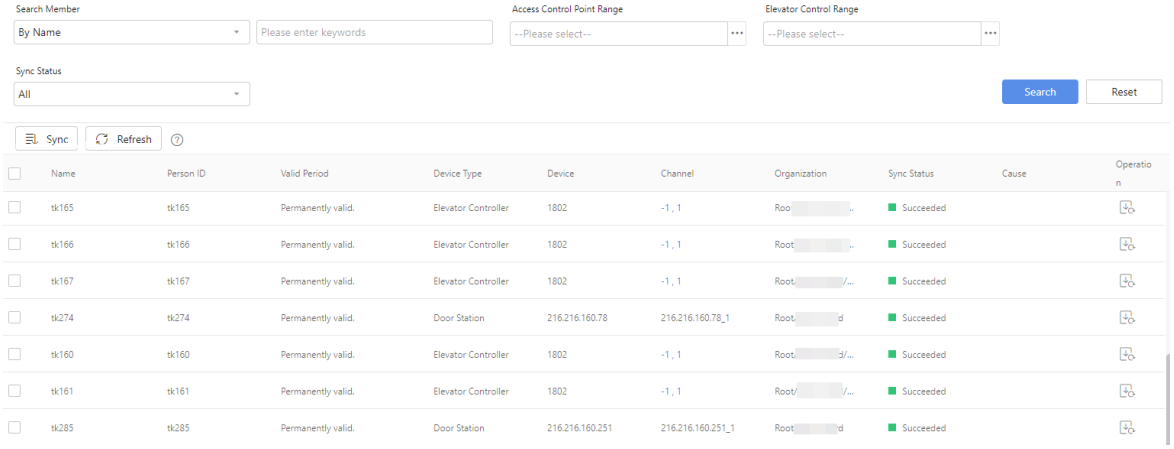
Note:
The system's default permission group can be modified for access control devices and elevator controllers but cannot be deleted.

- Edit access control points: Click in the **Operation** column to reselect the access control devices for the permission group.

- Edit elevator controllers: Click in the **Operation** column to reselect the elevator controllers for the permission group.
- Edit access persons: Click in the **Operation** column to reselect the access persons for the permission group.
- Edit permission group: Click in the **Operation** column to edit the permission group name or change a schedule template.
- Delete permission group: Click in the **Operation** column or select permission groups and click **Delete**.

15.1.3 Permission Search

View access permissions of persons. In normal situations, after configuring permission groups, personnel information will be automatically synced to access control devices and elevator controllers; in case of failed synchronization of personnel information, manual synchronization is also supported.



- Search: Select a search method (by name, by person/department, or by building) and enter keywords, set criteria including access control point(s), elevator controller(s), sync status (succeeded, failed, not synced) as needed, and then click **Search** to retrieve the detailed access permission information, such as valid period, access device, and sync status.

  Note:
  The validity period of permissions is determined by either the person's validity period or the resident's residency period. If someone's identity is both a person and a resident with different periods, the most recently updated period will take precedence.

- Sync to device:
  - Click for the record or select records and click **Sync**, all pending and failed data of the device associated with this record will be synced.
  - If no record is selected, all pending and failed data will be synced when you click **Sync**.

15.2 Remote Control

Go to **Access&Attendance** > **Access Control** > **Remote Control**.

Remotely controls access control channels (including face recognition terminals, door stations, zone stations, channels under access controllers, speed gate turnstile) to open/close door, keep open/closed, and restore.

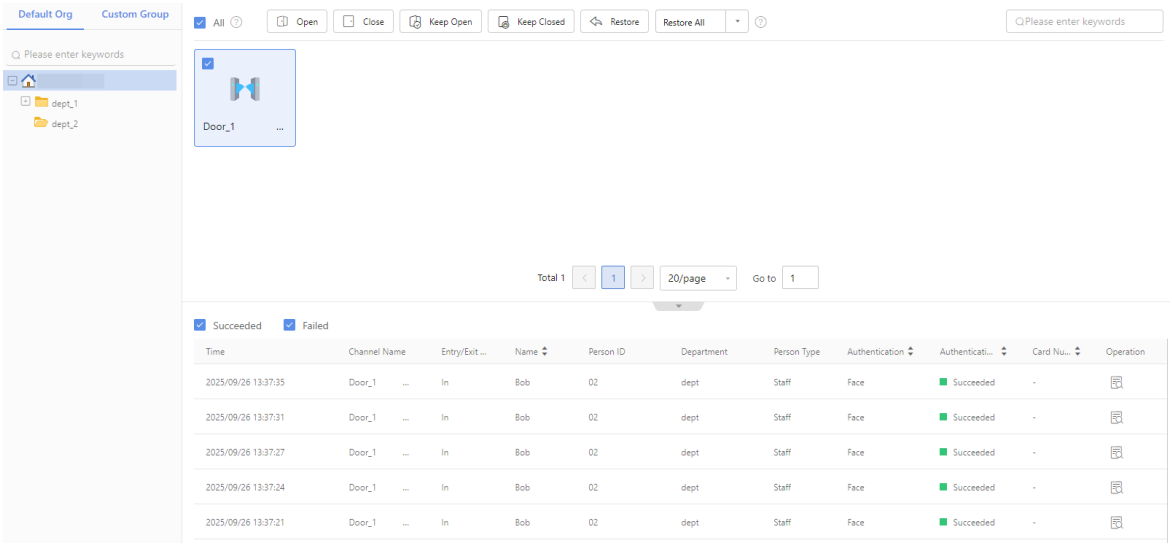
- Open: Temporarily opens the door for access. The door will automatically close after the person has passed through.
- Close: Manually closes the door.
- Keep Open: Opens the door and keeps it open until manually restored.
- Keep Closed: Closes the door and keeps it closed until manually restored. During this status, persons cannot open the door with verification.
- Restore: Cancels the Keep Open or Keep Closed status.

In scenarios such as emergencies or when someone lacks access permissions, the admin can, based on the actual situation (e.g., the access control area, number of channels, or the number of people), choose to: 1. select one or multiple channels for door control; 2. control all doors with one-click; 3. control doors in custom channel groups with one-click. Flexible channel group management and batch operations enhance response efficiency, allowing or denying access quickly.

15.2.1 By Default Organization

Manage access control channels by organization.

Go to **Remote Control** > **Default Org**. The upper-right side displays the access control channels in the organization, allowing you to perform door control operations on them. The lower-right side displays pass-thru records on access control channels.



Open/Close Door

Door control operations: Open, Close, Keep Open, Keep Closed, and Restore.

You can perform these operations on **online** access control channels one by one or in batches.

Control Selected Channels Only	1. Select access control channel(s). • Select All: Select **All** to select all online channels on the current page. • Custom Selection: Select online channels one by one or drag the mouse to select multiple channels from the right-side list. 2. Click **Open**/**Close**/**Keep Open**/**Keep Closed**/**Restore** above the right-side list to control the selected channels.
Control All Authorized Channels	Without selecting any channels, simply click **Restore All**/**Keep All Open**/**Keep All Closed** above the right-side list to control all authorized online channels in the system.

Pass-thru Records

Only the latest 20 pass-thru records are displayed. By default, the records are from all channels in the system. If you've selected any channels, only the records from the selected channels will be displayed.

- Filter: Select **Succeed** or **Failed** to view the corresponding pass-thru records.
- View Details: Click for a record to redirect to the **Pass-Thru Records** page to view the person's snapshot information.

15.2.2 By Custom Group

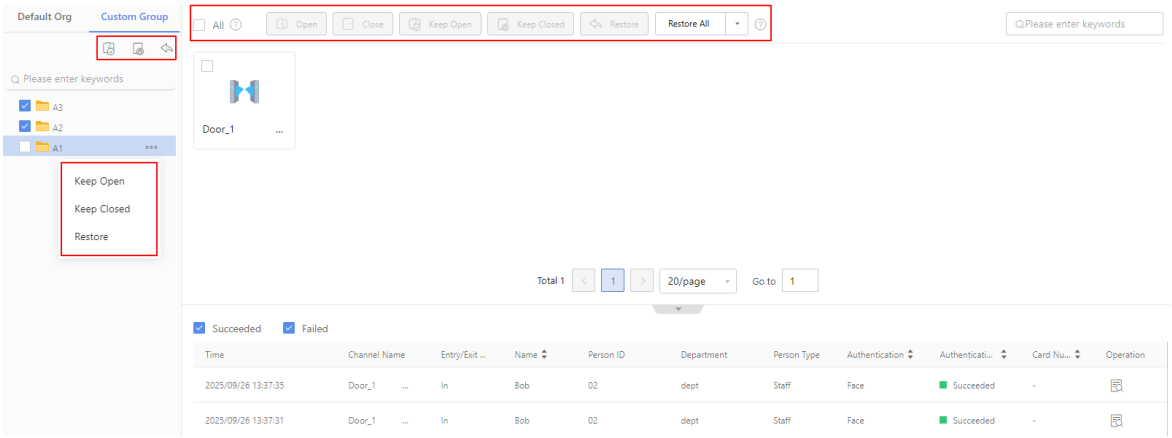
After adding access control channels into Custom Groups, you can perform door control operations on multiple channels by group with one-click.

Example: Add channels from multiple areas to an emergency group. In an emergency, you can quickly control all channels in the emergency group to open doors, allowing rapid access for people across different areas.

Go to **Remote Control** > **Custom Group**. The upper-right side displays the access control channels in the group, allowing you to perform door control operations on them. The lower-right side displays pass-thru records on access control channels.

Open/Close Door

Choose a method to control **online** access control channels:



Control Channels in Multiple Groups	Select groups from the left-side list, then click (Keep Open)/ (Keep Closed)/ (Restore) above the left-side list to control all online channels in the selected groups.
Control Channels in One Group	Click for a group, then click **Keep Open**/**Keep Closed**/**Restore** in the pop-up menu to control all online channels in the group.
Control Selected Channels Only	1. Select access control channel(s). • Select All: Select **All** to select all online channels on the current page. • Custom Selection: Select online channels one by one or drag the mouse to select multiple channels from the right-side list. 2. Click **Open**/**Close**/**Keep Open**/**Keep Closed**/**Restore** above the right-side list to control the selected channels.
Control All Authorized Channels	Without selecting any channels, simply click **Restore All**/**Keep All Open**/**Keep All Closed** above the right-side list to control all authorized online channels in the system.

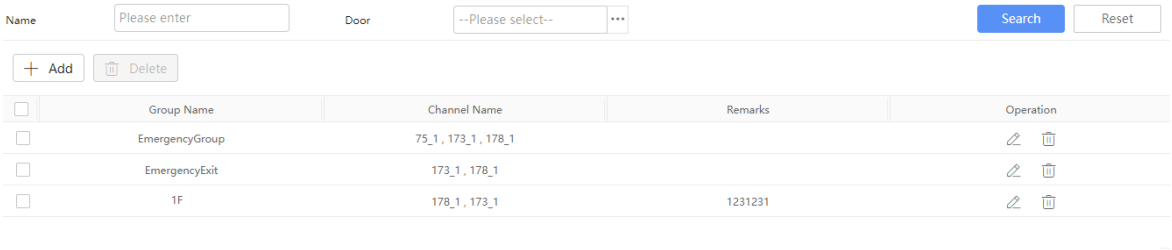
Pass-thru Records

Only the latest 20 pass-thru records are displayed. By default, the records are from all channels in the system. If you've selected any channels, only the records from the selected channels will be displayed.

- Filter: Select **Succeed** or **Failed** to view the corresponding pass-thru records.
- View Details: Click for a record to redirect to the **Pass-Thru Records** page to view the person's snapshot information.

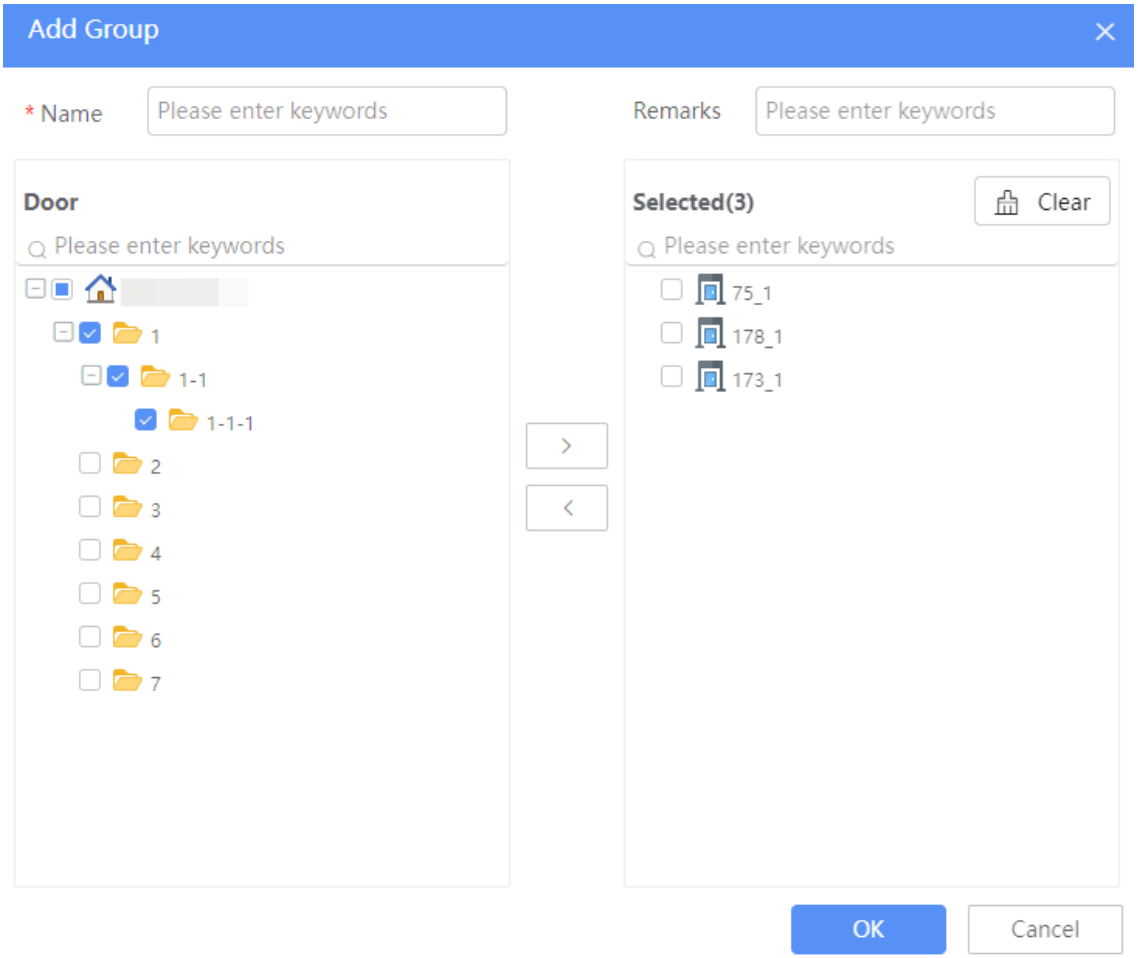
15.2.3 Custom Group Configuration

Go to **Remote Control** > **Custom Group**. You can group access control channels, which facilitates performing door control operations By Group.



Add Group

1. Click **Add**.



2. Enter a custom group name and remarks.
3. Select organization(s)/access control channel(s) from the left-side list, then click › to add them to the selected channel list.
4. Click **OK**.

Group Management

- Search: Search groups by group name and access control channel.
- Edit: Click for a group to edit the group name and channels in it.
- Delete: Click for a group or select group(s) and click **Delete**.

15.3 Access Control Configuration (Access Controller & Speed Gate & Turnstile)

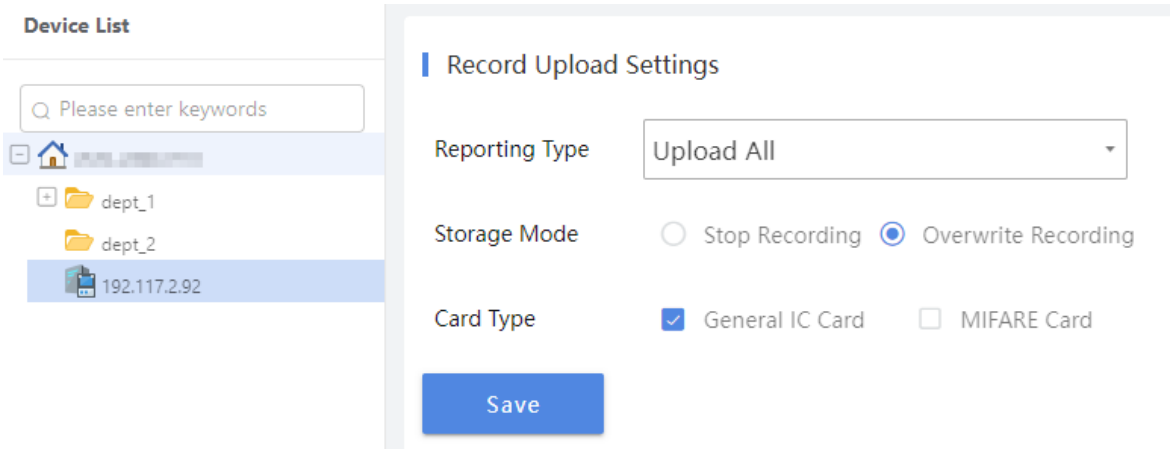
Go to **Access Control > Access Control > Access Control Config**.

Configure the parameters of the access controller, speed gate or turnstile device itself.

Note:
The functions described in this section can also be configured via the device's web interface. The UI display may vary with device version. For any discrepancies, please refer to the device's user manual.

15.3.1 Device Parameter Configuration

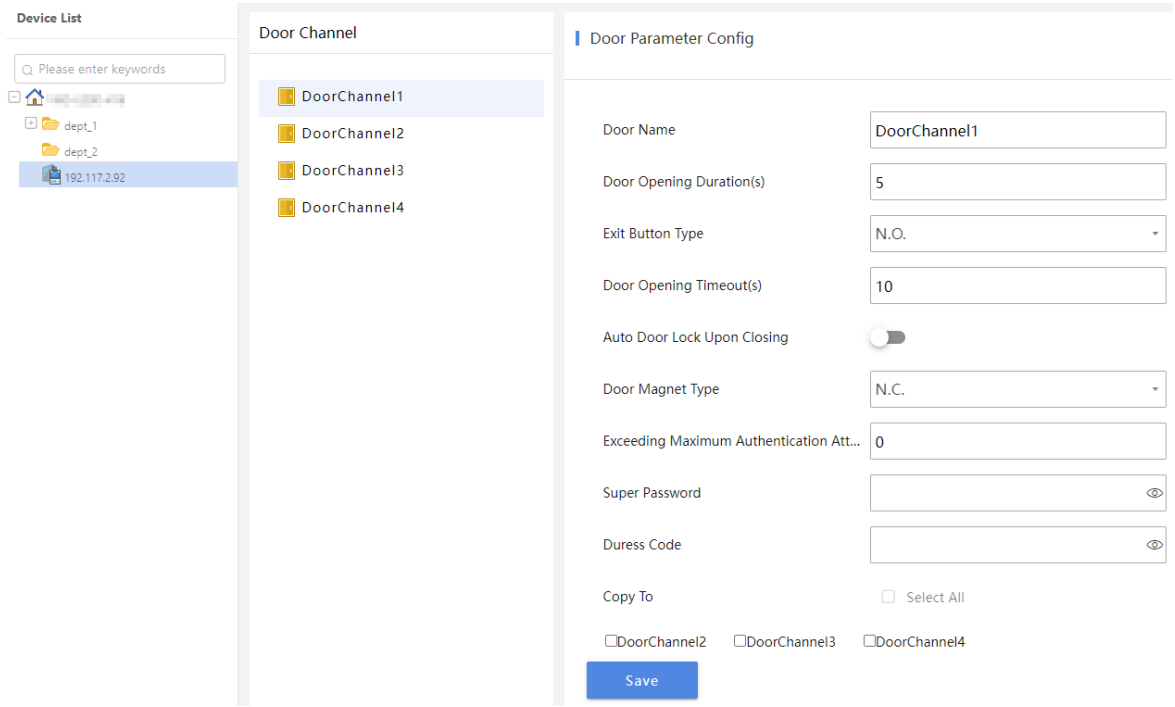
Select the access control device from the device list to configure how it handles verification records.



Reporting Type	For access control verification records: • Upload All: Includes both successful and failed verification records. • Upload Successful Records
Storage Mode	When verification records reach the device's storage limit: • Stop Recording: Stops receiving new records. • Overwrite Recording: New records overwrite the earliest records.
Card Type	Select the card type supported by the access control device for verification (General IC Card, MIFARE Card). Single choice. MIFARE cards allow key configuration to encrypt sectors and prevent card data leakage.

15.3.2 Door Parameter Configuration

In the device list, select the access control device to configure the opening and closing parameters for the door channel.

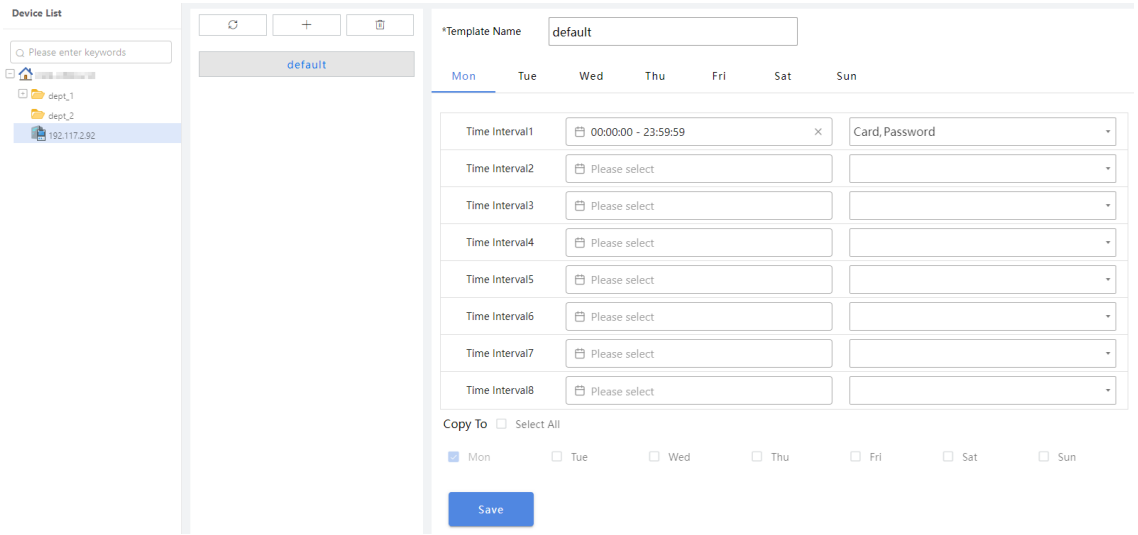


Parameter	Description
Door Name	Enter a custom name. Door names under the same access control device should be unique.
Door Opening Duration	The duration for a single door opening operation. The door will automatically close after this set time elapses.
Exit Button Type	Select based on the type of the connected button. • N.O. (Recommended): Circuit is open when the door is closed; pressing the button closes the circuit and triggers opening. • N.C.: Circuit is closed when the door is closed; pressing the button opens the circuit and triggers opening.
Door Opening Timeout	An alarm will be triggered if the door remains open beyond the set time. Set to 0 to disable this alarm.
Auto Door Lock upon Closing	The door lock will engage immediately after closing, even if the set lock action time has not been reached.
Door Magnet Type	Select based on the type of the connected door lock. • N.O.: Connected to an electric strike lock. Circuit is open when the door is closed and closed when the door is open. • N.C.: Connected to an electromagnetic lock. Circuit is closed when the door is closed and open when the door is open.
Exceeding Maximum Authentication Attempts	An alarm will be triggered when consecutive failed card swipe attempts reach the set value. Set to 0 to disable the alarm. If Alarm Linkage Configuration is completed, a corresponding alarm action will be triggered.
Super Password	This password can open the door with any verification method. Do not disclose the password.
Duress Code	When under coercion, entering this code will open the door and the device will report a duress event to the platform.
Copy To	Select other door channels to copy the current configuration to the selected door channels upon saving.

15.3.3 Verification Template Configuration

Verification templates define how the device performs verification during different time periods. Pre-configuring templates allows you to bind them to multiple door channels separately, enabling quick deployment of verification methods.

1. Select an access control device from the device list to view the configured verification template.
   The system includes a pre-set default verification template that is active 24/7; it can be modified but not deleted.



2. Click + to add a template, or select an existing template to modify it.

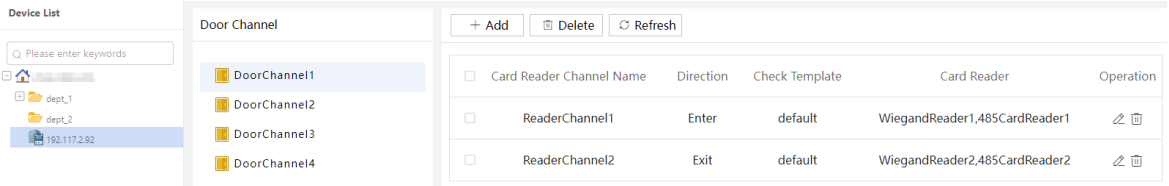
Time Period	Time periods on the same day cannot overlap.
Verification Method	Multiple verification methods can be selected simultaneously. • Card: Verification is successful when the swiped card number matches the number assigned to the person in the library. • Password: Verification is successful when the entered password is correct. • Card+Password: Verification is successful when the card number matches AND the password is correct.
Copy To	After setting the verification method for a specific day, select other dates to copy the current settings to them upon saving.

3. Click **Save**.

15.3.4 Door Verification Configuration

Bind card readers to door channels and assign verification templates to the card readers.

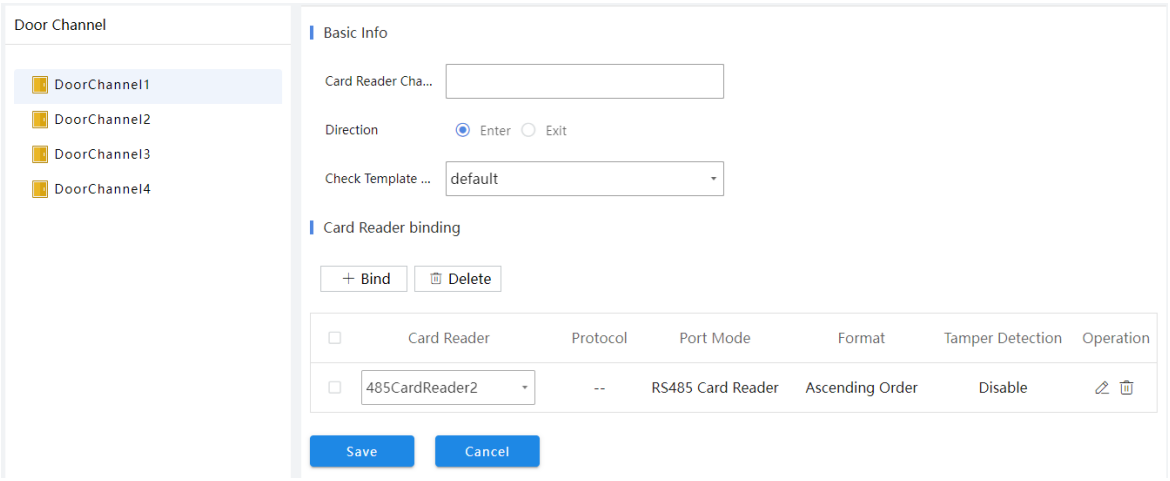
Select an access control device from the device list, then select a door channel to view its card readers (by default, one entry and one exit reader are pre-configured; parameters can be modified as needed).



Add Card Reader Channel

The card reader must be physically connected to the Wiegand or RS-485 interface on the access control device.

Click **Add**, configure the settings according to the table below, then click **Save**.



Card Reader Channel Name	Enter a custom name.
Direction	Enter or exit.
Check Template Binding	Select a Verification Template.
Card Reader Binding	Click **Bind** and select the card reader type (Wiegand or RS-485) based on the actual wiring. Click the corresponding to the card reader to modify its protocol parameters.

Modify Reader

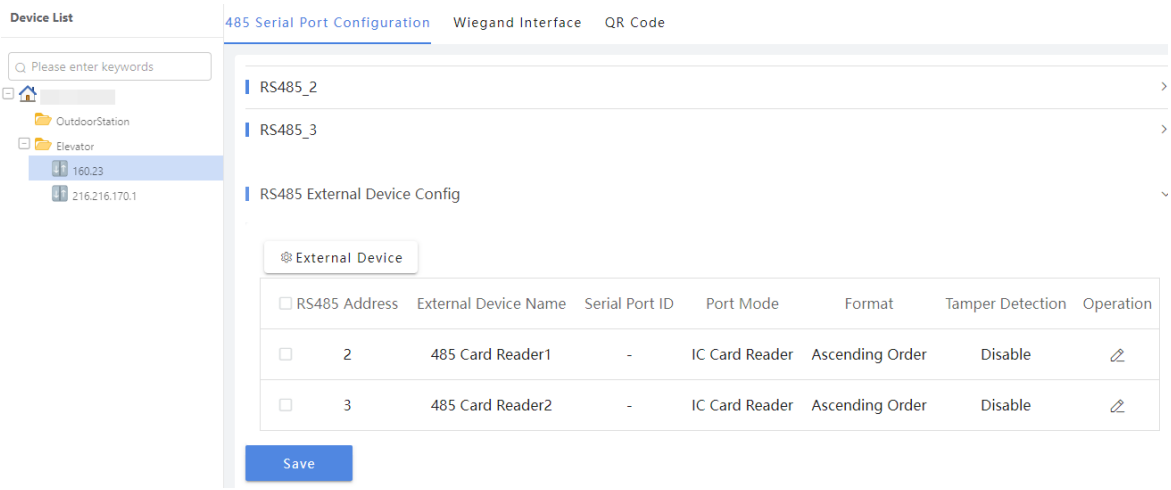
Click the corresponding to the card reader channel to modify parameters such as its verification template and bound devices.

Delete Reader

Click the corresponding to the card reader channel and confirm the deletion.

15.3.5 External Device Configuration

485 Serial Port Configuration



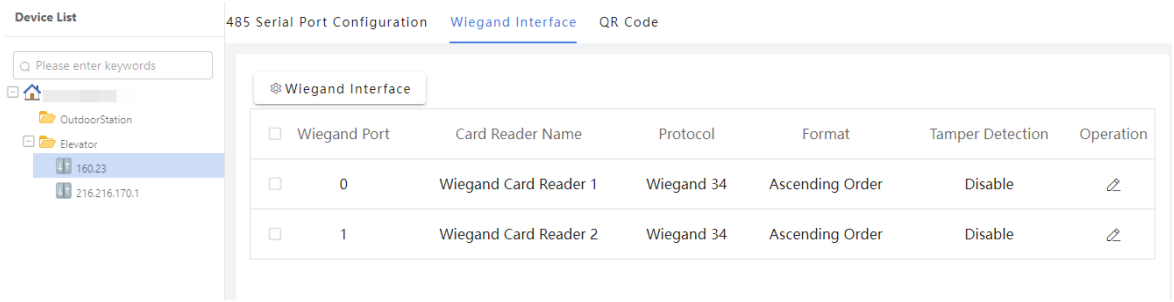
- Modify the data transmission parameters for RS485_2 and RS485_3; generally, using the system default values is sufficient.
- Configure the card readers connected to RS485_2 and RS485_3.

Parameter	Description
Card Reader Name	Enter a unique custom name.

Parameter	Description
Port Mode	• Disable: The port mode is disabled. • IC card reader: Connects an IC card reader. • QR code reader: Connects a QR code reader.
Port Number	When the serial port mode is set to QR code reader, this parameter must be configured and must be unique.
Format	• Ascending order: The card number sequence is the same as the sequence read by the card reader • Descending order: The card number sequence is the reverse of the sequence read by the card reader.
Tamper Detection	When enabled, an alarm will be triggered when card reader tampering is detected.
Copy To	Used to apply the same settings to other card readers.

Wiegand Interface Configuration

Configure the card reader connected to the Wiegand interface.

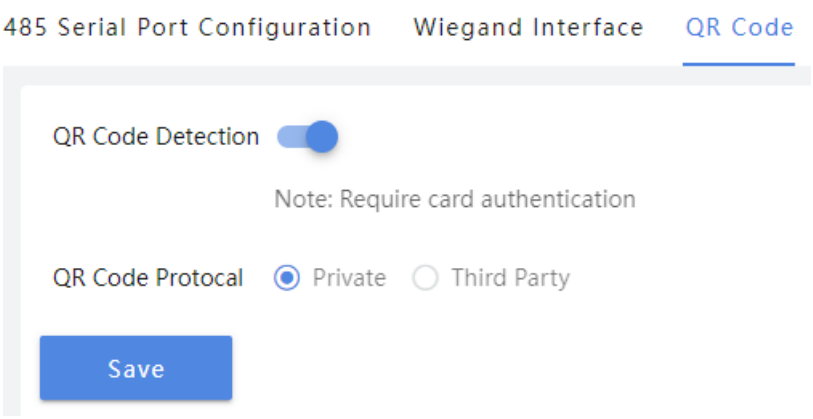


Parameter	Description
Card Reader Name	Enter a unique custom name.
Protocol	• Wiegand 26: Card numbers are read using the Wiegand 26 protocol (only reads 3-byte card numbers). • Wiegand 34: Card numbers are read using the Wiegand 34 protocol (only reads 4-byte card numbers). • Custom Wiegand: Protocols used by Wiegand card readers other than 26 and 34 (configuration rules need to be set in the device interface).
Format	• Ascending order: The card number sequence is the same as the sequence read by the card reader • Descending order: The card number sequence is the reverse of the sequence read by the card reader.
Tamper Detection	When enabled, an alarm will be triggered when card reader tampering is detected.
Copy To	Used to apply the same settings to other card readers.

QR Code Configuration

With QR code detection enabled, in the card number verification mode, personnel can scan the card number QR code on a QR code reader for verification.

Note:
The platform currently does not support generating card number QR codes.

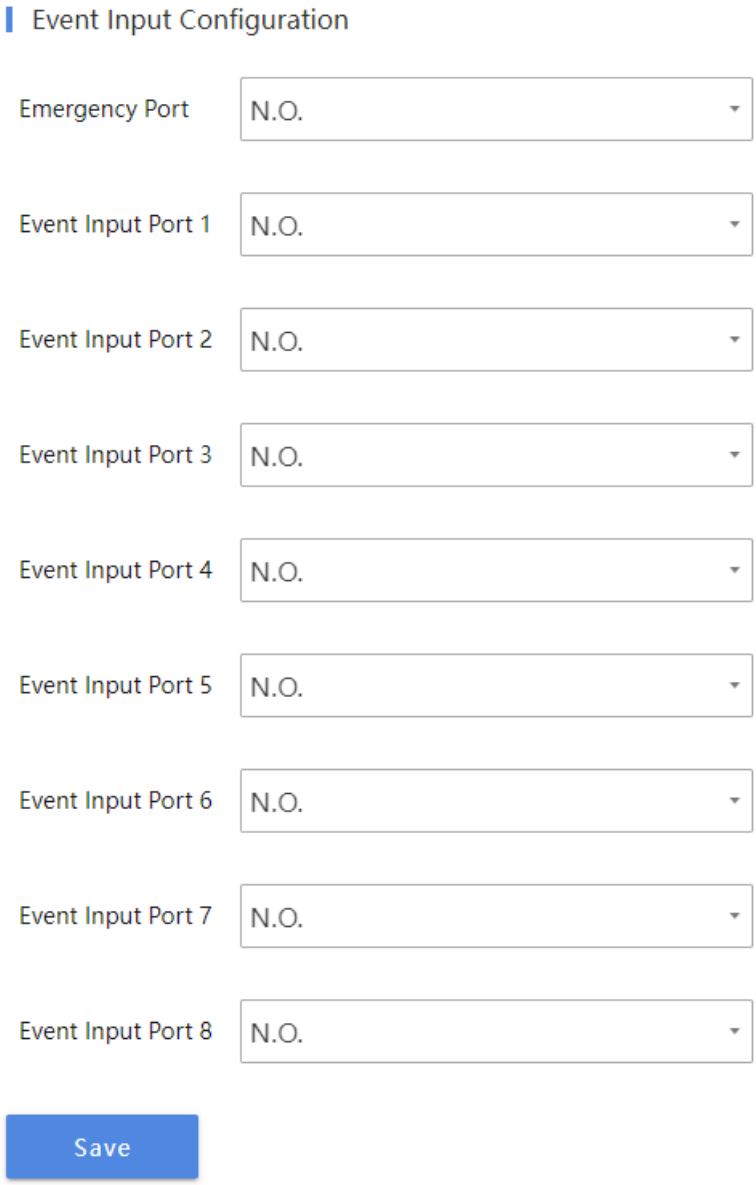


15.3.6 Event Input Configuration

After an alarm detector is connected to the access control device, the event input interface status can be configured according to the **detector's operation mode**.

- N.O.: In the default state, the circuit between the alarm detector and the access control device is open. When an abnormal event is detected, the circuit closes and the access control device reports an alarm.
- N.C.: In the default state, the circuit between the alarm detector and the access control device is closed. When an abnormal event is detected, the circuit opens and the access control device reports an alarm.

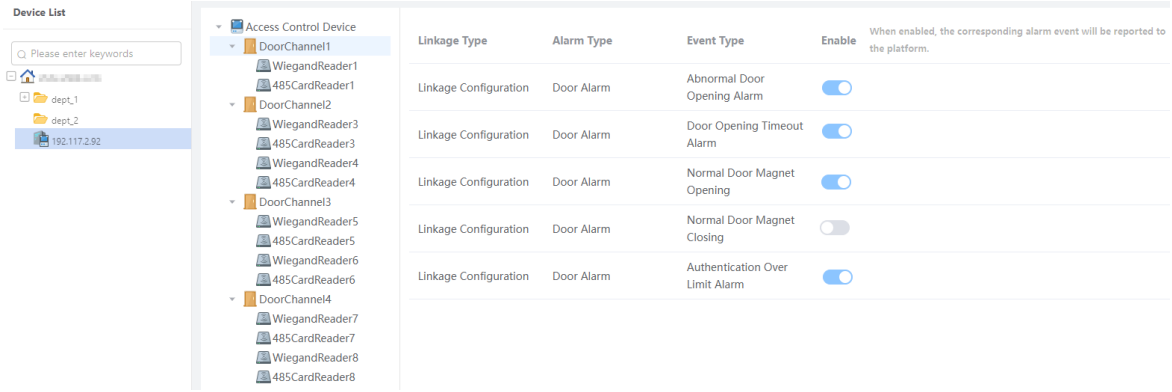
Note:
The number of interfaces varies among different models of access control devices. Please refer to the UI for accurate information.



15.3.7 Alarm Report Configuration

Configure whether access control devices, door channels, and card readers report alarms to the platform.

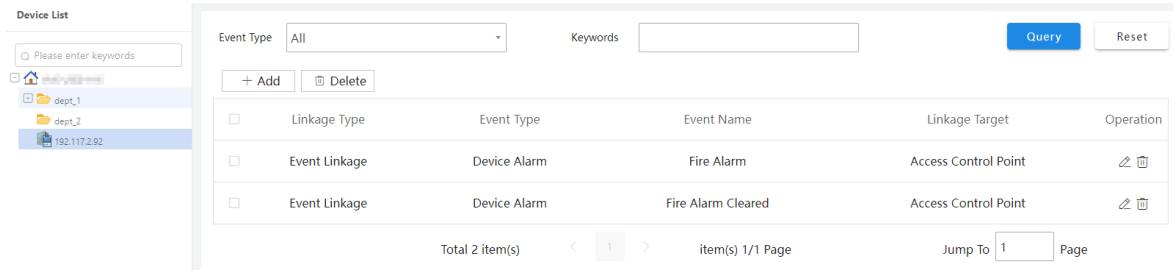
Note:
Please subscribe to alarms from the corresponding devices on the User Subscription page on the platform.



1. Select an access control device, door channel, or card reader on the left to view its corresponding event types. **The event types for these three** are different and should be configured separately.
2. Click to enable alarm reporting; click to disable alarm reporting.

15.3.8 Alarm Linkage Configuration

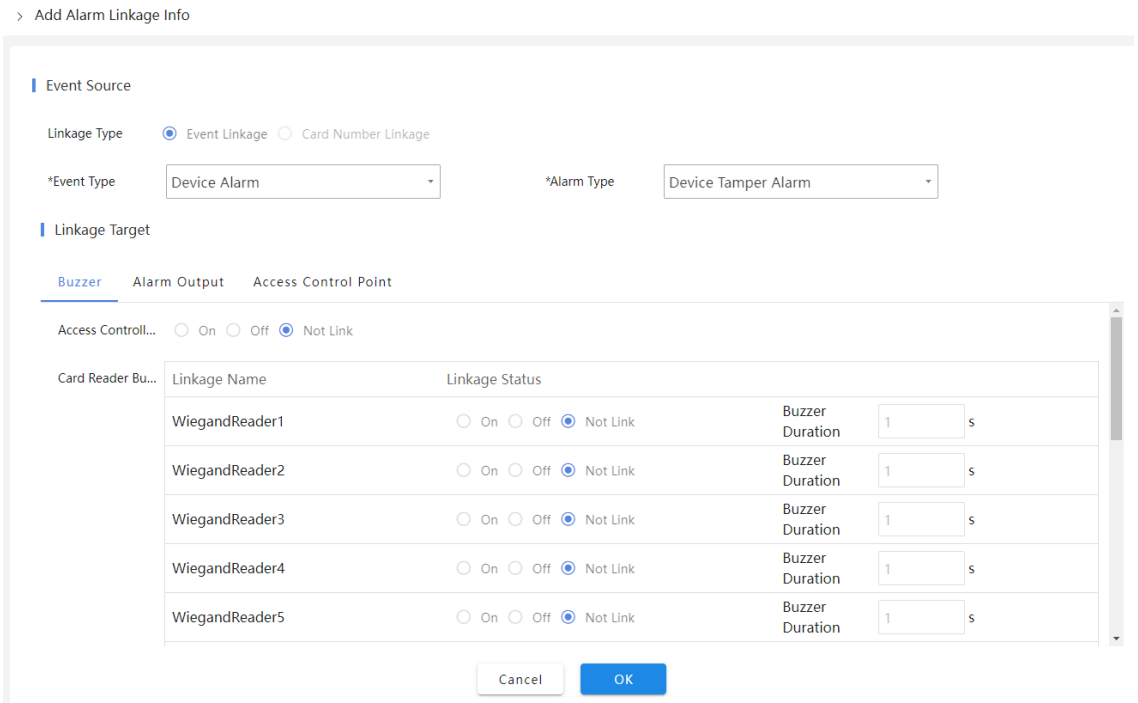
When specific events occur, the linked access control device will perform a series of actions. For example: when an alarm is triggered, the access control controller will sound a buzzer and open the door.



Add Linkage Configuration

Up to 30 linkage configurations can be added (including 2 default configurations: fire alarm keeps the door open, fire alarm cleared closes the door).

1. Click **Add** to go to the page as shown below. Currently, only **Event Linkage** is supported as the linkage type.



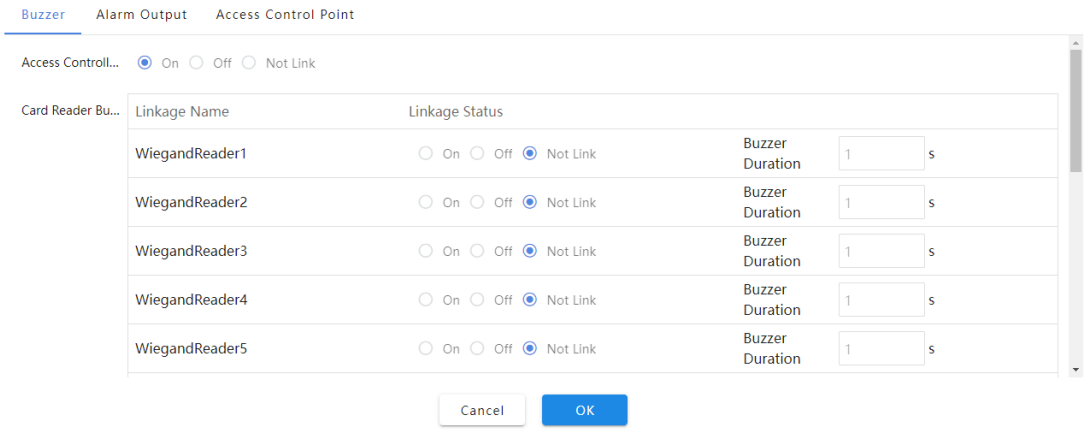
2. Select the event type and the corresponding alarm type.

Event Type	Alarm Type	Description
Device Alarm	The access control device itself triggers alarms.	
	Device Tamper Alarm	The access controller is opened.
	Fire Alarm	Fire hazards such as smoke or flames are detected.
	Device Tamper Alarm Cleared	The device tamper alarm stops.
	Fire Alarm Cleared	The fire alarm stops.
Door Alarm	Alarms triggered by doors connected to the access controller. If this type is selected, please also specify the corresponding door channel. To configure alarm linkage for multiple door channels, add them one by one.	
	Door Magnet Alarm	Alarm triggered by an unconventional door opening signal.

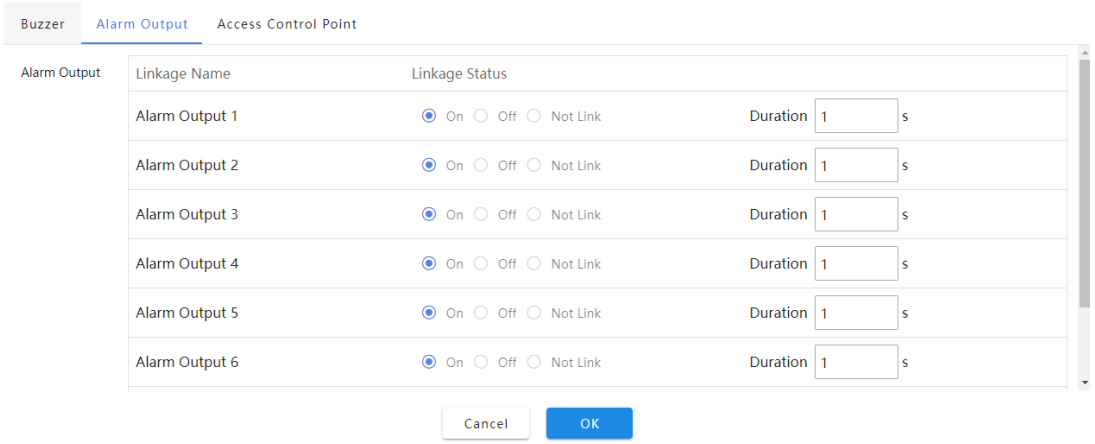
Event Type	Alarm Type	Description
	Door Opening Timeout Alarm	Alarm triggered when the door remains open beyond the timeout period set in door parameter configuration.
	Normal Door Magnet Opening Alarm	Door is opened normally via the magnetic sensor.
	Normal Door Magnet Closing Alarm	Door is closed normally via the magnetic sensor.
	Authentication Over Limit Alarm	Alarm triggered when the number of consecutive failed card swipes reaches the set limit.
Card Reader Alarm	Alarms triggered by card readers connected to the access control device. If this type is selected, please also specify the corresponding card reader and event input port. To configure alarm linkage for multiple card readers and input ports, add them one by one.	
	Card Reader Tamper Alarm	The card reader enclosure is opened.
	Duress Alarm	A duress code is used to unlock the door.
	Unauthorized List Alarm	An alarm triggered when an unauthorized person swipes a card.
	Card Reader Tamper Alarm Cleared	The card reader tamper alarm stops.
Event Input Alarm	Only applicable to pedestrian speed gates or turnstiles. Event alarms triggered by alarm detectors connected to the access control device.	
	Event Input Alarm	Event detected
	Event Input Cleared	Event cleared

3. Set linkage targets.

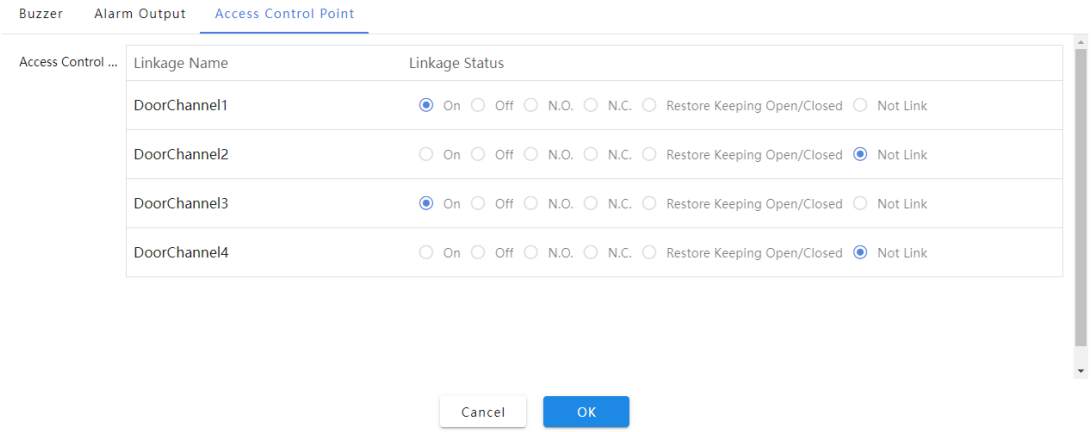
- **Buzzer**: Can trigger the access controller itself or externally connected card readers to beep. Linkage status includes **On** (activate buzzer), **Off** (deactivate buzzer), **Not Link** (no linkage).



  - Access controller buzzer: The access controller itself emits a beep. The built-in buzzer sounds 30 times, and the buzzer duration cannot be configured.
  - Reader buzzer: A card reader physically connected to the access controller emits a beep. After selecting **On** as the linkage state, the buzzer duration must be set.
- **Alarm Output**: If output devices such as alarm lights are connected, alarm output linkage can be configured. Linkage status includes **On** (activate alarm output), **Off** (deactivate alarm output), **Not Link** (no linkage).
  After selecting **On** as the linkage state, the alarm output duration must be set.



- **Access Control Point**: The linkage status includes **On** (activate), **Off** (deactivate), **N.O.** (keep open), **N.C.** (keep closed), **Restore Keeping Open/Closed** (cancel keeping open/closed).



4. Click **Save**.

15.4 Advanced Configuration

Go to **Access&Attendance** > **Access Control** > **Advanced Configuration**.

Configure advanced verification rules for access control.

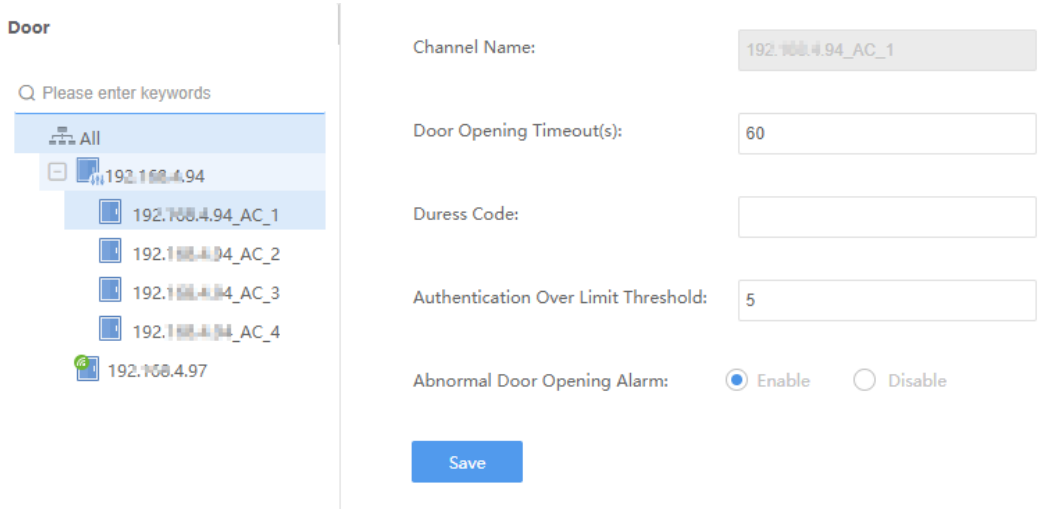
15.4.1 Door Channel Configuration(General Access Control)

Go to **Access Control** > **Advanced Configuration**>**Door Configuration**.

Note:
Only **general access control devices** support this configuration.

Configure abnormal door opening alarm parameters. When the door is opened abnormally, an alarm will be reported to the platform.

Select an general access control device in the Door list and configure it.



Item	Description
Door Opening Timeout(s)	After being set, if the door open duration has reached the limit, a door opening timeout alarm will be reported.
Duress Code	Set the duress code (0-8 digits). If an abnormal situation occurs, people can open the door using the duress code and the access control will trigger a duress alarm.
Authentication Over Limit Threshold	After being set, if the number of failed attempts to open the door has reached the threshold, an authentication over limit alarm will be reported.
Abnormal Door Opening Alarm	When enabled, an alarm will be reported when the door is opened abnormally.

15.4.2 Multi-Factor Authentication (Access Controller & Speed Gate & Turnstile)

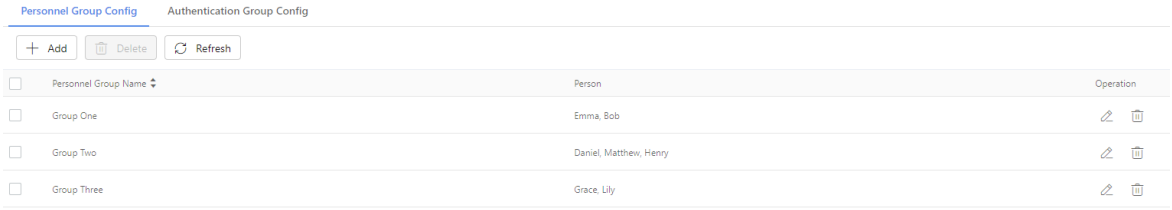
Multi-factor authentication is an access control mechanism that requires multiple individuals to be present simultaneously and all authenticate successfully before access is granted. This mechanism is commonly used in high-security locations (e.g., banks, warehouses), leveraging mutual supervision among on-site personnel to ensure the safety of funds, valuables, important documents, etc., within the premises.

Multi-factor authentication requires the configuration of personnel groups (assign multiple individuals with the same identity into a group), authentication groups (configure the door channel, personnel groups requiring simultaneous authentication, and effective time slots).

For example: If an authentication group is configured with two personnel groups: Group A requires at least 2 individuals present simultaneously, and group B requires at least 3 individuals present simultaneously. The door will only unlock after both groups successfully complete verification in sequence.

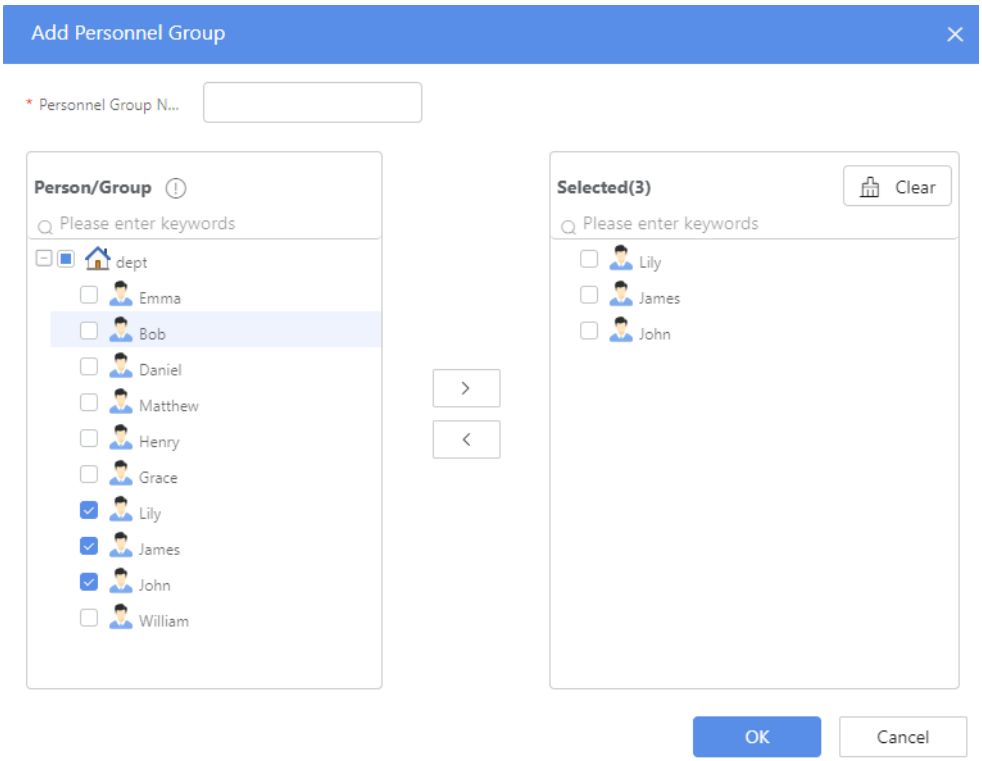
15.4.2.1 Personnel Group Configuration

Group individuals with the same identity to facilitate the selection of personnel groups when configuring authentication groups, enabling rapid configuration of authentication rules.



Add Personnel Group

1. Click **Add**.



2. Enter the group name, and select personnel.

   Note:
   Each personnel group allows up to 100 people.

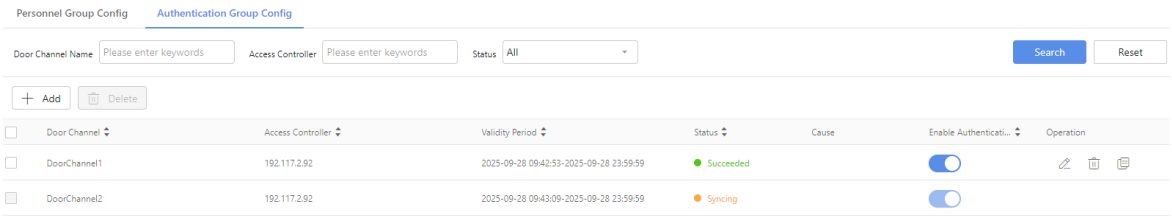
3. Click **OK**.

Personnel Group Management

- Edit: Click to change the group name and personnel.
- Delete: Click , or select personnel groups, and then click **Delete**.

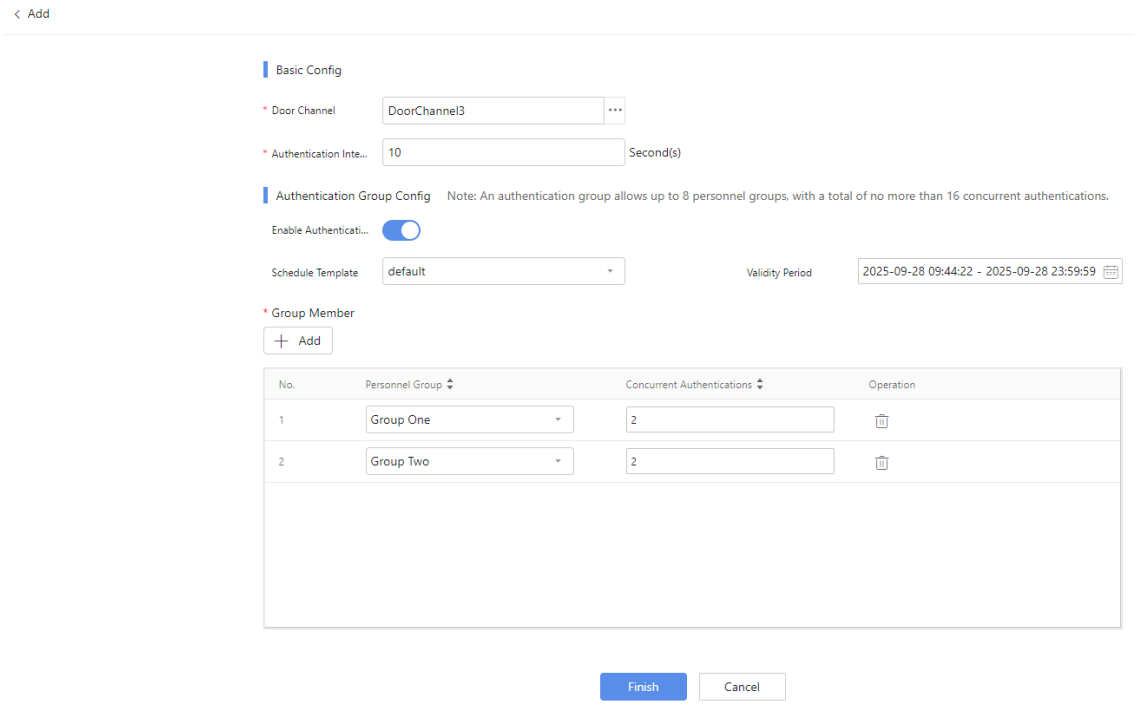
15.4.2.2 Authentication Group Configuration

An authentication group consists of door channels, personnel groups, and validity periods. Multiple personnel must successfully pass verification simultaneously at the door channel before the door can be opened.



Add Authentication Group

1. Click **Add**.



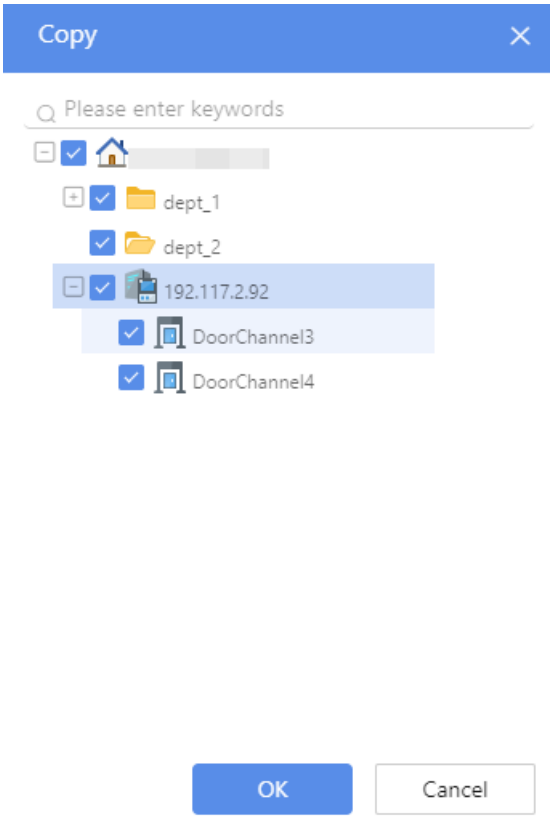
Parameter	Description
Door Channel	Select a channel under the access controller/speed gate or turnstile (single selection only). **Note:** Each channel can only be assigned to one authentication group. Channels already assigned to an authentication group will not be displayed in the device list.
Authentication Interval	All required personnel must complete authentication within a specified time interval of N seconds. Authentication is considered invalid if this interval is exceeded, and the process must be restarted.
Enable Authentication Group	The authentication group will only take effect after being enabled. If immediate activation is not required, you may choose not to enable it now and modify this setting later.
Schedule Template	Select a Schedule Template to set the daily access permission effective time.
Validity Period	Set the active time period for the authentication group. **Note:** If the authentication group is outside its validity period, all verification attempts will fail.
Authentication Group Members	(1) Click **Add** to add a personnel group. (2) Select personnel groups. For each personnel group, specify the number of individuals required to authenticate simultaneously (this number must be less than or equal to the total members in the group). **Note:** An authentication group can contain up to 8 personnel groups, and the total number of people that require simultaneous authentication across all groups cannot exceed 16.

2. After completing the configuration, click **Finish**.
   The system will automatically sync the authentication group information to the door channels.

Authentication Group Management

For successfully synced authentication groups, the following operations are supported:

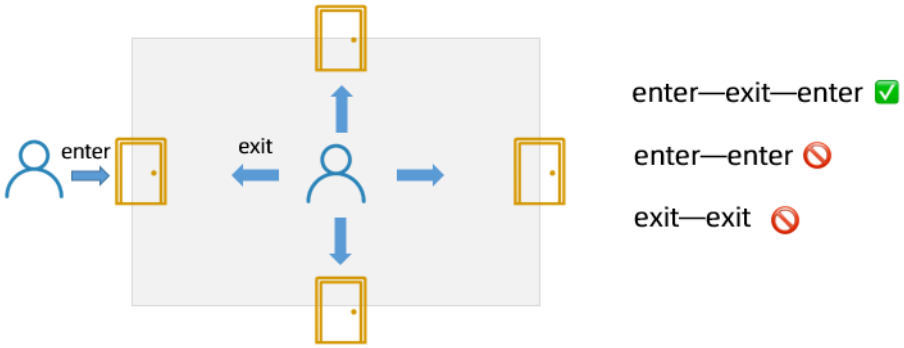
- Enable/Disable: Click to enable; click to disable. The group will be re-synced after status modification.
- Edit: Click to modify authentication group information. The updated configuration will be re-synced after the modification.
- Delete: Click , or select authentication groups and click **Delete**.
- Copy: Click to open the door channel list. Select target door channel(s) to copy the current authentication group configuration. The corresponding authentication group(s) will be created in the list.



15.4.3 Anti-Passback (Access Controller & Speed Gate & Turnstile)

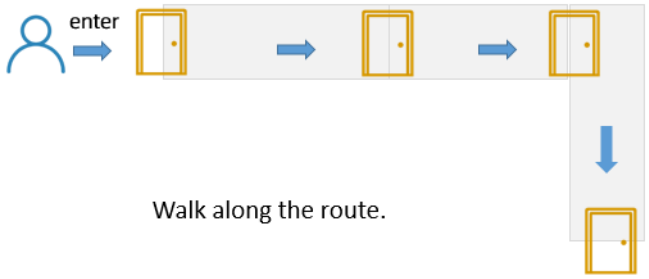
Anti-passback includes two types of rules:

- **Area anti-passback**: Card swipe records must strictly follow an "in-out" or "out-in" sequence.
  Example: If a premises has an entrance and an exit, a person who has entered but not yet exited will be unable to enter again through the entrance (prevents multiple individuals using one card). The same logic applies to the exit.



- **Route anti-passback**: Individuals must swipe their cards at readers in a specified sequence.

Example: If personnel are required to enter a warehouse in the order of Door A → Door B → Door C, they will be unable to proceed to the next door if they bypass any door (tailgating) or re-authenticate at a door that has already been passed (proxy authentication).



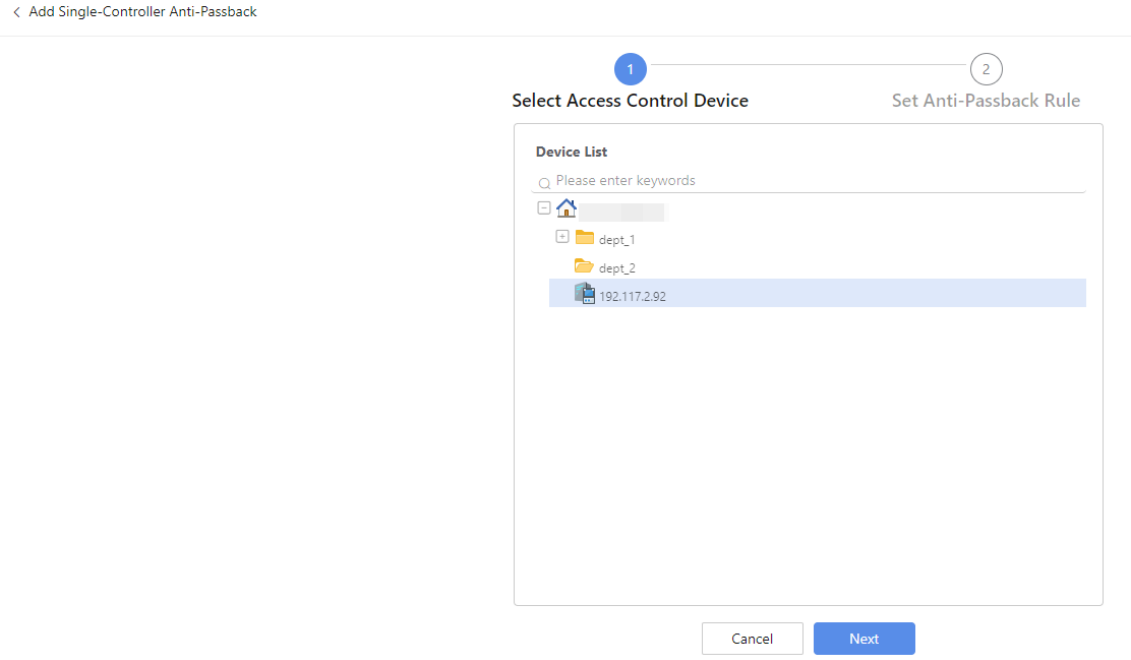
The system supports both single-controller anti-passback (configure rules for door channels under a single access controller) and cross-controller anti-passback (configure rules for door channels across multiple access controllers).

15.4.3.1 Single-Controller Anti-Passback

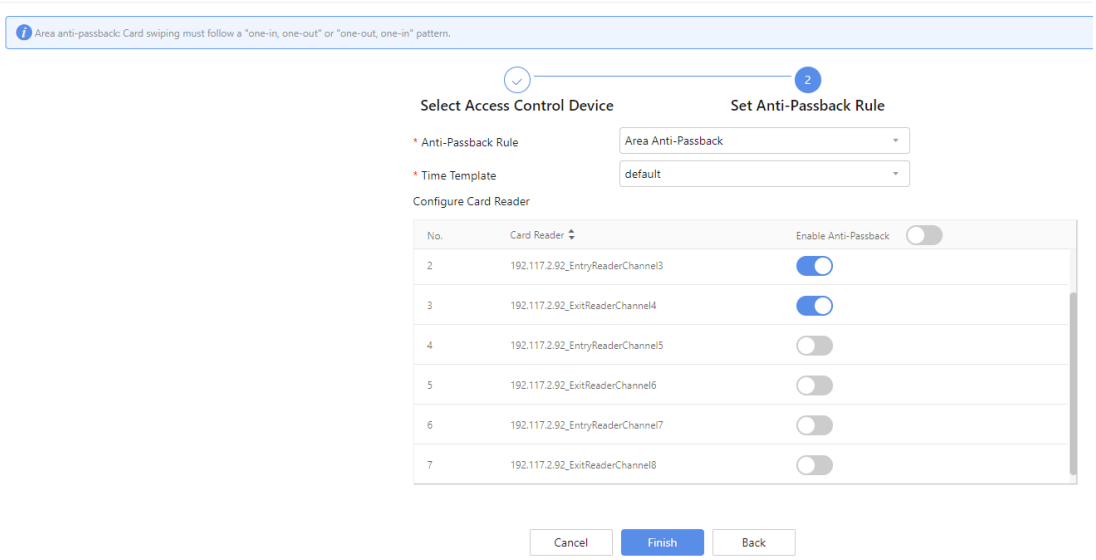
Configure area anti-passback or route anti-passback for door channels under a single access controller.

Add New Rule

1. Click **Single-Controller Anti-Passback**.
2. Select an access controller/speed gate or turnstile, then click **Next**.

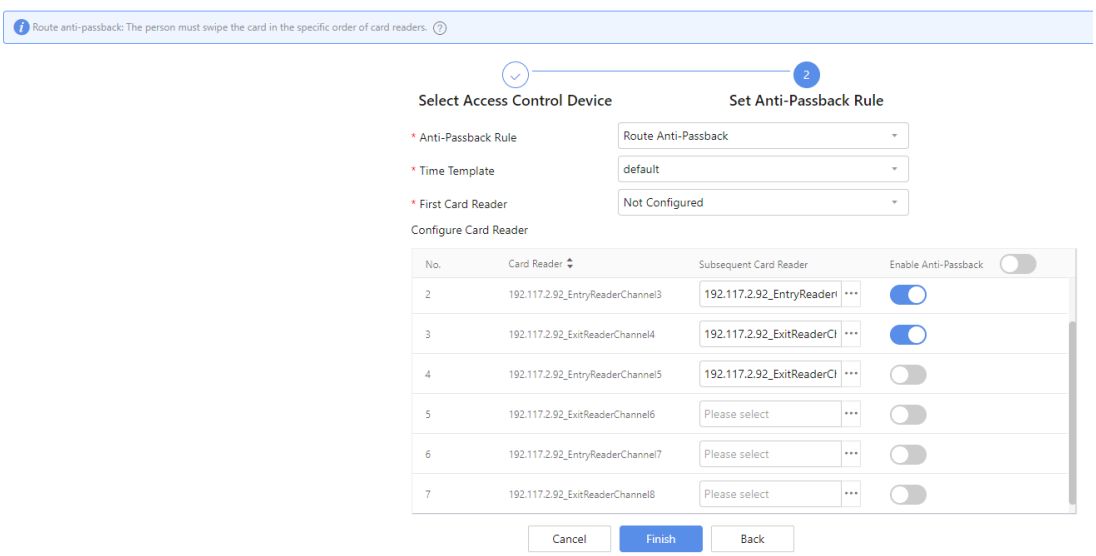


3. Configure the anti-passback rule.
   - Area anti-passback



Parameter	Description
Time Template	Select a Schedule Template to define the daily access permission effective time.
Configure Card Reader	Enable at least one entry card reader and one exit card reader. If multiple card readers are enabled, personnel may enter through any entry reader and exit through any exit reader. **Note:** The first authentication does not distinguish between entry and exit directions. After the initial successful authentication, subsequent verifications will perform anti-passback validation based on the previous entry/exit direction.

- Route anti-passback



Parameter	Description
Time Template	Select a Schedule Template define the daily access permission effective time.

First Card Reader	• First card reader not set: Card swiping can start from any card reader in the route.
	  • Non-closed routes (e.g., 1-2-3-4): Each person can pass through only once.
	  • Closed routes (e.g., 1-2-3-4-1): The same person can pass through multiple times.

Parameter	Description
	• First card reader set: Card swiping must start from the first card reader. Personnel may exit from any reader in the route and restart from the first reader at any time (e.g., for route 1-2-3-4, sequence 1-2-3-1 is also allowed).
Configure Card Reader	(1) Select subsequent card readers (multiple selections allowed) to form the route. (2) All readers in the route must have anti-passback enabled; otherwise, subsequent segments of the route will not function properly.

4. Click **Finish** to save and automatically sync the rule to the access control device.

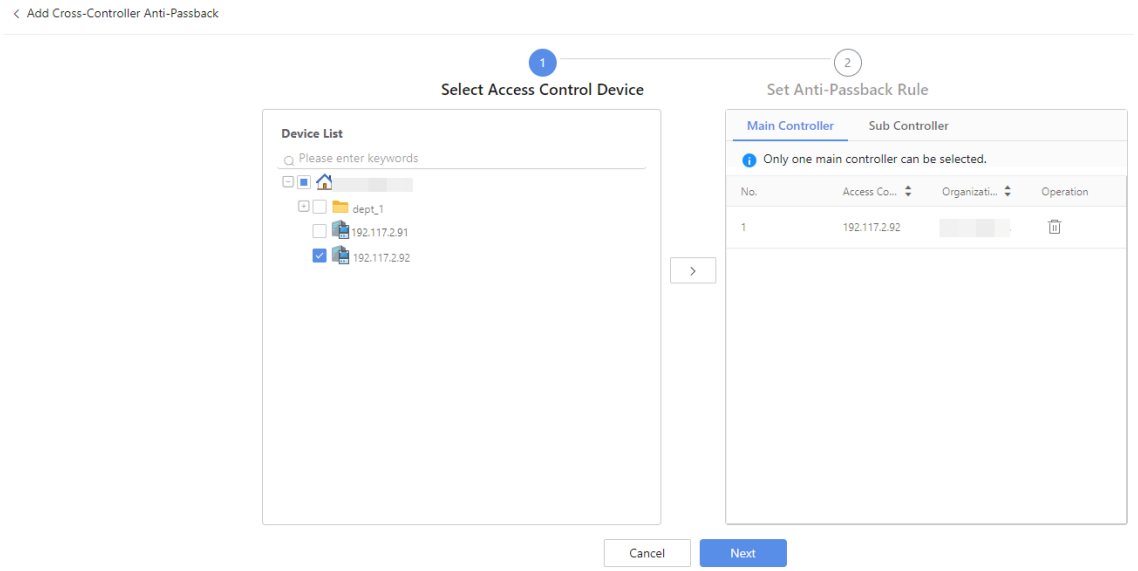
15.4.3.2 Cross-Controller Anti-Passback

Configure area anti-passback or route anti-passback for door channels under multiple access control devices.

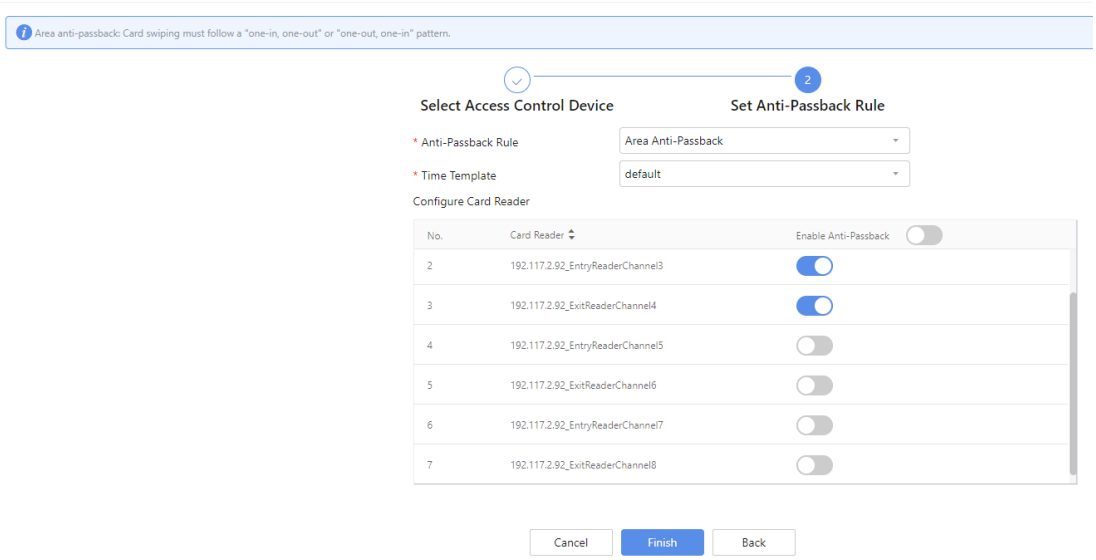
Add New Rule

1. Click **Cross-Controller Anti-Passback**.
2. On the **Main Controller** tab, select an access controller/speed gate or turnstile as the main controller. On the **Sub Controller** tab, select one or multiple access controllers/speed gates or turnstiles as the sub controller.

   Note:
   Some access controllers with lower specifications cannot be used as the main controller.

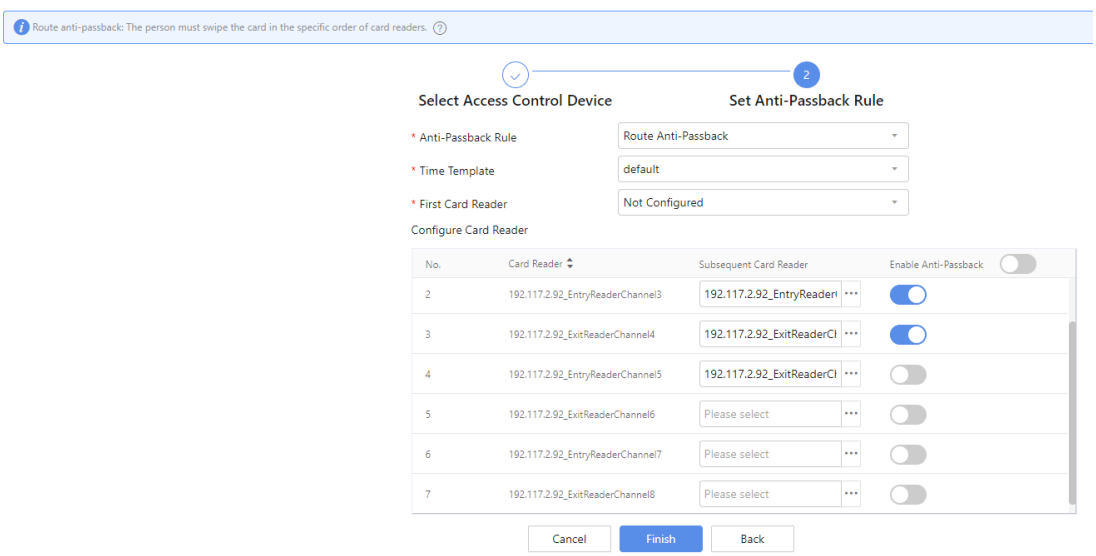


3. Click **Next**.
4. Configure the anti-passback rule.
   - Area anti-passback



Parameter	Description
Time Template	Select a Schedule Template to define the daily access permission effective time.
Configure Card Reader	Enable at least one entry card reader and one exit card reader. If multiple card readers are enabled, personnel may enter through any entry reader and exit through any exit reader. **Note:** The first authentication does not distinguish between entry and exit directions. After the initial successful authentication, subsequent verifications will perform anti-passback validation based on the previous entry/exit direction.

- Route anti-passback



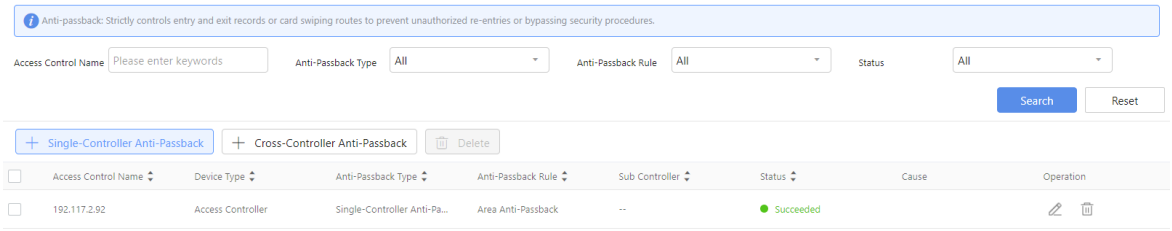
Parameter	Description
Time Template	Select a Schedule Template define the daily access permission effective time.

First Card Reader	• First card reader not set: Card swiping can start from any card reader in the route.
	  • Non-closed routes (e.g., 1-2-3-4): Each person can pass through only once.
	  • Closed routes (e.g., 1-2-3-4-1): The same person can pass through multiple times.

Parameter	Description
	• First card reader set: Card swiping must start from the first card reader. Personnel may exit from any reader in the route and restart from the first reader at any time (e.g., for route 1-2-3-4, sequence 1-2-3-1 is also allowed).
Configure Card Reader	(1) Select subsequent card readers (multiple selections allowed) to form the route. (2) All readers in the route must have anti-passback enabled; otherwise, subsequent segments of the route will not function properly.

5. Click **Finish** to save and automatically sync the rule to the access control device.

15.4.3.3 Rule Management



- Search: Enter keywords for access controller/speed gate or turnstile names, select an anti-passback type (single-controller or cross-controller), anti-passback rule (area, route), and status (successful, failed, syncing, configuration error), then click **Search**.
- Edit: Click to modify the anti-passback rule. The updated configuration will be re-synced after changes are made.
- Delete: Click , or select anti-passback rules and click **Delete**.

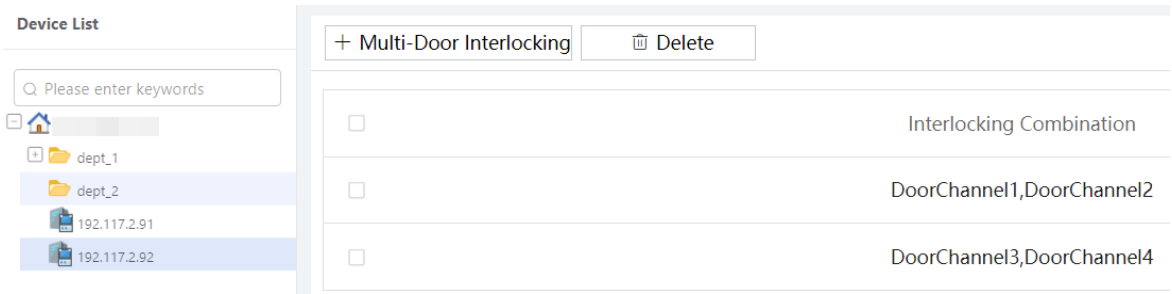
15.4.4 Multi-Door Interlocking (Access Controller & Speed Gate & Turnstile)

Multi-door interlocking refers to a configuration where multiple doors form an interlocking combination. Within this combination, only one door can be open at any given time; all other doors must remain closed.

Depending on the capabilities of the access controller or speed gate or turnstile, common configurations include 2-door interlock, 3-door interlock, and 4-door interlock.

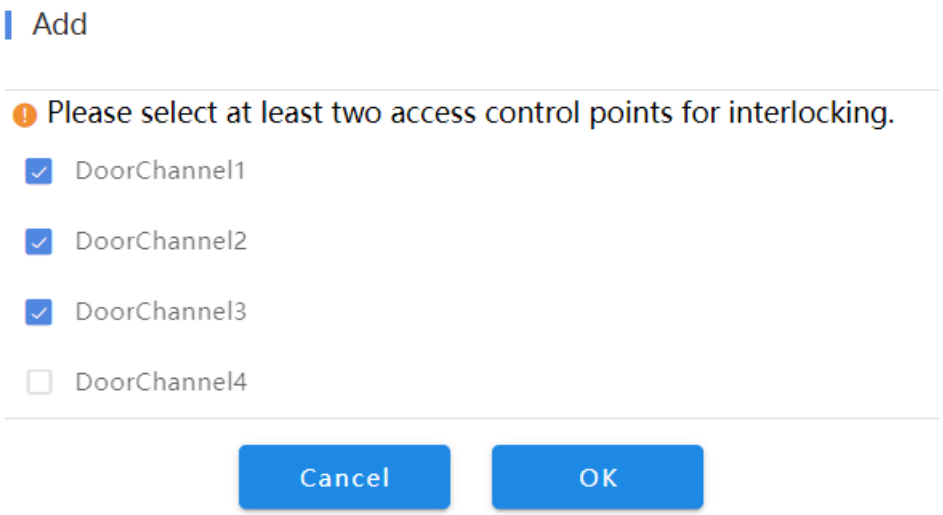
Example: If door channel A and door channel B form a 2-door interlock, when door A is open, door B cannot be opened using regular credentials by anyone.

This function is typically used in locations requiring high security or where ventilation needs to be controlled, such as bank vaults or pharmaceutical enterprises.



Add Multi-Door Interlocking

1. In the device list, select the access control device and click **Multi-Door Interlocking**.
2. Select at least 2 access control points for interlocking.



3. Click **OK**.

Delete Multi-Door Interlocking

Select the multi-door interlocking configuration, and then click **Delete**.

Important Notes

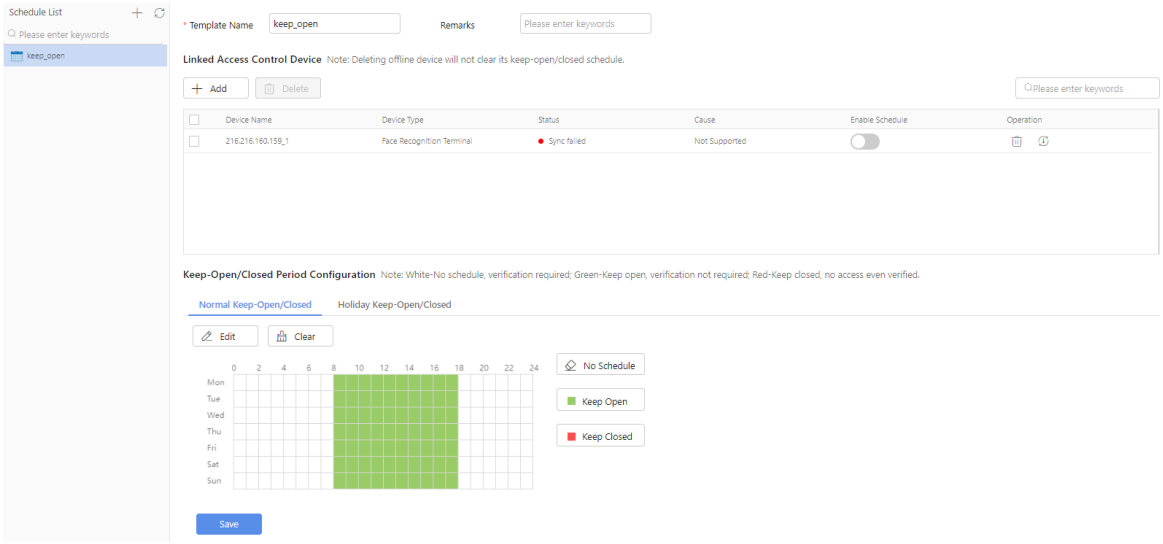
- Interlocked doors cannot be set to Keep Open.
- Super Users are not restricted by interlocking rules and can open doors directly.

15.4.5 Keep-Open/Closed Schedule

Configure keep-open/closed schedules for access control devices **(including face recognition terminals, door stations, zone stations, access controllers, speed gate turnstile)**.

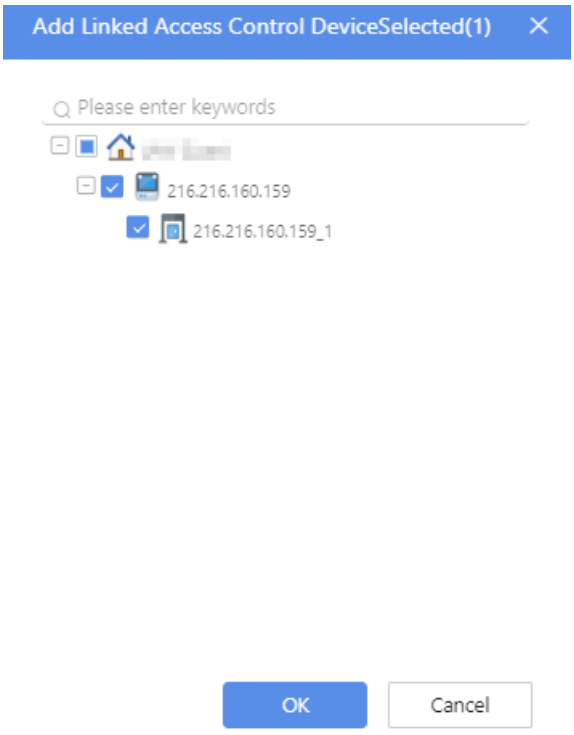
Note:
Some models of face recognition terminals do not support keep-open/closed schedule.

Keep-open periods	During the effective time period, the door opens automatically and keeps open, allowing personnel to pass without verification. If the door is manually closed during the keep-open period, it will keep closed until manually opened again and then keep open.
Keep-closed periods	During the effective time period, the door closes automatically and keeps closed, preventing personnel from verifying and opening the door. If the door is manually opened during the keep-closed period, it will keep open until manually closed again and then keep closed.
Other periods	Personnel must verify to open the door, and the door will close automatically after personnel pass through.

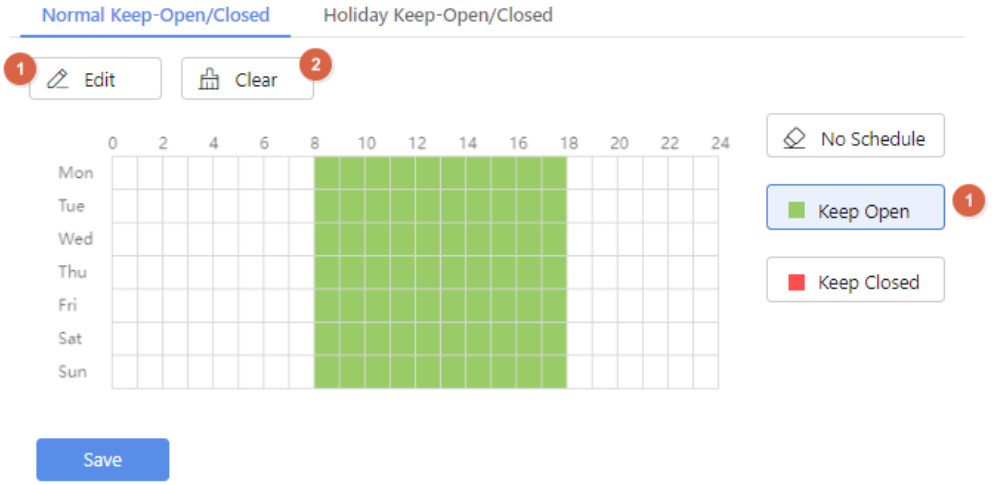


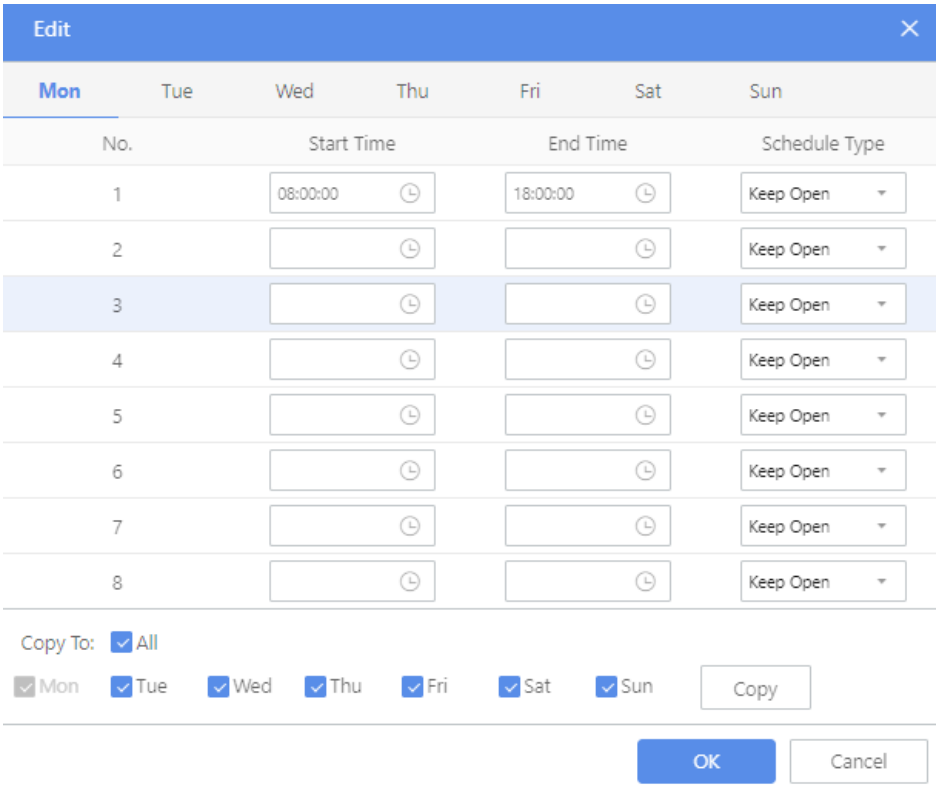
Configure Keep-Open/Closed Schedule

1. Click the ＋ after the schedule list to add a schedule template; or select an existing schedule template to modify.
2. Enter the template name and the remarks (optional).
3. Link access control devices.
   - Click **Add**, select the access control devices that need to apply the schedule template, and click **OK**.

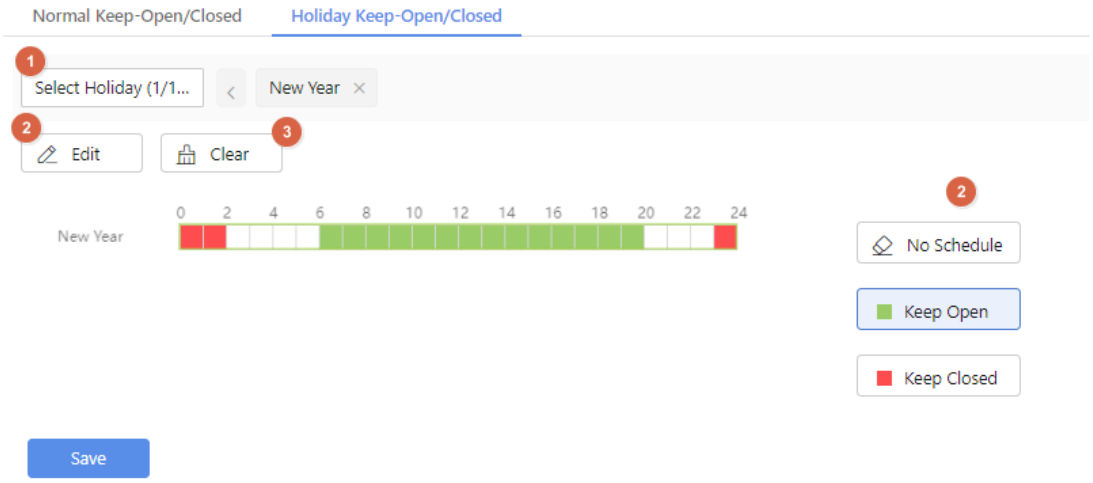


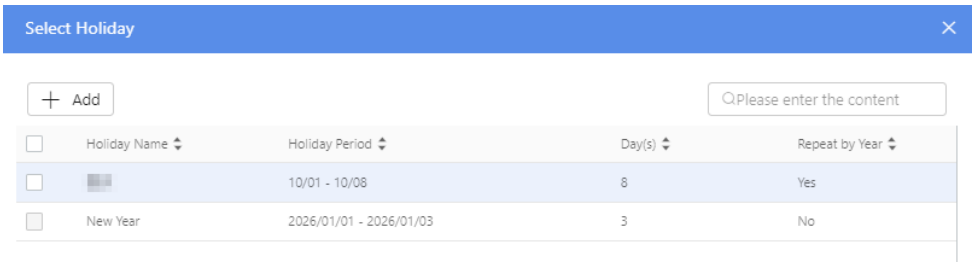
   - Click to sync the schedule template to the selected access control devices.
   - Click to enable the schedule; only when enabled will the keep-open/closed schedule take effect on the access control devices.
   - Click to delete an access control device; deleting an online access control device will also delete the device's keep-open/closed schedule, while deleting an offline access control device will not delete the device's keep-open/closed schedule.
4. Configure keep-on/closed periods.
   - **Normal Keep-Open/Closed**: Configure keep-open/closed periods for Monday through Sunday.



No.	Description
1	Two methods are available to set keep-open/closed periods: • Click **Keep-Open**, **Keep-Closed**, **No Schedule**, and click or drag to draw keep-open/keep-closed/no-schedule time periods on the calendar, with each cell representing one hour. **Note:** White indicates no schedule and verification is required for door opening, green indicates keep-open without verification, and red indicates keep-closed where verification will not open the door. • Click **Edit** to manually select time periods and the corresponding keep-open/keep-closed types, with precision to seconds. You can set up to 8 periods per day. After setting the schedule for a day, you can select other days and then click **Copy** to quickly apply the schedule to other days. 
2	Click **Clear** will remove all the configured periods from the current template.

- (Optional) **Holiday Keep-On/Closed**: Configure keep-on/closed periods on holidays.



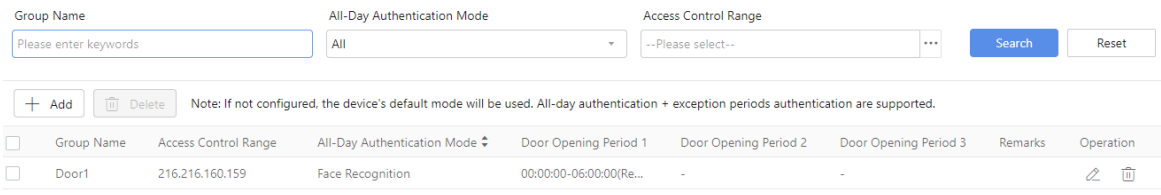
No.	Description
1	Click **Select Holiday**, select holidays, and then click **OK**. 
2	Two methods are available to set keep-open/closed periods: • Click **Keep-Open**, **Keep-Closed**, **No Schedule**, and click or drag to draw keep-open/keep-closed/no-schedule time periods on the calendar, with each cell representing one hour. • Click **Edit** to manually select time periods and the corresponding keep-open/keep-closed types, with precision to seconds. You can set up to 8 periods per day.
3	Click **Clear** will remove all the configured periods from the current template.

5. Click **Save**.

15.4.6 Door Opening Mode Configuration(Face Recognition Access Control)

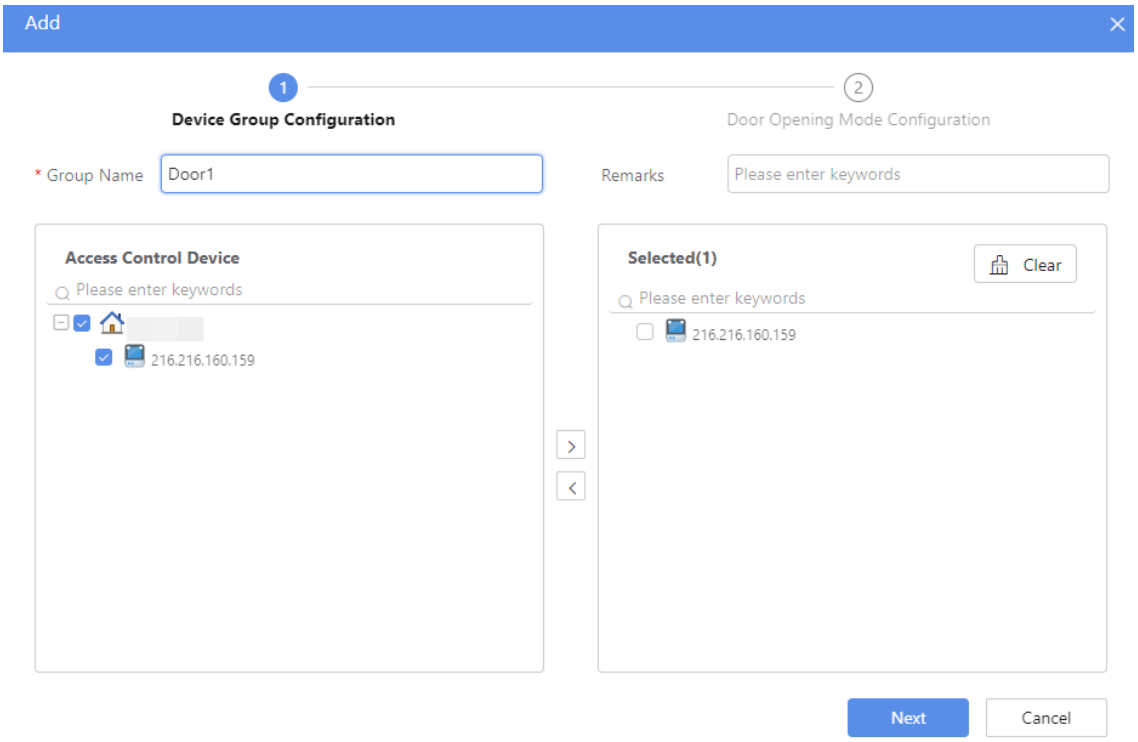
Configure the "all-day authentication + exception period authentication" door opening mode for **face recognition access control devices** in batches by group. If not configured, the device's default mode will be used.

Note:
Some models of face recognition terminals do not support door opening mode configuration.

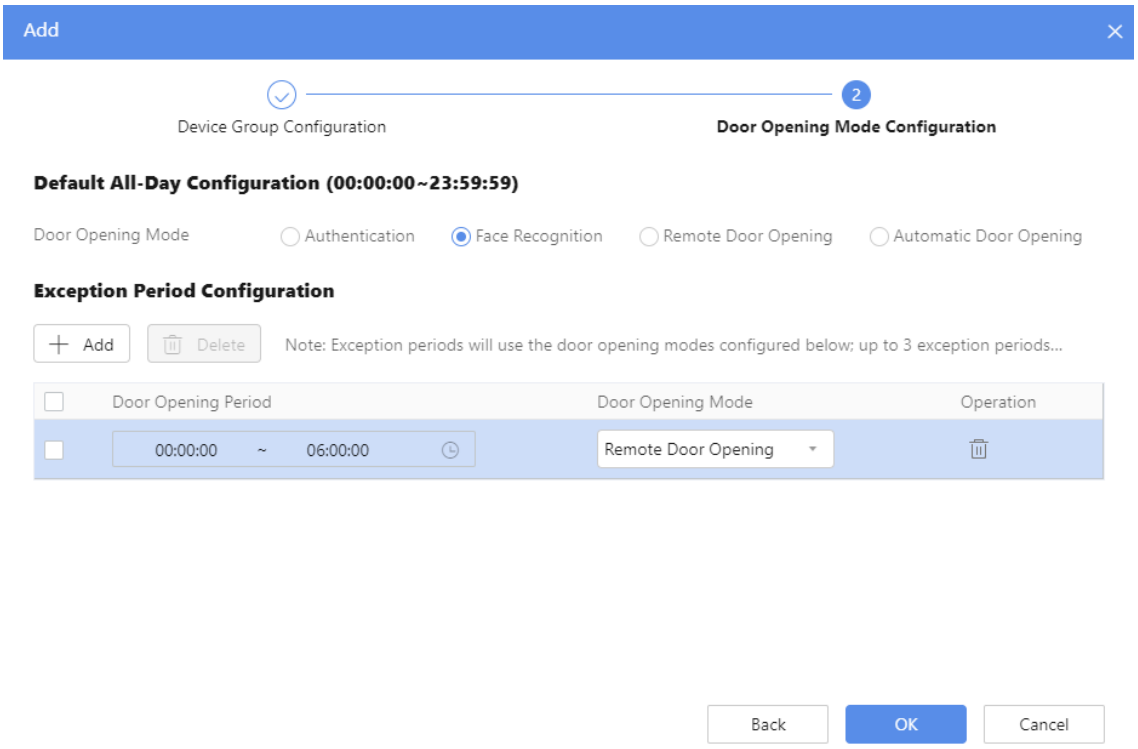


Configure Door Opening Mode

1. Click **Add**. The **Add** page appears.
2. Add device groups to facilitate batch configuration of devices by group.
   Enter a group name, select the access control devices, and click **Add** to add them to the selected devices list.



3. Click **Next**, configure door opening modes.



(1) Select the default door opening mode for all-day:

- Authentication: The door opens only after the person passes the authentication.
- Face Recognition: The door opens immediately when the access control device captures a face, without verifying permissions.
- Remote Door Opening: The access control device reports the person information to the platform, and the platform remotely controls the door opening based on the authentication result.
- Automatic Door Opening: The system tries remote door opening first. If no authentication is returned three consecutive times via the remote door opening mode, the system uses the local authentication mode for judgment.

(2) (Optional) Click **Add** to add a door opening mode for exception periods.

- Up to three exception periods can be configured.
- During exception periods, the door opening mode configured for exception periods will be used for door opening.

4. Click **OK**. The selected devices will use the configured door opening mode during the specified time periods.

More Operations

Edit or delete door opening mode groups as needed.

- Edit a door opening mode group: Click the corresponding in the **Operation** column to edit the door opening mode group.
- Delete a door opening mode group: Select door opening mode groups and then click **Delete** on the top to delete the selected door opening mode groups; or click the corresponding in the **Operation** column to delete a door opening mode group.

15.5 Face Recognition Access Control Configuration

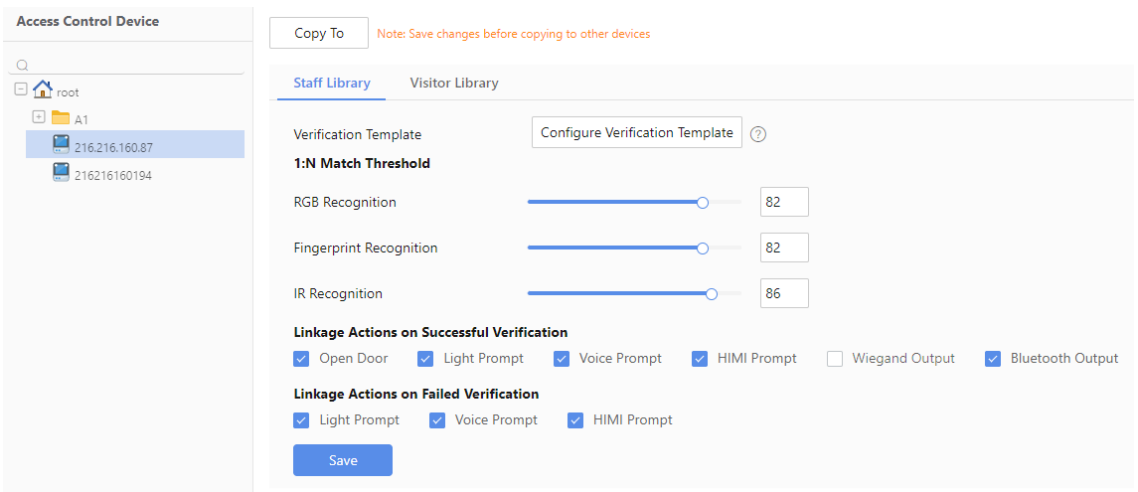
Go to **Access&Attendance > Access Control > Face Recognition Access Control Configuration**.

Configure face recognition access control parameters on the platform and sync them to the devices with one click. You can also copy the settings from a device to other devices for batch configuration.

15.5.1 Face Library Configuration

Configure parameters such as verification templates for the face library.

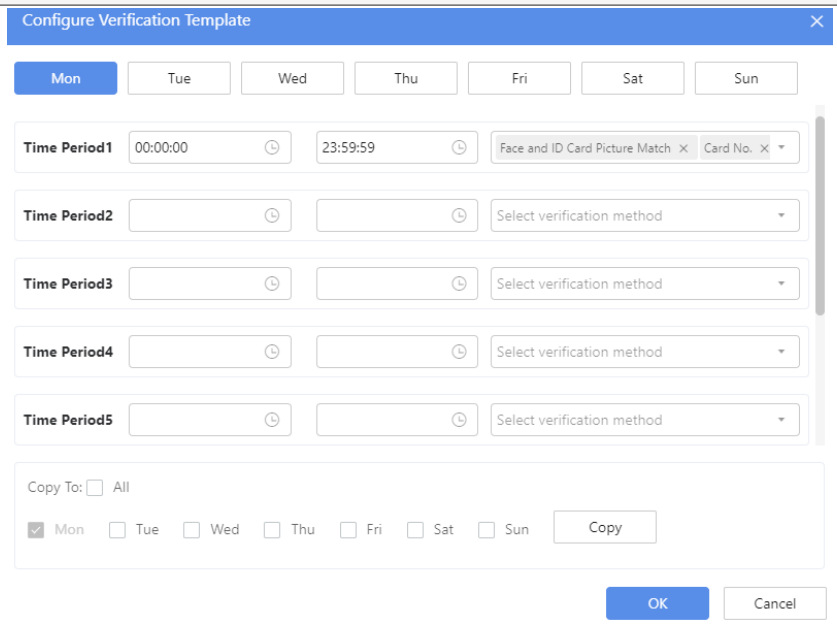
1. Select a face recognition access control device from the device list.



2. Refer to the table below to configure the parameters.

Table 15-1: Configuration Description

Parameter	Description
Library Type	• Employee Library: For long-term personnel, such as property owners, security guards, etc. • Visitor Library: For temporary personnel. **Note:** When configuring verification templates, face & ID card verification cannot be enabled simultaneously for both the employee library and visitor library.
Verification Template	Configure verification templates for the week (Monday to Sunday). Click **Configure Verification Template** to go to the configuration page.

Parameter	Description
	 • Set verification time periods for each day. The start time of each time period must not be later than the end time. Up to 8 non-overlapping time periods can be configured per day. • Supported verification methods: Face & ID Card Verification, Number Allowlist, Face Allowlist, Password, Face & ID Card + Number Allowlist, Number + Face Allowlist, Password + Face Allowlist, Fingerprint Allowlist, Face Allowlist + Fingerprint. • A maximum of three verification methods can be configured simultaneously within a single time period. • After setting the verification schedule for one day, you can select other days and click **Copy** to apply the same settings for quick configuration. **Note:** After saving the configuration, the system will automatically generate a verification template name and sync it to the device.
1:N Matching Threshold	For visible light / fingerprint/ infrared recognition, the 1:N matching degree must meet or exceed the set threshold to succeed. Visible light recognition threshold range: [0-100]. Default: 82. Fingerprint recognition threshold range: [0-100]. Default: 82 (only effective when used with a fingerprint module). Infrared recognition threshold range: [0-100]. Default: 86. **Note:** Some models of face recognition terminals do not support fingerprint/ infrared recognition configuration.
Linkage Actions on Successful Verification	Actions triggered after successful verification, such as door lock control and status indicator results. • Open Door: Sends an unlock signal to open the door. • Status Indicator Display: Indicator light turns green. • Audio Message: Plays "Verification successful." • Local Screen Display: Displays "Verification successful." • Wiegand Output: Sends a signal to the card reader for verification. • Bluetooth Output: Transmits signal via Bluetooth to bound devices (supported by some devices; subject to the actual UI).

