


# HikCentral Professional V3.1.1 Web Client

User Manual

# Contents

**Chapter 1 Introduction ..... 1**

**Chapter 2 Getting Started ..... 2**

2.1 Installation and Deployment ..... 2

2.1.1 Recommended Running Environment for Server ..... 2

2.1.2 Standalone Deployment ..... 3

2.1.3 Cluster Deployment ..... 6

2.2 Login ..... 9

2.3 Download Mobile Client ..... 11

2.4 Home Page Overview ..... 13

2.4.1 Application Market ..... 15

2.4.2 Customize Preset Workbench ..... 16

2.4.3 Customize Personal Workbench ..... 17

2.4.4 View Digital Dashboard ..... 18

2.5 License Management ..... 19

2.5.1 Activate License ..... 22

2.5.2 Update License ..... 25

2.5.3 Deactivate License ..... 28

**Chapter 3 Device and Server Management ..... 31**

3.1 Before You Start ..... 31

3.2 Add Device(s) ..... 31

3.2.1 Adding Modes Supported by Different Devices ..... 31

3.2.2 Parameters on Add Device Pages ..... 38

3.3 Add Server(s) ..... 43

3.4 After Adding Devices/Servers: Operations on Device List Page ..... 46

3.4.1 Add and Manage Applications ..... 49

3.4.2 Configurations After Adding Portable Enforcement Devices ..... 51

3.4.3 Configurations After Adding Speed LED Displays ..... 52
3.4.4 Configure Parameters for Access Control Devices / Sliding Gate Opener / Elevator Control Devices ..... 52
3.4.5 Upgrade Device Firmware ..... 62
3.4.6 Create Password for Inactive Device(s) ..... 64
3.4.7 Edit Online Device's Network Information ..... 65
3.4.8 Restore/Reset Device Password ..... 66
**Chapter 4 Area Management ..... 69**
4.1 Add an Area Manually ..... 69
4.2 Import Areas in a Batch ..... 70
4.3 Add Element to Area ..... 71
4.4 Operations on Area Page: After Adding Elements to Areas ..... 73
4.5 Edit Element in Area ..... 78
4.5.1 Parameters on Edit Camera Page ..... 79
4.5.2 Parameters on Edit Door Page ..... 83
4.5.3 Parameters on Edit Speaker Unit Page ..... 86
4.5.4 Parameters on Edit Optical Fiber Unit Page ..... 86
4.5.5 Edit Alarm Input/Output in an Area ..... 86
4.6 Remove Element from Area ..... 86
**Chapter 5 Person Management ..... 88**
5.1 Add Departments ..... 88
5.2 Basic Configuration Before Managing Persons ..... 90
5.3 Add Person ..... 91
5.3.1 Add a Single Person Manually ..... 92
5.3.2 Batch Add Persons by Template ..... 96
5.3.3 Import Domain Persons ..... 97
5.3.4 Import Persons from Device ..... 98
5.3.5 Operations Available on Person List ..... 100

5.4 Credentials Management ..... 103
5.4.1 Manage Credentials for a Single Person ..... 104
5.4.2 Import Profile Pictures ..... 109
5.4.3 Card Management ..... 110
5.5 Person Self-Registration ..... 117
5.5.1 Set Self-Registration Parameters ..... 118
5.5.2 Scan QR Code for Self-Registration ..... 120
5.5.3 Review Self-Registered Person Information ..... 121
5.6 Resigned Persons Management ..... 122
5.6.1 Add Resigned Persons ..... 123
5.6.2 Reinstate Persons ..... 124
5.6.3 Manage Resignation Types ..... 124
5.7 Position Management ..... 125
**Chapter 6 Vehicle Management ..... 126**
6.1 Manage Registered Vehicles ..... 126
6.1.1 Add a Registered Vehicle ..... 127
6.1.2 Batch Import Registered Vehicles ..... 129
6.2 Manage Vehicle Lists ..... 130
6.3 Manage Visitor Vehicles ..... 135
6.4 Manage Vehicles in Blocklist ..... 135
6.4.1 Add a Vehicle to Blocklist ..... 136
6.4.2 Batch Import Vehicles to Blocklist ..... 138
6.5 Customize Vehicle Information ..... 138
6.6 Configure Fuzzy Matching Rules for License Plate Search ..... 141
**Chapter 7 Management of Platform Accounts and Security ..... 143**
7.1 Add a Role ..... 143
7.2 User Management ..... 145
7.2.1 Manage Different Users via a User Group ..... 145

7.2.2 Add a Normal User ..... 146
7.2.3 Import Domain Users ..... 148
7.2.4 Import Normal Users via an Excel File ..... 148
7.2.5 Operations After Adding Users ..... 149
7.3 System Security Settings ..... 150
7.3.1 Set Basic Security Parameters ..... 150
7.3.2 Configure Security Questions ..... 152
7.3.3 Change Password of Current User ..... 152
7.3.4 Forgot Password ..... 154
7.4 Configure Permission Schedule ..... 156
**Chapter 8 System Configuration ..... 157**
8.1 Normal Settings ..... 157
8.1.1 Set User Preference ..... 157
8.1.2 Set Holiday ..... 159
8.1.3 Set Printer ..... 160
8.1.4 Set Card Template ..... 161
8.2 Calling Settings ..... 162
8.2.1 Add Call Recipients ..... 162
8.2.2 Add a Receiving Schedule Template ..... 162
8.2.3 Configure Call Parameters ..... 163
8.3 Network Settings ..... 164
8.3.1 Set NTP for Time Synchronization ..... 164
8.3.2 Azure Connection ..... 165
8.3.3 Set Active Directory ..... 166
8.3.4 Set Device Access Protocol ..... 169
8.3.5 Set Hik-Partner Pro Access ..... 169
8.3.6 Set WAN Access ..... 169
8.3.7 Set IP Address for Receiving Device Information ..... 170

8.3.8 Register Remote Site to Central System ..... 170
8.3.9 Allow for Remote Site Registration ..... 171
8.4 Storage Settings ..... 172
8.4.1 Set Storage on System Server ..... 172
8.4.2 Set Storage for Records ..... 173
8.5 Email Settings ..... 173
8.5.1 Configure Email Templates ..... 173
8.5.2 Configure Email Account ..... 174
8.6 Security Settings ..... 175
8.6.1 Set Transport Protocol ..... 175
8.6.2 Generate and Export Service Component Certificate ..... 179
8.6.3 Enable Export of Profile Pictures ..... 179
8.6.4 Enable Auto Update ..... 180
8.6.5 Set Database Password ..... 180
8.6.6 Watermark Settings ..... 180
8.7 Advanced Settings ..... 180
8.7.1 Configure System Hot Spare ..... 180
8.7.2 Diagnosis and Maintenance ..... 181
8.7.3 Reset Device Network Information ..... 182
8.8 Manage Workbenches ..... 182
8.9 Set Company Information ..... 183
**Chapter 9 Maintenance ..... 185**
9.1 Health Overview ..... 185
9.1.1 Real-Time Health Status Overview ..... 185
9.1.2 Real-Time Health Status Overview (Topology) ..... 188
9.1.3 Historical Health Data Overview ..... 193
9.2 Set Basic Maintenance Parameters ..... 196
9.2.1 Configure Scheduled Health Check ..... 196

9.2.2 Send Log Report Regularly ..... 197
9.2.3 Set Warning Threshold for Streaming Media Usage ..... 198
9.2.4 Set Network Timeout ..... 199
9.2.5 Set Auto-Check Frequency ..... 200
9.2.6 Set Topology Show Parameters ..... 201
9.3 Health Check ..... 201
9.3.1 Perform Manual Check ..... 201
9.3.2 Add Custom Pending Tasks ..... 205
9.4 Resource Status ..... 206
9.5 Log Search ..... 208
9.5.1 Search for Server Logs ..... 209
9.5.2 Search for Online/Offline Logs of Device ..... 209
9.5.3 Search for Logs Stored on Device ..... 210
9.5.4 Search for Online/Offline Logs of Resource ..... 211
9.5.5 Search for Recording Status of Resource ..... 212
9.5.6 Search for Call-Back Status of Resource ..... 216
9.5.7 Search for Maintenance Logs ..... 216
9.6 Service Manager ..... 217
9.7 Set System Data Backup ..... 218
9.8 Restore System Data ..... 219
9.9 Export Configuration Data ..... 220
9.10 Import Configuration Files ..... 221
**Chapter 10 Central Management ..... 224**
10.1 Add a Server ..... 224
10.2 Create and Edit Clusters ..... 226
10.3 Migrate Resources to Other Sub-Servers ..... 227
10.4 Take Over a Sub Server or a Standby Server ..... 227
10.5 Operation and Management Center ..... 228

**Chapter 11 Remote Site Management ..... 230**
11.1 Management of Remote Site Groups ..... 230
11.2 Enable Receiving Registration of Remote Sites ..... 231
11.3 Add a Remote Site ..... 231
11.4 Edit a Remote Site ..... 233
11.5 View Remote Site's Changes ..... 233
11.6 Review Information Changes Synchronized from Remote Sites ..... 234
**Chapter 12 Event and Alarm ..... 237**
12.1 Supported Events and Alarms ..... 238
12.2 Supported Linkage Actions ..... 241
12.3 Manage Event and Alarm ..... 245
12.3.1 Add Normal Event and Alarm ..... 245
12.3.2 Add Combined Alarm ..... 252
12.3.3 Add Generic Event ..... 257
12.3.4 Add User-Defined Event ..... 259
12.3.5 Add Text Warning Event ..... 260
12.4 Set Basic Event and Alarm Parameters ..... 262
12.4.1 Configure Receiving Schedule Template ..... 263
12.4.2 Custom Alarm Settings ..... 264
12.4.3 Configure Alarm Receiving Settings ..... 269
12.4.4 Send Event and Alarm Report Regularly ..... 270
12.5 Event and Alarm Search ..... 272
12.5.1 Event and Alarm Overview ..... 272
12.5.2 Search for Event and Alarm Logs ..... 273
12.5.3 View Device Application Events ..... 274
**Chapter 13 Third-Party Integration Settings ..... 276**
13.1 Integrate via Optimus ..... 276
13.2 Integrate via OpenAPI Gateway ..... 276

13.3 Set SIA Device Driver ..... 279
13.4 Integrate via SIA Gateway ..... 280
13.5 Set BACnet Device Driver ..... 282
13.6 Integrate via BACnet Gateway ..... 282
13.7 Integrate via Sur-Gard Gateway ..... 283
13.8 Data Interchange ..... 285
13.8.1 Synchronize Access Records to Third-Party Database ..... 285
13.8.2 Dump Access Records to Third-Party Database ..... 287
13.9 WhatsApp ..... 289
**Chapter 14 Video Management ..... 291**
14.1 Video Security ..... 291
14.1.1 Live View ..... 291
14.1.2 Live View Toolbar Applications ..... 298
14.1.3 Playback ..... 304
14.1.4 Customize Icons on Playback Window ..... 312
14.1.5 Set Video Parameters ..... 314
14.2 Picture Center ..... 316
14.2.1 Configure Picture Storage ..... 316
14.2.2 Configure Capture Schedule ..... 316
14.2.3 Search for Scheduled Captures ..... 316
14.2.4 Time-Lapse Photography ..... 317
14.2.5 Configure Scheduled Report ..... 317
14.3 Manage Face Picture Library ..... 318
14.3.1 Add Face Picture Library ..... 318
14.3.2 Add Persons to a Face Picture Library ..... 319
14.3.3 Import Persons or Profile Pictures ..... 319
14.3.4 Apply Face Picture Library to Device ..... 320
14.4 Intelligent Recognition ..... 321

14.4.1 Step 1. Add Task Schedule Template ..... 321
14.4.2 Step 2: Manage Face Picture Library ..... 322
14.4.3 Step 3. Add Intelligent Recognition Tasks ..... 322
14.4.4 Step 4. Apply Tasks to Devices ..... 327
14.5 AcuSeek Tuning Sample Group ..... 329
14.6 Video Application ..... 330
14.6.1 Configure Self-Learning Library ..... 330
14.6.2 Configure Visual Tracking ..... 330
14.6.3 Configure Person/Vehicle Arming ..... 331
14.6.4 Configure Panorama Tracking ..... 332
14.7 Video Overview ..... 335
**Chapter 15 Parking Management ..... 337**
15.1 Flow Chart of Parking Lot Management ..... 337
15.2 Flow Chart of Parking Fee Collection ..... 339
15.3 Flow Chart of Parking Guidance Configuration ..... 341
15.4 Manage Parking Lot ..... 342
15.4.1 Parking Lot Overview ..... 344
15.4.2 Add Parking Lot ..... 345
15.4.3 Add Entrance and Exit ..... 347
15.4.4 Add Lane ..... 348
15.4.5 Link Display Screen and Set Displayed Content ..... 354
15.4.6 Configure Entry & Exit Rules ..... 360
15.4.7 Configure Parking Fee Rules ..... 372
15.5 Methods for Parking Charges ..... 391
15.5.1 Top Up Parking Pass ..... 391
15.5.2 Pay in Toll Center ..... 395
15.6 Parking Guidance Configuration ..... 397
15.6.1 Add a Floor to the Parking Lot ..... 398

15.6.2 (Optional) Link Devices to the Floor ..... 400
15.6.3 (Optional) Configure a Map for the Floor ..... 402
15.6.4 Set Types for Parking Spaces on the Map ..... 405
15.6.5 Mark Devices on the Map ..... 408
15.6.6 Calibrate Parking Spaces Regularly ..... 412
15.6.7 Configure Parking Space Lights-out Time ..... 414
15.6.8 Parking Space Monitoring ..... 415
15.7 Record Search ..... 417
15.7.1 Search for Passing Vehicles Detected by Entrances & Exits ..... 417
15.7.2 Search for Parking Records ..... 419
15.7.3 Search for Parked Vehicles ..... 420
15.7.4 Search for Payment Records ..... 422
15.7.5 Search for Vehicle Top-Up and Refund Records ..... 423
15.7.6 Search for Transaction Records of Vehicle Owner Account ..... 423
15.7.7 Search for Work Records of Operators ..... 424
15.7.8 Search for Coupon Records ..... 424
15.8 Statistic and Report ..... 425
15.8.1 Export Operation Reports of Parking Lots ..... 425
15.8.2 Export Transaction Reports of Parking Lots ..... 430
15.8.3 Configure Scheduled Overtime Parking Reports ..... 431
15.9 Set Basic Parameters of Parking Management ..... 434
15.10 Audio Media Library Management ..... 437
15.11 Self-Service Vehicle Finding Client ..... 439
**Chapter 16 ANPR (Automatic Number Plate Recognition) ..... 440**
16.1 Search for Passing Vehicles Detected by Cameras and UVSSs ..... 440
16.2 Generate Vehicle Analysis Report ..... 442
16.3 Send Vehicle Analysis Reports Regularly ..... 445
**Chapter 17 On-Board Monitoring ..... 449**

17.1 Basic Settings ..... 450
17.1.1 Configure Basic Parameters ..... 450
17.1.2 Configure Route Parameters ..... 451
17.1.3 Configure Fuel Level Monitoring Parameters ..... 451
17.1.4 Configure Scheduled Reports ..... 452
17.2 Manage Drivers ..... 454
17.2.1 Add Drivers ..... 454
17.2.2 Add Drivers to a Driver Group ..... 457
17.2.3 Link Driver/Driver Group to a Vehicle ..... 457
17.3 Configure Driving Rules ..... 459
17.3.1 Configure Fence Rule ..... 459
17.3.2 Configure Deviation Rule ..... 460
17.3.3 Configure Rule Schedule Template ..... 462
17.4 Manage Stop & Route ..... 463
17.4.1 Step 1: Add Stops ..... 463
17.4.2 Step 2: Configure Driving Routes ..... 464
17.4.3 (Optional) Step 3: Configure Shift Schedules ..... 465
17.4.4 (Optional) Step 4: Add a Stop Event Rule ..... 466
17.5 Driving Monitoring ..... 467
17.6 Route Monitoring ..... 471
17.7 Search On-Board Monitoring Records ..... 474
17.7.1 Search for Vehicle Tracks ..... 474
17.7.2 Search for Driving Events ..... 475
17.7.3 Search for Routes ..... 476
17.7.4 Search for Fuel Level Monitoring Records ..... 478
17.8 Statistics and Reports ..... 478
17.9 On-Board Monitoring Overview ..... 486
**Chapter 18 Manage Smart Wall ..... 490**

18.1 Add Smart Wall Device ..... 490
18.2 Add Smart Wall ..... 491
18.3 Link Decoding Output with Window ..... 491
18.4 Display Alarms on Smart Wall ..... 492
18.5 Check Device Status ..... 496
**Chapter 19 Portable Enforcement Management ..... 498**
19.1 Before You Start ..... 498
19.1.1 Add Enforcement Officer ..... 498
19.1.2 Add Dock Station ..... 498
19.1.3 Add Portable Device ..... 498
19.1.4 Apply Person to Dock Station ..... 500
19.2 Basic Parameter Configuration ..... 503
19.3 Real-Time Monitoring ..... 504
19.4 How to Configure Group Intercom and its Application ..... 505
19.5 How to Save Files on the Dock Station to Evidence Center? ..... 506
19.6 How to Play Back Tracks? ..... 506
19.7 Search for Receiving Records ..... 507
19.7.1 Search for Receiving Records by Person ..... 508
19.7.2 Search for Receiving Records by Device ..... 508
**Chapter 20 Intelligent Analysis Report ..... 510**
20.1 Retail/Supermarket Scenario ..... 510
20.1.1 Add Store ..... 511
20.1.2 Configure Promotion Day ..... 515
20.1.3 View and Send Store Report ..... 516
20.1.4 View Store Intelligent Analysis Report ..... 521
20.1.5 View Store Report Dashboard ..... 527
20.2 Public Scenario ..... 528
20.2.1 Add Analysis Group ..... 530

20.2.2 Generate and View Analysis Report ..... 531
20.2.3 View Report Dashboard ..... 541
20.2.4 Send Analysis Report Regularly ..... 543
**Chapter 21 Traffic Incident Monitoring ..... 547**
**Chapter 22 Security Inspection Management ..... 549**
22.1 Flow Chart of Security Inspection ..... 549
22.2 Configure Security Inspection ..... 551
22.3 Add Security Inspection Channels to Area ..... 552
22.4 View Videos of Security Inspection ..... 552
22.5 Historical Data Search ..... 554
22.5.1 Search for Package Detection Records ..... 555
22.5.2 Search for Metal Detection Records ..... 556
22.5.3 Search for Absence Records ..... 556
22.6 Generate Package Detection Report ..... 557
22.7 Generate People Inspection Report ..... 557
**Chapter 23 Access Control Management ..... 559**
23.1 Flow Chart of Door Access Control ..... 560
23.2 Flow Chart of Floor Access Control ..... 562
23.3 Before You Start ..... 565
23.4 Assign Access Level to Persons ..... 565
23.4.1 Add Access Level ..... 565
23.4.2 Manually Assign Access Level ..... 567
23.4.3 Access Level Overview ..... 570
23.4.4 Set Access Schedule Template ..... 571
23.4.5 Set Holiday Group Schedule ..... 572
23.4.6 Regularly Apply Access Level Settings to Devices ..... 574
23.4.7 Clear Persons' Access Levels ..... 574
23.5 How to Open the Door by Your Smart Phone ..... 575

23.6 Real Time Monitoring ..... 581
23.7 Data Search ..... 585
23.8 Advanced Functions ..... 589
23.8.1 Add Remain Unlocked and Remain Locked Rule ..... 589
23.8.2 Configure First Person In ..... 589
23.8.3 Manage Multi-Factor Authentication ..... 590
23.8.4 Configure Multi-Door Interlocking ..... 591
23.8.5 Configure Anti-Passback ..... 592
23.8.6 Add a Batch Locking and Unlocking Group ..... 594
23.8.7 Add a Final Authentication Counting Group ..... 594
23.8.8 Configure Authentication Mode ..... 595
23.8.9 Apply Advertisement to Access Control Devices ..... 597
23.8.10 Add Audio Broadcast ..... 599
23.8.11 Add an Authentication Password ..... 600
23.8.12 Sync with Access Module ..... 601
23.9 Access Control Test ..... 602
**Chapter 24 Video Intercom Management ..... 606**
24.1 Flow Chart of Video Intercom ..... 606
24.2 Add Video Intercom Device ..... 608
24.3 Configure Device Parameters ..... 608
24.4 Button Settings ..... 610
24.4.1 Add Call Schedules for Door Stations ..... 610
24.4.2 Add Button Settings for Indoor Stations ..... 611
24.5 Link Resources with Indoor Stations ..... 611
24.5.1 Link Doorbell to Indoor Station ..... 611
24.5.2 Link Cameras to an Indoor Station ..... 612
24.5.3 Link Persons to Indoor Station ..... 613
24.6 Apply Data to Indoor Station ..... 613

24.6.1 Add and Apply a Notice ..... 613
24.6.2 Apply Software Package to Indoor Station ..... 614
24.7 Make and Receive Calls on Platform ..... 615
24.7.1 Add Call Schedule Template ..... 616
24.7.2 Add Call Recipients ..... 616
24.8 Apply Advertisements to Door Stations ..... 616
**Chapter 25 Attendance ..... 618**
25.1 Flow Chart of Time and Attendance ..... 619
25.2 Before You Start ..... 619
25.2.1 Add Devices, Departments, and Persons ..... 619
25.2.2 Add an Attendance Group ..... 620
25.2.3 Specify Attendance Check Points ..... 622
25.2.4 Add a Pay Code ..... 625
25.2.5 Edit a Fixed Code ..... 627
25.2.6 Add a Leave Rule ..... 628
25.2.7 Configure Storage Settings ..... 631
25.3 Check-In/Out via Mobile Client ..... 631
25.3.1 Step 1: Configure Function via Web Client ..... 631
25.3.2 Step 2: Check In/Out via Mobile Client ..... 633
25.3.3 Step 3: Handle Application via Web Client ..... 635
25.3.4 Step 4: Check Attendance Status via Mobile Client ..... 636
25.4 Approval Flow ..... 637
25.4.1 Step 1: Add Approval Role ..... 637
25.4.2 Step 2: Configure Approval Flow ..... 638
25.4.3 Step 3: Add Leave Rule ..... 638
25.4.4 Step 4: Employees Submit Applications ..... 639
25.4.5 Step 5: Reviewers Review Applications ..... 640
25.4.6 Step 6: Employees Check Application Status ..... 642

25.5 Configure Attendance Rules for Global / Department / Attendance Group ..... 643
25.5.1 Define Weekends ..... 643
25.5.2 Configure Attendance Calculation Rule ..... 643
25.5.3 Define Absence ..... 644
25.5.4 Add Holidays Requiring Attendance ..... 647
25.5.5 Calculation of Leaves ..... 648
25.5.6 Configure Overtime Parameters ..... 648
25.5.7 Configure Authentication Mode ..... 651
25.6 Shift Settings and Schedule ..... 651
25.6.1 Add Timetable ..... 651
25.6.2 Add Shift ..... 658
25.6.3 Manage Schedule ..... 658
25.7 Configure Calculation Mode of Attendance Results ..... 664
25.7.1 Manually Calculate Attendance Results ..... 664
25.7.2 Set Auto-Calculation Time of Attendance Results ..... 665
25.8 Attendance Records and Reports ..... 665
25.8.1 View Attendance Records ..... 665
25.8.2 Manage Attendance Reports ..... 667
25.9 Application Management for Admin ..... 672
25.9.1 Apply for a Leave / Check-In/Out Correction / Overtime ..... 672
25.9.2 Import Applications ..... 672
25.9.3 Review or Undo Applications ..... 673
25.10 Application Management for Employee ..... 673
25.10.1 Login via Web Client (Employee) ..... 673
25.10.2 Overview of Personal Attendance Data ..... 674
25.10.3 Submit and View Applications ..... 675
25.10.4 (Employee) Review or Undo Submitted Applications ..... 677
25.10.5 View and Export Attendance Records and Reports ..... 677

**Chapter 26 Visitor Management ..... 679**
26.1 Overall Process of Visitor Management ..... 679
26.2 Basic Configuration Guide ..... 681
26.2.1 Add a Visitor Group ..... 681
26.2.2 Add Access Level and Parking Lot Permission for Visitors ..... 682
26.2.3 Manually Apply Visitors' Access Level Settings to Visitor Terminals ..... 684
26.2.4 Set Review and Self-Service Reservation Parameters ..... 685
26.2.5 Set Self-Service Check-Out Point ..... 688
26.2.6 Add Visitor Receiving Template ..... 689
26.2.7 Add Visitor Pass Template ..... 690
26.2.8 Set Basic Parameters ..... 693
26.2.9 Manage Entry & Exit Rule for Visitors' Vehicles ..... 699
26.3 Visitor Reservation Guide ..... 700
26.3.1 Option 1: Administrator Makes Reservations for Visitors ..... 700
26.3.2 Option 2: Administrator Imports Visitor Reservation Information ..... 702
26.3.3 Option 3: Administrator Reviews Visitor Self-Service Reservations ..... 703
26.4 Visitor Check-In Guide ..... 704
26.4.1 Option 1: Check In a Reserved Visitor ..... 704
26.4.2 Option 2: Check In a Visitor Without Reservation ..... 705
26.5 Visitor Check-Out ..... 711
26.6 How to Set Up and Implement Self-Service Visit ..... 713
26.6.1 Step 1: Set Up Self-Service Reservations and Approval Workflow ..... 714
26.6.2 Step 2: Configure Default Visitor Access Levels ..... 715
26.6.3 Step 3: Configure Auto Check-Out Points ..... 715
26.6.4 Step 4: Visitor QR Code Reservation ..... 716
26.6.5 Step 5: Administrator Review & Approval ..... 716
26.6.6 Step 6: Visitor Receives QR Code for Entry ..... 716
26.6.7 Step 7: Visitor Auto Check-Out Upon Exit ..... 716

26.7 How to Use Watch List to Monitor Special Visitors ..... 716
26.7.1 Step 1: Add Entity Type ..... 717
26.7.2 Step 2: Set Match Method ..... 718
26.7.3 Step 3: Add an Entity to the Watch List ..... 719
26.7.4 Step 4: Import Existing Visitors to the Watch List ..... 719
26.8 How to Manage Visitor Information and Access Records ..... 721
26.8.1 View Visitor Information ..... 721
26.8.2 Check Visitor Access Records ..... 721
**Chapter 27 Emergency Mustering ..... 723**
27.1 Add Emergency Solution ..... 723
27.1.1 Select Areas ..... 723
27.1.2 Add Card Readers ..... 723
27.1.3 Add Doors Remaining Unlocked in Emergency ..... 724
27.1.4 Add Emergency Counting Groups ..... 724
27.1.5 Release Emergency Mustering Notifications ..... 725
27.1.6 Trigger Emergency Automatically ..... 726
27.2 Start a Roll Call ..... 726
**Chapter 28 Map Management ..... 728**
28.1 Configure Map ..... 728
28.1.1 Select and Set GIS or E-map for an Area ..... 729
28.1.2 Add Hot Spot to Map ..... 731
28.1.3 Add Hot Region to Map ..... 738
28.1.4 Add Tag to Map ..... 739
28.1.5 Add Resource Group to Map ..... 740
28.1.6 Add Parking Lot to Map ..... 742
28.1.7 Add Event and Alarm to Map ..... 742
28.1.8 Add Remote Site to GIS Map ..... 743
28.1.9 Add Geographic Area to Map ..... 743

28.2 Monitor on Map ..... 744
28.2.1 View and Operate Hot Spot ..... 744
28.2.2 Preview Hot Region ..... 747
28.2.3 Preview Resource Group ..... 748
28.2.4 View Remote Site Alarm ..... 749
28.2.5 Operate Resources from Geographic Area ..... 750
**Chapter 29 Augmented Reality (AR) Monitoring ..... 751**
29.1 Add Scene ..... 751
29.2 Add Scene to Map ..... 753
**Chapter 30 Alarm Detection ..... 754**
30.1 Alarm Detection Overview ..... 754
30.2 Flow Chart of Alarm Detection ..... 755
30.3 Add Security Control Partitions (Areas) from Device ..... 757
30.4 Add User of Security Control Device ..... 759
30.5 Configure Arming Schedule Template ..... 760
**Chapter 31 Evidence Management ..... 762**
31.1 Basic Settings ..... 762
31.1.1 Set Basic Parameters ..... 762
31.1.2 Set Storage Parameters ..... 762
31.2 Manage Files ..... 763
31.2.1 Upload a Local File ..... 763
31.2.2 Upload Files from Device ..... 764
31.2.3 Save Files in Other Modules ..... 765
31.2.4 View and Edit Files ..... 765
31.2.5 Share Files ..... 767
31.3 Manage Cases ..... 768
31.3.1 Add a Case ..... 768
31.3.2 View and Edit Cases ..... 769

31.3.3 Share Cases ..... 771
31.4 Link Files to Cases ..... 771
31.5 Manage Operation Records ..... 773
**Chapter 32 Patrol Management ..... 774**
32.1 Patrol Overview ..... 774
32.2 Flow Chart of Patrol Management ..... 775
32.3 Basic Configurations for Patrol Management ..... 777
32.3.1 Add Exception Types for Patrol Management ..... 778
32.3.2 Set Parameters for Patrol Management ..... 778
32.4 Add Patrol Points ..... 780
32.5 Add Patrol Person Group ..... 781
32.6 Add Patrol Schedule Template ..... 783
32.7 Add Patrol Route ..... 785
32.8 Real-Time Patrol Monitoring ..... 788
32.9 Search for Patrol-Related Event Records ..... 789
32.10 Check Patrol Statistics ..... 791
**Chapter 33 Commercial Display Management ..... 793**
33.1 Commercial Display Overview ..... 793
33.2 Flow Chart of Digital Signage Management ..... 794
33.3 Content ..... 796
33.3.1 Quickly Release Content ..... 796
33.3.2 Manage Template Library ..... 798
33.3.3 Create My Program ..... 800
33.4 Schedule ..... 803
33.4.1 Create an Ordinary Schedule ..... 803
33.4.2 Create a Cut-In Schedule ..... 805
33.4.3 View Release Records ..... 807
33.5 Review ..... 807

33.6 Material ..... 808
33.6.1 Upload Materials ..... 808
33.6.2 Manage Materials in My Favorites ..... 811
33.7 Statistics and Reports ..... 811
33.8 Basic Settings ..... 814
33.8.1 Set Weather Web Manufacturer ..... 814
33.8.2 Set Material Storage Location ..... 814
33.8.3 Add a Display Wall for Digital Signage Terminal ..... 814
33.9 Device Control ..... 816
33.9.1 Control a Device ..... 816
33.9.2 Create a Combined Control Command for Multiple Devices ..... 818
33.10 Application Management ..... 818
33.10.1 Add Applications ..... 818
33.10.2 Manage Applications on Devices ..... 820
**Chapter 34 Broadcast Management ..... 821**
34.1 Set Basic Settings for Broadcast ..... 821
34.2 Group Speaker Units ..... 822
34.3 Manage Media Files ..... 823
34.4 Configure Live Broadcast ..... 824
34.5 Search for Live Broadcast Records ..... 825
34.6 Add a Scheduled Broadcast Task ..... 826
34.7 Add a Linked Broadcast Task ..... 827
**Chapter 35 Skin-Surface Temperature Screening ..... 830**
35.1 Temperature Screening Configuration ..... 830
35.1.1 Group Temperature Screening Points ..... 830
35.1.2 Configure Temperature Screening Parameters ..... 831
35.2 Real-Time Skin-Surface Temperature Monitoring ..... 832
35.3 Search History Temperature Screening Data ..... 833

35.4 Registration ..... 834
35.4.1 Register Person Information ..... 834
35.4.2 Customize Registration Template ..... 836
35.4.3 View Registered Person Information ..... 836
35.5 Search for Temperature Screening Records ..... 837
35.6 Generate Skin-Surface Temperature Analysis Report ..... 838
35.7 Configure the Scheduled Report of Screening ..... 840
**Appendix A. Symbol Conventions ..... 843**
**Appendix B. Legal Information ..... 844**

# Chapter 1 Introduction

The platform is developed for the management of security system and features flexibility, scalability high reliability, and powerful functions.

The platform provides features including central management, information sharing, convenient connection, and multi-service cooperation. It is capable of adding devices for management, live view, video storage and playback, face picture comparison, access control, time and attendance, alarm linkage, and so on.

**Note**

The modules on the platform vary with the License you purchased. For detailed information, contact our technical support.

The complete platform contains the following components. You can install the components according to actual needs.

| Component | Introduction |
|---|---|
| System Management Service (SYS) | • Provides the unified authentication service for connecting with the clients and servers.<br>• Provides the management for the users, roles, permissions, devices, and services.<br>• Provides the configuration APIs for monitoring and management modules. |
| Streaming Service (Optional) | Provides forwarding and distributing the audio and video data of live view. |

The following table shows the provided clients for accessing or managing the platform.

| Client | Introduction |
|---|---|
| Control Client | Control Client is a Desktop client software which provides multiple operating functionalities, including live view, PTZ control, video playback and download, alarm receiving, log search, and so on. |
| Web Client | Web Client is a B/S client for managing system. It provides multiple functionalities, including device management, area management, recording schedule settings, event configuration, user management, and so on. |
| Mobile Client | Mobile Client is the software designed for getting access to the platform via Wi-Fi, 4G, and 5 G networks with mobile device. It fulfills the functions of the devices connected to the platform, such as live view, remote playback, PTZ control, and so on. |

# Chapter 2 Getting Started

The following content describes the tasks typically involved in setting a working system.

On the lower left of the log-in page, click **Scan QR Code for Help**, and then scan the QR Code by your smart phone or click **Go** to view the how-to videos of the platform.

Before accessing the SYS, finish the following tasks.

- Set the transfer protocol. For details, refer to ***Set Transport Protocol*** .
- Set the SYS's IP address before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

## 2.1 Installation and Deployment

You can select standalone deployment or cluster deployment.

The Stream Server and the Database Server cannot be installed on the same PC with the System Management Service.

Double-click (HikCentral Professional) to open the Install Wizard.

Note that during the installation process, the following programs will also be installed:

- Microsoft Visual C++ 2015 Redistributable
- vcredist2008×64.exe
- vcredist2008×86.exe
- vcredist2010×86.exe
- vcredist2013×64.exe
- vcredist2013×86.exe
- vcredist2015×64.exe
- vcredist2015×86.exe

### 2.1.1 Recommended Running Environment for Server

**Operating System**

- Microsoft® Windows Server 2025
- Microsoft® Windows Server 2022
- Microsoft® Windows Server 2019 (64-bit)
- Microsoft® Windows Server 2016 (64-bit)
- Microsoft® Windows 11 (64-bit) (including version 24H2)
- Microsoft® Windows 10 (64-bit)

**CPU**

For Standalone: Intel® Core™ i5-8500 and later

For Cluster: Intel® Xeon® Silver 4309Y *2

**Memory**

For Standalone: 8 GB+

For Cluster: 64 GB+

**Web Browser**

Firefox® 140+, Google Chrome® 138+, Microsoft® Edge 138+, and Safari® 16.6+.

**HDD**

SATA 7200 RPM Enterprise Class disk with 650 GB storage capacity. When running the SYS, there should be at least 1 GB free space.

**Note**

Upgrading from V1.x to V2.x requires double available disk spaces than usual.

## 2.1.2 Standalone Deployment

Two installation methods are available for building the standalone system. System Management Service, Control Client, Stream Server, and Database Server can be installed.

Double-click the installation program to open the installation wizard.

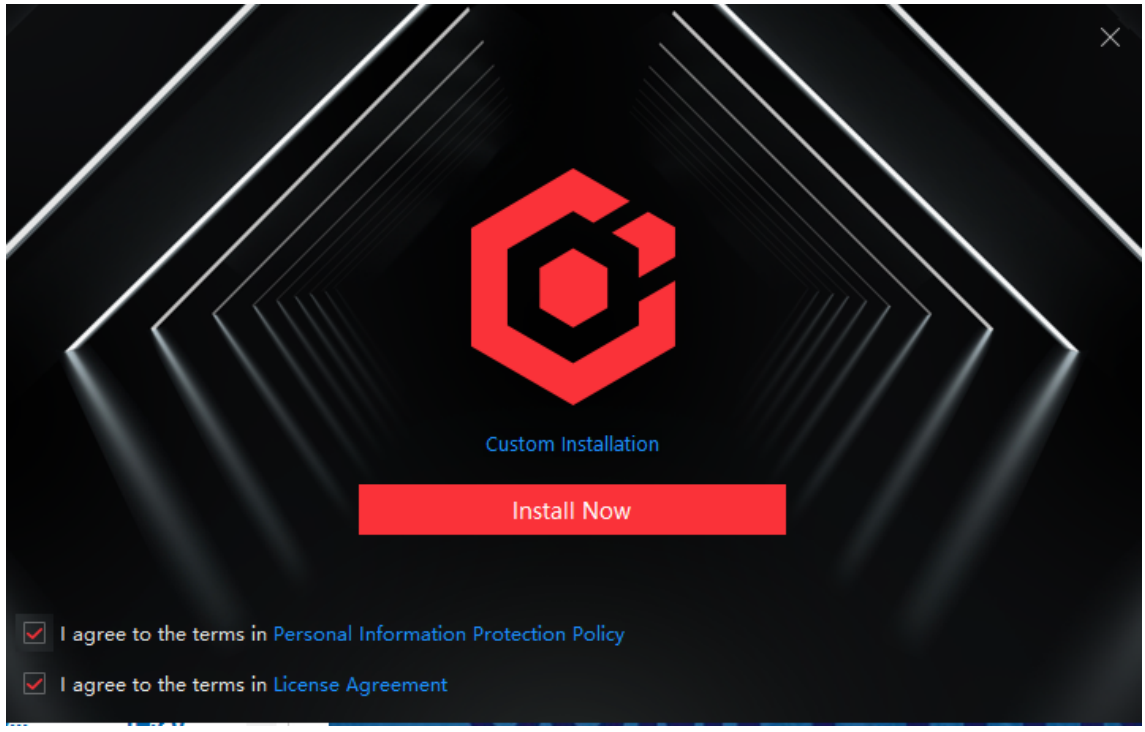



**Figure 2-1 Install Window**

**Install Now**

Start standalone installation, and the System Management Service and Control Client will be installed by default.

**Custom Installation**

Select this to show the installation options. Select **Standalone Installation**, check the installation option(s).

**Installation Mode**

**Normal**

The System Management Service and/or the Control Client is installed without any hot spare.

**Local/Remote Mirroring Hot Spare**

Select **Mirror Hot Spare** to build a double-server system. Local mirroring hot spare means the two servers are deployed in the same physical location or data center, while remote mirroring hot spare involves maintaining a real-time mirrored copy of data at a geographically distant location (e.g., a different city or data center). There will be two HikCentral servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real-time. When the host server fails, the spare server will take over the host server without interruption.

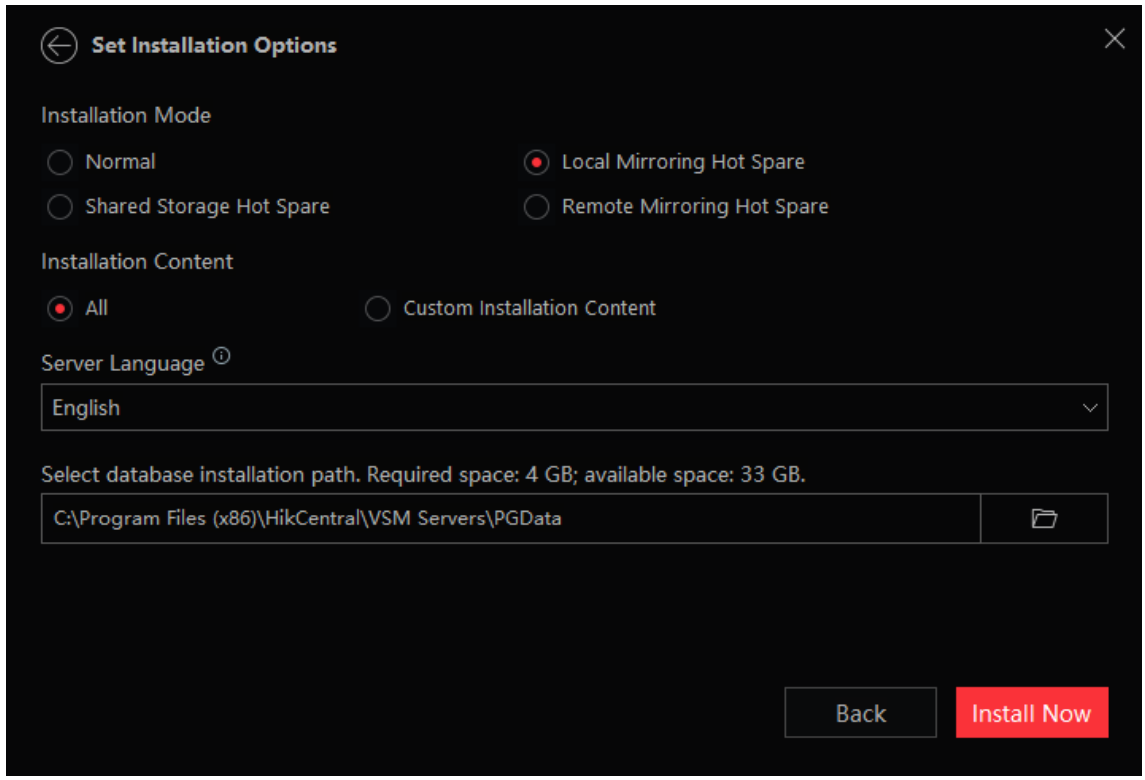



**Figure 2-2 Local Mirror Hot Spare**

**Note**

For building the hot spare system, contact our technical support engineer.

**Shared Storage Hot Spare**

Multiple servers share a disk of one server. All servers can load and find the shared disk on their own system, and can store data in the shared disk. You should select the path of the shared disk.

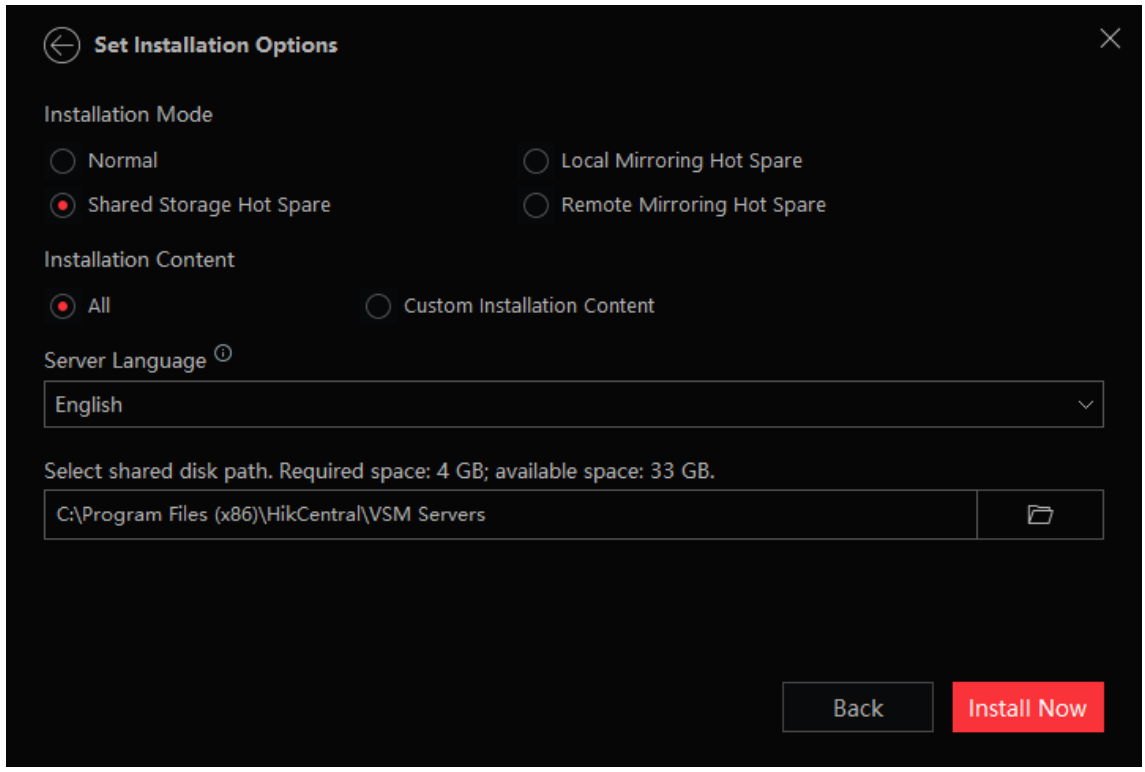



**Figure 2-3 Shared Storage Hot Spare**

**Installation Content**

**All**

The full version of the system will be installed.

**Custom Installation Content**

Select applications you need to install.

**Server Language**

Select the same language with your system.

### 2.1.3 Cluster Deployment

In Cluster Installation mode, the System Management Service, Control Client, and Database Server can be deployed.

Double click the installation program and select **Custom Installation**.

#### Install Database Server

The database server should be installed first, and it cannot be deployed on the same PC with the System Management Service or Control Client.

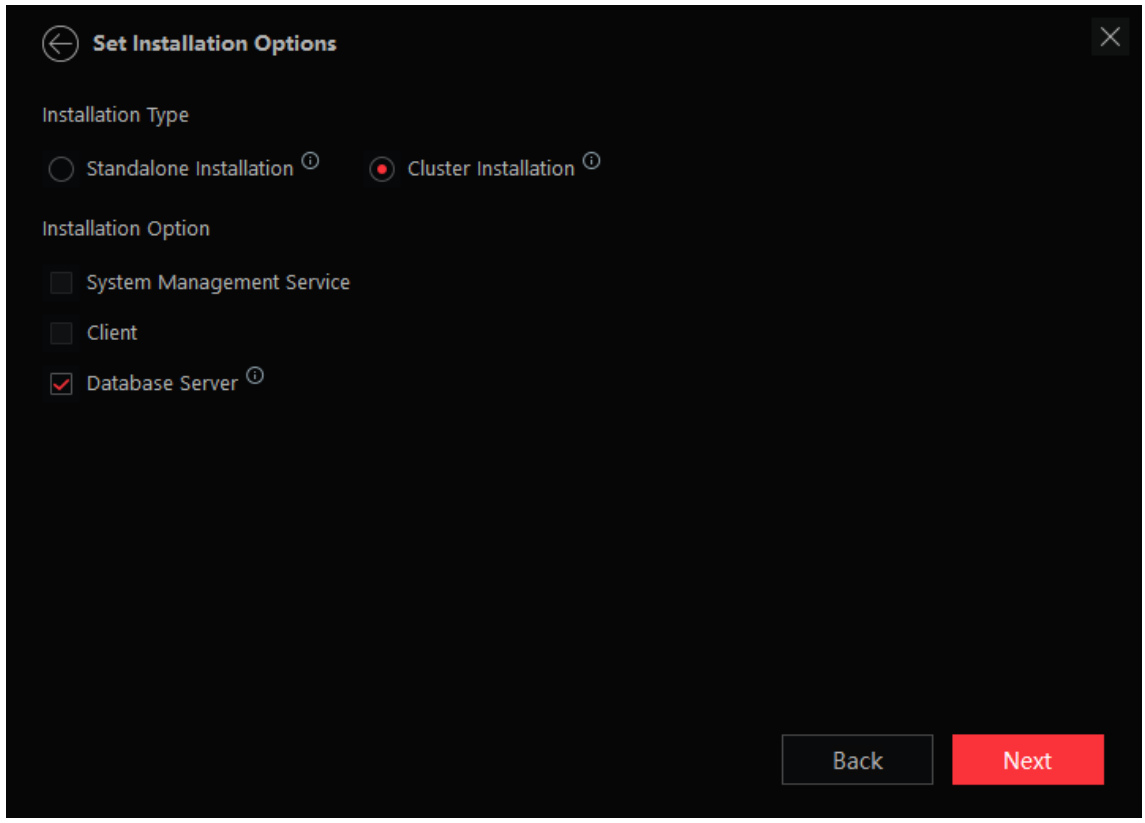



**Figure 2-4 Install Database Server**

**Server Language**

Select the same language with your system.

**Custom Service Data Saving Directory**

Select the saving path for different modules.

**Note**

It is recommended to restart after installation to ensure that the database server runs under optimal conditions.

## Install Main Server

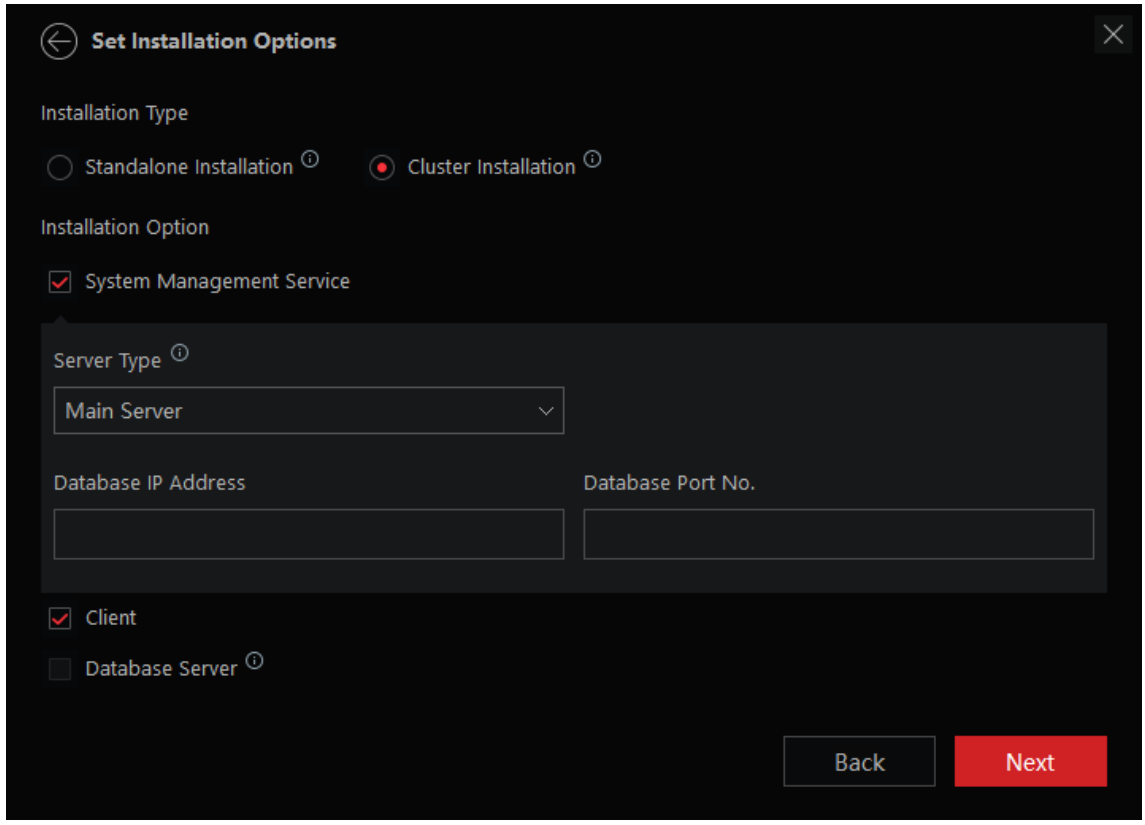



**Figure 2-5 Install Main Server**

The database server's IP address and port number should be entered here so that the main server can connect to the database server.

The Control Client can be installed together.

**Local/Remote Mirroring Hot Spare**

Select **Mirror Hot Spare** to build a double-server system. Local mirroring hot spare means the two servers are deployed in the same physical location or data center, while remote mirroring hot spare involves maintaining a real-time mirrored copy of data at a geographically distant location (e.g., a different city or data center). There will be two HikCentral servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real-time. When the host server fails, the spare server will take over the host server without interruption.

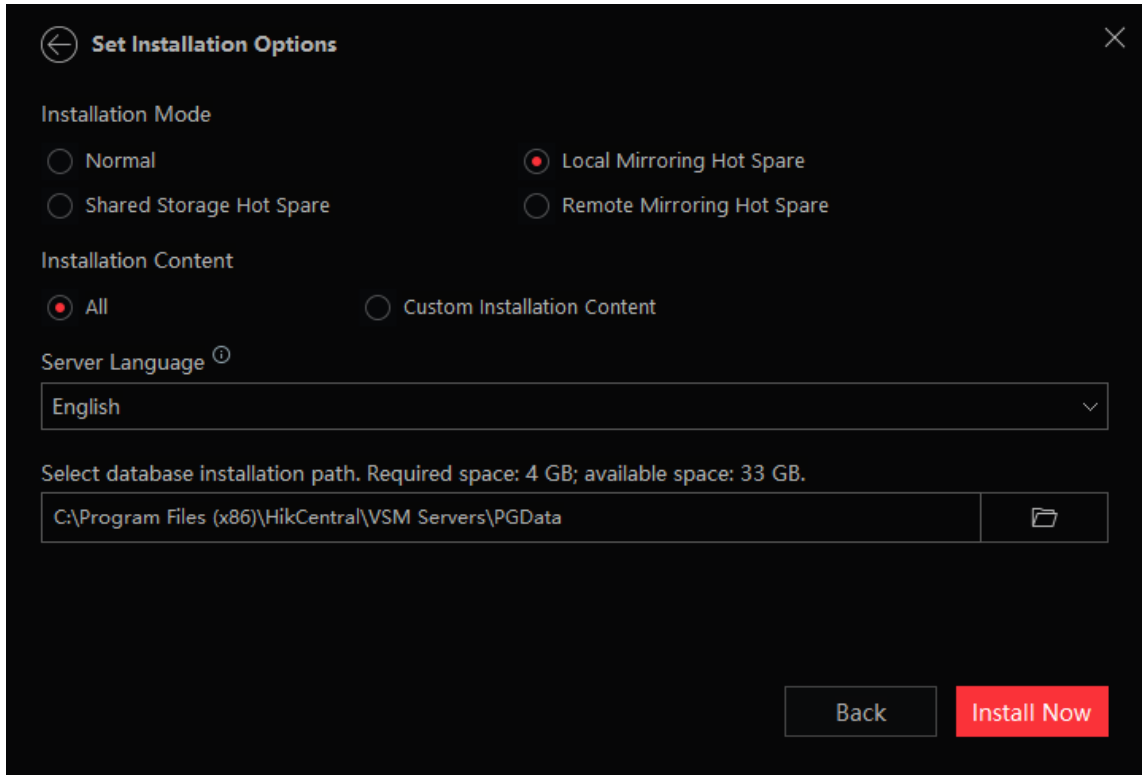



**Figure 2-6 Local Mirror Hot Spare**

**Note**

For building the hot spare system, contact our technical support engineer.

### Install Sub Server

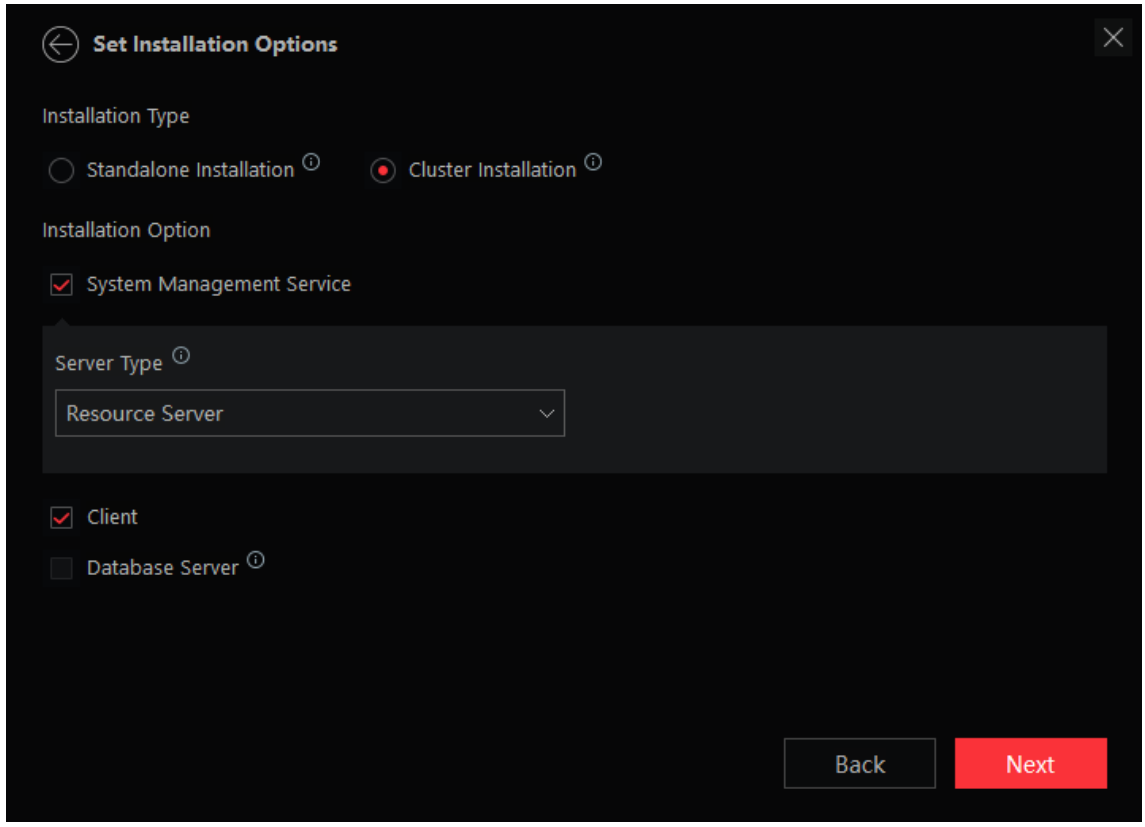



**Figure 2-7 Install Sub Server**

**Change Server Type**: If the cluster system has been installed, you can change a resource server into the main server by double-clicking the icon of installation program and selecting **Set Server Type to Main Server**, or change the main server into a resource server by double-clicking the icon of installation program and selecting **Set Server Type to Resource Server**.

## 2.2 Login

You can access and configure the platform via web browser directly, without installing any client on your computer.

**Steps**

**Note**

- If failed password attempt of current user is detected, you are required to input the verification code. The failed password attempts from current client, other client, and other address will all require the verification code.
- The failed password attempt and verification code attempt from current client, other client (e.g., Control Client), and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts detected.
- The account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from current client, other clients (e.g., Control Client), and other addresses will all be accumulated. When the account is frozen after accumulated failed password attempts, you can still try login on another PC.
- The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required strength, you will be asked to change your password.
- If your password is expired, you will be asked to change your password when login.

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key to open the login page.

   **Example**

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   - The Web Client transmits data via the HTTPS, using our self-developed HTTPS certificate, which is not issued by the Certificate Authority. So that a risk prompt will show when you opening the Web Client. To avoid the prompt, you can apply for a certificate from the Certificate Authority.
   - The login session of the Web Client will expire and a prompt with countdown will appear after the configured time period in which there is no action. For setting the time period, refer to ***Set Basic Security Parameters*** .
2. (For Administrator to login Web Client) On the login page, select the **Management** tab.
3. For first-time login for admin user:
   1) Enter a password and confirm the password for the admin user in the pop-up Create Password window, click **Next**, and select a method for password reset verification.

      **Email**

      Click **Verification Code → Next** and set the email address for receiving the password reset verification code.

      **Security Question**

      Click **Security Question → Next** , select security question(s) from the drop-down lists, and enter your answers accordingly.
   2) Click **Finish**.

**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.

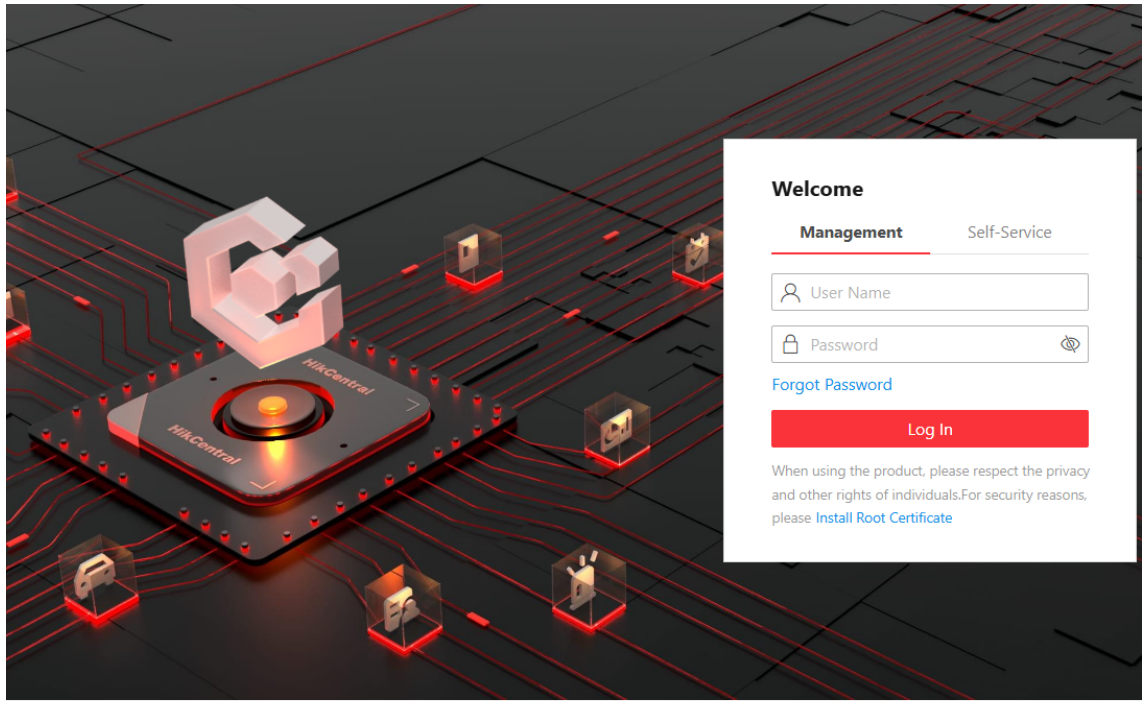
After you logged in, the Site Name window opens and you can set the site name for the current system as you want. You can also set it in **System → Normal → User Preference** . See ***Set User Preference*** for details.

4. For first-time login for normal users, or users whose passwords were reset:
   1) Enter the user name and password, and click **Log In**.
      You can contact the Administrator for the user name and initial password.
      The Change Password window shows.
   2) Set a new password and confirm the password.
   The Home page of the Web Client will show.
5. For all users except employees and first-time users, enter the user name and password, and click **Log In**.
   If the **Require Email Verification When Login** function is enabled for a user, a Double Authentications window will pop up. Users can send a verification code via the platform to their email, and then enter the code. Then the Home page of the Web Client will show.

## 2.3 Download Mobile Client

On the login page of Web Client, you can scan the QR code at the bottom to download the Mobile Client, or install it in the APP Store.

Scan the corresponding QR code on the Login page with your mobile terminal to download the Mobile Client.




Android iOS

**Figure 2-8 QR Code for Downloading Mobile Client**

## 2.4 Home Page Overview

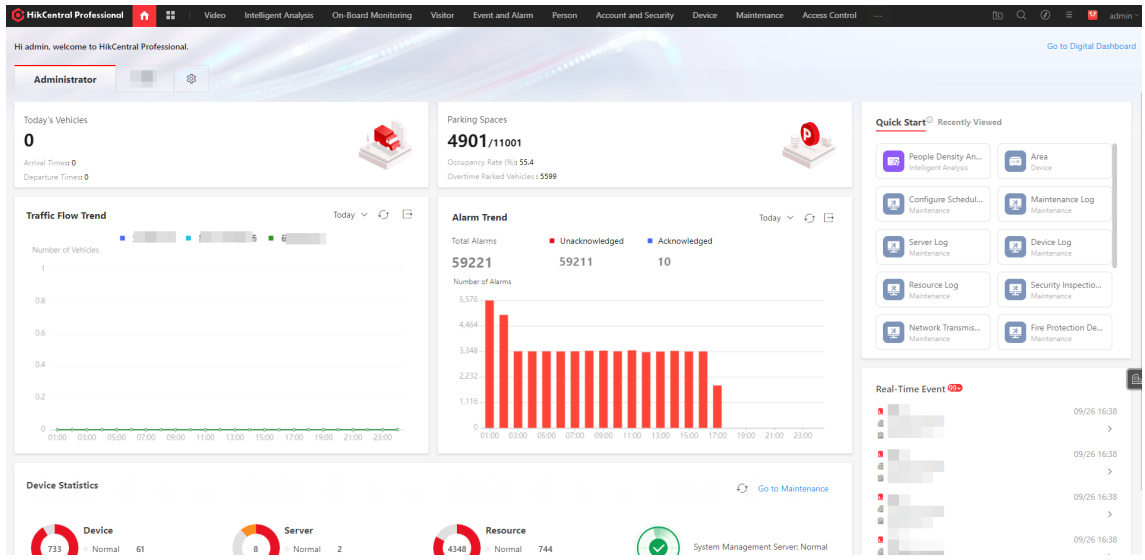



**Figure 2-9 Home Page Overview**

**Note**

The supported features and parameters are subject to the applications you installed.

**Table 2-1 Top Navigation Bar**

| Module | Description |
|---|---|
| Navigation Icon | The navigation bar shows the available functions determined by the Licenses you purchased.<br>On the top left, you can select and favorite frequently used or important modules to the navigation bar on the top for convenient access. |
| Download Center | You can view and manage all of the downloading and downloaded tasks on the Web Client. |
| Search Module | You can search for a specific function module and view the recently viewed pages. |
| Wizard | Wizards guides you through the management and applications of different modules. |
| Maintenance and Management | **License** |

| Module | Description |
| --- | --- |
| | You can view the License details, activate, upgrade, and deactivate the License if needed.<br>For details, refer to ***License Management*** .<br>**Back Up and Restore System Data**<br>You can manually back up the data in the system, or configure a schedule to run the backup task regularly. You can select different storage locations to suit your need.<br>When an exception occurs, you can restore the database if you have backed up the database.<br>For details, refer to ***Set System Data Backup*** and ***Restore System Data*** .<br>**Data Migration**<br>Only available on the Server. If you have used applications on the iVMS-4200, you can get configuration files of these applications (including configurations of devices, persons, events, and access levels) and import the files to HikCentral Professional via the Web Client for quickly configuring the corresponding applications on HikCentral Professional.<br>**Export Configuration Data**<br>You can export and save configuration data to your local PC.<br>For details, refer to ***Export Configuration Data*** .<br>**Download Web Control**<br>Click **Web Control** to start downloading the web control, or click to view its details and download it.<br>**Download Installation Package**<br>Download the installation package of the Control Client.<br>**Switch Language**<br>Click the language to select a new one to switch the system language.<br>**About**<br>Check the version information of the Web Client.<br>View the License Agreement and Open-Source License Agreement. |
| Application Market  | View the current capacity of the platform.<br>Display or hide applications on the Home page. |

| Module | Description |
|---|---|
| | On the application market page, install/uninstall applications, or repair/update installed applications. |
| Change Password | See ***Change the password of the current user*** . |
| Logout | Click the account name and select **Log Out** to quit from the system and go back to the login page. |

## Workbench / Digital Dashboard

**Workbench**

You can configure the available workbenches (including the preset workbench) and customize personal workbench by adding the frequently used components.

You can check the default and the added workbenches to display on the Home page for convenient use.

**Digital Dashboard**

Click **Go to Digital Dashboard** to view statistical information about digital campus overview, security control and management, persons, and vehicles.

### 2.4.1 Application Market

The application market supports installing, repairing, updating, enabling, or disabling applications according to your actual needs.

Click  on the top right.

## The Purchased Page

On this page, if there are purchased applications to install, a prompt will show on the top and you can install these applications.
This page displays the details of your purchased licenses and all installed and free-charged applications. You can disable or enable the applications.

## Applications

You can search for applications on the top, install/update/repair/uninstall applications, and download auxiliary tools.

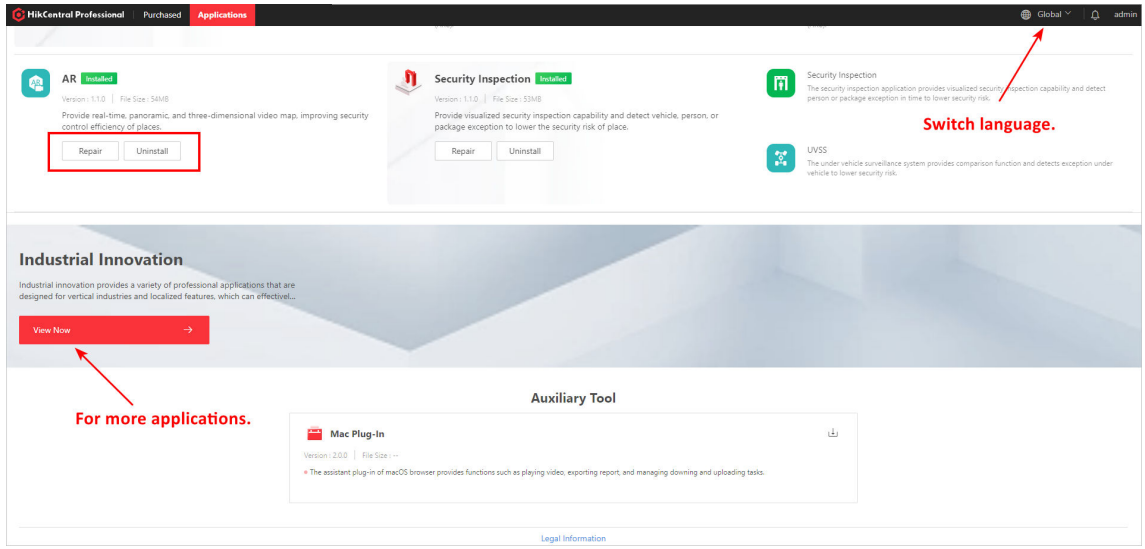



**Figure 2-10 Application Market**

**Note**

- The applications may vary by the countries or regions. You can click on the top right to select your location. Generally, the platform can get your country or region according to your IP address. When your PC disconnect from the network, you can select the country or region manually.
- For clients running in the LAN, the applications downloading will fail. You can go to the ***official Web Site*** to download the applications you need.

## 2.4.2 Customize Preset Workbench

As an administrator, you can link users with the default preset workbench. Also, you can customize preset workbenches.

**Note**

Make sure you have logged in to the Client by the administrator account.

You can customize a preset workbench by going to one of the two following entries.

- Click to enter the Home page. Then click to expand the workbench configuration pane. In the personal workbench area, click **Preset Workbench**.
- On the top left, select → **Basic Management** → **System** . Select **Workbench Management** on the left.

**Note**

- You can filter the preset workbenches by conditions, such as workbench name, linked users, and unlinked users.
- You can hover the cursor on the preset workbench, click **Preview** to preview the preset workbench.

### Configure Default Preset Workbench

Hover the cursor on the default preset workbench, including Administrator, Time and Attendance, Visitor Management, click , and click + on the left to display different components on the workbench.

**Note**

The default preset workbench name and remark cannot be edited.

### Add Preset Workbench

1. Click **Add Workbench** in the upper-right corner.
2. Click to edit the workbench name. Also, you can select an existing workbench as the template from the Copy From drop-down list, link users with the workbench, and add remark.
3. Click **OK**
4. Add displayed components of the workbench on the left.
5. Click **Save**. The added preset workbench will be displayed in the Preset Workbench pane on the Home page.

## 2.4.3 Customize Personal Workbench

You can customize personal workbench by adding the frequently used components for overview and quick access to modules, including person, time and attendance, security control and management, and vehicle.

1. On the Home page, click .
2. In the personal workbench area, click **Preset Workbench** on the top right to enter the Create Personal Workbench page.
3. Click to edit the workbench name and (if needed) select an existing workbench as the template from the Copy From drop-down list.
4. Click + on the right side of the component.
5. Drag in the lower right corner of a single component or set the display ratio (e.g., 100%, 60%, or 50%) in the top right corner to adjust the display size of the component.
6. Click **Save**. The added personal workbench will be displayed in the Personal Workbench pane on the Home page.

### 2.4.4 View Digital Dashboard

The platform provides visualized statistics about the digital campus information, including overview, persons, vehicles, and security control and management.

Click to enter the Home page. On the upper-right corner, click **Go to Digital Dashboard** to enter the Digital Campus page.

**Note**

- Click to select the time period (today, last 7 days, or last 30 days) to display the statistics.
- Click to refresh the real-time statistics.

## Overview

- On the left, you can view today's person statistics, access trend, and vehicle parking trend of parking lots.
- On the right, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), and device statistics, and you can set cameras auto-switch.




**Figure 2-11 Digital Campus Overview**

## Person

- On the left, you can view the total number of persons (including employees and visitors), today's person employee entry trend, and today's visitor entry trend.
- On the right, you can view the historical employee entry trend and historical visitor entry trend.

### Vehicle

- On the left, you can view the vehicle statistics, internal and external vehicle passing trend, and vehicle parking trend of parking lots.
- On the right, you can view the parking space statistics, parking space occupancy trend, and parking duration distribution.

### Security

- On the left, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), top 5 events, and top 5 areas with alarms.
- In the middle, you can select to view the live view of events.
- On the right, you can view the device statistics and device status.

## 2.5 License Management

After installing HikCentral Professional, you have a temporary License for a specified number of devices and limited functions. To ensure the proper use of HikCentral Professional, you can activate the SYS to access more functions and manage more devices. If you do not want to activate the SYS now, you can skip this chapter and activate the system later. You can also view license details and set SSP expiration prompt.

Two types of License are available for HikCentral Professional:

- **Base:** You need to purchase at least one basic License to activate the HikCentral Professional.
- **Expansion:** If you want to increase the capability of your system, you can purchase an expanded License to get additional features.

**Note**

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

On the top, click **Maintenance and Management → License Details** to open the License Details pane.

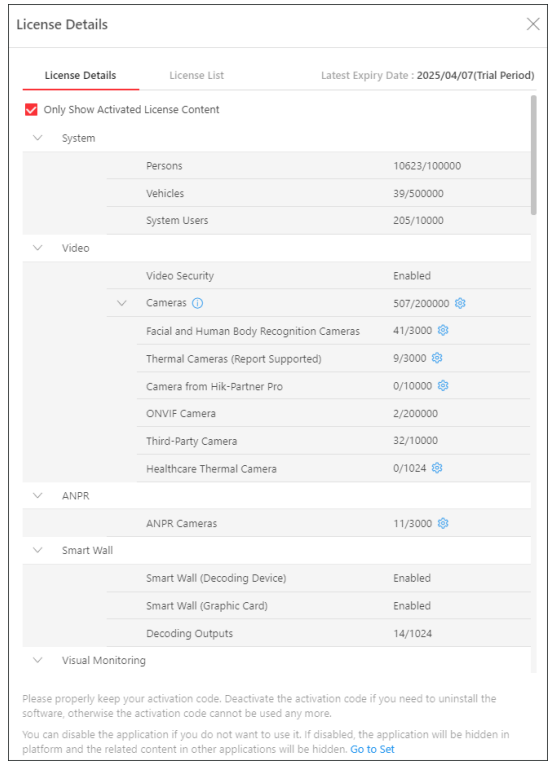



**Figure 2-12 License Details Page**

## View License Details

You can check the authorization details of the License you purchased and view the number of manageable devices and functions of your platform. If the License is not activated, you can also view the trial period.

1. Click › beside **Cameras** to show the number of facial and human body recognition cameras / thermal cameras (report supported) / ONVIF cameras / cameras from Hik-Partner Pro, and click ⚙ to select the added cameras as these types of cameras respectively.

   **Note**

   - Configuration of ONVIF cameras is not supported.
   - If you do not configure the facial and human body recognition camera / thermal camera, these cameras' functions (face recognition, plate recognition, and temperature report) cannot be performed normally in the platform.

2. Click **License List** to check all the activated License(s) of your platform and click an activation code to view the related authorization details.

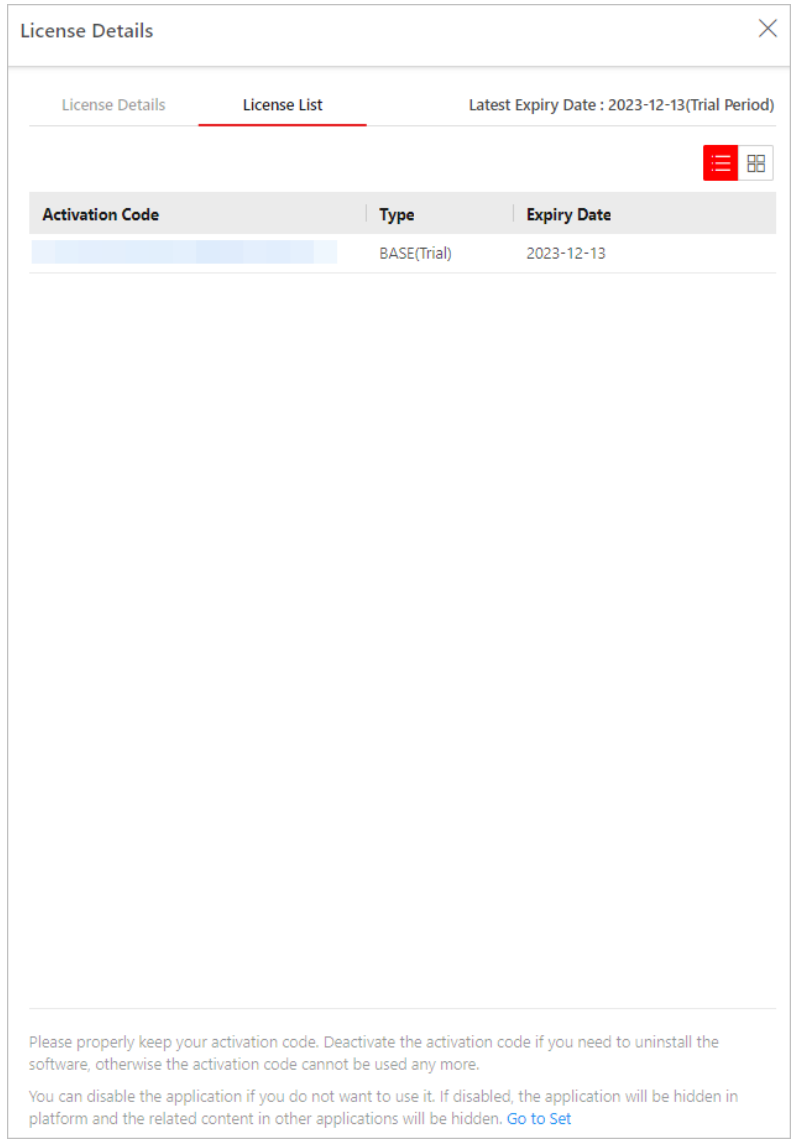



**Figure 2-13 License List Page**

## Set SSP Expiration Prompt

SSP (Software Service Program) refers to the platform's maintenance service, which has an expire date and needs to be upgraded before expiration. You can set SSP expiration prompt on the platform. After that, when the SSP is going to expire, you can receive an email reminding the expiration every day during the configured period.

1. Click ⚙ beside **Software Maintenance Service** to enter the SSP Expiration Prompt Settings pane.
2. Set the **Overdue Reminder** switch to ON.
3. Set the days when you will receive the prompt email before expiration.

**Note**

- You should enter an integer between 1 to 365.
- By default, the platform will send a prompt email 30 days before expiration.

4. Click **Add User** to add user(s) who can receive upgrade prompt.

**Note**

- You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
- Up to 64 recipients can be added.
- You can click × to delete the added user(s).

5. Click **Add Email** to add email address(es).

**Note**

You can add email of both the platform user(s) and other user(s). The platform will send expiration prompt to the added email address(es).

6. Click **Save**.

### 2.5.1 Activate License

If the SYS server to be activated can properly connect to the Internet, you can activate the SYS server in online mode. Otherwise, you can activate the License in offline mode.

On the Home page, click **Activate** to open the Activate License panel.

#### Activate License Online

Click **Online Activation**.

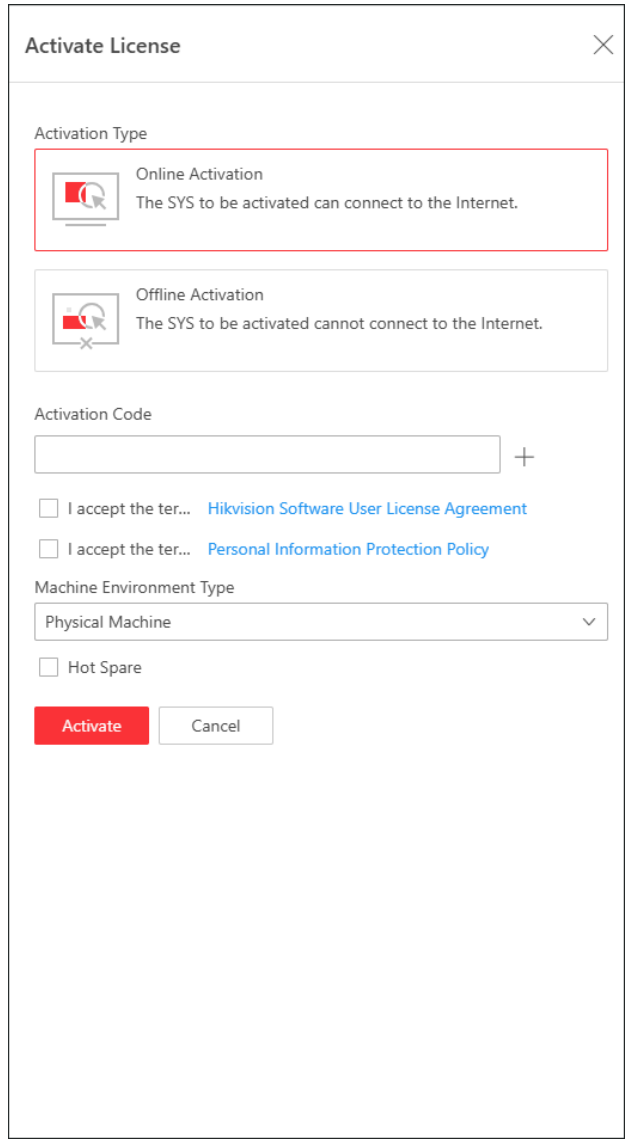



**Figure 2-14 Activate License in Online Mode**

Enter the activation code received when you purchased your License.
Select the machine environment type. If you select the AWS or Azure as the machine environment type, the pStor server, Streaming Server, and other external servers cannot access the platform. And the Rose hot spare system is also not supported.

**Physical Machine (Default)**

A physical computer that contains hardware specifications and is used for running the SYS. If the hardware changed, the License will be invalid, and the SYS may not run normally.

**AWS (Amazon® Web Services)**

A virtual machine that provides the cloud computing services for running the SYS.

**Azure (Microsoft® Azure)**

A virtual machine that provides the cloud computing services for running the SYS.

If you need to build a hot spare system, check the **Hot Spare**. For how to build the hot spare system, please contact our technical support engineers. You must select Hot Spare mode when you install the system.

After you activated the License, the email settings pane will appear. You need to enter an email address for the admin user. This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

Set the email server parameters. See details in ***Configure Email Account*** .

## Activate License Offline

Click **Offline Activation**.

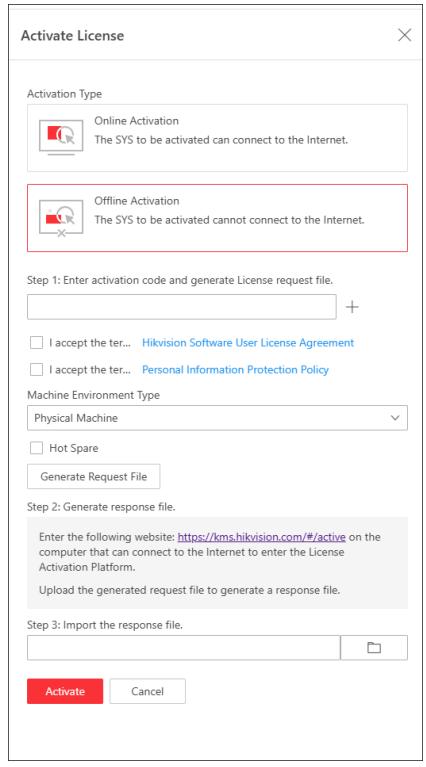



**Figure 2-15 Activate License in Offline Mode**

Enter the activation code received when you purchased your License.

Select the machine environment type. See machine environment type description in ***Activate License Online*** .

If you need to build a hot spare system, check the **Hot Spare**. For how to build the hot spare system, please contact our technical support engineers. You must select Hot Spare mode when you install the system.

Click **Generate Request File**. A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

Copy the request file to the computer that can connect to the Internet.
On the computer which can connect to the Internet, enter the website: ***https://kms.hikvision.com/#/active*** .
Click and then select the downloaded request file.

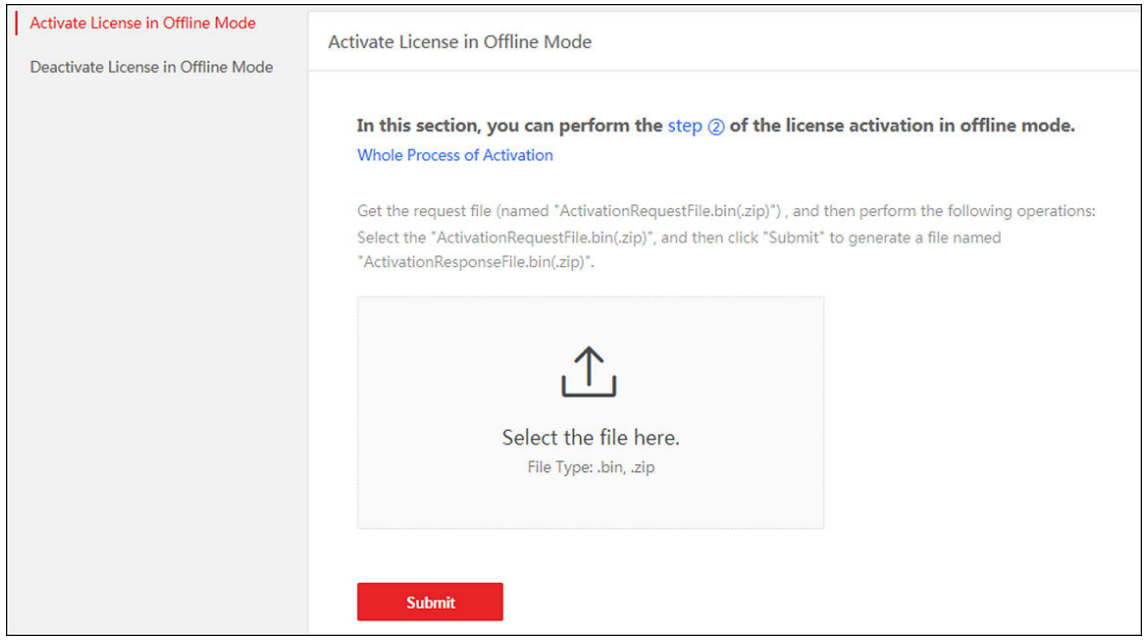



**Figure 2-16 Select Request File**

After submitting the request file, a respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
In the Activate License in Offline Mode panel, click to select the downloaded respond file.
After you activated the License, the email settings pane will appear. Enter an email address for the admin user. This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

## 2.5.2 Update License

As your project grows, you may need to increase the connectable number of resources (e.g., devices) for your HikCentral Professional. If the SYS to be updated can properly connect to the Internet, you can update the License in online mode. Otherwise, you can update the system in offline mode.

**Note**

Contact your dealer or our sales team to purchase a License for additional features.

On the top, move the cursor to **Maintenance and Management**.

Click **Update License** to open the Update License pane.

## Update License Online

Click **Online Update**, and enter the activation code received when you purchase your License. Before updating, the terms of the license agreement and the information protection policy should be accepted.

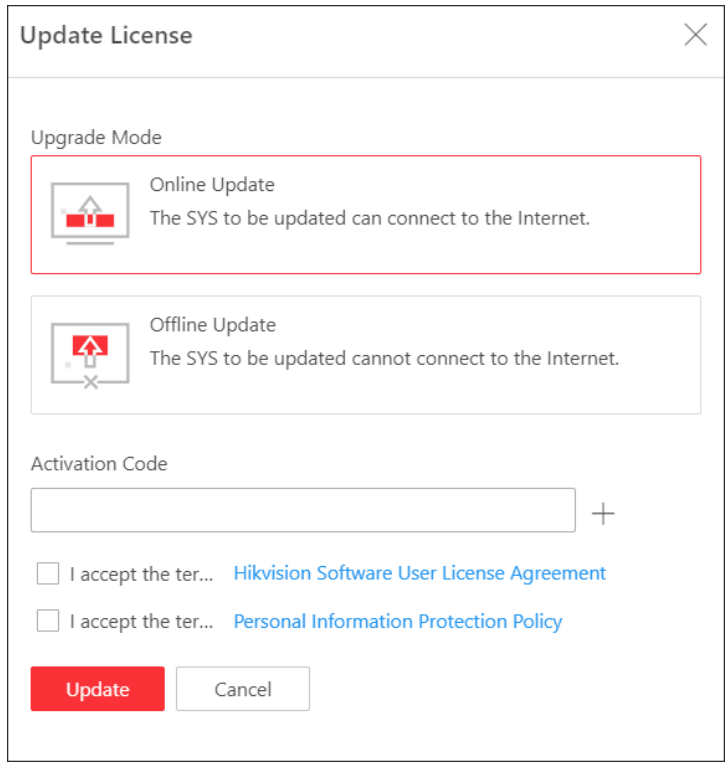



**Figure 2-17 Update License in Online Mode**

## Update License Offline

Click **Offline Update**.

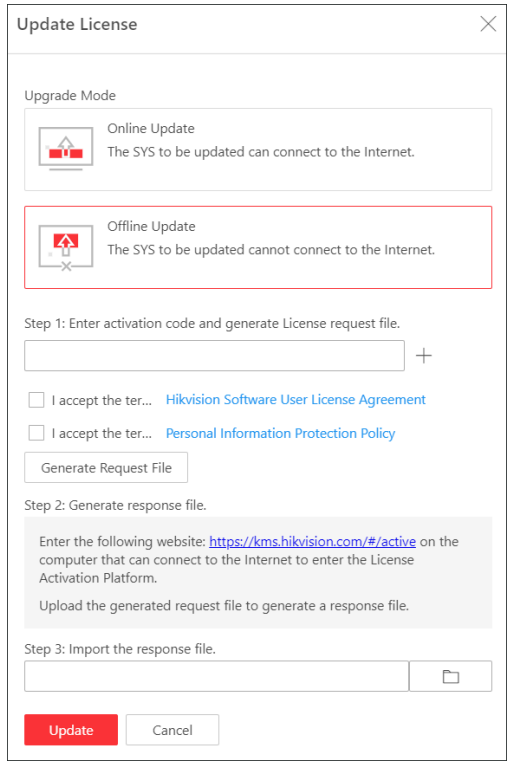



**Figure 2-18 Update License in Offline Mode**

Enter the activation code of your additional License, and accept the terms of the license agreement and the information protection policy.

Click **Generate Request File**, and a request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

Copy the request file to the computer connected to the Internet.

On the computer connected to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .

Click and then select the downloaded request file.

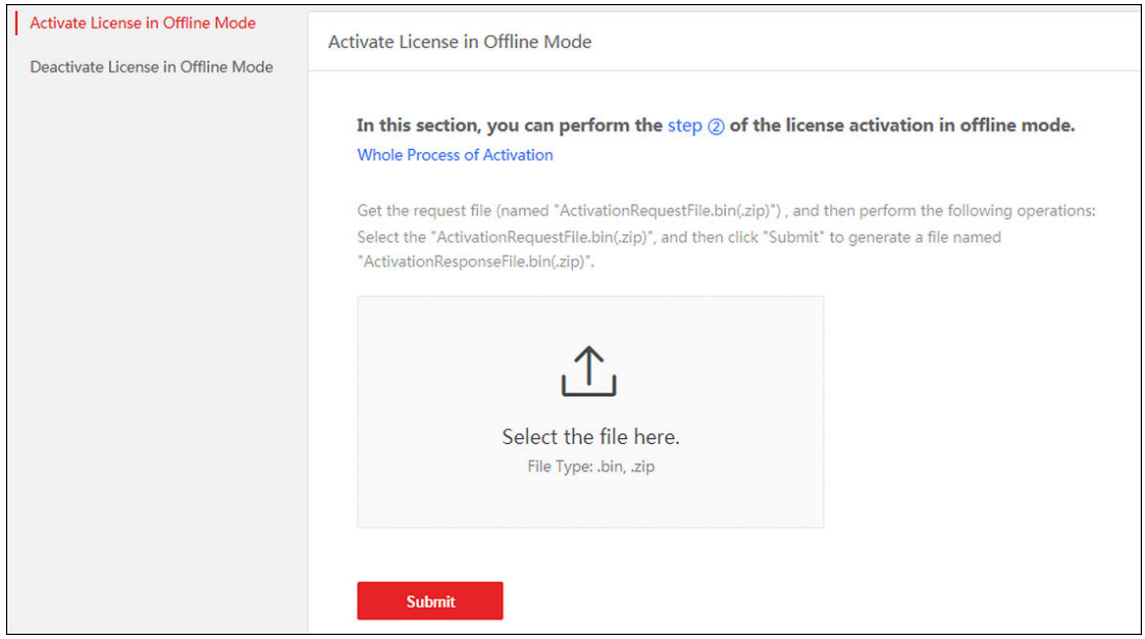



**Figure 2-19 Select Request File**

After submitting the request file, a respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).

Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.

In the offline update panel, click to select the downloaded respond file, and then update the License.

### 2.5.3 Deactivate License

If you want to run the SYS on another PC or server, you should deactivate the SYS first and then activate it again. If the computer or server on which the SYS running can properly connect to the Internet, you can deactivate the License in online mode. Otherwise, you can deactivate the License in offline mode.

On the top, move the cursor to **Maintenance and Management**.

Click **Deactivate License** to open the Deactivate License panel.

#### Deactivate License Online

Click **Online Deactivation**.

Check the activation code(s) to be deactivated and click **Deactivate**.

#### Deactivate License Offline

Click **Offline Deactivation**.

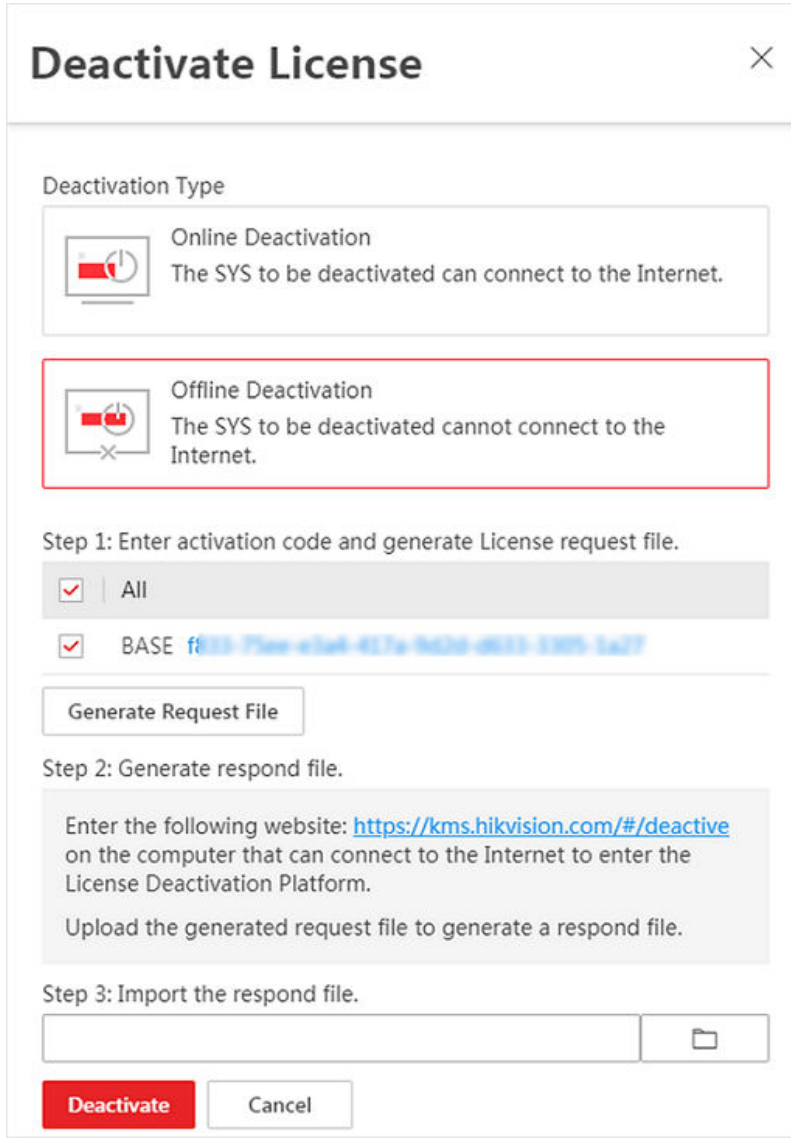



**Figure 2-20 Deactivate License in Offline Mode**

Check the activation code(s) to be deactivated.

Click **Generate Request File**. After the request file is generated, the selected activation code(s) will be unavailable. A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

Copy the request file to the computer connected to the Internet.

On the computer connected to the Internet, enter the website: ***https://kms.hikvision.com/#/deactive*** .

Click and select the downloaded request file.

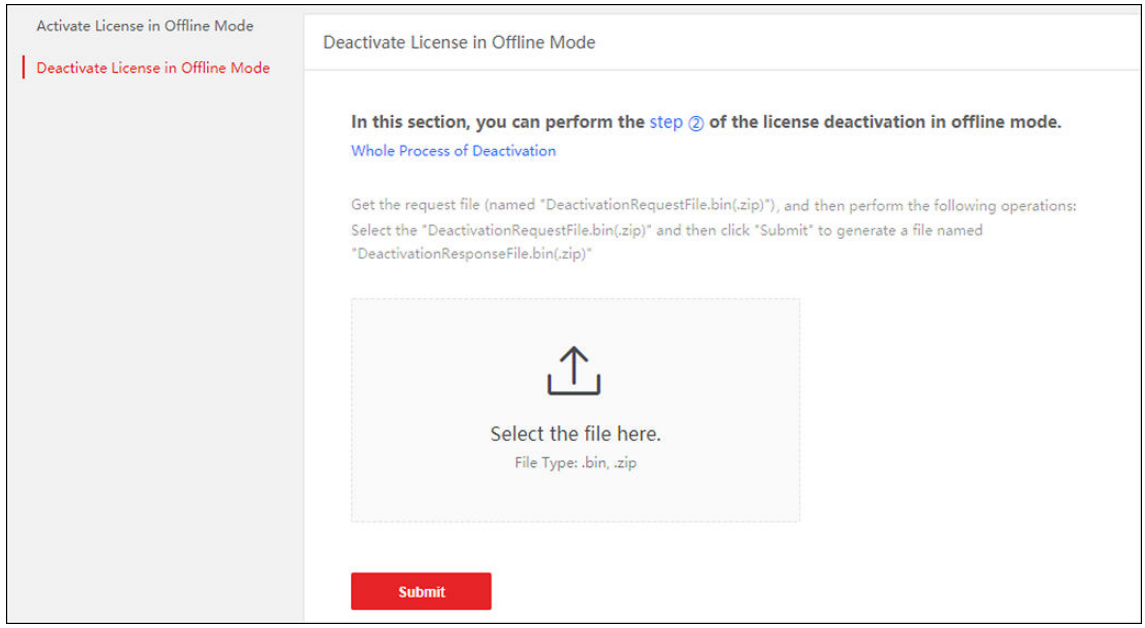



**Figure 2-21 Select Request File**

After submitting the request file, a respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).

Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.

In the Offline Deactivation pane, click to select the downloaded respond file and then deactivate the License.

# Chapter 3 Device and Server Management

Go to → **Basic Management → Device → Device and Server** .

## 3.1 Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the platform via network.
- To add devices via ISUP or ONVIF, you need to go to → **Basic Management → System → Network → Device Access Protocol** , and enable **Allow ISUP Registration** or check **Access via ONVIF Protocol**.
- For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC.

  You can also go to the top navigation bar, and click **Maintenance and Management → Web Control** to start downloading the web control, or click to view its details and download it.

## 3.2 Add Device(s)

This chapter introduces how to add online devices, add device manually, and batch import devices and explains parameters on Add Device pages.

### 3.2.1 Adding Modes Supported by Different Devices

To add devices via Hikvision Private Protocol / Hikvision ISUP Protocol in cluster mode, the protocol is shown as **Hikvision Private Protocol (Distributed) / Hikvision ISUP Protocol (Distributed)**, and you should select a device server.

#### Add Online Devices

Application scenario: the devices are on the same network as the Web Client.

1. In the Online Device area, select a network type.

   **Server Network**

   As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

   **Local Network**

The detected online devices in the same local subnet with the Web Client will be listed in the Online Device area.

2. In the Online Device area, select **Hikvision Private Protocol /Hikvision ISUP Protocol /ONVIF Protocol** to filter the detected online devices.
3. In the Online Device area, select the active device(s) to be added, and click **Add to Device List** to open the Add Online Device window.
4. Set basic information and time zone.

Supported device types are as follows.

- Encoding Device
- Access Control Device
- Elevator Control Device
- Video Intercom Device
- Visitor Terminal
- On-Board Device
- Guidance Terminal
- Security Control Device
- Certain Models of Parking Lot Screen
- Portable Device
- Digital Signage Terminal
- LED Controller
- BACnet Device
- Decoding Device
- IP Speaker
- Security Inspection Device
- Network Transmission Devices

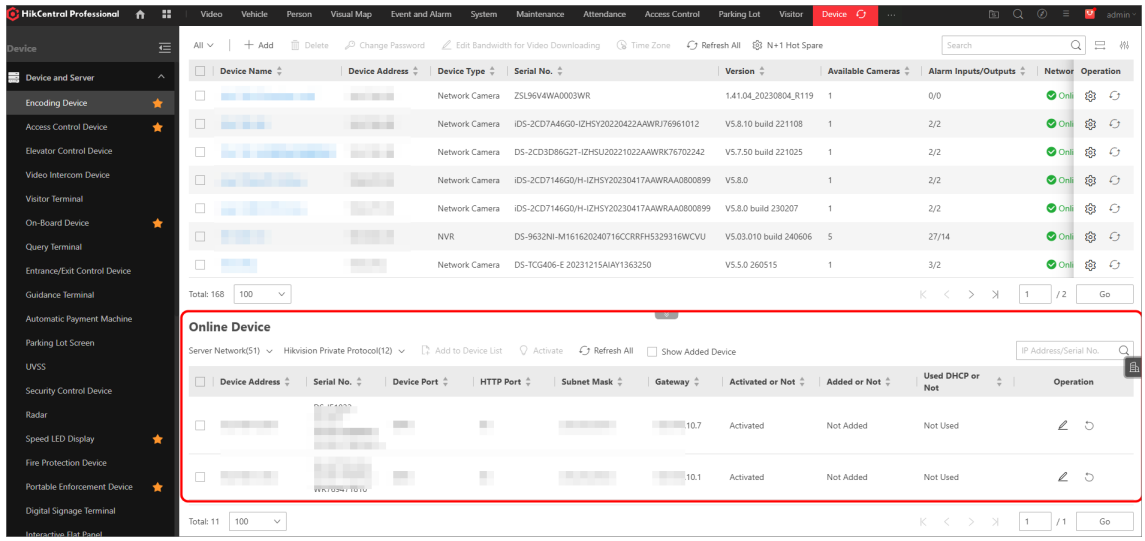



**Figure 3-1 Online Device**

## Add Devices Manually

On the left, select the type of device, and then click **Add** on the top.

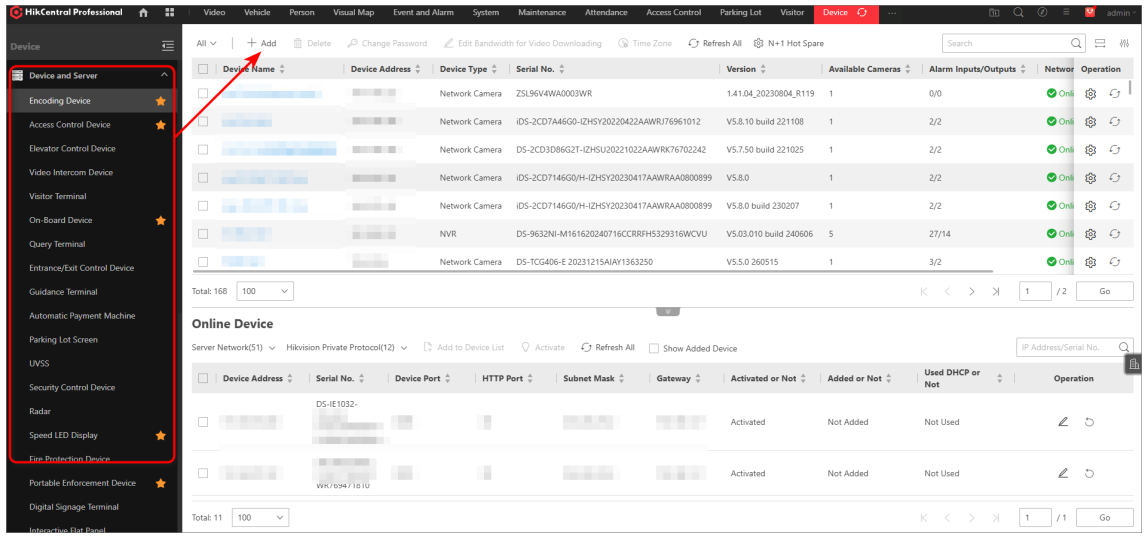



**Figure 3-2 Entry for Adding Device**

**Table 3-1 Add Devices Manually**

| Adding Mode | Scenario | Description | Supported Device Types |
|---|---|---|---|
| Add device by IP address / domain | When you know the IP address or domain name of a device, you can add it to the platform by specifying the IP address (or domain name), user name, password, etc. | Select **Hikvision Private Protocol / ONVIF Protocol / Dahua Private Protocol / Axis SDK Protocol / Hanwha SDK Protocol** as the Access Protocol, and select **IP Address/ Domain**.<br>In the Cluster mode, you should select a device server if you select **Hikvision Private Protocol**. | • Encoding Device<br>• Access Control Device<br>• Elevator Control Device<br>• Video Intercom Device<br>• Visitor Terminal<br>• Entrance/Exit Control Device<br>• Guidance Terminal<br>• Parking Lot Screen<br>• Under Vehicle Surveillance System (UVSS)<br>• Security Control Device |

| Adding Mode | Scenario | Description | Supported Device Types |
|---|---|---|---|
| | | | • Fire Protection Device<br>• Dock Station<br>• Digital Signage Terminal<br>• LED Controller<br>• Modbus Device<br>• Smart Wall<br>• Security Inspection Device<br>• Network Transmission Devices<br>• Smart Wall Device |
| Add devices by IP segment | When multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters. | Select **Hikvision Private Protocol / ONVIF Protocol** / **Dahua Private Protocol** / **Axis SDK Protocol** / **Hanwha SDK Protocol** as the Access Protocol, and select **IP Segment** as the adding mode. | • Encoding Device<br>• Access Control Device<br>• Elevator Control Device<br>• Visitor Terminal<br>• Guidance Terminal<br>• Security Control Device<br>• Fire Protection Device<br>• Dock Station<br>• Digital Signage Terminal<br>• LED Controller<br>• Smart Wall Device |
| Add devices by port segment | When multiple devices to be added have the same IP address, user name, password, and have different port numbers within a range, you can add devices by specifying the port segment and | Select **Hikvision Private Protocol / ONVIF Protocol** / **Dahua Private Protocol** / **Axis SDK Protocol** / **Hanwha SDK Protocol** as the Access Protocol, and | • Encoding Device<br>• Guidance Terminal<br>• Security Control Device<br>• Dock Station<br>• Smart Wall Device |

| Adding Mode | Scenario | Description | Supported Device Types |
|---|---|---|---|
| | some other related parameters. | select **IP Segment** as the adding mode. | |
| Add device by Hik-Connect DDNS | You can add devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. | Make sure you have enabled Hik-Connect service for devices to be added on the remote configuration page of the device.<br>Select **Hikvision Private Protocol** as the Access Protocol, and select **Hik-Connect DDNS** as the adding mode.<br>**Note**<br>The Hik-Connect DDNS Server Address is ***https://open.ezvizlife.com*** by default. | • Encoding Device<br>• Security Control Device |
| Add device by device ID | For the devices supporting ISUP, you can add them by specifying a predefined device ID, key, etc. | Select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID** as the adding mode. | • Encoding Device<br>• Access Control Device<br>• On-Board Device<br>• Query Terminal<br>• Security Control Device<br>• Speed LED Display<br>• Fire Protection Device<br>• Portable Device<br>• Portable Code Scanner<br>• IP Speaker<br>• Security Inspection Device<br>• LED Controller |

| Adding Mode | Scenario | Description | Supported Device Types |
|---|---|---|---|
| Add devices by device ID segment | If you need to add multiple devices which have no fixed IP addresses and support ISUP to the platform, you can add them at a time after configuring device ID segment for the devices | Select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID Segment** as the adding mode. | • Encoding Device<br>• Access Control Device<br>• On-Board Device<br>• Security Control Device<br>• Speed LED Display<br>• Fire Protection Device<br>• Portable Device |
| Add devices from sites on Hik-Partner Pro | If you have configured parameters for the site on Hik- Partner Pro accessing the platform, you can add devices from the site on Hik-Partner Pro to the platform. | To use the Hik-Partner Pro service, you need to purchase a license.<br>Select **Hik-Partner Pro Protocol** as the access protocol. | • Encoding Device<br>• Security Control Device |
| Add devices by Modbus protocol | You can add devices to the platform via Modbus protocol, and the parameters you need to configure include IP address, device name, device port number, etc. | Select **Modbus Protocol** as the Access Protocol, and set the required information. | Security Control Device |
| Add devices by SIA protocol | When the device supports the SIA protocol, you can add it to the system via the SIA protocol and then configure zones of the device. | Select **SIA Protocol** as the Access Protocol, and set the required information. | Security Control Device |
| Add devices by auto registration on device | If you have configured the platform's IP address for the device by a web browser, you can add devices by | Select **Add by Auto Registration** or click **Auto Registration**, and set the required information. | • Digital Signage Terminal<br>• Interactive Flat Panel |

| Adding Mode | Scenario | Description | Supported Device Types |
|---|---|---|---|
| | Auto Registration on Device. | | |
| Add devices by authentication code | You can add the device which supports OTAP/ISUP by Authentication Code. The authentication code is used for the terminal to register on the platform by OTAP/ISUP. | Click **Auto Registration → Add by Configuring General Authentication Code on Platform** .<br>Switch on **General Authentication Code** and set the required information. | • Digital Signage Terminal<br>• Interactive Flat Panel |
| Add devices by device serial No. | You can add device by device serial No. | Select **Serial No.** as the adding mode and set the required information. | IP Speaker |
| Add devices by device Instance No. | You can add BACnet devices to the platform by entering device instance No. | On the Add BACnet Device page, enter device instance No. and set the required information. | BACnet Device |

## Batch Import Devices

Scenario: When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the template to the platform to add devices in a batch.

1. Select an access protocol.
2. Click **Download Template** and save the predefined template (excel file) on your PC.
3. Open the exported template file and enter the required information of the devices to be added in the corresponding column.
4. Click and select the edited file.

Supported device types are as follows.

- Encoding Device
- Access Control Device
- Video Intercom Device
- Visitor Terminal
- On-Board Device

- Guidance Terminal
- Certain Models of Parking Lot Screen
- Security Control Device
- Speed LED Display
- Fire Protection Device
- Dock Station
- Portable Device
- Digital Signage Terminal
- LED Controller
- IP Speaker
- Portable Code Scanner
- Network Transmission Devices

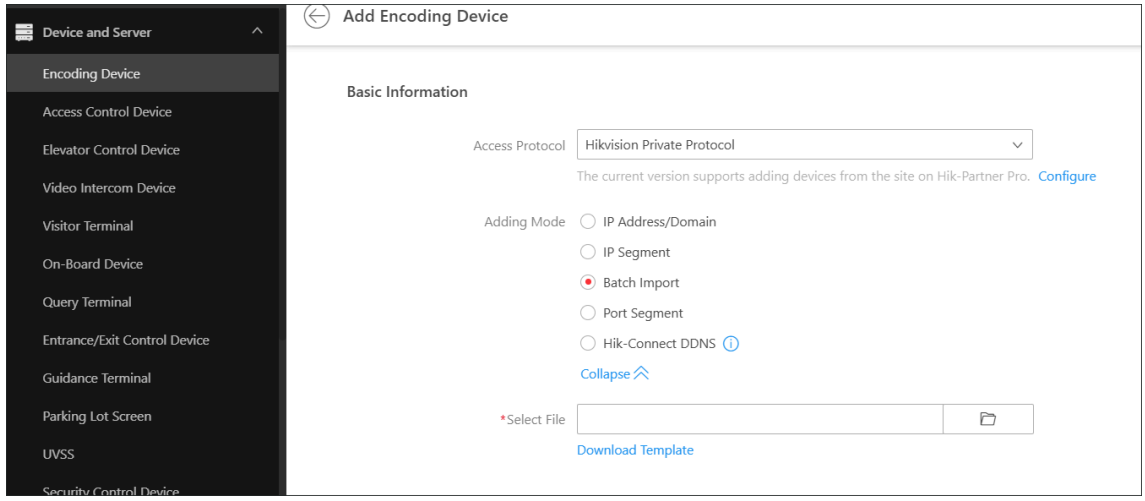



**Figure 3-3 Batch Import Devices**

## 3.2.2 Parameters on Add Device Pages

## Common Parameters on Add Device Pages

This chapter introduces parameters for adding devices.

**Note**

Parameters may vary by different access protocols.

### Basic Information

#### Device Address / Start and End IP Address

The IP address of the device. For online devices, the address is shown automatically. For other modes, you should enter them manually.

**Add by Encryption**

If you add the device via this method, the SDK service port should be encrypted.

**Device Port**

The port number of the device, which is shown automatically. The default port number is 8000.

**Mapped Port**

This function is only available when you select **Hikvision Private Protocol** to filter the detected online devices. If you want to download pictures from the device, switch on **Mapped Port** and enter the picture downloading port. By default, the port number is 80.

**Hik-Connect DDNS Server Address**

Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

**ISUP Login Password**

For devices supporting accessing the platform via ISUP 5.0, you should enter the ISUP login password.

**Get Stream via Device's Local Address**

By entering the device's local address, direct streaming will use this address when the client and device are on the same network.

**Verify Stream Encryption Key**

Switch on **Verify Stream Encryption Key**, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in SYS server for security purpose.

**Note**

This function should be supported by the devices. Refer to the user manual of the device for getting the key.

**Site on Hik-Partner Pro**

If you select Hik-Partner Pro as the access protocol, you need to select a site on Hik-Partner Pro to add the device.

**Picture Storage**

The captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

**Note**

- For details about configuring picture storage settings, see ***Edit Element in Area*** .
- If you select System Management Server as the storage location, the pictures will be stored on the SYS server. Click Configure to view the disk on SYS server and storage quota, which can be edited via the Web Client running on the SYS server. Refer to ***Set Storage on System Server*** for details.
- You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

**Time Zone**

Click **Get Device's Time Zone** to get the device's time zone, or click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

**Resource Information**

**Add Resource to Area**

Import the resources of the added device(s) to an existing area or a new area.

If you do not import resources to an area, you cannot perform further operations.

**Streaming Server**

Select a Streaming Server to get the video stream of the channels via the server. The cameras (if any) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it. You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

**Video Storage**

**Encoding Device**

The video files will be stored in the encoding device according to the configured recording schedule.

**CVR (Hybrid SAN)**

The video files will be stored in the Hybrid Storage Area Network according to the configured recording schedule.

**CStor**

The video files will be stored in the Cluster Storage according to the configured recording schedule.

**pStor**

According to the configured recording schedule, the video files will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

**SAC**

Refers to pStor Cluster Service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use SAC to manage these pStors.

**Note**

- For adding the encoding device by domain name, the video files can only be stored in the local storage of the device.
- Configure the CVR (Hybrid SAN), CStor or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cluster Storage or pStor.

**Get Device's Recording Settings**

Check to get the recording schedule from the device and the channels of the device will start recording according to the schedule.

## Parameters Exclusive for Adding On-Board Devices

**Device Info on Wi-Fi Network**

Switch on it and enter the address and port of the on-board device as well as the user name and password of the Wi-Fi.

**Note**

Once a vehicle reaches its destination and the on-board device successfully connects to the Wi-Fi there, the video recorded during the journey will be copied back to the platform.

**Verify Stream Encryption Key**

**AES128**

- Key Length: AES128 uses a 128-bit key, which is like a password made of 128 binary digits (0s and 1s). This provides a high level of security for everyday use.
- Security Level: It is considered very secure and efficient, suitable for protecting most personal and business data. While theoretically less robust than AES256, it is still extremely difficult to break with current technology.
- Performance: AES128 is faster and uses less computing power, making it ideal for devices with limited resources. In our software, it is the default option for general-purpose encryption to ensure smooth performance.

**AES256**

- Key Length: AES256 uses a longer 256-bit key, offering a significantly larger "key space." This means there are more possible combinations, making it even harder for unauthorized parties to guess the key.
- Security Level: It provides the highest level of security available in AES encryption, recommended for sensitive data like financial records, medical information, or government communications. It is resistant to advanced attacks, including brute-force attempts.
- Performance: Due to the longer key, AES256 requires more processing power and may slow down operations slightly on low-end devices. However, for G40-PRO series devices, the impact is minimal.

**Picture Storage**

- If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
- If you select **CVR (Hybrid SAN)**, **CStor**, **pStor**, or **NVR**, you need to select a storage medium from the drop-down list.

## Parameters Exclusive for Parking Lot Screen

The parameters vary by different device types.

**LAN IP Address**

IP address assigned to the display screen on LAN.

**Number of Display Rows**

The number of rows of the content can be displayed on the screen, which is determined by the device model.

For example, if the value is 2, it means the screen supports showing 2 rows of different information.




**Figure 3-4 Entrance Guidance Screen - One Row**

**Number of Directions**

The number of directions supported by the parking guidance screen, which is determined by the device model.

For example, if the value is 3, it means the screen supports showing the vacant parking spaces in three directions.



**Figure 3-5 Parking Guidance Screen - Three Directions**

### Parameters Exclusive for Dock Stations

**File Storage**

You can switch on to set the storage information of files uploaded by the dock station. You can select the storage location as CVR (Hybrid SAN), CStor, pStor, which should be configured in advance.

**Copyback Time**

You can set the copyback time of files stored on the portable enforcement device.

**Copy-Back File Type**

You can select the file types to be copybacked based on their importance which is configured on portable enforcement devices.

**Receiving Mode**

For persons are linked to a dock station and portable devices, set the portable device receiving mode to **Linkage Mode**. For persons can receive any portable devices, you set the mode to **Random Mode**.

### Parameters Exclusive for Security Control Device

**Device Source**

**New Device**

Add a new device to HikCentral Professional by Hik-Connect service.

**Hik-Connect DDNS Device List**

For users with a Hik-Connect account, you can add devices managed in your Hik-Connect account to HikCentral Professional in a batch.

## 3.3 Add Server(s)

This chapter introduces parameters on adding pages of different servers.

On the left, select a server type, and then click **Add** on the top.

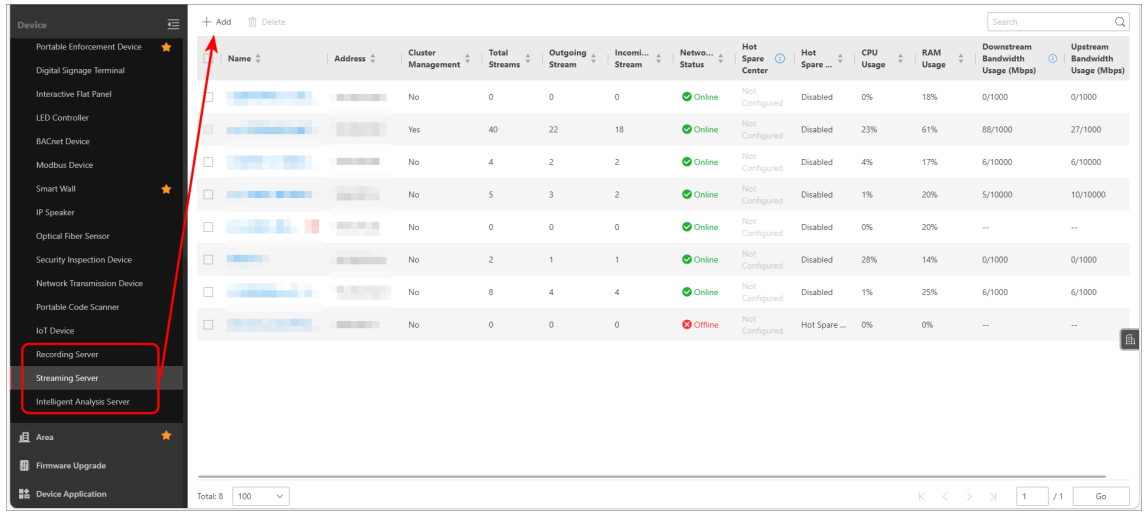



**Figure 3-6 Entry for Adding Server(s)**

## Parameters on Add Recording Server Page

**Note**

The parameters vary by different types of recording server.

**Address**

The server's IP address in LAN that can communicate with SYS.

**ANR Function**

You can check this field to enable the ANR function. This function is enabled default. If the network is disconnected between the pStor and the device, data can be stored on the pStor automatically.

**Control Port**

The control port No. of the server. If it is not changed, use the default value.

**Network Port**

The network port No. of the server. If it is not changed, use the default value.

**File Transmission Port**

The file transmission port No. of the server. If it is not changed, use the default value.

**Proxy Port**

The proxy port No. of the server. If it is not changed, use the default value.

**Signaling Gateway Port**

The signaling gateway port No. of the pStor server. If it is not changed, use the default value.

**Enable Picture Storage**

Switch on it for storing pictures in this server.

**Enable Stream Object Storage**

Enable stream object storage function for storing video streams, audio streams or other streaming data in this Hybrid SAN.

**Access Secret Key and Secret Key**

Enter the user's access secret key and secret key of the pStor server for downloading pictures.

For pStor servers and cluster storage servers, you can download these two keys on the pStor server's Web Client page, or contact our technical support.

**Enable WAN Access**

If you need to access the server via WAN, switch on it and set the corresponding parameters which are available when you access the server via WAN.

## Parameters on Add Streaming Server Page

**Network Location**

Select **LAN IP Address** if the Streaming Server and the SYS server are in the same LAN. Otherwise, select **WAN IP Address**.

**Address**

The IP address of streaming server to be added.

**RTSP Streaming Port (TCP)**

For Streaming Service to get stream. If it is not changed, use the default value.

**Network Port**

For getting the status of Streaming Service. If it is not changed, use the default value.

**Web Client Streaming Port**

For getting stream for Google Chrome or Firefox. If it is not changed, use the default value.

**Management Port (SSL)**

For security certificate authentication. If it is not changed, use the default value.

**Web Client Streaming Port (SSL)**

For Web Client streaming. If it is not changed, use the default value.

**RTMP Streaming Port**

For OpenAPI streaming. If it is not changed, use the default value.

**HLS Streaming Port**

For OpenAPI streaming. If it is not changed, use the default value.

**Enable WAN Access**

If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN.

**Note**

- The **Enable WAN Access** switch is available only when you set Network Location as **LAN IP Address**.
- Go to **System → Network → WAN Access** to set the default port No. of streaming media ports.

**Server Cluster Deployment**

In the cluster mode, select **Yes** or **No** for Server Cluster Deployment.

**Hot Spare**

In the stand-alone mode, switch on **Hot Spare** and set the hot spare type.

### Parameters on Add Intelligent Analysis Server Page

**Address**

IP address of the intelligent analysis server.

**Port No.**

Port No. of the intelligent analysis server. If it is not changed, use the default value.

**Enable WAN Access**

Enable the intelligent analysis server to access WAN (Wide Area Network).

**Note**

After enabling the WAN Access, you need to set the WAN IP address and port number of the server for WAN access.

## 3.4 After Adding Devices/Servers: Operations on Device List Page

After adding devices, you can perform further operations on the device list.

**Table 3-2 Operations Supported on Added Device List**

| Operations | Descriptions |
|---|---|
| Edit a Device/Servers | Click a device/Server's name to enter the editing page. |
| Remote Configurations | Click ⚙ in the Operation column to set the remote configurations of the corresponding device.<br>Click  in the Operation column to set the remote configurations of a camera. |

| Operations | Descriptions |
|---|---|
| | **Note**<br>For detailed operation steps about remote configuration, see the user manual of the device/camera. |
| Change Password | Select the added device(s) and click **Change Password** to change the password for the device(s).<br>**Note**<br>• You can only change the password for online Hikvision devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| Replace Device | When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform.<br>In the **Operation** column, click to replace the old device with the new device on the platform. |
| Edit Bandwidth for Video Downloading | Select one or more NVRs (V4.1.5 or later versions), and click **Edit Bandwidth for Video Downloading** to set the bandwidth upper-limit for video downloading of the selected NVR(s). |
| Set Time Zone | Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s). |
| Set N+1 Hot Spare for NVR | You can form an N+1 hot spare system with at least two NVRs (Network Video Recorder) or hybrid SANs. The system consists of several host servers and a spare server (cannot be selected for storing videos). When a host server fails, the spare server switches into operation (such as video recording, searching video for playback, etc.), and thus increasing the video storage reliability of HikCentral Professional.<br>1. On the Encoding Device page, click **N+1 Hot Spare** to set N+1 hot spare for NVRs.<br>2. Click **Add** to set N+1 hot spare.<br>3. Select a NVR in the **Spare** drop-down list to set it as the spare server.<br>4. Select the NVR(s) in the **Host** field to set them as the host server.<br>5. Click **Add**. |

| Operations | Descriptions |
|---|---|
| | **Note**<br>The recording schedules configured on the NVR will be deleted after setting it as the spare Recording Server.<br>6. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect. |
| Set Hot Spare for CVR | You can form an N+1 hot spare system with several host servers and a spare server (cannot be selected for storing videos). When a host server fails, the spare server switches into operation (such as video recording, searching video for playback, etc.), and thus increasing the video storage reliability of HikCentral Professional.<br>1. On the Recording Server page, click **CVR Hot Spare → Add** .<br>2. Select the CVR(s) in the **Host** field to set them as the host server.<br>3. Select a CVR in the **Spare** drop-down list to set it as the spare server.<br>4. Click **Add**.<br>**Note**<br>If added, the resources on the spare server will be deleted. |
| Wake Up the Solar Camera | After you add a solar camera, the network status will be displayed as offline, online (Asleep), or online (Waked up). You can click in the **Operation** column to wake up an asleep camera. You can also click the device name to enter the editing device page, and click **Wake Up** to wake the device up.<br>**Note**<br>If a device is in sleep mode, the communication between the solar camera and the platform is not supported. |
| Restore Default Settings | Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.<br>To restore all the device parameters, check **Restore device network parameters and account information, such as user name and password.** in the pop-up window. |
| Privacy Settings | To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices. |

| Operations | Descriptions |
|---|---|
| Search for Device/Server(s) | Enter a keyword in the search box on the upper right corner of the page to quickly search for the target device/server(s). |
| Delete Device/Servers | Check device/server(s) in the list, and click **Delete** to delete the selected server(s). |
| For Guidance Terminal: Configure Inductive Loop Battery Threshold | When the battery is lower than the configured value, the notification of low geomagnetic system battery will be displayed on the alarm details window. The **Maintenance → Resource Status → Guidance Terminal** also displays this parameter. |
| For Query Terminal: Configure Background Picture | It allows you to upload a custom background image, which will be displayed in the Query Terminal client or app. |

### 3.4.1 Add and Manage Applications

You can give algorithm capabilities to devices by configuring device application packages. After you finish configuring, you can add the applications to specific devices and manage the applications.

### Add Device Applications to Encoding Devices

**Note**

- Make sure the devices you are going to use are added to the platform and the devices are online.
- Currently not all encoding devices can be updated via device applications. See *Compatibility List of Hikvision Products* for models supporting this function.

1. On the left of the Device module, select **Device Application → All Applications → Add Application** .
2. Select the **Application Package Source**.
3. Upload related files or packages and enter related information.
4. Click **Next**.
5. Select available device(s) to add the application.
6. Click **Finish** to add the application to the device.
   The device application details are displayed in **All Applications** tab.

Perform the following operations after adding applications to device(s).

**Table 3-3 Optional Operations After Adding Application**

| Operation | Description |
|---|---|
| Enable/Disable Device Application | Click **Enable All** / **Disable All** to enable/disable the corresponding device application. |
| Delete Device Application | Click **Delete** to delete the device applications. |
| Import License | Click **Import License** and upload a license file to specific device(s). |
| Filter Applications by Status | Select status in the drop-down list of **Status**. |
| View Adding Records | Click **Adding Records** to open the adding records page, you can view the records about adding device applications in specific time period.<br>**Note**<br>The icon indicates that adding device application(s) failed. |
| Search for Applications | On the upper right, enter the keywords of application name, and click to search for added device applications. |

## Manage Applications on Devices

On the left of the Device module, select **Device Application → All Devices** .

**Table 3-4 Operations for All Devices**

| Operation | Description |
|---|---|
| View Device Application Details | Select an encoding device on the list to view device application details on the right, including device application name, device application version, system memory usage, smart RAM usage, and flash usage. |
| Enable/Disable Device Application | Select an encoding device on the list, click / to enable/disable the corresponding device application.<br>Or select an encoding device on the list, and select multiple applications on the right, and click **Enable/Disable** to batch enable/disable the device applications. |

| Operation | Description |
|---|---|
| Add Device Application to Specific Device | Select an encoding device on the list, click **Add** to add device application package for this device. |
| Refresh Device Application List | Select an encoding device on the list, click **Refresh** to refresh the device application list. |
| Delete Device Application | Select an encoding device on the list, and select the device application(s). Click **Delete** to delete the device application(s). |
| View Adding Records | Click **Adding Records** to open the adding records page, you can view the records about adding device applications in specific time period.<br>The icon ⓘ indicates that adding device application(s) failed. |

### 3.4.2 Configurations After Adding Portable Enforcement Devices

## For Dock Stations

Edit receiving mode of portable devices in a batch:

**Linkage Mode**

In this mode, a specific portable device is permanently or temporarily assigned to a particular officer or team. ***The binding is managed through the Portable Enforcement module.***

Use Cases:

- Daily Patrols: Officers use the same device consistently for shift-based duties.
- Evidence Management: Critical for legal chain of custody when footage must be tied to a specific officer.

**Random Mode**

Devices are assigned randomly to officers, with no pre-defined user-device linkage.

Use Cases:

- High-Turnover Scenarios: Ideal for large departments with frequent shift changes or reserve officers.
- Pooled Resources: When devices are shared across multiple teams without fixed assignments.
- Emergency Deployment: Rapid issuance during unforeseen events where prioritization trumps personalized allocation.

### For Portable Devices

On the Portable Device tab, you can perform the following operations.

**Apply Admin Password**

Batch edit the admin password of portable devices.

**Apply Recording Parameters**

Configure video resolution, pre-record duration, and video frame rate for portable devices.

**PPPoE**

Configure this for newly added portable devices, or portable devices whose operators are changed so that they can connect to the 4G network.

**Apply Parameters to All Portable Devices**

Configure multiple parameters of portable devices and apply these parameters to all devices.

**Other Operations**

In the Device Locking Status and Operation column, you can remotely lock the device, format the SD card, or shut it down. These functions help secure the device if it is lost.

## 3.4.3 Configurations After Adding Speed LED Displays

**Speeding Threshold**

Enter a numerical value (range: 0–200 km/h). A speeding alarm will trigger if the vehicle's speed exceeds this threshold.

**Low Battery Threshold**

Enter a numerical value (range: 10–50%). A low battery alarm will activate when the battery level drops below this threshold.

## 3.4.4 Configure Parameters for Access Control Devices / Sliding Gate Opener / Elevator Control Devices

You can configure parameters for access control devices and elevator control devices, including device time, linkage settings (linked device actions), maintenance settings, etc.

On the left, select **Access Control Device** or **Elevator Control Device**, and click ⚙ in the Operation column to enter the configuration page of a device.

Configure device parameters according to the following topics.

**Note**

- Device support required. Parameters vary with different device types and models.
- The supported features and parameters are subject to the applications you installed.

## Time

You can view the time zone where the device locates and set the following parameters.

**Device Time**

Click the **Device Time** field to customize time for the device.

**Sync with Server Time**

Synchronize the device time with the server of the platform.

## Biometrics

You can enable facial recognition and fingerprint recognition of access control devices if the devices support biometrics recognition.

**Facial Recognition**

Set facial recognition function for the device, and select a facial recognition mode.

**Single-Person Recognition**

The device can recognize one person at a time.

**Multiple-Person Recognition**

The device can recognize multiple persons at a time.

**Fingerprint Recognition**

Set persons' fingerprint recognition for the device. Once enabled, the device can recognize persons by their fingerprints.

## Skin-surface Temperature

Set **Temperature Measurement** to on to enable temperature screening function.

**Threshold(℃)**

Set the range of normal skin-surface temperature. The detected temperature that is not in this range is abnormal temperature. The maximum temperature should be higher than the minimum temperature.

**Open Door When Temperature is Abnormal**

If it is enabled, the door will open when person's skin-surface temperature is abnormal. By default, the door will not open for abnormal temperature.

**Linked Thermal Camera**

Enter the device IP address of the linked thermal camera for temperature screening.

**Note**

It is used for the access control devices that do not support temperature screening.

## Registration Device

If you enable this function, the information about added persons and credentials (including face pictures and fingerprints) added on the device will be automatically synchronized to the platform.

## Mask Settings

Set **Mask Detection** to on to enable mask detection function. Once enabled, the device can detect persons without face masks.

**Do Not Open Barrier when No Mask**

If it is checked, the barrier will still open for persons without masks.

## RS-485

**RS-485 Communication Redundancy**

You can check **RS-485 Communication Redundancy** to enable the function if you wire the RS-485 card to the device redundantly.

**Working Mode**

Select the working mode, including the card reader, door control unit, and access control host.

## Turnstile Parameters

You can configure passing mode for the turnstile linked to the device.

**Based on Lane Controller's DIP Mode**

The device will follow the lane controller's DIP settings to control the turnstile. The settings on the main controller will be invalid.

**Based on Main Controller's Settings**

The device will follow the settings of main controller to control the turnstile. The DIP settings of the lane controller will be invalid.

## Fingerprint Recognition Mode

**Front End**

In this mode, fingerprint data is stored directly on the reader device at each access point. The fingerprint matching process occurs locally on the reader itself, without relying on a central system. It is suitable when the number of users is small and stable, with infrequent changes (e.g., a family home or a small team with fixed members). You can use this mode if you lack reliable network connectivity or wish to avoid complex wiring. It operates offline, making it independent of network failures.

**Back End**

In this mode, fingerprint data is stored on an access controller. The reader only captures the fingerprint image and sends it to the controller system for verification. This mode enables centralized management and advanced functionality. It is essential for environments with

multiple doors, and is ideal for expanding systems, as new access points can be easily added to the centralized network without reconfiguring each reader. This mode requires a stable network connection.

## Keyfob Settings (for Sliding Gate Opener)

**Keyfob Detection Distance**

The max. distance that the keyfob can control the gate opener.

## Maintenance

You can reboot a device remotely and restore it to its default settings.

**Reboot**

Reboot the device.

**Restore Default Settings**

Restore the device to its default settings. The device needs to be activated after being restored.

## Facial Recognition Mode

You can check **Deep Mode** to enable the function. Once enabled, all the face credentials applied to the device will be cleared. Go to **Access Control → Access Level** and click to apply the data in the platform to the device.

## More

You can click **Configure** to open the remote configuration page of the device and configure more parameters. For details, refer to the user manual of the device.

## Configure Relations Between Relays and Floors

You can configure the relations between relays and floors to determine how floor control is managed, including options such as passengers selecting target floors, passengers calling elevators, or automatic floor button pressing and elevator summoning for passengers.

There are three types of relay available.

**Button**

Control the validity for buttons of each floor. For floors related to **Button**, passengers can press the button of the floors.

**Call Elevator**

Control to call the elevator to go to the specified floor. For floors related to this feature, people who are waiting for elevators can call elevator to the floor they stay.

**Auto Button**

Control to press the button when the user swipes card inside or outside of the elevator. The button of the floor will be pressed automatically according to the user's permission.

Configure the relations between the relays and the floors.

- Drag the unconfigured relay from the Unconfigured Relay panel to the target floor.
- 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.

Take the following picture as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents number of the relay, and the color under the number represents the relay type.

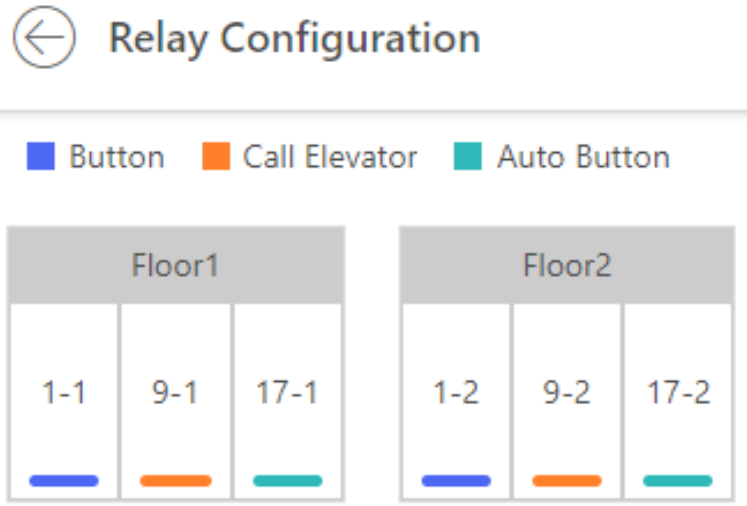



**Figure 3-7 Relay Configuration**

## Custom Wiegand Parameters

Based on the knowledge of uploading rule for the third-party Wiegand, you can configure Wiegand parameters to communicate between the device and the third-party card readers.

**Note**

- By default, the device disables the custom Wiegand function. If you enable the custom Wiegand function, all Wiegand ports in the device will use the customized Wiegand protocol.
- You can configure up to 5 custom Wiegand devices.

Switch on **Custom Wiegand** and configure the Wiegand parameters. You can select a device from the **Copy From** drop-down list to copy the settings of another device.

**Total Length**

Wiegand data length.

**Parity Type**

Set the valid parity for Wiegand data according to property of the third party card reader. You can select **Nothing**, **Odd Even Check**, or **XOR Parity**.

If you select **Odd Even Check**, you can configure the following:

**Odd Start, Length**

If the odd parity start bit is 1 and the length is 12, then the platform 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 Start, Length**

If the even parity start bit is 12, and the length is 12, then the platform will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

If you select **XOR Parity**, you can configure the following:

**XOR Parity Start Bit, Length per Group, Length for Parity**

Depending on the table displayed below, the start bit is 0, the length per group is 4, and the length for parity is 40. It means that the platform 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).

**Output Rule**

Set the output rule.

**Card ID Start Bit, Length, and Decimal Digit**

If you use the transformation rule, these items are available. Depending on the table displayed below, 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 below, 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.

**Note**

Take Wiegand 44 for example, the setting values in the Custom Wiegand are as follows:

| | | | | | |
|---|---|---|---|---|---|
| Custom Wiegand Name | Wiegand 44 | | | | |
| Total Length | 44 | | | | |
| Transformation Rule (Decimal Digit) | byFormatRule[4]=[1][4][0][0] | | | | |
| Parity Type | 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 |

## Set Wiegand Parameters

You can set Wiegand parameters for access control devices to facilitate communications between card readers and access control devices.

Select a Wiegand protocol in the list, and click ✎ in the Operation column to pop up a window of Wiegand information. On the pop-up window, set Wiegand parameters and click **OK**.

**Direction**

Whether the device is used for inputting (receiving) or outputting (sending) data.

Check **Input** or **Output**.

**Wiegand Mode**

The signal transmitting mode. Whether the device transmits 26-bit, 34-bit, 27-bit, and 35-bit data.

**Note**

Wiegand mode can only be selected when the direction is **Output**.

**Output Format**

Whether to output the signal as employee No. or card No.

**Note**

Output format can only be selected when the direction is output.

**Signal Sending Interval**

The interval of sending data.

**Linked Card Reader**

The card reader No. to be linked.

**Note**

Linked card reader can only be selected when the device supports linking to a card reader.

## Configure Device Actions

You can set the linkage actions of an access control device or elevator control device for different event sources, so that when the device detects a linkage source, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Click **Add** in the Linkage section. Set the event source, and then configure parameters of the linkage target.

**Buzzing**

**Buzzer on Controller**

**ON**

Turn on the buzzer on the access controller when the specified event is triggered.

**OFF**

Turn off the buzzer on the access controller when the specified event is triggered.

**No Linkage**

Disable the linkage action.

**Buzzer on Reader**

**ON**

Turn on the buzzer on the card reader when the specified event is triggered.

**OFF**

Turn off the buzzer on the card reader when the specified event is triggered.

**No Linkage**

Disable the linkage action.

**Capture/Recording**

**Capture**

Enable the device's linked camera to capture a picture when the specified event is triggered.

**Recording**

Enable the device's linked camera to record video footage when the specified event is triggered.

**Alarm Output**

**ON**

Trigger the alarm output when the specified event is triggered.

**OFF**

Stop the alarm output when the specified event is triggered.

**No Linkage**

Disable the linkage action.

**Zone**

**ON**

Arm the zone when the specified event is triggered.

**OFF**

Disarm the zone when the specified event is triggered.

**No Linkage**

Disable the linkage action.

**Access Point**

**Unlock**

Unlock the door or barrier when the specified event is triggered.

**Lock**

Lock the door or barrier when the specified event is triggered.

**Remain Unlocked**

The door or barrier will remain unlocked when the specified event is triggered.

**Remain Locked**

The door or barrier will remain locked when the specified event is triggered.

**No Linkage**

Disable the linkage action.

**Floor**

**Temporary Access**

Grant access to the floor for a limited time when the specified event is triggered.

**Access with Credential**

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

**Free Access**

Grant access to the floor indefinitely when the specified event is triggered.

**Access Forbidden**

Deny access to the floor indefinitely when the specified event is triggered.

**No Linkage**

Disable the linkage action.

## Card Swiping Parameters

You can configure card swiping parameters to allow authentication by entering card number on keypad, enable NFC clone card, enable M1 encryption, etc.

In Card Swiping section, configure card swiping parameters.

**Reader Communication Protocol**

Select the reader communication protocol.

**Input Card Number On Keypad**

If it is checked, users can enter card number on keypad for authentication.

**Enable NFC Card**

If it is enabled, users can use cloned cards for authentication.

**M1 Encryption**

If it is enabled, only the card with the same encrypted sector can be granted access, and you need to choose an encrypted sector.

**Voice Prompt**

If it is enabled, an audio prompt will be played when swiping cards.

**Upload Picture after Linked Capture**

Upload the pictures captured by the linked camera(s) to the platform automatically.

**Picture Storage**

If it is checked, the captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

**Picture Size**

Select a picture size from the drop-down list for the captured pictures saved to the storage location.

**Picture Quality**

Select a picture quality from the drop-down list for the captured pictures saved to the storage location.

**Capture Times**

Select the capture times from the drop-down list for the devices to capture face pictures for the times selected.

### 3.4.5 Upgrade Device Firmware

You can upgrade the devices with the firmware to be upgraded according to device type and upgrade mode.

Select **Firmware Upgrade** on the left navigation pane.

The upgrade mode is provided by the platform after you select the device, including via the current Web Client, local PC, Hik-Connect, and FTP.

#### Upgrade Device Firmware via Current Web Client

1. Select **Via Current Web Client**.
2. In the **Upgrade By** field, select the upgrade method.
3. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.
4. Select device(s).
5. Select an upgrade package from the local PC.
6. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.

#### Upgrade Device Firmware via Hik-Connect

1. Select **Via Hik-Connect**.
2. In the **Device Access Protocol** field, select the relevant protocol.
3. In the **Upgrade By** field, select the upgrade method.

**Note**

This field is not required if Hik-Partner Pro Protocol is selected as the device access protocol.

4. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.
5. Install the required web plug-in.

**Note**

If you select Local PC as the upgrade method, you should install the required web plug-in if the prompt pops up.

6. Select device(s).
7. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.

## Upgrade Device Firmware via FTP

1. Select **Upgrade Firmware via FTP**.
2. Set the basic information.

   **FTP Server Address**

   The address of FTP server, where you have uploaded the firmware upgrade package.

   **Port No.**

   The port number of FTP server.

   **User Name**

   The user name of FTP server.

   **Password**

   The password of the FTP server.

   **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.

   **Path**

   If you save FTP firmware upgrade package in a non-root directory, enter the root directory name. If you saved FTP firmware upgrade package in a root directory, keep the field empty.
3. Select a device type and select a device from the device list.

   **Note**

   If you select Dock Station as the device type, you need to select an upgrade object from the drop-down list.
4. Select an upgrade package from the local PC.
5. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.

**Wireless Network Settings (for On-Board Devices)**

**Wi-Fi Only**

It is recommended when a stable and reliable Wi-Fi connection is available and you want to avoid using cellular data to reduce potential data charges. The update may stop if the Wi-Fi signal is weak or disconnected. Ensure the vehicle remains within Wi-Fi range during the entire process.

**Wi-Fi and 4G Network**

The device will first attempt to use Wi-Fi. If no Wi--Fi is detected, it will proceed via 4G without requiring manual intervention. This option enables the device to prioritize Wi-Fi for updates but automatically switches to 4G cellular data if Wi-Fi is unavailable. It is suitable when seamless updates are critical, and Wi-Fi coverage may be intermittent, and cellular data usage is permitted (check your data plan to avoid excess charges).

**Note**

In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.
To view the devices with firmware upgraded, upgrading, to be upgraded, and not upgraded, you can click in the Upgrade Status column. In the upgrade task list, you can click in the Operation column to delete the upgrade task.

## 3.4.6 Create Password for Inactive Device(s)

The devices with simple default password may be accessed by the unauthorized user easily. For the security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them to the platform. Besides activating the device one by one, you can also batch activate multiple devices which have the same password simultaneously.

**Steps**

**Note**

This function should be supported by the device. Make sure the devices you want to activate support this function.

1. On the left, click **Device and Server** and select a device type.
2. In the Online Device area, view the device status and select one or multiple inactive devices.
3. Click **Activate** to open the device activation window.
4. 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.

5. Click **Save** to create the password for the device.

**Note**

If you have not set security questions, the window of setting security questions will pop up, and you should select the method of resetting password and set the security questions as needed.

An **Operation completed.** message is displayed when the password is set successfully.

6. Click in the Operation column to change the device's IP address, subnet mask, gateway, and so on if needed.

**Note**

For details, refer to ***Edit Online Device's Network Information*** .

### 3.4.7 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS or Web Client, can be detected by HikCentral Professional. For the detected online devices, you can edit their network information as desired via HikCentral Professional remotely and conveniently. For example, you can change the device IP address due to the changes of the network.

**Before You Start**

For some devices, you should activate it before editing its network information. Refer to ***Create Password for Inactive Device(s)*** for details.

Perform this task when you need to edit the network information for the detected online devices.

**Steps**

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, select a network type.

   **Server Network**

   The detected online devices in the same local subnet with the SYS will be listed.

   **Local Network**

   The detected online devices in the same local subnet with the Web Client will be listed.
3. View the device status, and click in the Operation column of an active device.
4. Edit the device parameters, such as IP address, device port, subnet mask, and gateway.

**Note**

The parameters may vary for different device types.

5. Click .
6. Enter the device's password.
7. Click **Save**.

### 3.4.8 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 system. Then you can access the device or add it to the system using the password.

#### Restore Device's Default Password

For some devices with old firmware version, if you forgot the password you use to access the online device, you can restore the device's default password through the platform and then you must change the default password to a stronger one for better security.
In the Online Device area, view the device status (shown on Security column) and click in the Operation column of an active device. Enter the security code in the pop-up window and restore the default password of the selected device.

**Note**

Contact our technical support to obtain a security code.

#### Reset Device Password

If you forget the password you use to access the online device, you can request for a key file from the technical support and reset the device's password through the platform.
In the Online Device area, view the device status (shown on Security column) and click icon in the Operation column of an active device. The Reset Password window pops up.

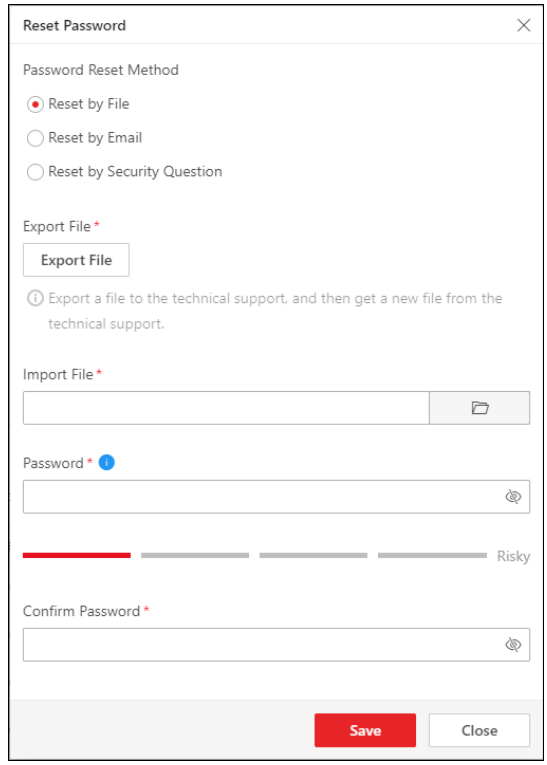



**Figure 3-8 Reset Password**

Select a password reset method and save the settings.

**Reset by File**

Click **Export File** to save the device file on your PC. Send the file to the technical support.

**Note**

For the following operations about resetting the password, contact the technical support.

**Reset by Email**

Export the QR code and sent it to the email displayed. You will receive the verification code in 5 minutes. Enter the code, new password, and confirm password.

**Reset by Security Question**

Enter the answer to the security question, new password, and confirm password.

**Note**

If you have not set security questions, the window of setting security questions will pop up, and you should set the security questions as needed.

**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.

# Chapter 4 Area Management

HikCentral Professional provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations and do some other operations of the devices after managing the resources by areas.

**Note**

If the current system is a Central System with a Remote Site Management module, you can also manage the areas on a Remote Site and add cameras on Remote Site into areas.

In the top left corner of Home page, select → **Basic Management** → **Device** , and click **Area** on the left.

## 4.1 Add an Area Manually

You should add an area before managing the elements by areas.

In the left panel. select the current/remote site from the drop-down site list to show its areas.

**Note**

- The icon indicates that the site is the current site.
- The icon indicates that the site is a Remote Site.

Click + on the area list panel to open the Add Area panel, select a parent area to add a sub area, and create a name for the area.

**Streaming Server**

Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server. After selecting a Streaming Server for the area, check off Wall Display via Streaming Server if you want to display the area's resources on the smart wall via this Streaming Server.

After adding the area, you can perform the following operations on the area list.

| Operation | Description |
|---|---|
| Edit Area | Hover the cursor on ··· and click **Edit** to edit the area. |
| Export Device Information in Area | Hover the cursor on ··· and click **Export Device Information in Area** to export all devices that you have permission to access in the current area. |

| Operation | Description |
|---|---|
| Delete Area | Select an area and click or hover the cursor on and click **Delete** to delete the selected area. You can also press **Ctrl** on your keyboard, select multiple areas, and then click to delete areas in a batch.<br>After deleting the area, the resources in the area will be removed from the area, as well as the corresponding recording settings, event settings, and map settings. |
| Move Area | Drag the added area to another parent area as the sub area. |
| Stick on Top | Hover the cursor on and click **Stick on Top** / **Cancel Stick Area On Top** to stick the area / cancel sticking the area to the top.<br>**Note**<br>The order of the parent area cannot be changed. |
| Import/Export Areas | Click to import areas with predefined template file; click to export all areas to local PC. |
| Customize Additional Information | In the area list panel on the left, click to enter the Customize Additional Information page. Click **Add**, set the name and type, and click **Add** to customize the additional area information. |

## 4.2 Import Areas in a Batch

You can batch add areas via importing a predefined template file.

Click . In the pop-up pane, click **Download Template** and enter the area related information in the downloaded template.

**Area**

| Rule |
|---|
| 1. Fields marked with asterisk (*) are required. |
| 2. Please enter the area to be imported in Area Name and its upper-level area path in Area Path. |
| 3. Area name: Required. 1 to 64 characters allowed. Special characters such as '/\:*?"<>\| cannot be entered. |
| 4. Area path: If the path is left blank, the area will be added to the root area by default. |

| Example | |
|---|---|
| **Area Name*** | **Area Path** |
| Area 1 | |
| Area 2 | First-Level Area |
| Area 3 | First-Level Area > Second-Level Area |
| Area 4 | First-Level Area > Second-Level Area > Third-Level Area |
| Area 5 | First-Level Area > Second-Level Area > Third-Level Area > Fourth-Level Area |

| Data Details | |
|---|---|
| **Area Name*** | **Area Path** |
| | |
| | |
| | |

**Figure 4-1 Downloaded Template**

## 4.3 Add Element to Area

### Add Devices to Area

Select a site and an area on the left, select a device type on the top, and click **Add**.

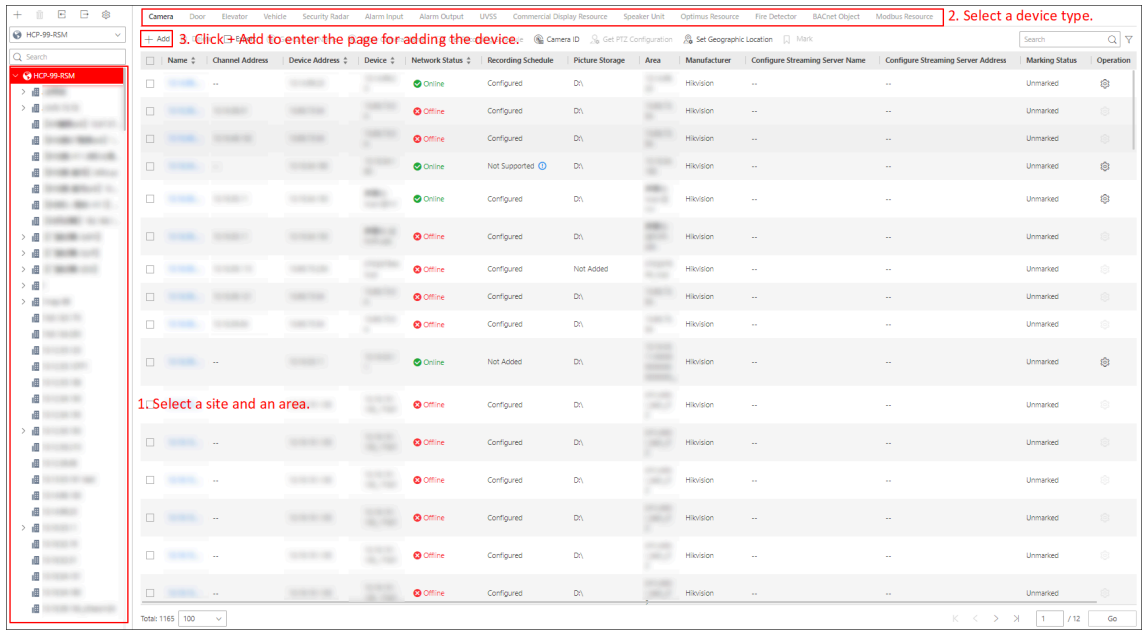



**Figure 4-2 Entry for Adding Element**

**Note**

- The icon indicates that the site is the current site. The icon indicates that the site is a Remote Site.
- For alarm output, when the alarm or event linked with the alarm output is detected, alarm devices (e.g., the siren, alarm lamp, etc.) connected with the alarm output will make actions. For example, when receiving the alarm out signal from the system, the alarm lamp will flash.

## Parameters on Add Device Page for Current Site

**Table 4-1 Parameters on Add Device Page**

| Device Type | Parameters | Descriptions |
|---|---|---|
| Camera | **Get Device's Recording Settings** | Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.<br>**Note**<br>If the recording schedule configured on the device is not continuous recording, it will be changed to event recording on the local device. |
| Elevator | **Range of Floor No.** | In the **Range of Floor No.** field, enter the start No. and end No. of the floors that you want to import to the area.<br>The floors between the start No. and end No. will be imported to the area. After imported, you can manage the floors in the system, such as adding to access levels, controlling status, etc. |
| Vehicle | **Linkage Device** | Select the on-board device linked with the vehicle from the Linkage Device drop-down list. |

| Device Type | Parameters | Descriptions |
|---|---|---|
| Alarm Input | **Device Type** | For the security control device, you need to select its zones as alarm inputs to add to the area. |
| Modbus Resource | **Batch Import** | For scenarios involving Hikvision Online UPS devices, it is mandatory to procure the R Series UPS SNMP Card (Sap code: 314001589) to ensure normal operation. Afterwards, click ***here*** to download the pre-configured mapping file, and then click to upload the file for batch configuring the mappings.<br>• DS-UPS01K24-R/TJS(/X)<br>• DS-UPS01K24-R/TS(/X)<br>• DS-UPS02K48-R/TJS(/X)<br>• DS-UPS02K48-R/TS(/X)<br>• DS-UPS03K72-R/TJS(/X)<br>• DS-UPS03K72-R/TS(/X)<br>• DS-UPS06K-R/TJL<br>• DS-UPS10K-R/TJL |

## 4.4 Operations on Area Page: After Adding Elements to Areas

After adding the element(s), you can do one or more of the followings.

**Table 4-2 Operations After Adding Elements to Areas**

| Operation | Description | Supported Element Types |
|---|---|---|
| Move Element(s) to Another Area | Select the areas, click , select a target area, and click **Move** to move the selected areas to the target area. | All types |
| Display Elements of Sub Areas | Check **Include Sub-Area** to display the elements of sub areas. | All types |

| Operation | Description | Supported Element Types |
|---|---|---|
| Filter Elements | Select the device type(s) to be displayed in the list from the drop-down list on the left of the search box. | • Camera<br>• Door<br>• Commercial Display Resource<br>• BACnet Object |
| Set Geographic Location | Click to enter Map Settings page and drag the elements to the map. See ***Add Hot Spot to Map*** for details. | • Camera<br>• Door<br>• Elevator<br>• Security Radar<br>• Alarm Input<br>• Alarm Output<br>• UVSS<br>• Speaker Unit<br>• Fire Detector<br>• Modbus Resource |
| Display Elements of Sub Areas | Check **Include Sub-area** to display the elements in sub areas. | All types |
| Search for Elements | Enter the keywords in the Search field to search for elements. | All types |
| Arm/Disarm Element | Select the element(s) and click **Arm/Disarm** to arm/disarm the selected element(s).<br>**Note**<br>An event will be triggered if any person or object enters an armed detection area. | • Security Radar<br>• Alarm Input |

## Operations Exclusive for Camera

**Export Information of Camera**

Click to export the information of the selected cameras added to the area to an Excel file.

**Get Camera Name**

Select the cameras and click **Get Camera Name** to batch get camera names.

**Apply Camera Name**

Select cameras and click  to batch apply the camera names to the cameras.

**Get Recording Schedule fro Device**

Select the cameras and click **Get Recording Schedule** to batch get cameras' recording schedules.

**Set Camera ID**

Click  to enter the Camera ID page, edit the default identifier number in the **ID** column of each camera, and click **Save**.

**Note**

The camera ID is unique and used to display a certain camera's live view on the smart wall via the network keyboard.

**Get PTZ Configuration**

Select the cameras and click to get the details of PTZ configurations from the devices in a batch.

**Mark Camera**

Select the cameras, click and check **Two-Way Audio Supported** to mark the cameras which support two-way audio.

**Migrate Videos from Third-Party Cameras to Hikvision Cameras**

**Application Scenario**: You are going to replace a third-party camera by a Hikvision camera, and videos recorded by these third-party cameras can still be searched in the Hikvision camera after replacement.

Third-party cameras include: Axis cameras, Dahua cameras, Hanwha cameras, and ONVIF cameras

In the Operation column, click  and select a camera to replace the existing one.

**Note**

- Both two cameras should be online.
- Migrating videos to cameras in another site is not supported.
- After the migration, new camera's recording schedule will be covered immediately.

**Consistency of Recording Schedules Between Platform and Devices**

The platform will check whether the platform and devices' recording schedules are consistent. In case of inconsistency, a red exclamation mark will show behind the device. You can apply the recording schedule of the platform to the device, or get the recording schedule from the device.

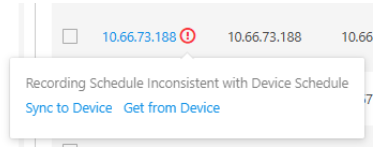



**Figure 4-3 Inconsistent Recording Schedule**

## Operations Exclusive for Door

### Synchronize Door Name

Select the doors and click **Synchronize Door Name** to get doors' names from the devices in a batch.

### Apply Door Name

Select doors and click to batch apply the door names to the doors.

## Operations Exclusive for Elevator

### Get Floor Name

Select elevators and click **Get Floor Name** to batch get floor names.

### Apply Floor Name

Select elevators and click to batch apply the floor names to the floors.

## Operations Exclusive for Vehicle

### Set Speed Threshold

Select the vehicle(s), click **Speed Threshold Settings**, and drag the slider or enter an integer in the text field.

### Configure Shutdown Delay

Select the vehicle(s), click **Configure Shutdown Delay**, and enable the delay time and enter a time range.

## Operations Exclusive for Speaker Unit

### Alarm/Broadcast Volume

Select speaker unit(s) and click **Alarm/Broadcast Volume** to adjust the output volume and input volume (used for Live Broadcast, Scheduled Broadcast, Alarm Linkage Broadcast, and Emergency Mustering Linkage Broadcast). Input and output volume levels can be viewed in the device list.

### Mixing Audio Volume

The Mixing Audio Volume determines the volume ratio of low-priority audio tasks relative to high-priority tasks. For example, when set to 40%, low-priority tasks are limited to 40% of the high-priority task's volume, ensuring critical audio remains dominant. This mechanism prioritizes essential alerts while allowing background audio to coexist without interference.

## Operations Exclusive for Alarm Input

### Bypass/Restore Bypass Alarm Input

When an exception of alarm input occurs, and other alarm inputs can work normally, click to bypass the abnormal alarm input, otherwise, you cannot arm the security control partition which the alarm input belongs to. When a bypassed alarm input works normally, click to restore bypass.

### View Alarm Input Status

In the **Status** column, the alarm input's online status, arming status, bypass status, alarm status, fault status, and detector connection status are displayed.

- **Online Status**: indicates alarm input online; indicates alarm input offline.
- **Arming Status**: indicates alarm input armed; indicates alarm input disarmed.
- **Bypass Status**: indicates alarm input bypassed; indicates bypass restored.
- **Fault Status**: indicates alarm input exception.
- **Alarm Status**: indicates that the alarm input is alarming.
- **Detector Connection Status**: indicates alarm input not enrolled or offline; indicates detector online.
- **Battery Status**: indicates normal alarm input's battery status; indicates abnormal alarm input's battery status.

## Operations Exclusive for Alarm Output

### Batch Set Alarm Output Duration

Select multiple alarm outputs, click **Alarm Output Duration**, and set the duration (sec).

### Batch Turn On/Off Alarm Outputs

Select multiple alarm outputs and click **Open/OFF**.

## Operations Exclusive for Optical Fiber Unit

On the optical fiber unit list page, you can perform the following operations:

### Get Configuration

Get an optical fiber unit's name, type, latitude and longitude, sensitivity, and intelligent algorithm enabling status.

### Link to Camera

Link selected optical fiber units with up to four cameras that capture pictures once the optical fiber unit triggers any alarm. For PTZ cameras, preset can be linked. You can define the analysis

area to focus on key zones and adjust the classification threshold to reduce false alarms caused by light interference

For details, see ***Parameters on Edit Optical Fiber Unit Page*** .

**Locate Unit on Map**

Calibrate optical fiber units on the GIS or a static map by drawing vertex to align units with geographical coordinates, enabling accurate monitoring and efficient response.

### Operations Exclusive for Security Radar

On the Security Radar list page, you can perform the following operations:

**Arm on Map**

Calibrate devices' location (via GIS map or on a static map) and orientation for accurate target display, and draw zones or trigger lines to define monitoring boundaries and reduce false alarms.

## 4.5 Edit Element in Area

You can edit the area's added elements, such as recording settings, event settings, and map settings for cameras, application settings, hardware settings, and so on.

Select an area on the left and a device type on the top.

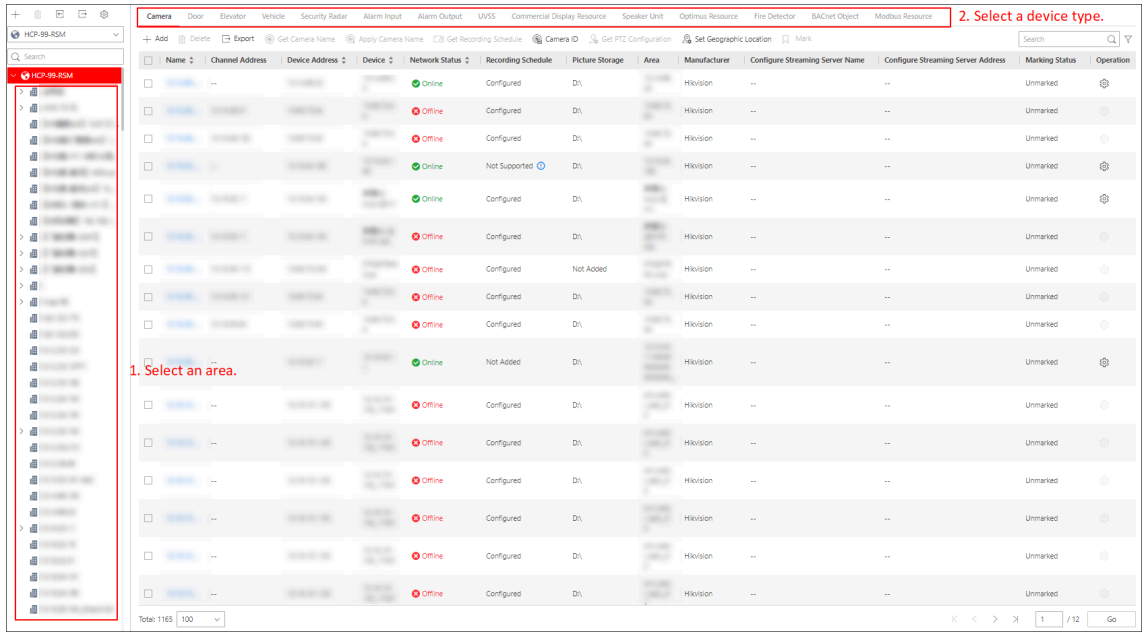



**Figure 4-4 Select Area and Device Type**

In the top left corner of Home page, select → **Basic Management** → **Device** → **Area** . Then select a site from the drop-down site list to show its areas, and select an area below.

**Note**

- The icon indicates that the site is the current site.
- The icon indicates that the site is a Remote Site.

### 4.5.1 Parameters on Edit Camera Page

**For Current Site**

## Basic Information

**Live View**

Click to view the live view of the camera and click again to switch to playback.

**Note**

- Click to refresh the live view.
- For cameras accessed via ONVIF protocol, you can set the main and sub-stream.

**Location Calibration**

For forest fire detection cameras (quickly detect and accurately locate fires, reducing fire losses), supports adding or editing calibration points (requiring coordinate verification) to correct installation deviations from true north.

**PTRZ Control**

For PTRZ cameras, it supports **PTRZ control**, including rotation, speed adjustment, zoom in/out, etc.

## Recording Settings

**Note**

The parameters vary according to the site (current site or Remote Site) you selected previously.

**Auxiliary Storage**

Switch on to configure another storage location for the video files.

**Note**

- If CStor, CVR (Hybrid SAN), pStor, or SAC is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded video files or select **Scheduled Copy-Back** to copy

recordings from the encoding device or pStor (main storage) to specified auxiliary storage location according to the scheduled period.

- Before setting **Scheduled Copy-Back**, make sure you have configured real-time recording schedule stored in device local storage or pStor for the main storage.
- The recordings can be copied only from the encoding device to CVR (Hybrid SAN), CStor, pStor or SAC, or from pStor to another pStor.

**Get Device's Recording Settings**

Get recording schedules of the device.

**Storage Location**

If you select **Encoding Device** as the storage location, you needn't select the storage type.

If you select **CVR (Hybrid SAN)**, **CStor**, **pStor**, or **SAC**, specify a server and (optional) select a Streaming Server to get video streams from cameras via it.

When the storage location is set to pStor and the device supports third stream, the **Stream Type** can be selected as third stream.

**Storage Type**

**Real-Time Storage**

Store the recorded video files in the specified storage location in real time.

**Scheduled Copy-Back**

Copy the recorded video files from the encoding device or pStor to the specified storage location according to scheduled period.

**Note**

The recordings can be copied only from the encoding device to CVR (Hybrid SAN), CStor, pStor or SAC, or from pStor to another pStor.

**Recording Schedule Template**

Set the template which defines the time periods to record the camera's video.

**All-Day Time-Based Template**

Record the video for all-day continuously.

**All-Day Event-Based Template**

Record the video when alarm occurs.

**Add**

Set the customized template.

**View**

View the template details.

**Upload Time**

Specify the time period to copy the recorded video files to the specified storage location.

**Recording for Copy-Back**

Select the type of recorded video file to backup. The event-based recording schedule can not be configured for the **Cluster Storage**, and the command-based recording schedule can not be configured for the **Cluster Storage** and **pStor**.

**Stream Type**

Select the stream type as main stream, sub-stream or dual-stream.

**Note**

For storing on CVR (Hybrid SAN), CStor, pStor or SAC, dual-stream is not supported.

**Pre-Record**

Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

This field displays when the storage location is set as Encoding Device, CStor, pStor or SAC. And it is available for the camera that is configured with event-based recording.

**Post-Record**

Record video from periods following detected events.

This field displays when the storage location is set as Encoding Device or CVR (Hybrid SAN). It is available for the camera that is configured with event-based recording.

**Video Expiry Time**

If you select **Encoding Device** as the storage location, switch on **Video Expiry Time** and enter expiration day(s).

Automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period to keep the videos as desired and the actual retention period for the videos depends on the allocated quota.

**Enable ANR**

If you select the **Encoding Device** or **CVR (Hybrid SAN)** as the storage location, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

**Max. Copy-Back Speed (KBps)**

Enter the maximum copy-back speed.

## Smart Functions

Enable **AcuSeek** / **AcuSearch** / **Smart Search** to enable these capabilities for the device.
When using the intelligent analysis server for AcuSeek analysis, it is necessary to select the associated intelligent analysis server for the camera.

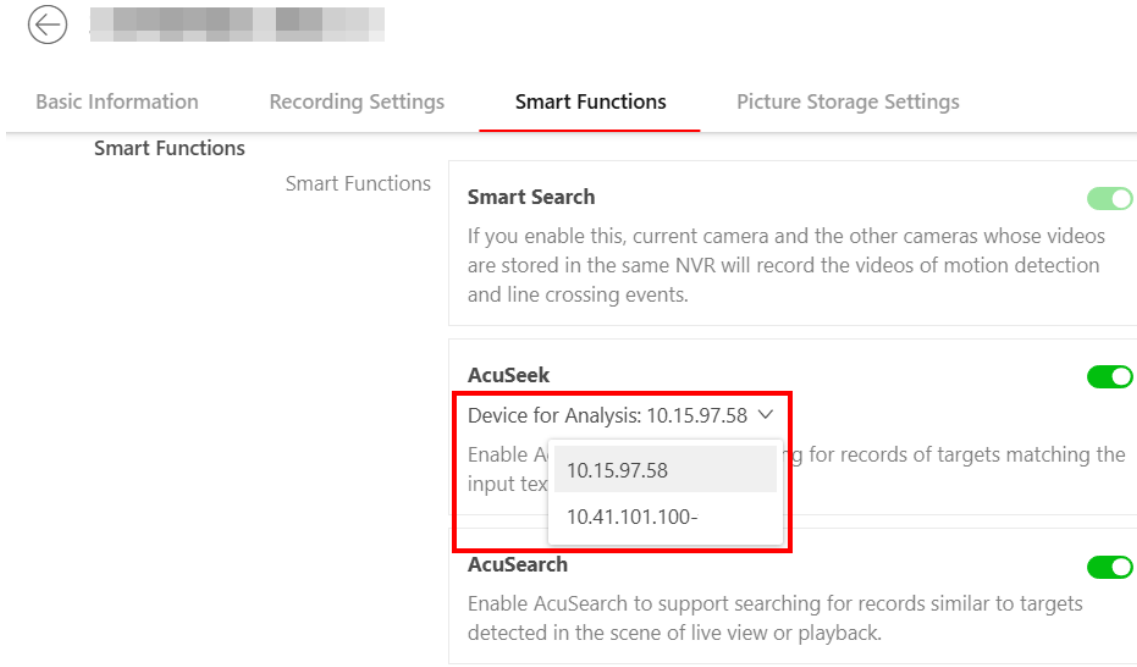



**Figure 4-5 Select an Intelligent Analysis server**

## Picture Storage Settings

- If you select System Management Server, the pictures will be stored on the SYS server. Click **Configure** to view the disk on SYS server and storage quota, which can be edited via the Web Client running on the SYS server. Refer to ***Set Storage on System Server*** for details.
- You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

## For Remote Site

If you are using a Central System with a Remote Site Management module, you can edit the cameras, doors, and elevators that have been added to the Remote Site.

**Parameters on Edit Camera Page**

**Basic Information**

**Name**

If you change the camera's name, you can click on the added camera list page to apply the new name to the device.

**Live View**

You can view the live view of the camera and hover over the window and click in the lower-right corner to switch to playback.

**Note**

Double authentications is required for live view and playback on the camera editing page. For details about configuring double authentications, refer to ***Set Basic Security Parameters*** .

**Recording Settings**

For recording settings, if no recording settings have been configured for the camera, click **Configuration on Site** to set the parameters.

## 4.5.2 Parameters on Edit Door Page

**Basic Information**

**Name**

Edit the name for the door.

**Note**

If you change the name, you can click in the door list page to apply the new name to the device.

**Door Contact**

The door contact's connection mode.

**Exit Button Type**

The exit button connection mode.

**Lock Door when Door Closed**

If it is enabled, the door will be locked once the door magnetic is closed. If there is no door magnetic, the door will be locked after the extended open duration ends.

**Note**

This function should be supported by the device.

**Open Duration**

The time interval between unlocking and locking the door again.

**Extended Open Duration**

The time interval between the door is unlocked and locked again for the person whose extended access function is enabled.

**Door Open Timeout Alarm**

After enabled, if the door has been configured with the event or alarm, when the door contact open duration has reached the limit, the event or alarm will be uploaded to the system.

**Duress Code**

If you enter this code on the card reader keypad, the Control Client will receive a duress event. It should be different from the super password and dismiss code.

**Super Password**

If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different from the duress code and dismiss code.

**Dismiss Code**

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different from the duress code and supper password.

**Link Camera**

Link cameras to the door, and you can view its live view, recorded videos, and captured pictures via the Control Client.

**Note**

- Up to 2 cameras can be linked to one door.
- You can click ↑ or ↓ to adjust the priority of cameras.
- You can switch on **Auto Capture** to enable automatic capture of the camera.

**Picture Storage**

Switch on and select a storage location from the drop-down list.

**Note**

If an error occurs during picture storage configuration, ⊙ appears on the right of the door name.

**Card Reader**

**Min. Card Swipe Interval**

After it is enabled, you cannot swipe the same card again within the minimum card swiping interval.

**Reset Entry on Keypad After(s)**

Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.

**Failed Card Attempts Alarm**

After it is enabled, if the door is configured with event or alarm, when the number of excessive failed card swiping attempts has reached the limit, the event or alarm will be uploaded to the system.

**Tampering Detection**

After it is enabled, if the door is configured with device tampered event or alarm, when the device body or panel is taken apart, the alarm will be triggered and sent to the system.

**OK LED Polarity**

Only supported when the device is connected via Wiegand interface. The polarity for OK core wire connection on the card reader mainboard.

**Error LED Polarity**

Only supported when the device is connected via Wiegand interface. The polarity for ERR core wire connection on the card reader mainboard.

**Face 1:N Matching Threshold**

Set the threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate. The maximum value is 100.

**Face Recognition Interval**

The time interval between continuous face recognition twice when authenticating.

**Face Anti-spoofing**

If it is enabled, the device can recognize the live face. Also, you can check **Protect Sensitivity of Face Anti-Proofing**, and set the face anti-spoofing security level.

**Face Recognition Application Mode**

Select **Indoor** or **Others** according to actual environment.

**Face Recognition Terminal**

For a turnstile or an access controller of certain types, switch on **Face Recognition Terminal** and add face recognition terminals to link with the selected turnstile.

**Copy To**

Click **Copy To** in the upper right corner to apply the current settings of the door to other door(s).

**Name**

For Remote Site, you can click a device name to edit the name.

## Parameters on Edit On-Board Monitoring Vehicle Page

In the Device module, click **Area → Vehicle** .

**Vehicle Icon**

The platform provides default icons for different vehicle types. You can also upload custom icons for different vehicle types. On the real-time monitoring page of On-Board Monitoring module, these icons can be displayed for distinguishing vehicle types.

Click **Icon Settings** to open the Vehicle Icon Settings pane. Select a vehicle type to expand, click **Add** to pop up a window where you can enter the icon category name and click + to upload pictures as the icons for statuses including **Normal**, **Alarm**, and **Offline**.

### 4.5.3 Parameters on Edit Speaker Unit Page

**Link Camera**

**Priority**

Click ↑ or ↓ to adjust the displaying sequence of the cameras.

### 4.5.4 Parameters on Edit Optical Fiber Unit Page

**Application Configuration**

**Intelligent Algorithm**

The intelligent algorithm will analyze false alarms to filter out interference caused by environmental factors (e.g., wind, rain, snow).

**Camera Linkage**

Configure camera linkage to enhance analysis in complex scenarios and reduce false alarms from environmental interference.

1. **Select Camera**.
2. **Select Preset & Set Preset Capture Delay Time**: Choose a predefined preset and define a delay (in seconds) after the camera moves to the preset position. This ensures the image stabilizes before analysis begins.

   **Note**

   The feature is only available for PTZ cameras.
3. **Draw Analysis Area**: Specify the region within the camera's view where the DeepinMind should perform analysis. This narrows the focus to critical zones.
4. **Adjust Classification Threshold**: Configure the classification threshold to reduce light interference and improve analysis accuracy. A higher value results in fewer alarms.

### 4.5.5 Edit Alarm Input/Output in an Area

You can click an alarm input/output name in the **Name** column to enter the Edit Alarm Input page and edit the alarm input/output name.

## 4.6 Remove Element from Area

Select a device type tab to show the added elements. Then select the elements below and click 🗑 to remove the elements from the area.

**Note**

- If you are using a Central System with a Remote Site Management module, you can remove only the cameras, doors, and elevators that have been added from the Remote Site.
- If ⊗ appears near the camera name, it means the camera has been deleted from the Remote Site. Hover the cursor over the ⊗ and click **Delete** to delete the camera from the area.

# Chapter 5 Person Management

You can add person information to the platform for further operations such as access control (linking a person to an access level), face picture comparison (adding a person to a face picture library), time and attendance (assign a schedule to a person), etc. After adding the persons, you can edit and delete the person information if needed.

On the top left, select → **Basic Management → Person** to enter the Person module.

## 5.1 Add Departments

When there are a large number of persons managed in the platform, you can put the persons into different departments. For example, you can group employees of a company to different departments.

**Steps**

1. Select **Person Management → Person** on the left navigation bar of Person module.
2. Click + at the top of the department list to enter the Add Department page.
3. Set the department information, including the parent department, department name, and description.

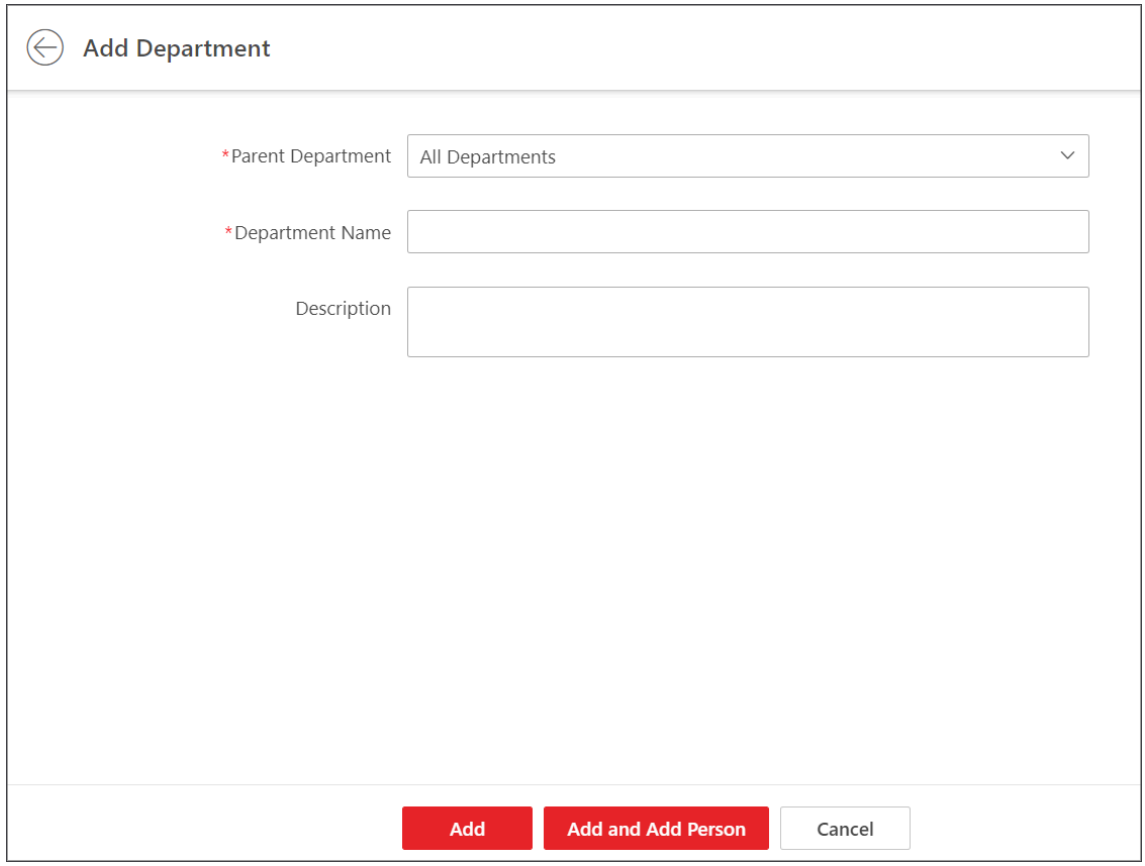



**Figure 5-1 Add Department**

4. Add department.
   - Click **Add** to add the department and go back to the person management page.
   - Click **Add and Add Person** to add the department and enter the Add Person page.
5. **Optional:** If your HikCentral Professional License contains the permission to access the Access Control module, set parameters of authentication via PIN code.
   1) Click ⚙ to open the Set Authentication via PIN Code window.
   2) Switch on **Authenticate via PIN Code**.

   **Note**

   - When enabled, if the authentication mode of the card readers at the access points is also set to **Authenticate via PIN Code**, all the added persons are allowed to use their PIN codes alone as the credential for access authentication.
   - When enabled, no duplicated PIN code is allowed.
   - You can set a PIN code for a person when setting basic information for the person. For details, see ***Add a Single Person Manually*** .

   3) Set the PIN code update mode.

   **Auto**

The platform will automatically reset all persons' PIN codes and apply the reset PIN codes to the access control devices. The system administrator needs to notify all users of the updated PIN codes.

**Manual**

The system administrator needs to manually filter out persons who have no PIN code or have duplicated PIN codes, change their PIN codes and then notify them of the updated PIN codes.

**Note**

The system administrator needs to notify relevant persons of the updated PIN codes in time. Otherwise these persons' access authentication and attendance results will be affected.

6. **Optional:** Perform the following operations after adding departments.

| | |
|---|---|
| **Edit Department** | Select a department, and click at the top of the department list to edit the parent department, department name, or remarks. |
| **Delete a Department** | Select a department and click at the top of the department list to delete the selected one.<br>**Note**<br>The root department cannot be deleted. |
| **Delete All Departments** | Click beside at the top of the department list to delete all added departments. |

## 5.2 Basic Configuration Before Managing Persons

The following configurations are preparations before managing persons.

### [Important] Set Person ID Rule

**Note**

Once a person is added to the platform, the ID rule will be **not configurable**, so we recommended that you should ensure the ID rule at the very beginning.

In the Person module, select **Basic Configuration → Person ID Rule** on the left. Set the total ID length, and select the ID generation mode, finally save the settings.

### Customize Additional Information

Customize a person's basic information by adding additional items as either custom private or custom public information. The former refers to private information such as the person's salary. The latter refers to public information such as the person's department and occupation. When an

additional information item is added, it will be displayed as an configuration option on the Basic Information tab of the Add Person page.
Select **Additional Information** on the left, and then click **Add**. In the pop-up window, enter the following parameters and save.

**Type**

Select the type to restrict the format of the contents of the item.

**Sharing Property**

Click **Private** or **Public** to set the sharing property of the contents of the item.

For example, if you select **General Text**, enter the text when adding a person. If you select **Date**, setting date as the content of the item is required when adding a person (see the figure below).

### Unauthorization Settings

**Auto Unauthorize Inactive Person**

If a person has no access records for the configured duration, he or she will be disabled.

In the Cause of Unauthorization area, click **Add** to add a custom cause. You will be required to select a cause when unauthorizing person(s).

### Admin Authorization Settings

Enable the **Admin Authorization Required for Deleting Department and Person** and you will be required to enter the Administrator's login password when deleting any departments or persons.

### Person Expiration Settings

The platform will automatically send expiration notification emails to persons close to expiry or employees close to self-service password expiry based on the configuration. Go to **System → Email → Expiry Notification Email Template → Employee Self-Service Login Password Expiry / Person Effective Period Expiry** to configure the email template.

## 5.3 Add Person

Multiple methods are provided for you to add persons to the platform. You can add a person manually. If you want to add multiple persons at a time, you can import persons by downloading and filling in a template or import persons from devices. In addition, you can batch import domain persons.

You can perform the following operations for adding persons.

If you have enabled the **Use This Device as Registration Device** function on the device's configuration page, the information about added persons and credentials, edited credentials on the device will be automatically synchronized to the platform.

### 5.3.1 Add a Single Person Manually

You can manually add a person to the platform by setting the person's basic information, credential information, and other information such as the person's access level. The above-mentioned person information constitutes the data basis for the applications related to identity authentication of the person, such as the access control application, the elevator control application, the attendance management application, and the video intercom application.

**Note**

Before adding persons to the platform, you should confirm and set the person ID rule. As once a person is added, the ID rule cannot be edited any more. For more about the ID rule settings, refer to ***Basic Configuration Before Managing Persons*** .

On the Person page, select a department from the department list on the left. Then click **Add** above the person list to enter the Add Person page.

#### Basic Information

Set the person's basic information, such as ID, department, first name, and last name.

**ID (Required)**

The default ID is generated by the platform. You can edit it if needed.

**Profile Picture**

See ***How to Collect a Profile Picture*** .

**Effective Period (Required)**

Set the effective period for the person in applications such as access control application and time & attendance application, to determine the period when the person can access the specified access points with credentials.

Click **Extend Effective Period** to show a drop-down list and select **1 Month / 3 Months / 6 Months / 1 Year** to quickly extend the effective period based on the configured end time. For example, if the period is from ***2021/10/23 13:30:00*** to ***2022/01/20 14:10:00*** and the extended time is selected as **1 Month**, the end time of effective period will change to ***2022/02/20 14:10:00***.

**Date of Employment**

The start date of employment for the person.

**Allow Login to Self-Service**

Switch on **Allow Login to Self-Service** and set a password to allow employees to log into the platform as an employee. On the Login page, employees select the **Self-Service** tab, and enter the employee ID and password to log in.

**Credential Management**

Add credential information for the person. See ***Manage Credentials for a Single Person*** for details.

## Access Level

Click **Access Level** tab, and assign access levels to the person to define the access points where the person can access during the authorized period.

**Super Access Permission**

Persons with this permission will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first person authorization.

**Extended Access**

When the person accesses the door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

**Note**

The extended access and super user functions cannot be enabled concurrently.

**Device Administrator**

Determine if the person has the administrator permission of access control devices.

If the check-box is checked, when you synchronize person information from access control devices, the administrator permission for the person will be retained.

**PIN Code**

If you have enabled the function of automatically generating PIN for persons, the platform will generate a PIN automatically. You can click **Auto Generate PIN** to generate a new PIN. In most cases, the PIN code cannot be used as a credential alone: it must be used after card or fingerprint when accessing; It can be used alone only when **Authenticate via PIN Code** is enabled on the platform and the authentication mode of the card readers is also set to **Authenticate via PIN Code**.

- The PIN code should contain 4 to 8 characters.
- For details about enabling **Authenticate via PIN Code** on the platform, see ***Add Departments*** .

**Assign Access Level**

Assign the permission for specified access points. You can click to view information on access points and access schedules.

## Schedule

Click **Schedule** tab, view and edit the schedule of the person in the table.

**Allow Check-In/Out via Mobile Client**

Switch on it to allow the person to check in/out via the Mobile Client.

**Allow Vehicle Attendance Check**

With this parameter checked, once the person accesses the campus by license plate No., the system will automatically check in for the person.

**Attendance Group**

Select an attendance group from the drop-down list. For details, refer to ***Add an Attendance Group*** .

**Leave Rule**

Select a leave rule for the person. For details, refer to ***Add a Leave Rule*** .

**Schedule Overview**

View the schedule of the person. You can click **Set Schedule** to set a schedule for the person. For details, refer to ***Assign Schedule to Person*** .

## Face Picture Library

On the **Face Picture Library** page, select a face picture library for the person. The person's profile picture will be added to the face picture library for comparison.

## Alarm Detection

On the **Alarm Detection** page, enable **Configure Operation Permission of Security Control Device**. Click **Add** to select device and configure operation permissions including **Arm**, **Disarm**, and **Auto Control** for selected device(s).

**User Property**

**Lifetime**

All permissions can be configured for the user.

**One-Off**

Expires after either a single arming or disarming action, or expires automatically after a 24-hour period. No duress code permission. No Keyfobs and tags permission.

**Keypad Password**

Only 4 to 6 digits are allowed.

**Duress Password**

Only 4 to 6 digits are allowed. One-Off users do not need to configure the duress password.

## Portable Enforcement

On the **Portable Enforcement** page, change the body camera password, click **Add** to link the body camera to a dock station, enable **Link to Portable Device for Receiving**.

## Resident Information

On the **Resident Information** page, set resident information to link the person with the indoor station and floor and room number.

**Note**

- Make sure you have added indoor stations to the platform.
- When you select an indoor station, the room number of the indoor station will be filled in automatically in **Room**. You can edit the room number.
- Up to 10 persons can be linked with one indoor station. And a person cannot be linked to multiple indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

## Vehicle Information

In the Vehicle area, add the vehicle information for the person.
After topping-up, the parking access permission will automatically show in the Parking Lot area.

## Emergency Counting Group

In Emergency Counting Group area, select an emergency counting group to add the person to it, or click **Add Emergency Counting Group** and enter a group name to create an emergency counting group and add the person to it.
When the platform is in emergency status, it is not allowed to add a person to an emergency counting group.

## Skin-Surface Temperature

Enter the person's skin-surface temperature and select the corresponding temperature status. For example, if a person's skin-surface temperature is 37 °C, then you can select her/his temperature status as normal.

## Additional Information

On the Additional Information tab, enter additional information to be applied, or select a public digital signage additional information. You can create additional information if there is not any additional information in the system.

## Platform User

**Add New User**

Create a new user and link it with the person.

**Select Existing User**

Link an existing user with the person.

### 5.3.2 Batch Add Persons by Template

You can batch add persons to the platform with the minimum effort by importing a template (an Excel file) which contains the person information such as the names of the department and the access levels.

**Steps**

1. Select **Person Management → Person** on the left.
2. Click **Import → Import Person Information via Excel** .

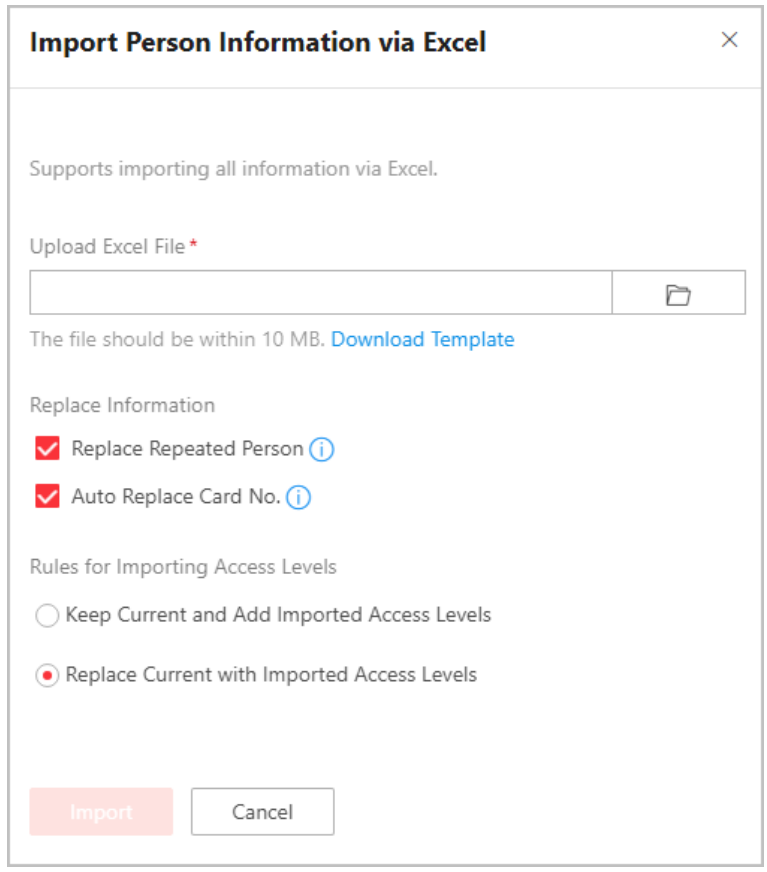



**Figure 5-2 Batch Add Persons by Template**

3. In the pop-up window, click **Download Template**.
4. Check the basic information items you want to include in the template, such as person type, card No., and email. You can also check custom additional information items.
5. Click **Download** to save the template to your PC.
6. In the downloaded template, enter the person information following the rules shown in the template.

   If you need to link a person to the indoor station, you should enter Community-Building No.-Unit No.-Room No. in the **Room No.** column.

7. Click , and then select the template (with person information) from your PC.
8. **Optional:** Check **Replace Repeated Person** to replace the person information if the imported ID repeats.

   **Keep Current and Add Imported Access Levels**

   The existing access levels will be kept and the new access level will also be assigned to the person.

   **Replace Current with Imported Access Levels**

   The existing access levels will be replaced with the imported access levels.
9. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if the imported ID repeats.
10. Click **Import** to start importing.

**Note**

- The importing process cannot be stopped once started.
- You can batch issue cards to the persons by importing the template with card No. information.

The importing progress shows and you can check the results.

**Note**

You can export the person information that failed to be imported, and try again after editing.

### 5.3.3 Import Domain Persons

You can import the users in the AD (Active Directory) domain to the platform as persons. After importing the person information (including person name and account name) in the AD domain, you can set other information for the persons, such as credentials.

**Before You Start**

Make sure you have configured the active directory settings. See ***Set Active Directory*** for details.

**Steps**

1. On the Person page, click **Import → Import Person Information via Domain Group** .
2. Select the importing mode.

   **Import Domain Persons**

   Import specified persons. Select the organization unit and select the persons under the organization unit which are displayed in the Domain Person list on the right. The person information will be synchronized based on each person.

   **Import Domain Organization Unit and Person**

   Import all the persons in the organization unit. The person information will be synchronized based on each group.

**Note**

The platform does not support this function if the Azure domain is configured.

**Person in Security Group**

Import the selected security groups in the AD domain.

3. When selecting **Import Domain Persons** or **Person in Security Group** as the importing mode, select a department to which the selected items (persons or security groups) need to be imported.
4. Set the effective period for the persons as needed.
5. **Optional:** Enable **Add Imported Persons as Users** and select a role for the users from the Linked Role drop-down list.
6. **Optional:** Check **Use Domain Password as Body Camera Login Password**.
7. Click **Import**.

**Note**

- If the profile picture/email in the domain is linked to the profile picture/email in the platform, the persons' profile picture/email will be imported to the platform from the domain as well. You can view the profile picture/email on the person details page but you cannot edit it. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .
- If the profile picture/email in the domain is NOT linked to the profile picture/email in the platform, you can take a picture or upload a picture as the person's profile picture and enter the email address. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .

### 5.3.4 Import Persons from Device

Import persons information to the platform from devices, including access control devices, video intercom devices, or enrollment station.

On the Person page, click **Import → Import Person Information from Device** to open the Import from Device pane. Select the **Device Type** as **Access Control Device** / **Video Intercom Device** / **Enrollment Station**.

**Note**

When importing, the platform will compare person information on the device with person information in the platform based on the person name. If the person name exists on the device but does not exist in the platform, the platform will create a new person. If a person name exists on both sides, the corresponding person information in the platform will be replaced by the one on the device.

## Import Persons from Access Control Devices or Video Intercom Devices

If the added access control devices and video intercom devices have been configured with person information, you can get the person information from these devices and import it to the platform. The person information that can be imported includes person names, profile pictures, credentials (PIN codes, cards, and fingerprints), effective periods, person roles, etc.

**Importing Range**

**Import All Persons**

Import all the persons stored in the selected devices.

**Import Specified Persons**

Specify the ID of up to 5 persons and import the persons to the platform.

**Select Department**

Select a department to which the persons will be imported.

**Replace Profile Picture**

Replace existed profile pictures with the new ones from the devices.

If the following window pops up, select a method to import the person information.

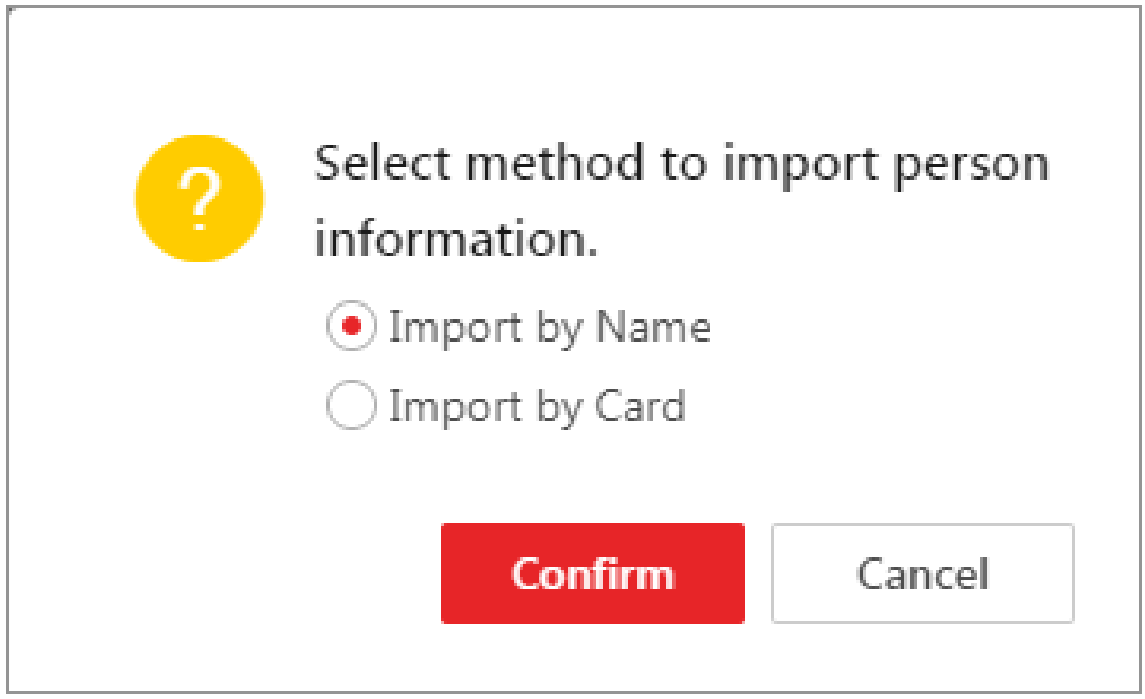



**Figure 5-3 Select an Import Method**

**Import by Name**

The person information directly linked to the access control devices will be imported.

**Note**

This method is usually used for the access control devices with facial recognition capability.

**Import by Card**

The person information linked to the cards of the access control devices will be imported

**Note**

This method is usually used for the access control devices which link person information via cards.

## Import Persons from Enrollment Station

You can apply the required person information to an enrollment station via a template or the person list on the platform, and then enroll the persons' credentials via the enrollment station. Once you complete the enrollment, you can import the person and credential information from the enrollment station to the platform by specifying the IP address, port number, user name and password of the device to allow the platform to access it.
Before application or importing, configure access mode, access protocol, address, port No., user name, and password of the enrollment station to link the platform to it.
Then, select the Stage as **Apply Person Information**.

**Import from Template**

If the persons are not added to the platform, download the template from the enrollment station and then edit the template and apply it to the enrollment station for enrolling the persons' credentials.

**Import from Person List**

If the persons have been added to the platform, select the department to apply the persons to the enrollment station for enrolling the persons' credentials.

Enroll person credentials, and select the Stage as **Copy Back Person and Credential Information**.
Select a department and click **Import**.

## 5.3.5 Operations Available on Person List

For added persons, you can perform the following operation(s).

| | |
|---|---|
| Edit Person | Click the person name to edit the person details. |

| | |
|---|---|
| | **Note**<br>When editing the person's effective period, if you have issued temporary card(s) to the person, make sure the expiry date(s) of the person's temporary card(s) are within the effective period. |
| Delete Persons | Check the person(s) and click **Delete** to delete the selected person(s).<br>Hover the cursor onto beside **Delete**, and then click **Delete All** to delete all persons. |
| Clear All Profile Pictures | Hover the cursor onto beside **Delete**, and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures. |
| Export Person Information | Click **Export → Export Person Information** , select the **Exporting Range**, and check information types you need to export person information to your PC. For information security, you need to enter your login password to authenticate. |
| Export Profile Pictures | Click **Export → Export Profile Picture** , select the **Exporting Range**, enter your login password and a password for decompressing the ZIP file, and click **Export**.<br>**Note**<br>Before using this function, you should activate this function first by going to **General → System Configuration → Security → Export Profile Pictures** page and checking the **Export Profile Pictures**. |
| Set Persons as Head of Department | Check one person, hover the cursor on **Set as Head of Department**, and select **Set as Head of Department**. |
| Adjust Department of Persons | Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed.<br>1. Select one or more persons, click **Adjust → Adjust Department** .<br>2. Select the target department to which the persons are about to be moved.<br>3. Click **Move**. |
| Adjust Effective Period | 1. Select one or more persons, click **Adjust → Adjust Effective Period** .<br>2. Select the effective period from the drop-down list.<br>3. Click **OK**. |
| Turn Persons as Resigned | 1. Select one or more persons, click **Adjust → Resigned** .<br>2. Set the departure date, resignation type, and reason. |

| | |
|---|---|
| | 3. (Optional) Select whether to stop calculating persons' attendance results, or whether to remove persons' access levels immediately.<br>4. Click **OK**. |
| Manage Persons' Cards | See ***Card Management*** . |
| Synchronize Domain Persons | Select person(s) whose information has changed in the AD domain and click **More → Synchronize Domain Persons** at the top of person list to get the latest person information. |
| Link Persons to Indoor Stations | Select one or more persons, and click **More → Link to Indoor Station** , then select an indoor station for each person to apply the person information to the indoor station.<br>**Note**<br>• A pop-up window will appear after you click **Save**. Click **Yes** to save the indoor station's room number as the room number, or click **No** to keep the old room number (if there is not an old room number, the room number of the indoor station you select will be saved).<br>• Make sure you have added indoor stations to the platform.<br>• Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.<br>• Make sure the room number is consistent with the actual location information of the indoor station. |
| Unauthorize/Restore Persons | Check one or more persons, click **More → Unauthorize Person** , and select a cause to disable selected person(s).<br>Check one or more persons, click **More → Restore Person** . |
| Clear Access Levels | Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons.<br>**Note**<br>The access levels of these persons cannot be restored once they are cleared. |
| Check Person Authorization | Select one or more persons, click **More → Check Access Levels of Person** to enter Check Person Authorization page. On the page, you can test whether the person's access levels and credentials are applied to the access control devices, elevator control devices, and video intercom devices. If failed to be applied, you can apply them again. |

| | |
|---|---|
| Attendance Settings | Select one or more persons, click **More → Attendance Settings** , and select to enable/disable the Check-In/Out via Mobile Client and Vehicle Attendance functions.<br>**Check-In/Out via Mobile Client**<br>After enabling this function, the selected person(s) can check in/out via the Mobile Client.<br>**Vehicle Attendance**<br>After enabling this function, once the person accesses the campus by license plate No., the system will automatically check in for the person. |
| Unlock Users | For persons whose account is locked due to too many failed attempts for login, Administrators can unlock their accounts for login. On the top, click **More → Unlock for Login** , check persons, and click **Unlock**. |
| Assign Person to a Remote Site | Application scenario: residential district; cross-city / multinational enterprise<br>The central Administrator can assign person(s) to a remote site so that the Administrator of the remote site can edit information about the person(s) such as editing credentials, issuing cards, editing vehicle information, etc. The changed information takes effect after the approval of the central Administrator. Information about deleted persons in remote sites cannot be edited before the deleting is approved by the central Administrator. |
| Copy Back Person to Central System | After editing person information in the remote site, you can check the changed persons and click **Copy Back Person to Central System** for review. Once approved by the admin in the Central System, the edited person information will be displayed in the Central System. |

## 5.4 Credentials Management

Before credential management, you can configure PIN rules and QR code mode.

In the left navigation bar of the Person module, click **Basic Configuration → Credential Settings** .

- PIN Rule
  **Auto Generate PIN for Person**: Enable this function so that you do not have to manually set PINs for newly-added persons. On the **PIN Rule** tab, check **Auto Generate PIN for Person**, select the **PIN Digits** and save.
- QR Code Mode
  **Set QR Code Mode**: You can select static QR code or dynamic QR code for employees or visitors. If you select dynamic QR code, the platform will generate a dynamic QR code for persons on the platform. Every time the employee uses the QR code to authenticate, the platform will invalidate

the current QR code in use. While static QR code will stay unchanged. The card in the personnel credential list does not display the QR code information.
On the **QR Code Mode** tab, select a QR code mode, and set the QR code validity period if you select **Dynamic QR Code**.
QR code updates can occur in three ways:

- Manually Update: The user actively updates the QR code.
- Automatic Update: The QR code will be refreshed once it has reached its pre-set expiration time.
- Update Upon App Re-entry: The QR code will be refreshed when the user re-enters the application.

### 5.4.1 Manage Credentials for a Single Person

When adding a person, you can add the required credential information for the person. The supported credentials include normal cards, profile pictures, fingerprints, palm prints/veins, and keyfobs. These credentials can be used for the access authentication in applications such as access control and elevator control.

You can add or change credentials on the Add/Edit Person page and the Person List.

- On the Add/Edit Person page, you can collect or add a profile picture, and click **Credential Management** to add other credentials such as cards, palm prints, and palm veins.

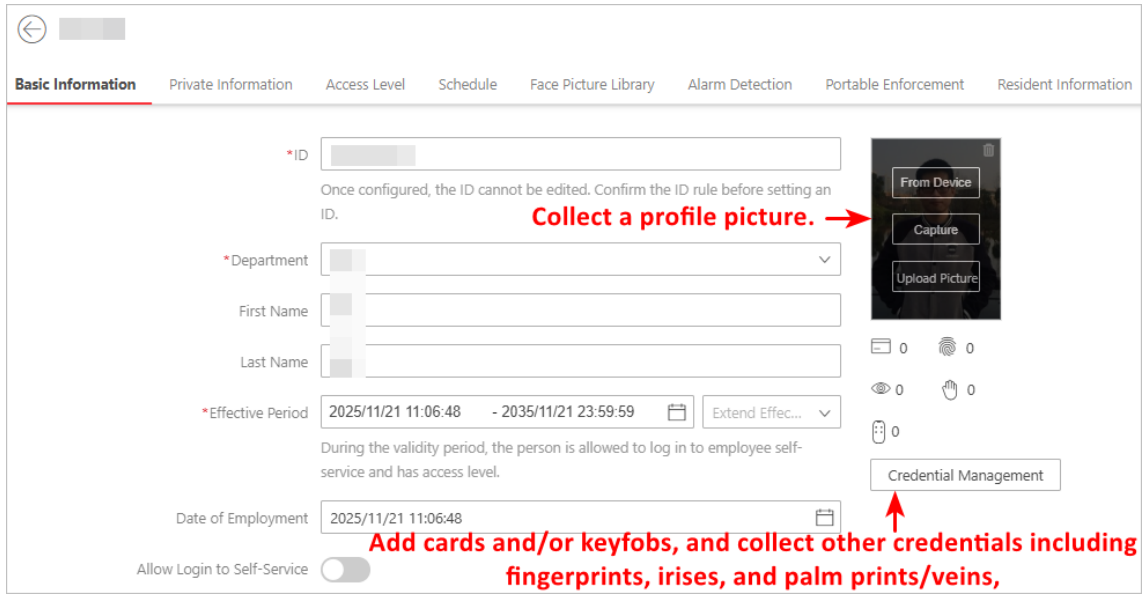



**Figure 5-4 Edit Person Page**

- On the Person List page, credentials (including cards, fingerprints, irises, palm prints/veins but profile pictures) are displayed in the Credential Information column. You can view numbers of them, or click their icons to view details or add one credential.

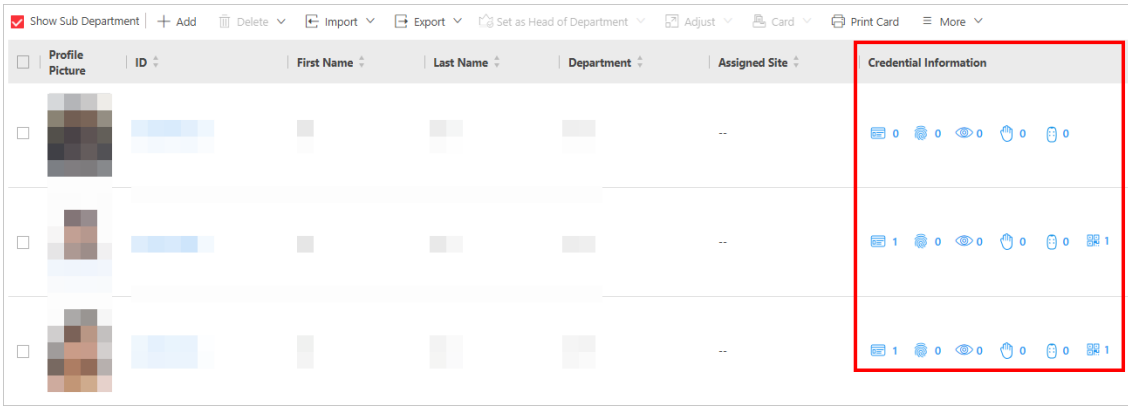



**Figure 5-5 Credential Information on Person List**

## How to Collect a Profile Picture

On the Add/Edit Person page, hover the cursor on , and select from three modes to add a profile picture.

**From Device**

This mode is suitable for non-face-to-face scenario when the person and the system administrator are on different locations.

**Note**

- For video intercom devices, door stations and outer door stations are supported.
- For enrollment stations, you need to set related parameters, including access mode, access protocol, device address, port, user name, password, face anti-spoofing, and security level.

**Capture**

Click **Capture** and then select one of the PC's webcams to take a picture.

**Upload Picture**

Click **Upload Picture** to select a picture from your PC. On top of the Upload Picture window, click **Detect Now** and select a device type and device to detect the face picture quality.

**Note**

- It is recommended that the face in the picture be in the full-face view directly facing the camera, without a hat or head covering.
- You can drag the picture to change its position or zoom in/out before cutting it.

**Note**

If you add a smart terminal to the platform, the smart terminal will automatically create models for the profile picture.

## How to Generate a QR Code for a Person

The QR code of card is only displayed when you set the QR code mode to static QR code.
A QR code will be generated automatically after adding a card and the icon will appear in the top right corner of the card area when you enter the Add Credential page from the editing person page. You can click to view and scan the QR code or click **Download** to download the QR code picture to the local storage for further operations.

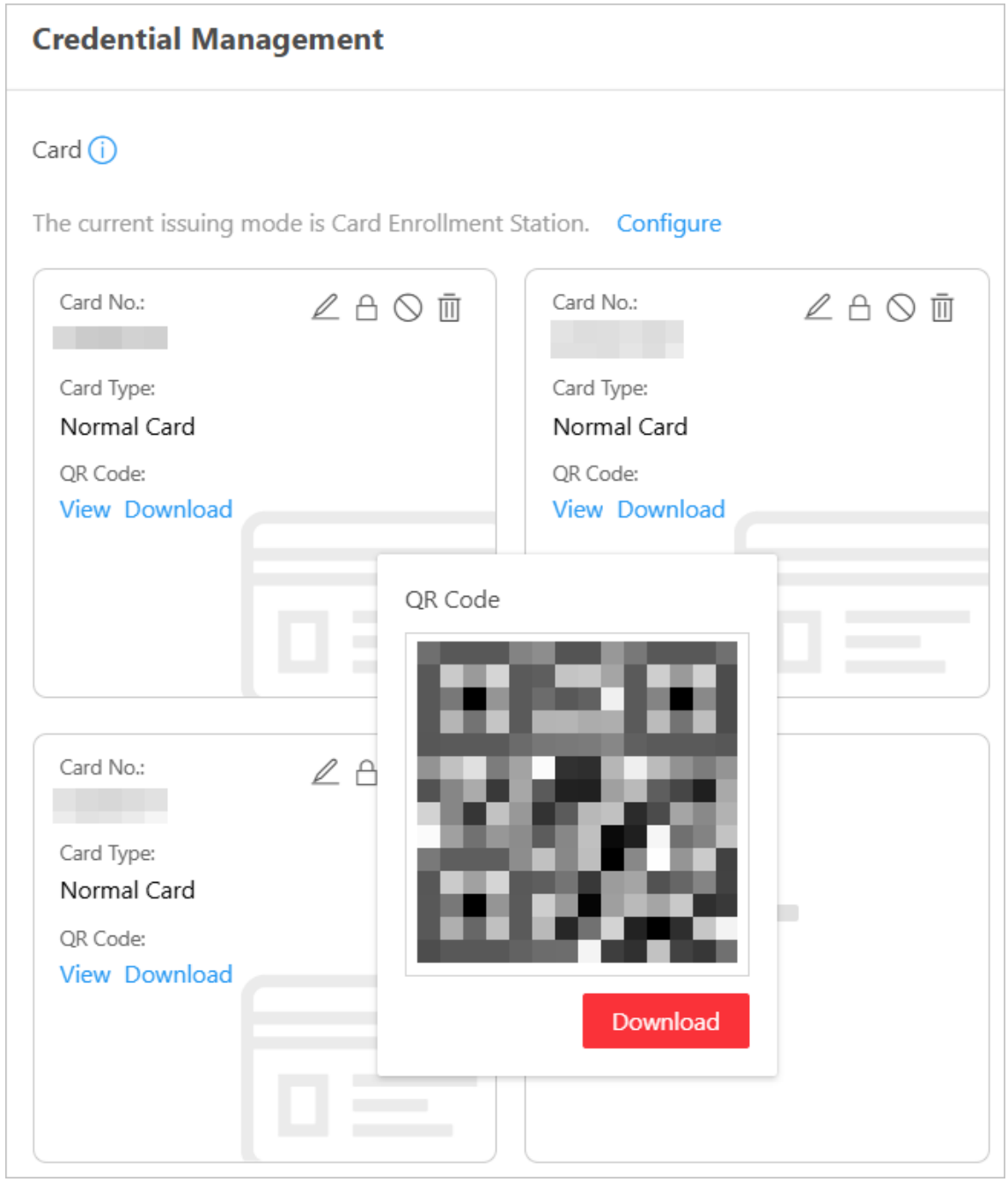



**Figure 5-6 View QR Code of Card**

## How to Collect Irises

In the Iris area, collect irises of the person. Click **Configure** to select a device used for collecting the person's irises. Click + and then start collecting irises.

## How to Collect Fingerprints

In the Fingerprint area, click **Configure** to set the method for collecting the person's fingerprint, and then collect the fingerprint.

**USB Fingerprint Recorder**

Plug the USB interface of the fingerprint recorder to the PC on which the Web Client runs and then collect the person's fingerprint via the device.

**Fingerprint and Card Reader**

Select a device type and then select a fingerprint and card reader to collect the person's fingerprint.

**Enrollment Station**

If you set network as the access mode, set other parameters of the enrollment station (e.g., access protocol, device IP address, and device port No.,) to allow the platform to access the device via network. And then collect the person's fingerprint via the device.

If you set USB as the access mode, plug the USB interface of the enrollment station to the PC on which the Web Client runs, and then collect the person's fingerprint via the device.

Switch on **Special Credential** and then add special cards and corresponding fingerprint information.

## How to Collect Palm Prints/Veins

Click **Configure** to select the collection mode as enrollment station or access control device. In the **Palm Prints or Palm Veins** area, click + to start collecting.

