

iVMS-4200 V3.14.2

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Summary of Changes 1
1.3 Symbol Conventions 3
Chapter 2 Service Management 4
Chapter 3 Device Management 5
3.1 Activate Devices 5
3.2 Add Device 6
3.2.1 Add Single or Multiple Online Devices 6
3.2.2 Add Device by IP Address or Domain Name 8
3.2.3 Add Devices by IP Segment 11
3.2.4 Add a Device via OTAP 12
3.2.5 Add Device by Hik-Connect 14
3.2.6 Import Devices in a Batch 15
3.3 Restore/Reset Device Password 17
3.3.1 Reset Device Password 17
3.3.2 Restore Device's Default Password 18
3.4 Upgrade Device Firmware Version 19
3.5 Manage Added Devices 21
3.6 Group Management 22
3.6.1 Group Resources 22
3.6.2 Edit Resource Parameters 24
3.7 Safety and Service 25
Chapter 4 Hik-Connect 28
4.1 Register a Hik-Connect Account 28
4.2 Log into Hik-Connect Account 30

Chapter 5 Live View 32
5.1 Live View Toolbar 32
5.2 Add Custom View 33
5.3 Start Live View 34
5.4 Auto-Switch in Live View 36
5.4.1 Auto-Switch Cameras in a Group 37
5.4.2 Auto-Switch All Cameras 38
5.4.3 Auto-Switch Cameras or Custom Views by Schedule 39
5.5 PTZ Control 40
5.5.1 PTZ Control Panel 40
5.5.2 Set Preset, Patrol, and Pattern 43
5.6 Sensor Control 44
5.7 Customize Window Division 44
5.8 Manually Record and Capture 45
5.8.1 Manually Record Video 45
5.8.2 View Local Videos 46
5.8.3 Capture Pictures 46
5.8.4 View Captured Pictures 47
5.9 Instant Playback 48
5.10 Live View for Fisheye Camera 48
5.10.1 Perform Live View in Fisheye Mode 48
5.10.2 PTZ Control in Fisheye Mode 50
5.10.3 Set a Preset and Patrol 50
5.11 Perform Smart Linkage 51
5.11.1 Configure Smart Linkage Rule 51
5.11.2 Enable Smart Linkage 53
5.12 Live View for Thermal Camera 53
5.12.1 View Fire Source Information during Live View 53

5.12.2 Show Temperature Information on Live View Image 55
5.12.3 Manually Measure Temperature 56
5.12.4 Display Fire Source Detection Shield Area 57
5.12.5 Display Waste Gas Information 57
5.13 Live View in Low Bandwidth 58
5.14 More Functions 58
Chapter 6 Remote Playback 61
6.1 Flow Chart 61
6.2 Remote Storage Configuration 62
6.2.1 Store Picture and Video on DVR, NVR, or Network Camera 62
6.2.2 Store Picture and Additional Information on Local PC 64
6.2.3 Configure Recording Schedule Template 64
6.2.4 Configure Capture Schedule Template 65
6.3 Toolbar for Playback 66
6.4 Normal Playback 68
6.4.1 Search Video Footage 69
6.4.2 Play Video Footage 70
6.5 Alarm Input Playback 72
6.6 Event Playback 72
6.7 ATM Playback 72
6.8 POS Playback 73
6.9 VCA Playback 73
6.10 Synchronous Playback 74
6.11 Fisheye Camera's Video Playback 75
6.12 Playback in Low Bandwidth 77
6.13 Search Targets by Picture 77
6.14 Download Video Footage 77
6.14.1 Download Video Footage by Date 78

6.14.2 Download for Multiple Cameras 78
Chapter 7 Event Configuration 80
7.1 Configure Event for Camera 80
7.2 Configure Event for Alarm Input 83
7.3 Configure Event for Encoding Device 85
Chapter 8 Event Center 88
8.1 Enable Receiving Event from Devices 88
8.2 View Real-Time Events 89
8.3 Search Historical Events 92
8.4 Get Events from Device 95
8.5 View Pop-up Event Information 96
Chapter 9 Map Management 98
9.1 Add Map 98
9.2 Edit Map Scale 99
9.3 Longitude and Latitude Calibration 100
9.4 Manage Hot Spot 100
9.4.1 Add Camera as Hot Spot 100
9.4.2 Add Alarm Input as Hot Spot 102
9.4.3 Add Alarm Output as Hot Spot 103
9.4.4 Add Zone as Hot Spot 105
9.4.5 Add Access Point as Hot Spot 107
9.4.6 Configure Security Radar Hot Spot 109
9.4.7 Edit Hot Spot 142
9.4.8 Preview Hot Spot 143
9.5 Manage Hot Region 146
9.5.1 Add Hot Region 146
9.5.2 Edit Hot Region 147
9.5.3 Preview Hot Region 147

9.6 View Person's Moving Pattern 148
Chapter 10 Statistics 150
10.1 People Counting Report 150
10.1.1 People Counting Report by Encoding Device 150
10.1.2 View People Counting Report by DeepinMind Server 154
10.2 View People Counting in Intersections Report 155
10.3 Queue Management 157
10.3.1 Queuing-Up Time Analysis 157
10.3.2 Queue Status Analysis 161
10.4 Heat Map 165
10.5 Skin-Surface Temperature Statistics 167
10.6 Real-Time Density and People Counting 168
10.7 Temperature Map 170
Chapter 11 Data Retrieval 172
11.1 Video Search 172
11.2 Target Retrieval 173
11.2.1 Face Picture Retrieval 173
11.2.2 Human Body Retrieval 183
11.2.3 Vehicle Retrieval 186
11.2.4 Search Target Pictures by Picture 188
11.3 Abnormal Event Detection 188
11.4 Hard Hat Retrieval 190
11.5 People Frequency Search 191
11.5.1 Search Frequently Appeared Person 191
11.5.2 Search Rarely Appeared Person 192
11.6 AI Dashboard Retrieval 194
11.6.1 Search Analysis Result for Video and Captured Picture Task 194
11.6.2 Search Analysis Result for Imported Picture Task 195

11.7 Facial Recognition Check-in 196
11.7.1 Search Facial Recognition Check-in Records 196
11.7.2 Search Facial Recognition Attendance Records 197
11.8 Community Inspection 200
11.8.1 Detect Fire Engine Access 200
11.8.2 Detect Elevator 201
11.8.3 Retrieve Urban Management Event 202
Chapter 12 AcuSeek 204
Chapter 13 AI Dashboard 208
13.1 Face Application 208
13.1.1 Set List Types for Face Picture Libraries 208
13.1.2 Set Cameras for Showing AI Information 209
13.1.3 Show AI Information 209
13.2 Multi-Target-Type Detection 210
13.2.1 Set Target Detection Parameters 211
13.2.2 Display Multi-Target-Type Detection 214
13.3 AI Open Platform 215
13.3.1 Configure Platform Parameters 216
13.3.2 Configure Platform Event 218
13.3.3 Analyze Picture Task 219
13.3.4 AI Platform Real-Time Display 221
13.4 Multidimensional People Counting 222
13.4.1 Configure People Counting Group 223
13.4.2 Display People Counting Data by Group 223
13.5 Linked Capture Alarm 224
13.5.1 Set Basic Parameters 224
13.5.2 View Live View and Alarms 225
13.6 Traffic Accident Alarm 226

13.6.1 Configure Display Parameter 226
13.6.2 View Traffic Accident Alarm 228
13.7 Arming and Tracking 229
13.7.1 Vehicle Arming and Control 229
13.7.2 Face/Human Body Arming and Control 230
13.8 Skin-Surface Temperature 232
13.8.1 Start Live View of Skin-Surface Temperature Detection 232
13.8.2 Display Skin-Surface Temperature Information 233
13.8.3 View Alarm Information 237
13.9 Abnormal Event Detection 238
13.10 Event Dashboard 240
Chapter 14 Video Tracing 243
14.1 Configuration 243
14.2 Retrieve Scanning Records 245
Chapter 15 Security Control Panel 248
15.1 Flow Chart 248
15.2 Configure Security Control Panel Remotely 249
15.3 Configure Client Linkage for Zone Event 249
15.4 Remotely Control Security Control Panel 251
15.4.1 Remotely Control Partitions 251
15.4.2 Remotely Control Zones 252
15.4.3 Remotely Control Relay 254
15.4.4 Remotely Control Siren 254
Chapter 16 Person Management 255
16.1 Add Organization 255
16.2 Add Persons 255
16.2.1 Configure Basic Information 256
16.2.2 Upload a Face Photo from Local PC 258

16.2.3 Add Credentials 259
16.2.4 Configure Access Control Information 270
16.2.5 Customize Person Information 272
16.2.6 Configure Resident Information 273
16.2.7 Configure Additional Information 273
16.3 After Adding Persons: Operations on the Person List 274
16.3.1 Report Card Loss 274
16.3.2 Batch Edit Persons' Validity Period 274
16.3.3 Move Persons to Another Organization 274
16.3.4 Import and Export Person Identify Information 275
16.3.5 Get Person Information from Access Control Device 279
16.3.6 Batch Issue Cards to Persons 280
16.3.7 Customize Column Display 280
16.3.8 View Resource Statistics 280
Chapter 17 Access Control 282
17.1 Flow Chart 282
17.2 Configure Schedule and Template 283
17.2.1 Add Holiday 284
17.2.2 Add Schedule Template 285
17.3 Assign Access Levels to Persons in Access Groups 286
17.4 Search Access Group 288
17.5 Configure Advanced Functions 289
17.5.1 Configure Access Control Parameters 289
17.5.2 Configure Remaining Unlocked/Locked 297
17.5.3 Configure Multi-Factor Authentication 299
17.5.4 Configure Custom Wiegand Rule 301
17.5.5 Configure Card Reader Authentication Mode and Schedule 303
17.5.6 Configure Person Authentication Mode 304

17.5.7 Configure Relay for Elevator Controller 305
17.5.8 Configure First Person In 309
17.5.9 Configure Anti-Passback 310
17.5.10 Configure Cross-Controller Anti-Passback 311
17.5.11 Configure Multi-door Interlocking 315
17.5.12 Configure Cross-Controller Multi-door Interlocking 316
17.5.13 Configure Authentication Code 316
17.6 Configure Other Parameters 317
17.6.1 Set Multiple NIC Parameters 317
17.6.2 Set Device Capture Parameters 318
17.6.3 Set Parameters for Face Recognition Terminal 319
17.6.4 Enable M1 Card Encryption 320
17.6.5 Set RS-485 Parameters 321
17.6.6 Set Wiegand Parameters 321
17.7 Configure Linkage Actions for Access Control 322
17.7.1 Configure Client Actions for Access Event 322
17.7.2 Configure Device Actions for Access Event 324
17.7.3 Configure Device Actions for Card Swiping 325
17.7.4 Configure Device Actions for Person ID 327
17.8 Door/Elevator Control 328
17.8.1 Control Door Status 328
17.8.2 Control Elevator Status 330
17.8.3 Check Real-Time Access Records 331
17.9 Distributed Controller Management 333
Chapter 18 Time and Attendance 334
18.1 Flow Chart 334
18.2 Configure Attendance Parameters 335
18.2.1 Set Weekend 335

18.2.2 Configure Authentication Mode 336
18.2.3 Configure Overtime Parameters 336
18.2.4 Configure Attendance Check Point 337
18.2.5 Configure Holiday 338
18.2.6 Configure Leave Type 339
18.2.7 Synchronize Authentication Record to Third-Party Database 340
18.2.8 Configure Attendance Calculation Accuracy 340
18.2.9 Configure Break Time 341
18.3 Add Flexible Timetable 342
18.4 Add General Timetable 344
18.5 Add Shift 347
18.6 Manage Shift Schedule 350
18.6.1 Set Department Schedule 350
18.6.2 Set Person Schedule 351
18.6.3 Set Temporary Schedule 352
18.6.4 Check Shift Schedule 353
18.7 Attendance Handling 354
18.7.1 Manually Correct Check-in/out Record 354
18.7.2 Add Leave and Business Trip 355
18.8 Calculate Attendance Data 356
18.8.1 Automatically Calculate Attendance Data 356
18.8.2 Manually Calculate Attendance Data 356
18.9 Attendance Statistics 357
18.9.1 Get an Overview of Employees' Attendance Data 357
18.9.2 Custom Export Attendance Records 359
18.9.3 Configure Report Display 359
18.9.4 Generate Instant Report 360
18.9.5 Send Report Regularly 360

Chapter 19 Video Intercom 362
19.1 Flow Chart 362
19.2 Manage Calls between Client Software and an Indoor/Door Station/Access Control Device 363
19.2.1 Call Indoor Station from Client 363
19.2.2 Answer Call via Client 364
19.3 View Real-Time Call Logs 365
19.4 Release a Notice to Resident 366
19.5 Enable Calling between Video Intercom Device and Client 366
19.6 Apply Application Package to Indoor Station 367
Chapter 20 Topology Management 368
20.1 Topology Display Overview 368
20.2 Set Topology Parameters 369
20.3 View Device Details 370
20.4 View Link Details 371
20.5 View Signal Transmission Path 373
20.6 Export Topology 374
20.7 More Functions 374
Chapter 21 Broadcast Management 375
21.1 Control Speaker Units 375
21.2 Manage Material Library 379
21.3 Configure Live Broadcast 379
21.4 Add a Scheduled Broadcast Task 380
Chapter 22 Log Search 382
Chapter 23 User Management 383
23.1 Add User 383
23.2 Change User's Password 384
Chapter 24 System Configuration 385

24.1 Set General Parameters 385
24.2 Set Live View and Playback Parameters 387
24.3 Set Image Parameters 388
24.4 Set Picture Storage 389
24.5 Set Alarm Sound 390
24.6 Set Access Control and Video Intercom Parameters 390
24.7 Set File Saving Path 391
24.8 Set Icons Shown on Toolbar 391
24.9 Set Keyboard and Joystick Shortcuts 392
24.10 Set Email Parameters 393
24.11 Manage Security Authentication 394
24.11.1 Export Certificate from Service Management 394
24.11.2 Import Certificate to Client 394
24.11.3 Certificate Verification for Transmission Encryption 395
Chapter 25 Operation and Maintenance 396
Appendix A. Custom Wiegand Rule Descriptions 398
Appendix B. Troubleshooting 400
B.1 Failed to get the live view of a certain device. 400
B.2 Local recording and remote recording are confused. 400
B.3 Failed to download the video files or the downloading speed is too slow. 400
Appendix C. FAQ (Frequently Asked Questions) 402
C.1 During live view, why an error message with error code 91 prompts ? 402
C.2 During live view, why the image is blurred or not fluent? 402
C.3 Why the memory leaked and the client crashed after running for a while? 402
C.4 How to get better performance of live view and playback when network bandwidth is low? 403
Appendix D. Error Code 405

Chapter 1 Overview

1.1 Introduction

iVMS-4200 Client Software is designed to configure and manage Hikvision devices in a unified and intuitive manner, including DVRs, NVRs, IP cameras, encoders, decoders, security control panels, video intercom devices, access control devices, etc.

The software provides multiple functionalities, including real-time live view, video recording, remote search and playback, file backup, alarm receiving, person management, access control, video intercom, security control, time & attendance, etc.

This user manual describes the functions, configurations and operation steps of the client software. To ensure the properness of usage and stability of the software, refer to the contents below and read the manual carefully before installation and operation.

1.2 Summary of Changes

The followings are the changes of this version.

Remote Playback

Event playback now allows you to jump to any point in the video by dragging the progress bar. See ***Event Playback*** .

Video Tracing

1. When searching recorded video, all channels that support video tracing are selected by default, and the corresponding channel information is displayed in the search results. See ***Video Tracing*** .
2. Adds a **Scanner Test** feature to verify that scanners can correctly read barcodes. See ***Video Tracing*** .
3. When only one channel of a dual-channel camera is stored, the system will automatically remind the user to complete the missing channel to ensure all workstations' recordings are fully accessible. See ***Video Tracing*** .

Person

1. Person information and face pictures can now be imported or exported simultaneously in a single ZIP file. See ***Import Person Information and Face Pictures*** and ***Export Person Information and Face Pictures*** .
2. The import template for person information now allows you to manually add custom columns. After export, the Excel file will also include custom columns. See ***Import Person Information*** , ***Export Person Information*** , ***Import Person Information and Face Pictures*** and ***Export Person Information and Face Pictures*** .

Time & Attendance

1. On the **Attendance Record → Get Events from Device** page, adds a method **Unencrypted File** to import non-encrypted attendance record. See ***Get an Overview of Employees' Attendance Data*** .
2. Optimizes ***regular report*** settings.
   a. Report names can only contain numbers and letters.
   b. Reports can now be sent daily or monthly.
   c. Adds a direct link to the Email Settings page.
   d. Added an **Email Test** feature to verify that email settings are configured correctly.

Access Control

1. Adds a **Distributed Controller Management** module. This feature registers sub-controllers (distributed controllers) connected to the access controllers. See ***Distributed Controller Management*** .
2. Adds a **Timed Anti-Passback** feature to the anti-passback page. This feature prevents individuals from re-entering the same area within a defined reset period. After the reset period expires, re-authentication is permitted. See ***Configure Anti-Passback*** .
3. Adds an **Access Control → Cross-Controller Multi-door Interlocking** module. This feature supports interlocking between access points across multiple independent access controllers. ***Configure Cross-Controller Multi-door Interlocking*** .

Broadcast

1. For the ***Broadcast Console*** :
   a. On the Device Batch Settings page:
      i. Adds the **Restore Default** feature.
      ii. Adds the **Algorithm Configuration** page for configuring noise reduction, equalizer, and automatic gain control.
      iii. Adds the **Others** page for configuring acoustic fidelity mode, listening audio encoding, and scene mode.
   b. SIP configuration now supports an accessible IP address list and DTMF task list.
   c. Adds the **URL Settings** page for network audio playback by entering a network audio address.
2. Scheduled broadcast now supports audio templates, allowing quick selection of pre-configured templates when creating tasks. See ***Add a Scheduled Broadcast Task*** .
3. Scheduled broadcast tasks now support custom task dates. See ***Add a Scheduled Broadcast Task*** .

System and Security

1. On the **System Configuration → General** page, supports **Auto UI Scaling**. Adaptive Mode follows system scaling and uses vector rendering, keeping text and controls sharp. Fixed Mode disables

Qt DPI scaling, which causes the system to stretch bitmaps, so the layout stays the same but text may look blurry. See ***Set General Parameters*** .

2. Some device accounts that remain inactive for an extended period will be automatically disabled and require unlocking. See ***Manage Added Devices*** .
3. The Safety & Service module now includes SADP and SDK configurations. See ***Safety and Service*** .

1.3 Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Chapter 2 Service Management

iVMS-4200 Service is mainly applicable for data storage, data management, and data calculation. With continuous running and processing, it can manage the data, such as event records and attendance records, received by the iVMS-4200 Client Software. iVMS-4200 Service also provides management for user permissions, devices, groups, logs, etc.

You can view the module running status, and click **Edit Port** to edit its ports. You need to restart the iVMS-4200 Service to take effect.

Check **Auto-Launch** to enable launching the iVMS-4200 Service automatically after the PC started up.

The iVMS-4200 Service will not show after running it. Enter the system tray and click to open the service management window.

Note

- After closing the service window, the client will log out and return to the login page. You need to run the service and then log in again.
- The client can be run by no more than one operating system user at the same time on the same computer.
- The Service should run on the same computer with the client.

Chapter 3 Device Management

The client supports various types of devices including network camera, DVR (Digital Video Recorder), NVR (Network Video Recorder), security control panel, video intercom device, access control device, etc.

Example
You can view live view or playback after adding encoding devices to the client; you can arm or disarm zones of a security control panel, receive alarm notifications after adding a security control panel to the client; and you can control entrance & exit and manage attendance after adding access control devices to the client.

3.1 Activate Devices

For the inactive devices, you are required to create a password to activate them before they can be added to the software and work properly.

Before You Start
Make sure the device to be activated is connected to the network and on the same subnet with the PC where the client runs.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Device** on the left.
3. Click **Online Device** to show the online device list at the bottom of the page.
   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Note

For the NVR device, you are required to create a password in **Network Cameras' Default Password** field and confirm the password for activating network camera(s) connected to the NVR.

7. **Optional:** Enable Hik-Connect service when activating the device if the device supports.
   1) Check **Enable Hik-Connect** to open the Note dialog.
   2) Create a verification code, and confirm the verification code.
   3) Click **Terms of Service** and **Privacy Policy** to read the requirements.
   4) Click **OK** to enable the Hik-Connect service.
8. Click **OK** to activate the device.

Note

If the device supports resetting password via the reserved email, security question, or GUID, you can configure them after activating the device.

9. **Optional:** Click in the Operation column to edit the network information (including IP address, port number, gateway, etc.) for the online device.

3.2 Add Device

The client provides various device adding modes including IP/domain, IP segment, and cloud P2P. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

On the right Maintenance and Management area, click **Device Management**.

On the left, click **Device → Device** .

3.2.1 Add Single or Multiple Online Devices

The client can detect online devices which are in the same network as the PC running the client. You can select a detected online device displayed in the online device list and add it to the client. For detected online devices sharing the same user name and password, you can add them to the client in a batch.

Before You Start

- The device(s) to be added are in the same network as the PC running the client.
- The device(s) to be added have been activated.

Steps

1. On the Device page, click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.

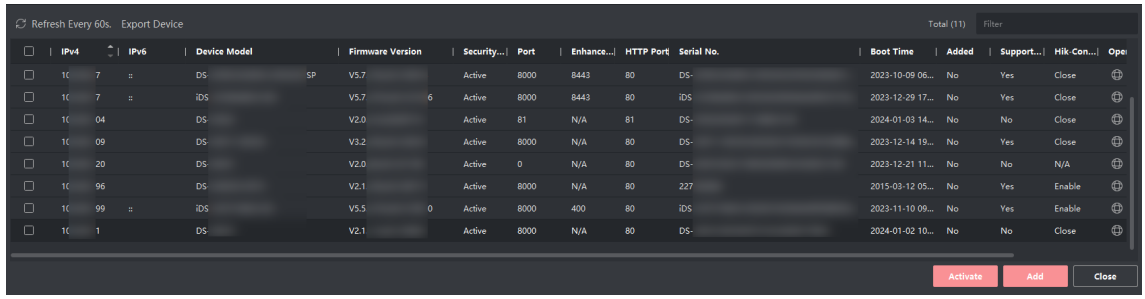


Figure 3-1 Online Device

2. In the **Online Device** area, check one or more online device(s), and click **Add** to open the device adding window.
3. Select the adding mode to **OTAP**.
4. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

You can customize the port number. The port number of the device is obtained automatically in this adding mode.

Note

For some device types, you can enter ***80*** as the port No. This function should be supported by the device.

User Name

By default, the user name is ***admin***.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See ***Certificate Verification for Transmission Encryption*** for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

   Example

   For encoding device, its encoding channels and alarm inputs/outputs will be imported to this group.

   For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. Click **Add**.
9. **Optional:** Click **Export Device**, select the saving path and device type, and click **OK** to export the device information to your PC.

Note

Currently, the platform only supports exporting the information of video intercom devices, including door stations, indoor stations, and main stations.

3.2.2 Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. On the Device page, click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
2. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
3. Enter the required information.

   Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is ***8000***.

Note

For some device types, you can enter ***80*** as the port No. This function should be supported by the device.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

4. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Enter the required information, including the device channel number and alarm input number.

   Note

   After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically.
5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See ***Certificate Verification for Transmission Encryption*** for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

   Example

   For encoding device, its encoding channels and alarm inputs/outputs will be imported to this group.

   For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
9. **Optional:** Perform the following operation(s).

Remote Configuration	On the device list page, click in the Operation column to perform remote configuration for a device. The is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.3 Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses ranges in the same IP segment, you can add them to the client by specifying the start IP address and the end IP address, port No., user name, password, etc of the devices.

Steps

1. On the Device page, click **Add** to open the Add window.
2. Select **IP Segment** as the adding mode.
3. Enter the required information.

   Start IP

   Enter a start IP address.

   End IP

   Enter an end IP address in the same network segment with the start IP.

   Port

   Enter the device port No. The default value is ***8000***.

   Note

   For some device types, you can enter ***80*** as the port No. This function should be supported by the device.

   User Name

   By default, the user name is ***admin***.

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
4. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Enter the required information, including the device channel number and alarm input number.

Note

After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Folder** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See ***Certificate Verification for Transmission Encryption*** for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to the group.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
9. **Optional:** Perform the following operation(s).

Remote Configuration	On the device list page, click in the Operation column to perform remote configuration for a device. The is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.4 Add a Device via OTAP

Some devices can be added via the OTAP.

Before You Start

Make sure the device is activated.

Steps

1. On the Device page, click **Add** to open the Add window, and then select **OTAP** as the adding mode.
2. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***8000***.

   Note

   For some device types, you can enter ***80*** as the port No. This function should be supported by the device.

   User Name

   Enter the device user name. By default, the user name is ***admin***.

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
3. **Optional:** Check **TLS** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default

directory to strengthen the security. See ***Certificate Verification for Transmission Encryption*** for details about enabling certificate verification.

- You can log into the device to get the certificate file by web browser.

4. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
5. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.
6. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.

3.2.5 Add Device by Hik-Connect

If the device supports Hik-Connect and its Hik-Connect function has been enabled, you can add it to both the client and Hik-Connect account by Hik-Connect mode; for devices already added to the Hik-Connect account, you can add them to the client after logging into the Hik-Connect account.

Before You Start

Make sure you have registered and logged into a Hik-Connect account first.

Steps

1. On the Device page, click **Cloud P2P Device → Add** to open the Add window.
2. Enter the device serial number.
   - Enter the serial number which you can find on the device label.
   - If the IP address of the device is in the same local subnet with the client, click **Online Device** and select an online device to get its serial number automatically.
3. Enter the verification code of the device.

Note

You can create the verification code when activating the device and enabling the Hik-Connect service, and is the same with the verification code created when enabling stream encryption. You can also create it on the device configuration page.

4. **Optional:** Check **Enable DDNS** to access the device by Hik-Connect Domain.

   Domain

   Customize the device domain name, which is used to get the IP address and port of the device registered on Hik-Connect server.

   UPnP Mode

   Auto

   Select **Auto** as the UPnP Mode to get the port number of the device automatically.

   Manual

   Select **Manual** as the UPnP Mode, and you need to input the port number of the device manually.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device password, which is created when you activate the device.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Note

If DDNS function is disabled, you cannot do some operations for the added device through client, such as viewing the device status, downloading the video files during remote playback, generating QR codes of devices, etc.

5. **Optional:** Check **Import to Group** to create a group by the Hik-Connect account name, and import all the channels of the device to the group.
6. Add device to the client software and Hik-Connect account.
   - Click **Add** to add the device and return to the device list.
   - Click **Add and New** to add the device and continue to add the next device.
7. **Optional:** Perform the following operation(s).

Remote Configuration	On the device list page, click in the Operation column to perform remote configuration for a device. The is in the rightmost column of the Device page. For details, refer to the user manual of device.
Edit Device Information	Click to edit the device details.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.2.6 Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.

3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Note

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter ***0*** or ***1*** or ***2***.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is ***8000***.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Add Offline Device

Enter ***1*** to enable adding an offline device.

After adding the offline device to the client, the device network status will be displayed as "Offline"; When the device comes online, the device network status will turn to "Online", and the client will connect it automatically. Enter ***0*** to disable adding an offline device.

Import to Group

Enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter ***0*** to disable this function.

Channel Number

If you enable **Add Offline Device**, enter the channel number of the device. If you disable **Add Offline Device**, this field is not required.

Alarm Input Number

If you enable **Add Offline Device**, enter the alarm input number of the device. If you disable **Add Offline Device**, this field is not required.

6. Click ··· and select the template file.
7. Click **Add** to import the devices.
8. **Optional:** Perform the following operation(s).

Remote Configuration	On the device list page, click in the Operation column to perform remote configuration for a device. The is in the rightmost column of the Device page. For details, refer to the user manual of device.
Device Status	Click in the Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click in the Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click in the Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click in the Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

3.3 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the client.

3.3.1 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
4. Select the device from the list and click on the Operation column.
5. Reset the device password.
   - Click **Export** to save the device file on your PC and then send the file to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

- Select the Safe Mode according to actual needs.

Note

For the following operations for resetting the password, contact our technical support.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

3.3.2 Restore Device's Default Password

If you forget the password of the detected online devices, you can restore their default password via the client.

Steps

1. Enter Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.
   All the online devices sharing the same subnet will be displayed in the list.
4. Select a device and click on the Operation column to open the Reset Password window.
5. Restore the device password.
   - Enter the security code, and then you can restore the default password of the selected device.

     Note

     For getting the security code, contact our technical support.
   - Click **Export** to save the device file on your PC and send the file to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

What to do next

The default password (12345) for the admin account is for first-time login purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

3.4 Upgrade Device Firmware Version

When there is a new firmware version available for the added device, you can upgrade its firmware version via the client.

Note

- The device should support this function.
- You can configure upgrading mode in System Configuration. See ***Set General Parameters*** for details.

Enter the Device Management module, and then click **Device** tab to show the device list.

Perform the following operations according to different upgrading modes.

Disable

On the Device for Management panel, if there is a new firmware version available, the status in the Firmware Upgrade column of the device will turn to **Upgradeable**.

Select the upgradeable device and click **Upgrade** to start upgrading the device firmware.

Note

The upgrade progress will show. When the upgrade is completed, the status in the Firmware Upgrade column of the device will turn to **Upgraded**.

Prompt Me If Download and Upgrade

If there is a new firmware version available, a prompt window will pop up. Click **Upgrade All** to start downloading and upgrading.

Download and Prompt Me If Upgrade

A dialog will pop up for selecting whether to upgrade after downloading package of new version. Click **Upgrade All** to start upgrading the device firmware.

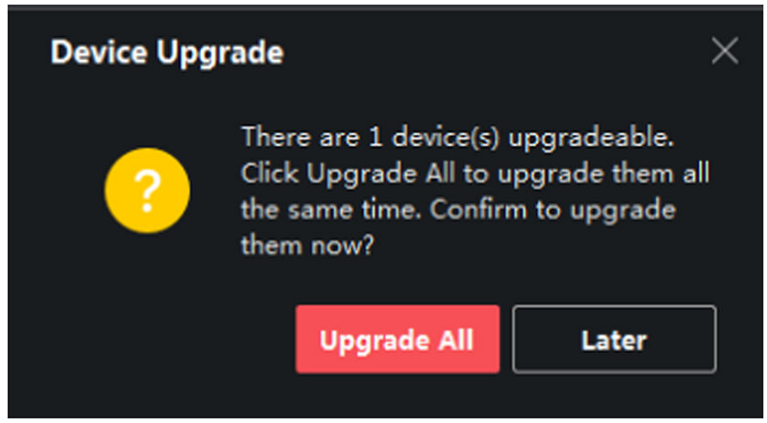


Figure 3-2 Device Upgrade Prompt

Note

After clicking **Upgrade All**, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt.

Upgrade Status

On the device management page, the following upgrade status will be shown in the Firmware Upgrade column.

No Available Version

No new firmware version available.

Upgradeable

A new firmware version available.

Note

Move the cursor on to view the current version, latest version, and upgrade content of the firmware version.

Waiting

The device is waiting for upgrade.

Downloading

The client is downloading the package of the new firmware version.

Upgrading

The upgrading of the device firmware is going on.

Upgraded

Hover the cursor on **Upgraded** to show the version after upgrading.

Upgrading Failed

When the upgrade fails, a prompt will pop up for viewing details. If you are not in Device Management page, click **View Details** to jump to Device Management page; if you are in Device Management page, close the prompt. Hover the cursor on **Upgrading Failed** to show the error details, and click **Upgrade Again** to try again.

3.5 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 3-1 Manage Added Devices

Edit Device	Click to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	On the device list page, click in the Operation column to perform remote configuration for a device. The is in the rightmost column of the Device page. For details, refer to the user manual of device.
View Device Status	Click to view device status, including cameras, recording status, signal status, hardware status, etc. **Note** For different devices, you will view different information about device status.
View Online User	Click to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click to refresh and get the latest device information.

Generate QR Code	Check one or more devices, and click **QR Code** to generate a QR code of the added device(s). You can add device(s) to the Mobile Client via scanning the QR code. **Note** Devices added by Hik-Connect cannot generate a QR code.
Upgrade Device	View device status in the Firmware Upgrade column, check one or more upgradable devices, and click **Upgrade Device Firmware** to upgrade the selected devices. For details, refer to ***Upgrade Device Firmware Version*** .
Get Events from Device	Check one device, and click **Get Events from Device** to synchronize events. For details, refer to ***Get Events from Device*** .
Export Device	Click **Export Device**, set the saving path and select device type to export the device details (such as device type, IP address, and port No.) to your local PC. **Note** The super user can enable **Password Protection** and enter the password, then the exported file of device information will be encrypted.
Unlock Device	Inactive device accounts are automatically disabled after a long period of non-login. To unlock, click , enter the administrator username and password, along with the device password. This function should be supported by the device.

3.6 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example
For example, on the 1st floor, there mounted 64 cameras, 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can get the live view, play back the video files, control door status, and do some other operations of the devices after managing the resources by groups.

3.6.1 Group Resources

The client provides two methods of adding a group: customizing a group or creating a group by device name. After customizing a group, you need to import resources into this group manually.

After creating a group by the device name, the resources of the device will be imported into the group automatically. You can choose one method to group your resources according to actual needs.

Steps

1. In the Maintenance and Management area, click **Device Management → Group** to enter the group management page.
2. Add a group.
   - **Customize a Group:** Click **Add Group** and create a name for the new group.
   - **Create a Group by Device Name:** Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device. After creating a group by the device name, the resources (such as encoding channels, alarm inputs, alarm outputs, and access points) of the device will be automatically imported to the group.

Note

- Up to 256 groups can be added.
- You can select multiple groups by pressing and holding Shift or Ctrl key on the keyboard.

3. After adding a group, you need to import resources into the group.

Note

For one resource, it can be added to different groups.

1) Select the type of resources to be imported, and click **Import**.
2) Select the resources to be imported, and click **Import** to import all the selected resources into this group.

4. **Optional:** After adding a group, perform one of the following operations if needed.

Expand or Fold Resource List	Click ▶ / ▼ to expand or fold the resource list in the group.
Search Resource	Enter the keyword and click 🔍 to search target resources.
Remove Resource from Group	Select resource(s) and click **Delete** to remove the selected resource(s) from the group.
Update Resource Name	You can update all the resource names in a group or in a channel. • Select a group, and click **Update Resource Name** to update all the resource names in the selected group. • Select a channel in one group, and update all the resource names in this channel. For example, click **Encoding Channels → Update Camera Name** to update all the camera names in encoding channels. **Note** This function should be supported by the device.

3.6.2 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For encoding channel, you can edit the channel name, stream type, protocol type, etc. For access point, you can edit the access point name. For alarm input, you can edit the alarm input name. Here we take encoding channel as an example.

Before You Start
Import the resources to group.

Steps
1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
   All the added groups are displayed on the left.
3. Select a group on the group list and click **Encoding Channel**.
   The encoding channels imported to the group will display.
4. Click in the Operation column to open the Edit Resource window.
5. Edit the camera information, including the camera name, the stream type, etc.
   Video Stream
   Select the stream type for live view of the camera as desired.

   Note
   You should start live view again to take effect.

   Playback Stream Type
   Select the stream type for playback of the camera as desired.

   Note
   - This field will display if the device supports dual-stream.
   - You should start live view again to take effect.

   Rotation Type
   Select the rotate type for the live view or playback of the camera as desired.

   Protocol Type
   Select the transmission protocol for the camera.

   Note
   You should start live view again to take effect.

   Streaming Protocol
   Select the protocol as RTSP or private for getting stream when live view.

Note

You should start live view again to take effect.

Copy to...

Copy the configured parameters to other camera(s).

Refresh

Get a new captured picture for the live view of the camera.

6. Click **OK** to save the new settings.

3.7 Safety and Service

The Safety and Service module centrally manages device network communication and security protection policies. Core features include:

- **Device List**: Displays basic device information, running status, and remote configuration.
- **Network Service**: Controls device access methods and transmission encryption policies.
- **IP Address Filter**: Configures IP access whitelists to restrict device access sources.
- **Security Audit Log**: Configures a log server to centrally upload security logs for future reference.

Device List

The device list displays information such as the device name, IP address, and online status. It supports configuring security protection policies for online devices individually or in batches. The configuration items displayed on the interface depend on the device's actual capabilities.

- Single Device Configuration: Click in the operation column, or select a single online device and click **Batch Configuration**.
- Batch Configuration: Select multiple online devices and click **Batch Configuration**.

Note

Batch configuration uses the first device's configuration as a template and applies it to the other devices.

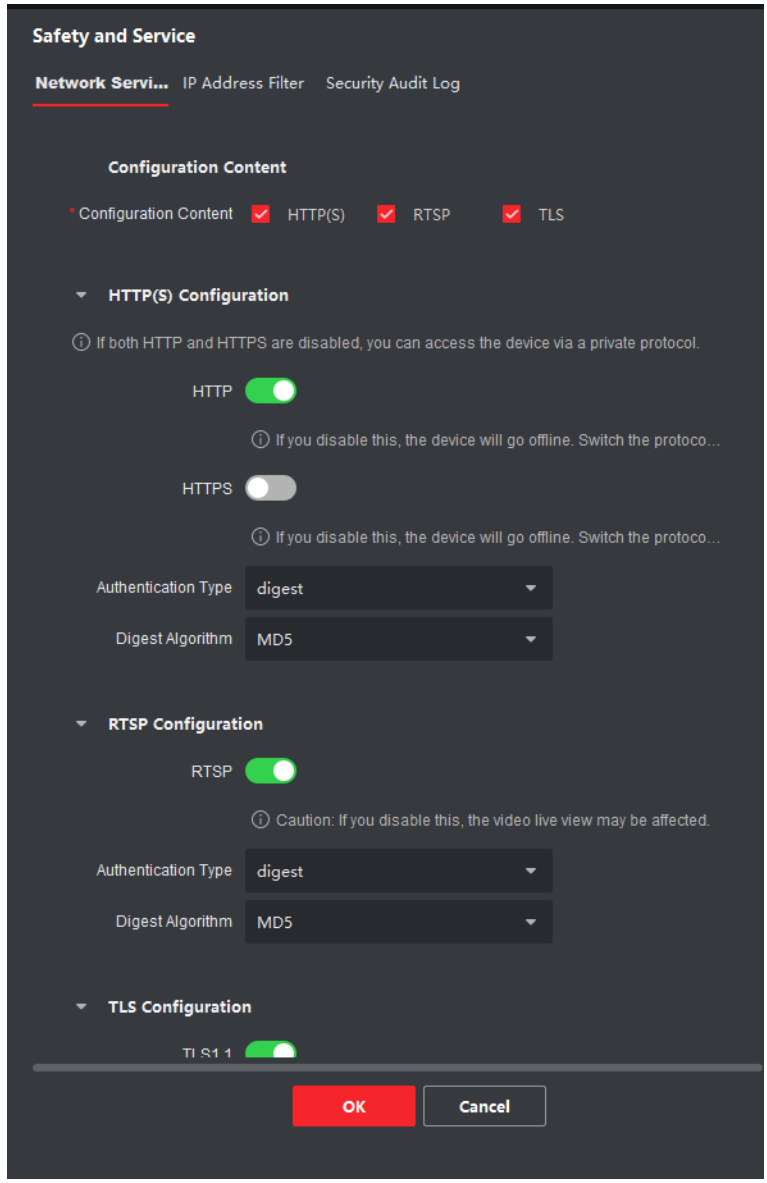


Figure 3-3 Configuration

Network Service Configuration

Sets the communication protocols and encrypted transmission levels supported by the device.

HTTP(S)

Configures the access protocol and secure transmission policy for the device's web interface.

- Authentication Type: The identity verification mechanism for access to the device.
- Digest Algorithm: Authentication encryption method.

Note

Disabling HTTP/HTTPS will cause the device to go offline. You need to switch the protocol (port) and log in again. Disabling both HTTP and HTTPS may affect some device features.

RTSP

Configures the real-time video stream transmission protocol and security policy.

Note

If RTSP is disabled, real-time video live view may be affected.

TLS

Configures the transmission encryption policy for the Transport Layer Security protocol. You can check the enabled TLS versions. Some device features may be affected if certain protocols are unchecked.

SADP

- Enable: The device can be discovered by tools or platforms on the local network, and maintenance write operations such as modifying the IP address and resetting the password are allowed via the SADP protocol.
- Discovery Only: The device can be discovered, but write operations such as modifying the IP address and resetting the password via the SADP protocol are prohibited, providing higher security.
- Disable: The device is hidden from the network, and tools or platforms cannot discover it via the SADP protocol.

SDK

- SDK Service: Controls whether the device opens SDK protocol access.
- SDK over TLS: An SDK service based on TLS encryption, providing higher security.

IP Address Filter Configuration

IP Address Filter configures the network access whitelist policy for the device. Once enabled, only IP addresses within the whitelist can access the device. When disabled, opening the interface will still fetch and apply the device IP list.
It supports manually adding a single IP address or IP network segment; you can also batch import the allowlist by downloading a template.

Security Audit Log Configuration

Configures the log upload server parameters to centrally upload the device's security operation logs to the central server for auditing and retention.
Enter the IP address and port of the central server receiving the logs, and set the upload interval.

Chapter 4 Hik-Connect

The client software also supports to register a Hik-Connect account, log into your Hik-Connect account and manage the devices which support the Hik-Connect service.

4.1 Register a Hik-Connect Account

The client supports registering a Hik-Connect account to manage devices which supports Hik-Connect service.

Steps

1. Enter the login page of a Hik-Connect account.
   - Click **Log in** in the upper-right corner of the client.
   - a. Click **Device Management → Device** to enter the Device Management page.
     b. Click **Cloud P2P Device → Add** to open the adding device pane.
     c. Select the region to log in.
     d. Click **Login**.

   The Login window pops up.

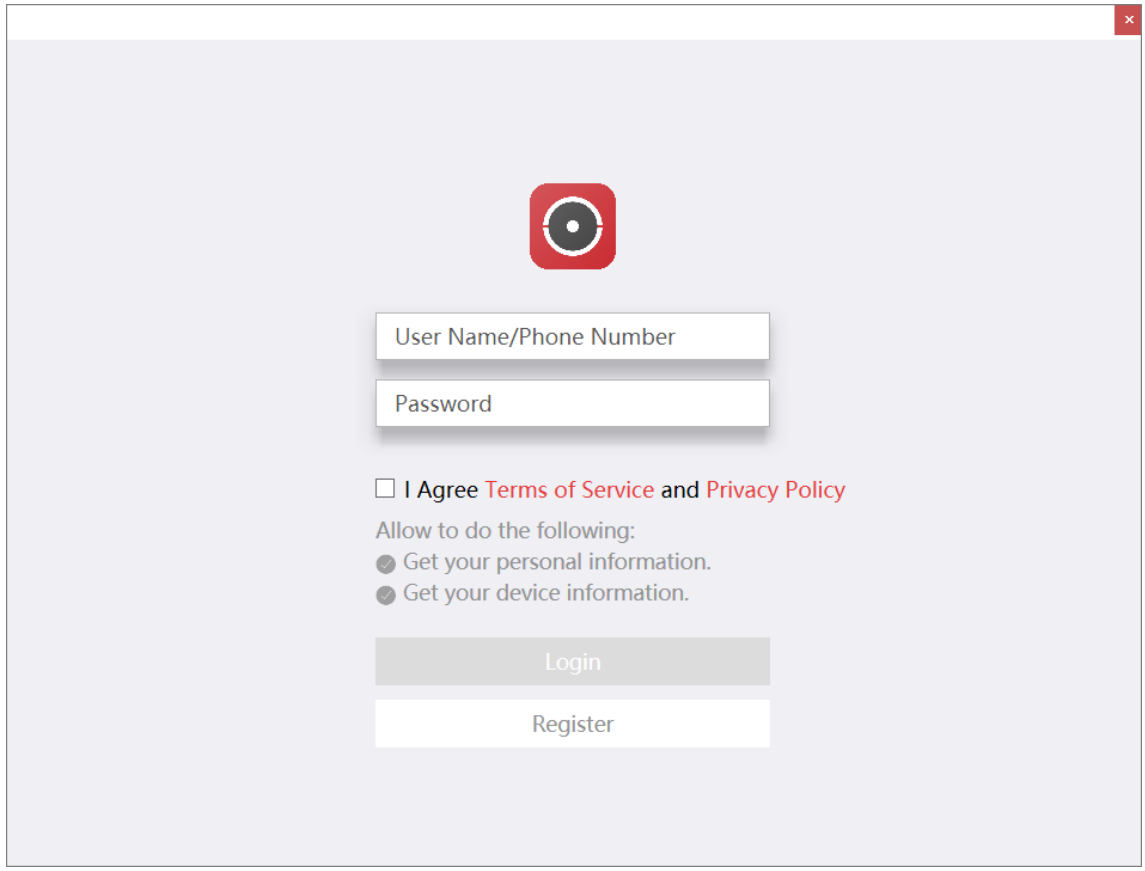


Figure 4-1 Login Window

2. Click **Register** to open the Register Account window.
3. Enter the required information, including user name, password, confirm password, and phone number/email address.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

4. Click **Send Message** to get a verification code.

   The system will send verification code to your phone or email.
5. Enter the received verification code in the **Verification Code** text field.
6. Check **I have read and agreed Terms of Service Privacy Policy**.

7. Click **Register** to finish the registration.

4.2 Log into Hik-Connect Account

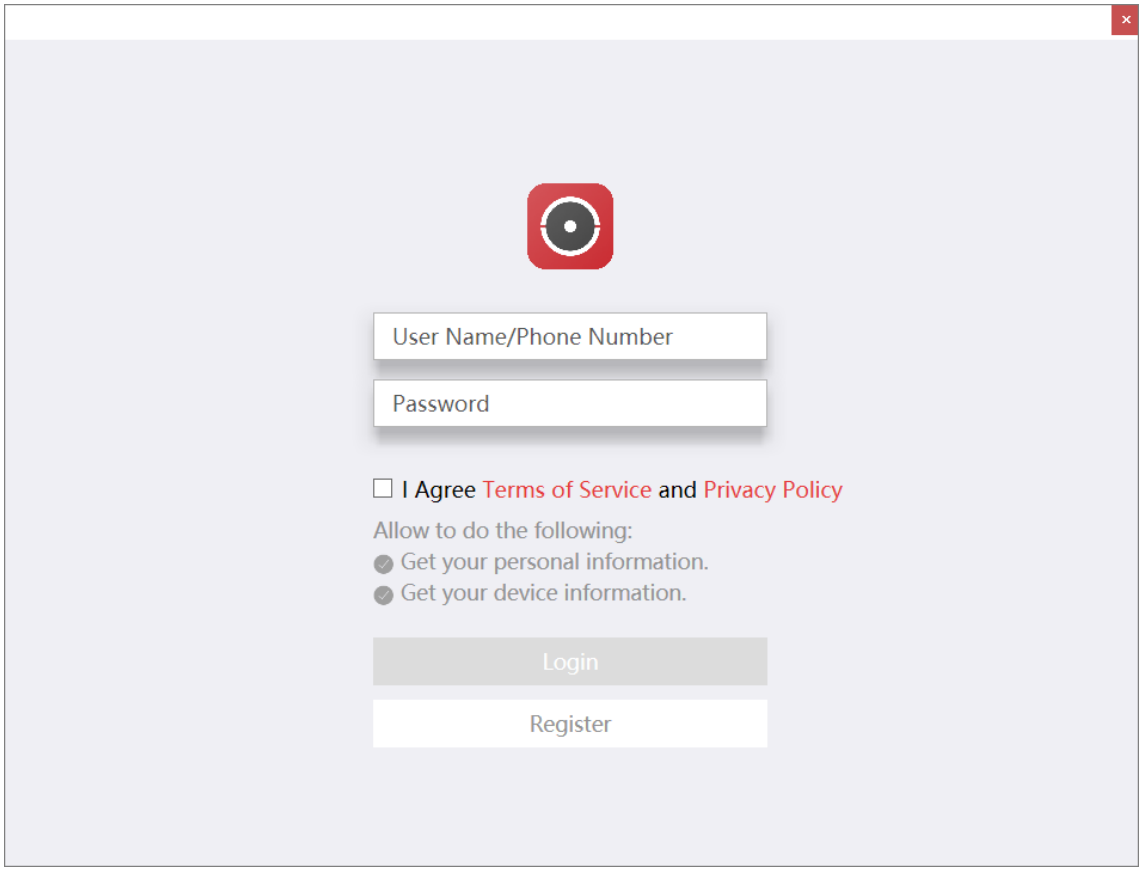
You can log into Hik-Connect account via the client, so as to operate devices managed by Hik-Connect account.

Before You Start
Register a Hik-Connect account.

Note
For details, refer to ***Register a Hik-Connect Account*** .

Steps
1. Enter the login page of a Hik-Connect account.
   - Click in the upper-right corner of the client.
   - a. Click **Device Management → Device → Cloud P2P Device → Add** to open the adding device pane.
     b. Select the region to log in.

   The Login window pops up.



2. Enter user name/phone number, and password.

3. Click **Log in** to log into your account.

   For devices shared to a Hik-Connect account via Hik-Partner Pro, the following features are available upon login: device management, live view, playback, recording download, alarm, and two-way audio.

4. **Optional:** Click **Logged in → Log out** to log out of your account.

Note

- Devices added by Hik-Connect will be hidden after logging out the Hik-Connect.
- Alarm-related pictures saved in Hik-Connect will be valid for 2 hours.

Chapter 5 Live View

You can view the live video of the added network cameras and video encoders on the Main View page. And some basic operations are supported, including picture capturing, manual recording, window division, PTZ control, Auto-Switch in live view, etc.

5.1 Live View Toolbar

The live view toolbar can help you operate and manage the live-view window more convenient and quick. For example, you can capture picture, record the audio, adjust the volume, split the window by the one-click of the tools on the toolbar.

Description of Global Toolbar Icons

Icon	Function Name	Function Description and Operation
	Save View	Save the view you create currently, which is convenient for quick viewing the cameras. Click to pop up the window of saving view. Select **Create View** or **Current View**, and name for the view.
	Stop Live View	Stop the all the live view cameras.
/	Mute/Cancel Mute	Click to pop up the volume bar， click to cancel the mute and you can adjust the volume. Click to pop up the volume bar, click again to set the live-view cameras as mute.
	Window Division	Select the different window division mode for live view. Click to select one window division mode (e.g. 9 window division). You can also click **Add** to customize a window division mode.
	Full Screen	Display the live view in full screen. Press ***Esc*** key to exit full screen mode.
	Configuration	Enter the live view parameters setting mode, configure for live view and playback, image, files and toolbar.
	Audible and Visual Alarm	Enable **Audible Warning** or **Strobe Light** for warnings and deterrence. For example, if audible warning is enabled, in warehouse security monitoring, when the system detects

Icon	Function Name	Function Description and Operation
		unauthorized intrusion via infrared device, sounder broadcast content will be played to deter intruders and notify on-duty staff. **Note** This function should be supported by device.

Description of Live View Toolbar Configuration

1. Click on the lower-right corner of Main View page, and select **Live View Toolbar** in the popping up pane on the right.
2. (Optional) Switch on **Enable Screen Toolbar Display**, the live view toolbar will appear when you hover the cursor on the live view window. Then you can switch on **Lock Toolbar**, the live view toolbar will be stuck on the live view window all the time.

   Note

   The function of locking toolbar is not supported when there are more than 9 windows in the live view image.
3. In **General Toolbar** and **Device Exclusive Toolbar**, you can select the icon(s) as needed. Also, you can drag an icon to move its location.

   Note

   The supported icons in device exclusive toolbar vary according to different devices.

Table 5-1 Description of Live View General Toolbar

Icon	Function Name	Function Description and Operation
	Capture	Manually capture the pictures for the live view window.
/	Start Recording/ Stop Recording	Click the first time to start recording and click again to stop recording, and automatically save the recording files to the path you have set.
	Switch to Instant Playback	On the current time, you can select to play back the video in previous 30 s, 1 min, 3 min, 5 min, 8 min, 10 min.

5.2 Add Custom View

A view is a window division with cameras configured to each window; View mode enables you to save the window division and the correspondence between cameras and windows as favorite to

quickly access the related cameras later. For example, you can link camera 1, camera 2, and camera 3 located in your office to display windows and save them as a view called office.

Steps

1. Enter the Main View page.
2. Click **Resource** tab.
3. Move the cursor to the Custom View in the resource panel and click + to create a new view.

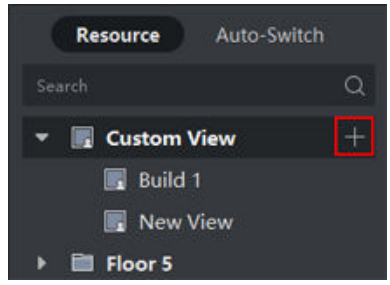


Figure 5-1 Add Custom View

4. Enter a name for the view.
5. **Optional:** Click in the live view toolbar to set window division mode for the new view.
6. Start live view for specified camera in specified window according to actual needs.
7. Click to save the current view or save it as a new view.

Note

Up to 16 custom views are allowed to add to the client.

8. **Optional:** Perform the following operations after adding the custom view.

Edit View Name	Move the cursor over the new view and click to edit the view name.
Delete View	Move the cursor over the new view and click to delete the view.

What to do next

Click again to select the custom window division.

5.3 Start Live View

You can start live view after adding device(s) to the client so that you can get to know the monitored area well. You can start the live view of one camera or all cameras in a group. You can also start the live view in custom view mode.

Click **Main View → Resource** to enter Main View page. On the left resource list, select resource(s) and start live view by the following ways.

Available Ways	Description	Operation
Start Live View for One Camera	Start the live view of only one camera in a group.	• Select a camera and drag it to the window. • Double-click the camera in a group. • Move your cursor over the camera name, and click .
Start Live View for Camera Group	Start the live view of all cameras in one group synchronously.	• Select a group and drag it to the window. • Double-click the group. • Move your cursor over the group name, and click , or click → **View All Cameras in Group** .
Start Live View in Custom View Mode	Start the live view of the cameras in the custom view.	• Select a custom view and drag it to the window. • Double-click the custom view. **Note** Customize a view which containing information such as window division, camera and correspondence between cameras and windows. See ***Add Custom View*** for details.

Note

If the device supports stream encryption, and the stream of its live view is encrypted, you are required to enter a stream key for double verification.

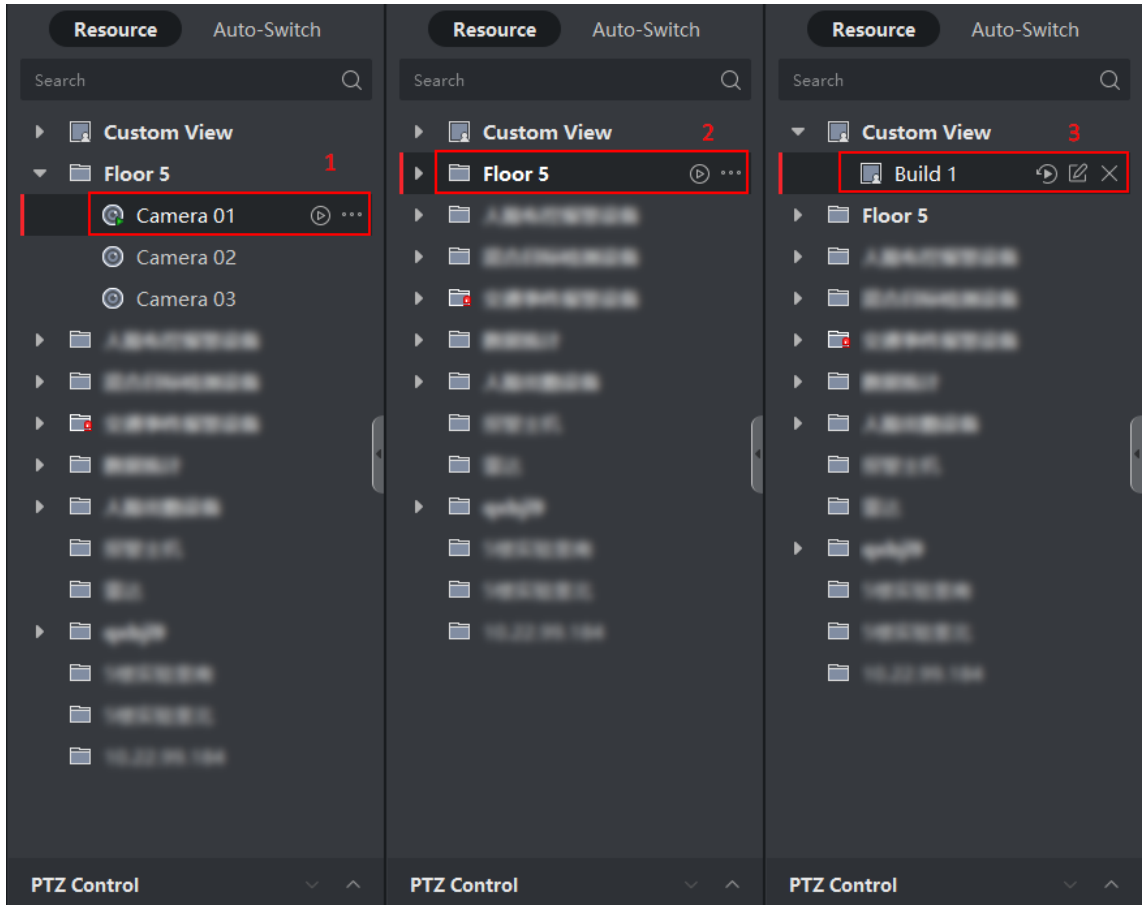


Figure 5-2 Start Live View

During live view, you can view the bitrate, frame rate and resolution information on the image. In the full-screen live view, you can drag any camera to any other windows.

5.4 Auto-Switch in Live View

You can display live view of cameras or display the custom views in turn, which is called "auto-switch". If you want to perform live view of a large amount of cameras, you can auto-switch the cameras in a group in a single screen or all cameras in multiple screens. You can also add an auto-switch schedule, which means you can add the selected cameras or custom views to windows, then the client will automatically switch live view of the selected cameras or custom views by the window No..

When auto-switching in live view, three modes are available:

- Auto-Switch All Cameras in Default View
- Auto-Switch Cameras in a Group
- Auto-Switch Cameras or Custom Views by Schedule

5.4.1 Auto-Switch Cameras in a Group

The video stream of the cameras from the same group can switch automatically in a selected display window. For example, if you start auto-switch of a group containing 5 cameras, the live view of the 5 cameras will be displayed in turn with an interval which can be configured. You can also switch to playback and perform other operations on the display window.

Steps

1. Enter the Main View page.
2. Click **Auto-Switch → Single Window Auto-Switch** on the left panel to show the groups.
3. Select a display window on the right panel.
4. Hover the cursor on a group name and click .

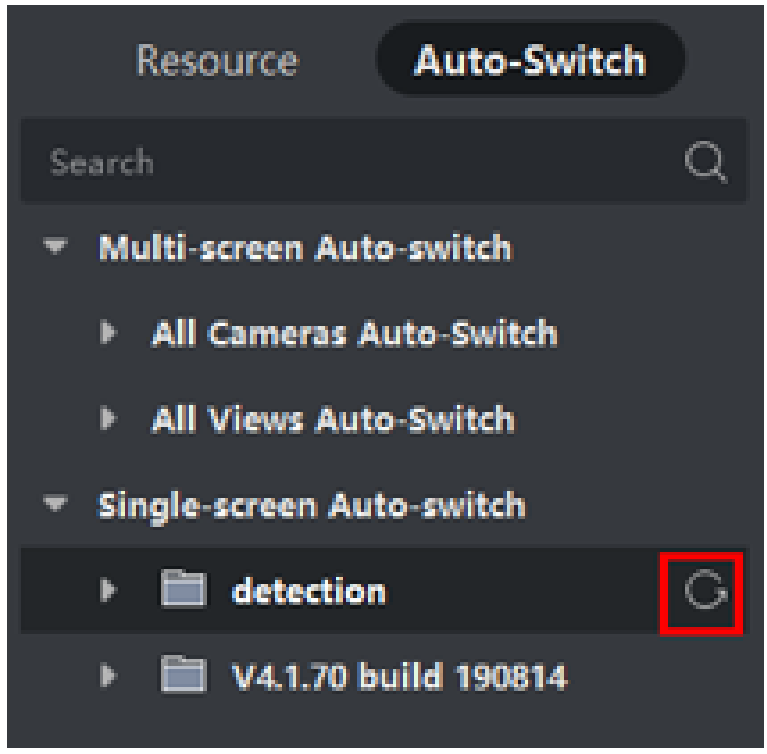


Figure 5-3 Start Auto-Switch of Cameras in a Group

The cameras in the selected group starts auto-switch in the display window.

Note

The audio is off by default after auto-switch starts.

5. **Optional:** Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click or to pause/resume auto-switch.

Go to Previous/ Next Page	Click < or > to display cameras of the previous/next group.
Set Dwell Time	After stopping the current auto-switch, click << or >> to decrease/ increase auto-switch dwell time, or click **20s** at the bottom of the page to change the auto-switch dwell time. You can also click **Custom Dwell Time** to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each group will be displayed for 10 seconds and then switch to next group.

5.4.2 Auto-Switch All Cameras

The video of all the cameras in the camera list can switch automatically in a self-adaptive mode. If you start auto-switch of all cameras, the live view of all cameras can be displayed quickly, which is an effective way for live view. The auto-switch is performed with an interval which can be configured. You can also switch to playback and perform other operations on the auto-switch window.

Steps

1. Enter the Main View page.
2. Click **Auto-Switch → Multi-Window Auto-Switch** on the left panel.
3. Hover the cursor on **Auto-Switch All Cameras**, and then click .

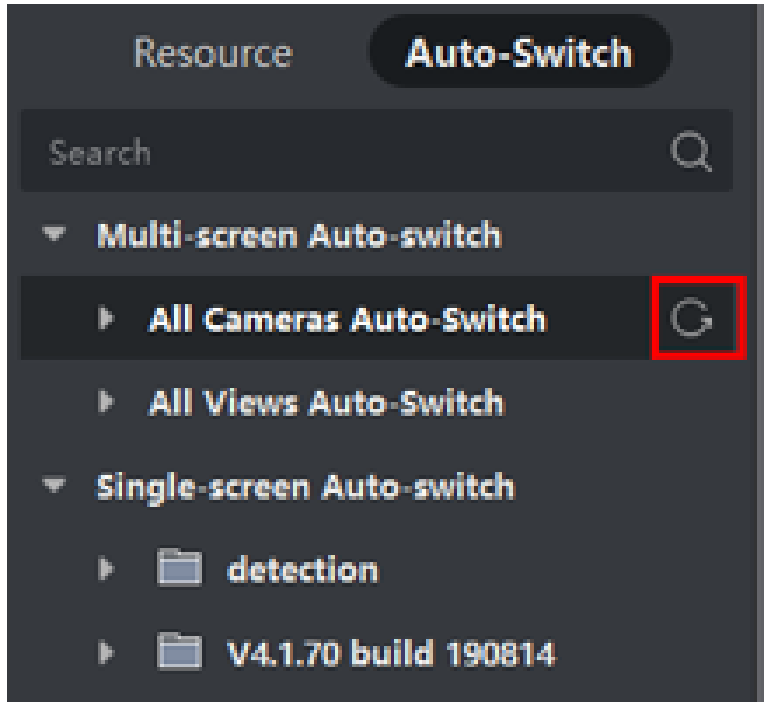


Figure 5-4 Start Auto-Switch of All Cameras

All cameras in the camera list start auto-switching in a self-adaptive mode.

4. **Optional:** Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click or to pause/resume auto-switch.
Go to Previous/ Next Page	Click or to display cameras on the previous/next page.
Set Dwell Time	After stopping the current auto-switch, click or to decrease/ increase auto-switch dwell time, or click **20s** at the bottom of the page to change the auto-switch dwell time. You can also click **Custom Dwell Time** to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each camera will be displayed for 10 seconds and then switch to next camera.

5.4.3 Auto-Switch Cameras or Custom Views by Schedule

You can add an auto-switch schedule by adding multiple windows, the window content include the selected cameras or custom views. Then, the client will automatically switch live view of the selected cameras or custom views by the window No.

Before You Start

Add the custom views. See ***Add Custom View*** for details.

Steps

1. Enter the Main View page.
2. Click **Auto-Switch → Auto-Switch Schedule** on the left pane.
3. Select a camera group or a custom view on the right list, click or drag the camera group or the custom view to the left window to add.

   Add the first window.
4. Repeat the previous step to add a new window.

Note

- You can add no more than 20 windows in total.
- You can drag other resources to replace the original content in the added window.
- No more than 64 window can be supported in a window.

Add an auto-switch schedule.

5. **Optional:** Click on the right side of a custom view or camera to replace the original content in the window.
6. Click to start window auto-switch.

   The cameras or the custom views in windows start auto-switch by the window No.
7. **Optional:** Perform the following operations.

Operation	Description
Pause/Resume Auto-Switch	Click or to pause/resume auto-switch.
Display Window in Full Screen	Click to display the window in full screen. Press ***Esc*** key to exit full screen mode.
Go to Previous/ Next Page	Click or to display the previous/next window.
Set Dwell Time	Click or to decrease/increase auto-switch dwell time, or click **20s** at the bottom of the page to change the auto-switch dwell time. You can also click **Custom Dwell Time** to set the dwell time according to your need. For example, if you set the interval as 10 seconds, the image of each window will be displayed for 10 seconds and then switch to next window.

5.5 PTZ Control

The software provides PTZ control for cameras with pan/tilt/zoom functionality. During the PTZ control, you can set preset, patrol, and pattern, and you can also open a new window for controlling the PTZ.

Caution

- Some functions should be supported by the device.

5.5.1 PTZ Control Panel

The software provides PTZ control operations via control panel, such as detection, speed, zoom in, zoom out, etc. You can also open a new window for controlling the PTZ.

Note

Hik-Connect device only supports the PTZ movements to the directions of up, down, left, and right.

Enter the **Main View** module, and select **Resource → PTZ Control** to open the PTZ control panel. The following icons are available on the PTZ control panel.

Table 5-2 Icons on PTZ Control Panel

Icon	Name	Description
	Direction Buttons	Click or hold the left mouse button to turn the PTZ around.

Icon	Name	Description
		Click to turn around the PTZ horizontally and continuously; click again to stop turning.
	Speed Control	Drag the slider to adjust the PTZ moving speed.
	Zoom in/out	Zoom in to view close image for details; zoom out to view a panoramic image.
	Focus +/-	Click **Focus +** move the focal point forward, and click **Focus -** to move the focal point backward.
	Iris +/-	Used for adjusting the luminance of the image. The larger the iris is, the more the light enters, and the brighter the image will be.
	3D Positioning	Use the left key of mouse to click on the desired position in the video image and drag a rectangle area in the lower right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.
	Auxiliary Focus	Click to focus automatically.
	Lens Initialization	Initialize the lens and focus again for a clear image.
	Light	Click to fill light. **Note** This function needs to be supported by the device.
	Wiper	Use the wiper to clear the dust on the camera lens.
	Manual Tracking	For speed dome with auto-tracking function, enable the auto-tracking (via right-click menu) for it and click the icon to manually track the target by clicking on the video.

Icon	Name	Description
	Menu	For analog speed dome, click the icon to display its local menu. For detailed operation of the menu, refer to user manual of the speed dome.
	One-Touch Patrol	For speed dome with one-touch patrol function, click the icon and the speed dome starts patrol from the predefined preset No.1 to preset No.32 in order after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	One-Touch Park	For the speed dome with one-touch park function, click the icon and the speed dome saves the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	Enable Manual Lens De-Icing Heater	Enable this function to ensure the camera performance by heating. **Note** We suggest you enable this function when the environment temperature is under 0 °C, otherwise the high temperature may affect the camera work.
	Enable Manual PT De-Icing	Enable this function to ensure the camera performance by wiping off the ice adhered on the PTZ camera.
	Manual Face Capture	Click this button, and hold the left mouse button to select a face in the image to capture it. The picture will be uploaded to the server for viewing.
	Synchronize FOV	For thermal cameras, click the icon to synchronize the optical channel's field of view with that of the thermal channel.

Icon	Name	Description
	Regional Exposure	For speed domes, click the icon and draw a rectangle on the image to optimize the exposure effect in this region.
	Regional Focus	For speed domes, click the icon and draw a rectangle on the image to optimize the focus effect in this region.
	Arming and Tracking	For cameras support arming and tracking, click the icon and select the target (person or vehicle) in the live view to arm and track this target.
	Hazardous Gas Detection	When you click the button, the device starts hazardous gas detection, and then the client displays hazardous gas information on the live view image.

5.5.2 Set Preset, Patrol, and Pattern

PTZ control supports setting and calling a preset, patrol, and pattern.

On the Home Page, click **Main View → PTZ Control** to show the PTZ Control panel.

Task	Definition	Operation
Preset	A preset links the key regions to mobile PTZ position and status. Monitoring people uses it to positioning to key regions rapidly. By sending setting preset command, mobile PTZ records the position and status of zoom, focus, and iris. When executing calling preset command, mobile PTZ rapidly rolls to the set position and resume to set status.	How to Set: select a preset from the preset list→turn the camera to a desired position→click 。
		How to Call: click 。
Pattern	By recording pattern, the movement path and the dwell time in a certain position can be recorded precisely. By	How to Set: click to start recording a pattern→click the direction buttons to shape the pattern→click .

Task	Definition	Operation
	calling pattern, mobile PTZ starts move totally according to the recorded path.	How to Call: click 。
Patrol	Patrol is the function that users specify a scan track with a group of defined presets. The patrol between two presets is performed with the set speed and time.	How to Set: click →select presets, and set speed and time→click **OK**.
		How to Call: click .

Note

You should set at least two presets beforehand.

5.6 Sensor Control

Supports remote control of the furnace combustion monitoring camera (referred to as sensors), including sensor advancement/retraction.

On the Resource panel, double-click a camera and click the live view window to open the **Sensor Control** panel in the lower-left corner.

After entering the panel, a list of sensors will be displayed. You can perform advance/retract operations on the sensors. After the operation, the current status of the sensors will be shown: **Retracted** / **Advanced**.

Advance

Move the camera forward to get a closer view of the inside of the furnace.

Retract

Move the camera backward to expand the viewing range or move away from high-temperature areas.

5.7 Customize Window Division

The client software provides multiple kinds of predefined window divisions. You can also set custom the window division as desired.

Steps

Note

Up to 5 window divisions can be customized.

1. Open the Main View or Remote Playback page.
2. Click on the live view or playback toolbar to open the window division panel.
3. Click **Add** to open the Add Custom Window Division dialog.
4. Enter the window numbers in both horizontal and vertical dimension in the Dimension field, and then press **Enter** on your keyboard.

Note

For remote playback, up to 16 windows can be played at the same time, so the custom window division with more than 16 windows is invalid.

5. **Optional:** Drag your mouse to select the adjacent windows, and click **Joint** to joint them as a whole window.
6. **Optional:** Select the joint window and click **Restore** to cancel the joint.
7. Click **Save**.
8. **Optional:** Click or drag a division mode to the displaying window to apply the mode for displaying.
9. **Optional:** Edit a customized window division mode.
   1) Click on the live view or playback toolbar to open the window division panel.
   2) Click **Edit** to open the Add Custom Window Division.
   3) Select a customized division mode and perform operations including renaming, setting dimension, jointing/undo jointing windows.

5.8 Manually Record and Capture

During live view, you can record videos and capture pictures manually, and then view the recorded video files and captured pictures in the local PC.

5.8.1 Manually Record Video

Manual recording function allows to record the live video on the Main View page manually, and you can store the video files in the local PC.

Steps

Note

Manual recording is not supported by Hik-Connect device during live view.

1. Open the Main View page.
2. Start the live view.
3. Perform one of the following operations to start manual recording.
   - Move the cursor to the display window in live view to show the toolbar and click on the toolbar.
   - Right-click on the display window and click **Start Recording** on the right-click menu.

The icon turns to . An indicator appears in the upper-right corner of the display window.

4. Click to stop the manual recording.

   The recorded video file is automatically saved to the local PC, and a small window with the saving path information appears in the lower-right corner of desktop.

Note

The saving path of the recorded video files can be set on the System Configuration page. See ***Set File Saving Path*** for details.

5.8.2 View Local Videos

You can view the recorded video files stored in your local PC.

Before You Start
Record the live video.

Steps

1. Click → **File** → **Open Video File** in the upper-right corner to open the Video Files page.
2. Select the camera to search the recorded video files from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

   The video files recorded between the start time and end time displays in thumbnail format on the page.
5. **Optional:** Perform the following operation(s) after the search.

Delete Video File	Select the video file, and click **Delete** to delete the video file.
Send Email	Select the video file, and click **Email** to send an email notification with the selected video file attached. **Note** To send an email notification, the email settings need to be configured before proceeding. For details, refer to ***Set Email Parameters*** .
Save Local Video	Select the video file, and click **Save as** to save a new copy of the video file.
Playback	Double-click the video file to start the local playback.

5.8.3 Capture Pictures

You can capture pictures during the live view.

Perform this task when you need to capture pictures during the live view.

Steps

1. Open Main View page and start the live view of a camera.
2. Perform one of the following operations to capture pictures.
   - Move the cursor to the display window in live view to show the toolbar and click on the toolbar.
   - Right-click the display window and click **Capture** on the right-click menu.

   The captured picture is automatically saved to the local PC, and a small window with the picture preview and saving path information appears in the lower-right corner of desktop.

Note

The saving path of the captured pictures can be set on the System Configuration page. For details, refer to ***Set File Saving Path*** .

5.8.4 View Captured Pictures

The pictures captured in the live view are stored in the PC running the software. You can view the captured pictures if needed.

Before You Start

Capture pictures in the live view.

Steps

1. Click → **File** → **Open Captured Picture** in the upper-right corner to open the Captured Picture page.
2. Select the camera to search the captured pictures from the Camera Group list.
3. Specify the start time and end time in the lower-left corner for the searching.
4. Click **Search**.

   The pictures captured between the start time and end time display in thumbnail format on the page.
5. **Optional:** Perform the following operation(s) after the search.

Enlarge Picture	Double-click the picture thumbnail to enlarge it for a better view.
Print Picture	Select the captured picture, and click **Print** to print the selected picture.
Delete Picture	Select the captured picture, and click **Delete** to delete the selected picture.
Send Email	Select the captured picture, and click **Email** to send an email notification with the selected picture attached.
Save Picture	Select the captured picture, and click **Save as** to save a new copy of the selected picture.

5.9 Instant Playback

Instant playback shows a piece of the video which is remarkable, or which is unclear on the first sight. So you can play the video files instantly on the Main View page and get an immediate review if needed.

Before You Start
Record the video files and store them on the storage devices, such as the SD/SDHC cards and HDDs on the DVRs, NVRs, network cameras, etc.

Steps
1. Open Main View page and start the live view.
2. Perform one of the following operations to show the pre-play durations' list of instant playback.
   - Move the cursor to the display window to show the toolbar and click .
   - Right-click the display window and select **Switch to Instant Playback** on the right-click menu.
   - Move the cursor to default view or custom view node on the View panel and click .

   A list with pre-play durations of 30s, 1 min, 3 min, 5 min, 8 min, and 10 min displays.
3. Select a time period from the appeared list to start the instant playback.

   Example

   If you select 3 min, and the current time of the live view is 09:30:00, then the instant playback will start from 09:27:00.

   During the instant playback, an indicator appears in the upper-right corner of the display window.
4. **Optional:** Click again to stop the instant playback and go back for the live view.

5.10 Live View for Fisheye Camera

For fisheye cameras, you can start the live view in fisheye mode, set presets and patrols, and perform PTZ control.

5.10.1 Perform Live View in Fisheye Mode

During live view of fisheye cameras, the whole wide-angle distorted view will be displayed. But you may have difficulty to view some details. To solve this problem, you can play the live videos in fisheye expansion mode. Fisheye expansion can expand images in various modes: 180° panorama, 360° panorama, PTZ, half sphere, etc. So that you can view the image clearly.

Before You Start
Make sure you have installed Microsoft DirectX component.

Steps
1. Open the Main View page and start the live view of fisheye camera.

2. Enter the Fisheye Expansion mode.
   - Right-click on the video and select **Fisheye Expansion**.
   - Click in the toolbar. See ***Set Icons Shown on Toolbar*** for details about setting the toolbar.

   turns to .
3. Click in the lower-left corner of the displaying window to open the Mounting Type & Expanding Mode Selection panel.
4. Select the mounting type of the fisheye camera according to its actual mounting position.
5. Select the expanding mode for live view as desired.

   Fisheye

   In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called Fisheye because it approximates the vision of a fish's convex eye. The lens produce curvilinear images of a large area, while distort the perspective and angles of objects in the image.

   Panorama

   In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

   PTZ

   The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

   Note

   Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

   Half Sphere

   By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

   AR Half Sphere

   AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

   Cylinder

   In Cylinder mode, the image is formed into a cylinder page.
6. **Optional:** Perform the following operation(s) after starting live view in fisheye mode.

Capture	Right-click on the window and select **Capture** to capture the picture in the live view process.
Enter Full Screen	Right-click on a playing window and switch the selected window to full-screen mode.

5.10.2 PTZ Control in Fisheye Mode

In fisheye mode, you can control the PTZ to adjust the PTZ window.

Note

The PTZ panel varies according to different devices.

The following functions are available on the PTZ control panel.

- Select a PTZ window, and click the direction buttons to adjust view angle. Or drag the No. label in the fisheye or panorama window to change the view angle of the PTZ window.
- Select a PTZ window, click to start auto-scan (the camera rotates in a horizontal direction) , and click it again to stop auto-scan.
- Drag the slider on to adjust the speed for PTZ movement.
- Click , or scroll the mouse wheel to zoom in or zoom out the selected PTZ window.

5.10.3 Set a Preset and Patrol

PTZ supports configuring and calling a preset and patrol.

Enter the **Main View** page, and select **Fisheye Expansion** after right-clicking a camera.

Task	Definition	Operation
Preset	A preset links the key regions to mobile PTZ position and status. Monitoring people uses it to positioning to key regions rapidly. By sending setting preset command, mobile PTZ records the position and status of zoom, focus, and iris. When executing calling preset command, mobile PTZ rapidly rolls to the set position and resume to set status.	How to Set: select a preset from the preset list→turn the camera to a desired position→click .
		How to Call: click .
Patrol	Patrol is the function that users specify a scan track with a group of defined presets. The patrol between two presets is performed with the set speed and time.	How to Set: click →select presets, and set speed and time→click **OK**.
		How to Call: click .

5.11 Perform Smart Linkage

The box or bullet camera which supports smart linkage function can locate or track the target according to your demand.

Note

- This function in only supported by the specific box or bullet camera.
- A speed dome with the auto-tracking function is required to be installed near the box or bullet camera.

5.11.1 Configure Smart Linkage Rule

Before performing smart linkage during live view, you should configure the smart linkage rules for the box or bullet camera, including setting VCA detection rule, linking to a speed dome, and calibrating camera and speed dome.

Set Intrusion Detection Rule

You should set the VCA detection rule for the bullet or box camera, and when the VCA event is triggered, the client can trigger speed dome to track the target. Here we take intrusion detection as an example.

Steps

1. Open Device Management page and select a box or bullet camera.
2. Click → **Advanced Configuration → VCA Config → Rule → Rule Settings** to enter rule settings page.
3. Click **Add** in Rule List panel to add a rule.
4. Select **Intrusion** as the event type.
5. Click to draw a detection region on the live video.
6. Click **Save**.

Link Speed Dome

When configuring the smart linkage for the box or bullet camera, you can link the camera to a speed dome and set the PTZ position for the speed dome for tracking.

Perform this task to link the box or bullet camera to a speed dome for smart linkage.

Steps

1. Open Device Management page and select a box or bullet camera.
2. Click → **Advanced Configuration → Smart Linkage** to enter smart linkage settings page.
3. Click **Login** on the display window to open the speed dome login window.

4. Input the speed dome's IP address, port No., user name, and password.
5. Click **Login** to log in to the speed dome.
6. Click **PTZ** and use the direction arrows to adjust the speed dome to a horizontal position.

What to do next
Calibrate the box or bullet camera and the linked speed dome, see ***Calibrate Camera and Speed Dome Automatically*** or ***Calibrate Camera and Speed Dome Manually*** for details.

Calibrate Camera and Speed Dome Automatically

When setting the bullet or box camera's smart linkage rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the auto calibration.

Before You Start
Link the camera to a speed dome, see ***Link Speed Dome*** for details.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click → **Advanced Configuration** → **Smart Linkage** to enter smart linkage settings page.
3. Select the calibration mode as **Auto Calibrating** in the lower-right corner of Calibration panel.
4. Move and zoom in/out the view of speed dome to make sure the live views of dome and camera are mostly same.
5. Click **Save**.

Calibrate Camera and Speed Dome Manually

When setting the bullet or box camera's smart linkage rule, you should calibrate the camera and the speed dome. Two calibration modes, including auto and manual, are available, here we introduce the manual calibration.

Before You Start
Link the camera to a speed dome. See ***Link Speed Dome*** for details.

Steps
1. Open Device Management page and select a box or bullet camera.
2. Click → **Advanced Configuration** → **Smart Linkage** to enter smart linkage settings page.
3. Select the calibration mode as **Manual Calibrating** in the lower-right corner of Calibration panel.
4. Select site No. 1 from the list and click .

   A blue cross appears in the center of the live view page, and the digital zoom view of the selected site appears on the right.
5. Repeat step 4 to add other manual calibration sites.
6. Adjust the distances among the four calibration sites evenly in the live view page.
7. Select the calibration site No. 1.

The digital zoom view of site No. 1 appears at the right.

8. Move and zoom in or out the view of speed dome to make sure the live views of speed dome and the digital zoom view of selected site are mostly same.
9. Click to save the current site position information.
10. Repeat step 7, 8, and 9 to set other sites' position.
11. Click **Save**.

5.11.2 Enable Smart Linkage

During live view, you can enable the smart linkage to locate or track the target appeared in the view of bullet or box camera with a speed dome.

Before You Start

Configure the smart linkage rules for the box or bullet camera.

Perform this task when you need to enable the smart linkage for box or bullet camera.

Steps

1. Enter the Main View page and start the live view of box or bullet camera.
2. Right-click on the live view window and click **Smart Linkage → Open → Manual Smart Linkage / Auto Smart Linkage** .
   - **Manual Smart Linkage**: Draw an area or select a specific target on the live view window, prompting the box or bullet camera to position accordingly.
   - **Auto Smart Linkage**: The the box or bullet camera automatically performs actions based on predefined smart linkage rules.

5.12 Live View for Thermal Camera

For thermal camera, you can view the fire source information and temperature during live view. You can also measure the temperature manually to get temperature information in the live view image.

5.12.1 View Fire Source Information during Live View

During the live view, you can view the detected fire source information.