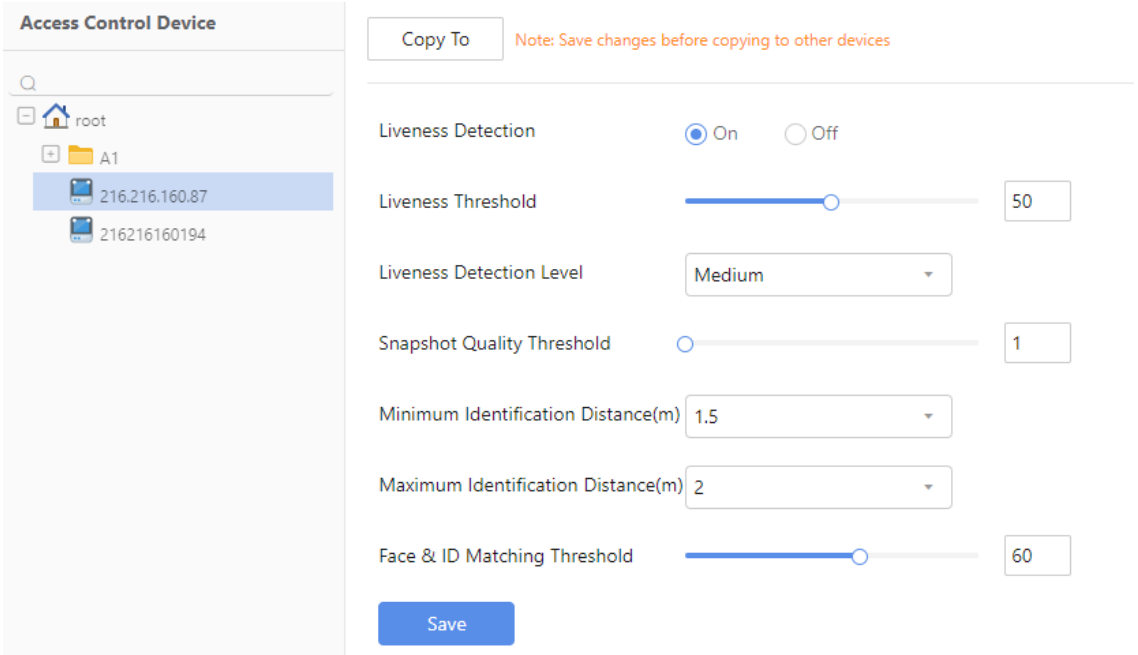
Parameter	Description
	Note: The linkage actions on successful verification may vary by device model. Refer to the actual device.
Linkage Actions on Failed Verification	Options for actions triggered after verification failure: • Status Indicator Display: Indicator light turns red. • Audio Message: Plays "No permission." • Local Screen Display: Displays "No permission." **Note:** The linkage actions on failed verification may vary by device model. Refer to the actual device.

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To** to copy the settings to other access control devices.

15.5.2 Face Detection Configuration

Configure face detection parameters.

1. Select a face recognition access control device from the device list.



2. Refer to the table below to configure the parameters.

Table 15-2: Configuration Description

Parameter	Description
Liveness Detection	Select **Enable** to activate the liveness detection function. **Note:** Algorithm-based detection determines whether the subject is live, effectively preventing spoofing using videos, photos, or other non-live materials.
Liveness Threshold	This parameter is displayed only when liveness detection is enabled. Valid range: [1–100]. A higher threshold requires more pronounced liveness features, improving the detection rate against non-live attempts.
Liveness Detection Level	This parameter is displayed only when liveness detection is enabled.

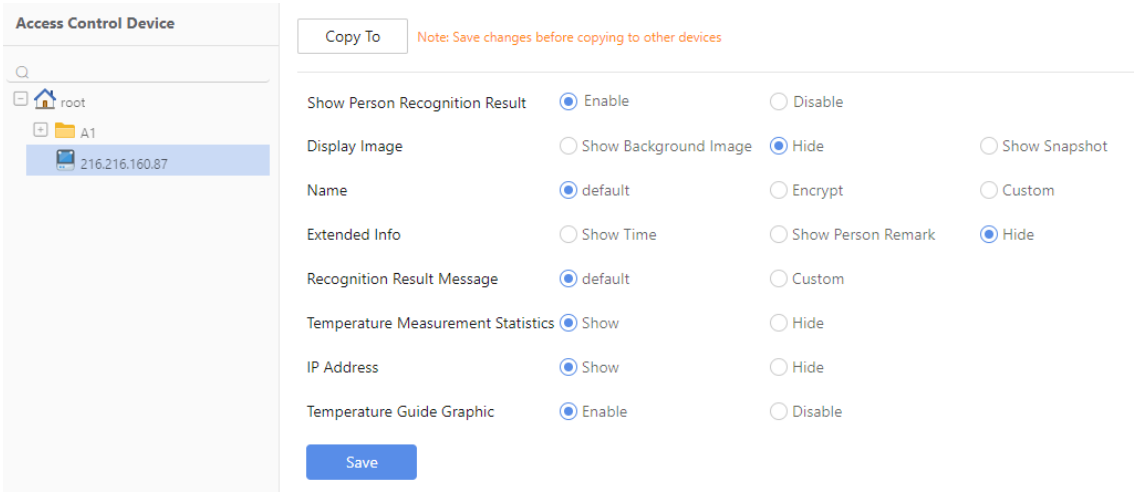
Parameter	Description
	It indicates the success rate of detecting non-live attempts such as videos or photos. Three levels are available: High, Medium, and Low. A higher level imposes stricter criteria for liveness judgment.
Snapshot Quality Threshold	The minimum matching threshold for a captured image to be recognized as a face during face verification. Images below this threshold are classified as "non-face" and fail the detection. Valid range: [1–100]. A higher value improves matching accuracy. Adjust the threshold by dragging the slider or entering a value.
Minimum (Maximum) Identification Distance (m)	Within this range, photos will be captured. **Note:** • If both parameters are set to non-adaptive options, ensure the maximum recognition distance is greater than the minimum recognition distance. • Some models of face recognition terminals do not support recognition distance configuration.
Face & ID Matching Threshold	When using ID card verification, this specifies the minimum similarity required between the face image recognized by the access control device and the ID card photo. Verification fails if the similarity is below the threshold. Valid range: [1–100]. A higher value requires greater similarity between the live person and the ID photo. Adjust the value by dragging the slider or entering a number.

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To** to copy all settings to other access control devices.

15.5.3 Recognition Display Configuration

Configure the content displayed on the screen after successful face verification.

1. Select a face recognition access control device from the device list.



2. Refer to the table below to configure the parameters.

Table 15-3: Configuration Description

Parameter	Description
Show Person Recognition Result	• Enable: After successful verification, the access control interface displays the person information. • Disable: After successful verification, the access control device screen does not display the person information.

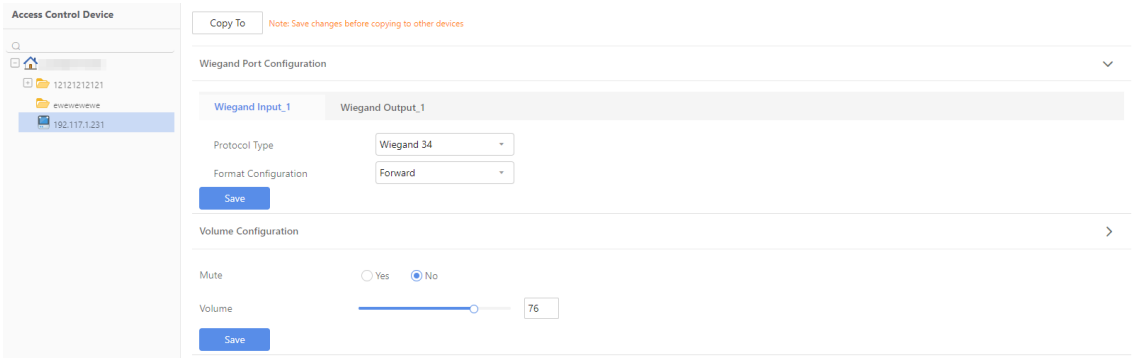
Parameter	Description
Display Image	• Show Background Image: After successful verification, the access control device screen displays the image uploaded to the face library. • Hide: After successful verification, the access control device screen does not display personnel image information. • Show Snapshot: After successful verification, the access control device screen displays the captured image.
Name	• Default: After successful verification, the access control device screen displays the recognized person's name. • Encrypt: After successful verification, the access control device screen encrypts the person's name, displaying only partial information. • Custom: After successful verification, the access control device screen displays custom information entered here.
Extended Info	• Show Time: Displays the detection time. • Show Person Remark: Displays the remarks of the successfully recognized person (set in the face library). • Hide: Default mode, no additional extended information is displayed.
Recognition Result Message	• Default: After successful face recognition, the access control device screen displays "Recognition Successful." • Custom: After successful face recognition, the access control device screen displays custom information entered here.
Temperature Measurement Statistics	• Show: The access control device screen displays the total number of temperature screenings and persons with normal body temperature. • Hide: The access control device screen does not display temperature measurement statistics.
IP Address	• Show: The access control device screen displays the device's IP address. • Hide: The access control device screen does not display the device's IP address.
Temperature Guide Graphic	• Enable: When the temperature measurement function is enabled, the access control device screen displays the temperature measurement guide image (for wrist temperature measurement devices). • Disable: When the temperature measurement function is disabled, the access control device screen does not display the guide image (for wrist temperature measurement devices).

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To** to copy all settings to other access control devices.

15.5.4 Port & Peripheral Configuration

Configure port and peripheral parameters.

1. Select the face recognition access control device from the device list.



2. Refer to the table below to configure the parameters.

Table 15-4: Configuration Description

Parameter	Description

Wiegand Interface Configuration	The Wiegand interface can connect to external IC card readers and CPU card readers.
	• Input and output ports can be configured separately.
	• Protocol Type: Wiegand 26 and Wiegand 34. Select according to the actual scenario.
	  • Wiegand 26: Card numbers are read using the Wiegand 26 protocol (reads only 3-byte card numbers).
	  • Wiegand 34: Card numbers are read using the Wiegand 34 protocol (reads only 4-byte card numbers).
	• Format Configuration: Specifies that the card number sequence read by our company's card readers is in positive order.
	  • Forward: Select this option for input/output when the sequence matches that read by our company's card readers.
	  • Reverse: Select this option for input/output when the sequence is the reverse of that read by our company's card readers.

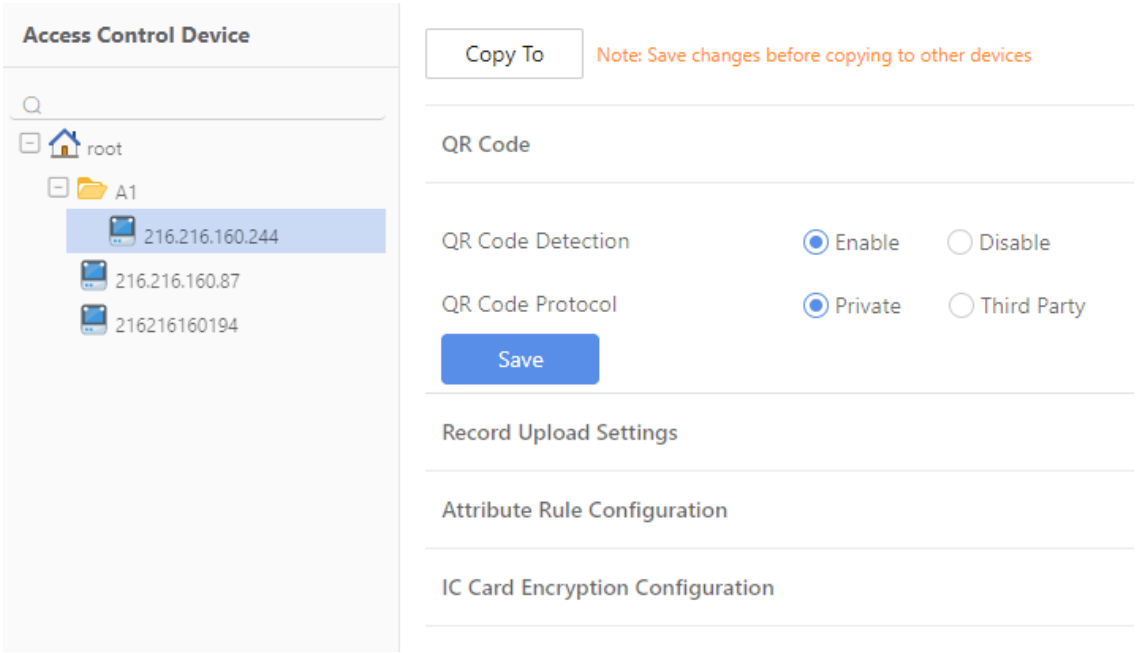
Volume Configuration	Sets whether the access control audio is muted. If not muted, the audio volume can be set. • Select **No** to enable the audio function. The audio volume can be set. • Select **Yes** to enable mute on the device. **Note:** When mute is enabled, there will be no prompt sounds during access control verification.

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To**> to copy all settings to other access control devices.

15.5.5 Advanced Configuration

Advanced configuration supports features such as QR code configuration, upload configuration, attribute rule configuration, and IC card encryption configuration.

1. Select the face recognition access control device from the device list.



2. Refer to the instructions below to configure the parameters.

- QR Code Configuration

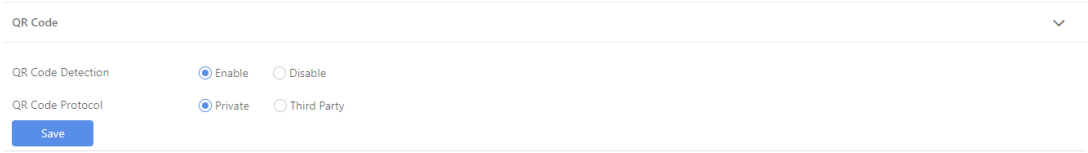


Table 15-5: Configuration Description

Parameter	Description
QR Code Detection	• Disable: The device camera will not collect QR code data. • Enable: When the verification template includes a number allowlist, the device camera will support collecting and verifying QR code data.
QR Code Protocol	• Private Protocol: The device will parse the QR code data locally. • Third-party Protocol: The QR code data will be uploaded to the face recognition speed gate management platform for parsing.

- Record Upload Configuration

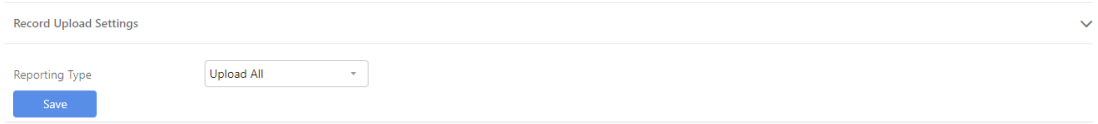


Table 15-6: Parameter Description

Parameter	Description
Report Type	• Upload All: The terminal will upload access records for all recognition outcomes (including all scenarios of both successful and failed recognition). • Upload Success Record: The terminal will only upload access records for successful recognitions.

- Attribute Rule Configuration

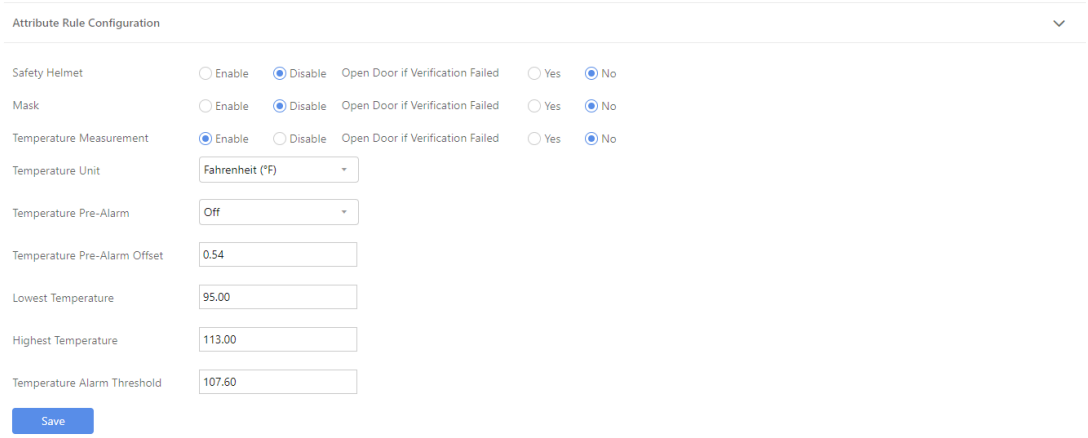


Table 15-7: Parameter Description

Parameter	Description
Safety Helmet	When enabled, the recognition terminal will provide both on-screen and voice prompts (Please wear a helmet) if a person is detected without a safety helmet. When helmet detection is enabled, configure whether to unlock upon verification failure. • Yes: If the recognition terminal detects a person not wearing a helmet, it does not affect the actual verification (e.g., face, card, face & ID card) and the door will unlock if verification is successful. • No: If the recognition terminal detects a person not wearing a helmet, the door will not unlock.
Mask	When enabled, the recognition terminal will provide both on-screen and voice prompts ("Please wear a mask") if a person is detected without a mask. When mask detection is enabled, configure whether to unlock upon verification failure. • Yes: If the recognition terminal detects a person not wearing a mask, it does not affect the actual verification (e.g., face, card, face & ID card) and the door will unlock if verification is successful. • No: If the recognition terminal detects a person not wearing a mask, the door will not unlock.
Temperature Measurement	When enabled, the temperature measurement module will provide both on-screen and voice prompts ("Abnormal Body Temperature") if a person's temperature exceeds the set alarm threshold. When temperature measurement is enabled, configure whether to unlock upon verification failure. • Yes: If the temperature measurement module detects a person's temperature exceeding the set alarm threshold, it does not affect the actual verification (e.g., face, card, face & ID card) and the door will unlock if verification is successful. • No: If the temperature measurement module detects a person's temperature exceeding the set alarm threshold, the door will not unlock.
Temperature Unit	Select the temperature unit: Celsius (°C) or Fahrenheit (°F).
Temperature Pre-alarm	• On: When the temperature measurement module detects a person's temperature within the range [Pre-alarm Threshold ~ Alarm Threshold], it will provide both on-screen and voice prompts ("High temperature detected, please retest"). • Off: Alarm prompts will only occur when a person's temperature reaches the alarm threshold.

Parameter	Description
Temperature Pre-alarm Offset	When temperature pre-alarm is enabled, set the pre-alarm offset value. Pre-alarm Threshold = Alarm Threshold - Pre-alarm Offset.
Lowest/Highest Temperature	Value range: [30~45]. The default lowest temperature is 35.5, and the default highest temperature is 42. Users can configure the temperature measurement range according to the actual application scenario.
Temperature Alarm Threshold	If the temperature measured by the module exceeds the value set here, the device and voice prompts will indicate "Abnormal Body Temperature". The value must be within the range of the lowest and highest temperature settings.

- IC Card Encryption Configuration

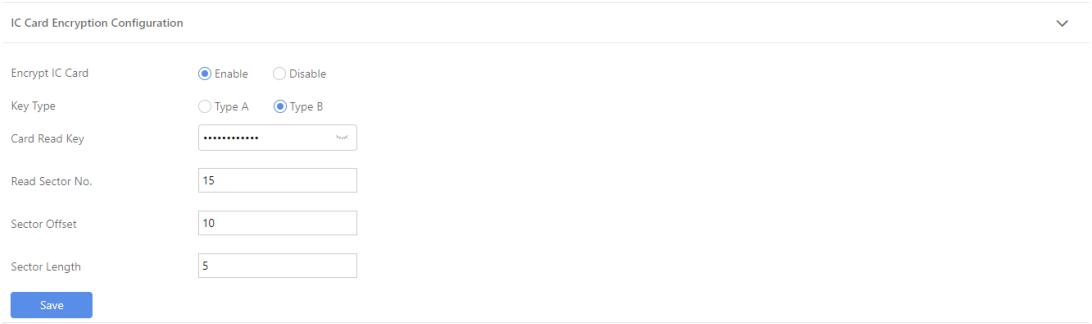


Table 15-8: Parameter Description

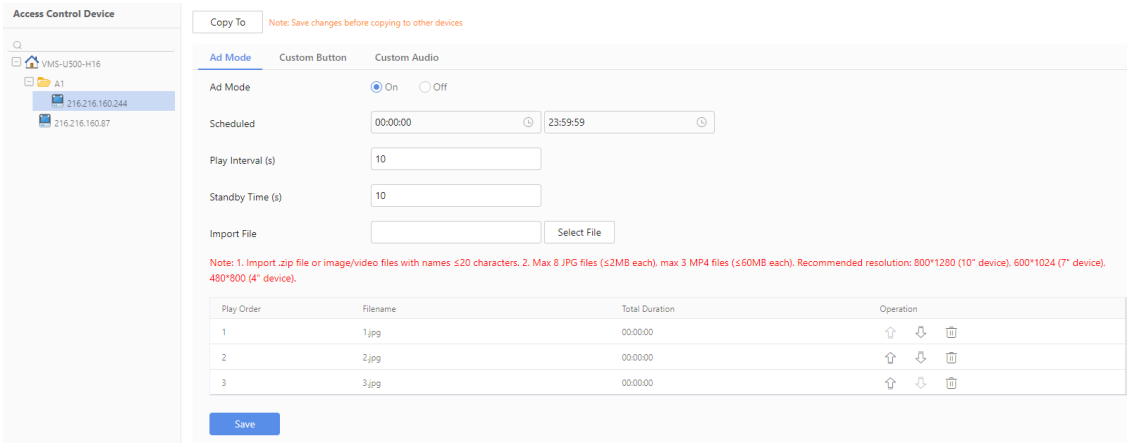
Parameter	Description
Encrypt IC Card	Enable or disable IC card encryption. **Note:** This must be configured based on whether the issued IC cards are encrypted or standard. For card configuration details, please refer to **Personnel Management > Card Information** . When IC card encryption is enabled, if a non-encrypted card is used for verification, access will be denied even if the card number has been registered on the access control device.
Key Type	Select **Type A** or **Type B** according to the actual scenario.
Card Read Key	The password for the MIFARE card. A six-byte password (in hexadecimal).
Read Sector No.	The storage space of the MIFARE card is divided into 16 sectors (0-15). Please select the appropriate sector number based on the actual scenario.
Sector Offset	Enter the sector offset for reading the MIFARE card. Integer range: [0-47], default value: 0.
Sector Length	4. Enter the sector length for reading the MIFARE card. Integer range: [1-8], default value: 4.

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To** to copy all settings to other access control devices.

15.5.6 Personalized Configuration

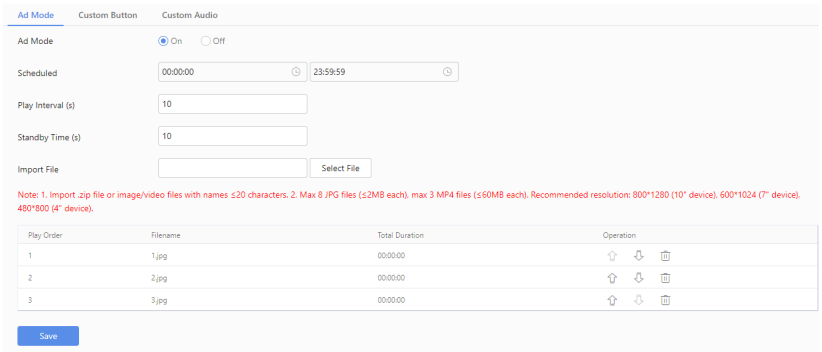
Configure personalized parameters such as advertising mode, custom keys, and custom audios.

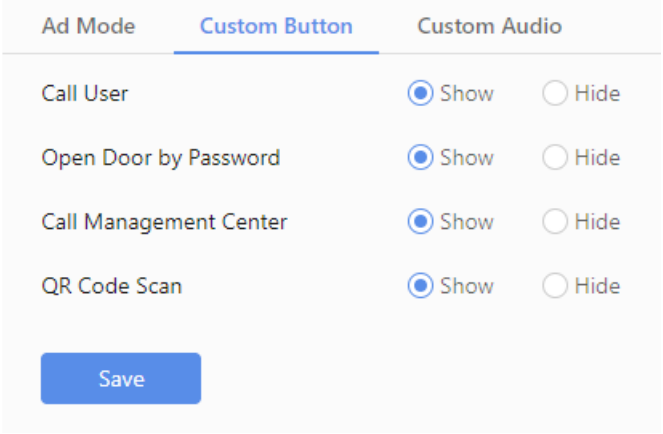
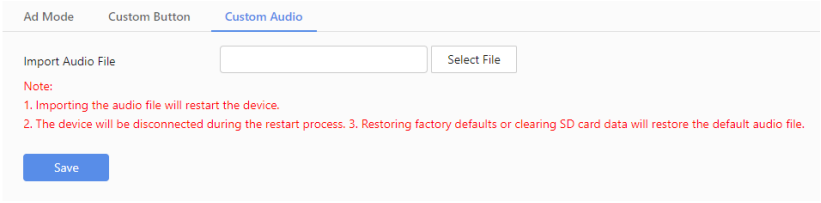
1. Select the face recognition access control device from the device list.



2. Refer to the table below to configure the parameters.

Table 15-9: Configuration Description

Parameter	Description
Ad Mode	Enable or disable the ad mode according to your needs.  • Scheduled Time Set the time period for playing ads. Ads will only play between the start time and end time. Requirement: The end time must be later than the start time; otherwise, the settings will not be saved. **Note:** Some models of face recognition terminals do not support scheduled time configuration. • Play Interval Set the time interval for playing ads. Requirement: Integer value in seconds, range [1–3600], default value: 10. • Standby Time When no face is detected by the device for the duration set here, it will enter ad mode. Requirement: Integer value in seconds, range [10–3600], default value: 10. • Import Ad File Users can upload custom ad files. For file requirements, see the "Note" on the page. Click **Select File** to upload an ad file. • Video Play Order Click ⇧ to move the video up in the play order. Click ⇩ to move the video down in the play order.
Custom Button	Choose to show or hide the following buttons on the device screen: Call User, Open Door by Password, Call Management Center, and QR Code Scan.

Parameter	Description
	
Custom Audio	Click **Select File** to choose and upload an audio file from your local device.  **Note:** • The device will restart after a successful upload. • Some models of face recognition terminals do not support custom audio configuration.

3. After completing the configuration, click **Save** to sync the settings to the device.
4. (Optional) After saving the configuration, click **Copy To** to copy all settings to other access control devices.

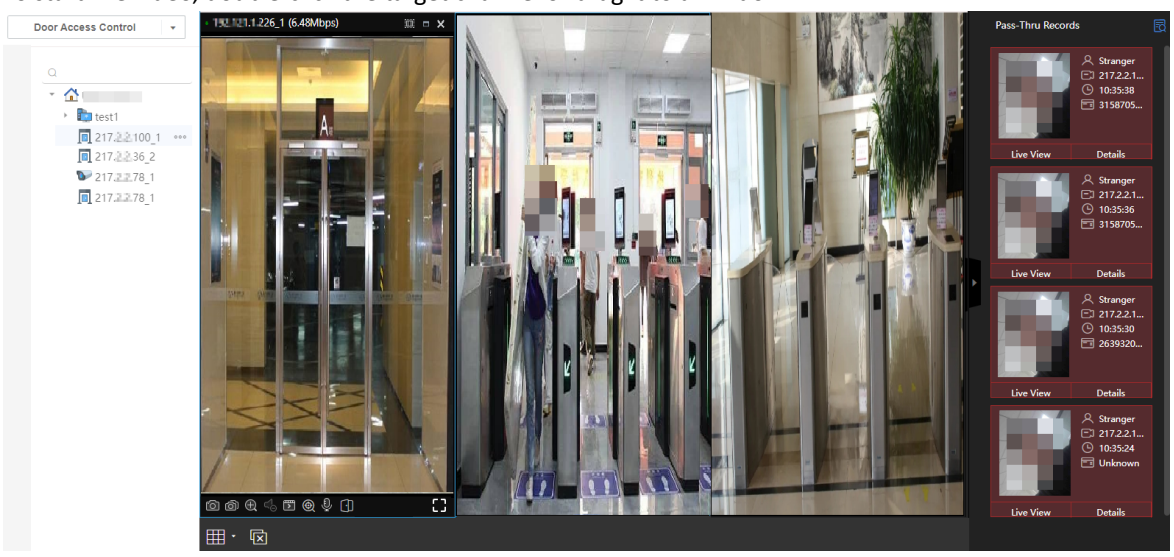
15.6 Access Control Live

Go to **Video Application > Smart Live View > Door Access Control**.

View live videos of access control devices and pass-thru records. You can take snapshots, zoom in on live video, open / close door remotely, etc.

View Live Video

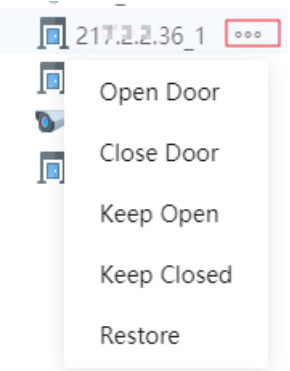
To start live video, double-click the target channel or drag it to a window.



Note:
The channels of general access control devices and access controllers do not provide live view; only pass-thru records are displayed.

More Operations

- Real-time pass-thru records: Pass-thru records are displayed on the right. The background color will be red if authentication fails, such as stranger.
- Toolbar: See Live View Toolbar Operations for reference. The functions are similar.
- View more: Click on the upper-right corner to view history pass-thru records on the **Pass-Thru Records** tab.
- View pass-thru details: Double-click a pass-thru record or click **Details** under the record (including snapshot, personal information, camera, snapshot time, and authentication result).
- View live video: Click **View Live Video** under the passing record to view the live videos of people passing through.
- Access control: Click next to an access control device in the left-side list, or click in the live view toolbar, and then select an option (Open Door, Close Door, Keep Open, Keep Closed, Restore (restore door from keeping open/closed)) in the pop-up list as needed.



15.7 Pass-Thru Records

Go to **Data Search > Access Records > Pass-Thru Records**.

View pass-thru records.

Note:

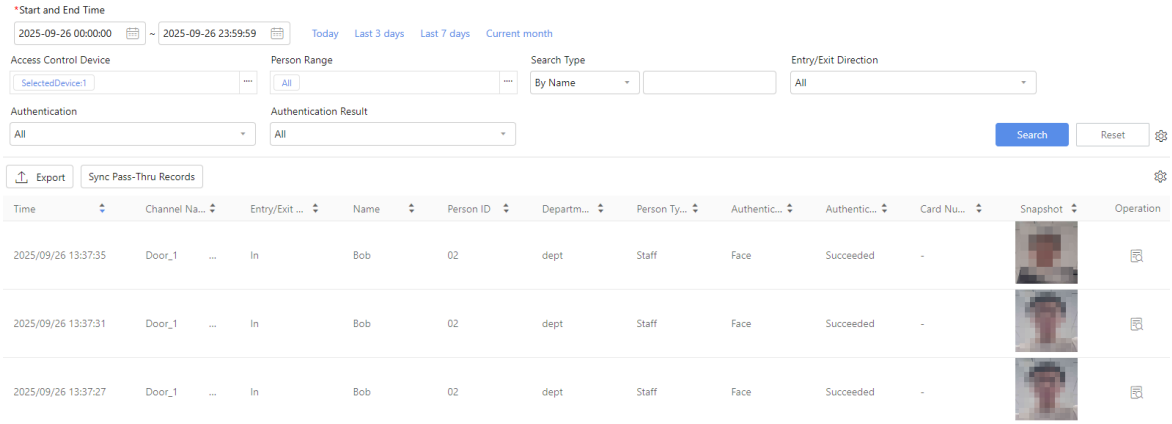
- The pass-thru records on the access control devices will be synced to the platform in real time.
- Conditions for successful verification: correct credentials (face, card, password, etc.), credentials within their validity period, access permission.

Search Pass-Thru Records

To search records, set the start and end time, channels under access control devices, person range (department/visitor/stranger), search type (by name/by card number/by person ID), entry/exit direction (in/out/not configured), authentication (face/ID card/IC card), authentication result (succeeded/failed), then click **Search**. The search results will be displayed.

Note:

- You can click to the right of the search criteria to customize the search criteria.
- Click at top right corner of the table to configure the display fields for the list.
- See Edit Channel Info to configure the entry and exit directions of the access control channels.



More Operations

- Export records: Select pass-thru records, and then click **Export**.
- View details: Click in the **Operation** column.
- Sync pass-thru records: Sync pass-thru records of an access control device to the platform, and then click **Search** to refresh the records.

  Note:
  Only pass-thru records on the online face recognition terminals can be synced manually. General access control devices and access controllers do not support manual sync.

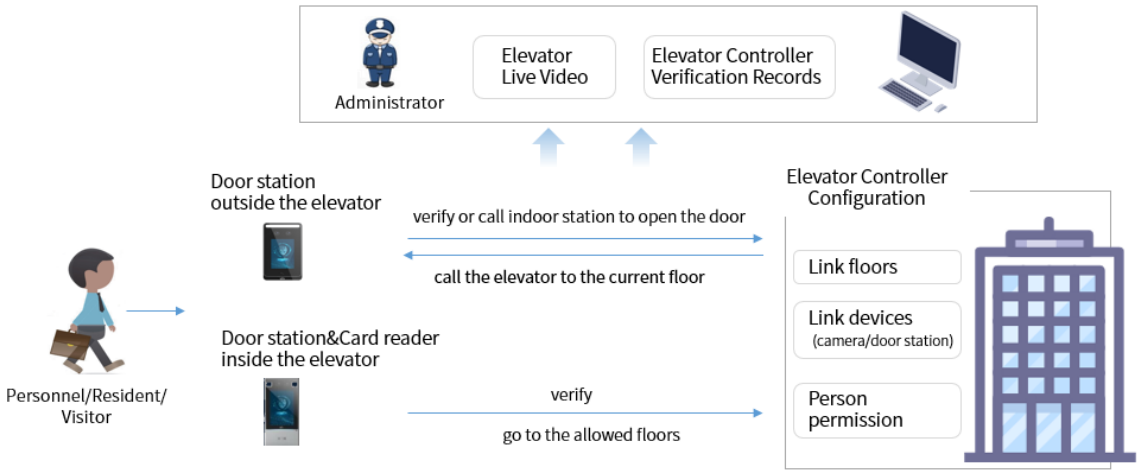
  1. Click **Sync Pass-Thru Records**. A window appears.
  2. Set a time period for the pass-thru records you want to synchronize on the device side.
  3. (Optional) If you choose to synchronize image data, images in the pass-thru records will also be synchronized.
  4. Select the desired access control device.
  5. Click **OK** to start synchronizing pass-thru records of the selected device.
  6. When sync succeeded, you can click **Search** to refresh to pass-thru record list.

16 Elevator Control Management

Elevator control management provides elevator permission management services for building scenarios in industrial parks, residential areas, schools, hotels, etc. Through elevator controllers installed in the elevator system, building administrators can assign permissions, so people can access specified floors by verifying their identity at card readers or door stations inside the elevators. People can also call elevators to their floor by verifying identity at door stations outside the elevators or call indoor stations to open the door. The administrator can also view real-time video in elevators and search access records. Elevator control management can automatically verify floor access permissions to prevent unauthorized intruders. It ensures assets security and personnel safety while enhancing the guard management efficiency.

Functions

Menu	Description
Elevator Control Configuration	Configure floors, linked devices (cameras/door stations), and verification mode related parameters.
Elevator Control Permission	Configure elevator control permissions (by specifying floors), so elevator users can only go to the floors they have access to, and call elevators to the floors they are currently located.
Elevator Live Video	View live video from the linked devices (cameras/door stations) to monitor the elevator's real-time status.
Elevator Controller Verification Records	Search verification records from elevator card readers to monitor personnel elevator usage records.



Configuration Procedure

1. Add persons and configure their cards and door opening passwords. See Personnel Management , Resident Management, Visitor Management.
2. Add elevator controllers, cameras/door stations. See **Device Management >** Private Device.
3. Add floors. See Community Room Management and Custom Units.
4. Configure elevator floors. See Floor Configuration.
5. Configure linked cameras/door stations. See Link Devices.
6. Assign permissions on elevator controllers and door stations. See Schedule Template,Access Permission Config.
7. View the live video of people entering/exiting elevators and elevator usage records. See **Smart Live View >** Elevator Live Video, **Data Search > Pass-Thru Records >**Elevator Controller Verification Records.

16.1 Elevator Control Configuration

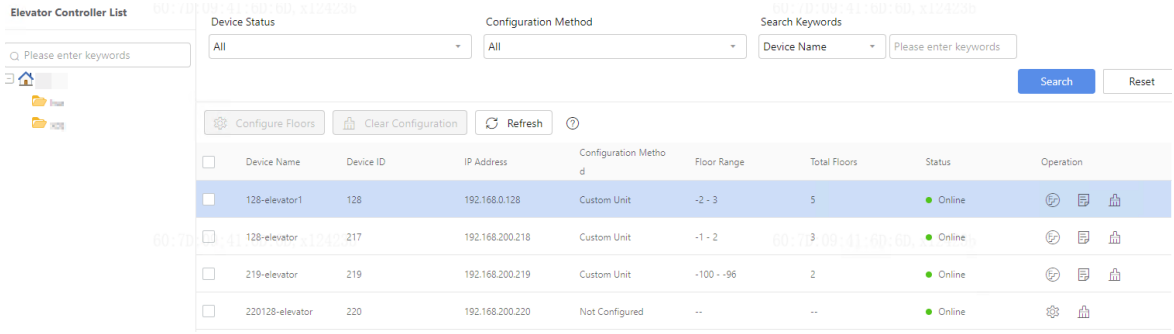
Go to **Access&Attendance > Access Control > Elevator Control Management**.

Configure the elevator floors managed by the elevator control system and the linked devices (cameras/door stations), as well as verification parameters of the elevator controller.

16.1.1 Floor Configuration

Configure the elevator floors managed by the elevator control system based on the actual situation of the building.

Select an organization on the left side, and elevator controllers in the organization will be displayed on the right side.

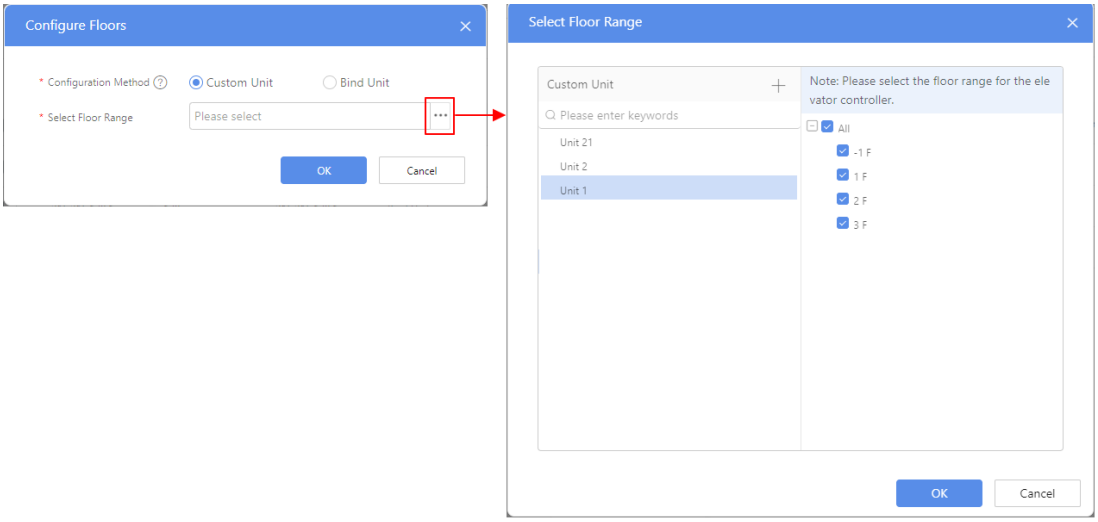


Configure Floors

1. Select elevator controllers (you can select multiple for batch configuration), and click **Configure Floors**; or click in the **Operation** column.
2. Select the configuration method.
   - Custom Unit: Select floors for the custom unit.

     Note:

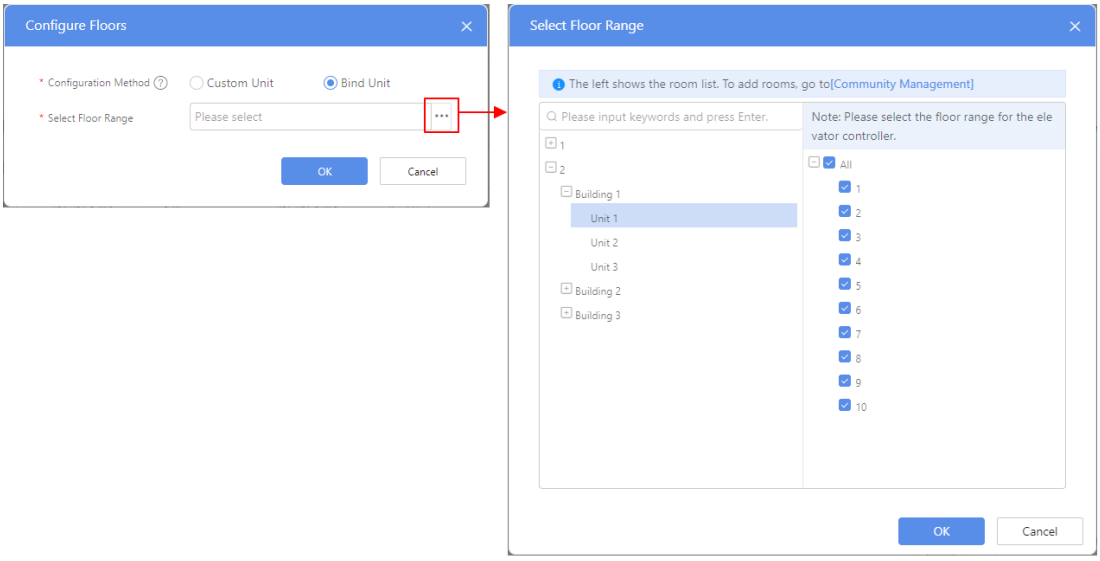
     - In the custom unit, you can add floors manually, which is suitable for scenarios where the existing units do not meet the elevator floor requirements.
     - Add units on the **Custom Unit** page, or click + in the **Select Floor Range** dialog box to add units.



   - Bind Unit: At the community level, select a unit, and then select the floors under that unit.

     Note:

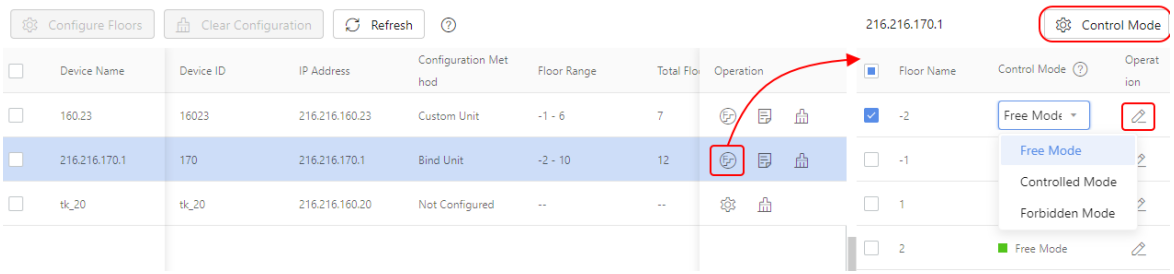
     - Units are created in Room Management.
     - After the elevator controller is bound to a unit, the residents of that unit automatically gain the elevator control permission for the floors they reside on.



3. Click **OK**.

View Floors, Modify Floor Control Mode

In the list, you can view the range of floors and the total number of floors bound with the elevator controller.

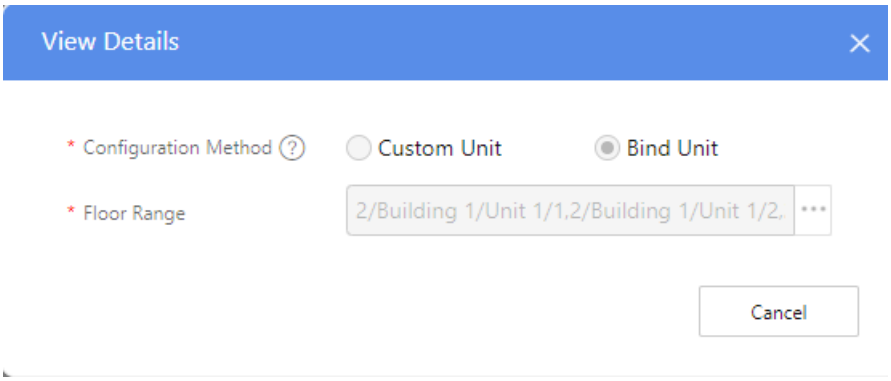


1. Click the corresponding for the elevator controller to expand the bound floors.
2. Click the corresponding for the floor, or select the floor and then click **Control Mode** to change the floor control mode.
   - Free Mode: All elevator users can light up the elevator buttons for that floor.
   - Controlled Mode: Only the verified elevator users can light up the elevator button for that floor.
   - Forbidden Mode: No elevator user can light up the elevator button for that floor.

View Elevator Control Configuration

Click the corresponding to view the detailed elevator control configuration.

Note:
Elevator control configuration cannot be modified directly. To modify the configuration method, you need to clear the configuration, and then configure again.

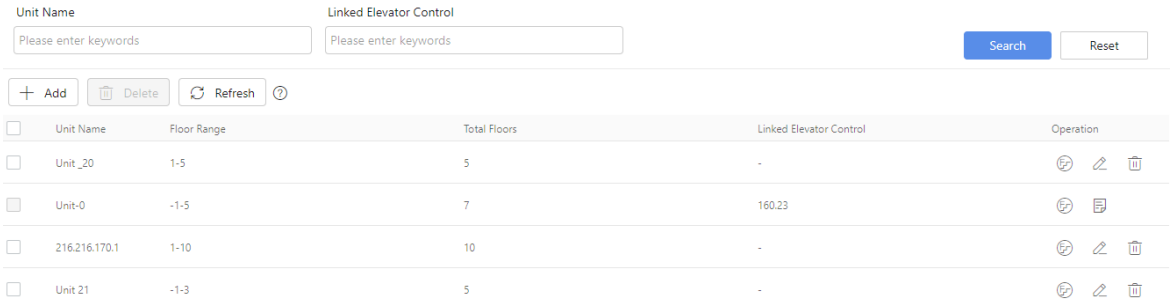


Clear Configuration

Select the elevator controller, click **Clear Configuration**, or click in the **Operation** column, to clear the bound floors and personnel permissions and restore the unconfigured state.

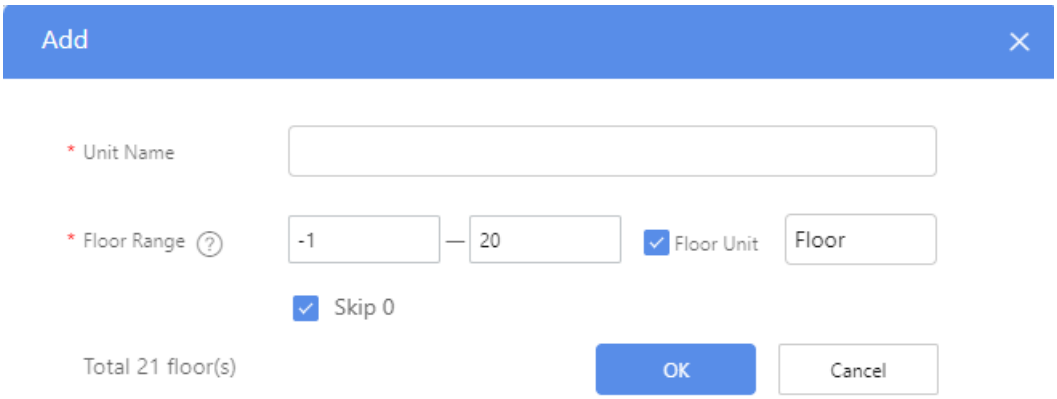
16.1.2 Custom Units

If the existing units in the community do not meet the elevator floor requirements, you can customize and add units and floors.



Add a Custom Unit

1. Click **Add**.

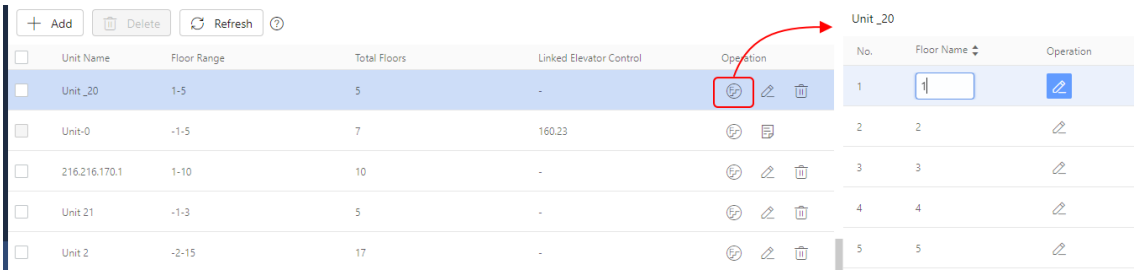


Unit Name	Enter a custom name.
Floor Range	Enter the range of floors.
Floor Unit	• If selected, the floor names will include units (such as "1st Floor"), and you can input a custom name as needed. • If cleared, the floor names will not include units.
Skip 0	If selected, the generated floors will not include the 0th floor.

2. Click **OK**.

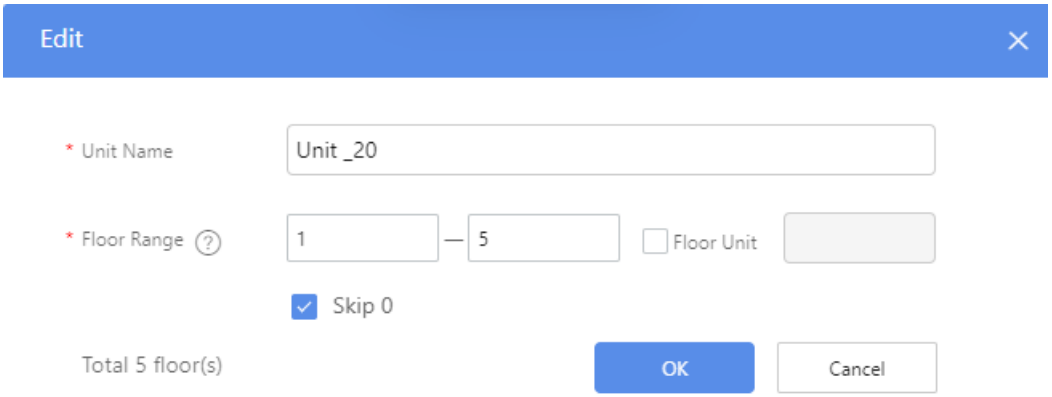
Edit Floor Name

1. Click for the corresponding unit to expand the floor list.
2. Click for the corresponding floor to edit the floor name.



View and Edit Units

- If the unit is not bound to any elevator controller, you can click corresponding to edit the unit configuration.



- If the unit is already bound to an elevator controller, you can click the corresponding to view the unit configuration (cannot modify).

Delete a Unit

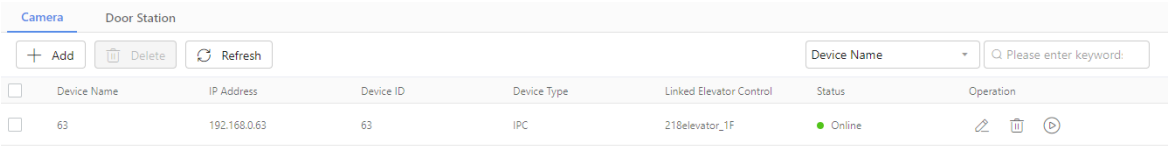
- If the unit is not bound to any elevator controller, you can click the corresponding to delete the unit.
- If the unit is already bound to an elevator controller, you need to clear the binding relation in Floor Configuration before you can delete the unit.

16.1.3 Link Devices

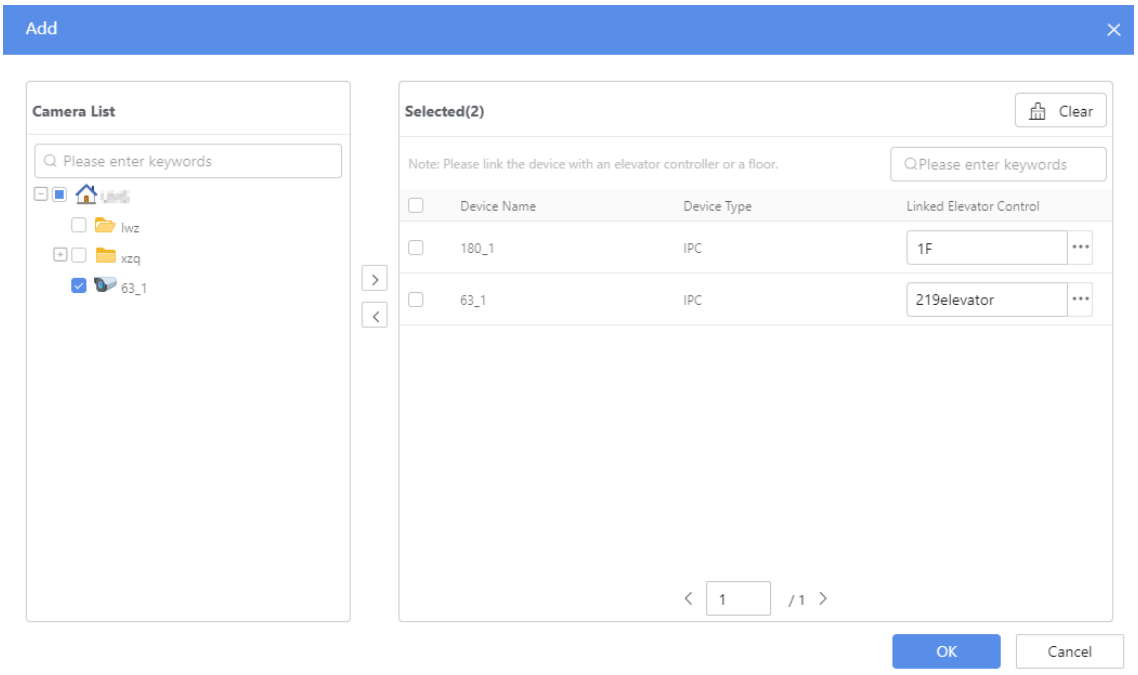
Link cameras, door stations, and video intercom devices with an elevator controller.

16.1.3.1 Camera

Link camera(s) with an elevator controller to view the live video of people entering/exiting the elevator. See Elevator Live Video.



1. On the **Camera** tab, click **Add**.



2. Select camera(s), and then click > to add the selected camera(s).

   Note:
   An elevator controller can link with multiple cameras; a camera can link with only one elevator controller location.

3. Choose the location of the linked elevator controller. You can choose an elevator controller or a floor.
4. Click **OK**.

To a linked camera, you can:

- : Modify the location of the linked elevator controller.
- : Remove the link between the camera and the elevator controller.
- : Go to Smart Live View to view the live video from the camera.

16.1.3.2 Door Station

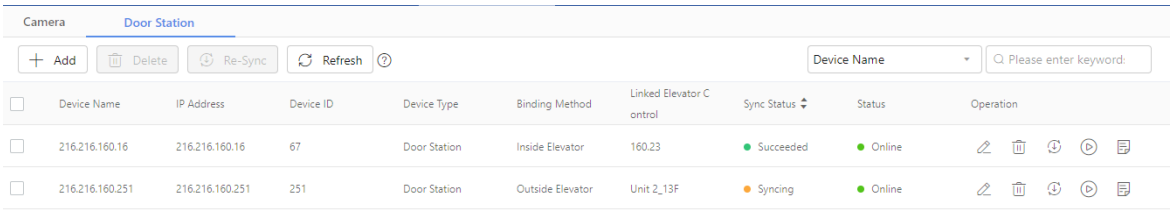
For scenarios where the elevator controller is bound to a custom unit.

After linking the elevator controller with a door station, elevator users can verify identity on the door station to gain access to the specified floors; administrators can view the live video from the door station and its access records.

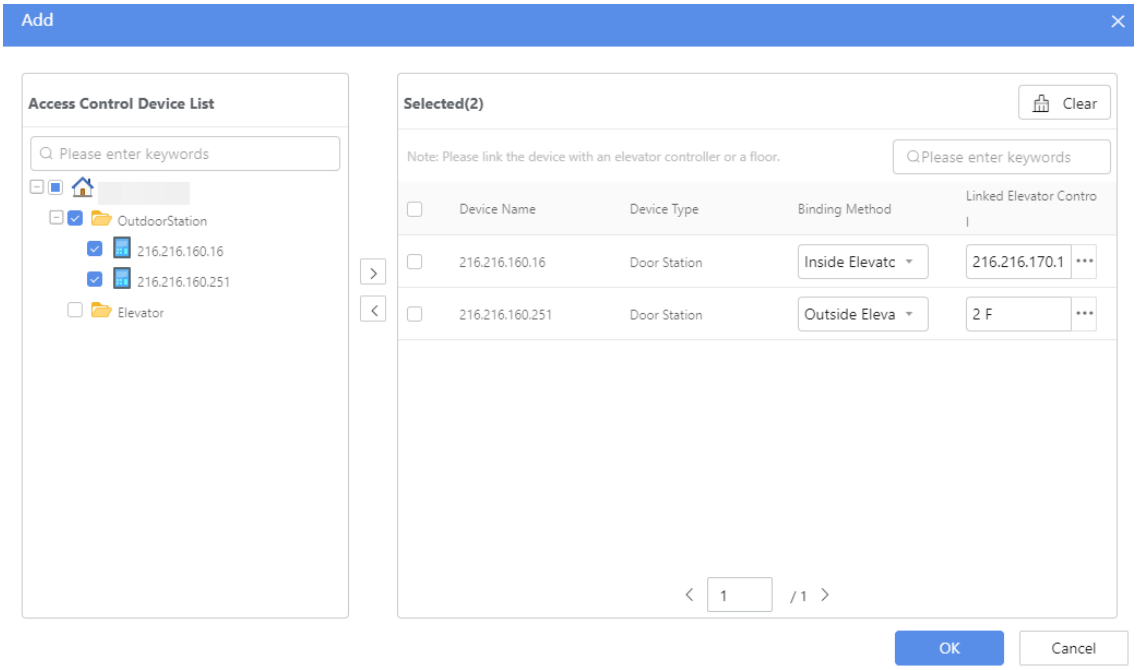
- The door station is outside the elevator: After successful verification on the door station, the elevator user calls the elevator to his/her current floor, and the elevator controller grants access to allowed floor(s).
- The door station is inside the elevator: After successful verification on the door station, the elevator controller grants access to the allowed floor(s).

Note:

- Door station permissions and elevator control permissions need to be configured separately for elevator users.
- After elevator users call the elevator through a door station, Pass-Thru Records will be generated, Elevator Controller Verification Records will not.



1. On the **Door Station** tab, click **Add**.



2. Select door station(s), and then click > to add the selected door station(s).

   Note:
   An elevator controller can link with multiple door stations; a door station can link with only one elevator controller location.

3. Choose the binding mode and the location of the elevator controller.
   - If the door station is **outside the elevator**, choose the floor of the elevator controller.

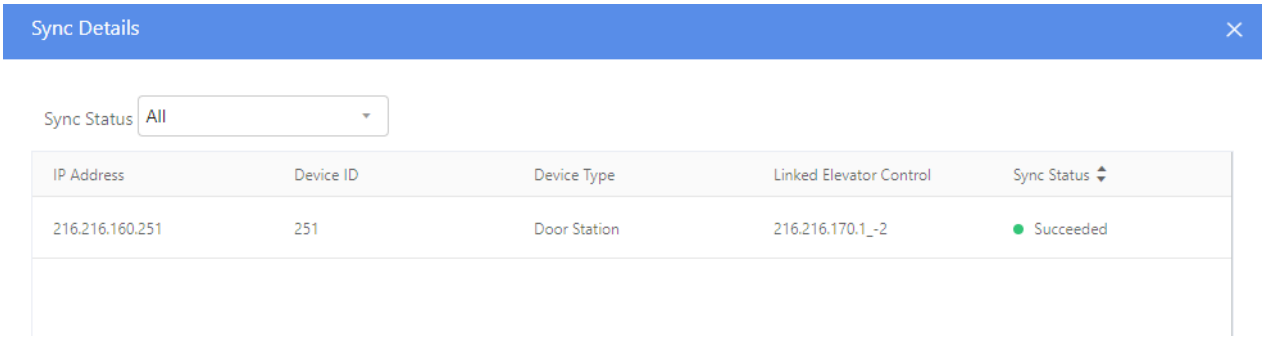
     Note:
     Here, only floors of a custom unit can be linked; to bind the door station to a unit, go to Video Intercom to configure the device location.

   - If the door station is **inside the elevator**, choose the elevator controller.
4. Click **OK**.

For a linked door station, you can:

- : Modify the location of the linked elevator controller.
- : Delete the link between the door station and the elevator controller.
- : After linking with a door station for the first time, the system will automatically sync door station information to the elevator controller. If the sync failed, you can click this button to resync.

  Note:
  Sync can succeed only when the device is online.
- : Go to Elevator Live Video to view the live video from the door station.
- : View the location of the linked elevator controller.



16.1.3.3 Video Intercom

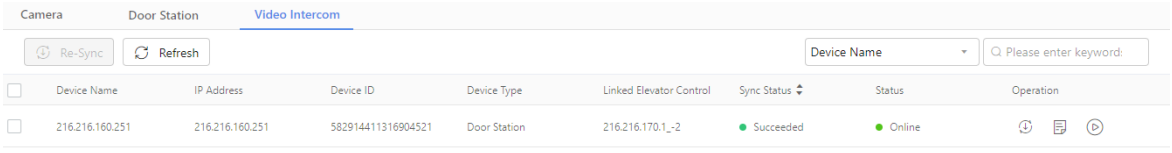
For scenarios where the elevator controller is bound to a community unit.

After linking the elevator controller with a door station at community floor, elevator users can use the door station to verify identity or call an indoor station for remote door opening so as to gain access to the allowed floor(s).

- After successful verification on the door station, an elevator user can call the elevator to his/her current floor; and the elevator controller will grant access to the allowed floor(s) (if the elevator user has access to only one floor, the corresponding floor button automatically lights up; if the elevator user has access to multiple floors, he/she needs to push the elevator button manually).
- The elevator user uses the door station to call an indoor station, or people in the room uses the indoor station to view the live video from the door station and opens the door remotely. The elevator arrives at the floor where the door station is located and automatically lights up the button for the floor where the indoor station is located.

Note:

- Door station permissions and elevator control permissions need to be configured separately for elevator users.
- After elevator users call the elevator through a door station, Pass-Thru Records will be generated, Elevator Controller Verification Records will not.



Follow the steps to bind the elevator controller with door stations. And then the Video Intercom tab will be displayed.

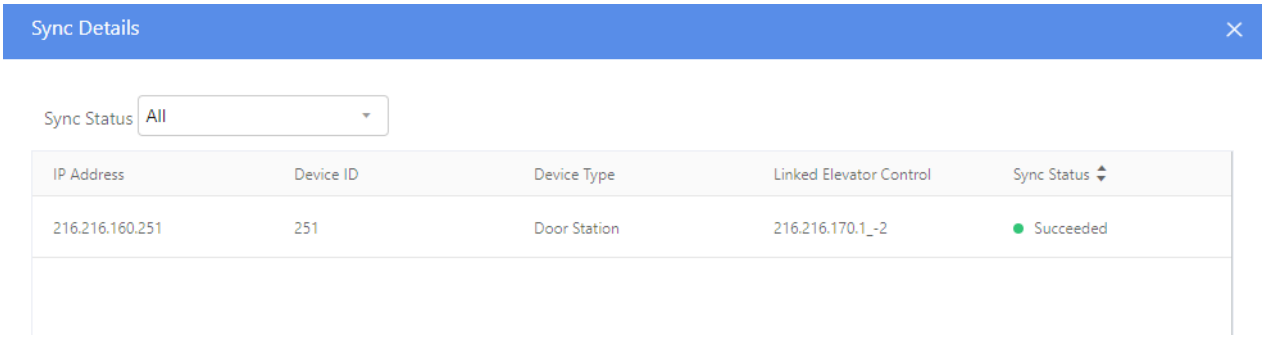
1. Go to **Video Intercom** > **Device Location Config** to bind door stations with floors in the unit, and bind rooms with indoor stations.
2. Go to **Elevator Control Permission** > **Floor Configuration** to bind the elevator controller with the unit (which shall include the floors where the door stations are located).
3. After the operation is completed, the system automatically generates the linking between the door station and the elevator controller.

For a linked door station, you can:

- : After linking with a door station for the first time, the system will automatically sync door station information to the elevator controller. If the sync failed, you can click this button to resync.

  Note:
  Sync can succeed only when the device is online.

- : View the location of the elevator controller linked with the door station (the door station automatically links with the corresponding floor).



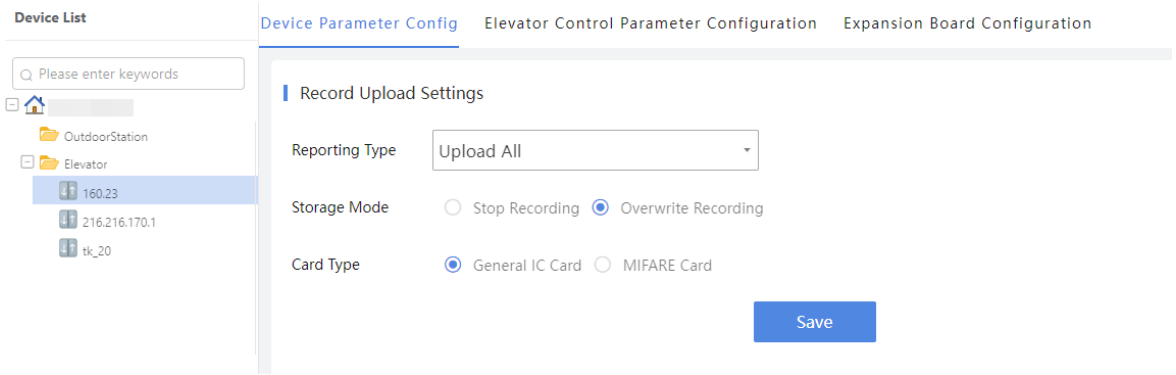
- : Go to Elevator Live Video to view the live video from the door station.

16.1.4 Device Parameter Configuration

Select the elevator controller in the device list and configure the device's own parameters.

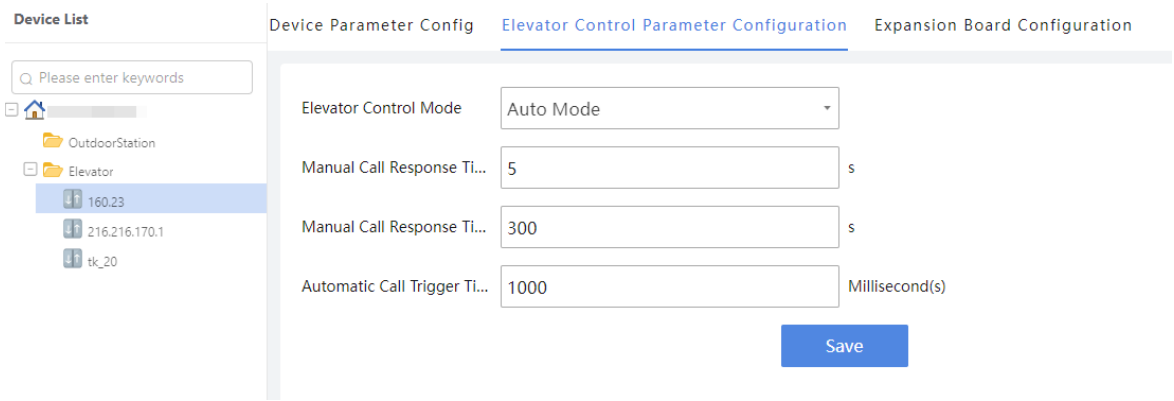
Note:
You can also configure device parameters in the device's web interface. The UI display may vary with the device version. If there are differences, please refer to the user manual of the device.

Device Parameter Configuration -- Record Upload Settings



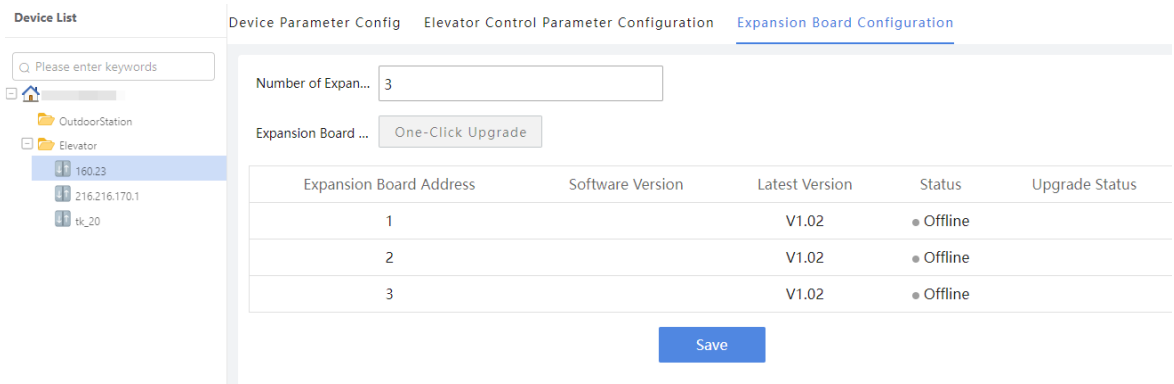
Reporting Type	For the elevator controller's verification records: • Upload All: Upload all person records, including person records of successful and failed verifications. • Upload successful records only.
Storage Mode	When verification records reach the device's specification limit: • Stop Recording: Stop receiving new records. • Overwrite Recording: New records overwrite the oldest records.
Card Type	Choose the card type that the elevator controller will use for verification (either general IC card or MIFARE card). MIFARE cards can be configured with keys to encrypt sectors and prevent data leakage from the cards.

Elevator Control Parameter Configuration



Elevator Control Mode	• Auto Mode: Upon successful verification, all elevator floors that the elevator user has access to automatically light up. • Manual Mode: Upon successful verification, the elevator user needs to press the elevator button manually. • Adaptive Mode: Upon successful verification, if the elevator user has access to only one floor, the elevator floor automatically lights up; if the elevator user has access to multiple floors, he/she must press the elevator button manually.
Manual Call Response Time (Inside Elevator)	Upon successful verification through the card reader inside the elevator or through the door station, the elevator user can press the floor button within N seconds; after N seconds, the access permission becomes invalid.
Manual Call Response Time (Outside Elevator)	Upon successful verification through the door station outside the elevator, the elevator user can press the floor button within N seconds; after N seconds, the access permission becomes invalid.
Automatic Call Trigger Time	Once the elevator button lights up, the elevator controller sends a signal to the elevator. • The elevator will only proceed to the target floor after this signal lasts for a certain length of time (N milliseconds). • If the signal disappears before this period (e.g., due to a mistaken press), the command is ignored.

Expansion Board Configuration



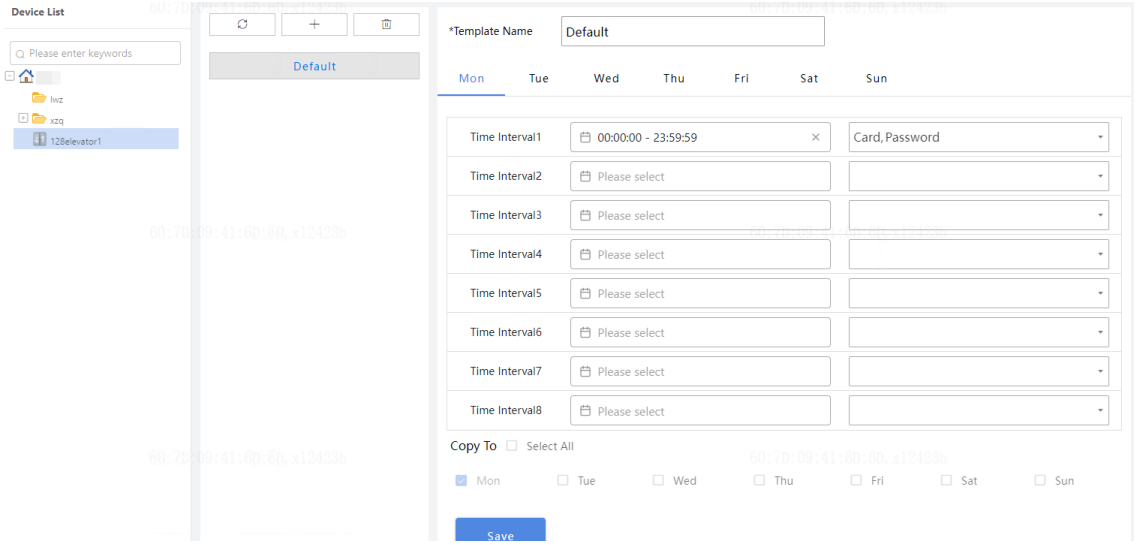
1. Enter the number of expansion boards connected to the elevator controller, and then click **Save** to automatically obtain the version information of the expansion boards.
2. Click **One-Click Upgrade** to upgrade the version of the expansion boards to the latest version.

16.1.5 Verification Template Configuration

Verification templates define different verification methods for different time periods for the device. You can preconfigure different verification templates and quickly apply them to different card readers of the elevator controller.

Note:
You can also configure verification templates in the device's web interface. The UI display may vary with the device version. If there are differences, please refer to the user manual of the device.

1. Select the elevator controller in the device list to view its existing verification templates.
   The system has a default verification template that is effective all day, supporting number allowlist or password comparison; the template can be modified but not deleted.



2. Click ＋ to add a new template, or select a template to modify it.

Time Interval	The verification time periods on the same day cannot overlap.
Verification Method	You can select multiple verification methods at the same time. • Number allowlist: Verification is successful if the swiped card number matches the person's card number in the library. • Password comparison: Verification is successful if the input password is correct. • Number allowlist + password comparison: Verification is successful if both the card number and the password are correct.
Copy To	After setting the verification method for a day, select other days and then click **Save**. The current configuration will be copied to other days.

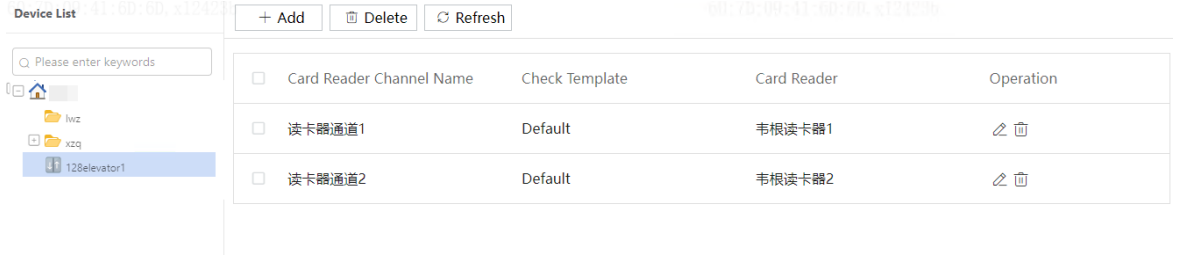
3. Click **Save**.

16.1.6 Verification Configuration

Bind card readers to the elevator controller, and bind verification templates to the card readers.

Note:
You can also configure verification in the device's web interface. The UI display may vary with the device version. If there are differences, please refer to the user manual of the device.

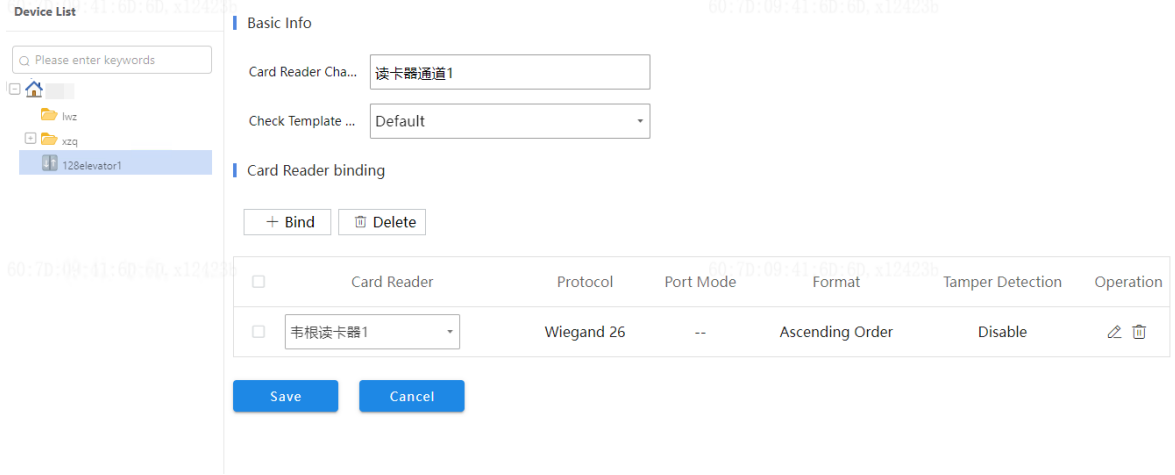
In the device list, select the elevator controller to view the card readers under it; an elevator controller supports up to two card readers.



Add Card Reader Channel

The card reader must be physically connected to the Wiegand interface/RS485 interface on the elevator controller.

Click **Add**, complete the configuration according to the instructions in the table below, and then click **Save**.



Card Reader Channel Name	Enter a custom name.
Verification Template Binding	Choose the verification template.
Card Reader Binding	Click **Bind**, and select the card reader type (Wiegand or RS485) based on the actual wiring. Click to modify the protocol parameters of the corresponding card reader.

Modify Card Reader

Click to modify the parameters of the corresponding card reader channel, such as verification template, bound device.

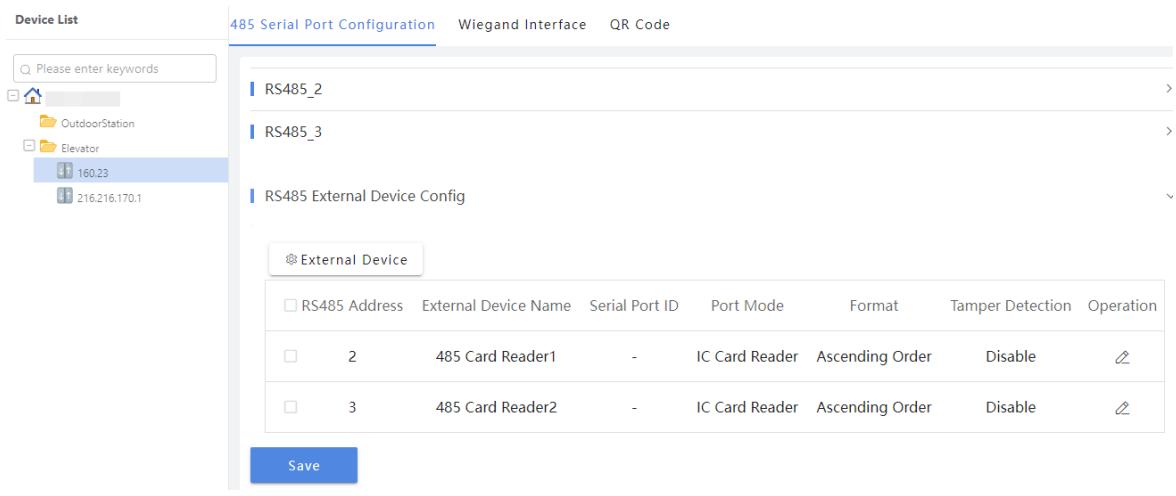
Delete Card Reader

Click for the card reader channel you want to delete, and then confirm the deletion.

16.1.7 External Device Configuration

Note:
You can also configure external devices in the device's web interface. The UI display may vary with the device version. If there are differences, please refer to the user manual of the device.

485 Serial Port Configuration

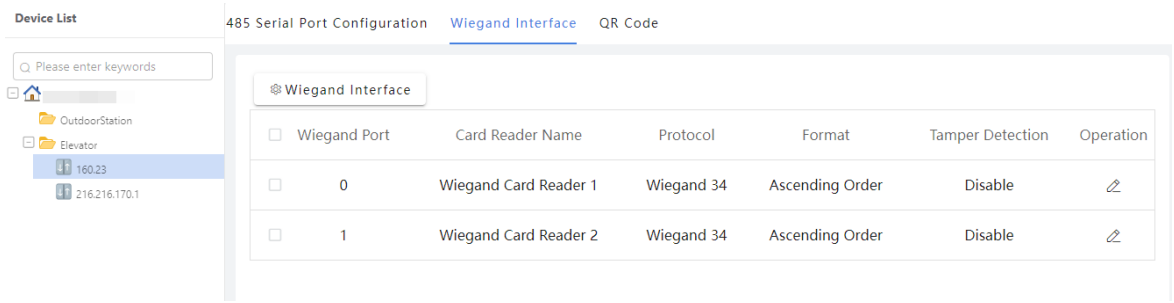


- Modify the data transmission parameters for RS485_2 and RS485_3; generally, using the system default values is sufficient.
- Configure the card readers connected to RS485_2 and RS485_3.

Parameter	Description
Card Reader Name	Enter a unique custom name.
Port Mode	• Disable: The port mode is disabled. • IC card reader: Connects an IC card reader. • QR code reader: Connects a QR code reader.
Port Number	When the serial port mode is set to QR code reader, this parameter must be configured and must be unique.
Format	• Ascending order: The card number sequence is the same as the sequence read by the card reader • Descending order: The card number sequence is the reverse of the sequence read by the card reader.
Tamper Detection	When enabled, an alarm will be triggered when card reader tampering is detected.
Copy To	Used to apply the same settings to other card readers.

Wiegand Interface Configuration

Configure the card reader connected to the Wiegand interface.

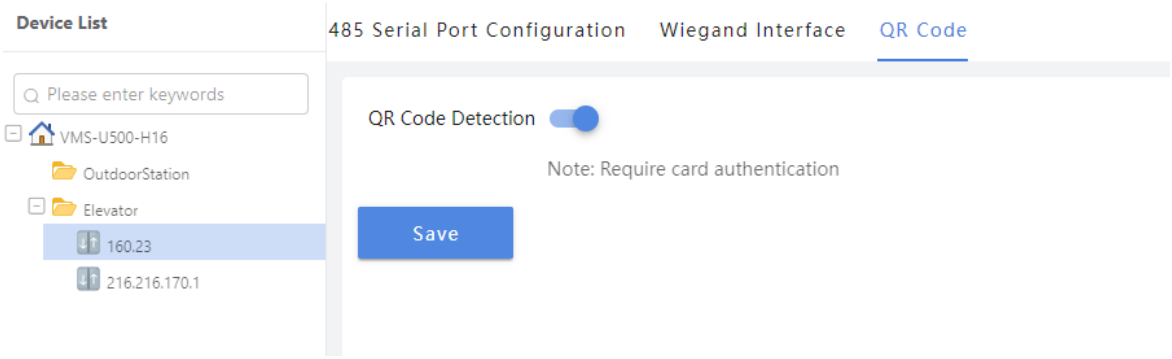


Parameter	Description
Card Reader Name	Enter a unique custom name.
Protocol	• Wiegand 26: Card numbers are read using the Wiegand 26 protocol (only reads 3-byte card numbers). • Wiegand 34: Card numbers are read using the Wiegand 34 protocol (only reads 4-byte card numbers). • Custom Wiegand: Protocols used by Wiegand card readers other than 26 and 34 (configuration rules need to be set in the device interface).
Format	• Ascending order: The card number sequence is the same as the sequence read by the card reader • Descending order: The card number sequence is the reverse of the sequence read by the card reader.
Tamper Detection	When enabled, an alarm will be triggered when card reader tampering is detected.
Copy To	Used to apply the same settings to other card readers.

QR Code Configuration

With QR code detection enabled, when operating in the number allowlist verification mode, people can scan QR codes on the connected QR code reader for verification.

Note:
The platform currently does not support generating QR codes for card numbers.



16.2 Elevator Control Permission

Access&Attendance > Access Control.

Configure floor access permissions and the validity period of access permissions. After completing the configuration, you can view, search, and modify the permissions as needed.

The configuration steps are as follows:

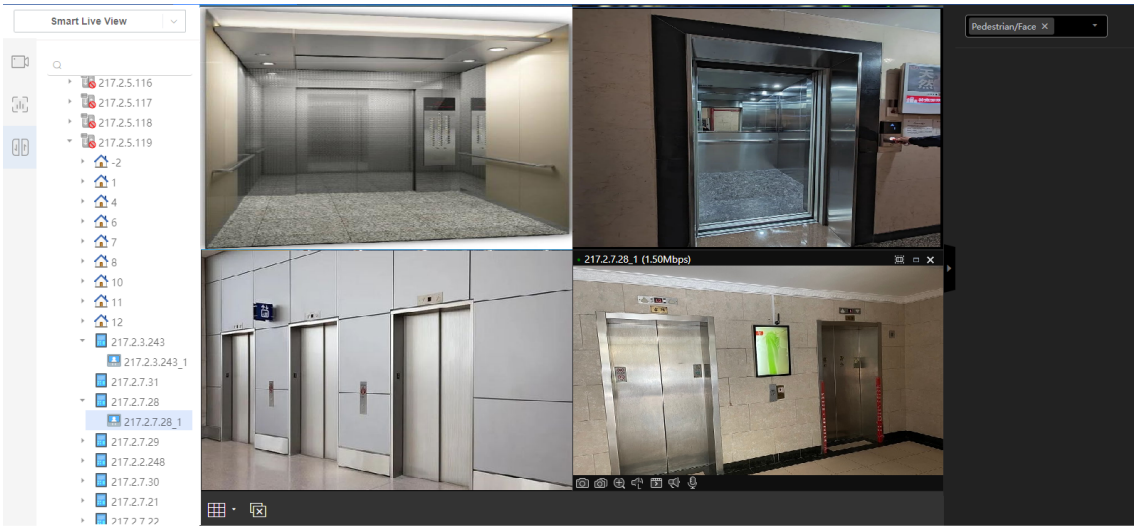
1. Schedule Template
2. Access Permission Config
3. Permission Search

16.3 Elevator Live Video

Go to **Video Application** > **Smart Live View** > **Elevator Live Video**.

After the elevator controller is linked with cameras or door stations, you can view live video from the linked devices to monitor the conditions inside and outside the elevator.

1. On the **Linked Device** page, click ▷ for a device to go to the **Smart Live View** page.
2. Click the **Elevator Live Video** tab, find the elevator controller on the resource tree.
3. Expand the elevator control device to view the linked cameras or door stations.
4. Drag the device to a window, or right-click the device and then choose **Start Live View**, to start its live video.



5. Real-time face snapshots are displayed on the right.

16.4 Elevator Controller Verification Records

Go to **Data Search > Access Records > Elevator Controller Verification Records**.

Search verification records from elevator card readers to monitor personnel elevator usage records.

Note:

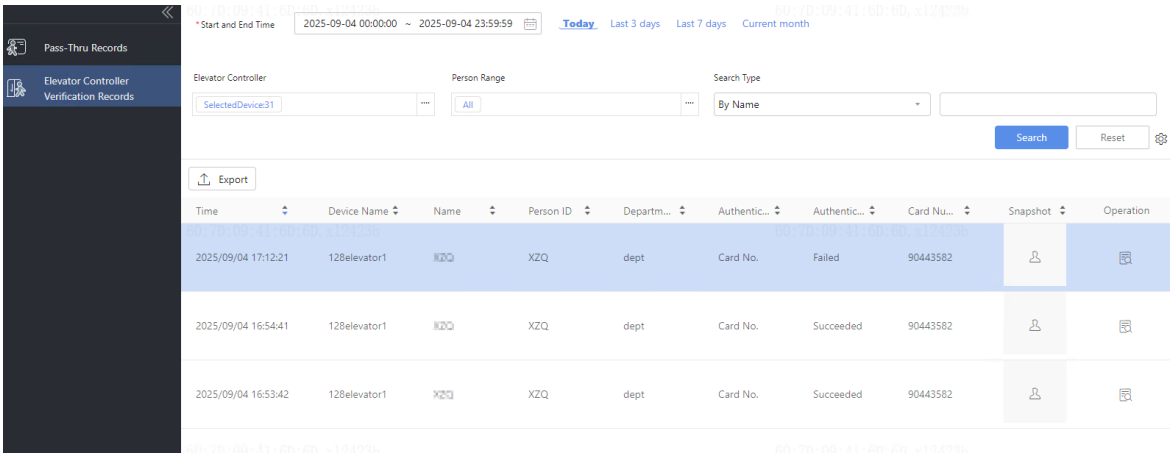
- The elevator controller's verification records will be synced in real time to the platform.
- Conditions for successful verification: the credential is correct, the credential is within its validity period, and the elevator user has the elevator control permission.
- To query verification records of door stations linked with elevator, go to Pass-Thru Records page.

Search Verification Records

Select the start and end times, elevator controller, person range (department/visitor/stranger), search type (by name/by card number/by employee ID), authentication (Card No./Password/Card Number + Password), and authentication result (succeeded/failed), and then click **Search**. The elevator controller verification records that meet the search criteria are displayed.

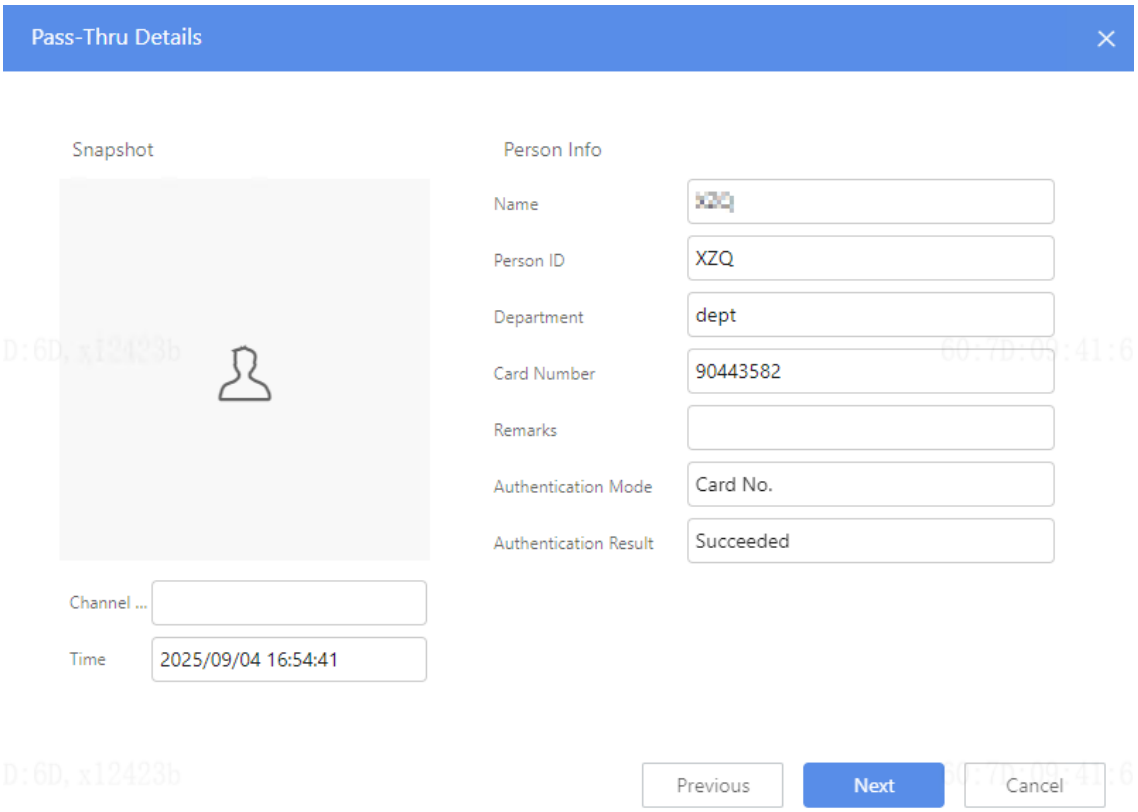
Note:

You can click to the right of the search criteria to customize the search criteria.



More Operations

- Export records: Select verification records and then click **Export** to export the selected verification records.
- View details: Click in the **Operation** column to view the details of the corresponding record.



17 Video Intercom

Go to **Access&Attendance > Video Intercom**.

Video intercom is mainly used in residential scenarios.

Video intercom can be performed between visitors (via door stations installed at the building entrance or zone stations installed at the community entrance), residents (via indoor stations installed at home), and security personnel (via client in management center or security room) to provide efficient access control.

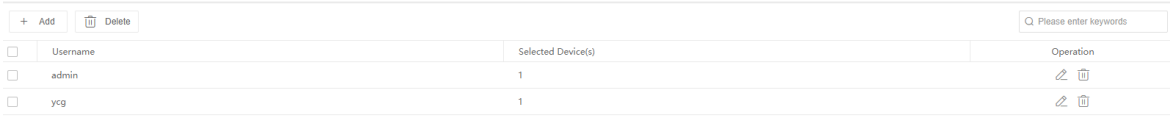
Workflow

1. Add zone stations, door stations and indoor stations. See Private Device.
2. Add persons and rooms, and then associate persons with rooms. See Personnel Management or Room Management.
3. Configure call and answer permissions for client users. See Call Recipient Management.
4. Associate the installation location (building or room) for zone stations, door stations and indoor stations to correspond with residents and clarify device usage for inbound and outbound persons. See Device Location Config.
5. Use zone stations, door stations, indoor stations, and the client to perform video intercom. See Incoming Call and Outgoing Call.
6. View intercom records. See Call Records.

17.1 Call Recipient Management

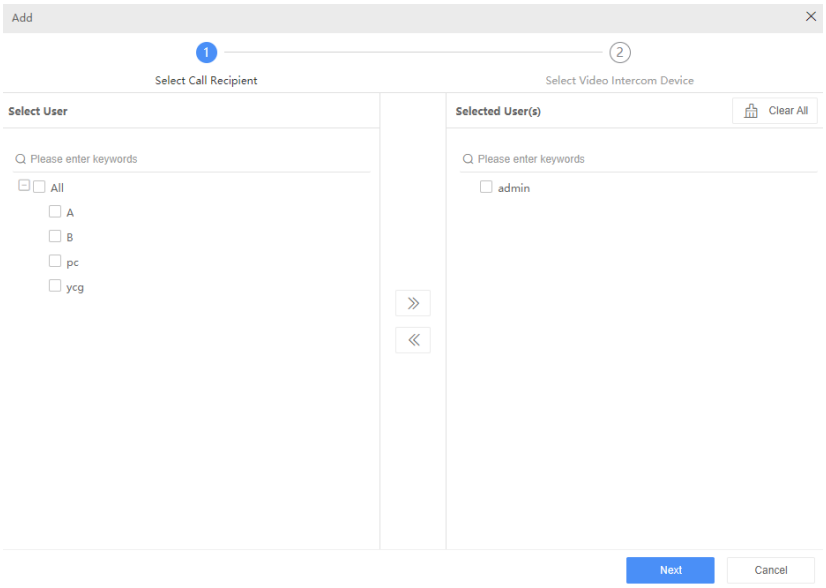
Assign answering permissions to different video intercom devices for different users. This configuration is used to manage the permissions of property managers.

Go to **Video Intercom** > **Call Recipient Mgt**.

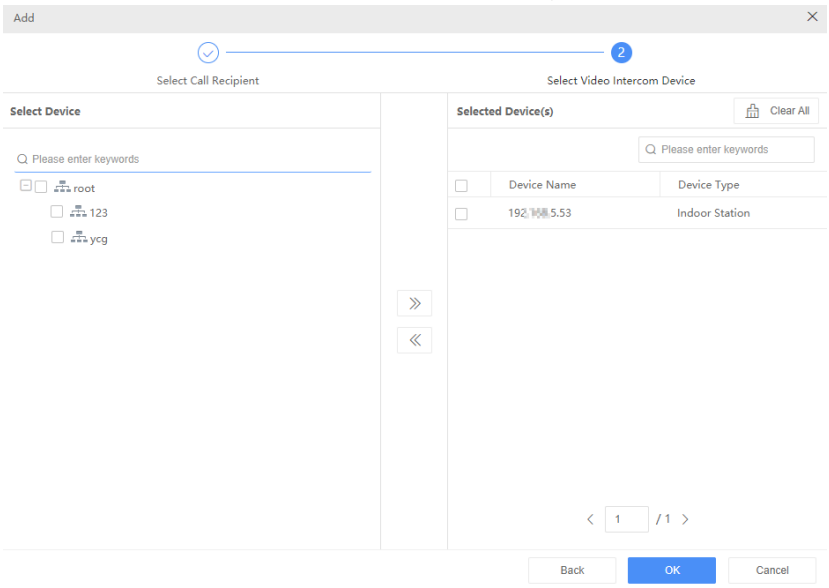


17.1.1 Add Call Receipt

1. Click **Add**. A page as shown below appears.
2. Select the user(s) from the left-side list and click » to add to the right-side list.



3. Click **Next**.
4. Select the device(s) from the left-side list and click » to add to the right-side list.



5. Click **OK**.

17.1.2 User Management

- Edit: Click in the **Operation** column to view the list of the devices the user can answer. You can add or delete devices as needed.
- Delete call recipient: Click in the **Operation** column, or select the user(s) to be deleted and click **Delete**.

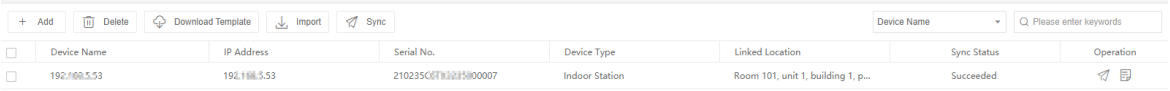
17.2 Device Location Config

Associate the installation location (community entrance/building/room) with the zone station, door station and indoor station, so as to match devices with residents and to specify devices used by callers and call recipients.

Prerequisite

- Zone stations, door stations and indoor stations have been added to the platform. See Device Management > Private Device.
- Buildings and rooms have been added to the community. See Room Management > Add Room.

Go to **Video Intercom** > **Device Location Config**.

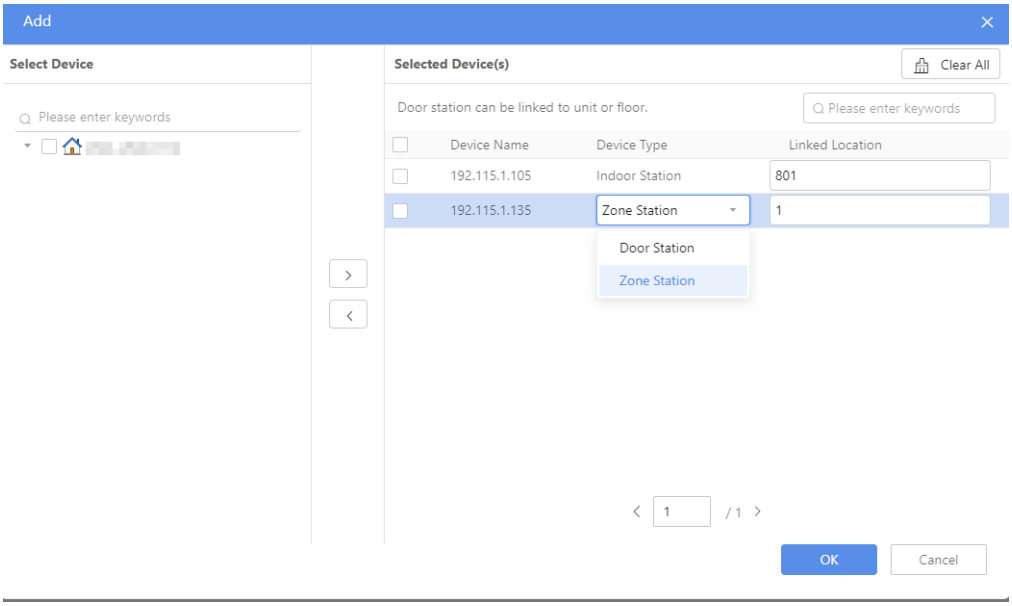


17.2.1 Add Device Location

You can add device locations in batches or one by one.

Add Directly

1. Click **Add**. A page as shown below appears.



2. Select device(s) from the left-side list and click » to add them to the right-side list.
3. Select the device location in the **Linked Location** column. A zone station can be linked with a phase. A door station can be linked with a unit or floor. An indoor station can be linked with a room.

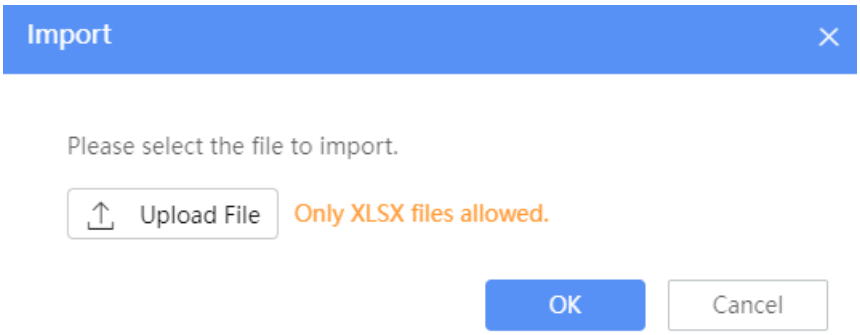
   Note:

   - After adding an outdoor station to the selected device list, you need to choose the device type (zone station or door station).
   - A community can be linked with multiple door stations; a room can be linked with multiple indoor stations.
   - To delete the selected devices from the right-side list, click **Clear All**; or select devices and click « to delete them from the list.
4. Click **OK**.

Add in Batches

1. Click **Download Template**.

2. Fill in the template with information about the device and its location, and then save.
3. Click **Import**. A dialogue box appears.



4. Click **Upload File** and select the completed template.

   Note:
   The file size cannot exceed 1MB.

5. Click **OK**.

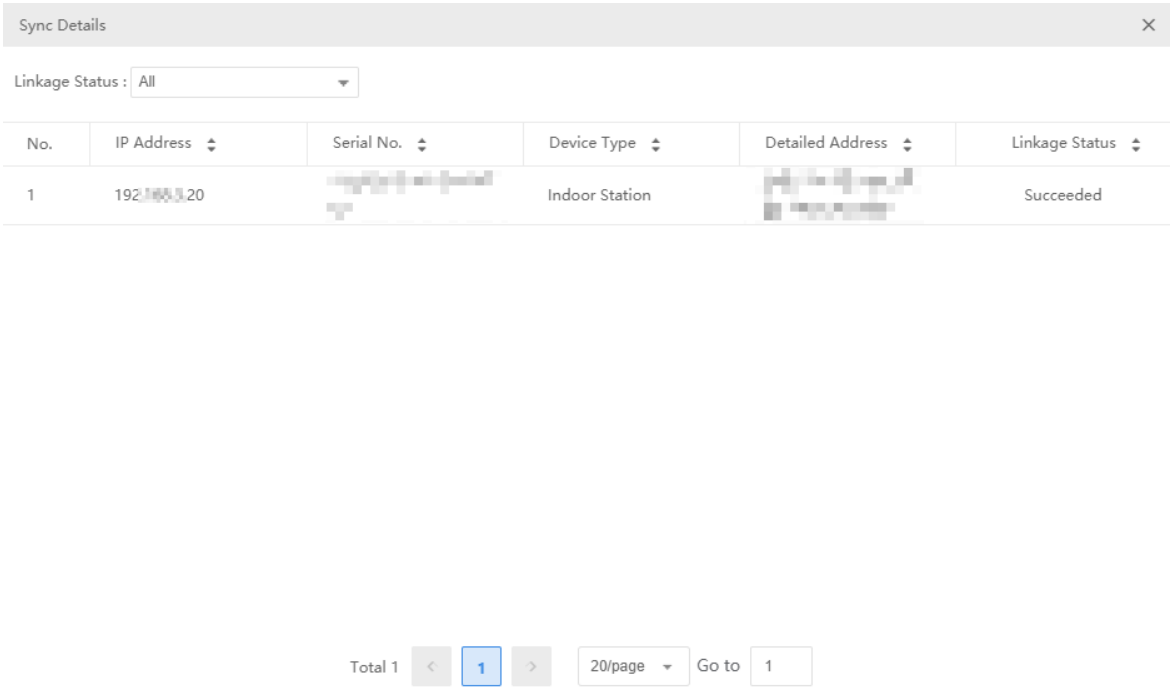
17.2.2 Sync Location

- Sync in batches: Select the devices in the device list and click **Sync** to synchronize the location information.
- Sync one by one: Click in the **Operation** column to synchronize the location information.

17.2.3 View Details

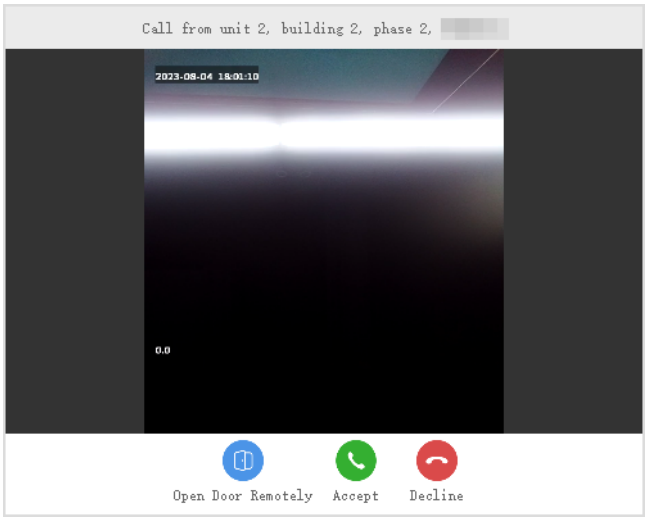
Once a zone station is linked with a phase, and the door station is linked with a unit, the zone station and the door station will be linked to all indoor stations within the respective phase/unit for subsequent call operations.

1. Click for the device to view the linkage status.
2. Filter the devices by selecting the linkage status (Not Linked/Succeeded/Failed).



17.3 Incoming Call

A call window appears on the client when a call comes in from a zone station, a door station or an indoor station. If the call is from the zone station or door station, you can also view the live video from the door station or zone station and open the door on the client.

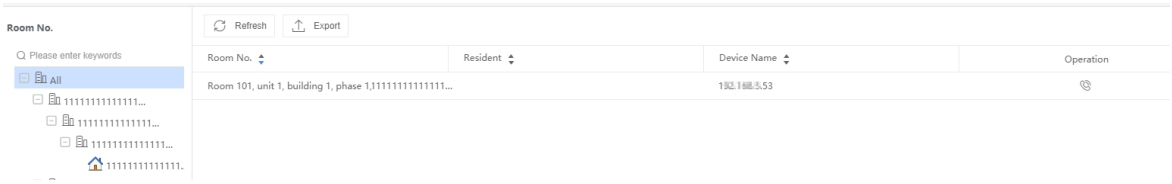


Note:

- Users can only answer incoming calls from the specified devices. See **Call Recipient Management**.
- You can configure the ringtone duration (40s~60s) for the video intercom. The system will end the call when it is not connected within the set duration. See **System Config > Service Config > Video Intercom**.

17.4 Outgoing Call

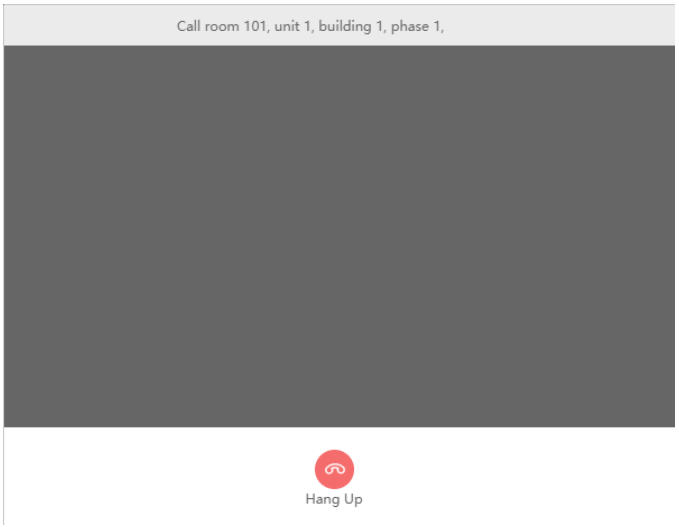
On the **Video Intercom** > **Contacts** page, you can view the residents and the linked indoor station of each room, and make calls to indoor stations.



Note:

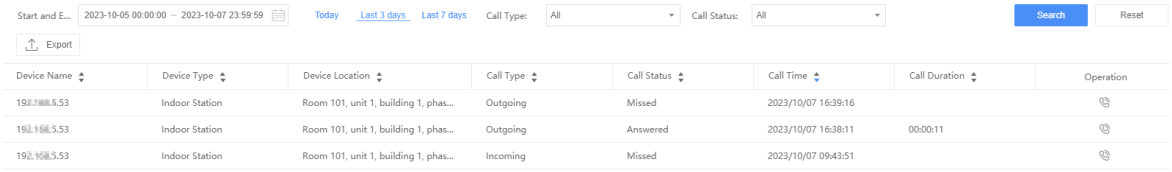
- You cannot call a zone station or a door station from the client.
- Users can only call devices in the organization(s) that they have access to.

1. Select a building/unit/room in the left list to view the rooms and residents.
2. Click for the room in the **Operation** column to call the indoor station linked with that room. Click **Hang Up** to end the call.



17.5 Call Records

View the call records in **Video Intercom** > **Call Records**.



- Search: Set the start and end time, call type, and call status as needed, and click **Search**.
- Call Back: Click in the **Operation** column to call an indoor station.
- Export: Click **Export** above the list to export the search results to a .xlsx file.

18 Attendance Management

Go to **Access&Attendance> Attendance Mgt**.

Attendance management provides an automated and comprehensive solution for tracking employee attendance. Companies can install access control devices at entrances and exits and configure attendance schedules according to their policies. When employees sign in and out using face recognition or card swiping, the attendance records are generated automatically. Administrators can view attendance data, handle leaves, and re-sign in/out for abnormal attendance records, ensuring efficient and accurate attendance management.

Functions

- Attendance Regulations: Set automatic calculation time of attendance.
- Staff Schedule: Configure workdays and daily attendance periods for personnel.
- Attendance Management: Administrators can handle leaves and re-sign in/out for abnormal attendance records.
- Attendance Statistic: View original data, attendance details, and attendance summary of check-in records.

Configuration Workflow

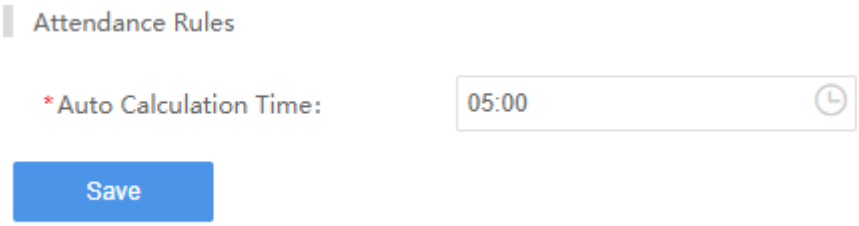
1. Add access control devices (face recognition terminal, general access control device, access controller). See Private Device.
2. Add personnel information. See Personnel Management .
3. Assign access control permissions to individuals. See Access Permission Config.
4. Set attendance schedule for personnel. See Staff Schedule.

5. People sign in/out on access control devices.
6. View attendance records. See Attendance Statistic.

Note:
Conditions for successful attendance recording: correct credentials (face, card, password, etc.), credentials within their validity period, access permission, and sign in within the specified period.

18.1 Attendance Regulations

Set automatic calculation time of attendance. The system will calculate the attendance data of the previous day at the set time every day. You can see attendance data in **Attendance Details**. If the automatic calculation of attendance data fails, please refer to Attendance Details for manual calculation.



18.2 Staff Schedule

Configure workdays and daily attendance periods for personnel.

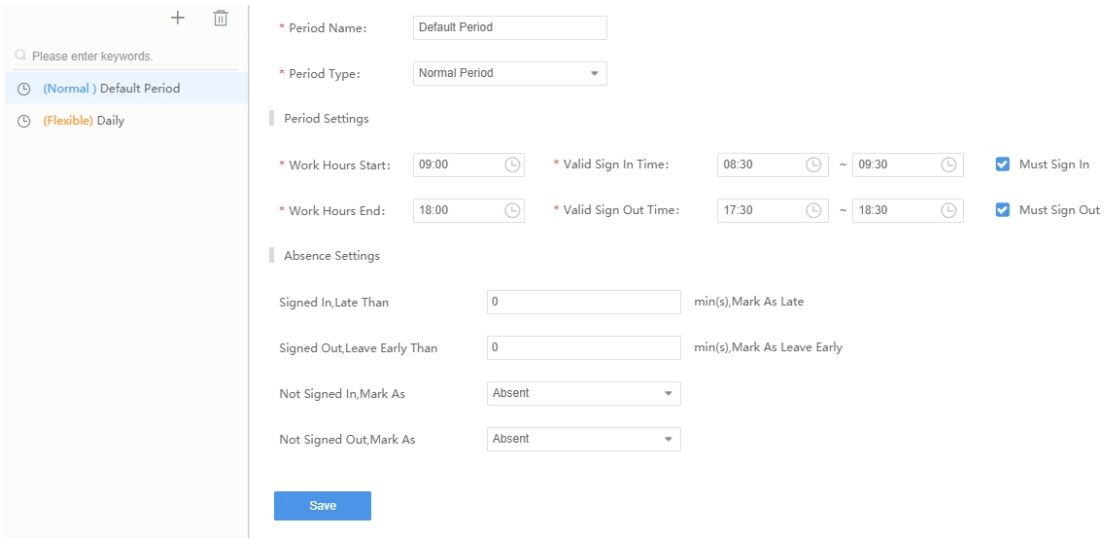
Configuration workflow: Configure daily attendance periods → Configure shift (workdays) → Schedule shifts for personnel (specify shifts)

18.2.1 Set Time Period

Set daily attendance period. There are two types of attendance periods: Normal period and flexible period.