## How to Add Keyfobs

The value of keyfobs lies in enabling "contactless, rapid door triggering within a certain range." Key application scenarios include:

- Vehicle Access Management (Most Common):
  Scenario: Underground parking lots or gates in enterprises, factories, or residential communities.
  Process: Drivers can trigger the gate to open remotely without leaving their vehicles, offering greater convenience than card swiping or scanning, especially in adverse weather.
- Convenient Access to Special Areas:
  Scenario: Warehouses, equipment rooms, financial offices, or laboratories requiring frequent authorized entry.
  Process: Authorized personnel (e.g., warehouse keepers, accountants) can open doors effortlessly using a keyfob when their hands are occupied.
- Temporary or Emergency Access
  Scenario: Temporary access for staff or vehicles during events, or as a backup when access systems malfunction.
  Process: Pre-authorized keyfobs are distributed and deactivated after use or system recovery.
- Integration with Alarm Systems: In perimeter security zones, keyfobs can be programmed as "arm/disarm" switches, simultaneously triggering door opening and alarm system adjustments.

When assigning keyfob credentials to individuals, two modes are supported:

**Add Manually**

Manually enter the keyfob's serial number.

**Auto Detect**

The platform will automatically obtain keyfobs' serial numbers in pairing mode. In this mode, select a sliding gate opener, point the keyfob toward it, and press any button. The system will then obtain the keyfob's serial number.

### 5.4.2 Import Profile Pictures

You can add multiple persons' profile pictures to the persons in a department. If you access the platform via the Web Client running on the SYS, you need to specify a path where the profile pictures are stored. If you access the platform via the Web Client running on other computers, you can import a ZIP file containing the profile pictures.

**Steps**

**Note**

If the ID in the name of the profile picture is duplicate with the person's ID that already exists in the platform, the former will replace the latter. If the ID in the name of the profile picture doesn't exist in the platform, or the name of the profile picture only contains the person name, the platform will create a new person.

1. Name the profile pictures according to the person name or person ID.

   **Note**

   - The naming rule of picture is: Person Name, Person ID, or Person Name ID. The person name should contain the first name and the last name, separated by a plus sign.
     The naming rule for profile pictures: First Name+Last Name_ID. At least one of first name and last name is required, and the ID is optional. For example, Kate+Smith_123.jpg; Kate_123.jpg; Smith_123.jpg.
   - Dimension recommendation for each picture: 295×412.
     Size recommendation for each picture: 60 KB to 100 KB.
   - The pictures should be in JPG, JPEG, or PNG format.

2. **Optional:** If you access the platform via the Web Client running on the SYS, move these pictures into one folder and then compress the folder in ZIP format.

   **Note**

   The ZIP file should be smaller than 4 GB, or the uploading will fail.

3. On the top navigation bar, select → **Basic Management** → **Person** .
4. Select **Person Management** → **Person** on the left.
5. Click → **Import Profile Picture** .

6. Select the person pictures.
   - If you access the platform via the Web Client running on the SYS, select a path where the profile pictures are stored.
   - If you access the platform via the Web Client running on other computers, select ZIP files containing the profile pictures.

   **Note**

   You can hold CTRL key and select multiple ZIP files. Each ZIP file should be no larger than 4 GB.
7. Select a department from **Department**.
8. **Optional:** Switch on **Check Face Quality by Device** and then select a device type and a device for verifying the face quality.
9. Click **Import** to start importing.

   The importing progress shows and you can check the results.
10. **Optional:** After importing profile pictures, click **Export Failure Details** to export an Excel file to the local PC and view the failure details.

### 5.4.3 Card Management

### How to Add a Card

In the ***Card*** area, click + , and then manually enter the card No. or swipe the card on devices (enrollment station, card enrollment station, or card reader) to add normal cards.

- For manually entering, digits, letters, and the combination of digits and letters can be entered.
- For swiping cards, you can read card information via the enrollment station, card enrollment station, or card reader. For details, see ***Batch Issue Cards to Persons*** .

### Set Card Issuing Parameters

The platform provides multiple modes for issuing cards, including reading card numbers via devices and manually entering card numbers.

**Steps**

1. Open the card issuing settings window when managing credentials or batch issuing cards to persons.
   - Open the window when managing credentials.
   - Open the window when batch issuing cards to persons.
   - Open the window when filtering persons in the person list.

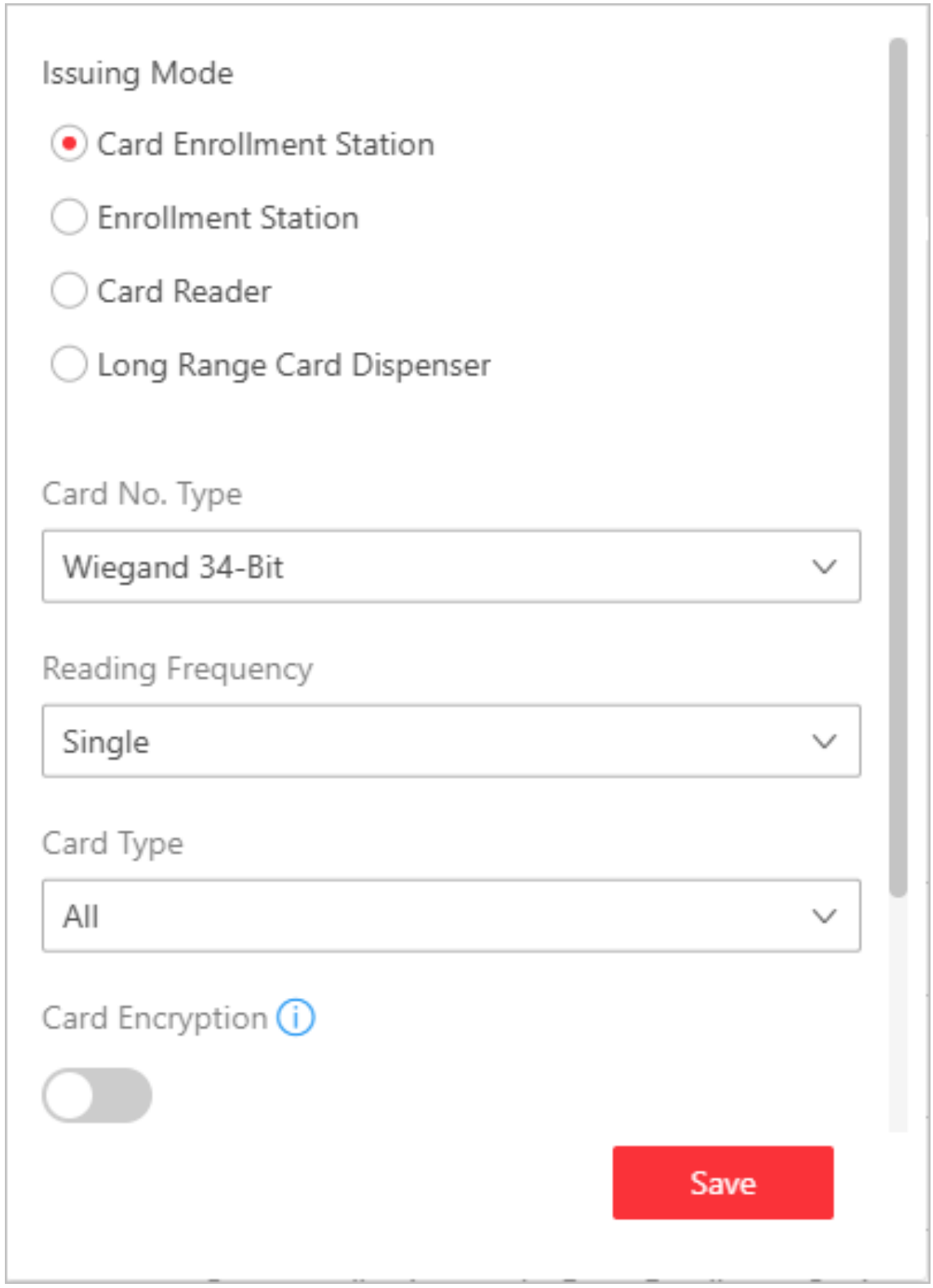



**Figure 5-7 Card Issuing Settings Window Opened When Batch Issuing Cards to Persons**

2. Select an issuing mode and set the related parameters.

**Card Enrollment Station**

Connect a card enrollment station to the PC on which the Web Client runs. You can place the card on the card enrollment station to get the card No.

If you select this mode, you should set the card format and card encryption function.

**Card No. Type**

If the card type is Wiegand card, select **Wiegand 34-Bit** or **Wiegand 26-Bit**. If not, select **Full Byte**.

**Reading Frequency**

If your card supports dual frequency (both IC and ID), select **Dual**. If not, select **Single**.

**Note**

If you select **Dual**, you cannot set card encryption for the card.

**Card Encryption**

If you set **Normal** as the card No. type, you can enable the card encryption function and select section(s) to be encrypted for security purpose. After enabled, you should enable the card encryption in the access control device's configuration page to make card encryption effective.

**Audio**

Turn on or turn off the audio.

**Enrollment Station**

You can enroll the card number remotely via the enrollment station and copy back to the platform.

If you select this mode, you should set the required parameters below.

**Access Mode**

The access mode of the enrollment station. Click **Network** or **USB** from the dropdown list.

**Access Protocol**

The access protocol of the enrollment station. By default, the access protocol is SDK.

**Device Address**

The IP address of the enrollment station.

**Device Port**

The port number of the enrollment station.

**User Name**

The user name used to log in to the enrollment station.

**Password**

The password used to log in to the enrollment station.

**Card Format**

If the card is Wiegand card, select **Wiegand 34-Bit** or **Wiegand 26-Bit**. If not, select **Full Byte**.

**RF Card Type**

Select the needed card type(s), including EM card, M1 card, etc.

**Note**

When selecting **M1 Card**, you can switch on **Card Encryption** and select section(s) if needed.

**Card Reader**

Select one card reader of one access control device added to the platform. You can swipe the card on the card reader to get the card number.

- One card reader can be selected for issuing cards by only one user at the same time.
- If you set a third-party card reader to read the card number, you should set the custom Wiegand protocol for the device to configure the communication rule first.

**Enter Manually**

**Note**

This parameter is not available on the card issuing settings window opened when managing credentials and filtering persons in the person list.

If you select this mode, you need to manually enter the card number. You can check **Auto Increment Card Number** to enter a start card number to issue cards with incremental numbers to the selected persons in the list

**Long Range Card Dispenser**

For UHF card, set the **Card Number Offset** to ***From the End***, and set the **Zero Padding Mode** to ***Leading Zero Padding***. And these values are selected by default.

3. Click **Save** (for Credential Management) or **Start** (for Batch Issue Cards to Persons).

## Batch Issue Cards to Persons

The platform provides a convenient way to batch issue cards to multiple persons.

**Steps**

**Note**

- Up to 5 cards can be issued to one person.
- You cannot issue cards to persons who have temporary cards.

1. Select **Person Management → Person** on the left.
2. Select persons to whom the cards will be issued.

3. Move the cursor onto **Card**, and then click **Batch Issue Cards to Persons**.
4. In the pop-up window, set the related parameters.

**Note**

For details about setting the card issuing mode and parameters, refer to ***Set Card Issuing Parameters*** .

5. Issue one card to one person according to the issuing mode you select.
   - If you set the issuing mode to **Card Enrollment Station**, place the card on the card enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Card Reader**, swipe the card on the card reader. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Enrollment Station**, place the card on the enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Enter Manually**, enter the card number manually in the Card Number field. Press **Enter** key on the keyboard to issue the card to the person.

   **Note**

   You can check **Auto Increment Card Number** and enter a start card number to issue cards with incremental numbers to the selected persons in the list.
6. Click **Start** to start issuing cards.
7. Repeat step 5 to issue the cards to the persons in the list in sequence.

**Note**

You cannot change the card issuing mode once you issue one card to one person.

8. Click **Save**.

## Print Cards

After adding persons to the platform, you can print their information onto blank physical cards. If you have set credential information (e.g., virtual card information) for the persons, the credential information will be linked to the physical cards once the physical cards are printed. For example, in the scenario of employee management, you can print physical cards as the employee ID badges, which can be used by your employees as the credentials for access authentication at the access points of your company.

**Before You Start**

- Make sure you have added the supported printers to the platform. For details, see ***Set Printer*** .
- Make sure you have added card templates to the platform. For details, see ***Set Card Template*** .

**Steps**

1. Select **Person Management → Person** on the left.

2. **Optional:** Set conditions to search for the target persons.
3. Select the persons for whom you need to print cards.
4. Click **Print Card** to open the Print Card window.

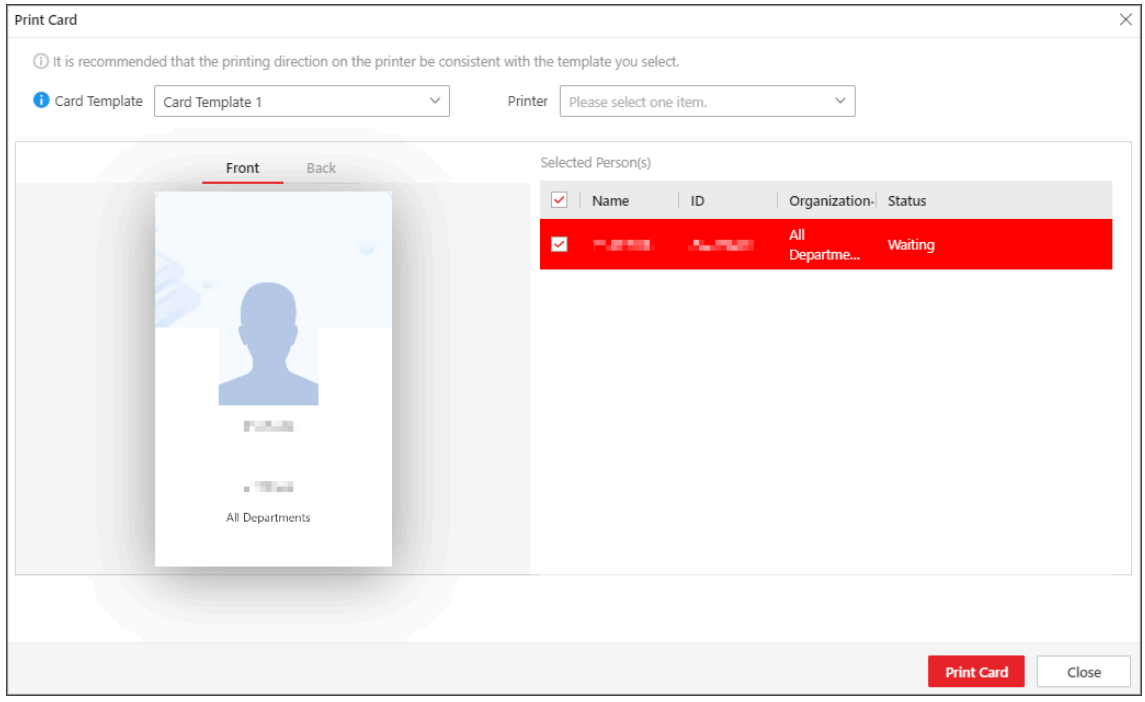



**Figure 5-8 Print Card Window**

5. Select a card template from **Card Template**.
6. Select a printer from **Printer**.
7. Select person(s) from the Selected Person list.
8. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
9. Click **Print Card**.

**What to do next**

If you have not manually added card information for the persons, batch issue card information to them. Otherwise the persons cannot use the physical cards for access authentication. See ***Batch Issue Cards to Persons*** for details.

## Card Loss

If a person cannot find her/his card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level of the lost card. The card issuer can issue a temporary card with effective period and access level to

the person. When the card is found, the card issuer need to take back the temporary card and cancel the card loss report, and then the found card will be active again.

### Report Card Loss

Click the name of the person in the person list to enter the basic information page, and then click **Credential Management** to expand the Add Credential panel. In the Card area, move the cursor onto the lost card and then click . After you report card loss, the access levels of the lost card will be inactive.

You can also select the persons in the person list, move the cursor onto **Card** on the top, and then select **Report Loss** on the top to batch report loss.

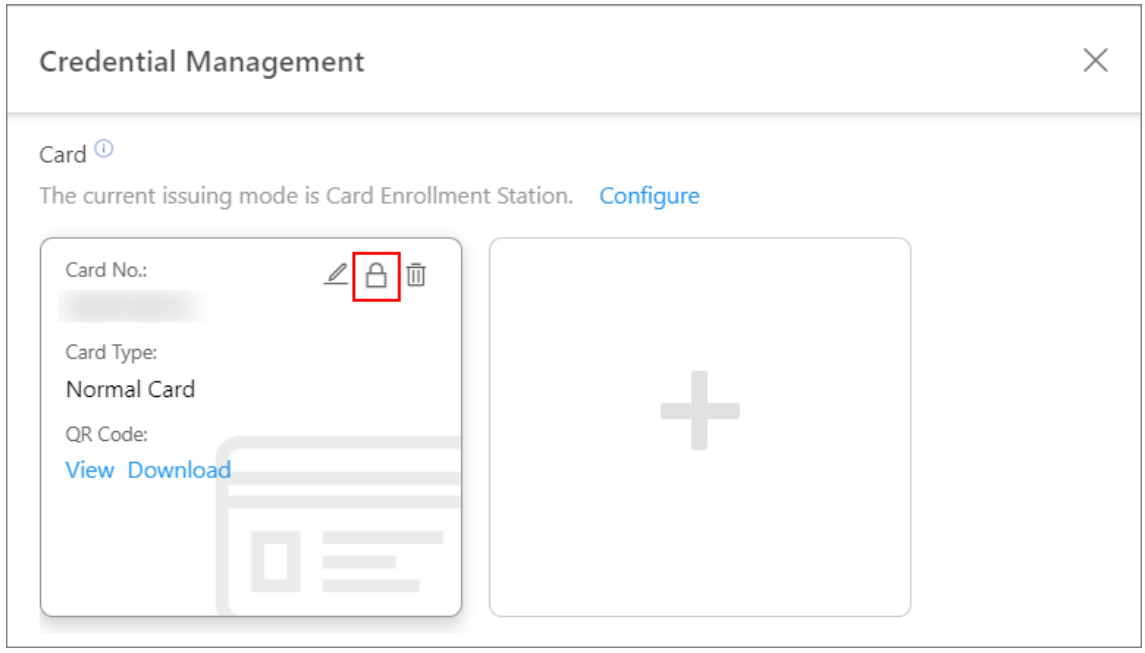



**Figure 5-9 Add Credential Panel**

### Issue a Temporary Card to a Person

If a card is reported as loss, you can issue a temporary card to the person who loses the card. Once the temporary card is issued, other cards linked to this person will be inactive, and the biometric credentials(such as fingerprints and profile) linked to these inactive cards will be transferred to this temporary card.

On the page of a single person. click **Credential Management** under the profile picture to open the Credential Management pane. In the Card area, click .

The expiry date of a temporary card should be within the effective period of the person (card owner). In other words, the expiry date cannot be later than the effective period. For details about setting or editing the person's effective period, see ***Add a Single Person Manually*** .

You can delete the temporary card for the person. Once the temporary card is deleted, the inactive cards of the person will restore to the active status, and their previously linked person information such as fingerprints will also restore.
Perform the following operation(s) if needed.

**Table 5-1 Operations for Temporary Card**

| Operation | Description |
|---|---|
| Edit the Temporary Card | Move the cursor onto the temporary card, and then click to edit the temporary card. |
| Delete the Temporary Card | Move the cursor onto the temporary card, and then click . |

### Batch Cancel Card Loss

If the lost cards are found, you can batch cancel the card loss reports for multiple persons. After that, the cards' access levels will return to be active and the original biometric credentials (such as fingerprints and face information) will be linked to these cards again.

Select the persons in the person list, hover the cursor on **Card**, and then click **Cancel Card Loss**.

### Disable/Restore Card

On the person list, check persons and click **Card → Disable Card** , select the card(s) to be disabled, select the cause of disabling, and click **Disable**.

If you want to restore cards, check persons and click **Card → Restore Card** , select the card(s) and click **Restore**.

## 5.5 Person Self-Registration

If there are persons to be added to the system, you can generate a QR code for them to scan. After scanning the generated QR code by smart phone, the persons can enter their personal information (including profile) on Self-Registration page. If you have enabled Review Self-Registered Persons function, you need to review and approve their person information, otherwise they cannot be added to the system.

This function is applicable to circumstances like a company where there is a large amount of new employees to be added to the system. For example, you print the generated QR code for the new employees to scan. After scanning the QR code by smart phone, new employees will enter Self-Registration page to import their personal information.

**Note**

You should set self-registration parameters beforehand. See ***Set Self-Registration Parameters*** for details.

### 5.5.1 Set Self-Registration Parameters

Before starting self-registration, you need to set self-registration parameters. A QR code is necessary for the persons to register their information by themselves. Besides, you can configure face quality verification and person information review.

Select **Basic Configuration → Self-Registration Settings** on the left panel, or click **Person Management → To Be Reviewed → Self-Registration Settings** to enter the Self-Registration Settings page.

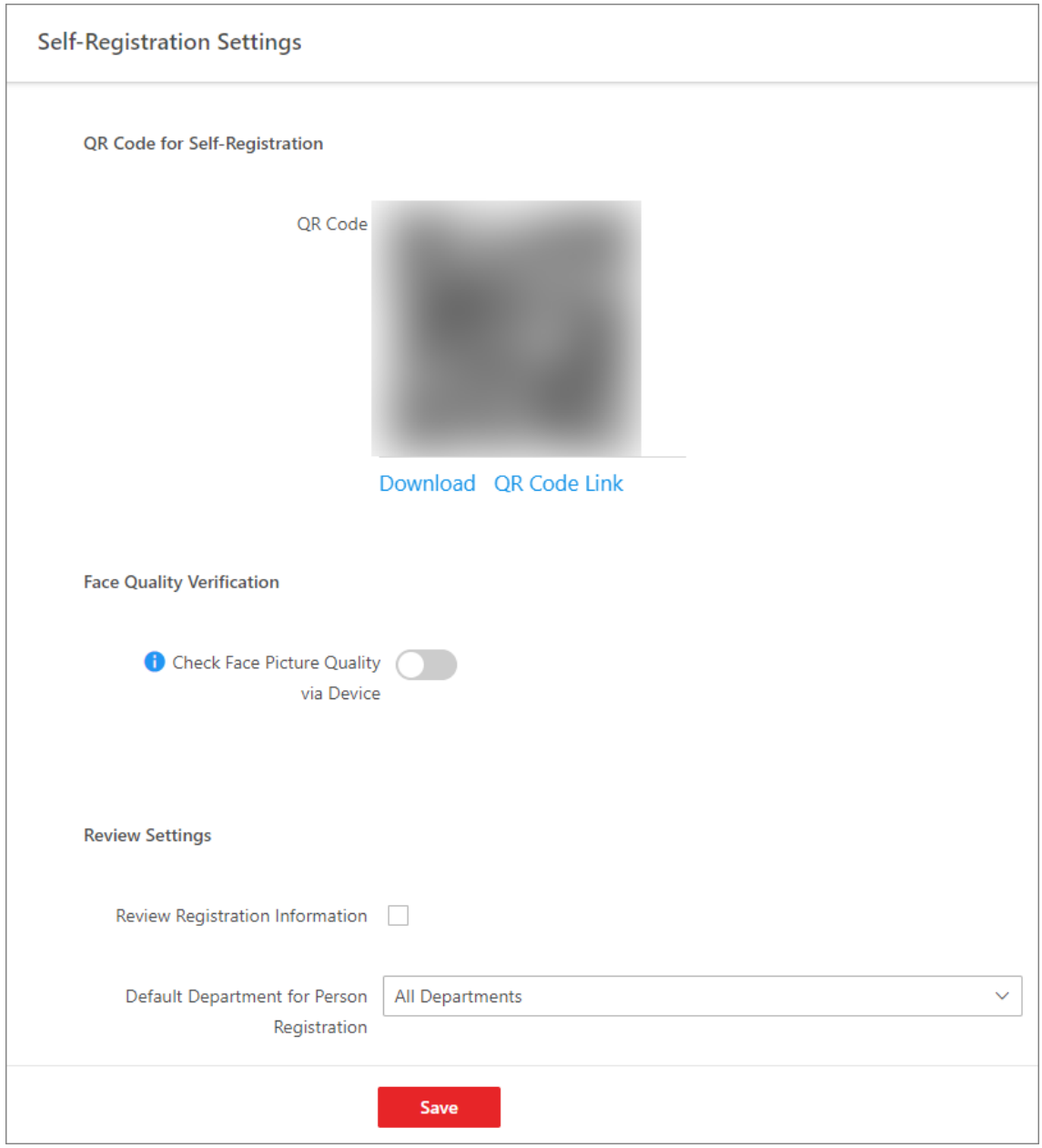



**Figure 5-10 Self-Registration Settings**

**QR Code for Self-Registration**

The platform will generate a QR code for you to download. After downloading the QR code, you can print it or send it to persons who are going to register. You can click **QR Code Link** to enter your personal information so as to add yourself to the platform.

**Face Quality Verification**

After the person uploads profile by a cellphone, the selected device will automatically start checking the profile's quality. If the profile picture is not qualified, the person will be notified. Only when the uploaded profile is qualified can the person register successfully. Otherwise, the person's information cannot be uploaded to the platform.

**Note**

To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

**Review Self-Registered Persons**

Set a default department. Once the person information is registered, the person will be added to this group.

If you enable **Review Self-Registered Persons**, after registration, you need to review the person information on the Persons to be Reviewed page. After verification, the person will be added to the selected department. See ***Review Self-Registered Person Information*** for details about how to review.

## 5.5.2 Scan QR Code for Self-Registration

If a person needs to register by self-service, the person should use a smart phone to scan the self-registration QR code to enter the Self-Registration page and enter person information. After registration, the person details will be uploaded to the platform for review.

**Before You Start**

The administrator can print the QR code or send the QR code to persons to scan. See ***Set Self-Registration Parameters*** about how to generate a self-registration QR code.

**Steps**

1. Use your smart phone to scan the self-registration QR code to enter the Self-Registration page.
2. Tap the profile frame to upload a face picture.

**Note**

- You can select a picture from your phone album, or take a photo by phone.
- After uploading a profile, profile quality checking will automatically start. If the profile is not qualified, you will be notified. Only when the uploaded profile is qualified can you register successfully. Otherwise, your personal information cannot be uploaded to the platform. See ***Set Self-Registration Parameters*** for details about setting Face Quality Verification function.

3. Set your personal information, including name, ID, email, phone number, etc.
4. Enter the verification code.
5. Tap **Save**.

- If **Review Self-Registered Persons** function is enabled, wait for the review. If you are approved, you will be added to the platform. See ***Review Self-Registered Person Information*** about how to review.
- If **Review Self-Registered Persons** function is disabled, the person information will be uploaded to the platform.

### 5.5.3 Review Self-Registered Person Information

If you have enabled **Verify Registration Information** function when you set self-registration parameters, after the persons registered, their person information will be displayed on the Persons to be Reviewed page, and their status will be displayed as **To be Reviewed**. You should review their personal information to approve. After approving, they will be added to the target department.

Then select **Person Management → To Be Reviewed** on the left panel to enter the Persons to Be Reviewed page.

Review the displayed person information and verify them.

**Table 5-2 Review Self-Registered Persons**

| Operation | Description |
|---|---|
| Approve Self-Registered Person Information | If the self-registered person information is correct, approve the information to add the registered persons into the platform.<br>• Select a registered person, and click to approve the person.<br>• Check multiple registered persons, and click **Approve** to approve them all. |
| Reject Self-Registered Person Information | If there is something wrong or missing with the self-registered person information, reject the person and tell the person to register again with right information.<br>• Select a registered person, and click to reject the person.<br>• Check multiple registered persons, and click **Reject** to reject them in a batch. |
| Delete Self-Registered Person Information | • Select a registered person, and click to delete the person from the Persons to be Reviewed list.<br>• Check multiple registered persons, and click **Delete** to delete them all from the Persons to be Reviewed list. |

Approved persons will be added to the target department; rejected persons will not be added to the target department, but they will stay in the Persons to be Reviewed list.

## 5.6 Resigned Persons Management

You can manage resigned persons by adding, deleting, and editing resigned persons. You can also reinstate resigned persons and export resigned person information.

### Manage Resignation Types

If the default resignation types do not meet your needs, you can add other resignation types.
Select **Basic Configuration → Resignation Type** on the left.

- Click **Add**, enter the departure type name, and click **Add** in the pop-up window to customize the type.
- Click in the Operation column to edit the added departure type.
- Click or **Delete** to delete the selected departure type(s).

**Note**

- The default types (dismiss, departure, redeployment, and suspension with pay) cannot be deleted or edited.
- Up to 100 departure types can be added.

### Add Resigned Persons

You can add one or multiple resigned persons, delete and export the resigned person information.
Select **Person Management → Resigned** on the left, and then click **Add** to open the Add Resigned Person pane. Click to select one or multiple persons from the departments.

**Departure Date**

Last day of the current employment.

**Disable Attendance**

Check it, then the platform will not calculate attendance results generated during the period between applying for resigning and departure date.

You can also select persons on the person list, and click **Adjust → Resigned** to quickly add resigned persons.
For persons to be resigned, their permissions of access and vehicles, and credentials such as the card, fingerprint, face picture, iris data will be deleted at the day of resignation.

### Reinstate Persons

You can reinstate persons who are resigned and to be resigned.

Select **Person Management → Resigned** on the left. Select one or multiple persons and click **Reinstate**. On the pop-up, select the department to which the person(s) will be reinstated, and click **Reinstate**.
After the person reinstatement, you can view the related persons in the person list.
After the reinstatement, the resigned persons need to upload their credentials, such as face picture, fingerprint, and iris data. Their access levels and attendance schedule will be accordance to that of their departments.

### 5.6.1 Add Resigned Persons

You can add one or multiple resigned persons, delete and export the resigned person information.

**Steps**

1. Select **Person Management → Resigned** on the left.
2. Click **Add** to open the Add Resigned Person pane.
3. Click to select one or multiple persons from the departments.

**Note**

- You can enter specific person name, department, or person ID click **Search** to filter the person information.
- You can check **Include Sub Department** for displaying the person in sub departments.
- You can check **Select All Persons** to select all matched persons.

4. Specify the following parameters.

**Departure Date**

Last day of the current employment.

**Departure Type**

Cause of the departure.

**Note**

You can click **Add Departure Type**, enter the departure type and click **Add** to customize the type. For details, see ***Manage Resignation Types*** .

5. **Optional:** Check **Disable Attendance**, then the platform will not calculate attendance results generated during the period between applying for resigning and departure date.
6. **Optional:** Specify the departure reason.
7. Click **OK**.

**Note**

You can also adjust the person's status as resigned in Person Management module. See details in ***Add a Single Person Manually*** and ***Batch Add Persons by Template*** .

For persons to be resigned, their permissions of access and vehicles, and credentials such as the card, fingerprint, face picture, iris data will be deleted at the day of resignation.

8. Perform the following operations.

| Operation | Description |
|---|---|
| **Edit Resigned Person** | Select a person and click in the Operation column to edit the resignation information. |
| **Filter Resigned Person** | Click to expand the conditions, set the filter conditions and click **Filter** for filtering the resigned persons. |
| **Export Resigned Person** | Click **Export** to export the resigned person information in the current page according to the filter conditions. |
| **Disable Attendance** | Select one or multiple persons whose attendance status is "enable", and click **Disable Attendance** to batch disable the function. |
| **Delete Resigned Person** | Select one or multiple persons and click **Delete** to delete them. |
| **Set Column Width** | Click to select **Complete Display of Each Column Title/Incomplete Display of Each Column Title** to set the column title width. |
| **Custom Column Item** | Click and select the needed column items to display. You can also click **Reset** to reset to the default column items. |

### 5.6.2 Reinstate Persons

You can reinstate persons who are resigned and to be resigned.

**Steps**

1. Select **Person Management → Resigned** on the left.
2. Select one or multiple persons and click **Reinstate**.
3. On the pop-up, select the department to which the person(s) will be reinstated, and click **Reinstate**.
   - After the person reinstatement, you can view the related persons in the person list.
   - After the reinstatement, the resigned persons need to upload their credentials, such as face picture, fingerprint, and iris data. Their access levels and attendance schedule will be accordance to that of their departments.

### 5.6.3 Manage Resignation Types

If the default resignation types do not meet your needs, you can add other resignation types.

On the top navigation bar, select → **Basic Management → Person** .

Select **Basic Configuration → Resignation Type** on the left.

- Click **Add**, enter the departure type name, and click **Add** in the pop-up window to customize the type.
- Click in the Operation column to edit the added departure type.
- Click or **Delete** to delete the selected departure type(s).

**Note**

- The default types (dismiss, departure, redeployment, and suspension with pay) cannot be deleted or edited.
- Up to 100 departure types can be added.

## 5.7 Position Management

The platform allows you to add positions to define the hierarchical levels of your company. By assigning the positions to employees, you can quickly understand the number of active employees in each position and the number of employees who have resigned. You can manually add positions one by one or import multiple positions at once via a predefined template.

Select **Position Management** on the left to enter the Position Management page.

### Add a Position Manually

Click above the left position tree to open the Add Position pane. Enter the name of the position. From the drop-down list, select the upper-level position to which the position to be added is subordinate. You can click to select the persons that have been assigned to this position.

### Import Positions

Click above the left position tree to open the Batch Import Positions pane.
Click **Download Template** to download the template to the local PC. Open the downloaded template file and fill in the required information, including the names of the positions and their upper-level positions. Click to select the edited template file from the local PC.
Check **Auto Replace Duplicated Position** to allow the platform to automatically replace existing positions if the file to be imported contains positions that are already added to the platform.

**Note**

If it is not checked and the file contains positions that are already added to the platform, the import may fail.

# Chapter 6 Vehicle Management

On the Web Client, you can add the vehicle information to the platform, categorize vehicles into different types (including registered vehicles, temporary vehicles, visitor vehicles, and vehicles in list), and set rules to define the accuracy when searching for vehicles by license plate number. The managed vehicles can be used in the applications such as ANPR (Automatic Number Plate Recognition) and entrance & exit control.

On the top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.

**Note**

- For Central System: Vehicle lists can be applied remote sites, and the information within these lists will be synchronized accordingly. Any further updates to vehicle information on the Central System will be automatically synchronized to the remote sites.
- For Remote Sites: If changes are made to the vehicle information from the Central System is changed, an approval request will be sent to the Central System. The changes will take effect on both the remote sites and the Central System once the request is approved.

## 6.1 Manage Registered Vehicles

A registered vehicle can park in a specific parking lot without paying any fee. To make a vehicle become a registered vehicle, you need to add its information (including the license plate number, vehicle type, etc.) to the platform first, and then you need to link a parking pass to it, so that the vehicle can enter and exit the parking lot as a registered vehicle.

You can perform the following operation(s) after adding registered vehicles.

| Operation | Function |
|---|---|
| Edit a Vehicle | Click a number in the License Plate Number column to edit the vehicle information. |
| Delete Vehicles | • Check the vehicle(s) and click **Delete** to delete the selected vehicle(s).<br>• Click → **Delete All** beside **Delete** to delete all the added vehicles in different vehicle lists. |
| Delete Expired Vehicles | Click **Delete Expired Vehicle** to delete all expired vehicles from different vehicle lists. |
| Filter Vehicles | Click and set conditions to filter specific vehicles. |

| Operation | Function |
|---|---|
| | **Note**<br>For the Middle East and North Africa, you can filter vehicles by country/region and plate category. |
| Export Vehicles | Click **Export All** to save the filtered vehicles or vehicles from all vehicle lists to your PC as an XLSX file, which can be imported to the platform again.<br>**Note**<br>For the Middle East and North Africa, the exported vehicle information will contain the country/region and plate category. |
| Edit Effective Period | Select a registered vehicle and click **Edit Effective Period** to edit the effective period for the vehicle. |
| Custom Column Items | On the top right, click to select column items to be displayed. You can click **Reset** to select again. |

### 6.1.1 Add a Registered Vehicle

You can add the information of one vehicle to the platform as a registered vehicle at one time.

**Steps**

1. On the left navigation pane, click **Vehicle Management → Registered Vehicle → Vehicle** .
2. In the top left corner of the Vehicle page, click **Add** to enter the Add Vehicle page.
3. Set the vehicle information, such as the license plate number, vehicle list, type, color, and brand.

**Country/Region, Plate Category, License Plate Size, License Plate Type, License Plate Color**

These parameters are available for configuration only when the area is set to **Middle East and North Africa**. In accordance with SIRA license plate standards, these parameters (along with the license plat No.) serve as factors for precisely identifying the same vehicle. To more reliable recognition, it is recommended to fill out the accurate and complete information.

For details about the area settings, refer to ***Customize Vehicle Information*** .

**Vehicle List**

Select a list that you predefined on the platform from the drop-down list to add the vehicle to. If you have not added any vehicle list to the platform before, you can click **Add** to create a new one. For details, refer to ***Manage Vehicle Lists*** .

**Effective Period**

Set the effective period for the registered vehicle in applications such as entrance & exit control, to determine the period when the vehicle can enter or exit a parking lot as a registered vehicle.

**Undercarriage Picture**

Upload an undercarriage picture of the registered vehicle for comparing the captured one to the uploaded one on the Control Client.

4. Set the information for the vehicle owner.
   - Enter the owner's first name, last name, and phone number.
   - Click **Person List** to select an existing person as the vehicle owner from a person list and select a card No. (if cards are issued to the person) for the owner to swipe card when entering and exiting the parking lot.

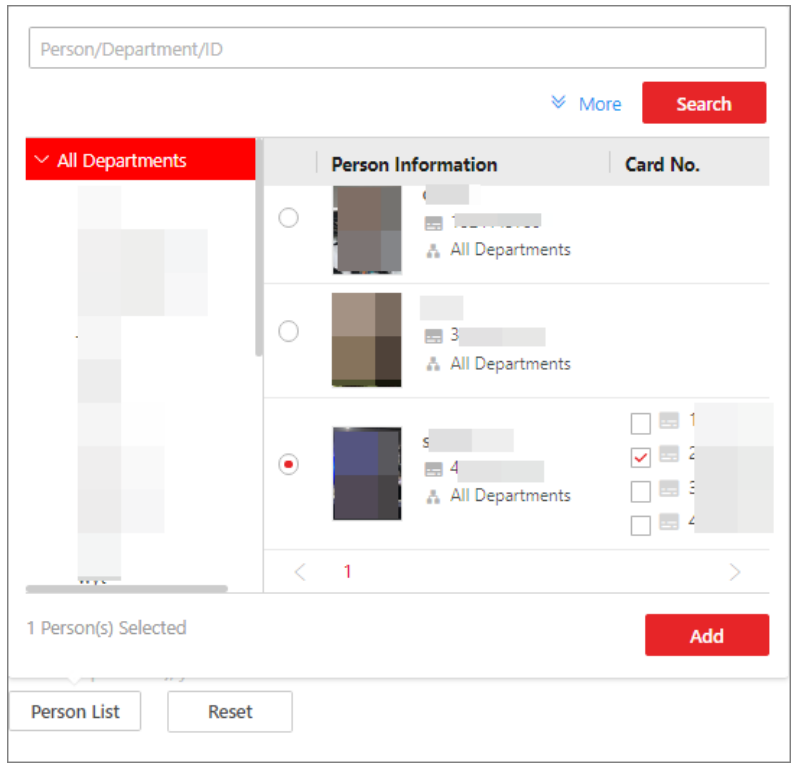



**Figure 6-1 Select an Existing Person as Vehicle Owner**

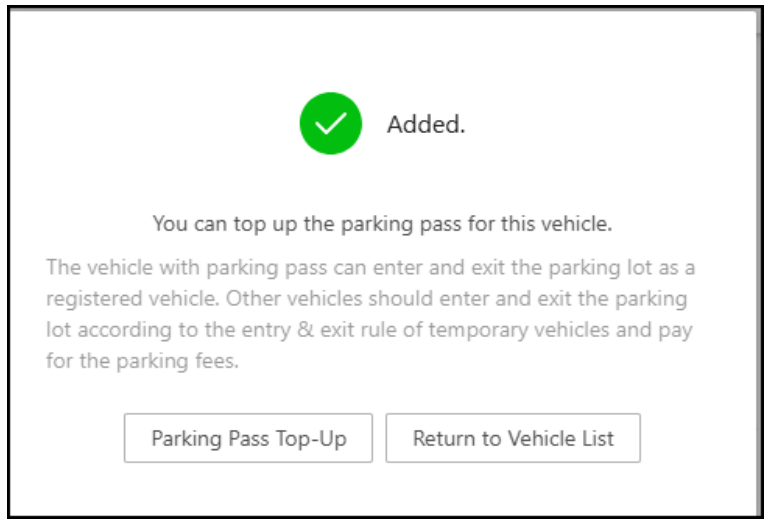
**Note**

- You can select a person who has been linked to another vehicle.
- For how to add persons and how to issue cards to persons, refer to ***Add a Single Person Manually*** and ***Batch Issue Cards to Persons*** .

5. Click **Add** to add the registered vehicle or click **Add and Continue** to continue adding another registered vehicle.

   A window pops up to remind you of topping up a parking pass for the vehicle.

Since only vehicles with a parking pass can access the parking lot as registered vehicles, you can click **Parking Pass Top-Up** to top up immediately, or return to the vehicle list and top up a parking pass later in the Top-Up Management module.




### 6.1.2 Batch Import Registered Vehicles

You can import the information of multiple vehicles to the platform as registered vehicles at one time.

**Steps**

1. On the left navigation pane, click **Vehicle Management → Registered Vehicle → Vehicle** .
2. In the top left corner of the Vehicle page, click **Import**.

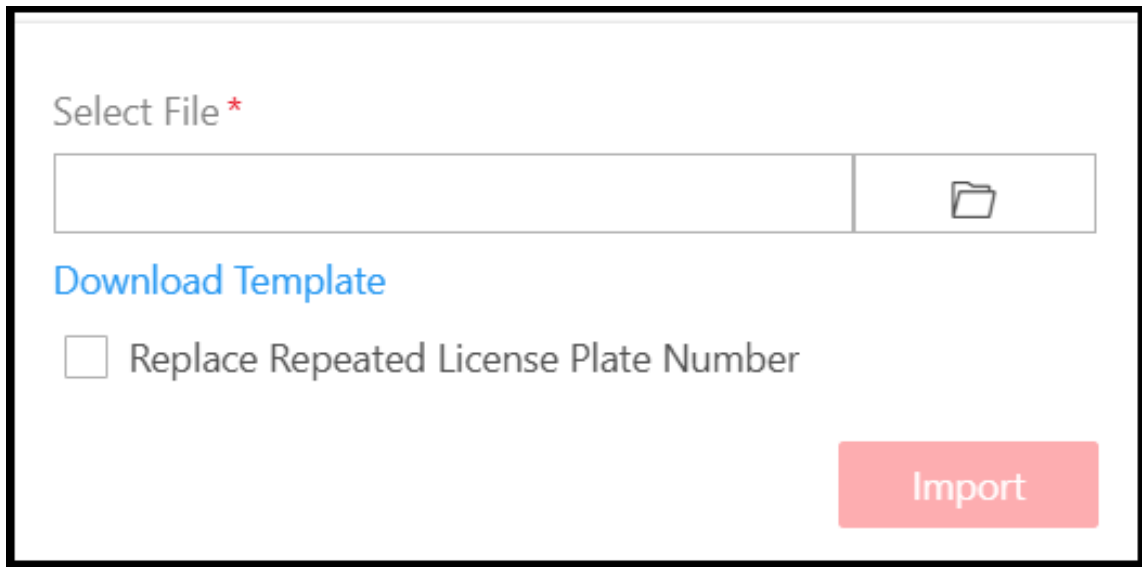



**Figure 6-2 Import File**

3. Click **Download Template** to download and save the template file to your PC.
4. Open the downloaded template file and enter the required information.

   If you want to set an added person as the owner of a vehicle, you can enter the person ID in the Vehicle Owner ID column.
5. Click and select the file.
6. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing vehicle information with the new vehicle information if the file contains the license plate number which has already been added to the platform. Otherwise, the original vehicle information will be reserved.
7. Click **Import**.

**What to do next**

Only the vehicle with a parking pass can enter and exit the parking lot as a registered vehicle. Therefore, after batch importing vehicles to the platform, you need to link a parking pass to each of them in the Top-Up Management module later.

## 6.2 Manage Vehicle Lists

A vehicle list can group multiple vehicles so that you can manage them more easily.

**Before You Start**

Make sure you have selected the vehicle list(s) allowing for further management by the role linked with your account. See ***Add a Role*** for details on permission settings.

**Steps**

**Note**

Up to 100 vehicle lists can be added.

1. On the left navigation pane, click **Vehicle Management → Registered Vehicle → List Management** .
2. On the top of the left pane, click + to open the Add Vehicle List pane.

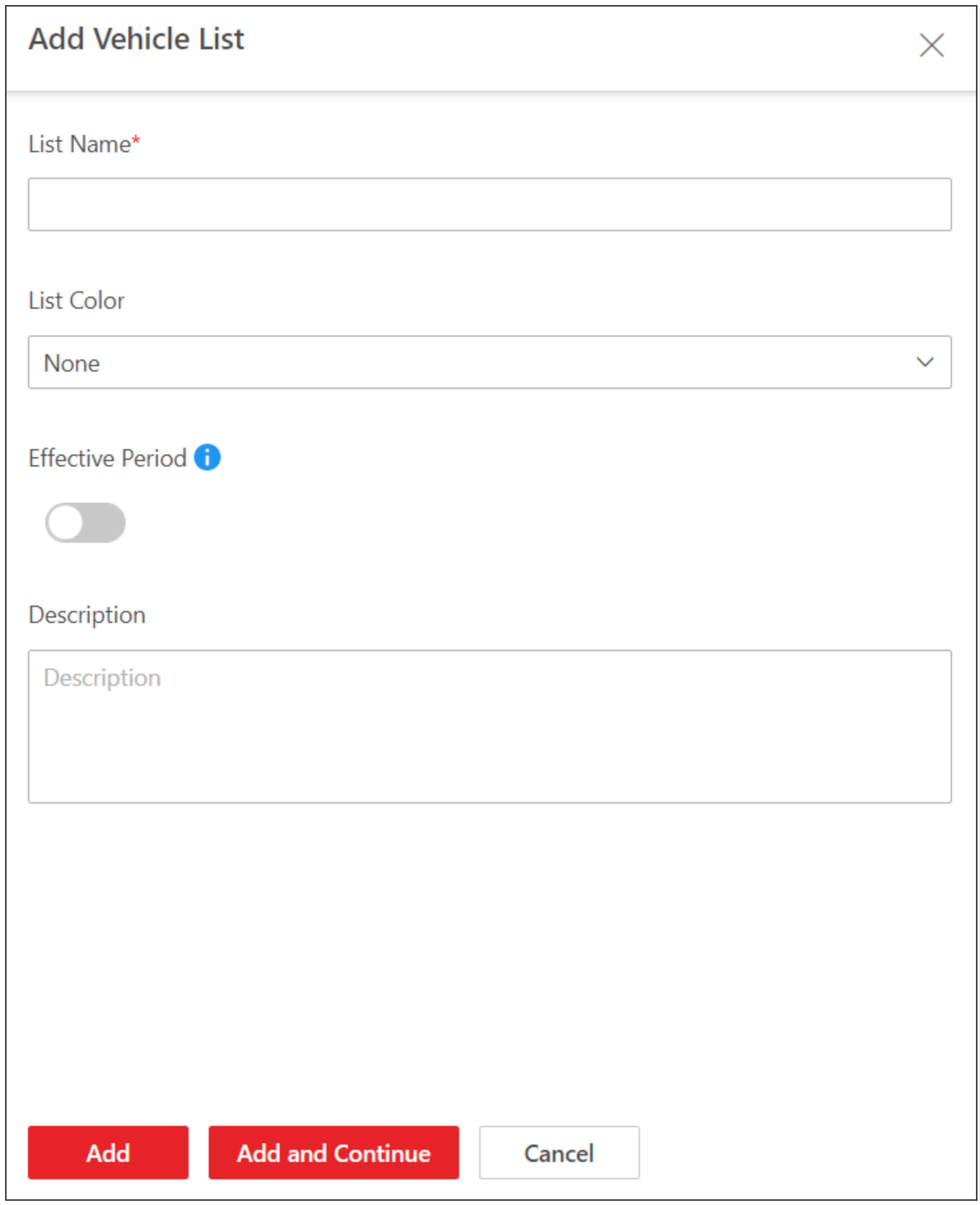



**Figure 6-3 Add Vehicle List Page**

**3.** Set the vehicle list's information, including list name, list color, effective period, and description.

**Note**

- The list color is used to mark different types of vehicle lists.
- If you enable and set the effective period, alarms related to vehicles in the list cannot be triggered and vehicles in the list will not be applied to the allowlist or blocklist after the vehicle list expires.
- When you adds a vehicle to this list later, you do not need to set an effective period for the vehicle, because the vehicle shares the same effective period as that of the vehicle list.

4. Click **Add** to add the vehicle list or click **Add and Continue** to continue adding another vehicle list.
5. **Optional:** Select the added list and click **Add** to search for vehicles to be added to the list.




**Figure 6-4 Add Vehicles to List**

**Note**

You can enter a keyword to search for vehicles on the Add Vehicle pane. Or you can click **Custom Information** to display vehicles' custom information fields, enable the field(s), and enter the corresponding keywords to make the search result more accurate. For more about the custom vehicle information, refer to ***Customize Vehicle Information*** .

6. **Optional:** Perform the following operation(s) after adding vehicle lists or adding vehicles to lists.

| | |
|---|---|
| **Search for Vehicle Lists** | At the top of the left pane, enter a keyword in the search box to search for specific vehicle lists. |
| **Edit a Vehicle List** | Select a vehicle list on the left pane and click at the top to edit it. |
| **Apply a Vehicle List to Cameras** | a. Select a vehicle list on the left pane, hover over on the top, and click **Apply to Camera** to open a pane.<br>b. Enable **Apply List** and select **Allowlist** or **Blocklist** as the list type.<br>c. Select cameras to be applied to.<br>d. Click **Save** to apply the vehicle list as an allowlist or a blocklist to the selected cameras. |
| **Apply a Vehicle List to Vehicles** | a. Hover over on the top, and click **Apply to Vehicle** to open the corresponding pane.<br>b. Select the list to be applied.<br>c. Click at the top.<br>d. Select the vehicles to receive the selected list.<br>e. Click **Apply**. |
| **Apply Vehicle Lists to Remote Sites** | a. Hover on at the top, and click **Apply to Remote Site** to open the corresponding pane.<br>b. Select the vehicle lists you need to apply.<br>c. Select the target Remote Sites for synchronization. |
| **Delete a Vehicle List** | Select a vehicle list on the left pane and click at the top to delete it. |
| **Remove Vehicle(s) from List** | • Select a vehicle list on the left pane to show its vehicles, check the vehicle(s), and click **Delete** to remove them from the current list.<br>• Select a vehicle list on the left pane to show its vehicles, click → **Delete All** beside **Delete** to remove all vehicles from the current list. |
| **Move Vehicle(s) to Another List** | Select a vehicle list on the left pane to show its vehicles, check the vehicle(s), and click **Move** to move them from the current list to another list. |
| **Export Vehicles in List** | Select a vehicle list on the left pane to show its vehicles, and click **Export All** to export vehicles in the current list to the local PC. |

| | |
|---|---|
| **Filter Vehicles in List** | Select a vehicle on the left pane to show its vehicles, click in the top right corner of the right pane and set conditions to filter specific vehicles in the current list. |
| **Custom Column Items** | On the top right, click to select column items to be displayed. You can click **Reset** to select again. |

## 6.3 Manage Visitor Vehicles

If a visitor comes by driving a vehicle, the license plate number will be recorded to the platform so that the platform can control the barrier to open when the capture unit detects this license plate. The recorded vehicles will be displayed in the visitor vehicle list, you can delete them, filter them by multiple conditions, and export the vehicle information to the local PC. Once the visitor checked out, the vehicle will be removed from the list.

On the left navigation pane, click **Vehicle Management → Visitor Vehicle** .

- **Delete Visitor Vehicles**: Select multiple vehicles and click **Delete** to delete them. Or click → **Delete All** to delete all visitor vehicles.
- **Filter Visitor Vehicle**: Click in the top right corner to display the filter pane.

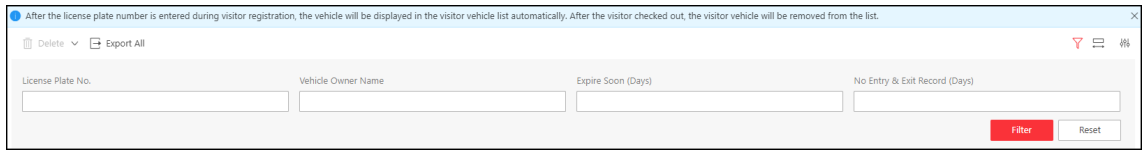



**Figure 6-5 Search for Visitor Vehicles**

**Expire Soon (Days)**

The days left before the status of the vehicle becomes **Expired**.

**No Entry & Exit Record (Days)**

The number of days during which the vehicle did not enter or exit.

- **Export Visitor Vehicles**: Click **Export All** to export the filtered vehicles to the local PC.

**Note**

If you do not filter vehicles before clicking **Export All**, all visitor vehicles will be exported.

## 6.4 Manage Vehicles in Blocklist

A vehicle added to the blocklist cannot enter the specified region as its license plate number will be recognized at the entrance. When adding a vehicle to the blocklist, the administrator can set a certain period during which the vehicle is not allowed to enter.

You can perform the following operation(s) to manage the blocklist.

| Operation | Function |
| --- | --- |
| Remove Vehicle(s) from Blocklist | • Select vehicle(s) and click **Delete** to remove the vehicle(s) from the blocklist one by one or in a batch.<br>• Click ⌄ next to **Delete** and click **Delete All** to remove all vehicles from the blocklist. |
| Export Vehicle Information | Click **Export All** to save the information of all vehicles in the blocklist to the local PC. |
| Search for Vehicles | Enter a keyword in the search box and click 🔍 to search for vehicles by license plate No., owner's first/last name, phone number, or description. |

### 6.4.1 Add a Vehicle to Blocklist

You can add vehicles to the blocklist one by one. Once added, the vehicle cannot enter the specified region during the period you set.

**Steps**

1. On the left navigation pane, click **Vehicle Management → Blocklist** .
2. Click **Add** to enter the Add Vehicle to Blocklist page.

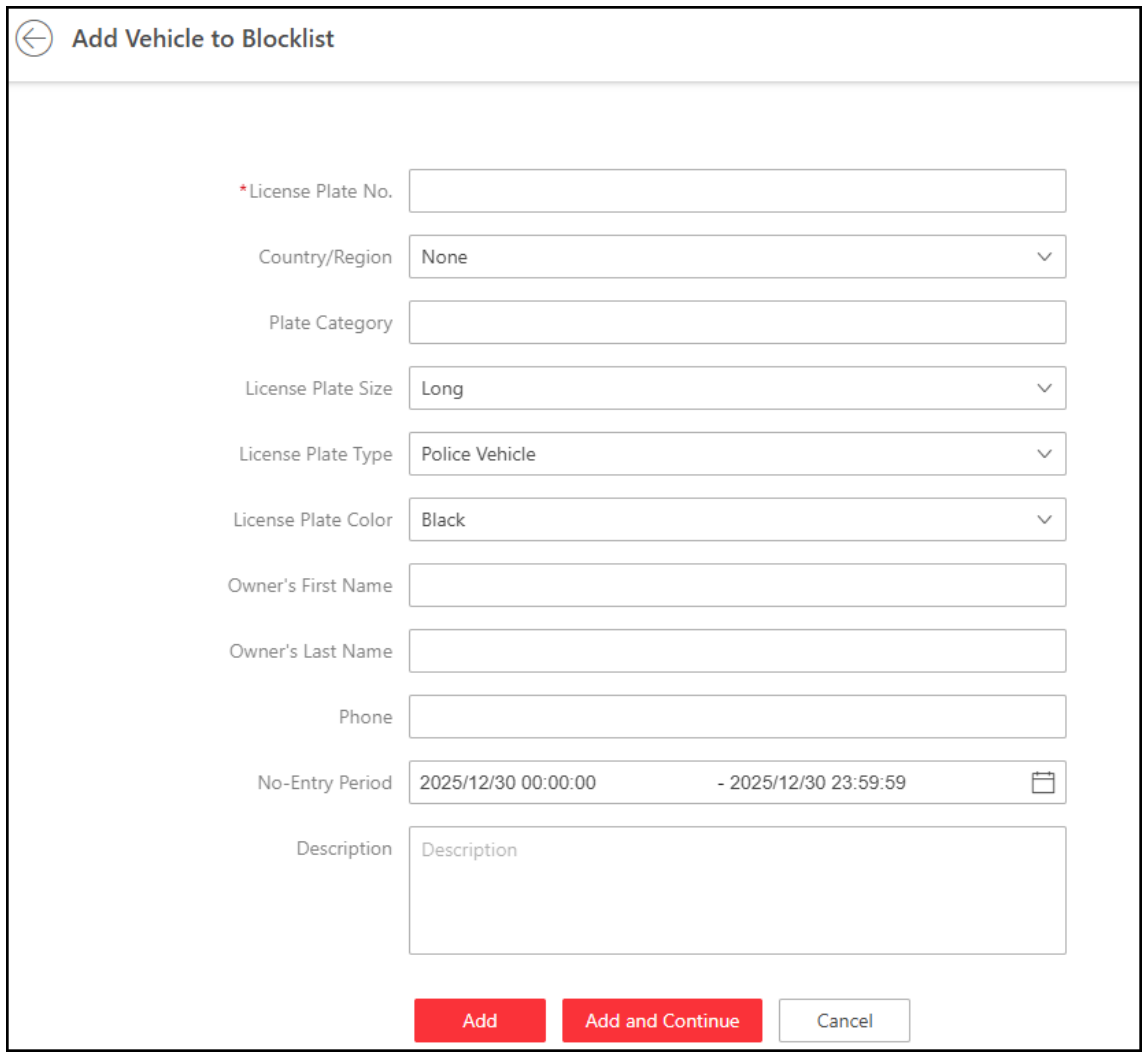



**Figure 6-6 Add Vehicle to Blocklist**

3. Enter the vehicle's license plate number.
4. Enter the country/region, plate category, license plate size, license plate type, and license plate color.

   These parameters are available for configuration only when the area is set to **Middle East and North Africa**. In accordance with SIRA license plate standards, these parameters (along with the license plat No.) serve as factors for precisely identifying the same vehicle. To more reliable recognition, it is recommended to fill out the accurate and complete information.
5. **Optional:** Enter the first name, last name, and phone number of the vehicle's owner.
6. Set the period in which the vehicle is not allowed to enter.
7. **Optional:** Enter remarks in the Description field if needed.
8. Click **Add** to finish, or click **Add and Continue** to add another vehicle.

### 6.4.2 Batch Import Vehicles to Blocklist

You can batch add multiple vehicles to the blocklist. Once added, the vehicles cannot enter the parking lot during the period you set.

**Steps**

1. On the left navigation pane, click **Vehicle Management → Blocklist** .
2. Click **Import**.

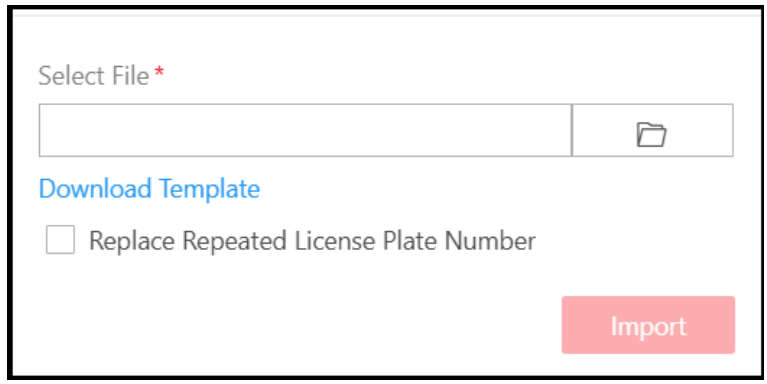



**Figure 6-7 Import File**

3. Click **Download Template** to download and save the template file to your PC.
4. Open the downloaded template file and enter the required information.
5. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing vehicle information with the new vehicle information if the file contains the license plate number which has already been added to the blocklist. Otherwise, the original vehicle information will be reserved.
6. Click **Import**.

## 6.5 Customize Vehicle Information

You can customize different items of vehicle information (such as vehicle model) which are not predefined. The customized vehicle information can help to recognize vehicles or search for vehicles more accurately.

**Steps**

1. On the left navigation pane, click **Vehicle Information**.
2. Add vehicle types.
   1) Click **Add** in the Vehicle Type area to open the Add Vehicle Type pane.

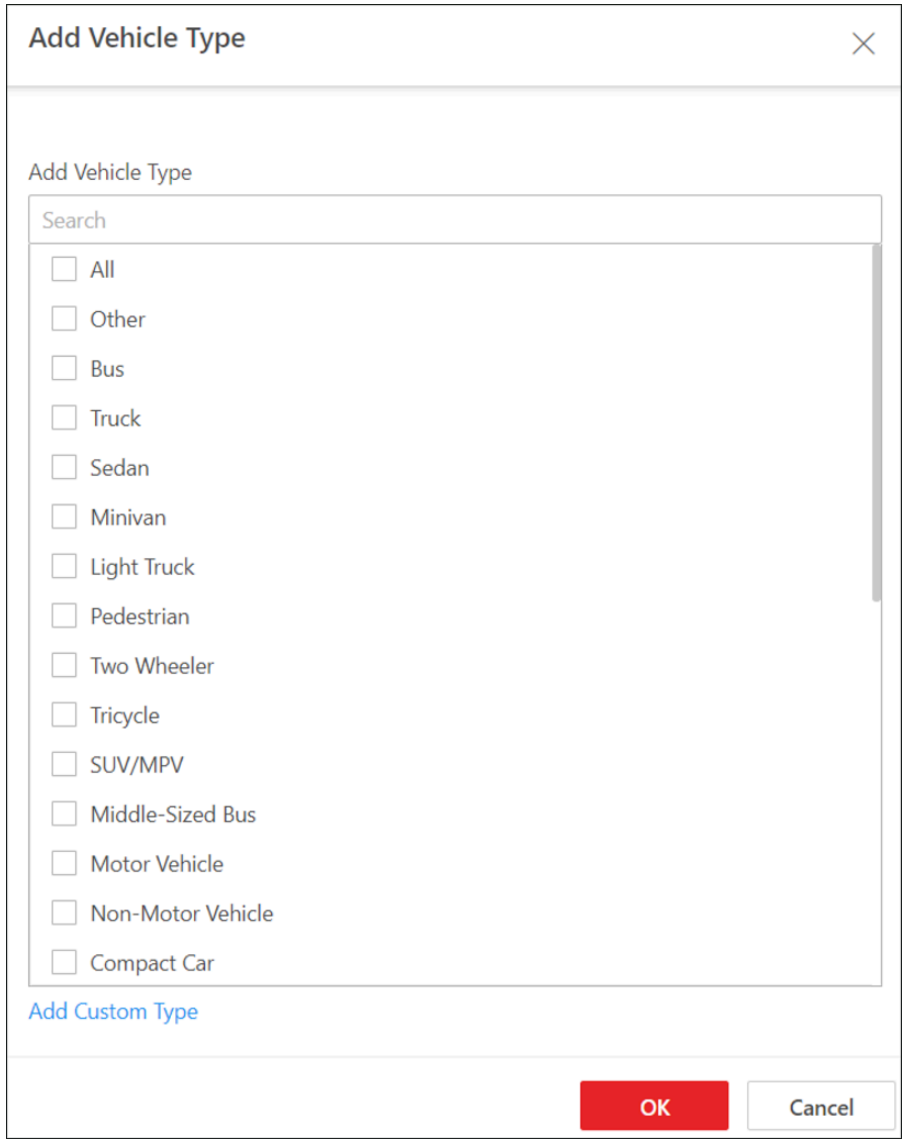



**Figure 6-8 Add Vehicle Type**

2) Check the vehicle type(s) in the list.

**Note**

If you cannot find the vehicle type you want in the list, click **Add Custom Type** to customize a vehicle type.

3) Click **OK**.

**3.** Add the additional information item(s), which can be used as the conditions during the vehicle search.

1) Click **Add** in the Additional Information area to open the following pane.

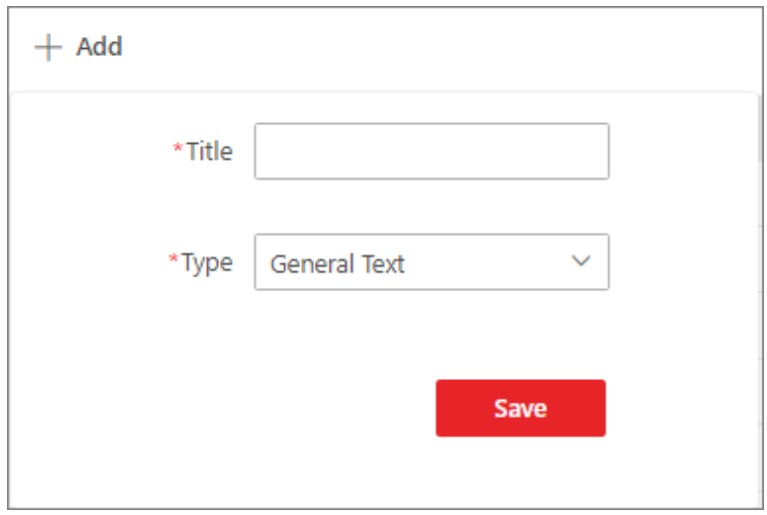



**Figure 6-9 Customize Additional Information**

2) Create a title for the information.
3) Select an information type.

**General Text**

The information must be a character string, which contains 1 to 32 characters and excepts certain special characters.

**Number**

The information must be an integer, which is between 1 to 32.

**Date**

The information must be in the date format. You should select a start date and an end date from the calendar.

**Single Selection**

The information must be selected from a drop-down list, whose options are predefined when setting the information type.

4) Click **Save**.

**4.** Set the area to **General** or **Middle East and North Africa**.

**Note**

If the area is set to **Middle East and North Africa**, the **License Plate Matching Rule** should be configured. This rule defines which license plate fields are considered when identifying two vehicles as the same.

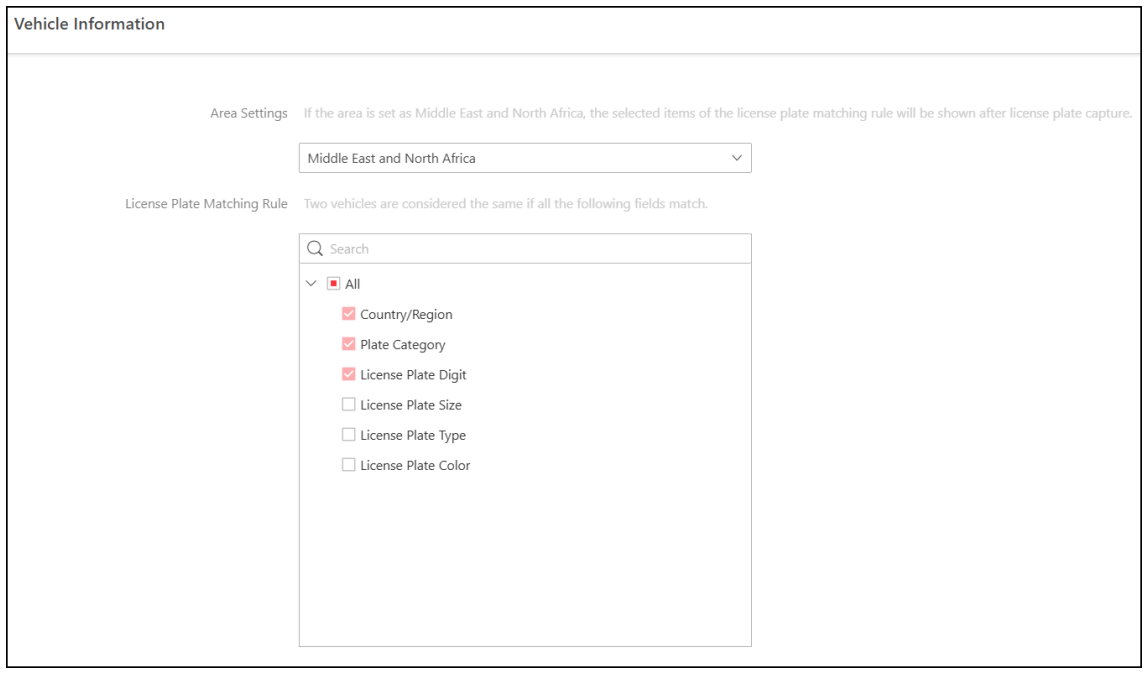



**Figure 6-10 Set Area**

## 6.6 Configure Fuzzy Matching Rules for License Plate Search

When searching for vehicles by license plate number on the Control Client, the system supports fuzzy matching. You can first set the fuzzy matching rules according to actual needs.

**Steps**

1. On the left navigation pane, click **Plate Fuzzy Search**.
2. Click **Add**.




**Figure 6-11 Add Fuzzy Matching Rule**

3. Set the rule.

   **<=>**

Enter an uppercase letter or a digit before and after this symbol respectively.

For example, 0<=>Q means: If you enter 0 or Q for search, the recognized license plate numbers with 0 and the ones with Q will be filtered.

**=>**

Enter an uppercase letter or a digit before and after this symbol respectively.

For example, G=>6 means: If you enter G for search, the recognized license plate numbers with G and the ones with 6 will be filtered. But if you enter 6 for search, the ones with G will not be filtered.

**Note**

Up to 16 rules can be added.

4. Click **Save**.
5. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Edit Rule** | Click in the Operation column of a rule to edit it. |
| **Enable/Disable Rule** | Click / in the Operation column of a rule to enable/disable it. |
| **Delete Rule** | Click in the Operation column of a rule to delete it. |

# Chapter 7 Management of Platform Accounts and Security

You can manage roles and users, assign roles with varying permissions to different users, configure security parameters and questions, and configure permission schedules to enhance system security.

On the top left corner of Home page, select → **Basic Management** → **Account and Security** .

## 7.1 Add a Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

**Steps**

**Note**

The platform has predefined two default roles: Administrator and Operator, which cannot be edited or deleted.

**Administrator**

Role that has all permissions of the platform.

**Operator**

Role that has all permissions for accessing resources and operating the Applications.

1. On the left, select **Roles**.
2. Click **Add** to enter Add Role page.
3. Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

   **Copy From**

   Copy all settings from an existing role.

   **Permission Schedule Template**

   Set the authorized time period when the role's permission is valid. Select **All-day Template**/**Workday Template**/**Weekend Template** as the permission schedule of the role, or click **Add** to customize a new permission schedule template.

   - When a role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.
   - The permission schedule's time zone is consistent with that of the platform.
   - By default, the role will be linked with All-day Template after updating the platform.
   - The permission schedule also goes for RSM client and OpenSdk client.

4. Configure permission settings for the role.

**Area Display Rule**

Show or hide specific area(s) for the role. If an area is hidden, the user assigned with the role cannot see and access the area and its resources.

**Resource Access**

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

**Note**

If you do not check the resources, the resource permission cannot be applied to the role.

**User Permission**

The role's permission for different operations on the platform. On the Custom tab, check permission items for the role and click **Save as a Template** so that the template can be applied to other roles. On the Use Template tab, select a permission template from the drop-down list for the role, and the permission details will show below.

5. Click **Add** to add the role and return to the role management page, or click **Add and Continue** to save the settings and continue to add another role.
6. **Optional:** After adding a role, you can perform the following operations on the Roles page.

**Disable a Role** Check a role and click **Inactivate**. Inactivated roles cannot be assigned to any user.

**Enable a Role** Check a role and click **Activate**.

**Refresh Roles** If any changes has been made for roles on the Server, you can click **Refresh All** to synchronize the changes to the current client.

**Filter Roles** On the upper right of the Roles page, click different buttons to filter roles.

**Assigned**

The role assigned to the current user.

**Created by Me**

Role(s) created by the current user.

**Others**

Roles except the role assigned to the current user and roles created by the current user.

## 7.2 User Management

### 7.2.1 Manage Different Users via a User Group

Add normal users or domain users to different user groups for convenient management.

#### Step 1 Add a User Group

On the left, select **Users → User Group →** ＋ , and then enter the group name to add. After adding, the group will be displayed in the left group list, and you will be guided to the Roles tab on the right for assigning role(s) to the group.

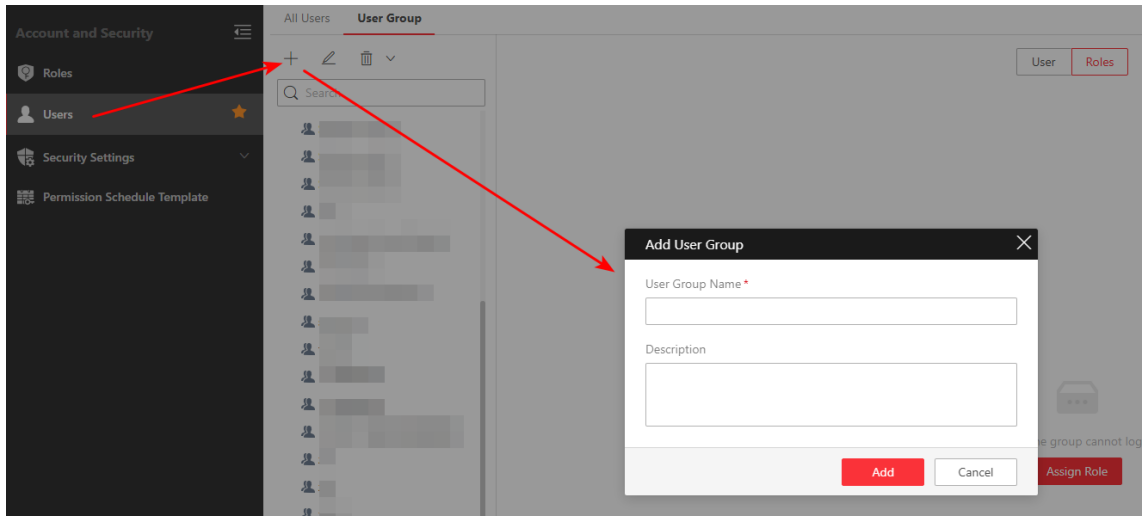



**Figure 7-1 Add a User Group**

#### Step 2 Assign Roles to the User Group

On the right, click **Assign Role**. Check role(s) and click **Save** to assign the permission of selected role(s) to the group. Users in this group will all share the same permission.
After the assignment, the assigned role(s) will be displayed in the role list. You can click **Assign Role** to edit roles of the group, or check a role and click **Unassign Role** to cancel the permission of the selected role.

#### Step 3 Add Normal/Domain Users to the User Group

On the top, click the **User** tab, and then click **Add User** in the middle. Then, check users and click **Add**. The added users will be displayed in the User tab page.
You can click **Synchronize Domain Users** to add domain users to the current group.

#### Other Operations

For existing user groups, perform the following operations if needed.

- Select a user group, and click **Add** to add more users to the current group.
- Check user(s) in a group and click **Move** to remove selected user(s) from the current group, or move selected user(s) to other groups.
- For other options such as Force Logout, Inactivate, Activate, Unlock for Login, see ***Operations After Adding Users*** .

### 7.2.2 Add a Normal User

You can add normal users and assign roles to them for accessing the system and assign role to the normal user. Normal users refer to all users except the admin user.

**Steps**

1. On the left, select **Users → All Users** .
2. Click **Add** on the top.
3. Set basic information and parameters related to login protection and permission for the user.

**Password**

Create an initial password for the user. The user will be asked to change the password when logging in for first time.

**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.

**Email**

The email address of the admin user can be edited by the user assigned with the role of administrator.

**User Status**

**Active** is selected by default. If you select **Frozen**, the user account will be forbidden to login until you activate it.

**Restrict Concurrent Logins**

To limit the maximum IP addresses logged in to the platform using the user account, switch on **Restrict Concurrent Logins** and enter the maximum number of concurrent logins.

**Allow Remembering Password When Login**

**Via Mobile Client / Control Client**

When you log in to the Mobile Client / Control Client, the password will be remembered by default. If the password does not need to be remembered, you can uncheck it.

**Require Email Verification When Login**

The admin user is not required when logging into the Server.

**Login via Authorization**

This feature is designed for configuring the validity period of user access to remote sites. As the platform's password expires every 3 months, modifying password of remote sites results in all sites in the central system going offline, requiring manual password updates one by one.

This mechanism replaces traditional passwords, enabling password-free login for remote sites. When the **Login via Authorization** is enabled, an AK/SK is automatically generated, and the validity period can be set (1/3/6 months or customized). The keys are hidden by default and can only be displayed after entering the administrator password for verification.

After adding the user, you can regenerate the AK and SK on the user details page.

**PTZ Control Permission**

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit. If the user with higher permission locks the PTZ, the user with lower permission level will not be able to control the PTZ unit. For example, when two users control the PTZ unit at the same time, the user who has the higher PTZ control permission level takes control of the PTZ.

**Set as Default Recipient**

It is not selected by default. If it is selected, the user will be able to receive alarms triggered by devices that he/she has permission to access.

**Join User Group**

Add the current user to an existing user group for convenient management.

**Assign Role**

Select the roles that you want to assign to the user. If no role has been added, two default roles are selectable: administrator and operator.

**Administrator**

The role that has all permissions.

**Operator**

The role that has all permissions of the HikCentral Professional Control Client.

**Note**

If you want to add new roles, click **Add**. See ***Add a Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

4. Click **Add** to add the user and return to the user management page, or click **Add and Continue** to save the settings and continue to add another user.

### 7.2.3 Import Domain Users

You can batch import the users (including the user name, real name, and email) in the AD domain to the platform and assign roles to the domain users.

**Note**

Make sure you have configured active directory settings. See ***Set Active Directory*** for details.

On the User List page, click **Import User → Via Domain Group** .

**Importing Mode**

**User in Organization Unit**

Import individual domain users.

**User in Security Group**

Import individual domain users in security groups of any organization unit.

**Organization Unit**

Import all domain users in the selected organization unit.

**Note**

The platform does not support this function if the Azure domain is configured.

**Security Group**

Import all domain users in the selected security group(s).

For parameters related to user status, login protection, and permission, see ***Add a Normal User*** .

Click **Add** to import the domain users and return to the user management page; or click **Add and Continue** to save the settings and continue to import other domain users.

After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client, Control Client, and Mobile Client with their domain accounts and passwords.

### 7.2.4 Import Normal Users via an Excel File

You can import normal users via a template (an Excel file) to batch add normal users.

Above the user list, click **Import User → Via Excel** on the top.

Click **Download Template** to download the template file.

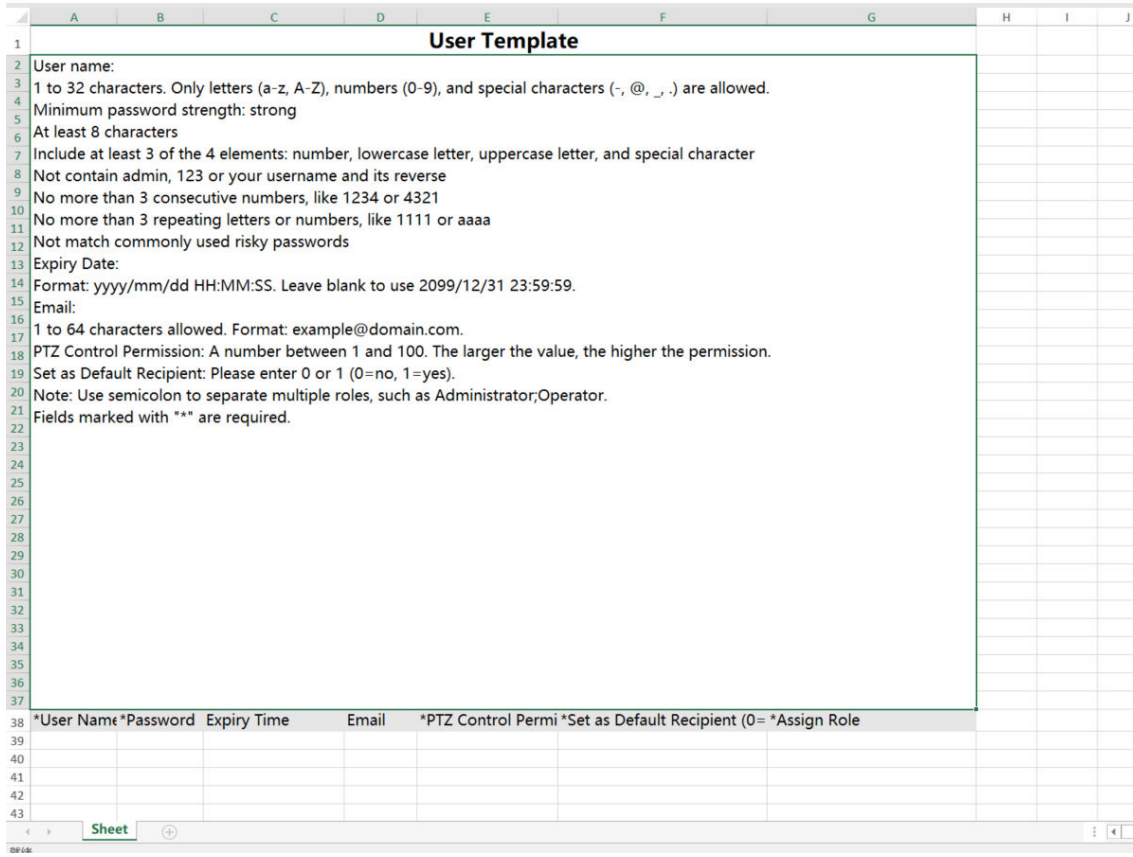



**Figure 7-2 Template File**

Enter user information in the downloaded template file and click to select the edited template file. You can also select an exported file with edited information of multiple users to modify user information.

You can check **Replace Repeated User Name** to replace the user name in the list which is duplicate with the imported user name.

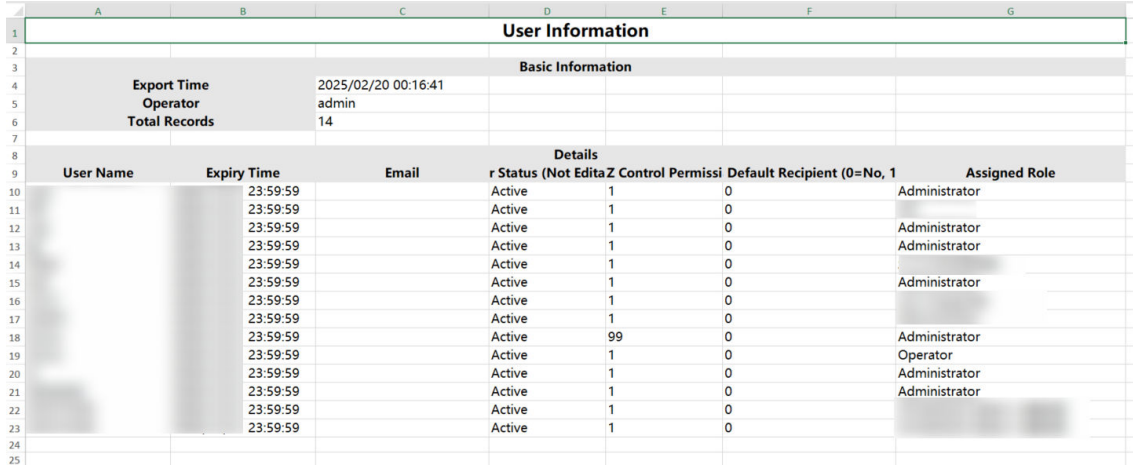
## 7.2.5 Operations After Adding Users

In the Users list, you can perform the following operations if needed.

**Table 7-1 Operations After Adding Users**

| Operation | Description |
|---|---|
| Synchronize Domain Users | After importing the domain user information to the platform, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the platform. If the users are imported by group, it will synchronize the |

| Operation | Description |
|---|---|
| | latest user information from the domain group (including added users, deleted users, edited users, etc., in the group). |
| Force Logout a User | In the user list, select an online user and click **Force Logout** to log out the user. |
| Disable a User | Check a user and click **Freeze**. Frozen users cannot log into the platform. |
| Enable a User | Check a frozen user and click **Unfreeze**. |
| Unlock a User | For users whose account is locked due to too many login failures, Administrators can unlock their accounts for login. |
| Refresh All | If any changes has been made for users on the Server, you can click **Refresh All** to synchronize the changes to the current client. |
| Export Normal Users | Select users in the user list and click **Export User** on the top. Confirm your password and click **Export**. |



User Information

Basic Information

| | |
|---|---|
| Export Time | 2025/02/20 00:16:41 |
| Operator | admin |
| Total Records | 14 |

Details

| User Name | Expiry Time | Email | r Status (Not Edita | Z Control Permissi | Default Recipient (0=No, 1 | Assigned Role |
|---|---|---|---|---|---|---|
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | |
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | |
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | |
| | 23:59:59 | | Active | 1 | 0 | |
| | 23:59:59 | | Active | 99 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | Operator |
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | Administrator |
| | 23:59:59 | | Active | 1 | 0 | |
| | 23:59:59 | | Active | 1 | 0 | |

**Figure 7-3 Exported User File**

## 7.3 System Security Settings

### 7.3.1 Set Basic Security Parameters

System security is crucial for your system and property. You can lock IP address to prevent malicious attacks, enable auto lock the Control Client, and set other security settings to increase the system security.

Select **Security Settings → Basic Parameters** on the left.

**Max. Failed Attempts Before Lockout**

Select the maximum allowable login attempts. Failed login attempts include failed password attempt and failed verification code attempt.

**Lock Duration**

Set the lock duration for this IP address. During the lock duration, the login attempt via this IP address is not allowed.

**Minimum Password Strength**

Define the minimum complexity requirements that the password should meet.

**Enable Maximum Password Validity Period**

Force user to change the password when the password expires.

**Password Will Expire In**

Set the maximum number of days that the password is valid. After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

**Days to Remind Before Password Expiration**

Set days to remind you at each time you login or in the small hours of each day by sending an email notification before password expiration. The Password Expiry Email Template is displayed below. You can click **View** to view or edit the template.

**Web Login Expires If No Action Within**

Set minutes after which the Web login will expire if there is no actions during the set minutes.

**Auto Lock Control Client**

The Control Client will be automatically locked after a time period of inactivity on the Control Client. You can select the predefined time period or customize the time period.

**Auto Log Out Mobile App**

The Mobile Client will be automatically logged out if there is no operation in a set time period. You can select the predefined time period or customize a time period.

**Request Terms Agreement for Mobile Client Login**

If it is checked, users should agree to the terms each time they log in to the Mobile Client.

**Double Authentications**

Select the authenticator and the users who need authentication. Double authentications means the users who need authentication should let the authenticator enter the user name and password so that they can use the functions of manual recording, video playback, and video exporting. Resources on the site support double authentication. Only one resource can be configured for a user who needs authentication.

### 7.3.2 Configure Security Questions

Security questions can be used to verify user identity when users want to reset the password. After setting the security questions, users needs to first answer the security questions correctly before they can reset the password, so as to ensure account security.

Select **Security Question** on the left.

Select a question from the drop-down list and set an answer to it. The answer is not case sensitive.

Resetting Administrator login passwords via security questions is exclusively permitted on the server. Should incorrect security answer attempts exceed the permitted limit, password modifications will be disabled. This restriction defaults to a 10-minute duration.

Click **Save** to save the settings.

### 7.3.3 Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.

**Steps**

1. Move the cursor to the user name at the top-right corner of the Web Client.
2. In the drop-down list, click **Change Password** to open the Change Password panel.

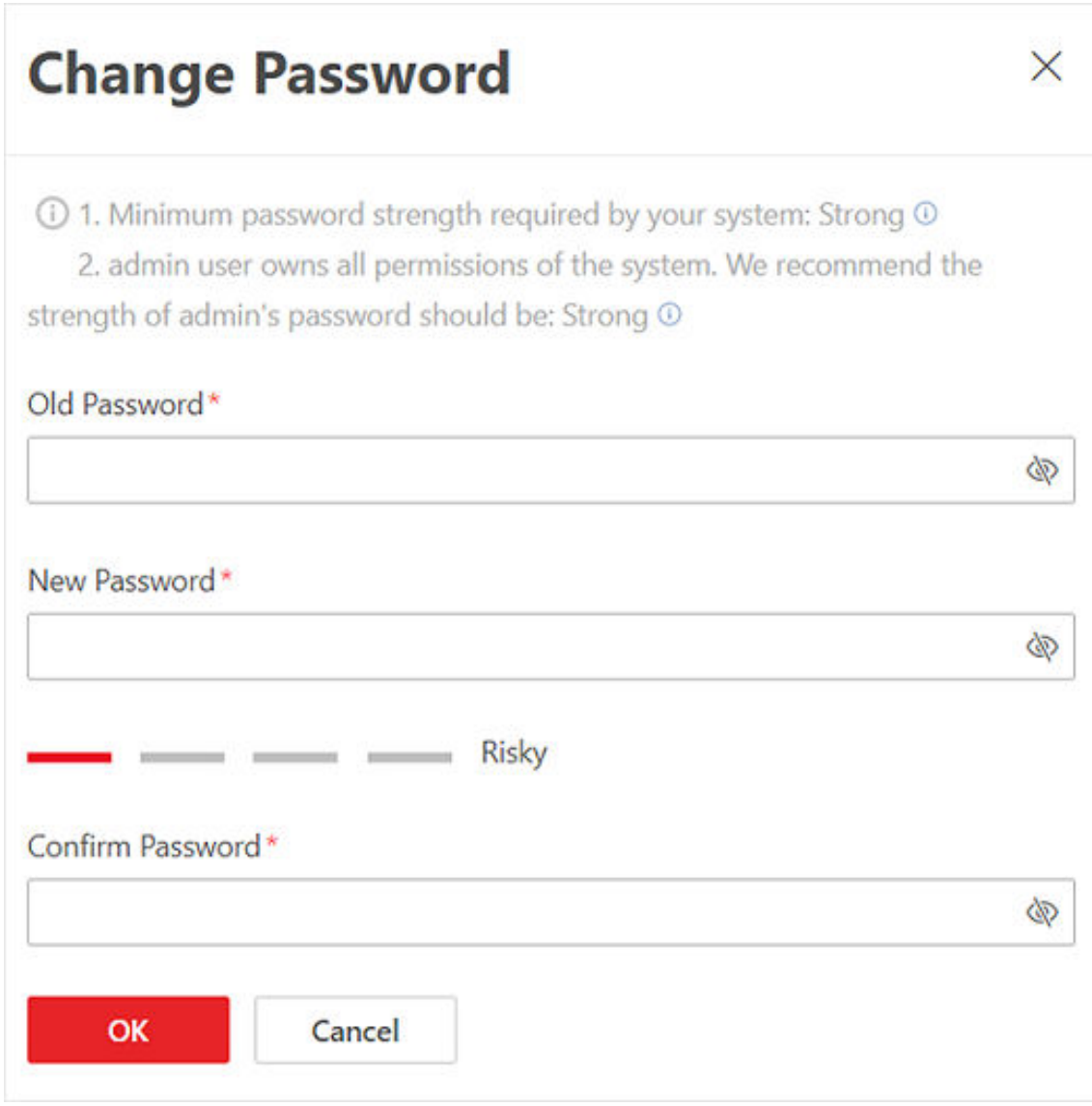



**Figure 7-4 Change Password Panel**

**3.** Enter the old password and new password, and confirm the new password.

**Caution**

The password strength of the device can be checked by the system. 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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

4. Click **OK** to save the change.

### 7.3.4 Forgot Password

If you forget the password of your account, you can reset the password.

**Before You Start**

- Make sure the normal user has been configured with an available email address.
- Make sure the email server is tested successfully.

**Steps**

1. On the login page, click **Forgot Password**.
2. Enter your user name and click **Next**.
3. Enter the required information on the Reset Password window.
   - If you are the admin user whose account is configured with security questions, you can only reset passwords on the server. Should incorrect security answer attempts exceed the permitted limit, password modifications will be disabled. This restriction defaults to a 10-minute duration.
   - If you are the admin user or a normal user whose account is configured with an email address, you can click **Get Verification Code** and a verification code will be sent to your email address. Enter the verification code you received, set a new password, and confirm the password within 10 minutes.

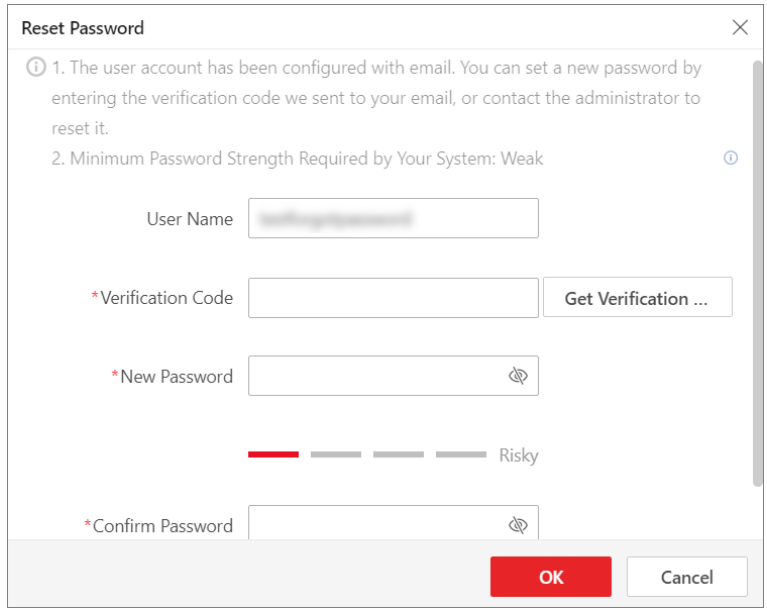



**Figure 7-5 Reset Password via Verification Code**

**Note**

If no email address is set for your normal user account, you need to contact the admin user to reset your password.

- If you are an admin whose account is configured with an email address, you can select **Activation Code** and click **Next**, and then reset the password by the code you get.

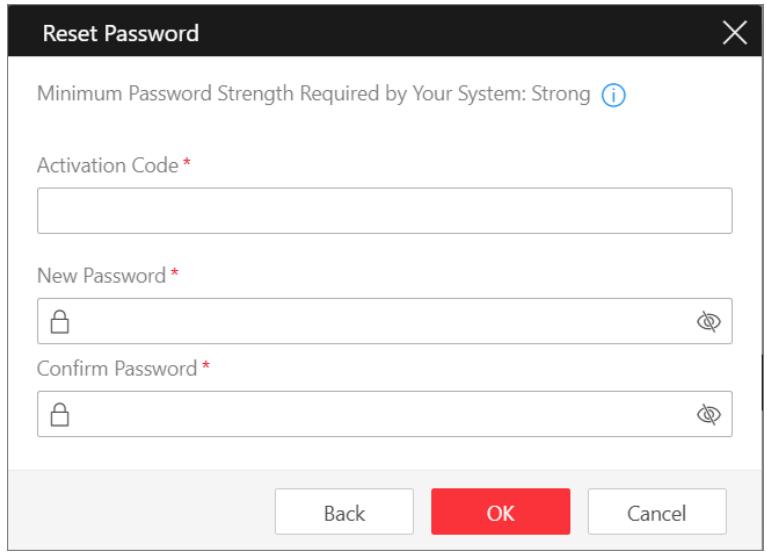



**Figure 7-6 Reset Password via Activation Code**

- If you are a domain user, you need to contact the admin user to reset your password.

**Note**

The password strength can be checked by the system and should meet the system requirements. If the password strength is lower than the required minimum strength, you will be asked to change your password. For setting the minimum password strength, refer to ***Set Basic Security Parameters*** .

**Caution**

- The password strength of the device can be checked by the system. 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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
  The password should:
  - Not contain admin, 123 or your username
  - Have no more than 3 consecutive numbers, like 1234 or 4321

- Have no more than 3 repeating letters or numbers, like 1111 or aaaa
- Not match commonly used risky passwords

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

4. Click **OK**.

## 7.4 Configure Permission Schedule

Permission schedule defines the time when a role's permissions are valid. During unauthorized time periods, the user assigned with the role will be forced to log out and cannot log in. The platform provides 3 default permission schedule templates: All-day Template, Workday Template, and Weekend Template. You can add new templates according to actual needs.

**Steps**

1. On the left, select **Permission Schedule Template**.
2. Click + on the top left.
3. Set basic information.

   **Copy From**

   Copy the settings from another existing template.
4. In the **Weekly Schedule** area, click **Authorize** to select or draw in the box to define the authorized time periods.

   **Note**

   You can set up to 6 separate time periods for each day.
5. **Optional:** Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.

   The holiday schedule has a higher priority than the weekly schedule.
6. Click **Add** to add the permission schedule template.

# Chapter 8 System Configuration

This module allows you to set different types (e.g., normal settings, network settings, storage settings, and so on) of parameters for the platform, such as defining a customized name for the site, setting NTP (Network Time Protocol) for synchronizing the time between the platform and the NTP server, and setting an IP address to allow the platform to access the WAN (Wide Area Network).

In the top right corner of the Web Client, select → **Basic Management** → **System** or click **System** on the top navigation bar (if the menu is added to the navigation bar) to enter this module.

## 8.1 Normal Settings

The normal settings menu provides entries of setting the user preference, holidays, printers, and card templates.

On the left navigation bar of the System page, select **Normal** to display the normal settings menu.

### 8.1.1 Set User Preference

For different countries, regions, cultures, and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, such as the site name, the first day of a week, and the calendar type.

Select **User Preference** on the left navigation bar to enter the following page.

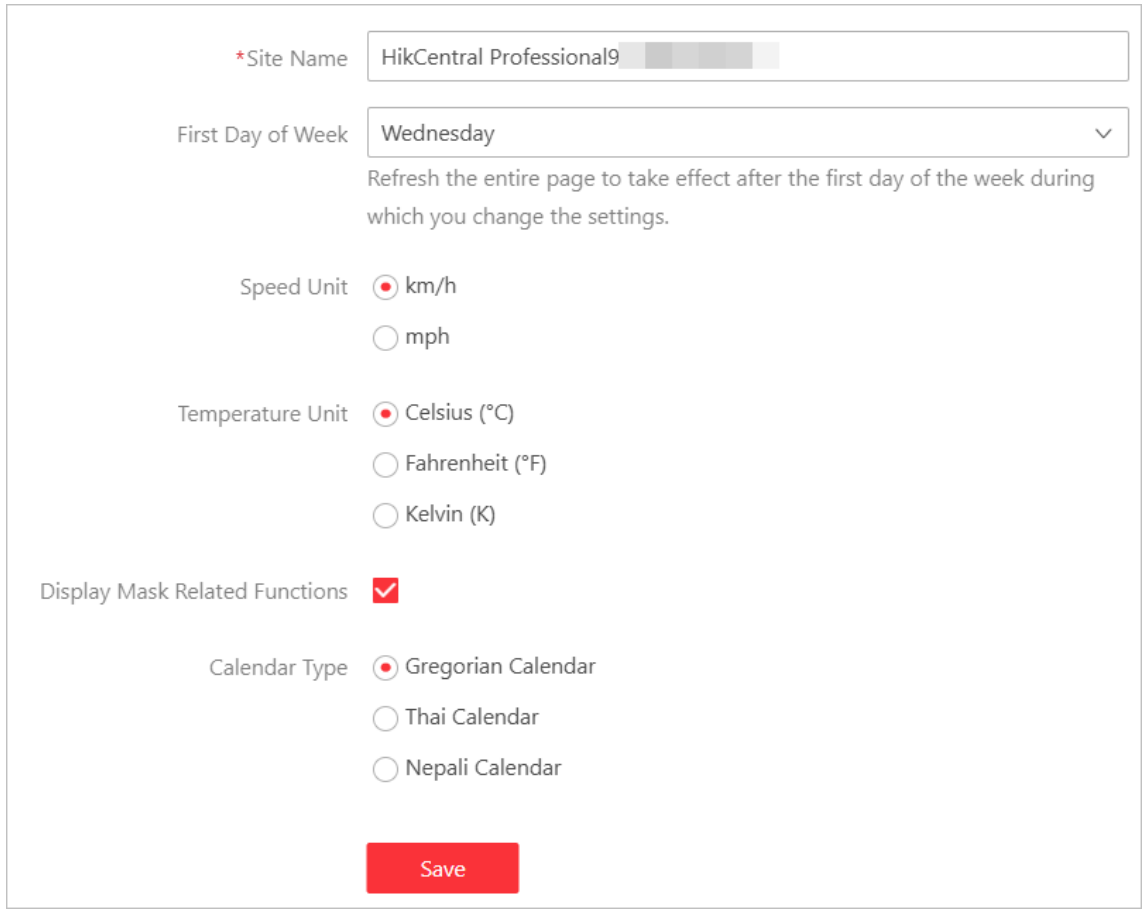



**Figure 8-1 User Preference**

Set the following parameters:

**Site Name**

Set the name of current site.

**First Day of Week**

Set the first day of a week as Sunday, Monday, Tuesday, etc., according to the custom of the actual scene.

**Note**

This parameter is used in the report generation, live view and playback, attendance settings, etc.

**Speed Unit**

Select vehicle speed units to accommodate usage habits in different regions worldwide. This parameter is applicable to businesses including ANPR, Portable Enforcement, Traffic Incident Monitoring, and On-Board Monitoring.

**Temperature Unit**

Set the temperature unit according to the custom of the actual scene.

**Note**

This parameter is used in the temperature analysis report generation, etc.

**Display Mask Related Functions**

Set whether to display mask related functions. Check the box to display the functions about masks on Control Client, Web Client and Mobile Client. Otherwise these functions will be hidden.

**Note**

This parameter is mainly used in temperature screening module.

**Calendar Type**

Set the calendar type as Gregorian Calendar, Thai Calendar and Nepali Calendar according to the custom of the actual scene.

## 8.1.2 Set Holiday

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday and an irregular holiday according to the actual scene.

Select **Holiday Settings** on the left navigation bar to enter the Holiday Settings page.

### Add Regular Holiday

The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of each year.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Regular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   **Start Time**

   The start date of the holiday.

   **Number of Days**

   The lasting days of the holiday.

   **Repeat Annually**

   If checked, the platform will generate the date of the holiday according to the date of SYS (System Server).
4. Click **Add**.

### Add Irregular Holiday

The irregular holiday is suitable for the holiday that is calculated by the weekdays, and the specified date might be different in a different year. For example, Mother's Day is on the second Sunday of each May.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Irregular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   **Start Time**

   The start date of the holiday.

   For example, select **May**, **Second**, and **Sunday** for Mother's Day.

   **Number of Days**

   The lasting days of the holiday.

   **Repeat Annually**

   If checked, the system will generate the date of the holiday according to the date of SYS.

   **Note**

   If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of SYS.
   For example, Mother's Day in 2019 and 2020 is on May 12th, 2019, and on May 10th, 2020. The system will automatically set these two days as holidays for Mother's Day if you have checked **Repeat Annually**.
4. Click **Add**.

## 8.1.3 Set Printer

You can set printers for the platform, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

**Note**

Make sure that the printers are installed on the same network with SYS.

Select **Printer Settings** on the left navigation bar to enter the Printer Settings page.

Click **Add** to select the printer(s) detected by the platform.

**Note**

After setting a printer for the platform, you can link the printer when configuring alarm/event whose source type is alarm input.

You can click in the Operation column to delete a printer or click **Delete All** to delete all added printers.

### 8.1.4 Set Card Template

The platform has provided two predefined card template for you. If they do not meet your requirements, you can set styles for card templates by yourself. After settings, the card will be applied in the format of the template.

**Steps**

1. Select **Card Template** to enter the Card Template page.
2. Click **Add**.
3. Create a name for the template.
4. **Optional:** Select the shape of the template.
5. Set the front style of the template.

| | |
|---|---|
| **Insert Picture** | Click **Insert Picture** to select a picture for the template. |
| **Insert Background Picture** | Click **Insert Background Picture** to select a background picture for the template. |
| **Insert Text** | Click **Insert Text** to set the text for the template. |
| **Customize Contents** | Check the attribute(s) for the content of the template. You can also click **Additional Information** to customize the attributes for the template. |
| **Configure Text Settings** | • Select a text box and set the font type, font size, font color, and bold front for the text in the box.<br>• Select one or multiple text boxes and click , , or in the Text Alignment field to adjust the alignment of the text in the box.<br>• Select multiple pictures or text boxes and click , , or in the Content Alignment to adjust these elements.<br>• Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the picture or text box displayed on the template.<br>• Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Delete** to remove the picture or text box. |

6. **Optional:** Refer to the previous step to set the back style of the template.
7. Click **Add** to add the template and go back to the card template list page.

   The added card template will be listed on the Card Template page.
8. **Optional:** Perform the following operation(s).

| | |
|---|---|
| **View Template** | Click in the Operation column to view the template details. |
| **Edit Template** | Click in the Operation column to edit template details. |

**Note**

The predefined card templates cannot be edited.

**Delete Templates**

Click in the Operation column of a template or click **Delete All** at the top to delete the template or delete all added templates.

**Note**

The predefined card templates cannot be deleted.

## 8.2 Calling Settings

You can add call recipients for receiving and answer calls, add receiving schedule templates defining when users can receive calls, and configure call parameters such as record storage.

### 8.2.1 Add Call Recipients

You can add users in the platform as call recipients. After adding call recipients, when someone calls the system, the added recipients can receive and answer the call.

Go to **Call Settings → Call Recipient** on the left.

Click **Add**, select users to receive calls, set devices for receiving calls from, select a receiving schedule template, and click **Add**.

### 8.2.2 Add a Receiving Schedule Template

Receiving schedule template defines when the user can receive calls. For example, if a resident is absent from home during workdays and is at home during weekends and holidays, the resident can customize a schedule template to receive calls from device during weekends and holidays.

**Steps**

1. Go to **Call Settings → Receiving Schedule Template** .
2. Click + to add a schedule template.

   The default templates, namely All-Day Receiving Schedule Template, cannot be edited or deleted.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy from** drop-down list.
5. Draw the receiving time. Click a grid or drag the cursor on the time line to draw a time period during which the user can receive calls.

**Note**

- Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  .
- Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.

6. **Optional:** Click **Add Holiday** to select a holiday template.
   1) You can select an existed holiday template, or click **Add** below the template list to configure a new template in the pop-up window.
   2) Click **Add**.
   3) Click a grid or drag the cursor on the time line to draw the receiving time as shown in the previous step.

**Note**

See ***Set Holiday*** for detailed information of configure a holiday template.

7. Click **Add** to save the template.
8. **Optional:** Select a template from the template list, and then click to delete it.

**Note**

Schedule templates that has been linked cannot be deleted.

### 8.2.3 Configure Call Parameters

You can configure call parameters, including record storage, calling parameters of radar, access control or video intercom devices, and whether to receive calls from devices to the platform.

Go to **Call Settings → Call Parameter** on the left.

Configure the following parameters as needed, then click **Save** to save settings.

**Records Storage**

You can store the records generated in the operation of video intercom, such as the records of linking the video or audio files to call logs.

Select **Local Storage** or **pStor** from the drop-down list to store the records on the local PC or on the pStor server. After that, you can view and select the corresponding resource pool.

**Note**

For **Local Storage**, make sure you have enabled local storage and added the local resource pool. For details, refer to ***Set Storage on System Server*** .

**Radar Devices Calling Parameters**

Supports configuring calling parameters of radar devices. You can select local ringtone files, valid only for calls received on the platform.

- **Max. Ring Duration**: The maximum duration of the ringtone when the radar device calls.
- **Max. Speaking Duration**: The maximum duration during which you can speak with the radar device.

**Access Control or Video Intercom Devices Calling Parameters**

Supports configuring calling parameters of access control or video intercom devices. You can select local ringtone files, valid only for calls received on the platform.

**Receive Calls**

Enable this to receive call from devices to the platform.

**Auto Record Two-Way Audio**

When enabled, two-way audio from the Web and Control Clients is automatically recorded and uploaded to the server. Recordings are available for download in **Video Intercom → Video Intercom → Recents → Operation → Download** .

**Note**

Auto-recording with a watermark will not function unless you download and install the video intercom plugin first.

## 8.3 Network Settings

The network settings menu provides entries of setting NTP for time synchronization, selecting device access protocol, setting an IP address to allow the platform to access the WAN, and so on.

On the left navigation bar of the System page, select **Network** to display the network settings menu.

### 8.3.1 Set NTP for Time Synchronization

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server.

**Steps**

1. Select **Network → Internet Time Sync** .

   Three time synchronization methods are supported. For time synchronization via network and the local server, just set the synchronization interval and click **Save**. For time synchronization via the NTP server, follow steps below.
2. Set the NTP server address and port No.

   **Note**

   If the local NTP server has been configured, click **Detect Local NTP** to fill in the NTP server address and port No. automatically.
3. Enter the interval of the automatic time synchronization.

4. **Optional:** Click **Test** to test the communication between resources and the NTP server.
5. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port No. for WAN mapping.

**Note**

If the NTP service is locally deployed, you can configure WAN mapping to synchronize the time for devices on the WAN. Otherwise, enabling mapping is not required.

6. Click **Save**.

### 8.3.2 Azure Connection

Once Azure application credentials (Tenant ID, Client ID, Client Secret) are configured in a global page, they will be shared across both Active Directory (AD) integration and Email Service configurations. Only major enterprise email service providers are supported, including Microsoft Outlook, Office 365, and Google Gmail.

#### Before You Start

Before configuring the Azure Connection, you must register an application to obtain the necessary credentials.

**Required API Permissions**

Ensure you have granted the following permissions to your registered application in the Azure Portal so that both AD and Email features can function properly:

- Active Directory: ***User.Read.All***
- Email Service: ***Mail.Send***

#### Configuration Steps

Click **Azure Connection** on the left, enter the Azure application credentials you obtained from the Azure Portal.

**Tenant ID**

The directory ID of your Azure instance.

**Application (Client) ID**

The unique identifier for your registered application.

**Secret ID**

The name of the client secret you generated.

**Client Secret Value**

The actual secret value for your application.

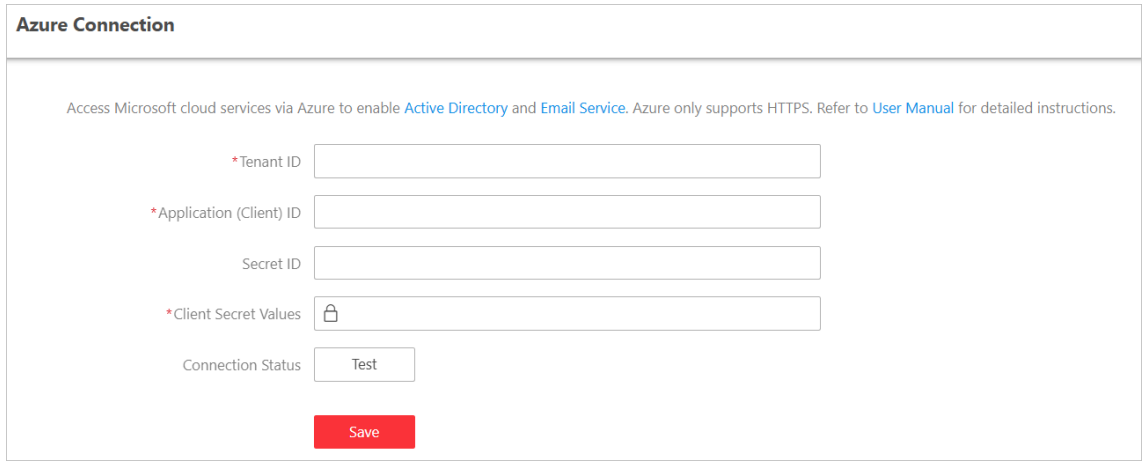



**Figure 8-2 Azure Connection**

Click **Test** to verify the connection status. Ensure the connection is successful before proceeding.
Click **Save** to store the global Azure configuration.

### 8.3.3 Set Active Directory

If you have an AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you can configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (OU) (e.g., a department of your company) to the platform conveniently.

**Steps**

1. Select **Active Directory** on the left navigation bar.
2. Select **Local Active Directory** or **Azure Active Directory** as the domain type
3. Configure the corresponding parameters for connecting the platform to the AD domain controller.

   **Local Active Directory**

   **Domain Name**

   The domain name of the AD domain controller. You can get it from the CMD window.

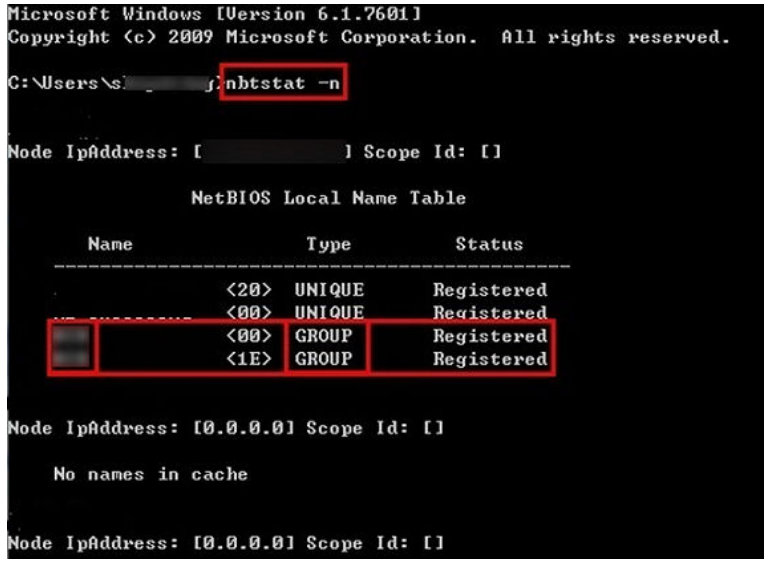



**Figure 8-3 How to Get NetBIOS Domain Name**

**Host Name**

The IP address of DNS server. You can get it in Network Connection Details.

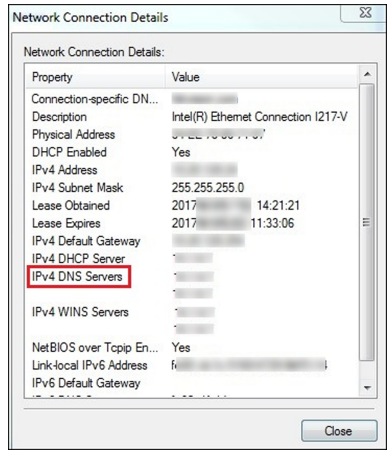



**Figure 8-4 How to Get Host Name**

**Port No.**

The port No. of the AD domain controller. By default, it is 389.

**Enable SSL (Optional)**

Enable SSL if it is required by the AD domain controller.

**User Name / Password**

The user name and password of the AD domain controller. The user should be the domain administrator.

**Base DN (Distinguished Name)**

Enter the filter condition in the text field if you are familiar with the format. Or you can click **Fetch DN** to get the filter condition entered automatically.

**Note**

- Only users found within an OU in the domain can be imported.
- If you enter the Base DN manually, you need to define the root node as desired. If you click **Fetch DN**, then the entire structure stored in the AD domain controller will be obtained.

**Azure Active Directory**

The credentials will be synchronized after a global configuration on the **Network → Azure Connection** page.

4. Set the time to automatically synchronize the users in the AD domain to the platform.
5. **Optional:** Link the person information you are concerned about in the domain to the person information on the platform.

**Note**

Once enabled, the corresponding person information on the platform will match the linked person information in the domain and cannot be edited.

1) Switch on **Linked Person Information**.

The basic and custom additional information items (see *Customize Additional Information*) are displayed by default. You can set the relationship for those or add new person information items as needed.

2) **Optional:** Click **Add** to add a person information item you are concerned about.

**Note**

- You do not need to add the basic person information items (including ID, first name, last name, phone, and remark) manually, which have the default relationship with the information in the domain.
- The person information item is case-sensitive.

3) Click + to show the person information items stored in the domain and check checkboxes in the domain to link them to the custom person information item when importing the domain's persons.
4) Click and drag one item to another to change the relationship between each other.
5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship.

6. Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the **Account and Security → Users** page.

### 8.3.4 Set Device Access Protocol

Before adding devices supporting ISUP and ONVIF protocol to the platform, you need to set the related configuration to allow these devices to access the platform.

Select **Device Access Protocol** on the left navigation bar.

Switch on **Allow ISUP Registration** or check **Access via ONVIF Protocol** to allow devices to access the platform via ISUP or ONVIF protocol.

**Note**

After **Allow ISUP Registration** is switched on, you can check **Allow ISUP of Earlier Version** to allow devices to access the platform via ISUP of version 2.6 or 4.0.

### 8.3.5 Set Hik-Partner Pro Access

After setting the Hik-Partner Pro access, you can add devices to Hik-Partner Pro via HikCentral Professional.

**Steps**

1. Select **Hik-Partner Pro Access** on the left navigation bar.
2. Switch on **Access Hik-Partner Pro**.
3. Enter the installer name of Hik-Partner Pro.
4. Click **Access Now** to open the Site Access pane.
   1) Enter the access key and secret key of Hik-Partner Pro.
   2) Select a domain name where the account locates.
   3) Click **Get Site** to get sites to be accessed.

      The number of accessed sites will be displayed. You can click to view the site name.
5. **Optional:** Switch on **Synchronize Device with DDNS Configured** and select a site to synchronize devices with DDNS configured of the Hik-Partner Pro account to the selected site in Hik-Partner Pro.
6. **Optional:** Switch on **Receive Event From Hik-Partner Pro** as needed.
7. Click **Save**.

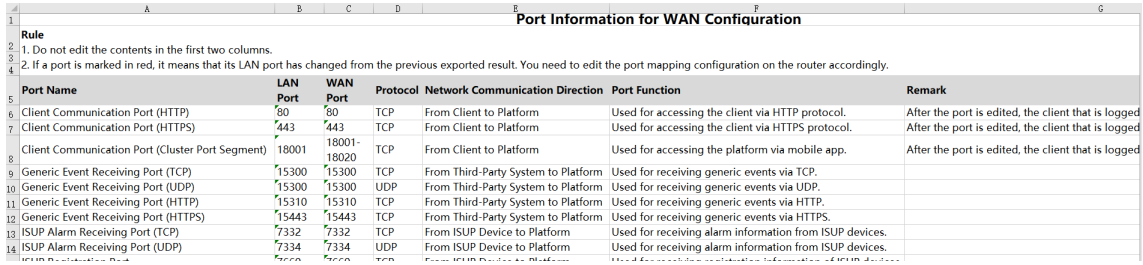
   **Note**

   After saving the settings, you cannot disable this function.

### 8.3.6 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for the platform to access WAN (Wide Area Network).

Select **WAN Access** and enable the button. You can select one or more application scenario(s) and click **Export Ports** to export an Excel file about the port information for WAN configuration.



Port Information for WAN Configuration

**Rule**

1. Do not edit the contents in the first two columns.
2. If a port is marked in red, it means that its LAN port has changed from the previous exported result. You need to edit the port mapping configuration on the router accordingly.

| Port Name | LAN Port | WAN Port | Protocol | Network Communication Direction | Port Function | Remark |
|---|---|---|---|---|---|---|
| Client Communication Port (HTTP) | 80 | 80 | TCP | From Client to Platform | Used for accessing the client via HTTP protocol. | After the port is edited, the client that is logged |
| Client Communication Port (HTTPS) | 443 | 443 | TCP | From Client to Platform | Used for accessing the client via HTTPS protocol. | After the port is edited, the client that is logged |
| Client Communication Port (Cluster Port Segment) | 18001 | 18001-18020 | TCP | From Client to Platform | Used for accessing the platform via mobile app. | After the port is edited, the client that is logged |
| Generic Event Receiving Port (TCP) | 15300 | 15300 | TCP | From Third-Party System to Platform | Used for receiving generic events via TCP. | |
| Generic Event Receiving Port (UDP) | 15300 | 15300 | UDP | From Third-Party System to Platform | Used for receiving generic events via UDP. | |
| Generic Event Receiving Port (HTTP) | 15310 | 15310 | TCP | From Third-Party System to Platform | Used for receiving generic events via HTTP. | |
| Generic Event Receiving Port (HTTPS) | 15443 | 15443 | TCP | From Third-Party System to Platform | Used for receiving generic events via HTTPS. | |
| ISUP Alarm Receiving Port (TCP) | 7332 | 7332 | TCP | From ISUP Device to Platform | Used for receiving alarm information from ISUP devices. | |
| ISUP Alarm Receiving Port (UDP) | 7334 | 7334 | UDP | From ISUP Device to Platform | Used for receiving alarm information from ISUP devices. | |

**Figure 8-5 Exported Template**

Send the template to your maintenance staff to enter the WAN port numbers, and get the completed template.

Click **Import Ports** to import the completed template.

Check the imported ports, and click **Save**.

## 8.3.7 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS (System Server) so that the platform can receive the alarm information of the device connected via ONVIF protocol, and to perform live view and playback for the devices connected via ISUP.

**Before You Start**

Make sure the server's ports ranging from 8087 to 8097 are available.

**Steps**

1. Select **Address for Receiving Device Info** on the left navigation bar.
2. Select **Get from NIC** or **Enter Manually**.

   **Get from NIC**

   Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will be displayed.

   **Enter Manually**

   If you have configured hot spare for the SYS, you should manually enter the IP address.
3. Click **Save**.

## 8.3.8 Register Remote Site to Central System

This page allows the platform without the Remote Site Management module (as we called Remote Site) to register to the Central System. The Central System is the platform that has the Remote Site Management module and can join multiple Remote Sites together to form a larger-scale union. The purpose of joining the Central System and Remote Sites is to allow the Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same platform.

**Before You Start**

For the Central System, the Receive Site Registration function should be enabled so that the Central System can receive the Remote Site registration. See ***Allow for Remote Site Registration*** for details.

**Steps**

**Note**

Registering to the Central System is only available for the platform without the Remote Site Management module.

1. Select **Site Registration and Connection** on the left.

   The Central System address and site connection status is displayed on the top.
2. Switch on **Register to Central System**.
3. Enter the IP address and port No. of the Central System.

   **Note**

   You can get the IP address and port of Central System from the Service Manager, which is installed on the PC running SYS of the Central System.
4. Click **Save**.

## 8.3.9 Allow for Remote Site Registration

This page allows the platform with the Remote Site Management module (as we called Central System) to receive the registration from Remote Sites. The Remote Site is the platform that does not have the Remote Site Management module and can register to the Central System to form a larger-scale union. The purpose of joining Central System and Remote Sites is to allow the Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

**Steps**

**Note**

Allowing for Remote Site registration is only available for the platform with the Remote Site Management module. For details about registering Remote Sites to the Central System, refer to ***Register Remote Site to Central System*** .

1. Select **Site Registration** on the left navigation bar.
2. Check **Receive Site Registration**.
3. Click **Save**.

## 8.4 Storage Settings

The storage settings menu provides entries of setting storage for pictures and files on SYS and specifying retention periods for different types of records.

On the left navigation bar of the System page, select **Storage** to display the storage settings menu.

### 8.4.1 Set Storage on System Server

The imported pictures (such as the static e-map pictures and the face pictures in the person list) and files (such as the broadcast recordings and video recordings) can be stored on SYS. You can configure the storage locations and the corresponding quotas for them.

**Steps**

**Note**

This configuration is available only when the Web Client is running on SYS.

1. Select **Storage on SYS Server** on the left navigation bar.

   The disks of SYS are displayed with current free space and total capacity.
2. Switch on **Enable Local Storage**.

   **Compatible with RSA Key Exchange**

   RSA key exchange provides lower encryption strength and is primarily used for compatibility with legacy devices that only support this method. It is disabled on newly installed systems by default. If you do not have such devices, it is recommended to keep this disabled.
3. Configure the related parameters for storing pictures.
   1) Select the disk to store the imported pictures.

      **Note**

      The disk should have at least 1.25 GB of free space for picture storage.
   2) **Optional:** Switch on **Set Quota for Pictures** and set the storage quota for the pictures.
4. Click **Add** to add a resource pool for storing files.
   1) Enter the name of the resource pool.
   2) Select a disk to store the files.

      **Note**

      The disk should have at least 9 GB of free space for file storage.
   3) **Optional:** Switch on **Restrict Quota for Pictures** and set the storage quota for the files.
   4) Check **Overwrite When Storage Space is Insufficient**, and the newly imported files will overwrite the existing files when the disk space is insufficient.
   5) Click **Add**.
   6) **Optional:** Click **Delete** or in the Operation column to delete a resource pool.
   7) **Optional:** Click a resource pool name to edit related settings.

5. Click **Save**.

### 8.4.2 Set Storage for Records

The data retention period specifies how long you can keep the events, logs, and some records on SYS.

**Steps**

1. Select **Records Storage** on the left navigation bar.
2. Select one language from the drop-down list to set the language of the sorting rule.
3. Set the data retention period from the drop-down list for the required data types.
4. Click **Save**.

## 8.5 Email Settings

The email settings menu provides entries of setting different email templates and configuring the basic email parameters.

On the left navigation bar of the System page, select **Email** to display the email settings menu.

### 8.5.1 Configure Email Templates

**Scheduled Report Email Template**

Applicable for all modules supporting generating reports. The platform will send reports to recipients once schedule reports are generated.

**Event and Alarm Email Template**

When the event or alarm is triggered, the platform can send email as the linkage action to the designate recipient regularly according to the predefined email template. You need to add a linkage action for events or alarms that you want to receive.

**Email Template for Pending Task**

When you add a custom pending task, you can enable the email notification and specify regular time to send email with the pending task information to the designated recipient regularly.

**Expiry Notification Email Template**

Notify recipients account password expiry or person effective period expiry. The email notification for account password expiry is applied by default, while you need to configure the reminder settings for person expiration settings in the Person module.

### 8.5.2 Configure Email Account

You should configure the parameters of the sender's email account before the system can send the message to the designated email account(s) as the email linkage.

**Steps**

1. Select **Email → Email Settings** on the left navigation bar.
2. Configure the parameters according to actual needs.

   **Sender Email Address**

   Enter the email address of the sender to send the message.

   **Sender Name**

   Enter the sender name to send the message.

   **SMTP Server**

   **Cryptographic Protocol**

   Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

   **SMTP Server Address**

   The SMTP server's IP address or host name (e.g., smtp.263xmail.com).

   **SMTP Server Port**

   The default TCP/IP port used for SMTP is 25.

   **Server Authentication**

   If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

   **User Name (Optional)**

   User name for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

   **Password (Optional)**

   Password for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

   **Note**

   For users of Google email, you should log in to your Google account, enable the 2-step verification function, generate the APP password, and enter here.

   **Microsoft Exchange Email**

   The credentials will be synchronized after a global configuration on the **Network → Azure Connection** page.
3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.

4. Click **Save**.

## 8.6 Security Settings

The security settings menu provides entries of setting the transfer protocol for SYS, exporting service component certificate, enabling export of profile pictures, enabling client auto update, enabling watermark in video or picture, and setting the database password.

On the left navigation bar of the System page, select **Security** to display the security settings menu.

### 8.6.1 Set Transport Protocol

You can set SYS's transport protocol to define the access mode for SYS via clients as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Select **Transport Protocol** on the left navigation bar.

In the **Transport Protocol Between Server and Web Client** field, select **HTTP** or **HTTPS**.

**Server Address**

Users can add up to 10 legitimate server addresses for HTTP/HTTPS protocols in system settings, improving flexibility.

**Note**

For HTTPS, only the TLS 1.2 and later versions are supported. The browser must support and has enabled the TLS 1.2 or later version. You are recommended to use the browser supporting TLS 1.3.

To ensure that the client connects only to trusted servers, HikCentral Professional supports server certificate validation, preventing connections to untrusted server addresses and thereby securing the communication channel. The system offers three certificate validation modes to meet security requirements in different scenarios:

**High**

Only allows connections to servers with public certificates issued by a trusted Certificate Authority (CA) or PKI certificates built by users. In this mode, servers using self-signed certificates will be rejected, ensuring the highest level of authentication and security. When users attempt to connect to a system with an invalid certificate or a mismatched hostname, a warning message will be displayed.

**Medium (Recommended)**

The Server can use only self-signed certificates.

If users try to connect to the Server via a domain name, the domain name should be added as a custom server.

**Basic**

No certificate validation is performed when connecting to a server. The system connects directly without displaying warning messages. However, disabling validation is not recommended, as certificate validation is an essential part of system security hardening.

Before the first time login, a warning message will pop up for installing root certificate.

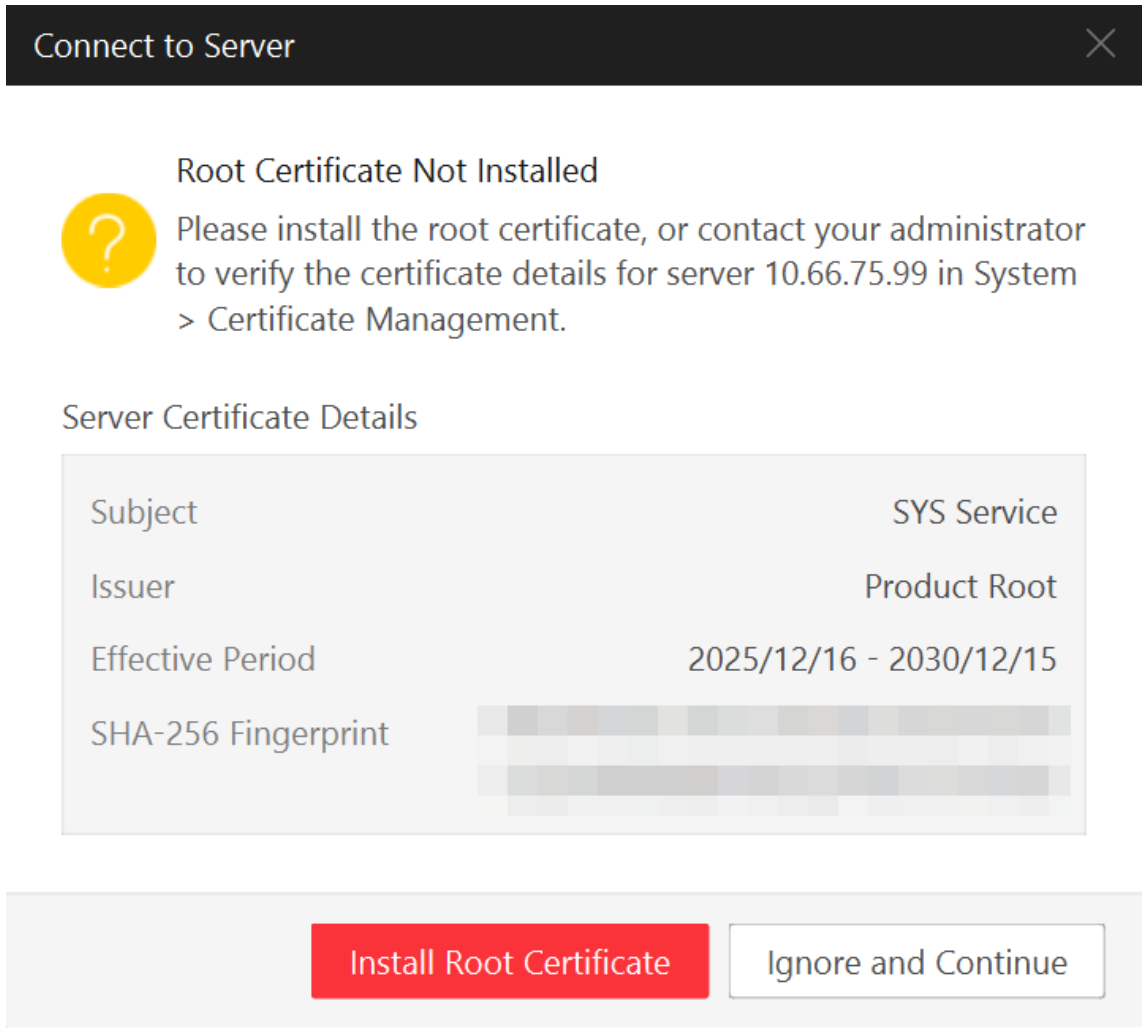



**Figure 8-6 Install Root Certificate**

### Step 1 Get Your SSL/TLS Certificate

As a digital certificate issued by the Certificate Authority (CA), the SSL/TLS certificate secures all types of information transferred to and from the server and proves the identity of the server owner. Compared with the platform provided certificate, the SSL/TLS certificate has a higher security level.

**Note**

The SSL/TLS certificate is purchased from a certificate authority.

1. Choose a CA that you trust.
2. Generate a certificate signing request (CSR) and a private key.
   There are multiple methods to generate a CSR and a private key: via Microsoft IIS, OpenSSL, or a trusted website.
3. Send the generated CSR to the CA to get the authorized SSL/TLS certificate.

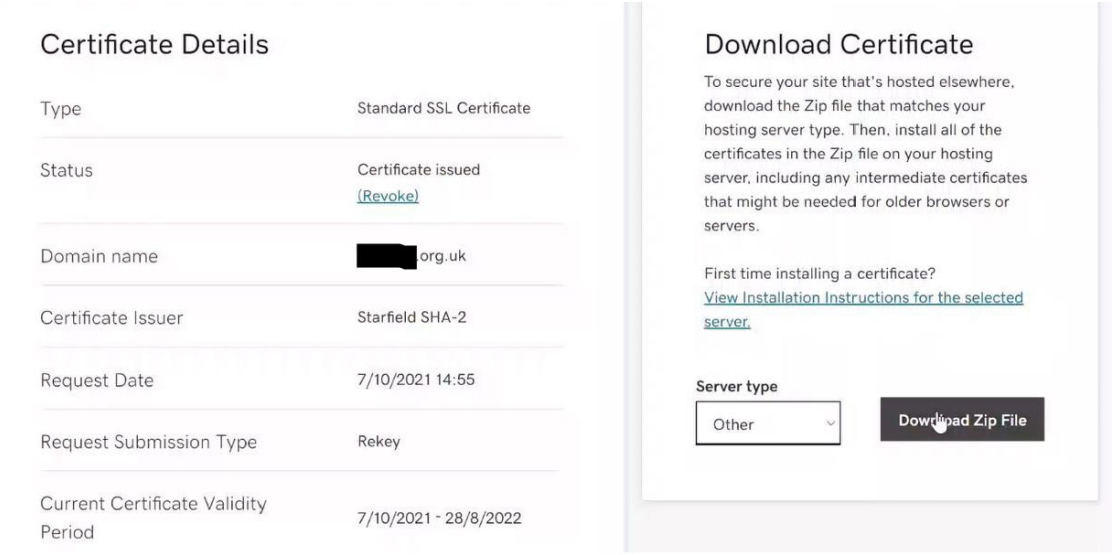



**Figure 8-7 SSL/TLS Certificate Example**

4. Download your SSL/TLS certificate to your local PC.
   Make sure that the certificate is in PEM format. You can try to edit the file extension to ***.pem*** or use a tool to convert its format to PEM.

## Step 2 Upload Your SSL/TLS Certificate to the System

1. Check your SSL/TLS certificate.
   Generally, the issued SSL/TLS certificate contains the certificate file in PEM format, certificate chain in PEM format, and certificate file in other formats (such as CRT and PLCS-7).
2. Get the certificate file in PEM format, the private key which is generated together with the CSR, and the certificate chain in PEM format. And concatenate them into one PEM file in order.
   You can use the CertTool provided by Hikvision to concatenate a certificate. (Tool download address: ***https://www.hikvision.com/en/support/download/software/hikcentral-professional-v2-6-0/*** .)

**Note**

- The PEM file encoding method should be UTF-8.
- The order of contents in the PEM file should be certificate file -> private key -> certificate chain.



```
-----BEGIN CERTIFICATE-----
MIIGbzCCBVegAwIBAgIMUIt4TGOLEB4xyfNBMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
tAqm/TgWlV8dwim1wc6t525+Hrl3lOnHA3FF78cwWMl5x5dNKhwf632dxMQz4IpB
8XMkRHge9AIdnlVMp2HUB7iOZW3K4Cv9O/YCwuHsnnFCibwWpXZUY2KSi521RxBJ
0/gC3Cr/WyI5fRzHqnrxnHmEqQ==
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApG3HSjP4zoyFCii+Ct2f7501VmzdnYdxEVqBdQtMie27pJk6
G4e5YQKBgCE/n8nqGm9spvRz6GW59tboV8eByZePkyn+8ydv4VeSgL9q5uTbHKTQ
N9VTTuYxmAyUQ46EDWKhAU5445uEUFSbY6X+77zPEvuNpqUSdsEsOjm9s4XmpibK
ptsahzxpzPKCKa1nN2nnGpvJ60ailfEMYzP5zMNiEQPbtEZ734yR
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIHAjCCBOqgAwIBAgIQBeEL6xHDBPMqVc/6KaEe1jANBgkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzErMCkGA1UEChMiVml0YWx3ZXJrcyBJbnRlcm5ldCBTb2x1
0y3ryvnRPxtYleAljYaHoa08klpIbWlOUZHL5T4DTFj6ko0J15MjGSTOanrvme52
oVOgwRlGPAUBRQyqbNA/N5PgYvnbYnP+3zLjV2fcsTQd9Ryk7ulSbK5ZTjds3PCC
Z/aCk1NiNYigUKZmFSniwaFMpojLdiBmKZjgepFJxMTiITr8ZqBG+lkJSZB88POf
AAyK5ka+CpCndiSV/gQnsMagCmeyhw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF4DCCBMigAwIBAgIQAtzIUa9xYrr53z9V1ROxXjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
FrgGtfX1rKPst8yZpX6jBLHy5eUUGJmG3VCGWRDrri1lWSajBC6RffzR7vzb0/wB
QOXi74AB8YHtYlzmjGGA7IY5Mjdur4CgcUWPlopqn4lgPvzRdRDvD01g3rvpF/ma
ySyHlhO/+GHWldxQRb0QdhxyF4g=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
-----END CERTIFICATE-----
```

**Figure 8-8 Example of Concatenated Certificate**

3. In the left of the System module, click **Security → Transport Protocol** .
4. Select the **Transfer Protocol Between Platform and Browser** as **HTTPS**.
5. Select **High** as the Certificate Security Level.
6. In the Upload Certificate area, click  to upload the concatenated certificate.
7. (Optional) In the Upper-Level Certificate section, you can click **Add** to upload the certificate chain to the server.
   The invalid or incomplete certificate chain of operating system will result in SSL/TLS certificate verification failure. In this case, users can download the certificate chain, convert it to CRT format, and double-click to install it on their PCs.

**Note**

- The SYS will restart automatically after the transport protocol is changed.
- All logged-in users will be forced to log out during the restarting, which takes about one minute and after that, the users can log in again.

## 8.6.2 Generate and Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the platform, you should generate the service component certificate stored in SYS and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in SYS and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and SYS are the same.

**Steps**

1. Select **Service Component Certificate** on the left navigation bar.
2. Click **Generate Again** below **Certificate between Services in System**, and enter the password for double authentication to generate the security certificate for Streaming Server verification.

   **Note**

   On the Service Manager of the Streaming Server you want to add, input the certificate information you generate.
3. Click **Export** to export the service component certificate in XML format and save it to the local PC.

   **Note**

   On the Cloud Storage Server you want to add, import the service component certificate you export.

## 8.6.3 Enable Export of Profile Pictures

In the Person module, you can export the profile pictures of the added persons as a ZIP file to your PC . For information security, you can choose to convert these profile pictures into unreadable modeling data for saving.

On the left navigation bar, select **Profile Picture** and check **Export Profile Pictures**.

Switch on **Save Model Data of Profile Picture Only** and select a validity period for the profile pictures.

### 8.6.4 Enable Auto Update

You can enable auto update to allow the clients to be updated automatically if there is a new version available.

Select **Auto Update** on the left navigation bar, check **Client Auto Update**, and click **Save**.

### 8.6.5 Set Database Password

You can set the database password of the platform on the Web Client running on SYS.

**Note**

Setting database password is only available when you access the Web Client on SYS locally.

Select **Database Password** on the left navigation bar.

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

### 8.6.6 Watermark Settings

On the left navigation bar, click **Watermark Settings**. and then enable **Watermark**.

1. Configure the display content, text style, transparency, rotation angle, and size.
2. click **Background Settings** to set the watermark's background
3. click **Save**.

## 8.7 Advanced Settings

The advanced settings menu provides entries of setting system hot spare, generating or debugging logs, downloading the event tracking information, and resetting the network information for devices.

On the left navigation bar of the System page, select **Advanced** to display the advanced settings menu.

### 8.7.1 Configure System Hot Spare

A hot spare is used as a failover mechanism to provide reliability for your system. If you build the hot spare system when installing SYS, you can enable the hot spare function and configure the hot spare property of the current SYS as host server or spare server. When the host server fails, the spare server takes over, thus ensuring the stability of the system.

**Steps**

1. Select **Hot Spare** on the left navigation bar.
2. Switch on **Hot Spare**.
3. Select a **Configuration Mode**.
4. Enter or set related parameters

   **Remote Hot Spare**

   **Virtual IP Address**

   A fixed IP for external use. The server taking over will automatically use this IP address without requiring users to change the access address, ensuring uninterrupted service.

   **Production Center**

   If you enable **Deploy 2 Servers**, the IP address of both Host Server and Spare Server should be entered.

   **Disaster Recovery Center**

   When 2 servers in the Product Center fail, the server in the Disaster Recovery Center will take over.

   **Streaming Server**

   Add streaming servers here to show the streaming server cluster.
5. Click **Save**.

## 8.7.2 Diagnosis and Maintenance

For the operation and maintenance personnel, they can generate and download logs of a specified time period for locating issues, debug logs, and view or download the event tracking information.

Select **Diagnosis & Maintenance** on the left navigation bar.

### Generate Logs

1. Check the service log type(s).
2. Specify the start and end time of the time period in which the logs are to be generated.
3. Click **Generate** to start generating a log file.
   When completes, a zip file name will appear at the bottom of the Maintenance Data section and you can click to download the log file to the local PC.

### Debug Logs

1. Click **Download Template** to download the template of log configuration file to the local PC.
2. Fill in the template with required information locally.
3. Click to upload the configured template to the platform and click **Start Debugging**.
   A 24-hour countdown will automatically start.

**Note**

When the countdown finishes, the on-going debugging will be canceled automatically. You can click **Extend Debugging** to extend the debugging duration.

4. (Optional) Click **Close Debugging** to stop the debugging.

### View and Download Event Tracking Information

Click **Event Tracking Information** in the top right corner of the Diagnosis and Maintenance page to open the Event Tracking Information page.
On the Event Tracking Information page, you can view the exception and general information and click **Download Event Tracking Information** in the top right corner to download the event tracking information to the local PC. You can also click **Refresh** to refresh the event tracking information.

## 8.7.3 Reset Device Network Information

When the system network domain changes (such as server migration), you must reset the network information for the added device to adapt to the new network environment. Otherwise, some functions of the device will be affected.

**Steps**

1. Select **Reset Network Information** on the left navigation bar.
2. Click **Reset** to one-touch reset the device network information.

# 8.8 Manage Workbenches

The platform provides three default preset workbenches for administrator, time and attendance, and visitor management which can only be edited. You can also add new workbenches and manage all of them.

Select **Workbench Management** on the left navigation bar.

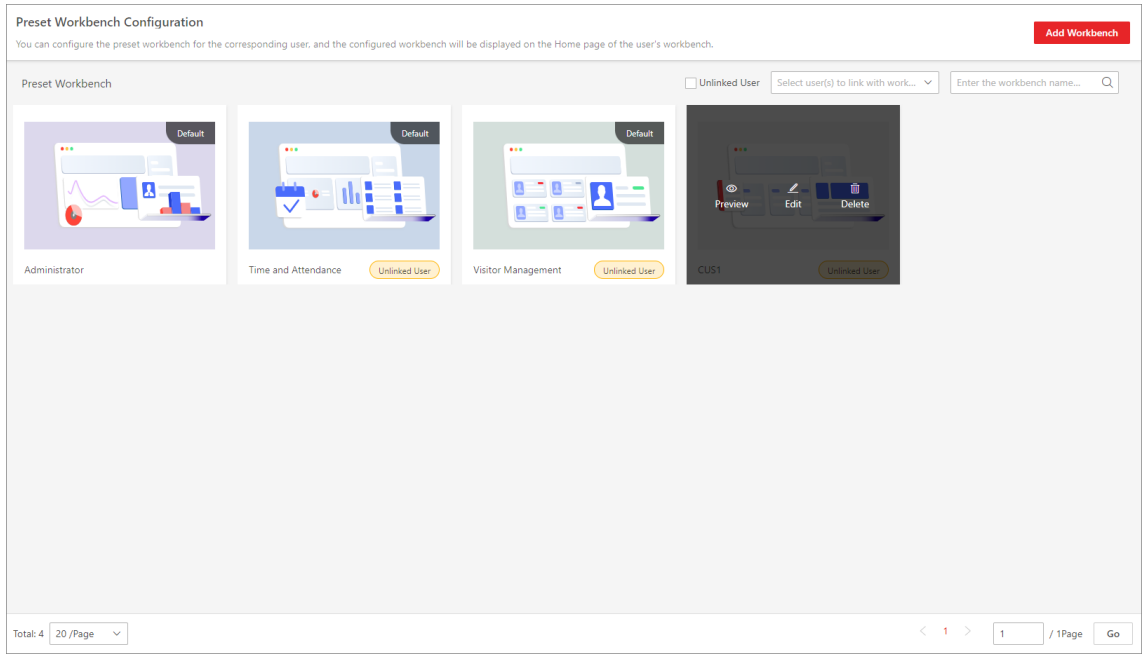



**Figure 8-9 Preset Workbench Configuration Page**

On the Preset Workbench Configuration page, you can perform the following operations.

- Click **Add Workbench** in the top right corner to create a workbench.
- Move the cursor on a workbench card and click **Preview** to view the workbench. On the Preview page, you can click **Copy and Add** in the top right corner to copy the settings to a new workbench.
- Move the cursor on a workbench card and click **Edit** to edit the configuration.
- Move the cursor on a workbench card and click **Delete** to delete the workbench.
- Check **Unlinked User** to display workbenches that are not linked with users.
- Select the linked user(s) to filter workbenches by user or enter a keyword to search for workbenches by name.

## 8.9 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

Select **Company Information** on the left navigation bar.

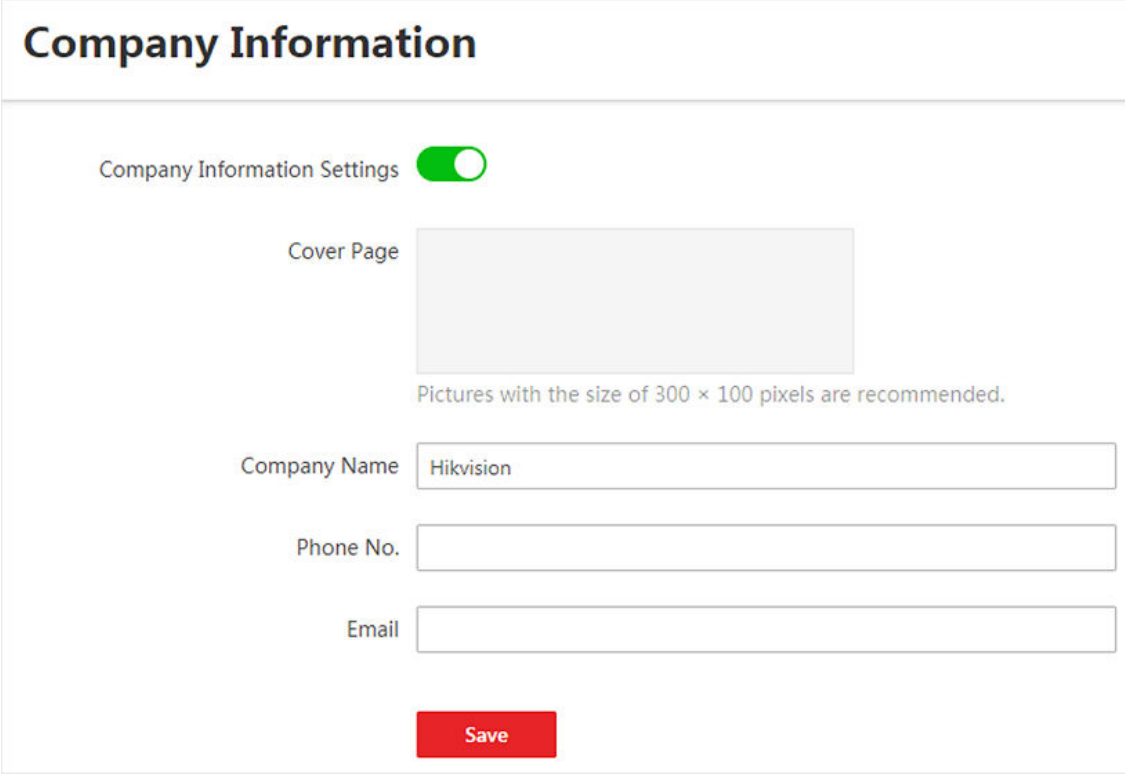



**Figure 8-10 Company Information Settings**

Switch on **Company Information Settings** to enable displaying company information on the Web Client. Then set the information (cover page, company name, etc.) as needed and click **Save**.

An icon appears at right of the Web Client and keeps displaying. You can click the icon to view the company information.

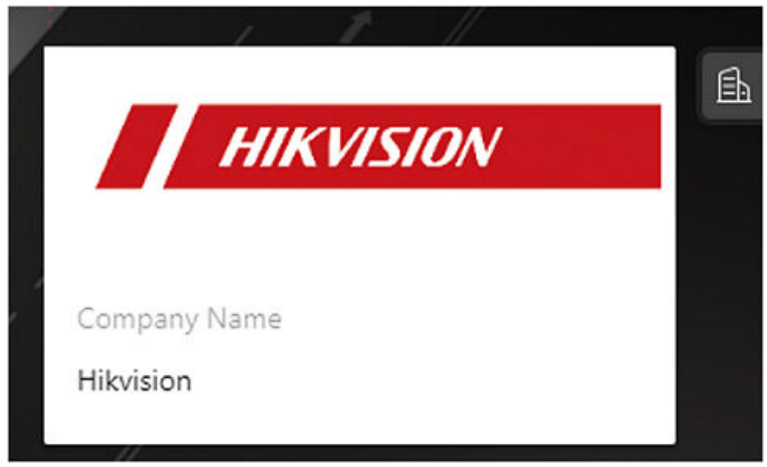



**Figure 8-11 Company Information Displayed on Web Client**

# Chapter 9 Maintenance

The system provides Service Manager to manage the installed services on the SYS server. You can check the service's running status, edit the service port, start/stop service via the Service Manager.

The system also provides backup of the database, so that your data can be well protected and recovered when an exception occurs.

You can also export the system's configuration data and save it to the local PC.

In the top left corner of Home page, select → **All Modules** → **Maintenance** .

## 9.1 Health Overview

Health Overview provides both near-real-time and history information about the status of the SYS and added resources. It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a resource exception occurs, you can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.

### 9.1.1 Real-Time Health Status Overview

In the Health Overview module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there is no network transmission devices added, the Real-Time Overview page provides an at-a-glance view of the health status with charts and basic data of resource status.

Select **Real-Time Overview** on the left.

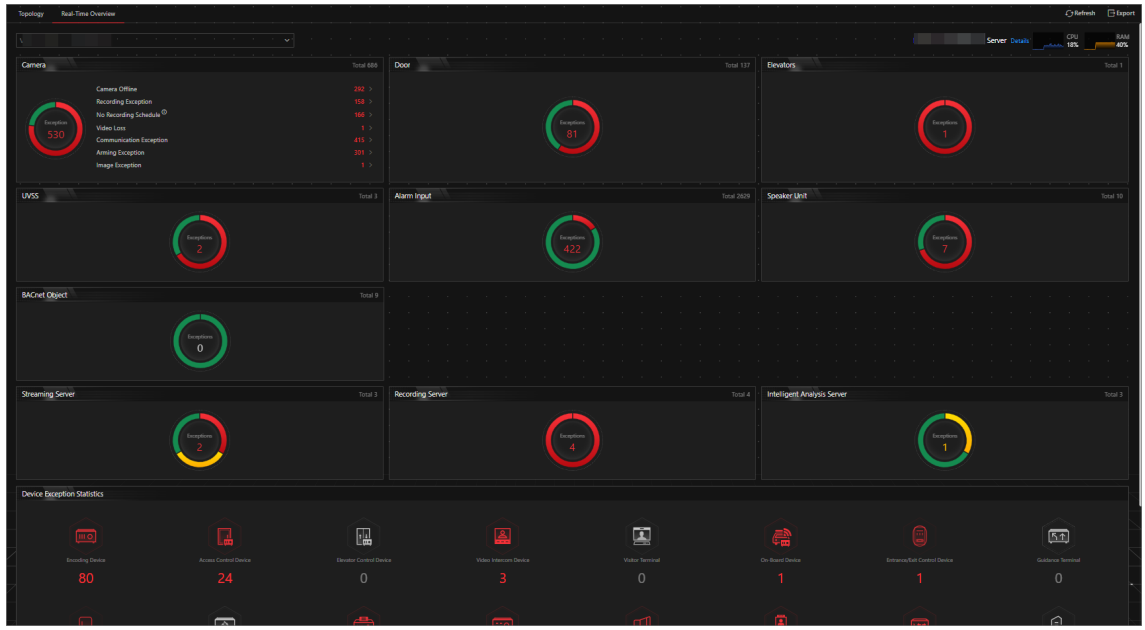
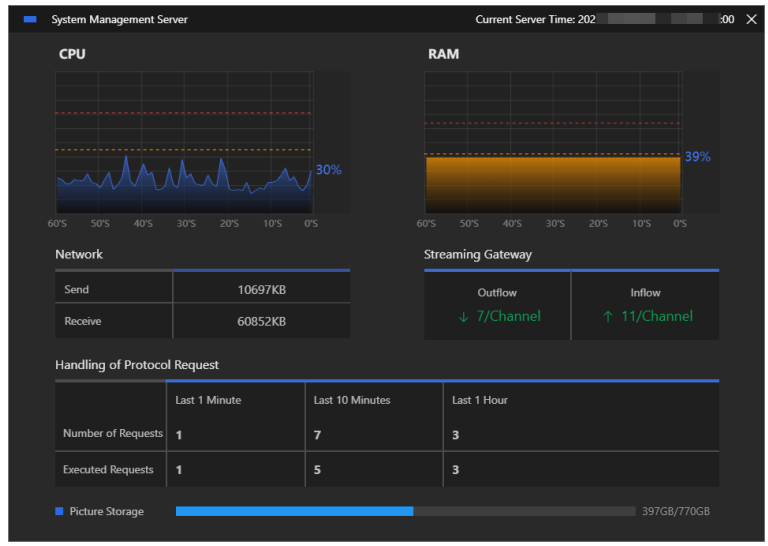
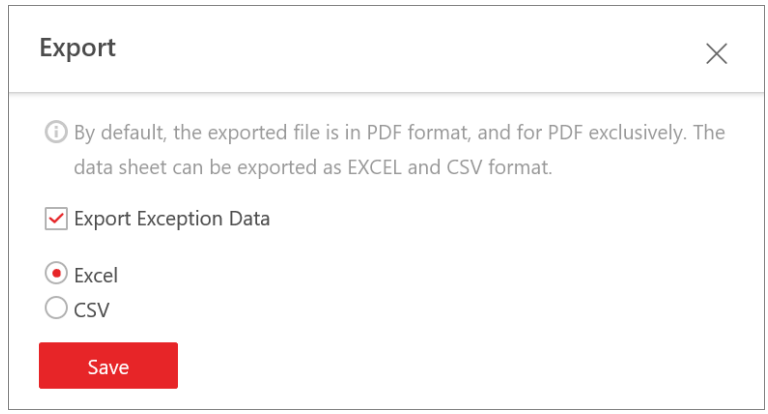



**Figure 9-1 Real-Time Health Status Overview**

**Table 9-1 Real-Time Health Status Page**

| Section | Description |
|---|---|
| Display Resource Status by Site | Select a site from the drop-down list in the upper left corner to display the status of resources on the selected site.<br>If an exception occurs on a site, the icon will appear beside the site name and you can move the cursor over it to view the exception details. |
| System Management Server Status | View the CPU and RAM usages of the site server in the top right corner of the overview page.<br>Click **Details** to open the System Management Server window to view the detailed status, including the current server time, CPU usage, RAM usage, network status, streaming gateway status, handling status of protocol request, and picture storage. |

| Section | Description |
|---|---|
| |  <br>**Figure 9-2 Status Details of System Management Server** |
| Resource Status | View the abnormal data of different resources added to the platform in the graphical way. You can move the cursor over the chart to display the exception types and the corresponding numbers of abnormal devices, and then click a type or the number on the chart to view the real-time status details of resources. |
| Device Exception Statistics | View the number of abnormal devices with different types added on the platform. You can click a number under the device picture to view the real-time status details of the device.<br>If the icon  appears at the top of device picture, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** . |
| Refresh Overview Page | • Manually Refresh: Click **Refresh** in the upper right corner of Real-Time Overview page to manually refresh the resource status on the page.<br>• Auto Refresh: Go to **Maintenance → Basic Configuration → Auto-Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Auto-Check Frequency*** . |
| Export Overview Page or Exception Data | Click **Export** in the upper right corner of Real-Time Overview page to export the page in PDF format. Or you can check **Export** |

| Section | Description |
| --- | --- |
| | **Exception Data** to export the exception data in Excel/CSV format.<br>  <br>**Figure 9-3 Export Overview Page or Exception Data** |

## 9.1.2 Real-Time Health Status Overview (Topology)

In the Health Overview module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there are network transmission devices managed on the platform, the Real-Time Overview page provides a topology of the managed devices. Topology is a figure that displays the connection relations among network transmission devices, security devices, etc. It is mainly used for network maintenance.

**Note**

- Make sure the network transmission devices have been added to the platform.
- If a network transmission device can not be recognized by the platform, it will be displayed as an unknown device.
- The topology does not support body cameras, but supports ticket dispensers.

In the Health Overview area, select **Real-Time Overview** on the left.

Click **Topology** at the top to enter the Topology page.

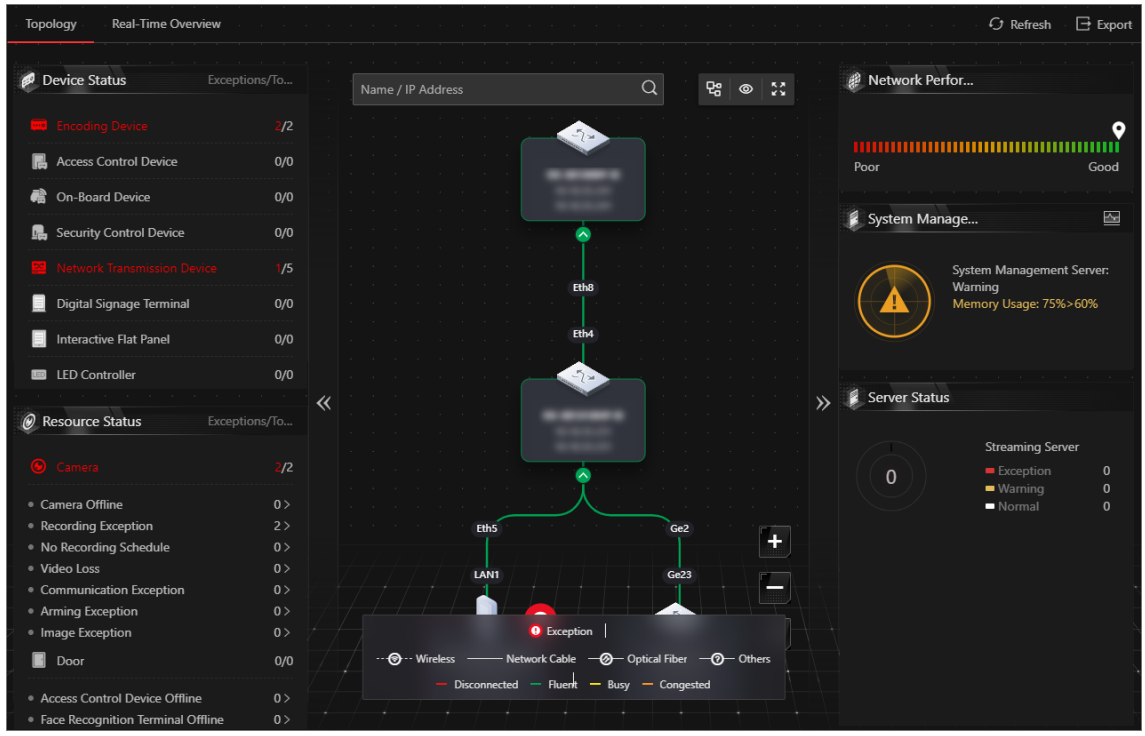
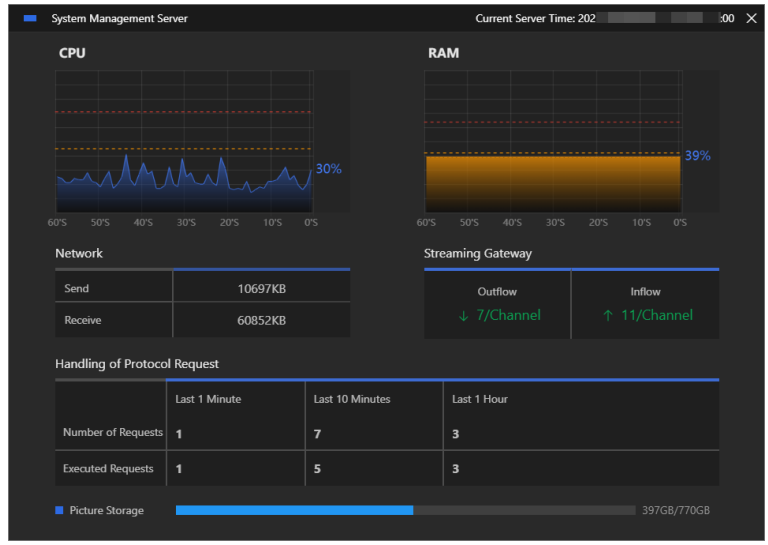
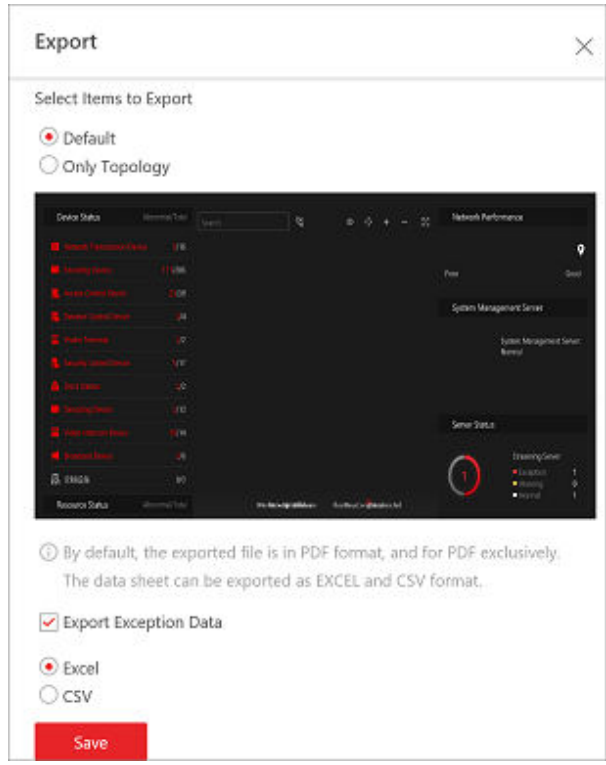



**Figure 9-4 Topology Overview**

**Table 9-2 Topology Page**

| Section | Description |
|---|---|
| Device Status | View the abnormal data of different devices added to the platform. You can click the number to locate the abnormal device in the topology or view the devices' real-time status.<br>If the icon appears beside the device type name, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** . |
| Resource Status | View the abnormal data of different resources added to the platform. You can click a number to view the real-time status details of resources. |
| Topology Details | View the relationships among devices, device information, link status, alarm information, etc. See details in ***Topology Details*** . |
| Network Performance | View the current network performance (poor or good) of the System Management Server. |
| System Management Server Status | Click in the upper right corner of the System Management Server section to view the detailed status, including the current |

| Section | Description |
|---|---|
| | server time, CPU usage, RAM usage, network status, streaming gateway status, handling status of protocol request, and picture storage.<br>  <br><br>**Figure 9-5 Status Details of System Management Server** |
| Server Status | View the status (i.e., exception, warning, normal) of servers added on the platform. |
| Generate Topology Again | Click **Refresh → Generate Topology Again** to draw the network topology again. |
| Refresh | • Manual Refresh: Click **Refresh** in the upper right corner to manually refresh the resource status on the page.<br>• Auto Refresh: Go to **Maintenance → Basic Settings → Health Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Auto-Check Frequency*** . |
| Export Topology or Exception Data | Click **Export** in the upper right corner and select the export type as **Default** (all the displayed information including topology and exception data on the Real-Time Overview page will be exported) or **Only Topology** to export the selected content in the needed format. |

| Section | Description |
| --- | --- |
| |  <br>**Figure 9-6 Export Topology** |

## Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

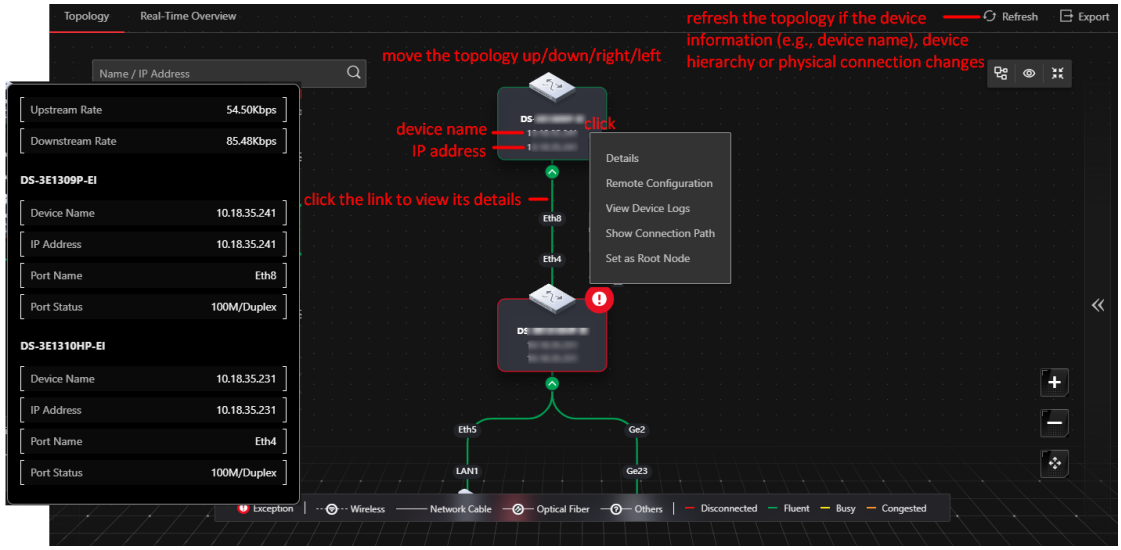



**Figure 9-7 Topology Details**

**Details**

View device details including the basic information (i.e., device name, IP address and device model), device usage (e.g., RAM usage, CPU usage, PoE power), arming status and disk array (for encoding device), live video (if the device is linked with a camera), linked lane name / entrance direction / entrance & exit name / barrier control status (if the entrance and exit is linked with a camera), device panel status (i.e., ports and ports usage), and port information (i.e., port name, and peer device type, peer device IP address, and peer device name).

The device details vary with different device models.

**Remote Configuration**

Configure device parameters including system settings, network and port configuration. You can configure the network parameters and device port according to the network usage. For details, refer to the user manual of the device.

This function should be supported by the device.

**View Device Logs**

When a device failure happens or trouble shooting is required, you can view the device's logs to know the alarms, notifications, operations and events of the device. And you can set the conditions to search the device logs.

This function should be supported by the device.

**View Connection Path**

If there is a data transmission failure between the devices, you can view the connection path to judge which link is disconnected and restore the link quickly. According to the information presented in the prompt window, click **Common Unknown Node** or **Select Node** to select the peer node, and then click **OK**. After that, the connection path between the two nodes will be displayed.

**Set as Root Node**

Set the current device node as the root node and adjust the topology structure.

## 9.1.3 Historical Health Data Overview

You can view the historical online rate of resources and devices, or the recording integrity rate.

On the Health Overview area, select **History Overview** on the left.

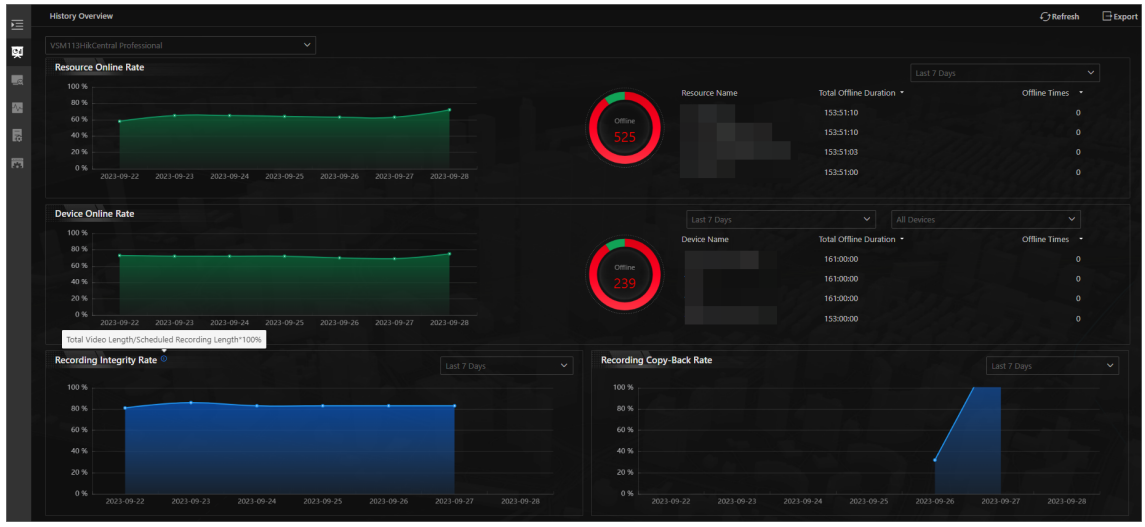
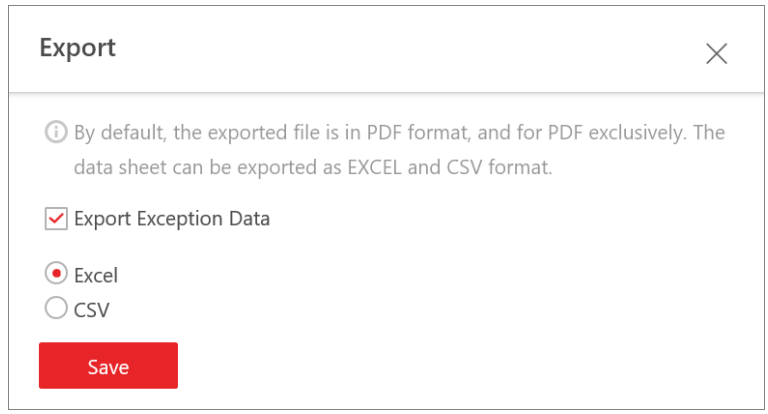



**Figure 9-8 Historical Health Data Overview**

**Table 9-3 Historical Health Data Page**

| Section | Description |
|---|---|
| Select Site | In the upper left corner of History Overview page, select a Current or Remote Site from the drop-down list to display the historical data of resources on the Site. |
| Filter Data | Select a time period from the drop-down list in the upper right corner of each section for filtering data by day, week, or month. |
| Resource Online Rate | • On the line chart, you can perform the following operations: |

| Section | Description |
| --- | --- |
| | ◦ Move the cursor on the line chart to view the camera online rate and the number of offline cameras at specific time points.<br>◦ Click the a dot on the line to go to Resource Log page to view the detailed network status of cameras at that time point.<br>• On the doughnut chart, you can perform the following operations:<br>◦ Move the cursor to red part of the doughnut chart to view the number of the cameras which once were offline and the offline rate during the time period you select.<br>◦ Move the cursor to the green part of the doughnut chart to view the number of the cameras which stay online and the online rate during the time period you select.<br>• On the table, you can do one of the followings:<br>◦ Click **Total Offline Duration** to rank the cameras in terms of total offline duration within the time period you select.<br>◦ Click **Offline Times** to rank the cameras in terms of offline times within the time period you select. |
| Device Online Rate | • On the line chart, you can do one of the followings.<br>◦ Move the cursor on the line chart to view the device online rate and the number of offline devices at specific time points.<br>◦ Click the a dot on the line to go to Device Log page to view the detailed network status of devices at that time point.<br>• On the doughnut chart, you can perform the following operations.<br>◦ Move the cursor to red part of the doughnut chart to view the number of the devices which once were offline and the offline rate during the time period you select.<br>◦ Move the cursor to the green part of the doughnut chart to view the number of the devices which stay online and the online rate during the time period you select.<br>• On the table, you can do one of the followings.<br>◦ Click **Total Offline Duration** to rank the devices in terms of total offline duration within the time period you select.<br>◦ Click **Offline Times** to rank the devices in terms of offline times within the time period you select. |

| Section | Description |
| --- | --- |
| Recording Integrity Rate | To get the recording integrity rate, divide the total video length by the scheduled recording length, and then multiply the result by 100%. On the line chart, you can move the cursor to view the recording integrity rate at specific time points. Click the a dot on the line to go to Resource Log page to view the detailed resource status of devices at that time point. |
| Recording Copy-Back Rate | On the line chart, you can move the cursor to view the recording callback rate at specific time points. Click a dot on the line to go to Resource Log page to view the detailed resource status of devices at that time point. |
| Refresh | • Manually Refresh: Click **Refresh** in the upper right corner of History Overview page to manually refresh the data on the page.<br>• Auto Refresh: Go to **Maintenance → Basic Configuration → Health Check Frequency** to set the interval for automatically refreshing the data on the page. See details in ***Set Auto-Check Frequency*** . |
| Export Overview Page or Exception Data | Click **Export** in the upper right corner of History Overview page to export the page in PDF format. Or you can check **Export Exception Data** to export the exception data in Excel/CSV format.<br>  <br>**Figure 9-9 Export Overview Page or Exception Data** |

## 9.2 Set Basic Maintenance Parameters

You can set parameters to regularly send device and resource log reports to specified users via email, set the warning threshold for SYS usage, configure the default response timeout of the interactions among the Web Client, SYS, and devices, specify the health check frequency, and set the hierarchy and bandwidth threshold for the topology.

### 9.2.1 Configure Scheduled Health Check

You can configure scheduled health check to proactively detect and address potential problems and maintain the stability and reliability of your devices, services, and systems.

**Before You Start**

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

**Steps**

1. Select **Basic Configuration → Scheduled Health Check** on the left.
2. Switch on **Scheduled Health Check**.
3. Select **Health Check Item**.

   **Device Health Check**

   The device check items include the password, recording exception, HDD temperature, and resolution mismatch.

   **System Health Check**

   The system check items include the disk space, device inspection frequency, and storage server CPU temperature.

   **Service Health Check**

   The service check items include the operation timeout and video loss.
4. Set the health check period.

   **Note**

   You can schedule health checks on a daily, weekly or monthly basis. For an automatic health check on the last day of each month, set the health check period to By Month and the health check time to Last Day. Avoid setting the health check time to 31 for months with fewer than 31 days.
5. Configure the advanced settings. This part will introduce key parameters.

   **Auto Import Results to Pending Task**

If you switch on **Auto Import Results to Pending Task** and check off **Replace Duplicated Pending**, the new pending task will automatically replace the old one when both the checked items and the objects of the pending tasks are the same.

**Auto Export Results as Report**

Switch on to send or save the health check reports.

**Send Report via Email**

If you have switched on **Send Report via Email**, select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

**Upload to SFTP**

To ensures secure, reliable, and efficient file transfer, upload the report to SFTP.

**Note**

You can click **Configure** to set the SFTP.

6. Click **Save**.

## 9.2.2 Send Log Report Regularly

You can send server, device, resource, and maintenance log reports to specific users regularly via email. Server log reports contain error logs, warning logs, or information logs of the user, system management server, and person. Device log reports contain information on the online/offline status of devices. Resource log reports contain the online/offline status of resources as well as the recording status. Maintenance log reports contain information on maintenance activities and tasks.

**Before You Start**

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

**Steps**

1. On the left, select **Basic Configuration → Scheduled Report** .
2. Click + to create a new report.
3. Enter the basic information of the report including report name, type and language.
4. Set report content.

**Note**

Skip this step if you select the report type as **Maintenance Log**.

5. Set report time.

**Statistical Cycle**

Set the frequency of generating the report.

**By Day**

The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

**By Week/Month**

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

**Report Time**

Set the time period during which the logs will be recorded.

6. Set advanced parameters.

**Send via Email**

If you have switched on **Send via Email**, Select an email template to define the recipient information and content. You can click **Add** to add a new email template. For details, refer to ***Email Settings*** .

**Upload to SFTP**

Switch on to upload the report to SFTP.

**Note**

You can click **Configure** to set the SFTP.

7. Click **Save**.

### 9.2.3 Set Warning Threshold for Streaming Media Usage

An alarm can be triggered if the Streaming Media's CPU usage and RAM usage reaches a predefined warning threshold and lasts for a predefined duration, or if the channel usage of Streaming Media reaches a predefined warning threshold. The related threshold value can be checked via the Control Client.

On the left, select **Basic Configuration → Server Usage Thresholds** .

### CPU/RAM Usage

Drag ⌂ to adjust the threshold value of CPU or RAM usage, and then define the duration in the **Notify if Value Exceeds for (s)** field.

**Example**

- If you set the Warning threshold value to 60%, and set 20 in the **Notify if Value Exceeds for (s)** field for the CPU usage, you can view the CPU usage reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the CPU usage reaches 60% and lasts for 20 seconds.
- If you set the Warning threshold value to 60%, set 20 in the **Notify if Value Exceeds for (s)** field for the CPU Usage, and set an alarm for CPU Warning (see ***Add Normal Event and Alarm*** ), the alarm will be triggered when the CPU usage reaches 60% and lasts for 20 seconds.

### Database Usage

Drag ⌂ to adjust the threshold value of RAM usage or network I/O usage of database.

### Streaming Server Usage

Drag ⌂ to adjust the threshold value of bandwidth usage (in and out). When the bandwidth usage (in or out) reaches a certain threshold value, the corresponding status (normal, warning, or abnormal) will be displayed in the list on the streaming server status page.

### Streaming Channels of Streaming Media

Enter a specific value in the text field or click ∧ / ∨ to adjust the threshold value for the number of input or output channels of Streaming Media.

**Example**

If you set the Warning threshold value to 160 for the number of input channels of Streaming Media, you can view the number of used input channels reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the number of used input channels reaches 160.

## 9.2.4 Set Network Timeout

Network timeout is a certain amount of time which is used to define whether the interaction among the Web Client, SYS, and devices is successful or not. To be specific, if one party fails to response after the configured timeout passes, the interaction between them is regarded as a failure.

On the left, select **Basic Settings → Network Timeout** .

Select the network timeout and click **Save**.

**Table 9-4 Minimum Response Timeout in Different Interactions**

| Interaction Relation | Minimum Response Timeout |
|---|---|
| Between Web Client and SYS | 60 s |
| Between SYS and Device | 5 s |
| Between Web Client and Device | 60 s |

**Note**

This parameter affects all Web Clients accessing the current SYS.

### 9.2.5 Set Auto-Check Frequency

The SYS will check the health of devices, resources, and servers managed on the platform. The platform will display the health check results in the Real-Time Overview module. You can set the frequency which controls how often the platform gets the latest status of the devices, servers, and resources.

On the left, select **Basic Settings → Auto-Check Frequency** .

#### Device Health Status

You can set the health check frequency for different devices managed on the platform. It controls how often the platform pings these devices to determine whether they are online.
After disabled, the platform will not update the status of the managed devices. You need to refresh manually to get the latest status.

**Note**

You should adjust the check frequency according to the number of devices. The greater the number of devices, the lower the frequency of health checks. When the frequency set is too high, you will be prompted and recommended to set a lower frequency.

#### Server Health Status

You can set the health check frequency for the managed recording servers and DeepinMind servers. It controls how often the platform pings these servers to determine whether they are online.
After disabled, the platform will not update the status of the managed servers. You need to refresh manually to get the latest status.

#### Others

- **Device Capabilities:** Set how often the platform gets the managed devices' capabilities. After disabled, the platform will not update the capability changes of all the managed devices. You need to refresh manually to get the latest capabilities.
- **Recording Status:** Set how often the platform checks the camera's recording status. After disabled, the platform will not update the cameras' recording status.
- **Alarm/Event Enabled or Not:** Set how often the platform checks whether the event and alarm rules are enabled or not. After disabled, the platform will not update the configured event and alarm rule status.
- **Remote Alarm Enabled or Not:** Set how often the platform checks whether the event and alarm rules configured on the Remote Sites are enabled or not. After disabled, the platform will not update the configured alarm rule status configured on the Remote Sites.

### 9.2.6 Set Topology Show Parameters

You can set show parameters for the topology.

**Note**

For details about health monitoring, see ***Health Overview*** .

On the left, select **Basic Configuration → Topology Show**

**Bandwidth Threshold**

When the bandwidth usage exceeds the threshold, the link on the topology will turns to the corresponding color.

## 9.3 Health Check

To control the health status of resources on the platform, you can perform manual health check to quickly scan the platform for potential risks by different check types, whose check items can be configured. For issues found during the health check, you can add them as pending tasks for further handling. You can also customize pending tasks according to the actual need.

On the Maintenance module, select **Health Check** on the left.

### 9.3.1 Perform Manual Check

You can manually start health check to quickly scan the platform for potential risks and configure check items for different check types.

Select **Manual Check** on the left.

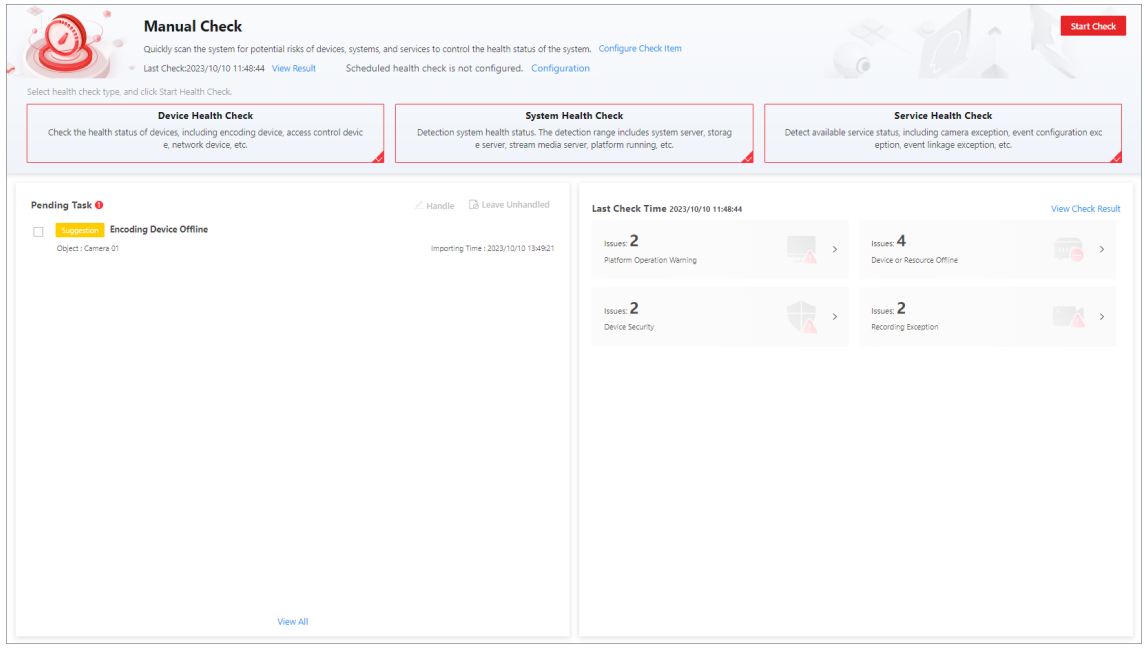



**Figure 9-10 Manual Check Page**

On this page, you can perform the following operations.

- ***Start Health Check Manually***
- ***Configure Check Items***
- ***Manage Pending Tasks***
- ***View Last Check Results***

## Start Health Check Manually

Click **Device Health Check**, **System Health Check**, or **Service Health Check** at the top of the Health Check page to select the type(s) to be checked, and then click **Start Health Check** in the top right corner to enter the Checking page.

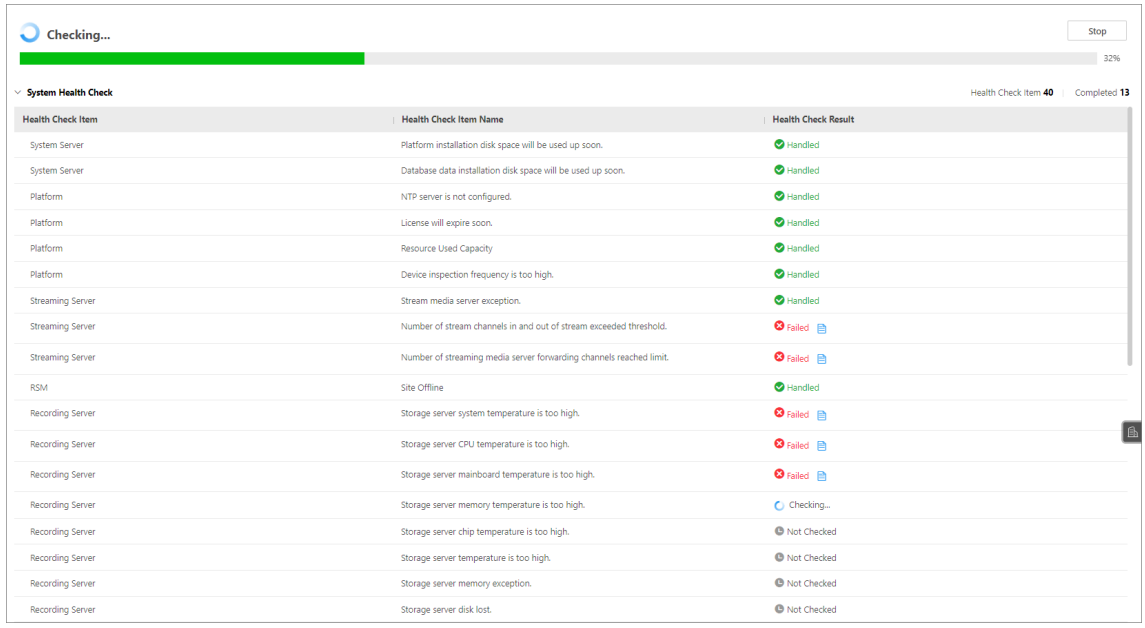



**Figure 9-11 Checking Page**

During the health check, you can view the progress percentage, real-time check items, and result. For failed items, you can click in the Health Check Result column to view the failure details. You can also click **Stop** in the top right corner to cancel the health check.

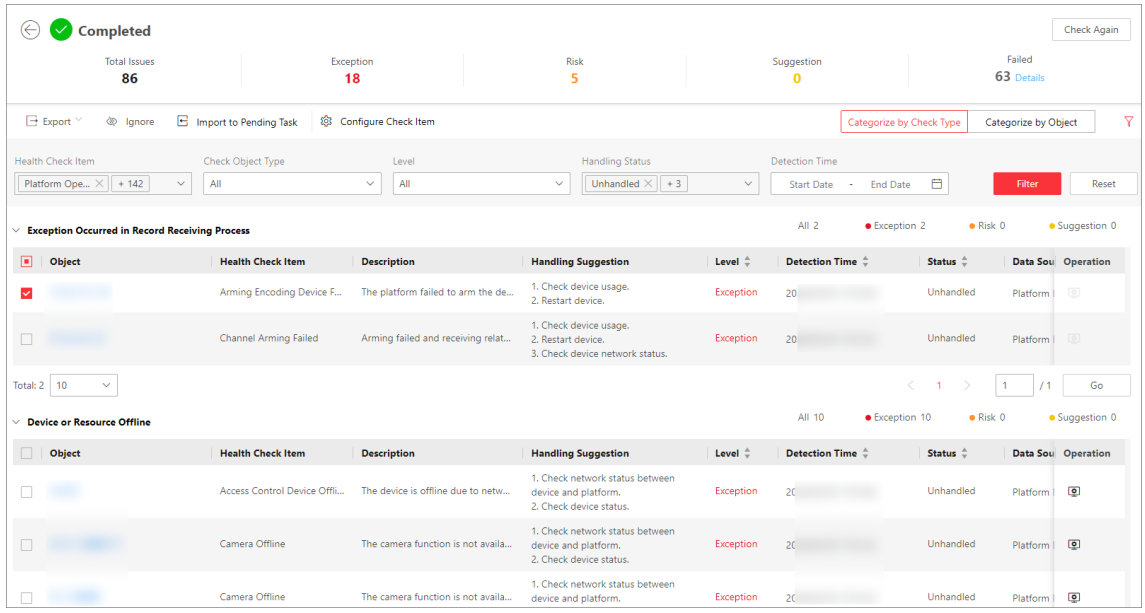



**Figure 9-12 Completed Page**

When the health check completes, you can perform the following operations.

- View the total numbers of issues, exceptions, risks, suggestions, and failed items, or click **Details** besides the number of failed items to view the failed item details.
- Click **Configure Check Item** to view the health check item list and ignored check items. For more operations on the Health Check Item List page, refer to ***Configure Check Items*** .
- Click **Categorize by Check Type** or **Categorize by Object** at the top of the issue list to display and calculate issues by health check type or object. You can click > in front of a category name to unfold the category to view more details.
- Click ▽ in the top right of the issue list to open the filter pane and set conditions to filter the issues.
- Move the cursor over the **Export** button and click **Export All** to export all issues to the local PC.
- Check the issue(s) in the list and click **Export** at the top of the issue list to export the selected issue(s) to the local PC.
- Check the issue(s) in the list and click **Import to Pending Task** to move the selected issue(s) to the pending task for further management. Refer to ***Manage Pending Tasks*** for details.
- Click the object name to view the device details and information, and click ⚙ to go to the device configuration page.
- Check the issue(s) in the list and click **Ignore** to ignore the selected issues.
- Click **Check Again** to start the health check again.

**Note**

If you want to start health check regularly, you can click **Configure** on the top of the Manual Check page to enable the scheduled health check. For detailed operations, refer to ***Configure Scheduled Health Check*** .

## Configure Check Items

On the top of the Manual Check page, click **Configure Check Item** to enter the Health Check Item List page.

- Under the **Configure Check Item** Tab
  - Click > in front of the category name to display the available check items.
  - Click ⊘ in the Operation column of an item which is not ignored and select the object to take effect. Once the check item is ignored, the issues of the selected object checked by this item will not be reported.
- Under the **Ignored Check Item** Tab
  - Click **Categorize by Check Type** or **Categorize by Object** to display the ignored check items by check type or object.
  - Check the ignored item(s) and click **Restore** to cancel ignoring them.

## Manage Pending Tasks

On the Pending Task section, the issues imported to the pending task will be listed.
Click a pending task name to edit its name, level, notes, and email notification settings on the right pane.
Move the cursor over a pending task and click **Handle** or **Leave Unhandled** to handle a single task.

Check the pending task(s) and click **Handle** or **Leave Unhandled** in the top right corner of the section to batch handle the selected task(s).
The handled pending tasks will disappear from the Pending Task section and display on the Maintenance Log page. For details, refer to ***Search for Maintenance Logs*** .
Click **View All** at the bottom of this section to enter the Pending Task page. For details, refer to ***Add Custom Pending Tasks*** .

### View Last Check Results

On the Last Check Time section, the last check time and the corresponding issue overview will be displayed.
Click > of an issue category to enter the Health Check Result page and locate to the corresponding details list.
Click **View Check Result** in the top right corner of the Last Check Time section or click **View Result** on the top of the Manual Check page to enter the Health Check Result page.

## 9.3.2 Add Custom Pending Tasks

The Pending Task page lists the custom pending tasks besides pending tasks imported from the Manual Check page. You can add custom pending tasks to accommodate your needs, handle, ignore, delete, and export pending tasks, and batch set notifications. This section will guide you through adding custom pending tasks.

**Steps**

1. Select **Pending Task** on the left.
2. Select **Add Custom Pending Task**. This part will introduce key parameters.

   **Level**

   Select one of the following three levels:

   - **Exception**: It refers to an error or an exceptional situation. For example, if a device goes offline due to network issues, it would be considered an exception.
   - **Risk**: It refers to potential compromise of a function or system due to certain factors. For example, if you set a weak password, the device information risks being leaked.
   - **Suggestion**: It refers to a recommendation or advice that improve the performance or functionality of a system. For example, configuring the NTP server or adjusting the device inspection frequency are suggestions to enhance the system's performance.

   **Email Notification**

   To receive emails of pending task notifications at a scheduled time, switch on **Email Notification**. You can add a new email template or select an email template to define the recipient information and content. For setting email templates, refer to ***Email Settings*** .
3. Click **OK** to save the settings.
4. **Optional:** After adding pending tasks, you can edit them, handle them, leave them unhandled, delete them, batch set notifications, batch disable notifications, export these tasks, filter these

tasks according to various conditions, set the adaptive column width, and customize column items.

## 9.4 Resource Status

You can monitor the status of the added resources, such as access control devices and Recording Servers, which helps you find out and maintain the abnormal resources in time, ensuring the smooth running of the platform to the greatest extent.

On the top, select → **Basic Management** → **Maintenance** → **Resource Status** .

Select a resource type to perform the following operations.

### Common Operations

| Operation | Description |
|---|---|
| Filter Resource Status | Check the checkbox in the top right of status display page to select exception types from the drop-down list to filter the resource status. |
| View Device Status | Click the device name to view the status details and basic information of the device. |
| Configure Device | Click in the Operation column to go to the Area page to configure the parameters of the specified device. |
| Filter Device | Select the device type(s) from the first drop-down list on the top to filter the device status by device type. |
| Export Status Data | Click **Export** to export the status data as CSV or Excel to the local PC. |
| Refresh Resource Status | Click in the Operation column to refresh the status of the specified resource, or click **Refresh** to refresh the status of all resources displayed on the page.<br>**Note**<br>The resource status will be automatically refreshed in a specified interval (see details in ***Set Auto-Check Frequency*** ). |
| Edit Current Value | Click in the Current Value column to edit current value of the device. |

## Camera Status

| Operation | Description |
|---|---|
| View Related Camera Status | Click the IP address to view the status of the device to which the camera is related. |
| View Online/Offline Records | Click in the Operation column to view the online/offline records of the specified camera. For details, see ***Search for Online/Offline Logs of Resource*** .<br>**Note**<br>This operation is not available for the cameras added on Remote Sites. |
| View the Recording Status | Click in the Operation column to view the recording status of the camera. For details, see ***Search for Recording Status of Resource*** .<br>**Note**<br>This operation is not available for the cameras added on Remote Sites. |
| View Camera with Abnormal Image | Click **View Camera with Abnormal Image** to view the videos of cameras with abnormal images. And you can also export the image diagnosis results of selected camera(s) or all cameras in PDF format. |

## Door Status

| Operation | Description |
|---|---|
| Control Door Status | Click in the Operation column and select a control type from the drop-down list to control the door status.<br>• **Unlock**: When the door is locked, unlock the door and it will be open. After the open duration (configured via the Web Client), the door will be closed and locked again automatically.<br>• **Lock**: When the door is unlocked, lock the door and it will be closed. The person who has the access permission can access the door with credentials.<br>• **Remain Unlocked**: The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required (free access). |

| Operation | Description |
|---|---|
| | **Note**<br>For the door linked to video intercom device, setting its status to remain unlocked is not available.<br>• **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 user with super access permission. |
| Ignore Device Status | Click on the top to ignore the RS-485 card reader status. |

### Encoding Device Status

| Operation | Description |
|---|---|
| View Error Details | In the **Disk Status** column, view the error details if a disk is abnormal. |
| View Recording Status of Channels | Click the status in the **Recording Status** column to view the recording status of channels configured to store the video files on this encoding device. If the recording settings are abnormal, you can click **Exception** in the **Recording Status** column to view the exception details in the pop-up pane. |
| Wake Up Solar-Powered Camera | Click to wake up a solar-powered camera if it is in the sleep mode. |
| View Online/Offline Records | Click in the Operation column to view the online/offline records of the encoding device. For details, see ***Search for Online/Offline Logs of Device*** . |

### On-Board Device Status

| Operation | Description |
|---|---|
| Print Debugging Log Command | Click in the Operation column to print debugging log command. |
| Export Device Logs | Click in the Operation column to export logs of an device. |

## 9.5 Log Search

Three types of log files are provided: server logs, device logs, and resource logs. The server logs refer to the logs files stored in the SYS server on the current site and remote sites; The device logs

refer to the log files stored on the connected devices, such as encoding device and security control device; The resource logs refers the logs about camera recording status, online status, and call-back status. You can search the log files, view the log details and backup the log files.

### 9.5.1 Search for Server Logs

You can search for server logs of the current site or Remote Sites, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

**Steps**

1. On the left, select **System Log → Server Logs** .
2. In the **Site** area, select the current site or a Remote Site.
3. In the **Event** area, select one or multiple log types and sub types.

   **Note**

   Error logs record failures or errors. Warning logs record license expiration events. Information logs refer to other general logs which record successful or unknown operation results.
4. In the **Source** area, set the source of the logs that you want to search for.
5. **Optional:** In the **Resource Name** area, enter the name of a resource to search the logs of the resource.
6. Set the time range for search.

   **Note**

   You can select **Custom** to set a precise start time and end time.
7. Click **Search**.

   All matched logs are listed with details on the right.
8. **Optional:** Check all or specific logs, click **Export**, and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

### 9.5.2 Search for Online/Offline Logs of Device

You can search for the online/offline logs of all devices. The online/offline logs provide information on the current device status (online or offline), latest offline time, total offline duration, etc.

**Steps**

1. On the left, select **System Log → Device Log** .
2. In **Type**, select **Online/Offline Log** as the log type.
3. Select a device type and check the devices you want to search.
4. Set the time range for search.

**Note**

You can select **Custom** to set a precise start time and end time.

5. **Optional:** If there are a large number of devices, switch on **Statistics Range** to set a range of total offline times during the specified time range to filter the devices, or set a total offline duration to filter the devices.
6. Click **Search**.

   The offline/online log of each device are listed on the right. You can check the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each device.
7. **Optional:** Perform further operations after searching for device logs.

| | |
|---|---|
| **View Offline History** | Click on device name to view history online duration (displayed as a line chart) and status (displayed as a list) of the device.<br>You can perform the following operations.<br>• Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data.<br>• View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point. |
| **View Device Logs** | Click in the Operation column to view the logs stored on the device. |
| **Export Logs** | Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC. |

## 9.5.3 Search for Logs Stored on Device

You can search for the logs stored on encoding devices, security control devices, decoding device, network transmission devicesaccess control devices, elevator control devices, on-board device, and fire protection device.

**Steps**

1. On the left, select **System Log → Device Log** .
2. Select **Log on Device** as the log type.
3. Select a device type and select the device you want to search.
4. Select the main event as **Normal** or **Battery Information** and check the sub event(s) to be searched for.
5. Specify the time range of this search.

**Note**

You can select **Custom Time Interval** to set a precise start time and end time.

6. Click **Search**.

   All matched logs are listed with details on the right.

7. **Optional:** Perform further operations after searching for device logs.

| | |
|---|---|
| **View Offline History** | Click on device name to view history online duration (displayed as a line chart) and status (displayed as a list) of the device.<br>You can perform the following operations.<br>• Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data.<br>• View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point. |
| **View Device Logs** | Click in the Operation column to view the logs stored on the device. |
| **Export Logs** | Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC. |

### 9.5.4 Search for Online/Offline Logs of Resource

You can search for the online/offline logs of cameras on the current site. The online/offline logs provide information on the current device's status (online or offline), latest offline time, total offline duration, etc.

**Steps**

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Online/Offline Log**.
3. Click to show the area list on the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

| | |
|---|---|
| **Remove a Camera** | Click to remove the camera from the list. |
| **Remove All Cameras** | Click to remove all cameras in the list. |

5. Set the time range for search.

**Note**

You can select **Custom** to set a precise start time and end time.

6. **Optional:** If there are a large number of devices, switch on **Statistics Range** to set a range of total offline times during the specified time range to filter the devices, or set a total offline duration to filter the devices.
7. Click **Search**.

   The offline/online log of each resource are listed on the right. You can view the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each resource.
8. **Optional:** Perform further operations after searching fro resource logs.

| | |
|---|---|
| **View Offline History** | Click resource name to view history online duration (displayed as a line chart) and status (displayed as a list) of the resource.<br>You can perform the following operations.<br>• Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter data.<br>• View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point. |
| **View Device Online/ Offline Logs** | Click the IP address to view the online/offline logs of the device where the resource is linked. |
| **Export Logs** | Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC. |

### 9.5.5 Search for Recording Status of Resource

You can search for the recording status of cameras on the current site. The recording status includes the recording integrity rate, total time length abnormal recording, times of recording interruptions, etc.

**Steps**

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Recording Status**.
3. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

   **Remove a Camera** Click and then click to remove a camera from the list.

   **Remove All Cameras** Click and then click to remove all cameras in the list.
5. In **Time**, specify the time range of this search.

   **Note**

   You can select **Custom Time Interval** to set a precise start time and end time.
6. **Optional:** If there are a large number of resources, check **Filter Condition** and set the filter conditions.

   **Retention Duration (Days)**

   Set a range of the retention duration of the recorded video footage to filter the cameras.

   **Recording Integrity Rate**

   Set a range of the recording integrity rate to filter cameras. The recording integrity rate refers to the percentage obtained from dividing the actual recording duration by the scheduled recording time.

**Note**

7. Click **Search**.

   Recording status of each camera are listed on the right, including camera name, camera IP address, area where the camera belong, video storage type, etc.

   **Start Time**

   The time when the camera started recording.

   **End Time**

   The latest time when the camera was recording.

   **Retention Duration (Days)**

   The retention duration (unit: day) of the recorded video footage refers to the duration between **Start Time** and **End Time**.

   **Total Length**

   The total time length of video storage.

   **Abnormal Total Length**

   The total time length of the video loss within the scheduled time.

   **Recording Interruption**

   The total times of recording interruption within the scheduled time.

8. **Optional:** Check historical recording status.

   1) **Optional:** Click **Rule** in the top right corner to view the analytical rules for history videos.

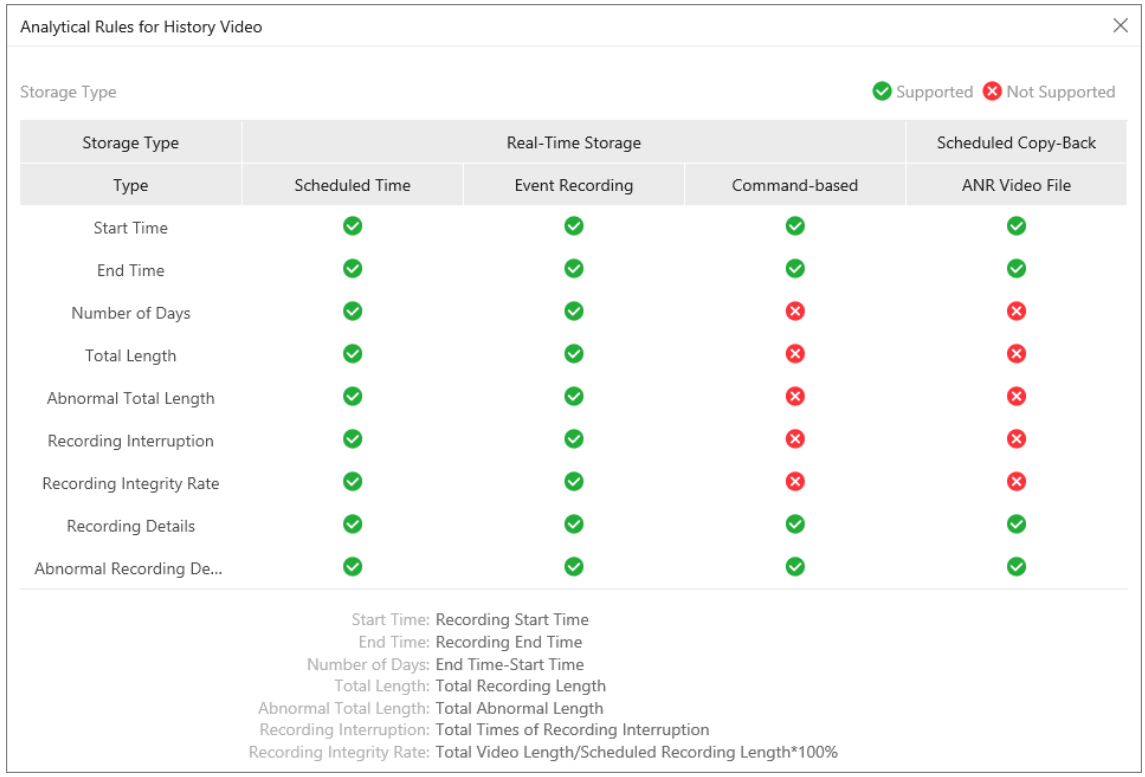



**Figure 9-13 Analytical Rules for History Video**

2) Click a camera name to open the History Recording Status panel.

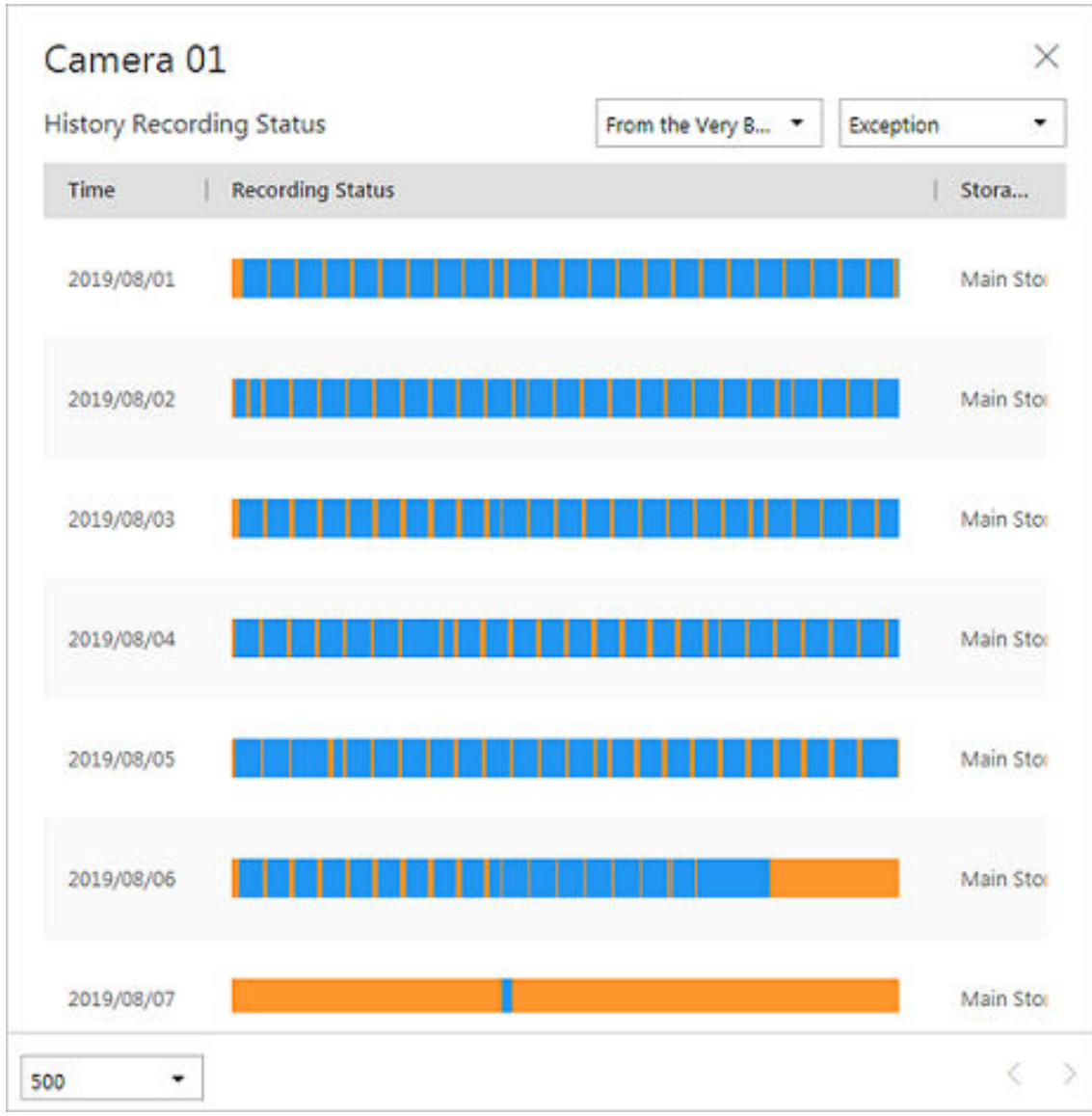



**Figure 9-14 History Recording Status**

**Note**

The blue parts on the time bars represent the time periods during which video footage were recorded. The orange parts on the time bars represent the time periods during which video loss occurred or the time periods during which no recording schedule existed.

3) Select a time period and a status (abnormal or all) from the drop-down lists respectively to filter data.
4) **Optional:** Select the number of records displayed on each page of the History Recording Status panel from the drop-down list at the lower-left corner of the panel.
5) **Optional:** Move the cursor to the time bar to show the 24 hours on it, and click one hour to view recording status details within the hour.

9. **Optional:** Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

### 9.5.6 Search for Call-Back Status of Resource

You can search for the call-back status of cameras on the current site. In search results, you can view the camera name, storage type, recording copy-back rate, etc.

**Steps**

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Call-Back Status**.
3. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

   **Remove a Camera** Click and then click to remove a camera from the list.

   **Remove All Cameras** Click and then click to remove all cameras in the list.
5. In **Time**, specify the time range of this search.

   **Note**

   You can select **Custom Time Interval** to set a precise start time and end time.
6. Click **Search**.

   Call-back status of each camera are listed on the right.
7. **Optional:** Click **Export** and then select a file format (i.e., Excel or CSV) to download the call-back status to your local PC.

### 9.5.7 Search for Maintenance Logs

Maintenance logs serve as a reference for troubleshooting and analyzing the history of maintenance events to improve efficiency and reliability. You can search for maintenance logs based on the handler, handling time, handling status and other conditions.

**Steps**

1. On the navigation bar, select → **Basic Management → Maintenance → System Log** .
2. Select **Maintenance Log** on the left.
3. Edit the search parameters, namely the pending task name, object, level, handler, handling time, and handling status. This part will introduce key parameters.

   **Object**

   The objects undergoing the health check.

   **Level**

   Select one of the following three levels:

- Exception: It refers to an error or an exceptional situation. For example, if a device goes offline due to network issues, it would be considered an exception.
- Risk: It refers to potential compromise of a function or system due to certain factors. For example, if you set a weak password, the device information risks being leaked.
- Suggestion: It refers to a recommendation or advice that improve the performance or functionality of a system. For example, configuring the NTP server or adjusting the device inspection frequency are suggestions to enhance the system's performance.

4. Click **Search**.

   All matched logs are listed with details on the right.

5. **Optional:** Select specific logs, click **Export** or click **Export → Export All** in the pull-down menu in the upper-right corner of the page, and then select a file format (Excel or CSV) to download the searched logs as a single file to your local PC.

## 9.6 Service Manager

After successfully installing the service module(s), you can run the Service Manager and perform related operations of service, such as starting, stopping, or restarting the service.

**Steps**

1. Right-click and select **Run as Administrator** to run the Service Manager.

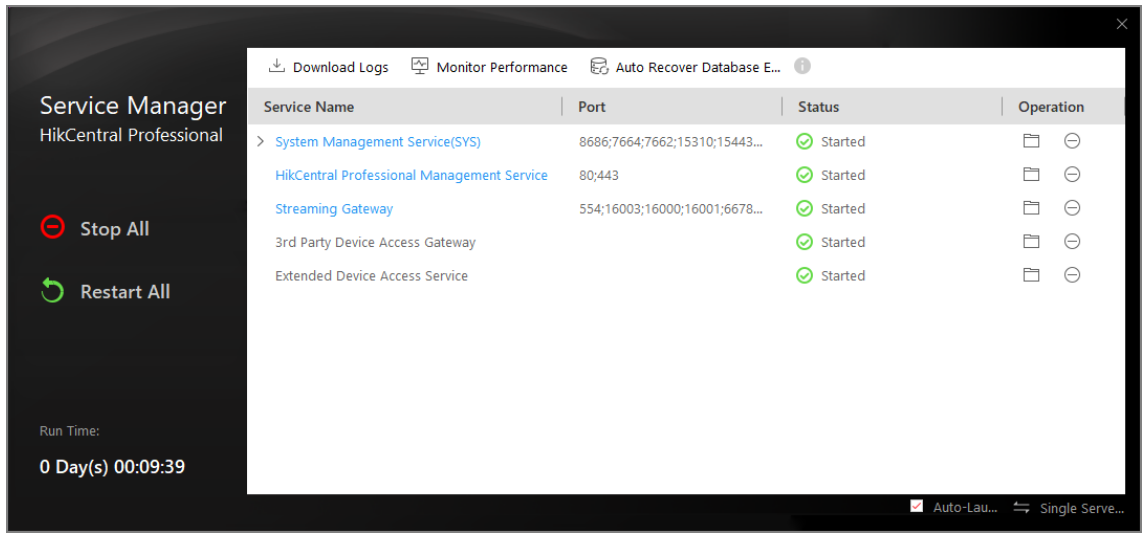



**Figure 9-15 Service Manager Main Page**

**Note**

The displayed items vary with the service modules you selected for installation.

2. **Optional:** Perform the following operation(s) after starting the Service Manager.

| | |
|---|---|
| **Stop All** | Click **Stop All** to stop all the services. |
| **Restart All** | Click **Restart All** to run all the services again. |

| | |
|---|---|
| **Stop Specific Service** | Select one service and click ⊖ to stop the service. |
| **Edit Service** | Click the service name to edit the port of the service.<br>**Note**<br>If the port number of the service is occupied by other service, the port No. will be shown in red. You should change the port number to other value before the service can work properly. |
| **Open Service Location** | Select one service and click 🗀 to go to the installation directory of the service. |

3. **Optional:** Click **Auto Recover Database Exception** to recover database exception caused by accidents such as power-off and unexpected reboot.
   1) Enable **Auto Recover Database Exception**.

   **Note**

   The database service will restart after you enable this function.

   2) Click 🗁 to set the archive path for recovering the database.

   **Note**

   - The remaining disk space of the archive path should be twice as the size of database data.
   - The archive path should be under a path in English.

   3) Click **OK** to finish setting.
4. **Optional:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.
5. Click **Dual-Server Deployment** to deploy the database on another server.

## 9.7 Set System Data Backup

Backing up system data refers to the process of configuring and initiating a backup of the system's data to a secure location. This ensures that in the event of a system failure, the data can be restored to a previous state, minimizing data loss.

In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data → Back Up** .

For Standalone Mode:

1. In **Type**, select the data that you want to back up.
2. Set the backup frequency and time.
3. Set the maximum number of backup files.
4. Click **Save** to save the backup schedule, or click **Save and Back Up Now** to back up the system data immediately.

For Cluster Mode

**Manual Backup**

Click **Back Up Now** to start backing up all the system data generated till now.

**Auto Backup**

The updated system data is automatically backed up every 6 hours.

## 9.8 Restore System Data

Restoring system data refers to the process of bringing back the system's data to a previous state, which is often done after a system failure or to revert changes that have caused exceptions.

**Note**

Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data → Restore** .

For Standalone Mode

1. Select a backup file to be restored.

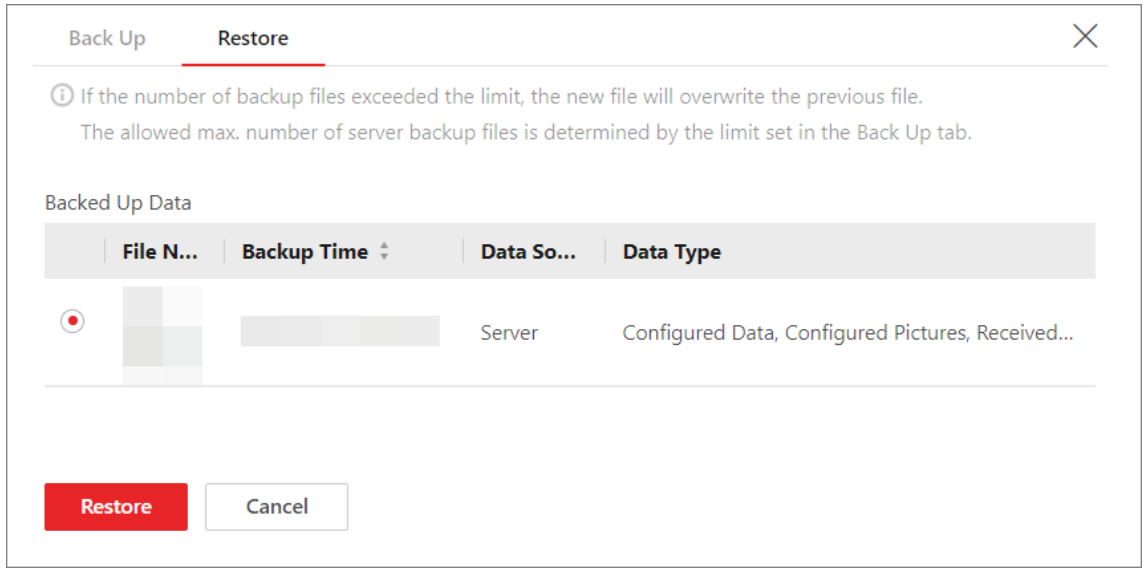



**Figure 9-16 Restore System Data**

2. Click **Restore**

**Note**

- After restoring the system data, you must reboot the SYS service via Service Manager and log in to Web Client again.
-

For Cluster Mode

1. Select a backup file source.
2. If you have selected the source as **Auto Backup**, set the backup time.
3. Select a backup file.
4. Click **Restore Now**.