Before You Start

Configure the alarm rules for the thermal device, see the user manual of the device for details.

Steps

1. Enter Main View page and start the live view of a thermal camera.

Note

For starting live view, refer to ***Start Live View*** .

2. Right-click on the live view image and select **File Source Information** in the right-click menu to show the list of information types.

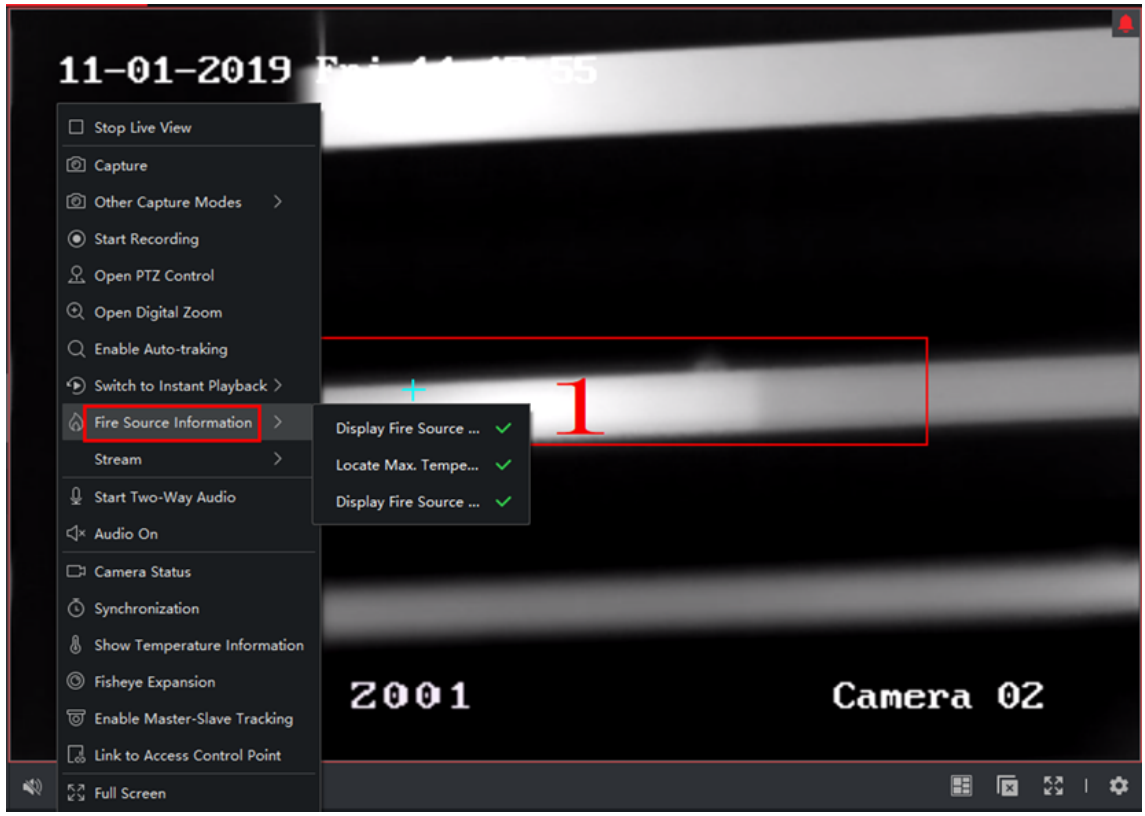


Figure 5-5 View Fire Source Information

3. Select a information type in the list to display the information.

Display Fire Source Region

The region in which the temperature is higher than the configured alarm threshold.

Locate Max. Temperature Region

Mark the region in which the temperature is highest in the fire source region. It is marked in green.

Display Fire Source Target

The distance between the device and fire source.

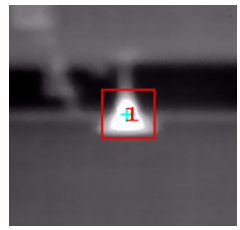


Figure 5-6 Fire Source Information on Live View Image

5.12.2 Show Temperature Information on Live View Image

You can show or hide the real-time temperature information of the monitoring scene when viewing the live video.

Before You Start

- Switch the device VCA source type as **Temperature Measurement + Abnormal Event Detection**.
- Enable the device temperature measurement function and set the temperature measurement rules, see the user manual of the device for details.

Perform this task when you need to show the temperature information on the live view image.

Steps

1. Enter Main View page and start the live view of a thermal camera.

   Note

   For starting live view, refer to ***Start Live View*** .
2. Adjust the scene to the area configured with temperature measurement rule.
3. Right-click on the live view image and select **Show Temperature Information** in the right-click menu.

   The temperature displays on the live view image.
4. Click on the image to view the detailed temperature information.

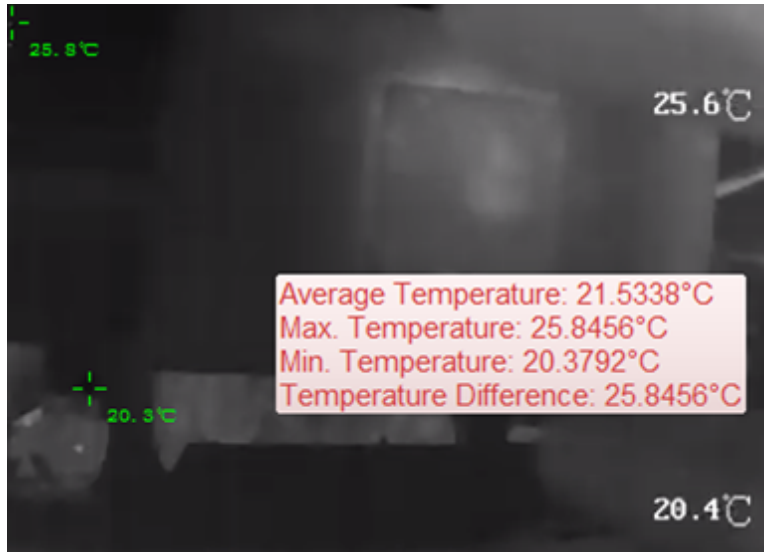


Figure 5-7 Temperature Information on Live View Image

5. **Optional:** Right-click on the live view image and select **Hide Temperature Information** to hide the temperature information.

5.12.3 Manually Measure Temperature

During the live view of thermal camera, you can click anywhere on the live view image to show the temperature of different points to locate the fire resource quickly.

Steps

Note

- The measured temperature will be displayed on the image for 5 seconds.
- Only one point's temperature can be displayed.
- When multiple clients are getting the live video of one camera, if one client adds or deletes the measurement points, other clients' live view will be affected as well. The measurement points will be cleared if all users stop live view of the camera.

1. Enter Main View page and start the live view of a thermal camera.

   Note

   For starting live view, refer to ***Start Live View*** .

2. Right-click on the live view image and select **Show Temperature Information**.
3. Click on the live view image to show the temperature of this position.

   The temperature of the clicked points is shown on the image.

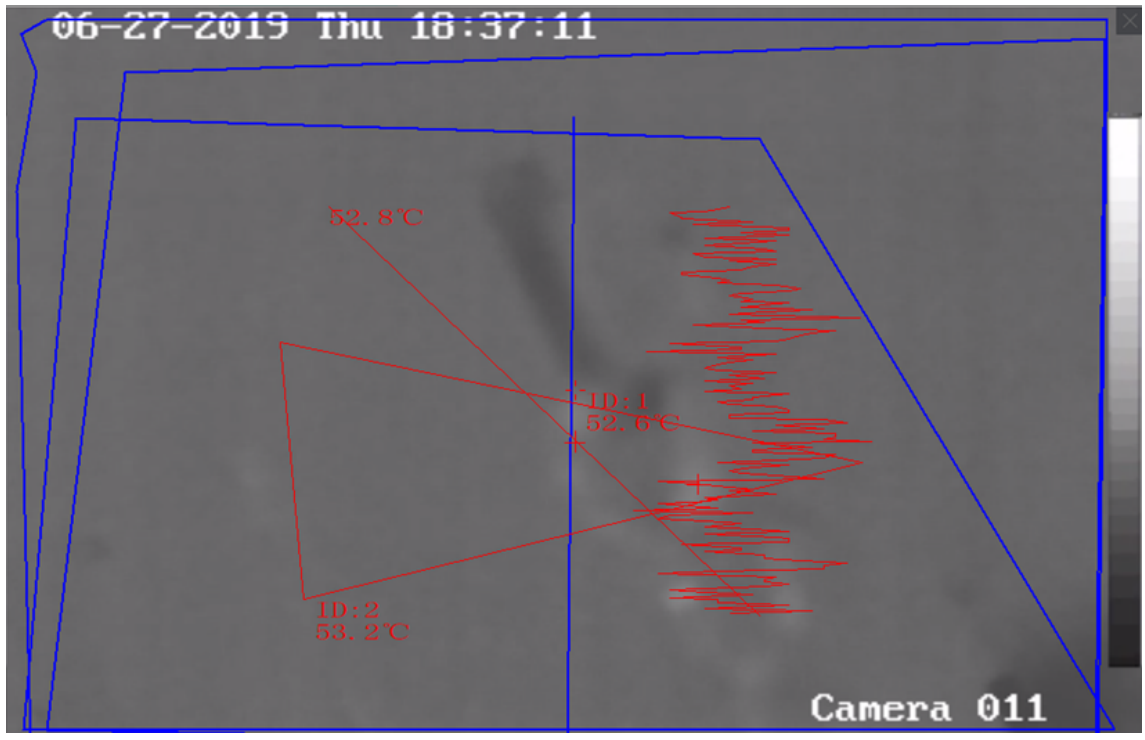


Figure 5-8 Manually Measure Temperature on Points

4. **Optional:** Right-click on the live view image and select **Hide Temperature Information** on the menu.

5.12.4 Display Fire Source Detection Shield Area

Fire source detection shield area is a predefined area that can be shielded from being detected in fire source detection. During live view, you can display the area on the image.

Right-click a live view image and select **Display Shield Area**. The shield area will be displayed on the thermal image of the camera.

Note

- This function needs to be supported by device.
- Make sure you have enabled and configured Fire Source Detection Shield function for the device. See the device user manual for details.



Figure 5-9 Fire Source Shield Area

5.12.5 Display Waste Gas Information

For the device supports waste gas information detection, you can enable **VCA Rule** on the System Configuration page to display the waste gas information during live view.

See ***Set Image Parameters*** for details about how to enable **VCA Rule**.

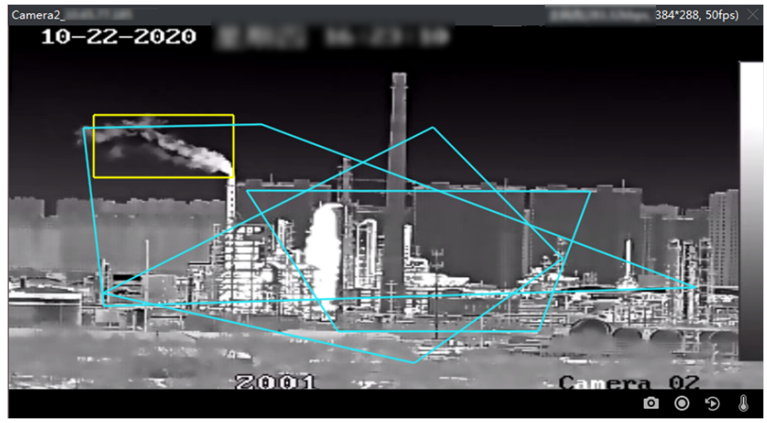


Figure 5-10 Display Waste Gas Information

5.13 Live View in Low Bandwidth

In situation of low network bandwidth, the speed of video streaming might be much slower due to the bandwidth limit. To provide normal quality in less streaming speed for low bandwidth users, the client provides live view in low bandwidth mode. Before that, you need to set the streaming protocol and perform other operations first.

For details about the settings, refer to ***How to get better performance of live view and playback when network bandwidth is low?*** .

5.14 More Functions

This page will introduce the following functions supported in the live view: auxiliary screen preview, digital zoom, channel-zero, two-way audio, camera status, synchronization, and enabling/disabling VCA rules for specific live view windows.

Auxiliary Screen Preview

Display the live video on different auxiliary screens for the convenient preview of multiple monitoring scenes.

Note

Up to 3 auxiliary screens are supported.

Digital Zoom

Drag the mouse to draw a rectangle area in the lower-right/upper-left direction to zoom in or out the drawn area. Or use the mouse wheel to zoom in or out the view in digital zoom mode.

Channel-Zero

For the channel-zero of the device, hold the **Ctrl** key and double-click to display the specific channel. Hold the **Ctrl** key and double-click again to restore.

Two-Way Audio

Two-way audio function enables the voice talk of the camera. You can get not only the live video but also the real-time audio from the camera. If the device has multiple two-way audio channels, you can select a channel to start two-way audio.

Note

- The two-way audio can be used for only one camera at one time.
- Hik-Connect device doesn't support selecting channel during two-way audio.

Camera Status

The camera status, such as recording status, signal status, connection number, etc., can be detected and displayed for checking. The status information refreshes every 10 seconds.

Synchronization

The synchronization function provides a way to synchronize the device clock with the PC which runs the client software.

Set Stream Type

Auto-Change Stream Type

Camera selects stream type according to its display window size. When the window division number is smaller than 9, the stream type will be main stream, otherwise sub stream.

Three ways are provided for setting stream type:

- In the resource list, hover the cursor on a camera's name and click → **Stream** to select a stream type, or click **Auto-Change Stream Type**. Or you can perform this operation for a device group to set stream type for all devices in this group.
- Click in the live view tool bar and select a stream type. See ***Set Icons Shown on Toolbar*** for details about editing tool bar.
- Right-click a live view window and click **Stream** to select a stream type for the camera.

Note

This function needs to be supported by device.

Lock Client in Full Screen Mode

Press **Ctrl** and **L** on your keyboard to lock the client after entering the full screen mode. After locking the client, you will be unable to operate the client including the other windows in the current window division mode. Click **Unlock** on the top and enter the login password for the client and click **Unlock** to unlock the client.

Enable/Disable VCA Rule

To enable/disable VCA rules on specific live view windows, right-click on the windows and select **Enable VCA Rule** or **Disable VCA Rule**.

Note

You can set VCA rules for all live view windows in System Configuration. For details, see ***Set Image Parameters*** .

Audio Broadcast

During the live view, click in the bottom right corner to start speaking to the added IP Speaker (online and currently unoccupied), including emergency broadcast and speak in real time.

Mode	Application Scenario	Operation
Emergency Broadcast	Broadcast real-time speaking about emergency mustering for guiding persons in specific areas to protect themselves.	Click **Emergency Broadcast** to start real-time speaking of emergency contents. Click **Pause Speaking** to pause the broadcast, and click **Resume Speaking** to continue the broadcast.
Speak in Real Time	Broadcast real-time speaking about general issues, such as news broadcast.	Click **Speak in Real Time** to start real-time speaking. Click **Pause Speaking** to pause the broadcast, and click **Resume Speaking** to continue the broadcast.

Chapter 6 Remote Playback

The device records the video according to the recording schedule. You can view the video files stored, to restore the event occurrence process for postmortem analysis and make the further judgment. Storing the valued video footage can provide basic materials for video analysis and video proof. The client supports multiple playback modes, such as: VCA playback, event playback, etc.

Note

There are two playback modes: one is the instant playback in the Main View module (refer to ***Instant Playback*** for details), another one is searching video files and play the video files in the Remote Playback module. In this chapter, we only introduce the playback in the Remote Playback module.

6.1 Flow Chart

Please follow the steps in the following flow chart for playback.

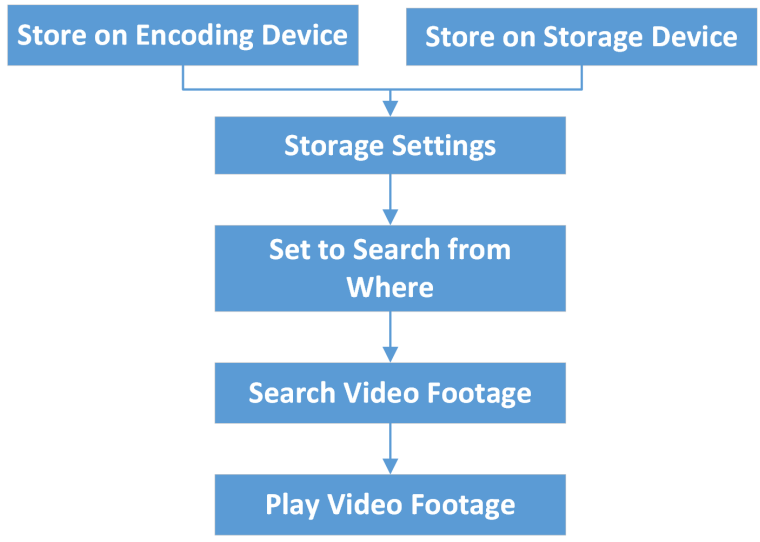


Figure 6-1 Flow Chart of Playback

- **Storage Settings:** Set recording schedule to define when the cameras start recording and where the video footage are stored. For details, refer to ***Remote Storage Configuration*** .
- **Search and Play Video Footage:** Start playback. For details, refer to the contents in this chapter.

6.2 Remote Storage Configuration

The video files and captured pictures can be stored on the HDDs, Net HDDs, or SD/SDHC cards on the local device.

Note

This function should be supported by the device.

6.2.1 Store Picture and Video on DVR, NVR, or Network Camera

Some local devices, including the DVRs, NVRs, and Network Cameras, provide storage devices such as the HDDs, Net HDDs and SD/SDHC cards for video and picture files. You can set a recording schedule or capture schedule for the channels of the local devices.

Perform this task when you need to store the picture and video files on the encoding device such as DVR, NVR, or network camera.

Steps

Note

The pictures captured through the capture schedule are stored on the local device and can be searched on the remote configuration page of the device.

1. Enter the Storage Schedule module.
2. Select the camera in the Camera Group list.
3. Set **Recording Schedule** switch or **Capture Schedule** switch to ON on **Storage on Encoding Device** area to enable device local recording or capture.
4. Select the recording or capture schedule template from the drop-down list.

   All-day Template

   All-day continuous recording.

   Weekday Template

   Working-hours continuous recording from 8:00 AM to 8:00 PM.

   Event Template

   All-day event triggered recording.

   Template 01 to 08

   Fixed templates for specific schedules. You can edit the templates if needed.

   Custom

   Customize a template as you want.

Note

If you need to edit or customize the template, refer to ***Configure Recording Schedule Template*** or ***Configure Capture Schedule Template*** .

5. Click **Advanced** of Recording Schedule to set the recording advanced parameters.

Note

The displayed items vary according to the devices.

Pre-record

Normally used for the event triggered record, when you want to record before the event happens.

Post-record

After the event finished, the video can also be recorded for a certain time.

Keep Video Files for

The time for keeping the video files in the storage device, once exceeded, the files will be deleted. The files will be saved permanently if the value is set as 0.

Redundant Recording

Save the video files not only in the R/W HDD but also in the redundant HDD.

Record Audio

Record the video files with audio or not.

Video Stream

Select the stream type for the recording.

Note

For specific type of devices, you can select **Dual-Stream** for recording both main stream and sub-stream of the camera. In this mode, you can switch the stream type during remote playback. Refer to ***Normal Playback*** for stream switch during playback.

6. Click **Advanced** of Capture Schedule to set the capture advanced parameters.

Resolution

Select the resolution for the continuous or event captured pictures.

Picture Quality

Set the quality for the continuous or event captured pictures.

Interval

Select the interval which refers to the time period between two capturing actions.

Captured Picture Number

Set the picture number for event capture.

7. **Optional:** Click **Copy to...** to copy the recording schedule settings to other channels.
8. Click **Save** to save the settings.

6.2.2 Store Picture and Additional Information on Local PC

You can store the pictures and the additional information, such as the heat map, people counting data, and road traffic data, to the local PC.

Perform this task when you need to store pictures and additional information on local PC.

Steps

1. Enter **Storage Schedule** module.
2. Select the camera in the Camera Group list.

   Note

   This function should be supported by the device.
3. Select storage content.

   Picture Storage

   Store the alarm pictures of the camera when event occurs. You can click **System Configuration → File** to modify the saving path of pictures.

   Additional Information Storage

   Store the additional information (e.g., heat map, people counting data, etc.) on local PC.
4. Click **Save** to save the settings.

6.2.3 Configure Recording Schedule Template

You can edit the recording schedule template, or customize a recording schedule template.

Steps

1. Enter the Storage Schedule module.
2. Open the template settings window.
   - Select **Template 01** to **Template 08** from the drop-down list and click **Edit**.
   - Select **Custom** from the drop-down list.
3. Drag on the time-line to set the time periods for the selected template when the cursor turns to  .

   Continuous

   Normal and continuous recording. The schedule time bar is marked with  .

   Event Recording

   The recording is triggered by event. The schedule time bar is marked with  .

   Command

   The recording triggered by command. The schedule time bar is marked with  .

Note

Command triggered recording is only available for the ATM transactions when the ATM DVR is added to the client.

Note

Up to 8 time periods can be set for each day in the recording schedule.

4. **Optional:** After setting the time periods, you can do one or more of the following:

Move	Drag a time period to move it when the cursors turns to .
Lengthen or Shorten	Select a time period and then lengthen or shorten it when the cursor turns to .
Set Accurate Time	Click a time period to set the accurate start time and end time of the period.
Delete	Select the configured schedule time period and click to delete it.
Delete All	Click to delete all the configured time periods.
Copy to	Select one date and click to copy the date's time period settings to the other dates.

5. **Optional:** For template 01 to 08, you can edit the template name as you want.
6. Click **OK** to save the settings.

Note

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

6.2.4 Configure Capture Schedule Template

You can edit the capture schedule template, or customize a capture schedule template.

Steps

1. Enter the Storage Schedule module.
2. Open the template settings window.
   - Select **Template 01** to **Template 08** from the drop-down list and click **Edit**.
   - Select **Custom** from the drop-down list.
3. Drag on the time-line to set time periods for the selected template when the cursor turns to .

   Continuous Capture

   Normal and continuous capture. The schedule time bar is marked with .

   Event Capture

   The capture is triggered by event. The schedule time bar is marked with .
4. **Optional:** After setting the time period, you can do one or more of the followings

Move	When the cursor turns to , you can move the time period you just edited. You can also edit the displayed time point to set the accurate time period.
Lengthen or Shorten	When the cursor turns to , you can lengthen or shorten the selected time period.
Delete	Select a time period and click to delete it.
Delete All	Click to delete all the configured time periods.
Copy to	Select one date and click to copy the date's time period settings to the other dates.

5. **Optional:** For template 01 to 08, you can edit the template name as you want.
6. Click **OK** to save the settings.

Note

If you select **Custom** to customize a template, you can click **Save as Schedule Template**, and then the custom template can be saved as template 01 to 08.

6.3 Toolbar for Playback

When playing back video on the Remote Playback module, you can operate the tools in the toolbar to implement different functions.

Note

The tools in different playback modes might be different. In this section, the tools in the Camera Playback module will be introduced.

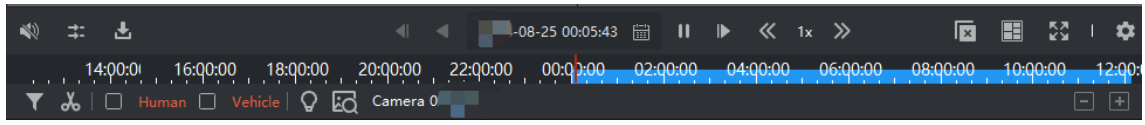


Figure 6-2 Tool for Playback

Table 6-1 Toolbar for Playback

Icon	Icon Name	Descriptions
	Reverse Playback	Play back the video file(s) reversely.
/	Pause/Play	Pause/play the video file(s).
	Close All	Close all the playing video file(s).
	Single Frame(Reverse)	Play the video file(s) by frame reversely.

Icon	Icon Name	Descriptions
	Single Frame	Play the video file(s) by frame.
/	Slow Forward/ Fast Forward	Set the rate of playing, and play back the video file(s) slowly or fast according to the rate.
	Volume	Click this icon to open/close the audio and adjust the volume.
	Clip	Set the start and end time for clipping and download the clipped video file to the local disk.
	Download for Multiple Cameras	Set the start time and end time for multiple cameras and download the video files of multiple cameras simultaneously.
	Window Division	Set the window division.
	Full Screen	Play back video file(s) in full screen. Press ***ESC*** to exit.
/	Asynchronous Playback/ Synchronous Playback	Switch to asynchronous/synchronous playback mode. **Note** For details, refer to ***Synchronous Playback*** .
	Settings	Enter the Video Parameters Settings module, configure the parameters for live view and playback, image, files and toolbar.
	Filter	Filter the video files by the recording type.
	Accurate Positioning	Set the accurate time to play back video file(s).
07/09	Video Date	The date of the playing video file(s) currently. You can switch to play back the video file(s) on the other date quickly. For example, if you switch the date to 07/30, the video will be automatically displayed from 00:00 on July 30 (if there is video at this time).
Human Vehicle	Filter Human or Vehicle Related Video	Check **Human** or **Vehicle** to filter the video with human body detected or vehicle detected. The human or vehicle related video will be remarked in orange on the time bar, and you can quickly locate the video on the time bar.

Icon	Icon Name	Descriptions
		Note This function should be supported by the device, otherwise the **Human** or **Vehicle** is gray and can not be checked.
	Smart Search	You can filter Human or Vehicle related video before searching for recordings with targets via the Region or Line searching mode. 1. Check **Human** or **Vehicle** to filter the video with human body detected or vehicle detected. 2. Follow the guidance during initial use. For details about smart search, see ***VCA Playback*** .
	Target Retrieval (AcuSearch)	Search targets by picture. See ***Search Targets by Picture*** for more information.
Keyboard Control	/	• **Space**: Start or pause playback. • **Left Arrow / Right Arrow**: Rewind or fast forward one frame. For details, see ***Play Video Footage*** .
Privacy Protection	/	Disable privacy protection. Right-click on the image and select **Disable Privacy Protection**. When privacy protection is enabled on the device configuration page, it will apply mosaic blurring (low/medium/high levels) to privacy information in the original stream. When it is disabled on the client, the original stream function must be enabled on the device configuration page to view unblurred recordings. **Note** Privacy protection function should be supported by device. You can go to the remote configuration page of the device to enable privacy protection.

6.4 Normal Playback

You can search video files by camera or group for normal playback and download found video files to local PC. You can also add a tag to mark important video footage, and so on.

You can right-click the playback window to select the required operations from the shortcut menu. Some are listed as follows:

Name	Description
Show/Hide Temperature Information	Show/Hide Temperature Information **Note** The temperature information overlay is only supported by thermal camera.
Tag Control	Add default (the default tag name is TAG) or custom tag (the tag name is customized) for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.
Other Capture Modes	• **Print Captured Picture:** Capture a picture and print it. • **Send Email:** Capture the current picture and then send an Email notification to one or more receivers. The captured picture can be attached. • **Custom Capture:** Capture the current picture. You can edit its name and then save it.

Note

- The Hik-Connect device only supports normal playback and it also does not support the functions of reverse playback, slow forward or fast forward, and adding tag.
- For NVR which is added to the client by device's other user name (except admin), if **Double Verification** is enabled on this NVR, when playing back videos on the client, you are required to enter the user name and password created for double verification. For details about double verification, refer to the user manual of the NVR.

6.4.1 Search Video Footage

You can search the video footage by date, and you can also enter keyword to filter the matched results for normal playback.

Steps

1. Enter the Remote Playback module.
2. Click on the left to enter the Camera Playback page.

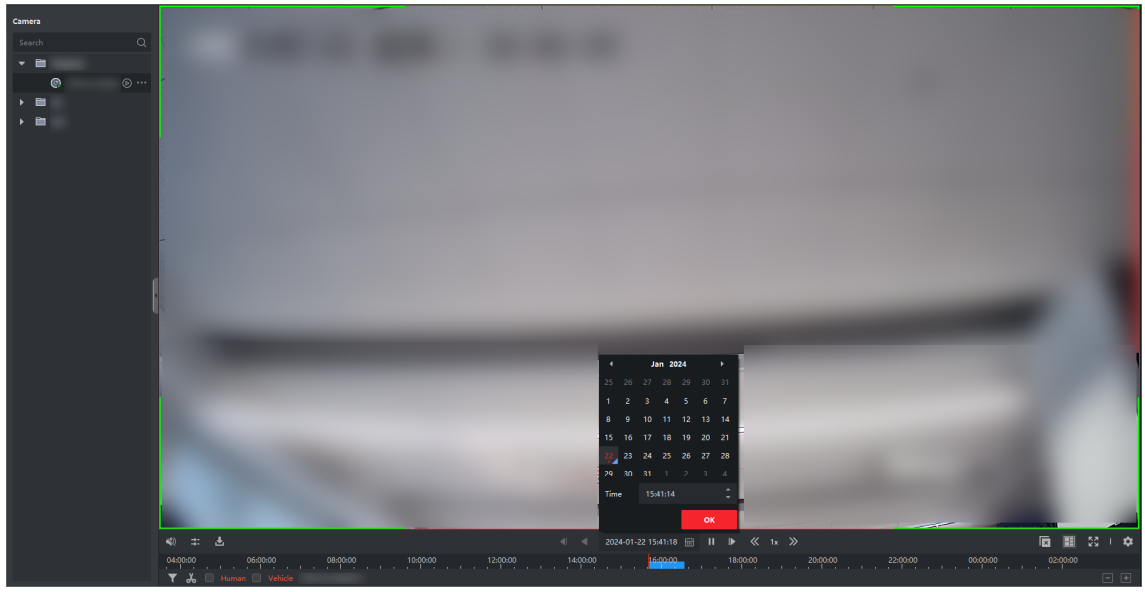


Figure 6-3 Search Video Footage

3. On the left Camera pane, start the playback of camera (s) to search the video footage of the selected camera (s).
   - Drag the camera or group to a display window.
   - Select a display window and double-click the camera or group to start playback in the selected window.
   - Double-click the cameras in turn to select the display window automatically and start playback in the windows.

Note

Up to 16 cameras can be searched simultaneously.

4. **Optional:** On the bottom timeline, click to set the start date and end date of searching time period.

Note

In the calendar, the date which has video footage recorded by schedule will be marked with , and the date which has video footage recorded based on event will be marked with .

6.4.2 Play Video Footage

After searching the video footage for the normal playback, you can play the video via time line.

Steps

1. Search the video footage. For details, refer to ***Search Video Footage*** .
2. Select a date with videos to start playing video and show the timeline after searching the video files.

The video footage will play automatically. You can click on the time line to position the desired video segment of specified time for normal playback.

3. Play video in specified time period by timeline or thumbnails.
   - Drag the timeline forward or backward to position the desired video segment.
   - Move the cursor over the timeline to take a quick view of video thumbnails (if supported by the device) and click the appearing thumbnail to play the specific video segment.

Note

Make sure the device supports this function and you have enable it by clicking in the lower-right corner.



Figure 6-4 Play Video Footage

4. **Optional:** Perform the following operations on the toolbar to control the playback.

Switch Stream Type	Click **Stream → Main Stream / Sub Stream** to switch the stream type for playback according to your actual need.
Scale Up/Down Time Line Bar	Use mouse wheel or click / to scale up or scale down the time line bar.
Single Frame (Reverse)	Click or scroll down the mouse wheel to play the video footage frame by frame (reversely).
Audio Control	Click or to turn off/on the sound. You can also adjust the volume when turning on.
Download for Multiple Cameras	Click to download video footage or captured pictures. **Note** For more details, refer to ***Download for Multiple Cameras*** .

Download Video/ Picture Files by Date	Click to download video footage or captured pictures of the camera by date and time, and store them to local PC. The downloading progress is displayed on the right-upper corner of the page, and you can manually pause downloading.
Keyboard Control	• **Space**: Start or pause playback. • **Left Arrow / Right Arrow**: Rewind or fast forward one frame. For details, see ***Play Video Footage*** .
Disable Privacy Protection	Right-click on the playback image to select **Disable Privacy Protection**. When enabled on the device configuration page, it will apply mosaic blurring (low/medium/high levels) to privacy information in the original stream. When it is disabled on the client, the original stream function must be enabled on the device configuration page to view unblurred recordings. This function should be supported by device.

6.5 Alarm Input Playback

When the alarm input is triggered and the linked video can be searched for alarm input playback. This function requires the support of the connected device.

For the description of the alarm input playback toolbar and right-click menu of display window, refer to ***Normal Playback*** .

Note

Some icons may be not available for alarm input playback.

6.6 Event Playback

The recorded video files triggered by event, such as motion detection, VCA detection, or abnormal event detection, can be searched for event playback. This function requires the support of the connected device.

For the description of the event playback toolbar and right-click menu of display window, refer to ***Normal Playback*** .

Note

Some icons may be not available for event playback.

6.7 ATM Playback

You can search the video files of ATM DVR for ATM playback. This function requires the support of the connected device which is configured with transaction rule.

For the description of the ATM playback toolbar and right-click menu of display window, refer to ***Normal Playback*** .

Note

Some icons may be not available for ATM playback.

6.8 POS Playback

You can search the video files which contain POS information for POS playback. This function requires the support of the connected device which is configured with POS text overlay.

For the description of the POS playback toolbar and right-click menu of display window, refer to ***Normal Playback*** .

Note

Some icons may be not available for POS playback.

6.9 VCA Playback

For the searched video files, you can set VCA rule to find the video footage that VCA event occurs, such as motion detection, line crossing detection, and intrusion detection. This function helps to search out the video that you may be more concerned and mark it with red color.

Before You Start

Make sure the device with VCA function has been installed.

Steps

Note

VCA playback is only supported in a single window, synchronous and asynchronous playback are not supported.

1. Enter the Remote Playback module.
2. Click on the left to enter the Camera Playback page.
3. Select the camera and start the camera's video playback.
4. Enter the VCA Search menu.
   - Right-click the playback window to pop up the shortcut menu, and then click **VCA Search**.
   - Click on the lower-right corner of the playback window.
5. Enable the VCA type, draw the detection region and set the sensitivity.

   Motion Detection

   When the view of the video changes (such as a person passes, the lens is moved), the video footage will be marked as red color on the time line, which is used for the automatic alarm scene or no-guard scene.

Line Crossing Detection

You can draw a virtual line on the video, and the video footage will be marked as red color on the time line when the client bi-directionally detects people, vehicles and other moving objects that cross the virtual line.

Intrusion Detection

You can draw a virtual region on the video, and the video footage will be marked as red color on the time line when there are people, vehicles and other moving objects intruding into the pre-defined region.

VCA Settings

Set the sensitivity and filter the searched video files by setting the target characters. The video footage will be marked as red color on the time line when a person (whose attributes match the setting attributes) occurs in the video.

Note

The higher the sensitivity, the more accurate the matched person is.

6. **Optional:** Click to set the start date and end date of searching time period.
7. Click to search for recordings with targets via the Region or Line searching mode.

   Follow the guidance during initial use. You can check **Human** or **Vehicle** to filter the video with human body detected or vehicle detected.
8. Start the VCA playback.

   The VCA events occurred in the defined area will be red marked on the timeline.

Note

- By default, the playback speed of concerned video will be 1X, and the playback speed of unconcerned video will be 8X.
- You can set to skip the unconcerned video during VCA playback in System Configuration and the unconcerned video won't be played during VCA playback. Refer to ***Set Live View and Playback Parameters*** for details.
- If you need to disable VCA playback, right-click the VCA playback window and click **VCA Search** to disable VCA playback.

6.10 Synchronous Playback

Be default, the client play the video files of multiple cameras in asynchronous playback mode: the playback time of different video files might be different. In synchronous playback, the video files can be played back in synchronization.

Steps

Note

- Video files from up to 16 cameras can be played back simultaneously.
- Synchronous and asynchronous playback are not supported in ATM video playback and VCA playback mode.
- Event video playback and POS video playback only support synchronous playback. To link multiple cameras, enter **Maintenance and Management → Event Management** , enable the linked camera according to event type.

1. Enter the Remote Playback module.
2. Start playback of at least two cameras.
3. Click in the toolbar to enable the synchronous playback.

   The camera under playback will start synchronous playback.
4. Click to disable the synchronous playback.

6.11 Fisheye Camera's Video Playback

When playing back the fisheye camera's video, there might be distortion in the view. To observe the details better, you can enable the fisheye expansion function, to rectify the view as an undistorted view. The client supports multiple fisheye expansion modes, such as: panorama, half sphere, PTZ, fisheye+PTZ mode.

Before You Start
Make sure you have installed Microsoft DirectX component.

Steps

Note

For other playback control instruction, refer to ***Normal Playback*** . Some icons may not be available for fisheye playback.

1. Enter the Remote Playback module.
2. Select a fisheye camera to start playback.

   Note

   For detailed configuration about playback and playback control, refer to ***Normal Playback*** .
3. Enter the Fisheye Expansion mode.
   - Right-click on the display window and select **Fisheye Expansion**.
   - Click in the toolbar. See ***Set Icons Shown on Toolbar*** for details about setting the toolbar.

Note

The mounting type in playback of fisheye expansion is set according to the mounting type in live view. For details, refer to ***Perform Live View in Fisheye Mode***

turns to .

4. Click in the lower-left corner of the display area to select an expanding mode for playback as you desired.

Fisheye

In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called **Fisheye** because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

Panorama / Dual-180° Panorama / 360° Panorama

In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

PTZ

The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

Note

Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

Half Sphere

By the half sphere mode, you can drag the image and rotate it centering on the diameter, in order to adjust the view to the desired angle.

AR Half Sphere

AR half sphere mode overlaps images far and near, so that you can view a dimensional image in a wide angle.

Cylinder

In Cylinder mode, the image is formed into a cylinder page, and you can drag the image to any direction flexibly to view everywhere of the detection area.

5. **Optional:** Right-click on a playing window in the Fisheye view mode and you can switch the selected window to full-screen mode.

Note

You can right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

6.12 Playback in Low Bandwidth

In situation of low network bandwidth, the speed of video streaming might be much slower due to the bandwidth limit. To provide normal quality in less streaming speed for low bandwidth users, the client provides playback in low bandwidth mode. Before that, you need to set the streaming protocol and perform other operations first.

For details about the settings, refer to ***How to get better performance of live view and playback when network bandwidth is low?*** .

6.13 Search Targets by Picture

Search for similar targets by the given picture for target tracking, recognition,crowd flow management, etc.

Steps

1. Enter the Remote Playback page.
2. Double-click the camera to play the video file.
3. Click in the lower left corner for image analysis.
4. Click on the target frame to search.

   Green frames are for faces, blue frames for bodies, and orange frames for vehicles.
5. After jumping to the search results page, you can perform the following operations:
   - Filter: Sort by similarity, time, favorites, etc.
   - Export: Including exporting pictures, exporting current page, and exporting all.
   - View Target Pictures: Click the target picture to view the playback. You can click to conduct a secondary analysis.

6.14 Download Video Footage

During playback, you can download the video files or captured pictures of one camera or multiple cameras to the local PC.

Note

- You can download the video files of the devices added by Hik-Connect.
- For NVR which is added to the client by device's other user name (except admin), if **Double Verification** is enabled on this NVR, when playing back videos on the client, you are required to enter the user name and password created for double verification. For details about double verification, refer to the user manual of the NVR.

6.14.1 Download Video Footage by Date

During playback, you can download the video footage or captured pictures of the camera and save in the local PC.

Steps

1. Enter Remote Playback page and select a camera to start playback.

   Note

   For details about starting playback, refer to ***Remote Playback*** .
2. Right click on the image and click **Download**.
3. **Optional:** Check **Original Stream** to download the original stream video; otherwise, the blurred video will be downloaded.

   The feature should be supported by the device and make sure you have checked it on the **Device Access → Device Configuration → Device Parameter → Privacy Protection → Original Stream Permission → Storage, Forward, and Export** page.
4. **Optional:** Select human or vehicle to download only relevant segments.
5. Set the start and end time of the video footage to download.
6. Enter a name for the video footage.
7. **Optional:** Check off **Download Player** to download the player.
8. **Optional:** Check off **Capture** to download the captured pictures.
9. Click **OK** to download the video footage or captured pictures to the local PC.

   Note

   Video download supports downloading either the original stream or the blurred video. If the original stream video will be downloaded;

6.14.2 Download for Multiple Cameras

During the playback of multiple cameras, you can download the video files and captured pictures of multiple cameras by date simultaneously.

Steps

1. Enter Remote Playback page and select multiple cameras to start playback.

   Note

   For details about starting playback, refer to ***Remote Playback*** .
2. Click to open the Download for Multiple Cameras window.

   All the cameras in playback will be displayed.
3. Select the cameras you want to download video files for.
4. **Optional:** Select human or vehicle to download only relevant segments.
5. Set the start time and end time of video duration for each camera.

You can batch setting the download time. After selecting multiple cameras, adjusting one selected camera's download time will syncs changes to others.

6. **Optional:** Check off **Download Player** to download the player.
7. **Optional:** Check off **Capture** to download the captured pictures.
8. Click **Download** to start downloading videos or pictures to the local PC.
9. **Optional:** Click **Stop** to stop downloading manually.

Note

Up to 16 cameras' video files can be downloaded simultaneously.

Chapter 7 Event Configuration

Event is used to notify security personnel of the particular situation which helps handle the situation promptly. Event can trigger a series of linkage actions (e.g., audible warning and sending email) for notification and event handling. You can enable the event and set linkage action(s) for the resources added to the client. If the selected events happen, the client will receive event notifications in real-time and you can check the details and handle the events accordingly.

Video Event

The video events refer to the special events triggered by video exception, monitoring area's exception, alarm input, encoding device's exception, etc. For more details, refer to ***Configure Event for Camera*** , ***Configure Event for Alarm Input*** , and ***Configure Event for Encoding Device*** .

Access Event

The access control events refer to the special events triggered at the access control devices, doors, card readers, elevators, video intercom devices, etc. For more details, refer to ***Configure Client Actions for Access Event*** .

Security Control Event

The security control events refer to the special events triggered by the zones of the security control panels. For more details, refer to ***Configure Client Linkage for Zone Event*** .

AI Open Platform Event

The AI open platform event refers to the event triggered by the AI model package on the device. For more details, refer to ***Configure Platform Event*** .

7.1 Configure Event for Camera

The event for camera refers to the video exception or the events detected in the monitoring area of the camera, such as motion detection, video loss, line crossing, and so on. You can enable an event for the cameras in the client. When the event is triggered on the camera, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration → Video Event → Camera** .

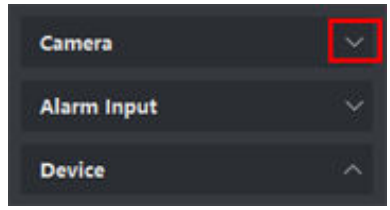


Figure 7-1 Display Camera Resource

2. Unfold the group and select a camera as event source.

Note

Make sure the resource is online.

All the event types supported by the selected camera will appear.

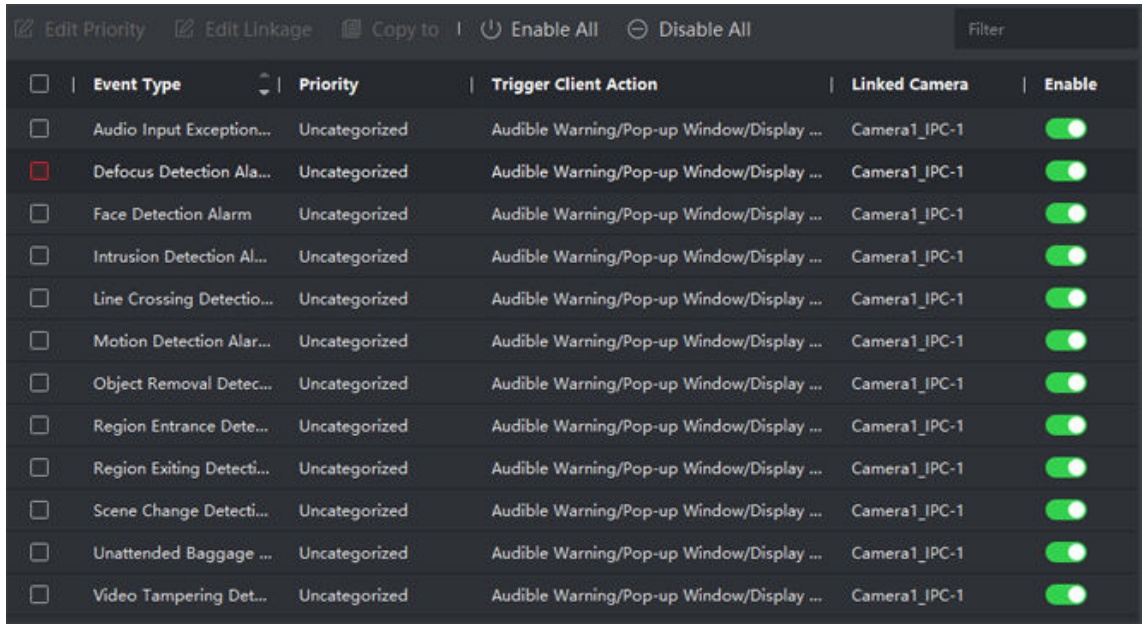


Figure 7-2 Configure Events for Camera

3. **Optional:** Enter keywords in **Filter** field to locate the desired event quickly.
4. **Optional:** Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this camera.

Note

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. **Optional:** Select the event(s), and then perform the following operations.

Edit Priority

Click **Edit Priority** to set the priority of the event(s).

Priority represents the emergency degree of the event.

Edit Event Linkage

Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera) on the client when the event is triggered. You can also enter remarks about how to the handle the event.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with twinkling aside when the event is triggered, which helps security personnel view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture or record video when the event is triggered.

Note

Up to 4 cameras can be selected.

Broadcast Linkage

Link the selected camera to broadcast certain audio file(s) when the event is triggered.

Note

Up to 100 speaker units, and up to 5 audio files can be selected.

PTZ Linkage

When the events are triggered, the cameras' **Preset**, **Patrol**, and **Pattern** will be called.

Note

Make sure you have configured presets, patrols, or patterns for the camera.

Alarm Output Linkage

The activation of an event will cause the connected alarm outputs (Max: 8) to activate, generating sounds, flashes, etc.

Access Point Linkage

When events are triggered, actions including Unlock Door, Lock Door, Remain Open, or Remain Closed are performed at the linked access points.

Copy Event Settings Click **Copy to** to copy the event settings of this camera to other camera(s).

Note

You can only copy the event settings to the resource(s) of the same type.

What to do next

You need to arm the device which the camera belongs to, otherwise the client cannot receive the configured events. For details, see ***Enable Receiving Event from Devices*** .

7.2 Configure Event for Alarm Input

The event for alarm input refers to the event triggered by alarm input. You can enable an event for the alarm inputs in the client. When the alarm input is triggered, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration → Video Event → Alarm Input** .

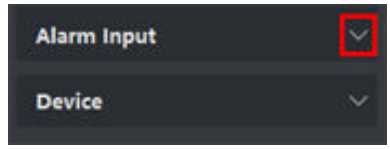


Figure 7-3 Display Alarm Input Resource

2. Unfold the group and select an alarm input as event source.

Note

Make sure the resource is online.

All the event types supported by the selected alarm input will appear.

3. **Optional:** Enter keywords in **Filter** field to locate the desired event quickly.
4. **Optional:** Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this alarm input.

Note

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. **Optional:** Select the event(s), and then perform the following operations.

Edit Priority Click **Edit Priority** to set the priority of the event(s).

Priority represents the emergency degree of the event.

Edit Event Linkage

Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Pop-up Window

Pop-up window to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera) on the client when the event is triggered. You can also enter remarks about how to the handle the event.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with twinkling aside when the event is triggered, which helps security personnel view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture picture or record video when the event is triggered.

Note

Up to 4 cameras can be selected.

Broadcast Linkage

Link the selected camera to broadcast certain audio file(s) when the event is triggered.

Note

Up to 100 speaker units, and up to 5 audio files can be selected.

PTZ Linkage

When the events are triggered, the cameras' **Preset**, **Patrol**, and **Pattern** will be called.

Note

Make sure you have configured presets, patrols, or patterns for the camera.

Alarm Output Linkage

The activation of an event will cause the connected alarm outputs (Max: 8) to activate, generating sounds, flashes, etc.

Access Point Linkage

When events are triggered, actions including Unlock Door, Lock Door, Remain Open, or Remain Closed are performed at the linked access points.

Copy Event Settings

Click **Copy to** to copy the event settings of this alarm input to other alarm input(s).

Note

You can only copy the event settings to the resource(s) of the same type.

What to do next

You need to arm the device which the alarm input belongs to, otherwise the client cannot receive the configured events. For details, see ***Enable Receiving Event from Devices*** .

7.3 Configure Event for Encoding Device

The event for encoding device refers to encoding device's exception, such as device offline. You can enable an event for the encoding devices added in the client. When the event is triggered on the device, the client can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event Configuration → Video Event → Device** .

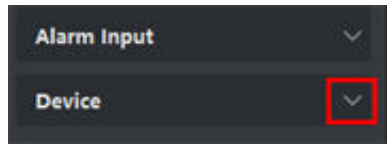


Figure 7-4 Display Device Resource

2. Select a device as event source.

Note

Make sure the resource is online.

All the event types supported by the selected device will appear.

3. **Optional:** Enter keywords in **Filter** field to locate the desired event quickly.

4. **Optional:** Turn on the switch on the Enable column to enable the event type, or click **Enable All** to enable all the event types of this device.

Note

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or disable all event types.

5. **Optional:** Select the event(s), and then perform the following operations.

Edit Priority

Click **Edit Priority** to set the priority of the event(s).

Priority represents the emergency degree of the event.

Edit Event Linkage

Click **Edit Event Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Broadcast Linkage

Link the selected camera to broadcast certain audio file(s) when the event is triggered.

Note

Up to 100 speaker units, and up to 5 audio files can be selected.

PTZ Linkage

When the events are triggered, the cameras' **Preset**, **Patrol**, and **Pattern** will be called.

Note

Make sure you have configured presets, patrols, or patterns for the camera.

Alarm Output Linkage

The activation of an event will cause the connected alarm outputs (Max: 8) to activate, generating sounds, flashes, etc.

Access Point Linkage

When events are triggered, actions including Unlock Door, Lock Door, Remain Open, or Remain Closed are performed at the linked access points.

Copy Event Settings

Click **Copy to** to copy the event settings of this device to other device(s).

Note

You can only copy the event settings to the resource(s) of the same type.

What to do next

You need to arm this device, otherwise the client cannot receive the configured events. For details, see ***Enable Receiving Event from Devices*** .

Chapter 8 Event Center

The event information (for example, device offline) received by the client displays. In the Event Center, you can check the detailed information of the real-time and historical events, view the event linked video, handle the events, and so on.

Before the client can receive the event information from the device, you need to enable the events of the resource and arm the device first. For details, refer to ***Event Configuration*** and ***Enable Receiving Event from Devices*** .

Before the you can view the pop-up alarm information, you need to enable event triggered pop-up image in the event center. For details, refer to ***View Pop-up Event Information*** .

8.1 Enable Receiving Event from Devices

Before the client software can receive event notifications from the device, you need to arm the device first.

Steps

1. Click → **Tool** → **Device Arming Control** to open Device Arming Control page.

   All the added devices appear on this page.
2. **Optional:** If there are to many devices, enter the key words in Filter filed to filter the device(s) you want.

   Note

   For the filtered devices, you can click **Arm All** or **Disarm All** to enable receiving event of these devices.
3. In the Auto-Arming column, turn on the switch to enable auto-arming.

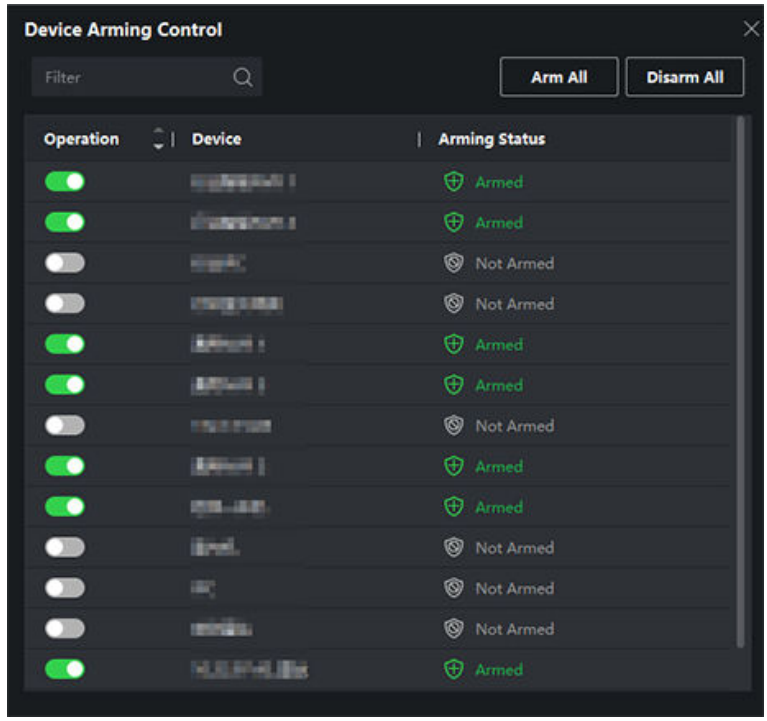


Figure 8-1 Arm Device

After turned on, the device(s) will be armed. And notifications about the events triggered by the armed device(s) will be automatically sent to the client software in real-time.

8.2 View Real-Time Events

The real-time event information received by the client of the connected resources are displayed. You can check the real-time event information, including event source, event time, and priority.

Before You Start

Enable receiving events from devices before the client can receive event from the device, see ***Enable Receiving Event from Devices*** for details.

Steps

1. Click **Event Center → Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

   Event Time

   For encoding device, event time is the client time when it receives the event. For other device types, event time is the time when the event is triggered.

   Priority

   Priority represents the emergency degree of the event.
2. Filter the events.

Filter by Device Type and (or) Priority	Select device type(s) and (or) priorities to filter events.
Filter by Keywords	Enter the keywords to filter the events.

3. **Optional:** Right-click the table header of the event list to customize the event related items to be displayed in the event list.
4. Select an event in the event list to view the event details.

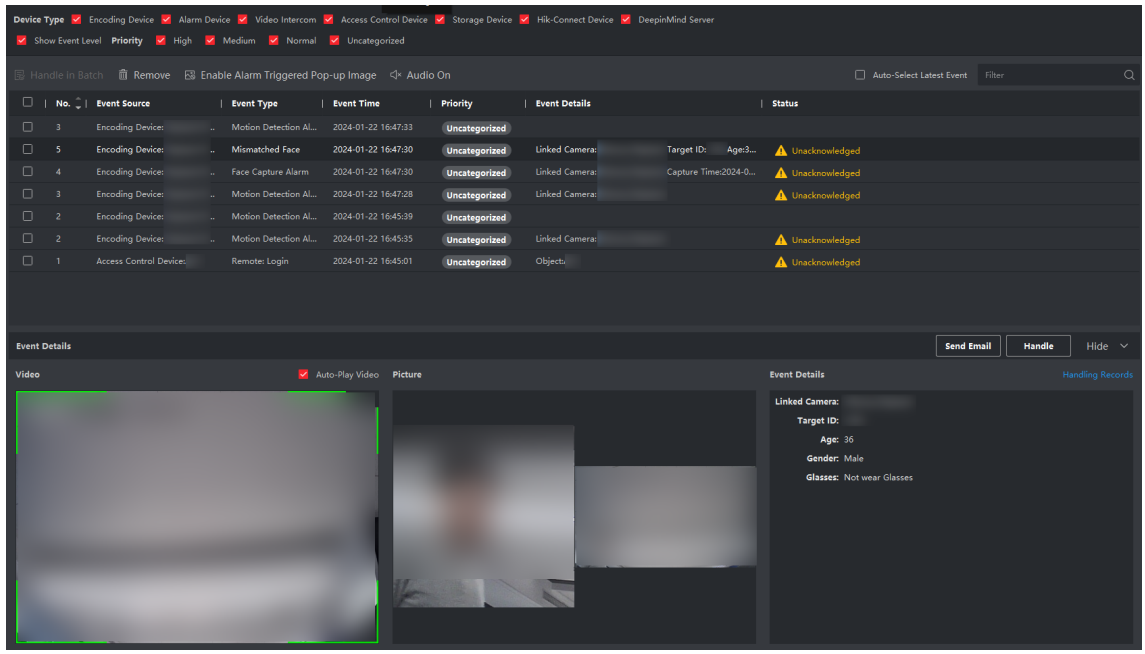


Figure 8-2 Real-Time Events

Note

When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details in Event Center. For details about **Save Pictures in Structure Data Format**, refer to ***Set General Parameters*** .

Note

- The event details include the captured picture(s), video (recorded video triggered by the event or live view of the device), and other event descriptions.
- To view the recorded video triggered by the event, you should link camera(s) with the device in event configuration. For details, refer to ***Event Configuration*** .
- On the Details pane, click **Handling Records** to view the handling records about the selected event.
- To view the captured picture(s), you need to configure picture storage in storage schedule.

5. **Optional:** Perform the following operations if necessary.

Handle Single Event	Click **Handle** to enter the processing suggestion, and then click **OK**.

	Note After an event is handled, the **Handle** button will become **Add Remark**. Click **Add Remark** to add more remarks for this handled event.
Handle Events in a Batch	Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **OK**.
Enable/Disable Alarm Audio	Click **Audio On**/**Mute** to enable/disable the audio of the event.
Select the Latest Event Automatically	Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.
Remove Events	Select the event(s) you want to remove from the list, and click **Remove**. You can search for the removed event(s) in the Event Search module.
Import to Self-Learning Library	Click **Import to Self-Learning Library**, the false alarm picture will be automatically imported into the self-learning library of front-end device or back-end device to avoid false alarms of line crossing detection and intrusion detection.
	Note This function should be supported by the device.
Send Email	Select an event and then click **Send Email**, and the information details of this event will be sent by email.
	Note You should configure the email parameters first, see ***Set Email Parameters*** for details.
Auto-Play Video	Check **Auto-Play Video** to automatically play video when displaying event details.
Enlarge Video or Picture	• Double click the video image to view video in a larger window. • Put the cursor on the picture, and click to view picture in a larger window.
Download Captured Picture	Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC.
Download Event Triggered Video	Hover the cursor on the recorded video, click to download the video (30s before the event happens) triggered by the event.

Enable/Disable Alarm Triggered Pop-up Image	If it is enabled, a window will pop up when the event happens, showing the event information, related pictures, and related videos.

8.3 Search Historical Events

You can search and view historical events by setting search conditions such as time, device type, and priority in the client. For the searched events, you can handle and export them.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see ***Enable Receiving Event from Devices*** for details.

Steps

1. Click **Event Center → Event Search** to enter the event search page.
2. Set the filter conditions to display the required events only.

Time

The time when the event starts.

Search by

Device

Search the events by device or the device's resource channels. If searched by device, you need to set the followings:

- **Device Type**: Select the device from which you want to search events.
- **Include Sub-Node**: Search the events of the device and all resource channels.

Group

Search the events by resource channels in the group.

Note

- For video intercom device, select **Search Scope**: All and Locking Log.
- For access control device, click **Show More** to set more conditions: status, event type, card reader type, person name, employee No., card No., and organization.

Priority

The priority including low, medium, high and uncategorized which indicates the emergency degree of the event.

Event Type

Select one or more event types to be searched from the drop-down list.

Note

You can enter a key word (supports fuzzy search) in the search box to search the target event type(s).

Status

The handling status of the event.

Search by Keyword

Enter a key word (supports fuzzy search) to quickly search the target historical event(s). For example, you can enter a person's name to search the events related with this person.

3. Click **Search** to search for events according the conditions you set.

Note

When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details field in Event Center. For details about **Save Pictures in Structure Data Format**, refer to ***Set General Parameters*** .

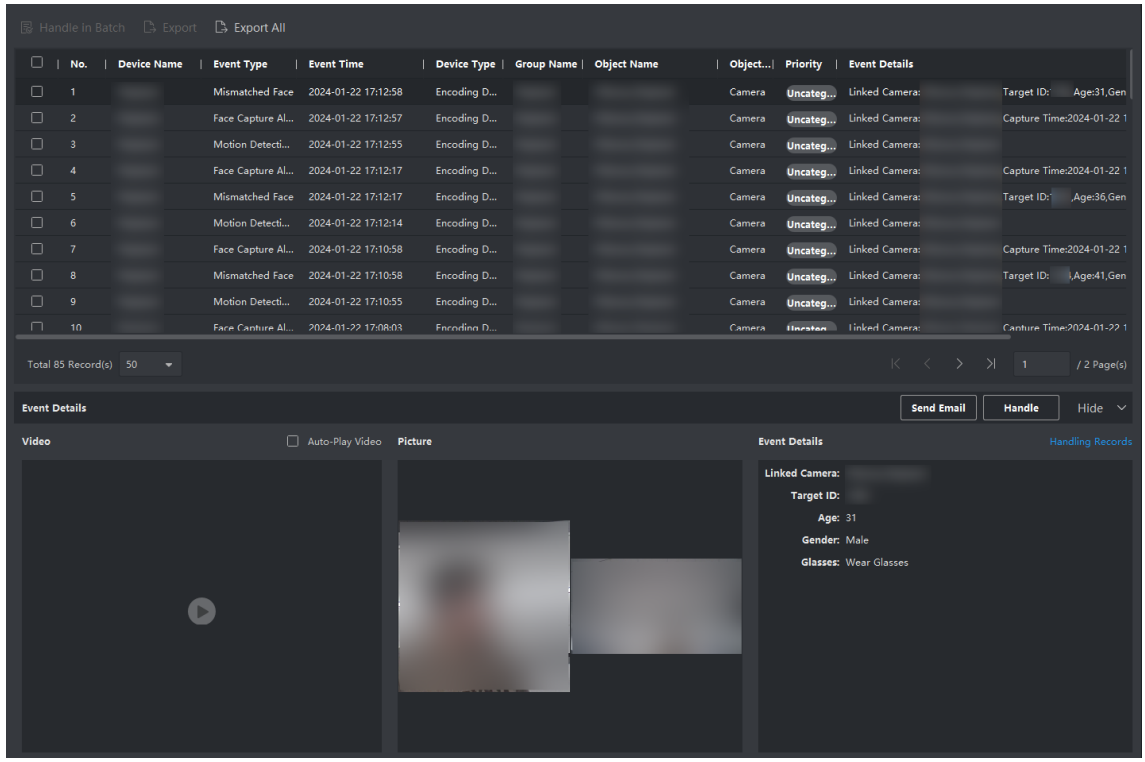


Figure 8-3 Search Historical Events

4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.
5. Select an event in the event list to view the event details.

Note

- The event details include the captured picture(s), video (recorded video triggered by the event or live view of the device), and other event descriptions.
- To view the recorded video triggered by the event, you should link camera(s) with the device in event configuration. For details, refer to ***Event Configuration*** .
- On the Details pane, click **Handling Records** to view the handling records about the selected event.
- To view the captured picture(s), you need to configure picture storage in storage schedule.

6. **Optional:** Perform one of the following operations.

Handle Single Event	Select one event that needs to be handled, and then click **Handle** in the event information details page, and enter the handling suggestion. **Note** After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.
Batch Handle Events	Select the events which need to be handled, and then click **Handle in Batch**, and enter the handling suggestion. **Note** After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.
Auto-Play Video	Check **Auto-Play Video** to automatically play video when displaying event details.
Enlarge Video or Picture	• Double click the video image to view video in a larger window. • Put the cursor on the picture, and click to view picture in a larger window.
Import to Self-Learning Library	Click **Import to Self-Learning Library**, the false alarm picture will be automatically imported into the self-learning library of front-end device or back-end device to avoid false alarms of line crossing detection and intrusion detection. **Note** This function should be supported by the device.
Send Email	Select an event and then click **Send Email**, and the information details of this event will be sent by email.

Note

You should configure the email parameters first, see ***Set Email Parameters*** for details.

Export Event Information	Click **Export** to export the event log or event pictures to the local PC in CSV/Excel file. You can set the saving path manually.
Download Captured Picture	Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC.
Download Event Triggered Video	Hover the cursor on the recorded video, click to download the video (30s before the event happens) triggered by the event.

8.4 Get Events from Device

For some scenarios (e.g., the client cannot start up, access control device has been armed by other client, etc.), the events received by the client and triggered on access control device are not consistent. You can get events from device remotely to synchronize the events from device to Event Center of the client.

Click **Device Management → Device → Device** , select access control device(s), and click **Get Events from Device**.

Synchronize the events by the two ways:

- **Online**: When the device is online and the device can communicate with client at real time, you can select **Online** and set the start time and end time to get the events during this period.
- **Encrypted file**: If the network is not good or the device cannot communicate with the client at real time, you can export the event file from the selected device firstly, and import this exported file on the client later by selecting **Encrypted file** and entering the password of the encrypted file.

  Note

  - For data security, you should encrypt the file when exporting on the device. Meanwhile, the selected access control device should be the one you exported the file from.
  - The function should be supported by the device.

- **Unencrypted file**: If the network is not good or the device cannot communicate with the client at real time, you can export the event file from the selected device firstly, and import this exported file on the client later by selecting **Unencrypted file**.

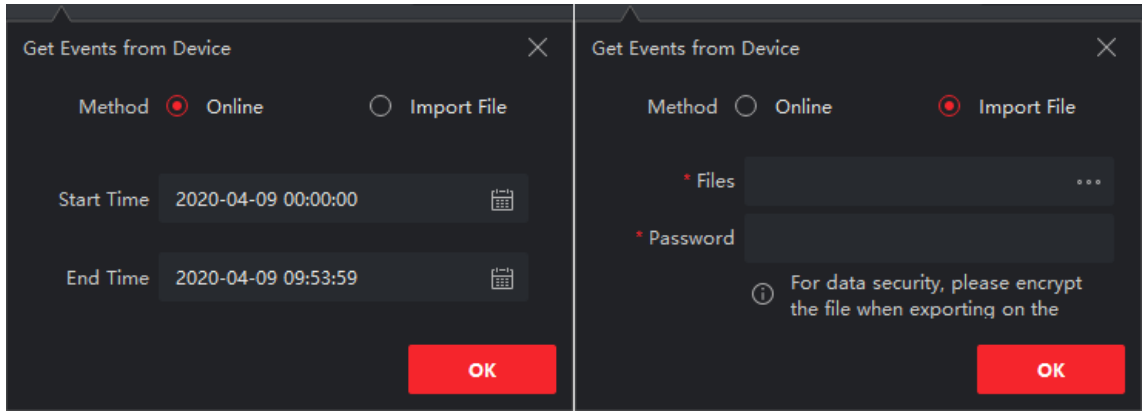


Figure 8-4 Get Events from Device

Note

If you want to get the events related with attendance only, you can also enter **Time & Attendance → Attendance Statistics → Attendance Records** , click **Get Events from Device** and select **Online** or **Import File** to get the events.

8.5 View Pop-up Event Information

If you have enabled event notification and set Event Triggered Pop-up Image as its linkage action, a window will pop up when the event happens, showing the event information, related pictures, and related videos.

Go to **Event Center → Real-Time Event** , and then click **Enable Alarm Triggered Pop-up Image** to enable the function.

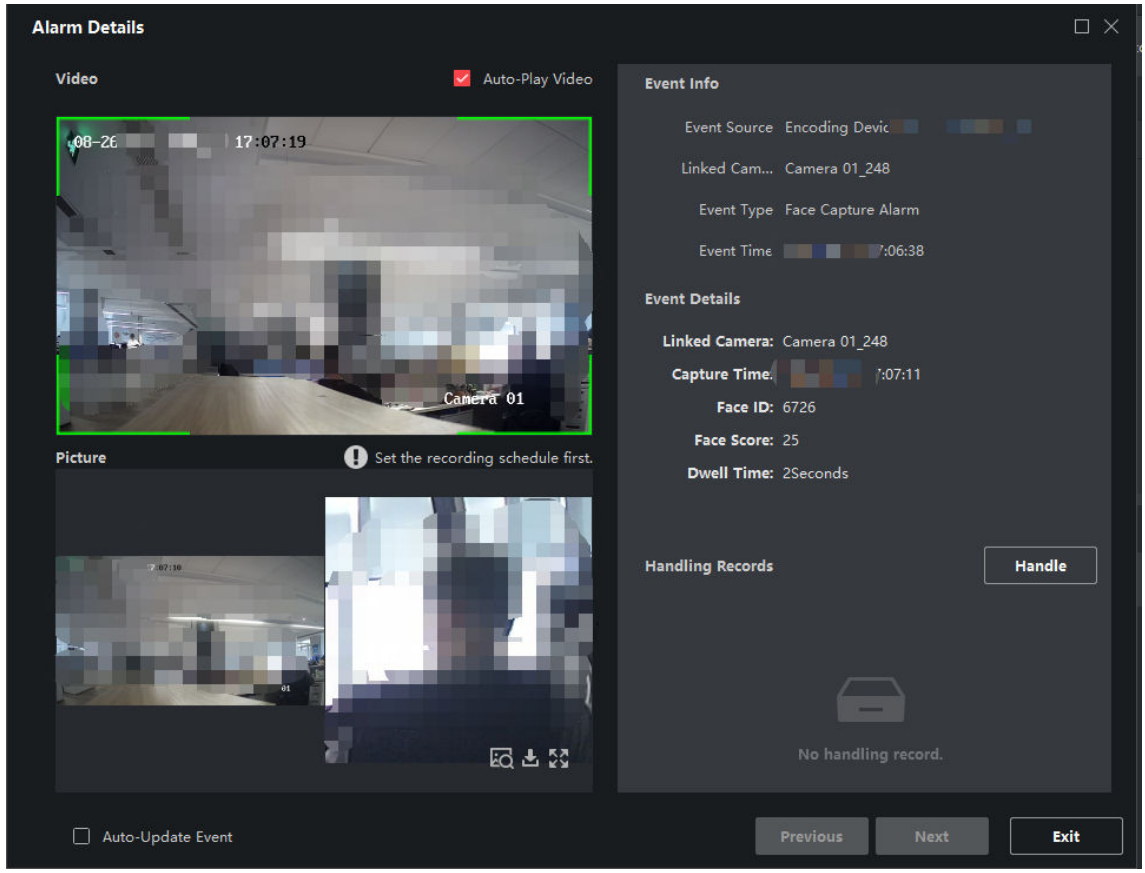


Figure 8-5 The Pop-up Event Information

You can view the event related video footage (from 30 s before the event to the end of the event), the picture captured when the event happens, as well as the event details such as event source, linked camera, event type, etc.

Note

- When the window is not closed, you should click **Next** to view the new event information if a new event is triggered.
- If you haven't clear the event information, you can click **Previous** to view the previous event information.
- When **Save Pictures in Structure Data Format** is enabled, pictures will not be displayed in the event information. See ***Set General Parameters*** for more details.

Click to search targets by picture. See ***Search Targets by Picture*** for more information.

You can check **Auto-Update Event** to enable the window to automatically switch to the latest event information when a new event is triggered.

Chapter 9 Map Management

The E-map function gives a visual overview of the locations and distributions of the installed cameras and alarm input devices. You can get the live view of the cameras on the map, and you will get a notification message from the map when alarm is triggered.

E-map is a static image (it do not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras and alarm inputs, and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

9.1 Add Map

You should add a map as the parent map for the hot spots and hot regions.

Steps

Note

Only one map can be added to one group.

1. Open the E-map page.
2. Select a group for which you want to add a map.

   Note

   For details about setting the group, refer to ***Group Management*** .
3. Click **Add Map** to open the map adding window.
4. Enter a descriptive name of the added map.
5. Select a map picture from the local path.

   Note

   The picture format of the map can only be PNG, JPEG or BMP.
6. Click **OK**.
7. **Optional:** Perform the following tasks after adding the map.

Zoom in/out	Use the mouse wheel or click + or - to zoom in or zoom out on the map.
Adjust Map Area	Drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.

9.2 Edit Map Scale

The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground. An accurate map scale is essential for defining radar's monitoring range.

Before You Start

Make sure you have added a map. See ***Add Map*** for details.

Perform this task if you need to add a security radar to the map.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Map Calibration → Edit Scale** to select two locations on the map.

   The cursor will turn to if you hover it on the map.

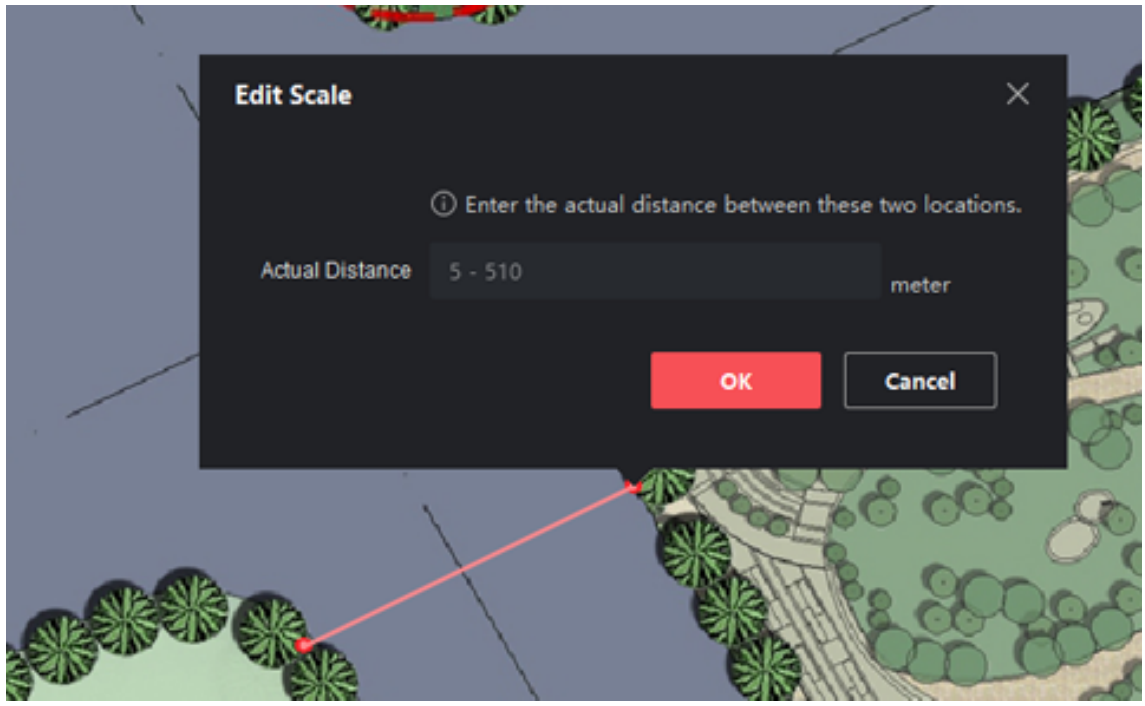


Figure 9-1 Edit Map Scale

4. Click on the map to select two locations.

   The Edit Scale window pops up.
5. Enter the ground distance between the two locations, and then click **OK**.

   The client will calculate the map scale automatically.

9.3 Longitude and Latitude Calibration

After calibrating the longitude and latitude of two points on the E-map, you can drag the radar in the group to the E-map. The radar will automatically move to the correct position on the E-map according to the longitude and latitude calibrating result.

Before You Start

1. Make sure you have added radar on the Client. For details, refer to ***Add Single or Multiple Online Devices*** .
2. Make sure you have set the longitude and latitude parameters of the radar by web browser.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Map Calibration → LongitudeLatitude Calibration** .
4. Click **Add Calibration Point**.
5. Click a point on the map, enter the longitude and latitude of the point in the pop-up window, and then click **Save**.
6. Click **Add Calibration Point** and repeat the previous step to add the second calibration point.
7. Drag the radar in the left resources group to the map.

   The radar will automatically move to the correct position on the map according to the longitude and latitude of two points calibration.

9.4 Manage Hot Spot

The devices added to the map are called hot spots. The hot spots show the locations of the devices, and you can also get the live view or alarm information of the monitoring scenarios through the hot spots.

9.4.1 Add Camera as Hot Spot

You can add cameras to the map as hot spots.

Before You Start

Make sure you have added an e-map and a camera to the client. See ***Add Map*** and ***Device Management*** for details.

Steps

1. Enter the E-map page.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot → Camera Hot Spot** to open the Add Hot Spot window.

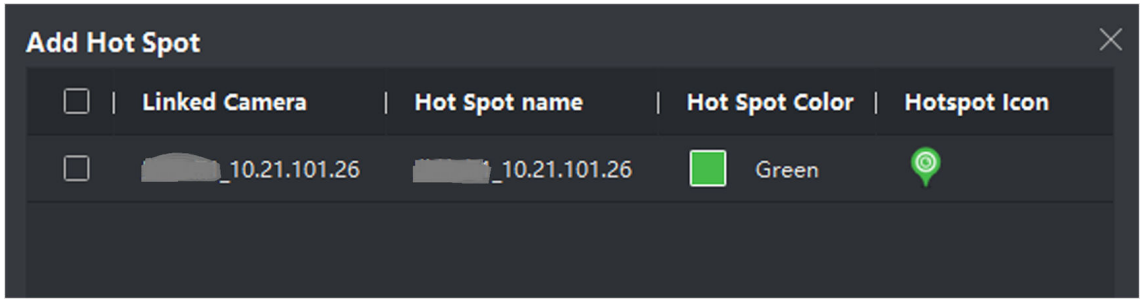


Figure 9-2 Add Hot Spot Panel

4. Select the cameras to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color and select the hot spot icon.
6. Click **OK** to save the settings.

Note

You can also drag the camera icons from the group list to the map directly to add the hot spots.

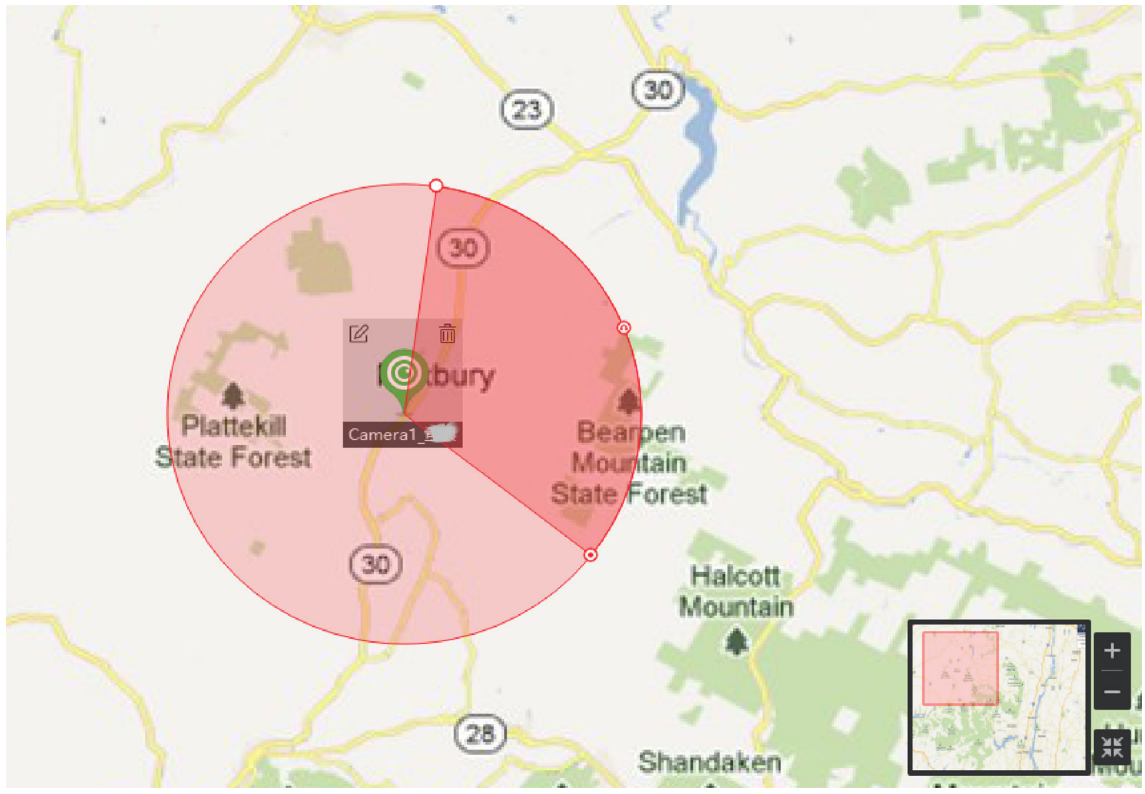


Figure 9-3 Camera on the Map

The camera icons are added on the map as hot spots and the icons of the added cameras in the group list change from to . The sector indicates the camera's field of view.

7. Perform the following operation(s).

Move the Hot Spot	Drag the hot spot to move it to a certain position.
Change the FOV Angle	Drag / and revolve to change the camera's field of view.
Change the FOV Size	Drag to change the FOV size.

9.4.2 Add Alarm Input as Hot Spot

You can add the alarm inputs to the map as hot spots.

Steps

1. Enter the E-map module.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Click **Add Hot Spot → Alarm Input Hot Spot** to open the Add Hot Spot window.
4. Select the alarm inputs to be added to the map.
5. **Optional:** Edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

Note

You can also drag the alarm input icons from the group list to the map directly to add the hot spot.

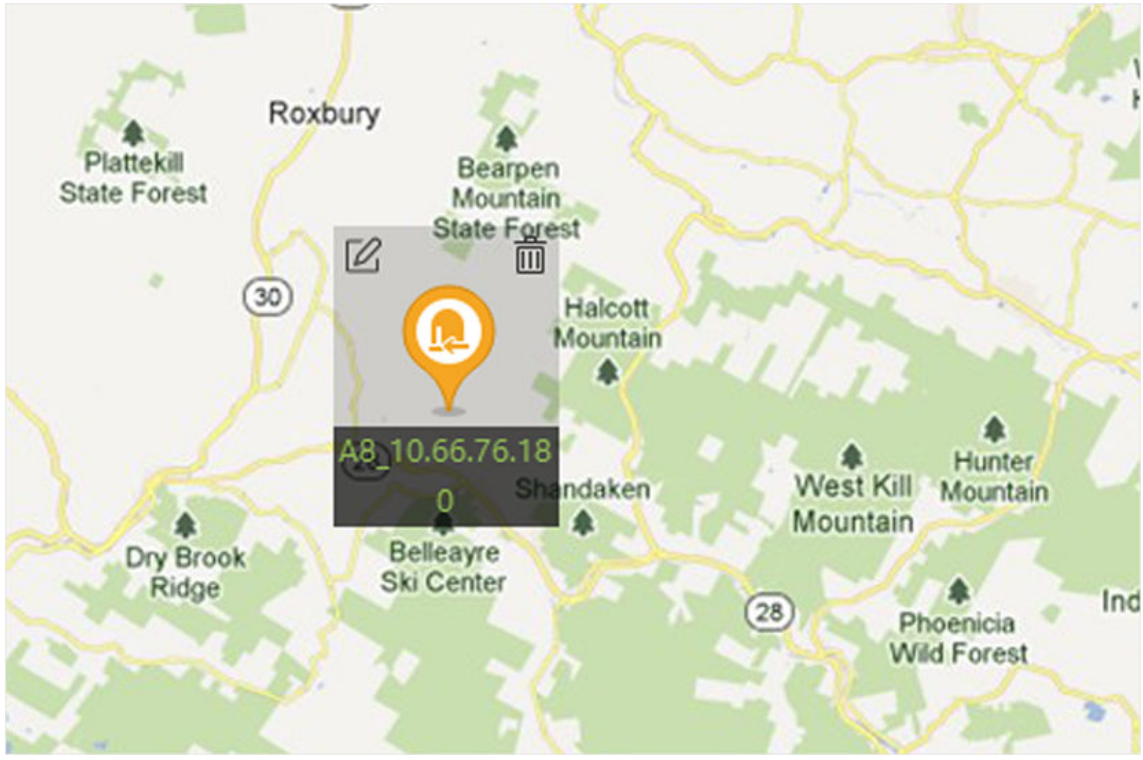


Figure 9-4 Alarm Input on the Map

The alarm input icons are added to the map as hot spots and the icons of the added alarm inputs in the group list change from to .