- Normal Period: For normal attendance, employees must sign in&out during the specified valid sign in&out time range.
- Flexible Period: For flexible attendance, employees can go to work at any time, and daily attendance duration can be calculated by the selected flexible duration calculation method.

Normal Period



1. Click +.
2. Enter a name for the period.

3. Select Normal Period.
4. Set when the work hours start and end. One day will be added automatically (+1) if the **Work Hours End** time is earlier than the **Work Hours Start** time. The **Work Hours Start** time and **Work Hours End** time must be within the range of **Valid Sign In Time** and **Valid Sign Out Time**.
5. Set whether sign-in and sign-out are mandatory. If selected:

   (1) Set Valid Sign In Time and Valid Sign Out Time: Specify a valid time range for sign-in and out. The time range includes the boundary values. For example, if the Valid Sign Out Time is 17:30-18:30, then sign-out is allowed during 17:30-18:30.

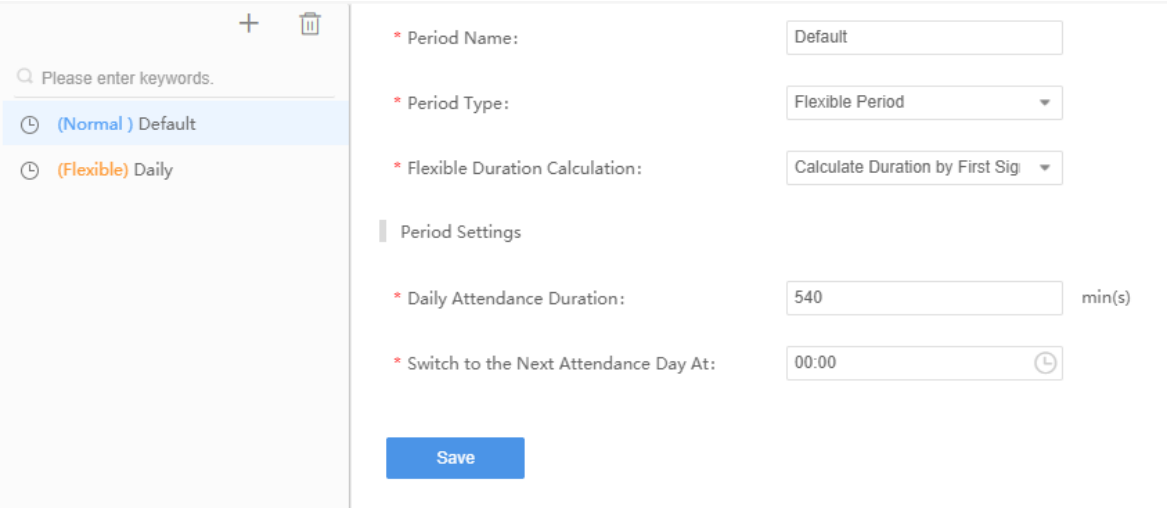
   (2) Configure absence settings.

   - Signed In, Late than x min(s), Mark As Late: If a person signs in within x min(s) after the Work Hours Start time, the attendance status is normal. x is no more than 999.
   - Signed Out, Leave Early Than x min(s), Mark As Leave Early: If a person signs out within x min(s) before the Work Hours End time, the attendance status is Normal. x is no more than 999.
6. Click **Save**.
7. To edit a time period, click the period name on the right window.

Note:

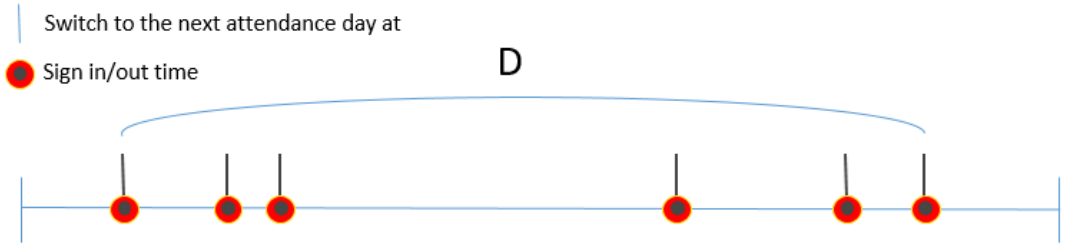
- When **+1** appears in the field, the time will be extended to the next day. All the related times must be earlier than the auto calculation time of the next day.
- The valid sign-in time range must not overlap with the valid sign-out time range.

Flexible Period

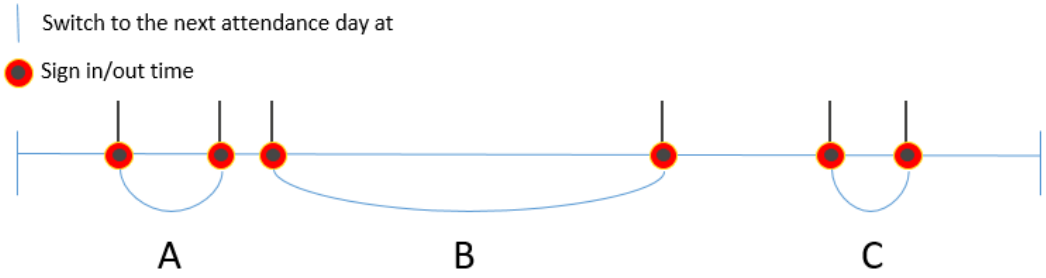


1. Click +.
2. Enter a period name.
3. Select Flexible Period.
4. Select a method of flexible duration calculation.

   - **Calculate Duration by First Sign-in and Last Sign-out**: Take the earliest sign-in time and the latest sign-out time during an attendance day to calculate the attendance duration. Taking the following figure as an example, the attendance duration is D.



- **Cumulate Duration by Multiple Sign Ins&Outs:** The attendance duration is cumulated by the duration of every two sign in&out during an attendance day. As shown in the figure below, the attendance duration is the total time period of the A+B+C. If the number of sign-ins&outs on one day is odd, the administrator can resign-in&out according to the actual situation and then calculate the attendance duration, otherwise all the sign ins&outs of the day would be invalid.



5. (For **Cumulate Duration by Multiple Sign Ins&Outs**) Set a valid sign in&out interval. The sign in&out is valid only if the interval between the two sign in&out is greater than or equal to the set interval.
6. Set a daily attendance duration. Absence will be recorded if the daily working time is less than the set daily attendance duration.
7. Set the time when the attendance day switches to the next attendance day. For example, if 01:00 is set, the attendance day is from today's 01:00 to the next day's 00:59. Signing in&out before 00:59 or at 00:59 in the next day is considered as today's attendance. Signing in&out after 01:00 or at 01:00 in the next day is considered as the next day's attendance.
8. Click **Save**.

Other Operations

You can edit and delete periods as needed.

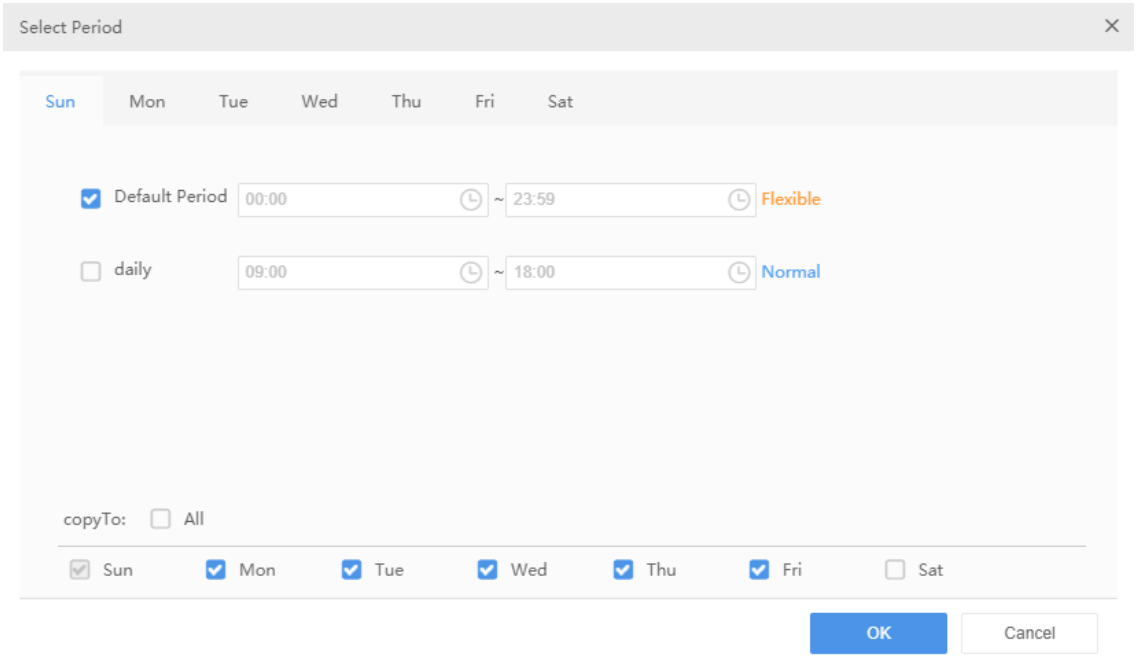
- Edit: Click a period name to edit the corresponding information on the right window.
- Delete: Select a period to be deleted, click , and confirm the deletion.

18.2.2 Shifts Management

Add shifts to set workdays for attendance and associate attendance periods to workdays.

Add Shifts

1. Click , enter the shift name, shift cycle (default is **Week**, repeat by week).
2. Click **Select Period**.



3. Select a workday on which the shift starts.
4. Select a time period (set in Set Time Period), and add it into a shift.

   Note:
   Up to 8 periods are allowed for each shift.
5. Select workday(s) to apply the same settings to other days. You can also select **All** to apply the same settings to every day (Monday through Sunday).
6. Click **OK**.

More Operations

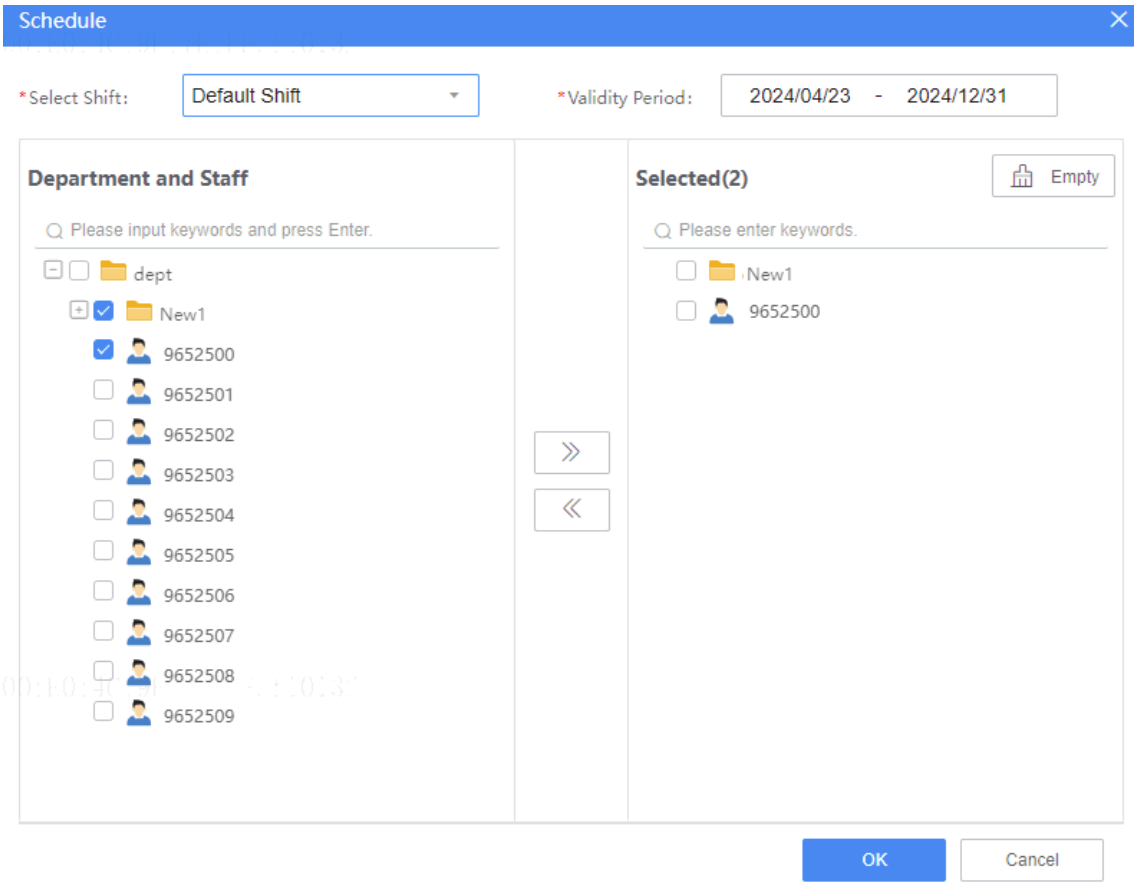
You can edit or delete shifts.

- Edit: Click the shift name and edit the shift information in the right window.
- Delete: Select the shift to be deleted, click , and confirm the deletion.

18.2.3 Schedule Management

Specify shifts for departments or staff.

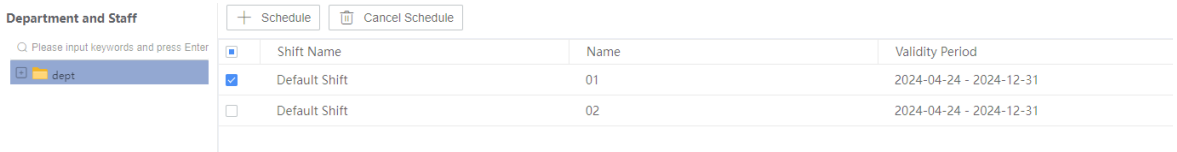
1. Click **Schedule**.



2. Select the department or people for which you want to set schedule (up to 5000 people are allowed for each shift).
3. Select a shift and set a validity period.

   Note:
   People may have multiple shifts with different dates, but each person can have only one shift every day.
   If the validity period of the new shift and the old shift overlap, the overlapping part of the validity periods belong to the new shift.
   If you initially set shift 1 to be executed from 1/1 to 1/31, and later you set shift 2 to be executed on 1/5, then you will have shift 1 being executed from 1/1 to 1/5 and 1/6 to 1/31, and shift 2 being executed on 1/5.
4. Click **OK**.

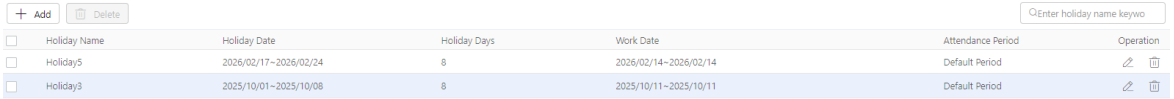
After scheduling shifts, select a department/person on the left side of the **Schedule Management** to view the corresponding schedule. To cancel a shift for a person, select the shift and then click **Cancel Schedule** on the top.



18.2.4 Holiday Adjustment

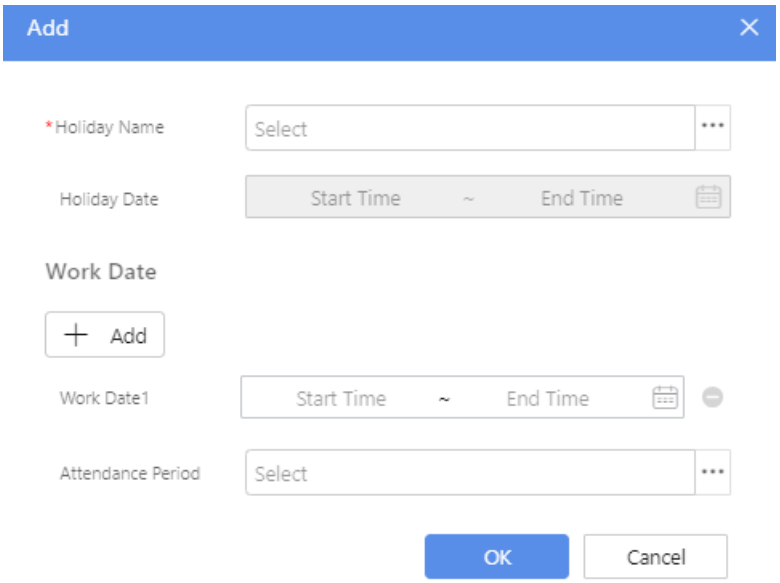
During holiday periods, you can set holiday dates, during which attendance will not be recorded; you can also set make-up workdays, on which normal attendance is required.

For example: If New Year's Day (Jan 1 to Jan 3) is set as a holiday, so attendance is not required from January 1st to January 3rd; if a make-up workday is required on the following Saturday (Jan 6), set January 6th as a workday.

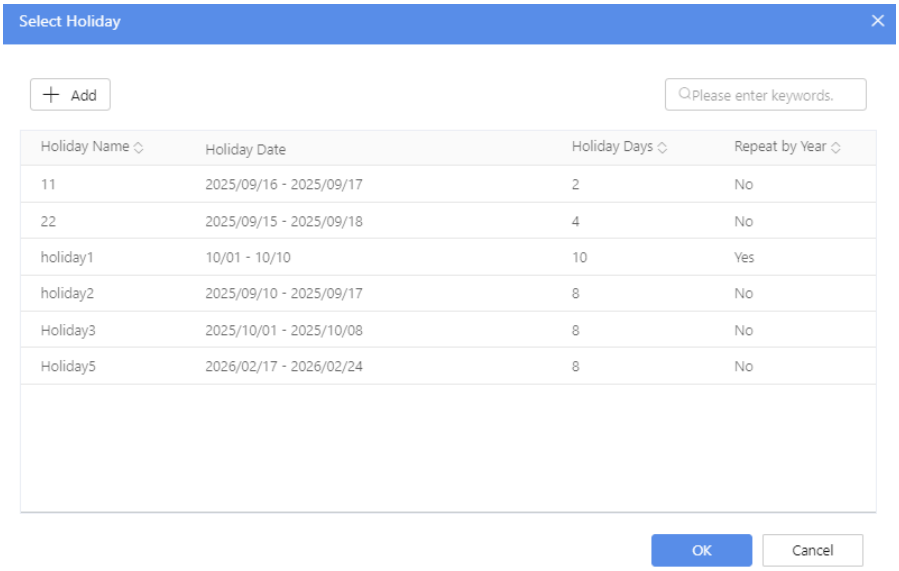


Add Holiday Adjustment

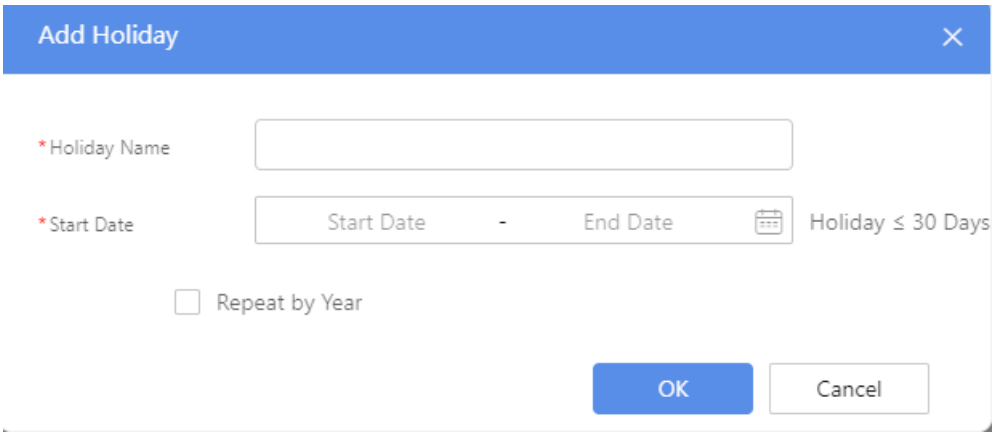
1. Click **Add**. The **Add** dialog box appears.



2. Click the selection box after the holiday name to select the holiday (holidays can be created in advance in **Service Configuration >Holiday Management**). The system will automatically get the holiday start and end dates.



If no holiday exists, click **Add** to add a holiday manually.



3. (Optional) Add work dates and attendance periods. During work dates, check-in and check-out must follow the attendance periods; otherwise, abnormal attendance will be recorded.

Note:

- Work dates and holiday dates cannot overlap.
- If a work date is added, attendance periods must be selected.
- Up to 5 work dates can be added.

4. Click **OK**.

More Operations

Edit or delete holiday adjustments as needed.

- Edit a holiday adjustment: Click the corresponding in the **Operation** column to edit the holiday adjustment.
- Delete a holiday adjustment: Select holiday adjustments and then click **Delete** on the top to delete the selected holiday adjustments; or click the corresponding in the **Operation** column to delete a holiday adjustment.

18.3 Attendance Management

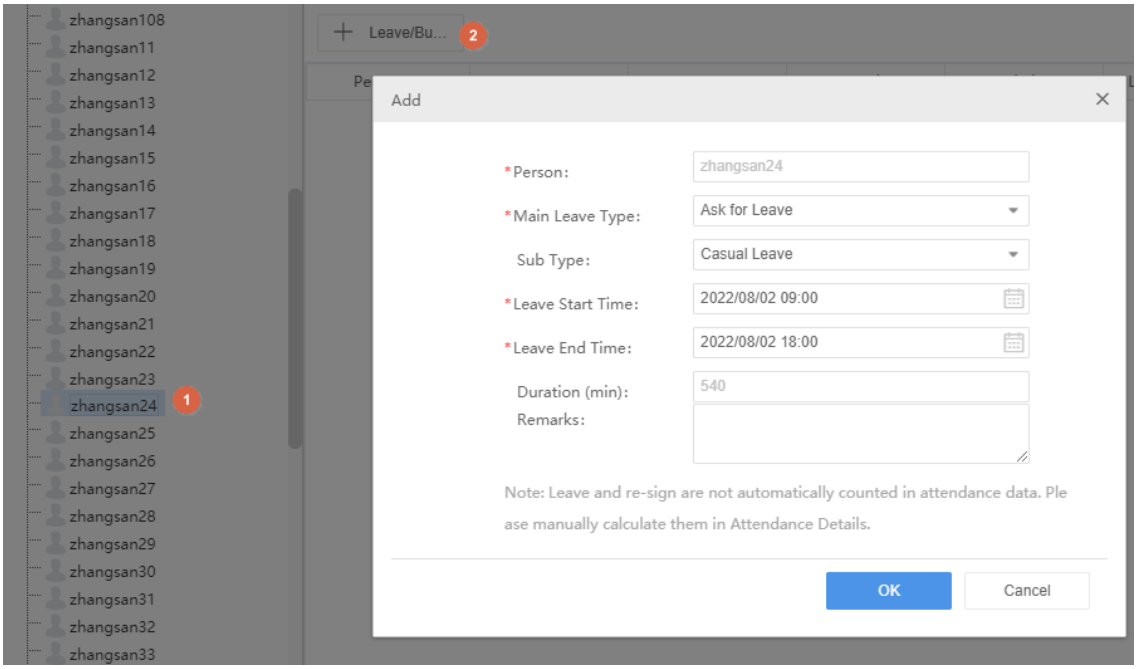
Administrators can handle leaves and re-sign in&out for personnel.

18.3.1 Leave Management

Add leave/business time period records for the staff. The recorded durations will not be seen as abnormal attendance. After a new leave/business record is added, you need to click **Calculate** in Attendance Details to update its attendance status and duration.

Add Leave/Business

1. Select the target person on the organization list.
2. Click **Leave/Business**.



3. Select the main leave type. When the main leave type is set as **Ask for Leave**, you need to select its sub type (specific reason for leave).
4. Set the leave start time and leave end time.
5. Click **OK**.

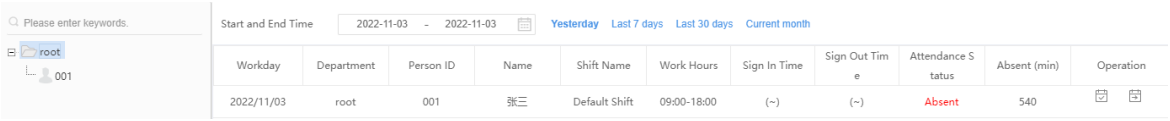
More Operations

You can edit or delete leave/business records.

- Edit: Click for the record in the **Operation** column to edit the information such as leave type and leave start and end time.
- Delete: Click for the record in the **Operation** column to delete the record.

18.3.2 Re-Sign In&Out Management

For abnormal attendance records such as absence, late arrival, you can modify the attendance records by re-sign in and out operations. After making a re-sign in or out, you can click **Calculate** in Attendance Details to update the attendance status and absent hours of this day.



1. Select the department or person on the left-side organization list.
2. Set a time range. All the abnormal attendance records of the specified department or person within this period are displayed.
3. Click (re-sign in) or (re-sign out) in the **Operation** column for the absence record you want to handle.
4. Modify the sign-in time or sign-out time as needed.
5. Click **OK**.

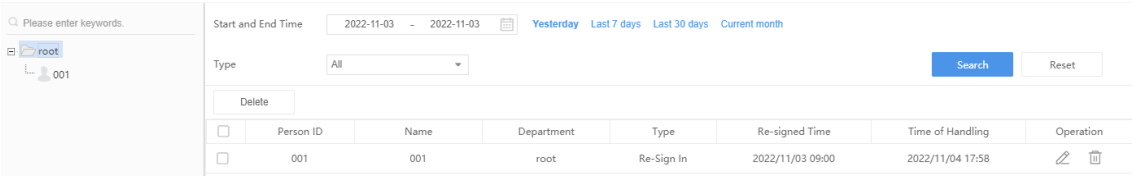
Note:

- The re-sign in or out time must be within the effective range, otherwise, the re-sign in or out operation is not effective.
- A person can be re-signed in or out up to 100 times a day. Before more re-sign operations can be performed for this person, you need to clean up re-sign in&out records for this person manually.
- If there are multiple re-sign records in one day, the earliest and the latest re-sign time within the valid time period will be considered as the re-sign time.

18.3.3 Re-Sign In&Out Records

A record is generated each time a sign-in or sign-out time is modified manually. You can search, edit or delete re-sign in&out records on this page.

1. Select the department or person from the organization list.
2. Specify a time range and type, click **Search**. Search records are displayed.



More Operations

Edit: Click in the **Operation** column to modify a re-signed time.

Delete: Click to in the **Operation** column delete a re-sign in&out record. After the record is deleted, the person's attendance statistics will use the original attendance data during the corresponding time period.

18.4 Attendance Statistic

Attendance statistics only include people in the system and do not include strangers. Entry/exit records of strangers are included in pass-thru records.

Original Data: View all records of people entering or leaving by face recognition or swiping cards during the specified period.

Attendance Details: View attendance details including attendance status and absence duration during the specified time period. One record is generated for each person every day.

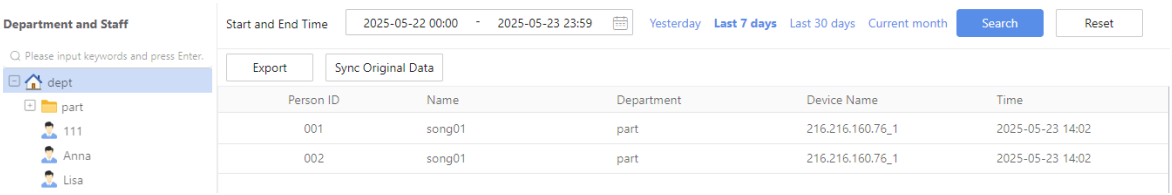
Attendance Summary: View the total length of absence during a specified period and the details.

Note:
The attendance calculation is precise to the minute. The attendance statistics and sign-in/sign-out time are based on minute counts. For example, a sign-in at 08:00:59 would be recorded as 08:00.

18.4.1 Original Data

View all the records of people entering or leaving by face recognition or swiping cards during a time period. For example, if there are five entries or exits, then five access records are displayed.

Search and view the access records of a specific department or a person, including person ID, name, department, access control device, access time.



1. Select the department or person from the organization list.
2. Set a time range.
3. Click **Search**.

Search results are displayed. You can click **Export** to export the data.

If the access control device failed to report access records automatically due to factors such as poor network, you can click **Sync Original Data** to sync manually.

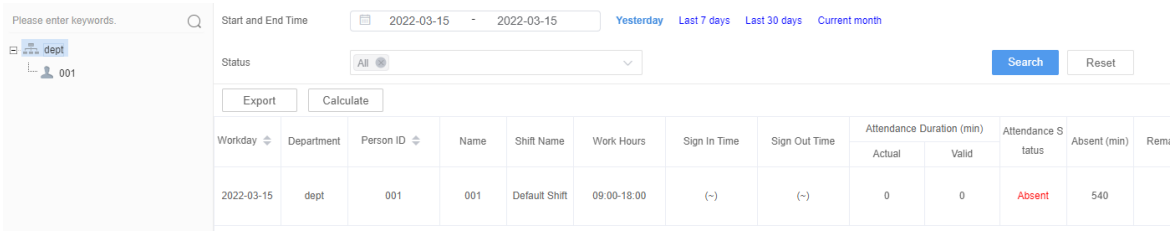
18.4.2 Attendance Details

View attendance details including attendance status and absence duration during a specified period. One record is generated for each person every day.

All the original data of a day will be generated at the automatic calculation time on the next day. If automatic calculation fails, or if any shifts have changed, you can select the department or person on the left-side organization list, set the start and end time, and then click **Calculate** to re-calculate attendance and generate attendance details.

Note:
When you calculate attendance for a certain day, if abnormal shifts are detected for this day, or if any shifts in this day are not yet started or ended, then attendance data of the relevant persons in this day will be deleted and will not be calculated.

You can search attendance statistics of a department or a person by setting search criteria including person ID, name, department, date, time, sign-in/out time.



The search results appear in the list. Click **Export** to export personnel attendance details.

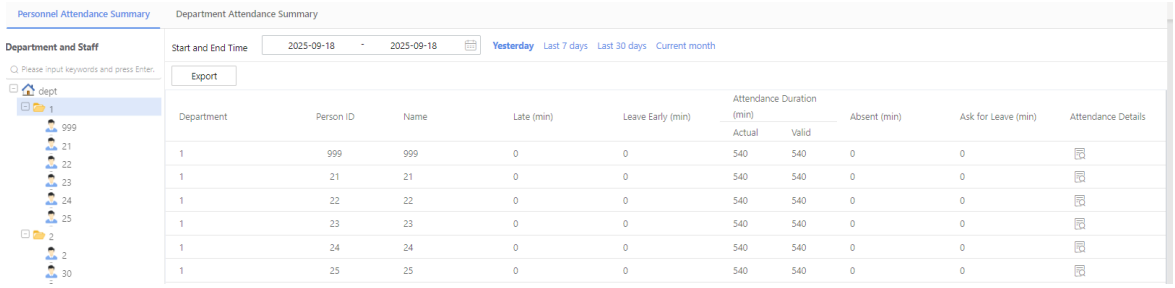
18.4.3 Attendance Summary

Summarize attendance data by personnel or department.

Personnel Attendance Summary

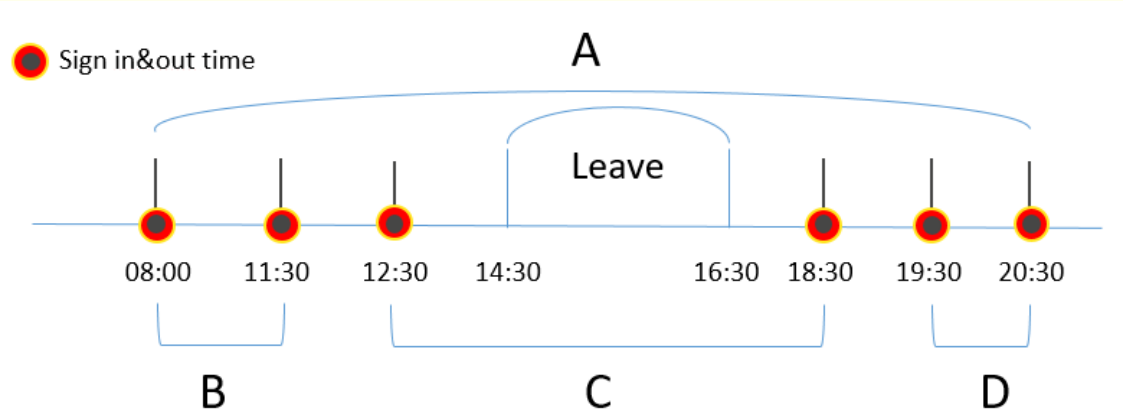
View the cumulative absence duration and attendance details of personnel within a specified time range. For example, calculate the total monthly duration of late arrivals, early departures, absences, leave, etc., for each person.

Select a department or person on the left, set the start and end time, then proceed to summarize attendance data.

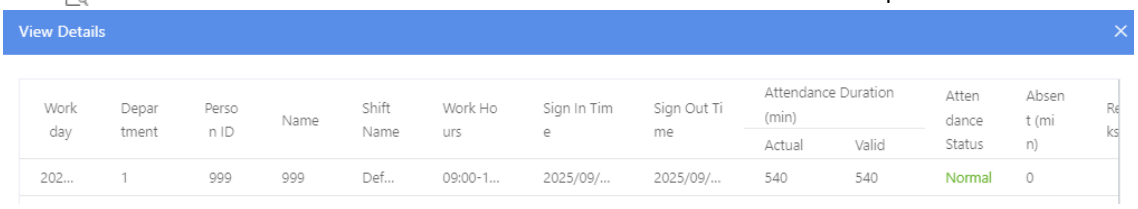


Note:

- For flexible time periods, attendance duration will not deduct leave time taken within that period. That is:
  - When attendance is calculated based on the first and last sign-in/sign-out times, attendance duration is the length of period A.
  - When attendance is calculated by accumulating durations between consecutive sign-ins/sign-outs, attendance duration is the total length of periods B + C + D.
- Absence duration is calculated as daily working hours minus attendance duration.



- Click **Export** to export all the retrieved attendance data.
- Click in the **Attendance Details** column to view the attendance details of that person.

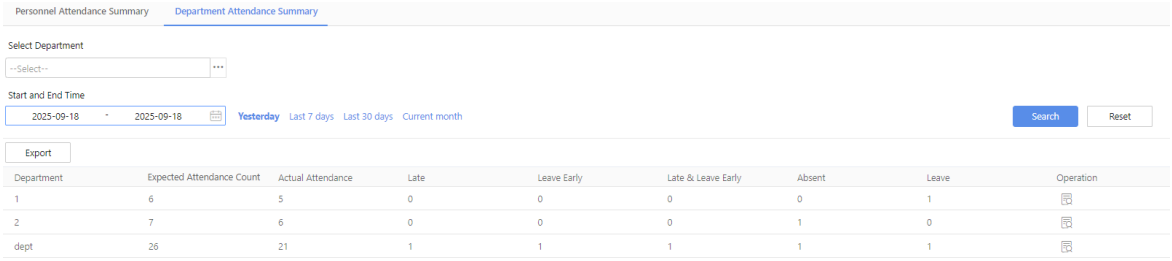


Department Attendance Summary

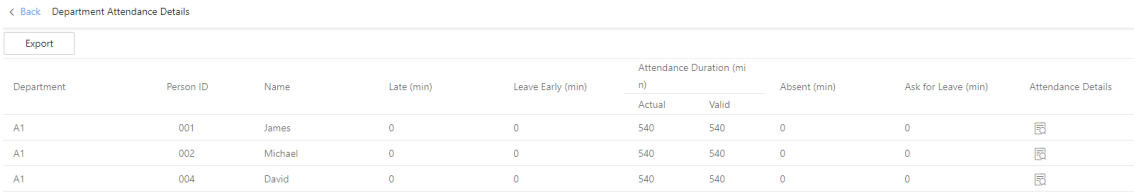
View the attendance count and the abnormal attendance count by department, including the expected attendance count, those with normal attendance, those who were late (but did not leave early), those who left early (but were not late), those who were both late and left early, those who were absent, and those on leave.

Note:
Count: If there are multiple attendance shifts within the specified time range, the cumulative headcount across all shifts is counted.

After selecting the department and start/end dates, you can view the summarized attendance information for personnel within the selected department (including sub-departments).



- Click **Export** to export all the retrieved attendance data.
- Click in the **Department Attendance Details** column to view the summary of absence duration and attendance details for each person in that department.



- Click in the **Personnel Attendance Details** column to view the attendance details for that person.

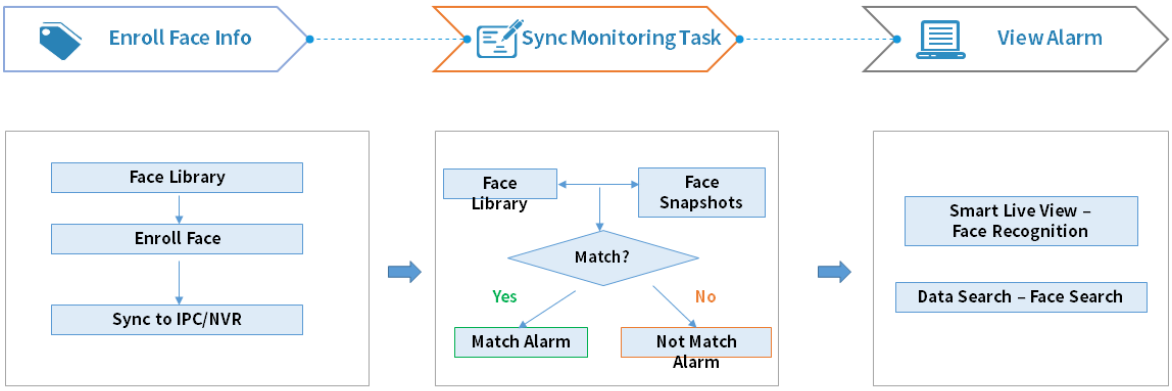
19 Face Monitoring

Go to **Park Application** > **Face Recognition**.

Face recognition is to compare the face snapshots with the images in the face libraries and determine whether it is the same person by the face match degree. When the match degree reaches the set threshold, it is recognized as a successful match, otherwise, it is a failed match. You can view the match/not match alarm and important person alarm records, as well as recognize the important person or abnormal guests.

Note:
Please add smart IPC/NVR in **Device Management** > **Private Device** on the platform for face recognition first.

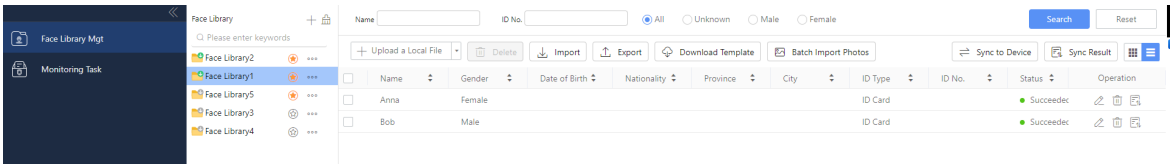
The processes of face monitoring service are as follows:



19.1 Face Library Management

Face library includes face related information. By adding face libraries, you can manage faces in different categories to meet different monitoring needs.

Go to **Face Recognition** > **Face Library Management**.



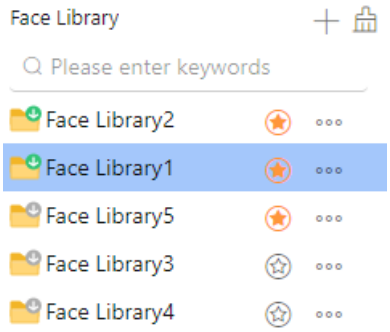
19.1.1 Manage Face Library

You can add, edit, or delete face libraries.

Note: Up to 128 face libraries are allowed.

Add Face Library

Click + in the face library list on the left to add a new face library (default name: Face Library+ID).



Set as Important Library

By default, newly added face libraries are **Common Libraries**, but can be designated as **Important Library**.

Use the icon next to the library name to switch: ☆ refers to a common library; ★ refers to an important library.

- Important Library: When monitoring the important library, both a **face match alarm** and an **important person alarm** will be triggered if a person's face matches an entry in the library. This helps distinguish important and common persons. For example, after adding VIP customers to the important library, staff will be notified when these customers appear, allowing for prioritized service.
- Common Library: When monitoring the common library, a **face match/not match alarm** will be reported based on whether a person matches an entry in the face library. For example, by adding staff to common library, the system can distinguish between internal staff and external visitors based on the alarm type.

Edit Face Library

Click ··· for the face library and select **Edit** to rename it.

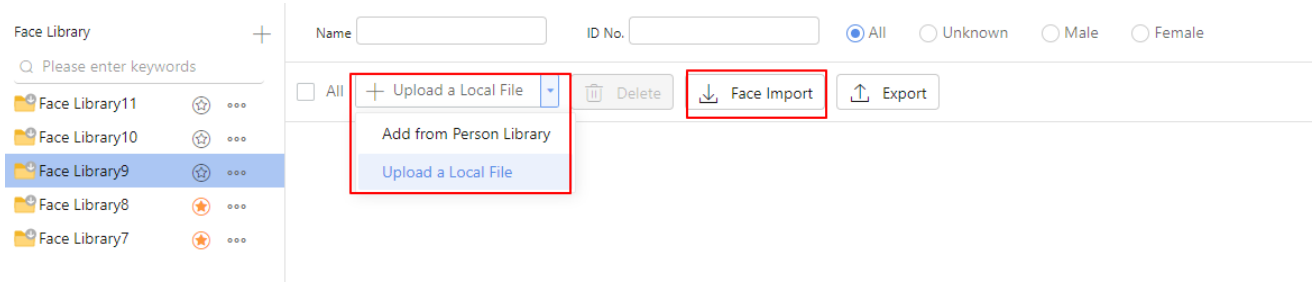
Delete Face Library

- Delete one by one: Click ··· for the face library and select **Delete** to delete it.
- Batch delete: Click 🧹 in the upper-right corner of the list to delete all face libraries.

Note: Deleting face libraries will also delete the related face data.

19.1.2 Add Face Data

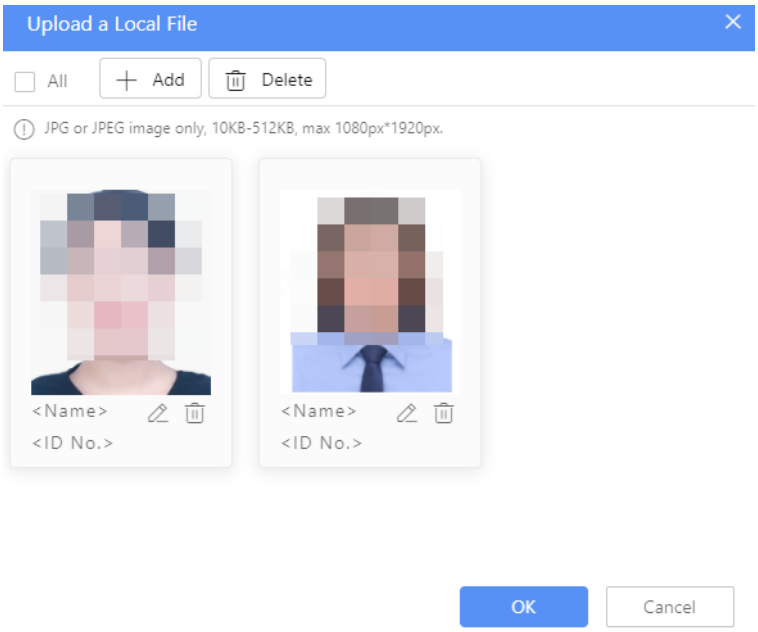
Add face information to face library. Choose a way to add face data as needed.



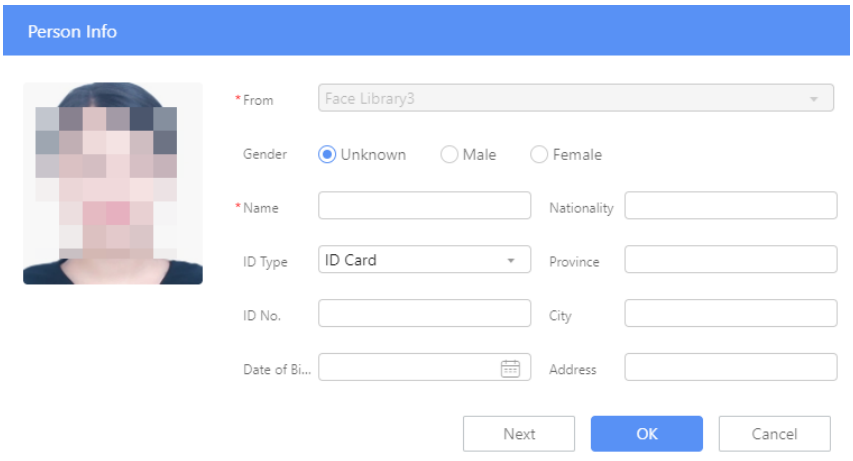
Upload from Local

1. Select a target face library on the left, and then click **Upload a Local File**.
2. Click **Add** and select a face photo from local.

Note:
The photo must be JPG files. Size: 10KB to 512KB. Max. resolution: 1080px*1920px.
Image verification is enabled by default. To disable it, see Face Image Verification.



3. Click for the uploaded face images. A page as shown below appears. Enter the person name, ID number and other information as needed. And then click **OK**.

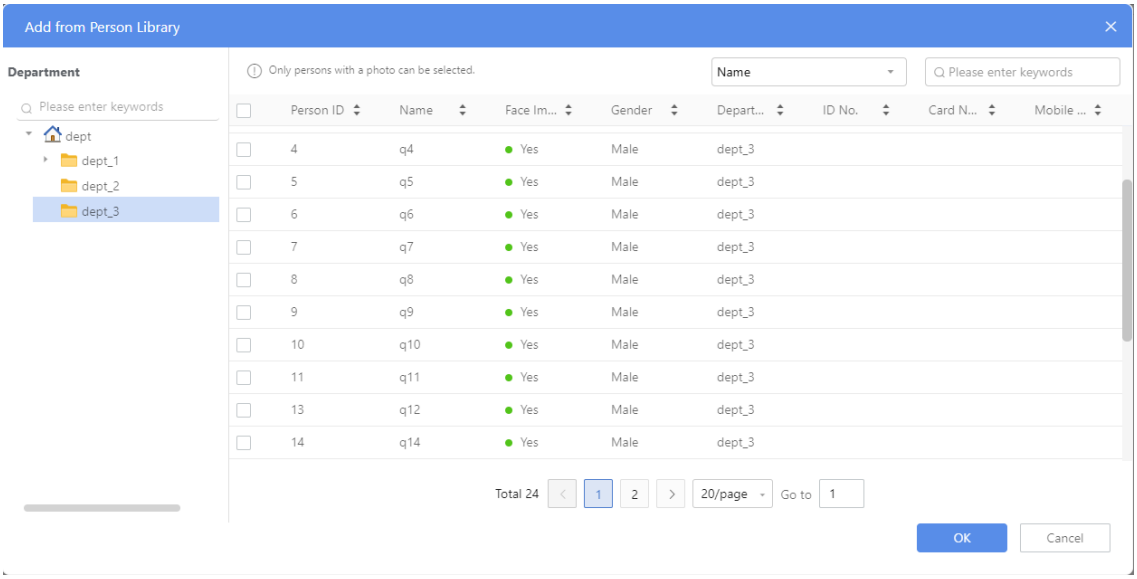


;

4. After completing all the person information, click **OK** on the **Upload a Local File** window.

Add from Person Library

1. Select a target face library on the left, and then click **Add from Person Library**.

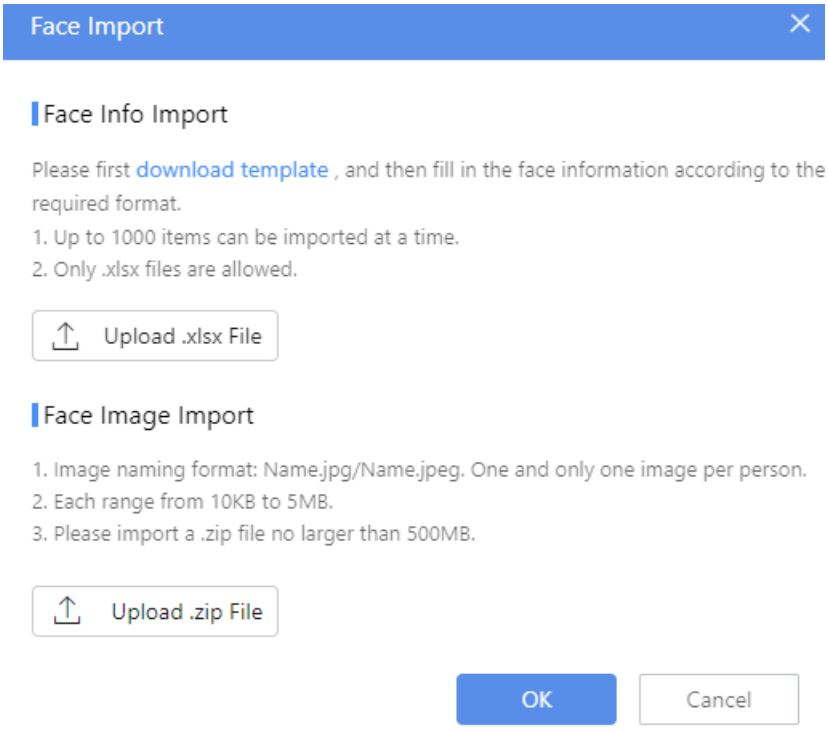


2. Select person(s) from the person library and click **OK** to add the selected persons to the face library.

Note: Only persons with face images can be added to the face library.

Batch Import

1. Select a target face library on the left, and then click **Face Import**.



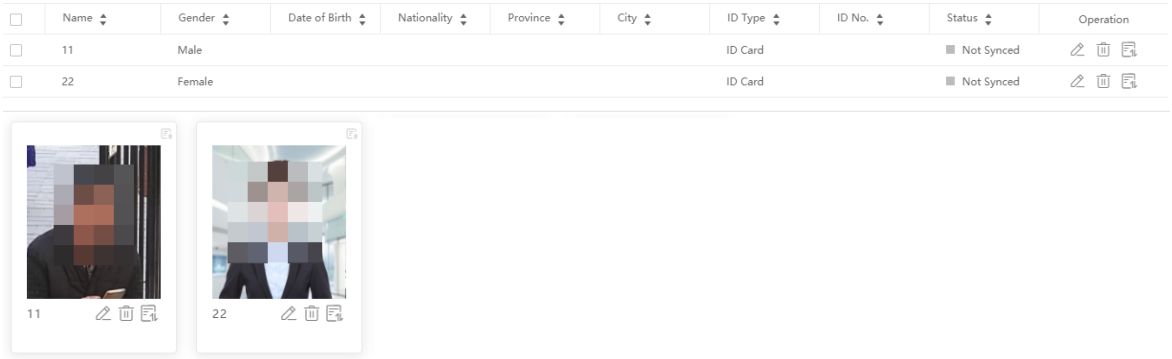
2. Face Info Import: Click **download template** to download the template to local, fill in the person information in the template, then click **Upload .xlsx File**.
3. Face Image Import: Name the face photos as Name.jpg/.jpeg. Only 1 photo is allowed per person. Pack all photos into a .ZIP file, then click **Upload .zip File**.
4. Click **OK**.

19.1.3 Manage Face Data

You can search, edit or delete the face data.

Switch View

Click to switch the view mode into Image or List.



Search Face Data

Set name, ID number, gender as needed, and click **Search**.

Edit Face Information

Click for the face information to edit it.

Delete Face Data

- Delete one by one: Click for the face data to delete it.
- Batch delete: Select multiple face data and then click **Delete** above the list.

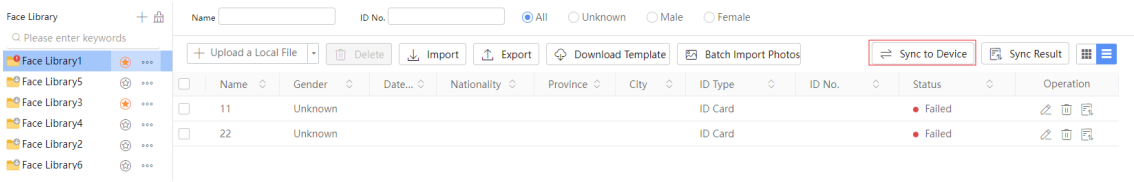
19.1.4 Sync Face Data

Sync the face data to the smart devices to create monitoring tasks.

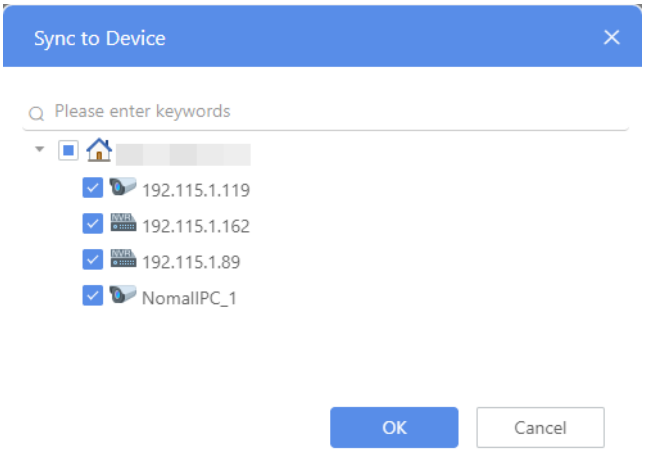
Sync to Device

1. Select a face library and click **Sync to Device**.

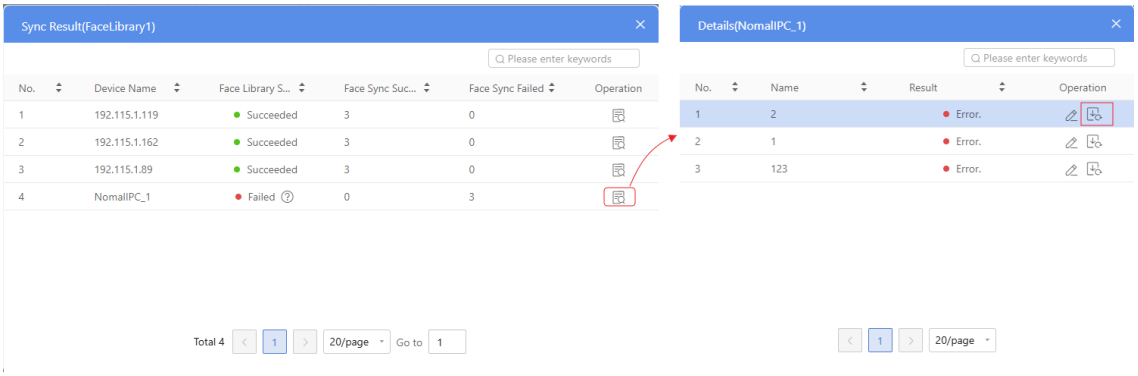
   Note: Only the entire face library can be synchronized.



2. Select the target IPC/NVR device(s) and click **OK**.



3. View the sync results of different devices in the pop-up window. Click to view the sync result for each people. For people that fail to synchronize, click to resynchronize.



View Sync Result

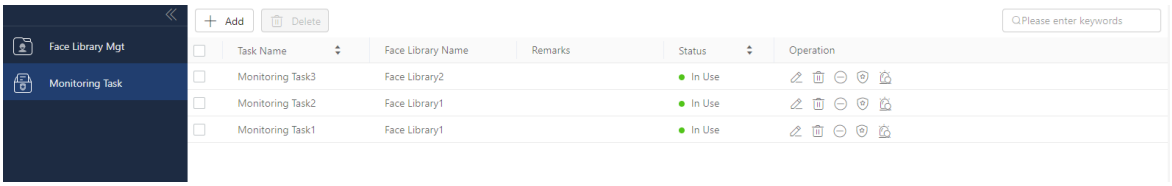
- The synchronization status can be viewed by the arrow icon in front of the face library: gray(unsynced); red(some failed); green(succeeded).
- Select a face library and click or **Sync Result** to view the synchronization status of devices and people. If the synchronization fails, it can be resynchronized.
- Click for the face data to view the sync status of that face in each device. If the synchronization fails, it can be resynchronized.

Note: For successfully synchronized face libraries, if the face information in the library is updated, it will be automatically synchronized to the device.

19.2 Monitoring Task

Create face libraries for face recognition. IPC/NVR will monitor the faces in the detection area, compare the face snapshots with the face images in the libraries, and report a match or not match alarm.

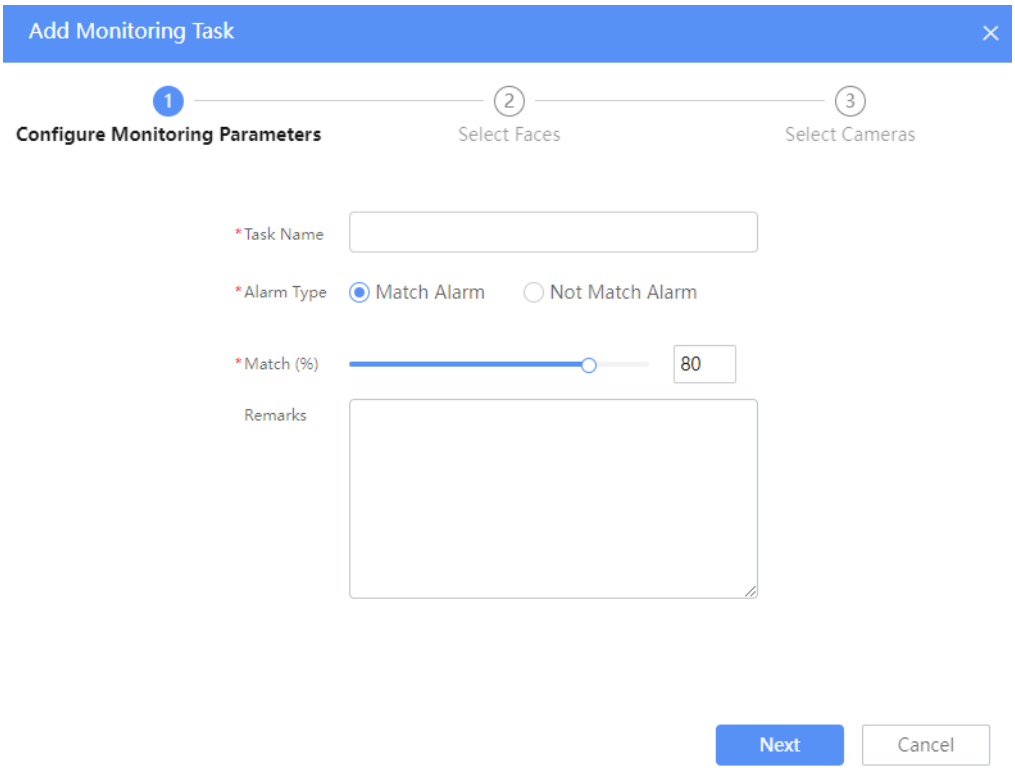
Go to **Face Recognition** > **Monitoring Task**.



19.2.1 Create Monitoring Task

Note: Up to 32 monitoring tasks are allowed.

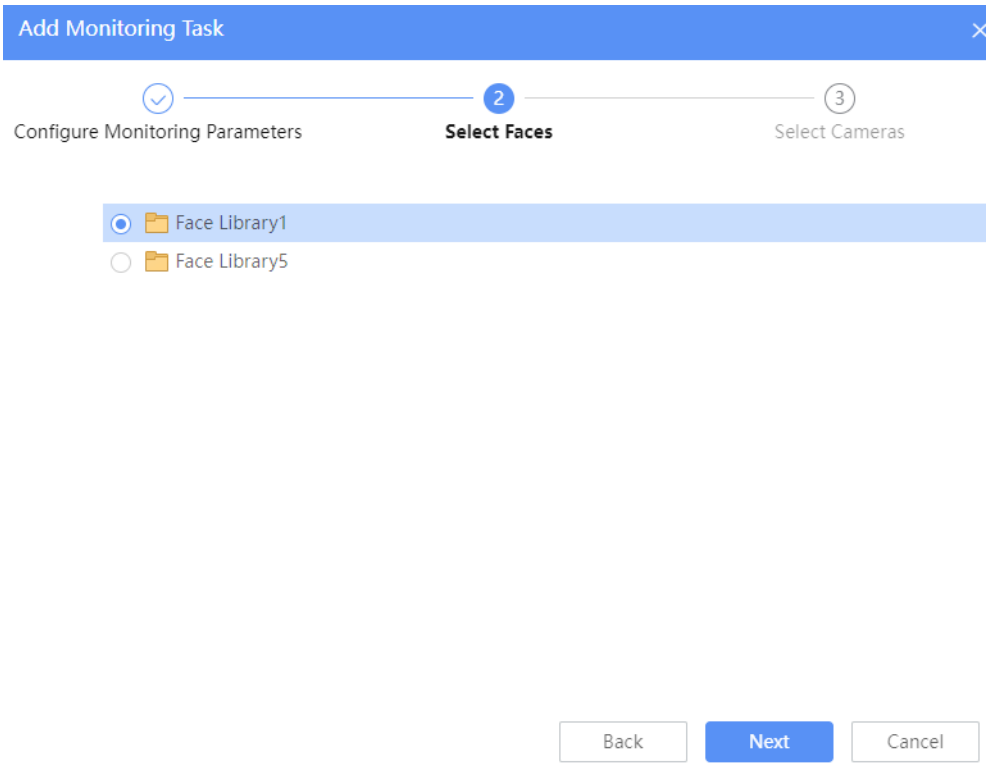
1. Click **Add**. A page as shown below appears.



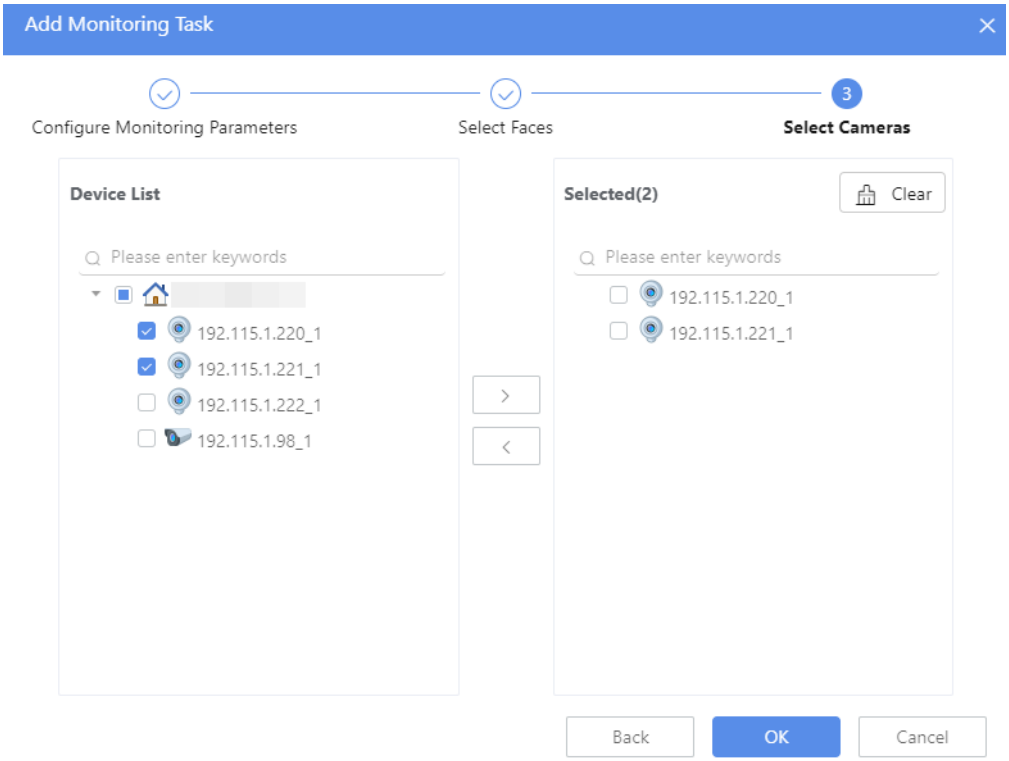
2. Set the parameters.

Item	Description
Task Name	Set the monitoring task name.
Alarm Type	• Match Alarm: The system reports a match alarm when the similarity between a captured face and a face in the monitored face library reaches the similarity threshold; for example, when the system detects a VIP guest. • Not Match Alarm: The camera reports a not match alarm when the similarity between a captured face and a face in the monitored face library fails to reach the similarity threshold; for example, when the system detects a stranger.
Match	Set the face similarity threshold.

3. Click **Next** and select face libraries (only face libraries that have been synced to the device can be selected) to be monitored.



4. Click **Next** and select cameras to be used for monitoring.



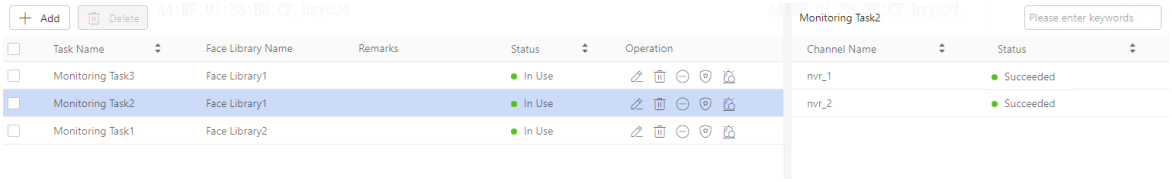
5. Click **OK**.

19.2.2 Manage Task

You can view, edit, delete or enable/disable the monitoring task.

View Monitoring Task

Select a monitoring task to view the monitoring status of each channel.

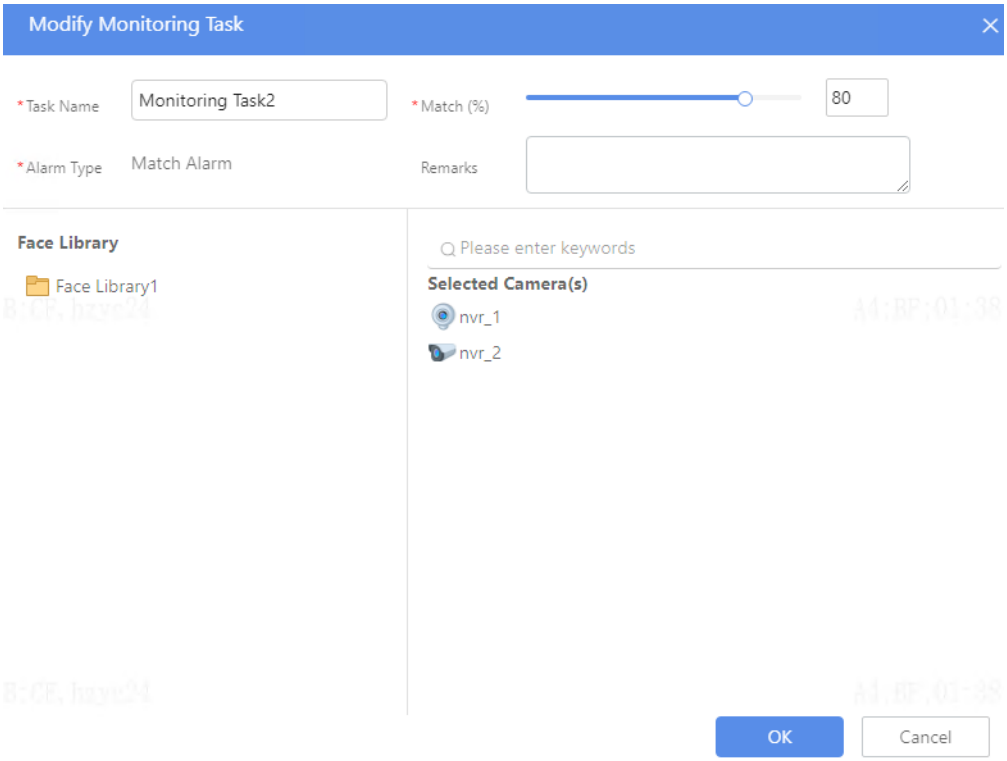


Re-Monitor

If there some channels failed to receive monitoring tasks, click to assign the monitoring task again.

Edit Monitoring Task

Click to edit the monitoring task, including the task name and match value.



Enable Monitoring Task

For the stopped monitoring tasks, click to enable the tasks.

Disable Monitoring Task

For the ongoing monitoring tasks, click to disable the tasks. After disabling, the face comparison will stop.

Search Alarm

Click to navigate to the Face Search page and view the face alarms generated by this task.

20 Comprehensive Search

Search face/pedestrian/motor vehicle/non-motor vehicle records by attributes, alarms, images, and other conditions based on video and image data.

20.1 SeekFree

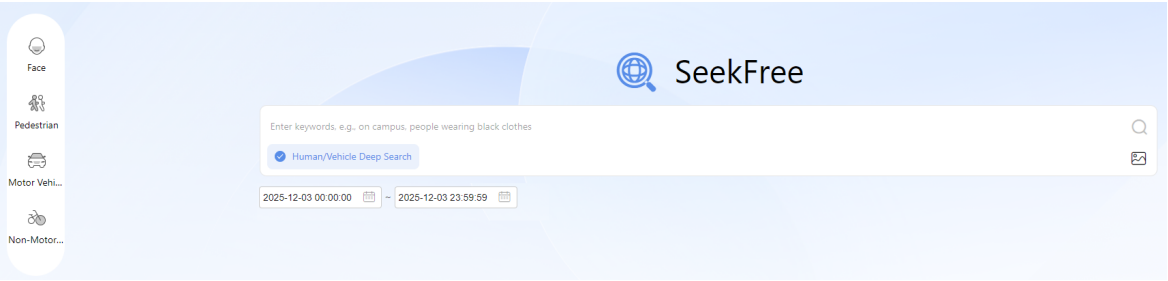
Go to **Data Search > Comprehensive Search > SeekFree**.

SeekFree is a comprehensive search method based on video and image data, providing a unified search entry for motor vehicles, non-motor vehicles, and pedestrian targets. It supports searching for specific targets in massive video and image data using text and images, improving the efficiency of information retrieval. It can provide valuable clues for finding objects or people.

When users lack specific target information, they can search using text descriptions or relevant images, quickly finding the first image of the target. Based on that image, they can then perform progressive searches to obtain accurate target results.

Combined with a visual map, SeekFree can restore the target's movement trajectory, helping users gain a comprehensive understanding of the target's activity information, and thus assess the target's appearance locations, enabling precise people searching and quick object retrieval.

Note:
The SeekFree feature relies on intelligent computing power: the platform needs to add smart NVR devices to enable this feature.



20.1.1 Search by Text

For scenarios where the search target is not clearly defined, users can directly enter a text query in the input box. The system, based on natural language processing technology, understands the semantics of the user's query and performs a search for relevant content.

1. Enter a text description (in either Chinese or English): target features + target type(motor vehicle/non-motor vehicle/pedestrian), such as "people wearing black clothes."
2. Enable/disable **Human/Vehicle Deep Search**.
   - Selected: The system searches for targets in the closeup image of humans or vehicles. The search results display closeup images of the targets for better viewing of details.
   - Not selected: The system searches for targets in the original images. The search results display the scene where the targets appear for better viewing of the scene.

     Note:
     Search results of the same target: In the original image, similarity values may be lower due to interference of other objects in the image. In the closeup image, the similarity values will be higher due to less interferences.
3. Choose a time range.

4. Click to start the search. The default search parameters are: any location, similarity of 60%.

5. If the results from the default settings do not meet expectations, change the search criteria, then click to search again.

Figure 20-1: Enable Human/Vehicle Deep Search

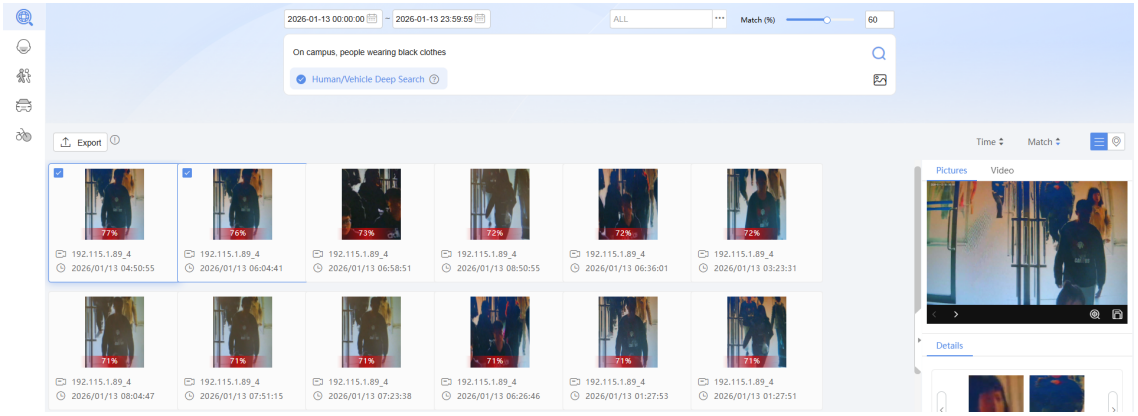
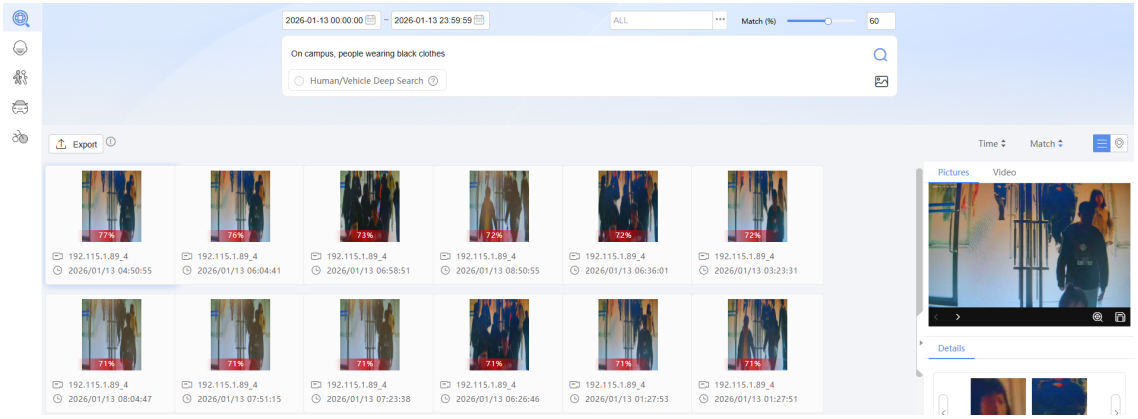


Figure 20-2: Disable Human/Vehicle Deep Search



20.1.2 Search by Image

For scenarios with existing search images, you can directly import images for searching.

1. Click (or **Upload**) to upload the target image.

   For scenes with large images, after uploading the image, the system automatically identifies and extracts all target images from the large image. You can select the specific target images you want to search. When queried, the system will search for multiple selected targets.

   Note:

   - Images must be in JPG format and less than 4MB.
   - You can upload up to 1 image; uploading again will overwrite the previously uploaded image.

2. Enable/disable **Human/Vehicle Deep Search**.

   - Selected: The system searches for targets in the closeup image of humans or vehicles. The search results display closeup images of the targets for better viewing of details.
   - Not selected: The system searches for targets in the original images. The search results display the scene where the targets appear for better viewing of the scene.

     Note:
     Search results of the same target: In the original image, similarity values may be lower due to interference of other objects in the image. In the closeup image, the similarity values will be higher due to less interferences.

3. Choose the time range, snapshot location, and similarity, then click **Search**.

   Note:
   If searching multiple targets simultaneously, the search results will display snapshots mixed for multiple targets.

Figure 20-3: Enable Human/Vehicle Deep Search

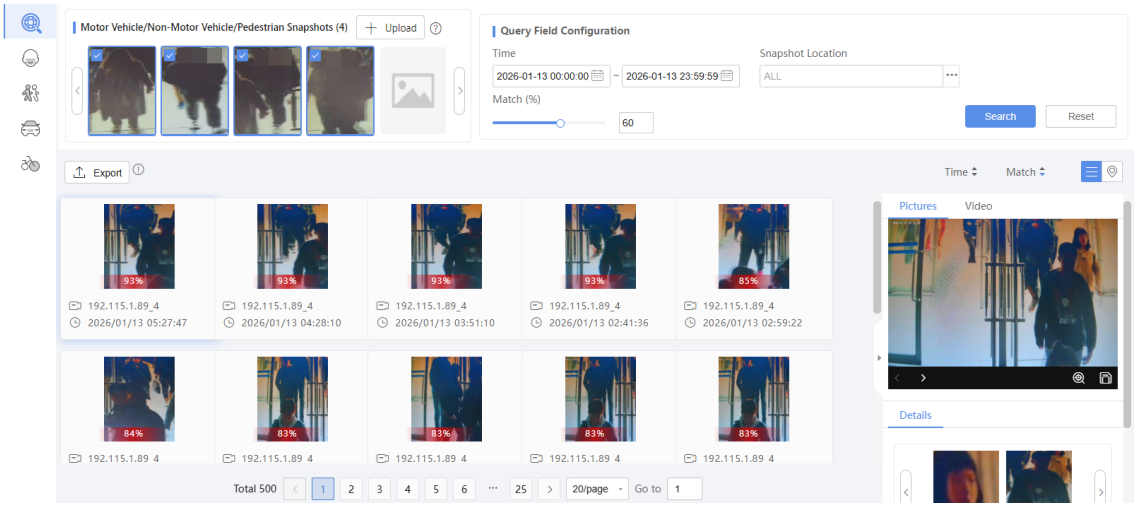
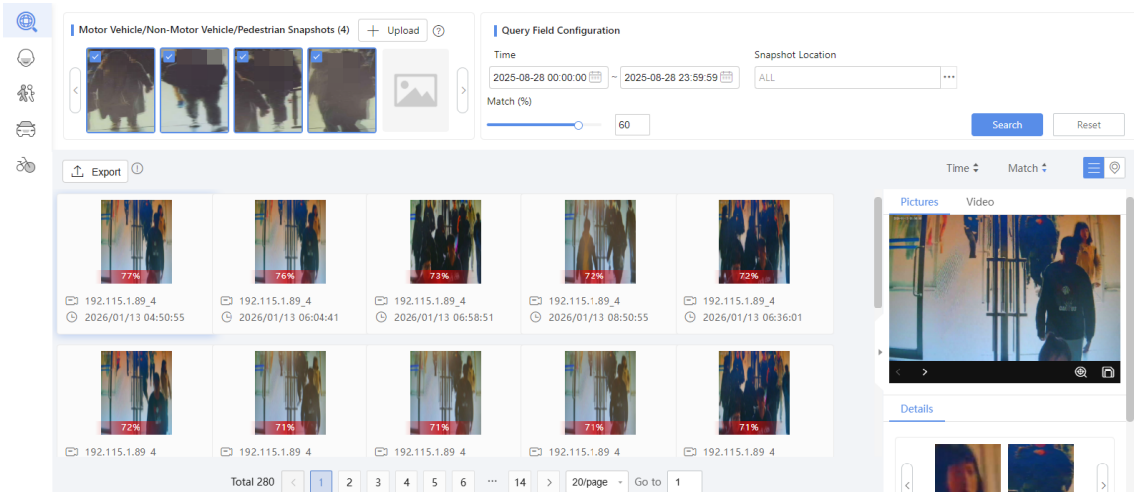


Figure 20-4: Disable Human/Vehicle Deep Search



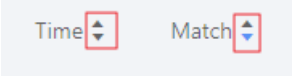
20.1.3 Search Results

Attention:
Switching level-3 menu will reset the existing search results, and a new search will need to be performed when re-entering the page.

The search results support the following actions:

Sorting

You can choose the sorting method from the top-right corner of the page.



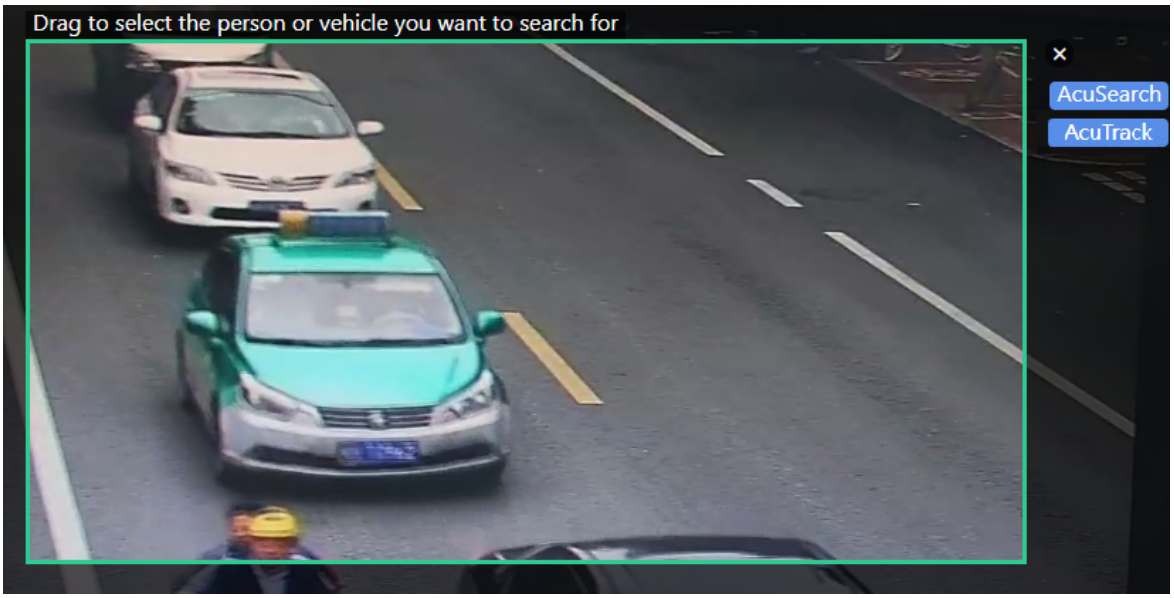
- By Time: Click the up arrow to sort from earliest to latest; click the down arrow to sort from latest to earliest.
- By Similarity: Click the up arrow to sort from low to high similarity; click the down arrow to sort from high to low similarity (default).

View Details

Select a search result to display the corresponding snapshot, the video before and after the snapshot, and the snapshot details on the right.

Click on the toolbar to download the image or recording to your local computer.

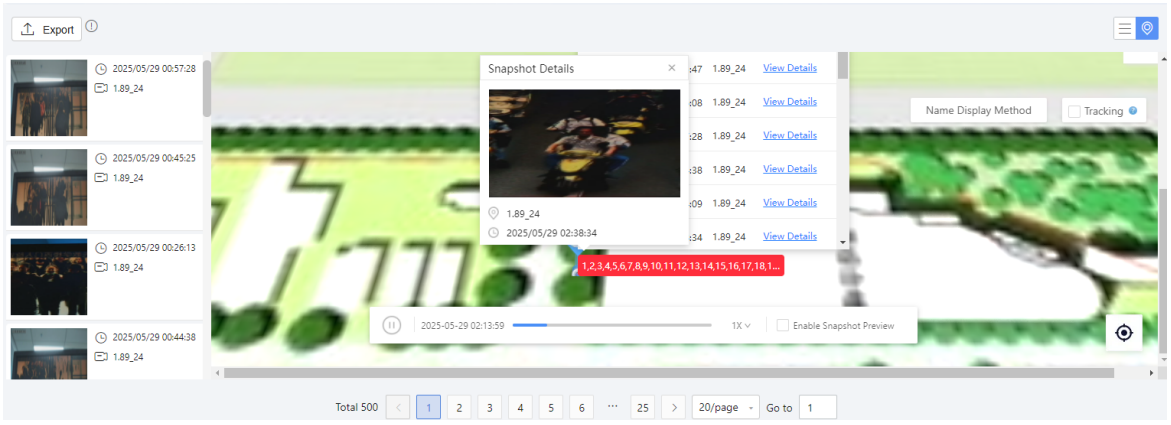
Click on the toolbar to search for targets within the image or video frame.



1. Select the target to search for:
   - Hold down the mouse and drag the area within the green box to move its position.
   - Hover the mouse over the edges or corners of the green box, when the cursor changes to an arrow, hold and drag to resize the green box.
   - To exit the search, click X.
2. Choose a search mode. Two modes are available:
   - Click the **AcuSearch** button at the top right corner of the green box to go to the SeekFree page, where the system will automatically search for all capture records of the target within the green box (see Search by Image).
   - Click the **AcuTrack** button at the top right corner of the green box to go to the AcuTrack page, where you can search for recordings containing the target in the green box.

View Trajectory

Click the at the top-right corner of the page to view the target's trajectory on the map. The locations where the target appeared will be connected in chronological order to generate the trajectory.



Click to play the trajectory, with adjustable play speed. Enable snapshot preview to view the person's snapshot at the device locations.

Note:

- Prerequisite: Please complete the Map Configuration first by uploading the map and marking the camera positions.
- The trajectory will be drawn for only the top 20 snapshots in the search results.
- Try to set more precise search criteria to ensure the system retrieves snapshots of the same target and generates the movement trajectory for that target.

Export

- Export the selected: Select search results and click **Export**.
- Export current page: Click **Export**.

20.2 Face Search

Go to **Data Search > Comprehensive Search >Face.**

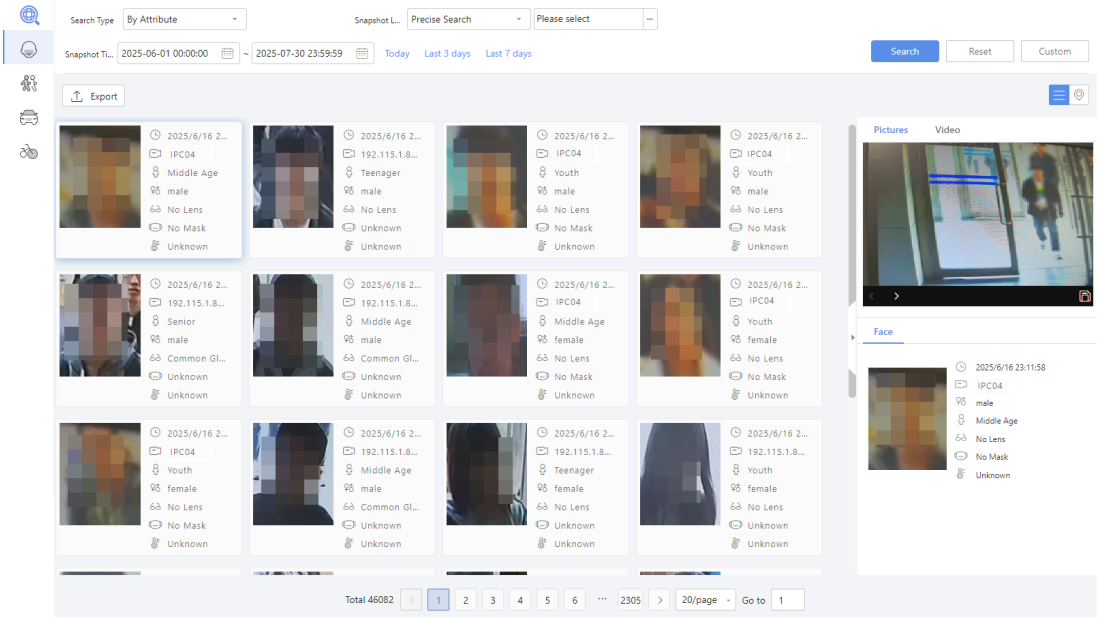
You can search persons by attribute, event, or face image in passing records from cameras or face libraries.

For example, in the event of a security incident or an urgent need to locate specific individuals, you can search information by attributes (location, snapshot time), event (match/not match alarm), or face images. This allows you to quickly retrieve the relevant person's passing records or his/her information in face library, providing additional details for investigation.

20.2.1 Search by Attribute/Alarm

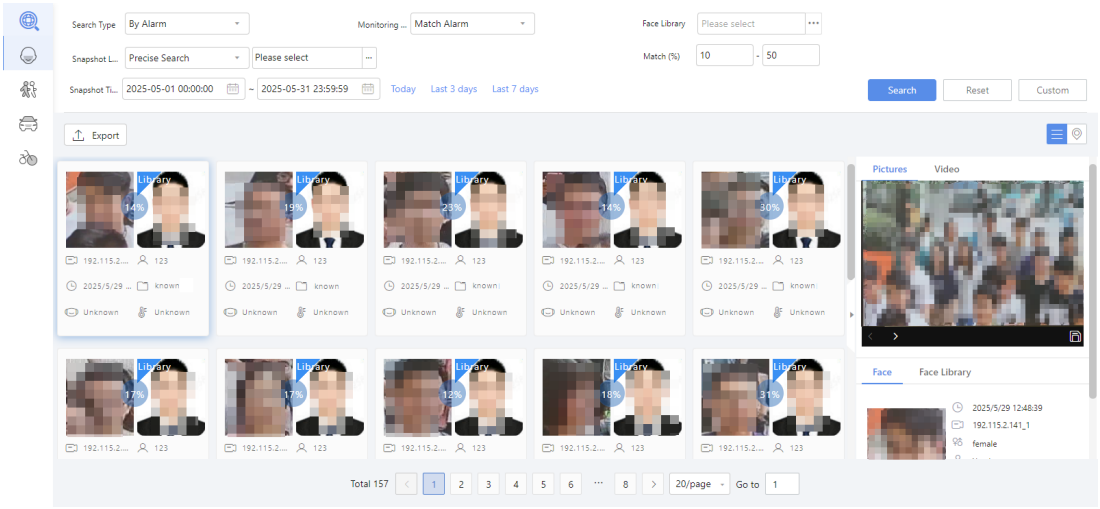
Search pass-thru records by face attributes or alarms.

1. Select a search type.
   - By attribute: Set the snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name) and snapshot time. Click **Custom** to set the gender, age, glass type, mask status, and body temperature range as needed.



   - By alarm: Set the monitoring type (match alarm/not match alarm/important person alarm), face library, snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name) , snapshot time and similarity range (0%~100%). Click **Custom** to set the name, gender, card type, mask status and body temperature range as needed.

     Note:
     Match alarm sources: Face Monitoring and visitor Vistor Monitoring Task. Not match/important person alarm sources: Face Monitoring.

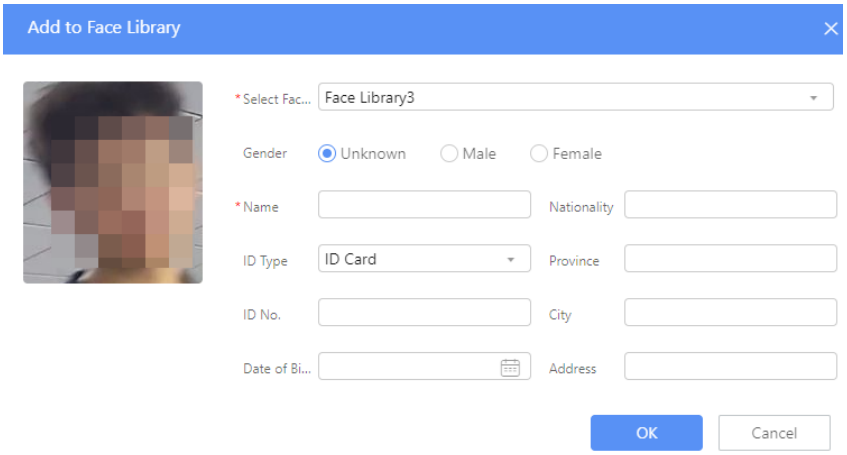


2. Click **Search** to find pass-thru records.

Search Results

Search results are displayed on the bottom side of the page.

- Click on a result to view the snapshot, recording (5s before and after the snapshot time), and face attributes on the right. To save the snapshot/recording, click under the tab.
- Add to face library:
  1. Add a stranger to a face library by hovering over the search result and clicking .
  2. Select the target face library, complete the person information, and click **OK**.



- Search by image: Hover the mouse over the result and click to Search by Image.
- Export: Click **Export** to export the search results to a .xlsx file.
- Trajectory: Click to view Face Trajectory.

Related Operation

You can customize the attributes displayed on the snapshot record and alarm record cards as needed. See Card Attribute.

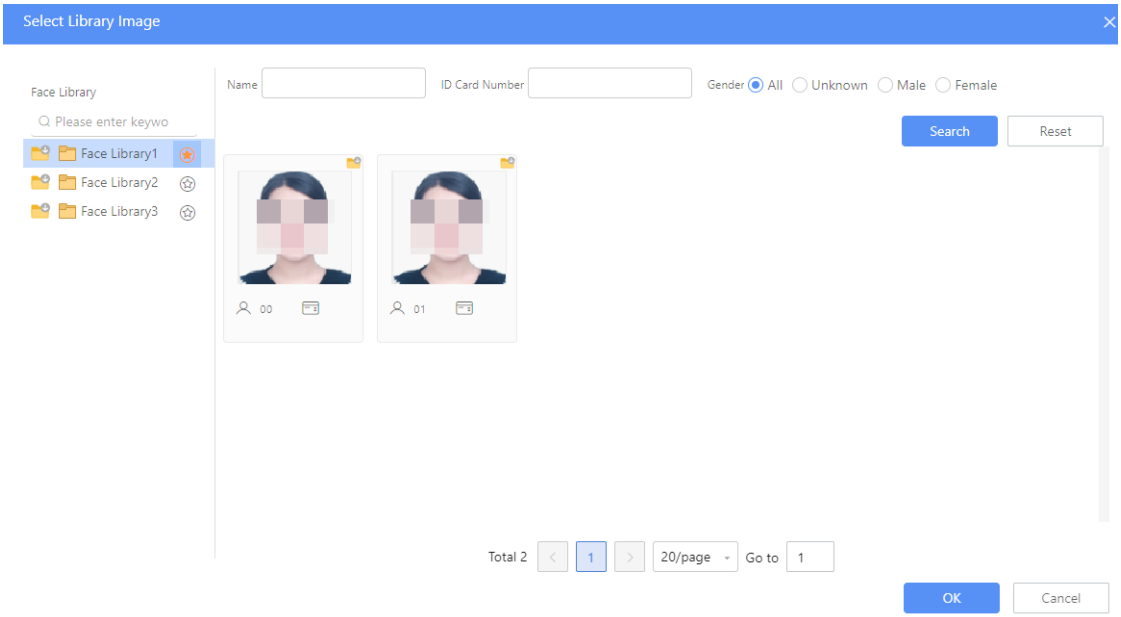
20.2.2 Search by Image

Search similar face images in the face libraries or pass-thru records.

Note:
You need to add smart NVR on the platform for face comparisons first.

1. Select the search type as **Search by Image**.

2. Select a search library type.
   - Pass-thru records: The system compares the uploaded image with the snapshots of pass-thru records in NVR.
   - Face library: The system compares the uploaded image with the face library images in NVR.
3. Upload an image to search (only 1 image is allowed).
   - Upload library image: Click **Upload Library Image**, select a face library and search the face image by entering the person name, ID number, and gender. Select the face image and click **OK**.



   - Upload local image: Click **Upload Local File**, and select the face image from local.
4. Set the search criteria.

Search in pass-thru records	Snapshot time	Set the start and end time.
	Snapshot location	Select NVR(s) or the video channels under NVR(s), and the uploaded image will be compared with the pass-thru records in NVR(s).
Search in face library	Face library	Select NVR(s), and the uploaded image will be compared with the face library images in NVR(s).
Match		Set the face similarity, and the system will display the face images that are greater than or equal to the set similarity.

5. Click **Search** to view the similar images.

Figure 20-5: Search Pass-Thru Records

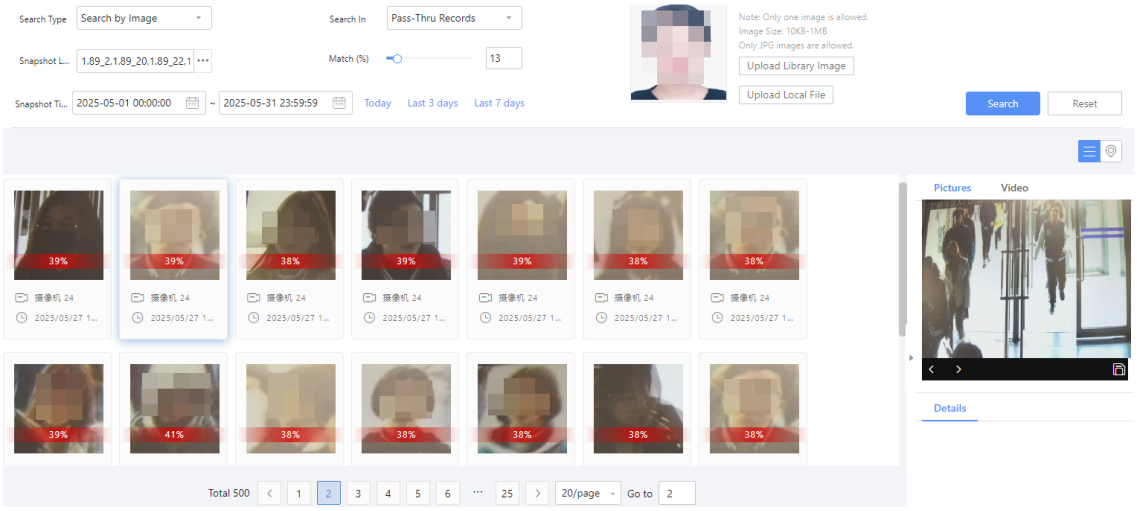
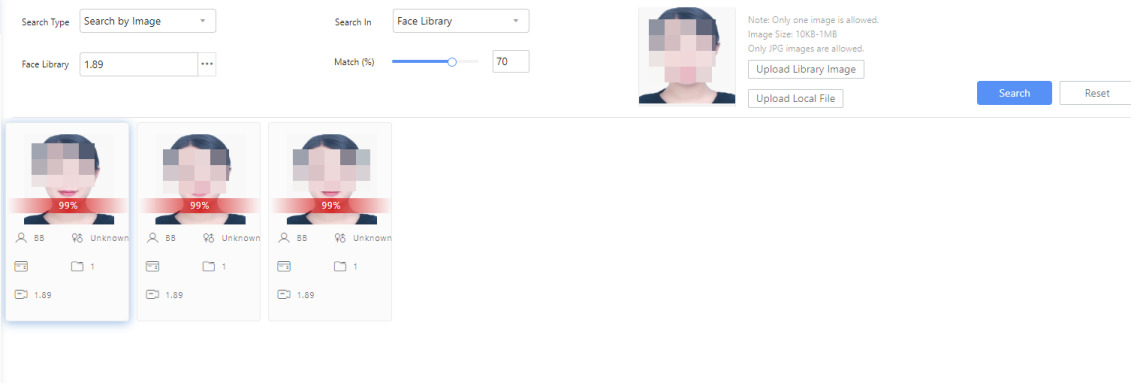


Figure 20-6: Search Face Library



More Operations

When you select the search type as **Pass-Thru Records**, from the search results, you can view snapshots, recordings, trajectories, add entries to the face library, export data, etc. For details, please refer to Search by Criteria > Search Results.

Related Operation

You can customize the attributes displayed on the face cards as needed. See Card Attribute.

20.2.3 Search by Frequency

People frequency refers to the number of times the same individual appears in the camera area over a specified period. This function allows specifying face libraries as the search range and customizing frequency parameters to identify high/low persons. It helps administrators track abnormal activities and manage targeted persons effectively.

- High frequency persons: Individuals who appear more frequently than a set threshold (e.g., repeat customers or line sitters).
- Low frequency persons: Individuals who appear less frequently than a set threshold (e.g., elders or students who have not been seen for a long time. Administrators need to stay updated on their safety status).

Prerequisites

Face Monitoring tasks have been created.

Data source: Matching records between persons in face libraries and captured persons.

Search Criteria

Select the search type as **Search by Frequency**, set search criteria as needed, and then click **Search**.

Search Criteria	Description
Frequency	Choose to search for high/low frequency persons. • High frequency: Search data ≥ input value; • Low frequency: Search data ≤ input value.
Face Library	Select one or multiple face libraries (including common and important libraries); default is all libraries.
Snapshot Location	Specify a camera or channel through precise search (by selecting the device on the resource tree) or fuzzy search (by entering keywords of the device name), default is all devices.
Snapshot Time	Set the snapshot time period (up to 7 days), or click Today, Last 3 Days, or Last 7 Days.
Match	Configure the similarity range (0%~100%) to filter and retrieve matching persons.

Search Results

Figure 20-7: High Frequency Person

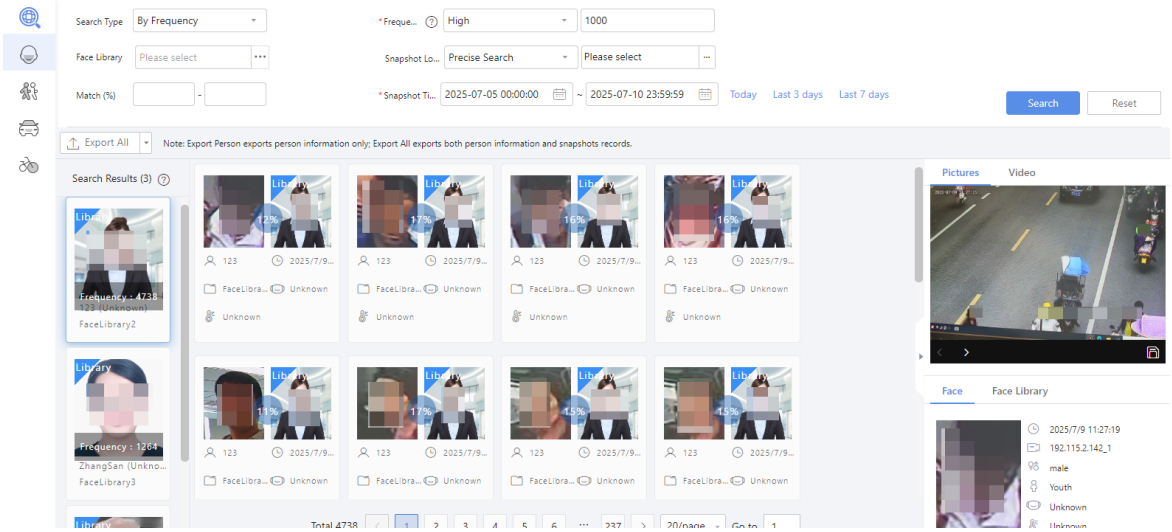
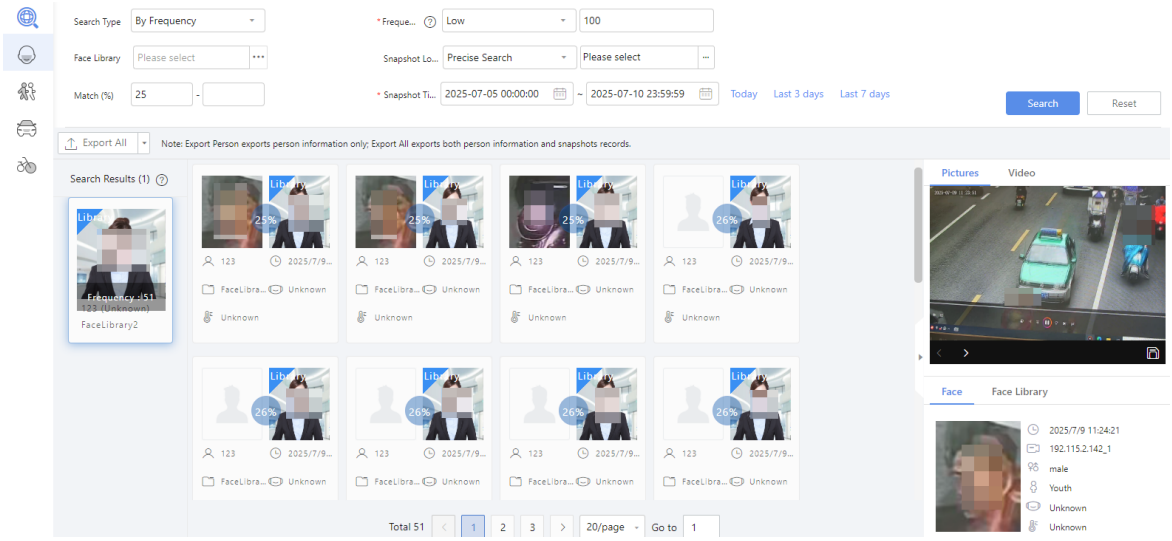


Figure 20-8: Low Frequency Person



1. View the matching results with the face library in the left-side column.
   - For high frequency searches, results are sorted in descending order of frequency. For low frequency searches, results are sorted in ascending order of frequency. Up to 100 people can be displayed in the result list. If results exceed 100, the top 100 are shown based on the sorting rules.
   - Each face library photo card displays frequency, person information, and library name.
2. Select a search result to view the matching snapshot records in the center. The number of records equals to the frequency.
   - The snapshot and library face photo are displayed in pairs, showing the match degree, snapshot information, etc.
   - Records are sorted in descending order of snapshot time, with the latest records displayed first.
3. Select a record to view alarm details on the right, including alarm snapshot, recording, face information and face library information.
4. Export data.
   - Click **Export Person** to export only the person information in the face library (data on the left side).
   - Click **Export All** to export both the person information in the face library and the snapshot information.

20.2.4 Face Trajectory

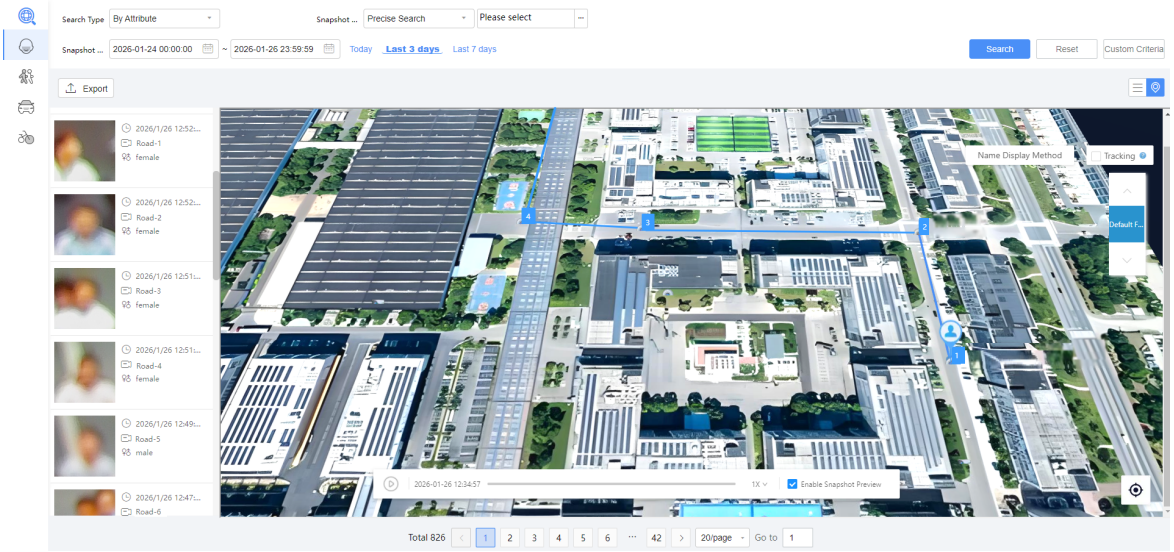
For face search records, you can view the location where the person is present on the map and the movement trajectory of the person plotted in chronological order. The trajectory provides valuable information, such as the person's activity range and residence place.

Operation Description

After the face that meets the search criteria is retrieved on the **Face Search** page, you can click in the upper-right corner of the result list to view the person's movement trajectory on the map. To play it, click . The speed is adjustable. If **Snapshot Preview** is enabled, a face image with snapshot information will be displayed when passes by the camera.

Note:

- Make sure that Map Configuration is completed (the map has been uploaded and cameras have been added to the map).
- The system only plots the trajectory based on the most recent 20 snapshot records.
- Please set the search criteria as precisely as possible to help the system retrieve snapshots of the same person and plot a more accurate trajectory.



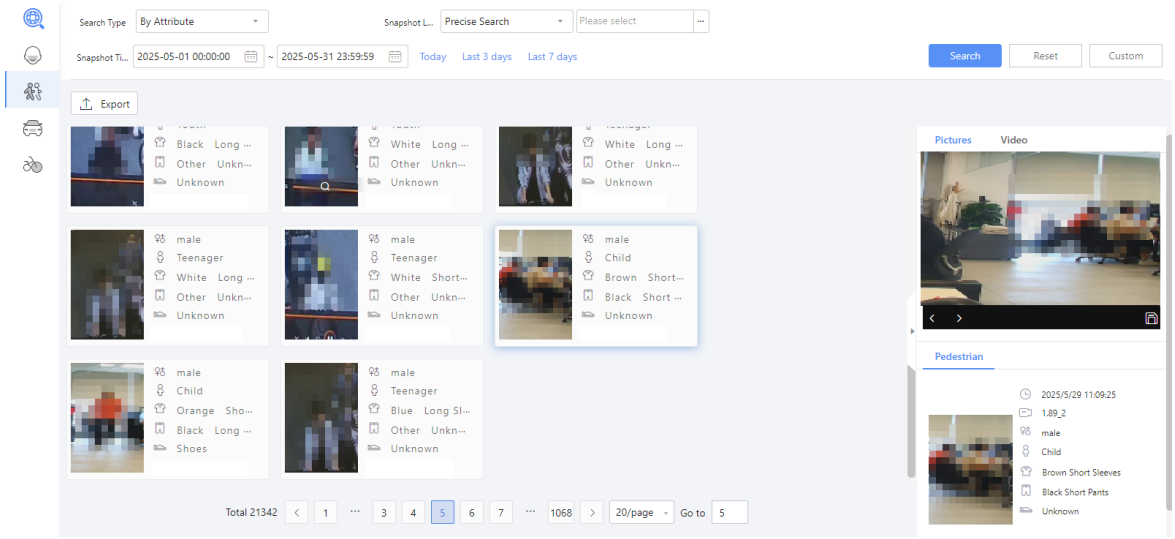
20.3 Pedestrian Search

Go to **Data Search > Comprehensive Search > Pedestrian**.

20.3.1 Search by Attribute

Search pedestrian snapshot records by snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name) , snapshot time, and age, garment style, etc. Click **Custom** to set more search criteria.

Search results are displayed below. Click a record view the alarm image and person attributes on the right.



More Operations

- Search by image: Hover the mouse over the result and click to search by image.
- Export: Click **Export** to export the search results to a .xlsx file.
- Download image/recording: Click under the**Image/Recording** tab to download the image/recording.

Related Operation

You can customize the attributes displayed on the snapshot record card as needed. See Card Attribute.

20.3.2 Search by Image

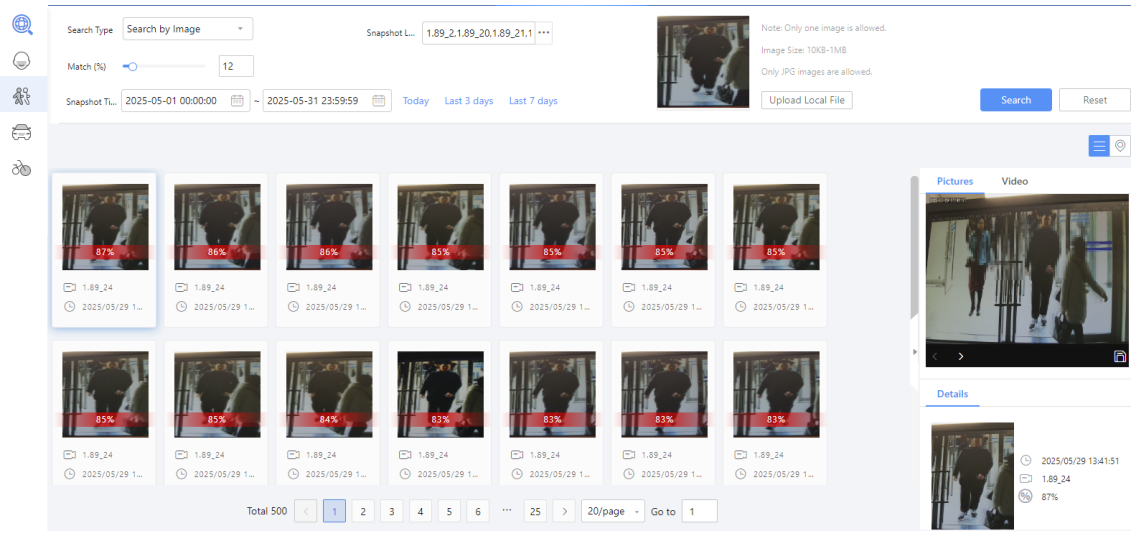
The system supports searching for similar individuals in pedestrian pass-thru records using pedestrian images.

Note:
Please first add the smart NVR on the platform for human body comparison via the smart NVR.

1. Select the search type as **Search by Image**.
2. Click **Upload Local File** to upload the image of the individual you want to search for (up to 1 image).
3. Set the search criteria.

Snapshot Time	Choose the start and end times for the records to search.
Snapshot Location	Select the NVR or video channels under the NVR (multiple NVRs can be selected simultaneously). The search image will be compared against the pedestrian pass-thru records on the NVR.
Match	Set the image similarity threshold. The search results will only display human body images with similarity greater than or equal to the threshold to the uploaded image.