## 9.9 Export Configuration Data

You can export and save configuration data to local disk, including recording settings and resource configurations.

**Steps**

1. In the top right of the client, click **Maintenance and Management → Export Configuration Data** .
2. Select the configuration data types that you want to export.

**Note**

If you enable Password Protection, you can export only the configuration data of encoding devices, and you need to set a password.

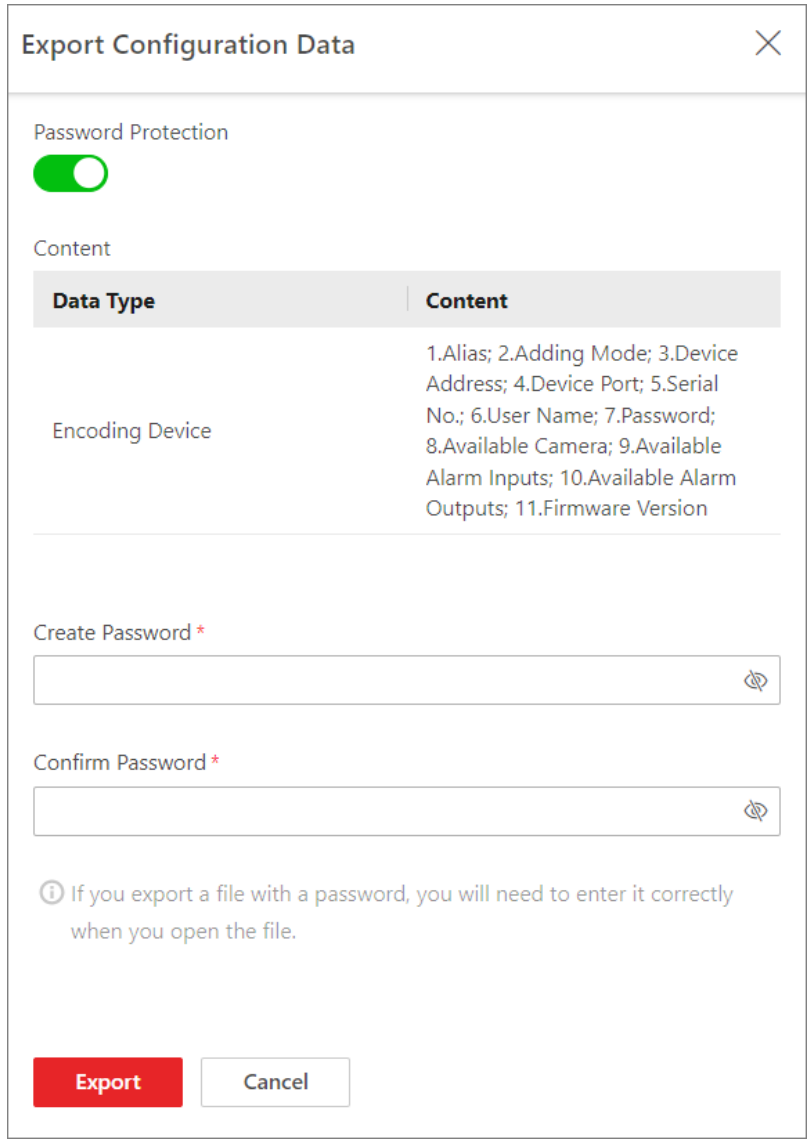



**Figure 9-17 Password Protection**

3. Click **Export** to download the data to the local PC.

**Note**

The configuration data file is in CSV format.

## 9.10 Import Configuration Files

If you have used applications on the iVMS-4200, you can get configuration files (including configurations of devices, persons, events, and access levels) of these applications and import

them to the system via the Web Client for quickly configuring the corresponding applications on the system.

**Steps**

**1.** In the top right of the Web Client, click **Maintenance and Management → Data Migration** .

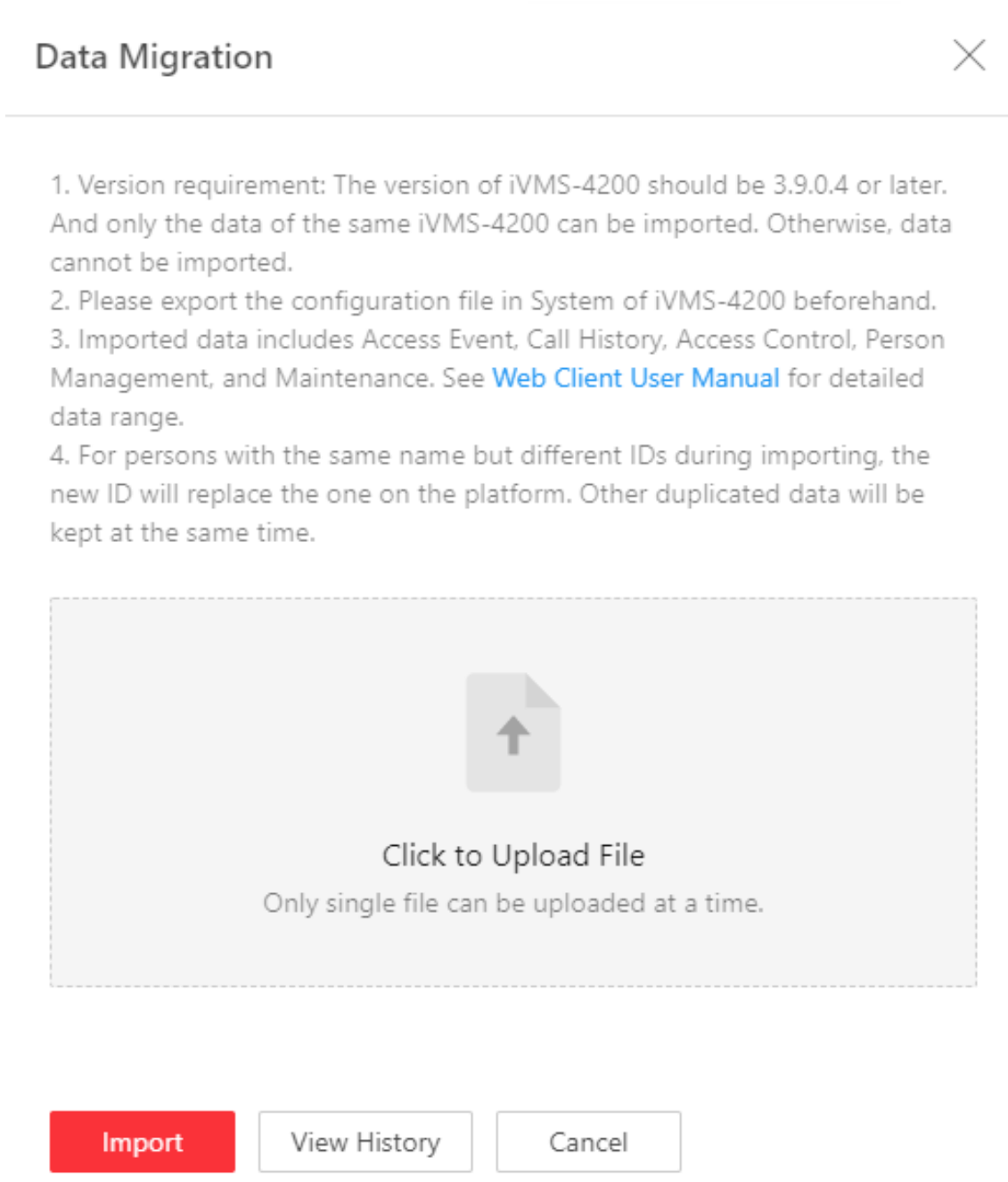



**Figure 9-18 Data Migration**

2. Click to select the configuration file(s) of iVMS-4200 from the local PC.
   - The data that can be imported include the followings.
     - Device: The information about access control devices, video intercom devices, and elevator control devices. The related area and channel resources will be added automatically according to devices.
     - Person: The basic information and credential information (i.e., card, fingerprint, face, and iris).
     - Event: Event types that are both supported by iVMS-4200 / iVMS-4200 AC and HikCentral Professional.
     - Access Level: The settings of access levels, holidays, and schedule templates.
   - When importing device configurations, if the number of resources exceeds the limit, the excess resources cannot be imported.
3. Click **Import** to start importing the configuration file(s) to the platform.

**Note**

During the import, you can close the details window and normally use the platform.

A progress bar will pop up and display the import progress, import result, and error information (if failed).

# Chapter 10 Central Management

For scenarios where large quantity of devices (no less than 10,000), server clusters can be deployed and displayed.

Go to → **Basic Management → Server Management** .

## 10.1 Add a Server

Add resource servers, streaming servers, recording servers, and intelligent analysis servers to the platform and configure parameters for them.

On the top left, click **Add Server** to open the adding pane, select the server type and configure corresponding parameters.

### Add a Resource Server

The server is deployed in the LAN by default.

**Main Server**

The main server is used for managing and monitoring all sub servers and standby servers. On the main server, you can add sub servers and standby servers to build clusters. Then, the cluster topology will show for overview or editing servers. You can manage all users & roles, resources, devices, events, and recording schedules, and search records generated by all servers on the main server.

**Sub Server**

The sub servers manage all resources and devices, receive and process data from devices, and is used for record storage.

**Standby Server**

When a sub server does not work, a standby server will take over.

**IP Address and Server Port**

The server's IP address and port number in the LAN.

**Access WAN and IP Address**

Enable the **Access WAN** when devices in the WAN need to access to this server. The address below is the address available to the WAN, and should be the same with the IP address configured on **System → Network → WAN Access** page. If you have configured the address on this page, the address will be copied and displayed here automatically. This address is the only IP/domain address of the whole resource server cluster, which means you enter this for one resource server and the other resource servers will share this address.

## Add a Streaming Server

**Network Location**

**LAN IP Address**: Select this when the streaming server is deployed in the same LAN with the main server. In this scenario, if devices in the WAN need to access to this server, switch on **Enable WAN Access** and enter the address available to the WAN. This IP address is exclusive for this server.

**WAN IP Address**: Select this when the streaming server is deployed in the WAN.

**Server Cluster Deployment**

Select **Yes** to add this server to the streaming server cluster.

Hover the cursor on the streaming server cluster and click **Check Relate Resource of Cluster** to view devices streaming via these servers.

## Add a Recording Server Cluster and Intelligent Analysis Server

The recording server should be deployed in the same network domain with the main server.
If you have added recording servers and intelligent analysis servers in the Device module, they will be displayed on the Server Management page. For parameter introduction, see ***Add Server(s)*** .

## Operations After Adding Servers

On the server topology, you can hover the cursor on a server, and click the server name to show the Edit Server Information Pane on the right. You can edit the server information, or click **Delete Server** at the bottom to remove the server from the system.

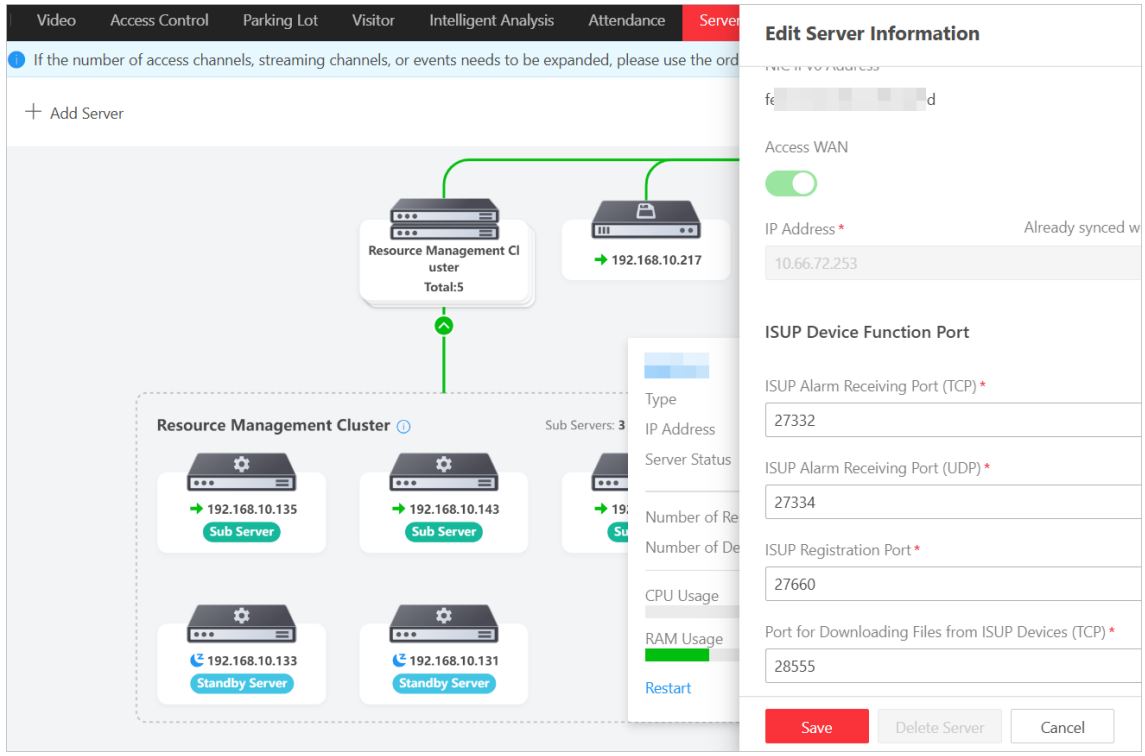



**Figure 10-1 Edit Server Information**

## 10.2 Create and Edit Clusters

A resource server cluster and streaming server cluster can be created on the Server Management page, after which the topology of servers will be displayed. You can view server details or edit them.

### Resource Server Cluster

If more than one resource server is added, all resource servers will be displayed together in the Resource Server Cluster area under the main server.
After adding, hover the cursor on any server to show its details. On the details card, you can restart a sub server or standby server, or click the server name to show the Edit Server Information pane on the right and edit the server settings on the pane.

### Streaming Server Cluster

When adding a single streaming server, you can select **Yes** under the **Server Cluster Deployment** to create a streaming server cluster, or add it to the existing streaming server cluster.
If you have added multiple streaming servers, a notification may pop up on the topology asking you whether to create a streaming server cluster for these servers. Click **OK** and select servers to create one.

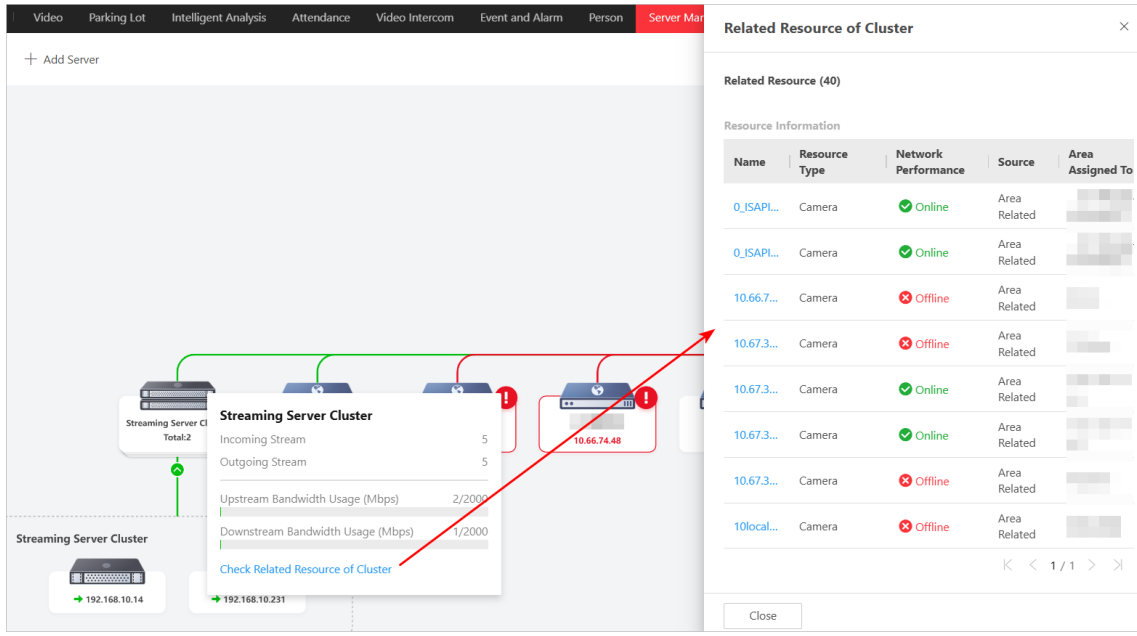



**Figure 10-2 Related Resource of Cluster**

## 10.3 Migrate Resources to Other Sub-Servers

When a sub server's CPU usage is too high, or there are too many devices available on the sub server, or after you change a resource server to the main server, you can try to migrate its devices to other servers.

On the left, click **Device Migration**, and select a sub server to show the Server Resource Details pane. Then, you can migrate part or all of the devices to another server.

- : Go to the details page of a single device.
- : Migrate a single device to another sub server.

## 10.4 Take Over a Sub Server or a Standby Server

By default, a standby server can automatically take over a sub server which does not work. But in some scenarios, you may need to manually make a standby server take over a sub server, and when the sub server restores, you can make the sub server take over the standby server.

On the Server Management page, hover the cursor on a standby server, and click **Take Over Sub Server**. Then, select a sub server (if there are more than one sub server) from the pop-up window and click **OK**. This operation will build a linkage between the sub server and standby server and a green line will show to link the two servers. When the sub server restores, you can hover the cursor on the sub server and click **Take Over Standby Server**.

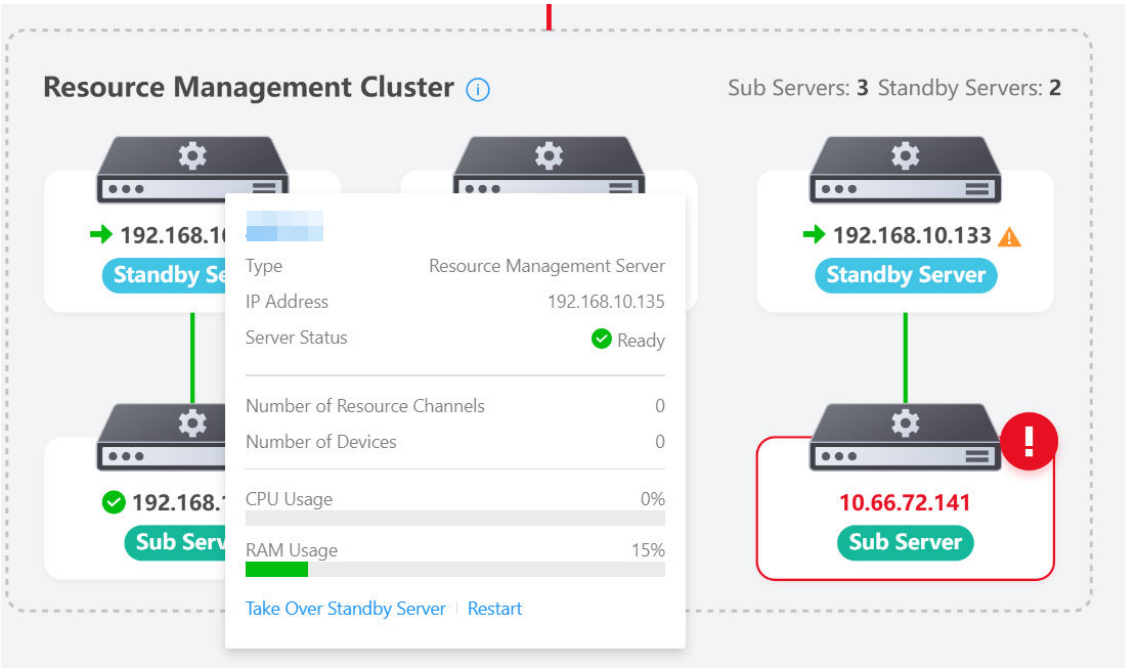



**Figure 10-3 Resource Server Cluster**

## 10.5 Operation and Management Center

The Operation and Management Center displays the status of the main server and sub servers, and shows the deployment details of clusters.

Three ways for the Administrator to go to the Operation and Management Center:

- On the PC desktop, double-click the (the installation program icon of the Operation and Management Center)
- On the Server Management page, click on the right of **Resource Management Center** and click **Go to Operation and Management Center**.

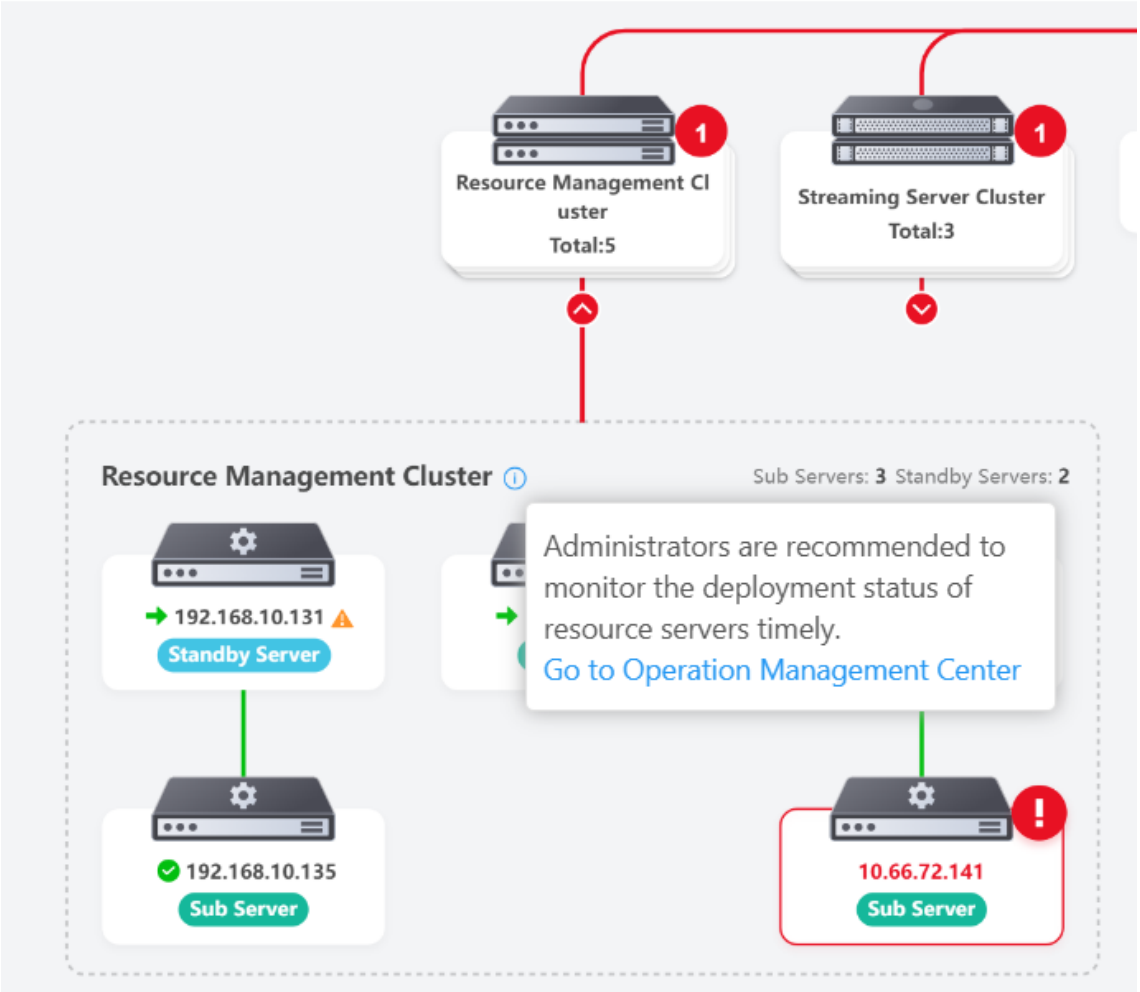



**Figure 10-4 Go to Operation and Management Center**

- In the Application Market of the main server, after installing/upgrading/uninstalling any add-ons, a notification will pop up telling you to go to the Operation and Management Center for installing these add-ons on all sub servers. Click **Deploy Now** to jump to the Operation and Management Center.

Click a server's card to show its details on the right. You can see what add-ons are synchronized to install on each sub server from the main server.

On the top right, click to display add-ons which need to be installed on all sub servers. Click **Upgrade to All Servers** and a notification window will pop up for you to confirm to start the installation. Click **OK** to start the installation. The installing progress will be displayed on the main server's card.

# Chapter 11 Remote Site Management

You can add other HikCentral Professional without RSM (Remote Site Management) module to the HikCentral Professional with RSM module as the Remote Site for central management.

On the top navigation bar, select → **Basic Management** → **Remote Site Management** .

After adding the Remote Site to the Central System, you can manage the Remote Site's cameras (such as live view and playback), add the Remote Site's configured alarms so that you can manage the alarms via the Central System, and set the recording schedule for the Remote Site's cameras and store the recorded video files in the Recording Server added to the Central System.

**Central System**

If the HikCentral Professional has RSM module (based on the License you purchased), you can add other Remote Sites to this system.

**Remote Site**

If the HikCentral Professional doesn't have RSM module (based on the License you purchased), you can add it to the Central System as Remote Site.

**Note**

- The system with RSM module cannot be added to other Central System as Remote Site.
- If one Remote Site has been added to one Central System, it cannot be added to other Central System.

On the left, click **Basic Configuration**, and check **Receive Site Registration** to allow the Central System to receive the registration from remote sites.

## 11.1 Management of Remote Site Groups

Users can create a new remote site group, or move a site to a site group.

On the left of the Remote Site Management module, click **Remote Site**.

- Create a new remote site group:
  - In the top left, click **New Group**, enter the group name, and select a parent group, finally click **Confirm**.

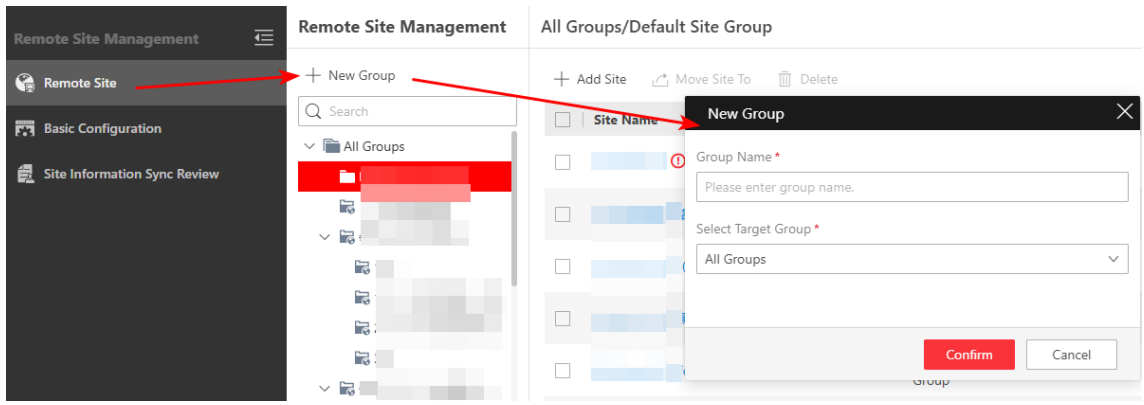



**Figure 11-1 Add Remote Site Group**

- Hover the cursor on a group below All Groups, and click ··· → **New Group** to create a group below the current group.

- Move a site group:
  - Drag a group to another group.
  - Hover the cursor on a group, click ··· → **Edit** , in the Select Target Group drop-down list, select a target group to move to.

## 11.2 Enable Receiving Registration of Remote Sites

After enabling the Receive Site Registration function, the Central System can receive the registration information from remote sites, so that you can add remote sites via the mode of Site Registered to Central System.

On the left of the Remote Site Management module, click **Basic Configuration**, check **Receive Site Registration**, and save the setting.

## 11.3 Add a Remote Site

You can add a remote site to the platform by IP address or domain name, add a remote site registered to the Central System, and batch adding remote sites.

Click **Add Site** to enter the Add Remote Site page.

**Note**

- If you did not set the NTP server which is used for synchronizing the time between the SYS and the NTP server, a message will be displayed on the top of this page. If you need, click the button to go to the System Configuration page.
- When adding remote site, the site's resource and area information are imported to the Central System by default.

**Adding Mode**

**IP Address/Domain**

Enter the IP/domain address of a remote site to add it. Enter a custom name for the remote site, or check **Get Name** to use the site's name.

**Site Registered to Central System**

Before adding remote sites via this mode, the ***Receive Site Registration*** should be enabled, and the ***Site Registration and Connection*** of the remote site should be finished.

Remote sites which has finished the registration and connection to the Central System will be displayed in the Select Site area. Check to-be-added remote sites before clicking **Add** at the bottom.

You can click **Show Added Site** to view added remote sites.

**Batch Import**

Before adding remote sites via this mode, the ***Receive Site Registration*** should be enabled, and the ***Site Registration and Connection*** of the remote site should be finished.

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | Rule | | | | | | | |
| 2 | 1. Fields marked with asterisk (*) are required. | | | | | | | |
| 3 | 2. If 1 is selected for login mode, you need to enter the user name and password; if 2 is selected for login mode, you need to enter the access key (AK) and secret key (SK). | | | | | | | |
| 4 | *IP Address / Server Address | *Port No. | *Login Method (1: Login via Account and Password, 2: Authorize Login) | User Name | Password | Access Key (AK) | Secret Key (SK) | Description |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |

**Figure 11-2 Downloaded Site Template**

**Login Mode**

**Login via User Name and Password**

Enter the remote site's admin user name and password. The password will be required to update every 3 months. The password change will cause a connection failure of the Central System.

**Login via Authentication Code**

The access key (AK) and secret key (SK) of the remote site's admin user are required. This mode avoids the disconnection from the remote sites caused by password expiration.

**Resource Importing Mode**

Only available when the adding mode is set to **IP Address/Domain**. You can import all or part of resources of the remote site to the Central System, or import resources later.

**Receive Site Alarm**

Making the Central System receive all or part of alarms configured in the remote site.

After receiving the alarm from Remote Site, the alarm will be configured as alarm in Central System automatically. You can click **Default Configuration Rule** to view the imported alarms' default settings including alarm name, alarm priority, actions, etc.

After receiving the alarm from Remote Site, the alarm will be configured as alarm in Central System automatically. You can click **Default Configuration Rule** to view the imported alarms' default settings including alarm name, alarm priority, actions, etc.

**Back up Remote Site's Configured Data in Central System**

Back up the Remote Sites' database in the Central System.

**Max. Number of Backups**

The earlist backup will be covered if the backup times exceeds the entered value.

## 11.4 Edit a Remote Site

After adding the Remote Site, you can view and edit the added Remote Site's information and set its GPS location.

In the site list, click a Remote Site name to open its details page.

View and edit the basic information of the Remote Site, including IP address, port, and name. See ***Add a Remote Site*** for parameter introduction.

In the original information section, view the Remote Site's site name, system ID, system version, and GPS location.

**Note**

If the GPS location is not configured, click **Configure** to set its location in Map module. See ***Map Management*** for details.

Click **Set Database Backup** to configure the schedule form backups, or click **Back Up Now** to start immediately.

In the upper-right corner, click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

## 11.5 View Remote Site's Changes

View new/deleted/changed resource in a remote site, or perform related operations.

**Note**

The site should be online if you need to view site changes.

In the upper-right corner of the site details page, click **Changes of Remote Site** to open the changes pane, which displays new/deleted/changed resource of the remote site. The resource includes cameras, doors, elevator control devices (including their floors), and parking lots.

**New Resource**

Newly added cameras, doors, elevator control devices (including floors), or parking lots that are not synchronized to the Central System.

**Import All**

Click **Start Importing** at the bottom to import all newly added resources to the Central System.

**Import Partially**

Select resources or parking lots to synchronize them to the Central System.

**Deleted Resource**

Resources deleted from the remote site are displayed. Click **Delete All** to remove them all from the Central System.

**Changed Resource**

The changed resource refers to the name changes of cameras, doors, and elevator control devices, and parking lots' changes of name, lane, entrance and exit, and linked camera channels.

**Import All**

Click **Start Importing** at the bottom to synchronize all resource changes to the Central System.

**Change Partially**

Select resources or parking lots to synchronize their changes to the Central System.

## 11.6 Review Information Changes Synchronized from Remote Sites

When changes occur in the personnel assigned to remote sites and the vehicle information in remote sites, the remote site automatically transmits the changes back to the Central System. These changes are displayed on the Site Information Sync Review page, awaiting approval by the Central System Administrator.

On the left of Remote Site Management module, select **Site Information Sync Review**.

In the Filter area, set the filtering conditions to filter information changes of remote sites.

Check multiple to-be-reviewed information changes, and click **Batch Review** to approve or reject multiple site information changes in a batch.

Adding person does not support batch review.

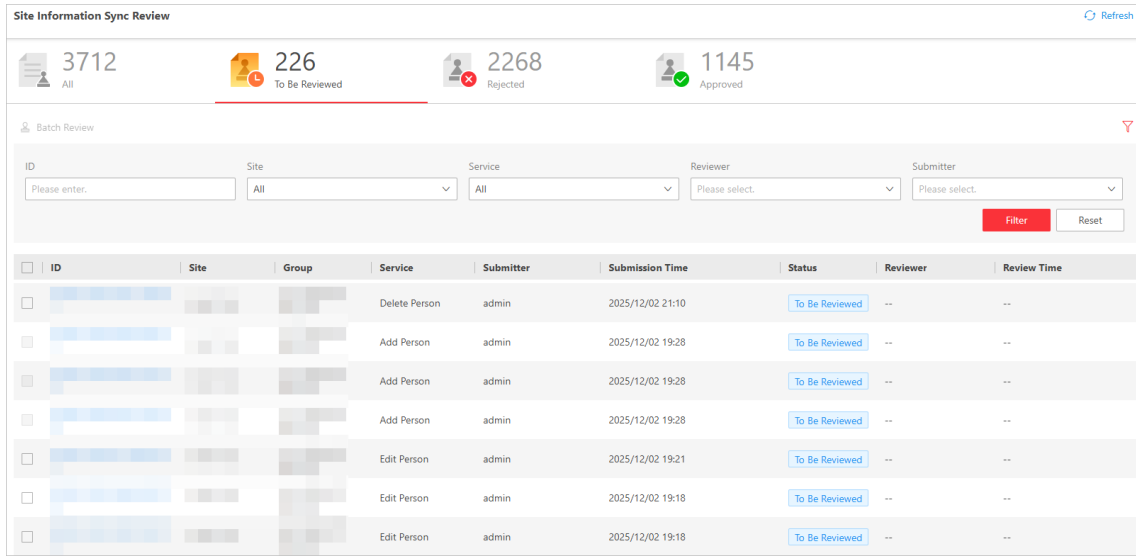



**Figure 11-3 Site Information Sync Review**

You can click an ID to open the details pane. The information changes will be marked by a red point. Click **Approve** or **Reject** according to your need.

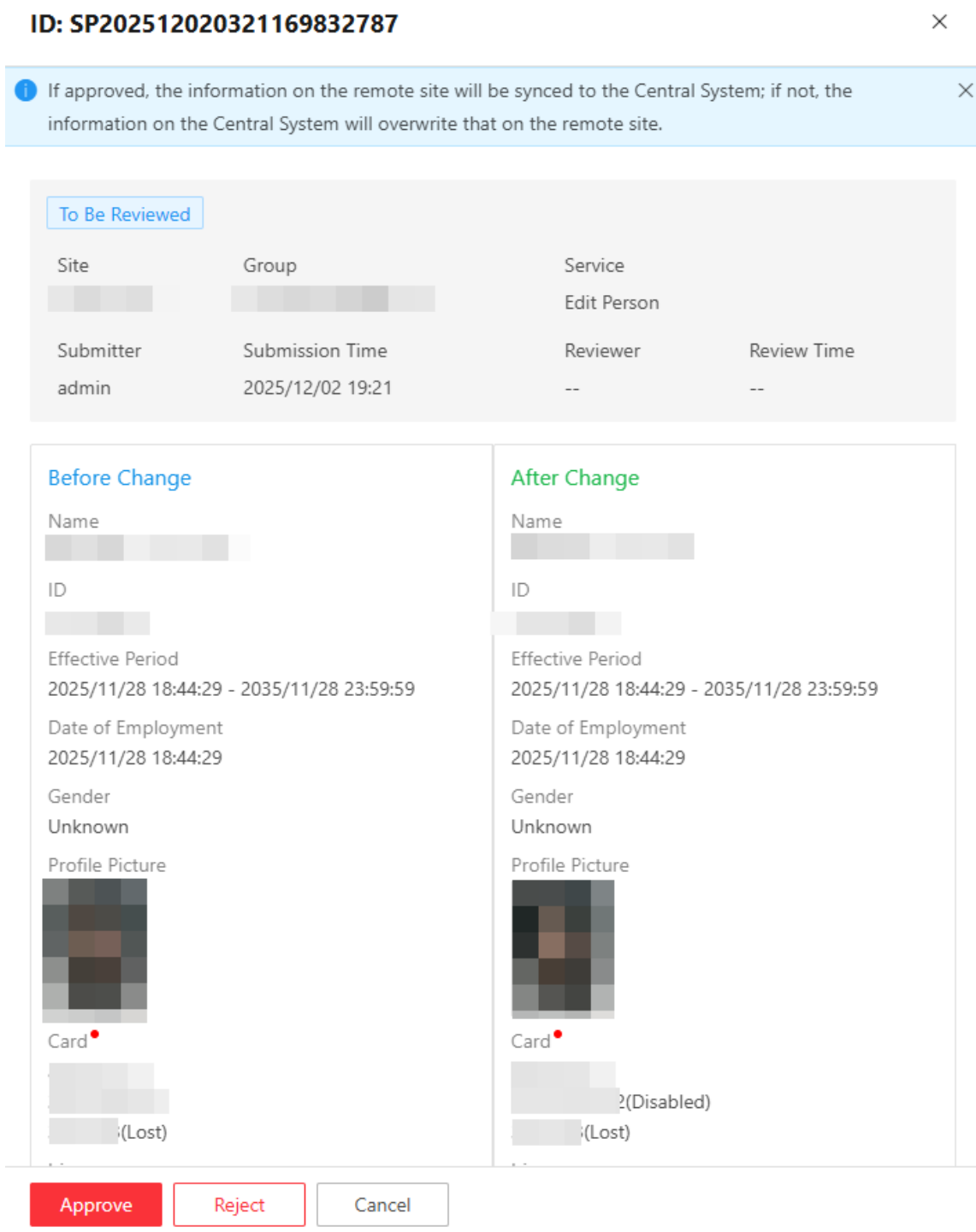



**Figure 11-4 Remote Site Changes to be Reviewed**

Approved changes will be synchronized to the Central System.

# Chapter 12 Event and Alarm

On the Web Client, you can set rules to detect events and alarms, and set linkage actions for notification. The detailed information of the events and alarms can be received and checked via the Mobile Client.

In the top left corner of the Home page, select → **Security Monitoring → Event and Alarm** .

**Event**

Event is the signal that resource (e.g., device, camera, server) sends when something occurs. The platform can receive and record events for checking, and can also trigger a series of linkage actions for notification. The event can also trigger an alarm for further notification and linkage actions (such as alarm recipients and pop-up window). You can check the event related video and captured pictures if you set the recording and capturing as event linkages.

The rule of an event includes four elements, namely, "event source" (i.e., the device which detects the event), "triggering event" (the specified event type), "what to do" (linkage actions after this event is detected), and "when" (during the specified time period, the linkage actions can be triggered).

**Alarm**

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. Alarm can trigger a series of linkage actions (e.g., popping up window, showing the alarm details) for notification and alarm handling. You can check the received real-time alarm information and search for history alarms.

The rule of an alarm includes six elements, namely, "alarm source" (i.e., the device which detects the triggering event), "triggering event" (the specified event type occurred on the alarm source and triggers the alarm), "when" (during the specified time period, the alarm can be triggered), "recipient" (the user on the platform who can receive this alarm), "priority" (the importance or urgency of this alarm), and "what to do" (linkage actions after this alarm is triggered).

**Linkage Action**

An event's linkage actions (such as recording and capturing) are used to record the event details and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, and sending email).

An alarm's linkage actions (such as popping up an alarm window, displaying on the smart wall, and audible warning) are used to record the alarm details and provide recipients multiple ways to view the alarm information for alarm acknowledgment and handling.

**Example**

What is an Event

The event can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("event source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened.

**Example**

What is an Alarm

The alarm can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("alarm source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened. This alarm is marked as High priority ("priority"), and users including the admin and operators ("recipient") can receive this alarm notification and check the alarm details.

## 12.1 Supported Events and Alarms

Currently, the platform supports following events and alarms for different types of resources.

**Video**

**Camera**

Video exceptions or events occurred in the monitoring area of the camera, such as the motion detection, line crossing, and so on.

**Alarm Input**

Events occurred on alarm inputs of video devices on the platform.

**Face Picture**

Events detected by facial recognition camera or temperature screening cameras, such as the face matched events, face mismatched events, rarely appeared person events, and so on.

**Person/Vehicle Arming Group**

Events occurred when the camera group detect and track a person or vehicle of interest, including auto person arming and tracking and auto vehicle arming and tracking.

**Portable Enforcement**

**Portable Device**

Events occurred on portable devices, including Low Battery Alarm, Use Device Before File Copied Back, Use Device Before Full Charging, etc.

**Alarm Input**

Events occurred on alarm inputs of portable devices on the platform.

**Access Control**

**Access Control Device**

Events occurred when specified operations performed for access control devices.

**Elevator Control Device**

Events occurred when specified operations performed for elevator control devices.

**Door**

Events occurred on doors of access control devices and video intercom devices, such as access event and door status event.

**Elevator**

Events occurred in elevators, such as card swiping event and elevator status event.

**Alarm Input**

Events occurred on alarm inputs of access control devices on the platform.

**Person**

Events occurred during the process of authentication by person, such as card No. matched events and person matched events.

**Patrol**

Events occurred during the patrol process, such as early patrol, late patrol, and so on.

**ANPR**

Events occurred during the vehicle recognition process, such as vehicle matched events, vehicle type matched events, and vehicle mismatched events.

**Parking Lot**

Events occurred in different parking lots or during the parking process, such as blocklist events, overstayed events, and so on.

**Alarm Detection**

**Radar**

Events detected by radar or during the radar configuration process, such as arming events, line crossing event, and so on.

**Alarm Input**

Events occurred on alarm inputs of security control devices on the platform, such as alarm input restored events, bypass events, and so on.

**Partition (Area)**

Events occurred in partitions (areas) of security control panels on the platform, such as away arming events, instant arming events, and so on.

**Peripheral**

Events occurred in peripherals of security control panels on the platform, such as deactivation, deactivation restored, and so on.

**Intelligent Analysis**

**Regional People Counting**

Events occurred during the regional people counting.

**Store People Counting**

Events occurred during the store people counting.

**Digital Signage**

Events detected by digital signage terminals, such as abnormal temperature events.

**Maintenance**

Operation exceptions occurred on the resources (e.g., cameras, doors, dock stations, recording servers) added to the platform, such as the device offline, server exception, and so on.

**Third Party**

Alarms of third-party devices.

**User**

Events occurred during the user login and logout process.

**Custom Event**

**User-Defined Event**

Events defined by users themselves.

**Generic Event**

Events transferred in the form of TCP/UDP/HTTP/HTTPS data packages from resources (e.g., external systems and devices) if something occurred and matched the configured expression.

**Device Application Event**

Events uploaded by the added resources which contain HEOP or AIOP application.

**Visitor**

Events occurred during the visiting process.

**Note**

You should enable the detection frequency of automatic checkout for visitor after the effective period.

**Broadcast**

Events occurred on alarm inputs linked with IP speakers.

**Optical Fiber Sensing**

Evens related to optical fiber sensing, such as fiber cut alarms and intrusion alarms.

**Security Inspection**

Events occurred on walk-through metal detectors.

**On-Board Monitoring**

Events detected by driving devices and occurring during the vehicle driving process.

**Fire Protection**

Events detected by fire detectors.

**Traffic Incident**

Events occurred during driving that are traffic incidents.

## 12.2 Supported Linkage Actions

Currently, the platform supports following linkage actions for alarms.

**Note**

When you add linkage actions, exceptions detected by the system will be displayed and you can fix the exceptions according to the guidance on the page.

**Trigger Recording**

Select the related camera to record the alarm video (make sure the related camera(s) have been configured with the recording schedule) when the alarm is triggered.

For video events, **Triggering Recording** is set as the linkage action by default.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location (i.e., **Store in Main Storage**, **Store in Auxiliary Storage**, and **Not Store**) for storing the video files.

  **Note**

  If the camera is not configured with the main storage, you can still select the storage location as **Store in Main Storage**, but the rule exception will be prompted.
- To relate other cameras, select **Specified Camera** and click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Event Video:** You can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record the video for after the alarm stops. You can also click **Custom** to custom the time period.
- **Lock Video Files For:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the video to be displayed by default on the Control Client when receiving the triggered alarm information. You can select the recorded video or the live video to be displayed.

**Capture Picture**

Select cameras to capture pictures during the alarm, and you can view the captured pictures when checking the alarm.

- If the alarm source is a camera, you can set it to trigger the source camera itself for capturing pictures by selecting **Source Camera**.
- To trigger other cameras for capturing pictures, select **Specified Camera** and select cameras for capturing pictures.

**Capture Picture**: Specify the number of seconds to define when the camera will capture pictures for the alarm. After you set the number of seconds for pre/post-event (here the event refers to the triggering event), the camera will capture one picture at 3 time points respectively: at the configured seconds before the alarm starts, at the configured seconds after the alarm ends, and when the event is happening (as shown in the picture below).

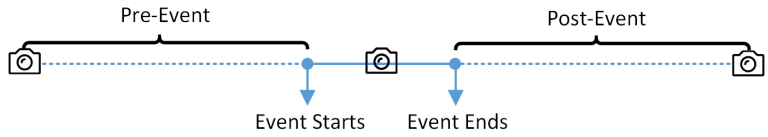



**Figure 12-1 Capture Pictures**

**Note**

The pre-event picture is captured from the camera's recorded video footage. This pre-event capture function is only supported by the camera which is set to store the video in the recording server.

**Create Tag**

Select the camera(s) to record video when the event occurs and set the storage location for storing video files. The platform will add a tag to the event-triggered video footage for convenient search.

- If the event source is a camera, to relate the source camera itself for tagged recording, select **Source Camera** and select the storage location (i.e., **Store in Main Storage**, **Store in Auxiliary Storage**, and **Not Store**) for storing the video files.

  **Note**

  If the camera is not configured with the main storage, you can still select the storage location as **Store in Main Storage**, but the rule exception will be prompted.

- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged length of the video footage. For example, you can set it to record the tagged video starting from 5 seconds before the event and lasting until 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

**Link Access Point**

You can enable this function to trigger the access points to take certain actions.

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the event occurs.

For floors, the elevators can access the floors freely, with credentials, temporarily, or the access is forbidden.

For example, you can set it to trigger all the doors remaining locked and all the floors access forbidden when the intrusion of a suspicious person is detected.

- **All Access Points**: When the alarm is triggered, the platform will trigger all the doors and floors to take certain actions.
- **Specified Access Point:** Click **Add** to select specified access points or batch locking and unlocking groups as the linkage targets. When the event occurs, the platform will trigger these doors/floors in the emergency operation groups to take certain actions.

**Link Alarm Input**

Select alarm inputs and these alarm inputs will be armed or disarmed when the event occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link to arm the alarm input B, C, and D, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects the intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules are configured), so that the security personnel will get to know where the suspect goes.

**Link Alarm Output**

Select alarm output (if available) and the external device connected can be activated when the event occurs.

**Note**

Up to 64 alarm outputs can be selected as event linkage.

**Alarm Output Closing Method**: The added alarm outputs can be closed manually, or you can set the time period after which the alarm outputs will be closed automatically.

**Trigger Audio Alarm**

Trigger audio alarms for camera sources.

**Trigger Strobe Light**

Trigger the strobe light for camera sources.

**Trigger PTZ**

Call the preset, patrol, or pattern of the selected cameras when the event occurs.

**Note**

Up to 64 PTZ linkages can be selected as event linkage.

**Link Optimus Resource**

Click **Add** to select the resources integrated from a third-party platform (via Optimus) and set the control about detailed operations that will happen when the event occurs.

**Send Email**

Select an email template to send the event information according to the defined email settings. If you have purchased the License for emergency mustering, you can select an emergency counting group of an area in the drop-down list of **Send Data of Emergency Counting Groups**. When the event occurs, the platform will send the data of the selected emergency counting group to the email in a PDF file.

**Note**

For details about setting the email template, refer to ***Set Email Template*** .

**Attach with Entry & Exit Counting**

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains information such as the number of people still in the building, their names and profile photos, phone numbers, and locations of last access.

**Trigger User-Defined Event**

Select the user-defined event(s) in the event list as the linkage action when the event occurs.

**Note**

- Up to 16 user-defined events can be selected as linkage actions.
- For setting the user-defined event, refer to ***Add User-Defined Event*** .

**Link Speaker Unit**

You can link the speaker unit to an event and set the broadcast content (audio file, custom broadcast content, or none). The linked speaker unit will play the set content when the event occurs. When you select **None** for the broadcast content, you can perform remote speaking via the Control Client.

**Link Printer**

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of a certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured on the platform so that they can get the information such as how many people are still in the building, their names and profile photos, phone numbers, and locations of last access.

For details about printer settings, refer to ***Set Printer*** .

**Apply Notice to Indoor Station**

If the source type you selected is **Alarm Input**, you can apply notice to specific indoor stations.

**Send HTTP(S) Request**

Set the HTTP(S) command, HTTP(S) link, user name, password, authentication mode (basic and digest), etc., to send the HTTP(S) request when the event occurs.

**Trigger Remaining Open for Entrance and Exit**

When the event occurs, the selected entrance(s) and exit(s) will turn to the status of remaining open so that the vehicles can enter or exit the parking lot without authentication or the allowance of guards.

**Trigger Arming/Disarming of Encoding Device**

When the event occurs, the selected encoding devices will be armed or disarmed automatically based on the settings.

**Note**

Up to 16 devices are supported.

**Link BACnet Resource**

Select BACnet resources for linkage when the event occurs.

**Link Modbus Resource**

Select Modbus resources for linkage when the event occurs.

**Link Custom Resource**

Select custom resources for linkage when the event occurs.

## 12.3 Manage Event and Alarm

You can configure parameters for event types provided by the platform to detect normal events or trigger normal alarms, or add combined alarms, generic events, and user-defined events for a wider range of applications.

### 12.3.1 Add Normal Event and Alarm

The platform provides multiple triggering event types for you to configure rules for detection or triggering alarms.

Select **Event and Alarm Configuration → Normal Event and Alarm** on the left.

Click **Add** to enter the Add Event and Alarm page

#### Basic Information

**Triggering Event**

The specific event type detected on the event source will trigger an event or alarm.

**Note**

If you select Intrusion (VCA Event) as the triggering event, you can select specific regions under a source.

**Source**

This field refers to the specific entity (such as devices, servers, etc.) which can trigger this event and alarm. You can select all or specified sources.

**Note**

- When setting a thermal-related event and alarm for thermal cameras, you can select areas, points, or lines as event and alarm sources.
- Triggering event types including **Camera**, **Alarm Input**, and **Face** in **Video** and **Camera**, **Encoding Device**, **Decoding Device**, **Recording Server**, and **Streaming Server** in **Maintenance** support selecting sources in remote sites. For different device types, the labels vary.

**Name**

After selecting the source(s), you need to name the event or alarm. You can customize a name, or click the labels below to name the event or alarm by the selected label(s). If you name the event or alarm by the selected labels, the platform will display the event/alarm name by the combination of source name and triggering event name, so that you can quickly know the location where the event/alarm occurs.

**Face Picture Library**

If the triggering event you select is **Face**, you need to select the face picture library so that the platform can compare the detected face pictures with face pictures in the library.

**Threshold**

If the triggering event you select is **Regional People Counting**, you need to set extra conditions to define the triggering event.

Currently, you can set **People Counting Above/Below Threshold** and **People Counting Above/Below Threshold (Pre-Alarm)** for the people counting group. For these two alarms, you need to set the threshold which determines whether the selected people counting groups will trigger an alarm when the detected number of people stayed less than or more than the threshold.

For example, if you set the threshold as ***"≥ 100 or ≤ 10"***, when the number of people detected in the selected people counting group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

**Min. Appeared Times to Trigger Alarm**

For the triggering events **Frequently Appeared Vehicles in All Selected Lists** and **Frequently Appeared Vehicles in One of the Selected Lists**, you need to set this threshold to define frequent appearance.

**Min. Vacant Parking Spaces to Trigger Event**

For the triggering events **Insufficient Vacant Parking Spaces for Floor**, **Insufficient Vacant Parking Spaces for Vehicle in List**, and **Insufficient Vacant Parking Spaces in Parking Lot**, you need to set this threshold to define insufficient parking spaces.

**Frequency**

For some sources and events, you can set the frequency. For example, if the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle in All Selected**

**Lists** or **Frequently Appeared Vehicle in One of the Selected Lists**, you can predefine the frequency.

For example, if you set the frequency to daily 3 times, when the devices in the source parking lot detect the license plate numbers of the vehicles in the selected vehicle list more than 3 times in one day, an alarm will be triggered.

**Vehicle List**

If you select triggering events related to vehicle recognition, you need to select vehicle lists, so that the platform will compare detected vehicles with vehicles in the selected list.

**Vehicle Type**

If the source type you selected is **Vehicle Features** and the triggering event is **Vehicle Type Matched Event**, you need to specify the vehicle type(s). When the source camera detects a vehicle the type of which matches the one(s) you selected here, a vehicle type matched alarm will be triggered.

For example, if the oil tank truck is not allowed on one road, you can set a vehicle type matched alarm for the camera mounted on this road and set the vehicle type as **Oil Tank Truck**. When the camera detects an oil tank truck, an alarm will be triggered.

**Color**

Select the color to indicate this event or alarm. You can set the color according to the emergency of this event or alarm. For example, you can set red color for the urgent alarm and set green color for the prompt event.

**Ignore Repetitive Events/Alarms**

This function is used to avoid the same event or alarm occurring frequently in a short time. You need to set the **Ignore For (Second)** which is the threshold of the recurring events or alarms.

For example, if you set **Ignore For (Second)** to 30 seconds, the events or alarms of the same type that occurred on the same camera within 30 seconds will be regarded as one event or alarm.

**Delay Alarm**

If the source type you selected is **Camera** of **Maintenance** and the triggering event is **Camera Offline**, you can enable this function and set a delay duration. During the delay duration, when the source detects the triggering event, the triggering event will not be uploaded to the platform. After this duration, if the source still detects this triggering event, the triggering event will be uploaded to the platform and trigger an alarm.

With this function, when the platform detects that the camera is offline, if the camera gets online again within the delay duration, it will not trigger a camera offline alarm. Thus the maintainers can focus on the cameras which are truly disconnected.

## Actions

The field links actions for the alarms, you can click **Add Linkage Action** to select actions.

**Note**

When you add linkage actions, exceptions detected by the system will be displayed and you can fix the exceptions according to the guidance on the page.

## Event Receiving Schedule

The field defines a time period when the event or alarm can be triggered.

**Receiving Schedule**

The source is armed for detecting or triggering events or alarms during the receiving schedule. The platform provides two types of receiving schedules:

- **Schedule Template**: Select a receiving schedule template for the event or alarm to define when the event or alarm can be detected or triggered. For customizing a template, refer to ***Configure Receiving Schedule Template*** .
- **Event Based**: Specify a user-defined event or an alarm input as the start or end of the receiving schedule. You can set the **Stop Receiving** switch to on and set the specified time to automatically stop receiving this event or alarm even if the schedule does not end.

**Note**

For example, assume that you have set event A as the start event, event B as the end event, and set the value of **Automatically Stop Receiving After** to ***60 s***. Under these conditions, when event A occurs at T1, if event B occurs within 60 s, the receiving schedule ends at the occurrence of event B (see the following figure Receiving Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Receiving Schedule 2).

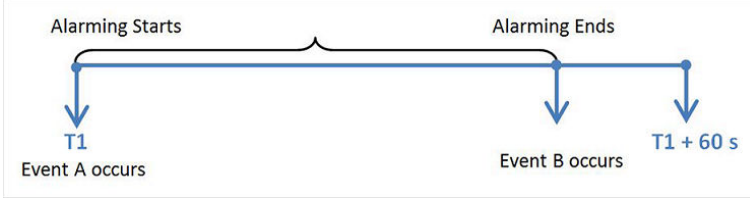



**Figure 12-2 Event Receiving Schedule 1**

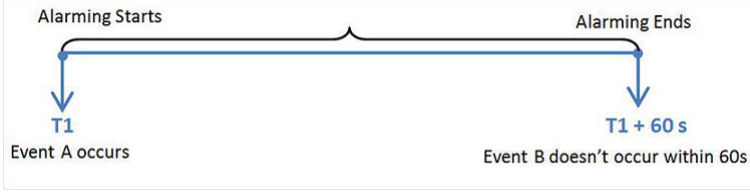



**Figure 12-3 Event Receiving Schedule 2**

When A occurs at time T1, the event or alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the event or alarm will be armed from T2 again.

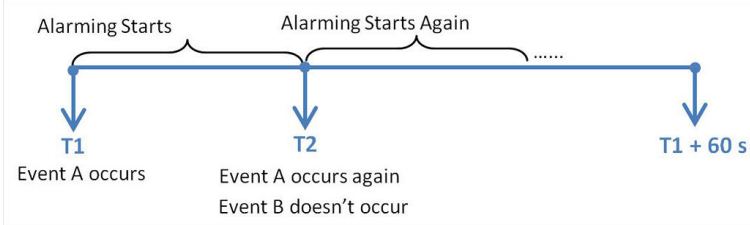



**Figure 12-4 Event Receiving Schedule 3**

## Alarm Settings

Switch on **Trigger Alarm** to trigger the configured event as an alarm. When an alarm is triggered, the map will automatically display the location of the alarm source is it is on the map, which requires no configuration.

**Alarm Priority**

The field defines the importance or urgency of this alarm. Priority can be used for filtering alarms.

**Recipients**

The field defines users who can receive the alarm notification and check the alarm details when the alarm is triggered.

Select the recipient groups or users to send the alarm information to and the recipients can receive the alarm information when they log in to HikCentral Professional via the Mobile Client.

You can select **Default Recipient**, so users set as default recipients in the user configuration will receive notifications of the alarm if they have permissions to access the selected alarm sources.

**Enable Pop-up Window**

Display the alarm window on the Control Client to show the alarm details and all the alarm-related cameras' live videos and playback when the alarm occurs.

**Trigger Emergency**

Select **Trigger Emergency** or **Turn Off Emergency**, and select the **Area for Triggering Emergency**. When the alarm is triggered by an emergency (such as a fire) in the selected area, the platform automatically switches to the **Trigger Emergency** mode or **Turn Off Emergency** mode.

**Display on Smart Wall**

Display the alarm video or the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Wall Related to Graphic Card**: Display the alarm video on the wall which adopts the graphic card of the PC that runs the Control Client to decode the video.
- **Wall Related to Decoding Device**: Display the alarm video on the wall which adopts the decoding device (namely the wall that is linked to the decoding device) to decode the video.

- **Alarm's Related Cameras**: Display the video of the alarm-related cameras on the smart wall. You can select to display the video on which smart wall and which window and set the video's stream type.
- **Public View**: A view enables you to save the window division and the correspondence between cameras and windows as the Favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the platform will display the selected public view on the specified smart wall and users can view the video of the cameras predefined in the view.
- **Smart Wall No.**: Select the No. of the smart wall window to display the alarm video.
- **Stop Displaying Alarm**: Define when the platform will stop displaying the alarm on the smart wall. The platform can stop displaying the alarm within specified seconds, or replace the original alarm when another alarm with higher alarm priority is triggered.

**Audio Alarm**

Set the voice text for playing on the PC when the alarm is triggered.

**Note**

You should set the voice engine as the alarm sound on the System Settings page of the Control Client.

**Restrict Alarm Handling Time**

Enable this function to trigger the user-defined event(s) / alarm output(s), or automatically acknowledge the alarm, or automatically forward the alarm, if the alarm is not handled within the configured alarm handling time.

**Note**

Up to 16 user-defined events and alarm outputs can be triggered when handling alarm timed out.

**Custom Alarm Receiving**

Enable this function to set and view the customized alarm receiving schedule.

## Other Operations

Click **Add** to add the event to the platform, or click **Add and Continue** to save the current settings and add another one. The added event will be listed on the Normal Event and Alarm page, and then you can perform the following operations if needed.

**Table 12-1 Other Operations**

| Operation | Description |
|---|---|
| Edit Event | Click the event name to enter the details page and edit the settings. |
| Copy to Other Events | 1. Click the event name to enter the details page.<br>2. Click **Copy To** in the top right corner of the page.<br>3. Select **Add a New Event/Alarm** to add a new event/alarm with the same settings, or **Copy Settings to Other Alarm** to copy the settings to the existing event/alarm.<br>4. Specify the settings of the source and select the target(s).<br>5. Click **OK** to copy the current event's specified parameter(s) to other added events for batch configuration. |
| Delete Events | Select events and click **Delete** to delete the selected ones. |
| Delete All Invalid Events | Click **Delete All Invalid Items** to batch delete all the invalid events. |
| Enable Events | Select an event and click **Enable → Enable** to enable the selected event, or click **Enable → Enable All** to enable all the added events. |
| Disable Events | 1. Select an event and click **Disable → Disable** , or click **Disable → Disable All** .<br>2. Set the time when the event(s) start being disabled and the duration of how long the event(s) will be disabled for.<br>3. (Optional) Enter the reason for disabling the event(s).<br>4. (Optional) Check **Disable Device Alarm** to change the alarm status of the device(s) displayed in the event list.<br>5. Click **OK** to disable the selected event(s) or all the events. |
| Test Events | Select the event(s) and click **Test** to manually trigger the event(s) for testing if the linkage actions work properly. |
| Batch Settings | Check multiple event/alarm rules, click **Batch Set** to batch set the linkage actions (for both events and alarms) and alarm recipients (for alarms only).<br>**Actions**<br>For different triggering conditions, set the same linkage actions.<br>**Alarm Recipients**<br>For different alarms, set the same alarm recipients. |

### 12.3.2 Add Combined Alarm

For some complicated scenarios, the alarm should be triggered when multiple events or alarms are detected or triggered. For example, the platform detects intrusion in area B, then the arming of area A starts. After that, if the platform detects intrusion in area A, then an alarm will be triggered to notify the security personnel.

**Steps**

1. On the left of the Event and Alarm module, select **Event and Alarm Configuration → Combined Alarm** .
2. Click **Add Combined Alarm** to open the Add Combined Alarm pane.

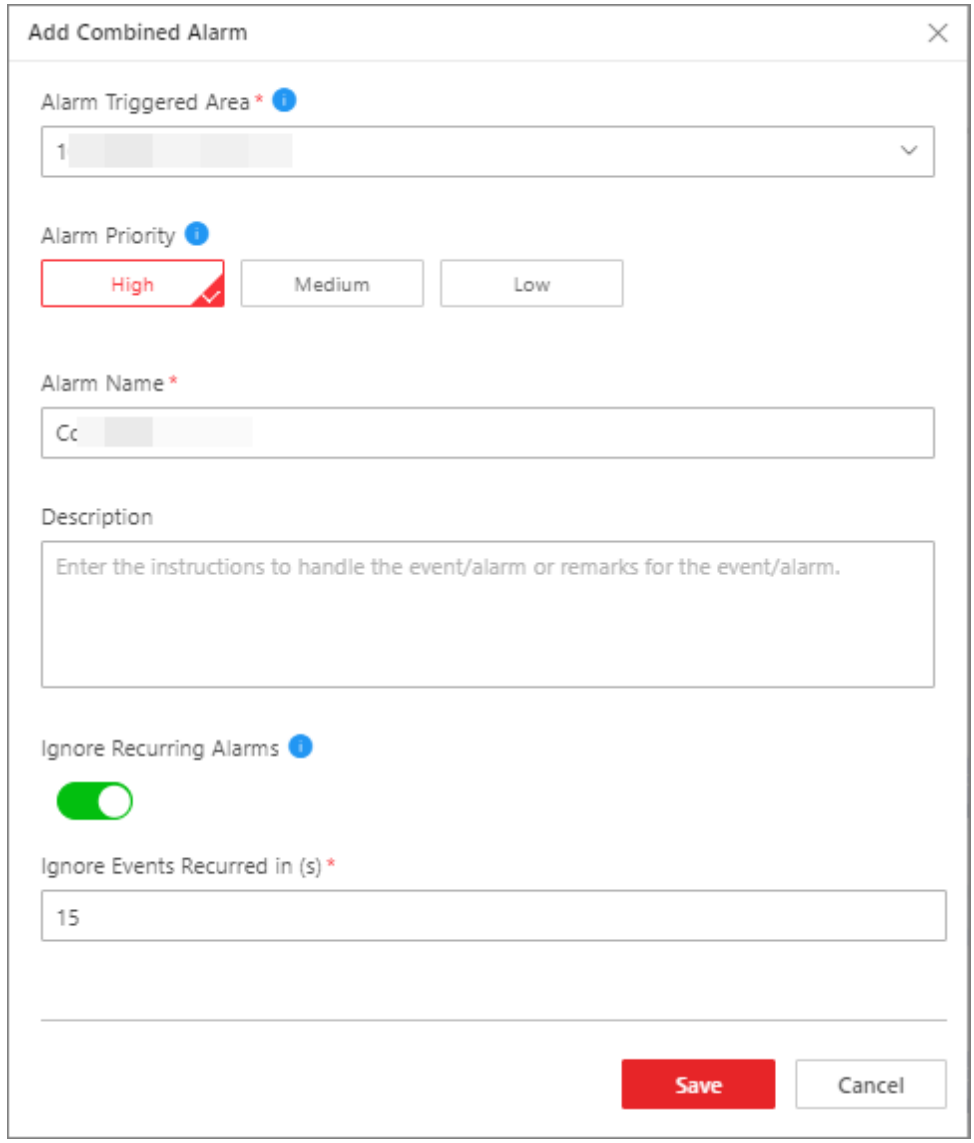



**Figure 12-5 Add Combined Alarm**

3. Set parameters on the page.

**Alarm Triggered Area**

Select the area where the combined alarm will be triggered.

**Alarm Priority**

The priority including low, medium, high, and custom level, which indicates the urgent degree of the combined alarm.

**Alarm Name**

Create a name for the combined alarm.

**Description**

Describe the combined alarm according to your requirements.

**Ignore Repetitive Events/Alarms**

Once it is enabled, the platform will ignore the combined alarm recurred within the configured time period.

4. Click **Save** to enter the configuration page.
5. Configure a receiving schedule for the combined alarm.
   1) Click on the configuration page to open the Select Schedule Template pane.
   2) Select a schedule template as **All-Day Template**, **Weekday Template**, **Weekend Template**, or a custom template.

   **Note**

   For how to customize a schedule template, refer to ***Configure Receiving Schedule Template*** .
   3) Click **Save**.
6. Configure conditions for triggering the combined alarm.
   1) Click at the right of the Receiving Schedule card to open the Select Alarm Triggering Scene pane.

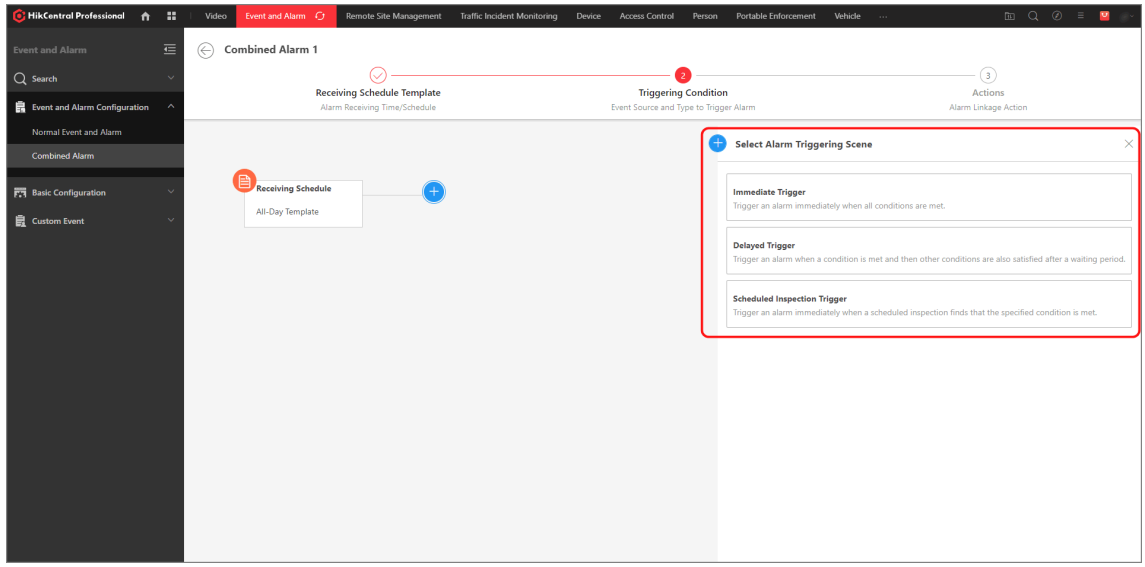



**Figure 12-6 Alarm Triggering Scene**

2) Select a triggering scene based on your needs.

**Table 12-2 Alarm Triggering Scene**

| Alarm Triggering Scene | Description |
|---|---|
| **Immediate Trigger** | Immediately trigger an alarm when all conditions are met. |
| **Delayed Trigger** | Trigger an alarm when a condition is met and then other conditions are also satisfied after a waiting period. |
| **Scheduled Inspection Trigger** | Trigger an alarm immediately when a scheduled inspection finds that the specified condition is met. |

3) For **Immediate Trigger** and **Scheduled Inspection Trigger**, select a triggering logic to continue.
For **Delayed Trigger**, this step is not needed.

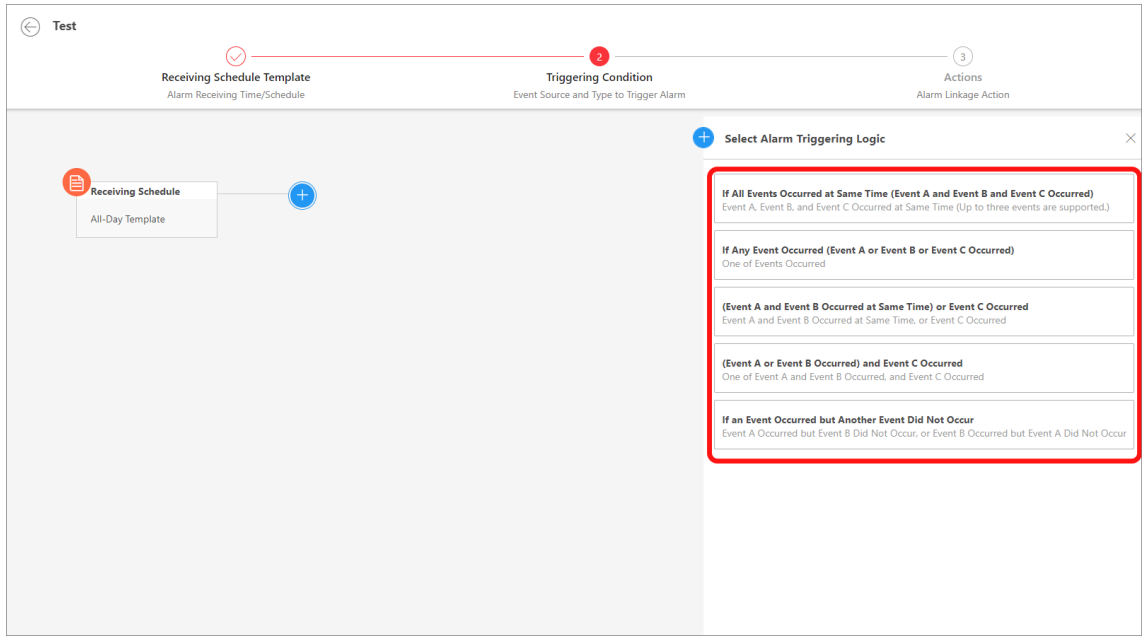



**Figure 12-7 Alarm Triggering Logic**

4) Click ⊕ on the condition card to open the Select Event Source and Event Type pane.
5) Select a triggering event and a source, and click **Save**.

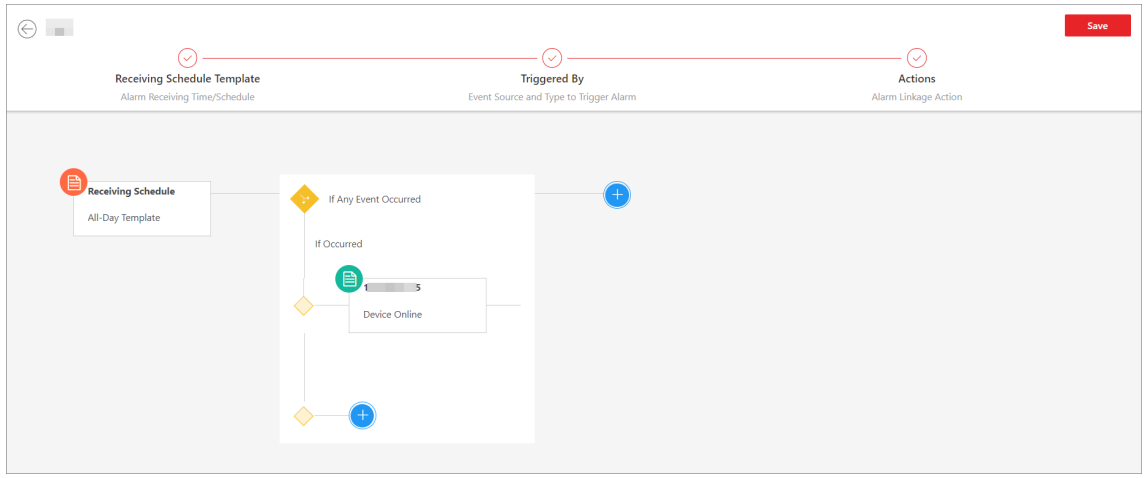



**Figure 12-8 Condition Card**

6) **Optional:** Click ⊕ below the newly added event source and type card to select more event sources and types.
7) **Optional:** Click ⚙ on the event source and type card to enter the remote configuration page of the event source. For details about remote configuration, refer to the user manual of the corresponding device.

**7.** Configure the alarm recipient(s) and linkage action(s) for the combined alarm.
1) Click ⊕ at the right of the triggering logic card to open the Select Alarm Linkage Action panel.

2) Click **Alarm Recipients** and select the recipient(s).

**Note**

If **Automatically Receive Alarm** is enabled for some users (refer to ***Add a Normal User*** for details), the Alarm Recipients card will be automatically generated after the event source and type is configured, and these users will be selected as recipients. You can click the generated card to edit the alarm recipients, but the selected users cannot be unselected.

3) Click **Save**.

4) Click ⊕ below the Alarm Recipients card to select a linkage action and set the corresponding parameters.

5) **Optional:** Click ⊕ below the Alarm Recipients card to add more linkage actions.

8. **Optional:** Click the icon on the top left of each card to reselect the content.

9. **Optional:** Move the cursor on each card and click 🗑 appeared on the top right of the card to delete the card.

**Note**

If the card is deleted, the following cards or sub cards (if any) will also be deleted.

10. Click **Save** in the top right corner of the combined alarm configuration page to add the combined alarm to the platform.

**Note**

If the alarm recipients are not configured for this combined alarm, you cannot save the combined alarm.

11. **Optional:** Perform the following operations according to your requirements.

| | |
|---|---|
| **Copy Parameters to Existing Alarm** | Click **Copy**, and select **Add Combined Alarm** to copy the current rule to other resources, or select **Copy Settings to Other Alarm** to copy selected settings (such as basic information, actions, receiving schedule, receiving mode) to the target. |
| **Delete Alarm** | Click **Delete** to delete this alarm. |
| **Test** | Click **Test** to trigger this alarm manually, and you can check whether the linkage actions take effect and whether the recipients can receive the notification. |
| **Enable/Disable** | Switch on the button beside **Status** to enable or disable this alarm. After the alarm is enabled, it can be received by the platform. If you disable this alarm, you will be required to set the start time and duration of disabling and the platform cannot receive the alarm in the duration. |

### 12.3.3 Add Generic Event

A generic event is a signal transferred in the form of TCP/UDP/HTTP/HTTPS data package from the resource (e.g., external systems and devices) if something occurred and matched the configured expression. In this way, you can easily integrate the platform with a very wide range of external sources, such as access control systems and alarm systems.

**Steps**

1. Select **Custom Event → Generic Event** on the left.
2. Click **Add** to enter the Add Generic Event page.

**Note**

You can also click **Import** to batch import the events by the template.

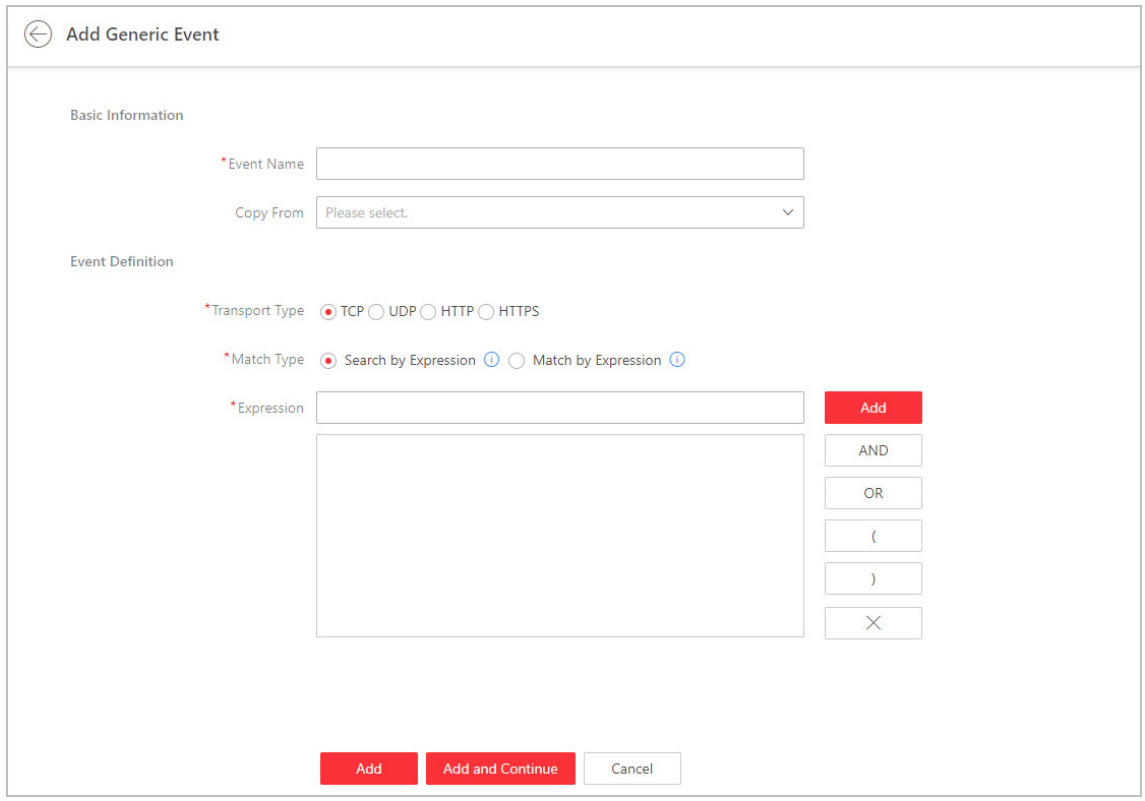



**Figure 12-9 Add Generic Event Page**

3. Set a name for the event.
4. **Optional:** Copy the settings from other generic events in the **Copy from** field.
5. Select **TCP**, **UDP**, **HTTP**, or **HTTPS** as the transport protocol.
6. Select the match type to define what received data packages can trigger events.

   **Search by Expression**

The received package must contain the text defined by the expression or more. For example, if you have defined the expression as 'Motion' AND 'Line Crossing', the event can be detected when the received package contains "Motion", "Intrusion", and "Line Crossing".

**Match by Expression**

The text in the received package must be exactly the same as that defined by the expression.

**Search by Keyword**

The received package must contain the keywords.

**7.** Define the expression for analyzing the received package.

1) Enter the term which should be contained in the expression in the text field.
2) Click **Add** to add the term to the expression.
3) Click the parenthesis or operator button to add it to the expression.
4) **Optional:** Click ✕ to remove the item at the left of the cursor from the expression.

**Note**

You can position the cursor inside the expression in order to determine where a new item should be included or where an item should be removed.

The parenthesis or operator buttons are described in the following:

**AND**

You specify that the terms on both sides of the AND operator must be included.

For example, if you define the rule as 'Motion' AND 'Line Crossing' AND 'Intrusion', the term Motion, and Line Crossing as well as the term Intrusion must be all contained in the received package for the conditions to be met.

**Note**

In generally, the more terms you combine with AND, the fewer events will be detected.

**OR**

You specify that any term should be contained.

For example, if you define the rule as 'Motion' OR 'Line Crossing' OR 'Intrusion', any of the terms (Motion, Line Crossing, or Intrusion) must be contained in the received package for the conditions to be met.

**Note**

In generally, the more terms you combine with OR, the more events will be detected.

**(**

Add the left parenthesis to the rule. Parentheses can be used to ensure that related terms are processed together as a unit; in other words, they can be used to force a certain processing order in the analysis.

For example, if you define the rule as ('Motion' OR 'Line Crossing') AND 'Intrusion', the two terms inside the parentheses will be processed first, then the result will be combined with

the last part of the rule. In other words, the system will first search any packages containing either of the terms Motion or Line Crossing, then it searches the results to look for the packages that contain the term Intrusion.

**)**

Add the right parenthesis to the rule.

8. Click **Add** to add the event and back to the event list page, or click **Add and Continue** to add the event and continue to add a new event.
9. **Optional:** Perform the following operations after adding the event.

| | |
|---|---|
| **Edit Event Settings** | Click the name in the Event Name column to edit the corresponding event settings. |
| **Receive Generic Event** | Select the events, click **Receive Generic Event** to open the settings pane, and check the checkboxes to enable receiving the generic events via different protocols. |
| **Import/Export Events** | Select the events, and click **Import/Export**. |

### 12.3.4 Add User-Defined Event

When you are viewing videos or checking the alarm information, if there is some information that needs to be paid attention to, you can manually define a new event type which is not in the provided event and alarm list or the defined generic events for triggering an alarm or being configured as a linkage action of alarms. This kind of event is called as the user-defined event.

**Steps**

1. Select **Custom Event → User-Defined Event** on the left.
2. Click **Add**.

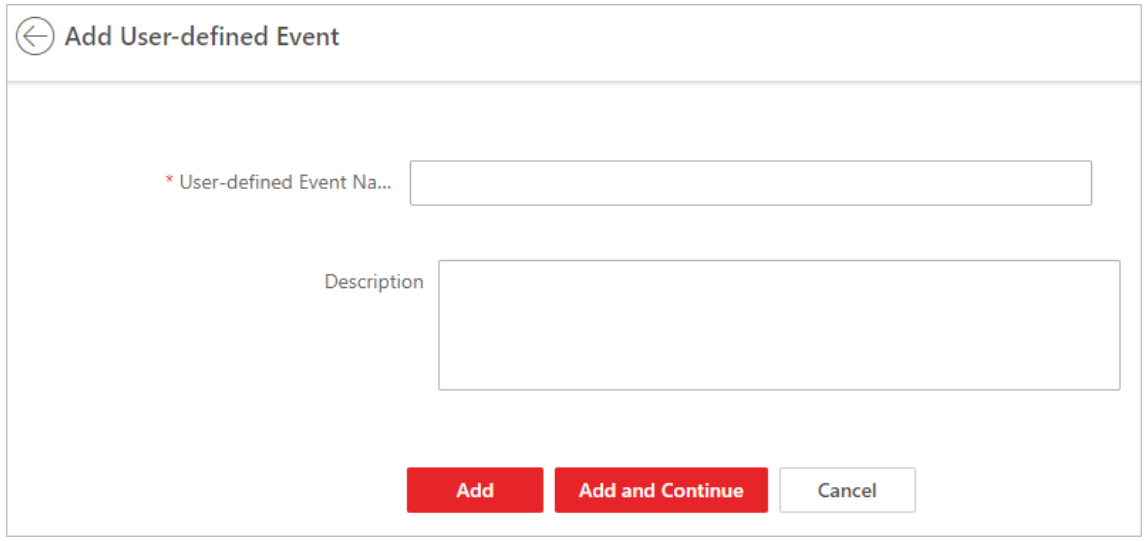



**Figure 12-10 Add User-Defined Event**

3. Create a name for the event.
4. **Optional:** Enter the information to describe the event.
5. Click **Add** to add the event and go back to the event list page, or click **Add and Continue** to add the event and continue to add a new one.

   With the customized user-defined event, the platform provides the following functions:

   - Integrate other third-party systems with HikCentral Professional by using the data received from the third-party system. The user-defined events can be triggered as an alarm outside the HikCentral Professional. For details, contact our technical support.

### 12.3.5 Add Text Warning Event

Describe a triggering condition to customize an event. Simulation test is supported.

**Steps**

1. Select **Event and Alarm → Custom Event → Text Warning Event** on the left.
2. Click **Add**.

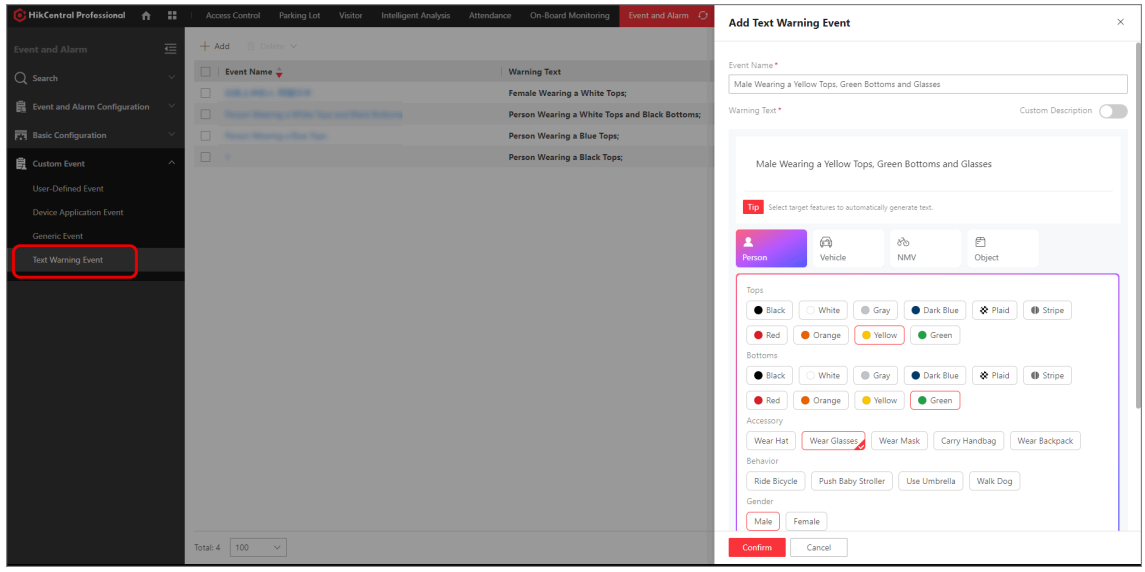



**Figure 12-11 Add Text Warning Event**

3. Create a name for the event.
4. Set the warning text via either of the following ways.

   **Select Feature Labels** Select target features to automatically generate text.

   **Custom Description** Turn on **Custom Description**. Select an existing term, or enter a custom one like "A Young Man in Red Long-Sleeved Tops".
5. **Optional:** Click **Show Advanced Settings**. Set the **Auxiliary Warning Text**, **Filtered Text**, and **Alarm Threshold** as needed.

   **Auxiliary Warning Text**

   Add more texts to describe the target more accurately for better arming effects.

   **Filtered Text**

   Describe the features that do not match the event to reduce false alarms.

   **Alarm Threshold**

   Threshold for triggering an alarm based on the matching accuracy percent. An alarm will be triggered when the matching accuracy percent is above the threshold.
6. Click **Confirm** to add the event and go back to the event list page.
7. **Optional:** Perform **Simulation Test**.

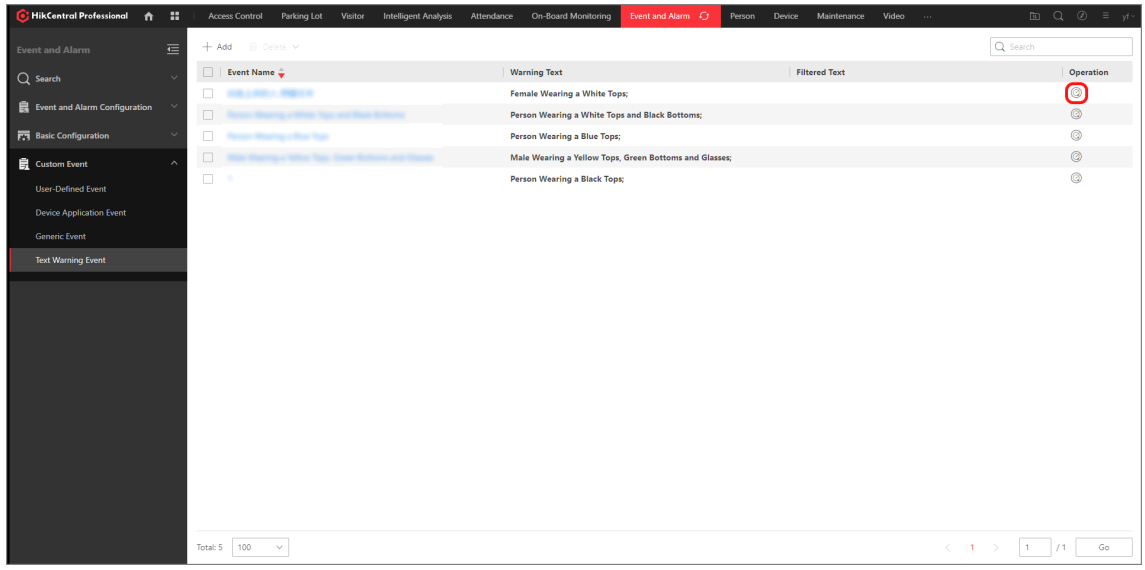



**Figure 12-12 Simulation Icon**

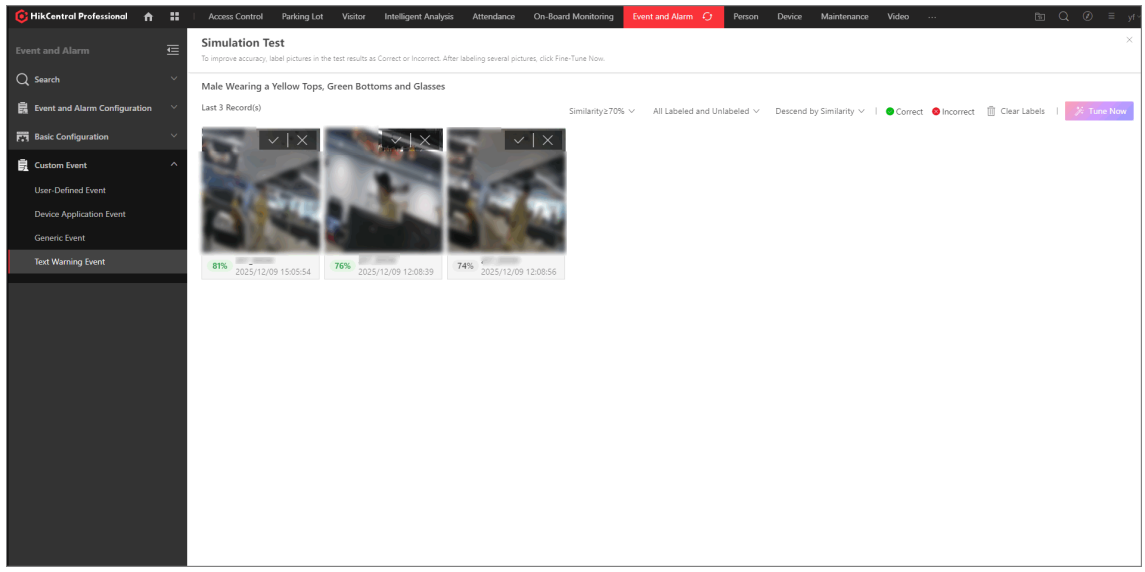



**Figure 12-13 Simulation Page**

## 12.4 Set Basic Event and Alarm Parameters

After setting basic parameters for events and alarms, you can set receiving schedules, and recipient groups or specific recipients who can receive events and alarms in specific timeout period, and you can send events/alarms reports regularly via email to the recipients / recipient groups. You can also define alarm priorities, alarm categories, and alarm icons to meet the actual requirements.

## 12.4.1 Configure Receiving Schedule Template

When adding events and alarms, you can select the predefined receiving schedule template to define when the event and alarm can be triggered and notifying the recipients. The platform has predefined three default receiving schedule templates: All-Day Template, Weekday Template, and Weekend Template. You can also customize a template according to actual needs.

**Steps**

**Note**

Receiving schedule template defines the time when you can receive events or alarms. If the event schedule differs from the alarm receiving schedule, make sure the time of the event receiving schedule covers that of the alarm receiving schedule.

1. Select **Basic Configuration → Receiving Schedule Template** on the left.
2. Click + to enter the Add Receiving Schedule Template page.

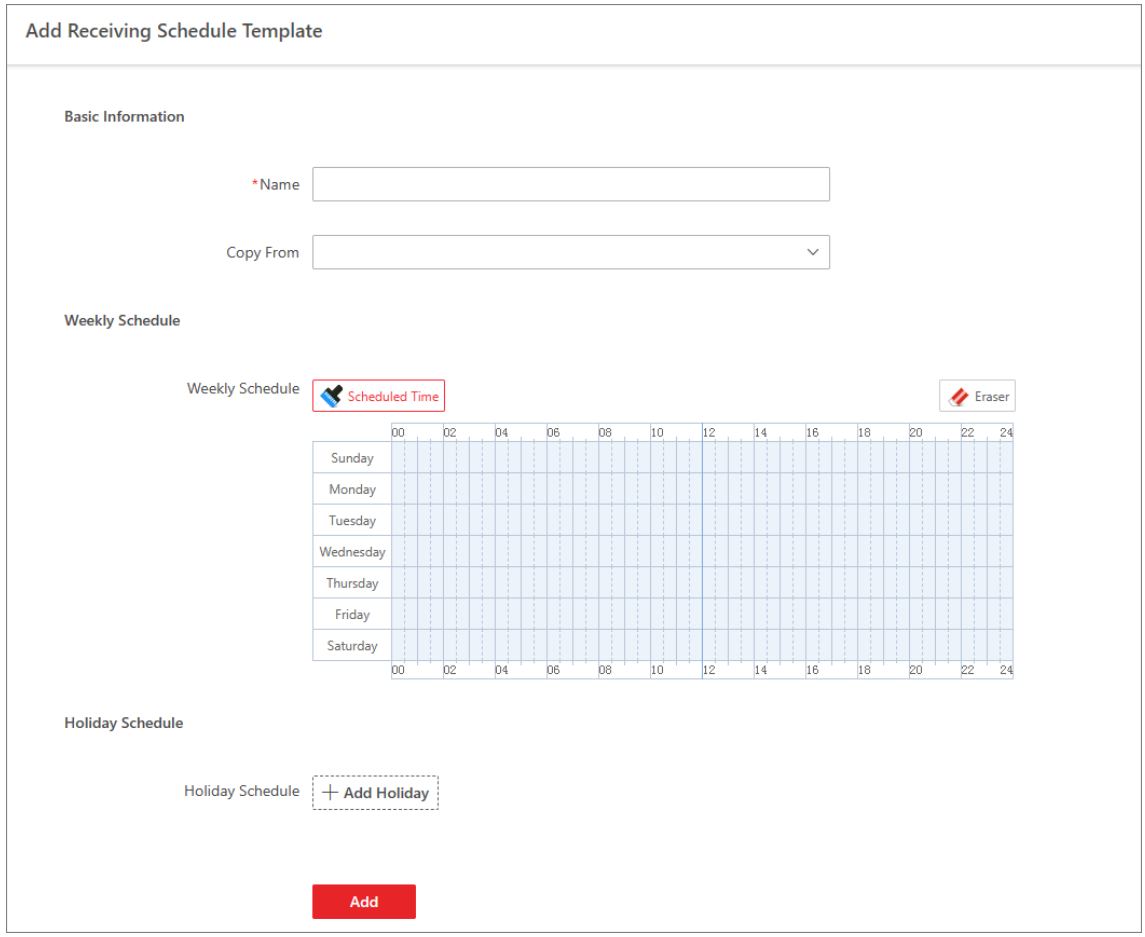



**Figure 12-14 Add Receiving Schedule Template**

3. Enter a name for the template.

4. **Optional:** Select another defined template to copy the settings to the current template.
5. Click **Scheduled Time** and drag on the time bar to set time periods during which the event can be triggered on the event source and notified the recipients.

**Note**

- Up to 4 time periods can be set for each day.
- On the schedule time table, you can click to set the specific time period which accurate to minute.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
7. **Optional:** Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.
8. Click **Add** to add the template.

   The receiving schedule template will be displayed on the receiving schedule template list.
9. **Optional:** Perform the following operations after adding the receiving schedule template.

| | |
|---|---|
| **View Template Details** | Click the template name to view its details. |
| **Edit Template** | Click the name of a custom template to edit template details.<br>**Note**<br>The predefined templates cannot be edited. |
| **Delete Template** | Select a template and click to delete the template.<br>**Note**<br>• The predefined templates cannot be edited.<br>• If there are events/alarms configured with this template, you can replace the template with other receiving schedule. Or you can click **Delete Now** to delete the template, and this operation will cause exceptions of related events/alarms. |

## 12.4.2 Custom Alarm Settings

The platform has predefined several alarm priorities, alarm categories, color template, and alarm icons for basic needs. You can edit the predefined alarm priority and alarm category, and customize alarm priority and alarm category according to actual needs.

**Steps**

**Note**

**Alarm Priority**

Define the importance or urgency of alarms for handling or acknowledgment.

**Alarm Category**

Used when the user acknowledges the alarm and categories what kind of alarm it is, e,g., false alarm, or alarm to be verified. You can search for alarms by the alarm category.

**Alarm Icon When Alarm Occurs**

The platform has predefined some icons of resources for several special alarms.
For example, it predefined the icon for the Door Opened Abnormally alarm. When this alarm is triggered, the door icon will turn to the icon displayed here to notify users.

1. Select **Basic Configuration → Alarm Custom Settings** on the left.
2. Customize alarm priorities according to actual needs. By default, three kinds of alarm priority exist.

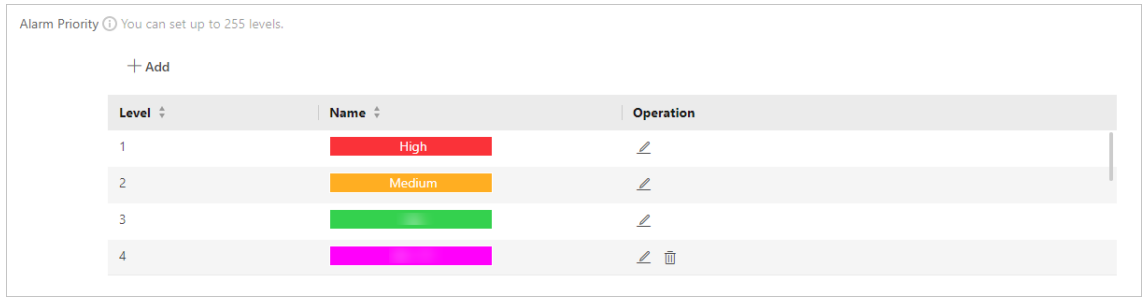



**Figure 12-15 Alarm Priority**

1) Click **Add** to open the adding alarm priority pane.

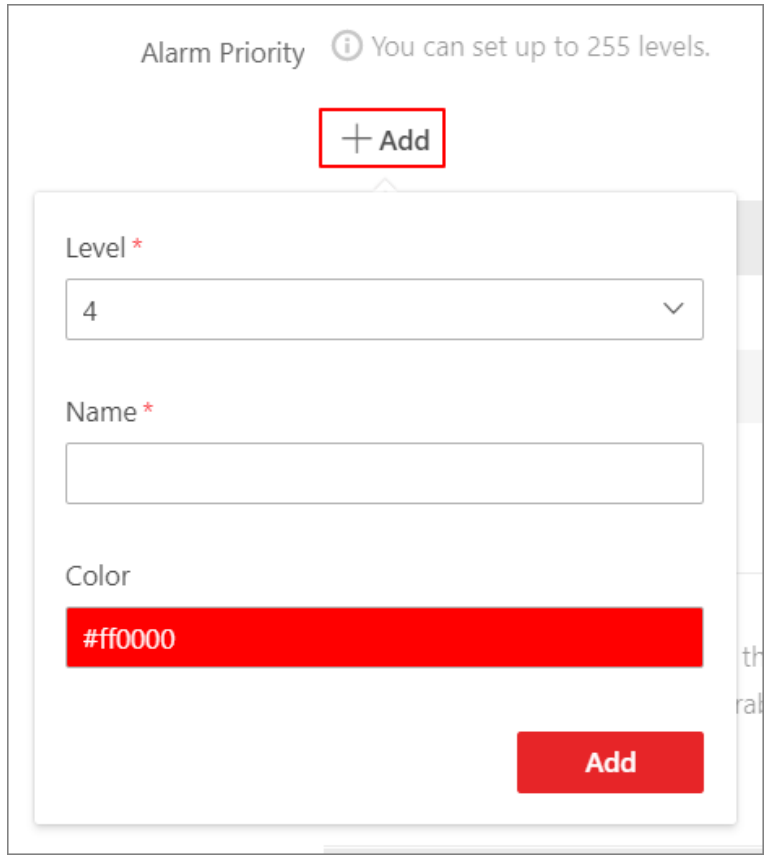



**Figure 12-16 Add Alarm Priority**

2) Select a level No. for the priority.
3) Enter a descriptive name for the priority.
4) Select the color for the priority.
5) Click **Add**.

The priority will be displayed on the alarm priority list.

**3.** Customize alarm categories according to actual needs. By default, four alarm categories exist.

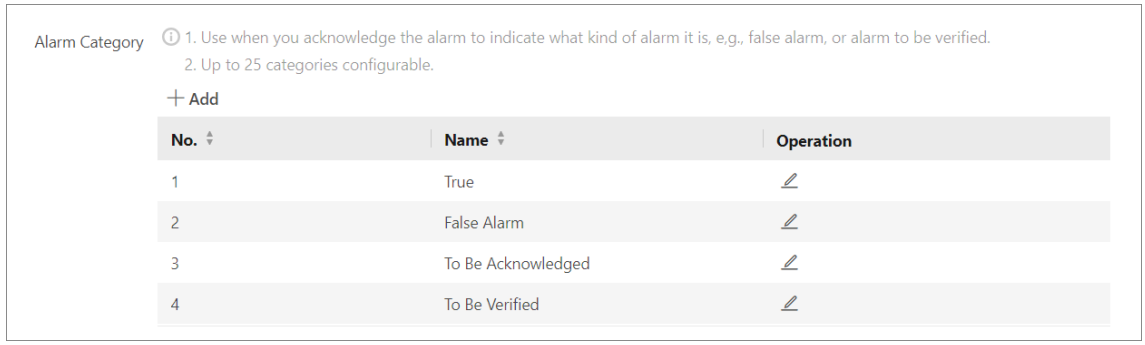



**Figure 12-17 Alarm Category**

1) Click **Add** to open the adding alarm category pane.

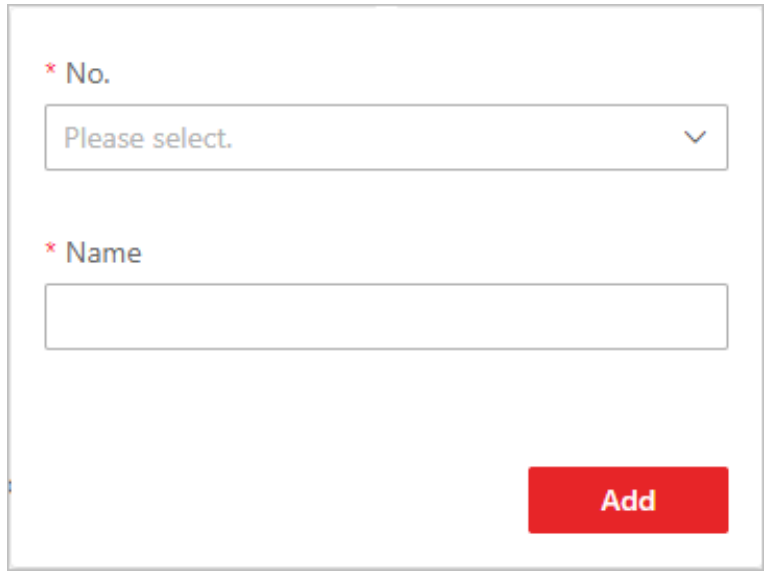



**Figure 12-18 Add Alarm Category**

2) Select a No. for the alarm category.
3) Enter a descriptive name for the alarm category.
4) Click **Add**.

The alarm category will be displayed on the alarm category list.

**4.** Customize color template according to actual needs. By default, three alarm categories exist.

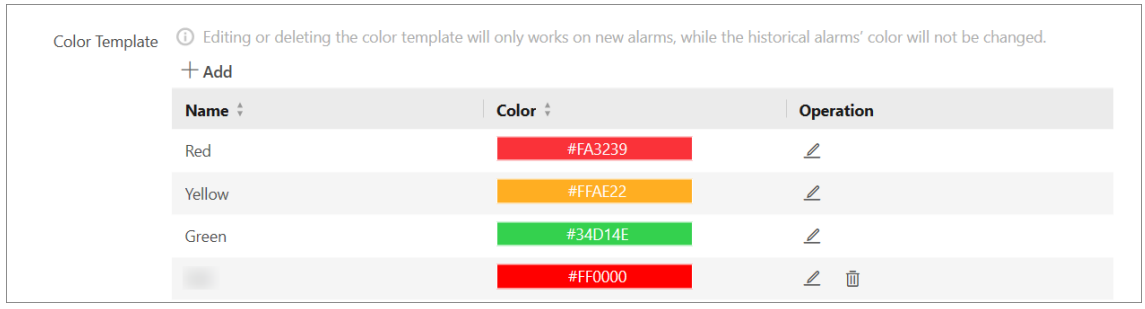



**Figure 12-19 Color Template**

1) Click **Add** to open the adding color template pane.

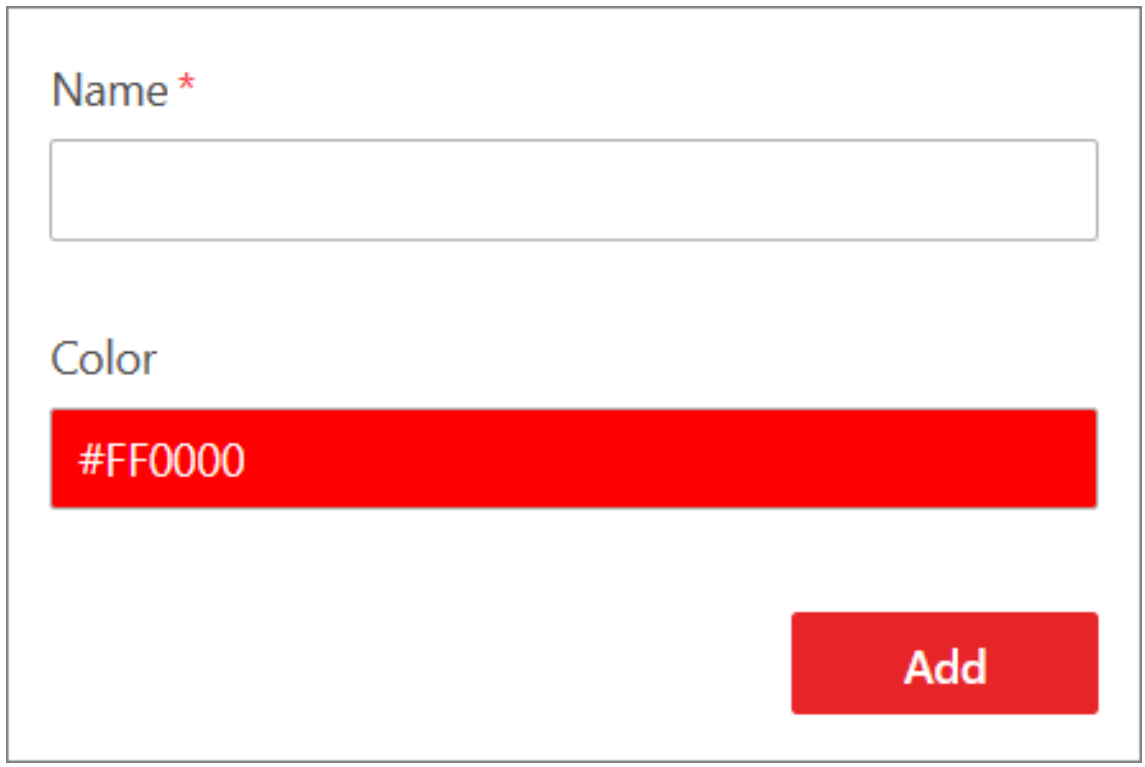



**Figure 12-20 Add Color Template**

2) Enter the name of the color template.
3) Select a color.
4) Click **Add**

The alarm category will be displayed on the alarm category list.

5. In the Alarm Icon When Alarm Occurs field, view the alarm icons provided by the platform which are used to notify the users that the alarm is triggered.

**Note**

These predefined alarm icons cannot be edited and deleted.

6. **Optional:** Perform the following operation(s) after adding alarm priority and category.

**Edit** Click to edit the alarm priority and category.

**Note**

You cannot edit the No. of predefined alarm priorities and categories.

**Delete** Click to delete the alarm priority and category.

**Note**

You cannot delete the predefined alarm priorities and categories.

### 12.4.3 Configure Alarm Receiving Settings

You can manage alarm recipients in groups to quickly set recipients for different categories of alarms, and set default alarm recipients who can receive all the alarms triggered by resources they have access permissions, so that you do not have to select recipients for each single alarm. You can also set the timeout period of acknowledging alarms for filtering alarms on the Control Client and upload historical alarms to the Control Client.

**Steps**

1. Select **Basic Configuration → Alarm Receiving Configuration** on the left.
2. In the Alarm Recipient Group field, click + above the group list to open the adding alarm recipient group pane.
3. Enter a name for the group and click **Add**.

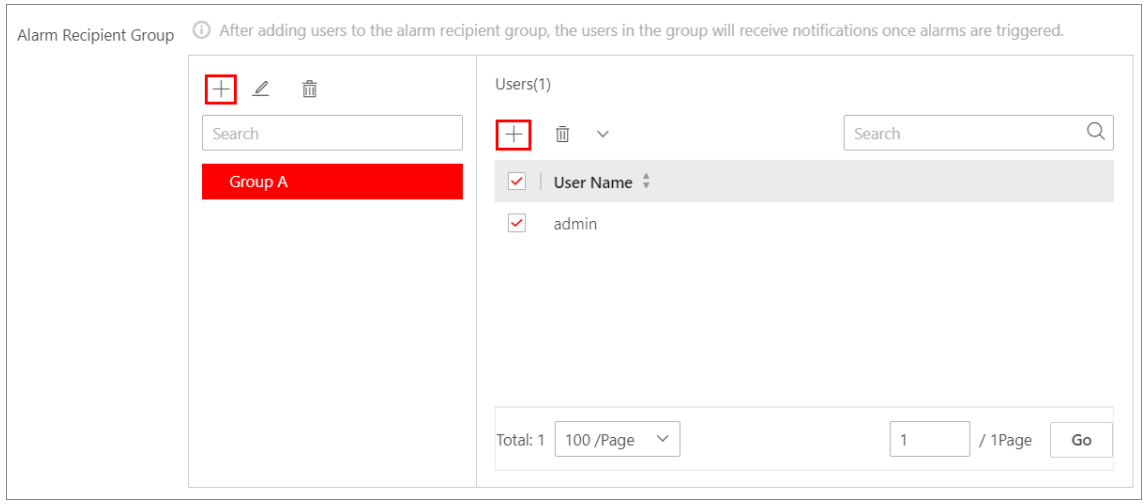



**Figure 12-21 Alarm Recipient Group Field**

4. Select an alarm recipient group and click + in the Users field to add user(s) to the group.
5. **Optional:** Check user(s) in the group and click to remove the selected user(s) from the group or click → **Delete All** to remove all the users from the group.
6. Check user(s) in the Recipient field as the default alarm recipient(s).

   The default alarm recipients will be automatically selected when setting recipients for alarms, and they cannot be deselected.
7. **Optional:** Switch on **Acknowledging Time Limitation** and set the timeout period for enable filtering timeout alarms on the Control Client.

   **Note**

   You can click **Custom** on the drop-down list to custom time out period.
8. **Optional:** Check **Upload Historical Alarm** to enable uploading the historical alarms to the Control Client.
9. Click **Save**.

The configured alarm recipient group(s) will appear on the Add Event and Alarm page and they can be selected when setting recipients for alarms.

### 12.4.4 Send Event and Alarm Report Regularly

You can set a scheduled report rule for specified events or alarms, and the platform can send an email with a report attached to the target recipients by day or week, showing the details of specified events or alarms triggered on the day or the week.

**Before You Start**

- Set the email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

**Steps**

**Note**

One report can contain up to 10,000 event records in total.

1. Select **Basic Configuration → Scheduled Report** on the left.
2. Click **Add** if there is no scheduled report rule or click + above the rule list to enter the Create Report page.
3. Set the basic information.

   **Report Name**

   Create a name for the report.

   **Format**

   Select **Excel** or **PDF** as the report format and select a language for report contents.

   **Note**

   You can skip this step if you want to keep the default settings.

   **Report Language**

   Select the report language.
4. In the Report Content field, select **Event Alarm Rule** or **Area** as the statistics dimension, and click **Add** to select statistical objects to be contained in the report.

   **Note**

   Up to 32 events and alarms can be added in one report.
5. Set the report sending rule and time.

   **Statistical Cycle**

   **By Day**

If the statistics cycle is selected as **By Day**, the report shows data on a daily basis. The platform will send a report at the sending time on the selected day(s) of the week, which contains information of the events triggered on the day (24 hours) before the sending date.

For example, if you select **Monday**, **Tuesday**, and **Friday** in the Send On failed, and set the sending time as 18:00, the platform will send a report at 18:00 on every Monday, Tuesday, and Friday, containing details of all the events triggered between 00:00 and 24:00 on every Sunday, Monday, and Thursday.

**By Week**

If the statistics cycle is selected as **By Week**, the report shows data on a weekly basis, which may be less time-consuming. The platform will send a report at the sending time on the selected day of the week, which contains information of events and alarms triggered on the recent 7 days or recent 14 days before the sending date.

For example, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing details of all the events triggered between last Monday and Sunday.

**Report Time**

Select the specific report time.

**Send On**

Select the date of a week for sending the report. You can click **Select All** to set all dates of a week.

**Send At**

Select the time of a day for sending the report.

**Effective Period**

Set an effective period for the report to improve the data security.

6. Set advanced parameters.

**Send via Email**

If it is enabled, you can select an email template from the drop-down list to define the recipient information and email format.

**Note**

You can click **Add New** to add a new email template. For setting the email template, refer to ***Email Settings*** .

**Upload to SFTP**

If it is enabled, the platform will automatically upload and save reports to the FTP server.

**Save to Local Storage**

If it is enabled, the platform will automatically upload and save reports to the local storage.

**Save to File Management**

If it is enabled, the platform will automatically upload and save reports to the Evidence Management Center. You can set the file tag and file description for the scheduled reports. For details, refer to ***Evidence Management*** .

**Note**

You can click **Configure** or click → **SFTP Settings / Configure Local Storage** to log in to the SFTP server by entering the IP address, port, user name, and password, and set the saving path on the SFTP server or local storage for reports.

7. Click **Save** to add the report rule.

## 12.5 Event and Alarm Search

The platform provides the statistics and analysis results of historical events and alarms for you to have an overview and further applications. You can also search for historical events and alarms by setting different conditions to view the details as required.

### 12.5.1 Event and Alarm Overview

In the event and alarm overview module, it gives you an overview of the event or alarm distribution, top 5 event types or alarm categories, and top 5 event or alarm areas.

In the top left corner of the Home page, select → **Security Monitoring** → **Event and Alarm** .

Select **Search** → **Overview** on the left.




**Figure 12-22 Event and Alarm Analysis**

| Module | Description |
|---|---|
| 1 | • Daily Trend: The numbers of events or alarms in the last 7 days or last 30 days are displayed in the vertical bar chart.<br>• Hourly Trend: The numbers of events or alarms of 24 hours for the last 7 days, the last 30 days, or the custom period are displayed in the line chart. |
| 2 | The data of top 5 event types or alarm categories triggered in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart. You can click the red number of an item to jump to the Event and Alarm Search page. |
| 3 | The data of the top 5 event or alarm areas in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart. |

You can click **Settings** in the upper-right corner to customize event types or alarm categories to be calculated on the overview page.

**Note**

The information displayed in each area will change according to the report target on the Settings pane. For example, if you select **Alarm** on the Settings pane as the report target, the upper area will only display the number of alarms, the lower-left area will only display the data of top 5 alarm categories, and the lower-right area will only display the data of top 5 alarm areas.

## 12.5.2 Search for Event and Alarm Logs

You can search for event and alarm log files of the added resource by setting different conditions.

**Before You Start**

Make sure you have configured events and alarms first. See ***Add Normal Event and Alarm*** for details.

**Steps**

1. Select **Search → Event and Alarm Search** .
2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom** and specify the start time and end time for search.
3. In the field of **Trigger Alarm**, select the event status (whether the event is triggered as the alarm).

   **All**

   Both events and alarms.

   **Disabled**

   The events happened but were not triggered as alarms.

**Enabled**

The events happened and were triggered as alarms. If you select this, you can set conditions for filtering alarms by marking status, acknowledging status, alarm priority, or alarm category.

4. Switch **Area** on and then click to select the area of the event or alarm source.
5. Switch **Triggering Condition** on and then click to select the triggering events and source from the current site or remote sites.

**Note**

- The remote site is only available for the Central System with Remote Site Management module (based on the License you purchased).
- If you select triggering events in the Access Control category, enter the entered/exited person's name.
- If you select triggering events in the Third-Party Resource Integration category and have entered the additional information about the alarm on the third-party system, enter the additional information.

6. Switch **Event/Alarm Name** on to select the event/alarm name in the drop-down list.
7. Click **Search**.

The matched event or alarm logs will be listed on the right page.

8. **Optional:** Check the alarms, and click **Acknowledge** to batch acknowledge those unacknowledged alarms.

**Note**

Only unacknowledged alarms (not events) support this feature.

9. **Optional:** Click **Export** and select the format as **Excel** or **PDF** to save all searched events and alarms to the local PC.

**Note**

When exporting all events and alarms in Excel format, you can check **Include Picture Information** to export the related pictures.

## 12.5.3 View Device Application Events

You can view and search for event and alarm log files uploaded by the added resources which contain HEOP or AIOP application.

**Note**

Make sure you have configured HEOP or AIOP events and alarms first. See ***Add Normal Event and Alarm*** for details.

Select **Custom Event → Device Application Event** on the left.

You can view the event list including event name, original event name, event type, and description. You can also enter the keywords to search for specific device application events.

You can click the event name to view the event details and edit the event name.

**Note**

Only the name of AIOP events are supported to be edited.

# Chapter 13 Third-Party Integration Settings

The Third-Party Integration module provides options to integrate via Optimus, OpenAPI Gateway, SIA Gateway, BACnet Gateway, Sur-gard Gateway, and ONVIF Gateway; configure SIA and BACnet device drivers; interchange data; and set up a WhatsApp merchant account.

On the left navigation bar of the System page, select **Third-Party Integration** to display the third-party integration settings menu.

To achieve granular permission control for third-party integration, you can go to the Account and Security module to create a dedicated role with specific permissions (view/edit) and assign it to users.

## 13.1 Integrate via Optimus

The platform supports integrating third-party resources via Optimus.

Select **Optimus Integration** on the left navigation bar and switch on **Integrate via Optimus**.

**Note**

- Only admin/administrator users have the permission to perform this function.
- For details about configuring the related parameters in Optimus, refer to the corresponding user manual.

The default icons of resources integrated from the third-party will be displayed. Hover the cursor over the default icon and click to change the resource icons according to your need.

Click **Save**.

## 13.2 Integrate via OpenAPI Gateway

The platform provides the OpenAPI gateway for the third-party system integration. By the provided open APIs (Application Programming Interfaces), the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

**Note**

- The gateway should be deployed on the same network with SYS.
- For open APIs provided by the platform, refer to *HikCentral Professional OpenAPI Developer Guide*, which can be obtained in folder ***..\OpenAPI\Document*** under the installation path.

Select **OpenAPI Gateway** on the left navigation bar, switch on **Open API**.

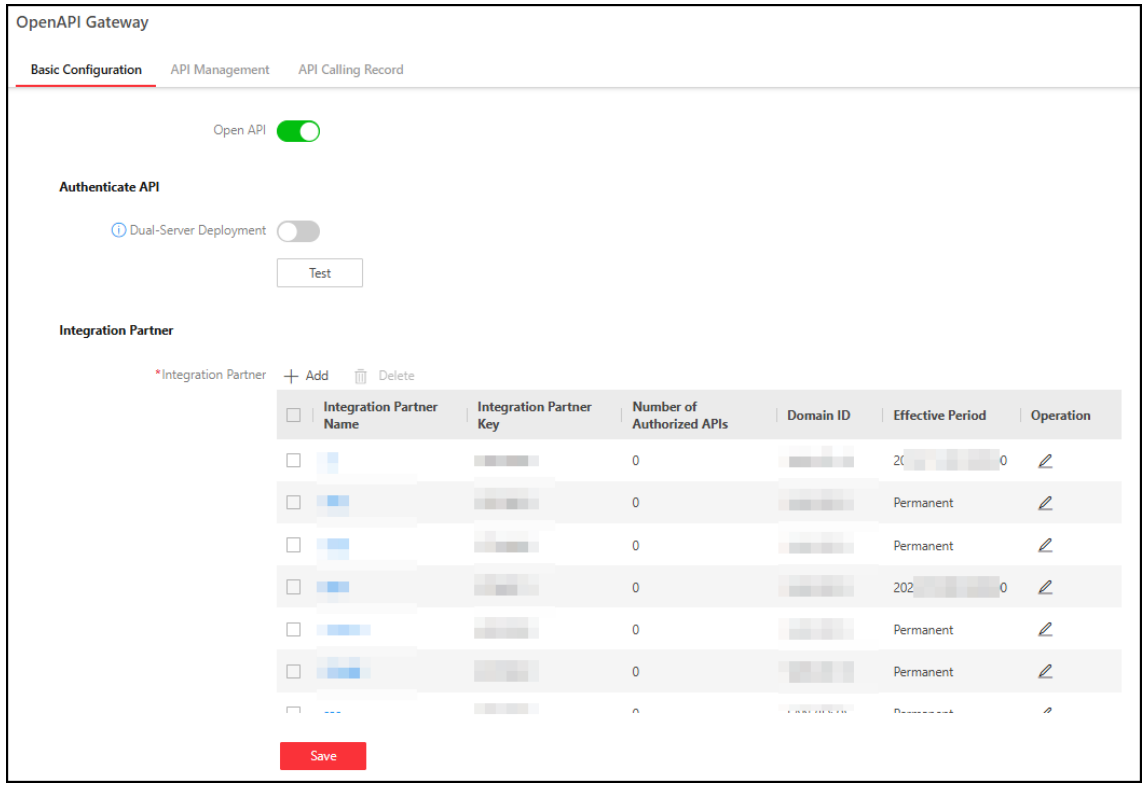



**Figure 13-1 OpenAPI Gateway**

## Basic Configuration

1. Enable the **Dual-Server Deployment** when the OpenAPI gateway and HikCentral Professional are deployed on different PCs. Set the IP address and port of the OpenAPI gateway and test the connection.
2. Click **Add** to add integration partners.

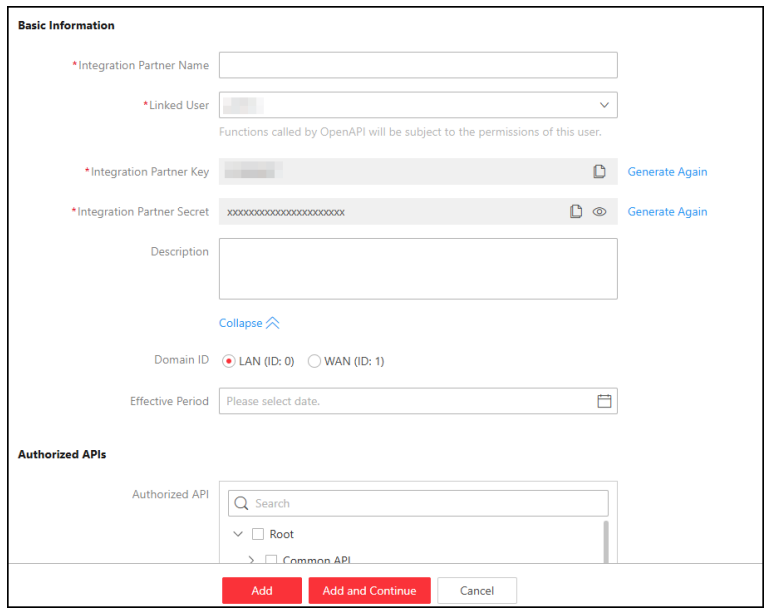



**Figure 13-2 Add Integration Partner**

**Linked User**

Select a platform user as the integration partner user, who can access and operate the OpenAPI gateway.

**Note**

The accessible API scope depends on the user permission, which is defined by the role assigned during user adding.

**Integration Partner Key**

It is generated automatically by the platform. It is used together with **Integration Partner Secret** for signature and authentication during API calling. Refer to the *HikCentral Professional OpenAPI Developer Guide* for detailed signature method.

**Note**

It is recommended to record the generated integration partner credentials (AK/SK). During reinstallation, you can manually enter these credentials to add the existing integrator and prevent the integration failure caused by the AK/SK change after reinstallation.

**Integration Partner Secret**

It is generated automatically by the platform. It is used together with **Integration Partner Key** for signature and authentication during API calling.

**Authorized APIs**

Select APIs accessible for the integration partner user.

### API Management

- APIs can be categorized by group.
- The integration partner user with permissions can add, import, export, edit, debug and delete APIs.

### API Calling Record

Users with permissions can filter API calling records by conditions such as time duration, caller, calling status, and API name.

## 13.3 Set SIA Device Driver

For zones configured with SIA event rules, linked security control devices will report events. Since supported SIA sub-protocols vary by device, you can define an appropriate sub-protocol for device access and data parsing. Next, manage the event types acting as the alarm data source by adding custom types or deleting predefined ones. Finally, configure alarm rules for SIA events in the Event and Alarm module.

Select **SIA Device Driver** on the left navigation bar.

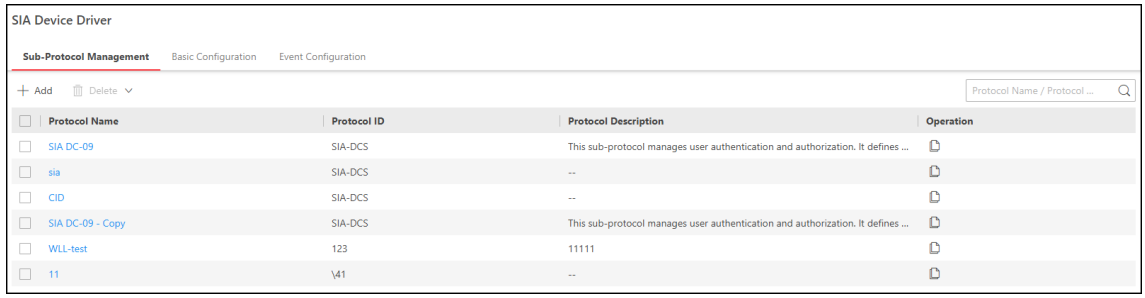



**Figure 13-3 SIA Device Driver**

### Sub-Protocol Management

Sub-protocol SIA DC-09 is predefined. You can also add custom sub-protocols as needed.

**Table 13-1 Sub-Protocol Management**

| Operation | Description |
|---|---|
| Add a Sub-Protocol | 1. Click **Add**.<br>2. Enter the parameters such as protocol name, protocol ID, protocol description.<br>3. Select an event code parsing method from SIA Code, CID Code, and Original Code.<br>4. Enter the regular expression and example message, click **Parse**. |

| Operation | Description |
|---|---|
| | 5. For each capturing group, select a built-in label or use an extension field as the label.<br>6. Click **Save**. |
| Copy a Sub-Protocol | In the operation column, click to create a copy of the sub-protocol. |
| Delete Sub-Protocol(s) | Select one or more sub-protocols and click **Delete**. |

### Basic Configuration

Enter the device offline threshold. An SIA device will be considered offline once the consecutive missed heartbeats reach the configured value. You can go to the Event & Alarm module to configure device online/offline alarms for timely notifications.

### Event Configuration

Standard event types are built-in. You can add custom events and delete added ones.

## 13.4 Integrate via SIA Gateway

The platform provides the SIA Gateway to integrate the third-party system. By the provided SIA protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **SIA Gateway** on the left navigation bar and switch on **SIA Gateway** to configure the basic parameters, zones, and event template.

### Basic Configuration

Select the access mode (listening mode or arming mode), select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, enter the IP address and port No. of the third-party system if the listening mode is selected, enter the linecard number and the receiver number, set the heartbeat interval, and then click **Save**.

**Note**

The default transport protocol is TCP/IP, which is not configurable, and you can check the connection status of the gateway.

### Zone Configuration

1. Click **Add** to enter the Add Zone page.
2. Enter a name for the configuration and set the account ID of SIA protocol.
3. Click **Add** to open the Add Resource pane.
4. Select a resource type for the zone.
5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

**Note**

- If you check **Auto Generate Zone ID**, the platform will generate zone IDs for all the selected resources. Otherwise, you should set a zone ID for each resource manually.
- You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.

6. Select an existing event template or click **Add Event Template** to add a new one (see ***Event Template Configuration*** ).
7. Click **Add** or **Add and Continue** to finish adding a zone and go back to the Zone Configuration page or continue to add another one.

After adding zones, you can perform the following operations on the Zone Configuration page.

- Click in front of the configuration name to display the linked resource name and zone ID.
- Click a configuration name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

## Event Template Configuration

1. Click **Add** to enter the Add Event Template page.
2. Enter a name for the template and select an event source type.
3. Click **Add** in the Template Content section to add events for the template by selecting event types and SIA codes.

**Note**

You can click in the Operation column of an event type to remove it or click **Delete All** to remove all the selected event types.

4. Click **Add** or **Add and Continue** to finish adding an event template and go back to the Event Template page or continue to add another one.

After adding event templates, you can perform the following operations on the Event Template Configuration page.

- Click in front of the template name to display the linked event type and SIA code, which can be edited by clicking in the Operation column.
- Click a template name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click **Import** to batch add event templates by the Excel file. During import, the duplicated templates can be overwritten by checking **Auto Replace Duplicated Template**.

- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** to adjust the column width.

## 13.5 Set BACnet Device Driver

Allows to configure the basic parameters for the BACnet device driver (bacnet.d), such as instance No., device name, and port No.

Click **BACnet Device Driver** on the left navigation bar and enter parameters.

**BACnet Instance No.**

Set a unique device instance number to ensure proper identification and addressing within the BACnet network.

**BACnet Device Name**

Configure a human-readable name for easy identification.

**Port No.**

Customize the BACnet/IP UDP port (default: 47808) to adapt to specific network policies or avoid port conflicts.

## 13.6 Integrate via BACnet Gateway

The platform provides the BACnet Gateway to integrate the third-party system. By the provided BACnet protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **BACnet Gateway** on the left navigation bar and switch on **BACnet Gateway** to configure the basic parameters, objects, and event template.

### Basic Configuration

Select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, enter the BACnet instance No. and BACnet device name, set the timeout duration and resending times for APDU, and then click **Save**.

**Note**

The default transport protocol is UDP/IP, which is not configurable.

### Add an Object

1. Click **Add** to enter the Add Object page.
2. Enter a name for the object.
3. Select an object template (see ***Object Template*** ).
4. Select a source type and the corresponding resource type for the object.

5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

**Note**

- If you check **Auto Generate Target Instance No.**, the platform will generate target instance No.s for all the selected resources. Otherwise, you should set a No. for each resource manually.
- You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.

6. Click **Add** to finish adding an object and go back to the Object Configuration page.

### Object Configuration

After adding objects, you can perform the following operations on the Object Configuration page.

- Click > in front of the object name to display the linked resource name and target instance No.
- Click an object name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Check one or more objects and click **Export** to save their configurations to an Excel file.
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

### Object Template

On the Object Template page, you can perform the following operations.

- View the information about four predefined object templates, including the object type, attribute, value definition, and the status of active event notification.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

## 13.7 Integrate via Sur-Gard Gateway

The platform provides the Sur-gard gateway to integrate the third-party system. By the provided Sur-gard protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **Sur-Gard Gateway** on the left navigation bar and switch on **Sur-Gard Gateway** to configure the basic parameters, zones, and event template.

## Basic Configuration

Select the access mode (listening mode or arming mode), select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, select the MRL mode, enter the IP address and port No. of the third-party system if the listening mode is selected, enter the linecard number and the receiver number, set the heartbeat interval, and then click **Save**.

**Note**

- The default transport protocol is TCP/IP, which is not configurable, and you can check the connection status of the gateway.
- For MRL2, the linecard No. is 1-bit, and for MRL2000, it is 3-bit.

## Zone Configuration

1. Click **Add** to enter the Add Zone page.
2. Enter a name for the configuration and set the account ID of Sur-gard protocol.
3. Click **Add** to open the Add Resource pane.
4. Select a resource type for the zone.
5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

   **Note**

   - If you check **Auto Generate Zone ID**, the platform will generate zone IDs for all the selected resources. Otherwise, you should set a zone ID for each resource manually.
   - You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.
6. Select an existing event template or click **Add Event Template** to add a new one (see ***Event Template Configuration*** for details).
7. Click **Add** or **Add and Continue** to finish adding a zone and go back to the Zone Configuration page or continue to add another one.

After adding zones, you can perform the following operations on the Zone Configuration page.

- Click > in front of the configuration name to display the linked resource name and zone ID.
- Click a configuration name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

### Event Template Configuration

1. Click **Add** to enter the Add Event Template page.
2. Enter a name for the template and select an event source type.
3. Click **Add** in the Template Content section to add events for the template by selecting event types and CID codes.

   **Note**

   You can click in the Operation column of an event type to remove it or click **Delete All** to remove all the selected event types.
4. Click **Add** or **Add and Continue** to finish adding an event template and go back to the Event Template page or continue to add another one.

After adding event templates, you can perform the following operations on the Event Template Configuration page.

- Click > in front of the template name to display the linked event type and CID code, which can be edited by clicking in the Operation column.
- Click a template name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click **Import** to batch add event templates by the Excel file. During import, the duplicated templates can be overwritten by checking **Auto Replace Duplicated Template**.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** to adjust the column width.

## 13.8 Data Interchange

The access records in HikCentral Professional can be used by third-party systems for pay calculation or other applications. You can synchronize the access records to a third-party database by entering the information of the database table in the required space. You can also dump the access records in CSV or TXT format, and then let the third-party database read the access records to get them.

### 13.8.1 Synchronize Access Records to Third-Party Database

You can enable synchronization function to apply the access records of specified resources from HikCentral Professional to the third-party database automatically.

**Steps**

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) and lanes for access records synchronization.

**Note**

- For card readers and lanes, you should set a direction when selecting them. Alternatively, you can batch set directions of added card readers / lanes by clicking **Set Direction (In/Out)**.
- Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
- Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.

4. Select the encoding format of data interchange.
5. Check **Push Wide Byte Data** to avoid character encoding issues between the platform and the database.
6. Check **Store in Unicode Format** to store data in the Unicode format to avoid character encoding issues between the platform and the database.
7. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
8. Select **Database Synchronization**.
9. **Optional:** Switch on **Auto Push Failed Record** to select the push mode.

   **Push at Fixed Time**

   The failed record will be pushed at the time you set.

   **Push at Fixed Interval**

   The failed record will be pushed according to the interval you set.
10. **Optional:** Select a database type.
11. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
12. Click **Test Connection** to test whether database can be connected.
13. Set table parameters of database table and table fields according to the actual configurations.
    1) Enter the table name of the third-party database.
    2) Enter the mode of the third-party database.
    3) Set the mapped table fields between the HikCentral Professional and the third-party database.
    4) **Optional:** Click **Customize Items to Display** to select the items to be displayed in the table.
14. Click **Save**.

    A window will pop up and you can choose to push the test data now or later.
15. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

    **Note**

    If there are errors found, you can export the failed data for checking.

### 13.8.2 Dump Access Records to Third-Party Database

Access records of specified resources can be dumped as CSV file or TXT files. Third-party systems can then read these dumped file (instead of accessing the database and mapping the table fields) for applications, such as attendance or payment calculation. You can also configure dump rules for dumping access records. After that, the access records will be dumped to the third-party database according to the added rules.

**Steps**

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) and lanes for access records dumping.

**Note**

- For card readers and lanes, you should set a direction when selecting them. Alternatively, you can batch set directions of added card readers / lanes by clicking **Set Direction (In/Out)**.
- Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
- Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.

4. Select the encoding format of data interchange.
5. Check **Push Wide Byte Data** to avoid character encoding issues between the platform and the database.
6. Check **Store in Unicode Format** to store data in the Unicode format to avoid character encoding issues between the platform and the database.
7. **Optional:** Check **Do Not Push Failed Records**.

   The failure records will not be pushed to the third-party system.
8. Select **Access Record Dump**.
9. In the Dump Rule area, click **Add** and set the required parameters.

   **Overwrite File**

   If it not checked, you re recommended to regularly view the disk capacity in case the new files cannot be generated if the disk if full.

   **File Name**

   The name of the CSV file or TXT file which the access records are dumped as.

   **Storage Location**

   **Local Storage**

   The access records can be dumped as a file saved in the local disk of the SYS. Then you need to copy this file from the server to your PC with the third-party system installed to read the dumped file.

**Note**

- You need to log in to the Web Client running on the SYS to configure related settings of local storage.
- You need to set **Saving Path**, which is the path where the CSV file or TXT file is saved.

**SFTP Storage**

You can access the SFTP server as the storage location for saving the dumped file by setting the SFTP address, port, user name, and password. And you can enter the path to save the dumped file in the folder on the SFTP server or leave it empty to save the file in the root directory.

**Note**

The third-party system should be installed in the SFTP server to read the dumped file.

**Content**

The display items and data in the dumped file.

**Department**

The group of persons. You can select and search for departments in the list.

**Min. Length of Person ID**

For some scenarios, the person IDs need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the person ID is shorter than the value, zero(s) will be added before the ID to make it equal to the value. If the length is longer than the value, the person IDs will be dumped according to the actual length.

**Designated Length of Card No.**

For some scenarios, the card numbers need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the card number is shorter than the value, zero(s) will be added before the card number to make it equal to the value. If the length is longer than the value, the card number will be dumped according to the actual length.

**Generate Table Header**

When the card swiping records are dumped from the system to the local PC, the column names will be included in the dumped file and used as the table header.

**File Format**

Two formats are supported, including CSV and TXT.

**Dump Frequency**

The frequency for dumping access records.

**Dump Time**

The time when dumping card swiping records is started.

10. Click **Add** on the Add Dump Rule page.

The added rules will be listed in the Dump Rule area.

**Note**

You can click × in the Operation column to delete the rule or click **Delete All** to delete all added rules.

11. Click **Save**.
12. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

**Note**

If there are errors found, you can export the failed data for checking.

## 13.9 WhatsApp

The platform supports integrating with WhatsApp. After the WhatsApp merchant account is configured and authenticated, the platform can send events messages and application messages (such as visitor reservation, dock reservation, and alarms from ReGuard) to application subscribers via WhatsApp.

Select **WhatsApp** on the left navigation bar and click **Enable**.

### Submit WhatsApp Merchant Account for Authentication

**Note**

You need to apply for a WhatsApp merchant account first for sending the platform message.

1. Enter the account basic information, including merchant account, phone No., application No., callback address, access token, verification token, and first push language.

   **Callback Address**

   The domain address and the port number.

   **First Push Language**

   The language of guidance messages pushed to individual WhatsApp accounts upon subscription.
2. (Optional) Switch on **Enable Limit** to configure the upper limit of daily and monthly conversation times.
3. Click **Submit for Authentication** to send a request of WhatsApp merchant account authentication.

**Note**

If the authentication is not passed, you can check the failure reason, edit the basic information, and submit for authentication again.

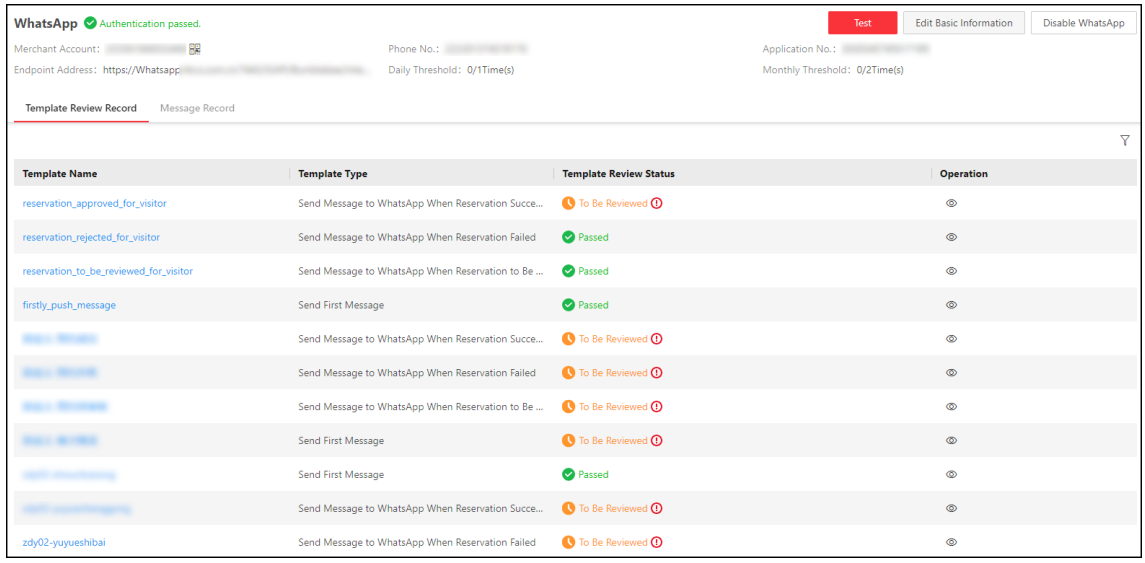



**Figure 13-4 WhatsApp Page**

## Manage Authenticated WhatsApp Account

When the merchant account is authenticated, you can view WhatsApp message templates related to the visitor reservation, dock management, ReGuard, and education messages receiving/sending records.

| Operation | Description |
|---|---|
| Test Account | Click **Test** and enter a recipient account to test the message sending of merchant account.<br>**Note**<br>The testing might cost fees. |
| View Account QR Code | Click the QR code thumbnail next to the account ID. You can refresh and download your account QR code for sharing. |
| View Template Review Status | Click **Template Review Record** tab to view the WhatsApp message templates.<br>The templates are configured within each module (such as Visitor, Re-Gard, and Education). |
| View Message Records | Click **Message Record** tab to view the message sending/receiving records. |

# Chapter 14 Video Management

In the Video module, you can set video basic parameters such as volume, video storage path, and recording, perform live view, playback, and PTZ control, as well as configure parameters for other important functions such as intelligent recognition, self-learning library, panorama tracking, and visual tracking.

**Note**

The platform supports video features with and without plugin. However, some functions are only available when there is a plugin. For example, view management, remote sites display on the resources tree, audio recording, dragging cameras to adjust the order of multiple windows, window division other than 1, 4, 9, 16 during live view and playback, and displaying alarm status and viewing alarm details in the camera window reporting the alarm.

## 14.1 Video Security

The HikCentral Professional provides functionality of live view, playback, and local configuration through web browser.

**Note**

- If the SYS's transfer protocol is HTTPS, the Video Security module (including Live View, Playback, and Local Configuration) is available only when accessing the Web Client via Internet Explorer.
- If the SYS's transfer protocol is HTTP, the Live View and Playback modules are available for Internet Explorer, Google Chrome, Firefox, and Safari 11 and above. But Local Configuration module is available for Internet Explorer only.

### 14.1.1 Live View

In the Live View module of Web Client, you can view the live video of the added cameras and do some basic operations, including picture capturing, recording, PTZ control.

In the top left corner of the Client, select → **Video** → **Video Security**

#### Before You Start

#### Step 1: Add Encoding Devices

Refer to ***Add Device(s)*** to add encoding devices.

### Step 2: Add Cameras to Area

Refer to ***Add Element to Area*** .

### Choice 1: Start Live View in Area Mode

**Note**

The areas which the current user has permission to access are listed and the resources which the user has permission to access are shown in the corresponding areas.

1. Click in the upper-right corner to change live view window division.
2. Start live view.
   - Drag a camera to the display window to start the live view of the camera, or double-click the camera to start the live view in a free display window.
   - Drag an area to a display window, and click **Batch Play**, or double-click the area to start the live view of all cameras in the area.

### Choice 2: Start Live View in View Mode

A view is a window division with resource channels (e.g., cameras and access points) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows (or correspondence between map and window) as the default so that you can quickly access these channels and/or map later. For example, you can link camera 1, camera 2, and camera 3 located in your office to the certain display windows and save them as a view called ***office***. Then, you can access the view ***office*** and these cameras will display in the linked window quickly.

**Note**

- For live view, the view mode can save resource type, resource ID, stream type, position, and scale after digital zoom, preset No., and fisheye dewarping status.
- For playback, the view mode can save resource type, resource ID, position, and scale after digital zoom, and fisheye dewarping status.

1. Click on the left navigation bar.
2. Add a custom view group.
   a. Select **Public View** or **Private View** to add the view group.

      **Note**

      The view groups and views that belong to the private view group are hidden from the other users.

   b. Click , set a name for the view group, and click **OK**.

3. Add a view.
   a. Select a view group, click , and set a name for the view.
   b. Click **Add** to select cameras.
   c. Set the required parameters, and click **Add** to add a view.
4. Double click a view or move the cursor over a view, and click → **Play** beside the view name to start live view of the cameras from the view.

## Choice 3: Start Live View of Favorited Cameras

1. Click on the left navigation bar.
2. Select a parent Favorites, click to add a Favorites under the parent Favorites, and select the camera(s) to be added to Favorites.

**Note**

Up to 5 levels of Favorites can be added.

3. (Optional) Select a Favorites, and click → **Share** on the right side of Favorites' name to share it with others.
4. When in Live View window, select a Favorites, and click → **Play All** to start viewing the live view of all the camera(s) added in Favorites.

## Choice 4: Auto-Switch Cameras in an Area

1. Start auto-switch in the area.
   - Drag an area to the live view window and select **Single-Window Auto-Switch** to start the auto-switch the cameras of the area in the selected display window.
   - Click on the right side of the area name and click **Area Auto-Switch** to switch the cameras of the area in the live view window.
2. Move the cursor over the live view window and perform further operations after auto-switch starts.

| Operations | Descriptions |
|---|---|
| Adjust Switching Interval | Click or in the lower-left corner of the live view window to adjust the interval of the auto-switch. |
| View Previous or Next Camera | Click or in the lower-left corner of the live view window to go to the previous or next camera. |
| Pause | Click in the lower-left corner of the live view window to pause the auto-switch. |

## (Optional) Start PTZ Control

The PTZ control for cameras with pan/tilt/zoom functionality is provided. You can set the preset, patrol and pattern for the cameras on the PTZ control pane.

In the top left corner of the Client, select → **Video** → **Video Security**

Start live view of a camera, and click **PTZ Control** to open the PTZ pane.

**Note**

The PTZ control function should be supported by the camera.

### Introduce the Main Pane

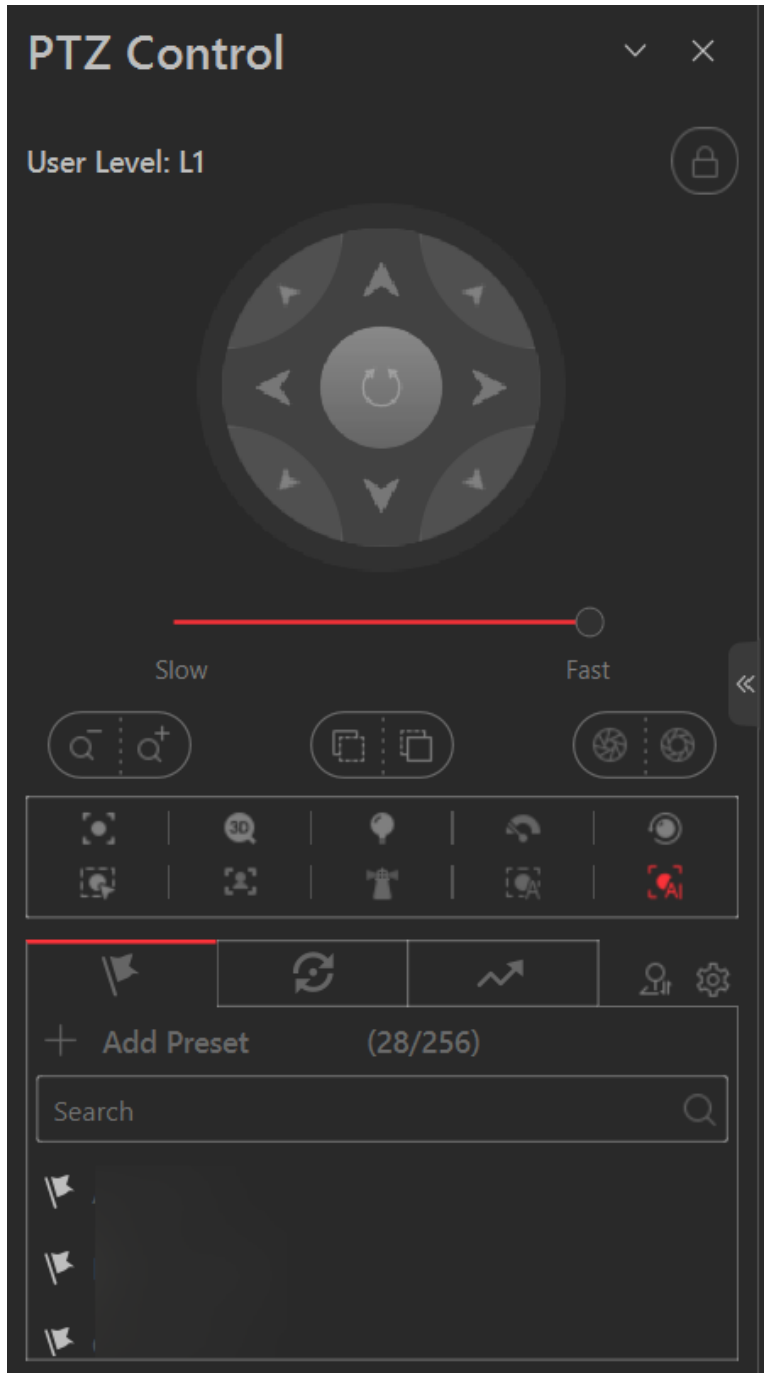



**Figure 14-1 PTZ Control Panel**

The following buttons are available on the PTZ control pane:

| | |
|---|---|
| | Lock the PTZ for a designated time period. When the PTZ is locked, users with lower PTZ control permission levels cannot change the PTZ controls.<br>**Note**<br>For details about setting the PTZ control permission level, refer to the *User Manual of HikCentral Professional Web Client*. |
|  | Direction Button, Auto-scan and PTZ speed. |
| / | Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function. |
| / | 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. |
| / | Click to move the focal point backward, and click to move the focal point forward. |
| | Auxiliary Focus: Click to focus automatically. |
| | 3D Positioning: 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. Click 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. |
| | Light: Click to fill light. |
| | Wiper: Use the wiper to clear the dust on the camera lens. |
| | Lens Initialization: Initialize the lens and focus again for a clear image. |
| | 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. |
| | 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. |
| | Park Action: 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. |

| | |
|---|---|
| | Auto Track: For cameras support and tracking, click the icon and select the target (person or vehicle) in the live view to arm and track this target. |
| | Self-Learning Focus: Compatible cameras can memorize the optimal focus parameters for each preset position, enabling fast and accurate auto-focus during patrols. This resolves occasional image blur after zooming or prolonged monitoring, ensuring consistently clear images. |

- In the live video display window, click the icon to start PTZ control. Click and drag the cursor with a white arrows to control the direction.
- Click to get device PTZ configuration.

## Configure Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom.

1. Click to enter the PTZ preset configuration pane.
2. Use the direction buttons to control the PTZ movement.
3. Select a PTZ preset number from the preset list and click to name and save the settings.

## Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets (including virtual presets), with the scanning speed between two presets and the dwell time of the preset separately programmable.

Before you start, make sure you have added two or more presets.

1. Click to enter the patrol configuration pane.
2. Select a PTZ patrol number and click to set the patrol.
   a. Select or as the preset type.

      **Note**

      A device preset ( ) is a predefined image position, while a virtual preset ( ) is a predefined and zoomed image position. You can add a virtual preset by starting live view, zooming in, and adding the image position as a virtual preset.

   b. Click to add a configured preset, hover your cursor over the values in the **Preset**, **Speed**, and **Time** columns, and slide the mouse to change the value.
   c. Click or to adjust the presets sequence.
3. Set other parameters, and click **OK**.
4. (Optional) Click to set a duration after which the patrol path will be restored if no manual operations are detected.

### Configure Pattern

By recording pattern, the movement path and the dwell time in a certain position can be recorded precisely. By calling pattern, mobile PTZ starts moving exactly according to the recorded path.

1. Click to enter the PTZ pattern configuration pane.
2. Click to start recording the movement path of the pattern, use the direction buttons and other buttons to control the PTZ movement, and click to stop and save the pattern recording.
3. Click to call the pattern.

## 14.1.2 Live View Toolbar Applications

You can customize the icons on the toolbar, start the fisheye dewarping mode, perform manual panorama tracking, and so on.

### View Dewarped Live View of Fisheye Camera

You can set center calibration and view dewarped live view of a fisheye camera in the client. Dewarping refers to the process of perspective correction of an image, to reverse the effects of geometric distortion caused by the fisheye camera lens. It allows the user to cover a wide area with a single device and have a "normal" view of an otherwise distorted or reversed image. Also, during live view, you can perform more operations such as adjusting view angle and zooming in/out view.

**Steps**

1. ***Start live view*** of a fisheye camera.
2. On the toolbar of display window, click to enter the fisheye dewarping mode and view live view.




**Figure 14-2 Fisheye Dewarping**

3. **Optional:** Perform the following operations as desired.

| | |
|---|---|
| **Adjust View Angle** | Put the cursor on the live video, and drag the video to adjust the view angle. |
| **Zoom in/out View** | Put the cursor on the live video, and scroll the mouse wheel to zoom in or out the view. |
| **Perform PTZ control** | Use the PTZ panel on the left side to perform PTZ control of the camera.<br>**Note**<br>Setting pattern is not supported by fisheye cameras. |

## Manual Recording and Capture

You can record video files and capture pictures manually during live view.

**Manual Recording**

Record the live video during live view if needed and store the video files in the local PC.

**Capture**

Capture pictures during live view if needed and store the pictures in the local PC.

## Manual Recording

1. In the top left corner of the platform, select → **Security Monitoring → Video → Video Security** .
2. Move the cursor to the live view display window to show the toolbar.
3. Click in the toolbar of the display window to start the manual recording. The icon turns to .

**Note**

During the manual recording, **Recording...** will display in the upper-right corner of the display window.

4. Click to stop recording.
   A dialog directing to the saving location of the file pops up.

**Note**

- The video cannot be saved if the free space on your disk is less than 2 GB.

5. (Optional) Click **Open Folder** to access the video file folder in the pop-up dialog box after manually recording.

## Capture Pictures

1. In the top left corner of the Client, select → **Security Monitoring → Video → Video Security** .
2. Move the cursor to the live view display window to show the toolbar.
3. Click in the toolbar to capture a picture.
   A dialog box directing to the saving location pops up.

**Note**

-
- The picture cannot be saved if the free space on your disk is less than 512 MB.

4. (Optional) After the dialog box popped up, perform the following operation(s).

| Operation | Description |
|---|---|
| Check Picture | Click **Open Folder** in the dialog box to open the folder where the captured pictures stored to and view pictures. |
| Edit Picture | a. Click **Edit** in the dialog box to open the Capture window.<br>b. Press and move the cursor on the picture to draw. For example, you can mark the suspicious persons in the picture.<br>c. Click **Save As** and specify the path to save the edited picture.<br>**Note**<br>The picture cannot be saved if the free space on your disk is less than 512 MB. |

## Perform Manual Panorama Tracking

During live view, you can enable the panorama tracking manually to locate or track the target appeared in the view of bullet or box camera with a linked speed dome. You can also check and test the calibration results about panorama tracking settings for auto-tracking.

**Before You Start**

Make sure you have configured the panorama tracking rules for the box or bullet camera on Web Client. For more details, refer to *User Manual of HikCentral Professional Web Client*.

**Steps**

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Start the live view of box/bullet camera, and linked speed dome.
3. Click on toolbar of box/bullet camera to enable manual panorama tracking.

**Note**

If you choose to enable manual panorama tracking, the auto panorama tracking will not take effect; if you choose not to enable manual panorama tracking and enable **Auto-Tracking** when configuring panorama tracking on the Web Client, when the configured VCA event is triggered by target, the linked speed dome will perform the automatic panorama tracking.

4. Click or draw a rectangle on the live view image of the box/bullet camera, and the speed dome will switch to the close-up view.

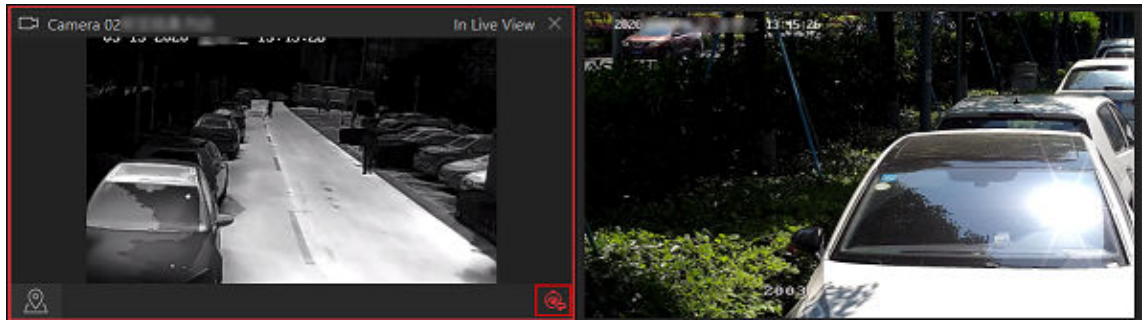



**Figure 14-3 Manual Panorama Tracking**

## Customize Icons on Live View Window

You can customize the icons on the toolbar of the live view window, adjust the icon order, and control whether to always show toolbar on the live view window or not.

**Steps**

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .
2. In the top right corner of the page, click → **Toolbar** .
3. In **Customize Live View Tool Bar** section, add or remove the icons to show or hide the icons on the live view toolbar.
4. Drag the icons in the icon list to adjust the order.

**Table 14-1 Icons on Live View Toolbar**

| | | |
|---|---|---|
| | Audio Control | Turn off/on the sound and adjust the volume. |
| | Capture | Take a snapshot of the current video and save it to the current PC.<br>**Note**<br>After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Picture Search** to search the captured picture, archive, and identity verification related with the captured picture. |
| | Record | Start manual recording. The video file will be stored in local PC. |
| | Instant Playback | Switch to instant playback mode to view the recorded video files. |

| | | |
|---|---|---|
|  | Two-Way Audio | Start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device. |
|  | Digital Zoom | Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function. |
|  | PTZ Control | Activate the PTZ icons on the image to pan, tilt, or zoom the image. |
|  | Fisheye Expansion | Available for fisheye camera. In the fisheye dewarping mode, the Client will correct the video image and reverse the effects of geometric distortions caused by the fisheye camera lens. See ***View Dewarped Live View of Fisheye Camera*** for details. |
|  | Camera Status | Show the camera's recording status, signal status, connection number, etc. |
|  | Switch Stream | Switch the live view stream to main stream, sub-stream (if supported), or smooth stream (if supported).<br>**Note**<br>The smooth stream will show if device supports. You can switch to smooth stream when in low bandwidth situation to make live view more fluent. |
|  | Alarm Output | Display the Alarm Output Control page and turn on/off the alarm outputs of the connected camera. |
|  | Manual Linkage | Locate or track the target appeared in the view of bullet or box camera with a linked speed dome. |
|  | Enhancement | Adjust the video image including brightness, saturation, etc. |
|  | Rotate Image | Rotate an image. |
|  | Park Action | Click the icon and the speed dome will save 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). |
|  | Locate Target | Click the icon to measure the distance between camera and target. |

| | | |
|---|---|---|
| | Panorama | Click to generate a cylindrical panorama image or fisheye panorama image. |
| | Clean Manually | Click the icon to clean the camera. |
| | Object Search | Select a person in the image and search for the person. |

**Note**

The icons on the toolbar in the live view window vary with the device's capabilities.

5. Click **Save**.

### 14.1.3 Playback

The video files stored on the local storage devices such as HDDs, Net HDDs, and SD/SDHC cards or the Recording Server, can be searched and played back remotely through the web browser.

In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .

#### Before You Start

#### Step 1: Add Encoding Devices

Refer to ***Add Device(s)*** to add encoding devices.

#### Step 2: Add Cameras to Area

Refer to ***Add Element to Area*** .

#### Step 3: Set Recording Schedule

Perform this task when you need to customize the schedule to record the video files.

1. In the top left comer of the Home page, select → **Video** → **Video Settings** → **Recording Schedule Template** .
2. Click + to enter the Adding Recording Schedule page.

**Note**

Up to 32 templates can be added.

3. Set the required parameters.

**Time-based**

Continuous recording according to the time you arranged. The schedule time bar is marked with blue.

**Event-based**

The recording triggered by the alarm (e.g., alarm input alarm or motion detection alarm). The schedule time bar is marked with orange.

**Command-based**

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

## Step 4: Set Recording Parameters

## Set General Recording Parameters

For cameras on the current site and Remote Site, the platform provides storage locations such as Hybrid SAN(CVR), Cluster Storage, and pStor for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding a camera to an area.

1. Enter the Recording Setting page.
   a. In the top left corner of the Home page, select → **Basic Management** → **Device** → **Area** .
   b. Select an area to show its cameras.

   **Note**

   refers to the current site and refers to Remote Site.

   c. Select a camera and click its name to enter the camera settings page.
   d. Select the **Recording Settings** tab.
2. On the editing camera page, click **Recording Settings** on the top.
3. In the Recording Settings area, switch on **Main Storage** (for the current site) or **Storage in Central System** (for Remote site).
4. Select the storage location for storing the recorded video files.
5. Select the storage type and configure other required parameters.

   **Note**

   The parameters vary according to the site (current site or Remote Site) you selected previously.

   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location in real time.

     **Note**

     - If you select **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.
     - If you select **Hybrid SAN(CVR)**, **Cluster Storage**, **pStor**, or **pStor Cluster Service**, specify a server and (optional) select a Streaming Server to get video streams from cameras via it.

     **Recording Schedule Template**

Set the template which defines the time periods to record the camera's video.

**All-Day Time-Based Template**

Record the video for all-day continuously.

**All-Day Event-Based Template**

Record the video when alarm occurs.

**Add New**

Set the customized template.

**View**

View the template details.

**Note**

The event-based recording schedule can not be configured for the **Cluster Storage**, and the command-based recording schedule can not be configured for the **Cluster Storage** and **pStor**.

**Stream Type**

Select the stream type as main stream, sub-stream or dual-stream.

**Note**

For storing on Hybrid SAN(CVR), Cluster Storage, pStor or pStor Cluster Service, dual-stream is not supported.

**Pre-Record**

Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

This field displays when the storage location is set as Encoding Device, Cluster Storage, pStor, or pStor Cluster Service. And it is available for the camera that is configured with event-based recording.

**Post-Record**

Record video from periods following detected events.

This field displays when the storage location is set as Encoding Device or Hybrid SAN(CVR). It is available for the camera that is configured with event-based recording.

**Video Expiry Time**

If you select **Encoding Device** as the storage location, switch on**Video Expiry Time** and enter expiration day(s).

Automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period to keep the videos as desired and the actual retention period for the videos depends on the allocated quota.

**Enable ANR**

If you select the **Encoding Device** or **Hybrid SAN(CVR)** as the storage location, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

- Select **Scheduled Copy-Back** as the storage type to copy the recorded video files from the encoding device or pStor to the specified storage location according to scheduled period.

**Note**

The recordings can be copied only from the encoding device to Hybrid SAN(CVR), Cluster Storage, pStor or pStor Cluster Service, or from pStor to another pStor.

**Upload Time**

Specify the time period to copy the recorded video files to the specified storage location.

**Recording for Copy-Back**

Select the type of recorded video file to backup.

**Max. Copy-Back Speed (KBps)**

Enter the maximum copy-back speed.

6. (Optional)Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

**Note**

- If Cluster Storage, Hybrid SAN(CVR), pStor, or pStor Cluster Service is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded video files or select **Scheduled Copy-Back** to copy recordings from the encoding device or pStor (main storage) to specified auxiliary storage location according to the scheduled period.
- Before setting **Scheduled Copy-Back**, make sure you have configured real-time recording schedule stored in device local storage or pStor for the main storage.
- The recordings can be copied only from the encoding device to Hybrid SAN(CVR), Cluster Storage, pStor or pStor Cluster Service, or from pStor to another pStor.

7. Click **Save**.

## Set Recording Parameters for VCA Search

### For NVR With Firmware Versions Higher Than V5.01

On the web page of NVR, enable **Save Smart Analysis Data of Camera**.

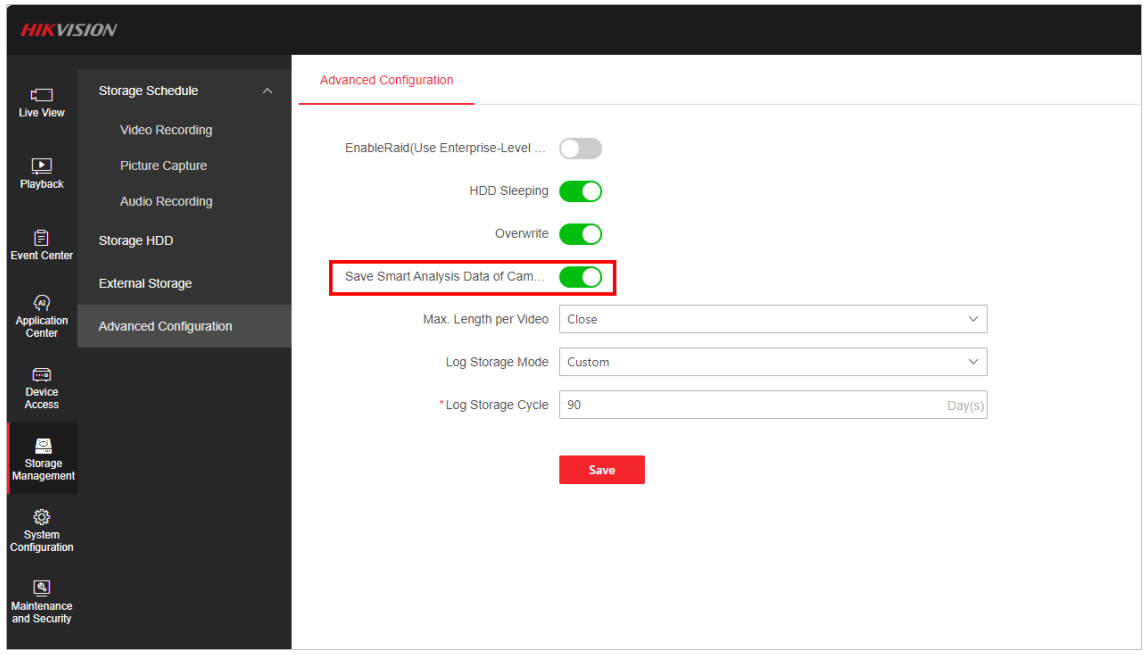



**Figure 14-4 Save Smart Analysis Data of Camera**

## For NVR With Firmware Versions Lower Than V5.01

Perform the following on the web page of NVR.

1. Enable **Dual-VCA** for the network camera.
2. Check **Enable Line Crossing Detection** and **Enable Intrusion**.

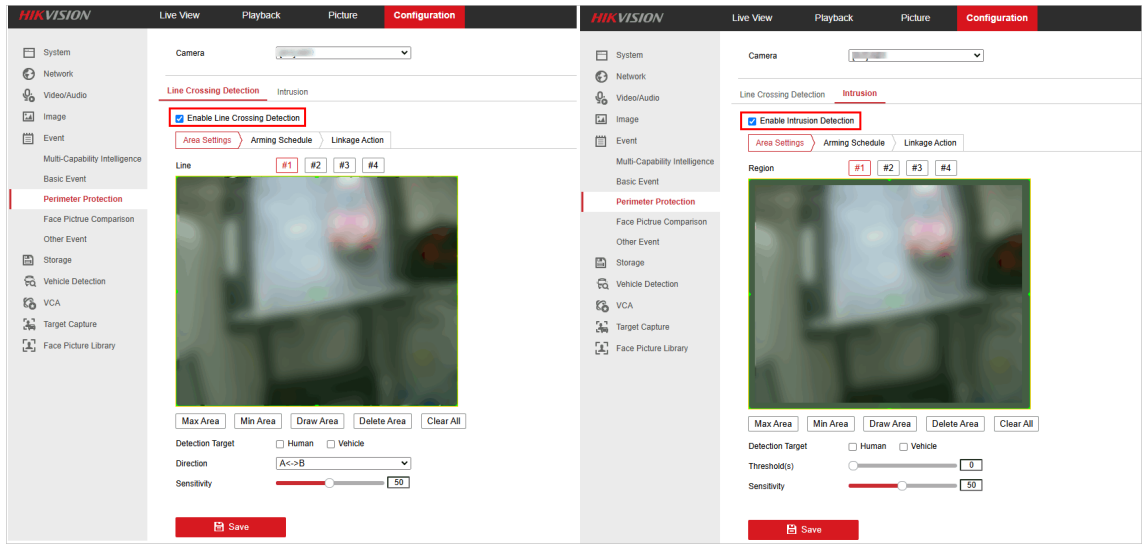



**Figure 14-5 Enable Line Crossing Detection & Enable Intrusion Detection**

3. Check **Save Camera VCA Data**.

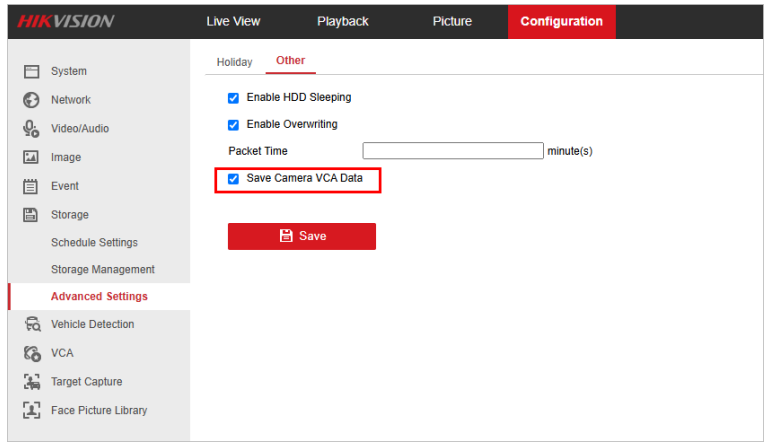



**Figure 14-6 Save Camera VCA Data**

## When Network Cameras Are Added to the Platform Directly or via NVRs/DVRs and Set Storage Location as Hybrid SAN(CVR)

1. Enable **Dual-VCA** for the network camera on the web page of the camera.

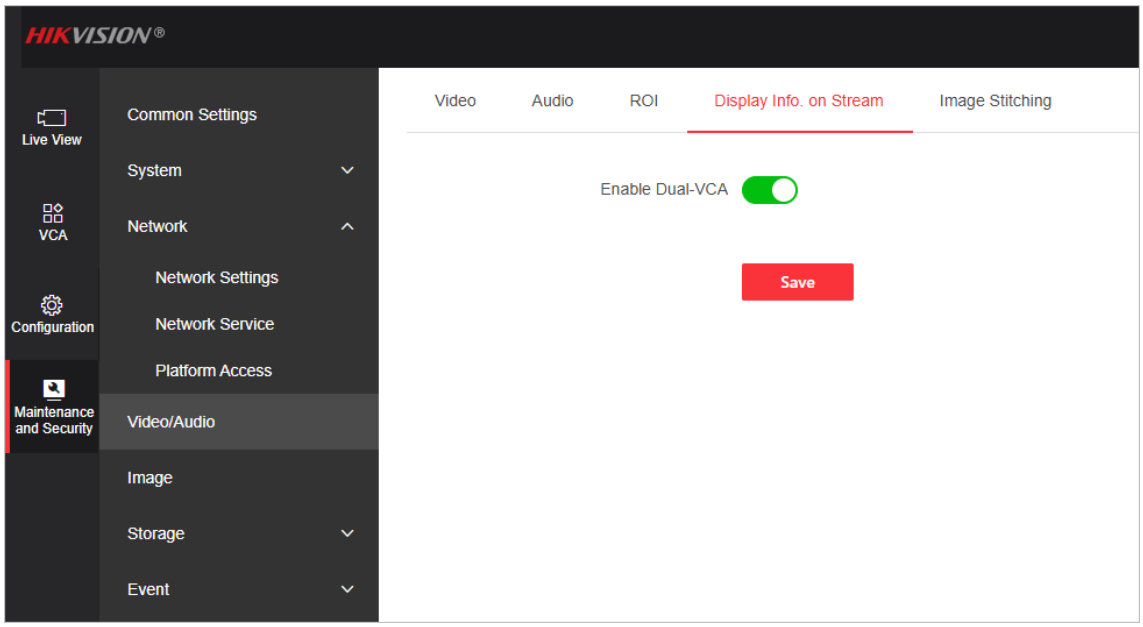



**Figure 14-7 Enable Dual-VCA**

2. Configure the video storage location as **Hybrid SAN(CVR)** on the Camera details page.

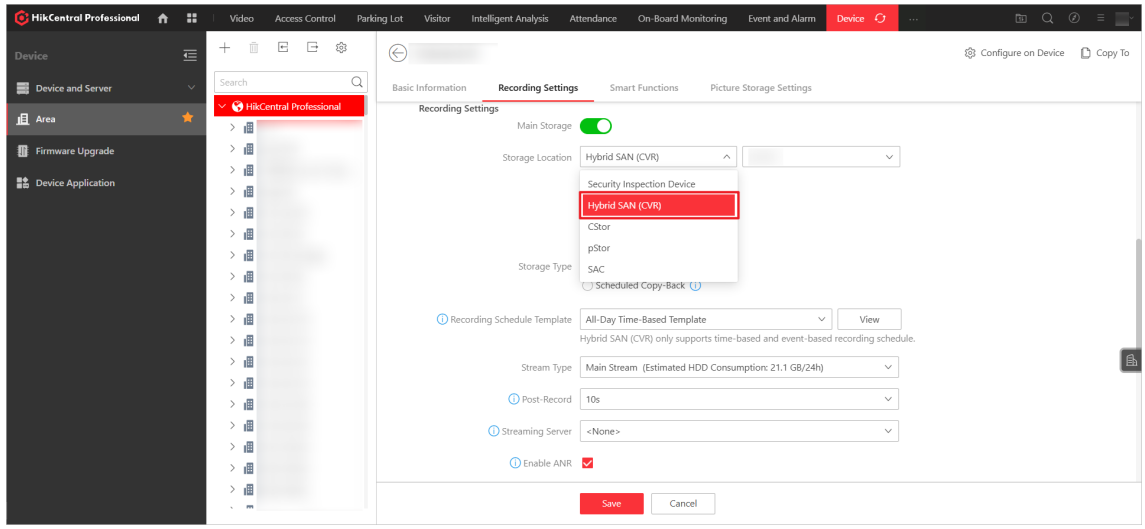



**Figure 14-8 Select Hybrid SAN(CVR)**

3. Log into the Hybrid SAN.




**Figure 14-9 Log in to Hybrid SAN**

4. Select **Smart function is enabled**.

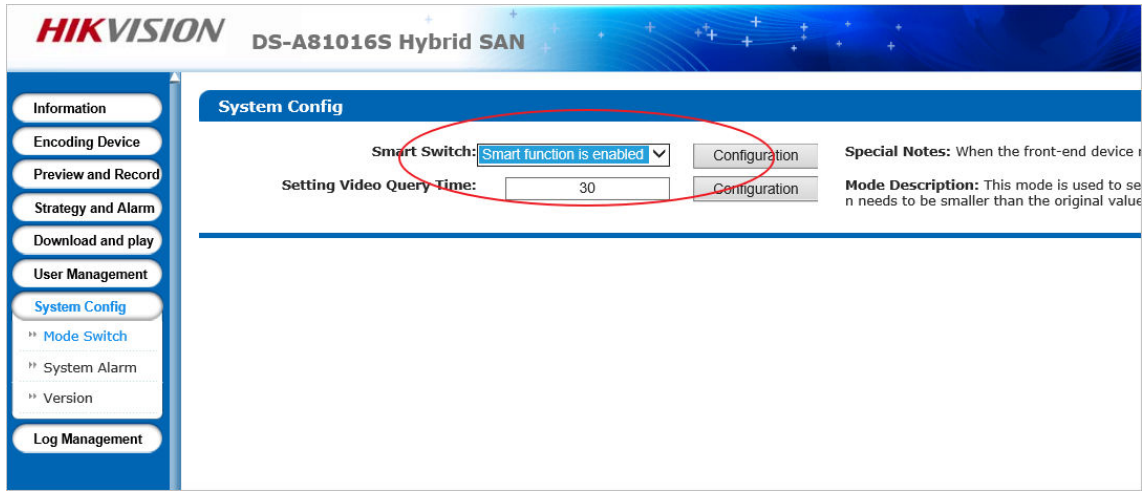



**Figure 14-10 Set Smart Switch**

## Choice 1: Start Playback in View Mode

Click on the left navigation bar.

Click the **Playback** tab to enter the playback page.

Click a view to quickly start the playback of all the cameras related to the view.

## Choice 2: Start Synchronous Playback

Start normal playback of at least two cameras.

After starting normal playback, click **Sync Play** on the playback toolbar to enable the synchronous playback.

## Choice 3: Start Fisheye Playback

Select a fisheye camera from the camera list to start playback.

Move the cursor to the display window, and click on the appearing toolbar to enter the fisheye dewarping mode.

Drag on the video to adjust the view angle, and scroll the mouse wheel to zoom in or zoom out the view.

### Choice 4: Start Playback of Favorited Cameras

1. Click on the left navigation bar.
2. Select a parent Favorites, click to add a Favorites under the parent Favorites, and select the camera(s) to be added to Favorites.

   **Note**

   Up to 5 levels of Favorites can be added.
3. (Optional) Select a Favorites, and click → **Share** on the right side of Favorites' name to share it with others.
4. When in Playback window, select a Favorites, and click → **Play All** to start viewing the live view of all the camera(s) added in Favorites.

## 14.1.4 Customize Icons on Playback Window

You can customize the icons shown on the toolbar of the playback window, adjust the icon order and set whether to always display toolbar on the playback window.

**Steps**

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Application** .
2. In the top right corner of the page, click → **Toolbar** .
3. Scroll down to **Customize Playback Tool Bar** section, add or remove the icons to show or hide the icons on the playback toolbar.
4. Customize playback toolbar.
   - Click an icon in the list to add it to the gray frame below to hide the icon. Icons in the gray frame will be hidden in the toolbar of the playback window.
   - Click the icon in the gray frame to add it back to the playback toolbar to show an icon on the toolbar.
5. Drag the icons in the icon list to adjust icon order.

**Table 14-2 Icons on Playback Toolbar**

| | | |
|---|---|---|
| | Audio Control | Turn off/on the sound and adjust the volume. |
| | Capture | Take a snapshot of the current video and save in the current PC.<br>**Note**<br>After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Picture Search** to search |

| | | |
|---|---|---|
| | | the captured picture, and identity verification related with the captured picture. |
|  | Clip | Clip the video files for current playback and save in the current PC. You can save the clipped video as evidence, and set the saving path for the clipped video files. |
|  | Add Tag | Add custom tag for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently. |
|  | Lock Video | Lock the video file to avoid deleting the video file and protect the video file from being overwritten when the HDD is full.<br>**Note**<br>For the camera imported from Remote Site, if the video files are stored on the encoding device locally, you cannot lock the video files. |
|  | Digital Zoom | Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function.<br>**Note**<br>When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function. |
|  | Export | Export the video files of the camera and save them to your PC or connected USB device. You can also save the video file as evidence, and set saving path for the video files. For details about saving video files as evidence and setting saving path, see ***Manual Recording and Capture*** . |
|  | Fisheye Expansion | Available for fisheye camera for entering the fisheye dewarping mode. |
|  | Camera Status | Show the camera's recording status, signal status, connection number, etc. |
|  | Switch Stream | Switch the stream to main stream, sub-stream (if supported), or smooth stream (if supported).<br>If the device supports transcoding playback, start transcoding and you need to set the resolution, frame rate and bitrate for transcoding. |

| | | |
|---|---|---|
| | | **Note**<br>• The smooth stream will show if device supports. You can switch to smooth stream when in low bandwidth situation to make playback more fluent.<br>• Only video files stored in DVR and I-series NVR support transcoding playback. |
| | Enhancement | Adjust the video image including brightness, saturation, etc. |
| | Two-Way Audio | Start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device. |
| | Rotate Image | Rotate a image. |
| | Object Search | Select a person in the image and search for the person. |

**Note**

The icons shown on the toolbar in the display window will vary with the device's capabilities.

6. Click **Save** to save the above settings.

### 14.1.5 Set Video Parameters

You can set network parameters, picture file format, display parameters, etc.

In the left navigation bar of Video Module, select **Video Security** → .

**Table 14-3 Set Video Parameters**

| Area | Parameters | Description |
|---|---|---|
| Set Network Parameters | Network Timeout | The default waiting time for the Client. |
| | Global Stream | Select the default stream type for global usage. |
| | Main Stream Live View / Playback: Window Divisions | When the number of divided windows is smaller than the number you set, the live videos or recorded videos will be displayed by main stream. |
| | Streaming Mode | Set the device access mode as Automatically Judge, Proxy, Directly Access, or Restore Default mode to define how the system accesses all the added encoding devices and decoding devices. |

| Area | Parameters | Description |
|---|---|---|
| | | If you select Proxy, the system will access the device via Streaming Gateway and Management Service, and it is less effective and less efficient than accessing directly. |
| Set File Parameters | Picture Format | Select the file format for pictures captured during live view or playback. |
| | File Saving Path | Set the saving path for the files you will download to your computer (manually recorded video files, captured pictures, etc.). |
| Set Display Parameters | Font Size | Set the font size for resources, views, and favorites. |
| | View Scale | The image display mode in each display window in live view or playback. |
| | Window Scale | The scale of the video in live view or playback. You can set it to 4:3 or 16:9 (default). |
| | Window Division | The number of window divisions. |
| | Display Window No. | Display the window No. in Monitoring module. |
| | Display VCA Rule | When switched on, the VCA rule in the live view and playback will be displayed. |
| | Video Caching | Larger frame caching will result in better video performance. It is determined based on network performance, computer performance, and bit rate. |
| | Enable Highlight | Enable this function to mark the detected objects with green rectangles in live view and playback. |
| | Overlay Transaction Information | When On, displays the transaction information on the live view and playback image. |
| | Wait Prompt for Synchronous Playback | Enable this function to show a prompt of waiting for the synchronous playback. |
| | Overlay Temperature Information | When On, displays the temperature information on the live view and playback image. |
| | GPU Hardware Decoding | When On, enables the GPU decoding for live view and playback to save CPU resources. |

| Area | Parameters | Description |
|---|---|---|
| | Low Frame Compensation | Set the low frame threshold, and when the value is reached, low frame compensation is enabled. |
| | Time Zone | Set the time zone of the client. |
| Set Audio Parameters | Auto Turn On Audio | if enabled, when you play video, the audio will be automatically turned on. |
| Set Toolbar | Customize the icons shown during the live view or playback as needed. If you check **Always Display Toolbar**, the toolbar will always be displayed at the bottom of live view or playback window. | |

## 14.2 Picture Center

In the Picture Center, you can search for captured picture(s) according to the capture schedule, cameras, and capture time, and use time-lapse photography to combine captured pictures to generate a video that shows the movement of a long period time.

### 14.2.1 Configure Picture Storage

Refer to ***Parameters on Edit Camera Page*** .

### 14.2.2 Configure Capture Schedule

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Capture Schedule** .
2. Click + to add a capture schedule.

**Note**

Capture Interval = Capture Cycle (Number of Days) * 24 / Capture Frequency

### 14.2.3 Search for Scheduled Captures

In the top left corner of Control Client, select → **Video** → **Picture Center** → **Scheduled Capture Search** .

Select a capture schedule, resources for capturing, and time, and click **Search**.

Click **Real-Time Capture** to capture pictures of the selected resources in real-time.

### 14.2.4 Time-Lapse Photography

In the time-lapse photography module, you can combine multiple captured images into a video, which shows the obvious change and movement that happened for an extended period of time. You can also download the combined videos to your local PC.

1. In the top left corner of the platform, select → **Video** → **Picture Center** → **Time-Lapse Photography** .
2. Set the material source as **Capture Schedule** or **Local Device**.

   **Capture Schedule**

   The first choice is to select a capture schedule configured on the platform, and select the captured pictures according to the schedule as the material resource. For example, if a project is from March to May, then you can configure a capture schedule of this period first, and then the captured pictures from the capture schedule will be used as the material source.

   **Local Device**

   The second choice is to select pictures captured by encoding device(s) that support time-lapse photography as the material resource.
3. Select a capture schedule and encoding device(s) according to the material source you set in the previous step.

   **Note**

   For encoding devices, you can select cameras whose videos are stored on CVR or pStor.
4. Set **Material Search Total Time** and **Material Search Time for One-Day** to set the time range of searching captured pictures.

   **Note**

   - You can further narrow down the time range by setting the date and time within one day.
   - Every second of a time-lapse video requires at least 25 pictures. It's recommended to set the time period as long as possible.
5. Select the video length to be generated.
6. Move your cursor to a video and click **Download** to download the video. You can view the downloading process in the task center.

### 14.2.5 Configure Scheduled Report

You can add a scheduled report so that captured pictures will be sent regularly via email.

Make sure you have added a capture schedule.

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Scheduled Report** .
2. Click + to add a scheduled report.

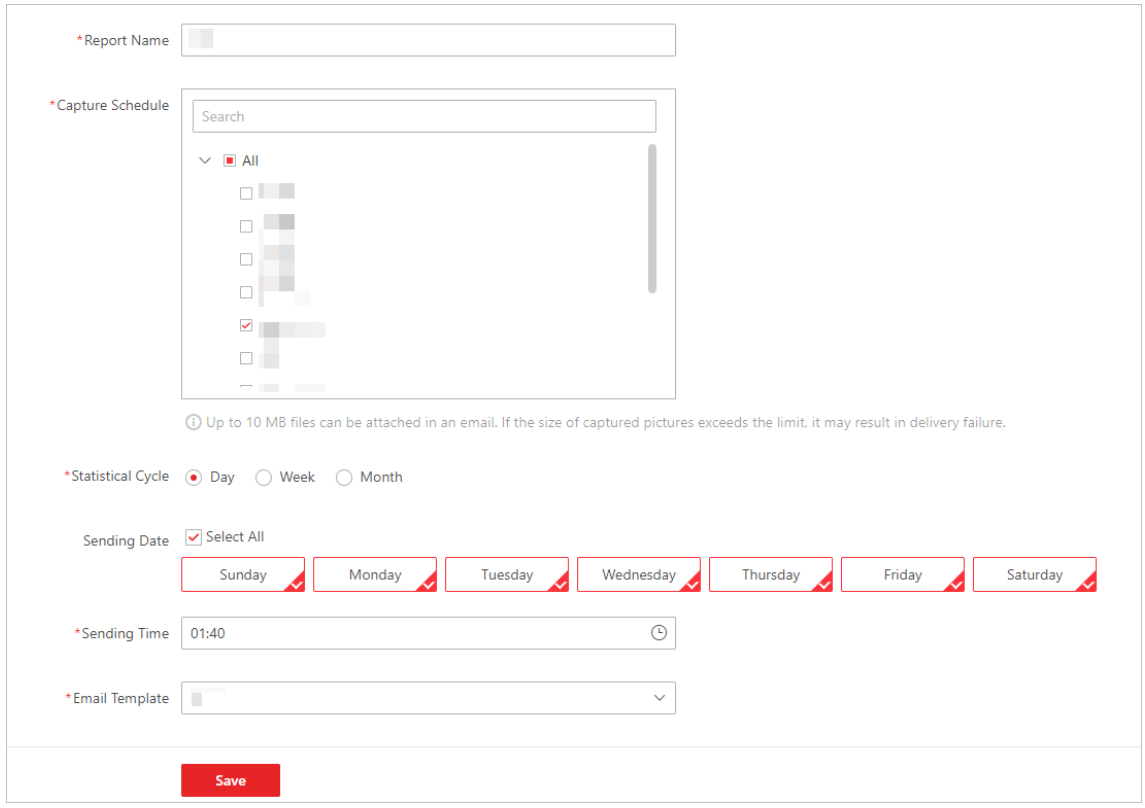



**Figure 14-11 Add a Scheduled Report**

3. Set the required parameters, and click **Save**.

## 14.3 Manage Face Picture Library

The platform supports face recognition and comparison functions. After adding devices which support face recognition, the devices can recognize faces and compare with the persons in the system.

**Steps**

**1.** In the top left corner of the Home page, select → **Video** → **Face Picture Library** .

### 14.3.1 Add Face Picture Library

**Steps**

**1.** Click **Face Picture Library Management** → + to add a single face picture library.

**2.** Click ⇄ to import face picture libraries from encoding devices or facial recognition servers.

**3. Optional:** Click ⇄ to apply a face picture library to a remote site.

### 14.3.2 Add Persons to a Face Picture Library

**Steps**

1. Select a group from the group list.
2. Click **Add → Add New Person** or **Add Existing Person** to add persons to the group.
3. Enter basic information of the person and enable **Face Picture Effective Period** to set when the person information will take effect on the platform.
4. Click on a person's name to add a face picture if the profile picture field is empty.
   - Add from Device: Hover the cursor onto the empty profile picture field, click **Add from Device**, and then select a device.
   - Add by Taking a Picture: Hover the cursor onto the empty profile picture field, and then click **Take a Photo** to take a photo.
   - Add by Uploading Picture: Hover the cursor onto the empty profile picture field, and then click **Upload Picture** to upload a face picture from the local PC.
5. Click **Add** or **Add and Continue**.
6. **Optional:** On the person list page, you can export persons, delete persons, and filter expired persons.

### 14.3.3 Import Persons or Profile Pictures

You can import person information by template, and import profile pictures by zipped profile pictures and from an enrollment station.

**Before You Start**

Make sure you have added the enrollment station to the platform if you want to import pictures from an enrollment station.

**Steps**

1. Select a face picture library.
2. Click **Import**, and click one among **Import by Template**, **Import Zipped Profile Pictures**, and **Import from Enrollment Station**.

**Table 14-4 Import Profile Pictures**

| Method | Description |
|---|---|
| Import by Template | a. Click **Download Template** on the pane to download the template.<br>b. Fill required information into the template, and then click to select the filled-in template from the local PC. |

| Method | Description |
|---|---|
| | c. Check **Replace Repeated Person** to allow the system to overwrite the person information already exists in the face picture library when you import the information.<br>d. Click **Import**. |
| Import Zipped Profile Pictures | Click to select a ZIP file from the local PC, and click **Import**. |
| Import from Enrollment Station | Set the required information, such as device IP address, device port, and password.<br>**Apply Face Information**<br>Import specific face information from the enrollment station to the face picture library.<br>**Copy Back Face Information**<br>Copy back all the face information acquired by the enrollment station to the selected face picture library.<br>**Select File**<br>Click **Download Template** to download a template and fill in it according to its prompts, and then click and select the filled-in template to import specific face information from the enrollment station to the selected face picture library. |

### 14.3.4 Apply Face Picture Library to Device

After setting the face picture library and adding person(s) to the group, you need to apply the group settings to the device which supports face picture comparison so that the camera can compare the detected faces with the face pictures in the face picture library and trigger alarms (if configured). After applying the face picture library to the device, if the data in the group are changed (such as adding a person to the group, removing person from the group, etc.), the platform will automatically apply the data in the group to the device to take effect.

**Before You Start**

- Make sure you have added devices which supports face picture comparison to the system.
- Make sure your license supports facial recognition functionality. Or turn to Home page, select **Maintenance and Management → License Details →** , and then click **Configuration** next to Facial Recognition Camera to added cameras as facial recognition cameras. Otherwise, facial recognition will be unavailable in the system.

**Steps**

**Note**

- You can only apply face picture libraries to cameras which support face picture comparison.
- The maximum number of groups that can be applied to the camera depends on the camera capability.

1. In the top left of the Home page, select → **Video** → **Face Picture Library** → **Applying Center** .
2. Select a facial comparison group from the group list on the left side.
3. Click **Face to Be Applied** to display the to-be-applied face information of the selected group.
4. Apply face information to device(s).
   - Apply Specific Face Information: Select face information, and then click **Apply**.
   - Apply All Face Information in the Group: Click **Apply All**.
5. Select the cameras to apply the selected picture libraries to.
6. Click **Apply** to start applying.

## 14.4 Intelligent Recognition

Intelligent recognition refers to the recognition and analysis of human face, body features, behaviors, vehicles in video images based on intelligent algorithms. The platform will record each recognition and the records can be searched via the Control Client and Mobile Client. The functionality is useful in various scenarios across industries for purposes such as searching for fugitive and finding out security threat.

### 14.4.1 Step 1. Add Task Schedule Template

A task schedule template is used for defining the weekly time arrangement for an intelligent recognition task. An all-day template is available by default. If you apply the all-day template to an intelligent recognition task, the task will be activated 24*7 hours. If the all-day template cannot meet your demands, you can add a custom template as required.

Go to → **Video** → **Intelligent Recognition** → **Task Schedule Template** .

Click + to add a schedule template.

Set required parameters.

| | |
|---|---|
| Draw Task Time | Click **Draw Task Time** and then click a grid or drag the cursor on the time line to draw a time period during which the task is activated. |
| Set Precise Time | Click **Draw Task Time**, move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  . |
| Erase Task Time | Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period. |

### 14.4.2 Step 2: Manage Face Picture Library

Refer to ***Manage Face Picture Library*** .

### 14.4.3 Step 3. Add Intelligent Recognition Tasks

### Add Person Recognition Task

You can add face picture comparison tasks, person feature analysis tasks, and archive analysis tasks here.

**Table 14-5 Add Person Recognition Task**

| Task | Parameters |
|---|---|
| **Add Face Picture Comparison Task**<br>Once a face picture comparison task is added, the security personnel can view real-time matched face information during live view and search face picture comparison records via the Control Client and Mobile Client. | Select **Person Recognition** and click **Add**.<br>**Device for Analysis**<br>Select a type of face picture comparison device.<br>**Select Device**<br>Select a specific face picture comparison device.<br>**Camera**<br>Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list.<br>**Face Picture Library**<br>Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).<br>**Similarity** |

| Task | Parameters |
| --- | --- |
| | Drag the slider to adjust the similarity threshold based on your face picture comparison requirements. The higher the threshold, the preciser the comparison will be. The lower the threshold, the higher comparison rate will be.<br>Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picture comparison record will be generated. |
| **Person Feature Analysis Task** The feature helps you to recognize and record body features of the persons appeared in the fields of view of the cameras linked to the person feature analysis device. Once a person feature analysis task is added, the security personnel can search and view person feature analysis records via the Control Client and Mobile Client. | Select **Person Recognition** and click **Add**.<br>**Device for Analysis**<br>Select a type of person feature analysis device for the execution of person feature analysis.<br>**Camera**<br>Select cameras for detecting persons.<br>**Detection Area**<br>Click **Draw Area** and the drag the cursor on the image to draw an area for detecting persons. |
| **Archive Analysis Task** Once an archive analysis task is added, the platform will save the features and information (including captured picture and video) of the captured person as archive. And the security personnel can search the related archives of a face picture to check the captured pictures or videos of similar persons in the library via the Control Client and the Mobile Client. They can also check whether a person is a stranger. | Select **Person Recognition** and click **Add**.<br>**Device for Analysis**<br>Select the device type for archive analysis.<br>**Camera**<br>Select camera(s) for detecting persons.<br>**Face Picture Library**<br>Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).<br>**Similarity**<br>Drag the slider to adjust the similarity threshold based on your face picture comparison requirements. The higher the threshold, the preciser the comparison will be.<br>Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the |

| Task | Parameters |
| --- | --- |
| | threshold, the detected face will be compared and a face picture comparison record will be generated. |

## Add Vehicle Analysis Task

Vehicle analysis refers to the analysis of vehicle features such as vehicle license plate number and color. You can add a vehicle analysis task to define the conditions such as the device and detection area for vehicle analysis. After the task is added, the specified device will perform vehicle analysis in the specified detection area during the configured time.

Select **Vehicle Analysis** and click **Add**.

**Device for Analysis**

Select a device from the drop-down list for vehicle analysis.

**Camera**

Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list.

**Detection Area**

Define the area for vehicle analysis. Click **Draw Area** to manually draw a specific area on the video image; Click **Draw Area in Full Screen** to make the whole video image as a detection area.

## Add Abnormal Behavior Task

Abnormal event detection analysis refers to the analysis of abnormal events of people, vehicle, and other objects for purposes such as finding out security threat. The available abnormal event analysis types include perimeter protection ( intrusion detection), street abnormal event analysis, prisoner abnormal event analysis, and people density analysis. You can add an abnormal event analysis task to define conditions such as time, device, and detection area for abnormal event analysis. Once an abnormal event analysis task is added, the specified device will perform abnormal event analysis in the specified detection area during the specified periods.

Select **Abnormal Behavior**, click **Add**, and set the parameters.

**Behavior Type**

The behavior types are categorized into different groups based on their usage scenarios, including behavior indoor, behavior on street, people density analysis, and perimeter protection.

**Task Name**

Set the task name.

**Task Schedule Template**

Select a task schedule template from the drop-down list to define the time when abnormal event detection is activated.

**Device for Analysis**

Select a device for abnormal event analysis.

**Camera**

Select camera(s) for detecting abnormal events.

**Detection Area**

Draw an area or line for abnormal event detection.

Take line crossing detection for an example, you need to click **Draw Detection Line** to draw a line on the image, and then set the following two parameters.

**Change Line Crossing Direction**

Set the crossing direction to determine whether line crossing detection is triggered. For example, if you select **Bidirectional**, when a person crosses the line, no matter what direction the person crosses, line crossing detection will be triggered.

**Filter Detection Size**

To set a rough detection area, check **Filter Detection Size** and set a maximum size and/or a minimum size. The areas which are bigger than the set minimum size and smaller than the set maximum size will be set as detection areas.

## Add Target Counting Task

**Table 14-6 Add Target Counting Task**

| Task | Parameters |
|---|---|
| **Frequently Appeared Person Analysis Task** The feature helps you search out the frequently appeared person in a specific area within a specific period. The function is useful for finding out persons who should not have appeared frequently in a specific area. For example, it can be used in a jewelry store for detecting persons who may commit robbery. | Select **Target Counting** and click **Add**.<br>**Device for Analysis**<br>Select the device type for frequently appeared person analysis.<br>**Camera**<br>Select camera(s) for detecting persons.<br>**Face Picture Library**<br>Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).<br>**Time Period**<br>Set a time period for counting the appearance times of a detected person. |

| Task | Parameters |
| --- | --- |
| | **Appeared Times**<br>Set threshold times for regarding a detected person as a frequently appeared person.<br>If the times that a person is detected by the specified camera(s) reaches or exceeds the threshold within the time period you set, he/she will be regarded as a frequently appeared person.<br>**Counting Interval**<br>Set a time interval for filtering out invalid counting.<br>If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.<br>**Similarity**<br>Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be. The lower the threshold, the higher recognition rate will be.<br>Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picture comparison record will be generated. |
| **Rarely Appeared Person Analysis Task** The feature helps you to search out the rarely appeared person in a specific area within a specific period. Rarely appeared person analysis is useful for finding out specific persons who shall appear regularly in a specific area. For example, in a community where many senile people live alone, when a senile person rarely leaves home (i.e., rarely been detected by the cameras in the community), he/she may need living assistance due to health problems. | Select **Target Counting** and click **Add**.<br>**Device for Analysis**<br>Select the device type for rarely appeared person analysis.<br>**Camera**<br>Select camera(s) for detecting persons.<br>**Face Picture Library**<br>Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).<br>**Time Period**<br>Set a time period for counting the appearance times of a detected person.<br>**Reporting Time** |

| Task | Parameters |
| --- | --- |
| | The time when the results of rarely appeared person analysis is reported to system each day.<br>**Appeared Times**<br>Set threshold times for regarding a detected person as a frequently appeared person.<br>If the times that a person is detected by the specified camera(s) is not larger than the threshold within the time period you set, he/she will be regarded as a rarely appeared person.<br>**Counting Interval**<br>Set a time interval for filtering out invalid counting.<br>If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.<br>**Similarity**<br>Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be.<br>Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picture comparison record will be generated. |
| **People Counting Excluding Staff** The task is applied when you want to count people with some of them excluded. For example, if you want to count day customer traffic of a store, but staff are obviously not customers, so only actual customers will be counted instead of all people captured by cameras if you use the task. | Select **Target Counting** and click **Add**.<br>**Camera**<br>Select camera(s) from the Available list, and then click > to add selected one(s) to the Selected list.<br>**Face Picture Library**<br>Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s). |

### 14.4.4 Step 4. Apply Tasks to Devices

In the top left of the Home page, select → **All Modules** → **Video** → **Face Picture Library** → **Applying Center** .

## View Applying Status

You can view the status of the applying of face picture libraries from different perspectives, including the cameras failed to receive face picture libraries, the cameras to which certain face picture libraries need to be applied, the person information failed to be applied, and the person information to be applied.

### Cameras Failing to Receive Faces

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of applying failure, including face picture library, analysis device, and exception details (e.g., the device reaches its maximum face picture library capacity, the face picture library reaches its maximum face picture capacity, face pictures not qualified, etc.) If face pictures are not qualified, you can click to view failure details.
You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

### Cameras to Be Applied To

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of the applying of face picture libraries: the applying status of each face picture library that need to be applied to the camera will be list.
You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

### Faces Failing to Be Applied

Select a face picture library from the group list on the left side to view the face information that fails to be applied to devices, and then click a piece of face information to view its exception details.

### Faces to Be Applied

Select a face picture library from the group list on the left side, and then the faces to be applied will be displayed on the right side.

## Apply Abnormal Applying Record Again

Applying of face information may fail due to various reasons. To ensure recognition of the target persons in your scenarios, it is important to check the abnormal applying records and apply the face information again.

Apply abnormal face applying records again.

- Click **Cameras Failing to Receive Faces**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again.
- Click **Cameras to Be Applied To**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again

- Click **Face Failing to Be Applied**, select a face picture library from the group list on the left, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.
  Click **Export All** to export all persons' information as a compressed Excel file to the local PC. You need to set a password for decompressing the compressed file.
- Click **Faces to Be Applied**, select a face picture library from the group list on the left, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.

## 14.5 AcuSeek Tuning Sample Group

You can fine-tune the AcuSeek model for specific text search queries to improve the accuracy of AcuSeek and reduce false positives (e.g., searching for "a person with a laptop" might incorrectly match people holding trays). After tuning searches on the Desktop Client by providing sample images for the AI to learn from, the samples will be automatically grouped by text and the tuned samples will be displayed on the Web Client.

Go to **Video → Intelligent Recognition → AcuSeek Tuning Sample Group** .

You can view, search for, and delete the terms with tuned results on the page.

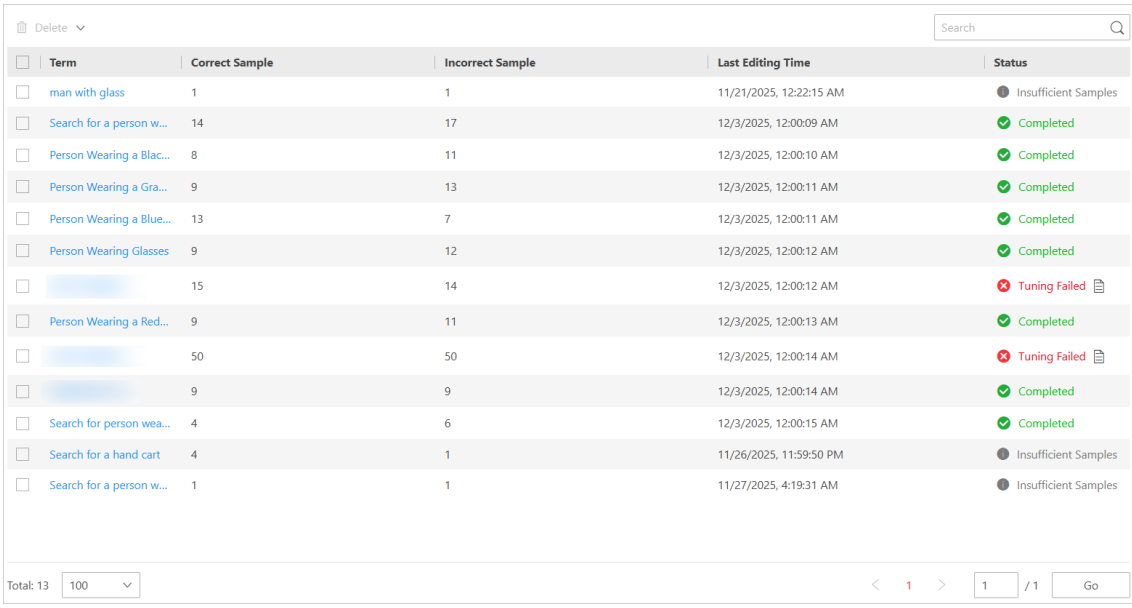



**Figure 14-12 AcuSeek Tuning**

You can tune samples again on the AcuSeek Tuning page.

1. Click a term to open the group details page.
2. Hover on a sample and click ✓ or ⊗ to re-mark the samples as correct or incorrect.
3. Hover on a sample, and click 🗑 to delete the sample.
4. Click **Tune Again** to save the changes.

## 14.6 Video Application

This section introduces advanced features including self-learning library, visual tracking, and person/vehicle arming and panorama tracking.

### 14.6.1 Configure Self-Learning Library

The self-leaning library is a library of false alarm pictures. The library can store those pictures which are identified as false alarms and help you avoid accepting the same kind of false alarms in the future.

In the top left corner of the platform, select → **Security Monitoring → Video → Video Application → Self-Learning Library** .

The devices which support the learn-by-example feature are displayed on the left pane.

Switch the **Learn by Example** feature for a certain device, so that the device can learn false alarms by example.

**Note**

It is recommended that you enable the **Learn by Example** feature to reduce false alarms, and after it is disabled, the self-learning library can still be configured but no longer takes effect.

You can perform the following operations.

| Operation | Description |
|---|---|
| View Applicable Events | Click a device on the left pane, and you can view applicable events on the top of the page. |
| Sort Pictures | Click to sort pictures in ascending or descending order. |
| Filter Pictures | Click to filter pictures by date. |
| Delete Pictures | Check pictures on their top right corner and click **Delete** to delete them. You can also click **Delete All** to delete all pictures. |
| Refresh Page | Click **Refresh** to refresh the page. |

### 14.6.2 Configure Visual Tracking

Visual tracking allows you to continuously track an individual (such as a suspect) across different areas . Before you can use this function, you need to associate a camera (hereafter named as "camera A") with other cameras nearby. After that, icons representing the nearby cameras will be

overplayed on the view of camera A. You can click these icons to redirect to the associated cameras' views during live view or playback.

**Steps**

1. In the top left corner of the platform, select → **Security Monitoring → Video → Video Application → Visual Tracking** .
2. Select an area from the area list.

   The page will display the thumbnails of the latest view of the cameras that support visual tracking settings in the selected area.
3. **Optional:** Check **Include Sub-Area** to display the available cameras in the sub-area(s) of the selected area.
4. Select **Not Added** and select a main camera.

   **Note**

   Up to 16 cameras can be linked.
5. **Optional:** Select **Configured** to edit the configured cameras.

**Example**

Visual Tracking in Hallway

The following picture shows the monitoring image of camera A in a hallway. There are three directions: B, C, and D, and each direction is monitored by camera B, C, and D respectively.

In this case, you can drag camera B to the B position so as to overlay the icon of camera B on the monitoring image, and then do similar operations for camera C and camera D. After that, when an individual passes by the hallway and turns to direction B, the security personnel can click the icon of camera B on the view of camera A to redirect to the view of camera B.




**Figure 14-13 Monitoring Image of Camera A**

## 14.6.3 Configure Person/Vehicle Arming

You can add a group with multiple cameras with the person/vehicle arming capability in it, and when a person or vehicle of interest is detected, the cameras will follow the target consecutively.

In the top left corner of the platform, select → **Security Monitoring → Video → Video Applications → Person/Vehicle Arming** .

Person/Vehicle arming groups are groups containing multiple cameras. The cameras are added to the same group so as to work cooperatively to track a vehicle or person target.

### Set Arming Group Information

1. Click **Add Person/Vehicle Arming Group** or **View Service Details → Add Person/Vehicle Arming Group** , and set a name for the arming group.
2. Select the arming type as person arming or vehicle arming. Person arming is to track target persons while vehicle arming is to track vehicles.
3. Select cameras to add them to the group. After a person or vehicle of interest is detected, the cameras will track the target consecutively.
4. (Optional) If you select person arming, drag the slider to adjust the similarity threshold or enter a value to set a similarity threshold. When a person is above the similarity with a target, the cameras in the group will start to track the person.
5. (Optional) If you select vehicle arming, select presets for each camera.
6. Click **Save and Next**.

### Set Target Information

1. Click **Add**, and select persons or license plate numbers of vehicles.
2. Click **Add** and the persons / license plate numbers will be applied to the devices. If applying to the device succeeds, you can see the target information show up on the page. If failed, check the items and click **Apply Again** to apply them again.
3. Click **Finish**.

## 14.6.4 Configure Panorama Tracking

Panorama tracking is a target tracking function based on the linkage between a bullet/box camera and a speed dome. After you configure panorama tracking on the Web Client, the security personnel will be allowed to enable this function during the live view of the bullet/box camera on the Control Client. If this function is enabled, when a Video Content Analysis (VCA) event is detected by the bullet/box camera, or the security personnel manually select a target, the bullet/box camera will work together with the speed dome to locate, zoom in, and track the target.

**Before You Start**

Make sure you have added the device supporting this function.

**Steps**

1. In the top left corner of the Home page, select → **Video → Video Application → Panorama Tracking** .
2. Select one area on the area list.
3. At the thumbnail center, click **Configure Panorama Tracking** to open the Panorama Tracking Settings window.

4. **Optional:** Click **Unlock PTZ** to unlock the PTZ and pan, tilt, and zoom the image to adjust the monitor range.

**Note**

The feature should be supported by device.

5. **Optional:** Select an elevation range which defines the allowed range of tilting.

**Note**

The feature should be supported by device.

6. **Optional:** Select **Manual Calibrating** or **Auto Calibrating** as calibration mode and click **Next**.
7. Calibrate the camera and the linked speed dome, and then click **Next**.
   - **Manual Calibrating**: In Manual Calibrating mode, click **Add Calibration Point**, and click the position on the left image of box/bullet camera to add a calibration point. Select the calibration point, and then pan, tilt, and zoom in or out the view of speed dome by digital zoom and PTZ control to make sure the live view of speed dome and the target position of the camera are mostly same.

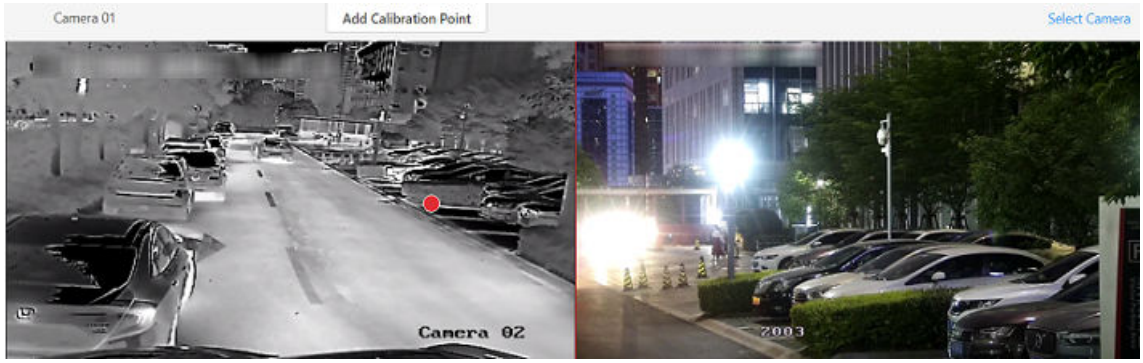



**Figure 14-14 Manual Calibrating**

**Note**

- You can repeat the operations to add more calibration points. At least 4 calibration points should be added. It is recommended to add at least 9 calibration points in one scene. For higher tracking precision, up to 12 calibration points are required.
- Click the added calibration point, and you can move it to other position, or delete it.
- It is recommended to place calibration points at distinct positions in live image (for example, corners). If no distinct position is available, you can place the points at something (for example, box, stool, or people) to mark the position.

   - **Auto Calibrating**: In Auto Calibrating mode, click **Start Calibration** to add calibration points automatically.

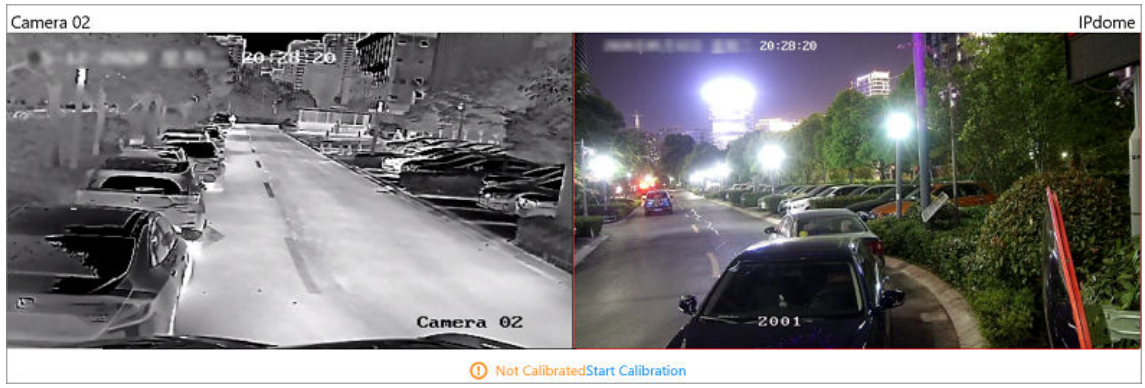



**Figure 14-15 Auto Calibrating**

**Note**

You should avoid using auto calibrating for vast similar scenes (for example, lake, lawn, or public square) or dark scenes (for example, night scenes).

8. Set other parameters.

**Auto-Tracking**

If **Auto-Tracking** is checked, when the VCA event is triggered during live view, the speed dome will track the target automatically.

**Note**

You need to configure VCA rule for the bullet/box camera on the device. For more details, refer to the user manual of the device.

**Target Tracking Mode**

**Track One Target Continuous**

The speed dome tracks the target continuously until the target disappears in the scene.

**Track One Target for Certain Duration**

Select this mode and set the duration of tracking. The speed dome switches to next target after the set duration time.

**Set Tracking Initial Position**

Select a preset as tracking initial position, or adjust the view by PTZ control and click **Save** to save the preset as tracking initial position. When tracking finishes or timed out, speed dome returns to the tracking initial position. When tracking initial position is not set, the speed dome stays where tracking finishes or timed out.

9. Click **Save and Test** to finish configuring panorama tracking.

To test the panorama tracking settings, click or draw a rectangle on the video of box/bullet camera, and the speed dome will show the close-up view.

10. **Optional:** After configuring panorama tracking, perform the following operations.

| | |
|---|---|
| **Edit Panorama Tracking Settings** | Click **Edit** to reconfigure panorama tracking. |
| **Cancel Panorama Tracking** | Click **Cancel Panorama Tracking** to delete all configurations about panorama tracking. |

## 14.7 Video Overview

The Video Overview page displays the brief information such as health status of different resources, face picture applying status, and face capture event. You can jump to other pages such as device management, maintenance, event and alarm configuration, and applying center.

In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Overview** .