7. **Optional:** Drag the hot spot to move it to a certain position.

9.4.3 Add Alarm Output as Hot Spot

You can add alarm outputs to the map as hot spots for management. After that, you can enable or disable it in a quick manner. If you enable an alarm output on the map, the security control devices (e.g. sirens, bells) connected to it will alarm for attention.

Before You Start

Make sure you have added an e-map and alarm output to the client. See ***Add Map*** and ***Device Management*** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot → Alarm Output Hot Spot** to open the Add Hot Spot panel.

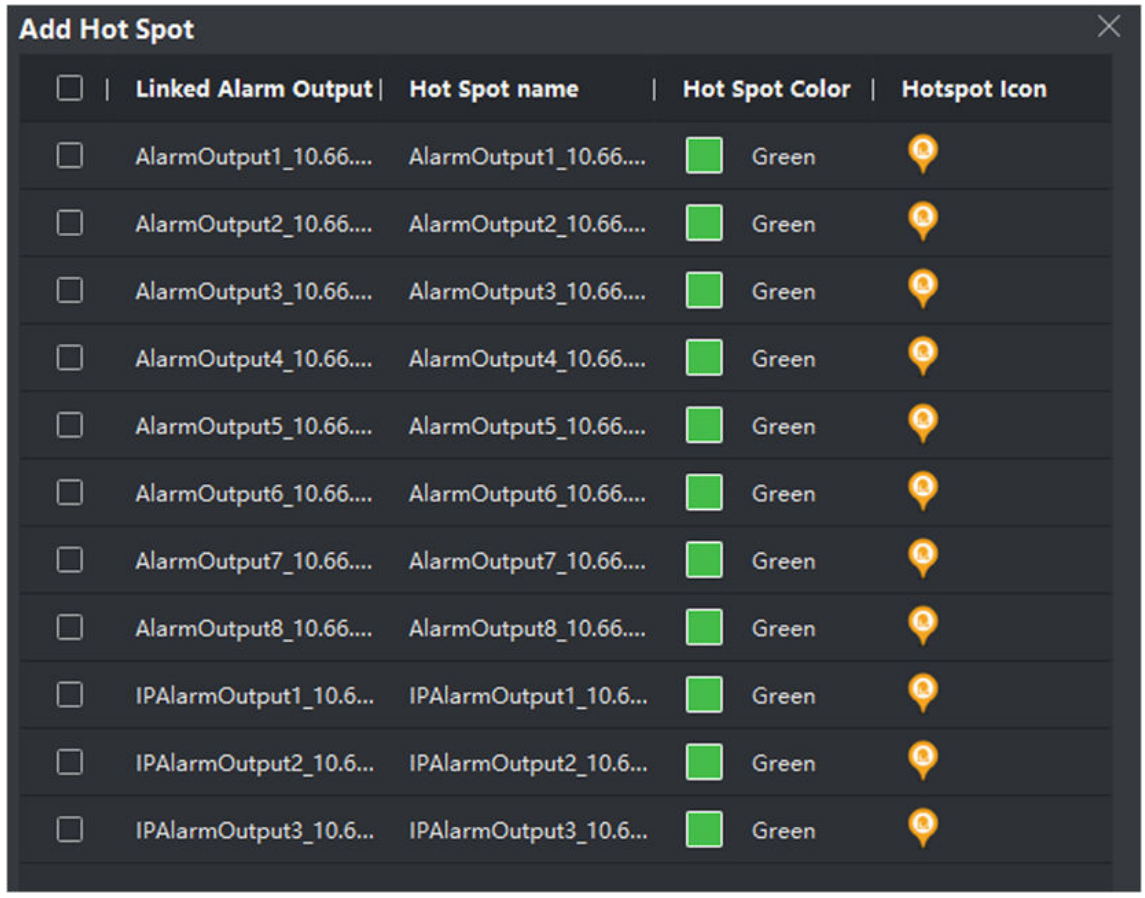


Figure 9-5 Add Hot Spot Panel

4. Select the alarm output to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

Note

You can also drag an alarm output icon from the alarm output list to the map to add the hot spot.

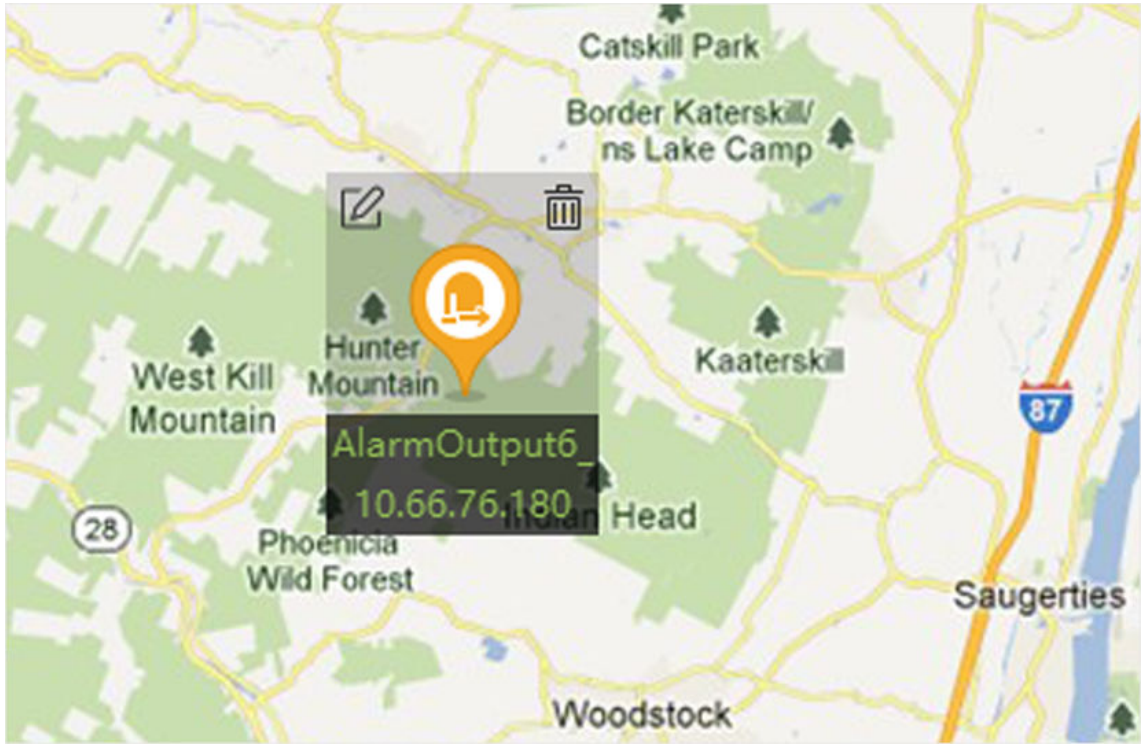


Figure 9-6 Alarm Output on the Map

The alarm output is added to the map as a hot spot and its icon in the group list changes from to .

7. **Optional:** Drag the alarm output to move it to a certain position.

9.4.4 Add Zone as Hot Spot

You can add zones to the map so that you can quickly locate the zone when an alarm is triggered.

Before You Start

Make sure you have added a map and zone to the client. See ***Add Map*** and ***Add Device*** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot → Zone Hot Spot** to open the Add Hot Spot panel.

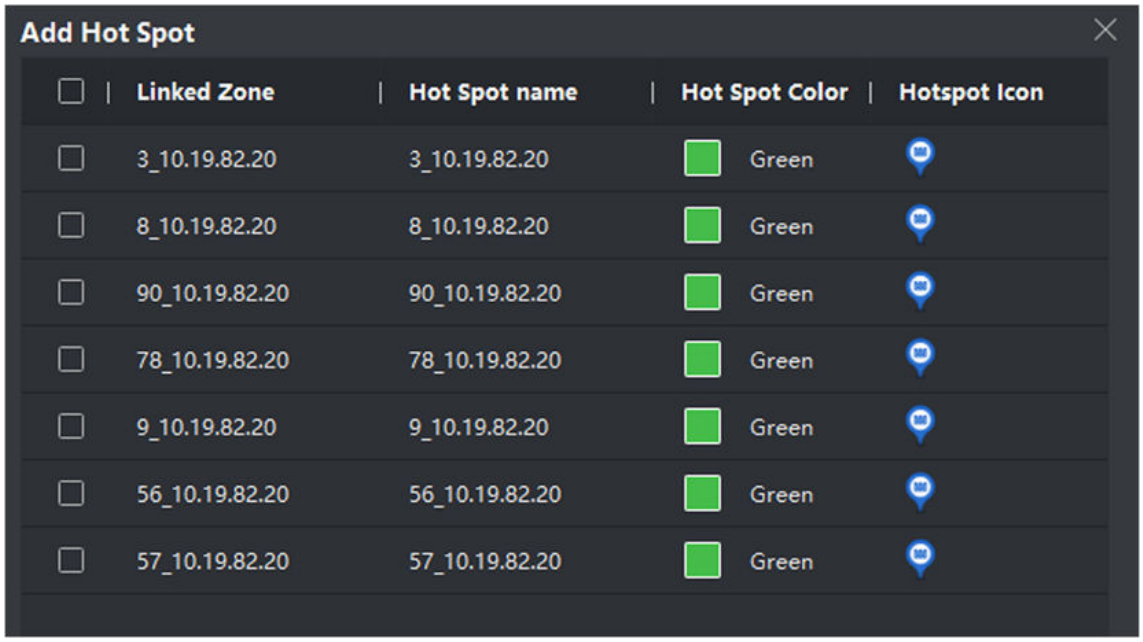


Figure 9-7 Add Hot Spot Panel

4. Select the zone(s) to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

Note

You can also drag the alarm output icons from the alarm output list to the map to add the hot spot.

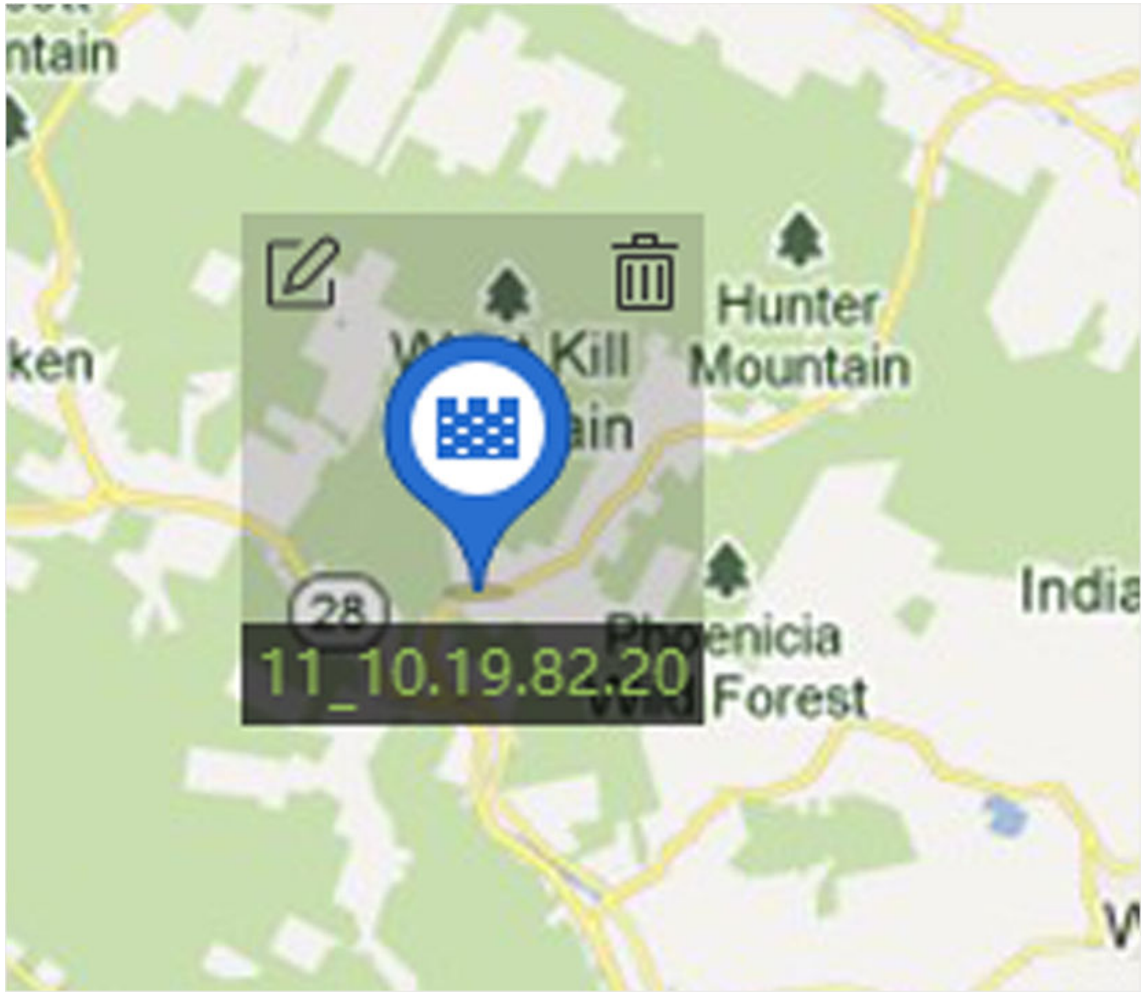


Figure 9-8 Zone on the Map

The zone is added to the map as a hot spot and its icon in the group list changes from to .

7. **Optional:** Drag the zone hot spot to move it to a certain position.

   When alarms are triggered, the number of the newest alarms will be displayed on the zone's icon. You can click the number to see the alarms details.

   Note

   No more than 10 newest alarms can be displayed.

8. **Optional:** Click **Clear Alarms** to mark the alarms of the zones on the current map as read.

9.4.5 Add Access Point as Hot Spot

You can add access points to the map as hot spots, so that you can find the hot spots and view their status and alarm numbers.

Before You Start

Make sure you have added a map and an access point to the client. See ***Add Map*** and ***Add Device*** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click **Add Hot Spot → Access Point Hot Spot** to open the Add Hot Spot window.

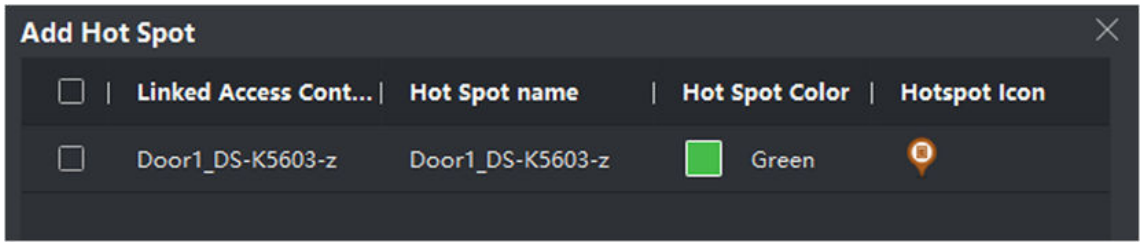


Figure 9-9 Add Hot Spot Panel

4. Select the access point(s) to be added to the map.
5. **Optional:** Edit the hot spot name, select the name color, and select the hot spot icon.
6. Click **OK**.

Note

You can also drag an access point icon from the access point list to the map.

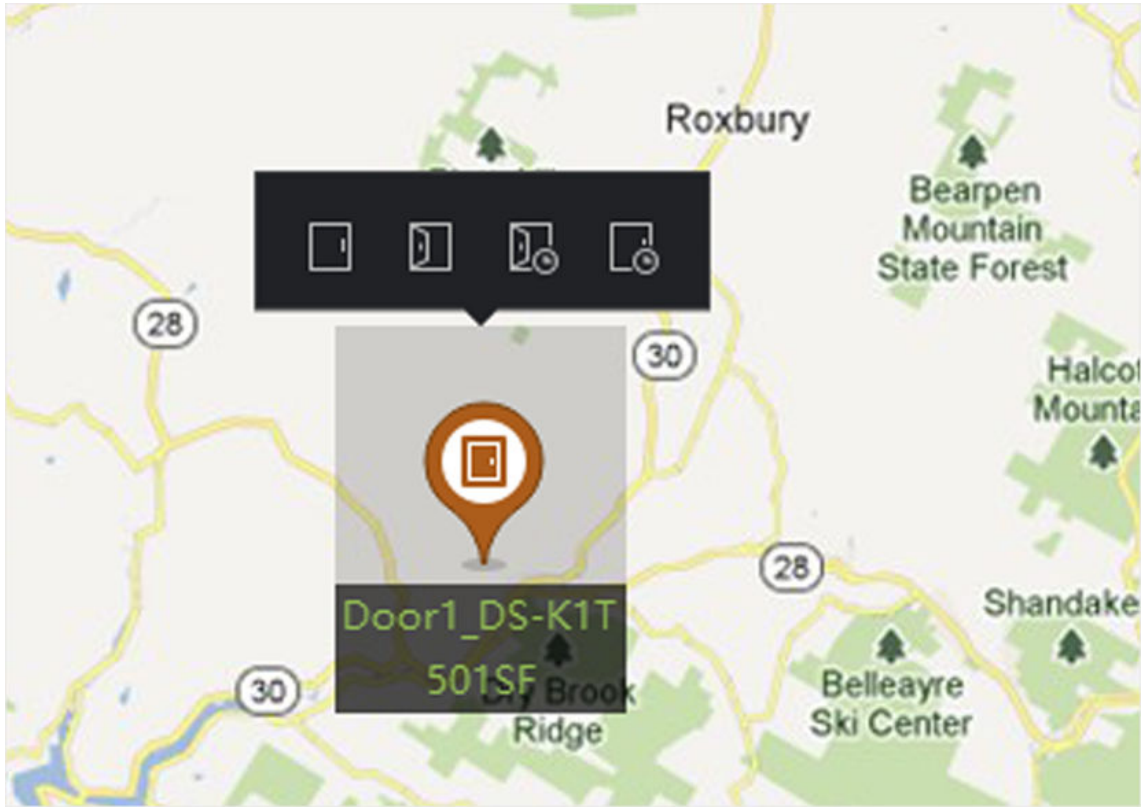


Figure 9-10 Access Point on the Map

The access point is added to the map as a hot spot and its icon in the group list changes from to .

7. **Optional:** Drag the access point hot spot to move it to a certain position.

   When alarms are triggered, the number of the newest alarms will be displayed on the hot spot icon. You can click the number to see the alarms details.

Note

No more than 10 newest alarms can be displayed.

9.4.6 Configure Security Radar Hot Spot

The client supports adding a security radar to the map to work as a hot spot. After that, you can configure parameters (including drawing zones and trigger lines, setting smart linkage, map calibration, etc.) for the radar and the parameters you set will take effect on the device. In this way, an intelligent monitoring in the radar's detection area can be realized by the client.

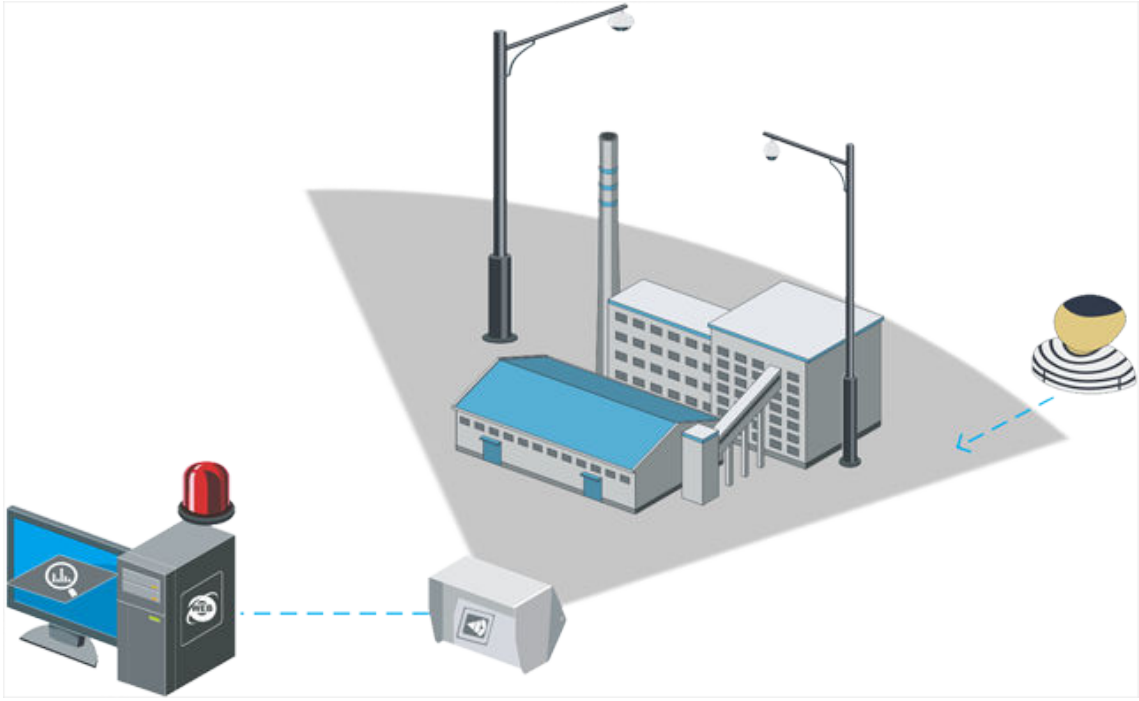


Figure 9-11 Scenario of Radar

Add Security Radar as Hot Spot

For an effective monitoring, you can add a security radar to the map as a hot spot and paint zones in its monitoring filed. So that when someone intrudes the zone, an alarm will be triggered for attention.

Before You Start

Make sure you have added an e-map and a security radar to the client. See ***Add Map*** and ***Device Management*** for details.

Steps

1. Enter the E-map module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. **Optional:** Edit map scale. See ***Edit Map Scale*** .
4. Select a security radar in the device list and drag it to the map.
5. **Optional:** Click the added radar and then click to edit the hot spot name, select the hot spot color, and select the hot spot icon.
6. Click **OK**.

   The security radar is added to the map as a hot spot and its icon in the group list changes from to . The sector indicates the monitoring field of the radar.



Figure 9-12 Radar on the Map

Note

- Orange sector indicates an armed radar, while black sector indicates a disarmed radar.
- Red point indicates the detected intruder.

7. **Optional:** Drag the security radar to move it to a certain position.

Draw a Zone

Zone is a basic concept in the security control system. It refers to a protection area in a radar's detection area, and is regarded as the maximum recognizable unit to distinguish the alarm event, determining whether to trigger an alarm according to the zone type and radar's arming status. You can see the target's location on the map the minute an alarm is triggered so as to take quick actions accordingly.

Before You Start

Make sure you have disarmed the radar: click **Finish**, and select **Disarm** after clicking the radar's icon.

Steps

1. Enter the E-Map module, and click **Edit** on the top right to enter the Edit mode.
2. **Optional:** Enable **Field Assistance** on the top left of the map. The target track will appear on the radar detection area. You can draw a zone with reference to the track.
3. Draw a zone.

Method	Step
Draw a Zone Manually	Click **Radar Settings → Draw Zone Manually** on the top of the map, and draw a zone on the radar detection area.

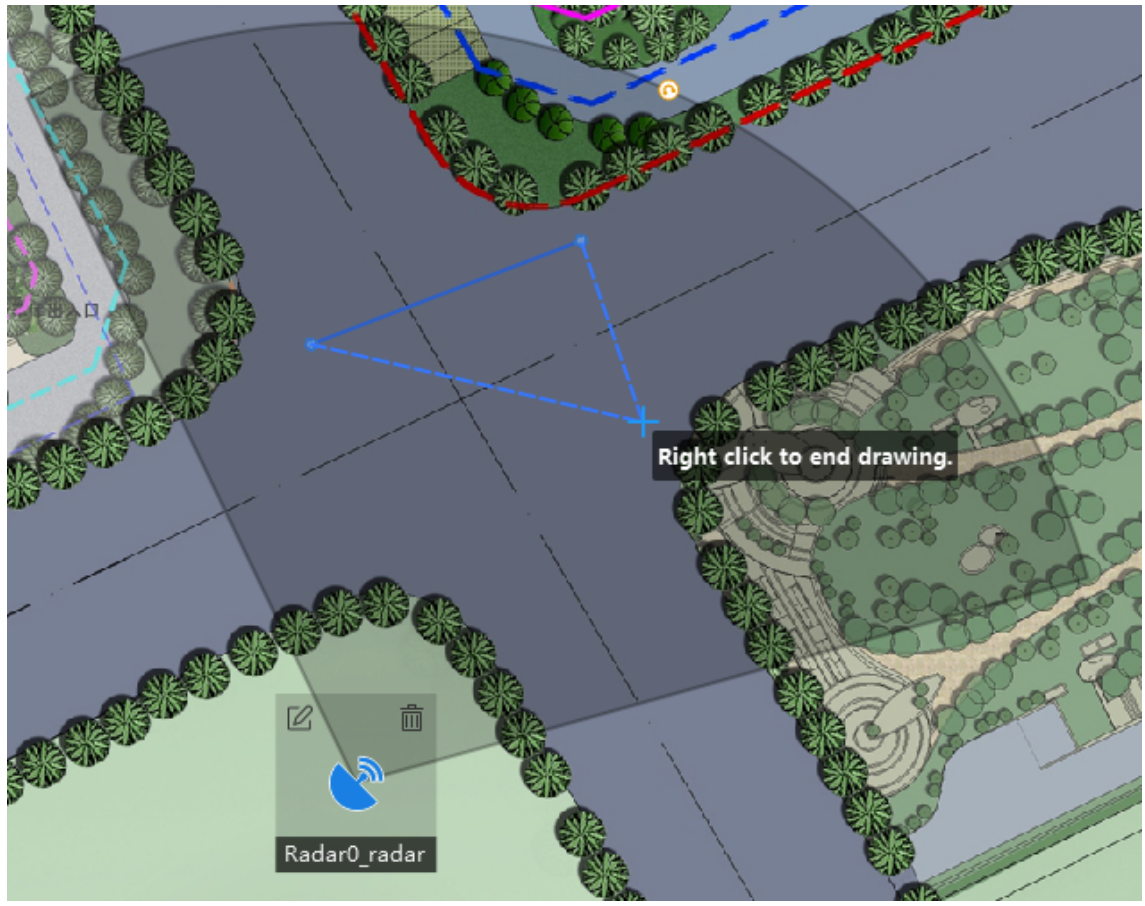


Figure 9-13 Draw a Zone Manually

Draw a Zone Quickly	Click **Radar Settings → Draw Quick Zone** on the top of the map, and left-click on the radar detection area to confirm the position of the zone.

Note

Currently, the default shape of the zone is square and it is not editable.



Figure 9-14 Draw a Quick Zone

4. Right-click to complete drawing, and a window will pop up. Enter the zone name, and select **Early Warning Zone**, **Warning Zone**, or **Disabled Zone** as the zone type.

   Early Warning Zone

   The early warning zone will identify target that has potential risks in advance and trigger an alarm, but will not store alarm track. The early warning zone is green.

   Warning Zone

   The warning zone will identify the targets entering the area and trigger alarm. The warning zone is orange.

   Disabled Zone

   The disabled zone will block the target track in the area. The disabled zone is black.

Note

- Adding zones is a batch operation. If you plan to add zones for only one radar, you need to right-click on the remaining radar detection area to cancel drawing a zone in detection area of other radars after drawing the desired zone.
- When drawing a zone, the actual lengths of the edges of the zone will be displayed; after drawing a zone, you can double-click it to view the actual lengths of its edges.
- Zones can overlap, the priority of the effective overlapping zone is: Disabled Zone>Warning Zone>Early Warning Zone. That is, Early Warning Zone can contain Warning Zone and Disabled Zone, and Warning Zone can contain Disabled Zone.
- You can zoom in/out to adjust the size of the displayed radar area.

5. Click **OK**.
6. Click **Finish** on the top right of the map.
7. **Optional:** After adding the zone and disarming the radar, double-click the zone to enter the editing mode, and perform the following operation(s) if needed.

Add a Marker	Hover the cursor on the line of the zone and it will change to a cross, and then click to add a marker.
Change the Zone Shape	Drag the marker to change the shape of the zone.
Move a Zone	Select a zone and drag the zone to move it.
Delete a Zone	Click to delete a zone.
Edit a Zone	Click to edit the zone name and type.

Draw Trigger Line

A trigger line refers to a virtual line drawn in a radar's detection area on the map. An alarm will be triggered when someone crosses it in its pre-defined direction.

Before You Start

The radar is added to the map. Click **Finish** on the top right to exit the editing mode. Click on the radar icon and select **Disarm** to disarm the radar.

Steps

1. On the E-map page, click **Edit** to enter the editing mode.
2. Click **Radar Settings → Draw Trigger Line** , and select **Trigger Line** or **Dual-Trigger Line**.

Note

Drawing a dual-trigger line that is too tortuous will cause a failure.

3. Draw trigger line.
   1) Click on the radar detection area to draw a trigger line.
   2) Select **Left -> Right**, **Left <- Right** or **Left <-> Right** in the pop-up window.
   3) **Optional:** Enter the distance between two lines. (Only for dual-trigger line)

Note

- Alarm rules: A single arrow  indicates that the target triggers an alarm when it crosses the trigger line in the direction of the arrow; a double arrow  indicates that the target triggers an alarm when it crosses the trigger line in any direction.
- The alarm can be triggered by crossing the Trigger Line according to the alarm rule; the alarm can be triggered only after crossing double lines of Dual-trigger Line according to the alarm rule.
- Direction determination: suppose you stand at the penultimate marker facing the last marker, the area on your left indicates the Left, while the area on your right indicates the Right.
- Up to 4 trigger lines can be drawn.
- Up to 1 dual-trigger line can be drawn.
- The trigger line cannot cross each other.

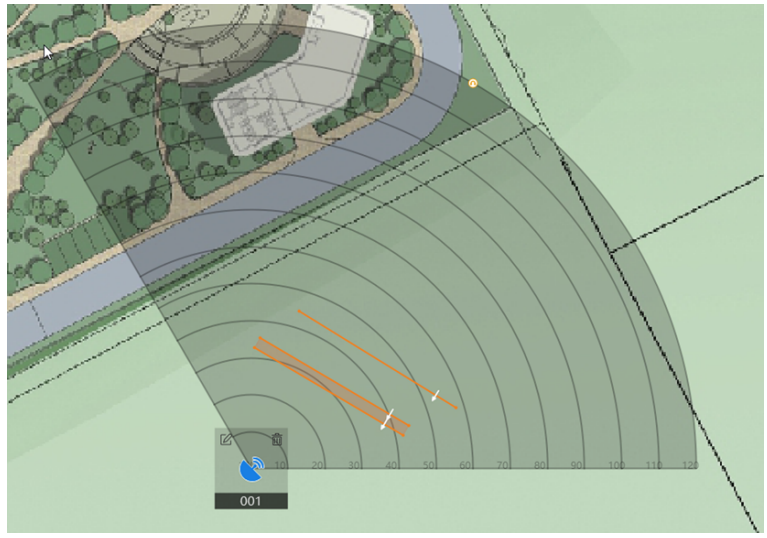


Figure 9-15 Draw Trigger Line

4. Click **OK**.
5. **Optional:** Click on the trigger line will appear different options: **Edit**, **Delete** and Move. You can edit the trigger line by clicking on it.
   - Add a Marker: Click on the line to add a marker.
   - Drag a Marker: Drag a marker on the trigger line to move it.
   - Move the Trigger Line: Hold the editing area to move the trigger line.
   - Edit: Click to edit the trigger line name, trigger line rule and distance (only for Dual-trigger Line).
   - Delete: Click to delete the trigger line.

Add Track Filter Zone

Track Filter Zone is an area in radar's detection area. When an object enters the track filter zone, alarms will not be triggered, and the object's moving pattern will not be uploaded to the client. This function is applicable for places with plenty of disturbing factors (such as trees) that may cause wrong alarms.

Before You Start

Make sure you have added a radar to map and have disarmed the radar. See ***Add Security Radar as Hot Spot*** for details.

Steps

Note

- This function should be supported by the device.
- Up to 32 track filter zones are supported.
- The size of track filter zone depends on device capability.

1. On the top right of the map, click **Edit** to enter the editing mode of the map.
2. Click **Radar Settings → Track Filter Zone → Add Track Filter Zone** .
3. On the map, hold the mouse and drag to set the semi-diameter of the track filter zone. Right-click to end drawing.

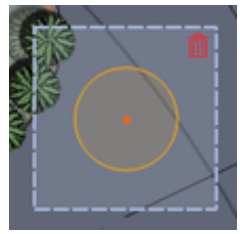


Figure 9-16 Track Filter Zone

4. **Optional:** Perform the following operations.

Edit Track Filter Zone	Double-click the track filter zone, hover the cursor on the border. When the cursor turns to a blue +, hold the mouse and drag to adjust the area.
Move Track Filter Zone	Double-click the track filter zone, and drag it to move it.
Display/Hide Track Filter Zone	Click **Radar Settings → Track Filter Zone → Display/Hide Track Filter Zone** to display or hide the track filter zone on/from the map.
Delete Track Filter Zone	Double-click the track filter zone, and click .

Add Point Cloud Filter Zone

After the radar detects the object, multiple points will be reported to the device and form the point cloud. Point cloud filter zone is an area in radar's detection area. Configuring it before environment learning can improve the accuracy of environment learning. When the object enters the point cloud filter zone, the point will not be reported to the device. This function is applicable for places with plenty of disturbing factors to reduce false alarms.

Before You Start

Make sure you have added a radar to map and have disarmed the radar. See ***Add Security Radar as Hot Spot*** for details.

Steps

Note

- This function should be supported by the device.
- Up to 16 point cloud filter zones are supported.
- The size of point cloud filter zone depends on device capability.

1. On the top right of the map, click **Edit** to enter the editing mode of the map.
2. Click **Radar Settings → Point Cloud Filter Settings → Draw Point Cloud Filter Zone** .
3. On the map, left-click to start drawing and right-click to end drawing.

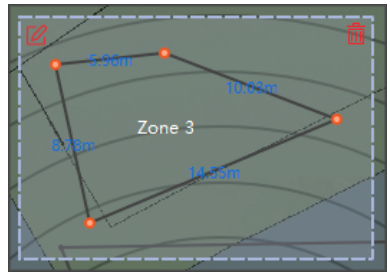


Figure 9-17 Point Cloud Filter Zone

4. Enter the name of the point cloud filter zone.
5. Click **OK**.
6. **Optional:** Perform the following operations.

Edit Point Cloud Filter Zone	Double-click the point cloud filter zone, hover the cursor on the border. When the cursor turns to a blue +, drag to adjust the area.
Move Point Cloud Filter Zone	Double-click the point cloud filter zone, and drag it.
Delete Point Cloud Filter Zone	Double-click the point cloud filter zone, and click .

Set Smart Linkage

Smart linkage works based on the calibration points you adds to the radar's detection area. That is the calibration points can tell the PTZ camera linked to the radar which direction to turn to when a target is detected so as to get the live view and track of the target by the client.

Note

Make sure you have performed the following operations before calibration:

- You need to disarm the radar before calibration: click **Finish** on the top right to exit the editing mode. Click the radar icon and select **Disarm** to disarm the radar.
- You need to link the PTZ camera to the zone before calibration, and set the PTZ camera initial position. See the PTZ camera user manual for details about how to set the PTZ camera initial position.
- Import the PTZ camera linked to the radar to the radar's group. See ***Group Resources*** for details.
- The installation height of the linked PTZ camera should be higher than 3 meters.
- Only PTZ camera supports this function.

According to the relative installation position of the radar and the camera, it is necessary to select a schedule (One-Point Calibration or Multi-Point Calibration) for the calibration point selection.

One-Point Calibration

Applicable to the scenario where the radar and the camera are installed on the same pole or the camera is installed within a radar-centered range of 2 meters (regardless of the altitude difference between the camera and the radar).



Figure 9-18 Scenario of One-Point Calibration

Multi-Point Calibration

The scenario which is not applicable to the one-point calibration needs to adopt the multi-point calibration.

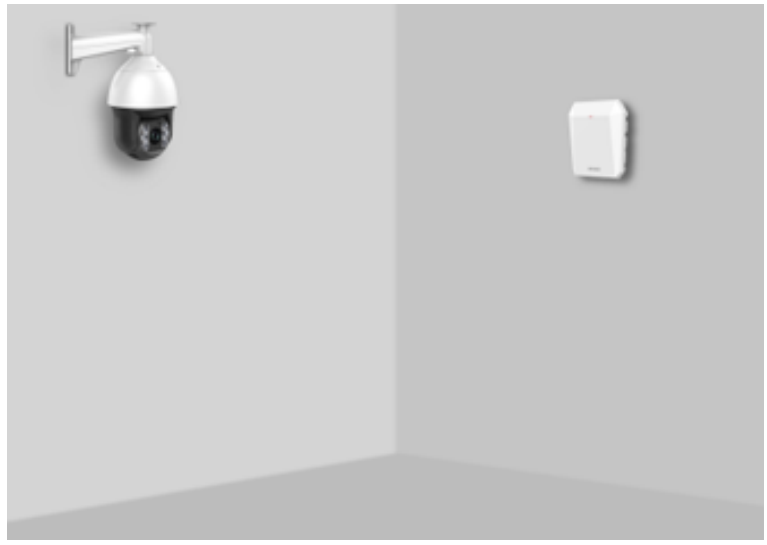


Figure 9-19 Scenario of Multi-Point Calibration

One-Point Calibration

One-point calibration is applicable to the scene where the radar and the camera are installed on the same pole or the camera is installed within a radar-centered range of 2 meters (regardless of the altitude difference between the camera and the radar).

Before You Start

To perform this function, a cooperation between two persons is required. Person A enters the detection area so that person B (the operator of the client) can see A's track on the client. And then B sets calibration points by the client according to A's track.

Steps

1. Click **Edit** on the top right of the map.
2. Click **Radar Settings → Smart Linkage Settings → Linked Positioning Settings** .
3. On the Smart Linkage Settings page, select a radar from the drop-down list on the top left.
4. Click a live view window at the bottom and select a camera in the **Linked Camera** list. The live view window displays the camera's live view.
5. Double-click the camera's live view window to enlarge it.

   Note

   You can click **+** or **-** to zoom in/out the map.
6. Select **One-Point Calibration** as the calibration mode.
7. Select the track of person A. Ask person A to move into the radar detection area. By comparing the moving object in the live view window of the camera and the track in the radar detection area, person B needs to select the track of person A and click it. The color of the selected track will turn from red to white.

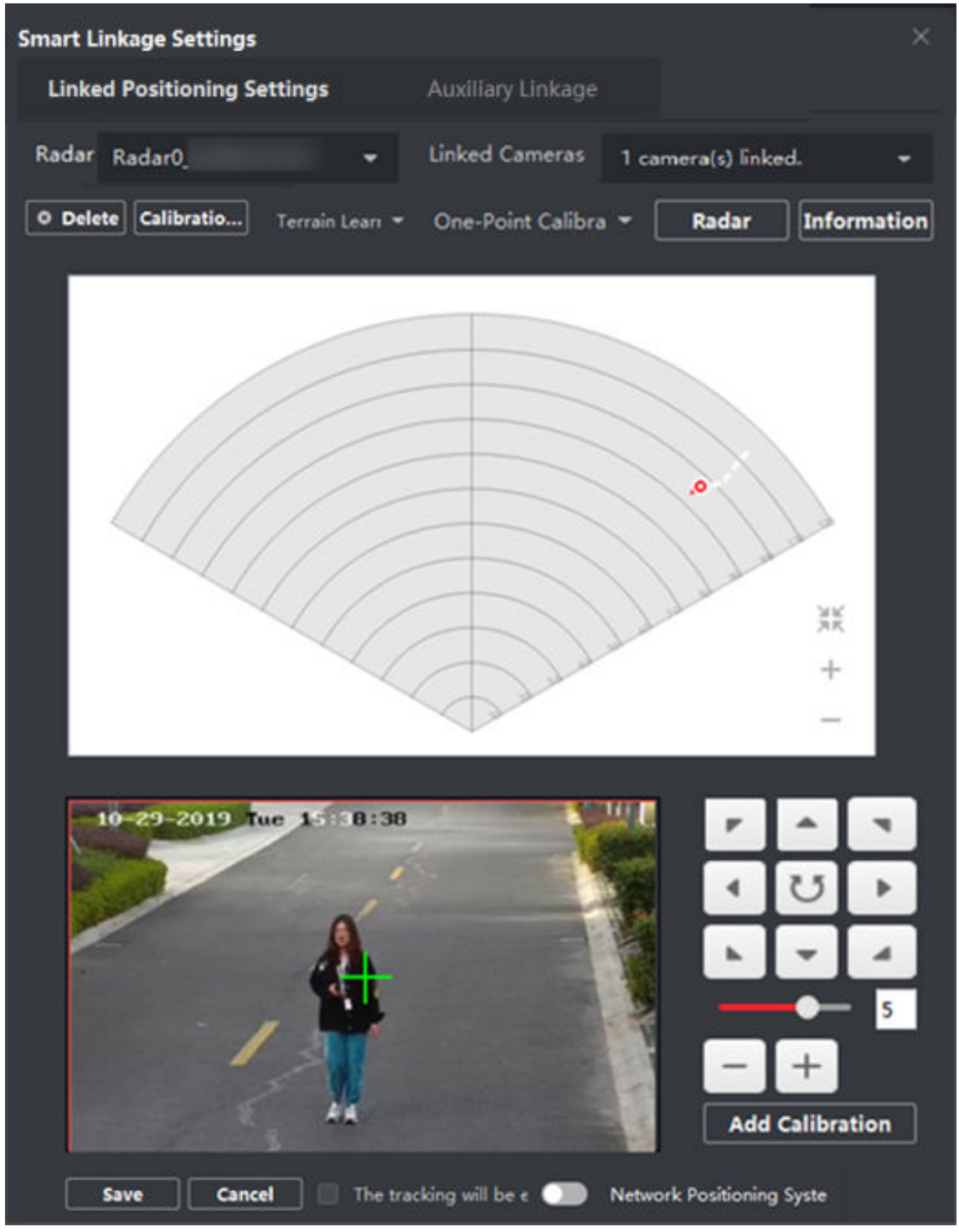


Figure 9-20 Select the Track

8. Ask person A to move to the calibration point within 20 to 40 m directly in front of the radar, and then stand at the calibration point.

9. Adjust the PTZ buttons in the live view window to get the PTZ position: Click + and - to adjust the altitude of person A to two-thirds of the altitude of the window, and click the direction buttons to align the central sign  with person A (For precise alignment, click on the center of the object and the screen will adjust automatically).
10. Click **Add Calibration** to add a calibration point. The PTZ position and the radar position of person A will be shown in the **Information** list. The option **The smart linkage will be enabled after completing the settings.** will be checked automatically.

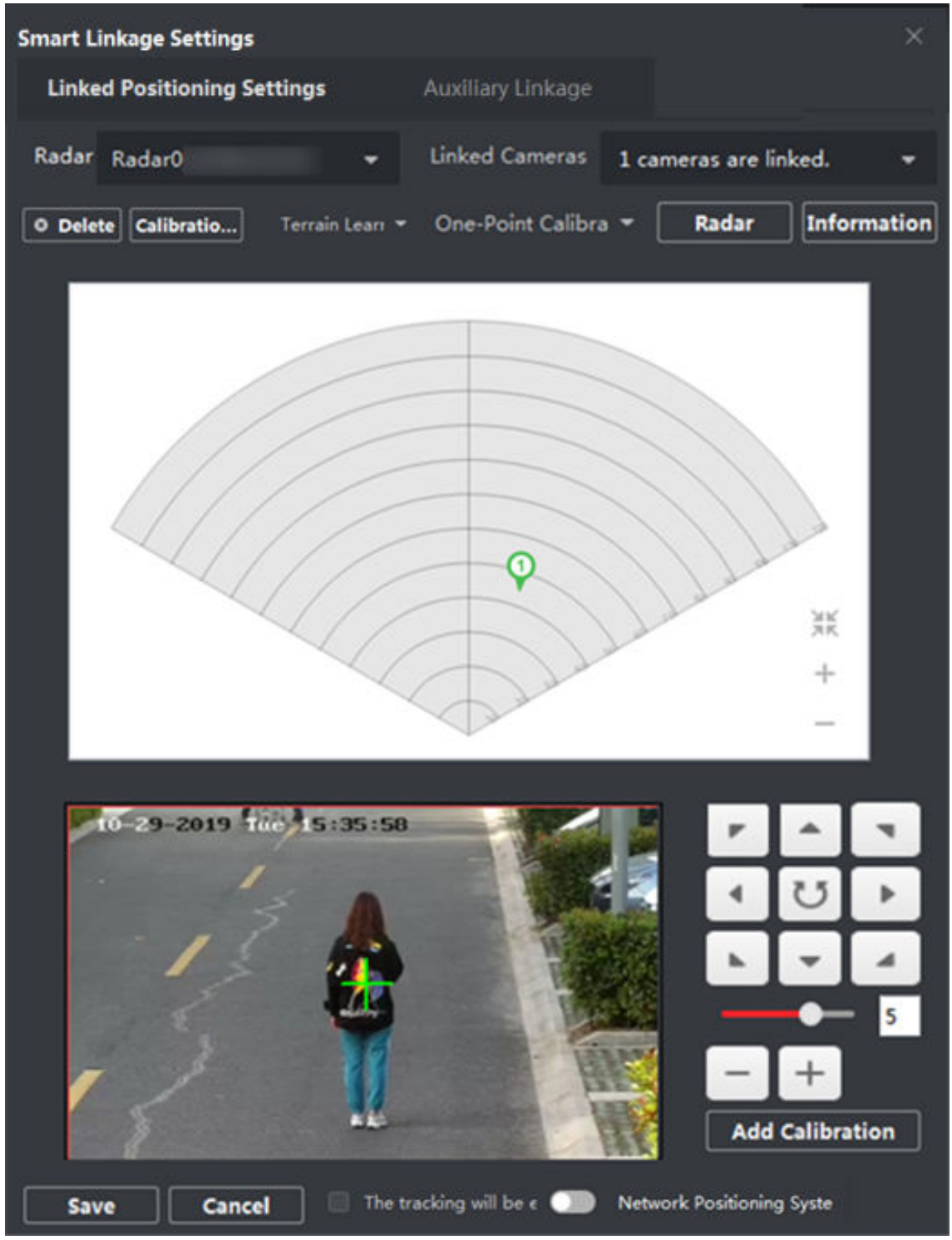


Figure 9-21 Add a Calibration

11. Click **Save**.

Multi-Point Calibration

Multi-point calibration is applicable to the scenario where the distance of the radar and the cameras linked to it is more than 2 meters.

Before You Start

This function needs the cooperation between 2 persons. Person A enters the detection area so that person B (the operator of the client) can see A's track according to which B set the calibration points by the client.

Steps

1. On the Smart Linkage Settings page, select **Multi-Point Calibration** as the calibration mode.
2. Select calibration points (equally distributed) on the center line of the radar's detection area, you can refer to the following figure to select points.



Figure 9-22 Multi-Point Distribution Instance

Note

At least 4 calibration points are required.

3. According to the calibration points, person A moves to a calibration point, and refer to step 2 to step 5 in One Point Calibration to calibrate the calibration point.
4. When the first calibration point is set, let person A move to the next calibration point after the yellow track disappears. And then refer to step 2 to step 5 in One Point Calibration to set the next calibration point. Follow this process to set all other calibration points in turn.

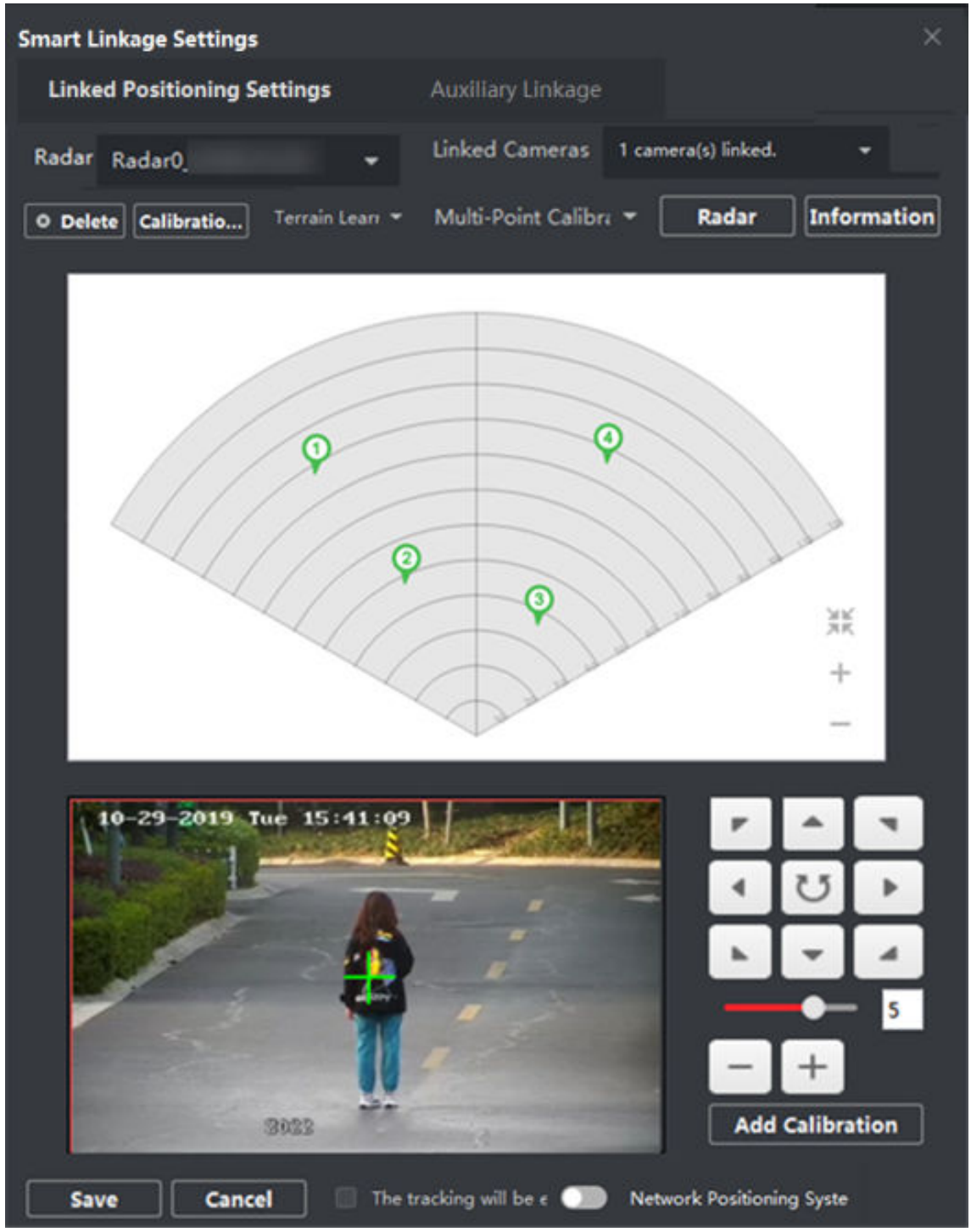


Figure 9-23 Multi-Point Calibration Radar Page

Note

Click **Delete** to delete a calibration point after selecting the calibration point in the Information list.

5. Click **Save** after all calibration points are set.

Note

You can save the calibration information successfully only if there are 4 calibration points, otherwise you cannot save it.

GPS Calibration

GPS Calibration refers to calibrating by device longitudes and latitudes, radar's orientation, and linked PTZ camera's position angle.

Before You Start

- Record the radar's longitude, latitude, and orientation.
- Record the linked PTZ camera's longitude, latitude, and position angle.

Steps

1. On the Smart Linkage Settings page, click **Set Longitude and Latitude** to open the Set Longitude and Latitude window.
2. Enable **Enable GPS Calibration**.
3. Enter **Radar Longitude** and **Radar Latitude**, and **Radar Orientation**.

Note

See radar user manual for details about setting radar orientation.

4. Enable **Network Positioning System**.

Note

You can also enable or disable this function on the Smart Linkage Settings page.

5. Enter **Camera Longitude**, **Camera Latitude**, and **Position Angle**.

Note

See PTZ camera user manual for details about setting position angle.

6. Click **OK**.

Set Auxiliary Linkage

Auxiliary Linkage is to add presets to the camera linked to the radar to help the radar accurately turn to the target with the assistance of presets. After adding presets, the camera will automatically turn to the presets if a target is detected, and in this way you can view the image of the target via the Client.

Before You Start

- Make sure you have calibrated the linked camera. For detailed information, see ***One-Point Calibration*** or ***Multi-Point Calibration*** .
- Make sure you have configured zones. For detailed information, see ***Draw a Zone*** .

Steps

1. Click **E-map**.
2. Click **Radar Settings → Smart Linkage Settings → Auxiliary Linkage** .

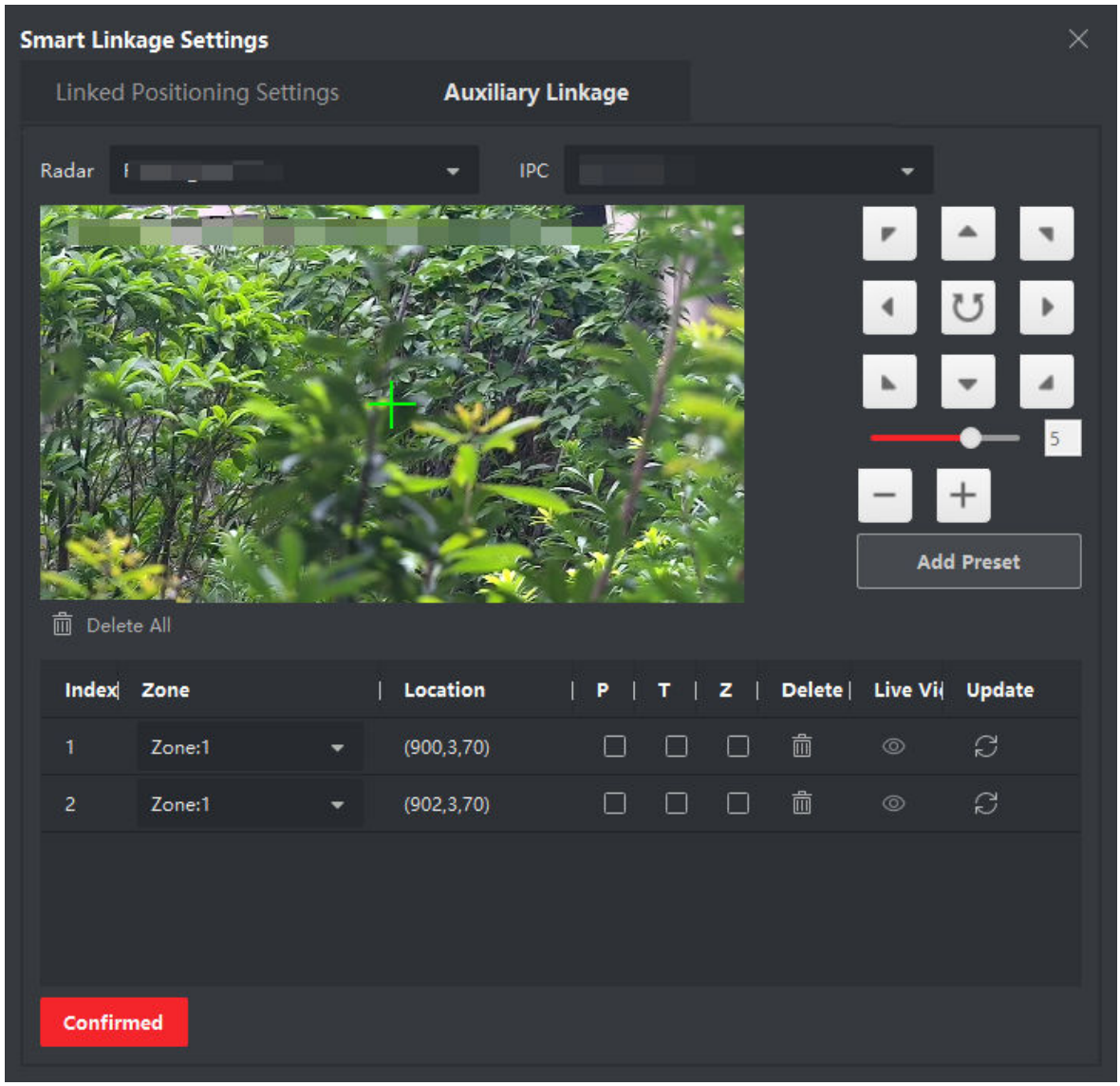


Figure 9-24 Auxiliary Linkage

3. Select a radar and a camera from the drop-down list.

Note

Make sure you have set the **Linked Camera** on the Smart Linkage Settings page, and saved the settings.

4. Click **Add Preset**.
5. Select a zone in the list.
6. **Optional:** Edit preset.

Button	Description
PTZ	Check P/T/Z, the checked value of the camera will remain unchanged.
Delete	Delete the preset.
Live View	Use the camera to view the presets.
Update	Update the preset coordinate to the current camera coordinate.

Note

The situation when you need to set PTZ is that if the calibrated camera cannot turn to the preset accurately, you can set P/T/Z to make it more accurate. You can check them all to fix the camera if the region is small or the terrain is not very undulating.

7. Use function buttons on the right to adjust the camera screen center position (cross icon position) to the watch point. You can click a position in the image and the position will become the center of the image.
8. Click **Confirmed**.

Set Environment Learning

To improve the accuracy of radar detection, you need to make the radar complete the environment learning.

Note

Make sure you have added the radar to the e-map.

Select a radar on the e-map in the client software, and click **Environment Learning** to start the environment learning.

Note

- The time for the environment learning is 10 seconds by default.
- Every time the radar starts to learn the environment, the previous learning data will be overwritten automatically.
- You can log in to the radar's remote configuration page via a web browser to configure the environment learning parameters. For details, refer to the user manual of the device.

Terrain Learning

By terrain learning, the radar can get the terrain of its detection area and make more accurate smart linkage.

Before You Start

Make sure you have completed calibration. See ***One-Point Calibration*** and ***Multi-Point Calibration*** for details.

Steps

Note

- This function should be supported by the device.
- To use this function, a cooperation between two persons is needed. Person A enters the radar's detection area, while person B operates the PTZ camera linked with the radar and display person A in the live view of the PTZ camera on the Smart Linkage Settings panel.

1. On the Smart Linkage Settings panel, click **Terrain Learning → Start Terrain Learning** .
2. In the radar's detection area, select person A's moving pattern.
3. Control the PTZ camera to keep person A in the center of the live view page by the buttons on the right.

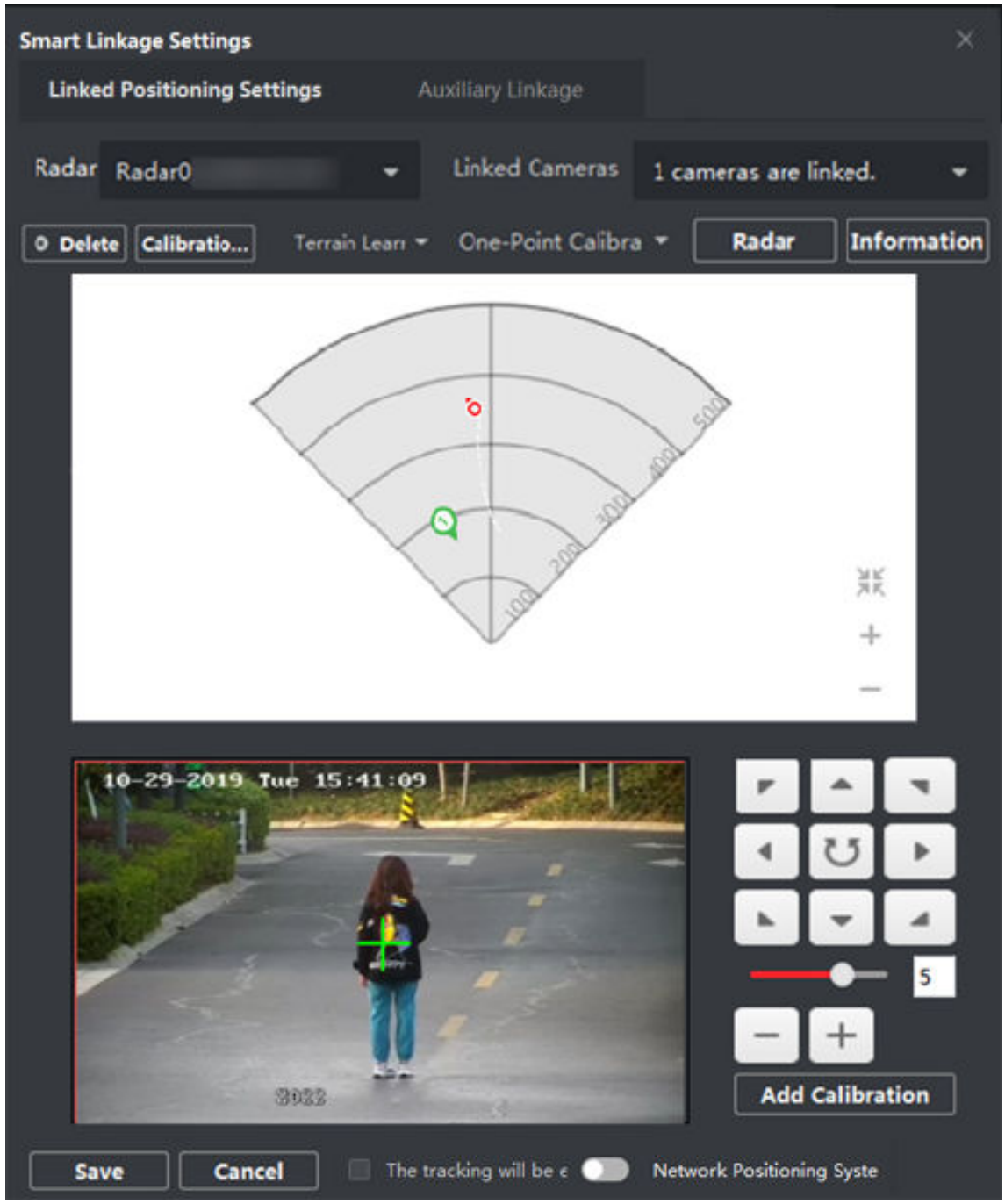


Figure 9-25 Terrain Learning

4. Click **Terrain Learning → Finish Terrain Learning** to end terrain learning.

Note

Old terrain learning results will be overwritten by new results.

5. **Optional:** Click **Terrain Learning → Clear Terrain Learning** to clear existing terrain learning results.

Calibration Compensation

Calibration Compensation makes calibration more accurate by adjusting Pan, Tilt, and Zoom of radar-linked PTZ camera.

Before You Start

Make sure you have finished a calibration.

Steps

1. On the Smart Linkage Settings page, click **Calibration Compensation** to open the Calibration Compensation window.
2. Select a camera from the Camera list.

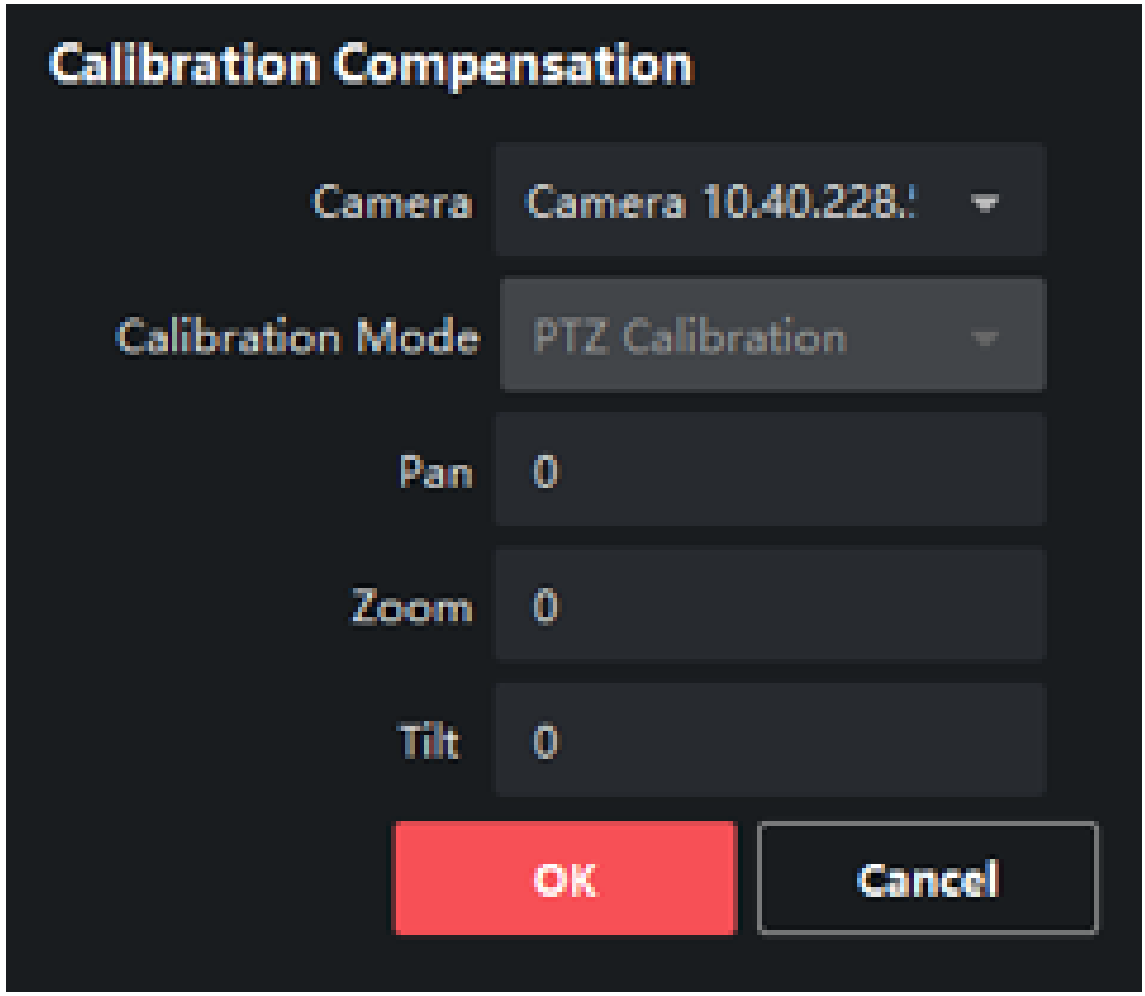


Figure 9-26 Calibration Compensation

3. Select a **Calibration Mode**.

GPS Calibration

If you had conducted GPS calibration before, select this mode.

PTZ Calibration

If you had conducted one-point calibration or multi-point calibration before, select this mode.

4. Enter the **Pan**, **Tilt**, and **Zoom**.

Note

The **Pan**, **Tilt**, and **Zoom** you entered here will be added to the former **Pan**, **Tilt**, and **Zoom**.

5. Click **OK**.

Set Parking Points for Linked Camera

After enabling the radar parking mode, the radar will control the linked camera to turn to the predefined parking point when no target detected within 10s in the radar detection area.

Before You Start

- Add the radar to the map.
- Link the camera to the radar, and add the camera to the client.
- Calibrate the camera and enable camera smart linkage.
- You need to disarm the radar before the operation. Click **Finish** on the E-map page to exit the editing mode. Click the radar icon and select **Disarm** to disarm the radar.

Steps

Note

This function is only applicable for cameras with PTZ control function.

1. Click **Edit** on the top right of the map to enter editing mode.
2. Click **Radar Settings → Set Parking Point** .
3. Select a radar from the **Radar** drop-down list.
4. Select a linked camera from the following list.
5. Use buttons on the right to adjust the camera screen center position (cross icon position) to the watch point. You can click on the screen and the screen will automatically adjust to the clicked center. You can also click the image to make the position you clicked the center.



Adjust the rotation speed of the camera. 1 is the slowest and 7 is the fastest.

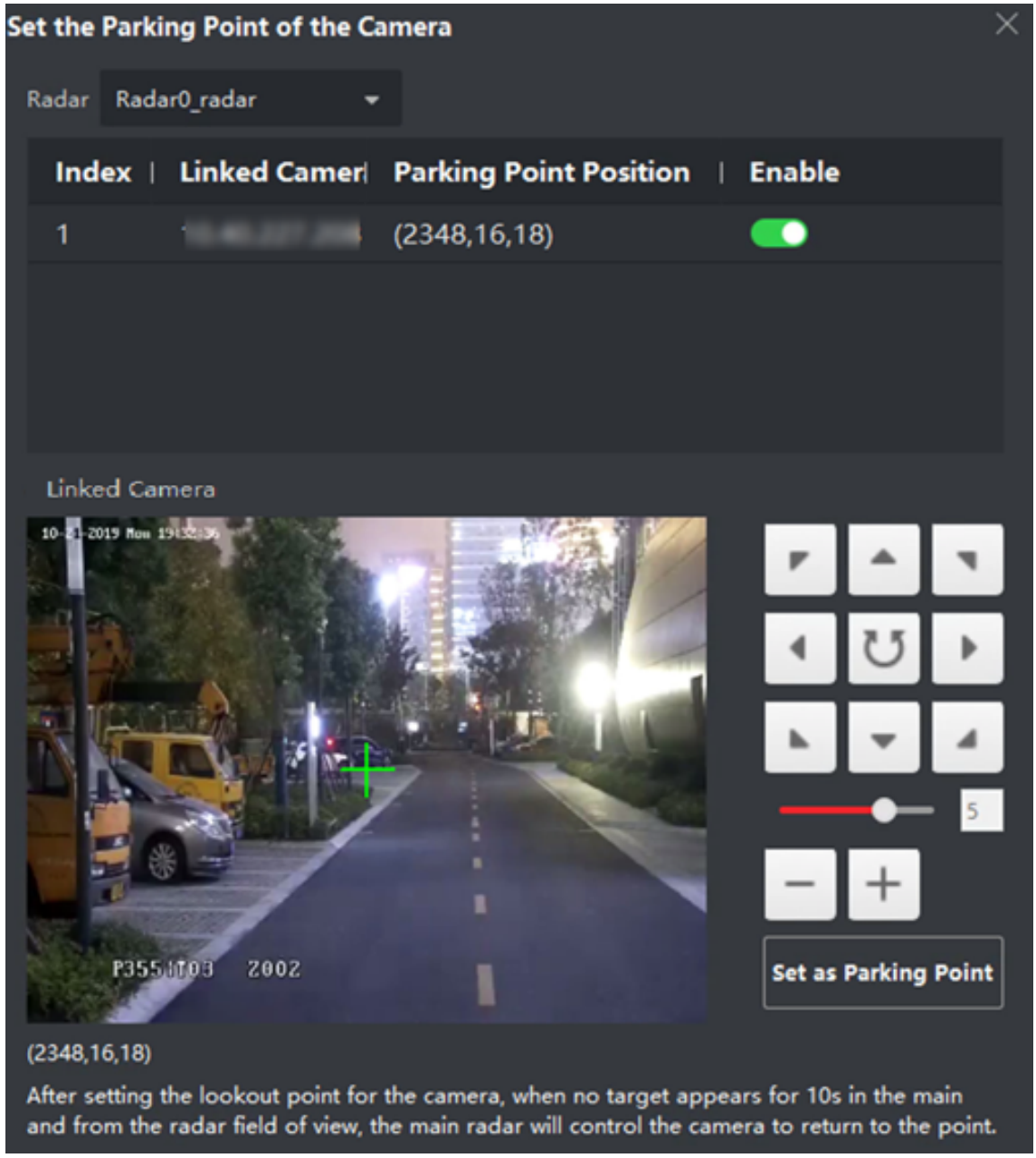


Figure 9-27 Set Parking Point

6. Click **Set as Parking Point**.

Set Preset Point

You can set a preset point for a zone or a trigger line. When an alarm is triggered in the zone or trigger line, the camera will automatically turn to the corresponding preset point.

Before You Start

- Add the radar to the map.
- Link the camera to the radar, and add the camera to the client.
- Zones and trigger lines are configured.
- You need to disarm the radar before the operation. Click **Finish** on the E-map page to exit the editing mode. Click the radar icon and select **Disarm** to disarm the radar.

Steps

Note

This function is only applicable for cameras with PTZ control function.

1. Click **E-map** and click **Edit** to enter the editing mode.
2. Click **Radar Settings → Preset Point Settings** .

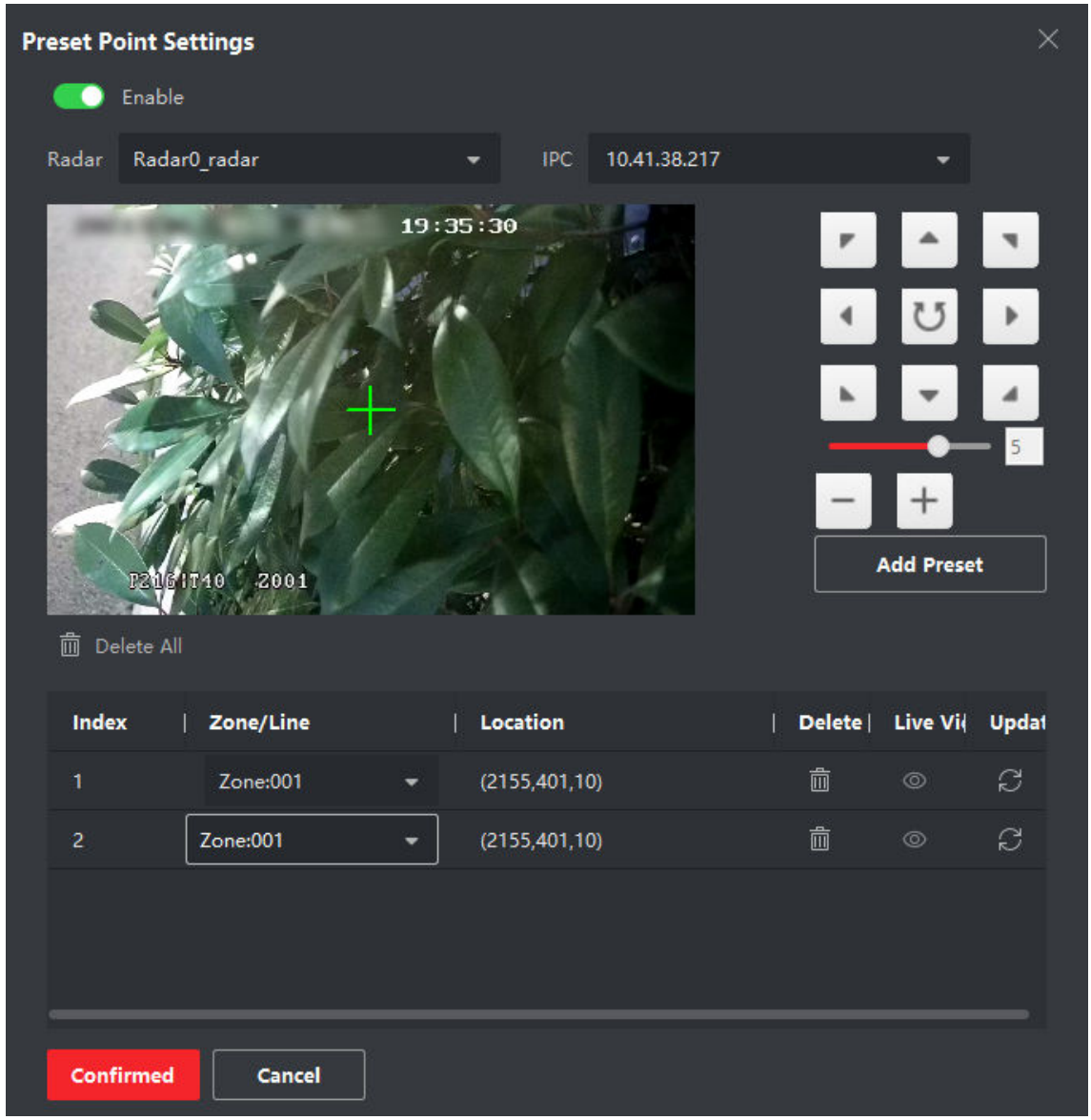


Figure 9-28 Preset Point Settings

3. Switch on **Enable**.
4. Select a radar and a camera from the drop-down list.
5. Use function buttons on the right to adjust the camera screen center (cross icon position) to the watch point.

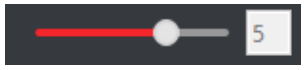
Note

You can also click on the image and the clicked point will be the camera screen center.

Operation	Description


Adjust the camera direction. Hold to move the camera direction continuously.


Rotate the camera horizontally. Hold to continuously rotate the camera horizontally.



Adjust the rotation speed of the camera. 1 is the slowest and 7 is the fastest.


Zoom the screen.

6. Click **Add Preset**.
7. Select a zone or trigger line from the list.
8. **Optional:** Edit the preset point(s).

Button	Description
Delete	Delete the preset point.
Live View	Use the camera to view the preset point.
Update	Update the coordinate of the preset point according to the coordinate of the current camera.

9. Click **Confirmed**.

Map Calibration

Map calibration is used to get the accurate scale of the map by the cooperation of three persons.

Before You Start

Make sure you have added the radar (when adding the device, check **Import to Group**) to the client and the map, and have set a scale for the map.

Steps

1. Click **Edit** to enter the editing mode.
2. Click **Radar Settings → Map Calibration** .
3. To perform this operation, an cooperation between three persons is needed. Person A and person B move into the radar's detection area. Person C selects their tracks by the client. A and B stop at the calibration points and the system will generate 2 markers at the terminal of tracks. Click **OK** on the pop-up window to confirm the terminal of the track or click **Delete** to select a new track.



Figure 9-29 Confirm Terminals

4. Click on the map to confirm the actual locations of marker 1 and marker 2.

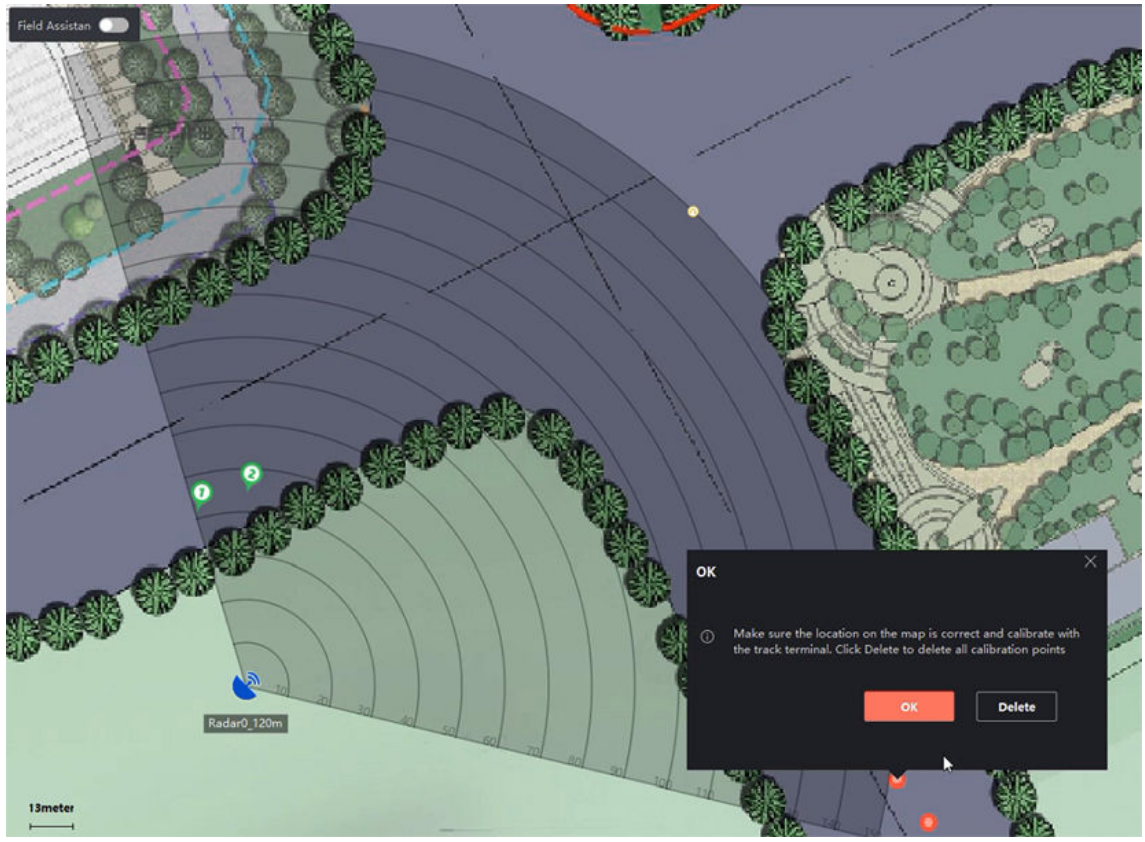


Figure 9-30 Confirm Actual Locations

5. A window pops up saying *Make sure the location on the map is correct and calibrate with the track terminal?* Click **Delete** to delete all calibration points. Click **OK** on pop-up window. The system will automatically match the markers to the actual locations.



Figure 9-31 Finish Map Calibration

Other Functions

When using the radar, you can perform some auxiliary functions such as arming/disarming, refreshing radar parameters, displaying OSD and PTZ camera's FOV (field of view), and enabling alarm output to meet different needs.

Note

Make sure you have exited the map editing mode before using the following functions.

Environment Learning

Click **Environment Learning** to enable the environment learning mode for the radar. For details, refer to ***Set Environment Learning*** .

Arm/Disarm All Radars

Click **Arm Radar → Arm All Radars/Disarm All Radars** to arm or disarm all radars on the map.

Arm/Disarm Single Radar

After exiting the editing mode, click the radar's icon to show its operation menu.