4. Click **Search** to search the images that meet the criteria.



Search Result Operations

You can perform actions such as viewing images, watching video recordings, viewing trajectories, etc.

20.3.3 Pedestrian Trajectory

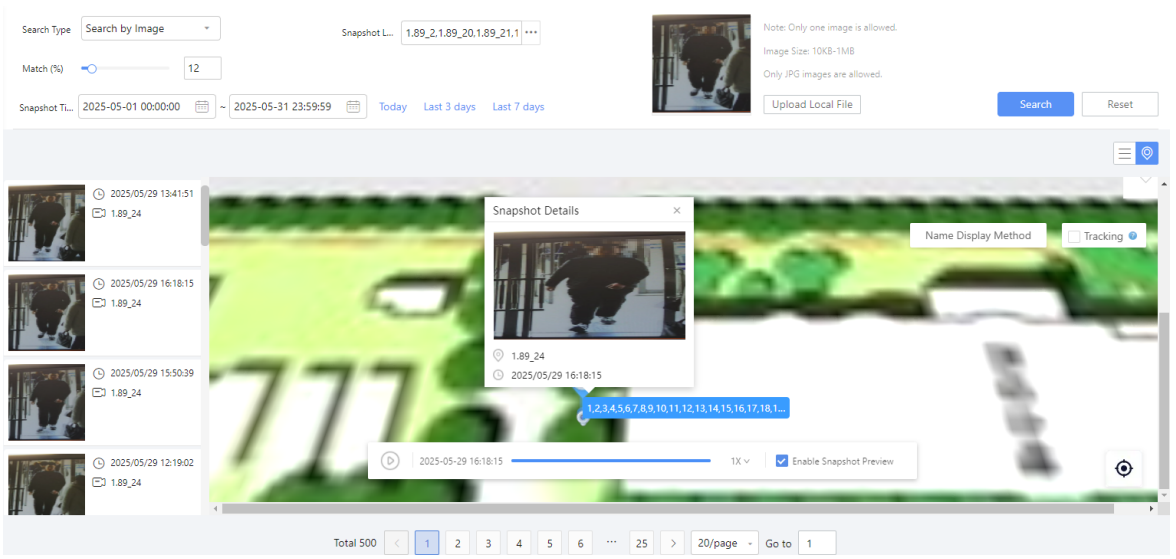
For pedestrian **image search records**, the system supports marking the locations where a pedestrian appeared on the map and generating his/her movement trajectory in chronological order. The trajectory provides information such as the pedestrian's activity range and stop points.

Operation Description

After finding the matching pedestrian on the **Pedestrian Search** page, click in the top-right corner of the result list to view the pedestrian's movement trajectory on the map. Click to play the trajectory, with adjustable playback speed. Enabling snapshot preview will allow you to view the pedestrian's snapshot images at the device locations.

Note:

- Please complete Map Configuration first: Upload the map and mark the camera locations.
- The system will only generate the trajectory for the most recent 20 snapshot records from the search results.
- Try to set more precise search conditions (such as a higher similarity threshold) to help the system retrieve snapshots of the same pedestrian, enabling the generation of the pedestrian's movement trajectory.



20.4 Motor Vehicle Search

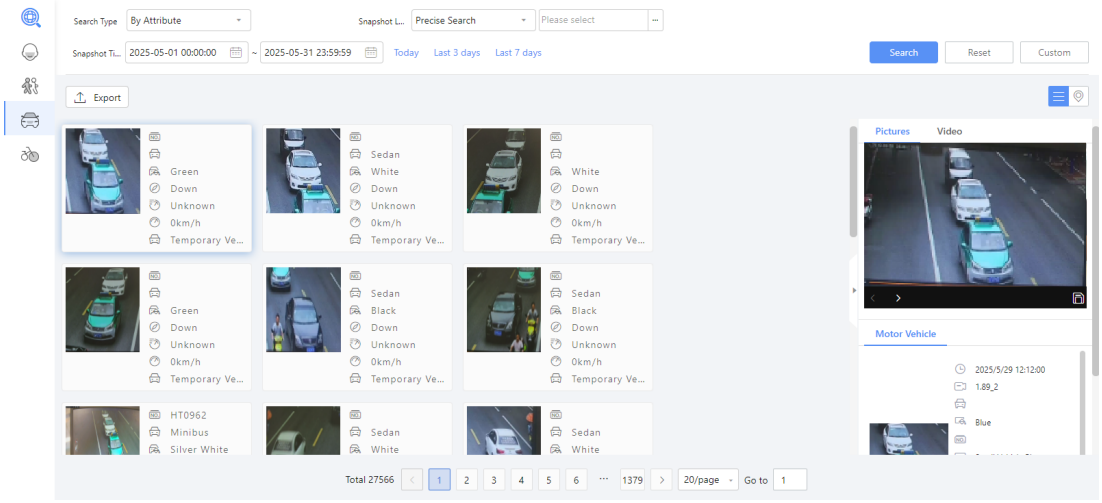
Go to **Data Search > Comprehensive Search > Motor Vehicle**.

20.4.1 Search by Attribute/Alarm/Violation

You can search target vehicles by vehicle attribute, alarm event, or violation in vehicle pass-thru records captured by cameras.

1. Select a search type.

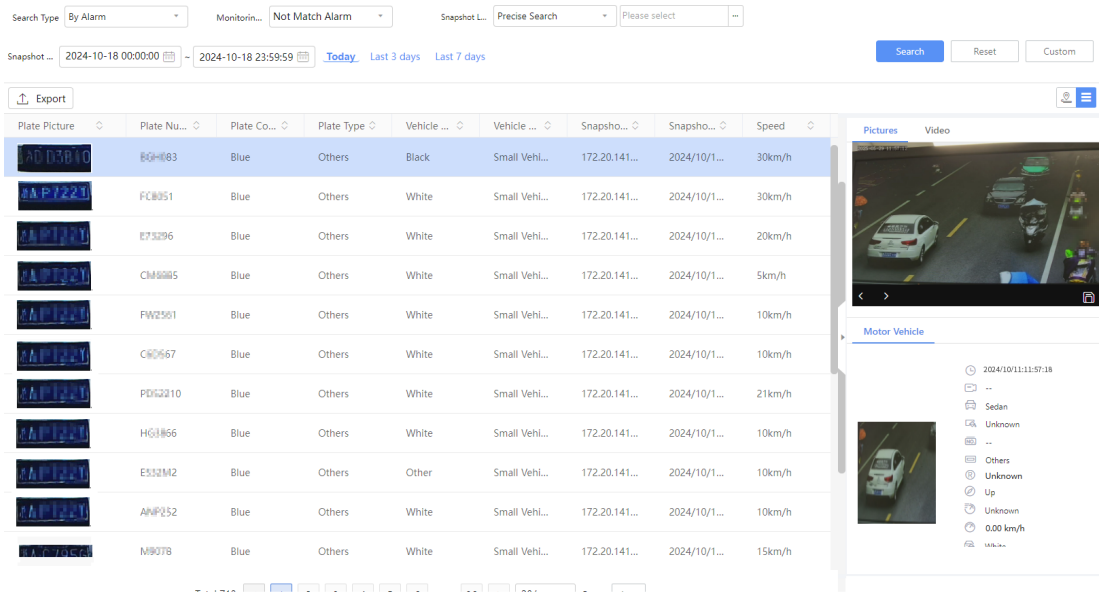
- By Attribute: Set the snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name) and snapshot time. Click **Custom** to set the plate number, vehicle type, plate color, plate type, driving direction, speed type, vehicle colors, vehicle attribute (authorized/forbidden/temporary vehicle) as needed.



Note:
The card also displays the vehicle's attribute (authorized/forbidden/temporary vehicle) in Parking Lot. For authorized vehicles, the owner's name and telephone number will also be shown in the detailed attributes on the right side.

- By Alarm: Set the vehicle monitoring type (match alarm/not match alarm), snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name), and snapshot time. Click **Custom** to set the plate number, plate color and vehicle color as needed.

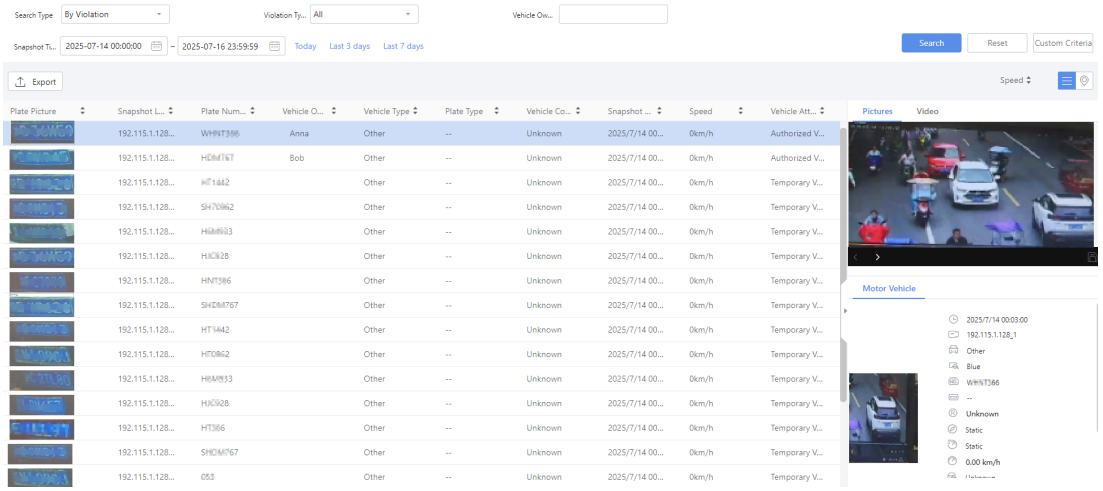
Note:
Vehicle alarm types are configured in Main Parking Lot.



- By Violation: Set the violation type (all/speeding), snapshot time. Click **Custom** to set the plate number, vehicle type, plate color, plate type, driving direction, speed type, vehicle color, vehicle attribute (authorized/forbidden/temporary vehicle) as needed.

  Note:

  - Please add radar vision cameras and configure speeding alarm rules first.
  - The record also displays the vehicle's attribute (authorized/forbidden/temporary vehicle) in Parking Lot. For authorized vehicles, the owner's name will also be shown.
  - Click the ⇕ in the table header to sort vehicles on the current page; click the Speed ⇕ above the table to sort all vehicles by speed.



2. Click **Search** to find motor vehicle records.

More Operations

Search results are displayed at the bottom of the page.

- For results searched by attribute/event: You can click a record to view picture, video (5s before and 5s after the snapshot time), and motor vehicle attributes on the right. And also click under the tab to save the picture/video.
- Search by image: Hover the mouse over the result and click to search by image.
- Click **Export** to export the search results to a .xlsx file.
- Click to view Motor Vehicle Trajectory.

Related Operation

You can customize the attributes displayed on the snapshot record and alarm record cards as needed. See Card Attribute.

20.4.2 Search by Image

The system supports searching for similar vehicles in vehicle pass-thru records using vehicle images.

Note:
Please first add the smart NVR on the platform for vehicle comparison via the smart NVR.

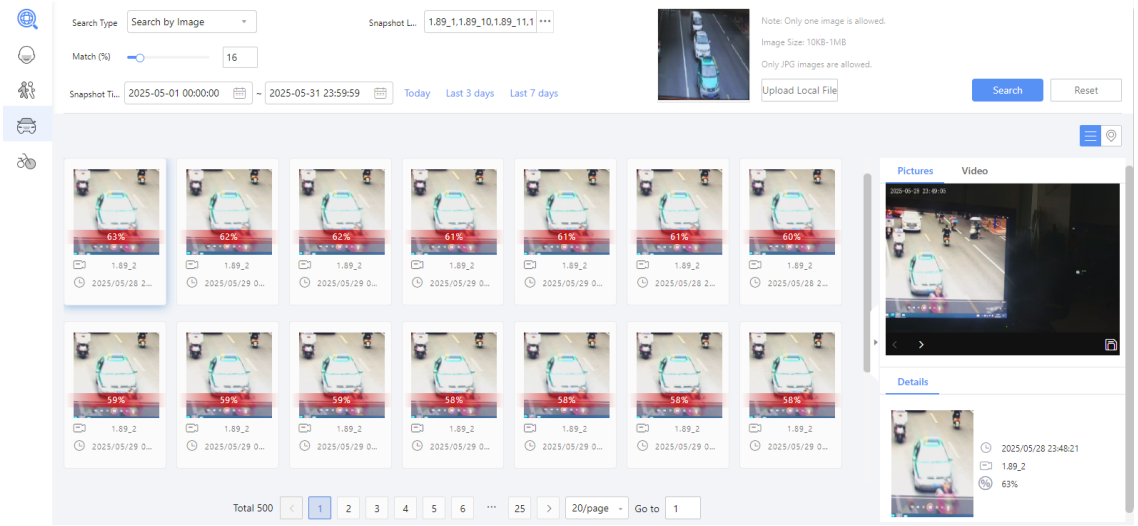
1. Select the search type as **Search by Image**.
2. Click **Upload Local File** to upload the image of the vehicle you want to search for (up to 1 image).
3. Set the search criteria.

Snapshot Time	Choose the start and end times for the records to search.
Snapshot Location	Select NVR(s) or the video channels under NVR(s), and the uploaded image will be compared with the vehicle pass-thru records in NVR(s).

Match	Set the image similarity threshold. The search results will only display vehicle images with similarity greater than or equal to the threshold to the uploaded image.

4. Click **Search** to search for vehicle pass-thru records that meet the criteria.

Figure 20-9: Search Vehicle Pass-Thru Records



Search Results

The search results are displayed at the bottom of the page.

- Click on a specific result to show the original snapshot, recording (5 seconds before and after the snapshot), and snapshot details on the right side. Click to save the image/recording.
- Click to view Motor Vehicle Trajectory.

20.4.3 Motor Vehicle Trajectory

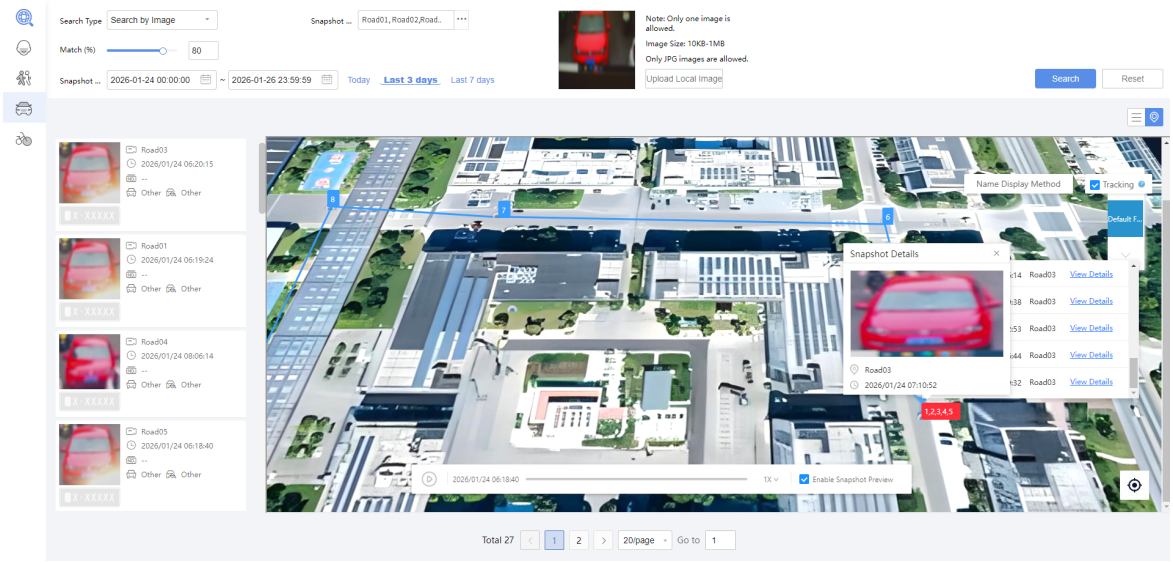
For motor vehicle search records, the system supports marking the locations where a motor vehicle appeared on the map and generating its movement trajectory in chronological order. The trajectory provides information such as the motor vehicle's activity range and stop points.

Operation Description

After finding the matching pedestrian on the **Motor Vehicle Search** page, click in the top-right corner of the result list to view the motor vehicle's movement trajectory on the map. Click to play the trajectory, with adjustable playback speed. Enabling snapshot preview will allow you to view the motor vehicle's snapshot images at the device locations.

Note:

- Please complete Map Configuration first: Upload the map and mark the camera locations.
- The system will only generate the trajectory for the most recent 20 snapshot records from the search results.
- Try to set more precise search conditions (e.g. a specific license plate number) to help the system retrieve snapshots of the same motor vehicle, enabling the generation of the motor vehicle's movement trajectory.



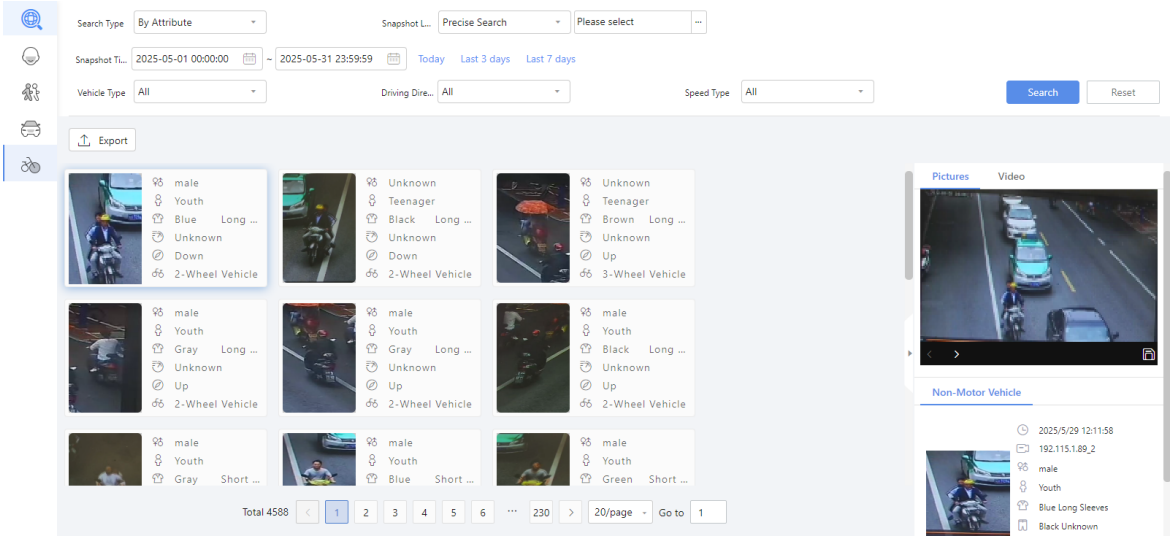
20.5 Non-Motor Vehicle Search

Go to **Data Search > Comprehensive Search > Non-Motor Vehicle**.

20.5.1 Search by Attribute

Search non-motor vehicle snapshot records by snapshot location (through precise search by selecting the device on resource tree or fuzzy search by entering keywords of the device name), snapshot time, vehicle type, driving direction and speed type.

Search results are displayed below. Click a record to view the alarm image and non-motor vehicle attributes on the right.



More Operations

Perform the following operations as needed.

- Search by image: Hover the mouse over the result and click to search by image.
- Export: Click **Export** to export the search results to a .xlsx file.
- Download image/recording: Click under the**Image/Recording** tab to download the image/recording.

Related Operation

You can customize the attributes displayed on the snapshot record card as needed. See Card Attribute.

20.5.2 Search by Image

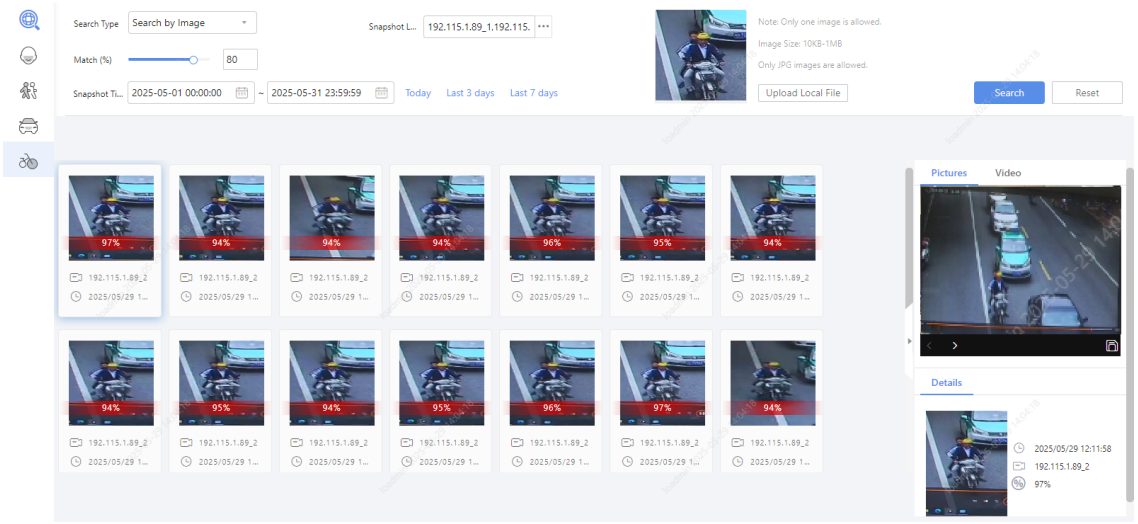
The system supports searching for similar non-motor vehicles in pass-thru records using images of non-motor vehicles.

Note:
Please first add the smart NVR on the platform for non-motor vehicles comparison via the smart NVR.

1. Select the search type as **Search by Image**.
2. Click **Upload Local File** to upload the image of the non-motor vehicle you want to search for (up to 1 image).
3. Set the search criteria.

Snapshot Time	Set the start and end times of the records.
Snapshot Location	Select NVR(s) or the video channels under NVR(s), and the uploaded image will be compared with the non-motor vehicle pass-thru records in NVR(s).
Match	Set the image similarity threshold. The search results will only display non-motor vehicle images with similarity greater than or equal to the threshold to the uploaded image.

4. Click **Search** to search non-motor vehicle pass-thru records that meet the criteria.



Search Results

The search results are displayed at the bottom of the page.

Click a specific result to show the original snapshot image, recording (5 seconds before and after the snapshot), and snapshot details on the right side. Click to save the image/recording.

20.5.3 Non-Motor Vehicle Trajectory

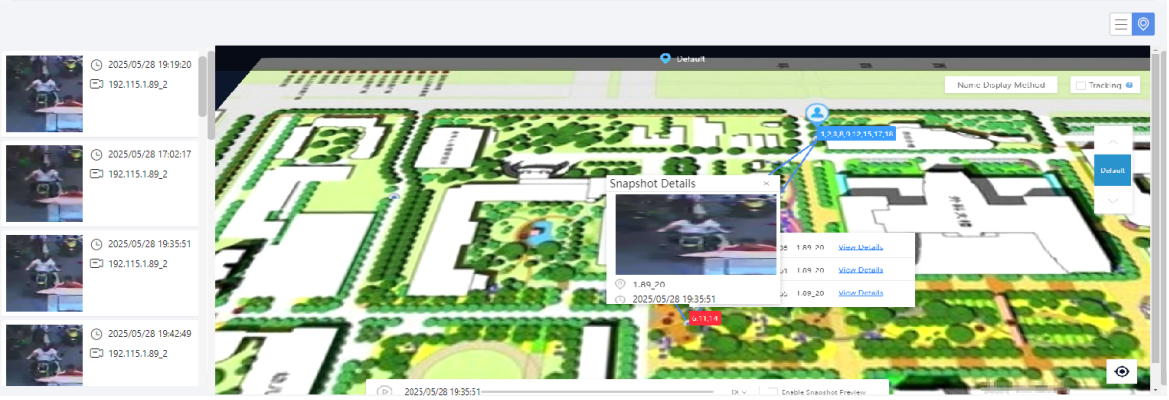
For non-motor vehicle **image search records**, the system supports marking the location where a non-motor vehicle appeared on the map and generating its movement trajectory in chronological order. The trajectory provides information such as the non-motor vehicle's activity range and stop points.

Operation Description

After finding the matching non-motor vehicle on the **Non-Motor Vehicle Search** page, click in the top-right corner of the result list to view the non-motor vehicle's movement trajectory on the map. Click to play the trajectory, with adjustable playback speed. Enabling snapshot preview will allow you to view the non-motor vehicle's snapshot images at the device locations.

Note:

- Please complete Map Configuration first: Upload the map and mark the camera locations.
- The system will only generate the trajectory for the most recent 20 snapshot records from the search results.
- Try to set more precise search conditions (such as a higher similarity threshold) to help the system retrieve snapshots of the same non-motor vehicle, enabling the generation of the non-motor vehicle's movement trajectory.



21 AcuTrack

Data Search > AcuTrack

AcuTrack can search for motor vehicle/non-motor vehicle/pedestrian targets in recorded videos by a target image. It can retrieve the video segments containing the target and mark the corresponding time periods on the playback progress bar. AcuTrack allows users to continuously view the video segments containing the targets, review the events, greatly reducing the workload of video investigation.

Note:
The AcuTrack function relies on intelligent computing power: you need to add smart NVRs to the platform.

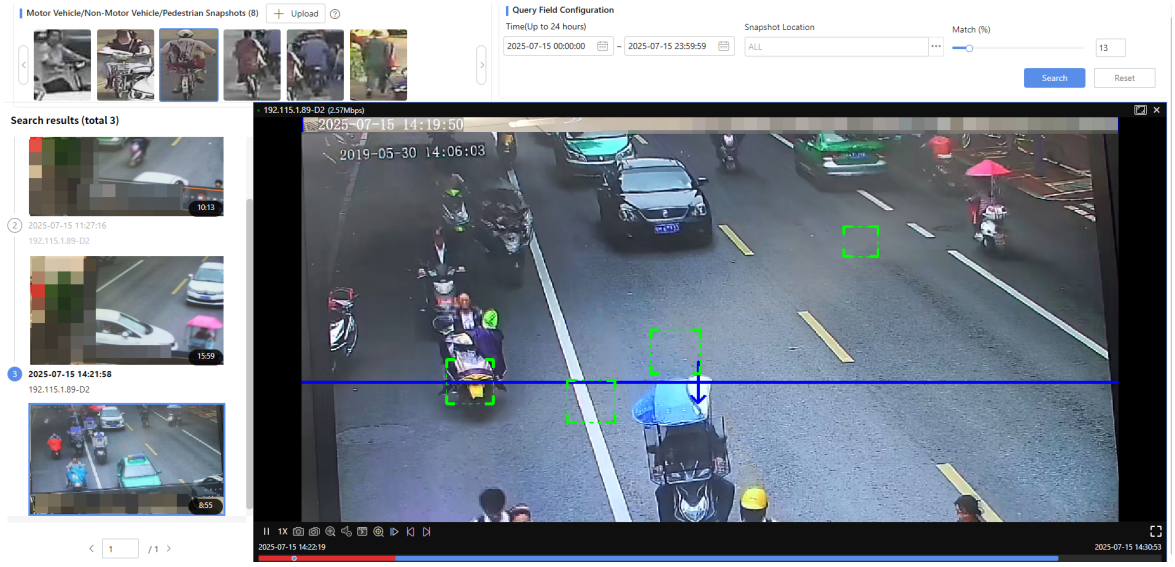
Target Search

1. Click **Upload** in the top left corner and upload an image of the target.
   For a large scene image, after the image is uploaded, the system automatically recognizes and extracts thumbnail images of all targets in it, and you must select **one** image that will be used for target search.

   Note:

   - The uploaded image must be in JPG format and less than 4MB.
   - Only one image is supported. Uploading again will overwrite the previously uploaded image.

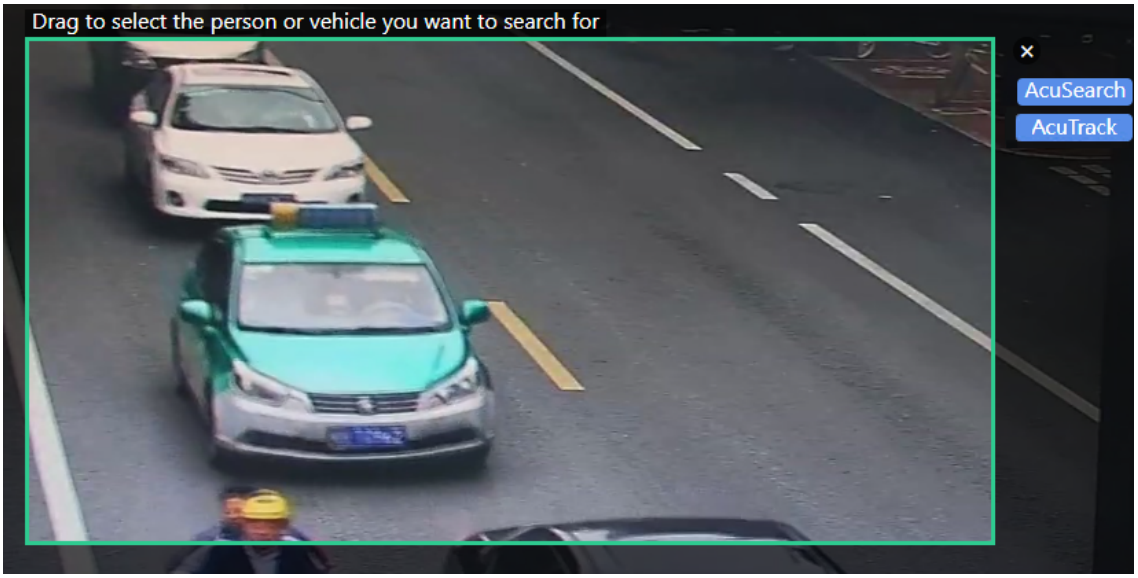
2. Set a time range (up to 24 hours), capture device, similarity, and click **Search**.



Search Results

Attention:
Switching page will reset the existing search results, and you will need to perform a new search when going back next time.

- The left side shows the video segments containing the target, sorted from early to late by time. The recording start time and camera name are shown above the video. The video duration is displayed in the lower right corner.
- Select a video segment to play it. On the timeline, red indicates video segments with target, and blue indicates regular video segments.
- Click on the playback toolbar to search for targets on the current video image.



1. Search the target to search:
   - Drag the mouse within the green box to move its position.
   - Hover over the edge or vertex of the green box. When the cursor turns into an arrow shape, drag to resize the green box.
   - To exit the search, click **X**.
2. Choose a search mode. Two modes are available:
   - Click the **AcuSearch** button at the top right corner of the green box to go to the SeekFree page, where the system will automatically search for all capture records of the target within the green box (see Search by Image).

- Click the **AcuTrack** button at the top right corner of the green box to go to the AcuTrack page, where you can search for recordings containing the target in the green box.

22 People Flow Counting

This function is applicable to people flow control scenarios such as campus areas, train stations, etc. The smart IPCs, NVRs or radar devices count the number of people entering and leaving an area and the number of people present in an area to track the dynamics of people flow, helping formulate evacuation or security measures in a timely manner to ensure safety.

Functions

Menu	Description
Real-Time People Counting	Allows users to view live video from devices and real-time data reported from devices, including people counting data and crowd density data, and will trigger an alarm when the number of people in an area exceeds the preset threshold.
Data Statistics	Allows users to view the people flow dynamics within an area by time period and view the details.

22.1 Real-Time People Counting

Go to **Video Application > Smart Live View > People Counting**.

View the live videos of the video channels under the smart IPC/NVR/radar and the people flow and crowd density data.

Note: Among radar devices, only visual intelligent alarm detectors support live view.

Prerequisite

- Smart IPC/NVR/radar devices have been added to the platform. See **Device Management** > Private Device.
- People flow counting and crowd density monitoring functions have been enabled on the device.

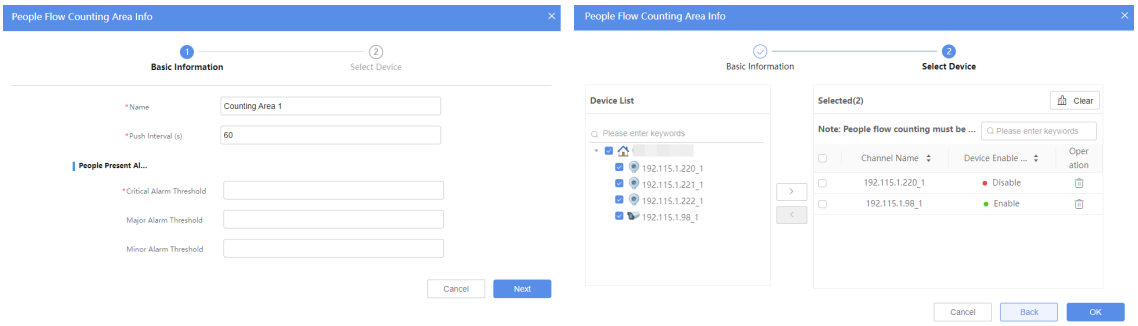
On the **Smart Live View** page, click and select **People Counting**.

22.1.1 People Flow Counting

Configure people flow counting tasks on the device, detect the number of people entered/exited and calculate their difference to get the number of people present in the monitoring area.

Add People Flow Counting Area

1. Click + for the people flow counting. A dialogue box appears.



2. Configure the area information.

Item	Description
Name	Set the counting area name.

Item	Description
Push Interval(s)	Set the alarm push interval.
Alarm Threshold	Set the critical, major and minor alarm threshold. An alarm is reported when the number of people present exceeds the threshold. **Note:** Threshold level: Critical (required) > Major > Minor.
Select Device	Select devices (maximum 20) for the people flow counting.

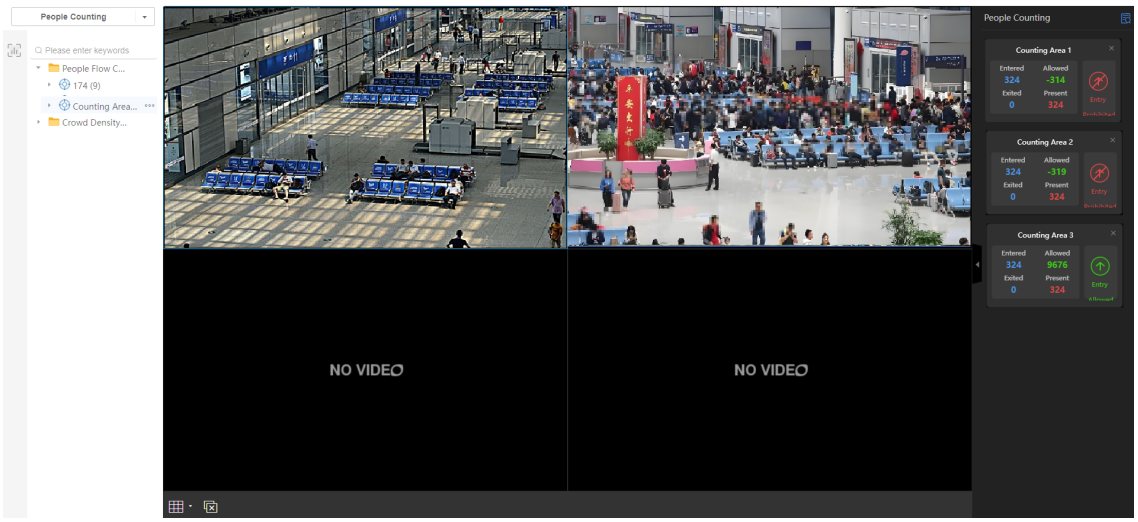
3. Click **OK**.

View People Flow Counting

- The counting area list is on the left and the critical alarm threshold are displayed next to the counting area name.
- On the people flow counting area, double-click on a device in the channel list to view its live video in a window.

Note:

- Up to 4 live videos can be displayed at the same time. You can click in the lower left corner to switch to 1/3/4 windows.
- To perform operations on the live view, see Live View Toolbar.



- Click ••• for the people flow counting area and select **Search**. The real-time data of people entered/exited/present/allowed (critical alarm threshold - people present) are displayed on the right side.
  If the number of people present is less than the critical alarm threshold, the status is Entry Allowed; otherwise, the status is Entry Prohibited.
- Click in the right corner to view Data Statistics.

Edit Area

Click ••• for the people flow counting area and select **Edit** to edit the area information, including the area name, push interval, alarm threshold and camera.

Delete Area

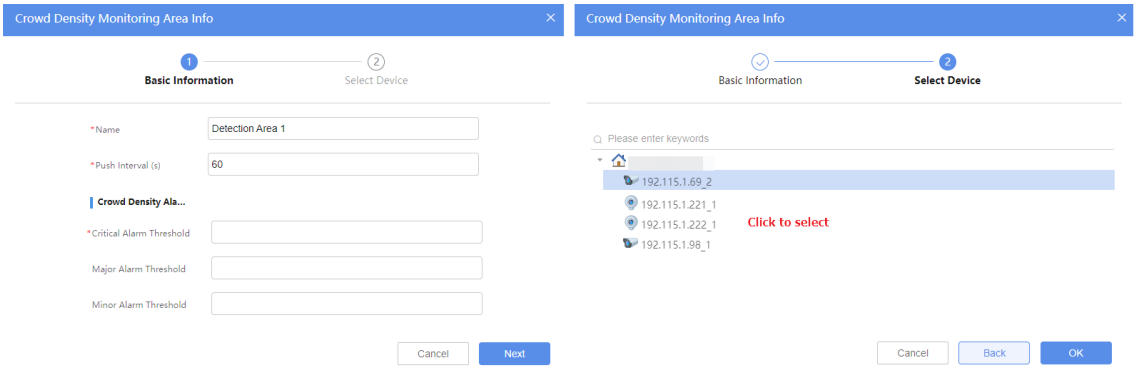
Click ••• for the people flow counting area and select **Delete** to delete the area.

22.1.2 Crowd Density Monitoring

Configure the crowd density monitoring tasks on the device and detect the number of people present (crowd density) in the monitoring area.

Add Crowd Density Monitoring Area

1. Click ＋ for the crowd density monitoring. A dialogue box appears.



2. Configure the area information.

Item	Description
Name	Set the counting area name.
Push Interval(s)	Set the alarm push interval.
Alarm Threshold	Set the critical, major and minor alarm threshold. An alarm is reported when the number of people present exceeds the threshold. **Note:** Threshold level: Critical (required) > Major > Minor.
Select Device	Select one device for the crowd density monitoring.

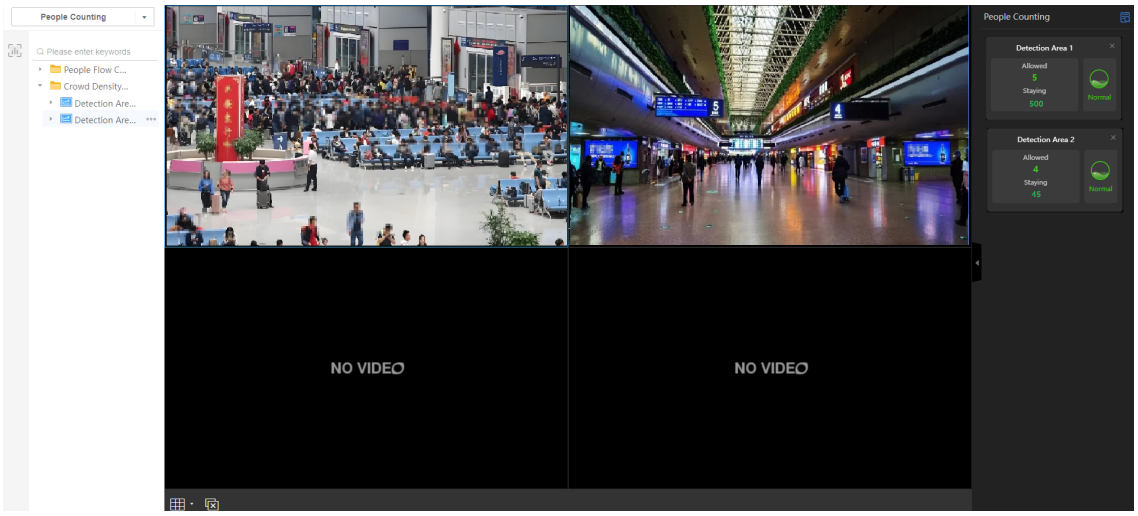
3. Click **OK**.

View Crowd Density

- The counting area list is on the left. The critical alarm threshold are displayed next to the counting area name.
- On the crowd density monitoring area, double-click on a device in the channel list to view its live video in a window.

Note:

- Up to 4 live videos can be displayed at the same time. You can click in the lower left corner to switch to 1/3/4 windows.
- To perform operations on the live view, see Live View Toolbar.



- Click ••• for the crowd density monitoring area and select **Search**. The real-time data of people present and allowed (critical alarm threshold - people present) are displayed on the right side.
  If the number of people present is less than the minor alarm threshold, the status is Normal; otherwise, the status is Minor Alarm/Major Alarm/Critical Alarm.

Edit Area

Click ⋯ for the crowd density monitoring area and select **Edit** to edit the area information, including the area name, push interval, alarm threshold and camera.

Delete Area

Click ⋯ for the crowd density monitoring area and select **Delete** to delete the area.

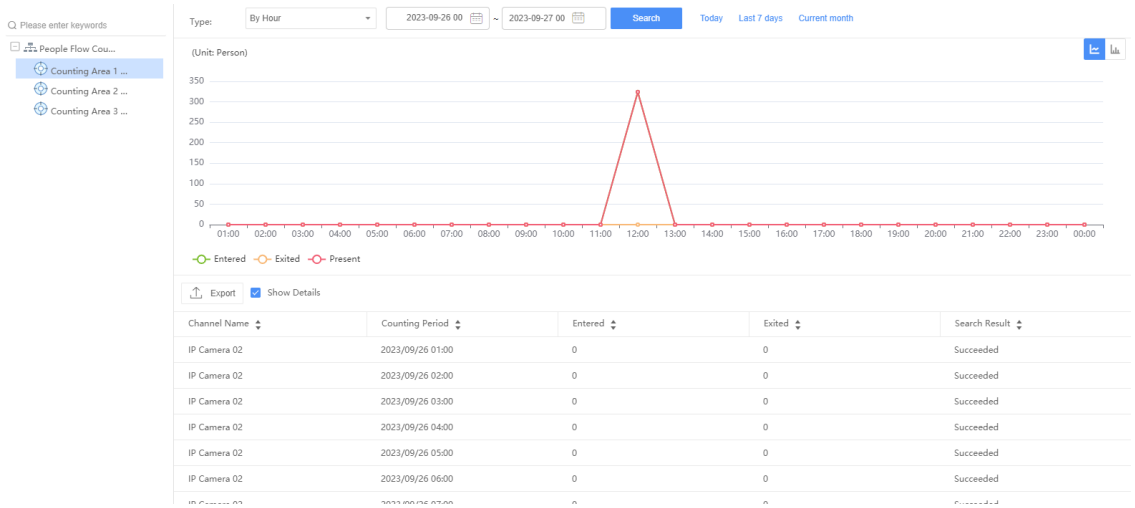
22.2 Data Statistics

Go to **Data Search > People Counting**.

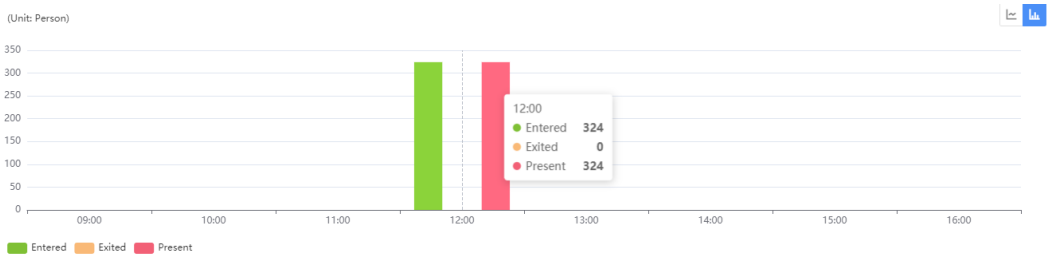
Users can view the people flow dynamics within an area by time period and view the details.

Note: You need to add a People Flow Counting area first.

1. Select a counting area in the people flow counting area list on the left.
2. Select the counting type, set the counting period, and then click **Search**.



- Statistical chart: Click in the upper-right corner to switch the view to line chart or bar chart.
  - The line chart shows the trend of the number of people entered/exited/present at each point of time. Click Entered Exited Present to filter the statistics.
  - The bar chart shows the number of people entered/exited/present. Click Entered Exited Present to filter the statistics.



- Data list: Shows the number of people entered/exited/present at each point of time.
  - Select **Show channel details** to show the channel name in the list.
  - Click **Export** to export data.

23 Area Appearance Frequency Counting

Go to **Data Search > Area Appearance Frequency Counting**

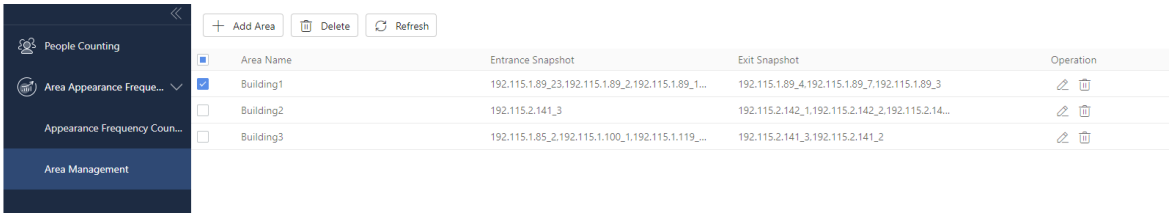
After setting up entry and exit capture cameras for an area, you can track the frequency of people entering and exiting the area, view their entry and exit records, and calculate the number of people staying in the area on a given day.

For example: Track the entry and exit frequency of employees in an office building and the number of employees on duty.

(Refer to this section for entry and exit frequency statistics, and refer to Data Dashboard for on-duty employee statistics.)

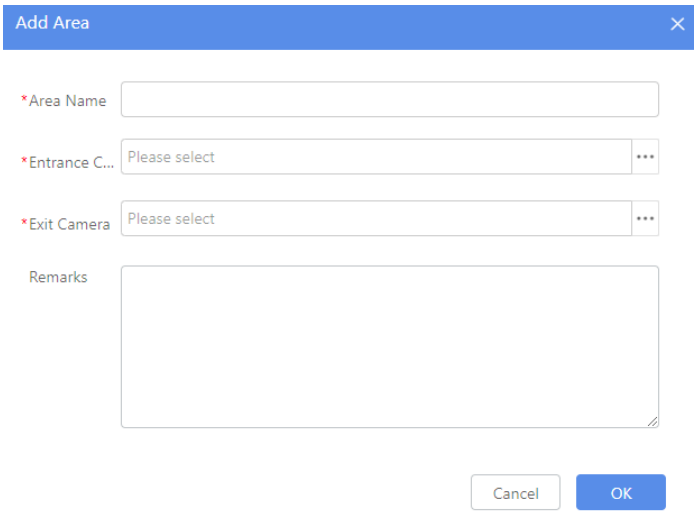
23.1 Area Management

Add the areas that require personnel frequency statistics and configure the entrance and exit cameras for these areas.



Add Area

1. Click **Add Area**.



2. Enter the area name (custom), and select the entrance camera and exit camera (support smart IPCs or IPCs under smart NVRs).
3. Click **OK**.

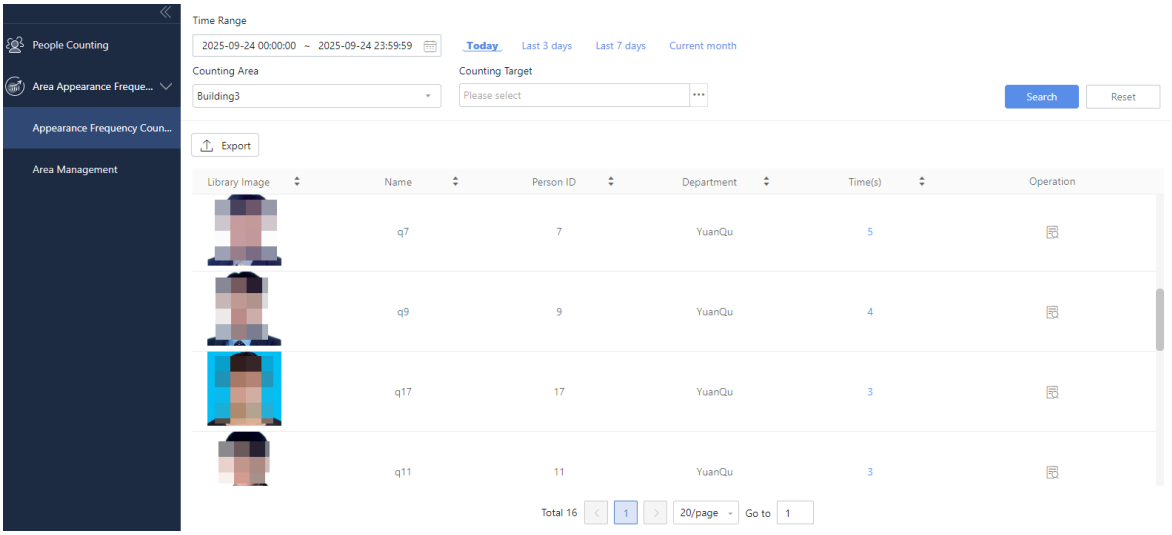
Area Management

- Modify an area: Click the corresponding in the **Operation** column.
- Delete an area: Click the corresponding in the **Operation** column, or select multiple areas and then click **Delete** on the top.

23.2 Appearance Frequency Counting

Select the time period, area (single choice), and counting target (person or department), then click **Search**.

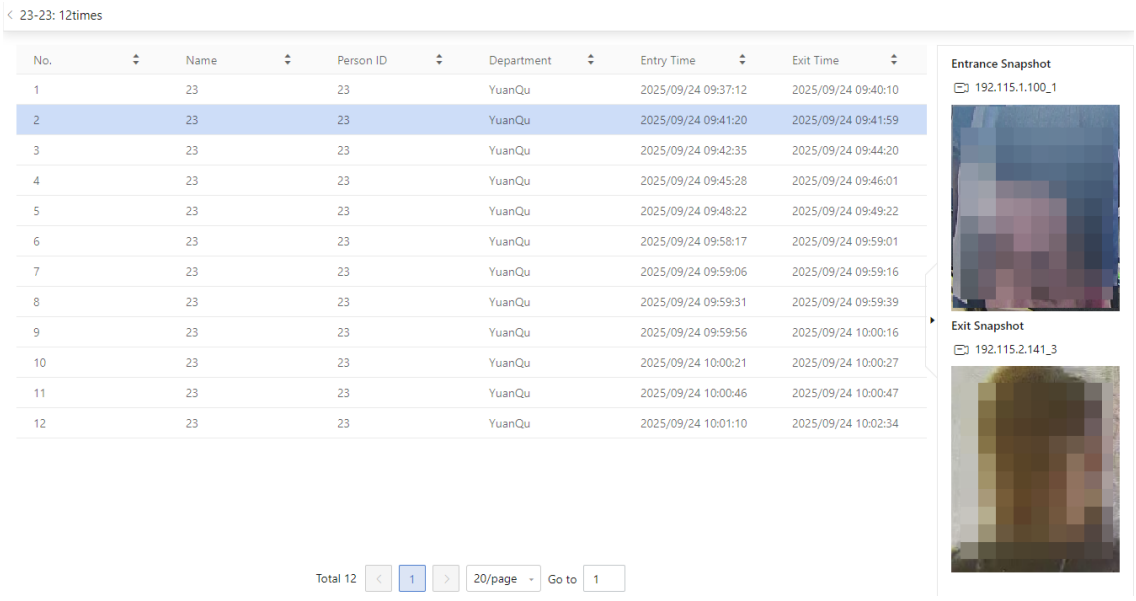
The search results will display the matching persons and the number of entries/exits of each person.



Note:

- The count will increase by 1 in these cases: Entry-Exit, Entry-Entry-Exit, Entry-Exit-Exit, Entry-Exit-Entry, only a single entry, or only a single exit.
- The data supports cross-day counting. For example, if someone enters on the first day and exits on the second day, the count will also increase by 1.

- **View Details**
  Click the corresponding count (blue font) or to view their entry and exit records. Each record includes entry time and exit time . By selecting a record, you can view the entry/exit snapshot images.



- **Export**
  Click **Export** to export all the search results.

24 Radar Control

Go to **Park Application** > **Radar Control**.

Radars support human presence detection, fall detection, people counting detection, and vital sign detection.

Once radars are connected to the platform via the private protocol and monitoring tasks have been assigned to them, radar detection alarms can be reported to the platform.

Prerequisite

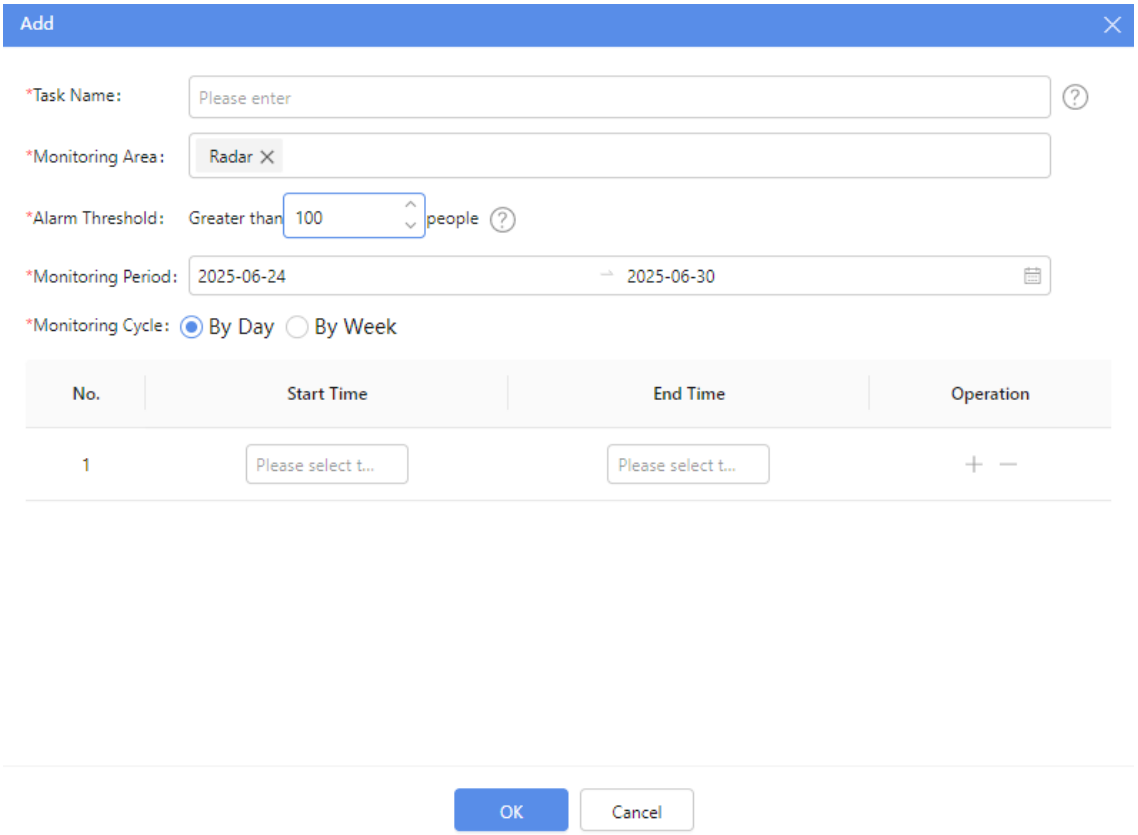
Radars have been added in Device Management > Frontend Device > Private Device.

24.1 People Counting Monitoring

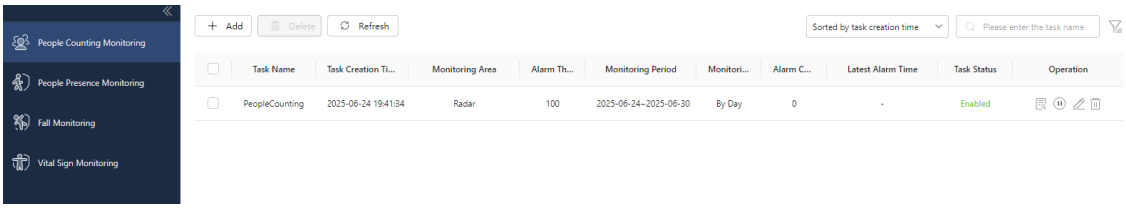
Triggers an alarm when the number of people in the monitoring area exceeds the set threshold.

Add Monitoring

1. Click **Add**.
2. Enter the task name, and then specify monitoring area, alarm threshold(maximum allowed people number), monitoring period, and monitoring cycle.
   - By day: Set up to 8 monitoring periods for a day. The task will be repeated daily.
   - By week: Set monitoring periods for each day of the week. The task will be repeated weekly.

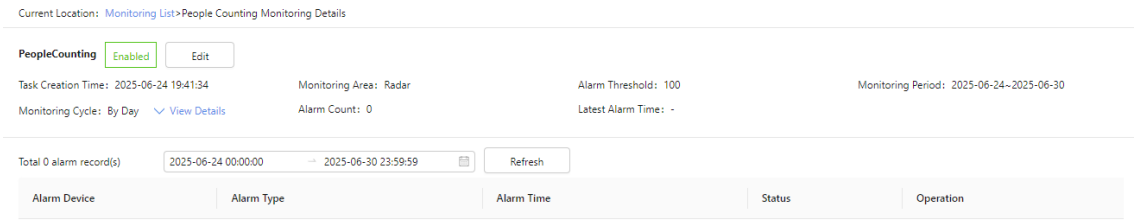


3. Click **OK**.



Other Operations

- Filter tasks: You can search monitoring tasks by task name, latest alarm time, and task status. You can also click to collapse the search criteria.
- View details: Click in the **Operation** column to view monitoring task details and alarm records.



Click **View Details** to view the alarm location and handle alarms. (Note: Currently, radars do not support camera connections, so live view and playback functions are unavailable now.)

- Stop task: Click in the **Operation** column to stop the monitoring task. Once stopped, alarms will not be triggered.
- Edit task: Click in the **Operation** column to edit the monitoring task.
- Delete task: Click in the **Operation** column or select task(s), and then click **Delete** above the list.

24.2 People Presence Monitoring

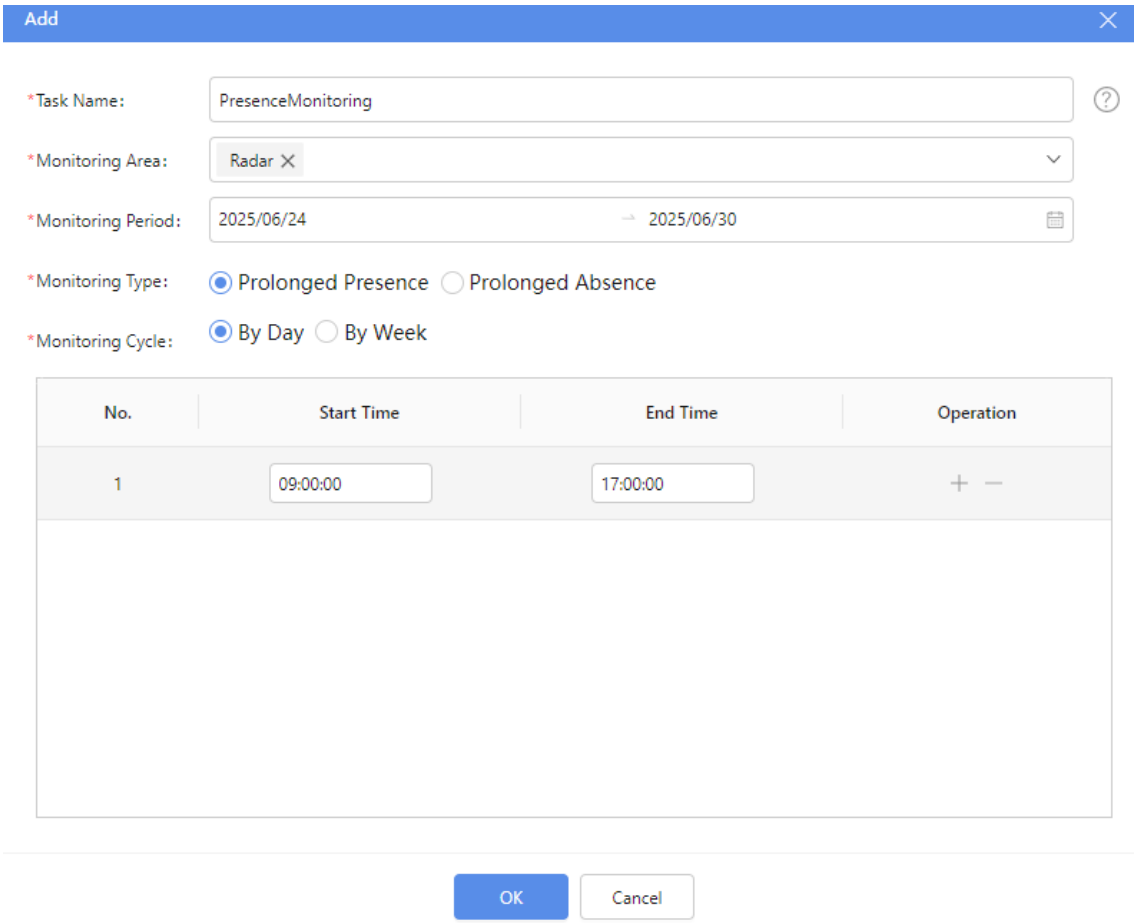
Detects the presence of individuals in the monitoring area.

- Presence alarm: Triggers an alarm when someone remains in the monitoring area for a long time, such as lingering in a hazardous zone.
- Absence alarm: Triggers an alarm when no one is present in the monitoring area for a long time, such as employees being away from their duties or absent for a long time.

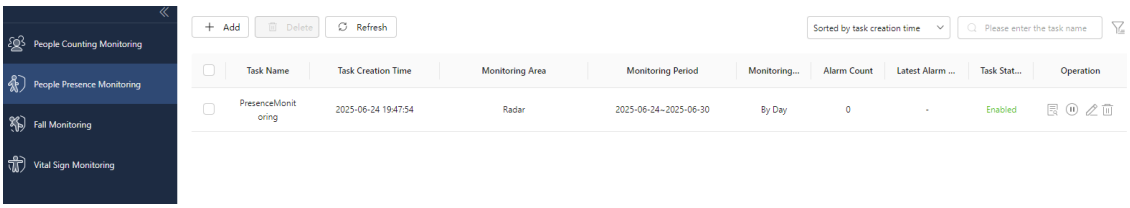
Note:
Time thresholds can be configured on the radar's management page.

Add Monitoring

1. Click **Add**.
2. Enter the task name, and then specify monitoring areas, monitoring period, monitoring type and monitoring cycle.
   - By day: Set up to 8 monitoring periods for a day. The task will be repeated daily.
   - By week: Set monitoring periods for each day of the week. The task will be repeated weekly.

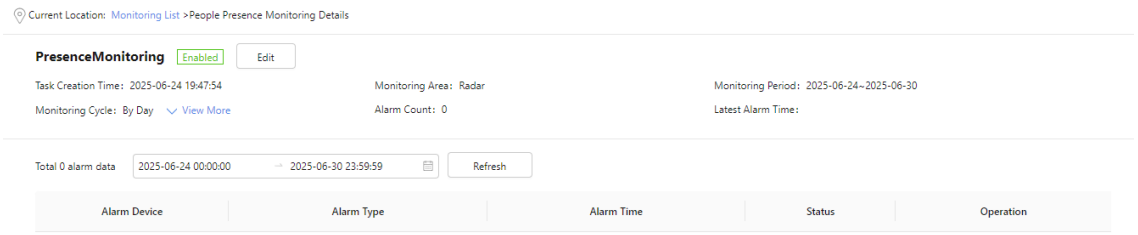


3. Click **OK**.



Other Operations

- Filter tasks: You can search monitoring tasks by task name, latest alarm time, and task status. You can also click to collapse search criteria.
- View details: Click in the **Operation** column to view monitoring task details and alarm records.



Click **View Details** to view the alarm location and handle alarms. (Note: Currently, radars do not support camera connections, so live view and playback functions are unavailable now.)

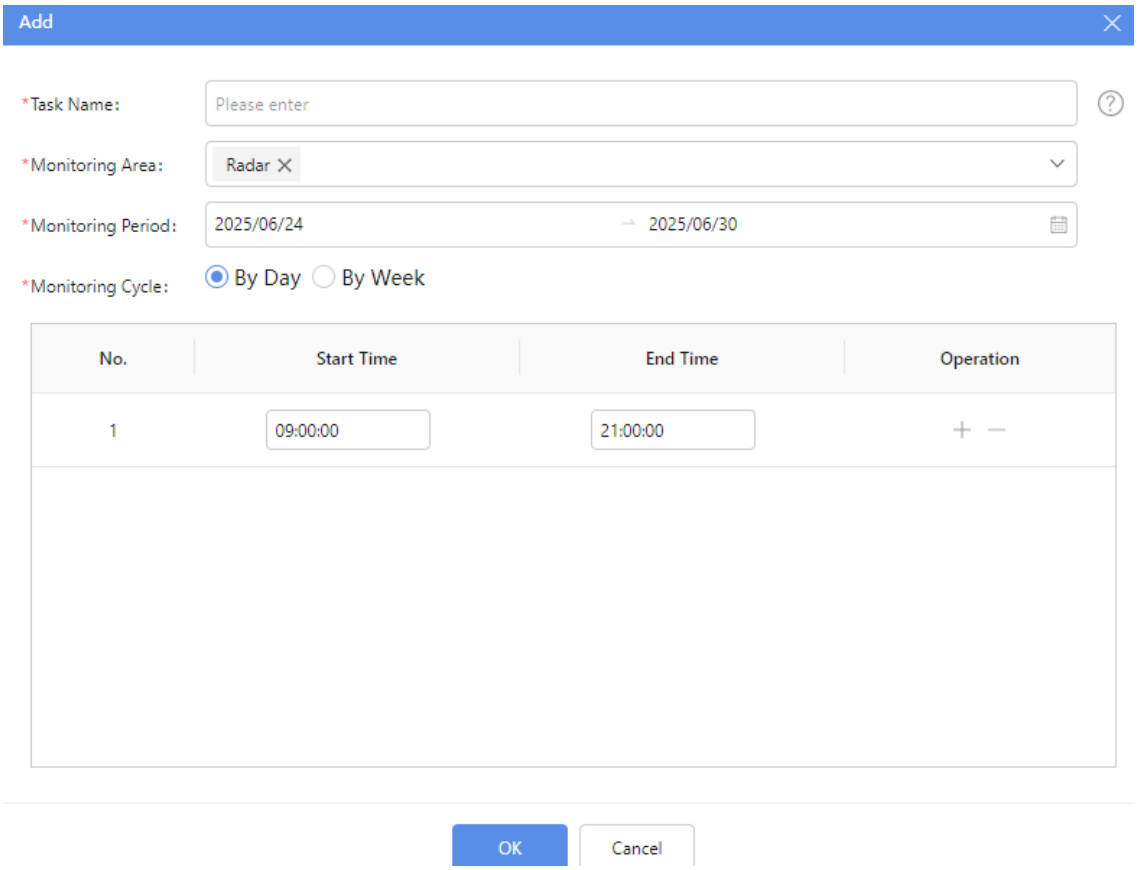
- Stop task: Click in the **Operation** column to stop the monitoring task. Once stopped, alarms will not be triggered.
- Edit task: Click in the **Operation** column to edit the monitoring task.
- Delete task: Click in the **Operation** column or select task(s), and then click **Delete** above the list.

24.3 Fall Monitoring

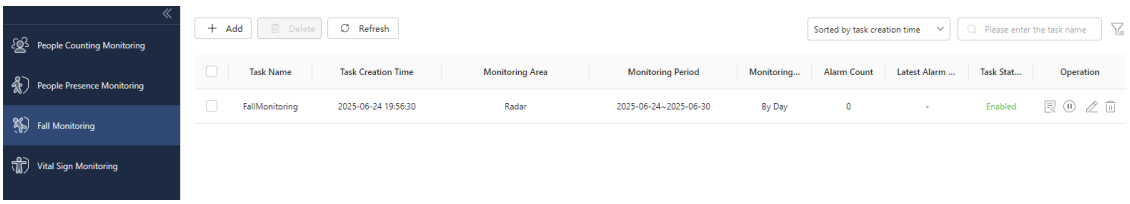
Triggers an alarm when someone falls in the monitoring area.

Add Monitoring

1. Click **Add**.
2. Enter the task name, and then specify monitoring areas, monitoring period, and monitoring cycle.
   - By day: Set up to 8 monitoring periods for a day. The task will be repeated daily.
   - By week: Set monitoring periods for each day of the week. The task will be repeated weekly.

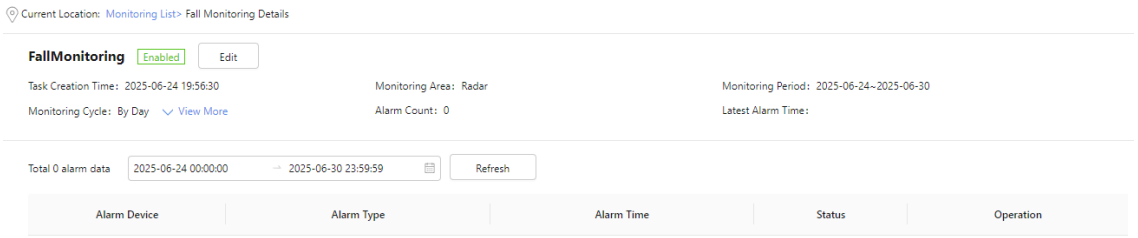


3. Click **OK**.



Other Operations

- Filter tasks: You can search monitoring tasks by task name, latest alarm time, and task status. You can also click to collapse the search criteria.
- View details: Click in the **Operation** column to view monitoring task details and alarm records.



Click **View Details** to view the alarm location and handle alarms. (Note: Currently, radars do not support camera connections, so live view and playback functions are unavailable now.)

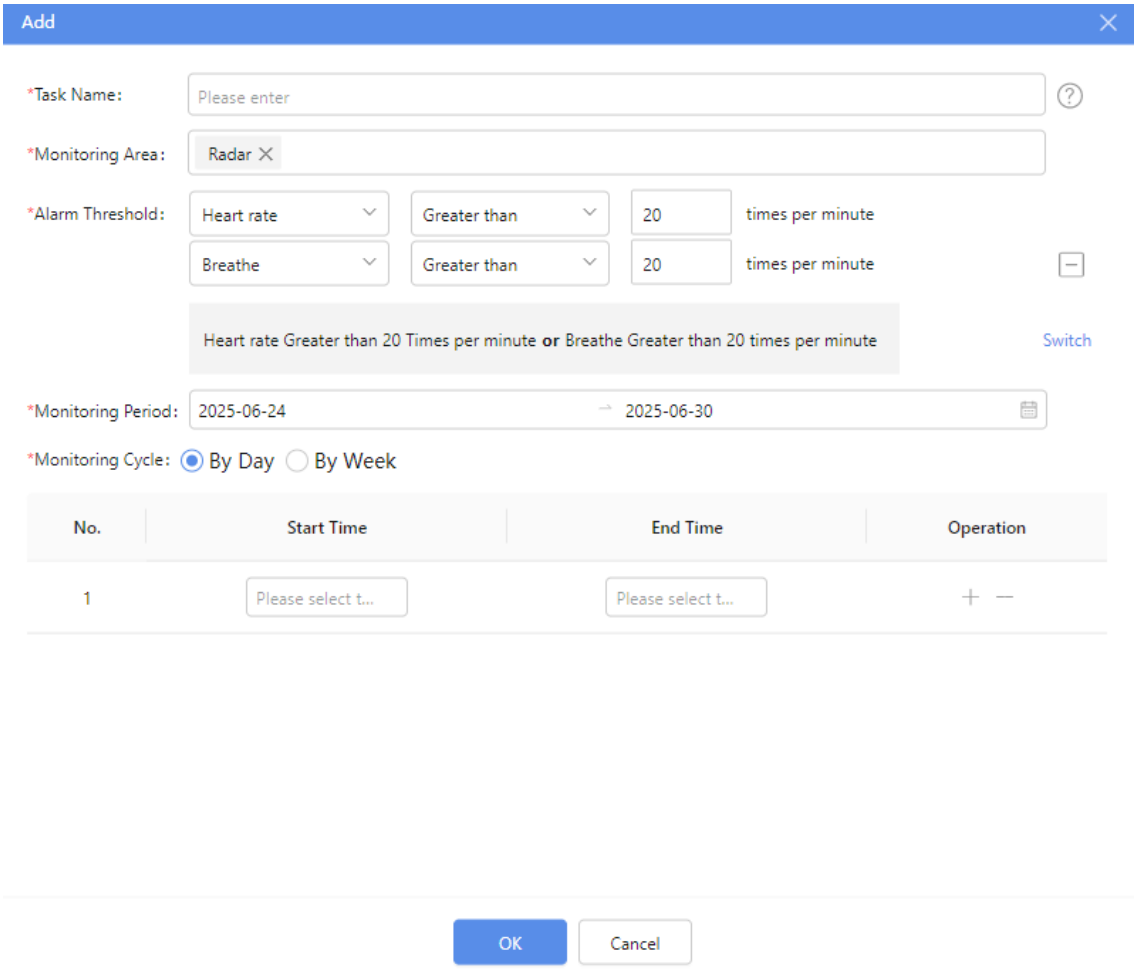
- Stop task: Click in the **Operation** column to stop the monitoring task. Once stopped, alarms will not be triggered.
- Edit task: Click in the **Operation** column to edit the monitoring task.
- Delete task: Click in the **Operation** column or select task(s), and then click **Delete** above the list.

24.4 Vital Sign Monitoring

Triggers an alarm when the vital sign (heart rate/respiration) does not meet the set threshold, allowing timely health conditions for personnel.

Add Monitoring

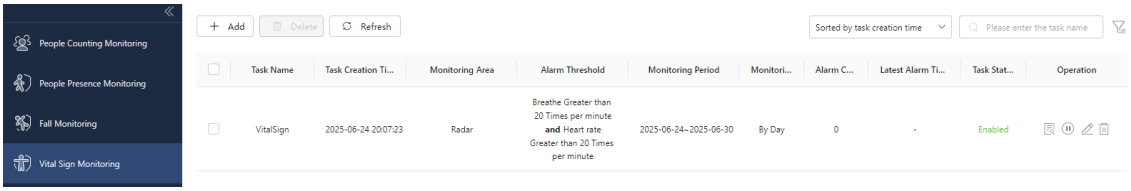
1. Click **Add**. Configure parameters as described below.



Item	Description
Task Name	Customize the rule name as needed.
Monitoring area	Select the radar(s) for monitoring.

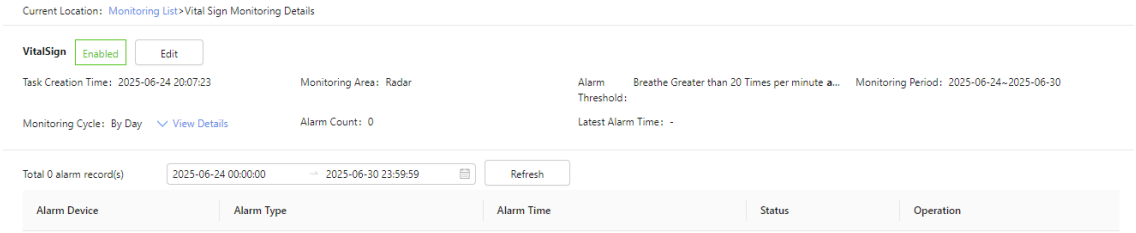
Item	Description
Alarm threshold	• Triggers an alarm when the respiration is greater than/less than N times per minute. • Triggers an alarm when the heart rate is greater than/less than N times per minutes.
Monitoring period	Set a start and end date for monitoring.
Monitoring Cycle	• By day: Set up to 8 monitoring periods for a day. The task will be repeated daily. • By week: Set monitoring periods for each day of the week. The task will be repeated weekly.

2. Click **OK**.



Other Operations

- Filter tasks: You can search monitoring tasks by task name, latest alarm time, and task status. You can also click to collapse the search criteria.
- View details: Click in the **Operation** column to view monitoring task details and alarm records.



Click **View Details** to view the alarm location and handle alarms. (Note: Currently, radars do not support camera connections, so live view and playback functions are unavailable now.)

- Stop task: Click in the **Operation** column to stop the monitoring task. Once stopped, alarms will not be triggered.
- Edit task: Click in the **Operation** column to edit the monitoring task.
- Delete task: Click in the **Operation** column or select task(s), and then click **Delete** above the list.

25 Parking Management

Go to **Park Application** > **Parking Mgt**.

The basic parking management services cater to parking scenarios **without parking fees**, such as corporate campuses, industrial sites, communities, and schools. It is designed for parking lot managers and staff, providing vehicle access management, as well as the search and analysis of vehicle flow and violation data, offering an intelligent parking management system and visual data management platform.

Key Functions:

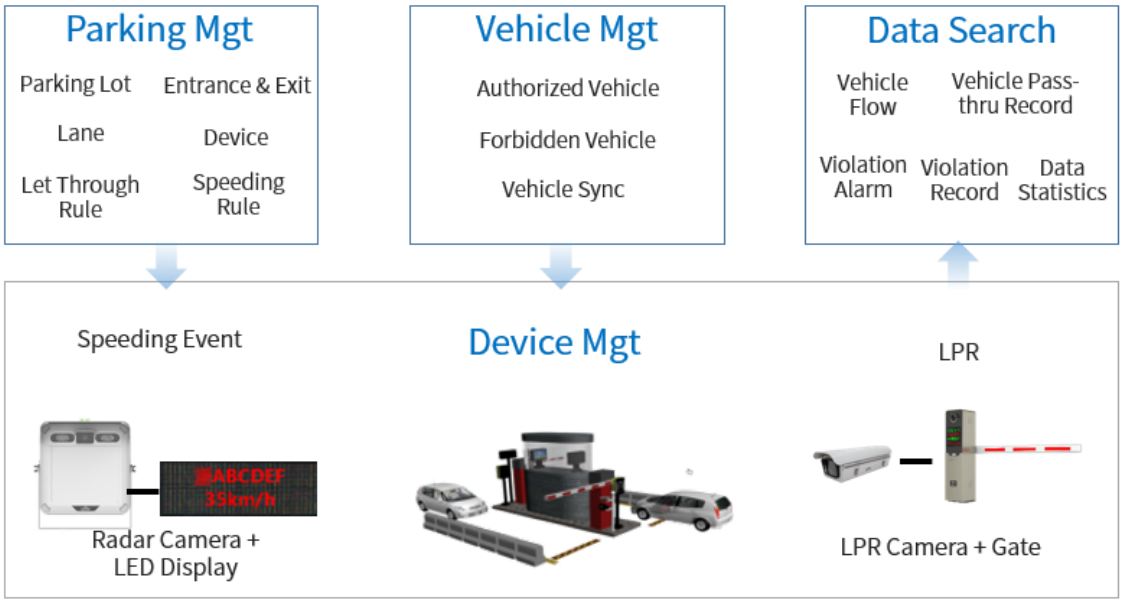
- Parking lot management: Manage parking lots and associated LPR cameras (for entrance/exit) + gates and radar cameras + LED displays, providing online configuration and remote control of parking lot devices.

Note:
Gates and LED displays do not need to be manually added to the platform.

- Gates are physically connected to LPR cameras (for entrance/exit), allowing for gate control through vehicle recognition. They are generally deployed at parking lot entrances and exits.
- LED displays are physically connected to radar cameras and display vehicle information when speeding is detected. They are generally deployed on campus roads with speed limits.

- Vehicle management: Add and manage information for authorized and forbidden vehicles. The system also allows for configuring validity periods and adding speeding vehicles to the forbidden vehicle list, ensuring effective vehicle permission management.
- Data search, analysis, and statistics: Provides vehicle flow statistics, pass-thru violation vehicle data, and violation alarms, offering insights into vehicle trends and supporting parking lot management.

Note:
Violation vehicle data can be viewed on related pages such as in Smart Live View > Vehicle Application, Comprehensive Search > Motor Vehicle Search, and Alarm Center.



25.1 Parking Lot Management

Before using this function, you must first add parking lots to the system. You can also add sub-parking lots (e.g., a main parking lot is divided to surface and underground sub-lots). When adding a parking lot, you need to provide detailed information about the parking spaces in both the main and sub-lots. If vehicles are already parked during setup, the number of available parking spaces should reflect the actual situation.

Once a parking lot is added, you can add entrances & exits and lanes, as well as bind cameras.
Up to 8 parking lots (1 main lot, 7 sub lots) and 16 entrances & exits are allowed. Each entrance & exit can have 2 lanes.

Note:
The number of parking spaces and let through rules for the main and sub-lots are independent.

25.1.1 Add Parking Lot

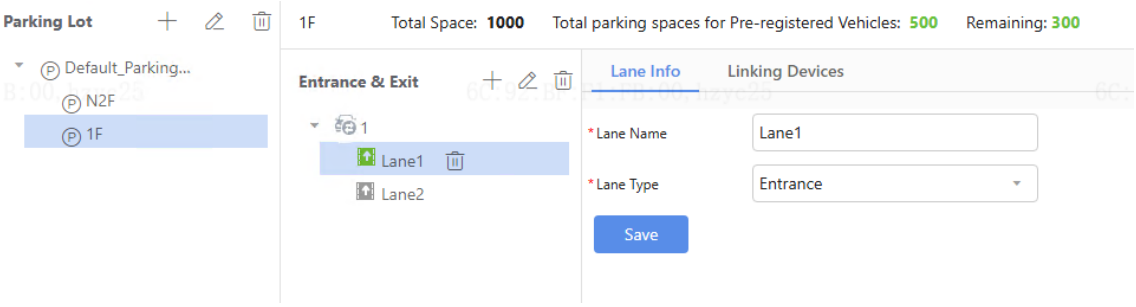
Prerequisites

Entrance & exit devices have been added in Device Management > Frontend Device > Private Device.

- For LPR cameras, select **LPR** as the device type.
- For radar cameras, select **Radar Vision** as the device type.

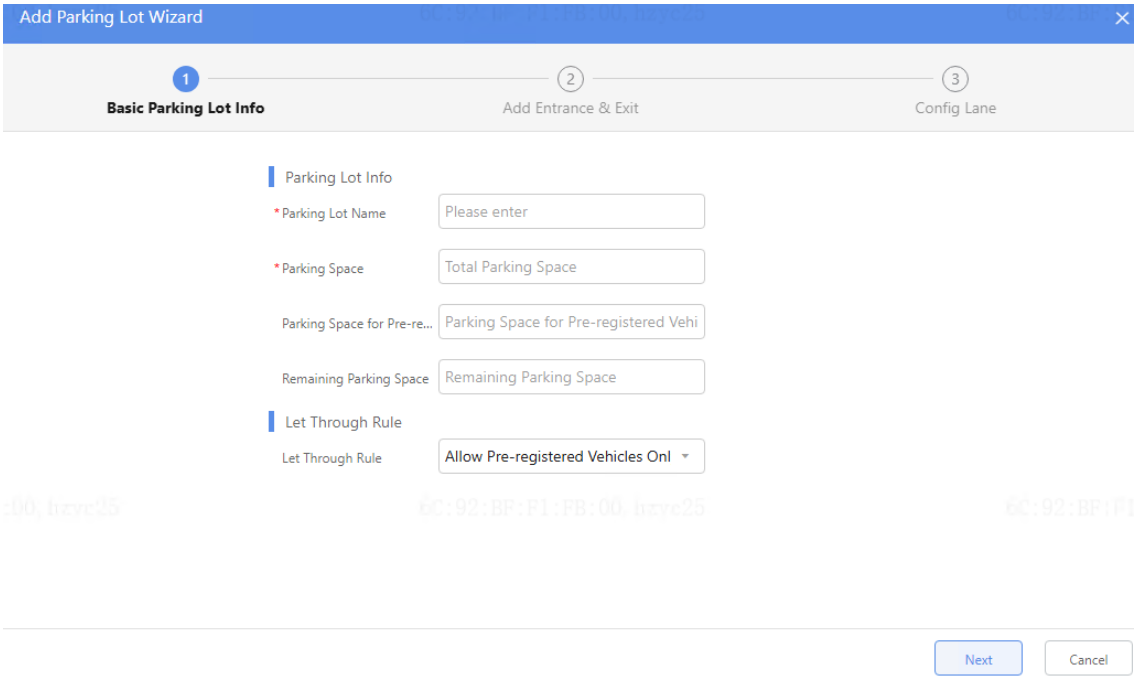
Add Parking Lot

1. Go to **Parking Mgt** > **Parking Lot Management**.



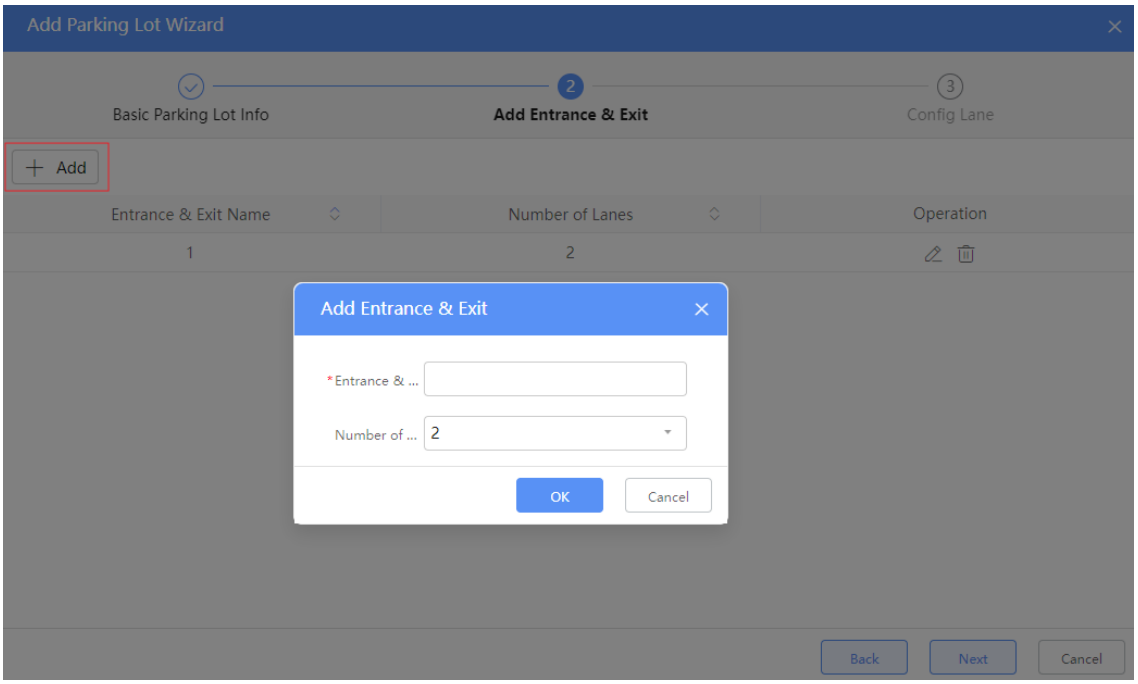
2. Click ＋ in the parking lot list.

3. Fill in the basic information for the parking lot.



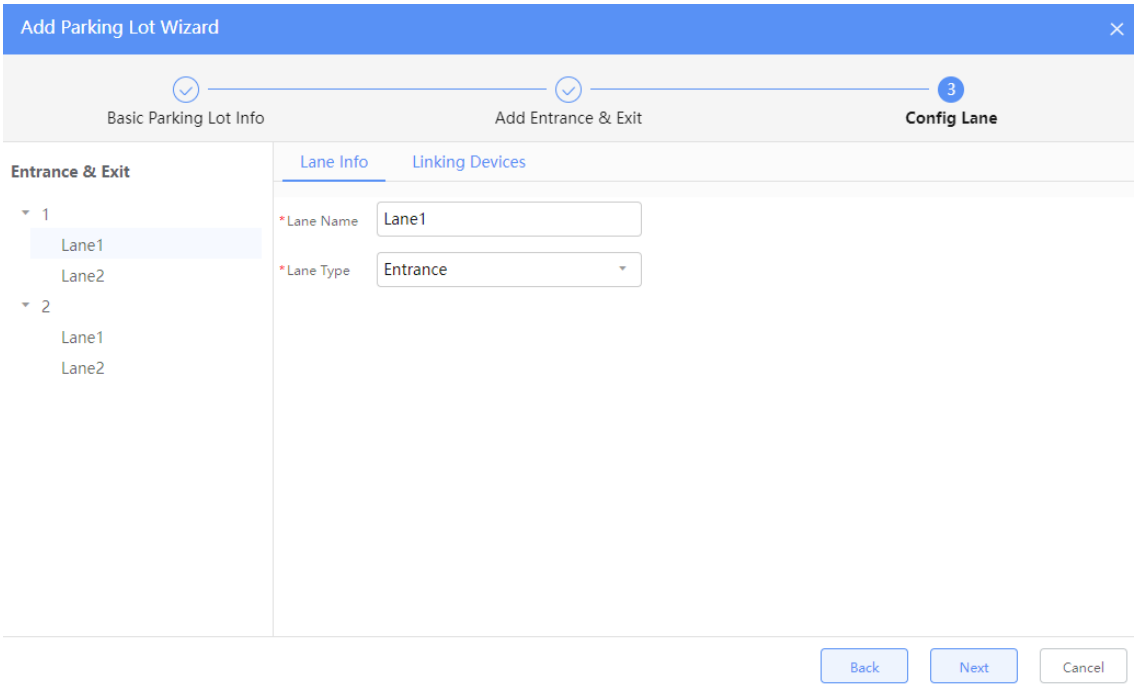
Item	Description
Parking Lot Name	Required. Enter a custom name.
Parking Space	Required. Enter the actual number of parking spaces.
Parking Space Count for Authorized Vehicles	Enter the actual number of parking spaces for authorized vehicles.
Remaining Parking Space	The current number of idle parking spaces. If there are vehicles already present in the parking lot at the start, the remaining number of parking spaces must match the actual count.
Let Through Rule	• Rule 1: Only authorized vehicles are allowed entry; forbidden vehicles and unlisted vehicles are denied entry. • Rule 2: Forbidden vehicles are denied entry; authorized vehicles and unlisted vehicles are allowed entry.

4. Add entrance & exit.



Item	Description
Entrance & Exit Name	Required. Enter a custom name.
Number of Lanes	Choose 1 or 2, based on the actual number of lanes.

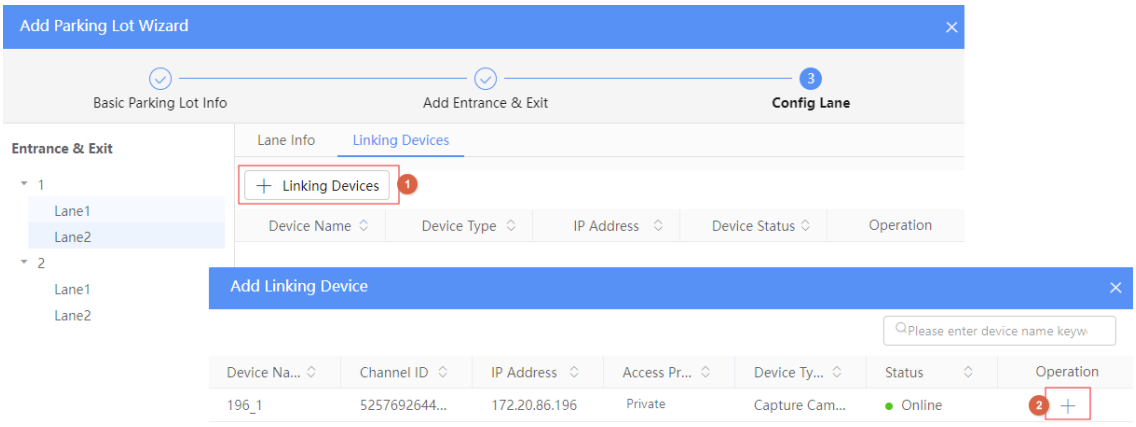
5. Configure the lane information.



Item	Description
Lane Name	Enter a custom lane name.
Lane Type	Choose **Entrance** or **Exit** as needed.

6. Link devices to the lane.
On the **Linking Devices** tab, click **Linking Devices**, and then select device(s) to link.

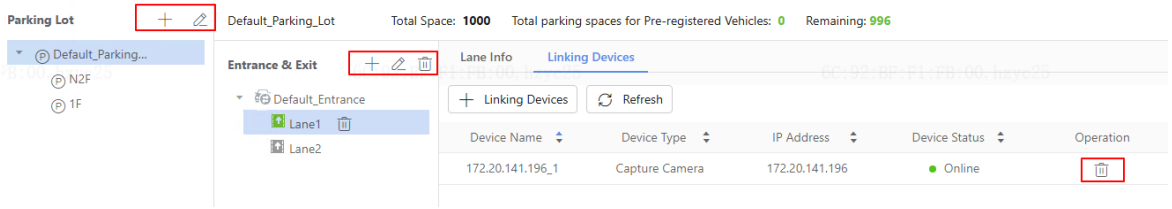
Note:
Only LPR cameras can be selected. Cameras are added in **Device Management > Frontend Device > Private Device**.



7. Click **Save**.

Manage Parking Lot

Click (or) to edit or delete parking lots, entrances & exits, lanes, and linked devices.



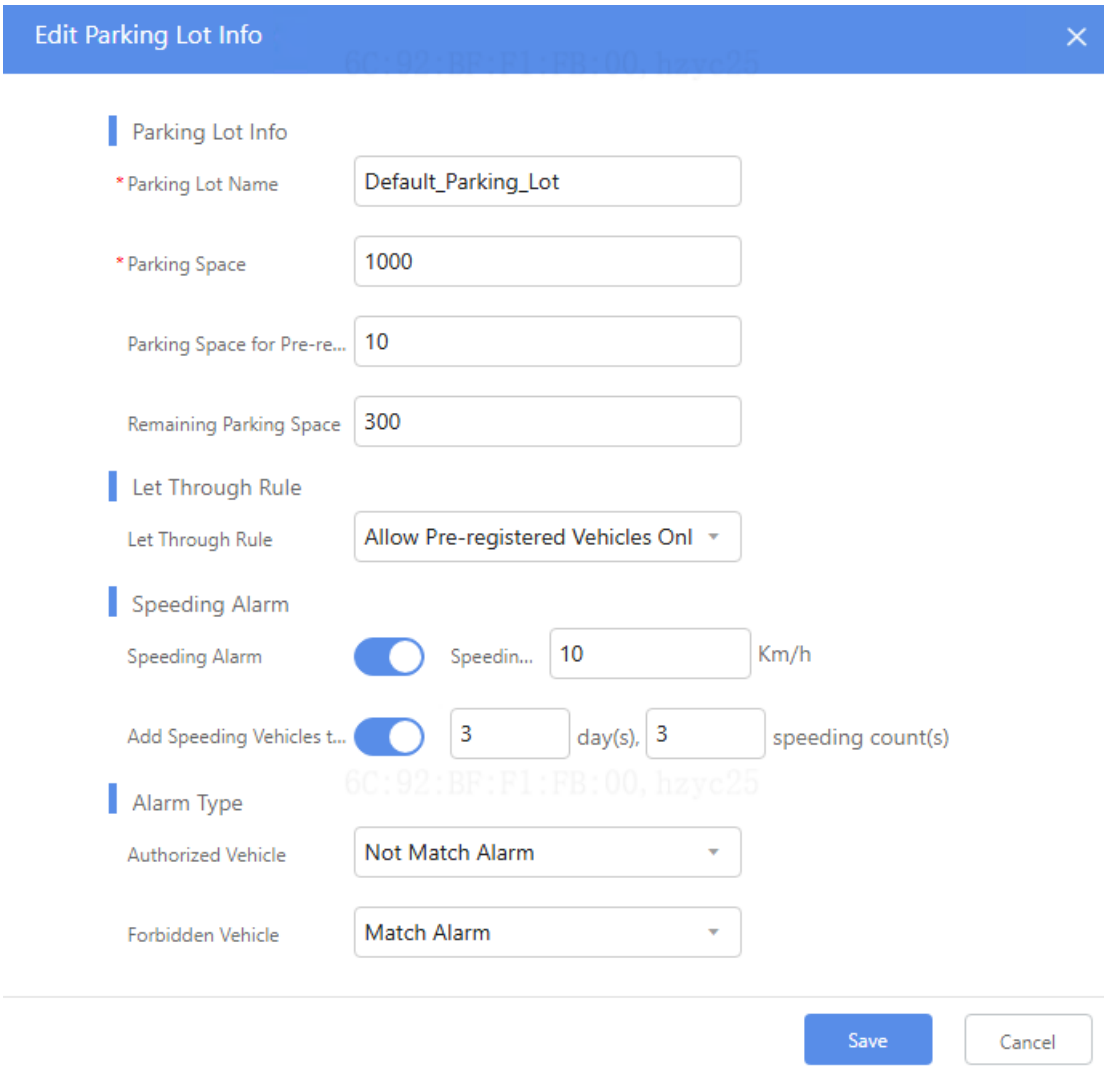
25.1.2 Configure Alarm Rules

- Speeding Alarm: Based on the speed detection capabilities of radar cameras, you can configure speeding alarm rules to receive speeding alarms and deny access to speeding vehicles.
- Match/Not Match Alarm: The system supports setting match and not match alarms for authorized and forbidden vehicles. It performs a license plate comparison between the vehicles captured by the camera and the registered vehicles. If the license plates match, it reports a match alarm; otherwise, it reports a not match alarm.

Note:
Alarm rules should be configured for the main parking lot and will apply to all LPR cameras and radar vision cameras added to the platform.

Steps

1. Select the main parking lot and click .



2. Configure speeding alarm rules.

Item	Description
Speeding Alarm	When enabled, set the threshold for speeding alarms (default is 10 km/h, range is 1-300 km/h). An alarm is triggered if a vehicle's speed exceeds the set threshold.
Add Speeding Vehicles to Forbidden Vehicle List	**Note:** This function can be enabled after the speeding alarm is enabled. When enabled, set the frequency threshold, so that when a vehicle exceeds the speed limit M times within N days, it is automatically added to the forbidden vehicle list.

3. Configure match alarms for authorized vehicles, and configure not match alarms for forbidden vehicles. Take authorized vehicle as an example:
   - If set to **Match Alarm**, when the captured vehicle's license plate matches that of an authorized vehicle, a match alarm is reported. This can be used to alert the appearance of authorized vehicles.
   - If set to **Not Match Alarm**, when the captured vehicle is not in the list of authorized vehicles, a not match alarm is reported. This can be used to alert the arrival of unfamiliar vehicles.
   - If set to **Disable**, then the license plate comparison will not be performed, and no alarms will be generated.
4. Click **Save**.

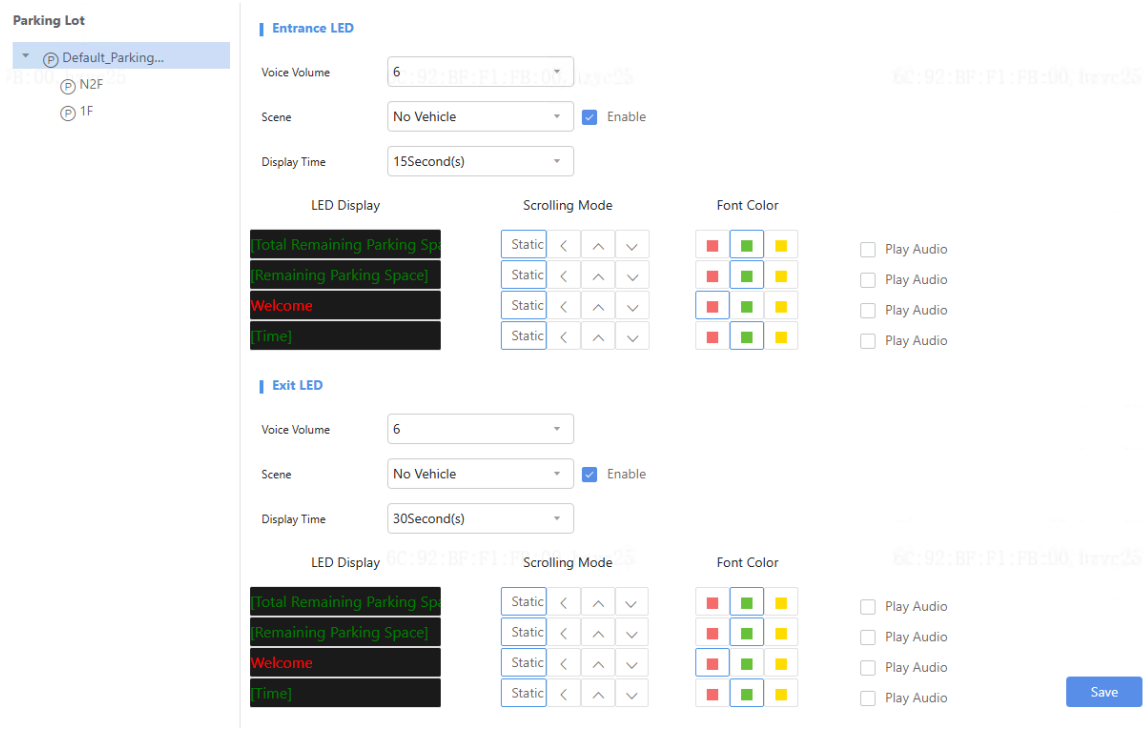
Related Operation

To search vehicle alarms, see Motor Vehicle Search.

25.1.3 LED Config

Go to **Parking Management > Parking Lot > LED Config**.

Configure LED screens at the entrance and exit of the parking lot for different scenes.



Configuration Description

You can configure exit/entrance LED screens to display different contents based on various scenes, including no vehicle, forbidden vehicle, temporary vehicle, and authorized vehicle. After configuring the scenes, you must select **Enable** for the corresponding scene to take effect. The entrance and exit cameras will recognize the vehicle type and link the LED screen to display the corresponding content. After the display time is over, the screen will automatically revert to the "no vehicle" scene.

For the display content in each scene, you can customize the text scrolling mode (static, left, up, down), font color (red, green, yellow), and whether to enable voice messages. After configuring the sound volume, the audio for each scene will be played according to the set volume.

The supported display content is described as follows:

Parameter	Description
Custom	Enter the content to be displayed in the field.
Time	Must be selected. The system time is displayed on this line and is updated in real time.
Remaining Parking Spaces	• If there is no sub parking lot, it displays the current total number of remaining parking spaces is the current parking lot. • If there is a sub parking lot, it displays the number of remaining parking spaces excluding those in the sub parking lot.
Remaining Sub Parking Lot Spaces	• If there is no sub parking lot, this configuration is meaningless. • If a sub parking lot exists, it displays the number of remaining spaces in the sub parking lot.
Total Remaining Parking Spaces	• If there is no sub parking lot, the total remaining spaces are the same as the remaining spaces in this parking lot.

Parameter	Description
	• If a sub parking lot exists, total remaining spaces = remaining parking spaces in the main lot + remaining parking spaces in the sub lot.

25.2 Vehicle Management

Manage vehicle access permissions for parking lots using the authorized and forbidden vehicle lists.

Vehicle Types

- Authorized Vehicle: Vehicles added to the authorized vehicle list are granted access to the parking lot during the specified validity period.
- Forbidden Vehicle: Vehicles added to the forbidden vehicle list are denied access to the parking lot during the specified validity period.
- Temporary Vehicle: A vehicle is considered temporary if it is unlisted on either the authorized or forbidden list, or if is listed but outside the validity period. Access permissions for temporary vehicles are determined by the parking lot's let through rule.

Priority Determination

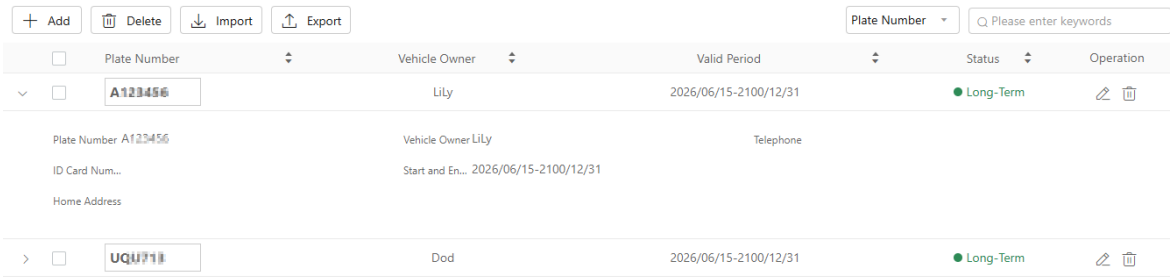
If a vehicle's license plate is on both the authorized and forbidden lists, and is within the validity period for both lists, the vehicle will be prioritized as a forbidden vehicle.

Effective Scope

Vehicle lists are applied uniformly across all parking lots.

25.2.1 Authorized Vehicle

Add authorized vehicle information, including vehicle information, owner information, authorized validity period, etc.



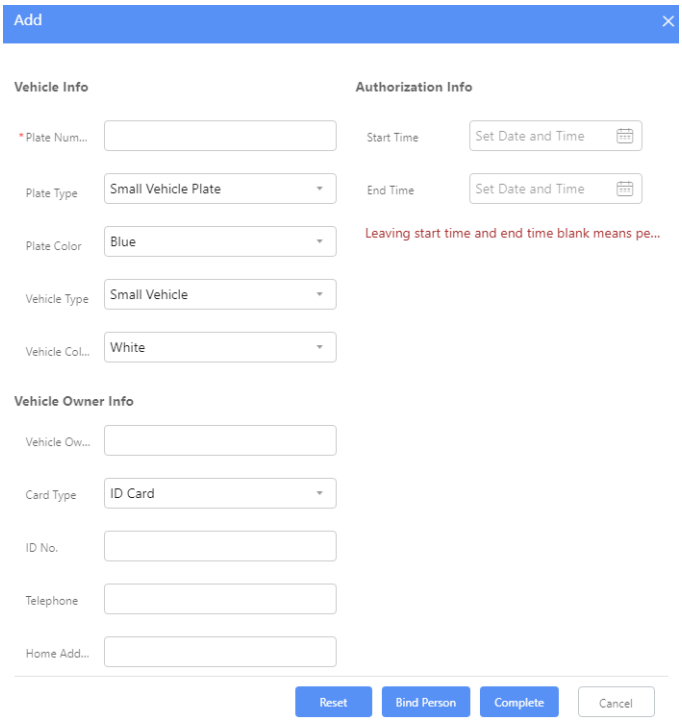
Note:
The authorized vehicle list synchronously displays vehicles associated with Person/Visitor.

Add Authorized Vehicle

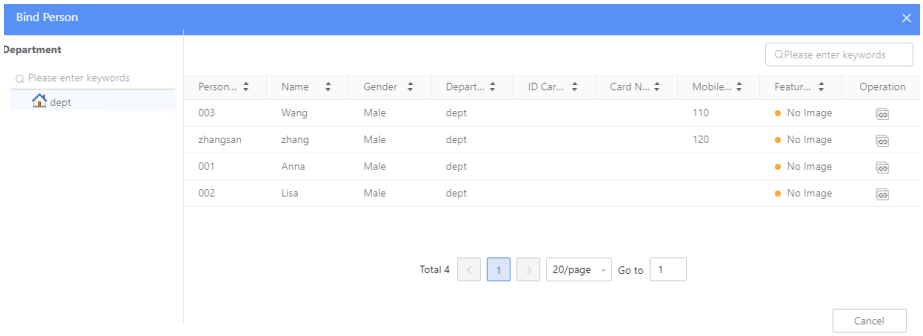
You can add authorized vehicles one by one or in batches.

Add one by one

1. Click **Add**.



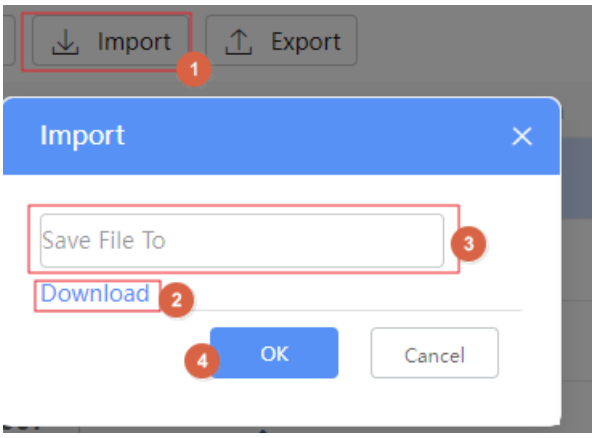
2. Complete the vehicle information.

Vehicle Info	Plate number is required.
Vehicle Owner Info	You can enter the information manually or click **Bind Person** to select a person from department to bind.  **Note:** After binding here, the vehicle will be accordingly added to the Person's vehicle list.
Authorization Info	Vehicles will only have access during the authorized validity period. Leaving the start time and end time blank means permanently valid.

3. Click **Complete** to save.

Batch import

1. Click **Import**.



2. Prepare a template.
   (1) Click **Download** to download the import template.
   (2) Fill in the template with vehicle information.
3. Import the template.
   (1) In the **Import** window, click the text box, and select the modified template from local.
   (2) Click **OK**.

Other Operations

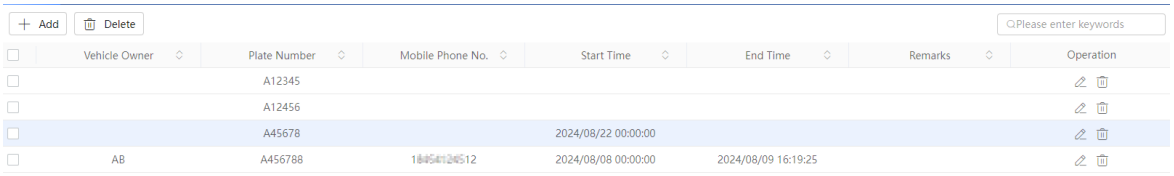
- Search: Select a search criteria in the upper-right corner and enter keywords to search for vehicles.
- Edit: Click for the vehicle to edit the vehicle information, see Add Authorized Vehicle.

  Note:
  If the vehicle is already associated with a person/visitor:
  - You cannot modify the vehicle's plate number, owner name, or authorized validity period.
  - You click **Reset** to unbind the person-vehicle association. The vehicle will also be removed from the Person's/Visitor's vehicle list.
  - After resetting, you can also rebind the vehicle to another person.
- Delete: Click for the vehicle, or select vehicle(s) to delete and click **Delete**.

  Note:
  If the deleted vehicle is already associated with a person/visitor, it will also be removed from the Person's/Visitor's vehicle list.
- Export: Select vehicle(s) and click **Export** to export the vehicle information into a file.

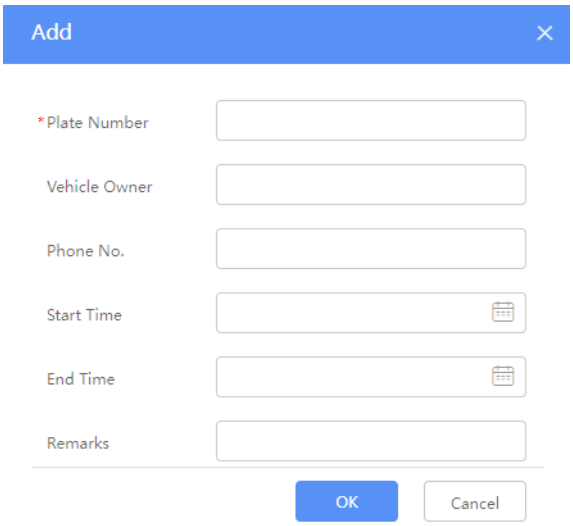
25.2.2 Forbidden Vehicle

Add forbidden vehicle information, including plate number, owner information, prohibited entry time periods, etc.



Add Forbidden Vehicle

1. Click **Add**.
2. Enter the required license plate information and other details as needed.



Note:
Vehicles will be denied access during the specified time period. Leaving start time and time blank means permanently prohibited.

3. Click **OK**.

Other Operations

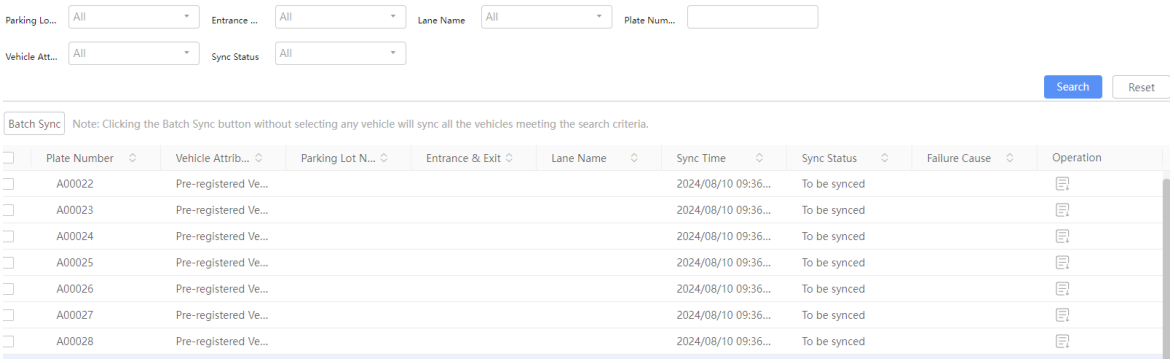
- Search: Enter the license plate keywords in the upper-right corner to search for a specific vehicle.
- Edit: Click for the vehicle to edit the vehicle information.
- Delete: Click for the vehicle, or select vehicle(s) to delete and click **Delete**.