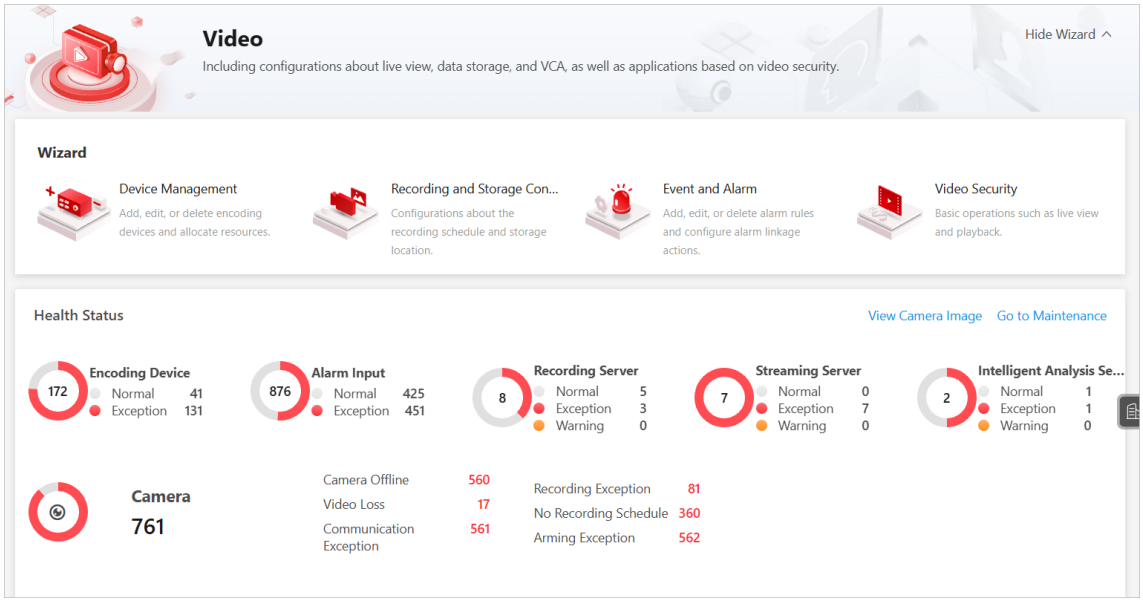



**Figure 14-16 Video Overview**

The following operations are supported.

| Operation | Description |
|---|---|
| Go to Other Pages | Hover the cursor on the module name (such as **Device Management**, **Recording and Storage Configuration**, **Event and Alarm**, and **Video** |

| Operation | Description |
|---|---|
| | **Security**) in Wizard panel and click ↗ to go to the corresponding page. |
| Go to Resource Status Page of a Resource Type | • Click the total number of one type of resources to go to the status page of that type of resources.<br>• Click the number of one type of resources in a certain exception status to go to the status page of that type of resources in the corresponding exception status. |
| View Camera Images | Click **View Camera Image** to view images of all cameras. |
| Go to Maintenance Module | Click **Go to Maintenance** to go to the Maintenance module. For further operations, refer to ***Maintenance*** . |
| Go to Applying Center | Click the face picture applying status in Face Picture Applying Status panel to go to ***Applying Center*** . |
| View Face Capture Event Details | View the information (such as profile picture, capture time, and event source) about captured face pictures in Face Capture Event panel. |

# Chapter 15 Parking Management

HikCentral Professional provides parking management services covering entry & exit rule management, parking fee rule management, and so on. The platform can perform relevant operations according to the rules you set.

On the Web Client, you need to create a parking lot and set its entrances and exits as well as lanes according to actual needs. For vehicles managed in the platform, you can predefine parking fee rules and entry & exit rules for them. For vehicles not managed in the platform, you can also set an entry & exit rule to define how to open the barrier when these vehicles are detected at the entrances and exits.

Upon synchronization of remote site parking lot resources (including parking lot information, lanes, and entrances/exits) to the Central System, it enables centralized parking management across multiple locations. Functions include parking spaces real-time monitoring via site-linked cameras, simultaneous viewing of resources from multiple remote sites, remote barrier control, and consolidation of real-time vacancy data for operational analysis.

On the top navigation bar, select → **Passing Management** → **Parking Lot** .

## 15.1 Flow Chart of Parking Lot Management

The flow chart below shows the overall process of parking lot management.

**Note**

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

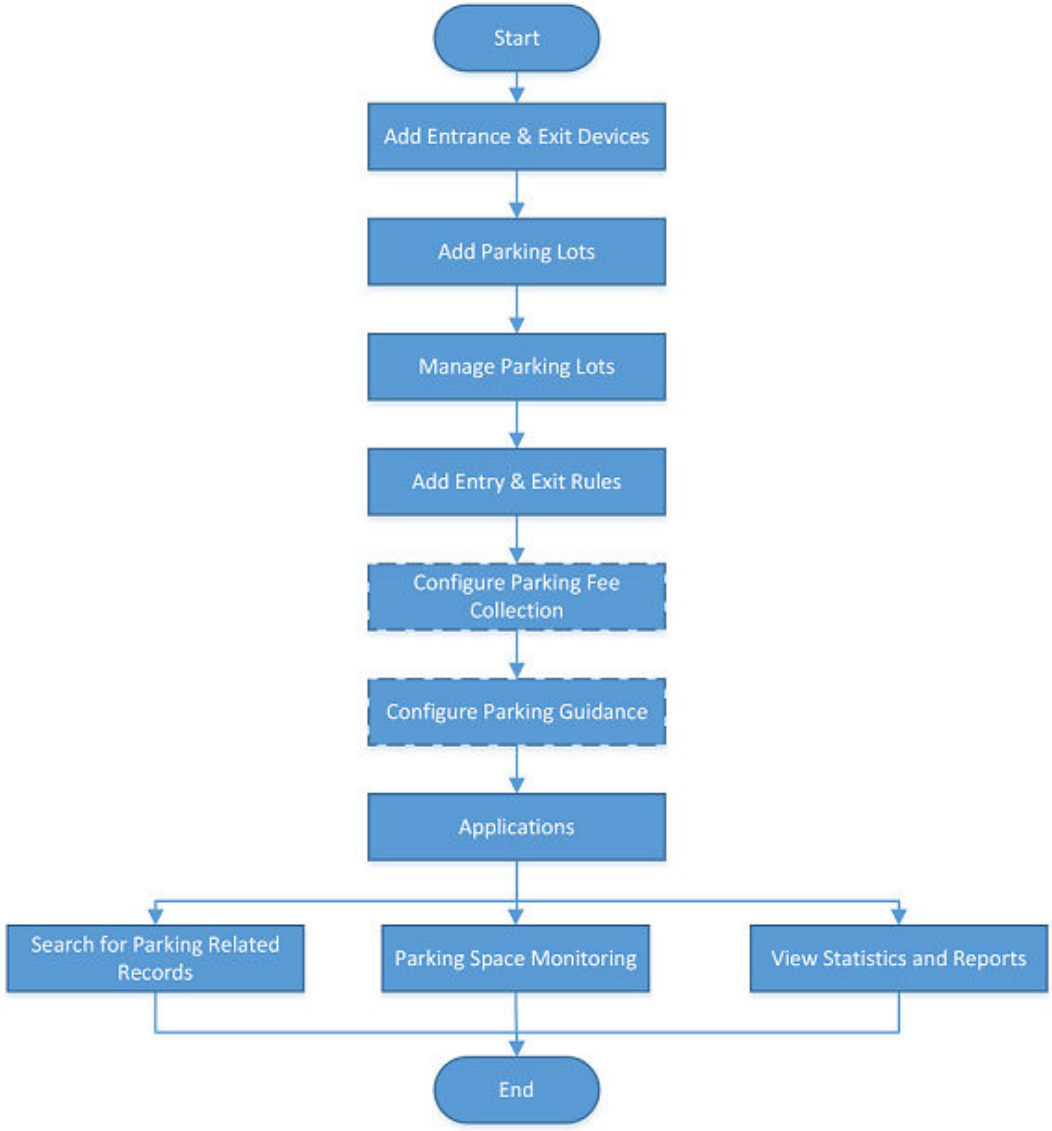



**Figure 15-1 Flow Chart of Parking Lot Management**

| Procedure | Description |
|---|---|
| Add Entrance & Exit Devices | Add the relevant devices, such as cameras, entrance/exit control devices, display screens, etc., to the platform via the Resource Management module according to your needs. |
| Add Parking Lots | Refer to ***Add Parking Lot*** for details about how to add parking lots to the platform. |
| Manage Parking Lots | After adding parking lots, you can add entrances and exits to the platform, add lanes for linking different devices to realize different |

| Procedure | Description |
|---|---|
| | functions, and link display screens to parking lots. Refer to ***Add Entrance and Exit*** , ***Add Lane*** , and ***Link Display Screen and Set Displayed Content*** respectively for more details. |
| Add Entry & Exit Rules | An entry & exit rule defines how the barrier gate opens when the platform detects a vehicle at the lane. The barrier gate can be set to open automatically when a vehicle is detected or you can also open it manually by clicking the **Allow** button on the Control Client after verifying its identity. Refer to ***Configure Entry & Exit Rules*** for details. |
| Configure Parking Fee Collection | If the parking lot is a paid parking lot that charges money for parking, you can configure rules for how to calculate and collect the parking fees. Refer to ***Flow Chart of Parking Fee Collection*** for details. |
| Configure Parking Guidance | For parking lots with guidance terminals and display screens, parking guidance can be configured so that the guidance terminal can link with multiple parking cameras for management, and the display screen displays the number of vacant parking spaces in a parking lot to guide drivers to those parking spaces. Refer to ***Flow Chart of Parking Guidance Configuration*** for details. |
| Applications | After completing the above-mentioned configurations, you can perform operations such as monitoring parking spaces, searching for parking related records, and viewing the relevant statistics and reports. For details, refer to ***Parking Space Monitoring*** , ***Record Search*** , and ***Statistic and Report*** respectively. |

## 15.2 Flow Chart of Parking Fee Collection

For paid parking lots that require a certain fee to park, the flow chart below shows the process of configuring parking fee collections.

**Note**

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

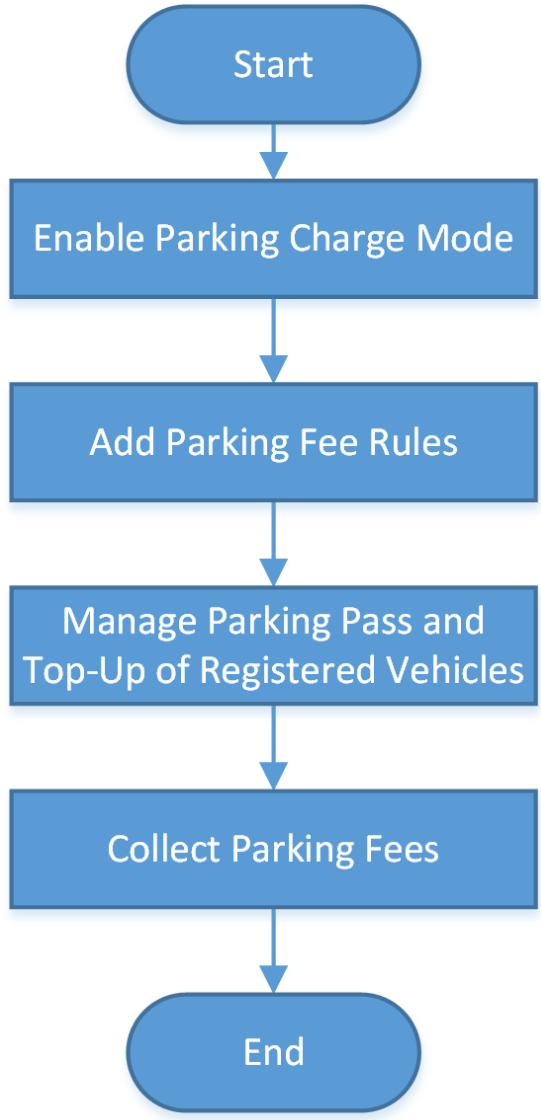



**Figure 15-2 Flow Chart of Parking Fee Collection**

| Procedure | Description |
|---|---|
| Enable Parking Charge Mode | To enable parking pass top up for registered vehicles or to charge other vehicles for temporary parking, you need to set the parking fee mode to Charge. Refer to ***Enable Parking Charge Mode*** for details. |
| Add Parking Fee Rules | You can set parking fee rules for a parking lot, including rules for certain types of vehicles, the parking pass rule, the discount rule, the parking fee rule for abnormal entry & exit, and the parking receipt template. Once you set a rule, the platform will automatically |

| Procedure | Description |
|---|---|
| | calculate the fee for parking based on this rule and present the parking fee related information. Refer to ***Configure Parking Fee Rules*** for details. |
| Manage Parking Pass and Top-Up | If a vehicle is topped up with a parking pass of a parking lot, it can enter and exit that parking lot as a registered vehicle and park without paying any additional fees. Refer to ***Top Up Parking Pass*** for details. |
| Collect Parking Fees | Registered vehicles can park in a parking lot without paying additional fees if they have been topped up with a parking pass, whereas other vehicles (e.g., temporary vehicles, vehicles in list, and vehicles with abnormal entries/exits) can pay for parking at the booth or in the toll center by searching for their parking information by license plate No., swiping the temporary card, or scanning the parking receipt. Refer to ***Pay in Toll Center*** for details. |

## 15.3 Flow Chart of Parking Guidance Configuration

The flow chart below shows the process of configuring parking guidance for parking lots with guidance terminals and display screens to guide drivers to vacant parking spaces.

**Note**

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

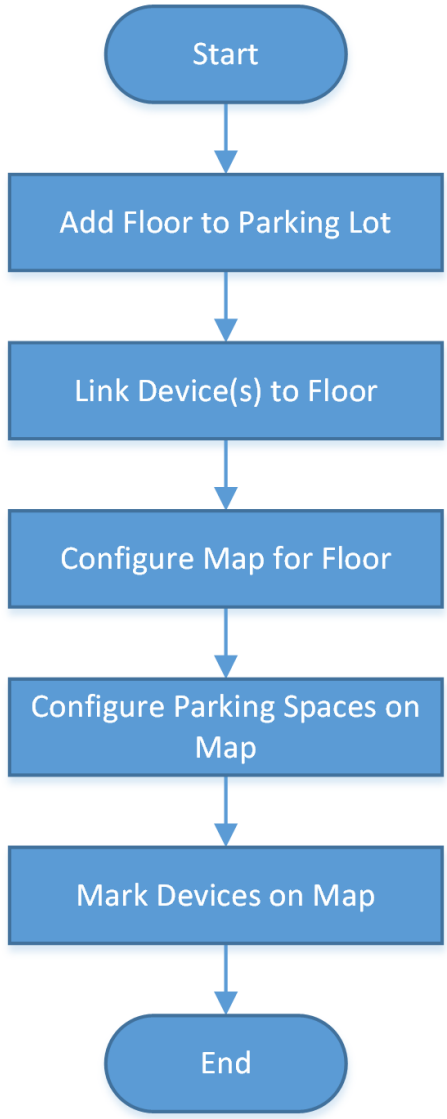



**Figure 15-3 Flow Chart of Parking Guidance Configuration**

Refer to ***Parking Guidance Configuration*** for details about each step.

## 15.4 Manage Parking Lot

Parking lot is a parking facility that is intended for parking vehicles. You can add one or multiple parking lots to the platform and set entrances and exits as well as lanes for them according to actual needs.

There are three elements in the parking management platform:

**Parking Lot**

A parking facility that is intended for parking vehicles. The platform supports adding multiple parking lots and you need to create them at the very beginning.

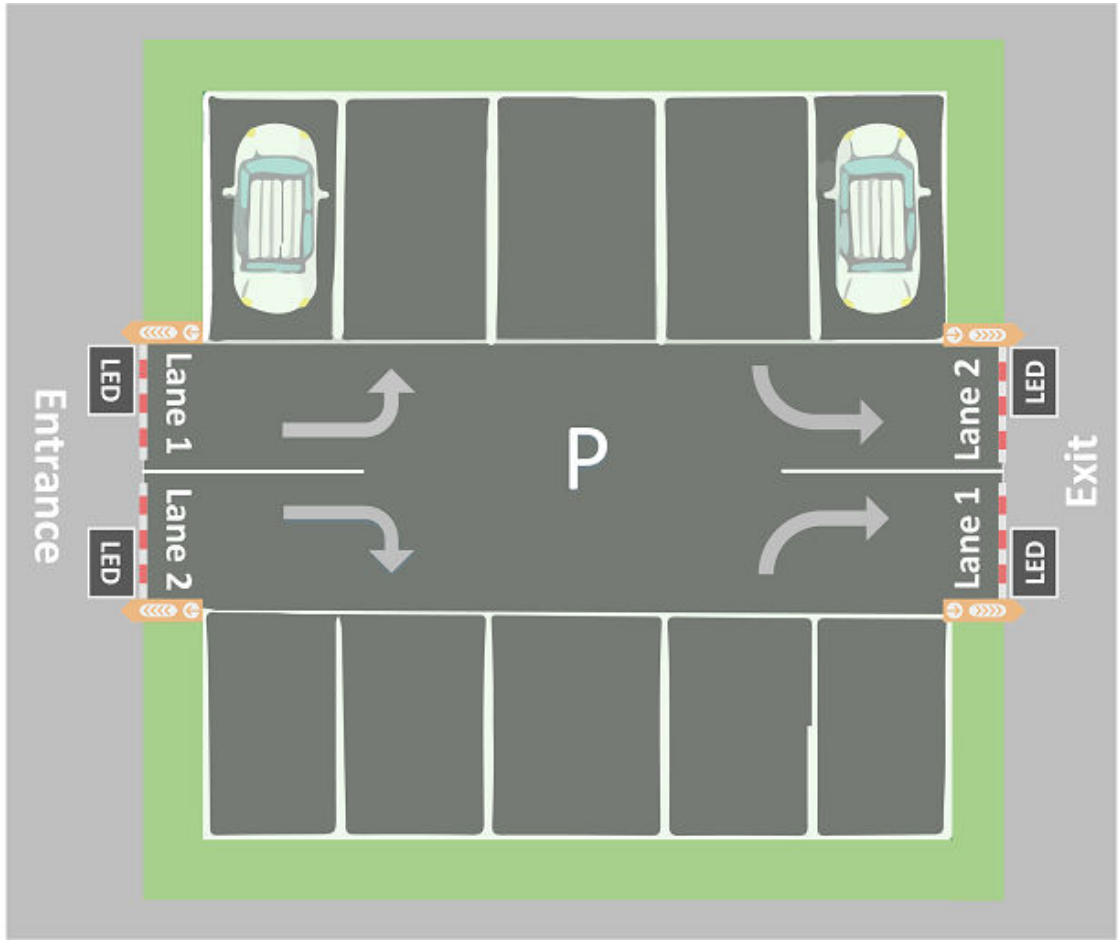
**Entrance & Exit**

The vehicles can enter or exit the parking lot via entrance & exit.

**Lane**

Each entrance or exit should contain at least one lane. The lane can be related with devices, including the capture unit, access control device, video intercom device, guidance screen, and entrance/exit station, which can be used for capturing and recognition, identity verification, video intercom, parking guidance, and barrier control. See ***Add Lane*** for details.

The two pictures below shows the typical relation of parking lot, entrances & exits, and lanes.



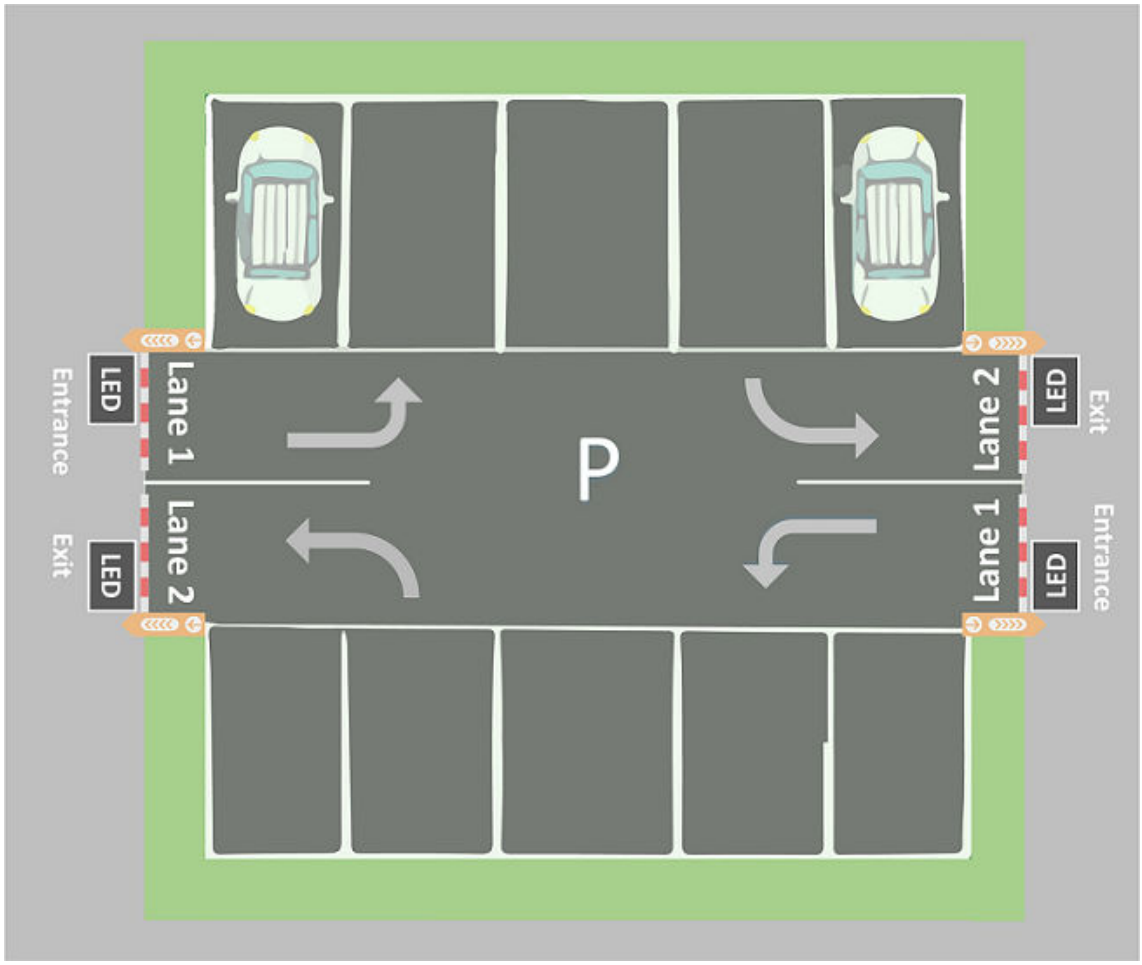



**Figure 15-4 Parking Lot**

### 15.4.1 Parking Lot Overview

On the Parking Lot Overview page, you can view different information about the parking lot, including the occupancy statistics of parking spaces, the number of daily entries and exits, the health of devices, etc. You can also go to different pages via hyperlinks to view detailed information.

**Occupancy:** You can view the total number of parking spaces, the number of vacant parking spaces, and the occupancy statistics of different types of parking spaces. You can click **Parking Space Overview** to go to the Parking Space Overview page and view more detailed statistics of parking spaces. See ***Parking Space Monitoring*** for details.

**Today's Entries & Exits:** You can view the number of daily entries and exits, the entry/exit trend, and the number of entries and exits at different entrances and exits.

**Vehicle Passing Event:** You can view the vehicle-passing information of the parking lot. If you are managing more than one parking lot, you can click the name of a parking lot to view its detailed vehicle-passing information.

**Device Monitoring:** You can view the health of devices related to the parking lot, including guidance terminals, parking cameras, and display screens. You can also click **Maintenance** to go to the Maintenance page and view more detailed statistics of the health of devices. See ***Maintenance*** for details.

**Other Parking Lot Entrance & Exit:** In the lower-right corner, you can view the list of devices linked to lane(s) for other parking lot(s). You can click **Configure Now** to configure settings of the parking lot.

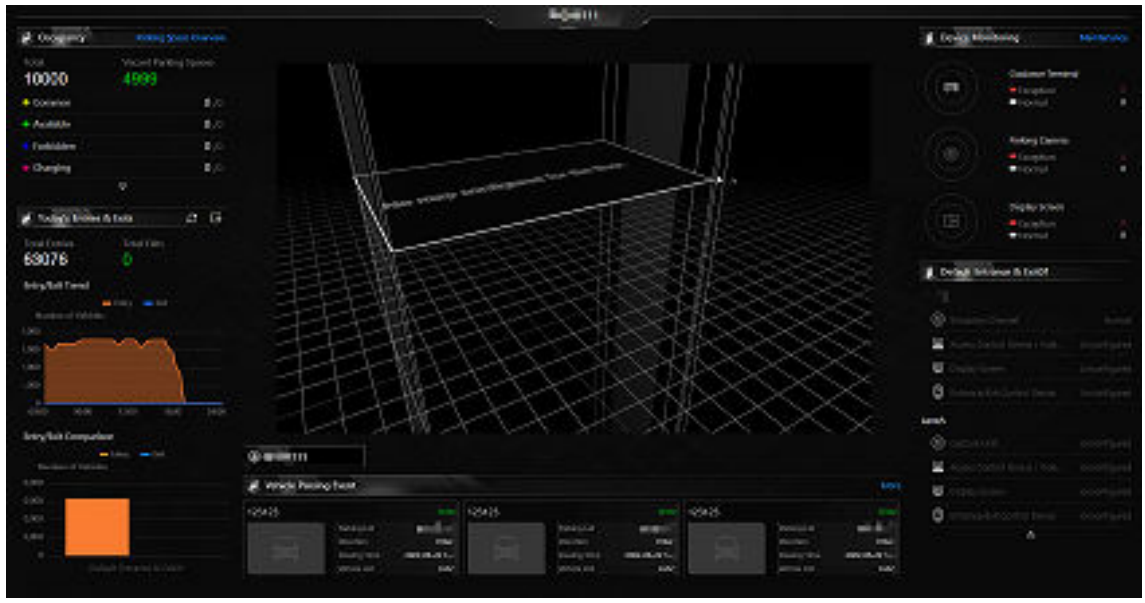



**Figure 15-5 Parking Lot Overview Page**

## 15.4.2 Add Parking Lot

You can add one or multiple parking lots for management, including adding entrances and exits, setting the number of parking spaces, editing the parking lot formation, setting entry & exit rules and parking fee rules.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. In the top right corner of the page, click **Add Parking Lot** to open the Add Parking Lot pane.

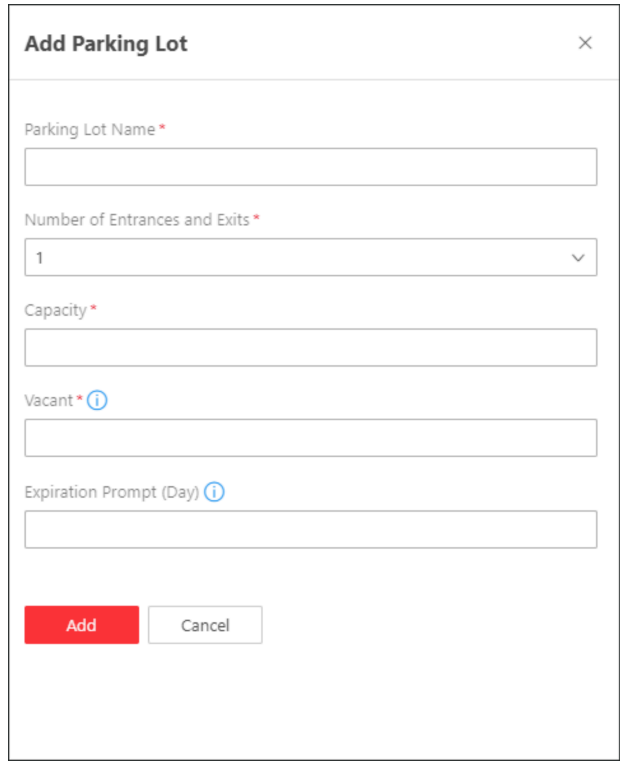



**Figure 15-6 Add Parking Lot**

3. Set the parking lot name, number of entrances and exits, the total parking capacity, etc.

   **Expiration Prompt (Day)**

   Take a vehicle that expires on Jan. 6th, 2023 as an example, if you enter 5 here, the expiration prompt will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2023 to Jan. 5th, 2023.

4. Click **Add** to create the parking lot.
5. **Optional:** Edit the parking lot.

| | |
|---|---|
| **Edit the Number of Vacant Parking Spaces** | In a parking lot area, click above **Vacant** to edit it. |
| **Edit the Number of Vacant Parking Spaces for Registered Vehicles** | In a parking lot area, click above **Vacant Parking Spaces for Registered Vehicles** to edit it. |
| **Edit Parking Lot Information** | a. In a parking lot area, click **Settings → Basic Information** .<br>b. In the upper-right corner, click **Edit** to open the Edit Parking Lot pane. |

**Note**

You can also click on the top of the parking lot list to edit its information.

c. Edit the information of the parking lot, such as the name, capacity, etc.
d. Click **Save**.

**Add Allowed Parking Duration**

a. In a parking lot area, click **Settings → Basic Information** .
b. On the right side of **Allowed Parking Duration**, click **Add**.
c. In the pop-up window, select a vehicle category (such as temporary vehicle and visitor vehicle).
d. Enter the maximum parking duration allowed for the selected vehicle category parked in the created parking lot.

**Note**

You can configure an event or alarm which will be triggered when a vehicle's parking is due. For example, if you enter 300 here, an event or alarm (if any) will be triggered if a vehicle of the selected type has parked longer than 5 hours (i.e., 300 minutes).

**Add/Edit/Delete a Sub Parking Lot**

In a parking lot area, click **Settings → Basic Information** .

- On the top of the parking lot list, click to add a sub parking lot.
- Select a sub parking lot, and click on the top of the parking lot list or **Edit** in the upper-right corner to edit it.
- Select a sub parking lot and click on the top of the parking lot list to delete it.

## 15.4.3 Add Entrance and Exit

An entrance or exit helps control vehicles to enter/exit the parking lot or prevent vehicles from entering/exiting the parking lot. For example, the entrance or exit allows a vehicle in the allowlist to enter/exit the parking lot, and prevent a vehicle in the blocklist from entering the parking lot. You need to configure lanes linked with devices for an entrance and exit to control the barriers.

**Before You Start**

Make sure you have added a parking lot. See ***Add Parking Lot*** for details.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the configuration page of this parking lot.
3. Select a parking lot from the left list and click .

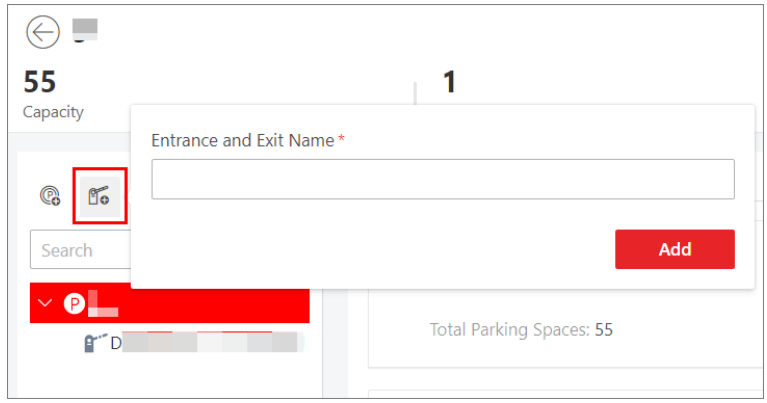



**Figure 15-7 Add Entrance and Exit**

4. Enter the name of the entrance and exit.
5. Click **Add**.
6. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Edit an Entrance & Exit** | Select an entrance & exit, and click to edit it. |
| **Delete an Entrance & Exit** | Select an entrance & exit, and click to delete it. |

**What to do next**
Add lane for the entrance and exit. See ***Add Lane*** for details.

## 15.4.4 Add Lane

A lane links various devices to perform specific functions. For example: a lane linked with an entrance/exit control device manages vehicle entry and exit; a lane linked with a capture unit (which can recognize a vehicle at the lane and compare the vehicle information with vehicles in a vehicle list) or card-swiping device (e.g., access control or video intercom device) controls the barrier; a lane linked with a camera captures pictures; a lane linked with a display screen shows information such as the number of vacant parking spaces.

### Prerequisites

Make sure you have added at least an entrance/exit for the parking lot. See ***Add Entrance and Exit*** for details.

### Add Lane

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the configuration page of this parking lot.
3. Select an entrance & exit from the left list.
4. Click to enter the Add Lane page.

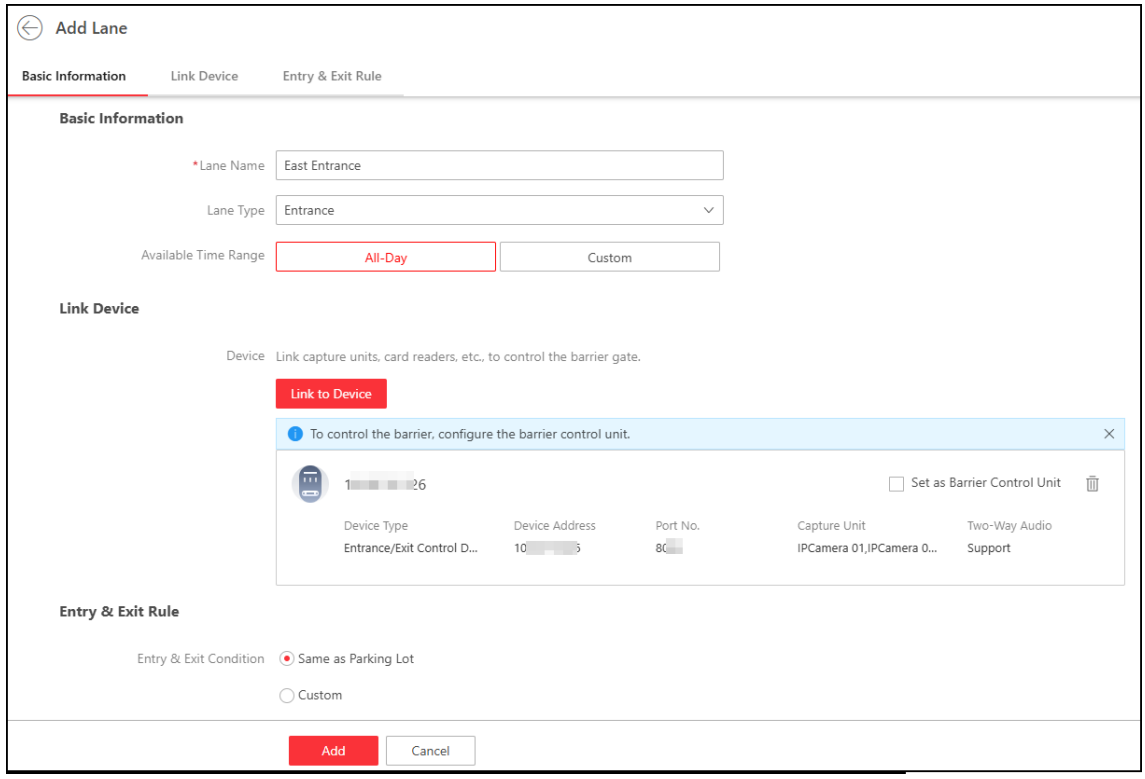



**Figure 15-8 Add Lane Page**

5. Set the lane basic information.

   **Lane Name**

   Create a name for the lane.

   **Lane Type**

   Set the lane as **Entrance** or **Exit**. Entrance lanes are for incoming traffic, and exit lanes are for outgoing traffic.

   **Available Time Range**

   Set the period during which the lane is available.

6. In the Link Device area, click **Link to Device** to link device(s) such as entrance/exit control devices, capture units, and access control devices to the lane.

**Note**

Barrier control requires designating a capable device as the control unit.

- Entrance/Exit Control Device
  An entrance/exit control device manages the entry or exit of a parking lot, especially unattended ones. After a vehicle takes a ticket or card from the device, it controls the barrier to open for entry; after the vehicle returns the ticket or card, it allows exit. Additionally, if the

device issues cards instead of tickets, its guidance screen is configurable. See ***Link Display Screen and Set Displayed Content*** for details.

- Capture Unit
  A capture unit captures and recognizes license plates to control barrier. For example, it opens the barrier to allow entry upon recognizing a license plate number in the vehicle list, and remains closed to deny entry if the plate is in the blocklist. See ***Configure Entry & Exit Rules*** for details about setting an entry & exit rule.

**Note**

You can link up to two capture units to a lane. If two units are linked, set the **Matching Time**. When both capture a plate within this time, the picture with the higher confidence value is kept.

- Linked Camera
  Linked cameras are only used to capture images upon vehicle entry/exit. These snapshots can be viewed within the vehicle-passing information.

**Note**

- Make sure you have enabled picture storage for the camera; otherwise, captured pictures will not be available. .
- Up to three different cameras can be linked to a lane. One camera can be linked to multiple lanes.

- Access Control Device
  If an administrator selects a card (already issued to the owner) when adding the owner's vehicle, the card is bound to the vehicle's license plate number. The barrier opens when the owner swipes the card on the access control device at the lane. In this case, a capture unit is not required.

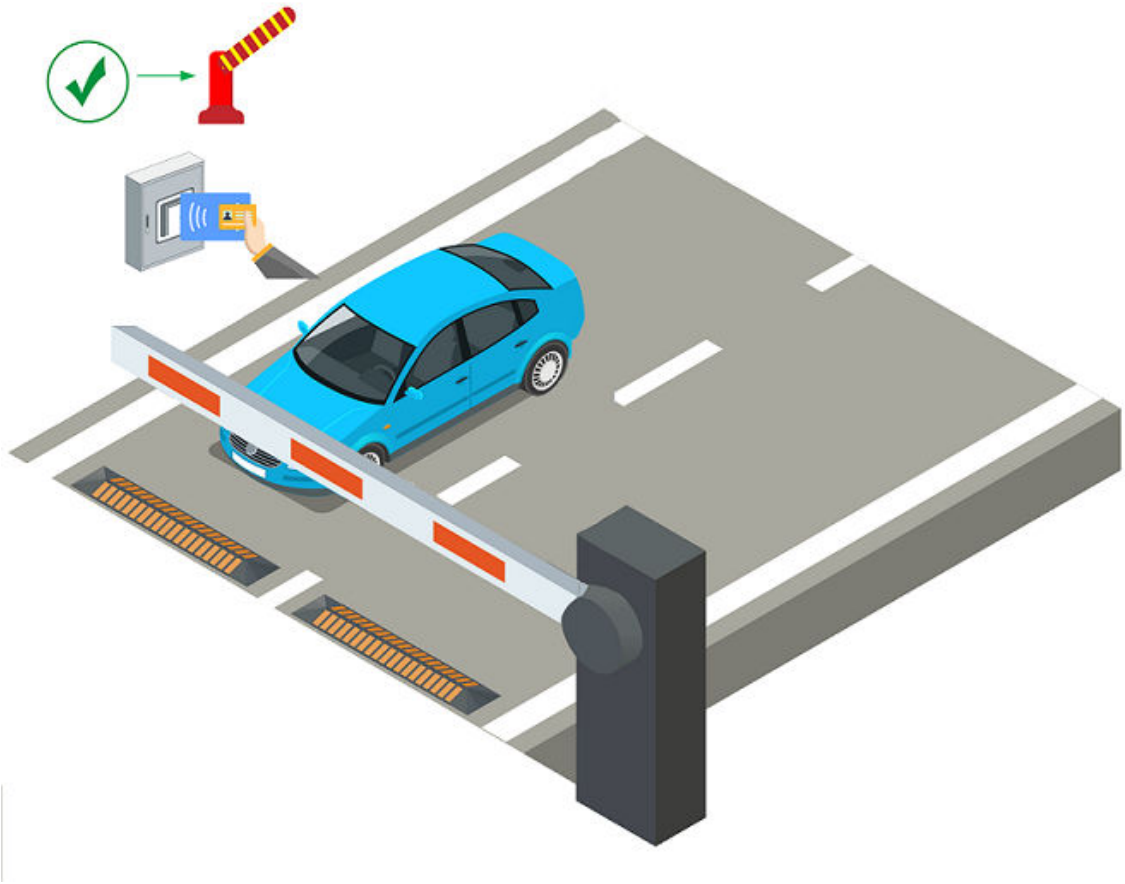


**Figure 15-9 Opening Barrier by Card Swiping**

- Video Intercom Device
  a. The vehicle owner calls the security guard via the video intercom device (some access control devices also support video intercom).
  b. The security guard verifies the owner's identity via the video intercom or by checking the license plate captured by a capture unit.
  c. The security guard opens the barrier manually when the owner is authenticated.

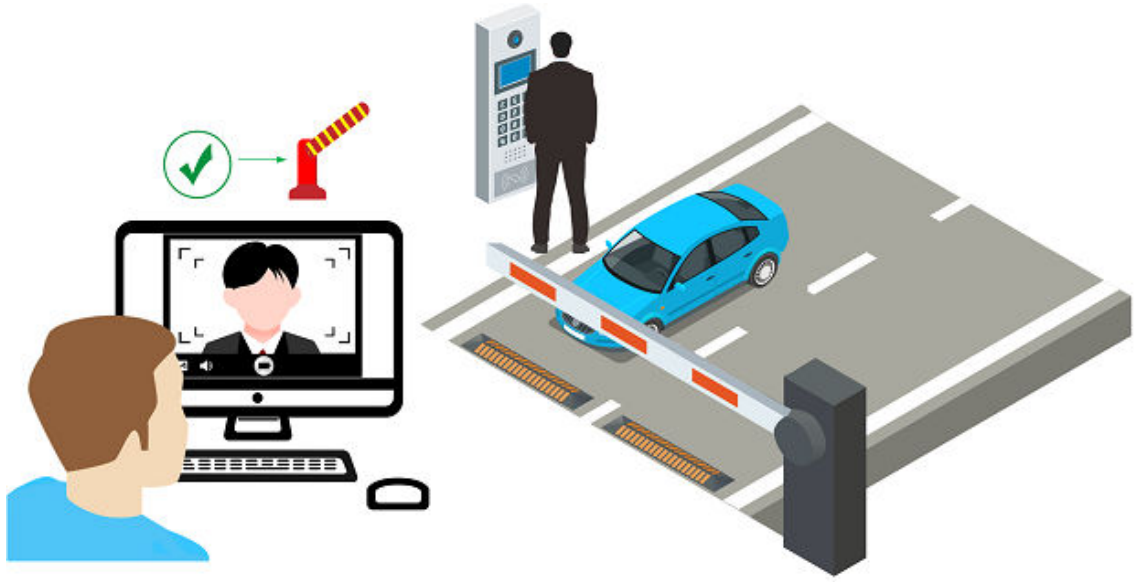


**Figure 15-10 Opening Barrier by Video Intercom**

- Display Screen
  A display screen shows information such as the number of vacant parking spaces and parking permission expiration dates. See ***Link Display Screen and Set Displayed Content*** for details.

7. In the Entry & Exit Rule area, set the entry & exit condition (that is, vehicle passing authentication mode) and entry & exit rules for different vehicle categories.
   You can select **Same as Parking lot** to use the same settings of the parking lot, or **Custom** to set a new rule. For how to configure entry & exit rules, refer to ***Configure Entry & Exit Rules*** .

## Configure Lane Linked Devices

**Note**

Some functions depend on the device capabilities.

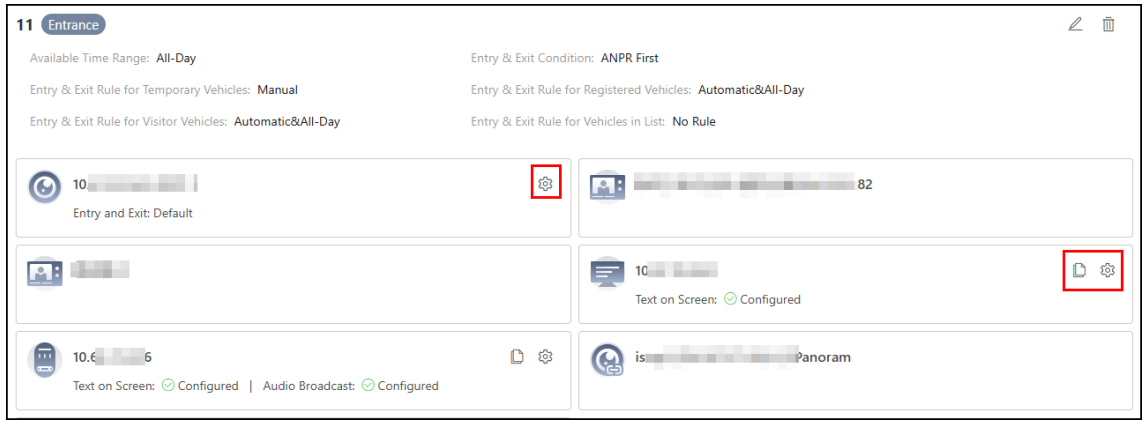



**Figure 15-11 Lane Details**

| Operation | Description |
|---|---|
| Set Display Content on Screen | 1. Click next to the device.<br>2. Click **Display Settings** and set the display content for different vehicle categories. See ***Link Display Screen and Set Displayed Content*** for details. |
| Set Device Audio Broadcast | **Note**<br>Make sure that audio files are already applied to the devices. See ***Audio Media Library Management*** .<br>1. Click next to the device.<br>2. Click **Audio Broadcast**, select a vehicle category, and select an audio file for it.<br>The device will play the selected audio when vehicles in this category are recognized.<br>3. You can also set audio files for specific scenarios (e.g., no vacant parking spaces and expiring parking permissions). |
| Copy Configurations to Other Lanes | Click next to the device, select items to copy, and choose a target lane.<br>**Note**<br>Only lanes with linked devices supporting the matching capabilities are available. |
| Set Driving Direction | When a single capture unit controls the barriers of two lanes, you can set the traffic direction for the capture unit to recognize the front or rear license plate. |

| Operation | Description |
|---|---|
| | 1. Click next to the device.<br>2. Set the driving direction.<br>- **Default**: Defaults to forward.<br>- **Forward**: Recognize the front license plate (vehicle approaching the camera).<br>- **Reverse**: Recognize the rear license plate (vehicle moving away from the camera). |

### 15.4.5 Link Display Screen and Set Displayed Content

The display screen linked to the parking lot can be used for displaying information including the date and time, parking duration, license plate number, expiration prompt, etc.

**Note**

Make sure you have added display screens to the platform.

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the parking lot configuration page.
3. Click **Display Screen Configuration**.
4. Click **Relate Display Screen** and select a display screen on the Relate Display Screen pane to link a screen to the parking lot.
5. Click **Display Screen Configuration** beside the name of the display screen.

### Configure Entrance and Exit Display Screen

**Note**

The parameters to be configured for the entrance and exit display screen vary according to the linkage between the screen and the lane. If the screen is linked with a lane, both the Vehicle Detected screen and the Idle screen should be configured. If the screen has not been linked with a lane, only the Idle screen is required to be configured.

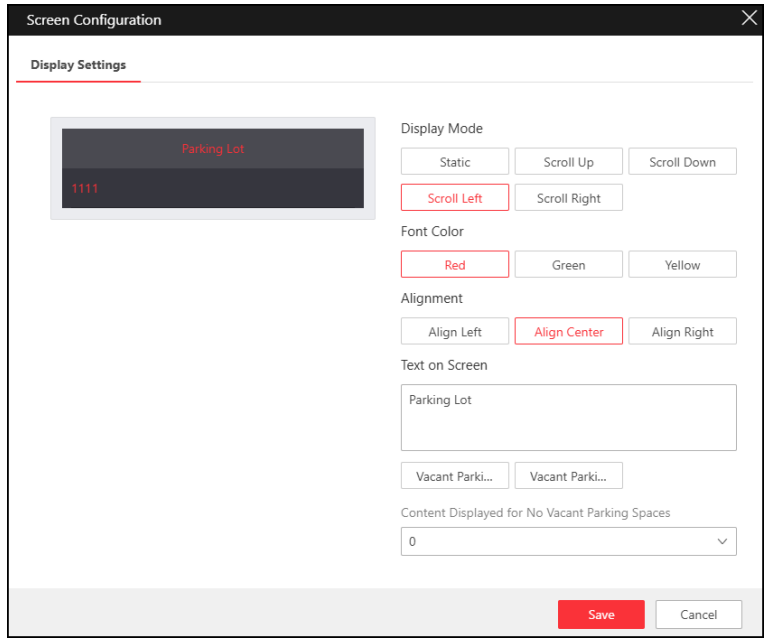



**Figure 15-12 Configure the Entrance and Exit Display Screen Not Linked with a Lane**

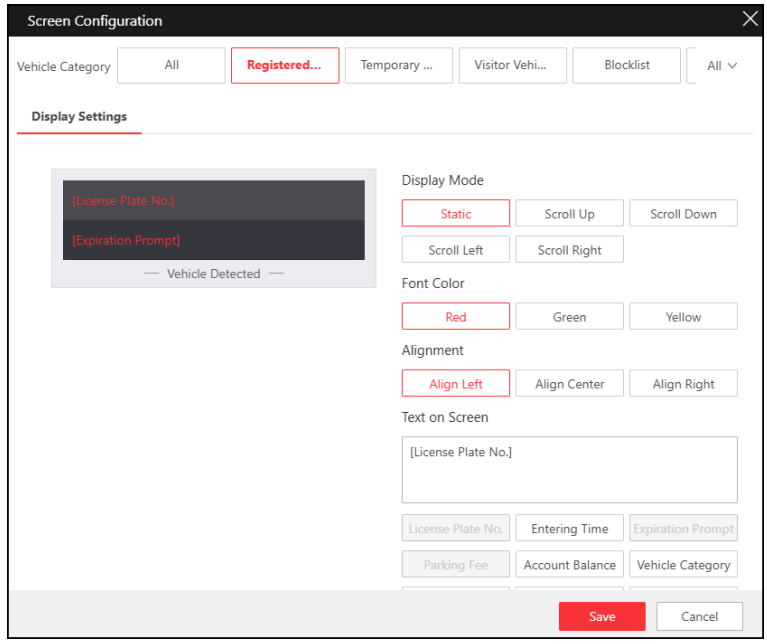



**Figure 15-13 Configure the Entrance and Exit Display Screen Linked with a Lane**

1. Select a vehicle category.

   **Note**

   This is valid for the entrance and exit display screens that are linked with a lane.

2. Configure the Vehicle Detected screen.

a. Click a line on the Vehicle Detected screen to set its **Display Mode**, **Font Color**, and **Alignment**.
b. Select the information to be displayed on the line from **Text on Screen**.

**License Plate No.**

Display the license plate number recognized by the capture unit. By default, this text is selected to be displayed on the screen linked with a lane.

**Entering Time**

The time when a recognized vehicle enters the parking lot. This text is selectable only when the display screen is linked with an entrance lane.

**Exit Time**

The time when a recognized vehicle exits the parking lot. This text is selectable only when the display screen is linked with an exit lane.

**Parking Duration**

Display the parking duration when the vehicle exits the parking lot.

**Expiration Prompt**

Inform the vehicle owners that their vehicles are about to expire. You need to enable the expiration prompt for a parking lot and set when to inform vehicle owners the expiration date. See ***Add Parking Lot*** for details. This text is selectable only when the display screen is linked with an exit lane.

**Parking Fee**

Display the parking fee to be paid when the vehicle exits the parking lot. This text is selectable only when the parking lot is in the Charge mode.

**Account Balance**

The balance in the vehicle owner's account.

**Vehicle Category**

Display the vehicle category recognized by the capture unit.

**Vacant Parking Spaces**

Display the number of vacant parking spaces on the selected floor with which the display screen is linked.

**Vacant Parking Spaces in Vehicle List**

Display the number of vacant parking spaces for vehicles in a vehicle list. However, in the case that a parking lot is used by more than one company at the same time, a vehicle list can be regarded as a company.

**Entry and Exit Not Allowed Prompt**

Inform the driver of reasons why the entry/exit is not allowed. For example, to remind the driver to pay the parking fee before exiting.

c. Configure the content displayed for no vacant parking space.

From the drop-down list, select "0", "X", "FULL", or "Custom" to define your preferred text.

d. Configure other lines in the same way.

**Note**

There is only one line for displaying information on the screen not linked with a lane.

3. Configure the Idle screen in the same way you configure the Vehicle Detected screen.
4. Click **Save**.

## Configure Indoor Guidance Screen

**Note**

The number of sub screens on the indoor guidance screen varies with the model. Here only take the model with one sub screen as an example.

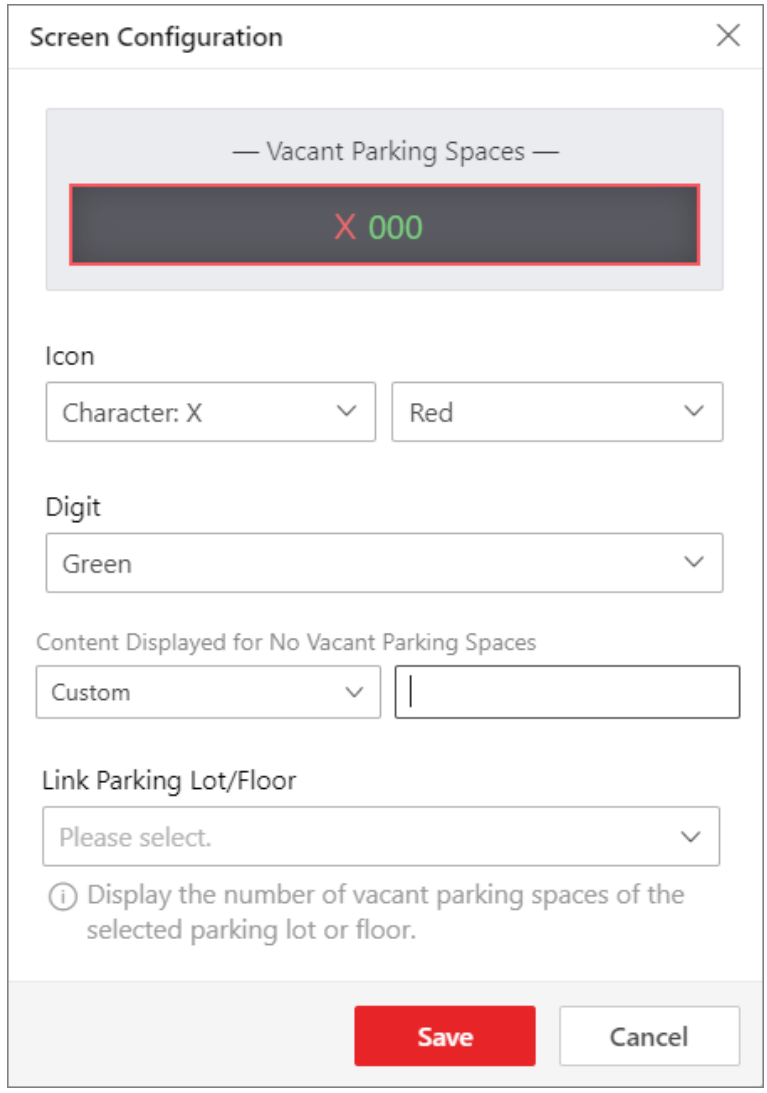



**Figure 15-14 Configure Indoor Guidance Screen**

1. Click a sub screen and select an icon type and color to be displayed.
2. Select a color for the digits displayed on the screen.
3. Configure the content displayed for no vacant parking space.
   From the drop-down list, select "0", "X", "FULL", or "Custom" to define your preferred text.
4. Select the parking lot(s) or floor(s) to be linked with the indoor guidance screen.

   **Note**

   If the linked parking lots contain sub parking lots, the parking space information of sub parking lots will be displayed by default. If the sub parking lots are linked, only the parking space information of sub parking lots will be displayed.
5. Click **Save**.

## Configure Entrance Guidance Screen

**Note**

The number of sub screens on the entrance guidance screen varies with the product model. Here only take the product model with three sub screen as an example.

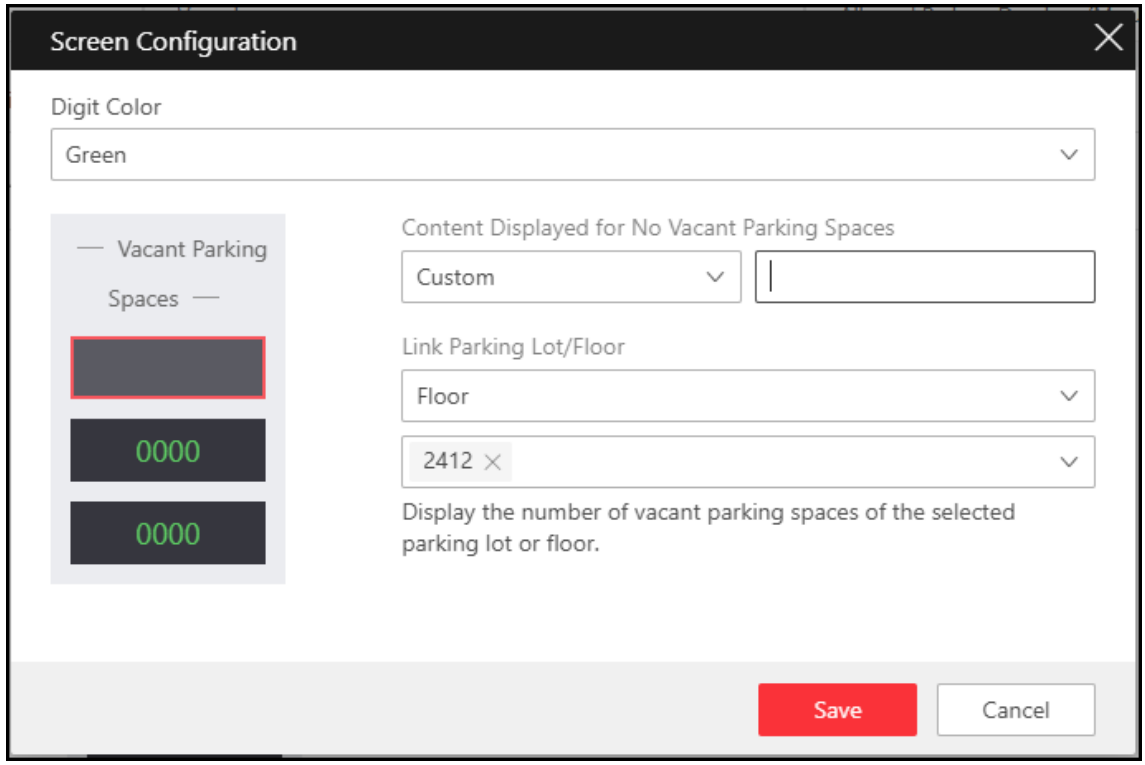



**Figure 15-15 Configure Entrance Guidance Screen**

1. Click a sub screen and select a color for the digits displayed on the screen.
2. Configure the content displayed for no vacant parking space.
   From the drop-down list, select "0", "X", "FULL", or "Custom" to define your preferred text.
3. Select the parking lot(s) or floor(s) to be linked with the indoor guidance screen.

   **Note**

   If the linked parking lots contain sub parking lots, the parking space information of sub parking lots will be displayed by default. If the sub parking lots are linked, only the parking space information of sub parking lots will be displayed.
4. Click **Save**.

## 15.4.6 Configure Entry & Exit Rules

The entry & exit rules define how to open the barrier gate when a vehicle is detected at the lane. You can set the vehicle entering & exiting verification mode for a parking lot, set entry & exit rules for different types of vehicles, including temporary vehicles, registered vehicles, visitor vehicles, and vehicles in list. You can also set an entry & exit rule for a special time period, such as a holiday. With this function, you can manage the entrances and exits in parking lots more easily.

### Set Vehicle Verification Mode

You can set the vehicle entering & exiting verification mode and account deduction mode for a parking lot, which can help you manage the entry and exit of vehicles more easily.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Vehicle Verification Mode**.

**Note**

When the parking fee mode has been set to **Charge** in the basic configuration, the account deduction mode needs to be configured. Refer to ***Set Account Deduction Mode*** for details.

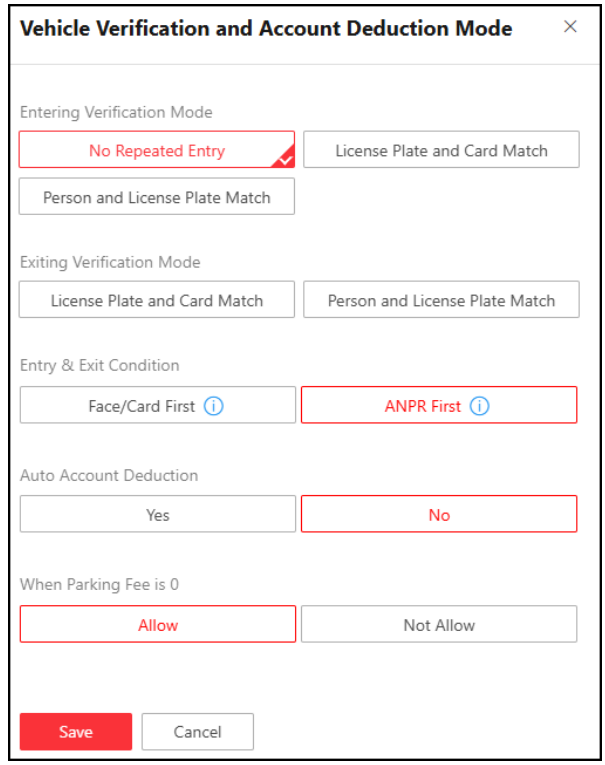



**Figure 15-16 Set Vehicle Verification Mode**

5. Set the vehicle verification mode and the account deduction mode.

**Entering Verification Mode**

The condition in which a vehicle is allowed to enter.

**No Repeated Entry**

Repeated entry for a vehicle is not allowed.

**License Plate and Card Match**

The vehicle is allowed to enter only when the license plate and the card match.

**Person and License Plate Match**

The vehicle is allowed to enter only when the driver and the license plate match.

**Exiting Verification Mode**

The condition in which a vehicle is allowed to exit.

**Entry & Exit Condition**

Set the vehicle authentication methods (ANPR, face, and card). It defaults to ANPR First.

**Auto Account Deduction**

Whether to automatically deduct the parking fee from the vehicle owner's account.

**When Parking Fee is 0**

Whether to allow a vehicle to enter and exit when its parking fee is 0.

6. Click **Save**.

## Set Entry & Exit Rule for Temporary Vehicles

Temporary vehicles are the ones that are not added to the platform and just park in the parking lot for a certain period. You can set the entry & exit rule for temporary vehicles, which can help you to manage the entry and exit of them more easily.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Temporary Vehicles** to open the following pane.

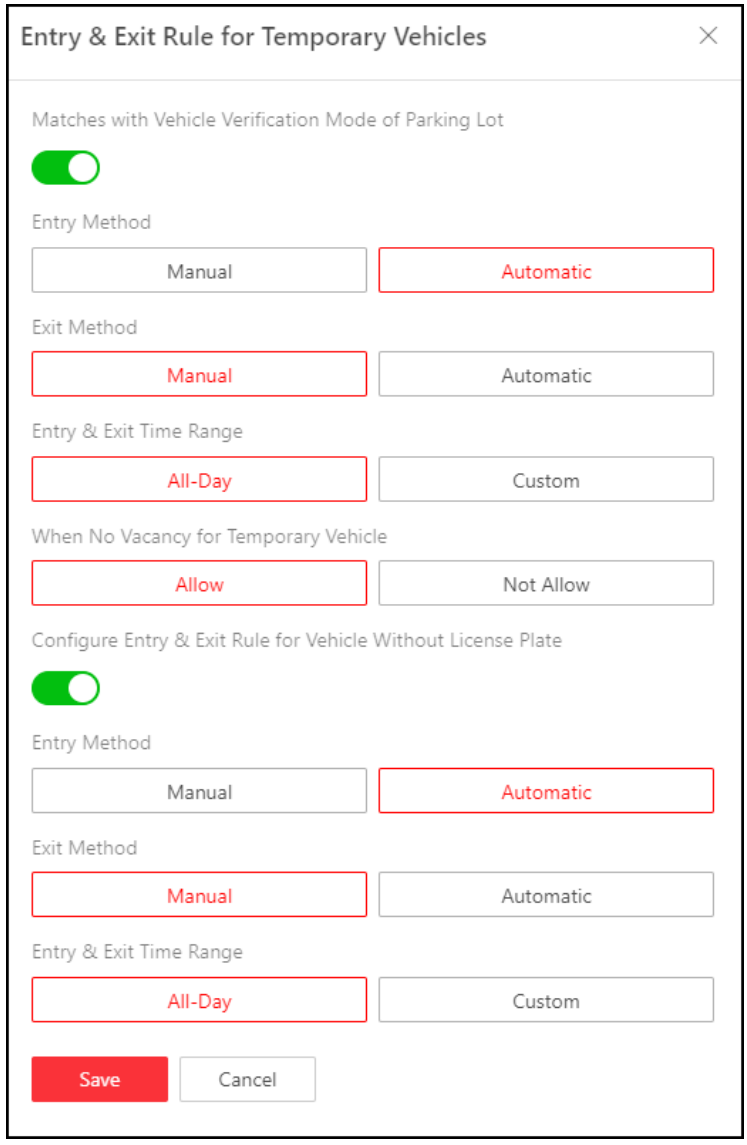



**Figure 15-17 Entry & Exit Rule for Temporary Vehicles**

5. Set the rule.

**Matches with Vehicle Verification Mode of Parking Lot**

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

**Entry Method**

How the barrier gate is opened when a vehicle enters.

**Exit Method**

How the barrier gate is opened when a vehicle exits.

**Entry & Exit Time Range**

The period in which the vehicles are allowed to enter and exit.

**Note**

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

**When No Vacancy for Temporary Vehicle**

Whether to allow the temporary vehicles to enter when where are no vacant parking spaces.

**Configure Entry & Exit Rule for Vehicle Without License Plate**

Set a rule for the vehicle's automatic or manual passing at entry or exit without license plate.

6. Click **Save**.

## Set Entry & Exit Rule for Registered Vehicles

Registered vehicles are the ones that have been added to the platform. You can set the entry & exit rule for registered vehicles, which can help you to manage the entry and exit of them more easily.

**Before You Start**

Make sure that at least one vehicle has been added to the platform.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Registered Vehicles** to open the following pane.

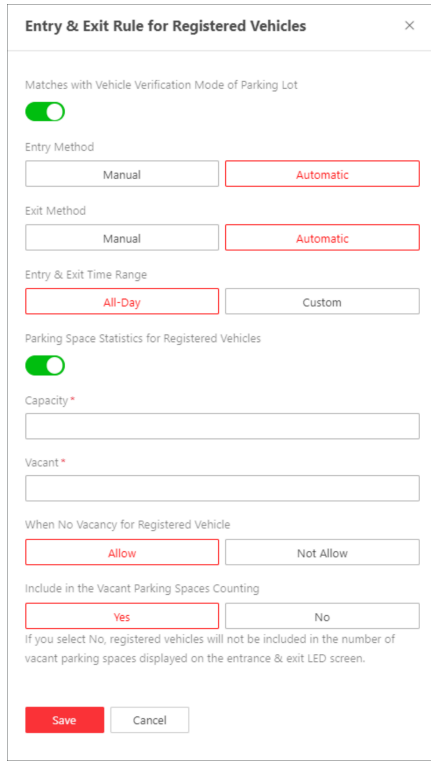



**Figure 15-18 Entry & Exit Rule for Registered Vehicles**

5. Set the rule.

**Matches with Vehicle Verification Mode of Parking Lot**

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

**Entry Method**

How the barrier gate is opened when a vehicle enters.

**Exit Method**

How the barrier gate is opened when a vehicle exits.

**Entry & Exit Time Range**

The period in which vehicles are allowed to enter and exit.

**Note**

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

**Parking Space Statistics for Registered Vehicles**

Set the independent parking space statistics logic for registered vehicles.

**When No Vacancy for Registered Vehicle**

Whether to allow the registered vehicles to enter when there are no vacant parking spaces.

6. Click **Save**.

## Set Entry & Exit Rule for Visitor Vehicles

Visitor vehicles are the ones that are not added to the platform and are driven by visitors who come for a visit. You can set the entry & exit rule for visitor vehicles, which can help you to manage the entry and exit of them more easily.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Visitor Vehicles** to open the following pane.

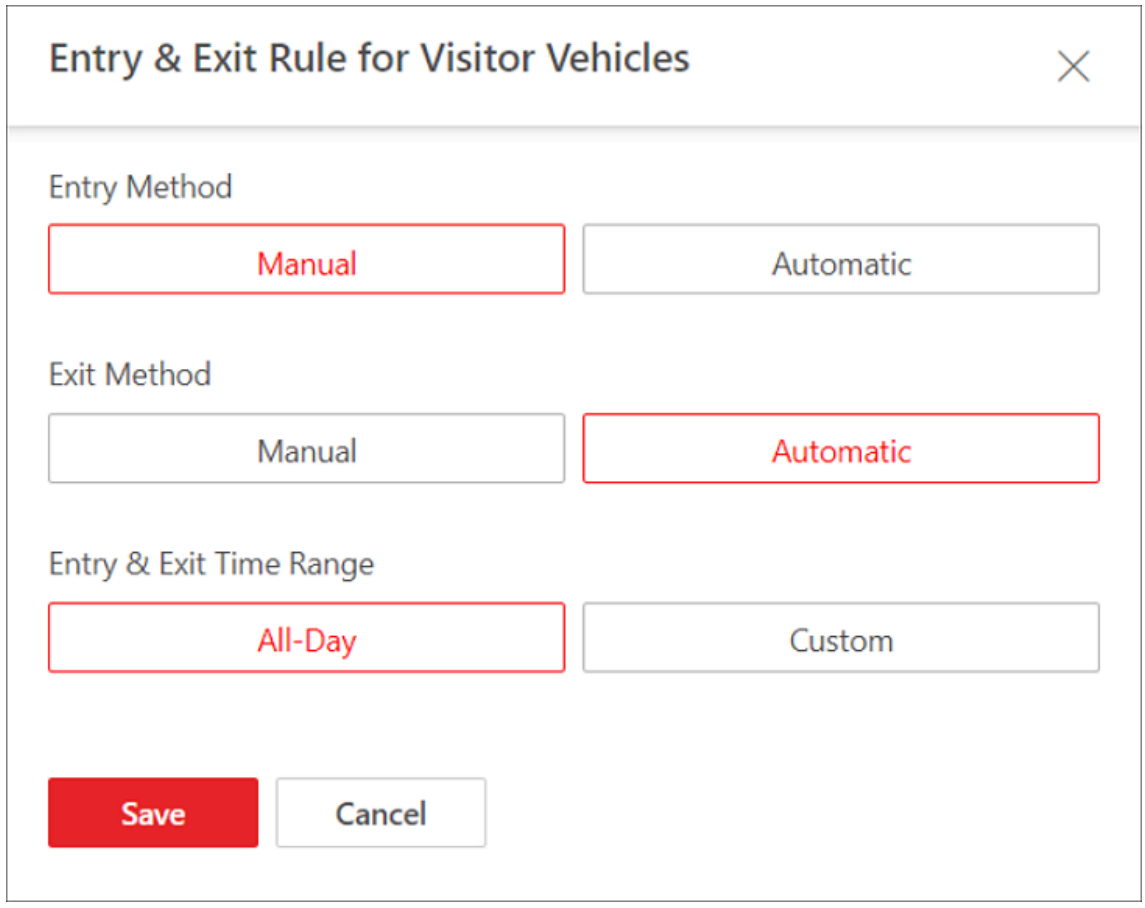



**Figure 15-19 Entry & Exit Rule for Visitor Vehicles**

5. Set the rule.

**Entry Method**

How the barrier gate is opened when a vehicle enters.

**Exit Method**

How the barrier gate is opened when a vehicle exits.

**Entry & Exit Time Range**

The time period when vehicles are allowed to enter and exit.

**Note**

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

6. Click **Save**.

## Add Entry & Exit Rule for Vehicles in List

Vehicles in list are the ones that have been added to the platform and managed in the list you created. You can add the entry & exit rule for a vehicle list, so that the entry and exit of all vehicles in this list will be controlled by the rule.

**Before You Start**

Make sure that at least one vehicle list has been added.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Entry & Exit Rule for Vehicles in List** to open the Add Rule pane.

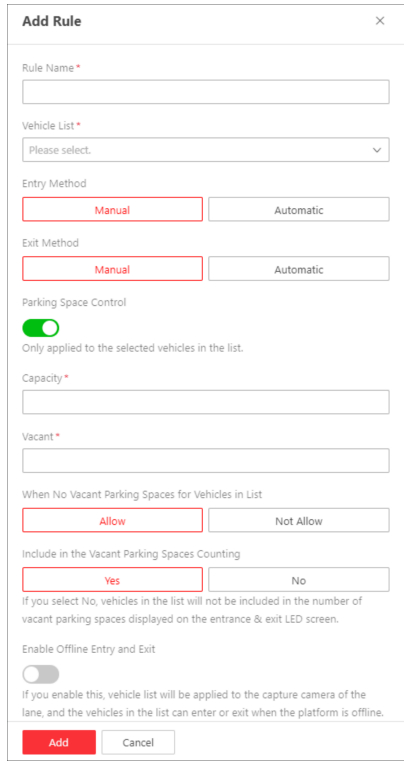



**Figure 15-20 Add Rule**

5. Set the rule.

**Matches with Vehicle Verification Mode of Parking Lot**

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

**Vehicle List**

The list of vehicles that the rule is applied to.

**Entry Method**

How the barrier gate is opened when a vehicle enters.

**Exit Method**

How the barrier gate is opened when a vehicle exits.

**Entry & Exit Time Range**

The period in which vehicles are allowed to enter and exit.

**Note**

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

**Parking Space Control**

Set the independent parking space statistics logic for vehicles in the selected list.

**Capacity**

The total number of parking spaces for vehicles in list.

**Vacant**

The number of vacant parking spaces for vehicles in list.

**When No Vacant Parking Spaces for Vehicles in List**

Whether to allow vehicles in list to enter when there are no vacant parking spaces.

6. Click **Add**.
7. **Optional:** Click and select the parking lot(s) to which the rule is to be copied.

## Add Entry & Exit Rule for Holidays

You can configure free entry and exit for vehicles during holidays or certain days of a week, which can help you to manage the entry and exit of vehicles in this period more easily.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Auto Entry & Exit on Holidays** to open the Add Holiday pane.

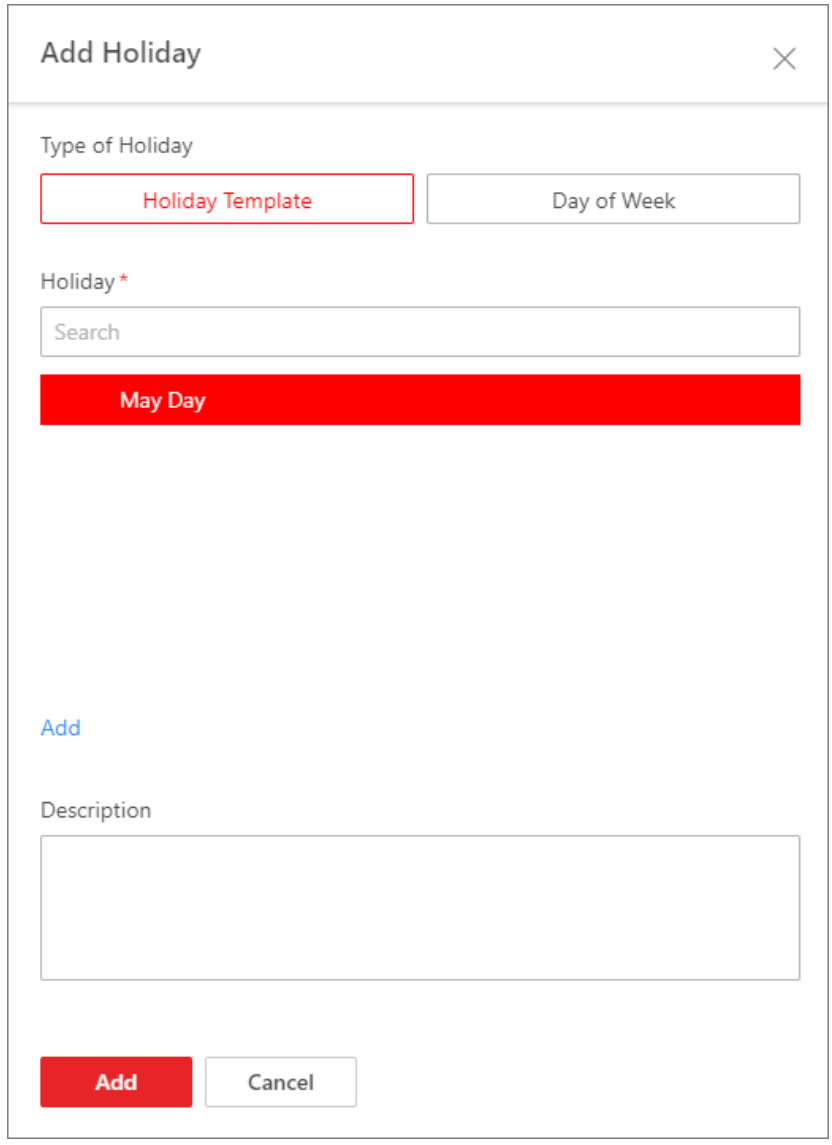



**Figure 15-21 Holiday Template**

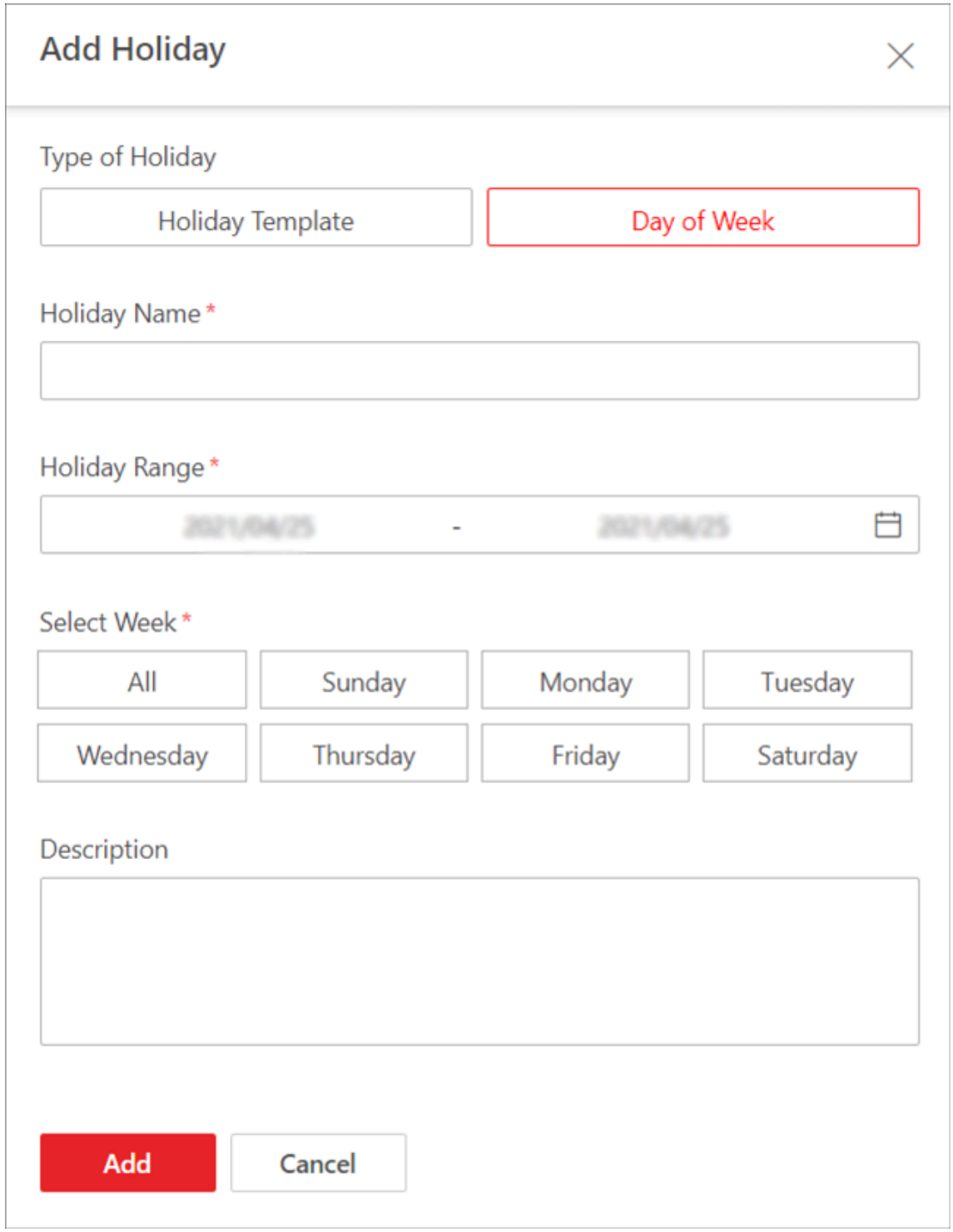



**Figure 15-22 Day of Week**

5. Select **Holiday Template** or **Day of Week** and complete relevant settings.

| | |
|---|---|
| **Holiday Template** | a. Select a holiday from the list if any holiday has been added, or click **Add New** to create a new holiday.<br>b. (Optional) Enter remarks in the Description field if needed.<br>c. Click **Add**. |
| **Day of Week** | a. Create a name for the holiday.<br>b. Click to set a time range for the holiday.<br>c. Select the day(s) of a week that the rule is applied to.<br>d. (Optional) Enter remarks in the Description field if needed.<br>e. Click **Add**. |

6. **Optional:** Manage added rules.

| | |
|---|---|
| **Copy a Rule to Other Parking Lots** | Click and select the parking lot(s) to which the rule is to be copied. |
| **Edit a Rule** | Click to edit a rule. |
| **Delete a Rule** | Click to delete a rule. |

## Specify User to Receive Entry & Exit Calls

You can specify users to receive calls from the entry & exit devices on the Control Client, and then the user can remotely perform further operations for the vehicles, such as correcting license plate number and manually allowing passing.

On the left navigation pane, click **Basic Configuration → Call Recipient Settings** .

Click **Add** to select user(s) to receive entrance & exit calls on the Control Client.

Click next to a user name to open the **Receiving Range of Calling Event** pane and select entrances & exits in the list. The user will only receive calls from devices linked to the selected entrances & exits.

## 15.4.7 Configure Parking Fee Rules

You can set parking fee rules for parking lots, including adding parking fee rule for certain types of vehicles, adding parking pass rule, adding discount rule, adding parking fee rule for abnormal entry & exit. Once you set a rule, the platform will automatically calculate the fee for the parking based on this rule and present the information related to the fee.

**Note**

Make sure that the parking fee mode has been set to **Charge**. See ***Enable Parking Charge Mode*** for details.

## Enable Parking Charge Mode

You can set the parking fee mode for parking lots, and select the type of currency to pay. This configuration will affect the functions related to parking fee.

**Steps**

1. On the left navigation pane, click **Basic Configuration → Parking Fee Mode** .

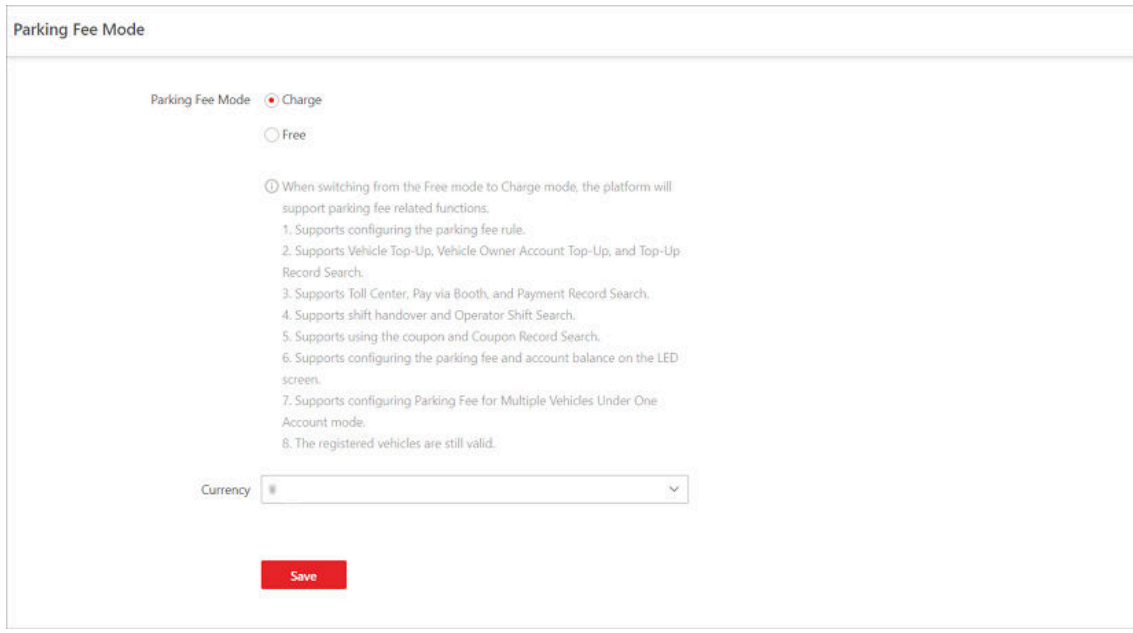



**Figure 15-23 Parking Fee Mode Settings Page**

2. Select **Charge** or **Free** as the parking fee mode.

**Note**

If you select **Free**, the settings related to parking fee are disabled.

3. Select a type of currency from the drop-down list.

**Note**

This step is valid only when you set the parking fee mode to **Charge**.

4. Click **Save**.

## Set Account Deduction Mode

You can set the account deduction mode for a parking lot, which can help you manage parking fee payments more easily.

**Before You Start**

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Vehicle Verification and Account Deduction Mode**.

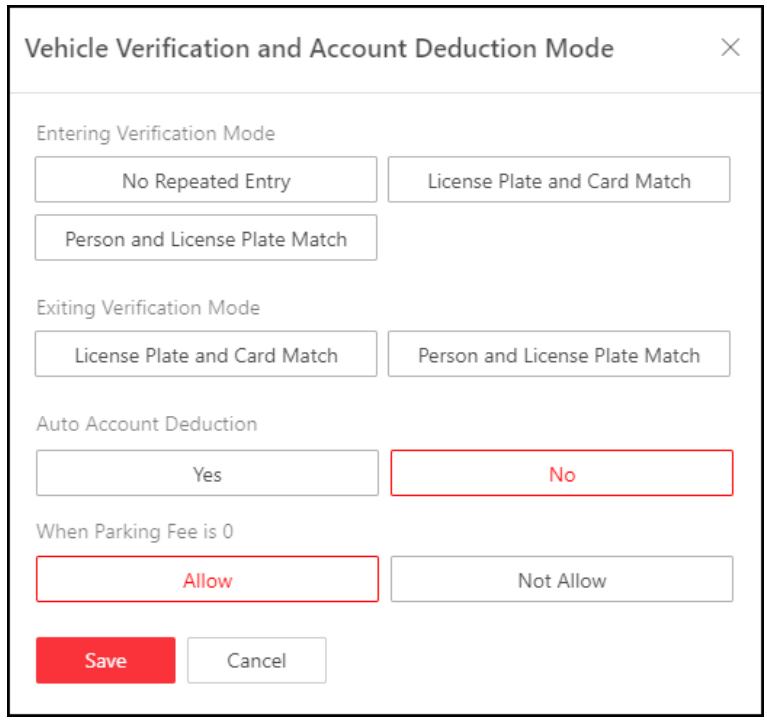



**Figure 15-24 Vehicle Verification and Account Deduction Mode**

5. Set the modes.

   **Entering/Exiting Verification Mode**

   The condition in which a vehicle is allowed to enter/exit the parking lot. Refer to ***Set Vehicle Verification Mode*** for details.

   **Auto Account Deduction**

   Whether to automatically deduct the parking fee from the vehicle owner's account.

   **When Parking Fee is 0**

   Whether to allow a vehicle to enter and exit when its parking fee is 0.
6. Click **Save**.

## Add Parking Fee Rule for Temporary Vehicles

You can add parking fee rule for temporary vehicles, which can help you calculate parking fees more easily.

**Before You Start**

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Temporary Vehicles** to enter the Add Parking Fee Rule pane.

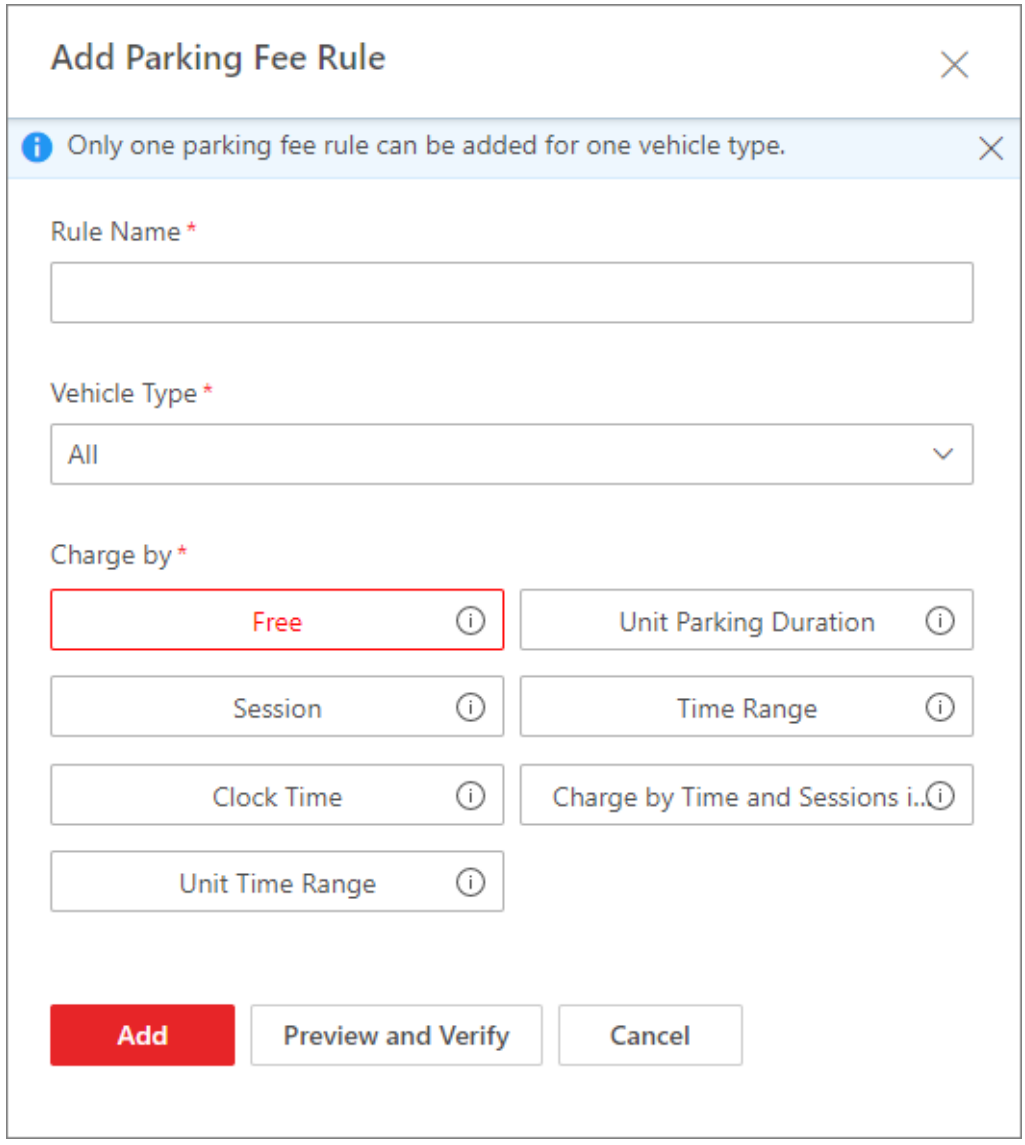



**Figure 15-25 Add Parking Fee Rule for Temporary Vehicles**

5. Create a name for the rule.
6. Select the type of vehicle to which the rule applies.

**Note**

No more than one rule can be added for each vehicle type.

7. Select the way by which vehicles of the selected type will be charged and complete the corresponding settings.

| | |
|---|---|
| **Free** | No charge for any parking. |
| **Unit Parking Duration** | The duration of one parking is separated into different parts and these parts are charged different fees. For example, if a vehicle has parked for 2 hours, the |

parking fee for the first hour is a specific amount, and the parking fee for the duration after the first hour is an another amount.

a. Enter the parking duration that is free of charge.
b. Enter the fee for the initial parking duration.
c. Enter the fee for subsequent parking duration.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Session**

The parking fee is charged by session. For example, if a vehicle has parked twice in a parking lot, its times of parking are counted as two sessions.

Enter the fee for each session.

**Time Range**

The parking fee is charged by the duration of a parking.

a. Enter the parking duration that is free of charge.
b. Enter a time range and the fee for a parking within this range.

**Note**

You can click **Add** to add different time ranges and fees.

c. Enter the fee for the duration beyond the maximum duration allowed.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Clock Time**

The parking fee is charged according to the time of a day.

a. Enter the parking duration that is free of charge.
b. Click to select a time range and enter the fee for a parking within this range.

**Note**

You can click **Add** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Charge by Duration and Session in Daytime and Nighttime**

The parking fee is charged according to the time of a day (daytime and nighttime).

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to set the time when daytime starts.

**Note**

The parking fee is charged by time range in daytime.

d. Enter the fee for the initial parking duration.
e. Enter the fee for subsequent parking duration.
f. Click to set the time when nighttime starts.

**Note**

The parking fee is charged by session in nighttime. You can select a charging mode from **Count One Entry and Exit as One Session** and **Count Multiple Entries and Exits as One Session** below.

g. Enter the fee for each parking.
h. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
i. (Optional) Switch on **Charge by Daytime If Parking Duration Includes Daytime**.

**Unit Time Range**

The parking fee is charged by the time range of a day.

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to select a time range, and enter relevant information in **Charged Parking Duration**, **Parking Fee**, **Max. Fee**, and **Min. Threshold Duration**.

**Note**

You can click **Add** to add different time ranges and fees.

d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

8. **Optional:** Click **Preview and Verify** to preview and verify the rule.
9. Click **Add**.

**Note**

A temporary card will be issued for a temporary vehicle as it enters the parking lot for calculating its parking duration (see ***Issue Temporary Cards*** for details), and the parking fee can be paid accordingly in the toll center (see ***Pay in Toll Center*** for details).

10. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Copy a Rule to Other Parking Lot(s)** | Click and select the parking lot(s) to which the rule is to be copied. |
| **Edit a Rule** | Click to edit a rule. |
| **Delete a Rule** | Click to delete a rule. |

## Add Parking Fee Rule for Registered Vehicles

A parking pass costs a certain amount of money. Within the validity period of a parking pass, the vehicle can enter and exit a specific parking lot as a registered vehicle, so that it can park in that parking lot without paying any fees. You can add rules for parking passes.

**Before You Start**

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Registered Vehicle** to enter the Add Parking Pass Rule pane.

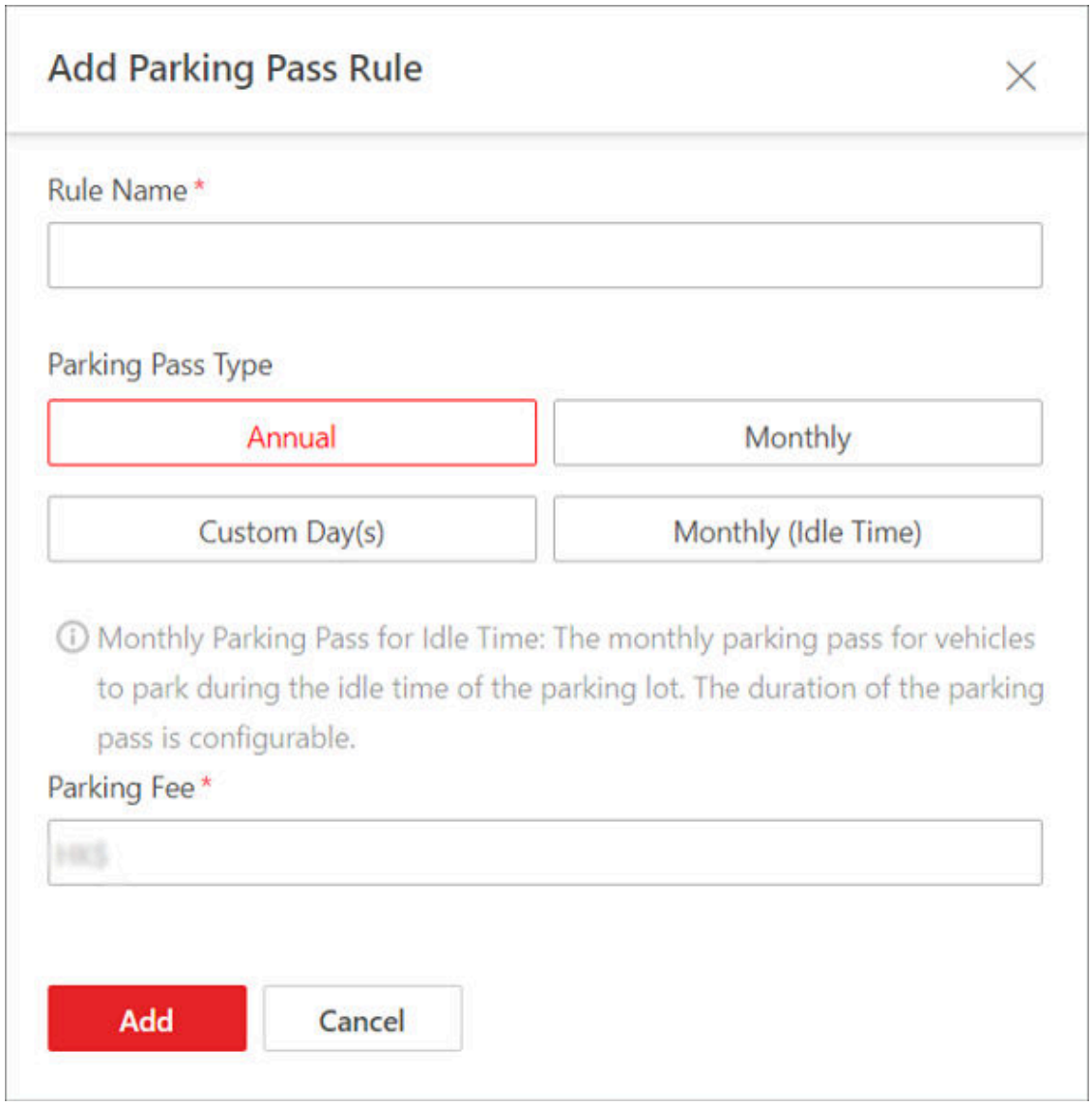



**Figure 15-26 Add Parking Pass Rule Pane**

5. Create a name for the rule.
6. Select a type for the parking pass and complete the corresponding settings.

| | |
|---|---|
| **Annual/ Monthly** | Enter the fee for an annual/monthly parking pass. |

| | |
|---|---|
| **Custom Day(s)** | Enter the valid days of a parking pass and the fee for it. |
| **Monthly (Idle Time)** | Select a template of monthly parking pass for idle time from the drop-down list, and enter the fee for the parking pass. |

**Note**

- This parking pass is used during the period in which the parking lot is not busy (in idle time).
- If you have not added any template, you need to click **Template of Monthly Parking Pass for Idle Time** to create a template first.

7. Click **Add**.

**Note**

Vehicle owners can top up their parking passes as needed. Refer to ***Top Up Parking Pass*** for details.

8. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Copy a Rule to Other Parking Lot(s)** | Click and select the parking lot(s) to which the rule is to be copied. |
| **Edit a Rule** | Click to edit a rule. |
| **Delete a Rule** | Click to delete a rule. |

## Add Parking Fee Rule for Vehicles in List

You can add parking fee rule for vehicles in list, which can help you calculate parking fees more easily.

**Before You Start**

- Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.
- Make sure that at least one vehicle list has been added.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Vehicles in List** to enter the Add Parking Fee Rule pane.
5. Create a name for the rule.
6. Select a vehicle list from the drop-down list.

**Note**

No more than one rule can be added for each vehicle list.

**7.** Select the way by which vehicles in the selected list will be charged and complete the corresponding settings.

**Free**
No charge for any parking.

**Unit Parking Duration**
The duration of one parking is separated into different parts and these parts are charged different fees. For example, if a vehicle has parked for 2 hours, the parking fee for the first hour is a specific amount, and the parking fee for the duration after the first hour is an another amount.

a. Enter the parking duration that is free of charge.
b. Enter the fee for the initial parking duration.
c. Enter the fee for subsequent parking duration.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Session**
The parking fee is charged by session. For example, if a vehicle has parked twice in a parking lot, its times of parking are counted as two sessions.

Enter the fee for each session.

**Time Range**
The parking fee is charged by the duration of a parking.

a. Enter the parking duration that is free of charge.
b. Enter a time range and the fee for a parking within this range.

**Note**

You can click **Add** to add different time ranges and fees.

c. Enter the fee for the duration beyond the maximum duration allowed.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Clock Time**
The parking fee is charged according to the time of a day.

a. Enter the parking duration that is free of charge.
b. Click to select a time range and enter the fee for a parking within this range.

**Note**

You can click **Add** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

**Charge by Duration and Session in Daytime and Nighttime**
The parking fee is charged according to the time of a day (daytime and nighttime).

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to set the time when daytime starts.

**Note**

The parking fee is charged by time range in daytime.

d. Enter the fee for the initial parking duration.
e. Enter the fee for subsequent parking duration.
f. Click to set the time when nighttime starts.

**Note**

The parking fee is charged by session in nighttime. You can select a charging mode from **Count One Entry and Exit as One Session** and **Count Multiple Entries and Exits as One Session** below.

g. Enter the fee for each parking.
h. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
i. (Optional) Switch on **Charge by Daytime If Parking Duration Includes Daytime**.

**Unit Time Range**

The parking fee is charged by the time range of a day.

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to select a time range, and enter relevant information in **Charged Parking Duration**, **Parking Fee**, **Max. Fee**, and **Min. Threshold Duration**.

**Note**

You can click **Add** to add different time ranges and fees.

d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

8. **Optional:** Click **Preview and Verify** to preview and verify the rule.
9. Click **Add**.

**Note**

A temporary card will be issued for a temporary vehicle as it enters the parking lot for calculating its parking duration (see ***Issue Temporary Cards*** for details), and the parking fee can be paid accordingly in the toll center (see ***Pay in Toll Center*** for details).

10. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Copy a Rule to Other Parking Lot(s)** | Click and select the parking lot(s) to which the rule is to be copied. |
| **Edit a Rule** | Click to edit a rule. |
| **Delete a Rule** | Click to delete a rule. |

## Add Discount Rule

You can add the discount rule to manage parking fee more flexibly.

**Before You Start**
Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**
1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Discount Rule** to enter the Add Discount Rule panel.
5. Create a name for the rule.
6. Select a discount method and complete relevant settings.

| | |
|---|---|
| **Discount** | Here you can set a discount rate. For example, if you enter 70, the discount rate is 70%. If the parking fee due is 100 RMB, the actual amount tendered is 70 RMB. |
| **Fee Discount** | Here you can set a discount amount. For example, if you enter 70 and the parking fee due is 100 RMB, the actual amount tendered is 30 RMB. |
| **Free** | Here you can set a period during which the vehicles are allowed to park without being charged. |
| **Parking Duration Reduction** | Here you can set a duration, which will be deducted from the total parking duration. For example, if you enter 2 and the parking duration of a vehicle is 6 hours, the actual duration counted for parking fee is 4 hours. |

7. Click **Save**.
8. **Optional:** Perform the following operations as needed.

| | |
|---|---|
| **Issue & Print a Rule** | Click to issue and print the discount rule in the coupon format. |
| **Copy Rule to Other Parking Lots** | Click and select the parking lot(s) that the rule is copied to. |
| **Edit a Rule** | Click to edit the rule. |
| **Delete a Rule** | Click to delete the rule. |

## Add Parking Fee Rule for Abnormal Pass

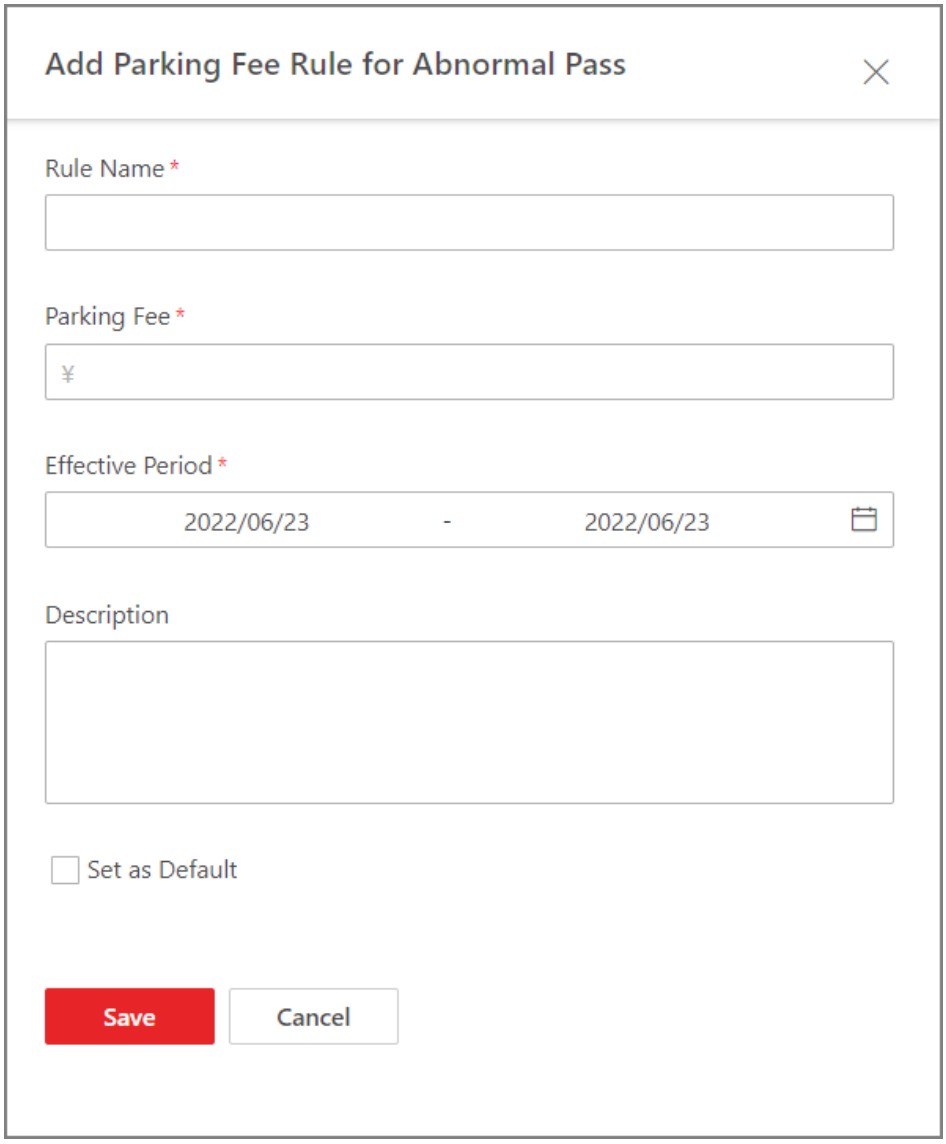
You can add parking fee rule for abnormal pass (e.g., a vehicle with an entry record but without an exit record), which can help you manage abnormal entries and exits more easily.

**Before You Start**

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Abnormal Pass**.




5. Create a name for the rule.
6. Enter the parking fee for abnormal pass.
7. Set a validity period for the rule.
8. **Optional:** Enter remarks in the Description field as needed.
9. **Optional:** Check **Set as Default** to set the rule as the default rule for abnormal entry & exit.

10. Click **Save**.

**Note**

The parking fees incurred in this case will have to be paid at the booth or in the toll center. See ***Pay in Toll Center*** for details.

11. **Optional:** Perform the following operations as needed.

| | |
|---|---|
| **Copy a Rule to Other Parking Lot(s)** | Click and select the parking lot(s) to which the rule is to be copied. |
| **Edit a Rule** | Click to edit a rule. |
| **Delete a Rule** | Click to delete a rule. |

## Customize Parking Receipt Templates

Customize parking receipt templates by selecting general elements (e.g., parking lot name and license plate number), adding custom information (such as taxpayer ID and logos), and adjusting the layout on a visual canvas. The templates can be applied to parking lots when setting up additional parking fee rules.

**Steps**

1. On the left navigation pane, click **Basic Configuration → Receipt Settings** .

**Note**

Make sure that you have updated the web control to the latest version.

2. Click + to enter the Add Parking Receipt page.

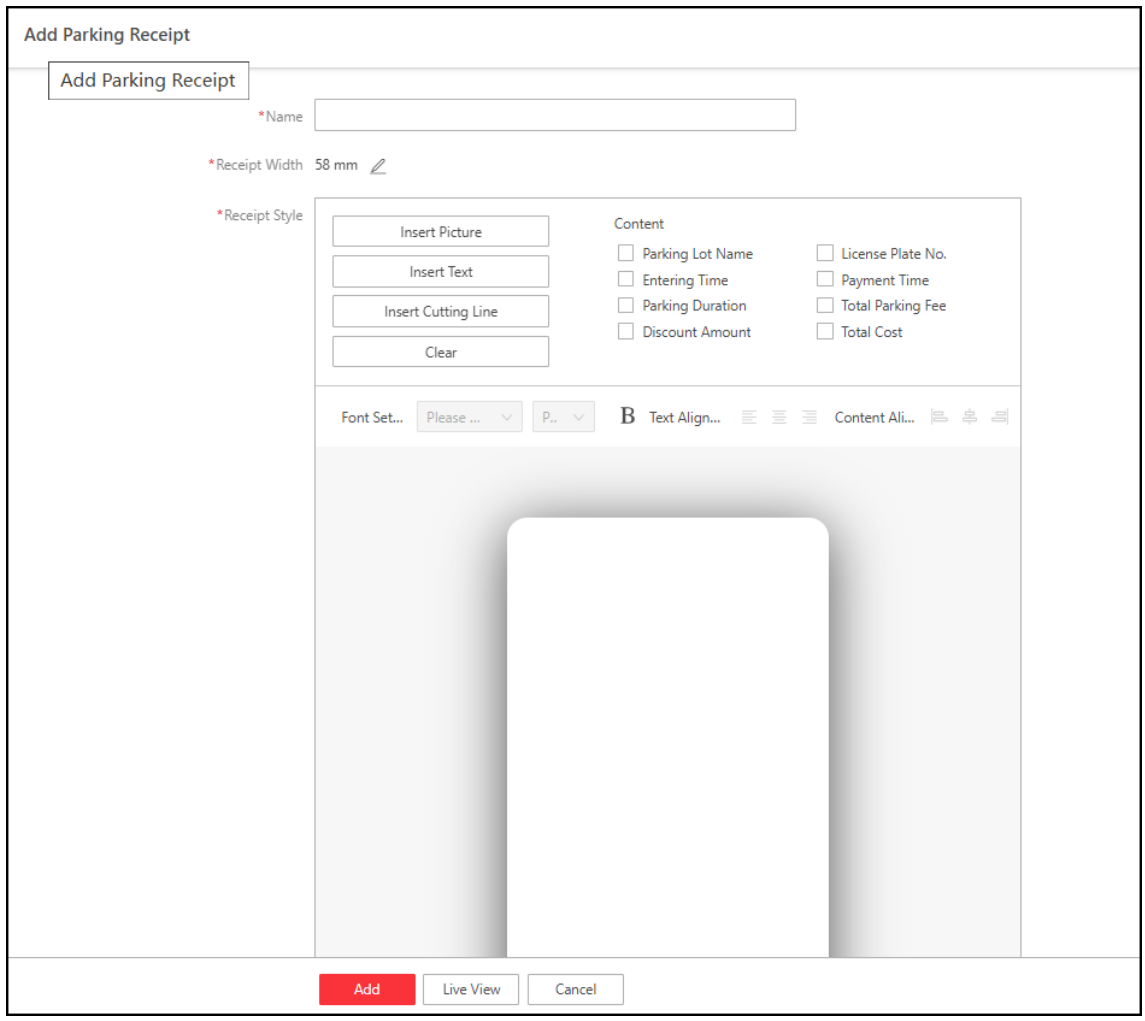



**Figure 15-28 Add Parking Receipt Page**

3. Enter the template name and configure the receipt width, contents, and element layout.

| | |
|---|---|
| **Move Elements** | Drag one element to adjust its position. |
| **Batch Select Elements** | Drag to select multiple elements for batch operations. |
| **Adjust Element Layer** | Right-click on an element and click **Bring to Front** / **Send to Back** / **Bring Forward** / **Send Backward** to change the element layer order. |
| **Delete Elements** | • Delete one element: Right-click one element and click **Delete**.<br>• Batch delete: Drag to select multiple element and press the Delete key.<br>• Delete all: Click **Clear** to delete all elements on the canvas. |

4. Click **Save** to save the template.

**What to do next**
Apply the parking receipt template to parking lots on the Additional Configuration page of parking fee rule configuration.

## Set Additional Parking Fee Rule

You can set additional parking fee rules, including free parking duration after payment, and the parking fee rule for multiple vehicles under one account, which can help you to manage parking fee more flexibly.

**Before You Start**
Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

**Steps**
1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click the **Parking Fee Rule** tab.
4. Click **Edit** beside **Additional Configuration** to open the Additional Configuration pane.

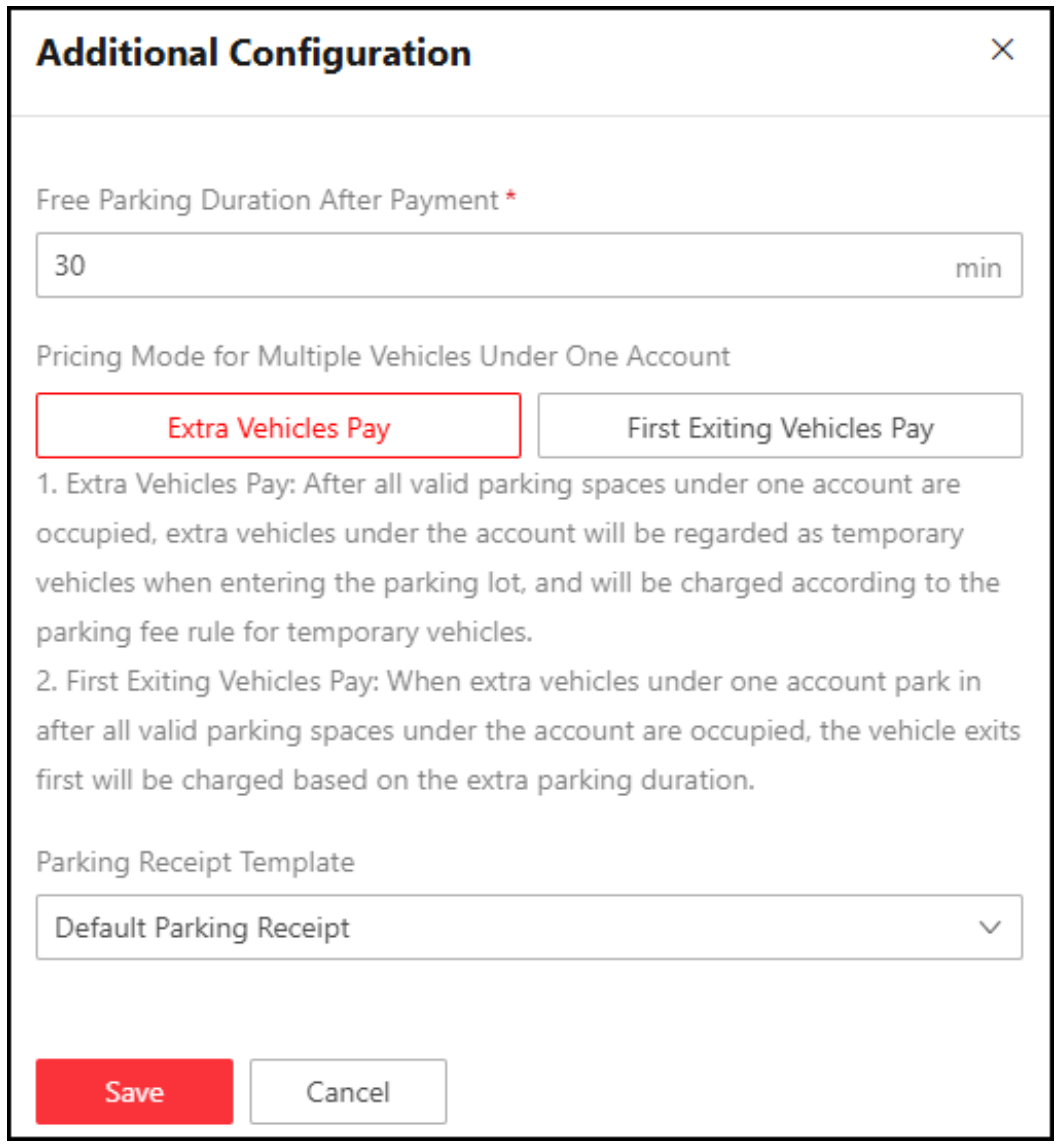



**Figure 15-29 Additional Configuration**

5. Enter the parking duration that is free of charge after paying the parking fee.
6. **Optional:** Set the parking fee rule for multiple vehicles under one account to **Extra Vehicles Pay** or **First Exiting Vehicles Pay**.

   **Extra Vehicles Pay**

   After all valid parking spaces under one account are occupied, extra vehicles under the account will be regarded as temporary vehicles when entering the parking lot, and charged according to the parking fee rule for temporary vehicle.

   **First Exiting Vehicles Pay**

When extra vehicles under one account park in after all valid parking spaces under the account are occupied, the vehicle exiting first will be charged based on the extra parking duration.

7. Select a parking receipt template from the drop-down list.
8. Click **Save**.

## Issue Temporary Cards

You can add temporary cards to parking lots. The temporary cards are mainly designed for temporary vehicles. Before a temporary vehicle enters a parking lot, the driver needs to take a temporary card from the machine. Before exiting the parking lot, the driver needs to return the card and pay the parking fee.

**Steps**

1. On the left navigation pane, click **Temporary Card**.

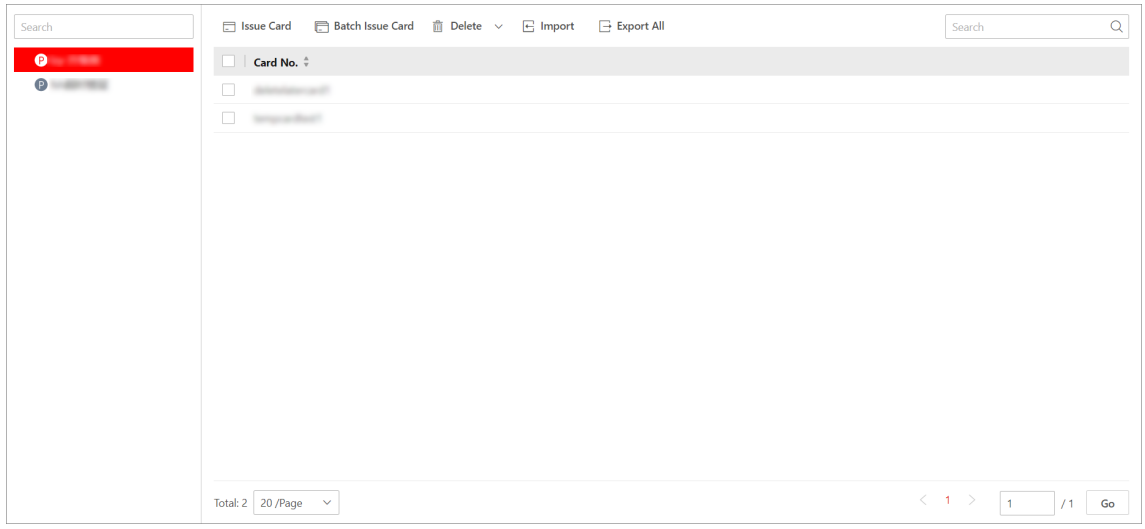



**Figure 15-30 Issue Temporary Card Page**

2. Select a parking lot from the left list.
3. Click **Issue Card**.

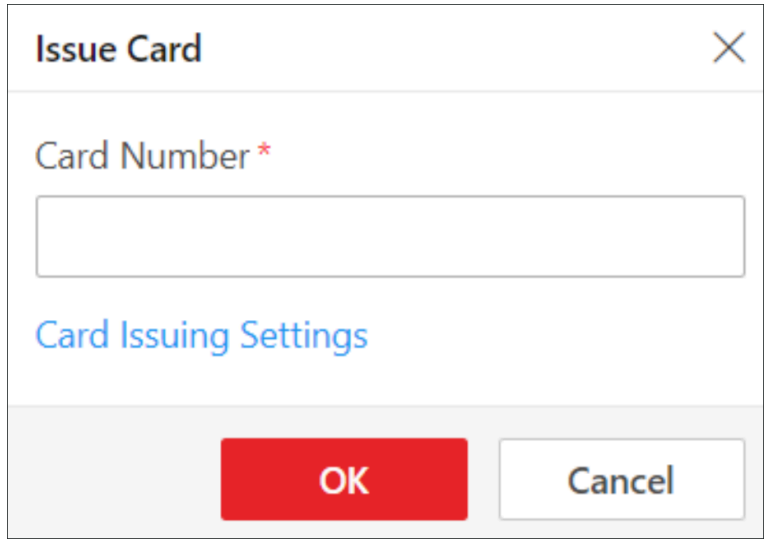



**Figure 15-31 Issue Card Window**

4. Enter the card number.
5. **Optional:** Click **Card Issuing Settings** to set card issuing parameters.
6. Click **OK**.

   The card will be added to the selected parking lot.
7. **Optional:** Perform the following operations as needed.

| | |
|---|---|
| **Batch Issue Cards** | Click **Batch Issue Card** to issue multiple temporary cards at the same time. |
| **Delete Selected Card(s)** | Select the temporary card(s) and click **Delete** to delete the selected card(s). |
| **Delete All Cards** | Click next to **Delete**, and click **Delete All** to delete all temporary cards of the selected parking lot. |
| **Import Temporary Card Information** | Click **Import**, click , select a template file from your PC, and click **Import**.<br>**Note**<br>• You can click **Download Template** and save the predefined template (in XLSX format) to the local PC.<br>• You can check **Auto Replace Duplicate Card No.** to allow the platform to overwrite card numbers that already exist. |
| **Export Temporary Card Information** | Click **Export All** to save the information about all temporary cards added for the selected parking lot to the local PC. |
| **Search for Temporary Cards** | Enter a keyword in the search box and click to search for temporary cards by card number. |

## 15.5 Methods for Parking Charges

There are several ways to pay for parking in paid parking lots for different types of vehicles. Registered vehicles can park in a parking lot without paying additional fees if they or their owners have been topped up with a parking pass, whereas other vehicles (e.g., temporary vehicles, vehicles in list, and vehicles with abnormal entries/exits) can pay at the booth or in the toll center by searching for their parking information by license plate No., swiping the temporary card, or scanning the parking receipt.

### 15.5.1 Top Up Parking Pass

A parking pass costs a certain amount of money and is valid for a specific time period. You can top up parking passes by vehicle or by person (vehicle owner) in Top-Up Management.

On the left navigation pane, click **Top-Up Management**.

When vehicles or vehicle owners have been topped up with parking passes, you can perform the following operations.

**Note**

When topping up a parking pass, a pop-up will appear if unpaid fees are detected, allowing one-click redirection to the payment page.

#### In Top-Up by Vehicle Mode

- Click a license plate No. in the list to enter the parking pass details page of the vehicle. The parking pass information and the vehicle owner (if configured) information card are displayed.
- On the vehicle owner information card, click **Top-Up** / **Refund** to top up / refund the account. You can also click **Settings** to set the upper limit for auto deduction and low balance notice.
- In the upper-right corner, click **Add Parking Pass** to top up by vehicle.
- Click **Top-Up** of a parking lot to renew the parking pass of the vehicle in this parking lot.

#### In Top-Up by Person Mode

- Click a vehicle owner name in the list to enter the parking pass details page of the person.
- On the vehicle owner information card, click **Top-Up** / **Refund** to top up / refund the account. You can also click **Settings** to set the upper limit for auto deduction and low balance notice.
- In the upper-right corner, click **Add Parking Pass** to top up by person.

#### Top Up by Vehicle

If a vehicle is topped up with a parking pass, within the effective period, it can enter, park in, and exit a specific parking lot as a registered vehicle without paying any fees. You can top up parking passes for one or multiple vehicles at the same time.

**Before You Start**

Make sure you have added parking pass rule(s) to the platform. See ***Add Parking Fee Rule for Registered Vehicles*** for more details.

**Steps**

1. On the left navigation pane, click **Top-Up Management**.
2. Click **Top-Up by Vehicle** in the upper-right corner.
3. Select one or multiple vehicles in the list, and click **Top-Up** in the upper-left corner.

**Note**

You can also click **Top Up All** to top up for all vehicles in the list.

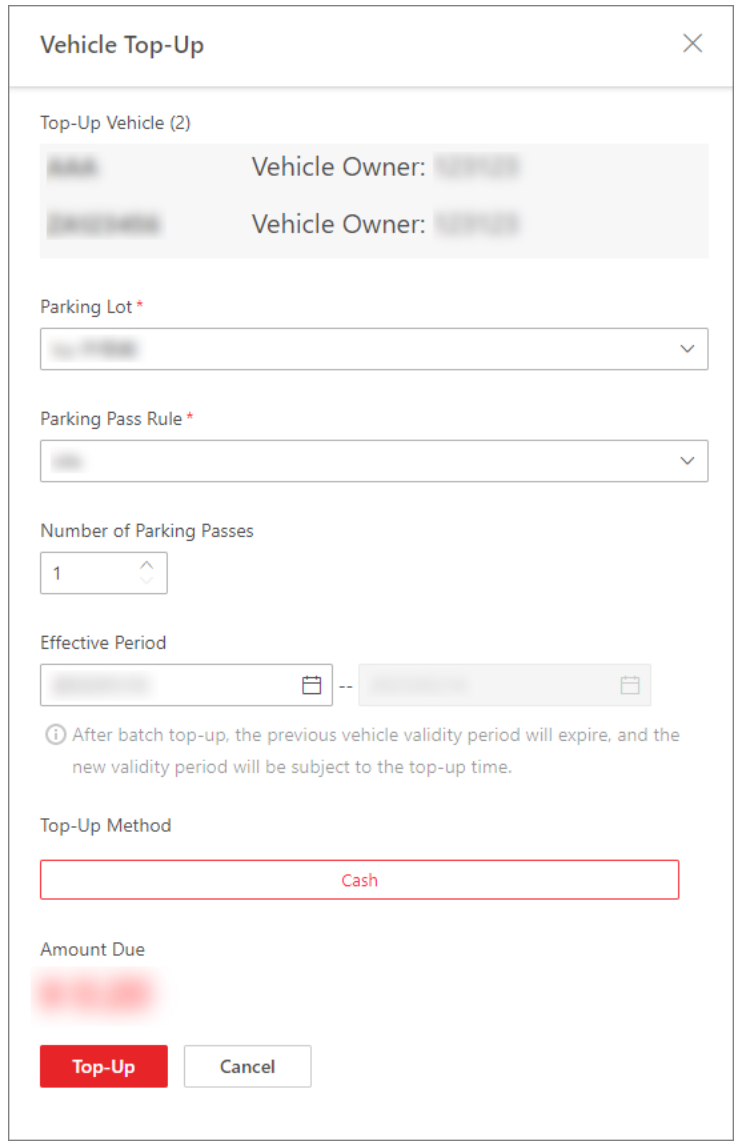



**Figure 15-32 Vehicle Top-Up Pane**

4. Select a parking lot for the vehicle(s) to park in.
5. Select a parking pass rule from the drop-down list.
6. Set the number of parking passes to be topped up.

   **Example**

   If the number here is set to 2 and the type of parking pass you selected in **Parking Pass Rule** is an annual pass, the parking pass will be valid for 2 years.
7. Set the effective period of the parking pass.

   **Note**

   - You can only select the start date for the parking pass; the end date will be automatically calculated by the platform according to the parking pass rule and the number of parking passes you set.
   - For a monthly parking pass, you can select the effective period as **Natural Month** or **30 Days**. For example, when the start date of the effective period is 2023/7/10, if **Natural Month** is selected, the end date will be 2023/8/10, and the total effective period is 31 days.
8. Select the top-up method.

   **Note**

   Currently, the platform only supports cash top-ups when you are topping up for more than one vehicle, whereas you can select from **Cash** and **Account Balance** when topping up for one vehicle only. The amount due will be automatically calculated according to the parking pass rule and the number of parking passes you set.
9. Click **Top-Up**.

   A result window will pop up and you can click **Print Receipt** to print the top-up receipt.

## Top Up by Person

If a vehicle owner is topped up with a parking pass, within the effective period, one of vehicles linked to this person can enter, park in, and exit the specific parking lot without paying any fees. You can top up parking passes for one or multiple vehicle owners at the same time.

**Before You Start**

Make sure you have added parking pass rule(s) to the platform. See ***Add Parking Fee Rule for Registered Vehicles*** for more details.

**Steps**

1. On the left navigation pane, click **Top-Up Management**.
2. Click **Top-Up by Person** in the upper-right corner.
3. Select one or multiple vehicle owners in the list, and click **Top-Up** in the upper-left corner.

   **Note**

   You can also click **Top Up All** to top up for all vehicle owners in the list.

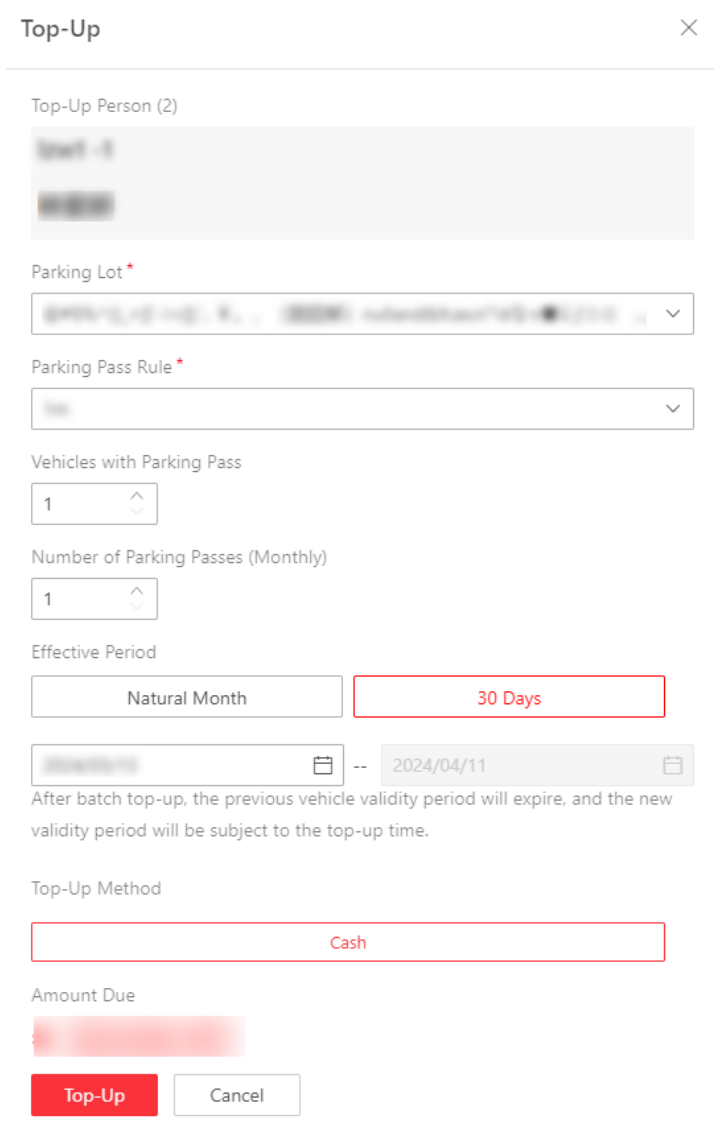



**Figure 15-33 Person Top-Up Pane**

4. Select a parking lot for the vehicle(s) to park in.
5. Select a parking pass rule from the drop-down list.
6. Set the number of vehicles with parking pass.

   **Example**

   If the number here is set to 2, parking passes for two vehicles of the owner will be topped up.
7. Set the number of parking passes to be topped up.

   **Example**

   If the number here is set to 2 and the type of parking pass you selected in **Parking Pass Rule** is an annual pass, the parking pass will be valid for 2 years.
8. Set the effective period of the parking pass.

**Note**

- You can only select the start date for the parking pass; the end date will be automatically calculated by the platform according to the parking pass rule and the number of parking passes you set.
- For a monthly parking pass, you can select the effective period as **Natural Month** or **30 Days**. For example, when the start date of the effective period is 2023/7/10, if **Natural Month** is selected, the end date will be 2023/8/10, and the total effective period is 31 days.

9. Select the top-up method.

**Note**

Currently, the platform only supports cash top-ups when you are topping up for more than one person, whereas you can select from **Cash** and **Account Balance** when topping up for one person only. The amount due will be automatically calculated according to the parking pass rule, the number of vehicles with parking pass, and the number of parking passes you set.

10. Click **Top-Up**.

A result window will pop up and you can click **Print Receipt** to print the top-up receipt.

### 15.5.2 Pay in Toll Center

In the Toll Center module, you can search for a specific vehicle to view its parking information, such as the parking duration and the total parking fee. Once all the information is confirmed, the vehicle owner can pay the parking fee in the toll center.

**Steps**

1. On the left navigation pane, click **Toll Center**.

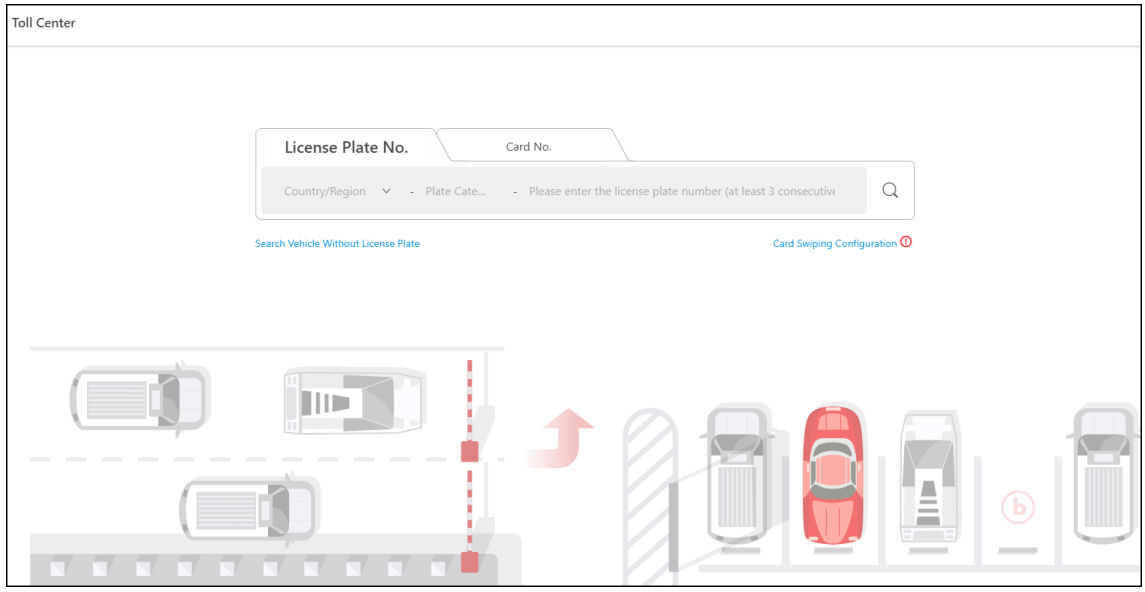



**Figure 15-34 Toll Center Page**

2. Search for a specific vehicle to get its parking information.
   - Enter License Plate Number
     Select the **License Plate No.** mode, enter at least three digits of a license plate number to search for the vehicle.
   - Scan Parking Receipt
     Select the **Card No.** mode, and scan the code on a parking receipt. The parking details will be displayed.
   - Swipe Temporary Card
     Swipe the temporary card that the vehicle owner received when entering the parking lot. After swiping the card at the site, the parking details will be displayed. You can click **Card Swiping Configuration** to switch on/off the card encryption and turn on/off the audio.
   - Search by Vehicle Picture
     If a vehicle's license plate is not captured and recorded, you can click **Search Vehicle Without License Plate** and select the target vehicle from the displayed picture(s).

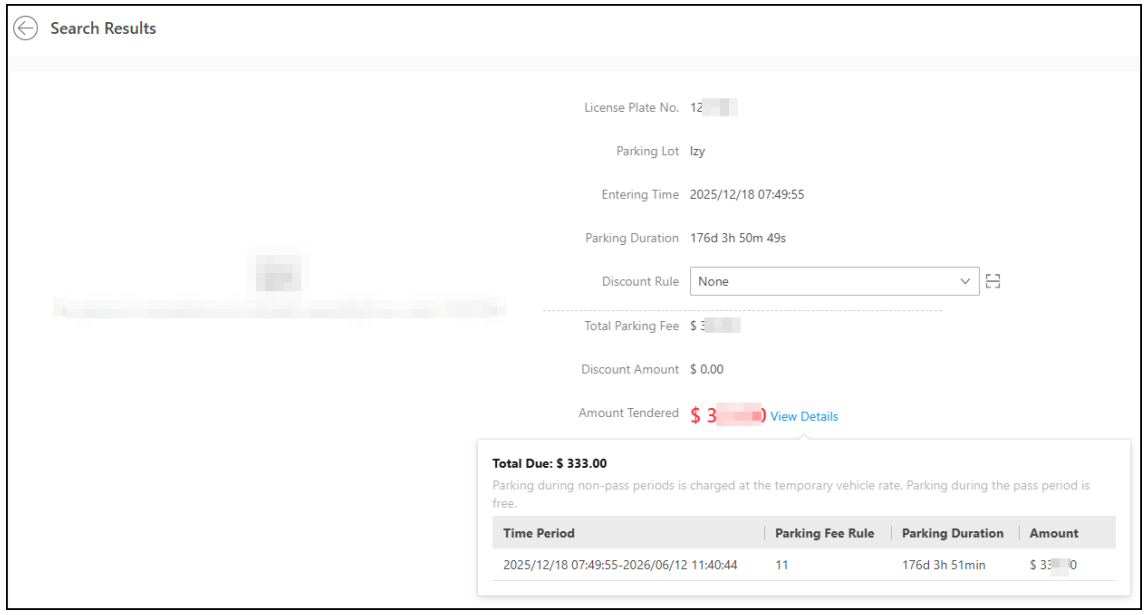



**Figure 15-35 Search Result Page**

3. **Optional:** Set the discount rule on the Search Results pane.
   - Select a coupon from the drop-down list.
   - Click to add a coupon.
4. Check the information and click **Confirm**.
5. **Optional:** On the pop-up window, click **Print Receipt** to print the receipt or save the receipt to the local PC in PDF format.

## 15.6 Parking Guidance Configuration

Parking guidance is designed for both the administrator and the vehicle owners, and it is performed by two devices: the guidance terminal and the display screen. The guidance terminal can relate multiple parking cameras for management, and the display screen can guide the vehicle owners to the area where there are vacant parking spaces. With parking guidance, the parking lot can be better operated.

**Note**

Make sure you have added a parking lot. For details, refer to ***Add Parking Lot*** .

On the left navigation pane, click **Parking Guidance Configuration**, and then select a parking lot to enter the corresponding configuration page.

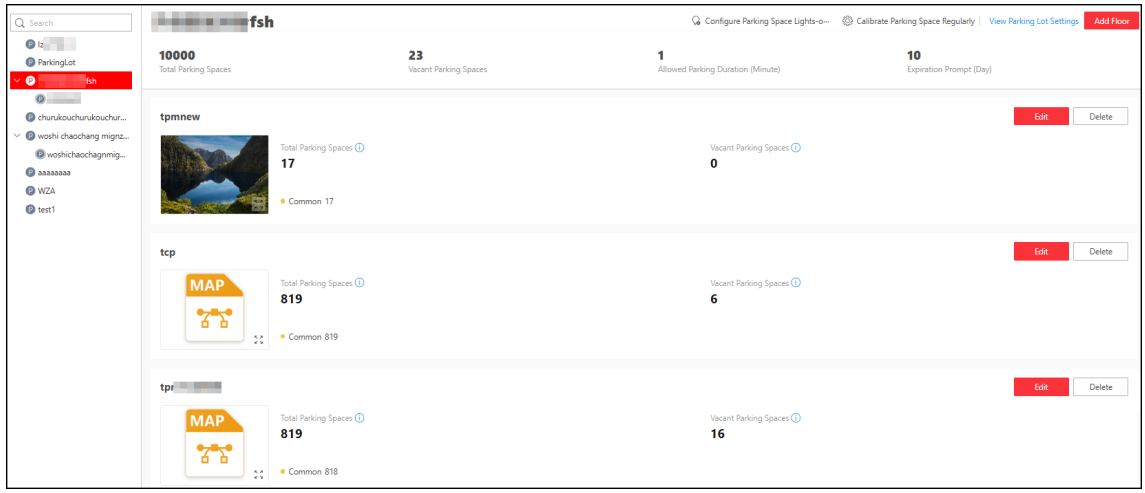



**Figure 15-36 Parking Guidance Configuration Page**

You can follow the steps below to finish the parking guidance configuration.

1. ***Add a Floor to the Parking Lot***
2. ***(Optional) Link Devices to the Floor***
3. ***(Optional) Configure a Map for the Floor***
4. ***Set Types for Parking Spaces on the Map***
5. ***Mark Devices on the Map***

## 15.6.1 Add a Floor to the Parking Lot

Before configuring parking guidance, you need to add a floor to a parking lot. After that, you can perform further operations to the floor, including relating devices, configuring a map, marking display screens, and configuring the types of parking spaces.

**Steps**

**1.** On the parking guidance configuration page of a selected parking lot, click **Add Floor**.

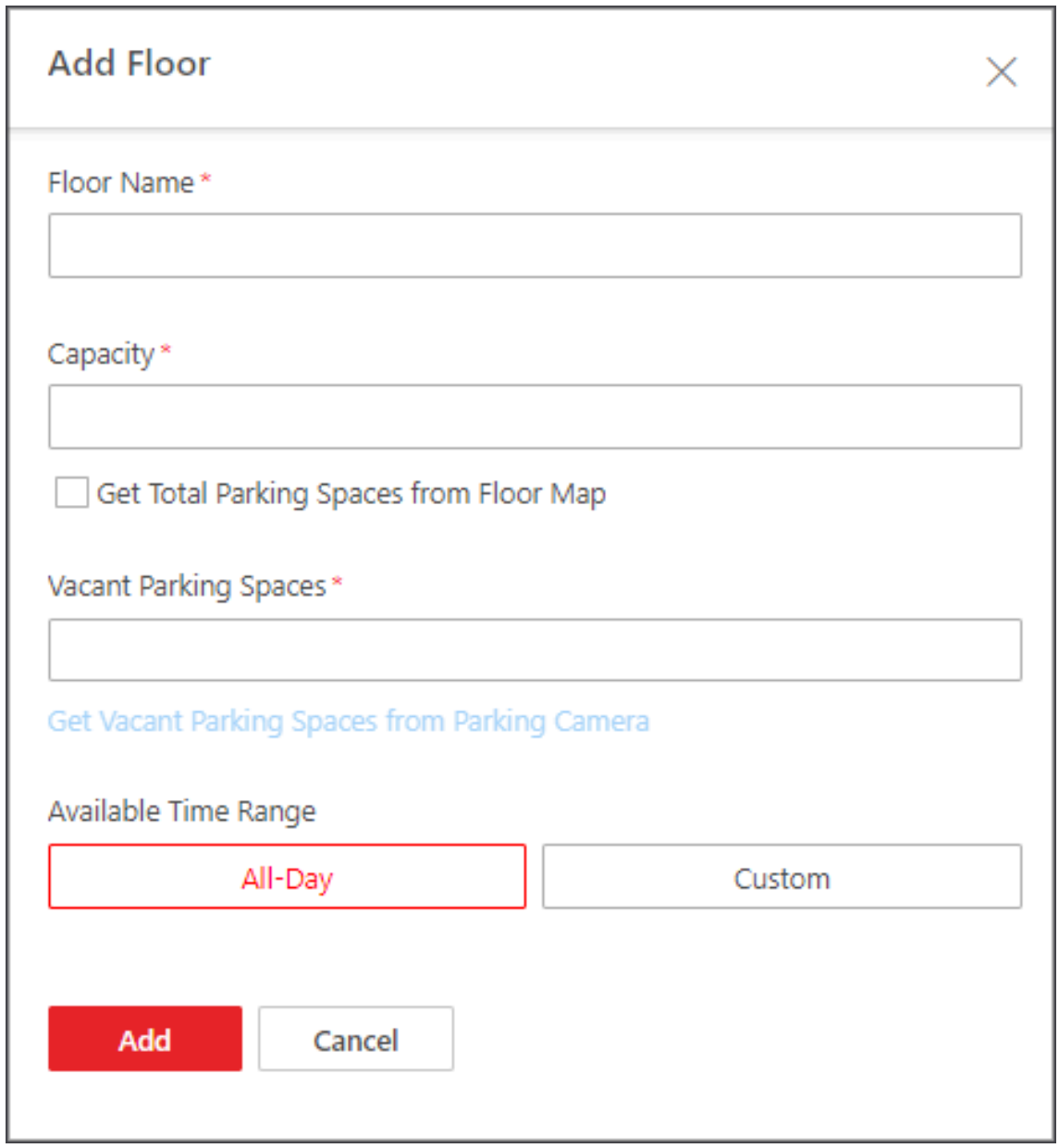



**Figure 15-37 Add Floor Pane**

2. Create a name for the floor.
3. Set the total number of parking spaces (capacity) of the floor.

**Note**

If you have added parking spaces on the map of the floor, you can check **Get Total Parking Spaces from Floor Map**, and the number of parking spaces on the map will be synchronized here.

4. Set the number of vacant parking spaces of the floor.

**Note**

If the floor has been related with parking camera(s), you can check **Get Vacant Parking Spaces from Parking Camera**, and the number of vacant parking spaces counted by the parking camera(s) will be synchronized here.

5. Set the period during which the floor is available for parking. Click **All-Day**, or click **Custom** to customize a period.
6. Click **Add**.

   You will enter the page where you can relate devices, configure a map, mark guidance screen, and configure types for parking spaces.

## 15.6.2 (Optional) Link Devices to the Floor

After adding a floor to the parking lot, you can link devices (guidance terminal, indoor guidance screen, ANPR camera, query terminal) to the floor. A guidance terminal can be related with multiple parking cameras for management, such as playing the live video and playing back the recorded video from linked cameras. A guidance screen can display the number of vacant parking spaces in the parking lot and guide vehicles to the area where there are vacant parking spaces. An ANPR camera can recognize license plates, capture the pictures of license plates and vehicles, and count the number of vehicles entering and exiting the parking lot that will be used to calculate the number of vacant and occupied parking spaces.

**Steps**

1. Enter the following page after adding a floor.

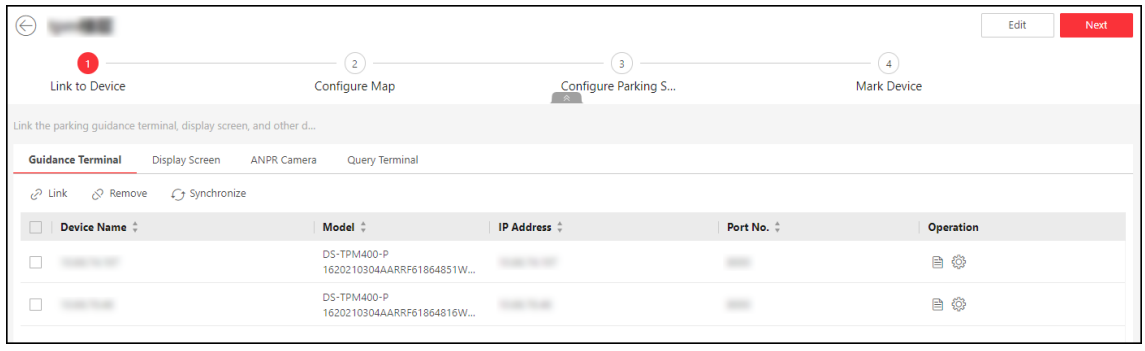



**Figure 15-38 Link Device**

2. Click **Link to Device**.
3. Link device(s) to the floor.

   1) Click **Guidance Terminal → Link** , and select guidance terminal(s) to link.

   **Note**

   After relating a guidance terminal, you can perform the following operation(s) if needed.

- Select one or multiple guidance terminals and click **Synchronize** to synchronize the parking spaces monitored by the parking cameras linked to the terminal(s).
- Click to view the parking camera(s) linked to a guidance terminal, and the parking spaces monitored by the parking camera(s).
- Click to edit settings of a guidance terminal.

2) Click **Display Screen → Link** , and select indoor guidance screen(s) to link.

**Note**

If both of the ANPR cameras and parking cameras are linked to a parking lot, the indoor guidance screen displays the number of vacant parking spaces counted by ANPR cameras and parking cameras respectively.

3) Click **ANPR Camera → Link** , and select ANPR camera(s) to link. After relating a camera, you need to set its calculation mode in the **Entry and Exit** field.

**Standard (Entry Detection) / Standard (Exit Detection)**

Count the number of vehicles entered detected by the camera as the number of vehicles entered the floor, and count the vehicles exited as those exited the floor. Select this mode when the direction for entry detection configured on the camera is the same as the actual entry direction.

**Reverse (Entry Detection) / Reverse (Exit Detection)**

Count the number of vehicles entered detected by the camera as the number of vehicles exited the floor, and count the vehicles exited as those entering the floor. Select this mode when the direction for entry detection configured on the camera is opposite to the actual entry direction.

**Note**

- An ANPR camera can be linked to different floors.
- The number of vacant parking spaces on the top floor is counted by the ANPR camera.

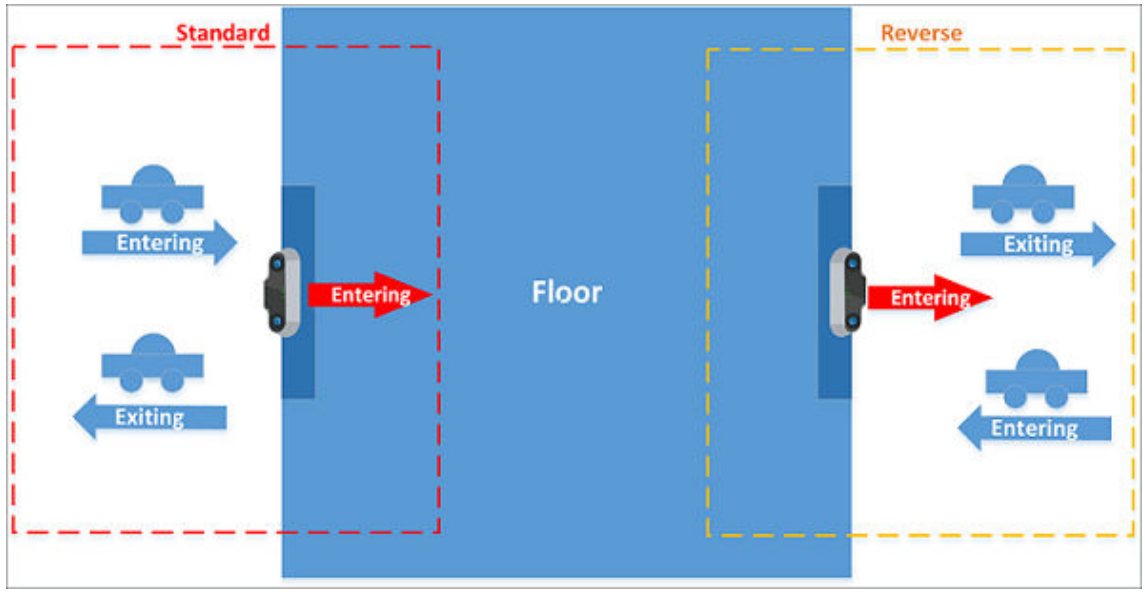



**Figure 15-39 Schematic Diagram of Calculation Mode**

4) Click **Query Terminal** and select query terminal(s) to link.

**Note**

A query terminal is mounted inside a parking lot and is installed with the Self-Service Vehicle Finding Client for vehicle owner to locate and find their vehicles in the parking lot. See ***Self-Service Vehicle Finding Client*** for details.

4. **Optional:** Select one or multiple devices, and click **Remove** to remove the device(s) from the floor.

## 15.6.3 (Optional) Configure a Map for the Floor

You can add a map to the floor, add parking spaces to the map, and configure the layout of parking spaces.

**Steps**

1. Enter the following page after linking device(s) to the floor.

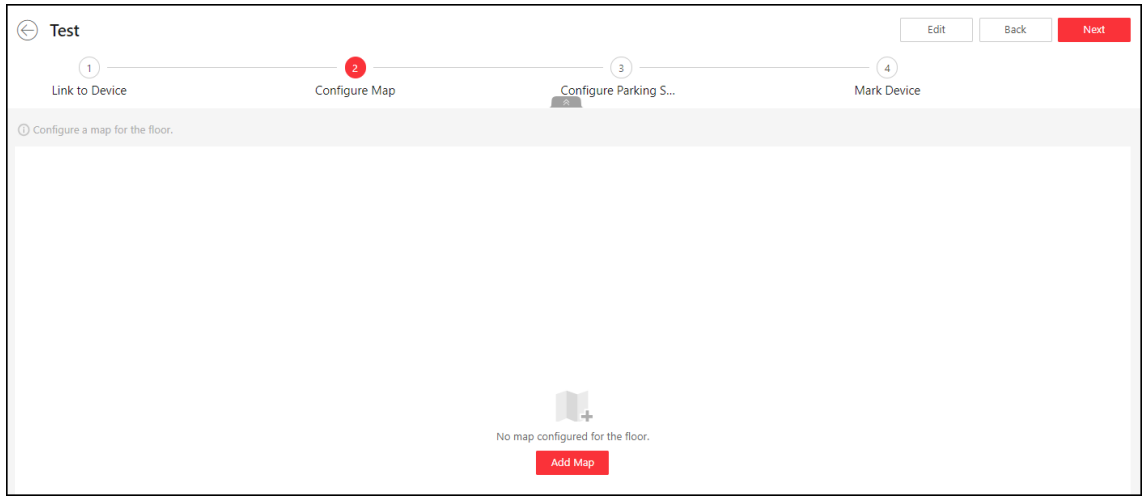



**Figure 15-40 Add a Map**

2. Click **Add Map**.
3. Select **E-Map** or **Vector Map** as the map type, and click **Confirm**.
4. Select a map from your PC and add it to the floor.

**Note**

The vector map does not support adding/deleting parking spaces. You can directly go to the next step of configuring parking space type.

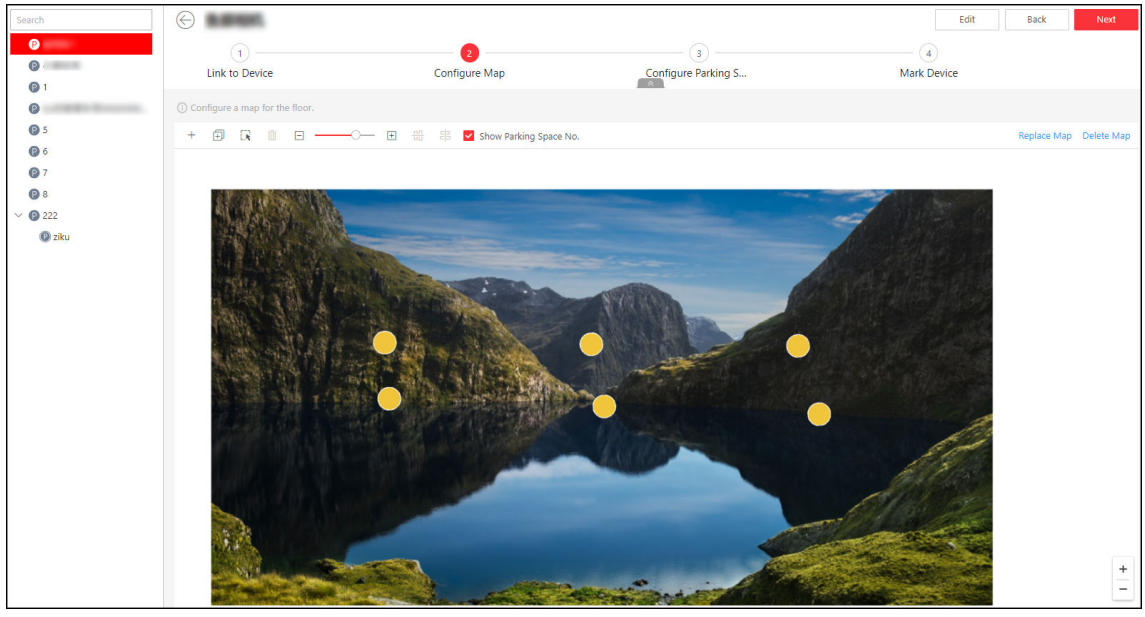



**Figure 15-41 Configure the Map**

5. Add parking space(s).
   - Add parking spaces one by one.

a. Click + to add one parking space.
b. On the pop-up panel, enter a No. for the parking space.
c. Click **Save**.

- Batch add multiple parking spaces at one time.

a. Click .
b. Click on the map to draw a line.
c. On the pop-up panel, check **Parking Space No.** or **Number of Parking Spaces** as the adding mode.

**Note**

For the **Parking Space No.** mode, the start No., end No., and No. interval are required; for the **Number of Parking Spaces** mode, the start No., end No., No. interval, and display order (i.e., ascend or descend) are required.

d. Click **Save**.

6. **Optional:** Perform the following operation(s) if needed.

| | |
|---|---|
| **Move Parking Space** | Drag a parking space to move it. |
| **Delete Parking Space(s)** | • Click one parking space (the green point) and click to delete it.<br>• Click , drag you cursor to select multiple parking spaces, and click to batch delete them. |
| **Adjust the Size of the View of Parking Space(s)** | • Click one parking space and click or to make it bigger or smaller.<br>• Click , drag you cursor to select multiple parking spaces, and click or to make them bigger or smaller. |
| **Align Parking Spaces Horizontally** | Click , drag you cursor to select multiple parking spaces, and click to align them in a horizontal line. |
| **Align Parking Spaces Vertically** | Click , drag you cursor to select multiple parking spaces, and click to align them in a vertical line. |
| **Show Parking Space No. on Map** | Check **Show Parking Space No.** to display the parking space No. on the floor map during parking space monitoring. |
| **Replace Map** | Click **Replace Map** and select a new map.<br>When a vector map is replaced with another vector map, the parking space configuration and device marking data will be retained. If you want to clear the data, you can delete the map. |

**What to do next**

Click **Next** to set types for parking spaces on the map. See ***Set Types for Parking Spaces on the Map*** .

## 15.6.4 Set Types for Parking Spaces on the Map

You can set types for parking spaces and manage the types according to actual needs.

**Steps**

**1.** Enter the following page after configuring the map.

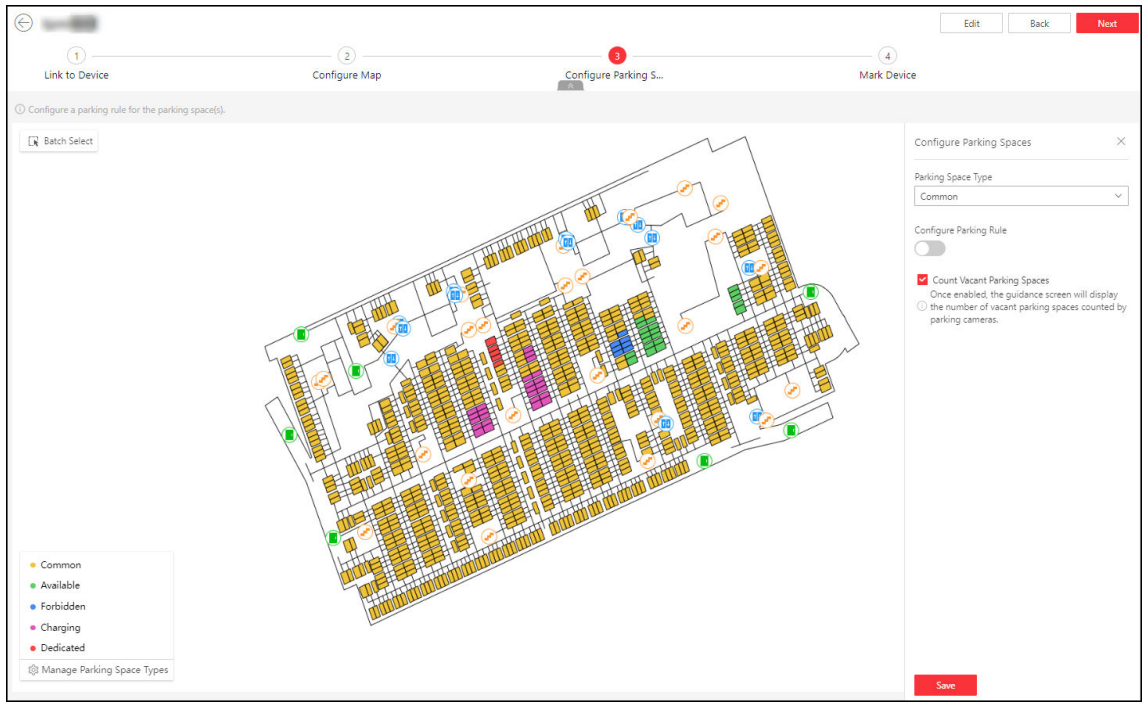



**Figure 15-42 Set Types for Parking Spaces**

**2.** Configure parking spaces.

1) Click a parking space or click **Batch Select** to select multiple parking spaces.
2) Select a type for the parking space from the drop-down list.
3) **Optional:** Switch on **Configure Parking Rule** to specify which vehicles are allowed or forbidden to park in this parking space.

**Parking Allowed**

When no vehicle is selected, all vehicles can park here by defaults.

**No Parking**

When no vehicle is selected, no vehicles can park here by defaults.

**Note**

This step is not supported during batch configuration.

4) **Optional:** Check **Reserve Parking Space** to reserve the selected parking spaces.

- The reserved parking spaces are displayed as "occupied" on the display screen and parking camera indicator light, while the platform counts available spaces based on real-time occupancy.
- During batch configuration, if some of the selected parking spaces are configured with the vacancy counting function, the checkbox will be displayed as ■ , you can still check or uncheck it.

3. **Optional:** Click **Manage Parking Space Types** on the floating pane and perform the following operations.

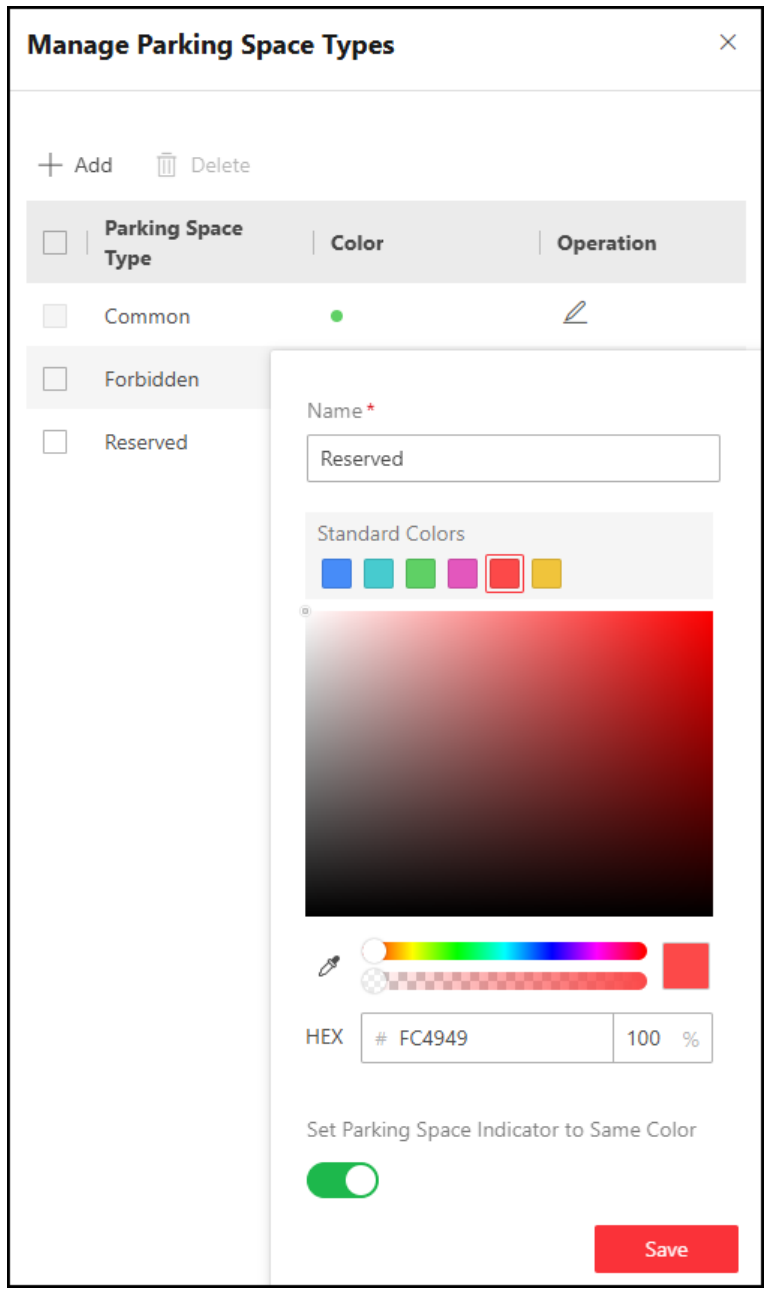



**Figure 15-43 Manage Parking Space Types**

**Add a Parking Space Type**

a. Click **Add**.
b. Create a name for the type.
c. Set a color for the type. Except the standard color, you can customize colors.

d. Enable **Set Parking Space Indicator to Same Color** to apply the selected color to the indicator lights of parking cameras monitoring this type of space.
e. Click **Save**.

**Edit a Parking Space Type**

Click ✎ to edit the name and color of a type.

**Note**

The name of the default type (common) cannot be edited.

**Delete Parking Space Type(s)**

Select one or multiple types and click **Delete** to delete them.

**Note**

The default type cannot be deleted.

**What to do next**

Click **Next** to mark device(s) on the map. See ***Mark Devices on the Map*** .

## 15.6.5 Mark Devices on the Map

You can link display screens (indoor guidance screens and parking space screens) to parking spaces in the parking lot. Once linked, the indoor guidance screen can display the number of vacant parking spaces and guide vehicles to them, while the parking space screen will display the real-time status of linked parking space.

1. Enter the following page after configuring the parking space type.

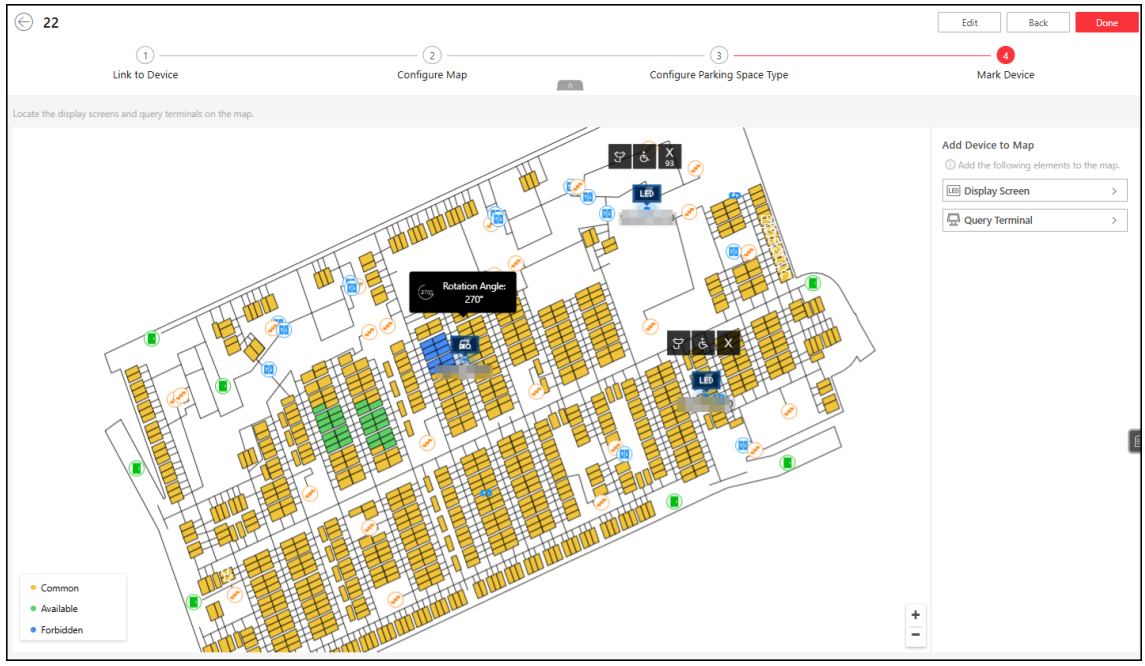



**Figure 15-44 Mark Device**

2. Add a device (display screen or query terminal) to the map by dragging the device from the device list to the map.

**Note**

As display screens, only the indoor guidance screen and parking space screen can be marked. The entrance guidance screens or entrance and exit display screens will not be displayed in the list.

3. Configure devices added to the map.
   - Query Terminal
     Click the device icon on the map, and click **Configure Rotation Angle** to configure its direction for the self-service vehicle finding client to display a more adaptable map view.
   - Indoor Guidance Screen

| Operation | Description |
|---|---|
| Link Parking Spaces | Click the device icon on the map, and click **Link Parking Space** on the pop-up menu to open the parking spaces marking pane.<br>Select the parking space(s) and click **OK** to link the selected parking space(s) with the device. |

| Operation | Description |
|---|---|
| | **Note**<br>- When you select the parking space(s), you can click a parking space icon on the map, then click **Batch Select**, or check **Select All Parking Spaces**.<br>- If the current floor has linked with multiple maps, you can click **Switch Map** to switch to another map for marking. |
| Configure Guidance Screen | Click the device icon on the map and click **Guidance Screen Configuration** on the pop-up menu to enter the Guidance Screen Configuration page. Refer to ***Link Display Screen and Set Displayed Content*** for details. |
| Check Information Currently Displayed on Screen | Click the device icon on the map and click **Guidance Screen and Parking Space Status** on the pop-up menu to check information currently displayed on the guidance screen.<br>You can click a screen to view the detailed information about the parking space(s) linked to it, such as parking space No., floor where the parking space is located, whether the parking space is occupied, and the picture of the parking space captured now.<br>**Note**<br>This function is only supported by some guidance screens. |

- Indoor Guidance Screen

| | |
|---|---|
| Link Parking Spaces | Click the device icon on the map, and click **Link Parking Space** on the pop-up menu to open the parking spaces marking pane.<br>Select the parking space(s) and click **OK** to link the selected parking space(s) with the device.<br>**Note**<br>- When you select the parking space(s), you can click a parking space icon on the map, then click **Batch Select**, or check **Select All Parking Spaces**.<br>- If the current floor has linked with multiple maps, you can click **Switch Map** to switch to another map for marking. |
| Configure Guidance Screen | Click the device icon on the map and click **Guidance Screen Configuration** on the pop-up menu to enter the Guidance Screen |

| | |
|---|---|
| | Configuration page. Refer to ***Link Display Screen and Set Displayed Content*** for details. |
| Check Information Currently Displayed on Screen | Click the device icon on the map and click **Guidance Screen and Parking Space Status** on the pop-up menu to check information currently displayed on the guidance screen.<br>You can click a screen to view the detailed information about the parking space(s) linked to it, such as parking space No., floor where the parking space is located, whether the parking space is occupied, and the picture of the parking space captured now.<br>**Note**<br>This function is only supported by some guidance screens. |

- Parking Space Screen

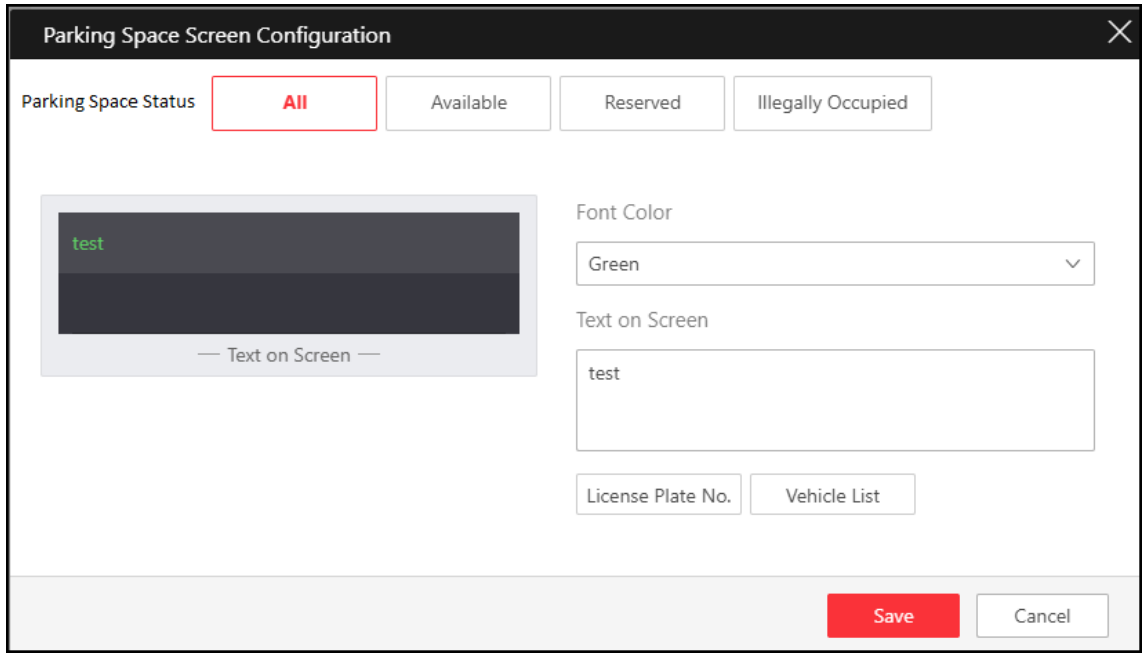



**Figure 15-45 Parking Space Screen Configuration**

| | |
|---|---|
| Configure Parking Space Screen | - Click a device icon on the map and click **Parking Space Screen Configuration** on the pop-up menu.<br>- Select a parking space status and configure the corresponding text on screen. |
| Check Information Currently Displayed on Screen | Click the device icon on the map and click **Parking Space Screen and Parking Space Status** on the pop-up menu to check |

| | |
|---|---|
| | information currently displayed on the screen and the parking space information. |

4. Click **Done** to finish the parking guidance configuration.

## 15.6.6 Calibrate Parking Spaces Regularly

To reduce the manual operation costs of a parking lot and avoid parking disputes caused by the incorrect number of vacant parking spaces displayed on the display screen, you can enable the functions of regularly calibrating vacant parking spaces on each floor or in the parking lot, so the real-time number of vacant parking spaces in the parking lot will be counted regularly and the number of vacant parking spaces to be reserved for vehicles that entered the parking lot but not parked will also be regularly counted and displayed by floor.

**Before You Start**

Make sure you have deployed ANPR cameras if you want to regularly calibrate parking spaces on floors.

**Steps**

1. On the parking guidance configuration page of a selected parking lot, click **Calibrate Parking Space Regularly** in the top right corner of the parking lot details page.

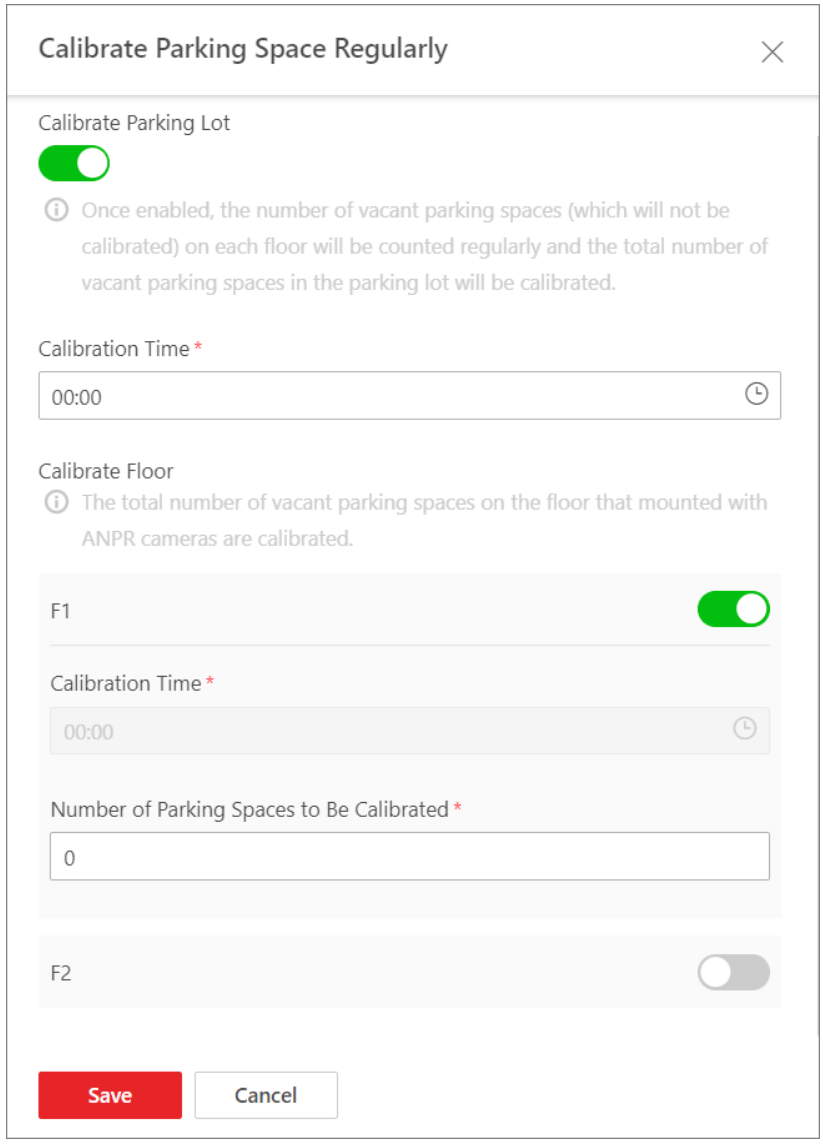



**Figure 15-46 Calibrate Parking Spaces Regularly**

2. Switch on **Calibrate Parking Lot**.
3. Set the calibration time for the parking lot.

   **Example**

   If you set the calibration time to 12:00, the number of vacant parking spaces in the parking lot will be calibrated at 12:00 every day.
4. In the Calibrate Floor field, enable the switch beside a floor name.

**Note**

Only the floors deployed with ANPR cameras will be displayed in the Calibrate Floor field.

Two configuration fields will be displayed and the calibration time will automatically inherit that from the parking lot.

5. Set a number of parking spaces on the floor to be calibrated.

**Note**

The entered number must be smaller than the total number of parking spaces on the floor, otherwise, a window with the error information will appear when you save the settings.

6. **Optional:** Repeat the above two steps to enable regular calibration for other floors.
7. Click **Save**.

## 15.6.7 Configure Parking Space Lights-out Time

To reduce energy costs, some commercial parking lots require scheduled shutdowns of parking camera indicator lights. You can configure the parking space lights-out schedule for parking lots based on their operation requirements.

**Steps**

1. On the parking guidance configuration page of a selected parking lot, click **Configure Parking Space Lights-out Time** at the top.

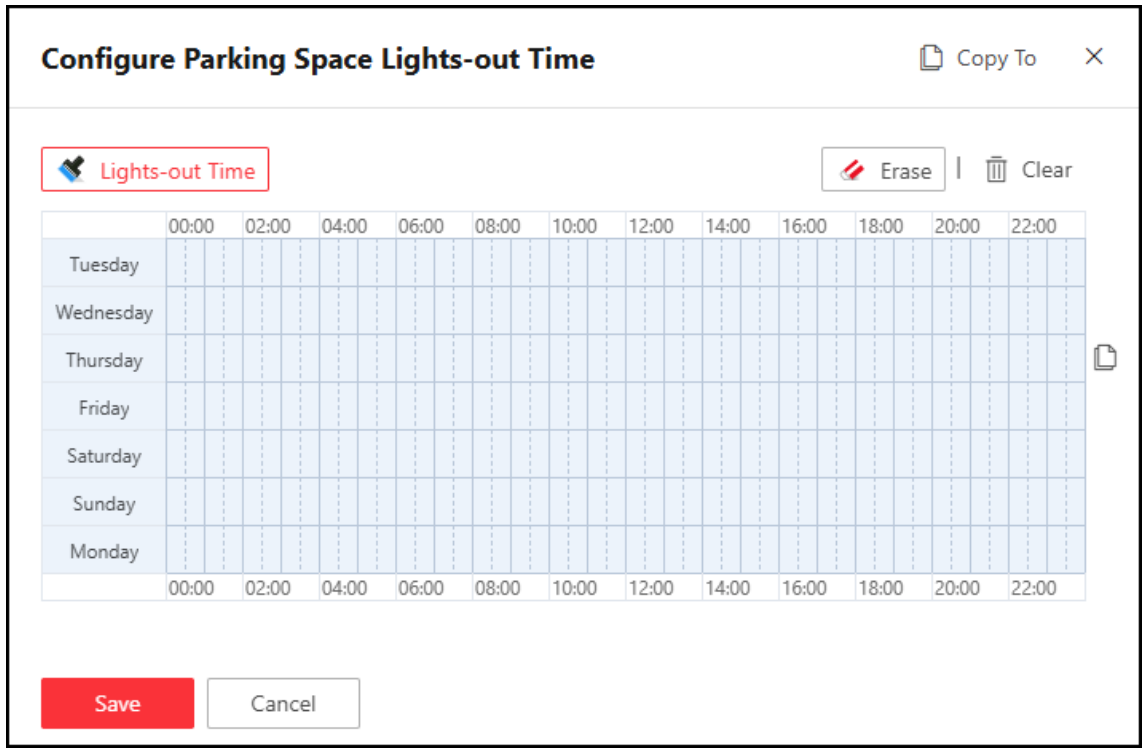



**Figure 15-47 Configure Parking Space Lights-out Time**

2. Click **Lights-out Time** and click or drag on the timetable to define the period.

**Note**

Up to two periods are allowed per day.

3. **Optional:** Copy a day's schedule or a parking lot's schedule.

| | |
|---|---|
| **Copy a Day's Schedule** | Click at the end of the table row to copy the current day's schedule to other days. |
| **Copy a Parking Lot's Schedule** | Click **Copy to** in the upper-right corner to copy the schedule of current parking lot to other parking lots. |

4. Click **Save**.

## 15.6.8 Parking Space Monitoring

On the Parking Space Overview page, you can view the statistics of parking spaces, and can search for specific statistics by parking space No., license plate No., and parking time.

The Parking Space Overview page displays parking occupancy status (including parking spaces occupancy rate, vacant/occupied/unknown-status parking spaces counts, and the number of overtime parking and parking violations) of parking lots.

**Note**

- If there is no map added for the parking lot, parking space information will be overlaid directly on the monitoring video.




**Figure 15-48 Parking Space Overview of Parking Lot**

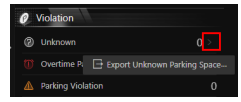
Click on a floor name to view its parking space statistics, and switch the statistics dimension by selecting **Occupancy Status Overview** or **Parking Duration Overview**.




**Figure 15-49 Floor Parking Space Overview**

The following operations are available on the floor parking space overview page.

**Table 15-1 Operations During Parking Space Monitoring**

| Operation | Description |
|---|---|
| Export Information of Unknown-Status Parking Spaces | Select → **Export Unknown Parking Space Information** next to the number of unknown-status parking spaces under **Violation**. The details such as the related parking space numbers and the corresponding parking lot and floor information will be exported to the local PC as an XLSX file.<br>  |
| View Details of a Parking Space | • Hover over a parking space to show the details.<br>• Click a parking space to view its real-time status and search for parking records. |
| Reserve Parking Spaces | Click **Configure Reserved Parking Space**, drag and select the parking spaces.<br>• Click **Reserve Parking Space** to reserve selected parking spaces.<br>• Click **Cancel Parking Space Reservation** to cancel reserved parking spaces. |

| Operation | Description |
|---|---|
| | **Note**<br>The parking camera indicator light of reserved parking spaces will displays as an occupancy status. |

## 15.7 Record Search

You can search for various types of records, including passing vehicles, parking records, payment records, etc. Each record is attached with highly detailed information related to it, which can give the vehicle owner and the administrator a whole picture of the vehicle's activity in a parking lot. Therefore, these records can help you to manage parking much better.

### 15.7.1 Search for Passing Vehicles Detected by Entrances & Exits

If the license plate number of a vehicle is recognized by cameras or capture units linked to an entrance and exit, you can search for the related vehicle passing information.

**Steps**

1. On the left navigation pane, select **Search → Vehicle Search at Entrance & Exit** .
2. Select one or multiple entrances and exits where you want to search for the vehicle passing records.
3. Set the time duration for search.
4. Switch on and set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

**Note**

For the Middle East and North Africa regions, you can enable Country/Region, Plate Category, License Plate Size, License Plate Type, and License Plate Color for more accurate search.

**Country/Region**

Select the country/region where the vehicle's license plate number is registered.

**License Plate No.**

- **No License Plate**: Search for vehicles without license plates.
- **With License Plate**: Enter a vehicle's license plate number or part of it.

**Enter or Exit**

Select whether the vehicle is entering or exiting.

**How to Open Barrier**

Select how the barrier gate is opened when a vehicle enters/exits the parking lot. **Manual** indicates that a security guard manually controlled the barrier gate to open after identifying the vehicle owner; **Auto Allow for Entry and Exit** indicates that the barrier gate opened automatically after the license plate number was recognized by a capture unit; **Not Opened** indicates that the barrier gate did not open even after the capture unit recognized the license plate number.

**Reason**

Select the reason(s) for allowing or not allowing the vehicle to enter/exit from the drop-down list.

**Vehicle List**

Select from the drop-down list to search for records of temporary vehicles, visitor vehicles, registered vehicles, or vehicles in the blocklist or other custom lists.

**Additional Information**

The item(s) of additional vehicle information you customized.

5. Click **Search**.

The matched results will be displayed on the right.

6. **Optional:** Perform the following operations as needed.

| | |
|---|---|
| **View Vehicle Details** | Click a license plate number in the License Plate No. column to open the vehicle details pane.<br>You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit. |
| **View Owner's Picture** | Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit.<br>**Note**<br>This operation can only be performed if the entry & exit modes of the parking lot are set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** . |
| **Export a Passing Vehicle** | Click **Export** and select **Excel** or **CSV** as the format of the exported file. |

**Note**

- If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file. The exported pictures will be named and sorted by the capture time.
- No more than 500 passing vehicles with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them.
- No more than 100,000 passing vehicles without captured pictures can be exported at one time.

## 15.7.2 Search for Parking Records

On the platform, you can search for parking records generated in a specific parking lot or records of a specific vehicle by setting relevant search conditions according to actual needs, and perform further operations, such as viewing the detailed information of vehicles and exporting the records to your PC.

**Steps**

1. On the left navigation pane, select **Search → Parking Record Search** .
2. Set the time duration for search.
3. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   **Parking Space No.**

   Enter the parking space No. of a specific parking lot to search for records of vehicles which park or have parked in that parking space.

   **Parking Status**

   Select a parking status. **Parking** indicates the vehicle still parks in the parking lot, whereas **Exit** indicates the vehicle has already left the parking lot.
4. Click **Search**.

   The matched results will be displayed on the right.

   **Note**

   You can click ☰ or ⊞ to switch between list mode and thumbnail mode.
5. **Optional:** Perform the following operations as needed.

| | |
|---|---|
| **View Vehicle Details** | Click a license plate number in the License Plate No. column to open the vehicle details pane.<br>You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit. |

**View Owner's Picture**

Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit.

**Note**

This operation can only be performed if the entry & exit modes of the parking lot are set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** .

**Export Vehicle Parking Records**

Click **Export** and select **Excel** or **CSV** as the format of the exported file.

**Note**

- If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file.
- No more than 500 parking records with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them.
- No more than 100,000 parking records without captured pictures can be exported at one time.

## 15.7.3 Search for Parked Vehicles

If the actual number of vacant parking spaces is different from the number displayed on the guidance screens, you can search for the vehicles that already exited but still recorded in the parking lot to edit the vehicle information. For example, for parking lots requiring all on-site vehicles out at the end of a day, you can search for the vehicles that are still in the parking lot and export the vehicles' information. In another situation, if a vehicle is manually allowed to exit the parking lot, the number of vacant parking spaces may not be updated in time. In this situation, you can search for the vehicle and delete it from the vehicle list of the parking lot to update the number of vacant parking spaces.

**Steps**

1. On the left navigation pane, select **Search → Parked Vehicle Search** .
2. Select a parking lot from the drop-down list.
3. Switch on and set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   If the License you purchased does not support ANPR functions, the displayed search conditions may vary.

   **Country/Region**

   Select the country/region where the vehicle's license plate number is registered.

   **License Plate No.**

- **No License Plate**: Search for vehicles without license plates.
- **With License Plate**: Enter a vehicle's license plate number or part of it.

**How to Open Barrier**

Select how the barrier gate is opened when a vehicle enters/exits the parking lot. **Manual** indicates that a security guard manually controlled the barrier gate to open after identifying the vehicle owner; **Automatic** indicates that the barrier gate opened automatically after the license plate number was recognized by a capture unit; **Barrier Not Open** indicates that the barrier gate did not open after the capture unit recognized the license plate number.

**Vehicle List**

Select from the drop-down list to search for records of temporary vehicles, visitor vehicles, registered vehicles, or vehicles in the blocklist or other custom lists.

**Additional Information**

The item(s) of additional vehicle information you customized.

4. Click **Search**.

The matched results will be displayed on the right.

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

| | |
|---|---|
| **View Vehicle Details** | Click a license plate number in the License Plate No. column to open the vehicle details pane.<br>You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit. |
| **View Owner's Picture** | Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit.<br>**Note**<br>This operation can only be performed if the entry & exit modes of the parking lot is set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** . |
| **Export All Records** | Click **Export** and select **Excel** or **CSV** as the format of the exported file.<br>**Note**<br>• If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file.<br>• No more than 500 records with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them.<br>• No more than 100,000 records without captured pictures can be exported at one time. |

| | |
|---|---|
| **Delete Vehicle from Parking Lot** | Click **Delete All** to remove all displayed vehicles from the parking lot.<br>Select vehicles and click **Delete** to delete the selected records. |

## 15.7.4 Search for Payment Records

When a vehicle pays the parking fee and exits the lot, its payment details (such as the payment method and transaction time) are recorded in the platform. You can search for records by specific parking lots or vehicles using customizable filters, and export the results to your local device. These statistics enable you to monitor transaction activity, facilitating better parking lot management.

**Steps**

1. On the left navigation pane, select **Search → Payment Record Search** .
2. Set the time duration for search.
3. Set the search condition(s). Here we only introduce conditions that may confuse you.

   **Operator**

   Select the person responsible for collecting the fee from the drop-down list.

   **Payment Method**

   Select how the parking fee is paid.

   - Cash
     Payment is made in cash.
   - Vehicle Owner Account
     The fee is deducted from the owner's account balance.
   - POS
     Paid via POS terminal.

   **Payment Source**

   Select where the parking fee is paid. (**Booth**, **Toll Center**, and **Automatic Payment Machine**)

   **Parking Fee Rule**

   Select the parking rate for fee calculation.
4. Click **Search**.
5. **Optional:** In the Amount Due column, click  to check the parking fee details.
6. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

## 15.7.5 Search for Vehicle Top-Up and Refund Records

In the Search module, you can search for the top-up and refund records of vehicles or parking lots, and export the records to your PC. With the statistics, you can monitor some of the transactions happened in the parking lots, which can help you manage the parking lots better.

**Steps**

1. On the left navigation pane, select **Search → Top-Up and Refund Record Search** .
2. Set the search mode to **By Vehicle** or **By Person**.
3. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
4. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   **Transaction Type**

   Select the transaction type. **Top-Up** indicates adding money to a parking pass to keep it valid or extend its validity period; **Refund** indicates getting paid back (e.g., when you paid too much for one parking).

   **Transaction Method**

   Select how the transaction is made. **Cash** indicates the transaction is made in cash; **Vehicle Owner Account** indicates the transaction is made with/to the vehicle owner's account.

   **Operator**

   Select the person responsible for handling the top-up/refund transaction from the drop-down list.
5. Click **Search**.
6. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

## 15.7.6 Search for Transaction Records of Vehicle Owner Account

You can search for the transaction records of a specific vehicle owner account, and export the records to your PC. With the statistics, you can see the details about the transactions between a vehicle owner and the parking lot.

**Steps**

1. On the left navigation pane, select **Search → Account Transaction Record Search** .
2. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
3. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   **Transaction Type**

Select the transaction type. **Top-Up** indicates adding money to a parking pass to keep it valid or extend its validity period; **Refund** indicates getting paid back (e.g., when you paid too much for one parking); **Deduction** indicates paying parking fees with the account balance.

**Operator**

Select the person responsible for handling the transaction from the drop-down list.

4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

## 15.7.7 Search for Work Records of Operators

You can search for the work records of operators (i.e., the person responsible for payment management) to get the information such as the on-duty and off-duty time of an operator as well as the amount of payment the operator managed during working hours.

**Steps**

1. On the left navigation pane, select **Search → Operator Shift Search** .
2. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
3. Select an operator (the person responsible for collecting the fee or handling a transaction) or **All** from the drop-down list.
4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

## 15.7.8 Search for Coupon Records

You can search for coupon records and view detailed information about the coupons, such as the discount rule, expiration time, and the coupon status.

**Steps**

1. On the left navigation pane, select **Search → Coupon Record Search** .
2. **Optional:** Select a specific parking lot, coupon status, and discount rule from the drop-down lists as needed.
3. Click to specify a time range for the search.

**Note**

Only coupons of which the effective period falls within the specified time range will be displayed as search results.

4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

## 15.8 Statistic and Report

In the Statistics and Report module, you can view and export the operation report and transaction report of each parking lot for having a general understanding of the usage, revenue, and expenditure of the parking lot.

### 15.8.1 Export Operation Reports of Parking Lots

You can view the statistics related to the operations of parking lots, such as real-time parking space statistics, parking space occupancy rate and times, parking duration distribution, and traffic flow. The statistics can give you a general picture of the operation situation of parking lots.

**Steps**

1. On the left navigation pane, select **Statistics and Reports → Operation Report** .
2. In the top right corner of the Operation Report page, click **Configure Report Contents** and select the types of statistics to be displayed for the parking lot(s).

   **Note**

   - Any user with the permission to view the parking lot operation is able to set which content(s) to display on the page.
   - All users share a common configuration.

3. Select a report type from **Day**, **Month**, and **Year**, or click **Custom** to customize a time period for generating the operation data.
4. View statistics of all parking lots by default or select a parking lot from the drop-down list to view statistics of the specific parking lot.

   **Note**

   You can view the last update time and refresh the statistics by clicking **Refresh** on the top right corner.

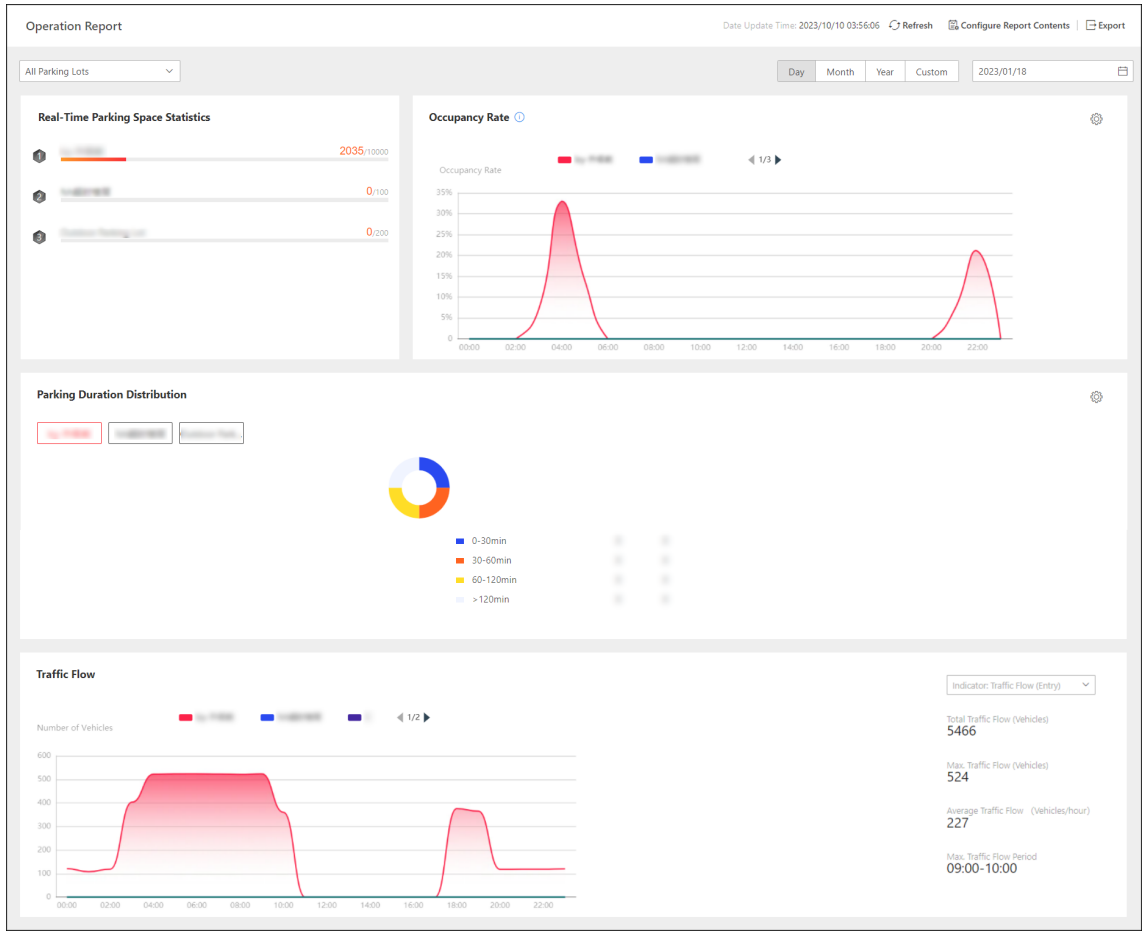



**Figure 15-50 Operation Report of All Parking Lots**

**Table 15-2 Operation Report of All Parking Lots**

| Statistics Type | Description |
|---|---|
| Real-Time Parking Space Statistics | Display the real-time numbers of occupied and total parking spaces in each parking lot. |
| Occupancy Rate | Click ⚙ to set a time period. The statistics generated in the set period will be displayed. |
| Parking Duration Distribution | Click ⚙ to set the parking duration(s) to be calculated.<br>The distribution of the selected parking duration(s) will be displayed.<br>Click tabs above the pie chart to switch between parking lots for viewing the corresponding distribution. |
| Traffic Flow | In the top right corner of the area, select one or multiple indicators from the drop-down list. |

| Statistics Type | Description |
| --- | --- |
| | **Traffic Flow (Entry)**<br>Total number of vehicles that entered parking lots.<br>**Traffic Flow (Exit)**<br>Total number of vehicles that exited parking lots.<br>**Note**<br>If the user only has permissions related to parking guidance, there will be no drop-down list in this area used for selecting indicators. |

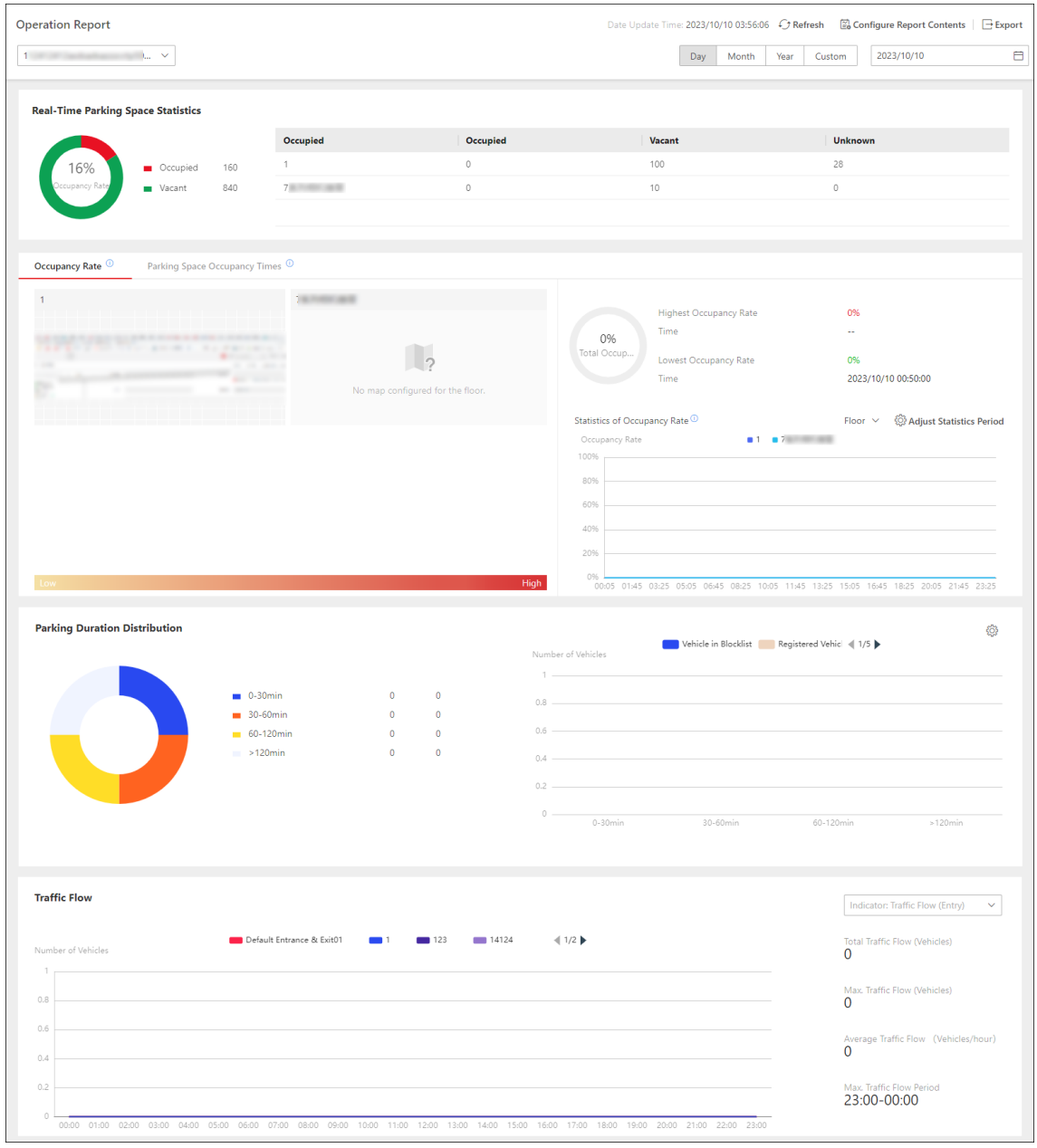



**Figure 15-51 Operation Report of a Parking Lot**

**Table 15-3 Operation Report of a Parking Lot**

| Statistics Type | Description |
|---|---|
| Real-Time Parking Space Statistics | Display the real-time numbers of occupied/vacant parking spaces in the parking lot and numbers of occupied/vacant/unknown parking spaces on each floor of the parking lot. |
| Occupancy Rate | Click **Adjust Time Period** at the right to set a time period.<br>The map on each floor of the parking lot will be displayed, and you can click the map to enlarge it for viewing. The parking space icons on the map are marked with different colors that indicate different occupancy rates. The deeper the color, the higher the occupancy rate of the parking space during the selected time.<br>The statistics generated in the set time period, including the total occupancy rate of the parking lot, the maximum/minimum occupancy rate, the corresponding happening time, and the occupancy rate of each floor or parking space type, will be displayed. |
| Parking Space Occupancy Times | The report of occupancy times indicates the exposure rates of areas in the parking lot, which can help the parking lot manager to determine whether to place advertisements.<br>Click **Adjust Time Period** at the right to set a time period.<br>The map on each floor of the parking lot will be displayed, and you can click the map to enlarge it for viewing. The parking space icons on the map are marked with different colors that indicate different occupancy times. The deeper the color, the more times the parking space is taken up during the selected time period.<br>The statistics generated in the set time period, including the total occupancy times of the parking lot, the maximum/minimum occupancy times, the corresponding parking floors, and the occupancy times of each floor, will be displayed. |
| Parking Duration Distribution | Click to set the parking duration(s) to be calculated.<br>The distribution of the selected parking duration(s) will be displayed in a pie chart.<br>The number(s) of vehicles with the selected parking duration(s) will be displayed by vehicle list. |
| Traffic Flow | In the top right corner of the area, select one or multiple indicators from the drop-down list. |

| Statistics Type | Description |
|---|---|
| | **Traffic Flow (Entry)**<br>Number of vehicles that entered the parking lots.<br>**Traffic Flow (Exit)**<br>Number of vehicles that exited the parking lots.<br>**By: Entrance and Exit**<br>If only one indicator is selected, you can select the entrance(s) and exits(s) for displaying the traffic flow by entrance and exit.<br>**By: Vehicle List**<br>If only one indicator is selected, you can select the vehicle list(s) for displaying the traffic flow by vehicle list.<br>**Note**<br>If the user only has permissions related to parking guidance, there will be no drop-down list in this area used for selecting indicators. |

5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported data file(s), and click **Save** to download the report and the detailed statistics to the local PC.

**Note**

The entire operation report will be saved as a PDF files by default. For the operation report of a parking lot, the floor map(s) containing the parking space occupancy information will also be saved as the PDF file(s) named by the floor name(s) by default. Other than the report, each type of statistics will be individually exported in the format you selected.

## 15.8.2 Export Transaction Reports of Parking Lots

You can view the statistics (trend and type) related to the revenue and expenditure of parking lots, the analysis of revenue sources, and the analysis of payment methods. The statistics can give you a general picture of the transactions done in the parking lots.

**Steps**

1. On the left navigation pane, select **Statistics and Reports → Transaction Report** .

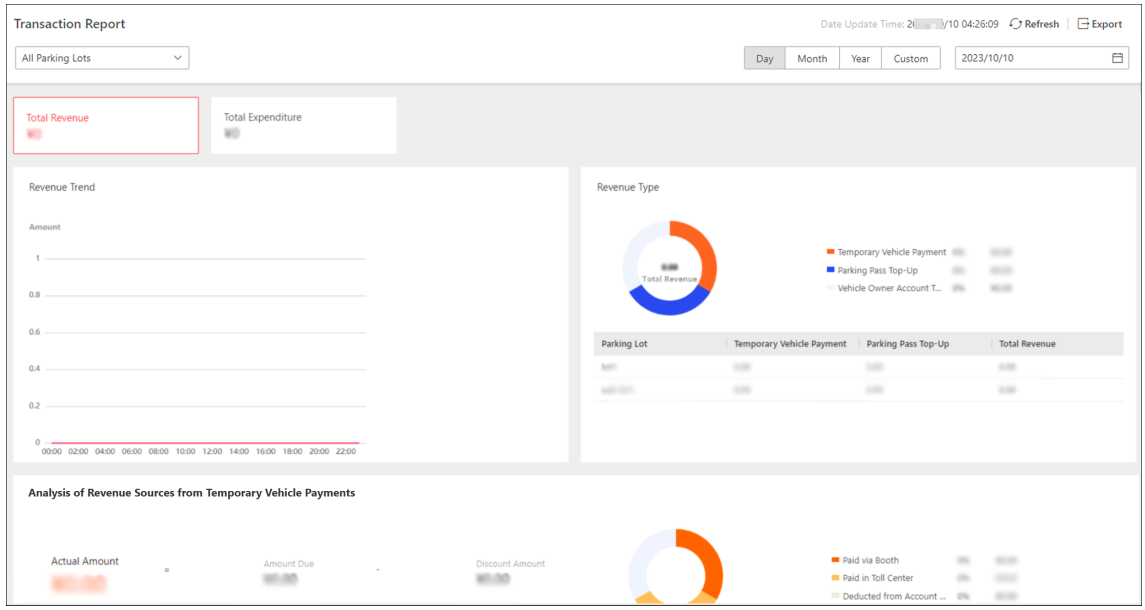



**Figure 15-52 Transaction Report Page**

2. Select a parking lot from the drop-down list.
3. Select a report type from **Day**, **Month**, and **Year**, or select **Custom** to display the operation data generated within the custom period.
4. Click **Total Revenue** to view the statistics of revenue, and the parking fee analysis of temporary vehicles.
5. Click **Total Expenditure** to view the statistics of expenditure.
6. **Optional:** Click **Refresh** on the top right corner to refresh the statistics.
7. **Optional:** In the upper-right corner, click **Export** to save the analysis report to your PC.

## 15.8.3 Configure Scheduled Overtime Parking Reports

You can configure scheduled overtime parking reports by specifying parking lot(s) and the statistical cycle. Once set, the platform will send an email to the specified recipient(s) regularly with the report attached, which shows the records of overtime parking vehicles detected during the set time period.

**Before You Start**

- Set the email template with recipient information, subject, and content.
- Set email settings such as the sender's email address, name, and SMTP server address and port No.
- Make sure you have added the parking lot(s). For details, refer to ***Add Parking Lot*** .

**Steps**

1. On the left navigation pane, select **Basic Configuration → Overtime Parking Report** .
2. Enter the Create Report page.

- For configuring scheduled reports for the first time, click **Add** in the middle of the page.
- If you have configured scheduled reports before, click + at the top of the left pane.

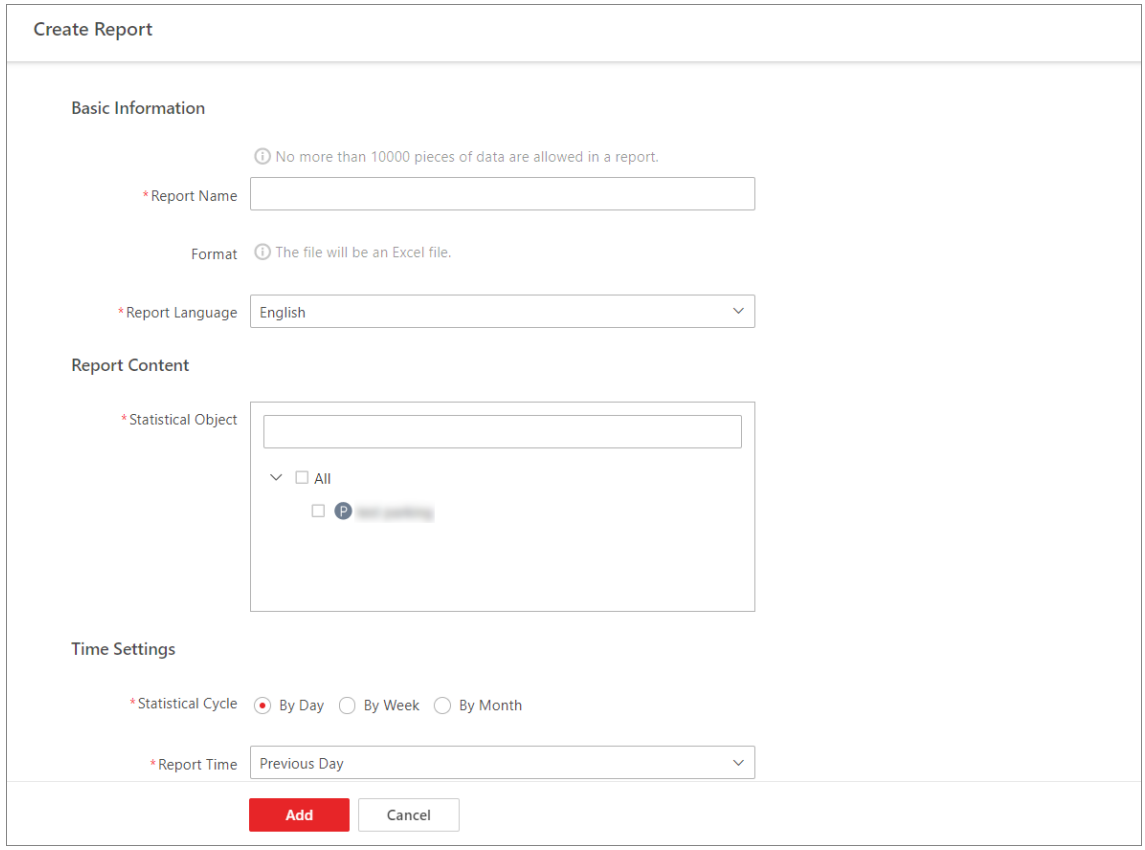



**Figure 15-53 Configure Scheduled Report**

3. Create a name for the report and select a report language from the drop-down list.
4. Select the parking lot(s) as the statistical object(s).
5. Set time parameters for the report.

**Statistical Cycle**

**By Day**

The report contains analysis results of a day.

**By Week**

The report contains analysis results of a week or two weeks.

**By Month**

The report contains analysis results of a month.

**Report Time**

The available report time varies with the statistical cycle you selected.

- If the statistical cycle is set to **By Day**, you can select **Previous Day** as the report time, which means the report will contain analysis results of the day (24 hours) before the sending time.
- If the statistical cycle is set to **By Week**, you can select **Recent 7 Days** or **Recent 14 Days** as the report time, which means the report will contain analysis results of the last 7/14 days before the sending time.
- If the statistical cycle is set to **By Month**, you can select **Current Month** or **Last Month** as the report time, which means the report will contain analysis results of the current/last month.

**Sending Date / Sending Time**

- When the statistical cycle is set to **By Day**, the Sending Date field is required, as you need to select the day(s) of the week to determine the day(s) of which analysis results will be contained in the report and on which the report will be sent.
  For example, if you select **Friday** and **Monday**, and set the Sending Time field to ***08:00***, a report containing analysis results of Thursday will be sent at 08:00 on Friday and another report containing analysis results of Sunday will be sent at 08:00 on Monday.
- When the statistical cycle is set to **By Week**, you should set the time and a day of the week to determine the period during which analysis results will be contained in the report and at what time the report will be sent.
  For example, if you select **Recent 7 Days** in the Report Time field and set the Sending Time field to ***Sunday*** and ***12:00***, a report containing analysis results between the last Sunday and the current Saturday (7 days in total) will be sent at 12:00 on the current Sunday.
- When the statistical cycle is set to **By Month**, you should set the time and a specific date to determine the period during which analysis results will be contained in the report and at what time the report will be sent.
  For example, if you select **Current Month** in the Report Time field and set the Sending Time field to ***30*** and ***12:00***, a report containing analysis results of the current month will be sent at 12:00 on the 30th.

**Effective Period (Optional)**

Set a period in which the above time settings will take effect. Outside the effective period, no report will be sent according to the configured sending time.

6. **Optional:** Set the advanced parameters.

**Send Report via Email**

Select an email template from the drop-down list to define the recipient information and email format (subject and content), so that the report can be sent to the recipient(s) regularly via email.

**Note**

You can select an existing email template or click **Add** to add a new one.

**Upload to SFTP**

Configure SFTP settings including the SFTP address, port No., user name, password, and the saving path for the report to be uploaded to the SFTP server regularly.

**Note**

You can also click ⚙ → **SFTP Settings** at the top of the left pane to configure the corresponding parameters.

**Save to Local Storage**

Configure a saving path for the report to be saved to the local storage regularly.

**Note**

You can also click ⚙ → **Configure Local Storage** at the top of the left pane to configure the saving path.

**7.** Click **Add** to finish setting the scheduled report rule.

## 15.9 Set Basic Parameters of Parking Management

On the Web Client, you can select the statistical source of parking and enable fuzzy search for the Self-Service Vehicle Finding Client in the parking lot to help vehicle owners find their vehicles more quickly and conveniently. The date format displayed on the Self-Service Vehicle Finding Client or display screens of the parking lot can also be predefined.

On the left navigation pane, select **Basic Configuration → Basic Parameter** .