Arm a Radar

Arm the radar's detection area. A question will pop up saying *There are targets in the zone, enable mandatory arming?* if you arm the radar when a target exists in the warning zone. You can click **OK** to arm the radar mandatorily.

Note

The radar cannot be edited if it is armed.

Disarm a Radar

Disarm the radar's detection area.

Event

Search alarms triggered by certain cameras during certain time range, and view the alarm related videos. See ***Preview Hot Spot*** for details.

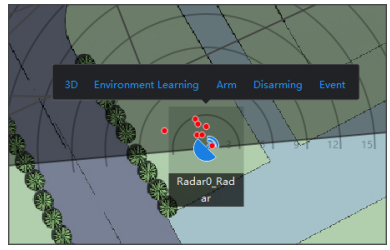


Figure 9-32 Radar's Function List

Enable Alarm Output

An alarm output refers to sirens linked to a radar. It flashes or generates alarm sound when an alarm or pre-alarm is triggered if you enable it.
Operation: click **Radar Settings → Alarm Output** after entering editing mode. Select a relay, and switch on in the Operation column; or click **Enable All** to enable all the relays in the list.

Target Number Display

After exiting the editing mode, Move your cursor on the radar's icon to show the number of person, vehicle and other target.

Display 3D Detection Area

Move your cursor on the radar's icon in the editing mode, click **3D** to enter the view page of detection area. You can click on different direction of the Radar's 3D view to adjust the display angle.

Note

This function should be supported by the device.

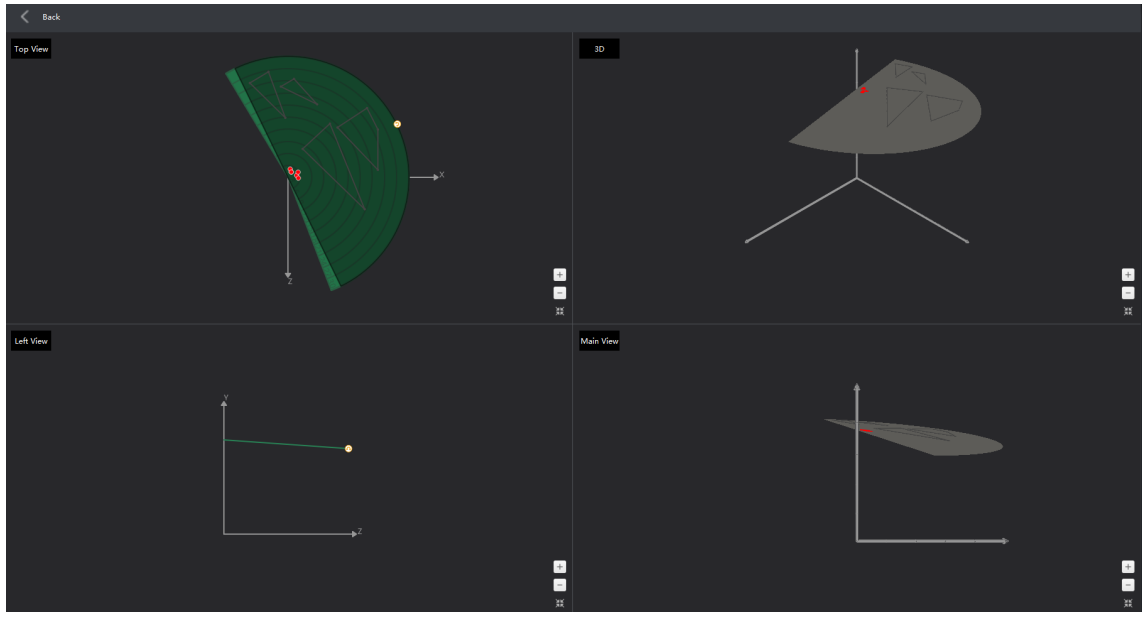


Figure 9-33 3D Detection Area View

Display 3D Detection Area View

Move your cursor on the radar's icon in the non-editing mode, click **3D** to enter the view page of detection area, including 3D view, original point cloud diagram, laser beam diagram, and background outline.

Note

- You can click different direction of the Radar's 3D view to adjust the display angle.
- On the original point cloud diagram, you can switch on **Environment Information** on the top-right corner to view the added point cloud filter zone. For details about drawing the point cloud filter zone, refer to ***Add Point Cloud Filter Zone*** .

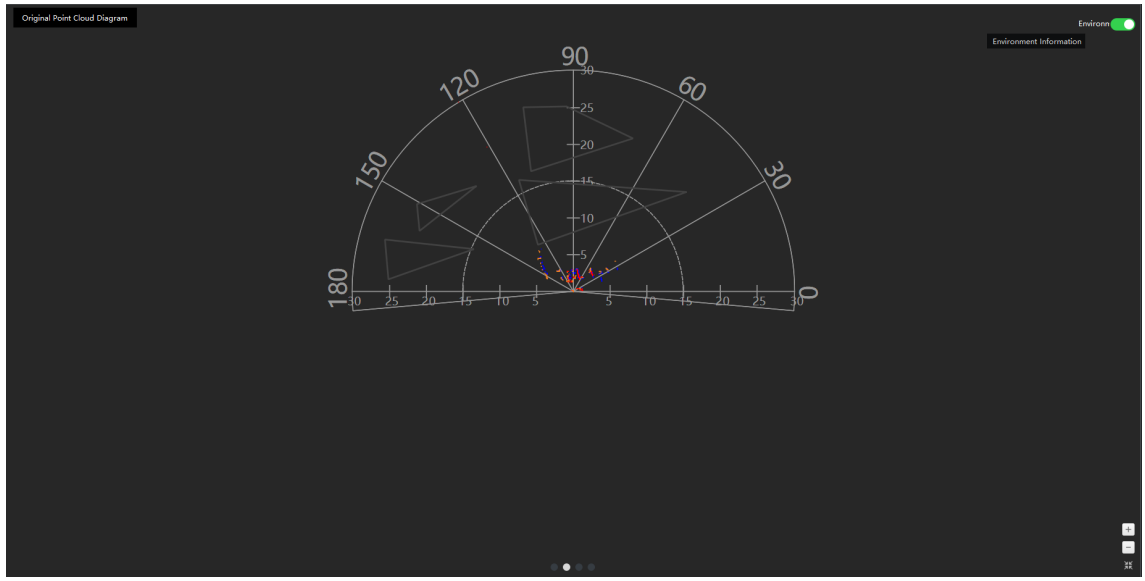


Figure 9-34 Original Point Cloud Diagram

Pattern Playback

After exiting the editing mode, click the radar and then click **Event** to enter the Event Search window on the right. You can search for the event according to the conditions you set, including time period and the zone. The pattern playback video will be played in the middle of the page.

Note

Make sure the PTZ camera has been linked to the radar.

Display OSD

On the top of the map, click **Display → Display OSD** to display the detected target No., target's moving speed, distance and duration between the target and radar.

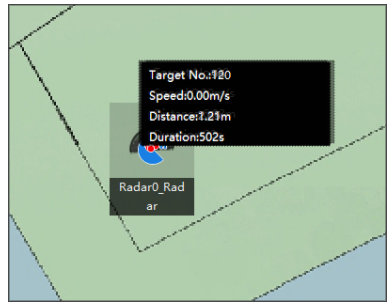


Figure 9-35 OSD on the Map

Display PTZ Camera's FOV

On the top of the map, click **Radar Settings → Camera FOV** to display the linked PTZ camera's filed of view (FOV) and camera's IP address on the map.

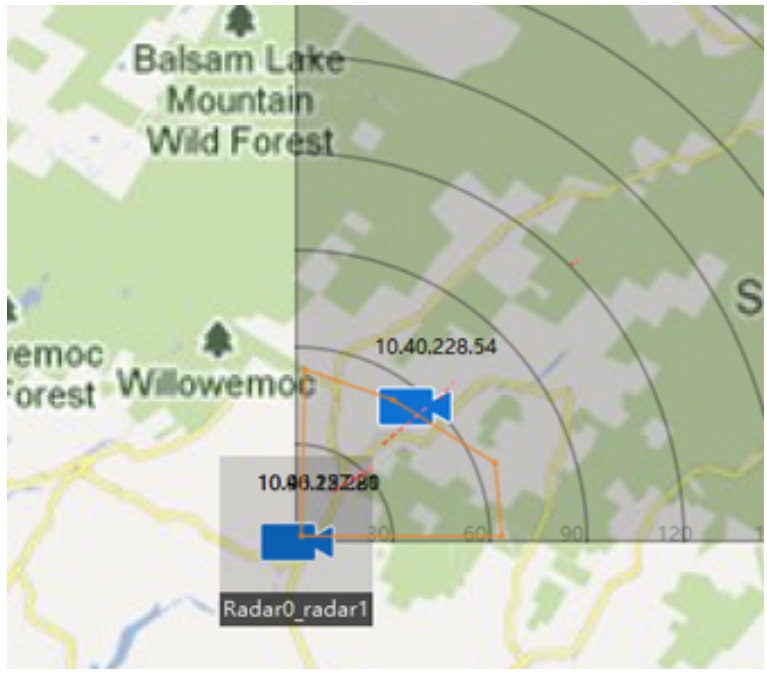


Figure 9-36 PTZ Camera's Field of View

Refresh

Click **Radar Settings → Refresh** on the top of the map to refresh the radar's newest detection angle, detection distance, trigger lines, and arming status.

9.4.7 Edit Hot Spot

You can edit the information of the added hot spots on the map, including the name, the color, the icon, etc.

Steps

1. Enter the E-map module.
2. Click **Edit** in the upper-right corner to enter the map editing mode.
3. Select the hot spot icon on the map and then click to open the Edit Hot Spot window.
4. Edit the hot spot name in the text field, select the hot spot name's color and hot spot icon shown on the map.
5. Check **Apply to Other Camera Hot Spots/Apply to Other Alarm Input Hot Spots/Apply to Other Alarm Output Hot Spots/Apply to Other Zone Hot Spots** to apply the color and icon settings to other hot spots.

6. Click **OK**.
7. **Optional:** Select the hot spot icon and click to delete the hot spot.

9.4.8 Preview Hot Spot

After adding hot spots (including camera, alarm input/output, zone, security radar, and zone) to the map, you can view the live view of the camera hot spot and the triggered alarm information of all the types of hot spots on the map.

Before You Start
Make sure you have added hot spots to the map. See ***Manage Hot Spot*** for details.

Steps
1. Enter the E-map module.

Note
If you are in the editing map mode, click **Exit** on the upper-right corner to enter the map preview mode.

2. Click **Display** to show the hot spots on the map.

Note
Hot spot type with will be shown on the map.

3. Click a hot spot to perform the following operation(s).

Hot Spot Type	Operations
Camera	Live View: Click to pop up the live view window of the camera. **Note** • When an alarm is triggered during live view, the client will play a video file of 30 s first. • You can capture, start recording and instant playback during live view.
Alarm Output	Click an alarm output, and select **Open/Close**. **Note** The security control channels managed by the alarm output will also be opened/closed.
Access Point	View door status: the current door status of the access point is displayed on the icon. Click the icon to switch the door status. **Open Door**

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Security Radar Arm/Disarm zones in the monitoring field of the radar: After exiting editing, click the icon of a security radar, and then select **Arm**/**Disarm**; or click **Event** to search events triggered during certain time range.

Note

- You can still arm the radar even if there is a target in the radar's detection area.
- The warning zone and early warning zone will be armed after arming the radar, which means an alarm will be triggered and reported to the Event Center once a target enters the warning zone and early warning zone.
- For the camera linked with radar, you can select the linked radar and move the camera through the operations keys on the PTZ control panel. The real-time location will be applied to the linked radar. For details about icons of PTZ control panel, refer to ***PTZ Control Panel*** .

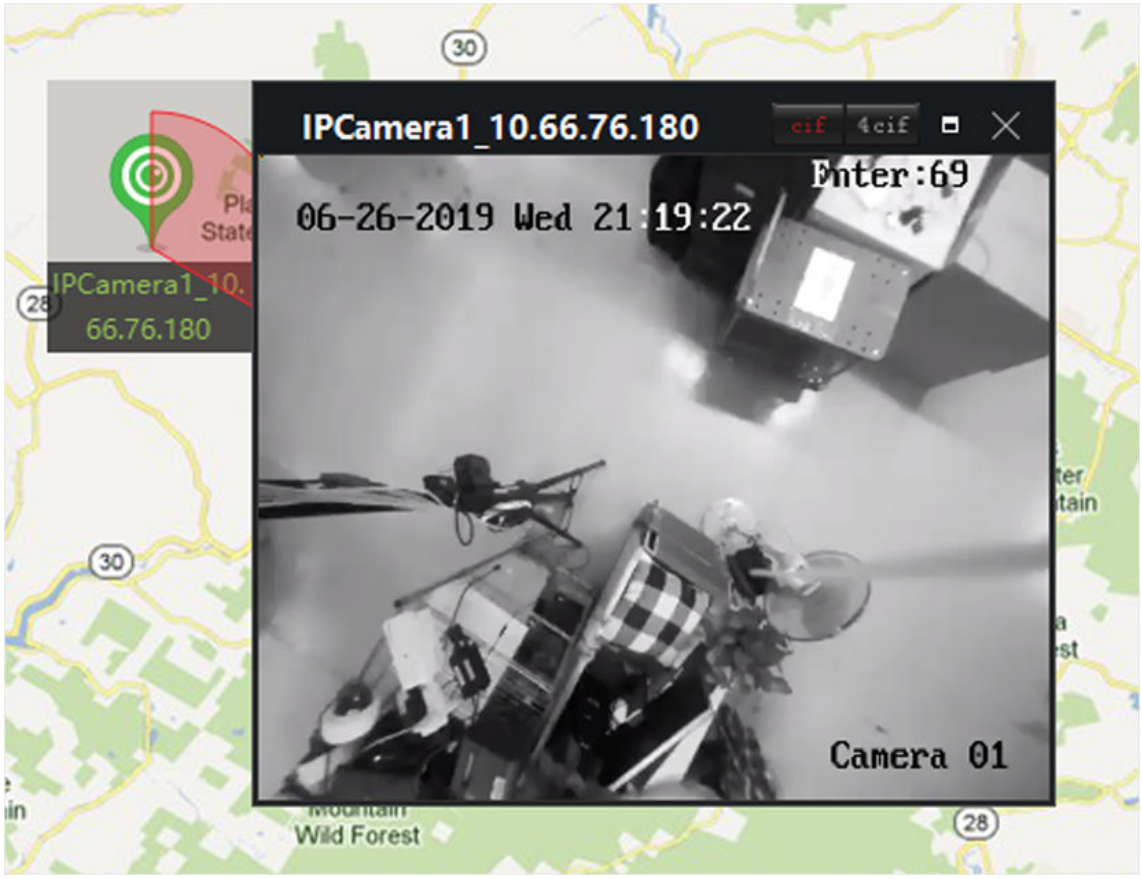


Figure 9-37 Live View of Camera on the Map

4. **Optional:** Perform the following operation(s).

View Alarm Information	Click the alarm number on a hot spot icon to open the alarm information page to view the alarm type and triggering time.
Clear Alarm	Click **Clear Alarm** on the top of the map to mark all the alarms of the hot spot as read.
View Multiple Cameras' Live View on the Map	a. Click **Live View** to show 4 small windows on the bottom of the client. b. Drag a camera from the device list to a window to start the live view. **Note** Up to 4 cameras' live view is supported at the same time.

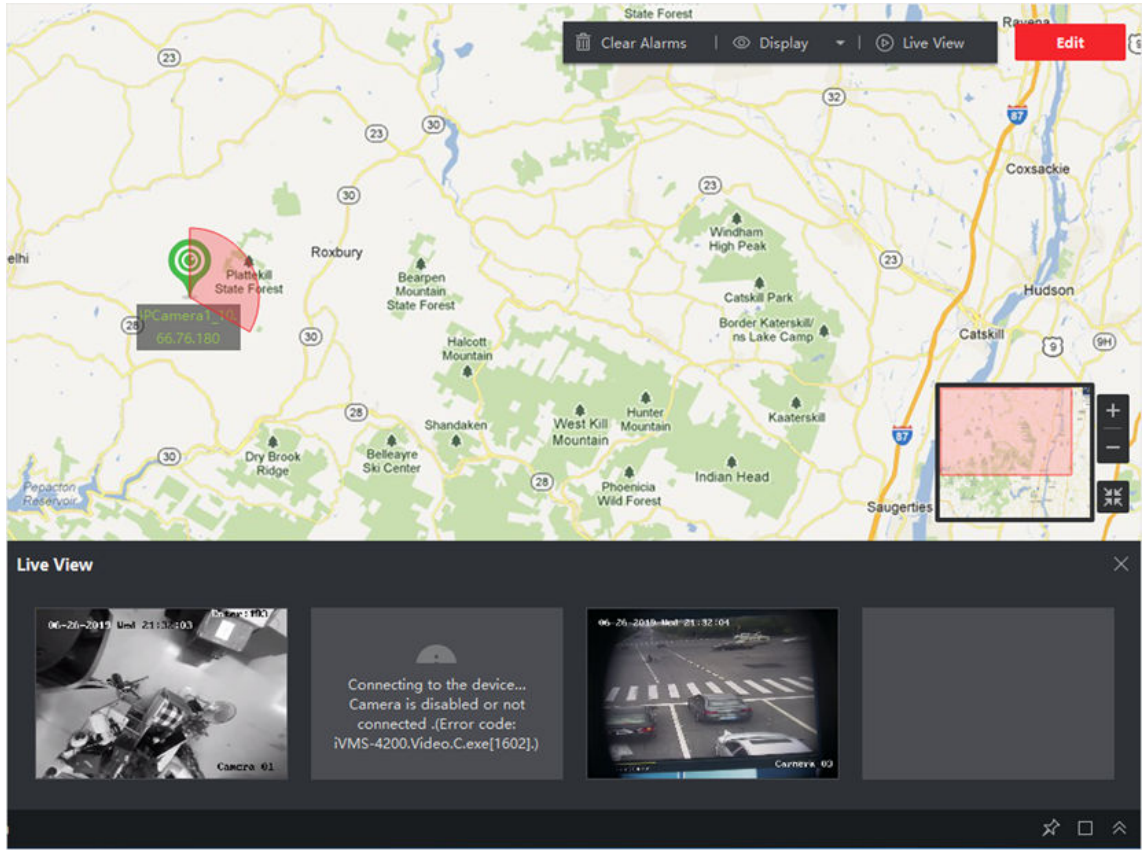


Figure 9-38 Preview Camera Hot Spot

9.5 Manage Hot Region

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

After linking a child map to a parent map, a hot region icon will display on the parent map. You can click it to enter the child map to view the resources on the child map for convenience.

With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

9.5.1 Add Hot Region

You can add a map to another map as a hot region and an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Before You Start

At least two maps should be added. Refer to ***Add Map*** for details about adding maps.

Steps

Note

A map can only be added as the hot region for once.

1. Enter the E-map page.
2. Click **Edit** on the upper-right corner to enter the map editing mode.
3. Select an added map as the parent map.
4. Click **Add Hot Region** to open the Add Hot Region window.
5. Select the child map.
6. **Optional:** Edit the hot region name, and select the hot region color and icon by double-clicking the corresponding field.
7. Click **OK**.

   The child map icons are added on the parent map as the hot regions.

9.5.2 Edit Hot Region

You can edit the information of the hot regions on the parent map, including name, color, icon, etc.

Steps

1. Enter the E-map module.
2. Click **Edit** on the upper-right corner to enter the map editing mode.
3. Select a hot region icon on the parent map and click to open the Edit Hot Region window.
4. Edit the hot region name in the text field, select the hot region name's color and hot region icon.
5. Check **Apply to Other Hot Regions** to apply the color and icon settings to other hot regions.
6. Click **OK**.

9.5.3 Preview Hot Region

After adding a hot region, you can click the hot region icon on the parent map to enter the child map. You can view the resources and alarms on the child map.

Steps

1. Enter the E-map page.

   Note

   If you are in the editing map mode, click **Exit** on the upper-right corner to enter the map preview mode.

2. Click the hot region icon on the parent map to enter the linked child map.

You can view the resources on the child map. If there is any alarm triggered on the child map, you can view the alarm details.

3. **Optional:** Click **Back to Parent Map** on the upper-left corner to go back to the parent map.
4. **Optional:** Click **Clear Alarm Info.** on the upper-right corner to clear the alarm information triggered by the resources on the current map.

9.6 View Person's Moving Pattern

With the help of facial recognition devices, you can view the target person's moving pattern on the map, which is generated by several cameras' locations. E-map allows you to search and view the moving pattern of an individual (such as a suspect, a missing child, etc.) on the map to help finding him/her.

Before You Start

Make sure you have added a map for a group and added the cameras in the group to the map. See ***Add Map*** and ***Add Camera as Hot Spot*** for details.

Steps

1. Enter the E-map module.
2. Click a group name in the resource list on the left column.

   The group's map and resources on the map appear in the display area.
3. **Optional:** Click **Add Map** to add a map for the group and add cameras in the group to the map.
4. Click **Moving Pattern** on the top of the map to open the Search Moving Pattern page.
5. Click to set a time period for searching moving pattern.
6. Check face picture analysis device in the list.

   Note

   The picture you upload in Step 7 will be compared with pictures stored in the checked devices.
7. Click **Select Picture** to select a face picture to upload or drag a picture to the picture area.

   Note

   You can upload a picture containing multiple face pictures from which you need to select one for comparison.
8. Drag the slider or enter a number to select a similarity.

   Note

   The client will search face pictures stored in the selected face picture analysis devices whose similarity with the uploaded picture is higher than the configured similarity, and then display the moving pattern of the matched person on the map.
9. Click **Search**.

   Moving pattern of the person who is similar to the uploaded picture is displayed on the map, the cameras captured pictures will be numbered showing the person's arriving order, and the capture records will be displayed on the left with the captured picture thumbnail displayed also.

10. **Optional:** Perform the following operation(s) after searching moving pattern.

Operation	Description
Filter Capture Records	Click and check **Show Last Record** to show the last record of every camera through the moving pattern.
View Person Related Videos and Pictures	Click a captured picture thumbnail to open the Capture Details window and you can view the detailed information of the picture you clicked. All pictures of the person captured by the camera will be displayed on the right. Select a captured picture to show its related video of 10 seconds on the left, including the 5 seconds before the capturing time and the 5 seconds after the capturing time. Click to start displaying the video.
Disable Pattern	Click on the top of the record list or **Disable Pattern** to exit moving pattern mode.

Chapter 10 Statistics

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In this software, reports can be generated daily, weekly, monthly, annually, and by custom time period. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

10.1 People Counting Report

People counting statistics is to calculate the number of line crossing people in a specific area and a certain time period by the people counting camera(s) or abnormal event detection server(s), which can help the storekeeper to analyze the customers flow and number in different time, and the storekeeper can flexibly do some business adjustment according to the report.

10.1.1 People Counting Report by Encoding Device

People counting report by encoding device displays people counting data collected by encoding devices. You can search the people counting data in different dimensions.

Before You Start

Add an encoding device with people counting function to the software and properly configure the corresponding area and people counting rule. Refer to ***Add Device*** for details about adding people counting device.

Steps

1. Click **Report → People Counting** to enter People Counting page.
2. Select **Encoding Device** as the **Device Type**.
3. Select daily report, weekly report, monthly report, or annual report as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the number of people in each hour of one day.

   Weekly Report, Monthly Report and Annual Report

   As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in each day of one week, in each day of one month, in each month of one year.

   Custom Report

   Users can customize the days in the report to analyze the number of people in each day or month of the custom time interval.

Note

You can select no more than 31 days on the calendar.

4. Select the statistics time type and click to set the time.

One Period

Generate the statistics in one time period.

Multiple Periods

Generate the statistics in two time periods, which can help you to compare the people flow and number in two time periods.

For example, if you set the report type as month report, and set the March and April as the statistic time, the people counting results in March and April will be displayed in a same chart with different color, and you can compare the data in different day of each month.

5. Select **Statistics Type**.

Display by Device

Display the report by device.

For example, if you select one NVR (with 4 people counting cameras), the report will display the total number of people summed by the 4 people counting cameras.

Display by Camera

Display the report by camera.

For example, if you select one NVR (with 4 people counting cameras), the report will display the each camera's statistics respectively, namely display the statistics in 4/8 colors (each one or two colors representing one camera).

Display by Grouping Statistics

Display the report by grouping statistics.

For example, if you select one device group (the group is created on the Client), the report will display the total number of people summed by the total people counting cameras in the group.

Note

- For details of device group, refer to ***Group Resources*** .
- This function should be supported by the device.

6. Select filtering mode.

Channel

Display people counting data collected by channels of an encoding device.

Region

Display number of people in selected regions of a camera.

Note

You need to configure regions for the camera beforehand. See user manual of the device for details.

7. Select camera(s) or region(s) from the **Camera** list.
8. Set the content to be displayed.

Direction

Calculate the number of people in different directions, such as enter, exit, or enter and exit.

Enter

The people entered will be counted.

Exit

The people exited will be counted.

Enter and Exit

Both people entered and exited will be counted.

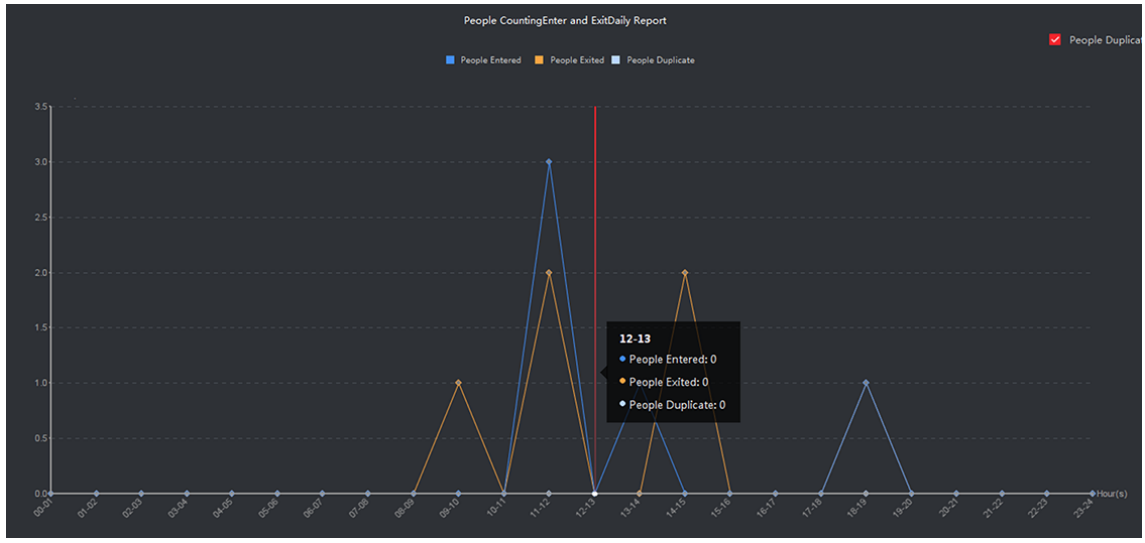


Figure 10-1 People Counting by Direction

Facial Features

Generate the report based on the facial feature.

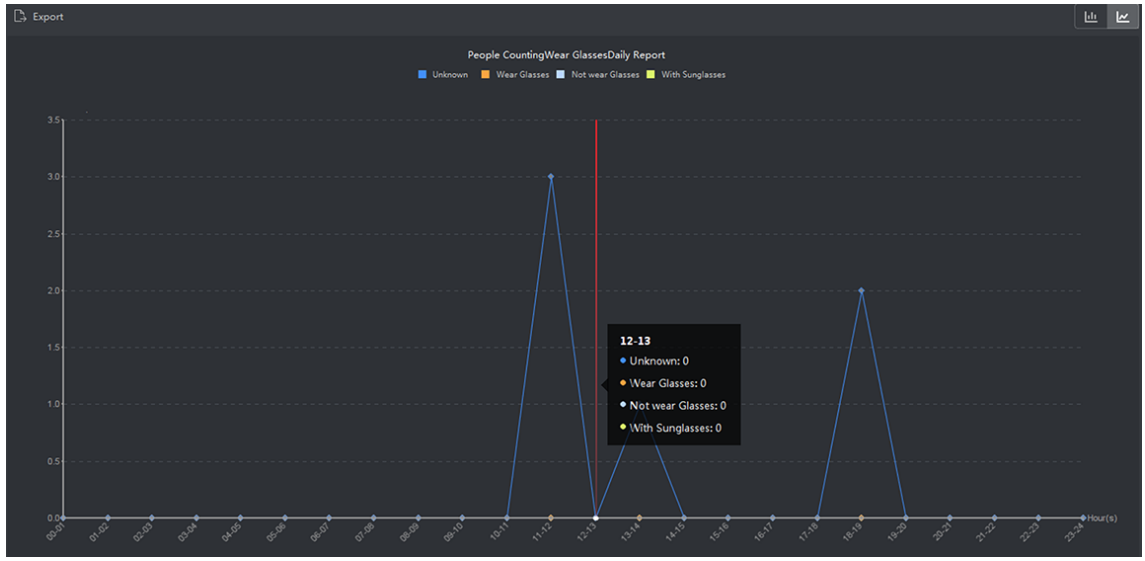


Figure 10-2 People Counting by Facial Features

9. **Optional:** Check **Children Only** to generate report of recognized children.

Note

- The client counts detected people shorter than a predefined height which can be configured on device's remote configuration page. See the device user manual for details about configuring height threshold.
- This function needs to be supported by the device.

10. Click **Search** to get the people counting statistics and detailed data for each hour, day, or month.

    By default, the statistics are shown in histogram form.

11. **Optional:** For the report by direction, you can check **People Duplicate** on the right-upper corner of the report page to display the number of duplicate people.

Note

The number of duplicate people is calculated by the device. If the same face is recognized more than once, he/she will be calculated as duplicate person.
For example, if a cashier enter or exit the supermarket more than once, he/she will be calculated as duplicate person. In this way, the supermarket can get the actual number of people shopping.

12. **Optional:** Perform the following operations after search.

Switch to Line Chart	Click to switch it to line chart.

Note

By default, the statistics are shown in bar chart.

Switch to Bar Chart	Click to switch it to bar chart.
Save to Local PC	Click **Export** to save the detailed data of people counting to your PC.

10.1.2 View People Counting Report by DeepinMind Server

People counting data by DeepinMind server are data counted based on predefined calculation rules. Data not conformed to the calculation rules will be omitted in the people counting report. This gives you more accurate people counting data.

Before You Start

Add a DeepinMind server to the software and properly configure a calculation rule. See ***Add Device*** for details about adding a DeepinMind server. See the device user manual about configuring calculation rule.

Steps

1. Click **Report → People Counting** .
2. Select **DeepinMind Server** as the device type.
3. Select hourly report, daily report, monthly report, or annual report as the report type.

   Hourly Report

   Hourly Report can be used for analyzing people counting data generated during peak time.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the number of people in each hour of one day.

   Monthly Report and Annual Report

   Compared with daily report, monthly report and annual report can be less time consuming, since they are not submitted every day. The system will calculate the number of people in each day of one month and in each month of one year.
4. Click to select time.
5. Select a calculation rule.
6. Select the content to be displayed.

   Direction

   Calculate the number of people moving in different directions, including enter, exit, and enter & exit.

   Enter

   The number of people entered will be displayed.

   Exit

   The number of people exited will be displayed.

   Enter and Exit

   The number of people entered and exited will be displayed.

7. Click **Search** to get the people counting data of each minute, hour, day, or month.

Note

By default, the report will be shown in a line chart.

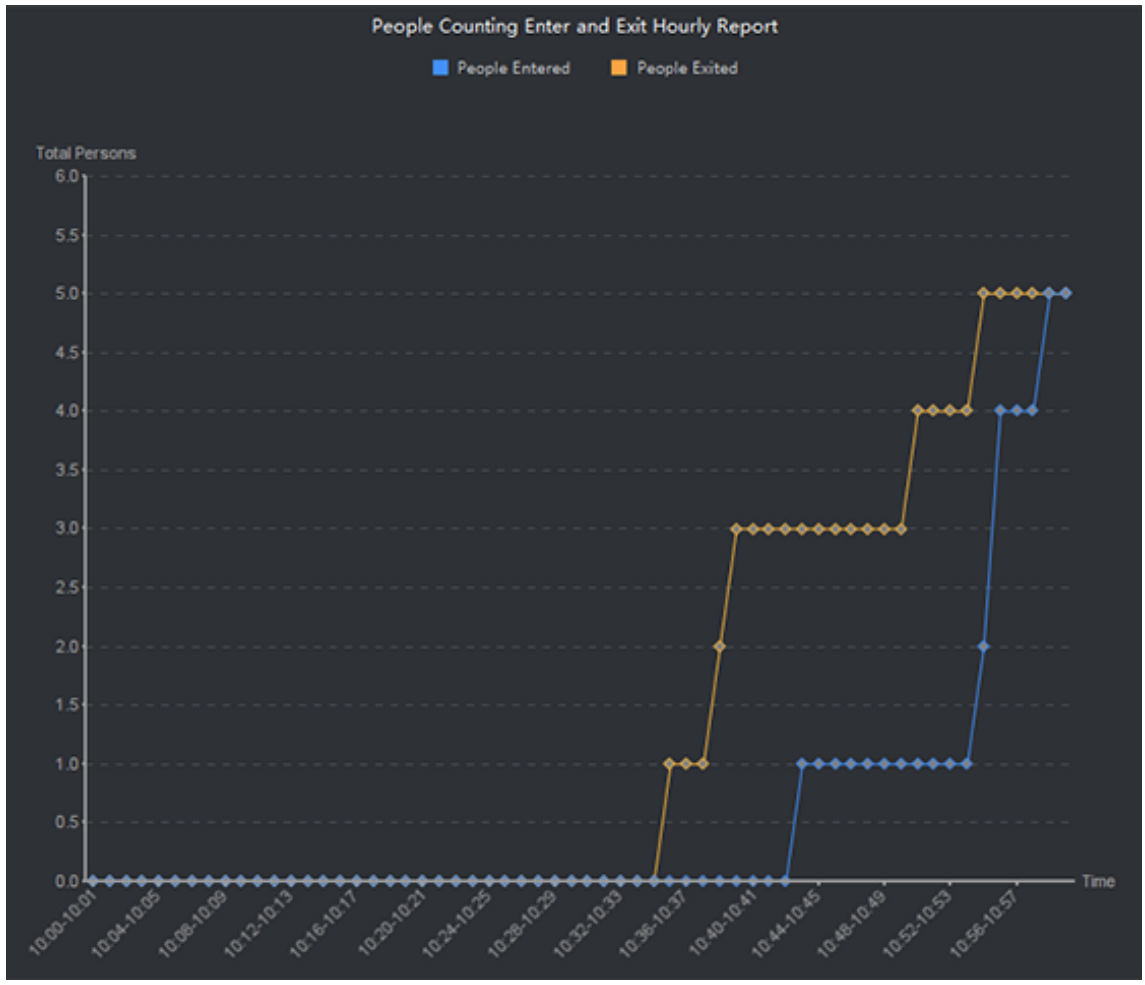


Figure 10-3 People Counting Report by DeepinMind Server

8. **Optional:** Click **Export** to save the report to your PC.

10.2 View People Counting in Intersections Report

Intersection analysis is used to monitor people flow and number in an intersection-like scene. The arrows in the image refer to different directions. By selecting one direction (e.g. A) as the entrance, the other directions will be set as the exits by default, so that multiple paths are generated (e.g., A to A, A to B, A to C, and A to D). You can view the people counting who passed by each path, respectively, which can help the shopkeeper to analyze the people flow in different door. The statistics result can show in daily, weekly, monthly, and annual report.

Before You Start

Make sure a fisheye camera which supports intersection analysis function has been configured properly and be added to the software. Refer to ***Add Device*** for details about adding the device.

Steps

Note

Up to 10 intersections can be analyzed.

1. Click **Report → Intersection Analysis** to enter the intersection analysis module.
2. Select daily report, weekly report, monthly report, or annual report as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the number of people in intersection report in a each hour of one day.

   Weekly Report, Monthly Report and Annual Report

   As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the number of people in intersection report in each day of one week, in each day of one month, in each month of one year.
3. Set the start time for the report.
4. Select the camera for generating the report.
5. Select one direction as the entrance from the drop-down list in the **Flow in** filed.
6. Click **Search** to get the statistics result.

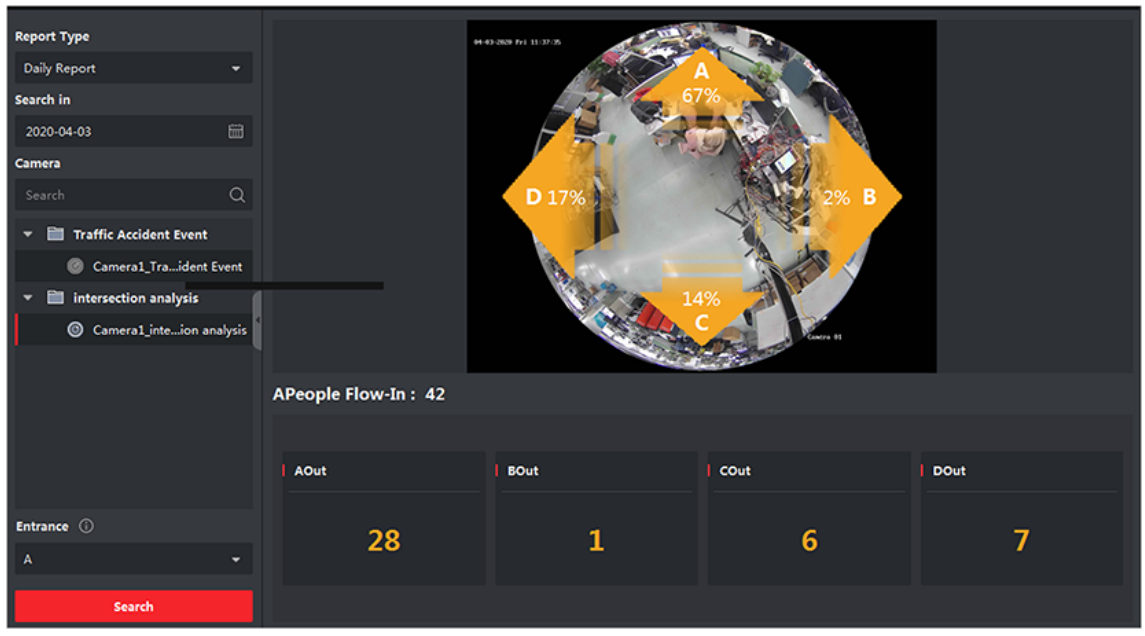


Figure 10-4 Results

The people number for each path will show on the right.

10.3 Queue Management

Queue management supports data analysis and report output from multiple dimensions.

Commonly Used Data Analysis

- To see queuing-up people number of a certain waiting time level in a queue/region, use queuing-up time analysis, check a target region and set a waiting time level.
- To compare queuing-up people number of a certain waiting time level in multiple queues/regions, use queuing-up time analysis, check target regions and set a waiting time level.
- To compare queuing-up people number of different waiting time levels in multiple queues/regions, use queuing-up time analysis, check target regions and set waiting time levels.
- To see the time and duration that a queue stays a certain length in a queue/region, use queue status analysis, check a target region and set a queue length level.
- To compare the time and duration that a queue stays a certain length in multiple queues/regions, use queue status analysis, check target regions and set a queue length level.
- To compare the time and duration that a queue stays at different length in multiple queues/regions, use queue status analysis, check target regions and set queue length levels.

10.3.1 Queuing-Up Time Analysis

Queuing-Up Time Analysis calculates people number of different waiting time levels. Regional comparison and multiple waiting time level comparison are supported.

Compare Queuing-up People Amount for Different Regions

With cameras for queuing-up people amount counting, you can search the queuing-up people amount during time period of certain length in different regions, helping the storekeeper to find areas where customers tend to go. For example, the regions with larger people amount are more popular than the regions with lower people amount, so that you can put goods in these regions to sell more of them.

Before You Start

- Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.
- Make sure you have configured no more than 3 regions in the detection area of a camera on device remote configuration page. See device user manual for details about configuring regions.

Steps

Note

This function should be supported by the connected device.

1. Click **Report → Queue Management → People Amount in Region** .

2. Select **Daily Report**/**Weekly Report**/**Monthly Report**/**Custom Report** as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different regions in a each hour of one day.

   Weekly Report, Monthly Report

   As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different regions in each day of one week, in each day of one month.

   Custom Report

   Users can customize the days in the report to analyze the number of people on each day or month of the custom time interval.

   Note

   You can select no more than 31 days on the calendar.

3. Click to set time period for searching.
4. Select cameras and no more than 3 regions for every camera in the **Region** list.
5. Select **Regional Comparison** as the statistics type.
6. Select a waiting time level based on which the report is generated.
7. Click **Search** to generate the statistics result.

   The line chart of the calculated people amount in the specified waiting time will show on the result area. The lines with different colors indicate the people from the selected regions.

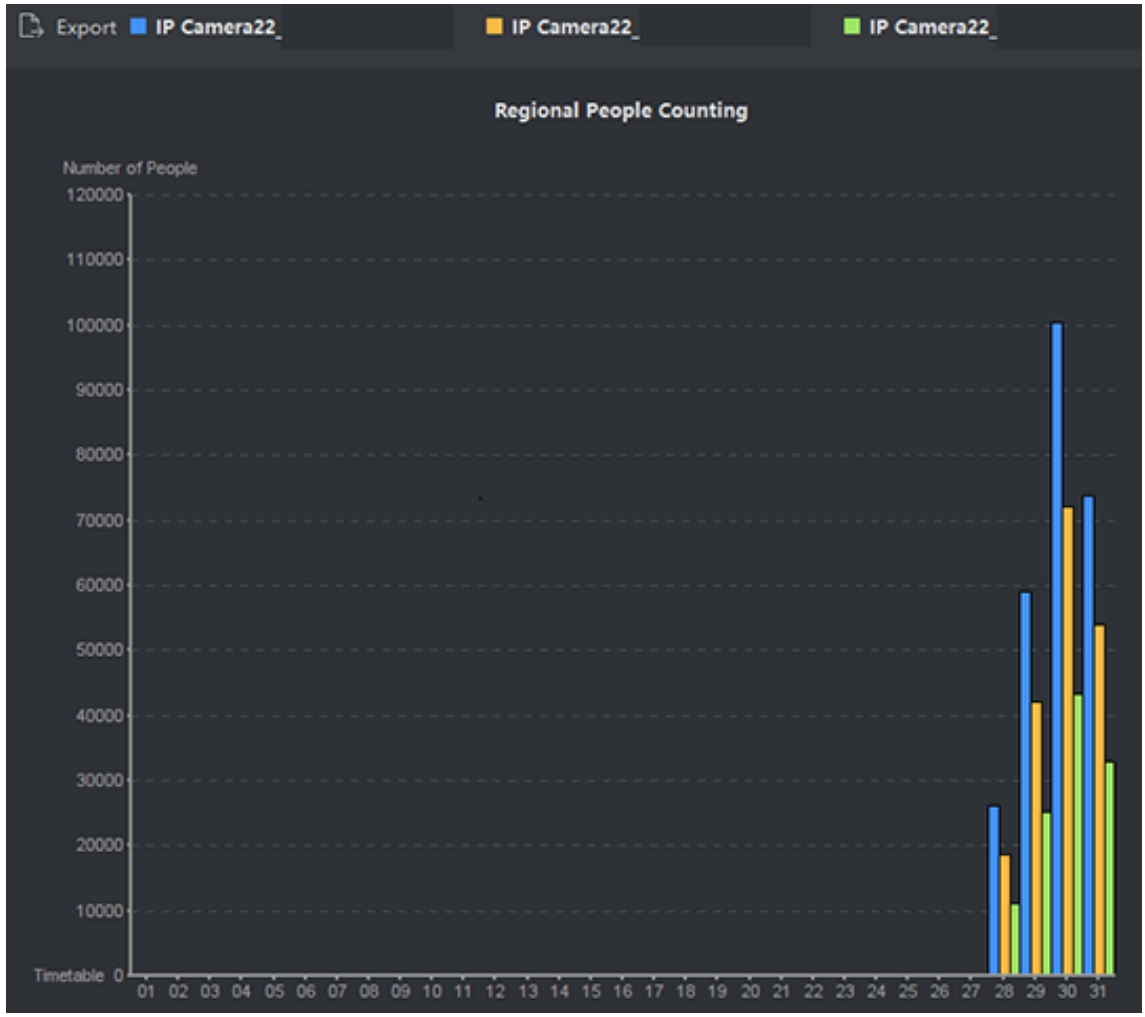


Figure 10-5 Result

8. Optional: Click **Export** to export the data in Excel file.

Compare Queuing-up People Amount for Different Waiting Time Levels

With cameras for queuing-up people amount counting, you can search the queuing-up people amount during time periods of different length in a certain region, helping analyzing perception of crowding in different regions to make it easy to know when and how to change service window amount, staff amount, and whether to set a guider for people, etc.

Before You Start

- Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.
- Make sure you have configured no more than 3 regions in the detection area of a camera on device remote configuration page. See device user manual for details about configuring regions.

Steps

Note

This function should be supported by the connected device.

1. Click **Report → Queue Management → Regional People Counting** .
2. Select **Daily Report/Weekly Report/Monthly Report/Custom Report** as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different regions in a each hour of one day.

   Weekly Report, Monthly Report

   As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different regions in each day of one week, in each day of one month.

   Custom Report

   Users can customize the days in the report to analyze the number of people on each day or month of the custom time interval.

   Note

   You can select no more than 31 days on the calendar.
3. Click to set time period for searching.
4. Select cameras and no more than 3 regions in the **Region** list.
5. Select **Multi-Level Comparison** as the statistics type.
6. Select the waiting time level and enter the seconds for calculating people amount waiting for the specified time period.
7. Click **Search** to generate the statistics result.

   The line chart of the calculated people amount in the same region will show on the result area. The lines with different colors match the waiting time levels.

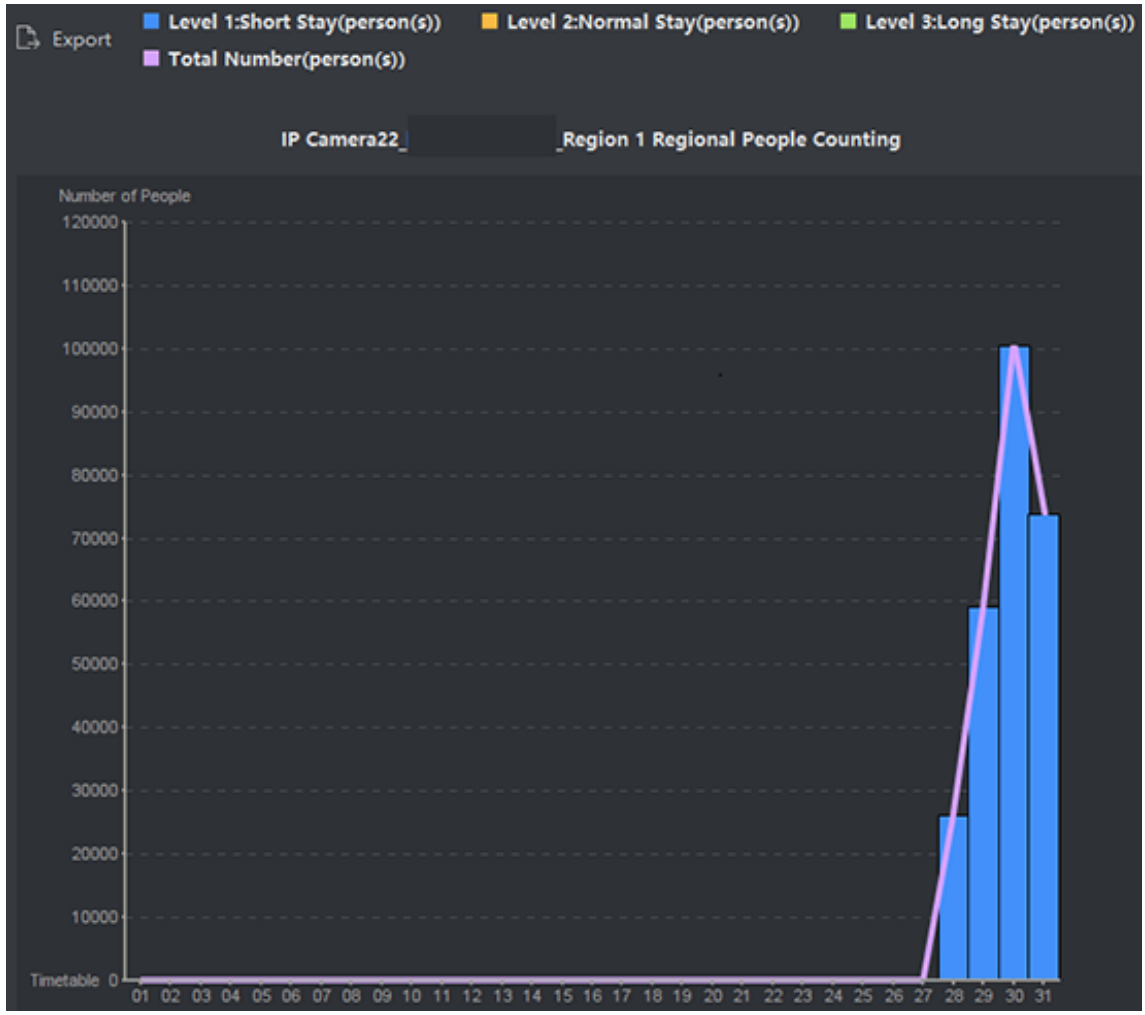


Figure 10-6 Result

8. Optional: Click **Export** to export the data in Excel file.

10.3.2 Queue Status Analysis

Queue Status Analysis calculates the time and duration that a queue stays with a certain length. Regional comparison and multiple queue length level comparison are supported.

Compare Queuing-up Duration for Different Regions

With cameras for queuing-up duration counting, you can search and compare the queuing-up durations in different regions during the same time period, helping analyzing perception of crowding in different regions to make it easy to know when and how to change service window amount, staff amount, and whether to set a guider for people, etc.

Before You Start

- Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.
- Make sure you have configured no more than 3 regions in the detection area of a camera on device remote configuration page. See device user manual for details about configuring regions.

Steps

Note

This function should be supported by the connected device.

1. Click **Report → Queue Management → Waiting Duration** .
2. Select **Daily Report**/**Weekly Report**/**Monthly Report**/**Custom Report** as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different regions in a each hour of one day.

   Weekly Report, Monthly Report

   As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different regions in each day of one week, in each day of one month.

   Custom Report

   Users can customize the days in the report to analyze the queuing-up duration on each day or month of the custom time interval.

   Note

   You can select no more than 31 days on the calendar.
3. Click to set time period for searching.
4. Select cameras and no more than 3 regions for every camera in the **Region** list.
5. Select **Regional Comparison** as the statistics type.
6. Set the length of queue based on which the report is generated.
7. Click **Search** to generate the statistics result.

   The line chart of the calculated duration for staying the specified queue length will show on the result area. The lines with different colors match the selected regions.

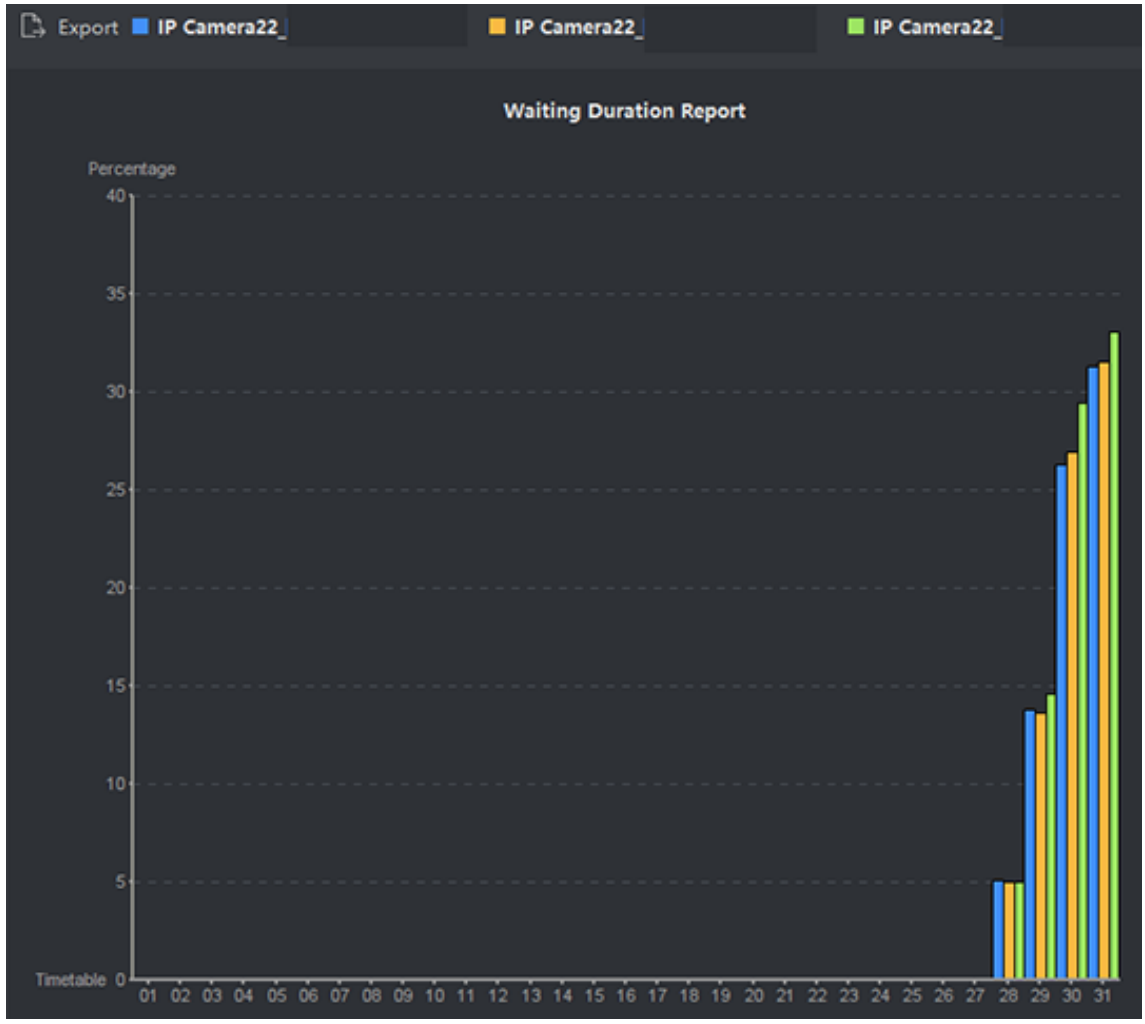


Figure 10-7 Result

8. **Optional:** Click **Export** to export the data in Excel file.

Compare Queuing-up Duration for Different Queue Length Levels

With cameras for queuing-up duration counting, you can search and compare the queuing-up durations of queues of different length during the same time period, helping analyzing perception of crowding in different regions to make it easy to know when and how to change service window amount, staff amount, and whether to set a guider for people, etc.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Report → Queue Management → Waiting Duration** .
2. Select **Daily Report/Weekly Report/Monthly Report/Custom Report** as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the queuing-up duration for different regions in a each hour of one day.

   Weekly Report, Monthly Report

   As compared to daily report, weekly report and monthly report can be less-time consuming, since they are not to be submitted every day. The system will calculate the queuing-up duration for different regions in each day of one week, in each day of one month.

   Custom Report

   Users can customize the days in the report to analyze the queuing-up duration on each day or month of the custom time interval.

   Note

   You can select no more than 31 days on the calendar.
3. Click to set time period for searching.
4. Select cameras and no more than 3 regions in the **Region** list.
5. Select **Multi-Level Comparison** as the statistics type.
6. Set the length of queue based on which the report is generated.
7. Click **Search** to generate the statistics result.

   The line chart of the calculated duration in the same region will show on the result area. The lines with different colors match the queue length levels.

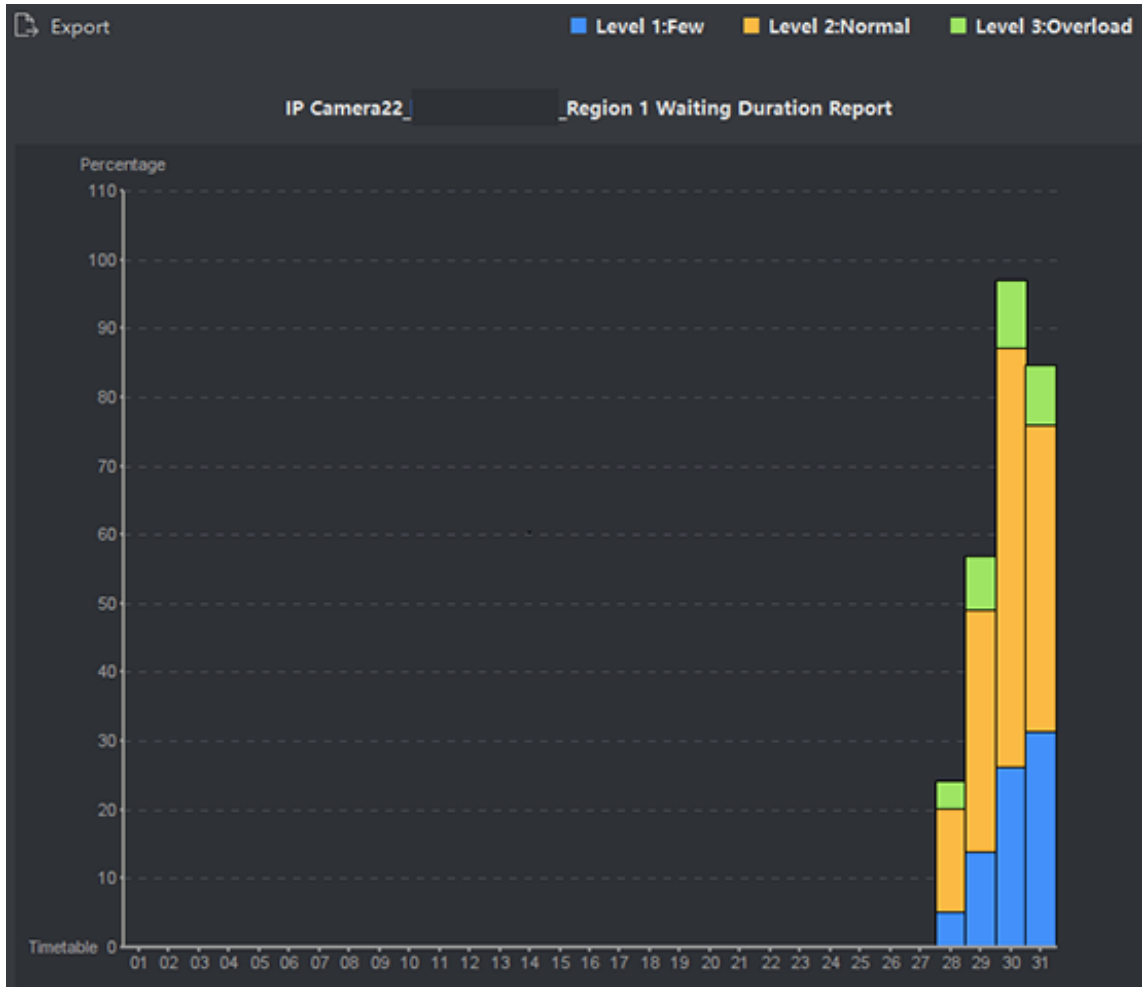


Figure 10-8 Result

8. **Optional:** Click **Export** to export the data in Excel file.

10.4 Heat Map

Heat map is a graphical representation of data represented by colors and the heat map data can be displayed in line chart. You can use the heat map function of the camera to analyze the visit times and dwell time of customers in a configured area, which can help the storekeeper analyze the customers' interested area and make the arrangement of goods.

Before You Start

Add a heat map network camera to the software and properly configure the corresponding area. The added camera should have been configured with heat map rule. See ***Add Device*** for details about adding heat map network camera.

Steps

1. Click **Report → Heat Map** to enter the heat map page.
2. Select **Daily Report**/**Weekly Report**/**Monthly Report**/**Annual Report**/**Custom Report** as the report type.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the data of heat map in a each hour of one day.

   Weekly Report, Monthly Report and Annual Report

   As compared to daily report, weekly report, monthly report and annual report can be less-time consuming, since they are not to be submitted every day. The system will calculate the data of heat map in each day of one week, in each day of one month, in each month of one year.

   Custom Report

   You can customize the days in the report to analyze the dwell time or crowd trend on each day or month of the custom time interval.

   Note

   The time period in the custom report should be no more than 31 days.

3. Select **By Dwell Time** or **By Crowd Trend** as the statistics type.

   By Dwell Time

   The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the people's dwell time.

   By Crowd Trend

   The system calculates the heat map value (the ordinate value in the line chart or the color in pictures) according to the number of detected people.
4. Set the time period for searching.
5. Select a heat map camera in the camera list.
6. Click **Generate Heat Map** to show the heat map of the camera.

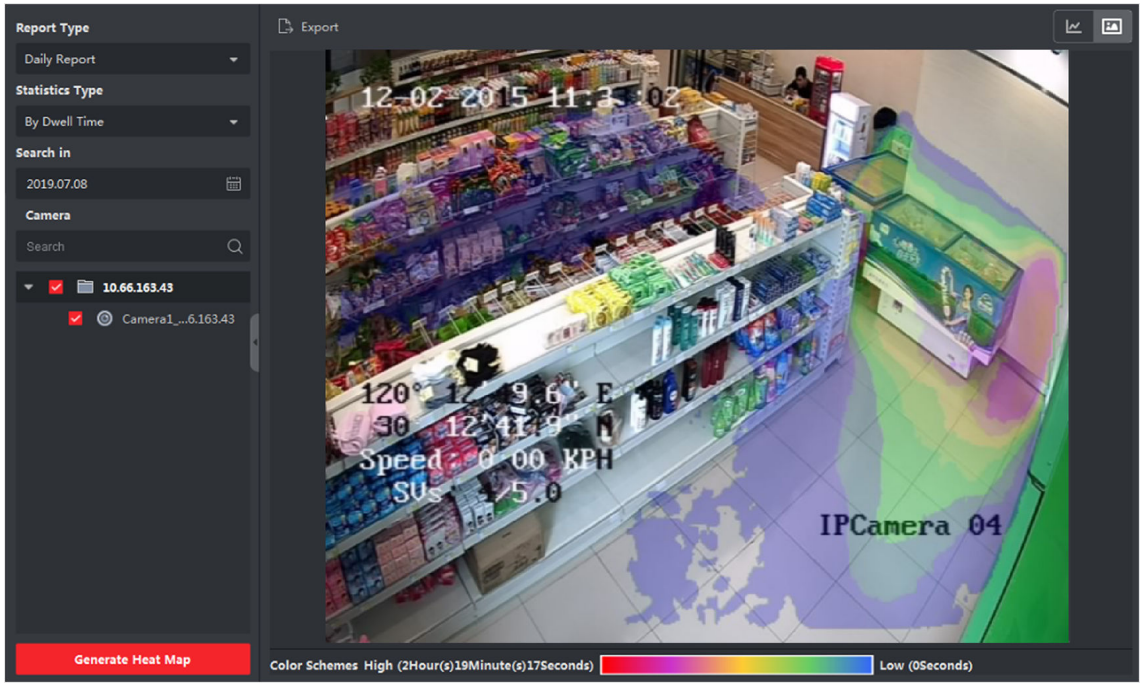


Figure 10-9 Results

7. **Optional:** After generating heat map report, you can perform the following operations.

Display in Line Chart	Click to display the statistics in line chart.
Display in Picture Mode	Click to display the statistics in picture mode. The red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.
Save Statistics Data	Click **Export** to save the detailed data of heat map to your PC.

10.5 Skin-Surface Temperature Statistics

The system can calculate the total number of people, the number of people whose skin-surface temperature is abnormal and the number of people who do not wear mask. The system provides the statistics report per day, per week and per month, to help you judge the trend of the number of people whose skin-surface temperature is abnormal and the number of people who do not wear mask.

Before You Start

Add the devices which support skin-temperature measurement, such as the intelligent device with face skin-temperature measurement function.

Steps

1. Select **Report → Skin-Surface Temperature**.

2. Select the report type by the drop-down list, including **Daily Report**, **Weekly Report**,**Monthly Report** or **Annual Report**.
3. Click to select the time range.
4. Select a camera, device or group.
5. Click **Search**.

   Display the report in histogram on the right area.

Note

The **All**、**Abnormal**、**No Mask** and **Normal Skin-Surface Temperature** is displayed on the upper area of the report, you can select the detection attribute(s) to be displayed.

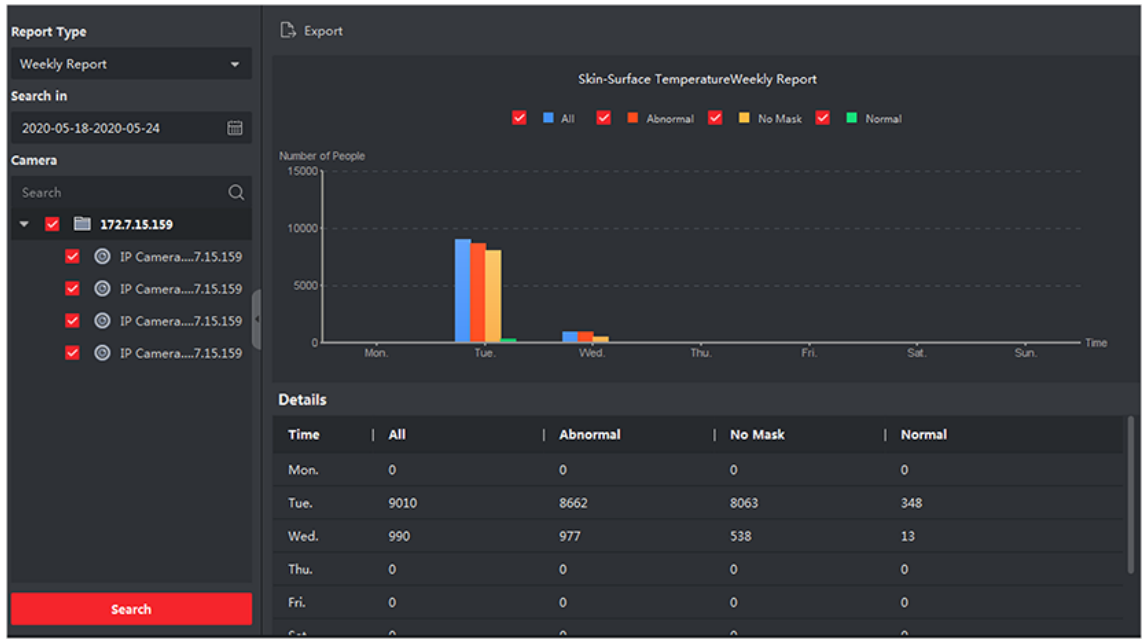


Figure 10-10 Report of Skin-Surface Temperature Statistics

6. **Optional:** Click **Export** to save the data in local by CSV format.

10.6 Real-Time Density and People Counting

Real-time density and people counting supports generating people density analysis report and real-time people counting report.

Before You Start

Add a DeepinMind server to the software and properly configure a calculation rule. See ***Add Device*** for details about adding a DeepinMind server. See the device user manual about configuring calculation rule.

Steps

1. Click **Report → Real-Time Density and People Counting** .

2. Select hourly report, daily report, monthly report, or annual report as the report type.

   Hourly Report

   Hourly Report can be used for analyzing data generated during peak time.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the number of people in each hour of one day.

   Monthly Report and Annual Report

   Compared with daily report, monthly report and annual report can be less time consuming, since they are not submitted every day. The system will calculate the number of people in each day of one month and in each month of one year.
3. Click to select time.
4. Select event type.

   People Density Analysis

   The density of people in an area at different times.

   Real-Time People Counting

   The numbers of people in an area at different times.
5. Select a calculation rule.
6. Click **Search**.

Note

By default, the report will be shown in a line chart.

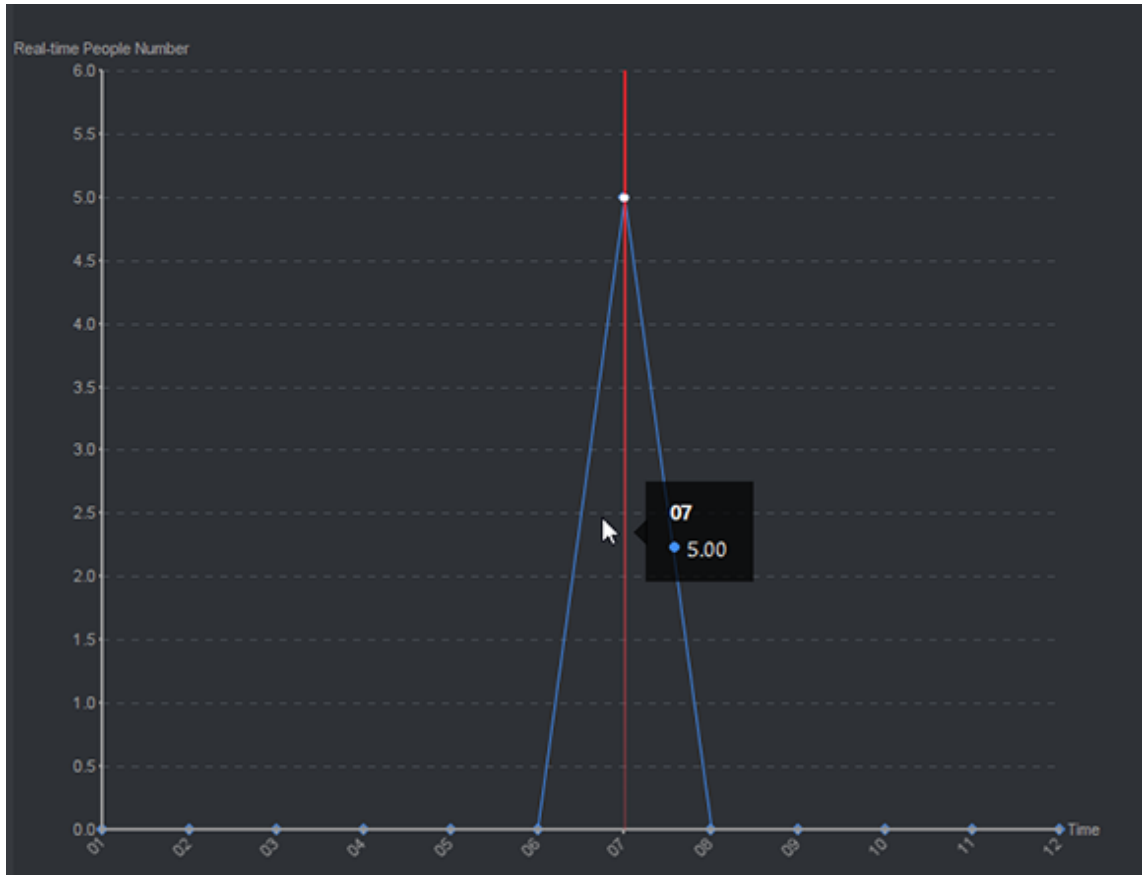


Figure 10-11 People Density Analysis Report

7. **Optional:** Click **Export** to save the report to your PC.

10.7 Temperature Map

A temperature map displays the temperature trend of a region during a certain day. If you have configured temperature monitoring regions, you can generate temperature map of specific regions to see the overview of each region's temperature trend.

Before You Start

- Make sure you have drawn regions for temperature map on the device configuration page. See user manual of the device for details.
- Make sure you have added at least one device for temperature map to the client. See ***Add Device*** for details.

Steps

Note

This function should be supported by device.

1. Click **Report → Temperature Map** .
2. Select a date from the calendar.
3. In the Camera list, select a camera.

Note

You can enter a keyword in the searching field to search a camera.

4. Select a unit.
5. Select a preset.



Figure 10-12 Temperature Map

6. On the right panel, check region(s) for generating the report.

Note

No more than 8 regions can be checked.

7. Click **Search**.

   The temperature map will be displayed in a line chart with each line representing a region.
8. **Optional:** Select another unit to display the temperature map in another unit.

Chapter 11 Data Retrieval

In the Data Retrieval module, you can search the face pictures captured by the face recognition camera, search the human body pictures captured by DeepinMind device, view abnormal event detection related pictures and videos, search the vehicle pictures captured by DeepinMind device, search the frequently appeared person pictures captured by DeepinMind device, and search the not wearing hard hat pictures.

11.1 Video Search

You can search for videos by time period and specified cameras. After search, you can export the matched video files to the local PC.

Steps

1. Click **Data Retrieval → Video Search** to enter the Video Search page.
2. Set search conditions.

   Search By

   By Time

   Search by specified the time period, you should set the start and end time.

   By Event Type

   Search by specified event type, you should set the event type and start/end time.

   By Tag

   Search by specified tags, you should set the tag type and start/end time.

   Note

   If you select **Custom** as the tag type, you should set the corresponding tag name.

   Camera

   Select a device from the camera list.

   Note

   You can enter a key word (supports fuzzy search) in the search box to quickly search for the target device.
3. Click **Search** to start searching.

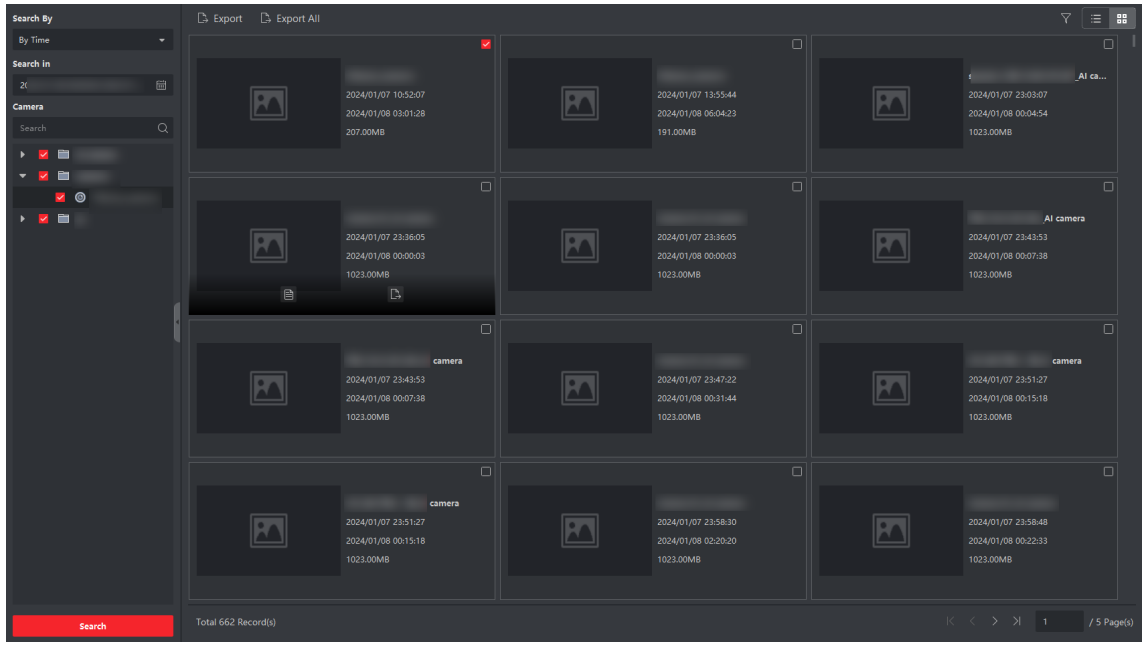


Figure 11-1 Video Search

The videos which meet the search conditions are displayed on the right panel.

4. **Optional:** Perform the following operations if needed.

Export Video Footage	• Hover on the target video, click to export the single video. • Check target videos and click **Export** to export the videos to the local PC. • Click **Export All** to export
View Video Details	Hover on a target video, click to view the video details.
Filter	Click to filter the videos by camera.
Switch Display Mode	Click or to display the videos by thumbnails or by list.

11.2 Target Retrieval

Target retrieval (AcuSearch) can quickly locate and extract targets, including face retrieval, human retrieval, vehicle retrieval, and search by picture.

11.2.1 Face Picture Retrieval

When the connected device (e.g. NVR or HDVR) supports face search, you can search the related picture and play the picture related video file.

Search Face Pictures by Uploaded Picture

You can upload a face picture from your PC and compare the uploaded picture with the captured face pictures.

Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval → Face Picture Retrieval** to enter the face picture retrieval page.
2. Click to set the start time and end time for searching the captured face pictures or video files.
3. Select device(s) in the camera panel.
4. Select **Picture** from the drop-down list.
5. Select a face picture for search.
   1) Click **Select Picture** to upload the pictures from your PC.
   2) Select a detected face from uploaded picture for matching the captured face pictures.

   Note

   - The resolution of the picture should be smaller than 4096×4080.
   - Only JPG and JPEG formats are supported.
6. Set the similarity level.

   Example

   If you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded face picture will list.
7. Set the maximum number of displayed results.
8. Click **Search** to start searching.

   The search results of the pictures are displayed on the right.
9. Export the pictures and save them in your PC.

   Export Picture

   Select the pictures to be exported and save them in local PC.

   Export Current Page

   Export all the pictures in the current page.

   Export Segment

   You can download the pictures by packages. Each package contains up to 1,000 pictures.

   Export All

   Export all searched pictures.

10. Select a searched face picture to show the captured picture and person information.



Figure 11-2 Result

11. Optional: After searching, you can do one or more the following operations.

View Details	View the captured face picture, and the person information (similarity, temperature status, captured time, etc.) on the page. You can also click to show the large picture, and click to restore.
Play Related Videos	Click to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right. **Note** • You can click to show the large video, and click to restore. • You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window. • You can click to view the captured picture.
Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, or capture details of single record to local PC.
Add Picture to Face Picture Library	Click to add the captured picture to the face picture library.

Note

You can select the face picture library and enter the person information for the captured picture, such as person name, mobile phone, etc.

12. **Optional:** Perform secondary search based on the search result.
    1) In the person information page, click .

       All the faces in this picture will be analyzed and displayed.
    2) In the pop-up window, move the red frame to select a face you want to do secondary search.

       Note

       If there are multiple faces in the picture, the window will pop up for selecting.
       If there is only one face in the picture, skip this step.
    3) Click **OK**.

       The client will search and compare the faces in the captured pictures based on the face picture you selected.

Search Face Pictures by Event Type

You can search the device's captured face pictures by filtering different event types.

Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval → Face Search** to enter the face picture retrieval page.
2. Click to set the start time and end time for searching the captured face pictures or video files.
3. Select device(s) in the camera panel.
4. Select **Event Type** from drop-down list to search by event type.
5. Select event type.

   No Limit

   Search all captured face pictures.

   Matched Face

   Search the captured pictures the face in which matched with the face in face library.

   Mismatched Face

   Search the captured pictures the face in which mismatched with the face in face library.

   Stranger Detection Alarm

Search the pictures captured when the stranger detection alarm is triggered.

6. Set the maximum number of displayed results.
7. Click **Search** to start searching.

   The search results of the pictures are displayed on the right.
8. Export the pictures and save them in your PC.

   Export Picture

   Select the pictures to be exported and save them in local PC.

   Export Current Page

   Export all the pictures in the current page.

   Export Segment

   You can download the pictures by packages. Each package contains up to 1,000 pictures.

   Export All

   Export all searched pictures.
9. Select a searched face picture to show the captured picture and person information.

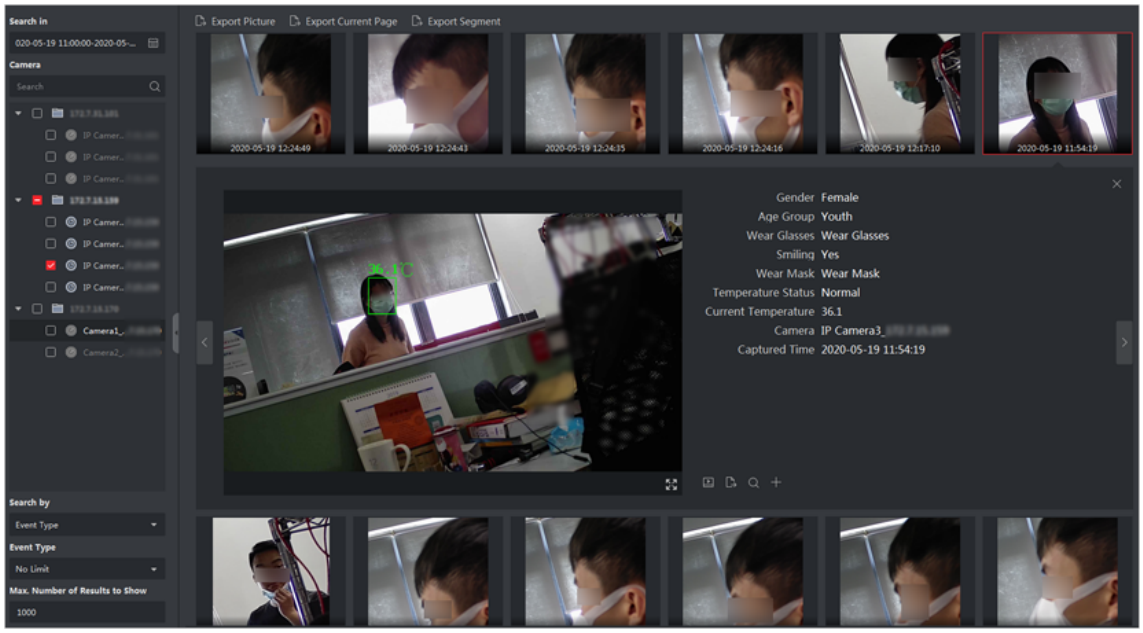


Figure 11-3 Result

10. **Optional:** After searching, you can do one or more the following operations.

View Details	View the captured face picture, and the person information (similarity, temperature status, captured time, etc.) on the page. You can also click to show the large picture, and click to restore.
Play Related Videos	Click to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to show the large video, and click to restore.
- You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window.
- You can click to view the captured picture.

Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, or capture details of single record to local PC.
Add Picture to Face Picture Library	Click to add the captured picture to the face picture library. **Note** You can select the face picture library and enter the person information for the captured picture, such as person name, mobile phone, etc.

11. **Optional:** Perform secondary search based on the search result.
    1) In the person information page, click .
       All the faces in this picture will be analyzed and displayed.
    2) In the pop-up window, move the red frame to select a face you want to do secondary search.

       Note
       If there are multiple faces in the picture, the window will pop up for selecting.
       If there is only one face in the picture, skip this step.
    3) Click **OK**.
       The client will search and compare the faces in the captured pictures based on the face picture you selected.

Search Face Pictures by Person Name

You can search the device's captured face pictures by person name.

Before You Start
Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Steps

Note
This function should be supported by the connected device.

1. Click **Data Retrieval → Face Search** to enter the face picture retrieval page.
2. Select device(s) in the camera panel.