25.2.3 Vehicle Data Sync

You can sync authorized and forbidden vehicle information to parking lot devices.

The list displays the matching relationship between all vehicles and parking lot lanes. You can search for vehicles using criteria such as parking lot name, entrance & exit, lane name, plate number, vehicle attribute, and sync status.

- Sync one by one: Click for the vehicle to sync its information to the corresponding lane's device.
- Batch sync: Select vehicle(s) and click **Batch Sync** to sync the information of the selected vehicles to the devices. If you click **Batch Sync** without selecting any vehicles, all vehicles meeting the search criteria will be synced.

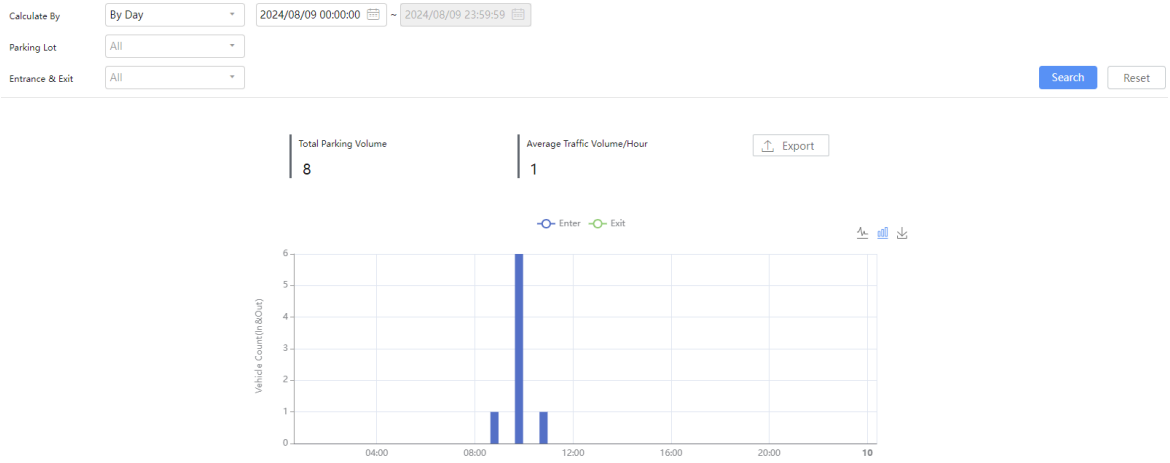


25.3 Vehicle Volume

You can search for parking lot vehicle flow statistics on the **Vehicle Flow** page.

Search criteria:

- Statistical unit: By Day/Month/Year (default is the current day/month/year; you can specify a different day/month/year)
- Parking Lot
- Entrance & Exit



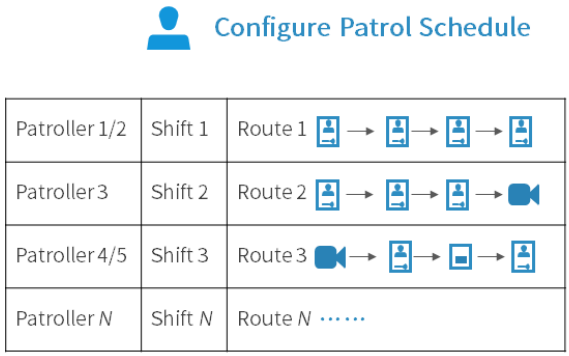
Search Results:

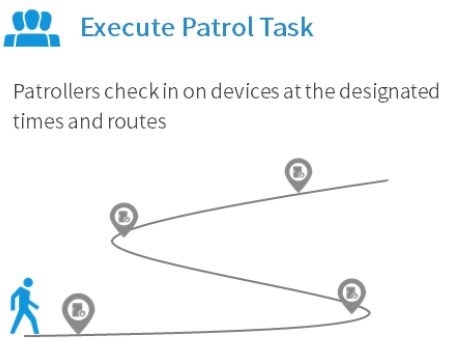
Total Parking Volume	The total number of vehicles that meet the search criteria, including both vehicles entered and exited.
Average Traffic Volume	• By Day: Average vehicle flow per hour = (Total daily vehicles entered + Total daily vehicles exited) / 24 hours. • By Month: Average vehicle flow per day = (Total monthly vehicles entered + Total monthly vehicles exited) / 30 days. • By Year: Average vehicle flow per month = (Total yearly vehicles entered + Total yearly vehicles exited) / 12 months.
	Click to display the data as a line chart.
	Click to display the data as a bar chart.
	Click to save the current chart as an image file.
Export	Click **Export** to download the detailed record search data as a vehicleFlowList.csv file locally.

26 Electronic Patrol

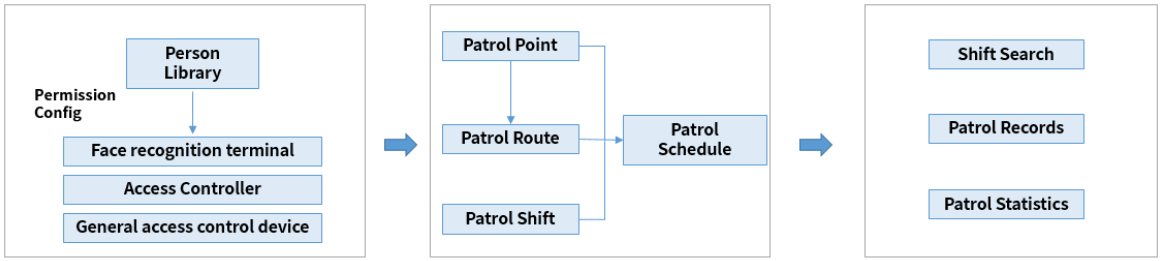
This function is mainly used for campus area scenes where security guards patrol the premise according to the patrol schedule.

You can configure patrol schedules on the platform, specify personnel to conduct patrols according to the schedule and designated routes. After patrollers check in at patrol points through face recognition terminals/general access control devices/access controllers, the system generates patrol records accordingly to keep track of patrol tasks.





The general patrol process is as shown below:



Prerequisite

- Patrollers have been added in the person library. See Personnel Management .
- Device permissions have been assigned to patrollers. See the descriptions below.
  1. Add face recognition terminals, general access control devices, and access controllers. See **Device Management** > **Frontend Device** > Private Device.
  2. Configure device permissions for persons in the personnel library. See **Access&Attendance** > Access Control Permission.

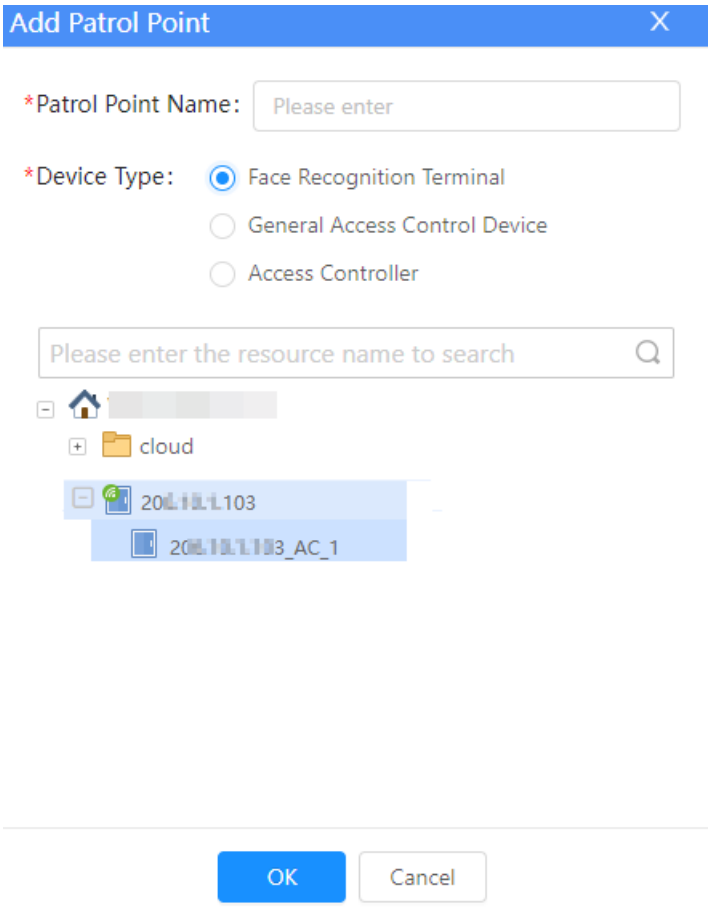
26.1 Patrol Configuration

26.1.1 Patrol Point

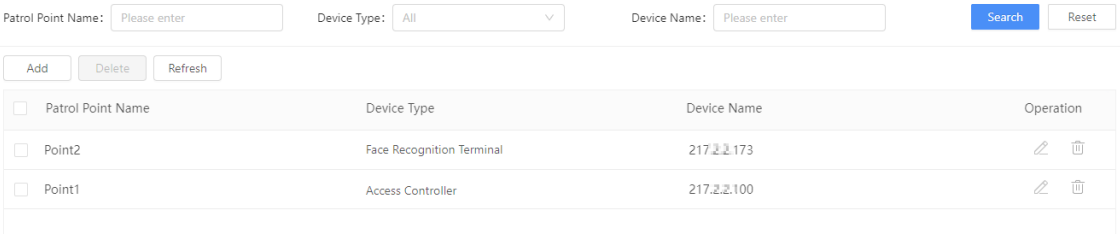
Add face recognition terminals, general access control devices, and access controllers as patrol points. Patrollers need to check in on the specified devices to complete the patrol schedule.

Add Patrol Point

1. Click **Add** to add a patrol point.
2. Enter a name for the patrol point, choose a device type, and then select a device from the list.



3. Click **OK**. The patrol point is added.
4. Repeat the above steps to add all the needed patrol points.



Manage Patrol Point

You can search, edit, or delete patrol points.

- Edit: Click to rename a patrol point (cannot change the patrol device).
- Delete: Click to delete a patrol point; or select multiple patrol points and then click **Delete** on the top to delete the selected patrol points.
- Search: Set search criteria such as patrol point name, device type, device name, and then click **Search**.

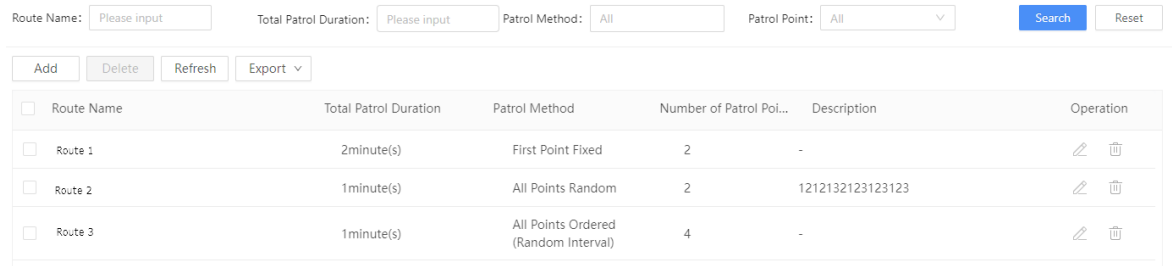
26.1.2 Patrol Route

A patrol route includes patrol points arranged in certain order at certain time interval for patrollers to follow when conducting patrols.

- A patrol route can include face recognition terminals, general access control devices, and access controllers.
- In a patrol route, one device can be added only once that is to say, one device cannot be patrolled multiple times in a patrol route.
- The following patrol methods are available:

Patrol Method	Description
All Random	Patrollers are allowed to patrol in random order, so long as all the patrol points are covered.
First Point Fixed	Except for the first patrol point, other points allow check-in in any order.
First and Last Points Fixed	Except for the first and last patrol points, other points allow check-in in any order.
All Points Ordered (Random Interval)	The patrol must be conducted in the order specified by the patrol list, with no specific time interval required between adjacent patrol points.
All Points Ordered (Fixed Interval)	The patrol must be conducted in the order specified by the patrol list, with the same time interval between adjacent patrol points.
All Points Ordered (Custom Interval)	The patrol must be conducted in the order specified by the patrol list, with the user-set time interval between adjacent patrol points.

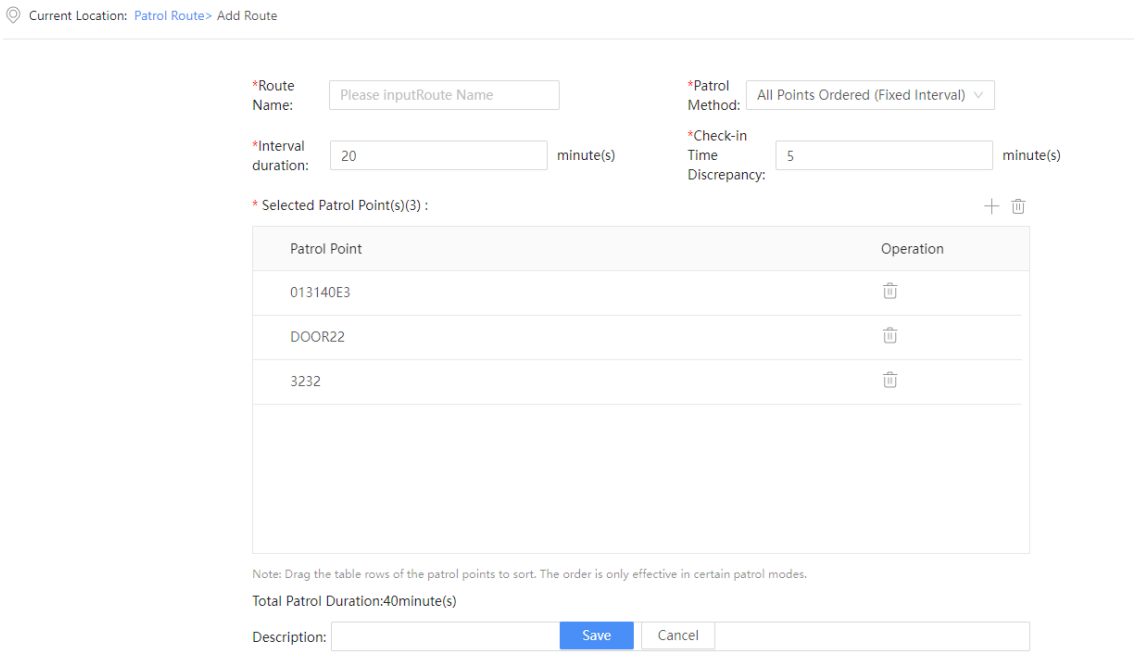
Figure 26-1: Patrol Route



Add Patrol Route

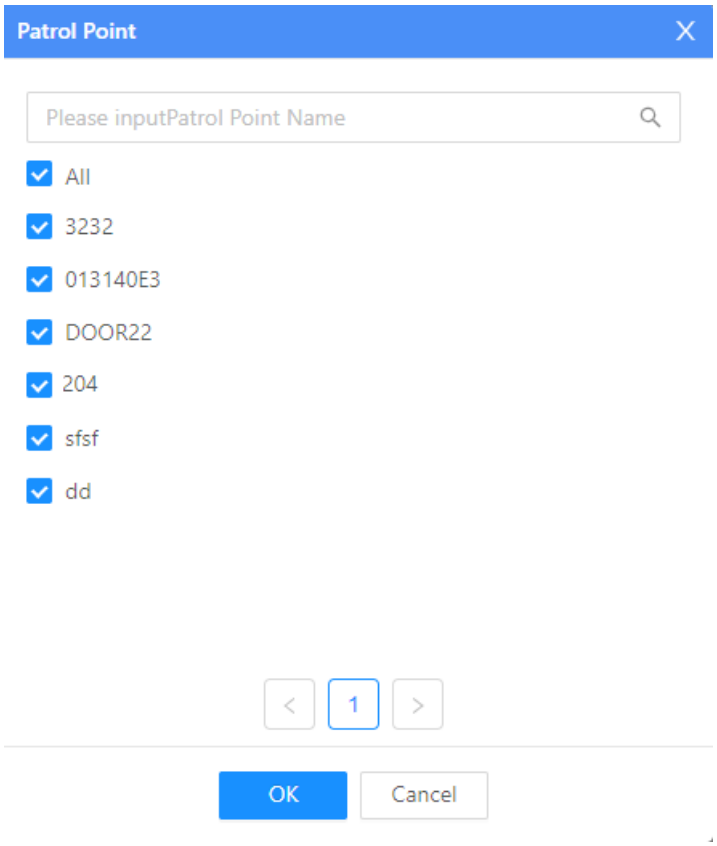
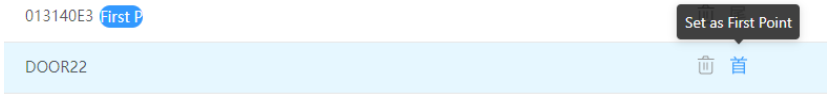
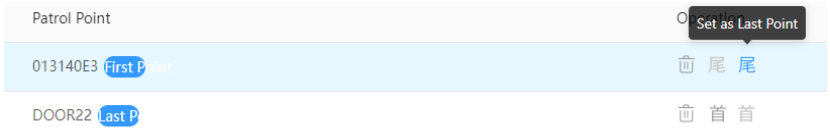
1. Click **Add**. A page as shown below appears.

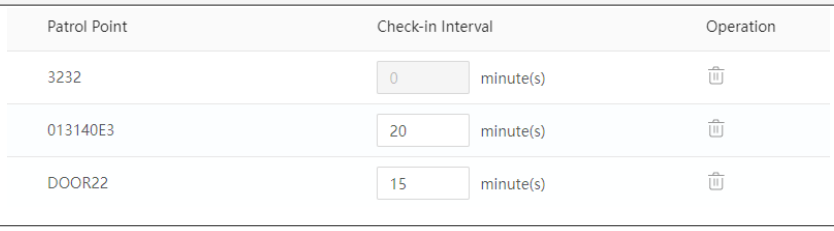
   Figure 26-2: Patrol Route



2. Set the patrol route. The parameters are described below.

Parameter	Description
Route Name	Enter a name for the route.
Patrol Method	Choose a patrol method. See patrol methods.
Total Patrol Duration	Required for the following patrol methods: All Random, First Point Fixed, First and Last Points Fixed, and All Points Ordered (Random Interval)

Parameter	Description
	Set the total duration of the patrol (maximum duration is 300 minutes).
Time Interval	Required for All Points Ordered (Fixed Interval). Set the time interval between two patrol points.
Time Discrepancy Range	Set the allowable range of patrol time deviation, within which it is considered normal patrol; otherwise, it is considered unscheduled patrol.
Patrol Point	Click + in the upper-right corner of the patrol list to add patrol points.  You can perform the following actions to a patrol list: • Click in the upper-right corner to clear all the patrol points. • Click for a patrol point to delete it. • Drag a patrol point to change its sequence in the list (only available to certain patrol methods). • First point fixed: You must set the first point. Click the corresponding Set as First Point. The patrol point appears on the top of the list.  • First and Last Points Fixed: You must set the first point and the last point separately. Click the corresponding Set as First Point. The patrol point appears on the top of the list. Click the corresponding Set as Last Point. The patrol point appears on the bottom of the list.  • All Points Ordered (Custom Interval): You need to set the time interval between each patrol point and the previous patrol point.

Parameter	Description
	
Description	Input a description of the patrol route.

3. Click **OK**.

Manage Patrol Routes

You can search, edit, delete, or export patrol routes.

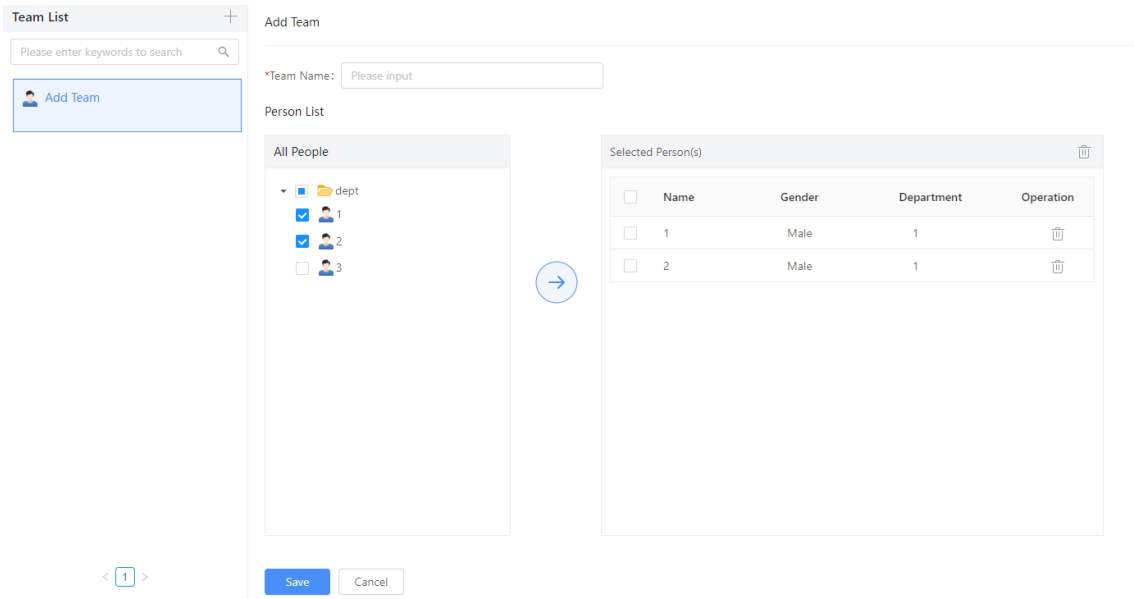
- Search: Set search criteria such as route name, total patrol duration, patrol method, and then click **Search**.
- Edit: Click to edit a patrol route.
- Delete: Click to delete a patrol route; or select multiple patrol routes and then click **Delete** on the top to delete the selected routes.
- Export: Select multiple patrol routes, and then click **Export** > **Export Selected** or **Export All** to export the routes to a form.

26.1.3 Patrol Team

Assign patrollers to different teams so you can assign shifts when making a patrol schedule.

Create Patrol Team

1. Click in the team list to create a team.
2. Enter the team name, select patrollers, and then click to add them to the team.



3. Click **Save**.

Manage Patrol Team

View team members, edit teams, or delete unneeded teams.

Click in the upper-right corner to toggle between list or card mode.

Figure 26-3: Patrol Team-List Mode

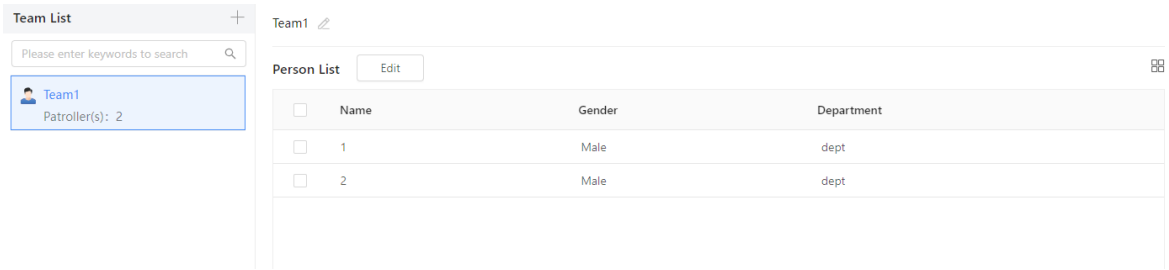
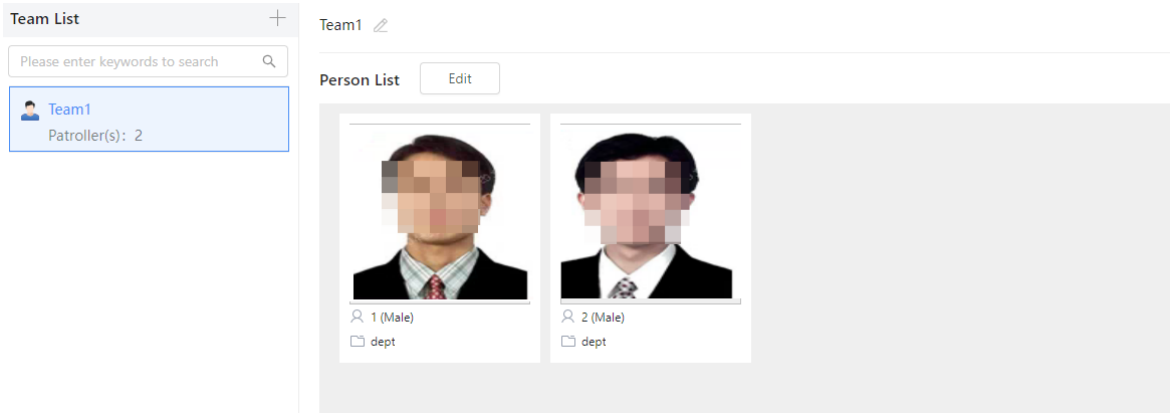


Figure 26-4: Patrol Team-Card Mode



- View: Select a team in the team list to view the team members on the right.
- Edit: Click **Edit** on the right side to rename the team, add or remove team members.
- Delete: Hover over the team name and then click **Delete** to delete the team.

26.1.4 Patrol Schedule

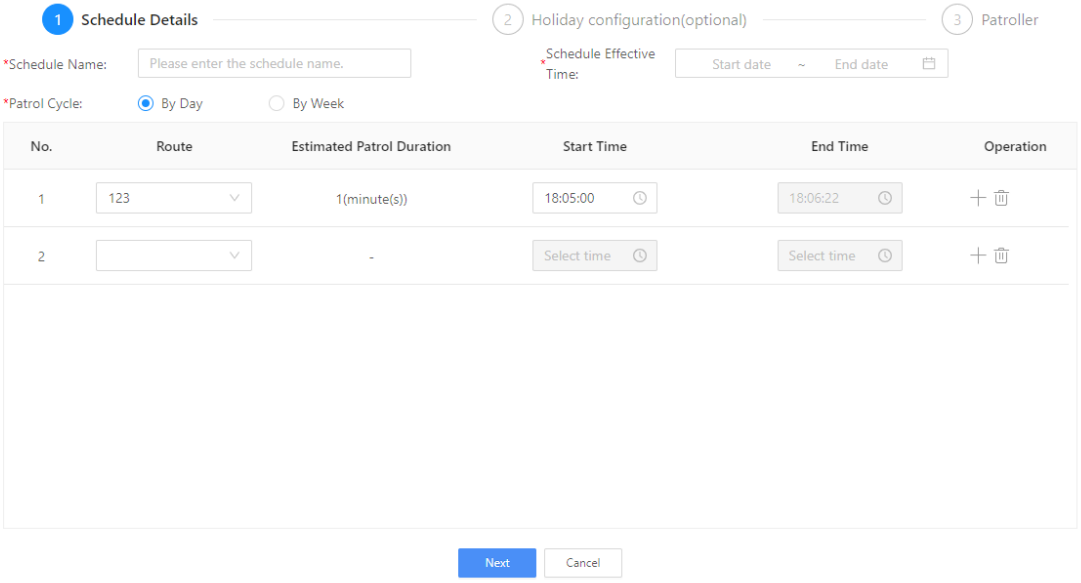
Configure patrol schedules so patrollers can patrol the specified routes according to the set shifts.

Figure 26-5: Patrol Schedule

Add Patrol Schedule

1. Click **Add**. A page as shown below appears.

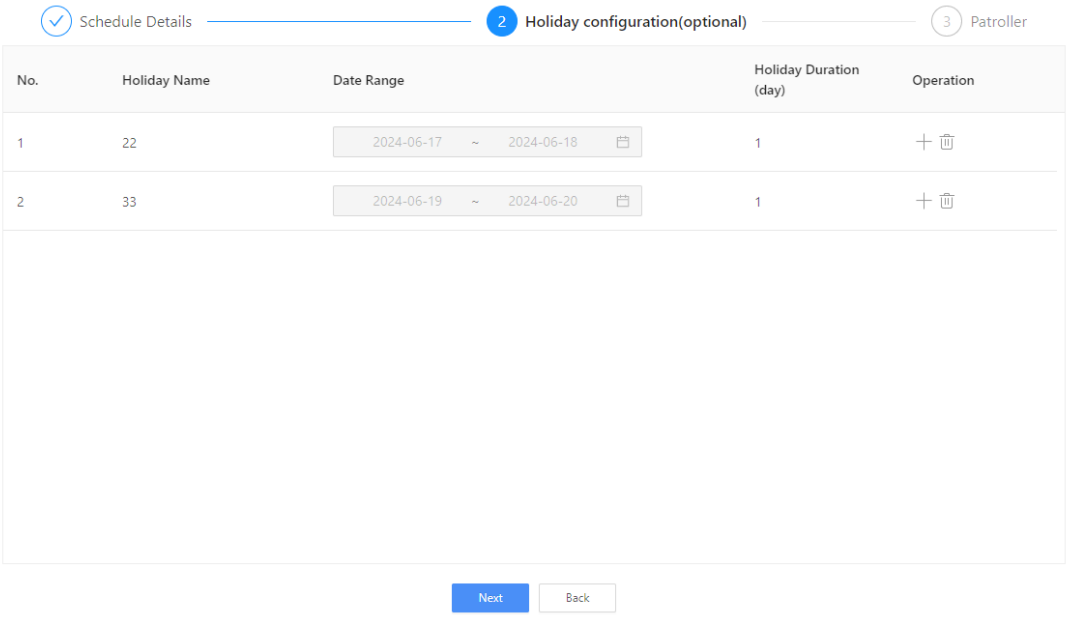
Figure 26-6: Add



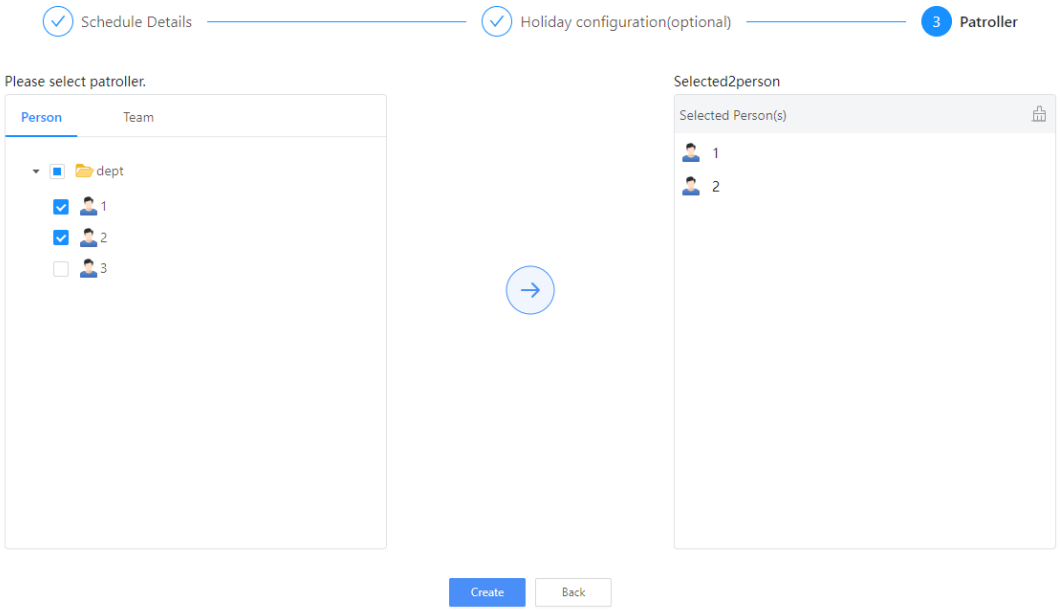
2. Configure the patrol schedule. See parameter descriptions below.

Parameter	Description
Schedule Name	Enter a name for the patrol schedule.
Schedule Effective Time	Configure the time during which the schedule is effective. The schedule needs to be carried out only during the effective time.
Patrol Cycle	• By Day: Set a patrol schedule for a day, and the schedule will be repeated every subsequent day. • By Week: Set a patrol schedule for a week, and the schedule will be repeated every subsequent week.
Daily Patrol Schedule	When setting a daily patrol schedule, you need to complete the following in sequence: patrol route, patrol start time (patrol end time will be calculated automatically).

3. (Optional) Configure holiday dates. Set days on which patrol schedules will not be performed. Multiple exception dates are allowed. Click Add, and then select a holiday



4. Click **Next**, select patrollers from the team or from a person library.



5. Click **Create** to complete patrol schedule.

   Note:
   All patrols in the patrol schedule are required to patrol all patrol routes.

Manage Patrol Schedule

Search, edit, or delete patrol schedules.

- Search: Set search criteria including schedule name, patrol route, schedule effective time, patrol cycle (by day or by week), and then click **Search**.
- Edit: Click to edit a schedule.
- Delete: Click to delete a patrol schedule; or select multiple patrol schedules and then click **Delete** on the top to delete the selected schedules.

26.2 Patrol Search

26.2.1 Schedule Search

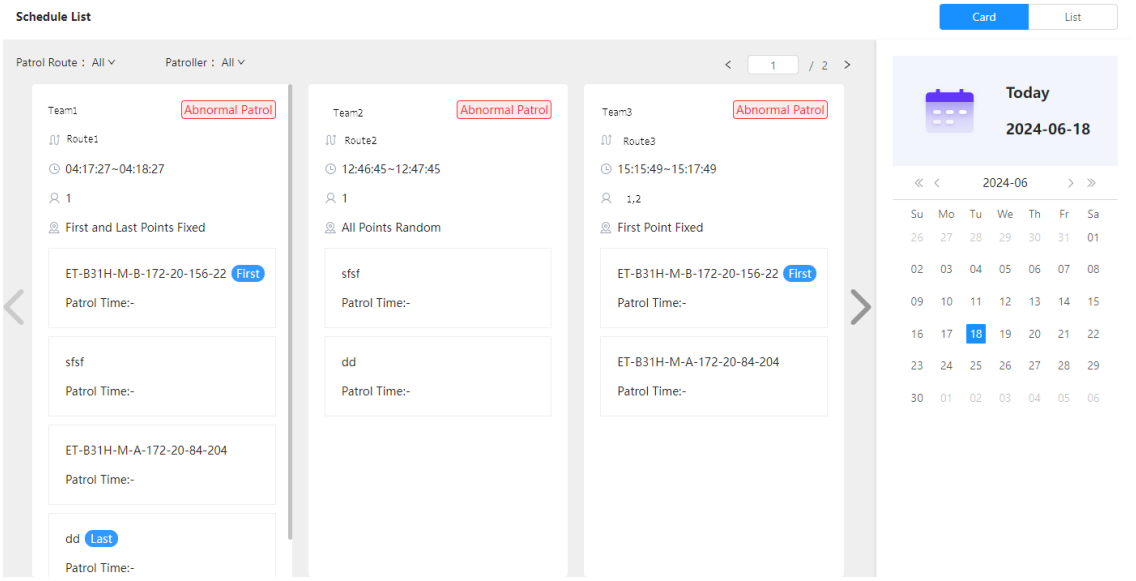
View patrol schedules and their status.

Schedule Records

You can filter schedules by patrol route and patroller.

Schedule records can be displayed in two styles: card and list.

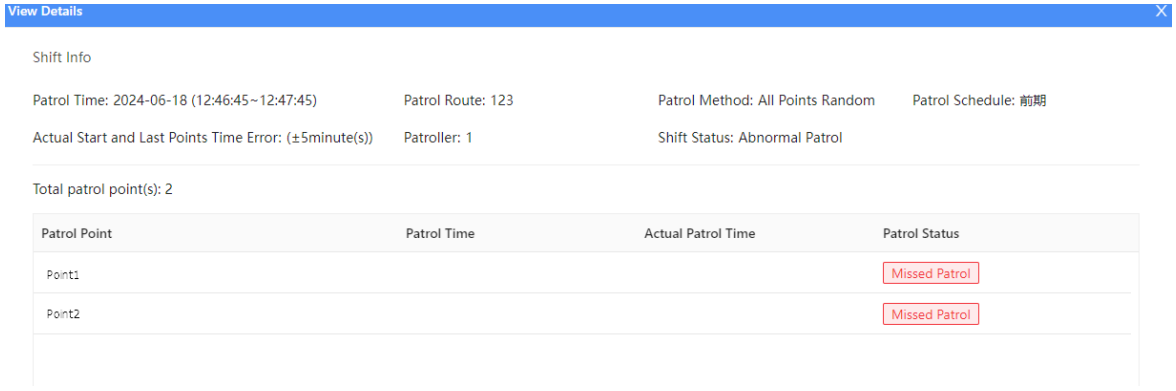
- When displayed as cards, each card represents a patrol shift and displays information about this shift, including patrol route, patrol time, patroller, scheduled check-in time at each patrol point, current patrol status of each patrol point (completed/not patrolled).
  By default, the calendar on the right side shows schedules of the current month. The dates with shifts are marked with a blue dot. The currently selected date is marked with a red dot.
  Click the left or right arrow to view more shifts.



- The following shows shifts displayed as a list.

Shift Details

Click **View Details** in list mode or double-click a card in card mode to view detailed information about a schedule, including shifts, patrol points, and patrol time.



26.2.2 Records Search

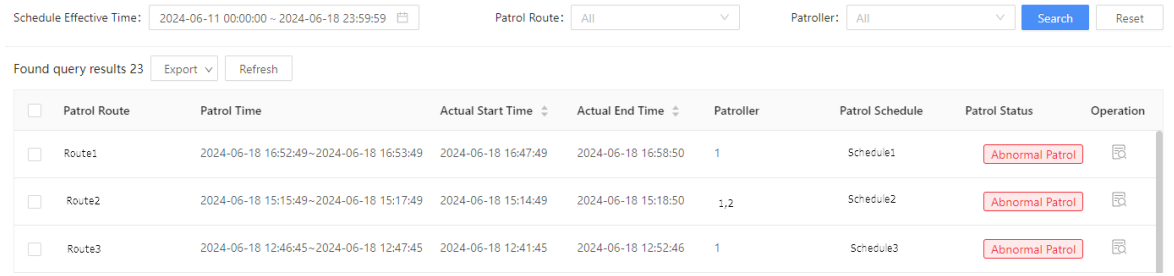
Search patrol records to view the details of a patrol schedule.

Patrol Records

You can search patrol records by criteria such as schedule effective time, patrol route, and patroller.

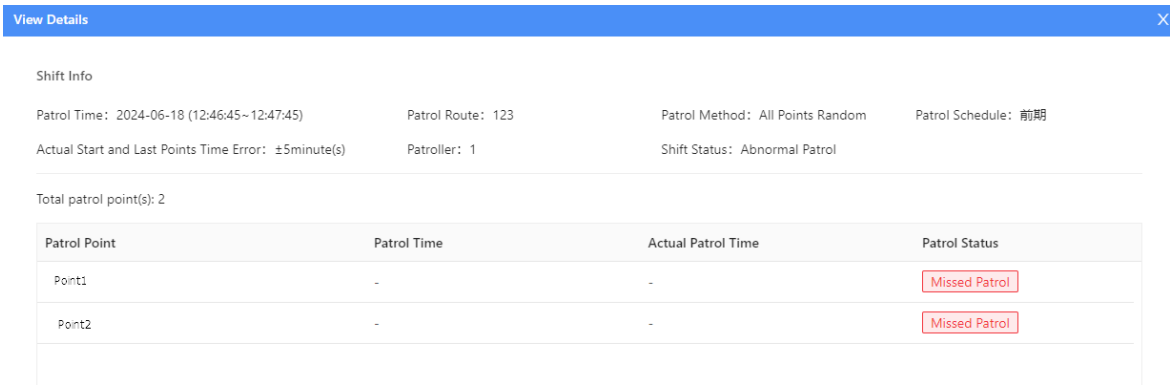
In the list of patrol records, you can view the patrol status of each patroller on each patrol route in the patrol plan. Patrol results are divided into Normal and Abnormal.

Note:
For a patrol route, if any point is abnormal (early patrol / late patrol / missing patrol), the route is abnormal; if every point completes the patrol according to the plan, the route is normal.



Patrol Details

Click to view the details of a patrol route, including shift information, and patrol status of each patrol point.



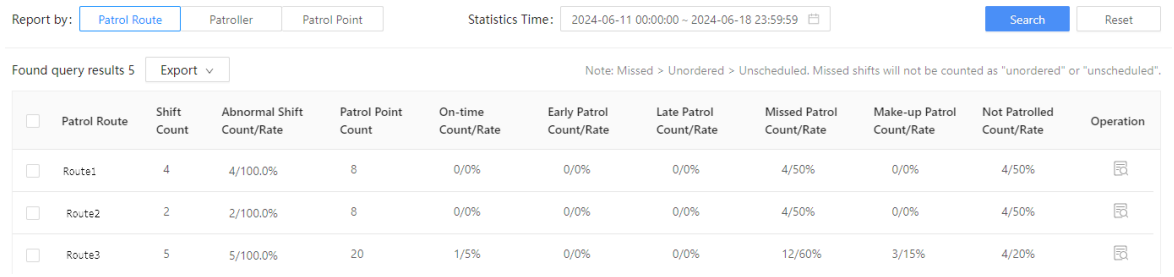
Export Patrol Records

- Export selected: Select patrol records to export, and then choose **Export Selected**. The selected patrol records are exported.
- Export all: Choose **Export All** to export all patrol records.

26.2.3 Patrol Statistics

You can collect patrol statistics from different dimensions, including patrol route, patroller, and patrol point, and set search criteria such as time range and patrol route.

After setting search criteria, click **Search** to view the statistical results.



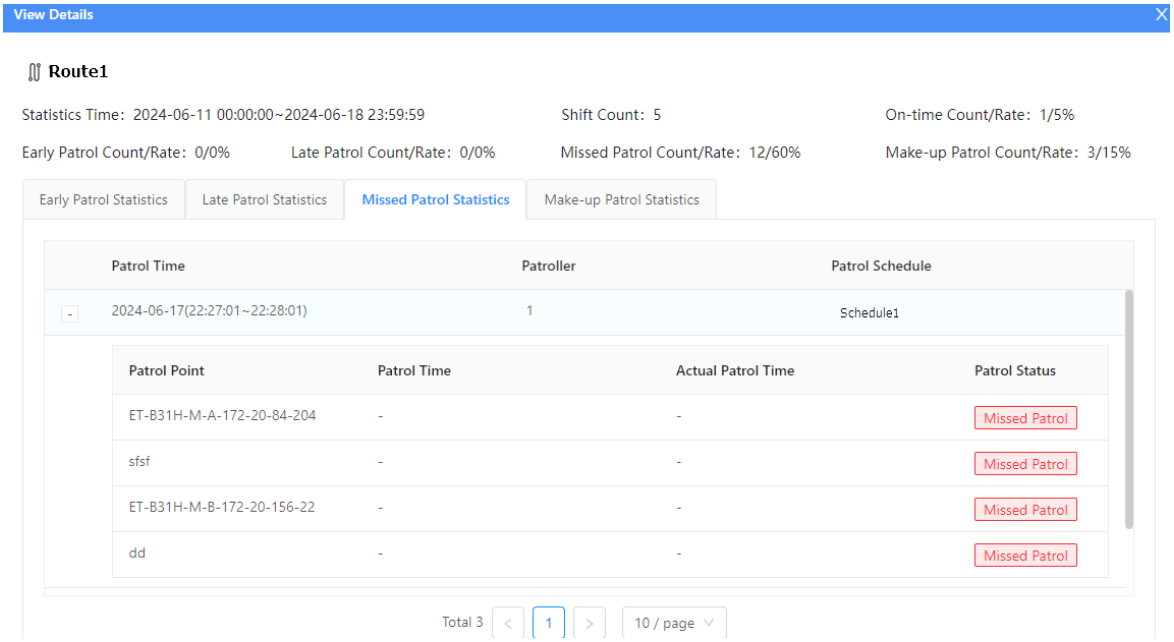
The statistical items include: shift count, on-time patrol count/rate, early patrol count/rate, late patrol count/rate, missed patrol count/rate, make-up patrol count/rate, not patrol count/rate.

Patrol Result	Description of Judgment Rules
Normal	Complete the patrol within the route [start time, end time].
Missed patrol	Not patrol within the route [start time, end time].
Early patrol	In an **all points ordered (fixed interval)** or **all points ordered (custom interval)** route, patrol earlier than the point within the route [start time, end time].
Late patrol	In an **all points ordered (fixed interval)** or **all points ordered (custom interval)** route, patrol later than the point within the route [start time, end time].
Make-up patrol	In an **all points ordered** route, within the route [start time, end time], the latter location has been patrolled and then the former location is patched.

Patrol Result	Description of Judgment Rules
Not patrol	Patrol time has not started and patroller are not on patrol.

View Details

Click to view patrol details and statistics of early patrol, late patrol, missed patrol, and make-up patrol.



Export Patrol Statistics

- Export selected: Select patrol data to export, and then click **Export** > **Export Selected**. The selected data are exported.
- Export all: Click **Export** > **Export All** to export all patrol data.

27 Map Configuration

Go to **Basic Config > Map Configuration**.

E-map is applicable in various scenarios such as campus areas, enterprises, and residential areas. Maps, including flat maps, model maps, and GIS maps, can be bound to areas to display the location of multiple resources and alarm events reported by devices. You can also perform operations on devices and manage resources on the map visually, which provides you with an immerse operating experience.

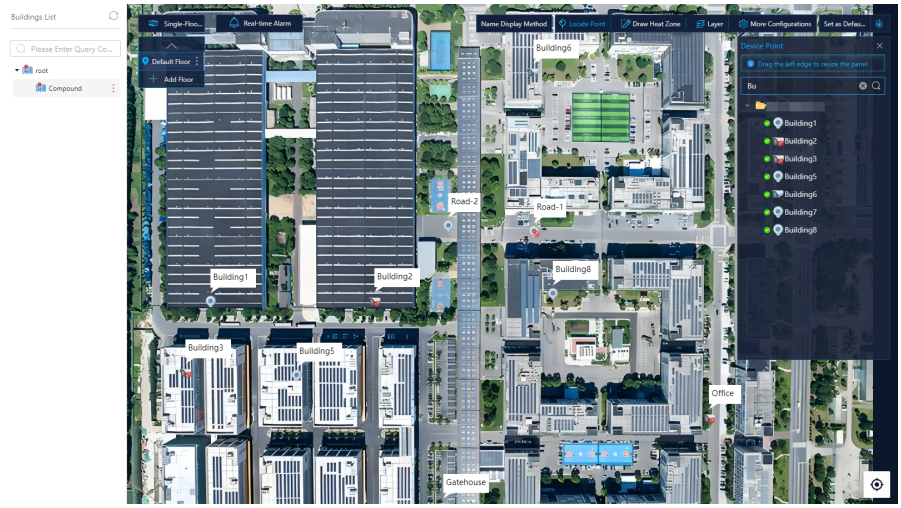
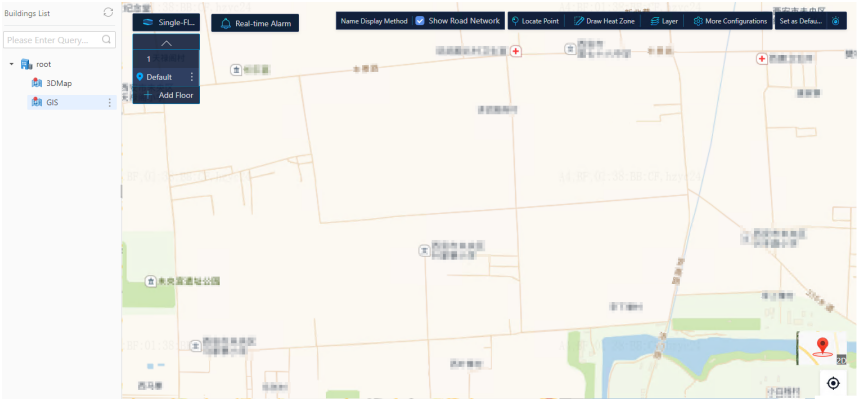
Functions

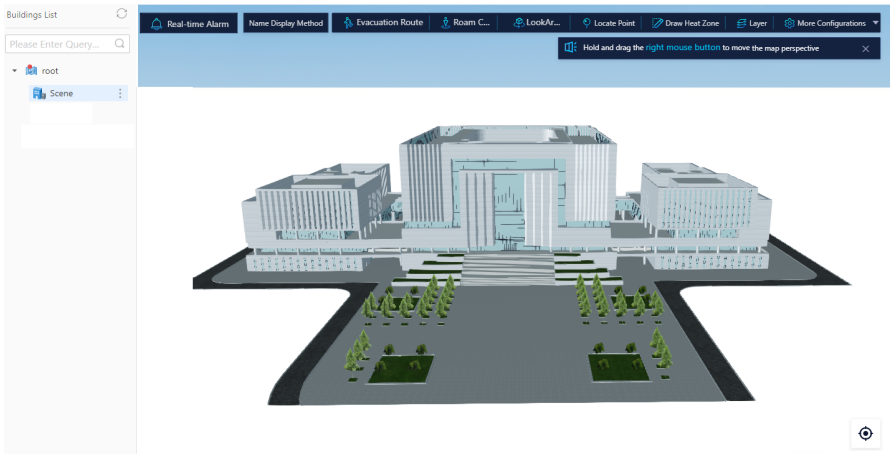
- Map Engine Management: GIS maps and scene maps carry longitude and latitude information and need to be managed through the map engine service. On the map engine management page, users can upload GIS maps and configure scene maps.
- Edit Map: Users can bind maps (including flat map, model map, GIS map, and scene map) with an area, add devices to the map, and draw hot zones.
- Map Application: With the map background, users can view device locations, alarm locations, and trajectories of a person more intuitively.

Configuration

Prepare the maps that you will use. See the table for detailed descriptions.

Flat map	**Flat maps are maps in JPEG, JPG, PNG, and BMP format, such as the floor plan of an area or a room, applicable to small campus areas, shopping malls, etc.** Upload the flat map. See Edit Map-Bind Map.

	Figure 27-1: An example of flat map 
GIS map	**GIS maps are generally map resources released by map manufacturers, such as Google Maps and Baidu Maps, which can present the real ground environment, including administrative regions, buildings, roads, etc., and are suitable for management scenarios in wide regions.** Follow the steps to upload a GIS map: 1. Upload a GIS map file in gmdb format. See Map Engine Management -Add Map. 2. Bind a GIS map with an area. See Edit Map-Bind Map. **Figure 27-2: An example of GIS map** 
Model map	**A model map is a 3D map model in 3dtiles or gltf format. It is usually the internal space of a floor, which can reflect the 3d space layout of buildings. Model maps are suitable for the internal scenes of office buildings and residential buildings.** Upload model map. See Edit Map-Bind Map. **Figure 27-3: An example of model map**

Scene map	**A scene map is a model in unw format. A model is one or more complete buildings, including multiple floors. Scene maps usually carry latitude and longitude information and can be overlaid on GIS maps to both represent location information through the GIS map and visualize the internal structure of a building through the model. For model maps, scene maps are more professional and applicable to the general scenarios of office buildings, residential buildings, etc.** 1. Upload the scene map files in unw format. See Edit Map-Bind Map. 2. For instructions on modifying scene map parameters (longitude and latitude, sky styles, GIS map), see Map Engine Management- Scene Management. **Figure 27-4: An example of scene map** 

27.1 Map Engine Management

Go to **Basic Config > Map Config > Map Engine Management**.

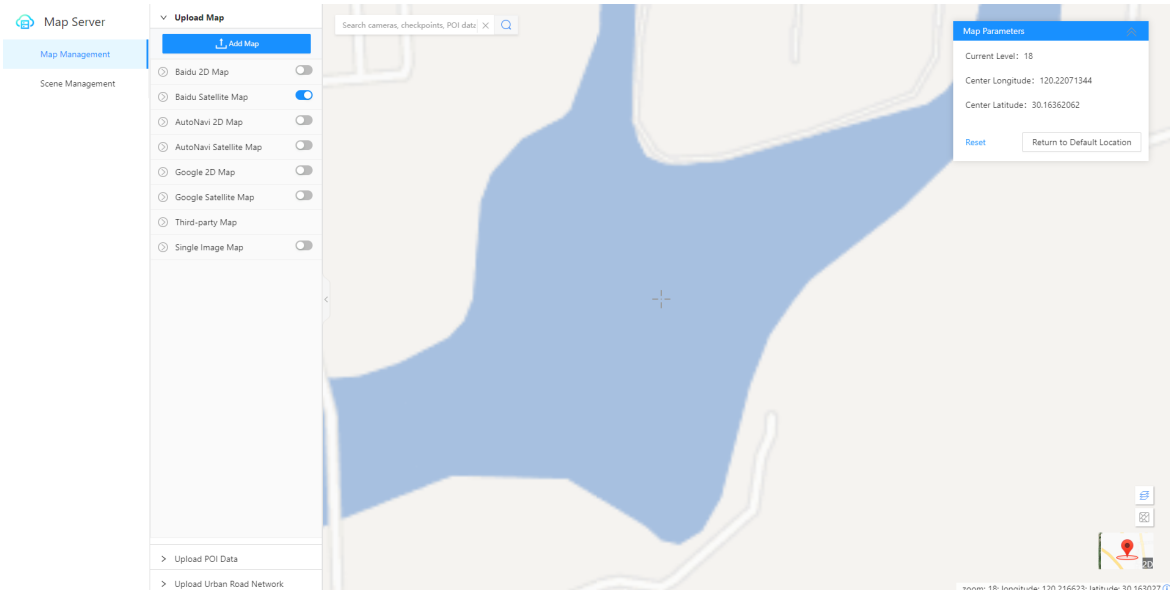
Configure the map service, including adding maps and configure scene maps.

Note:
For instructions on uploading flat maps, 3D model maps, or scene maps, see Edit Map-Bind Map.

27.1.1 Map Management

27.1.1.1 Add Map

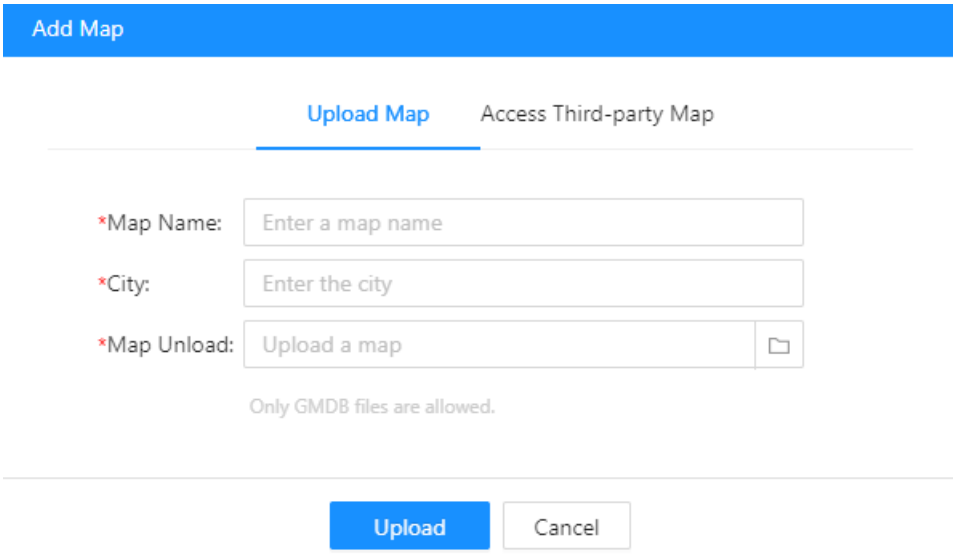
You may upload GIS maps (offline maps), access third-party maps (online maps).



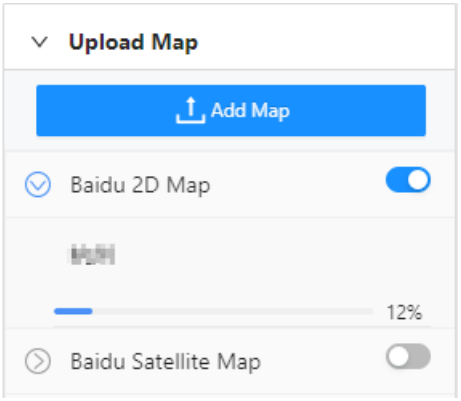
Upload GIS Map

The system will analyze the GIS map type (including 2D maps, satellite maps) after you upload a map.

1. Go to **Upload Map**, click **Add Map**.
2. Click the **Upload Map** tab.



3. Enter the map name, city, and then click and select the map file (.gmdb format, max. 512MB) to upload.
4. Click **Upload**.

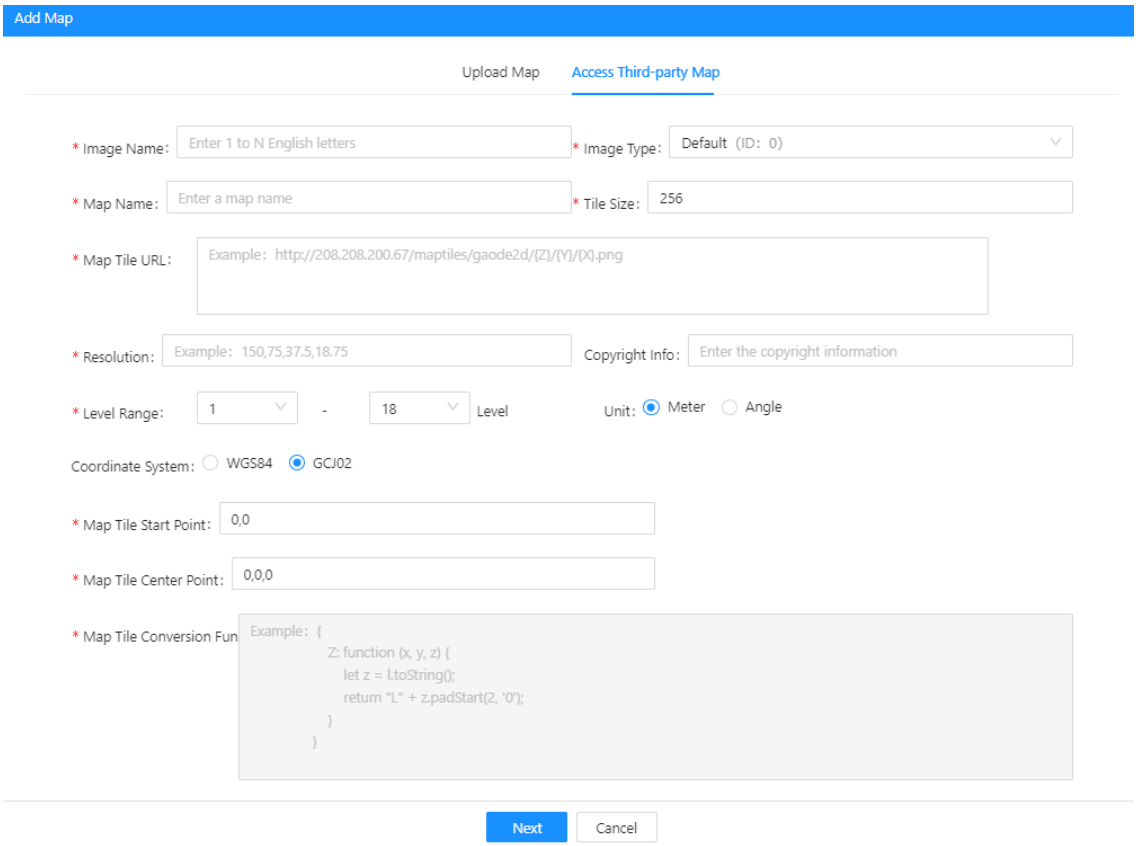


Note:
Do not close the page or browse to other pages before the map is uploaded.

Access Third-party Map (online maps)

The system supports third-party maps (which released on website by map-makers).

1. Go to **Upload Map**, click **Add Map**.
2. Click the **Access Third-party Map** tab.



3. Configure the parameters (obtain parameter values, you can either download the map service information file from the third-party map service publishing website or contact the third party for assistance).

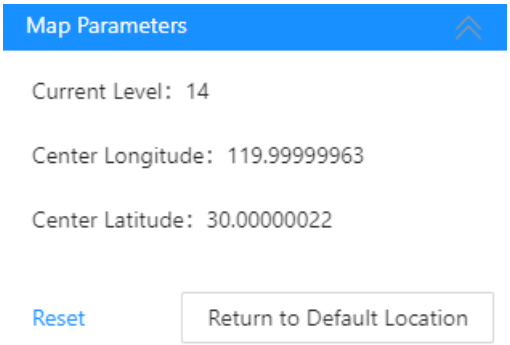
Parameter	Description
Image Name	Name of the map source, used for internal differentiation, and can be customized. It consists of letters, such as "Google".
Image Type	You may choose **Default**, **2D**, and **Satellite**, or click **Customize** to add a custom type.
Map Name	Enter a map name as needed. The name will be displayed in the map list.
Tile Size	Size of map tile. The default unit is pixel (px). You can check it in the map service information file.
Map Tile URL	Third-party map address. You can check it in the map service information file.
Resolution	Resolution of each level of map, separated by commas, refers to the actual distance represented by one pixel on the screen. You can check it in the map service information file.
Copyright Info	Copyright information of the map.
Level Range	The supported range of levels for the map, from 1 to 18. You can check it in the map service information file.
Unit	Unit of the map, which can be Meter or Angle. You can check it in the map service information file.
Coordinate System	Coordinate systems used in the map. You may choose Default (Mercator), WGS84, and Mars. You can check the map service information file for the available options.
Map Tile Start Point	Longitude and latitude of the starting point for map tiles. You can check it in the map service information file.
Map Tile Center Point	The level, longitude, and latitude of the center point of a map tile can be found in the map service information file.

Parameter	Description
Map Tile Conversion Function	Manipulates the map tile sequence number, such as adding prefixes or converting to hexadecimal, and thereby concatenate the complete address to retrieve the map tile.
Add Correct Point	Used to compare and align the coordinates of the third-party map with the base map. If they are not consistent, at least three correction points should be added on both sides at the corresponding positions.

4. Click **Next** to preview the map.
5. Click **OK** to save the map.

Map Management Operations

- Enable map: Only enabled maps will be displayed. Only one map can be enabled at a time.
  Click to enable a map. Blue means the enabled status.
- Set the center position of the map, which is the default position displayed when you open the map page. In the floating window above the map, you can view the current status, including the map level and the longitude and latitude of the center position.



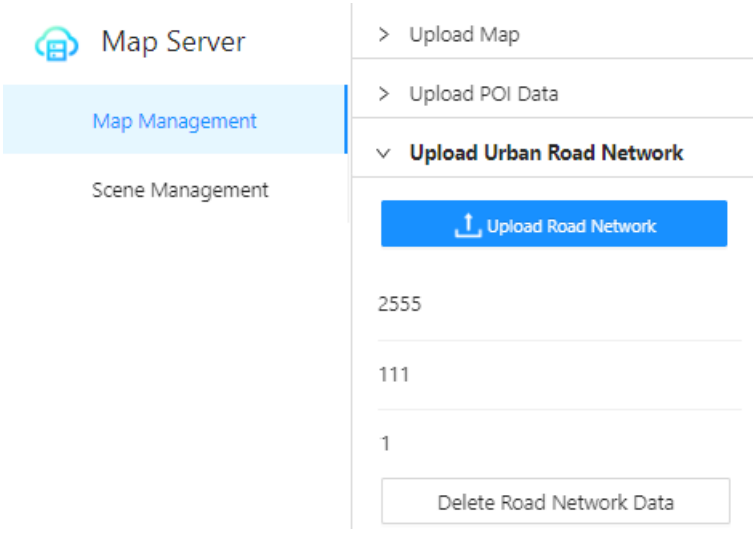
  1. To change the center position, click **Reset**.
  2. A "+" symbol will be displayed on the map. Drag the map to align the center with the "+".
  3. Click **Set as Default Position** to set the marked position as the center position.
- Return to the default location: Click **Return to Default Location** to quickly return to the default position.

27.1.1.2 Upload Urban Road Network

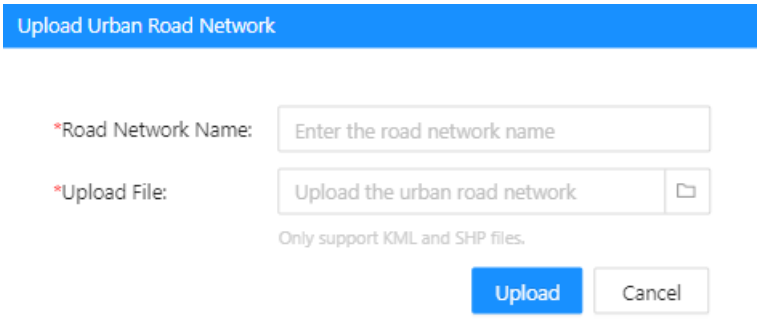
Road network refers to the actual distribution of roads on a map. When a road network is added to a map, the route (or trajectory) will be drawn based on the road network, otherwise, it will be a straight line segment between the starting point and the destination.

Upload Road Network

1. Expand the **Upload Urban Road Network** tab, click **Upload Road Network**.



2. Enter the road network name, and upload the road network file.



Note:
The road network file must be in .kml or .shp format.

3. Click **Upload**.

Road Network Management Operations

- Show or hide road network: Click / in the bottom right corner of the map to show or hide the road network.
- View details: Click and then choose **View Details** to view the detailed information about the uploaded road network file.
- Delete road network: Click **Delete Road Network Data**, and then confirm. All road network data will be deleted.

27.1.2 Scene Management

A scene map is a model in unw format. A model is one or more complete buildings, including multiple floors. Scene maps usually carry latitude and longitude information and can be overlaid on GIS maps to both represent location information through the GIS map and visualize the internal structure of a building through the model.

You can add scene image models and configure model parameters as needed.

- The scene maps added on this page will not be automatically synchronized to e-map (Edit Map). However, after completing configuration, you can export the map model and upload it in e-map.
- The scene maps added in e-map will be synchronized to this page. You can modify the model parameters here, and the changes will be automatically synchronized to the scene maps in e-map.

27.1.2.1 Add Scene Map

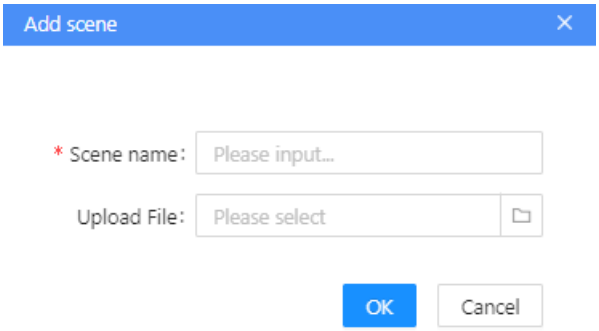
A scene map (.unw format) includes models of multiple layers.

Add Scene

1. Go to **Scene Management**, click **Add Scene**.

2. In the **Add scene** dialog box, enter the scene name, and upload a map (.unw format) for the scene.

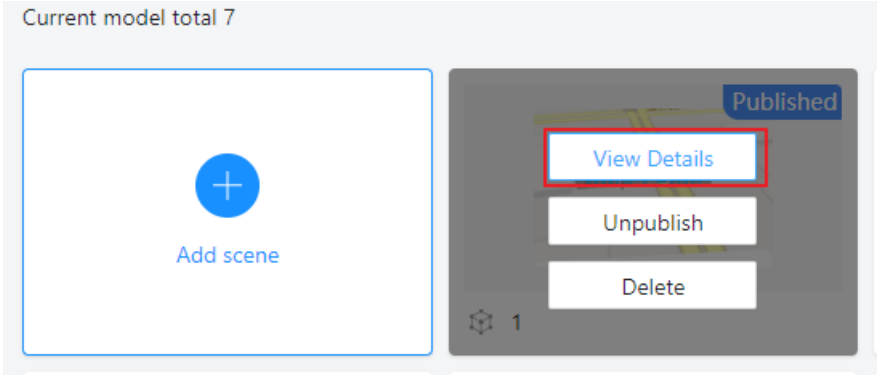
> **Note:**
> The models of each layer will be analyzed after you upload a scene map here.
> You may also add layers (see Add Layer) and upload models in the **Edit scene** dialog box.



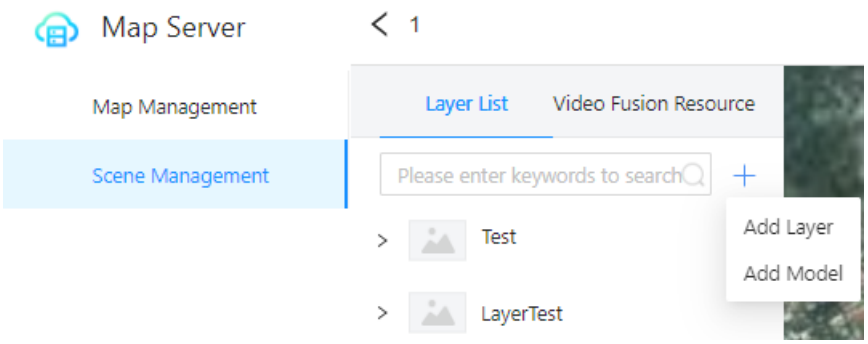
3. Click **OK**.

Add Layer

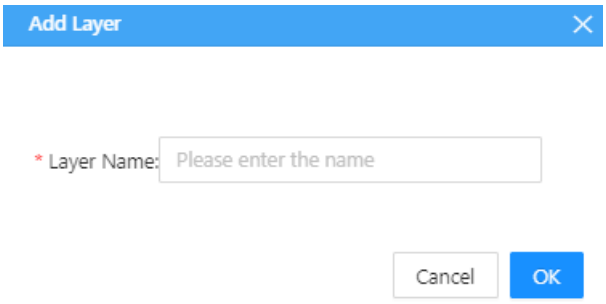
1. On the **Scene Management** page, hover over a card, click **View Details**.



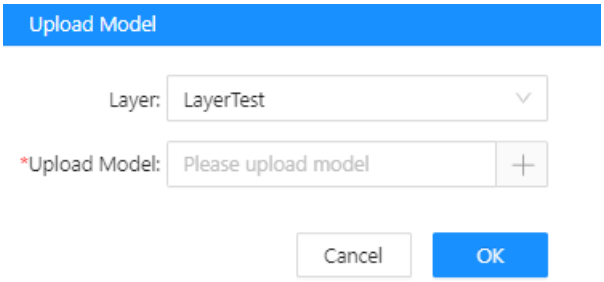
2. In the layer list, click ＋, choose **Add Layer**.



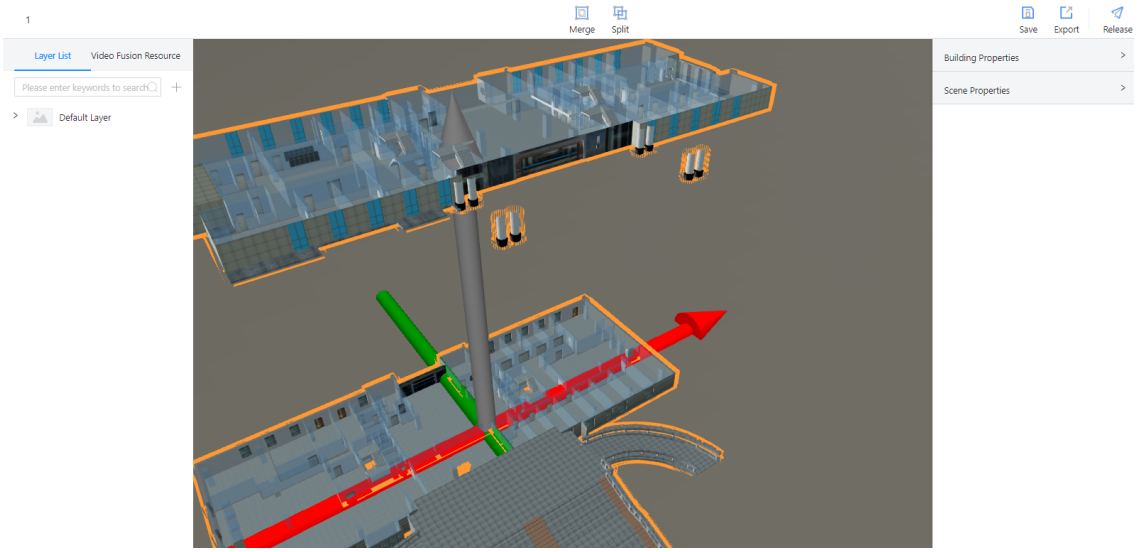
3. Enter the layer name, and then click **OK**. The layer is created.



4. In the layer list, click ＋, choose **Add Model**.
5. Select the layer, and then upload the model file (.zip format).



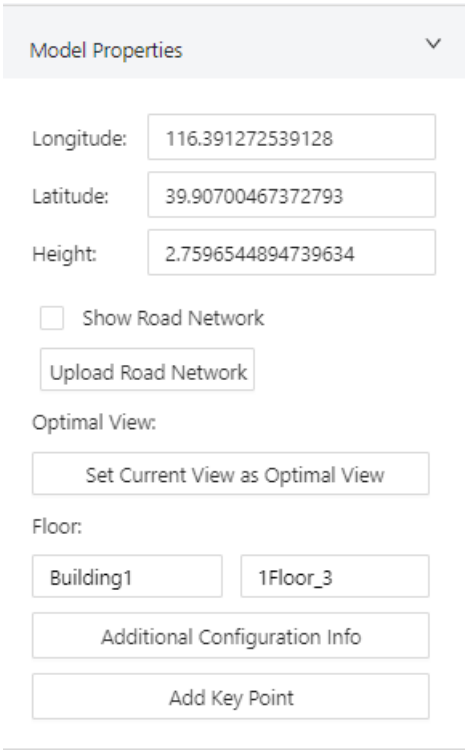
6. Click **OK**. The model is created.



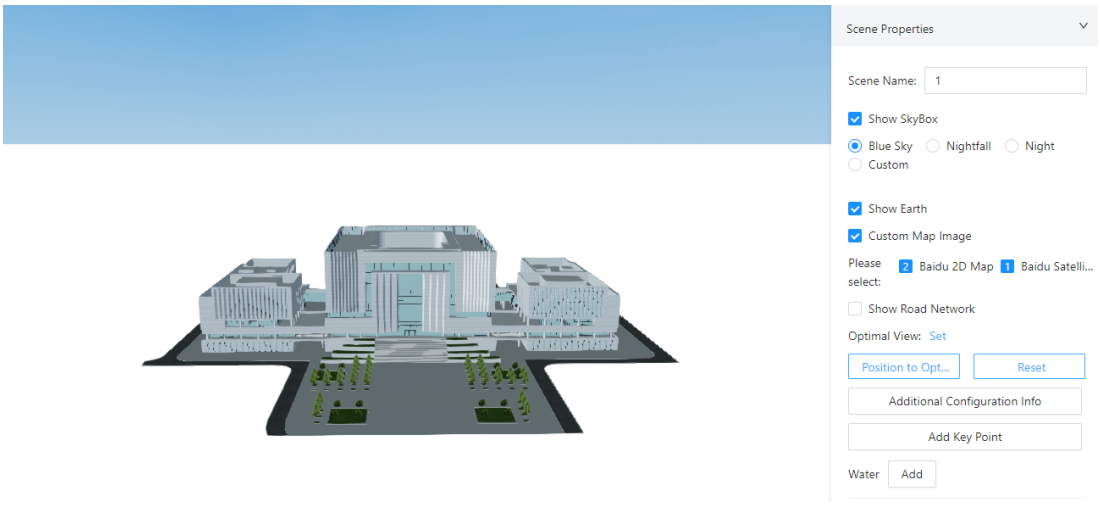
27.1.2.2 Configure Model Properties

Configure model properties and scene properties after the model is uploaded.

1. Go to **Scene Management** > **Layer List**, and then select a model.
2. Configure properties on the right side.
   - Model properties: Configure the latitude and longitude coordinates of the model, road network, and optimal view.



- Scene properties: Configure the scene models to be displayed on the earth scene to enhance the visual appeal of the model map.
  - SkyBox: The display style for the sky.
  - Show Earth: Place the scene model on the earth sphere.
  - Custom Map Image: Select an uploaded GIS map source to display the scene model on the GIS map according to the latitude and longitude.
  - Show Road Network: Displays road networks on the scene model.
  - Water/Wall: Click **Add** and use mouse to draw lines as water surfaces or walls.



3. Click **Save** in the upper-right corner when you complete the configuration.

27.1.2.3 Export Model

After completing the configuration of the scene model, click on **Export** in the upper-right corner to export the scene map (.unw format).

More Operations

You can upload a scene map in Bind Map.

27.2 Edit Map

Go to **Basic Config > Map Configuration > Edit Map**.

Users can bind maps to different areas, add devices to the maps, and draw hot zones on the maps.

Note: Flat maps, model maps, GIS maps, and scene maps are supported.

Figure 27-5: An example of a flat map

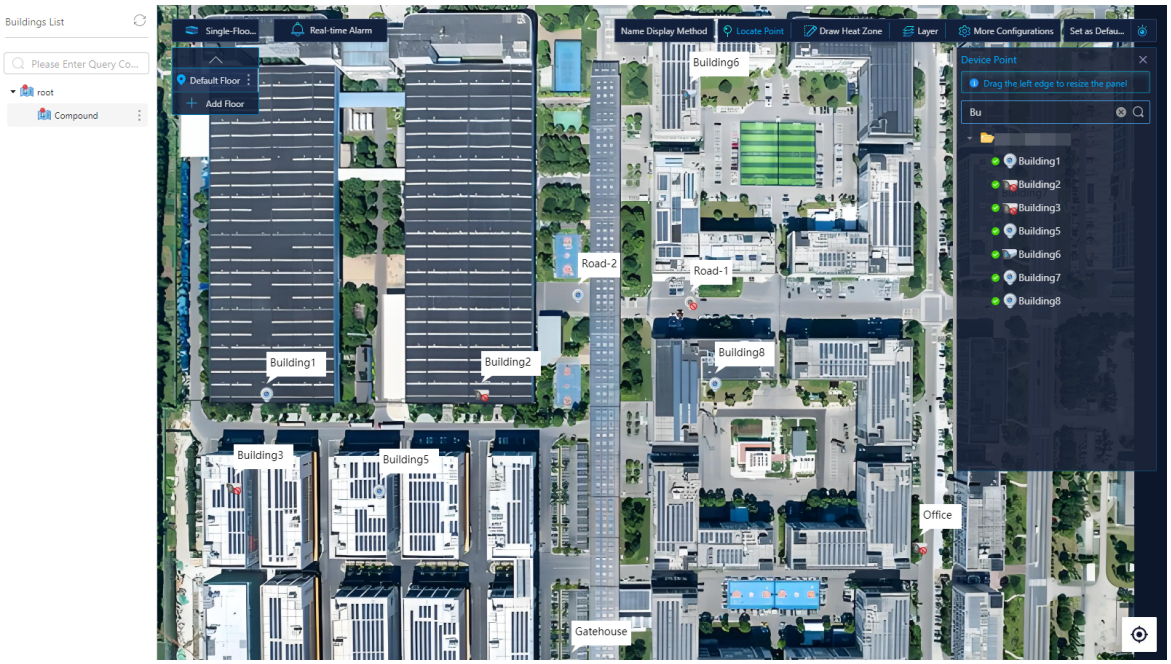
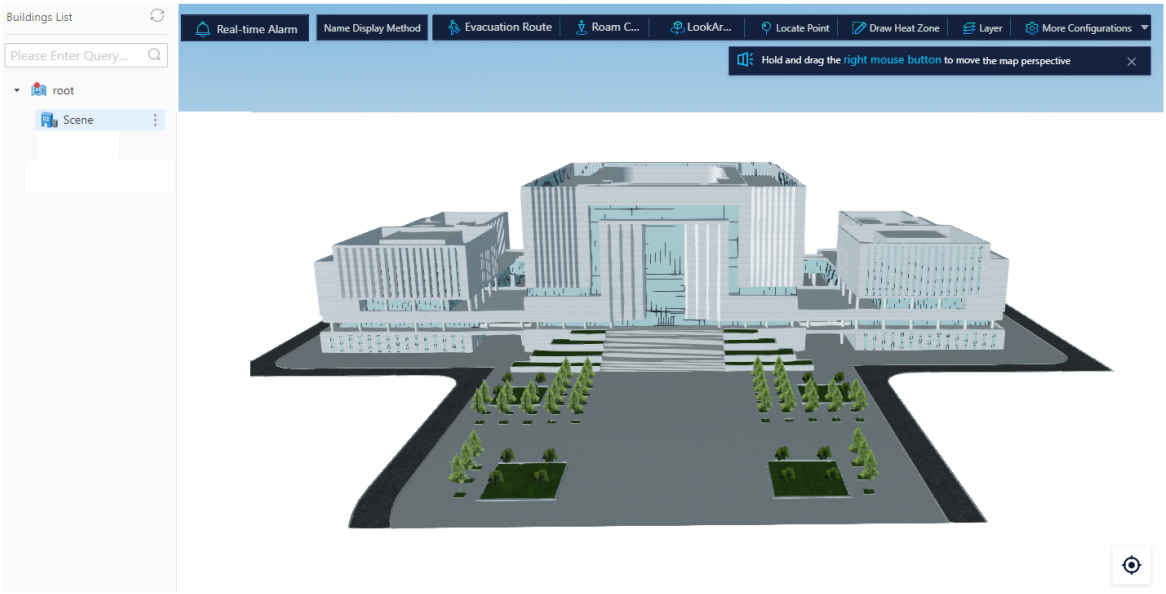


Figure 27-6: An example of a scene map



27.2.1 Bind Map

Create areas and floors and bind them to a map according to the actual building.

Prerequisite

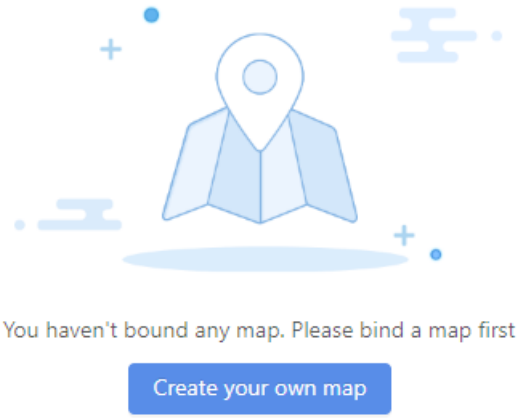
To use the GIS map and city road network, please make sure you have uploaded them in **System Configuration** > Map Engine Management.

Note:
For images, model maps (including road networks), and scene maps, you can upload them directly in E-map page.

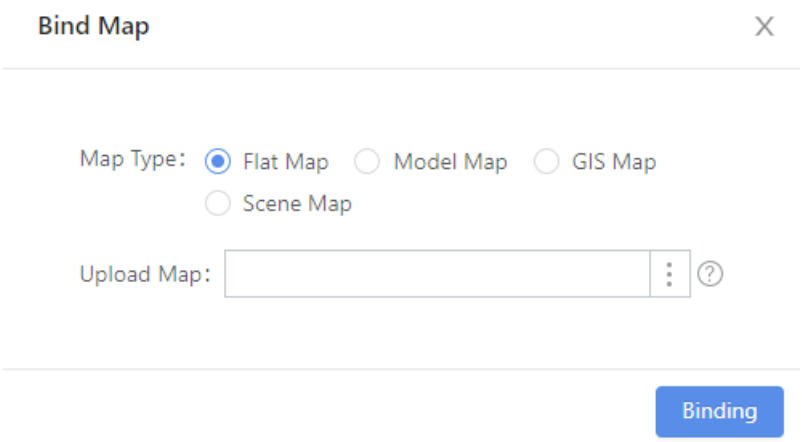
1. Bind Map

For the first-time use, please add a default map first. It is recommended that the default map provides an overview of the area. You can then add submaps as needed. For example, Area Map > Building Map > Floor Map.

1. On the **MapEdit** page, click **Create your own map**.



2. Select the map type and upload the corresponding file. Then click **Binding**.



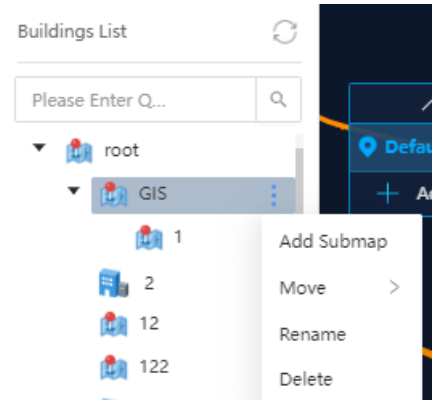
Note:

- Flat map: ① Must be JPEG, JPG, PNG, or BMP images, max size 100MB. Both the height and width cannot exceed 8190px. ② Cannot be paused or canceled after the file is uploaded.
- Model map: ① Supports single gltf model; 3dtiles models/gltf models compressed into a ZIP file can also be uploaded. Please make sure there is a tileset.json file/index.gltf in the root directory after unzipping and the size of the model must be within 100MB.② Road networks allow Shapefile data in a zip file. Road network data must include point data and route data.
- GIS map: After uploading a GIS map in **Resource Management** > **Map Engine Management**, you can bind the map on this page.
- Scene map: Must be .unw format scene maps (no size limit). After uploading, the scene map will be overlaid on the enabled GIS map according to the latitude and longitude.

2. Add Submap

In the building list, the first uploaded map is designated as the root layer.

1. Choose the parent map, click ⋮, and click **Add Submap** to add a submap.



Note:

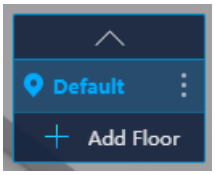
- Up to 4 levels of maps are allowed.
- The root map can be renamed but cannot be deleted.
- You can click **Move** > **Up**/**Down** to change the map sequence on the list.

2. For newly added submaps, please bind the map by referring to 1. Bind Map.

3. Add Floor

For flat maps, model maps, and GIS maps, there is a default floor in the floor list, you can also add multiple floors to the area map. (Scene maps already have multiple floors included by default, so you don't need to add floors)

1. Click **Add Floor** to add a floor.



2. To bind a map for newly added floors, see operations in 1. Bind Map.

Note:

- Click ⋮ for the floor to set it as the default floor, rename or delete it, or move it up or down in the floor list.
- The default floor can be renamed but cannot be deleted.
- The default floor is displayed each time you access the map. You can also change the default floor.

4. Change Map

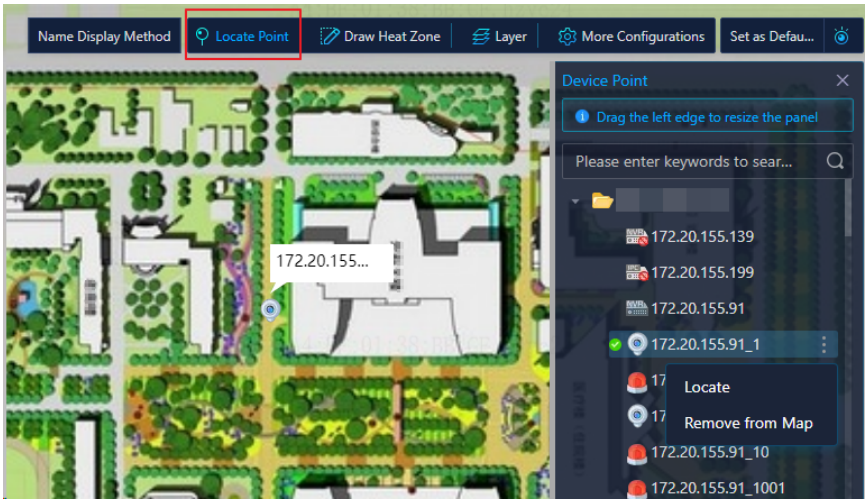
Click **More Configurations** > **Change Map** in the upper-right corner to upload a new map.

27.2.2 Device Point Management

Mark devices on the map to visualize device locations.

Mark Device Point on the Map

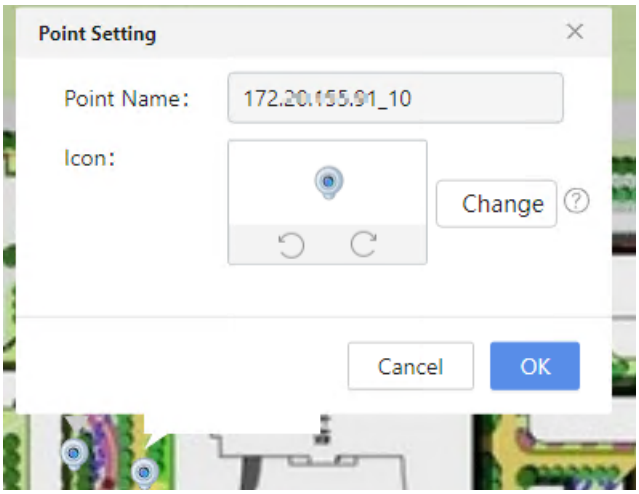
1. Click **Locate Point** above the map. All devices in the local domain are listed.



Note:

- indicates devices that are already marked on the map.
- Click for the device to locate it on the map or remove the device from the map.
- If the device name is not fully displayed, drag the left edge to resize the panel.

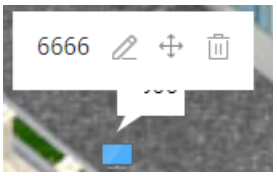
2. Select a device and drag it to the desired position on the map.
3. Change the device icon in the pop-up window as needed.



4. Click **OK**.

Manage Device Points on the Map

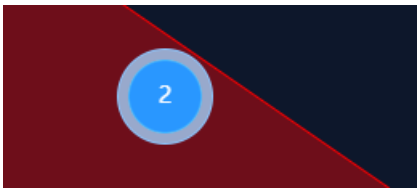
For devices marked on the map, you can edit the device information, move the device position, or remove them from the map.



- Click to edit the point name and icon.
- Click to move the point position.
- Click to delete the point.

Aggregate Points

If device points on the map are very close together, they will be aggregated and a number will be displayed to indicate the total number of aggregated devices.



27.2.3 View Map

After binding a map and marking device points to the area, you can view device points visually.

1. By default, the page shows the default floor of the root area.
2. Select an area map from the map list on the left and the default map for that area will be displayed on the right.
3. Click on the floor list in the map's upper-left corner to switch to the map of the desired floor.

Note:

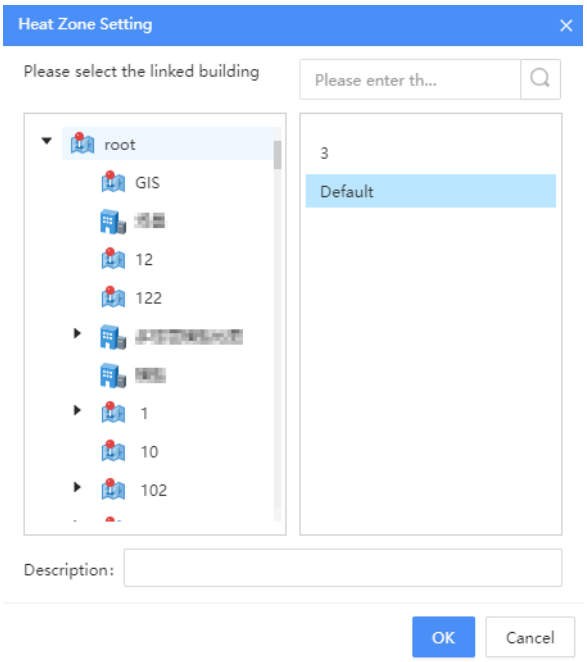
- You can use the scroll wheel to zoom in or out on the map.
- You can hold and drag the left mouse button to move the map.
- For model map and scene map, you can hold and drag the right mouse button to move the map perspective.
- Click in the map's lower-right corner to restore the default perspective.

27.2.4 Heat Zone

Draw heat zones on the map. A heat zone is to jump from the current area to another linked area. For example, if an alarm occurs at location A and you also need to check the situation at location B, you can set A as a heat zone linked to B.

Draw Heat Zone

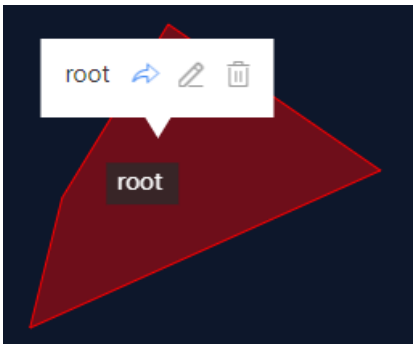
1. Click **Draw Heat Zone** above the map.
2. Use the left button to draw a closed area on the map, and double-click to complete the drawing.
3. Select a map to link to in the pop-up window and click **OK**.



Heat Zone Management

Hover the mouse over a heat zone to display operation icons.

- Click to jump to the linked area from the current area.
- Click to edit the linked area.
- Click to delete the heat zone.

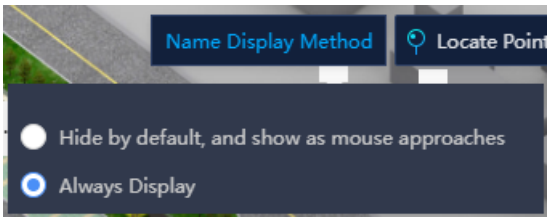


27.2.5 Map Display Management

Mange the display of on-map device resources, road networks, and map perspectives.

Show/Hide Device Name

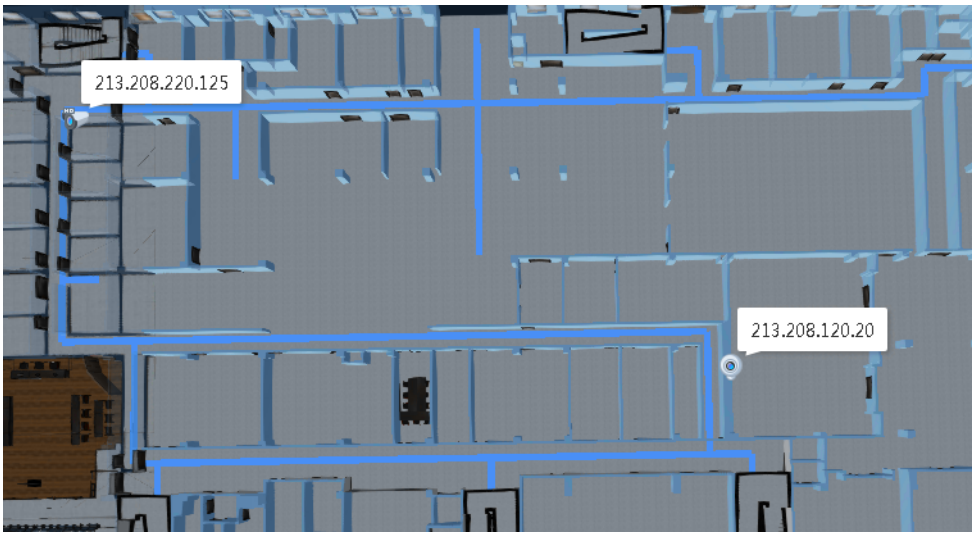
Click **Name Display Method** above the map to choose whether to display device names on the map.



Show/Hide Road Network

After uploading a road network to a model map or a GIS map, you can set whether to display the road network.

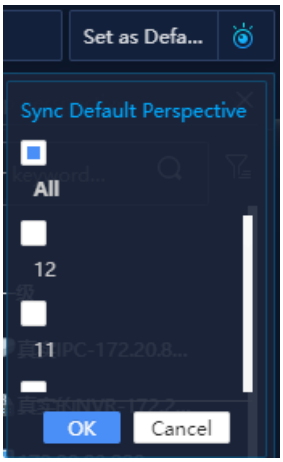
Select **Show Road Network**. The road network is shown as blue paths in the figure below.



Set Default Perspective

You can set a default perspective in flat maps, model maps, or GIS maps.

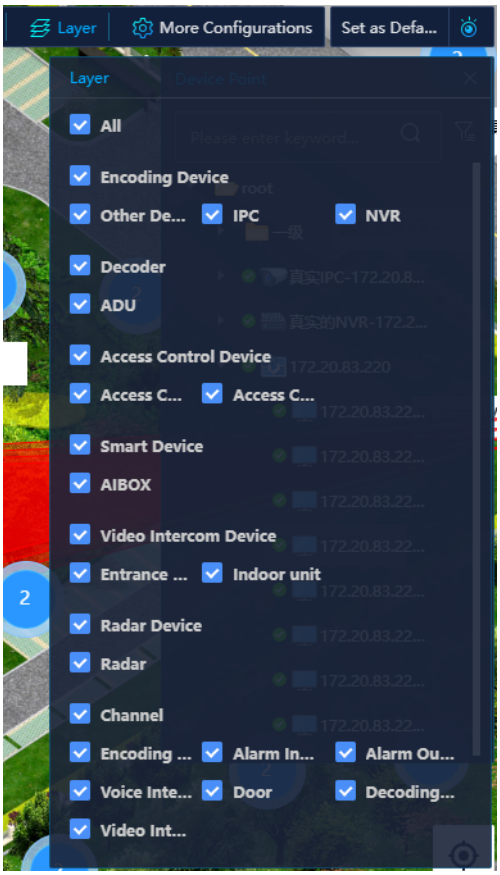
- Click **Set as Default Perspective** in the upper-right corner to set the current map view as the default perspective. After adjusting the map view, you can click in the bottom right corner to restore the default perspective.
- Click in the upper-right corner, and select map(s) of the same type as the current map to sync the current default perspective setting to the selected map(s).



Manage Layer Display

Configure the types of device resources to be displayed on the map for a clearer view.

Click **Layer** in the upper-right corner and select the types of devices to be displayed on the current map.



Clear Data

Click **More Configurations** > **Clear Data** in the upper-right corner to clear all devices and heat zones on the map.

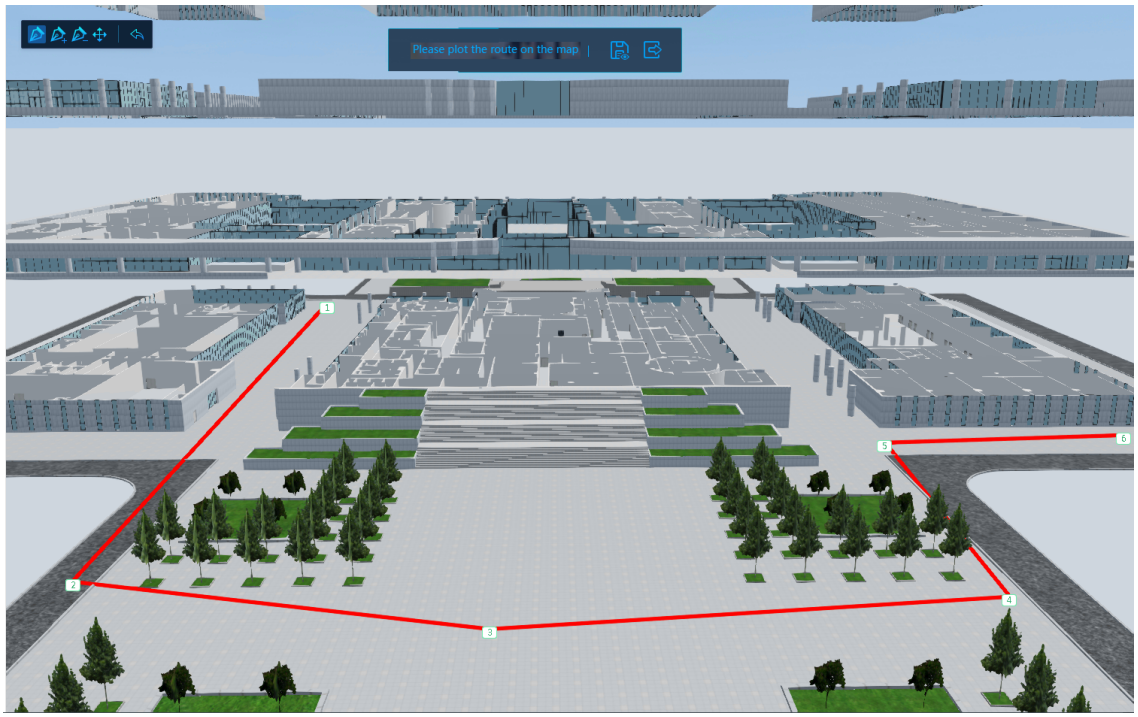
27.2.6 Evacuation Route

Draw evacuation routes on the map so when an emergency occurs, people can follow the route to safely evacuate.

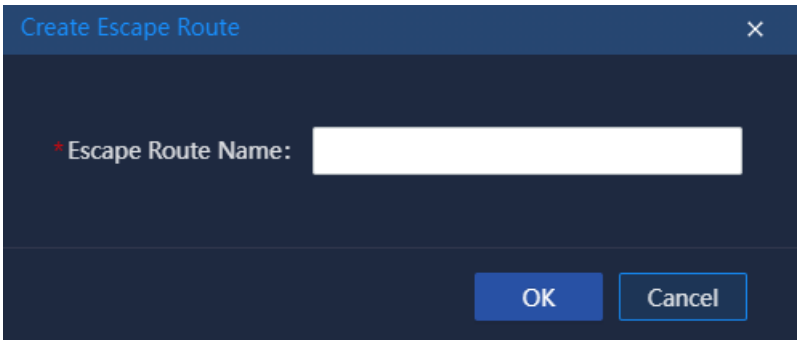
Note:
Evacuation routes can be drawn on scene maps only.

Draw Evacuation Route

1. Click **Evacuation Route** in the top toolbar to display the evacuation route list.
2. Click **Add Path** in the list to start drawing a route.



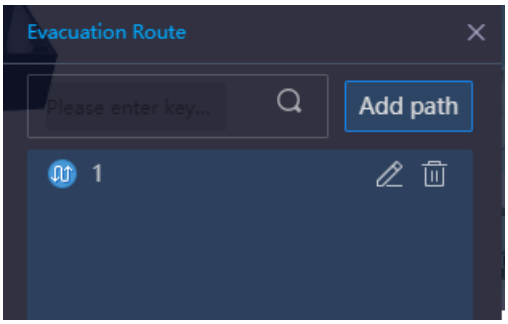
3. Click to draw anchor points. The system will connect the anchor points in sequential order to form line segments. Click to enter preview mode.
4. Click again, and then enter a name for the route.



5. Click **OK** to save the route.

Edit Evacuation Route

1. Click **Evacuation Route** in the top toolbar to display the evacuation route list.



2. Click for the route you want to edit.
3. Modify the route by referring to the descriptions in the table below.

Table 27-1: Icon Description

Icon	Description
	Add an anchor point. Click anywhere on the map to add an anchor point.

Icon	Description
	Insert an anchor point. Click anywhere between two anchor points on the route to insert a new anchor point.
	Delete an anchor point. You can delete any anchor point on the route, and after deletion, the two adjacent anchor points will automatically connect to form a line segment.
	Move an anchor point. You can drag and move any anchor point.
	Undo the previous action.

4. Click to save the changes and enter preview mode.

   Note: To exit the editing mode, click and then confirm the prompt message.

5. Click .
6. Set the route name, and then click **OK** to save the changes.

Delete Evacuation Route

In the evacuation route list, click for the route you want to delete, and then confirm the action.

27.2.7 Roam Config

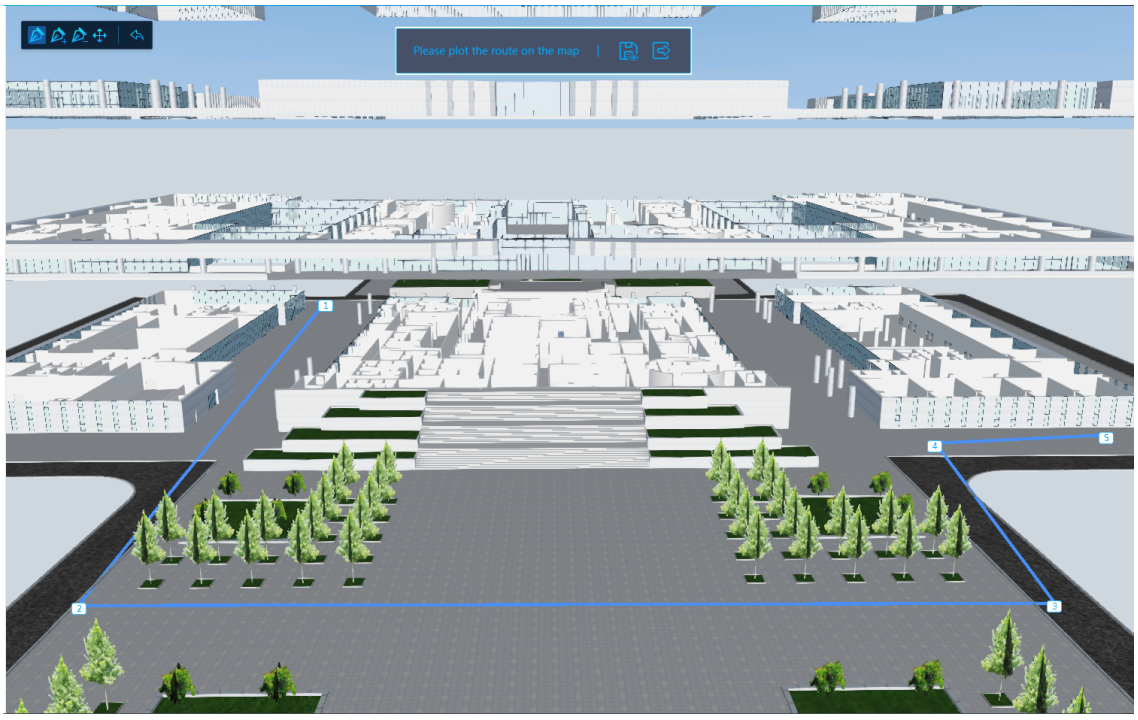
Draw roam paths on the map to enable automatic movement of the map perspective along the roam path.

Note:
Roam paths can only be drawn on scene maps.

Draw Roam Path

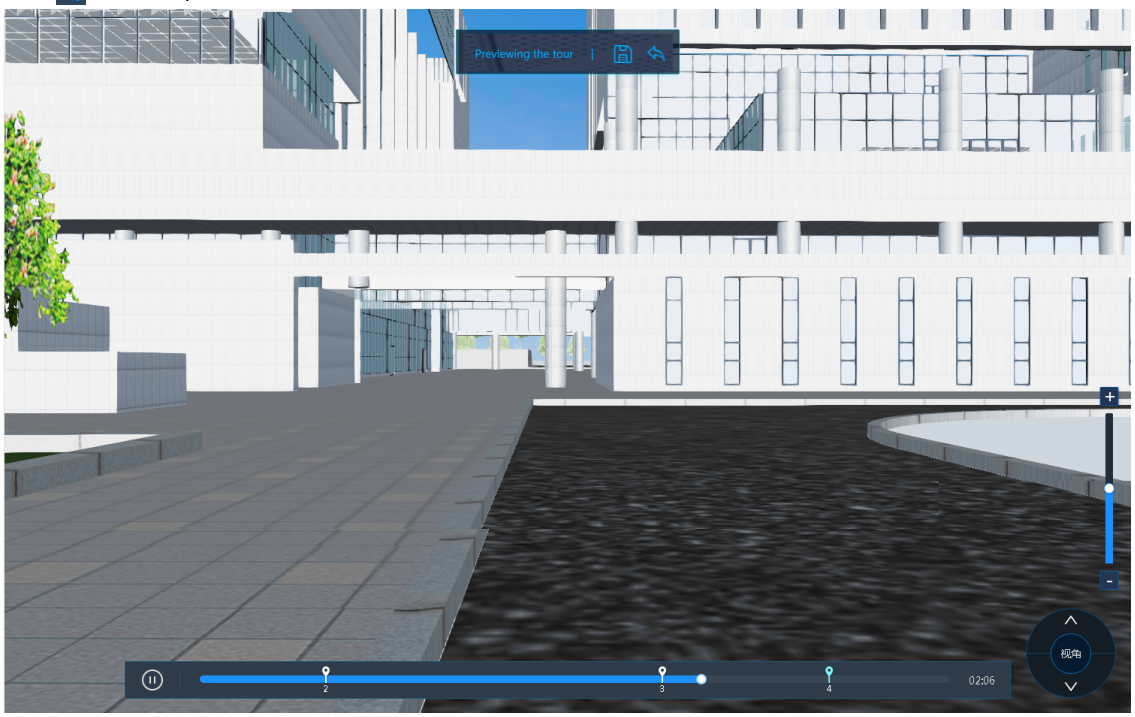
1. Click **Roam Config** in the top toolbar to show the roam path list.
2. Click **Create Path** in the list to start drawing the path.

   Figure 27-7: Draw Roam Path



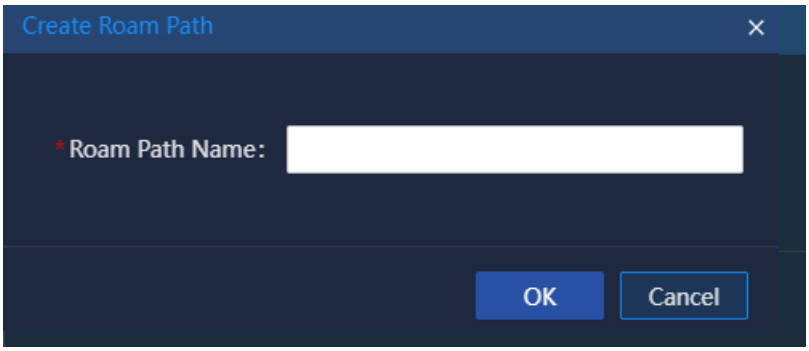
3. Click to draw anchor points. The system will connect the anchor points in sequence to form line segments.

4. Click to enter preview mode.



5. Click again, and then enter a name for the roam path.

Figure 27-8: Create Roam Path



6. Click **OK** to save the settings.

Preview Roam Path

You can adjust the video speed and viewing angle in preview mode.

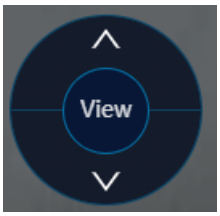
Progress bar

The progress bar at the bottom shows the preview progress.

- Click to play the preview video; click to pause the video.
- Drag the progress indicator to adjust the progress; or click on the progress bar to navigate to the desired time point.
- The progress bar shows the positions of the various anchor points. Click a marker to navigate to the corresponding time point of the anchor point.

Adjust view

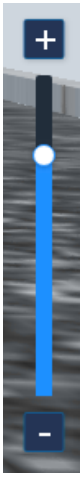
Adjust the view upward or downward.



- : Adjust the view upward.
- : Adjust the view downward.

Adjust speed

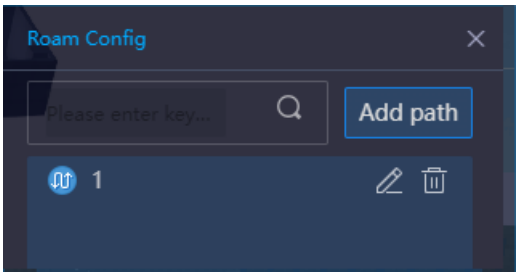
Adjust the video playing speed in preview.



- : Increase the video playing speed in preview.
- : Decrease the video playing speed in previews.
- Drag the slider up or down to increase or decrease the video playing speed.

Edit Roam Path

1. Click **Roam Config** in the top toolbar to show the roam path list.



2. Click for the path you want to edit.
3. Edit the path by referring to the descriptions in the table below.

Table 27-2: Icon Description

Icon	Description
	Add an anchor point. Click anywhere on the map to add an anchor point.
	Insert an anchor point. Click anywhere between two anchor points on the path to insert a new anchor point.
	Delete an anchor point.

Icon	Description
	You can delete any anchor point on the path, and after deletion, the two adjacent anchor points will automatically connect to form a line segment.
	Move an anchor point. You can drag and move any anchor point.
	Undo the previous action.

4. Click to save the changes and enter preview mode.

   Note: To exit the editing mode, click and then confirm the prompt message.

5. Click .
6. Set the path name, and then click **OK** to save the changes.

Delete Roam Path

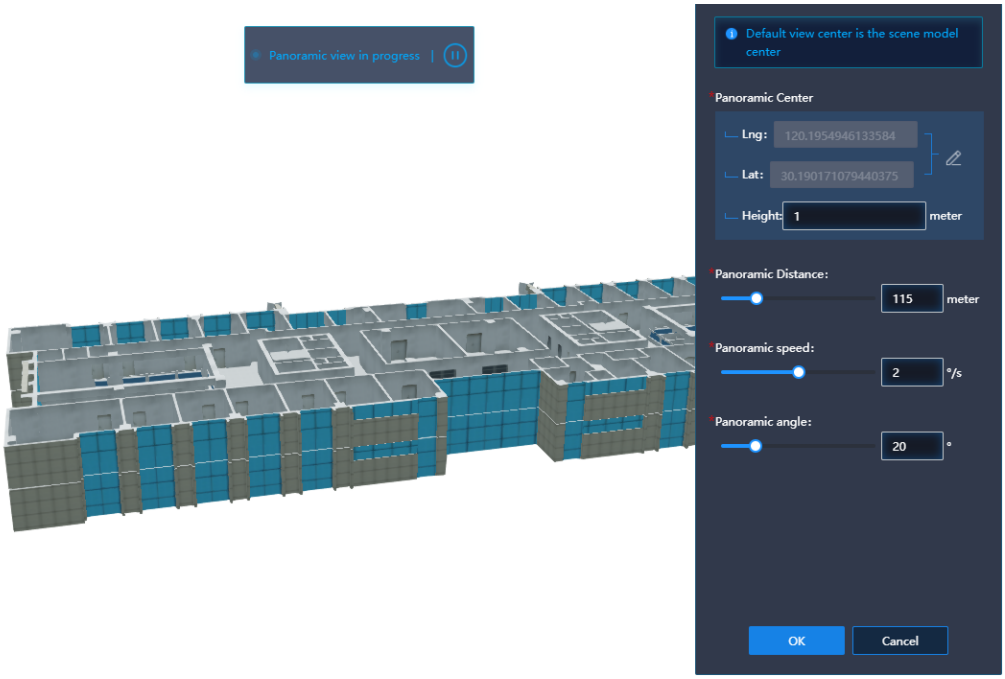
In the roam path list, click for the path you want to delete, and then confirm the prompt message.