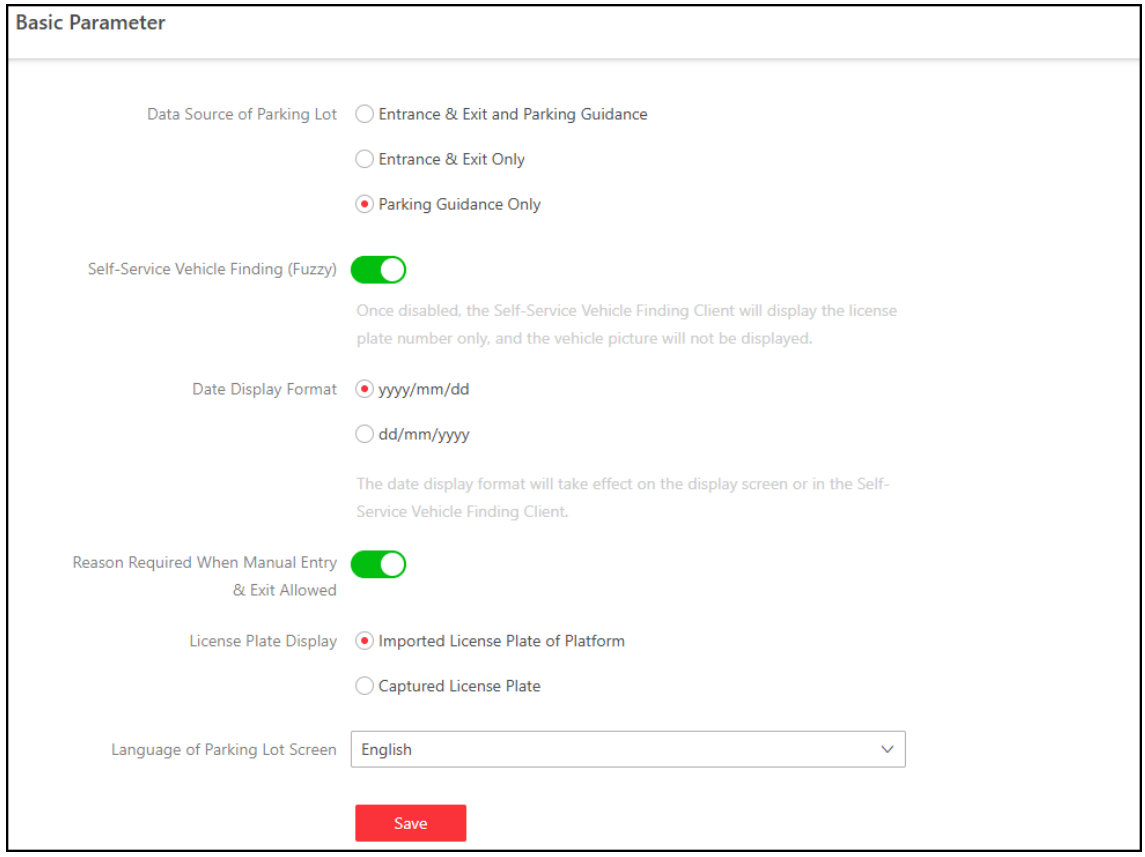



**Figure 15-54 Set Basic Parameters**

## Data Source of Parking

Select a source for parking statistics. The following table shows the relations between statistics types and sources.

**Table 15-4 Relations Between Statistics Types and Sources in Different Modes**

| Mode | Statistics Type | Source |
|---|---|---|
| Entrance & Exit and Parking Guidance Mode | (Web Client) Real-Time Parking Space Statistics in Operation Report | Entrance & Exit |
| | (Web Client) Parking Space Occupancy Statistics in Operation Report | Parking Guidance |
| | (Web Client) Parking Duration Distribution in Operation Report | Entrance & Exit |
| | (Web Client) Traffic Flow Statistics in Operation Report | Entrance & Exit |

| Mode | Statistics Type | Source |
|---|---|---|
| | (Web Client & Control Client) Parking Space Overview | Entrance & Exit |
| | (Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring | Entrance & Exit |
| | (Control Client) Occupancy Rate of Floor in Parking Space Monitoring | Parking Guidance |
| | Alarms "No Vacant Parking Space" and "Overstayed Parking" | Entrance & Exit |
| Entrance & Exit Mode | (Web Client) Real-Time Parking Space Statistics in Operation Report | Entrance & Exit |
| | (Web Client) Parking Space Occupancy Statistics in Operation Report | By default, the statistics is not displayed. You can configure the source by yourself. |
| | (Web Client) Parking Duration Distribution in Operation Report | Entrance & Exit |
| | (Web Client) Traffic Flow Statistics in Operation Report | Entrance & Exit |
| | (Web Client & Control Client) Parking Space Overview | Entrance & Exit |
| | (Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring | Entrance & Exit |
| | (Control Client) Occupancy Rate of Floor in Parking Space Monitoring | Entrance & Exit |
| | Alarms "No Vacant Parking Space" and "Overstayed Parking" | Entrance & Exit |
| Parking Guidance Mode | (Web Client) Real-Time Parking Space Statistics in Operation Report | Parking Guidance |
| | (Web Client) Parking Space Occupancy Statistics in Operation Report | Parking Guidance |
| | (Web Client) Parking Duration Distribution in Operation Report | Parking Guidance |
| | (Web Client) Traffic Flow Statistics in Operation Report | By default, the statistics is not displayed. You can configure the source by yourself. |

| Mode | Statistics Type | Source |
|---|---|---|
| | (Web Client & Control Client) Parking Space Overview | Parking Guidance |
| | (Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring | Parking Guidance |
| | (Control Client) Occupancy Rate of Floor in Parking Space Monitoring | Parking Guidance |
| | Alarms "No Vacant Parking Space" and "Overstayed Parking" | Parking Guidance |

### Self-Service Vehicle Finding (Fuzzy)

Switch on **Self-Service Vehicle Finding (Fuzzy)** to enable fuzzy search for the Self-Service Vehicle Finding Client. Once enabled, the Self-Service Vehicle Finding Client will display license plate numbers without displaying vehicle pictures when finding vehicles, so that the time consumption in vehicle finding will be reduced.
For details, refer to ***Self-Service Vehicle Finding Client*** .

### Date Display Format

Select **yyyy/mm/dd** or **dd/mm/yyyy** in the Date Display Format field to determine the date format displayed on the Self-Service Vehicle Finding Client or display screens of the parking lot.

### Reason Required When Manual Entry & Exit Allowed

Switch on **Reason Required When Manual Entry & Exit Allowed** to require entering a reason when the entry & exit is allowed manually.

### License Plate Display

Select the license plate display mode for display screens, real-time events, and passing records of parking lots. **Imported License Plate of Platform** is to display the registered license plate number, and **Captured License Plate** is to display the actual license plate number recognized by ANPR cameras.

### Language of Parking Lot Screen

Set the language of contents (e.g., entry and exit not allowed prompt) displayed on parking lot screens. The corresponding language packages should be installed on the parking lot screens in advance.

## 15.10 Audio Media Library Management

The platform supports uploading and managing audio files (.wav), which can be applied to connected devices (e.g., entrance/exit control device). Users can configure broadcast content for

different vehicle types (e.g., registered, visitor, or VIP) to deliver personalized prompts, such as welcome or parking access permission expiration messages.

On the left navigation pane, click **Audio Media Library**.

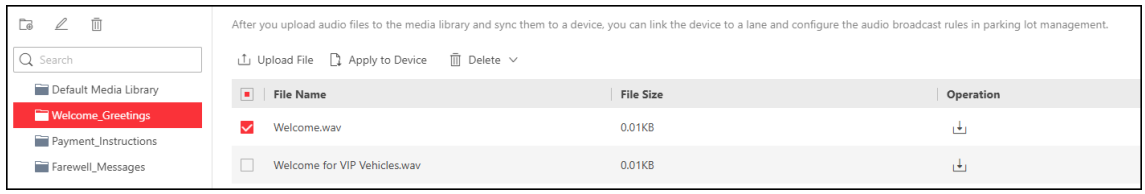



**Figure 15-55 Audio Media Library**

## Audio Media Library Management

For convenient management of audio files, you can group them in different library by purpose.

**Table 15-5 Audio Media Library Management**

| Function | Description |
|---|---|
| Add a Library | Click in the upper-left corner and enter the library name. |
| Edit a Library | Select a library and click in the upper-left corner to edit the library name. |
| Delete a Library | Select a library and click in the upper-left corner to edit the library name. |

## Audio Files Management

**Table 15-6 Audio Files Management**

| Function | Description |
|---|---|
| Upload Audio Files | Select a library and click **Upload File** to upload upload .wav files.<br>**Note**<br>The maximum file size is 400 KB. |
| Apply Audio Files to Device(s) | 1. Select audio file(s) and click **Apply to Device**.<br>2. Check **Specified Device(s)** to choose target devices, or leave unchecked to apply to all.<br>3. Check **Apply All** to overwrite the existing audio files on the target device(s) with the selected ones |
| Download an Audio File | In the Operation column, click . |
| Delete Audio File(s) | Select the audio file(s) and click **Delete** or click **Delete All** to remove all audio files from the library. |

### Configure Broadcast Content

Once the audio files are applied to devices, navigate to **Parking Lot Management** to configure broadcast content for specific vehicle types or scenarios of the devices linked to lanes.

## 15.11 Self-Service Vehicle Finding Client

The self-service vehicle finding client is for users to find their vehicles in the parking lot easily and accurately.

- You can search for your vehicle by license plate No., parking space No., and the time the vehicle is parked in.
- If your vehicle does not have a license plate, you can click **No License Plate**, and set specific conditions to search for it.
- When you are searching for your vehicle, both your and your vehicle's position will be displayed on the map, which makes it more helpful for you to find your vehicle.
- When entered a parking lot, you can quickly find vacant parking spaces. When leaving a parking lot, you can get the route to find the vehicle on the map by entering the license plate number.

**Note**

On the Web Client, you can choose whether to enable fuzzy search for the self-service vehicle finding client and set the date display format of the client. For details, see ***Set Basic Parameters of Parking Management*** .

# Chapter 16 ANPR (Automatic Number Plate Recognition)

You can search for passing vehicles detected by ANPR cameras and UVSSs (Under Vehicle Surveillance Systems), generate a report for showing the number of passing vehicles detected by the specified ANPR camera(s) during the specific period, and set parameters to regularly send the generated report to target recipients.

On the top navigation bar, select → **Passing Management** → **ANPR** .

## 16.1 Search for Passing Vehicles Detected by Cameras and UVSSs

If the added ANPR (Automatic Number Plate Recognition) cameras and UVSSs (Under Vehicle Surveillance Systems) are properly configured, and the vehicles' license plates are successfully detected and recognized, you can search for the related passing vehicle information.

**Before You Start**

Make sure the License you purchased supports ANPR function.

**Steps**

1. On the left navigation pane, click **Passing Vehicle Search** .
2. Select **Camera** or **UVSS** as the type of sources that detected the passing vehicles.
3. Select the source(s).
   - If **Camera** is selected as the source type, click , select the current site or a remote site, and specify the ANPR camera(s).
   - If **UVSS** is selected as the source type, check the UVSS(s).
4. Set the time duration for search.
5. Switch on and set the search condition(s) according to your needs. Here we only introduce some conditions that may confuse you.

**Note**

For the Middle East and North Africa regions, you can enable Country/Region, Plate Category, License Plate Size, License Plate Type, and License Plate Color for more accurate search.

**Country/Region**

The country/region where the vehicle's license plate number is registered.

**License Plate Number**

- **No License Plate**: Search for vehicles without license plates.
- **With License Plate**: Enter a keyword to search for vehicles by license plate number.

**Driving Speed**

Range of vehicle driving speed. This condition is available only when the source type is selected as **Camera**.

**Driving Direction**

- **Forward**: The vehicle moved toward the camera with its headstock facing the camera.
- **Reverse**: The vehicle moved away from the camera with its rear facing the camera.
- **Other**: The vehicle moved toward or away from the camera in other directions.

**Vehicle List**

Search for passing vehicles in the specific vehicle list(s). This condition is available only when the source type is selected as **Camera**.

**Additional Information**

The item(s) of additional vehicle information you customized. For how to customize vehicle information, refer to ***Customize Vehicle Information*** .

6. Click **Search**.

The matched passing vehicles will be displayed on the right.

7. **Optional:** Perform the following operation(s) after searching for passing vehicles.

| | |
|---|---|
| **View Vehicle Details** | Click a license plate number in the License Plate No. column to open the vehicle details pane.<br>You can view the captured vehicle / undercarriage / license plate picture, the recognized license plate number, the vehicle owner information, the vehicle information, and the detection source information. |
| **Export Passing Vehicles** | Click **Export** and select **Excel** or **CSV** as the exported file format.<br>• If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file.<br>• No more than 500 passing vehicles with captured pictures can be exported in the Excel format at one time. Otherwise, you need to go to the Control Client to export them.<br>• No more than 100,000 passing vehicles without captured pictures can be exported at one time.<br>• Check the export task status and progress in **Download Center**. |
| **Sort Search Results** | **Sort by Time**<br>Sort search results by the time when vehicles are passing through the camera or UVSS.<br>**Sort by Vehicle Passing Times**<br>Sort search results by times that vehicles passed through the camera. |

## 16.2 Generate Vehicle Analysis Report

For ANPR cameras, you can generate a report to show the number of passing vehicles detected by specified cameras during specified time periods.

**Steps**

1. On the left navigation pane, click **Vehicle Analysis** .
2. Select the camera(s) for this report.
   1) Click in the Camera field to open the Select Camera pane.
   2) Select a site from the drop-down list to display its areas.
   3) Click an area to show the ANPR cameras within it.

   **Note**

   Only online ANPR cameras are displayed.
   4) Check the camera(s) for analysis.

   **Note**

   You can select up to 20 ANPR cameras at a time.
   5) Click anywhere outside the pane to finish.
3. Select the report type as daily report, weekly report, monthly report, or annual report, or customize the time interval for a report.

   **Daily Report**

   The daily report shows data on a daily basis. The platform will calculate the number of vehicles in each hour of one day.

   **Weekly Report / Monthly Report / Annual Report**

   As compared with the daily report, the weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The platform calculates the number of vehicles on each day of a week, on each day of one month, and in each month of one year.

   **Custom Time Interval**

   Customize the days in the report to analyze the number of vehicles on each day or in each month of the custom time interval.
4. Set the time or a time period for analysis.
5. Enable **Driving Speed** and set the speed range.
6. Click **Generate Report**.

   The statistics of passing vehicles detected by all the selected camera(s) are displayed on the right pane.

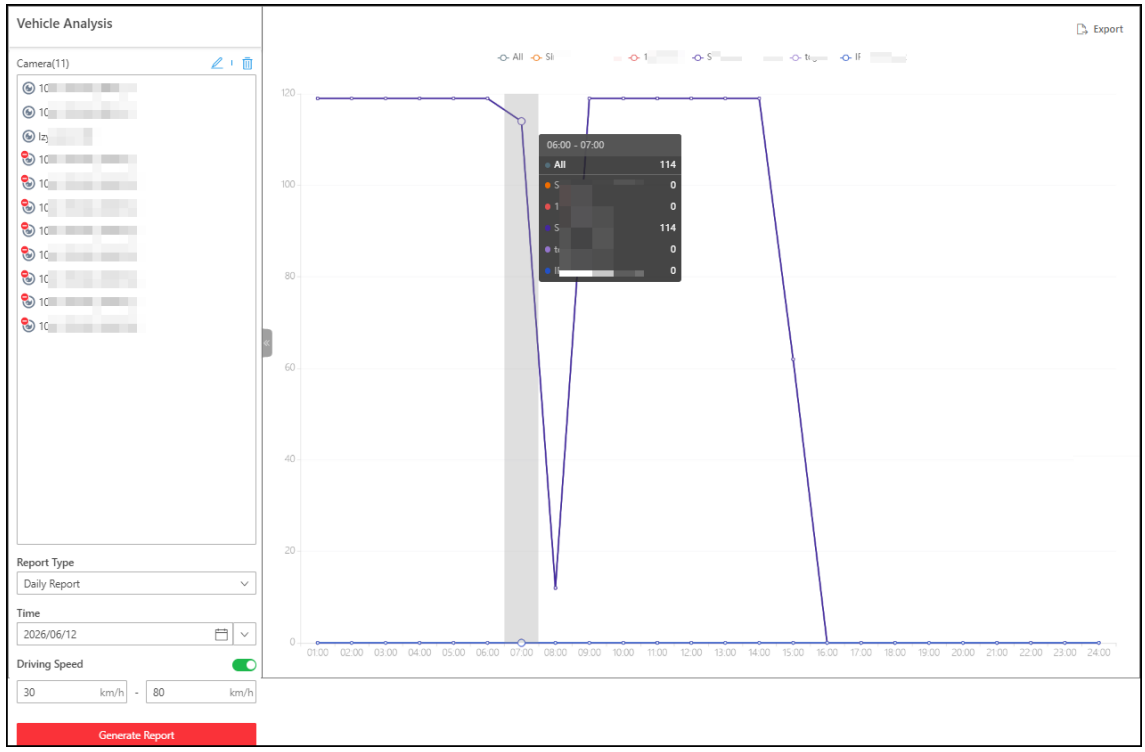



**Figure 16-1 Vehicle Analysis Report**

7. **Optional:** Export the generated report to the local PC.
   1) Click **Export** in the top right corner of the report pane.

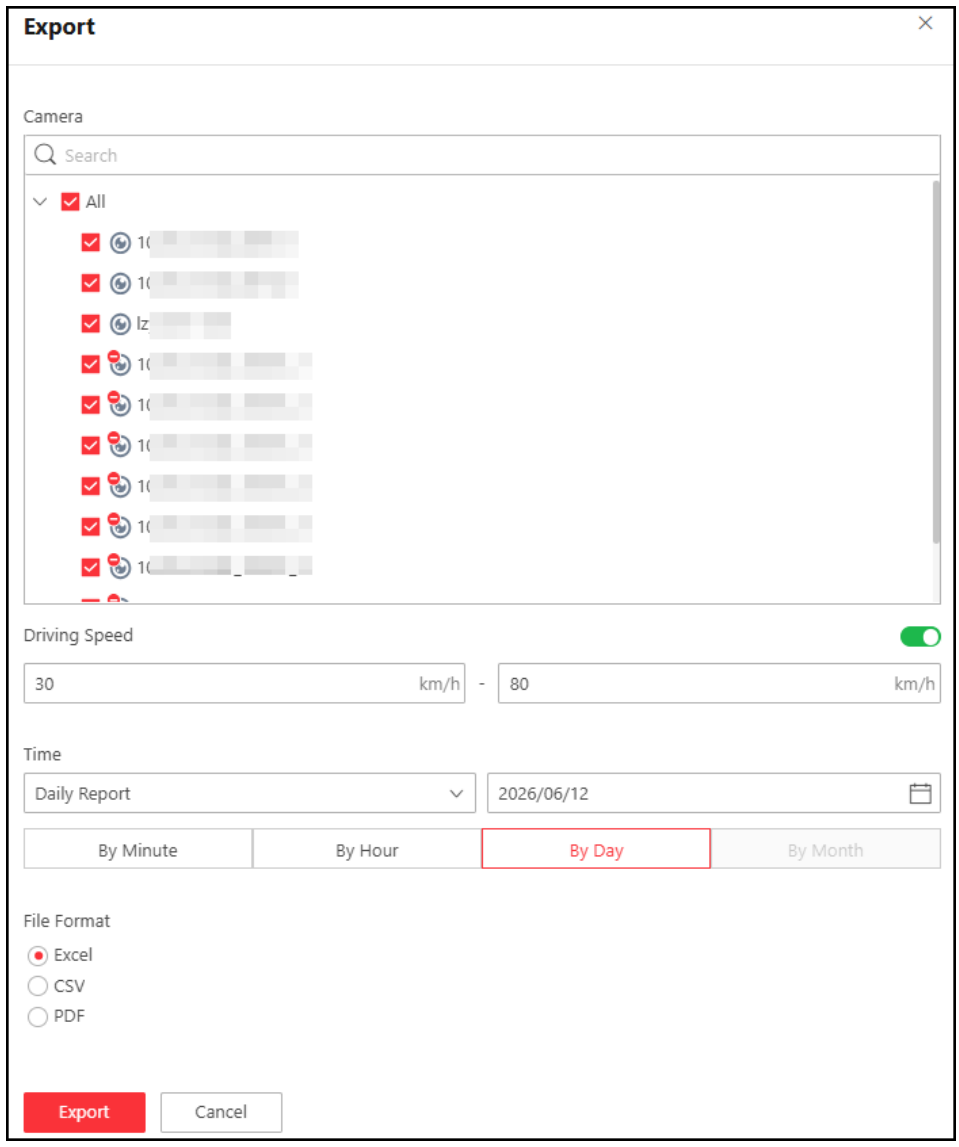



**Figure 16-2 Export Vehicle Analysis Report**

2) **Optional:** Select the camera(s), set the driving speed range, and change the report type or time.
3) Select a shorter time period to view more detailed data of each camera.

**By Minute**

The exported report shows the detailed data of each minute for each camera (if the camera has been configured to report vehicle analysis data to the platform every minute). This option is only available for the daily report.

**By Hour**

The exported report shows the detailed data of each hour for each camera. This option is available for the daily/weekly/monthly/customized-interval report.

**By Day**

The exported report shows the detailed data of each day for each camera. This option is available for all types of reports.

**By Month**

The exported report shows the detailed data of each month for each camera. This option is available for the monthly/annual report.

4) Set the exported file format to **Excel**, **CSV**, or **PDF**.
5) Click **Export** to start exporting the report.

**Note**

You can check the export task status and progress in Download Center.

## 16.3 Send Vehicle Analysis Reports Regularly

You can set a regular report rule for specified ANPR cameras. Once set, the platform will send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of passing vehicles detected by these ANPR cameras during the set time periods.

**Before You Start**

Set the email template with recipient information, subject, and content, and set email account. For details, refer to ***Email Settings*** .

**Steps**

1. On the left navigation pane, click **Scheduled Report Configuration** .
2. Enter the Create Report page.
   - For the first time, click **Add** in the middle of the Scheduled Report Configuration page.
   - For non first time, click + at the top of the left pane.

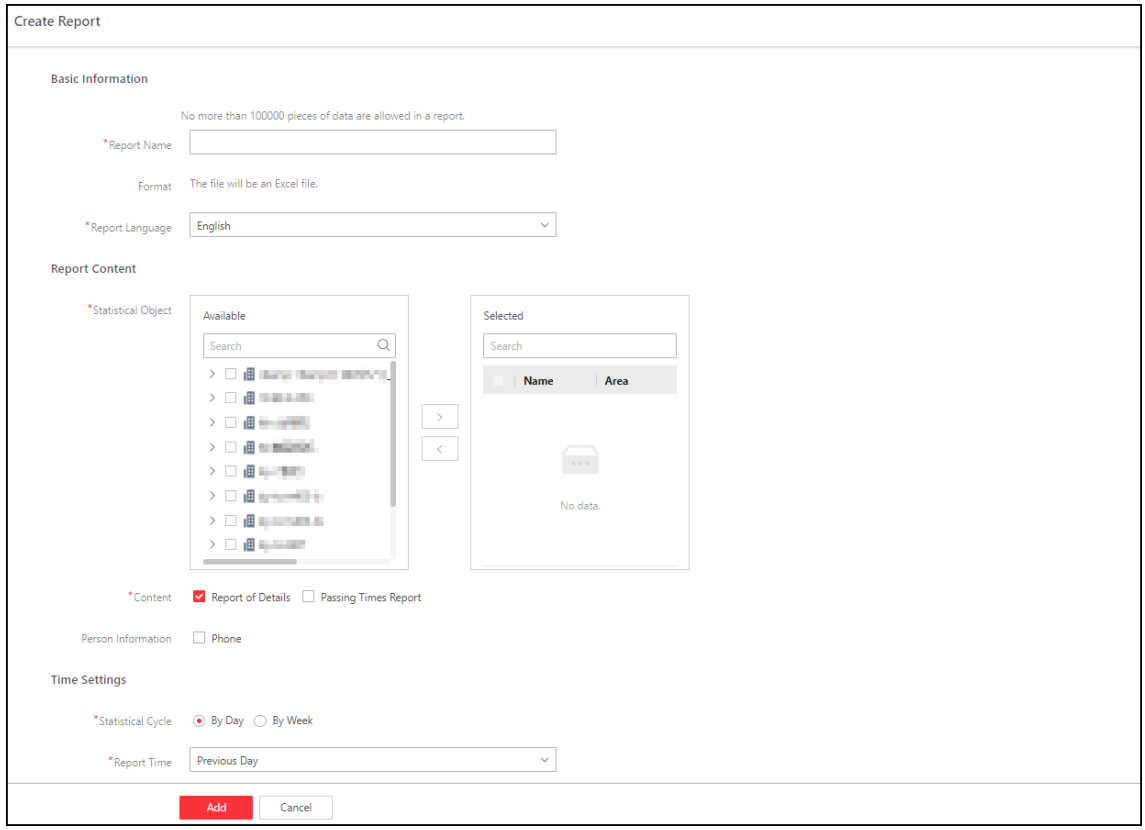



**Figure 16-3 Create Report Page**

3. Create a name for the report and select a report language from the drop-down list.
4. Set the report content.

   **Statistical Object**

   Select the ANPR camera(s) whose analysis results should be contained in the report.

   **Content**

   Check **Report of Details** or **Passing Times Report** or both of them to determine the content contained in the report. If you checked **Passing Times Report**, you can get the statistics of vehicle passing times in the report.

   **Person Information**

   Check the sensitive information about the vehicle owner to be exported in the report.
5. Set time parameters for the report.

   **Statistical Cycle**

   **By Day**

   The report contains analysis results of a day.

   **By Week**

   The report contains analysis results of a week or two weeks.

**Report Time**

The available report time varies with the statistical cycle you selected.

- If the statistical cycle is set to **By Day**, you can select **Previous Day** as the report time, which means that the report will contain analysis results of the day (24 hours) before the sending time.
- If the statistical cycle is set to **By Week**, you can select **Recent 7 Days / Recent 14 Days** as the report time, which means that the report will contain analysis results of the recent 7/14 days before the sending time.

**Send Date / Send Time**

- When the statistical cycle is set to **By Day**, the Send Date field is required, as you need to select the day(s) of the week to determine the day(s) of which analysis results will be contained in the report and on which the report will be sent.
  For example, if you select **Friday** and **Monday** in the Send Date field, and set the Send Time field to ***08:00***, a report containing analysis results of Thursday will be sent at 08:00 on Friday and another report containing analysis results of Sunday will be sent at 08:00 on Monday.
- When the statistical cycle is set to **By Week**, you should set the time and a day of the week to determine the period during which analysis results will be contained in the report and at/on which the report will be sent.
  For example, if you select **Recent 7 Days** in the Report Time field and set the Send Time field to ***Sunday*** and ***12:00***, a report containing analysis results between the last Sunday and the current Saturday (total 7 days) will be sent at 12:00 on the current Sunday.

**Effective Period (Optional)**

Set a period in which the above time settings will take effect. Outside the effective period, the report will not be sent according to the configured sending time.

6. **Optional:** Set advanced parameters.

**Send Report via Email**

Select an email template from the drop-down list to define the recipient information and email format, so that the report can be regularly sent to the recipient via email.

**Note**

You can click **Add** to add a new email template.

**Upload to SFTP**

Configure SFTP settings including address, port No., user name, password, and saving path for the report to be uploaded to the SFTP regularly.

**Note**

You can also click → **SFTP Settings** at the top of the left pane to open the SFTP Settings pane to configure the corresponding parameters.

**Save to Local Storage**

Configure a saving path for the report to be saved to the local storage regularly.

**Note**

You can also click → **Configure Local Storage** at the top of the left pane to configure the corresponding parameter.

7. Click **Add** to finish setting the scheduled report rule.

# Chapter 17 On-Board Monitoring

You can monitor driving vehicles, including locating vehicles to get their real-time GPS information and driving speed, talking to drivers via two-way audio, playing videos streamed from vehicle-mounted cameras, playing back the tracks vehicles have traveled along, and record search. You can configure driving rules to assist you to monitor vehicles by regulating the areas where vehicles are allowed or not allowed to drive and the routes that vehicles are required to drive along.

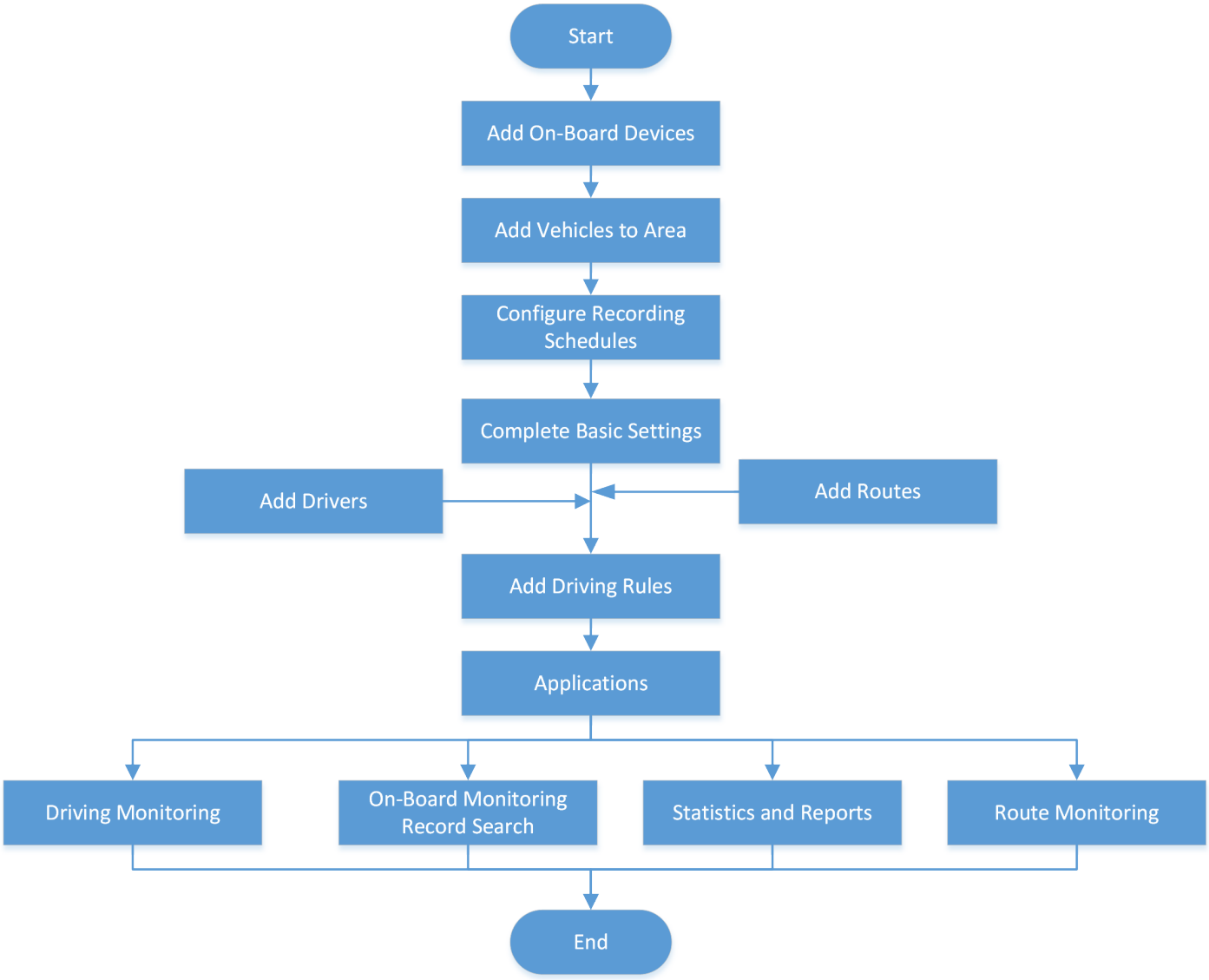



**Figure 17-1 Flow Chart of On-Board Monitoring Configuration**

- ***Basic Settings***
- ***Manage Drivers***

- ***Create Driving Rules***
- ***Manage Stop & Route***
- ***Driving Monitoring***
- ***Route Monitoring***
- ***Search On-Board Monitoring Records***
- ***Statistics and Reports***
- ***On-Board Monitoring Overview***


## 17.1 Basic Settings

To ensure the smooth operations of on-board monitoring, you need to configure the basic parameters, route parameters, fuel level monitoring parameters, and scheduled reports in advance.

### 17.1.1 Configure Basic Parameters

You can configure the basic parameters including the GIS map, and retention period of GPS data.

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Basic Configuration** → **Basic Parameters** .

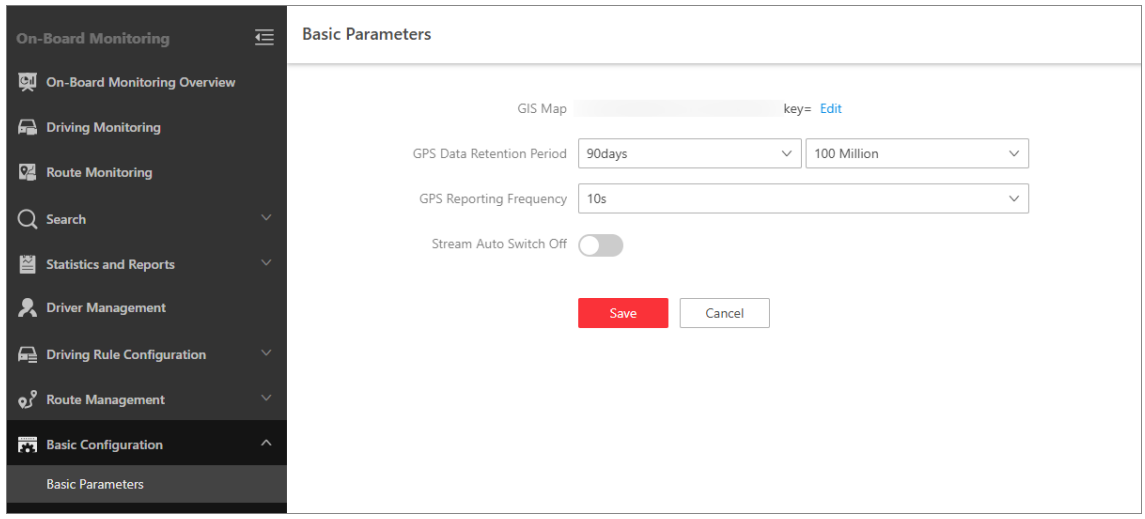



**Figure 17-2 Basic Parameter Configuration**

2. Click **Edit** to edit the GIS map.

**Note**

If you have not configured a GIS map, you should click **Configure GIS Map** to configure an online or offline GIS map first.

3. Select the retention period of GPS data.

**Note**

GPS data can be retained for one year at most.

4. Set the frequency at which the GPS information is reported to the platform.
5. Switch on **Stream Auto Switch Off** and set a duration. If a user has enabled live view or playback but does not perform any operation during the set duration, the platform will automatically stop streaming cameras to reduce data usage.

### 17.1.2 Configure Route Parameters

By configuring route parameters, you can change the rules for deciding a late departure or arrival, and you can customize the causes of unpunctual departure/arrival to select on the Route Monitoring page.

On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Basic Configuration → Route Parameters** , configure the parameters as needed, and click **Save**.

**Flexible Duration for Departure**

If the time difference between the actual departure time and scheduled departure time is less than this flexible duration you set, the departure will not be determined as an unpunctual departure.

**Flexible Duration for Arrival**

If the time difference between the actual arrival time and scheduled arrival time is less than this flexible duration you set, the arrival will not be determined as an unpunctual arrival.

**Cause of Unpunctual Departure/Arrival**

You can customize the causes of unpunctual departures or arrivals for vehicles according to your needs. When an unpunctual departure or arrival happens, you can select a cause on the Route Monitoring page.

### 17.1.3 Configure Fuel Level Monitoring Parameters

You can configure parameters for fuel level monitoring, including fuel quantity unit, fuel tank model, and fuel tolerance in tank.

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Basic Configuration → Fuel Level Monitoring Parameters** .
2. Enable **Fuel Level Monitoring Parameters**.

**Note**

When it is disabled, the functions of searching for fuel level monitoring records and generating fuel consumption statistics reports are unavailable.

3. Enable **Fuel Consumption Monitoring**.

**Note**

It is disabled by default; when it is enabled, the fuel consumption per 100 km will be displayed and reported in **Driver Analytics**.

4. Select the **Fuel Quantity Unit** for fuel consumption calculation.
5. Add a fuel tank model.
6. Click **Add**.
7. Enter the fuel tank name, capacity, fuel height, and threshold of fuel consumption.

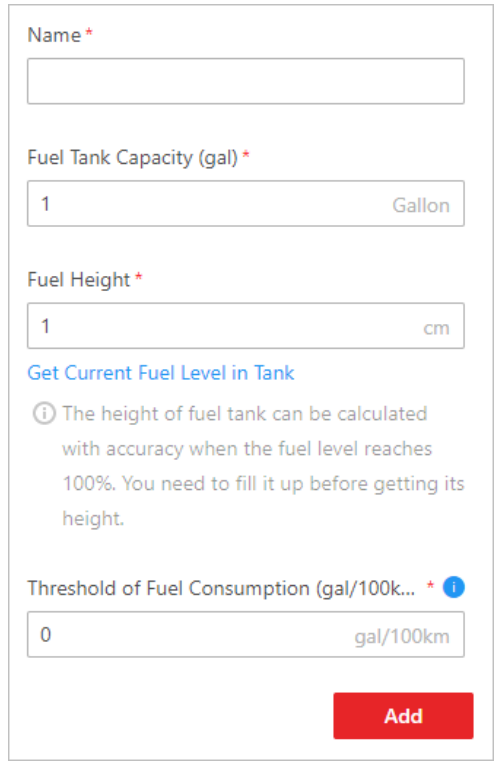



**Figure 17-3 Window of Adding Fuel Tank Model**

**Threshold of Fuel Consumption**

When the actual fuel consumption each 100 km exceeds the configured value, the Abnormal Fuel Consumption per 100 Kilometers event will be triggered.

8. Click **Get Current Fuel Level In Tank**, and then select a vehicle to get the current fuel level of the vehicle's tank.
9. Enter the **Fuel Tolerance in Tank**. Click **Save**.

## 17.1.4 Configure Scheduled Reports

You can set parameters for sending scheduled reports including driver analysis reports, fuel level analysis reports, and stop traffic analysis reports.

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Basic Configuration** → **Scheduled Report** .
2. Click + to enter the Create Report page, or click a report to enter the report's page.
3. Set the basic information, including the report name, analysis type, report format, and report language.
4. Select the contents to be included in the report.

   **Note**

   The report contents change according to the analysis type.
5. Complete the time settings.
   a. Select a statistical cycle.

      **By Day**

      The report shows data on a daily basis. The platform will send one report every day. The report contains data recorded on the day prior to the current day.

      For example, if you set the sending time to 20:00, the system will send a report at 20:00, containing data between 00:00 and 24:00 prior to the current day.

      **By Week**

      The platform will send one report every week. The report contains data of the recent one/two weeks.

      For example, for weekly report, if you set the sending time to 6:00 on Monday, the platform will send a report at 6:00 a.m. every Monday, containing data of the last week or recent two weeks based on your selection.

   b. Select the report time, which means the statistical range of the report.

      **Note**

      The options change according to the statistical cycle you select.

   c. Select a day and/or time of sending the report at the **Send At** / **Send On** field.
   d. Select an effective period for the settings.
6. Complete the advanced settings.
   a. Enable **Send Report via Email**, and then select an email template.

      **Note**

      You can click **Add** to add a new email template.

   b. Enable **Upload to SFTP** and/or **Save to Local Storage**.

      **Note**

      To set the SFTP or local storage, click → **SFTP Settings / Configure Local Storage** on the top left of the page.
7. Click **Add**/**Save**.

## 17.2 Manage Drivers

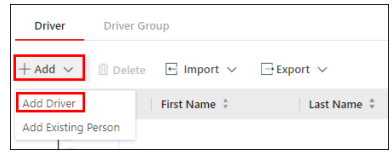
You can add driver information to the platform in multiple ways and add driver groups for further management. In addition, you can export information and profile photos of drivers from the platform.

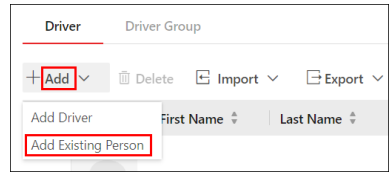
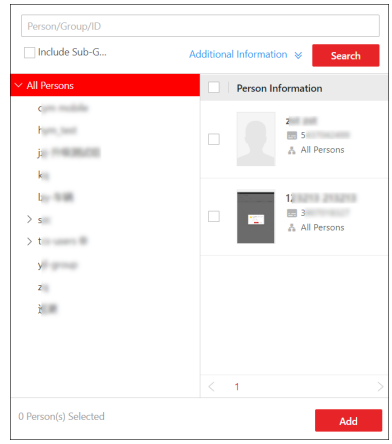
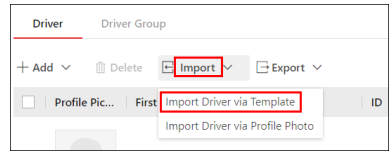
On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** .

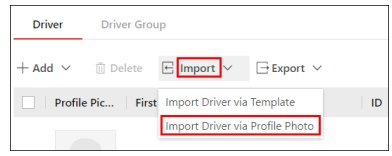
### 17.2.1 Add Drivers

Multiple methods are provided for adding drivers to the platform. You can add a single driver by entering his/her information or add drivers from existing persons. You can also batch add driver information by importing a template with driver information or importing ZIP files containing driver's profile photos.

1. Click **Driver** → **Add** .
2. Select one of the following ways to add drivers.

| Adding Methods | Description |
|---|---|
| Add a Single Driver | a. Click **Add Driver**.<br>  <br><br>**Figure 17-4 Add Driver**<br>b. Set the driver's basic information, such as the ID, driver group, first name, last name.<br>**Caution**<br>Once the driver is added, the ID cannot be edited any more.<br>c. Set the driver's driving license information, including the driving license No. and picture.<br>d. Click **Add**.<br>e. Click to filter drivers by name, ID, phone No., driver group or driving license No. |
| Add from Existing Persons | Make sure you have added persons to the platform.<br>a. Click **Add Existing Driver**. |

| Adding Methods | Description |
|---|---|
| |  <br>**Figure 17-5 Add Existing Driver**<br>b. Select one or multiple persons from the list and click **Add**.<br>  <br>**Figure 17-6 Add Existing Person Page**<br>c. Click to filter drivers by name, ID, phone No., driver group or driving license No. |
| Add Drivers via an Imported Template | a. Hover the mouse cursor over **Import** and click **Import Driver via Template**.<br>  <br>**Figure 17-7 Import Drivers via the Template**<br>b. In the pop-up window, click **Download Template** to save the template to the local PC.<br>c. In the downloaded template, enter the driver information by following the rules shown in the template.<br>d. Click and select the template with driver information from the local PC. |

| Adding Methods | Description |
|---|---|
| | e. Check **Auto Replace Duplicate Driver** to replace the existing driver information if the imported ID is the same as that of the existing driver.<br>f. Click **Import** to start importing driver information. |
| Add Drivers via Imported Profile Photos | a. Hover the mouse cursor over **Import** and click **Import Driver via Profile Photo**.<br>  <br>**Figure 17-8 Import Drivers via Profile Photos**<br>b. Click and select the ZIP files from the local PC.<br>c. Click **Import**. |

3. Export the driver information.
   a. Hover the mouse cursor over **Export** and click **Export Driver Information** or **Export Driver Profile Photo** as required.
   b. Set a password and confirm the password for decompressing the exported ZIP file.

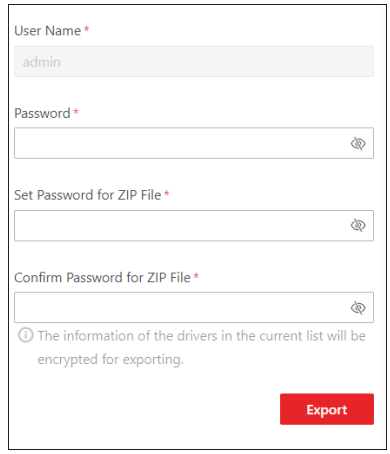


**Figure 17-9 Export Driver Profile Photos**

   c. Click **Export**.

**Note**

You can use the password you set previously to decompress the exported ZIP file.

### 17.2.2 Add Drivers to a Driver Group

1. Add a driver group.
   a. Click **Driver Group** → + and enter the driver group name.
   b. Click **OK**.
   c. Enter a key word in the search box, and click 🔍 to search for the target driver group.
2. Add drivers to the driver group for management.
   a. Select the added driver group in the left list, and click **OK**.
   b. Select drivers and click **Add**.

### 17.2.3 Link Driver/Driver Group to a Vehicle

When adding vehicles to an area, you can link added drivers or driver groups to a vehicle and check the face picture applying status.

1. Go to **Device** → **Area** and select an area.
2. Click **Vehicle** → + to set the vehicle information, including the license plate No., vehicle type, vehicle color, and more.

**Note**

You can set icons only for the following vehicle types: Default, Bus, Truck, and Sedan.

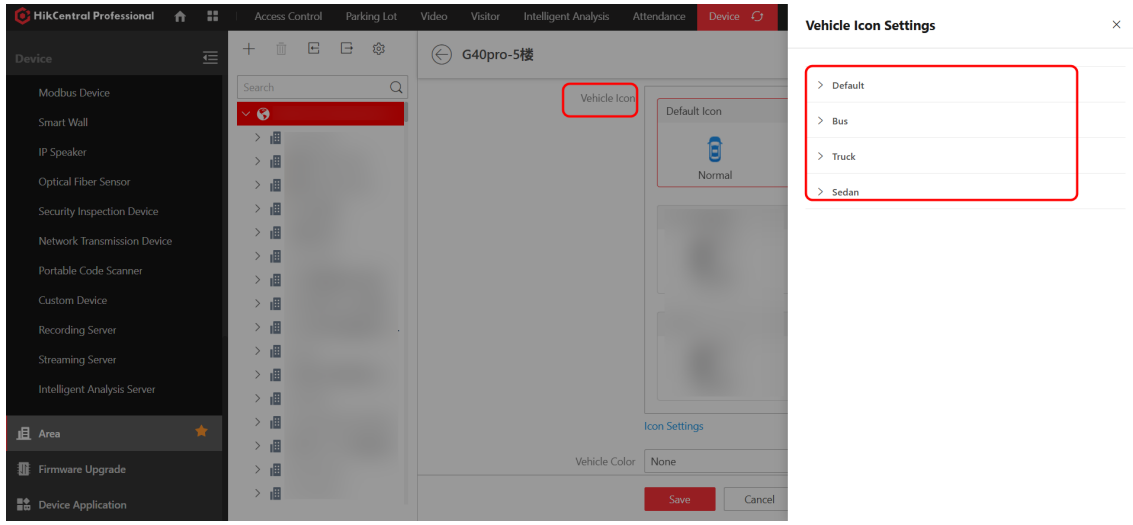



**Figure 17-10 Set Vehicle Icon**

3. After setting the license plate No., select a driver or driver group.

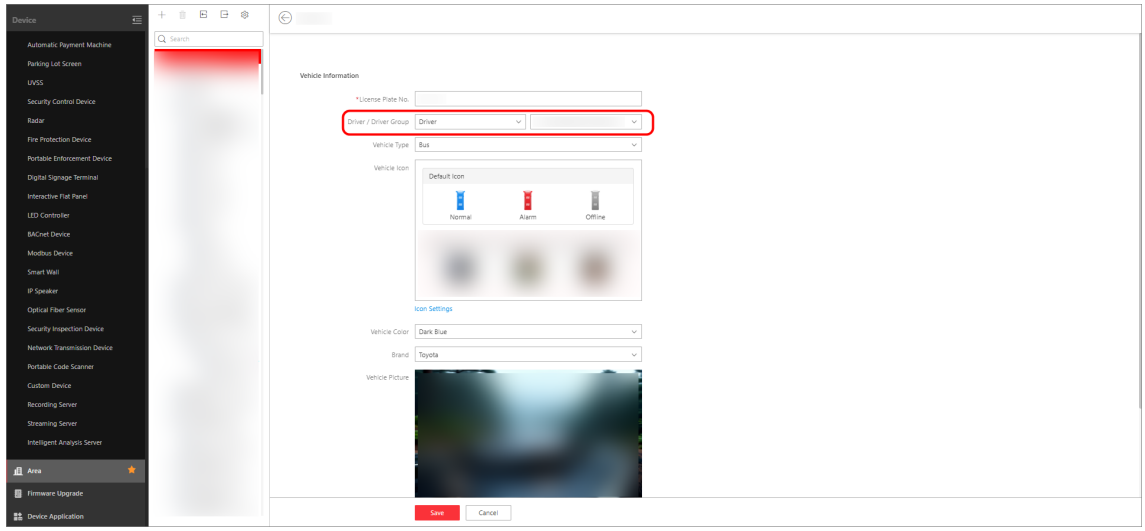



**Figure 17-11 Link Driver to Vehicle**

4. Click **Save**. You can go to Face Picture Application Center to check the face picture applying status.

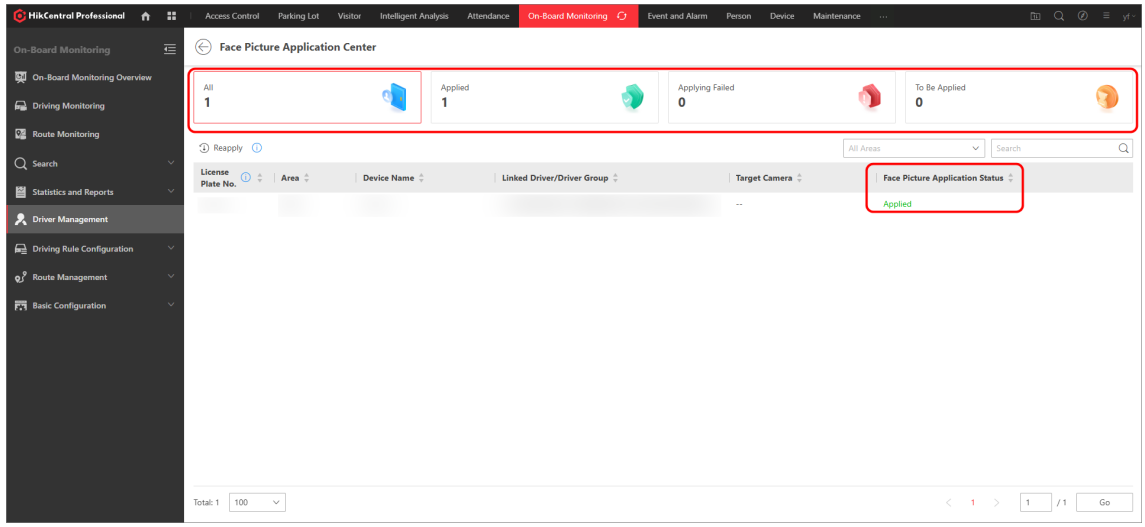



**Figure 17-12 Check Face Picture Applying Status**

**Note**

Licenses are required for network cameras connected to mobile DVRs/dash cams for facial recognition.

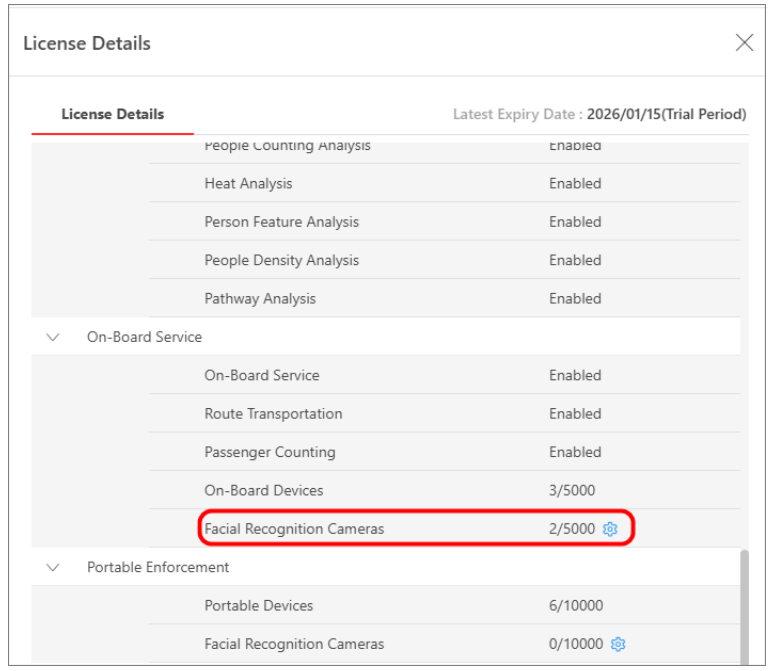



**Figure 17-13 Facial Recognition Camera License**

## 17.3 Configure Driving Rules

There are two types of driving rule: fence rule and deviation rule. A fence rule specifies the area where vehicles are allowed or not allowed to drive and a deviation rule specifies the route that vehicles should drive along. Besides, you can configure rule schedule templates to define when the rules should take effect. As a result, if a vehicle breaks an effective rule, an alarm will be triggered and uploaded to the platform.

Before adding driving rules, configure a GIS map first. Refer to ***Configure Basic Parameters*** .

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driving Rule Configuration** .

### 17.3.1 Configure Fence Rule

1. Click **Fence Rule** → **Add** .
2. Set the rule name and description.

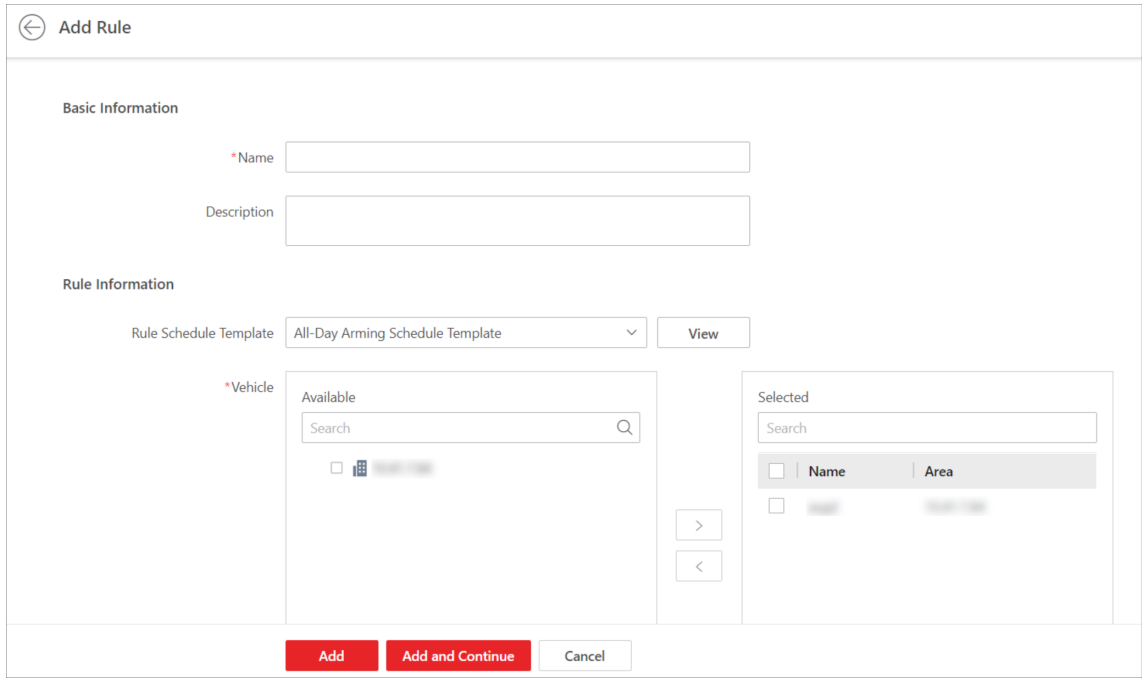



**Figure 17-14 Add a Fence Rule**

3. Set rule information.
   a. Select a rule schedule template.

   **Note**

   You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, refer to ***Configure Rule Schedule Template*** for how to configure one.

   b. Select vehicle(s) that the fence rule will be applied to.
   c. Set the fence type.

   **Fence for Entry Detection**

   An alarm and event will be triggered when a selected vehicle enters the fence area.

   **Fence for Exit Detection**

   An alarm and event will be triggered when a selected vehicle exits the fence area.
   d. Set **Threshold for Triggering Rule**.
   e. In the Fence Area, click to draw a fence area on the map.
4. Click **Add** to finish or click **Add and Continue** to add another fence rule.

## 17.3.2 Configure Deviation Rule

1. Click **Deviation Rule → Add** .
2. Set the rule name and description.

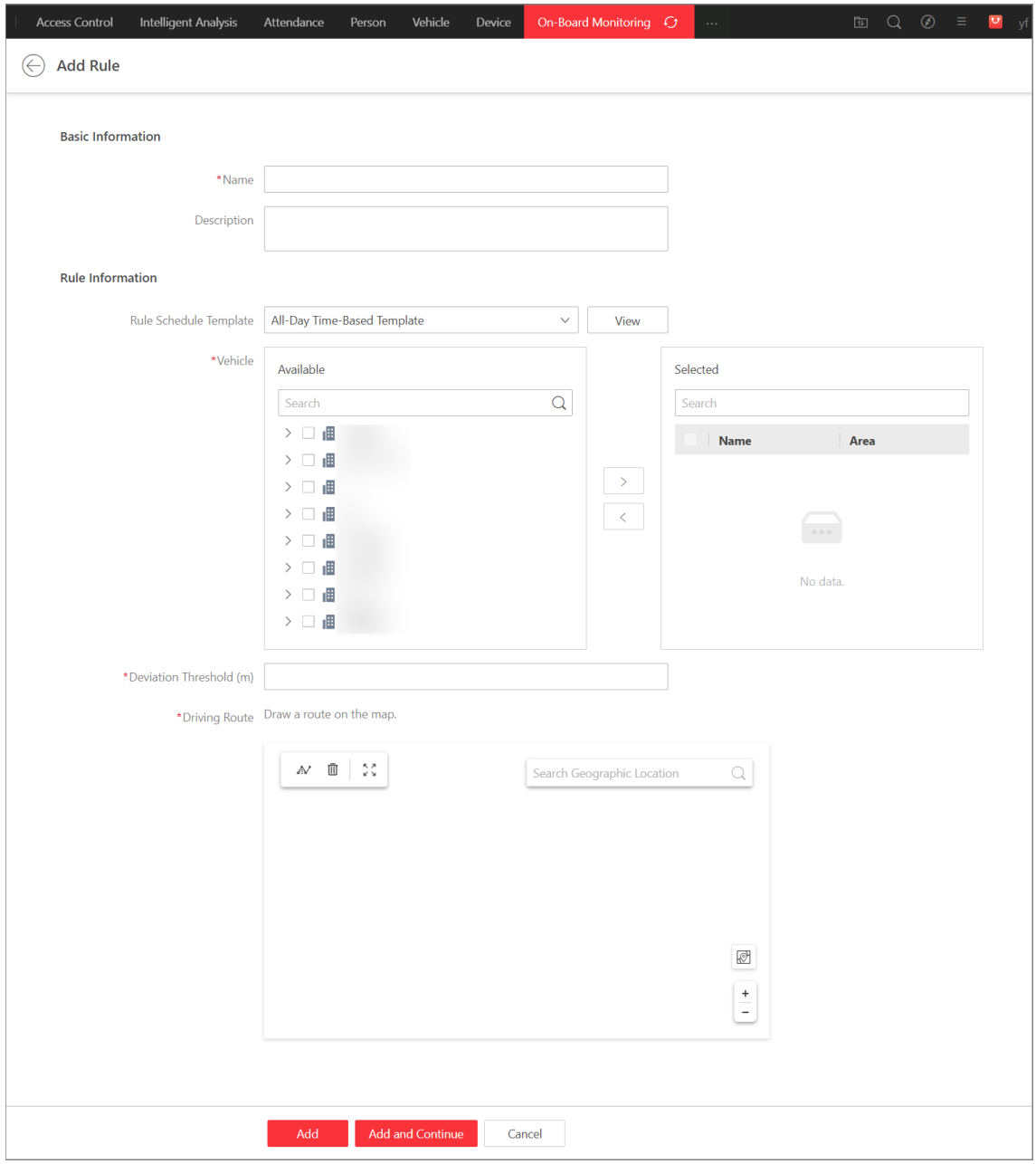



**Figure 17-15 Add a Deviation Rule**

3. Set rule information.
   a. Select a rule schedule template.

**Note**

You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, refer to ***Configure Rule Schedule Template*** for how to configure one.

b. Select vehicle(s) that the fence rule will be applied to.
c. Set the deviation threshold. An event will be triggered if a selected vehicle deviates from the route beyond the threshold.
d. In the Driving Route area, click to draw a route on the map.
e.

4. Click **Add** to finish or click **Add and Continue** to add another fence rule.

### 17.3.3 Configure Rule Schedule Template

1. Click **Rule Schedule Template** → + .

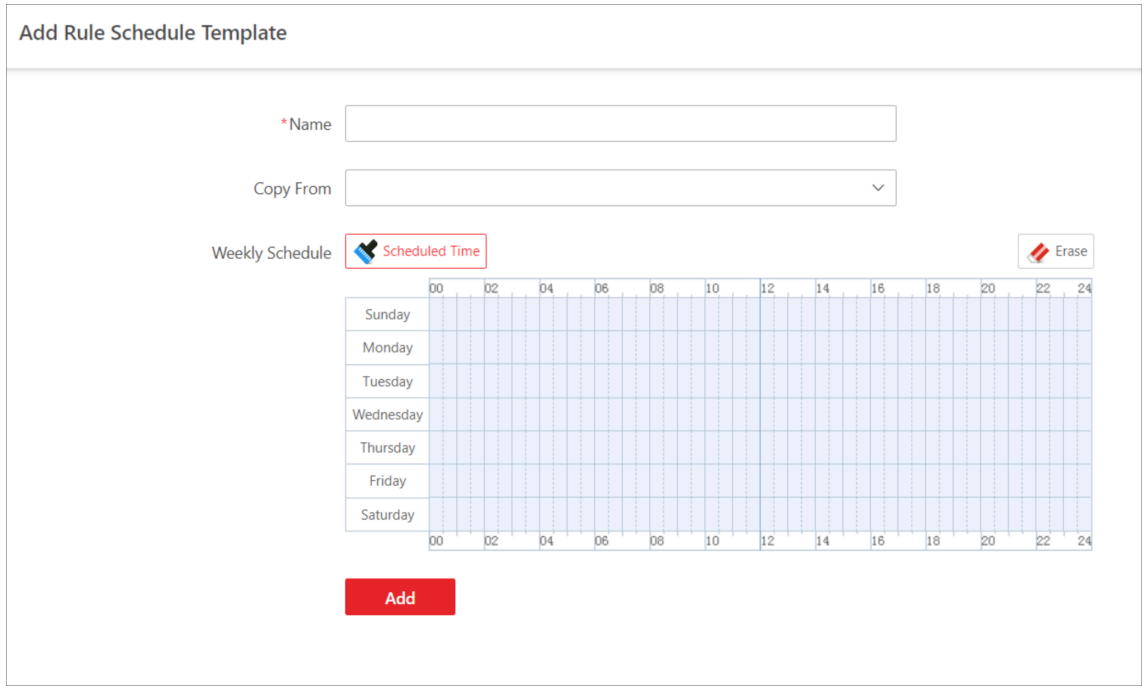



**Figure 17-16 Add Rule Schedule Template**

2. Create a name for the rule schedule template.
3. In the **Copy from** field, select an existing template to copy its weekly schedule to the current one.
4. Click **Scheduled Time** and click or drag on the timetable to define the period.
5. Click **Add**.

## 17.4 Manage Stop & Route

You can add stop groups to the platform and add stops to the groups in multiple ways for further management. Then you can select stops for a driving route and configure shift schedules. Also, you can configure event rules for specified stops.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** .

### 17.4.1 Step 1: Add Stops

You can add driving stop groups to the platform. After that, you can add a single stop to the groups for further management. Also, you can import multiple stops in a batch to the added groups via a predefined template.

### Add a Stop

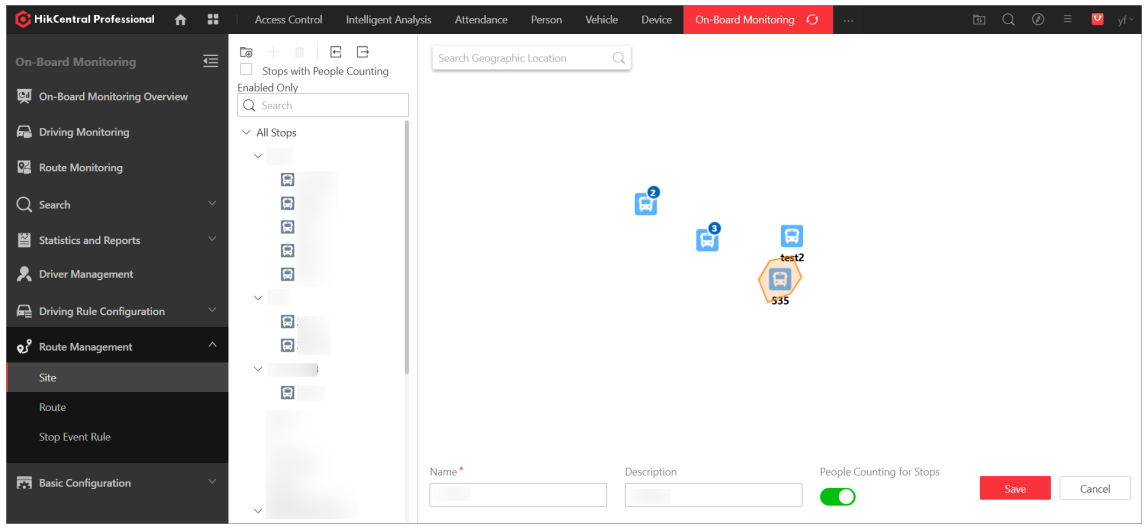



**Figure 17-17 Add Stops**

1. Click in the top left corner, enter the stop group name, and click **Add** to add a stop group.
2. Select a stop group in the stop group list, and click + .
3. Move your mouse cursor to the target location on the map and click .
4. Select **Circle** or **Polygon** as the stop shape, move your mouse cursor to adjust the size, and click to confirm.
5. Enter a name and description for the stop and switch on/off **People Counting for Stops**.
6. Click **Save**.

### Batch Add Stops by Importing a Template

1. Click , and click **Download Template** and save the predefined template (EXCEL file) in your PC.
2. Open the downloaded template file and edit the required information of the stops to be added in the corresponding column.
3. Click and select the template file, and then click **Import**.

## 17.4.2 Step 2: Configure Driving Routes

1. Click **Route**, click **Add Route** (if no route exists) or + (if routes exist), enter a name for the route, and click **Add**.

**Note**

If there are routes added before, hover the cursor over a route on the route list page and click to create a copy and edit it as needed.

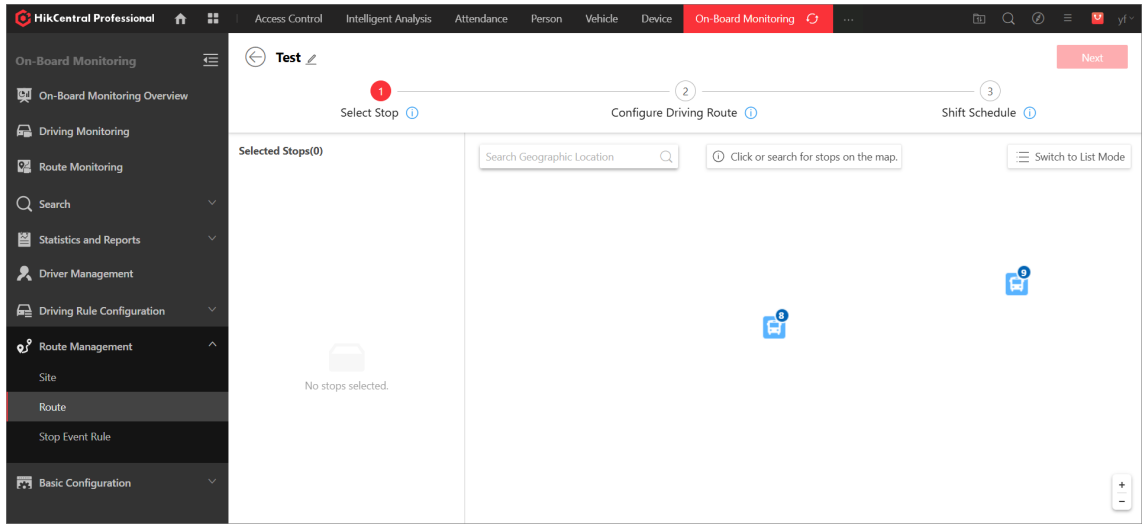



**Figure 17-18 Select Stops**

2. Select at least two stops on the map. You can select stops in one of the following ways:
   - Click **Switch to List Mode** and select stops in the list.
   - Click the stop icon on the map to select the stop.

**Note**

You can click **Reverse** to reverse the order of the selected stops.

3. In the top right corner of the page, click **Next** and configure the driving route. You can configure in one of the following ways:

- Adjust the driving route manually: Hover the cursor over the line between two stops and drag to adjust the driving route manually.
- Generate the driving route automatically: Click **Auto Generate Route** to generate the route automatically.

**Caution**

To generate the driving route automatically, you need to enable the Google map charging service.

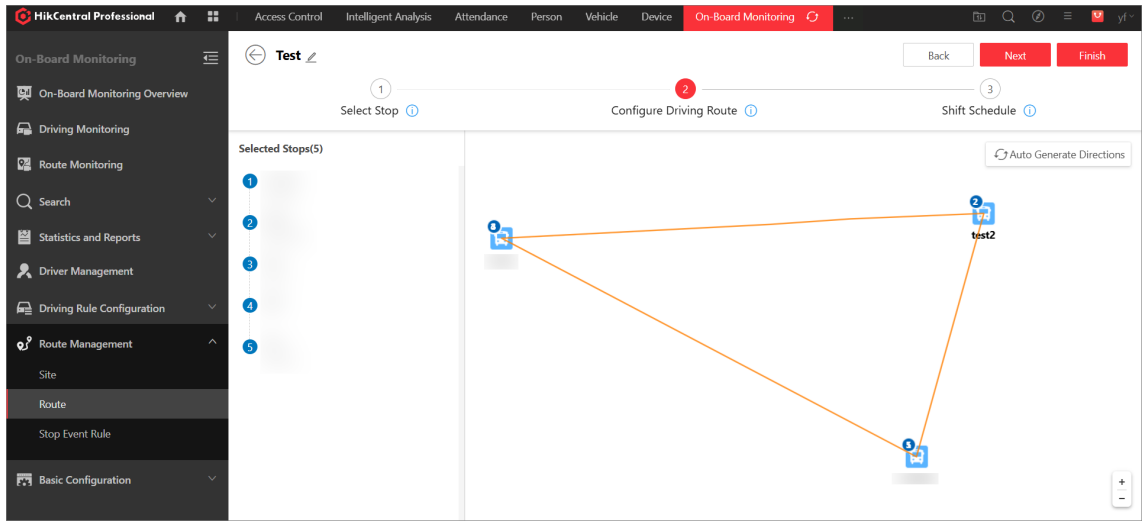



**Figure 17-19 Configure Driving Route**

## 17.4.3 (Optional) Step 3: Configure Shift Schedules

1. Click **Next**, and click **Add Schedule** or **Batch Add Schedules**.
2. Set the schedule information.

| Add a Single Schedule | Batch Add Schedules |
|---|---|

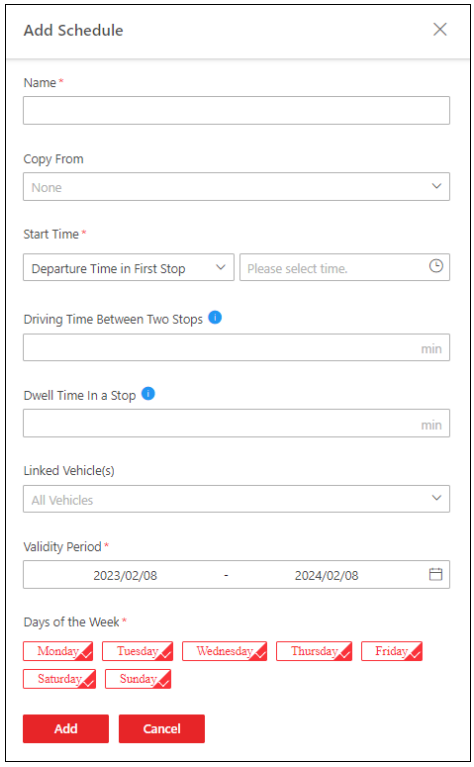



**Figure 17-20 Add a Single Schedule**

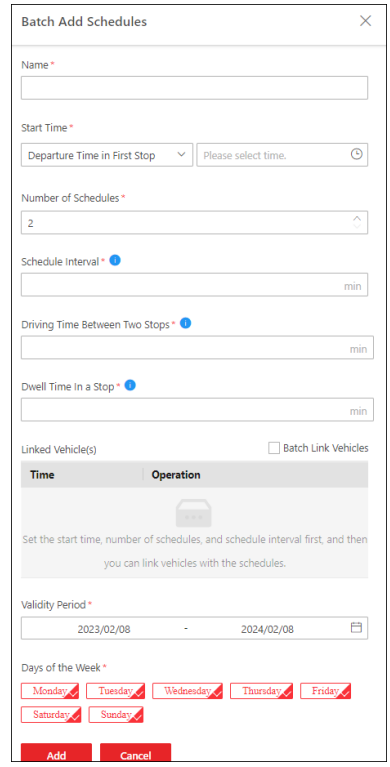



**Figure 17-21 Batch Add Schedules**

3. Click **Add**.

**Note**

You can set route parameters to define late arrivals/departures for the schedules. For details, refer to ***Configure Route Parameters*** .

4. You can click ⊘ / ⊖ to enable/disable the route.

## 17.4.4 (Optional) Step 4: Add a Stop Event Rule

You can configure event rules for specified stops. After configurations, alarm inputs triggered outside/within the selected stops will be recorded as unintended alarm inputs.

1. Click **Stop Event Rule → Add** to add a stop event rule.
2. Set the basic rule information such as rule name.
3. Select the rule type.
4. Select the alarm input and stops.
5. Click **Add** to finish or click **Add and Continue** to add another rule.

## 17.5 Driving Monitoring

On the Driving Monitoring page, you can monitor driving vehicles to get their real-time information such as locations, speeds, and events. You can also play the live videos streamed from vehicle-mounted cameras, talk to drivers via two-way audio, track vehicles in real time, play back the tracks vehicles have traveled along, and add vehicles to the Favorites list for quick and easy management.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driving Monitoring** .

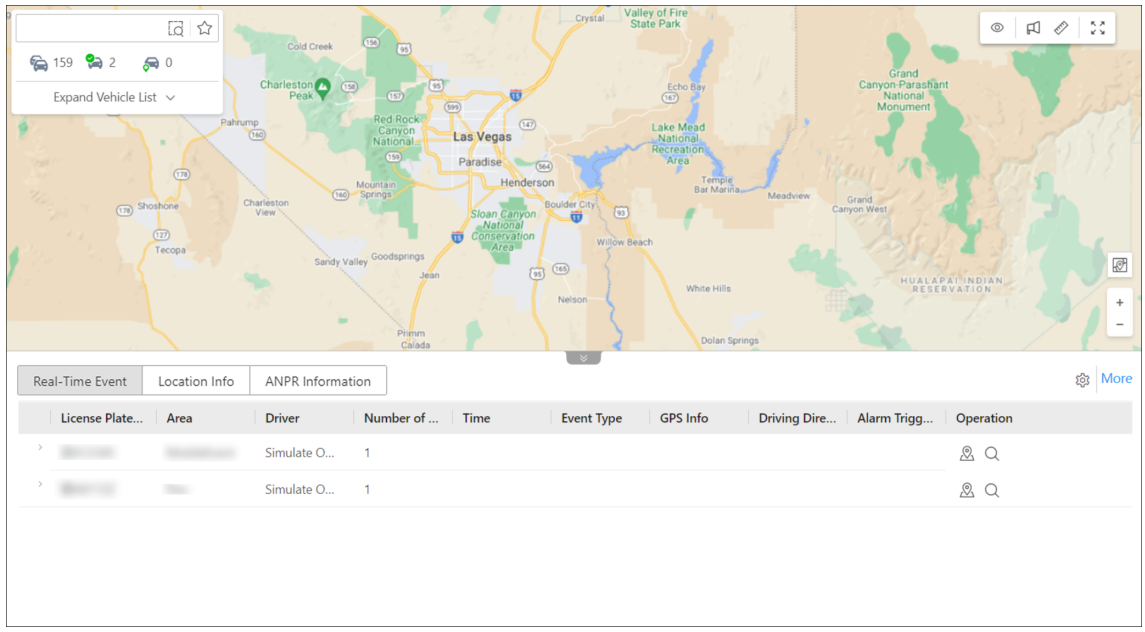



**Figure 17-22 Driving Monitoring Page**

### Vehicle List Pane

Perform the following operations as needed:

| Operation | Step |
|---|---|
| Search for / Filter Vehicles | • Enter keywords in the search box to search for target vehicles.<br>• Click to specify an area for vehicle search.<br>• Click / / to view all/online/located vehicles.<br>• Click to view vehicles in the Favorites list. |
| Locate / Broadcast to Vehicles | Click , click on the map to select a center and move the mouse to draw a circle based on the selected center, and then click on the map again to finish drawing. Hover over the drawn circle and |

| Operation | Step |
|---|---|
| | click **Locate** or **Broadcast** to locate or broadcast to all vehicles in the circle. |
| View Vehicle Details | On the vehicle list, hover over a vehicle to view its real-time information, including its location, speed, etc. |
| Locate Vehicle | On the vehicle list, hover over a vehicle and click to locate the vehicle on the map and click again to cancel locating it. |
| Play Back Track | On the vehicle list, hover over a vehicle and click to play back the track the vehicle has traveled along. |
| Start Live View | Expand the camera list of a specific vehicle, and double-click to view the live videos streamed from the vehicle-mounted cameras. |
| Other | On the vehicle list, hover over a vehicle and click ··· to display the operation menu. You can choose to play video, talk to a driver via two-way audio, track a vehicle in real time, play back the track the vehicle has traveled along, control alarm outputs, and add/remove a vehicle to/from the Favorites list. |

**Note**

You should wake up sleeping dash cameras (G40 Pro) to ensure continuous remote access for live view and playback. When ACC is turned off, the dash camera will enter sleep mode after the configured shutdown delay time.

## Driving Monitoring on the Map

On the GIS map, you can view the number of unacknowledged alarms on the vehicles. You can click the icon of a located vehicle on the map to open the driving monitoring pane. On the pane, you can view the vehicle's real-time information including its location, speed, etc, and can perform the following operations:

**Note**

For an event that has been subscribed and configured with alarm trigger, only one record will be displayed and will be marked as an alarm.

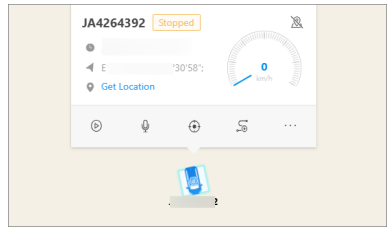



**Figure 17-23 Driving Monitoring Pane**

| Operation | Step |
|---|---|
| Cancel Locating Vehicle | Click to cancel locating the vehicle. |
| Get Vehicle's Location | Click **Get Location** to get the vehicle's real-time location. |
| Play / Play Back Video | Click **Play** to play live or recorded videos streamed from vehicle-mounted cameras. |
| Talk to Driver | Click **Two-Way Audio** to talk to the driver. |
| Track Vehicle | Click **Real-Time Tracking** to track the vehicle in real time. You can click **Stop** in the upper-left corner of the vehicle-tracking page to stop tracking. |
| Play Back Track | Click **Track Playback** and select a period and camera to play back the track recorded by the camera in the specified period. |
| Control Alarm Output | Click **More → Alarm Output** and then click / in the Operation column to enable/disable the alarm output related to the vehicle. |
| Send Text | Click **More → Send Text** to send a text to the vehicle, and the text will be converted to audio. |
| View History Alarms | Click **More → View History Alarms** to view the vehicle's history alarms. |
| View Alarm Details | The number of triggered alarms is marked on the icon of the vehicle on the map. You can click the number to view alarm details. You can also view the videos streamed from the vehicle-mounted cameras. |
| Wake up Sleeping Dash Cam | You should click to wake up sleeping dash cameras (G40 Pro) to ensure continuous remote access for live view and playback. |

## Real-Time Event

The Real-Time Event table presents real-time events triggered by monitored online vehicles. Each record is attached with detailed information such as the license plate number, driver, event type, and GPS information. You can perform the following operations:

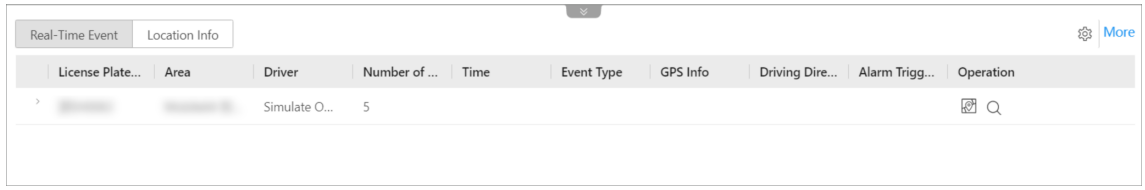



**Figure 17-24 Real-Time Event Table**

| Operation | Step |
|---|---|
| Locate Vehicle | Click in the Operation column to locate a vehicle. |
| Center Vehicle | Click in the Operation column to place a located vehicle in the center of the map. |
| Search for Track | Click in the Operation column to go to search for the track a vehicle has traveled along. |
| Save As Evidence | Click in the Operation column to save the event as the evidence. |
| Select Event Type | Click to open the Settings pane and select the types of event to be reported to the platform. |
| Search for Driving Event | Click **More** to go the Driving Event Search page to search for driving events triggered in the past. |

## Location Info

The Location Info table presents the real-time locations of located vehicles. Each record is attached with detailed information such as the license plate number, GPS info, and driving direction. Besides, you can perform the following operations:

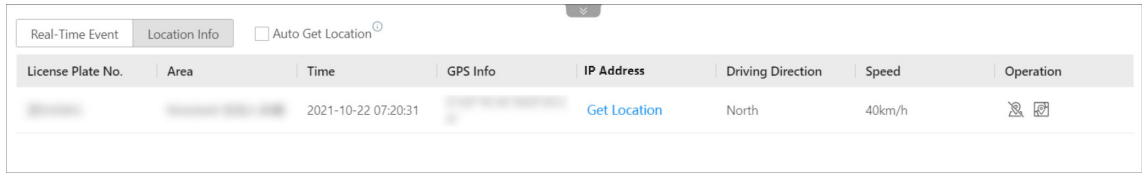



**Figure 17-25 Location Info Table**

| Operation | Step |
|---|---|
| Get Vehicle's Location | Click **Get Location** in the IP Address column to get the real-time location of a vehicle. |
| Auto Refresh Location | Check **Auto Get Location** to automatically refresh locations frequently. |

| Operation | Step |
|---|---|
| Cancel Locating Vehicle | Click in the Operation column to cancel locating a vehicle. |
| Center Vehicle | Click in the Operation column to place a vehicle in the center of the map. |

### ANPR Information

The ANPR Information table presents the vehicle passing records. Each record is attached with detailed information such as the license plate number, GPS info, and driving direction.
Click **More** to jump to **Passing Vehicle Search** in the ANPR module; you can also click the different buttons in the operation column of each record to jump to **Passing Vehicle Search** with different conditions.

### Map Management

You can perform the following operations on the map:

| Operation | Step |
|---|---|
| Display Driving Rule | Click and select **Fence Rule** or/and **Deviation Rule** to display the areas where vehicles are allowed or not allowed to drive and the routes that vehicles should drive along. |
| Broadcast to Vehicle | Click and select vehicle(s) to broadcast to them. |
| Measure Distance | Click and specify the start point and end point on the map to measure the actual distance between them. |
| Full-Screen Display | Click to display the map in full-screen mode. |

## 17.6 Route Monitoring

On the route monitoring page, you can monitor the vehicles' driving routes to get stop information, route status, unpunctual causes, and vehicles' driving status. You can also view the detailed information of vehicles in the routes, such as locations, speeds, and events.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Monitoring** .

## Route List

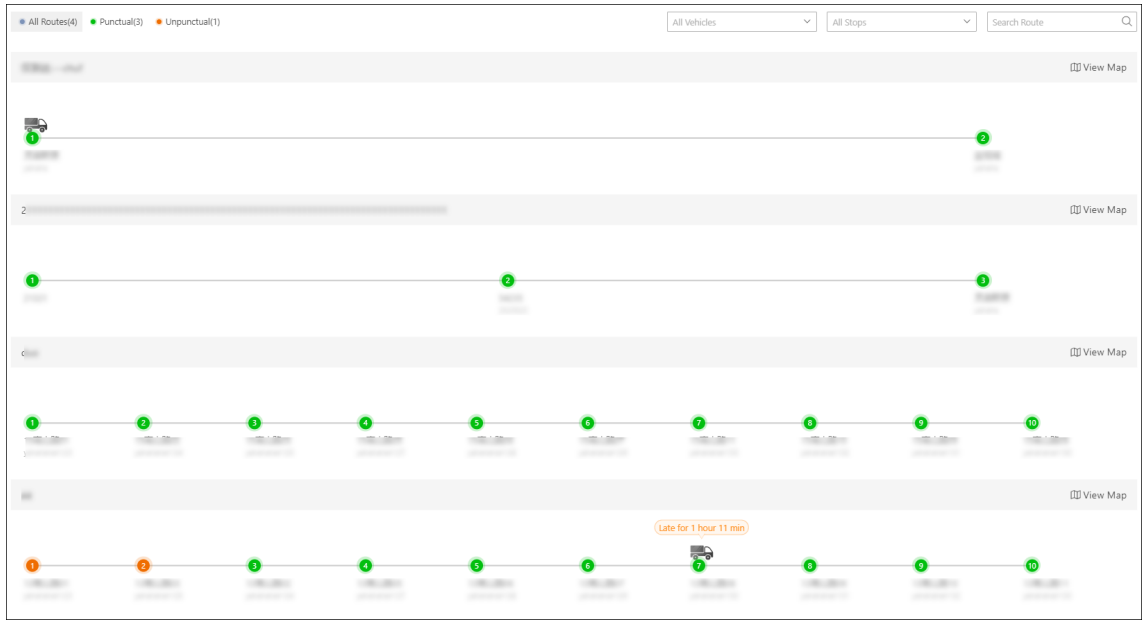



**Figure 17-26 Route List**

Perform the following operations as needed:

| Operation | Description |
|---|---|
| Filter / Search for Routes | • In the top left corner of the page, click **All Routes** / **Punctual** / **Unpunctual** to view corresponding routes.<br>• In the top right corner, select vehicles and/or stops from the drop-down list and/or enter keywords in the search box to quickly find target routes. |
| View Route Details | • You can view the total number of stops, the stop names, the status (punctual/early/late) and the current location of vehicles in each route.<br>• Hover the mouse cursor over a stop to view its details, including punctual rate, vehicle, scheduled arrival time, actual arrival time, scheduled departure time, and actual departure time. |
| Add Cause of Unpunctual Departure/Arrival | Hover the mouse cursor over a stop, click in the Operation column to add notes for unpunctual departures/arrivals. |

## Single Route Monitoring

Click **View Map** to view the details of a single route.

**Note**

The two panes on the left and at the bottom of the page can be displayed or hidden by clicking the arrows.

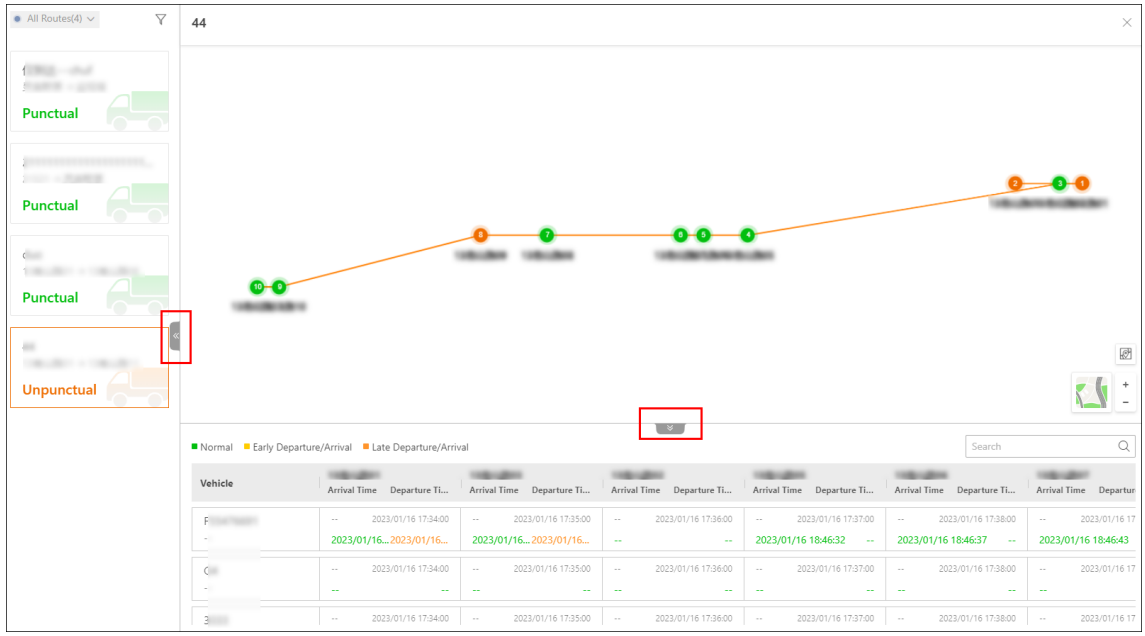



**Figure 17-27 Single Route Monitoring**

Perform the following operations as needed:

| Operation | Description |
|---|---|
| View Route Details | • You can view the stops and vehicles in the selected route on the GIS map.<br>• You can view the scheduled departure/arrival time and actual departure/arrival time in the table at the bottom, with different colors for different status (normal, early departure/arrival, and late departure/arrival). |
| Add Cause of Unpunctual Departure/Arrival | Hover the mouse cursor over the actual departure/arrival time in the timetable and click **Add Remarks** to add notes for unpunctual departures/arrivals. |
| Monitor Vehicles in the Route | Click the icon of a vehicle on the map to open its driving monitoring pane. For details about driving monitoring, see ***Driving Monitoring*** . |

| Operation | Description |
|---|---|
| View Alarm Details | The number of triggered alarms is marked on the icon of the vehicle on the map. You can click the number to view alarm details. |
| Filter / Search for Routes | • In the top left corner, you can filter routes by route status (all/punctual/unpunctual).<br>• Click to select vehicles and/or stops from the drop-down list and/or enter keywords in the search box to quickly find target routes. |
| Switch to Another Route | You can select another route on the left pane to view its details. |

## 17.7 Search On-Board Monitoring Records

On-board monitoring records include the tracks vehicles have traveled along, the events triggered by them in a specified period, the routes related to specific vehicles / vehicle groups, and fuel level monitoring records. You can search for records, view the details of each record, and export records to your PC for further use.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** .

### 17.7.1 Search for Vehicle Tracks

You can search for the tracks that vehicles have traveled along in the specified period, view detailed information of each record, play back tracks, and export records to the PC.

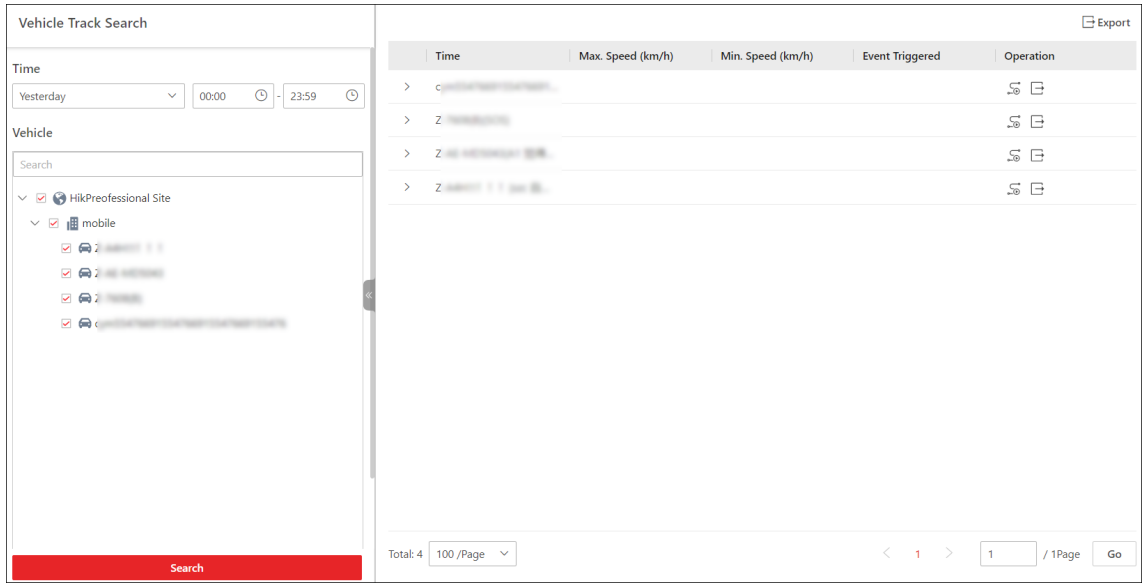



**Figure 17-28 Vehicle Track Search**

1. Click **Vehicle Track Search**.
2. Set search conditions by specifying the search period and selecting vehicles.
3. Switch on **Speed Range** and set a speed range.
4. Switch on **Triggering Condition** and click to select the event type.
5. Click **Search**.
6. Perform the following operations.

| Operation | Description |
|---|---|
| Play Back Track | Click to play back a track. |
| Export Record | Click to export a single record to the PC.<br>Click **Export** in the upper-right corner to export all records to the PC. |

## 17.7.2 Search for Driving Events

You can search for the events triggered by vehicles, drivers, or driver groups, view detailed information of each record, and export records to the PC.

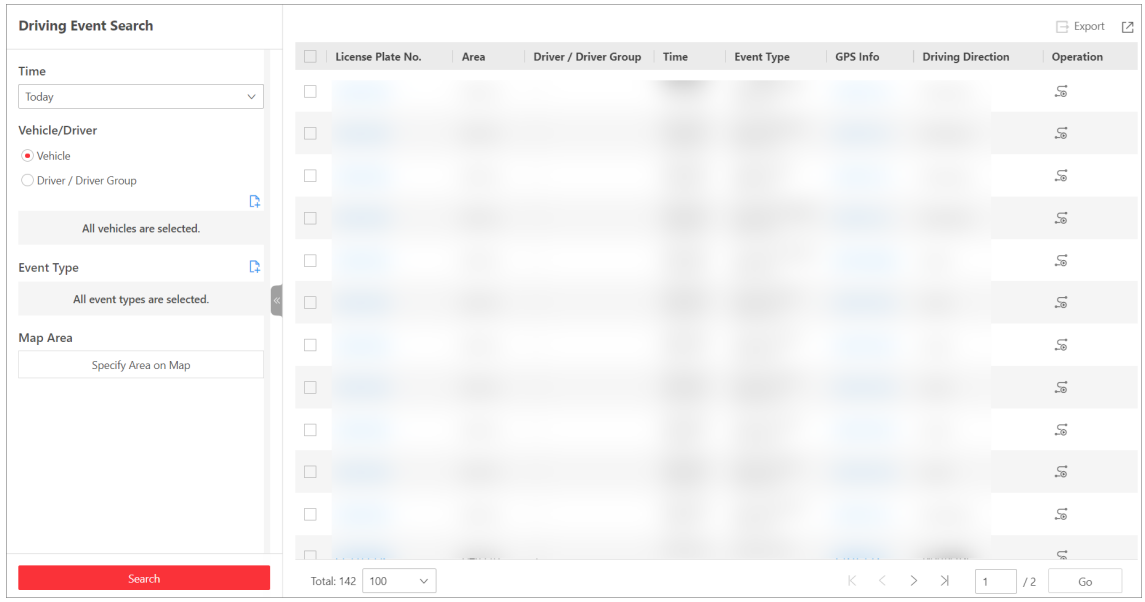



**Figure 17-29 Search Driving Events**

1. Click **Driving Event Search**.
2. Set the following search conditions: the search period, vehicle/driver, event type, and area.
3. Click **Search**.
4. Perform the following operations.

| Operation | Description |
|---|---|
| Play Back Track | Click to play back a track. |
| Export Record | Click to export a single record to the PC.<br>Click **Export** in the upper-right corner to export all records to the PC. |

## 17.7.3 Search for Routes

You can search for routes, view detailed information of each route, and export route information to the local PC.

1. Click **Route Search**.
2. Set the following search conditions: the search time, route, stop, and vehicle/driver.

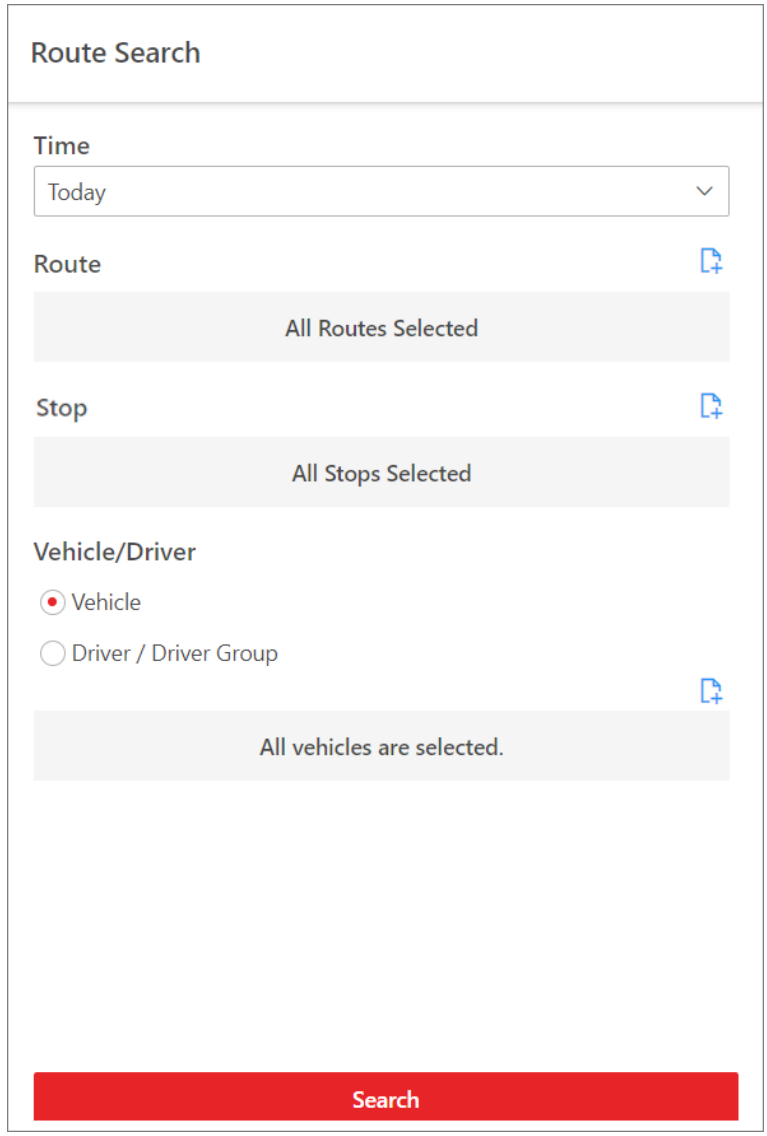



**Figure 17-30 Search Conditions**

3. Click **Search**.

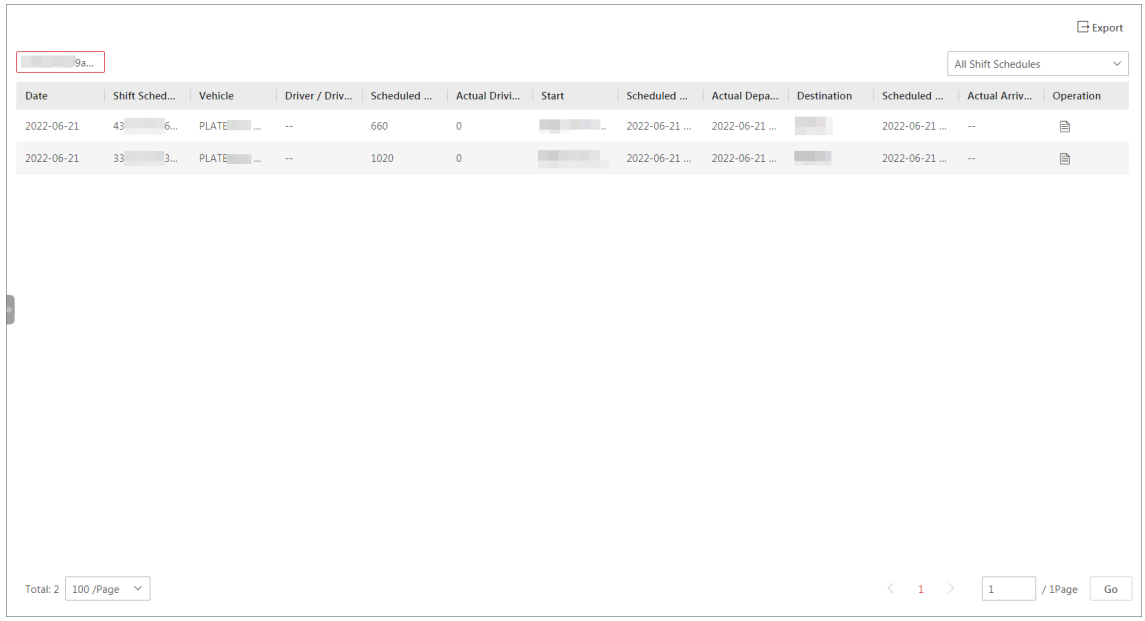



**Figure 17-31 Search for Routes**

### 17.7.4 Search for Fuel Level Monitoring Records

You can search for records of fuel level in the specified period and view details of the license plate No., area, driver's name, fuel tank model, fuel quantity, fuel level in tank (%), GPS info, and fuel filling or not.

1. Click **Fuel Level Record Search**.
2. Set the following search conditions: the search time and vehicle/driver.
3. Click **Search**.

**Note**

You can click **Export** in the upper-right corner to export the records to your local PC.

## 17.8 Statistics and Reports

HikCentral Professional provides multiple types of reports for you to get insight into the variation trend of the driving data, driving behaviors, number of passengers, and device online rate related to the vehicles in your company/organization. These reports, which can be exported to your local PC, demonstrate data in a visualized way through charts and (or) tables, helping you make better business decisions, operation strategies, device maintenance plans, etc.

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** . The report export tasks can be managed in **Download Center**.
2. Select a report.

3. Set the search conditions such as the search time, vehicle, report type, and statistics type.
4. Click **Generate Report**。
5. Perform the following operations as needed.

## Driver Analytics Report

You can create a driver analytics report showing the driver analytics information of specific drivers in a certain period, including the basic information of driver, driving distance, driving duration, events per 100 km, number of events, total fuel consumption, etc.

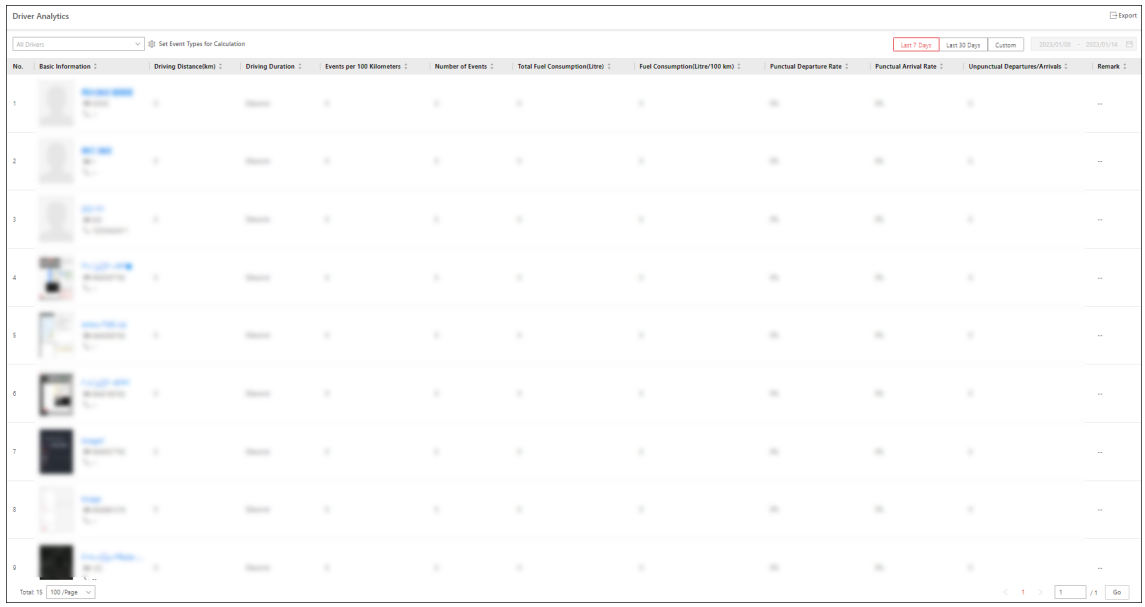



**Figure 17-32 Generate a Driver Analytics Report**

## GPS Information Report

You can create a GPS information report showing the GPS information of specific vehicles in a certain period, including the number of locations detected by GPS, license plate number, area, time, GPS, driving direction, and driving speed.

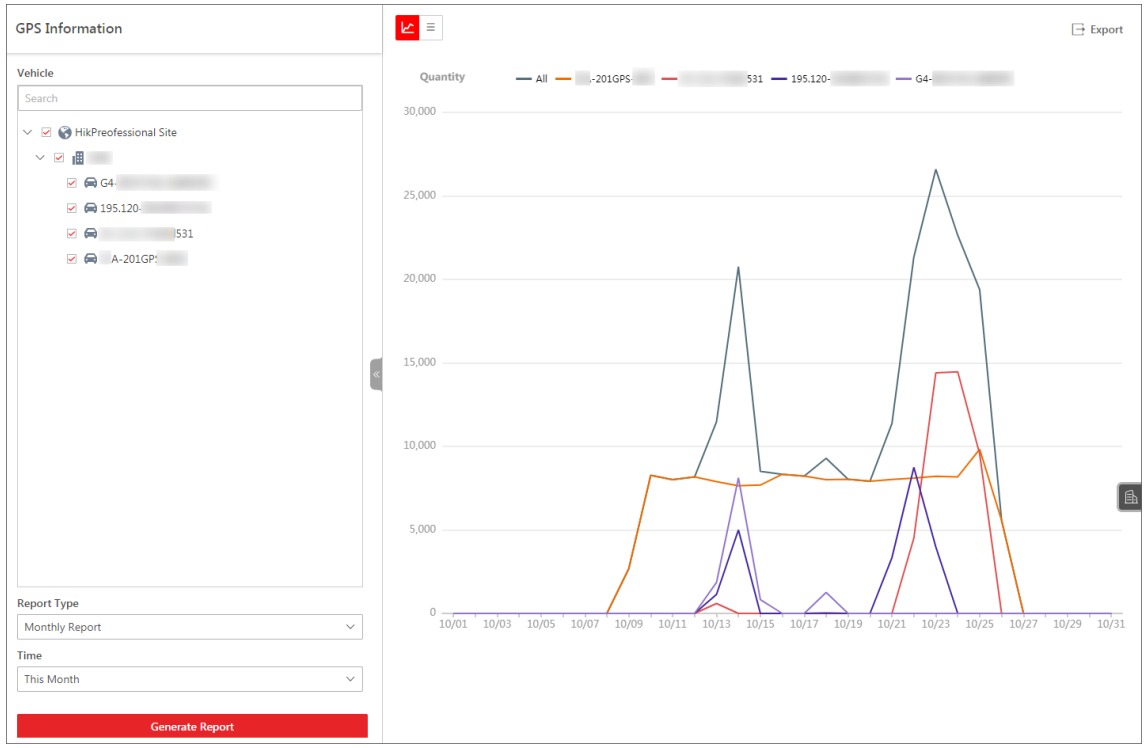



**Figure 17-33 View Data in Line Chart**

## Driving Distance Report

You can create a driving distance report to view the driving distance of specific vehicles or drivers in a certain period.

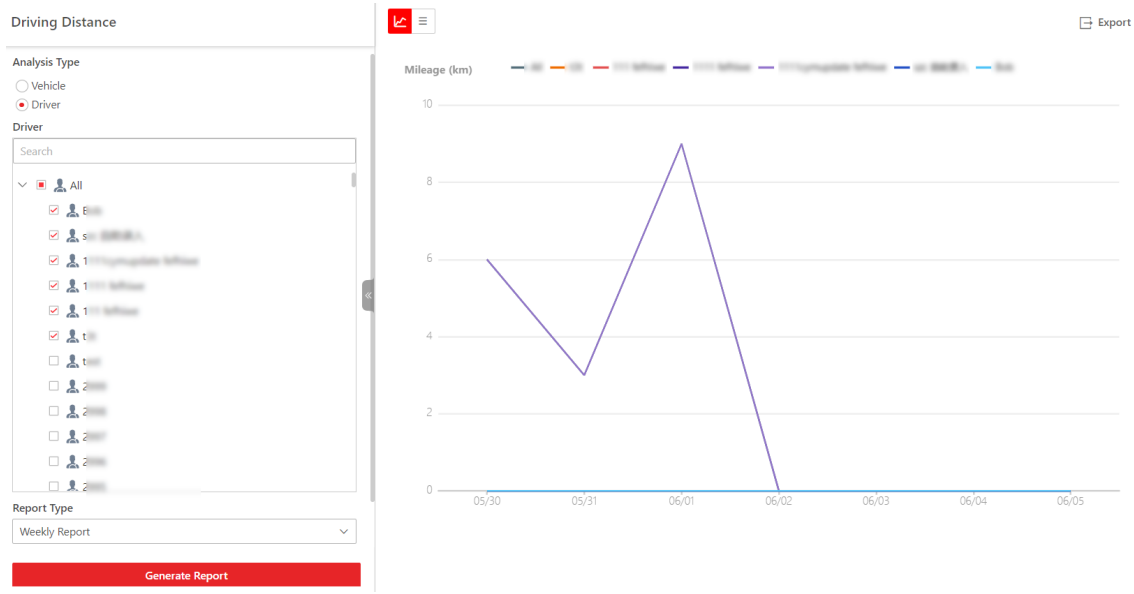



**Figure 17-34 Generate Report**

## Driving Duration Report

You can create a driving duration report to view the driving duration of specific vehicles or drivers at a certain speed in a certain period.

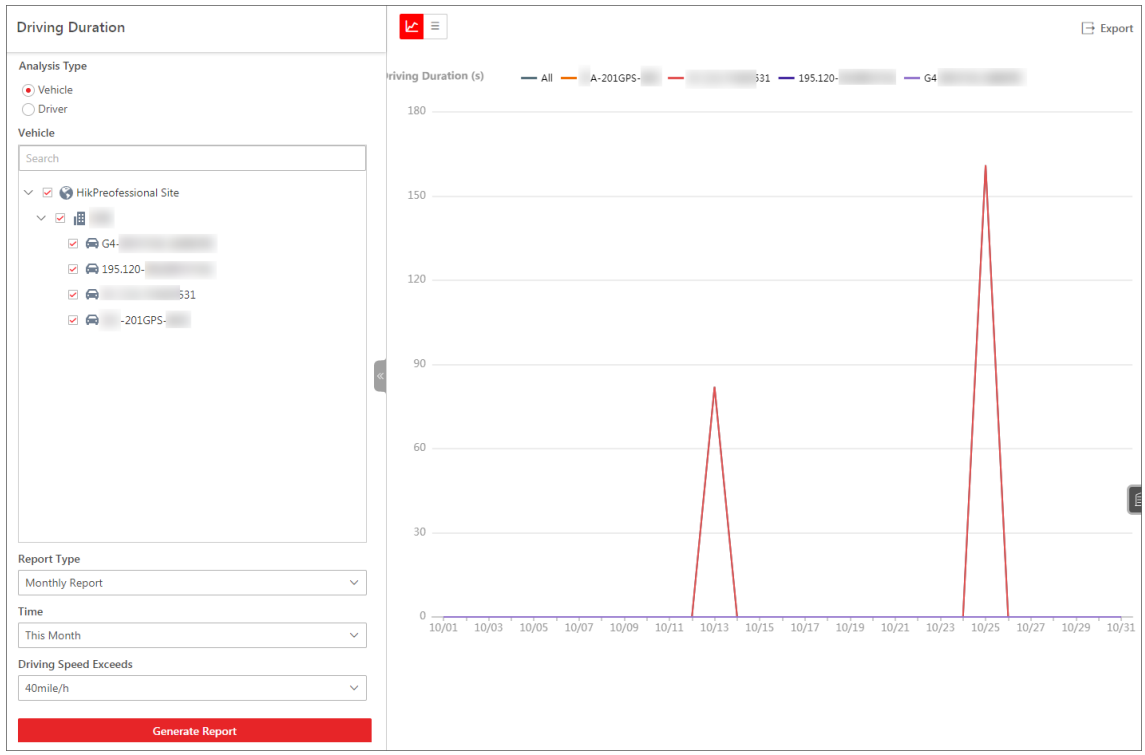



**Figure 17-35 Monthly Report Example**

## Speeding Report

You can create a speeding report to view the vehicles' speeding records in a specific period.

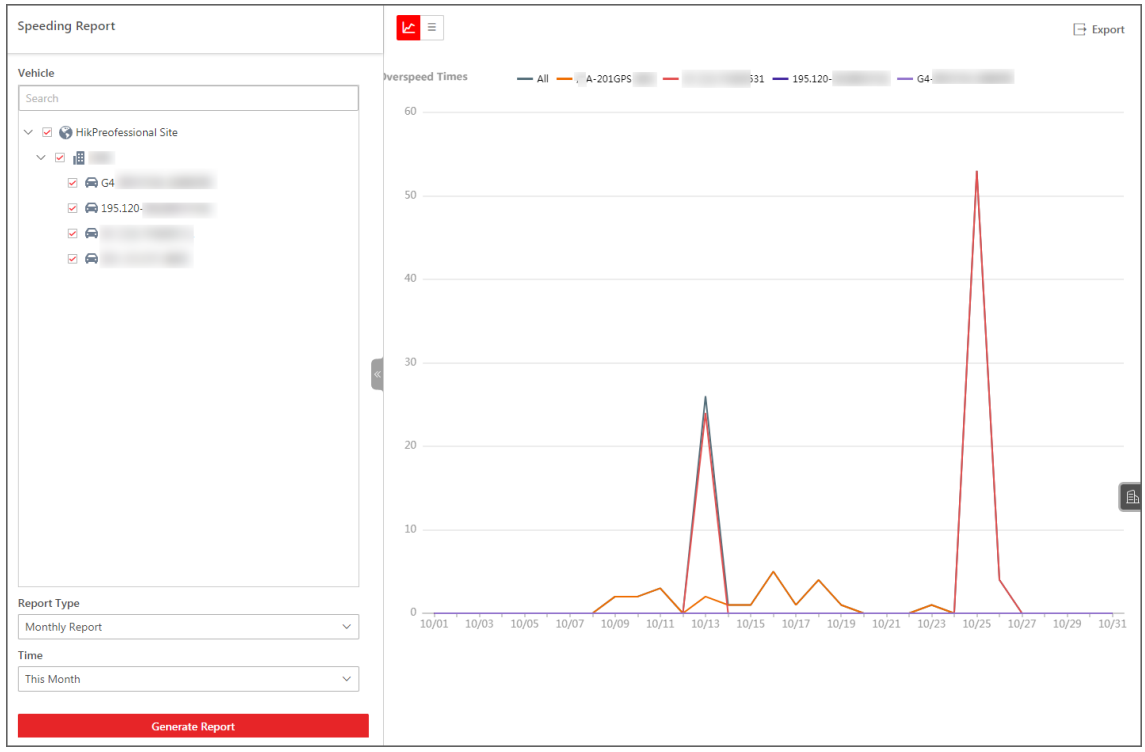



**Figure 17-36 View Data in Line Chart**

## Stop Analytics Report

You can create a stop analytics report showing the overall statistics of the selected stops in a certain period, including the average punctual departure rate, average punctual arrival rate, average dwell time (in minutes), total unpunctual arrivals, and total unpunctual departures. When enough results are generated, the report also shows the top 10 / bottom 10 stop rankings for punctual departure rate, punctual arrival rate, and dwell time.

## Driving Event Report

You can create a driving event report to view the times of event detection related to specific vehicles in a specific period.

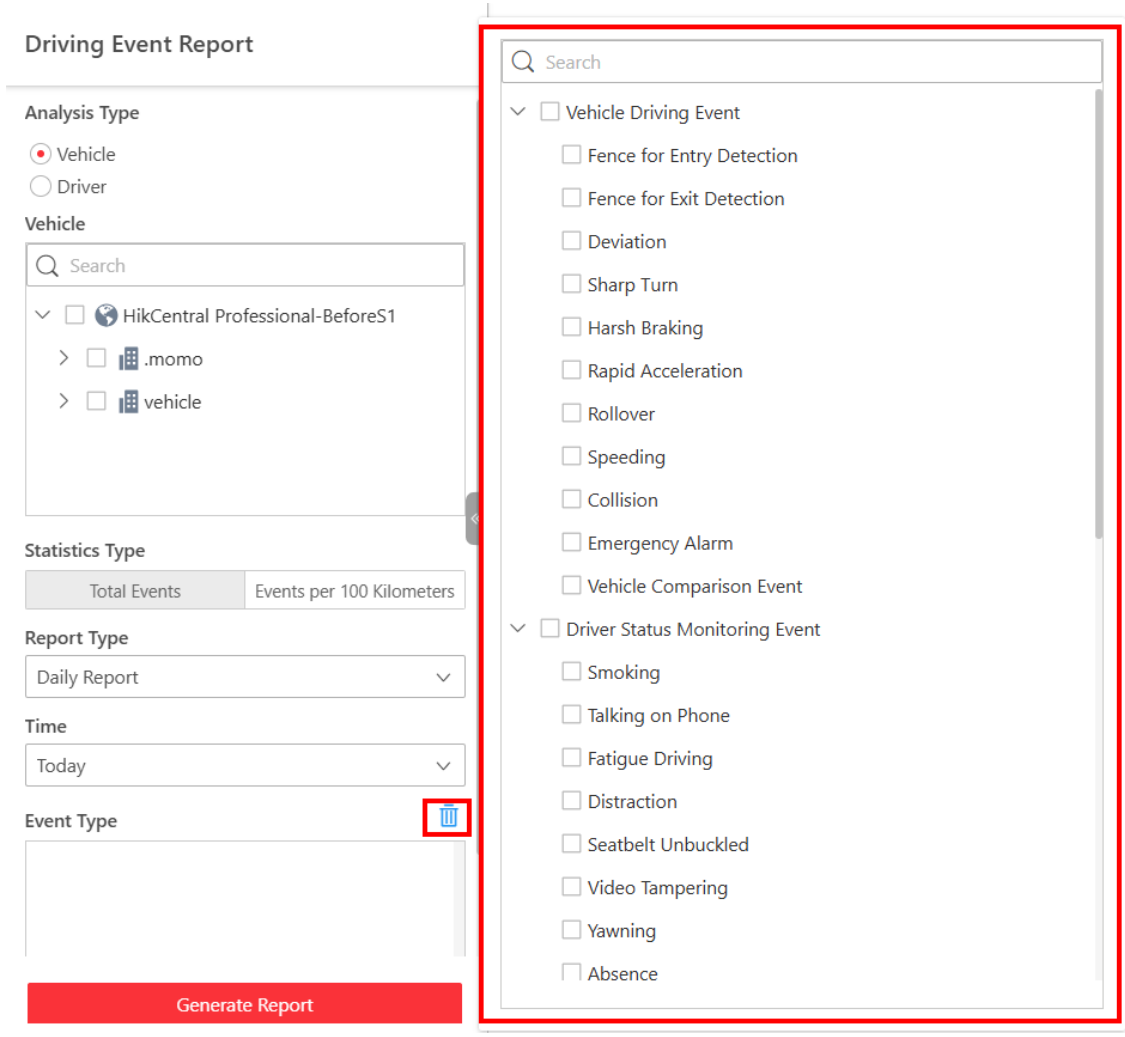



**Figure 17-37 Select Events**

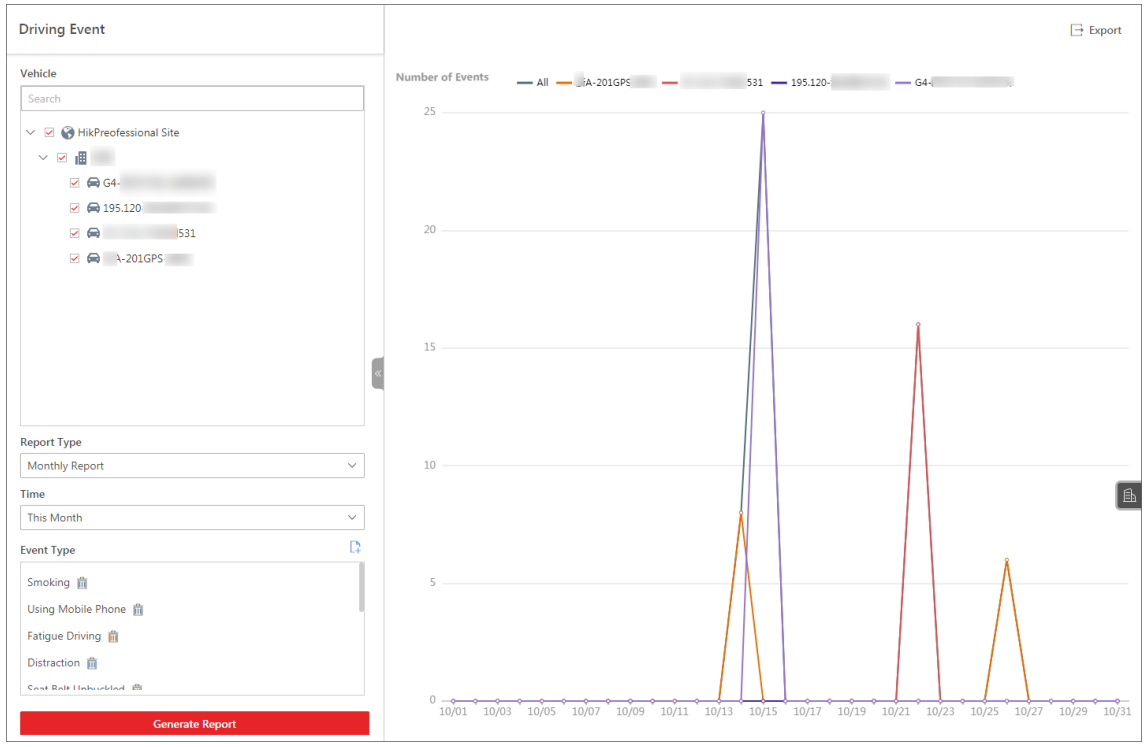



**Figure 17-38 View Data in Line Chart**

## Fuel Consumption Analytics Report

You can create a fuel consumption analytics report to view the fuel consumption of specific vehicles or drivers in a certain period.

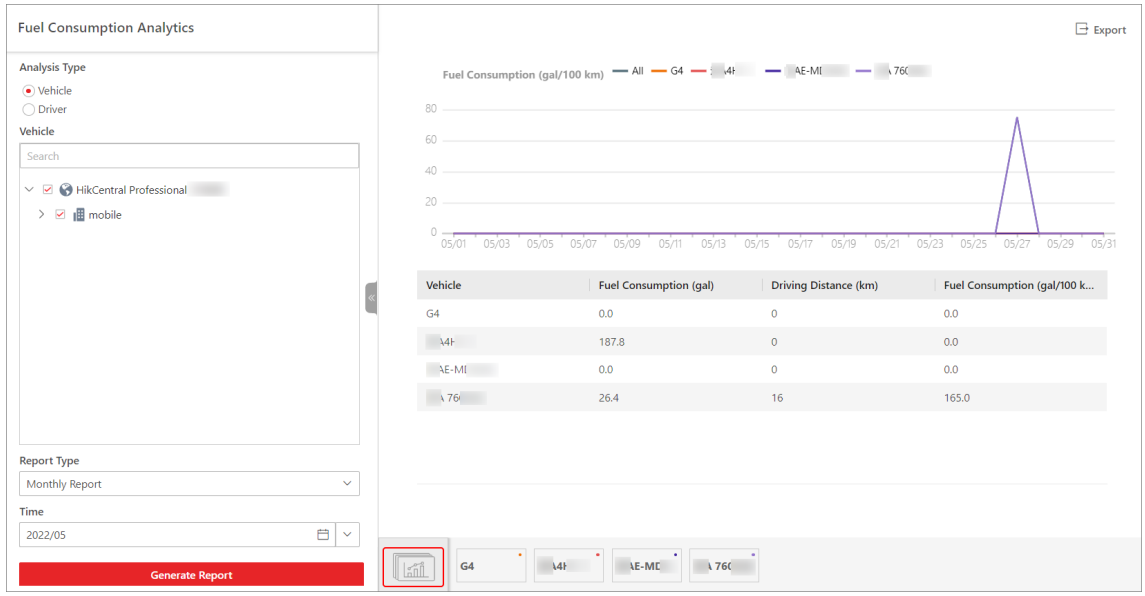



**Figure 17-39 Monthly Report Example**

## Passenger Counting Report

You can create a passenger counting report to view the number of passengers who got on/off in a specific period.




**Figure 17-40 Generate a Passenger Counting Report**

## Device Online Rate Report

You can create a report to view the online rate of the on-board devices mounted on the selected vehicles in a specific period.

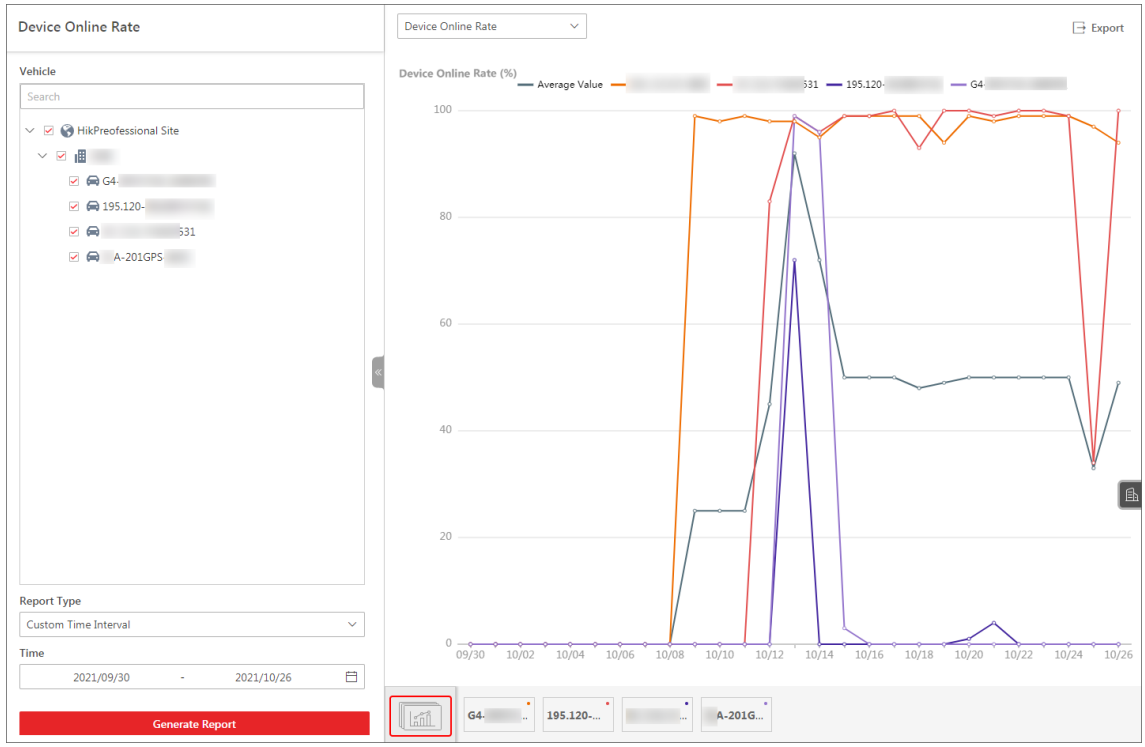



**Figure 17-41 View Data in Line Chart**

## 17.9 On-Board Monitoring Overview

The Overview page displays the major steps of On-Board Monitoring configuration and presents statistics reports by different contents and device health check reports.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **On-Board Monitoring Overview** .

### Wizard

On the top of the overview page, you can view the brief introduction of the On-Board Monitoring function and the major steps of configuration, including device management, vehicle monitoring configuration, event and alarm configuration, and driving monitoring. Hover the cursor over each step and click ↗ to go to the corresponding page.

### Report

Click the **Report** tab.
You can have an overview of on-board monitoring data in the last 7 days on one page, including the GPS information, driving distance, driving duration, overspeed times, and driving events. See ***Statistics and Reports*** for how to view more details and reports.

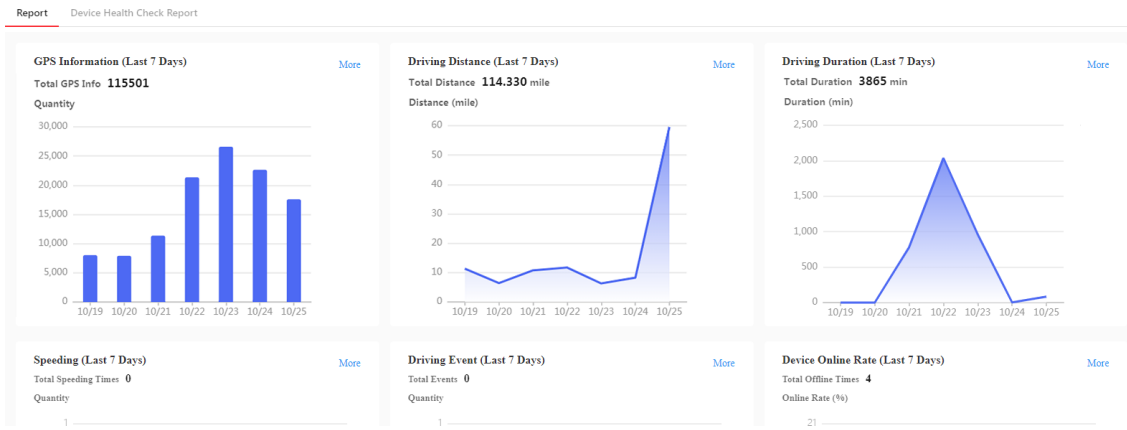



**Figure 17-42 Statistics Overview**

You can perform the following operations on the page.

- **View One Day's Data**
  Hover the cursor onto a chart to view the data of a specific day.

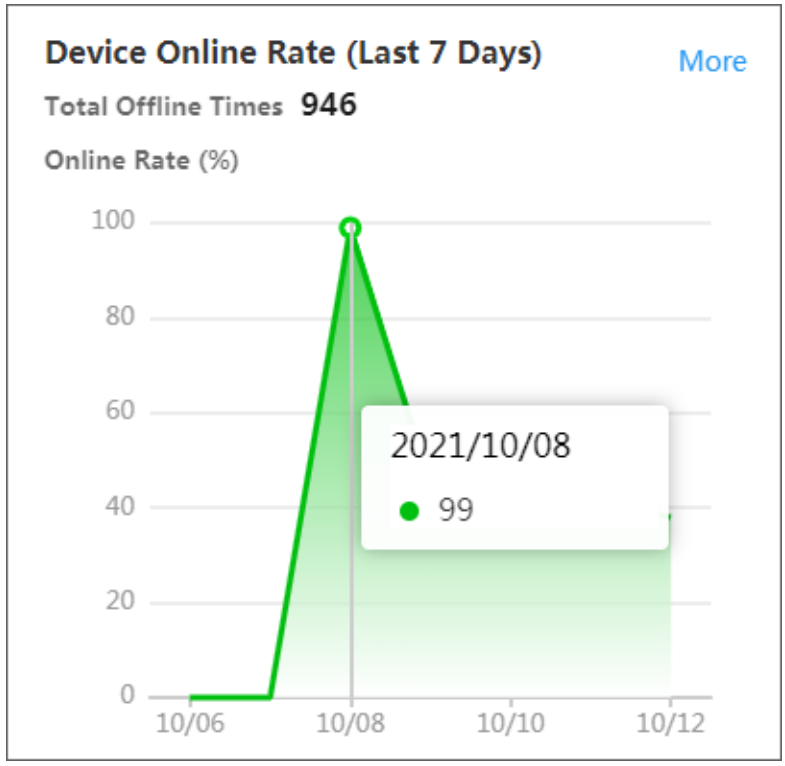



**Figure 17-43 Example**

- **Jump to the Report Generation Page**
  If you need to view the data in other periods, click **More** in the upper-right corner of a chart. For example, you can click **More** in the Driving Distance chart area to jump to the page as shown in

the figure below and be ready for generating driving distance reports according to the conditions you set.

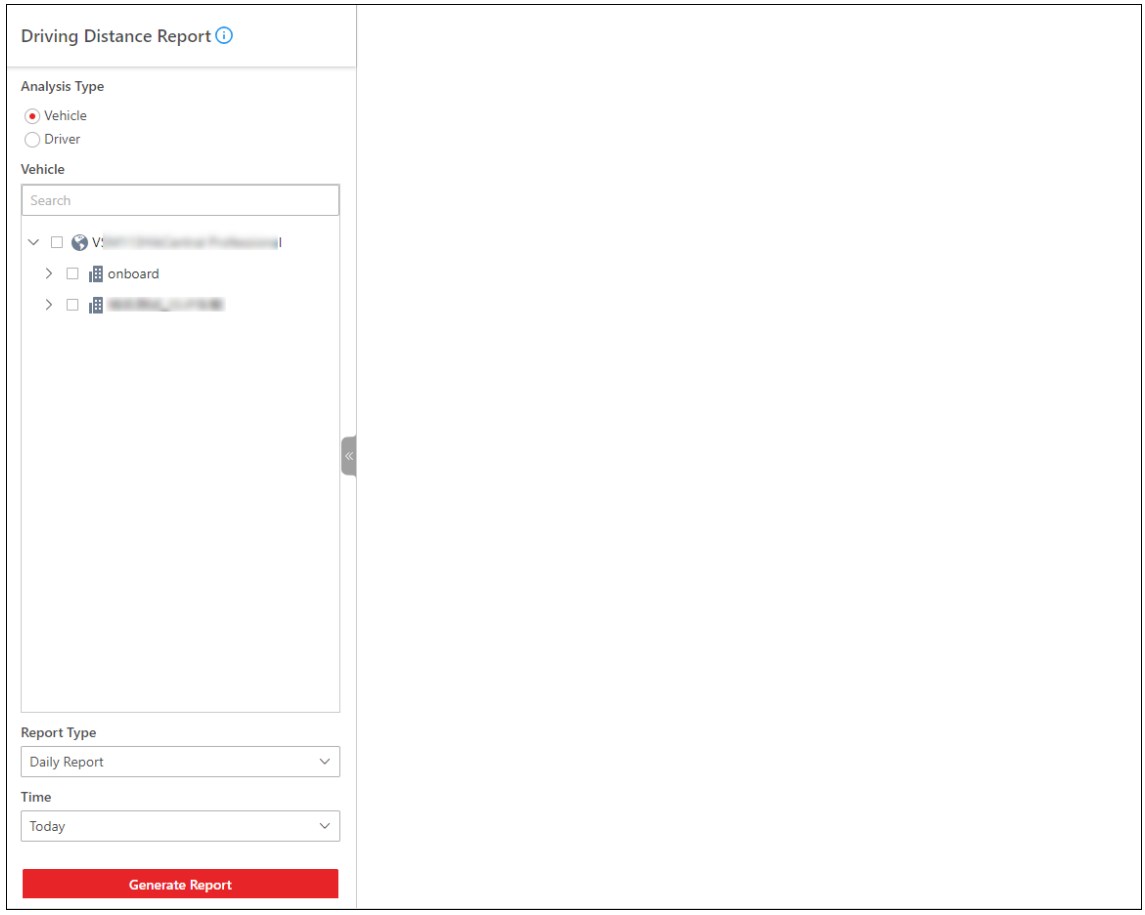



**Figure 17-44 Generate Report**

## Device Health Check Report

Click the **Device Health Check Report** tab.
You can view the device health check by different vehicles.

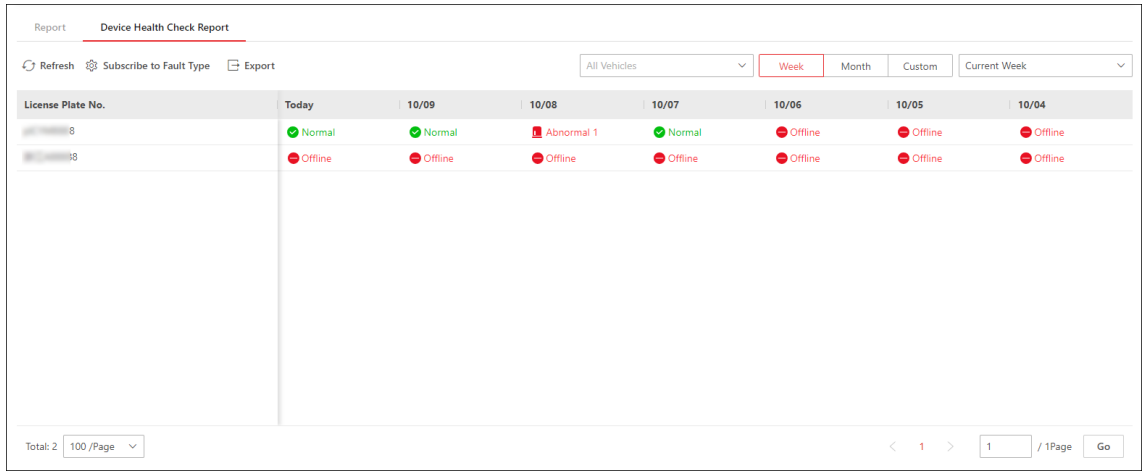



**Figure 17-45 Device Health Check Report**

Perform the following operations as needed.

| | |
|---|---|
| Specify Vehicle | Click **All Vehicles** and select vehicles from the drop-down list to be displayed. |
| View Health Check of A Specific Device | Click the status of a device on a specific date to view the health check details on the right. In the panel of health check details, you can click **All Fault Types** and select a fault type from the drop-down list to filter the fault(s) displayed. |
| Select Time Range | Click **Week** or **Month**, and select a specific week or month; click **Custom**, and customize the time range as needed. |
| Refresh Health Check | Click **Refresh** to refresh the health check for devices. |
| Subscribe to Fault Type | Click **Subscribe to Fault Type**, and check fault type(s) as needed. |
| Export | Click **Export** to open the Export Report panel, check contents to be exported as needed, and click **Save** to export the report. |

# Chapter 18 Manage Smart Wall

Smart wall can provide security personnel with a rich visual overview of the areas you want to keep an eye on. After you configure a virtual smart wall, you can add smart wall devices like video wall controllers and link device's decoding outputs with windows of the smart wall to show videos on LED or LCD displays.

To add smart wall devices and smart walls, go to the top navigation bar and select → **Basic Management → Device → Device and Server → Smart Wall** .

## 18.1 Add Smart Wall Device

A smart wall device refers to the decoder, video wall controller, or multi-functional video center. A video wall controller is a device that manages the content displayed on a video wall, which is a large display made up of multiple screens tiled together to form a single display area.

1. In the **Smart Wall Device** section, select **Add**.
2. Set the adding mode.

| Adding Mode | Scenario |
|---|---|
| Online Device | Devices are within the network where the Web Client or SYS server is located.<br>**Note**<br>- For Google Chrome, install the SADP service according to the instructions. For Firefox, install the SADP service and import the certificate according to the instructions.<br>- Server Network: The detected online devices in the same local subnet with the SYS server will be listed. Local Network: The detected online devices in the same local subnet with the Web Client will be listed. |
| IP Address | Add devices one by one when you know the IP address. |
| IP Segment | Add multiple decoding devices with the same port number, user name and password, but different IP addresses within a range. |
| Port Segment | Add multiple decoding devices with the same IP address, user name and password, but different port numbers within a range. |

3. Select **Add**.

## 18.2 Add Smart Wall

1. In the **Smart Wall** section, click **Add**.
2. Set the following parameters: **Smart Wall Name**, **Smart Wall Type**, **Max. Resolution of Single Output**, and **Row × Column**.

**Note**

For LED smart walls, you need to set the row height and column width.

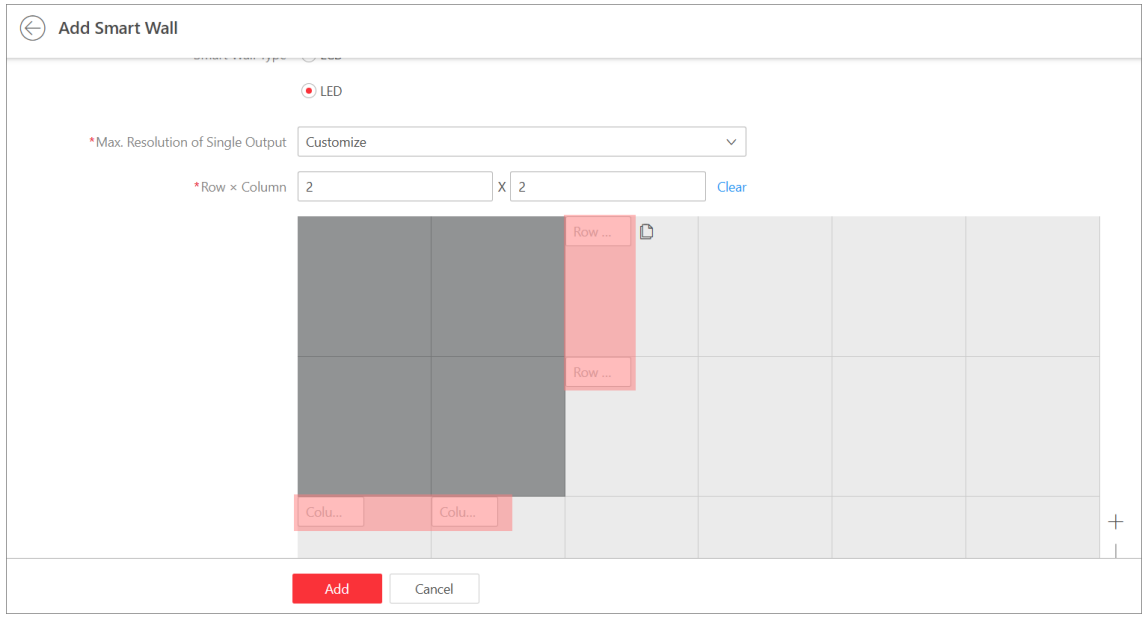



**Figure 18-1 Set Row Height and Column Width**

3. Click **Add**.
4. Perform the following operations as needed.
   - Select **Stream Type Settings** to set the default stream type for channels on the smart wall.

     **Caution**

     To ensure the stream type setting takes effect, go to the video wall controller's web configuration page, select **Sub-Stream Auto-Switch**, and disable automatic switching to the sub-stream when the smart wall window number exceeds the threshold.
   - Select **Delete All** to delete all smart walls.

## 18.3 Link Decoding Output with Window

After you add the smart wall device and virtual smart wall, link the smart wall device's decoding outputs with the windows of the smart wall to display videos.

1. Click › in front of a decoding device to show its decoding outputs.
2. Click › in front of a smart wall to show its windows.
3. Drag a decoding output to the window of the smart wall.

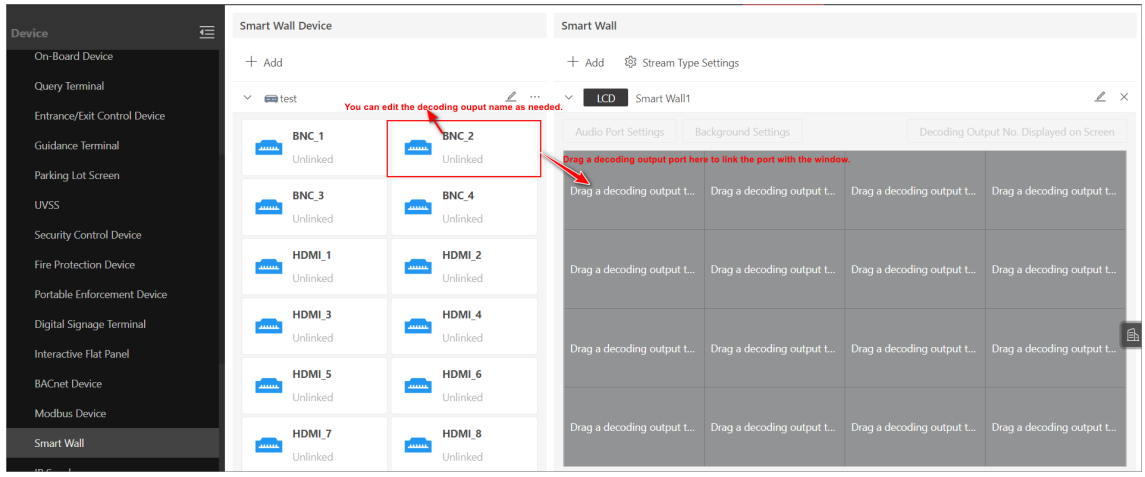



**Figure 18-2 Link Decoding Device with Window**

4. Set the audio port and background.

**Note**

- To play the audio of the video wall on the Control Client, select a decoding output as the audio port first.
- Setting a background picture is only available for certain types of devices.

## 18.4 Display Alarms on Smart Wall

To view the linked alarms on the Control Client, you should configure the alarm linkage on the Web Client.

1. Select → **Event and Alarm** → **Event and Alarm Configuration** → **Normal Event and Alarm** .
2. Select **Add** and set the triggering event and source.

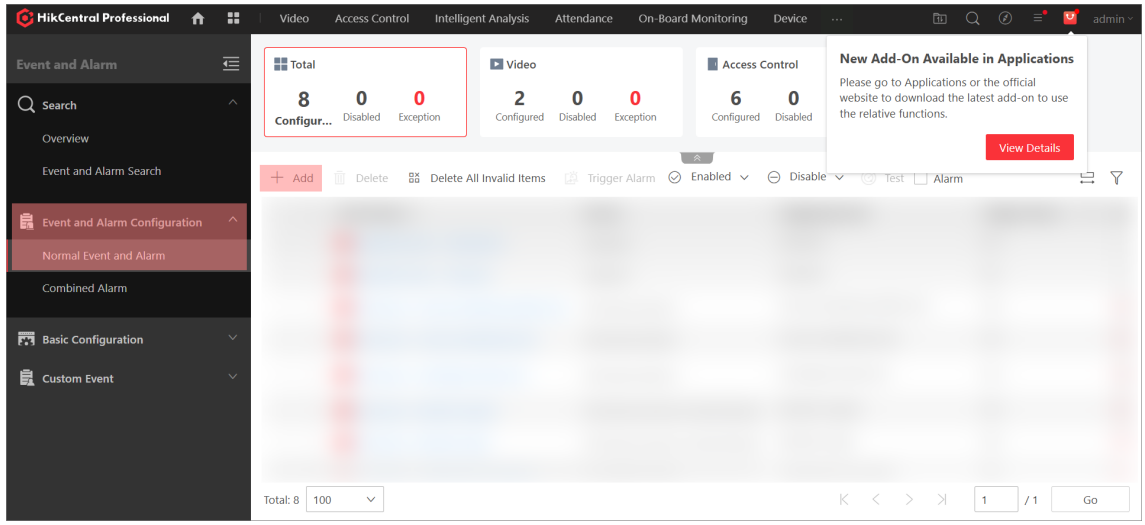



**Figure 18-3 Add Event and Alarm**

3. In the Basic Information section, select triggering events and sources as needed.

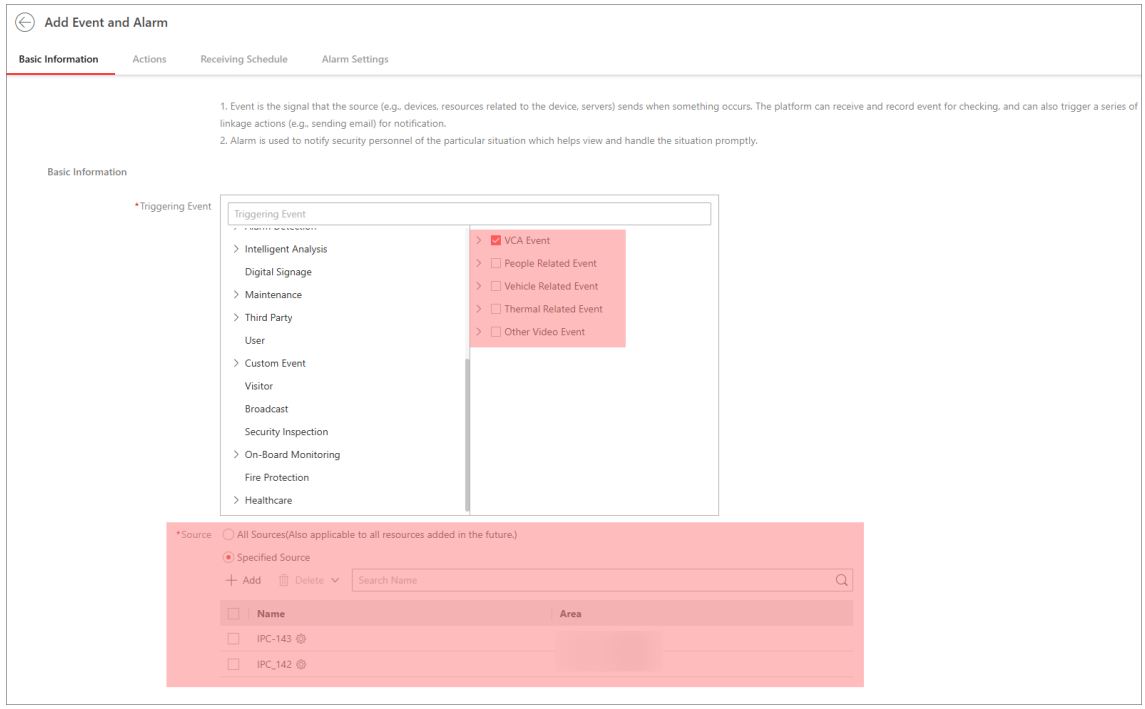



**Figure 18-4 Select Triggering Events and Sources**

4. In the Alarm Settings section, enable **Trigger Alarm** to set the alarm priority and recipients.

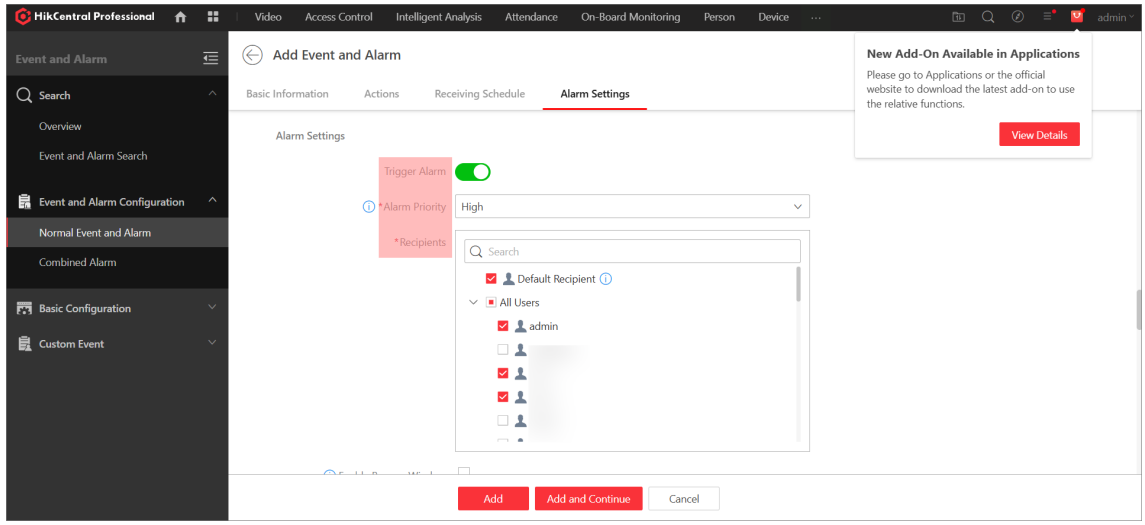



**Figure 18-5 Set Alarm Priority and Recipients**

**Note**

You can go to **Basic Configuration → Alarm Custom Settings → Add** to customize the alarm priority.

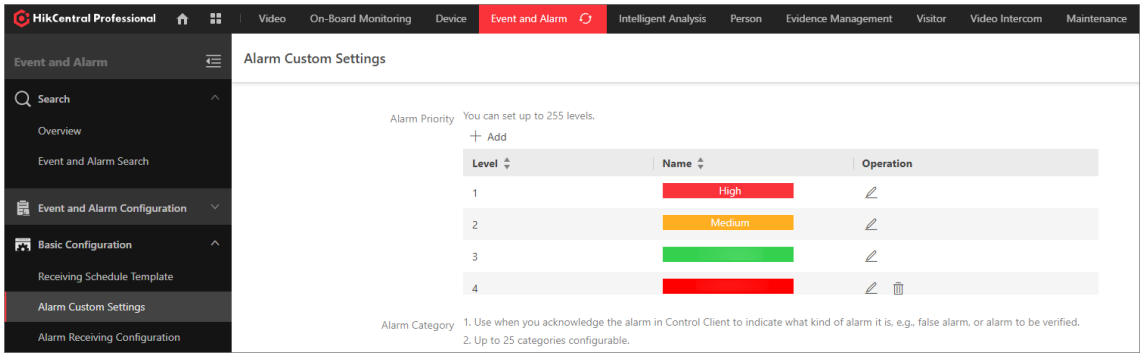



**Figure 18-6 Customize Alarm Priority**

5. Enable **Display on Smart Wall** to set the smart wall type, display resource, stream type, smart wall name, alarm display window (for LCD smart walls), and alarm display duration. The following table will show major parameters.

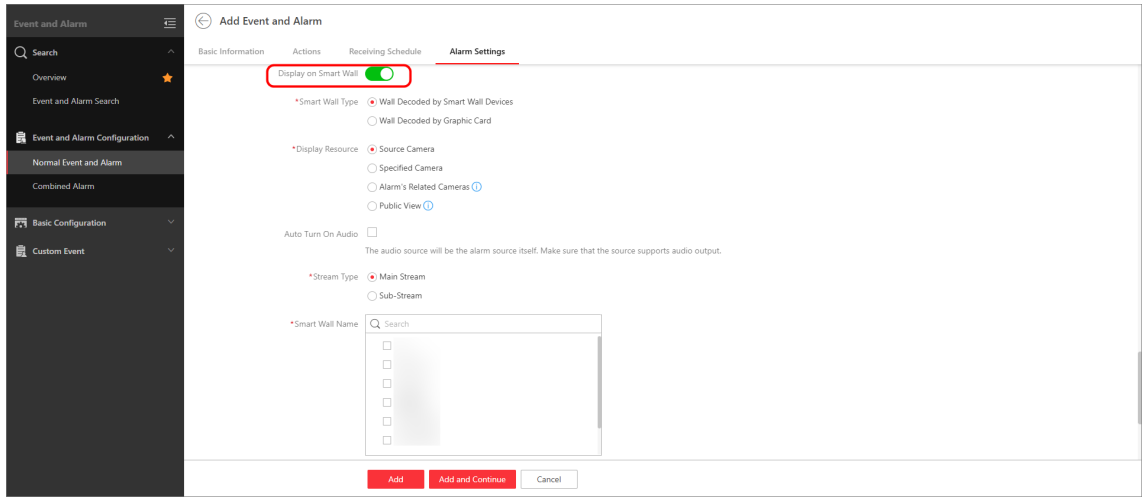
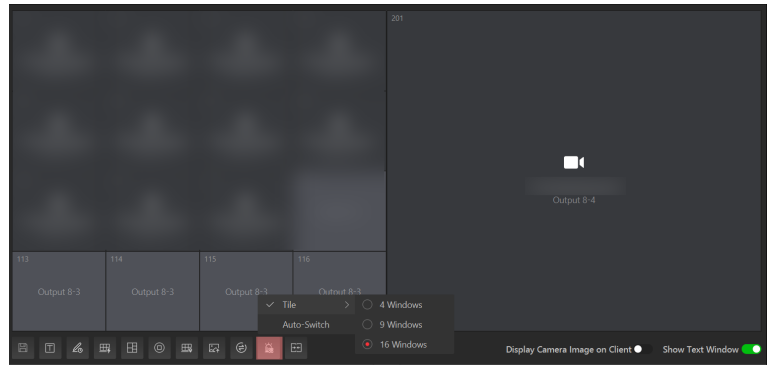



**Figure 18-7 Display Alarms on Smart Wall**

| Parameter | Description |
|---|---|
| Smart Wall Type | - Wall Linked to Device: The video streams will be decoded by linked smart wall devices such as video wall controllers and decoders.<br>- Wall Related to Graphic Card: The PC running the Control client can decode the video streams by its graphic card. |
| Display Source | - Source Camera: When an alarm is triggered, display live videos from the camera that directly reports the alarm (e.g., the specific camera for motion or intrusion detection).<br>- Specified Camera: When an alarm is triggered, display live video from specified linked cameras. You can link up to 16 cameras.<br>- Alarm's Related Cameras: When an alarm is triggered, display live video from the source camera and you can play back the recorded alarm-related video. Set the Trigger Recording as the linkage action first.<br>- Public View: When an alarm is triggered, the system displays the pre-saved public view from the Monitoring or Smart Wall module. For example, if a fire is detected, the smart wall will display the public view of all entrances for monitoring evacuation procedures. |
| Auto Turn On Audio | Enable automatic alarm audio playback from the following display sources: Source Camera, Specified Camera, and Alarm's Related Cameras when an alarm video is displayed on a smart wall. The |

| Parameter | Description |
|---|---|
| | latest alarm audio is prioritized when multiple alarms are triggered. |
| Stop Displaying Alarm | - **Alarm Display Duration**: Alarms will not be displayed on the smart wall after the specified duration.<br>- **Display Alarm with Higher Priority and in More Recent Time**: On the Control Client, if all alarm windows have reached the maximum division number in Tile mode, or if all alarm windows have reached the maximum number of alarm auto-switch in Auto-Switch mode, any new alarms will cover lower priority alarms and will be displayed in the order of their occurrence. If you don't check this parameter, any new alarms will not be displayed on the smart wall.<br>  <br>**Figure 18-8 Alarm Display Mode** |

**Note**

- For LED smart walls, you don't need to specify an alarm window. If multiple windows are opened and no alarm windows are specified on the Control Client, alarms will be displayed on the smart wall from left to right and from top to bottom.
- For LCD smart walls, if alarm windows are specified on both the Web Client and Control Client, alarms will be prioritized for display within the alarm windows specified on the Control Client.

6. After adding events, go back to the Normal Event and Alarm page, select the added event, and select **Test**. You can view the triggered alarm in a window on the Control Client.

## 18.5 Check Device Status

After adding smart wall devices such as video wall controllers, you can monitor the real-time status of both the chassis and cards.

1. Go to → **Basic Management → Maintenance → Resource Status → Smart Wall Device** .
2. In the Operation column, click to view the detailed device status.

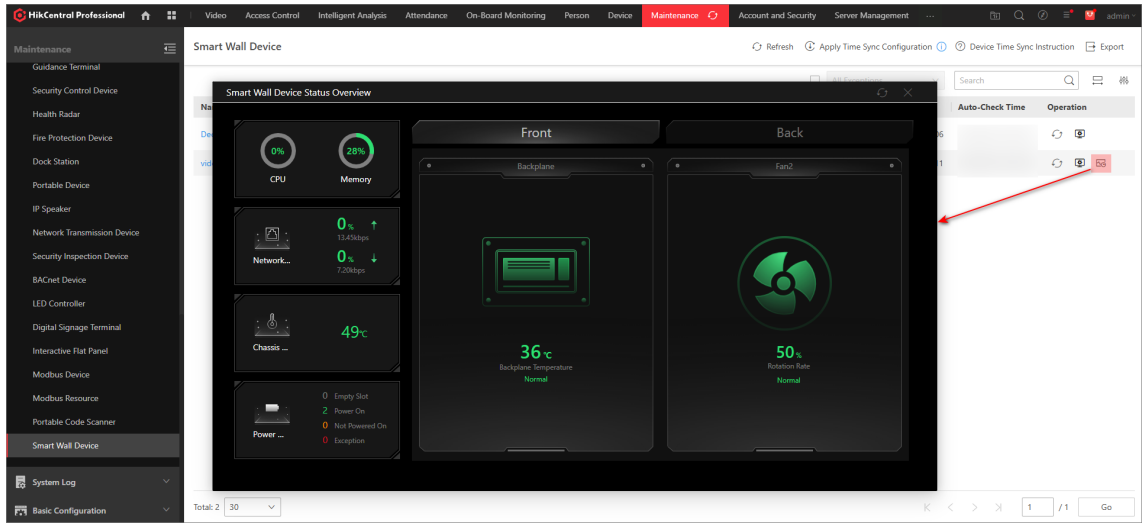



**Figure 18-9 Check Device Status**

# Chapter 19 Portable Enforcement Management

In the Portable Enforcement module, you can apply person information to dock stations and search for device receiving records after the persons receive portable devices. Also, you can monitor in real time the locations of persons who have received portable devices, search for person's historical moving path on the map in a specific time duration, and search for files on the portable devices.

In the top left corner of the Web Client, Go to → **Portable Enforcement** → **Portable Enforcement** to enter the this module.

## 19.1 Before You Start

### 19.1.1 Add Enforcement Officer

An enforcement officer is a person authorized to enforce laws and regulations. They are typically responsible for maintaining public order and conducting patrols to prevent from violations.

For details about adding enforcement officer, refer to ***Add Person*** .

### 19.1.2 Add Dock Station

After on-site enforcement, enforcement officers will return portable devices to the dock station. A dock station is to manage portable devices, including securely storing the portable devices not in use, charging portable devices, and collecting data from portable devices for analysis, which ensure that portable devices are always ready for the next enforcement.

For details about adding dock stations, refer to ***Add Device(s)*** .

For more parameter settings, refer to ***Parameters Exclusive for Dock Stations*** .

### 19.1.3 Add Portable Device

A portable device is a lightweight battery-powered device carried by the enforcement officer in a pocket or hand for on-site enforcement. It can be used for collecting on-site evidence, two-way audio among enforcement officers, etc.

For details about adding portable devices, refer to ***Add Device(s)*** .

For Android portable devices, captured face pictures can be compared against a face picture library by an intelligent fusion server, enabling rapid identification of suspicious individuals during events like huge concerts. Take the following steps:

1. Apply for licenses for face picture comparison.

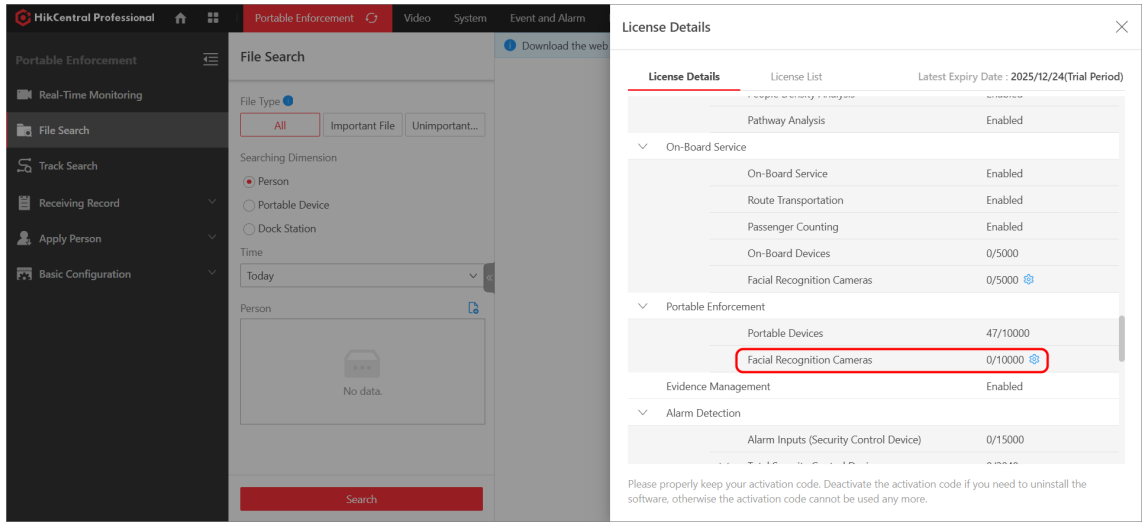



**Figure 19-1 Apply for License**

2. Go to **Video → Intelligent Recognition → Intelligent Recognition Task → Add** .

**Note**

You should set the **Analysis Type** to **Face Picture Comparison**and **Device for Analysis** to **Intelligent Fusion Server**.

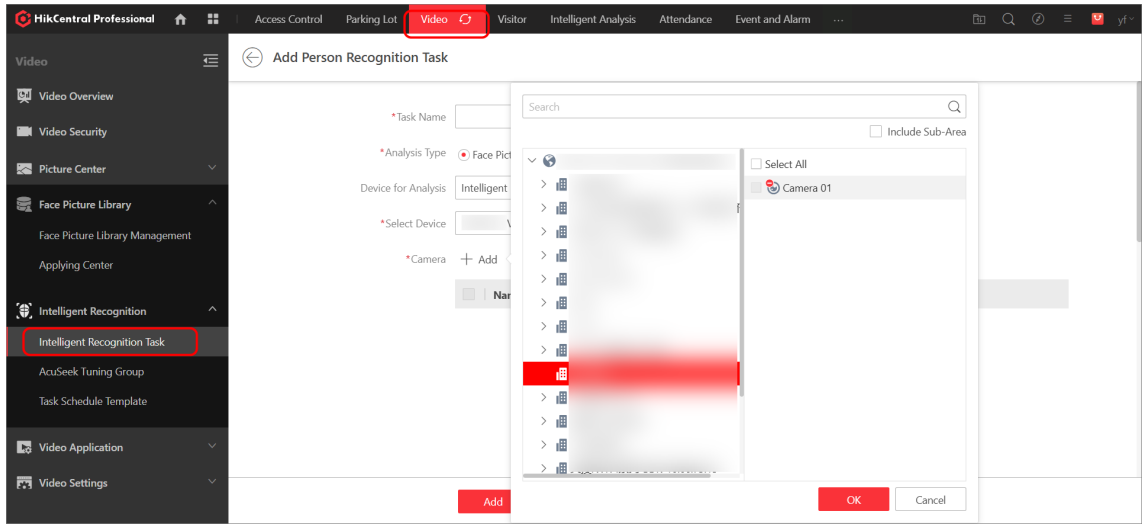



**Figure 19-2 Configure Face Comparison Task on Video Page**

3. Set the task information.

**Note**

You should set the **Analysis Type** to **Face Picture Comparison**and **Device for Analysis** to **Intelligent Fusion Server**.

4. Add cameras with the face recognition license.
5. Select a face picture library and similarity.
6. Click **Add**

### 19.1.4 Apply Person to Dock Station

You should apply person information to the dock stations, so that the corresponding person can log in to the dock station to receive and use the portable device. You can apply by person, by department, or by device.

Go to → **Portable Enforcement** → **Portable Enforcement** , and select **Apply Person** on the left panel.

On the Application Overview page, you can:

- have an overview of person application records including the number of all persons added to the platform, persons failed to be applied, persons applied, and persons to be applied, etc. Click **All**, **Invalid**, **valid**, and **Not Configured** to view the detailed persons.
- apply persons to dock stations by person. refer to ***Apply by Person*** for details.
- apply person to dock stations by device. refer to ***Apply by Device*** for details.

**Note**

You can apply up to 3,000 persons to a dock station.

#### Apply by Person

You can select persons and apply the information of selected persons to the dock stations. After applying, you can view application details, reapply failed records, etc.

#### Entry 1 of Applying by Person

1. Click **Apply by Person** on the left navigation bar.
2. Click **Add Linked Person** on the top.
3. On the Add Linked Person panel, click to select person(s).
4. Select dock station(s). represents that the dock station is offline.
5. Enable **Link to Portable Device for Receiving** and select one or more portable devices.

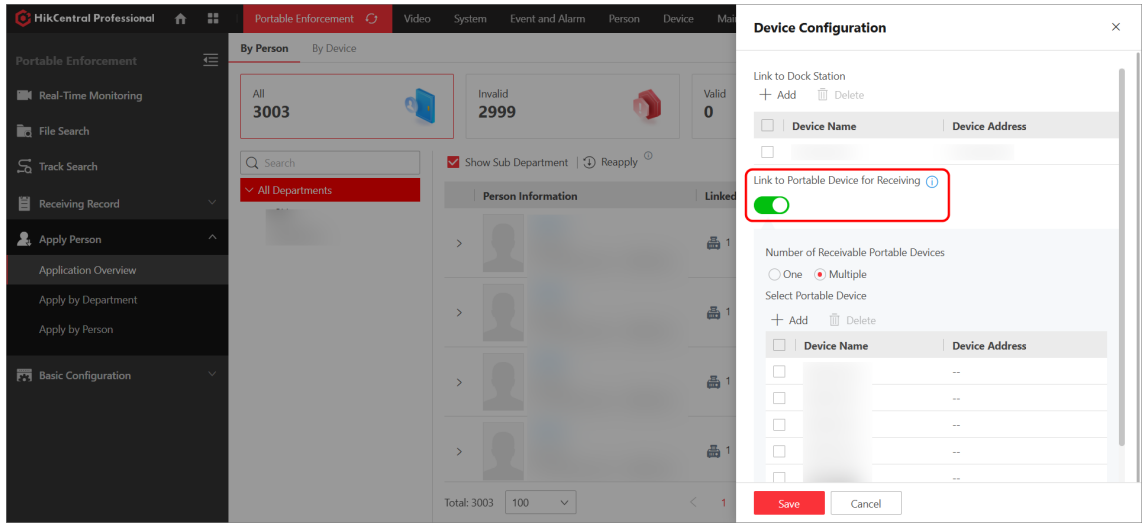



**Figure 19-3 Link to Portable Device for Receiving**

6. Click **OK**.

## Entry 2 of Applying by Person

1. Click **Application Overview → By Person** .
2. Select a department on the left and then select a person in this department.
3. Click in the Operation column.
4. Click **Add** to select dock station(s). represents that the dock station is offline.
5. Enable **Link to Portable Device for Receiving** and select one or more portable devices.
6. Click **OK**.

## Operations After Applying by Person

- View Dock Station Linked with Person: click › beside the person profile to view the dock station details including device name and IP address.
- For persons are linked to a dock station and portable devices, go to **Device → Portable Enforcement Device → Dock Station** , select the linked dock station, and set the receiving mode to **Linkage Mode**.

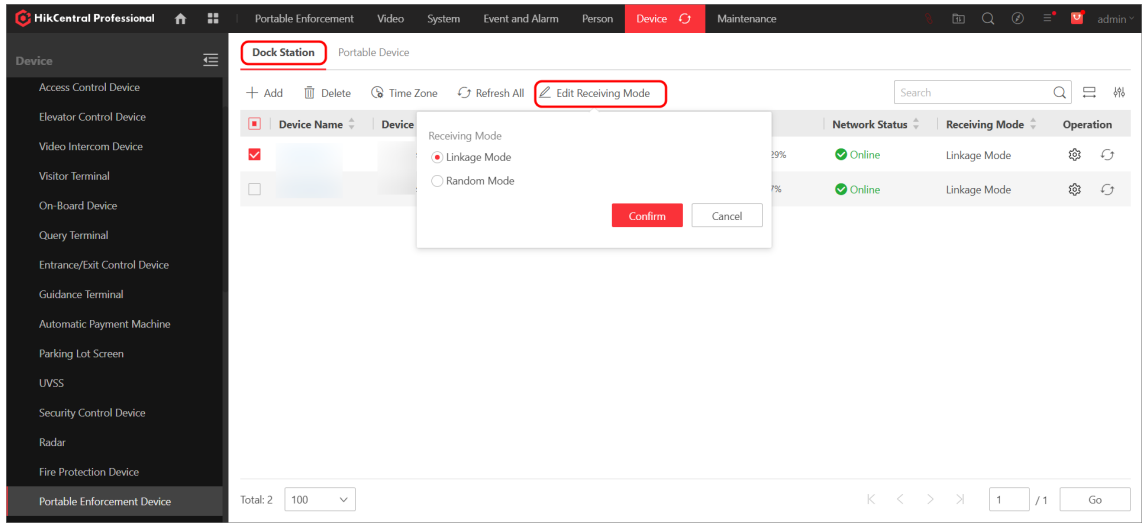



**Figure 19-4 Change Receiving Mode**

## Apply by Department

You can select a department and apply the information of persons in the selected department to dock stations. After applying, you can view the application details, unlink the dock station with the department, etc.

**Steps**

1. Select **Apply by Department** on the left navigation bar.
2. **Optional:** Select a department on the left.
3. Link department(s) to dock station(s).
   - Click **Link to Dock Station**, select dock station(s), and click **OK**.

     **Note**

     represents that the dock station is offline.
   - Click **Batch Link**, select departments and dock station(s), and click **OK**.

   The persons in the selected department(s) are applied to the selected device(s). You can view the applying results. If applying failed, you can view the failure details.
4. Enable **Link to Portable Device for Receiving** and select one or more portable devices.
5. Click **OK**.
6. **Optional:** Perform the following operations.

| | |
|---|---|
| **Unlink Dock Station With Department** | Select one or more dock stations, and click **Unlink** to unlink the dock stations with department(s).<br>Move the mouse cursor to ⌄, and click **Unlink All** to unlink all dock stations with departments. |

| | |
|---|---|
| **View Failed Applying Details** | If there are failed applying records, ⓘ will be displayed beside **Link to Device**. Hover on ⓘ and click **View Details** to view the failure details. |

### Apply by Device

You can link dock stations with persons.

**Steps**

1. Select **Apply Person → Application Overview → By Device** .
2. Cursor on ⌄ to select **Dock Station** or **Portable Device**, and set conditions to filter devices.
3. Click ✎ in the Operation column.
4. Click 🗎 to select the linked persons.
5. Click **OK**.
6. **Optional:** Unlink persons from devices.
   - Select devices, click **Unlink from Person** or 🔗 in the Operation column to unbind the selected devices from all linked persons and departments.
   - Click ⌄ **→ Unlink All from Person** to unbind all devices in the device list from all linked persons and departments.

## 19.2 Basic Parameter Configuration

You can configure basic parameters such as distant unit and GPS data retention period for the portable enforcement module.

**Steps**

1. Select **Basic Configuration → Basic Parameter Configuration** on the left panel.
2. Configure the parameters.

   **Distance Unit**

   Select **Kilometer (km)** or **Mile (mi)** as the distance unit according to actual needs.

   **GIS Map**

   Click **Edit Configuration**, enable **GIS Map** and configure online or offline GIS map. For online GIS map, enter the API URL of the GIS map; for offline GIS map, configure the map beforehand and upload the file to the platform.

   **Show GIS Map**

   Enable/disable GIS map display as needed for the portable enforcement real-time monitoring page.

   **GPS Data Retention Period**

   The retention period of the GPS data. Select from the drop-down list to set the retention period and data volume.
3. Click **Save** to save the above settings.

## 19.3 Real-Time Monitoring

On the Real-Time Monitoring page, you can monitor the person with portable device on the map in real-time. You can also directly locate and monitor devices based on the device itself, eliminating the need for complex personnel configuration and boosting management flexibility.

**Note**

To use this function, make sure you have configured the GIS map. For details, refer to ***Basic Parameter Configuration*** . Make sure you have added portable devices and persons to the platform.

Go to → **Portable Enforcement** → **Portable Enforcement** → **Real-Time Monitoring** . Select a person or device in the list, and refer to the following for the supported operations on this page.

**Note**

For many retail scenarios without GPS information indoors, the Web Client also supports real-time monitoring in GPS free mode. Click **Configure Now** on the top and turn off the GIS map display. After it is disabled, the section of GIS map on this page will be hidden. The configuration will be remembered next time you log in.

- Switch between **Device Overview** and **Person Overview** to monitor devices by the linked person or the device itself.

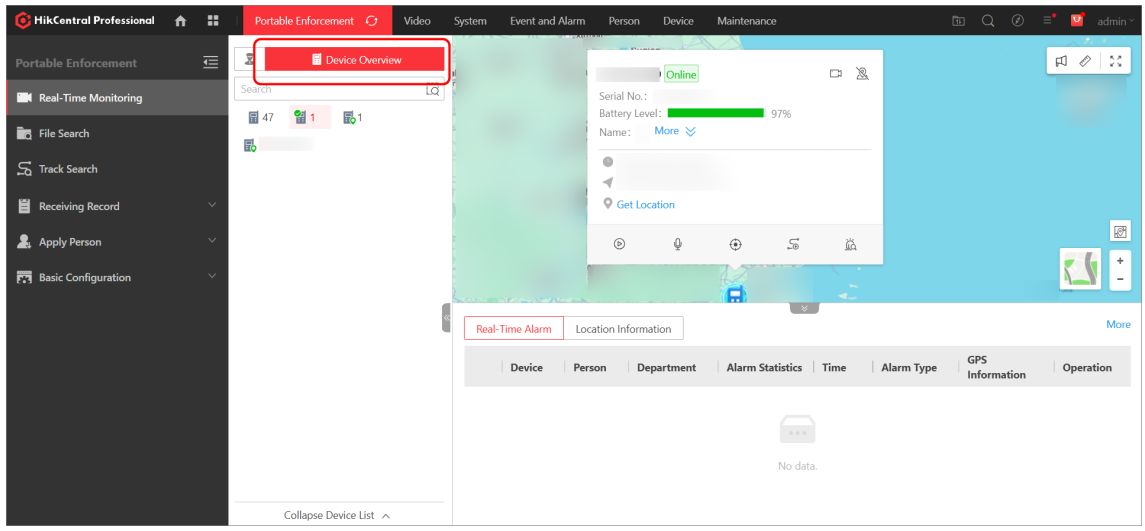



**Figure 19-5 Real-Time Monitoring by Device**

- : Search for the target person(s) by drawing an area. During search, you can locate person(s) and broadcast to person(s).
- **View Person Details**: View person's profile picture, department, battery capacity of the portable device, phone number, location information, etc.
- / : Locate or cancel locating the person on the map.

- : Make the person in the center of the view.
- **Play Video**: View the live view of the person.
- **Two-Way Audio**: Start two-way audio with the person.
- **Track in Real Time**: View the real-time moving path of the person.
- **Play Back Track**: View the history moving path of the person during the selected time period. You can view the video on the right side if it is recorded.
- : Remotely start or stop portable device recording. This allows command center staff to instantly manage on-site recording in emergencies, ensuring both evidence collection and officer privacy. You can also go to **Device → Portable Enforcement Device → Portable Device** to enable/disable video recording.
- **Format Storage**: Clear all SD card data to prevent data leakage.
- **Lock Device**: Disable buttons and screen to prevent unauthorized access or tampering.
- **Remote Shutdown**: Power down the device to prevent unauthorized or malicious use.
- **View History Alarm**: View history alarm uploaded by the person.
- : Start broadcasting to the person.
- : Measure the distance on the map.
- : View real-time monitoring in full screen.
- **Real-Time Alarm**: View the real-time alarm uploaded by the person. You can view the alarm type, alarm time, GPS information, etc.
- **Location Information**: View person's detailed longitude and latitude information, which will be refreshed every 10 seconds by default (the refresh frequency can be edited on the device). You can check **Auto Get Location** to get person's location information automatically.

## 19.4 How to Configure Group Intercom and its Application

You can configure person groups for group intercom. In the same group intercom, persons can listen and speak to each other. Up to 128 groups can be added and up to 100 persons can be added to each group.

**Steps**

1. Select **Basic Configuration → Group Intercom Configuration** on the left panel.
2. Click + on the left of the page to add a group intercom group.
3. On the pop-up pane, configure the following parameters.

   **Group Name**

   Enter a group name of the group intercom as required.

   **Streaming Server**

   If this parameter is enabled, select a server from the drop-down list.

   **Group Person**

   Click and check persons from different apartments. Click **Add**.
4. Click **Add** to add the group intercom group.

The list of added group intercom group(s) will be displayed on the left.

**What to do next**

Persons in the same group make individual or group calls via their portable devices.

## 19.5 How to Save Files on the Dock Station to Evidence Center?

You can set conditions such as file type, searching dimension, and time to search for files on portable devices. For the searched files, you can mark files as important, save files to the evidence management center, export files, etc.

**Steps**

1. On the left navigation bar, select **File Search**.
2. Set the search conditions including file type, searching dimension, time, and the corresponding device(s)/person(s).

   **Note**

   For searching by persons, up to 200 persons are allowed.
3. Click **Search**.

   The search results are displayed and sorted by person/device on the right side. You can filter searched files by file type, person/device name, and tag (make sure you have applied tags to device in Device module). Also, you can click a file to view its detailed information.
4. Select one or more files, click **Save to Evidence Management Center**, configure the parameters such as adding mode and file tag, and click **OK** to save the selected files to the evidence management center.

   **Note**

   For details about managing files in the evidence management center, refer to ***View and Edit Files*** .

## 19.6 How to Play Back Tracks?

Track search and playback are important for analyzing specific incidents or events to understand what happened, verifying whether the recorded data is accurate. You can set conditions to search for and play back tracks.

**Steps**

1. Select **Track Search** on the left panel.
2. Set the searching dimension and time range for search.
3. Click to select a person or device.
4. Click **Search**.

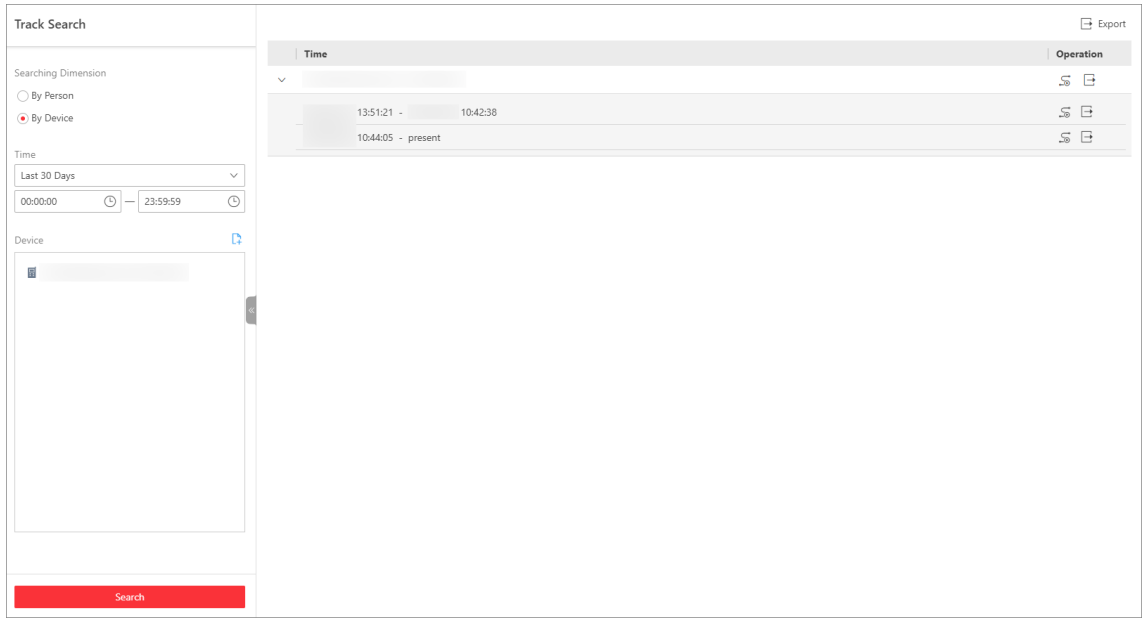



**Figure 19-6 Search Results**

5. Click in the Operation column to play back all tracks, or the track in a specific time duration on the map.
6. **Optional:** During track playback, perform the followings on the map.
   - Click **Stop** to stop playing back person's track.
   - Click to start broadcasting.
   - Click to measure the distance of track.
   - Click to view the track in full screen.
7. **Optional:** During track playback, perform the followings on the bottom toolbar.
   - Click **Skip No-Recording Time** to skip the no-recording time of the video.
   - Click **Switch Time** to switch to another time period for viewing playback.
   - Click **Center Person** or **Cancel Centering Person** to center or cancel centering the person on the map.

## 19.7 Search for Receiving Records

After the persons receive portable devices, you can set conditions to search for receiving records. You can either search by person or by device. For the search result(s), you can export them as needed.

On the left pane of the Portable Enforcement module, select **Receiving Record**.

For search results, you can perform the following operations as needed:

- Click and select a self-adaptive column width mode.
- Click and select display items like the name of portable device, person ID, dock station of receiving/returning, battery when receiving/returning, department, receiving time, return time, etc. as needed. By default, all supported column items are selected. You can click **Reset** to reset the selected items.

## 19.7.1 Search for Receiving Records by Person

You can select persons and set other conditions to search for receiving records.

**Before You Start**

- Make sure you have added portable devices to the platform.
- Make sure you have added persons to the platform.

**Steps**

1. On the left pane of the Receiving Record page, select **Receiving Record by Person**.
2. **Optional:** Set the search conditions including receiving time, return status, and person range.
3. Click **Search**.

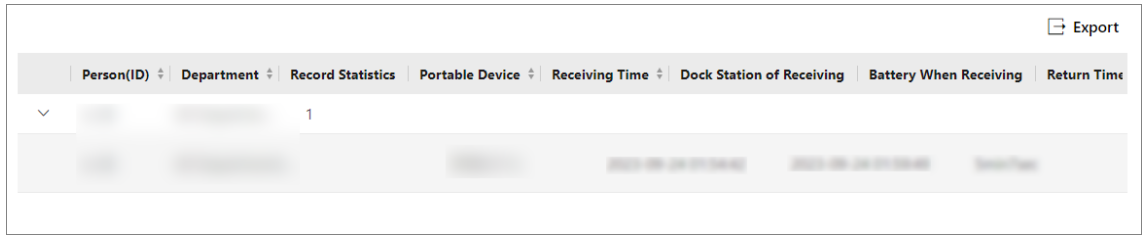



**Figure 19-7 Search for Receiving Records by Person**

The search results are displayed on the right side.

4. **Optional:** Click **Export** in the upper-right corner to export the receiving records to local PC.

## 19.7.2 Search for Receiving Records by Device

You can select devices and set other conditions to search for receiving records.

**Before You Start**

- Make sure you have added portable devices to the platform.
- Make sure you have added persons to the platform.

**Steps**

1. On the left pane of the Receiving Record page, select **Receiving Record by Device**.
2. **Optional:** Set the search conditions including receiving time, return status, and device.
3. Click **Search**.

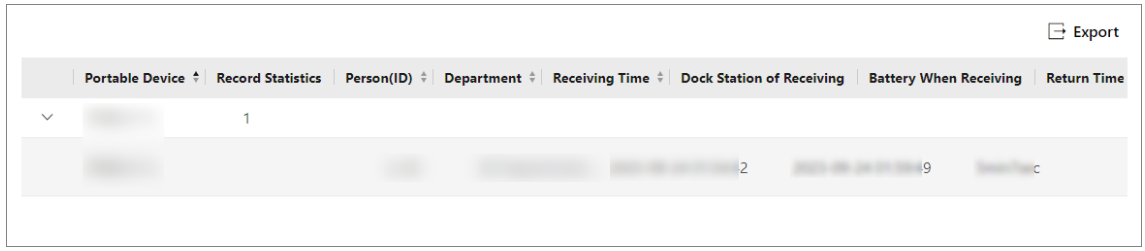



**Figure 19-8 Search for Receiving Records by Device**

The search results are displayed on the right side.

4. **Optional:** Click **Export** in the upper-right corner to export the receiving records to local PC.

# Chapter 20 Intelligent Analysis Report

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In HikCentral Professional, reports can be generated daily, weekly, monthly, annually, and by custom time period. The reports can also be added to the dashboard for browsing at a glance. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

### Before You Start

1. Make sure you have added devices that support specific detection functions to the platform ( ***Device and Server Management*** ), and added group resources linked with devices to different areas ( ***Add Element to Area*** ).
2. Select the scenario: public scenario or retail/supermarket scenario. After you switch to the other scenario, a navigation in accord with the scenario will be generated, and the platform will be refreshed and loaded to a scenario-fit status.

   **Public Scenario**

   Non-Store Scenario (e.g., Subway, Square). You can view reports collected from an analysis group or camera about people counting, person features, heat data, etc.

   **Retail/Supermarket Scenario**

   The scenario is specially designed for stores. In this scenario, you can view reports of a store or multiple stores.

   **Note**

   After you switch scenarios, the data of the previous scenario will be preserved for 30 days before cleared.

### Entry

In the top left corner of the Web Client, select → **Operation Analytics** → **Intelligent Analysis** to enter the this module.

## 20.1 Retail/Supermarket Scenario

The Retail/Supermarket Scenario is designed for stores in the retail industry. In the section, you can view single/two/multiple store reports. You can also view intelligent reports such as store people counting and store heat analysis reports.

### Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario

The following flow chart shows the process of configurations and operations required for intelligent analysis reports in retail or supermarket scenario.

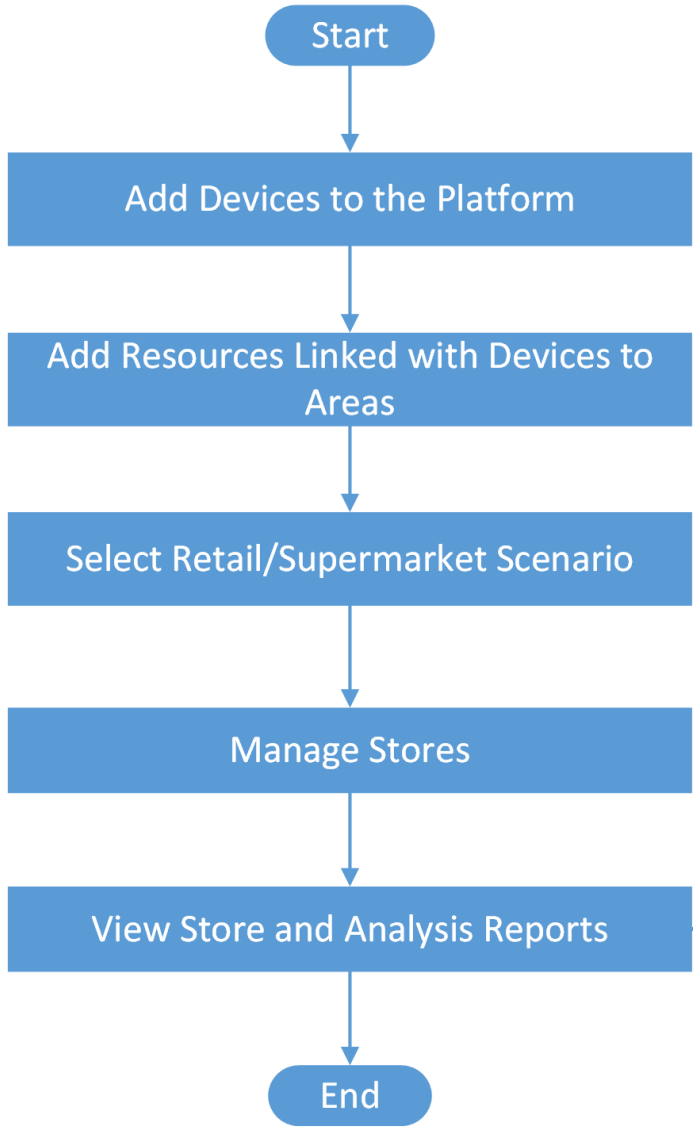



**Figure 20-1 Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario**

### 20.1.1 Add Store

HikCentral Professional supports people counting report and heat analysis report of stores. With the reliable data, store manager can have insight into the customer traffic, dwell rate, tendency of people amount change around promotion days, and consumers movements of stores. Before generating reports of stores, you need to add stores to the platform first, and add the resource group to stores.

In the Intelligent Analysis module, select **Store Management → Configure Store** .

## Add a Single Store

1. Click **Add Store**/ + and set the store parameters.
   - For business hours, at least one and up to 5 time periods are allowed. The added business hours cannot overlap and will be sorted by start time. The list of business hours will be sorted again every time you edit a start time.
   - After setting the store location on the map, its coordinates will be automatically generated.
2. Add resources to the added store.
   a. Select an added store, and click **Configure** to open the Configure Resources page.
   b. In the **Configure Resource Capability** section, click **Add** to add a device, and you can switch on/off a certain capability of the resource.

   **Note**
   - Enabling different capabilities will result in different parameters below.
   - You can click **Configure** to draw the dwell area of heat analysis.

   c. In the **Configure People Counting** section, click **Add** to add entries & exits.
   d. Optional:
   - Select entries and exits of the store for collecting store statistics.
   - Switch on **Regularly Clear All**, and set a time when all data will be cleared.
   - Switch on **Store Capacity Limit**, and when the number of people in the store exceeds the limit, you will be notified. For details, click **Configure Event and Alarm** to configure it.
   - Click **Configure People Counting Excluding Staff Task** to configure who will be excluded when counting people.

   **Note**

   For details, refer to ***Step 3. Add Intelligent Recognition Tasks*** .

   e. For **Deduplication Interval in Device**, click **Sync from Device** to sync the deduplication interval information from the selected resource, or click **Batch Configured and Apply** to enter a specific interval and click **Apply** to apply the interval to all.

   **Note**

   For DeepinMind device, click **Configure People Counting Excluding Staff Task** to set deduplication interval.

   f. Click **Save and Continue**.
3. Add resources to floor.
   a. (Optional) Select a map for the floor.
   b. Select a floor under the Resource tab on the right pane.
   c. Drag the resources to the left map.
   d. Click **Finish**. You will see a dashboard displaying resource status.
4. Configure heat areas and camera coverage. After adding the camera to the floor, configure the heat areas on the camera snapshot and calibrate the camera coverage area on the floor map.

**Note**

Even if the store has only one fisheye camera, you can add the camera to the floor map and continue with heat-area configuration.

| Step | Instruction |
|---|---|
| **1. Open Heat Area Configuration** | a. After adding the camera to the target floor, click **Divided Heat Area Configuration**.<br>b. The system automatically retrieves the camera snapshot.<br>c. If the camera supports rectangular snapshots, the system retrieves the corresponding rectangular image. |
| **2. Draw Heat Areas on the Camera Snapshot** | a. Click to switch to the camera snapshot.<br>b. On the camera snapshot, click **Draw Area** to draw one or more heat areas according to the actual areas to be analyzed, such as an entrance, checkout area, product display area, or promotional area.<br>c. Adjust the position and size of each heat area to match the actual monitored area.<br>d. Name the heat areas if required.<br>e. Click **+ Add** on the right to and add areas for analysis.<br>The configured heat areas are used for single-camera heat map display, heat-zone analysis, ranking, and report generation. |
| **Calibrate Camera Position and Coverage on the Floor Map** | a. Click to switch to the floor map.<br>b. Based on the actual installation location and viewing direction of the camera, adjust the position, orientation, and coverage area of the camera snapshot on the floor map. You can also click **Auto Calibration**.<br>c. Ensure that the camera coverage area is aligned with the corresponding physical area on the floor map.<br>d. Save the calibration result. |

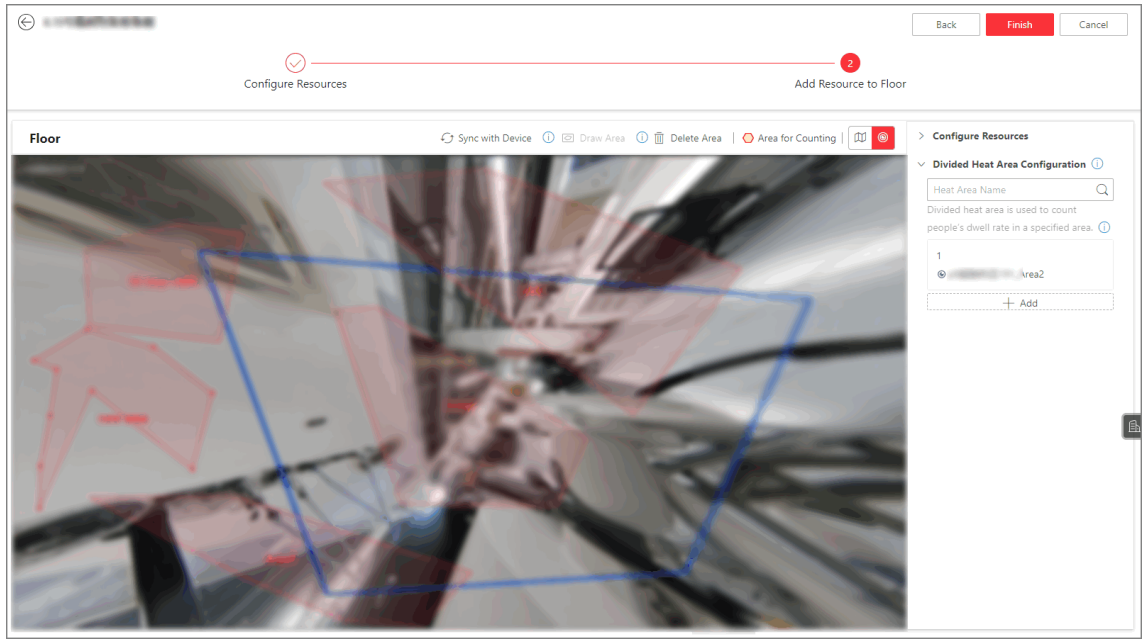



**Figure 20-2 Heat Area Configuration**

## Batch Add Stores

1. Click **Batch Import**/ .
2. Download the store template to your PC, and enter the store information (such as store name, site, and area) following the rules shown in the template.
3. Click to upload the template, and click **OK**. You can view the importing progress and the results.

## Operations for Managing Added Stores

| Operations | Description |
|---|---|
| Edit the Store Information | Select a store and click **Edit** on the right top corner to edit the store information. |
| Edit Opening Hours of Store(s) | • Edit opening hours of a single store: Select a store from the store list panel and click **Configure Opening Hours** on the store details page. Adjust the opening hour and click **Save**.<br>• Batch edit opening hours of multiple stores: Check multiple stores of a site and click **Configure Opening Hours**. Adjust the opening hour and click **Save**. |

| Operations | Description |
| --- | --- |
| | **Note**<br>The opening hours of store(s) should be within one day. |
| Edit Configuration of Resource Capability and People Counting | After you add a store, click the store, and select **Resource Capability/Floor Configuration** to view and edit the resource status, people counting parameters, resources of floors, etc.<br>**Note**<br>For resources for people counting, supports configuring regular clearing time. |

### 20.1.2 Configure Promotion Day

After setting promotion days, you can get the customer traffic on promotion day so as to analyze how many customers the promotions bring more than the days without a promotion.

**Steps**

1. In the top left corner of Home page, select → **Operation Analytics** → **Intelligent Analysis** → **Store Management** → **Configure Promotion Day** .
2. Click **Add** to open the promotion day configuration page.

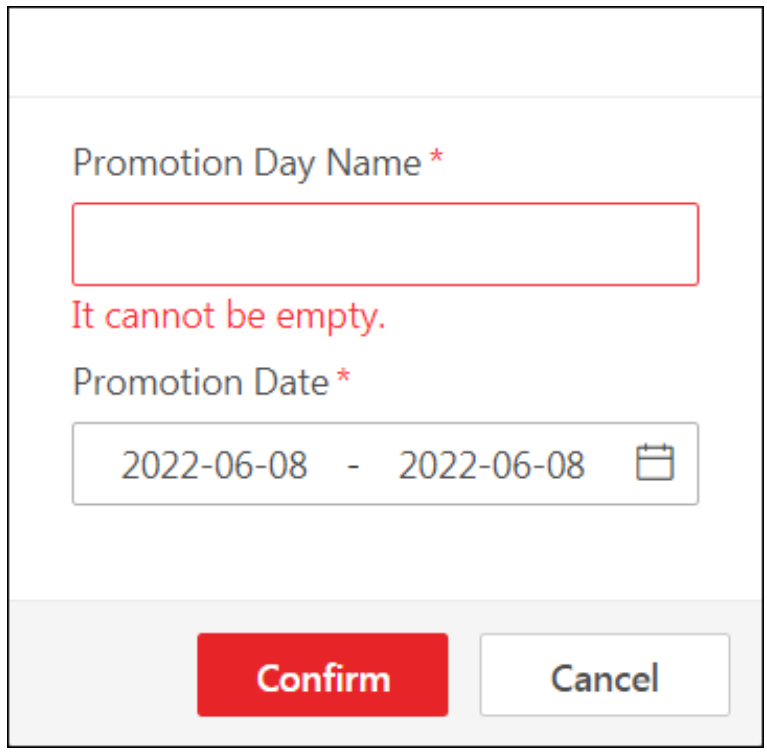



**Figure 20-3 Promotion Day Configuration**

3. Enter the promotion day name.
4. Set the promotion duration.

**Note**

The promotion time period should be within 30 days.

5. Click **Confirm** to finish adding a promotion day.
6. **Optional:** Perform the following operations after adding promotion days.

| | |
|---|---|
| **Edit a Promotion Day** | Click the promotion day name to open the promotion day configuration pane, and edit the promotion day information. |
| **Delete Promotion Days** | Check one or multiple promotion days, and click **Delete** to delete the selected promotion days. |
| **Search Promotion Days** | Enter a keyword in the search field to search for promotion days. |

### 20.1.3 View and Send Store Report

In the retail/supermarket scenario, you can view store reports of a single store, two stores, and multiple stores, and send regular reports to designated recipients as scheduled.

## View Store Report

- **Single Store Report**: View the daily and hourly trend of people counting (in), foot traffic (in + passby), walk-in rate, etc., and data collected from each floor and their rankings of a single store.

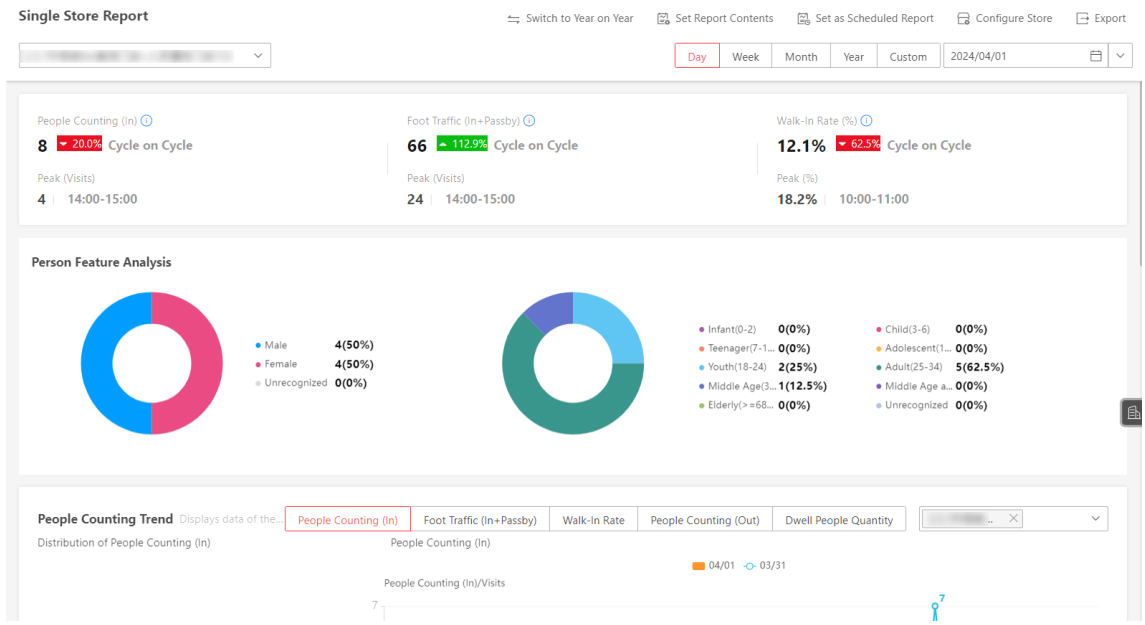



**Figure 20-4 Single Store Report**

- **Multiple-Store Reports**: View the daily and hourly trend of people counting (in), foot traffic (in + passby), walk-in rate, etc. of multiple stores.

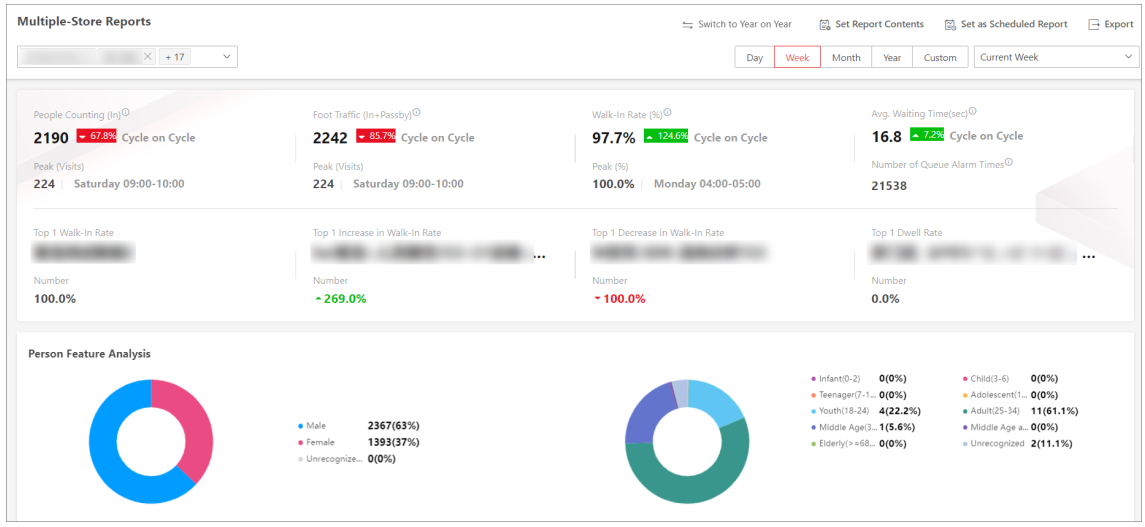



**Figure 20-5 Multiple-Store Reports**

- **Comparison Report**: View the differences of people counting (in), foot traffic (in + passby), walk-in rate, etc. between 2 specified stores.

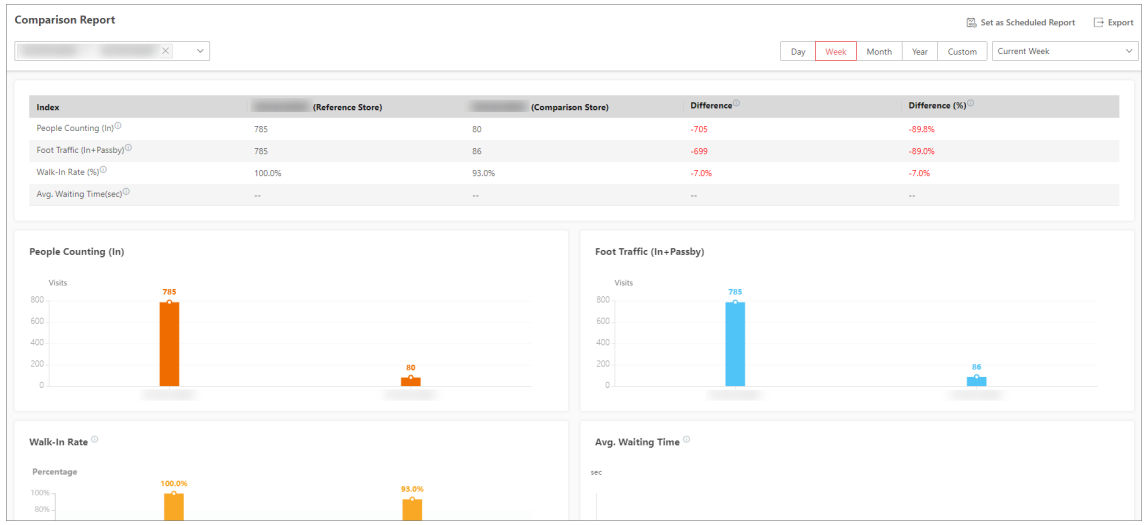



**Figure 20-6 Comparison Report**

- **Store Promotion Day Report**: View the report containing people counting, foot traffic, and walk-in rate on a promotion day, and get a direct view of people counting trend and rankings of different store(s).

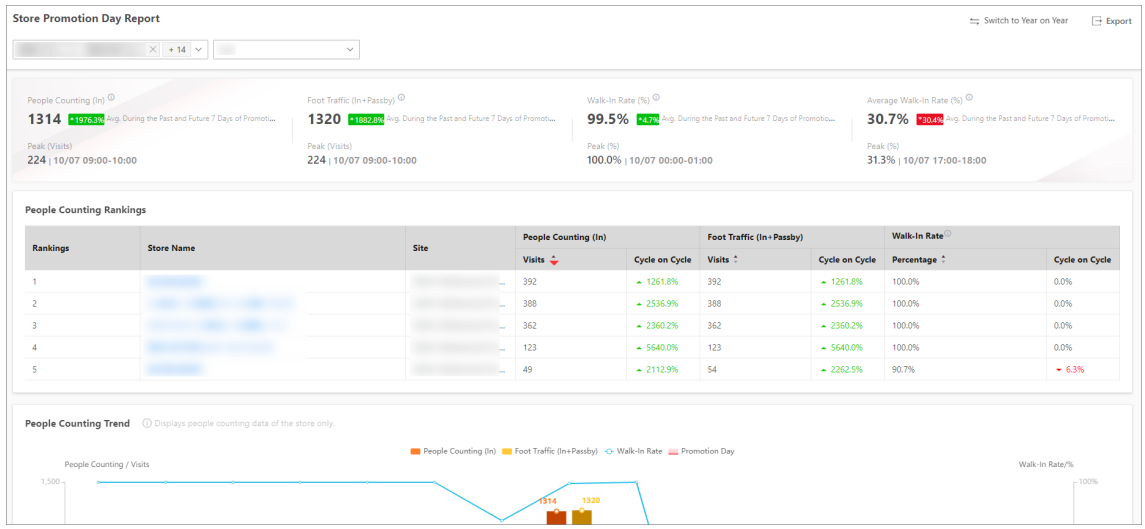



**Figure 20-7 Store Promotion Day Report**

See the example operations you can perform when viewing a single store report. Some specific parameter configurations may vary by report type.

1. In the Intelligent Analysis module, select **Store Report → Single Store Report** .
2.

| Operation | Description |
|---|---|
| Select Store | Click ⌄ to select a store. |
| Set Report Time | Click **Day/Week/Month/Year/Custom** to select the report time. |
| View Parameter Meaning | Hover your cursor over ⓘ on the top right corner of a certain parameter, and you will view the explanations of the parameter. |
| Switch Between Year on Year and Cycle on Cycle | Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways.<br>**Note**<br>For exporting reports, year on year statistics and cycle on cycle statistics will be both exported. |
| Set Report Contents | Click **Set Report Contents** to open the Set Report Contents pane.<br>- Switch on **Stick Statistics on Top**, and check the items so that they will be displayed on the top of the report.<br>- Switch on the other items such as person feature analysis so that you can view the selected reports of the store. |
| Configure Store | Click **Configure Store** to configure the store. For details, refer to ***Add a Single Store*** . |
| Set as Scheduled Report | Click **Set as Scheduled Report** to set the current report as a scheduled report.<br>For details, refer to ***Send Store Report Regularly*** . |
| Export Report | Check/uncheck **All** for **Statistics Target**. When it is checked, the report contents will be displayed. Check the items as needed and click **Export**. |

## Send Store Report Regularly

You can set scheduled reports to designated recipients.

1. In the Intelligent Analysis module, select **Store Management → Scheduled Report** .
2. Click **Add**/ + to open the Create Report panel.
3. Set basic information such as report name, report type, report language.
4. Set the report contents.

**Statistical Object**

Select the available stores as the report statistics targets.

**Note**

Up to 32 targets are supported in one report.

**Dwell Duration**

For example, if you set the dwell duration as > 15s, then when a person stays in an area for over 15 seconds, they will be considered as dwelling within the area.

**Queuing Duration**

For example, if you set it as Range 1 < 300 < Range 2 <600 < Range 3, then you can view reports about the number of queuing people who waited for less than 300 sec / from 300 to 600 sec / more than 600 sec.

**Number of Queuing People**

For example, if you set it as Range 1 < 5 < Range 2 <10 < Range 3, then you can view reports about the distribution of queues whose number of people are less than 5 / from 5 to 10 / more than 10.

5. Set time settings which define how often and when the report will be sent to the recipient. For example, if you select By Week, Recent 7 Days, and Send at Sunday 06:00, then the recent 7 days store report will be sent to you weekly at every Sunday 6:00.
6. In the Advanced Settings section, perform the following operations as you need.
   a. Switch on **Send via Email**, and select the email template from the drop-down list to define the recipient information and email format.

   **Note**

   You can click **Add** to add a new email template.

   b. Switch on **Upload to SFTP**, and click **Configure** beside **Saving Path** to configure the SFTP settings, including SFTP address, port number, user name, password, and saving path.

   **Note**

   If you have configured the SFTP settings, you can click → **Configure SFTP** in the top left corner to edit SFTP settings. For details, refer to the table below.

   c. Switch on **Save to Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

   **Note**

   If you have configured the local storage, you can click → **Configure Local Storage** in the top left corner to edit the saving path of local storage. For details, refer to the table below.
7. Click **Add**. On the left pane, you can see all scheduled reports you added. You can perform the following operations.

| Operation | Description |
| --- | --- |
| Edit Report | Click the name of a certain report, and you can edit the report. |
| Delete Report | Select a store, and click in the top left corner to delete the store. |
| Configure SFTP / Local Storage | Click in the top left corner to configure SFTP or Local Storage.<br>- Click **SFTP Settings** to configure the SFTP settings, including SFTP address, port number, user name, password, and saving path.<br>- Click **Configure Local Storage** to set the local saving path. |

### 20.1.4 View Store Intelligent Analysis Report

In the retail/supermarket scenario, to view intelligent analysis reports including people counting analysis, person feature, heat analysis, pathway analysis, and queue analysis, you should configure store(s) and add them to the platform in advance.

- **Store People Counting Report**: You can generate a people counting report which displays the period over period data and trend of people counting statistics to have a direct view of people entering, exiting, passing by, and walk-in rate. You can also export the report to the local PC.

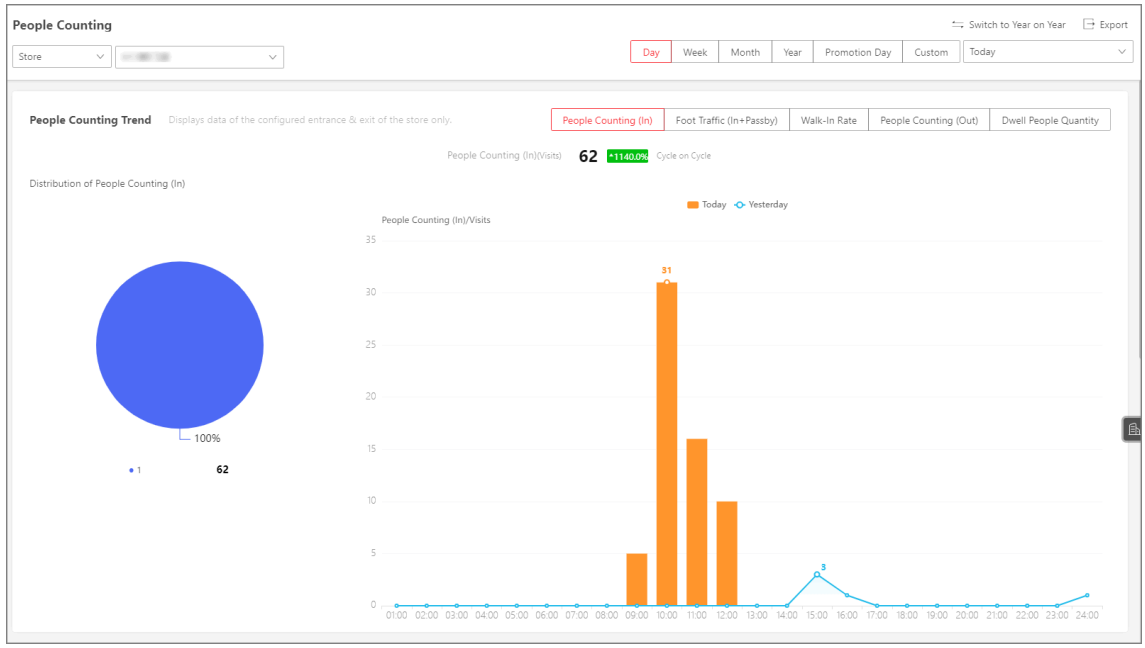



**Figure 20-8 Store People Counting Report**

- **Store Person Feature Analysis Report**: The platform supports saving features of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different features in different time period. It can be used in places such as shopping mall to analyze interests of people in different features.

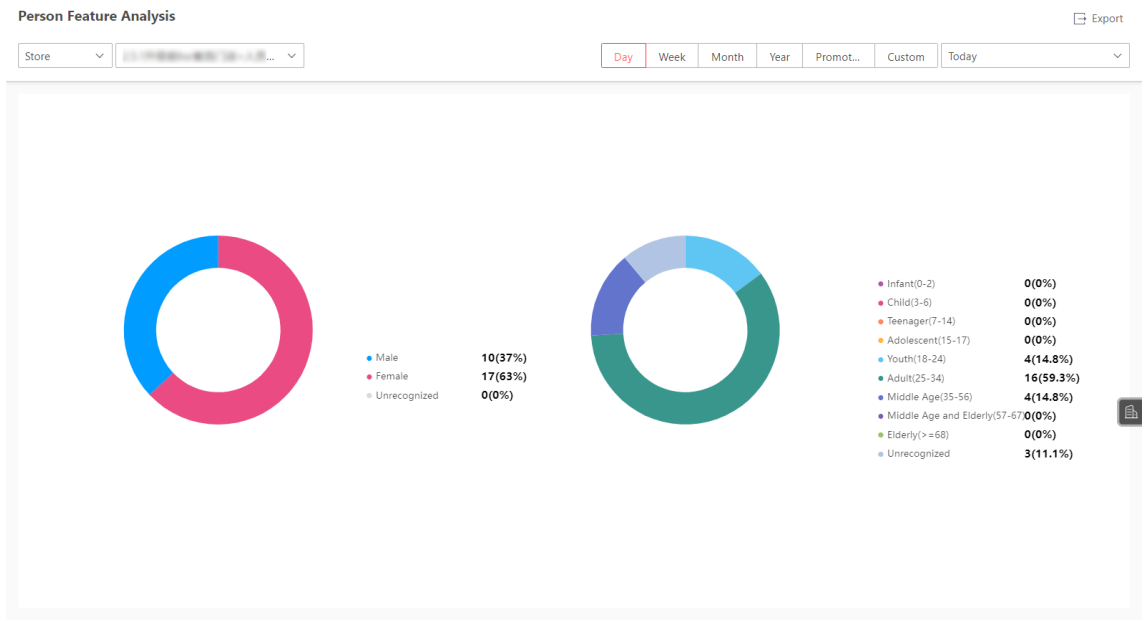



**Figure 20-9 Store Person Feature Analysis Report**

- **Store Heat Analysis Report**: You can generate a heat analysis report to show consumer movements, the visit times, and dwell time in a configured area.