3. Select **Name** from the drop-down list to search by person name.
4. Click to set the start time and end time for searching the captured face pictures or video files.
5. Enter a keyword for the person name.
6. Set the maximum number of displayed results.
7. Click **Search** to start searching.

   All the persons whose name match the search condition (fuzzy match is supported) will be displayed.

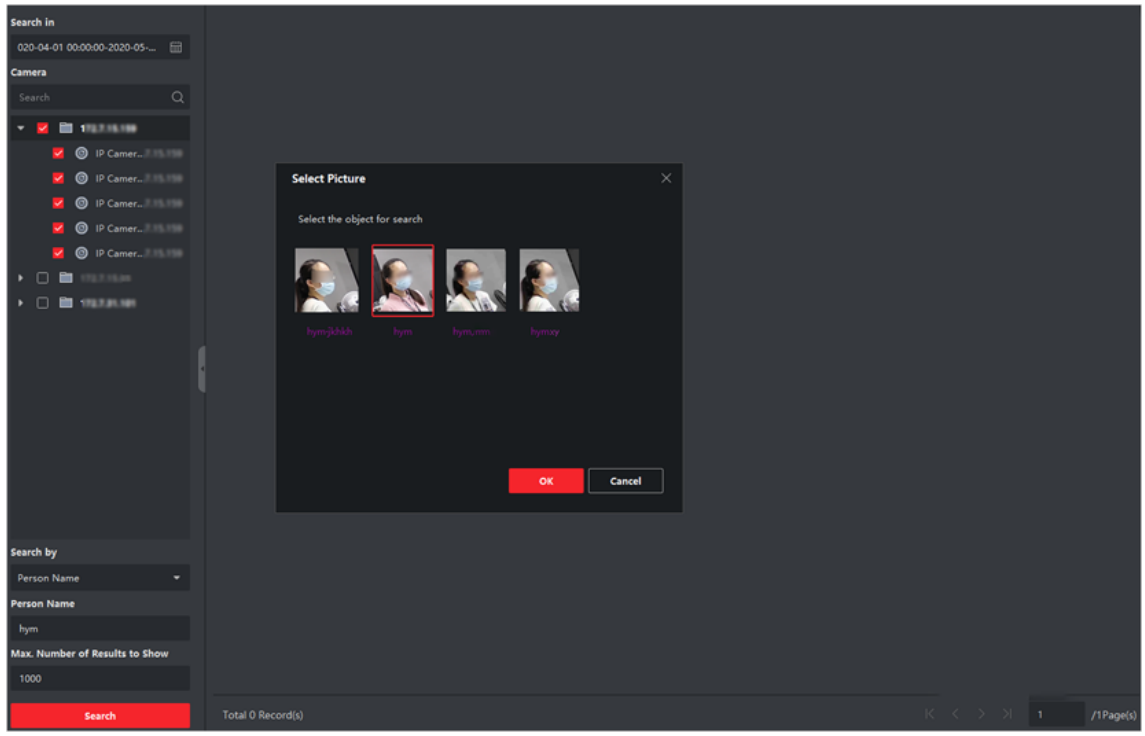


Figure 11-4 Results

8. Select one picture to search, and then click **Confirm**.

   The search results of the pictures are displayed on the right.
9. Export the pictures and save them in your PC.

   Export Picture

   Select the pictures to be exported and save them in local PC.

   Export Current Page

   Export all the pictures in the current page.

   Export Segment

   You can download the pictures by packages. Each package contains up to 1,000 pictures.

   Export All

   Export all searched pictures.
10. Select a searched face picture to show the captured picture and person information.

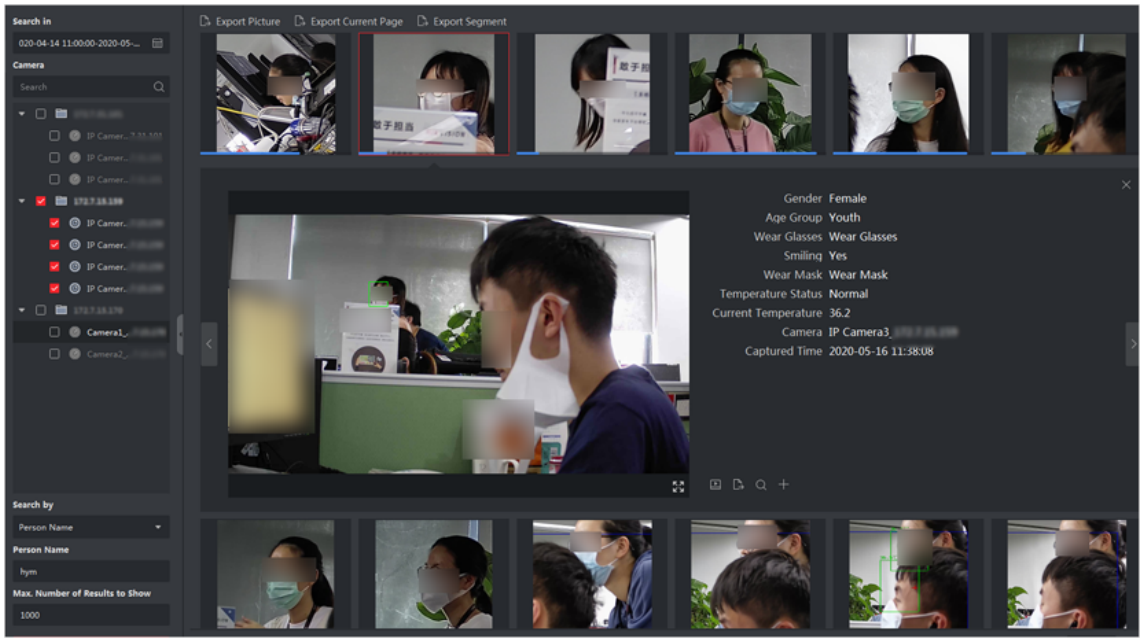


Figure 11-5 Results

11. Optional: After searching, you can do one or more the following operations.

View Details

View the captured face picture, and the person information (similarity, temperature status, captured time, etc.) on the page.

You can also click to show the large picture, and click to restore.

Play Related Videos

Click to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to show the large video, and click to restore.
- You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window.
- You can click to view the captured picture.

Export Single Record

In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, or capture details of single record to local PC.

Add Picture to Face Picture Library

Click to add the captured picture to the face picture library.

Note

You can select the face picture library and enter the person information for the captured picture, such as person name, mobile phone, etc.

12. **Optional:** Perform secondary search based on the search result.
    1) In the person information page, click .
       All the faces in this picture will be analyzed and displayed.
    2) In the pop-up window, move the red frame to select a face you want to do secondary search.

       Note

       If there are multiple faces in the picture, the window will pop up for selecting.
       If there is only one face in the picture, skip this step.
    3) Click **OK**.
       The client will search and compare the faces in the captured pictures based on the face picture you selected.

Search Face Pictures by Facial Features

The client supports searching detected face pictures by facial features.

Steps

1. Click **Data Retrieval → Face Picture Retrieval** .
2. Select a time period for searching.
3. Select a camera in the camera list.
4. Select **Facial Features** as the searching type.
5. Configure facial features to be searched, including wear glasses, smiling and wear mask.
6. Enter the maximum number of results to show.
7. Click **Search**.
   The searched face pictures are displayed on the right.
8. Export the pictures and save them in your PC.

   Export Picture

   Select the pictures to be exported and save them in local PC.

   Export Current Page

   Export all the pictures in the current page.

   Export Segment

   You can download the pictures by packages. Each package contains up to 1,000 pictures.

   Export All

   Export all searched pictures.
9. **Optional:** Select a searched face picture to show the captured picture and person information.

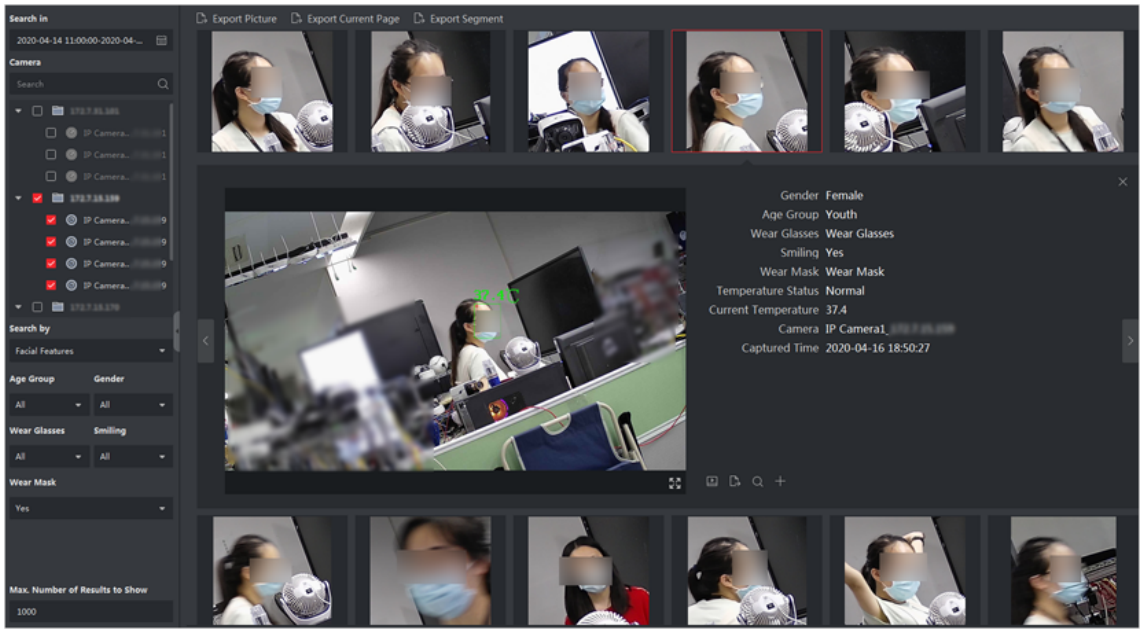


Figure 11-6 Result

10. **Optional:** After searching, you can do one or more the following operations.

View Details	View the captured face picture, and the person information (similarity, temperature status, captured time, etc.) on the page. You can also click to show the large picture, and click to restore.
Play Related Videos	Click to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right. **Note** • You can click to show the large video, and click to restore. • You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window. • You can click to view the captured picture.
Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, or capture details of single record to local PC.
Add Picture to Face Picture Library	Click to add the captured picture to the face picture library. **Note** You can select the face picture library and enter the person information for the captured picture, such as person name, mobile phone, etc.

11. **Optional:** Perform secondary search based on the search result.
    1) In the person information page, click .
       All the faces in this picture will be analyzed and displayed.
    2) In the pop-up window, move the red frame to select a face you want to do secondary search.

       Note

       If there are multiple faces in the picture, the window will pop up for selecting.
       If there is only one face in the picture, skip this step.
    3) Click **OK**.
       The client will search and compare the faces in the captured pictures based on the face picture you selected.

11.2.2 Human Body Retrieval

For the DeepinMind device, you can search the captured human body pictures by setting search conditions including uploading a picture from local PC and setting features, and view related videos of the picture.

Search Human Body by Uploaded Picture

For the DeepinMind device, you can upload a human body picture from local PC and compare the uploaded picture with the device's captured human body pictures, or search all the human body pictures captured by the specific camera(s) during a specific time.

Before You Start
Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval → Human Body Retrieval** to enter the human body retrieval page.
2. Click to set the start time and end time for searching the captured human body pictures or video files.
3. Select device(s) in the camera panel.
4. Select the search condition in the Search by field.

   Picture

   Upload a picture to compare the uploaded picture with the device's captured human body pictures. All the human bodies in this picture will be analyzed and displayed.

   a. Click **Select Picture** to select a picture for comparison from the computer.

Note

- The picture should be smaller than 4 MB.
- The resolution of the picture should be smaller than 4096*4080.
- Only JPG and JPEG formats are supported.

b. Set the similarity level. For example, if you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded human body picture will list.

All

Search all the pictures captured by the selected camera(s) during the time duration.

5. Set the maximum number of displayed results.

Note

If the number of pictures captured by the selected cameras(s) during the selected time duration exceeds the number of maximum number to be displayed, only the lasted pictures will be displayed.

For example, if the number of pictures captured by the selected cameras during the selected time duration is 2000, and the maximum number to be displayed is 1000, only the lasted 1000 pictures will be displayed.

6. Click **Search** to start searching.

The search results of the pictures are displayed in list.

7. **Optional:** Perform secondary search based on the search result

1) Move to the searched picture and click

All the human bodies in this picture will be analyzed and displayed.

2) Select a human body you want to do secondary search.
3) Set the similarity and time period.
4) Click **Search**.

The client will search and compare the human bodies in the captured pictures based on the human body picture you selected.

8. **Optional:** After searching human body, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click to show the large picture, and click to restore.
Play Related Videos	Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to show the large video, and click to restore.
- You can click 1x to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable audio, double-click the playback window to maximize the window.

Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, and capture details of single record to local PC.
Export Segments of Pictures	For the searched pictures, you can click **Export Segment**, then select the range (segmented by every 1000 pictures, e.g., 1 to 1000, 1001 to 2000) to export the pictures in batch.

Search Human Body by Personnel Features

You can search the device's captured human body pictures by setting the personnel features as the search conditions.

Before You Start

Add the device to the software and properly configure the corresponding settings. Refer to ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Click **Data Retrieval → Human Body Retrieval** to enter the human body retrieval page.
2. Click to set the start time and end time for searching the captured human body pictures or video files.
3. Select device(s) in the camera panel.
4. Select **Features** as the search mode.
5. Set the person features such as top's color, wearing glasses or not, etc.
6. Select the event type of the human body pictures you want to search.
7. Set the maximum number of displayed results.
8. Click **Search** to start searching.

   The search results of the pictures are displayed in list.
9. **Optional:** Perform secondary search based on the search result
   1) Move to the searched picture and click .

      All the human bodies in this picture will be analyzed and displayed.
   2) Select a human body you want to do secondary search.
   3) Set the similarity and time period.
   4) Click **Search**.

      The client will search and compare the human bodies in the captured pictures based on the human body picture you selected.
10. **Optional:** After searching, you can do one or more the following operations.

View Details	Click on a picture from the list to view details. You can also click to show the large picture, and click to restore.

Play Related Videos	Click to play the picture's related video file in the view window on the bottom right. **Note** • You can click to show the large video, and click to restore. • You can click to adjust the play speed of the playback, click to play back the video files frame by frame, click to enable the audio, double-click the playback window to maximize the window.
Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, or capture details of single record to local PC.
Export Segments of Pictures	For the searched pictures, you can click **Export Segment**, then select the range (segmented by every 1000 pictures, e.g., 1 to 1000, 1001 to 2000) to export the pictures in batch.

11.2.3 Vehicle Retrieval

For devices that support vehicle retrieval, you can search the related vehicle pictures and videos by setting the search conditions such as plate number and captured time.

Before You Start

Add the device that supports vehicle retrieval to the client and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Vehicle Retrieval** to enter the vehicle retrieval page.
2. Click to set the start time and end time for search.
3. Select the search type.

Vehicle

Search and display the captured vehicle pictures by entering the vehicles' license plate number.

Mix-traffic Detection

Search and display the mix-traffic detection related pictures of the specific vehicle by entering the vehicle's license plate number.

Note

The camera should support mix-traffic detection.

Traffic Violations

Search and display the traffic violation related pictures of the specific vehicle by entering the vehicle's license plate number.

Note

The camera should support traffic violation.

4. Select a device from the camera list.

Note

You can enter a key word (supports fuzzy search) in the search box to quickly search the target device.

5. **Optional:** Check **Vehicle Features** and select the related vehicle features such as brand and color from drop-down list to search vehicles with specific features.

Note

This function should be supported by the device. For different devices, you can search different vehicle features.

6. **Optional:** Enter the license plate number (support fuzzy search) for search.
7. **Optional:** Set the maximum number of searched results to be displayed.
8. Click **Search** to start searching.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
9. **Optional:** Perform the following operations if needed.

Export Picture	You can export one or more searched pictures. a. Click **Export Picture**. b. Check one or more picture(s), or check **Select All** on the page below. c. Click **Export** to export the selected picture(s) to local PC.
View Capture Details	Click a picture to view its capture details such as captured time and camera name. **Note** You can click to view an enlarged picture.
Play Related Video	Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window. **Note** • You can click to view the video in a larger window. • You can click to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.
Export Single Record	In the enlarged picture page, click and then click **Export Picture**, **Export Video File** or **Export Details** to export the picture, video file, and capture details of single record to local PC.

11.2.4 Search Target Pictures by Picture

Searching target pictures by picture uses recognition and retrieval tech to swiftly find specific targets. It supports face, human, and vehicle picture uploads for search.

1. Go to **Data Retrieval → AcuSearch → Search by Picture** .
2. Select **Time** and **Channel**.
3. Select a picture to upload for analysis. Suitable for searching faces, individuals, and vehicles.
4. Click on the target frame to search.
   Green frames are for faces, blue frames for bodies, and orange frames for vehicles.
5. After jumping to the search results page, you can perform the following operations:
   - Filter: Sort by similarity, time, favorites, etc.
   - Export: Including exporting pictures, exporting current page, and exporting all.
   - View Target Pictures: Click the target picture to view the playback. You can click to conduct a secondary analysis.

11.3 Abnormal Event Detection

After adding the device that supports abnormal event detection, you can search the related events such as line crossing, people gathering and loitering in the client. You can view the event details including the captured pictures and related videos.

Before You Start

Add the device that supports abnormal event detection to the client and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Abnormal Event Detection** to enter the abnormal event detection page.
2. Click to set the start time and end time for search.
3. Select the search type as camera, task or rule from the drop-down list.

   Camera

   Search and display abnormal event detection related information detected by the camera.

   Task

   Search and display the results according to the tasks you have added for the abnormal event detection server.

   Rule

   Search and display the results according to the rules you have configured for a task of the abnormal event detection server.

Note

Searching by task and rule should be supported by the device. You should have added tasks to the abnormal event detection server and configure related rules for the tasks. For each task, you can configure multiple rules such as line crossing and region entrance.

4. Select a search method.
   - When selecting **Camera** as the search type, select a camera from the camera list.
   - When selecting **Task** as the search type, select a task or a abnormal event detection server from the task list.
   - When selecting **Rule** as the search type, select a rule from the rule list.

Note

You can enter a key word in the search box (supports fuzzy search) to quickly find the target camera, task, or rule.

5. **Optional:** Check **False Alarm Deduction** to remove the false alarms from the results.

   Example

   The camera might sometimes take tree-shaking as a motion detection alarm or take an animal as a person triggering line crossing alarm probably for high sensitivity, which will be taken as false alarms by an NVR or DVR.
6. **Optional:** Select one or more event types from the drop-down list for search.

Note

You can skip this step if you select **Rule** in step 3.

7. Click **Search** to start searching.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
8. **Optional:** For the searched pictures, you can perform the following operations.

Export Picture	You can export one or more searched pictures. a. Click **Export Picture**. b. Check one or more picture(s), or check **Select All** on the page below. c. Click **Export** to export the selected picture(s) to local PC.
Export Segments of Pictures	For the searched pictures, you can click **Export Segment**, then select the range (segmented by every 1000 pictures, e.g., 1 to 1000, 1001 to 2000) to export the pictures in batch.
View Capture Details	Click a picture to view its capture details such as captured time and camera name. **Note** You can click to view an enlarged picture.

Play Related Video	Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window.

Note

- You can click to view the video in a larger window.
- You can click 1x to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.

11.4 Hard Hat Retrieval

After adding the hard hat detection device to the client, when the device detects a person who doesn't wear a hard hat, it will trigger an event and capture some pictures to notify the managers. You can search the alarm pictures in which the detected person doesn't wear a hard hat. By this way, you can remind the builders to wear hard hats, and thus to improve builders' safety awareness.

Before You Start

Add the device(s) with hard hat detection function to the client. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Hard Hat Search** to enter the hard hat search page.
2. Click to set the start time and end time for search.
3. Select the camera for search.

   Note

   You can enter a key word (support fuzzy search) in the search box to quickly search the target camera(s).
4. **Optional:** Select the hard hat detection status.
5. **Optional:** Select the face picture comparison result.

   Note

   When selecting the results of succeeded face picture comparison, you can search by the person name or the face picture library.
6. **Optional:** Set the maximum number of searched results to be displayed.
7. Click **Search**.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
8. **Optional:** Perform the following operations if needed.

Export Picture	You can export one or more searched pictures.

a. Click **Export Picture**.
b. Select one or more picture(s), or check **Select All** on the page below.
c. Click **Export** on the page below to export the selected picture(s).

View Capture Details

Click a picture to view its capture details such as captured time and camera name.

Note

You can click to view an enlarged picture.

Play Related Video

Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to view the video in a larger window.
- You can click to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.

11.5 People Frequency Search

People frequency refers to the appearance frequency of a person happened in the detection area during a certain period of time. Frequently appeared person refers to a person whose appearance frequency exceeds the predefined threshold, while rarely appeared person refers to a person whose appearance frequency is lower than the predefined threshold. The client supports searching frequently appeared people to protect places requiring high security and rarely appeared people who may be in trouble if they rarely appear during a certain time period.

11.5.1 Search Frequently Appeared Person

The person's captured face picture can be compared with the face pictures in the face picture library. If mismatched, he/she will be judged as frequently appeared person, and trigger an event to notify the security person. For example, in some high-safety demanded scene (e.g. bank), if a stranger appears frequently, the event can be triggered to notify the security personnel or related person. If matched, he/she will be judged as a person in allowlist and will not trigger frequently appeared person alarm. You can search the event information in a certain time, such as the captured pictures, captured time, and you can view the detailed pictures and play back the related video.

Before You Start

Make sure the frequently appeared person alarm has been configured on the device.

Steps

1. Click **Data Retrieval → People Frequency Search → Frequently Appeared Person** .

2. Set the start time and end time for searching.
3. Select the device(s) for searching.
4. Click **Search**.

   The frequently appeared person alarm related pictures will be displayed on the right panel.

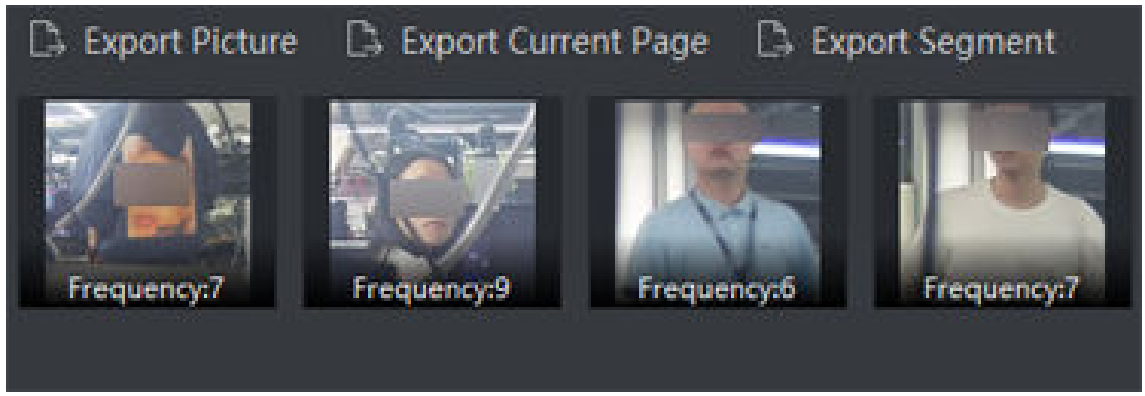


Figure 11-7 Results

5. **Optional:** Click the picture to view the whole captured picture, the captured time, etc.
6. **Optional:** Export the picture(s) to the local PC.
   - Click **Export Picture**, and then select the picture to be exported, and then click **Export**.
   - Click **Export Current Page** to export all the pictures and information on the current page.
   - Click **Export Segment** to download the pictures and capturing information by packages. Each package contains up to 1,000 pictures.
7. **Optional:** Perform the following operations if needed.

Add to Face Picture Library	Click **Add to face picture library** to add current face picture to the library .
View Detailed Information	Click **View** to view the historical captured pictures of this person, the captured time.
Playback	Click **Playback** to play back the video of 5-seconds before and after the capturing time.
Export	Click the picture to be exported, and then click **Export** to export this picture.

11.5.2 Search Rarely Appeared Person

The device will send rarely appeared person report to the client regularly giving information including who did not appear for enough times so that security persons will know on time and go to check the person. This function is often used for seniors living alone and prisoners. If they have not appear for a period of time, security persons need to find them and confirm they are not in trouble or escaped.

Before You Start

- Make sure the frequently appeared person alarm has been configured on the device.
- Make sure you have configured detecting time, statistic period, frequency threshold, and face picture library on the device remote configuration page.

Steps

1. Click **Data Retrieval → People Frequency Search → Rarely Appeared Person** .
2. Set the start time and end time for searching.
3. Select the device(s) for searching.
4. Click **Search**.

   The rarely appeared person reports will be displayed on the right panel.

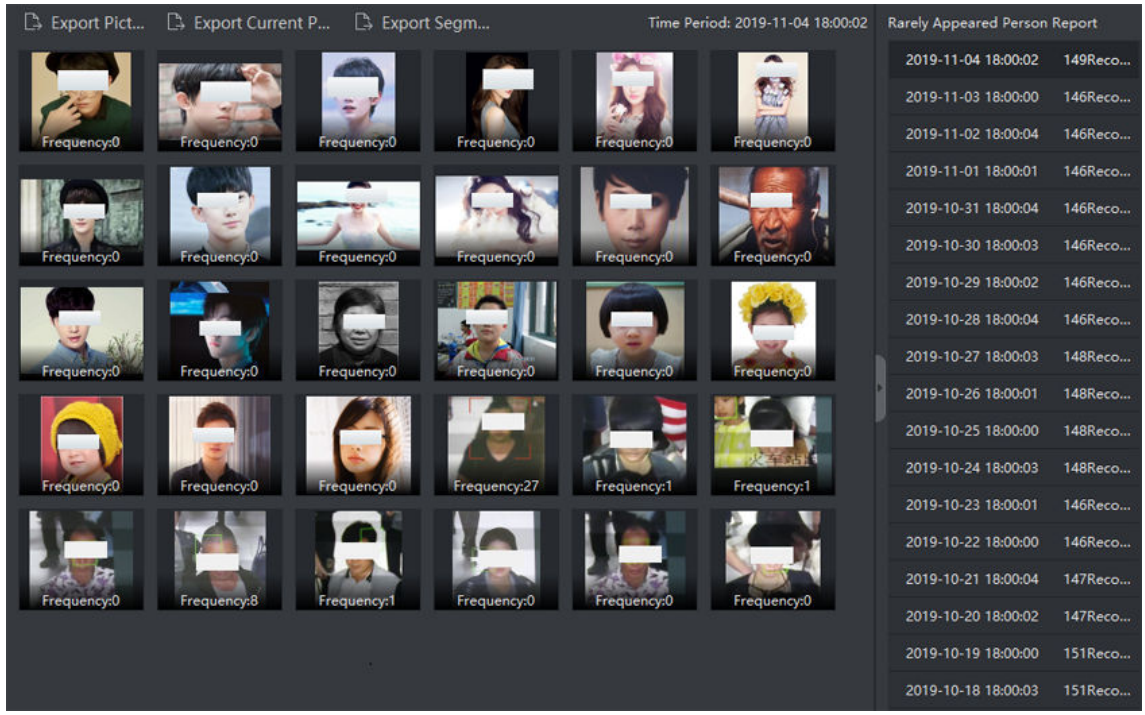


Figure 11-8 Result

5. Double-click a report to show the rarely appeared persons.
6. **Optional:** Click the picture to view the captured picture's details.
7. **Optional:** Export the picture(s) to the local PC.
   - Click **Export Picture**, and then select the picture to be exported, and then click **Export**.
   - Click **Export Current Page** to export all the pictures and information on the current page.
   - Click **Export Segment** to download the pictures and capturing information by packages. Each package contains up to 1,000 pictures.

11.6 AI Dashboard Retrieval

You can search result for video and captured picture task and imported picture task, to view the detailed information of the task.

Note

The video analysis task is only configured on web client, while picture analysis task can be configured on web client or control client.

11.6.1 Search Analysis Result for Video and Captured Picture Task

You can search result for video and captured picture analysis task, to view the related video and pictures.

Before You Start

Add the device that support AI Dashboard Platform to the platform.

Steps

1. Enter **Data Retrieval** module.
2. Select **AI Dashboard Retrieval**.
3. Click to set the time range for task searching.
4. Select **Video & Capture Analysis Task** as task type.
5. Select **Task** or **Camera** as the major type.
6. Select a task or camera.
7. Select one or multiple algorithms or device engines.
8. Click **Search**, and the task list will be displayed on the right area.

Note

If the device has been configured combined rule alarm, the combined rule will displayed on the result.

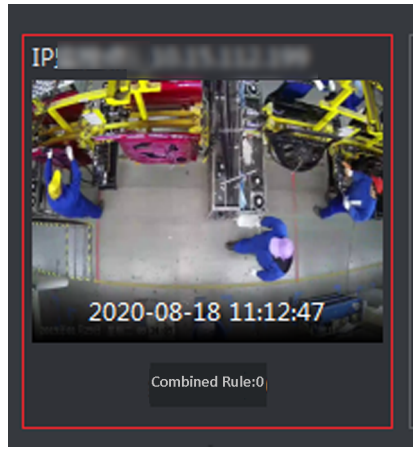


Figure 11-9 Combine Rule Alarm

9. **Optional:** Perform the following operations according to actual requirement.

Export Picture	Select the picture or information record on the right area and then click**Export Picture** to save the picture to the designed path.
Export Segments of Pictures	For the searched pictures, you can click **Export Segment**, then select the range (segmented by every 1000 pictures, e.g., 1 to 1000, 1001 to 2000) to export the pictures in batch.
View Details	Select one picture or information record and then click it to view the alarm information or video footage. **Note** The video is recorded 5 seconds before or after the capture time. Supports playing, pausing, single frame playing and volume adjusting.
Display Mode	Click or to display the task by thumbnails or by list.

11.6.2 Search Analysis Result for Imported Picture Task

You can search result for imported picture analysis task, to view the related picture files and picture information.

Before You Start

Add the device that support AI Dashboard Platform to the platform.

Steps

1. Enter **Data Retrieval** module.
2. Select **AI Dashboard Retrieval**.
3. Click to set the time range for task searching.
4. Select **Picture Importing Analysis Task** as task type.

5. Select **Task** or **Camera** as the major type.
6. Select a task or camera.
7. Select one or multiple algorithms or device engines.
8. Click **Search**.

   The task list is displayed on the right area.
9. **Optional:** Perform the following operations according to actual requirement.

Export Picture	Select the picture or information record on the right area and then click**Export Picture** to save the picture to the designed path.
Export Segments of Pictures	For the searched pictures, you can click **Export Segment**, then select the range (segmented by every 1000 pictures, e.g., 1 to 1000, 1001 to 2000) to export the pictures in batch.
View Picture Details	Select one picture or information record, click it to amplify the picture or tag information (such as vehicle).
Display Mode	Click or to display the task by thumbnails or by list.

11.7 Facial Recognition Check-in

For the device that supports facial recognition, the person can check in on the device by facial recognition. By comparing the recognized face with the face picture library, if matched, the system will record it as a successful face comparison record. If the successful face comparison record is during the check-in period, it will be regarded as a check-in record. Further more, the attendance records can also be calculated based on the successful face comparison records.

According to your requirement, you can search facial recognition check-in records or facial recognition attendance records.

11.7.1 Search Facial Recognition Check-in Records

You can search for the check-in records of the persons who checked in by facial recognition during the specified period and export the data to the local PC.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

Note

This function should be supported by the connected device.

1. Enter **Data Retrieval → Face Recognition Check-in → Check-In Search** .
2. Click to set the start time and end time for searching.

Example

If you need to search the check-in records in march, you can set the time as 2020-03-01--2020-03-31.

3. Set the **Check-In Period**.
4. Check cameras used for face recognition check-in.
5. Check one or multiple face picture libraries to search the persons attendance in the selected library.
6. Enter the maximum number of the results to show.
7. Click **Search** to start searching.

   The searched results show the attendance records including the face picture, face library, name, and check-in counts.

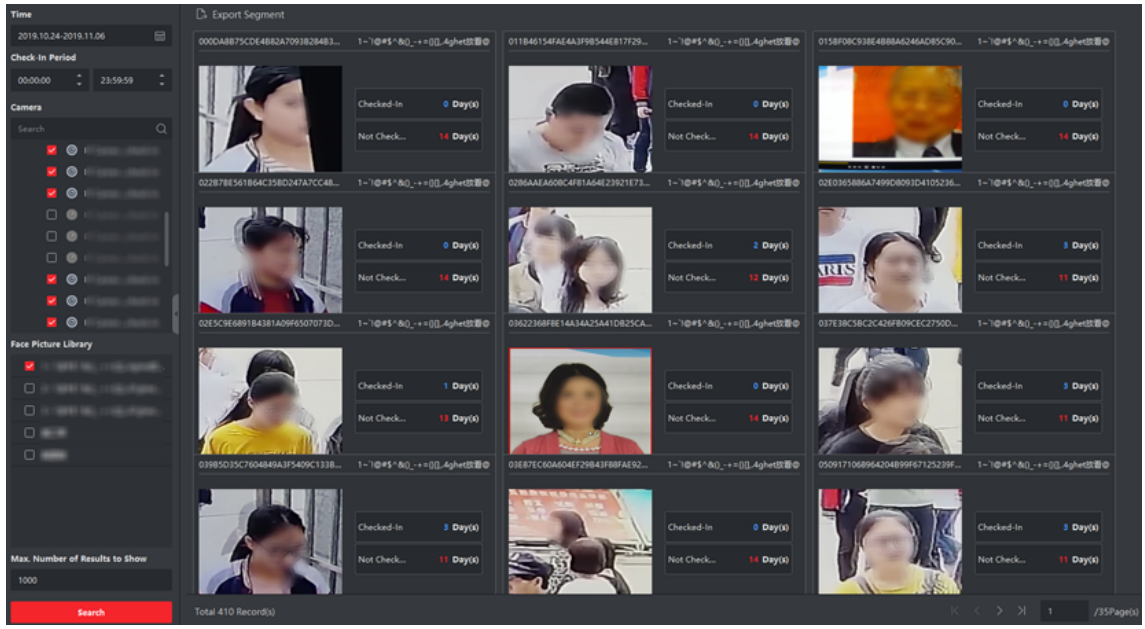


Figure 11-10 Result

8. **Optional:** Click **Export All** in the upper right corner to export the data to local PC.

11.7.2 Search Facial Recognition Attendance Records

You can search the attendance records of the persons who checked in by facial recognition. You can search the daily, monthly, yearly attendance records of the persons who checked in successfully on the face picture library to help you know the attendance status (normal, late, leave early or absent) of the staffs. Attendance status is the result calculated by comparing the check-in period on the search condition with the successful face comparison records (earliest and latest). You can export the attendance records to view the attendance data of the staffs.

Before You Start

Add the device to the software and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Select **Data Retrieval → Facial Recognition Check-in → Attendance Search** .
2. Set time range of records for searching.

   Example

   If you need to search the attendance records of march, you can set the time as 2020-03-01 - 2020-03-31.
3. Set the **Check-In Period**.

   Example

   If the **Check-in Period** is set as 08:00 - 17:00, the check-in earlier than 08:00 and check-out later than 17:00 will be regarded as normal attendance.
4. Select **Attendance Period** according to the work day.

   Example

   If the weekend is for rest, you can select Monday, Tuesday, Wednesday, Thursday and Friday as **Attendance Period**.
5. Select the camera for facial recognition check-in.

   Note

   You can only select the camera(s) in the same NVR.
6. Select the **Face Picture Library**.

   After selecting the face picture library, only the attendance records of the persons in the library will be searched. You configure the face picture library on the remote configure page of device, or log into the device to configure.
7. Set the Max. Number of Results to show.
8. Click **Search**.

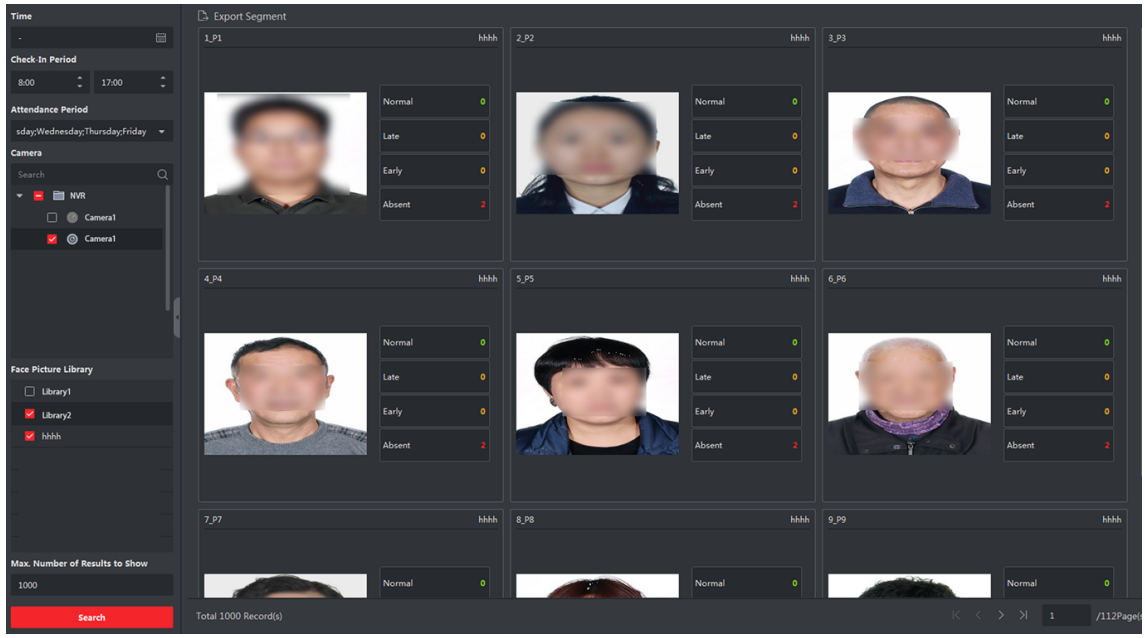


Figure 11-11 Face Recognition Attendance Search

Normal

The earliest check-in record (the earliest facial recognition comparison successful record) should not be later than the check-in start time, while the latest check-out record (the latest facial recognition comparison successful record) should not be earlier than the check-in end time.

For example, if the **Check-in Period** is set as 08:00 - 17:00, the check-in earlier than 08:00 and check-out later than 17:00 will be regarded as normal attendance.

Late

The check-in record (the earliest facial recognition comparison successful record) is later than the check-in start time.

If you set the **Check-in Period** as 08:00- 17:00, the check-in between 08:00-17:00 and check-out later than 17:00 will be regarded as late.

Leave Early

The check-out record (the latest facial recognition comparison successful record) is earlier than the check-in end time.

If you set the **Check-in Period** as 08:00- 17:00, the check-in earlier than 08:00 and check-out between08:00- 17:00 will be regarded as late.

Absent

If no facial recognition comparison successful record is found during the check-in period, the attendance record will be regarded as absent.

The searched results show the attendance records including face picture, face library, name and check-in counts.

9. **Optional:** Click **Export by Segment**, to export the attendance records to the local PC.

11.8 Community Inspection

For the added device that supports community inspection, you can search the captured pictures and the related video file for community related events, including fire engine access detection, elevator detection, and urban management event.

11.8.1 Detect Fire Engine Access

When the added device detects a place (such as the stairway and passage) where the fire engine access is occupied, an event will be triggered, and the device will capture pictures and videos. You can search and view the device's captured pictures and related videos via the client. This can help to remove the objects that occupy the fire engine access and perform rescue operations when a fire happens.

Before You Start

You should have added the device to the client and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Fire Engine Access Detection** to enter the fire engine access detection page.
2. Click to set the start time and end time for search.
3. Select a camera in the camera list.

Note

You can enter a key word (supports fuzzy search) in the search box to quickly find the target camera(s).

4. **Optional:** Set the maximum number of searched results to be displayed.
5. Click **Search** to start searching.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
6. **Optional:** For the searched pictures, you can perform the following operations.

Export Picture	You can export one or more searched pictures. a. Click **Export Picture**. b. Check one or more picture(s), or check **Select All** on the page below. c. Click **Export** to export the selected picture(s) to local PC.

View Capture Details

Click a picture to view its capture details such as captured time and camera name.

Note

You can click to view an enlarged picture.

Play Related Video

Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window.

Note

- You can click to view the video in a larger window.
- You can click to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.

11.8.2 Detect Elevator

When the added device detects an electric moped entering the elevator, an event will be triggered, and the device will capture pictures and videos. You can view the device's captured pictures and the related video in the client. This can help to ease the loading burden of elevators.

Before You Start

You should have added the device to the client and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Elevator Detection** to enter the elevator detection page.
2. Click to set the start time and end time for search.
3. Select a camera in the camera list.

   Note

   You can enter a key word (supports fuzzy search) in the search box to quickly find the target camera(s).
4. **Optional:** Set the maximum number of searched results to be displayed.
5. Click **Search** to start searching.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
6. **Optional:** For the searched pictures, you can perform the following operations.

   Export Picture

   You can export one or more searched pictures.

   a. Click **Export Picture**.
   b. Check one or more picture(s), or check **Select All** on the page below.
   c. Click **Export** to export the selected picture(s) to local PC.

View Capture Details	Click a picture to view its capture details such as captured time and camera name. **Note** You can click to view an enlarged picture.
Play Related Video	Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window. **Note** • You can click to view the video in a larger window. • You can click to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.

11.8.3 Retrieve Urban Management Event

After adding the device that supports urban management analysis, you can search the related events such as unregistered street vendor and packed package in the client. The event details include the captured picture and related video file. It is an intelligent way to help the urban management department to manage environment and improve the overall living quality of the city.

Before You Start

You should have added the device to the client and properly configure the corresponding settings. See ***Add Device*** for details about adding the device.

Steps

1. Click **Data Retrieval → Urban Management Event Retrieval** to enter urban management event retrieval page.
2. Click to set the start time and end time for search.
3. Select a camera in the camera list.

   Note

   You can enter a key word (supports fuzzy search) in the search box to quickly find the target camera(s).
4. Select an event type such as unregistered street vendor and packed package from the drop-down list for search.
5. **Optional:** Set the maximum number of searched results to be displayed.
6. Click **Search** to start searching.

   The captured pictures which meet the search conditions are displayed on the right panel. Up to 30 pictures can be displayed on one page.
7. **Optional:** For the searched pictures, you can perform the following operations.

Export Picture

You can export one or more searched pictures.

a. Click **Export Picture**.
b. Check one or more picture(s), or check **Select All** on the page below.
c. Click **Export** to export the selected picture(s) to local PC.

View Capture Details

Click a picture to view its capture details such as captured time and camera name.

Note

You can click to view an enlarged picture.

Play Related Video

Click **Playback** to play the picture's related video file (5s before and 5s after the capture) in the view window on the bottom right.

Note

- You can click to view the video in a larger window.
- You can click 1X to adjust the play speed of the playback, click to play back the video file frame by frame, and click to enable audio.

Chapter 12 AcuSeek

The AcuSeek's key features include:

- **Natural language search**: Enables open-ended queries (e.g., "a person in red clothing") to pinpoint targets instantly via text input.
- **Rapid object search**: Quick lookup of people, vehicles, objects, or animals.
- **Advanced filters**: Filters results by camera, time range, or similarity; supports playback, AcuSearch, and exporting target images.
- **AcuSeek Tuning**: When search results are not accurate enough, enable it to improve relevance.

Search

The AcuSeek supports instant searches for people/vehicles/objects/animals or text-based queries, boosted by smart recommendations and favorites for faster retrieval.

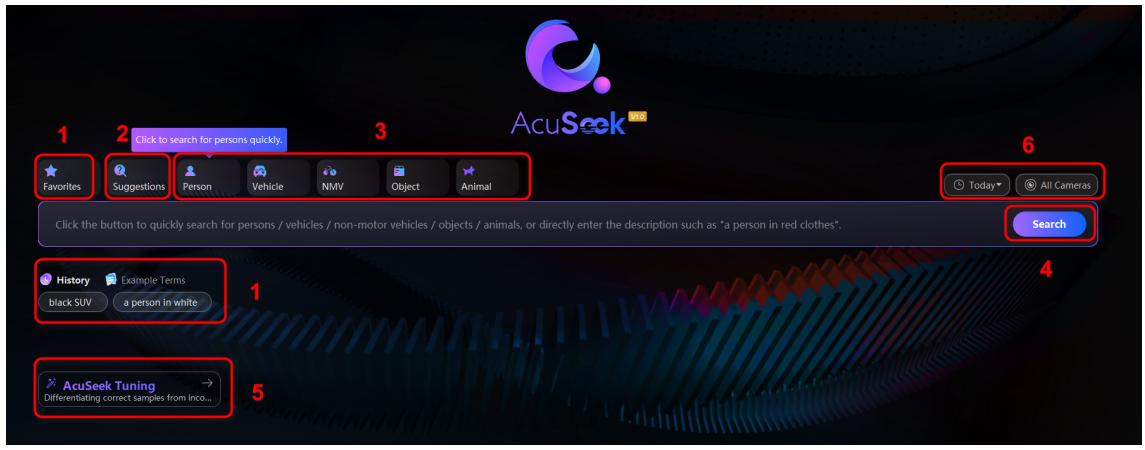


Figure 12-1 Search Page

Table 12-1 Introduction of Search Page

Number	Description
1	• **History**: Supports up to 20 records. You can hover the cursor on a record and click to add it to the Favorites. • **Favorites**: Displays favorite search records. You can click a favorite word to search. A maximum of 100 words are allowed in Favorites.
2	**Suggestions**: Provides words that you may also search for quick searches. For example, behaviors (making phone calls, using a mobile phone, etc.) and transportation methods (bicycle, shared bike, etc.).
3	Quickly find people, vehicles, objects, or animals. Vehicles can be searched by license plate number.

Number	Description
	Note Searching for objects or animals requires device support.
4	Enter keywords or a text description to locate specific targets, such as "a girl walking her dog".
5	**AcuSeek Tuning**: A fine-tuning feature to improve search accuracy. Label at least 4 correct and 6 incorrect samples from search results to initiate automatic fine-tuning training.
6	Filter by time and cameras.

View Search Results

After retrieving search results, you can filter them by similarity or time, view or export video clips containing the targets, or perform an image-based search. You can perform the following operations:

Export Images

Select one or more images, then click **Export** to save the selected images.

Use **Export Current Page** or **Export All** to save images to an Excel file, where the images will be presented as hyperlinks.

Note

Upon the first export, a usage statement will pop up: To better protect your rights and interests, please ensure that you abide by relevant laws and regulations when using the data you export, and do not infringe upon the legitimate rights and interests of other organizations or individuals.

View Videos

Click an image to view the video displayed on the top right.

AcuSearch

Hover the cursor on a video and click to perform an image-based search.

Click the red search box over the target to search for similar images across the channels selected on the top right.

Note

For animal search and object results, AcuSearch is not supported.

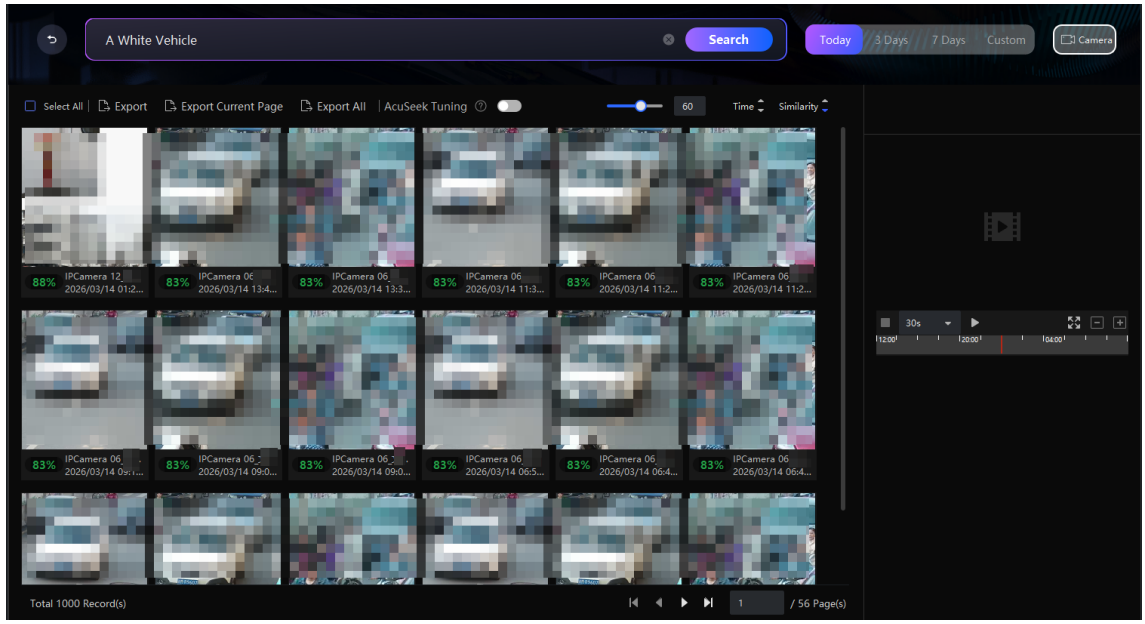


Figure 12-2 Search Results

AcuSeek Tuning

When search results are not accurate enough, enable **AcuSeek Tuning** to improve relevance. Follow the steps below:

1. **Enable AcuSeek Tuning**: Click to turn on the feature.
2. **Label Samples**: Mark search results as correct or incorrect. You need at least 4 correct and 6 incorrect labeled samples.
3. **Start Tuning**: After labeling, select **Start Tuning** in the upper-right corner. The system will begin fine-tuning and apply improvements immediately.

Note

You can click **View Labeled Pictures** to check, modify, or delete labeled samples.

4. **Enable or Disable Tuning**: Tuned entries are marked with . Click it to toggle: = enabled; = disabled.
5. **Manage Tuned Terms**: Access **AcuSeek Tuning** from the main page to view all tuned terms You can delete them or restart tuning by clicking .

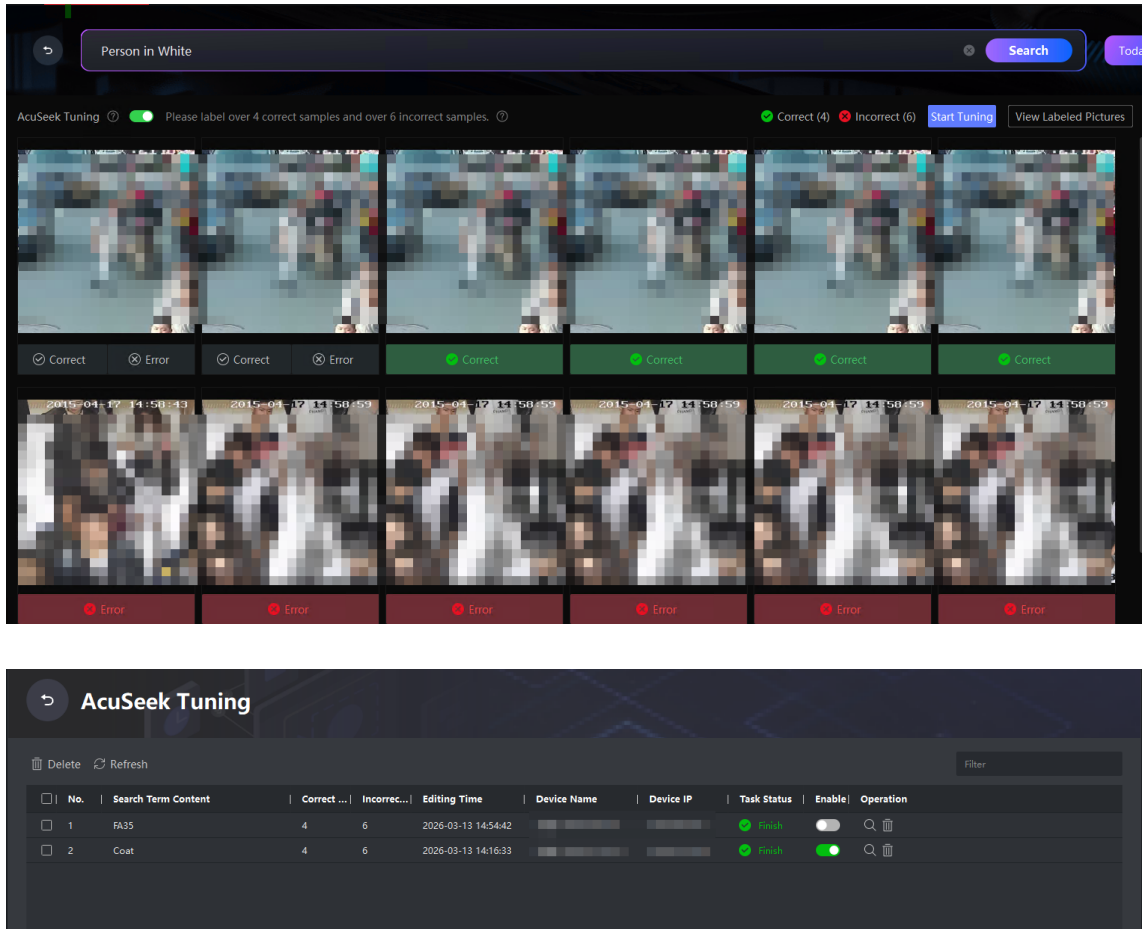


Figure 12-3 AcuSeek Tuning

Chapter 13 AI Dashboard

The client provides AI Dashboard module through which you can experience the advanced functions of the devices with AI features, such as face comparison and linked capture of fixed camera and panoramic camera, traffic accident alarm, AI open platform to access to third-party applications.

13.1 Face Application

For some devices, such as DeepinMind NVRs, DeepinView cameras, and dual-lens camera, Face Application function provides showing face comparison alarm for the persons in the blocklist, VIP or regular costumers during live view. If the detected face pictures are matched with the persons in the blocklist or VIP face picture library, the security center will receive relative alarms to take appropriate actions quickly and effectively. It can also help you to evaluate the regular costumers, which is widely used in the hospital, supermarket, shopping mall and so on.

13.1.1 Set List Types for Face Picture Libraries

You can configure list type for each face picture library of the device(s), so that the software can check whether the persons detected during live view are in the blocklist, very important person, or the regular costumers.

Click **AI Dashboard → Face Application** , and then click in the upper-right corner to select the list type for each face picture library on the devices.

Blocklist

If the alarm type is set to **Blocklist**, AI dashboard will show the blocklist alarm once the captured pictures are matched with the ones in the face picture library.

VIP

If the face picture library is set to **VIP** , AI dashboard will show the VIP alarm once the captured pictures are matched with the ones in the face picture library.

Normal

The face pictures libraries which belong to neither blocklist nor the VIP can be set to **Normal**. AI dashboard will not show any alarms when the captured face pictures are matched with the ones in the face picture library.

Note

This function should be supported by the device and the face picture library need be configured in the device firstly.

13.1.2 Set Cameras for Showing AI Information

You can specify the displaying camera(s) or other cameras in the camera list to show AI information during live view. For example, if you select a camera (not in live view in the displaying window) for showing VIP information, this camera will perform static detection in the background and show the AI information about VIP.

Click **AI Dashboard → Face Application** , and then click in the upper-right corner to select cameras for showing the AI information in real-time.

Select the alarm type to be displayed for different cameras: Blocklist Alarm, VIP Alarm or Regular Customer Alarm.

All Cameras in Live View

If check **All Cameras in Live View**, only the AI information of the camera(s) in live view in the displaying window can be shown.

Custom Cameras

If check **Custom Cameras** and select the desired cameras, the AI information of the selected camera(s) can be shown, whether the cameras are in live view or not.

13.1.3 Show AI Information

After setting the cameras for showing AI information and list type for face picture libraries, you can view the AI information.

Click **AI Dashboard → Face Application** , and then select the camera(s) from the camera list to start live view and show AI information.

Note

This function should be supported by the device.

Camera List

The camera list on the left panel shows all the resources added to the client software, and you can select the appropriate window division and desired camera(s) to show AI information.

Note

The channels for live view at the same time are limited by the performance of the PC running the client.

Right-click the camera in the camera list, you can switch stream type between main stream and sub-stream.

Display Intelligent Information on Live View

You can view the real-time video of the selected camera(s).

Click in the global toolbar of the live view area and select the window to enable the desired intelligent display. For example, if the blocklist alarm is enabled for all live view windows, the recognized targets will be marked dynamically on the images of all windows. You can also click at the bottom of each window to enable the intelligent display for the camera in this window.

Face Comparison

If you set **Face Comparison** switch to ON, when detecting blocklist person, VIP, or regular customer, the related alarm notification with corresponding colors will list on the right panel. You can view the alarm time, camera, and other details of the alarm.

Historical Captured Picture

You can view the historical captured pictures at the bottom of the page.



Figure 13-1 Show AI Information

Enable Alarm Triggered Pop-up Window

Click to enable alarm triggered pop-up window, and after that, a window will be pop up when the blocklist alarm is triggered, including the captured pictures and alarm details information.

13.2 Multi-Target-Type Detection

Multi-Target-Type Detection refers to a function that recognizing and capturing multiple types of detection targets including faces, human bodies, motor vehicles, and non-motor vehicles. When the device detects targets, you can view live view, captured pictures, and target features. Alarms can be triggered for high similarity between captured face/human body picture and the one in picture library, or high/low appearing frequency of a person/vehicle, or an appearance of a vehicle

in the blocklist, etc. It is often used in places such as crossroad and train station where there are large amount of people and vehicles showing and places requiring strong security.

13.2.1 Set Target Detection Parameters

The client supports customizing the display layout of detected targets and their details, selecting which feature to display with the detected targets, and selecting cameras of which alarms will be displayed.

Set Display Mode

You can customize the display layout and select information to display according to your needs.

Steps

1. Click **AI Dashboard → Multi-Target-Type Detection** .
2. Click on the upper-right corner to open the Configure window.
3. Click **Basic Settings** tab.
4. Select a live view mode.
   - Select **Single Channel** to display one live view window.
   - Select **Dual Channels** to display two live view windows.
   - Select **Channel 4** to display four live view windows.
5. Check information to be displayed in the corresponding positions.

Note

- The **Face Arming** function should be supported by the device.
- Up to 2 items can be selected to be displayed on the bottom of the page.

The checked information will be displayed in the following window.

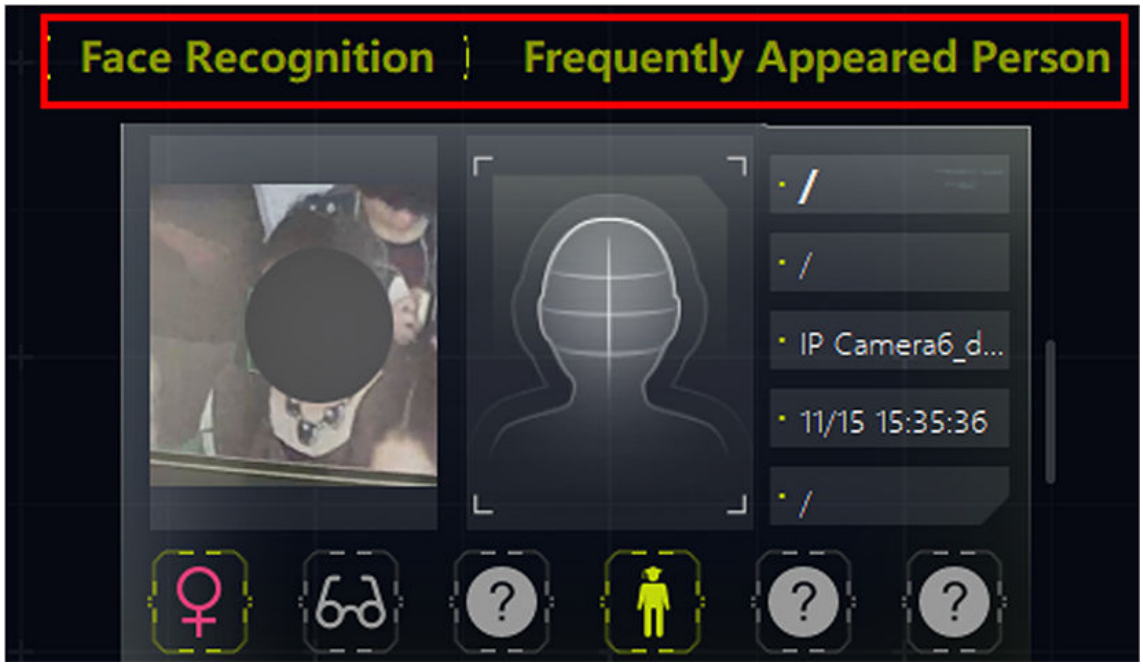


Figure 13-2 Display on Right

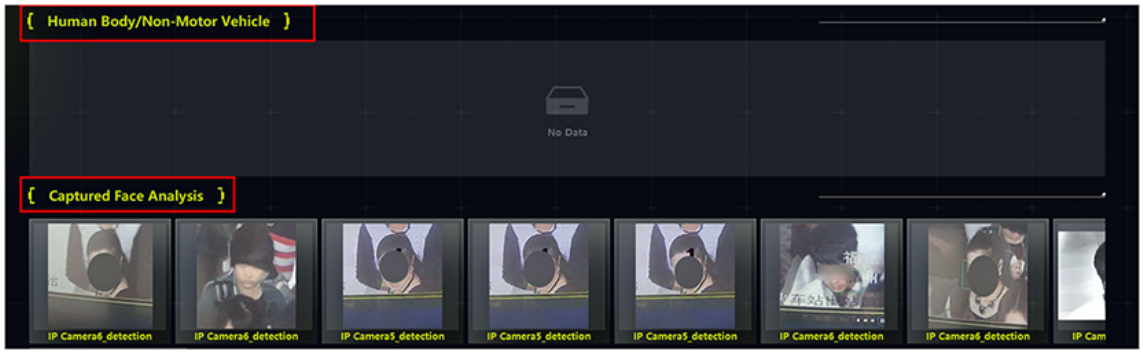


Figure 13-3 Display on Bottom

6. **Optional:** Enable **Save Picture** so that all the captured pictures will be saved in a specified folder and then click the saving path to change it.
7. Click **Save** to save the settings.

Set Capture Parameters

For captured pictures, the device will analyze the features of the captured targets. You can select features to be displayed according to your needs. Take face detection as an example, you can select the feature: glasses wearing to display with the picture.

Steps

1. Click **AI Dashboard → Multi-Target-Type Detection** .

2. Click on the upper-right corner to open the Configure window.
3. Click **Capture Parameters** tab.
4. Enable **Display Features**.
5. Enable **Features in Face Detection/Features in Motor Vehicle Detection/Features in Human Body Detection/Features in Non Motor Vehicle Detection** and check corresponding features.

Note

No more than 6 features of each function can be selected.

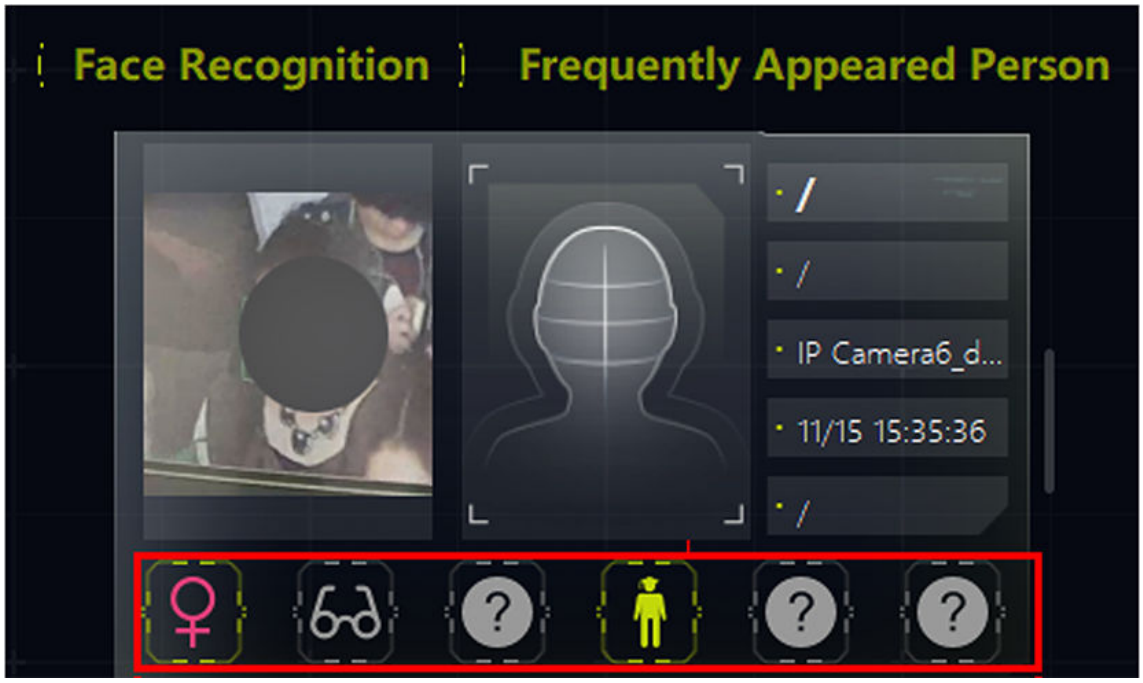


Figure 13-4 Displayed Features

6. Click **Save** to save the settings.

Set Cameras Receiving Alarm

For cameras configured with detection alarm, you can select cameras to display their alarms on the right panel with detailed alarm information provided.

Before You Start

Make sure you have configured alarms for the cameras whose alarms you select to display.

Steps

1. Click **AI Dashboard → Multi-Target-Type Detection** .
2. Click on the upper-right corner to open the Configure window.
3. Click **Receiving Alarm Settings** tab.
4. Check cameras whose alarms will be displayed on the right panel.

Note

Alarms of checked cameras will be displayed on the right panel with detailed alarm information.

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

13.2.2 Display Multi-Target-Type Detection

Multi-Target-Type Detection supports displaying detected information (including live view of capture cameras, captured pictures, target details, target amount, and alarm details) after configuring corresponding parameters.

Note

This function needs to be supported by device.

Live View

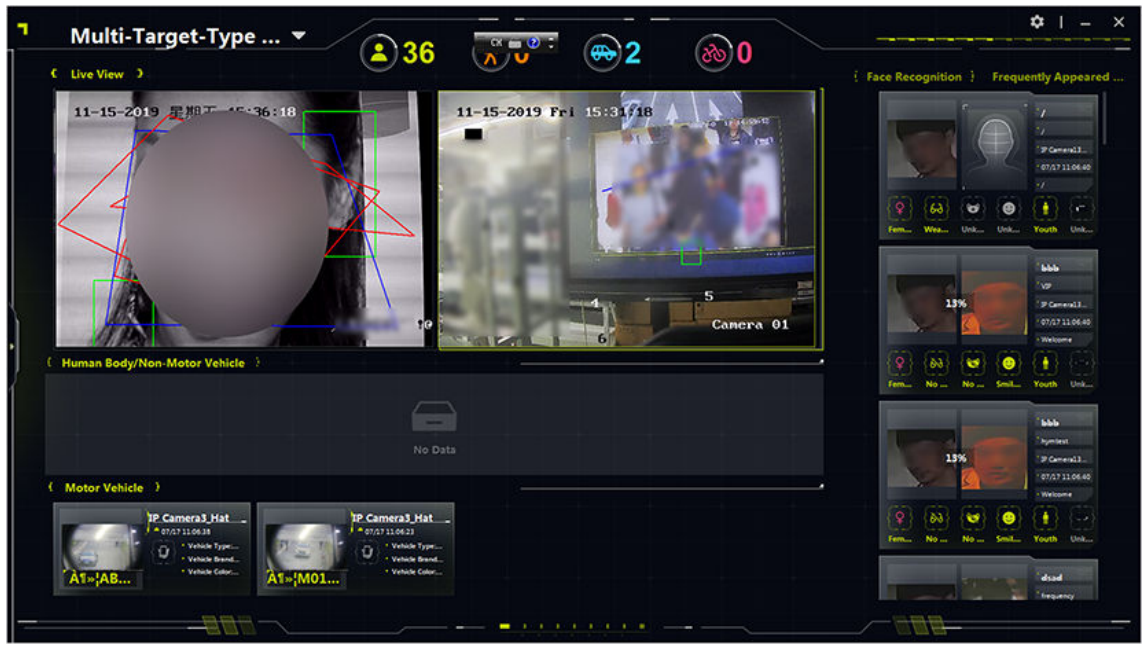


Figure 13-5 Multi-Target Detection Display

Supports displaying live view in single channel mode, dual-channel mode, or 4-channel mode. You can capture a picture or start recording quickly with tool bar in the live view window when something important happens. You can also perform PTZ control or 3D position by a right-clicking for a panoramic detailed view.

Human Body/Non Motor Vehicle

Captured human body/non motor vehicle pictures will be displayed in this area with a highlight box on the target. Meanwhile, features of the captured target will be displayed with the pictures.

Captured Face Analysis

Display captured face pictures with face features (glasses wearing, etc.) displayed.

Motor Vehicle

Display captured motor vehicle picture with vehicle features (such as plate No., vehicle color, vehicle type, etc.) displayed.

Facial Recognition/Frequently/Rarely Appeared Person

Display facial comparison or face arming results, captured face pictures of strangers, human body with captured face picture, and appearing frequency.

- Display captured face picture and the similar face picture in face picture library if the two faces match.
- Display captured face pictures that mismatched with that in the face picture library.

Note

For a device supporting stranger recognition, the captured faces will be compared with pictures in face picture library. The person will be recognized as a stranger if her/his face matches with no faces in the face picture library.

- For captured human body pictures, the face picture of the person will also be displayed.
- Appearing Frequency: Frequently Appeared People will be displayed whose appeared times is larger than the threshold, while Rarely Appeared People will be displayed whose appearance amount is less than the threshold.

Note

Person information including the last captured face picture, appearance amount, and alarm time will show after clicking the alarm information. You can add the detected person to face picture library.

- Display the human features of the detected persons. For example, the person who wears glasses is marked in highlight icon ( ), and the person who does not wear glasses is marked in highlight icon with diagonal ( ), and the undetected feature is marked in gray icon ( ).

13.3 AI Open Platform

AI Open Platform is a software platform that can be accessed to third-party software application, algorithm, etc. By this way, different intelligent objects can be connected by network, and more software developer can work efficiently on this platform.

13.3.1 Configure Platform Parameters

You can add intelligent devices to the client for displaying on the AI Open Platform. On the AI Open Platform, you can get model package, select the cameras to be displayed, set the saving path for picture storage and set the storage mode.

Configure Local Storage

You can select to save the alarm information and pictures to the local path, and set the saving path and storage mode.

Steps

1. Click **AI Dashboard**, and then select **AI Open Platform**.
2. Click on the right-upper corner to open the Local Storage Settings window.
3. Set **Local Storage** to ON.
4. Click the entering box of **Saving Path** to select the saving path.

   Note

   Make sure the storage space is larger than 2 GB, otherwise the pictures can not be stored.
5. Select the **Storage Mode**.

   Overlap Earliest Alarm(Max. 10000 Alarms for Each Channel)

   In this mode, up to 10000 alarms (including pictures) can be stored for each channel, and if the storage space is full, the new alarm and pictures will overlap the earliest alarm.

   Do Not Overlap

   In this mode, up to 10000 alarms (including pictures) can be stored for each channel, and if the storage space is full, the new alarm and picture will not be saved.
6. Click **OK**.

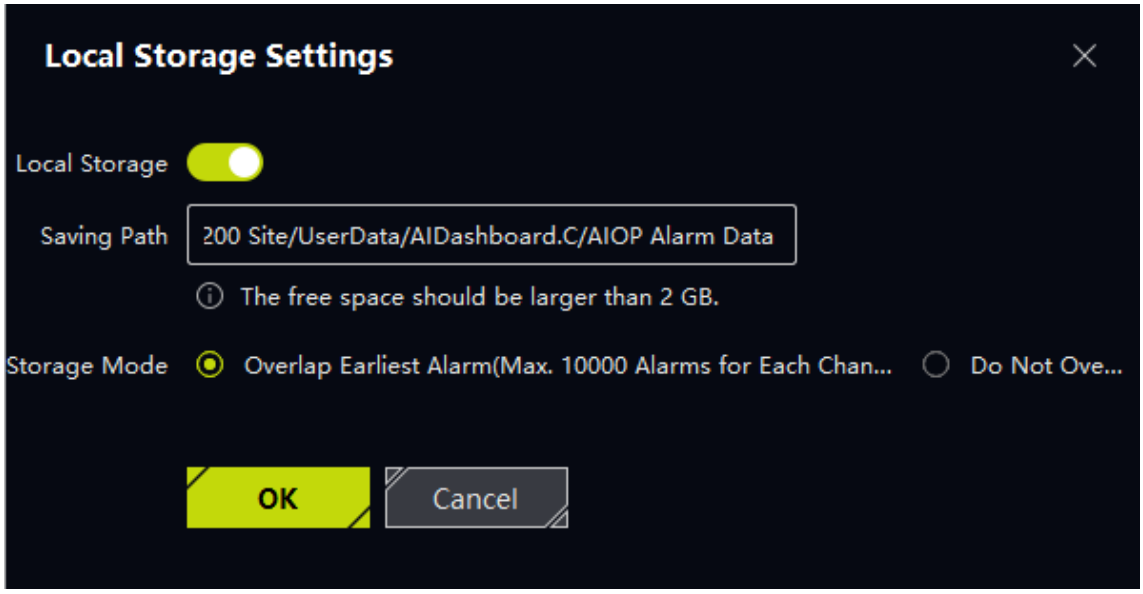


Figure 13-6 Configure Local Storage

Get Model Package

Model package is a product generated by algorithm model training on AI Algorithm Training Platform. The model package can be imported to devices for task analysis. If the model package saved in device is modified, you can synchronize the model package from the device, to make the data information accordant.

Steps

1. Click **AI Dashboard**, and then select **AI Open Platform**.
2. Click on the right-upper corner to open the model package selecting window.
3. Check the cameras to get model package from the cameras.
4. Click **OK**.

Set Objects to Be Displayed

By default, the AI Open Platform receives alarm information from all cameras and all tasks. You can also choose specific camera(s) or task(s) to display received alarms.

Steps

1. Click **AI Dashboard**, and then select **AI Open Platform**.
2. Click on the right-upper corner to open the camera(s) selecting window.
3. Choose the camera(s) or task(s) to display received alarms.
4. Click **OK**.

13.3.2 Configure Platform Event

The AI open platform event refers to the event triggered by the AI model package on the device. When the device triggers an alarm of a corresponding AI model package, such as AI open platform alarm, the client can receive all of the events for the same alarm, trigger the linkage action, and display the name and triggering time of the AI model package. To distinguish an alarm of the same corresponding AI model package, you can edit the alarm name on the client, then the edited alarm name will be displayed on the Real-Time Event page and Event Search page.

Steps

1. Enter the Maintenance and Management page.
2. Click **Event Configuration → AI Open Platform Event** .

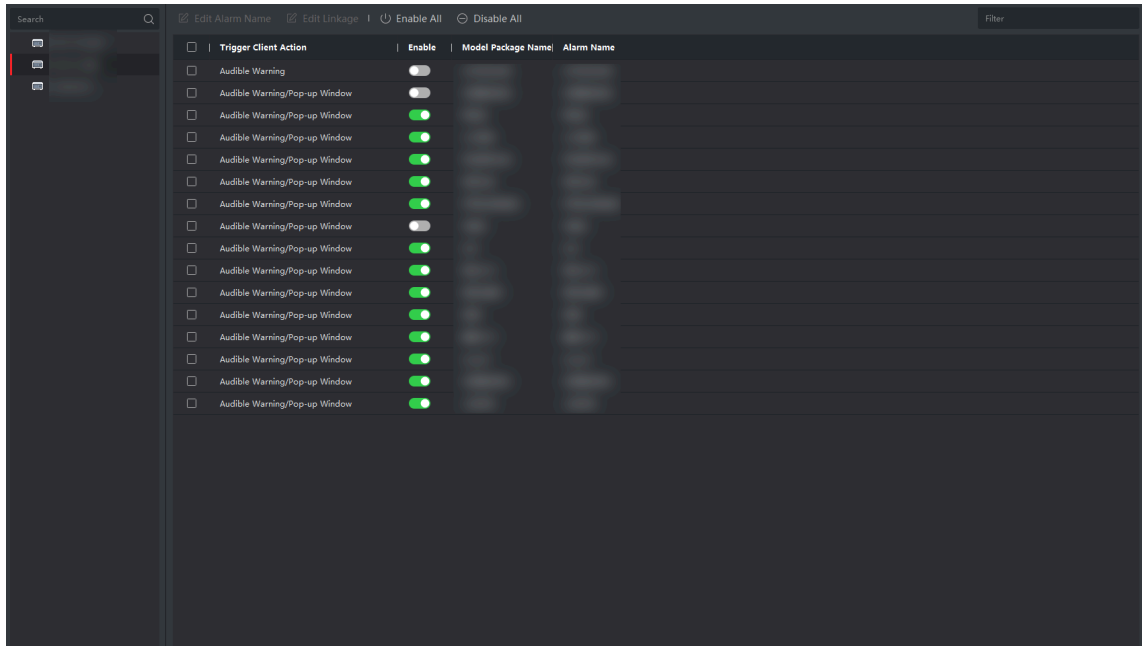


Figure 13-7 AI Open Platform Event Page

3. Select a device as the event source.

Note

Make sure the resource is online.

All the event types supported by the selected device will appear.

4. **Optional:** Switch on the button in the **Enable** column to enable the event type, or click **Enable All** to enable all the event types of the AI model package.

Note

After enabled, the event can be received by the client and trigger the linkage action(s). You can also disable an event type or click **Disable All** to disable all event types.

5. **Optional:** Select the AI model package(s), and then perform the following operations.

Edit Alarm Name
Select an event, click **Edit Alarm Name** to set a custom alarm name for the corresponding AI model package.

The edited alarm name will be displayed on Real-time Event page, refer to ***View Real-Time Events*** for details.

Edit Event Linkage
Select an event, click **Edit Linkage** to set the linkage action(s) of the event(s).

Audible Warning

Trigger the client's audible warning when the event is triggered.

You can select the audio file on the drop-down list, or click **Add** to add new audio file (in WAV format).

You can click to make an audition of the selected audio file.

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Pop-up Window

A window pops up to display the event related information (including event details, live video of the source camera, captured pictures of the linked camera) on the client when the event is triggered. You can also enter remarks about how to the handle the event.

What to do next
You need to arm the device which the alarm input belongs to, otherwise the client cannot receive the configured events. For details, see ***Enable Receiving Event from Devices*** .

13.3.3 Analyze Picture Task

AI Open Platform can analyze and recognize objects in the picture(s). The client can apply the picture(s) to the device. The device will analyze the picture(s) and upload the results (e.g. object classification, attribute) to the client for displaying.

Steps
1. Click **AI Dashboard**, and then select **AI Open Platform**.
2. Click in the right-upper corner of the page.

   The Picture Importing & Analysis window pops up.
3. Select the **Device** to analyze the offline picture(s).

   Note

   Only the device supporting offline picture analysis function will be displayed in the drop-down list.
4. Select **Device Engine** or **Algorithm List** for selecting the model package.

5. Enter the path of folder, which stores the offline pictures for analyzing.

Note

The supported picture format and size vary according to different devices.

6. **Optional:** Check **Display Alarm Target Frame** to display the frame on the target which is recognized.

Note

If you select the **Device Engine** as OCR model package, the **Display Alarm Target Frame** function is gray, and you can not check this function.

7. **Optional:** Set the detection frame for the target to be analyzed, thus to improve the accuracy rate.

Note

When selecting a single classification model package, the detection frame is required.

8. Click **Start**.

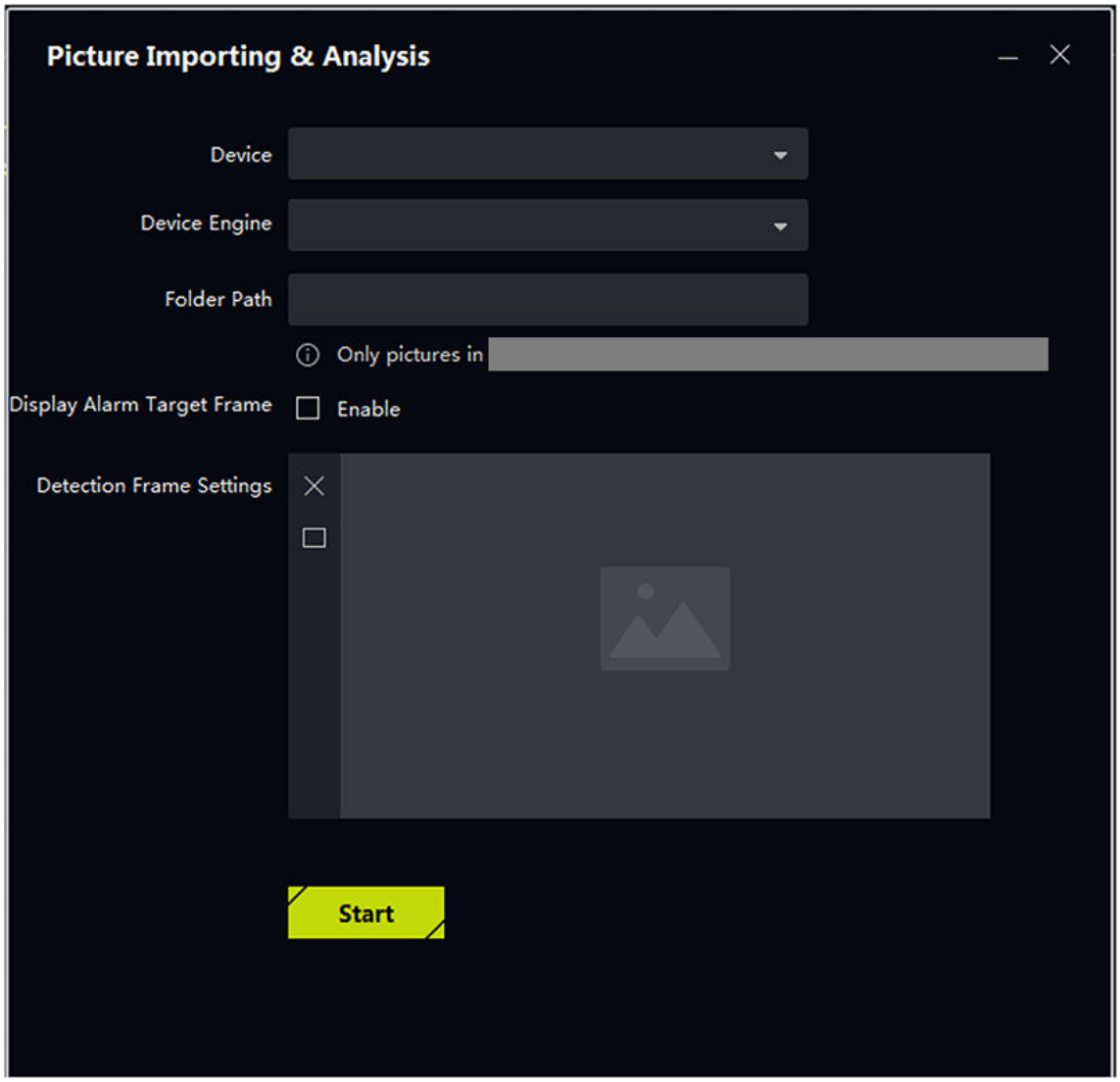


Figure 13-8 Picture Importing and Analysis

13.3.4 AI Platform Real-Time Display

The AI Platform can display the live video of the camera, and display the uploaded pictures and alarm information from the device.