27.2.8 Panoramic Config

Customize look around view parameters to achieve panoramic viewing of the scene model (where the model rotates around a central axis, allowing you to view all sides of the model).

Configure Panoramic View

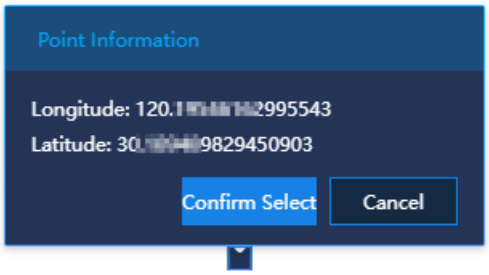
1. Click **Panoramic Config** on the top toolbar to enter editing mode.



2. Configure look around view parameters by referring to the descriptions in the table below. After the configuration is completed, the left side of the page will display the look around view effects.

Table 27-3: Panoramic View Parameters

Parameter		Description
Panoramic Center	Longitude, latitude	(1) Click to enter the top-down view mode. (2) Click to select a point. A dialog box as shown below appears. Check the longitude and latitude and then click **Confirm Selection**.

Parameter		Description
		
	Height	Enter the height (meters) of the center of the panoramic view. **Note:** The height must be an integer in the range of 1 to 500.
Panoramic Distance		Set the distance (meters) for the panoramic view. The value must be an integer in the range of 1 to 500. You may also drag the slider to adjust the value.
Panoramic speed		Set the speed (°/s) for the panoramic view. The value must be an integer in the range of -180 to 180. You may also drag the slider to adjust the value.
Panoramic angle		Set the angle (°) for the panoramic view. The value must be an integer in the range of 0 to 90. You may also drag the slider to adjust the value.

3. Click **OK** to save the settings.

27.3 Map Display Configuration

Go to **Basic Config > Map Configuration > Parameter Configuration**.

You can customize the map display style as needed.

Map Applications Screen Display Name Configuration

You can customize the e-map title displayed in full-screen mode.

1. Enter the title name as needed.
2. Click **Save**.

Figure 27-9: Set Title

Points Display Method

For scene maps, to meet different needs for point icon clarity and loading speed, we provide 2 display modes: Fluency Mode (fast loading but low clarity) or High-definition Mode (high clarity but slow loading).

1. Choose a point display mode as needed (Fluency Mode/High-definition Mode).
2. Click **OK**.

Figure 27-10: Points Display Method

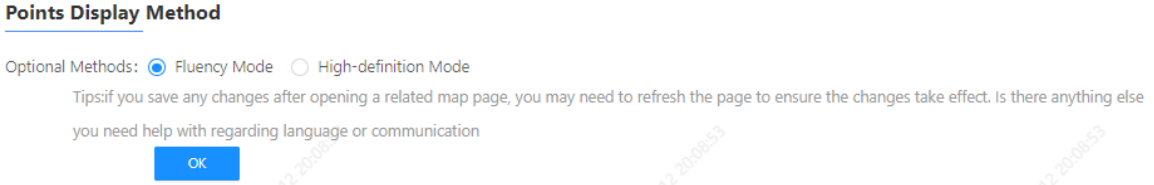
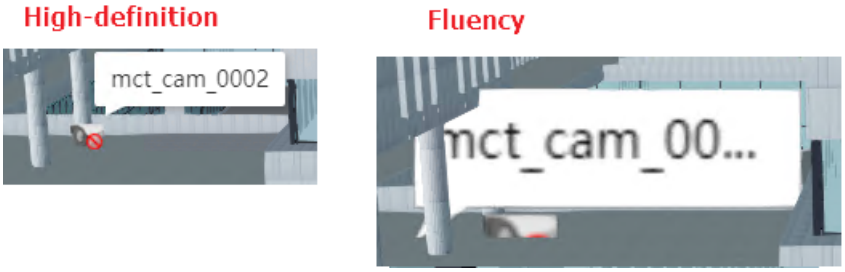


Figure 27-11: Points Display Effect



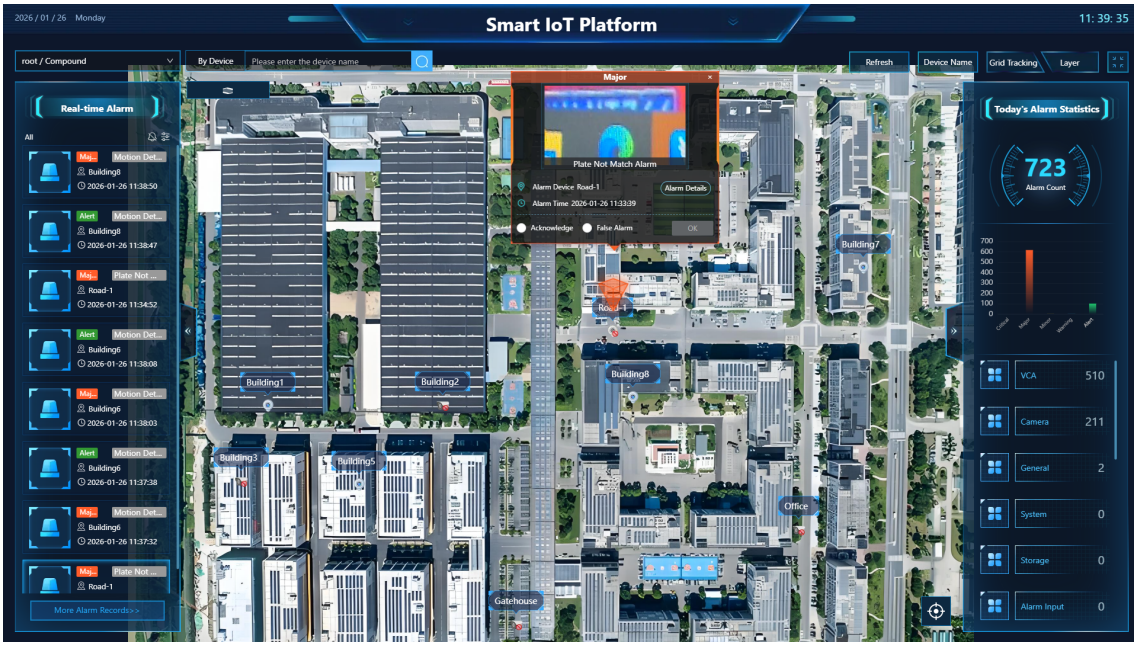
Map Zoom Step

Configure the zoom speed when using the mouse wheel to zoom the map: the larger the step size, the more zoom levels are changed per single mouse wheel operation.

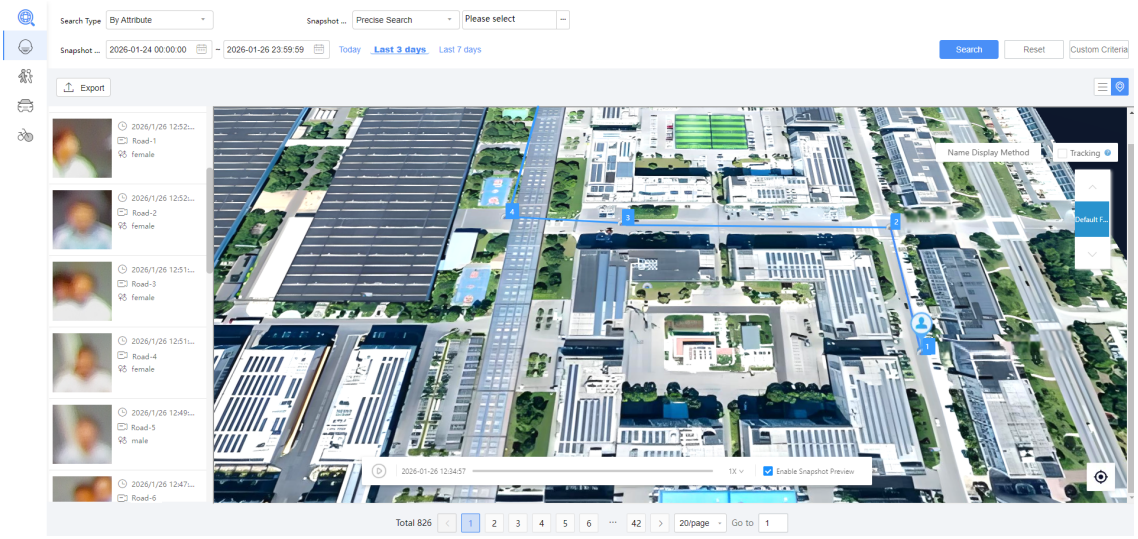
27.4 Map Application

With the map background, users can view device locations, alarm locations, and trajectories of a person more intuitively.

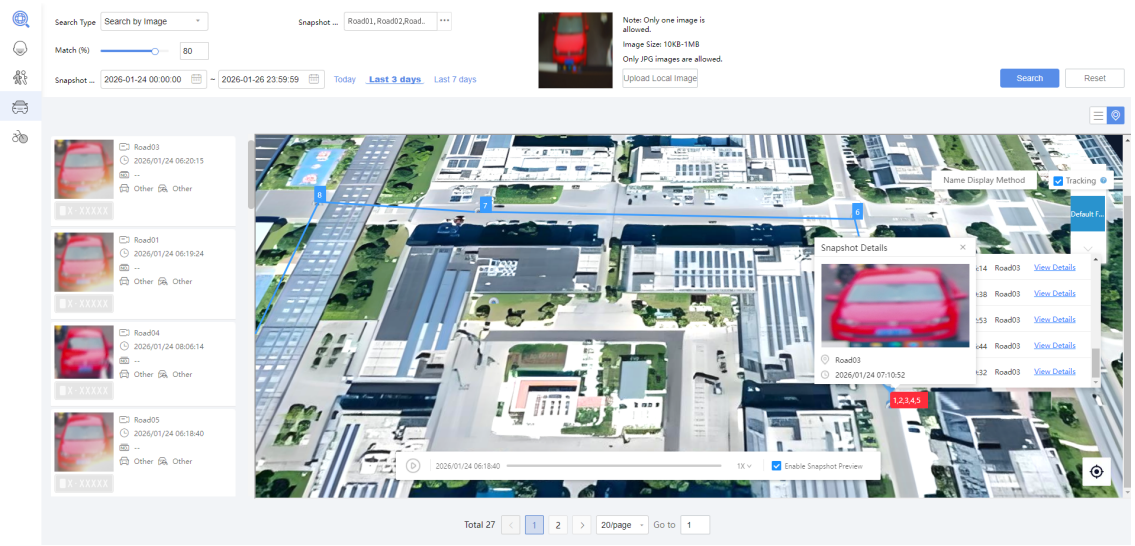
- Real-time Alarm: Allows users to view various types of devices and device alarms on the map and control the devices intuitively.



- Face Trajectory: The system can retrieve the snapshots of a person of interest based on specified features or face image, and then marks his/he geolocation on the map based on time and geographical coordinates to display his/her trajectory on the map. The trajectory provides useful information, including the range of activity and specific locations where the target person has been present.



- Motor Vehicle Trajectory: The system can retrieve the snapshots of a motor vehicle of interest based on specified features/event/violation, and then marks it's geolocation on the map based on time and geographical coordinates to display it's trajectory on the map. The trajectory provides useful information, including the range of activity and specific locations where the target vehicle has been present.



28 Alarm Center

You can manage all types of alarms in the system. Real-time alarm and alarm linkage are available for you to detect abnormalities promptly. You can also search and analyze historical alarms to understand alarm trends and review events.

Function Description

Function Menu	Description
Alarm Configuration	• Allows users to configure alarm recipients, aggregation rules, and sounds to push targeted notifications to users based on their needs. • Allows users to configure alarm linkage methods so that when an alarm occurs, it can automatically trigger associated actions (play live view, display a pop-up alarm window, etc.), ensuring users can promptly perceive and view alarm details.
Real-time Alarm	Allows users to view various device resources and alarms on a map and control devices in a visualized way, providing an immersive operational experience.

Function Menu	Description
Historical Alarm	Allows users to search and handle various kinds of alarms received by the system.

28.1 Alarm Configuration

Configure alarm recipients, aggregation rules, sounds, and alarm linkage.

28.1.1 User Subscription

Configure subscription information for users so that they can receive and view alarms on the Web interface when specified alarms occur on certain devices.

Note:
By default, the admin and loadmin users can receive all alarms without manual alarm subscription.

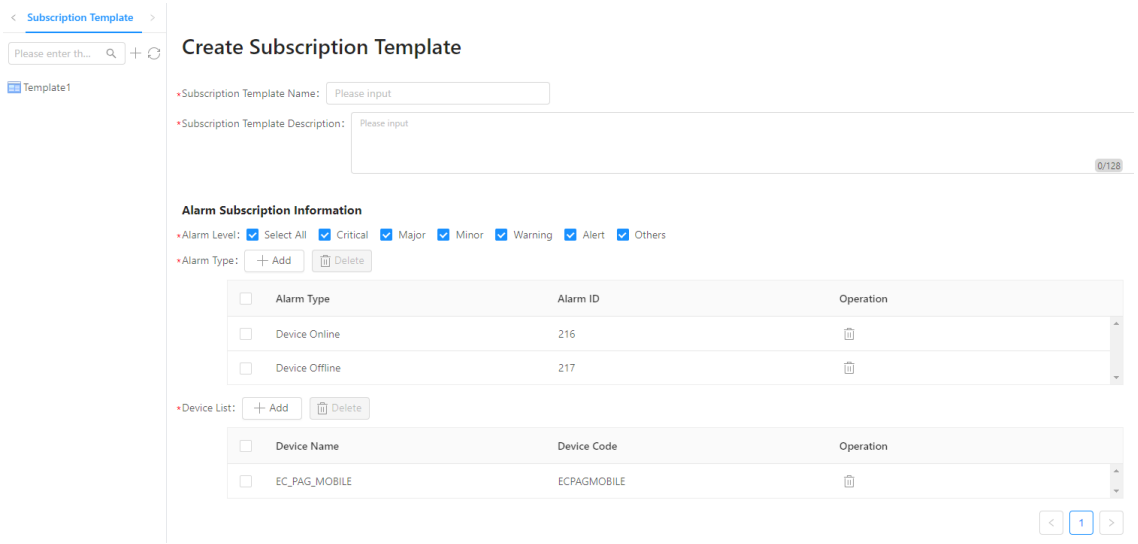
- You can manage subscription information by user or by subscription group.
- Subscription information can be manually entered or auto-filled by template.

Configure Subscription Template

You can create a subscription template for specific alarm types and apply it when configuring subscription information for users or groups, reducing the workload of repeat configuration.

1. Go to **Alarm Config** > **User Subscription**.
2. On the **Subscription Template** tab, click ＋.
3. Complete the subscription information on the right-side.

Figure 28-1: Create Subscription Template



(1) Customize the template name and description.

(2) Select alarm level(s) to subscribe.

(3) Click **Add** next to **Alarm Type** to select alarm type(s) to subscribe.

(4) Click **Add** next to **Device List** to select device(s) to subscribe.

4. Click **Save**.

The successfully saved templates will be displayed in the left-side list. You can enter keywords in the search bar to search for the template or hover the mouse over a template name and click 🗑 to delete it.

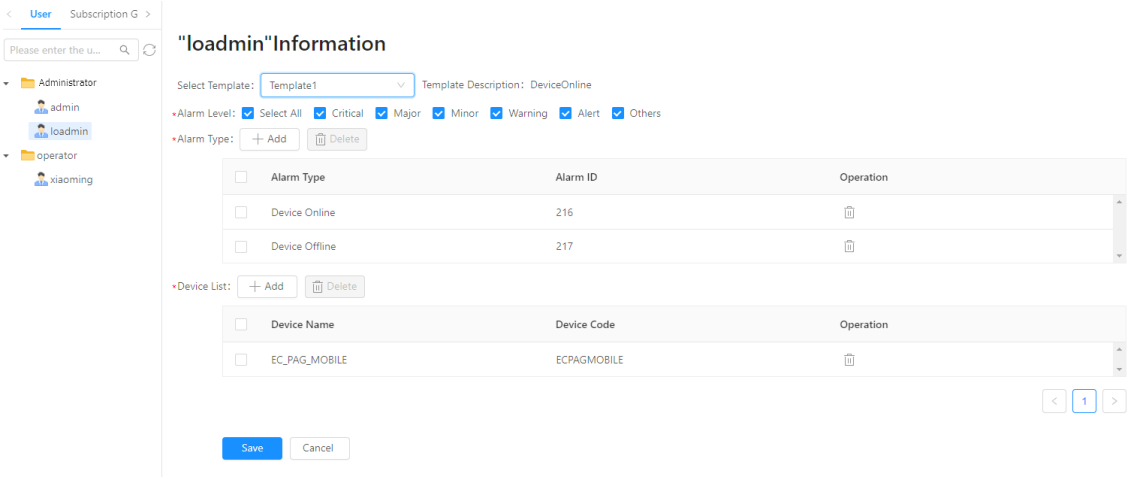
Subscribe by User

Configure alarm subscription information one by one.

1. On the **User** tab, select a user from the left-side user list.

2. Click **Add** in the right-side and complete the subscription information.

Figure 28-2: Configure User Subscription Information



- By Template: Select an existing **subscription template**, and the subscription information in the template will be automatically filled in.
- Manual Enter: Select alarm level(s), alarm type(s) and alarm device(s) to subscribe manually.

3. Click **Save**.

After saving, you can click on the user in the left-side list to view the subscription information.

Other Operations:

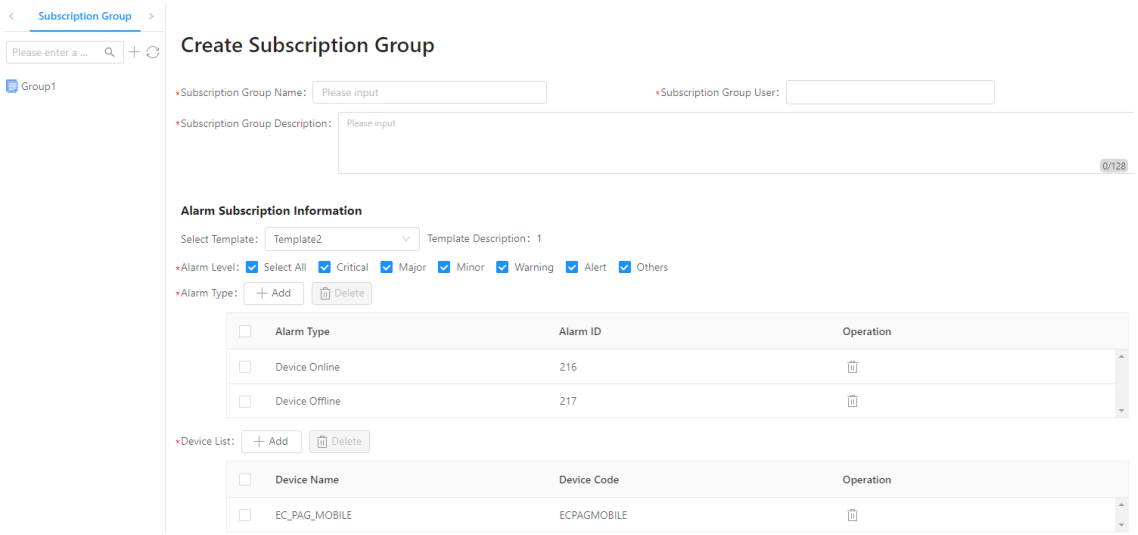
- Edit Subscription Information: Click **Edit** to edit the subscription information.
- Cancel Subscription: Click **Cancel Subscription** to cancel the user's subscription.
- Save as a Template: Click **Save As a Template**, enter the template name and description to save the current configuration as a template.
- Copy Subscription Information: Click **Copy To**, select user(s) to replicate the current configuration.

By Subscription Group

Add users to groups and configure subscription information by group.

1. On the **Subscription Group** tab, click ＋.
2. On the right-side, customize the subscription group name and description, and then select users for the group.

Figure 28-3: Configure Subscription Information for Subscription Group



3. Configure subscription information for subscription group.

- By Template: Select an existing **subscription template**, and the subscription information in the template will be automatically filled in.
- Manual Enter: Select alarm level(s), alarm type(s) and alarm device(s) to subscribe manually.

4. Click **Save**.

After saving, you can click on the group name in the left-side list to view the subscription information. You can click **Edit** to edit the subscription information or hover the mouse over the template name and click to delete it.

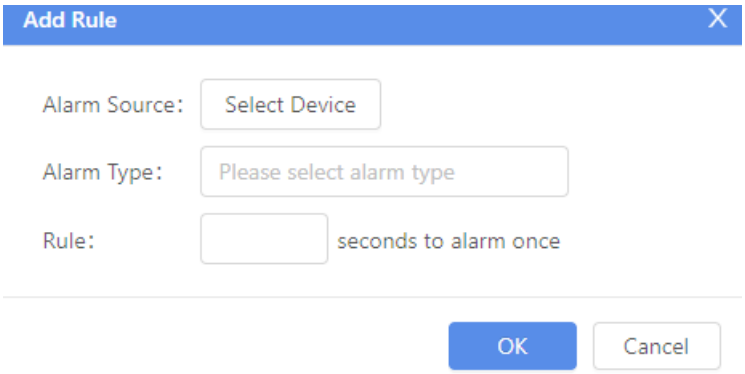
28.1.2 Alarm Aggregation

Set alarm aggregation rules to group same types of alarms from the same source within a specified time period. This function automatically filters repeated alarms in a short period of time, improving alarm handling efficiency and ensuring that important alarms are not missed.

Configure Alarm Aggregation Rule

1. Click **Add.**
2. Select alarm source and alarm type, and set the aggregation time (0s-1800s; repeated alarms within this period are automatically aggregated and the total alarm count will be recorded).

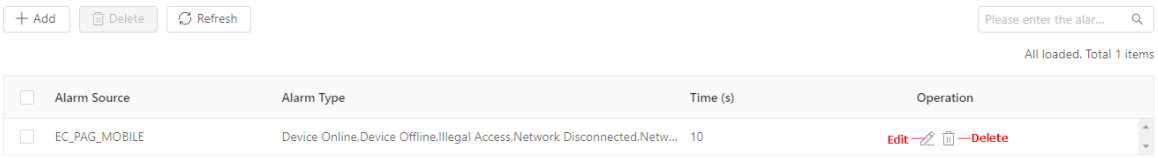
Figure 28-4: Add Rule



3. Click **OK**.

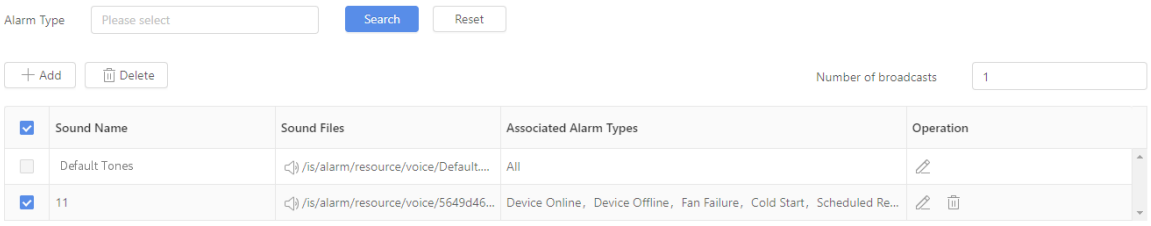
You can search, edit (alarm type/time), or delete configured rules.

Figure 28-5: Rule List



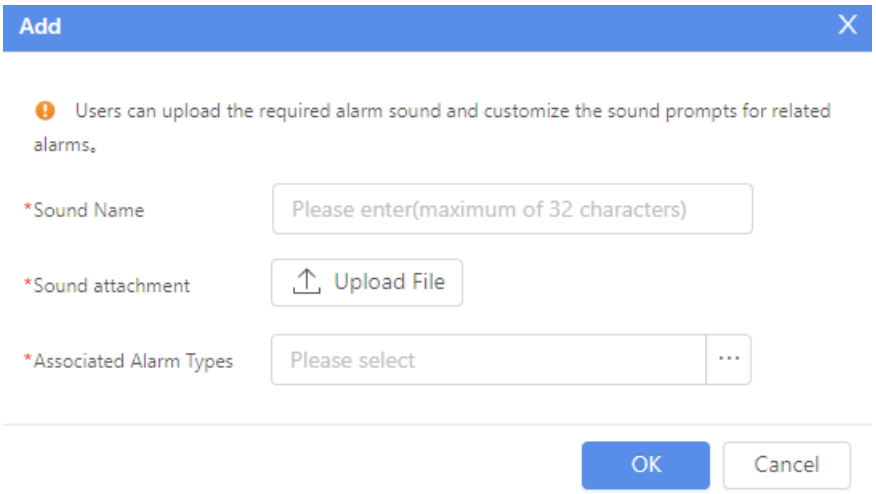
28.1.3 Alarm Sound

Configure alarm sounds for alarms to remind users to promptly check alarms.



Add Alarm Sound

1. Click **Add**.



2. Click **Upload File**, select a sound to upload. Click to listen, click **Reupload** if you need change the sound.

   Note:
   The file supports .mp3 and .wav formats, with a maximum allowed size of 30 MB.

3. Click ... , select alarm types.

   Note:
   Each alarm type can only be associated with one alarm sound.

4. Click **OK**

Configure play times

In the upper-right corner of the page, modify the number of times the alarm sound plays. After making the changes, click anywhere in the blank area of the interface to save the settings.

Note:
The play times setting applies uniformly to all alarm types.

Search alarm sounds

Select the alarm type and click on **Search** to query the alarm sound associated with that particular alarm type.

28.1.4 Alarm Linkage

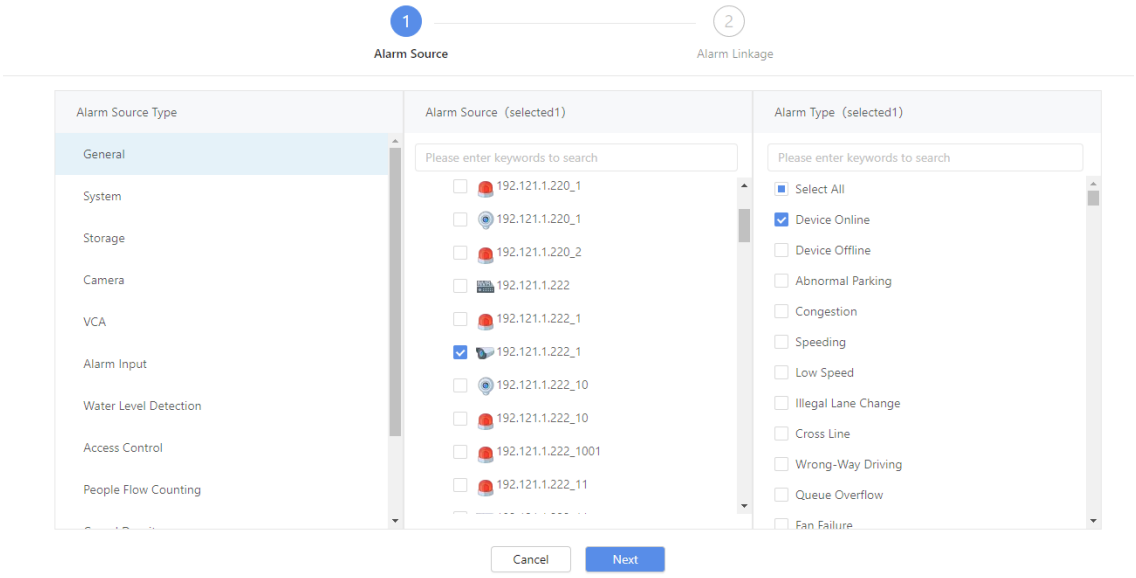
Configure alarm linkage to automatically trigger actions on linked devices (e.g., display live video on a video wall, access control) when an alarm is generated. This allows users to promptly perceive and review alarm events. The system also supports the use of time templates to define the active periods for alarm linkage, preventing activations during designated "Do Not Disturb" hours.

28.1.4.1 Alarm Linkage Configuration

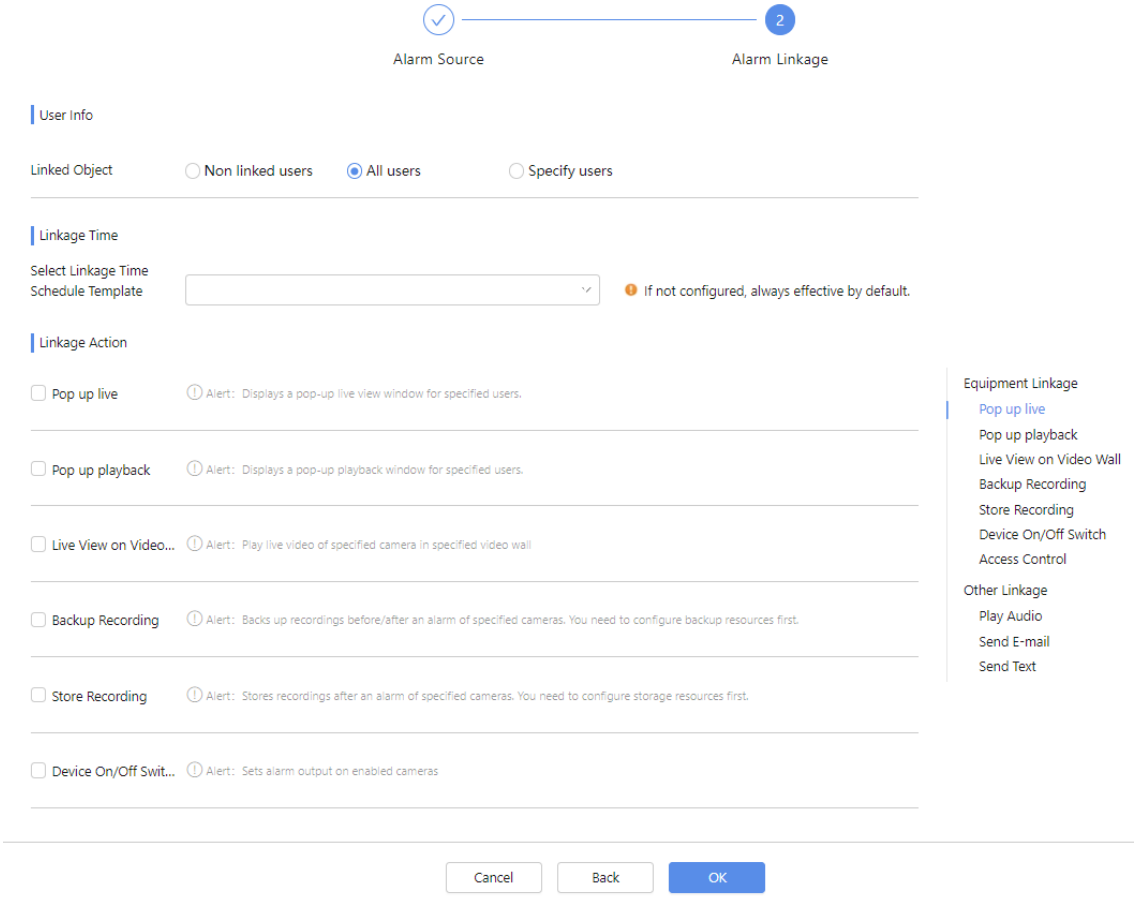
Configure linkage actions based on different alarm types from the alarm source.

Configure Alarm Linkage

1. Click **Add**. A page as shown below appears.
2. Select the alarm source type, alarm source, and alarm type. (Only supported alarm types for the selected source type will be displayed.)

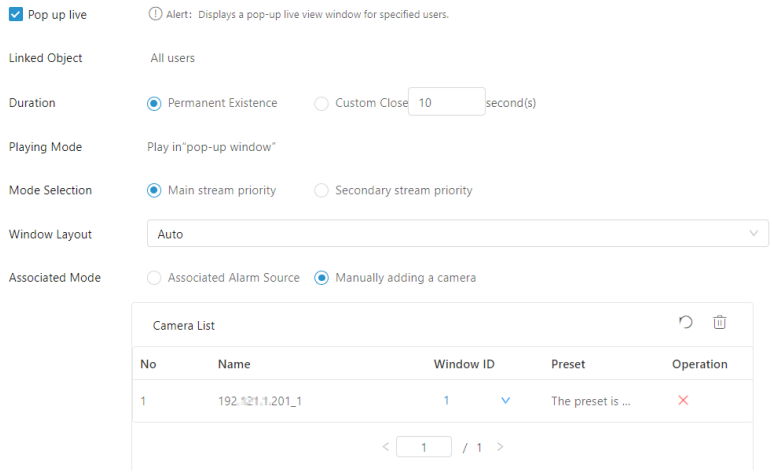


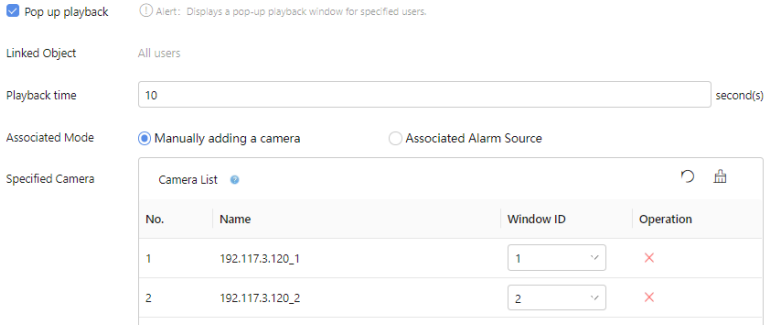
3. Click **Next** to configure alarm linkage. When an alarm occurs, the corresponding linkage actions are triggered.



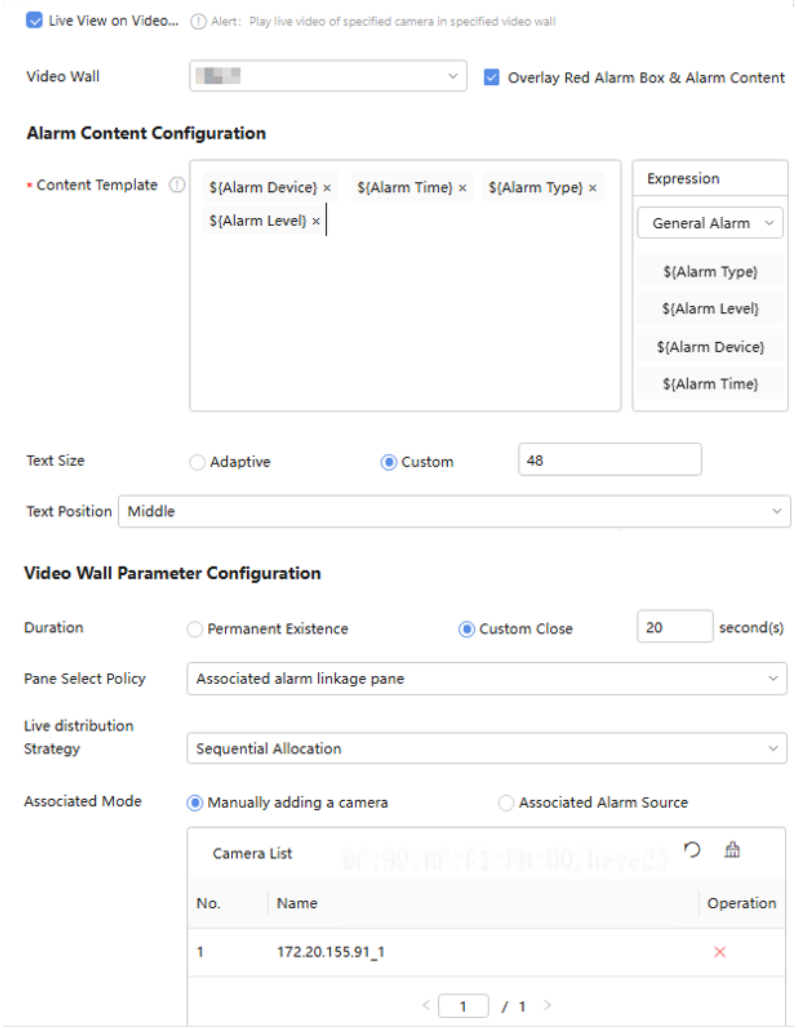
Item		Description
User Info	Linked Object	Trigger action for the selected user(s) or all users when the selected alarm source reports an alarm. • Non linked users: No users are linked. Only Live View on Video Wall, Backup Recording, Store Recording, Device On/Off Switch, Access Control, and Send E-mail are available for linkage. • All users: Link all users logged into the same server. • Specify users: Link selected users only (up to 32 users).

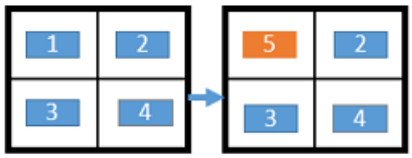
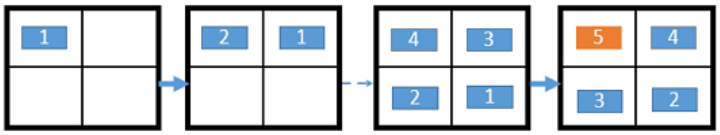
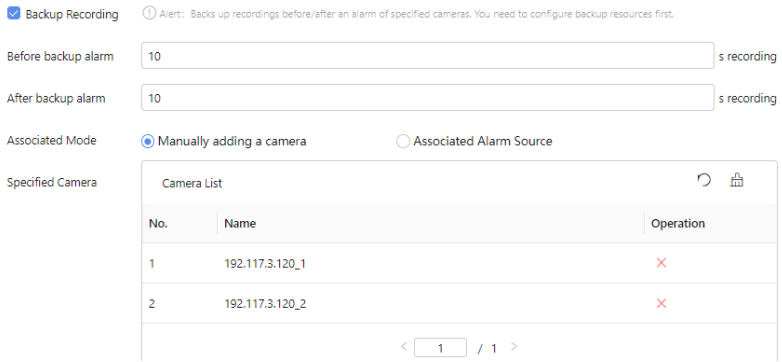
Item		Description
Linkage Time	Select Linkage Time Schedule Template	Select an alarm linkage Time Template. The alarm linkage will only be active during the periods defined in the template. Alarms generated outside these scheduled times will not trigger the linked actions If no template is configured, the linkage is always active by default.

Linkage Action	Pop up live	Displays a pop-up live view window for specified users.
		 
		• Duration: Set the window to display permanently or close after the specified duration.
		• Playing Mode: The pop-up live view window will overlay on any client interface.
		• Mode Selection: Select a stream (main/sub stream) for live view.
		• Window Layout: Auto (based on the number of cameras), or specified (1/4/9/13).
		• Associated Mode: Select which camera(s) to play live view.
		  • Associated Alarm Source: Play the live view of the alarm source.
		  • Manually adding a camera: Select camera(s) and specify each camera's live view window and preset.
		• Text Overlay: Custom text information that can be overlaid on the live view.

	Pop-up Playback	Displays a pop-up playback window for specified users.
		 
		• Playback time: Set the duration of the playback window. Recordings of N seconds before an alarm will be played.
		• Associated Mode: Select which cameras for playback.
		  • Manually adding a camera: Add multiple cameras and specify the playback window for each.
		  • Associated alarm source: Play back the recording from the camera that triggered the alarm itself.

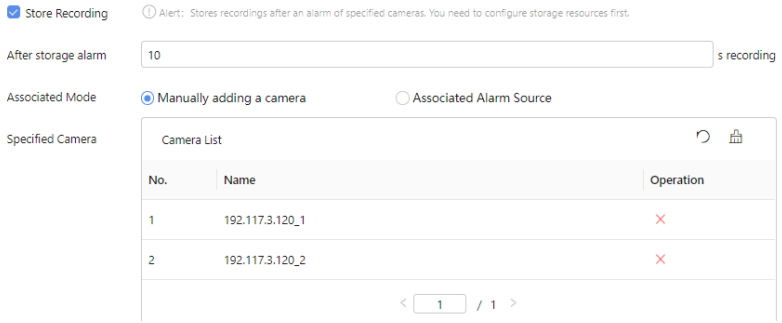
Item		Description

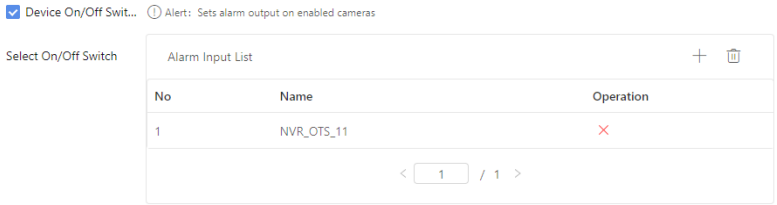
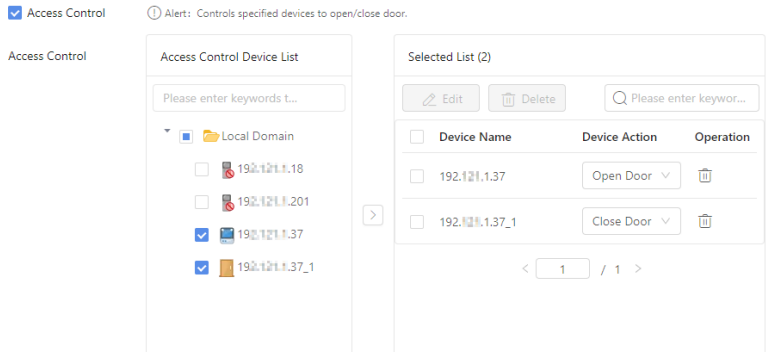
	Live View on Video Wall	Plays live videos of specified camera on a specified video wall.
		 
		
		• Video Wall: Select a video wall for live videos.
		• Overlay Red Alarm Box & Alarm content: When selected, a red frame will appear around the alarm linkage window, and the alarm content will be displayed on the window.
		• Alarm content: You can select fields for the expression (the fields will be replaced with specific alarm information when an alarm is triggered), or add your own description. You can also set the text size/position as needed.
		  • Expressions are divided into:
		  • General alarms: Alarm type, alarm level, alarm device, alarm time.
		  • Vehicle events (only valid for vehicle alarms): License plate number, owner's name, vehicle speed.
		  • Text size: Choose adaptive or custom text size.
		  • Text position: The position of the text in the alarm linkage window (top, middle, bottom).
		• Duration: The duration for which the live videos is displayed on the wall. After the time limit, the linked live videos will be closed and the original videos in the windows will be restored.
		• Pane Select Policy (window selection strategy): Configure windows/split screen for live view display.
		  • Fixed First pane (fixed first window): All cameras' live videos are played in the first opened window (window ID is 1).

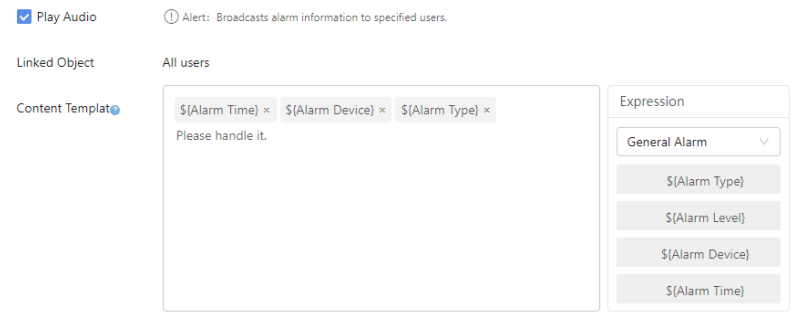
Item		Description
		• Associated alarm linkage pane (Associate alarm linkage window): After specifying alarm linkage windows on the video wall, camera's live videos will be played in these windows. • Custom pane List (custom window list): Add window(s) and specify the layout (one window can be split into multiple windows). • Live Distribution Strategy: Select the camera assignment sequence for specified windows/split screens (windows/split screens are specified in Window Selection Strategy) • Sequential Allocation: Cameras will be assigned sequentially to specified windows or split screens, overwriting existing content in windows. If camera count exceeds the window count, newly added cameras will overwrite the earliest displayed cameras.  • First Pane First (first split window priority): The newest camera video will be assigned to the first split screen of the specified window, pushing the original first video to the second split screen, and so on. If camera count exceeds the window count, the earliest displayed camera will be removed. **Note:** This strategy cannot be selected when using the Custom Pane List configuration.  • Free Pane Priority (idle split screen priority): Cameras' live videos are assigned to idle split screens in sequence. If no idle split screens, they will preempt other windows. If the camera count exceeds the window count, newly added cameras will overwrite the earliest displayed cameras. • Associated Mode: Select which camera(s) to play live view. • Associated Alarm Source: Play the live view of the alarm source. • Manually adding a camera: Select camera(s).
	Backup Recording	Back up recordings before/after an alarm of specified cameras. You need to configure backup resources first.  • Back up recordings from N seconds before the alarm to N seconds after the alarm.

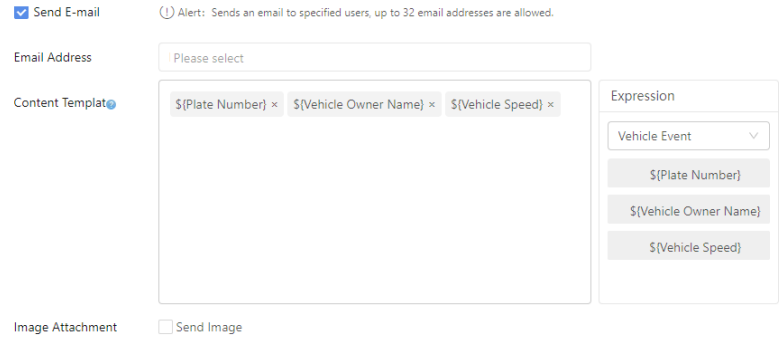
Item		Description

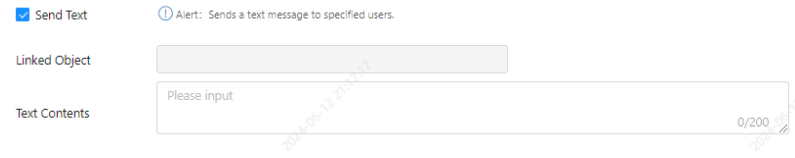
		• Associated Mode: Select which cameras for recording backup.
		  • Manually adding a camera: Add multiple cameras.
		  • Associated alarm source: Back up the recording from the camera that triggered the alarm itself.

	Store Recording	Store recordings after an alarm from specified cameras. You need to configure storage resources first.
		 
		
		• Store N seconds of recordings after the alarm.
		• Associated Mode: Select which cameras for recording storage.
		  • Manually adding a camera: Add multiple cameras to store their recordings.
		  • Associated alarm source: Store the recording from the camera that triggered the alarm itself.

	Device On/ Off Switch	When an alarm occurs, turn on the alarm output of the camera. 
	Access Control	When an alarm occurs, the specified access control devices can be controlled to open or close door.  • Access control device: Select face recognition terminal(s), general access control device(s), and access controller(s) from the left-side list and add them to the selected list. • Device action: Open Door, Close Door, Keep Open, Keep Closed, Restore (restore door from keeping open/closed).
	Play Audio	Broadcasts alarm information to specified users. For broadcast contents, you can choose from the provided expressions (which will be replaced with the specific alarm information) or enter custom descriptions.

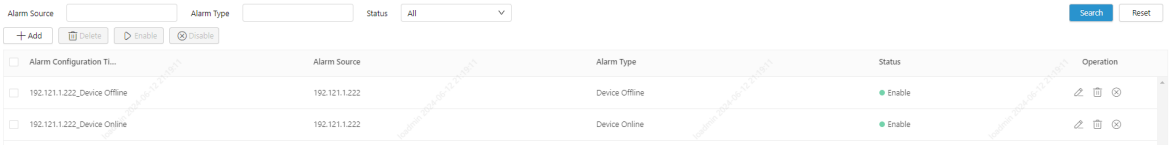
Item		Description
		 Supported expression types: • General Alarm: Alarm Type, Alarm Level, Alarm Device, and Alarm Type. • Vehicle Event (only applicable to vehicle event alarms): Plate Number, Vehicle Owner Name, and Vehicle Speed.

	Send E-mail	Sends an email to specified users.
		 
		Note:
		Before using this function, you need to configure the email server and contacts first. See System Config > Service Config > Email.
		• Email Address: Select email addresses (up to 32 email addresses).
		• Content Template: you can choose from the provided expressions (which will be replaced with the specific alarm information) or enter custom descriptions.
		Supported expression types:
		  • General Alarm: Alarm Type, Alarm Level, Alarm Device, and Alarm Type.
		  • Vehicle Event (only applicable to vehicle event alarms): Plate Number, Vehicle Owner Name, and Vehicle Speed.
		• (The configuration is displayed only for vehicle event alarms)If want to attach vehicle alarm snapshot in the email body, you can select **Send Image**.

	Send Text	Sends a custom text message (displayed in a pop-up window) to specified users. 

Manage Alarm Linkage

You can edit, delete, enable, disable alarm linkages. Linkages must be enabled to take effect.



- Edit: Click in the **Operation** column to modify alarm linkage configuration.
- Delete: Click in the **Operation** column or select linkage(s) and click **Delete** above the list, and then confirm the deletion.
- Enable alarm linkage: Click in the **Operation** column or select linkage(s) and click **Enable** above the list to enable the linkage.
- Disable alarm linkage: Click in the **Operation** column or select linkage(s) and click **Disable** above the list to disable the linkage.

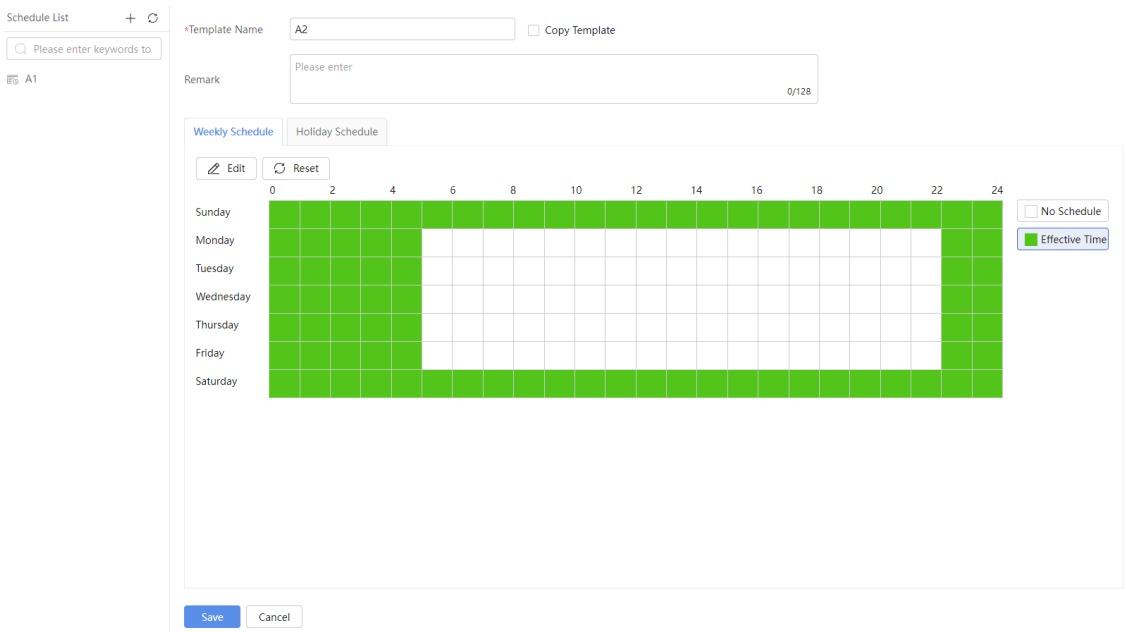
28.1.4.2 Time Template

A time template defines the active periods for alarm linkage configurations. Linkage actions will only be executed for alarms that occur within the scheduled time defined in the template. Pre-configuring time templates allows for quick selection when setting up alarm linkage, improving configuration efficiency.

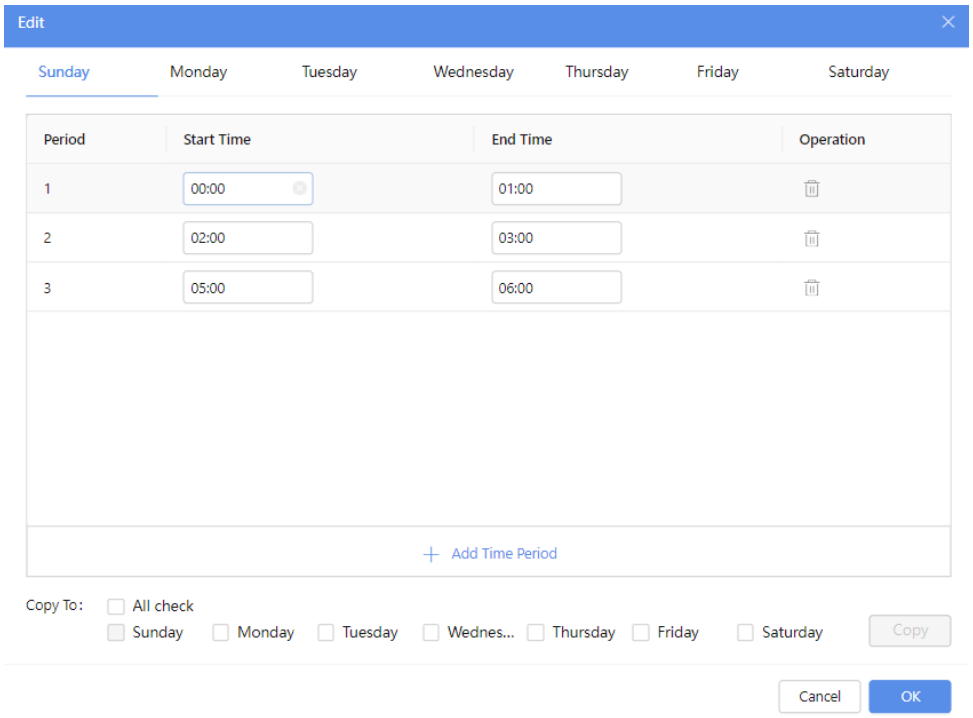
Note:
A time template consists of two parts: a weekly schedule and a holiday schedule. The weekly schedule governs alarm linkage during regular days, while the holiday schedule takes priority during holidays. For example, if a holiday is configured as Do Not Execute Linkage Actions, linkage will not be triggered during that period, even if it falls within an active time slot in the weekly schedule.

Add a New Time Template

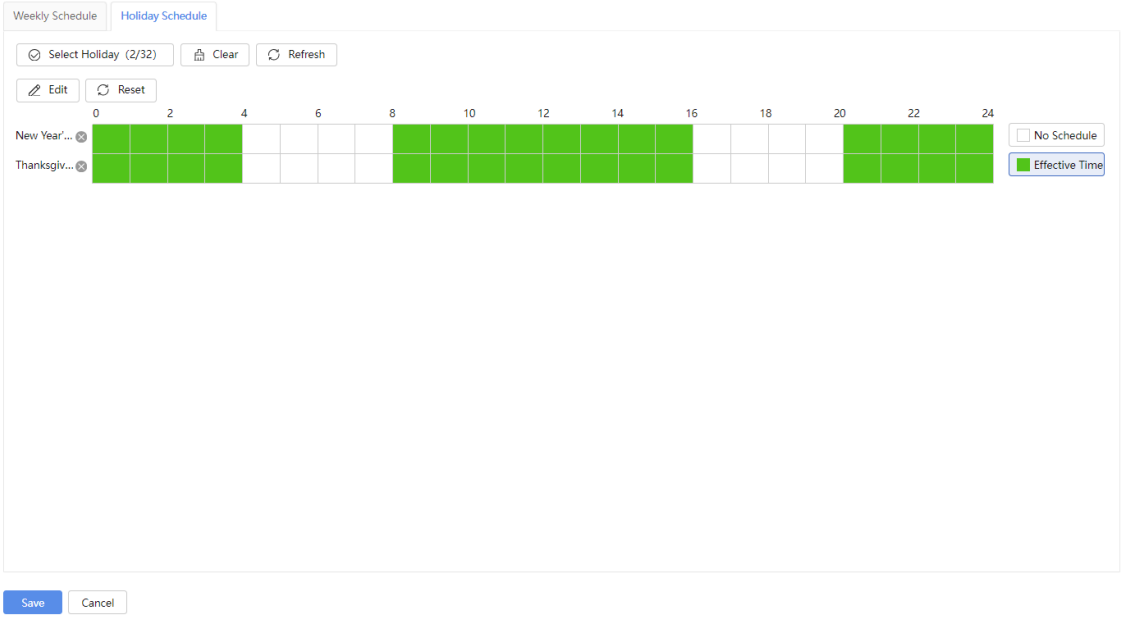
1. Click + to add a new time template.
2. Configure the **weekly schedule**.



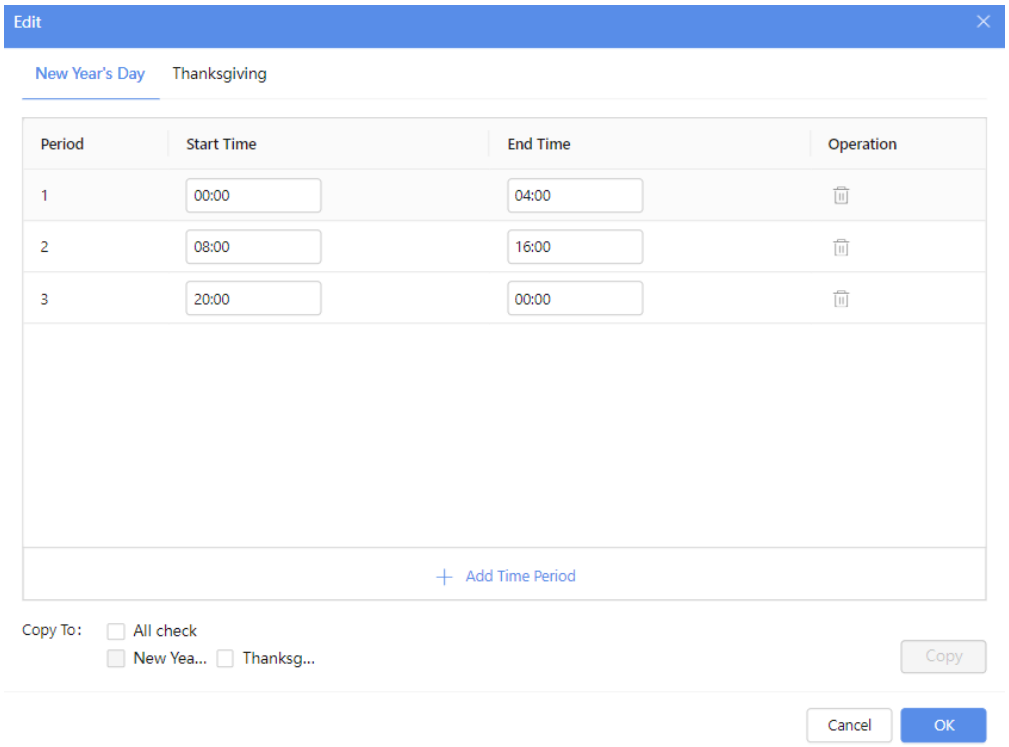
No.	Description
1	Enter a template name.
2	Select **Copy Template** to select an existing template. Its time configuration will be copied to the new template for further editing.
3	Configure effective time periods using one of two methods. • Click **Effective Time** or **No Schedule**. On the time chart, click or click-and-drag to define periods. Each block represents one hour.

No.	Description
	Note: White blocks (No Schedule) indicate periods where linkage is inactive. Green blocks (Effective Time) indicate periods where linkage is active. • Click **Edit** to manually add up to 12 precise time periods (to the minute) per day. After configuring one day, you can select other days and click **Copy To** to apply the same schedule for quick setup. 
4	Click **Reset** to clear all configured time periods for the current template. |

3. (Optional) Configure the **holiday schedule**.



No.	Description
1	Select Holidays. (Holidays are created in **System Configuration > Service Configuration > Holiday Management**) • A maximum of 32 holidays can be selected per template.

No.	Description
	• Click ⊗ next to a selected holiday to remove it.
2	Click **Edit** to set precise active time ranges (up to 12 per day) for each selected holiday.  After configuring one holiday, select other holidays and click **Copy To** to apply the same schedule.
3	Click **Clear** to remove all selected holidays from the current template.
4	Click **Reset** to clear all configured time periods for holidays in the current template.
5	Click **No Schedule**, click or click-and-drag on the time chart to erase periods (set as inactive).
6	Click **Effective Time**, click or click-and-drag on the time chart to draw periods (set as active).

4. Click **Save** to complete the configuration.

28.2 Real-time Alarm

View device resource points and device alarms on the map. You can also perform operations on devices and manage resources on the map visually, which provides you with an immerse operating experience.

Operation entry: Click the in the upper-right corner of the main interface

Prerequisite

By default, the system marks all devices on the background image.

To display devices on the actual map, bind the area map and mark device locations on the Edit Map page.

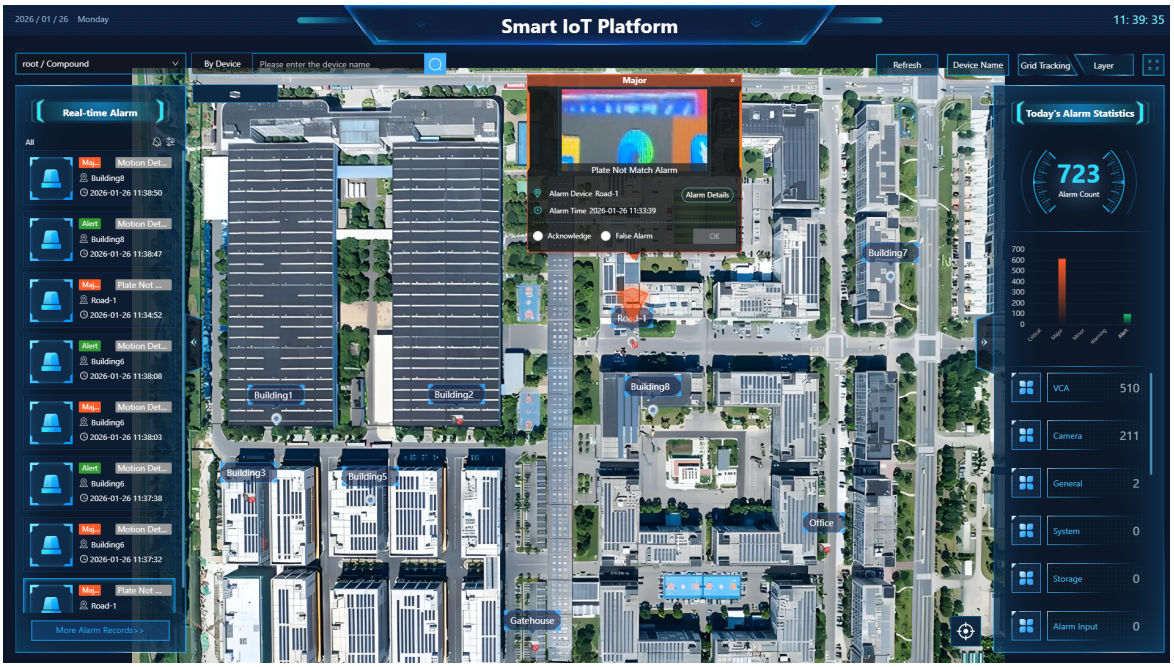
Map Overview

By default, the page shows the default floor of the root area.

Click the map list in the upper-left corner of the map to select the map of an area.

Click on the floor list in the map's upper-left corner to switch to the map of the desired floor.

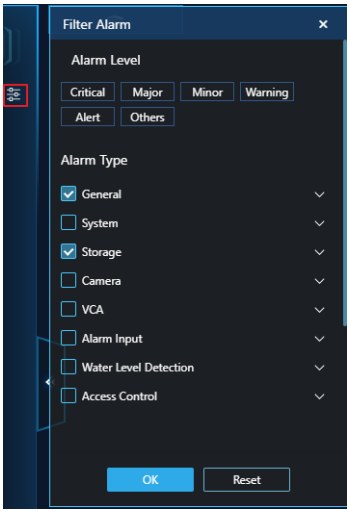
Device points and alarm information are displayed on the map.



Note:

- You can use the scroll wheel to zoom in or out on the map, or hold and drag the left mouse button to move the map.
- Click in the map's lower-right corner to restore the default perspective.
- Click in the map's upper-right corner to enlarge to the full screen. The screen name support customization, see Map Display Configuration.

Table 28-1: GUI Introduction

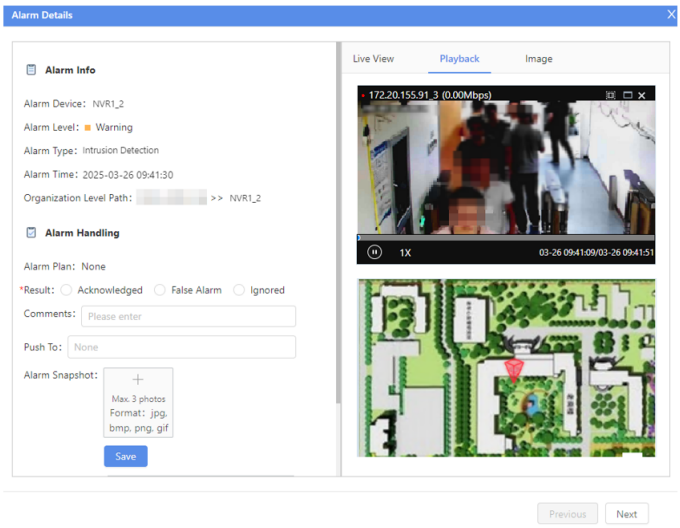
Tab	Description
Realtime Alarm	The left-side realtime alarm pane shows the latest 20 alarms. Alarms are sorted by time, with the latest alarm at the top. • You can click to filter alarm types to be displayed.  • Click **More Alarm Records** to go to the Alarm Records page.
Alarm Details	• Click an alarm card to switch to the map where the device is located, locate the device on the map, and show alarm handling operation panel. • Double-click an alarm card to view alarm details.

Tab	Description
Today's Alarm Statistics	Display the total number of alarms reported today, and the number of alarms that are classified by alarm level/alarm type. **Note:** The number of alarms reported today is counted in real time; the data is cleared in the early morning of the next day.

Alarm handling

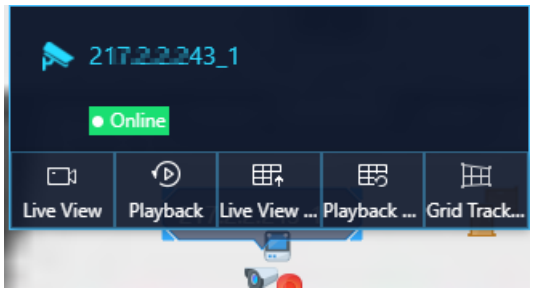
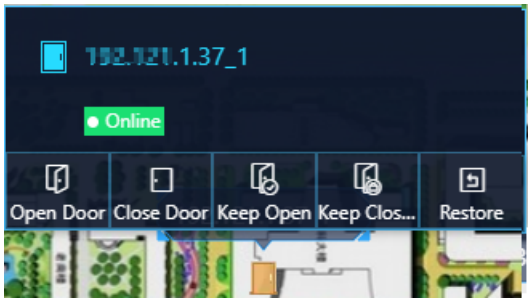
In the realtime alarm list, you can click an alarm card to locate the alarm on the map and display the alarm handling panel.

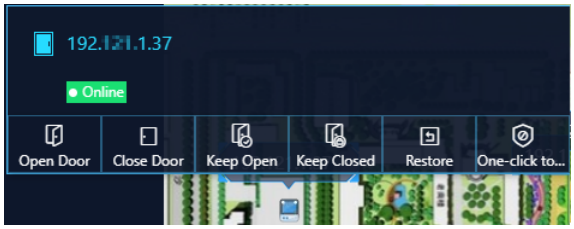
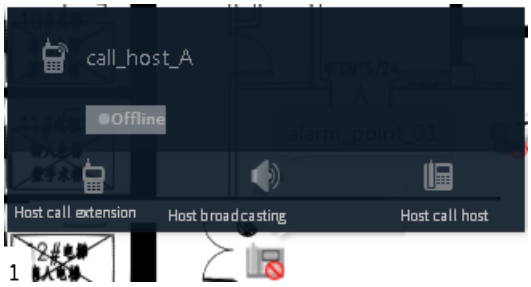
Table 28-2: Alarm Handling Operations

Operation	Description
View alarm details	Click **Alarm Details** to view alarm details and perform the following operations.  • View the device on the map, its live and recorded video and images, and alarm information. • Verify to acknowledge or discard the alarm, and give a comment. • Choose a user and forward the alarm to the user. • Upload alarm images for archiving.
Acknowledge alarm	If the alarm is valid, select **Acknowledge Alarm** and then click **OK** to set it as a valid alarm.
Discard alarm	If the alarm is false, click **False Alarm** and then click **OK** to discard it.

On-map device operations

Click the device to view the operations allowed. For example:

<table>
<tr>
<td>Camera: View live or recorded video, play video on the video wall.
 
</td>
<td>Face recognition terminal/General access control device/Access controller: Open door, close door, keep door open, keep door closed, restore door from keeping open/closed.
Face recognition terminal: You can clear the alarm-triggered action on the device if the alarm is false. Additionally, you can click in the left-side alarm list to clear alarms on all access control devices in batches.
 


</td>
</tr>
<tr>
<td>Two-way audio: Make two-way audio calls.
 
</td>
<td>Temperature/humidity sensors: View historical data.
</td>
</tr>
</table>

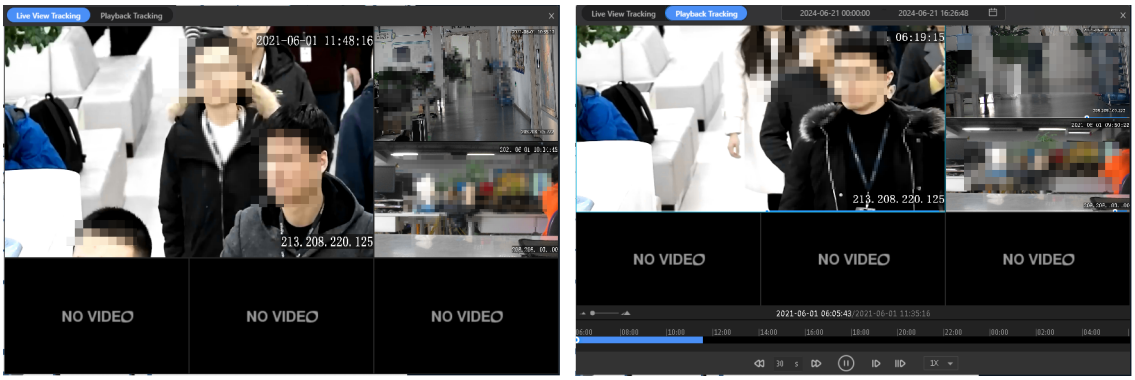
Note: If device points on the map are very close together, they will be aggregated and a number will be displayed to indicate the total number of aggregated devices.

Grid Tracking

Grid tracking lets you view live or recorded videos of neighboring cameras of a certain device.

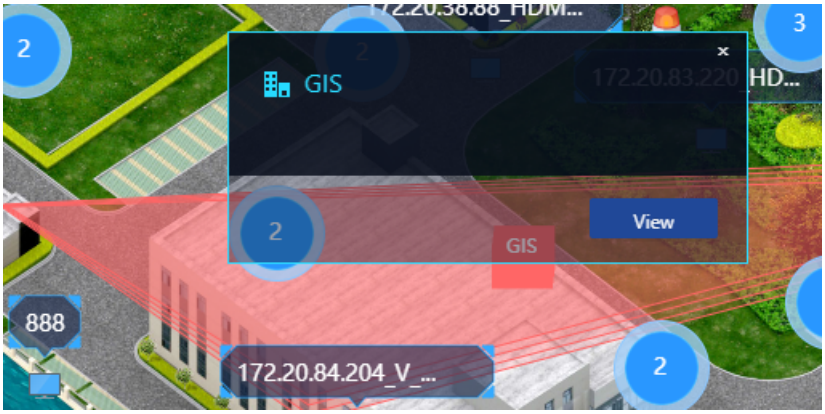
1. Click **Grid Tracking**, the cursor changes to .
2. Click the marked location on the map, the system will searches cameras around the specified location according to the straight line distance from near to far and plays video of the discovered cameras in the windows until all the windows are populated.

   Note: You can click the video image of a camera to start grid tracking again with that camera as the center.



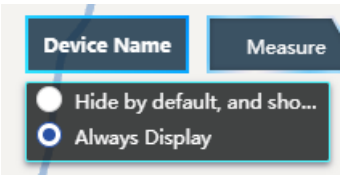
Heat Zone

Click on a heat zone to jump from the current area to another linked area.



Show/Hide Device Name

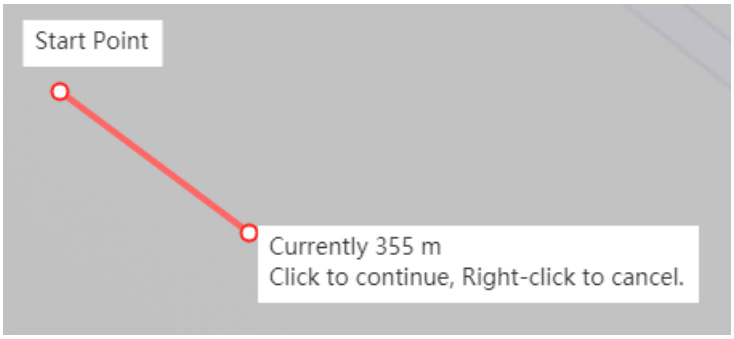
Click **Device Name** above the map to choose whether to display device names on the map.



Measurement

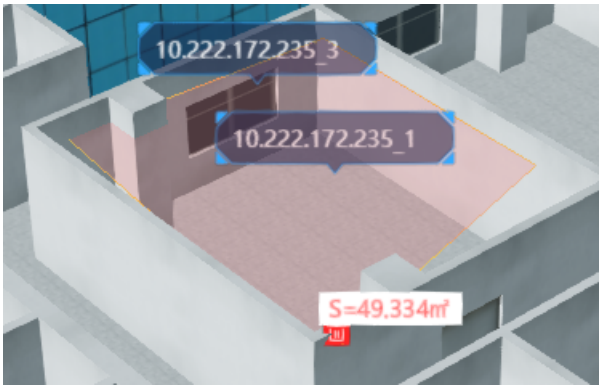
You can measure line distances and closed areas in the scene map.

- Measure distance: Marking points on the map to get the route distance from each point to the start point (the length of the whole route is displayed at the last point).
  1. Click **Measure** > **Measure Distance**.
  2. Hover the mouse over the map and left-click once to determine the start point. Then, draw the route by using the left button several times. Finally, right-click on the map to complete the drawing.



- Measure area: Marking points on the map to get the area of a closed figure.

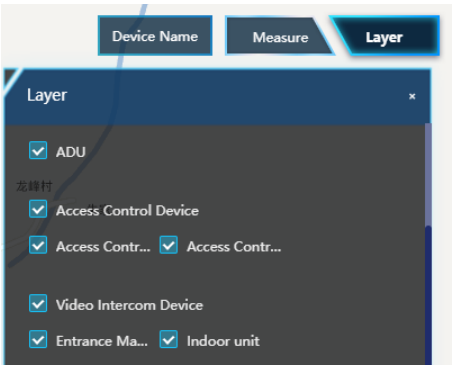
1. Click **Measure** > **Measure Area**.
2. Hover the mouse over the map and use the left button to draw a closed figure on the map. Finally, right-click on the map to complete the drawing.



Layer

Configure the types of device resources to be displayed on the map for a clearer view.

Click **Layer** in the upper-right corner and select the types of devices to be displayed on the current map.



Roaming Route

Note:
Only scene maps support roam path, see Roam Config.

1. Click **Roam Route** in the top toolbar to show the roam path list.
2. Click ▷ to view roam path, you can play a video of the roaming route in the map screen from the first viewpoint.

Panoramic View

Note:
Only scene maps support panoramic view, see Panoramic Config.

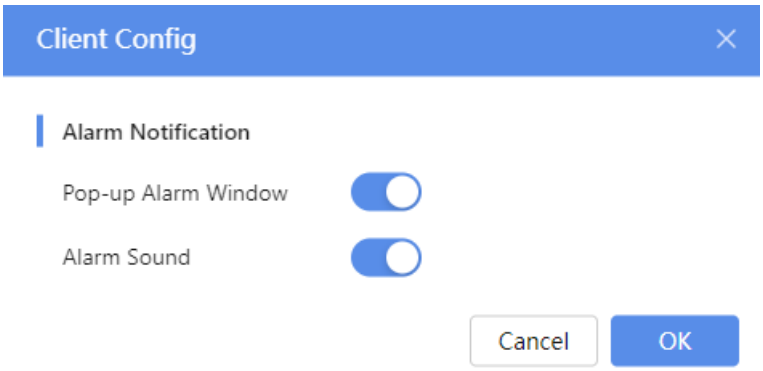
Click **Enable Panoramic View** in the top toolbar to start panoramic view, the model rotates around a central axis, allowing you to view all sides of the model.

28.3 Alarm Notification

When an alarm occurs, users can be notified by alarm pop-up window and alarm sound.

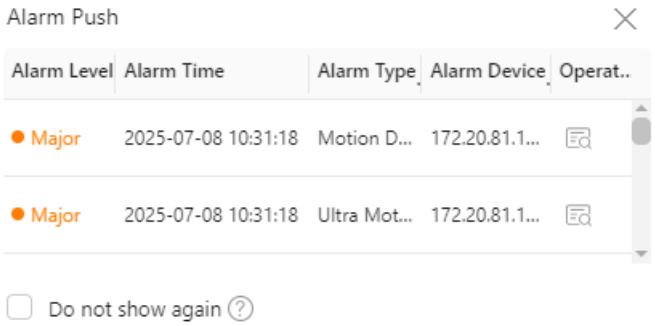
Prerequisite

Click ⚙ in the upper-right corner and select **Client Config**. You can choose whether to enable alarm sound and pop-up alarm window as needed.



Alarm Pop-up Window

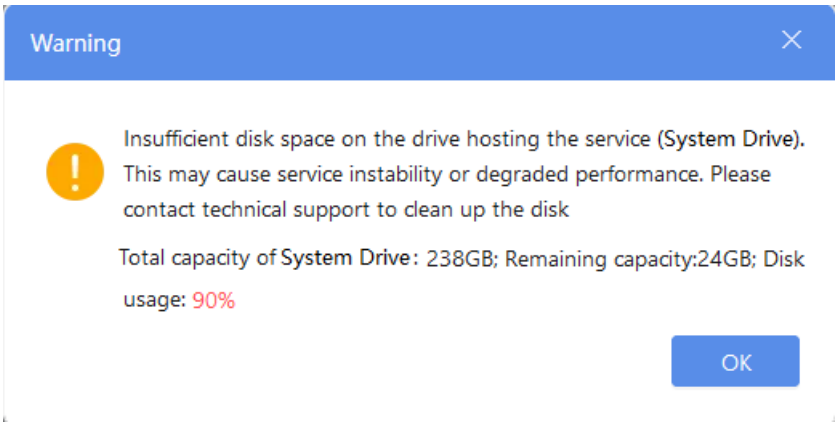
If enabled, when an alarm occurs, a pop-up window will appear in the lower-right corner of the page displaying alarm information and accompanies by an alarm sound.



28.4 Disk Full Alarm

When **the disk space on the drive hosting the service** becomes insufficient, it may cause service anomalies or performance degradation. The system will display a global pop-up alarm—please contact technical support to clean up the disk.

- Disk usage between 80%–90%: warning displayed in yellow text. Disk usage ≥90%: alarm displayed in red text.
- The disk full pop-up alarm cannot be disabled by the **Alarm Notification Settings** and will always appear on the top.
- After closing the alarm, the system will check disk usage every 3 minutes and re-trigger the alarm if usage remains at or above 80%. The alarm will stop only when disk usage falls below 80%.



28.5 Historical Alarm

Go to **Alarm Center > History Alarm**.

Search and handle historical alarms received by the system.

28.5.1 Alarm Records

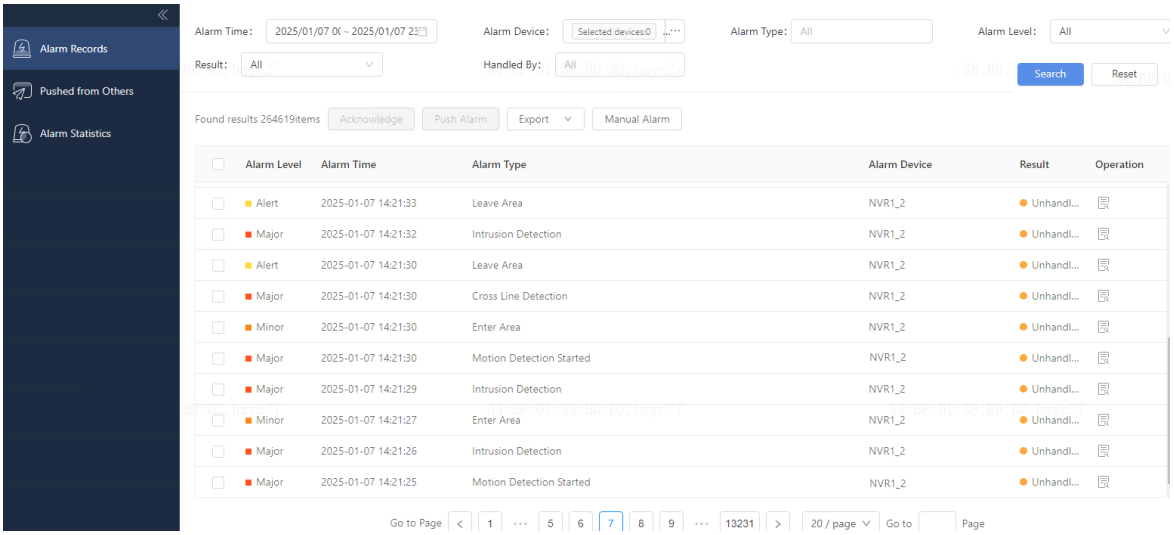
View historical alarm records and handle alarms.

Search Alarm

You can search alarms by alarm time, alarm device (default: all; or click ••• to select devices within permissions), alarm type, alarm level (critical/major/minor/warning/alert/others), handling result (unhandled/acknowledged/ false alarm/ignored), and user who handled the alarm.

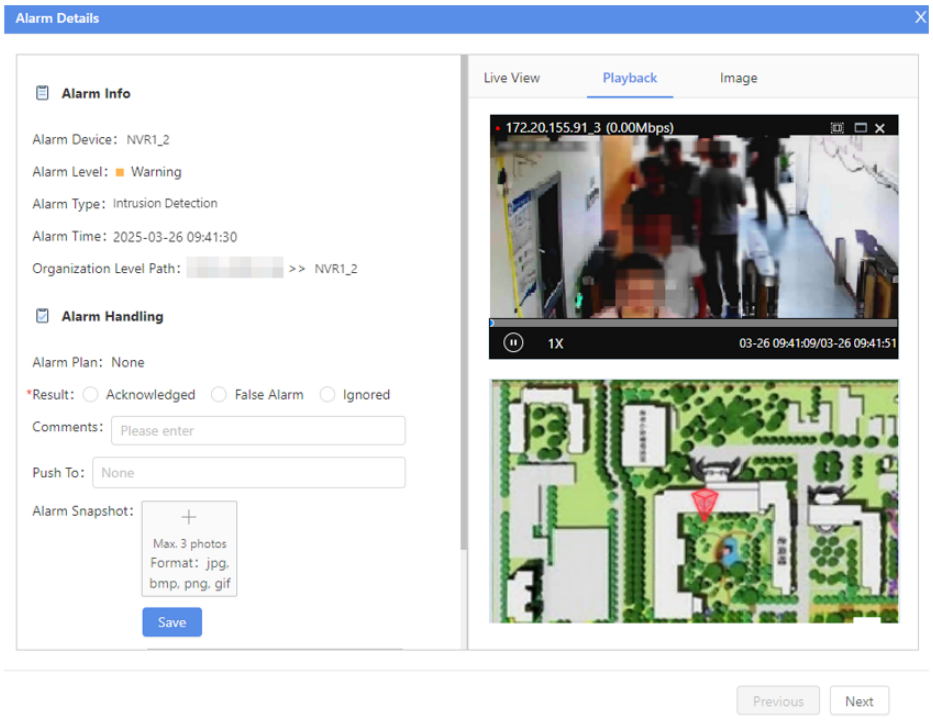
After setting the search criteria, click **Search** to display the alarm records that match the set search criteria.

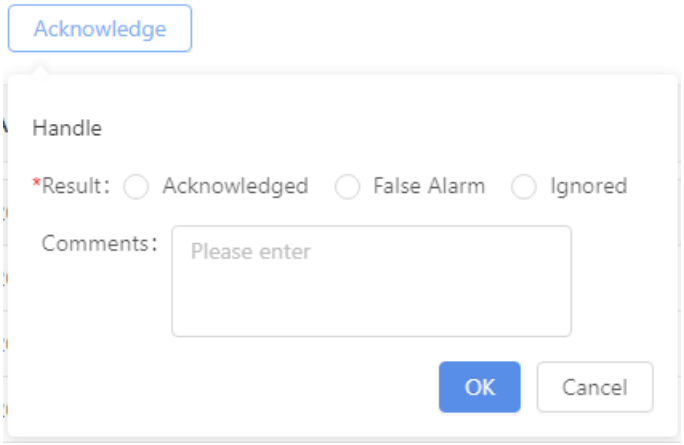
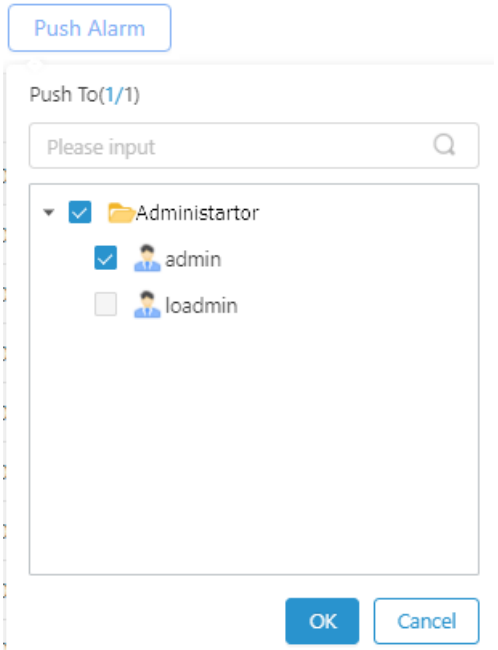
Figure 28-6: Historical Alarm Records

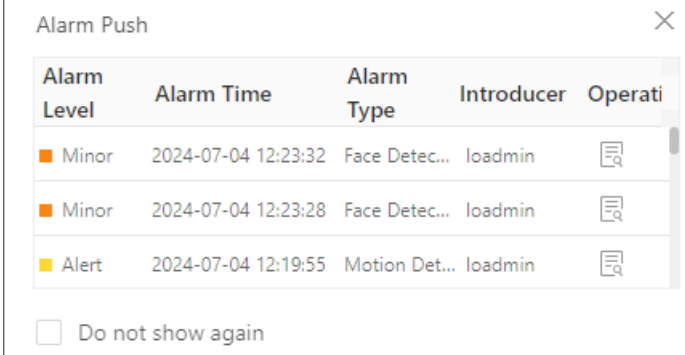
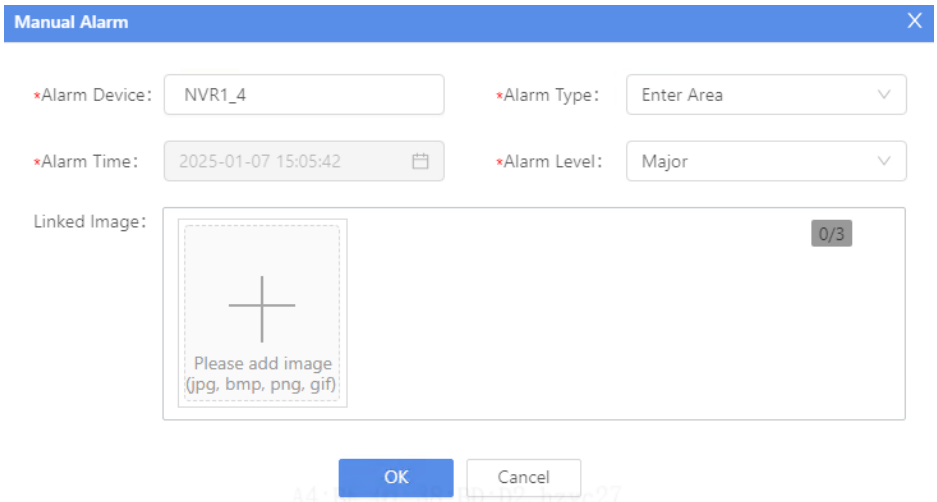


Handle Alarm

Table 28-3: Alarm Handling Operations

Operation	Description
View alarm details	Click for the alarm record to view alarm details.  The following operations are supported: • View the channel's location on e-map, live videos, recordings, snapshots, and alarm information.

Operation	Description
	For important person, face match, face not match, unauthorized area access, and unauthorized time access alarms, you can view the face snapshot and library information. For unauthorized alarms, you can also click **Track Trajectory** to redirect to the **Face Search** page to view the face trajectory. **Note:** • If there are no alarm images, the image tab is not displayed. • If the alarm device is not bound to a map, you can click **Bind Map** to quickly go to the **Map Configuration** page for binding. • Acknowledge alarm, mark the alarm as a false alarm, or ignore the alarm, and add handling comments. • Select user(s) to push the alarm. • Upload alarm snapshots.
Acknowledge alarm	Click **Acknowledge**/**False Alarm**/**Ignored** next to **Result** on the **Alarm Details** page or select alarm(s) in the alarm list and click **Acknowledge** to handle alarm. 
Push alarm	For example, when the administrators receive an alarm, they can push the alarm to other unauthorized users for alarm handling. Click the check box next to **Push To** in the **Alarm Details** page or select alarm(s) in the alarm list and click **Push Alarm**, and then select the alarm recipient(s).  When succeeded, the recipient will receive the corresponding pop-up alarm window.

Operation	Description
	
Export alarm	Select alarm(s) in the alarm list and click **Export** to export the selected alarm record(s) to local.
Manual alarm	Click **Manual alarm** above the alarm list and complete the alarm information.  After configuration, a manual alarm record will be added to the alarm list.

28.5.2 Pushed from Others

View alarms pushed from others and handle alarms.

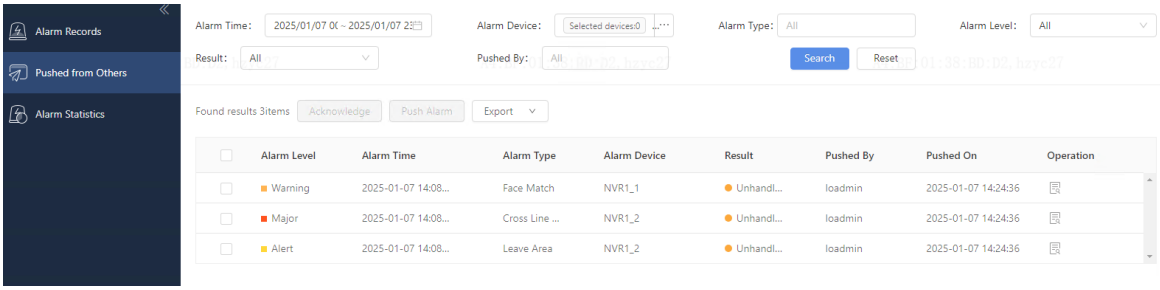
Note:
For push operations, please refer to Push alarm.

Search Alarm

You can search alarms by alarm time, alarm device (default: all; or click ••• to select devices within permissions), alarm type, alarm level (critical/major/minor/warning/alert/others), handling result (unhandled/acknowledged/ false alarm/ignored), and user who handled the alarm.

After setting the search criteria, click **Search** to display the alarm records that match the set search criteria.

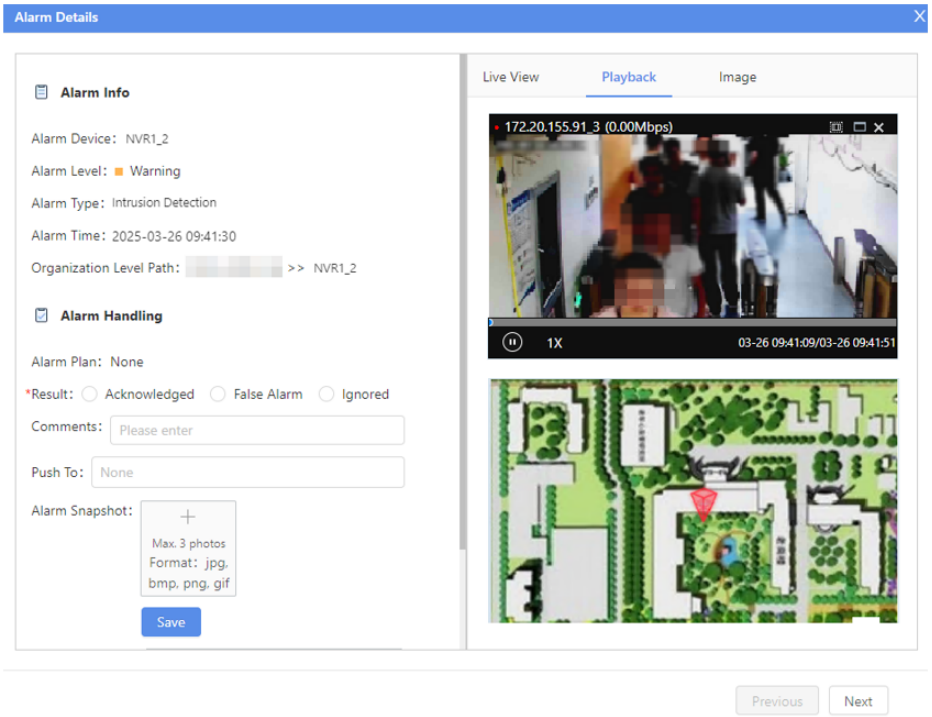
Figure 28-7: Alarm Records Pushed from Others

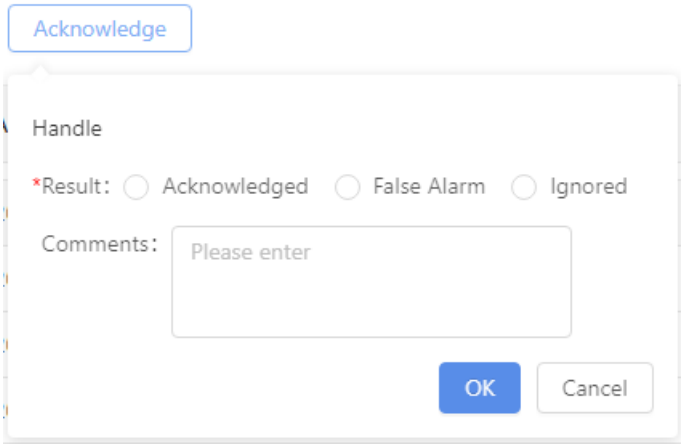
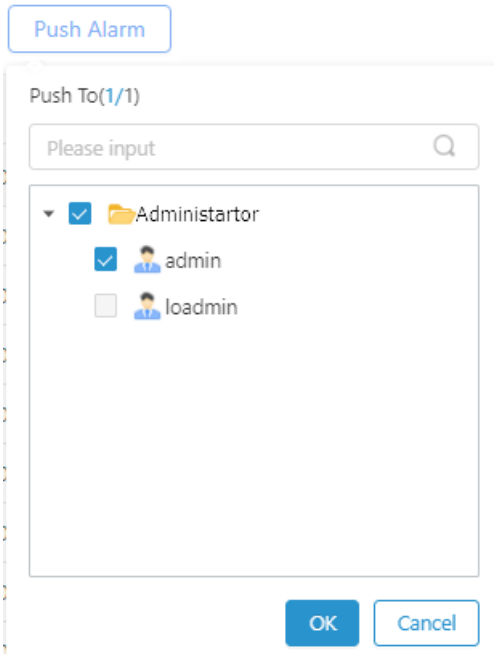
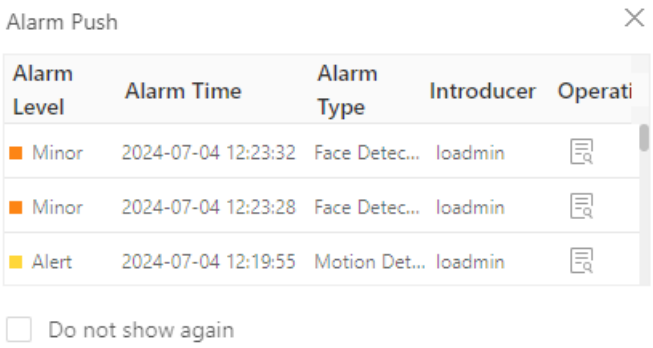


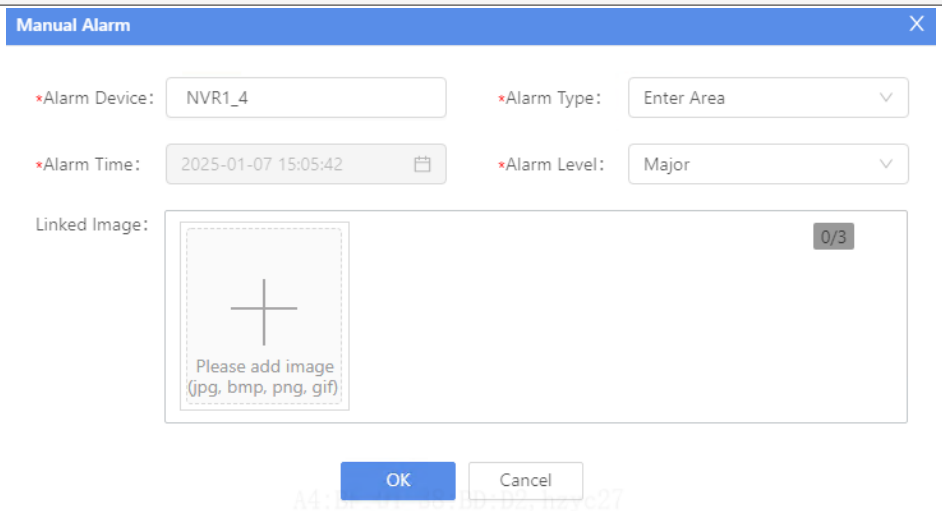
Note: On the **Pushed form Others** page, you can re-handle alarms that previously handled by others and update the handling result.

Handle Alarm

Table 28-4: Alarm Handling Operations

Operation	Description
View alarm details	Click for the alarm record to view alarm details.  The following operations are supported: • View the channel's location on e-map, live videos, recordings, snapshots, and alarm information. For important person, face match, face not match, unauthorized area access, and unauthorized time access alarms, you can view the face snapshot and library information. For unauthorized alarms, you can also click **Track Trajectory** to redirect to the **Face Search** page to view the face trajectory. **Note:** • If there are no alarm images, the image tab is not displayed. • If the alarm device is not bound to a map, you can click **Bind Map** to quickly go to the **Map Configuration** page for binding. • Acknowledge alarm, mark the alarm as a false alarm, or ignore the alarm, and add handling comments. • Select user(s) to push the alarm. • Upload alarm snapshots.
Acknowledge alarm	Click **Acknowledge**/**False Alarm**/**Ignored** next to **Result** on the **Alarm Details** page or select alarm(s) in the alarm list and click **Acknowledge** to handle alarm.

Operation	Description
	
Push alarm	For example, when the administrators receive an alarm, they can push the alarm to other unauthorized users for alarm handling. Click the check box next to **Push To** in the **Alarm Details** page or select alarm(s) in the alarm list and click **Push Alarm**, and then select the alarm recipient(s).  When succeeded, the recipient will receive the corresponding pop-up alarm window. 
Export alarm	Select alarm(s) in the alarm list and click **Export** to export the selected alarm record(s) to local.
Manual alarm	Click **Manual alarm** above the alarm list and complete the alarm information.

Operation	Description
	 After configuration, a manual alarm record will be added to the alarm list.

28.5.3 Alarm Statistics

View alarm trends and the count of each alarm type by time and device.

- Statistical criteria: Supports statistics by time (by day/week/month) and device (default: all; or click ••• to select devices within permissions).
- Statistical charts: Includes a trend chart by time and a bar chart of alarm counts by alarm type. Hover the mouse over the chart to display the alarm count within that time period.
- Detailed data: Displays the detailed number of alarms reported.

Figure 28-8: Alarm Statistics-Trend Chart

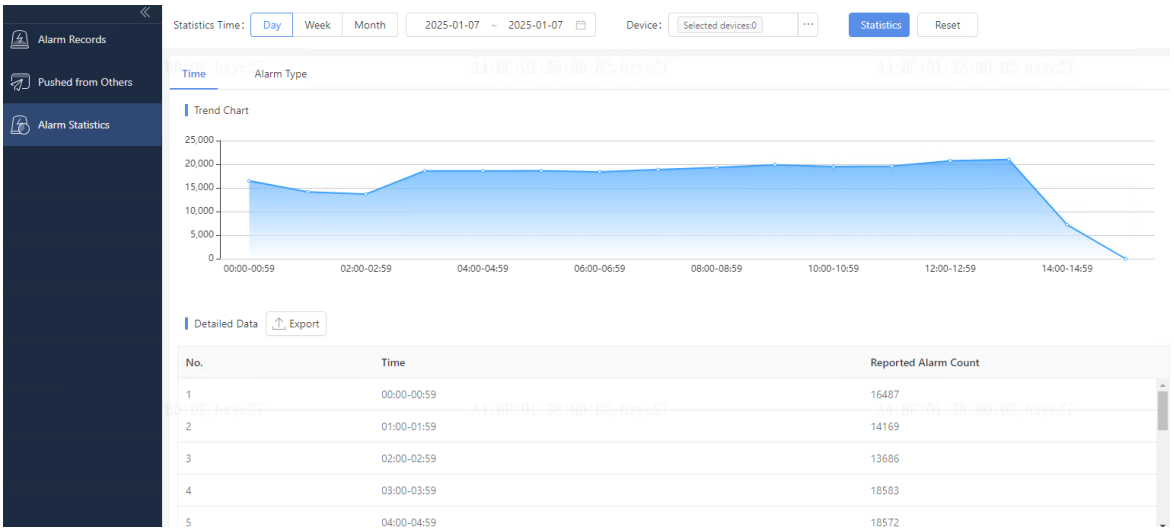
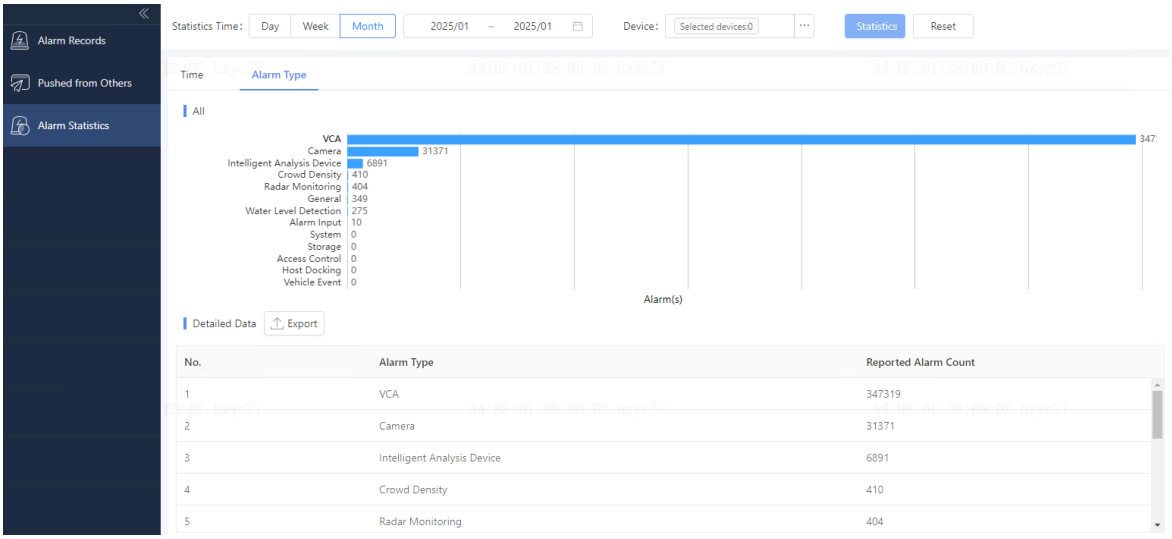
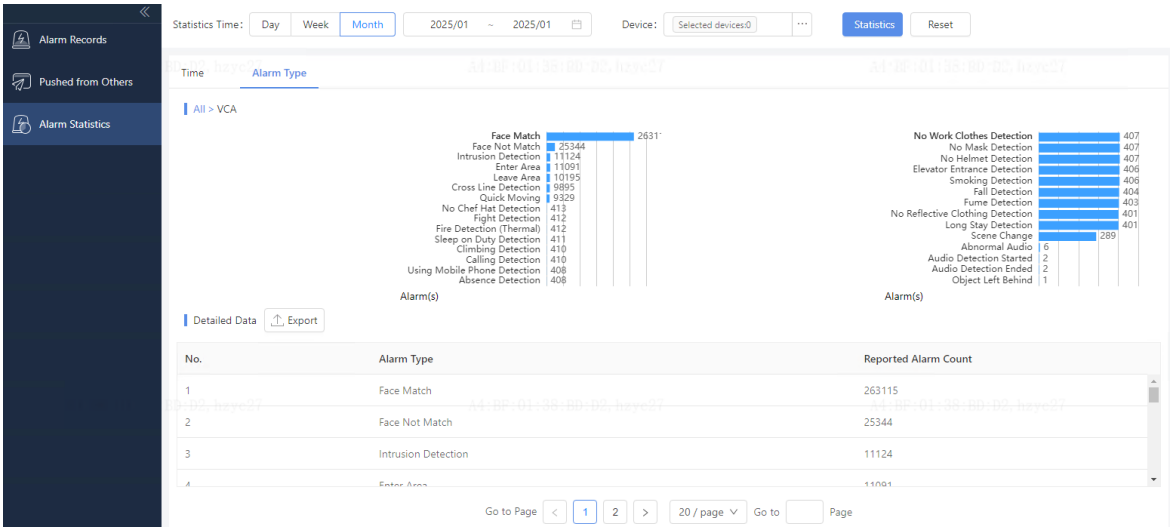


Figure 28-9: Alarm Statistics-By Alarm Type



For the bar chart, click on the bar to view the specific alarms under that type. For example, the following displays the subtype statistics for service-related alarms.

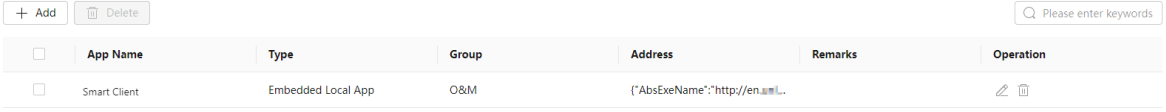
Figure 28-10: Alarm Subtype Statistics



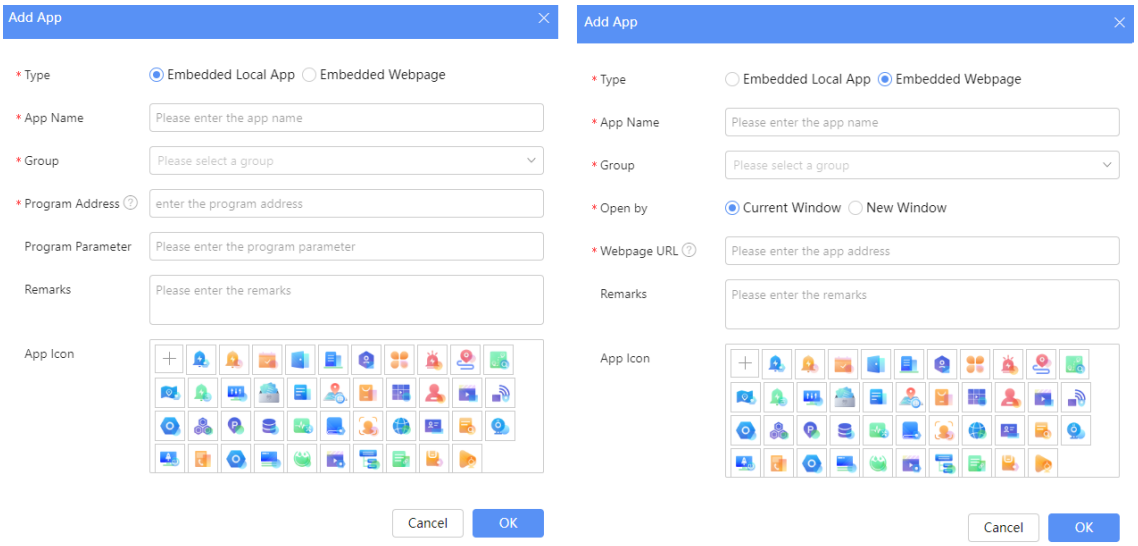
29 System Configuration

29.1 Third-Party Application

You can add third-party applications (webpage or program) to the platform so you can open them on the platform as a function menu directly.



1. Click **Add**.



2. Choose to add a program or a webpage. For detailed operation descriptions, please refer to the on-screen instructions.
   - Embedded program: Enter the program address and startup parameters. The program (e.g. a client) must be installed on the local PC.
   - Embedded webpage: Enter the URL (e.g. http://www.google.com/). The webpage must be can accessed in Google Chrome.
3. Click OK. When added, you can view the application in **Function Navigation** on the homepage.

29.2 Platform Cascading

Build a multi-domain networking environment to enable lower-level platforms to share resources with upper-level platforms.

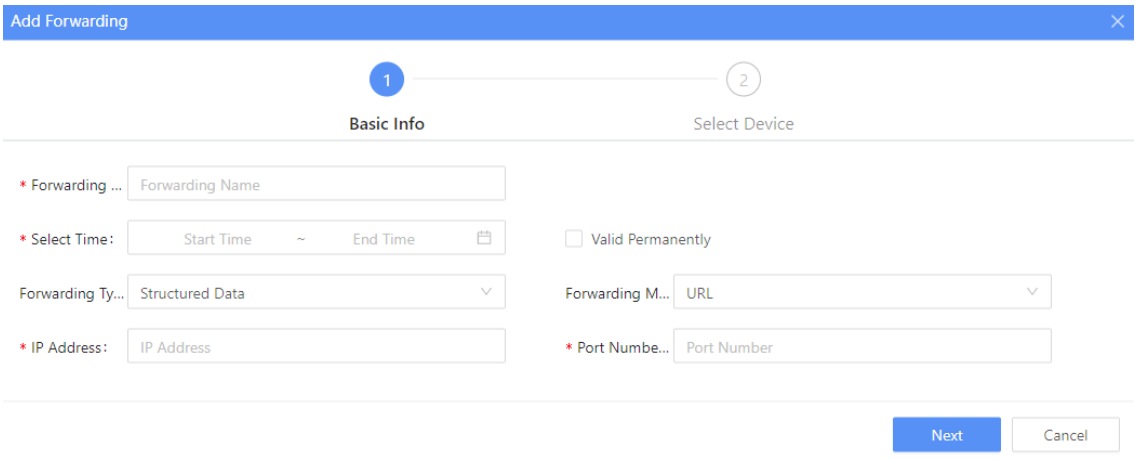
29.2.1 Private Cascading

Go to **Platform Cascading> Private Cascading**.

Forward platform data to a certain address via the private protocol (OpenAPI).

Add Forwarding

1. Click **+New**.



2. Enter the basic information.

Item	Parameter
Forwarding name	Customize a name as needed.

Item	Parameter
Forwarding type	• Structured data: You need to select a forwarding mode (image/URL). • Device: You need to enter the parent organization ID. • Alarm
IP address/Port number	Enter the IP address and port number of the destination side.

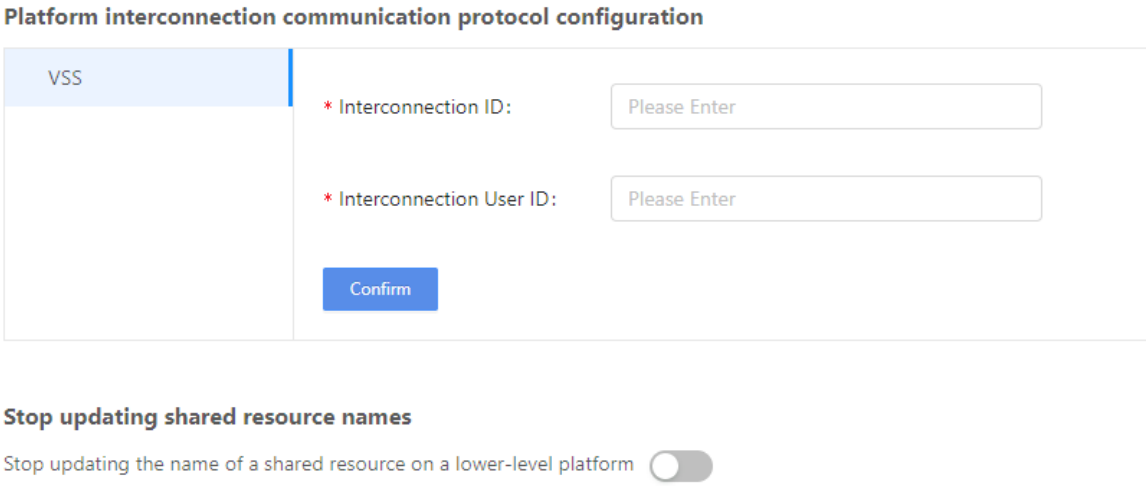
3. Click **OK**.