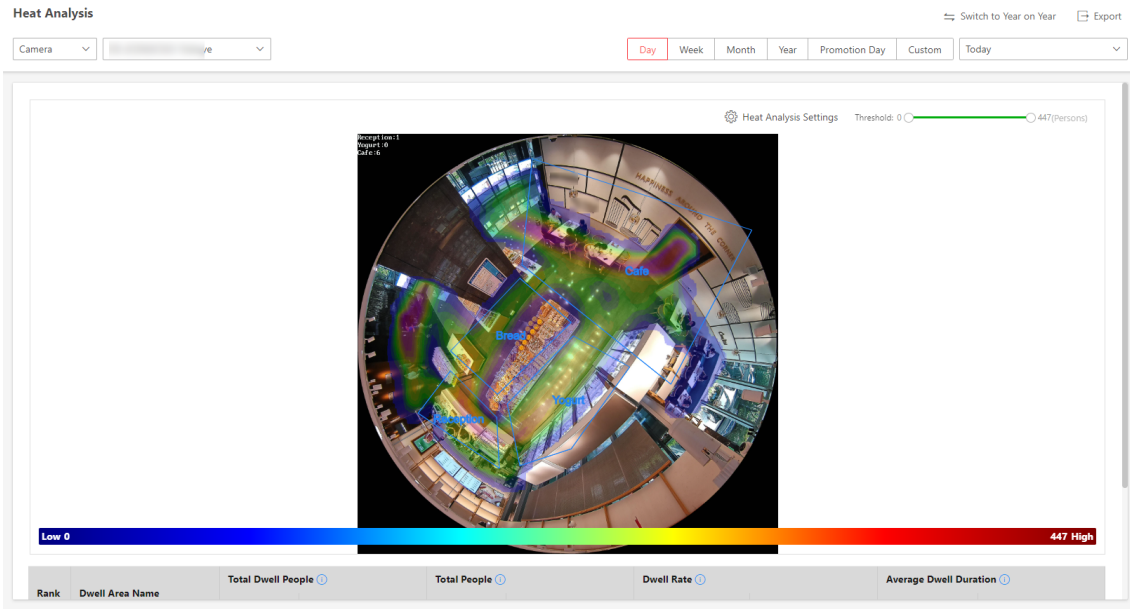



**Figure 20-10 Store Heat Analysis Report**

**Note**

- Make sure you have added a heat map network camera to the platform and properly configure the camera with heat map rule for the required area. To add a heat map network camera, please refer to the *User Manual of HikCentral Professional Web Client*. To configure the heat map rule, please refer to the user manual of heat map network camera.
- Make sure you have added the camera to a static map. For details about how to add a camera to the static map, refer to *User Manual of HikCentral Professional Web Client*.

- **Store Pathway Analysis Report**: Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the platform can collect the consumers data (for example, where the customers walk mostly). This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the platform calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

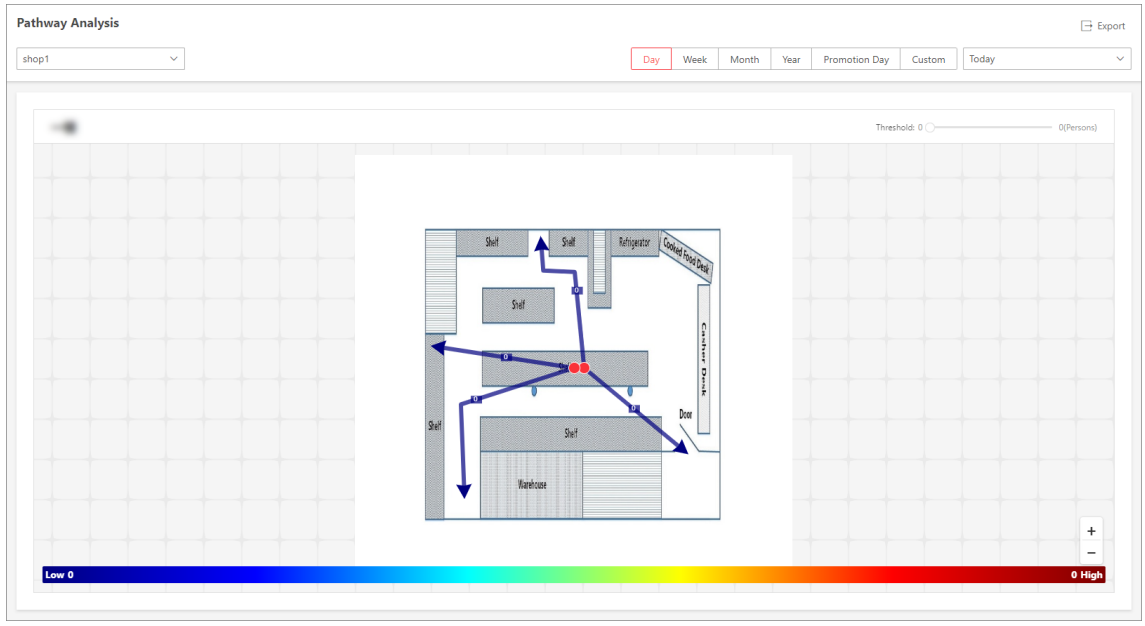



**Figure 20-11 Store Pathway Analysis Report**

**Note**

- Make sure you have properly added the camera to a static map and set its pathways on the map via the Web Client first. For details about adding camera to map and set pathways, refer to the *User Manual of HikCentral Professional Web Client*.
- You should have added pathway analysis groups. For details, see ***Add Analysis Group*** .

- **Store Queue Analysis Report**: For cameras which support queue management, you can generate a report to show the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length.

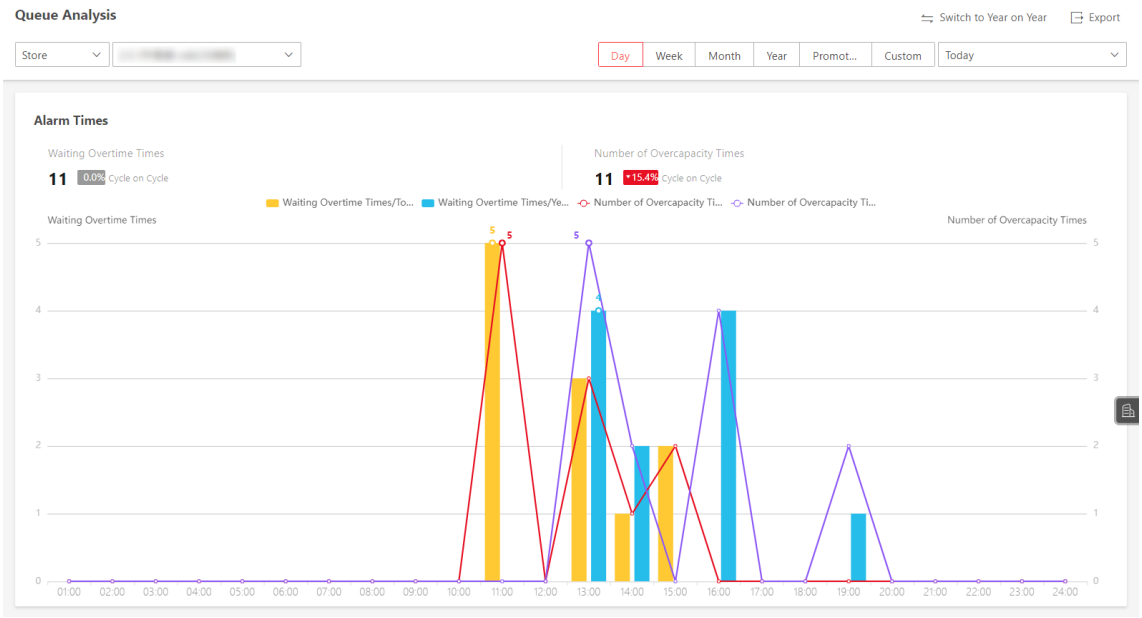



**Figure 20-12 Store Queue Analysis Report**

**Note**

Make sure you have added a camera which supports queue management to the system and configure queue regions. To configure the queue region, refer to user manual of the camera.

See the example process of viewing a heat analysis report. Some specific parameter configurations may vary by reports.

1. Under the Intelligent Analysis module, select **Analysis Center → Heat Analysis** .
2. Select a store/camera to search for queue data. A queue analysis report of the selected camera/ store will be displayed.
3. (Optional) Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, **Promotion Day**, or **Custom**.

   **Daily Report**

   Daily report shows data on a daily basis. The system will calculate the queue data detected 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 platform will calculate the number of people or people dwell time in each day of way week, in each day of one month, and in each month of one year.

   **Promotion Day**

   Promotion day report shows data on a promotion day basis. The platform will send one report at the sending time on a promotion day, which contains analysis results on the day.

**Note**

For details of configuring a promotion day, refer to ***Configure Promotion Day*** .

**Custom Time Interval**

Users can customize the days in the report to analyze the number of people or people dwell time in each day or month of the custom time interval.

4. (Optional) Set the time or time period for statistics.

**Note**

For custom time interval report, you need to set the start time and end time to specify the time period.

5. (Optional) Perform the following operation(s).

| Operation | Description |
|---|---|
| Set Heat Analysis Parameters | a. Click **Heat Analysis Settings**.<br>b. Set the **Dwell Duration** to get statistics within the configured range.<br>**Note**<br>For example, if you set the dwell duration as > 15s, then when a person stays in an area for over 15 seconds, they will be considered as dwelling within the area.<br>c. Select the **Meaning of Heat Color**, including total people and dwell time.<br>d. Check **Show** or **Hide** the divided heat areas.<br>e. Click **Save**.<br>f. Drag the threshold slider in the upper-right corner to adjust the range of the statistical dimension. The heat data out of the range will not be displayed. |
| Switch Between Year on Year and Cycle on Cycle | Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. |

| Operation | Description |
| --- | --- |
| | **Note**<br>For exporting reports, year on year statistics and cycle on cycle statistics will be both exported. |
| Export Report | a. Click **Export**.<br>b. Set the format of the exported file as Excel, CSV, or PDF.<br>c. Select the time dimension as **By Hour**, **By Day**, or **By Month**.<br>d. Click **Export**.<br>**Note**<br>You can get the exported report in the Download Center. |

## 20.1.5 View Store Report Dashboard

The report dashboard provides an at-a-glance view for stores. You can select a store or multiple stores to view reports.

1. Under the Intelligent Analysis module, select **Dashboard**.

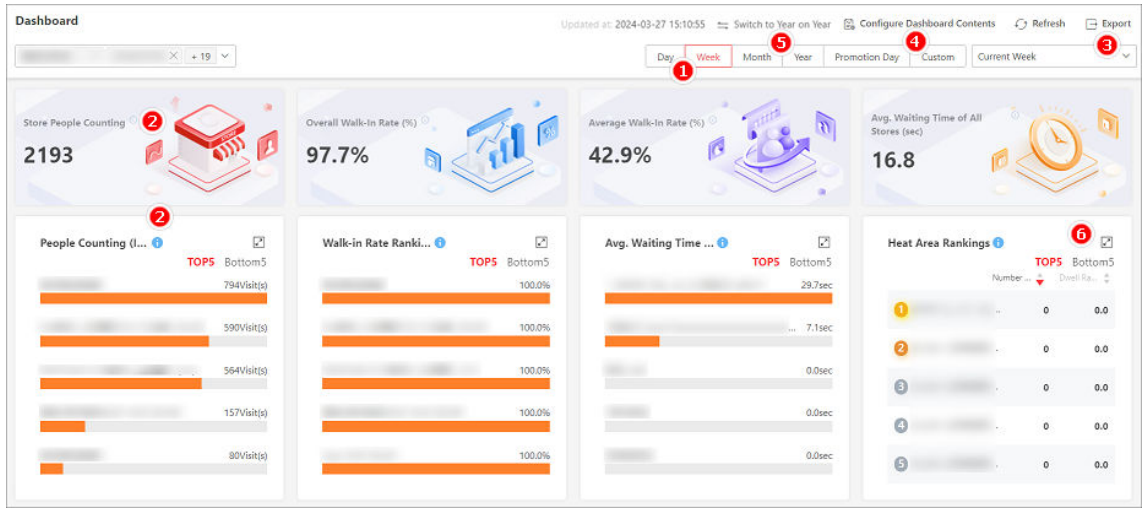



**Figure 20-13 Dashboard**

2. Select a store or multiple stores, and you can perform the following operations.

| Operation | Description |
|---|---|
| ①Set Report Time | Click **Day**, **Week**, **Month**, **Year**, **Promotion Day** or **Custom** to select the report time. |
| ②View Dashboard/Report Meaning | Hover your cursor over or on the top right corner of a certain parameter, and you will see the explanations of the dashboard/report. |
| ③Export Dashboard | Click **Export** to export the dashboard in PDF format to the local PC.<br>**Note**<br>You can get the exported report in the Download Center. |
| ④Configure Dashboard Contents | Click **Configure Dashboard Contents** to select dashboard/report contents to be displayed. |
| ⑤Switch Between Year on Year and Cycle on Cycle | Click **Switch to Cycle on Cycle** or **Switch to Year on Year** for switching the report statistics mode. |
| ⑥Zoom in Dashboard/Report | Click to zoom in the dashboard or report. |

## 20.2 Public Scenario

The Public Scenario is designed for public situations such as stations and hospitals. You can view reports such as people counting and heat analysis reports.

### Flow Chart of Intelligent Analysis Report in Public Scenario

The following flow chart shows the process of configurations and operations required for intelligent analysis reports in public scenario.

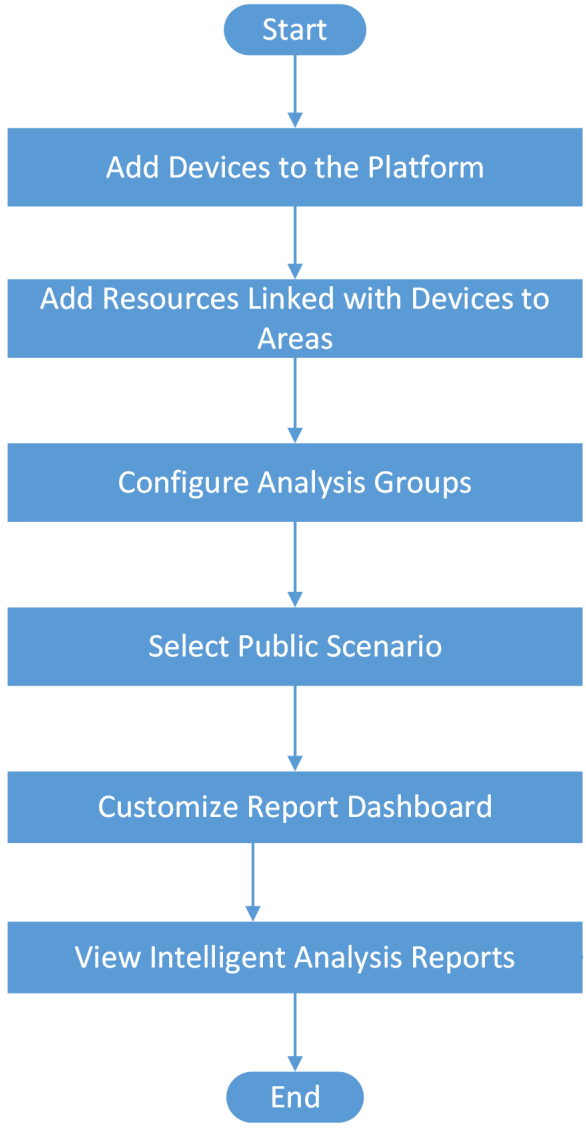



**Figure 20-14 Flow Chart of Intelligent Analysis Report in Public Scenario**

**Note**

To check the resource status, go to **Analysis Group → Troubleshooting** . For resources for people counting, supports viewing uploaded real-time data (reported number of people in last hour) and configuring regular clearing time.

### 20.2.1 Add Analysis Group

Before generating people counting report, you can add people counting group before the report; before generating heat analysis report, person feature analysis report, and pathway analysis report, you can add the corresponding analysis groups.

**People Counting Group**: The people counting group is used to group the doors, people counting cameras, queue management cameras, and fisheye cameras of certain region. You can set some doors and cameras as the region edge. Only the persons accessing these doors or detected by the cameras are calculated, and other doors and cameras outside the region are ignored. By grouping these doors and cameras, the platform provides counting functions based on the detected records on these doors and cameras.

**Heat Analysis Group**: The heat analysis group is used to group the resources (such as doors, fisheye cameras, people counting cameras) in certain region. By grouping these resources, you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people. This function is mainly used to calculate and show the popularity of each stores in one shopping mall.

**Person Feature Analysis Group**: Person feature analysis is a group of cameras which support face recognition and feature analysis. You can group the cameras in one region into one group. After that, when generating a report, you can view the features of the persons appeared in this region, based on the data detected by the cameras in the group. For example, if there are five cameras which support facial recognition mounted in the store, the store manager can add these five cameras into one group. Then you can view features of the customers who entering the store in the Intelligent Analysis module.

**Pathway Analysis Group**: Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the system calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

**Note**

Adding analysis groups is not supported by queue analysis report, people density analysis report, temperature analysis report, and multi-target-type analysis report.

The process of adding analysis groups for these reports can be generally divided into 3 sections: basic configuration, adding analysis resource, adding analysis group to map. Some specific parameter configurations may vary by reports.

See the example process of adding person feature analysis group.

1. Under the Intelligent Analysis module, select **Analysis Group → Person Feature Analysis Group** .
2. Click **Add**.

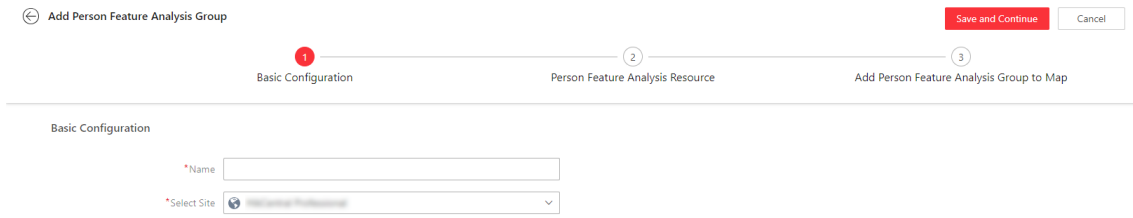



**Figure 20-15 Add Analysis Group (Person Feature Analysis Group)**

3. Set basic configurations such as name and site, and click **Save and Continue**. Click **Save and Continue**.
4. Configure resources for analyzing the detected persons' features.
   a. In the **Person Feature Analysis Resource** part, click **Add** to select the resources.
   b. Click **Save**.
   c. (Optional) Click **Remote Configuration** to go to Remote Configuration page of the device.
   d. Click **Save and Continue**.
5. (Optional) Locate the person feature analysis group on the map by setting the locations of the cameras in the group and setting the edge of the region for detection.
   a. Drag the person feature analysis group from the Resource Group list on the right to the map. The region as well as the cameras in the group will be added on the map.
   b. Drag to draw the region according to the actual needs.
   c. Drag the icons of the cameras to set the their locations on the map.
   d. Right click to finish.
   e. (Optional) Check **Only Display the Current Group** to only display the added analysis group on the map.
6. Click **Finish**. After adding the person feature analysis group on the map, you can view the features of the persons appeared on the Control Client.

## 20.2.2 Generate and View Analysis Report

Generate and view people counting reports, heat analysis reports, person feature analysis reports, queue analysis reports, pathway analysis reports, people density reports, temperature analysis reports, and multi-target-type analysis reports. For people counting report, heat analysis report, pathway analysis report, and person feature analysis report, make sure you have added the corresponding analysis groups. After that, you can set a regular report rule for the specified analysis groups/cameras, and the system will send emails with the reports attached to the target recipients daily, weekly, or monthly. You can also manually generate an analysis report at any time to view the data if required.

## People Counting Report

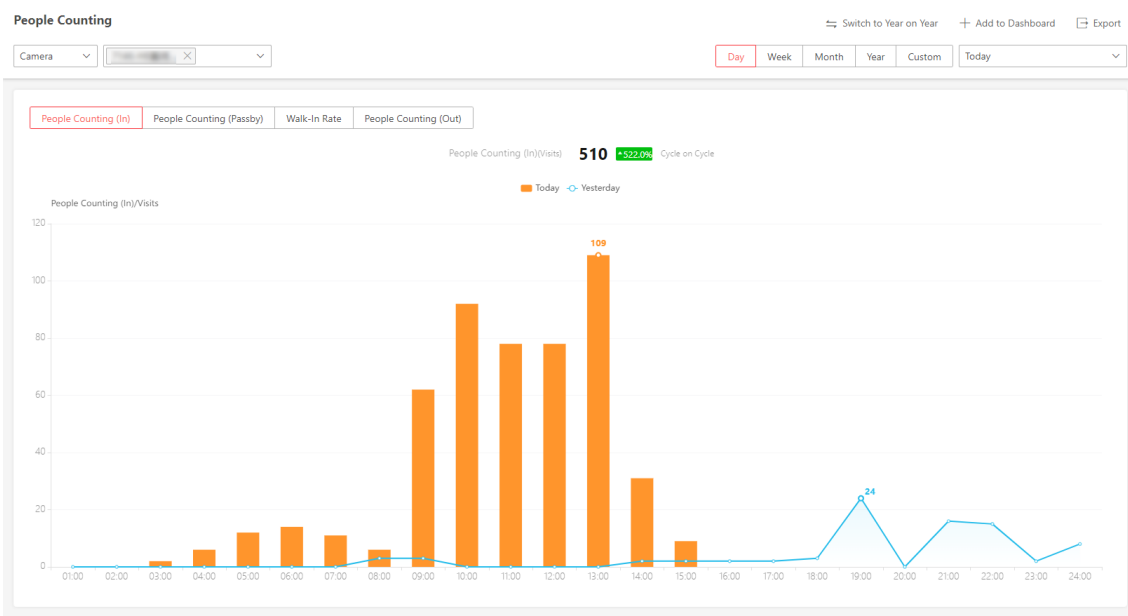



**Figure 20-16 People Counting Report**

People counting report shows the number of line crossing people counted by people counting cameras or obtained from access records of access control devices in a specific region and within a certain time period. The report lets you know the number of persons who stay in a specific region, which can be used for certain commercial or emergency scenarios. For example, for emergency scenario, during a fire escape, the number of stayed persons will be displayed on the map which is required for rescue. For commercial scenario, the shopping mall manager can get the people counting report to know whether the store is attractive and get the number of people entering each stores to determine whether to limit the number of customers staying in the mall for security reasons during the peak time. You can also generate a people counting report for a single store or multiple stores.

**Note**

Before generating a people counting report, you should add people counting group(s) to group the doors and people counting cameras of a certain region so as to define region edge.

## Heat Analysis Report

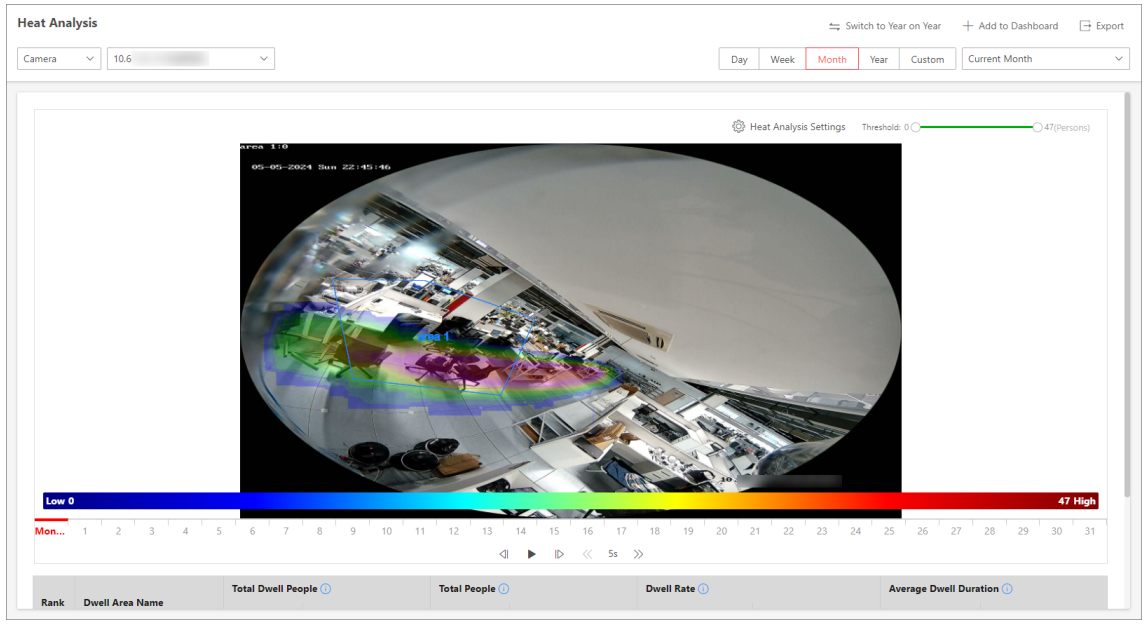



**Figure 20-17 Heat Analysis Report**

Heat analysis report shows data with a heat map, which is a graphical representation of data represented by colors. The heat map function of the camera is usually used to track the consumers movements (where the customers walk, and what items they stop to touch and pick up) and analyze the visit times and dwell time in a configured area. This report is mainly used for store managers or retailers to see which part of the store got the most attention from consumers and which got least. Knowing where customers move is useful for retailers. They can optimize store layouts, for example, where to place popular and unpopular goods.

**Note**

Before you begin:

- Make sure you have added a heat map network camera to the platform and properly configure the camera with heat map rule for the required area. To configure the heat map rule, please refer to the user manual of heat map network camera.
- Make sure you have added the camera to a static map.
- Make sure you have added a heat analysis group to define the region for heat analysis.

## Person Feature Analysis Report

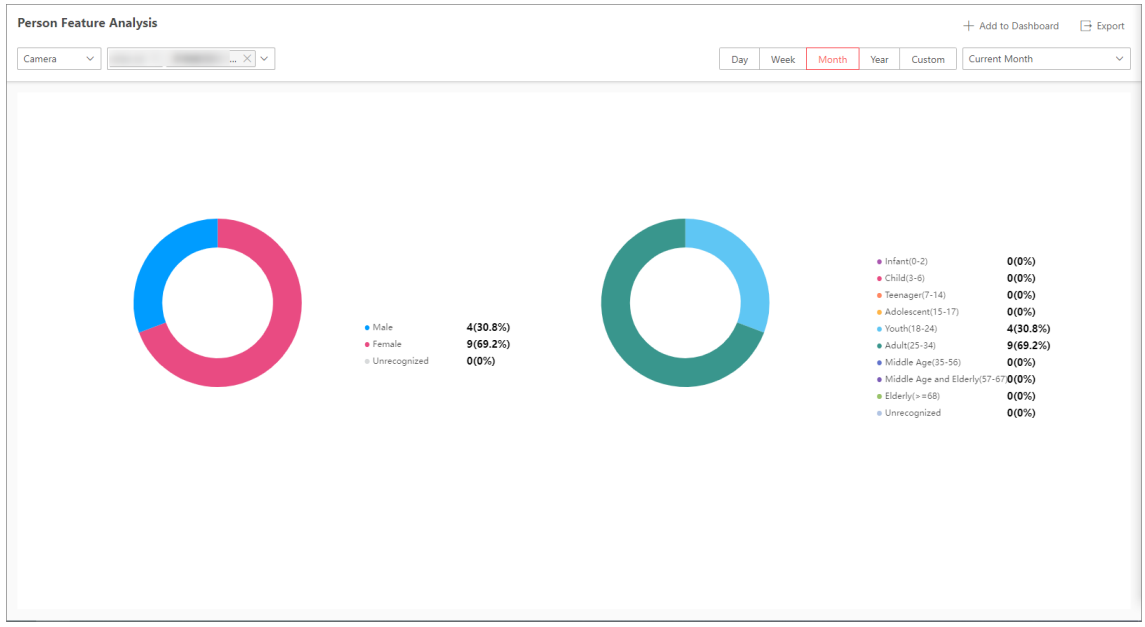



**Figure 20-18 Person Feature Analysis Report**

The platform supports saving features of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different features detected by cameras in different time period. It can be used in places such as shopping mall to analyze interests of people in different features.

**Note**

You should add a person feature analysis group ( ***Add Analysis Group*** ) before generating a report to define the region for person feature analysis by grouping the cameras which support facial recognition and feature analysis.

## Queue Analysis Report

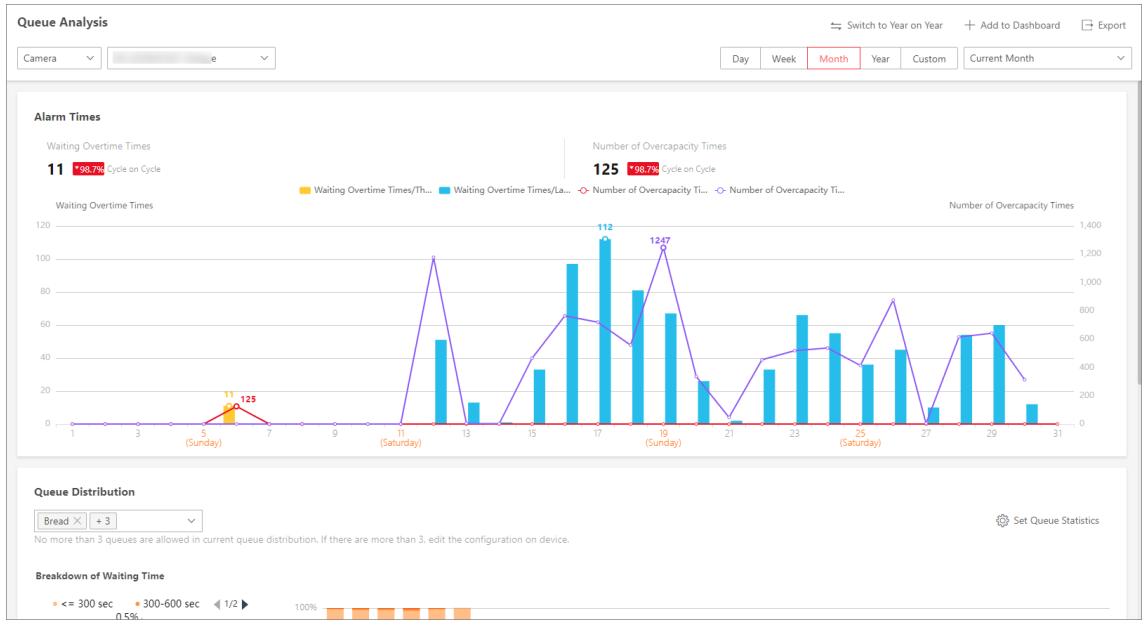



**Figure 20-19 Queue Analysis Report**

Queue analysis report shows the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length. It is helpful for allocating resources for retailers.

**Note**

Before you begin, make sure you have added a camera which supports queue management to the system and configure queue regions. To configure the queue region, refer to user manual of the camera.

## Pathway Analysis Report




**Figure 20-20 Pathway Analysis Report**

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the platform calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

**Note**

Before you begin:

- Make sure you have properly added the camera to a static map and set its pathways on the map via the Web Client first. For details about adding camera to map and set pathways, refer to the *User Manual of HikCentral Professional Web Client*.
- Before you begin, make sure you have added pathway analysis groups. For details, see ***Add Analysis Group*** .

## People Density Analysis Report

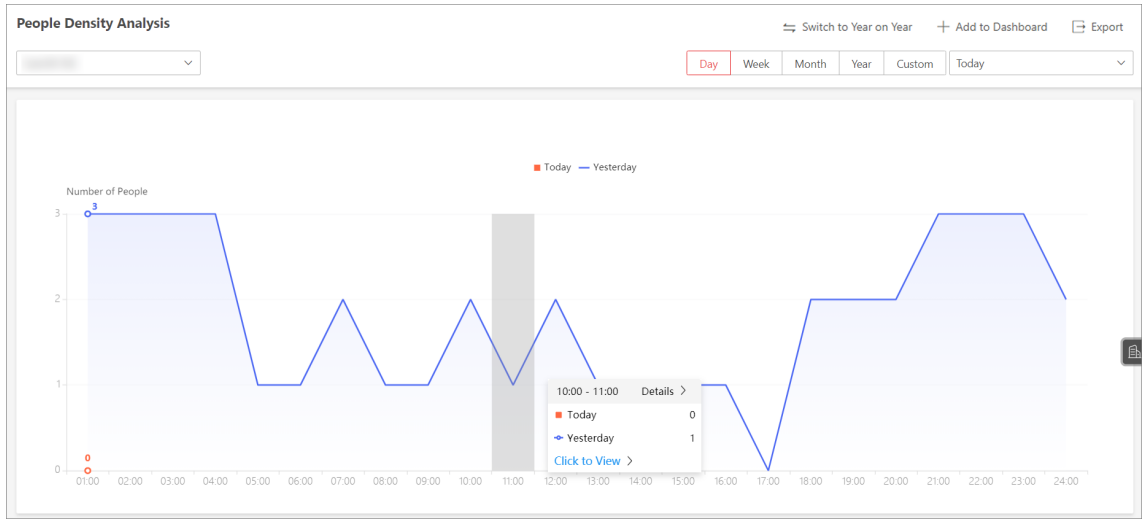



**Figure 20-21 People Density Analysis Report**

People density analysis report shows the variation trend of the people density data in line chart. The people density data refers to the peak amount of people appeared in the images of a specific camera during a certain time period. The data is useful for the management and control of the amount of people in specific areas or space during special time periods. For example, assume that you were a manager of a shopping mall during epidemic outbreak, you could generate a people density analysis report to find out the time period(s) during which excessive people density usually occurs in the shopping mall, and then arrange in advance the personnel and related works accordingly to limit people gathering at those time periods to prevent the spread of the infectious disease.

**Note**

- Before you begin, make sure you have purchased the License that supports people density analysis, or the function will be unavailable.
- Before you begin, make sure you have added the abnormal event detection server to the HikCentral Professional and linked cameras to the server.
- Before you begin, make sure you have configured people density analysis on the abnormal event detection server. For details, see the user manual of the server.

## Temperature Analysis Report

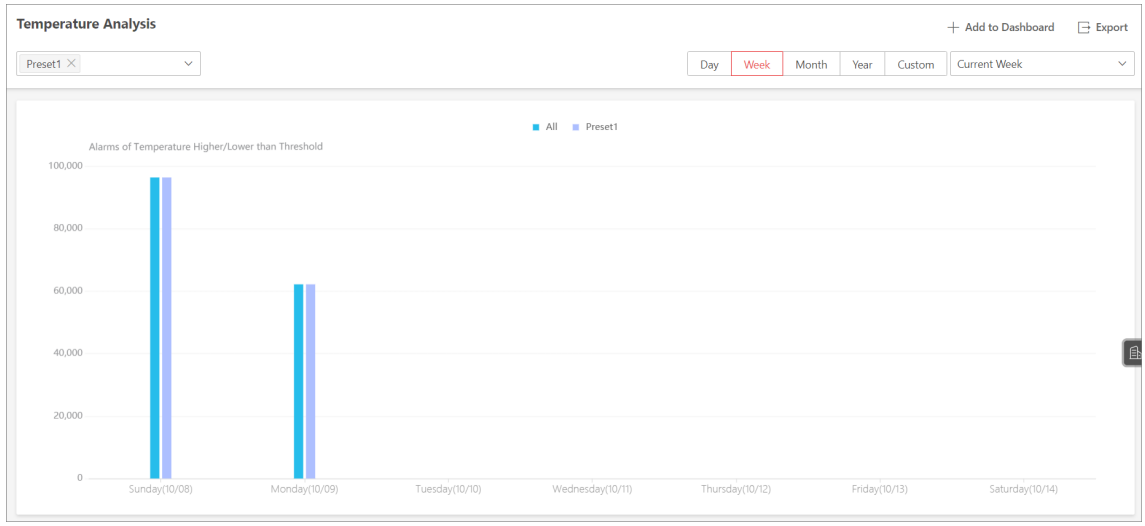



**Figure 20-22 Temperature Analysis Report**

The temperature analysis report shows the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets.

## Multi-Target-Type Analysis Report

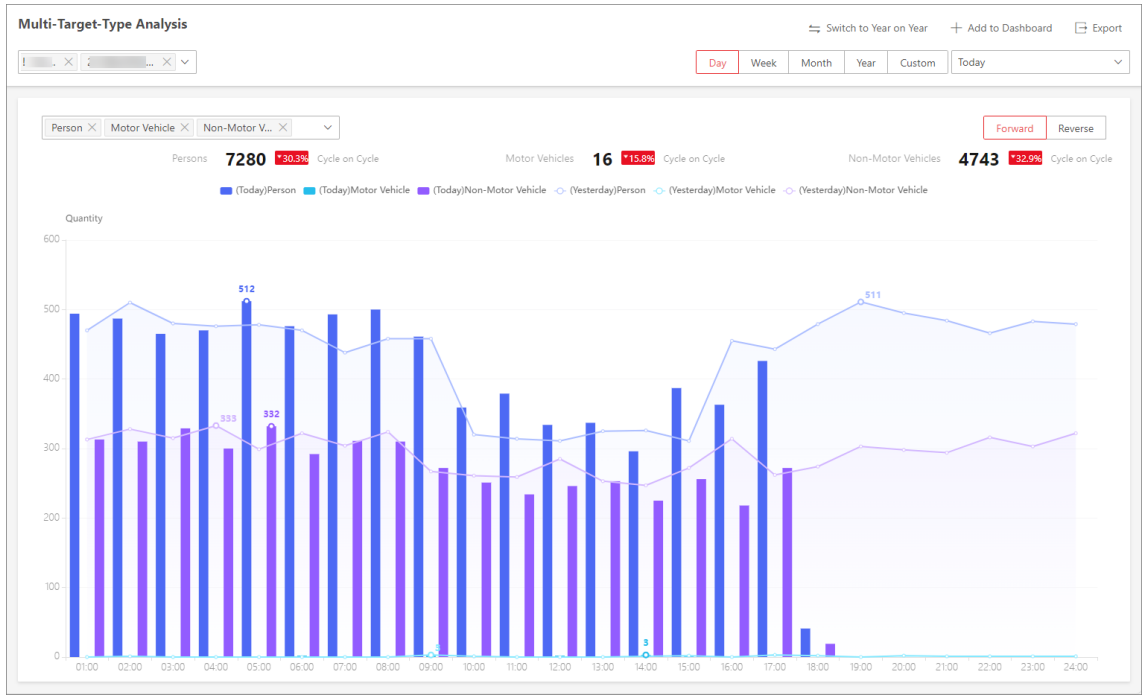



**Figure 20-23 Multi-Target-Type Analysis Report**

The multi-target-type analysis report shows the number of persons, motor vehicles, and non-motor vehicles within a specified period. You can set a regular report rule for the specified cameras and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a analysis report at any time to view the data if required.

## Generate Analysis Report

The process of generating these reports can be generally divided into 4 sections: selecting report data resource, setting statistical cycle, setting the time or time period for statistics, and perform subsequent operations on the report as needed. Some specific parameter configurations may vary by reports.

See the example process of generating a people counting report.

1. Under the Intelligent Analysis module, select **Analysis Center → People Counting** .
2. Select the report data resource type.

   **Camera**

   A people counting report based on the data from the cameras you select will be generated. You can compare the data of different cameras.

   **Analysis Group**

   A people counting report based on the data from the people counting groups you select will be generated. You can compare the data of different groups.

   **Note**

   Make sure you have added people counting groups. See ***Add Analysis Group*** for details.
3. Select people counting camera(s) or people counting group(s) based on the data resource type you set in the previous step.

   **Note**

   Up to 20 cameras/groups can be selected.

   The corresponding report of selected camera(s)/group(s) will be displayed.

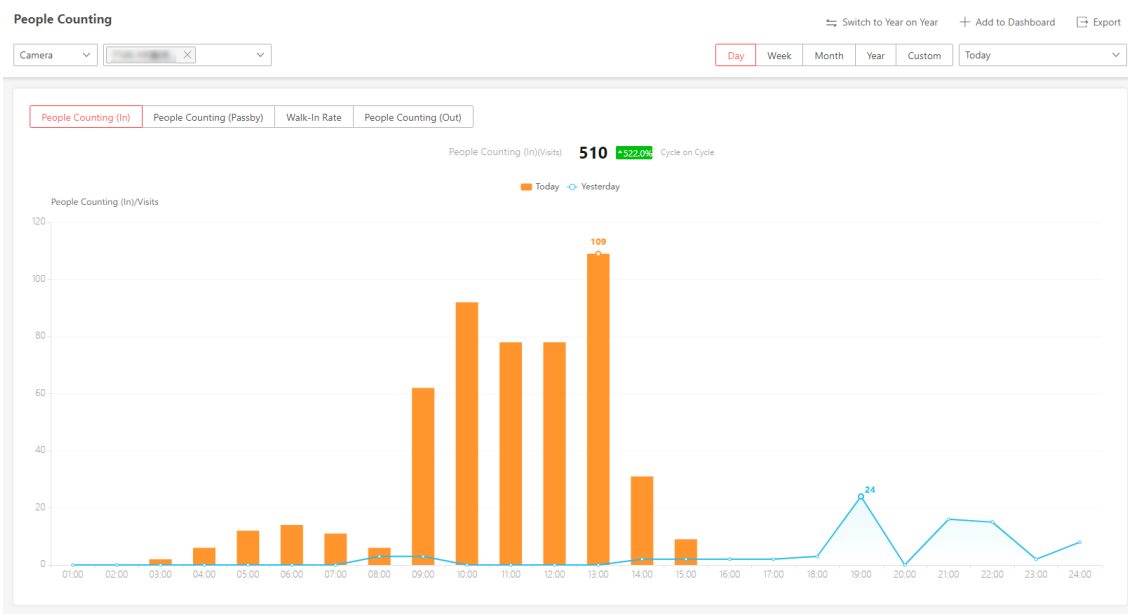



**Figure 20-24 People Counting Report**

4. Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.

   **Daily Report**

   Daily report shows data on a daily basis. The platform will display the people counting data detected in each hour of two adjacent days.

   **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 platform will display the people counting data detected in each day of two adjacent weeks, in each day of two adjacent months, and in each month of two adjacent years.

5. Select a pre-defined time period or customize a time period for statistics.

   **Note**

   For custom time interval report, you need to set the start time and end time to specify the time period.

6. Perform the following operation(s) after generating the people counting report.

| Operation | Description |
|---|---|
| Switch Between Year on Year and Cycle on Cycle | Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. |

| Operation | Description |
|---|---|
| | **Note**<br>For exporting reports, year on year statistics and cycle on cycle statistics will be both exported. |
| Add to Dashboard | a. Click **Add to Dashboard** in the upper-right corner of the page.<br>b. Create a report name.<br>c. Select a dashboard. Or click **New** to create a new board and then select it.<br>d. Click **OK** or **Add and Go to Dashboard**. |
| Export Report | a. Click **Export**.<br>b. Check/uncheck **All** for **Statistics Target**. When it is checked, only Excel will be available for file type in the next step.<br>**Note**<br>This option is only available for people counting analysis report.<br>c. Set the format of the exported file as Excel, CSV, or PDF.<br>d. Select the time dimension as **By Hour**, **By Day**, or **By Month**.<br>e. Click **Export**. |

### 20.2.3 View Report Dashboard

The report dashboard provides an at-a-glance view for the public scenario reports. There are people counting reports, heat analysis reports, vehicle analysis reports, queue analysis reports, etc. You can customize the report dashboard as required.

1. Under the Intelligent Analysis module, select **Dashboard**.
2. On the top left corner, click ∨ → **Add Dashboard** on the report dashboard page and create a name to add a new dashboard. You can view the added dashboard by clicking ∨ to expand the list of added dashboard(s).

**Note**

- You can add up to 100 dashboards.
- The new dashboard appears and it is by default named as "Dashboard + The Time When It was Added" by default. For example, in "Dashboard20190916102436", "2019" represents year, "09" month, "16" date, "10" hour, "24" minute, and "26" second.

3. (Optional) You can perform the following operations.

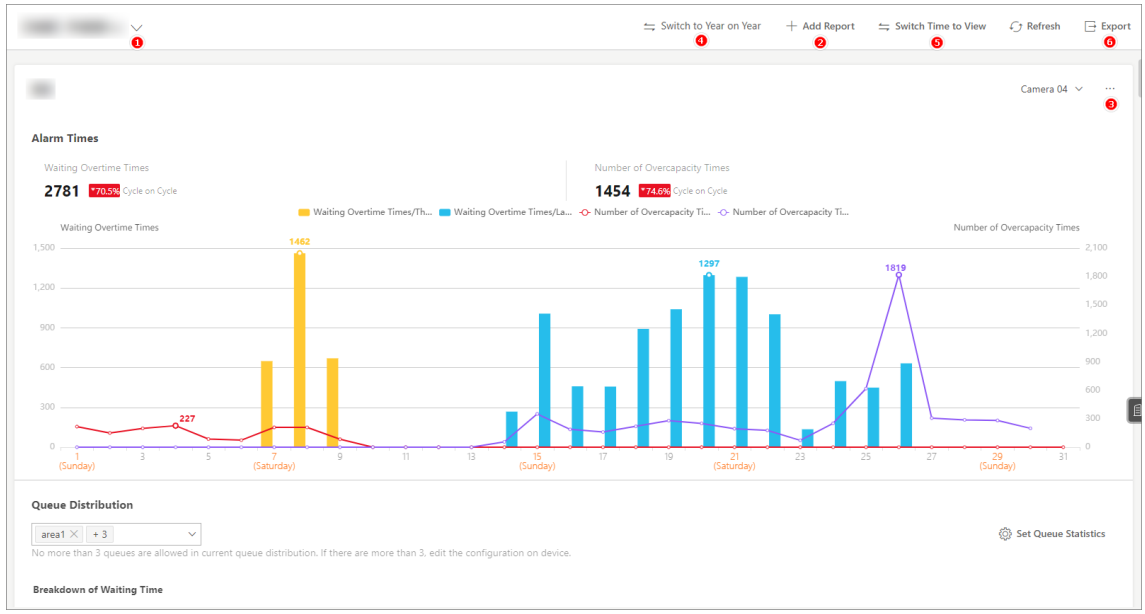



**Figure 20-25 Dashboard**

| Number | Operation | Description |
|---|---|---|
| ① | Edit Dashboard Name | On the top left corner, click ⌄ . Click ✎ to edit the dashboard name. |
| | Delete Dashboard | On the top left corner, click ⌄ . Click 🗑 to delete the dashboard. |
| ② | Add Report to Dashboard | a. After you select a dashboard, click **Add Report**, select a report type, and click **Next**.<br>b. Set the report name, analysis type, report type, and time.<br>**Note**<br>- If you select analysis for one camera, you need to select the camera already added to the platform.<br>- If you select analysis in one region, you need to select the analysis group already added to the platform. |

| Number | Operation | Description |
|---|---|---|
| | | c. Click **Add** to add the report to dashboard. The report will appear on the selected dashboard.<br>d. Click **Add Report** to add more reports to the dashboard as needed. |
| ③ | Edit Report Name | On the top right corner of a report, click ··· and then click **Edit**. |
| | Delete Report from Dashboard | On the top right corner of a report, click ··· and then click **Delete**. |
| ④ | Switch Between Year on Year and Cycle on Cycle | Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. |
| ⑤ | Switch Time to View Report Data | Select a dashboard and then click **Switch Time to View** to set the report type and time.<br>**Report Type**<br>Select the time basis for the reports. For example, daily report shows data on a daily basis.<br>**Time**<br>Set the specific time for generating the reports. For example, if you select **Custom Time Interval** as the report type, you can click 🗓 to specify a time interval for generating report data.<br>Click **Save** to change the default time basis of all the reports in the dashboard to the time you set in the previous sub step. |
| ⑥ | Export report | Export report(s) on the dashboard to the local PC. |

## 20.2.4 Send Analysis Report Regularly

You can set a regular report rule for specified analysis resources or targets, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the corresponding analysis data during the specified time periods. You can regularly send people counting reports, heat analysis reports, person feature analysis reports, queue analysis reports, pathway analysis reports, people density reports, temperature analysis reports, and multi-target-type analysis reports.

**Note**

- Set the email template with recipient information, subject, and content, and set the email settings such as sender address, SMTP server address and port. For details, refer to ***Email Settings*** .
- The report will be an Excel file.

The process of setting the report sending schedule be generally divided into 4 sections: setting basic information of the report, setting report content, setting the time-related information for statistics, and advanced parameters. Some specific parameter configurations may vary by reports. See the example process of generating a heat analysis report.

1. Under the Intelligent Analysis module, select **Analysis Group → Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.

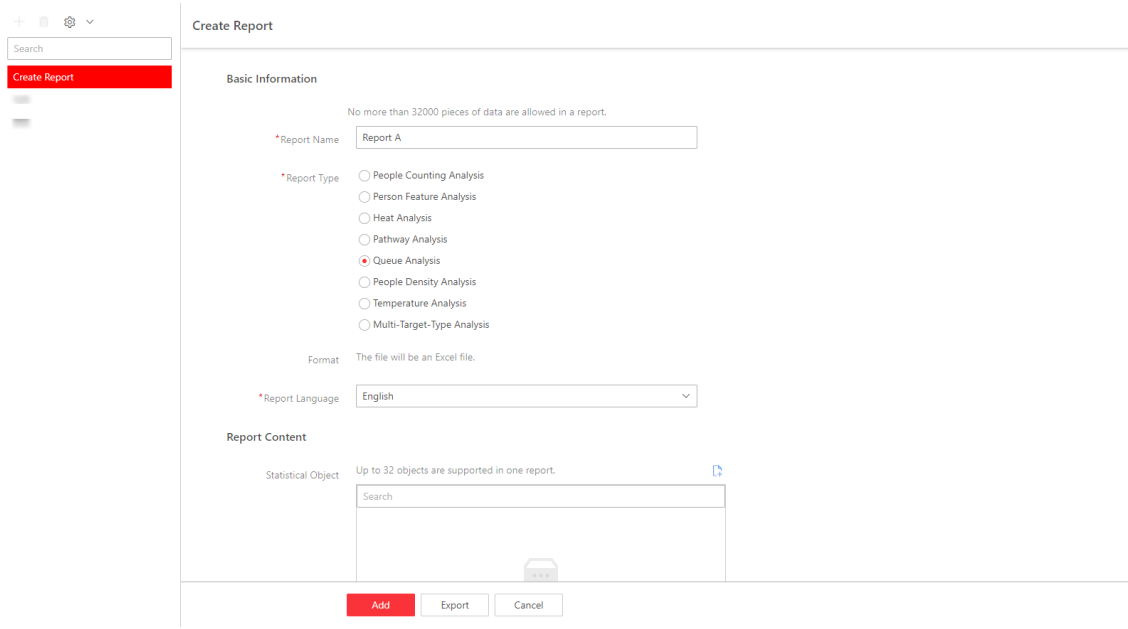



**Figure 20-26 Send Analysis Report Regularly (Heat Analysis)**

3. Create a name for the report.
4. Select the report category as **Heat Analysis**.
5. Select a language as **Report Language**.

**Note**

By default, the language is the same with the selected language when you log in on the Web Client.

6. Select heat analysis type.

**Heat Analysis for One Camera**

Analyze people dwell time and number of people detected by the specified camera(s).

**Heat Analysis in One Region**

Analyze people dwell time and number of people detected by the cameras in the specified heat analysis group(s).

**Note**

For details about adding heat analysis group, see ***Add Analysis Group*** .

7. Select the stores, heat analysis camera(s) or groups contained in the report.

**Note**

If you select **Heat Analysis for One Camera** as the analysis type, you should select camera(s). If you select **Heat Analysis in One Region**, you should select heat analysis group(s).

8. (Optional) Set the dwell duration.
9. Set the **Statistical Cycle** as **By Day**, **By Week**, or **By Month** and set the sending time, and set how the report will present results analyzed in the specified time period.

**Daily Report**

Daily report shows data on a daily basis. The platform will send one report at the sending time every day, which contains analysis results on the day (24 hours) before the current day. For example, if you set the sending time as 20:00, the platform will send a report at 20:00 every day, containing analysis results between 00:00 and 24:00 before the current day.
For example, if you select the report type as Daily, you can select Calculate by Hour or Calculate by Minute. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of passing vehicles detected in each hour or each minute for one camera.

**Weekly Report and 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 platform will send one report at the sending time every week or every month, which contains analysis results on the last 7 days or last month before the sending date.
For example, for weekly report, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing analysis results between last Monday and Sunday.

10. Set the report time and sending time according to the report type.
11. (Optional) Set the effective period (start time and end time) of sending the report regularly.
12. (Optional) Switch on **Send via Email**, and select the email template from the drop-down list to define the recipient information and email format.

**Note**

You can click **Add** to add a new email template.

13. (Optional) Switch on **Upload to SFTP**, and click **Configure** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

**Note**

You can also hover the cursor on , then click **Configure SFTP** from the drop-down list to enter the panel to configure the corresponding information.

14. (Optional) Switch on **Save to Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

**Note**

You can also hover the cursor on and click **Configure Local Storage** to enter the panel to configure the corresponding information.

15. Click **Add**.
16. (Optional) Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

# Chapter 21 Traffic Incident Monitoring

In the Traffic Incident Monitoring module, you can access the Traffic Incident Analysis dashboard for multi-dimensional data visualization, helping you identify high-incidence areas, event type patterns, and peak activity periods. You can also use the Traffic Incident Search feature to filter specific incidents by time, camera, event type, or license plate details, view full event information, and export results in Excel or CSV format after password verification.

In the top left corner of the Home page, select → **Passing Management** → **Traffic Incident Monitoring** .

## Traffic Incident Analysis

1. Click **Traffic Incident Analysis**.
2. Select an area and camera, and select time to view the data.

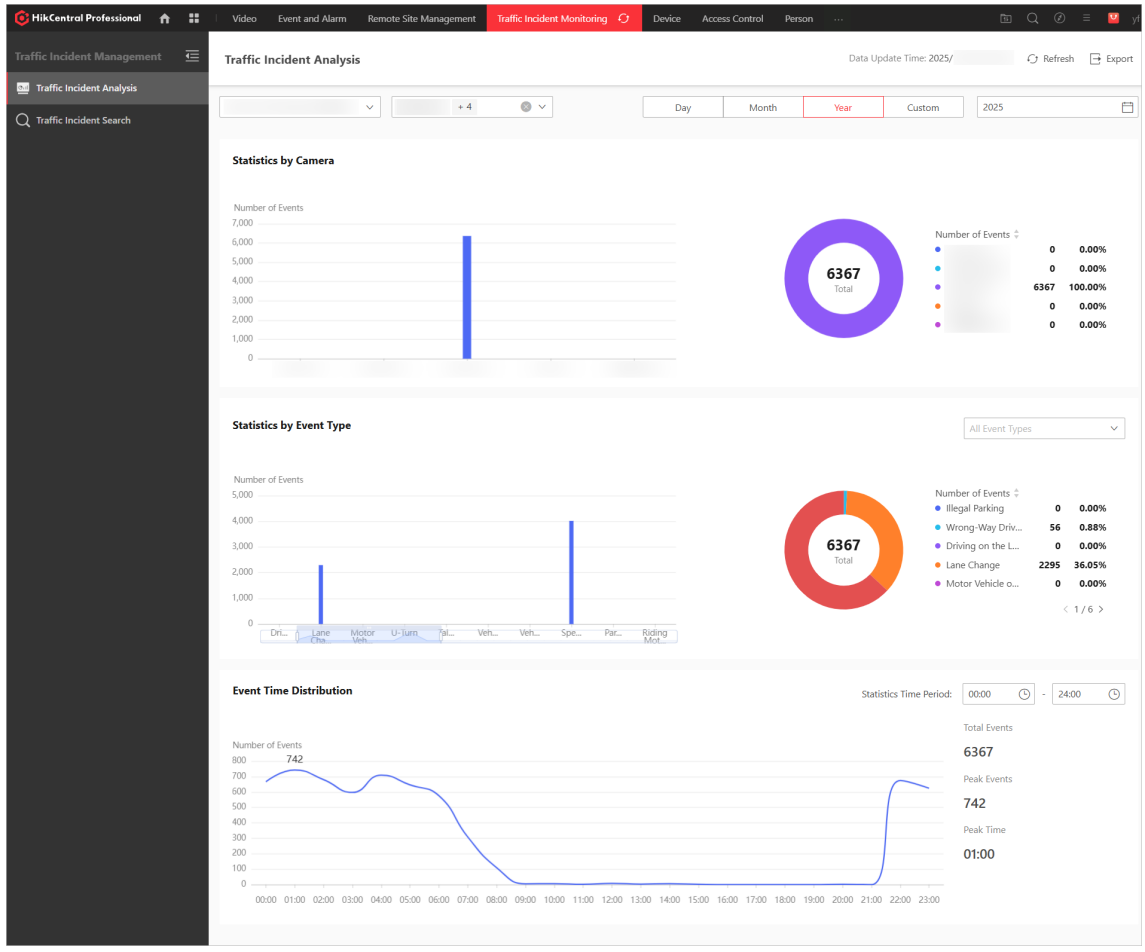



**Figure 21-1 Traffic Incident Analysis**

3. The three data sections will be displayed.

- The Statistics by Camera section provides an overview of total events and their percentage distribution across cameras, enabling you to quickly identify high-incidence areas.
- The Statistics by Event Type section displays an overview of total events and their percentage distribution across event types, enabling data-driven enforcement strategies tailored to the frequency and severity of each event type.
- The Event Time Distribution section provides hourly event counts, helping to identify peak activity periods, temporal patterns, and potential anomalies such as sudden surges during rush hours or unusual nighttime activity.

4. Hover over a chart element to see the total events. Click on a figure to navigate to the Search page with the corresponding filter applied.
5. (Optional) Export the data.
   a. On the dashboard, configure your desired filters.
   b. Click **Export**.
   c. Select the export format: PDF, Excel, or CSV.
   d. The file will be available in the Download Center.

## Traffic Incident Search

1. Go to **Traffic Incident Search**.
2. Filter traffic incidents by time range (such as Today, Yesterday, or a custom period of up to 30 days), specific cameras, event types, or license plate details including country/region, license plate size, and license plate type, and click **Search**.

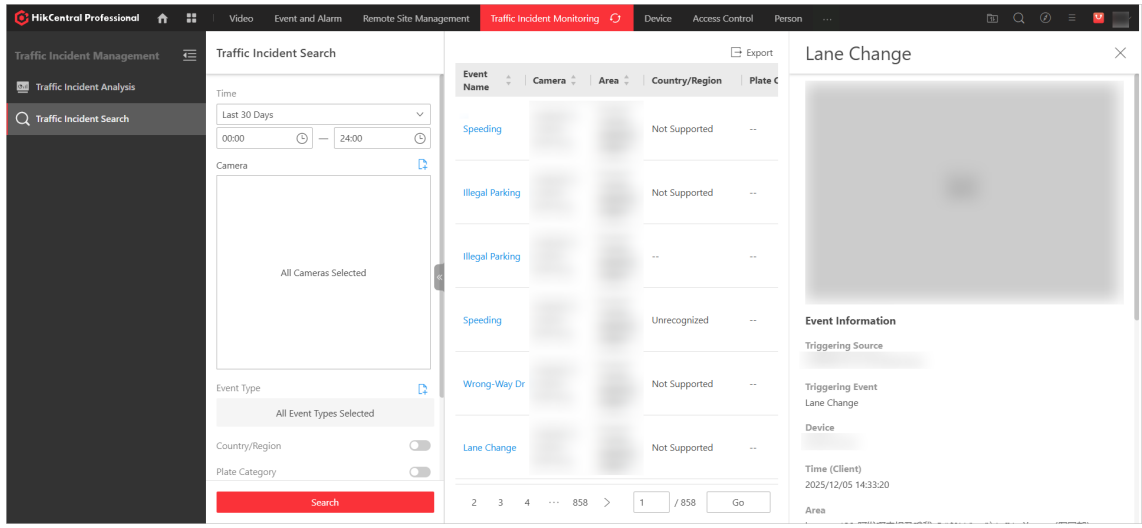



**Figure 21-2 Traffic Incident Search**

3. Results will be displayed in a list format, and clicking any event name opens a slide-out panel with full details.
4. Click any record to view details in a sidebar panel, including images.
5. (Optional) Click **Export**, select format, and complete password authentication to export the results.

# Chapter 22 Security Inspection Management

You can manage the added security inspection devices in the platform and perform the related operations, such as adding security inspection channels to the area, viewing videos of security inspection, searching for historical data, etc.

In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** .

## 22.1 Flow Chart of Security Inspection

The following flow chart shows the process of the configurations and operations of security inspection.

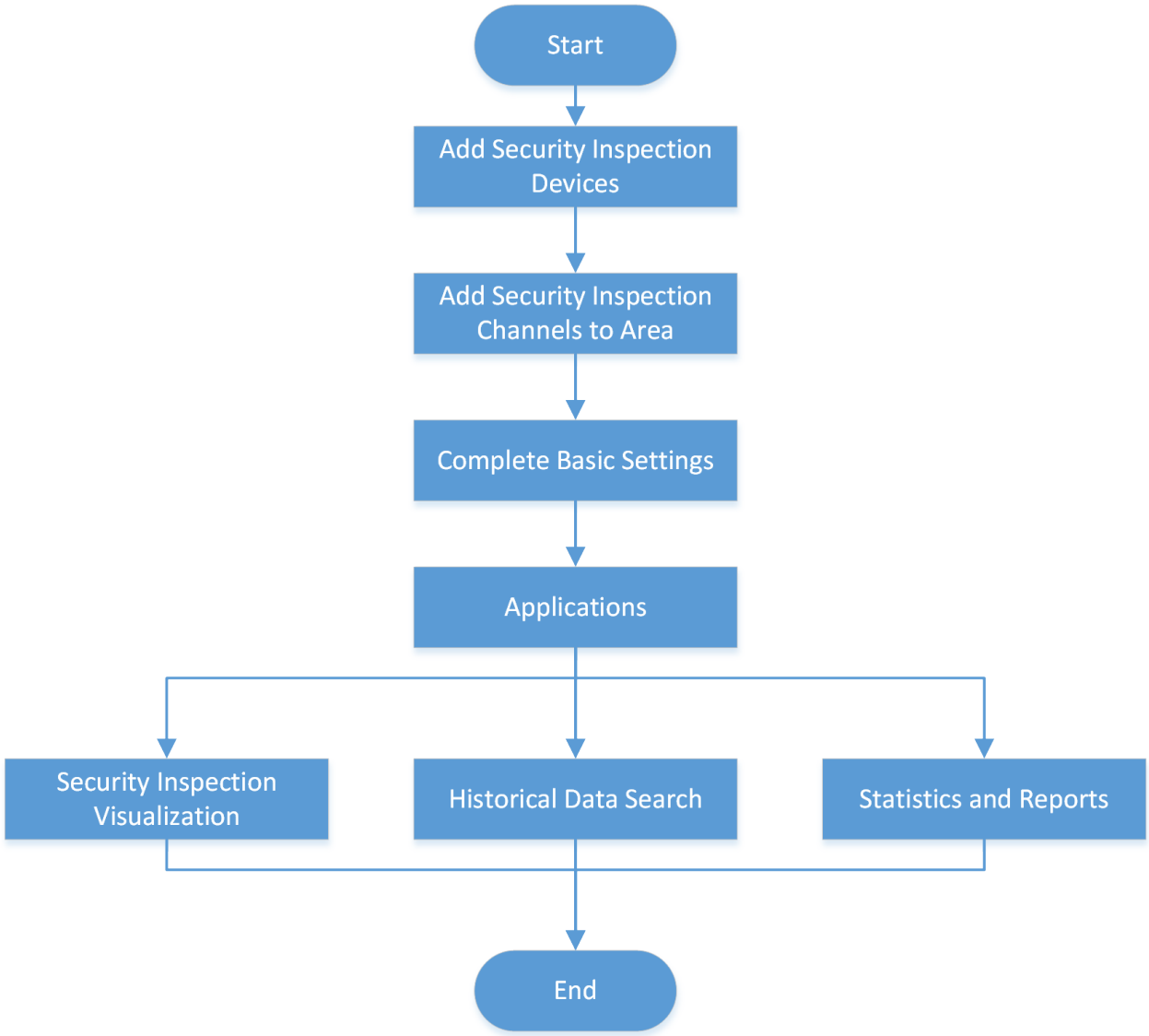



**Figure 22-1 Flow Chart of Security Inspection**

**Table 22-1 Flow Chart of Security Inspection**

| Step | Description |
|---|---|
| Add Security Inspection Devices | Add devices that support security inspection to the platform by different methods (e.g., online detection, IP address, port segment, device ID). |
| Add Security Inspection Channels to Area | Add security inspection channels and link security inspection devices to them for live view and playback.<br>For details, refer to ***Add Security Inspection Channels to Area*** . |

| Step | Description |
|---|---|
| Complete Basic Settings | Configure the basic parameters for security inspection, such as absence alarm interval and event retention duration.<br>For details, refer to ***Configure Security Inspection*** . |
| Security Inspection Visualization | During live view and playback of the videos streamed from analyzers, you can view the marked out articles of the checked package, package information, and package owner. For those of walkthrough metal detectors, you can view the information of the checked people.<br>For details, refer to ***View Videos of Security Inspection*** . |
| Historical Data Search | Search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.<br>For details, refer to ***Historical Data Search*** . |
| Statistics and Reports | Generate a package detection report and a people inspection report based on the specified features. You can also export reports to the local PC.<br>For details, refer to ***Generate Package Detection Report*** and ***Generate People Inspection Report*** . |

## 22.2 Configure Security Inspection

You can configure the basic parameters for security inspection.

**Steps**

1. Click **Basic Settings → Parameter Configuration** on the left.
2. Configure the following parameters and click **Save**.

**Time of Matching Person with Package (sec)**

This parameter is for analyzers. When the package is detected, the owner is more likely to be captured within the configured time range.

**Absence Alarm Interval (sec)**

Set the interval to upload the absence alarm information.

**Abnormal Skin-Surface Temperature Threshold (℃)**

Set the abnormal skin-surface temperature threshold. An alarm will be triggered if a person's skin-surface temperature above the threshold is detected.

**Event Retention Duration**

Select the duration that the event information can be saved for.

**Real-Time Alarm Configuration**

Select the prohibited article(s) for package detection, the abnormal event type(s) for abnormal event detection, and the alarm type(s) for metal detection.

**Manual Handling Action**

Click **Add** to customize manual handling actions which will be displayed in the alarm pop-up window.

## 22.3 Add Security Inspection Channels to Area

You can add security inspection channels and link security inspection devices to them for live view and playback.

**Steps**

1. Click **Basic Settings → Security Inspection Channel Management** on the left.
2. Click **Add** to enter the Add Security Inspection Channel page.
3. Enter the channel name.
4. Select an area from the area list.
5. **Optional:** In the Link Device field, select one security inspection device in the available list and click .

   **Note**

   If you do not link a device to the channel, live view and playback are not available via this channel.

   The device will be displayed in the added list.
6. **Optional:** In the Link Camera field, click **Add** to add camera(s) in the available list.

   **Linked Device**

   After adding a linked camera, you can select the linked device which can receive the face capture events of the corresponding camera.
7. Click **Add**.

## 22.4 View Videos of Security Inspection

During live view and playback of the videos streamed from analyzers, you can view the marked out articles of the checked package, package information, and package owner. For those of walk-through metal detectors, you can view the information of the checked people.

**Note**

Make sure you have added security inspection channels and linked devices with them. See details in ***Add Security Inspection Channels to Area*** .

Click **Security Inspection Visualization** on the left.

Select a security inspection device and click **Live View** or **Playback**.

**Note**

- In the top right corner of the Live View or Playback page, you can click to set video parameters.
- You can double click a camera in the camera list to start the live view / playback in a window on the right and you can add repeatedly.
- At the bottom, it displays the information about package, package owner, and checked person. The pictures captured by the linked cameras (including built-in cameras and external network cameras) will be displayed.

## Live View

Move the mouse cursor to the lower edge of the live view window and perform more operations.

| Icon | Function | Description |
|---|---|---|
|  | Capture | Take a snapshot of the current video. |
|  | Start Recording | Start recording the video. |
|  | Enable Audio | Turn off/on the sound and adjust the volume. |
|  | Enable Video Enhancement | Adjust the video image including brightness, saturation, contrast, and hue. |
|  | Stream Switch | Switch the video stream to main stream, sub-stream (if supported), or smooth stream (if supported). |
|  | Instant Playback | Switch to instant playback mode to view the recorded videos. |
|  | Turn on Alarm Output | Turn on/off the alarm outputs linked with the camera. |
|  | Start Two-Way Audio | Start two-way audio to realize voice talk with the person at the device. |

## Playback

Move the cursor to the lower edge of the playback window and perform more operations.

| Icon | Function | Description |
|---|---|---|
|  | Capture | Take a snapshot of the current video. |
|  | Clip | Clip the video files for current playback. |
|  | Enable Audio | Turn off/on the sound and adjust the volume. |
|  | Open Digital Zoom | Zoom in/out the video. |
|  | Show Stream Information | Display the stream information in the video image. |
|  | Enable Video Enhancement | Adjust the video image including brightness, saturation, contrast, and hue. |
|  | Stream Switch | Switch the video stream to main stream, sub-stream (if supported), or smooth stream (if supported). |
|  | Fisheye Expansion | Correct the video image and reverse the effects of geometric distortions caused by fisheye camera lens.<br>**Note**<br>This function is available only for fisheye cameras. |
|  | Add a Tag | Add a tag to the video file to mark a time point. |
|  | Add a Lock | Lock a video segment to protect it from being deleted or being overwritten when the HDD is full. |
|  | Counterclockwise Rotate | Counterclockwise rotate the video image. |
|  | Start Two-Way Audio | Start two-way audio to realize voice talk with the person at the device. |

## 22.5 Historical Data Search

You can search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.

### 22.5.1 Search for Package Detection Records

You can set search conditions, including time, article type, and location, to search for the package detection records.

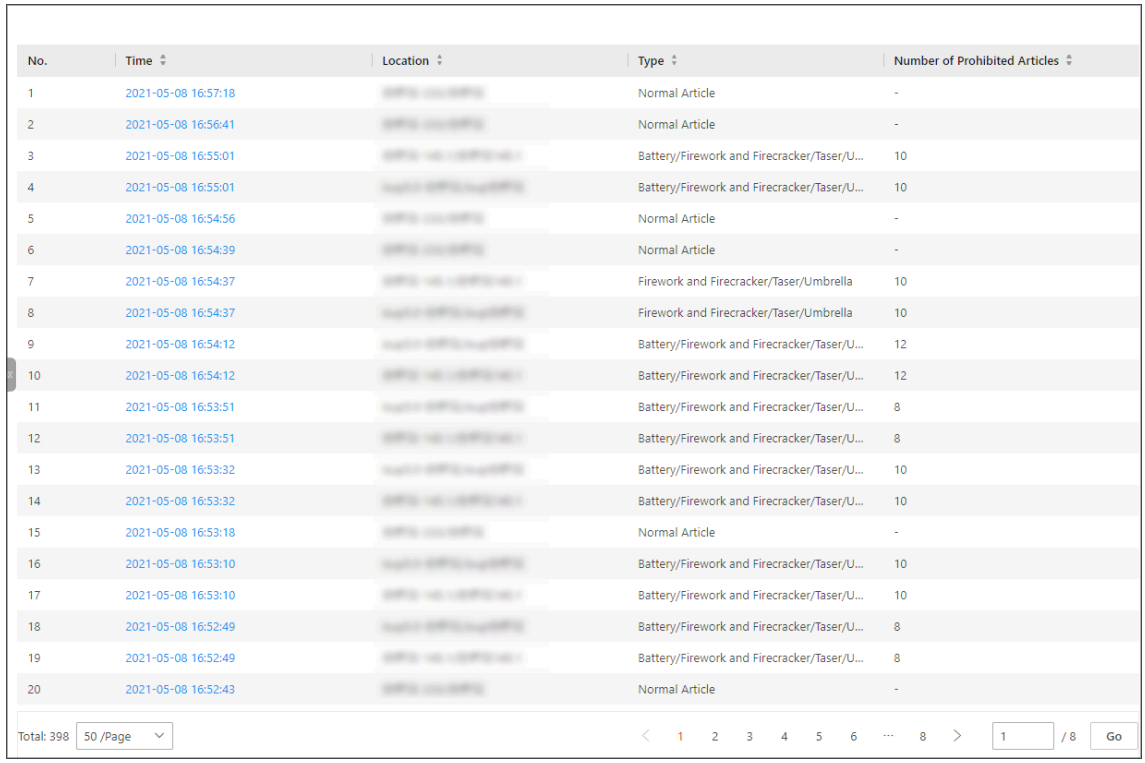
**Steps**

1. Click **Historical Data Search → Package Detection Record Search** on the left.
2. Select a period of time from the drop-down list.
3. In the Article Type field, select one or multiple prohibited or normal articles.
4. In the Location field, select one or multiple channels from the list.
5. Click **Search**.

   The matched records will be displayed.

**Note**

You can view the event details by clicking the event time.



| No. | Time | Location | Type | Number of Prohibited Articles |
|---|---|---|---|---|
| 1 | 2021-05-08 16:57:18 | [redacted] | Normal Article | - |
| 2 | 2021-05-08 16:56:41 | [redacted] | Normal Article | - |
| 3 | 2021-05-08 16:55:01 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 4 | 2021-05-08 16:55:01 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 5 | 2021-05-08 16:54:56 | [redacted] | Normal Article | - |
| 6 | 2021-05-08 16:54:39 | [redacted] | Normal Article | - |
| 7 | 2021-05-08 16:54:37 | [redacted] | Firework and Firecracker/Taser/Umbrella | 10 |
| 8 | 2021-05-08 16:54:37 | [redacted] | Firework and Firecracker/Taser/Umbrella | 10 |
| 9 | 2021-05-08 16:54:12 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 12 |
| 10 | 2021-05-08 16:54:12 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 12 |
| 11 | 2021-05-08 16:53:51 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 12 | 2021-05-08 16:53:51 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 13 | 2021-05-08 16:53:32 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 14 | 2021-05-08 16:53:32 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 15 | 2021-05-08 16:53:18 | [redacted] | Normal Article | - |
| 16 | 2021-05-08 16:53:10 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 17 | 2021-05-08 16:53:10 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 18 | 2021-05-08 16:52:49 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 19 | 2021-05-08 16:52:49 | [redacted] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 20 | 2021-05-08 16:52:43 | [redacted] | Normal Article | - |

Total: 398 50 /Page 1 2 3 4 5 6 ··· 8 1 / 8 Go

**Figure 22-2 Search for Package Detection Records**

## 22.5.2 Search for Metal Detection Records

You can set the search conditions, including time and location, to search for the metal detection records.

**Steps**

1. Click **Historical Data Search → Metal Detection Record Search** on the left.
2. Select a period of time from the drop-down list.
3. In the Location field, select one or multiple channels from the list.
4. Click **Search**.

   The matched records will be displayed.

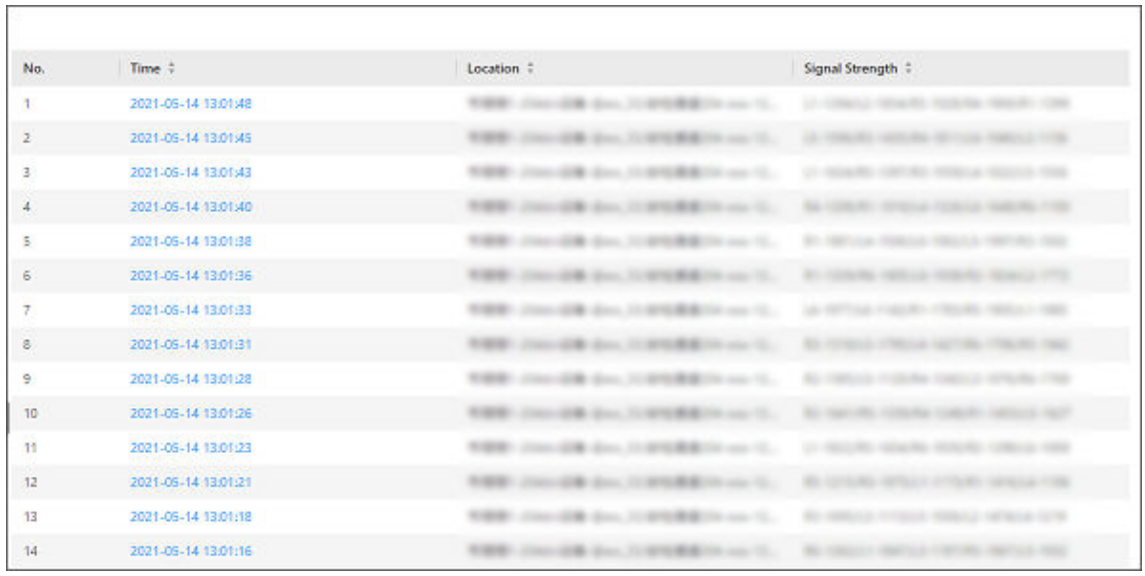



**Figure 22-3 Search for Metal Detection Records**

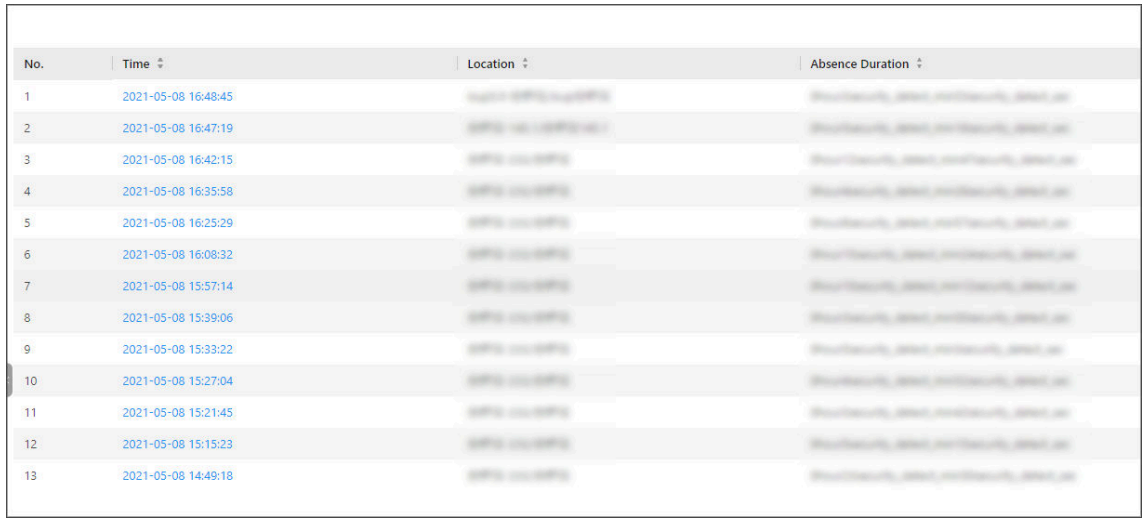
## 22.5.3 Search for Absence Records

You can set the search conditions, including time and location, to search for the absence records.

**Steps**

1. Click **Historical Data Search → Absence Record Search** on the left.
2. Select a period of time from the drop-down list.
3. In the Location field, select one or multiple channels from the list.
4. Click **Search**.

   The matched records will be displayed.



| No. | Time | Location | Absence Duration |
|---|---|---|---|
| 1 | 2021-05-08 16:48:45 | | |
| 2 | 2021-05-08 16:47:19 | | |
| 3 | 2021-05-08 16:42:15 | | |
| 4 | 2021-05-08 16:35:58 | | |
| 5 | 2021-05-08 16:25:29 | | |
| 6 | 2021-05-08 16:08:32 | | |
| 7 | 2021-05-08 15:57:14 | | |
| 8 | 2021-05-08 15:39:06 | | |
| 9 | 2021-05-08 15:33:22 | | |
| 10 | 2021-05-08 15:27:04 | | |
| 11 | 2021-05-08 15:21:45 | | |
| 12 | 2021-05-08 15:15:23 | | |
| 13 | 2021-05-08 14:49:18 | | |

**Figure 22-4 Search for Absence Records**

## 22.6 Generate Package Detection Report

You can generate a package detection report based on the package detection records, percentage of packages with prohibited articles, or prohibited article types. You can also export the report to the local PC.

**Steps**

1. Click **Statistics and Reports → Package Detection Report** on the left.
2. In the Type field, select **Package Detection Records**, **Percentage of Packages with Prohibited Articles**, or **Prohibited Article Types**.
3. In the Location field, select one or multiple channels from the list.
4. Select a report type and a specific time period.
5. Click **Generate Report**.
6. **Optional:** Click **Export** to export the report to the local PC.

## 22.7 Generate People Inspection Report

You can generate a people inspection report based on the number of checked persons or percentage of metal detection alarms. You can also export the report to the local PC.

**Steps**

1. Click **Statistics and Reports → People Inspection Report** on the left.
2. In the Type field, select **Number of Checked Persons** or **Percentage of Metal Detection Alarms**.
3. In the Location field, select one or multiple channels from the list.
4. Select a report type and a specific time period.

5. Click **Generate Report**.
6. **Optional:** Click **Export** to export the report to the local PC.

# Chapter 23 Access Control Management

Access control is a security technique that can be used to regulate who can get access to the specified door and floor control can be used to regulate who can get access to the specified floors by taking the elevator.

In the top left corner of Home page, select → **Passing Management → Access Control** .

On the Web Client, the administrator can add access control devices, elevator control devices, and video intercom devices to the system, group resources (such as doors) into different areas, and define access permissions by creating an access level to group the doors/floors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors and floors in the access level with their credentials during the authorized time period.

The following are high-frequency scenarios for your reference.

- ***Assign by Person*** : Assign access level to persons, so that the assignees can have the access to the access points in the access levels.
- ***Manage Multi-Factor Authentication*** : An access authentication scheme which requires all the predefined persons to be present and authenticate.
- ***Configure Anti-Passback*** : Only one person can pass the access point after swiping the card.
- ***How to Open the Door by Your Smart Phone*** : Open the door quickly when getting close, by rotating phones, by waving at the access point, or by manually selecting a door on the Mobile Client.

To get a better understanding of the Access Control module, go to **Access Control Overview** on the left navigation bar. You can perform the following operations as needed.

| Name | Description |
|---|---|
| Wizard | You can view the brief introduction of the Access Control function and the major steps of configuration. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page; click **Quick Configure** to complete the configuration process step by step in the Access Control Wizard. |
| Health Status | In Health Status, click the number in a circle to view status of each resource type, or click the number on the right of **Exception** to go to the Maintenance page for details about alarm inputs.<br>In the upper-right corner, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** . |
| Person Credential Status | Click the number in the circle of each credential to go to the Person page. |

| Name | Description |
| --- | --- |
| | Click the number under the application items (including person information and credentials) to go to the corresponding pages for details. |
| Access Event Statistics | Click and select a period to view the statistics of this period.<br>Hover over , select a file format, and click **Export** to export the data generated in the selected period. |
| Person Access Event Statistics | Click to show the details of the recognized person. Click **Auto Update Record** to automatically display the latest record. Click **More** to go to the Person Authentication Record page to search for more data. |

## 23.1 Flow Chart of Door Access Control

The following flow chart shows the process of the configurations and operations of door access control.

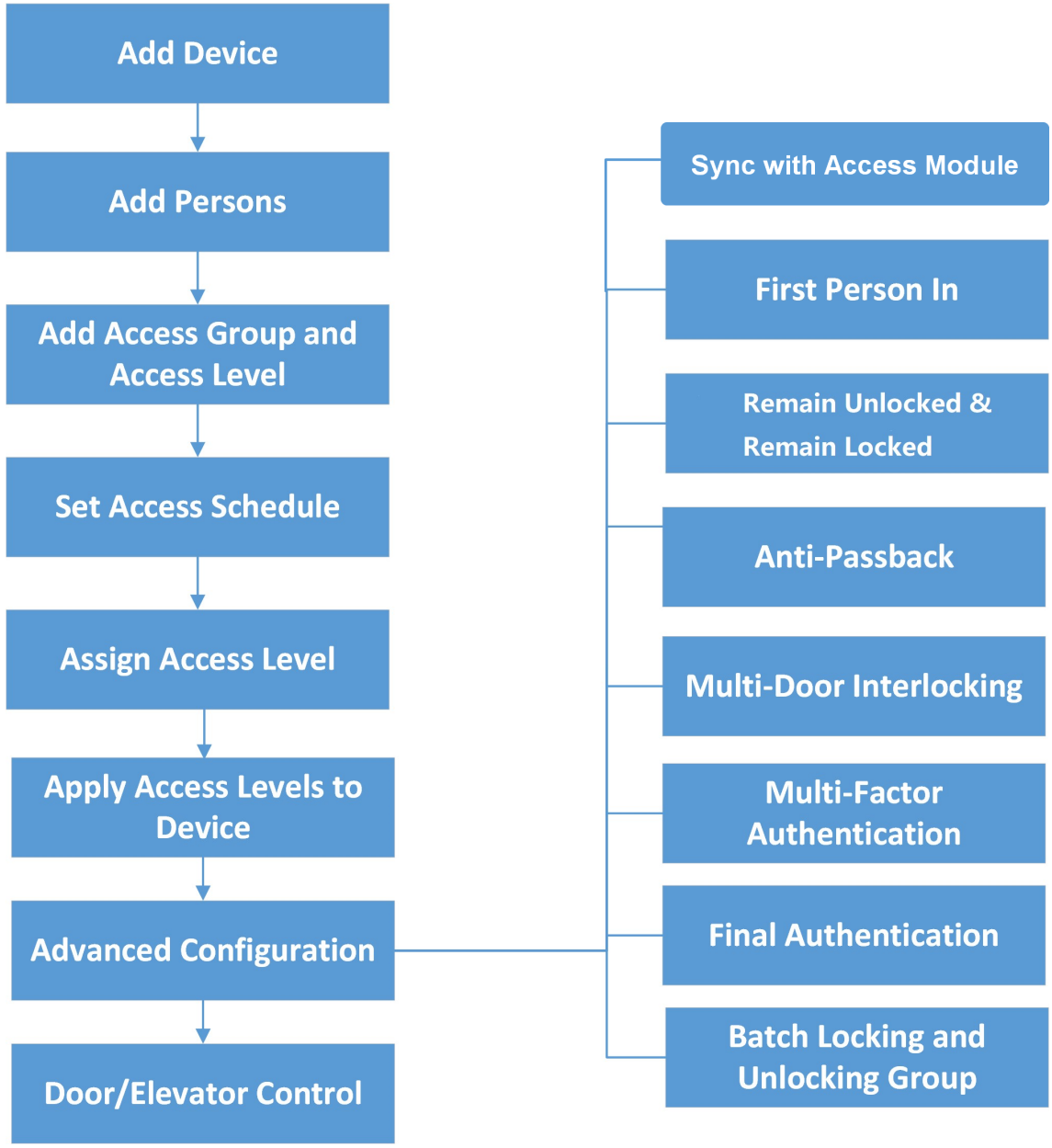



**Figure 23-1 Flow Chart of Door Access Control**

**Table 23-1 Procedures of Door Access Control**

| Procedure | Description |
|---|---|
| Add Access Control Devices to the Platform | You need to add access control devices to the system. |
| Add Doors Linked with Devices to Areas | Group doors linked with added devices for management. Refer to ***Add an Area Manually*** for details. |

| Procedure | Description |
|---|---|
| Add Departments and Persons | Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** . |
| Set Access Schedules | The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** . |
| Add Access Levels | An access level is a group of doors. After assigning access level, the assigned objects can get access to these doors during the authorized time period. For details, refer to ***Add Access Level*** . |
| Assign Access Levels to Persons | You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department. For details, refer to ***Manually Assign Access Level*** . |
| Control Door Status | You can manually change the door status to locked, unlocked, remaining locked, or remaining unlocked. Refer to ***Real Time Monitoring*** for details. |
| Advanced Functions | Refer to ***Add Remain Unlocked and Remain Locked Rule*** , ***Configure First Person In*** , ***Add a Multi-Factor Authentication Rule*** , ***Configure Multi-Door Interlocking*** , ***Configure Anti-Passback*** , ***Add a Batch Locking and Unlocking Group*** , ***Add a Final Authentication Counting Group*** , ***Configure Authentication Mode*** , ***Apply Advertisement to Access Control Devices*** , ***Add Audio Broadcast*** , and ***Sync with Access Module*** for details. |
| Data and Record Search | Refer to ***Data Search*** for details. |

## 23.2 Flow Chart of Floor Access Control

The following flow chart shows the process of the configurations and operations of floor access control.

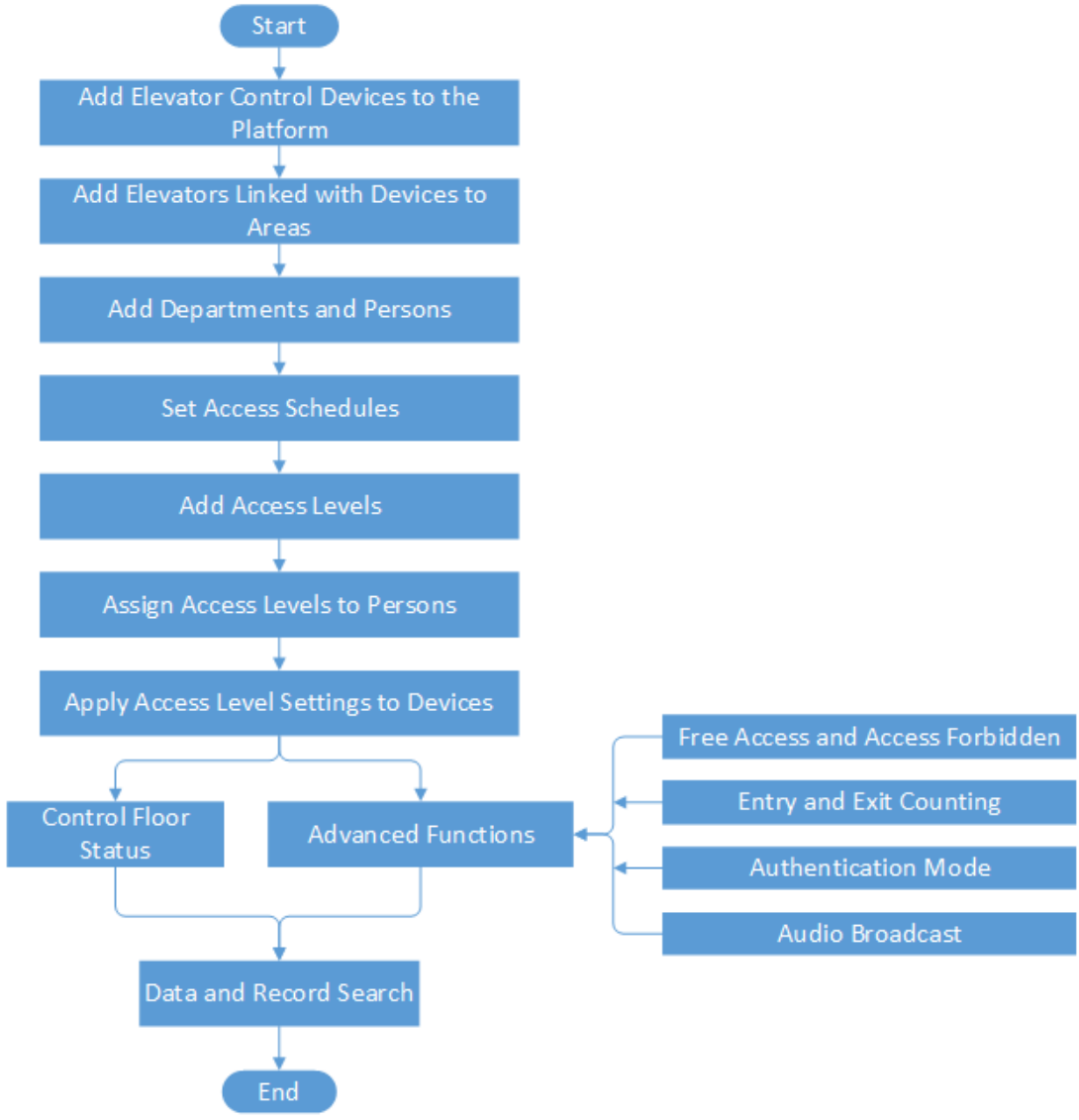



**Figure 23-2 Flow Chart of Floor Access Control**

**Note**

Some functions in this flow chart need the License. For details about License, refer to ***License Management*** .

**Table 23-2 Procedures of Floor Access Control**

| Procedure | Description |
|---|---|
| Add Elevator Control Devices to the Platform | You need to add elevator control devices to the system. |
| Add Elevators Linked with Devices to Areas | Group elevators linked with added devices for management. |
| Add Departments and Persons | Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** . |
| Set Access Schedules | The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** . |
| Add Access Levels | An access level is a group of floors. After assigning access level, the assigned objects can get access to these floors during the authorized time period. For details, refer to ***Add Access Level*** . |
| Assign Access Levels to Persons | You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department. For details, refer to ***Assign Access Level to Persons*** . |
| Apply Access Level Settings to Devices | After setting the linkage between the persons and the access level, the person's access level settings will be automatically applied to the elevator control devices of the elevators linked to the access level to take effect. After that, the persons can access these floors during the authorized time period defined by the related access level. You can also set a schedule to apply the settings regularly. For details, refer to ***Regularly Apply Access Level Settings to Devices*** . |
| Control Floor Status | You can manually change the floor status to temporary access, access with credential, free access, or access forbidden. Refer to ***Door & Barrier Control*** for details. |
| Access Control Application | Refer to ***Add Remain Unlocked and Remain Locked Rule*** , ***Add a Final Authentication Counting Group*** , ***Configure Authentication Mode*** , and ***Add Audio Broadcast*** for details. |
| Data and Record Search | See ***Data Search*** for details. |

## 23.3 Before You Start

To implement Access Control function, you need to add devices and persons to ensure a smooth deployment.

### Add Device

You must add access control devices, elevator control devices, or video intercom devices to the platform. You can add different types of devices as needed and select the appropriate method (by device ID, IP address, etc.).

**Table 23-3 Add Devices**

| Device | Access |
|---|---|
| Access control devices | Go to → **Device** → **Access Control Device** . |
| Elevator control devices | Go to → **Device** → **Elevator Control Device** . |
| Video intercom devices | Go to → **Device** → **Video Intercom Device** . |

### Add Person

You must add persons to perform the following procedures, such as assigning access levels. You can choose the adding methods as needed, including adding a single person and importing person information. For details, see ***Add Person*** .

## 23.4 Assign Access Level to Persons

Assigning access level to persons can define which persons can get access to which access points during the authorized time period.

### 23.4.1 Add Access Level

**Steps**

1. Select **Access Level** → **Manage Access Level** .
2. Click **Add** to enter the Add Access Level page.
3. Create a name for the access level.
4. **Optional:** Edit the description for the access level.
5. Select the access point type.
6. Select the access point(s).

   In the **Available** list, select the access point(s) and click › . You can view your selection in the **Selected** list.

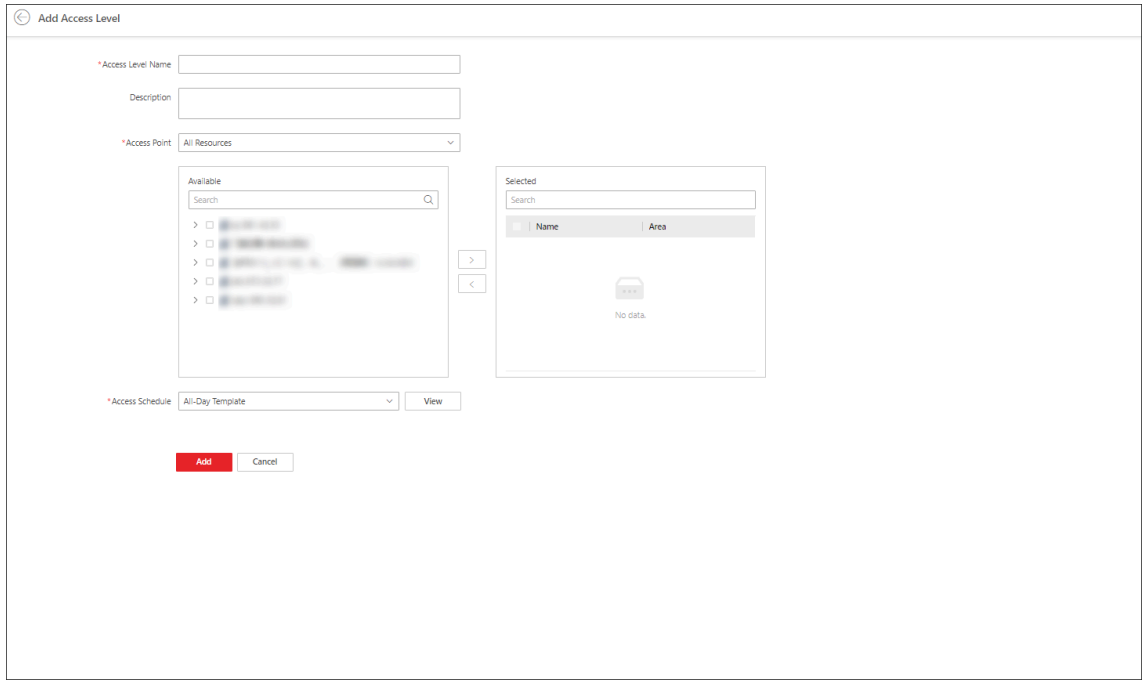



**Figure 23-3 Select Access Points**

7. Select an access schedule to define in which time period, persons are authorized to access the access points you select in the previous step.

**Note**

All default and custom access schedules are shown in the **Access Schedule** drop-down list. You can click **New Access Schedule Template** to customize a schedule. Or you can predefine access schedule templates. For details, refer to ***Set Access Schedule Template*** .

8. Click **Add** to add the access level and return to the access level management page.
9. **Optional:** Perform further operations on the added access level(s).

| | |
|---|---|
| **Edit Access Level** | Click the name of an access level to view and edit its configurations. |
| **Delete Access Level** | Select an access level and click **Delete** to delete it or click → **Delete All** to delete all access levels.. |
| **View Details of Access Schedule or Access Point** | Click to view details of access schedules or access points. |

**What to do next**

You need to assign the access level to persons, so that the assignees can have the access to the access points in the access level according to the access schedule. For details, refer to ***Manually Assign Access Level*** .

## 23.4.2 Manually Assign Access Level

You need to assign access levels to persons, so that the assignees can have the access to the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person, department, or access group.

For applying large-scale access levels, go to **Basic Configuration → General → Apply Large-Scale Access Level** . Once enabled, data will be applied to devices in the form of packaged files, which requires high server I/O performance (at least an SSD).

### Assign by Access Level

You can assign an access level to multiple persons so that the assigned persons can have the access to the access points in the access level.

**Before You Start**

- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .
- Make sure you have added persons to the system. For details, refer to ***Person Management*** .

Follow the steps to assign an access level to persons.

**Steps**

1. Select **Assign Access Level** on the left.
2. Click **Assign by Access Level** on the top.

   **Note**

   For the first time assignment, click **Add** at the center of the page to enter the assignment page.
3. Click on the access level that you want to assign to persons.
4. On the assignee pane, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.

   **Note**

   If you check **Select All**, all persons who matched the search conditions you set will be selected.

   The access level settings will be applied to devices automatically.

**What to do next**

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

### Assign by Person

You can assign access levels to persons, so that the assignees can have the access to the access points in the access levels.

**Before You Start**

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific persons.

**Steps**

1. Select **Assign Access Level** on the left.
2. Click **Assign by Person** on the top.
3. Check persons in the list, and click **Assign Access Level** to open the Assign Access Level pane.
4. **Optional:** In the Assign Access Level pane, click to add persons.
5. In the Access Level list, check the access levels that you want to assign to the selected persons.
6. Click **Assign**.

   The access level settings will be applied to devices automatically.

**What to do next**

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

## Assign by Department

You can assign access levels to departments, so that the persons in the department can have the access to the access points in the access levels.

**Before You Start**

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific departments.

**Steps**

1. Select **Assign Access Level** on the left.
2. Click **Assign by Department** on the top.
3. **Optional:** For the first time assignment, click **Assign Now** in the center of the page to open the Batch Assign Access Level to Departments page, and then see the second choice in ***4*** .
4. Do one of the following to assign access levels to departments.
   - Assign access levels to each department one by one.
     a. In the department list, click a department.
     b. Click **Assign Access Level** on the top.
     c. In the Assign Access Level pane, select the access levels you want to assign to the selected department.
     d. Click **Assign**.
   - Assign access levels to multiple departments at a time.
     a. Click **Batch Assign** on the upper left.
     b. In the department list, select the departments where you want to assign access levels.

**Note**

Sub-departments are excluded from selection by default. To include all sub-departments of each department, check **Select Sub-Departments**.

c. In access level list, select the access levels you want to assign to the departments.
d. Click **Save**.

The access level settings will be applied to devices automatically.

**What to do next**

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

## Assign by Access Group

An access group is the group of persons who have the same access permissions (In a specified time period, they have the permission to access the specified access points). You can add the persons who have the same access permission to the same access group. For example, the employees in the same department should access the company gates during the working hours. The employees can be added to the same access group and be related to the access level which contains the access permission of the company gates. You can assign one or multiple access levels to the access group, and the persons in the access group will get the permission to access all the access points in the access level(s).

**Before You Start**

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the platform. For details, refer to ***Add Access Level*** .

**Steps**

1. Select **Assign Access Level** on the left.
2. Click **Assign by Access Group** on the top.

**Note**

For the first time assignment, click **Assign Access Level** at the center of the page to enter the assignment page.

3. **Optional:** Add access groups.
   1) Click + at the top of the access group list to open the Manage Access Group pane, and then click **Add** to enter the Add Access Group page.

   **Note**

   If no access group is added to the access group list, click **Add Access Group** in the access group list to enter the Add Access Group page.

   2) In the **Group Name** field, enter the name of the access group.
   3) In the **Group Member** area, click **Add** to open the person list, select the person(s) to be added to the access group.

**Note**

If you check **Select All**, all persons who matched the search conditions you set will be selected.

4) Click **Add** to add the selected person(s) to the access group.
5) Click **Add** at the bottom.

4. Check access group(s) to assign access levels to.
5. Click **Assign Access Level** on the top.
6. In the Assign Access Level page, select the access level(s) to be assigned to.
7. Click **Assign**.

   The access level settings will be applied to devices automatically.

**What to do next**

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

## 23.4.3 Access Level Overview

The platform provides an overview of all persons' access levels for access points. You can filter persons and perform some operations on their access levels.

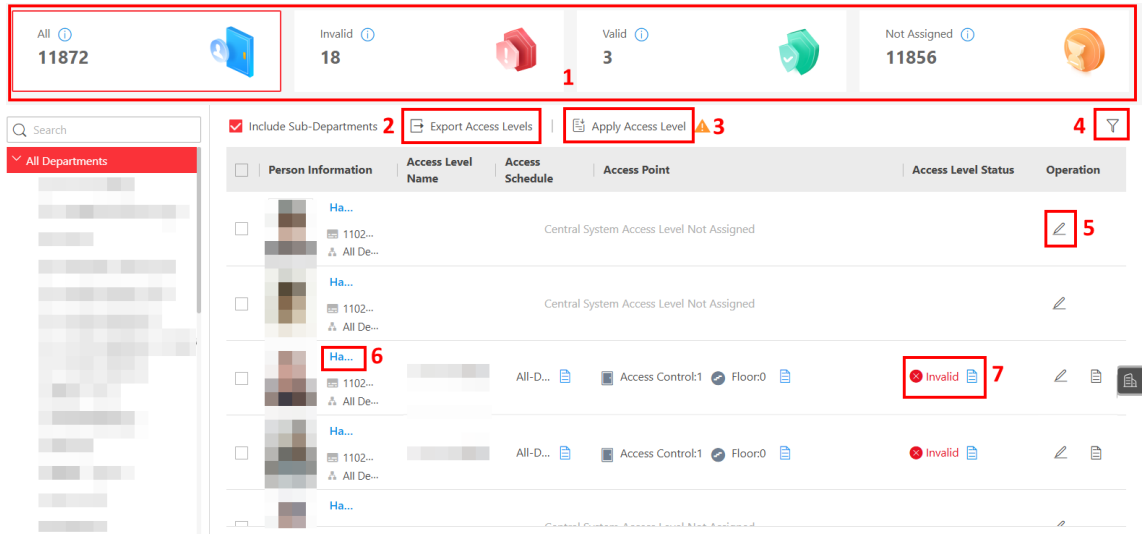



**Figure 23-4 Access Level Overview**

| | |
|---|---|
| 1 | On the top, you can click the cards to display all persons, persons with invalid access levels, persons with valid access levels, or persons not assigned with access levels if needed. |
| 2 | Export access levels. |

| | |
|---|---|
| | • Export a list of persons and their linked access levels in Excel or CSV format.<br>• Export a list of access levels and their linked person information in Excel format. |
| 3 | For persons whose access levels failed to be applied, persons with invalid access levels, or persons not assigned with access levels, you can apply access levels for them. You can select access points before applying. |
| 4 | Filter persons by different conditions such as person name, ID, access level. |
| 5 | Click to edit a persons access levels. You can add or delete access levels. |
| 6 | Click a person name to view the person information. |
| 7 | If a person's access level failed to be applied, "Invalid" will show in the Access Level Status column. You can click to view the details. |

### 23.4.4 Set Access Schedule Template

Access schedule defines when persons can open access points in an access level with credentials, or when access points remain unlocked so that persons can open the access points with free access. The system provides three default access control schedule templates: All-day Template, Workday Template, and Weekend Template. You can also add customized templates according to your needs.

**Steps**

1. Go to **Basic Configuration → Access Schedule Template** .
2. Click + to create a blank template.
3. Configure the template in the template information panel on the right.

**Copy From**

You can select to copy the settings from existing templates.

**Weekly Schedule Template**

Select or draw in the box to define the authorized time periods. After drawing, you can enter a time or adjust the time by clicking the arrows in the box popped up. You can set up to 8 separate time periods for each day.

Click **Erase** and select or draw on the authorized time periods to clear the selection. If you want to define the authorized time periods again, click **Authorize**.

**Holiday Schedule**

Set a holiday schedule if you want different schedules for specific days. Holiday schedule has a higher priority than weekly schedule.

a. Click **Select Holiday Group Schedule**.
b. Select existing holiday groups, or click **Add Holiday Group Schedule** to create a new holiday group.
c. Click **Add**.
d. Set a schedule pattern for holidays.

4. Click **Add** to save the template.
5. **Optional:** Perform further operations on added templates.

| | |
|---|---|
| **View and Edit Template Details** | Click a template item to view and edit its configurations. |
| **Delete Template** | Click a template item and click 🗑 to delete it. |

## 23.4.5 Set Holiday Group Schedule

In scenarios where departments share specific holiday schedules across multiple access schedules, configuring holidays individually for each schedule can be inefficient and may exceed device capacity limits. The Holiday Group Schedule feature addresses this by decoupling holidays from access schedules, allowing you to manage multiple holidays as a unified group. This enhances configuration flexibility and efficiency, as a single holiday group can be applied across various access schedules.

**Steps**

1. In the left navigation bar of the Access Control module, click **Basic Configuration → Holiday Group Schedule** .
2. Click + (on the upper left) or **Add**(in the middle of the page, only showing when no holiday group schedule in the platform) to enter the Add Holiday Group Schedule page.
3. Set Basic Information such as name, copy from, and remark.

   **Copy From**

   You can select to copy the settings from existing templates.

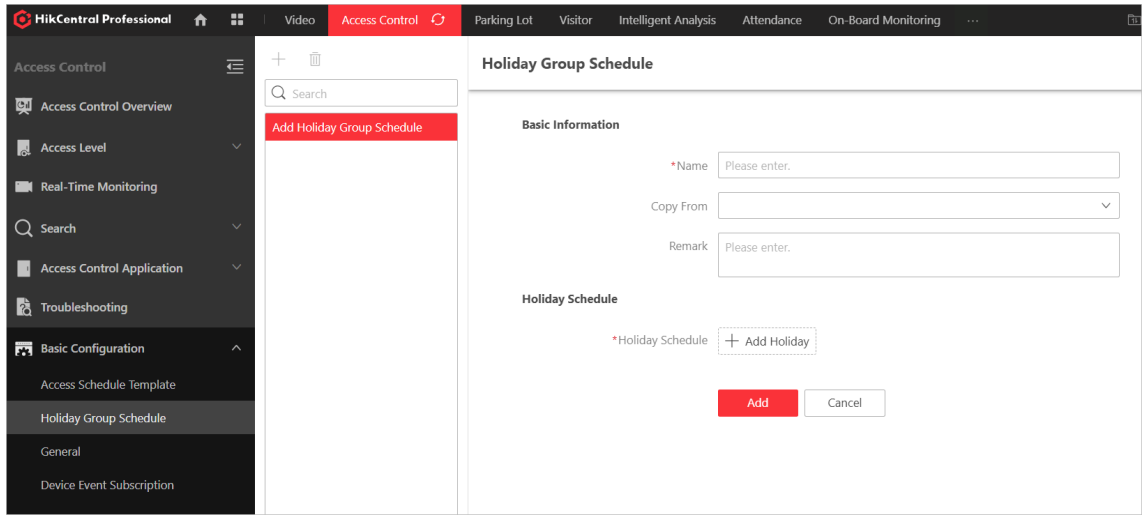



**Figure 23-5 Add Holiday Group Schedule**

4. Click **Add Holiday**, check holidays and click **Add**.

   The window for drawing holiday schedule will show.

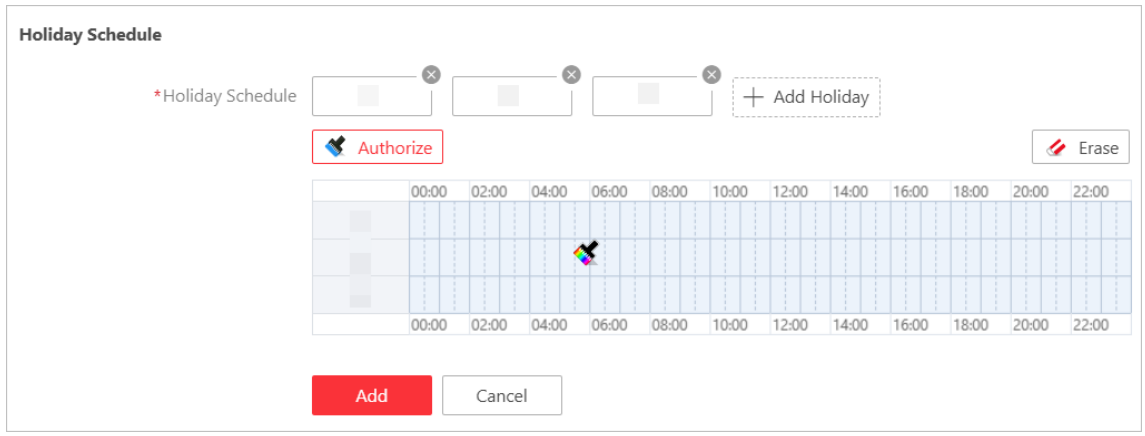



**Figure 23-6 Holiday Schedule**

5. Configure the time schedule for each added holiday by dragging the blue bars onto the timeline.
6. Click **Add** to finish adding.

   If all holidays within a group are deleted, the holiday group will be automatically deleted.
7. **Optional:** Perform the following operations.

| | |
|---|---|
| **Edit a Holiday Group Schedule** | In the holiday group schedule list, select a holiday group schedule to show and edit details on the right. |
| **Delete a Holiday Group Schedule** | In the holiday group schedule list, select a holiday group schedule and click . |

### 23.4.6 Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings that failed to be automatically applied to devices.

**Before You Start**
Make sure you have assigned access levels to persons in the system. For details, refer to ***Manually Assign Access Level*** .

**Steps**
1. Go to **Basic Configuration → General** .
2. Switch on **Apply to Device (Scheduled)**.
3. Select an applying mode.
   - **Apply at Fixed Time**: Apply the changed access level settings and the settings that failed to be applied last time to devices at a specific time (System Management Server time) on a daily basis. You can select a time in the **Auto-Apply At** drop-down list.
   - **Apply Every Certain Hours**: Apply the changed access level settings and the settings that failed to be applied last time to devices immediately and every certain hours afterward. You can select an interval in the **Time Interval** drop-down list.
4. Click **Save**.

### 23.4.7 Clear Persons' Access Levels

You can clear the access levels of persons so that they cannot access the access points in the access levels. For example, if there is no access record of certain persons entering or exiting for a long time, the administrator can clear their access levels to make sure the persons' credentials will not be misused.

On the left, select **Assign Access Level**, then select an access level assigning mode on the top.

The unassigning operations vary by different assigning modes.

- On the **Assign by Access Level / Assign By Person** page, select the target person, hover the cursor on ⌄ , and select **Unassign All Access levels** or **Unassign Specified Access Levels**.

  **Note**

  For the latter one, if you selected multiple persons, only the common access levels shared by the selected persons can be unassigned.
- On the **Assign by Department / Assign by Access Group** page, check access level(s) and click **Unassign**, or hover the cursor on ⌄ and select **Unassign All**.

**Note**

- Once cleared, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.
- After the access level settings of the selected persons are cleared , these persons will be removed from the related access groups.
- After the access levels are unassigned, the changes will be automatically applied to devices, and the access level settings of the persons will be deleted from the devices.

## 23.5 How to Open the Door by Your Smart Phone

Users can open the door quickly by the Mobile Client or by rotating their phone by the reader. With a specific configuration, they can open the door without logging into the Mobile Client.

### Step 1 Add Access Control Devices

First, you need to go to the Device module to add an access control device that supports Bluetooth. See details in ***Add Device(s)*** .
Then, go to the Maintenance page to check the device capability.

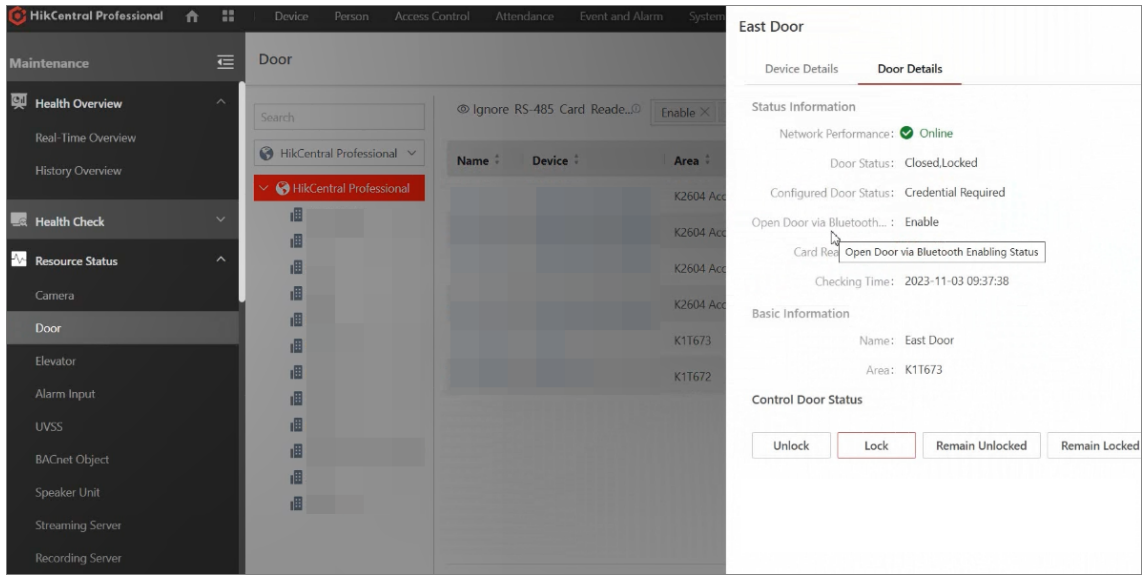



**Figure 23-7 Check Device Capability**

### Step 2 Enable Self-Service Login for the Person

Go to the Person page, click a person name to enter the editing page, and then enable the **Allow Login to Self-Service** for the person. This allows the person to log into the Mobile Client and the Self-Service of Web Client.

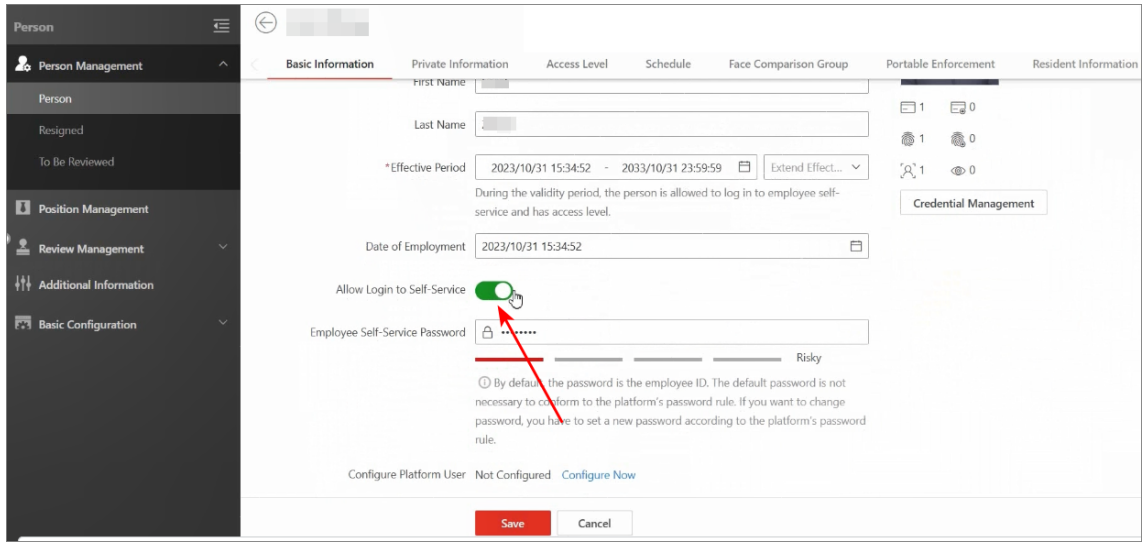



**Figure 23-8 Enable Self-Service Login**

Go to the Access Level tab, and enable **Open Door via Bluetooth on Mobile Client**.

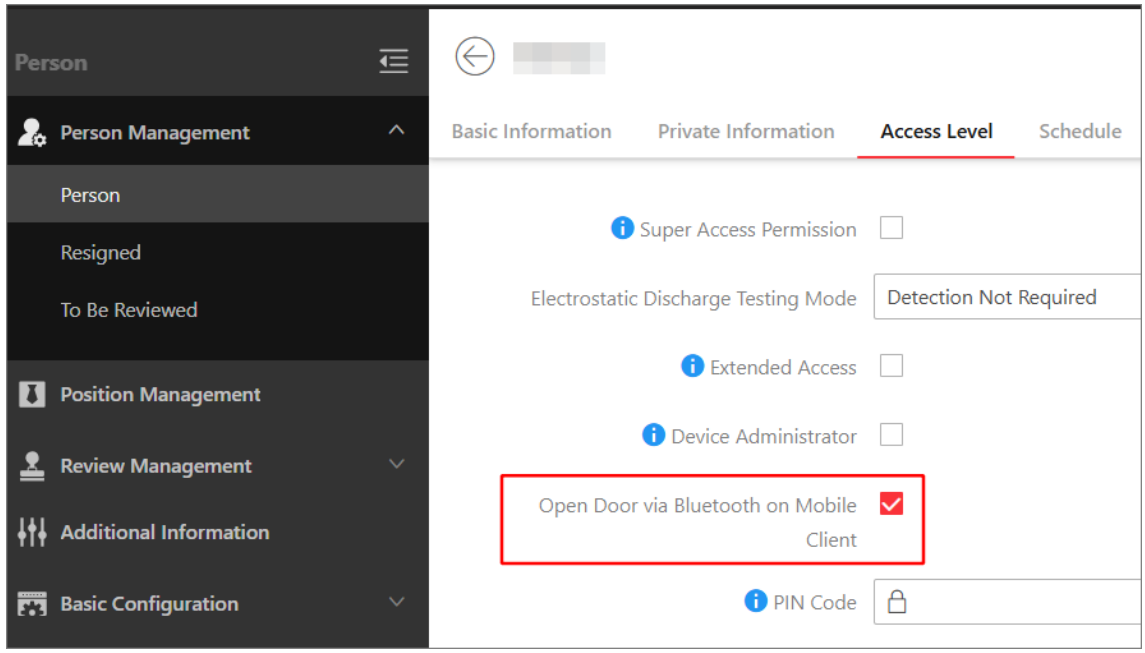



**Figure 23-9 Access Level Tab on Person Page**

## Step 3 Basic Settings in Access Control Module

1. Go back to the Access Control page, create an access level for the door supporting Bluetooth.

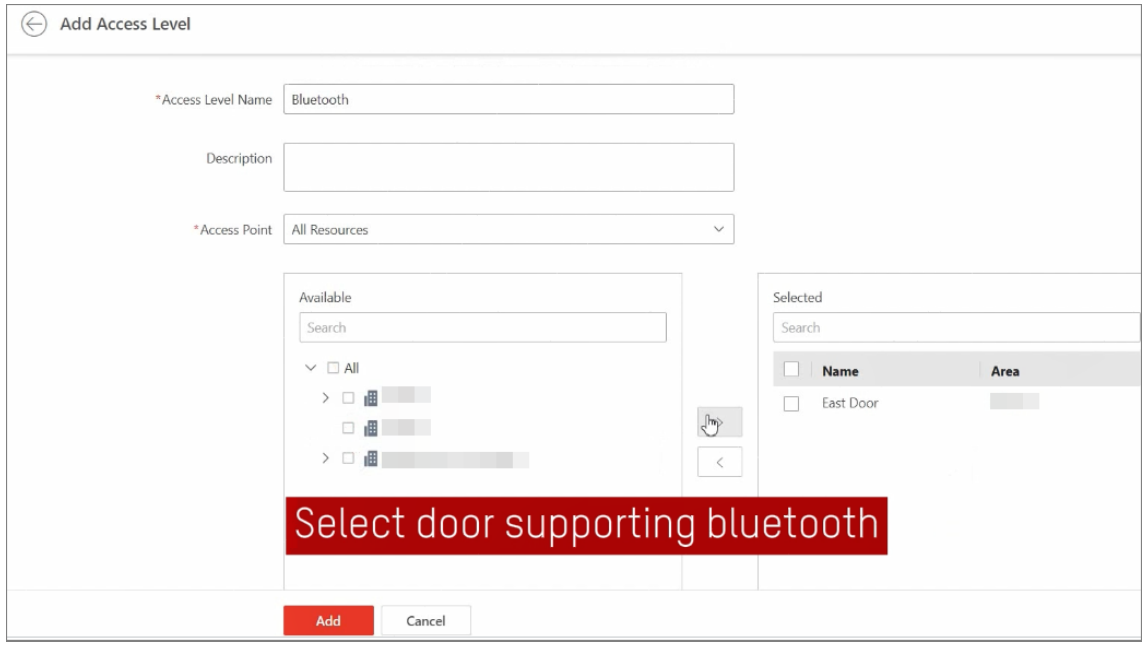



**Figure 23-10 Create Access Level**

2. Assign the added access level to person(s).

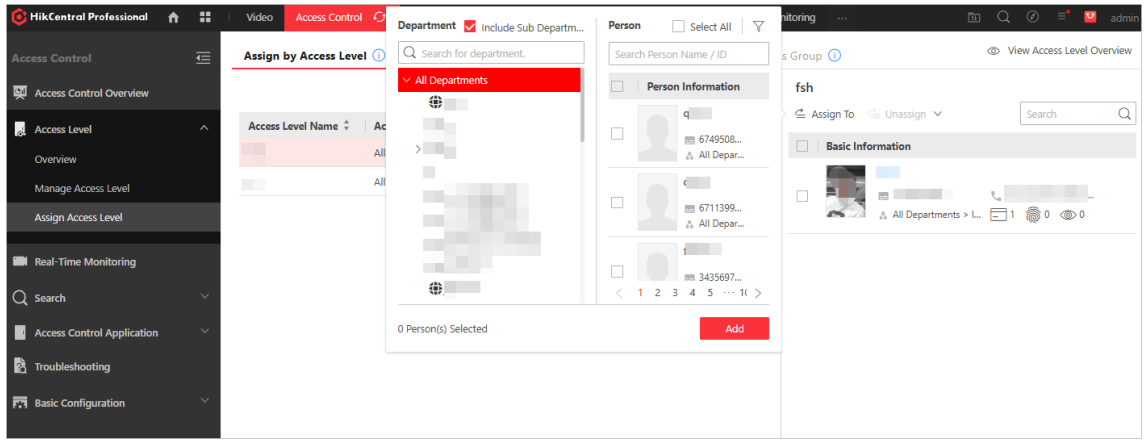



**Figure 23-11 Assign Access Level to Person(s)**

3. Select a door opening method and set offline unlocking validity (optional). This can be done on either the Web Client or Mobile Client.
   - (Web Client) Go to **Basic Configuration → General → Open Door via Bluetooth** and select a door-opening mode.
     (Optional) In the Offline Unlocking area, select the validity of offline unlocking.

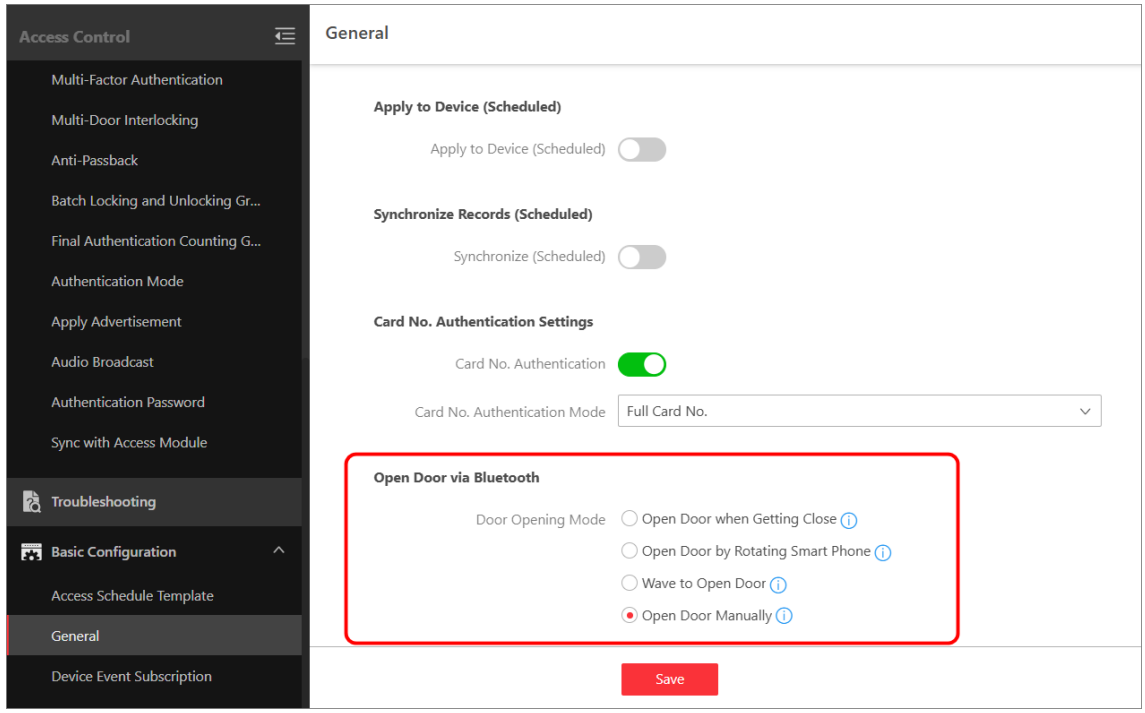



**Figure 23-12 Open Door via Bluetooth**

- (Mobile Client) For admins, go to **Me → Settings → Open Door via Bluetooth** and select a door-opening mode.
  (Optional) In the Validity Period of Offline Unlocking area, select the validity.

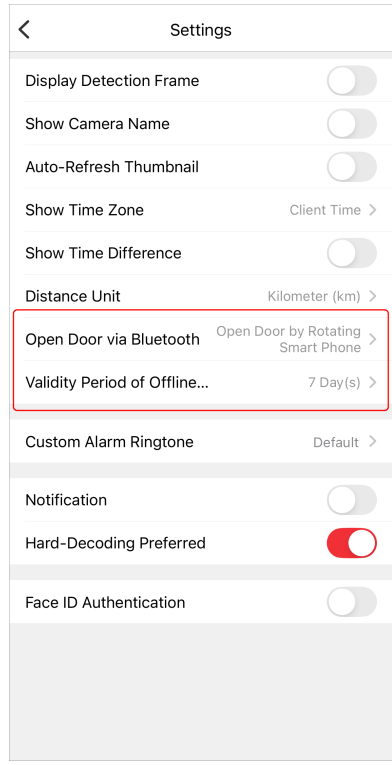



**Figure 23-13 Admin Account**

## Step 4 Open Door via Bluetooth on the Mobile Client

After completing the above steps, you can open the door via Bluetooth on the Mobile Client according to the selected mode.

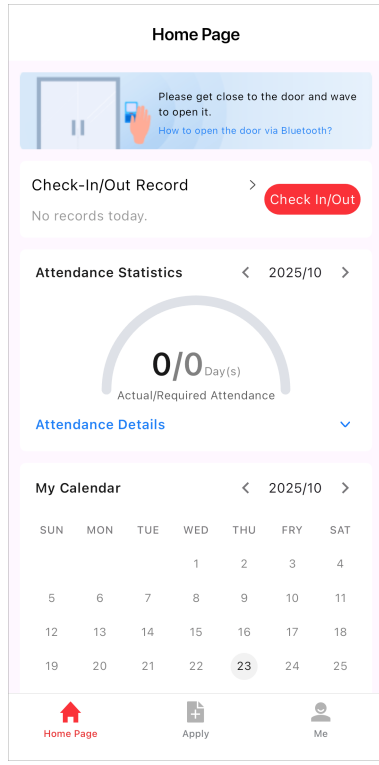



**Figure 23-14 Wave to Open Door**

## Step 5 View Real-Time Events and Search History Access Records

The operation of opening door via smart phone may trigger configured events. You can find the access event in the Real-Time Event area on the Real-Time Monitoring page.
Or click to search for history access records stored on the device.

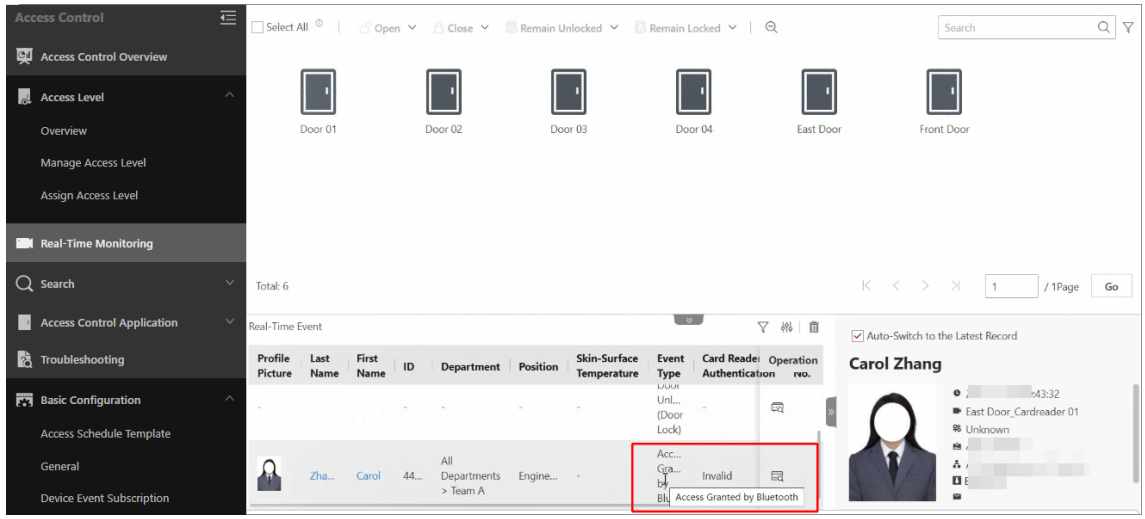



**Figure 23-15 View Real-Time Events**

## 23.6 Real Time Monitoring

With batch locking and unlocking group, you can control access point status in a batch when an emergency happens. For example, after grouping the access points of a school's main entrances and exits into one group, school's security personnel can lock down the access points in the group, so that no one can enter or leave the school except for maintenance and high-level admins. This function can also block out teachers, custodians, students, etc. In addition, you can also start live view of devices and view real-time access events.

**Note**

- Make sure you have grouped access points into a batch locking and unlocking group. See details in ***Add a Batch Locking and Unlocking Group*** .
- Only the users with Administrator or Operator role can control all access points in a batch.

On the left, select **Real-Time Monitoring**.

You can control all or part of the access points in the selected site and area according to your need. When the emergency is over, you can restore the status to Access with Credential.

On the top right, click to select a site and area.

### Start Live View of Access Control / Floor Control Devices

For access control devices with cameras installed inside or linked outside, and elevator control devices linked with cameras, you can start live view of these devices.

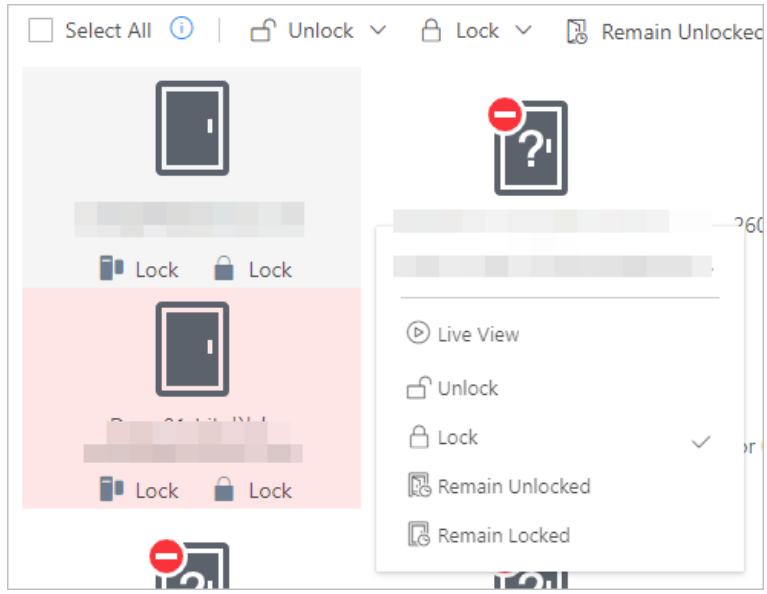



**Figure 23-16 Real-Time Monitoring Page**

## View Real-Time Access Event

In the Access Control module, you can view events triggered by doors and floors.
Make sure you have subscribed to device and access events. Go to **Basic Configuration → Device Event Subscription → Device Event / Normal Access Event / Abnormal Access Event** . Enable the event types you want to subscribe to and disable those you don't need. You can still search for device/access records via the Web Client. See ***Data Search*** .
Select the site and area that you want to view the access events. Real-time access events are displayed at the bottom of the page.

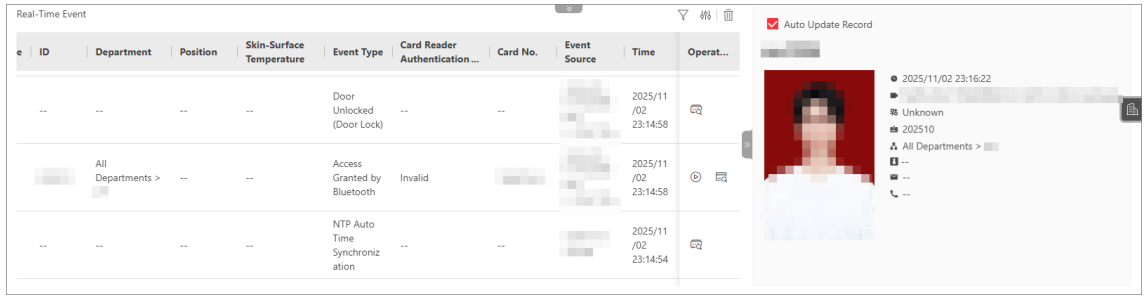



**Figure 23-17 Real-Time Access Event**

| | |
|---|---|
| Search for Device Records | Click in the Operation column to go to the Device Recorded Data Retrieval page to search for records by customizing search conditions. |
| Filter Events | You can filter the real-time events by setting conditions according to record types and event source. Click to set conditions. |
| Custom Column | Click to customize the columns to be displayed. |
| Clear Events | Click to clear all events in the list. |
| View Details of Latest Access Record | On the lower-right corner of this page, check **Auto Update Record** to display the person/ visitor information contained in the newest access record. If you uncheck the **Auto Update Record**, the platform will display the person/ visitor information contained in the historical access records. The platform supports hiding the window. |

## Door & Barrier Control

For doors and barrier gates, you can change their status or those in specific batch locking and unlocking groups to locked, unlocked, remaining locked, or remaining unlocked.

Only online doors and barrier gates will have their status updated when batch changing to remain locked or unlocked, while offline ones will retain their current state.

**Unlock**

When a door or barrier gate is unlocked, persons can pass the door or barrier gate without any credentials for a certain time period. When open duration is over, the door or barrier gate will be closed and locked again automatically.

Select a door or barrier gate and click **Unlock** to unlock a door or barrier gate or click **Select all** to unlock all doors or barrier gates.

Click **Unlock → ⌄ → Unlock Access Points in Batch Locking and Unlocking Group** to unlock doors or barrier gates in the batch locking and unlocking group you have added.

**Note**

For details about setting the door's open duration, see ***Parameters on Edit Door Page*** .

**Lock**

When the door or barrier gate is locked, persons who has the access permission can access the door or barrier gate with credentials.

Select a door or barrier gate and click **Lock** to lock a door or barrier gate or click **Select all** to lock all doors or barrier gates.

Click **Lock → ⌄ → Unlock Access Points in Batch Locking and Unlocking Group** to lock doors or barrier gates in the batch locking and unlocking group you have added.

**Remain Unlocked**

Doors or barrier gates will be unlocked. All persons can access the door or barrier gate with no credentials required. This function is used when an emergency happens and all people are required to leave as quickly as possible, such as in a fire escape.

Select a door or barrier gate and click **Remain Unlocked** and the door or barrier gate will remain unlocked. Click **Select all** and all the doors or barrier gates will remain unlocked.

Click **Remain Unlocked → ⌄ → Remain Access Points Unlocked in Batch Locking and Unlocking Group** and the doors or barrier gates in the batch locking and unlocking group you have added will remain unlocked.

**Remain Locked**

Doors or barrier gates will be closed and locked. No person, except for the users with super access permission, can access the door or barrier gate even with authorized credentials. This function is applicable for situations such as preventing unwanted persons in the building from getting away.

Select a door or barrier gate and click **Remain Locked** and the door or barrier gate will remain locked. Click **Select all** and all the doors or barrier gates will remain locked.

Click **Remain Locked → ⌄ → Remain Access Points Locked in Batch Locking and Unlocking Group** and the doors or barrier gates in the batch locking and unlocking group you have added will remain locked.

## Sliding Gate Opener Control

With sliding gate openers, you can change their status to locked, unlocked, locked open, etc
For more parameter settings such as opening and closing speed, please go to the device configuration page of sliding gate opener.

**Trigger**

Toggles the opener's operation. When stationary, it starts moving in the opposite direction (Open ↔ Close). When moving, it stops immediately. For example:

1. Gate is closed and stationary → Trigger → Gate starts opening.
2. Gate is opening (moving) → Trigger → Gate stops immediately.
3. Gate is now open and stationary → Trigger → Gate starts closing.

Select a gate opener or click **Select all**, and click .

**Pedestrian**

The door starts from a stationary state, moves automatically to a preset half-open position, and then stops. Suitable for short-term passage scenarios.

Select a gate opener or click **Select all**, and click to change the gate opener's or all gate openers' status to half open.

**Lock**

Locks the gate opener in its current state (e.g., closed, partially open, or fully open). Once locked, only the **Unlock** command is valid.

Select a gate opener and click to lock it or click **Select all** to lock all.

**Unlock**

Removes the **Lock** state, restoring normal gate opener control functionality.

Select a gate opener and click to unlock it or click **Select all** to unlock all.

**Locked Open**

The gate opener first moves automatically to the fully open position, then enters a locked state and remains open until the lock is canceled.

Select a gate opener or click **Select all**, and click to change the gate opener's or all openers' status to locked-open.

**Cancel Remaining Open**

Cancels the locked-open state, allowing the gate opener to resume normal operation.

Click to cancel the status of **Locked Open**.

## Floor Control

You can change the status of all floors in a site or floors in specific batch locking and unlocking groups to temporary access, access with credential, free access, or access forbidden.

**Note**

Make sure you have grouped floors into a batch locking and unlocking group. See details in ***Add a Batch Locking and Unlocking Group*** .

Control all or part of floors in the current site.

**Temporary Access**

During the temporary access time, persons can access this floor with no credentials required. After the access time, the floor will recover to Access with Credential status.

Click an elevator, and select **Elevator Control** → → **Temporary Access** to set the floor in the current site to Temporary Access.

**Access with Credential**

Person who has the access permission can access this floor with credentials.

Click an elevator, and select **Elevator Control** → → **Access with Credential** to set the floor in the current site to Access with Credential.

**Free Access**

All persons can access this floor with no credentials required.

Click an elevator, and select **Elevator Control** → → **Free Access** to set the floor in the current site to Free Access.

**Access Forbidden**

No person, except the users with super access permission, can access this floor even with authorized credentials. This function is applicable for situations such as preventing unauthorized persons in the building from getting away.

Click an elevator, and select **Elevator Control** → → **Access Forbidden** to set the floor in the current site to Access Forbidden.

## 23.7 Data Search

On the Search page, you can search for person authentication records, data recorded on devices, and perform final authentication counting.

On the left, select **Search**.

**Note**

You can go to **Basic Configuration → General → Apply to Device (Scheduled) / Synchronize Records (Scheduled)** to enable the feature of synchronizing access records and device logs to the platform on schedule.

## Search Access Records

On the Person Authentication Record page, you can search for persons' authentication records triggered on specified access points by setting search conditions. For example, if you select specific access points and set the event type to access denied by card, you can get all access denied events (accessing by swiping a card) triggered on the access points.

**Note**

Make sure you have configured the access point event.

You can import person authentication records to the system from devices or files. Go to **Import Event → Import From Device / Import From File** .

**Import From Device**

- If the device has uploaded records to the system before, switching on **Specified Time Range** is not required and records during the past 7 days of the selected device(s) will be imported by default if no time range is specified.
- If the device has never uploaded any record to the system before, you must switch on **Specified Time Range** for importing records from the selected device(s).

**Import From File**

Import from the file which is exported from the device. Only the encrypted file can be imported.

**Table 23-4 More Operations**

| Operation | Description |
|---|---|
| View Record Details | Click the person name in the Full Name column to view the record details, such as person information, access information, alcohol detection, etc. |
| Forgive Anti-Passback Violation | When a person attempts to use a card without following the anti-passback rule, the access will be denied. This is called "Anti-Passback Violation". When the anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.<br>You can click **Forgive Anti-Passback** on the top to forgive all the anti-passback violation events in the search results. |
| Export Single Record | Click in the Operation column to save a record as an Excel or CSV file on your PC, including the event details, the person |

| Operation | Description |
|---|---|
| | information, person profile, recorded video file (if configured), etc. |
| Export All Searched Records | Click **Export** in the upper-right corner to save the searched record details in your PC. You can select the file format as an Excel, PDF or a CSV file, and select items to export. |
| Save a Record As Case | Click to save the record to the evidence management center. |

## Search Data Recorded on Device

The logs can be events/alarms triggered by abnormal events detected by devices and those triggered by devices (such as device faults). You can search for the logs in different dimensions according to your needs.

**Access Point(s)**

Access points include doors of access control devices and video intercom devices, and floors of elevator control devices. The logs can be access records, operation records, and alarms triggered by human behaviors.

**Device**

Devices include access control devices, elevator control devices, and video intercom devices. The logs recorded in these devices can cover all events triggered by devices (such as device faults).

**Alarm Input**

The alarm inputs included in devices. The logs are arming status changes.

**Table 23-5 More Operations**

| Operation | Description |
|---|---|
| View Record Details | Click the device name in the Source column to view the record details, such as the device name and record type. |
| Export Single Record | Click in the Operation column to save the record to the local PC as a CSV file. |
| Export All Searched Records | Click **Export** to save all the searched records to the local PC as an Excel, PDF, or a CSV file. |

## View Final Authentication Statistics

The system can count individuals in a region by grouping doors and using final authentication records. This allows you to see who has been granted access and how many people are still in the area. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.
Make sure you have added final authentication counting groups to group the doors. See ***Add a Final Authentication Counting Group*** .

**All Persons**

All the entering and exiting access records in the last 24 hours will be listed.

**People Stayed**

Persons who are still staying in the region will be listed. The system filters the persons whose entering record is found but exiting record is not found.

**People Exited**

Persons who entered and exited the region afterward will be listed.

**Table 23-6 More Operations**

| Operation | Description |
|---|---|
| View Event Details | Click the person name in the Name column to view the record details, including the recorded video of the access point's related camera (if configured), person information, and access information. |
| Export Single Record | Click in the Operation column to download the record, including the person information, person profile, phone number, location of last access, etc. |
| Export All Searched Records | Click **Export** in the upper-right corner to export the searched access control events details (including the person information, person profile, phone number, location of last access, etc.). |

Up to 100,000 records can be exported each time.

# 23.8 Advanced Functions

## 23.8.1 Add Remain Unlocked and Remain Locked Rule

To set access points accessible or inaccessible during certain periods, configure this rule for certain access points.

**Steps**

**Note**

This function should be supported by the device.

1. On the left navigation bar, select **Remain Unlocked & Remain Locked**.
2. Click **Add** to enter the Add Remain Unlocked & Remain Locked Rule page.
   For the first-time configuration, click **Configure Now** in the center of the page.
3. Enter the rule name.
4. Select an access point from the following area list.
5. Select weekly schedule for the access point(s).
6. Click **Add**.
   The system will automatically apply the schedule(s) to devices.

## 23.8.2 Configure First Person In

First Person In refers to a rule where only after the first person is authorized to enter using their card, fingerprint, or face, can other people's permissions be activated. You can set the door opening rule to allow free access after the first person or require authorization by the first person, which is suitable for scenarios such as quick emergency response or personnel access control.

**Steps**

**Note**

This function should be supported by the device.

1. Go to **Access Control Application → First Person In → Add** .
   For the first time configuration, click **Configure Now** in the center of the page to enter the Add First Person In Rule page.
2. Enter the rule name.
3. Select a door from the resource list.
4. Set **Rule of Opening Door**.
5. Set the consecutive authentication times and the interval of consecutive authentication.
6. **Optional:** Enable **First Person Authentication Time** to set a time when the rule takes effect and a fixed time period requiring first person authentication.

7. In the First Person area, click **Add** to select first person(s).

   If you check **Select All**, all persons who matched the search conditions you set will be selected.
8. Click **Add** to add the rule.

   After adding a rule, you can click the rule name to edit the rule.

### 23.8.3 Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and authenticate. It is generally used in places such as bank vault to ensure the security of important assets and data.

On the left, select **Access Control Application → Multi-Factor Authentication** . If any multi-factor authentication rule is added, the multi-factor authentication list will show. You can manage multi-factor groups and users to receive remote door open request. For the first time usage, click **Configure Now** to enter the Add Multi-Factor Authentication Rule page.

**Multi-Factor Authentication Group**

Persons in the group have the permission for multi-factor authentication of specific doors.

**User to Receive Remote Door Open Request**

Configure this when the access mode is Remotely Unlock After Granted.

**Note**

This function should be supported by the device.

### Add a Multi-Factor Authentication Rule

**Steps**

1. On the Multi-Factor Authentication page, click **Add**.
2. Enter the rule name.
3. Select a door from the following area list.
4. In the Access Schedule area, set the time periods in which the persons are allowed to authenticate.

   You can click **Copy From** to copy the access schedule of another rule.
5. Click **Link to Group** to set the access group(s) to define who have the permission to access the door.

   For the first-time configuration, click **Add Group** to create a multi-factor authentication group by selecting persons as the group members.

   **Card Swiping Order**

   Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.

   **Number of Persons for Authentication**

Define how many persons should authenticate.

For example, if you set 3 for access group Security Guard and 1 for access group Bank Manager, it means three security guards should swipe cards on the card reader (or other access mode), and one bank manager should swipe card on the card reader (or other access mode) for this multi-factor authentication.

6. Set the access mode of the door.

**Unlock After Access Granted**

The door will be unlocked automatically after the persons swipe their cards (or other type of credentials) on the card readers of the door and the access is granted.

**Remotely Unlock After Granted**

After the persons authenticate, a window will pop up on the Control Client for the operator. The operator should select whether to unlock the door.

**Unlock by Super Password When Offline**

If the user to receive remote door open request is offline, the persons in the multi-factor authentication group can enter the super password.

**Enter Super Password After Granted**

After the persons swipe their cards (or other type of credentials) on the card readers of the door and the access is granted, they should enter the super password on the card reader. After that, the door will be unlocked successfully.

7. Set the card swiping interval and make sure the interval between two authentications on the card reader is within this value.

**Example**

When you set the interval as 5s, if the interval between two authentications is longer than 5s, the authentications will be invalid, and you should authenticate again from the beginning.

8. Click **Add**.
9. **Optional:** If you select **Remotely Unlock After Granted** as the access mode, click **User to Receive Remote Door Open Request** above the multi-factor authentication list to add users who are going to receive the request.

## 23.8.4 Configure Multi-Door Interlocking

Multi-door interlocking is used to control the entry of persons to a secure area such as a clean room, where dust or small particles may cause a major issue. One multi-door interlocking group is composed of at least two doors and only one door can be opened simultaneously.

**Before You Start**

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

**Steps**

1. Go to **Access Control Application → Multi-Door Interlocking → Add** .

For the first time configuration, click **Configure Now** in the center of the page.

2. Create a name for the group.
3. Select doors and click › .
4. Click **Add**.

   After adding a group, you can click **Set Geographic Location** to view the real-time alarms triggered in the region. For details, see ***Add Geographic Area to Map*** .

## 23.8.5 Configure Anti-Passback

The anti-passback is designed to minimize the misuse or fraudulent use of access credentials such as passing back the card to an unauthorized person, or tailed access. Only one person can pass the access point after authentication. This function is mainly used for enhanced access security of some important or specific places (e.g., laboratories, offices).

You can configure area anti-passback rules or route anti-passback rules for different scenarios. Go to **Access Control Application → Anti-Passback → Area Aniti-Passback / Route Anti-Passback** .

### Area Anti-Passback

A person with an entry record must also have an exit record to re-enter or exit the area. The area anti-passback function creates a specific door group. For example, when a person enters the area by swiping a card, they must exit through a door in the same group. If they exit without swiping at a door in the group, they cannot re-enter through any door in the group.
Make sure you have added the access points to different areas. For details, refer to ***Add Element to Area*** .

**Control Anti-Passback by Device**

Control anti-passback by selecting specific doors through which people are allowed to enter and exit.

Suitable for general environments. For example, a small office building with a few entry and exit points, where the security system needs to ensure that employees enter and exit through designated doors.

For the 260X series access controllers, you can configure multiple distinct anti-passback rules for interconnected doors. For instance, if the controller is linked to four doors, you can establish one rule governing door 1 and door 2, while applying a separate rule to door 3 and door 4.

**Control Anti-Passback by Platform**

Control anti-passback by the rules set by the platform. By setting a rule that requires specified personnel to enter and exit through the same door during fixed time periods, you can ensure that only authorized personnel access these areas during the specified times. For example, from 8 PM to 6 AM every day, only specific on-duty personnel can enter and exit the data center, and they must do so through the same door.

If you select this option, check **Enable Rule Now**. In the **Rule Configuration** step, you can:

- Select persons who should enter and exit through the same door.
- Select doors through which people are allowed to enter and exit.
- Specify the times during the week when people should follow the entry and exit order.

**Select Door**

Select doors by which people are allowed to enter and exit. You need to assign entry/exit readers with either combination: Card Reader 01 (Entry) + Card Reader 02 (Exit) or Card Reader 02 (Entry) + Card Reader 01 (Exit).

**Allow Multiple Exits per Entry**

Only available when selecting **Control Anti-Passback by Device**. If you check it, a single entry can be associated with multiple exits, i.e., Entry A → Exit C/D.

## Route Anti-Passback

Persons must authenticate through a configured sequence of doors in one direction. The route anti-passback depends on the card swiping route. Set up a card reader sequence for access control, defining initial and subsequent card readers to enforce anti-passback based on stored entry and exit data.

**Control Anti-Passback by Device**

Control anti-passback by setting the card reading order people should follow for entry and exit.

Suitable for general environments. For example, you need to ensure that employees enter and exit through designated route from Card Reader 1 to Card Reader 2.

**Control Anti-Passback by Platform**

Control anti-passback by the rules set by the platform. By setting a rule that requires specified personnel to enter and exit in a specific order during fixed time periods, you can ensure that only authorized personnel enter and exit these areas in the correct sequence during the specified times. For example, during an event, staff must enter and exit the event area through multiple doors in a specified order, ensuring the safety and order of the event.

If you select this option, check **Enable Rule Now**. In the **Rule Configuration** step, you can:

- Select persons who should enter and exit through the same door.
- Set the order that people follow for entry and exit.
- Specify the times during the week when people should follow the entry and exit order.

**Card Reader Order**

Set the order that people follow for entry and exit. The direction indicated by the arrow represents the direction of entry and exit.

**First Card Reader**

Set the first card reader in the route to the first card reader. If you violate the route anti-passback rule, you should swipe the card again from the first card reader.

## Shared Parameters

**Forgive Anti-Passback Violation Regularly**

Set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.

**Non Anti-Passback Period**

Set a fixed time during which persons can access the area without following the rule. This function should be supported by the device.

**Edit Anti-Passback Group**

Click the group name to edit the anti-passback group settings.

You can edit the name of the group, add or delete doors in the group, change the settings of forgiving anti-passback violation regularly, and edit the locations of the group and doors on the map.

**Set/Cancel Forgiving Anti-Passback Regularly**

Select the group(s), click **Set Forgiving Anti-Passback Regularly**, and specify a fixed time so that the platform can automatically forgive the anti-passback violations occurred in the selected anti-passback group(s) at that time everyday.

You can also select the group(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected group(s).

## 23.8.6 Add a Batch Locking and Unlocking Group

The batch locking and unlocking group is a group for access points which need to be controlled in a batch. This function is mainly applicable for emergent situations. You can add doors of access control devices, doors of video intercom devices, and floors of elevator control devices to the group.

**Before You Start**

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

**Steps**

1. Go to **Access Control Application → Batch Locking and Unlocking Group → Add** .

   For the first time configuration, click **Configure Now** in the center of the page.
2. Create a name for the group.
3. In the Access Point area, select the access points and click › to add them to the group.
4. Click **Save**.

## 23.8.7 Add a Final Authentication Counting Group

The final authentication counting group is used to group the access points in a certain area. You can set certain access points as the region edge. Only the number of persons accessing these access points are counted. By grouping these access points, the platform provides counting functions based on the entry and exit records on these access points. With this function, you can know who enters/exits this region and how many persons still stay in this region. This is applicable

for certain emergency scenes. For example, during a fire escape, the number of the remaining/ stayed-in persons and name list are required for rescue.

**Before You Start**
Add the access points into different areas. For details, refer to ***Add Element to Area*** .

**Steps**
1. Go to **Access Control Application → Final Authentication Counting Group → Add** .
   For the first time configuration, click **Configure Now** in the center of the page.
2. Create a name for the group.
3. Click **Add** and select doors from the area list.
4. Set the entering or exiting direction of the card readers of the selected access points.
5. Click **Save**.
   After adding a group, you can click **Set Geographic Location** to view the real-time number of people entered, exited or stayed in the region. For details, see ***Add Geographic Area to Map*** .

**Result**

After adding final authentication groups, you can view final authentication statistics. See ***View Final Authentication Statistics*** .

## 23.8.8 Configure Authentication Mode

The authentication mode is used to determine whether a person has the permission to pass the access point by using single or multiple authentication modes (e.g., employee ID, face, fingerprint, password, PIN code, or a combination of them). You can set the reader authentication mode for access points or set the private authentication mode for persons. If a device has been configured with different authentication modes by two methods, the person's private authentication mode has higher priority than the reader authentication mode.

### Set Reader Authentication Mode

You can set the reader authentication mode to employee ID, password, face, fingerprint, PIN code, or a combination of them in normal time periods or custom time periods according to your actual need.

**Before You Start**
Make sure you have added doors to the area. See ***Add Element to Area*** for details.

**Steps**

**Note**
This function should be supported by the device.

1. Go to **Access Control Application → Authentication Mode → Card Reader Authentication Mode** .
2. Select an area from the area list, and doors in that area will be displayed on the right.
3. Click a door name on the right.
4. Select the Card Reader Authentication Mode Settings.

   **Batch**

   Set the same reader authentication mode for all the readers of a door.

   **Single**

   If you want to set different reader authentication modes for different readers, select this mode.
5. Select the Card Reader Authentication Mode.

   **Reader Authentication Mode**

   Set the reader's authentication mode in normal time periods. For example, if you select **Card**, persons on the platform should open the door by swiping the card for authentication each time.

   **Reader Authentication Mode (Custom)**

   When you want persons on the platform to open the door via another authentication mode in some special time periods, you need to set the reader's authentication mode and select the custom time period. For example, if you select **Fingerprint** and **Weekend Template**, persons on the platform should open the door via fingerprint at weekends.
6. **Optional:** Click **Copy To** in the upper-right corner to apply the settings to other doors.
7. Click **Save**.

## Set Person Private Authentication Mode

You can set private authentication methods (such as card, fingerprint, etc.) for different persons. The person's private authentication mode has higher priority than the existing authentication mode of the device. This is suitable for the following two scenarios, allowing for more flexible and secure personnel management: different persons can use different authentication modes for accessing the same access point and a person can use different authentication modes for accessing different access points.

**Steps**

1. Go to **Access Control Application → Authentication Mode → Private Authentication Mode** .
2. Select a department from the left list.

   All persons in the department will be listed on the right panel.
3. Click in the Operation column to open the Authentication Device pane.
4. Click **Add**, check the device(s) from the list, and select the authentication mode from the drop-down list for the selected device(s).
5. Click **OK** to add the device(s) for authentication for the person.

6. **Optional:** Perform one of the following operations to edit the authentication mode(s) for the device(s).
   - Select an authentication mode from the Authentication Mode drop-down list to configure the authentication mode for each device.
   - Click **Batch Configuration**, select an authentication mode from the drop-down list, and click **Save** to configure the same authentication mode for all added devices.
7. **Optional:** In the Private Authentication Mode page, click in the Operation column, select the person(s), and click **OK** to copy the person's private authentication mode settings to another person or other persons.

**Result**

The number of devices added for each person is displayed in the Device for Authentication column. You can click beside the number to view names and authentication modes of all devices.

## 23.8.9 Apply Advertisement to Access Control Devices

You can add picture(s), video(s), and text(s) in the advertisements, then apply the advertisements to access control devices. After applying advertisements, you can filter or delete them.

**Steps**

1. Go to **Access Control Application → Apply Advertisement → Apply Advertisement** .
2. Select the available door station in the left list and click to add it to the right list. You can click to remove it from the selected door station list on the left.
3. Add materials (picture, video, or text) for an advertisement to be applied to access control devices.

**Note**

- The material type (picture, video, or text) should be supported by devices.
- You can check two types of advertisement materials at the same. For example, you can check both picture and video at the same time, excluding text.
- You can add up to 8 videos and pictures, or 3 texts at one time.

- a. Click **Picture →** to add picture(s) for an advertisement.
  b. Set the duration for pictures switching interval.
  c. Set the time period to play the added picture(s).

  **Note**

  Up to 2 time periods are allowed. You can click **Add** to add the time period if needed.
- a. Click **Video →** to add a video for an advertisement.
  b. Set the duration for videos switching interval.
  c. Set the time period to play the added video.

a. Click **Text** → + to add a text for an advertisement.
b. Set the advertisement texts, including uploading the background picture, setting the text title/font size/color, and selecting the layout style.
c. Set the time period to play the added texts.

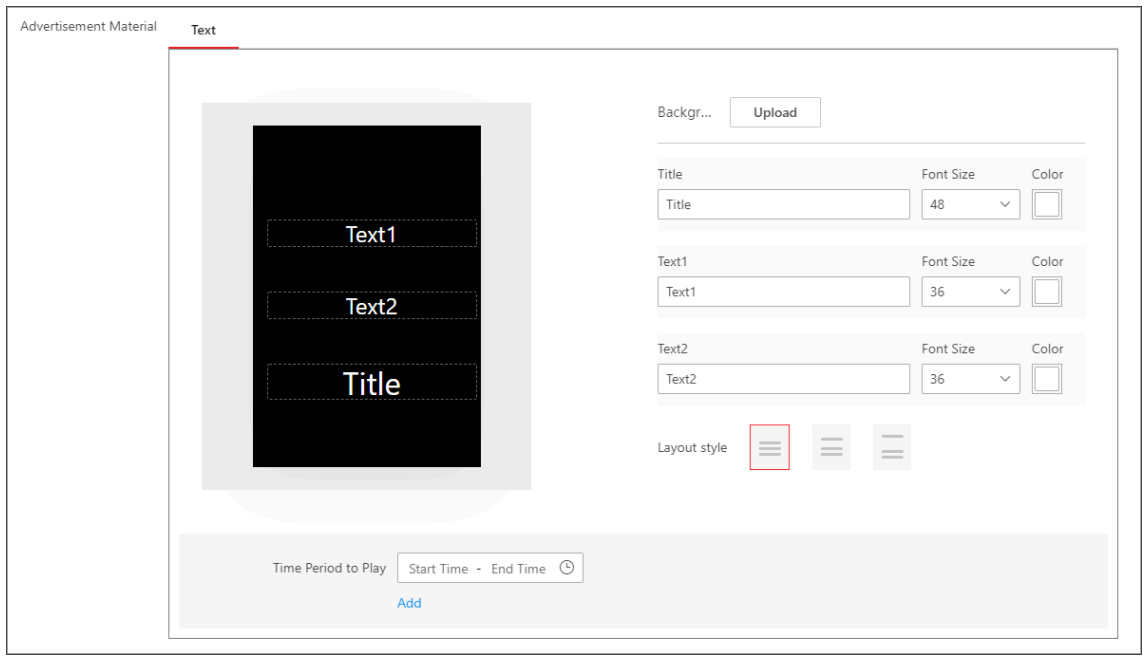



**Figure 23-18 Add Text in Advertisement**

4. The playing schedules set for the picture(s), video(s), and text(s) in the advertisement will be displayed by different color blocks.
5. Switch on **Sleep**, and set the sleep duration (from 20 to 60 seconds). For example, if you set the sleep duration to 20 seconds with three videos added, each video played will be followed by a 20-second pause.
6. Click **Apply**.
7. **Optional:** Perform the following operations.

| | |
|---|---|
| **Filter Advertisement** | Click and set filter conditions such as device name, and then click **Filter** to filter the target advertisement. |
| **Delete Advertisement** | Select one or multiple advertisements in the list and click **Clear Advertisements** to delete the advertisements. Also, you can click **Delete All** to delete all of the advertisements. |
| **Copy Advertisement** | Select one advertisement in the list, click in the operation column to copy the current advertisement to other devices. |
| **View Details** | Select one advertisement in the list, click to view the details of applying progress. |

## 23.8.10 Add Audio Broadcast

You can add daily audio broadcasts for regular use and particular broadcasts for holidays or special days after the authentication of persons. These broadcasts of the devices can be tailored to meet providing routine, holiday, or special date announcements (e.g. broadcast **Access Granted** when the authentication result is **When Access Granted**. After creating the broadcasts, you can apply them to the selected devices.

**Steps**

1. Go to **Access Control Application → Audio Broadcast → Add Audio Broadcast** .
2. Select the broadcast device(s).
3. Enable the daily broadcast. Audio broadcasts will be played according to the specified timetable on days without particular broadcasts.

   **Note**

   For the two types of authentication result, 4 time periods in total can be added.

   1) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
   2) Set the broadcast time and content.
      - Click **Add** to add new broadcast time and content.
      - Click to create a copy and set the time and content based on the existing one.
4. In the Particular Broadcast area, click **Add** to add particular broadcasts. Audio broadcasts will be played according to the specified timetable on holiday or specified dates.

   **Note**

   For the two types of authentication result, 4 time periods in total can be added.

   1) Select the particular day type.
   2) Select the holidays(s) or select the specified day(s).

      **Note**

      - If the specified days overlap the holidays, the broadcasts for specified days will be played.
      - Click **Add** to add new holidays. For details, refer to ***Set Holiday*** .

   3) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
   4) Set the broadcast time and content.
      - Click **Add** to add new broadcast time and content.
      - Click to create a copy and set the time and content based on the existing one.
   5) Click **Save**.
5. Click **Add**.

   The settings will be applied to the selected device(s).
6. **Optional:** After applying, perform the following operations as needed.

   **View Device Details** Click the device name to view the broadcast details of the device. You can also edit the broadcast settings to apply for another time.

| | |
|---|---|
| **View Broadcast Details** | Click to view broadcast details. |
| **Copy Broadcast Settings to Other Devices** | In the operation column, click to select the device(s) to copy to. Click **Copy** and the settings will be applied to the selected device(s). |
| **Apply Failed Broadcast to Device** | • At the top of the broadcast list page, click **Details** to view failure details or click **Apply Again**.<br>• In the Operation column, click to apply again. |
| **Delete Broadcast of Device** | Check the device(s) and click **Delete** to delete the broadcast(s) of the selected device(s). You can also click → **Delete All** to delete the broadcasts of all devices. |

## 23.8.11 Add an Authentication Password

You can set an authentication password for a person so that they can access the devices by entering the authentication password. This ensures that only authorized personnel can enter specific areas, such as offices and warehouses, or that strict access control is implemented for certain areas.

**Before You Start**

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

**Steps**

1. Go to **Access Control Application → Authentication Password → Add** .
2. If there are cards without PIN, select **Auto Generate** or **Enter Manually** to automatically generate or enter an authentication password manually.

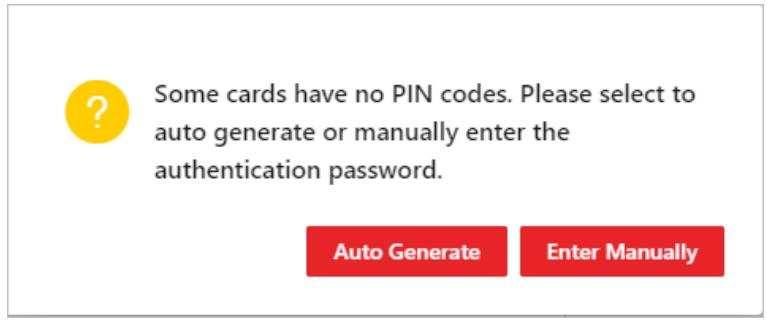



**Figure 23-19 The Prompt**

3. **Optional:** Enter the authentication password for persons whose authentication password is empty, or check persons and then click **Auto Generate Authentication Password**.
4. Select devices in the following list.

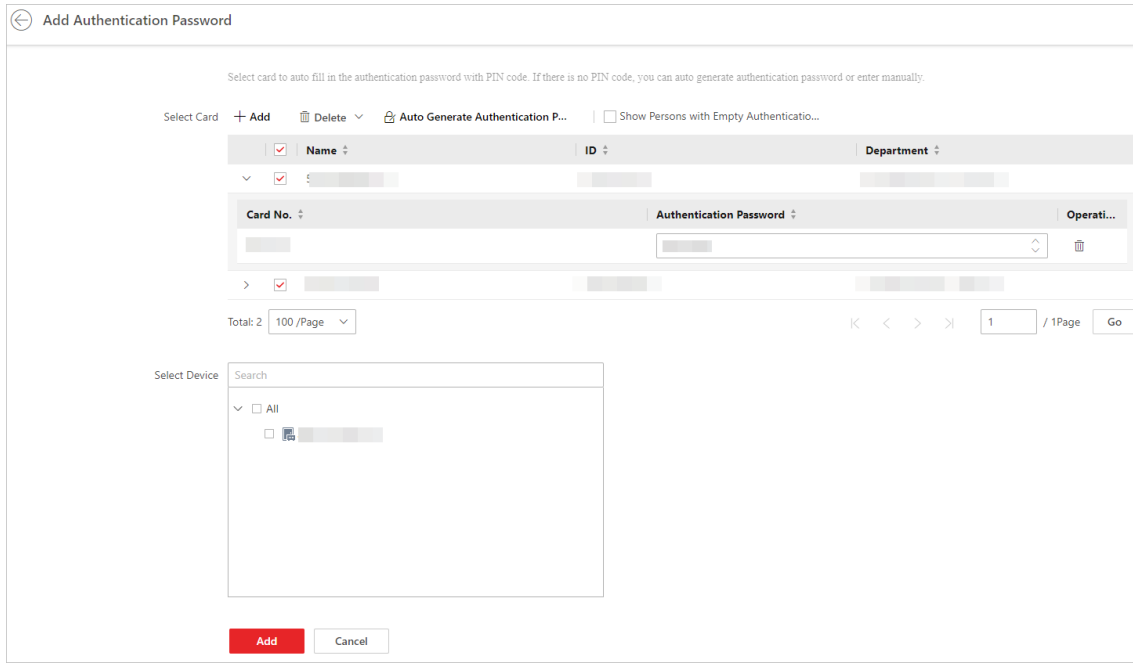



**Figure 23-20 Add Authentication Password Page**

5. Click **Add**.

   The platform will automatically apply the authentication passwords to the selected devices, and the applying progress will be displayed.
6. **Optional:** Check persons and click **Batch Edit Linked Devices** to batch add or delete devices they can access via authentication password.

## 23.8.12 Sync with Access Module

Apply persons to access modules to allow normal access of the persons even if these access modules are offline.

Go to **Access Control Application → Sync with Access Module → Configure Now / Add** .

Select persons and linked access modules.

**Note**

Up to 5,000 persons/cards can be selected.

After applying persons to access modules, you can delete them or delete access modules. The **Apply Full** mode is applicable to the first time deployment. In full application, all access levels configured on the device will be cleared first and the access levels on the platform will be applied.

## 23.9 Access Control Test

HikCentral Professional provides **Access Control Test**. It is a tool through which you can test whether the configurations about access control (such as persons' credentials and access levels for access control and video intercom) are set correctly and completely and whether the devices are running properly.

Select **Troubleshooting** on the left.

### Check Credential Status

Select the **Credential Status** tab to view the status of the added credentials.

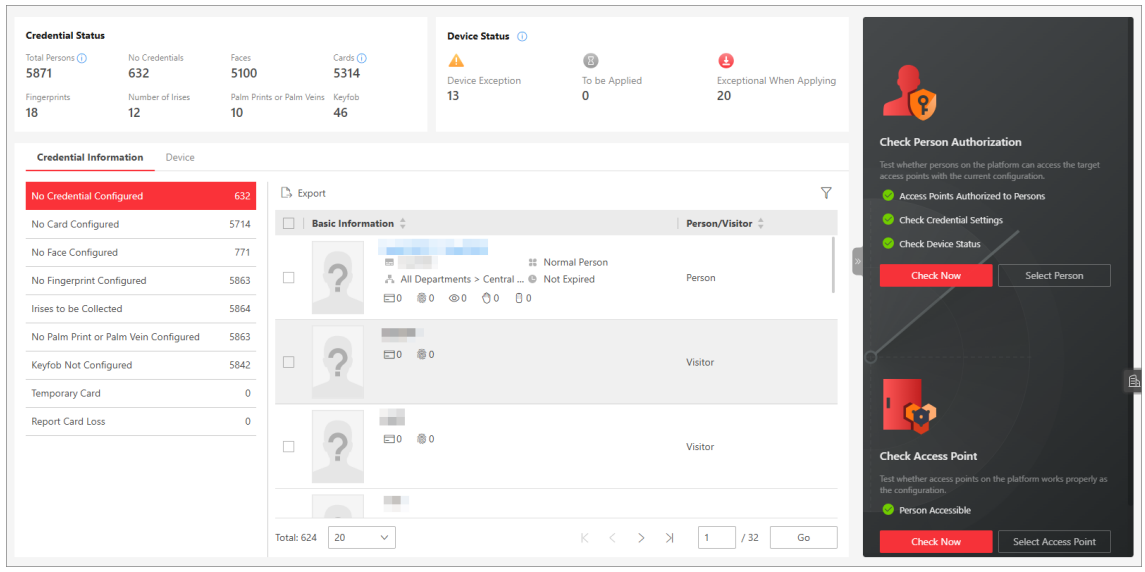



**Figure 23-21 Credential Status**

There are 9 types of exceptions on credential settings in the system. The number next to each exception type indicates the number of persons and visitors whose credential settings are abnormal.
Click each exception type to view the information about the persons and visitors with exceptions. You can click the person's name to edit the credentials if necessary.

### Check Device Status

Select the **Device** tab to view the status of the devices (including access control devices, elevator control devices, and video intercom devices). You can check person information and credential information that are already applied to the devices, configured in the system, fails to be applied, and check information of persons to be applied to the devices.

**Note**

Only the status of the devices which have been configured with access levels are shown.

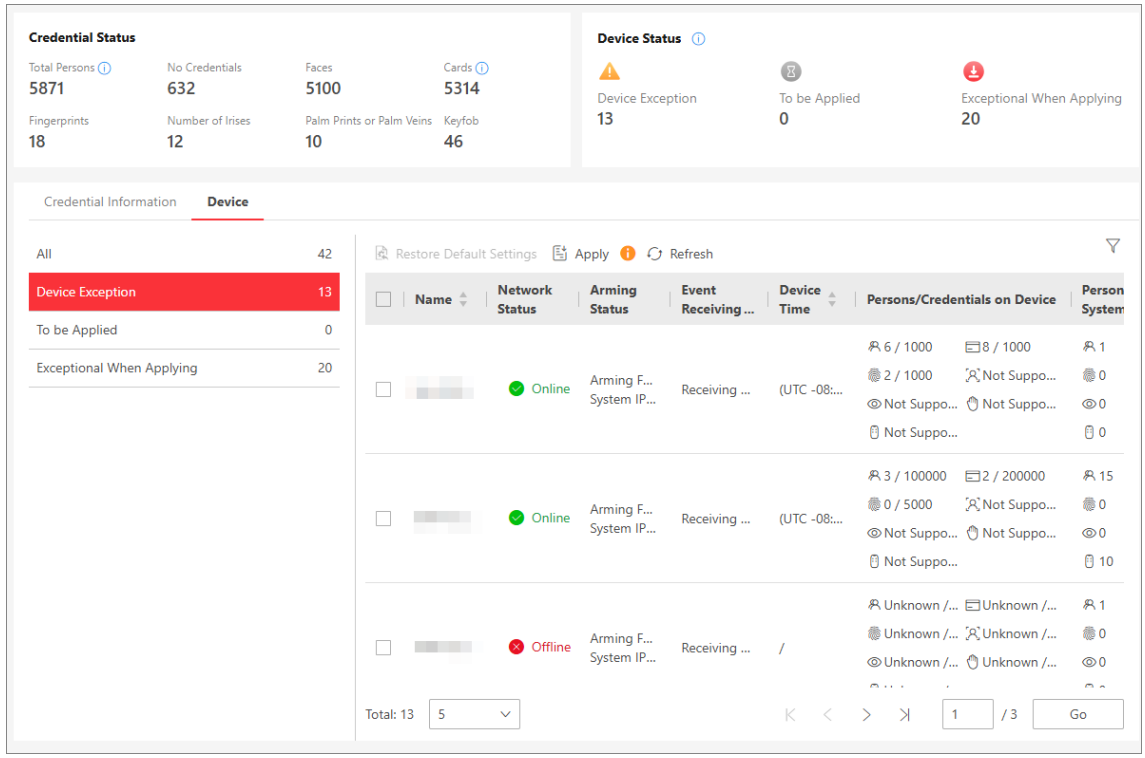



**Figure 23-22 Device Status**

Click each exception type to view the information about the persons and visitors with exceptions. You can select the devices and click the following buttons to solve device issues.

| | |
|---|---|
| **Restore Default Settings** | Restore the settings on the devices to the default value. |
| **Apply** | Apply person information and credential settings to these devices again. |
| **Refresh** | Refresh the list to get the latest device status. |

## Check Authorization Settings of Persons/Visitors

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specific persons or visitors in the system. This function helps you to test whether the persons can access the target access points according to the current settings.

Click  to expand the side panel.

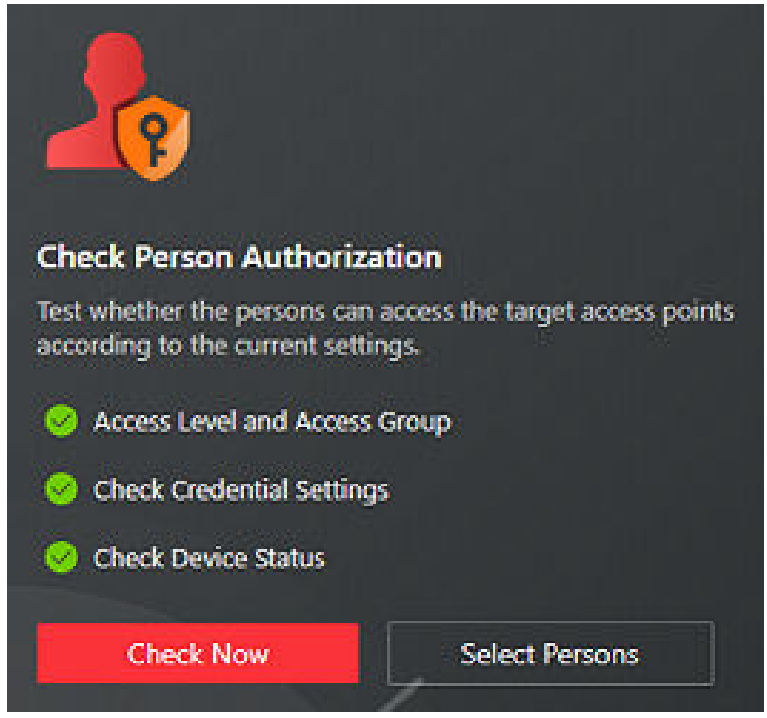



**Figure 23-23 Check Authorization Settings**

In the **Check Person Authorization** section, select the item(s) you want to check.
Click **Check Now** to test the authorization settings of all existing persons and visitors.
Or click **Select Persons** to select the persons or visitors you want to test and then click **Check Now** to test the authorization settings of the selected persons or visitors.

## Check Access Point Settings

You can test whether the persons can access the access points according to the settings in the system.

Click « to expand the side panel.

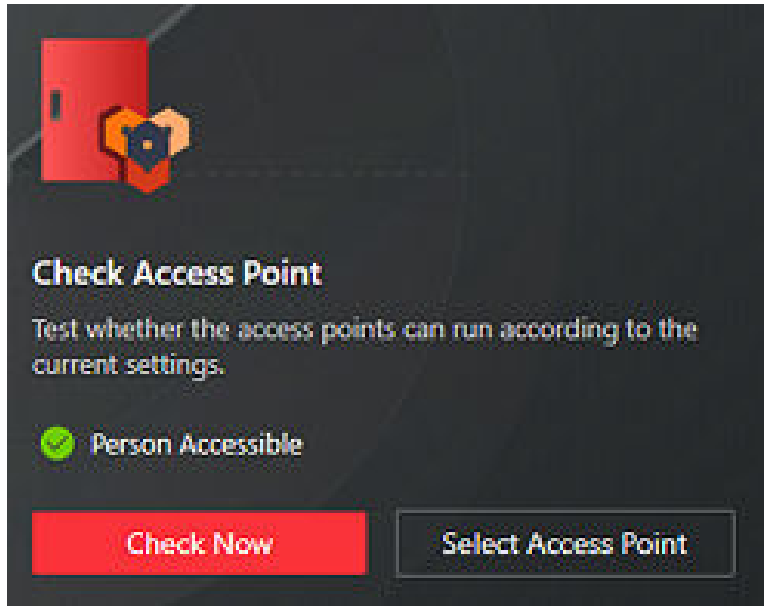



**Figure 23-24 Check Access Point Settings**

In the **Check Access Point** section, select the item(s) you want to check.
Click **Check Now** to test the settings of all existing access points in the system.
Or click **Select Access Points** to select the access points you want to test and then click **Check Now** to test the settings of the selected access points.

**Note**

The access points which are not added to any access levels will not be checked.

# Chapter 24 Video Intercom Management

Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and cameras at both sides, it enables the intercommunication via video and audio signals and provides a safe and easy monitoring solution for apartment buildings and private houses.

On the Web Client, you can add video intercom devices to the system, group resources (e.g., doors and cameras) into different areas, configure call schedules, link resources (cameras, persons, and doorbells) with indoor station, manage notices, call indoor stations, and view recents. After settings related parameters, the person can view the live video of the camera, call indoor station, answer call via Control Client, etc.

In the top left corner of Home page, select → **Passing Management** → **Video Intercom** .

## 24.1 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

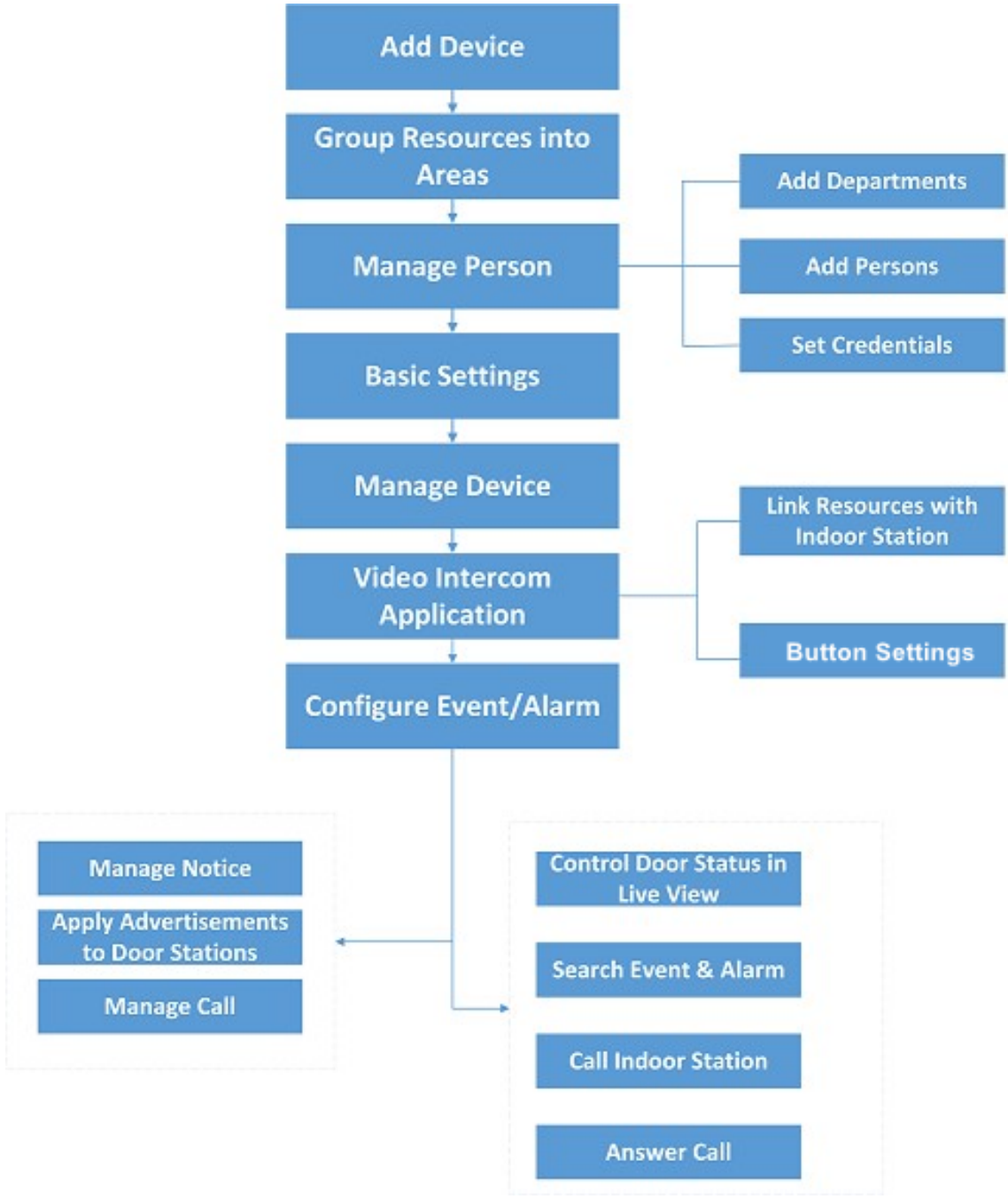



**Figure 24-1 Flow Chart of Video Intercom**

- **Add Device**: Add video intercom devices (such as main station, outer door station, indoor station, and door station) to HikCentral Professional and configure device parameters remotely.
- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors) into different areas according to the resources' locations.
- **Manage Person**: Add departments and persons to the system, and set credential information.

- **Basic Settings**: Add call recipients, add call schedule templates, add receiving schedule template, and configure call parameters.
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices.
- **Video Intercom Application**: Add call schedules and apply them to devices, add button settings for indoor stations, link resources (camera, person, and doorbell) to indoor stations.
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources.
- **Manage Notice**: Add notices and apply them to indoor stations.
- **Apply Advertisements to Door Stations**: Apply pictures or video to door stations as advertisements.
- **Manage Call**: Call indoor stations and view recents.
- **Operations on Control Client**: After the above configurations on the Web Client, you can control door status during live view, search event and alarm, call indoor station and answer call. For more details, refer to *User Manual of HikCentral Professional Control Client*.

**Note**

The doors of video intercom device can be used similarly as the doors of access control device.

## 24.2 Add Video Intercom Device

Device Management

1. Select **Device Management** on the left.
2. Select **Add** or ⌄ → **Batch Add** to set the basic information and location information. For example, when entering location values like:
   - **Number of Management Areas**: 8
   - **Building No.**: 8
   - **Block No**.: 1
   - **Floor**: 0
   - **Room No.**: 909

     The system will display the consolidated format as: 8#8#1#0#909 (Area 8#Building 8#Unit 1#Floor 0#Room 909).
3. Select **Apply Settings**, select devices and the applying mode, and select **Apply** to apply the location information to devices.

## 24.3 Configure Device Parameters

After adding the video intercom devices, you can configure parameters for them remotely, including device time, maintenance settings, etc.

After adding a video intercom device, click ⚙ in the **Operation** column to configure the device.

**Note**

The parameters may vary with different models of devices.

## Time

You can view the time zone where the device locates and set the following parameters.

**Device Time**

Click **Device Time** field to customize time for the device.

**Sync with Server Time**

Synchronize the device time with that of the SYS server of the system.

## Call Management Center

For door station, you can set this function switch to on and select a shortcut button. When the configured button on the device is pressed, it will call management center. The default button is 1.

**Note**

This should be supported by the device.

## Card Swiping

For outer door station and door station which supports M1 encryption, you can enable **M1 Encryption** and select the sector. Only the card with the same encrypted sector can be granted by swiping the card on the card reader.

## Related Cameras

For indoor station, you can relate the camera(s) with it to view the video of the related camera(s) on the indoor station. You can also delete the related camera(s). Up to 16 related cameras are supported.

## Maintenance

You can reboot a device remotely, and restore it to its default settings.

**Reboot**

Reboot the device.

**Restore Default**

Restore the device to its default settings. The device should be activated after restoring.

## More

For more configurations, you can click **Configure** to go to Remote Configuration page of the device.

## 24.4 Button Settings

You can add a call schedule for a door station to configure when door stations can call indoor stations or management centers. You can also assign frequently used functions (e.g., Call, Live View, Open Door) to custom buttons, streamlining centralized management.

### 24.4.1 Add Call Schedules for Door Stations

You should add call schedules for door stations and apply these schedules to devices.

On the top navigation bar, select **Video Intercom Application → Button Settings → Door Station → Add** .

Select a door station in the list and configure call schedules. You can click ⌄ **→ Add Call Schedule Template** to set the template name, weekly schedule template, and holiday schedule, and select a room number for each button.

**Copy from**

Select an existing template from the drop-down list. For adding call schedule templates, see ***Make and Receive Calls on Platform*** .

**Indoor Station / Management Center**

Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.

**Note**

If you configure a template for a management center, the Room cannot be selected.

**Draw Task Time**

Click a grid or drag the cursor on the time line to draw a time period during which the task is activated.

**Set Precise Time**

Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as 

.

**Add Holiday**

Select an existing holiday template, or select **Add** to add a new template.

After adding schedules, select **Apply Settings** to apply call schedules to devices in the door station list.

To add call templates to devices in a batch, select **Batch Import Call Schedule → Download Template** , fill in the template, upload the template, and select **Import**.

### 24.4.2 Add Button Settings for Indoor Stations

On the top navigation bar, select **Video Intercom Application → Button Settings → Indoor Station → Add** .

You can select one or multiple indoor stations and configure four custom button settings.

**Note**

Only indoor stations in the same unit can be selected for batch configuration.

**Table 24-1 Button Settings**

| Button | Device Type | Description |
|---|---|---|
| Call | • Master Station<br>• Indoor Station | If you select indoor station, select the room No.. |
| Live View | • Door Station<br>• Camera | Select the specific door station or camera bound to the indoor station. |
| Open Door | / | Select the specific door bound to the indoor station. |
| Call Elevator | / | / |

After adding schedules, select **Apply Settings** to apply call schedules to devices in the indoor station list.

## 24.5 Link Resources with Indoor Stations

After adding an indoor station to the plaform, you can relate cameras with the added indoor station to view video of the related camera(s) by the indoor station. You can also link persons with an indoor station. You can also relate a doorbell with an indoor station. When the Call Management Center function of this doorbell is disabled, you can call the related indoor station by the doorbell.

### 24.5.1 Link Doorbell to Indoor Station

**Steps**

1. On the left pane, select **Video Intercom Application → Link Doorbell to Indoor Station** .
2. Select **Link** to enter the Link Doorbell with Indoor Station page.
3. From the drop-down list of **Device Name**, select a location. And then select the doorbell to be linked to the indoor station.
4. In the indoor station list, select the corresponding indoor station that the doorbell is to be linked to and click **Add**.

**Note**

The location information of the indoor station is the same as that of the doorbell.

## 24.5.2 Link Cameras to an Indoor Station

After adding indoor stations to the system, you can link cameras to indoor stations to view videos of the linked cameras on the indoor station. You can link up to 16 cameras to an indoor station.

**Before You Start**

Make sure the cameras to be linked are correctly installed and are added to the system by Hikvision Private Protocol/ONVIF.

**Steps**

1. In the top left corner of the Home page, select **Video Intercom Application → Link Camera to Indoor Station** .
2. Select **Link**.

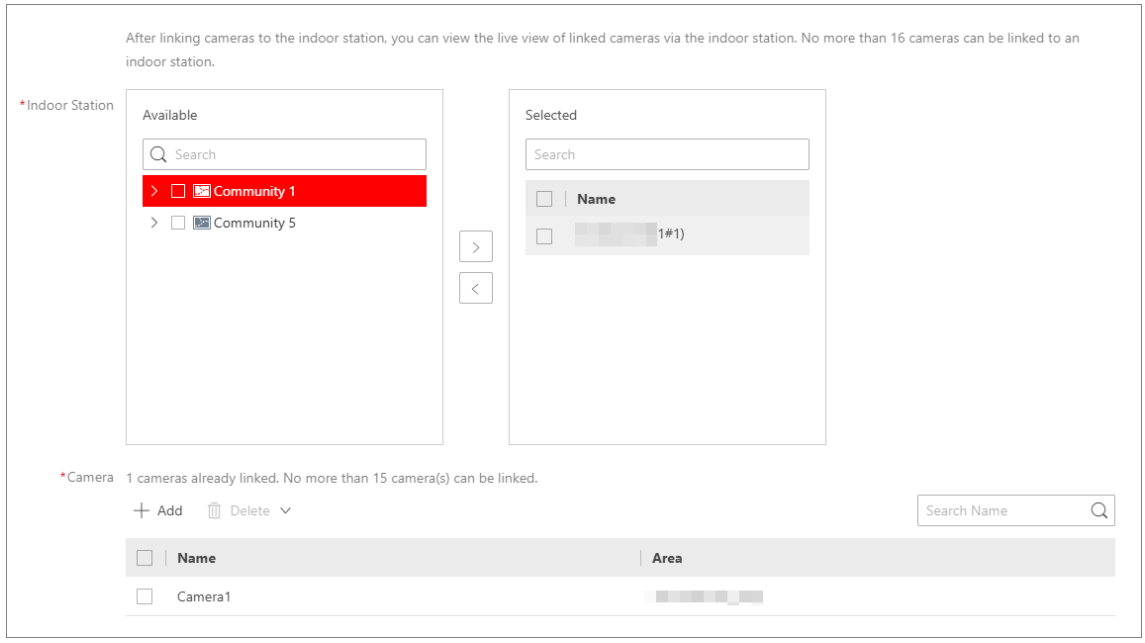



**Figure 24-2 Add Linked Camera**

**Note**

You can also link camera to indoor station in the configuration page of the indoor station. For details, refer to ***Configure Device Parameters*** .

3. In the Indoor Station list, select an indoor station.
4. In the Camera list, check one or more cameras.
5. Select **Add**.
6. Select **Apply Settings** to apply the settings to devices.

### 24.5.3 Link Persons to Indoor Station

**Steps**

1. Select **Video Intercom Application → Link Person to Indoor Station** on the left.
2. Click **Link**.

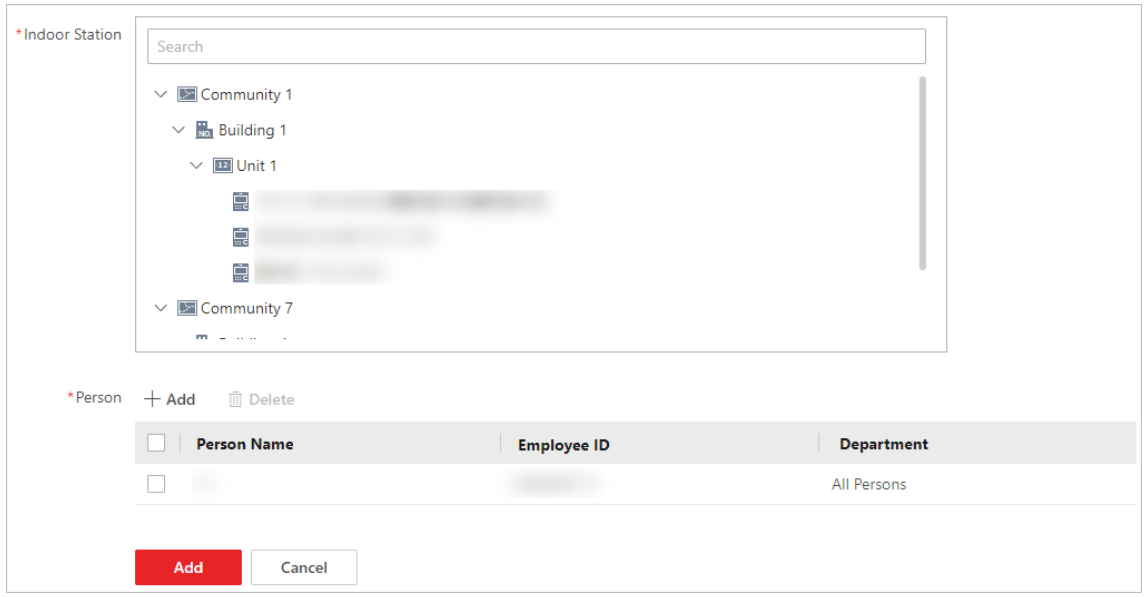



**Figure 24-3 Add Linked Person**

3. Select an indoor station.

**Note**

Up to 10 persons can be linked to an indoor station and the person cannot be linked to multiple indoor stations.

4. Click **Add** to select persons to be linked to the indoor station.
5. Click **Add**.

## 24.6 Apply Data to Indoor Station

You can apply notices to an indoor station to alert people in emergencies or install a software on indoor stations to expand their functions. After applying a software package to the indoor stations, the software will be installed automatically.

### 24.6.1 Add and Apply a Notice

There are four types of notice, including advertisement, property information, alarm, and notification. They are used for sending information to residents. You can add and apply notices to

indoor stations. For example, when an emergency occur, you can add and apply a notice to indoor stations to inform residents for timely actions. After adding and applying notices, you can delete, filter, and export them. You can also copy a notice and apply it to indoor stations conveniently.

1. On the left pane, select **Apply Data to Indoor Station → Manage Notice** .
2. Select the **Apply Notice** tab, and select **Add** to add a notice.
3. Configure the notice.
   a. Create a title of the notice and set the notice type.
   b. Select + to add pictures.

      **Note**

      Up to 6 JPG pictures can be added, and each picture should be no larger than 512 KB.

   c. Enter the content of the notice.
   d. Select indoor stations to receive the notice.
4. Select **Preview** to preview the notice.
5. Select **Apply** to apply the notice to indoor stations.
6. (Optional) Select the **Apply Notice** tab.
   - Select one or more notices, and select **Copy and Apply** to apply notices to indoor stations.
   - If you want to edit the notice content, select to copy the current notice and edit the notice as needed. Select **Apply** to apply the notice to indoor stations.

## 24.6.2 Apply Software Package to Indoor Station

This function is only supported by certain models.

**Steps**

1. In the left pane of the Home page, select **Apply Data to Indoor Station → Apply Software Package** .
2. Click **Apply Software Package**.
3. Select **All Indoor Stations** or **Specified Indoor Station(s)**.

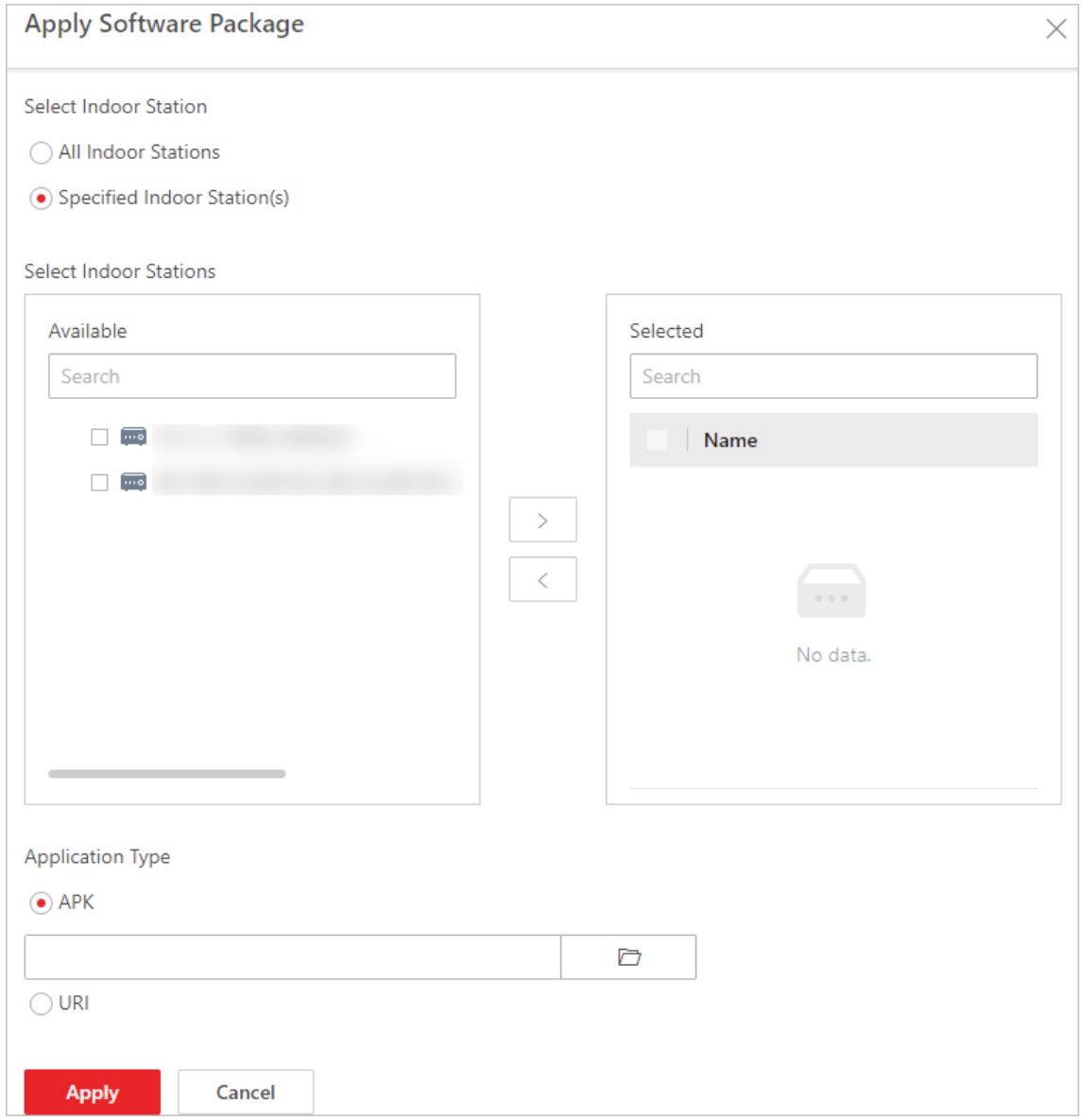



**Figure 24-4 Apply Software Package**

4. Select an application type.
5. Select **Apply**.

## 24.7 Make and Receive Calls on Platform

You can configure a receiving schedule template to define when the platform user can receive calls. After configuring receiving schedule templates, you can adding platform users as call recipients. When someone calls the platform, the added recipients can receive and answer the call.

### 24.7.1 Add Call Schedule Template

**Steps**

1. On the top navigation bar, select **Basic Configuration → Schedule Template → Call Schedule Template** .
2. Select + to add a schedule template.

   You cannot edit or delete The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Call Center.
3. Configure the template.
   1) Create a name for the template.
   2) **Optional:** Select an existing template from the **Copy from** drop-down list.
   3) Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.
   4) Set the weekly schedule.

| Operations | Description |
|---|---|
| Set Task Time | Click a grid or drag the cursor on the time line to draw a time period during which the task is activated. |
| Set Precise Time | Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  . |



   5) **Optional:** Select **Add Holiday** to select an existing holiday template, or click **Add** to add a new template.
4. Select **Add** to save the template.

### 24.7.2 Add Call Recipients

Go to **System → Call Settings → Call Recipient** .

## 24.8 Apply Advertisements to Door Stations

You can add pictures or videos in the advertisements, then apply the advertisements to door stations. After applying advertisements, you can filter or delete them. This function should be supported by the device.

**Steps**

1. Select **Video Intercom → Apply Advertisements to Door Stations** .
2. Click **Apply Advertisements to Door Stations** on the top.
3. Select the available door station in the left list and click › to add it to the right list.

4. Add picture(s) or a video for an advertisement to be applied to door stations.

**Note**

For the picture advertisement, you can add up to six pictures. For the video advertisement, you can add up to three videos.

- a. Click **Picture** → + to add picture(s) for an advertisement.
  b. Set the **Picture Switching Interval**.
  c. Set the time period to play the added picture(s).

  **Note**

  Click **Add** to add the time period if needed.
- a. Click **Video** → + to add a video for an advertisement.
  b. Set the time period to play the added video.

  **Note**

  Click **Add** to add the time period if needed.

5. The playing schedules set for the picture(s) and the video in the advertisement will be displayed by different color blocks.
6. Click **Apply**.

# Chapter 25 Attendance

In the Attendance module, you can easily manage the time & attendance system of your department and check your employees' attendance.

On the top left, select → **Integrated Service** → **Attendance** .

On the Home page, you can view the attendance report, attendance status statistics, and overall work hours / overtime.

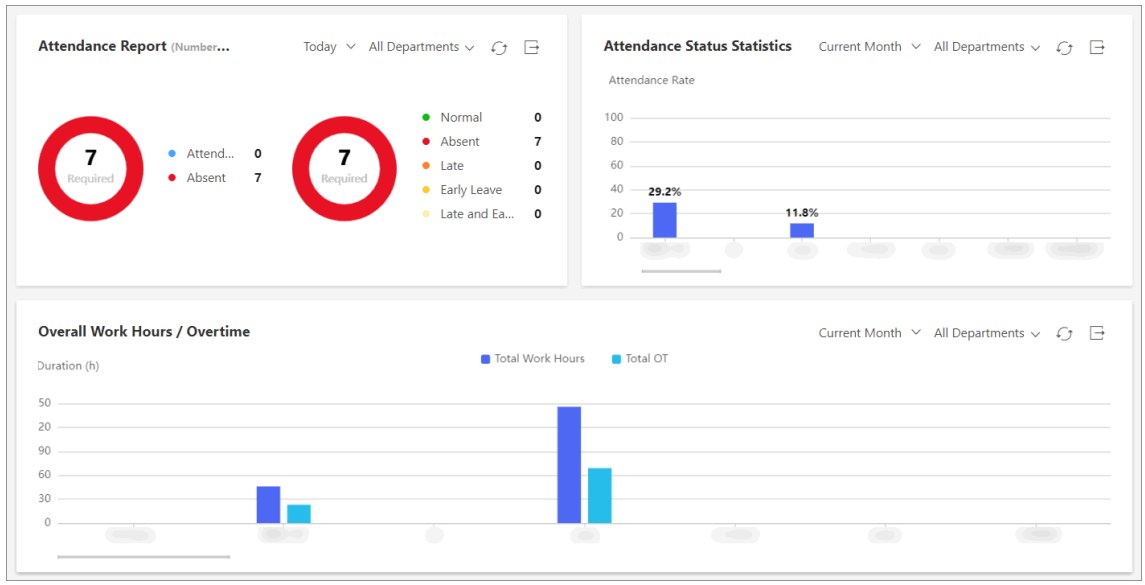



**Figure 25-1 Attendance Charts**

## 25.1 Flow Chart of Time and Attendance

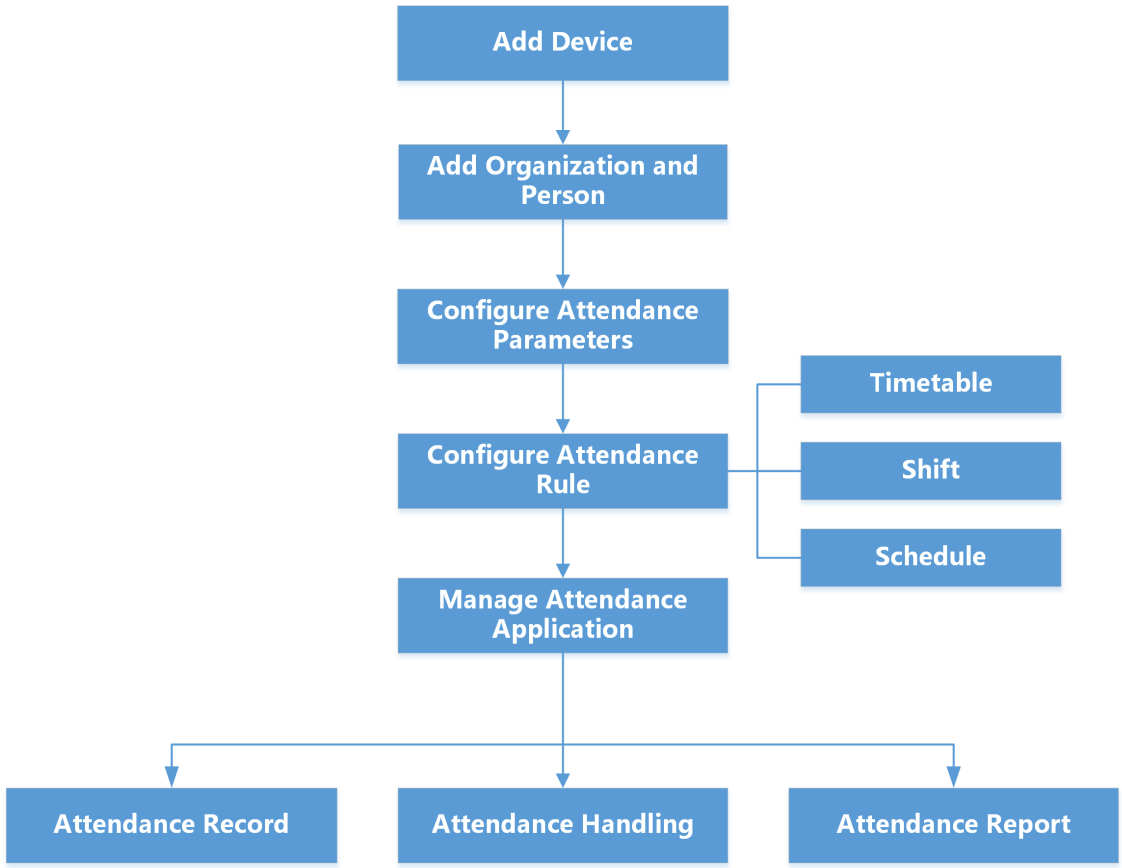



**Figure 25-2 Flow Chart of Time & Attendance**

## 25.2 Before You Start

Before you start, you need to accomplish the following procedures.

### 25.2.1 Add Devices, Departments, and Persons

You need to add devices (e.g., access control devices), departments, and persons to the platform before you implement the Attendance module.

## 25.2.2 Add an Attendance Group

For situations where users need to set exclusive attendance rules for specified employees, users can add the employees to an attendance group configured with attendance rules different from and prior to that of a department.

**Before You Start**

Make sure you have added the employees to the platform. See ***Add Person*** .

**Steps**

1. Go to **Attendance Group → Add** .
2. On the Add Attendance Group pane, enter a name of the group.

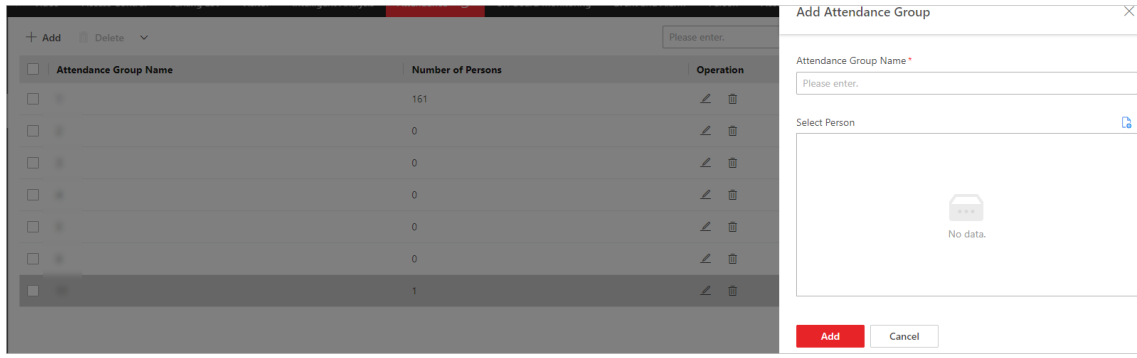



**Figure 25-3 Add Attendance Group**

3. Click and check persons in different departments, and click **Add** to save the selections.

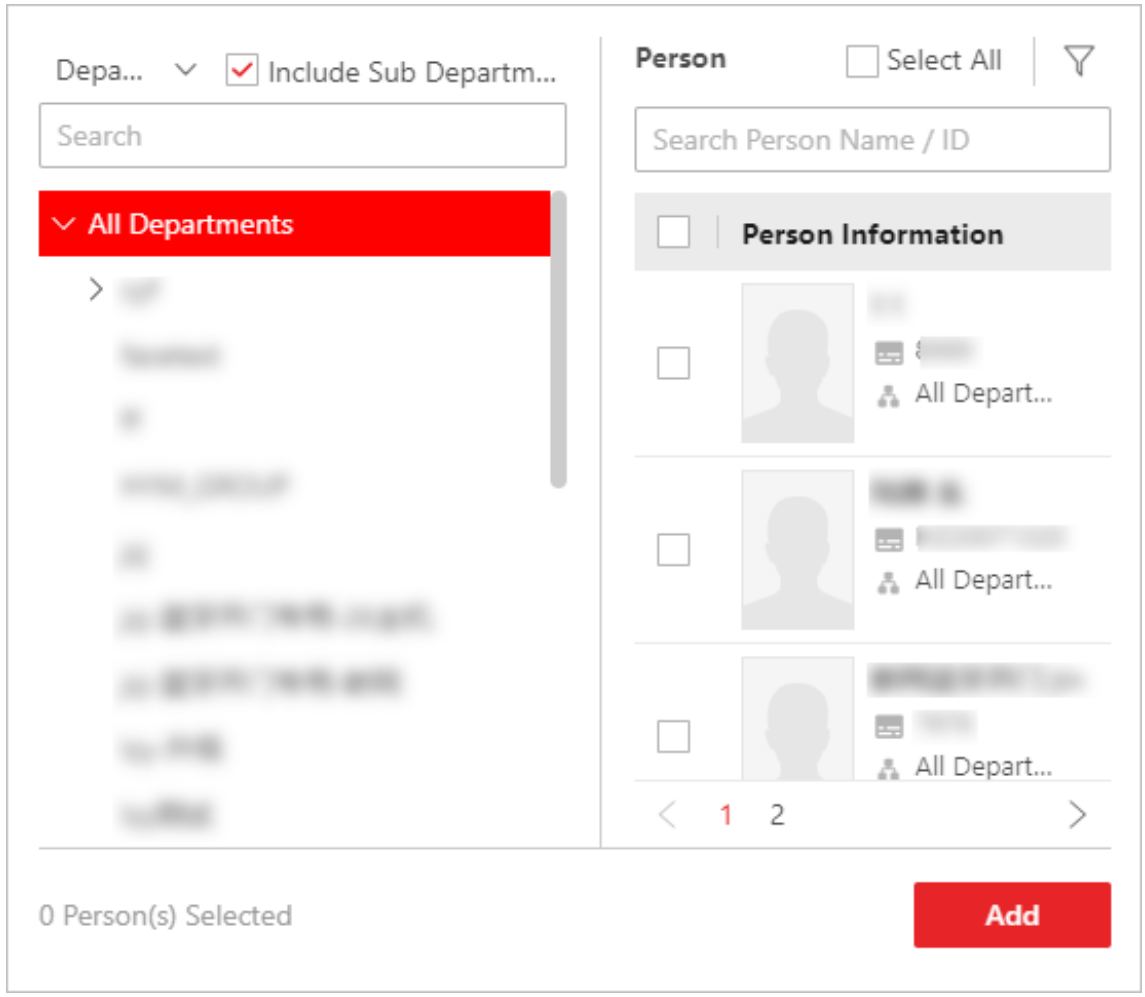



**Figure 25-4 Add Persons to Attendance Group**

**Note**

You can click on the top left to filter persons by additional information.

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

| | |
|---|---|
| **Edit an Attendance Group** | Click and then edit the group name or click to add persons to the group. |
| **Add Persons to an Attendance Group** | Click an added group to show persons on the right. Then click **Assign To** to add persons to the group. |
| **Remove Persons from an Attendance Group** | Click an added group to show persons on the right. Then check persons and click **Unassign** to remove the selected persons from the group. Or click → **Unassign All** to remove all persons from the group. |

**Set Display Mode of Each Column** Click ⇄ to display each column title completely/incompletely.

**What to do next**

Configure attendance rules for the group. See ***Configure Attendance Rules for Global / Department / Attendance Group*** .

## 25.2.3 Specify Attendance Check Points

By default, all devices are attendance check points. You can specify some access points for attendance check, so that the check-in/out by credentials (such as swiping card on the access point's card reader, or face detected by the (linked) camera) will be valid and will be recorded.

**Steps**

1. Select **Basic Configuration → Attendance Check Point** on the left.
2. **Optional:** Click **Customize Attendance Status** to select attendance mode and custom attendance parameters. For details, see ***Customize Attendance Status on Device*** .
3. **Optional:** Check **Get Historical Data Stored in Devices** to synchronize the historical data generated by attendance check points to existing data. This will cause a recalculation of attendance results.
4. Click **Specify** to start customizing attendance check points.
5. Click **Add**.
6. Select the type of the attendance check point.

   **Check-In & Out**

   The attendance records of check-in or check-out on the attendance check point are both valid.

   **Check-In Only**

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-in. Persons cannot check out on this check point.

   **Check-Out Only**

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-out. Persons cannot check in on this check point.
7. Select the resource type (e.g., door) from the drop-down list.