Matched Results Display

On the AI Platform, the monitoring scene is compared with the scene learned by model to generate the result. In the **Matched Results** area, the results are displayed, including alarm pictures, camera information, alarm time, category, detection result, tags and attributes of the

target. When the object is recognized, you can move the cursor to the object to view the category or detection result, and click the alarm picture to view the details.

Note

The alarms in the figure above is OCR alarm, which are uploaded to the client when the devices recognize characters in the video. If there are more than 3 characters recognized, only 3 characters are displayed, and you can click to view more character(s) in the next page.

Live View

In the lower-left corner of the page, the live video of the camera is displayed.

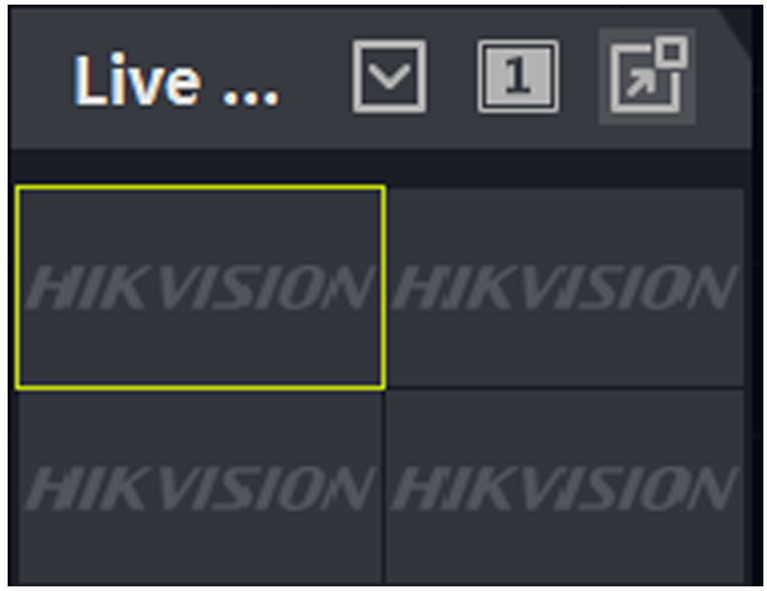


Figure 13-9 Live View in AI Open Platform

Click to switch the window division to 1 window or 4 window.
Click to hide the live view window.
Click to pop up the live view window. After the window is popped up, you can click to display the window in full screen.

Note

Live view is not supported by DeepinMind Server.

13.4 Multidimensional People Counting

Multidimensional People Counting function includes live view and real-time statistics display of people counting data. The real-time statistics includes the number of people entry or exit, the real-time people number, etc. Accurate business strategies can be provided by analyzing the statistics to boost store operation efficiency.

Note

- This function should be supported by the device.
- For the historical data of people counting, refer to ***People Counting Report by Encoding Device*** .

Click **AI Dashboard → Multidimensional People Counting** .

13.4.1 Configure People Counting Group

Configuring people counting group to enable the live view and real-time statistics display of people counting data based on defined group parameters.

Steps

1. Go to **AI Dashboard → Multidimensional People Counting → Configuration** .
2. Click **Add**, enter the group name, and select channel(s).

   Supported channels include multidimensional, vertical, and tilted people counting. If the selected channels include multidimensional people counting and other channels, Gender Statistics and Age Group Statistics will be counted based on the data from the multidimensional people counting only.
3. Once added, groups are visible in the left-side list.

13.4.2 Display People Counting Data by Group

After configuring people counting group(s), people counting data can be displayed by group, including live view and real-time data.

Multidimensional People Counting Live View

1. Select camera(s) in the left list, double-click the selected camera to the live view window to view its live view.
2. Perform the following operation(s) if needed.
   - Click , and then select one window division mode.

     Note

     Supports up to 4 window divisions.
   - Click to stop all live views.
   - Click to display the live view in full screen. Press ***Esc*** key to exit from full screen mode.

Multidimensional People Counting Real Time Data

Double-click one group to view real-time data.

Number of People Enter/Exit

Display the number of people entry or exit within 24 hours. Check **Display All Types** to view the total number.

Real Time People Number

Display the real-time number of people entry or exit reported by the device within 24 hours.

You can also view real-time entry/exit trends in the line chart.

Gender / Age Group Statistics

Display the number of people entry or exit within 24 hours. Check **Display All Types** to view the total number.

Note

If the selected group includes only vertical or tilted people counting channels, Gender and Age Group statistics will not be generated. If the selected group includes multidimensional people counting channels along with other types, these statistics will be calculated based exclusively on data from the multidimensional channels.

Note

You can log in to the web browser to configure the report interval. For details, refer to the user manual of the device.

Multidimensional People Counting Historic Data

Click **People Counting Statistics** to navigate to the People Counting page and view the collected data.

13.5 Linked Capture Alarm

This function allows the users to view two different channels (one fixed channel and one PTZ channel) of a device simultaneously. Therefore, you can view the panoramic image and captured details at the same time when an alarm is triggered.

Note

This function needs to be supported by the device.

13.5.1 Set Basic Parameters

The capture saving function can be enabled or disabled manually, and you can also set the saving path of the captured picture, so that you can view the captured pictures in your PC.

Steps

1. Enter the AI Dashboard module.
2. Select **Linked Capture Alarm** to open the Linked Capture Alarm window.

3. Click to open the setting window.

   The introduction of the displayed content shows.
4. Switch **Save Picture** on to enable picture saving function.
5. Click the **Saving Path** to select a saving path of the captured pictures.
6. Click **Save** to save the settings.

   The pictures captured when events and alarms are triggered will be saved in the configured path.

13.5.2 View Live View and Alarms

When fixed camera triggers an alarm, the fixed camera will capture a panoramic picture related to the alarm, which will be displayed in the panoramic linked alarm window; and the linked PTZ camera will capture a picture with details about the alarm, and the picture will be displayed in the linked channel alarm window. In this way, the user views the panoramic image with details displayed simultaneously.

Generally speaking, Panoramic Channel Live View window is used to display the live view of fixed camera, while Linked Channel Live View window is used to display the live view of PTZ camera connected to the fixed camera.

1. Enter the **AI Dashboard** and select **Linked Capture Alarm** to open the Linked Capture Alarm window.
2. Click to expand the device list.
3. Select a window and double-click a camera to start live view, or drag a camera from the device list to a window, or hover the cursor on a camera name and then click .

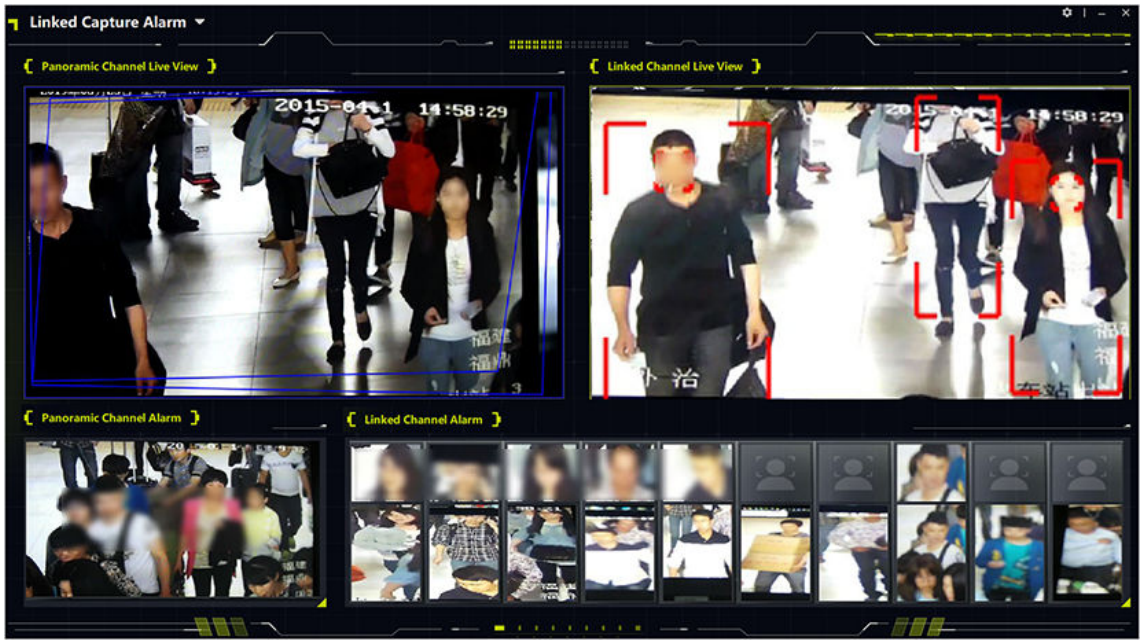


Figure 13-11 View Live View and Alarms

13.6 Traffic Accident Alarm

The intelligent traffic device (e.g. traffic speed dome) can be added to the client for real-time live view of the traffic violations or abnormal traffic events happened on the road. When the camera detects the accident, the camera will capture the picture and upload the picture and accident alarm to the client, which is convenient for the enforcement. The client can display the enforcement alarm, traffic accident alarm and road traffic alarm.

13.6.1 Configure Display Parameter

You can configure the displaying parameters of traffic accident event, which will be displayed on the right panel of the live-view window. If the Save Picture function is enabled, you can double-click the picture to show the original picture. If the Save Picture function is not enabled, you can double-click the picture to show the traffic accident event alarm. Make sure you can configure the traffic accident alarm rule for the traffic device added to the client.

Before You Start

Make sure you can configure the traffic accident alarm rule for the traffic device added to the client.

Steps

1. Select **AI Dashboard → Traffic Accident Alarm** to enter the traffic accident alarm page.
2. Click on the right-upper corner of the page to enter the parameter configuration page.

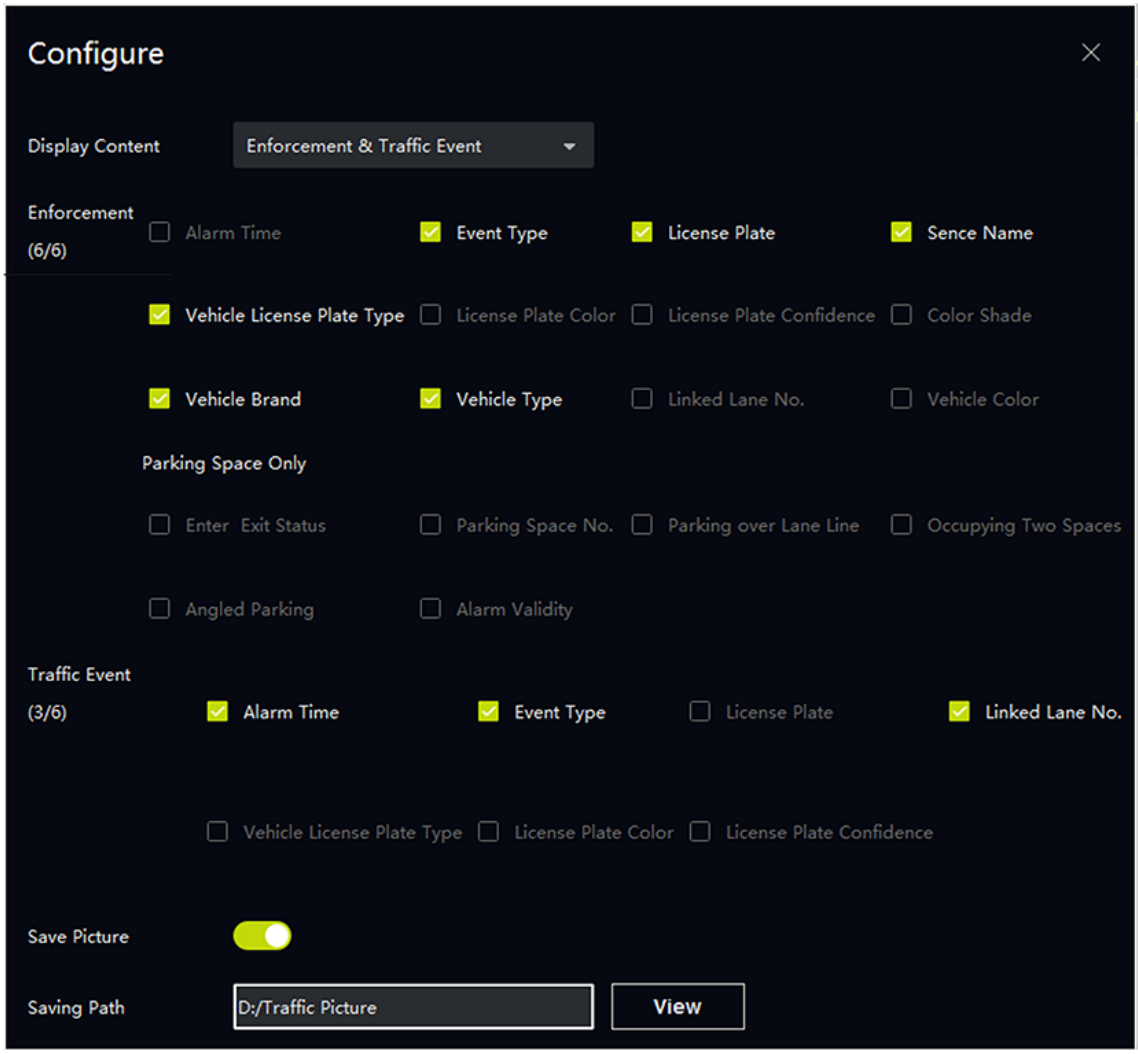


Figure 13-12 Parameter Configuration Page

3. Click the drop-down list, select the **Display Content**, such as Enforcement&Traffic Event.
4. Configure the parameters of the display content.

   Example

   For example, you can select parking over lane line, angled parking for enforcement.

   Note

   Up to 6 items can be selected for displaying.
5. **Optional:** Enable **Save Picture** and set the saving path.
6. Click **Save**.

13.6.2 View Traffic Accident Alarm

On the Traffic Accident Alarm Module, you can view the real-time traffic monitoring view, and receive the alarm information triggered by the traffic device. You can view the monitoring video by 1 channel or 2 channels, and display the enforcement alarms, traffic accident alarms or road alarms from the corresponding camera(s).

Select **AI Dashboard Traffic → Accident Event** to enter the Traffic Accident Event page.

Click on the left of the page to select the cameras for live view.



Live View Window

The live view window display the real-time traffic monitoring video. Click 1 or 2 on the right-lower corner to set the window division. Up to 2 cameras can be viewed simultaneously.

Note

Display live video of 1 or 2 cameras in main stream mode. Stream switch is not supported.

Click or on the right-lower corner of the live window, to manually record the video or capture picture of the camera.

Display Traffic Event

Display the parameters information of traffic event, enforcement or road traffic event information in real-time. Up to 6 parameters can be displayed for each event, such as alarm time, vehicle type, event type, etc.

13.7 Arming and Tracking

For the devices that support arming and tracking, the devices can be configured in a designed order to detect and track the target (human or vehicle), and display the video or captured picture of the target on the client. This is suitable for the situation that the target (vehicle) should be continuously tracked. For example, the vehicle with traffic violation can be armed, and then it will be tracked and monitored by multiple cameras.

13.7.1 Vehicle Arming and Control

For the devices that support vehicle arming and control, the vehicle can be armed by license plate number on the device or on the client, and the devices can be installed and configured in a designed order to detect the armed vehicle and track this vehicle. When the first camera detects this vehicle (the recognized license plate number matches the armed one), the vehicle will be continuously tracked by the other cameras in the designed order, and the related videos and recognized license plate number will be displayed on the client to track this vehicle continuously.

Before You Start
Make sure the devices support vehicle arming and control.

Steps
1. Enter the AI Dashboard module, and then select **Arming and Control** to enter the Arming and Control module.
2. Click to switch to **Vehicle**.
3. Click to open the Configure window.
4. Click **Add Device** to add the devices to be armed.
5. Click / in the Operation column to adjust the order of the devices to be armed.
6. **Optional:** Click **Add License Plate** in the License Plate sheet to add the license plate number of the vehicle(s) to be armed.

   Note
   - The vehicle can be armed both on the device and on the client. Only the vehicle that is not armed on the device should be armed here on the client.
   - Up to 100 license plate number can be added for arming.
   - Only the license plate number added in the latest time will be armed and take effect.
7. **Optional:** For the license plate number that do not need to be armed, click in the Operation column to delete it.
8. Click to arm the devices.

   The videos of the detected vehicle will be displayed.

   The license plate number of the detected vehicle is displayed in the right-upper corner of the middle window.



Figure 13-14 Vehicle Arming and Control

Note

- The video of the camera which detects the vehicle recently is always displayed in the middle window of the page. The previous video will be switched to the left by one window.
- For example, when camera1 recognizes the vehicle for the first time, the video of camera1 is displayed in the middle window. When camera2 recognizes the vehicle, the video of camera2 is displayed in the middle window, and the video of camera1 will be switched to the left window. When camera3 recognizes the vehicle, the video of camera3 is displayed in the middle window, the video of camera2 will be switched to the left window, the video of camera1 will be switched to the right window.

9. **Optional:** Click to switch the view to the following video.
10. **Optional:** Click to switch the view to the previous video.
11. **Optional:** If you want to disarm the device, click to disarm the device.

13.7.2 Face/Human Body Arming and Control

For the devices that support face/human body arming and control, the person can be armed on the devices and the devices can be installed and configured in a designed order to detect the person and track the person. When the first camera detects this person (the facial picture or human body picture captured by the device matches the armed one), the person will be continuously tracked by the other cameras in the designed order, and the related videos and comparison result (captured picture and armed picture) will be displayed on the client to track this person continuously.

Before You Start

Make sure the devices support arming and control, and the related face picture or human body picture are correctly armed on the device. For details, refer to the user manual of the device.

Steps

1. Enter the AI Dashboard module, and then select **Arming and Control** to enter the Arming and Control module.
2. Click to switch to **Face/Human Body**.
3. Click to open the Configure window.
4. Click **Add Device** to add the devices to be armed.
5. Click / in the Operation column to adjust the order of the devices to be armed.

   The videos of the detected person will be displayed on the middle window and right window.

   The comparison result (the captured facial picture, the armed picture and similarity) will be displayed on the left window.



Figure 13-15 Face/Human Body Arming and Control

Note

The video of the camera which detect the person recently is always displayed in the middle window of the page. The previous video will be switched to the right window.

6. **Optional:** Click to switch the view to the following video.
7. **Optional:** Click to switch the view to the previous video.

13.8 Skin-Surface Temperature

In some special scene, you can supervise the human body's skin-surface temperature. When the Client receives alarm information of abnormal skin-surface temperature or no mask, it will trigger the linkage of alarm audio or pop-up window. This is suitable for the scene that requires people wearing mask and skin-temperature measurement.

Note

The function should be supported by the devices.

13.8.1 Start Live View of Skin-Surface Temperature Detection

In the Skin-Surface Temperature page, you can view the persons in the live view, and get the statistic number of the persons whose temperature are abnormal, normal and the persons do not wear mask. You can also view the alarm information of the face picture comparison, temperature measurement picture, face capture alarm, and the historical captured face pictures.

Click **AI Dashboard → Skin-Surface Temperature** to enter the Skin-Surface Temperature page. Start live view in the Skin-Surface Temperature page.

- Click on the left panel and double-click the camera to display the live video of the camera.
- Click on the left panel, and then click on the right side of the camera to display the live video of the camera.



Figure 13-16 Skin-Surface Temperature Page

13.8.2 Display Skin-Surface Temperature Information

In the Skin-Surface Temperature page, you can select the alarm types (face comparison alarm, temperature measurement picture and face capture alarm) to be displayed on the right area. The statistic number of persons are displayed on the top of the page. The captured face pictures are displayed on the bottom of the page. You can set the audio linkage file for received alarms.

Enable Information Display

You can select the alarm types (face comparison alarm, temperature measurement picture and face capture alarm) to be displayed on the Client. The alarm types are distinguished by different color.

1. In the Skin-Surface Temperature page, click  to select the alarm type(s) to be displayed.

   Face Comparison Alarm

   After enabled, the captured face picture and the comparison picture in the face picture library will be displayed, as well as the related classification (e.g. person name, stranger or unrecognized) in the library. Click **View Details** to view the detailed person information, including person name, ID No., etc.

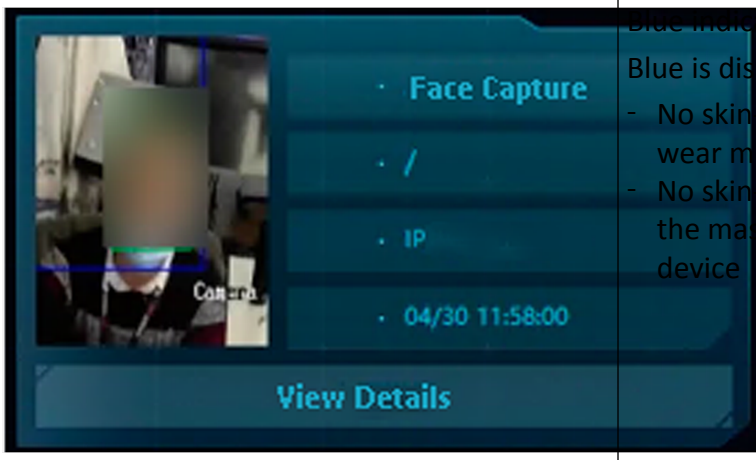
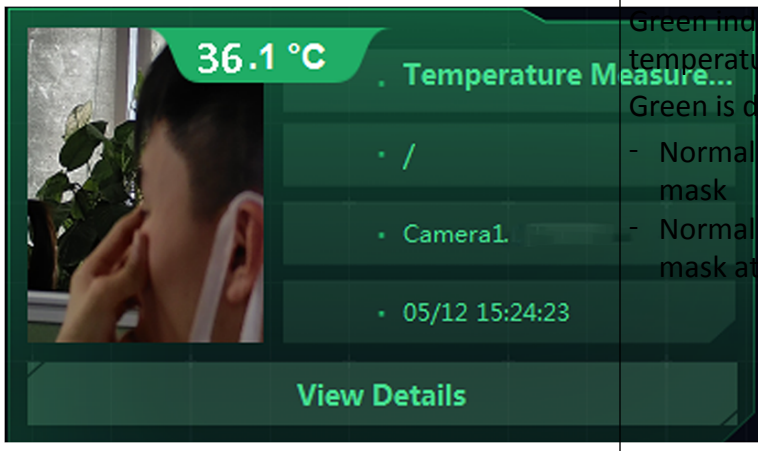
   Temperature Measurement Picture

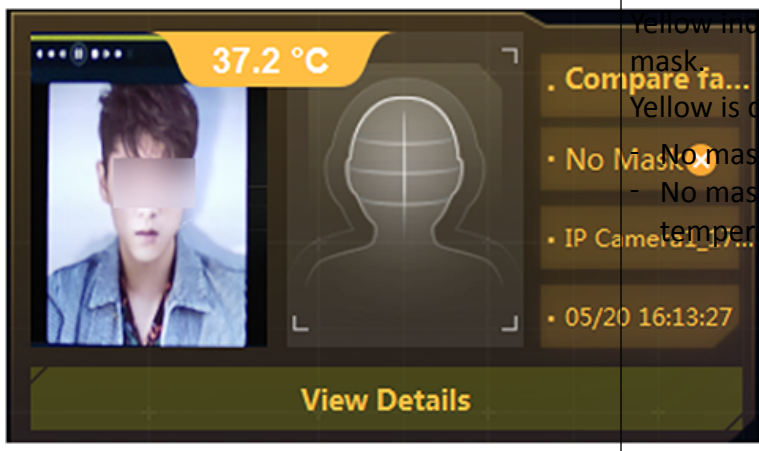
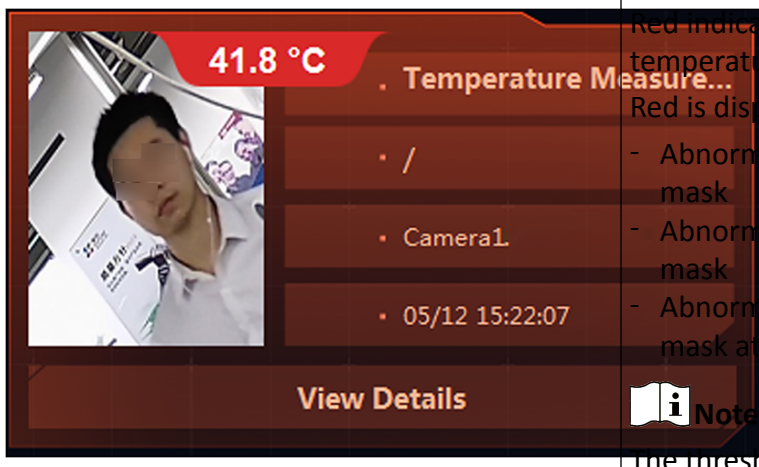
   After enabled, the measured temperature will be displayed on the captured face picture, and the alarm is distinguished as normal or abnormal by different color.

   Face Picture Alarm

   Display the captured face picture detected in the detection area.
2. Set **Display** switch to ON to display the event information in the right area.

Table 13-1 Descriptions of Different Color

Picture	Description
	Blue indicates no temperature information. Blue is displayed in the following cases: - No skin-surface temperature information + wear mask - No skin-surface temperature information + the mask attribute is not detected by the device
	Green indicates the person is normal temperature. Green is displayed in the following cases: - Normal skin-surface temperature + wear mask - Normal skin-surface temperature + the mask attribute is not detected by the device

Picture	Description
	Yellow indicates the person does not wear mask. Yellow is displayed in the following cases: - No mask + normal skin-surface temperature - No mask + the device does not support temperature measurement function.
	Red indicates the person's skin-surface temperature is abnormal. Red is displayed in the following cases: - Abnormal skin-surface temperature + wear mask - Abnormal skin-surface temperature + no mask - Abnormal skin-surface temperature + the mask attribute is not detected by the device **Note** The threshold of the skin-surface temperature abnormal can be set on the device.

Statistic Number of Persons

In the Skin-Surface Temperature page, the Client calculate the number of persons based on the received alarms, to get the number of passing persons, the number of persons whose skin-temperature are abnormal and the number of persons who do not wear mask.

Note

Turn the **Display** switch to ON to get the real-time statistic number of persons.

- All: the total number of alarms received in the Skin-Surface Temperature page.
- Abnormal: the number of persons whose skin-temperature are abnormal. When a camera detects a person whose skin-temperature is abnormal, it will trigger the alarm of abnormal temperature, and the number of Abnormal and All will be added by 1.

- No Mask: the number of persons in the live view who do not wear mask. When a camera detects a person who does not wear mask, it will trigger the alarm of no mask, and the number of No Mask and All will be added by 1.
- Normal: the number of persons in the live view whose skin-temperature is normal. When a camera detects a person whose skin-temperature is normal, it will trigger the alarm of normal temperature, and the number of Normal and All will be added by 1.

Captured Face Pictures Display

On the bottom of the Skin-Surface Temperature page, the captured face pictures can be displayed in real-time.

Note

- Turn the **Display** switch to ON to receive and display the captured face pictures in real-time.
- The displayed pictures are the captured face pictures for the face comparison alarm, temperature measurement alarm or face capture alarm. Make sure at least one alarm is selected by clicking .

Drag the slider under the captured face pictures to view the previous captured face pictures.
On the bottom of the captured face picture, click to add the face picture to the face picture library and enter the person information.

Audio Linkage Settings

You can set audio linkage file(s) for the received alarms.

1. Click on the upper-right corner of the Skin-Surface Temperature page.
2. Set the switch(es) to ON to enable audio linkage for different alarms.

   Note

   By default, audio linkages of all the alarms (no mask, normal temperature, abnormal temperature) are enabled.
3. Click to select the audio file in .wav format to modify the audio file.

   Note

   Upload the audio file to the designed path of the Client. In **Audio Configuration** window, click to view the designed path of the Client.

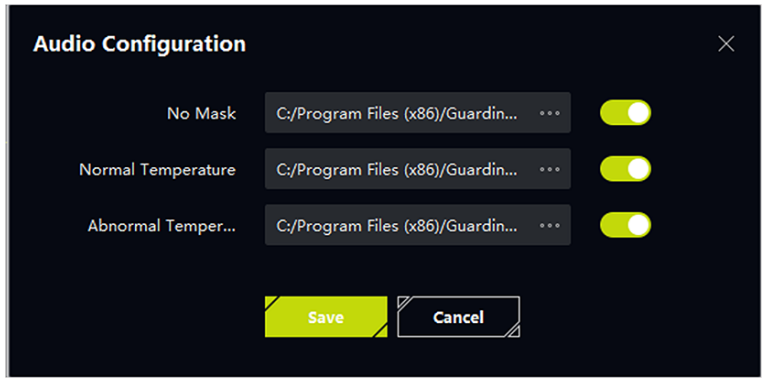


Figure 13-17 Audio Configuration

13.8.3 View Alarm Information

When the devices detect alarm of abnormal skin-surface temperature or no mask, it will trigger alarm pop-up window to display the alarm information. Besides, the duration of window pop-up can be set, which can help you to flexibly control the duration of viewing the alarm information.



Figure 13-18 Alarm Pop-up Window

No Mask

The alarm window pops up to show the captured face picture of the person who does not wear mask.

Abnormal Temperature

The alarm window pops up to show the captured face picture of the person whose skin-surface temperature is abnormal.

Note

The priority of abnormal temperature alarm is higher than the priority of no mask alarm. If No Mask and Abnormal Temperature are both enabled, when the client receives the alarm of no mask and abnormal temperature, the abnormal temperature alarm window will pop up and the audio of abnormal temperature (if enabled. Refer to ***Display Skin-Surface Temperature Information*** for details.) will be played.

Note

- Before viewing alarm information, make sure enabling receiving alarm information. For details, refer to ***Enable Receiving Event from Devices*** .
- Before receiving alarm window pop-up, make sure enabling alarm pop-up window.
  In the skin-surface temperature page, click on the upper-right corner to pop up the window of **Alarm Pop-up Window** to set the configuration.

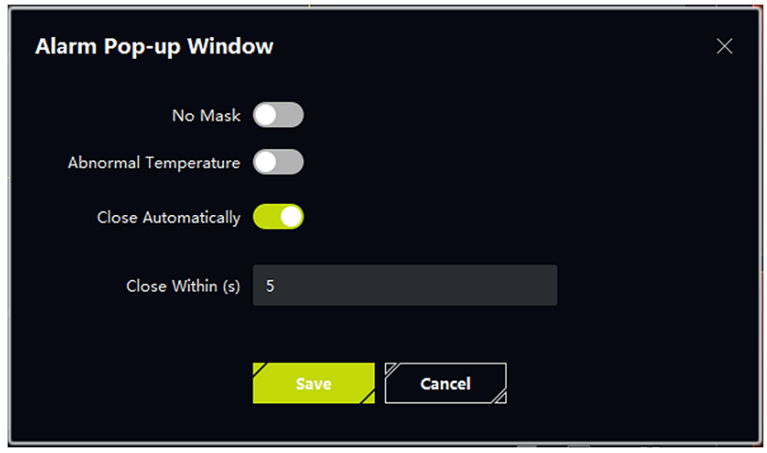


Figure 13-19 Alarm Pop-up Window Configuration

13.9 Abnormal Event Detection

The abnormal event detection server can be added to the client to display the analysis results of multiple analysis tasks. The following analysis tasks are supported: perimeter prevention related alarms (e.g. line crossing detection, intrusion detection, parking detection), street behavior related alarms (e.g. , getting up detection, climbing alarm), indoor behavior related alarms (e.g. in-toliet overtime, absence detection), and people density analysis, etc. The analysis results (alarms) will be displayed.

Enter the AI Dashboard module, and then select **Abnormal Event Detection** to enter the Abnormal Event Detection page. In the task list, double-click the task, or select and drag the task to the live view window, and the video of the task will be displayed in the live view window.

The people density analysis results are displayed by 3 parts in the same window. The live video is displayed in the upper-left part of the window. The heat map of the video is displayed in the upper-right part of the window. The number of people is displayed in the bottom part of the window in real time.

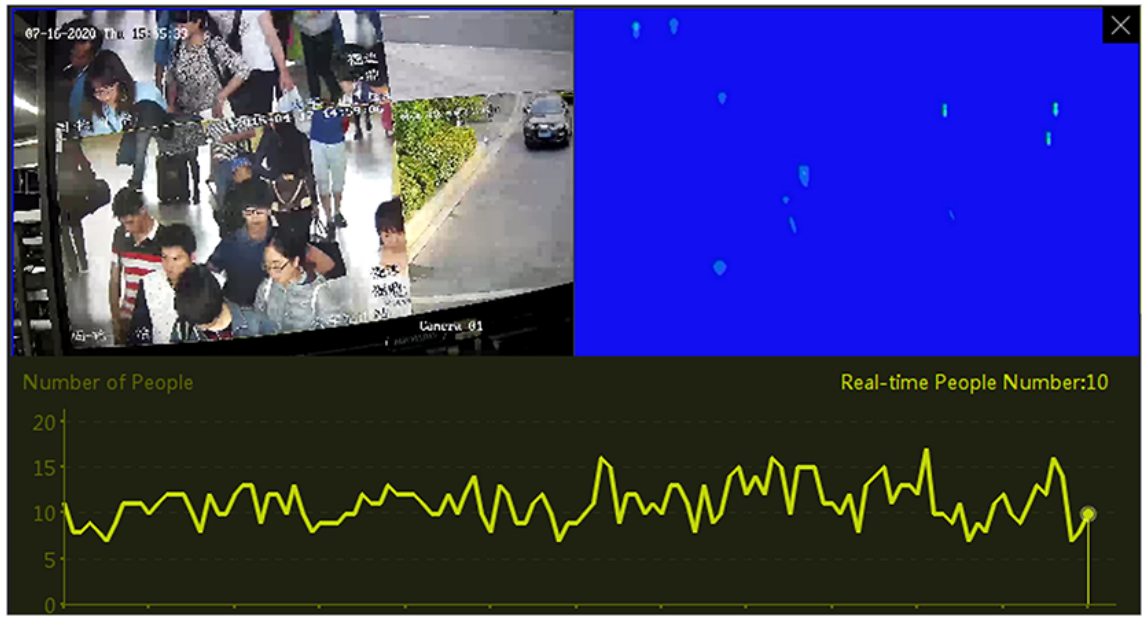


Figure 13-20 People Density Analysis Task Display

For the other tasks (not people density analysis task), only the task related video is displayed in the window.



Figure 13-21 Other Analysis Task Display

- Click the view and then click **Capture** to capture the picture of current video.
- Click the view and then click **Start Recording** to record the video.

Note

The video is saved in the path that is configured in the System Settings module. For details about setting the path to save video, refer to ***Set File Saving Path*** .

- Click to end the live view of the video.
- Click to change the window division of the video. Up to 6 windows are supported to be viewed simultaneously.
- Click to view the video in full screen.

13.10 Event Dashboard

When the abnormal event detection server detects events, the client can receive the events from the server. The client can calculate the number of different events, the event time distribution and risk assessment (the total number of events and frequently-occurred events of different tasks), and display the statistic data in the same page, to help you get a overview of the behavior events. For example, if one event was mainly detected in a certain time period, you can investigate the reason in that time period and adopt measures to solve the problem.

Set Filter Conditions

Enter the AI Dashboard module, and then select **Event Dashboard** to enter the Event Dashboard module. Click to set the filter condition as follows:

Device

Select the abnormal event detection server to display its events statistic data.

Note

Only the abnormal event detection server can be selected here.

Event Type

Select the event(s) to be calculated and displayed.

Statistic Time

Display the statistic data of the events in last 7 days or last 31 days.

Refresh Frequency

Get the statistic data of the events from the devices every 0.5 hour or 1 hour.

Abnormal Event Detection Overview

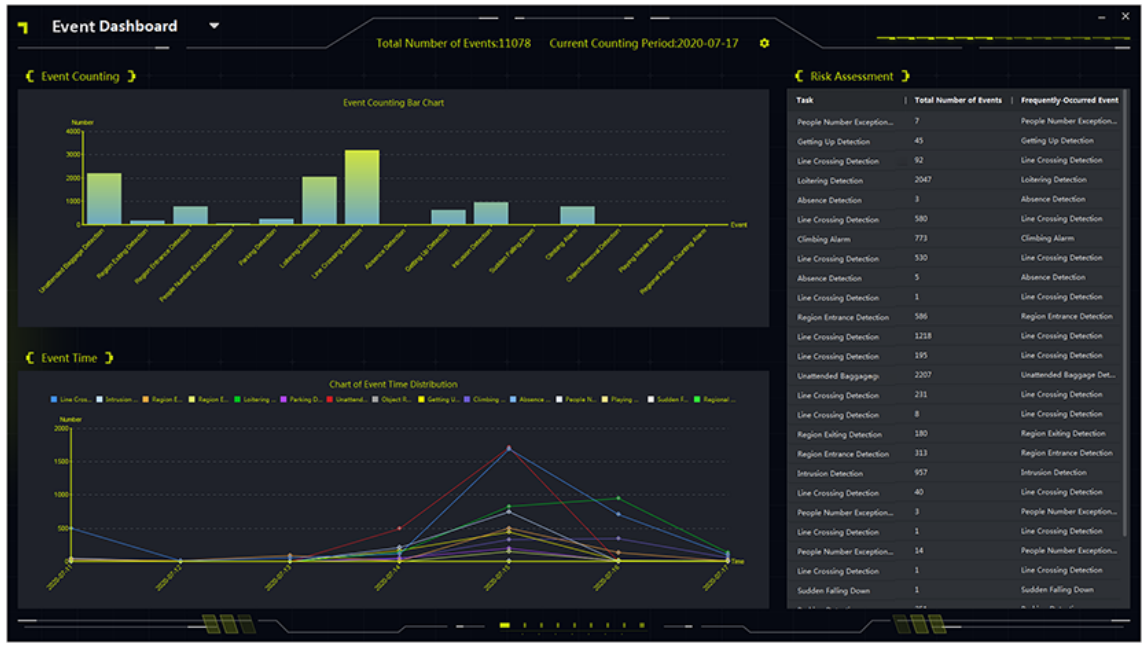


Figure 13-22 Abnormal Event Detection Overview

Event Counting

In the bar chart, display the number of different events in bar chart. You can view the event that happened a lot and mainly investigate the reason that caused this event.

Event Time

In the line chart, display the time distribution of different events in last 7 days or 31 days. You can view the date that the events happened a lot and mainly investigate the reason that caused the events in this date.

Risk Assessment

In the list, display the total number of events and frequently occurred events of different tasks.

Chapter 14 Video Tracing

The system links workstations with connected cameras to automatically capture video footage before and after each scan operation. This enables end-to-end visibility and real-time management of items throughout the logistics process. You can select a designated camera, define pre-/post-recording intervals, input an ID (via scanner or manual entry) to access and download records.

Go to **Video Application → Video Tracing** .

14.1 Configuration

Link cameras with each workstation to record videos and configure general settings such as ID length, code-scanning interval, and voice prompt. After configuration, click **Save** to proceed to the Scanning Record page. For multiple workstations, repeat the process until all configurations are complete.

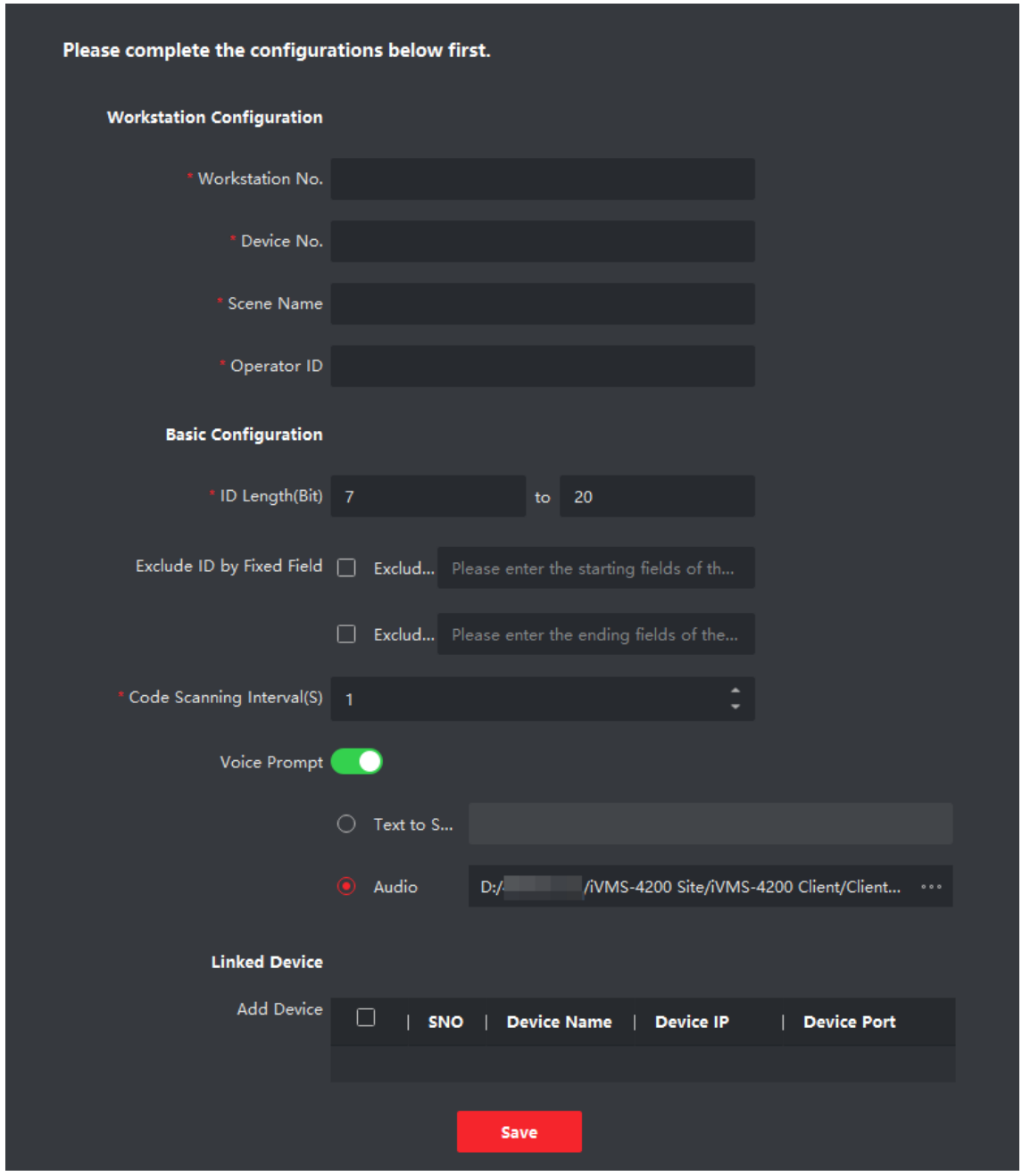


Figure 14-1 Configuration

Workstation Configuration

The configuration ensures each scan record can be traced to the specific workstation location, the device used, and the operator, while allowing custom scenarios for workstations to facilitate management.

Workstation No.

The specific workstation on the logistics line.

Device No.

The device bound to this workstation.

Scene Name

Customize the workstation's purpose (e.g., "Packaging Inspection Area").

Operator ID

The personnel responsible for this workstation.

Basic Configuration

Configure general settings for logistics ID, code-scanning intervals, and voice prompts.

ID Length

Set vaild ID length.

Exclude ID by Fixed Field

Exclude prefixes/suffixes (e.g., "SN-") to extract core ID.

Code Scanning Interval(S)

Minimum interval (seconds) between scans to prevent duplicate records.

Voice Prompt

When the linked device detects a scan, it plays either the entered text (as speech) or the uploaded audio file.

Linked Device

Select the linked device for recording scanning operations.

Scanner Test

Click **Scanner Test** in the upper-right corner to verify that scanners can correctly read barcodes. If no response is received after scanning, inspect the scanner connection and verify the device status. If the device status is confirmed normal, escalate the issue to technical support.

14.2 Retrieve Scanning Records

On the main panel, select a device, set the interval before/after scanning (or a custom span), and input an ID (via scanner or manual entry). Click **Search** to retrieve records.

The search results will display ID, start time, end time, device, and video recordings. You can:

- Click ▷ to play related videos. Supports playback controls (fast-forward/rewind, timeline scrubbing, speed adjustment, etc).

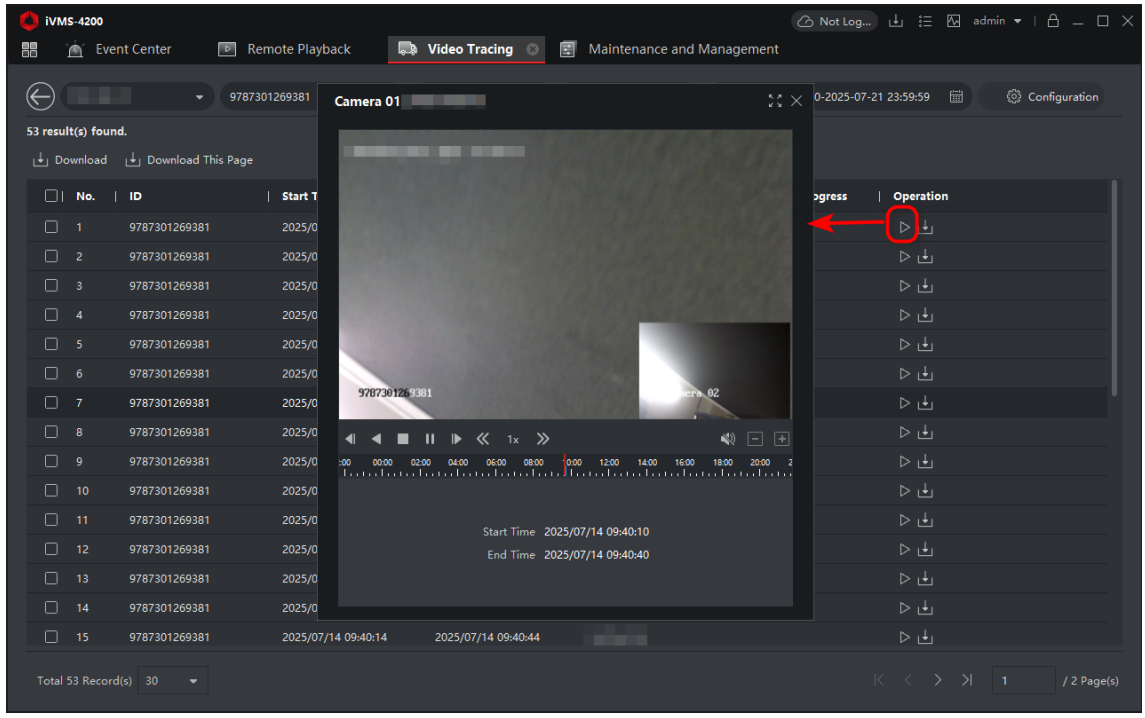


Figure 14-2 Playback

- Click to download single/multiple records or an entire page. If **Transcoding** is enabled, videos will be converted to 1080P resolution. If not, the videos will retain the original resolution. You can also customize watermarks (ID, workstation, start/end time) and font size.

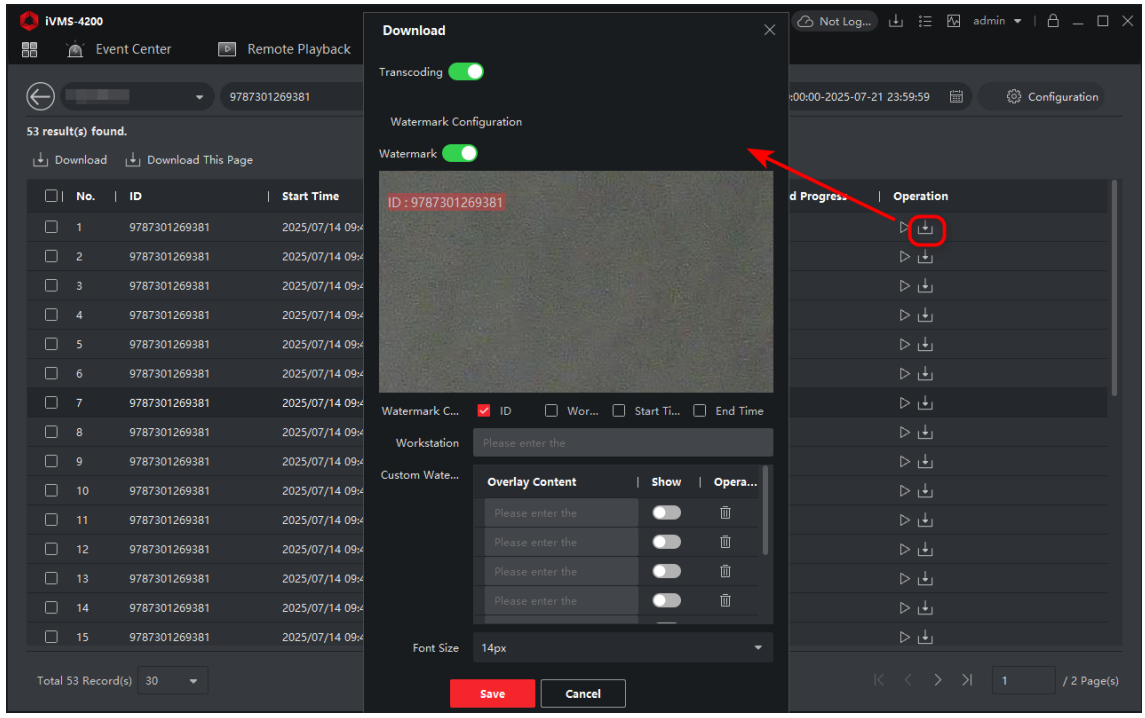


Figure 14-3 Download

Chapter 15 Security Control Panel

The Security Control Panel module provides remote control and configuration of the partitions and zones via the client software.

Note

For the users with security control panel permissions, they can enter the Security Control Panel module to manage the security control panel and real-time alarm. For setting the user permission of Security Control Panel module, refer to ***Add User*** .

15.1 Flow Chart

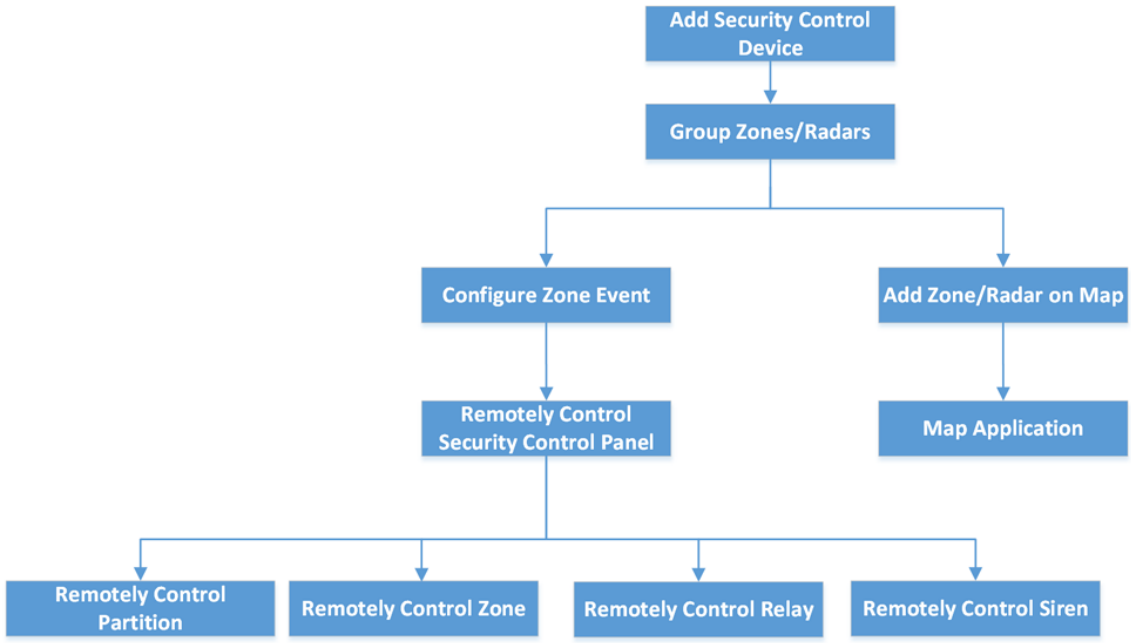


Figure 15-1 Flow Chart of Security Control Panel

- **Add Security Control Device**: You can add security control devices on the client. After adding devices, you can view the device status. For more details, refer to ***Add Device*** .
- **Group Zones/Radars**: You can group the added zones/radars into groups for convenient management. For more details, refer to ***Group Management*** .
- **Configure Zone Event**: By configuring linked actions of zone event on the client, you will be notified once the event is triggered. For more details, refer to ***Configure Client Linkage for Zone Event*** .
- **Remotely Control Security Panel**: You can remotely security control panel, including partition, zone, relay, and siren. For more details, refer to ***Remotely Control Security Control Panel*** .

- **Add Zone/Radar on Map**: You can add zone/radar to the map as hotspots. For more details, refer to ***Add Zone as Hot Spot*** and ***Add Security Radar as Hot Spot*** .
- **Map Application**: You can locate the resources, view alarm information and perform related control. Refer to ***Map Management*** .

15.2 Configure Security Control Panel Remotely

After adding security control panel to the client, you can go to the remote configuration page to configure related parameters of the device via the client. For the device added by Hik-Connect, if the second verification is enabled, you need to enter the user name and password of the device for remote configuration. It is widely used for the batch device maintenance scenario. For example, the installer can log in via Hik-Connect account and remotely maintain the devices of the end user.

Steps

1. Select **Device Management → Device → Device** .
2. Select the added security control panel, and click on Operation column.
3. **Optional:** For the device with the second verification enabled, enter the user name and password of the device, and click **OK**.

Result

The remote configuration page will be displayed.

15.3 Configure Client Linkage for Zone Event

Even if you are far away from a zone, you can still know what happens and how urgent the event is in a zone by configuring linked actions of zone event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of multiple zones in a batch at a time.

Before You Start

- Make sure you have added a security control panel.
- Make sure zones have been defined beforehand.
- Make sure events have been configured beforehand.

Steps

1. Click **Event Configuration → Alarm Event** .
2. Expand the zone list of a security control panel, and then select a zone from the list.
3. Check one or more event.
4. Click **Edit Linkage** to configure client actions.

   Audible Warning

   The client software gives an audible warning when an event is triggered. You can select the alarm sound for audible warning.

Note

Click **Add** to enter the alarm sound name and select a sound in your PC. For details, refer to ***Set Alarm Sound*** .

Send Email

Send an email of the alarm information to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Pop-up Window

Pop-up window to display the event related information (including event details, captured pictures of the linked camera, process record, and process field) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with red number (indicates the number of events, and the maximum number is 10) aside when the event is triggered, which helps the security guard to view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera (s).

Linked Camera

Link the selected camera(s) to capture picture when the zone event is triggered.

Select the camera(s) in the drop-down list.

Note

Up to 4 cameras can be selected as the linked cameras for a zone event.

Broadcast Linkage

Link the selected camera to broadcast certain audio file(s) when the event is triggered.

Note

Up to 100 speaker units, and up to 5 audio files can be selected.

PTZ Linkage

When the events are triggered, the cameras' **Preset**, **Patrol**, and **Pattern** will be called.

Note

Make sure you have configured presets, patrols, or patterns for the camera.

Alarm Output Linkage

The activation of an event will cause the connected alarm outputs (Max: 8) to activate, generating sounds, flashes, etc.

Access Point Linkage

When events are triggered, actions including Unlock Door, Lock Door, Remain Open, or Remain Closed are performed at the linked access points.

5. **Optional:** Click **Edit Priority** to set event priority as Uncatergorized/Low/Medium/High.
6. **Optional:** Click **Copy to...** to copy the event settings (including event priority, triggered client actions, and enabling/disabling the event) to other zones.
7. Click **OK**.
8. **Optional:** Enable or disable client actions for zone event.
   - Click **Enable All** or **Disable All** to enable or disable client actions of all zone events.
   - Switch **Enable** to ON/OFF to enable or disable client actions of one zone event.

   Enable Client Actions

   When client actions are enabled, client actions will be triggered when client receives zone event.

   Disable Client Actions

   When client actions are disabled, client actions will not work and actions will not be triggered when client receives zone event.
9. Click **Save**.

15.4 Remotely Control Security Control Panel

After adding the security control panel to the client, you can remotely control the partitions, zones, relays, and sirens of security control panel via the client software. For instance, you can arm, disarm, bypass, group bypass, etc. for both partitions and zones, and you can enable or disable relays.

Note

- The displayed interface is subject to the types of added security control panels.
- By default, AX Hub device uses HTTP port, and it does not support private ports.

15.4.1 Remotely Control Partitions

You can perform operations remotely on security control panel's partitions using the client such as away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and recovering group bypass.

Steps

Note

- The supported functions are subject to the added devices.
- If a zone of a partition does not work, you should bypass it before arming/disarming the partition, and then recover bypass when the zone works.

1. Enter **Security Control Panel** module.

2. Select a security control panel and click **Partition**.

   The name, status, arming status and linked zone of the partitions will be displayed in the list.
3. Select one or multiple partitions and click the following button(s).

   Away Arming

   An arming mode that works when all persons are absent from the monitored region. When away arming is enabled, all zones of the partition work properly.

   Stay Arming

   An arming mode that works when persons stay in the monitored region. When stay arming is enabled, zones inside of the region are armed while zones outside of the region will be bypassed where you can move in the zones without triggering any event.

   Instant Arming

   After arming a partition, its zone will alarm instantly when an event is triggered.

   Disarming

   All the zones (except 24-hour zones) in the partitions does not work any more after clicking, so that no event will be triggered in the disarmed zones.

   Note

   24-hour zones (e.g. 24-hour annunciating zones, 24-hour silent alarm zone, etc.) still can detect events and then alarm even if the partition is disarmed.

   Clear Alarm

   Stop the alarming of alarming devices.

   Group Bypass

   Bypass all the zones in one or more partition so that no event will be triggered in the bypassed zones before group bypass recovery.

   Note

   You should disarm the partition before bypassing it.

   Group Bypass Recovery

   Recover a group bypass to make all the zones in a partition work, so that you can arm the group.

15.4.2 Remotely Control Zones

You can use the client to remotely control the security control panel's zones including bypassing and recovering bypass.

Steps

1. Enter **Security Control Panel** module.
2. Select a security control panel and click **Partition**.

The name, status, arming status and linked zone of the partitions will be displayed in the list .

3. Click to open the Zone Operation panel.

   The zones linked with the partition, zone No., zone name, zone status, zone alarm status, battery will be displayed.

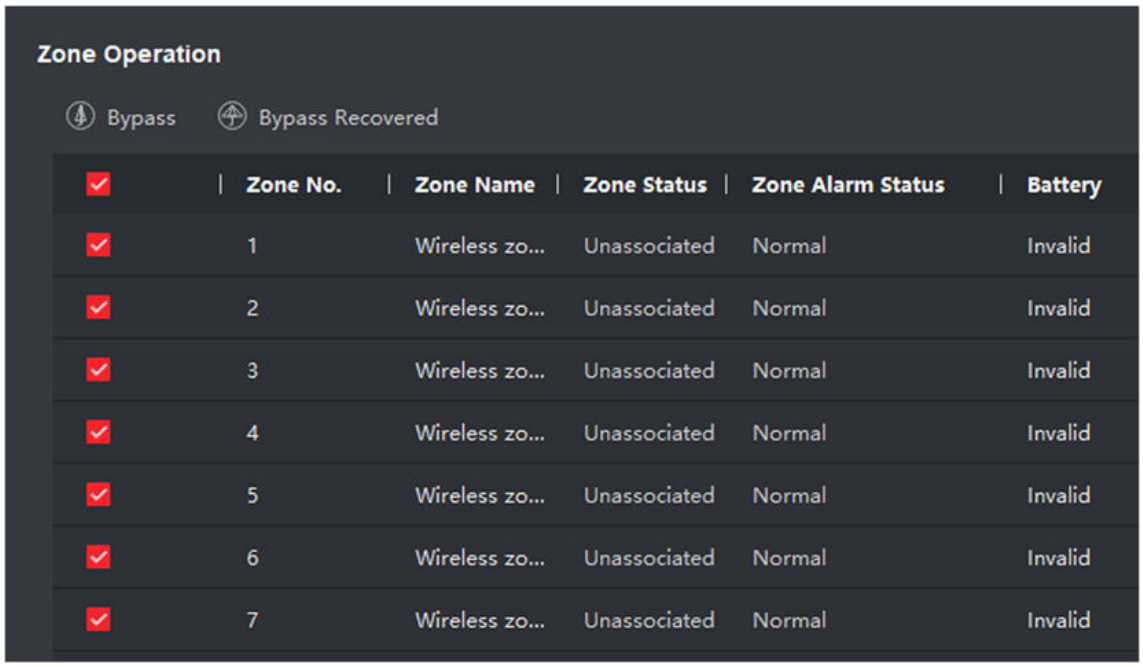


Figure 15-2 Zone Operation

Zone Status

Zone status can be unassociated, armed, disarmed, fault, shield, tamper-proof, etc.

Battery

The power of a zone's detector.

4. Check one or more zone in the list and click the following buttons.

Bypass

When a zone is bypassed, no event will be triggered in the zone, and you are not allowed to arm or disarm the zone, while other zones can be armed or disarmed.

Note

You should disarm the zone before bypassing it.

Bypass Recovery

After recovering bypass for a zone, you can arm it.

15.4.3 Remotely Control Relay

You can use the client to remotely change the on/off status of relay, and view the linked event of the relay.

Steps

1. Enter **Security Control Panel** module.
2. Select a security control panel, and then click **Relay**.

   The name, status, and linked event of the relay will be displayed.
3. Check one or multiple relays and click **Open** or **Close**.

Note

For AX Hub, you should set the **Relay Associated Event** as **Manual Control** in Device Management module.

15.4.4 Remotely Control Siren

You can control the siren status via the client remotely, including open and close. When the status of the siren is open, the detected alarm will trigger the alarm sound on the siren.

Enter **Security Control Panel** module, select a security control panel , and click **Siren** tab. Select one or multiple sirens, click **Open** or **Close** to open or close the sirens.

Chapter 16 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

16.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

   Note

   Up to 10 levels of organizations can be added.
4. **Optional:** Perform the following operation(s).

Edit Organization	Hover the mouse on an added organization and click to edit its name.
Delete Organization	Hover the mouse on an added organization and click to delete it. **Note** • The lower-level organizations will be deleted as well if you delete an organization. • Make sure there is no person added under the organization, or the organization cannot be deleted.
Show Persons in Sub Organization	Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

16.2 Add Persons

You can add persons to the client software one by one. The person information contains basic information, detailed information, profiles, access control information,credentials, custom information, etc.

16.2.1 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, email, phone number, etc.

Steps

1. Enter **Person** module.

   Note

   For the first time you enter **Person** module, a window pops up, and you can set the rules to generate person ID (letters and numbers supported) when adding person. When getting person information from device, if there are no person IDs, the person IDs will be generated according to the rule.

2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.

   The Person ID will be generated automatically.
4. Enter the basic information including person name, telephone number, email address, validity period, etc.

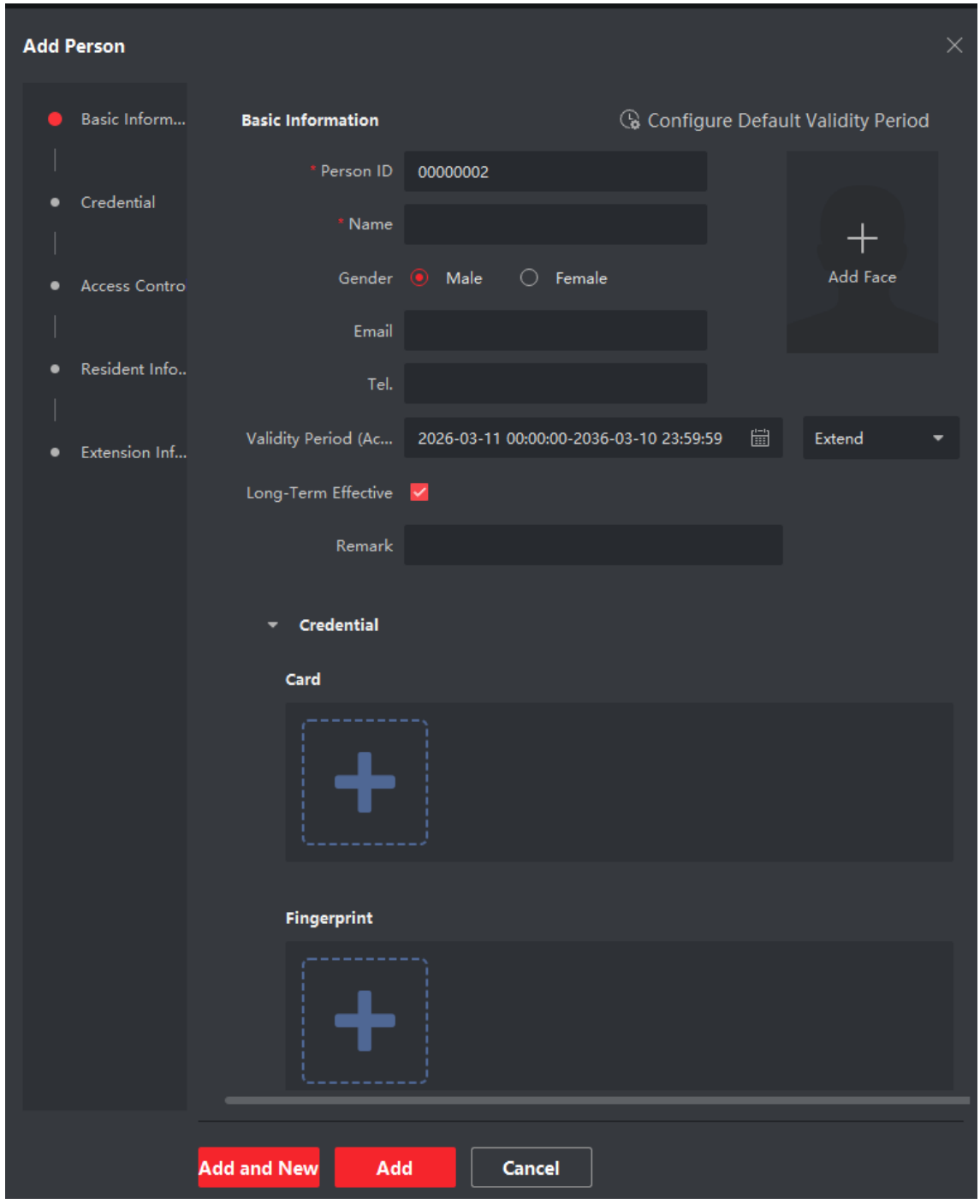


Figure 16-1 Configure Basic Information

Note

- **Configure Default Validity Period**: Upon completion of the configuration, the default validity period (access control) for any subsequent person will be set to this period.
- Once validity period expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors. You can click **Extend** to extend the person's validity period for 1 month, 3 months, 6 months, or 1 year.
- **Long-Term Effective**: When checked, the person's permissions remain valid permanently.

5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.
6. Delete Registered Face Picture

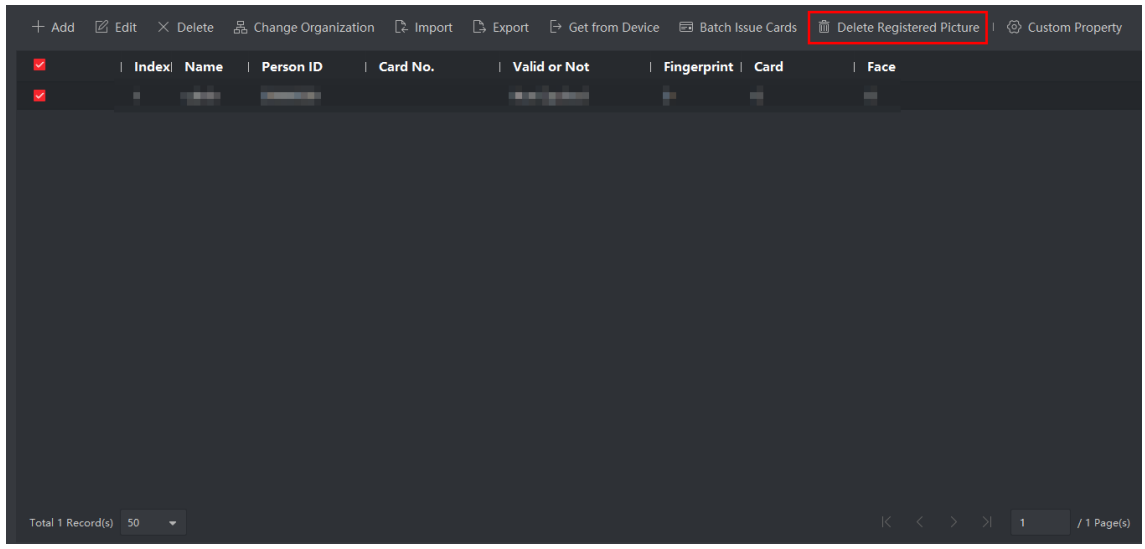


Figure 16-2 Delete Registered Picture

Note

If **Save Pictures in Structure Data Format** is enabled, the **Delete Registered Picture** button will be added to the **Person** page. In general, the registered face picture will be deleted automatically once the person's information is applied to the device. By double clicking the person, the **Edit Person** window will pop up, and you can check whether the registered face picture has been deleted. If not, you can select this person and click **Delete Registered Picture** to delete the picture manually.

16.2.2 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

   Note

   The picture should be in JPG or JPEG format and smaller than 200 KB.
6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.

   Note

   This function is hidden or shown according to the device capacity.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

16.2.3 Add Credentials

You can add credentials for persons, including card, face, fingerprint, iris, voice print, and palm print.

Issue a Card to One Person

When adding a person, you can issue a card to him/her as a credential to access the door(s). Before issuing a card to one person, you need to set the card issuing mode to get the card number. Except for manually entering the card number, the client also provides the other two modes for reading the card number: by local mode (via card enrollment station) or by remote mode (via the card reader of the access control device).

Note

Up to five cards can be issued to one person.

Issue a Card by Entering Card Number

When there is no device (card enrollment station/card reader) available to read card number, you can issue a card by manually entering card number.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Card** area, click + .

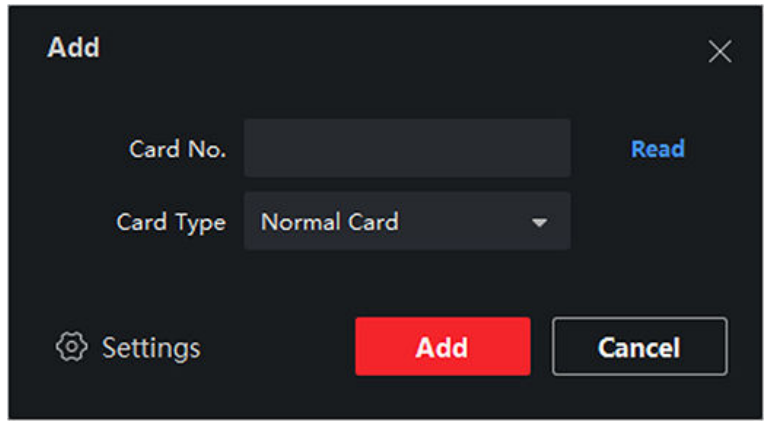


Figure 16-3 Add Card Page

4. Manually enter the card number in the Add page.
5. Click **Add**.

   The card will be issued to the person.

Issue a Card by Local Mode

If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Card** area, click + .
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.

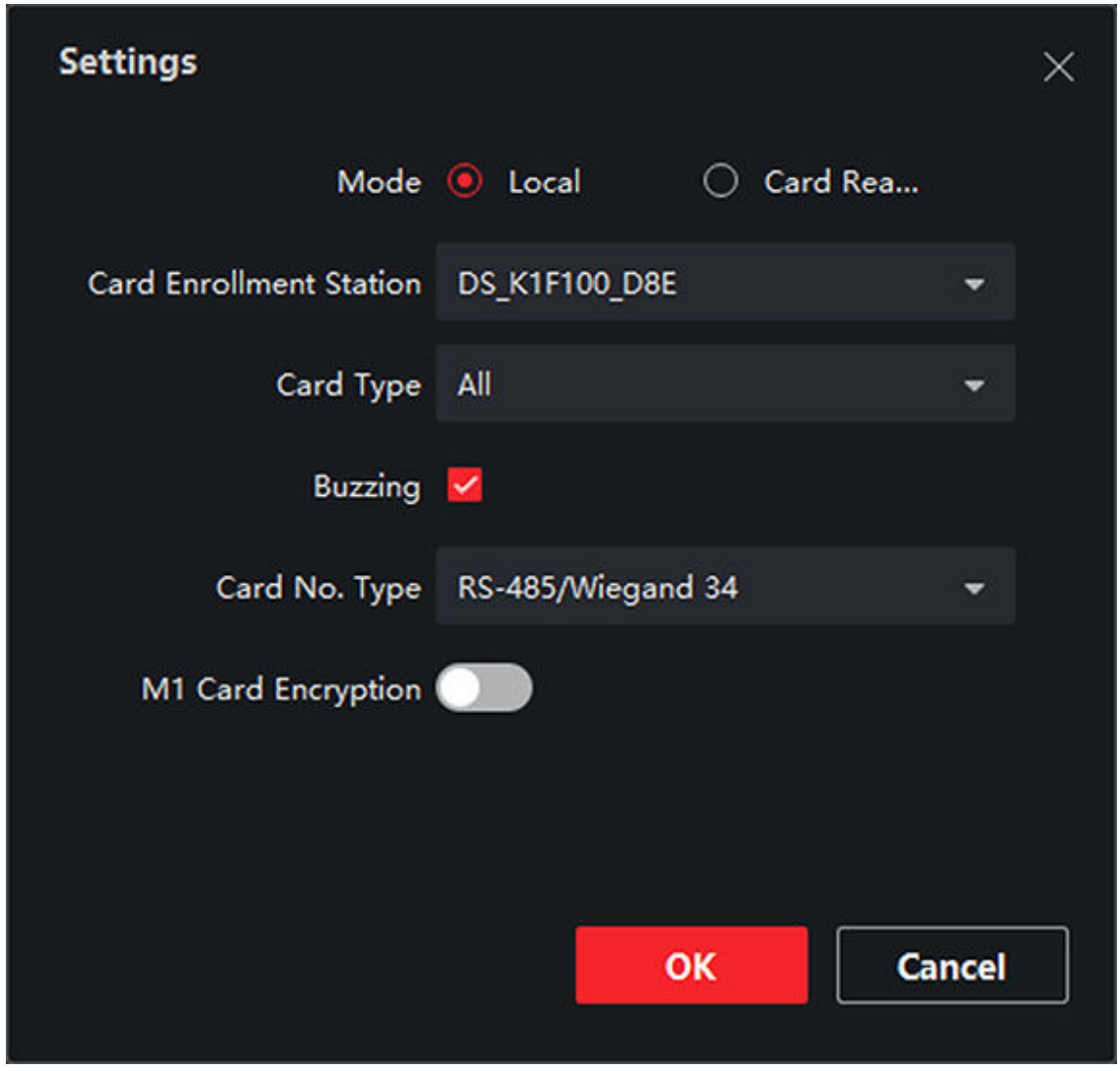


Figure 16-4 Issue a Card by Local Mode

6. Set other related parameters.

Card Enrollment Station

Select a model of card enrollment station from the drop-down list. You can connect the card enrollment station to the PC, and transfer the basic information about the added person between the two devices through USB.

RF Card Type

When choosing **Enrollment Station**, you can select the RF card type as EM card, CPU card, FeliCa card, etc.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E. Select the card type as EM card or M1 card according to the actual card type.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E. If the card is M1 card, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.

   The card number will display in the Card No. field automatically.
9. Click **Add**.

   The card will be issued to the person.

Issue a Card by Remote Mode

Except for issuing a card by local mode, you can also swipe the card on the card reader of the added access control device to get the card number. This is applicable when the client and the persons need issuing cards are not in the same location. For example, you can issue cards for employees in the branch company by remote mode via the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Card** area, click + .
4. Click **Settings** to enter the Settings page.
5. Select **Card Reader** as the card issuing mode.

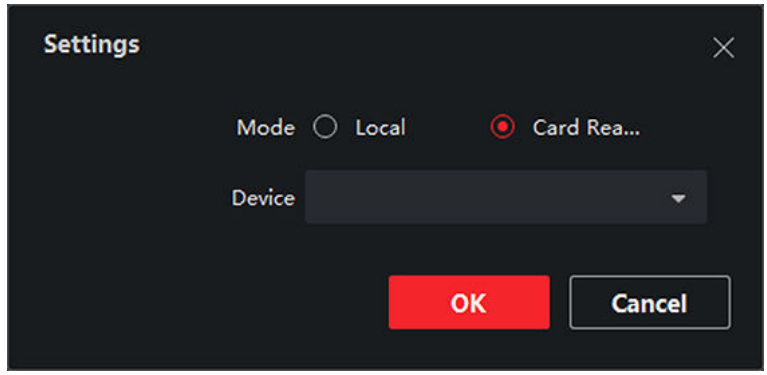


Figure 16-5 Issue a Card by Remote Mode

6. Select an access control device added in the client.
7. Select an added access control device or the enrollment station from the drop-down list.

Note

- If you select access control device, make sure you have armed the devices.
- If you select the enrollment station, you should click **Log In** to set related parameters of the device including IP address, port No., user name, and password. Also, you should check RF card type(s) as needed.

8. Click **OK** to confirm the operation.
9. Place the card on the card reader, and click **Read** to get the card number.

   The card number will display in the Card No. field automatically.
10. Click **Add**.

    The card will be issued to the person.

Take a Photo via Client

When adding a person, you can take a photo of a person by the client integrated camera, USB camera or enrollment station, and set this photo as the person's profile.

Before You Start

Make sure the PC running the client meets one of the following conditions:

- The client has a camera.
- You have connected USB camera to the PC.
- You have connected enrollment station to the PC by USB interface.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person window.

Note

Enter the person's basic information first. For details, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. Click to select the integrated camera or enrollment station from the drop-down list.

   When enrollment station is selected, live view is supported.
6. **Optional:** Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.

Note

This function is hidden or shown according to the device capacity.

7. Take a photo.
   1) Face to the camera and make sure your face is in the middle of the collecting window.
   2) Click to capture a face photo.
   3) **Optional:** Click to capture again.
   4) Click **OK** to save the captured photo.

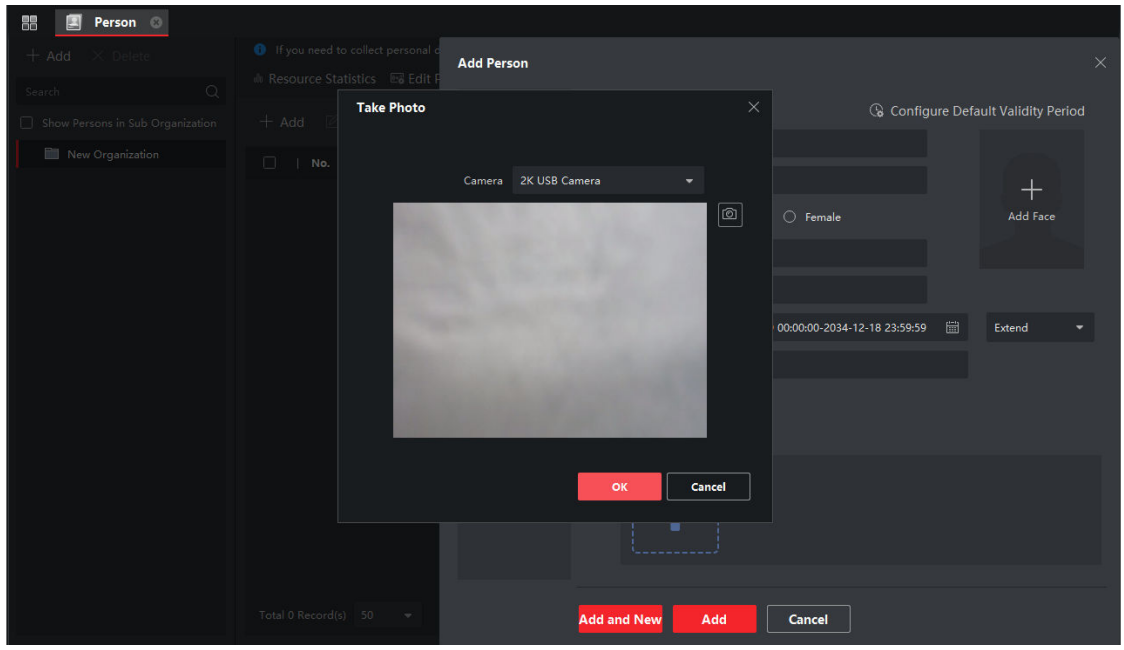


Figure 16-6 Captured Photo

8. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Log In** to set related parameters of the device including IP address, port No., user name, and password. Also, you can check **Face Anti-Spoofing** and select the liveness level as Low, Medium, or High. Live view is supported.

   Face Anti-Spoofing

   If you check this function, then the device can detect whether the face to be collected is an authentic one.
6. **Optional:** Click **Card Reader**, select the card reader ID, click **OK**.

   Note

   This function should be supported by device.
7. Collect face.
   1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
   2) Click to capture a photo.
   3) Click **OK** to save the captured photo.
8. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder or the enrollment station connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure the PC running the client meets one of the following conditions:

- The fingerprint recorder has been connected to the client.
- The enrollment station has been connected to the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Fingerprint** panel, click + .
4. In the pop-up window, select the collection mode as **Local**.
5. Select the model of the connected fingerprint recorder or the enrollment station.

   Note

   If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.
6. Choose the fingerprint type as normal, duress, or dismiss fingerprint.

   Normal Fingerprint

   Used for daily identity verification. The door unlocks normally upon successful authentication.

   Duress Fingerprint

   Used when a person is under coercion. The door unlocks normally after authentication, and the system automatically reports a duress event.

   Dismiss Fingerprint

   Used to disarm the alarm state at an access point.
7. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
8. Confirm to add the person.

Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click + .
4. In the pop-up window, select the collection mode as **Card Reader**.
5. Select an added access control device or the enrollment station from the drop-down list.