29.2.2 Platform Configuration

Configure the parameters of the local platform for use in platform cascading.

Platform interconnection communication protocol configuration

The platform interconnection communication protocol is used for VSS device access to the platform or cascading between VSS platforms.



parameters	Description
Platform interconnection communication protocol	VSS
Interconnection ID	The VSS-compliant inter-platform interconnection ID is a 20-digit code, where digits 11 to 13 are "200". **Note:** • Inter-platform interconnection IDs using the same inter-platform communication protocol must not be duplicated. • After adding an higher- or lower-level platform, if you modify the inter-platform interconnection ID, the system will prompt you to restart the service. Please proceed with caution as instructed on the screen.
Interconnection User ID	It will be automatically generated based on the Interconnection ID. **Note:** • Interconnection User ID must not be duplicated and must not be the same as their corresponding platform Interconnection ID. • After adding an external domain, if you modify the Interconnection User ID, the system will prompt you to restart the service. Please proceed with caution as instructed on the screen.

Stop updating shared resource names

Click to enable the function. When a lower-level platform modifies a resource name, the change will not be automatically synchronized to the local platform.

29.3 Protocol&Interconnection

Configure various protocols to achieve data interconnection between different platforms.

29.3.1 Cloud Service

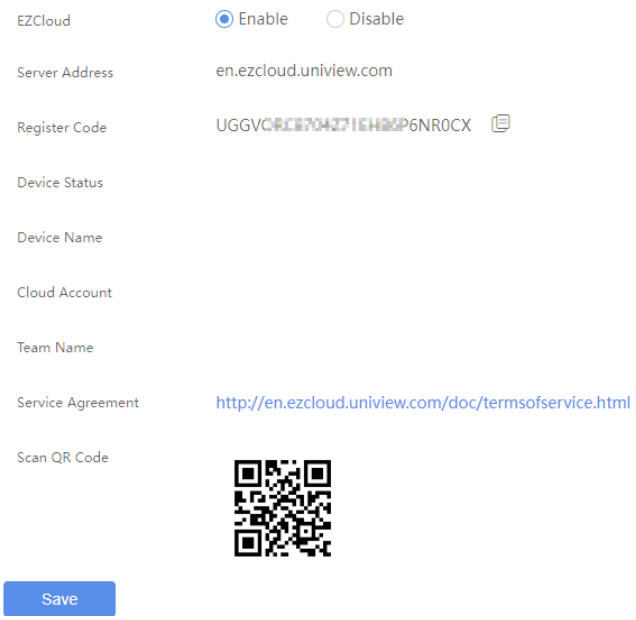
In WAN scenarios, you can add the platform to EZCloud to manage persons, visitors, access permissions, etc. on the EZCloud's Web interface.

Note:
After successful connection with EZCloud:

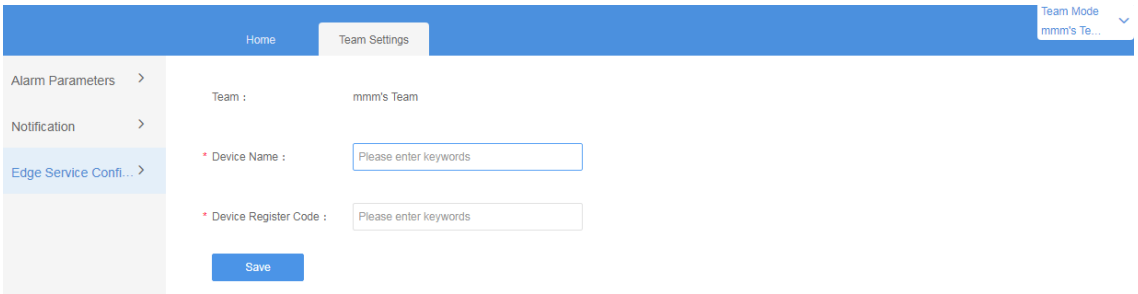
- You can add, edit, and delete organizations/devices/channels/rooms linked to video intercom devices on the platform only.
- You can add, edit, and delete rooms/persons/visitors/access permissions/schedule templates/holidays on EZCloud only, and you can only view such information on the platform.

Register to Cloud

1. Select **Enable** to enable EZCloud, and then click **Save**.



2. Log in to EZCloud website: https://en.ezcloud.uniview.com.



(1) Click **Team Mode** in the upper-right corner and select **UNV Guard Team** to enter team mode.

(2) Go to **Team Management** > **Team Settings** > **Edge Service Config**. Enter the platform's device name and register code, and then click **Save** to connect the platform to EZCloud.

Note:
The register code can be found on the **EZCloud** page on the platform.

(3) After successful connection (device status is online), click **Sync Data** and select **From Device** to synchronize data from the platform.

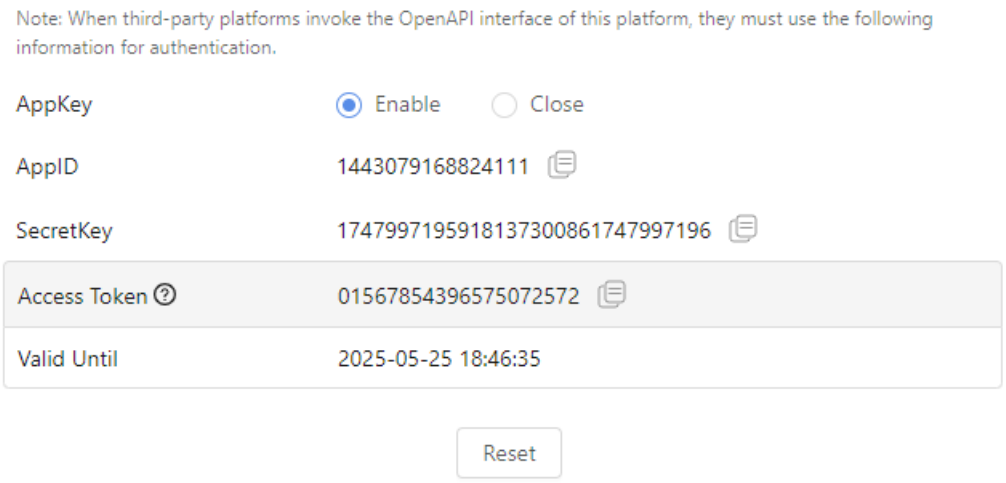
Attention:
After successful connection, if you disable EZCloud on the platform, the client will exit and unbind the platform from EZCloud, and the data will no longer be synced.

29.3.2 OpenAPI

When third-party platforms invoke the OpenAPI interface of the platform, they need AppKey information of the platform for authentication.

Note:
Supported interface authentication methods:

- Access Token + Username/Password
- Access Token + AppID/SecretKey
- Interface Signature + Username/Password
- Interface Signature + AppID/SecretKey



AppKey	• Enable: Requires authentication via key. When enabled, the following information will be generated automatically.
	  • AppID: Remains permanently valid if not updated.
	  • SecretKey: Remains permanently valid if not updated.
	  • Access Token: Used to verify interface access or invocation permissions, valid only for 48 hours.
	• Disable: Does not require key authentication.

Copy Info	Click the corresponding to copy the AppID, SecertKey, and Access Token for third-party platform use.
Reset Info	Click **Reset** to geneate new AppID, SecretKey, and Access Token.

Note:
When you reset or disable the AppKey:

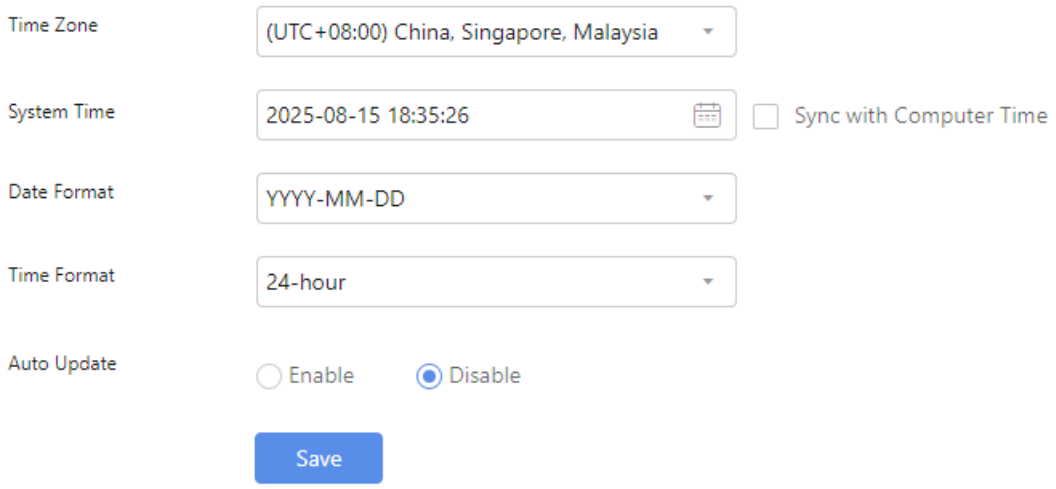
- If the previous Token is still valid, this operation will only invalidate the old AppID and SecretKey. The old Token is still valid.
- If the previous Token has expired, this operation will invalidate all.

29.4 Service Configuration

Configure services globally.

29.4.1 Time Configuration

Configure time information for the platform, including time zone, date and time format, and system time.



- Sync with Computer Time: When selected, the platform's system time syncs with the PC time.
- Auto Update: When enabled, an NTP server needs to be configured. Once configured, the platform's system time syncs with the NTP server time.

Note:
Modifying the time zone requires a server restart to take effect; modifying other parameters will take effect after saving.

29.4.2 Holiday Management

Set public holidays or specified days as holiday. Holiday has higher priority than weekly schedule and attendance rules.

- Scene 1: During holidays, access control permissions are executed based on the holiday schedule.

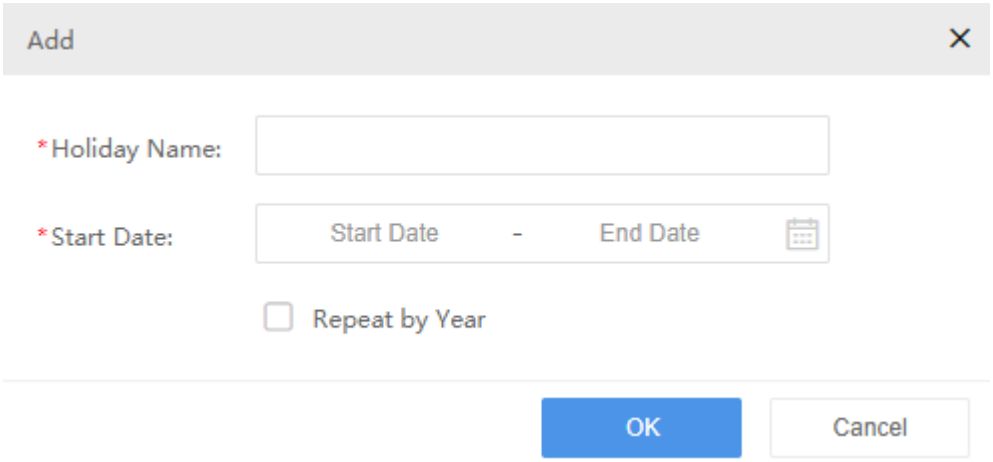
  Note:
  After adding holidays on this page, you need to configure the holiday Schedule Template and associate it with access control devices in Access Permission Config.

- Scene 2: Absence in holidays does not record as attendance exceptions.
  For example, attendance rules require attendance during 9:00-17:00 from Monday to Friday. If New Year's Day is set as holiday, then holiday attendance rules are applied on New Year's Day.

  Note:
  After adding holidays on this page, you also need to configure the Holiday Adjustment rules.

Add Holiday

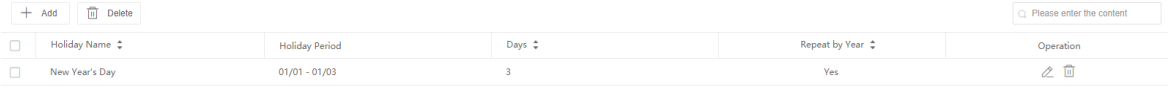
1. Click **Add**.



2. Enter the holiday name and set the holiday period. The holiday name must be unique.
3. (Optional) If **Repeat By Year** is selected, the holiday will repeat every year.
4. Click **OK**.

More Operations

You can edit and delete holidays.



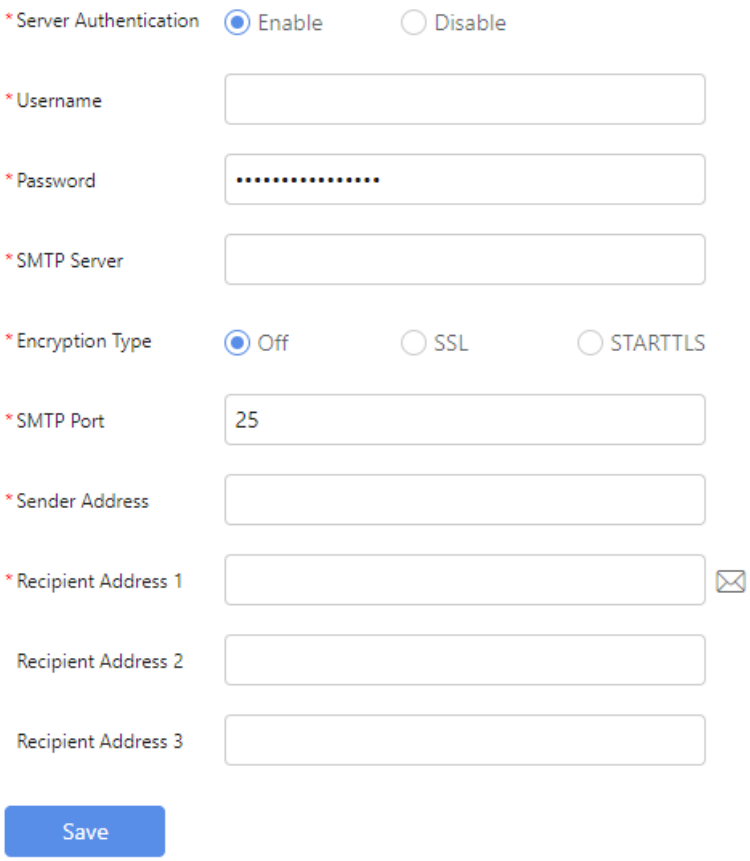
- Edit: Click in the **Operation** column.
- Delete: Select the holidays to be deleted and click **Delete**, or click in the **Operation** column.

29.4.3 Email

Configure SMPT server settings, sender email information, etc. When configured, you can use the email sending function in functions such as alarm linkage.

29.4.3.1 Email Server

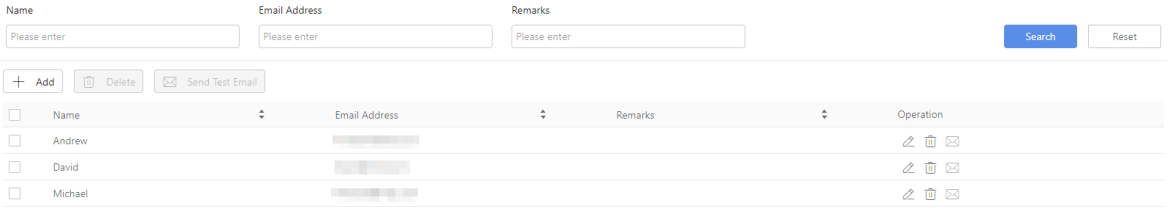
Configure the mail server, sender email address, and other related information.



Parameter	Description
Server Authentication	• Enable SMTP server authentication: Requires verification of the sender's username and password to prevent unauthorized use. • Disable SMTP server authentication: No need to fill in the sender's username and password; any service can send messages through this server. **Note:** Authentication must be enabled if sending emails via public networks, cloud services, or third-party email providers.
Username/Password	After enabling SMTP server authentication, you need to enter the username and password of the sender's email account. **Note:** The password entered here is the authorization code provided by the SMTP service, not the email account's login password.
SMTP Server	Enter the address of the SMTP server.
Encryption Type	When SSL/STARTTLS is enabled, the data between the platform and the SMTP server is encrypted, protecting email content from interception.
SMTP Port	Enter the port number of the SMTP server. **Note:** The SMTP port corresponds to the encryption type. • No Encryption: Port 25 or Port 587(Note: Port 25 is typically used for server-to-server communication and may be restricted for client use on some networks). • SSL Encryption: Port 465. • STARTTLS Encryption: Port 587.
Sender Address	Enter the sender's email address. The system emails will be sent from this address.
Recipient Address	Enter the recipient's email address. Click ✉ to test if emails can be sent successfully.

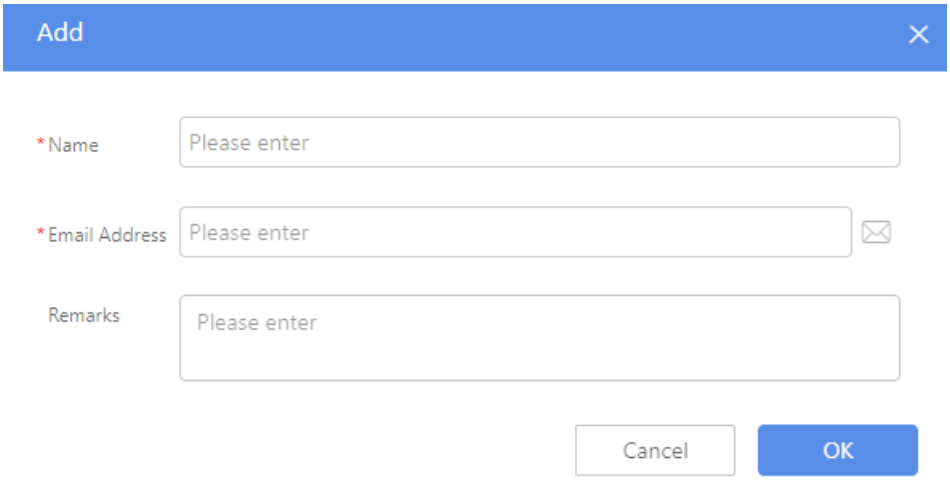
29.4.3.2 Contacts

Configure email address information.



Add Contact

1. Click **Add**, then enter the contact's name and email address.



2. (Optional) Click ✉ to send a test email to the corresponding address and verify if the email sending function is working properly.

   Note:
   The Email Server must be configured before sending test emails.

3. Click **OK** to save the configuration.

Send Test Email

Supports sending test emails one by one or in batches.

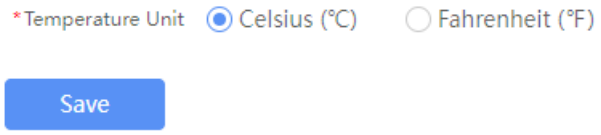
- Send one by one: Click ✉ in the **Operation** column to send a test email to the corresponding address.
- Send in batches: Select multiple contacts and click the **Send Test Email** button above to send test emails to the selected addresses in batches.

More Operations

- Search: Quickly search address book information by contact name, email address, or remarks.
- Edit: Click ✎ in the **Operation** column to modify contact information.
- Delete: Select the contact(s) and click the **Delete** button above, or click 🗑 in the **Operation** column.

29.4.4 Temperature

Choose a temperature unit as needed. The temperature unit on pages such as Face Search will use the one specified here.

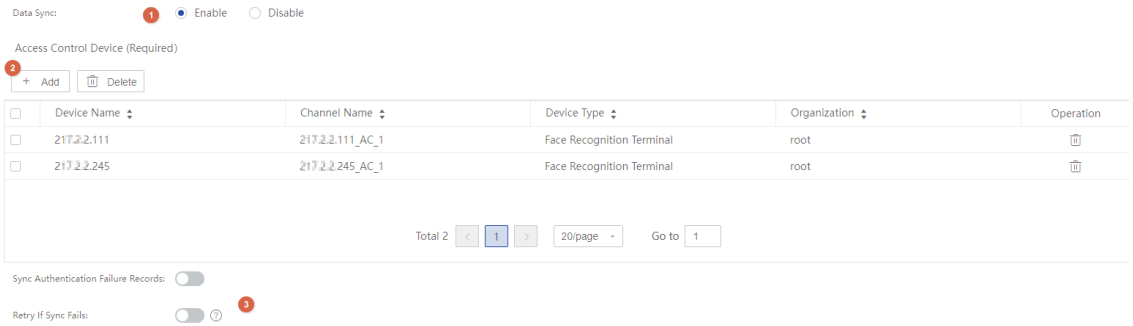


29.4.5 Data Sync Configuration

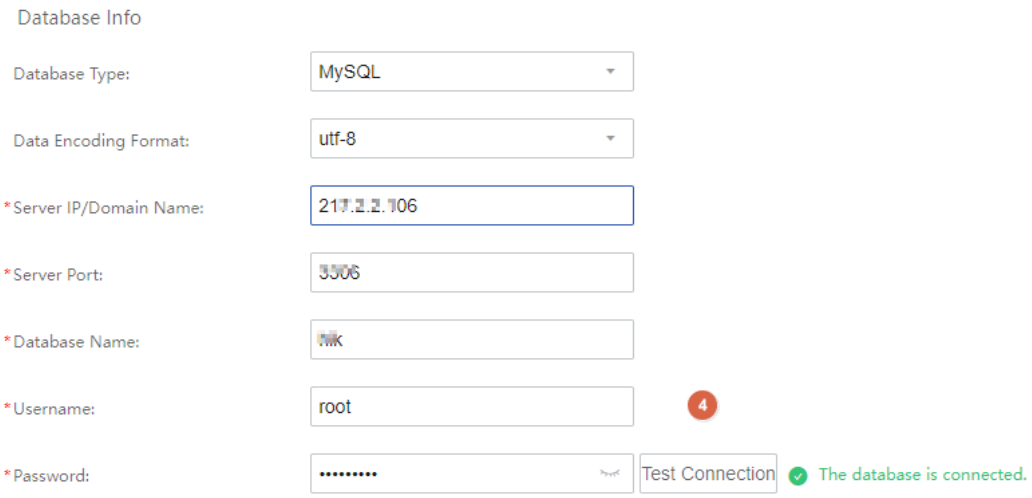
System Config > Security > Data Sync Configuration

You may synchronize personnel authentication records from the platform to a third-party database for direct use in a third-party attendance system.

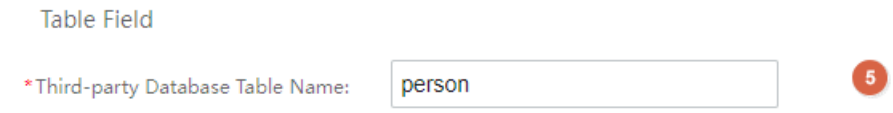
1. Enable **Data Sync**.



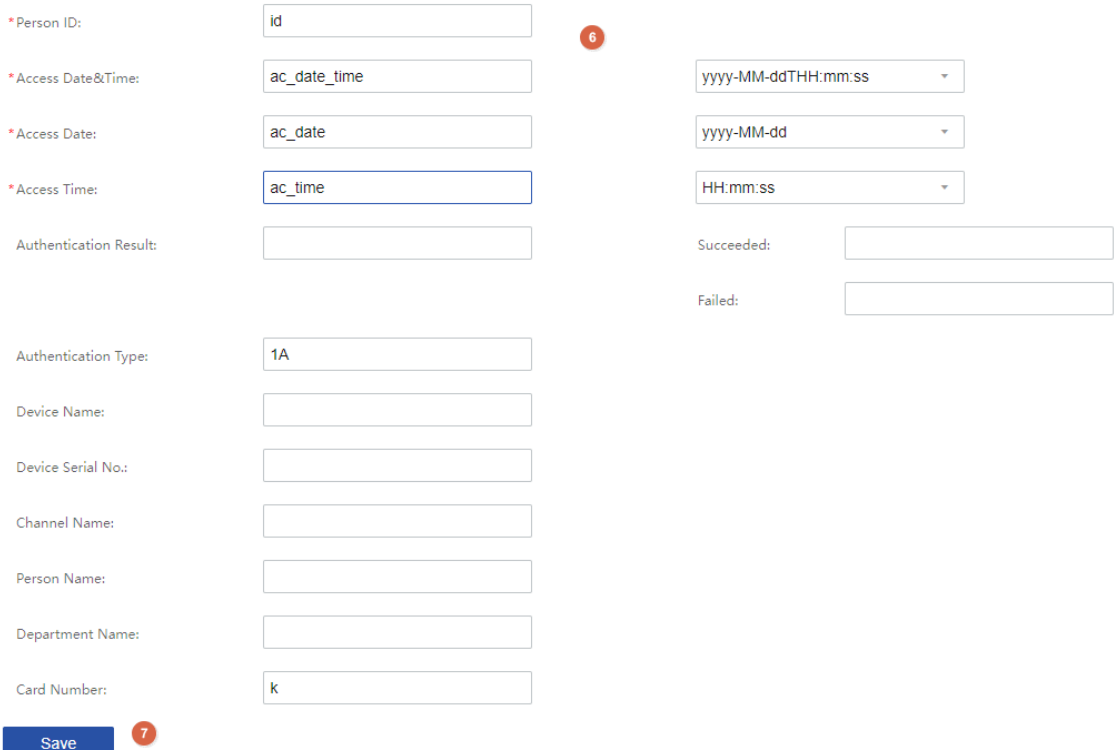
2. Select access control device(s) and synchronize personnel authentication records to the third-party platform. Click **Add**, select access control device(s), and click **OK**.
3. Configure handling measures for the abnormal data.
   - Sync Authentication Failure Records: When enabled, authentication failure records will also be synced to the third-party platform; otherwise, they will not be synced.
   - Retry If Sync Fails: When enabled, if data synchronization fails, the system will automatically synchronizes the failed data again every hour; otherwise, the data will not be synchronized again.
4. Configure the third-party server and database information, including the database type (PostgreSQL, MySQL, SQL Server), data encoding format, server IP/domain name, database name, and database username/password.
   Once completed, click **Test Connection** to test if the connection with the database is successful.



5. Enter the name of the third-party database table where the data will be synchronized to.



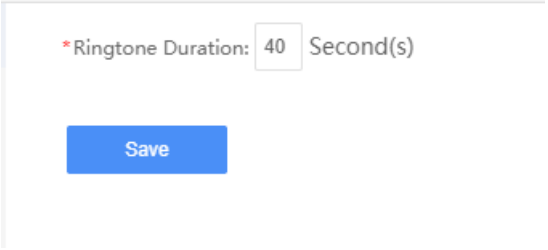
6. Enter the third-party database field name that corresponds to the platform data type and select the field format.
   Please complete the information according to the third-party database table.
   For example: If the third-party database field for “Access Data&Time” is “ac_data_time” with the format “yyyy-MM-DDTHH:mm:ss”, the platform’s access data&time data will be synced to this field in the set format.



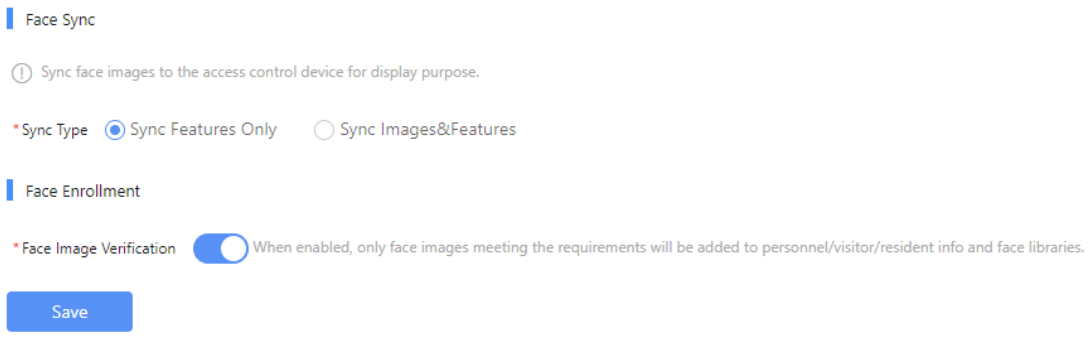
7. Click **Save**.

29.4.6 Video Intercom

Configure the ringtone duration (40s~60s) for the video intercom. The system will end the call when it is not connected within the set duration.



29.4.7 Face Sync



Face Sync Type

When using the access control verification function, face images and features should be synced to access control devices for verifying the matching degree between the captured person and people in the library.

Set the sync type for face information to be synced to face recognition terminals when configuring Permission Group.

- Sync Features Only: It will not sync face images to the access control device. Even if verification succeeded, there won't be any face image on the access control device.
- Sync Images&Features: It will sync face images to the access control device so that the corresponding face image will be displayed on it when the verification succeeded.

Note:
Some access control devices do not support direct sync of face features from the platform. So you need to manually sync face images to these devices, and they will then extract the face features themselves.

Face Image Verification

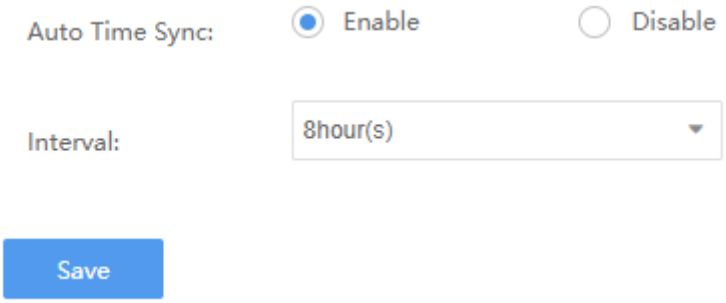
Set whether to verify image quality when adding face images to personnel/visitor/resident info and face libraries.

- On: Only face images meeting the requirements can be added.
- Off: The system does not verify image quality, allowing low-quality images and images partially obscured.

29.4.8 Auto Time Sync

Use the current time of the UNV Guard server as a reference to adjust the time on the device and keep it synchronized with the server time.

Enable Auto Time Sync and set the synchronization interval. The system automatically synchronizes the time once when the function is enabled, and then continues to synchronize the time regularly at the set time interval.



29.4.9 Alarm Input/Output Config

Configure alarm input and output types for the server.

Before configuring alarm channels, complete the wiring of the server alarm interfaces first, and then configure the channels with corresponding numbers on the configuration page based on the wired interfaces.

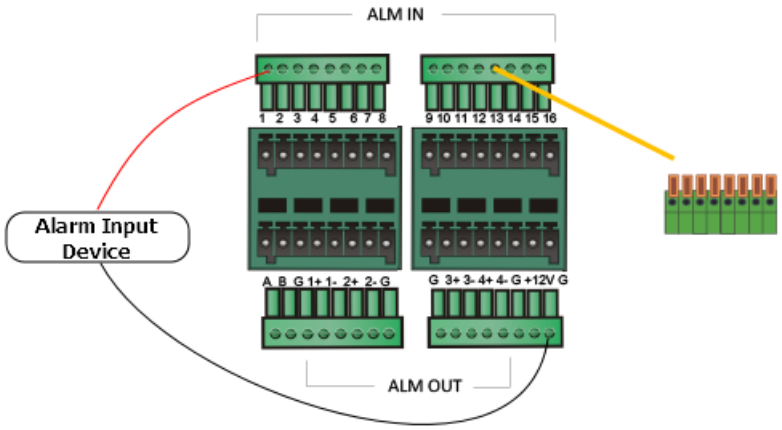
Connecting Alarm Input Devices

Connect alarm input devices to the ALARM IN interface on the rear panel of the server. When an alarm rule is triggered, the alarm input device sends a switch signal to the server to report an alarm to the platform.

Common alarm input devices include door contacts, infrared detectors, and smoke detectors.

The ALARM IN interface on the server requires an external Phoenix terminal.

Note:
The following figure is for reference only: 1–16 are 16 alarm input interfaces respectively, and G is the grounding port. Multiple alarm input devices can share the same G port.



1. Insert the external Phoenix terminal into the ALARM IN interface.
2. Press the orange terminal with a miniature flathead screwdriver, insert the signal wire of the alarm input device into the jack, and release the screwdriver. Connect the common terminal (COM) of the alarm input device to the G port on the server.

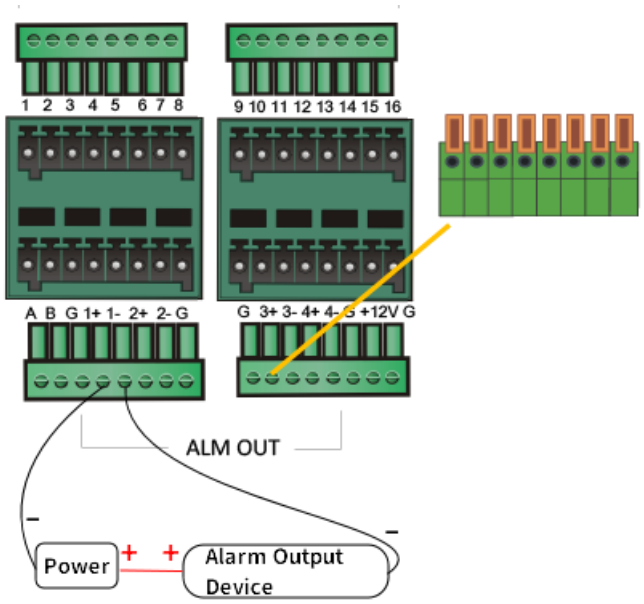
Connecting Alarm Output Devices

Connect alarm output devices to the ALARM OUT interface on the rear panel of the server. When an alarm rule is triggered, the alarm output device activates the corresponding alarm.

Common alarm output devices include alarm lights and alarm bells.

The ALARM OUT interface on the server requires an external Phoenix terminal.

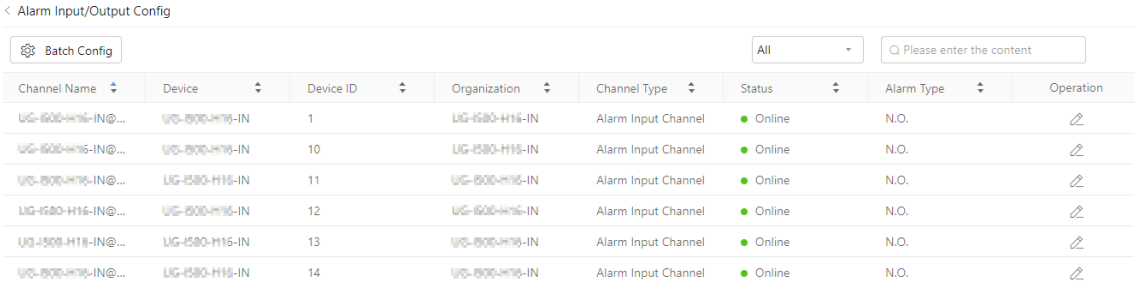
Note:
The following figure is for reference only: 1+/1–, 2+/2–, 3+/3–, 4+/4– are four pairs of alarm output interfaces. If one end of the alarm device is connected to 1+, the other end should be connected to 1-. There is a relay switch between 1+/1-, and the wiring does not distinguish between positive and negative poles.



1. Insert the external Phoenix terminal into the ALARM OUT interface.
2. Press the orange terminal with a miniature flathead screwdriver, insert the positive/negative signal wires of the alarm output device into the jacks, and release the screwdriver.
3. Connect the alarm output device to the power supply, and connect the positive pole of the power supply to the positive pole of the alarm output device.

Alarm Channel Configuration

1. Go to **Alarm Input/Output Config**.



2. Click the corresponding for the alarm channel, or click **Batch Configure**, modify the alarm type. After the modification, you need to select **Enable Alarm Input Channel** for the changes to take effect.

Figure 29-1: Configure One by One

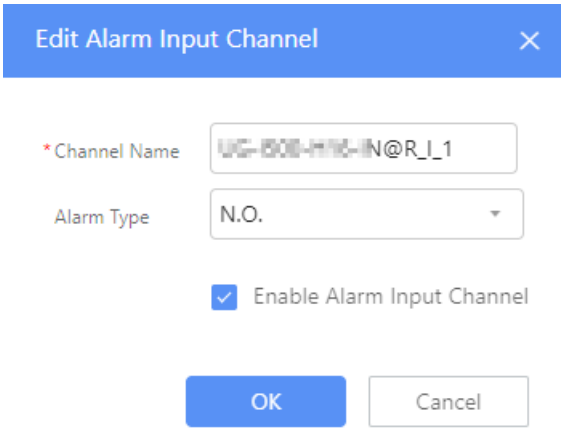
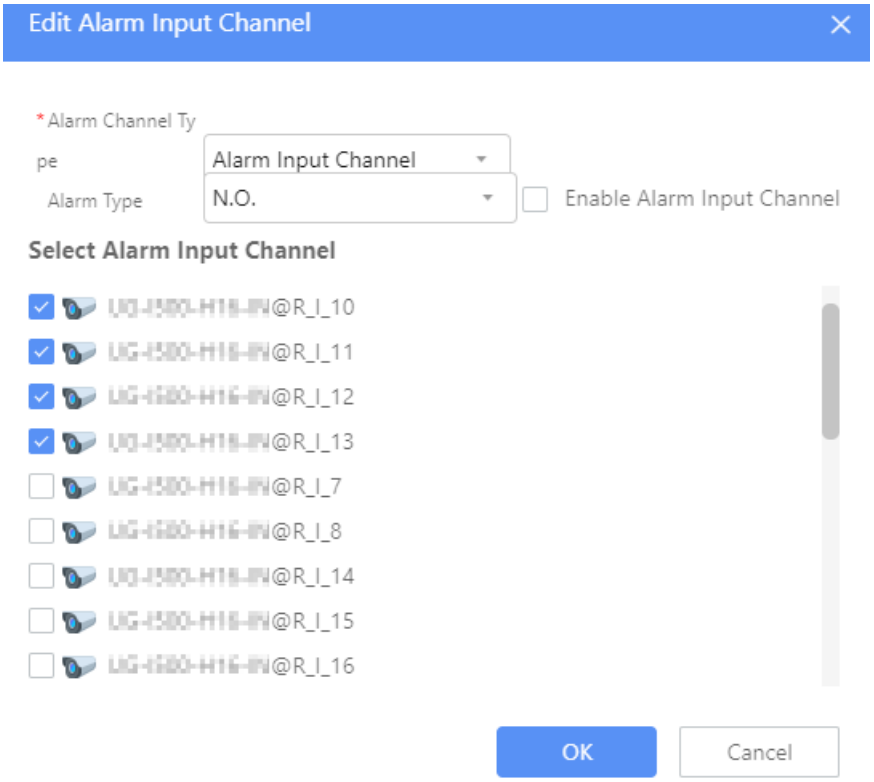


Figure 29-2: Configure in Batches

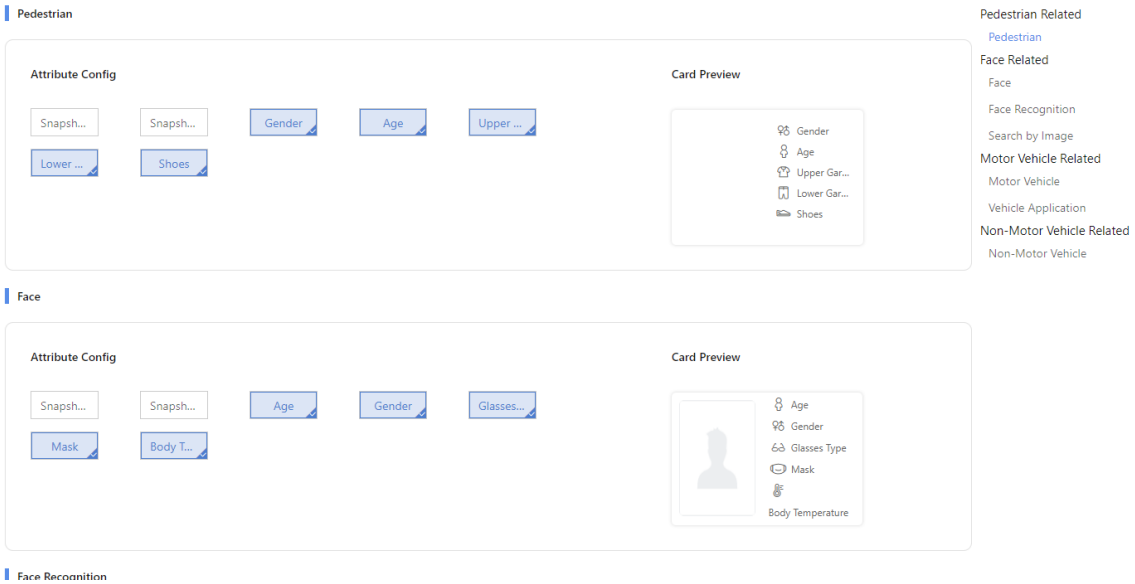


Alarm Channel Type	Alarm Type Setting
Alarm Input	The alarm type is the same as the alarm state of the alarm input device. • If the alarm input device is normally closed (alarm triggered when the circuit is open), select "Normally Open" for the alarm type(alarm is reported when an open circuit signal is detected). • If the alarm input device is normally open (alarm triggered when the circuit is closed), select "Normally Closed" for the alarm type(alarm is reported when a closed circuit signal is detected). Note: An incorrect alarm type selection will result in no alarm being reported.
Alarm Output	The alarm type is the same as the normal state of the alarm output device. Take an alarm light connected to the server alarm output as an example: • If the light is off under normal conditions, select "Normally Open" for the alarm type. When an alarm occurs, the circuit closes and the alarm light turns on. • If the light is on under normal conditions, select "Normally Closed" for the alarm type. When an alarm occurs, the circuit opens and the alarm light turns off.

29.4.10 Card Attribute

This function supports the customization of snapshot information and structured attributes displayed on pedestrian/face/motor vehicle/non-motor vehicle snapshots on the **Smart Live View** page and **Comprehensive Search** page.

- By default, all card attributes are displayed on the card.
- Only the selected attributes will be displayed on the card. To conceal an attribute, deselect it. A preview of the card can be viewed on the right side.



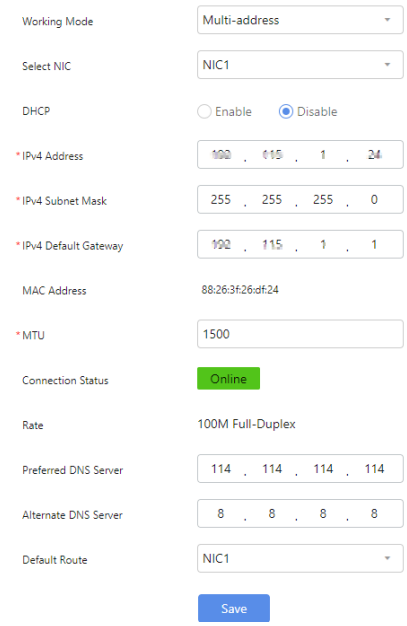
Item	Description
Pedestrian	Attributes displayed on cards in Smart Live View > Pedestrian Snapshot, Multi-Target Detection > Pedestrian Snapshot, and Pedestrian Search > By Attribute.
Face	Attributes displayed on cards in Smart Live View > Face Snapshot, Multi-Target Detection > Face Snapshot, and Face Search >By Attribute.
Face Recognition	Face match/not match attributes displayed on cards in Smart Live View > Face Comparison, Face Recognition, and Face Search > By Alarm.
Search by Image	Face library and people pass-thru record attributes displayed on cards in Face Search > Search by Image.
Motor Vehicle	Attributes displayed on cards in Smart Live View > Motor Vehicle Snapshot, Multi-Target Detection > Motor Vehicle Snapshot, and Motor Vehicle Search > By Attribute.
Vehicle Application	Vehicle match/not match and violation attributes displayed on cards in Smart Live View > Vehicle Comparison and Vehicle Application.
Non-Motor Vehicle	Attributes displayed on cards in Smart Live View > Non-Motor Vehicle Snapshot, Multi-Target Detection > Non-Motor Vehicle Snapshot, and Non-Motor Vehicle Search > By Attribute.

29.5 Network Management

29.5.1 Network Configuration

29.5.1.1 TCP/IP

Set TCP/IP parameters in different working modes, including IP obtainment (static or DHCP), IP address, subnet mask, default gateway, MTU, preferred and alternate DNS server, and default route.



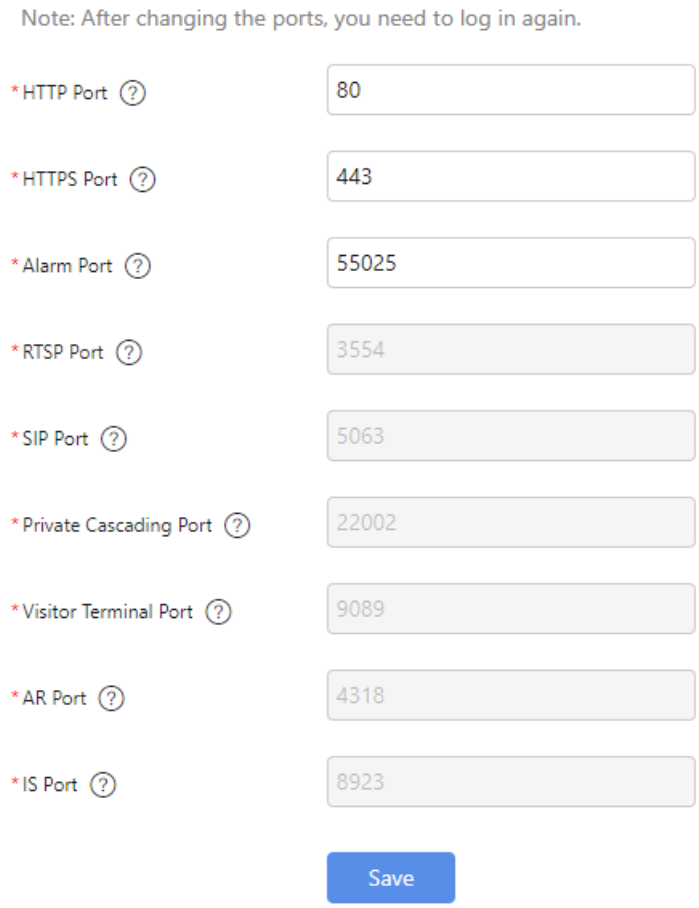
Note:

- The configured IPv4 addresses of the NICs must belong to different network segments.
- After the Working Mode/NIC/DHCP/IP address is modified: (1) The system will refresh its configuration and return to the login page. It will be ready to log in within 5-10 minutes. Do not restart or power off the device during this time. (2) Custom routes will be cleared.
- When the working mode is Load Balance or Net Fault-tolerance, do not configure NIC aggregation on the switch side, otherwise network issues may occur.

Working Mode	• Multi-address: Default mode. The Network Interface Cards (NICs) work independently with different IP addresses. • Load Balance: NICs that make up a virtual NIC use the same IP and work together to share the network load. • Net Fault-tolerance: NICs that make up a virtual NIC use the same IP and work as a backup to each other. If either NIC becomes faulty, the other takes over.
DHCP	Use a DHCP server to automatically assign an IP address.
IPv4 Address	Server' IP address. Users access the system at this address from a Web or software client.
Connection Status	The connection status of the selected NIC. The status is "Online" when the network port has a cable connected and the connection is active.
DNS Server	Domain Name Server, which resolves a domain name into an IP address.
Default Route	Specifies the default NIC that the server uses to send data. The default route may be different from the NIC set in the Select NIC drop-down list.

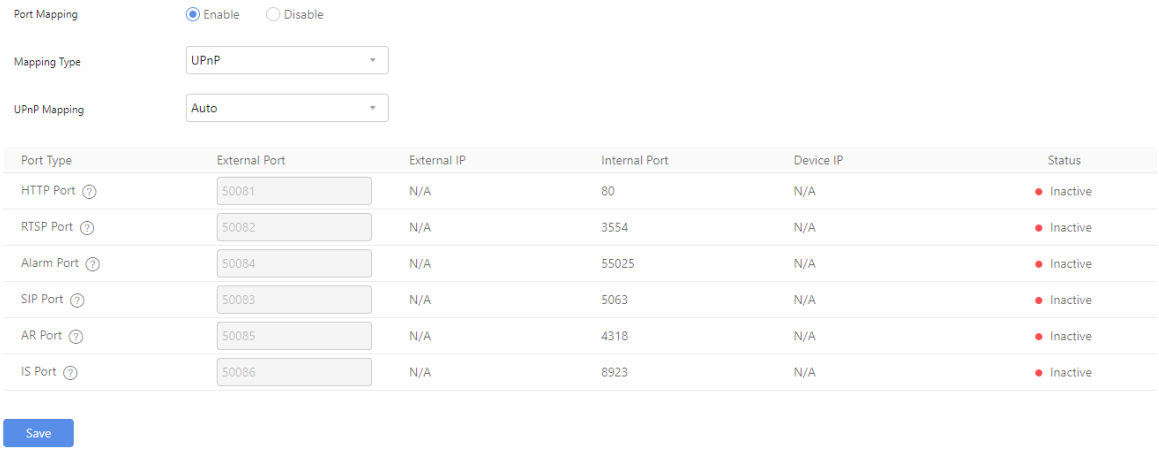
29.5.1.2 Port

Configure HTTP, HTTPS and alarm ports. Other ports can only be viewed.



29.5.1.3 Port Mapping

Use port mapping to configure mapping relations between internal and external ports, enabling access to internal ports by simply visiting the external port.



By default port mapping is disabled.

The platform supports two port mapping modes:

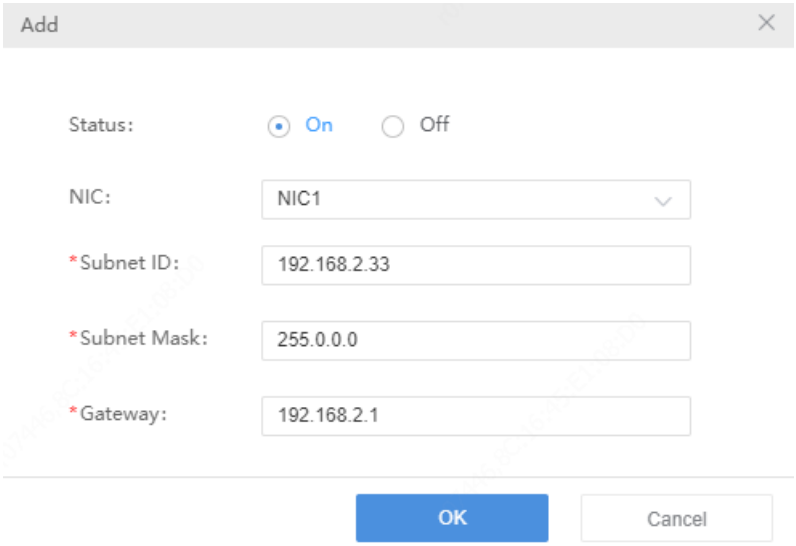
Mapping Type	Description
UPnP	Enable UPnP in the router first before you setting UPnP on this page. UPnP requires the router's support.

Mapping Type	Description
	• Auto: The VMS automatically negotiates external ports with the router. If an external port is already in use, the VMS will negotiate with the router again with another port number. • Manual: Specify external ports manually. If the specified port is already in use, the VMS will not try again with another port, and port mapping will fail.
Manual	Usually this mode is used when the router does not support UPnP. Complete settings on the router first and then fill in the settings on this page.

29.5.1.4 Custom Route

Add static routes to interconnect the VMS with destination networks. Up to 100 custom routes are allowed.

You need to choose the NIC and set the subnet ID, subnet mask and gateway. A custom route is enabled by default and can be disabled.



Note:
Changing the NIC's working mode will clear all the existing custom routes.

29.5.2 Security Configuration

29.5.2.1 HTTPS

Go to **Network Management > Security Config > HTTPS**.

HTTPS is a secure communication method that enhances the data transmission security via mechanisms such as data encryption and identity verification.

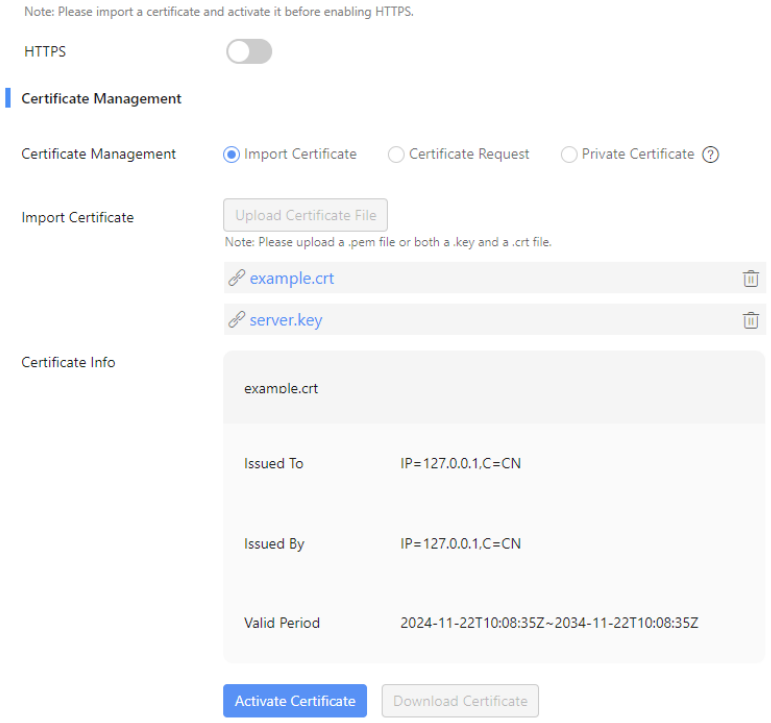
HTTPS only allows encrypted communication using the more secure **TLS 1.2 or higher protocol versions**. Modern browsers enable support for the latest TLS versions by default, eliminating the need for manual configuration by the user, automatically ensuring the best security and compatibility.

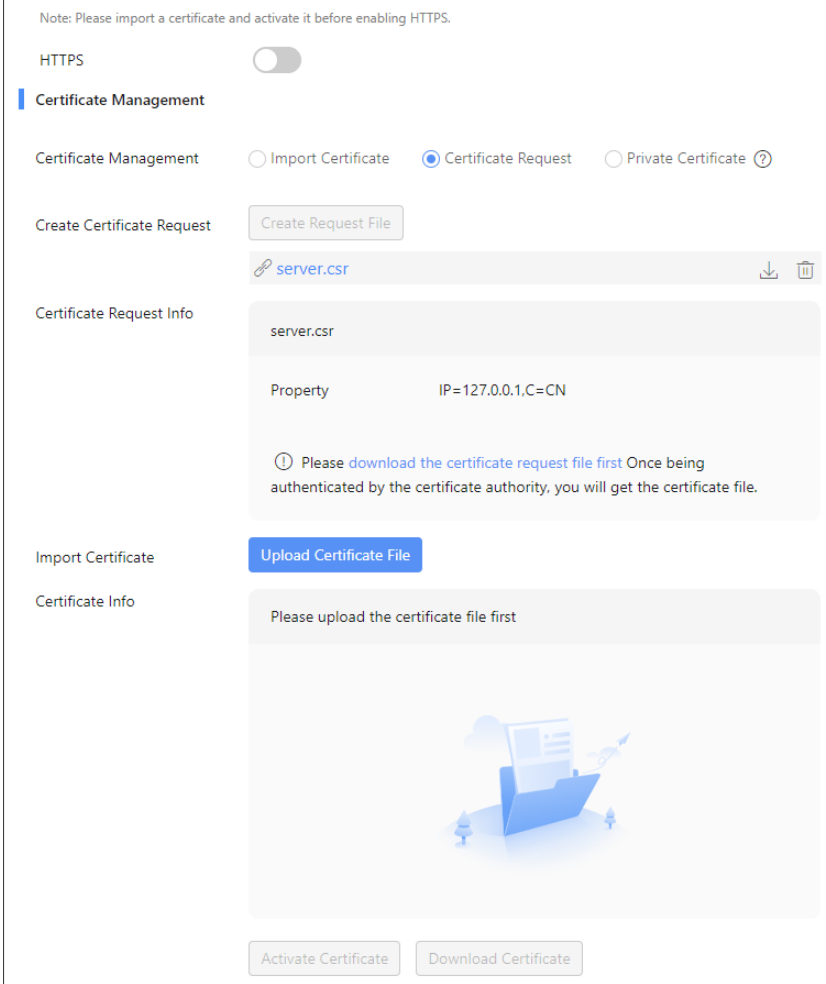
When enabled, you can log in to the platform or integrate with third-party systems securely via the HTTPS protocol.

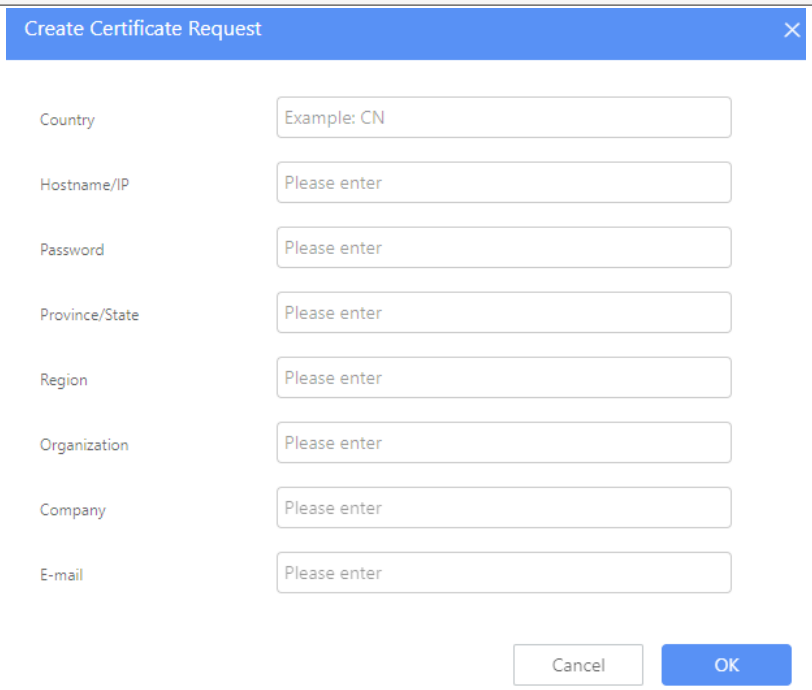
To enable HTTPS, you must first activate a digital certificate, which is generally issued by a Certificate Authority (CA) to verify the identity of an entity, such as a website, server, or user. When a user tries to access a webpage secured by HTTPS, the server presents its digital certificate to the user's browser. The browser verifies the certificate's validity and authenticity. If normal, an encrypted communication channel is established between them.

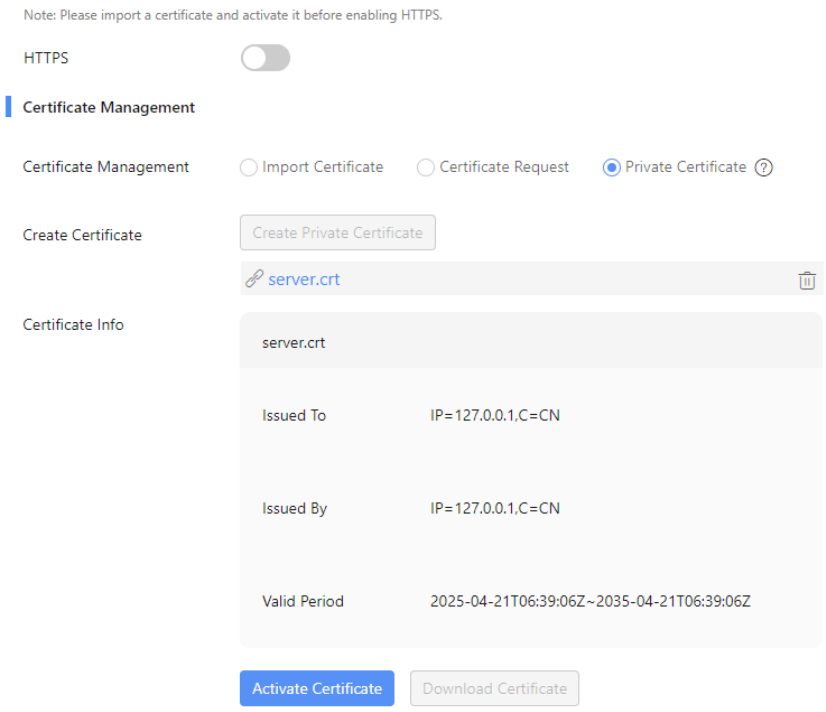
Certificate Management

Choose a method to import and activate the certificate.

Method	Description
Import Certificate	If you already have a certificate (either official or private), you can import it directly.  1. Select **Import Certificate** for **Certificate Management**. 2. Click **Upload Certificate File** to upload the certificate file from local. **Note:** Two types of certificate formats are supported: • .key file + .crt file: The .key file is the private key generated by the certificate holder, and the .crt file is the certificate generated by the CA. • .pem file: Packages the .key file and the .crt file into one. 3. Click **Activate Certificate**.
Certificate Request	If you do not have a certificate, you can submit a request file to request an official certificate from the CA.

Method	Description
	 1. Select **Certificate Request** for **Certificate Management**. 2. Create a certificate request file. Click **Create Request File**. Enter the device information, organization information, and the email address to receive the certificate. After confirmation, the system will generate a certificate request file (server.csr), which can be downloaded locally.

Method	Description
	 3. Submit the certificate request file to the CA to request a certificate. 4. Click **Upload Certificate File** to upload the certificate file from local. **Note:** • Only the certificate (.crt format) generated from the above request can be uploaded. Inconsistent data will fail the upload. • When creating a certificate request, a .key file is generated in the background, which will be automatically verified by the system. Therefore, you don't need to upload a .key file. 5. Click **Activate Certificate**.
Private Certificate	A private certificate is created by the software developer for testing purposes or internal network use and is not trusted on the Internet.

Method	Description
	 1. Select **Private Certificate** for **Certificate Management**. 2. Create a private protocol. Click **Create Private Certificate**. Enter the device information, organization information, and the validity period. After confirmation, the system will generate a private certificate file (server.crt). 3. Click **Activate Certificate**.

Once the certificate is activated, you can:

- Download Certificate: Click **Download Certificate** to download the certificate file (server.pem) locally. The downloaded certificate can be imported directly.
- Delete Certificate: Click for an imported certificate file to delete the certificate.

Note:
Once deleted, the webpage will return to a status without a certificate, and the HTTPS function will be automatically disabled.

Enable HTTPS

Once the certificate is activated, please enable HTTPS manually. Then, the system will return to the login page.

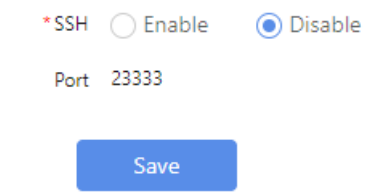
Please log in again using the HTTPS protocol.

- For B/S client: Visit https://*server IP address* using a browser.
- For C/S client: Select HTTPS as the protocol on login page.

29.5.3 Network Security

29.5.3.1 SSH

After enabling SSH, you can login to the platform via SSH on port 23333.



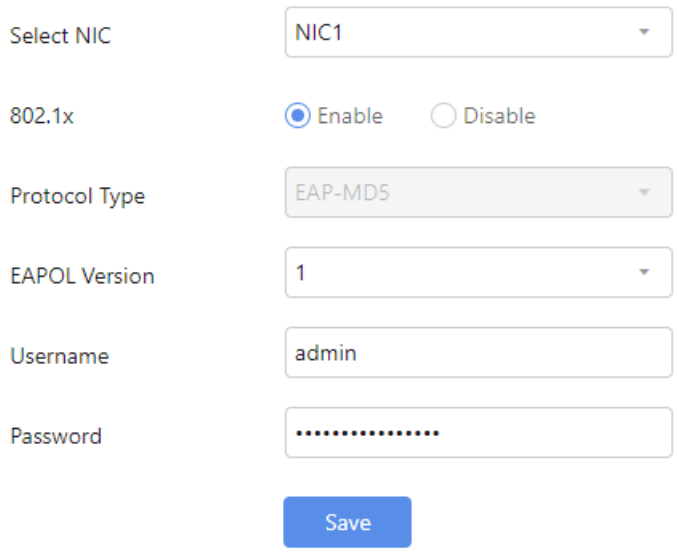
Note:

- SSH is disabled by default.
- SSH will automatically disable after remaining enabled for 30 minutes without any operations.
- Service restarts will cause SSH to shut down automatically.

29.5.3.2 802.1x

Enable **802.1x** to control access to the device with username and password set in the network switch.

Note:
802.1x must also be properly configured on the authenticator (such as Ethernet switch).

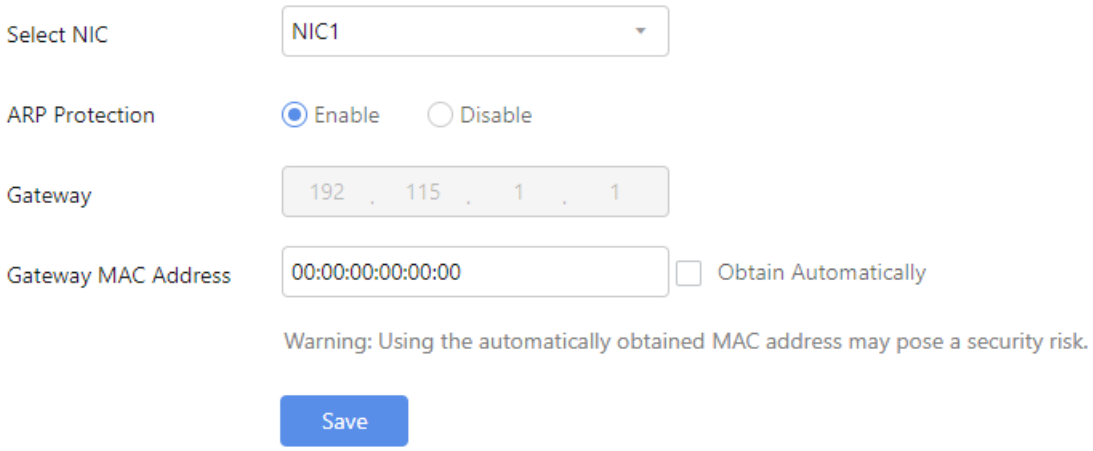


Select NIC	You may select an NIC to enable 802.1x; authentication is independent among NICs. **Binding 1** and **Binding 2** are displayed if the working mode of the selected NIC is **Load Balance** or **Net Fault-tolerance**.
Protocol type	Currently only EAP-MD5.
EAPOL Version	1 for 802.1x-2001, and 2 for 802.1x-2004.
Username and password	Used for authentication. Authentication succeeds when the entered username and password match that on the authenticator (such as Ethernet switch).

29.5.3.3 ARP Protection

Enable **ARP Protection** and bind the IP of the platform' gateway to the gateway's MAC address to prevent spoofing attacks that impersonate the gateway.

Select **Auto** to obtain an MAC address automatically, or fill in an MAC address manually.



Note:
ARP protection is effective only when it is enabled and configured before an ARP attack occurs. Protection may fail if you edit the gateway MAC address during an attack.

29.5.3.4 IP Address Filtering

Use blocklist/allowlist to forbid or allow login from certain IP addresses only.

- Blocklist: When enabled, login from the specified IP addresses is forbidden.
- Allowlist: When enabled, login only from the specified IP addresses are allowed.

Note:

- Blocklist and Allowlist cannot be enabled at the same time.
- Blocklist/allowlist is effective to IP-based logins.
- You can click a field in the list to edit an IP address.

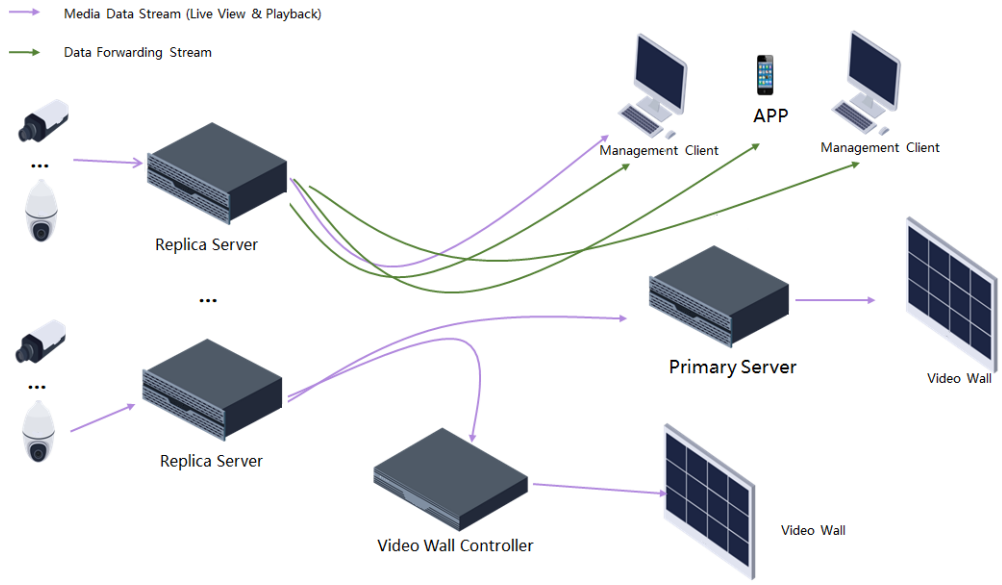
29.6 Cluster Management

29.6.1 Primary/Replica Management

When a single server cannot meet the required storage bandwidth, forwarding bandwidth, or access capacity, adding replica servers can expand system management, storage, and forwarding capabilities.

In primary/replica mode, one server acts as the primary server, provides user management, storage, and forwarding functions, while the other servers act as the replica servers, providing only storage and forwarding capabilities. The primary and replica servers must be deployed within the same LAN.

Attention:
In primary/replica mode, the primary server's performance is halved. If more than 3 replica servers are configured, the primary server is used only for management purposes.

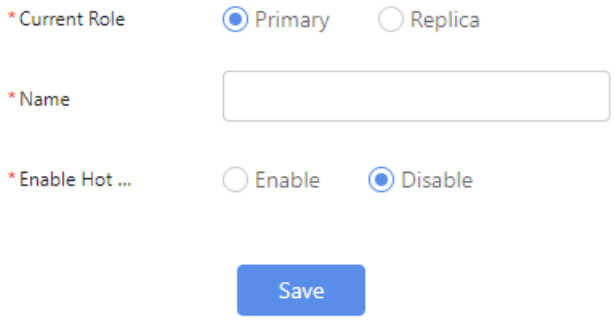


29.6.1.1 Configure Primary/Replica

Go to the **Cluster Config** page to configure the primary/replica mode.

Configure Primary Server

Log in to the primary server, select **Primary** and enter the primary server name. Click **Save**.



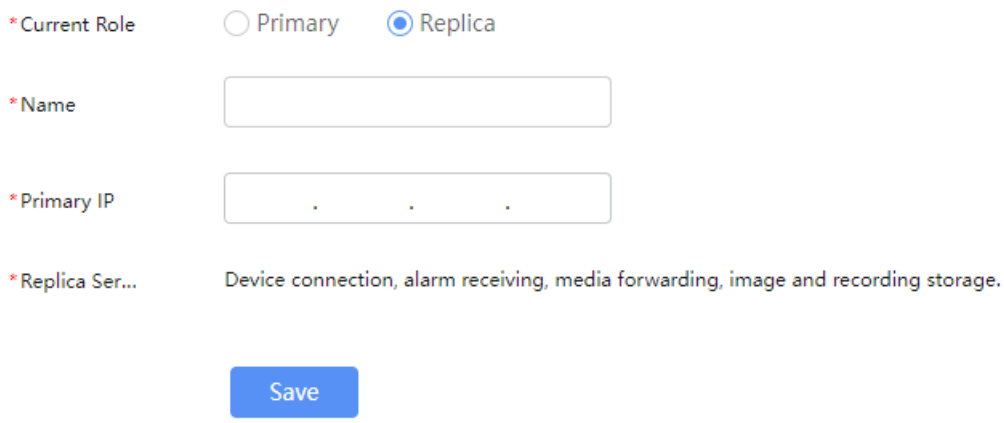
Note:
The device name can be customized, but if hot standby is to be enabled, it must match the actual host name.

Configure Replica Server

Note:

- Please log in to the replica server (input the IP address of the primary server after switching to the replica server).
- The hardware, version, and model of the primary and replica servers need to be the same.
- When switching between primary and replica servers, the service will restart, all data will be cleared, and the password will be restored to the default.
- There is a maximum number of replica servers that can be supported. Once the limit is reached, no more replica servers are allowed.
- After the configuration is completed, clients will not be able to log in to the replica server, and users cannot recover the server on the web page.

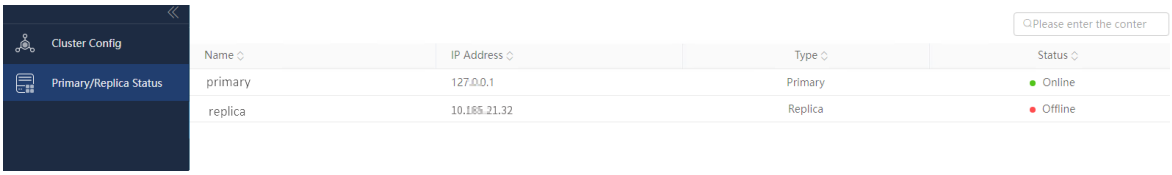
1. Log in to the replica server, select **Replica** and enter the primary server's IP address.



2. Click **Save**. After switching, the replica server's status is **Online**.

29.6.1.2 Primary/Replica Status

View replica server's information and status.



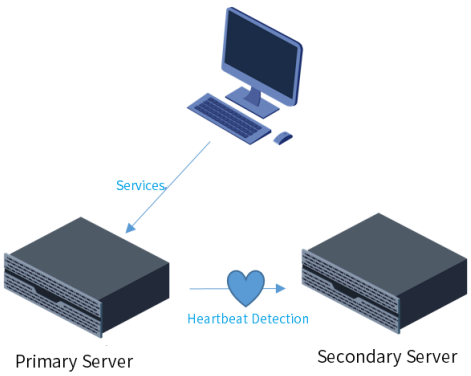
29.6.2 Dual-Server Hot Standby

Dual-server hot standby is to configure a secondary server for the primary server to back up its working data, ensuring high system availability. The primary server regularly sends heartbeat detection packets to the secondary server. If the primary server fails, the secondary server automatically switches to operational mode to ensure uninterrupted user services.

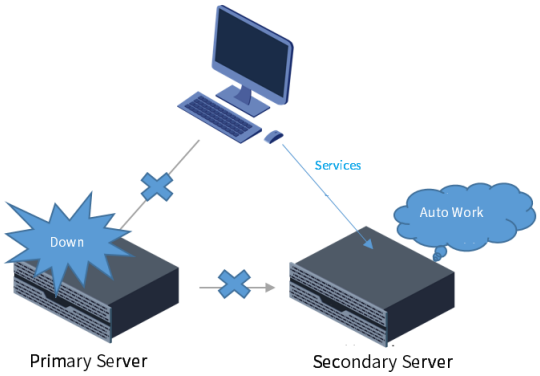
During video playback, the system will simultaneously query recordings from both the primary and secondary servers.

The primary and secondary servers must be deployed within the same LAN and connected via same NIC to transmit system configuration data. The actual application descriptions are as follows:

1. When the primary server is functioning normally, the secondary server monitors the heartbeat of the primary server.



2. If the primary server fails and the secondary server does not detect a heartbeat within 10 seconds, the secondary server automatically switches to operational mode.



3. When the primary server comes back online, it will be use as the secondary server.

29.6.2.1 Hot Standby Configuration

Go to the **Cluster Configuration** page and configure the hot standby mode.

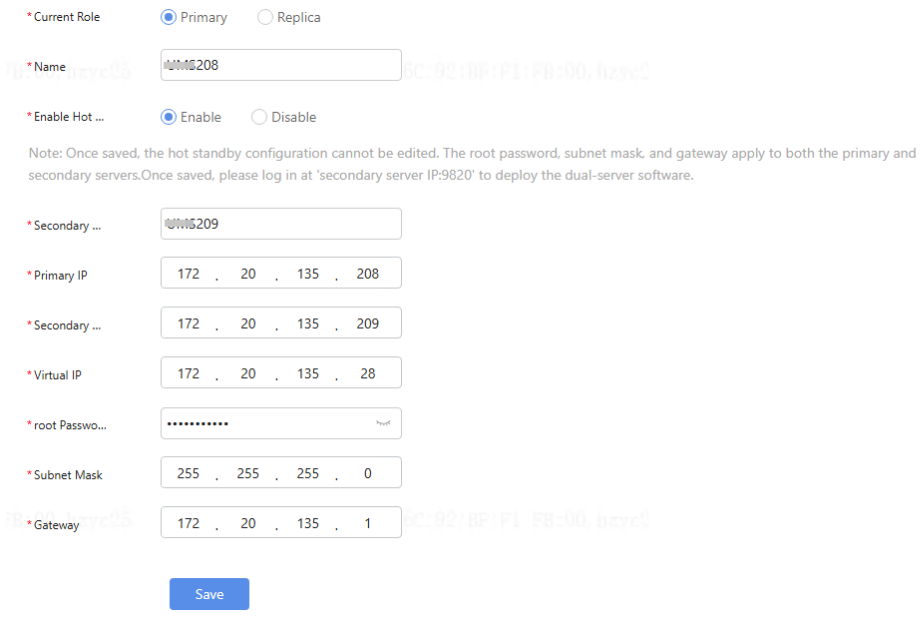
Prerequisites

- The primary and standby servers must have identical hardware, software version, model, and network interface cards (NICs).
- The primary and standby servers must be on the same network segment. If they are deployed across different segments, the switch must be configured with NQA (Network Quality Analysis).
- The primary and standby servers must have identical root passwords, subnet masks, and gateways.
- The names of the primary and standby servers must be different from each other and cannot be "localhost".
- The primary and standby servers must be running normally, with no power or network interruptions during configuration.

Configure Hot Standby

Note:

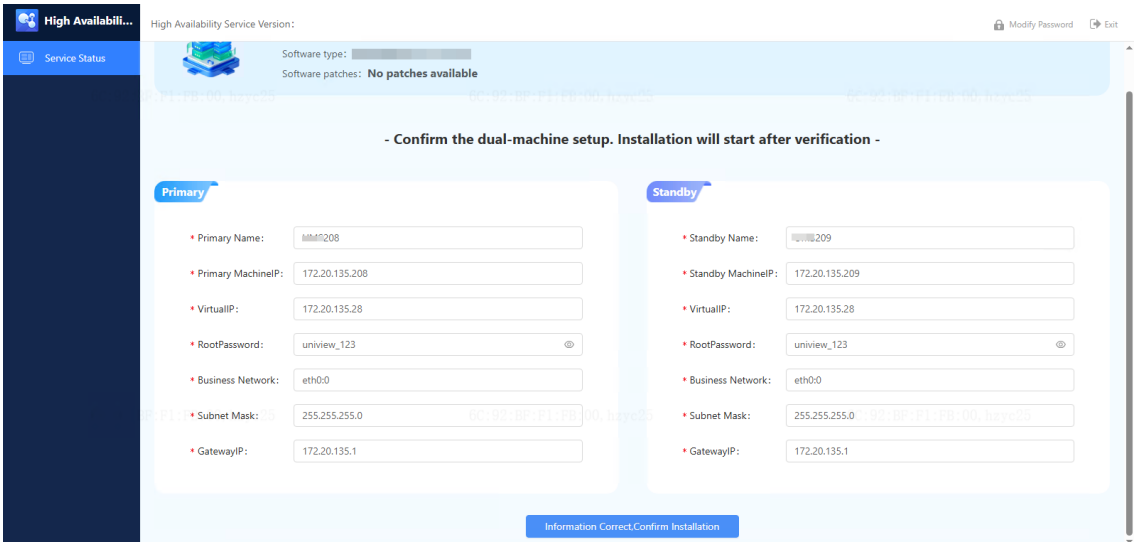
- Perform hot standby configuration on the primary server.
- When the primary server has replicas attached and hot standby is enabled, to ensure normal primary-replica connectivity, you must change the primary server's IP to the virtual IP in the replica's backend.



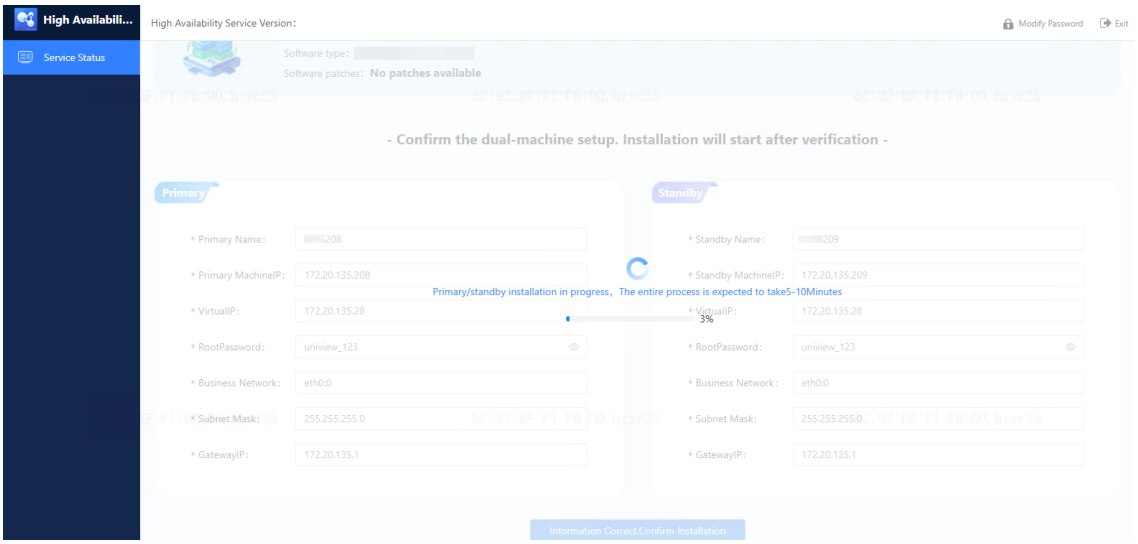
1. Log in to the primary server page, select **Primary**, and select **Enable** for hot standby. Configure the settings as described below.

Name	The actual hostname of the primary server. You can log in to the local server backend and run the ***hostname*** command to check it.	**Attention:** • The hostnames of the primary and standby servers must be different from each other and cannot be "localhost". • To change the hostnames of the primary and standby servers, log in to the server backend and run the command: ***hostnamectl set-hostname <new hostname>.***
Secondary Name	The actual hostname of the standby server. You can log in to the standby server backend and run the ***hostname*** command to check it.	
Primary IP	IPv4 address of the primary server (see TCP/IP).	
Secondary IP	IPv4 address of the standby server (see TCP/IP).	
Virtual IP	Select an unused IP address in the network. After completing the primary-standby configuration, you can use this virtual IP address to log in to the client.	
root Password	root password for the primary/standby servers (must be identical in a dual-server).	
Subnet Mask	Subnet mask for the primary/standby servers (must be identical in a dual-server).	
Gateway	Gateway for the primary/standby servers (must be identical in a dual-server).	
Business Network	Business network interface for the primary/standby servers (must be the same in a dual-server setup), formatted as "interface:0" , "0" is a fixed suffix— for example, eth0:0.	

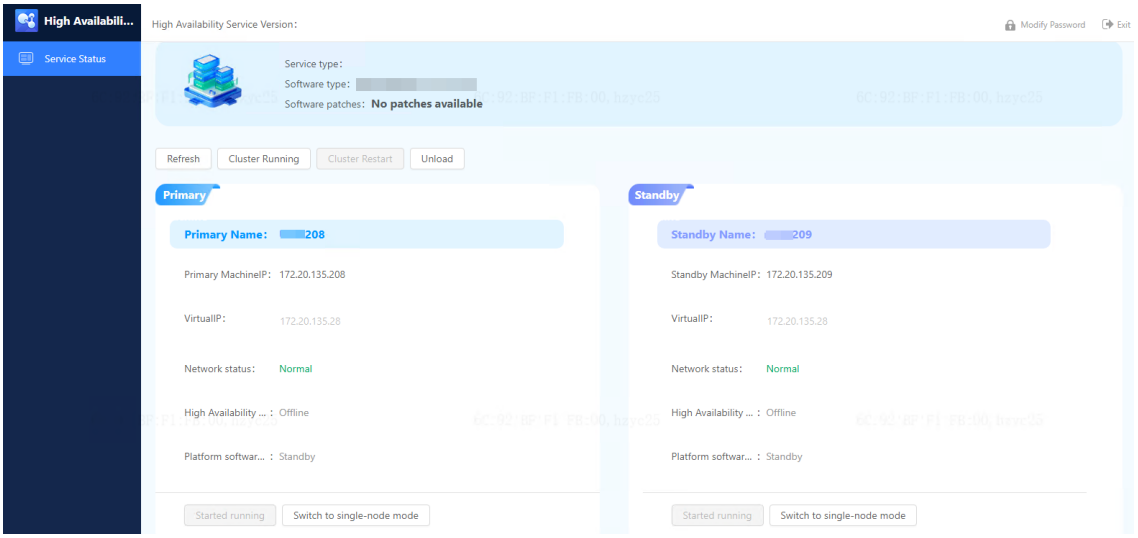
2. After completing the configuration, click **Save**. The system will sync the settings, and the services on both the primary and standby servers will restart, making the web interface temporarily unavailable.
3. Access ***http://standby server IP:9820***, log in to the High Availability software interface (*default username/password: admin/admin*), and view the dual-server information.
   - The primary/standby server names, IP addresses, and virtual IP cannot be modified;
   - The root password, business network interface, subnet mask, and gateway IP can be modified.



4. After confirming that all information is correct, click **Information Correct, Confirm Installation** to start installing the dual-server software on the primary and standby servers.



5. After installation is complete, click **Cluster Running** at the top of the interface to start the cluster service. The hot standby environment is now ready, and you can access the system by navigating to ***http://virtual IP address*** to log in and manage services.



Note:
In the high-availability software interface, the primary/standby relationship is determined by the roles assigned during configuration. Even if services fail over to the standby server, their roles will not be swapped. You can view the currently active server from the **Platform Software Running Status**.

Hot Standby Service Management

In the High Availability software interface, you can click the buttons to perform the following operations:

- **Cluster Running/Cluster Stopping**: Starts or stops the cluster service. Once stopped, the hot standby environment becomes unavailable.
- **Cluster Restart** : Restarts the cluster service.
- **Refresh**: Refresh the cluster status.
- Primary Server-**Stop Running** : Stops the primary server service, triggering a failover to the standby server.
- Standby Server-**Stop Running**: Stops the standby server service. This does not affect the primary server's operation, but if the primary server fails, services cannot fail over to the standby server.
- Primary Server(Standby Server)-**Switch to Single-node Mode**: The primary server is unlinked from the standby server, and the standby service is stopped. This does not affect the primary server's operation. The primary server remains accessible via either its physical IP or the virtual IP (since device registration is bound to the virtual IP). However, if the primary server fails, services cannot fail over to the standby server.

Note:

- This operation can not be performed on both the primary and standby servers simultaneously.
- Switching to standalone mode does not uninstall the High Availability software; you can later click **Cluster Running** to restore the dual-server hot standby configuration.
- After switching, storage must be reconfigured, and historical stored data will be lost!

- **Unload** the high-availability software will result in data loss. Please contact technical support—do not perform this operation on your own!

29.7 Disk Configuration

The server can utilize either local disk or IPSAN for resource storage.

- Local disk: The hard disks of the server, used for image storage, recording storage, recording backup and hot spare.
- IPSAN: External Uniview IPSAN, used solely for recording storage and recording backup.

After configuring the hard disk, please refer to Video Storage Configuration to configure video storage services.

29.7.1 Local Disk

View the installed hard disks, configure disk usage and create RAIDs.

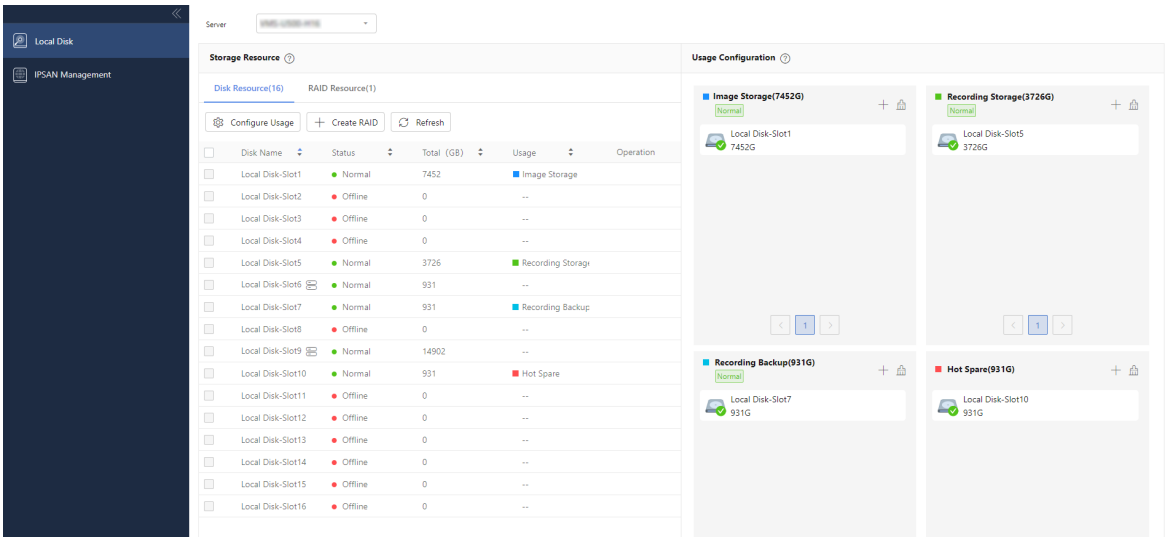
Once the configuration is done, the system will automatically create corresponding storage space for the specified use.

Note:

- To ensure normal storage, it is strongly recommended to install hard disks in slots 1/2/3 of the server, and during the initial installation, the system automatically configures the hard disk usage: Slot 1 – Image Storage, Slot 2 – Recording storage, Slot 3 –Recording backup.
- The hard disks are hot-swappable, so you can continue using the existing storage after replacing a hard disk.
- If a new hard disk replaces the old one, data on the old disk becomes inaccessible. If the hard disk is removed and reinserted, its data remains accessible.

29.7.1.1 Disk Resource

On the **Disk Resource** page, the left side lists the hard disks of the server, including the disk status, total capacity, and usage of each disk slot, and you can click the column header to sort the contents; on the right side, the hard disks and RAID resources are displayed separately by their respective usages.



Disk Status

Disk Status	Description
Normal	A hard disk is inserted in the slot and functioning properly.
Abnormal	A hard disk is inserted in the slot but has read/write errors.
Offline	No hard disk is inserted in the slot.
Partition does not meet config requirements	After deleting an RAID including an offline disk, when the offline disk comes back online, it still retains the old RAID and partition information, and this status will be displayed. To resolve this issue, click in the **Operation** column to clear the RAID and partition information (this will also erase all data on the disk). The disk can then be used normally.

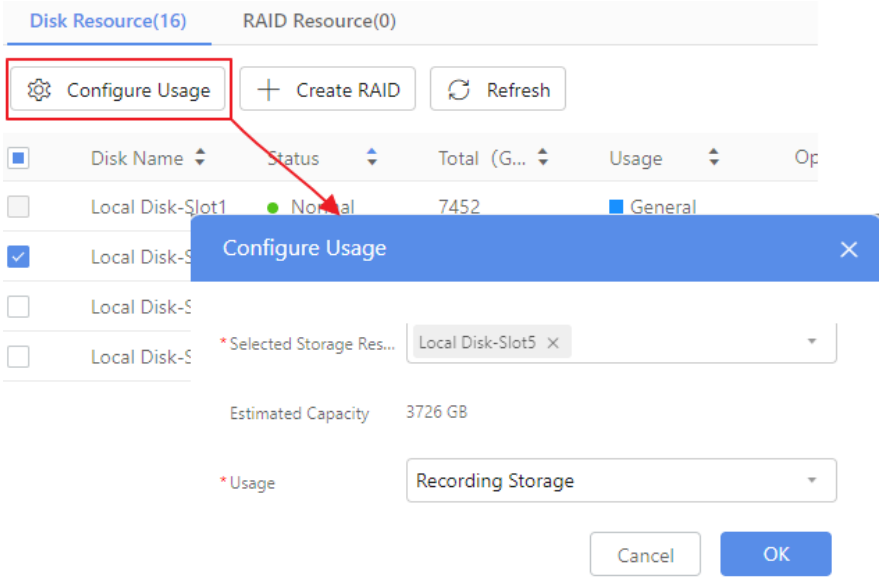
Set Disk Usage

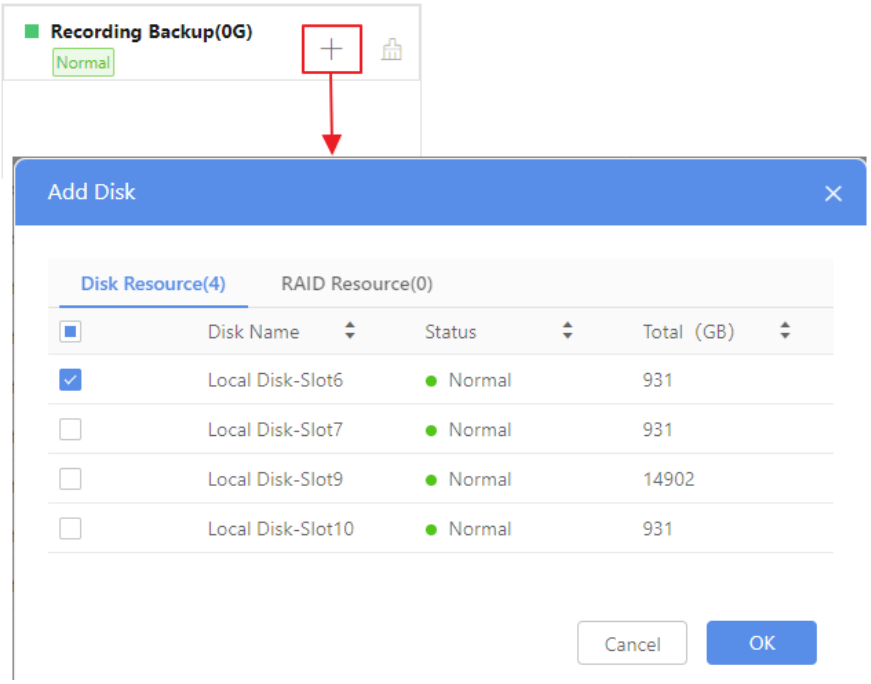
Disk Usage	Description
Image Storage	Used to store images.
Recording Storage	Used to store recordings.
Recording Backup	Used to store backup recordings.
Hot Spare	Once a disk is set as a hot spare, the RAID will automatically select the hot spare disk to replace any damaged disk during automatic rebuilding to ensure normal operation.

Two methods for configuring hard disk usages:

Note:

- Only hard disks with capacity greater than or equal to 512GB and in normal status can be configured with usage.
- Each hard disk can only be configured with one usage.
- The system automatically initializes the usage for slots 1/2/3 (Slot 1 – Image Storage, Slot 2 – Recording storage, Slot 3 –Recording backup). Supports clearing the usage and reconfiguring.

Method 1	1. In the disk list, select a disk in normal status but without usage configured, click **Configure Usage**. 2. Select the usage in the pop-up window, and then click **OK**. 

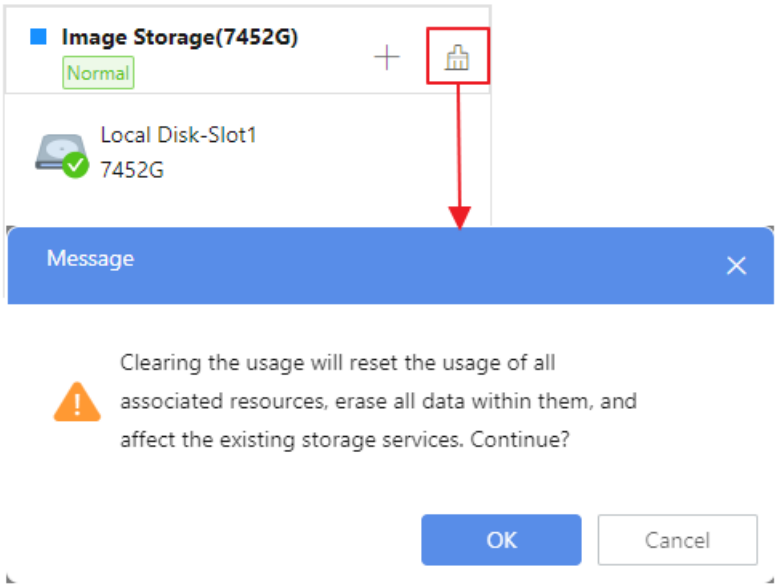
Method 2	1. Click + on the right side 2. Select the disk in the pop-up window, and then click **OK**. 

Clear Disk Usage

To modify disk usage, you must clear the disks/RAIDs of that usage and reconfigure.

Attention:

- After clearing a usage, all disks/RAIDs configured with this usage will be reset to "no usage," and all data on the resources will be erased -- affecting the existing storage services.
- If locked recording exists, it is not allowed to clear recording storage and recording backup usages.



29.7.1.2 RAID Resource

A RAID refers to combining multiple hard disks to work together to achieve higher performance, larger storage capacity, or enhanced data redundancy and fault tolerance.

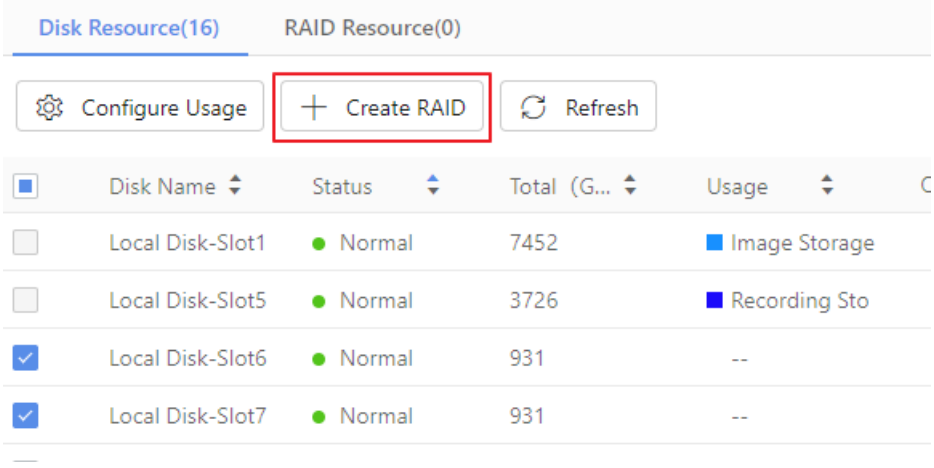
Type	Requirement	Description
RAID0	Number of hard disks: 2-8	• Feature: Striping Data is split into blocks and distributed across multiple disks. • Advantage: Delivers the highest read/write performance. Total storage capacity = N × (capacity of the smallest disk). • Disadvantage: No redundancy. A single disk failure will cause complete data loss across the array.
RAID1	Number of hard disks: 2	• Feature: Mirroring - Data is duplicated across two hard disks. • Advantage: Provides data redundancy - one failed disk won't compromise data integrity. • Disadvantage: Low storage efficiency, requires 2× disk space. Total capacity = capacity of the smallest disk.
RAID5	Number of hard disks: 3-8	• Feature: Striping with distributed parity - Data and parity information are spread across multiple disks. • Advantage: Provides data redundancy - one failed disk won't compromise data integrity. • Disadvantage: Requires minimum 3 disks. Capacity = (N-1) × capacity of smallest disk. Reduced write performance.
RAID6	Number of hard disks: 4-8	• Feature: Striping with dual parity - Stores redundancy equivalent to two disks' capacity. • Advantage: Higher fault tolerance – two failed disks won't compromise data integrity. • Disadvantage: Requires minimum 4 disks. Capacity = (N-2) × capacity of smallest disk. Further reduced write performance.

Create RAID

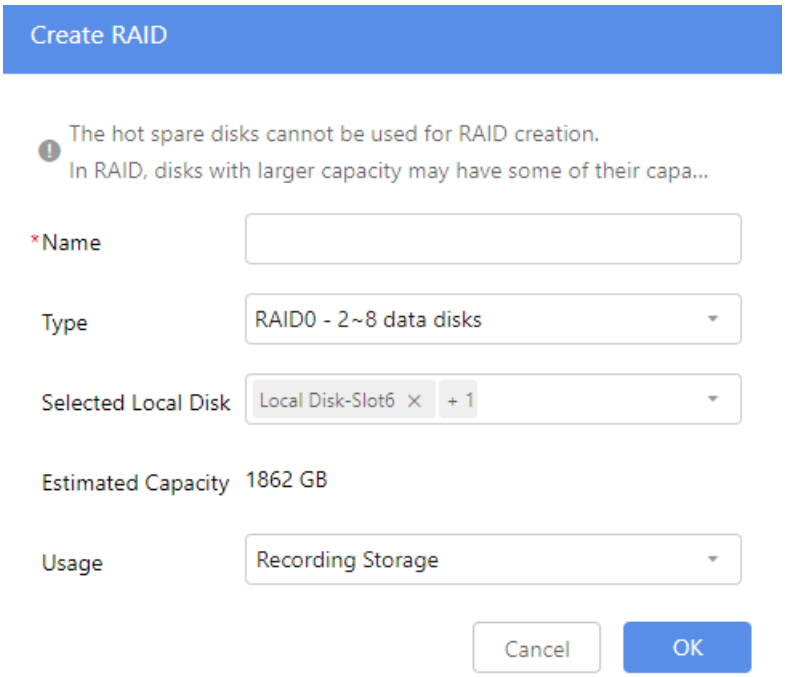
Attention:

- It is recommended to choose unused and normal hard disks to create RAID.
- Hot spare disks cannot be used to create RAID.
- When creating RAID, it is advisable to choose hard disks with the same capacity. If the capacities of the hard disks in the RAID are different, the effective capacity of the RAID will be calculated based on the capacity of the smallest hard disk, leading to wasted capacity on larger disks.
- The capacity of the RAID should be greater than or equal to 512GB. Please select hard disks that meet the capacity requirements according to the effective capacity calculation rules for different RAIDs.

1. Select the number of hard disks according to the RAID type. You may also select hard disks on the **Create RAID** page.



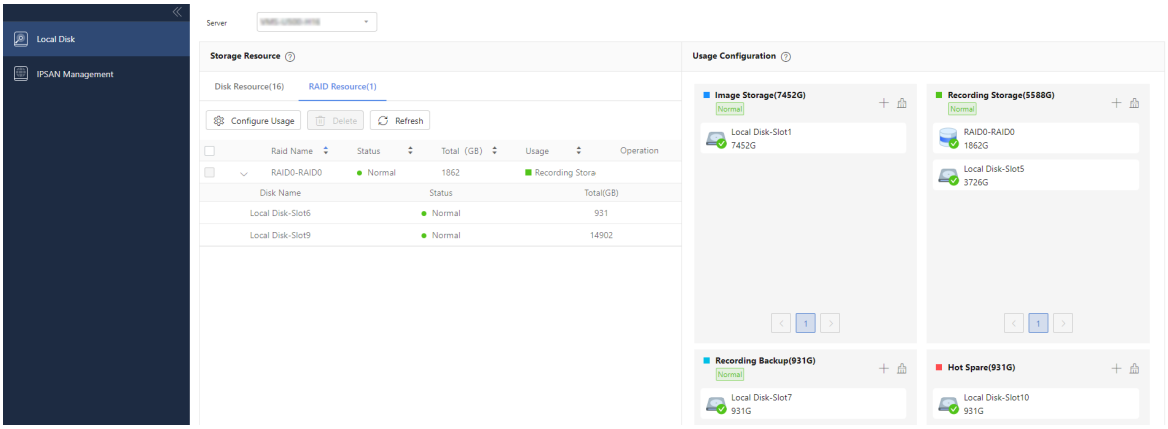
2. Click **Create RAID**.



3. Enter the RAID name, select the RAID type, choose hard disks for the RAID, and specify the RAID usage (Image Storage/recording storage/recording backup).
4. Click **OK**.
   Hard disks that have been added to the RAID are marked with after their names.

View RAID

After creating a RAID, you can view the RAID information in **RAID Resource** page.

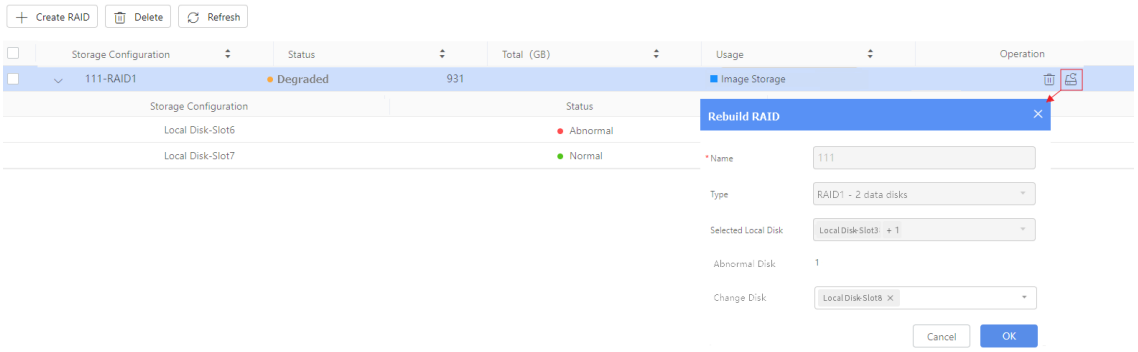


- Expand the RAID to view the included hard disks.
- RAID status includes:
  - Normal.
  - Degraded: The number of abnormal hard disks in the RAID is within the allowed range (different RAID types have different allowed ranges). Degraded RAID can be rebuilt.
  - Unusable: The number of abnormal hard disks in the RAID exceeds the allowed range, storage fails, and rebuild is impossible.

Rebuild RAID

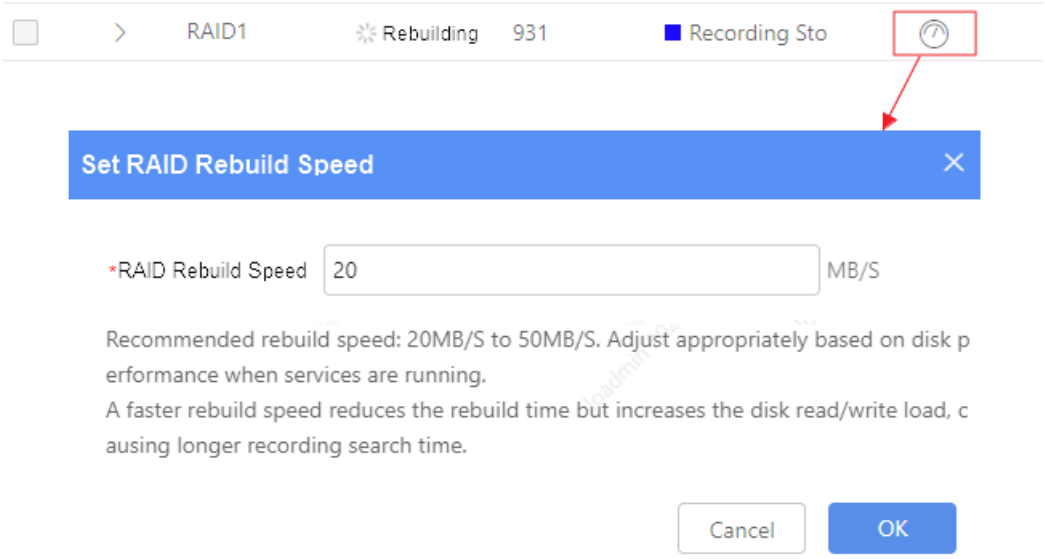
- Automatic rebuild: 10 minutes after the RAID degrades, if a hot spare disk is detected (the capacity of the hot spare disk must be ≥ the damaged disk), the system will automatically start the rebuild process and replace the damaged hard disk with the hot spare disk.

- Manual rebuild: Click for the degraded RAID, select a hot spare disk or a hard disk with no usage configured (its capacity must be ≥ the damaged disk), then click **OK** to start the rebuild process.



The rebuild process status progresses from "Initializing" to "Rebuilding," providing progress updates and estimated time remaining.

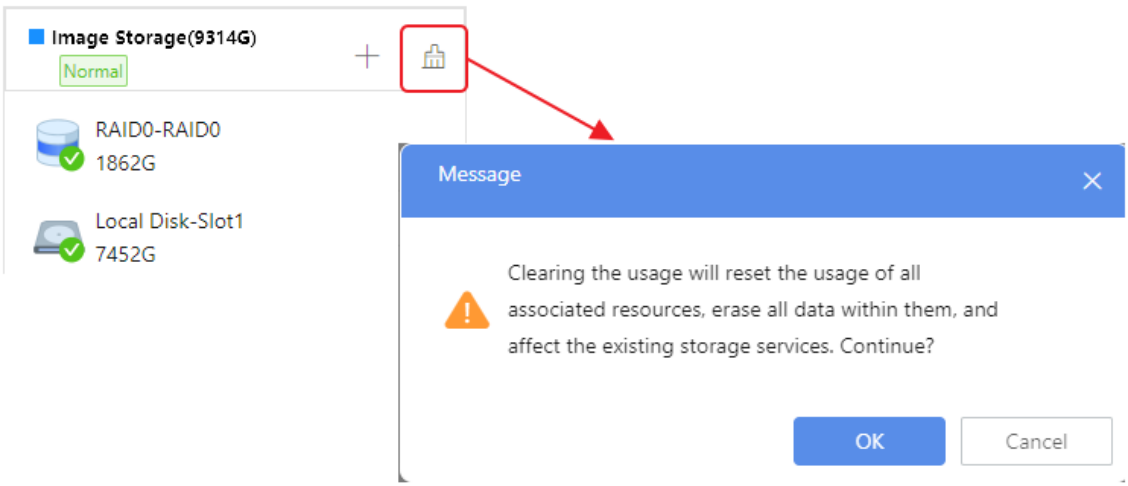
During the RAID rebuilding process, you can click in the **Operation** to view and adjust the rebuild speed (ranging from 1MB/s ~ 200MB/s, recommended 20MB/s~50MB/s). A faster rebuild speed reduces the rebuild time, but it increases the read/write load on the hard disks, causing longer video search times. Avoid high speed settings when disk performance is poor.



Note:
If the number of new disks is less than the number of damaged disks, the RAID will remain degraded after the rebuild. Once all damaged disks are replaced with new ones, the RAID status will return to normal after the rebuild.

Configure RAID Usage

- If usage configuration fails during the RAID adding process, or if the RAID usage is cleared, you can reconfigure RAID usage using the following methods:
  - Method 1: Select the RAID, click **Configure Usage**, and choose the usage.
  - Method 2: In the usage area on the right side, click +, select the RAID to add to the usage.
- If you need to modify the RAD usage, you will need to clear the hard disks/RAIDs associated with that usage and reconfigure.



Delete RAID

Select the RAID without usage configured, click **Delete**, and then confirm to delete the RAID.

Attention:
After the RAID is deleted, the hard disks in the RAID will become independent, resulting in irreversible data loss. The original storage services will be unavailable.

29.7.1.3 Cluster Environment

Primary/Replica Environment	
Configuration description	• View and configure the hard disks/RAIDs of replica servers on the primary server's interface: Select **Server** in the upper left corner to view the resources under the corresponding servers. • For the same storage usage, a single server will create only one storage resource; the primary and replica servers will create different storage resources.
Video storage	On Recording Storage > Recording Backup, by default, the system allocates the largest available recording storage/recording backup resources to the cameras. • If a camera is allocated the primary server's storage resource, its recordings will be stored on the primary server. • If a camera is allocated the replica server's storage resource, its recordings will be stored on the replica server.
Image storage	There is no need to manually allocate storage resources. • Business images from the primary server are stored in the primary server's image storage resources. • Business images from the replica server are primarily stored in the replica server's image storage resources; if the replica server lacks image storage resources, its images will be stored on the primary server.