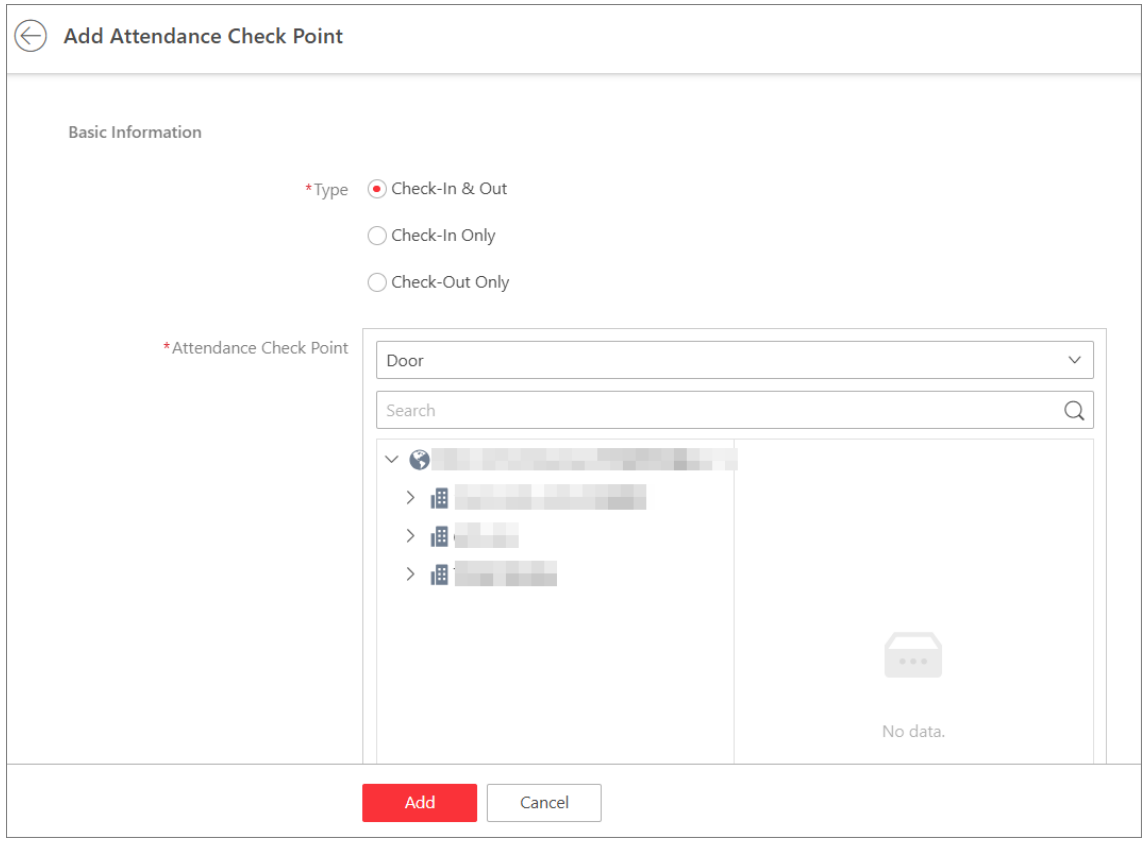



**Figure 25-6 Add Attendance Check Point**

All the resources which have not been set as attendance check point will be displayed.

8. Select the resources.

**Note**

If you select Door as the resource type, you can set the attendance check point type for different card readers separately. For example, there is a card reader installed at both side of the door. You can set the card reader of the entry direction as check-in only and the exit one check-out only.

9. Click **Add**.

The selected resources will be displayed in the attendance check point list.

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

| | |
|---|---|
| **Change Check Point's Type** | For the added attendance check points, you can select one or more items and click **Set as Check-In Only**, **Set as Check-Out Only**, or **Set as Check-In/Out** from drop-down list to change the current type to another. |
| **Delete Check Point** | To delete the added attendance check point, select the added attendance check point(s) and click **Delete**. |

**Note**

If the attendance check point is deleted, the attendance records on this attendance check point will be deleted as well, and it will affect the persons' attendance results for the days on which the attendance data haven't been calculated.

## Customize Attendance Status on Device

You can customize the rules of attendance status on device. After setting up Attendance Status on Device and applying the settings to the devices, you can choose to use the attendance status on the devices to calculate the attendance results.

**Steps**

1. In the left navigation pane of the Attendance module, select **Basic Configuration → Attendance Check Point** .
2. Click **Custom Attendance Status** on the top right.
3. Switch on **Enable Attendance Status on Device**.
4. Set the parameters.

**Attendance Mode**

**Manual**: No attendance schedule. Manual selection of attendance status is required when a person checks in or checks out on a device.

**Automatic**: Specify an attendance schedule and the attendance status of a person is judged according to the schedule.

**Manual And Auto**: Specify an attendance schedule and the attendance status of a person is judged according to the schedule. The person can also change the attendance status manually on device.

**Attendance Status Required**

**On**: Manual selection of attendance status is required for a valid check-in/out.

**Off**: Manual selection of attendance status is optional.

**Note**

Not available when in Manual mode, because manual selection of attendance status is always required.

**Custom Name of Working**

Customize the status name for check-in and check-out.

**Custom Break Name**

Customize the status name for the start and end of a break.

**Custom Overtime Name**

Customize the status name for the start and end of an overtime.

**Time Template**

Select a status and drag on the template to define the attendance status of a period of time.

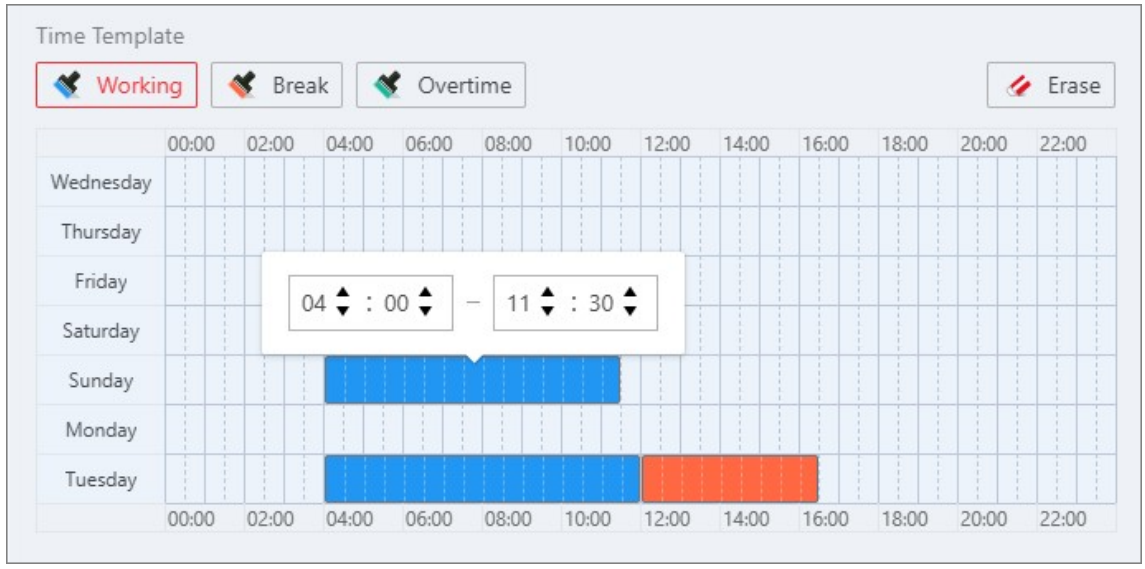



**Figure 25-7 Time Template**

**Note**

- Not available when in Manual mode. Because manual selection of attendance status is always required and no attendance schedule is needed.
- Work time and break time must be continuous.
- Overtime cannot be continuous with work and break time.
- Overtime must be before or after work or break time.

5. Click **Save** to save the settings and apply the settings to the attendance check points you added.

**Note**

- You can view the applying result on the Apply Custom Status window.
- See details about adding attendance check points in ***Specify Attendance Check Points*** .
- You can switch on **Enable T&A Status on Device** when configuring break timetables, timetables, or shifts to record the T&A status on devices, which will be used in attendance results calculation.

## 25.2.4 Add a Pay Code

Pay code defines the attendance status and calculation codes for calculating the attendance statistics on the third-party system. You can add, edit, and delete pay codes, filter the pay codes by conditions, set the column title, and custom column items.

**Steps**

1. Go to **Basic Configuration → Pay Code → Add** .
2. Create the pay code name.
3. Set the pay code type and related parameters.

   **Leave**

   leave type which displays in reports and leave applications.

   **Unit**: Unit of pay code. Select from minute, hour, day, and HH:MM (time accurate to minute).

   **Overtime**

   Overtime type which displays in configuration of overtime rules, reports and overtime applications.

   **Work Hour Rate**

   Used for calculating the overtime period, e.g., the actual working time of overtime is 2 hours and the work hour rate is 1.5, then the overtime period is 3 hours.

   **Color**

   Used for making differences among pay codes.
4. Customize a symbol for the pay code.

   You can choose to display the pay code in reports by symbol or by name. See ***Set Display Rules for Attendance Report*** .
5. Set the rounding rule.

   **Round Up**

   Round the number of pay code up, e.g., if you make 0.5 go up, then 6.5 rounds up to 7.

   **Round to Nearest**

   Round decimal numbers to nearest integers either by rounding up or rounding down based on the tenths places, e.g., 6.5 rounds to 7 and 6.4 rounds to 6.

   **Round Down**

   Round the number of pay code down, e.g., if you make 0.5 go down, then 6.5 rounds down to 6.
6. Set the Min. Value for the rounding rule.
7. Set whether to display the pay code in report.
8. Click **Add**.
9. **Optional:** Perform the following operations.

| Operation | Description |
|---|---|
| **Edit Pay Code** | Click in the Operation column to edit the pay code information. |
| **Delete Single Pay Code** | Click in the Operation column to edit the pay code information. |
| **Batch Delete Pay Codes** | Select one or multiple pay codes and click **Delete** to delete them. Or Select **Delete All** to delete all the pay codes. |

| | |
|---|---|
| **Filter Pay Code** | Click to expand the conditions, set the filter conditions and click **Filter** for filtering the pay codes. |
| **Set Column Width** | Click to select **Complete Display of Each Column Title/Incomplete Display of Each Column Title** to set the column title width. |
| **Custom Column Item** | Click and select the needed column items to display. You can also click **Reset** to reset to the default column items. |

## 25.2.5 Edit a Fixed Code

Fixed code refers to the calculation rules of attendance types. You can set parameters of fixed codes such as the unit, symbol, and rounding rule.

Go to **Basic Configuration → Fixed Code** .

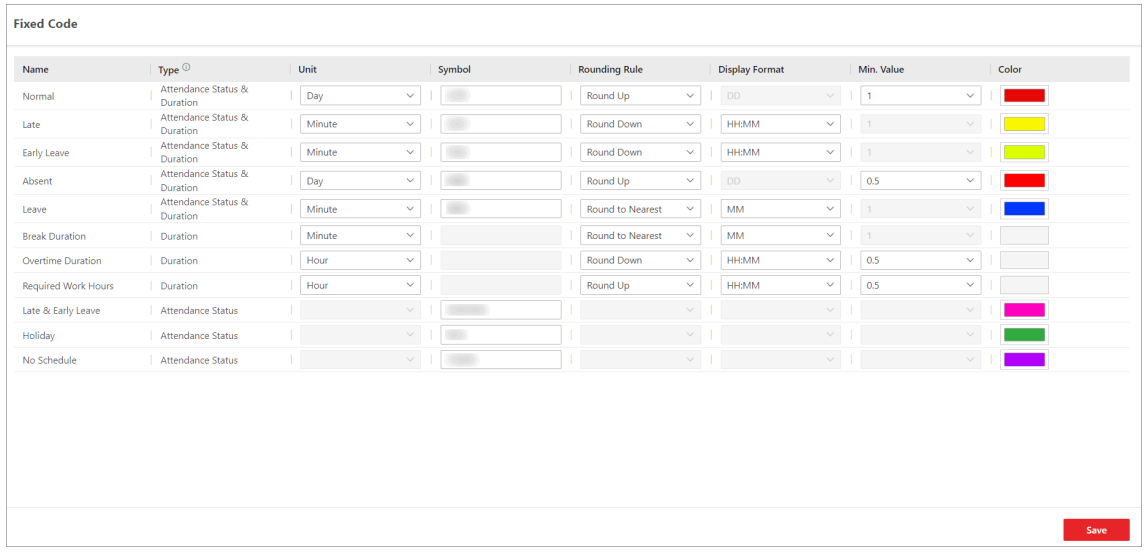



**Figure 25-8 Edit Fixed Code**

You can set the following parameters and click **Save** to finish editing.

**Unit**

Unit of pay code. Select from minute, hour, and day.

**Symbol**

Different symbols indicate different status respectively, including late, absent, no schedule, holiday, etc. You can customize these marks according to actual needs.

**Rounding Rule**

Rule for calculating the attendance.

**Round Up**

Round the number of pay code up, e.g., to make 0.5 go up, so 6.5 rounds up to 7.

**Round to Nearest**

Round decimal numbers to nearest integers either by rounding up or rounding down based on the tenths places, e.g., 6.5 rounds to 7 and 6.4 rounds to 6.

**Round Down**

Round the number of pay code down, e.g., to make 0.5 go down, so 6.5 rounds down to 6.

**Display Format**

Time format of the fixed code, including HH:MM, DD, HH, and MM.

**Min. Value**

The minimum value of the fixed code. Select from 1 and 0.5.

**Note**

When the Unit is "hour", the min. value is 0.25.

**Color**

Used for making differences among fixed codes.

## 25.2.6 Add a Leave Rule

A leave rule refers to a group of leave types and persons, where the persons in the group enjoys certain leaves.

**Steps**

1. Go to **Basic Configuration → Leave Rule → Add Leave Rule** .

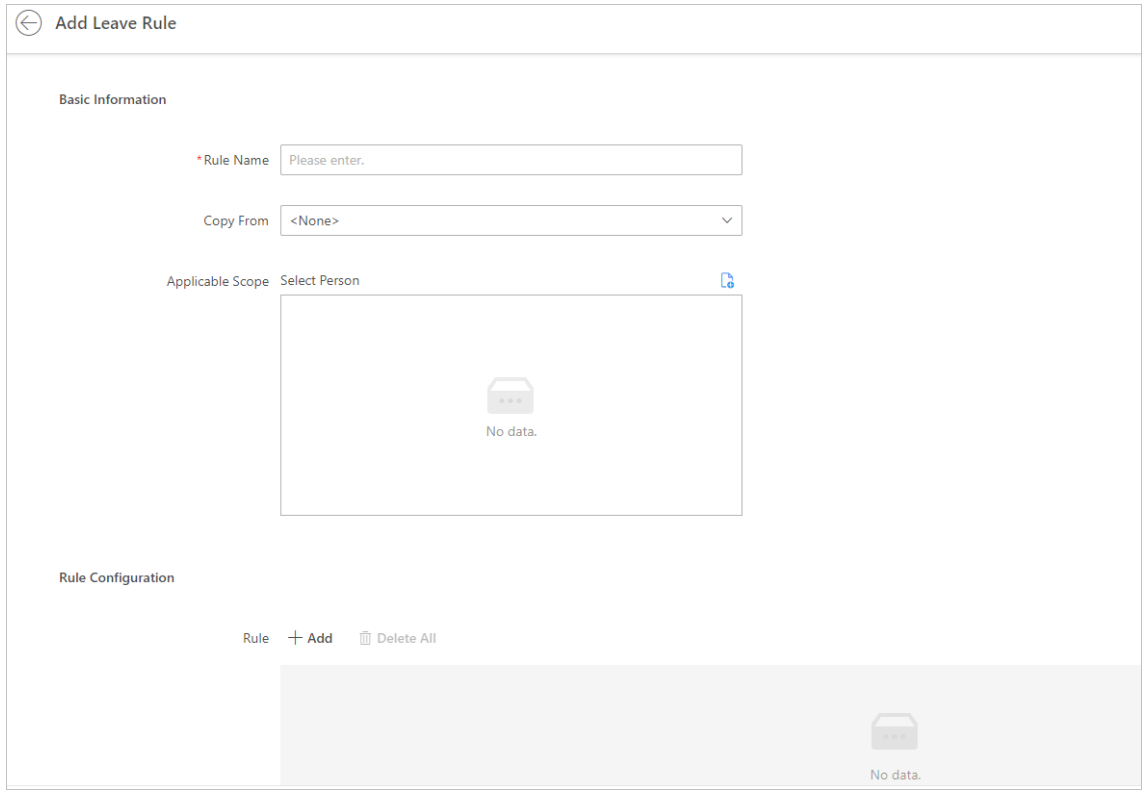



**Figure 25-9 Add Leave Rule**

2. Enter a rule name.
3. **Optional:** Select an existing leave rule from the drop-down list of **Copy From** to copy the persons using the selected leave rule here.
4. Click to select persons who are going to use the leave rule.
5. Add a rule.
   1) In the Rule Configuration area, click **Add** to open the Add Rule pane.
   2) Select a pay code from the drop-down list.
   3) Set the related parameters.

      **Min. Days of Employment Allowed for Leave Application**

      Only when the days of employment reaches this value, can the employee apply for a leave.

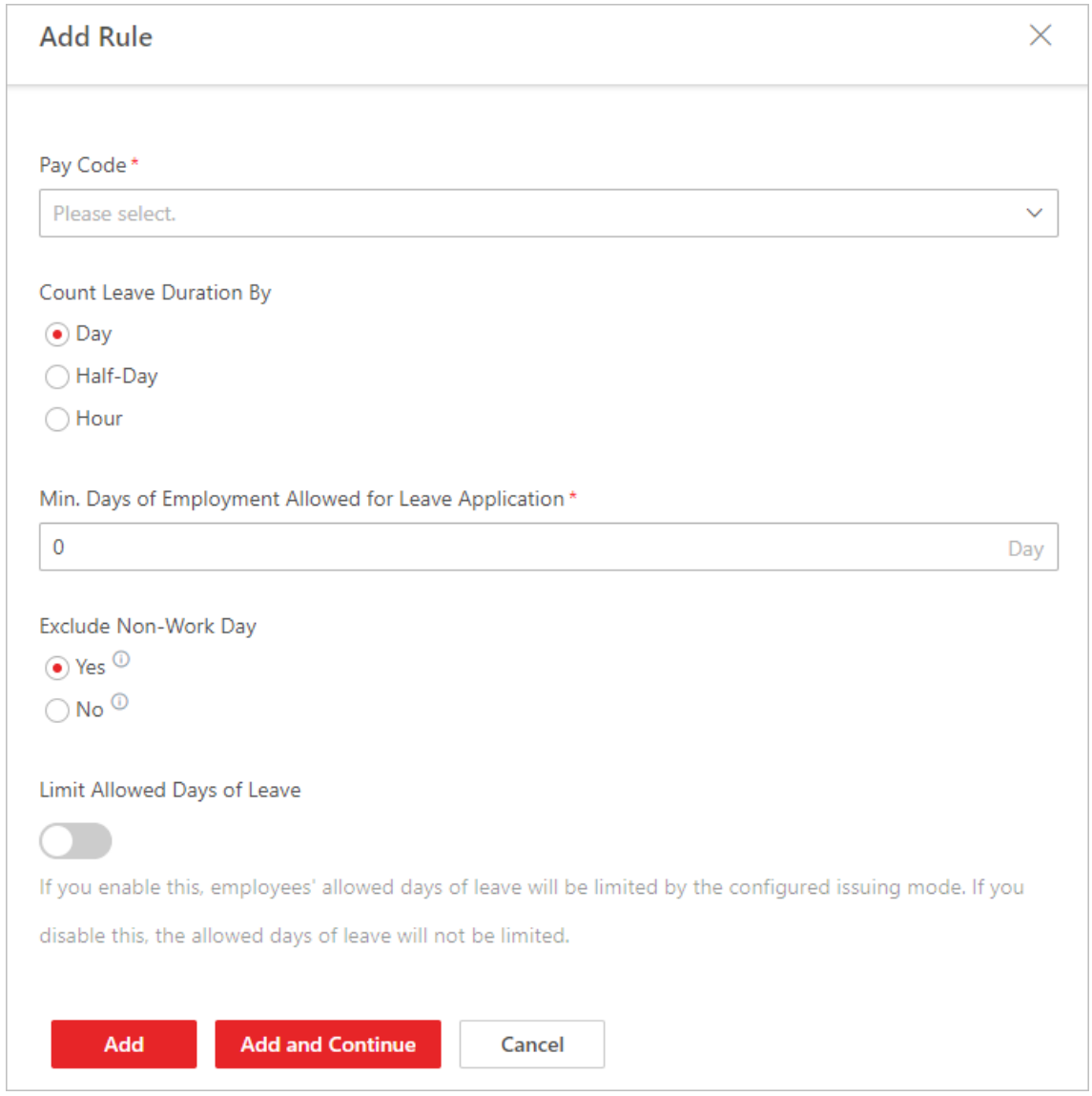



**Figure 25-10 Add Rule**

4) **Optional:** Enable **Limit Allowed Days of Leave** and set the related parameters.

**Issuing Mode**

**Auto Issue Annually**

The platform issues allowed days of leave to employees on a specified day each year. You need to select an issuing date and select an issuing rule.

**Issuing Rule**

**Fixed Amount**

The platform issues the same days of leave to employees each year.

**Depends On Employment Years**

The issued days of leave depend on the employment years.

**Issue All Days of Leave Once**

Issue all days of leave to employees once. You need to set the number of days and you can configure expiry date of the days if needed.

6. Save the settings.

### 25.2.7 Configure Storage Settings

You can set the storage location of the attachment in exception application.

1. Go to **Basic Configuration → Storage Settings** .
2. Select a backup file to be restored.
3. Click **Save**.

## 25.3 Check-In/Out via Mobile Client

After configuring the check-in/check-out function via the Web Client, employees can quickly check in/out within the valid geographic scope via the Mobile Client. The platform will perform attendance calculation of check-in records collected by the Mobile Client.

To enable employees to successfully check in/out via the Mobile Client, the following steps are required:

1. Administrators configure the function of **Check-In/Out Area via Mobile Client** via the Web Client (Management).
2. Employees check in/out inside the valid geographic scope via the Mobile Client (Self-Service).
3. Reviewers handle attendance via the Web Client (Self-Service).
4. Employees check their check-in/out status after attendance approval via the Mobile Client (Self-Service).

### 25.3.1 Step 1: Configure Function via Web Client

Administrators log into the Web Client (Management) and go to **Attendance → Check-In/Out Area via Mobile Client** .

#### For Configuration of the First Time

For configuration of the first time, you will enter the following page.

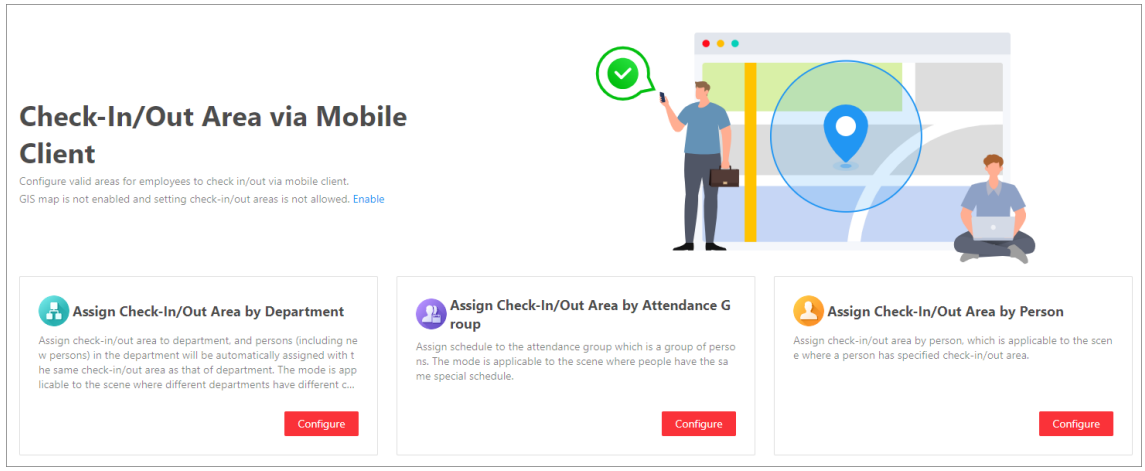



**Figure 25-11 Page for Configuration of the First Time**

Click **Enable** to enable GIS map for setting check-in/out areas.
Click **Configure** to start assigning check-in/out area by department / attendance group / person.
Take assigning check-in/out area by department as an example. Click **Configure** to show the page of Assign Check-In/Out Area by Department. Select department(s) and click **Next** on the top left. Enter an area name, an draw the area in the radius mode or custom mode. Hover the cursor on the edge of the area and drag to change the scope.

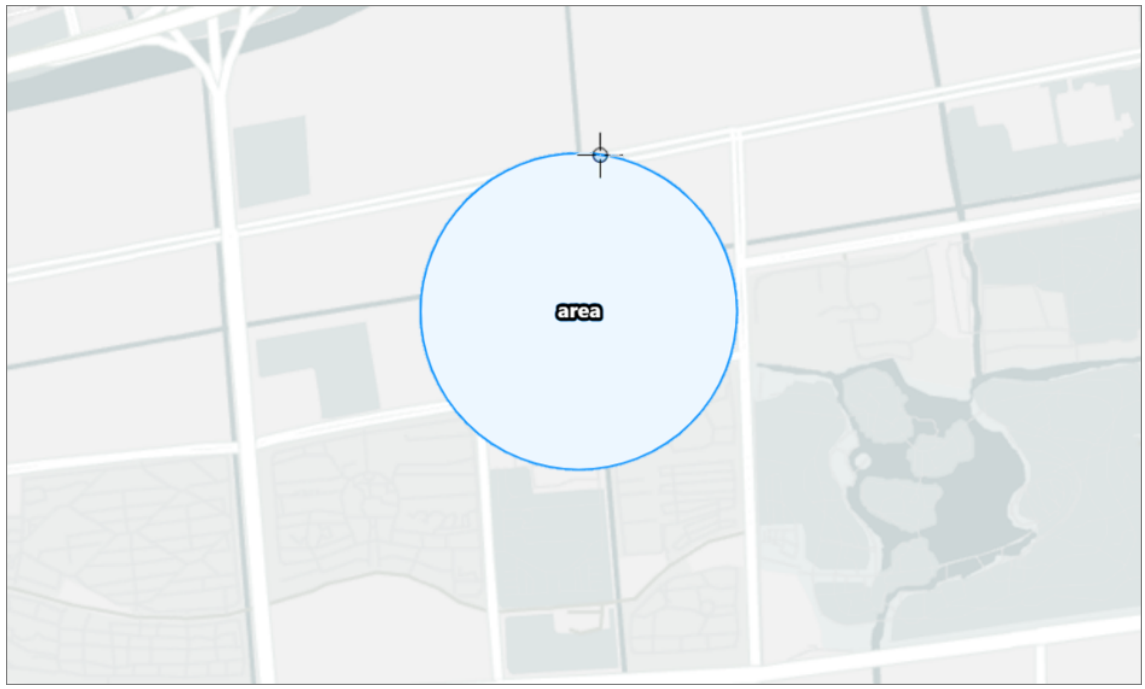



**Figure 25-12 Draw Check-In/Out Area**

### For Configuration of Not the First Time

For configuration of not the first time, you will enter the following page. You can also perform operations such as adding/editing/deleting check-in/out area(s).

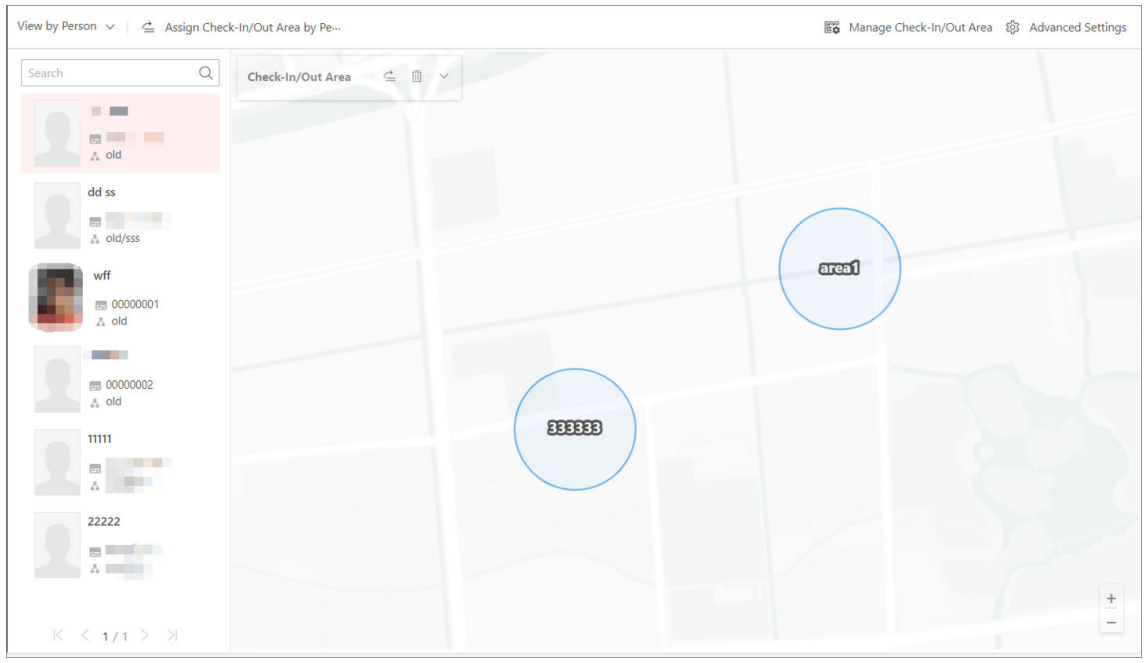
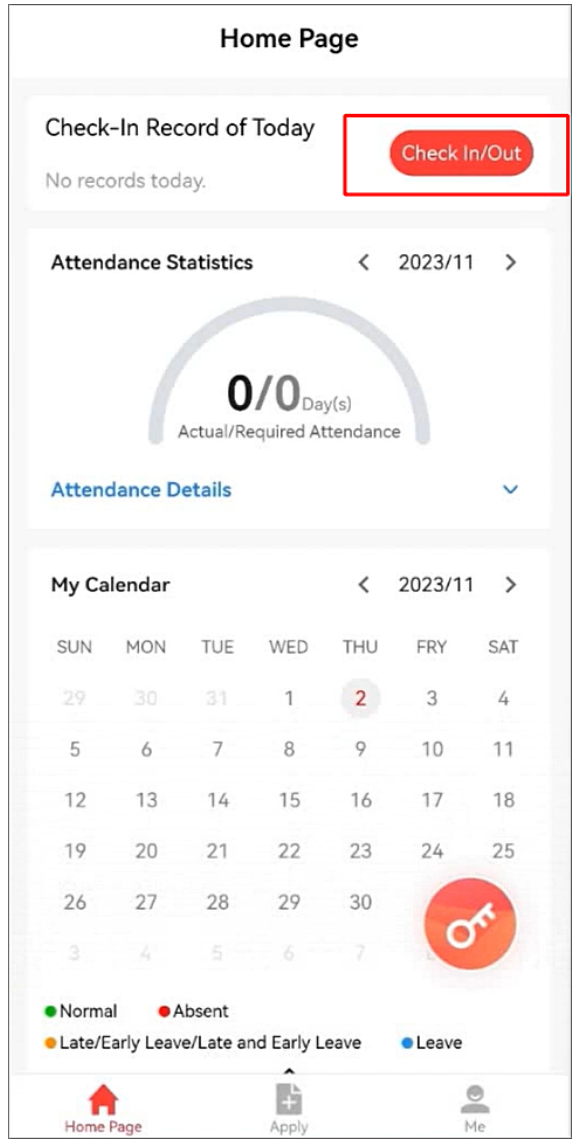



**Figure 25-13 Page for Configuration of Not the First Time**

## 25.3.2 Step 2: Check In/Out via Mobile Client

Employees log into the Mobile Client (Self-Service) and check in/out inside the valid geographic scope.

On the Home page, tap **Check In/Out** to enter the Check In/Out page. Allow access to location, take a picture as record, and then tap **Check In/Out**.


Home Page
Check-In Record of Today
No records today.
Check In/Out
Attendance Statistics
2023/11
0/0 Day(s)
Actual/Required Attendance
Attendance Details
My Calendar
2023/11
SUN MON TUE WED THU FRY SAT
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30
3 4 5 6 7
Normal
Absent
Late/Early Leave/Late and Early Leave
Leave
Home Page
Apply
Me

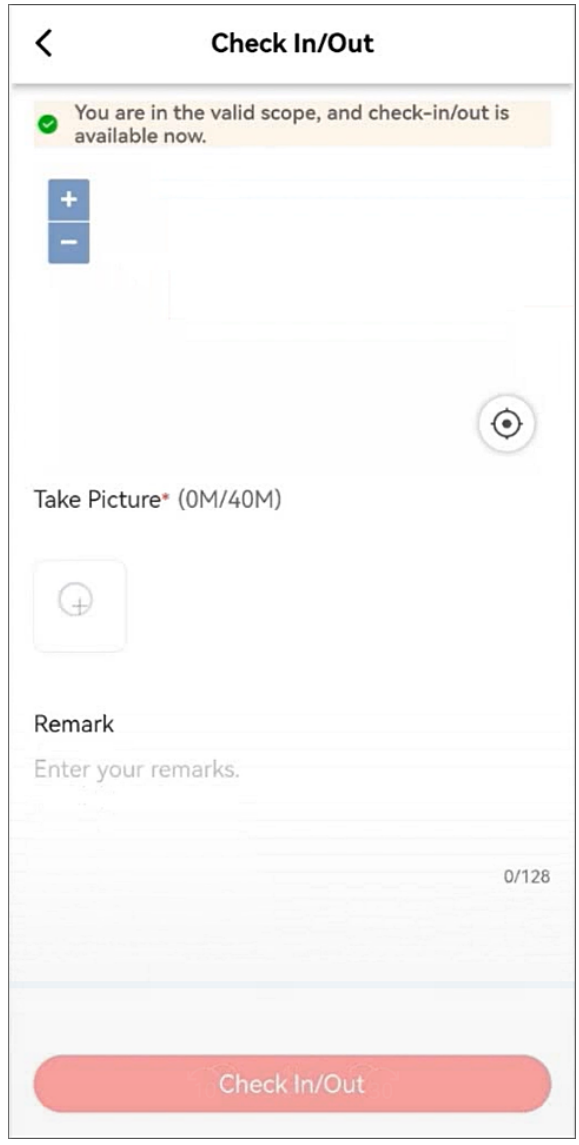



**Figure 25-14 Check In/Out via the Mobile Client**

### 25.3.3 Step 3: Handle Application via Web Client

After employees submit their Check In/Out applications, reviewers log into the Web Client (Self-Service) to process the application.

**Note**

Make sure the reviewer can review **Check-In/Out Area via Mobile Client** approval flow. Go to **Person → Review Management → Approval Flow** . See ***Approval Flow*** for details.

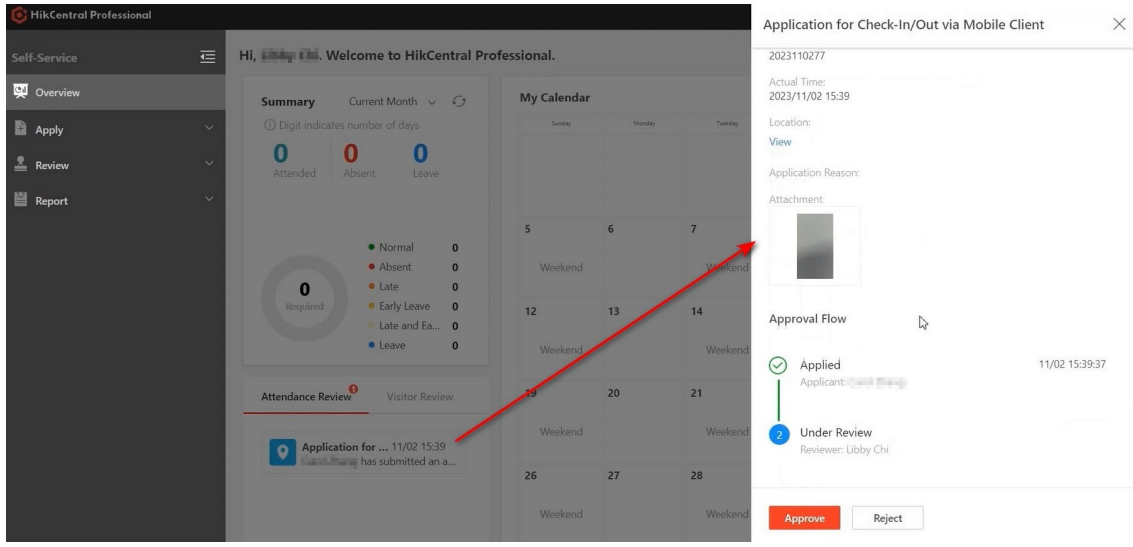



**Figure 25-15 Review Application**

## 25.3.4 Step 4: Check Attendance Status via Mobile Client

After approval, employees can check their check-in/out status via the Mobile Client (Self-Service).

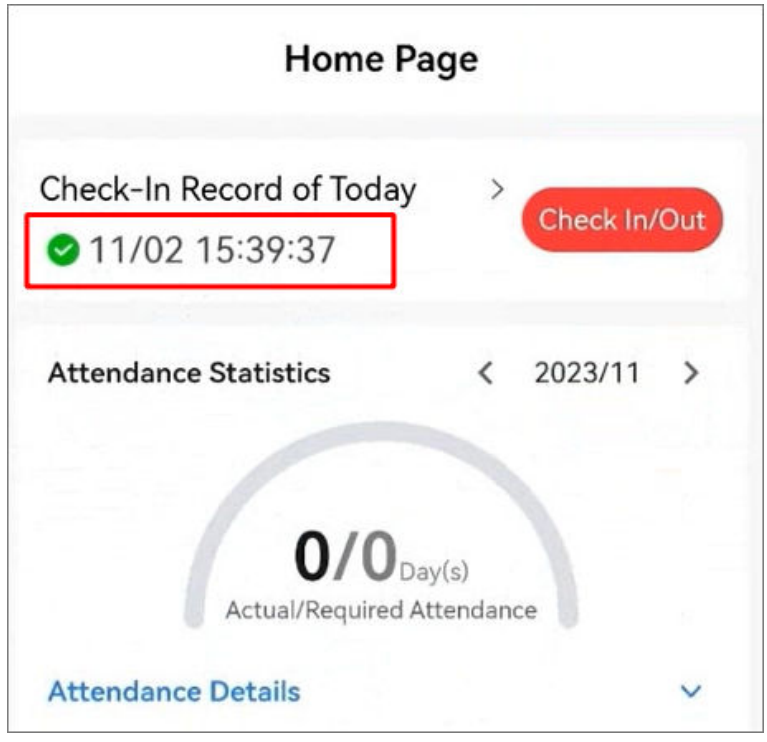



**Figure 25-16 Check Status**

## 25.4 Approval Flow

When employees submit attendance applications, including leave, overtime, attendance correction, and check-in/out via the Mobile Client, reviewers should process these applications. This entire process is the approval flow, which defines the steps of the approval process.

To complete an entire approval flow, follow these steps. Here, take applying for a leave as an example.

1. Add approval roles for an application and link persons to each role.
2. Configure the approval flow with the added approval roles to regulate the flow of reviewing applications.
3. Add leave rules for specific persons. When these persons apply for leave, they should follow the leave rules.
4. Employees submit applications via the Mobile Client or the Web Client (Self-Service).
5. Reviewers review applications from employees via the Mobile Client or the Web Client (Self-Service).
6. Employees check their application status via the Mobile Client or the Web Client (Self-Service).

### 25.4.1 Step 1: Add Approval Role

Add approval roles for an application and link persons to each role.

Go to **Person → Review Management → Approval Role → Add Now / Add** .

For example, you can add approval roles as HR or Team Manager and link persons to each role.

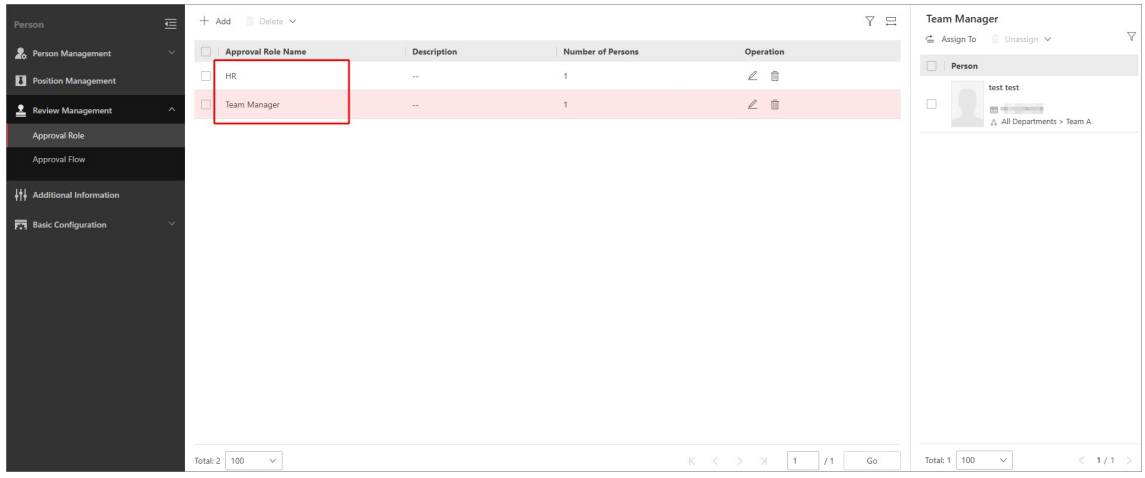



**Figure 25-17 Approval Role**

### 25.4.2 Step 2: Configure Approval Flow

Configure the approval flow with the added approval roles to regulate the flow of reviewing applications.

Go to **Person → Review Management → Approval Flow → Add → Department / Attendance Group / Position / Personal** .

Check **Transfer to Administrator for Approval When No Approval Flow is Configured** if needed.

**Note**

If no approval flow is configured for a person and the option **Transfer to Administrator for Approval When No Approval Flow is Configured** is unchecked, that person will not see the **Add** button for submitting leave, overtime, or attendance correction requests after logging into Self-Service. As a result, they can only view pending or handled applications but cannot create new ones.

Take adding a **Department Approval Flow** as an example, which defines the leave approval process of reviewing applications from a department. Employees in the Team A and B will follow the leave flow when they apply for leave.

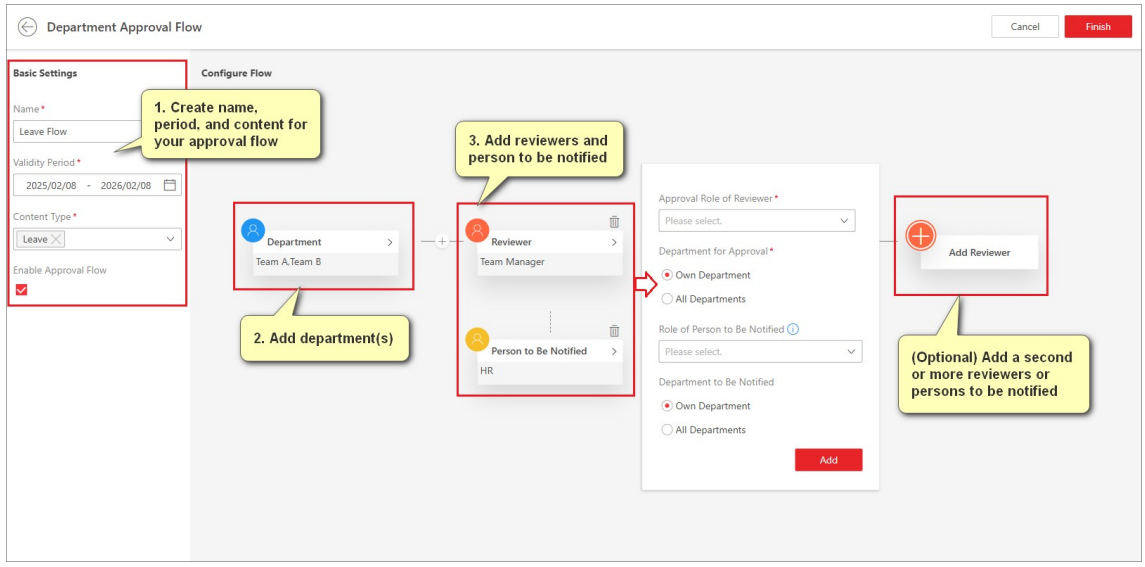



**Figure 25-18 Approval Flow**

### 25.4.3 Step 3: Add Leave Rule

Add leave rules for specific persons. When these persons apply for leave, they should follow the leave rules.

Go to **Attendance → Basic Configuration → Leave Rule → Add Leave Rule** .

For details, see ***Add a Leave Rule*** .

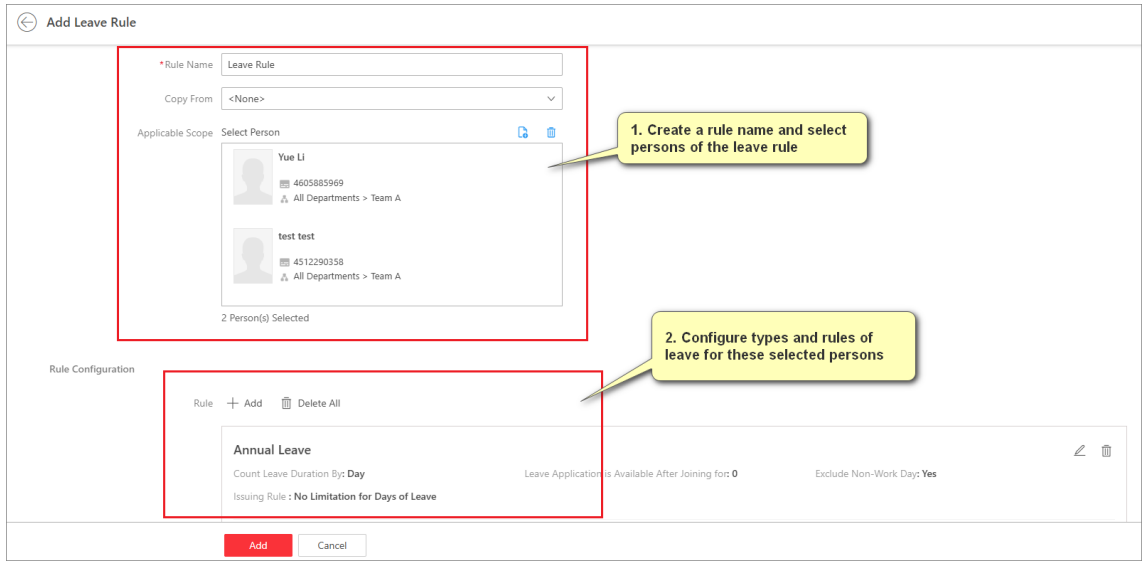



**Figure 25-19 Leave Rule**

## 25.4.4 Step 4: Employees Submit Applications

Employees submit applications via the Web Client or the Mobile Client (Self-Service).

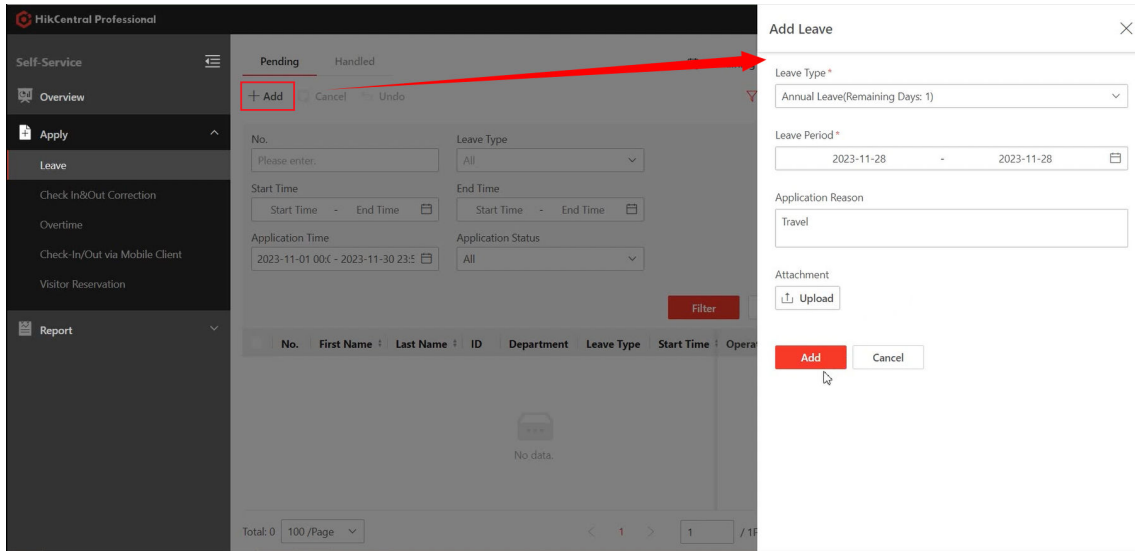



**Figure 25-20 Via the Web Client**

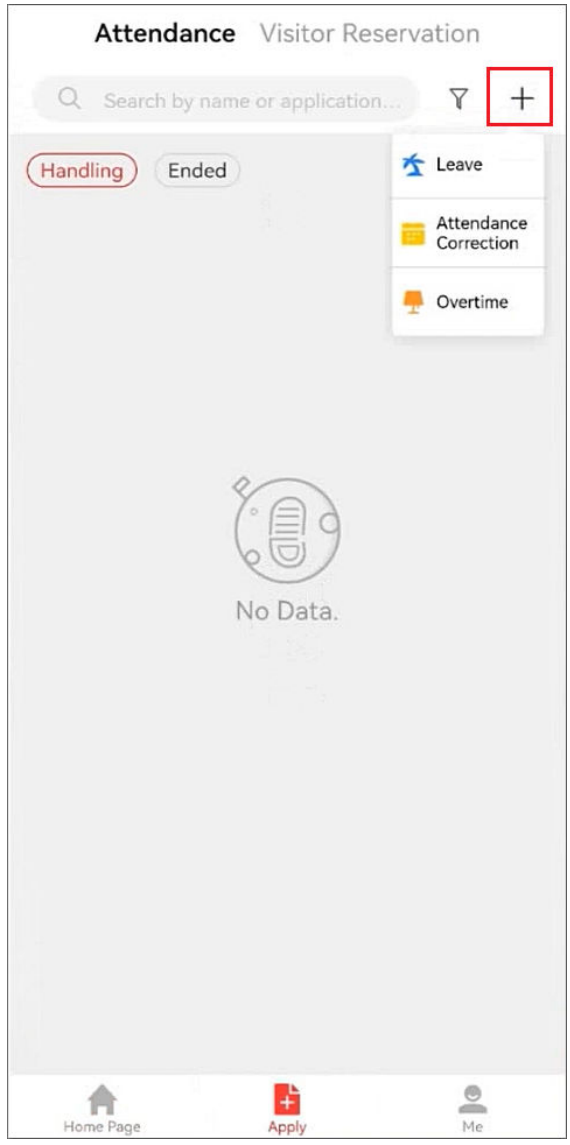



**Figure 25-21 Via the Mobile Client**

### 25.4.5 Step 5: Reviewers Review Applications

Reviewers review applications from employees via the Web Client or the Mobile Client (Self-Service). Persons to be notified (if any) can view the application flow.

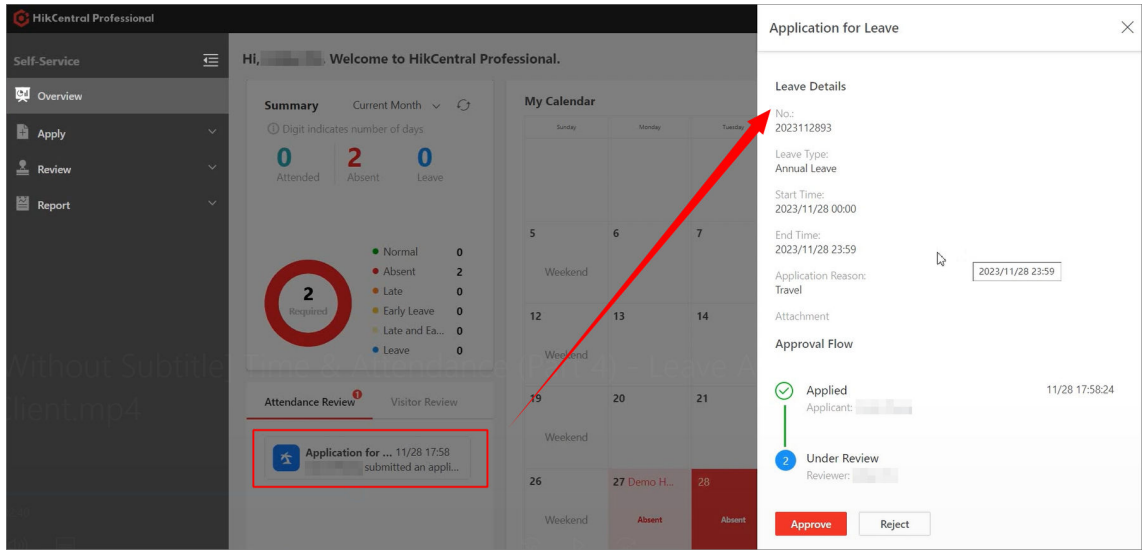



**Figure 25-22 Via the Web Client**

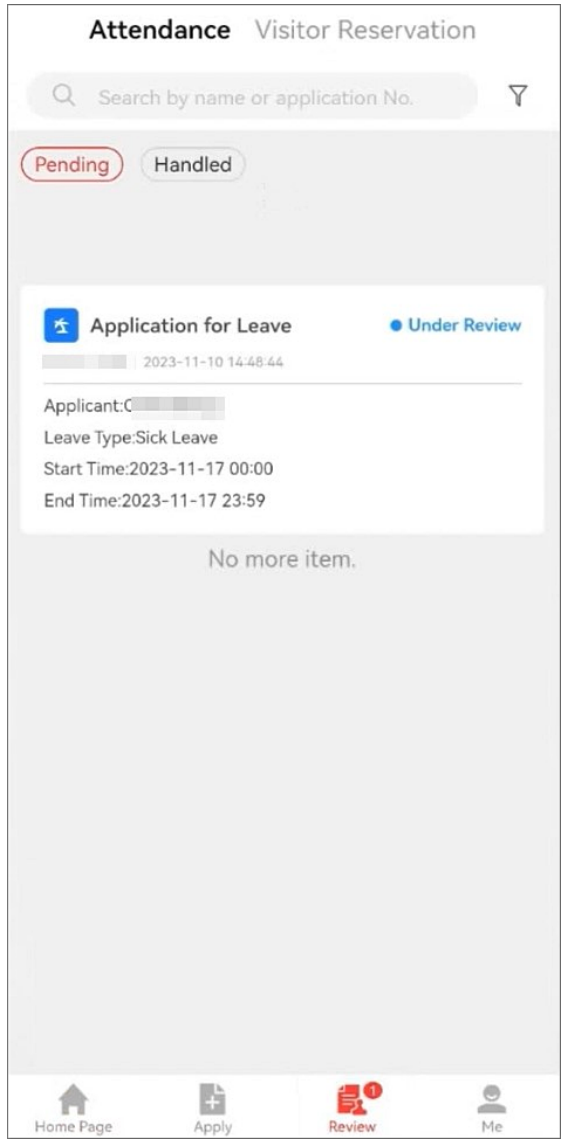



**Figure 25-23 Via the Mobile Client**

## 25.4.6 Step 6: Employees Check Application Status

After applications are reviewed, employees can check their application status on the page where they submit the application via the Web Client or the Mobile Client (Self-Service).

## 25.5 Configure Attendance Rules for Global / Department / Attendance Group

The attendance rule indicates a set of parameters about time and attendance, including the weekend settings, absence rule, overtime parameters, attendance calculation mode, holiday settings, the calculation of leaves, the authentication mode selection of attendance check, etc. It can be defined as a global / department / group attendance rule. You can configure an attendance group with a group attendance rule which has higher priority than the department rule. You can also configure a department with a department rule which has higher priority than the global rule used for the whole company or institution.

Go to **Attendance Rule → Global Rule / Department Rule / Group Rule** . For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

### 25.5.1 Define Weekends

Different countries or regions adopt different weekend convention. HikCentral Professional provides weekends definition function. You can select one or more days of week as the weekends according to actual situation.

In the Weekend Settings area, select the day(s) of week from Monday to Sunday. The attendance data of the selected date(s) will be calculated with the weekend rule.

### 25.5.2 Configure Attendance Calculation Rule

**Calculated by**

**First In & Last Out**: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

**Each Check-In/Out**: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

**Count Work Hours in Check-in/out Period Only**

Only the working hours within the valid check-in and check-out time period are counted as valid working hours. This feature is only effective during normal shifts when using the **First In & Last Out** method. For example, if the valid check-in and check-out time period is from 9:00 to 18:00, and an employee checks in at 8:30 and checks out at 17:00, the valid working hours are from 9:00 to 17:00.

**Consecutive Check-In / Consecutive Check-Out**

This feature is only effective when using the **Each In & Last Out** method. When multiple check-in or check-out records exist for a single day (e.g., at 8:00 AM, 9:00 AM, 4:00 PM, and 5:00 PM):

- **Use Earliest Check-In Time**: 8:00 AM will be used as the record for attendance calculation.
- **Use Latest Check-In Time**: 9:00 AM will be used as the record for attendance calculation.
- **Use Earliest Check-Out Time**: 4:00 PM will be used as the record for attendance calculation.
- **Use Latest Check-Out Time**: 5:00 PM will be used as the record for attendance calculation.

**Enable T&A Status on Device**

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

**Note**

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.
  If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

**Day Change Time**

Set a time to mark the change of a day. For example, if the day change time is set as 08:00:00, check-in before 08:00:00 will be calculated into the attendance of the previous day, and check-in after 08:00:00 will be calculated into the attendance of the current day.

## 25.5.3 Define Absence

You can define the absence rule in the global dimension or define an absence rule for a certain department or attendance group. When the employee's attendance conforms to the absence rule, the attendance record will be marked as absent or other status you define.

In the Absence Settings area, you can define the absence rules.

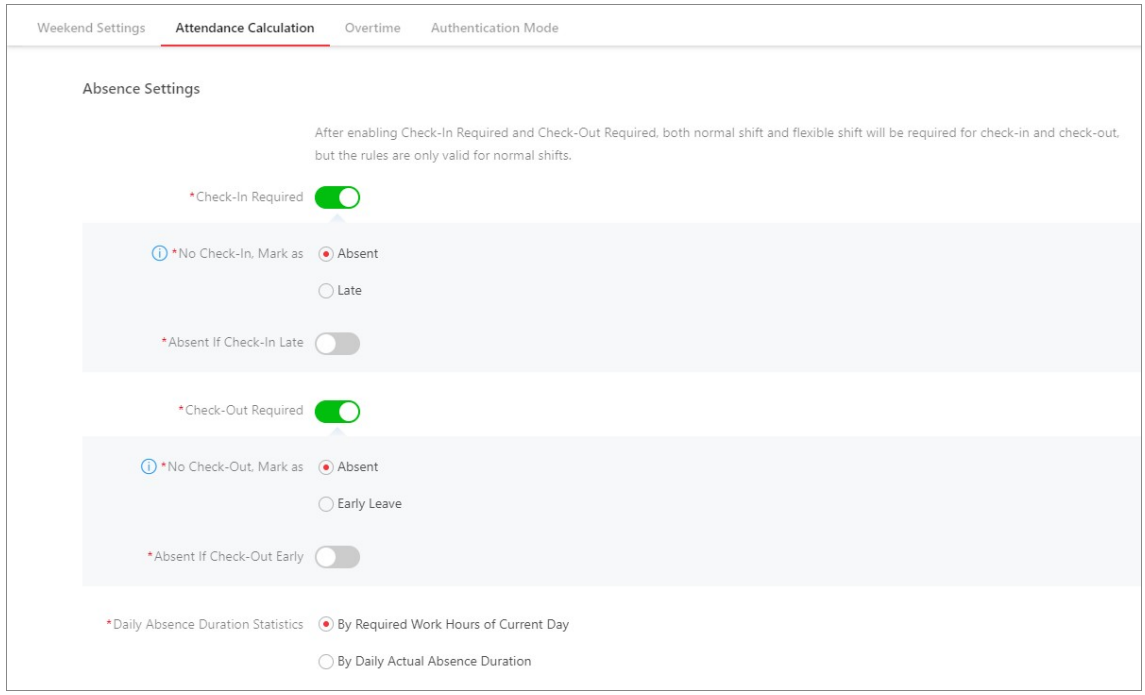



**Figure 25-24 Absence Settings**

## Set Absence Rule for Check-In

Switch on **Check-In Required**. Once this function is disabled, employees will not be required to check in.

In **No Check-In, Mark as**, specify an attendance status when a person does not check in or fails to check in within the valid check-in period. If you select **Late**, you need to set a fixed late duration. For example, if the scheduled start work time is 9:00, valid check-in period is 6:00-12:00 (defined in Timetable - Attendance), **Late Duration** is set to 60 minutes, and **No Check-In, Mark as** is set to **Absent**, the attendance status of an employee will be:

- Normal, if the employee checks in between 6:00 and 9:00.

  **Note**

  You can set overtime rules to count the extra hours before scheduled start work time as overtime. See details in ***Configure Overtime Parameters*** .

- Late, if the employee checks in between 9:01 and 9:59.
- Absent, if the employee checks in after 10:00 or does not check in.

Switch on **Absent If Check-In Late** and set a tolerant threshold in **Late for**. When the employee's check-in time minus scheduled start work time is longer than the **Late for** value, the employee's attendance status on that day will be marked as Absent.

## Set Absence Rule for Check-Out

Switch on **Check-Out Required**. Once this function is disabled, employees will not be required to check out.

In **No Check-Out, Mark as**, specify an attendance status when a person does not check out or fails to check out within the valid check-out period. If you select **Early Leave**, you need to set a fixed late duration.
For example, if the scheduled end work time is 18:00 and valid check-out period is 17:00-21:00 (defined in Timetable - Attendance), and **Early for** is set to 60 minutes, the attendance status of an employee will be:

- Absent, if the employee checks out before 17:00 or does not check out.
- Early Leave, if the employee checks out between 17:01 and 17:59.
- Normal, if the employee checks out between 18:00 and 21:00.

**Note**

You can set overtime rules to count the extra hours after scheduled end work time as overtime. See details in ***Configure Overtime Parameters*** .

Switch on **Absent If Check-Out Early** and set a tolerant threshold in **Early for**. When the scheduled end work time minus employee's check-out time is longer than the **Early for** value, the employee's attendance status on that day will be marked as Absent.

## Daily Absence Duration Statistics

This feature records the specific absence duration of personnel on a daily basis. The duration will be displayed in both the total time card (daily report) and the person attendance summary (summary report). There are two methods for calculating daily absence duration:

- **By Required Work Hours of Current Day**: The required work hours for the current day will be counted as the absence duration and displayed in the **Absent** field of the total time card or the person attendance summary. For example, if the required work hours for the current day are 8 hours, but the actual work hours are 2 hours, the absence duration will be 8 hours.
- **By Daily Actual Absence Duration**: The actual absence duration for the day will be recorded and displayed in the **Absent** field of the total time card or the person attendance summary. For example, if the actual absence duration 2 hours, the absence duration will be 2 hours.

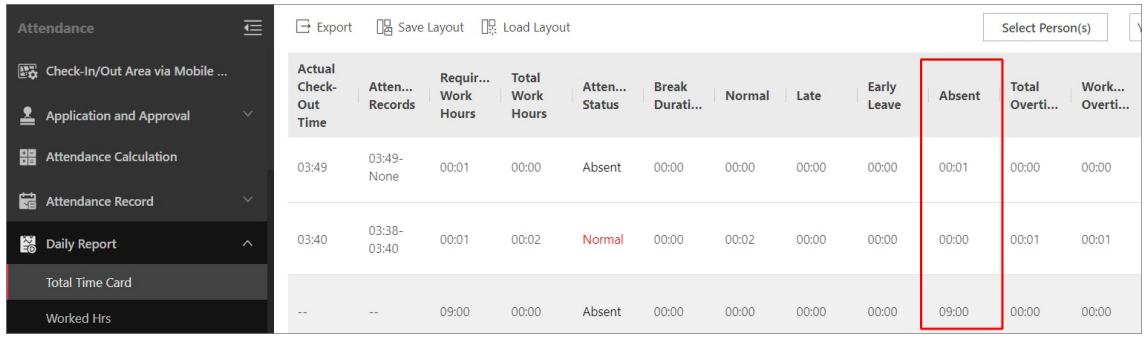



**Figure 25-26 Absence Duration (Total Time Card)**

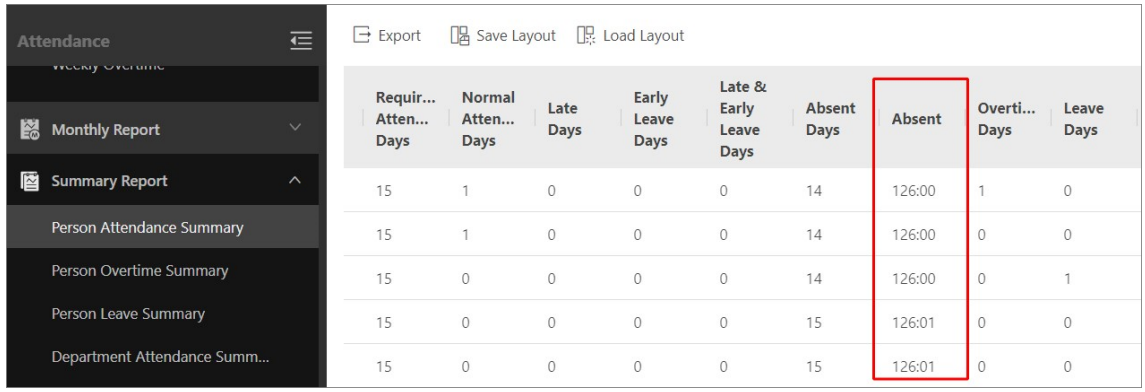



**Figure 25-27 Absence Duration (Person Attendance Summary)**

## 25.5.4 Add Holidays Requiring Attendance

You can set a holiday that requires normal attendance as in weekdays.

**Steps**

1. Select the **Attendance Calculation** tab.

   **Note**

   For details of adding a holiday, see ***Add a Holiday*** .

2. In **Holidays Requiring Attendance** area, select a holiday that requires attendance. You can click **Add** to add a holiday.

## Add a Holiday

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday or an irregular holiday according to the actual scene.

**Steps**

1. Select **Basic Configuration → Holiday Settings** on the left. You can also access the Holiday Settings page in **System**.
2. Click **Add** to add a holiday.

   **Regular Holiday**

   The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of every year.

   You can set the **Start Time** and the number of daysfor the holiday, and choose whether to **Repeat Annually** in the system.

   **Irregular Holiday**

The irregular holiday is suitable for the holiday that is calculated by the day in a specific week, and the specified date might be different every year. For example, Mother's Day is on the second Sunday of each May.

For the **Start Time**, you can set the start day of the holiday. For example, select May, Second, and Sunday for Mother's Day. Then, you can set the number of days for the holiday, and choose whether to **Repeat Annually** in the system.

### 25.5.5 Calculation of Leaves

You can set the status of leaves as normal attendance, leave, or absent.

In the **Attendance Calculation → Leave Settings** area, you can choose to mark leave as **Normal**, **Leave**, or **Absent**. The leave status will be displayed in the attendance results.

### 25.5.6 Configure Overtime Parameters

Overtime is the amount of time a person works beyond scheduled work hours. You can configure parameters, including work hour rate, overtime level, and attendance status for overtime, for workdays, weekends, and holidays.

**Overtime on Workday/Weekend**

**Calculation Mode**

Select a calculation mode.

**By Total Work Hours**

Overtime is calculated according to the extra work hours that exceed the required work hours.

**OT Duration Calculation Mode**

Select a method for overtime duration calculation.

**Fixed**

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

**Actual**

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set the threshold to 60 minutes:

- Overtime duration is 0 if a person works for 59 minutes longer than the required work hours;
- Overtime duration is 61 if a person works for 61 minutes longer than the required work hours.

**By Time Points**

Overtime duration is calculated according to the extra work hours earlier than the start-work time or later than end-work time in one day.

You can enable **Count Early Check-In as OT** and **Count Late Check-Out as OT** to set the overtime duration calculation mode respectively.

**OT Duration Calculation Mode**

Select a method for overtime duration calculation.

**Fixed**

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

**Actual**

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set **Earlier than Check-In Time for Mark as Valid Overtime** to 30 minutes, and the start-work time is 9:00:

- Overtime duration is 0 if a person checks in at 8:31.
- Overtime duration is 31 if a person checks in at 8:29.

**Overtime Level Settings**

Click **Configure Rule** to open the Configure Overtime Rule window. Select an attendance data, and click **Add Rule** to set a total overtime duration and select an overtime mode. You can click **Copy** to copy another day's overtime rule. The total work hours will be calculated according to the work hour rate of each overtime level.

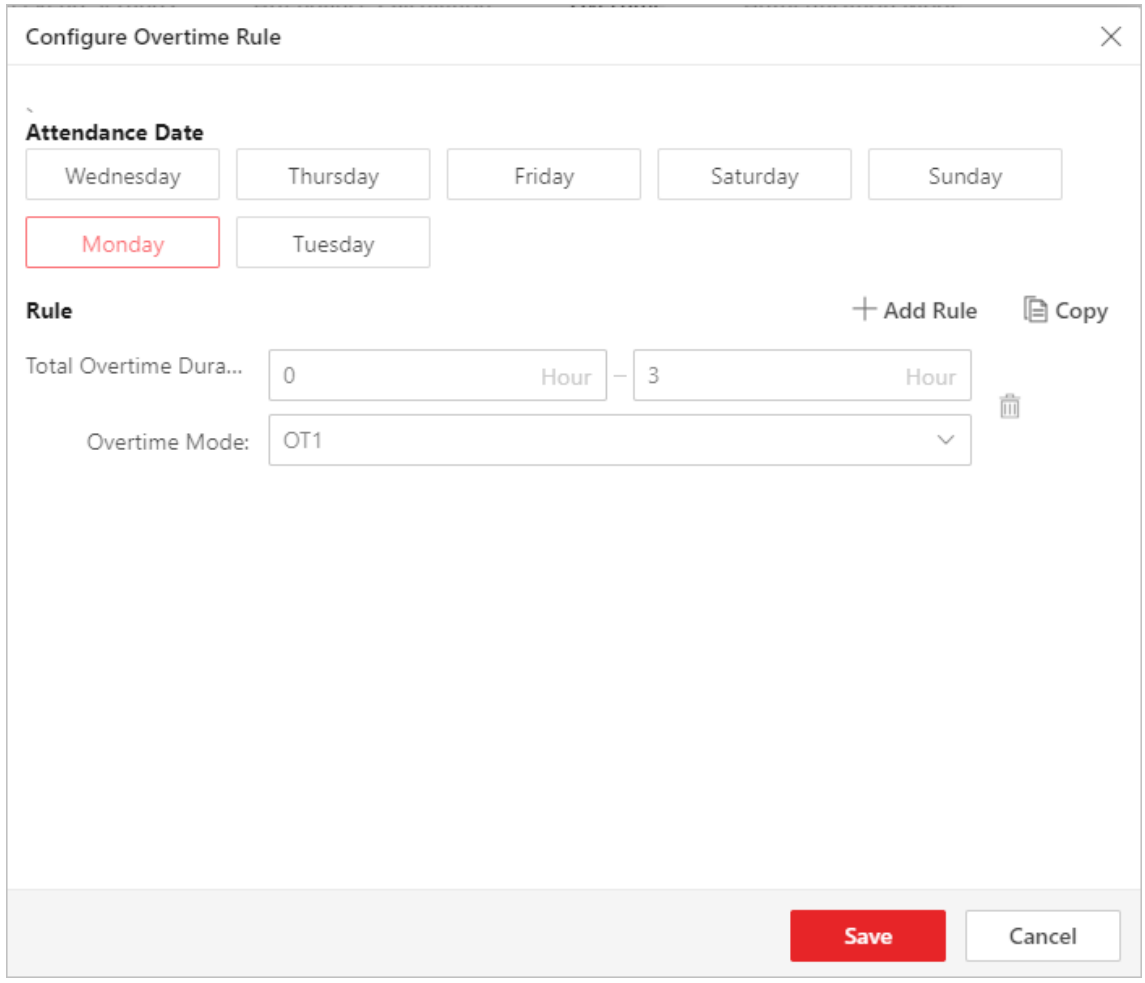



**Figure 25-28 Configure Overtime Rule**

**Overtime on Weekends**

You can switch on **Overtime on Weekends** and set the valid overtime threshold. Then when a person's work hours on weekends are less than the threshold, the overtime will be 0.

**Overtime on Holidays**

**If Works Longer than Mark as Valid Overtime**

Set a minimum threshold for a valid overtime.

**Set Max. Overtime**

Switch on to set an upper limit for the overtime duration in the **If Works Longer than Mark as Invalid Overtime** field. Exceeded work hours will not be counted as valid overtime.

**Overtime Level on Holiday**

Set the overtime level for each holiday.

You can select multiple holidays and click **Batch Set Overtime Level** to batch set the overtime level, or set the overtime level for each holiday separately.

**Note**

- To add a new holiday, click **Add Holiday**.
- To edit holidays, click **Holiday Settings**.

**Overtime Not in Valid Attendance Check Period**

Count the extra work time outside the valid check-in/out period as valid overtime.

### 25.5.7 Configure Authentication Mode

You can configure authentication modes, including card, fingerprint, face, and iris, etc. After setting authentication mode, you can get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

Select **Authentication Mode** on the right, switch on **Customize Authentication Mode**, and select card, fingerprint, iris, faces or/and palm print or palm vein as the authentication mode.

**Note**

This function requires device capability.

## 25.6 Shift Settings and Schedule

After configuring the basic rules, you can configure the attendance shift and schedule:

- **Shift**: Go to **Shift Settings → Break Timetable / Timetable / Shift** .
- **Schedule**: After setting shifts, you need to assign them to departments, groups, persons, or add a temporary schedule and attendance records will be calculated based on these schedules. Go to **Schedule → Schedule → Department Schedule / Group Schedule / Person Schedule / Temporary Schedule** .

### 25.6.1 Add Timetable

The timetable defines the detailed time rules for attendance, such as work time, break time, etc. According to the actual requirements, you can select normal shift or flexible shift as timetable type for further configuration and application, and then the employees need to follow the time rules to check in, check out, etc.

## Add Break Timetables

Break timetables define the start/end time of breaks and the calculation method of break duration. You can create break timetables in advance and use them as templates when configuring break time in a timetable.

**Steps**

1. Select **Shift Settings → Break Timetable** on the left.
2. Click **Add**.
3. Set parameters for the break timetable.

**Name**

Create a descriptive name for the break timetable, such as "Launch Break".

**Start Time**

Start time of the break.

**Earliest Allowable Start Time**

Flexible start time of the break. If a person checks out earlier than **Earliest Allowable Start Time**, the check-out will not be counted as the break start time and no break will be recorded.

**End Time**

End time of the break.

**Latest Allowable End Time**

Flexible end time of the break. If a person checks in later than **Latest Allowable End Time**, the check-in will not be counted as the break end time.

**Break Duration Calculation Mode**

Method for counting the duration of a break.

**Period**

Fixed duration. The actual break start/end time of persons will only be recorded but not be used to calculate the duration of breaks.

**Break Duration**

Set the duration of the break.

**Must Check**

Actual duration calculated by the check-out time and check-in time.

In **Count Early/Late Return**, you need to choose to count early or late return time **By Duration** or **By Time Point**.

**By Duration**

When the actual break duration (end time minus start time) is shorter than or longer than the specified duration, it will be counted as early or late return.

**By Time Point**

When the actual return time is earlier than or later than the specified end time, it will be counted as early or late return.

You also need to set the threshold and the attendance status for the early/late return time.

**If early/late for**

Threshold for counting the early/late return time.

**Mark as**

Choose to count the remaining time of a early return as overtime or the exceeded time of a late return as late, early leave, or absent.

If you do not want to count the early/late return time, set it to **Normal**.

**Set Calculation Mode**

Switch on to set the calculation method of break duration.

**Calculated by**

**First In & Last Out**: Only count and calculate the duration of the first and last check-in/out records during the start/end time of the break.

**Each Check-In/Out**: Count each check-in/out record during the start/end time of the break and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/outs.

**Enable T&A Status on Device**

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

**Note**

To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

4. Click **Add** to finish adding the timetable, or click **Add and Continue** to finish adding the timetable and add a new break timetable.
5. **Optional:** Perform further operations after adding the break timetable.

| | |
|---|---|
| **Edit Break Timetable** | Click on the name of a break timetable to edit it. |
| **Delete Break Timetable** | Select the break timetables you want to delete and click **Delete** to delete them. |

**What to do next**

Use the break timetable to set the break time in a timetable. See ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

## Add Timetable for Normal Shift

Normal shift is usually used for the attendance with fixed schedule. The employees should check in before the start-work time and check out after the end-work time. Otherwise, their attendance status will be late, early leave, or absent. You can add the timetable for normal shift to define the detailed rules (e.g., start-work time, end-work time, late rule, valid check-in/out time, break time, etc.), in order to monitor employees' working hours and attendance.

**Steps**

1. Select **Shift Settings → Timetable** on the left.
2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.
   2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
   3) Select **Normal Shift** as the time period type, and set the following parameters.

      **Scheduled Work Time**

      Range of the scheduled work time, including start-work time and end-work time.

      **Valid Check-In Period**

      If the employee does not check in during the valid check-in period, the check-in will not be recorded and the attendance status will be absent or late depending on the absence settings.

      **Note**

      It is allowed to set the valid check-in period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 08:00:00 on the previous day, set the end time to 10:00:00 on the current day.

      **Valid Check-Out Period**

      If the employee does not check out during the valid check-out period, the check-out will not be recorded and the attendance status will be absent or early leave depending on the absence settings.

      **Note**

      It is allowed to set the valid check-out period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 18:00:00 on the previous day, set the end time to 19:00:00 on the current day.

      **Min. Work Hours**

      Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

      **Flexible Mode**

**Allow Late/Early Leave**

The employees are allowed to arrive late or leave early for a specific period of time. For this mode, you need to set the allowable time for late and early leave. If an employee checks in/out within the period after the start-work time or before the end-work time, the attendance status will be **Normal**. For example, if the start-work time is set to 09:00:00, and the late allowable duration is 30 minutes, and the employee checks in at 09:15:00, the attendance status will be **Normal**.

**Flexible Period**

Flexible period allows employees to extend their start-work time and end-work time. For this mode, you need to set the flexible duration, which defines the extended duration for both start-work time and end-work time. If the total late and early leave time is within the flexible duration, the attendance status will be **Normal**. For example, if the scheduled work time is set to 09:00:00 to 18:00:00, and the flexible duration is 30 minutes, and the employee checks in at 09:15:00, and checks out at 18:15:00, the attendance status will be **Normal**.

**Note**

This feature is available only if you upgrade from HikCentral Professional versions earlier than 2.4. It is not available in the latest version.

4. In **Break Period**, set the following parameters.

**Break Time**

Click **Add** to select one or multiple break timetables. For adding timetables, see ***Add Break Timetables*** .

**Exclude Break Duration from Work Hours**

Enable the function and set the break duration which will not be counted into work hours.

5. In **Attendance Calculation**, set the following parameters.

**Note**

The attendance calculation rule has higher priority than the department, group, and global rules.

**Set Calculation Rule**

Set the calculation method of work duration. See details in ***Configure Attendance Calculation Rule*** .

**Absence Settings**

Set a different absence rule instead of using the general absence rule.

**Note**

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

**Note**

- The overtime timetable has higher priority than the department, group, and global rules.
- See details about setting an overtime timetable in ***Configure Overtime Parameters*** . You can also refer to this chapter for explanations of the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a time line.

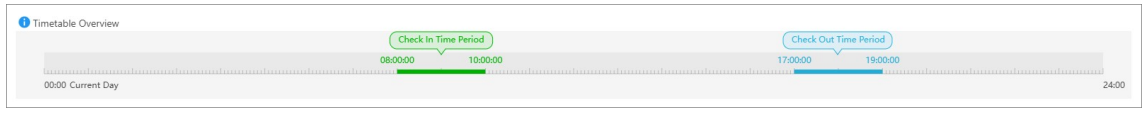



**Figure 25-29 Timetable Overview**

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

**What to do next**

Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

## Add Timetable for Flexible Shift

Flexible shift is usually used for the attendance with flexible schedule. It does not require a strict check-in time and check-out time and only requires that the employees' work hours are longer than the minimum work hours.

**Steps**

1. Go to **Shift Settings → Timetable** .
2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.
   2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
   3) Select **Flexible Shift** as the time period type, and set the following parameters.

      **Valid Check-In/Out Period**

      If the employee does not check in/out within the valid check-in/out period, the check-in/out will not be recorded and the attendance status will be late or absent.

      **Min. Work Hours**

      Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

      **Latest Check-In Time**

      If the actual check-in time is later than this time, the attendance status will be marked as Late.

4. In **Break Period**, click **Add** to select the break timetables to define the break time in the timetable.

**Note**

- You can click **Add** to create a new break timetable. See details in ***Add Break Timetables*** .
- Enable **Exclude Break Duration from Work Hours** and set the break duration which will not be counted into work hours.

5. In **Attendance Calculation**, switch on **Set Calculation Mode**, and set the following parameters.

**Note**

The attendance calculation rule has higher priority than the department and global rules.

**Calculation Rule**

Set the calculation method of work duration. See details in ***Configure Attendance Calculation Rule*** .

**Absence Settings**

Set a different absence rule instead of using the general absence rule.

**Note**

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

**Note**

- The overtime timetable has higher priority than the department and global rules.
- See details about setting a overtime timetables in ***Configure Overtime Parameters*** . You can also refer to this topic for explanations for the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a timeline.




**Figure 25-30 Timetable Overview**

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

**What to do next**

Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

## 25.6.2 Add Shift

Shift is the time arrangement for employees. Shifts can be assigned to employees to regulate their duties. You can adopt one or multiple timetables in one shift.

**Before You Start**

Make sure you have added timetables. See details in ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

**Steps**

1. Go to **Shift Settings → Shift**
2. Click **Add**.
3. Set the shift's basic information, including creating a descriptive name and editing its description.
4. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
5. Set the shift's repeating pattern.

   **Week**

   The shift will repeat every 1 to 52 weeks based on your selection.

   **Day**

   The shift will repeat every 1 to 31 days based on your selection.

   **Month**

   The shift will repeat every 1 to 12 months based on your selection.
6. Select a timetable and click on the table below to apply the timetable on each day.

   **Note**

   You can use up to 8 different timetables in one shift.
7. Switch on **Configure Attendance During Holidays**, and select the holidays. On holidays, the shift will not be effective.

   **Note**

   For setting the holiday, refer to ***Set Holiday*** .
8. Click **Add** to finish adding the shift.

**What to do next**

Assign shift to persons or departments. See details in ***Assign Schedule to Person*** or ***Assign Schedule to Department*** .

## 25.6.3 Manage Schedule

Schedule is used to specify the persons and effective periods during which the persons perform their duties following the attendance rule defined in the shift. After setting the shift, you need to

assign it to the departments, attendance groups,persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this schedule.

## Schedule Overview

The schedule overview shows the schedule information of each person in the department / attendance group. You can also view the detailed schedule of one person for each day in one month/week.

On the left, select **Schedule → Schedule Overview** .

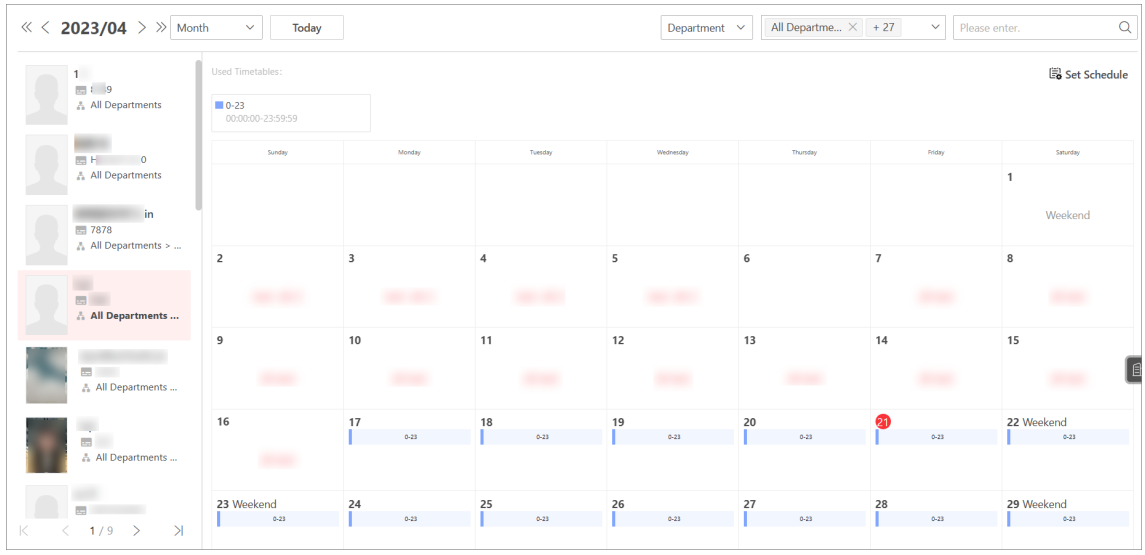



**Figure 25-31 Schedule Overview**

On the top, select **Department** / **Attendance Group** to view the schedule information by department or attendance group.

Select specific department / attendance group.

**Note**

- You can check **Include Sub-Department** to display the persons of sub-departments.
- You can enter keywords to search for specific departments / attendance groups.

On the left, you can view the schedule information about every person in the department / attendance group.

Click the person name to enter the detailed schedule of this person for each day in one month, such as effective period, schedule name, and so on.

You can perform the following operations.

- Select **Month**/**Week** to view the schedule by month or week.
- Click **Today** to locate today in the schedule.

- Click **Set Schedule** to edit the schedule. For details, see ***Assign Schedule to Person*** .
- On the upper-right corner, enter the keyword to search for specific persons to view schedules related to them.

## Assign Schedule to Department

After setting the shift, you need to assign it to the department so that it will calculate the attendance records for persons in the department according to this schedule.

**Steps**

1. On the top left, select **Schedule → Department Schedule** .
2. Open the add schedule page.
3. Set schedule parameters.

   **Effective Period**

   The shift is effective within the period you set.

   **Shift**

   Select a shift to be assigned, and you can click **View** to preview the schedule.

   **Note**

   You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .
4. **Optional:** Click to select attendance check points linked with the schedule.

   Only authentications at the linked attendance check points will be counted.
5. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

   **Check-In Not Required**

   Persons in the person group(s) in this schedule do not need to check in when they arrive.

   **Note**

   This feature is available only if you upgrade from HikCentral Professional versions earlier than 2.4. It is not available in the latest version.

   **Check-Out Not Required**

   Persons in the person group(s) in this schedule do not need to check out when they leave.

   **Note**

   This feature is available only if you upgrade from HikCentral Professional versions earlier than 2.4. It is not available in the latest version.

   **Effective for Overtime**

   The overtime of the persons in the person group(s) in this schedule will be recorded.
6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

## Assign Schedule to Attendance Groups

After setting the shift, you need to assign it to an attendance group so that the platform will calculate the attendance records for persons in the group according to this schedule.

**Steps**

1. On the top left, select **Schedule → Group Schedule** .
2. Click **Add Schedule** to open the Add Schedule pane on the right.
3. In the Attendance Group area, check group(s) you want to assign a schedule to.

   **Note**

   You can click **Add Attendance Group** to add a new one.
4. Set schedule parameters.

   **Effective Period**

   The shift is effective within the period you set.

   **Shift**

   Select a shift to be assigned.

   **Note**

   - click **View** to preview the schedule.
   - Click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .

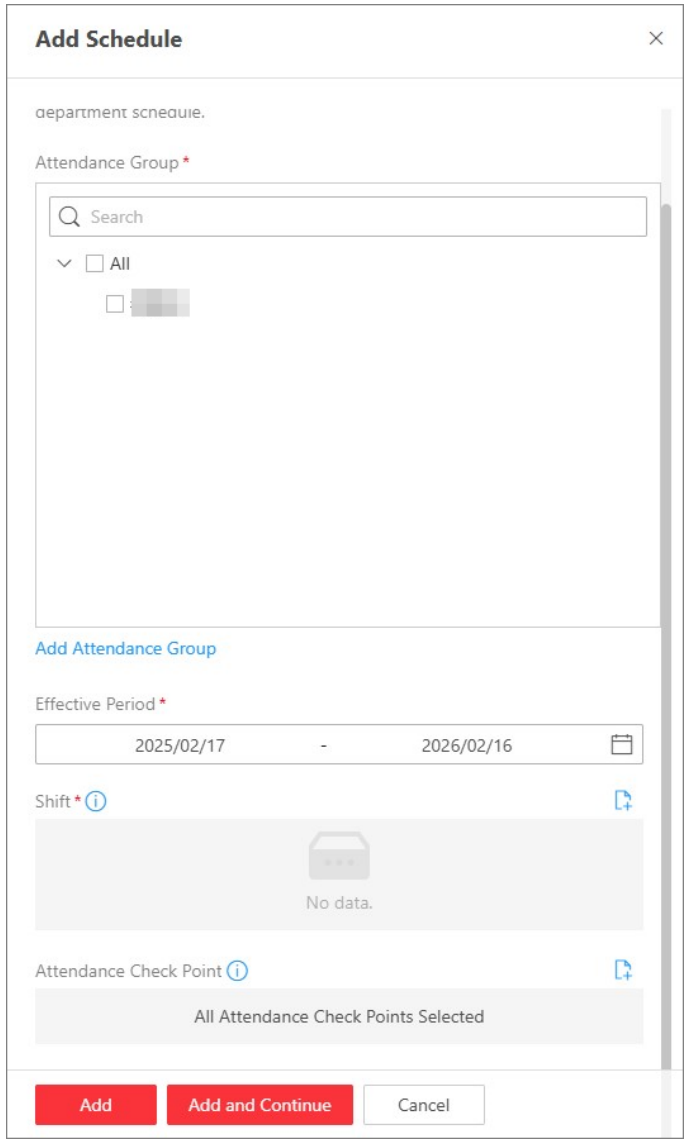



**Figure 25-32 Add Schedule**

5. **Optional:** Click to select attendance check point(s) linked with the schedule.

   Only authentications at the linked attendance check points will be counted.
6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

## Assign Schedule to Person

You can add a person schedule and assign a shift to one or more persons, so that it will calculate the attendance records for the persons according to this schedule.

**Steps**

**Note**

The person schedule has the higher priority than department schedule.

1. On the top left, select **Schedule → Person Schedule** .
2. Click **Add Schedule** to enter the Add Schedule page.
3. On the Add Schedule pane, click to select person(s) you want to assign schedule to,
4. Set required parameters.

   **Effective Period**

   Within the period you set, the shift is effective.

   **Shift**

   Select a shift to be assigned, and you can click **View** to preview the schedule.

   **Note**

   You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .
5. **Optional:** Click to select attendance check points linked with the schedule.

   Only authentications at the linked attendance check points will be counted.
6. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

   **Check-In Not Required**

   Persons in the person group(s) in this schedule do not need to check in when they arrive.

   **Check-Out Not Required**

   Persons in the person group(s) in this schedule do not need to check out when they leave.

   **Effective for Overtime**

   The overtime of the persons in the person group(s) in this schedule will be recorded.
7. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
8. **Optional:** Perform the following operations.

| | |
|---|---|
| **Edit Schedule** | Select a person in the list and click to edit the person's schedule. |
| **Filter Schedule** | Click and set filter conditions such as person name, and then click **Filter** to filter the target schedule. |
| **Delete Schedule** | Select one or multiple schedules in the list and click **Delete Schedule** to delete the schedules. Also, you can click **Delete All** to delete all of the schedules. |

## Add Temporary Schedule

You can add a temporary schedule for a person and the person will be assigned with the schedule temporarily. You can also view and edit the temporary schedule details.

**Before You Start**

You should have added the person(s) and the shift. For details, refer to ***Add Person*** and ***Add Shift*** .

**Steps**

**Note**

The temporary schedule has the higher priority than other schedules.

1. On the top left, select **Schedule → Temporary Schedule** .
2. Click **Add** to enter Add Temporary Schedule page.
3. In **Select Person** area, click and select the needed persons.
4. In **Select Timetable(s)** area, select the needed timetable.

   **Note**

   You can also click to add timetable if needed. For details, refer to ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .
5. Above the calendar, select the year and month.
6. In the calendar area, click one or multiple dates, then the selected timetable will be added to the selected date(s).
7. **Optional:** In the specific date of the calendar, click and select whether to perform the following operations.

   **Clear Shifts**

   Click to clear all schedules of the selected date.

   **Restore to Initial Schedule**

   Click to cancel the adding and restore to the initial schedule.

   **Specify Attendance Check Points**

   Click to select specific devices as the attendance check points. By default, all devices are attendance check points.
8. Click **Finish** on the top right.

## 25.7 Configure Calculation Mode of Attendance Results

You can set the attendance calculation mode as manual calculation or auto calculation. Go to **Attendance → Attendance Calculation → Manual Calculation / Auto Calculation** .

### 25.7.1 Manually Calculate Attendance Results

If department or schedule changes or abnormal attendance records are handled, you can recalculate the attendance results according to the latest data. After re-calculation, the original results will be replaced by new attendance results.

**Steps**

**Note**

HikCentral Professional can calculate the attendance data automatically at a fixed time point (4 o'clock by default) every day. You can edit the time point in **Attendance → Attendance Calculation → Auto Calculation** .

1. Select **Manual Calculation**.
2. Set the start time and end time for attendance calculation.
3. Select target person(s) for attendance calculation.
   - **All Persons**: Calculate all persons' attendance records.
   - **Specified Attendance Group(s)**: Select one or multiple attendance groups for calculation.
   - **Specific Person(s)**: Click to select one or multiple persons for calculation.
4. Click **Calculate**.

**Note**

It can only calculate the attendance data recorded within three months.

### 25.7.2 Set Auto-Calculation Time of Attendance Results

Attendance results calculation refers to calculating the attendance status and duration according to persons' check-in/out records. You can set an auto-calculation time so that the platform will calculate the attendance results for all persons at a specific time every day.

**Steps**

1. Select **Auto Calculation**.
2. Select a time in **Calculate at**.
3. **Optional:** Enable **Recalculate Historical Data**.
4. Click **Save**.

## 25.8 Attendance Records and Reports

You can view persons' attendance records and manage attendance reports (attendance results of the specific departments or persons in a certain time period).

### 25.8.1 View Attendance Records

Persons' attendance records will be recorded and stored in the system. You can view different types of attendance records.

In the **Attendance Record** part of the left navigation bar, select **Transaction**, **Time Card**, **Check In&Out Record**, **First & Last Access Report**, **Leave Record**, **Check In&Out Correction Record**, or **Overtime Record** according to your need.

You can perform the following operations on the pages of attendance records.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- For transactions, click **Import** to import transactions recorded in files or devices to the system.
- Click to customize column items. Custom person information added in **Person → Additional Information** will also be displayed in the items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  **Exporting Allowed**

  After enabled, the layout can be exported in the report.

  **Sharing Allowed**

  After enabled, the layout will be shared among accounts.

  **Fixed Date**

  After enabled, you can set a specific time period for attendance data displayed the layout. Only attendance data generated during this time period will be displayed in the layout.
- Click **Load Layout** to display the report in a layout shared by other users. You can search for a layout before loading it. For layout saved by yourself, you can edit or delete them.
- Click to display each column title completely/incompletely.

## Import Transactions

Transactions on the attendance check devices could fail to be transmitted to HikCentral Professional due to many causes, such as device offline and network connection failure. Or some of your attendance check devices are not added to the platform, but you still need to manage their transactions on the platform. You can use this function to get the latest transactions from the devices.

Select **Attendance Record → Transaction → Import → Import from Device / Import from File** .

## Import from Device

Applicable to getting the latest transactions on the attendance check devices that are added to the platform.
Select the devices that store the transactions, and then select the time range to be imported. Click **OK** to import the transactions within the range on the selected devices.

## Import from File

Applicable to attendance check devices added or not added to the platform.

**Note**

For devices that are not added to the platform, you need to make sure that the devices are supported by the platform. See *HikCentral Professional Compatibility List* for reference.

Many attendance check devices have the ability to export a file that contains persons' transactions. You can import the file to the platform so that the transactions can be managed on the platform.

**Note**

- To export the data file on an attendance check device, please refer to the user manual of the device.
- Usually, you need to enter the back-stage management page of the device to export the event file to a connected external storage device via USB port, and then transfer the event file to the PC where the platform runs.

## 25.8.2 Manage Attendance Reports

Attendance report is the statistics of the attendance results of the specific department(s) or person(s) in a certain time period. For example, the employer or related persons can view the employees' attendance via attendance report and make it as the standard of performance evaluation or pay calculation. You can define the display rules on the report, set the rule of sending reports regularly, add a custom report, and manually export reports.

### Set Display Rules for Attendance Report

You can configure the contents displayed in the attendance report, such as the company name, logo, date format, time format.

On the top left, select **Basic Configuration → Report Settings → Report Display** to set the following display rules.

**Company Information**

The company information (including company name and logo) will be displayed on the cover page of the attendance report. You can customize the company name. You can also upload a picture for the logo.

**Note**

Hover over your cursor on the uploaded logo picture, and you can click **Delete Logo** to delete the picture.

**Format of Date and Time**

The formats of date and time may vary for the persons in different countries or regions. You can set the date format and time format according to the actual needs.

**Display Pay Code or Fixed Code in Report**

**By Symbol**

The exported report displays Pay Code / Fixed Code as symbol.

**By Name**

The exported report displays Pay Code / Fixed Code as name.

## View Daily/Weekly/Monthly/Summary Attendance Reports

You can view and export daily/weekly/monthly/summary attendance reports.

In the Attendance module, select **Daily Report**, **Weekly Report**, **Monthly Report**, or **Summary Report** on the left as needed.

| Report Type | Description |
|---|---|
| Daily Report | Daily report shows data on a daily basis. The report contains data recorded on the day prior to the current day. |
| Weekly Report | The report contains the persons' attendance results of the recent one week. |
| Monthly Report | The report contains the persons' attendance results of the current month. |
| Summary Report | The summary report provides an overview of the person's/ group's/department's attendance results. |

Under these four types of reports, you can select a report as needed.

For some kinds of reports, you can perform the following operations as needed.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- Click **Select Person(s)** and select the desired persons to filter the attendance report by person.
- Click and select the desired time range to filter the attendance report by time range.
- Click and select the order to sort the attendance report.
- Click to customize column items. Custom person information added in **Person → Additional Information** will also be displayed in the items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  **Exporting Allowed**

  After enabled, the layout can be exported in the report.

  **Sharing Allowed**

  After enabled, the layout will be shared among accounts.

  **Fixed Date**

  After enabled, you can set a specific time period for attendance data displayed in the layout. Only attendance data generated during this time period will be displayed in the layout.

- Click **Load Layout** to display the layouts saved by you and the layouts shared by other users. After loading layouts, you can search for a specific layout, and edit or delete the layouts you saved.
- Click to display each column title completely/incompletely.

## Send Attendance Report Regularly

You can set a regular report rule for specific departments, and the platform will send an emails attached with a report (an Excel file) to the recipients daily, weekly, or monthly, showing the attendance records of the persons in these departments during specific periods.

**Before You Start**

Set the email template with recipient information, subject, and content, and set the email parameters such as sender address, SMTP server address and port, etc. For details, refer to ***Email Settings*** .

**Steps**

1. Select **Basic Configuration → Report Settings → Scheduled Report** on the left.
2. Click **Add** (for first time) or click + .
3. Create a report name.
4. Select a type and language for the scheduled report.
5. In **Statistics Content**, select the **Person Selection Method** as **Department** or **Attendance Group**.

   **Note**

   - For Department Attendance / Overtime Summary, you can only select departments. For Group Attendance / Overtime Summary, you can only select attendance groups.
   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and filter persons by status (all, employed, or resigned).
6. **Optional:** For reports excluding Attendance/Overtime Summary and Attendance/Overtime Summary, click **Select Extra Person**, and click to include individual persons whose attendance data will be delivered in this report.
7. In the **Time Settings** section, set the statistical cycle to **By Day**, **By Week**, or **By Month** and set the report time range and sending time.

   **Report Time**

   **Previous day**

   Daily report shows data on a daily basis. The platform will send one report at the sending time every day. The report contains data recorded on the day prior to the current day.

   For example, if you set the sending time to 20:00, the system will send a report at 20:00 every day, containing the persons' attendance results between 00:00 and 24:00 prior to the current day.

   **Last 7 Days / Last 14 Days**

The platform will send one report at the sending time every one or two week(s). The report contains the persons' attendance results of the recent one/two weeks.

For example, for weekly report, if you set the sending time to 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing persons' attendance results of the last week or recent two weeks based on your selection.

**Current Month / Last Month**

The platform will send one report at the sending time every month. The report contains the persons' attendance results of the current/last month of the sending date.

**Note**

To ensure the accuracy of the report, you are recommended to set the sending time at least one hour later than the auto-calculation time of the attendance results. By default, the platform will calculate the attendance results of the previous day at 4 A.M. every day. You can change the auto calculation time in General Rule. See details in ***Set Auto-Calculation Time of Attendance Results*** .

8. In the Export Settings, select a format for the report.

**Note**

If you select PDF, you can customize the paper size and direction of printing.

9. **Optional:** Select and enable the way of sending the report from **Send via Email**, **Upload to SFTP**, and **Save to Local Storage**.

**Note**

- If you enable **Send via Email**, you can click **Add** to add a new email template. For setting the email template, refer to ***Email Settings*** .
- To set up the SFTP or local storage, click > **SFTP Settings** or **Configure Local Storage**.

10. Click **Save** to save the report schedule.

The report will be generated and sent to the recipient at the specified sending time.

## Add a Custom Report

You can create a fully-customized attendance report. After creating a custom report, you can export the report manually or set a schedule to send the report to your email regularly.

**Steps**

1. On the top left, select **Custom Report**.
2. Click + to add a custom report.
3. Create a descriptive name for the report in the **Report Name** field.
4. Choose whether to merge the data of the same person/department/date.
5. Select a sorting rule for records from the **Table Display Rule** drop-down list.
6. Select the data items you want to include in the report from **Optional Fields**.

- Custom fields will be displayed if you have added additional person information in **Person → Additional Information** . These fields can be exported in the report.
- You can drag the items in **Selected Fields** to set the order of the items.

7. **Optional:** Click **Preview** to view the report to make sure the format and content are correct.
8. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
9. **Optional:** Perform further operations.

| | |
|---|---|
| **Edit Report** | Select a report and click to edit it. |
| **Delete Report** | Select a report and click to delete it, or click → **Delete All** to delete all reports. |
| **Export Report** | Click **Export** and specify the departments, target persons, time range, and report format to export the report to the PC. See ***Export a Custom Report*** . |
| **Send Report Regularly** | You can set a schedule to send the report regularly. See details in ***Send Attendance Report Regularly*** . |

## Export a Custom Report

You can specify the department / attendance group, time period, and format to export a custom report to your local PC.

**Before You Start**
Make sure you have ***added a custom report*** .

**Steps**
1. Select a custom report on the left pane, and click **Export** to open the Export Settings page.
2. On the Person Selection Method area, select **Department** / **Attendance Group**.
3. Check the desired departments / attendance groups.

   If you select **Department**, you can check **Include Sub-Department** to display the persons of sub-departments. You can also click to filter persons by status (all, employed, or resigned).
4. **Optional:** Click **Select Extra Persons**, and click to include individual persons whose attendance data will be delivered in this report.
   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and select person status (all, employed, or resigned), or enable **Additional Information** and enter the keyword in the text field to search for matched persons.
5. Specify the time period by selecting the predefined time period, or clicking **Custom** to customize the start and end date.
6. Specify the report format.

   If you select PDF, you can customize the paper size and direction of printing.
7. Enter password and click **Export** to export the custom report to the local PC.

## 25.9 Application Management for Admin

The persons' attendance records will be recorded and stored in the system. As the administrator, you can search for the target persons and perform attendance applications for a single person or multiple persons according to the actual need, including applying for leave, overtime, and attendance correction. After submitting applications, you can view the application details and status of each handling. You can also review (approve or reject) and undo applications.

Go to **Attendance → Application and Approval** .

### 25.9.1 Apply for a Leave / Check-In/Out Correction / Overtime

As the administrator, you can apply for leaves and working overtime, and correcting the check-in or check-out records for the employee(s).

Select **Leave / Check-In/Out Correction / Overtime** and click **Add** in the top left corner.

Select a person or multiple persons and set required parameters.

**Leave Type / Correction Item / Overtime Type**

- **Leave Type**: Sick leave, maternity leave, annual leave, etc.
- **Correction Item**: The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.
- **Overtime Type**: OT1, OT2, and OT3.

**Attendance Check Point**

For Check-In/Out Correction, you can select the specific attendance check point.

**Application Reason (Optional)**

The application reason for the leave / correction / overtime.

**Attachment (Optional)**

The attachment for the leave / correction / overtime application, such as the medical records for sick leave, the certificate of the right attendance time, attendance records, etc.

**Auto Approve (Optional)**

If the box is checked, the added application for the person will be approved automatically.

After applications, you can click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.

You can also review or undo the application. For details, refer to ***Review or Undo Applications*** .

### 25.9.2 Import Applications

As the administrator, you can batch apply for leave, overtime, or attendance correction for multiple employees.

**Steps**

1. Select **Application and Approval → Leave / Check-In&Out Correction / Overtime** on the left.
2. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
3. Click **Import**.
4. In the pop-up window, click **Download Template** and edit the related information in the downloaded template.
5. Click and import the template with the corrected attendance records.
6. Click **Import**.

**What to do next**

You can review or undo the imported applications. For details, refer to ***Review or Undo Applications*** .

### 25.9.3 Review or Undo Applications

As an administrator, after applying for employees' leave, overtime, attendance correction, or check in&out via Mobile Client, you can review (including approving or rejecting) or undoing the application.

1. On the left, select **Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client**.
2. (Optional) Click to filter the target employee by setting conditions (such as name, ID, department).
3. Select the target employee, the employee's application flow will be displayed on the right.
4. You can perform the following operations.
   - (Optional) Click to view the check in/out areas of the employee.
   - Check employee(s) and click **Approve** to approve the employee's attendance application.
   - Check employee(s) and click **Reject** to reject the employee's attendance application.
   - Check employee(s) and click **Undo** to undo the employee's attendance application.

## 25.10 Application Management for Employee

If you are an employee, you can log in to the Self-Service module where you can have an overview of your attendance records, review applications (if you are an administrator and assigned with the approval role as reviewer), and view your schedule. Besides, in this module, you can submit applications for leave, overtime, or attendance correction, and view the details and the handling status of applications. You can also view and export attendance records.

### 25.10.1 Login via Web Client (Employee)

Employees can access the system via web browser.

**Before You Start**

The administrator should enable self-service login and set the login password for employees.

**Steps**

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

   **Example**

   If the IP address of the PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.
2. Select the **Self-Service** tab.
3. Enter the employee ID and password.
4. Click **Log In** to log in to the system.

**Note**

- Employees are required to change the password and set security questions for password retrieval upon the first login.
- If employees forget the password, they can retrieve the password in **Forgot Password** by answering security questions.
- If the password is expired, employees will be asked to change the password upon login.

**Result**

Web Client home page displays after employees successfully log in to the system.

## 25.10.2 Overview of Personal Attendance Data

You can have an overview of your attendance records in a specific time period, review applications, and view personal schedule.

When you log in to the Self-Service module, the overview page will be displayed, which shows the recent and history attendance statistics.

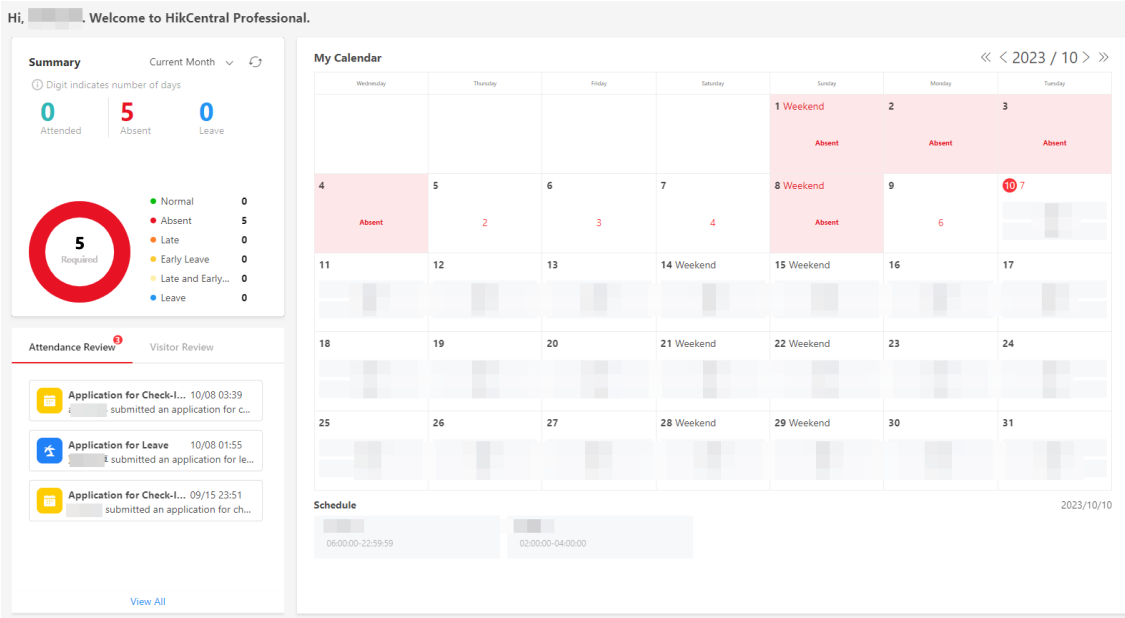



**Figure 25-33 Overview of Personal Attendance Data**

| | |
|---|---|
| Summary | Click ⌄ to select a time period to view the attendance records in the time period. |
| My Calendar | You can have an overview of your attendance data and schedule in a month. Move the cursor to a day on the calendar and click ⚙, you can submit an application for the current day. For details about submitting applications, refer to ***Submit and View Applications*** . |
| Attendance/Visitor Review | You can select an application and click **Handle** to handle the application. |
| Schedule | View personal schedule. |

## 25.10.3 Submit and View Applications

As an employee, you can submit attendance applications for leave, overtime, or attendance correction, and the applications will be reviewed by the administrator. Also, you can view the application details and the application flow to know the status of each handling.

**Note**

For details about reserving a visitor, see the chapter of Visitor Management.

On the left, go to **Apply → Leave / Check-In/Out Correction / Overtime → Pending → Add** .

**Note**

If no approval flow is configured for a person and the option **Transfer to Administrator for Approval When No Approval Flow is Configured** is unchecked, that person will not see the **Add** button for submitting leave, overtime, or attendance correction requests after logging into Self-Service. As a result, they can only view pending or handled applications but cannot create new ones.

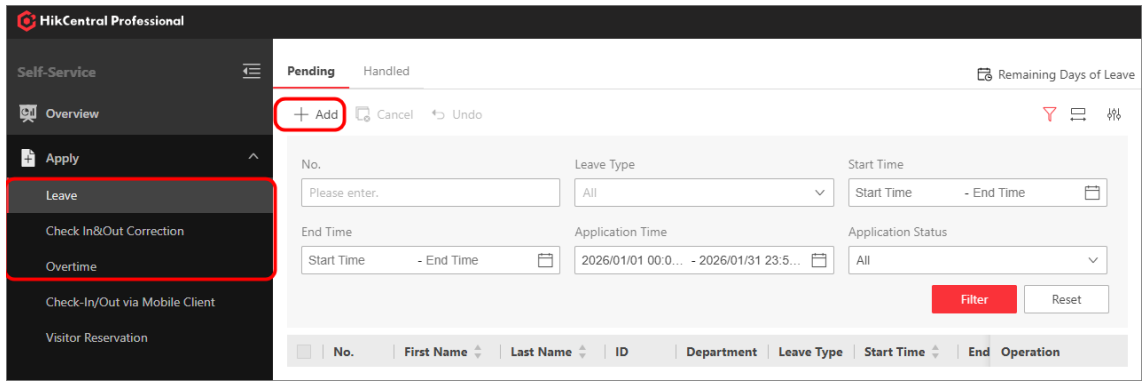



**Figure 25-34 Approval Flow Configured or Administrator Approval Enabled**

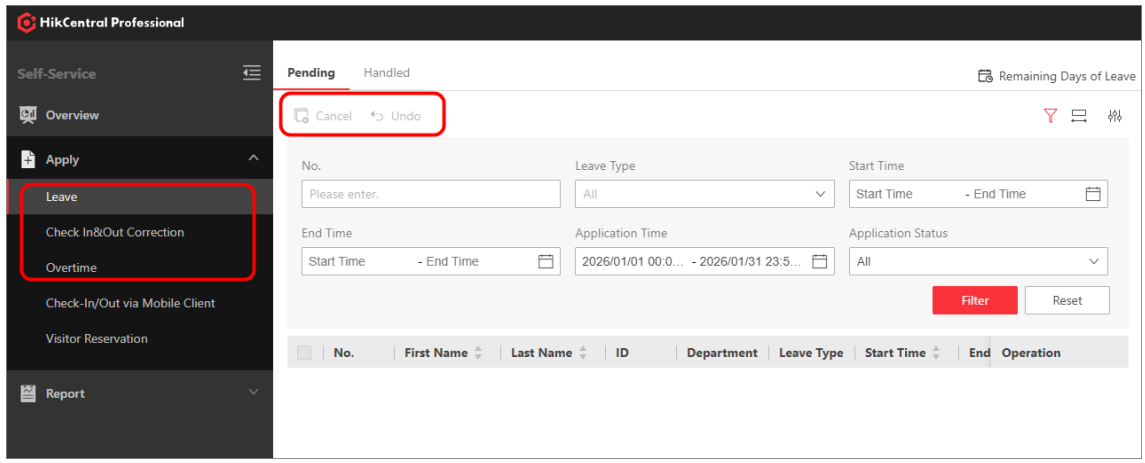



**Figure 25-35 No Approval Flow and Administrator Approval Unchecked**

**Leave Type / Correction Item / Overtime Type**

- **Leave Type**: Sick leave, maternity leave, annual leave, etc.
- **Correction Item**: The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.
- **Overtime Type**: OT1, OT2, and OT3.

**Application Reason (Optional)**

The application reason for the leave / correction / overtime.

**Attachment (Optional)**

The attachment for the leave / correction / overtime application, such as the medical records for sick leave, the certificate of the right attendance time, attendance records, etc.

After applications, you can view and export them. For details, refer to ***View and Export Attendance Records and Reports*** .

## 25.10.4 (Employee) Review or Undo Submitted Applications

The employee can review or undo the submitted application(s) for attendance after logging into the self-service account.

Select **Review → Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client** on the left. Select the **Pending** or **Handled** tab.

You can perform the following operations in the Operation column after checking applications.

- Click to approve the employee's attendance application.
- Click to reject the employee's attendance application.

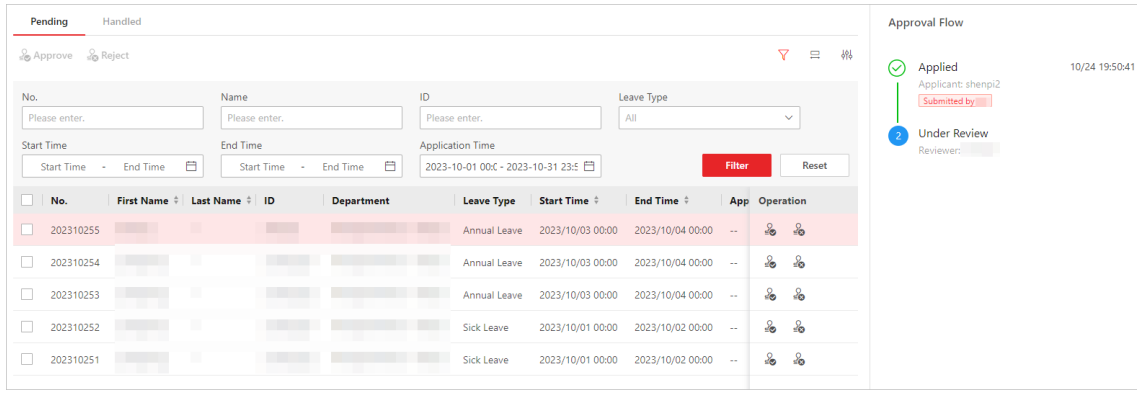



**Figure 25-36 Review Employees' Applications**

## 25.10.5 View and Export Attendance Records and Reports

As an employee, you can view the attendance records and reports. Also, you can export the records or reports in the file format of Excel, PDF, or CSV.

1. Select **Report** on the left.
2. Select the menu item as needed to view the records or report details.
3. You can perform the following operations in the Operation column for application review.

- Click **Export** to export the records or reports in the file format of Excel, PDF, or CSV.
- On the top-right corner, click to select the type of self-adaptive column width (complete or incomplete display of each column title).
- On the top-right corner, click to select the items for custom display in the column.

# Chapter 26 Visitor Management

The system provides an entire process for visitor management from reservation to check-out. You can add visitor information to the system and assign access levels to the visitors to define which doors and which floors the visitors can access with credentials (visitor passes).

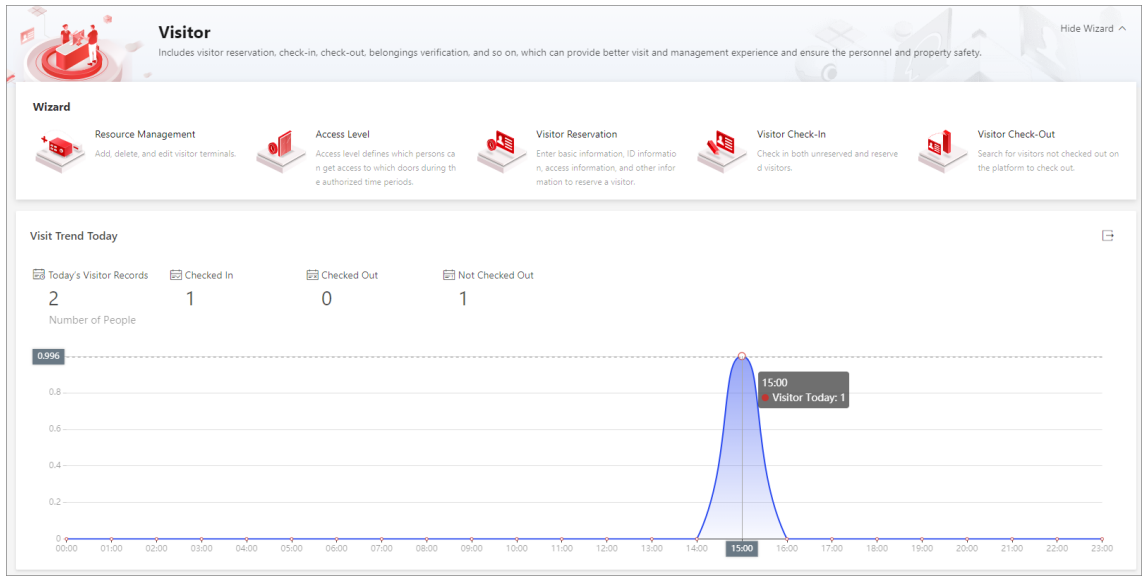



**Figure 26-1 Visitor Information Overview (Wizard & Visit Trend)**

## 26.1 Overall Process of Visitor Management

The flow chart below shows the process of visitor settings management.

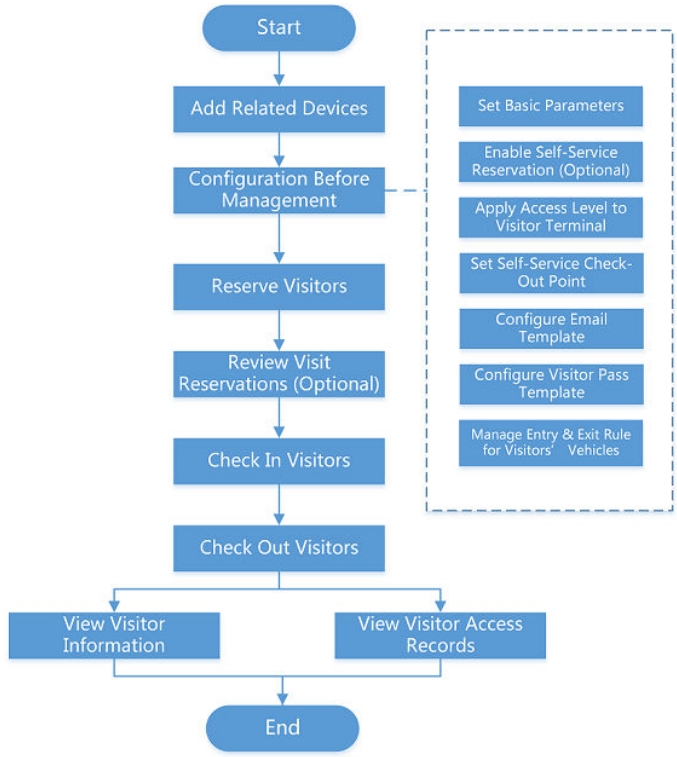



**Figure 26-2 Flow Chart of Visitor Management**

**Table 26-1 Flow Chart Description**

| Procedure | Description |
|---|---|
| Add Related Devices | Add devices used for visitor reservation, check-in, check-out, authentication, etc. |
| Configuration Before Visitor Management | Before any operations in the visitor system, you need to set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc. See ***Basic Configuration Guide*** for details. |
| Manage Entry & Exit Rule for Visitors' Vehicles | Register license plate number of the visitors' vehicles to allow the system to control the barrier to open when capture unit of parking lot detect license plate number. See ***Manage Entry & Exit Rule for Visitors' Vehicles*** . |
| Reserve the Visitors | Before visiting, visitors can make a reservation. The Administrator can make a reservation for the visitors by entering the visitor and host information on the platform. Visitors can also reserve by themselves. After self-reservation, the Administrator should review |

| Procedure | Description |
|---|---|
| | the visitor information to approve or disapprove the reservation. See ***Visitor Reservation Guide*** for details. |
| Visitor Check-In | The platform supports checking in visitors both with or without a reservation. |
| Visitor Check-Out | You should check out for the visitor before him/her leaves, or let visitors check out at self-service check-out point. After checking out, the visitor's access information will expire. See ***Visitor Check-Out*** for details. |
| Manage Visitors & Access Records | Manage all checked-in visitors (including those who have checked out) in the visitor list and perform other operations such as deleting visitors, and check visitor access records. See ***How to Manage Visitor Information and Access Records*** for details. |

## 26.2 Basic Configuration Guide

Before any operations in the visitor system, you need to set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc.

### 26.2.1 Add a Visitor Group

You can add visitor groups to categorize different visitors for convenient management. For example, you can add a business group for visitors coming for business communication and add a tour group for touring visitors. Moreover, you can control other users' access to any visitor group to ensure the security of visitor data if you have corresponding configuration permissions.

**Steps**

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Visitor Information** .
2. Click + to open the Group Name window.
3. Create a visitor group name, and then click **Add** to add a visitor group.

**Note**

System administrators or other roles who have the permission to manage roles can define which HikCentral Professional users have permission to access the visitor group.

4. **Optional:** Perform the following operations after adding the visitor group.

| | |
|---|---|
| **Edit Visitor Group** | Click to change the information about the visitor group. |
| **Delete Visitor Group** | Select a visitor group and click to delete it. |

## 26.2.2 Add Access Level and Parking Lot Permission for Visitors

### Add Access Level for Visitors

An access level contains access points that are accessible during a certain time period. If you select an access level for a visitor for check-in and apply the settings to devices, the visitor can access the access points during the specified time period with credentials.

**Before You Start**

Make sure you have added at least one access level in the Access Control module.

**Steps**

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Permission Management** → **Access Level** .

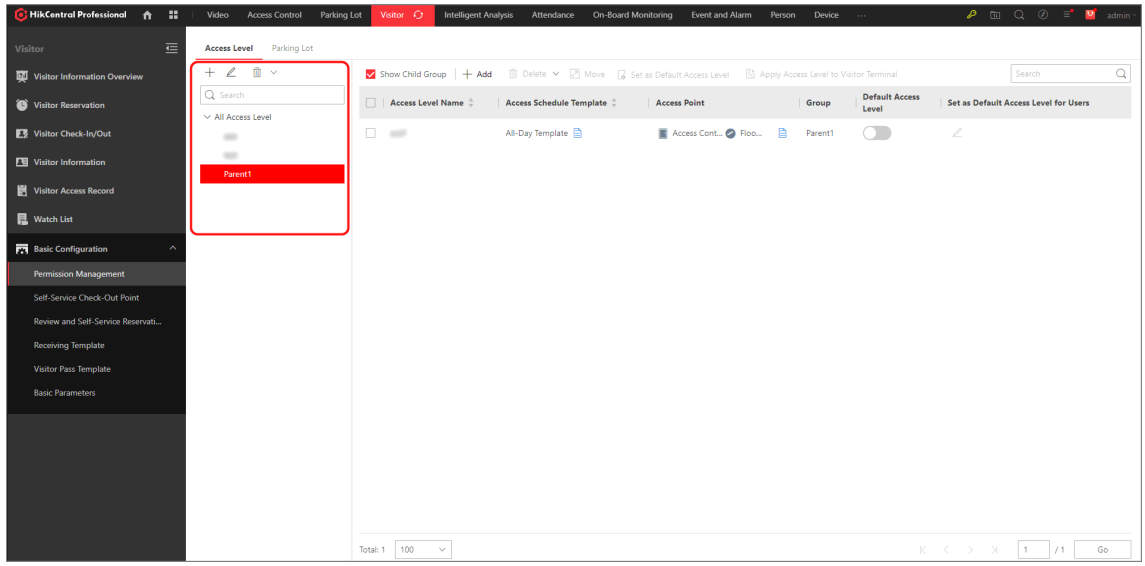



**Figure 26-3 Access Level**

2. Click **+** on the left to add a new access level group or select an existing access level group.
3. Click **Add** on the right.
4. Select existing access levels.
5. Click **Add**.

   The added access levels will be displayed in the access level list. You can view its accessible access points and time periods.
6. **Optional:** Perform the following operations after adding access levels.

| | |
|---|---|
| **View Access Schedule Template Details** | Click in the Access Schedule Template column to view when the access point is accessible for the visitor. |

| | |
|---|---|
| **View Access Point Details** | Click in the Access Point column to view the name of related access points. |
| **Set Default Visitor Access Level for Different Users** | You can set dedicated default visitor access levels for different system users from different departments to enable precise visitor management.<br>You can set via either of the following ways:<br>a. Check the added access levels, and click **Set as Default Access Level**, select users, and click **OK**.<br>b. Select an added access level and switch on the button in the **Default Access Level** column, and click in the **Set as Default Access Level for Users** to select users.<br>The default access level will be automatically selected when a visitor makes reservation for themselves, under the precondition that you have enabled the Self-Service Reservation feature (see ***Set Review and Self-Service Reservation Parameters*** ).<br>The default access level will also be automatically selected when you reserve for visitors again and check in visitors again on the Visitor Information page (see ***How to Manage Visitor Information and Access Records*** ). |
| **Delete Access Levels for Visitors** | Select access levels and click **Delete** to delete the selected access level.<br>Or click → **Delete All** to delete all the access levels. |

**What to do next**

Apply visitor's access levels to the visitor terminals connected to the platform. See ***Manually Apply Visitors' Access Level Settings to Visitor Terminals*** for details.

## Add Parking Lot Permission for Visitors

Manage parking lots for visitor reservation and unreserved check-in.

**Before You Start**

Make sure you have added at least one parking lot in the Parking Lot module.

**Steps**

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Permission Management** → **Parking Lot** .

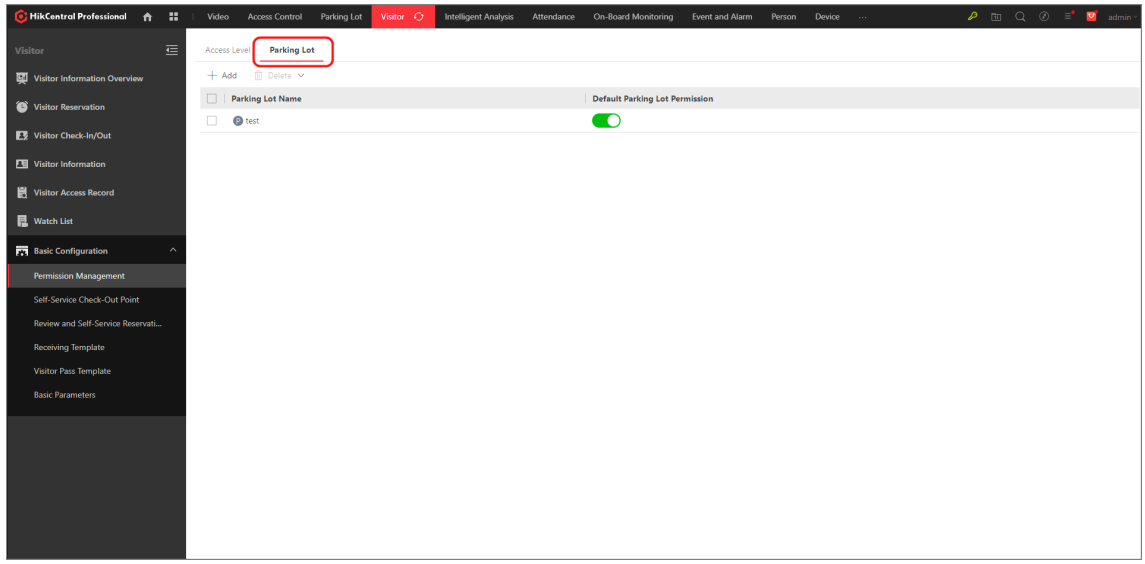



**Figure 26-4 Parking Lot Permission**

2. Click **Add**.
3. Select existing parking lots.
4. Click **Add**.
5. **Optional:** Turn on the button in the **Default Parking Lot Permission**, so the corresponding parking lots will be selected by default during reservation and unreserved check-in.

## 26.2.3 Manually Apply Visitors' Access Level Settings to Visitor Terminals

If you have added visitors to an access group, or deleted/edited visitors of an access group, or changed access levels of an access group, you have changed the access group's settings. In these cases, you should apply the changes to the connected visitor terminals to make the changes take effect.

### Before You Start

- Make sure you have added access levels for visitors.
- Make sure you have added the visitor terminal to the platform.

### Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Access Level** .
2. Select the access levels that need to be applied to visitor terminals.

   **Note**

   You can select up to 10 access levels that need to be applied.
3. Click **Apply Access Level to Visitor Terminal** to apply the selected access levels to the visitor terminals.

If the applying process failed, will be displayed next to **Apply Access Level to Visitor Terminal**. In this case, you can move the cursor to it and then click **View** or **Apply Again** to view the failure details or apply the access levels again respectively.

### 26.2.4 Set Review and Self-Service Reservation Parameters

Self-service reservations refer to visit reservations made by visitors themselves. You can set whether to auto approve the reservations. You can also enable the Self-Service Reservation feature to get a QR code, which you can send to visitors to allow them to make visit reservations by scanning the QR code. In addition, you can set related parameters to ensure that self-service reservations meet the visitor management standards of your organization/company.

**Steps**

**Note**

Self-reserved visitors are only allowed to access the access points contained in the default access level for visitors.
To configure a different access level for a visitor, you need to make a reservation for them. For details, refer to ***Visitor Reservation Guide*** .

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Review and Self-Service Reservation** .
2. **Optional:** Enable **Auto Approve Reservation**.
   If you enable this, visitor reservations will be approved automatically. If you disable this, visitor reservations need to be approved according to the configured approval flow. The configuration is only valid to the current users.
3. Enable **Self-Service Reservation**.
   The platform will generate a QR code. After downloading the QR code, you can print it or send it to the hosts or visitors who are going to reserve. The host can scan the QR code to reserve for the visitor, while the visitor can also scan the QR code to reserve if the visitor knows the visitor's person ID.

   **Note**

   QR codes generated by different users are different, and a user can only review the visitors reserved via the QR code the user generated, which allows different users to manage their own visitors independently.
4. **Optional:** Configure the following parameters.

   **Face Quality Verification**

   After the visitor uploads a profile picture by a cellphone, the selected device will automatically start checking the profile picture's quality. If the profile picture is not qualified, the visitor will be notified. Only when the uploaded profile picture is qualified can the visitor reserve successfully. Otherwise, the visitor information cannot be uploaded to the platform.

**Note**

To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

**Visitor Group**

Select a visitor group. After reserving successfully, the visitors will be added to the group. If you do not select, the visitor will be added to the default visitor group.

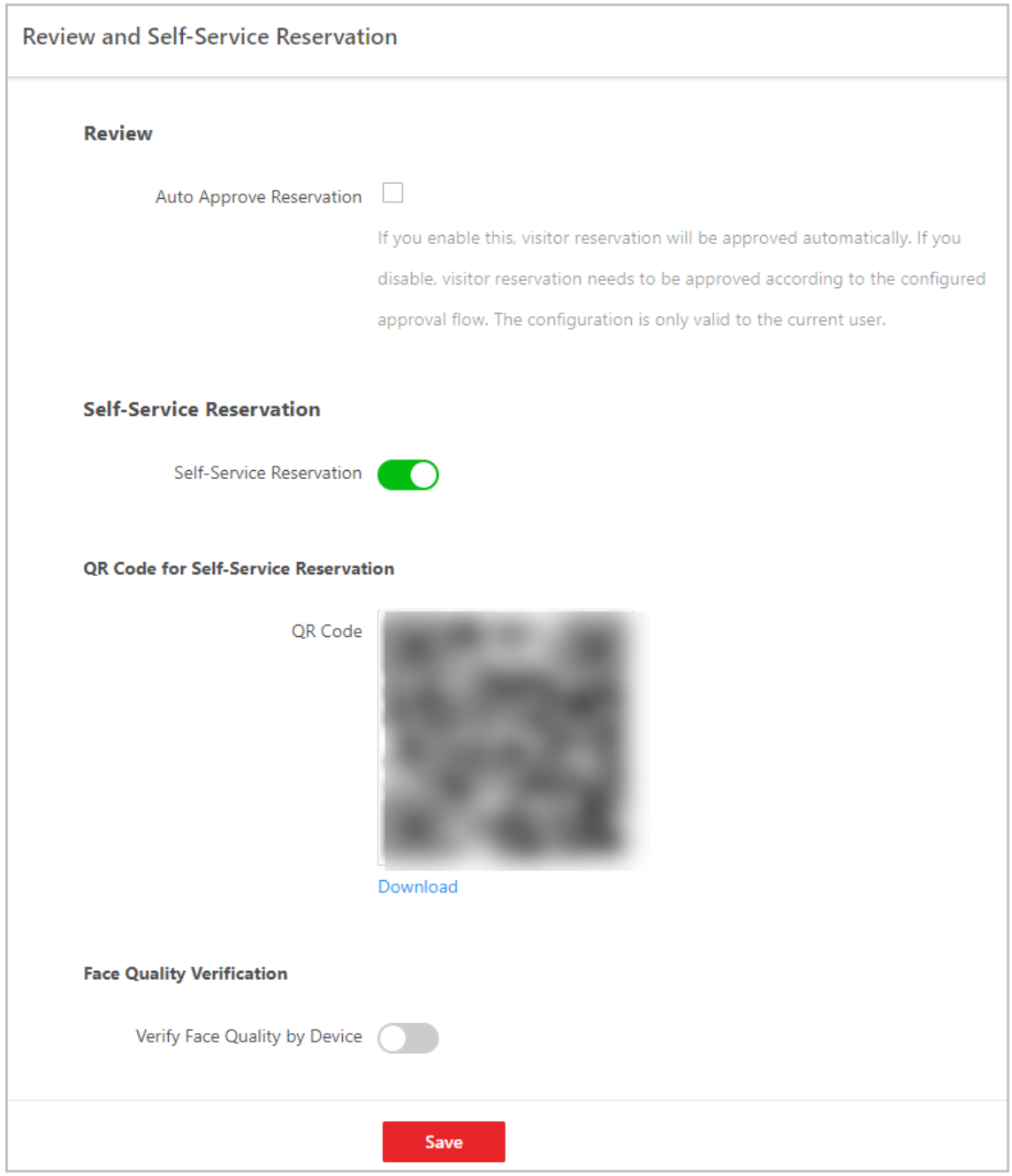



**Figure 26-5 Review and Self-Service Reservation**

5. Click **Save**.

**Note**

If the auto approval of visitor reservation has been disabled, you will be prompted to configure the approval flow. Click **Yes** to enter the Approval Flow page to configure a visitor approval flow.

## 26.2.5 Set Self-Service Check-Out Point

After setting self-service check-out points, visitors can check out by credentials at the self-service check-out points without the help of receptionists. If you have issued a card to a visitor when you check in the visitor, after checking out, the visitor should put the card in the place for card collection. The access permission granted via visitor cards, fingerprints, face pictures, and QR codes will expire automatically.

**Before You Start**

Make sure you have added at least one device that supports this function.

**Steps**

**Note**

This function needs to be supported by devices.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Self-Service Check-Out Point** .
2. Click **Add** to show the resource list.

   **Note**

   You can enter a keyword of a door name in the searching bar to search for wanted doors.
3. Select one or more doors / card readers and click **Add**.

   **Note**

   - If there are two card readers related to one door, you can specify one for check-out, so the other one can be used for check-in.
   - After setting self-service check-out points, the visitors can check out at the points according to the assigned access levels by swiping cards or fingerprint/face authentication.




**Figure 26-6 Set Self-Service Check-Out Point Page**

4. **Optional:** Select a self-service check-out point and click to cancel setting the door as a self-service check-out point.

## 26.2.6 Add Visitor Receiving Template

You can set the receiving template (including the template type, recipient, and content) so that the platform can send emails or WhatsApp messages automatically to the recipient according to the predefined template.

**Before You Start**
Before adding the template, you should set the sender's email account first.

**Steps**
1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Receiving Template** .
2. Click **Add**.
3. Enter the required parameters.

**Template Name**

Set the template name.

**Receiving Mode**

The platform sends emails or WhatsApp messages.

**Template Type**

The email type defines when the platform automatically sends a predefined email or WhatsApp message to the recipient.

**Recipient**

Set the type of the email recipient (visitor or host).

**Subject**

Enter the subject for the email template if required. You can also click the button in the lower part of the window to add the related information to the subject.

**Template Content**

Define the content to be sent. You can also click the buttons below **Content** to add the related information to the content.

**Note**

If you add the arrival time to the email subject or email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed time period may have some deviations.

**Text on Button**

If required, define the text on the button for WhatsApp messages.

**Picture**

For email templates, upload a picture to show in the email if needed.

4. Finish adding the template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed in the email template list.

## 26.2.7 Add Visitor Pass Template

The platform offers default receipt and card templates of visitor passes. If the default templates do not meet your needs, you can add a template to customize the style.

### Add Receipt Visitor Pass Template

The platform offers a default receipt template that defines a default style. If the default style does not meet your needs, you can add a receipt template to customize the style.

**Steps**

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Visitor Pass Template** → **Receipt Template** .
2. Click + to enter the Create Receipt Template page.

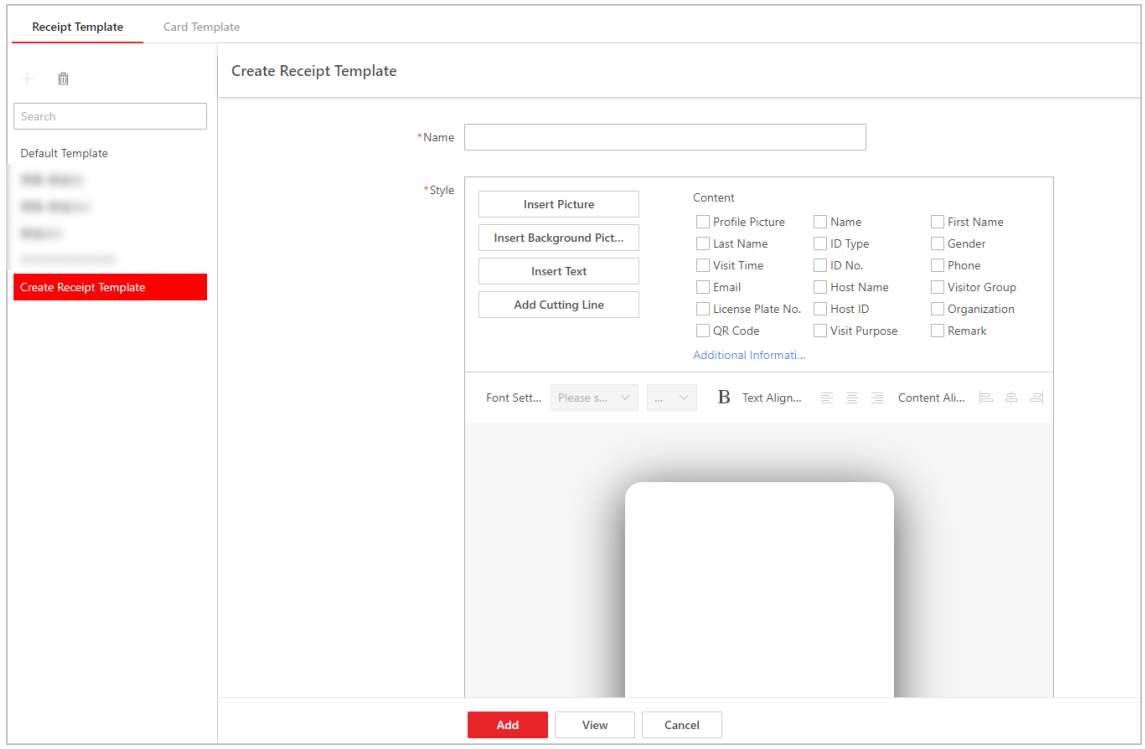



**Figure 26-7 Create Receipt Template Page**

3. Create a name for the receipt template.

4. Perform one or more of the following operations to add elements to the template.

| | |
|---|---|
| **Insert Background Picture** | Click **Insert Background Picture** to select a picture from the local PC and set it as the background of the template. |
| **Set Content** | Check the check-box(es) to add the content element(s). Or click **Custom Information** and then select element(s) in the pop-up window to add them. |

**Note**

Make sure you have set custom visitor attributes; otherwise, **Custom Information** will be unavailable. For details about setting custom visitor attributes, see ***Set Basic Parameters*** .

| | |
|---|---|
| **Insert Picture** | Click **Insert Picture** to select a picture from the local PC and add it to the template. |
| **Insert Text** | Click **Insert Text** to add a text box to the template.<br>You can set the font, font size, and text alignment for the entered text. |
| **Add Cutting Line** | Click **Add Cutting Line** to add a cutting line to the template. |

5. Adjust positions of the added elements.

| | |
|---|---|
| **Manually Adjust Position** | Drag an element to adjust its position. |
| **Align Elements** | Drag to select elements and then click , , or . |
| **Adjust Position via Right-Click Menu** | Right click an element and then click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down**. |

6. **Optional:** Right click an element and then click **Delete** in the right-click menu.
7. **Optional:** Click **View** to preview the template.
8. Click **Add** to add the template.

   The added template will be displayed in the template list on the left.
9. **Optional:** Perform the following operations.

| | |
|---|---|
| **Edit a Template** | Select a template from the template list to edit it. |
| **Delete a Template** | Select a template from the template list and then click . |

## Add Card Visitor Pass Template

The platform offers two default card templates (horizontal and vertical). If the default templates do not meet your needs, you can add a card template to customize the style.

**Steps**

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Visitor Pass Template** → **Card Template** .

2. Click + to enter the Create Card Template page.

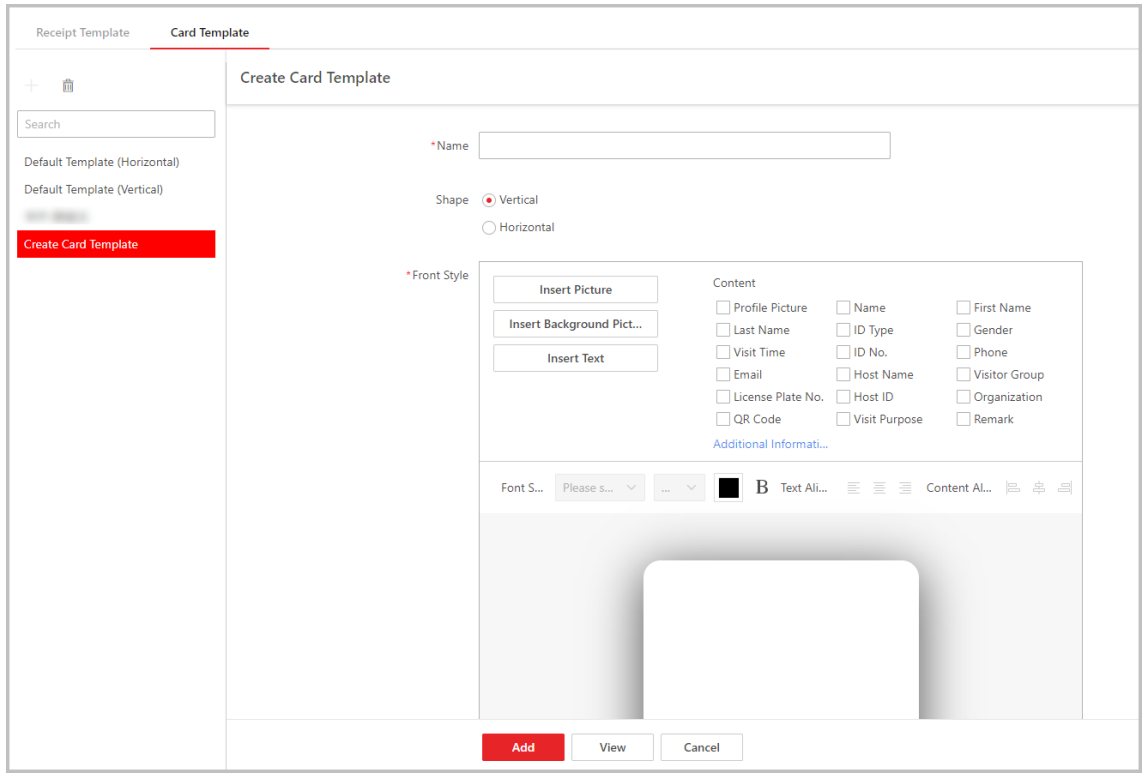



**Figure 26-8 Create Card Template Page**

3. Create a name for the card template.
4. Set the shape of the card template to **Vertical** or **Horizontal**.
5. Perform one or more of the following operations to add elements to the template in the Front Style section.

**Insert Background Picture**
Click **Insert Background Picture** to select a picture from the local PC and set it as the background of the template.

**Set Content**
Check the check-box(es) to add the content element(s). Or click **Custom Information** and then select element(s) in the pop-up window to add them.

**Note**

Make sure you have set custom visitor attributes; otherwise, **Custom Information** will be unavailable. For details about setting custom visitor attributes, see ***Set Basic Parameters*** .

**Insert Picture**
Click **Insert Picture** to select a picture from the local PC and add it to the template.

| | |
|---|---|
| **Insert Text** | Click **Insert Text** to add a text box to the template.<br>You can set the font, font size, color, and text alignment for the entered text. |

6. Adjust positions of the added elements.

| | |
|---|---|
| **Manually Adjust Position** | Drag an element to adjust its position. |
| **Align Elements** | Drag to select elements and then click , , or . |
| **Adjust Position via Right-Click Menu** | Right click an element and then click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down**. |

7. **Optional:** Right click an element and then click **Delete** in the right-click menu.
8. **Optional:** Set the back style.

**Note**

The operations are the same as that of the front style. You can refer to steps 5 to 7 when you set the back style.

9. **Optional:** Click **View** to preview the template.
10. Click **Add** to add the template.

The added template will be displayed in the template list on the left.

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

| | |
|---|---|
| **Edit a Template** | Select a template from the template list to edit it. |
| **Delete a Template** | Select a template from the template list and then click . |

## 26.2.8 Set Basic Parameters

To manage visitors in actual scenarios, you can set basic parameters such as Take Photo of Visitor's Belongings, Default Check-Out Time, Visiting Purpose, and Digits of Reservation Code.

**Steps**

**Note**

If you do not configure basic parameters, the platform will manage visitors according to the default settings.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Basic Parameters** .
2. Configure the following parameters according to your needs.

**General Settings**

**Take ID Photo as Visitor Profile Picture**

If enabled, the ID photo can be read via a connected passport reader and set as the visitor profile picture when you reserve for a visitor or check in a visitor without reservation.

**Auto Import Visitor Face Picture to Face Picture Library**

When this is enabled, the system automatically syncs visitor photos to the default Visitor Face Group during reservation or check-in, and removes them after check-out, effectively reducing false alarms triggered by strangers. Additionally, visitor records now display linked face picture library information for easier management.

**Visit Purpose**

You can define visiting purposes as options on the Reserve page. Click **Add** to add a new visiting purpose. You can also edit the name of an added visiting purpose, delete an added visiting purpose, or search for a visiting purpose.

**Custom Visitor Attribute**

Click **Add** to add custom visitor attributes. The added ones will be displayed as fields on the Reserve page and the Unreserved Visitor Check-In page.

You can set a custom visitor attribute as a **General Text**, **Number**, **Date**, or **Single Selection** field. For example, if you name a custom visitor attribute as ***Covid-19 Vaccination Date*** and set it as a **Date** field, it will be displayed on the Reserve page as shown in the figure below.

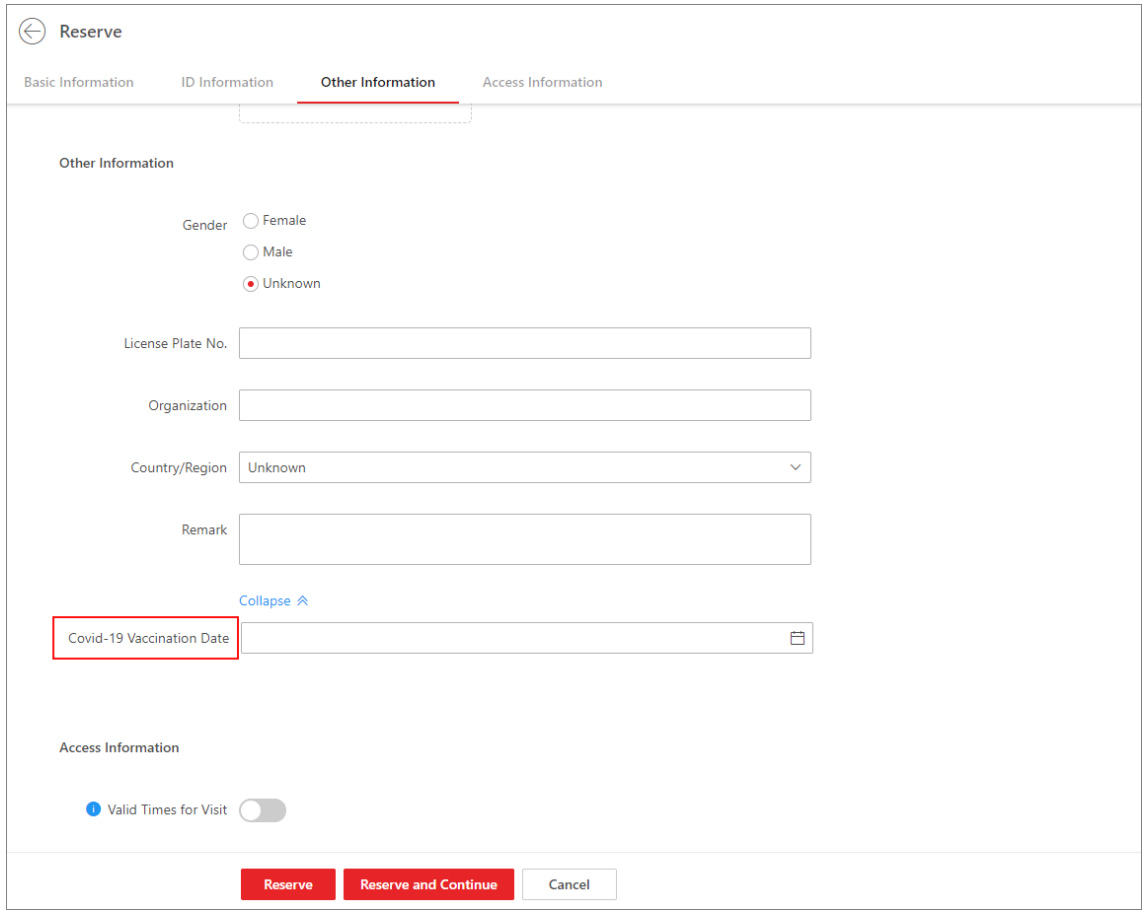



**Figure 26-9 Example**

### Custom Field for Reservation & Check-In

Turn on **Show or Hide** for fields to display on the visitor reservation page and the visitor check-in page.

Moreover, you can check the boxes in the **Set as Required** column to set corresponding fields as required fields.

**Note**

When the area settings is set to **Middle East and North Africa** in **Vehicle → Vehicle Information → Area Settings** , the country/region of license plate, plate category, license plate size, license plate type, and license plate color are offered in the **Custom Field for Reservation & Check-In**.

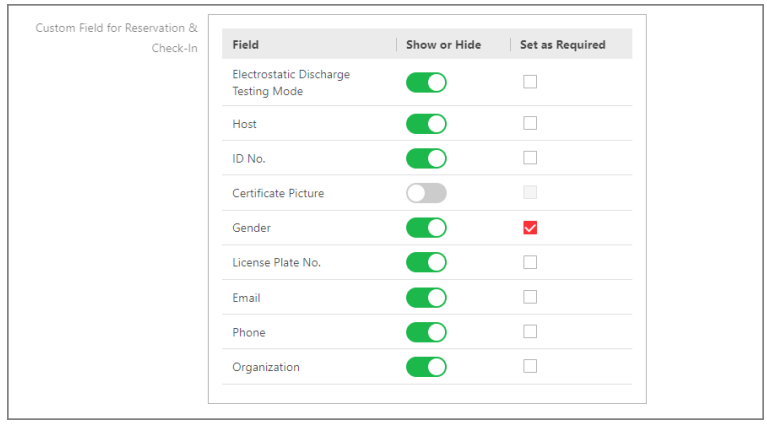



**Figure 26-10 Check Fields to Display**

### Visitor Reservation

#### Check-In Not Required If Reservation Confirmed

Applicable to reception areas where neither a receptionist nor a visitor terminal is deployed. If this is checked, visitors will be automatically checked in when reservations are made for them.

#### Digits of Reservation Code

Define the number of digits (4 digits or 6 digits) contained in each reservation code. The visitor reservation code acts as a verification code for visitor check-in. After reservation, the visitor will receive the reservation code by email and text message. When checking in, the visitor should provide the reservation code.

#### Send Email When Reservation Approved

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visit reservation is approved.

#### Send Email When Reservation Rejected

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visit reservation is rejected.

#### Send WhatsApp When Reservation Approved

Send WhatsApp to the visitor.

#### Send WhatsApp When Reservation Failed

Send WhatsApp to the visitor.

#### Send WhatsApp When Reservation to Be Reviewed

Send WhatsApp to the visitor.

#### Send First Message to WhatsApp

Send WhatsApp to the visitor.

**Note**

- If the recipient is the host, make sure that the host's email address is provided when you add the host to the platform. For details, see ***Add a Single Person Manually*** .
  If the recipient is the visitor, make sure that the visitor's email address is provided when you make a reservation for or check in the visitor.
- You can customize email templates according to your needs. See ***Add Visitor Receiving Template*** for details.

**Visitor Check-In**

**Print Visitor Pass Once Checked In**

When checked, the printer connected to your PC will automatically print a visitor pass once a visitor is checked in.

**Format of Visitor Pass**

Select **Receipt** or **Card** as the format of the printed visitor passes.

**Visitor Pass Template**

Select a template as the one that will be automatically printed.

You can click **View Template** to preview the selected template.

**Note**

Make sure you have set templates as needed. For details about setting visitor pass templates, see ***Add Visitor Pass Template*** .

**Take Photo of Visitor's Belongings**

If you enable this function, you can take a picture of the visitor's belongings and upload it to the platform when checking in/out the visitor.

**Send Email When Checked In**

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visitor checks in.

**Note**

- If the recipient is the host, make sure that the host's email address is provided when you add the host to the platform. For details, see ***Add a Single Person Manually*** .
  If the recipient is the visitor, make sure that the visitor's email address is provided when you make a reservation for or check in the visitor.
- You can customize email templates according to your needs. See ***Add Visitor Receiving Template*** for details.

**Visitor Check-Out**

**Default Check-Out Time**

The default check-out time will be displayed on the Reserve page. After setting the time, you need not enter the visitor check-out time when reserving for a visitor. By default, the check-out time is 23:59:59. You can specify a time according to your needs.

**Visitor Not Checked Out After Exit Time**

If a visitor does not check out before the end time of the visit or the exit time, the platform can automatically check out the visitor or trigger an alarm.

**Check Out Automatically**

When this is selected, if a visitor does not check out before the end time of the visit or the exit time, the platform will automatically check out the visitor. You can set the **Detection Frequency** for detecting whether the visitors have checked out. For example, if you set it to 30 min, the platform will check the visiting status of all visitors every 30 minutes on the platform. The **Detection Frequency** should range from 30 to 60 minutes.

**Trigger Alarm**

When this is selected, if a visitor does not check out before the end time of the visit or the exit time, an alarm will be triggered for notification. You can set the **Alarm Detection Frequency** for detecting whether the visitors have checked out. For example, if you set it to 3 min, the platform will check the visiting status of all visitors every 3 minutes on the platform. The **Alarm Detection Frequency** should range from 3 to 10 minutes.

**Authorization Code for Self-Authentication on Visitor Terminal**

Set the authorization code for allowing visitors to perform self-authentication on visitor terminals. The authorization code will be the initial verification code for all visitor terminals connected to the platform. The receptionist (or other similar staff) needs to enter the authorization code to allow visitors to skip authentication.

**Note**

This parameter is available only when the visitor terminal is added to the platform.

**Send Email When Checked Out**

Send an email based on the selected email template to the host specified in the template when a visitor checks out.

**Note**

- Make sure that the host's email address is provided when you add the host to the platform. For details, see ***Add a Single Person Manually*** .
- You can customize email templates according to your needs. See ***Add Visitor Receiving Template*** for details.

**Visitor Information Reading**

**ID Type for Recognition**

- By checking **Passport**, you can read and collect visitor information on their passports via the KR420 passport reading device.
- By checking **United Arab Emirates / Thai / Ecuador / Argentina ID Card**, you can read and collect visitor information (email, phone number, expiration date, and so on) on the United Arab Emirates / Thai / Ecuador / Argentina ID cards via the corresponding ID card reader.

**Verify Visitor ID Validity Period**

If you enable this, the reading device will check the validity of the IDs provided by visitors and a hint will come up if the IDs have expired. If this is disabled, the validity of ID will not be checked.

**Visitor Credential**

**Unlocking Door by PIN**

When **Visitor PIN** is enabled, visitors can enter using the PIN. Set **PIN Digits** to define the number of digits of the generated PIN. You can check **Auto Generate PIN** to auto generate the PIN during reservation.

**Unlocking Door by QR Code**

Set the QR code mode for unlocking the door: static QR code (remaining unchanged on visitor information and visitor pass) and dynamic QR code (changing regularly after the set time period, in your phone or the invitation link).

3. Click **Save**.

**Note**

After you click **Save**, the platform will apply the authorization code to all the connected visitor terminals. If the authorization code failed to be applied to specific visitor terminals, will appear next to **Authorization Code for Self-Authentication on Visitor Terminal**. In this case, you can move the cursor to the icon and then click **View** or **Apply Again** to view the failure details or apply the authorization code to visitor terminals again.

## 26.2.9 Manage Entry & Exit Rule for Visitors' Vehicles

If one visitor comes by driving a vehicle, when checking in, you need to enter the license plate number so that the platform can make the barrier open when the capture unit of the parking lot detects this license plate.

### Default Vehicle List for Visitors

There is a default vehicle list which is for the vehicles of visitors and is only in the Vehicle module. After visitor check-in, if you enter the license plate number for the visitor, the license plate number will be displayed in this default vehicle list automatically.
You can click to edit the color of the vehicle list and enter description for the list if needed.

**Note**

This vehicle list cannot be deleted.

### Entry & Exit Rule for Visitors' Vehicles

There is one default entry & exit rule for the vehicles of the checked-in visitors on the **Entry & Exit Rule** page.
By default, the rule is that whenever the vehicles in the list enter/exit the parking lot, the platform will automatically open the barrier. You can edit the rule according to actual needs.

**Note**

This rule cannot be deleted.

## 26.3 Visitor Reservation Guide

Before visiting, visitors can make a reservation. The Administrator can make a reservation for the visitors by entering the visitor and host information on the platform. Visitors can also reserve by themselves. After self-reservation, the Administrator should review the visitor information to approve or disapprove the reservation.

### Applicable Scenario

Before visitors gain access to a facility, the administrator makes reservations for visitors on the platform, or visitors make reservations for themselves and then the administrator approves the reservations on the platform.

**Table 26-2 Roles**

| Role | Description |
|---|---|
| Visitor | Ask the park administrator to make a reservation for them, or reserve by themselves. |
| Park Administrator | Make reservations for visitors and approve visitor reservations. |

### 26.3.1 Option 1: Administrator Makes Reservations for Visitors

**Note**

Before any operations in the visitor system, you can set the parameters according to actual situations such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc. See ***Basic Configuration Guide*** for details.

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .
2. Click **Reserve** on the top left to enter the Reserve page.
3. Set the basic information for the visitor, such as the name, visitor group, email, phone, and license plate number. You can also set a profile picture for the visitor.

**Note**

- You can connect a KR420 passport reader to read the information on the visitor's passport/ID card (including the name, ID No., and ID photo) and set the information for the visitor automatically. You have to enable the corresponding ID Type for Recognition on the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a United Arab Emirates / Thai / Ecuador / Argentina ID card reader to read the information on the visitor's corresponding ID card (including the name, ID No., ID photo, email, phone number, and expiration date) and set the information for the visitor automatically. You have to enable the corresponding ID Type for Recognition on the Basic Parameters page. See ***Set Basic Parameters*** .
- You can customize parameters such as the visit purpose. See ***Set Basic Parameters*** .
- Enter the email address for the visitor to receive an email containing the reservation code or notification that the reservation is approved/rejected.
- The license plate number will be shared with the parking lot system so that the visitor's vehicle will be allowed to enter or exit the parking lot.

4. Set the visiting information (visit purpose, hosts, estimated entry time, access level, etc).

**Visit Purpose**

Business, training, etc.

**Host**

Add up to 5 hosts. Each host with different visiting settings.

**Estimated Entry Time**

Set the estimated entry time for the visitor.

**Access Level**

Click **Configure** to assign access levels to the visitor so that the visitor can access the corresponding access points according to the access schedule of the access levels.

**Note**

To add a new access level for the visitor, see instructions in ***Add Access Level and Parking Lot Permission for Visitors*** .

**PIN**

If **Unlocking Door by PIN** is enabled in **Basic Parameters**, this field will be displayed. You can set the PIN manually or click **Auto Generate** to generate one.

**Valid Times for Visit**

The maximum times a visitor can access certain doors or floors by QR code authentication. For example, if you set it to 4, the visitor can access the authorized doors and floors up to 4 times by QR code authentication.

**Extended Access**

If you check **Extended Access**, the access points that are configured with extended open duration will stay unlocked or open longer for the visitor.

5. Set ID information for the visitor, including the ID type, ID No., and ID picture.
6. Set other information, such as the gender, organization, country/region, and remark.
7. Click **Configure** to set the parking lot permission.
8. Click **Reserve** to finish the reservation, or click **Reserve and Continue** to finish the reservation and continue to reserve for other visitors.

**Note**

Under the precondition that you have enabled **Check-In Not Required If Reservation Confirmed**, when a visitor is reserved, the platform will perform the following operations automatically:

- Checks in the visitor.
- Applies the access level to the visitor.
- Sends an email with a QR code to notify the specified recipient that the visitor is checked in (if the email address is provided).

### 26.3.2 Option 2: Administrator Imports Visitor Reservation Information

**Note**

Before any operations in the visitor system, you can set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, assigning access levels to visitors, etc. See ***Basic Configuration Guide*** for details.

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .
2. Click **Import** to open the Import Visitor Reservation Information panel.
3. Click **Download Template** to save the template file in your PC.
4. In the downloaded template, enter the visitor information following the rules in the template.
5. Click and select the excel file with visitor information from local PC.
6. Check **Replace Repeated Visitor**.

**Note**

If you check **Replace Repeated Visitor**, the existing visitor information (with repeated certificate type and number) in the list will be replaced. Otherwise, importing visitors with repeated certificate number will fail.

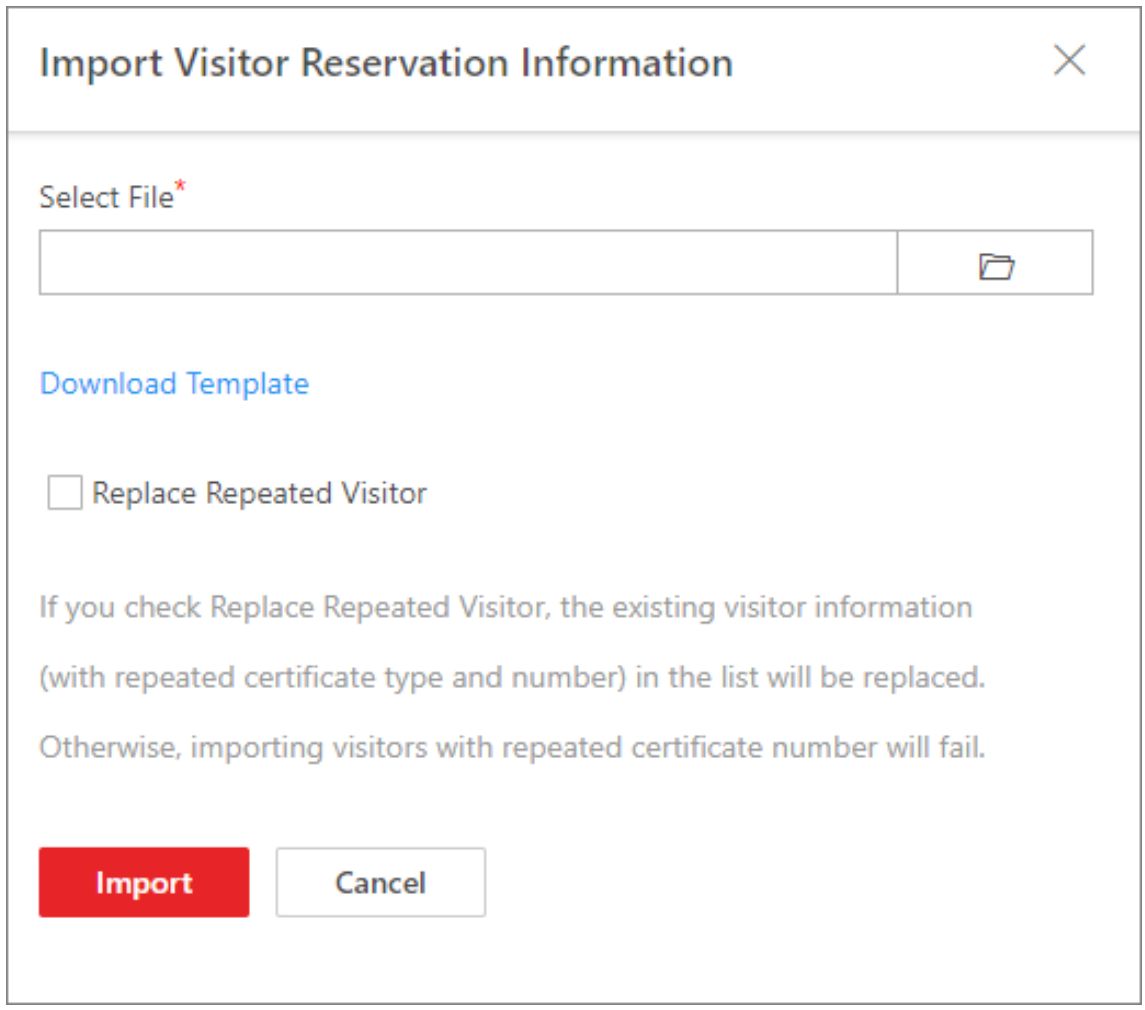



**Figure 26-11 Import Visitor Reservation Information**

7. Click **Import**.

### 26.3.3 Option 3: Administrator Reviews Visitor Self-Service Reservations

If you have enabled self-service reservation when you set visitor self-service reservation parameters, after the visitors reserve, their information will be displayed on the Visitor to Be Approved page. You should review their information to approve or reject the reservations. After approving, they will be added to the target visitor group.

**Note**

1. Make sure you have enabled self-service reservation and configured related parameters. See ***Set Review and Self-Service Reservation Parameters*** for details.
2. You need to have the permission ( **User Permission → Configuration Permission → Visitor → Visitor Reservation and Review → Review** ) shown in the picture below before you can review reservations.
3. If you are set as a reviewer in the visitor approval flow, you can review the visitors. If you are the administrator, all expired flows and all flows with no reviewers will be shown on the page for you to review.

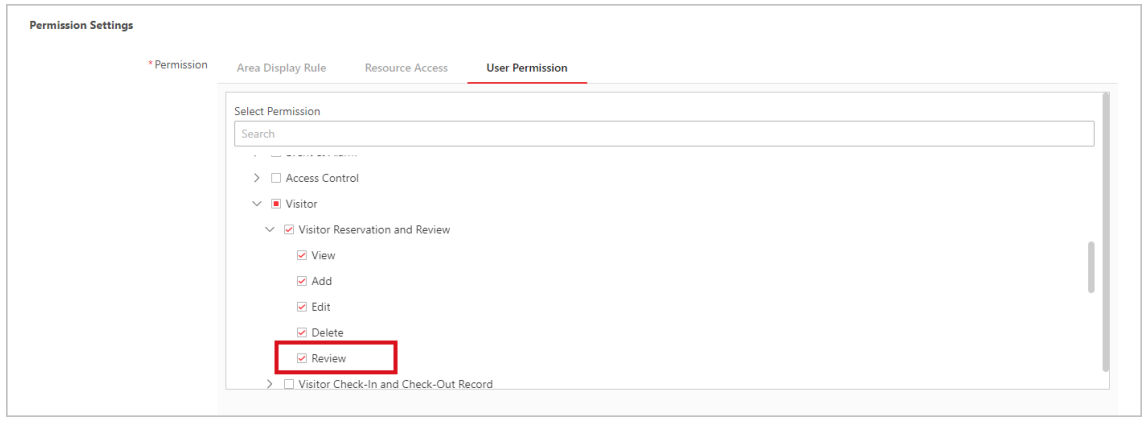



**Figure 26-12 The Permission for Reviewing Reservations**

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .
2. For visitors to be approved, click to approve the reservation, or click to reject the reservation.

   **Note**

   Approved visitors will be added to the target visitor group; rejected ones will not be added to the target visitor group, but they will stay in the Visitors to be Reviewed list.
3. Click to filter reserved visitors by name, ID, status, etc. to quickly find your wanted visitors.

## 26.4 Visitor Check-In Guide

The platform supports checking in visitors both with or without a reservation.

### 26.4.1 Option 1: Check In a Reserved Visitor

If a visitor has a reservation, you can check in the visitor by entering reservation information and visitor information.

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Check-In/Out → Visitor Check-In** .
2. Click **Reserved Visitor Check-In**.
3. Select a reservation credential type.
4. Enter the reservation code, or phone number, or select a ID type and enter the ID No.
5. Click **Edit Visitor Information** to edit the visitor information.
6. Click **Check In**.

**Note**

If the operation succeeds and you have enabled **Print Visitor Pass Once Checked In** when you set basic parameters, the Preview window will pop up showing the preview of the visitor pass for the visitor. You can click **Print** on the window to print the visitor pass.

7. Go back to the Visitor Check-In page to check whether the visitor information fails to be applied to the visitor terminal(s). If it fails, check failure details, troubleshoot, and apply again.

**Note**

If there is visitor information failing to be applied to visitor terminal(s), a notification will show above the visitor list on the Visitor Check-In page. In this case, you can click **View** to view the failure details and troubleshoot according to the reasons shown on the window, and then click **Apply Now** or **Apply Again** to apply the visitor information to visitor terminal(s) again.

8. Perform these operations on the Visitor Check-In page if needed.

| Operation | Description |
|---|---|
| Export Visitors | Select visitors and click **Export** to export checked-in visitors to the local PC as a file. |
| Edit Visitor Information | Click on a visitor (checked in but not checked out yet) to edit the information. |
| Download a Visitor QR Code | Click in the **QR Code** column to download the QR code for the visitor. You can print it or send it to the visitor for identity authentication at access points. |
| Print a Visitor Pass | Click to print the visitor pass for the visitor. |

## 26.4.2 Option 2: Check In a Visitor Without Reservation

Prior to a visitor's arrival or when the visitor arrives, you need to add the visitor's information to the platform. Once added and checked in, the visitor can authenticate by biometrics (including the fingerprint and face) or QR code, and be able to access the predefined doors and floors.

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Check-In/Out → Visitor Check-In** .
2. Click **Unreserved Visitor Check-In**.
3. Enter the first name and last name.
4. Set other basic information, including the profile picture, visitor group, email, phone, and license plate number.

**Note**

- For visitors who have visited before, you can click **Select** next to **First Name** to reuse the information.
- You can connect a KR420 passport reader to read the information on the visitor's passport/ID card (including the name, ID No., and ID photo) and set the information for the visitor automatically. You have to enable the corresponding ID Type for Recognition on the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a United Arab Emirates / Thai / Ecuador / Argentina ID card reader to read the information on the visitor's corresponding ID card (including the name, ID No., ID photo, email, phone number, and expiration date) and set the information for the visitor automatically. You have to enable the corresponding ID Type for Recognition on the Basic Parameters page. See ***Set Basic Parameters*** .
- You can set the visitor profile picture in four ways: collecting a face picture from devices, taking a picture by the camera of your computer, uploading a picture saved in your computer, or reading from the passport / ID card via passport reader (as mentioned in the previous list item).
- Enter the email address for the visitor to receive an email containing the QR code or notification that the visitor has checked in.
- The license plate number will be shared with the parking lot system so that the visitor's vehicle will be allowed to enter or exit the parking lot.

5. Click **Credential Management** to set the credentials for the visitor, including the card, fingerprint, and iris.

**Card**

Issue a card to the visitor to assign the card number to the visitor. You can enter the card number manually, or swipe a card on the card enrollment station, enrollment station, or card reader to get the card number, and then issue it to the visitor.

**Note**

Only one card can be issued to a visitor.

a. Click + in the **Card** field.
b. Place the card that you want to issue to this visitor on the USB fingerprint recorder, fingerprint and card reader, or enrollment station, and the card number will be read automatically. Or you can enter the card number manually.

**Note**

You can click **Card Issuing Settings** to set the issuing parameters.

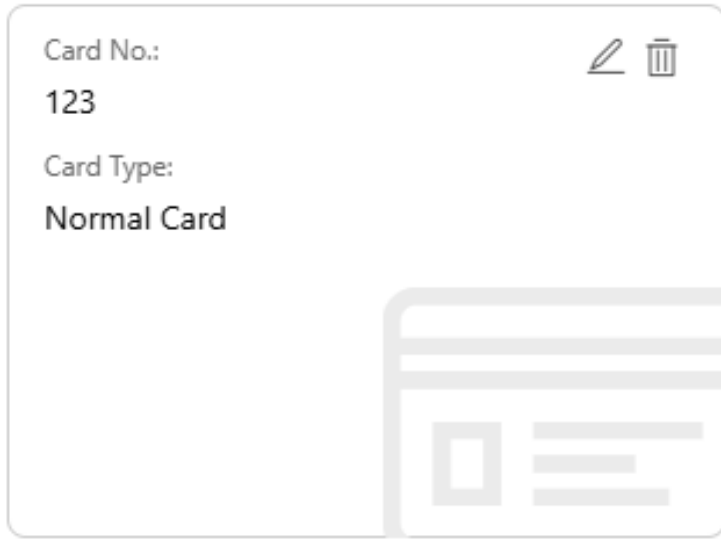



**Figure 26-13 Read Card**

**Fingerprint**

The platform provides three ways to collect fingerprints: via a USB fingerprint recorder, via an enrollment station, or via a fingerprint and card reader.

Click **Configure** to set the collection mode as follows.

**USB Fingerprint Recorder**

Collect fingerprints via a USB fingerprint recorder connected to the computer running the Web Client, which is plug-and-play and does not require any settings. This mode is suitable for face-to-face scenarios where the person and the system administrator are in the same location.

After connecting the fingerprint recorder to your computer, click + , place and lift your finger on the recorder following the prompts, and it will collect your fingerprint automatically.

**Fingerprint and Card Reader**

Collect fingerprints via the fingerprint scanner of an access control device or a video intercom device which is managed in the system. This mode is suitable for non-face-to-face scenarios where the person and the system administrator are in different locations.

Select an access control device or a video intercom device from the managed device list.

Click + , place and lift your finger on the selected fingerprint and card reader following the prompts, and it will collect your fingerprint automatically.

**Enrollment Station**

You need to specify the device IP address, port number, user name, and password to access the enrollment station. Then click + , place and lift your finger on the device, and it will enroll your fingerprint automatically.

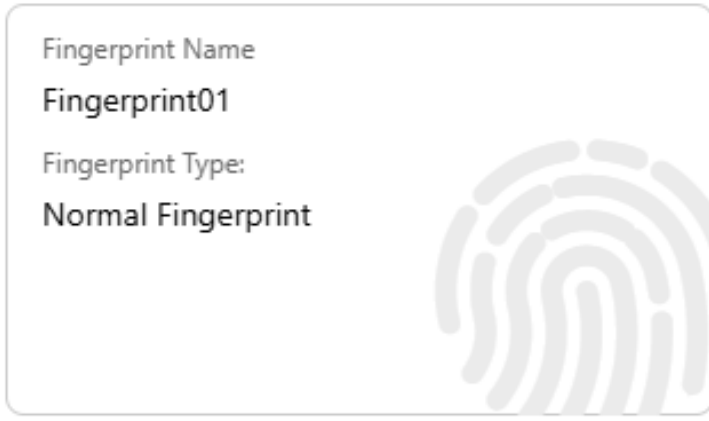



**Figure 26-14 Fingerprint Recorded**

**Note**

- No more than one fingerprint can be collected for 1 visitor.
- You can configure either cards or fingerprints.

**Iris**

The platform supports collect iris via iris collection devices.

Click **Configure** to set the collection device.

Click + to start collecting the visitor's iris.

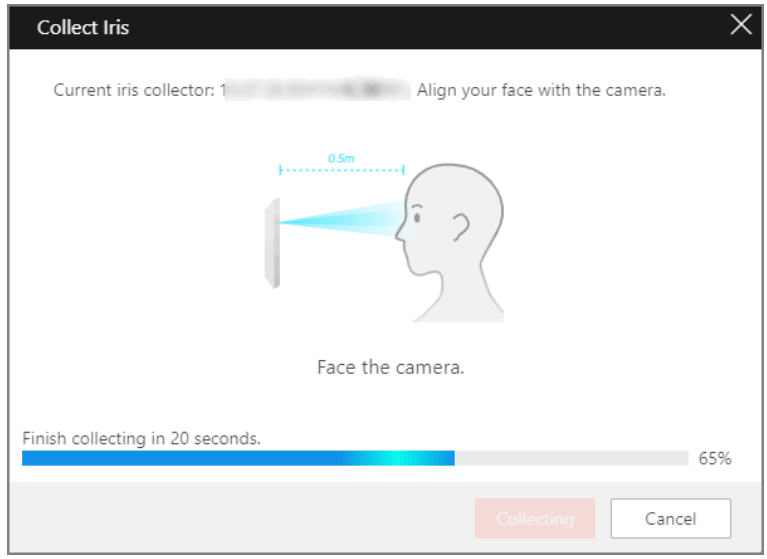



**Figure 26-15 Iris Collection**

6. Set the visiting information (visit purpose, host, end visit time, access level, valid times for visit, extended access, etc.).

**Visit Purpose**

Business, training, etc.

**Host**

You can click **Select** next to **host** to select an existing person as the host.

**End Visit Time**

When to check out.

**Access Level**

Click **Configure** to assign access levels to the visitor so that the visitor can access the access points within the access schedule of the access levels.

**Note**

To add a new access level for the visitor, see the instructions in ***Add Access Level and Parking Lot Permission for Visitors*** .

**PIN**

If **Unlocking Door by PIN** is enabled in **Basic Parameters**, this field will be displayed. You can set the PIN manually or click **Auto Generate** to generate one.

**Valid Times for Visit**

The maximum times a visitor can access certain doors or floors by QR code authentication. For example, if you set it to 4, the visitor can access the authorized doors and floors up to 4 times by QR code authentication.

**Extended Access**

If you check **Extended Access**, the access points that are configured with extended open duration will stay unlocked or open longer for the visitor.

7. Edit the ID information, including the ID type, ID No., and ID picture.
8. Take a phone of the visitor's belongings.

**Note**

Make sure you have enabled this function. See ***Set Basic Parameters*** for details.

9. Set other information, such as the skin-surface temperature, organization, and country/region.
10. Click **Configure** to set the parking lot permission.
11. Click **Check In** or **Check In and Continue**.

**Note**

If the operation succeeds and you have enabled **Print Visitor Pass Once Checked In** when you set basic parameters, the Preview window will pop up showing the preview of the visitor pass for the visitor. You can click **Print** on the window to print the visitor pass.

12. Go back to the Visitor Check-In page to check whether the visitor information fails to be applied to the visitor terminal(s). If it fails, check the failure details, troubleshoot, and apply again.

**Note**

If there is visitor information which fails to be applied to visitor terminal(s), a notification will show above the visitor list on the Visitor Check-In page. In this case, you can click **View** to view the failure details and troubleshoot according to the reasons shown on the window, and then click **Apply Now** or **Apply Again** to apply the visitor information to the visitor terminal(s) again.

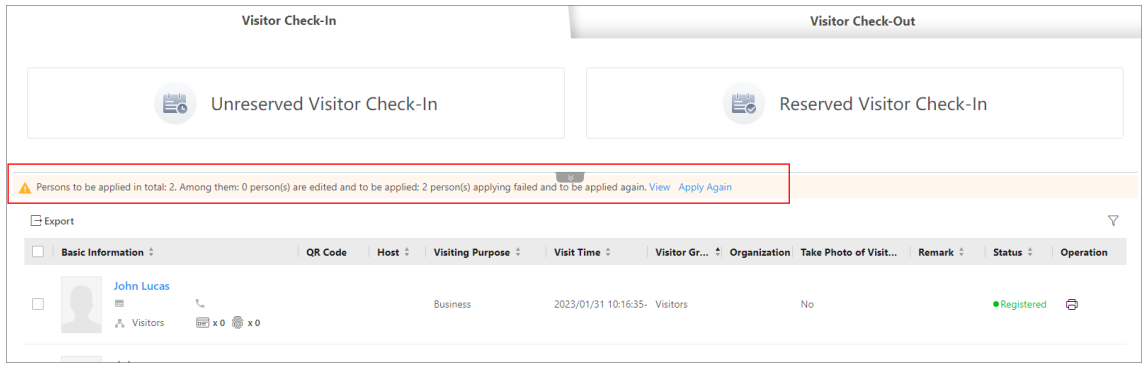



**Figure 26-16 Notification of Applying Failures**

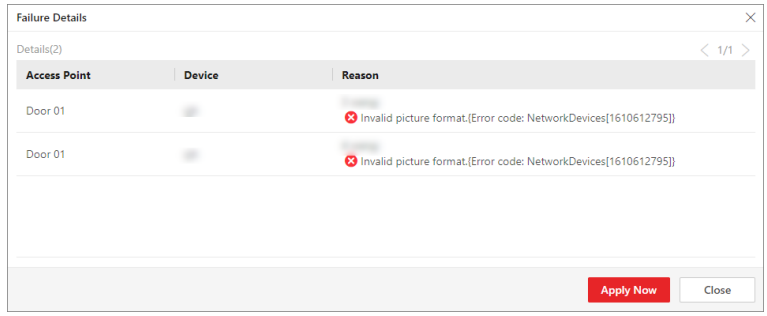



**Figure 26-17 Failure Details**

13. Perform these operations on the Visitor Check-In page if needed.

| Operation | Description |
|---|---|
| Export Visitors | Select visitors and click **Export** to export checked-in visitors to the local PC as a file. |
| Edit Visitor Information | Click on a visitor (checked in but not checked out yet) to edit the information. |
| Download a Visitor QR Code | Click in the **QR Code** column to download the QR code for the visitor. You can print it or send it to the visitor for identity authentication at access points. |
| Print a Visitor Pass | Click to print the visitor pass for the visitor. |

## 26.5 Visitor Check-Out

You should check out a visitor or let the visitor check out at a self-service check-out point before the visitor leaves. This is to ensure that the access level assigned to the visitor expires after they leaves.

On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Check-In/Out → Visitor Check-Out** to enter the Visitor Check-Out page.

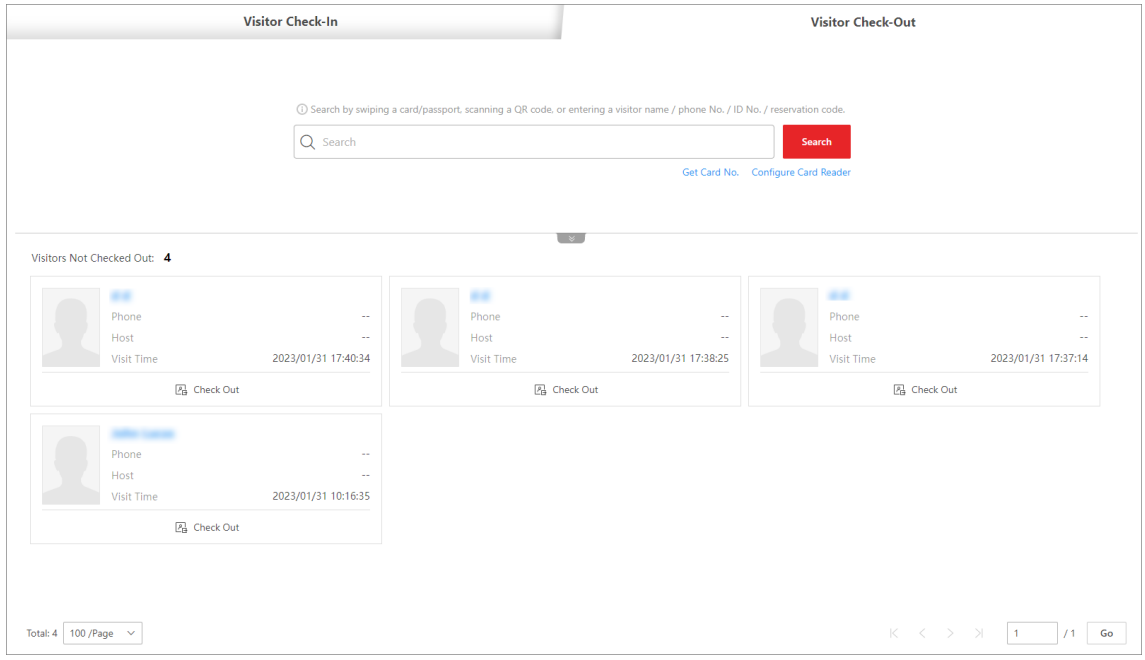



**Figure 26-18 Visitor Check-Out Page**

A visitor can be checked out in the following ways:

## Check Out at Self-Service Check-Out Point

If you have set a self-service check-out point, the visitor can check out by authenticating at the self-service check-out points without the help of the receptionist. If you have issued a card to a visitor when checking in, after checking out, the visitor should put the card in the place for card collection. The access level of their cards, fingerprints, face pictures, and QR codes will expire automatically.

**Note**

See ***Set Self-Service Check-Out Point*** for details about how to set a self-service check-out point.

## Check Out by Swiping Card

If you want to allow visitors to check out by swiping their cards, you need to click **Configure Card Reader** in the upper-right corner of the Visitor Check-Out page to configure the card reader first.

**Note**

Before configuring the card reader, make sure that you have added the corresponding device (enrollment station or card enrollment station) to the platform, otherwise ⓘ will appear next to **Configure Card Reader**, indicating that the platform fails to detect the device.

By default, **Card Enrollment Station** is selected as the card reader. If you select **Enrollment Station** and complete related settings, you need to click **Get Card No.** on the Visitor Check-Out page to activate the settings.

### Search for and Check out a Visitor

You can swipe a card/passport, scan a QR code, or enter a visitor name / phone No. / ID No. / reservation code, and click **Search** to search for the visitor, and then click **Check Out** on the search result page to check out them.

**Note**

- Only if a bar code reader is plugged into the PC where the platform runs, can you use the bar code reader to scan the QR code on the visitor pass of a visitor to search for the visitor to check them out.
- Only if a KR420 passport reader / United Arab Emirates ID card reader / Thai ID card reader is plugged into the PC where the platform runs, can you use the KR420 passport reader / United Arab Emirates ID card reader / Thai ID card reader to swipe the passport / ID card to search for the visitor to check them out.

### Check Out Visitors in the Visitors Not Checked Out Section

Visitors not checked out will be displayed on the Visitor Check-Out page, you can click **Check Out** on the visitor card to check them out, or you can click the name of a visitor to go to the details page and click **Check Out**.

### Automatic Check-Out

If you do not manually check out a visitor, the visitor will be checked out by the platform automatically when the configured visiting duration ends.

**Note**

Automatic check-out is available only when **Check Out Automatically** is selected for visitors not checked out after the exit time on the Basic Parameters page. For details, see ***Set Basic Parameters*** .

## 26.6 How to Set Up and Implement Self-Service Visit

### Applicable Scenario

Enable self-service visitor access to a facility using QR code-based reservations. Visitors can book their entry, receive approval, and gain access without manual intervention, reducing administrative workload.

**Table 26-3 Roles**

| Role | Description |
|---|---|
| Visitor | Scans a QR code to submit a reservation request, receives approval, and uses the generated QR code to enter the facility. |
| Park Administrator | Reviews and approves visitor requests, configures permissions, and manages access control settings. |

### 26.6.1 Step 1: Set Up Self-Service Reservations and Approval Workflow

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Review and Self-Service Reservation** .
2. Enable **Auto Approve Reservation**.

   **Note**

   If you enable this, visitor reservations will be approved automatically. If you disable this, visitor reservations need to be approved according to the configured approval flow. The configuration is only valid to the current users.
3. Enable **Self-Service Reservation**. The platform will generate a QR code. After downloading the QR code, you can print it or send it to the hosts or visitors who are going to reserve. The host can scan the QR code to reserve for the visitor, while the visitor can also scan the QR code to reserve if the visitor knows the visitor's person ID.

   **Note**

   QR codes generated by different users are different, and a user can only review the visitors reserved via the QR code the user generated, which allows different users to manage their own visitors independently.
4. Configure the following parameters.

   **Face Quality Verification**

   After the visitor uploads a profile picture by a cellphone, the selected device will automatically start checking the profile picture's quality. If the profile picture is not qualified, the visitor will be notified. Only when the uploaded profile picture is qualified can the visitor reserve successfully. Otherwise, the visitor information cannot be uploaded to the platform.

   **Note**

   To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

   **Visitor Group**

Select a visitor group. After reserving successfully, the visitors will be added to the group. If you do not select, the visitor will be added to the default visitor group.

5. Click **Save**.

**Note**

If the auto approval of visitor reservation has been disabled, you will be prompted to configure the approval flow. Click **Yes** to enter the Approval Flow page to configure a visitor approval flow.

### 26.6.2 Step 2: Configure Default Visitor Access Levels

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Access Level** .
2. Click **Add**.
3. Select existing access levels.
4. Click **Add**.
5. Select an added access level and switch on the button in the **Default Access Level** column.

### 26.6.3 Step 3: Configure Auto Check-Out Points

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Self-Service Check-Out Point** .
2. Click **Add** to show the resource list.
3. Select one or more doors / card readers and click **Add**. After setting self-service check-out points, the visitors can check out at the points according to the assigned access levels by swiping cards or fingerprint/face authentication.




**Figure 26-19 Set Self-Service Check-Out Point Page**

### 26.6.4 Step 4: Visitor QR Code Reservation

1. Visitors scan the QR code (generated by the park administration in Step 1, displayed at facility entrances or shared online).
2. They complete the reservation form, including the name, contact info, purpose of visit, date and time of entry request, etc.
3. The platform submits the request for administrator approval.

### 26.6.5 Step 5: Administrator Review & Approval

1. The park administrator reviews incoming visitor requests on the platform.
2. If the request is valid, the administrator approves it.
3. Upon approval, the platform auto assigns the access level to the visitor.

### 26.6.6 Step 6: Visitor Receives QR Code for Entry

1. Approved visitors receive an entry confirmation email containing their unique QR code.
2. Upon arrival, the visitor scans the QR code at the designated access point to enter the facility.

### 26.6.7 Step 7: Visitor Auto Check-Out Upon Exit

1. When leaving, visitors scan out at an anto check-out point.
2. The system revokes their access levels to prevent unauthorized re-entry.

## 26.7 How to Use Watch List to Monitor Special Visitors

You can use the watch list to monitor special visitors for security or other purposes.

### What is the Watch List

The watch list contains entities (individual visitors, companies, or countries/regions) that need to be monitored in the visitor reservation or check-in process.
Different from the visitor blocklist, which only contains visitors whose visits are denied in any case, the watch list can contain both the unwanted entities and ones that deserve preferential treatment.

### How the Watch List Works

The platform can detect whether a visitor registered in the reservation or check-in process has attributes (e.g., name, ID, company, and country/region) that match entities in the watch list.
When entities are matched, the Entities in Watch List Matched window will pop up.
In this case, if the visitor is unwanted, you can reject the reservation or check-in directly on the pop-up window; if the visitor deserves preferential treatment, you can approve the reservation

and notify related personnel, so that they can prepare corresponding work beforehand for the visitor.

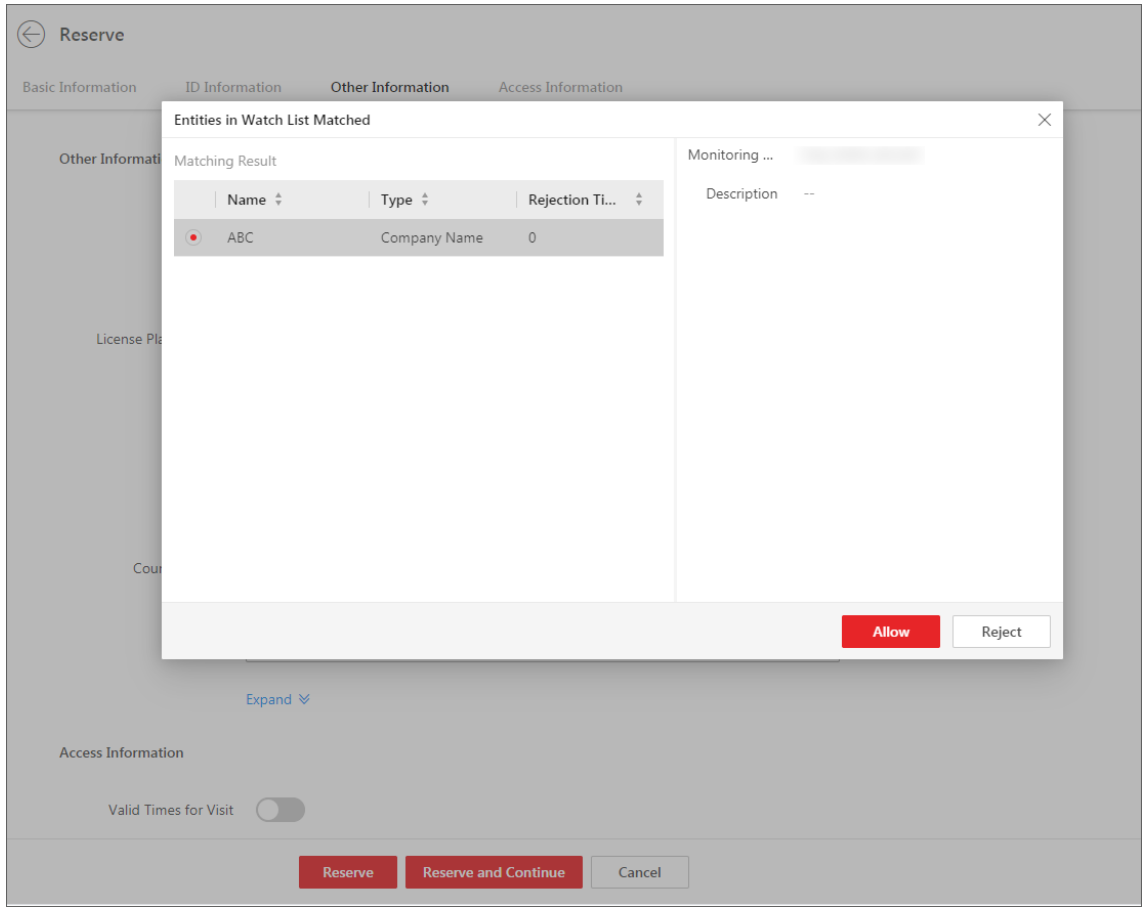



**Figure 26-20 The Entities in Watch List Window**

## 26.7.1 Step 1: Add Entity Type

You can add and define the types of entities to be monitored.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Category on Watch List** to open the Category on Watch List pane.
3. Click **Add** on the top left of the pane.
4. Create a type name.
5. Enter a remark for the type.
6. Click **Add** to finish adding the type.
7. Perform one or more of the following operations.

| | |
|---|---|
| Edit Type | Click a type name to edit it. |
| Delete Type(s) | Select type(s) and then click **Delete** to delete the selected one(s). Or move the cursor to and then click **Delete All** to delete all types. |

## 26.7.2 Step 2: Set Match Method

You can set the match methods to determine the match items (e.g., the name and ID) to match the visitors and the entities to be monitored when checking in and reserving for visitors.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Match Method** to open the Match Method pane.
3. Set the match items for matching the visitors and the entities during reservations or checked-in.

   **Match via Name**

   If the name of a visitor matches that of an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   **Match via ID**

   If the ID number of a visitor matches that of an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   **Match via Company**

   If a visitor's company matches an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   **Match via Country/Region**

   If a visitor's country/region matches an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.
4. Configure name match settings.

   **Note**

   To make the name match settings take effect, you need to check **Match via Name** first.

   **Match First Name Only**

   If the first name of a visitor matches that of an entity in the watch list, the platform will determine that the visitor name matches the entity. For example, assume that the name of a visitor is Andrew Lee and an entity in the watch list is Andrew Peterson, the platform will determine that the former matches the latter.

   **Match Full Name**

   Only when the full name of a visitor matches that of an entity in the watch list will the platform determine that the visitor name matches the entity.
5. Click **OK**.

### 26.7.3 Step 3: Add an Entity to the Watch List

You can add a to-be-monitored entity to the watch list and determine how long the entity will be monitored.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Add** to open the Add Entity page.
3. Set the entity type (**Person**, **Company**, or **Country/Region**).
4. Set other information for the entity.

   **Category**

   Select a category to which the entity belongs. Or click **Create New Category** to create a new one.

   You can manage categories in **Category and Match Method**.

   **Effective Period**

   If enabled, you can determine the time period when the platform monitors the entity. If disabled, the platform monitors the entity indefinitely.
5. Click **Add** or **Add and Continue**.
6. Perform the following operations if needed.

| | |
|---|---|
| Disable Entities | Select entities and then click **Disable** to disable them. Once disabled, they will not be monitored. |
| Enable Entities | Select disabled entities and then click **Enable** to enable them. Once enabled, they become monitored. |
| Edit an Entity | Click the name of an entity to edit it. |

### 26.7.4 Step 4: Import Existing Visitors to the Watch List

You can import specific existing visitors to the watch list. Existing visitors refer to the visitors once reserved or checked in.

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Import Existing Visitor** to show the Import Existing Visitor pane.
3. Click to select the existing visitors from a specific visitor group and then click **Add**.

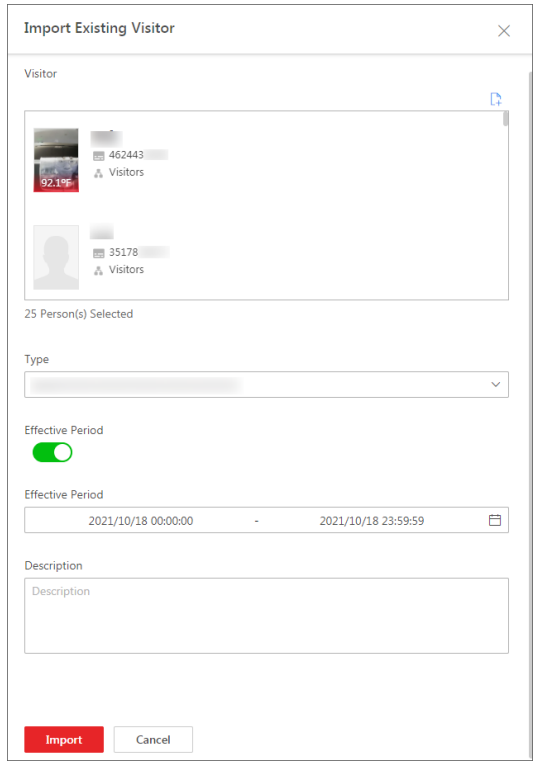



**Figure 26-21 Import Existing Visitor**

4. Set other information, including the type, effective period, and description.

   **Type**

   Select a type to which the entity belongs.

   Make sure you have added types in **Category on Watch List**.

   **Effective Period**

   Determine the time period when the selected visitors will be monitored if their reservations are made or they check in again.
5. Click **Import**.
6. Perform the following operations if needed.

| | |
|---|---|
| Disable Monitoring of Existing Visitors | Select visitors and then click **Disable** to disable them. Once disabled, they will not be monitored. |
| Enable Monitoring of Existing Visitors | Select disabled visitors and then click **Enable** to enable them. Once enabled, they become monitored. |
| Edit an Existing Visitors in the Watch List | Click the name of an entity to edit it. |

# 26.8 How to Manage Visitor Information and Access Records

## 26.8.1 View Visitor Information

You can view all checked-in visitors (including those who have checked out) in the visitor list and perform related operations such as adding visitors to the blocklist.

On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Visitor Information** to view the list of all visitors.

You can perform the following operations on the Visitor Information page.

- **Delete Visitor**: Check one or more visitors and click **Delete** to delete the selected visitor(s). Or click → **Delete All** to delete all visitors.

  **Note**

  After deleting the visitor's personal information, you can still search the visitor's visiting records in the Visitor List.

- **Move Visitors to Blocklist**: Select the visitors and click **Move to Blocklist** to move the selected visitors to the blocklist.
- **Remove Visitors from Blocklist**: Select the visitors and click **Remove from Blocklist** to remove the selected visitors from the blocklist.
- **Move Visitor to Another Group**: Check one or more visitors and click **Move** to move the selected visitor(s) into a different visitor group.
- **Clear Visitor Information**: When enabled, the platform will clear all visitors who did not check in during the time period which you specify by setting **Not Checked In For**.
- **Reserve Again**: For normal visitors who have checked out, you can click to make reservation for them again quickly without the need to set the visitors' existing basic information (e.g. visitor name, ID, fingerprint) again.
- **Check In Again**: For normal visitors who have checked out, you can click to check in them again quickly without the need to set the visitors' existing basic information (e.g., profile picture and fingerprint).

  **Valid Times for Visit**

  The times a visitor can enter/exit the area managed by the related access group after authentication. For example, if you enter 5 as the valid times and relate an access group for a door to the visitor, the visitor can enter/exit the door for 5 times. After 5 times of authentication, the visitor cannot enter/exit the door.

## 26.8.2 Check Visitor Access Records

When a visitor accesses an access point by credentials, a visitor access record is stored on the platform. After searching for a visitor, you can view all access records of the visitor, no matter the

visitor has checked out or not. This allows you to track all the access points where the visitor has visited and view the corresponding visit times.

On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Visitor Access Record** to display the visitor access records. By default, only the current-day records will be displayed. If you need to view other time's records, manually filter the records.

You can perform the following operations.

## Filter Visitors

Click on the top right to filter visitors by ID No., name, phone, company, host, visit purpose, visit time, status, and skin-surface temperature status. You can also click **Select Additional Information** to select additional information to filter.

For the **Status** condition, you can click to select one or more reservation status (checked-in, checked-out, checked-out (auto), self checked-out, and not check out in effective period) to filter visitors.

After filtering, you can click the visitor name to view the information of the visitor.

## View Information on First & Last Authentication

By default, only the first and last access authentication records are displayed. To view more information, click to open the Visitor Access Authentication Records window to view all access authentication records of the visitor.

# Chapter 27 Emergency Mustering

The emergency mustering module facilitates the safe evacuation of people during a crisis or emergency situation. You can customize emergency solutions for various areas and then start a roll call to verify who is safely accounted for at evacuation sites and mustering points.

Take the following steps to configure the emergency mustering system.

1. Go to → **Integrated Service → Emergency Mustering** .
2. Customize your emergency solution by area. For details, see ***Add Emergency Solution*** .
3. Select area(s) to trigger an emergency and start a roll call. For details, see ***Start a Roll Call*** .

## 27.1 Add Emergency Solution

Take the following steps to add an emergency solution:

1. ***Select Areas***
2. ***Add Card Readers***
3. ***Add Doors Remaining Unlocked in Emergency***
4. ***Add Emergency Counting Groups***
5. ***Release Emergency Mustering Notifications***
   - ***Add Emergency Mustering Programs***
   - ***Add Text Notifications***
   - ***Set Broadcast Linkage***
6. ***Trigger Emergency Automatically***

### 27.1.1 Select Areas

- If you are configuring the emergency solution for the first time, select **Configure**, and then select area(s) for emergency mustering.
- If you have configured the emergency solution, select **Emergency Solution Settings → Add Solution for Emergency Evacuation** , and then select area(s) for emergency mustering.

### 27.1.2 Add Card Readers

To add an entrance & exit point and a mustering point, you should select card readers for authentication, headcounts or other measures. Authenticated individuals are marked as "In" at an entrance and "Out & Not Check in" at an exit. A mustering point is the designated location to assemble after an emergency evacuation. Those who have checked in at the mustering point are marked as "Checked In At Mustering Point". This part will guide you through adding mustering points.

Select **Mustering Point → Add → Card Reader → OK** .

**Note**

Ensure that you have added card reader(s) to the platform before setting the entrance point, exit point, and mustering point.

### 27.1.3 Add Doors Remaining Unlocked in Emergency

In an emergency, unlocked doors ensure that occupants can exit their work site quickly and efficiently and help emergency responders access the building rapidly to conduct rescue operations without authentication at the card reader.

To add doors remaining unlocked in emergency, select **Doors Remain Unlocked in Emergency → Add → Door → OK** .

### 27.1.4 Add Emergency Counting Groups

After setting the resource access permission and adding persons, you can add emergency counting groups for headcounts based on the authentication status.

#### Set Permissions

To access and manage emergency counting groups, set the resource access permission.

1. Go to → **Account and Security → Roles → Add** , and set the basic information.
2. Select **Resource Access**, set the resource type to Emergency Counting Group, and select a group in an area as needed.

#### Add Emergency Counting Groups

To add an emergency counting group on the Emergency Solution Settings page, access is available via two options:

- Go to → **Emergency Mustering → Emergency Counting Group →** + .
- Go to → **Person → ID → Emergency Counting Group** . You can select an emergency counting group already added or click **Add Emergency Counting Group**. The emergency counting group added here will be synchronized to the Emergency Solution Settings page.

**Adding Mode**

- **By Person**: Person(s) selected will be added in the emergency counting group. On the Roll Call page, the group will be marked as **Person Group**.
- **By Department**: Department(s) will be linked, and all persons in the linked departments will be added to the emergency group. On the Roll Call page, the group will be marked as a **Department Group**. Subsequent new personnel in the linked departments will be automatically included. New personnel added during an emergency will be included in the next emergency.

**Count Data Days Before Emergency Triggering**

Supports selecting the number of days before the emergency is triggered to start data collection. If you choose **From Emergency Triggering**, it means the data will be counted from the moment of emergency triggering and the check-in status of all personnel prior to the emergency triggering will be cleared.

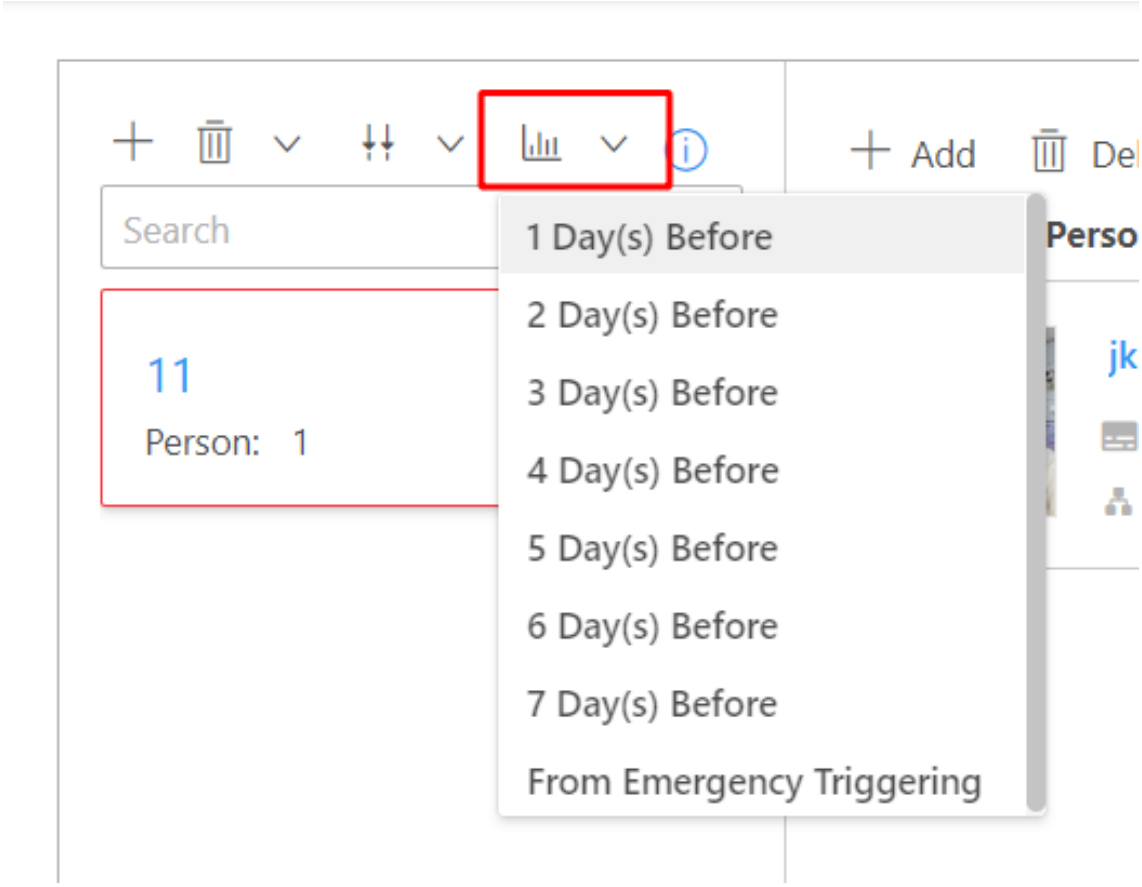



**Figure 27-1 Days Before Emergency Triggering**

## 27.1.5 Release Emergency Mustering Notifications

To ensure safety, coordination, and effective communication during critical situations, you can configure emergency mustering programs and text notifications. These notifications will be displayed on digital signal terminals or disseminated by broadcasts when an emergency is triggered.

### Add Emergency Mustering Programs

To add an emergency mustering program, take the following steps:

1. Select **Prompt by Digital Signage Terminal → Configure** .
2. Select a template, and click **Create**.
3. Set the page and background music, and select **Release → Select Device → OK** .

### Add Text Notifications

To add a text notification, take the following steps:

1. Select **Prompt by Digital Signage Terminal → Configure** .
2. Select **Text Notification Emergency** and click **Create**.
3. Set the notification name and content.
4. Select the device.
5. Select **Release**.

### Set Broadcast Linkage

To set the broadcast linkage, take the following steps:

1. Select **Prompt by Broadcast → Configure** .
2. Configure the following parameters: the broadcast name, area, speaker unit, broadcast content, audio file, and play mode.
3. Select **Save and Apply**.

## 27.1.6 Trigger Emergency Automatically

You can add events and alarms to allow the platform to automatically trigger an emergency by area when the event or alarm is triggered.

1. In the top left corner of Home page, select → **Security Monitoring → Event and Alarm → Event and Alarm Configuration → Normal Event and Alarm → Add** .
2. Set the triggering condition.
3. Set the linkage action to **Send Email**, select a template, and then select emergency counting groups by area.
4. Enable **Trigger Alarm** to set the alarm priority and recipients.
5. Enable **Trigger Emergency** to set **Reaction of Platform** to **Trigger Emergency**, and to select an area.

# 27.2 Start a Roll Call

After configuring the emergency solutions, you can start a roll call to check that all personnel have safely evacuated from a hazardous area or are present in designated mustering point. During emergencies, it is essential to manage information effectively. Roll call provides a systematic way to gather and relay information about individuals' whereabouts.

Take the following steps to start a roll call.

1. Select **Roll Call → Select Area for Triggering Emergency** .
2. View the detailed personnel information of all selected areas to ensure the safety and accountability of all individuals.
3. (Optional) Click a card to view the detailed personnel information of a single area, including the overall information, profile picture, name, phone number, and status.

**Note**

Click to check in a person who shows at the mustering point but the person status is not Checked In At Mustering Point.

4. (Optional) You can perform the following operations as needed.

| Operation | Description |
|---|---|
| End the emergency status. | - Select **Turn off Emergency of All Areas** to end the emergency status of all areas.<br>- Select **Turn Off Emergency** to end the emergency status of the selected area. Before you edit the emergency solution, end the emergency status. |
| Select person statuses. | Click **Set Statistics Type** on the upper-right corner. |
| Export emergency mustering report. | Click **Export Report** to select areas/groups, set sorting rules, select the report export mode, and confirm your password. If you set the report export mode to **Send Email**, you can select **New Email Template** to quickly configure a new email template. |
| Search by group name. | Enter the group name (fuzzy search supported), and press Enter or click to get results. Clicking on the group will display the personnel information for that group. |
| Automatically print the emergency mustering report when you end the emergency status of a selected area. | Select → **Security Monitoring → Event and Alarm → Event and Alarm Configuration → Normal Event and Alarm → Add** , enable **Trigger Alarm → Trigger Emergency** , set the reaction of platform to **Turn off Emergency**, enable **Print Report**, and select an emergency counting group for report printing. |

# Chapter 28 Map Management

Two types of map are available: GIS map and E-map. On the GIS map, you can set and view the current site, Remote Site, and element's geographic location. On the e-map, which is a static map, you can set and view the geographic locations of the installed cameras, alarm inputs, and alarm outputs, etc.

With the GIS map, you can see the geographic locations of your security system. This type of map uses a geographic information system to accurately show all the hot spots' (resources placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access devices at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video from the cameras. With the hot region, you can link to the e-map to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

E-map is a static image (it does 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 placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., 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.

After configuring the e-map via Web Client, you can view the live video and playback of the elements via both Web Client and Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

On the top navigation bar, select → **Security Monitoring → Visual Map → Map** .

## 28.1 Configure Map

You need to configure GIS maps and e-maps before using them. You can add hot spots, hot regions, labels, resource groups, etc. to the maps.

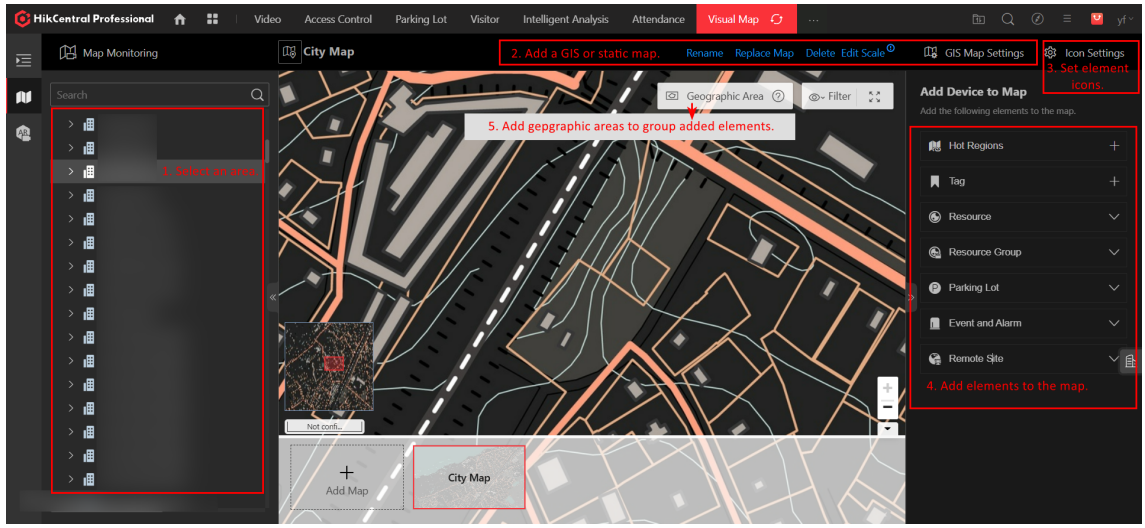



**Figure 28-1 Main Interface of Configuring Map**

## 28.1.1 Select and Set GIS or E-map for an Area

You can either set a GIS map for an area or upload an E-map for an area. Click **Map Settings** in the top right corner of the map module to enter the map settings page.

## Add E-Map for Area

You can add and link e-maps to the area so that the elements assigned to the area can be added to e-map.

**Steps**

1. Select an area on the left.
2. Open the Add Map pane.
   - If you have configured GIS map, click **+** on the lower right of the map.
   - If you did not configure GIS map, click **Add Map** at the center of the page.
3. Select an adding mode.
4. Select a map.
   - If you select **Add E-Map** as the adding mode, select a map picture saved on the PC.
   - If you select **Link to Other Map**, select an area from the following list.
5. Click **Add**.
6. **Optional:** Set a map scale.

**Note**

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 a radar's detection area. Perform this step if you plan to add a radar to the map.