Note

If you select the enrollment station, you should click **Log In**, and set IP address, port No., user name and password of the device.

6. Choose the fingerprint type as normal, duress, or dismiss fingerprint.

   Normal Fingerprint

   Used for daily identity verification. The door unlocks normally upon successful authentication.

   Duress Fingerprint

   Used when a person is under coercion. The door unlocks normally after authentication, and the system automatically reports a duress event.

   Dismiss Fingerprint

   Used to disarm the alarm state at an access point.

7. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
8. Confirm to add the person.

Collect Iris via Client

When adding a person, you can collect the iris information by the iris recorder connected to the Client via USB. The iris recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure the iris recorder has been connected to the Client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Iris** panel, click + .
4. In the pop-up window, select the collection mode as **USB**.
5. Collect the iris.
   1) Click **Start** to recording the iris.
   2) Click **Add** to save the recorded iris.
6. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

Collect Iris via Access Control Device

When adding person, you can collect the person's iris information via access control device which supports iris recognition function.

Before You Start

Make sure iris collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Iris** panel, click + .
4. In the pop-up window, select the collection mode as **Card Reader**.
5. Select an added access control device from the drop-down list.
6. Collect the iris.
   1) Click **Start** to recording the iris.
   2) Click **Add** to save the recorded iris.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

Collect Voiceprint via Access Control Device

When adding person, you can collect voiceprint information via the access control device's voiceprint module. The voiceprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure voiceprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Voiceprint** panel, click + .
4. In the pop-up window, select the collection mode as **Card Reader**.
5. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Log In**, and set IP address, port No., user name and password of the device.
6. Collect the voiceprint.
   1) Click **Start**.
   2) Record the voice on the selected access control device to collect the voiceprint.
   3) Click **Add** to save the recorded voiceprint.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

Collect Palm Print via Client

When adding a person, you can collect the palm print by the palm print collector connected to the Client via USB. The palm print collected can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure the palm print collector has been connected to the Client via USB.

Steps

1. Enter **Person** module.
2. Select an organization in the left bar to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Palm Print** panel, click + .
4. In the pop-up window, select the collection mode as **USB**.
5. Collect the palm print.

Collected palm print images are stored by the system and included in retrieved person records.

Collect Palm Print via Access Control Device

When adding person, you can collect the person's palm print via the access control device supporting palm print collection. This is suitable for scenarios where the person being collected and the operator are in different locations, or where the palm print collector is fixed and cannot be connected to a computer via USB.

Before You Start
Make sure the access control device supporting palm print collection has been added to the Client.

Steps
1. Enter **Person** module.
2. Select an organization in the left bar and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Palm Print** panel, click + .
4. In the pop-up window, select the collection mode as **Card Reader**.
5. Select an added access control device from the drop-down list.
6. Collect the palm print.

   Collected palm print images are stored by the system and included in retrieved person records.

16.2.4 Configure Access Control Information

When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps
1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.
3. In the **Access Control** area, click ▾ to select access group(s) for the person.

Note

For details, refer to ***Assign Access Levels to Persons in Access Groups*** .

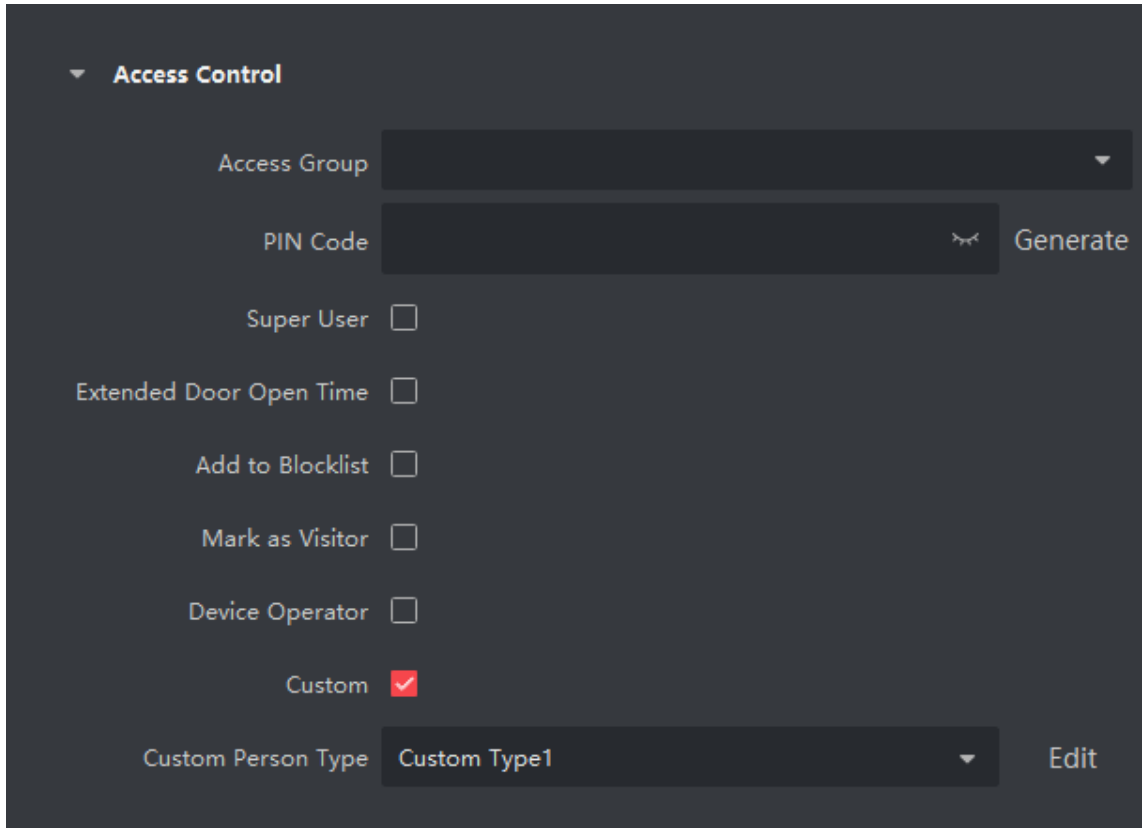


Figure 16-7 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
   - Manually enter a PIN code containing 4 to 8 digits.

     Note

     Persons' PIN codes cannot be repeated.
   - Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.

     Note

     If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.
5. Check the person's operation permissions.

   Super User

   If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

   Extended Door Open Time

   Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

For details about setting the door's open duration, refer to ***Configure Parameters for Door/ Elevator*** .

Add to Blocklist

Add the person to the blocklist and when the person tries to access doors/floors, an event will be triggered and sent to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.

Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

Custom

Custom person type for specific requirements.

6. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

16.2.5 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
   1) Click **Custom Property**.
   2) Click **Add** to add a new property.
   3) Enter the property name.
   4) Click **OK**.
3. Set the custom information when adding a person.
   1) Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

   2) In the **Custom Information** panel, enter the person information.

3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

16.2.6 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Resident Information** panel, select the indoor station to bind it to the person.

   Note

   If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

16.2.7 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

16.3 After Adding Persons: Operations on the Person List

After adding persons, you can perform the following operations on the person list.

16.3.1 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click on the added card to set this card as lost card.

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

16.3.2 Batch Edit Persons' Validity Period

Supports batch modification of validity periods for multiple personnel in the personnel list.

Before You Start

You have added persons.

Steps

1. Go to the **Person** page.
2. Select multiple personnel and click **Edit Validity Period**.
3. Extend the validity period or reset it as needed.

   Extend time options: 1 month, 3 months, 6 months, 1 year, 3 years, or long-term effective.
4. After saving, double-click any personnel row to check updated validity.

16.3.3 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

   The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.
6. Click **OK**.

16.3.4 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

   Note

   - If the person has multiple cards, separate the card No. with semicolon.
   - Items with asterisk are required.
   - By default, the Hire Date is the current date.
   - You can add custom columns after the last column.
7. Click ... to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.

Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start
Be sure to have imported person information to the client beforehand.

Steps
1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click ... to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

Import Person Information and Face Pictures

This feature allows you to import person information (XLSX/CSV) and face pictures (JPG) at one time through a ZIP package. The correspondence between person information and pictures is established by filling in the picture file name in the **Face Pictures** column of the template. Custom columns are also supported for import.

1. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
2. Click **Import → Person Information and Face** .
3. Click **Download Template for Importing Person** to save the XLSX/CSV template to your local device.

4. Edit the person information in the template.
   In the **Face Pictures** column, enter the exact file name of the corresponding face picture. You can also add custom columns after the last column, with a maximum of 5 additional columns.
5. Create a folder to store all face pictures.
6. Compress the template file and the picture folder into a single ZIP file.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.
- The file should be smaller than 800 MB. Only ZIP format zipper by WinRar is supported.
- Each face picture should be smaller than 200 KB. Only JPG pictures are supported.

7. Click ... to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.
   Once the import is successful, the custom fields will appear in the person list.

Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start

- Make sure you have added persons to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See ***Set General Parameters*** for details.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

Note

All persons' information will be exported if you do not select any organization.

3. Click **Export**.
4. Enter the super user name and password for verification.
   The Export panel is displayed.
5. Select **Person Information → Persons on Client / Persons on Device** .
   - **Persons on Client**: Export person information stored in the Client.
     Select column items to be exported, such as such as ID, organization, person name, gender, email, etc. If custom person properties or column items are configured in the person list, these custom columns can be selected for export. See ***Customize Column Display*** .
   - **Persons on Device**: Export person information stored in access control devices.
     The exported information includes person details (person ID, name, gender, validity period) and card number.

6. Click **Export** and enter encryption key (account password) to save the exported file in CSV/Excel file on your PC.

Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

- Make sure you have added persons and their face pictures to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See ***Set General Parameters*** for details.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' face pictures will be exported if you do not select any organization.
3. Click **Export** on the top menu bar.
4. Enter the super user name and password for verification.

   The Export panel is displayed.
5. Check **Face** as the content to export.
6. Click **Export** and set an encryption key to encrypt the exported file.

   Note

   - The exported file is in ZIP format.
   - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

Export Person Information and Face Pictures

Supports exporting person information and face pictures (ZIP) to PC simultaneously.

Note

- Make sure you have added persons to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See ***Set General Parameters*** for details.

1. Select an organization in the list.

   Note

   All persons' information will be exported if you do not select any organization.
2. Click **Export**.

   Enter the super user name and password for verification.

3. Select **Person Information → Person Information and Face** .
4. Select column items to be exported, such as such as ID, organization, person name, gender, email, etc.
   If custom person properties or column items are configured in the person list, these custom columns can be selected for export. See ***Customize Column Display*** .
5. Click **Export** and enter encryption key (account password) to save the exported file in CSV/Excel file on your PC.

16.3.5 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the added device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- Persons will be **Male** by default.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.
5. Select the **Getting Mode**.

   Note

   The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.
6. Click **Import** to start importing the person information to the client.

   Note

   Up to 2,000 persons and 5,000 cards can be imported.

   The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

16.3.6 Batch Issue Cards to Persons

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. **Optional:** Select a person group, and select the persons with no card issued.
   - The selected persons with no card issued in the person group will be displayed in the right panel.
   - If you do not select the persons with no card issued in a person group, all the added persons with no card issued will be displayed in the right panel.
3. Click **Batch Issue Cards**.
4. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
5. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to ***Issue a Card to One Person*** .
6. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
7. Click the **Card No.** column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Manually enter the card number and press the **Enter** key.

   The person(s) in the list will be issued with card(s).

16.3.7 Customize Column Display

You can customize the column items displayed in the person list, and these customized items can be selected for export.

Click **Customize Column Display** and you can choose which field to display or hide, including:

- Card number
- Credentials (card, face, iris, fingerprint, voiceprint)
- Number of palm prints

16.3.8 View Resource Statistics

After applying persons and access control credentials (including faces, cards, irises, fingerprints, voiceprints, and palm prints) to device, you can view resource statistics on client and on device to know whether the resources have been successfully applied.

You have applied persons and credentials to device. For details, refer to ***Assign Access Levels to Persons in Access Groups*** .

Click **Person Management → Resource Statistics** to enter Resource Statistics window.

In **Overview on Device** area, select a device from drop-down list, and click **Counting** to view device resources. By comparing resources on client and that on device, you can know whether the client resources have been applied to device.

Note

This function should be supported by device. If the device does not support face or fingerprint, a prompt will pop up on the bottom right corner of the PC desktop.

Chapter 17 Access Control

The Access Control module is applicable to access control devices and video intercom device. It provides multiple functionalities, including access group configuration, video intercom, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to ***Add User*** .

17.1 Flow Chart

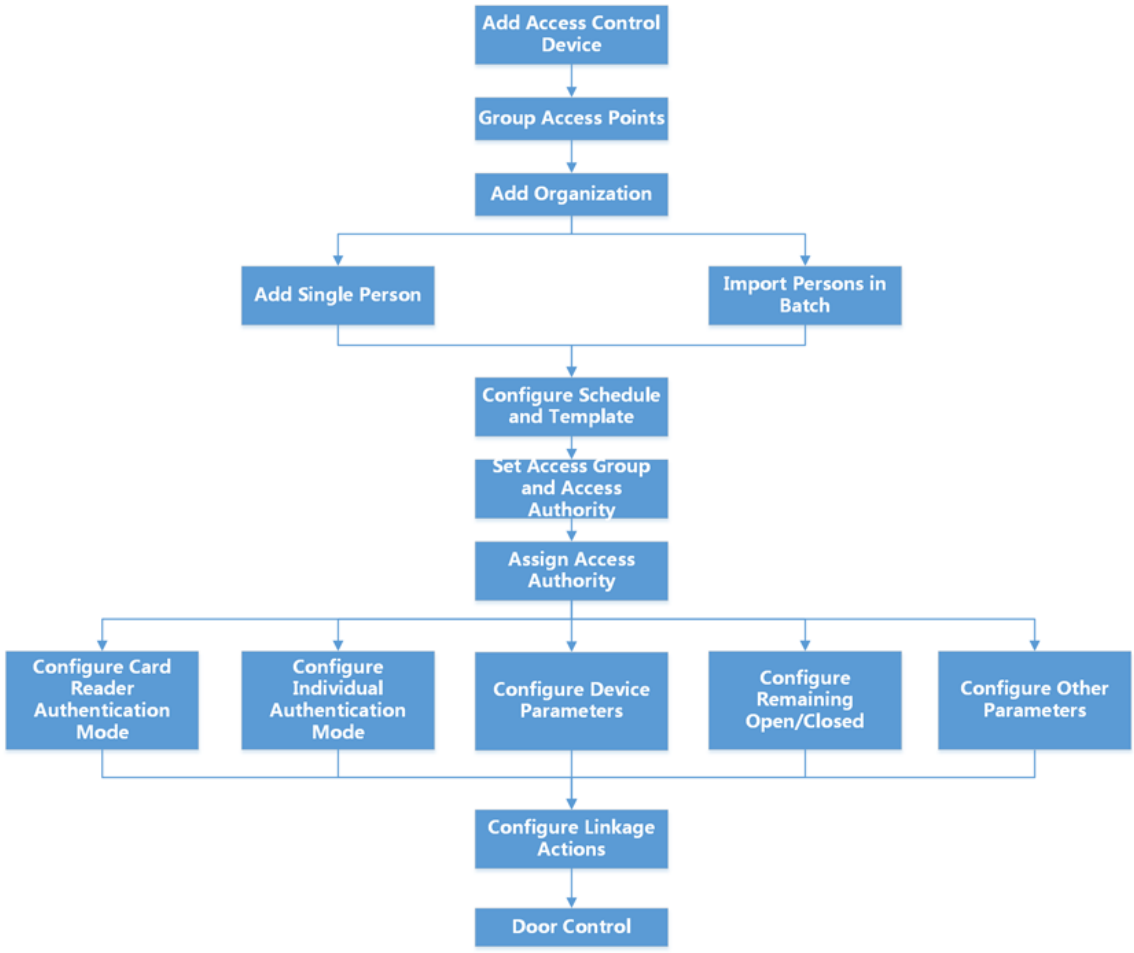


Figure 17-1 Flow Chart of Access Control

- **Add Access Control Device:** You can add access control devices on the client. For more details, refer to ***Add Device*** .
- **Group Access Points:** You can group the added access points into groups for convenient management. For more details, refer to ***Group Management*** .
- **Add Organization:** You can add an organization and import person information to the organization for managing persons. For more details, refer to ***Add Organization*** .
- **Configure Schedule and Template:** You can configure the template including holiday and week schedule. For more details, refer to ***Configure Schedule and Template*** .
- **Set Access Group and Access Authority:** You can set an access group to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect. For more details, refer to ***Assign Access Levels to Persons in Access Groups*** .
- **Configure Device Parameters:** You can configure parameters for the access control device, including device time, linkage settings, maintenance settings, etc. For more details, refer to ***Configure Access Control Parameters*** .
- **Configure Remaining Open/Closed:** You can set the status of the door as open or closed and set the elevator controller as free and controlled. For more details, refer to ***Configure Remaining Unlocked/Locked*** .
- **Configure Card Reader Authentication Mode:** You can set the passing rules for the card reader of the access control device according to your actual needs. For more details, refer to ***Configure Card Reader Authentication Mode and Schedule*** .
- **Configure Individual Authentication Mode:** You can set the passing rules for person to the specified the access control device according to your actual needs. For more details, refer to ***Configure Person Authentication Mode*** .
- **Configure Other Parameters:** You can set parameters for access control devices such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc. For more details, refer to ***Configure Other Parameters*** .
- **Configure Linkage Actions:** You can configure linkage action for access control, so that the events can trigger a series of linkage actions to notify the security personnel. For more details, refer to ***Configure Linkage Actions for Access Control*** .
- **Door/Elevator Control:** You can view the real-time status of the doors or elevators managed by the added access control device. For more details, refer to ***Door/Elevator Control*** .

17.2 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to ***Assign Access Levels to Persons in Access Groups*** .

17.2.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control → Schedule → Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

   Note

   Up to 16 holiday periods can be added to one holiday.

   1) Click **Add** in the Holiday List field.
   2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

      Note

      Up to 8 time durations can be set to one holiday period.

   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Click the time duration, check **Enable Authentication Attempts** and enter the max. authentication attempts.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
   4) **Optional:** Select the time duration(s) that need to be deleted, and then click in the Operation column to delete the selected time duration(s).
   5) **Optional:** Click in the Operation column to clear all the time duration(s) in the time bar.
   6) **Optional:** Click in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

17.2.2 Add Schedule Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control → Schedule Template → Schedule Template** to enter the Template page.

   Note

   There are two default templates: **All-Day Authorized** and **All-Day Denied**, and they cannot be edited or deleted.

   All-Day Authorized

   The access authorization is valid in each day of the week and it has no holiday.

   All-Day Denied

   The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
3. Create a name for the template.
4. Enter the descriptions or some notification of this template in the Remark field.
5. Edit the week schedule to apply it to the template.
   1) Click **Week Schedule** tab on the lower panel.
   2) Select a day of the week and draw time duration(s) on the timeline bar.

      Note

      Up to 8 time duration(s) can be set for each day in the week schedule.

   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Click the time duration, check **Enable Authentication Attempts** and enter the max. authentication attempts.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
   4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.

Note

Up to 4 holidays can be added to one template.

1) Click **Holiday** tab.
2) Select a holiday in the left list and it will be added to the selected list on the right panel.
3) **Optional:** Click **Add** to add a new holiday.

Note

For details about adding a holiday, refer to ***Add Holiday*** .

4) **Optional:** Select a selected holiday in the right list and click to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.

7. Click **Save** to save the settings and finish adding the template.

17.3 Assign Access Levels to Persons in Access Groups

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, iris, voice print, palm print, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

Note

You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.

7. Click **Save**.

Note

Up to 50 access groups can be added.

You can view the selected person(s) and the selected access point(s) on the right side of the interface.

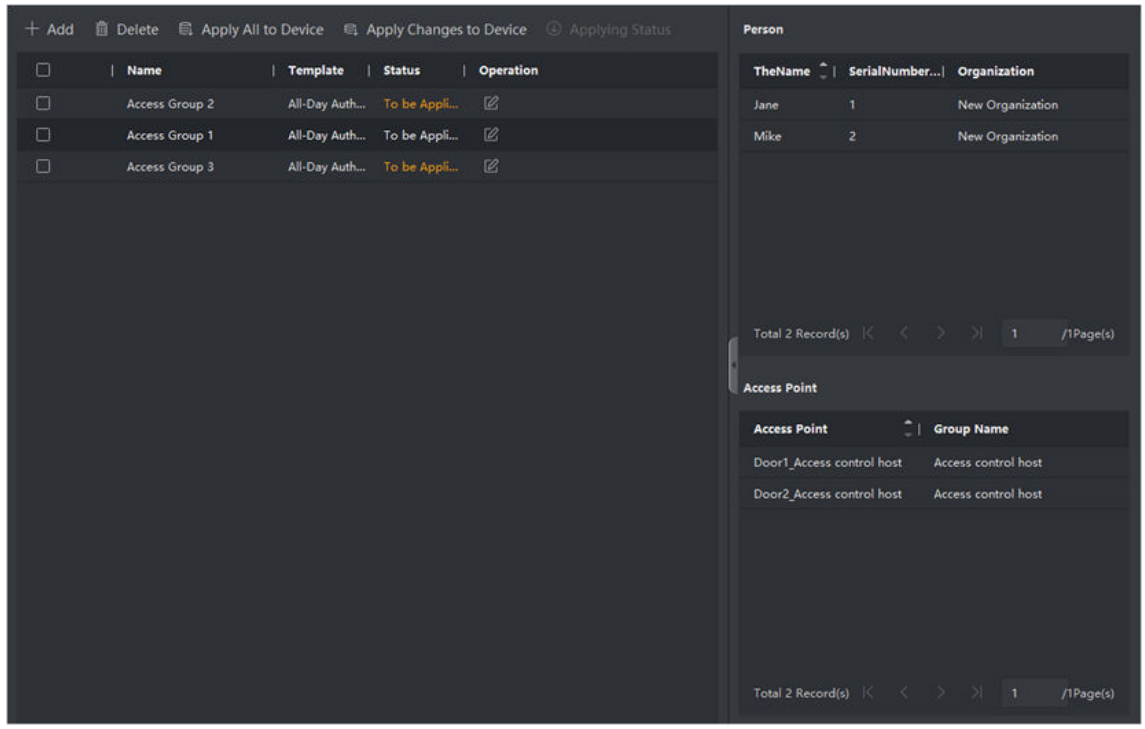


Figure 17-2 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

      Apply All to Devices

      This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

      Apply Changes to Devices

      This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).
   4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.
You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

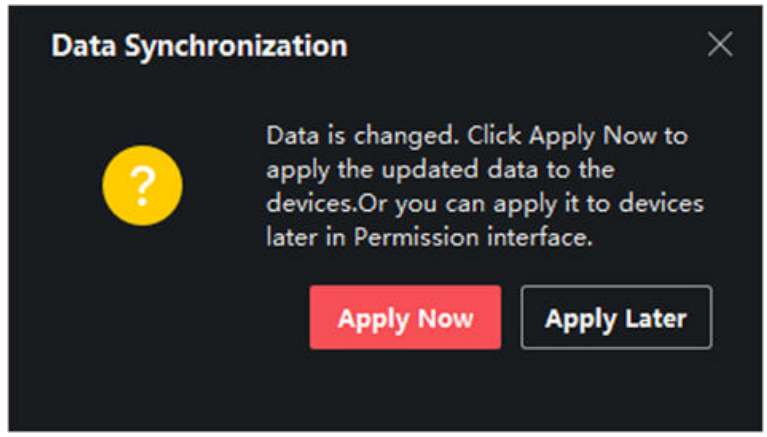


Figure 17-3 Data Synchronization

17.4 Search Access Group

After setting access group and assigning access authority to persons, you can search the access group that the person belongs to and view other related information including credential No., credential type, applying status, etc.

Note

Make sure you have set access group to assign access authorization to designed persons and applied it. For details, refer to ***Assign Access Levels to Persons in Access Groups*** .

Click **Access Control → Authorization → Search** . Select a device name, and set search condition (including person name and applying status, optional), and then click **Search**.

You can view the application statistics of the access group which counting the applied person information and credentials, and view other information on the list including the credential type, door name, credential No., applying status, remark, etc.

17.5 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click to customize the advanced function(s) to be displayed.

17.5.1 Configure Access Control Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Before You Start
Add access control device to the client.

Steps
1. Click **Access Control → Advanced Function → Device Parameter** .

   Note

   If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click to select the Device Parameter to be displayed.
2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

   Note

   - The displayed parameters may vary for different access control devices.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

   RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Fingerprint Recognition Mode

Recognition on Card Reader

The fingerprint storage and comparison are performed on the card reader.

Recognition on Access Controller

The fingerprint storage and comparison are performed on the access controller.

Note

The fingerprint data for the two modes are not compatible. You need to reapply the data when switching modes.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. Select an access control device on the left panel, and then click to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Remind Before Locking Door

Remind users that the door is about to close.

Reminder

Set the time (seconds) to warn users that the door is about to close. It should be less than the Open duration and Extended Open Duration.

Passing Detection

Check whether the door has been pushed open or used after the door lock is opened. If it has not been pushed open or used, an event will be uploaded.

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.
6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Repeated Authentication Interval

Within the specified interval, repeated authentication of the same card number (uploaded by different devices) is invalid, and only one authentication is performed. You can set it as 0 to 65535 seconds.

Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.

Before You Start

Add access control device to the client, and make sure the device supports alarm input.

Steps

Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

Name

Edit the alarm input name as desired.

Detector Type

The detector type of the alarm input.

Zone Type

Set the zone type for the alarm input.

Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

Trigger Alarm Output

Select the alarm output(s) to be triggered.

4. Click **OK**.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start
Add access control device to the client, and make sure the device supports alarm output.

Steps
1. Click **Access Control → Advanced Function → Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.
4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Before You Start
Add access control device to the client.

Steps
1. Click **Access Control → Advanced Function → Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

   Passing Mode

   Select the controller which will control the barrier status of the device.

   - If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
   - If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

   Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Barrier Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

Note

The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .

Note

0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

17.5.2 Configure Remaining Unlocked/Locked

You can set the status of the door as remaining unlocked, remaining locked, normal, and set the elevator controller as free and controlled. For example, you can set the door remaining locked in the holiday, and set the door remaining unlocked in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control → Advanced Function → Remain Locked/Unlocked** to enter the Remain Locked/Unlocked page.
2. Select the device that need to be configured on the left panel.
3. Click the **Week Schedule** and perform the following operations.
   1) For door, click **Remain Unlocked**, **Remain Locked**, **Normal**, **Inductive Mode**, or **Barrier-Free Mode**.

Note

- **Inductive Mode**: The door opening and closing is triggered by infrared induction of human body.
- **Barrier-Free Mode**: When a large number of people need to pass the door, the door will remain open (without frequent authentication) if the person and ID comparison succeeds. Only when the person and ID comparison fails, the door will be closed.
- Inductive mode and barrier-free mode should be supported by device.

2) For elevator controller, click **Free** or **Controlled**.
3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to each day in the week schedule.

4) **Optional:** Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
5) Click **Save**.

Related Operations

Copy to Whole Week	Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.
Delete Selected	Select one duration on the time bar, click **Delete Selected** to delete this duration.
Clear	Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
1) Click one specific mode.
2) Click **Add**.
3) Enter the start date and end date.
4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

5) Perform the following operations to edit the time durations.

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
- Click the time duration and directly edit the start/end time in the appeared dialog.
- Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

6) **Optional:** Select the time duration(s) that need to be deleted, and then click in the Operation column to delete the selected time duration(s).
7) **Optional:** Click in the Operation column to clear all the time duration(s) in the time bar.
8) **Optional:** Click in the Operation column to delete this added holiday period from the holiday list.
9) Click **Save**.

5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

17.5.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Assign Access Levels to Persons in Access Groups*** .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multi-Factor Auth** .
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
   1) Click **Add** on the right panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the person/card group.
   4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

   Note

   - Make sure you have issue card(s) to the person. For details refer to ***Issue a Card to One Person*** .
   - Make sure you have set access group and apply the access group to the access control device successfully. For details, refer to ***Assign Access Levels to Persons in Access Groups*** .

   5) Click **Save**.
   6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
   7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.

4. Configure an authentication group.

1) Select an access control point (door) of the selected device on the left panel.
2) Enter the **Authentication Interval** (the maximum interval when entering password).
3) Click in the Operation column to enter the Edit Authentication Group pane.
4) Select a configured template as the authentication template from the drop-down list.

Note

For setting the template, refer to ***Configure Schedule and Template*** .

5) Select the authentication mode as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

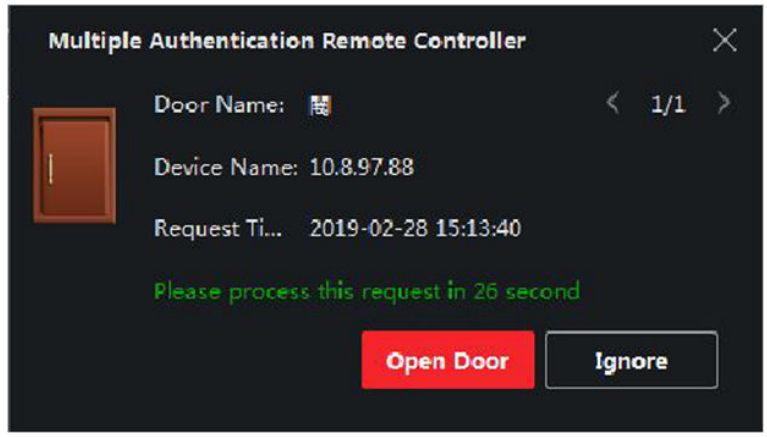


Figure 17-4 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

6) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
7) Switch on **Offline Authentication** to enable authentication via the super password when the device is offline.
8) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

9) Click **Save**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

5.
6. Click **Save**.

17.5.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start
Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.
- For details about the custom Wiegand, see ***Custom Wiegand Rule Descriptions*** .

1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the Custom Wiegand page.
2. Select a custom Wiegand on the left.
3. Create a Wiegand name.

Note

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

Note

- Up to 80 bits are allowed in the total length.
- The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
- The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.

6. Set output transformation rule.

1) Click **Set Rule** to open the Set Output Transformation Rules window.

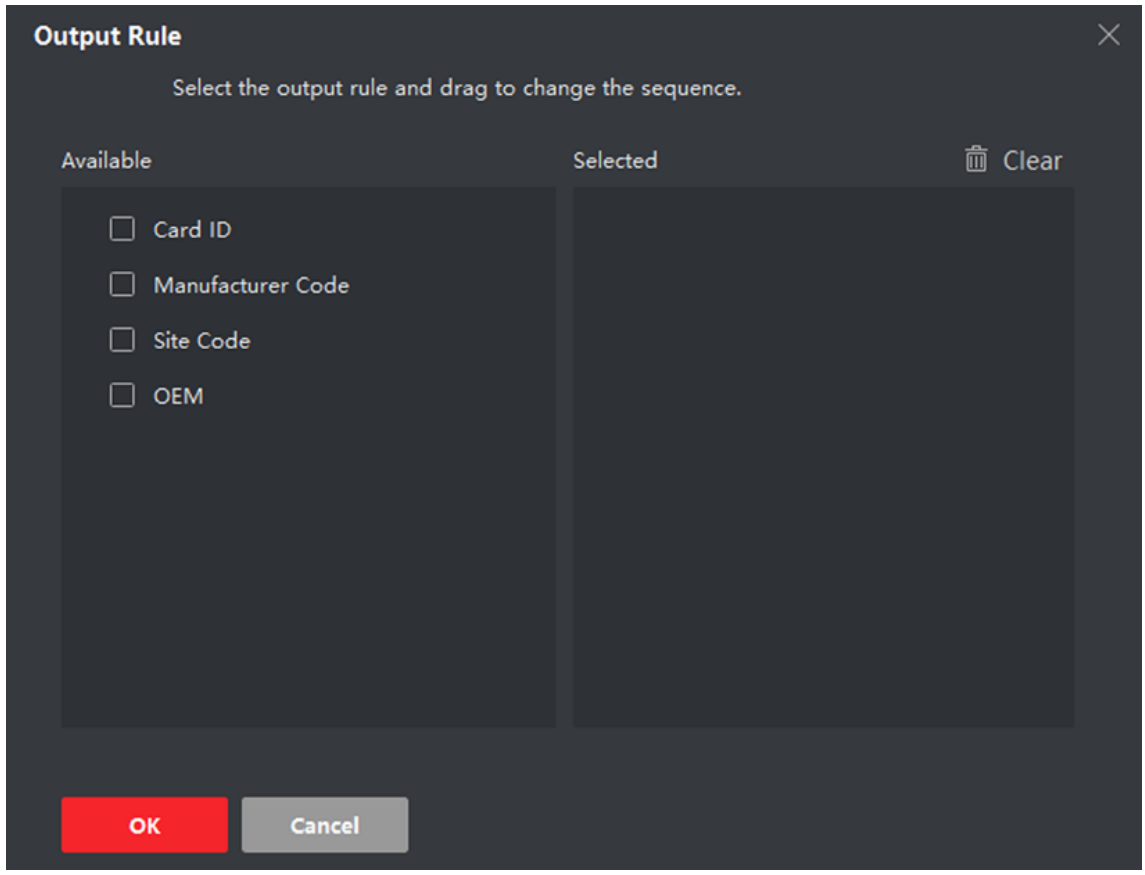


Figure 17-5 Set Output Transformation Rule

2) Select rules on the left list.

The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.

4) Click **OK**.

5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

17.5.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control → Advanced Function → Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
   1) Click **Configuration**.

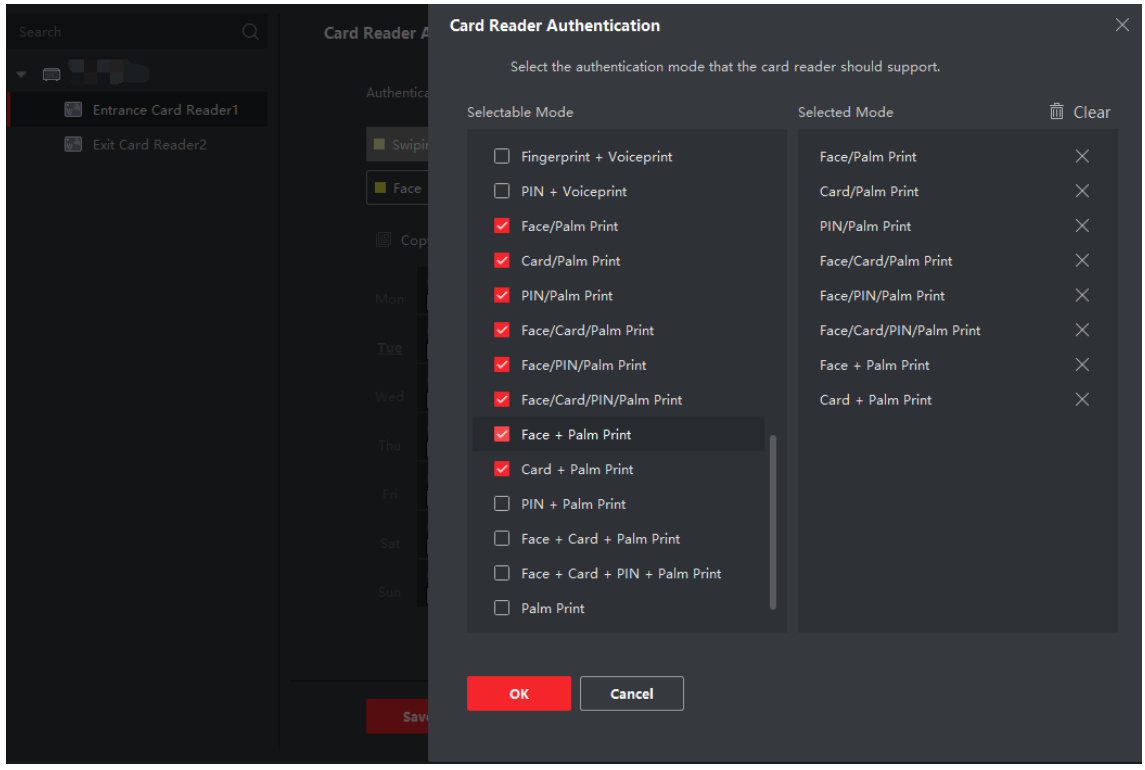


Figure 17-6 Set Card Reader Authentication Mode

Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information*** .

   2) Check the modes in the Available Mode list and they will be added to the selected modes list.
   3) Click **OK**.

   After selecting the modes, the selected modes will display as icons with different color.
4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.

5. Repeat the above step to set other time periods.

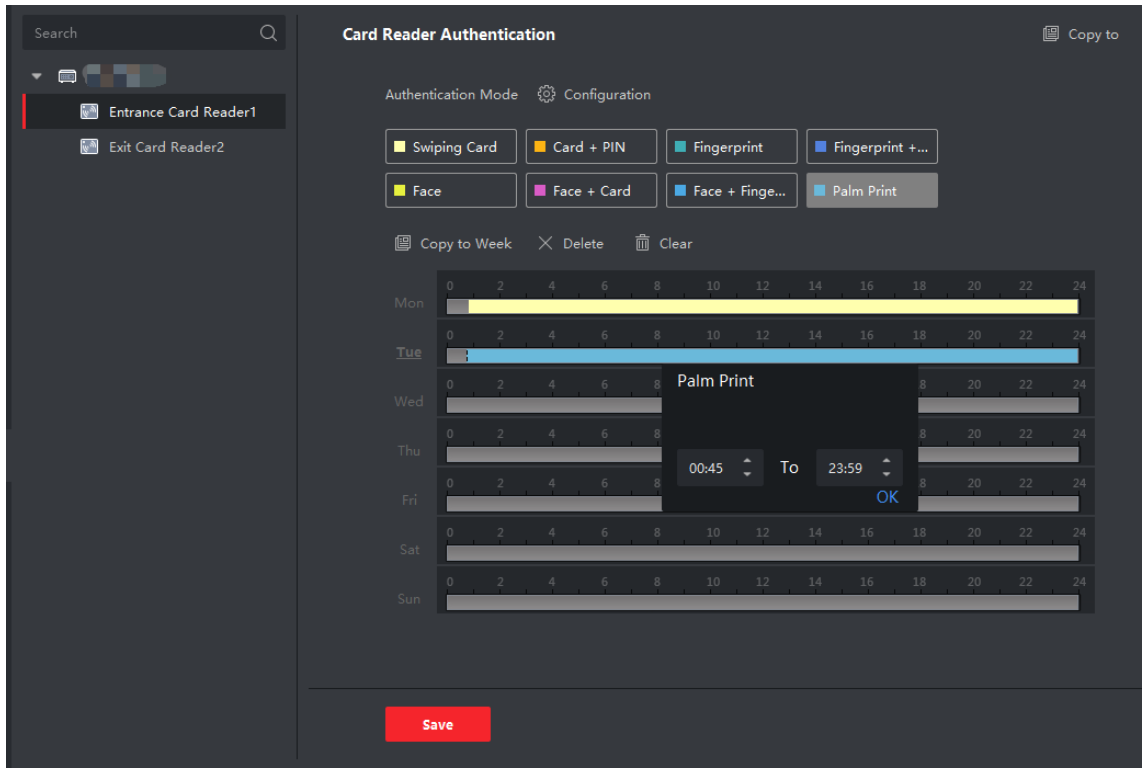


Figure 17-7 Set Time Period

6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

17.5.6 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to your actual needs.

Before You Start

- Add access control device to the client, and make sure the access control device support the function of person authentication.
- Add person and assign access authorization to designed person. For details, refer to ***Person Management*** and ***Assign Access Levels to Persons in Access Groups*** .

Steps

1. Click **Access Control → Advanced Function → Authentication** .
2. Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.

3. Click **Add** to enter the Add window.
4. Select the person(s) need to be configured on the left panel.

   The selected person(s) will be added to the right panel.
5. Select the authentication mode on the drop-down list of **Authentication Mode**.
6. Click **OK**.

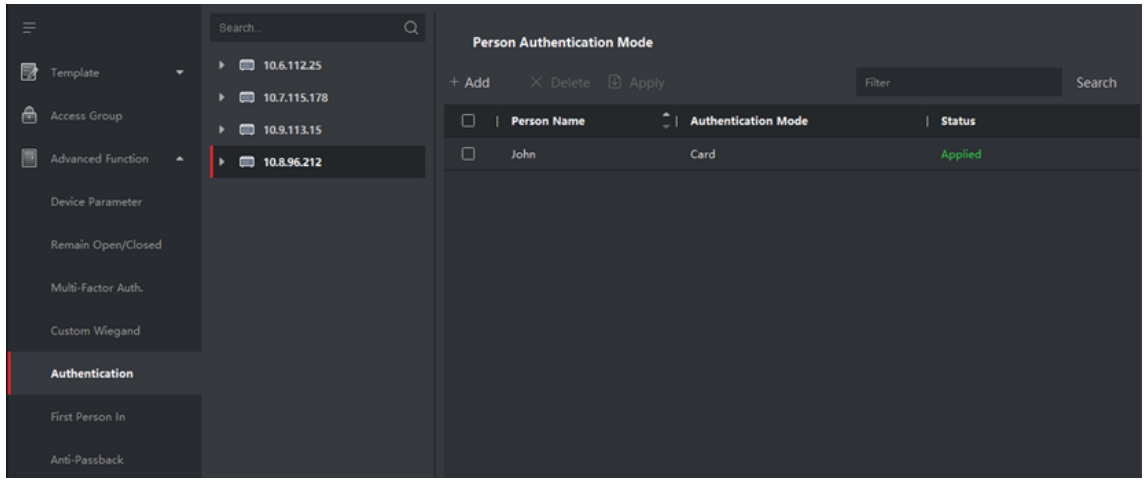


Figure 17-8 Set Authentication Modes for Persons

7. **Optional:** Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

Note

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

17.5.7 Configure Relay for Elevator Controller

For elevator controller, you can manage the relationship between the floor and the relay and configure the floor's relay type. Different relay type can implement different functions. By configuring the relationship between the floor and the relay, you can assign different functions to the elevator and control the elevator.

Configure Relationship between Relay and Floor

You can assign different relay types to the target floors, and each floor can be assigned with 3 relay types. By this way, you can call the elevator, and assign the operations for different floors.

Before You Start

Add the elevator controller to the client.

Steps

1. Click **Access Control → Advanced Function → Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right.

   There are three types of relay available.

   Button

   Control the validity for buttons of each floor.

   Note

   represents button relay.

   Call Elevator

   Control to call the elevator to go to the specified floor by indoor station or outdoor station.

   Note

   represents the call elevator relay.

   Auto

   Control to press the button when the user swipes card inside the elevator. The button of the floor will be pressed automatically according to the user's permission.

   Note

   represents the auto button relay.

   Example

   Take the following picture as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the relay, and the icon represents the relay type. You can change the relay type. For details, refer to ***Configure Relay Type*** .



Figure 17-9 Relay

4. Configure the relationship between the relays and the floors.
   - Drag the unconfigured relay from the Unconfigured Relay panel to the target floor in the Floor List panel.
   - Drag the relay from the Floor List panel to the Unconfigured Relay panel.
   - Drag the relay from one floor to another floor in the Floor List panel. If the target floor has already configured with a relay of the same type as the dragged one, it will replace the existed one of the same type.

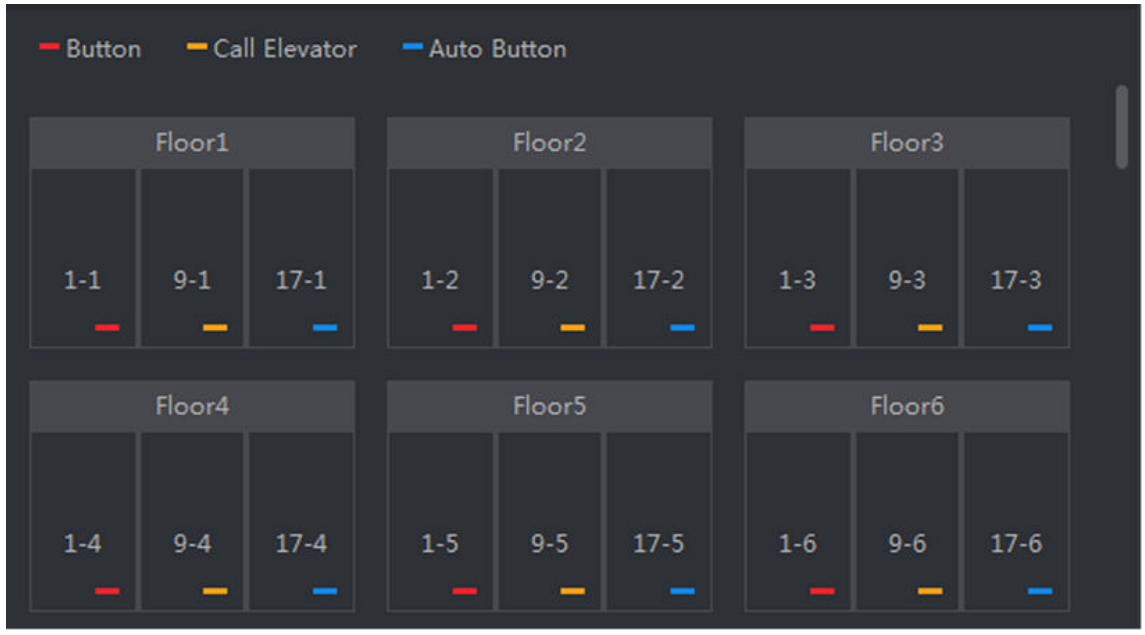


Figure 17-10 Relationship Between Relay and Floor

Note

- An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
- By default, the relay total amount is the added floor number *3 (three types of relay).
- Up to 3 types of relay can be dragged to one floor.
- If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.

5. **Optional:** Click **Skip-Floor Configuration** in the upper-right corner to configure skip-stop operations by selecting target floors as non-stopping floors. Access-forbidden floors (e.g., mechanical rooms, staff zones) will be omitted from elevator service when designated as non-stop floors.
6. Click **Save** to apply the settings to the selected elevator controller.

Configure Relay Type

To implement different functions, you can configure different relay type, including: button relay, call elevator relay and auto button relay. Different relay type can implement different functions. The button relay is to control the validity for buttons of each floor.. The call elevator relay is to call the elevator to the specified floor by indoor station or outdoor station. The auto button relay is to control to press the button when the user swipes card inside the elevator, the button of the floor will be pressed automatically according to the user's permission.

Steps

1. Click **Access Control → Advanced Function → Elevator Configuration** to enter the Relay Settings page.
2. Select an elevator controller on the left of the page.
3. Click **Relay Type Settings** to open the Relay Type Settings window.

Note

- All relays in the Relay Type Settings window are unconfigured relays.
- Three types of relay are available: represents the button relay, represents the call elevator relay, and represents the auto button relay.

4. Drag the relay from one relay type panel to the target one.

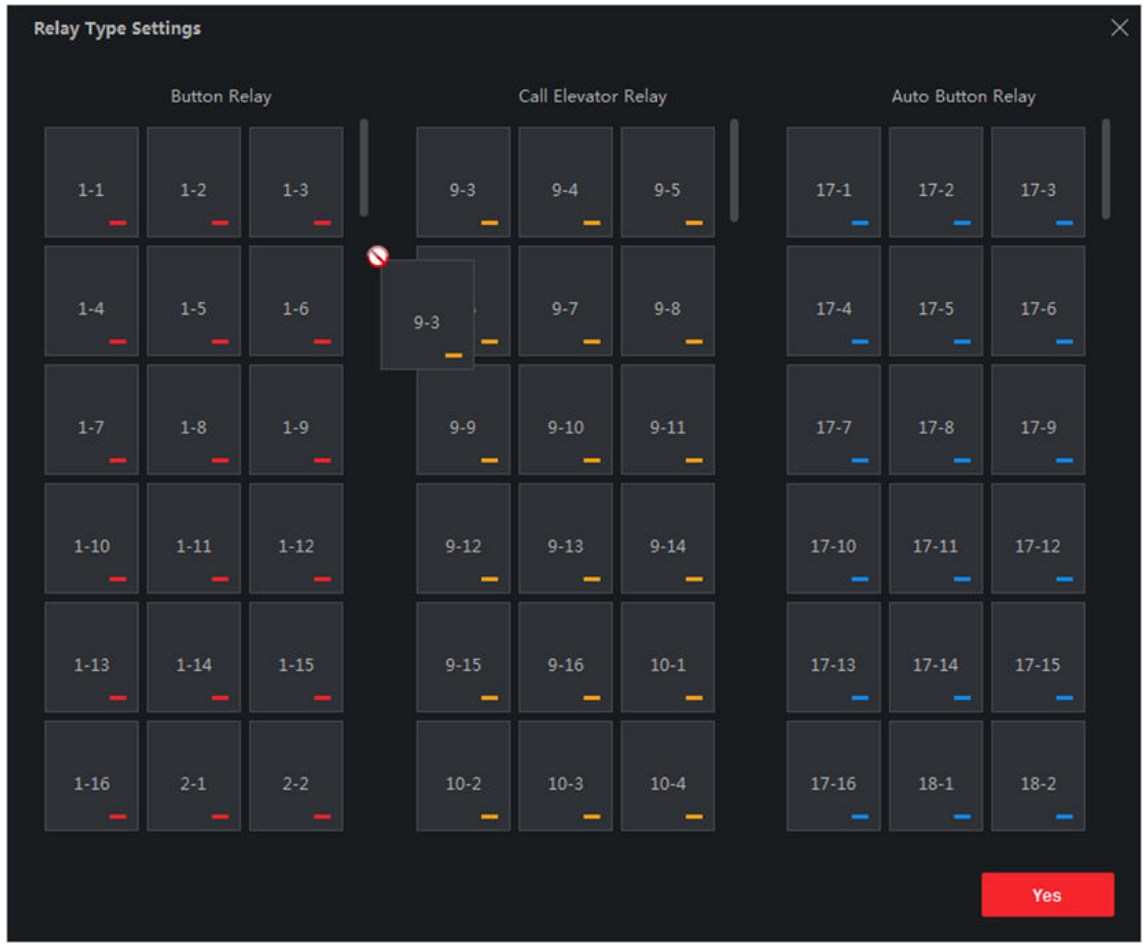


Figure 17-11 Configure Relay Type

5. Click **OK**.

17.5.8 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to ***Person Management*** and ***Assign Access Levels to Persons in Access Groups*** .

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

   Enable Remaining Open after First Person

   The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the consecutive authentication times and interval of consecutive authentication.

   Note

   The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

   Disable Remaining Open after First Person

   Disable the function of first person in, namely normal authentication.

   Authorization by First Person

   All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

   Note

   You can authenticate by the first person again to disable the first person mode.
4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

17.5.9 Configure Anti-Passback

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which access credentials must be used in order to grant access. You can set the sequence according to the actual path via the client and if the person uses the credential in wrong sequence, you can also reset the anti-password records.

Before You Start
Add access control device to the client, and enable the anti-passing back function of the access control device.

Steps

Note
Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking*** .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

   Note
   Up to four afterward card readers can be added as afterward card readers for one card reader.
6. Click **OK** in the dialog to save the selections.
7. Select an anti-passback reset mode:
   - Reset authentication validity period: After a successful authentication, re-authentication is not allowed within the set duration. Access is automatically restored once the duration elapses.
   - Reset time: After a successful authentication, re-authentication is not allowed until the set time point is reached. Access is automatically restored at that time point.
   - Disable: No restriction on repeated authentication.
8. Enable timed anti-passback: Set the reset time and select the reader. This feature prevents personnel from re-entering the same area within the set reset period. After the reset time elapses, they can authenticate again to gain entry.

   This feature requires device support.
9. Disable anti-passback function in specified time period: Set the time periods during which anti-passback is not enforced.
10. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

11. Click **Reset Anti-Passback** and select the person(s) to delete the related anti-passback records about the person(s) on the device.

Note

This function should be supported by the device.

17.5.10 Configure Cross-Controller Anti-Passback

You can set anti-passback for card readers in multiple access control devices. You should swipe the card according to the configured swiping card route. And only one person could pass the access control point after swiping the card. You can configure area anti-passback rules or route anti-passback rules for different scenarios.

Note

It should be supported by the device.

Configure Route Anti-Passback Based on Card

The route anti-passback depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will judge the anti-passback according to the entrance and exit records on the card.

Perform this task if you need to configure route anti-passback and judge the anti-passback according to the entrance and exit records on the card.

Steps

Note

It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to ***Enable M1 Card Encryption*** .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-Passback** to enter the cross-controller Anti-Passback configuration page.
2. Check **Enable Cross-Controller Anti-Passback** to enable the function.
3. Select **Based on Card** as the anti-passback mode.
4. Select **Route Anti-Passback** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passback.

Note

Up to 64 devices with anti-passback function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

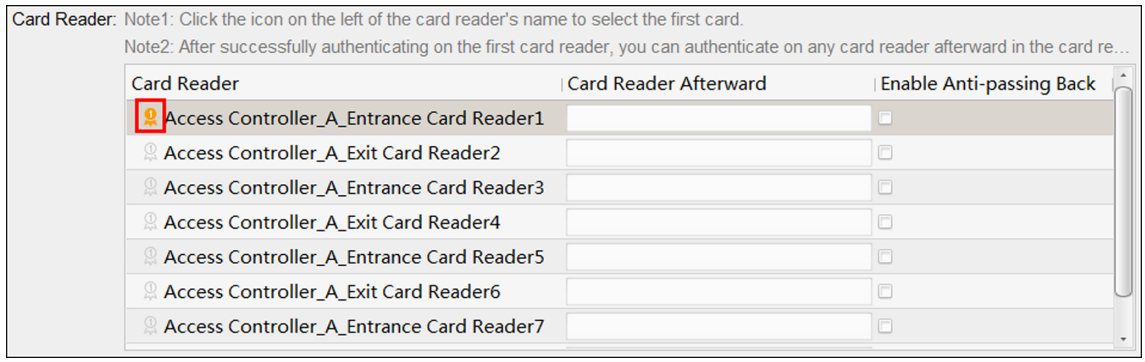


Figure 17-12 Select First Card

   The icon will turn to .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

Note

- Up to 16 card readers afterward can be added for each card reader.
- The displayed card readers in the card reader afterward input field should be in authentication order.

   3) Check the checkbox in the **Enable Anti-Passback** column to enable the Anti-Passback function.
8. Click **Save**.

Configure Route Anti-Passback Based on Network

The route anti-passback depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will authenticate the anti-passback according to the entrance and exit information stored on the card reader.

Perform this task if you need to configure route anti-passback and authentice the anti-passback result according to the entrance and exit information stored on the card reader.

Steps

1. Click **Access Control → Advanced Function → Cross-Controller Anti-Passback** to enter the cross-controller anti-passback configuration page.
2. Check **Enable Cross-Controller Anti-Passback** to enable the function.
3. Select **Based on Network** as the anti-passback mode.

4. Select **Route Anti-Passback** as the rule.
5. Select a server in the drop-down list for judging the anti-passback.

Note

- You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passback.

Note

Up to 64 devices with anti-passback function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

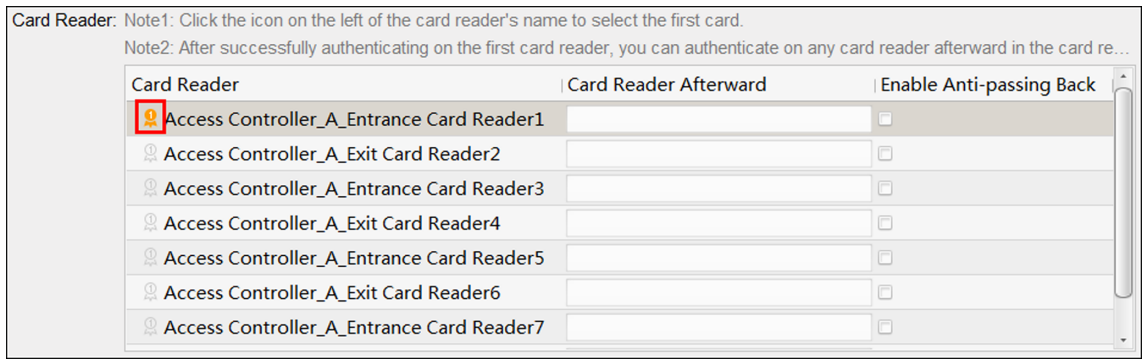


Figure 17-13 Select First Card

   The icon will turn to .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

Note

- Up to 16 card readers afterward can be added for each card reader.
- The displayed card readers in the card reader afterward input field should be in authentication order.

   3) Check the checkbox in the **Enable Anti-Passback** column to enable the anti-passback function.
8. Click **Save**.

Configure Area Anti-Passback Based on Card

You can set the entrance card reader and the exit card reader only for entering and exiting, without setting the first card reader and the card readers afterwards. It will judge the anti-passback according to the entrance and exit records on the card.

Perform this task if you need to configure area anti-passback and judge the anti-passback according to the entrance and exit records on the card.

Steps

Note

It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to ***Enable M1 Card Encryption*** .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-Passback** to enter the cross-controller anti-passback configuration page.
2. Check **Enable Cross-Controller Anti-Passback** to enable the function.
3. Select **Based on Card** as the anti-passback mode.
4. Select **Area Anti-Passback** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passback.

   Note

   Up to 64 devices with anti-passback function can be added.
7. In the Card Reader area, check the checkboxes in the **Enable Anti-Passback** column to select the entrance card reader and the exit card reader.

   Note

   Up to one entrance carder and one exit card reader should be checked.
8. Click **Save**.

Configure Area Anti-Passback Based on Network

You can set the entrance card reader and the exit card reader only for entering and exiting, without setting the first card reader and the card readers afterwards. It will authenticate the anti-passback according to the entrance and exit information on the card reader.

Perform this task if you need to configure area anti-passback and judge the anti-passback according to the entrance and exit information stored on the card reader.

Steps

1. Click **Access Control → Advanced Function → Cross-Controller Anti-Passback** to enter the cross-controller anti-passback configuration page.
2. Check **Enable Cross-Controller Anti-Passback** to enable the function.
3. Select **Based on Network** as the anti-passback mode.
4. Select **Area Anti-Passback** as the rule.
5. Select a server in the drop-down list for judging the anti-passback.

Note

- You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passback.

Note

Up to 64 devices with anti-passback function can be added.

7. In the Card Reader area, check the checkboxes in the **Enable Anti-Passback** column to select the entrance card reader and the exit card reader.

Note

Up to one entrance carder and one exit card reader should be checked.

8. Click **Save**.

17.5.11 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Before You Start

Add access control device to the client, and make sure the device supports the multi-door interlocking function.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback*** .

1. Click **Access Control → Advanced Function → Multi-door Interlocking** .
2. Select an access control device on the left panel.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) from the list.

Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click **OK** to add the selected access control point(s) for interlocking.

The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.

If the device supports configuration of an extended open duration (set during the addition or editing of a device), the multi-door interlocking list will include a column for Extended Open Duration.

6. **Optional:** Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Apply** to apply the settings to the access control device.

17.5.12 Configure Cross-Controller Multi-door Interlocking

Multi-door interlocking groups multiple doors into a linked set, where only one door in the group can be open at any given time — all others must remain closed. Cross-controller multi-door interlocking extends this capability beyond a single controller, enabling interlocking between access points across multiple independent door controllers. This is ideal for high-security environments with multiple entry points, such as bank vaults, data centers, and laboratories.

Add access control device to the client, and make sure the device supports the cross-controller multi-door interlocking function.

Note

- Cross-controller multi-door interlocking function is only supported by the access control device which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback*** .

1. Click **Access Control → Advanced Function → Cross-Controller Multi-door Interlocking** .
2. Select a device to act as the server, which will handle the interlocking logic.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) from the list.

   Note

   The number of doors can be added in one multi-door interlocking combination and the number of interlocking combinations depends on the capability of the server.

5. Click **OK** to add the selected access control point(s) for interlocking.

17.5.13 Configure Authentication Code

You can configure authentication code on the client. And after that, you can open door by entering authentication code when you forget to bring the card with you.

Before You Start
Add access control device to the client, and make sure the device supports authentication code as the authentication mode.

Steps
1. Click **Access Control → Advanced Function → Authentication Code** to enter the authentication code configuration page.
2. Select an access control device in the list of Controller List panel.
   All the applied cards and persons will display on the Card List panel.

   Note
   For setting and applying the permissions to the device, refer to ***Assign Access Levels to Persons in Access Groups*** .
3. Click the field of each card in the Authentication Code column to enter the authentication code.

   Note
   The authentication code should contain 4 to 8 digits.
4. Click **Save** at the upper-right corner of Authentication Code page to save the settings.
   The authentication code function of the card will be enabled automatically.
   Upon saving, the authentication code syncs to both the device and client, ensuring the client access to the authentication code even when the device is offline.

What to do next
You should set the card reader authentication mode of access control device as **Card/ Authentication Code**. Refer to ***Configure Card Reader Authentication Mode and Schedule*** for details.

17.6 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

17.6.1 Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

Before You Start
Add access control device to the client, and make sure the device supports multiple NICs.

Steps
1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .

3. Select an access control device in the device list and click **NIC** to enter Multiple NIC Settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

   MAC Address

   A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

   MTU

   The maximum transmission unit (MTU) of the network interface.
6. Click **Save**.

17.6.2 Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture and event triggered capture.

Note

- The capture function should be supported by the device.
- Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to ***Set Picture Storage*** .

Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to ***Set Picture Storage*** .

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Linked Capture**.
4. Set the picture size and quality.

5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

Before You Start
Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to ***Set File Saving Path*** .

Steps

Note
This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Manual Capture**.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as **High**, **Medium**, or **Low**. The higher the picture quality is, the larger size the picture will be.
6. Click **Save**.

17.6.3 Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note
This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Face Recognition Terminal**.
4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

17.6.4 Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

17.6.5 Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Before You Start
Add access control device to the client, and make sure the device supports RS-485 interface.

Steps
1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.

   Note

   When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - When you change the working mode or connection mode, the device will reboot automatically.

17.6.6 Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Before You Start
Add access control device to the client, and make sure the device supports Wiegand.

Steps
1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

Note

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

17.7 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

17.7.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is via the client by configuring client actions for the access event. Client actions here refer to the actions automatically executed by the client itself, such as making an audible warning and sending an email. Once an event is triggered, the client will notify the security personnel, so that he/she can handle the event in time.

Before You Start

Add access control device to the client.

Steps

1. Click **Event Configuration → Access Event** .

   The added access control devices will display in the device list.
2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

   The event types which the selected resource supports appear.
3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
   1) Select the event(s) and click **Edit Linkage** to set the client actions when the event(s) are triggered.

      Audible Warning

The client software gives an audible warning when the event is triggered. You can select alarm sound for the audible warning.

Note

For details about setting the alarm sound, refer to ***Set Alarm Sound*** .

Send Email

Send an email notification about the event to one or more receivers.

For details about setting email parameters, refer to ***Set Email Parameters*** .

Pop-up Window

Pop-up a window to display the event information (including event details, the event-related video footage, the event-related picture) on the software client when the event is triggered.

Display on Map

When the event source is added as a hot spot on the map, the hot spot will be displayed with red number (indicates the number of events, and the maximum number is 10) aside when the event is triggered, which helps the security personnel to view the location of the event.

You can also click the hot spot to view the event details and the live video of the linked camera.

Linked Camera

Link the selected camera to capture a picture when the access event is triggered.

Select the camera in the drop-down list.

Broadcast Linkage

Link the selected camera to broadcast certain audio file(s) when the event is triggered.

Note

Up to 100 speaker units, and up to 5 audio files can be selected.

PTZ Linkage

When the events are triggered, the cameras' **Preset**, **Patrol**, and **Pattern** will be called.

Note

Make sure you have configured presets, patrols, or patterns for the camera.

Alarm Output Linkage

The activation of an event will cause the connected alarm outputs (Max: 8) to activate, generating sounds, flashes, etc.

Access Point Linkage

When events are triggered, actions including Unlock Door, Lock Door, Remain Open, or Remain Closed are performed at the linked access points.

2) Click **OK**.

5. Enable the event so that when the event is detected, event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to** to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

17.7.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. After that, when an event is triggered, it can trigger the alarm output, buzzer on access controller, and other actions.

Steps

Note

The linkage actions should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Event Linkage** as the event source.
5. Select the event type and detailed event to set the linkage.

   Supports selecting all alarm inputs, doors, or card readers corresponding to the chosen event type.
6. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Capture

   An event-related picture will be captured when the selected event happens.

   Recording

   An event-related recording will be captured when the selected event happens.

   Note

   The device should support recording.

   Call Center

   Initiates a call to the management center when the selected event occurs.

   Note

   The feature is available when choosing the alarm input event.

   Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification when the selected event happens

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain close will be triggered.

Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the followings:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

17.7.3 Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card, In this way, you can monitor the card holder's behaviors and whereabouts.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Card Linkage** as the event source.
5. Enter the card number or select the card from the drop-down list.
6. Select the card reader where the card swipes.

7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

17.7.4 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, buzzer on card reader, and other actions, so as to implement special monitoring on the specified person.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Person Linkage** as the event source.
5. Enter the employee number or select the person from the drop-down list.
6. Select the card reader where the card swipes.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support zone function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.
9. **Optional:** After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

17.8 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to ***Add User*** .

17.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Assign Access Levels to Persons in Access Groups*** .
- Make sure the operation user has the permission of the access points (doors). For details, refer to ***Add User*** .

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.

Note

For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

4. Click the following buttons to control the door.

Unlock Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Lock Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Unlocked

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Locked

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Controlled

The door will transition from the status of remain unlocked/remain locked to a state where access is routinely controlled based on permissions.

Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to ***Set File Saving Path*** .

Remotely Unlocking Door Station

When the group includes door stations, you can check **Lock1** or **Lock2**, then click **Unlock Door** to unlock the door station.

Note

By default, **Lock1** is checked for door stations.

Refresh Status

Click **Refresh Status** to get the door's newest status.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

17.8.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (floors). For details, refer to ***Person Management*** and ***Assign Access Levels to Persons in Access Groups*** .
- Make sure the operation user has the permission of the access points (floors). For details, refer to ***Add User*** .

Steps

Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control the elevator at one time.
- The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The elevators in the selected access point group will display.
3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

   Open Door

   When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

   Controlled

   You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

   Free

The selected floor's button in the elevator will be valid all the time.

Disabled

The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

17.8.3 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to ***Person Management*** and ***Add Device*** .

Steps

1. Click **Monitoring** to enter the Monitoring module.

   Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc. For access events via card, supports displaying person name and organization.

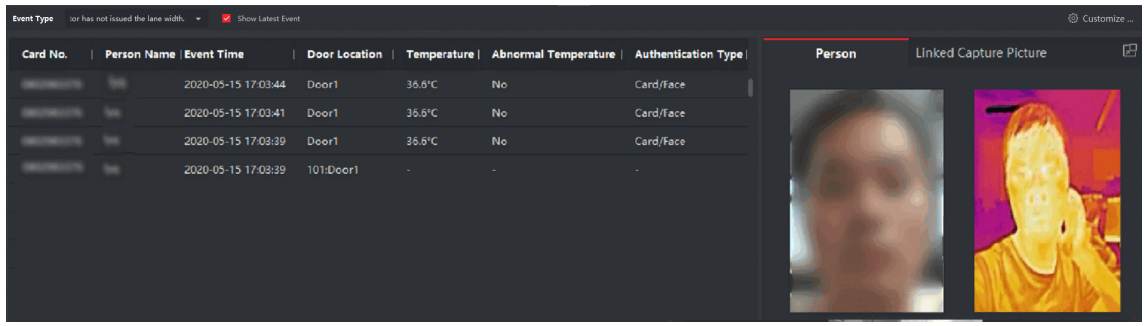


Figure 17-14 Real-time Access Records

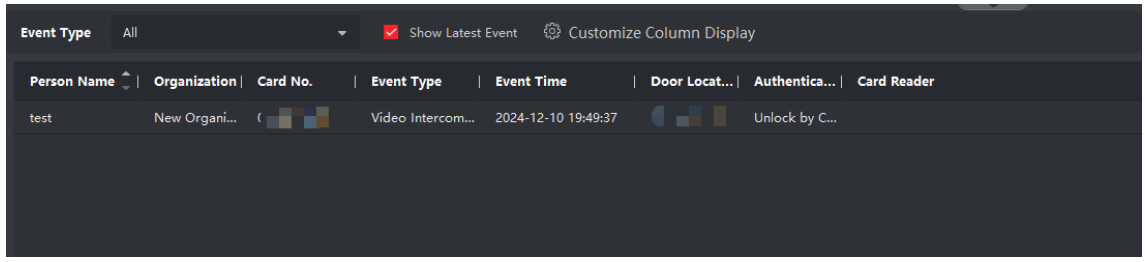


Figure 17-15 Access Events via Card

Note

You can right click the column name of access event table to show or hide the column according to actual needs.

2. Filter events.
   1) In the upper-right corner, select an access point group from the drop-down list to show the real time access records of the selected group.
   2) Check the event type.
   3) **Optional:** Check **Show Latest Event** to view the latest access record.
3. **Optional:** View event records and perform more operations.

Enable Abnormal Temperature Prompt	Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt. When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.
View Pictures	Click an event to view person pictures (including captured picture and profile). In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.
View Event Details	Click to view monitoring details (including person's detailed information and the captured picture). In the pop-up window, you can click to view monitoring details in full screen.
Customize Column Display	Click **Customize Column Display** to customize the columns to be displayed.

17.9 Distributed Controller Management

Distributed Controller Management is used to register the sub-controllers (distributed controllers) connected to the access controller, enabling the controller to identify and manage the distributed controllers.

Note

Make sure you have added access controller(s).

1. Go to **Access Control → Distributed Controller Management** .
2. Select an access controller from the left list, then click **Add** or **Search Not Added Device**.

   Search for Unadded Devices

   The distributed controller is physically connected to the access controller correctly but has not yet been registered to the access controller.

   a. After the device is found, click  in the operation column.
   b. Select the working mode.
      After selecting the configuration mode: You can choose to enable the Offline feature, which allows the distributed controller to use its own permissions to open doors when offline, without access controller verification. If not enabled, the distributed controller must remain online and pass access controller verification.

   Add

   No distributed controller connection or online status is required.

   Enter the device name and DIP switch address. Ensure the DIP switch address matches the DIP switches on the device back panel.
3. Click **Save**. The distributed controller resources will be imported under the access controller's group.

Chapter 18 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

18.1 Flow Chart

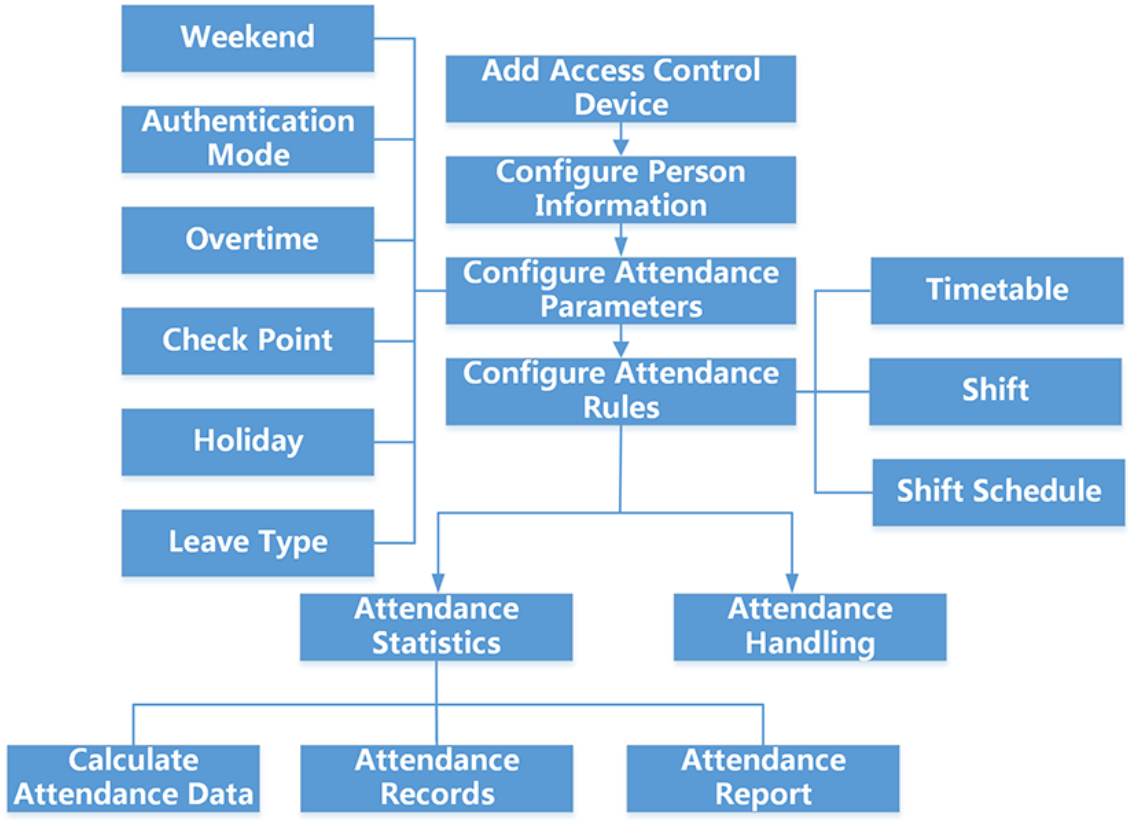


Figure 18-1 Flow Chart of Time and Attendance

- **Add Access Control Device:** You can add access control devices on the client. For more details, refer to ***Add Device*** .
- **Configure Person Information:** You should add person information to the client before configuring time and attendance parameters for them. For more details, refer to ***Person Management*** .

- **Set Weekend:** You can select one or more days as the weekends according to actual requirements on the client. For more details, refer to ***Set Weekend*** .
- **Configure Authentication Mode:** You can configure authentication mode such as card, fingerprint, face, etc. For more details, refer to ***Configure Authentication Mode*** .
- **Configure Overtime Parameters:** You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, etc. For more details, refer to ***Configure Overtime Parameters*** .
- **Configure Attendance Check Point:** You can set the card reader(s) of the access point as the attendance check point on the client. For more details, refer to ***Configure Overtime Parameters*** .
- **Configure Holiday:** You can add the holiday during which the check-in or check-out will not be recorded on the client. For more details, refer to ***Configure Holiday*** .
- **Configure Leave Type:** You can customize the leave type according to actual needs. For more details, refer to ***Configure Leave Type*** .
- **Add Timetable:** You can add general timetable and flexible timetable for employees on the client according to actual needs. For more details, refer to ***Add Flexible Timetable*** and ***Add General Timetable*** .
- **Add Shift:** You can add shift for employees including setting shift periods and the effective attendance time. For more details, refer to ***Add Shift*** .
- **Manage Shift Schedule:** You can set department schedule, person schedule, and temporary schedule on the client. For more details, refer to ***Manage Shift Schedule*** .
- **Calculate Attendance Data:** The client can calculate the attendance data automatically or you can manually calculate the attendance data. For more details, refer to ***Calculate Attendance Data*** .
- **Attendance Records:** You can search and view the employee's attendance records on the client, including attendance time, attendance status, check point, etc. For more details, refer to ***Get an Overview of Employees' Attendance Data*** .
- **Attendance Report:** The client supports generating attendance reports to view the employees' attendance results. Also, you can pre-define the report content and it can send the report automatically to you via email. For more details, refer to ***Generate Instant Report*** and ***Send Report Regularly*** .

18.2 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

18.2.1 Set Weekend

The days of weekends may vary in different countries and regions. The client provides weekends definition function. You can select one or more days as the weekends according to actual requirements, and set different attendance rules for weekends from workdays.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. Select the day(s) as weekend, such as Saturday and Sunday.
4. Click **Save**.

18.2.2 Configure Authentication Mode

The client supports configuring authentication modes, including card, fingerprint, face, card or fingerprint, etc. After setting authentication mode, you can get device events of the configured authentication mode via the client and the client will calculate attendance data of the configured authentication mode.

Click **Attendance Settings → General Rule** .

On the Authentication Mode area, select the authentication mode from the drop-down list.

Note

- This selected authentication mode should be supported by device.
- After setting authentication mode, you can only get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

18.2.3 Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Click **Time & Attendance → Attendance Settings → Overtime** .
2. Set required information.

Overtime Level for Workday

When you work for a certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3. You can set different work hour rate for three overtime levels, respectively.

Work Hour Rate

Work Hour Rate is used to calculate work hours by multiplying it by overtime. When you work for a certain period after end-work time on workday, you will reach different overtime level. You can set different work hour rates (1-10, can be a decimal) for three overtime levels. For

example, your valid overtime is one hour (in overtime level 1), and the work hour rate of overtime level 1 is set as 2, then the work hours in the period will be calculated as 2 hours.

Overtime Rule for Weekend

You can enable overtime rule for weekend and set calculation mode.

3. Click **Save**.

18.2.4 Configure Attendance Check Point

You can set the card reader(s) of the access control device as the attendance check point(s), so that the authentication on the card readers will be recorded for attendance.

Before You Start

- You have added access control device(s). For details, refer to ***Add Device*** .
- You have enabled T&A Status. For details, refer to ***Add General Timetable*** .

By default, all card readers of the added access control devices are set as start/end-work check points. If you need to edit check point function of card reader(s), you can perform the following operations.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Attendance Check Point** to enter the attendance check point settings page.
3. Set **Set All Card Readers as Check Points** switch to off.
4. Check the desired card reader(s) as attendance check point(s) in the list below.
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.

Note

When selecting **Start-Work** or **End-Work**, the attendance status uploaded from the device will be decided by the check point function you set here.

Start-Work

Attendance status uploaded from the device will all be calculated as Check-in.

End-Work

Attendance status uploaded from the device will all be calculated as Check-out.

Start/End-Work

Attendance status will be calculated as Check in/out according to the actual attendance status on the device.

6. Click **Set as Check Point**.

The configured attendance check point(s) are displayed on the right list.

7. **Optional:** After setting attendance check points, and perform the following operations.

Edit Check Point	Check one attendance check point, click **Edit** to edit its information including name, check point function, etc. Check two or more attendance check points, click **Edit** to batch edit check point function, enter remark, etc.
Delete Check Point	Check one or more check points, and click **Delete** to delete it/them.

18.2.5 Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

   The added holiday will display in the holiday list and calendar.

   If the date is selected as different holidays, it will be recorded as the first-added holiday.
10. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday	Click to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.

2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

   Example

   If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.
7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year
10. Click **OK**.

    The added holiday will display in the holiday list and calendar.

    If the date is selected as different holidays, it will be recorded as the first-added holiday.
11. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday	Click to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

18.2.6 Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.

Edit	Move the cursor over the major leave type and click to edit the major leave type.
Delete	Select one major leave type and click **Delete** on the left to delete the major leave type.

5. Click **Add** on the right to add a minor leave type.
6. **Optional:** Perform one of the following operations for minor leave type.

Edit	Move the cursor over the minor leave type and click to edit the minor leave type.
Delete	Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

18.2.7 Synchronize Authentication Record to Third-Party Database

The attendance data recorded on the client can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from the client to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Third-Party Database** .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Select database Type as **SQLServer** or **MySQL**.

   Note

   - Supported versions：SQLServer 2008, MySQL V5.7.26.
   - You should set the field type of the database type as varchar.
   - If you select **MySQL**, you should import the configuration file (libmysql.dll) from local PC.

5. Set the other required parameters of the third-party database, including server IP address, port No., database name, user name and password.

   Note

   The default port No. of the selected database type is displayed automatically. You can enter a number ranging from 1 to 65535 to customize the port No if needed.

6. Set table parameters of database according to the actual configuration.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the client and the third-party database.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
   - The attendance data will be written to the third-party database.
   - During synchronization, if the client disconnects with the third-party database, the client will start reconnection every 30 mins. After being reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

18.2.8 Configure Attendance Calculation Accuracy

To calculate the attendance data accurately, you can set the attendance calculation accuracy for different attendance items, including the minimum unit for attendance calculation and round-off control rule. For example, you can set the minimum unit as 1 hour for leave duration, and set the round-off control rule as round up.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Settings → General Rule** .

3. In the Advanced Function area, set the minimum units (including min, Hour(s) and Workday) for different statistic items.
4. Set the round-off control rules (including Round Down, Round Off and Round Up) for different statistic items.
5. Set the **Display Format** as **MM** or **HH:MM**.
6. Click **Save**.

Example
Set the minimum unit as 1 hour and the round-off control rule as round down for overtime duration, and if the overtime duration is less than 1 hour, it will be calculated as 0. If the overtime duration is 1.5 hour, it will be calculated as 1 hour.

18.2.9 Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps
1. Click **Time & Attendance → Timetable → Break Time** .
   The added break time is displayed in the list.
2. Click **Break Time Settings** to enter Break Time Settings window.
3. Click **Add**.
4. Enter a name for the break time.
5. Set related parameters for the break time.

   Start Time / End Time

   Set the time when the break starts and ends.

   No Earlier Than / No Later Than

   Set the earliest swiping time for starting break and the latest swiping time for ending break.

   Break Duration

   The duration from start time to end time of the break.

   Calculation

   Auto Deduct

   The break duration will be calculated according to the time you set.

   Must Check

   The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

   Return from Break Early for

   The actual check-in and check-out time does not exceed the break time, and can be marked as normal work or work overtime.

Return from Break Late for

The actual check-in and check-out time exceeds the break time, and can be marked as late, absent or early leave.

Calculated by

Each Check in/out: Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the break time duration.

First In & Last Out: The first check-in time is recorded as start break time and the last check-out time is recorded as the end break time.

Enable T&A Status

Set **Enable T&A Status** switch to on to calculate the actual break time according to attendance status on the device.

Note

This function should be supported by the device.

Valid Authentication Interval

During the valid authentication interval, person swiping card for several times will only be calculated as once when calculating attendance data.

6. Click **Save** to save the settings.
7. **Optional:** Click **Add** to continue adding break time.

18.3 Add Flexible Timetable

On the timetable page, you can add flexible timetable for employees, which does not requires the check-in/out time but requires the staffs' working time (from the start time you set) is equal or greater than the predefined work hours.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter add timetable page.
3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar.