29.7.2 IPSAN Management

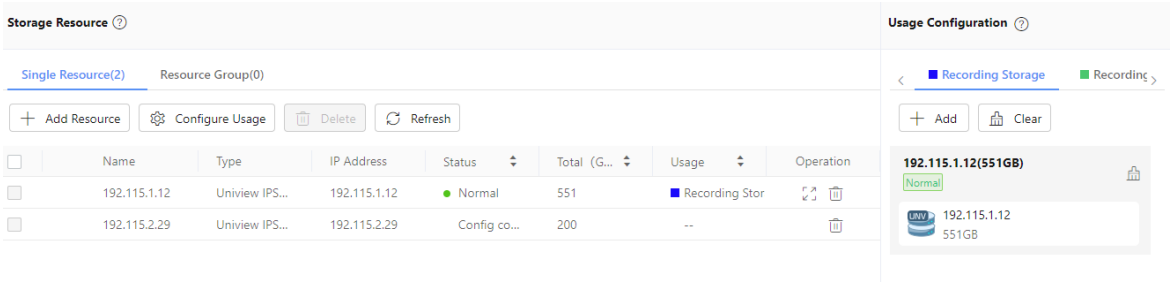
Add an Uniview IPSAN (support VX-U series and CX series, and the compatible VX-U component needs to be installed on the IPSAN) . You can also create a resource group consisting of multiple CX series IPSAN devices to expand the storage capacity.

After adding an IPSAN device, you need to configure its usage (Recording Storage/Recording Backup). The system will automatically create a storage resource for the usage.

Note:
IPSAN does not support image storage.

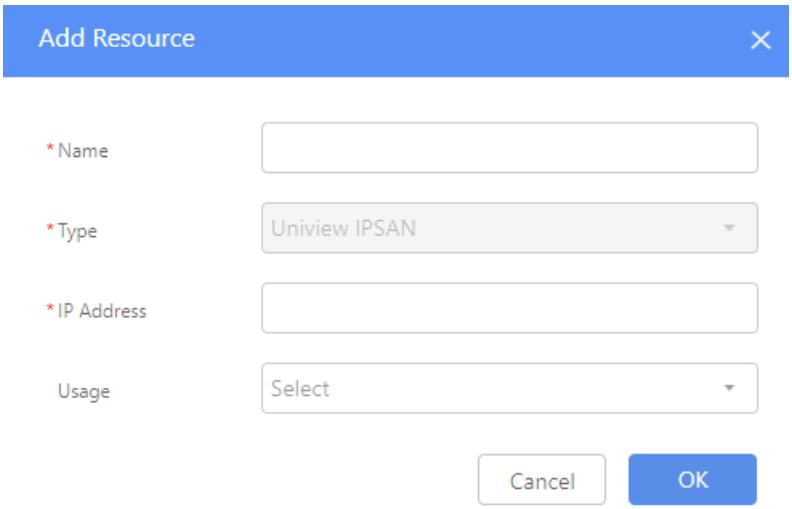
29.7.2.1 Single Resource

Add Uniview IPSAN and configure its storage usage.



Add Resource

1. Click **Add Resource**.



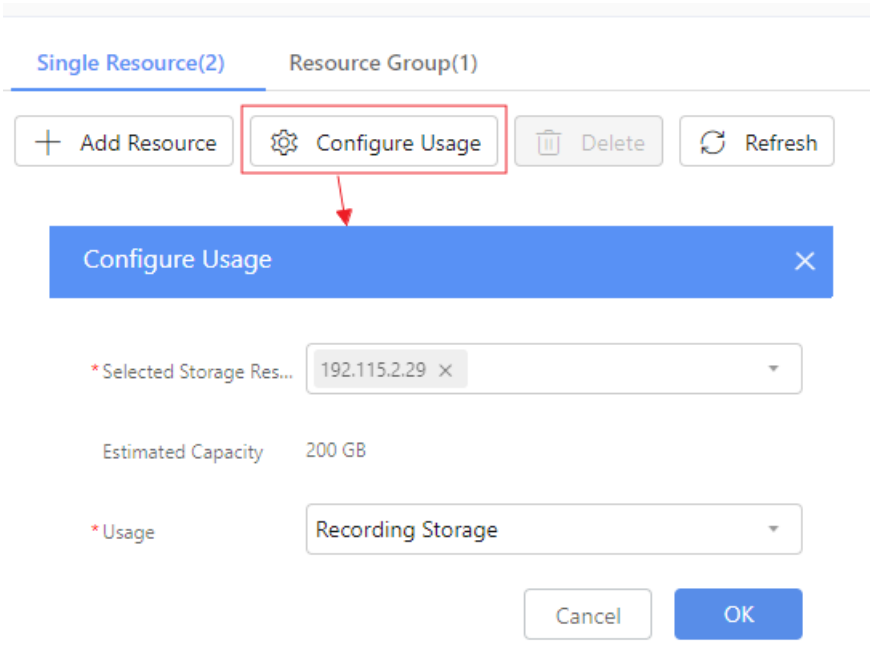
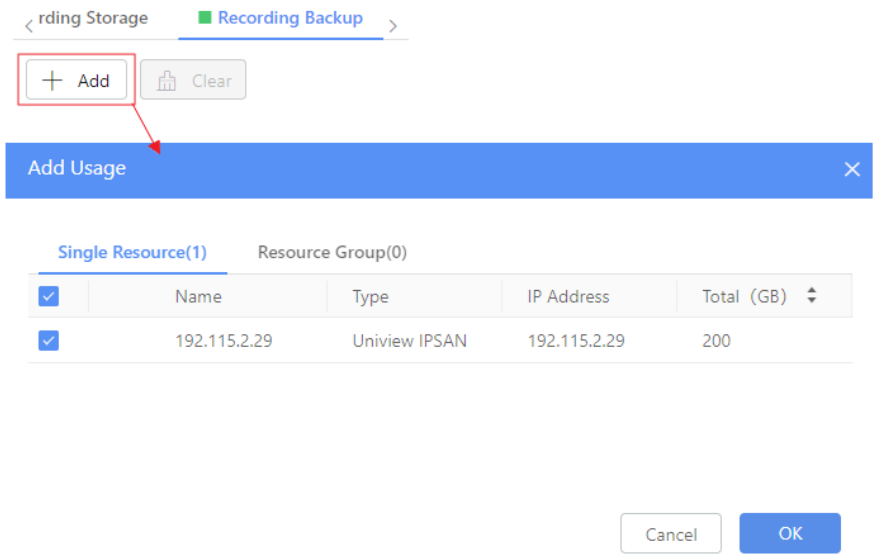
Item	Description
Name	Enter a custom resource name.
Type	Uniview IPSAN.
IP Address	Enter the IP address of the IPSAN device.
Usage	Select Recording Storage or Recording Backup as needed.

2. Click **OK**.

Configure Storage Usage

If the usage configuration fails during IPSAN adding or if the IPSAN usage is cleared, you can reconfigure its usage.

Method 1	1. In the device list, select normal IPSAN(s) with no usage, and then click **Configure Usage**. 2. Configure the storage usage in the pop-up window, and then click **OK**.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Method 2</td><td>1. Click + in the corresponding usage tab on the right.
2. Select IPSAN(s) in the pop-up window, and then click OK.
 
</td></tr>
</table>

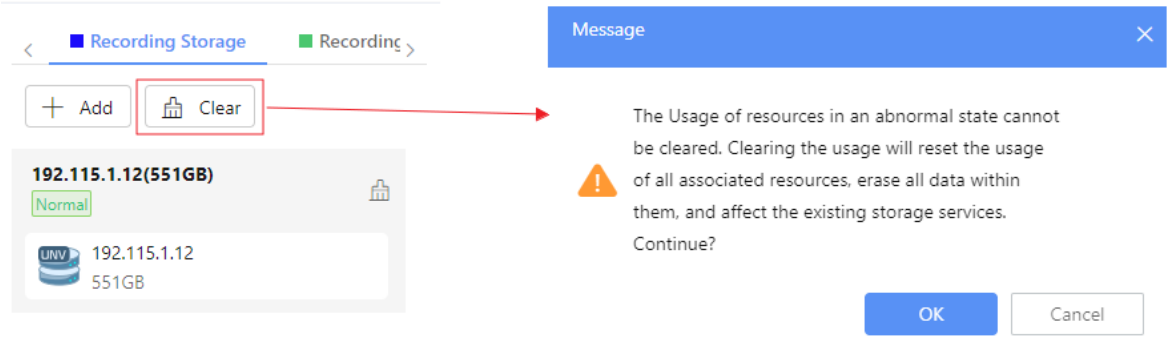
Clear Storage Usage

If you want to edit the IPSAN usage, you need to clear its current usage and reconfigure it.

Attention:

- Clearing the usage will erase all data within the IPSAN resource and affect the existing storage services.
- If locked recording exists, it is not allowed to clear recording storage and recording backup usages.

- Clear usage for all resources: Click **Clear** to reset all resources of that usage to no usage.
- Clear usage for a single IPSAN: Click in the upper-right corner of an IPSAN. The IPSAN usage will be reset to no usage.



Delete Resource

- Delete one by one: Click for an IPSAN and confirm the deletion.
- Batch delete: Select IPSANs with no usage, click **Delete**, and then confirm the deletion.

Attention:

- After deletion, the storage data will be lost and cannot be recovered, and the existing storage services will be unavailable.
- If the IPSAN is part of a resource group, you must unbind the resource group before deletion.

29.7.2.2 Resource Group

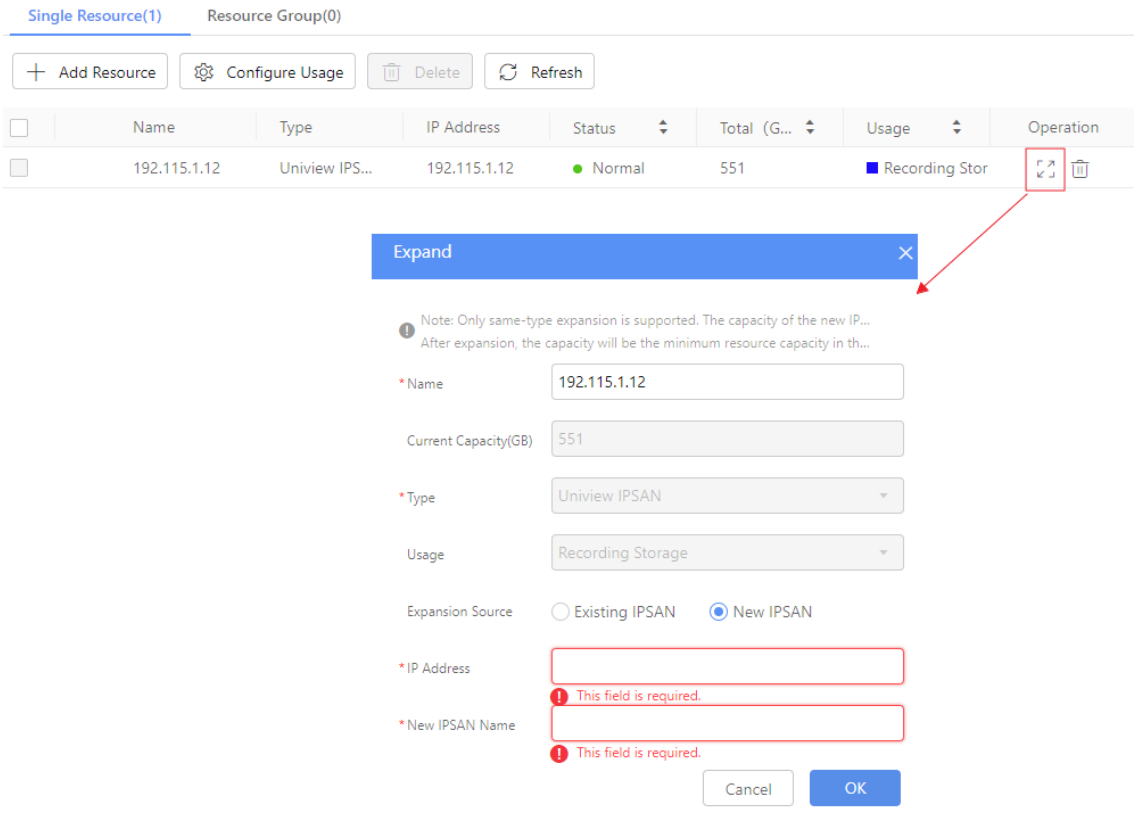
Create resource group consisting of multiple Uniview IPSANs to expand the storage capacity and enhance the reliability.

Note:
The CX series storage device supports resource group creation, while the VX-U series does not.

Add Resource Group

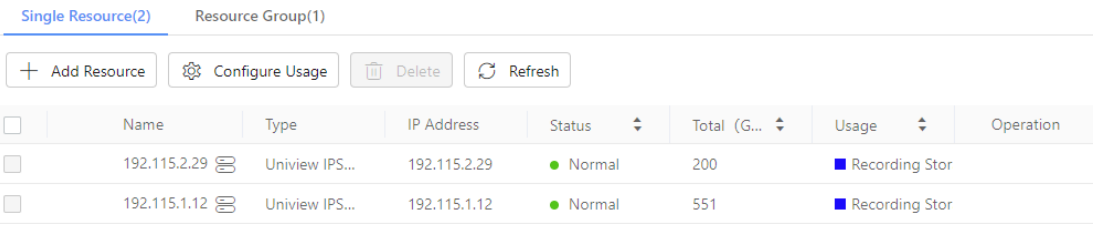
Only **normal** IPSANs with **usage configured** can be expanded to a resource group.

1. On the **Single Resource** tab, click for an IPSAN.



Item	Description
Name	Enter a custom resource group name.
Usage	The resource group inherits the usage configuration of the IPSAN before expansion. This field is non-editable.
Expansion Source	• Existing IPSAN: Select existing IPSAN with no usage configured. • New IPSAN: Enter the IP address and name of the new IPSAN. **Note:** • The new IPSAN's capacity must be greater than or equal to the minimum capacity of the IPSAN in the current group. • The new IPSAN must be a Uniview IPSAN.

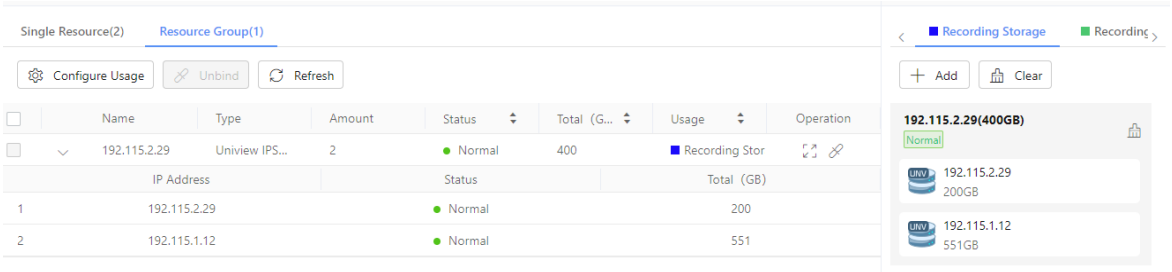
2. Click **OK**.
   - A icon will appear next to the name of the IPSAN that has been added to a resource group.



   - A single IPSAN can only be expanded once. Subsequently, you can continue to expand the normal resource group with usage configured: Click for a resource group to add more IPSANs. See operations in **Add Resource Group**.

View Resource Group

After creating a resource group, you can view it in the **Resource Group** tab.



- Unfold a resource group to view the IPSAN devices in it.
- Total group capacity = Number of IPSANs in the group * Smallest capacity of IPSAN in the group.
- Resource group statuses:
  - Normal: All devices in the resource group are online.
  - Partially Online: Some of the devices in the resource group are offline.
  - Offline: All devices in the resource group are offline.

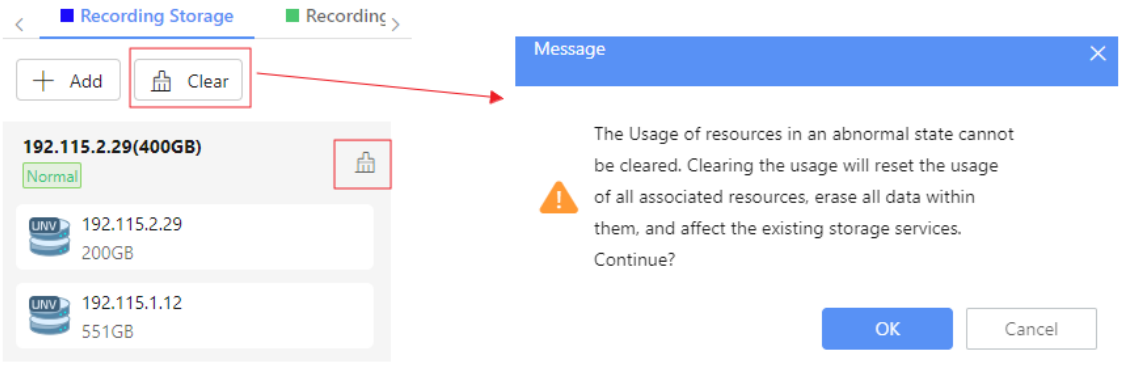
Configure Resource Group Usage

- If the usage of a resource group is cleared, you can reconfigure its usage.
  - Method 1: Select resource group(s), click **Configure Usage**, and then select a usage.
  - Method 2: Click + in the corresponding usage tab on the right, and then select resource group(s).
- If you want to edit the resource group usage, you need to clear its current usage and reconfigure it.

Attention:

- Clearing the usage will erase all data within the resource group and affect the existing storage services.
- If locked recording exists, it is not allowed to clear recording storage and recording backup usages.

- Clear usage for all resources: Click **Clear** to reset all resources of that usage to no usage.
- Clear usage for a single resource group: Click in the upper-right corner of a resource group. The resource group usage will be reset to no usage.



Unbind

- Unbind one by one: Click for a resource group and confirm the operation.
- Batch unbind: Select resource groups with no usage, click **Unbind**, and then confirm the operation.

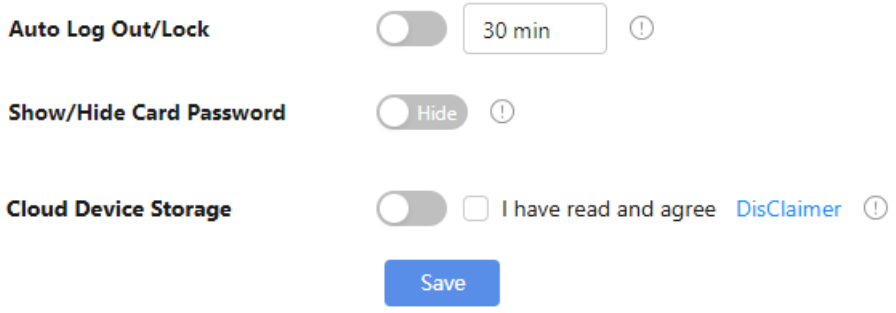
Attention:
After unbinding, the resource group will no longer exist, the IPSAN devices under it will be independent with their usage cleared, the stored data will be lost and cannot be recovered, and the existing storage services will be unavailable.

29.8 Advanced Configuration

Press the shortcut key **Ctrl+Shift+Alt+Y** on the homepage to enter the **Advanced Config** page and configure some system parameters.

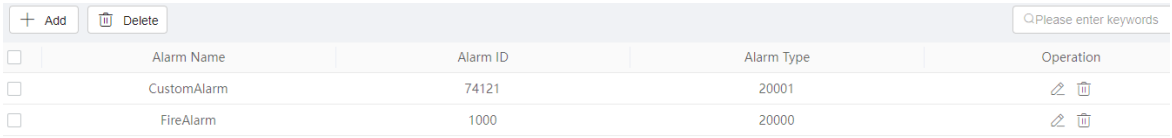
29.8.1 Function Switch

Use toggle buttons to enable/disable functions.

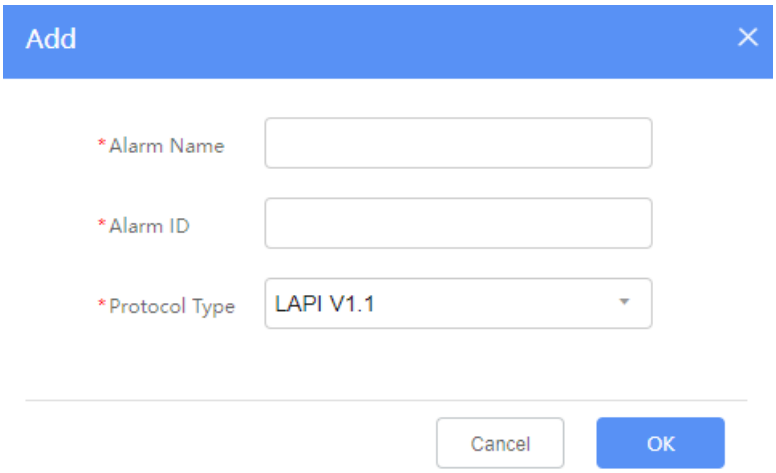


29.8.2 Alarm Customization

You can add alarms types of third-party devices on the platform to receive alarms reported by them. After adding alarm types here, you can view the added alarm types under the **General** category in Alarm Configuration and Alarm Linkage Configuration.



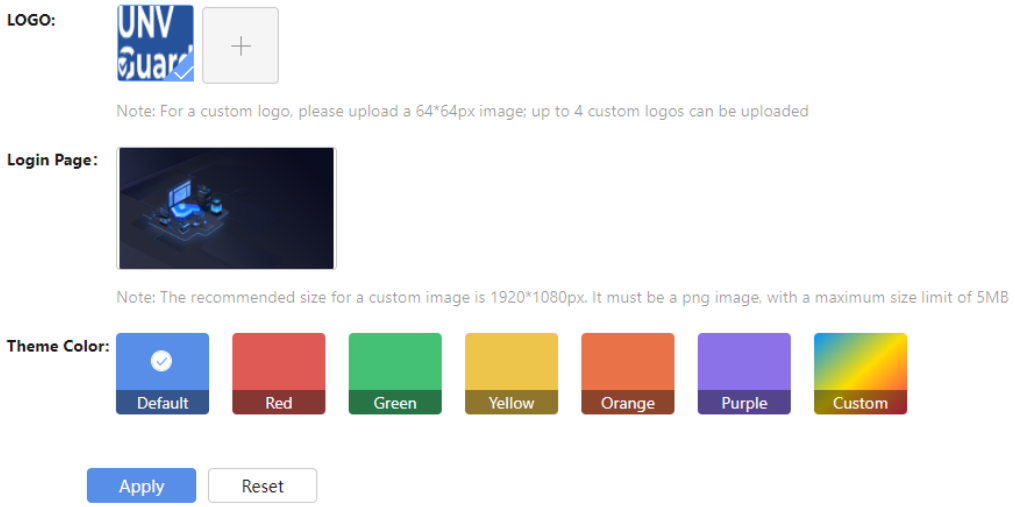
1. Click **Add**.



2. Enter the alarm name and ID (must match the one in the third-party device).
3. Click **OK**.

29.8.3 Style Personalization

Customize the system logo, and background image of the login page.



1. Customize the settings as needed.

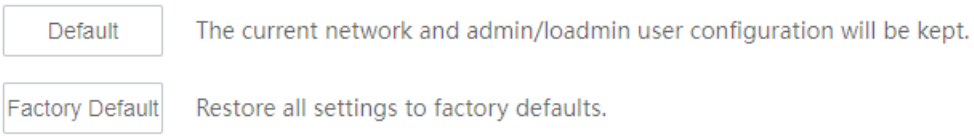
LOGO	The logo is displayed on the login page and the system's upper-left corner. (1) Click + to upload a logo image (.png format; resolution: 60px*64px). (2) Select the target logo image. A "√" will appear at the lower-right corner of the selected image.
Login Page	Set the background image for the login page. Hover the mouse over the image, and then click ↑ to upload a new image (.png format, resolution: 1920px*1080px). After uploading, the new image will replace the existing background image.
Theme Color	Change the color of the interface elements (menu bar, buttons, highlighted texts, etc.). The default is blue. You can choose other colors as needed.

Note:
The theme color configuration is permanently valid to all users and all clients (B/S client and C/S client).

2. Click **Apply** to activate the settings.

29.8.4 Restore Defaults

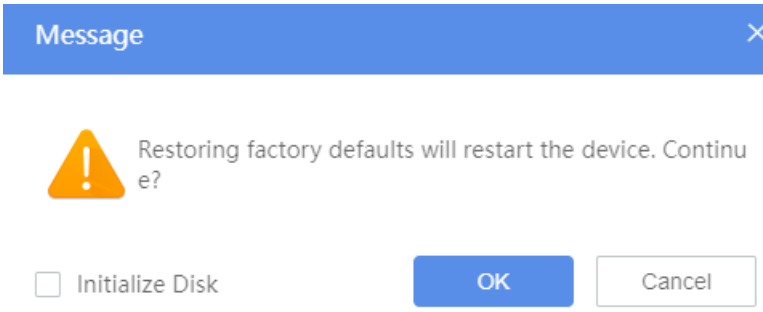
You can restore the server to factory defaults. This operation will clear all data and configuration. Please handle with caution.



- Default: Restore all factory default settings except network and admin/loadmin user configuration.
- Factory Default: All settings will be restored to factory defaults.

Note:
After clicking **Default** or **Factory Default**, in the pop-up prompt window:

- If **Initialize Disk** is checked, the hard disk's storage configuration will be cleared and all data on the disk will be deleted. The data cannot be recovered using database backup files.
- If **Initialize Disk** is not checked, the hard disk's storage configuration and existing data will be preserved.



29.9 License Management

License is used to authorize the system's supported functions and capacity.

The system provides a free version with limited functions by default. To access full functions, please import a license file.

Note:
Only the **administrator** can manage licenses.

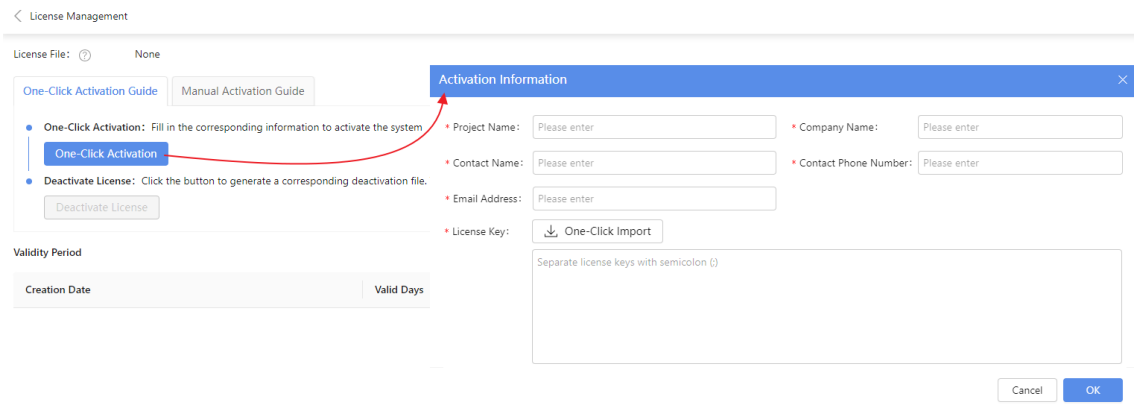
29.9.1 License One-Click Activation

Activate licenses online in an Internet-connected environment.

Note:
Please contact our sales personnel in advance to obtain the license key.

1. Click ⚙ in the upper-right corner of the page, and select **License Management > One-Click Activation Guide**.
2. Follow the on-screen instructions: ① Click **One-Click Activation**, fill in the user information and the license key. ② Click **OK**. After verification is passed, the activation will proceed directly.
   - Input license keys: Separate license keys with semicolon.

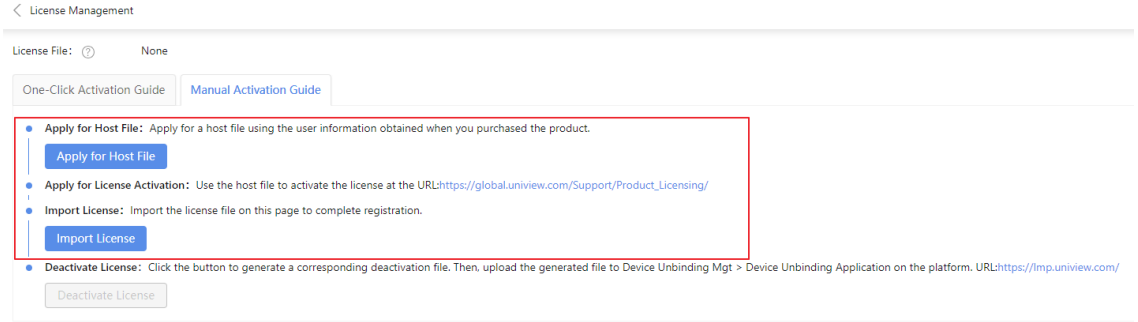
- One-Click Import: Click **One-Click Import**, download the template in the pop-up window, fill in the license keys in the template, and once the template is successfully imported, the license keys will be automatically populated into the input field.



3. After activation is complete, the system will restart and return to the login page. Please log in again.

29.9.2 License Manual Activation

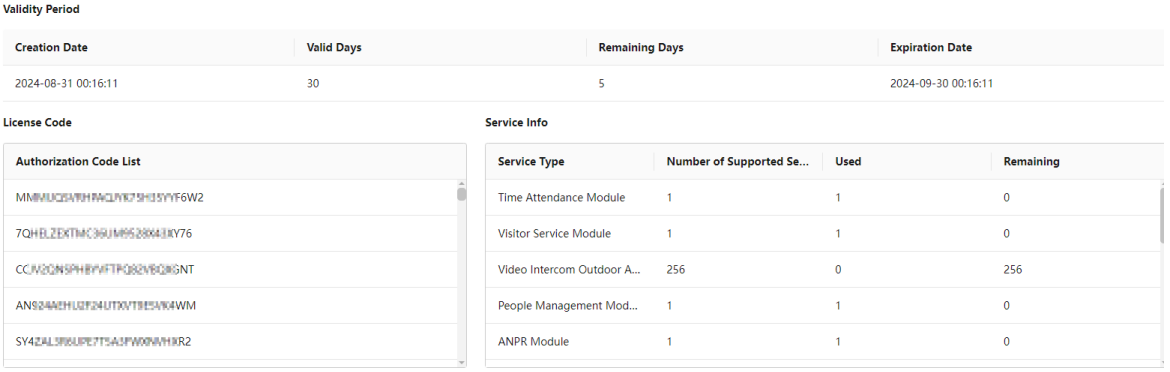
1. Click ⚙ in the upper-right corner and select **License Management > Manual Activation Guide**.
2. Follow the on-screen wizard to import a license file: ① Click **Apply for Host File** and then enter the user information to apply for a host file; ② Use the host file to activate the license on our company's official website (https://global.uniview.com/Support/Product_Licensing/); ③ Click **Import License** to import the license file.



3. When imported, the system will restart and return to the login page. Please log in again.

29.9.3 View License

After successfully importing the license, you can view the license's expiration date and the authorization details.



- If the license has 5 or fewer days remaining, the remaining days will be displayed at the top of the interface (or in the login page). Please import a new license as soon as possible to avoid any disruption to your normal use.
- The authorization details include the available subsystems and the number of devices allowed for connection.

29.9.4 License Deactivation

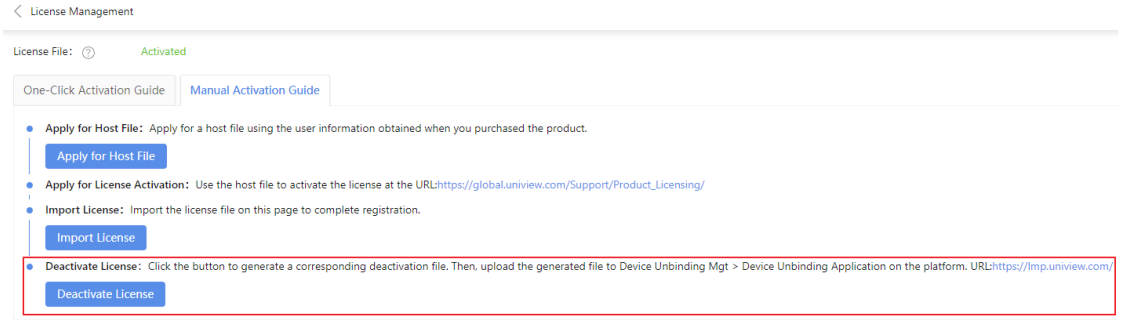
License deactivation restores the system to its original status before a license was imported.
Scenario Example: When changing servers, if Server A has a license applied using its host.id and an authorization code, you need to deactivate the license and unbind the authorization code from Server A's host.id first. Then, use Server B's host.id and the authorization code to apply for a new license for Server B.

Note:
Once the license is deactivated, the Server will no longer be able to use the original license.

License deactivation process: ① Generate the deactivation file > ② Submit the unbinding application.

Generate Deactivation File

1. Click ⚙ in the upper-right corner of the page and select **License Management**, enter the **One-Click Activation Guide** or **Manual Activation Guide** interface.



2. Click **Deactivate License**.
3. In the **User Verification** pop-up window, enter the current user's login password and click **OK**.
4. The system will prompt “The system license will be immediately unavailable after deactivation”. Acknowledge the risks and click **OK**. Then, the system will automatically generate and download the license deactivation file (deactive.id).
5. Re-log in to the system, and check that the authorization code is no longer listed on the **License Management** page.

Submit Unbinding Application

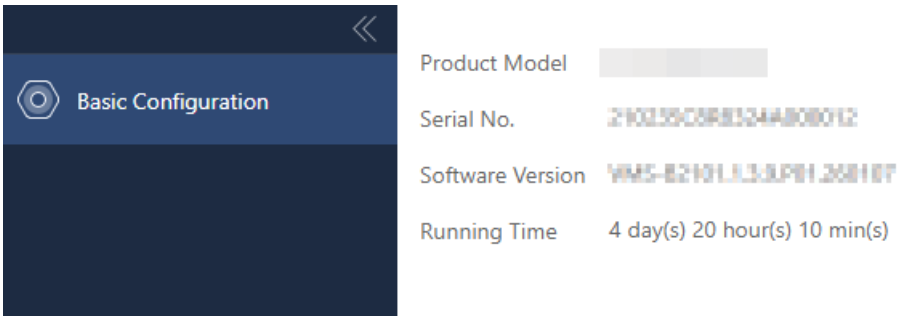
Access to the license unbinding website requires permissions. Please contact our technical support to obtain access.

To proceed:

1. Log in to the website at https://lmp.uniview.com/ and go to the **Device Unbinding Application** page.
2. Select the product category.
3. Upload the device's host.id and the deactivation file separately, and complete the required fields.
4. Click **Submit** to unbind the authorization code from the host.id.

29.10 Basic Configuration

Go to **Basic Configuration > Basic Configuration** to view the basic configuration information of the server, including product model, serial number, software version, and running time.



30 Operations&Maintenance

30.1 Operation Logs

View the operations performed by the user in system's functional modules.

- Set criteria and click **Search** to search the operation logs that match the criteria.
- Select operation log(s) and click **Export** to export them.

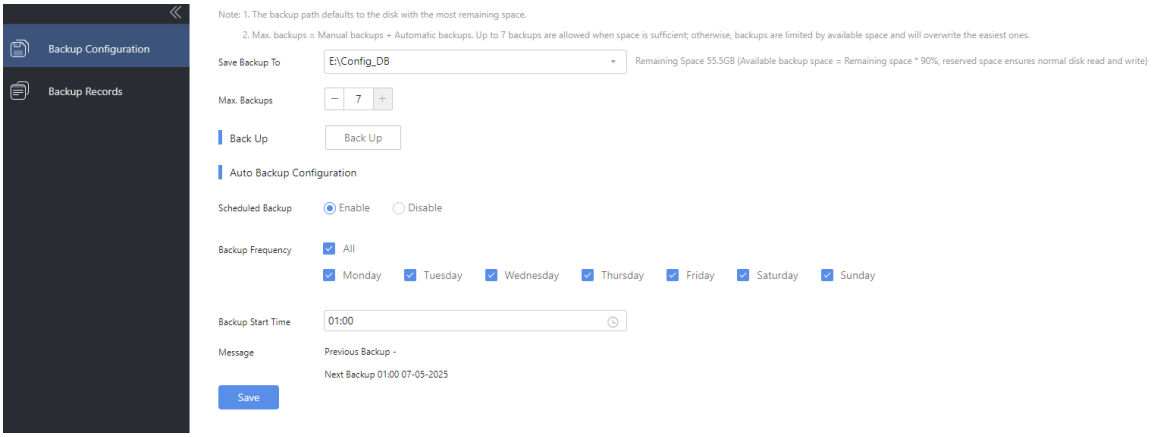
30.2 Database Backup

Operations&Maintenance > Database Backup

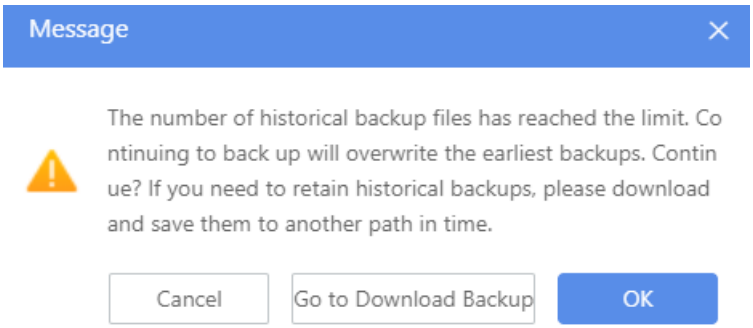
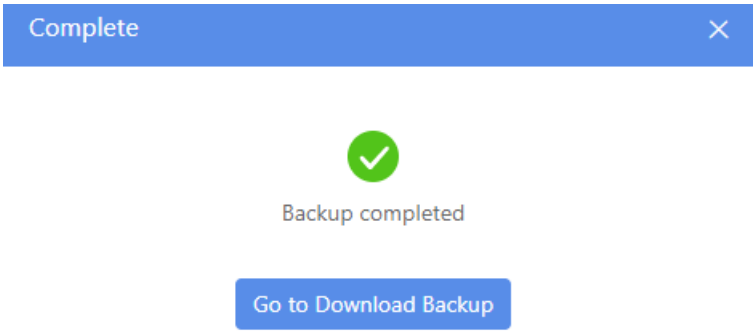
By using scheduled backup and manual backup functions to back up database data, you can restore the database to a specific point in time from backup files in case of data loss or configuration errors.

Note:
Backup and restoration operations will consume certain system resources, so it is recommended to perform these tasks during idle periods.

Backup Configuration

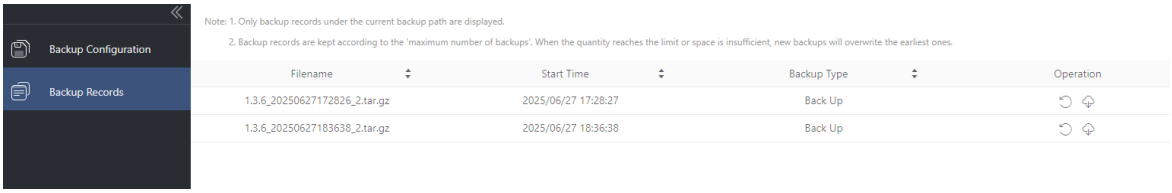


1. Choose the backup path where the backup files will be stored. By default, the backup files are saved in the disk with the largest remaining space on the PC where the service is located, and it is advisable to select a non-system disk.
2. Set the maximum number of backups (manual + automatic) that can be retained, up to a maximum of 7. If there is not enough space, the actual number of backups supported will be performed.
   Once the maximum number is reached, new backups will overwrite the oldest backup.
   When you reduce the maximum number, the system will delete historical backups in the current path that exceed the limit.
3. Click **Save**.

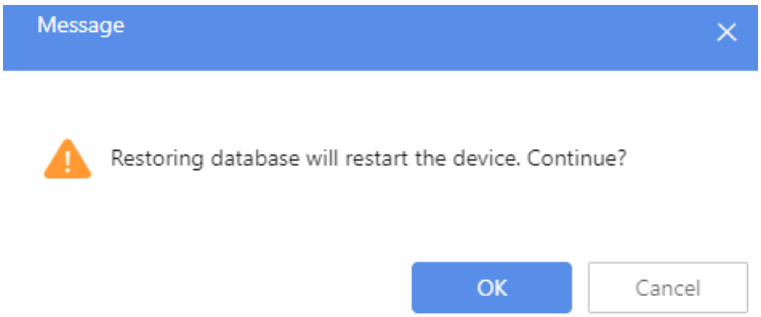
Manual Backup	1. Click **Back up**. 2. The system will perform the following operations based on the current number of historical backup files: • If the number of historical backup files has not reached the backup count limit: the system starts backup directly. • If the number of historical backup files has reached the backup count limit: the system displays a prompt:  • Click **Go to Download Backup** to navigate to the **Backup Records** page, where you can download historical backup files to your local computer. After downloading, perform the manual backup operation if needed. • If you do not need to download historical backups, click **OK**; the system will overwrite the oldest backup file and start this manual backup. 3. After the backup is complete, click **Go to Download Backup** to go to the **Backup Records** page and download the backup file to your local computer. 
Scheduled Backup	1. Enable scheduled backup. 2. Set the backup date and time, and the system will automatically perform backup at the specified date and time on a weekly cycle. 3. Click **Save**.

Backup Records

You can view completed backup tasks in the **Backup Records** page.



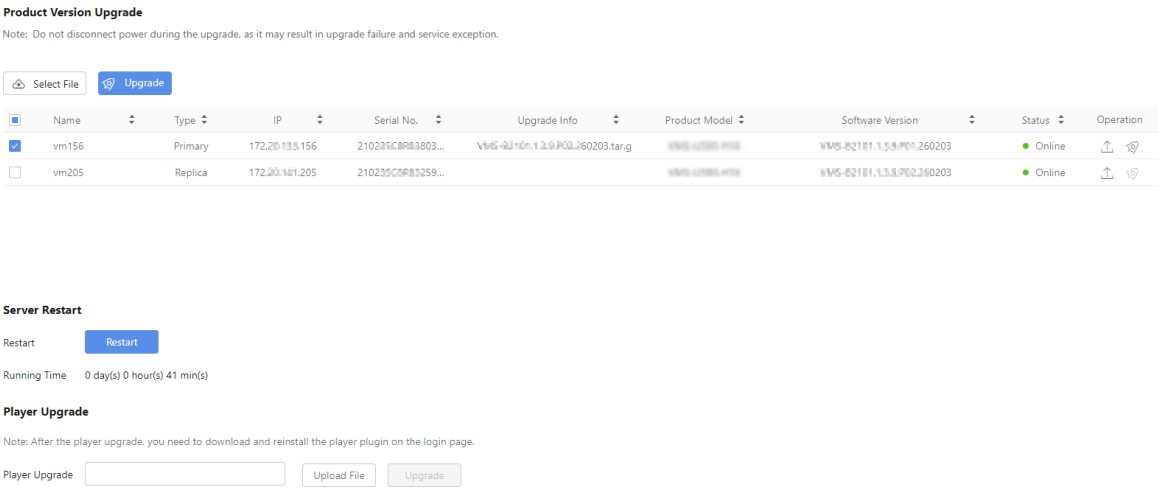
Restore	1. Click . A message appears, indicating that restoring the database will restart the device. Click **OK** to start restoring.

	 2. The restoration process may take some time, so please be patient and do not disconnect the power. 3. After the device restarts, it will automatically return to the login page. And you need to log in again.
Download	Click to download the backup file to your local computer. **Note:** • To avoid overwriting the backup file, please download it timely. • To restore using a local file, copy the file to the backup path. The **Backup Records** page will detect and load the local file, after which you can perform the restoration.

30.3 Restart&Upgrade

Go to **Operations&Maintenance > Restart&Upgrade**.

Upgrade the system software version, player version, restart the device.



Product Version Upgrade

Attention:

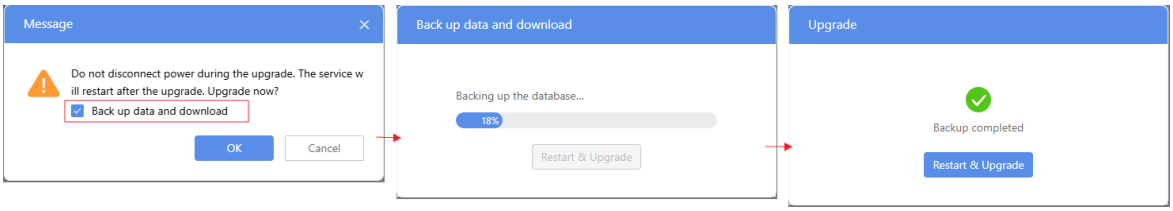
- Before upgrading, ensure that the system services are normal, and the network connection is stable.
- Do not power off the device during the upgrade process, as it may result in upgrade failure and service abnormality.
- The system will restart during the upgrade process, causing service interruption. Proceed with caution.
- The previous system configuration and data will be retained after the normal upgrade, but it is recommended to manually back up data in case of upgrade issues.
- If upgrading from the current version to the modular version, some functions have been optimized in the modular version, which may result in functional differences after the upgrade. Please contact technical support for evaluation.

Single-node/Primary-Replica Mode Upgrade

Upgrades for both Primary server and Replica server are performed in the Primary's interface.

Upgrade One by One	1. Click next to the server, select a new software package from your computer, and upload it to the server. 2. Click next to the server.
Batch Upgrade	1. Select the servers to upgrade; both Primary and Replica can be selected simultaneously. 2. Click **Select File**, select and upload a new version package from your computer. The package will be distributed to the selected servers. 3. Select the servers and click **Upgrade**.

In the pop-up prompt, select "**Back up data and download**", wait for the data backup to complete before continuing the upgrade, so that data can be restored in case of upgrade issues.



The upgrade progress will be displayed in **Upgrade Info** column, wait for the restart to complete and then log in again.

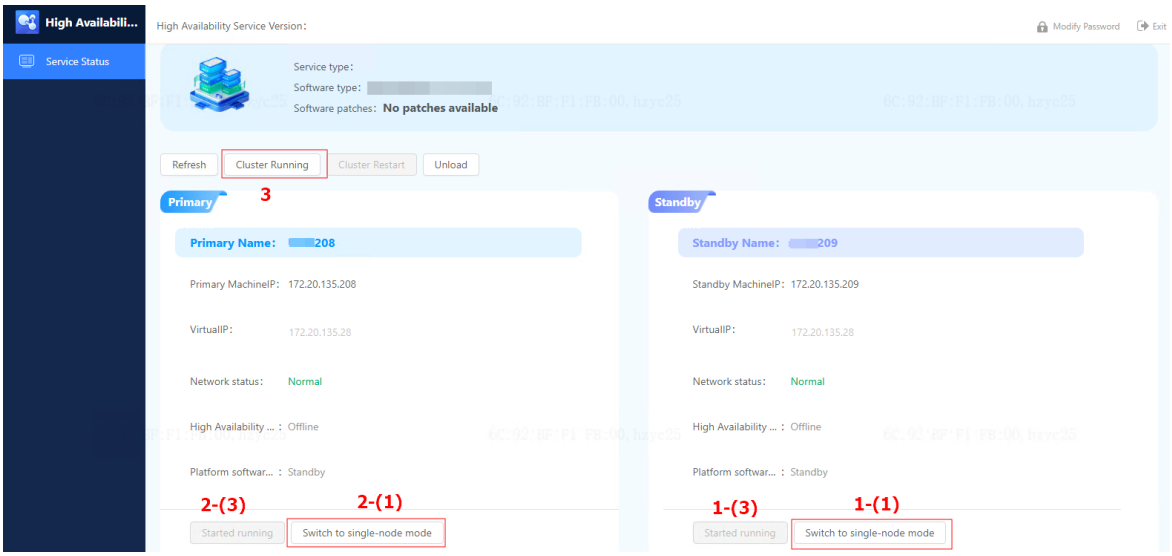
Primary/Standby Mode Upgrade

Attention:

- You must switch to single-node mode in the High Availability interface ("**http://standby server IP:9820**") before upgrading.
- The primary and standby servers cannot be upgraded simultaneously. The standby server must be upgraded first, and only after it completes can the primary server be upgraded.
- Before upgrading, ensure that the High Availability service is running normally.

The primary/standby upgrade procedure is as follows. For details, refer to the *Deployment Guide*.

1. Upgrade the standby server.
   (1) Log in to the High Availability interface and switch the standby server to single-node mode.
   (2) Log in to the standby server interface and upgrade it. After the standby server upgrade & restart is complete, log in to the standby server to verify the version number is correct.
   (3) Log in to the High Availability interface and stop the standby server from running.
2. Upgrade the primary server.
   (1) Log in to the High Availability interface and switch the primary server to single-node mode.
   (2) Log in to the primary server interface and upgrade it. After the primary server upgrade & restart is complete, log in to the primary server to verify the version number is correct.
   (3) Log in to the High Availability interface and stop the primary server from running.
3. Re-enable the cluster.



Server Restart

Attention:
Restarting the device will interrupt the service. Proceed with caution.

1. Click **Restart**.
2. The system will return to the login page. Please wait for the restart to complete and then log in again.

Player Upgrade

Attention:

- Before upgrading, ensure that the system services are normal, and the network connection is stable.
- Do not power off the device during the upgrade process, as it may result in upgrade failure and service abnormality.
- Exiting the page during the upgrade will not interrupt the upgrade.

1. Click **Upload File**, select and upload the new player version package from your computer.
2. Click **Upgrade**. The upgrade progress will be displayed.
3. After the player upgrade, you need to download and reinstall the player plugin on the login page.

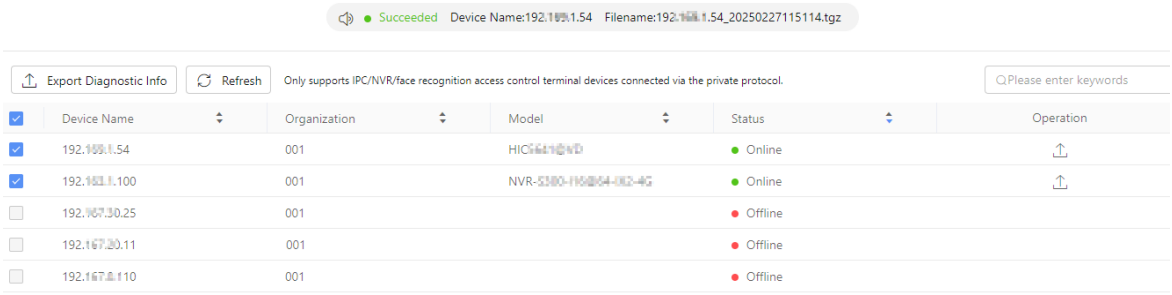
30.4 System Diagnosis

30.4.1 Device Diagnostic Info

Export diagnostic information of IPC/NVR/face recognition access control terminal devices that directly connected to the platform via the private protocol.

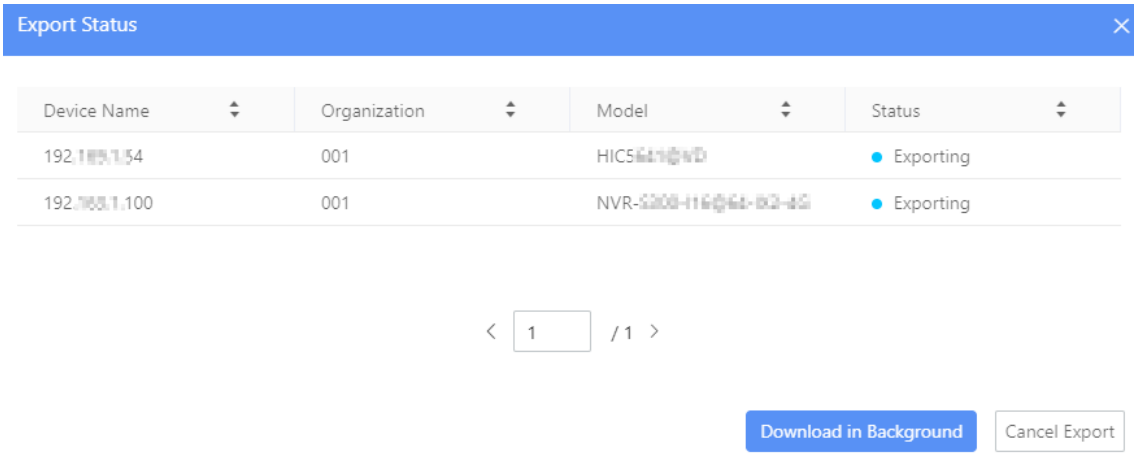
Real-time Diagnostic Information

Real-time diagnostic information can only be exported when the device is online.

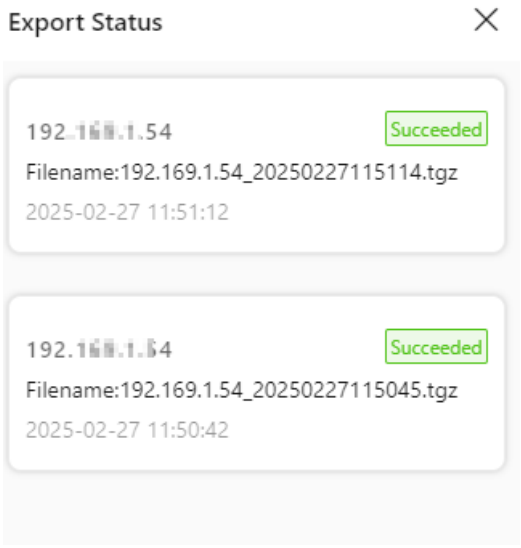


1. Click in the **Operation** column or select multiple devices and click **Export Diagnostic Info**.

2. In the pop-up **Export Status** window, you can view export status and choose **Download in Background** or **Cancel Export** for ongoing export tasks as needed.



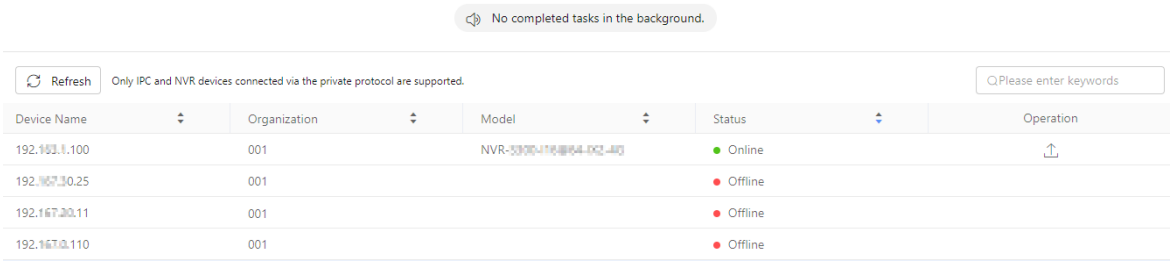
3. The latest export status is displayed at the top of the page. You can click the prompt to view all export records.



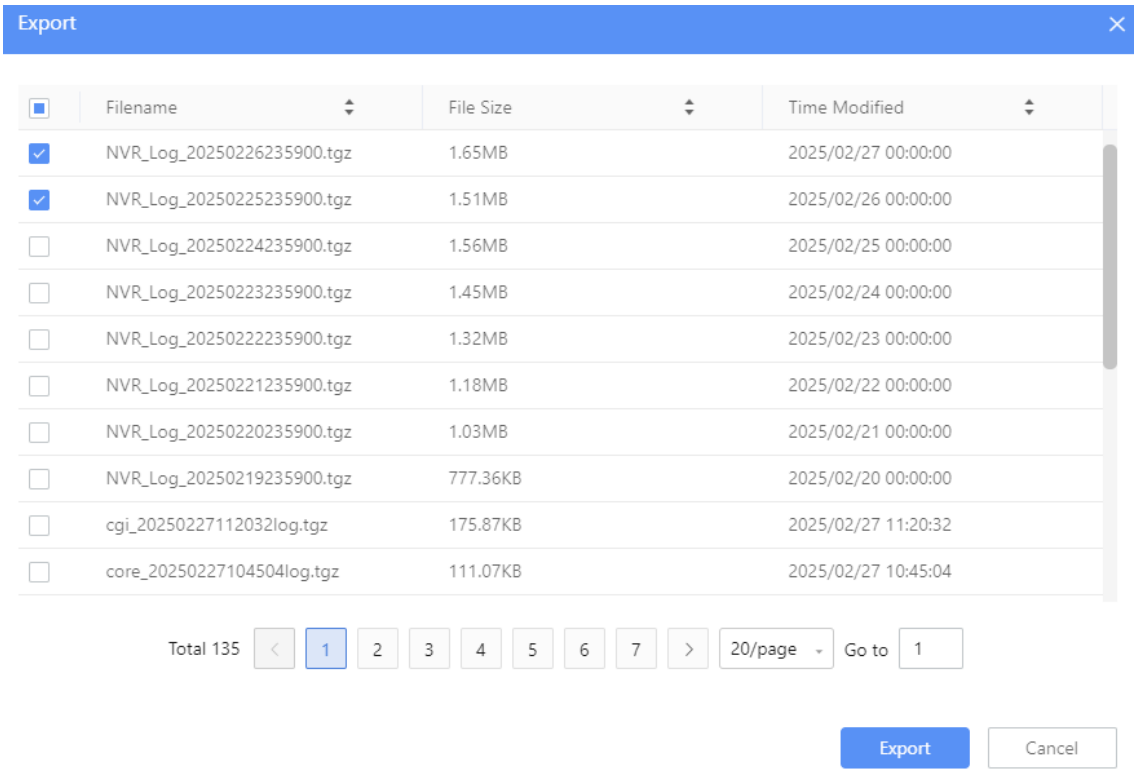
Historical Diagnostic Information

After exporting real-time diagnostic information for devices, you can view previously packaged diagnostic information in **Historical Diagnostic Info**. You can export diagnostic information from the past 15 days at most.

Historical diagnostic information can only be exported when the NVR is online (the IPC does not have to).



1. Click in the **Operation** column.
2. In the **Export** window, you can view the diagnostic information files available for export for that device.



3. Select diagnostic information file(s) and click **Export**.
4. In the pop-up **Export Status** window, you can view export status and choose **Download in Background** or **Cancel Export** for ongoing export tasks as needed.

30.4.2 Server Diagnostic Info

Export diagnostic information of the server for troubleshooting.

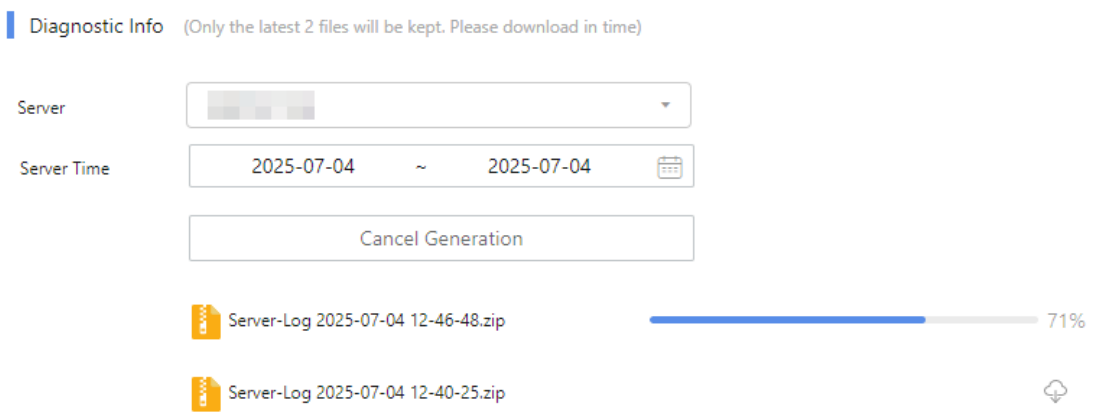
Diagnostic information includes service logs, installation logs, configuration information, etc.

1. Select the server, which can be the primary or replica server.
2. Specify a server time period and click **Generate** to create a compressed package of the diagnostic information within that period. During the generation process, you may click **Cancel Generation** to cancel the task.

   Note:
   During the generation process, if the disk space is insufficient (less than 4GB), the task will automatically stop, and the status will show "failed"

3. Click to download the compressed package to local.

   Note:
   The system can keep the latest 2 compressed packages. Please download in time to avoid being overwritten by new files.



30.4.3 Server Packet Capture

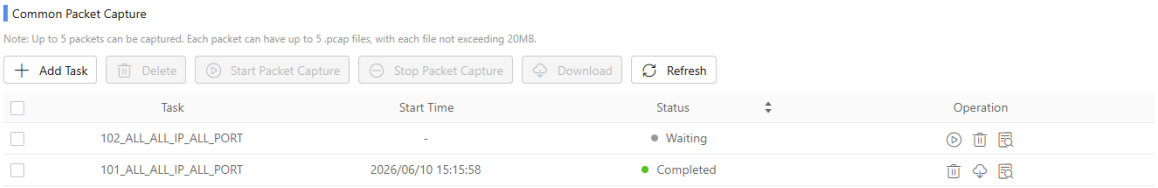
Perform network packet capture on the server to collect interaction messages between the server and network devices, thereby understanding network data exchange details and locating network issues.

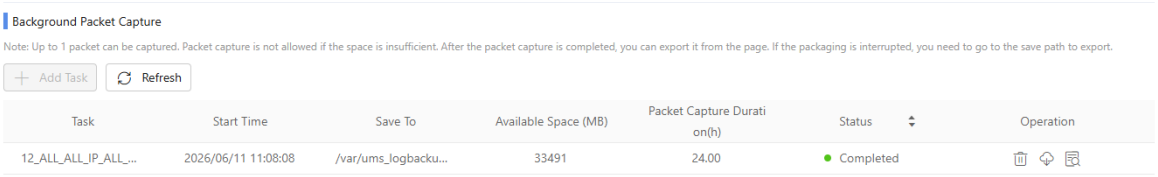
Note:
Network devices can be any devices added to the server, PCs accessing the server, or other devices.

Two packet capture modes are available:

- Common packet capture: Short-duration packet capture for reproducible issues, generating smaller capture files.
- Background packet capture: Long-duration packet capture for intermittent issues, generating larger capture files.

Note:
By default, only **Common Packet Capture** is displayed. To display **Background Packet Capture**, press **<Ctrl+Alt+Shift+B>**.





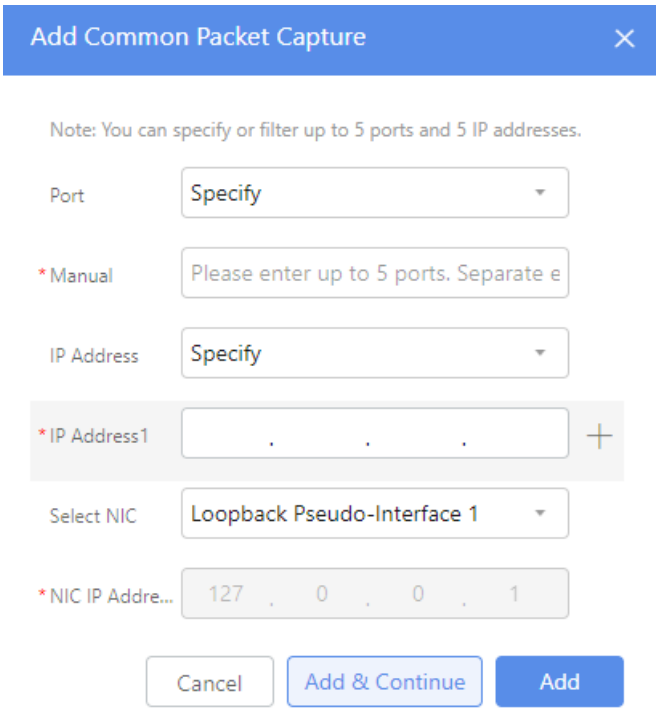
Common Packet Capture

Perform packet capture as tasks, with a maximum of 5 capture tasks allowed, each capturing one packet. Depending on traffic volume, each task retains up to 5 pcap files, with each file limited to 20MB. If exceeding 5 files, the newest pcap file overwrites the oldest one.

Note:

- When capturing packets on a specified NIC, each task retains up to 5 pcap files, with each file limited to 20MB. If exceeding 5 files, the newest pcap file overwrites the oldest one.
- When capturing packets on all NICs, each NIC retains up to 2 pcap files, with each file limited to 20MB. If exceeding 2 files, the newest pcap file overwrites the oldest one.

1. Click **Add Task** to set capture conditions: IP address/port of the network device, and the server's NIC.



Device	Parameter	Description
Peer Network Device	Port	Port numbers of network devices interacting with this server. • All: Capture all port numbers. • Specify: Capture only specified port numbers (up to 5 ports, separated by commas). • Filter: Exclude specified port numbers (up to 5 ports, separated by commas).
	IP Address	IP addresses of network devices interacting with this server. • All: Capture all IP addresses. • Specify: Capture only specified IP addresses (up to 5 IPs). • Filter: Exclude specified IP addresses (up to 5 IPs).
This Server	Select NIC	• All NICs: Capture interaction packets between all server NICs and specified network devices. • Specified NIC: Capture interaction packets between a specified server NIC and specified network devices.

2. Click **Add** to create a task and exit; click **Add and Continue** to save the current task and create next one.

   Note:
   Task name format: Task ID_NIC Name_IP Type_Port Type.

3. The new capture task is in waiting status; click to start capture, and the status changes to "Ongoing".

4. Click to stop capture, and the status changes to "Packaging" and then "Completed".

   Note:
   If no packets are captured, the task status shows "Failed" after stopping. You can click in the upper-right corner to view the reason for the failure.

5. After the task is completed, click to download the capture file to your local computer.

Other Operations

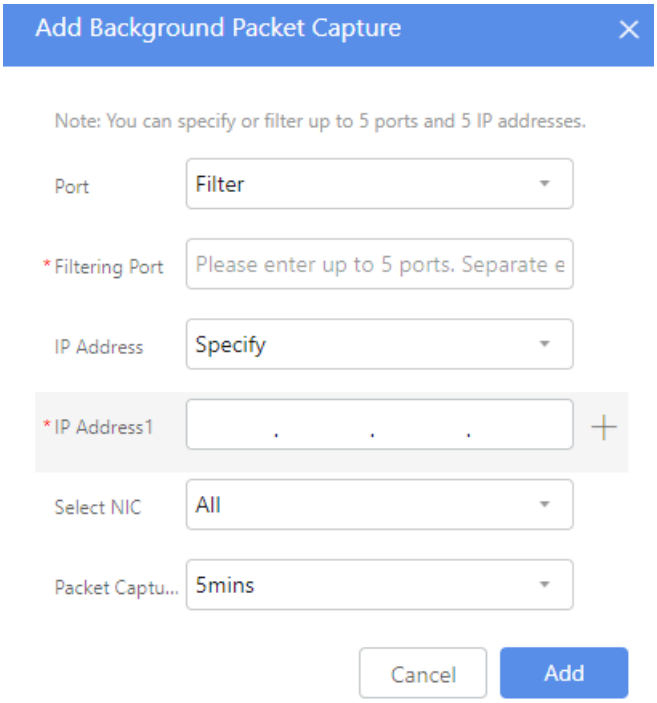
- View task parameters: Click to view capture parameters (same as the Add page).
- Delete task: Click to delete a task. (**Attention:** This will also delete all capture files of this task).

- Batch operations: Select tasks, then click the buttons above the task list to perform batch "Start Capture/Stop Capture/Download/Delete".

Background Packet Capture

Perform packet capture as tasks, with a maximum of 1 capture task allowed. Depending on traffic volume, the capture results may contain multiple pcap files. Each pcap file has a maximum size of 200MB.

1. Click **Add Task** to configure capture conditions: Background packet capture requires setting capture duration, other parameters are the same as Common Packet Capture.



2. The new capture task is in "Waiting" status; click to start capture, and the status changes to "Ongoing".
3. For unfinished capture, you can click to stop capture manually; after reaching the duration, the capture stops automatically; the status changes to "Packaging" and then "Completed".

   Note:
   During capture, if **the disk space runs low or the service restarts, the task will stop and package file automatically**.
   If no packets are captured, the task status shows "Failed" after stopping. You can click in the upper-right corner to view the reason for the failure.

4. After the task is completed, click to download the capture file to your local computer. If the packaging is interrupted, you need to log in to the server backend and go to the file path indicated on the screen to view the capture files.

Other Operations

- View task parameters: Click to view capture parameters (same as the Add page).
- Delete task: Click to delete a task. (**Attention:** This will also delete all capture files of this task).

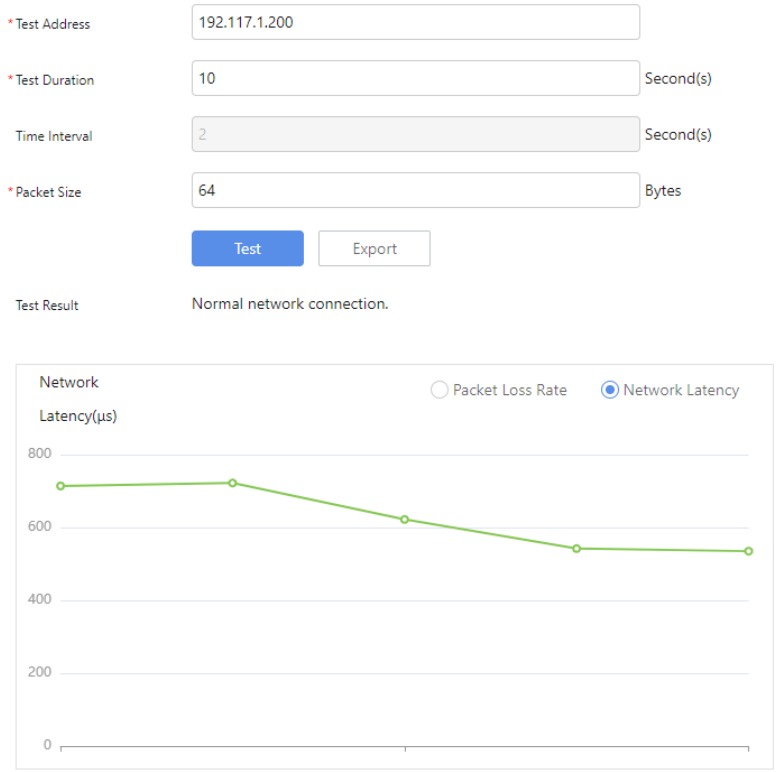
30.4.4 Network Test

Test network connectivity between the platform and other devices by sending data packets to a specified address. The test evaluates network latency and packet loss rate based on the responses received.

1. Set the test parameters.
   - Test Address: The domain name or IP address of the target device.
   - Test Duration: The duration for which the platform pings the target address. The test stops after this duration.

- Time Interval: The interval at which ping results are obtained. The interval is calculated automatically by the system based on the set test duration.
- Packet Size: The size of the data packets to be sent. Larger packets can simulate high-load conditions to test network latency and packet loss, while smaller packets are suitable for quick connectivity tests.

2. Click **Test** to start the test. Once completed, you can view the dynamic changes in packet loss rate and network latency in the chart.



3. Click **Export** to export the current test records to a table. The number of records equals to the floor value of the test duration divided by the time interval.

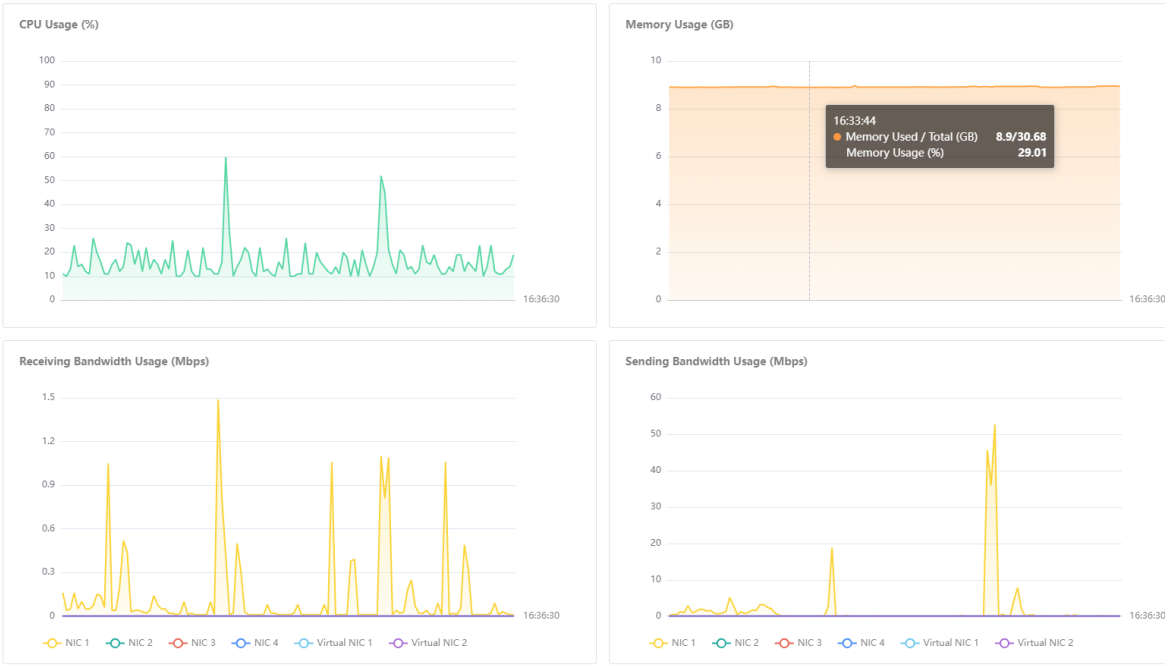
30.5 Information Statistics

Go to **Operations&Maintenance > Information Statistics**.

Collect statistics on server performance, device status, storage capacity, recording status, etc.

30.5.1 Server Performance

Collect statistics on server CPU usage, memory usage, and receiving/sending bandwidth information.



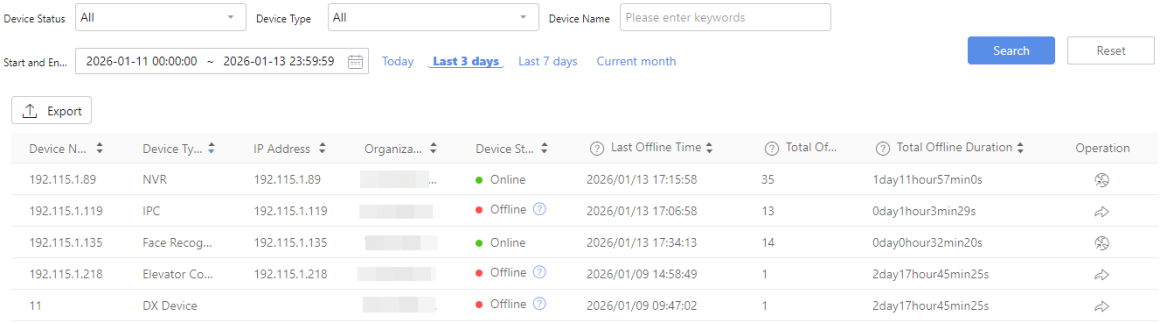
Statistics automatically begin when the page is opened. The statistics are based on the current PC time, displaying up to 240 seconds of statistical results. Closing the page will clear the statistical data.

Hover over the chart to view statistical information for a specific moment.

If multiple network interface cards (NICs) are configured, the statistics for each NIC will be displayed as trend lines in different colors. Click the NIC names below the horizontal axis to choose whether to include specific NICs in the bandwidth statistics.

30.5.2 Device Status

Provides statistics on the online/offline status and online/offline duration of devices connected to the system.



- Search device status: Choose device status (online/offline), device (IPC/NVR/Smart Box/ EIA/Radar/Radar vision/Indoor station/Outdoor station/Face recognition terminal/General access control device/Access control/Speed gate & Turnstile/Elevator controller/LPC/LPR/DX Device), start and end time (up to 31 days), and then click **Search**.
  Search results include the current online status, last offline time, total offline count and duration within the specified time period.

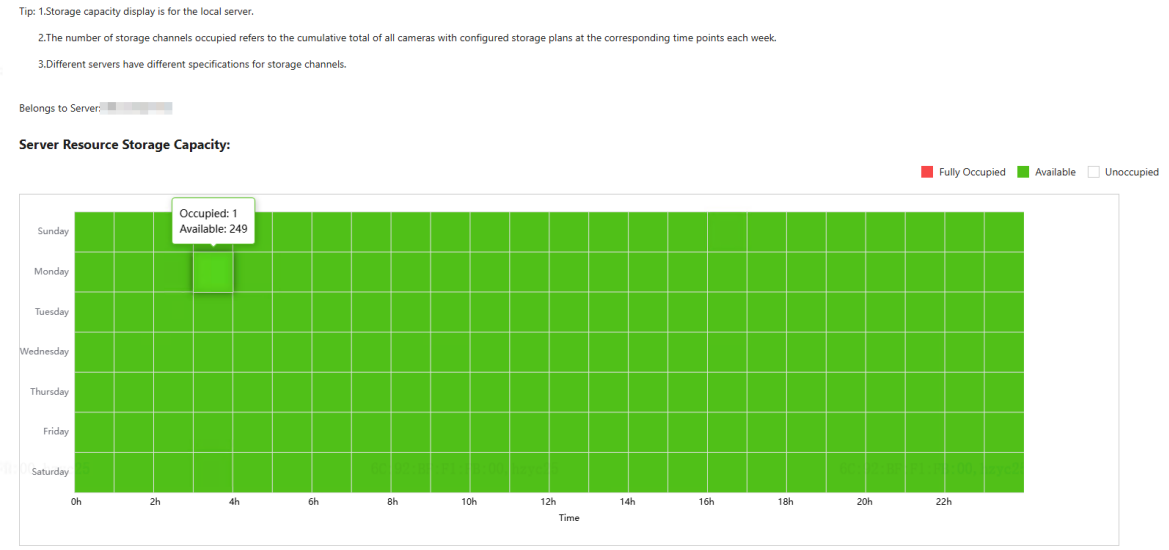
  Note:
  Last offline time: The actual time when the device went offline, regardless of the specified time period. If the device has never been online or has been continuously online, the time when the device was added is displayed.

- Hover over ⓘ next to the offline device to view the reason for its offline.
- Click next to the offline device to open the Device Management interface, you can check whether the device addition parameters are correct.

- Click next to the online device to open the device's Web interface, you can configure the device's own parameters.

30.5.3 Storage Capacity

View statistics on server storage capacity to prevent server overload and potential malfunctions when the number of storage channels is excessively high.

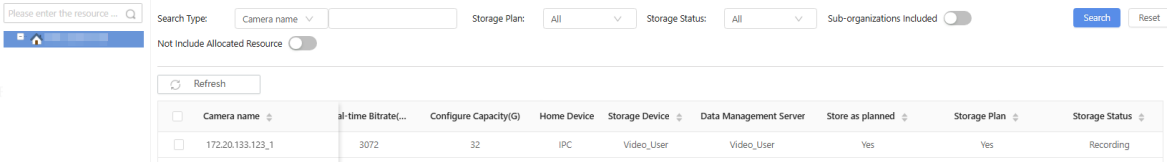


In the chart, the vertical axis represents the days of the week (Sunday to Saturday), and the horizontal axis represents the time of day (0:00 to 24:00, divided into 24 segments).

- Different servers have varying specifications for the number of storage channels. Hover the mouse over the chart to view the occupied and available storage capacity for the corresponding time period.
- Three colors indicate three different statuses:
  - Red: Indicates no available storage capacity during the corresponding time period. It is not recommended to configure recording schedules at this time.
  - Green: Indicates available storage capacity during the corresponding time period. Recording schedules can be configured.
  - White: Indicates no storage capacity is being used during the corresponding time period. Recording schedules can be configured.

30.5.4 Recording Status

View statistics on the storage information of cameras under the server.



- Search criteria: Supports querying storage information by camera name, storage plan, storage status, etc.
- List: Displays information such as real-time storage bitrate, configured storage capacity, and storage status for each camera.

30.6 Video Diagnosis

Note:
A valid license is required to enable this feature.

Diagnose the quality of camera videos. The results are displayed in visual charts for easy understanding of the video service status.

Diagnosis items include offline, image capture, video loss, high/low brightness, color, contrast, screen frozen, image blurry, noise interference, reinforced cross-gain, scrolling, video masking, scene change, black and white image, drastic changes in a video, video jitter, real-time usage time, packet loss rate, PTZ control.

30.6.1 Diagnosis Configuration

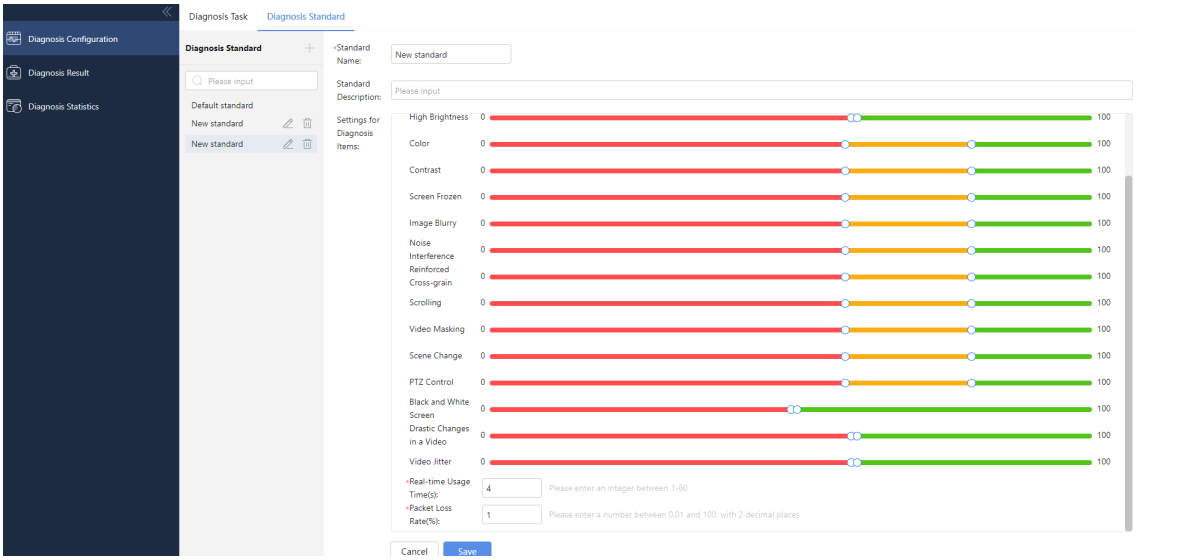
Configure diagnosis standards and create diagnosis tasks.

30.6.1.1 Diagnosis Standard

You can customize different diagnosis standards based on the actual needs for flexibility and convenience. For example, different standards for indoor and outdoor, day and night, sunny and rainy conditions, etc.

Add Standard

1. Click +.



Standard Name Standard Description	Custom input.
Settings for diagnosis Items	Set the threshold for **abnormal**, **warning**, and **normal**. Hover the mouse over the white block on the ratio bar to display the ratio value and drag left/right to adjust the value. Higher values for abnormal and warning settings indicate stricter standards.
Real-time Usage Time	Set the live view retrieval time. An alarm is reported if the value is exceeded. Enter an integer in the range of 1-60.
Packet Loss Rate	Set the packet loss rate, which is the loss ratio of the camera video stream. An alarm is reported if the value is exceeded. Enter a number in the range of 0.01-100, with up to 2 decimal places.

2. Click **Save**.

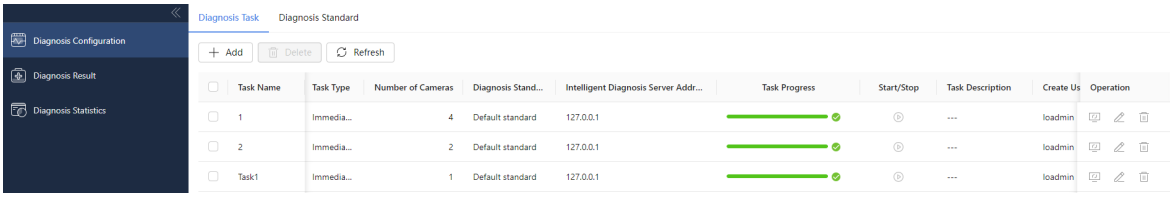
Other Operations

- View/Edit: Select a standard in the left-side list to display its details on the right. Click **Edit** to modify diagnosis standard parameters. Click **Save** to save the settings.
- Delete: Select a standard in the left-side list and click .

Note:
The default standard cannot be edited or deleted.

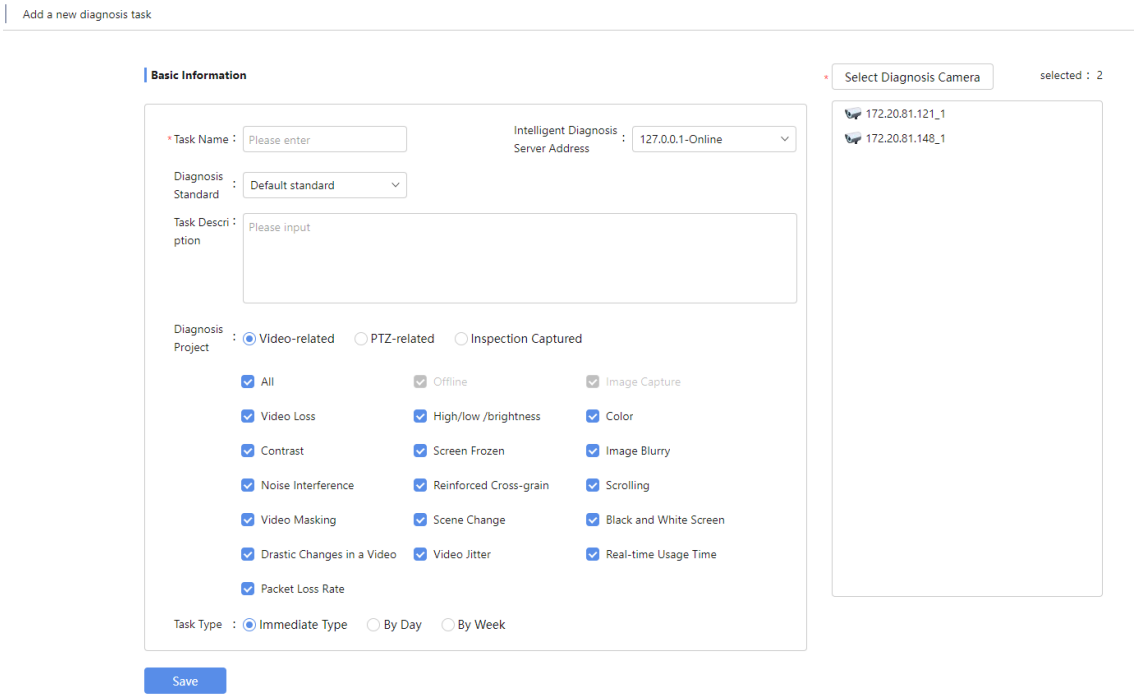
30.6.1.2 Diagnosis Task

Create video diagnosis tasks for cameras.



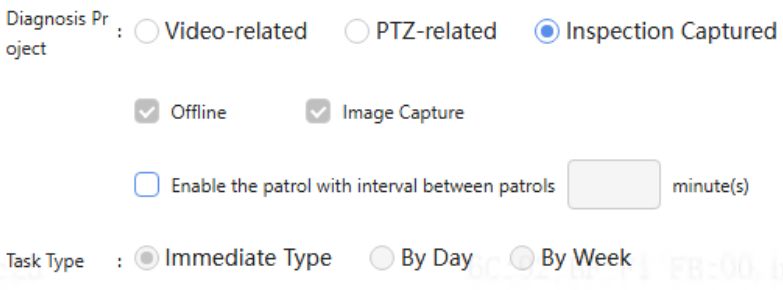
Add Task

1. Click **Add**.
2. Enter the task name and description, and then select a diagnosis standard.



3. Diagnosis items including video-related, PTZ-related and inspection captured. Select diagnosis item(s) as needed by referring to the following table.

Diagnosis Item	Description
Offline	Detects the camera's online status on the video management platform, possibly due to power outage or network disconnection.
Image Capture	Detects anomalies where the camera fails to capture images, possibly due to power outages network disconnection, camera obstruction, or excessively live view retrieval time.
Video Loss	Detects intermittent or persistent video loss, possibly due to camera malfunction, poor contact of video transmission cable, lens detachment, malicious tempering, or video transmission failure.
High/Low Brightness	Detects images with excessively high/low contrast, possibly due to camera settings, lens aging, or environmental factors.
Color	Detects discoloration in the video image, possibly due to external interference or camera malfunctions.
Contrast	Detects image with excessively high or low contrast, possibly due to camera settings, lens aging, or environmental factors.
Screen Frozen	Detects image freezing, possibly due to video transmission or camera malfunctions.
Image Blurry	Detects blurry images, possibly due to camera lens damage or improper focus.
Noise Interference	Detects noise or snow-like interference on the video image, possibly due to line aging, transmission fault, poor contact, or electromagnetic interference.

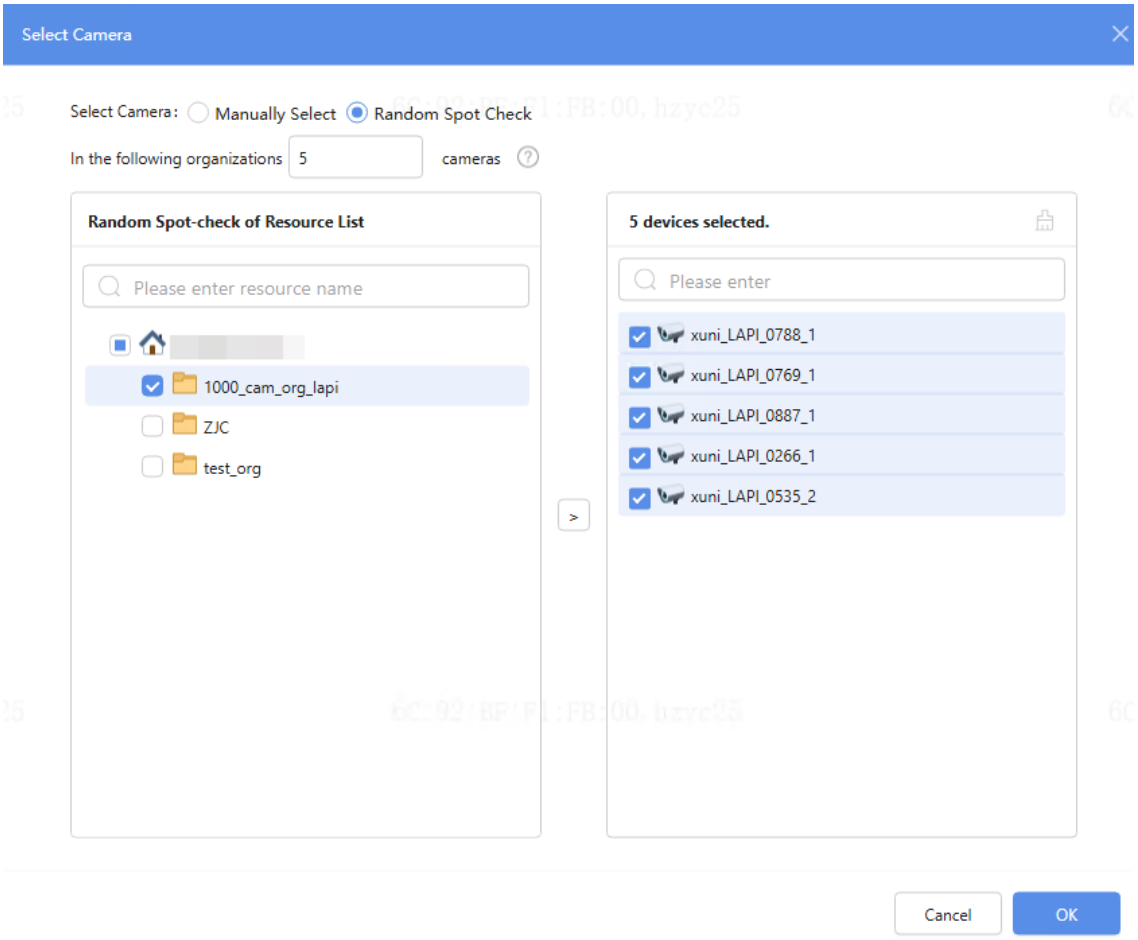
Diagnosis Item	Description
Reinforced Cross-gain	Detects prominent horizontal stripe interference on the video image, possibly due to line aging, transmission fault, poor contact, or electromagnetic interference.
Scrolling	Detects rolling of the video image, possibly due to line aging, transmission fault, poor contact, or electromagnetic interference.
Video Masking	Detects partial or complete occlusion of the camera lens, possibly due to deliberate obstruction.
Scene Change	Detects changes in the scene, such as object moving/moving out or partial human interference, possibly due to deliberate object movement.
Black and White Image	Detects absence of color in the video image, possibly due to infrared mode or color rendering failure.
Drastic Changes in a Video	Detects significant changes in the image over a period, possibly due to continuous PTZ movement, line aging, transmission fault, or electromagnetic interference.
Video Jitter	Detects abnormal video jitter, possibly due to unstable installation or significant ground vibrations. Suitable for high-attitude or elevated camera installations.
Real-time Usage Time	Detects the time the camera retrieves live video. An alarm is reported if the set value is exceeded.
Packet Loss Rate	Detects the size of video packet loss. If the loss ratio exceeds the set value or there is no video stream, an alarm is reported.
PTZ Control	Detects abnormalities in PTZ control.
Inspection Captured	Offline detection and image capture detection are enabled by default (see previous description). • If **Patrol** is enabled and a patrol interval (5–360 minutes) is configured, inspections will be performed at the specified interval. • If **Patrol** is not enabled, the task defaults to an immediate type, executed only once. 

4. Select a task type.

Item	Description
Immediate Type	Executes immediately after task creation and complete at once.
By Day	Executes every day. You need the set the task start and end time. Default is 00:00:00-23:59:59 everyday.
By Week	Executes every week with specified time periods. You need to configure each day from Monday to Sunday separately, with up to 4 different time periods per day. **Note:** When finished the settings for a day, you can sync the settings for other days by selecting the corresponding day and clicking **Copy**.

5. Click **Select Diagnosis Camera**, select camera(s) to be diagnosed from the organization tree.

Note:
For random sampling, enter the number of cameras to be sampled in the **Random Spot Check** column and select organizations, and then the system will automatically select the corresponding number of cameras for diagnosis. If the set value exceeds the existing cameras under the camera, all cameras under the organization will be diagnosed.



6. Click **Save**.

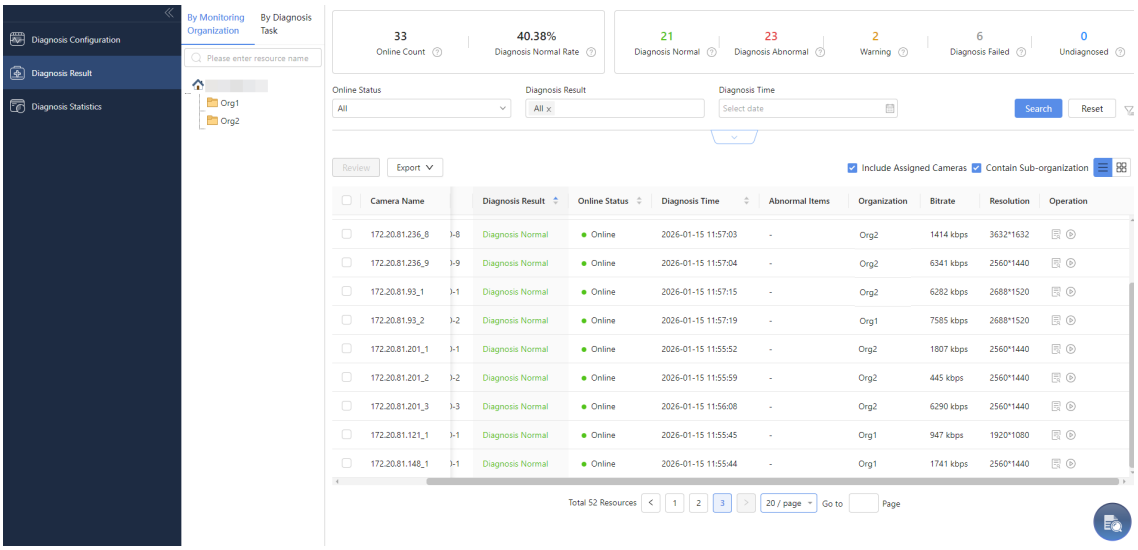
Other Operations

- Start/Pause task: Click ▷ / || to start/pause the task.
- Re-diagnose: Click for the task to restart the diagnosis task, the task progress will reset to 0.
- View/edit task configuration: Click for the task to view or edit task details.
- Delete: Click for the task or select task(s) and click **Delete**.
- Refresh task: Click **Refresh** to refresh the task.

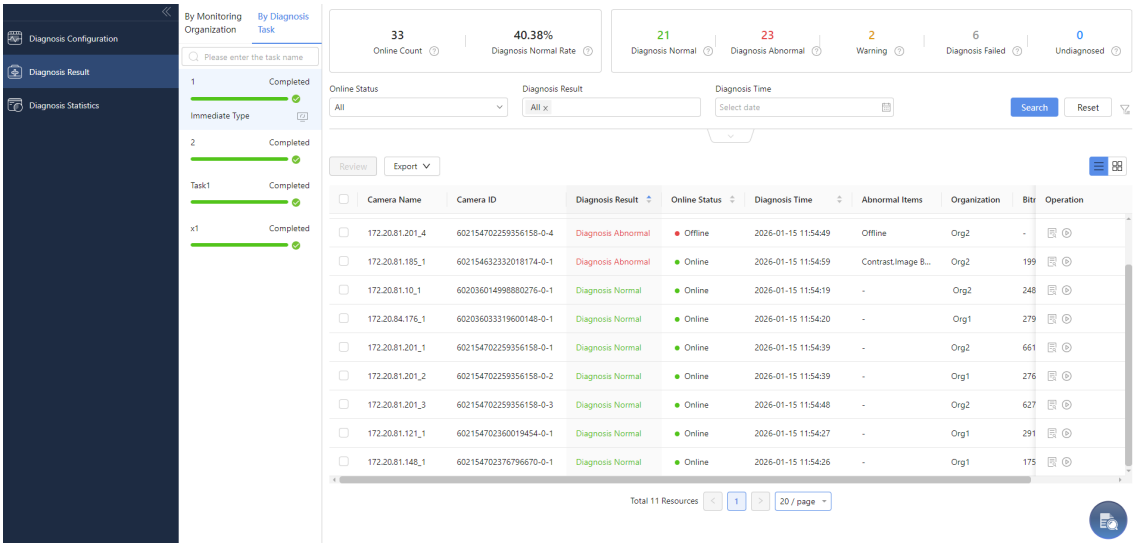
30.6.2 Diagnosis Result

Search diagnosis results by organization or diagnosis task, view details and export results.

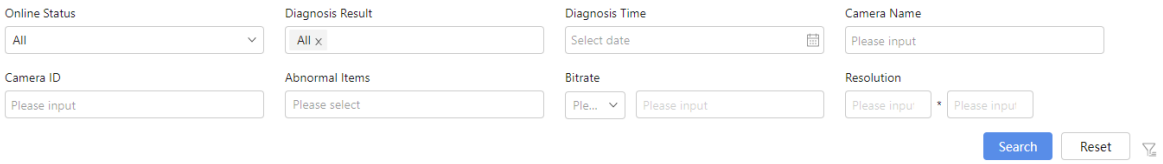
- Search by Monitoring Organization: On the **By Monitoring Organization** tab, select an organization in the left-side list, and set search criteria on the right-side. Click **Search**, and the video diagnosis results under the organization are displayed.



- Search by Diagnosis Task: On the **By Diagnosis Task** tab, select a task in the left-side list, and set search criteria on the right-side. Click **Search**, and the video diagnosis results under the task are displayed.



Search Criteria Description

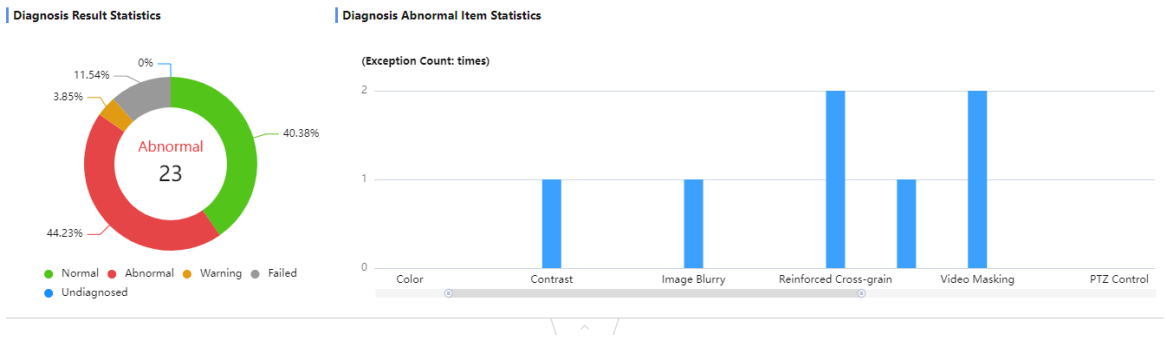


- Online Status: Including online, offline, and all.
- Diagnosis Result: Perform statistics based on the camera diagnosis results, including all, normal, abnormal, warning, failed, undiagnosed. You can select one or more items.
- Diagnosis Time: Perform statistics based on the camera diagnosis time.
- Camera Name: Search by keywords.
- Camera ID: Search by keywords.
- Abnormal items: Search by offline, video loss, low brightness, high brightness, color, contrast, screen frozen, image blurry, noise interference, reinforced cross-grain, scrolling, video masking, scene change, black and white screen, drastic changes in a video, video jitter, PTZ control, real-time usage time, image capture, and packet loss rate. You can select one or more items.
- Bitrate: Perform statistics based on the camera bitrate; operators include: =, >, <, ≥, ≤, and between; an integer must be entered.
- Resolution: Perform statistics based on the camera resolution.

- Filter by Organization: Perform statistics on cameras under the selected organization; supported only when searching by diagnosis task.

Statistical Chart

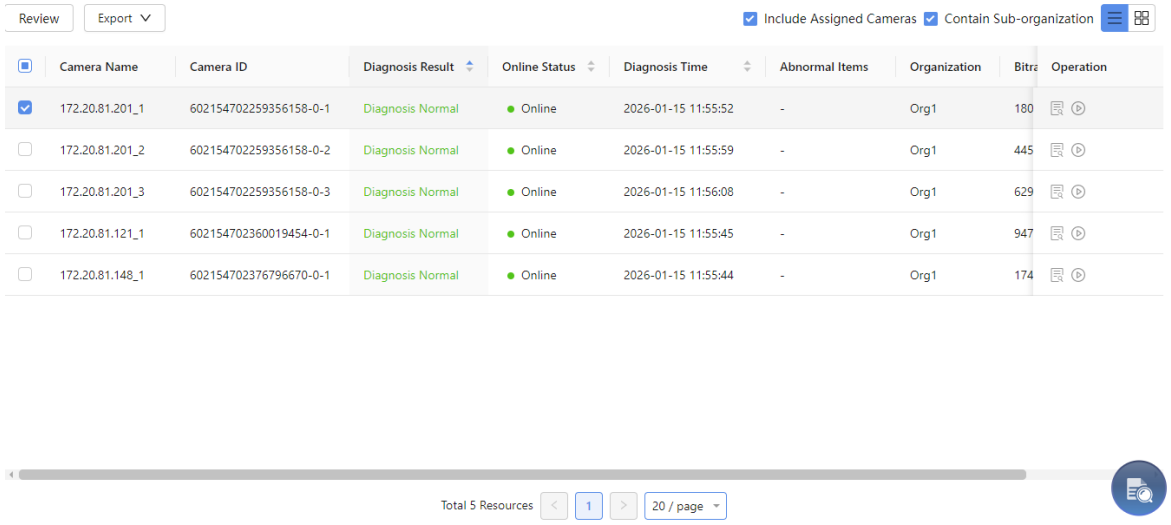
Click above the list to expand the statistical chart; click again to collapse it.



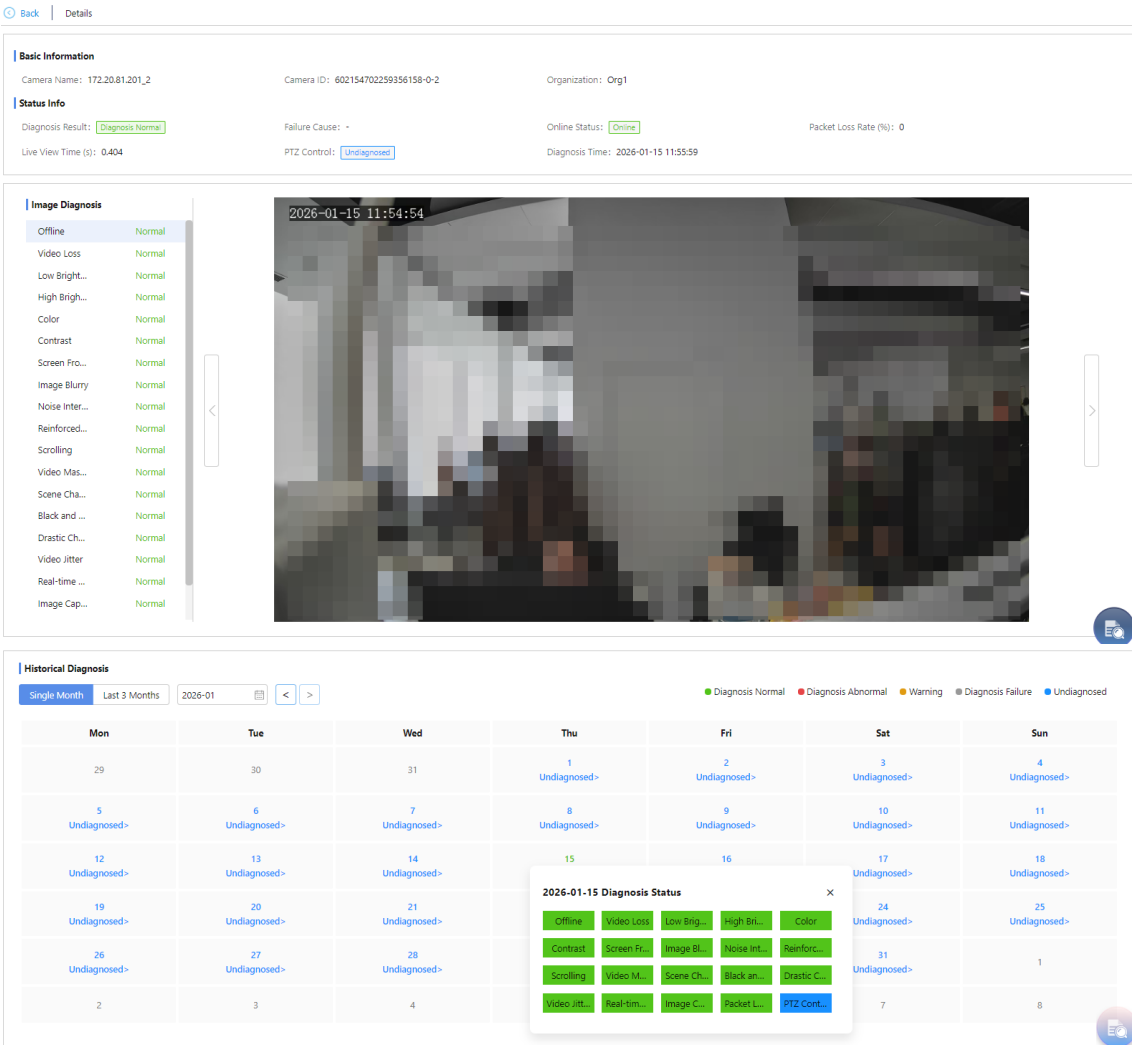
- Diagnosis result statistical chart: Displays the number of cameras for each evaluation and their percentage of all cameras.
- Diagnosis abnormal item statistical chart: Displays the occurrences of video anomalies under the search criteria. You can adjust the displayed anomalies by dragging the horizontal slider.

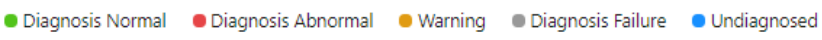
Detailed Data

Detailed data includes camera name, camera ID, diagnosis results, online status, diagnosis time, abnormal items, organization, bitrate, and resolution.



- Click to switch the data list to card view.
- Review: Select cameras and click **Review** to create a review task for re-diagnosing the cameras. Click in the lower-right corner of the page to check task progress. After diagnosis is complete, information such as diagnosis result and diagnosis time will be updated.
- Export: Select cameras and click **Export**, then choose **Export Selected** or **Export All** to download the diagnosis results to your local computer for viewing.
- Include Assigned Camemras: Select **Include Assigned Cameras** to display video diagnostic information of devices assigned to the organization.
- Contain Sub-organization: Select **Contain Sub-organization** to display video diagnostic information of devices under subordinate organizations.
- Play live video: Click in the operation column to view the camera's live video.
- View details: Click in the operation column to view the camera's diagnosis details.

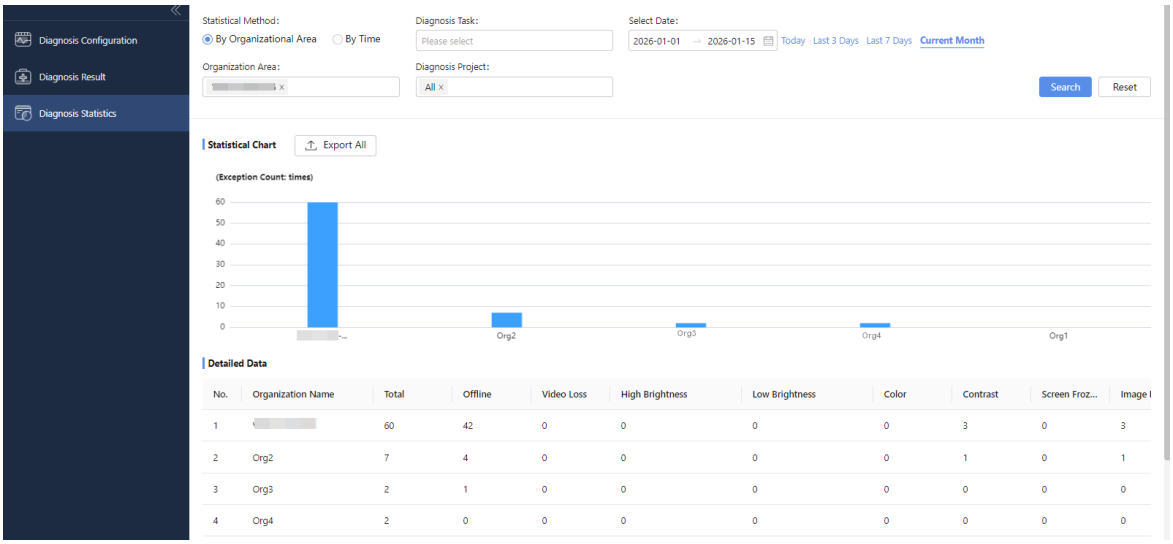


Basic Information	Displays camera name, camera ID, organization.
Status Information	Displays diagnosis result, failure cause, online status, packet loss Rate, live view time, PTZ control, diagnosis time
Image Diagnosis	The left-side list displays the results of image diagnosis items, and the right side shows the snapshots.
Historical Diagnosis	• You can filter by single month, last 3 months, or custom time range. • Diagnosis results are distinguished by color.  • Click on a date with abnormal diagnosis to view the specific reason for the anomaly. **Note:** Details cannot be viewed for dates that have not been diagnosed.

30.6.3 Diagnosis Statistics

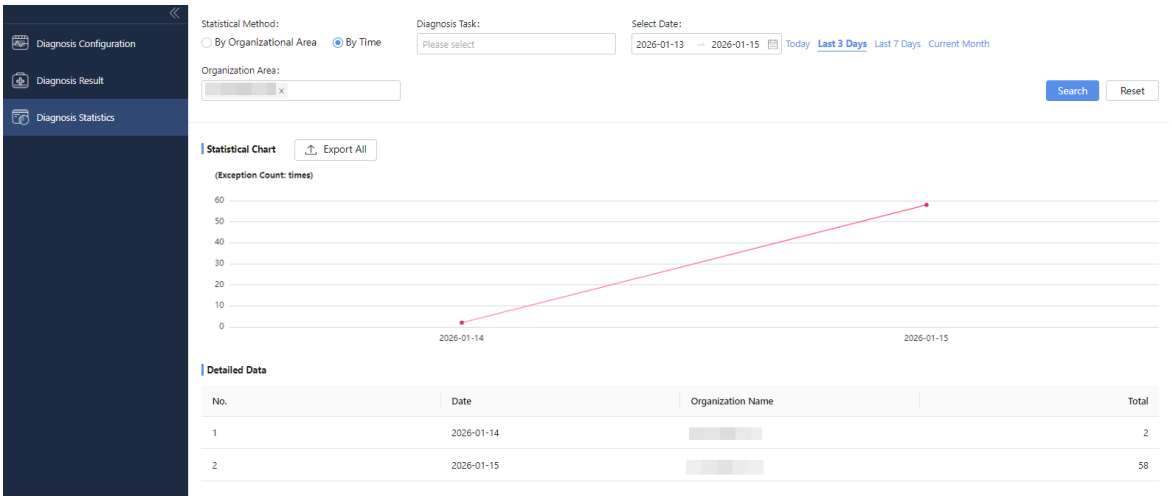
Perform statistics and analyze video diagnosis results. The results can be displayed in statistics chart or data list.

By Organization Area



- Search criteria: Diagnostic task, custom time period, organization area, and diagnostic item.
- Statistical chart: Displays the exception count under each organization in a chart.
- Detailed data: Displays the exception count under each organization is a list. Click **Export All** to export the retrieved results locally.

By Time



- Search criteria: Diagnostic task, custom time period, and organization area.
- Statistical chart: Displays the exception trend in a chart.
- Detailed data: Displays the exception count at each time point in a list. Click **Export All** to export the retrieved results locally.