1) Click **Edit Scale** on the top right of the map.
2) Click two locations on the map to form a line.
3) Enter the real distance between the two points in the Actual Length field.
4) Click **OK** to finish setting the map scale.

7. **Optional:** Hover the mouse over the added e-map area to perform the following operations.

| | |
|---|---|
| **Edit Picture** | Click and change a picture. |
| **Edit Map Name** | Click and set a custom name for the map. |
| **Unlink Map** | Click to remove the map or cancel the linkage between the map and area. |

## Set GIS Map and Icons

This page allows you to enable GIS (Geographic Information System ) map function to display the online or/and offline GIS map on the Web Client and Control Client, so that the geographic location of the resources (such as current site, Remote Sites, cameras) can be shown on the map.

**Steps**

1. On the top right, click **GIS Map Settings** and set the GIS Map.
   1) Switch the **GIS Map** on to enable the GIS map function.
   2) According to the actual requirements, select **Online** or **Offline** to set the online GIS map or offline GIS map.
      - For online GIS map, enter the GIS map API URL.

        **Note**

        - The Google map API is supported currently.
        - Google Maps are provided by Google Inc. (Hereinafter referred to as "Google"). We only provide you the URLs to use Google Maps. You shall apply by yourself for the use of Google Maps from Google. You shall comply with Google terms and provide certain information to Google if required.
        - You shall set the correct GIS map API URL, otherwise the configuration can not be saved.

      - For offline GIS map, you can upload map files in tar.gz or tar format, of which the size is no larger than 1 GB.

        **Note**

        Click **Download Offline Map Configuration Guide** to refer to the guide and the interface instruction to add and configure the offline map.

3) Click **Save**.

2. Click **Icon Settings** to set the customized icons.
   1) Select a device type to enter the icon settings page.
   2) Set the icon size, including width (px) and height (px).
   3) Click **Add** to select a picture file from the local PC.

   **Note**

   The icon picture format can only be PNG, JPG, or JPEG.

   4) **Optional:** Click to constrain the aspect ratio.
   5) Click **Save**.

**Note**

You can customize door icons for the five status, namely general, door open, door closed, remain open, remain closed, and unknown.

**Result**

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

## Operations After Adding Maps

**Result**

| | |
|---|---|
| Filter | Click and select the object type you want to show on the map. |
| Full Screen | Click to show the map in full-screen mode. |
| Zoom In/Out | Scroll the mouse wheel or click + / − to zoom in or zoom out the map. |
| Adjust Map Area | Click-and-drag the map to adjust the map area for view. |
| View Resource Latitude and Longitude (For GIS Map) | Hover over a resource, and you can view its latitude and longitude on the GIS map. |

## 28.1.2 Add Hot Spot to Map

You can add elements (e.g., doors, alarm inputs, etc. ) as the hot spot and place the hot spot on the e-map. Then you can view the elements on the map and perform further operations via Mobile Client.

**Before You Start**

A map should ***have been added*** .

**Steps**

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Resource Group** on the right.
5. Select a device type and an area from the drop-down lists.
6. Select a device and drag it to the map.

   The hot spot is displayed on the map.
7. **Optional:** Perform the following operations after adding the hot spot.

| | |
|---|---|
| **Adjust Hot Spot Location** | Drag the added hot spot on the map to the desired locations. |
| **Edit Hot Spot** | Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as selecting icon style). |
| **Delete Hot Spot** | Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map. |

## Draw Zone or Trigger Line for Radar

You can draw zones or trigger lines for radar, so if an object is detected to have crossed the trigger line or entered the area shaped by the dual-trigger line or zone, the event and alarm will be triggered.

**Before You Start**

A radar has been added to the area and map.

**Steps**

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Click the radar's icon on the map and then select **Draw Zone/Trigger Line** from the drop-down list to start drawing zone or trigger line for radar.
3. Select a zone drawing method in the tool bar in the upper-left corner of the map.



**Draw Trigger Line**

A trigger line is a virtual line drawn in the radar's detection area. An event or alarm will be triggered if an object is detected to have crossed the line. Click to draw a trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the trigger line, or drag the trigger line to move it to another place.

**Note**

No more than 4 trigger lines can be drawn.

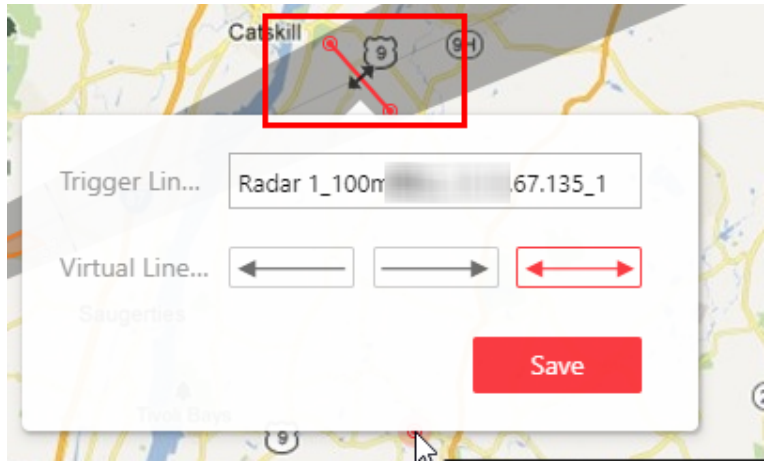



**Figure 28-3 Trigger Line in the Detection Area**

**Draw Dual-Trigger Line**

A dual-trigger line consists of 2 virtual lines drawn in the radar's detection area. Generally, it is used to mark an area in the radar's detection area. An event or alarm will be triggered if an object is detected to have entered the area shaped by the dual-trigger line. Click to draw a dual-trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the dual-trigger line, or drag the dual-trigger line to move it to another place.

**Note**

Only 1 dual-trigger line can be drawn in the radar's detection area.

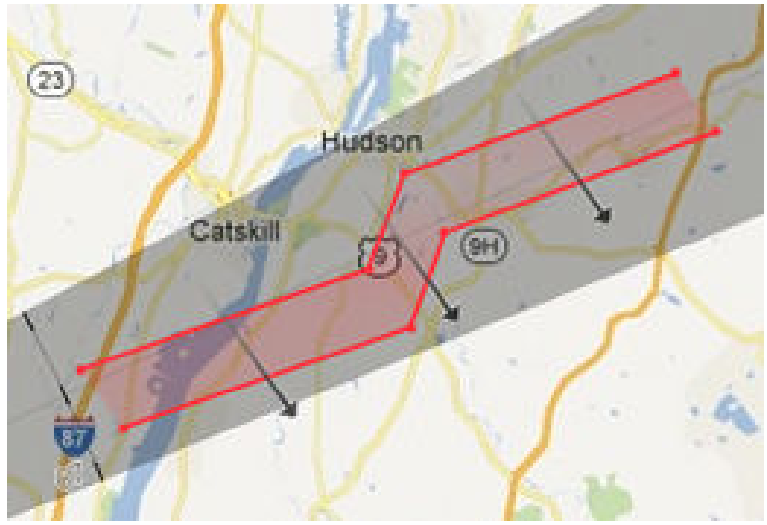



**Figure 28-4 Dual-Trigger Line in the Detection Area**

**Manually Draw**

You can draw any shape for the zone using this method.

**Zone Segmentation**

Split a zone into two smaller zones by a line.




**Figure 28-5 Zone Segmentation**

**Distance Segmentation**

Split a zone into two smaller zone by an arc.

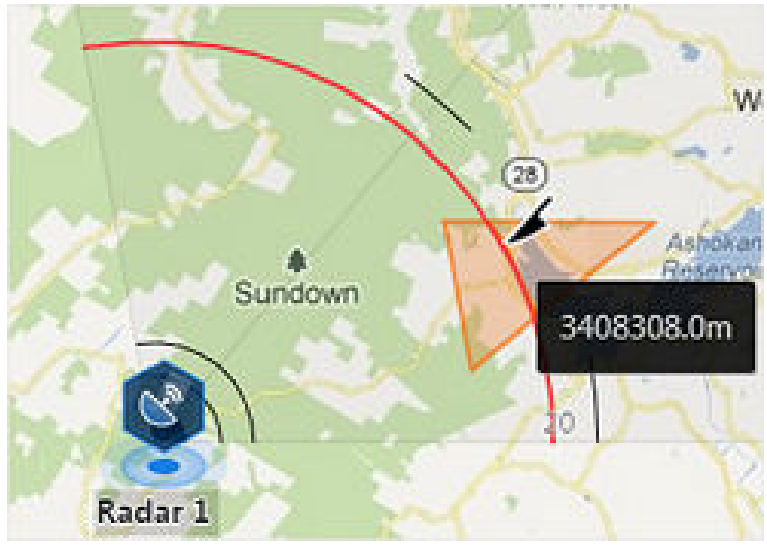



**Figure 28-6 Distance Segmentation**

4. Right click to finish drawing and open a configuration window.
5. Set parameters for the drawn trigger line or zone.
6. Click **Save**.
7. Right click to exit the zone or trigger line drawing mode.

## Relate Calibrated Camera to Radar

This operation requires two persons' teamwork: person A walks into the radar's detection area (the person's position will be displayed on the map as a red point), while person B who operates the computer running the Web Client adds calibration points by PTZ control of the camera(s) according to person A's position.

**Before You Start**

A radar has been added to the area and map.

**Steps**

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Click the radar's icon on the map and then select **Relate Calibrated Camera** from the drop-down list to relate cameras.
3. Click **Resource** on the Map Settings panel and drag camera(s) to the map.

**Note**

- This function needs to be supported by the device.
- Up to 4 calibrated cameras can be added.

4. Click the radar's icon first, and then click camera icon(s) to relate the camera(s) with the radar.

**Note**

You can right click to finish relating cameras or it will automatically finish when no camera can be related.

5. Click the radar's icon on the map and then select **Calibrate PTZ Camera** from the drop-down list to enter the camera calibration settings page.
6. Person A goes to the location which can be detected by one of the cameras.

   Person A's location will appear on the map as a red point .
7. Person B clicks on the map to open the adding calibration point window.

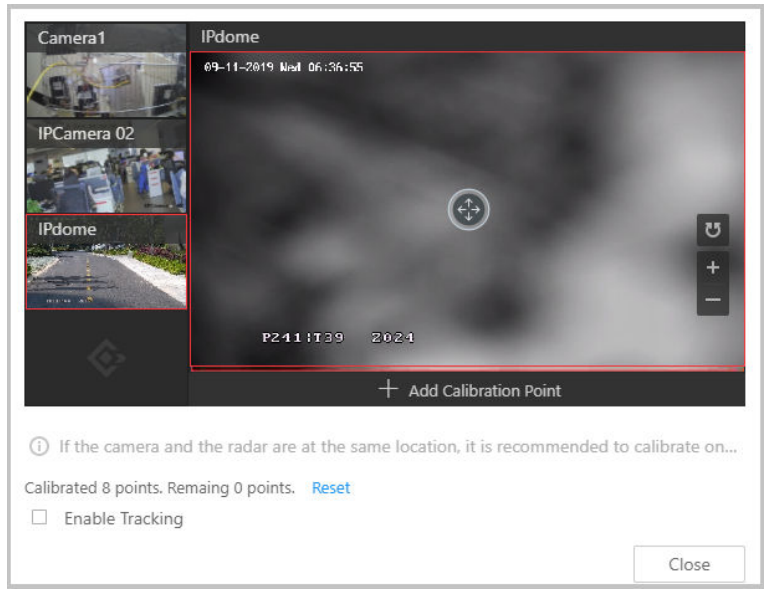



**Figure 28-7 Add Calibration Point**

The cameras' thumbnails will be displayed on the left of the window.

8. **Optional:** Undo-check the **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
9. Click a camera's thumbnail to display its image in the window on the right.
10. Click the image to turn the camera to the position of person A until person A appears in the image.
11. Click **Add Calibration Point** to add the current image as a calibration point.

**Note**

- If the camera locates above or under the radar vertically, only 1 calibration point is enough; if not, at least 4 calibration points are required.
- Up to 8 calibration points can be added for one cameras.

12. **Optional:** Check **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
13. Close the Add Calibration Point window and click to save the settings.

### 28.1.3 Add Hot Region to Map

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.

**Before You Start**
At least 2 maps should ***have been added*** .

**Steps**
1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Hot Region** icon on the right.
5. Click a position on the map to select it as the location of the hot region.
6. Select an area from the area list.
7. Click **Save** on dialog to add the hot region.

   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

| | |
|---|---|
| **Adjust Hot Region Location** | Drag the added hot region on the parent map to the desired locations. |
| **Edit Hot Region** | Click the added hot region icon on the map to view and edit the detailed information, including GPS location (only available when parent map is GIS map), hot region name, icon style, name color, and remarks on the appearing dialog. |
| **Edit Hot Region Area** | Drag the white point on the hot region's line to edit the hot region's size or shape as the following picture. |
| **Delete Hot Region** | Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region. |

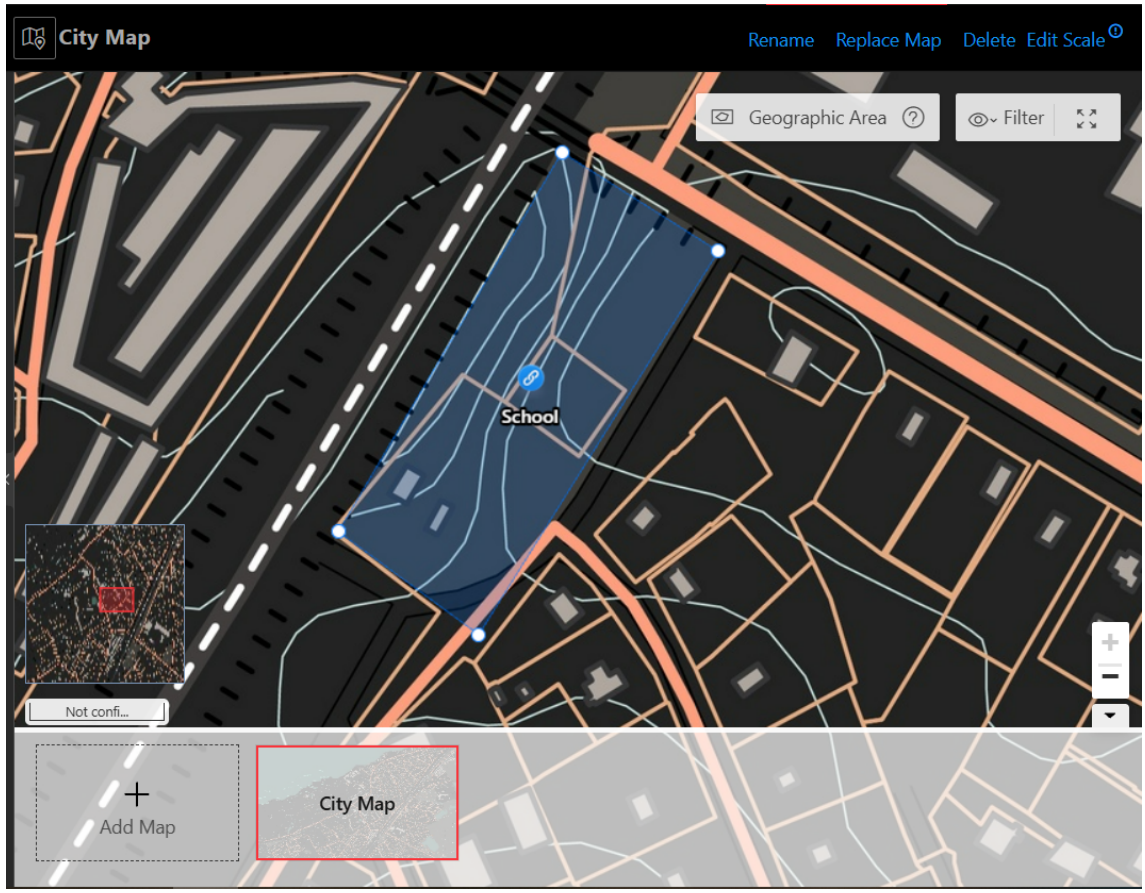



**Figure 28-8 Edit Hot Region Area**

## 28.1.4 Add Tag to Map

You can add tags with description on the map.

**Before You Start**

At least one map should ***have been added*** .

**Steps**

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Tag** icon on the right.
5. Click on the map where you want to place the tag.
6. Customize a name for the tag, and you can input content for the tag as desired.
7. Click **Save**.

   The added tag icon will be displayed on the map.
8. **Optional:** Perform the following operation(s) after adding the tag.

| | |
|---|---|
| **Adjust Tag Location** | Drag the added tag on the map to the desired locations. |
| **Edit Tag** | Click the added tag icon on the map to view and edit the detailed information, including name and content on the appearing dialog. |
| **Delete Tag** | Click the tag icon on the map and click **Delete** on the appearing dialog to delete the tag. |

### 28.1.5 Add Resource Group to Map

You can also add the resource groups on the map by locating the resources in the group on the map and setting the edge of the region for detection.

Click **Map Settings** in the top right corner of the map module to enter the map settings page.

**Note**

Before adding resource groups to a map, make sure that at least one map ***has been added*** .

Currently, the following resource groups can be added on the map for further operations:

**People Counting Group**

After adding the people counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

**Heat Analysis Group**

After adding the heat analysis group on the map, the resources (such as doors, fisheye cameras, people counting cameras) will be grouped in certain region and displayed on map, and you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people.

**Pathway Analysis Group**

After adding the pathway analysis group on the map, you can view the real-time number of people walking by in the Monitoring module on the Control Client.

**Person Feature Analysis Group**

After adding the person feature analysis group, the cameras which support facial recognition and feature analysis will be grouped in one region and displayed on the map. You can view the features of the persons appeared in this region, based on the data detected by the cameras in the group.

**Anti-Passback Group**

After adding the anti-passback group on the map, when an anti-passback alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and

you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile ClientControl Client.

For details about how to add an anti-passback group on the map, refer to ***Configure Anti-Passback*** .

**Multi-Door Interlocking Group**

After adding the multi-door interlocking group on the map, when multi-door interlocking alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile ClientControl Client.

For details about how to add a multi-door interlocking group on the map, refer to ***Configure Multi-Door Interlocking***

**Final Authentication Counting Group**

After adding the entry & exit counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Mobile ClientControl Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

For details about how to add an entry & exit counting group on the map, refer to ***Add a Final Authentication Counting Group*** .

**Batch Locking and Unlocking Group**

After adding the emergency operation group on the map, you can operate access points (remaining locked/unlocked) in the group in a batch.

This function is mainly applicable for emergent situation. For example, after grouping the doors of the school's main entrances and exits into one emergency operation group, the school's security personnel can lock down the doors in this group by quick operation on the Mobile ClientControl Client, so that the school closes and no one can get into the school except for maintenance and high level admins. This function would block out teachers, custodians, students, etc.

For details about adding an emergency operation group, refer to ***Add a Batch Locking and Unlocking Group*** .

**Partition Group**

After adding the security control partition (area) on the map, the security control device's alarm inputs will be grouped according to the zones on the device and displayed on map, and you can set an arming schedule to define when and how to arm the alarm inputs in a batch.

For details about adding a security control partition, refer to ***Add Security Control Partitions (Areas) from Device*** .

### 28.1.6 Add Parking Lot to Map

You can add parking lots and entrance and exits on the map to locate them for a visualized monitoring.

**Before You Start**
A map should ***have been added*** .

**Steps**
1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Parking Lot** on the right.
5. Drag a parking lot or an entrance and exit to the map.

   The parking lot, entrance or exit will be displayed on the map.
6. **Optional:** Perform the following operations after adding the entrance and exit.

| | |
|---|---|
| **Adjust Parking Lot/ Entrance and Exit Location** | Drag the added parking lot/entrance and exit on the map to the desired locations. |
| **Edit Parking Lot/ Entrance and Exit** | Click the added parking lot/entrance and exit icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map), and selecting icon style). |
| **Delete Parking Lot/ Entrance and Exit** | Click the parking lot/entrance and exit icon on the map and click **Delete** to remove the parking lot/entrance and exit from the map. |

### 28.1.7 Add Event and Alarm to Map

You can add the combined alarms and generic alarms on map to locate the alarm for a visualized monitoring.

**Before You Start**
Make sure you ***have added a map*** .

**Steps**
1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Event and Alarm** on the right.
5. Drag a combined alarm or generic event to the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

| | |
|---|---|
| **Adjust Event and Alarm Location** | Drag the added element on the map to the desired locations. |
| **Edit Event and Alarm** | Click the added element icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map), and selecting icon style). |
| **Delete Event and Alarm** | Click the element icon on the map and click **Delete** to remove the element from the map. |

## 28.1.8 Add Remote Site to GIS Map

After adding remote sites to GIS map, you can get and manage the global view of the central system. The GIS map shows the geographic locations of remote sites, of which the resources can be displayed.

**Before You Start**

Make sure you ***have configured a GIS map*** .

**Steps**

1. Click **Map Settings** in the top right corner of the map module to enter the map settings page.
2. **Optional:** Select an area on the left to show its GIS map.
3. Click **Remote Site** on the right to display available remote site(s).
4. Drag a remote site to the map.

   The icon will be displayed on the map.
5. **Optional:** Perform the following operations.

| | |
|---|---|
| **View Site's Resources** | Click the site on the map, and select **View Site's Resources**. The resource list of the site will be displayed on the left. |
| **Edit Site** | Click the site on the map, and select **Edit** to enter the description of the site. |
| **Delete Site** | Click the site on the map, and select **Delete** to remove the site from the map. |
| **Move Site** | Drag the site to change its location on the map. |

**Note**

Editing remote site resource is not supported.

## 28.1.9 Add Geographic Area to Map

Geographic areas refer to a customized map area with elements added to the map. Geographic areas are used to manage multiple elements added to the map. After adding a geographic area to the map, you can batch operate the elements within the area.

Click **Map Settings** in the top right corner of the map module to enter the map settings page.

Select an area on the left, and select an E-map or GIS map.

Click **Geographic Area**, left-click to draw a point, and right-click to finish.

**Note**

- When an alarm occurs from a camera in the area, the geographic area will blink in the color configured in the event and alarm module.
- A resource within the area will be highlighted to indicate that it has been successfully associated with the area. Resources can be dragged in and out so that you can add or remove resources to the region.

## 28.2 Monitor on Map

After configuring the maps via Web Client, you can view hot spots, hot regions, and resource groups etc., on the map. You can also zoom in/out to view the map and search locations on the map.

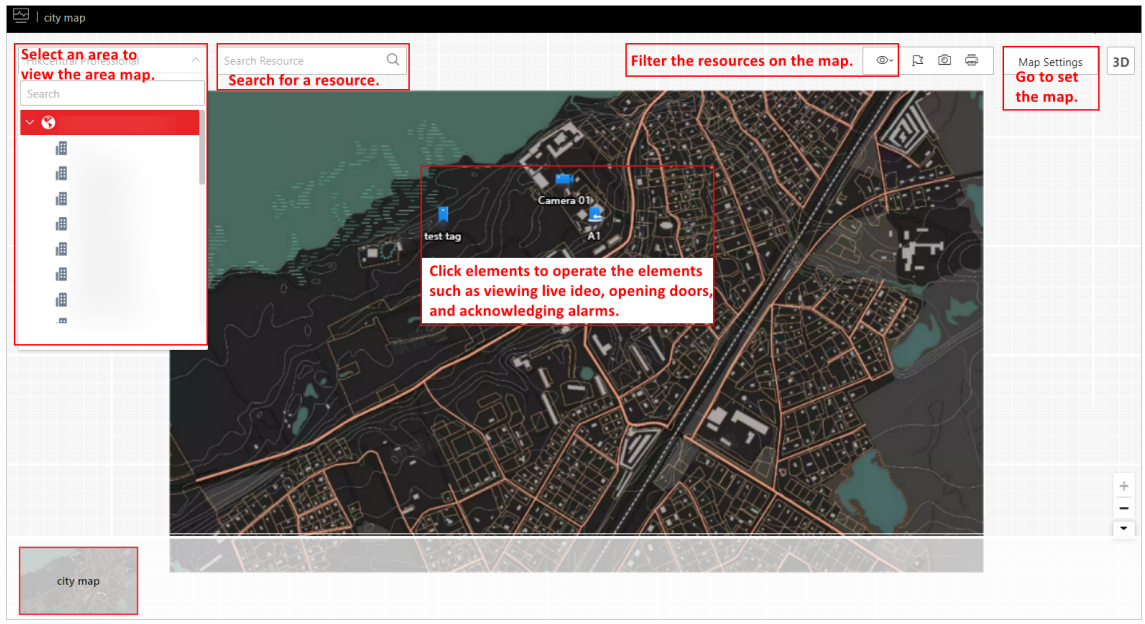



**Figure 28-9 Map Monitoring**

### 28.2.1 View and Operate Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, radars, sites, UVSS, etc. on the map. Also, you can set the arming control and view history alarms

of monitoring scenarios through the hot spots. You can view latitude and longitude information and available operations of a certain resource by hovering over a resource on GIS map as well.

**Before You Start**

Configure the map settings via the Web Client. For details, see ***Map Management*** .

**Steps**

1. Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page. On the top left of the map, select an area from the **Select Map** drop-down list.

   All maps of the area will be displayed.
2. Select a map to enter the map.
3. **Optional:** Perform the following operations on the map.

| | |
|---|---|
| **Filter Resource on Map** | Click and check resource type(s) as desired. |
| **More Tools** | : Add a label on map.<br>**2D/3D**: Switch the displaying dimension of the map.<br>: Search hot spot or location on the map. |

4. Hover over a hot spot to open the dialog which displays its related functions.

**Note**

- If there is an alarm triggered on the hot spot, the hot spot icon will turn into red alarm mode. Click the red icon, and you can view the detailed alarm information.
- Click parking lot data, a panel of parking lot details will pop-up. You can view detailed parking lot information such as parking space occupancy rate and parking floor details.

5. Operate in the dialog.

| | |
|---|---|
| **Arm or Disarm Hot Spot** | You can arm or disarm the hot spots via the arming control function. After arming the device, the current Client can receive the triggered alarm information from the hot spot.<br>Click a hot spot to open the dialog which displays its related functions. In the dialog, click **Arm**/**Disarm** to arm/disarm the hot spot. |
| **Trigger/ Disable Audio Alarm** | Click a hot spot to open the function list, and click **Trigger Audio Alarm** to trigger the audio alarm.<br>Click **Disable Audio Alarm Linkage** to disable audio alarm permanently or for a customized period. |
| **Trigger/ Disable Strobe Light** | Click a hot spot to open the function list, and click **Trigger Strobe Light** to trigger the strobe light alarm.<br>Click **Disable Strobe Light Linkage** to disable strobe light permanently or for a customized period. |
| **View History Alarm** | When an alarm is triggered, it will be recorded in the system. You can check the history log related to an alarm, including the alarm source details, alarm category, alarm triggered time, etc. |

Click a hot spot to open the dialog which displays its related functions. In the dialog, click to enter the event and alarm search page. Then you can search history alarms of the hot spot. See ***Search for Event and Alarm Logs*** for details.

**Broadcast via Hot Spot**

You can broadcast via hot spot through real-time speaking or playing the saved audio files.

**Note**

Make sure you have added broadcast resources on the map.

a. On the map, click the broadcast resource to view details such as Status, Area, and Remark.
b. Click **Broadcast** to select the broadcast mode.
c. Select **Speak** or **Play Audio File** as the broadcast mode.

**Note**

**Speak**: Speak in real-time, and the audio will be recorded and uploaded to the server.

**Play Audio File**: Play the files saved in the server. You can search or select a desired audio file to play. You can click **Download** to download a selected audio file, and the broadcast will be more fluent.

d. Click **Start**.
   - If you select Speaking, the broadcast will start immediately.
   - If you select **Play Audio File**, it will start downloading the audio file from the cloud if you choose a cloud file, or playing the audio file immediately if it is a local file.

**6.** You can click a resource to open a side pane, showing simplified information by default. On the side pane, you can view the latest 20 records (e.g., alarms, vehicle passes, face captures) of over 20 types of resources including cameras, vehicles, access control devices, broadcast devices, radars, etc.

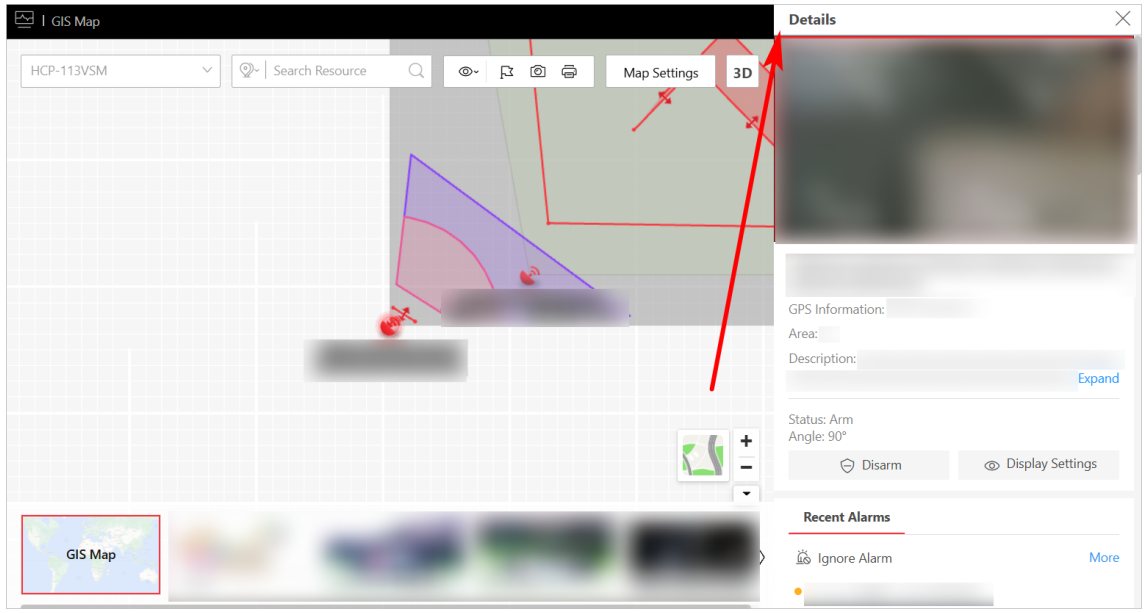



**Figure 28-10 Click Resource to View Details**

## 28.2.2 Preview 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.

**Before You Start**

Configure the map settings via the Web Client. For details, see ***Map Management*** .

**Steps**

1. In the top left corner of Home page, select → **Visual Map → Map → Map Monitoring** .
2. Click an area on the top left to display the map(s) of an area.
3. **Optional:** If an area has multiple maps, click a map to select it.
4. Click a hot region on the map, and on the Details page you can click a map to enter the map of the hot region.

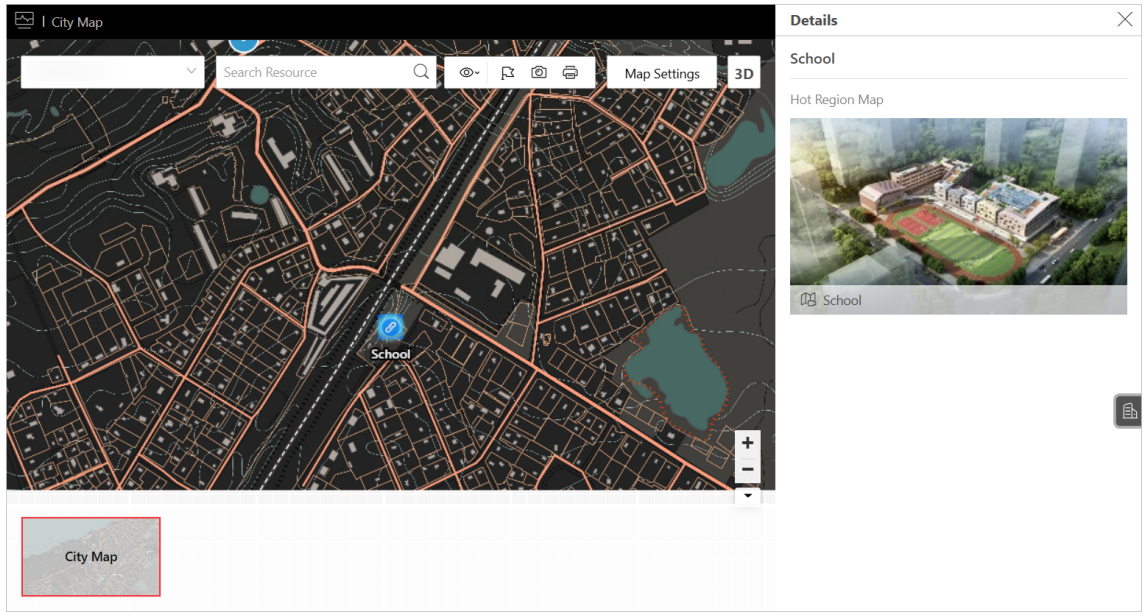



**Figure 28-11 Open the Details Pane**

**Note**

If you enter an area map from a particular map, the full path of the hot region map will be displayed in the upper-left corner. Each time you click **Back**, it only returns to the previous level of the map.

### 28.2.3 Preview Resource Group

During displaying map, you can view locations and regions of the resource groups, including people counting group, multi-door interlocking group, and anti-passback group. You can also perform further operations on the resources in the group.

**Note**

Make sure you have configured the required resource group and map settings via the Web Client. For details, see ***Map Management*** .

Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page.

- People Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the region of the group will be highlighted on the map to notify the user on the Client.
- Pathway Analysis Group: You can view the real-time number of people walking by in the Monitoring module on the Client.

- Anti-Passback Group: When an anti-passback alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Client.
- Multi-Door Interlocking Group: When multi-door interlocking alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Client.
- Entry & Exit Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

### 28.2.4 View Remote Site Alarm

If you have added a remote site on a GIS map, you can view the information of alarms triggered on the remote site. Even if there is no alarm triggered at the current time, you can also view history alarms of the site.

**Before You Start**

Make sure you ***have added a remote site*** on the GIS map.

**Steps**

1. Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page.
2. **Optional:** Select an area on the left to show its GIS map.
3. Click the site icon to open the site details page.

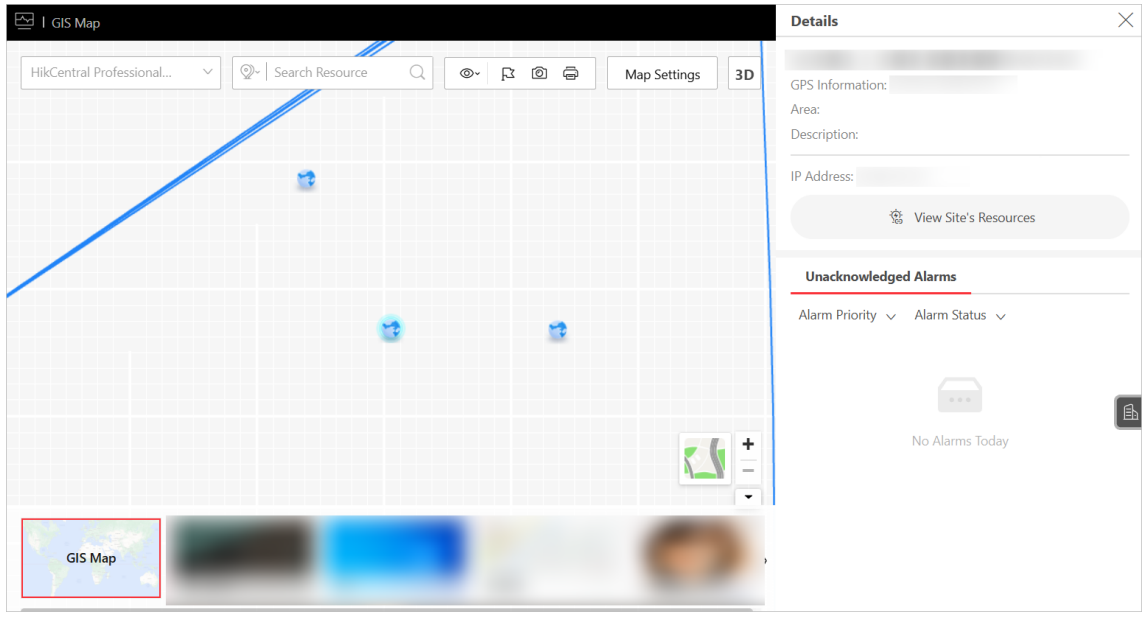



**Figure 28-12 Site Details**

4. **Optional:** Perform the following operation(s).

| | |
|---|---|
| **Filter Alarm by Priority** | Click **Alarm Priority** on the Alarm Priority column to filter alarms by alarm priority. |
| **Filter Alarm by Status** | Click **Alarm Status** on the Alarm Status column to filter alarms by alarm status. |

## 28.2.5 Operate Resources from Geographic Area

After you add a geographic area to a map, you can batch operate the resources within the area.

Click **Map Monitoring** in the top left corner of the map module to enter the map monitoring page.

Click **Select Map** on the top left to display the map(s) of an area.

**Note**

- When multiple geographic regions overlap, you can select the geographic region from the list first and then click the menu.
- Batch operation is not supported when there are more than 100 resources in a geographic area.

Click the geographic area to perform the following operations.

| | |
|---|---|
| Block All Alarms | Click **Ignore All** to block all alarms in the area. |
| Broadcast | Click **Broadcast**, and all IP speakers in the area will start to broadcast and the device icon status will change. |
| Audio Alarm Control | Click **Audio Alarm Control** to start audible alarms. |
| Strobe Light Alarm Control | Click **Strobe Light Alarm Control** to start sound and light alarm of all devices in the area with the feature. |

# Chapter 29 Augmented Reality (AR) Monitoring

To start AR monitoring, you need to first add AR cameras, then add scenes, and finally add scenes to maps on the Web Client. After configuration on the Web Client, you can monitor on the Control Client.

Based on the augmented reality (AR) technology and AR real map service (ARRM), by analyzing the person/vehicle event information overlaid in the real-time videos that are streamed from linked AR camera channels and speed dome channels, you are able to grasp the key area's situation and develop strategies for commanding and dispatching in response.

**Note**

If the AR license is not purchased, the AR menu will not be displayed.

## 29.1 Add Scene

Scenes refer to panoramic images captured by AR channels. You can add a scene to an area, and link an AR camera channel and a speed dome camera with the scene.

Go to → **Visual Map** → **AR** → **Add Scene** .

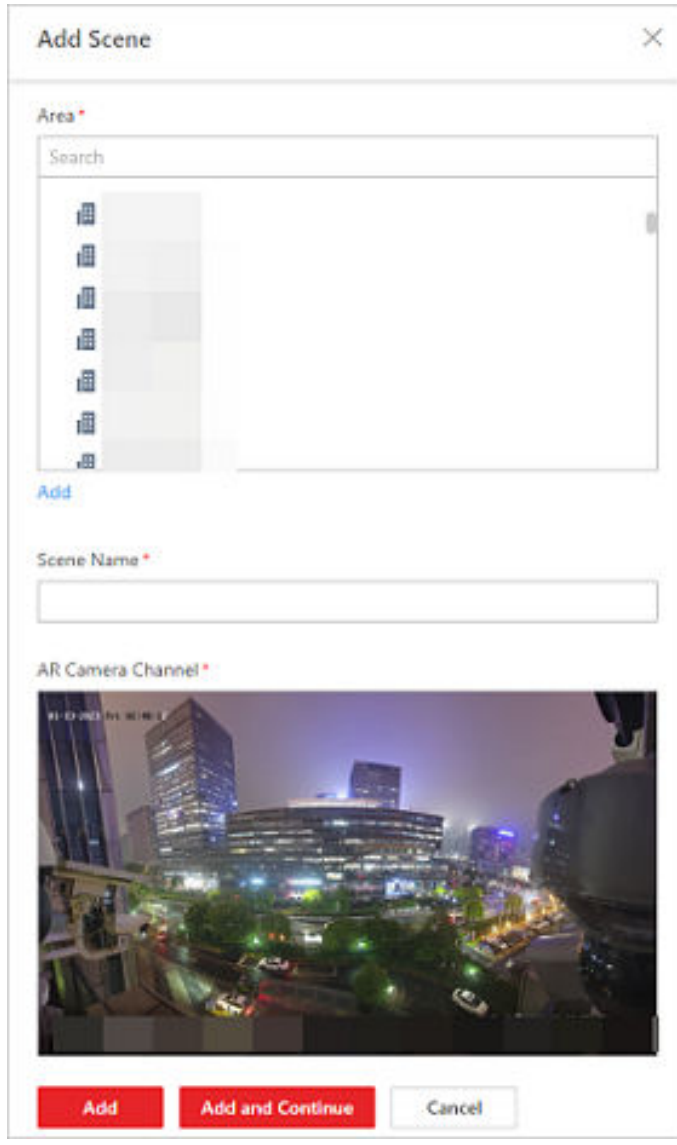



**Figure 29-1 Add Scene**

Select an area for the scene and set a name for the scene.

You can add an AR camera and a speed dome to a scene or just add an AR camera. AR cameras are for getting panoramic images, and speed domes are for tracking targets or zooming in parts on panoramic images.

**Note**

Under the condition that speed domes are not configured for the scene, visual tracking will not be available.

Click **Add**, or click **Add and Continue** to add another scene.

After adding scenes, you can set their locations on the map. For details, refer to ***Add Scene to Map*** .

## 29.2 Add Scene to Map

After scenes are added, you need to configure their locations on maps.

**Note**

Make sure you add scenes first. For details, refer to ***Add Scene*** .

1. Go to → **Security Monitoring** → **Visual Map** → **AR** .
2. In the scene list, click in the Operation column, and you will be redirected to the Geographic Location Configuration page.
3. Hover over a scene, click , and drag its icon to adjust its location on the map.

   **Note**

   The added scene will be marked with a small map icon in its upper right corner.

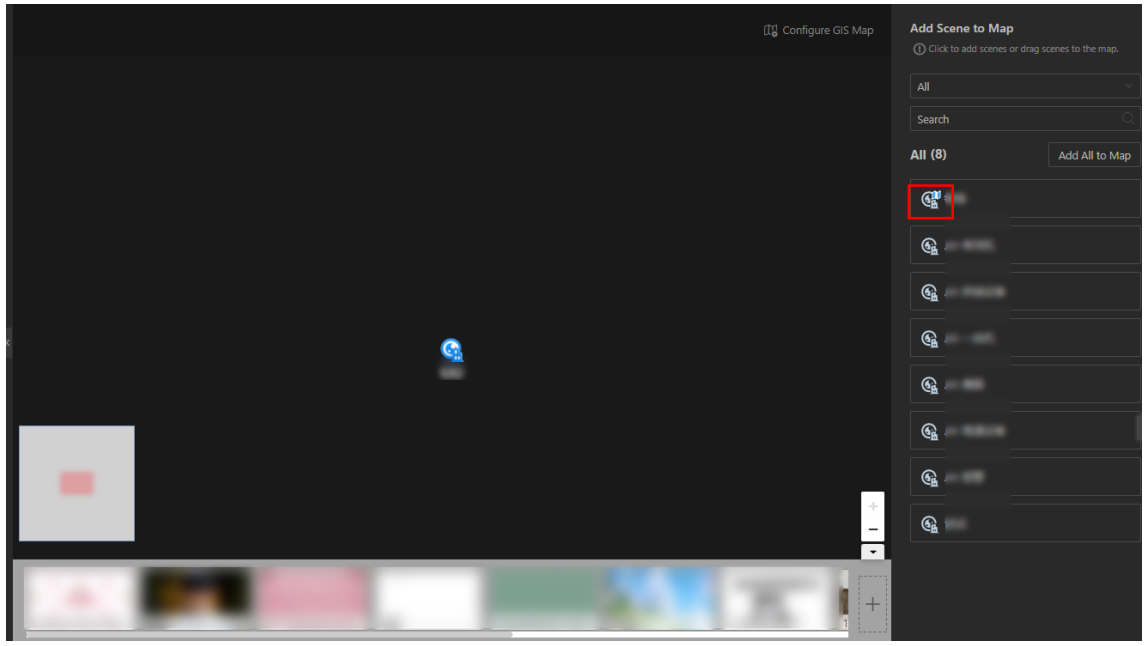



**Figure 29-2 Icon of Added Scene**

4. Click **Finish**.

# Chapter 30 Alarm Detection

A security control device detects persons, vehicles, or other emergency events in the detection region, and reports event/alarm information (such as location) to the security personnel.

On the Web Client, after adding a security control device to the system, you need to group the device's alarm inputs into areas on the platform. You also need to set one arming schedule for the alarm inputs in a security control partition (area) which defines when and how to arm the alarm inputs in this security control partition (area).

For example, area 1 is created to manage all the resources on the first floor. If there is one security control device mounted on the first floor, you need to add its zones (alarm inputs) into area 1 first, link the zones with security control partitions (areas) and set arming schedules for these security control partitions (areas). After that, the zones in different partitions (areas) can be armed according to the schedules respectively.

## 30.1 Alarm Detection Overview

On the Alarm Detection Overview page, you can view the health status of security control devices and alarm detection event details.

On the top navigation bar, go to → **Security Monitoring → Alarm Detection → Alarm Detection Overview** .

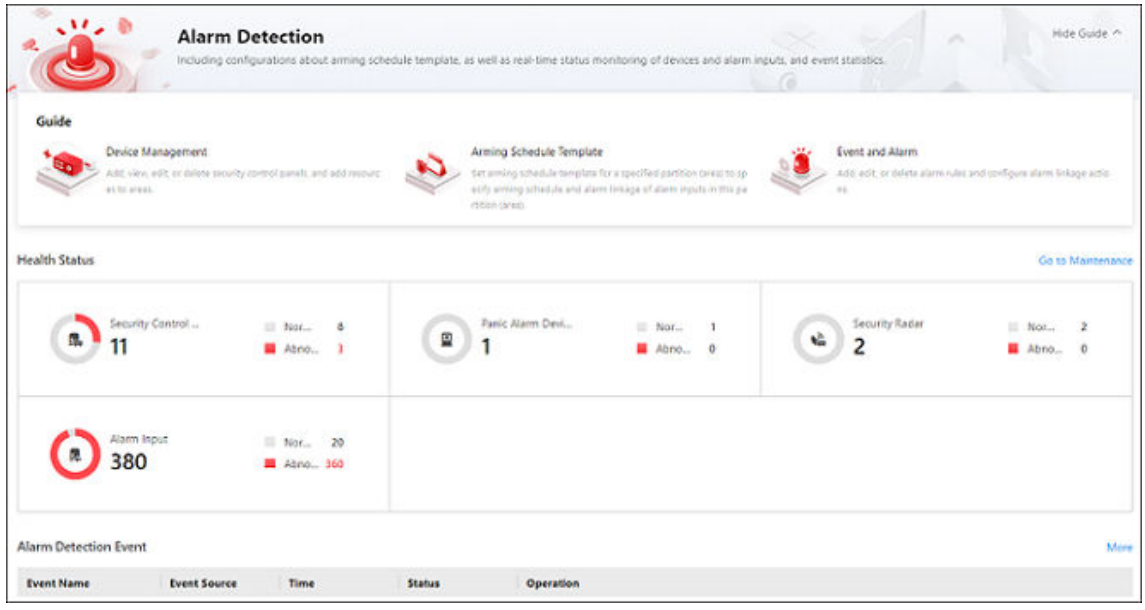



**Figure 30-1 Alarm Detection Overview**

| Content | Description |
|---|---|
| Guide | You can view the brief introduction of the Alarm Detection function and the major steps of configuration, including device management, arming schedule template setting, and event and alarm configuration. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page. |
| Health Status | You can view the health status of devices including security control panels, panic alarm devices, security radars, and alarm inputs. Click on the number under the resource type or the number besides **Abnormal** to view their details.<br>Click **Go to Maintenance** to enter the Maintenance module. |
| Alarm Detection Events | You can view the event details, including the event time, event source, time, status, and available operations. |

## 30.2 Flow Chart of Alarm Detection

The following flow chart shows the process of the configurations and operations of alarm detection.

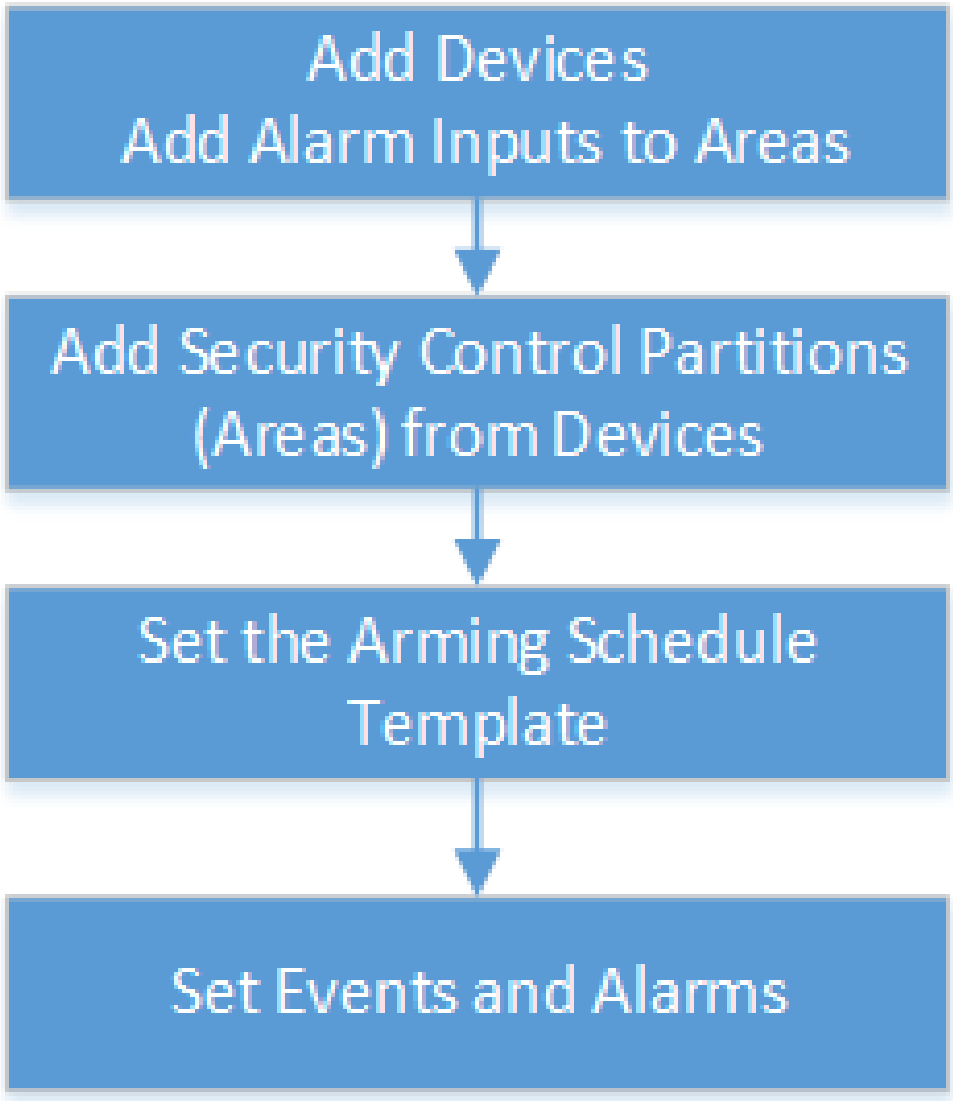



**Figure 30-2 Flow Chart of Alarm Detection**

- **Add Devices**: Add security control devices to detect persons, vehicles, or other emergency events in the detection region. And then add alarm inputs to areas for management.
- **Add Security Control Partitions (Areas) from Devices**: Add alarm inputs and partitions (areas) from devices for arming or disarming zones, bypassing zones, and clearing alarms. Refer to ***Add Security Control Partitions (Areas) from Device*** for details.
- **Set the Arming Schedule Template**: Set an arming schedule template for a specified partition (area) to specify the arming schedule of the alarm inputs in this partition (area). Refer to ***Configure Arming Schedule Template*** for details.
- **Set Events and Alarms**: Set event and alarm parameters and linkage actions to view event and alarm details on the Client, timely remind the security personnel to handle related issues, or

search history events and alarms when an emergency occurs. Refer to ***Event and Alarm*** for details.

## 30.3 Add Security Control Partitions (Areas) from Device

After adding security control devices to the platform, you need to import the partitions (areas) configured on the devices and the alarm inputs in the partitions (areas) to areas on the platform for further operations, including configuring arming schedules for the partitions (areas), arming/disarming partitions (areas), bypassing zones, clearing alarms, etc.

**Before You Start**

Make sure you have added security control devices.

**Steps**

1. On the top navigation bar, go to → **Security Monitoring → Alarm Detection → Partition (Area)** .
2. Click + **Add** to show the Add Security Control Partition (Area) pane.

   In the Partition (Area) list, all the security control devices with partitions (areas) which are not added to the platform will be displayed.
3. Select the partitions (areas) that you want to add to the platform.
4. **Optional:** Switch on **Import Alarm Inputs** and select an area that the partitions (areas) and alarm inputs are imported to.

   **Note**

   After adding the alarm inputs to the area, you can manage them by different areas.
5. Click **Save**.

   The partitions (areas) will be displayed in the partition (area) list.
6. **Optional:** Perform further operations.

| | |
|---|---|
| **Edit Security Control Partition (Area)** | Click the name of a partition (area) to display the partition (area) details and then edit its name or set the arming schedule for it (see details in ***Configure Arming Schedule Template*** ).<br>**Note**<br>For the partition (area) of AX security control panel, you configure the arming schedule directly on the partition (area) details page rather than select a template from the platform. |
| **Arm/Disarm Security Control Partition (Area)** | After arming the partitions (areas), the platform can receive the triggered alarms in the partitions (areas).<br>There are three arming modes available. |

**Note**

The supported arming modes are displayed according to the device's capability.

- **Away Arm**: If all people in the detection area are going to leave, turn on this mode to arm the zones in the area after the defined dwell time.
- **Stay Arm**: It is used when people stay inside the detection area. Turn on the Stay mode to turn on all the perimeter burglary detectors (such as perimeter detectors, magnetic contacts, curtain detectors in the balcony). Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarms will not be triggered.
- **Instant Arm**: When people leave the detection area, the zones will be armed immediately without delay.

In the partition (area) list, select one or multiple partitions (areas) and click these buttons above to arm the partitions (areas), or click **Disarm** to disarm them.

Or you can click **Batch Operation** on the left and select devices to batch arm/disarm all partitions (areas) of the selected devices.

**Arm/Disarm Zone**

**Note**

For partitions (areas) that are disarmed, you can arm only a part of their zones.

Expand the partition (area) details and click / to arm/disarm the zone of the alarm input.

**Bypass/ Restore Zone**

**Note**

When some exception occurs in one zone, and other zones can work normally, you need to bypass the abnormal zone to turn off the protection of it. Otherwise, you cannot arm the security control partition (area) which the zone belongs to.

Expand the partition (area) details and enable/disable **Bypass** to bypass/ restore the zone of the alarm input.

**Clear Alarm**

Select one or multiple partitions (areas) and click **Clear Alarms** to clear the generated alarms.

**Add Partition (Area) on Map**

Select one or multiple partitions (areas) and click **Set Geographic Location** to add them on the map.

**Configure Arming Schedule**

Click **Configure Arming Schedule** and you can select multiple areas to batch set the arming schedule for them.

Click an area and in the Copy Arming Schedule From section, you can select an area to copy its arming schedule to the current area.

**Capture Picture**

For supported security control panels and detectors, click to capture a picture.

**Note**

- Supported models: DS-PWA64-M-WE (V1.3.2 and later), DS-PWA64-M-WB (V1.3.2 and later), and DS-PA502-128 (V2.1.2 and later).
- Supports both single- and dual-lens detectors. When two images are generated, they are merged and displayed together.

## 30.4 Add User of Security Control Device

You can add and manage users (operators) of AX PRO security control devices.

**Before You Start**

Make sure you have added security control devices.

**Steps**

1. On the top navigation bar, go to → **Security Monitoring** → **Alarm Detection** → **User Management** .

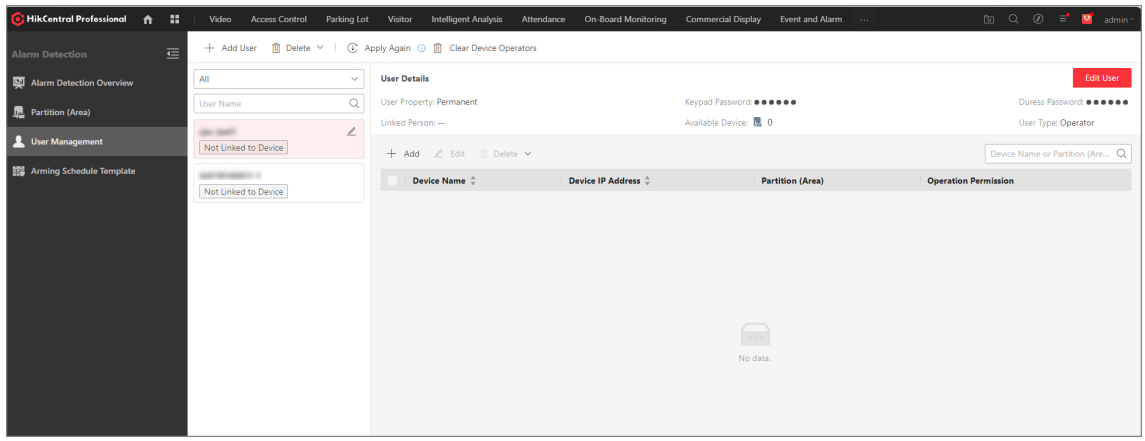



**Figure 30-3 User Management**

2. Click **Add User**.
3. Set **Basic Information** to add a user.

**User Name**

Enter a new one or select from the person list.

**User Property**

**Permanent**

All permissions can be configured for the user.

**One-Time User**

Expires after arming or disarming once, or automatically expires after 24 hours. No duress code permission. No keyfobs and tags permission.

**Keypad Password**

Optional.

**Duress Password**

Optional.

4. In the **Available Device** area, click **Add** and select devices and partitions (areas) to assign this user to. You can check the operations needed (**Arm**/**Disarm**/**Auto Control**).
5. Click **Add** or **Add and Continue**.

## 30.5 Configure Arming Schedule Template

The arming schedule defines the arming mode (instant arming / away arming / stay arming) in different periods for the partitions (areas) of the added security control devices.

**Steps**

1. On the top navigation bar, go to → **Security Monitoring** → **Alarm Detection** → **Arming Schedule Template** .
2. Click + to enter the Add Arming Schedule Template page.
3. Enter a name for the template.
4. **Optional:** In Copy from field, select an existing template from the drop-down list to copy the settings.
5. Select an arming mode and drag the mouse on the time bar to draw a time period.

**Note**

Up to 8 time periods can be set for each day.

**Instant Arm**

When people leave the detection area, the zones will be armed immediately without delay.

**Away Arm**

If all people in the detection area are going to leave, turn on this mode to arm the zones in the area after the defined dwell time.

**Stay Arm**

It is used when people stay inside the detection area. Turn on this mode to turn on all the perimeter burglary detectors (such as perimeter detectors, magnetic contacts, curtain

detectors in the balcony). Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarms will not be triggered.

6. **Optional:** Click **Erase** and click on the drawn time period to clear it.
7. Click **Add**.

The arming schedule template will be displayed on the arming schedule template list.

# Chapter 31 Evidence Management

In the Evidence Management module, you can manage case and the files (including pictures, videos, audios and other files), which contain important information about incidents such as traffic accidents and violent crimes for settling disputes or legal cases.

In the top left corner of the platform, select → **Security Monitoring** → **Evidence Management** .

## 31.1 Basic Settings

You can set the storage location for case and set custom items to define the file type, case tag, and additional content for file management and case management.

### 31.1.1 Set Basic Parameters

Before managing the files and cases, you should add case types, file tags, and additional contents to the platform for further filtering and searching.

**Steps**

1. On the left pane, select **Basic Configuration** → **Basic Parameter** .
2. Set the following parameters.

   **Case Type**

   The type of accident or suspect incident recorded in the case, such as theft, robbery, attack, and missing person, which is used for adding cases.

   Default case types are provided, and you can click **Add** to add more.

   **File Tag**

   The tag of file describing the file format, related case, etc, which is used for uploading files.

   Click **Add** and enter the file tag name to add a file tag.

   **Case Additional Content**

   The text such as the result/conclusion of incidents based on the evidence collected from the on-site organization, such as arrested, warned, and injured, which is used for adding cases.

   a. Click **Add**, and enter the additional content name.
   b. Select the type. If you select **Single Selection**, you need enter the options. If you select **General Text**, you can click **Add** to finish adding.
3. Click **Save**.

### 31.1.2 Set Storage Parameters

You can set the storage location for files and cases.

**Steps**

1. On the left pane, select **Basic Configuration → Storage Configuration** .
2. Set the storage location and configure related parameters.

   **Local Storage**

   Select the local resource pool.

   **SFTP**

   Set the required fields including address, port, user name, and password.
3. Click **Save**.

## 31.2 Manage Files

The files refer to the videos, pictures, and documents about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases. You can upload files from the local PC, set schedules for getting files from devices, and share added files. You can also link the added files with the specific cases.

**Note**

- The permission (such as viewing, editing, exporting, and sharing) of specified files (files linked to cases or files uploaded by portable devices) varies according to the user roles. On the User Permission page of an uploaded file displays the permission details.
- If the file is a portable device file uploaded by a police officer, then the officer is the default file owner.
- The file owner has all permissions. Upper-level users of the file owner have the same file permissions as the file owner. Users with super access permission can view all files.

### 31.2.1 Upload a Local File

You can upload files from your local PC to the Evidence Management Center. For the uploaded files, you can perform more operations such as viewing the added files by file type and file tag, and filtering and exporting the files.

**Steps**

1. Select **File Management** on the left.

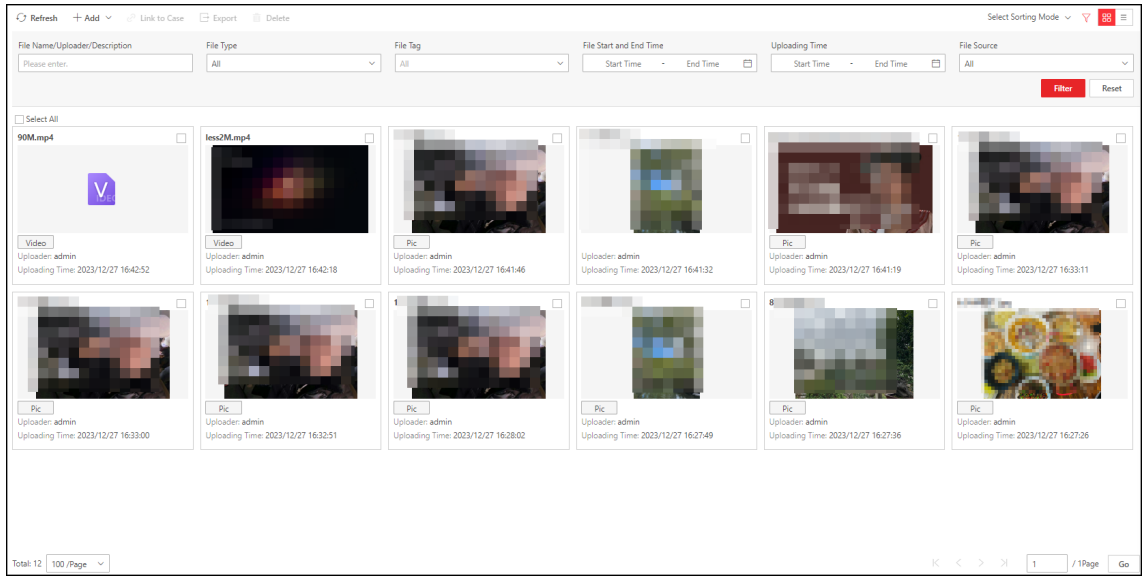



**Figure 31-1 File Management Page**

2. Click **Add → Upload Local File** to open the Upload Local File pane.
3. **Optional:** Select one or multiple file tags.

**Note**

Make sure you have added file tags, refer to ***Set Basic Parameters*** .

4. **Optional:** Set the geographic location when file was created according to the instructions on the interface.
5. Click **Upload** and select the pictures, videos, audios, or other files from the local PC to add.
6. Click **Save**.

## 31.2.2 Upload Files from Device

You can set a schedule to upload files from on-board cameras, portable devices, etc. to the Evidence Management Center. For the added files, you can perform more operations such as viewing the added files by file type and file tag, filtering and exporting the files.

**Before You Start**

Make sure you have added device(s) to the platform. For details, refer to ***Device and Server Management*** .

**Steps**

1. Select **File Management** on the left.
2. Click **Add → Upload from Device** .
3. **Optional:** Select one or multiple file tags, and enter the file description.

**Note**

Make sure you have added file tags, refer to ***Set Basic Parameters*** .

4. Select the uploading mode and set related parameters.

**Upload at Specified Time**

Specify the start time and end time of file uploading and recording.

**Upload When Wi-Fi Connected**

The files will be automatically uploaded once the Wi-Fi is detected and connected, so you are only required to specify the start/end recording time of cameras.

**Note**

Make sure you have added devices such as on-board devices and portable devices which support connecting to Wi-Fi.

5. Select one or multiple cameras in the Linked Camera list.
6. Click **Save**.

### 31.2.3 Save Files in Other Modules

Files generated from other modules can be saved in the Evidence Management Center, including Portable Enforcement and Event and Alarm module. When saving the videos/audios/pictures/documents in other modules to the Evidence Management Center, you can specify the adding mode and file tag of the files for further management.

### 31.2.4 View and Edit Files

After adding files to the Evidence Management Center, you can view the details of files and edit the information. For example, you can play the video files, add masks and texts, clip videos, enable the silent mode for linking video files with corresponding cases afterward.

Select **File Management** on the left.

#### Manage Added Files

| Operation | Description |
|---|---|
| Filter the Files | Click in the upper right corner to unfold the filter pane, set conditions such as file type and file tag, and then click **Filter** to filter the target file. |
| Refresh the Files | Click **Refresh** to refresh the file list. |
| Link the Files to Case | Select files to link to cases. For details, refer to ***Link Files to Cases*** . |

| Operation | Description |
|---|---|
| Export the Files | Select the files and click **Export** to export them.<br>**Note**<br>For viewing the file exporting records, refer to ***Manage Operation Records*** . |
| Delete the Files | Select the files and click **Delete** to delete them. |
| Switch Display Mode | Click or or to display added files in card mode or list mode or map mode. |

## View and Edit a File

In the card mode or list mode, you can click the file name to open the file details pane and perform the following operations if needed.

**Note**

Only videos in PS, TS, or MPEG-4 container format can be played and edited after fully loaded.

| File Format | Operation | Description |
|---|---|---|
| Common | View Details | View who uploaded the file, uploading time, file size, and description. Persons of the file owner's department have the permission to view file details. |
| | Edit Basic Information | Edit the file name, file tag, and description. |
| | Edit User Permission | In User Permission, click to edit the file permissions of the shared users. |
| | Link to Case | Click and enter the case name, ID, or description to search for the cases to be linked. |
| | Confirm Integrity Verification Value | Click to copy the case's integrity verification value. You can check the file integrity by comparing the integrity verification value of the platform and that of the exported file. |
| | Search File on Map | Click to search files on the map by entering a geographic location or specifying an area for search. |
| Picture | Zoom in Picture | Click to zoom in the picture. |
| Video | Start/Pause/Stop Video Play | Click / / to start/pause/stop playing the video. |

| File Format | Operation | Description |
|---|---|---|
| | Normal/Reverse Playback | Click to perform reverse playback.<br>Click and to perform speed playback. |
| | Full Screen | Click to show the video in full-screen mode. |
| | Edit Video | Click to enter the Edit Video page, and drag the timeline to position the desired video segment.<br>• Click **Add Text** to enter the text, and drag it to the proper location.<br>• Click **Add Mosaic**, and draw a desired region of mosaic on the video.<br>• Select a clip, click **Clip**, drag the timeline to a desired position, and click again to finish clipping.<br>• Select one or multiple clips and click **Delete** to delete them.<br>• Select the audio and click **Audio Off** to set the video to the mute mode. |

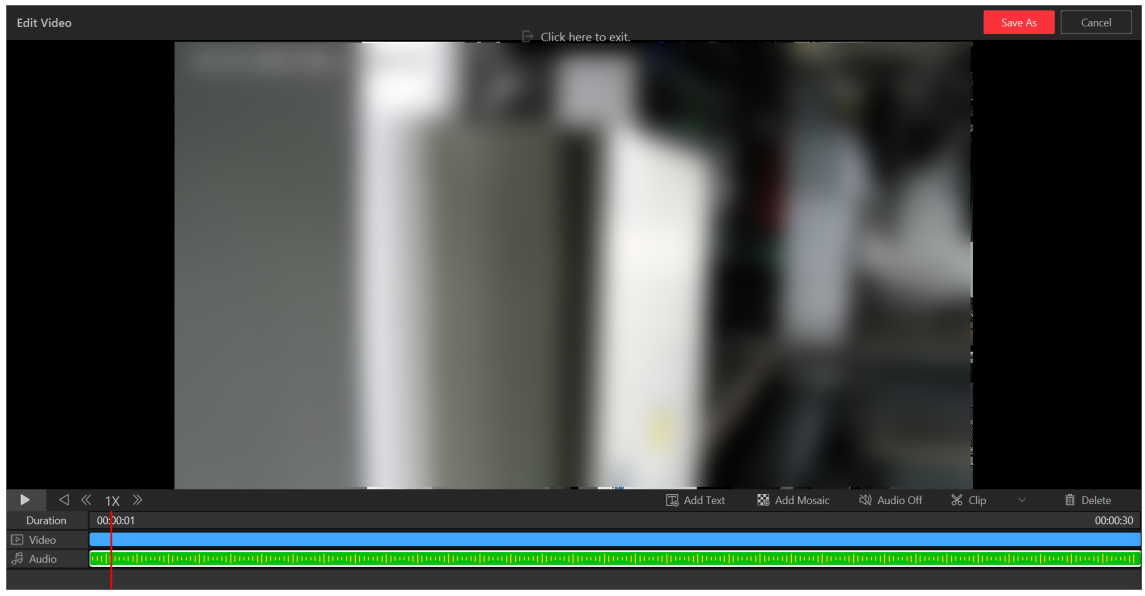



**Figure 31-2 Edit a Video File**

## 31.2.5 Share Files

You can share files to users whom you have the permission to share with. The shared users have the permissions for, such as viewing, sharing, and editing the file, as you set. You can also view the files shared by other users.

Selected the added files and click **Share**.

### Share to System Internal User

Click **Add** to select users as file receivers. Set the permissions of receivers, and click **Share**.

### Share to System External User

Click **Add Email** to add the emails of file receivers. Set the email title and content. Set the permissions of receivers and the expiry date, and click **Share**.

## 31.3 Manage Cases

A case is about incidents such as traffic accidents and violent crimes. You can add, edit, and share cases. After adding cases, you can link files uploaded from the local/device to cases and the linked files can be used as materials for settling disputes or legal cases.

**Note**

- The case permission (such as viewing, editing, exporting, and sharing) varies according to the user roles. On the User Permission page of an added case displays the permission details.
- The case owner has all permissions. Upper-level users of the case owner have the same permissions as the case owner. Users with super access permission can view all cases.

### 31.3.1 Add a Case

You can add case about incidents such as traffic accidents and violent crimes for settling disputes or legal cases. You can set detailed information for the added case, including the case name, ID, type, tag, on-site organization, result/conclusion, status, and time. Also, you can upload the file (including pictures, audios, videos, Excel files, CSV files, PDF files, and others) as the case content from cameras or the File Management page.

**Before You Start**

Make sure you have configured basic settings. For details, refer to ***Basic Settings*** .

**Steps**

1. On the left navigation pane, select **Case Management**.
2. Click **Add** to enter the Add Case page.

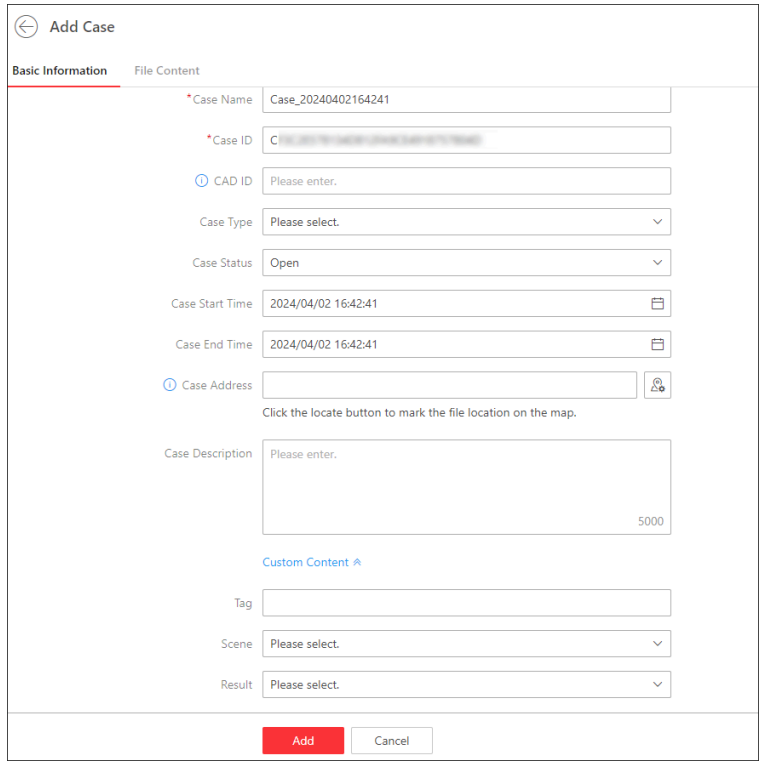



**Figure 31-3 Add Case**

3. Create a name for the case.

   The case ID will be generated automatically on the Client. You can edit the case ID which should include 1 to 64 letters or digits.
4. **Optional:** Set the CAD ID, type, status, time (start time and end time of the case event), case address, description, etc. for the case.
5. Click **File Content** tab to enter the File Content page.
6. **Optional:** Set the mode of adding files to the case.
   - Select **Add → Upload Local File** to upload files (such as pictures, audios, and videos) from the local PC for the case content.
   - Select **Import From File Management**, check one or multiple files related to the case, and click **Confirm**.
7. Click **Add** to add the case and back to the Evidence Management page.

## 31.3.2 View and Edit Cases

Select **Case Management** on the left.

You can view the details of cases, edit the case information, and export cases to your local PC.

| Operation | Description |
|---|---|
| Refresh Case | Click **Refresh** to refresh the latest view of case information. |
| Switch Display Mode | Click or or to display added cases in card mode or list mode or map mode. |
| Select Sorting Mode | Click **Select Sorting Mode** to select the display order. |
| Delete Case | Select the case(s) and click **Delete** to delete the case(s). |
| Filter Case | Click on the upper right corner of the Evidence Management page, enter a keyword in the search box or set filter conditions, and click **Filter** to filter the target case(s). You can also click **Save Filtering Condition** to save the current filtering conditions settings for later use. |
| Open/Close Case | Select one or multiple cases, and click **Close Case** to close the case if the related case is settled, or click **Open Case** to open the selected case if the related-case is pending. |
| Export Case Record | Click **Export** to export the selected case record(s) in Excel, CSV, or PDF format. Or click **Export All** to export all cases.<br>**Note**<br>• You can check **Include Case File** to export the attached case file.<br>• You can view the download records in the Download Record page. |
| View Case Details and Edit Case | • In the card mode or list mode, you can click the case name to view the case's basic information, file content, and operation records.<br>• You can edit the case's basic information, such as the case type, time, and tag.<br>• You can upload more related files from local PC for the case content, delete unneeded files, and search for files.<br>• You can click **Case Report** to download the case report. The report includes case basic information, linked evidence file, and detailed operation record. You can view the download records in the Download Record page. |
| Search Case on Map | In the map mode, you can search for cases by entering a geographic location or specifying an area. |

### 31.3.3 Share Cases

You can share cases to users whom you have the permission to share with. The shared users have the permissions for, such as viewing, sharing, and editing the case, as you set.

Selected the added files and click **Share**.

#### Share to System Internal User

Click **Add** to select users as case receivers. Set the permissions of receivers, and click **Share**.

#### Share to System External User

Click **Add Email** to add the emails of file receivers. Set the email title and content. Set the permissions of receivers and the expiry date, and click **Share**.

## 31.4 Link Files to Cases

You can link the added file to the existing case or newly added case. The linked files recorded in the case can be used as materials for settling disputes or legal cases.

**Note**

Make sure you have added the file(s).

On the left pane, select **File Management**.

#### Link a Single File to One or Multiple Cases

1. Click a file to open the file details pane.
2. In **Basic Information** page, click + to add a case field.

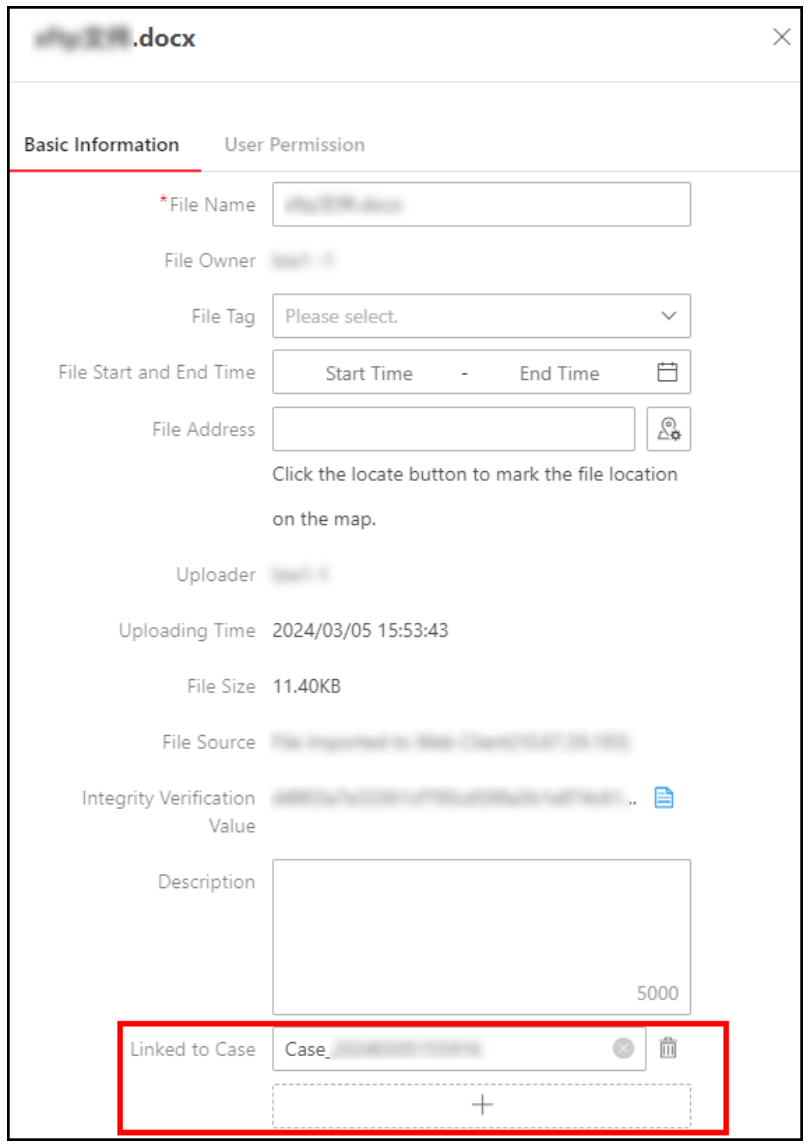



**Figure 31-4 Link a Single File to Case**

3. Search and select a case by the name or ID.
4. Click **Save**.

## Batch Link Files to One Case

1. Select multiple files.
2. Click **Link to Case** to open the Link to Case pane.
3. Search and select a case by the name or ID.
4. Click **Save**.

## 31.5 Manage Operation Records

You can manage the operation records, including viewing or deleting the upload/download records of case or files.

Select **Operation Record → Upload Record** or **Operation Record → Download Record** on the left.

On the Upload Record page, you can view the records (including case or file size and upload status) of the case or files uploaded from local PC or related cameras. And on the Download Record page, you can view the records (including case or file size and download status) of exporting case or files on the platform.

You can also search for records by name, check a record and click / / in the Operation column to pause/resume/retry the upload/download task. Or you can check record(s) and click **Delete** to delete the selected record(s).

# Chapter 32 Patrol Management

The system provides the service for patrol management, with which you can create patrol routes and arrange patrol persons to perform the patrols (by checking in at the patrol points offline) according to the shift schedules. You can monitor the patrol online in real time to conveniently know whether exceptions occur during patrols, and view and export patrol-related events records / statistics.

On the Web Client, you can set patrol points, patrol person groups, patrol schedule templates, patrol routes, etc., perform real-time monitoring, search for patrol-related event records, and view patrol statistics.

## 32.1 Patrol Overview

The Patrol Overview page shows the wizard for the Patrol Management module, and Today's Patrol Route Statistics (including Patrol Shift Status Statistics and Patrol Route Status Statistics).

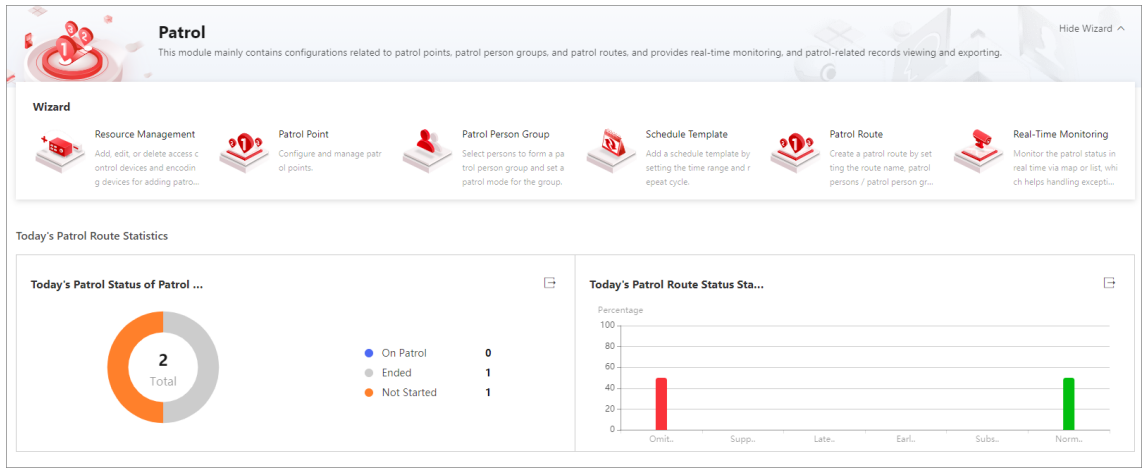



**Figure 32-1 Patrol Overview**

### Patrol Shift Status Statistics (Today's Patrol Route Statistics)

You can view the total number of patrol routes which have shift(s) for the current day, and the numbers of patrol routes with different patrol shift status. You can also click the total number to switch to the Real-Time Monitoring page, or click to export the chart in PDF, PNG, or JPG format.

**On Patrol**

Shows the number of patrol routes of which the earliest shift has started/ended and the last shift is not ended.

**Ended**

Shows the number of patrol routes of which all the shifts for the current day have ended.

**Not Started**

Shows the number of patrol routes of which the earliest shift has not started.

### Patrol Route Status Statistics (Today's Patrol Route Statistics)

You can view the percentages of patrol routes with different status (omitted patrol, supplemented patrol, etc.). You can also click to export the chart in PDF, PNG, or JPG format.

**Omitted Patrol**

Indicates that the patrol is not performed within the scheduled time period.

**Supplemented Patrol**

Indicates that the patrol is performed after the scheduled time period.

**Late Patrol**

Indicates that within one patrol shift, the patrol is first performed before the scheduled time period, and then performed again after the scheduled time period.

**Early Patrol**

Indicates that the patrol is performed before the scheduled time period.

**Substitute Patrol**

Indicates that the actual patrol person who performed the patrol is not the planned patrol person.

**Normal Patrol**

Indicates that the patrol is performed within the scheduled time period by the planned patrol persons.

## 32.2 Flow Chart of Patrol Management

The flow chart below shows the process of configuring and managing patrols.

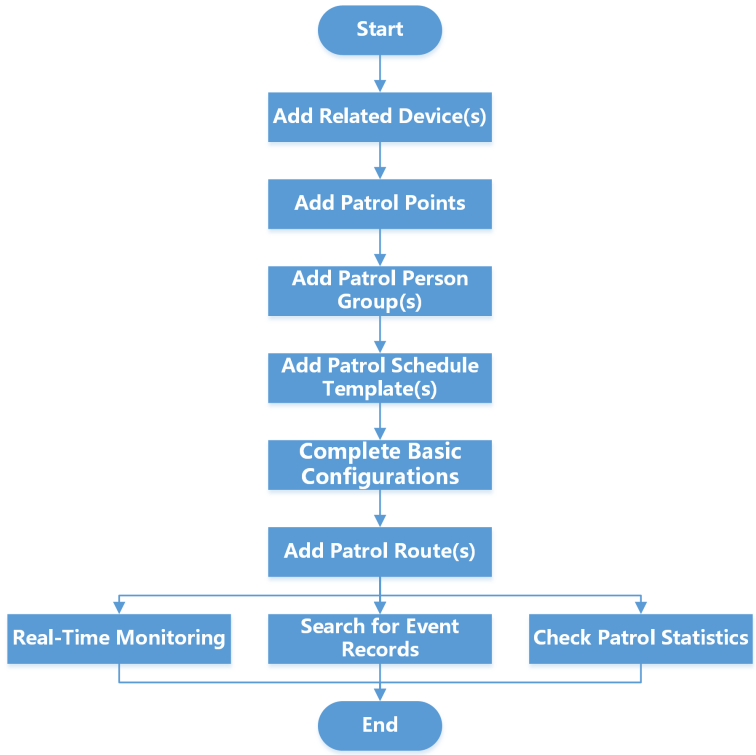



**Figure 32-2 Flow Chart of Patrol Management**

**Table 32-1 Flow Chart Description**

| Step | Description |
|---|---|
| Add Related Device(s) | Add devices used for adding patrol points, real-time monitoring, etc. |
| Add Patrol Points | Before you create a patrol route and start a patrol, you need to add patrol points. You can set access points as patrol points, or generate QR codes to be patrol points. The patrol persons have to check in at the patrol points to perform the patrol. See ***Add Patrol Points*** for details. |
| Add Patrol Person Group(s) | Before adding a patrol route, you can select persons to form a patrol person group and set their patrol mode. See ***Add Patrol Person Group*** for details. |

| Step | Description |
|---|---|
| Add Patrol Schedule Template(s) | You need to set the schedule template first in order to schedule a patrol. See ***Add Patrol Schedule Template*** for details. |
| Complete Basic Configurations | To manage patrols, you need to set the parameters according to your needs. You can set the exception types for patrol persons to report, storage location of attachments, time for advance notification, and detection interval at which the server detects patrol route status. See ***Basic Configurations for Patrol Management*** for details. |
| Add Patrol Route(s) | Set the route name, patrol person / patrol person group, patrol schedule, patrol duration, patrol point, patrol pattern, shift schedule, etc., to form a complete patrol route. See ***Add Patrol Route*** for details. |
| Real-Time Monitoring | Monitor the patrol status in real time via map or list, to conveniently know whether an exception occurs during the patrol, which helps handling the exception in time. See ***Real-Time Patrol Monitoring*** for details. |
| Search for Event Records | Search for and export patrol-related event records including patrol events and exception reporting. See ***Search for Patrol-Related Event Records*** for details. |
| Check Patrol Statistics | Filter, check, and export patrol statistics by patrol route, patrol point, and patrol person. See ***Check Patrol Statistics*** for details. |

## 32.3 Basic Configurations for Patrol Management

To manage patrols, you need to set the parameters according to your needs. You can set the exception types for patrol persons to report, storage location of attachments, time for advance notification, and detection interval at which the server detects patrol route status.

### 32.3.1 Add Exception Types for Patrol Management

You can add exception types for patrol persons to select from when they need to report exceptions via Mobile Client during patrols.

**Before You Start**
Make sure you have configuration permissions for patrol management.

**Steps**
1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Basic Configuration** → **Exception Type** .
2. On the top left of the page, click **Add**.

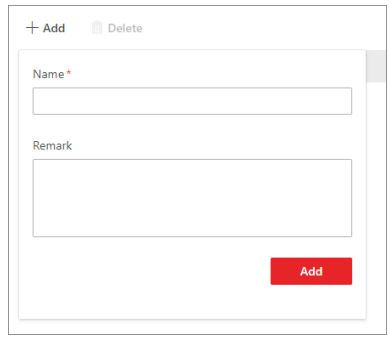



**Figure 32-3 Add Exception Type**

3. Enter a name for the exception type.
4. **Optional:** Enter the remark for the exception type.
5. Click **Add**.

   The added exception type will be displayed on the exception type list.
6. **Optional:** Perform the following operations according to your needs.

| | |
|---|---|
| **Edit an Exception Type** | In the Operation column, click to edit the name and remark of the exception type. |
| **Delete Exception Type(s)** | Select the exception types to be deleted and click **Delete** on the top left of the page. |

### 32.3.2 Set Parameters for Patrol Management

You can set parameters including Local Storage Configuration, Notification Time, and Detection Frequency to manage patrols and patrol-related attachment storage.

**Note**

Make sure you have configuration permissions for patrol management.

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Basic Configuration** → **Parameter Configuration** .

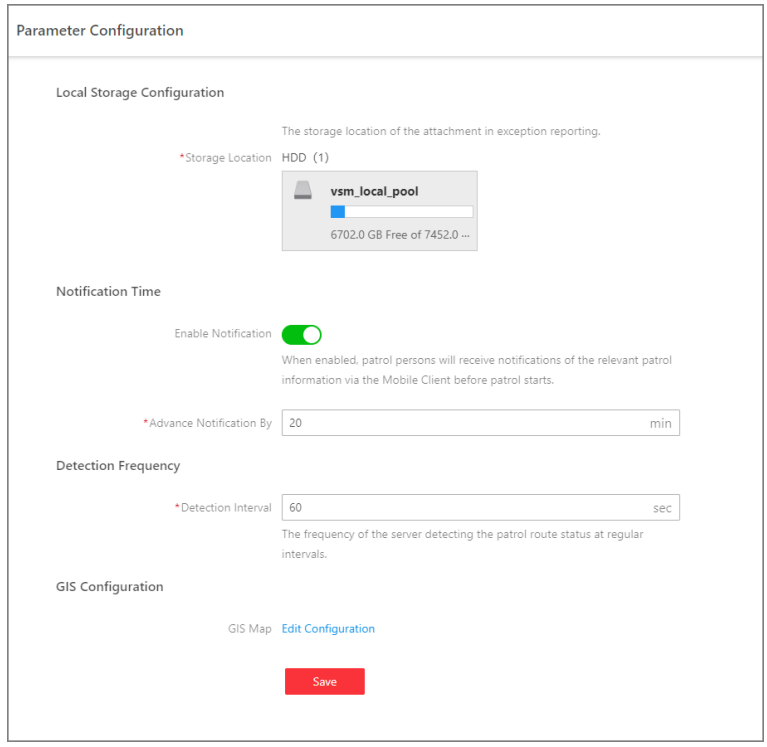



**Figure 32-4 Parameter Configuration**

2. Configure the following parameters according to your needs.

**Local Storage Configuration**

Configure the **Storage Location** for the attachments in exception reporting.

**Notification Time**

When the notification is enabled, patrol persons will receive notifications of the relevant patrol information via Mobile Client before patrols start. After it is enabled, you can edit the time by which the notification is advanced.

**Detection Frequency**

Set the **Detection Interval** at which the server detects the patrol route status.

**GIS Configuration**

Enable **GIS Map** so that you can configure patrol points on the GIS map.

**Note**

To use the basic functions of the GIS map, you need to subscribe to the Geocoding API, Maps JavaScript API, and Places API from Google Maps. If you want to search for geographic locations, you need to subscribe to the Geolocation API.

## 32.4 Add Patrol Points

Before you create a patrol route and start a patrol, you need to add patrol points. You can set access points as patrol points, or generate QR codes to be patrol points. The patrol persons have to check in at the patrol points to perform the patrol.

**Before You Start**

Make sure you have configuration permissions for patrol management and permissions for related resources.

**Steps**

1. 1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Patrol Management** → **Patrol Point** .
2. On the top left of the page, click **Add**.

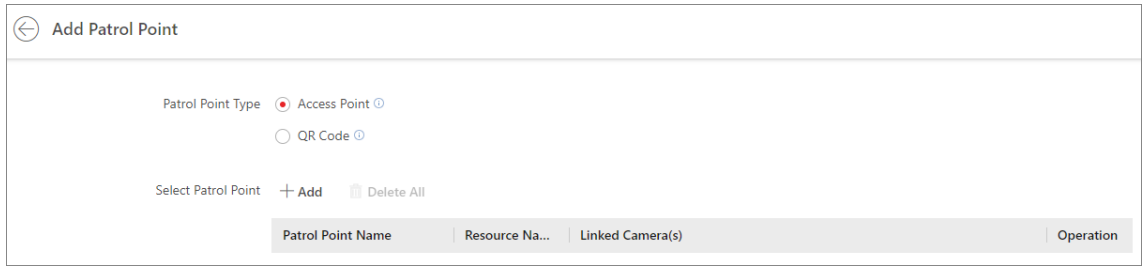



**Figure 32-5 Add Patrol Point**

3. Select the patrol point type and add patrol points of either type according to your needs.
   - Add Patrol Points of Access Point Type:

     Select **Access Point** as the **Patrol Point Type**, click **Add**, select card readers, and click **Add** to add the patrol points to the list. Click **Add** again to add more patrol points to the list.

     **Note**

     - Only one patrol point will be added for each card reader.
     - The patrol point name is generated automatically based on the resource name. You can edit the name if required.
   - Add Patrol Points of QR Code Type:

     Select **QR Code** as the **Patrol Point Type**, click **Add**, and enter the name for the patrol point to add the patrol point to the list. Click **Add** again to add more patrol points to the list.
4. Click **Link** and select camera(s) to link to the patrol point.

   **Note**

   No more than 4 cameras can be linked to each patrol point.
5. **Optional:** For patrol points of QR code type, you can turn on **GPS Verification** to set the valid patrol scope.

   You can set the valid patrol scope by searching for the location or by manually drawing a circle.

6. **Optional:** Click **Delete All** to delete all patrol points, or click to delete one patrol point.
7. Click **Save**.

   The added patrol points will be displayed on the patrol point list.
8. Perform the following operations according to your needs.

| | |
|---|---|
| **Filter Patrol Points** | On the top right of the page, click , set the conditions (patrol point name, patrol point type, linked cameras, resource, and area) according to your needs, and click **Filter**. |
| **Delete Patrol Points** | Select the patrol points to be deleted and click **Delete**. |
| **Edit a Patrol Point** | Click the name of a patrol point to enter the patrol point information page. You can edit the patrol point name and linked cameras. |
| **View Thumbnails of Camera Views** | In the Linked Camera(s) column, click to view the thumbnails of the latest views of the linked cameras. |
| **View/Download the QR Code of a Patrol Point** | For a patrol point of QR code type, click in the Patrol Point Type column to view and download the QR code. |
| **Enable GPS Verification** | For a patrol point of QR code type, turn on **GPS Verification** to enable the GPS verification. After this is enabled, patrols will be valid only if they are performed within this scope. |

## 32.5 Add Patrol Person Group

You can select persons to form a patrol person group and set a patrol mode for the group.

**Before You Start**

Make sure you have configuration permissions for patrol management and permissions to access the related person groups.

**Steps**

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Patrol Management** → **Patrol Person Group** .
2. Click **Add**.

**Note**

If you have already added a patrol person group before, click + on the top left of the page to add another one.

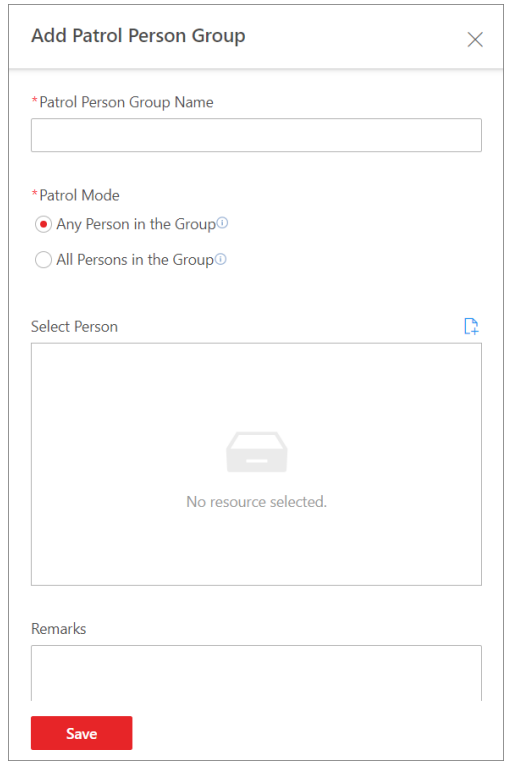



**Figure 32-6 Add Patrol Person Group**

3. Enter a name for the patrol person group.
4. Select a patrol mode.

   **Any Person in the Group**

   The patrol at a patrol point is performed when any person in the group checks in at the patrol point.

   **All Persons in the Group**

   The patrol at a patrol point is performed when all persons in the group check in at the patrol point.
5. Click to select persons to form the patrol person group.

**Note**

- No more than 100 persons can be selected for one patrol person group.
- You can also skip this step for now and add persons to the patrol person group later.

6. **Optional:** Enter remarks for the patrol person group.
7. Click **Save**.

**Note**

No more than 300 patrol person groups can be created for a system.

The added patrol person groups will be displayed on the left pane.

8. **Optional:** Perform the following operations according to your needs.

| | |
|---|---|
| **Edit a Patrol Person Group** | On the left pane, select a patrol person group and click on the top to open the Edit Patrol Person Group pane. You can edit the name, patrol mode, person(s), and remarks of the group accordingly. |
| **Delete Patrol Person Groups** | On the left pane, select a patrol person group and click on the top to delete the selected group. Click → **Delete All** to delete all patrol person groups. |
| **Search for Patrol Person Groups** | On the left pane, enter keyword(s) in the search box to search for patrol person groups. |
| **Add Persons to a Patrol Person Group** | Select a patrol person group and click **Add** to add patrol persons to the patrol person group. |
| **Search for Persons in a Patrol Person Group** | Select a patrol person group and enter keyword(s) in the upper-right search box to search for patrol persons in the patrol person group. |
| **Delete Persons from a Patrol Person Group** | Select a patrol person group, select the patrol persons to be deleted, and click **Delete**. You can also click → **Delete All** to delete all patrol persons from the group. |

## 32.6 Add Patrol Schedule Template

You need to set the schedule template first in order to schedule a patrol.

**Before You Start**

Make sure you have configuration permissions for patrol management.

**Steps**

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Patrol Management** → **Schedule Template** .
2. Click **Add Schedule Template**.

**Note**

If you have already added a schedule template before, click + on the top left of the page to add another one.

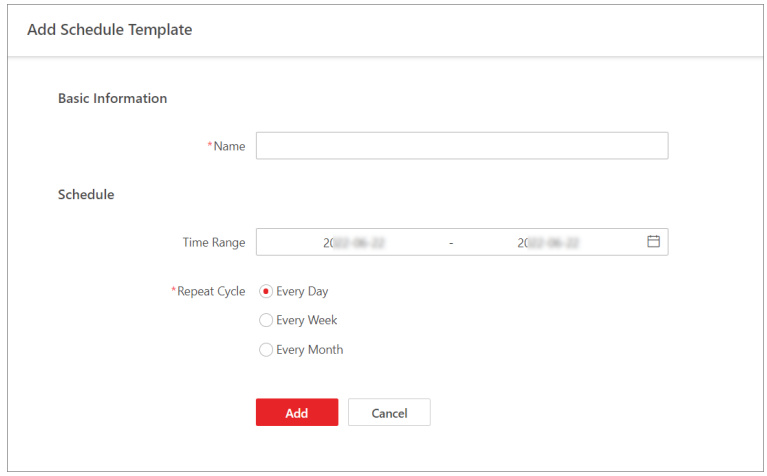



**Figure 32-7 Add Schedule Template**

3. Enter a name for the schedule template.
4. Set a validity period for the schedule template.
5. Choose a repeat cycle for patrol scheduling.

   **Every Day**

   Patrols will be scheduled for each day of the set time period.

   **Every Week**

   Patrols will be scheduled on the selected days of every week within the set time period.

   **Every Month**

   Patrols will be scheduled on the selected dates of every month within the set time period.
6. Click **Add**.

   The added schedule templates will be displayed on the left pane.
7. **Optional:** Perform the following operations according to your needs.

| | |
|---|---|
| **Edit a Schedule Template** | Select a schedule template and edit its configuration accordingly, including the name, time range, and repeat cycle. |
| **Delete a Schedule Template** | Select a schedule template and click **Delete**.<br>**Note**<br>Schedule templates cannot be deleted if being linked with shift schedules of a patrol route. |
| **Search for Schedule Templates** | On the left pane, enter keyword(s) in the search box to search for schedule templates. |

## 32.7 Add Patrol Route

To start a patrol, you need to create a patrol route. Set the patrol point(s), patrol pattern, patrol duration, and shift schedule(s) to form a complete patrol route.

**Before You Start**

- Make sure you have configuration permissions for patrol management and permissions to access the related patrol points and person groups.
- Make sure you have already added patrol points and patrol schedule templates to the system. For details about adding patrol points, see ***Add Patrol Points*** . For details about adding patrol schedule templates, see ***Add Patrol Schedule Template*** .

**Steps**

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Patrol Management** → **Patrol Route** .
2. Click **Add Route**.
3. Enter a name for the patrol route.
4. **Optional:** Enter remarks for the route.
5. Click **Save** to open the patrol route configuration page.

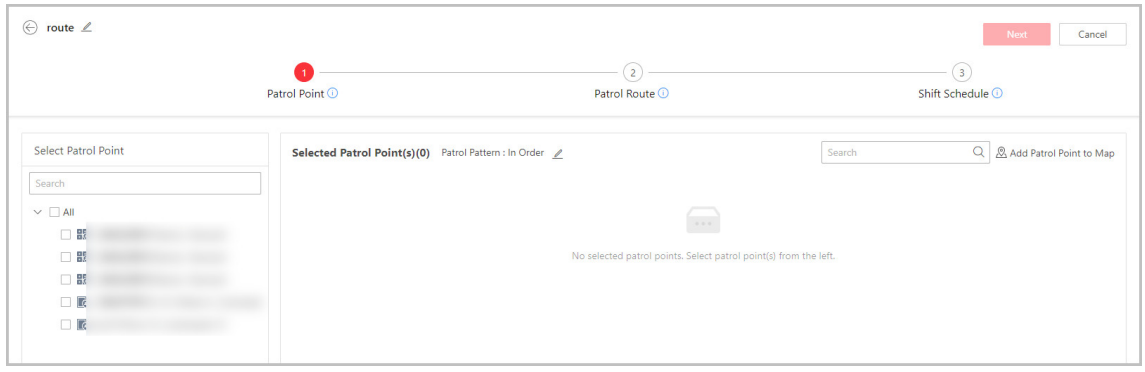



**Figure 32-8 Patrol Route Configuration Page**

6. Select the patrol point(s) that the patrol persons need to patrol on a route.
7. Click beside **Patrol Pattern: In Order** to set the patrol pattern for the route.

**Note**

- The patrol pattern is **In Order** by default.
- You can click ↑ and ↓ to rearrange the patrol list order as needed.

**In Order**

Patrol according to the order in the patrol list.

**No Order**

Patrol the patrol points on the route in no particular order.

**First Point First and Last Point Last**

Patrol the first patrol point on the patrol list at first and the last point on the list at last.

**First Point First**

Patrol the first patrol point on the patrol list at first.

**Last Point Last**

Patrol the last patrol point on the patrol list at last.

8. Click **Next**.

**Note**

If a patrol point has not been added to a map, you can click **Add Patrol Point to Map** and drag it onto a map. If there are points with GPS verification enabled, GIS map will be automatically selected for you to add points to it; otherwise, you will have to choose between **GIS Map** and **Static Map**.

9. Set the total patrol duration (in minutes) for the patrol route.
10. Set the time error and interval for patrolling the patrol points, and click **Next**.

**Note**

Time error and interval settings are for patrols of the "In Order" patrol pattern only.

**Time Error**

The time error allowed to pass a patrol point during actual patrol.

You can set a common time error for all patrol points, or set the time error for each patrol point individually by entering values in the table cells or the textboxes that appear when hovering over the Rule Preview pane.

**Interval**

The time interval of patrolling the current patrol point and the previous one.

You can set a common interval for all adjacent patrol points, or set each interval individually by entering values in the table cells or the textboxes that appear when hovering over the Rule Preview pane.

**Note**

The sum of all patrol intervals should be less than the set total duration of the patrol route.

11. Click **Add Schedule**.
12. Configure the parameters for adding a shift schedule.

**Name**

Enter a name for the shift schedule.

**Copied From**

If you have already added at least one shift schedule to the patrol route, you can select a shift schedule from the drop-down list to replicate its settings for schedule template and patrol person / patrol person group selection.

**Schedule Template**

Select a schedule template from the drop-down list.

**Patrol Start Time**

Set a start time for the patrol.

**Note**

The patrol time periods of shift schedules cannot overlap with one another.

**Patrol Person or Patrol Person Group**

Select persons or select an added patrol person group for the shift schedule. For details about adding patrol person groups, see ***Add Patrol Person Group*** .

13. Click **Add**.

**Note**

- If needed, click **Add Shift Schedule** again and repeat the step above to continue adding shift schedules. No more than 8 shift schedules can be added for a patrol route.
- You can edit an added shift schedule and delete one or delete all shift schedules according to your needs. The editing of a shift schedule will be applied to the route according to the time range and repeat cycle in the selected schedule template.

14. Click **Finish** to complete the patrol route configuration.
15. **Optional:** Perform the following operations according to your needs.

| | |
|---|---|
| **Switch Display Mode for Patrol Routes** | On the top right of the page, click to view the added patrol routes in calendar mode, or click to view them in list mode. For the calendar mode, you can switch among day, week, and month views. |
| **Filter Patrol Routes** | On the top right of the page, click , set the conditions (route name, patrol points, persons, patrol person groups, schedule templates, patrol route status, and time range) according to your needs, and click **Filter**. |
| **View Route Details** | Click the name of a route to enter its route details page. You can view information such as patrol points, patrol pattern, patrol duration, and shift schedules configured for the route. You can also view maps to which the patrol points of the route are being added. |
| **Edit a Patrol Route** | Click the name of a patrol route, and click **Edit Route** on the top right of the page to enter the route configuration page. You can edit the route settings such as patrol points, patrol pattern, patrol duration, and shift schedules. |
| **Disable Patrol Routes** | Select the routes to be disabled and click **Disable Route**. |
| **Enable Patrol Routes** | Select the routes to be enabled and click **Enable Route**. |

| | |
|---|---|
| **Delete Patrol Routes** | Select the routes to be deleted and click **Delete**. |

## 32.8 Real-Time Patrol Monitoring

You can monitor the patrol status in real time via map or list, to conveniently know whether an exception occurs during the patrol, which helps handling the exception in time.

**Note**

Make sure you have the operation permission for patrol monitoring.

On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Real-Time Monitoring** . On the patrol monitoring page, you can view the real-time status of patrol routes and information about real-time events related to the patrols.

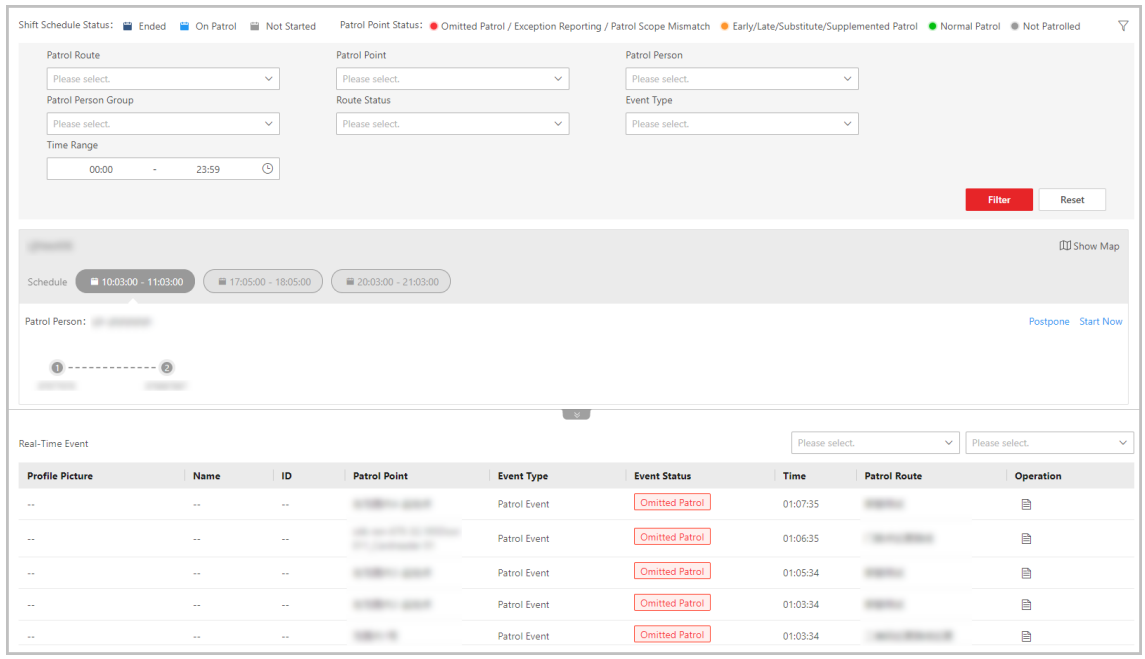



**Figure 32-9 Real-Time Monitoring Page**

### Patrol Route Status

The real-time status of all enabled patrol routes with shifts scheduled for the current day are displayed by default. You can filter the routes by clicking on the top right of the page and setting the filter criteria (e.g., patrol route, patrol point, patrol person / patrol person group, route status, event type, and time range).

Information such as the route name, patrol person / patrol person group, scheduled time period for each shift, and a list of patrol points are displayed for each patrol route. The shift schedule status (e.g., ended, on patrol, and not started) and patrol point status (e.g., omitted patrol /

exception reporting, patrol scope mismatch, early patrol, late patrol, substitute patrol, supplemented patrol, normal patrol, and not patrolled) are indicated with different colors with respect to the legends on the top of the page.
You can click a patrol point already being patrolled to view its status and the related patrol event information. You can also hover over a shift to view its status and detailed information. If needed, you can manually start or postpone a shift not started yet by selecting the shift schedule and clicking **Start Now** or **Postpone** respectively.
For patrol routes with patrol points that have been added to maps, you can also click **Show Map** to switch to monitoring the patrol status in real time via maps.

### Real-Time Event

The patrol monitoring page also supports showing information about real-time patrol-related events (e.g., patrol events, exception reporting, and patrol scope mismatch), including the patrol person information (e.g., profile picture, name, ID), event information (e.g., event type, event status), patrol information (e.g., patrol point, valid patrol scope, patrol route, shift schedule, scheduled/actual patrol time, and planned/actual patrol person), and related video/picture files and attachments.

**Note**

The actual information displayed may vary depending on the event type and patrol status.

You can filter the real-time events by event type and view details about each event by clicking in the Operation column.

## 32.9 Search for Patrol-Related Event Records

You can search for and export patrol-related event records, including patrol events and exception reporting.

**Before You Start**

Make sure you have the operation permission for patrol search.

**Steps**

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Search** → **Event Record Search** .

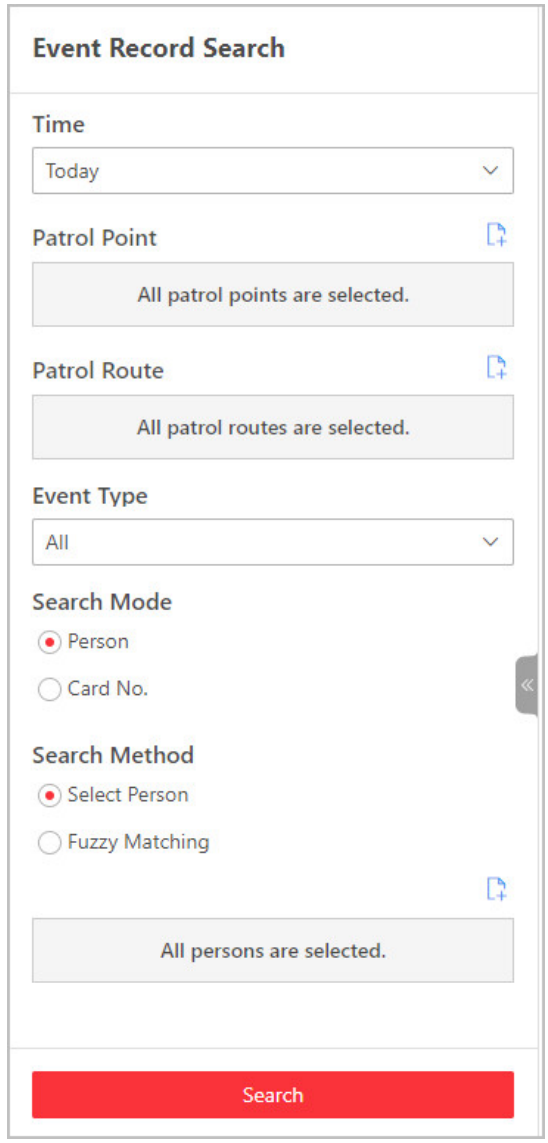



**Figure 32-10 Event Record Search**

**2.** Set the search conditions.

**Time**

Select from **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, and **Last 30 Days**, or set a custom time interval of no more than 31 days.

**Patrol Point**

By default, all patrol points are selected. Click to select certain patrol point(s) to filter the search results.

**Patrol Route**

By default, all patrol routes are selected. Click to select certain patrol route(s) to filter the search results.

**Event Type**

By default, all patrol-related event records will be searched. Select **Patrol Event**, **Exception Reporting**, or **Patrol Scope Mismatch** from the drop-down list to search for the specified type of event records only.

**Search Mode**

Choose whether to search for the event records by **Person** or **Card No.**.

- Search by person: In the **Search Method** field, choose whether to search by person selections or fuzzy matching of persons' names.
- Search by Card No.: Enter the card No. in the search box.

3. Click **Search**.

The matched records will be shown on the right side of the page.

4. **Optional:** Perform the following operations according to your needs.

| | |
|---|---|
| **View Details of an Event Record** | In the Operation column of an event record, click to view detailed information about the record.<br>• For a patrol event, you can view the event information (e.g., patrol status), patrol information (e.g., patrol point, valid patrol scope, patrol route, shift schedule, scheduled/actual patrol time, and planned/actual patrol person) depending on the patrol status, and videos/pictures related to the patrol.<br>• For an exception reporting, you can view the event information (e.g., exception type and description), patrol information (e.g., patrol point, patrol route, and patrol person), and the file(s) attached to this exception reporting. |
| **Export an Event Record** | In the Operation column of an event record, click to export the record. |
| **Export All Matched Event Records** | On the top right of the result page, click **Export** to export all matched results. You can choose whether to export in XLSX format or CSV format, and whether to export the event records with picture. |

## 32.10 Check Patrol Statistics

You can filter, check, and export patrol statistics by patrol route, patrol point, and patrol person.

**Note**

Make sure you have the operation permission for patrol search.

On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Search** → **Patrol Statistics** to enter the patrol statistics page.

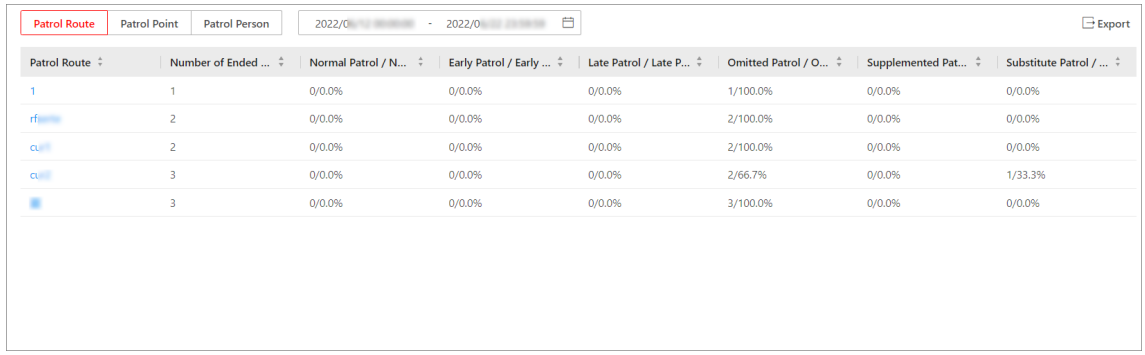



**Figure 32-11 Patrol Statistics Page**

You can select the type of patrol statistics to be displayed from **Patrol Route**, **Patrol Point**, and **Patrol Person**, and filter the results by specifying a time range. Information such as the number of shift schedules, number of patrols of a certain status (e.g. normal patrol, early patrol, late patrol, omitted patrol, supplemented patrol, and substitute patrol), and the percentage of each status will be displayed in a table. If needed, you can export the patrol statistics in either XLSX format or CSV format.

You can click the name of a patrol route, patrol point, or patrol person to view detailed information about each patrol in a list, including the patrol status, scheduled start time, actual start time, scheduled and actual patrol duration, shift schedule, and the person who performed the patrol. You can filter the patrol records by status and export the statistics in either XLSX format or CSV format.

# Chapter 33 Commercial Display Management

In the Commercial Display module, you can use digital signage related functions and centralized device control functions. Digital signage management includes managing contents, schedules, release, materials, etc. You can select a proper method to create contents according to actual needs and set schedules to release the contents to the specific devices. The contents should be reviewed before they are released and played on the devices according to the configured schedule. Centralized device control management includes controlling digital signage terminals and interactive flat panels, managing applications, viewing flat panel usage statistics and other playing statistics.

In the top left corner of Home page, select → **Integrated Service** → **Commercial Display** .

## 33.1 Commercial Display Overview

The following is the overview of the Commercial Display module.

On the left, select **Overview**.

### Centralized Device Control

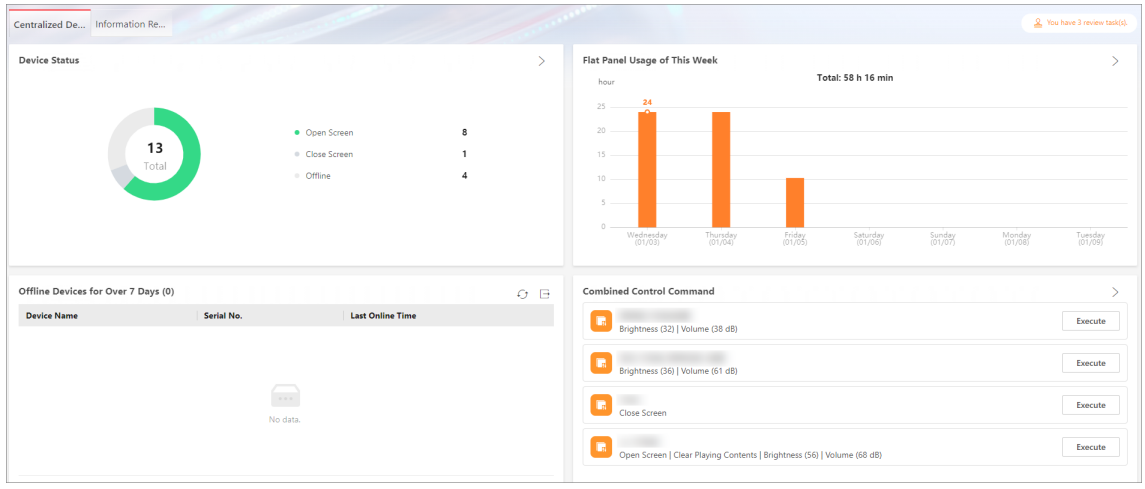



**Figure 33-1 Centralized Device Control**

The central device control mode supports viewing device status, flat panel usage of the this week, offline devices for over 7 days, and combined control command. You can also click › to go to the Device Control page or Flat Panel Usage Statistics page for details. In the Offline Devices for Over 7 Days area, you can refresh the list or export the information about the devices.

### Information Release

In the Wizard area, click an application to perform the corresponding task.

Below the Wizard, Quick Release, Release by Template, and Material Library are displayed.

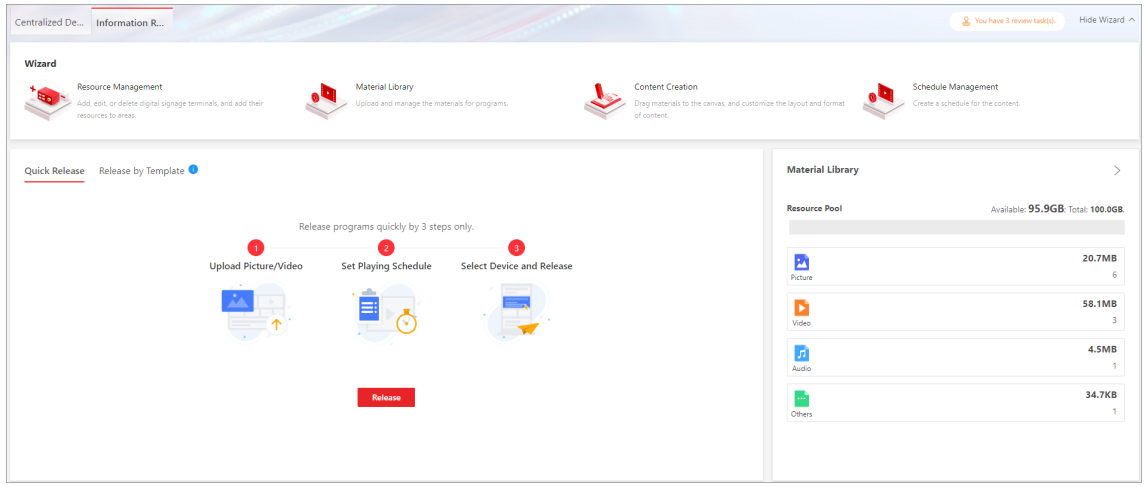



**Figure 33-2 Information Release**

## 33.2 Flow Chart of Digital Signage Management

You can follow the flow chart below for using the digital signage module for the first time.

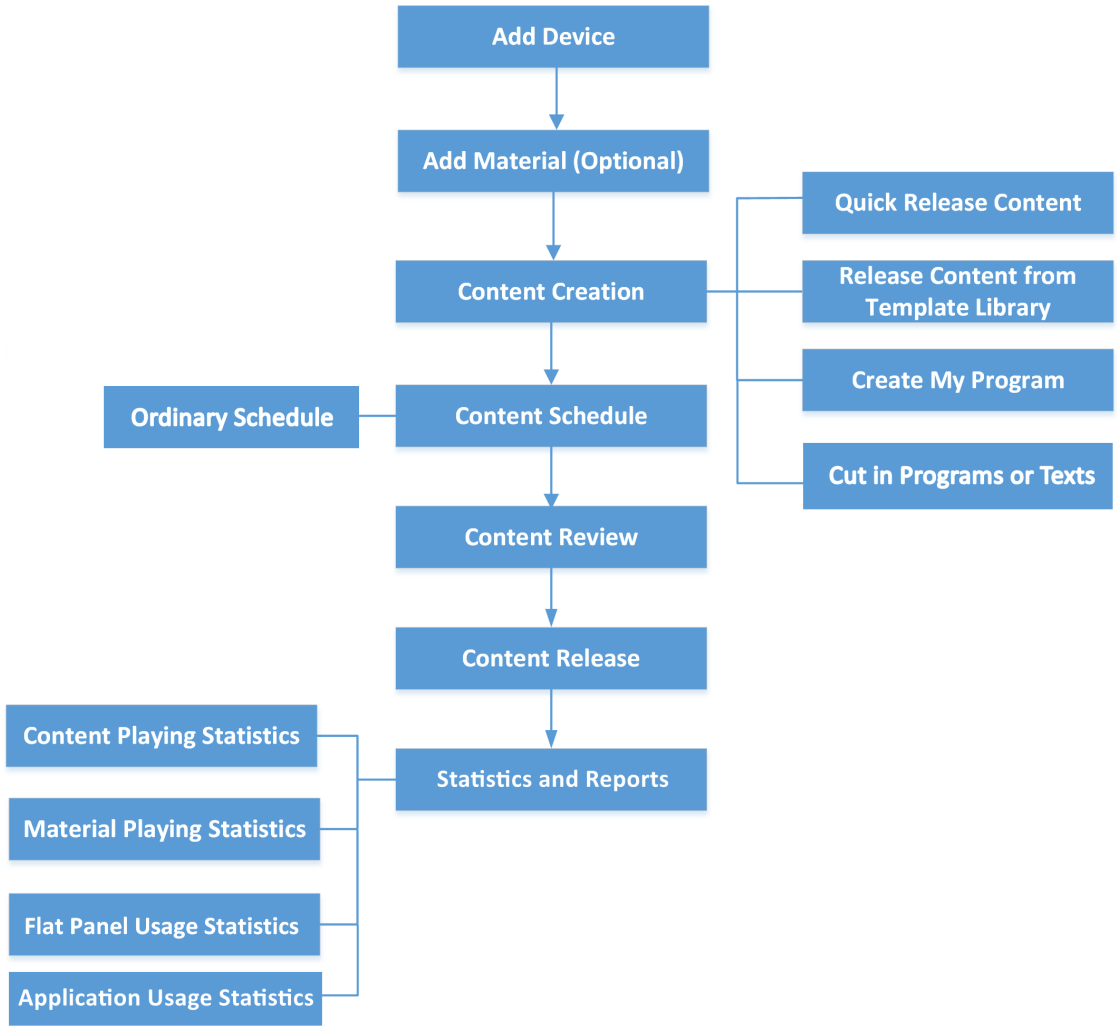



**Figure 33-3 Flow Chart of Digital Signage Management**

- **Add Device**: You should add devices to the platform.
- **Add Material**: Material is used for creating programs. You can upload materials to the platform. For details, refer to ***Material*** .
- **Content Creation**: You can quickly release content, use template libraries, create programs, or cut in programs/texts as needed. For details, refer to ***Content*** .
- **Content Schedule**: You can create an ordinary schedule for the added programs, which will then be played according to the scheduled time or method on the terminals. For details, refer to ***Create an Ordinary Schedule*** .
- **Content Review**: The added contents should be reviewed before they are used. For details, refer to ***Review*** .

- **Content Release**: You can view release records of all the tasks and the details of their release status. For details, refer to ***View Release Records*** .
- **Statistics and Reports**: You can view statistics of content playing, material playing, application usage and flat panel usage. For details, refer to ***Statistics and Reports*** .

## 33.3 Content

The platform supports creating contents and releasing them to selected devices. Then the contents can be played on the devices to function as prompts, notices, etc. According to actual needs, you can select from three entries/methods to create contents, namely, quick releasing contents, creating contents from template library, and creating my programs. When creating contents via the latter two entries/methods, you can customize the layout of the program, add materials to the program, preview the program, etc. You can also cut in specific programs or text messages on specific devices according to the scheduled time.

### 33.3.1 Quickly Release Content

You can quickly release contents by selecting device type(s), selecting material(s) from local PC or material library, setting the content playing schedule, setting the release mode, and selecting device(s) to release the contents.

**Before You Start**
Make sure you have added device(s) to the platform. For details, refer to ***Device and Server Management*** .

**Steps**
1. On the left, select **Content Creation**.
2. Click **Quick Release** on the left to enter the Quick Release page.

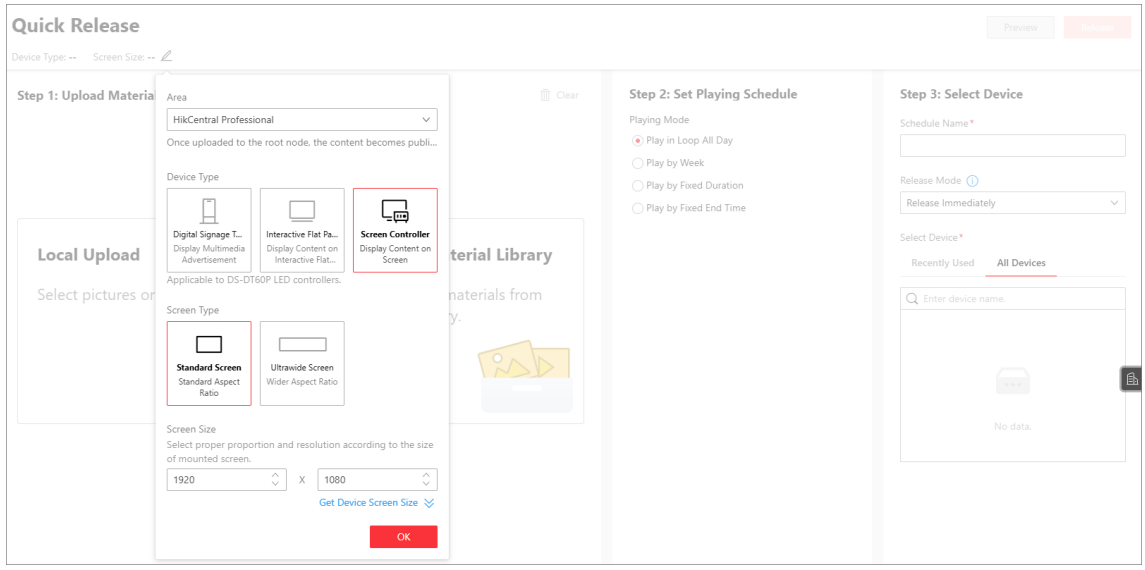



**Figure 33-4 Quick Release Page**

3. Select the area, device type, screen size, and click **OK**.
4. Upload the material(s).
   - Click **Local Upload**, and select picture(s) and/or video(s) form local PC.
   - Click **Select from Material Library**, select an area from the drop-down list, and select material(s) from the Material Library.

**Note**

- For the selected material, move the mouse cursor to it and you can click **Edit** to edit the material size, or click **Delete** to delete the material. You can also click **Clear** to delete all the selected materials.
- On the editing material page, you can check **Show Original Aspect Ratio** to view the material in its actual proportion (only picture material supports). After resizing the material, you can click **Reset** to revert the material size to its original size.

5. Set the playing schedule.
   1) For multiple uploaded materials, drag them to adjust the playing order, and set the switching effect as **Gradient** or **None**.
   2) Set the playing duration for picture materials.
   3) Set the playing schedule as **Play In Loop All Day**, **Play by Week**, **Play by Fixed Duration**, or **Play by Fixed End Time**.
6. Select the device(s) to release the content.
   1) Enter the task name.
   2) **Optional:** Select the release mode as **Release Later**, or select **Release Immediately** and set the release time.
   3) **Optional:** Switch on **Device Sync Playing** (for digital signage terminals only).

**Note**

Make sure you have enabled the time synchronization of NTP server. See details in ***Set NTP for Time Synchronization*** .

4) Select device(s) from recently used devices or all devices.

7. Click **Release** to start releasing the content.
8. **Optional:** Click **Preview** to preview the content.

## 33.3.2 Manage Template Library

The platform provides multiple templates which can be used in different application scenarios such as chain retail and financial bank. You can preview the template, add it to My Template, and select a template and then start creating the content.

Select **Content Creation → Template Library** on the left.

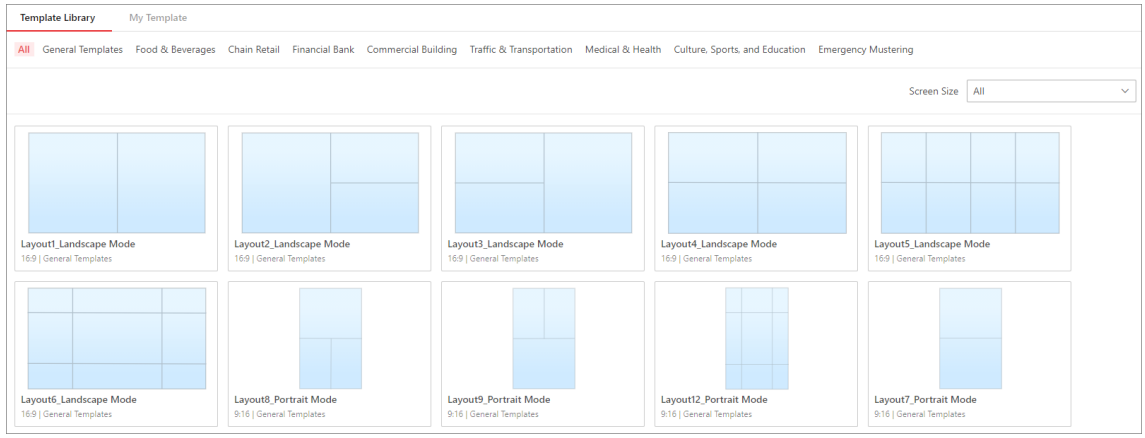



**Figure 33-5 Template Library**

You can perform the following operations.

- Filter templates by template type or screen size.
- Hover over a template and click **Preview** to preview the template.

**Note**

You can click **Emergency Mustering** and select a template for creating the emergency mustering program. After being created, the program will be played on the device when the emergency is triggered.

- Hover over a template, and click **Add to My Template** to add it to My Template. On the My Template page, you can also filter and preview the templates, and remove them from My Template.
- Hover over the target template, and click **Create** or click **Preview → Create Program** to enter the creating content page.

## Add Emergency Mustering Text Notification

You can add emergency mustering text notifications on the platform by configuring related parameters, and the added text notifications will be displayed on the digital signal terminals when the emergency is triggered.

**Before You Start**

Make sure you have added devices to the platform.

**Steps**

**Note**

For one device, only the latest added text notification can be displayed.

1. On the left, select **Content Creation → Template Library** .
2. Click **Emergency Mustering** on the top.
3. **Optional:** Click **Emergency Solution Settings** to enter Emergency Mustering module and view emergency solution settings.

   **Note**

   For details, refer to ***Add Emergency Solution*** .
4. Move the mouse cursor to the template of Text Notification for Emergency, and click **Create** to enter the adding text notification page.
5. Set the needed parameters, including text notification name and content.
6. Select an area and check device(s) under the area.

   **Note**

   Only the latest text notification can be displayed on one device. Therefore, if you select a device which has already been configured with a text notification, the previous text notification will be invalid and will not display any more.

   The text notification will be displayed on the selected devices.
7. Click **Release**.

   **Note**

   The text notification is released and will be displayed when the emergency is triggered.

   You can view the release status on the right side of the page.
8. **Optional:** Perform the following operations.

| | |
|---|---|
| **View Text Notification in List/Thumbnail Mode** | Click / to view the added text notifications in the thumbnail mode or in the list mode. |

| | |
|---|---|
| **Copy Text Notification** | Move the mouse cursor to a text notification, and click **Copy** to enter the adding text notification page. A new text notification which is of the same content as the original one will be displayed. You can edit the content before releasing the new text notification, or click **Release** to release the current text notification directly.<br>**Note**<br>If you do not reselect device(s) for the new text notification, the previous text notification(s) configured on the device(s) will be invalid and will not display any more. |
| **View Device Release Details** | Move the mouse cursor to a text notification, and click **Device Status** to view release details of the text notification on the device. |
| **Share / Cancel Sharing Text Notification** | Select one or more text notifications, click **Share** or **Cancel Sharing** to set the sharing property of text notifications as **Public** or **Private**.<br>**Public**<br>All users in the current organization (i.e., the organization where the user who adds the text notification belongs to) and the higher-level organizations can see the text notification.<br>**Private**<br>All users in the current organization (i.e., the organization where the user who adds the text notification belongs to) can see the text notification. |
| **Search for Text Notification** | In the upper right corner, enter keywords in the search box to search for the text notification(s). |
| **Refresh List** | Click **Refresh** to refresh the text notification list. |
| **Delete Text Notification** | Check one or more text notifications, and click **Delete** to delete the selected text notifications. |

### 33.3.3 Create My Program

The platform supports creating and displaying content on digital signage terminals (single-sided screens and display walls), interactive flat panels, screen controllers (standard screens and ultrawide screens). When creating the program, you can select the needed materials and design the layout. After creating the programs, you can perform more operations such as previewing, releasing, and filtering programs.

On the left, select **Content Creation → My Program → Add** .

## Create A Program

Configure basic program parameters such as name, area, device type, screen type, etc.

**Area**

If you select the root area, the content will be visible to all users.

**Device Type**

For ultrawide screen programs, the video format and max. resolution of are as follows.

**Table 33-1 Ultrawide Screen Program**

| Video Format | Max. Resolution |
|---|---|
| MP4 | 16384 |
| MKV | 32768 |
| ASF | 32768 |
| MPG | 4095 |
| 3GP | 2048*1152 |
| MOV | 16384 |
| WMV | 32768 |
| FLV | 32768 |

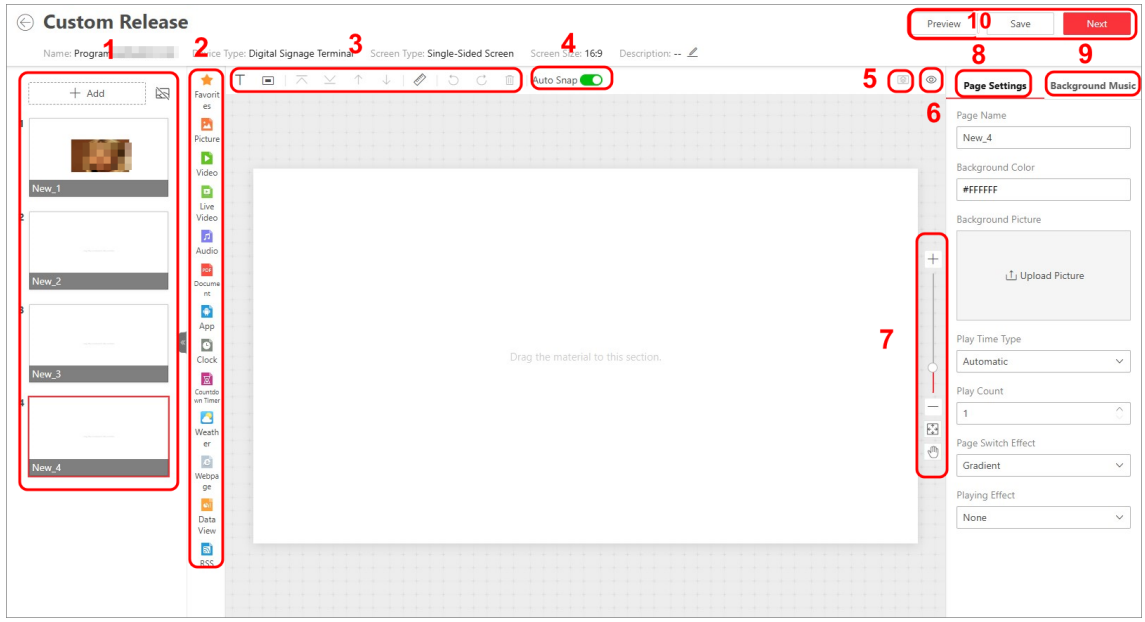



**Figure 33-6 My Program**

**Table 33-2 Description**

| Number | Description |
|---|---|
| 1 | • Click to show thumbnail and click to hide it.<br>• Drag the page to change the page order.<br>• Hover over a page and click to copy or delete it. |
| 2 | Drag multiple types of materials to pages.<br>Select a material and set window properties, including micro animation, window position, window type, switching method, etc. Some display effects may be invalid for devices not supported.<br>**Weather**<br>Make sure you have configured the weather web manufacturer. See ***Set Weather Web Manufacturer*** . |
| 3 | Supports text insertion, in-window layer management (move up/down/bring to front/send to back), ruler display, and undo/redo operations. |
| 4 | **Auto Snap**: If enabled, two windows will be connected when they are near enough. |
| 5 | **Window Layer**: View the number of current window layers and what each layer is. |
| 6 | : Preview the content of the current page.<br>**Preview**: Preview the program. |
| 7 | Perform zoom, pan, and other adjustment operations on the current canvas. |
| 8 | Edit page settings, including page name, background, play time type, playing effect, etc. |
| 9 | **Upload**: Upload the background music from the local PC or Material. After uploading, you can enable the background music, which will be played on the current page. |
| 10 | Preview, save, or schedule release of the program. For scheduled release, see ***Create a Cut-In Schedule*** and ***Create an Ordinary Schedule*** . |

## Operations on the Program List

After creating programs, you can move, share, edit, preview programs, etc on the program list.

**Share Program**

Select one or more programs, click **Share** to set the sharing property of programs as **Public** or **Private**.

**Abnormal Program**

When hovering over an abnormal program ⚠ :

- Supports replacing or deleting expired materials.
- Supports deleting or re-editing the empty program.

## 33.4 Schedule

You can create a schedule and define a playing schedule to play the added programs on the devices according to the scheduled time or method. The platform supports two types of schedules: ordinary schedule and cut-in schedule. When creating schedules, you can select the needed programs and device(s) to release the programs. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, and filtering.

On the left, select **Schedule Management**.

### 33.4.1 Create an Ordinary Schedule

You can create an ordinary schedule to play the added programs on the devices according to the scheduled time or method. The platform supports loop schedule, default schedule, or you can customize your schedule and play the programs by day or by week. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, etc.

**Before You Start**

- Make sure you have added program(s) to the platform. For details, refer to ***Create My Program*** .
- Make sure you have added device(s) to the platform.

**Steps**

1. On the left, select **Schedule Management → Ordinary Schedule → Add** .

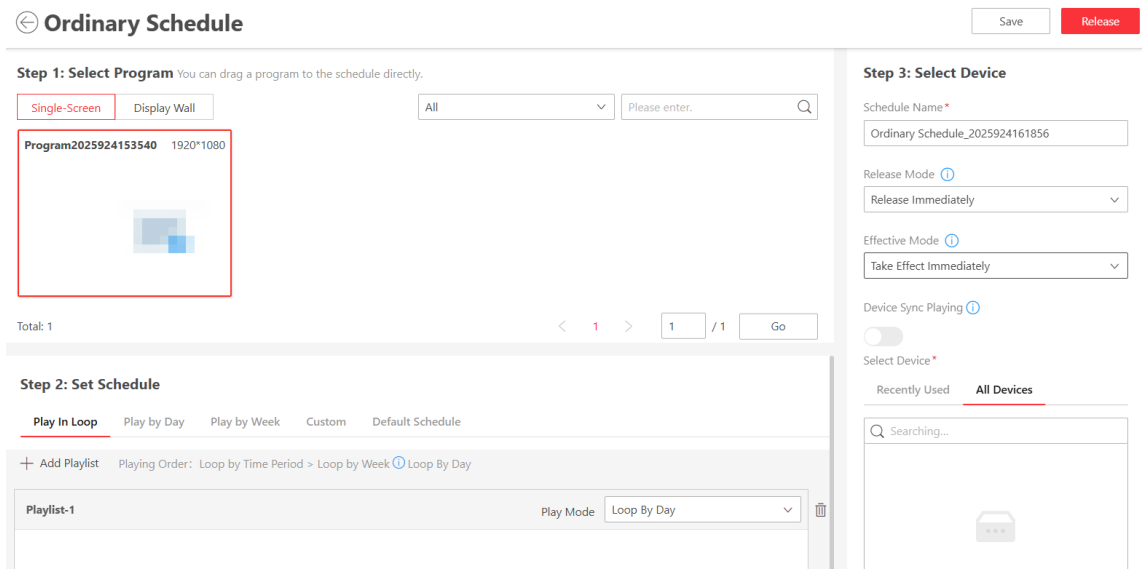



**Figure 33-7 Ordinary Schedule**

**2.** Select a program and set the schedule for it.

**Play In Loop**

a. Select a program in the program list and drag the program to the playlist.

**Note**

You can click **Add Playlist** to add more playlists as needed. Up to 8 playlists can be added, and up to 16 programs can be added to a single playlist.

b. Set the play mode as by day, by week, or by time period.

- **Play by Day**
- **Play by Week**
- **Custom**

Play the program according to a daily/weekly/custom schedule.

a. Select a program from the program list and drag to the desired location on the timeline.

**Note**

You can add multiple programs to one day. When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

b. Adjust the playing time of program(s).

c. Click on the right side of the timeline or **Delete All** to delete one or all the selected programs.

**Default Schedule**

Play the default content automatically when no contents are scheduled on the device.

Select a program in the program list, and drag the program to the playlist.

**3.** Save or release the ordinary schedule.

**4. Optional:** You can perform the following operations.

| | |
|---|---|
| **Edit Schedule** | Click the schedule name to enter Ordinary Schedule page and you can edit the schedule information. |
| **Share / Cancel Sharing Schedule** | Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**. |
| **Release Schedule** | Click in the Operation column to open the Schedule Releasing window. |
| **Export Schedule** | Hover over a schedule and click in the Operation column, and select the saving path to export the selected schedule to the local PC. |
| **Filter Schedules** | In the upper right corner, select one or more play modes, or enter keywords in the search box to filter the schedules which meet the conditions.<br>You can check Empty Schedule to filter empty schedules. You can delete or re-edit them. |

## 33.4.2 Create a Cut-In Schedule

You can create a cut-in schedule to cut in the specific programs or text messages on the specific devices according to the scheduled time. The cut-in programs or text messages will precede other contents. After creating schedules, you can perform more operations such as editing, releasing, searching, etc.

**Before You Start**
Make sure you have added program(s) and device(s) to the platform.

**Steps**
1. On the left, select **Schedule Management → Cut-In Schedule** .
2. Click **Add** to enter the Cut-In Schedule page.

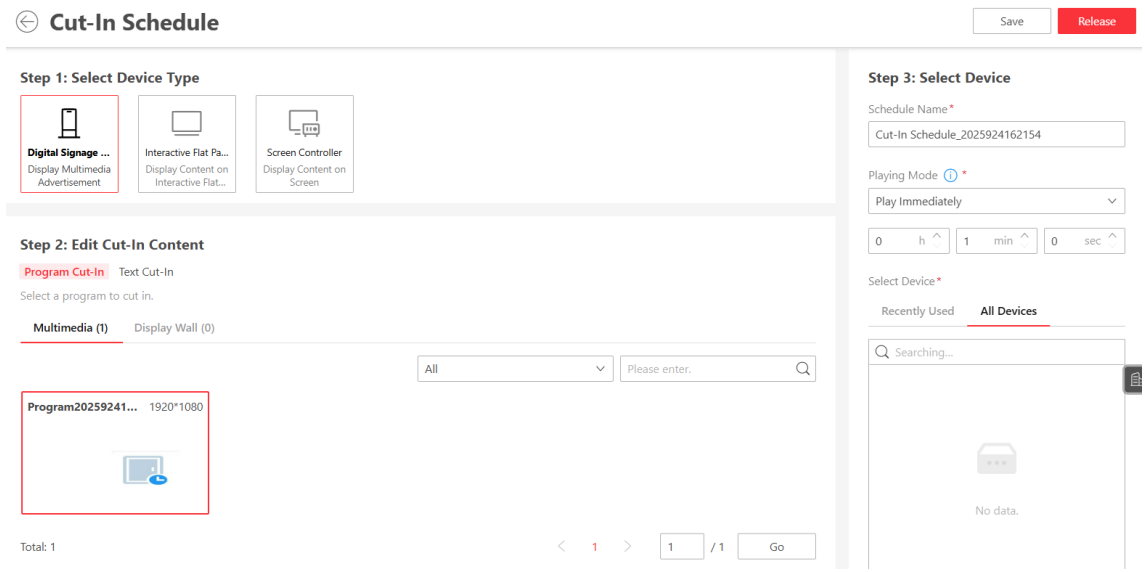



**Figure 33-8 Cut-In Schedule Page**

3. Select **Digital Signage**, **Interactive Flat Panel**, or **Screen Controller** as the device type.
4. Select the cut-in content.
   - Cut in a program: Click **Program Cut-In**, and select a program.
   - Cut in the text message:
     a. Click **Text Cut-In**, and select the screen size as **Landscape Mode** or **Portrait Mode**.

     **Note**

     For the interactive flat panel, you can check **Notification Sound**. A notification sound will be played when the text is released.

     b. In the Edit Text Message area, set the content and the corresponding play time.

     **Note**

     The play time for different text messages can be overlapped. You can click in the Operation column to view the playing effect of the current text message on the left side of the page.

     c. Set the configuration mode, front size and color, background, etc., for the text message.
5. Select the device(s) to release the content.

   Switch on **Device Sync Playing** (for digital signage terminals only).

   **Note**

   Make sure you have enabled the time synchronization of NTP server. See details in ***Set NTP for Time Synchronization*** .
6. Save or release the cut-in schedule.
7. **Optional:** Perform the following operations if you save the schedule in the previous step.

| | |
|---|---|
| **Edit Schedule** | Click the schedule name to enter Cut-In Schedule page and you can edit the schedule information. |
| **Share / Cancel Sharing Schedule** | Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**. |
| **Release Schedule** | Click in the Operation column to open the Schedule Releasing window. |
| **Filter Schedule** | In the upper right corner, select the playing mode, or enter keywords in the search box to filter the schedules which meet the conditions.<br>You can select **Empty Schedule** to filter empty schedules. You can delete or re-edit them. |

### 33.4.3 View Release Records

You can view release records of all the tasks and the details of their release status.

On the left, select **Schedule Management → Release** .

- In the Operation column, you can click to view release details or to release the task that failed to be released.
- For tasks failed to be released due to network or electricity disconnection, they can continue to be released within the effective period (48 hours) if connected to the network or electricity again.

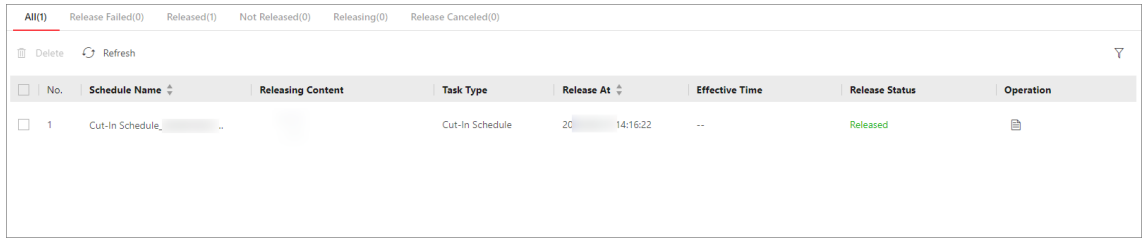



**Figure 33-9 View Release Records**

## 33.5 Review

The added contents should be reviewed before they are used. After being reviewed, the contents can be released automatically. You can review items individually or in batches.

On the left, select **Review Management**.

**Note**

- The contents created by the user who has the review permission can be released directly, otherwise the contents should be reviewed by the user who has the review permission.
- Review records containing empty programs/schedules cannot be approved.

## 33.6 Material

Material is used for creating programs. The platform supports various types of materials to meet different program requirements. You can upload local materials (such as picture and video) and other materials (such as webpage and picture URL) to the platform. After uploading the materials, you can mange materials including editing, searching, replacing, etc.

**Note**

On the left, select **Material Library** to enter the Material Library page.

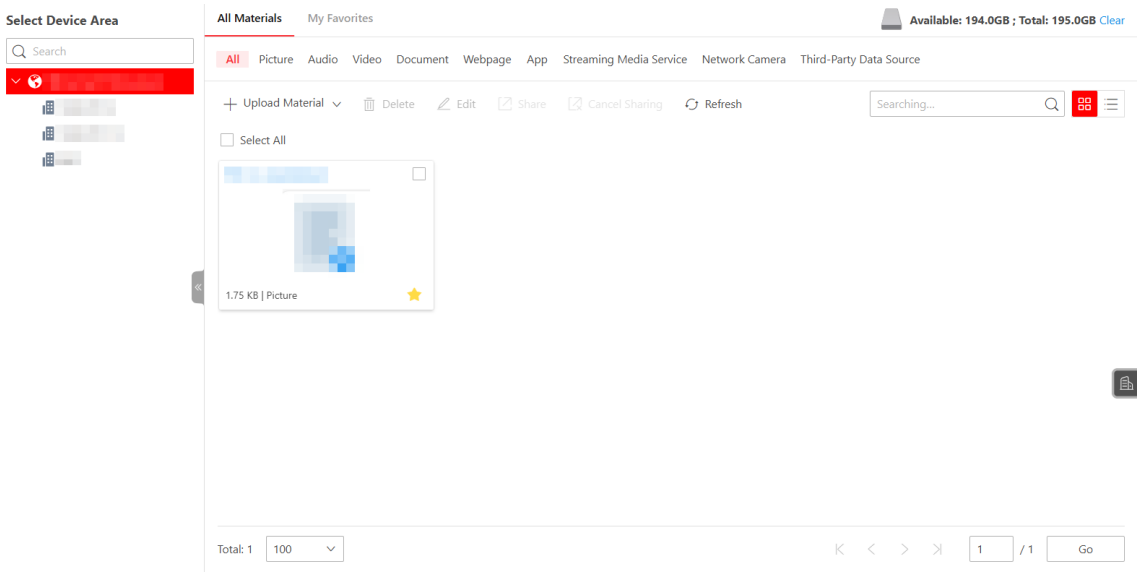



**Figure 33-10 Material**

### 33.6.1 Upload Materials

You can upload materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, webpage, network picture, stream media server, network camera, etc. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

**Steps**

1. On the left, select an area.
2. Click **All → Upload Material** to select the uploading mode. Or select a material type to perform operations.

**Table 33-3 Operations about Supported Material Types and Formats**

| Material Type | Format | Operation |
|---|---|---|
| Picture | BMP, JPG, PNG, GIF, JPEG | • Click **All / Picture → Upload Material → Create URL Picture Material** , enter the name, URL of the picture, and select areas.<br>• Click **All / Picture → Upload Material → Local Upload (Picture / Audio / Video / Document / Web Page / App) / Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails). |
| Video | ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4 | • Click **Video / Audio / Document / App → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).<br>• Click **All → Local Upload (Picture / Audio / Video / Document / Web Page / App)** , and follow the above steps. |
| Audio | MP3, WAV, WMA | |
| Document | PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX | |
| App | APK | |
| Webpage | HTML, HTM | • Click **Webpage → Upload Material → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).<br>• Click **Webpage → Upload Material → Create Webpage Material** , enter the name, URL of the webpage, and select areas.<br>• Click **All → Upload Material → Local Upload (Picture / Audio / Video / Document / Web Page / App) / Create Webpage Material** and follow the above steps. |
| Streaming Media Service | / | • Click **Streaming Media Service → Create Material** to receive streams from the streaming media server.<br>• Click **All → Create Material of Streaming Media Service** and follow the above steps. |

| Material Type | Format | Operation |
|---|---|---|
| | | If you disable **Built-In Steaming Media Service**, you should enter the URL of the streaming media server.<br>If you enable **Built-In Steaming Media Service**, you should enter the IP address, port No., channel No., user name, and password of the network camera. |
| Network Camera | / | • Click **Network Camera → Create Material** to get video streams from network camera.<br>• Click **All → Create Network Camera Material** and follow the above steps.<br>You should enter the required information of network camera such as IP address, port No., and channel No. |
| Third-Party Data Source | / | • Click **Third-Party Data Source → Create Material** .<br>• Click **All → Create Material of Third-Party Data Source** and follow the above steps.<br>There are two types of data source: Auto-Push Data Source and Third-Party Database. If you select **Auto-Push Data Source**, you should enter data source ID and select the data type; If you select **Third-Party Database**, you should set the basic information of the third-party database, including data source ID, database type, encoding format of data interchange, database name, IP address, etc. |

**Note**

- A single material should be smaller than 4 GB. The names of any two materials cannot be the same.
- Up to 1,000 materials can be uploaded to the platform at a time. Up to 10,000 materials can be stored in the platform.
- For those materials that fail to be uploaded, click to upload again or click to replace the material. For those materials with the failure reason "duplicated material", you can replace the material or click **Close** to cancel uploading.
- If you set **Sharing Property** to **Public**, all users in the current organization (i.e., the organization where the user who creates the material belongs to) and the higher-level organizations can see and use the material. If you set **Sharing Property** to **Private**, all users in the current organization (i.e., the organization where the user who creates the material belongs to) can see and use the material.

### 33.6.2 Manage Materials in My Favorites

Click ☆ or ★ to add the material to **My Favorites** or remove it from **My Favorites**.

On the top, click **My Favorites** to view favorite materials.

## 33.7 Statistics and Reports

You can select devices and set conditions to search for the content playing statistics, material playing statistics, application usage statistics, and flat panel usage statistics. Also, you can export the search results to the local PC.

On the left, select **Statistics and Reports**. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

### Content Playing Statistics

Select **Content Playing Statistics** on the left.

Select a device, and the interface will display the programs and their specific playing durations for that device.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter a program name to filter your search results (fuzzy search supported).
- Click ⇅ to sort by playing duration.

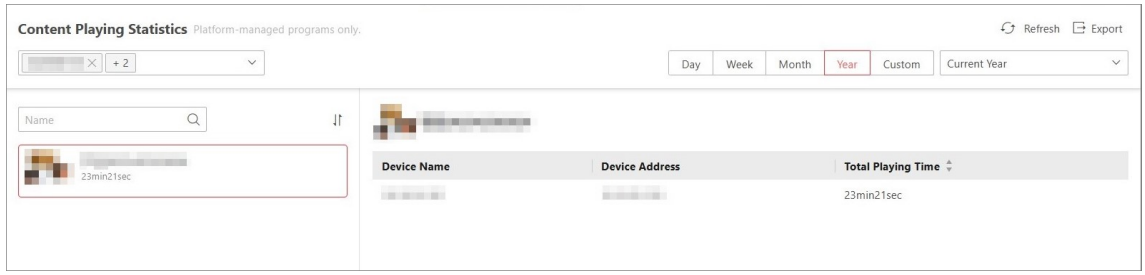



**Figure 33-11 Content Playing Statistics**

### Material Playing Statistics

Select **Material Playing Statistics** on the left.

Select a device, and the interface will display the materials and their specific playing durations and playing count for that device.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter a material name to filter your search results (fuzzy search supported).
- Click ⇅ to sort by playing duration.

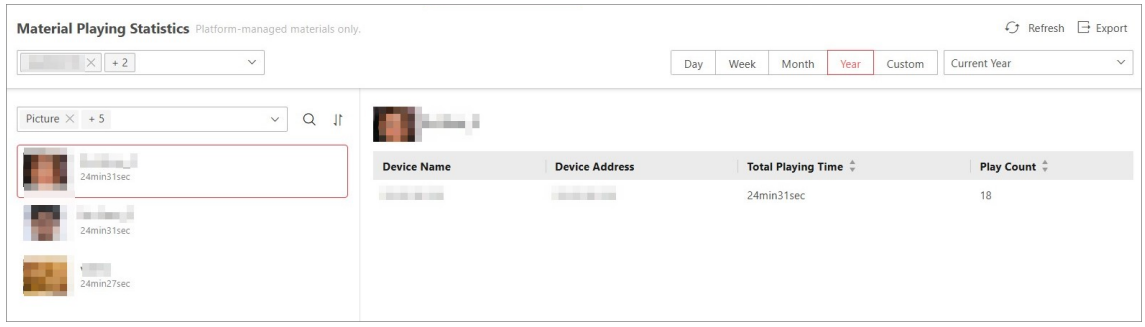



**Figure 33-12 Material Playing Statistics**

## Application Usage Statistics

Select **Application Usage Statistics** on the left.
Select a device or devices, and the interface will display the application list and their specific usage durations.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter an application name to filter your search results (fuzzy search supported).
- Click ⇵ to sort by usage duration.

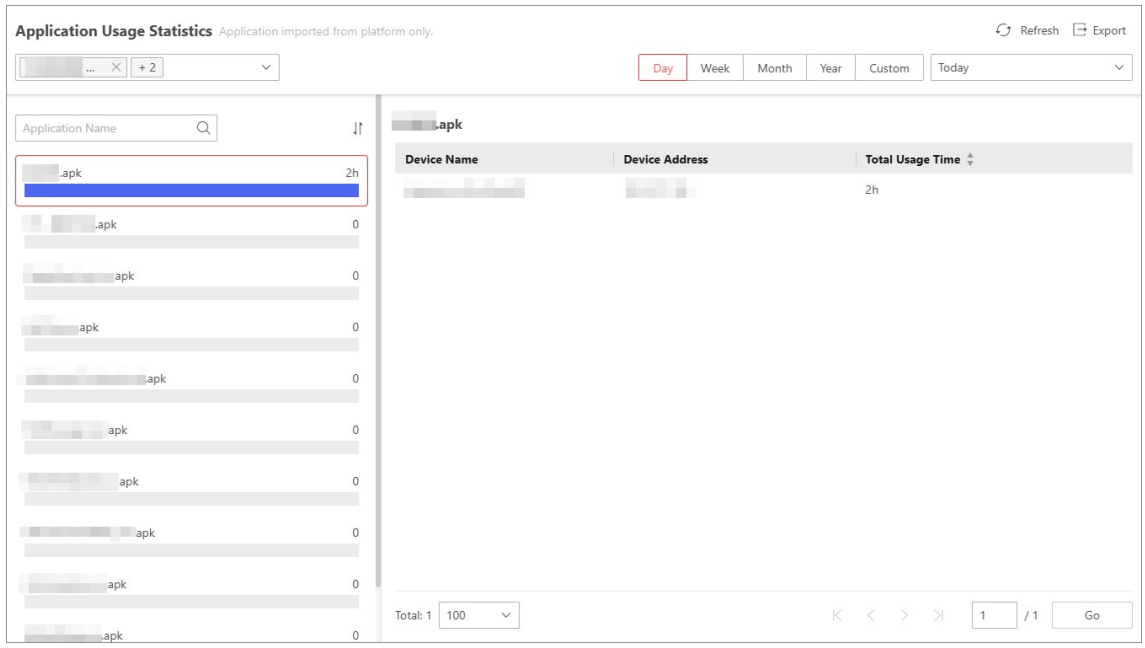



**Figure 33-13 Application Usage Statistics**

## Flat Panel Usage Statistics

Select **Flat Panel Usage Statistics**.
Select a device or devices, you will view the bar chart of usage time of each time period.
You can filter data by daily, weekly, monthly, yearly, or custom time periods.

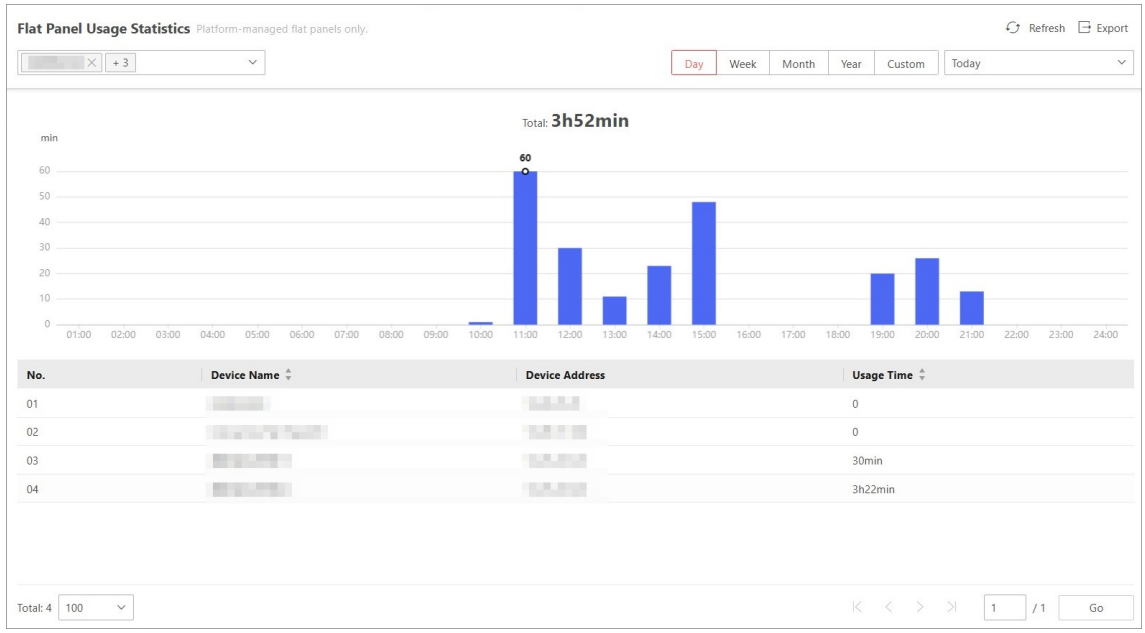
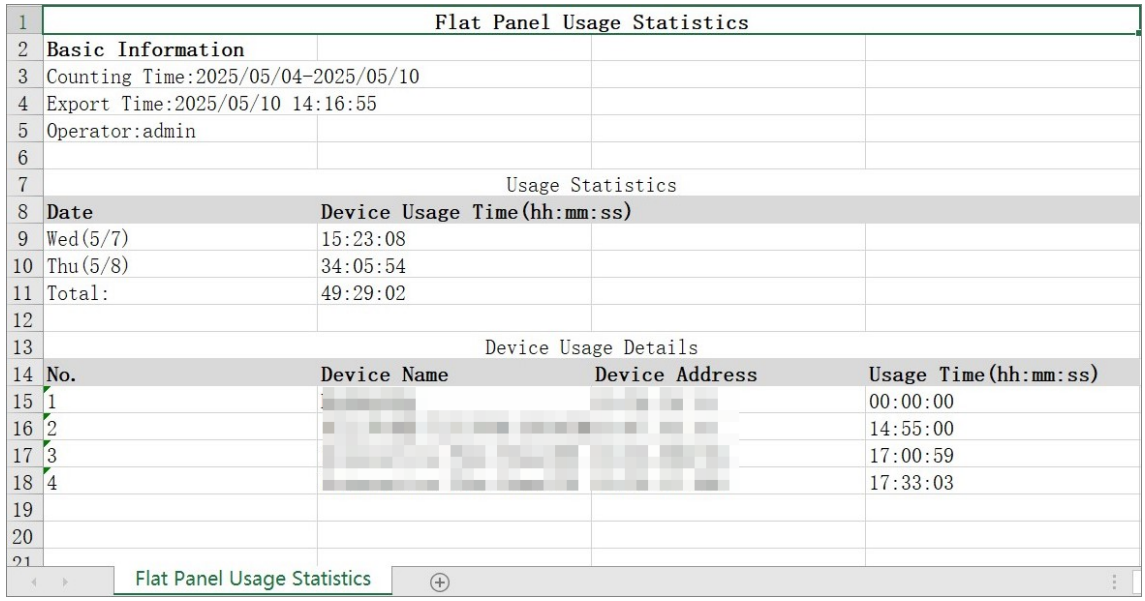



**Figure 33-14 Flat Panel Usage Statistics**

## Export Reports

After viewing the statistics, you can click **Export** in the upper right corner and select a file type to export the searched statistics to the local PC.

Take **Flat Panel Usage Statistics** as an example. The exported Excel file is as follows.



| | | | | |
|---|---|---|---|---|
| 1 | Flat Panel Usage Statistics | | | |
| 2 | Basic Information | | | |
| 3 | Counting Time:2025/05/04-2025/05/10 | | | |
| 4 | Export Time:2025/05/10 14:16:55 | | | |
| 5 | Operator:admin | | | |
| 6 | | | | |
| 7 | Usage Statistics | | | |
| 8 | Date | Device Usage Time(hh:mm:ss) | | |
| 9 | Wed(5/7) | 15:23:08 | | |
| 10 | Thu(5/8) | 34:05:54 | | |
| 11 | Total: | 49:29:02 | | |
| 12 | | | | |
| 13 | Device Usage Details | | | |
| 14 | No. | Device Name | Device Address | Usage Time(hh:mm:ss) |
| 15 | 1 | | | 00:00:00 |
| 16 | 2 | | | 14:55:00 |
| 17 | 3 | | | 17:00:59 |
| 18 | 4 | | | 17:33:03 |
| 19 | | | | |
| 20 | | | | |
| 21 | | | | |

Flat Panel Usage Statistics

**Figure 33-15 Flat Panel Usage Statistics**

## 33.8 Basic Settings

In Basic Settings module, you can configure material storage location and configure video walls.

### 33.8.1 Set Weather Web Manufacturer

You can enable weather service and set the weather manufacturer for the programs including weather information. After enabled, you can add a weather window in the program and display the weather information provided by the manufacturer.

Select **Weather Web Manufacturer** on the left navigation bar, and enable **Weather Web Manufacturer**.

Select the manufacturer name, and then enter the authorization code.

**Note**

The user should buy the weather service from the weather manufacturer and get the authorization code.

### 33.8.2 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

**Steps**

1. On the left navigation pane, click **Basic Settings → Material Storage Location** .
2. Set the storage location as **Local Storage** or **pStor**, and select a resource pool.

   **Note**

   To select **pStor** as the storage location, make sure you have added pStor servers to the platform.
3. Click **Save** to save the above settings.

### 33.8.3 Add a Display Wall for Digital Signage Terminal

A display wall is made up of multiple terminals. After adding more than one terminals to the platform, you can configure display walls with custom dimensions (row × column).

**Before You Start**

Make sure you have added at least two terminals to the platform and have enabled the ***time synchronization of NTP server*** .

**Steps**

1. On the left, select **Basic Settings → Video Wall Configuration** .
2. Click **Add**.

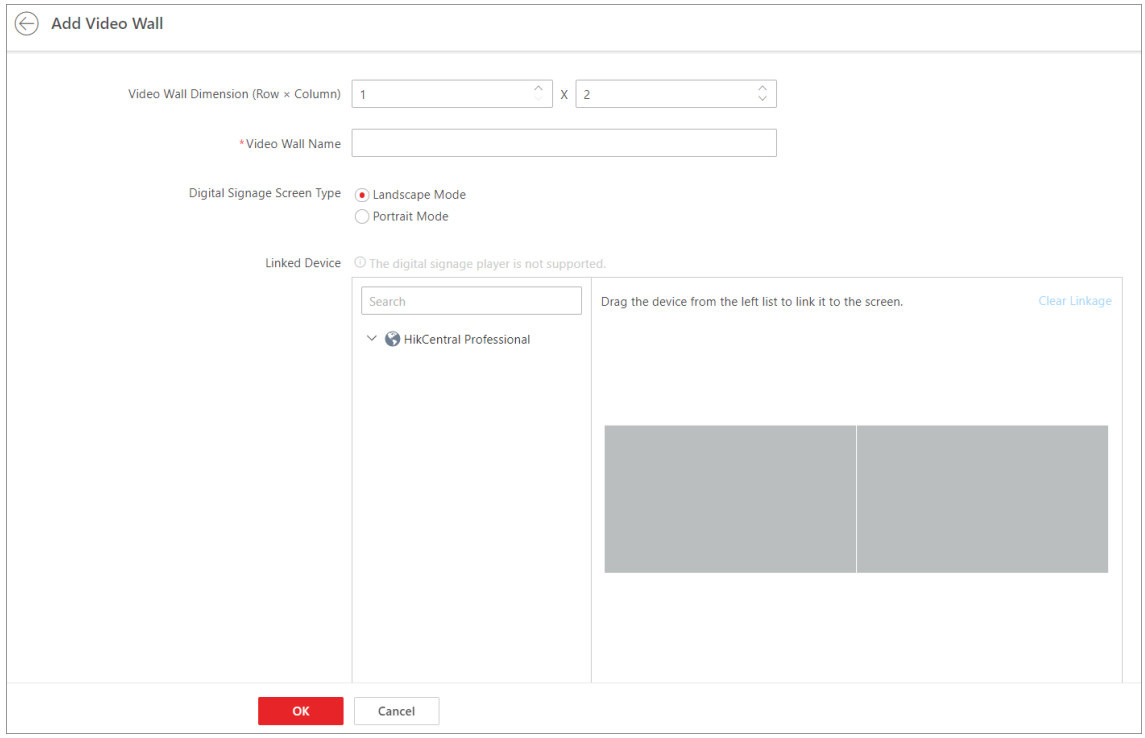



**Figure 33-16 Add Display Wall**

3. Specify the display wall dimension (row × column).
4. Enter the display wall name.
5. Select **Landscape Mode** or **Portrait Mode** as the screen type.
6. In Linked Device area, drag the devices from the device list to the screen on the right.

**Note**

The digital signage player is not supported.

7. **Optional:** Click **Clear Linkage** to clear the linked devices from the screen.
8. **Optional:** Enter the description of the display wall.
9. Click **OK**.
10. **Optional:** After adding display walls, you can perform the following operations.

| | |
|---|---|
| **Switch Display Mode** | Click / to display the added display walls in the thumbnail/list mode. |
| **Edit Display Wall Information** | • In thumbnail mode, click the display wall card to enter the display wall information page and edit the information.<br>• In list mode, click the name of the display wall to enter the display wall information page and edit the information. |
| **Delete Display Walls** | Select one or multiple added display walls and click **Delete** to delete the selected display walls. |

| | |
|---|---|
| **Refresh Display Wall List** | Click **Refresh** to refresh the display wall list. |
| **Search for Display Walls** | Click , set the search conditions such as dimension and screen type, and click **Search** to search for the target display walls. |

## 33.9 Device Control

The platform supports controlling selected devices (including digital signage terminals, interactive flat panels, LED controllers, and display walls) by clicking buttons of general functions, and creating a combined control command to control devices.

### 33.9.1 Control a Device

You can control the devices after adding them to the platform.

**Note**

Make sure you have added devices to the platform.

On the left, select **Device Control → Device Control** .

#### General Operations When Devices are Selected

Check devices of different types, and then click buttons on the top.

**Open/Close Screen**

Turn on/off the device sleep mode. If it is turned off, the screen will be woke up from the sleep mode.

**Restart**

Restart selected devices.

**Play/Stop**

Play/stop the programs on the terminal(s).

**Stop Cut-In**

Stop cutting in programs.

**Clear Playing Contents**

Clear all the contents to be played on the screen(s), including programs, cut-in programs, etc.

**Volume**

Set the output volume of the selected device(s).

**Time Startup/Shutdown**

The device(s) will start up / shut down according to the schedule.

**Combined Control**

When you need to control multiple devices in a batch, you can create a combined control command for the devices and then control them in a batch. See ***Create a Combined Control Command for Multiple Devices*** .

**Restore Default Settings**

Only available for digital signage terminals.

**Enable/Disable Sync Playing**

Enable/disable sync playing the same released contents on different digital signage terminals.

**Note**

Make sure you have enabled the time synchronization of NTP server.

**Remote Debugging**

Enable the Android debug bridge for the device(s), and enter the debugging contents.

**Export Log**

Export the logs of the device(s) in ZIP format.

**Remote Control**

Hover the cursor on a device, and click **Remote Desktop** to connect the device and operate on the device remotely.

**Note**

This should be supported by the device.

**Note**

The operations should be supported by the selected device type(s).

## Other Operations

**Switch Display Mode**

Click / to display the added devices in thumbnail/list mode.

In the Show Thumbnail mode, hover over a device and click in the lower-right corner to view device information.

**Filter by Device Type**

In the drop-down list of the **Device Type**, select **Digital Signage Terminal** / **Interactive Flat Panel** / **Display Wall**.

**Filter by Device Status**

Select **Open Screen** / **Close Screen** / **Offline** to filter devices by status.

**Refresh Device List**

Click **Refresh** to refresh the device list.

**Search for a Device**

In the text bar on the right, enter a device name to search for it.

### 33.9.2 Create a Combined Control Command for Multiple Devices

When you need to send multiple control commands to devices at a time, you can create a combined control command for the devices. The platform supports controlling digital signage terminals, interactive flat panels, and display walls.

**Before You Start**
Make sure you have added devices to the platform.

**Steps**
1. On the left, select **Device Control → Combined Control Command** .
2. Click **Add** to enter the Create Combined Control Command page.
3. Enter a name for the command group.
4. Select a device type.
5. In the Select Control Command area, click the buttons under each tab to add it to the Command Details on the right.
6. Click **Save** to save the command, or click **Execute** to execute the command.
   The added command will be displayed in the command list.
7. **Optional:** Perform the following operations if needed.

| | |
|---|---|
| **Execute a Command** | Click **Execute** to execute a command in the list. |
| **Delete Command(s)** | Click **Delete** behind a command to delete it, or check **All Commands**, and then click **Delete** on the top to delete all commands in the list. |
| **Search for Command(s)** | On the upper-right, enter the name of the combined control demand to search for it. |

## 33.10 Application Management

You can give algorithm capabilities to devices by configuring device application packages. After you finish configuring, you can add and apply the applications to interactive flat panels and manage the applications.

### 33.10.1 Add Applications

You can add device applications to the platform, and then apply them to interactive flat panels.

**Before You Start**
Make sure the interactive flat panels you are going to use are added to the platform.

**Steps**
1. On the left, select **Application Management** to enter the Application Management page.

2. Click **All Applications → Add** .
3. Click to upload application package(s) from the local PC, and add function descriptions if there are any.
4. Click **Next**, and then select available device(s) to apply the application.
5. Click **Save**.
6. **Optional:** Perform the following operations after applying applications to device(s).

**Control Application Installation**

On the upper right, click **Application Installation Control** to select the installation control mode. After the mode settings, you can view which applications are allowed / not allowed to be applied to the selected device(s) on the **All Applications** pane.

**All Applications Allowed**

All applications are allowed to be applied to devices.

**Only Selected Applications Allowed**

Only selected applications are allowed to be applied to the selected devices.

**Only Selected Applications Not Allowed**

Only selected applications are not allowed to be applied to the selected devices.

**Apply Application to Device**

Select added application(s) and click **Apply to Device** to apply the selected application(s) to the device(s). There will be a pop-up window showing the process of the application, and you can click **Cancel** to cancel the applying process. If the device loses power during the applying process, the platform will continue to apply the application after powering on the device again.

**View Application Usage Statistics**

On the upper right, click **View Application Usage Statistics** to view statistics of application usage. You can export the statistics data to the local PC. See ***Statistics and Reports*** for details.

**View Application Records**

Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time period.

**Note**

The icon indicates that adding device application(s) failed.

**Operations for a Device**

After applying applications to the device, you can go to **All Devices** to view the applied applications of a device. You can select a device on the left and perform the following operations:

- Click **Add** to upload and apply application(s) to the selected device.
- Select application(s) and click **Uninstall** to uninstall the selected application(s) on the device.

### 33.10.2 Manage Applications on Devices

You can manage device applications after adding them.

**Note**

Make sure the devices you are going to use are added to the platform.

On the LEFT, select **Application Management** to enter the Application Management page.

You can perform the following operations.

| | |
|---|---|
| Add Device Application to Specific Device | Select an interactive flat panel in the list, and click **Add** to add an application to the device.<br>**Note**<br>Only one application can be added at a time. |
| Uninstall Application | Select an interactive flat panel in the list, select applications on the right, and click **Uninstall** on the top to uninstall applications. |
| Refresh Device Application List | Click **Refresh** to refresh the application list. |
| View Application Records | Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time periods.<br>**Note**<br>The icon ⓘ indicates that applying device application(s) failed. |

# Chapter 34 Broadcast Management

You can manage the added speaker units in the platform and configure the related functions for them. For example, you can group multiple speaker units, configure live broadcast, configure scheduled broadcast, etc.

On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.

## 34.1 Set Basic Settings for Broadcast

You can set locations to save the audio file and live broadcast recording file, set parameters related with live broadcast, such as broadcast mode and encoding format, and set advanced parameters, such as the delay time of custom content broadcast and audio file broadcast.

On the left navigation pane, click **Basic Configuration**, set the required parameters, and save the settings.

**Audio File**

Select **Local Storage** or **pStor** (make sure you have added pStor) as the location to save the audio file, and select the corresponding resource pool.

**Live Broadcast Recording**

check **Live Broadcast Recording**. Select **Local Storage** or **pStor** as the location to save the recording file, and select the corresponding resource pool.

**Live Broadcast Parameters**

**Broadcast Mode**

**Default**

The SYS server automatically judges via which method to send the broadcast data to the speaker unit according to the network domain of the Client (Web Client, Control Client, or Mobile Client).

**Via Streaming Server Proxy**

The Client sends the broadcast data to the speaker unit via the streaming server.

**Direct Access**

The Client directly sends the broadcast data to the speaker unit.

**Via Center Proxy**

The Client sends the broadcast data to the speaker unit via the SYS server.

**Encoding Format**

Select MP3 or G711_u. MP3 is a compressed audio format primarily used for music and general audio storage, offering smaller file sizes with some loss of quality, suitable for streaming and playback. G.711_u is an uncompressed, low-latency codec designed for telephony, preserving voice clarity in real-time communications like VoIP calls.

**Prompt Sound**

Enable and select a media file (make sure you have added media files) to play the corresponding audio as a prompt of alarm during live broadcast.

**Broadcast Priority**

To prevent situations where multiple audio tasks (e.g., live broadcasts, alarm linkage broadcast) are triggered simultaneously and cannot be played flexibly according to actual needs, you can customize priority for different scenarios. Set unified priorities (0-15, the higher the value, the higher the priority) for live broadcasts, emergency mustering linkage broadcast, and scheduled broadcast. High-priority tasks can interrupt low-priority ones; different task types can be mixed audibly.

**Custom Content Broadcast Delay**

If you select Broadcast Mode as **Custom Broadcast Content** and enable this, the broadcast will be auto delayed to play across multiple devices.

This feature ensures synchronized playback across multiple broadcast terminals by addressing inconsistencies caused by processing sequences or network delays. After NTP time synchronization, Audio playing is scheduled for a specific future time (current time + delay), ensuring all terminals start simultaneously at the agreed moment.

**Audio File Broadcast Delay**

If you select Broadcast Mode as **Audio File** and enable this, the broadcast will be auto delayed to play across multiple devices.

This feature ensures synchronized playback across multiple broadcast terminals by addressing inconsistencies caused by processing sequences or network delays. After NTP time synchronization, Audio playing is scheduled for a specific future time (current time + delay), ensuring all terminals start simultaneously at the agreed moment.

## 34.2 Group Speaker Units

You can group multiple speaker units for convenient management. Take the scenario of an industrial park for example, if there are 10 speaker units on the first floor, you can group all these speaker units into a group.

**Steps**

1. On the left navigation pane, click **Speaker Unit Group**.
2. Create a speaker unit group.
   1) Click .
   2) Enter the name for the group.
   3) Click **Add**.

3. Add speaker unit(s) to the speaker unit group.
   1) Click **Add**.
   2) In the pop-up device list, select speaker unit(s) to be added.
   3) Click **Add**.
4. **Optional:** Perform the following operations.

| | |
|---|---|
| **View Audio File** | Click to view the audio file(s) of the corresponding speaker unit. |
| **Delete Speaker Unit** | Check one or more speaker units to be deleted, and click to delete the selected devices. |
| **Adjust Volume** | Check one or more speaker units, and click **Alarm/Broadcast Volume** to adjust the volume of scheduled broadcast, live broadcast, alarm linkage broadcast, emergency mustering linkage broadcast for the selected devices.<br>**Note**<br>For Hikvision devices, you can only adjust the volume of live broadcast. |
| **Mixing Audio Volume** | Click **Mixing Audio Volume** to set volume for multiple audios.<br>Mixing audio volume defines the percentage of low-priority volume relative to high-priority volume when tasks of different priorities play simultaneously.<br>Example: In a scenario where background music (Priority 5) mixes with a fire alarm audio (Priority 15) in a shopping mall, setting the mixing volume to 30% reduces the background music to 30% volume during alarms. Normally, the background music plays at 100% volume; during alarms, the alarm audio plays at full volume while the background music continues at 30%; after alarms, the background music returns to 100%. |

## 34.3 Manage Media Files

You can upload and manage media files to the platform. The uploaded media files can be used for live broadcast, scheduled broadcast, etc.

**Before You Start**

Make sure you have saved the media files to be uploaded to your local PC.

**Steps**

1. On the left navigation pane, click **Media Library**.
2. Select a media library (except the root library on the top) from the list, or click to add a new media library under the root library.

   You can view all the media file(s) in the selected media library.
3. Click **Add**.
4. Select one or more media files from local PC.

**Note**

The file should be in MP3 or WAV format, and no larger than 100 MB.

5. Click **Upload**.

**Note**

You can view the uploading progress and result(s).

The uploaded media file(s) are displayed in the list.

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

| | |
|---|---|
| **Add** | Click **Add** to add more media files. |
| **Delete** | Select one or more media files, click **Delete** to delete the selected files. |
| **Download** | Click in the Operation column to download the media file to local PC. |
| **Play** | Click in the Operation column to play a media file. |
| **Apply to Paging Microphone** | Select media file(s) and click **Apply to Paging Microphone** to apply the media file to the selected paging microphone for audio broadcast. |

## 34.4 Configure Live Broadcast

You can select the speaker unit(s) and the broadcast mode to configure live broadcast. The corresponding audio file or the user's voice will broadcast on the speaker unit(s) in real time.

**Before You Start**

- Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.
- Make sure you have added media file(s) to the media library. Refer to ***Manage Media Files*** for details.

**Steps**

1. On the left navigation pane, click **Live Broadcast and Recording → Live Broadcast** .
2. Select the online speaker unit(s) for live broadcast.
   - Select **Group**, and select one or more speaker units from speaker unit group(s). You can click **Display Terminals Not Grouped** to display the speaker unit(s) that are not grouped.
   - Select **Area**, and select one or more speaker units from the area(s) where the speaker units are added.

**Note**

- You can hover on a speaker unit, and click to listen to the live broadcast content. During listening, you can click to adjust the volume, and click to stop listening. This function should be supported by the device.
- You can check **Exclude Abnormal Device** to filter out abnormal devices.

3. Select the broadcast mode.
   - Check **Speak**.

- Check **Audio File**, and select an audio file from the media library. You can click **Download** to download and play the selected audio file beforehand to ensure the audio can broadcast fluently and correctly.
- Check **Custom Broadcast Content**, select a language, and enter the broadcast content as needed.

  Select **Once** or **Specified Duration** as the play mode.

4. Click **Start**.

**Note**

After starting broadcasting, you can click in the Operation column to listen to the broadcast content; click to adjust the volume; and click to stop listening. This function should be supported by the device.

**What to do next**

Speak to the PC microphone, play the audio file, or play the custom broadcast content.

## 34.5 Search for Live Broadcast Records

You can set search conditions including the start time, end time, and the broadcaster to search for live broadcast records.

**Before You Start**

- Make sure you have finished live broadcast. Refer to ***Configure Live Broadcast*** for details.
- Make sure you have enabled the function of **Live Broadcast Recording**. For details, refer to ***Set Basic Settings for Broadcast*** .

**Steps**

1. On the left navigation pane, click **Live Broadcast and Recording → Live Broadcast Recording** .
2. Set the start time.
3. Set the end time.
4. Select a broadcaster from the drop-down list.
5. Click **Search**.

   You can view the search results on the right side and view the details of each record, including the broadcaster, the number of the speaker units, the start time, the broadcast mode, and the file size.
6. **Optional:** Perform the following operations.

| | |
|---|---|
| **View Speaker Unit** | Click › to view the speaker unit. |
| **View Custom Broadcast Content** | If the broadcast mode is **Custom Broadcast Content**, hover the mouse cursor over in the Operation column to view the custom broadcast content. |

## 34.6 Add a Scheduled Broadcast Task

You can configure the parameters such as the period type and play mode to add a scheduled broadcast task in the platform and then apply the task to the speaker unit(s). After that, the audio file(s) you have selected will be played on the corresponding speaker unit(s) according to the schedule. For the added scheduled broadcast task(s), you can view the task details, search for target task(s), etc.

**Before You Start**

Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.

**Steps**

1. On the left navigation pane, click **Scheduled Broadcast**.
2. Click **Add** to enter Add Scheduled Broadcast page.
3. Enter the name for the scheduled broadcast task.
4. Select the speaker unit(s) to execute the task.
   - Check **Group**, click **Add**, select one or more speaker units from speaker unit group(s), and click **Add**.
   - Check **Area**, select one or more speaker units from the Available list, and add them to the Selected list.
5. Configure broadcast priority.
6. Configure the broadcast content.
   - Select **Audio File**: click **Add** to add audio files from media library. You can click ↑ or ↓ to adjust the sequence of playing audio files.
   - Select **Custom Broadcast Content**: select a language and enter the playing content.
7. Configure the playing schedule.
   1) Select **Every Day** or **Every Week** as the period type, and set the start and end date, etc.

      **Example**

      If you select **Every Week**, set the start and end date as "2025.02.01" and "2025.02.28", and set the repetition day of week as "Tuesday", then the scheduled broadcast task will be played on Tuesday every week from 2025.02.01 to 2025.02.28.
   2) Set the playing time, including the broadcast time and play mode.

      **Example**

      If you set the broadcast time as "8:00", and the play mode as once, then the broadcast task will be played at 8:00 once a day.
8. Click **Save and Apply**.
9. **Optional:** Perform the following operations.

| | |
|---|---|
| **View Details** | View the details of the added scheduled broadcast task, including the broadcast time, start date and end date, period type, the number of speaker units, etc. |

**Note**

You can click › to view more details.

| | |
|---|---|
| **Play/Stop Audio** | • Click **Play** to play the audio of a corresponding scheduled broadcast task.<br>• Click **Stop** to stop playing the audio. |
| **Apply** | • Click **Apply All** to apply all the tasks to the speaker units.<br>• Select the tasks to be applied, click **Apply All** to apply the selected tasks to the speaker units. |

**Note**

You can view the application process and the results. For the applying failed tasks, you can view the failure reasons.

| | |
|---|---|
| **Search** | Enter keywords in the search box in the upper-right corner, and click to search for the target task(s). |
| **Delete** | Check one or more tasks, click **Delete** to delete the selected tasks. |
| **Enable/ Disable** | Click **Enable** or **Disable** to quickly resume or pause scheduled broadcast tasks without deleting or editing the task content. |

## 34.7 Add a Linked Broadcast Task

You can configure the parameters such as the broadcast content and play mode to add a linked broadcast task in the platform and then apply the task to the speaker unit(s). After that, the broadcast content will be played when the emergency is triggered in the selected areas. For the added linked broadcast task(s), you can view the task details, search for target task(s), etc.

**Before You Start**

Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.

**Steps**

1. On the left navigation pane, click **Linked Broadcast**.
2. Click **Add** to enter Add Broadcast Linkage page.
3. Enter the name for the linked broadcast task.
4. Select a broadcast area.
5. Select the speaker unit(s) to execute the task.
6. Select the broadcast content.
   - Check **Audio File**, and click **Add** to add the audio file(s) from the media library.

**Note**

- For the added audio files, you can click ↑ or ↓ to adjust their playing sequences; click 🗑 to delete an audio file.
- For details about adding media files, refer to ***Manage Media Files*** .

- Check **Custom Broadcast Content**, and enter the broadcast content as needed.

7. Add an audio file as needed.
8. Select the play mode.

**Once**

The linked broadcast will only be played once.

**Specific Duration**

The linked broadcast will be played for the configured duration.

**Repeat**

The linked broadcast will be played continuously until the status of emergency is ended.

9. Click **Save and Apply**.

You can view the applying progress and the result.

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

| | |
|---|---|
| **Edit a Task** | Click the broadcast name to edit its parameters as needed. |
| **View Emergency Mustering Configuration** | Click **View Emergency Mustering Configuration** to enter Emergency Mustering module and view the emergency mustering configuration.<br>**Note**<br>For details, refer to ***Add Emergency Solution*** . |
| **View Applying Failed Task(s)** | ⓘ indicates that the broadcast task(s) are failed to be applied.<br>• Move the mouse cursor to ⓘ beside the broadcast name, and click **View Details** to view the failure details of the current task.<br>• Move the mouse cursor to ⓘ beside **Apply All**, and click **View Details** to view the failure details of all the tasks. |
| **Apply Task Again** | When there are task(s) that failed to be applied, you can apply the task(s) to the speaker units again.<br>• Move the mouse cursor to ⓘ beside the broadcast name, and click **Try Again** to apply the current task again.<br>• Move the mouse cursor to ⓘ beside **Apply All**, and click **Try Again** to apply all the tasks again. |

**Note**

During the applying process,you can view the application process and the results. For the applying failed tasks, you can view the failure reasons.

**Delete a Task**

Click **Delete** to delete a linked broadcast task.

**Note**

If a linked broadcast is taking effect as the emergency is triggered in the selected areas, it cannot be deleted.

# Chapter 35 Skin-Surface Temperature Screening

After adding the temperature screening cameras and access control devices with temperature screening function to the system, you can view the temperature of the detected persons in the Skin-Surface Temperature module. The system also shows whether the detected person is wearing a mask or not. With skin-surface temperature screening and mask detection functions, the system provides an alert if an individual is running a fever or not wearing a mask.

In the Skin-Surface Temperature module, you can view the real-time and history temperature screening records and face mask detection records. You can also generate a report about these records to view the overall information.

**Note**

The mask detection function will show when the mask related function is turned on in the **System → Normal → User Preference** page.

## 35.1 Temperature Screening Configuration

Before temperature screening, you should set temperature screening point groups and add related temperature screening points to the added groups. Also, for the temperature screening points, you can configure their parameters including temperature screening threshold and alarm threshold.

### 35.1.1 Group Temperature Screening Points

You can group multiple temperature screening points for convenient management. For example, you can group all the temperature screening points on the same floor into a group.

**Steps**

1. On the top navigation bar, select → **Passing Management → Temperature Screening** .
2. On the left pane, click **Basic Configuration → Temperature Screening Configuration** .
3. Create temperature screening point group(s).
   1) Click + on the upper left corner of the page.
   2) Enter the name for the temperature screening point group as desired.
   3) Click **Add**.
4. Add temperature screening point(s) for the added temperature screening point group.

   **Note**

   Temperature screening points can be cameras and access control points that support temperature screening.

   1) Click **Add**.
   2) In the pop-up device list, check temperature screening point(s) as desired.

**Note**

You can enter a key word (supports fuzzy search) in the search box to quickly search for the target device(s).

3) Click **Add**.

5. **Optional:** After adding temperature screening point(s), perform following operations.

| | |
|---|---|
| **Delete** | • Click to delete single temperature screening point.<br>• Check multiple temperature screening points, and click **Delete** to batch delete the selected devices. |
| **Configure Parameters** | Check one or multiple temperature screening points, and click **Configuration** to configure related parameters for the selected device(s). |
| | **Note**<br>For details, refer to ***Configure Temperature Screening Parameters*** . |
| **Export** | Click **Export** to export detailed information of temperature screening point(s) such as device type, serial No., and temperature screening threshold to the local PC. |

## 35.1.2 Configure Temperature Screening Parameters

For the added temperature screening point(s), you can configure the related parameters including temperature screening threshold and alarm threshold.

Check one or more added temperature screening point(s), and click **Configuration** to configure temperature screening parameters.

**Temperature Screening Threshold**

Set the threshold for temperature screening. When the detected skin-surface temperature is higher than the threshold, a temperature screening event will be triggered.

**Alarm Threshold**

Set the threshold for alarm. When the detected skin-surface temperature is higher than the threshold, an alarm will be triggered.

**Note**

- The temperature screening threshold should be smaller than alarm threshold.
- For temperature screening points which are access control points, you should configure their temperature screening parameters on the device parameters configuration page.

## 35.2 Real-Time Skin-Surface Temperature Monitoring

You can view the latest skin-surface temperature information detected by screening points. If there are persons whose skin-surface temperatures are abnormal, you will know at the first time. Besides, you will be able to quickly locate the persons according to the displayed screening point name and screening group. For unregistered persons, you can quickly register for them.

On the top navigation bar, select → **Passing Management** → **Temperature Screening** . Then on the left pane, click **Skin-Surface Temperature**. Select a temperature screening point group on the left. Red number indicates the number of skin-surface temperature screening points. Black number indicates the total number of devices in a temperature screening point group.

In the Picture area, the latest captured picture is displayed on the left. When new pictures are captured and displayed here, old captured pictures will be displayed on the right as thumbnails with faces, screening point name, person name, similarity, temperature, wearing mask or not, and detecting time.

Persons with different features will be marked by different colors. Orange means the captured person is not wearing a mask, but skin-surface temperature is normal; red means the captured person's skin-surface temperature is abnormal; green means the captured person's skin-surface temperature is normal and the person is wearing a mask. Click **More** to jump to the History page to view more captured pictures.

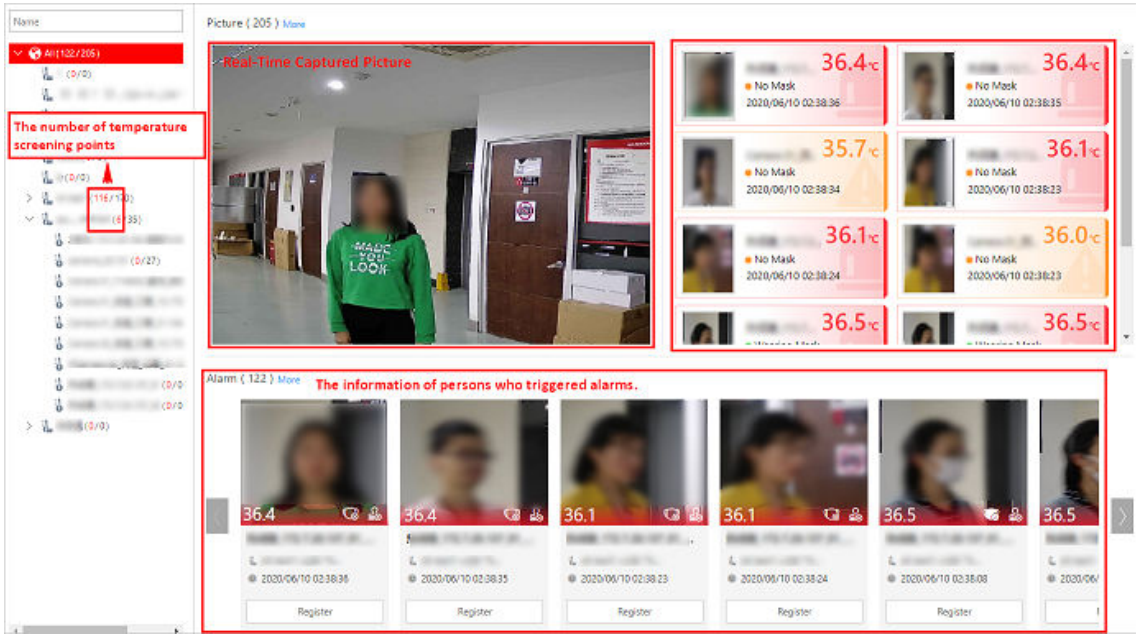



**Figure 35-1 Real-Time Skin-Surface Temperature**

When a person's skin-surface temperature exceeds the threshold you set, or the person is not wearing a mask, an alarm will be triggered. In the Alarm area, the pictures and information of persons who have triggered alarms are displayed. Following the title Alarm, the alarm amount is

displayed. See *The User Manual of HikCentral Professional Web Client* for details about how to set a temperature threshold.

The person information includes skin-surface temperature, wearing mask or not, registered or unregistered, temperature screening point name, temperature screening point group name, and detecting time. You can click **Register** to register for the person, or click **More** to go to the History page to view more alarm information.

## 35.3 Search History Temperature Screening Data

You can set search conditions such as start time, end time, and skin-surface temperature to search for history temperature screening data.

**Before You Start**

Make sure temperature screening data has been generated in real-time skin-surface temperature monitoring.

**Steps**

1. On the top navigation bar, select → **Passing Management** → **Temperature Screening** .
2. On the left pane, click **History**.
3. Select a temperature screening point group or a temperature screening point from the list.
4. Click to unfold the Filter panel.
5. Set the search condition(s) including start time, end time, skin-surface temperature, etc.
6. Click **Filter**.

   History temperature screening data that meets the search condition(s) will be displayed below.
7. **Optional:** For the searched results, perform the following operations as desired.

| | |
|---|---|
| **View Result Details** | You can view the detailed information of the searched results, including temperature screening group, temperature screening point, captured time, person's skin-surface temperature, whether wearing masks, etc.<br>**Note**<br>represents that the person wears a mask, and represents that the person doesn't wear a mask. |
| **Edit/Register Person Information** | You can edit or register person information based on the different icons.<br>• : The person is registered. For the registered person, click **Edit** to edit the person information.<br>• : The person is unregistered. For the unregistered person, click **Register** to enter person's registration information. For details, refer to ***Register Person Information*** . |
| **Export** | Click **Export** to export temperature screening data including temperature screening point, temperature screening point group, temperature status, etc., in excel file. |

## 35.4 Registration

To manage the people who have been screened skin-surface temperature conveniently, you can register for them by entering their personal information. After registration, you can view and filter the registered persons' information.

### 35.4.1 Register Person Information

For unregistered persons displayed on real-time skin-surface temperature page or history page of skin-surface temperature, you can register for them.

**Steps**

1. On the top navigation bar, select → **Passing Management** → **Temperature Screening** .
2. On the left pane, select **Skin-Surface Temperature** or **History**.

   The skin-surface temperature screening information will be displayed.
3. If a screened person is not registered, you can click **Register** to enter the Register page to register for the person.

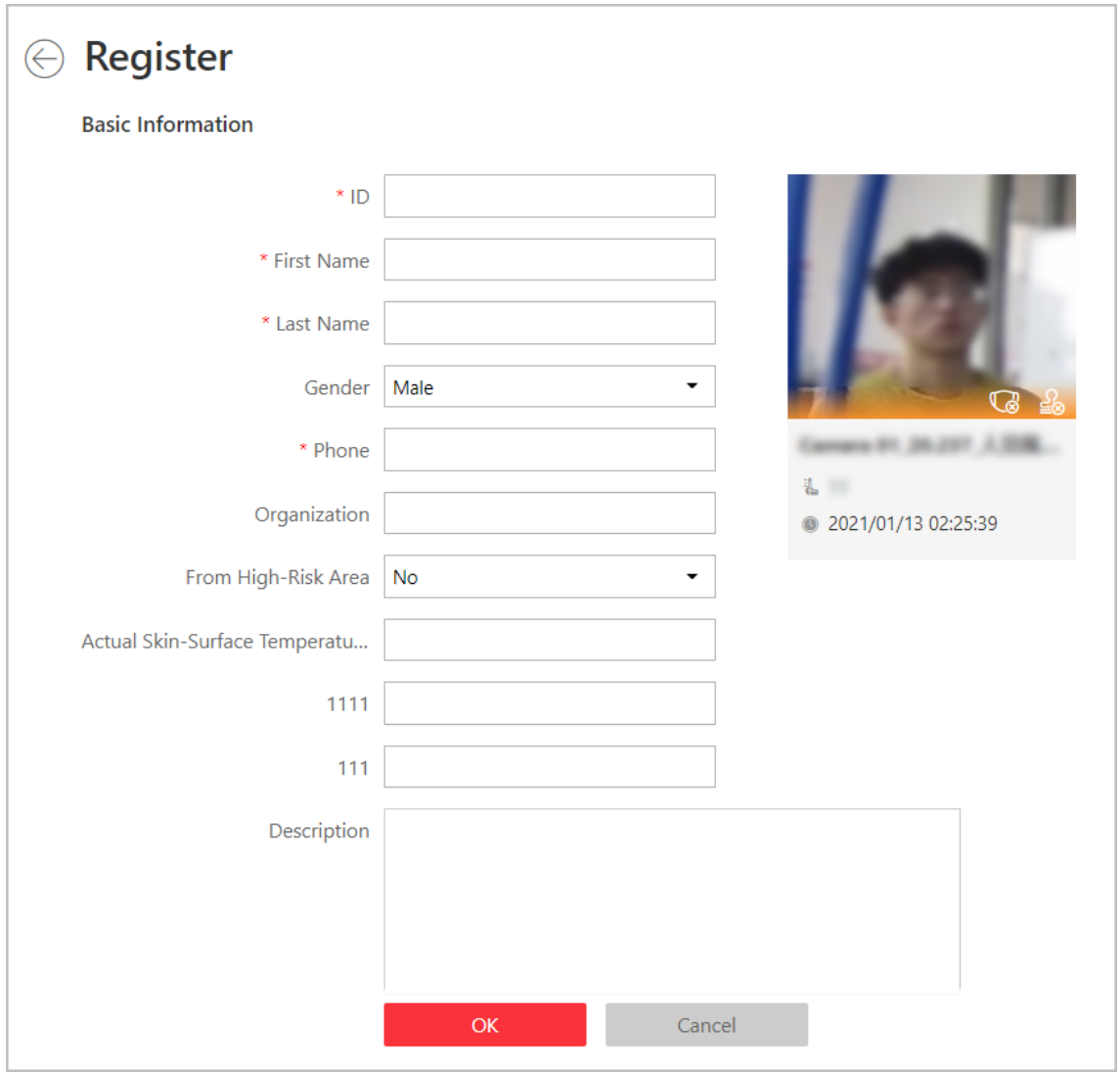



**Figure 35-2 Register Page**

4. Set personal information, including ID, name, phone number, whether from high-risk areas etc.

**Note**

You can custom the information displayed on this page according to your needs. See ***Customize Registration Template*** for details.

5. Click **OK** to finish the registration.

Registered persons' information will be displayed on Registration page for a centralized management. See ***View Registered Person Information*** for details.

### 35.4.2 Customize Registration Template

You can set customized person information for registration which are not predefined in the system according to your actual needs.

**Steps**

**Note**

Up to 5 additional items can be added.

1. On the top navigation bar, select → **Passing Management** → **Temperature Screening** .
2. On the left pane, click **Registration**.
3. Click **Registration Template** to enter the Registration Template page.
4. Click **Add**.
5. Create a name for the additional item.

   **Note**

   Up to 32 characters are allowed for the name.
6. Select the format type as general text, number, date or single selection for the additional item.

   **Example**

   For example, if you select general text, you need to enter words for this item when registering person information.
7. Click **Add**.
8. **Optional:** Perform one or more of the following operations.

   **Edit Name** Click to edit the name.

   **Delete** Click to delete the additional item.

### 35.4.3 View Registered Person Information

For the registered persons, you can view their detailed information including person name, ID, phone, skin-surface temperature, wearing mask or not, etc.

On the top navigation bar, select → **Passing Management** → **Temperature Screening** . Then on the left pane, click **Registration**.

You can view person name, ID, phone, skin-surface temperature, wearing mask or not, registering time and other information in the list.

Click in the Operation column to edit person information as desired.

Click **Export** on the upper left corner of the page to export and view detailed registered person information in excel file.

## 35.5 Search for Temperature Screening Records

Skin-surface temperature screening records give you an overview of skin-surface temperature, mask-wearing detection results, and registered person information. Based on the temperature status and mask-wearing detection results, you will quickly learn how many person's skin-surface temperatures are abnormal and how many persons are not wearing masks. With registered person information, you can quickly filter persons with abnormal skin-surface temperature or with no mask on to learn their detailed information such as name, location, face picture, from high-risk area or not, etc.

On the top navigation bar, select → **Passing Management** → **Temperature Screening** . Then on the left pane, click **Search**.

Select a temperature screening point group or temperature screening point, set the time range at the bottom and click **Generate Report**.

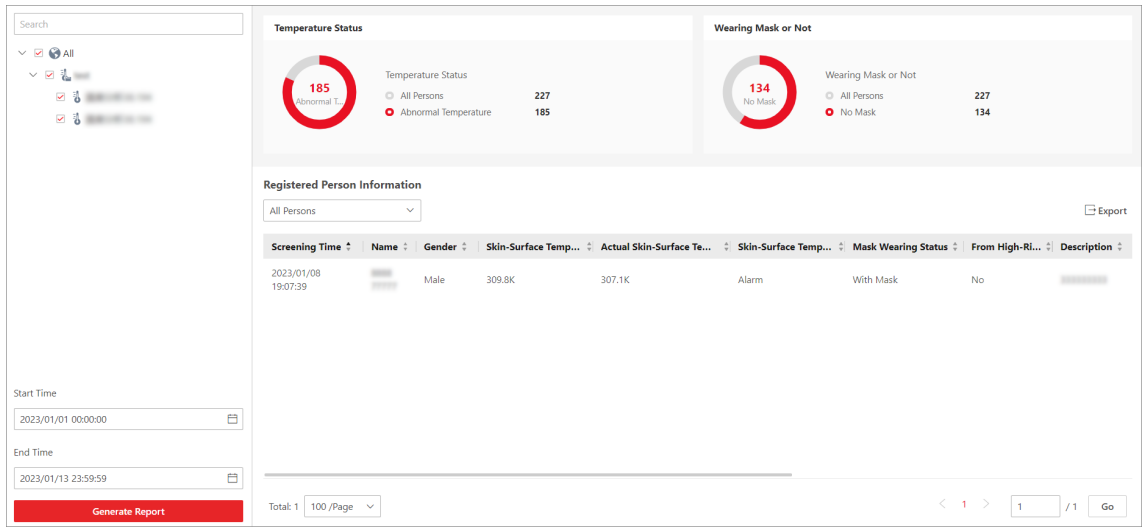



**Figure 35-3 Skin-Surface Temperature Screening Records**

### Temperature Status

Temperature Status gives you the total number of persons whose skin-surface temperatures are screened and the number of persons with abnormal temperature.

### Wearing Mask or Not

It gives you the total number of persons whose mask wearing status had been detected, and the number of persons with no mask on.

### Registered Person Information

You can filter persons with abnormal skin-surface temperature or those not wearing any mask quickly to view their detailed information. For example, if a person with abnormal skin-surface temperature is not wearing a mask, you need to pay attention to him or her. Based on the

temperature screening point name or temperature screening point group name, you can quickly locate the person.
Click to view a person's detailed information including an enlarged face picture, event details, and registered information.
Click **Export** to save the registered person information in your PC as an Excel file.

## 35.6 Generate Skin-Surface Temperature Analysis Report

You can generate skin-surface temperature analysis reports to view the variation trend of the number of people with abnormal skin-surface temperature over a specified time period.

**Before You Start**
Make sure you have added device that supports temperature screening and have enabled temperature screening on the device. For details, see the user manual of the device.

**Steps**
1. On the left navigation bar of the Temperature Screening page, select **Statistics Analysis**.
2. Select a statistics type for the analysis report from **Temperature Screening Point** and **Department**.
3. Select temperature screening point(s) or department(s) for analysis.
   - For selecting temperature screening points:
     a. Click to open the resource list pane.
     b. Select an area in the area list to show the corresponding temperature screening points.
     c. Check the temperature screening point(s) of which the screening results are to be analyzed.
   - For selecting departments:
     Check the department(s) of which the persons' skin-surface temperature screening results are to be analyzed.

     **Note**
     You can check **Select Sub-Groups** to simultaneously select/deselect the sub department(s) of the department that you have selected/deselected.
4. Select a report type from **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report**, or a report with custom time interval.
5. In the Time field, select a predefined time period or customize a time period accordingly.
6. Click **Generate Report**.




**Figure 35-4 Skin-Surface Temperature Analysis Report**

The statistics of the selected item(s) will be displayed.

7. **Optional:** Perform the following operations if required.

| | |
|---|---|
| **Show/Hide Certain Data** | Click the legend to show or hide the screening results of the corresponding statistical object, such as certain temperature screening point or certain department. |
| **View Abnormal Temperature or No Mask Statistics** | In the top left corner of the chart, select Abnormal Temperature or No Mask from the first drop-down list to display the statistics of people with abnormal temperature or those not wearing any face masks respectively. |
| **Switch Between Line Chart and Histogram** | Click / to switch between line chart and histogram. |

8. **Optional:** Export the report to the local PC.
   1) On the top right of the page, click **Export**.
   2) Select the dimension (time-related) of the report to be exported.

      **Example**

      For example, if you are exporting a daily report, you can select from **By Day** and **By Hour**, and you will be able to export 1 or 24 records respectively for each statistical object (i.e., temperature screening point or department).

      **Note**

      For reports of department(s), you may also choose the export content from **By Department** and **By Person**.

   3) Select the format of the exported file from **Excel**, **CSV**, and **PDF**.
   4) Click **Export**.

## 35.7 Configure the Scheduled Report of Screening

You can configure scheduled temperature screening analysis reports by specifying a statistical cycle, the analysis type, and the relevant statistical objects (i.e., temperature screening points or departments). Once set, the platform will send an email to the specified recipient(s) regularly with the report attached, which shows the variation trend of the number of people whose skin-surface temperatures are abnormal during the set time period.

**Steps**

**Note**

- A report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. On the top navigation bar, select → **Passing Management → Temperature Screening → Basic Configuration → Scheduled Report** .
2. Enter the Create Report page.
   - For configuring scheduled reports for the first time, click **Add** in the middle of the page.
   - If you have configured scheduled reports before, click + at the top of the left pane.

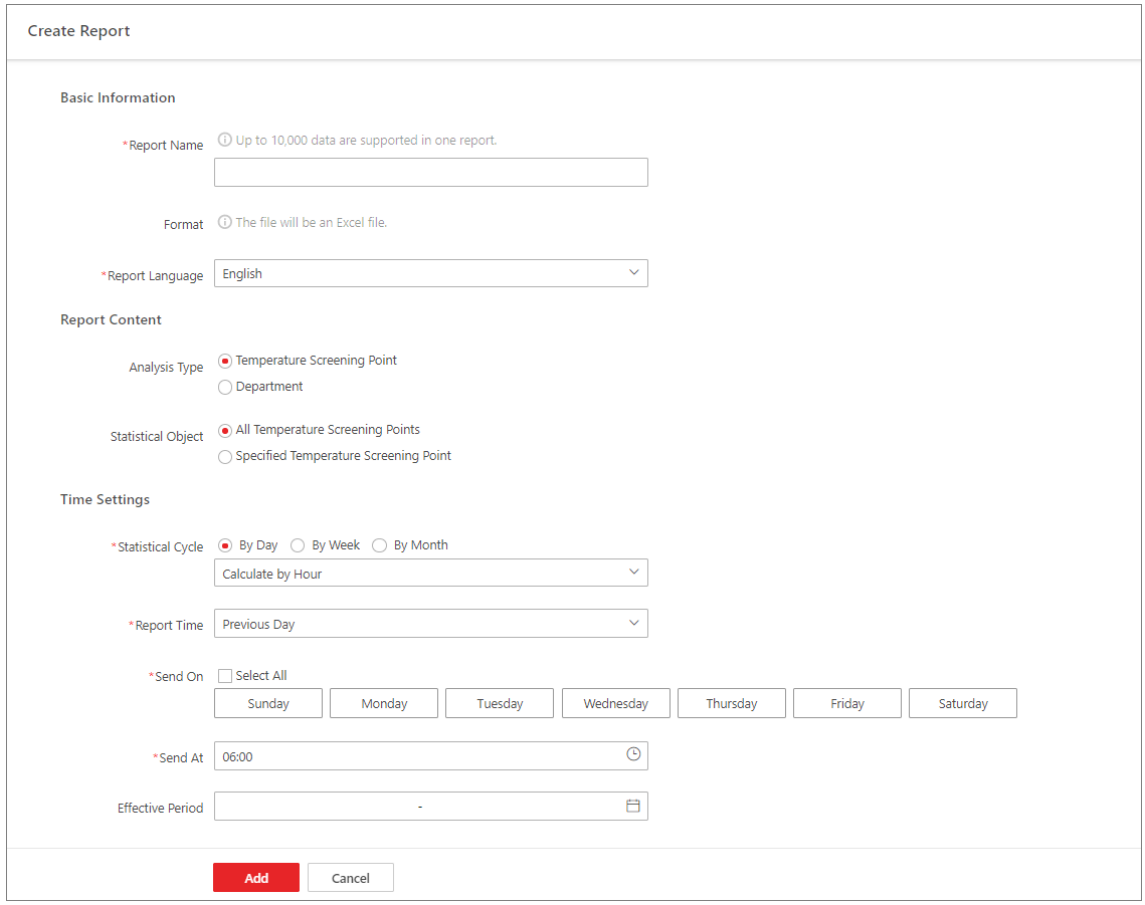



**Figure 35-5 Configure Scheduled Report**

3. Create a name for the report and select a report language from the drop-down list.
4. Set the report content.
   1) Select an analysis type from **Temperature Screening Point** and **Department**.
   2) Select the statistical objects accordingly. You can select all or specify specific temperature screening points / departments.

   **Note**

   If the analysis type is set to **Department**, you may also select the way you would like to export the report content from **By Department** and **By Person**.
5. Select a statistical cycle from **By Day**, **By Week**, and **By Month**, and set the statistical period and report sending time accordingly.

   **By Day**

   The daily report shows data on a daily basis. The platform will send one report at the set sending time on the specified day(s) with analysis results of the previous day.

For example, if you set the sending time as 20:00 and select all days of a week, the platform will send a report at 20:00 every day, containing the analysis results of the day before the current day between 00:00 and 24:00.

**By Week or By Month**

Compared with the daily report, the weekly/monthly report can be less time consuming, since they are not to be generated every day. The platform will send one report on the set day/date at the specified sending time every week/month with analysis results of the last 7/14 days or the current/last month respectively.

For example, for the weekly report, if you set the sending time as 6:00 on Monday and the statistical period as the last 7 days, the platform will send a report at 6:00 every Monday morning, containing the analysis results between last Monday and Sunday.

**Note**

If the analysis type is set to **Temperature Screening Point**, you may also set how the report will present the analysis results generated in the specified time period below the statistical cycle options. You can choose from **Calculate by Hour** and **Calculate by Day** accordingly.

6. **Optional:** Set an effective period (start time and end time) for the scheduled report.
7. **Optional:** Set the advanced parameters.

**Send Report via Email**

Select an email template from the drop-down list to define the recipient information and email format (subject and content), so that the report can be sent to the recipient(s) regularly via email.

**Note**

- You can select an existing email template or click **Add** to add a new one.

**Upload to SFTP**

Configure SFTP settings including the SFTP address, port No., user name, password, and the saving path for the report to be uploaded to the SFTP server regularly.

**Note**

You can also click → **SFTP Settings** at the top of the left pane to configure the corresponding parameters.

**Save to Local Storage**

Configure a saving path for the report to be saved to the local storage regularly.

**Note**

You can also click → **Configure Local Storage** at the top of the left pane to configure the saving path.

8. Click **Add** to finish setting the scheduled report rule.

# Appendix A. 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. |

# Appendix B. 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.**


See Far, Go Further