4. Select the timetable type as flexible.

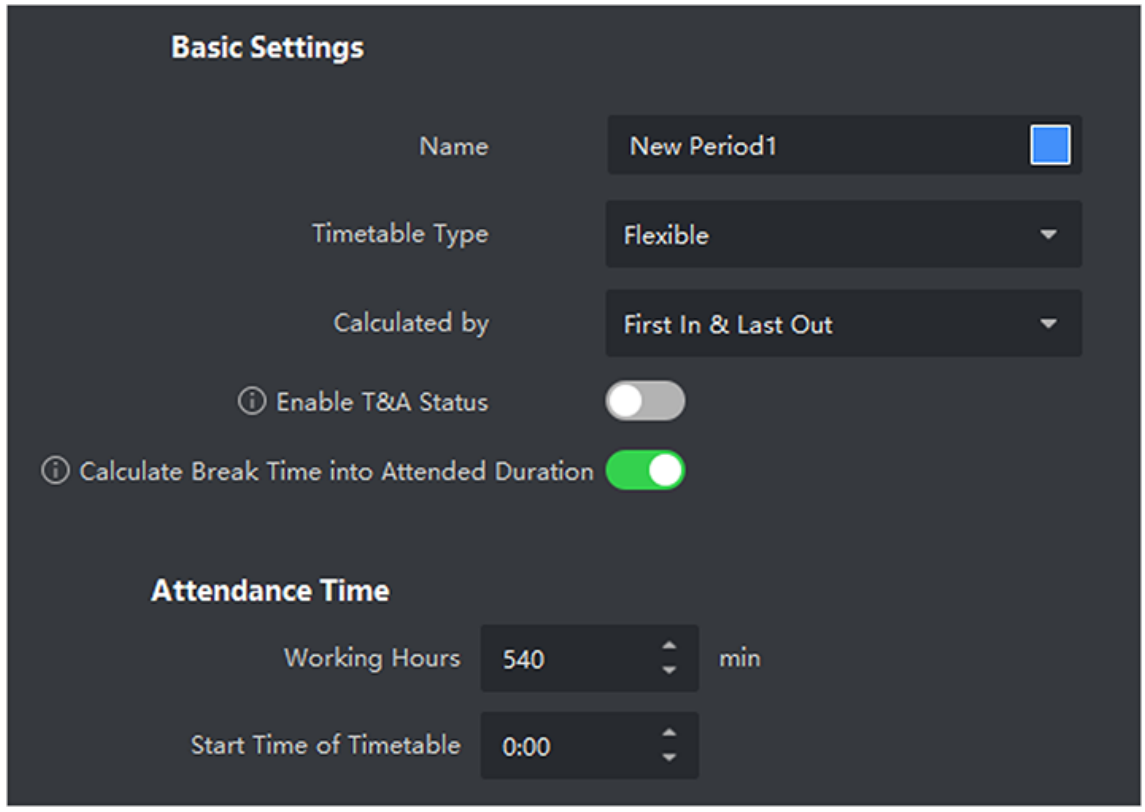


Figure 18-2 Add Flexible Timetable

5. Select calculation method.

   First In & Last Out

   The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

   Each Check-In/Out

   Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

   You need to set **Valid Authentication Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Enable **Enable T&A Status** to calculate according to attendance status of the device.

   Note

   This function should be supported by the device.

7. **Optional:** Enable **Calculate Break Time into Attended Duration**.

Note

When enabled, break time will be calculated into the overall attendance duration. That is, the actual attendance duration equals to the overall attendance duration (includes break time).

8. Set the related attendance time parameters as the following:

Working Hours

The employees' working hours should be equal or greater than the set value.

Start Time of Timetable

Calculate the working hours of each day from the set value.

For example, if you have set the working hours as 8 hours, and the start time of timetable as 9:00 am, and the staff A checked-in at 8:00 am and checked-out at 5:00 pm (effective working hours are 9:00 am to 5:00 pm, totally 8 hours), the attendance result for staff A will be calculated as normal.

9. Click **Save** to add the timetable.
10. **Optional:** Perform one or more following operations after adding timetable.

Edit Timetable	Select a timetable from the list to edit related information.
Delete Timetable	Select a timetable from the list and click **Delete** to delete it.

18.4 Add General Timetable

On the timetable page, you can add general timetable for employees, which requires the fixed start-work time and end-work time. Also, you can set valid check-in/out time, allowable timetable for being late and leaving early.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter add timetable page.

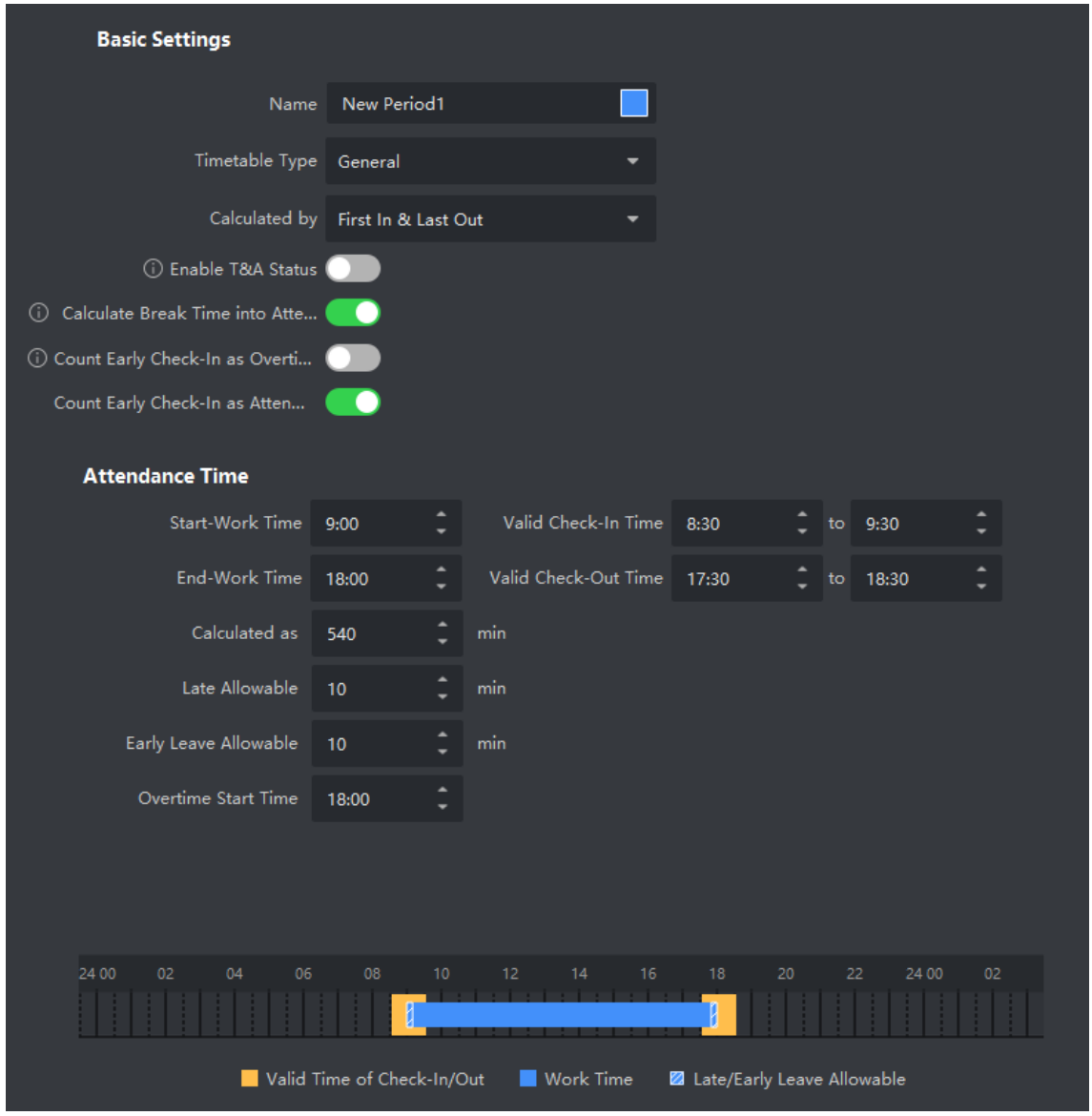


Figure 18-3 Add Timetable

3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar in the Configuration Result area.

4. Select the timetable type as general.
5. Select calculation method.

First In & Last Out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Authentication Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Set **Enable T&A Status** switch to on to calculate according to attendance status of the device.

Note

This function should be supported by the device.

7. **Optional:** Enable **Calculate Break Time into Attended Duration**.

Note

When enabled, break time will be calculated into the overall attendance duration. That is, the actual attendance duration equals to the overall attendance duration (includes break time).

8. **Optional:** Enable **Count Early Check-In as Overtime**, then the period between your early check-in and the official start-work time will be calculated as overtime.
9. **Count Early Check-In as Attendance**: The time of early check-in will be counted as the official start-work time.
10. Set the related attendance time parameters as the following:

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

11. Set absence related parameters.

Check-In, Late for

You can set the late time duration for the employee who has checked in but is late for work. If the employee exceeds the required time period, his/her attendance data will be marked as absent.

Check-Out, Early Leave for

You can set the early leave time duration for the employee who checks out earlier than the normal leave time, and his/her attendance data will be marked as absent.

No Check-in

If the employee does not check in, his/her attendance data may be marked as absent or late.

No Check-Out

If the employee does not check out, his/her attendance data may be marked as absent or early leave.

12. Click **Save** to add the timetable.
13. **Optional:** Perform one or more following operations after adding timetable.

Edit Timetable	Select a timetable from the list to edit related information.
Delete Timetable	Select a timetable from the list and click **Delete** to delete it.

18.5 Add Shift

You can add shift for employees including setting shift period (day, week, month) and the effective attendance time. According to the actual requirements, you can adding multiple timetables in one shift for employees, which requires them to check in and check out for each timetable.

Before You Start

Add a timetable first. See ***Add General Timetable*** for details.

Steps

1. Click **Time & Attendance → Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.

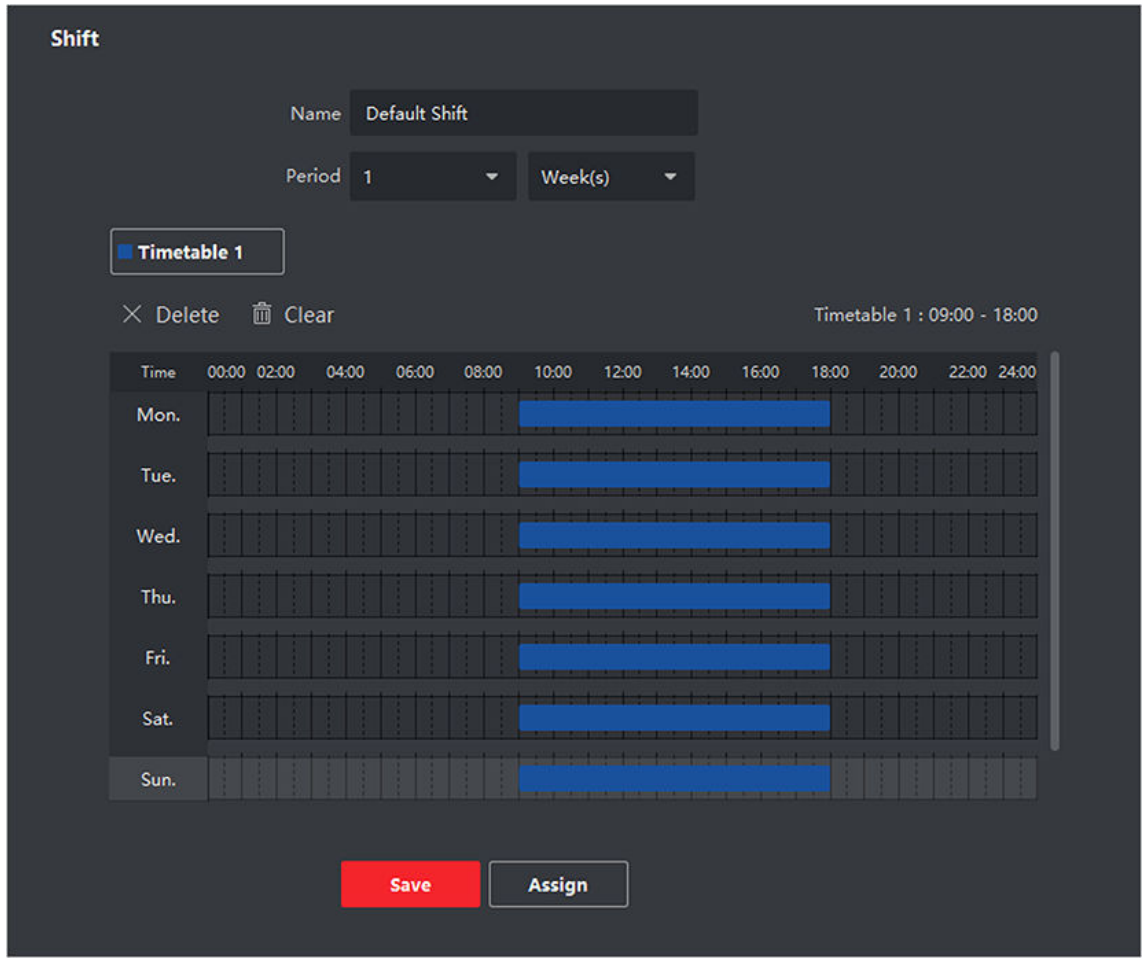


Figure 18-4 Add Shift

Note

You can select more than one timetables. The start and end work time and the valid check-in and out time in different time tables can not be overlapped.

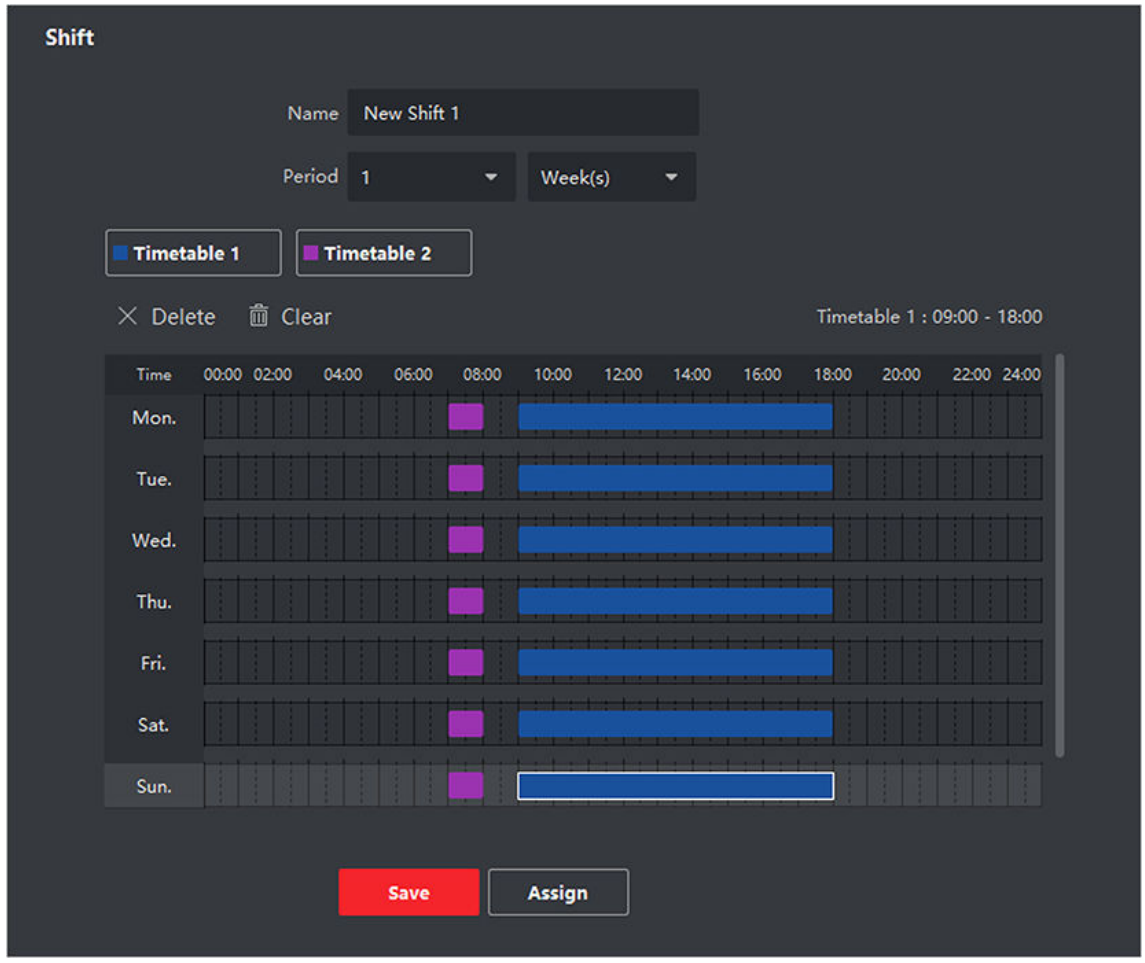


Figure 18-5 Add Multiple Timetables

6. Click **Save**.

   The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. **Optional:** Assign the shift to organization or person for a quick shift schedule.

   1) Click **Assign**.

   2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.

      The selected organizations or persons will list on the right page.

   3) Set the Expire Date for the shift schedule.

   4) Set other parameters for the schedule.

      Check-in Not Required

      Persons in this schedule do not need to check-in when they come to work.

      Check-out Not Required

      Persons in this schedule do not need to check-out when they end work.

      Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

5) Click **Save** to save the quick shift schedule.

18.6 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

18.6.1 Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See ***Person Management*** for details.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.

Note

If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

   Check-in Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Scheduled on Holidays

   On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.

   Flexible Shift Schedule on Weekend

   The person's attendance on the weekend will be recorded as overtime.
8. Click **Save**.

18.6.2 Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start
Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule page.
2. Click **Person Schedule** to enter Person Schedule page.
3. Select the organization and select the person(s).
4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

Flexible Shift Schedule on Weekend

The person's attendance on the weekend will be recorded as overtime.

8. Click **Save**.

18.6.3 Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start
Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).

4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

   If **Non-Workday** is selected, you need to set the following parameters.

   Calculated as

   Select normal or overtime level to mark the attendance status for temporary schedule.

   Timetable

   Select a timetable from drop-down list.

   Multiple Shift Schedule

   It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

   Rule

   Set other rule for the schedule, such as **Check-in Not Required**, and**Check-out Not Required**.
6. Click **Save**.

18.6.4 Check Shift Schedule

You can check the shift schedule in calendar or list mode. You ca also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click  or  to view the shift schedule in calendar or list mode.

   Calendar

   In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

   List

   In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

18.7 Attendance Handling

If your attendance status appears abnormal due to reasons such as forgetting to check in/out, having business trips, or taking leave, you can rectify your attendance records by manually correcting check in/out record and add leave or business trips.

18.7.1 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, and export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Person module. For details, refer to ***Person Management*** .
- The person's attendance status is incorrect.

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-in/out** to enter adding check-in/out correction page.
3. Select one or more persons from left list for correction.
4. Select the correction date.
5. Select the correction type as **Check-in**, **Check-out**, **Break-in**, **Break-out**, etc,. and set the correct time.

   Note

   You can click ⊕ to add multiple correction items. At most 8 check-in/out items can be added.
6. **Optional:** Enter the remark information as desired.
7. Click **Save** to save the above settings.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

   View Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.

   Edit
   - In calendar mode, click ✎ → **Edit** to edit the details.
   - In list mode, double-click the related field in Date, Handling Type, Time, or Remark column to edit the details.

     Note

     The edited check-in/out correction will take affect.

   Delete
   - In calendar mode, select one check-in/out correction, and click **Delete** to delete the selected item.
   - In list mode, check one or more check-in/out corrections, and click **Delete** to delete the selected items.

Note

The deleted check-in/out correction will no longer take affect.

Export In list mode, check one or more check-in/out corrections to export the attendance handling details (CSV file) to local PC.

18.7.2 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to ***Person Management*** .

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.
5. Select the major leave type and minor leave type from the drop-down list.

   Note

   You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type*** .
6. Set the time for leave.

   Click **Add** to set a second leave period for the selected date.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

   View Click or to view the added attendance handling information in calendar or list mode.

   Note

   In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

   Edit
   - In calendar mode, click the related label on date to edit the details.
   - In list mode, double-click the filed in Date, Handling Type, Time, or Remark column to edit the related information.

   Delete Delete the selected items.

   Export Export the attendance handling details to local PC.

Note

The exported details are saved in CSV format.

18.8 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

18.8.1 Automatically Calculate Attendance Data

You can set a schedule so that the client can automatically calculate attendance data of the previous day at the time you configured every day.

Steps

Note

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data.
4. Click **Save**.

   The client will calculate the attendance data of the previous day from the time you have configured.

18.8.2 Manually Calculate Attendance Data

You can manually calculate attendance data by setting conditions including attendance time, department, attendance status, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Calculation** .
3. Set the start time and end time to define the attendance data range.
4. Select the department from the drop-down list.
5. **Optional:** Set other conditions, including name and person ID.
6. Check attendance status (supports multi-selection).
7. Click **Calculate**.

Note

Only the attendance data within three months can be calculated.

8. **Optional:** Perform one of the following operations.

Correct Check-in/out	Select one person, click **Correct Check-in/out** to add check-in/out correction.
Select Items to Display	Click on the upper right corner, or right click the table header of the attendance data list to customize the items to be displayed in the list.
Adjust Items Sequence	Click one item (except Person ID) and move the mouse to customize the sequence of different items.
Generate Report	Click **Report** to generate the attendance report. **Note** The report items will be displayed in the sequence you have set.
Export Report	Click **Export** to export attendance data (CSV file) to local PC. **Note** The report items will be displayed in the sequence you have set.

18.9 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

18.9.1 Get an Overview of Employees' Attendance Data

You can search and view the employee's attendance data uploaded from devices by the client, including attendance time, attendance status, check point, etc.

Before You Start

- You should add organizations and persons in Person module and the persons have swiped cards. For details, refer to ***Person Management*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am, or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Attendance Record** .
3. Set the attendance start time and end time that you want to search.
4. Set other search conditions, including department, name, and person ID.
5. Select data source as **All**, **Original Records on Device** or **Manually Handled Records**.

Note

After selecting **Original Records on Device**, you can specify the **Attendance Check Point**.

6. **Optional:** Click **Get Events from Device** to get the attendance data from the device.

Note

There are three methods for getting attendance events from the device, including **Online**, **Encrypted File**, and **Unencrypted File**. For more details about operations, refer to ***Get Events from Device*** .

7. **Optional:** Click **Reset** to reset all the search conditions and edit the search conditions again.
8. Click **Search**.
9. **Optional:** For the displayed search results, perform one of the following operations.

Edit Attendance Status	Select one incorrect record, double click the field of **Attendance Status** column and select from the drop-down list to edit single piece of attendance status. Check two or more incorrect records, click **Edit Attendance Status** on the upper left corner and select from the drop-down list to batch edit multiple pieces of attendance status.
Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** and select saving path to export the attendance report (CVS file) to the local PC.
Custom Export	Click **Custom Report** and set conditions to export attendance records according to actual needs. For details, refer to ***Custom Export Attendance Records*** .
Custom Columns	On the upper right of the report, click and select columns displayed in the report.

18.9.2 Custom Export Attendance Records

After viewing the employee's attendance data, you can export the attendance records according to actual needs.

Before exporting the necessary attendance records, you should search and get employee's attendance data. For details, refer to ***Get an Overview of Employees' Attendance Data*** .

Click **Custom Export** to set the related information.

Start/End Time

You can set the start and end time of exporting attendance records.

Saving Path

You can select the file path for saving attendance records.

File Name

The file will be named according to the actual exporting date. You can select format of the date such as **dd-MM-yyyy** and **dd-MM-yy**.

Format

You can export the original attendance records in .TXT and .CVS formats.

Separator

You can select to have/not have separators (including comma, space, tab) for separating different items in the exported file.

Export

You can select the items you need to export including ID, person name, department, date, etc.

Default Value

When there is no information for the item you have selected to export, you can set a default value to replace the blank space.

18.9.3 Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics → Report Display** .
3. Set the display settings for attendance report.

   Company Name

   Enter a company name to display the name in the report.

   Attendance Status Mark

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click **Save**.

18.9.4 Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start
Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

18.9.5 Send Report Regularly

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Regularly Send Report** .
3. Click **Add** to enter the add custom report page.
4. Set the report content.

Report Name

Report names can only contain numbers and letters.

Report Time

The time to be selected may vary for different report type.

Person

Select the added person(s) whose attendance records will be generated for the report.

Note

You can view the selected person(s) in the right side of the Person area.

5. Set the schedule to send the report to the email address(es) automatically.

Note

The **Auto-Send Email** function is enabled by default.

1) Set the Effective Period during which the client will send the report on the selected sending date(s).
2) Select the sending frequency as Every Month, Every Week, or Everyday.
3) Select the Sending Date(s) on which the client will send the report.
4) Set the Sending Time at which the client will send the report.

Example

If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

Note

Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

5) Enter the receiver email address(es).

Note

Up to 5 email addresses can be added. You can click **+** to add a new email address and click **Email Settings** to navigate to the email settings page.

6) **Optional:** Click **Live View** to view the email details.
7) **Optional:** Click **Email Test** to verify that email settings are configured correctly.

6. Click **OK**.

7. **Optional:** After adding the custom report, you can do one or more of the followings:

Edit Report	Select one added report and click **Edit** to edit its settings.
Delete Report	Select one added report and click **Delete** to delete it.
Generate Report	Select one added report and click **Report** to generate the report instantly and you can view the report details.

Chapter 19 Video Intercom

Video intercom is an audiovisual communication system used within a building or a small collection of buildings. With microphones and video camera devices at both sides, it enables the inter-communication via video and audio signals. A video intercom system can provide a safe and easy monitoring solution for apartment buildings and private houses.

Be sure to add video intercom devices to the client and link the indoor stations to the persons beforehand. You should also set the access authorization for the persons to open doors via the linked indoor stations.

Note

- For details about adding persons, refer to ***Add Persons*** .
- For details about setting person's access authorization, refer to ***Assign Access Levels to Persons in Access Groups*** .

19.1 Flow Chart

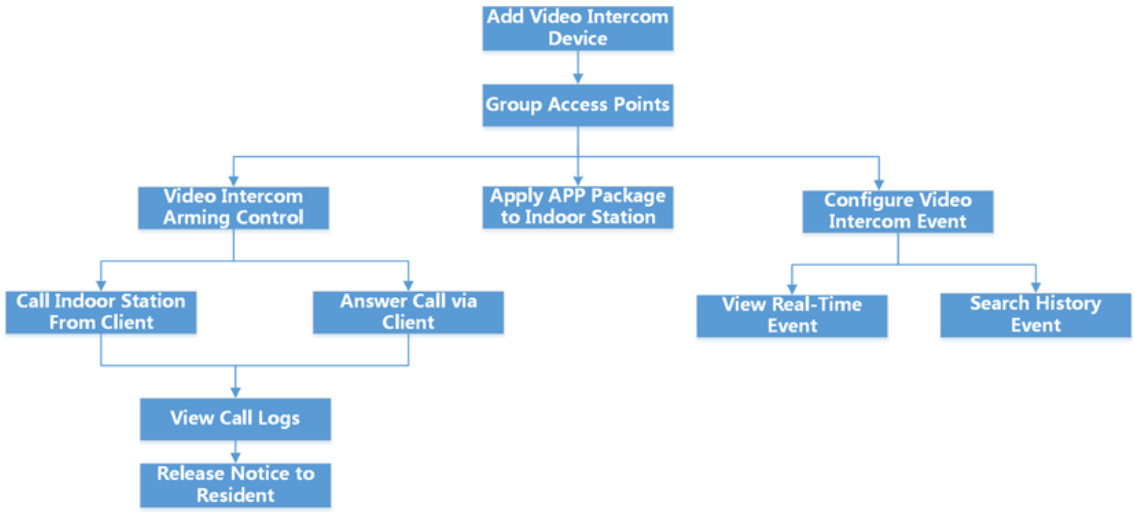


Figure 19-1 Flow Chart of Video Intercom

- **Add Video Intercom Device:** You can add video intercom devices on the client. For more details, refer to ***Add Device*** .
- **Group Access Points:** You can group the added access points into groups for convenient management. For more details, refer to ***Group Management*** .

- **Video Intercom Arming Control:** You can enable or disable the calling between the added video intercom devices and the client. For more details, refer to ***Enable Calling between Video Intercom Device and Client*** .
- **Apply APP Package to Indoor Station:** You can apply the application package saved in local PC to one or multiple indoor stations remotely via the client. For more details, refer to ***Apply Application Package to Indoor Station*** .
- **Call Indoor Station From Client:** You can call the added indoor station by the client to perform video intercom. For more details, refer to ***Call Indoor Station from Client*** .
- **Answer Call via Client:** You can answer call from the added indoor station, door station, etc. via the client to perform video intercom. For more details, refer to ***Answer Call via Client*** .
- **View Call Logs:** You can view details of all the calls. For more details, refer to ***View Real-Time Call Logs*** .
- **Release Notice to Resident:** You can send a notice to the residents by one-touch on the client. For more details, refer to ***Release a Notice to Resident*** .
- **Configure Video Intercom Event:** By configuring linked actions of video intercom event on the client, you will be notified once the event is triggered. For more details, refer to ***Configure Client Actions for Access Event*** .
- **Search Real-Time/History Event:** You can view the real-time events, search the historical events on the client. For more details, refer to ***Event Center*** .

19.2 Manage Calls between Client Software and an Indoor/Door Station/ Access Control Device

You can call the residents by the client, and vice versa. You can also use an indoor station/door station or specified access control device to call the client.

Before making calls, you can set the parameters such as ring duration and speaking duration. For details, refer to ***Set Access Control and Video Intercom Parameters*** .

19.2.1 Call Indoor Station from Client

You can call the added indoor station by the client to perform video intercom.

Before You Start

- Be sure to have added a resident to the client. For details, refer to ***Add Persons*** .
- Be sure to have linked the resident with an indoor station and configured the resident information (including floor No. and room No.) in Person module. For details about configuring the linkage and resident information, refer to ***Configure Resident Information*** .

Steps

Note

- A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.
- You can remotely configure the Max. Ring Duration and the Max. Speaking Duration.

1. Click **Access Control → Video Intercom → Contacts** .
2. Unfold the organization list on the left panel and select an organization.

   The information (including resident name, device name, floor No. and room No.) of all the residents in the selected group will be displayed on the right panel.
3. Select a resident, or enter a keyword in the Filter field to find the desired resident.
4. Click to start calling the selected resident.

   After the call is answered, you will enter the In Call window.
5. **Optional:** After the call is answered, perform the following operation(s).

Adjust Loudspeaker Volume	Click to adjust the volume of the loudspeaker.
End Speaking	Click **Hang Up** to end speaking.
Adjust Microphone Volume	Click to adjust the volume of the microphone.

19.2.2 Answer Call via Client

You can answer call from the added indoor station, door station, or specific access control device via the client and perform video intercom.

Steps

Note

A video intercom device can be added to more than one client, but perform video intercom with only one client at a time.

1. Call the client by an indoor station, door station, or specific access control device.

   An incoming call dialog will pop up.

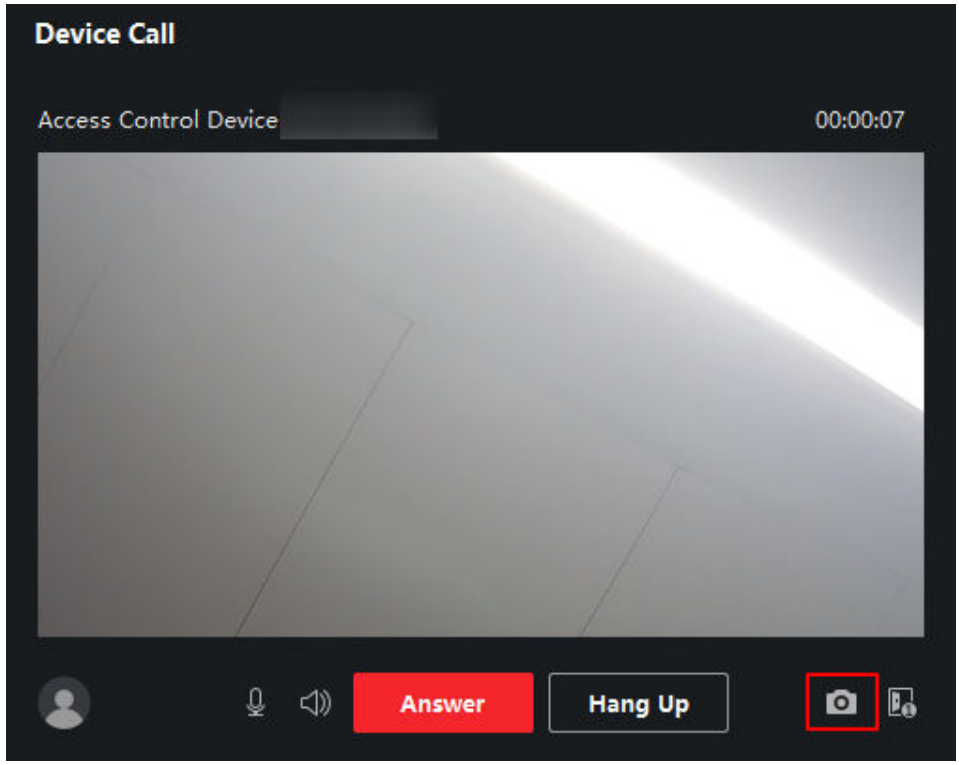


Figure 19-2 Incoming Call

2. Click **Answer** to answer the call.

   After the call is answered, you will enter the In Call window.
3. **Optional:** In the In Call window, perform the following operation(s).

Adjust Loudspeaker Volume	Click to adjust loudspeaker's volume.
End Speaking	Click **Hang Up** to end speaking.
Adjust Microphone Volume	Click to adjust the microphone's volume.
Capture Picture	Click to take a screenshot of the current call screen.
Open Door	When an indoor station is linked with a door station, click to open the door linked with the door station.

19.3 View Real-Time Call Logs

You can view details of all the calls, and you can call the residents or export the logs if they are needed.

Steps

1. Click **Access Control → Video Intercom → Call Log** .

Details of all the calls will be displayed on the right panel including call status, start time, speaking duration, device type and name, and organization and name of resident.

2. **Optional:** Click to re-dial the resident.
3. **Optional:** Set search conditions (including call status, device type, and time) on the top of the page to filter call logs.
4. Click **Export** to save the logs (a CSV file) in your PC.

19.4 Release a Notice to Resident

You can send a notice to the residents by one-touch. Four notice types are available: advertising, property, alarm, and notice information.

Steps

1. Click **Access Control → Video Intercom → Notice** .
2. Click **Add** to open the Create Notice panel.
3. Click to select the residents you are going to deliver notice to.
4. Enter the required information.

Note

- Up to 63 characters are allowed in the Subject field.
- Up to 1023 characters are allowed in the Content field.
- You can add up to 6 pictures. Each picture should be in JPG format and smaller than 512 KB.

5. Click **Send** to send the notice to the selected resident(s).

   Information about the sent notices will be displayed on the left panel. Click a notice to view its details on the right panel.
6. **Optional:** Click **Export** to save all the notices in your PC.

19.5 Enable Calling between Video Intercom Device and Client

You can enable or disable the calling between the added video intercom devices and the client. If enabled, you can call the intercom device via client, and the client can receive the calling from the device; If disabled, the client and video intercom device cannot call each other.

Note

You needn't enable this function for the door stations added by ISUP for calling.

Click → **Tool → Video Intercom Arming Control** to open Video Intercom Arming Control page. The list shows the status of the video intercom devices. You can set the switch to on for the video intercom device to enable calling between the video intercom device and the client. If required, perform the following operations.

- **Filter Device** ：If there are too many devices, you can enter the key words in the Filter field to filter the device.
- **Arm All / Disarm All**: Click **Arm All** to arm all devices. Click **Disarm All** to disarm all devices.

19.6 Apply Application Package to Indoor Station

If you want to install application on indoor station, you can apply the application package saved in local PC to one or multiple indoor stations remotely via the client. The package will be installed on the indoor stations automatically after the indoor stations receive the package.

Note

This function should be supported by the device.

Click **Access Control → Video Intercom → Application** to enter the applying application page. Select one or multiple added indoor stations, and click **Apply Application**. You can select the installation package from local folder to apply the application package to the selected indoor stations.

After the indoor stations receive the package, the application will be installed on the devices automatically.

Up to two applications can be installed on the indoor station. If two applications have been installed, you need to uninstall one for installing another one. Click to uninstall the application installed on indoor station remotely.

Chapter 20 Topology Management

The topology management module provides network health status monitor functions based on the hardware and software, in order to ensure normal link transmission and better usage of the resources in network. It is mainly used for network maintenance and management. The administrator can check the status of the device and its connected devices via topology view, and know real-time network status.

20.1 Topology Display Overview

The topology display page shows the relationships among different devices obtained by the client, including the devices added to the client, the devices searched via SADP, and the devices connected with the added devices or searched devices. You can check device information, link transmission status, etc.

Note

- When the devices are searched via SADP, the device names in topology view are consistent with their IP addresses.
- For the unknown device, the topology view will show the device type only.

Enter Topology module, click to get the latest device list and display the topology relationship. If you enter the Topology page for the first time, you can follow the guide and click **Add Topology** to generate the topology view. Then you can click → **Get Topology Again** to refresh it according to actual requirements.

Note

You can also click → **Refresh Status** to get the online or offline status of the devices.

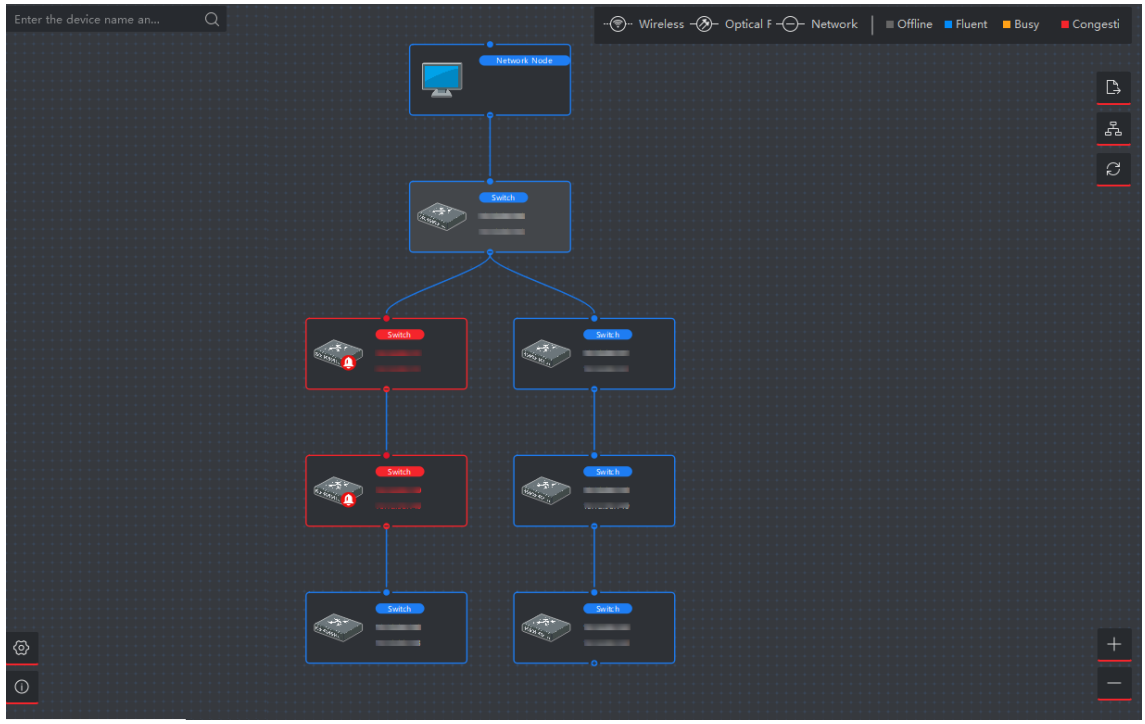


Figure 20-1 Topology Display

Device Node

- **View Device information**: You can check the device type and IP address.

  Note

  If the device name, IP address, online status, or other information of the device is edited, the device information in topology view will change synchronously.

- **Expand/Hide**: You can click 或 to expand or hide the sub node(s) of certain device.
- **Adjust Topology View**: On the lower right corner, you can click the icons or scroll your mouse wheel to enlarge or narrow the typology.
- **Search Topology**: On the top left corner, you can enter another name or IP address of a device to view the corresponding typology.

Line

On the top right corner, you can view the icon of lines (wireless, optical fiber, and network) and the meaning of different colors.

20.2 Set Topology Parameters

You can set the parameters for the topology display, including display level and bandwidth alarm threshold.

Enter Topology module, and click in lower left corner to set the related parameters as follows.

Set Display Level

When there are too many devices combined into a complex topology, you can set the display level to show the main structure more clearly. After changing the typology settings, you need to click to view the latest topology. If the device node is hidden, you can click to expand the hidden the device node.

Set Upstream Bandwidth L1/L2 Alarm

You can set upstream bandwidth L1 alarm and L2 alarm. The line will turn to yellow (busy)/red (congestion) when the bandwidth exceeds the threshold of L1/L2 alarm.



Figure 20-2 Set Topology Parameters

20.3 View Device Details

You can view the details of the devices in topology, such as basic information, device usage, device panel status, and port information.

On Topology page, double-click the device node to show the device details as follows.

Basic Information

The basic information shows the device type, model, and IP address of the device.

Device Panel Status

The device panel status shows the supported port type, and port usage.

Port Information

The port information shows the ports of the device, and the peer device information.

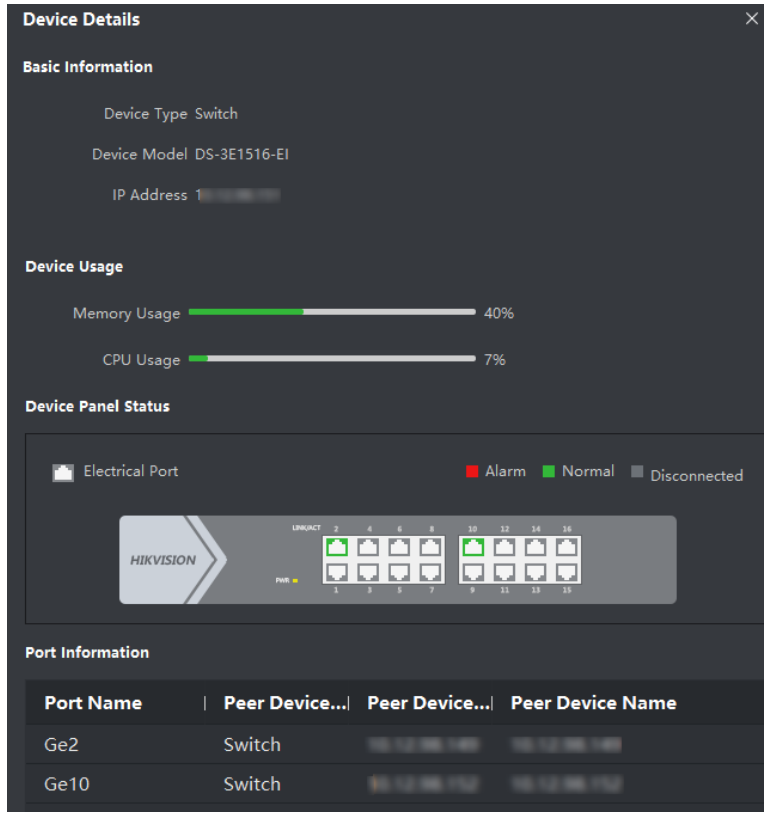


Figure 20-3 Device Details

20.4 View Link Details

You can view the details of the link between two device nodes, such as transmission rate, device type, port status, IP address, and port name of each device.

On Topology page, double-click the line between two device nodes to show the link details as follows.

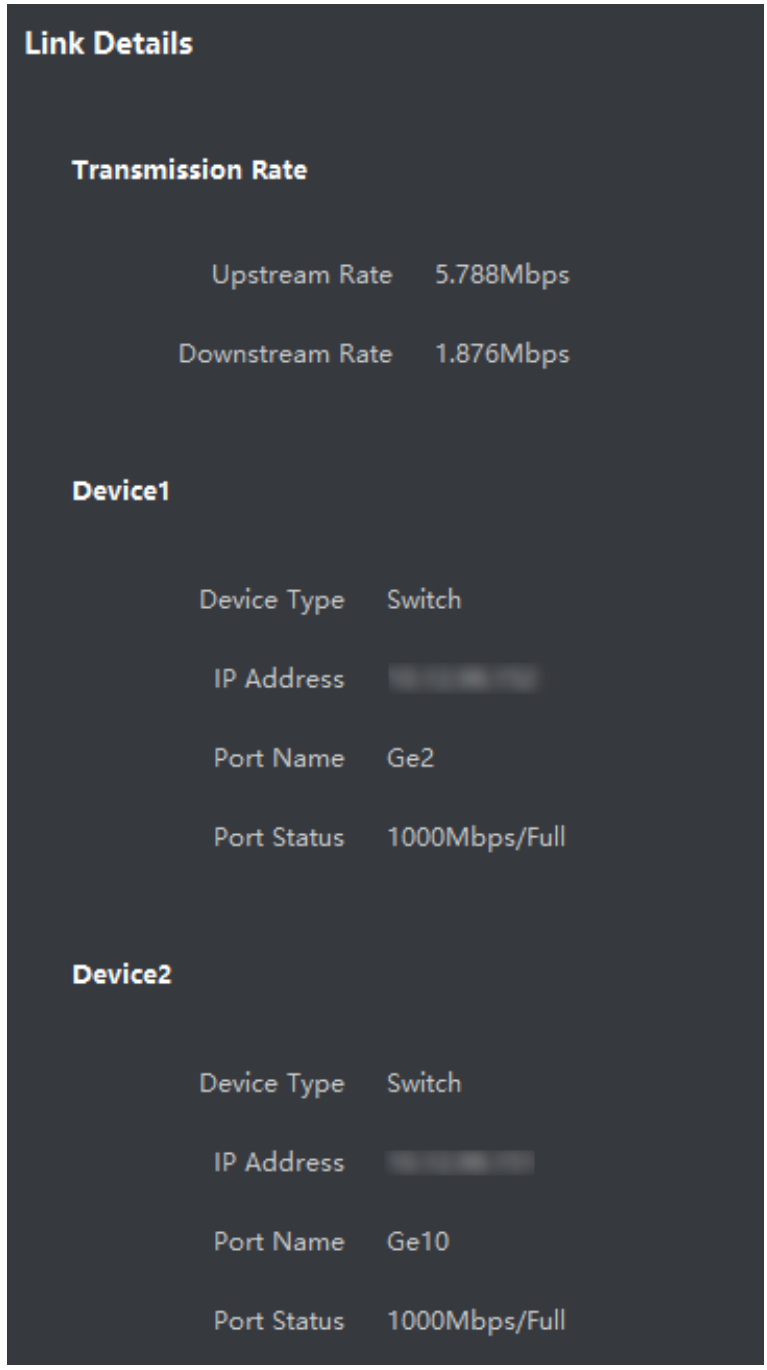


Figure 20-4 Link Details

20.5 View Signal Transmission Path

When the data transmission between the network camera and the switch is abnormal, you can check the signal transmission path to find the faulted link for link maintenance.

On Topology page, click in top right corner, and select network camera and NVR/transmission device to show the flash of the signal transmission (including link and devices) between the two devices.

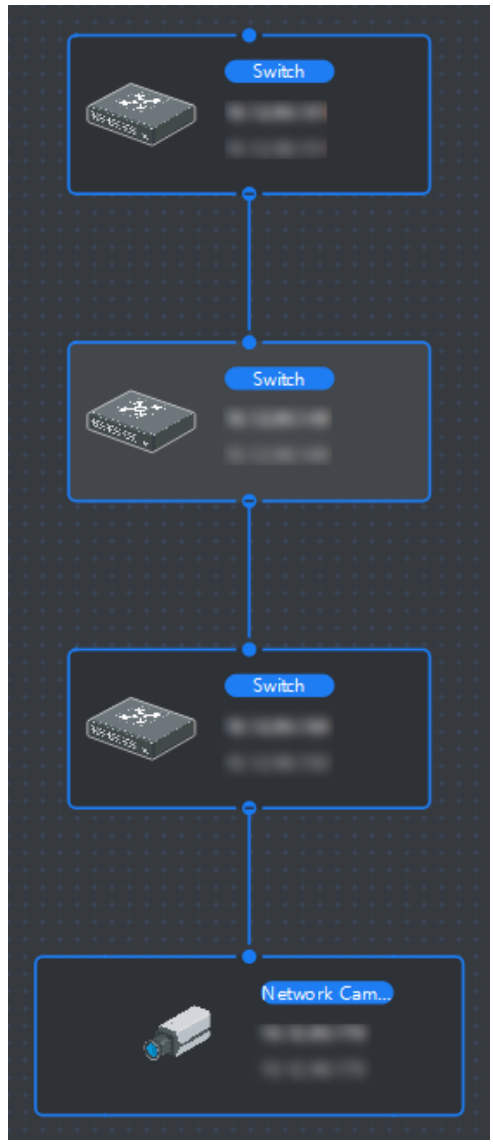


Figure 20-5 View Signal Transmission Path

20.6 Export Topology

You can export the topology view as PDF file, in order to view the device connection status, level, type, IP address and other information.

On Topology page, click , and select the path to export the typology.

20.7 More Functions

More functions in Topology module are supported, including handling events, viewing device status, remote configuration, etc.

Note

The displayed functions may vary for different devices.

Right-click the device note in topology, and perform one of the following operations.

Event Handling

When the events are detected for the device, a red alarm icon appears on the device node. You can enter Event Handling page to view the event information (e.g., event source, event time, and event details) .
Select one or multiple events in the list, and click **Clear Events** to delete the selected events. If all events are cleared, the red alarm icon on device node will disappear.

Note

This function is supported by the switch, wireless network bridge, and fiber converter.

Remote Configuration

The remote configuration function provides a quick entry to configure the related device parameters, such as system parameters, network parameters, port configuration, and link aggregation.

Edit Name

You can edit the device name as you want.

Set as Root

You can set the device as root node to adjust the topology structure and connection. After the setting, the topology will be refreshed automatically.

Note

This function is supported by the switch, wireless network bridge, fiber converter, and virtual switch.

Chapter 21 Broadcast Management

You can manage the added speaker units and configure the related functions for them, such as grouping multiple speaker units, configuring live broadcast, and configuring scheduled broadcast.

21.1 Control Speaker Units

After adding speaker units, you can batch control multiple speaker units in a group, such as adjusting volume and setting linkage actions.

Note

- Make sure you have added speaker units on **Device Management → Device** . Refer to ***Add Device*** .
- Make sure you have grouped speaker units on **Device Management → Group** . Refer to ***Group Resources*** .

On the left, select **Broadcast Console**, select a speaker unit group, and all speaker units in the group will be displayed.

You can perform the following operations to control speaker units.

Device Card Operations

Adjust volume for the device.

Play the device's default audio to test if the speaker functions properly.

Click **Configure** to go to the event configuration page, and configure linked broadcast tasks for events. Refer to ***Configure Event for Camera*** .

Configure input volume and channel input.

Configure additional parameters such as Bluetooth input volume and output volume.

Device Batch Settings

Select one or multiple devices, then click **Device Batch Settings**.

Table 21-1 Device Batch Settings

Operation	Description
Audio	**Input Volume Adjustment** Set volume levels individually for each source (e.g., Bluetooth, USB, Microphone). **MIC 1/2/3/4** Adjust the input volume for microphones. **RCA IN 1/2/3/4** Adjust the input volume for external audio devices (e.g., players, computers). **Bluetooth / USB** Adjust the playback volume for digital audio sources. **Output Volume Adjustment** Adjust the final output volume played through the speakers.
Algorithm	**Noise Reduction** Removes background noise from the environment. Noise Reduction Level: Sets the intensity of noise reduction. Higher values produce stronger noise suppression. **Dereverberation** Removes echo and reverberation to make sound clearer. Dereverberation Level: Sets the intensity of dereverberation. Higher values produce stronger echo suppression. **Equalizer** Allows you to boost or attenuate sound at specific frequencies to correct frequency response deviations during audio capture or playback. • Uplink: Adjusts sound captured by the microphone. • Downlink: Adjusts sound played through the speaker. 1. Click **Upward EQ / Downward EQ → Configuration → Enable** . 2. Click to select one or multiple frequency points. - HPF (High-Pass Filter): Cuts off low frequencies and retains only high frequencies. Ideal for eliminating low-frequency noise (e.g., electrical hum). - LSF (Low Shelf): Adjusts the overall level of low frequencies. Great for making bass fuller or cleaner.

Operation	Description
	- 1–8 (Parametric EQ): Precisely adjusts the level of a specific frequency. Best for fine-tuning. - HSF (High Shelf): Adjusts the overall level of high frequencies. Great for making sound brighter or softer. - LPF (Low-Pass Filter): Cuts off high frequencies and retains only low frequencies. Ideal for eliminating high-frequency noise (e.g., hissing). 3. Adjust frequency points: - Drag up = increase volume (boost) - Drag down = decrease volume (attenuate) - Drag left/right = change the frequency position controlled by that point You can also enter values directly in the table below for Freq (frequency position) and Gain (gain level) — the effect is the same as dragging. 4. Click **OK** to save and apply the settings. 5. (Optional) Click **Reset Defaults** to restore defaults. Use case: If the microphone sounds muffled or vocals are unclear, go to Uplink → Enable Equalizer → select the middle frequency point (No. 4) → drag upward to boost vocals → listen to confirm → click OK. **Automatic Gain Control (AGC)** Automatically adjusts audio gain to keep output volume at a stable level, preventing sound from fluctuating between too loud and too quiet. • Target: The desired output volume level. • Output Noise: The maximum acceptable noise level. If exceeded, gain is automatically reduced. • Maximum Gain: The maximum amount of gain adjustment, preventing over-amplification. • Adjustment Speed: Controls how quickly gain is adjusted. Higher values respond faster to changing sound levels; lower values adjust more gradually for stable audio environments. Use case: In a multi-person meeting where speakers sit at different distances from the microphone, audio levels can vary significantly. Enabling AGC automatically adjusts gain so everyone's voice stays at a consistent volume — no manual adjustment needed.
Other Settings	**Acoustic Fidelity Mode** Balances audio quality against network transmission latency to suit different network conditions.

Operation	Description
	Listening Audio Encoding Sets the audio compression format used for listening. The default codec is MP3. **Scene Mode** • Balanced Mode: Maintains a natural frequency balance across all bands, preserving the original sound character. • Voice Enhancement: Improves clarity and detail, optimizing vocal intelligibility and instrument layering. • Loudness Enhancement: Boosts overall perceived loudness, making sound fuller and more impactful.

Channel Batch Settings

Select one or multiple devices, then click **Channel Batch Settings** to configure volume settings. Adjust overall audio levels and fine-tune final output effects.

Time Settings

Click **More Settings → Time Batch Settings** to configure time settings for the selected devices.

NTP

Automatically synchronize time based on a time server.

Manual Time Sync

Manually set the time or synchronize with the computer's time.

SIP (Session Initiation Protocol)

Click **More Settings → SIP** to perform SIP registration and configure SIP call parameters for the selected devices.
SIP allows speaker units to register with a network audio system. Once configured, the Client can initiate voice calls to the devices over the network.

SIP Register

Devices authenticate and report their status to the SIP server.

SIP Call

Set rules for how devices handle incoming call requests.

Encoding/Decoding

Audio compression format. Multiple selections are allowed.

Allowed Call

Control whether the device accepts calls.

Application Channel

Specify the output path for the audio stream received during SIP calls, meaning the audio will be broadcast through the selected channel.

DTMF

DTMF (Dual-Tone Multi-Frequency) allows you to trigger predefined tasks on the device using buttons.

For example, create a DTMF task named **Emergency**, set the trigger button to **1**, and link it to an emergency evacuation notification audio file. Once configured, when a user presses **1**, the device will play the emergency evacuation audio, enabling emergency broadcasting.

After successfully creating a DTMF task, click  to quickly adjust the volume.

URL

Click **More Settings → URL** and enter a network audio URL to play audio directly from the network — no need to pre-download the file to the device.

21.2 Manage Material Library

You can add media library, upload audio files, and play the audios.

Steps

1. On the left, select **Material Library**.
2. Select a media library, or **New Directory**.
3. Click **Add**, and select audio files (in MP3 and WAV formats) from the local PC for uploading.
4. **Optional:** After adding materials, click  to play the audio. You can also edit the materiel name (which cannot be duplicated).

21.3 Configure Live Broadcast

You can select the speaker units and a broadcast mode (emergency broadcast, speak in real-time, play audio, FM broadcast, and text notification) to configure the live broadcast. The corresponding audio file, speech synthesis, or your voice will be played by the speaker units in real time.

Before You Start:

Note

- Make sure you have added speaker units on **Device Management → Device** . Refer to ***Add Device*** .
- Make sure you have grouped speaker units on **Device Management → Group** . Refer to ***Group Resources*** .

On the left, select **Broadcast Console**, select a speaker unit group, and check the desired speaker units. Select a broadcast mode on the right to start live broadcast.

Mode	Application Scenario	Operation
Emergency Broadcast	Broadcast real-time speaking about emergency mustering for guiding persons in specific areas to protect themselves.	Click **Emergency Broadcast** to start real-time speaking of emergency contents. Click **Pause Speaking** to pause the broadcast, and click **Resume Speaking** to continue the broadcast.
Speak in Real Time	Broadcast real-time speaking about general issues, such as news broadcast.	Click **Speak in Real Time** to start real-time speaking. Click **Pause Speaking** to pause the broadcast, and click **Resume Speaking** to continue the broadcast.
Play Audio	Play audio files such as class bell and background music.	Click **Play Audio**, select the audio files on the media library, and click **Start Playing**.
FM Broadcast	Achieving directional audio coverage using FM signal transmission. For instance, in industrial parks, distinct FM frequencies are allocated to production zones and office areas to deliver tailored safety announcements.	Click **FM Broadcast**, and the system will automatically scan and list all available channels. The first channel detected during the scanning process will begin playing immediately. Once the scan is complete, you can select any channel in the list and click **Start Playing**. The speaker unit will then transmit FM signals at the selected frequency, enabling directional audio broadcasting.
Text Notification	Transmit texts to AI person voice for reading and broadcasting.	Click **Text Notification**, enter the text, select the play mode and audio type, and click **Start Playing**.

21.4 Add a Scheduled Broadcast Task

You can add a scheduled broadcast task by configuring the parameters such as the period type and play mode to add a scheduled broadcast task in the client and then apply the task to speaker units. For the added scheduled broadcast tasks, you can view the task details, search for target tasks, etc.

Before You Start

- Make sure you have added speaker units on **Device Management → Device** , refer to ***Add Device*** .
- Make sure you have grouped speaker units on **Device Management → Group** , refer to ***Group Resources*** .

Steps

1. On the left, select **Scheduled Broadcast**.
2. Click **Add**.
3. Specify the task name, speaker unit, and time period.

   You can set the schedule by day, week, or custom time.
4. **Optional:** Select a task type.
5. Click **Add** and set the execution time.
6. Select the play content and play mode.
   - For **Audio File**: select audio files, and set the play mode. For the **Loop** mode, set the play duration.
   - For **Speech Synthesis**, enter the text, select the play mode and audio type, and set the play duration.

     If an audio template is configured in the task list, click **Select Template** to quickly insert the text.
   - For **URL**: Enter or choose the URL, and then configure the playback mode and duration accordingly.
7. **Optional:** Set the broadcast priority and volume.

   Note

   If **Increase Volume** is enabled, the broadcast volume will be doubled.
8. Click **OK**.
9. **Optional:** On the Scheduled Broadcast page, perform the following operations.

Apply Task	Select a scheduled broadcast task and click to apply it. Or select multiple tasks, and click **Batch Apply** to apply them.
View Failure Records	Click **View Failure Records** to view the failure records. If necessary, reapply the failure records.
Edit Task	Click to edit the task information.
Audio Template	Click **Audio Template** to add a template, then enter the audio content.

Chapter 22 Log Search

Two log types are provided: operation log and system log. The operation logs refer to the normal operations that the user did on the client, such as adding device, resetting password, starting live view, etc.; and the system logs record the system information, such as login, logout, locking and unlocking, etc. You can search the log files and view the log details, including time, user, etc.

Steps

1. Enter the Log Search module.
2. Click to specify the start time and end time.

   Note

   You can search the logs within one month.
3. Select a user to search the log files which are generated when this user operate on the client.
4. Select **Operation Log** or **System Log** as log type.
5. Click **Search**.

   The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.
6. **Optional:** Perform the following operations if there are too many log files.

   Filer Click on each table header and select to filter the logs.

   Sort Click the table header to sort the logs by the time or letter sequence.

Chapter 23 User Management

To improve the system security, the administrator should create different account for different user, and assign different permissions to the user. To avoid different people sharing the same user account, we recommend you manage the user accounts periodically.

23.1 Add User

The super user and administrator can add new users, and assign different permissions for different users if needed.

Perform this task to add an user account.

Steps

Note

The user account you registered to log in the software is set as the super user.

1. Enter the User Management module.
2. Click **Add User** to show user information area.
3. Select the user type from the drop-down list.

   Administrator

   The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own.

   Operator

   The operator account has no permission by default and you can assign the permissions manually. An operator can only change the passwords of its own account and the accounts which are added by it.
4. Enter the user name, password, and confirm password as desired.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
5. Check the checkboxes to assign the permissions to the created user.
6. **Optional:** Click **Default Value** to restore the default permissions of this user.

7. Click **Save**.

Note

Up to 50 user accounts can be added for the client software.

After created user account successfully, the user account is added to the user list on the Account Management page.

8. **Optional:** Perform the following operations after the user account is created.

Edit User Click a user from the list to edit the user information.

Note

Only the password of the super user can be edited.

Delete User Select the user from the list and click **Delete User**.

Note

You cannot delete the super user.

23.2 Change User's Password

The administrator can change normal user's password without entering the old password, while the administrator should enter the old password when changing the password of itself.

Before You Start

Add user to the software client.

Steps

1. Enter the User Management module.
2. Select the user need to be change password, click **Change**.
3. **Optional:** Enter the old password.

Note

When changing the administrator's password, you need to enter the old password first.

4. Enter the new password and confirm the password.
5. Click **OK**.

Chapter 24 System Configuration

24.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

Date Format / Time Format

The display style of date and time on related pages.

Log Retention Period

The time for keeping the log files. Once exceeded, the files will be deleted.

Maximum Mode

Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

Network Performance

Set the network conditions to **Normal**, **Better** or **Best**.

Save Pictures in Structure Data Format

- After **Save Pictures in Structure Data Format** is enabled, the **Delete Registered Picture** in **Person** module will be available. If a person's information is applied to the device(s) successfully, the person's picture will be automatically deleted and no picture will be displayed in Basic Information. The **Face** column in **Person** module will display the number of the added face picture(s).
- When **Save Pictures in Structure Data Format** is enabled, no pictures will be displayed in Event Details field in Event Center.

Enable Keyboard and Joystick

Enable the keyboard or joystick. After enabled, you can set the shortcuts for the keyboard and joystick.

Note

For details, refer to ***Set Keyboard and Joystick Shortcuts*** .

Export Person Information

If you enable this, the **Export** button for exporting person information will be displayed on the Person Management page. Please pay attention to person information security.

Event Retention Period

The time period for keeping the event information. When the retention period expires, the event record will be deleted automatically.

Detect New Software Version

Enabled

The client automatically checks for software updates upon startup. If a newer version is detected, click to choose from **Update Now**, **Upgrade Later**, or **Ignore the Version**. See ***Operation and Maintenance*** for details.

Note

WAN connection is mandatory for successful data transfer.

Disabled

You must manually check for updates: Go to → **Help** → **About** → **Software Update** .

Auto-Upgrade Device

Set the upgrading mode after the new version of device are detected.

Disable

After enabled, the client will not download the firmware package and upgrade even if the client detects a new version of the client.

Prompt Me If Download and Upgrade

After the client detects a new version of the device, it will prompt the user whether to download the firmware package and upgrade.

Download and Prompt Me If Upgrade

After the client detects the new version of the device, it will download the firmware package automatically, and prompt the user whether to upgrade.

Download and Prompt Automatically

After the client detects the new version of the devices, it will download the firmware package and upgrade the new version automatically.

You need to set a schedule in the **Upgrade Time** field, during which the client upgrades the new version automatically.

Auto Exit Once Timeout

When no user operation is detected for the set duration, the system will auto exit.

Default timeout: 10 minutes (range: 1-60 minutes).

Auto Close Server

If the function is enabled, the server will be closed automatically when the client is closed and the event information will not be received.

Automatic Time Synchronization

Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.

Country/Region

Select the server's region for Hik-Connect, you can select the region you belong to or the nearest region around.

Device Auto Refresh Time

Set the time for automatic refresh of the device (time range: from 1 to 5 minutes, 3 minutes by default). For example, if you set the time to 3 minutes, the device automatically refreshes every 3 minutes.

User Experience Program

If you enable it, we will collect user operation records and software usage data (including main panel operations and software exceptions). All data is only used for product enhancement.

Upon first login to the Client, a pop-up will appear inviting you to join the Program. Please read and agree to the Privacy Policy before enabling the feature.

Auto UI Scaling

Adaptive Mode follows system scaling and uses vector rendering, keeping text and controls sharp. Fixed Mode disables Qt DPI scaling, which causes the system to stretch bitmaps, so the layout stays the same but text may look blurry.

4. Click **Save**.

24.2 Set Live View and Playback Parameters

You can set the parameters for live view and playback, including picture format, pre-play duration, etc.

Steps

1. Enter the System Configuration module.
2. Click **Live View and Playback** tab.
3. Configure the live view and playback parameters.

Picture Format

Select **JPEG** or **BMP** as the image format for storing pictures.

Note

If **Display Temperature on Captured Pictures** switch is set to ON, JPEG is selected as the image format by default and cannot be changed.

Video Format

Select **MP4/AVI** as the format of recorded videos.

Merge Downloaded Video Files

Set the maximum size of merged video file for downloading the video file by date.

Search Video Files Stored in

Search the video files stored in the local device for playback.

Pre-play for

Set the pre-play time for event playback. By default, it is 30s.

Resume Latest Live View Status After Restart

Resume the latest live view status after you log into the client again.

Disconnect Background Videos in Single Live View

In multiple-window division mode, double-click a live video to display it in 1-window division mode, and the other live videos will be stopped for saving the resource.

Enable Wheel for Zoom

Use the mouse wheel for zoom in or out of the video in PTZ mode, or for zoom in or restoring of the video in digital zoom mode. In this way, you can directly zoom in or out (or restore) the live video by scrolling the mouse.

Skip Unconcerned Video during VCA Playback

Skip the unconcerned video during VCA playback and the unconcerned video will not be played during VCA playback.

4. Click **Save**.

24.3 Set Image Parameters

The image parameters of the client can be configured, such as view scale, play performance, etc.

Steps

1. Open the System Configuration page.
2. Click **Image** tab to enter the Image Settings interface.
3. Configure the image parameters.

View Scale

The view scale of the video in live view or playback. It can be set as **Full Screen**, **4:3**, **16:9**, or **Original Resolution**.

Note

You can also set the view scale in Live View module. For details, refer to ***Live View*** .

Play Performance

The play performance of the live video. It can be set as **Shortest Delay**, **Balanced**, or **Fluency**.

You can also select **Custom** and configure the frame rate according to actual needs.

Hardware Decoding Preferred

Select **D3D9** or **D3D11** to enable decoding by hardware for live view and playback. Hardware Decoding can provide better decoding performance and lower CPU usage when playing the HD video during live view or playback.

Enable Highlight

Mark the detected objects with green rectangles in live view and playback.

Display Transaction Information

Display the transaction information on the live view image.

VCA Rule

Display the VCA rule in the live view.

Enable Frame Extracting for High-speed Playback

When playing back the video at high speed (8x speed and above), you can disable this function to make the image of playback more fluent to view the details.

Display Target's Pattern

After enabled, you can view the target person's motion track on the view window.

Overlay Rules on Captured Picture

For the thermal device, set to display the temperature information and fire source information on the captured pictures.

Note

After enabled this function, the Picture Format configured in **System Configuration → Live View and Playback** will change to JPEG and is not editable.

Noise Reduction

Noise reduction mode, which can be set as **Disable**, **Self-adaptive**,or **Enable**.

4. Click **Save**.

24.4 Set Picture Storage

The captured pictures triggered by the events on the devices, can be saved in the PC running the iVMS-4200 Service. You can set the picture storage location here manually.

Steps

1. Enter the System Configuration module.
2. Click **Event Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.

   All the disks of the PC running the iVMS-4200 service will show.
4. Select the disk to save the pictures.

   Note

   The default saving path is: Disk/iVMS-4200alarmPicture
5. Click **Save**.

24.5 Set Alarm Sound

When the event is triggered, the client can give an audible warning to notify the security personnel. You can set the sound of the audible warning in this section.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. **Optional:** Click ··· and select the audio files from the local path for different events.
4. **Optional:** Add customized alarm sound.
   1) Click **Add** to add customized alarm sound.
   2) Double click the **Type** field to customize the alarm sound name as desired.
   3) Click ··· and select the audio files from the local path for different alarms.
5. **Optional:** Click for a testing of the audio file.
6. **Optional:** Click in the Operation column to delete the custom sound.
7. Click **Save**.

Note

The format of the audio file can only be WAV.

24.6 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

   Ringtone

   Click ··· and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click for a testing of the audio file.

   Max. Ring Duration

   Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

   Max. Speaking Duration with Indoor Station

   Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

   Max. Speaking Duration with Door Station

   Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

Max. Speaking Duration with Access Control Device

Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.

Card Reading Mode

Specify the card reading mode as three bytes, four bytes, or full card No..

4. Click **Save**.

24.7 Set File Saving Path

The video footage (manually recorded during live view and clipped during playback) and captured pictures are stored on the local PC. The saving path of these files can be set.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click ··· and select a local path for the files.
4. Click **Save**.

24.8 Set Icons Shown on Toolbar

The icons and the order on the toolbar in the live view and playback window can be customized. You can set to display what icons and set the icon order.

Perform the following task when you need to set icons shown on Toolbar.

Steps

1. Enter the System Configuration module.
2. Click **Toolbar** tab to enter the Toolbar Settings page.
3. Set **Enable Screen Toolbar Display** switch to ON to enable displaying the toolbar on in the live view and playback window.
4. Click the required icon to display on the toolbar.
5. **Optional:** Drag the icon to set the icon order when displaying on the toolbar.

Table 24-1 Icons on Live View Toolbar

	**Stop Live View**	Stop the live view in the display window.
	**Capture**	Capture the picture in the live view process. The capture picture is stored in the PC.
	**Record**	Start manual recording. The video file is stored in the PC.

	PTZ Control	Start PTZ mode for speed dome. Click and drag in the view to perform the PTZ control.
	Two-way Audio	Start the two-way audio with the device in live view.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Instant Playback	Switch to the instant playback mode.
	Remote Configuration	Open the remote configuration page of the camera in live view.

Table 24-2 Icons on Playback Toolbar

	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
	Record	Start manual recording. The video file is stored in the PC.
	Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Download	Download the video files of the camera and the video files are stored in the PC.
	VCA Playback	Set the VCA rules. For more details, refer to ***VCA Playback*** .
	Tag Control	Add default or custom tag for the video files to mark the important video point. You can also edit the tag.

6. Click **Save**.

24.9 Set Keyboard and Joystick Shortcuts

The keyboard can be connected to the client and be used to control the PTZ cameras. You can set the shortcuts for keyboard and joystick to get quick and convenient access to the commonly used actions.

Perform this task when you need to set keyboard and joystick shortcuts.

Steps

Note

This configuration page will display after enabling keyboard and joystick in General Settings. For details, refer to ***Set General Parameters*** .

1. Enter the System Configuration module.
2. Click **Keyboard and Joystick** to show the Keyboard and Joystick Shortcut Settings area.

3. Select the COM port from the drop-down list for keyboard if the keyboard is connected to the PC installed with the client.

Note

You can enter the Device Manger of the PC to check the COM port, which the keyboard is connected to.

4. Set shortcuts for keyboard and joystick.
   1) Select a certain function name on Function column.
   2) Double-click the item field under the PC Keyboard, USB Joystick or USB Keyboard column.
   3) Select the compound keys operation or number from the drop-down list to set it as the shortcuts for the function of the keyboard or USB joystick.
5. Click **Save**.

Example

For the **Focus (+)** function, if you set **Home**, **1**, and **F1** as the shortcuts of the PC Keyboard, USB Joystick and USB Keyboard, you can press the Home key on PC keyboard, control the joystick to the 1 direction, or press F1 key on USB keyboard to zoom in.

24.10 Set Email Parameters

When an event is triggered, if you can set **Send Email** as linkage action for this event, the client will an email to the recipients for notification. You need to set the email settings and specify target recipients in this section.

Steps

1. Enter the System Configuration module.
2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

STMP Server

The STMP server IP address of host name (e.g., smtp.263xmail.com)

Encryption Type

You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS** .

Port

Enter the communication port used for SMTP. The port is 25 by default.

Sender Address

The email address of the sender.

Security Certificate (Optional)

If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

User Name

Enter the user name of the sender email address if **Server Authentication** is checked.

Password

Enter the password of the sender Email address if **Server Authentication** is checked.

Receiver 1 to 3

Enter the email address of the receiver. Up to 3 receivers can be set.

4. **Optional:** Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

24.11 Manage Security Authentication

For the data security purpose, the security certificate of clients and added servers should be same. You can set the verify certificate is required or not when enabling transmission encryption using TLS (Transport Layer Security) protocol.

Before adding a server to the client, you should export the service certificate from the client service, and import it to the server. If multiple clients use the same server, you should make the security certificates of the clients and the server same with each other.

24.11.1 Export Certificate from Service Management

You can export the security certificate from the current client service and import the exported certificate file to other clients.

Steps

1. Enter the Service Management.
2. Click **Export** to save the certificate file in the local PC.

Note

The certificate file is in XML format.

What to do next

After exporting the certificate, you can copy the certificate to the PC installed with the client and import it to other clients.

24.11.2 Import Certificate to Client

If there are multiple clients accessing the same steam media server, you should import the same certificate to the clients and server.

Before You Start

Make sure you have exported the security certificate from one of the client service.

Note

For details, refer to ***Export Certificate from Service Management*** .

Steps

1. Copy the certificate file exported from other client to the local PC.
2. Enter the System Configuration module.
3. Click **Security Authentication** tab to enter the security authentication setting interface.
4. Click **Import**.
5. Select the certificate file from your local PC and click **Open**.

Note

Please restart the client to take effect.

24.11.3 Certificate Verification for Transmission Encryption

On the Security Authentication page, you can set the device certificate verification is required or not for transmission encryption.

Click **System Configuration → Security Authentication** to enter the security authentication interface. Select the Verify Certificate as **Yes** or **No**.

Yes

You must put the device certificate to the designed directory if you enable transmission encryption when adding device. And the device will be added with transmission encryption and the certificate will be verified, which improves the security level.

No

The device certificate is not required if you enable transmission encryption when adding device. And the device will be added with transmission encryption.

Chapter 25 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convenient usage of the client.

File / System / Tool

In the upper-right corner of the client, click → **File / System / Tool** .

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files from local PC to the client if needed, and vice versa.

When exporting configuration files, you can export all files (including all configuration parameters and historical events) or export only configuration parameters.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backed up data.

Note

- When disk space falls below 2 GB, older backup files get overwritten.
- For disk space between 2 GB and 10 GB, a low storage warning is triggered, yet the backup function remains unaffected.

Skin

Change the skin of the client, including bright-color series and black-color series.

Broadcast

Check one or more devices to enable the broadcast function of the device(s).

Batch Wiper Control

Batch turn on/off the wiper.

1 VS 1 Face Comparison

Select two face pictures from the local PC for comparison. The similarity between the two pictures will be shown.

Note

This function can be used for identity verification and is only supported by the DeepinMind device.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the email to the receiver.

Feedback

In the upper-right corner of the client, click → **Feedback** to report usage-related issues by filling in fields including title, problem type, description, attachment, device, and email.

Note

- WAN connection is mandatory for successful data transfer.
- A maximum of 5 feedback submissions per day is allowed.
- For attachments, you can add up to 1 TXT log file and 4 JPG/JPEG/PNG pictures simultaneously.
- Up to two linked devices can be selected. Only device model and firmware version will be collected.

Version Update

In the upper-right corner, if a newer version is detected, click to choose from **Update Now**, **Upgrade Later**, or **Ignore the Version**.

Update Now

Update to the latest version.

Upgrade Later

You can click when needed.

Ignore the Version

The update button will not show until the new version is available.

Appendix A. Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data

Wiegand Data = Valid Data + Parity Data

Total Length

Wiegand data length.

Transportation Rule

4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode

Valid parity for Wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length

If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length

If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length

If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

Appendix B. Troubleshooting

Here are some common symptoms when operating the client software. We provide the possible causes and corresponding solutions to solve the problems.

B.1 Failed to get the live view of a certain device.

Problem

Failed to get the live view of a certain device.

Possible Reasons

- Unstable network or the network performance is not good enough.
- The device is offline.
- Too many accesses to the remote device cause the load of the device too high.
- The current user has no permission for live view.
- The version of the client software is below the needed version.

Solutions

- Check network status and disable other not in use process on your PC.
- Check the device network status.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

B.2 Local recording and remote recording are confused.

Problem

Local recording and remote recording are confused.

Solutions

- The local recording in this manual refers to the recording which stores the video files on the HDDs, SD/SDHC cards of the local device.
- The remote recording refers to the recording action commanded by the client on the remote device side.

B.3 Failed to download the video files or the downloading speed is too slow.

Problem

Failed to download the video files or the downloading speed is too slow.

Possible Reasons

- Unstable network or the network performance is not good enough.
- The NIC type is not compatible.
- Too many accesses to the remote device.
- The current user has no permission for playback.
- The version of the client software is below the required version.

Solutions

- Check network status and disable other not in use process on your PC.
- Directly connect the PC running the client to device to check the compatibility of the NIC card.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

Appendix C. FAQ (Frequently Asked Questions)

Here are some frequently asked questions when operating the client software. We provide the corresponding answers to help the users to solve the problems.

C.1 During live view, why an error message with error code 91 prompts ?

Question

During live view, why an error message with error code 91 prompts ?

Answer

For live view of multiple windows, the channel may not support sub stream. You should disable the function of **Auto-change Stream Type** in **System Configuration → Image** , and select the appropriate steam type for live view.

C.2 During live view, why the image is blurred or not fluent?

Question

During live view, why the image is blurred or not fluent?

Answer

Check the driver of video card. We highly recommend you update the driver of video card to the latest version.

C.3 Why the memory leaked and the client crashed after running for a while?

Question

Why the memory leak and the client crashed after running for a while?

Answer

In the installation directory of the client software, open the **Setup.xml** file with Notepad and modify the value of **EnableNetandJoystickCheck** to **false**. Restart the client, and if the problem is still not solved, contact our technique support.

C.4 How to get better performance of live view and playback when network bandwidth is low?

Question

If the network bandwidth is low, how to get better performance of live view and playback?

Answer

This function should be supported by the device. You can perform the following operations to realize live view in low bandwidth:

Note

You should disable **Auto-Change Stream Type** beforehand.

- Firstly, after adding the encoding devices to the client, you need to set the camera's streaming protocol.
  1. Enter **Device Management → Group** .
  2. Select the camera in the Encoding Channel list and click .
  3. In the Edit Camera window, set the **Protocol Type** (for live view) and **Playback Protocol Type** (for playback) as **Adaptive UDP**.

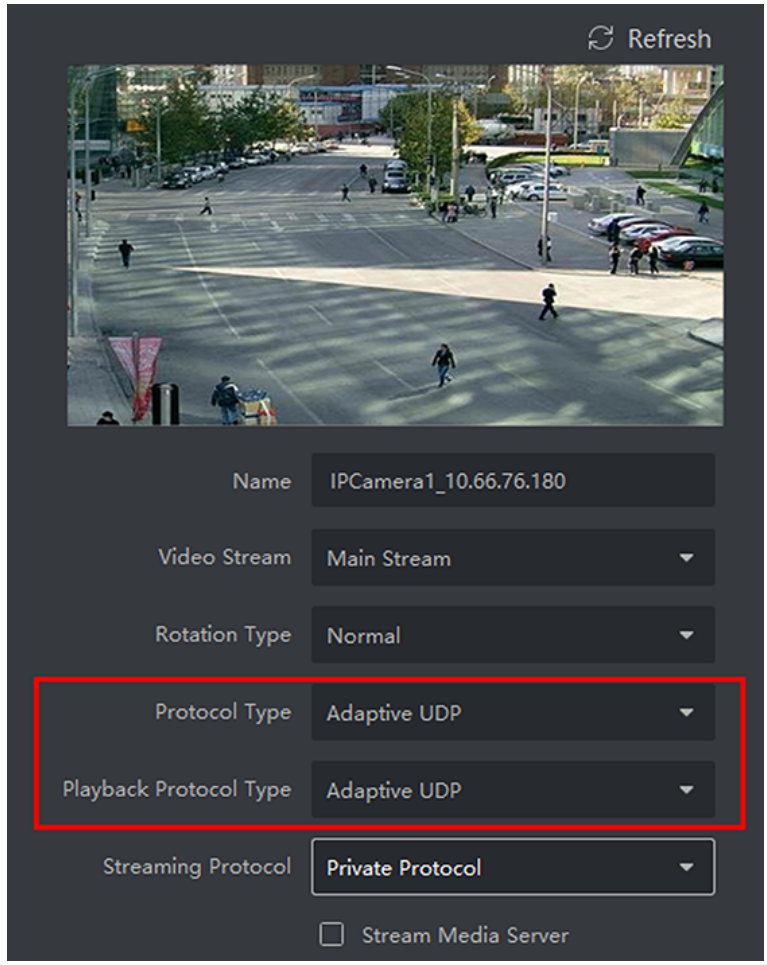


Figure C-1 Set Protocol Type

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

- Select stream type for live view.

1. Enter Main View module.
2. In the device list on the left, move the cursor to the camera name and click → **Stream** .

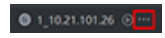


Figure C-2 Select Stream Type

3. For network camera, set the stream type as **Third Stream**.
   For DVRs or NVRs, set the stream type as **Virtual Stream**.
4. Start live view.

Appendix D. Error Code

Code	Error Name	Description
iVMS-4200		
317	No videos.	It will be prompted when the user has no permission to play back.
HCNetSDK.dll		
1	Invalid user name or password.	
2	No permission.	The user in the device has no enough permission.
4	Invalid channel number.	It will be prompted in the live view of remote screen control.
5	No more devices can be connected.	
7	Failed to connect the device.	
23	Not supported.	
29	Operation failed.	
43	No buffer.	It will be prompted when adding a device and the device port is occupied by a web server.
55	Invalid IP address.	
56	Invalid MAC address.	
91	The channel does not support the operation.	It will be prompted when failed to get the sub stream.
96	The device is not registered on the DDNS.	
153	The user is locked.	
250	The device is not activated.	
404	Channel No. error or the device does not support the sub stream.	It will be prompted when failed to get the sub stream or the sub stream does not exist.
424	Failed to receive the data for RTSP SETUP.	It will be prompted when adding the live view for the software DVS via external network.
800	No more bandwidth can be used.	
Playctrl.dll		

Code	Error Name	Description
2		The stream is not a Video & Audio stream.
6		The playback window turns black when adopting H.265 in the 64-bit operating system.


See Far, Go Further